Politiques FlexConfig

Les rubriques suivantes décrivent comment configurer et déployer les politiques FlexConfig.

Présentation de la politique FlexConfig

Une politique FlexConfig est un conteneur d'une liste ordonnée d'objets FlexConfig. Chaque objet comprend une série de commandes du langage de script Apache Velocity, de commandes de configuration logicielle ASA et des variables que vous définissez. Le contenu de chaque objet FlexConfig est essentiellement un programme qui génère une séquence de commandes ASA qui seront ensuite déployées sur les périphériques affectés. Cette séquence de commandes configure ensuite la fonction associée sur le périphérique défense contre les menaces .

Défense contre les menaces utilise des commandes de configuration ASA pour implémenter certaines fonctionnalités, mais pas toutes. Il n'y a pas d'ensemble unique de commandes de configuration défense contre les menaces . L'objectif de FlexConfig est plutôt de vous permettre de configurer des fonctionnalités qui ne sont pas encore prises en charge directement par les politiques et les paramètres centre de gestion.

Mise en garde Cisco recommande **fortement** d'utiliser les politiques FlexConfig uniquement si vous êtes un utilisateur avancé avec de solides connaissances en ASA, et ce, à vos propres risques. Vous pouvez configurer des commandes qui ne sont pas interdites. L'activation de fonctionnalités par le biais de politiques FlexConfig peut entraîner des résultats imprévus avec d'autres fonctionnalités configurées.

Vous pouvez communiquer avec le centre d'assistance technique de Cisco pour obtenir de l'aide concernant les politiques FlexConfig que vous avez configurées. Le Centre d'assistance technique de Cisco ne conçoit ni n'écrit de configurations personnalisées au nom d'un client. Cisco n'exprime aucune garantie quant au bon fonctionnement ni à l'interopérabilité avec d'autres fonctionnalités du système Firepower. Les fonctionnalités FlexConfig peuvent être obsolètes à tout moment. Pour obtenir une prise en charge des fonctionnalités entièrement garantie, vous devez attendre le soutien centre de gestion. En cas de doute, n'utilisez pas les politiques FlexConfig.

Utilisation recommandée des politiques FlexConfig

Il y a deux utilisations principales recommandées pour FlexConfig :

- Vous passez d'ASA à défense contre les menaces , et vous utilisez (et devez continuer à utiliser) des fonctions compatibles qui ne sont pas directement prises en charge par centre de gestion. Dans ce cas, utilisez la commande **show running-config** sur l'ASA pour afficher la configuration de la fonctionnalité et créez vos objets FlexConfig pour la mettre en œuvre. Expérimentez avec les paramètres de déploiement de l'objet (une fois/chaque fois et ajout/préfixe) pour obtenir le bon paramètre. Vérifiez en comparant la sortie **show running-config** sur les deux périphériques.
- Vous utilisez défense contre les menaces , mais il y a un paramètre ou une fonctionnalité que vous devez configurer. Par exemple, le centre d'assistance technique de Cisco vous indique qu'un paramètre particulier devrait résoudre un problème précis que vous rencontrez. Pour les fonctionnalités complexes, utilisez un appareil de laboratoire pour tester FlexConfig et vérifiez que vous obtenez le comportement attendu.

Le système comprend un ensemble d'objets FlexConfig prédéfinis qui représentent des configurations testées. Si la fonctionnalité dont vous avez besoin n'est pas représentation par ces objets, déterminez d'abord si vous pouvez configurer une fonctionnalité équivalente dans les politiques standard. Par exemple, la politique de contrôle d'accès comprend la détection et la prévention des intrusions, HTTP et d'autres types d'inspection de protocole, le filtrage d'URL, le filtrage d'applications et le contrôle d'accès, que l'ASA met en œuvre à l'aide de fonctionnalités distinctes. Étant donné que de nombreuses fonctionnalités ne sont pas configurées à l'aide des commandes CLI, vous ne verrez pas toutes les politiques représentés dans la sortie de **show running-config**.

Remarque Gardez à tout moment à l'esprit qu'il n'y a pas de recouvrement direct entre ASA et défense contre les menaces . N'essayez pas de recréer complètement une configuration ASA sur un périphérique défense contre les menaces . Vous devez tester attentivement toute fonctionnalité que vous configurez à l'aide de FlexConfig.

Commandes de l'interface de ligne de commande dans les objets FlexConfig

Le défense contre les menaces utilise des commandes de configuration ASA pour configurer certaines fonctionnalités. Bien que toutes les fonctionnalités de l'ASA ne soient pas compatibles avec le défense contre les menaces , certaines fonctionnalités peuvent fonctionner sur le défense contre les menaces centre de gestion, mais que vous ne pouvez pas configurer dans les politiques. Vous pouvez utiliser les objets FlexConfig pour préciser l'interface de ligne de commande requise pour configurer ces fonctionnalités.

Si vous décidez d'utiliser FlexConfig pour configurer manuellement une fonctionnalité, vous êtes responsable de connaître et de mettre en œuvre les commandes selon la syntaxe appropriée. Les politiques FlexConfig ne valident pas la syntaxe des commandes CLI. Pour plus d'informations sur la syntaxe appropriée et la configuration des commandes CLI, utilisez la documentation d'ASA comme référence :

- Les guides de configuration de l'interface de ligne de commande ASA expliquent comment configurer une fonctionnalité. Vous trouverez les guides à l'adresse https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html
- Les références de commande ASA fournissent des informations supplémentaires triées par nom de commande. Vous trouverez les références à l'adresse https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-command-reference-list.html

Les rubriques suivantes expliquent plus en détail les commandes de configuration.

Déterminer la version du logiciel du périphérique ASA et la configuration actuelle de la CLI

Comme le système utilise les commandes du logiciel ASA pour configurer certaines fonctionnalités, vous devez déterminer la version actuelle de l'ASA utilisée dans le logiciel s'exécutant sur le périphérique défense contre les menaces . Ce numéro de version indique quels guides de configuration de CLI ASA utiliser pour obtenir des instructions sur la configuration d'une fonctionnalité. Vous devez également examiner la configuration actuelle basée sur l'interface de ligne de commande et la comparer à la configuration ASA que vous souhaitez mettre en œuvre.

Gardez à l'esprit que toute configuration ASA sera très différente d'une configuration défense contre les menaces . De nombreuses politiques défense contre les menaces sont configurées en dehors de la CLI, de sorte que vous ne pouvez pas voir la configuration en regardant les commandes. N'essayez pas de créer de correspondance un à un entre une configuration ASA et défense contre les menaces .

Pour afficher ces informations, établissez une connexion SSH à l'interface de gestion du périphérique et saisissez les commandes suivantes :

- **show version system** et recherchez le numéro de la version logicielle du périphérique de sécurité adaptatif Cisco. (Si vous saisissez la commande à l'aide de l'outil d'interface de ligne de commande Cisco Secure Firewall Management Center, omettez le mot-clé **system**.)
- **show running-config** pour afficher la configuration actuelle de l'interface de ligne de commande.
- **show running-config all** pour inclure toutes les commandes par défaut dans la configuration actuelle de l'interface de ligne de commande.

Vous pouvez également saisir ces commandes à partir de centre de gestion en utilisant la procédure suivante.

Procédure

Étape 1 Sélectionnez **System (Système)** > **Health (Intégrité)** > **Monitor** (Moniteur).

Étape 2 Cliquez sur le nom du périphérique ciblé par la politique FlexConfig.

Vous devrez peut-être cliquer sur la flèche d'ouverture/fermeture dans la colonne **Nombre** du tableau d'état pour voir les périphériques.

Étape 3 Cliquez sur **Afficher les détails du système et du dépannage**

Étape 4 Cliquez sur **Advanced Troubleshooting** (Dépannage avancé).

Étape 5 Cliquez sur **Threat Defense CLI** (Interface de ligne de commande Threat Defense).

Étape 6 Choisissez **Device** (Périphérique), puis choisissez la commande **show** (afficher) et saisissez **version** ou l'une des autres commandes comme paramètre.

Étape 7 Cliquez sur **Execute** (Exécuter).

En ce qu concerne la version, recherchez le numéro de version du logiciel du périphérique de sécurité adaptatif Cisco.

Vous pouvez sélectionner le résultat et appuyer sur Ctrl + C, puis le coller dans un fichier texte pour analyse ultérieure.

Commandes CLI interdites

Le but de FlexConfig est de configurer les fonctionnalités disponibles sur les périphériques ASA que vous ne pouvez pas configurer sur les périphériques défense contre les menaces à l'aide de centre de gestion.

Ainsi, vous ne pouvez pas configurer les fonctionnalités ASA qui ont des équivalents dans centre de gestion. Le tableau suivant répertorie certaines de ces zones de commande interdites.

En outre, certaines commandes **clear** sont interdites, car elles se chevauchent avec des politiques gérées et peuvent supprimer une partie de la configuration d'une politique gérée.

L'éditeur d'objet FlexConfig vous empêche d'inclure des commandes interdites dans l'objet.

Commandes CLI interdites	Description
AAA	Configuration bloquée
Serveur AAA	Configuration bloquée
Accès-Liste	Les listes de contrôle d'accès avancées, étendues et standard sont bloquées. La liste de contrôle d'accès Ethertype est autorisée. Vous pouvez utiliser des objets ACL standard et étendus définis dans le gestionnaire d'objets à l'intérieur du modèle en tant que variables.
Inspection ARP	Configuration bloquée
Objet en tant que chemin	Configuration bloquée
Bannière	Configuration bloquée
BGP	Configuration bloquée
Horloge	Configuration bloquée
Community-list Object	Configuration bloquée
Copier	Configuration bloquée
Supprimer	Configuration bloquée
DHCP (protocole de configuration dynamique des hôtes)	Configuration bloquée
Activer le mot de passe	Configuration bloquée
Effacer	Configuration bloquée
Paramètre de fragmentation	Bloqué, sauf pour **fragment reassembly**.
Fsck	Configuration bloquée
HTTP	Configuration bloquée
ICMP	Configuration bloquée
Interface	Seules les commandes **nameif**, **mode**, **shutdown**, **ip address** et **mac-address** sont bloquées.

Commandes CLI interdites	Description
Routage multidiffusion	Configuration bloquée
NAT	Configuration bloquée
Objet réseau/groupe d'objets	La création d'objets de réseau dans l'objet FlexConfig est bloquée, mais vous pouvez utiliser les objets de réseau et les groupes définis dans le gestionnaire d'objets à l'intérieur du modèle en tant que variables.
NTP;	Configuration bloquée
OSPF/OSPFv3	Configuration bloquée
téléavertisseur	Configuration bloquée
Chiffrement de mot de passe	Configuration bloquée
Objet Liste de politiques	Configuration bloquée
Objet Liste des préfixes	Configuration bloquée
Rechargement	Vous ne pouvez pas planifier de rechargements. Le système n'utilise pas la commande **reload** pour redémarrer le système, il utilise la commande **reboot**.
RIP	Configuration bloquée
Objet de carte de routage	La création d'objets de carte de routage dans l'objet FlexConfig est bloquée, mais vous pouvez utiliser les objets de carte de routage définis dans le gestionnaire d'objets à l'intérieur du modèle en tant que variables.
Objet de service/groupe d'objets	La création d'objets de service dans l'objet FlexConfig est bloquée, mais vous pouvez utiliser les objets de port définis dans le gestionnaire d'objets à l'intérieur du modèle en tant que variables.
SNMP	Configuration bloquée
SSH	Configuration bloquée
Route statique	Configuration bloquée
Syslog	Configuration bloquée
Synchronisation du temps	Configuration bloquée
Délai d'expiration	Configuration bloquée
VPN	Configuration bloquée

Scripts de modèles

Vous pouvez utiliser un langage de script pour contrôler le traitement dans un objet FlexConfig. Les instructions de langage de script sont un sous-ensemble de commandes prises en charge dans le moteur de modèles Apache

Velocity 1.3.1, un langage de script basé sur Java qui prend en charge la boucle, les instructions if/else et les variables.

Pour en savoir plus sur l'utilisation du langage de script, consultez le *Guide du développeur Velocity* à l'adresse http://velocity.apache.org/engine/devel/developer-guide.html.

Variables FlexConfig

Vous pouvez utiliser des variables dans un objet FlexConfig dans les cas où une partie d'une commande ou d'une instruction de traitement dépend d'informations d'exécution plutôt que d'informations statiques. Lors du déploiement, les variables sont remplacées par des chaînes obtenues à partir d'autres configurations pour le périphérique en fonction du type de variable :

- Les variables d'objets de politique sont remplacées par des chaînes obtenues à partir d'objets définis dans centre de gestion.
- Les variables système sont remplacées par des informations obtenues à partir du périphérique lui-même ou des politiques configurées à cet effet.
- Les variables de traitement sont chargées avec le contenu de l'objet de politique ou des variables système lorsque les commandes de script sont traitées. Par exemple, dans une boucle, vous chargez de manière itérative une valeur d'un objet de politique ou d'une variable système dans une variable de traitement, puis utilisez la variable de traitement pour former une chaîne de commande ou effectuer une autre action. Ces variables de traitement ne s'affichent pas dans la liste des variables dans un objet FlexConfig. De plus, vous ne pouvez pas les ajouter à l'aide du menu **Insérer** de l'éditeur d'objets FlexConfig.
- Les variables de clés secrètes sont remplacées par la chaîne unique définie pour la variable dans l'objet FlexConfig.

Les variables commencent par le caractère $, sauf les clés secrètes, qui commencent par le caractère @. Par exemple, $ifname est une variable d'objet de politique dans la commande suivante, alors que @keyname est une clé secrète.

```
interface $ifname
key @keyname
```

Remarque La première fois que vous insérez un objet de politique ou une variable système, vous devez le faire par l'intermédiaire du menu **Insérer** de l'éditeur d'objets FlexConfig. Cette action ajoute la variable à la liste des **variables** au bas de l'éditeur d'objet FlexConfig. Vous devrez toutefois saisir la chaîne de variable lors des utilisations ultérieures, même lorsque vous utilisez des variables système. Si vous ajoutez une variable de traitement qui n'a pas d'affectation d'objet ou de variable système, n'utilisez pas le menu **Insérer**. Si vous ajoutez une clé secrète, utilisez toujours le menu **Insérer**. Les variables de clés secrètes ne s'affichent pas dans la liste des variables.

La résolution d'une variable comme une chaîne unique, une liste de chaînes ou un tableau de valeurs dépend du type d'objet de politique ou de variable système que vous affectez à la variable. (Les clés secrètes résolvent toujours une chaîne unique.) Vous devez comprendre ce qui sera renvoyé afin de traiter les variables correctement.

Les rubriques suivantes expliquent les différents types de variables et la façon de les traiter.

Comment traiter les variables

Au moment de l'exécution, une variable peut se résoudre en une chaîne unique, une liste de chaînes du même type, une liste de chaînes de types différents ou un tableau de valeurs nommées. En outre, les variables qui se résolvent en plusieurs valeurs peuvent être de longueur déterminée ou indéterminée. Vous devez comprendre ce qui sera renvoyé afin de traiter les valeurs correctement.

Voici les principales possibilités.

Variables à valeur unique

Si une variable se résout toujours en une chaîne unique, utilisez la variable directement sans modification dans le script FlexConfig.

Par exemple, la variable de texte prédéfinie tcpMssBytes se résout toujours en une valeur unique (qui doit être numérique). La variable **Sysopt_basic** FlexConfig utilise ensuite une structure if/then/else pour définir la taille maximale de segment en fonction de la valeur d'une autre variable de texte à valeur unique, tcpMssMinimum :

```
#if($tcpMssMinimum == "true")
  sysopt connection tcpmss minimum $tcpMssBytes
#else
  sysopt connection tcpmss $tcpMssBytes
#end
```

Dans cet exemple, vous utilisez le menu **Insertion** de l'éditeur d'objets FlexConfig pour ajouter la première utilisation de $tcpMssBytes, mais vous devez saisir la variable directement sur la ligne #else.

Les variables à clé secrète constituent un type particulier de variable à valeur unique. Pour les clés secrètes, vous utilisez toujours le menu **Insérer** pour ajouter la variable, même pour la deuxième utilisation et les suivantes. Ces variables ne s'affichent pas dans la liste des variables de l'objet FlexConfig.

Remarque Les variables d'objet de politique pour les objets réseau correspondent également à une spécification d'adresse IP unique, soit une adresse d'hôte, une adresse réseau ou une plage d'adresses. Cependant, dans ce cas, vous devez savoir à quel type d'adresse vous attendre, car les commandes ASA requièrent des types d'adresses spécifiques. Par exemple, si une commande nécessite une adresse hôte, l'utilisation d'une variable d'objet réseau qui pointe vers un objet qui contient une adresse réseau entraînera une erreur pendant le déploiement.

Variables à valeurs multiples, toutes les valeurs sont du même type

Plusieurs objets de politique et variables système sont résolus en plusieurs valeurs du même type. Par exemple, une variable d'objet qui pointe vers un groupe d'objets réseau se résout en une liste d'adresses IP du groupe. De même, la variable système $SYS_FW_INTERFACE_NAME_LIST se résout en une liste de noms d'interface.

Vous pouvez également créer des objets texte pour plusieurs valeurs du même type. Par exemple, l'objet texte prédéfinienableInspectProtocolList peut contenir plusieurs noms de protocole.

Les variables à valeurs multiples qui se résolvent en une liste d'éléments du même type sont souvent de longueur indéterminée. Par exemple, vous ne pouvez pas savoir à l'avance combien d'interfaces d'un périphérique sont nommées, car les utilisateurs peuvent configurer ou annuler la configuration des interfaces à tout moment.

Ainsi, vous utilisez généralement une boucle pour traiter plusieurs variables valeur du même type. Par exemple, la valeur prédéfinie **Default_Inspection_Protocol_Enable** de FlexConfig utilise une boucle #foreach pour parcourir l'objet EnableInspectProtocolList et traiter chaque valeur.

```
policy-map global_policy
    class inspection_default
    #foreach ( $protocol in $enableInspectProtocolList)
    inspect $protocol
    #end
```

Dans cet exemple, le script affecte chaque valeur à tour de rôle à la variable $protocol, qui est ensuite utilisée dans une commande ASA **inspect** pour activer le moteur d'inspection pour ce protocole. Dans ce cas, il vous suffit de taper $protocol comme nom de variable. Vous n'utilisez pas le menu **Insertion** pour l'ajouter, car vous n'affectez pas d'objet ni de valeur système à la variable. Cependant, vous devez utiliser le menu **Insertion** pour ajouter $enableInspectProtocolList.

Le système parcourt le code entre #foreach et #end jusqu'à ce qu'il n'y ait plus de valeurs dans $enableInspectProtocolList.

Variables à valeurs multiples; les valeurs sont de types différents

Vous pouvez créer des objets texte à valeurs multiples, mais chaque valeur sert un objectif différent. Par exemple, l'objet de texte prédéfini **netflow_Destination** doit avoir trois valeurs, dans l'ordre, le nom d'interface, l'adresse IP de destination et le numéro de port UDP.

Les objets définis de cette manière doivent avoir un nombre déterminé de valeurs. Sinon, ils seraient difficiles à traiter.

Utilisez la méthode get pour traiter ces objets. Tapez **.get(*n*)** à la fin du nom de l'objet, en remplaçant *n* par un index dans l'objet. Commencer à compter à 0, même si l'objet texte répertorie ses valeurs à partir de 1.

Par exemple, l'objet Netflow_ Add_Destination utilise la ligne suivante pour ajouter les 3 valeurs de netflow_Destination à la commande ASA **flow-export**.

```
flow-export destination $netflow_Destination.get(0) $netflow_Destination.get(1)
$netflow_Destination.get(2)
```

Dans cet exemple, vous utiliseriez le menu **Insert** (Insertion) de l'éditeur d'objets FlexConfig pour ajouter la première utilisation de $netflow_Destination, puis ajouter **.get(0)**. Mais vous devez saisir la variable directement pour les spécifications **$netflow_Destination.get(1)** and **$netflow_Destination.get(2)**.

Variables à valeur multiple qui se résolvent en un tableau de valeurs

Certaines variables système renvoient un tableau de valeurs. Ces variables comprennent MAP dans leur nom, par exemple, $SYS_FTD_ROUTED_INTF_MAP_LIST. La carte de l'interface routée renvoie des données qui ressemblent à ce qui suit (les retours de ligne ont été ajoutés pour plus de clarté) :

```
[{intf_hardwarare_id=GigabitEthernet0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.10.1, intf_ipv6_link_local_address=,
intf_logical_name=outside},

{intf_hardwarare_id=GigabitEthernet0/1, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.11.1, intf_ipv6_link_local_address=,
intf_logical_name=inside},
```

```
{intf_hardwarare_id=GigabitEthernet0/2, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=},

{intf_hardwarare_id=Management0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=diagnostic}]
```

Dans l'exemple ci-dessus, des informations sont renvoyées pour quatre interfaces. Chaque interface comprend un tableau de valeurs nommées. Par exemple, intf_hardwarare_id est le nom de la propriété de nom du matériel d'interface et renvoie des chaînes telles que GigabitEthernet0/0.

Ce type de variable est généralement de longueur indéterminée, vous devez donc utiliser une boucle pour traiter les valeurs. Mais vous devez également ajouter le nom de la propriété au nom de la variable pour indiquer la valeur à récupérer.

Par exemple, la configuration IS-IS nécessite que vous ajoutiez la commande ASA **isis** à une interface qui a un nom logique en mode de configuration d'interface. Cependant, vous saisissez dans ce mode en utilisant le nom du matériel de l'interface. Par conséquent, vous devez identifier quelles interfaces ont des noms logiques, puis configurer uniquement ces interfaces en utilisant leurs noms matériels. Pour ce faire, la configuration FlexConfig prédéfinie ISIS_Interface_Configuration utilise une structure if/then imbriquée dans une boucle. Dans le code suivant, vous pouvez voir que la commande de script #foreach charge chaque mappage d'interface dans la variable $intf, puis l'instruction #if supprime la valeur intf_logic_name dans la mappe ($intf.intf_logical_name) et si la valeur est dans la liste définie dans la variable de texte prédéfinie isisIntfList, saisit la commande d'interface en utilisant la valeur intf_hardwarare_id ($intf.intf_hardwarare_id). Vous devrez modifier la variable isisIntfList pour ajouter les noms des interfaces sur lesquelles configurer IS-IS.

```
#foreach ($intf in $SYS_FTD_ROUTED_INTF_MAP_LIST)
 #if ($isIsIntfList.contains($intf.intf_logical_name))
  interface $intf.intf_hardwarare_id
   isis
   #if ($isIsAddressFamily.contains("ipv6"))
   ipv6 router isis
   #end
 #end
#end
```

Afficher ce qu'une variable retournera pour un périphérique

Un moyen simple d'évaluer ce qu'une variable va renvoyer consiste à créer un objet FlexConfig simple qui ne fait rien d'autre que de traiter une liste annotée de variables. Vous pouvez ensuite l'affecter à une politique FlexConfig, affecter la politique à un périphérique, enregistrer la politique, puis prévisualiser la configuration pour ce périphérique. L'aperçu affiche les valeurs obtenues. Vous pouvez sélectionner le texte de l'aperçu, appuyer sur Ctrl + C, puis coller le résultat dans un fichier texte pour l'analyse.

Remarque Cependant, ne déployez pas FlexConfig sur le périphérique, car il ne contiendra aucune commande de configuration valide. Vous obtiendriez des erreurs de déploiement. Après avoir obtenu l'aperçu, supprimez l'objet FlexConfig de la politique FlexConfig et enregistrez cette dernière.

Par exemple, vous pouvez construire l'objet FlexConfig suivant :

```
Following is a network object group variable for the
IPv4-Private-All-RFC1918 object:

$IPv4_Private_addresses

Following is the system variable SYS_FW_MANAGEMENT_IP:

$SYS_FW_MANAGEMENT_IP

Following is the system variable SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST:

$SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST

Following is the system variable SYS_FTD_ROUTED_INTF_MAP_LIST:

$SYS_FTD_ROUTED_INTF_MAP_LIST

Following is the system variable SYS_FW_INTERFACE_NAME_LIST:

$SYS_FW_INTERFACE_NAME_LIST
```

L'aperçu de cet objet peut ressembler à ce qui suit (retours de ligne ajoutés pour plus de clarté) :

```
###Flex-config Prepended CLI ###

###CLI generated from managed features ###

###Flex-config Appended CLI ###
Following is an network object group variable for the
IPv4-Private-All-RFC1918 object:

[10.0.0.0, 172.16.0.0, 192.168.0.0]

Following is the system variable SYS_FW_MANAGEMENT_IP:

192.168.0.171

Following is the system variable SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST:

[dns, ftp, h323 h225, h323 ras, rsh, rtsp, sqlnet, skinny, sunrpc,
xdmcp, sip, netbios, tftp, icmp, icmp error, ip-options]

Following is the system variable SYS_FTD_ROUTED_INTF_MAP_LIST:

[{intf_hardwarare_id=GigabitEthernet0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.10.1, intf_ipv6_link_local_address=,
intf_logical_name=outside},

{intf_hardwarare_id=GigabitEthernet0/1, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.11.1, intf_ipv6_link_local_address=,
intf_logical_name=inside},

{intf_hardwarare_id=GigabitEthernet0/2, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=},

{intf_hardwarare_id=Management0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=diagnostic}]
```

```
Following is the system variable SYS_FW_INTERFACE_NAME_LIST:

[outside, inside, diagnostic]
```

Variables de l'objet politique FlexConfig

Une variable d'objet de politique est associée à un objet de politique spécifique configuré dans le gestionnaire d'objets. Lorsque vous insérez une variable d'objet de politique dans un objet FlexConfig, vous donnez un nom à la variable et sélectionnez l'objet qui lui est associé.

Bien que vous puissiez donner à la variable exactement le même nom que l'objet associé, la variable elle-même n'est pas la même chose que l'objet associé. Vous devez utiliser le menu **Insert** > **Insert Policy Object** > ***Object Type*** (Insérer > Insérer l'objet Politique > Type d'objet) dans l'éditeur d'objet FlexConfig pour ajouter la variable pour la première fois au script dans FlexConfig afin d'établir l'association avec l'objet. La simple saisie du nom de l'objet précédé du signe $ ne crée pas de variable d'objet de politique.

Vous pouvez créer des variables pour pointer vers les types d'objets suivants. Assurez-vous de créer le bon type d'objet pour chaque variable. Pour créer des objets, accédez à la page **Objects** > **Object Management** (Objets > Gestion des objets).

- **Text Objects** : pour les chaînes de texte, qui peuvent inclure des adresses IP, des chiffres et d'autres textes en forme libre comme des noms d'interface ou de zone. Sélectionnez **FlexConfig** > **Text Object (objet texte)** dans la table des matières, puis cliquez sur **Add Text Object**(ajouter un objet texte). Vous pouvez configurer ces objets pour contenir une valeur unique ou plusieurs valeurs. Ces objets sont très flexibles et conçus spécifiquement pour une utilisation au sein des objets FlexConfig. Pour de plus amples renseignements, voir Configurer les objets texte FlexConfig, à la page 30.
- **Network** (réseau) : pour les adresses IP. Vous pouvez utiliser des objets ou des groupes réseau. Sélectionnez **Network** (Réseau) dans la table des matières, puis **Add Network (Ajouter un réseau)** > **Add Object (Ajouter un objet)** ou **Add Group** (Ajouter un groupe). Si vous utilisez un objet de groupe, la variable renvoie une liste de chaque spécification d'adresse IP dans le groupe. Les adresses peuvent être un hôte, un réseau ou des plages d'adresses, selon le contenu de l'objet. Consultez Réseau.
- **Security Zones** (zones de sécurité) : pour les interfaces au sein d'une zone de sécurité ou d'un groupe d'interfaces. Sélectionner **Interface** dans la table des matières, puis **Add (Ajouter)** > **Security Zone (Zone de sécurité)** or **Interface Group** (Groupe d'interface). Une variable de zone de sécurité renvoie une liste des interfaces de cette zone ou de ce groupe pour le périphérique en cours de configuration. Consultez Interface.
- **Objet ACLstandard** : pour les listes de contrôle d'accès standard. Une variable ACL standard renvoie le nom de l'objet ACL standard. Sélectionnez **Access List (Liste d'accès)** > **Standard** dans la table des matières, puis cliquez sur **Add Standard Access List Object** (Ajouter un objet de liste d'accès standard). Consultez Liste d'accès.
- **Objectif d'ACL étendue** : pour les listes de contrôle d'accès étendues. Une variable d'ACL étendue renvoie le nom de l'objet d'ACL étendu. Sélectionnez **Access List (Liste d'accès)** > **Extended (étendue)** dans la table des matières, puis cliquez sur **Add Extended Access List Object** (ajouter un objet de liste d'accès étendue). Consultez Liste d'accès.
- **Carte de routage** : pour les objets de carte de routage. Une variable de carte de routage renvoie le nom de l'objet de carte de routage. Sélectionnez **Route Map** (carte de routage) dans la table des matières, puis cliquez sur **Add Route Map** (Ajouter une carte de routage). Consultez Carte de routage.

Variables système FlexConfig

Les variables système sont remplacées par des informations obtenues à partir du périphérique lui-même ou des politiques configurées à cet effet.

Vous devez utiliser le menu **Insérer** > **Insérer la variable système** > ***Nom de la variable*** dans l'éditeur d'objets FlexConfig pour ajouter la variable pour la première fois au script dans FlexConfig afin d'établir l'association avec la variable système. La simple saisie du nom de la variable système précédée du signe $ ne crée pas de variable système dans le contexte de l'objet FlexConfig.

Le tableau suivant explique les variables système disponibles. Avant d'utiliser une variable, examinez ce qui est généralement renvoyé pour la variable; voir Afficher ce qu'une variable retournera pour un périphérique, à la page 9.

Nom	Description
SYS_FW_OS_MODE	Le mode de système d'exploitation du périphérique. Les valeurs possibles sont ROUTÉ ou TRANSPARENT.
SYS_FW_OS_MULTIPLICITY	Si le périphérique fonctionne en mode contexte unique ou multiple. Les valeurs possibles sont SINGLE, MULTI ou Not_APPLICABLE.
SYS_FW_MANAGEMENT_IP	L'adresse IP de gestion du périphérique
SYS_FW_HOST_NAME	Nom d'hôte de l'appareil
SYS_FTD_INTF_POLICY_MAP	Une carte avec le nom de l'interface comme clé et une carte de politiques comme valeur. Cette variable ne renvoie rien si aucune politique de service basée sur l'interface n'est définie sur le périphérique.
SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST	La liste des protocoles pour lesquels l'inspection est activée.
SYS_FTD_ROUTED_INTF_MAP_LIST	Liste des mappages d'interfaces routées sur le périphérique. Chaque mappage comprend un ensemble de valeurs nommées liées à la configuration de l'interface routée.
SYS_FTD_SWITCHED_INTF_MAP_LIST	Une liste des mappages d'interfaces commutées sur le périphérique. Chaque mappage comprend un ensemble de valeurs nommées liées à la configuration de l'interface commutée.
SYS_FTD_INLINE_INTF_MAP_LIST	Une liste des mappages d'interface en ligne sur le périphérique. Chaque mappage comprend un ensemble de valeurs nommées liées à la configuration de l'interface d'ensemble en ligne.
SYS_FTD_PASSIVE_INTF_MAP_LIST	Une liste des mappages d'interface passifs sur le périphérique. Chaque mappage comprend un ensemble de valeurs nommées liées à la configuration de l'interface passive.
SYS_FTD_INTF_BVI_MAP_LIST	Une liste des mappages d'interfaces virtuelles de pont sur le périphérique. Chaque mappage comprend un ensemble de valeurs nommées liées à la configuration des BVI.
SYS_FW_INTERFACE_HARDWARE_ID_LIST	Une liste des noms de matériel pour les interfaces sur le périphérique, comme GigabitEthernet0/0.

Nom	Description
SYS_FW_INTERFACE_NAME_LIST	Une liste de noms logiques pour les interfaces sur le périphérique, par exemple, interne.
SYS_FW_INLINE_INTERFACE_NAME_LIST	Une liste de noms logiques pour les interfaces configurées comme passives ou ERSPAN.
SYS_FW_NON_INLINE_INTERFACE_NAME_LIST	Une liste de noms logiques pour les interfaces qui ne font pas partie d'ensembles en ligne, comme toutes les interfaces routées.

Objets FlexConfig prédéfinis

Les objets FlexConfig prédéfinis fournissent des configurations testées pour certaines fonctionnalités. Utilisez ces objets si vous devez configurer ces fonctionnalités, qui ne peuvent autrement pas être configurées à l'aide du centre de gestion.

Le tableau suivant dresse la liste des objets disponibles. Prenez note des objets texte associés. Vous devez modifier ces objets texte pour personnaliser le comportement de l'objet FlexConfig prédéfini. Les objets texte vous permettent de personnaliser la configuration en utilisant les adresses IP et d'autres attributs requis par votre réseau et votre appareil.

Si vous devez modifier un objet FlexConfig prédéfini, copiez l'objet, apportez des changements à la copie et enregistrez-la sous un nouveau nom. Vous ne pouvez pas modifier directement un objet FlexConfig prédéfini.

Bien que vous puissiez configurer d'autres fonctionnalités basées sur ASA à l'aide de FlexConfig, la configuration de ces fonctionnalités n'a pas été testée. Si une fonctionnalité d'ASA recoupe quelque chose que vous pouvez configurer dans les politiques centre de gestion, n'essayez pas de la configurer par FlexConfig .

Par exemple, l'inspection Snort comprend le protocole HTTP, donc n'activez pas l'inspection HTTP de style ASA. (En fait, vous ne pouvez pas ajouter **http** à l'objet EnableInspectProtocolList. Dans ce cas, vous ne pouvez pas mal configurer votre périphérique.) Configurez plutôt la politique de contrôle d'accès pour effectuer le filtrage des applications ou des URL, selon les besoins, pour mettre en œuvre vos exigences d'inspection HTTP.

Tableau 1 : Objets FlexConfig prédéfinis

Nom Objet FlexConfig	Description	Objets texte associés
Default_Inspection_Protocol_Disable	Désactive les protocoles dans la liste des politiques par défaut de global_politique.	disableInspectProtocolList
Default_Inspection_Protocol_Enable	Active les protocoles dans la liste des politiques par défaut de global_politique.	enableInspectProtocolList
Inspect_IPv6_Configure	Configure l'inspection IPv6 dans la liste des politiques global_policy, la journalisation et l'abandon du trafic en fonction du contenu de l'en-tête IPv6.	IPv6RoutingHeaderDropLogList, IPv6RoutingHeaderLogList, IPv6RoutingHeaderDropList.
Inspect_IPv6_UnConfigure	Efface et désactive l'inspection IPv6.	—

Nom Objet FlexConfig	Description	Objets texte associés
ISIS_Configure	Configure les paramètres globaux pour le routage IS-IS.	isIsNet, isIsAddressFamily, isISType
ISIS_Interface_Configuration	Configuration d'IS-IS au niveau de l'interface.	isIsAddressFamily, IsIsIntfList Utilise également la variable système SYS_FTD_ROUTED_INTF_MAP_LIST
ISIS_Unconfigure	Efface la configuration du routeur IS-IS sur le périphérique.	—
ISIS_Unconfigure_All	Efface la configuration du routeur IS-IS du périphérique, y compris l'affectation du routeur de l'interface du périphérique.	—
Netflow_Add_Destination	Crée et configure une destination d'exportation NetFlow.	Netflow_Destinations, netflow_Event_Types
Netflow_Clear_Parameters	Restaure les paramètres globaux par défaut d'exportation NetFlow.	—
Netflow_Delete_Destination	Supprime une destination d'exportation NetFlow.	Netflow_Destinations, netflow_Event_Types
Netflow_Set_Paramètres	Définit les paramètres globaux pour l'exportation NetFlow.	netflow_Parameters
NGFW_TCP_NORMALIZATION	Modifie la configuration de normalisation TCP par défaut.	—
Policy_Based_Routing	Pour utiliser cet exemple de configuration, copiez-le, modifiez le nom d'interface et utilisez l'objet texte r-map-object text pour identifier un objet de carte de routage dans le gestionnaire d'objets.	—
Policy_Based_Routing_Clear	Efface les configurations de routage basé sur les politiques du périphérique.	—
Sysopt_AAA_radius	Ignore la clé d'authentification dans les réponses de gestion RADIUS.	—
Sysopt_AAA_radius_negate	Annule la configuration Sysopt_AAA_radius.	—
Sysopt_basic	Configure le temps d'attente sysopt, la taille maximale de segment pour les paquets TCP et les statistiques de trafic détaillées.	tcpMssMinimum, tcpMssBytes
Sysopt_basic_negate	Efface les statistiques de trafic détaillées sysopt_basic, le temps d'attente et la taille maximale du segment TCP.	—

Nom Objet FlexConfig	Description	Objets texte associés
Sysopt_clear_all	Efface toutes les configurations Sysopt du périphérique.	—
Sysopt_noproxyarp	Configure les interfaces de ligne de commande noproxy-arp.	Utilise la variable système SYS_FW_NON_INLINE_INTF_NAME_LIST
Sysopt_noproxyarp_negate	Efface les configurations Sysopt_noproxyarp.	Utilise la variable système SYS_FW_NON_INLINE_INTF_NAME_LIST
Sysopt_Preserve_Vpn_Flow	Configure syopt pour préserver le flux VPN.	—
Sysopt_Preserve_Vpn_Flow_negate	Efface la configuration Sysopt_Preserve_Vpn_Flow.	—
Sysopt_Reclassify_Vpn	Configure le VPN de reclassification sysopt.	—
Sysopt_Reclassify_Vpn_Negate	Annule le VPN de reclassification de sysopt.	—
Threat_Detection_Clear	Effacez la configuration TCP Intercept pour la détection des menaces.	—
Threat_Detection_Configure	Configurez les statistiques de détection des menaces pour les attaques interceptées par TCP Intercept.	threat_detection_statistics
Wccp_Configure	Ce modèle fournit un exemple de configuration de WCCP.	isServiceIdentifier, serviceIdentifier, wccpPassword
Wccp_Configure_Clear	Efface les configurations de WCCP.	—

Objets FlexConfig obsolètes

Le tableau suivant répertorie les objets qui configurent les fonctionnalités. Vous pouvez désormais configurer en mode natif dans l'interface graphique. Cessez d'utiliser ces objets dès que possible.

Tableau 2 : Objets FlexConfig prédéfinis obsolètes

Version obsolète	Objet FlexConfig	Description	Configurer désormais dans
7.3	DHCPv6_Prefix_Delegation_Configure	Configurez une interface externe (client de délégation de préfixe) et une interface interne (destinataire du préfixe délégué) pour la délégation de préfixe IPv6. Pour utiliser ce modèle, copiez-le et modifiez les variables. Objets texte associés : pdoutside, pdinside Utilise également la variable système SYS_FTD_ROUTED_INTF_MAP_LIST	Paramètres IPV6 de l'interface;
7.3	DHCPv6_Prefix_Delegation_UnConfigure	Supprime la configuration de délégation de préfixe DHCPv6.	Paramètres IPV6 de l'interface;
6.3	Default_DNS_Configure	Configurez le groupe DNS par défaut, qui définit les serveurs DNS qui peuvent être utilisés lors de la résolution de noms de domaine complets sur les interfaces de données. Objets texte associés : defaultDNSNameServerList, defaultDNSParameters	Paramètres de la plateforme
6.3	DNS_Configure	Configurez les serveurs DNS dans un groupe de serveurs DNS autre que celui par défaut. Copiez l'objet pour modifier le nom du groupe.	**Groupe de serveurs DNS** dans le gestionnaire d'objets.
6.3	DNS_UnConfigure	Supprime la configuration de serveur DNS réalisée par Default_DNS_Configure et DNS_Configure. Copiez l'objet pour modifier les noms de groupes de serveurs DNS si vous avez modifié DNS_Configure.	**Groupe de serveurs DNS** dans le gestionnaire d'objets.

Version obsolète	Objet FlexConfig	Description	Configurer désormais dans
7.2	Eigrp_Configure	Configure le saut suivant de routage EIGRP, le récapitulatif automatique, l'identifiant du routeur et la souche EIGRP. Objets texte associés : eigrpAS, eigrpNetworks, eigrpDisableAutoSummary, eigrpRouterId, eigrpStubReceiveOnly, eigrpStubRedistributed, eigrpStubConnected, eigrpStubStatic, eigrpStubSummary	Pour tous les objets EIGRP, consultez EIGRP. Le système vous permet d'effectuer un déploiement après la mise à niveau, mais vous avertit également de refaire vos configurations EIGRP. Pour vous aider dans ce processus, nous fournissons un outil de migration de ligne de commande.
7.2	Eigrp_Interface_Configure	Configure le mode d'authentification de l'interface EIGRP, la clé d'authentification, l'intervalle Hello, la durée d'attente et le partage de l' horizon. Objets texte associés : eigrpIntfList, eigrpAS, eigrpAuthKey, eigrpAuthKeyId, eigrpHelloInterval, eigrpHoldTime, eigrpDisableSplitHorizon Utilise également la variable système SYS_FTD_ROUTED_INTF_MAP_LIST	
7.2	Eigrp_Unconfigure	Efface la configuration EIGRP pour un système autonome du périphérique.	
7.2	Eigrp_Unconfigure_all	Efface toutes les configurations EIGRP.	
6.3	TCP_Embryronic_Conn_Limit	Configure les limites de connexion amorce pour vous protéger contre les attaques par déni de service (DoS) par inondation SYN. Objets texte associés : tcp_conn_misc, tcp_conn_limit	Politique de service.
6.3	TCP_Embryonic_Conn_Timeout	Configure les délais d'expiration de connexion amorces pour la protection contre les attaques par déni de service (DoS) par inondation SYN. Objets texte associés : tcp_conn_misc, tcp_conn_timeout	Politique de service.

Version obsolète	Objet FlexConfig	Description	Configurer désormais dans
7.2	VxLAN_Clear_Nve	Supprime le NVE 1 configuré lorsque VxLAN_Configure_Port_And_Nve est utilisé à partir du périphérique.	Pour tous les objets VxLAN, consultez Configurer les interfaces VXLAN. Si vous avez configuré les interfaces VXLAN avec FlexConfig dans une version précédente, elles continuent de fonctionner. En fait, FlexConfig prévaut dans ce cas : si vous refaites vos configurations VXLAN dans l'interface Web, supprimez les paramètres FlexConfig.
7.2	VxLAN_Clear_Nve_Only	Efface le NVE configuré sur l'interface lors du déploiement.	
7.2	VxLAN_Configure_Port_And_Nve	Configure le port VLAN et NVE 1. Objets texte associé : vxlan_Port_And_Nve	
7.2	VxLAN_Make_Nve_Only	Définit une interface pour NVE uniquement. Objets texte associés : vxlan_Nve_Only Utilise également les variables système SYS_FTD_ROUTED_MAP_LIST et SYS_FTD_SWITCHED_INTF_MAP_LIST	
7.2	VxLAN_Make_Vni	Créer une interface VNI. Après l'avoir déployé, vous devez annuler l'enregistrement et réenregistrer le périphérique pour découvrir correctement l'interface VNI. Objets texte associés : vxlan_Vni	

Objets texte prédéfinis

Il existe plusieurs objets texte prédéfinis. Ces objets sont associés aux variables utilisées dans les objets FlexConfig prédéfinis. Dans la plupart des cas, vous devez modifier ces objets pour ajouter des valeurs si vous utilisez l'objet FlexConfig associé, sinon vous constaterez des erreurs lors du déploiement. Bien que certains de ces objets contiennent des valeurs par défaut, d'autres sont vides.

Pour en savoir plus sur la modification des objets texte, consultez Configurer les objets texte FlexConfig, à la page 30.

Nom	Description	Objet FlexConfig associé
Liste par défaut du serveur de noms DNS (Obsolète.)	L'adresse IP du serveur DNS à configurer dans le groupe DNS par défaut. À partir de la version 6.3, configurez le DNS pour les interfaces de données dans la politique des paramètres de la plateforme Threat Defense.	Default_DNS_Configure
defaultDNSParameters (Obsolète.)	Les paramètres permettant de contrôler le comportement du DNS pour le groupe de serveurs DNS par défaut. L'objet contient des entrées distinctes, dans l'ordre, pour les tentatives, délai d'expiration, le délai d'expiration de l'entrée, l'interrogation, le nom de domaine. À partir de la version 6.3, configurez le DNS pour les interfaces de données dans la politique des paramètres de la plateforme Threat Defense.	Default_DNS_Configure
disableInspectProtocolList	Désactive les protocoles dans la liste des politiques par défaut (global_politique).	Disable_Default_Inspection_Protocol
dnsNameServerList	L'adresse IP du serveur DNS à configurer dans un groupe DNS défini par l'utilisateur.	DNS_Configure
dnsParameters	Les paramètres pour contrôler le comportement du DNS pour un groupe de serveurs DNS autre que celui par défaut. L'objet contient des entrées distinctes, dans l'ordre, pour les tentatives, le délai d'expiration, le nom de domaine, l'interface de serveur de noms.	DNS_Configure
enableInspectProtocolList	Active les protocoles dans la liste des politiques par défaut (global_politique). Vous ne pouvez pas ajouter de protocoles dont l'inspection est en conflit avec l'inspection Snort.	Enable_Default_Inspection_Protocol
IPv6RoutingHeaderDropList	La liste des types d'en-tête de routage IPv6 que vous souhaitez interdire. L'inspection IPv6 abandonne les paquets qui contiennent ces en-têtes sans journaliser l'abandon.	Inspect_IPv6_Configure
IPv6RoutingHeaderDropLogList	La liste des types d'en-tête de routage IPv6 que vous souhaitez interdire et journaliser. L'inspection IPv6 abandonne les paquets qui contiennent ces en-têtes et envoie un message syslog concernant l'abandon.	Inspect_IPv6_Configure

Nom	Description	Objet FlexConfig associé
IPv6RoutingHeaderLogList	La liste des types d'en-tête de routage IPv6 que vous souhaitez autoriser mais journaliser. L'inspection IPv6 autorise les paquets qui contiennent ces en-têtes, mais envoie un message syslog concernant l'existence de l'en-tête.	Inspect_IPv6_Configure
isIsAddressFamily	Famille d'adresses IPv4 ou IPv6.	ISIS_Configure ISIS_Interface_Configuration
IsIsIntfList	Liste des noms d'interface logique.	ISIS_Interface_Configuration
isIsISType	Type de IS (niveau 1, niveau 2 seulement ou niveau 1-2).	ISIS_Configure
isIsNet	Entité du réseau.	ISIS_Configure
isServiceIdentifier	Lorsque la valeur est False, utilise l'identifiant de service standard **web-cache**.	Wccp_Configure
netflow_Destination	Définit l'interface, la destination et le numéro de port UDP d'une destination d'exportation NetFlow unique.	Netflow_Add_Destination
netflow_Event_Types	Définit les types d'événements à exporter pour une destination composée de n'importe quel sous-ensemble des éléments suivants : **all**, **flow-create**, **flow-defined**, **flow-teardown**, **flow-update**.	Netflow_Add_Destination
netflow_Parameters	Fournit les paramètres globaux de l'exportation NetFlow : intervalle d'actualisation active (nombre de minutes entre les événements de mise à jour de flux), délai (délai de création du flux en secondes; par défaut 0 = la commande ne s'affichera pas) et taux d'expiration du modèle en minutes.	Netflow_Set_Paramètres
PrefixDelegationInside	Configure l'interface interne pour la délégation de préfixe DHCPv6. L'objet comprend plusieurs entrées, l'ordre, le nom d'interface, le suffixe IPv6 avec la longueur du préfixe et le nom de l'ensemble de préfixes.	Aucun, mais pourrait être utilisé avec une copie de DHCPv6_Prefix_Delegation_Configure.
PrefixDelegationOutside	Configurez le client de délégation de préfixe DHCPv6 externe. L'objet comprend plusieurs entrées, l'ordre, le nom d'interface et la longueur du préfixe IPv6	Aucun, mais pourrait être utilisé avec une copie de DHCPv6_Prefix_Delegation_Configure.

Nom	Description	Objet FlexConfig associé
serviceIdentifier	Numéro d'identifiant de service WCCP dynamique	Wccp_Configure
tcp_conn_limit (Obsolète.)	Paramètres utilisés pour configurer les limites de connexion amorcesTCP. À partir de la version 6.3, configurez ces fonctionnalités dans la politique de service Threat Defense, que vous pouvez trouver sous l'onglet Avancé de la politique de contrôle d'accès attribuée au périphérique.	TCP_Embryronic_Conn_Limit
tcp_conn_misc (Obsolète.)	Paramètres utilisés pour la configuration des paramètres de connexion TCP amorce. À partir de la version 6.3, configurez ces fonctionnalités dans la politique de service Threat Defense, que vous pouvez trouver sous l'onglet Avancé de la politique de contrôle d'accès attribuée au périphérique.	TCP_Embryonic_Conn_Limit, TCP_Embryonic_Conn_Timeout
tcp_conn_timeout (Obsolète.)	Paramètres utilisés pour configurer les délais d'expiration de la connexion TCP amorce. À partir de la version 6.3, configurez ces fonctionnalités dans la politique de service Threat Defense, que vous pouvez trouver sous l'onglet Avancé de la politique de contrôle d'accès attribuée au périphérique.	TCP_Embryonic_Conn_Timeout
tcpMssBytes	taille de segment maximum.	Sysopt_basic
tcpMssMinimum	Vérifie s'il faut définir la taille maximale de segment (MSS), qui n'est définie que si cet indicateur prend la valeur True..	Sysopt_basic
threat_detection_statistics	Paramètres utilisés pour les statistiques de détection des menaces pour l'interception TCP.	Threat_Detection_Configure
vxlan_Nve_Only	Paramètres de configuration de NVE uniquement sur l'interface : • nom logique de l'interface • Adresse IPv4 (facultative pour l'interface routée) • Masque réseau IPv4 (facultatif pour l'interface routée)	VxLAN_Make_Nve_Only

Nom	Description	Objet FlexConfig associé
vxlan_Port_And_Nve	Paramètres utilisés pour la configuration des ports et de NVE pour VXLAN : • port vxlan • Nom de l'interface source • type (homologue ou mcast) • Adresse IP homologue ou groupe mcast par défaut	VxLAN_Configure_Port_And_Nve
vxlan_Vni	Paramètres utilisés pour la création de la VNI : • Numéro d'interface (1 à 10 000) • ID de segment (1 à 16777215) • nameif (Nom logique de l'interface) • type (routage ou transparent) • Adresse IP (utilisée dans le cas d'un périphérique en mode routé) ou numéro de groupe de ponts (utilisé dans le cas d'un périphérique en mode transparent) • masque réseau (si le périphérique est en mode routé) ou inutilisé	VxLAN_Make_Vni
wccpPassword	Mot de passe WCCP	Wccp_Configure

Exigences et conditions préalables pour les politiques FlexConfig

Prise en charge des modèles

Défense contre les menaces

Domaines pris en charge

N'importe quel

Rôles utilisateur

Admin

Lignes directrices et limites de FlexConfig

- Si vous commettez une erreur dans la politique FlexConfig, le système restaurera toutes les modifications incluses dans la tentative de déploiement qui comprend FlexConfig ayant échoué. Étant donné que la restauration due à un déploiement échoué comprend l'effacement de la configuration, cela peut perturber votre réseau. Pensez à planifier les déploiements qui comprennent des modifications de FlexConfig en dehors des heures de travail. Pensez également à isoler le déploiement de sorte qu'il n'inclue que les modifications FlexConfig, et aucune autre mise à jour de politique.
- Lorsque vous utilisez l'objet VxLAN_Make_VNI, vous devez déployer la même configuration FlexConfig sur toutes les unités d'une grappe ou d'une paire à haute disponibilité avant de former la grappe ou la paire à haute disponibilité. Le centre de gestion exige que les interfaces VXLAN correspondent sur tous les périphériques avant de former la grappe ou la paire à haute disponibilité.
- Si vous configurez un service qui s'applique aux connexions, comme l'inspection SIP, accédez à l'interface de ligne de commande du périphérique et saisissez la commande **clear conn** pour effacer les connexions. Lorsque les connexions sont rétablies, la nouvelle configuration est appliquée aux sessions.

Personnalisation de la configuration du périphérique à l'aide des politiques FlexConfig

Utilisez les politiques FlexConfig pour personnaliser la configuration d'un périphérique défense contre les menaces .

Avant d'utiliser FlexConfig, essayez de configurer toutes les politiques et tous les paramètres dont vous avez besoin à l'aide des autres fonctionnalités décrites dans centre de gestion. FlexConfig est une méthode de dernier ressort pour configurer les fonctionnalités basées sur ASA qui sont compatibles avec défense contre les menaces , mais qui ne sont pas autrement configurables dans centre de gestion.

Voici la procédure de bout en bout de configuration et de déploiement d'une politique FlexConfig.

Procédure

Étape 1 Déterminez la séquence de commandes CLI que vous souhaitez configurer.

Si la configuration d'un périphérique ASA fonctionne correctement, utilisez **show running-config** pour obtenir la séquence de commandes dont vous avez besoin. Apportez des ajustements à des éléments tels que les noms d'interface et les adresses IP, le cas échéant.

S'il s'agit d'une nouvelle fonctionnalité, il est préférable d'essayer de la mettre en œuvre sur un périphérique ASA dans un environnement de laboratoire pour vérifier que vous avez la bonne séquence de commandes.

Pour plus d'informations, consultez les rubriques suivantes :

- Utilisation recommandée des politiques FlexConfig, à la page 2
- Commandes de l'interface de ligne de commande dans les objets FlexConfig, à la page 2

Étape 2 Choisissez **Objects (Objets)** > **Object Management**(gestion des objets), puis sélectionnez **FlexConfig** > **FlexConfig Objects (Objets FlexConfig)** dans la table des matières.

Examinez les objets FlexConfig prédéfinis pour déterminer s'ils seront en mesure de générer les commandes dont vous avez besoin. Cliquez sur **Afficher** ( ) pour voir le contenu de l'objet. Si un objet existant est similaire à ce que vous souhaitez, commencez par faire une copie de l'objet, puis modifiez la copie. Consultez Objets FlexConfig prédéfinis, à la page 13.

L'examen des objets vous donnera également une idée de la structure, de la syntaxe des commandes et du séquençage attendu pour un objet FlexConfig.

Remarque Si vous trouvez des objets que vous comptez utiliser, directement ou sous forme de copies, examinez la liste des variables au bas de l'objet. Prenez note des noms des variables, sauf ceux en majuscules commençant par SYS, qui sont des variables système. Ces variables sont des objets textuels que vous devrez probablement modifier et pour lesquels vous devrez définir des valeurs de remplacement, en particulier si la colonne des valeurs par défaut indique que l'objet ne comporte pas de valeur..

Étape 3 Si vous devez créer vos propres objets FlexConfig, déterminez les variables dont vous avez besoin et créez les objets associés.

L'interface de ligne de commande que vous devez déployer peut contenir des adresses IP, des noms d'interface, des numéros de port et d'autres paramètres que vous pourriez souhaiter ajuster au fil du temps. Il est préférable de les isoler dans des variables, qui pointent vers des objets contenant les valeurs nécessaires. Vous pourriez également avoir besoin de variables pour les chaînes qui font partie de la configuration, mais qui peuvent changer au fil du temps.

Déterminez également si vous avez besoin de valeurs différentes pour chaque périphérique auquel vous affecterez la politique. Par exemple, vous pourriez souhaiter configurer la fonctionnalité sur trois périphériques, mais vous pourriez devoir spécifier un nom d'interface ou une adresse IP différent sur une commande donnée pour chacun de ces périphériques. Si vous devez personnaliser l'objet pour chaque périphérique, veillez à activer les remplacements lors de la création de l'objet, puis définissez les valeurs de remplacement par périphérique.

Consultez les rubriques suivantes pour obtenir une explication des différents types de variables et de la configuration des objets connexes lorsque cela est nécessaire.

- Variables FlexConfig, à la page 6
- Variables de l'objet politique FlexConfig, à la page 11
- Variables système FlexConfig, à la page 12
- Configurer les objets texte FlexConfig, à la page 30

Étape 4 Si vous utilisez les objets FlexConfig prédéfinis, modifiez les objets texte utilisés comme variables.

Consultez Configurer les objets texte FlexConfig, à la page 30.

Étape 5 (Si nécessaire.) Configurer les objets FlexConfig, à la page 25.

Vous ne devez créer des objets que si les objets prédéfinis ne peuvent pas accomplir la tâche.

Étape 6 Configurer la politique FlexConfig, à la page 31.

Étape 7 Définir les périphériques cibles pour une politique FlexConfig, à la page 32.

Vous pouvez également affecter la politique à des périphériques lorsque vous créez la politique. Au moins un périphérique doit être affecté à la politique pour que vous puissiez en avoir un aperçu.

Étape 8 Prévisualiser la politique FlexConfig, à la page 33.

Vous devez enregistrer les modifications avant de pouvoir afficher un aperçu de la politique.

Vérifiez que les commandes générées sont celles prévues et que toutes les variables sont résolues correctement.

Étape 9 Choisissez **Deploy** > **Deployment** (Déployer > Déploiement) dans la barre de menu.

Étape 10 Sélectionnez les périphériques affectés à la politique, puis cliquez sur **Deploy** (Déployer).

Attendez que le déploiement soit terminé.

Étape 11 Vérifier la configuration déployée, à la page 34.

Étape 12 (Si nécessaire.) Supprimer des fonctionnalités configurées à l'aide de FlexConfig, à la page 36.

Contrairement à d'autres types de politique, la simple suppression de l'attribution d'une FlexConfig d'un périphérique peut ne pas supprimer la configuration associée. Si vous souhaitez supprimer une configuration générée par FlexConfig, vous devez suivre la procédure indiquée.

Si vous supprimez une fonctionnalité parce qu'elle est désormais directement prise en charge par le produit, consultez aussi Conversion de la fonctionnalité FlexConfig vers la fonctionnalité gérée, à la page 37.

Configurer les objets FlexConfig

Utilisez les objets FlexConfig pour définir une configuration à déployer sur un périphérique. Chaque politique FlexConfig est composée d'une liste d'objets FlexConfig. Les objets sont donc essentiellement des modules de code composés de commandes de script Apache Velocity, de commandes de configuration logicielle ASA et de variables.

Il existe plusieurs objets FlexConfig prédéfinis que vous pouvez utiliser directement ou dont vous pouvez faire des copies si vous devez les modifier. Vous pouvez également créer vos propres objets de toutes pièces. Le contenu d'un objet FlexConfig peut aller d'une simple chaîne de commande à des structures de commandes élaborées qui utilisent des variables et des commandes de script pour déployer des commandes dont le contenu peut différer d'un périphérique à l'autre ou d'un déploiement à l'autre.

Vous pouvez également créer des objets de politique FlexConfig lors de la définition des politiques FlexConfig.

Avant de commencer

Gardez les éléments suivants à l'esprit :

- Les objets FlexConfig se transforment en commandes qui sont ensuite déployées sur le périphérique. Ces commandes sont déjà saisies en mode de configuration globale. Par conséquent, n'incluez pas les commandes **enable** et **configure terminal** dans l'objet FlexConfig.
- Déterminez les types de variables dont vous aurez besoin et créez les objets de règles dont vous avez besoin. Vous ne pouvez pas créer d'objets pour les variables lors de la modification d'un objet FlexConfig.
- Assurez-vous que vos commandes n'entrent en conflit de quelque façon que ce soit avec la configuration du VPN ou du contrôle d'accès sur les périphériques.
- S'il y a plusieurs ensembles de commandes pour une interface, seul le dernier ensemble de commandes est déployé. Par conséquent, nous vous recommandons de ne pas utiliser les commandes de début et de fin pour configurer des interfaces. Pour obtenir un exemple de configuration d'interfaces, consultez l'objet FlexConfig prédéfini ISIS_Interface_Configuration.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Choisissez **FlexConfig** > **FlexConfig Object** (FlexConfig > Objets FlexCoonfig) dans la liste des types d'objet.

Étape 3 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add FlexConfig Object** pour créer un nouvel objet.
- Cliquez sur **Edit** () pour modifier un objet existant.
- Cliquez sur **Afficher** () pour voir le contenu d'un objet prédéfini.
- Si vous souhaitez modifier un objet prédéfini, cliquez sur **Copier** () pour créer un nouvel objet avec le même contenu.

Étape 4 Saisissez un nom pour l'objet (sous **Name**) et, facultativement, une description.

Étape 5 Dans la zone du corps de l'objet, saisissez les commandes et les instructions pour produire la configuration requise.

Le contenu de l'objet est une séquence de commandes de script et de commandes de configuration qui génère une séquence de commandes logicielles ASA valide. Le périphérique défense contre les menaces utilise des commandes logicielles ASA pour configurer certaines fonctionnalités. Pour en savoir plus sur les commandes de script et de configuration, consultez :

- Scripts de modèles, à la page 5
- Commandes de l'interface de ligne de commande dans les objets FlexConfig, à la page 2

Vous pouvez utiliser des variables pour fournir des renseignements qui ne peuvent être connus qu'au moment de l'exécution ou qui peuvent différer d'un périphérique à l'autre. Il vous suffit de saisir les variables de traitement, mais vous devez utiliser le menu **Insertion** pour ajouter des variables associées à des objets de politique ou à des variables système, ou qui sont des clés secrètes. Pour une description complète des variables, consultez Variables FlexConfig, à la page 6.

- Pour insérer des variables système, choisissez **Insert** > **Insert System Variable** > ***Variable Name*** (Insérer > Insérer des variables système > Nom de la variable). Pour une explication détaillée de ces variables, consultez Variables système FlexConfig, à la page 12.
- Pour insérer des variables d'objets de politique, choisissez **Insert** > **Insert Policy Object** > ***Object Type***(insérer le type d'objet de politique) et sélectionnez le type d'objet approprié. Ensuite, donnez un nom à la variable (qui peut être le même nom que l'objet de politique associé), sélectionnez l'objet à associer à la variable et cliquez sur **Save** (Enregistrer). Pour une explication détaillée de ces types, consultez Variables de l'objet politique FlexConfig, à la page 11. Pour plus de détails sur la procédure, consultez Ajouter une variable d'objet de politiques à un objet FlexConfig, à la page 28.
- Pour insérer des variables de clé secrète, choisissez **Insert** > **Secret Key** et définissez le nom et la valeur de la variable. Pour plus de détails sur la procédure, consultez Configurer des clés secrètes, à la page 29.

Remarque Vous devez utiliser le menu **Insertion** pour créer un nouvel objet de politique ou une variable système. Cependant, pour les utilisations ultérieures de cette variable, vous devrez la saisir, $ inclus. Cela est également vrai pour les variables système : la première fois que vous l'utilisez, ajoutez-la à partir du menu **Insertion**. Ensuite, saisissez-le pour une utilisation ultérieure. Si vous utilisez le menu **Insertion** plus d'une fois pour une variable système, la variable système est ajoutée à la liste des variables plusieurs fois et FlexConfig ne sera pas validé, ce qui signifie que vous ne pouvez pas enregistrer vos modifications. Pour les variables de traitement (qui ne sont pas associées à un objet de politique ou à une variable système), saisissez simplement la variable. Si vous ajoutez une clé secrète, utilisez toujours le menu **Insérer**. Les variables de clés secrètes ne s'affichent pas dans la liste des variables.

Étape 6 Choisissez la fréquence et le type de déploiement.

- **Deployment** (déploiement) : s'il faut déployer les commandes dans l'objet **Une fois** ou un **À chaque fois**. La seule façon de choisir la bonne option est de tester les résultats du déploiement.

  Commencez par sélectionner **À chaque fois**. Ensuite, après avoir associé l'objet à une politique FlexConfig, déployez la configuration. Après un déploiement réussi, revenez à la politique FlexConfig et prévisualisez la configuration pour l'un des périphériques affectés, comme décrit dans Prévisualiser la politique FlexConfig, à la page 33. Si la section étiquetée `###CLI generated from managed features ### (###CLI générée à partir des fonctionnalités gérées ###` contient des commandes qui effacent ou annulent les commandes dans l'objet, et la section `###Flex-config Appended CLI ###` (###CLI de Flex-config ajoutée ###) contient les commandes pour reconfigurer la fonctionnalité, vous sachez que **À chaque fois** est la bonne option.

  Même si vous ne voyez pas de commandes d'annulation, apportez quelques modifications mineures à la configuration du périphérique, puis exécutez un autre déploiement. Si le déploiement se termine avec succès, vous pouvez consulter la transcription du déploiement (voir Vérifier la configuration déployée, à la page 34). Si vous voyez que les commandes ont été de nouveau exécutées (même si elles étaient déjà configurées) sans erreur, vous pouvez conserver **À chaque fois**.

  Définissez la valeur **Une fois** seulement si le système n'annule pas d'abord les commandes de l'objet avant de les relancer ou si le déploiement entraîne des erreurs spécifiques à la commande. Dans certains cas, le système ne vous permet pas d'émettre une commande qui est déjà configurée, mais ceci reste l'exception.

  Quelques conseils supplémentaires :

  - Si l'objet FlexConfig pointe vers des objets gérés par le système, tels que des objets réseau ou ACL, choisissez **À chaque fois**. Sinon, les mises à jour des objets pourraient ne pas être déployées.
  - Utilisez **Une fois** si la seule chose que vous faites dans l'objet est d'effacer une configuration. Supprimez ensuite l'objet de la politique FlexConfig après le prochain déploiement.

- **Type** : sélectionnez l'une des options suivantes :
  - **Append** (Ajouter) : (valeur par défaut) Les commandes de l'objet sont placées à la fin des configurations générées à partir des politiques centre de gestion. Vous devez utiliser la fonction Append si vous utilisez des variables d'objets de politique, qui pointent vers des objets générés à partir d'objets gérés. Si les commandes générées pour d'autres politiques chevauchent celles spécifiées dans l'objet, vous devez sélectionner cette option pour que vos commandes ne soient pas remplacées. Il s'agit de l'option la plus sûre.
  - **Prepend** (Ajouter au début) : les commandes dans l'objet sont placées au début des configurations générées à partir des politiques centre de gestion. Vous utilisez généralement Prepend pour les commandes qui effacent ou annulent une configuration.

Étape 7 (Facultatif) Cliquez sur **Validate** () au-dessus du corps de l'objet pour vérifier l'intégrité du script.

L'objet est toujours validé lorsque vous cliquez sur **Enregistrer**. Vous ne pouvez pas enregistrer un objet non valide.

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Ajouter une variable d'objet de politiques à un objet FlexConfig

Vous pouvez insérer des variables dans un objet de politique FlexConfig qui sont associées à d'autres types d'objet de politique. Lorsque FlexConfig est déployé sur un périphérique, ces variables résolvent les noms ou le contenu de l'objet associé.

Utilisez la procédure suivante pour la première utilisation d'une variable d'objet de politique dans un objet FlexConfig. Si vous devez de nouveau vous référer à l'objet, saisissez la variable (y compris le signe $). Pour comprendre comment utiliser ces variables, consultez Comment traiter les variables, à la page 7.

Avant de commencer

Pour en savoir plus sur la modification d'un objet FlexConfig, consultez Configurer les objets FlexConfig, à la page 25.

Procédure

Étape 1 Lors de la modification d'un objet de politique FlexConfig, choisissez **Insert (Insérer)** > **Insert Policy Object (Insérer un objet Politique)** > ***Object Type (Type d'objet)***, en sélectionnant le type d'objet approprié.

Étape 2 Saisissez un nom pour la variable et, éventuellement, une description.

Le nom doit être unique dans le contexte de l'objet FlexConfig. Il ne peut pas contenir d'espaces. Vous êtes autorisé à utiliser exactement le même nom que l'objet associé à la variable.

Étape 3 Sélectionnez l'objet à associer à la variable et cliquez sur **Add** (Ajouter) pour le déplacer vers la liste **Selected Object** (objet sélectionné).

Vous ne pouvez associer une variable qu'à un seul objet.

Remarque Pour les objets texte, vous pouvez sélectionner n'importe quel objet prédéfini selon vos besoins. Cependant, bon nombre de ces objets n'ont pas de valeur par défaut. Vous devez mettre à jour les objets pour ajouter les valeurs requises directement ou en tant que remplacements pour le périphérique sur lequel vous déploierez l'objet FlexConfig. Essayer de déployer une configuration FlexConfig sans mettre à jour ces objets entraîne généralement des erreurs de déploiement.

Étape 4 Cliquez sur **Save** (enregistrer).

La variable s'affiche dans la liste Variables au bas de l'éditeur d'objets FlexConfig.

Configurer des clés secrètes

Une clé secrète est une variable à chaîne unique dont vous souhaitez masquer le contenu, comme les mots de passe. Le système offre un traitement spécial à ces variables afin de vous aider à empêcher la diffusion de renseignements confidentiels.

Les variables à clé secrète ne s'affichent pas dans la liste Variables de l'objet FlexConfig.

Utilisez la procédure suivante pour créer, insérer et gérer des variables de clé secrète dans un objet FlexConfig. Contrairement à d'autres types de variables, vous pouvez utiliser la commande **Insert** (Insérer) chaque fois que vous devez insérer une variable de clé secrète donnée. En ce qui concerne le traitement, ces variables se comportent comme des variables d'objet texte à valeur unique; voir Variables à valeur unique, à la page 7.

Remarque Toutes les données définies dans une variable de clé secrète sont masquées pour les utilisateurs, sauf lors de la prévisualisation d'une politique FlexConfig. En outre, si vous exportez une politique FlexConfig, le contenu de toute variable de clé secrète est effacé. Lorsque vous importerez la politique, vous devrez modifier manuellement chaque variable de clé secrète pour saisir les données.

Avant de commencer

Pour en savoir plus sur la modification d'un objet FlexConfig, consultez Configurer les objets FlexConfig, à la page 25.

Procédure

Étape 1 Lors de la modification d'un objet de politique FlexConfig, choisissez **Insert (Insérer)** > **Secret Key (Clé secrète)**.

Étape 2 Dans la boîte de dialogue **Insert Secret Key** (insérer la clé secrète), effectuez l'une des opérations suivantes :

- Pour créer une clé, cliquez sur **Add Secret Key** (Ajouter une clé secrète), remplissez les champs suivants et cliquez sur **Add** (Ajouter).
  - **Secret Key Name** (nom de la clé secrète) : nom de la variable. Ce nom apparaît dans l'objet FlexConfig précédé de @.
  - **Password**(mot de passe), **Confirm Password**(confirmer le mot de passe) : chaîne secrète masquée par des astérisques lorsque vous la saisissez.
- Pour insérer une variable de clé secrète dans l'objet FlexConfig, cochez la case de la variable.
- Pour modifier la valeur d'une variable de clé secrète, cliquez sur **Edit** ( ) en regard de la variable. Apportez vos modifications et cliquez sur **Add** (Ajouter).
- Pour supprimer une variable de clé secrète, cliquez sur **Supprimer** ( ) en regard de la variable.

Étape 3 Cliquez sur **Save** (enregistrer).

Configurer les objets texte FlexConfig

Utilisez des objets de texte dans les objets FlexConfig comme cible des variables d'objet de politique. Vous pouvez utiliser des variables pour fournir des renseignements qui ne peuvent être connus qu'au moment de l'exécution ou qui peuvent différer d'un périphérique à l'autre. Lors du déploiement, les variables qui pointent vers des objets texte sont remplacées par le contenu de l'objet texte.

Les objets texte contiennent des chaînes de forme libre, qui peuvent être des mots-clés, des noms d'interface, des numéros, des adresses IP, etc. Le contenu dépend de la façon dont vous utiliserez les informations dans un script FlexConfig.

Avant de créer ou de modifier un objet texte, déterminez exactement le contenu dont vous avez besoin. Cela inclut la manière dont vous avez l'intention de traiter l'objet, ce qui vous aidera à choisir entre la création d'un objet à chaîne unique ou à chaînes multiples. Consultez les rubriques suivantes :

- Variables FlexConfig, à la page 6
- Comment traiter les variables, à la page 7

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Choisissez **FlexConfig** > **Text Object** (Objet texte) dans la liste des types d'objet.

Étape 3 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add Text Object** (Ajouter un nouvel objet) pour créer un nouvel objet.
- Cliquez sur **Edit** (✎) pour modifier un objet existant. Vous êtes autorisé à modifier les objets texte prédéfinis, ce qui est obligatoire si vous souhaitez utiliser les objets FlexConfig prédéfinis.

Étape 4 Saisissez un nom pour l'objet (sous **Name**) et, facultativement, une description.

Étape 5 (Nouveaux objets uniquement.) Sélectionnez un **type de variable** dans la liste déroulante :

- **Single** (unique) : si l'objet ne doit contenir qu'une seule chaîne de texte.
- **Multiple** (multiple) : si l'objet doit contenir une liste de chaînes de texte.

Vous ne pouvez pas modifier le type de variable après avoir enregistré l'objet.

Étape 6 Si le type de variable est **Multiple**, utilisez les flèches vers le haut et vers le bas pour préciser le **Nombre**.

Des lignes sont ajoutées ou supprimées de l'objet à mesure que vous modifiez le nombre.

Étape 7 Ajouter du contenu à l'objet.

Vous pouvez soit cliquer dans la zone de texte à côté d'un numéro de variable et saisir une valeur, soit configurer des remplacements de périphérique pour chaque périphérique auquel un objet FlexConfig utilisant l'objet texte sera affecté. Vous pouvez également faire les deux, auquel cas les valeurs configurées dans l'objet de base agissent comme valeurs par défaut dans les cas où un remplacement n'existe pas pour un périphérique donné.

Lors de l'édition d'objets prédéfinis, il est conseillé d'utiliser des remplacements de périphériques, afin que les valeurs par défaut du système restent en place pour les autres utilisateurs qui pourraient avoir besoin d'utiliser l'objet dans d'autres politiques FlexConfig. L'approche que vous adopterez dépend des besoins de votre entreprise.

Astuces Certains objets prédéfinis nécessitent plusieurs valeurs, chaque valeur servant un objectif spécifique. Lisez attentivement le texte de la description pour déterminer les valeurs attendues dans l'objet. Dans certains cas, les instructions précisent que vous devez utiliser les remplacements au lieu de modifier les valeurs de base. Dans le cas de EnableInspectProtocolList, vous ne pouvez pas saisir des protocoles dont l'inspection est incompatible avec l'inspection Snort.

Si vous décidez d'utiliser les remplacements de périphérique, procédez comme suit.

a) Cochez la case **Allow Overrides** (autoriser les remplacements) .
b) Développez la zone Overrides (Remplacements) (au besoin) et cliquez sur **Add** (Ajouter).

   Si un remplacement existe déjà pour le périphérique, cliquez sur Edit (modifier) concernant ce remplacement pour le modifier.

c) Dans **Targets** (Cibles) de la boîte de dialogue Add Object Override (ajouter un remplacement d'objet), sélectionnez le périphérique pour lequel vous définissez des valeurs, puis cliquez sur **Add** (Ajouter) pour le déplacer vers la liste Selected Devices (Périphériques sélectionnés).
d) Cliquez sur **Override**(Remplacer), ajustez le champ **Count** (nombre) au besoin, puis cliquez dans les champs de variable et saisissez les valeurs pour le périphérique.
e) Cliquez sur **Add** (ajouter).

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Configurer la politique FlexConfig

Une politique FlexConfig contient deux listes ordonnées d'objets FlexConfig, une liste ajoutée au début et l'autre ajoutée. Pour une explication de l'ajout/complément, consultez Configurer les objets FlexConfig, à la page 25.

Les politiques FlexConfig sont des politiques partagées que vous pouvez affecter à plusieurs périphériques.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **FlexConfig**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **New Policy** pour créer une nouvelle politique FlexConfig. Vous êtes invité à saisir un nom. Si vous le souhaitez, sélectionnez des périphériques dans la liste des périphériques disponibles et cliquez sur **Add to Policy** (Ajouter à la politique) pour affecter des périphériques. Cliquez sur **Save** (enregistrer).
- Cliquez sur **Edit** ( ) pour modifier une politique existante. Vous pouvez modifier le nom ou la description en cliquant dessus en mode d'édition.
- Cliquez sur **Copier** ( ) pour créer une nouvelle politique avec le même contenu. Vous êtes invité à saisir un nom. Les affectations de périphérique ne sont pas conservées pour la copie.

- Cliquez sur delete (supprimer) pour supprimer une politique dont vous n'avez plus besoin.

Étape 3 Sélectionnez les objets FlexConfig requis pour la politique dans la liste **FlexConfig disponible** et cliquez sur > pour les ajouter à la politique.

Les objets sont automatiquement ajoutés à la liste, ajoutée au début ou à la fin, en fonction du type de déploiement spécifié dans l'objet FlexConfig.

Pour supprimer un objet sélectionné, cliquez sur **Supprimer** ( ) à côté d'un objet.

Étape 4 Pour chaque objet sélectionné, cliquez sur **Afficher** ( ) à côté de l'objet pour identifier les variables utilisées dans l'objet.

À l'exception des variables système, qui commencent par SYS, vous devez vous assurer que les objets associés aux variables ne sont pas vides. Un espace ou des crochets sans rien entre eux, [ ], indiquent un objet vide. Vous devrez modifier ces objets avant de déployer la politique.

Remarque Si vous utilisez des remplacements d'objets, ces valeurs ne s'afficheront pas dans cet affichage. Ainsi, une valeur par défaut vide ne signifie pas nécessairement que vous n'avez pas mis à jour l'objet avec les valeurs requises. Un aperçu de la configuration affichera si les variables se résolvent correctement pour un périphérique donné. Consultez Prévisualiser la politique FlexConfig, à la page 33.

Étape 5 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Définir les machines cibles pour la politique; voir Définir les périphériques cibles pour une politique FlexConfig, à la page 32.
- Déployer les changements de configuration.

Définir les périphériques cibles pour une politique FlexConfig

Lorsque vous créez une politique FlexConfig, vous pouvez sélectionner les périphériques qui utilisent la politique. Vous pouvez ultérieurement modifier les affectations de périphérique pour la politique comme décrit ci-dessous.

Remarque Normalement, lorsque vous annulez l'attribution d'une politique à un périphérique, le système supprime automatiquement la configuration associée lors du prochain déploiement. Cependant, comme les objets FlexConfig sont des scripts pour déployer des commandes personnalisées, la simple suppression d'une politique FlexConfig d'un périphérique ne supprime pas les commandes qui étaient en cours de configuration par les objets FlexConfig. Si votre intention est de supprimer les commandes générées par FlexConfig de la configuration d'un périphérique, consultez Supprimer des fonctionnalités configurées à l'aide de FlexConfig, à la page 36.

Procédure

Étape 1 Choisissez **Devices (Périphériques)** > **FlexConfig** et modifiez une politique FlexConfig.

Étape 2 Cliquez sur **Policy Assignments** (Attributions de politiques)

Étape 3 Su les **Targeted Devices** (périphériques ciblés), créez votre liste de cibles :

- Add (ajouter) : choisissez un ou plusieurs **Available Devices** (périphériques disponible), puis cliquez sur **Add to Policy** (ajouter à la politique) ou faites un glisser-déposer vers la liste des **périphériques sélectionnés**. Vous pouvez affecter la politique aux périphériques, aux paires à haute disponibilité et aux périphériques en grappe.
- Delete (Supprimer) : Cliquez sur **Supprimer** ( ) à côté d'un seul périphérique, ou sélectionnez plusieurs périphériques, effectuez un clic droit, puis choisissez **Delete Selection** (Supprimer la sélection).

Étape 4 Cliquez sur **OK** pour enregistrer votre sélection.

Étape 5 Cliquez sur **Save** pour enregistrer la politique FlexConfig.

Prochaine étape

- Déployer les changements de configuration.

Prévisualiser la politique FlexConfig

Présélectionnez une politique FlexConfig pour voir comment les objets FlexConfig sont traduits en commandes CLI. L'aperçu montre les commandes qui seront générées pour un périphérique sélectionné à partir des scripts et des variables utilisées dans les objets FlexConfig. Les variables sont résolues en fonction de la configuration du périphérique, de sorte que vous avez une idée claire de ce qui sera déployé.

Utilisez l'aperçu pour rechercher des problèmes potentiels dans les objets FlexConfig. Corrigez les objets jusqu'à ce que l'aperçu affiche les résultats attendus.

Vous devez prévisualiser la configuration séparément pour chaque périphérique, car les variables peuvent se résoudre différemment en fonction de la configuration du périphérique.

Procédure

Étape 1 Choisissez **Devices (Périphériques)** > **FlexConfig** et modifiez une politique FlexConfig.

Étape 2 Si des modifications sont en attente, cliquez sur **Save** (Enregistrer).

L'aperçu affiche uniquement les résultats des objets FlexConfig qui se trouvent dans la dernière version enregistrée de la politique. Vous devez enregistrer la politique pour voir un aperçu des objets nouvellement ajoutés.

Étape 3 Cliquez sur **Preview Config** (Prévisualiser la configuration).

Étape 4 Sélectionnez un périphérique dans la liste déroulante **Select Device** (Sélectionner un périphériques).

Le système récupère les informations du périphérique et des politiques configurées, et détermine les commandes CLI qui seront générées lors du prochain déploiement sur le périphérique. Vous pouvez sélectionner le résultat

et utiliser les touches Ctrl + C pour le copier dans le presse-papiers, où vous pourrez le coller dans un fichier texte pour une analyse plus approfondie.

La prévisualisation comprend les sections suivantes :

- Flex-config Prepended CLI : ces commandes générées par FlexConfigs sont ajoutées au début de la configuration.
- Interface de commande en ligne générée à partir des fonctionnalités gérées : Il s'agit de commandes générées pour les politiques configurées dans le centre de gestion. Des commandes sont générées pour les politiques nouvelles ou modifiées depuis le dernier déploiement réussi sur le périphérique. Ces commandes ne représentent pas toutes les commandes nécessaires pour mettre en œuvre les politiques attribuées. Aucune commande dans cette section n'est générée à partir d'objets FlexConfig.
- Flex-config Appended CLI : ces commandes générées par les configurations FlexConfig sont ajoutées à la configuration.

Étape 5 Cliquez sur **Close** pour fermer la boîte de dialogue d'aperçu.

Vérifier la configuration déployée

Après avoir déployé une politique FlexConfig sur un périphérique, vérifiez que le déploiement a réussi et que la configuration qui en résulte est celle à laquelle vous vous attendez. Vérifiez également que le périphérique fonctionne comme prévu.

Procédure

Étape 1 Pour vérifier que le déploiement a réussi :

a) Cliquez sur **Notifications** dans la barre de menus, qui est sans nom entre **Deploy** et **System**(Déploiement et Système).

L'icône ressemble à l'une des suivantes, et elle peut inclure un chiffre en cas d'erreur :

- **Indique qu'il n'y a aucun avertissement** : indique qu'aucun avertissement ou erreur n'est présent sur le système.
- Indique **un ou plusieurs avertissements** : indique un ou plusieurs avertissements et qu'aucune erreur n'est présente sur le système.
- **Indique une ou plusieurs erreurs** : indique qu'une ou plusieurs erreurs et un certain nombre d'avertissements sont présents sur le système.

b) Dans la section **Deployments**(déploiements), vérifiez que le déploiement a réussi.

c) Pour voir des informations plus détaillées, en particulier sur les déploiements qui ont échoué, cliquez sur **Afficher l'historique**.

d) Sélectionnez la tâche de déploiement dans la liste de tâches de la colonne de gauche.

Les emplois sont classés en ordre chronologique inverse, le travail le plus récent en haut de la liste.

e) Cliquez sur download (télécharger) dans la colonne **Transcription** pour le périphérique dans la colonne de droite.

La transcription de déploiement comprend les commandes envoyées à l'appareil et toutes les réponses renvoyées par l'appareil. Ces réponses peuvent être des messages informatifs ou des messages d'erreur. Pour les déploiements qui ont échoué, recherchez les messages qui indiquent des erreurs dans les commandes que vous avez envoyées par l'intermédiaire de FlexConfig. Ces erreurs peuvent vous aider à corriger le script dans l'objet FlexConfig qui tente de configurer les commandes.

Remarque Il n'y a aucune distinction faite dans la transcription entre les commandes envoyées pour les fonctionnalités gérées et celles générées par les politiques FlexConfig.

Par exemple, la séquence suivante montre que les commandes centre de gestion envoyées pour configurer GigabitEthernet0/0 avec le nom logique à l'extérieur. L'appareil a répondu qu'il réglait automatiquement le niveau de sécurité sur 0.Défense contre les menaces n'utilise le niveau de sécurité pour rien. Les messages relatifs à FlexConfig se trouvent dans la section Appliquer l'interface CLI de la transcription.

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

Étape 2 Vérifiez que la configuration déployée comprend les commandes attendues.

Pour ce faire, vous pouvez établir une connexion SSH à l'adresse IP de gestion du périphérique. Pour afficher la configuration, utilisez la commande **show running-config**.

Vous pouvez également utiliser l'outil CLI dans Cisco Secure Firewall Management Center.

a) Choisissez > **Intégrité** > **Moniteur** et cliquez sur le nom du périphérique.

   Vous devrez peut-être cliquer sur la flèche d'ouverture/fermeture dans la colonne **Nombre** du tableau d'état pour voir les périphériques.

b) Cliquez sur **Advanced Troubleshooting** (Dépannage avancé).
c) Cliquez sur **Threat Defense CLI** (Interface de ligne de commande Threat Defense).
d) Sélectionnez **show** (afficher) comme commande et saisissez **running-config** comme paramètre.
e) Cliquez sur **Execute** (Exécuter).

   La configuration en cours s'affiche dans la zone de texte. Vous pouvez sélectionner la configuration et appuyer sur Ctrl + C, puis la coller dans un fichier texte pour une analyse ultérieure.

Étape 3 Vérifiez que le périphérique fonctionne comme prévu.

Utilisez les commandes **show** associées à la fonctionnalité pour afficher des informations détaillées et des statistiques. Par exemple, si vous avez activé des inspections de protocole supplémentaires, la commande **show service-policy** fournit cette information. Les commandes exactes à utiliser dépendent de la fonctionnalité et doivent être mentionnées dans le guide de configuration ASA et la référence de commande que vous avez utilisée pour apprendre comment configurer la fonctionnalité.

Si les commandes qui affichent des statistiques indiquent que les chiffres ne changent pas (par exemple, le nombre de résultats, le nombre de connexions, etc.), la configuration peut être valide, mais non significative. Si vous savez que le trafic passe par le périphérique et que cela devrait apparaître dans les statistiques, cherchez ce qui manque dans votre configuration. Par exemple, la NAT ou les règles d'accès peuvent supprimer ou modifier le trafic avant qu'une fonctionnalité ne puisse agir.

Vous pouvez utiliser les commandes **show** à partir d'une session SSH ou à l'aide de l'outil CLI centre de gestion.

Toutefois, si la commande **show** que vous devez utiliser n'est pas disponible directement dans la CLI défense contre les menaces , vous devrez établir une connexion SSH avec le périphérique pour utiliser les commandes. À partir de l'interface de ligne de commande, saisissez la séquence de commandes suivante pour passer en mode d'exécution privilégié dans l'interface de ligne de commande de dépistage. À partir de là, vous devriez être en mesure de saisir ces commandes **show** non prises en charge.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> enable
Password: <press enter, do not enter a password>
firepower#
```

Supprimer des fonctionnalités configurées à l'aide de FlexConfig

Si vous décidez que vous devez supprimer un ensemble de commandes de configuration que vous avez configurées à l'aide de FlexConfig, vous devrez peut-être supprimer cette configuration manuellement. L'annulation de l'attribution de la politique FlexConfig à un périphérique peut ne pas supprimer toute la configuration.

Pour supprimer manuellement la configuration, vous créez de nouveaux objets FlexConfig pour effacer ou annuler les commandes de configuration.

Avant de commencer

Pour déterminer si vous devez supprimer manuellement une partie ou toute la configuration générée par un objet :

1. Examinez l'aperçu de la configuration, comme décrit dans Prévisualiser la politique FlexConfig, à la page 33. Si la section `###CLI générée à partir des fonctionnalités gérées ###` contient les commandes clear ou negate pour supprimer toutes les commandes de l'objet FlexConfig, vous pouvez simplement supprimer l'objet de la politique FlexConfig, l'enregistrer et la redéployer.
2. Supprimez l'objet de la politique FlexConfig, enregistrez la modification, puis prévisualisez à nouveau la configuration. Si l'interface de ligne de commande (`CLI générée à partir des fonctionnalités gérées) # #` section ## n'inclut toujours pas les commandes d'effacement ou de refus requises, vous devez suivre cette procédure pour supprimer manuellement la configuration.

Procédure

Étape 1 Choisissez **Objects (Objets)** > **Object Management (gestion des objets)** et créez les objets FlexConfig pour effacer ou annuler les commandes de configuration.

Si une fonctionnalité comporte une commande **clear** qui peut supprimer tous les paramètres de configuration, utilisez cette dernière. Par exemple, l'objet prédéfini ISIS_Unconfigure_All contient une seule commande qui supprime toutes les commandes de configuration liées à ISIS :

```
clear configure router isis
```

S'il n'y a pas de commande **clear** pour cette fonctionnalité, vous devez utiliser la forme **no** de chaque commande que vous souhaitez supprimer. Par exemple, l'objet prédéfini Sysopt_basic_negate supprime les commandes configurées au moyen de l'objet prédéfini Sysopt_basic.

```
no sysopt traffic detailed-statistics

no sysopt connection timewait
```

Vous devez généralement configurer un objet FlexConfig qui supprime les configurations en tant qu'objet à déploiement unique ajouté au début.

Étape 2 Choisissez **Devices (Périphériques)** > **FlexConfig** et créez une nouvelle politique FlexConfig ou modifiez la politique existante.

Si vous souhaitez conserver la politique FlexConfig qui déploie les commandes de configuration, créez une nouvelle politique spécifiquement pour annuler les commandes et affectez les périphériques à la politique. Ajoutez ensuite les nouveaux objets FlexConfig à la politique.

Si vous souhaitez supprimer complètement les objets de configuration FlexConfig de tous les périphériques, vous pouvez simplement supprimer ces commandes de la politique FlexConfig existante et les remplacer par les objets qui annulent la configuration.

Étape 3 Cliquez sur **Save** pour enregistrer la politique FlexConfig.

Étape 4 Cliquez sur **Aperçu de la configuration** et vérifiez que les commandes d'effacement et de négation sont générées correctement.

Étape 5 Choisissez **Deploy** > **Deployment** (déployer > déploiement) dans la barre de menus, sélectionnez le périphérique et cliquez sur **Deploy**(déployer).

Attendez que le déploiement soit terminé.

Étape 6 Vérifiez que les commandes ont été supprimées.

Affichez la configuration en cours sur le périphérique pour confirmer que les commandes sont supprimées. Pour de plus amples renseignements, voir Vérifier la configuration déployée, à la page 34.

Étape 7 Lors de la modification de la politique FlexConfig, cliquez sur **Policy Affectations** (affectations de politiques) et supprimez le périphérique. Vous pouvez également supprimer les objets FlexConfig de la politique.

En supposant que la politique FlexConfig supprime simplement les commandes de configuration indésirables, il n'est pas nécessaire de conserver la politique attribuée au périphérique une fois la suppression effectuée.

Toutefois, si la politique FlexConfig conserve des options que vous souhaitez toujours configurer sur le périphérique, supprimez les objets de négation de la politique. Ils ne sont plus nécessaires.

Conversion de la fonctionnalité FlexConfig vers la fonctionnalité gérée

Chaque version du logiciel ajoute des fonctionnalités gérées au produit, c'est-à-dire des fonctionnalités que vous configurez directement au moyen de politiques contrôlées à l'extérieur de FlexConfig. Cela peut rendre obsolètes les commandes FlexConfig que vous utilisez actuellement; vos configurations ne sont pas converties automatiquement. Après la mise à niveau, vous ne pourrez plus affecter ou créer des objets FlexConfig à l'aide des nouvelles commandes obsolètes. Après la mise à niveau du logiciel, examinez vos politiques et vos objets FlexConfig.

Lorsqu'une fonctionnalité que vous avez configurée à l'aide de FlexConfig commence à être prise en charge en tant que fonctionnalité gérée, vous devez passer de l'utilisation de FlexConfig à l'utilisation de la fonctionnalité gérée. Dans la plupart des cas, vos configurations FlexConfig existantes continuent de fonctionner après la mise à niveau et vous pouvez toujours procéder au déploiement. Cependant, dans certains cas, l'utilisation de commandes obsolètes peut entraîner des problèmes de déploiement. La configuration d'une fonctionnalité à la fois dans l'interface graphique et dans FlexConfig n'est pas prise en charge.

Remarque Utilisez l'outil de migration au lieu de cette procédure si l'outil prend en charge la configuration de fonctionnalité que vous migrez.

Procédure

Étape 1 Supprimez FlexConfig, comme expliqué dans Supprimer des fonctionnalités configurées à l'aide de FlexConfig, à la page 36.

Étape 2 Configurez les paramètres de la nouvelle fonctionnalité gérée prise en charge.

Les notes de version contiennent une liste des nouvelles fonctionnalités pour la version.

Exemples de FlexConfig

Voici quelques exemples d'utilisation de FlexConfig.

Configurer le protocole PTP (Precision Time Protocol) (ISA 3000)

Le protocole PTP (Precision Time Protocol) est un protocole de synchronisation horaire développé pour synchroniser les horloges de divers périphériques au sein d'un réseau par paquets. Ces horloges sont généralement de précision et de stabilité variables. Le protocole est spécialement conçu pour les systèmes de mesure et de contrôle industriels en réseau. Il est idéal pour une utilisation dans les systèmes distribués, car il nécessite une bande passante et un surdébit de traitement minimaux.

Un système PTP est un système en réseau distribué, composé d'une combinaison de périphériques PTP et non-PTP. Les périphériques PTP comprennent les horloges normales, les horloges périphériques et les horloges transparentes. Les périphériques non PTP comprennent les commutateurs réseau, les routeurs et les autres périphériques de l'infrastructure.

Vous pouvez configurer le périphérique défense contre les menaces pour qu'il soit une horloge transparente. Le périphérique défense contre les menaces ne synchronise pas son horloge avec les horloges PTP. Le périphérique défense contre les menaces utilisera le profil PTP par défaut, comme défini sur les horloges PTP.

Lorsque vous configurez les périphériques PTP, vous définissez un numéro de domaine pour les périphériques destinés à fonctionner ensemble. Ainsi, vous pouvez configurer plusieurs domaines PTP, puis configurer chaque périphérique non PTP pour utiliser les horloges PTP d'un domaine spécifique.

Avant de commencer

Déterminez le numéro de domaine configuré sur les horloges PTP que le périphérique doit utiliser. Cet exemple suppose que le numéro de domaine PTP est 10. Déterminez également les interfaces par lesquelles le système peut atteindre les horloges PTP du domaine.

Voici des consignes pour la configuration du PTP :

- Cette fonctionnalité est uniquement disponible sur le périphérique Cisco ISA 3000.
- Cisco PTP prend uniquement en charge les messages PTP en multidiffusion.
- Le PTP est disponible uniquement pour les réseaux IPv4, et non pour les réseaux IPv6.
- La configuration PTP est prise en charge sur les interfaces de données Ethernet physiques, qu'elles soient autonomes ou membres d'un groupe de ponts. Elle n'est pas prise en charge sur l'interface de gestion, les sous-interfaces, les EtherChannels, les interfaces virtuelles de pont (BVI) ou toute autre interface virtuelle.
- Les flux PTP sur les sous-interfaces VLAN sont pris en charge, en supposant que la configuration PTP appropriée est présente sur l'interface parente.
- Vous devez vous assurer que les paquets PTP sont autorisés à circuler dans le périphérique. Le trafic PTP est identifié par les ports de destination UDP 319 et 320 et par l'adresse IP de destination 224.0.1.129, donc toute règle de contrôle d'accès qui autorise ce trafic devrait fonctionner.
- En mode de pare-feu routé, vous devez activer le routage de multidiffusion pour les groupes de multidiffusion PTP. En outre, si une interface sur laquelle vous activez le PTP ne se trouve **pas** dans un groupe de pont, vous devez configurer l'interface pour qu'elle rejoigne le groupe de multidiffusion IGMP 224.0.1.129. Si l'interface physique est un membre d'un groupe de pont, vous ne la configurez pas pour rejoindre le groupe de multidiffusion IGMP.

Procédure

Étape 1 (Mode routé uniquement.) Activez le routage de multidiffusion et configurez le groupe IGMP pour les interfaces.

En mode routage, vous devez activer le routage de multidiffusion. De plus, pour les interfaces physiques autonomes, c'est-à-dire celles qui ne sont pas membres de groupes de ponts, vous devez également configurer l'interface pour qu'elle rejoigne le groupe IGMP 224.0.1.129. Vous ne pouvez pas configurer les membres d'un groupe de ponts pour qu'ils rejoignent un groupe IGMP, mais la configuration PTP sur les membres du groupe de ponts fonctionnera sans la jonction IGMP.

Effectuez cette procédure pour chaque périphérique sur lequel vous configurerez PTP.

Remarque Notez les noms matériels de chaque interface orientée vers l'horloge PTP sur chaque appareil, par exemple GigabitEthernet1/1.

a) Sélectionnez **Devices (périphériques)** > **Device Management (gestion des périphériques)**, et modifiez le périphérique.
b) Cliquez sur **Routing** (Routage).
c) Choisissez **Multicast Routing(Routage de multidiffusion)** > **IGMP**.
d) Cochez la case **Enable Multicast Routing** (activer le routage de multidiffusion).
e) Cliquez sur **Join Group** (Rejoindre le groupe).

f) Cliquez sur **Add**(ajouter) puis, dans la boîte de dialogue **Add IGMP Join Group Settings** (ajouter des paramètres de groupe de jonction IGMP), configurez les options suivantes, puis cliquez sur **OK**.

- **Interface** : Sélectionnez l'interface autonome PTP orientée vers l'horloge.
- **Join Group** (Rejoindre le groupe) : Cliquez sur **+** pour ajouter un nouvel objet réseau. Créez un objet Hôte avec l'adresse 224.0.1.129. Lors de la configuration d'interfaces supplémentaires, sélectionnez simplement cet objet. (Consultez Création d'objets réseau.)

Répétez cette étape pour chaque interface autonome PTP dirigée vers l'horloge sur le périphérique.

g) Cliquez sur **Save** (Enregistrer) dans la page Routing (routage).

Étape 2 Créez l'objet FlexConfig pour activer PTP globalement et sur l'interface.

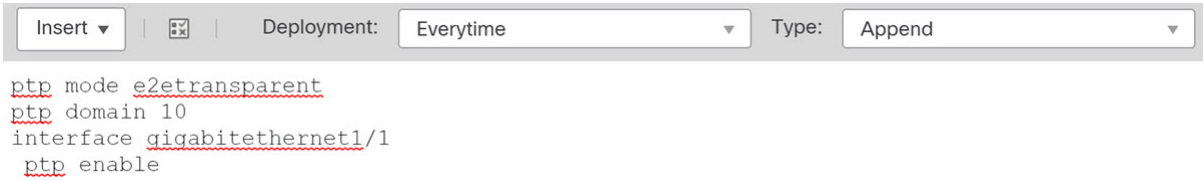
La procédure suivante suppose que l'interface PTP dirigée vers l'horloge est la même sur tous les périphériques que vous configurez. Si vous avez utilisé différentes interfaces sur différents périphériques, vous devez créer des objets distincts pour chaque combinaison distincte. Par exemple, si vous utilisez GigabitEthernet1/1 sur les périphériques A et B, GigabitEthernet1/2 sur les périphériques C et D et GigabitEthernet1/1 et 1/2 sur les périphériques E et F, vous avez besoin de 3 objets FlexConfig distincts et, par la suite, de 3 politiques FlexConfig distinctes (explications à l'étape suivante).

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.
b) Choisissez **FlexConfig** > **FlexConfig Object(Objet FlexConfig)** dans la table des matières.
c) Cliquez sur **Add FlexConfig Object** (Ajouter un objet FlexConfig), configurez les propriétés suivantes, puis cliquez sur **Save** (Enregistrer).

- **Name** : nom de l'objet. Par exemple, Enable_PTP.
- **Deployment** (déploiement) : sélectionnez **Anytime** (à tout moment). Vous souhaitez que cette configuration soit envoyée à chaque déploiement pour qu'il demeure configuré.
- **Type** : conservez la valeur par défaut, **Append** (Ajouter). Les commandes sont envoyées au périphérique après les commandes des fonctionnalités directement prises en charge. Cela garantit que toutes les autres modifications que vous apportez à la configuration de l'interface sont configurées avant ces commandes.
- **Object body** (Corps de l'objet) : dans le corps de l'objet, saisissez les commandes nécessaires pour configurer PTP globalement et sur chaque interface PTP oriente vers l'horloge. Par exemple, les commandes nécessaires à la configuration globale pour le domaine PTP 10 et à la configuration d'interface sur GigabitEthernet1/1 sont les suivantes :

```
ptp mode e2etransparent
ptp domain 10
interface gigabitethernet1/1
 ptp enable
```

Le corps de l'objet doit ressembler à ce qui suit :



Étape 3 Créez la politique FlexConfig et attribuez-la aux périphériques.

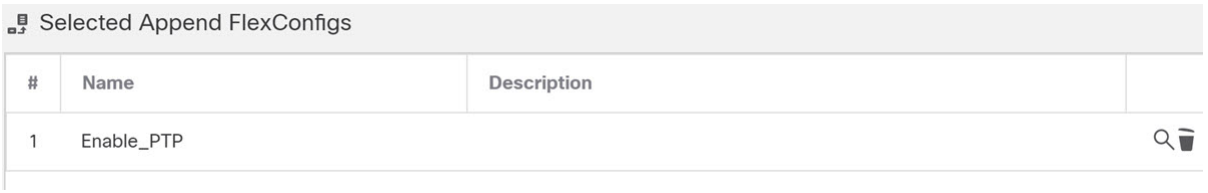
Si vous avez créé plusieurs objets FlexConfig pour différentes combinaisons d'interfaces PTP dirigées vers l'horloge, vous devez créer des politiques FlexConfig distinctes pour chaque objet et affecter ces politiques aux périphériques appropriés en fonction des interfaces que vous devez configurer. Répétez la procédure suivante pour chaque groupe de périphériques.

a) Sélectionnez **Devices (Périphériques)** > **FlexConfig**.
b) Cliquez sur **New Policy** (nouvelle politique) ou si une politique FlexConfig existante doit être affectée (ou est déjà affectée) aux périphériques cibles, modifiez simplement cette dernière.

Lors de la création d'une nouvelle politique, affectez les périphériques cibles à la politique dans la boîte de dialogue où vous nommez la politique.

c) Sélectionnez l'objet PTP FlexConfig dans le dossier **défini par l'utilisateur** dans la table des matières, puis cliquez sur > pour l'ajouter à la politique.

L'objet doit être ajouté à la liste **Selected Appended FlexConfigs** (FlexConfigs sélectionnées et ajoutées).



d) Cliquez sur **Save** (enregistrer).
e) Si vous n'avez pas encore affecté tous les périphériques ciblés à la politique, cliquez sur le lien **Policy Affectations** (affectations de politiques) ci-dessous Save and make the assignments now (enregistrer et effectuer les affectations maintenant).
f) Cliquez sur **Preview Config** (Aperçu de la configuration et dans la boîte de dialogue d'aperçu, sélectionnez l'un des périphériques attribués.

Le système génère un aperçu de l'interface de ligne de commande de configuration qui sera envoyée au périphérique. Vérifiez que les commandes générées à partir de l'objet PTP FlexConfig semblent correctes. Celles-ci seront affichées à la fin de l'aperçu. Notez que vous verrez également les commandes générées à partir d'autres modifications que vous avez apportées aux fonctionnalités gérées. En ce qui concerne les commandes PTP, le résultat devrait ressembler à ce qui suit :

```
###Flex-config Appended CLI ###
ptp mode e2etransparent
ptp domain 10
interface gigabitethernet1/1
 ptp enable
```

Étape 4 Déployez vos modifications.

Comme vous avez affecté une politique FlexConfig aux périphériques, vous recevez toujours un avertissement de déploiement destiné à vous mettre en garde contre l'utilisation de FlexConfig. Cliquez sur **Proceed (** continuer) pour poursuivre le déploiement.

Une fois le déploiement terminé, vous pouvez vérifier l'historique de déploiement et afficher la transcription du déploiement. Cela est particulièrement utile si le déploiement échoue. Consultez Vérifier la configuration déployée, à la page 34.

Étape 5 Vérifiez la configuration PTP sur chaque périphérique.

À partir d'une session SSH ou d'une session de console sur chaque périphérique, vérifiez les paramètres PTP :

```
> show ptp clock
 PTP CLOCK INFO
  PTP Device Type: End to End Transparent Clock
  Operation mode: One Step
  Clock Identity: 34:62:88:FF:FE:1:73:81
  Clock Domain: 10
  Number of PTP ports: 4
> show ptp port
 PTP PORT DATASET: GigabitEthernet1/1
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 1
  PTP version: 2
  Port state: Enabled

 PTP PORT DATASET: GigabitEthernet1/2
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 2
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/3
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 3
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/4
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 4
  PTP version: 2
  Port state: Disabled
```

Configurer le contournement matériel automatique en cas de panne de courant (ISA 3000)

Le contournement matériel garantit que le trafic continue de circuler entre une paire d'interfaces en ligne pendant une panne de courant. Les paires d'interfaces prises en charge sont les interfaces en cuivre GigabitEthernet 1/1 et 1/2; et GigabitEthernet 1/3 et 1/4. Si vous avez un modèle Ethernet à fibre optique, seule la paire Ethernet en cuivre (GigabitEthernet 1/1 et 1/2) prend en charge le contournement matériel.

Lorsque le contournement matériel est actif, le trafic passe entre ces paires d'interfaces au niveau de la couche 1. L'interface de ligne de commande de FTD verra les interfaces comme étant en panne. Aucune fonction de pare-feu n'est en place, assurez-vous donc de comprendre les risques de laisser le trafic passer par le périphérique.

Dans la console de l'interface de ligne de commande ou dans une session SSH, utilisez la commande **show hardware-bypass** pour surveiller l'état opérationnel.

Avant de commencer

Pour que le contournement matériel fonctionne :

- Vous devez placer les paires d'interfaces dans le même groupe de ponts.

- Vous devez connecter les interfaces pour accéder aux ports du commutateur. Ne les connectez pas aux ports de ligne principale.

Nous vous recommandons de désactiver la répartition aléatoire des numéros de séquence TCP globalement à l'aide de la politique de service de défense contre les menaces associée à la politique de contrôle d'accès attribuée au périphérique. Par défaut, l'ISA 3000 réécrit le numéro de séquence initial (ISN) des connexions TCP qui le traversent en nombre aléatoire. Lorsque le contournement matériel est activé, l'ISA 3000 ne se trouve plus dans le chemin de données et ne traduit pas les numéros de séquence. Le client destinataire reçoit un numéro de séquence inattendu et interrompt la connexion. La session TCP doit donc être rétablie. Même lorsque la répartition aléatoire des numéros de séquence TCP est désactivée, certaines connexions TCP devront être rétablies car la liaison a été temporairement interrompue pendant le basculement.

Procédure

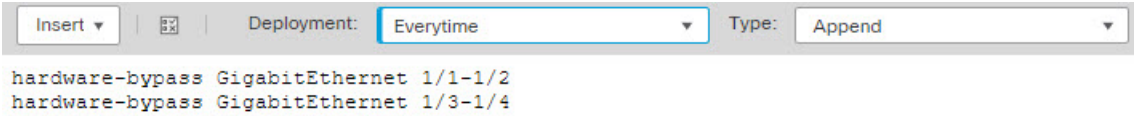
Étape 1 Créez l'objet FlexConfig pour activer le contournement automatique.

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).
b) Choisissez **FlexConfig** > **FlexConfig Object (Objets FlexConfig)** dans la table des matières.
c) Cliquez sur **Add FlexConfig Object** (Ajouter un objet FlexConfig), configurez les propriétés suivantes, puis cliquez sur **Save** (Enregistrer).

- **Name** : nom de l'objet. Par exemple, Enable_HW-Bypass.
- **Deployment** (déploiement) : sélectionnez **Anytime** (à tout moment). Vous souhaitez que cette configuration soit envoyée à chaque déploiement pour qu'il demeure configuré.
- **Type** : conservez la valeur par défaut, **Append** (Ajouter). Les commandes sont envoyées au périphérique après les commandes des fonctionnalités directement prises en charge.
- **Corps de l'objet** dans le corps de l'objet, saisissez les commandes nécessaires pour activer le contournement matériel automatique. Par exemple, les commandes nécessaires pour les deux paires d'interfaces possibles :

```
hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4
```

Le corps de l'objet doit ressembler à ce qui suit :



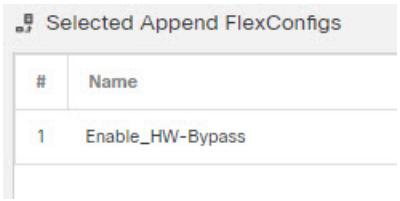
Étape 2 Créez la politique FlexConfig et attribuez-la aux périphériques.

a) Sélectionnez **Devices (Périphériques)** > **FlexConfig**.
b) Cliquez sur **New Policy** (nouvelle politique) ou si une politique FlexConfig existante doit être affectée (ou est déjà affectée) aux périphériques cibles, modifiez simplement cette dernière.

Lors de la création d'une nouvelle politique, affectez les périphériques cibles à la politique dans la boîte de dialogue où vous nommez la politique.

c) Dans la table des matières, sélectionnez l'objet FlexConfig de contournement matériel dans le dossier **défini par l'utilisateur**, puis cliquez sur > pour l'ajouter à la politique.

L'objet doit être ajouté à la liste **Selected Appended FlexConfigs** (FlexConfigs sélectionnées et ajoutées).



d) Cliquez sur **Save** (enregistrer).

e) Si vous n'avez pas encore affecté tous les périphériques ciblés à la politique, cliquez sur le lien **Policy Affectations** (affectations de politiques) ci-dessous Save and make the assignments now (enregistrer et effectuer les affectations maintenant).

f) Cliquez sur **Preview Config** (Aperçu de la configuration et dans la boîte de dialogue d'aperçu, sélectionnez l'un des périphériques attribués.

Le système génère un aperçu de l'interface de ligne de commande de configuration qui sera envoyée au périphérique. Vérifiez que les commandes générées à partir de l'objet FlexConfig de contournement matériel semblent correctes. Celles-ci seront affichées à la fin de l'aperçu. Notez que vous verrez également les commandes générées à partir d'autres modifications que vous avez apportées aux fonctionnalités gérées. Pour les commandes de contournement matériel, vous devriez voir quelque chose qui ressemble à ce qui suit :

```
###Flex-config Appended CLI ###
hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4
```

Étape 3 Déployez vos modifications.

Comme vous avez affecté une politique FlexConfig aux périphériques, vous recevez toujours un avertissement de déploiement destiné à vous mettre en garde contre l'utilisation de FlexConfig. Cliquez sur **Proceed (** continuer) pour poursuivre le déploiement.

Une fois le déploiement terminé, vous pouvez vérifier l'historique de déploiement et afficher la transcription du déploiement. Cela est particulièrement utile si le déploiement échoue. Consultez Vérifier la configuration déployée, à la page 34.

Prochaine étape

Si vous souhaitez appeler manuellement le contournement matériel ou le désactiver manuellement, vous devez créer deux objets FlexConfig :

- Une commande qui démarre manuellement le contournement, qui contiendrait une des commandes suivantes ou les deux, selon que vous souhaitez appeler le contournement pour les deux paires :

```
hardware-bypass manual GigabitEthernet 1/1-1/2
hardware-bypass manual GigabitEthernet 1/3-1/4
```

- Une commande qui désactive manuellement le contournement, qui contient l'une des commandes suivantes ou les deux :

```
no hardware-bypass manual GigabitEthernet 1/1-1/2
no hardware-bypass manual GigabitEthernet 1/3-1/4
```

Vous devrez ensuite ajouter l'un ou l'autre objet à la politique FlexConfig et déployer les modifications pour activer ou désactiver le contournement. Vous devrez également supprimer immédiatement l'objet de la politique FlexConfig après le déploiement. Si vous appelez manuellement le contournement, vous devrez ensuite répéter le processus pour le désactiver à nouveau. Par conséquent, l'utilisation de cette méthode manuelle nécessite des modifications fréquentes et prudentes de la politique FlexConfig et des déploiements supplémentaires.

Migration des politiques FlexConfig

Attention Cette section sur la migration des politiques FlexConfig s'applique uniquement à la migration des politiques ECMP, VXLAN et EIGRP.

Les politiques ECMP, VXLAN et EIGRP ont été configurées à l'aide des objets et des politiques FlexConfig dans les versions antérieures de centre de gestion. Vous pouvez maintenant configurer directement ces politiques dans l'interface utilisateur du centre de gestion. Lorsque vous mettez à niveau le centre de gestion à partir de versions antérieures, la configuration FlexConfig est conservée. Cependant, pour gérer les politiques à partir de l'interface utilisateur, vous devez refaire la configuration dans la page **Périphérique (Modifier)** > **Routage**correspondante et supprimer la configuration de FlexConfig. Pour automatiser la création des politiques dans l'interface utilisateur, centre de gestion offre une option de migration des politiques FlexConfig vers l'interface utilisateur. Cependant, cela ne supprime pas les politiques migrées à partir de de FlexConfig. Pour la procédure de post-migration, consulter Étape 7, à la page 46.

Avant de commencer

- Vérifier que la politique FlexConfig déployée est à jour et non obsolète. L'option de migration ne sera disponible que si la politique est à jour sur au moins un périphérique. La migration n'a pas lieu pour les périphériques dont des politiques obsolètes.
- Si la politique est configurée dans FlexConfig et dans le centre de gestion :
  - La migration ne sera pas lancée si la politique est déjà configurée au niveau du **routage** > **périphérique (modifier)**.
  - Pendant le déploiement, le centre de gestion affiche un message d'erreur. Exemple de message d'erreur de migration EIGRP - *EIGRP est configuré via l'objet FlexConfig et également sous Liste des périphériques -> Routage EIGRP pour le périphérique. Maintenez la configuration du protocole EIGRP dans Routing EIGRP (Routage EIGRP) ou FlexConfig.*
- Si les objets réseau utilisés dans la politique existent dans le centre de gestion, pendant la migration, ils sont réutilisés. Pendant la migration, quand un objet réseau correspondant à la configuration IP n'est pas disponible, un nouvel objet réseau est créé car *bb* est ajouté à un horodatage et un entier, comme ***bb_***<timestamp> _<integer> . Pour plusieurs de ces objets réseau, la variable entière dans le nom serait incrémentée de un.

Procédure

Étape 1 Choisissez **Devices (Périphériques)** > **FlexConfig**, cliquez sur **Edit** ( ) en fonction de la politique FlexConfig que vous souhaitez migrer.

Étape 2 Cliquez sur **Migrer la configuration**.

Remarque Une fois la migration commencée, les options **Migrer la configuration** et **Modifier** FlexConfig ne sont pas disponibles.

L'option de **migration de la configuration** n'est pas disponible dans les cas suivants :

- Il n'y a aucune interface de commande en ligne FlexConfig applicable à migrer.
- La politique FlexConfig n'est associée à aucun objet FlexConfig.
- Aucun périphérique n'est associé à la politique FlexConfig.

Étape 3 Dans la boîte de dialogue **Migrate Flex Configuration** (migrer la configuration Flex), sélectionnez le périphérique vers lequel vous souhaitez migrer la configuration, puis cliquez sur **OK**.

La progression de la migration s'affiche sous forme de notification de tâche. Une fois la migration terminée, cliquez sur le lien *View Details* (afficher les détails) et téléchargez le rapport de migration (format PDF).

Étape 4 Pour afficher les modifications de politique, choisissez **System** > **Monitoring** > **Audit** (audit de surveillance des systèmes), puis cliquez sur le message *Flex Config Migration* (Migration FlexConfig).

Étape 5 Pour afficher le rapport de migration FlexConfig, choisissez **System** > **Monitoring** > **Audit** (audit de surveillance du système) et cliquez sur le message *Flex Config Migration* (Migration FlexConfig). Pour afficher le rapport complet de migration, cliquez sur l'icône **Report** (rapport).

Étape 6 Vérifiez les paramètres de configuration migrés dans la page **Device (Edit) (Périphérique (Modifier))** > **Routing (Routage)** correspondante.

Étape 7 Pour supprimer la configuration de politique spécifique de FlexConfig pour le périphérique, dans le centre de gestion, procédez comme suit :

a) Déterminez la politique FlexConfig migrée pour le périphérique.
b) Utilisez l'option de copie et créez un doublon de la politique FlexConfig.
c) Supprimez les objets CLI correspondants de la politique FlexConfig dupliquée.
d) Associez le périphérique à la politique FlexConfig dupliquée.

Étape 8 Enregistrez et déployez la configuration.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.