Exemple de configuration de Syslog ASA

Contenu

Introduction

Ce document fournit une configuration d'échantillon qui explique comment configurer différentes options se connectantes sur une appliance de sécurité adaptable (ASA) cette version 8.4 ou ultérieures de code de passages.

La version 8.4 ASA a introduit des techniques de filtrage très granulaires afin de permettre seulement certains messages spécifiés de Syslog à présenter. La section Configuration Syslog de base de ce document explique une configuration Syslog traditionnelle. La section avancée de Syslog de ce document affiche les nouvelles caractéristiques de Syslog dans la version 8.4. Référez-vous aux messages du journal système guide d'appareils de sécurité Cisco, des versions 8.x et 9.x pour le guide complet de messages du journal système.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ASA 5515 avec la version de logiciel 8.4 ASA
- Version 7.1.6 du Cisco Adaptive Security Device Manager (ASDM)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

> Remarque: Référez-vous à ASA 8.2 : Configurez le Syslog utilisant le ASDM pour en savoir plus pour les détails semblables de configuration avec la version 7.1 et ultérieures ASDM.

Configuration Syslog de base

> Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Sélectionnez ces commandes afin d'activer se connecter, logs de vue, et paramètres de configuration de vue.

- **logging enable** - Active la transmission des messages de Syslog à tous les emplacements de sortie.
- **aucun logging enable -** Débronchements se connectant à tous les emplacements de sortie.
- **show logging -** Répertorie le contenu de la mémoire tampon de Syslog aussi bien que les

informations et les statistiques qui concernent la configuration en cours.

L'ASA peut envoyer des messages de Syslog à de diverses destinations. Sélectionnez les commandes dans ces sections afin de spécifier les emplacements que vous comme les informations de Syslog seriez envoyé :

Envoyez les informations de journalisation à la mémoire tampon interne

```
logging buffered severity_level
```

Le matériel ou logiciel externe n'est pas exigé quand vous enregistrez les messages de Syslog dans la mémoire tampon interne ASA. Sélectionnez la commande de **show logging** afin de visualiser les messages enregistrés de Syslog. La mémoire tampon interne a une taille maximale de 1 Mo (configurable avec la commande **se connectante de taille de mémoire tampon**). En conséquence, il pourrait s'envelopper très rapidement. Maintenez ceci dans l'esprit quand vous choisissez un niveau se connectant pour la mémoire tampon interne comme des niveaux plus bavards de se connecter pourraient rapidement remplir, et le bouclage, la mémoire tampon interne.

Envoyez les informations de journalisation à un serveur de Syslog

```
logging host interface_name ip_address [tcp[/port] | udp[/port]] [format emblem]
logging trap severity_level
logging facility number
```

Un serveur qui exécute une application Syslog est requis afin d'envoyer des messages Syslog à un hôte externe. L'ASA envoie le Syslog sur le port UDP 514 par défaut, mais le protocole et le port peuvent être choisis. Si le TCP est choisi comme protocole se connectant, ceci fait envoyer l'ASA des Syslog par l'intermédiaire d'une connexion TCP au serveur de Syslog. Si le serveur est inaccessible, ou la connexion TCP au serveur ne peut pas être établie, l'ASA, par défaut, bloquera TOUTES LES nouvelles connexions. Ce comportement peut être désactivé si vous activez **se connecter l'autorisation-hostdown**. Voyez le guide de configuration pour plus d'informations sur la commande **se connectante d'autorisation-hostdown**.

Envoyez les informations de journalisation comme courriers électroniques

```
logging mail severity_level
logging recipient-address email_address
logging from-address email_address
smtp-server ip_address
```

Un serveur SMTP est requis quand vous envoyez les messages Syslog dans les messages électroniques. La configuration correcte sur le serveur SMTP est nécessaire afin de s'assurer que vous pouvez avec succès transmettre par relais des courriers électroniques de l'ASA au client de courrier électronique spécifié. Si ce niveau se connectant est placé à un niveau très bavard, comme *mettez au point* ou *informationnel,* vous pourriez générer un nombre important de Syslog puisque chaque courrier électronique envoyé par cette configuration de journalisation entraîne vers le haut des logs quatre ou plus supplémentaires à générer.

Envoyez les informations de journalisation à la console série

```
logging console severity_level
```

La journalisation console permet à des messages de Syslog d'afficher sur la console ASA (téléscripteur) comme ils se produisent. Si la journalisation console est configurée, toute se connecte la génération sur l'ASA ratelimited à 9800 bps, la vitesse de la console série ASA. Ceci pourrait causer des Syslog d'être relâché à toutes les destinations, qui incluent la mémoire tampon interne. N'utilisez pas la journalisation console pour des Syslog bavards pour cette raison.

Envoyez les informations de journalisation à une session Telnet/SSH

```
logging monitor severity_level
terminal monitor
```

Se connecter le moniteur permet à des messages de Syslog d'afficher pendant qu'ils se produisent quand vous accédez à la console ASA avec le telnet ou le SSH et la commande terminal monitor est exécuté de cette session. Afin d'arrêter l'impression des logs à votre session, ne sélectionnez l'**aucune** commande de **terminal monitor**.

Messages de log d'affichage sur l'ASDM

```
logging asdm severity_level
```

ASDM a également une mémoire tampon qui peut être utilisée pour enregistrer les messages Syslog. Sélectionnez la commande d'**asdm de show logging** afin d'afficher le contenu de la mémoire tampon de Syslog ASDM.

Envoyez les logs à une station de gestion SNMP

```
logging history severity_level
snmp-server host [if_name] ip_addr
snmp-server location text
snmp-server contact text
snmp-server community key
snmp-server enable traps
```

Les utilisateurs ont besoin d'un environnement fonctionnel existant de Protocole SNMP (Simple Network Management Protocol) afin d'envoyer des messages de Syslog avec le SNMP. Voir les commandes pour placer et gérer des destinations de sortie pour une référence complète sur les commandes que vous pouvez employer pour placer et gérer des destinations de sortie. Voir les messages répertoriés par le niveau d'importance pour des messages répertoriés par le niveau d'importance.

Ajoutez les horodateurs aux Syslog

Afin d'aider à aligner et des événements de commande, des horodateurs peuvent être ajoutés aux Syslog. Ceci est recommandé afin d'aider à tracer des questions basées sur le temps. Afin d'activer des horodateurs, sélectionnez la commande de **logging timestamp**. Voici deux exemples de Syslog, un sans horodateur et un avec :

```
logging history severity_level
snmp-server host [if_name] ip_addr
snmp-server location text
snmp-server contact text
snmp-server community key
snmp-server enable traps
```

Exemple 1

Cette sortie affiche une configuration d'échantillon pour se connecter dans la **mémoire tampon** avec le niveau d'importance de l'**élimination des imperfections**.

```
logging enable
logging buffered debugging
```

Voici un exemple de sortie.

```
logging enable
logging buffered debugging
```

Configurez le Syslog de base avec l'ASDM

Cette procédure explique la configuration ASDM pour toutes les destinations disponibles de Syslog.

1. Afin d'activer ouvrir une session l'ASA, configurez d'abord les paramètres se connectants de base. Choisissez **Configuration > Features > Properties > Logging > Logging Setup**. Cochez l'**enable se connectant la** case afin d'activer des Syslog.
2. Afin de configurer un serveur externe comme destination pour des Syslog, choisir des **serveurs de Syslog** en se connectant et cliquer sur Add afin d'ajouter un serveur de Syslog. Saisissez les détails du serveur syslog dans la zone Add Syslog Server (Ajouter un serveur Syslog) et choisissez **OK** lorsque vous avez terminé.
3. Choisissez l'**installation de courrier électronique** dans la commande logging on pour envoyer des messages de Syslog comme courriers électroniques aux destinataires spécifiques. Précisez l'adresse électronique source dans la zone de l'adresse électronique source et choisissez **Add** afin de configurer l'adresse électronique de destination des destinataires des messages électroniques et le niveau de gravité du message. Cliquez sur **OK** quand vous avez terminé.
4. Choisissez la **gestion de périphérique**, **se connectant,** choisissez le **SMTP**, et entrez dans l'adresse IP du serveur primaire afin de spécifier l'adresse IP de serveur SMTP.
5. Si vous voulez envoyer des Syslog comme déroutements SNMP, vous devez d'abord définir un serveur SNMP. Choisissez le **SNMP** dedans dans le menu d'**Access de Gestion** afin de spécifier l'adresse des stations de gestion SNMP et de leurs propriétés spécifiques.
6. Choisissez **Add** afin d'ajouter une station de gestion SNMP. Saisissez les détails de l'hôte SNMP et cliquez sur **OK**.
7. Afin de permettre à des logs d'être envoyé aux destinations mentionnées antérieures l'unes des, choisissez le **Logging Filters** dans la section se connectante. Ceci vous présente avec chaque destination de journalisation possible et le niveau actuel des logs qui sont envoyés à ces destinations. Choisissez la destination de journalisation souhaitée et cliquez sur **Edit**. Dans cet exemple, « la destination des serveurs de Syslog est modifiée.
8. Choisissez une sévérité appropriée, dans ce cas **informationnelle, du filtre sur la** liste déroulante de **sévérité**. Cliquez sur **OK** quand vous avez terminé.
9. Cliquez sur **Apply** après être revenu à la fenêtre des filtres de journalisation.

Envoi de messages Syslog par un VPN à un serveur Syslog

Dans la conception simple du site à site VPN ou la conception plus compliquée d'en étoile,

l'administrateur pourrait vouloir surveiller tous les Pare-feu du distant ASA avec le serveur SNMP et le serveur de Syslog situés à un lieu d'exploitation principal.

Afin de configurer la configuration du VPN d'IPsec de site à site, référez-vous à PIX/ASA 7.x et en haut : PIX--PIX À l'exemple de configuration de tunnel VPN. Indépendamment de la configuration VPN, vous devez configurer le SNMP et le trafic intéressant pour le serveur syslog dans le site central et le site local.

Configuration centrale ASA

```
!--- This access control list (ACL) defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two ASA.
!--- It also includes the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind the ASA 5515.

access-list 101 permit ip 172.22.1.0 255.255.255.0 172.16.1.0 255.255.255.0

!--- This lines covers SNMP (TCP/UDP port - 161), SNMP TRAPS(TCP/UDP port - 162)
!--- and syslog traffic (UDP port - 514) from SNMP/syslog server
!--- to the outside interface of the remote ASA.

access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 161
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 161
access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 162
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 162
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 514


logging enable
logging trap debugging

!--- Define logging host information.
logging facility 16
logging host inside 172.22.1.5

!--- Define the SNMP configuration.
snmp-server host inside 172.22.1.5 community ***** version 2c
snmp-server community *****
```

Configuration distante ASA

```
!--- This ACL defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two ASA.
!--- It also covers the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind ASA 5515.
access-list 101 permit ip 172.16.1.0 255.255.255.0 172.22.1.0 255.255.255.0

!--- This lines covers SNMP (TCP/UDP port - 161), SNMP TRAPS (TCP/UDP port - 162) and
!--- syslog traffic (UDP port - 514) sent from this ASA outside
!--- interface to the SYSLOG server.
access-list 101 permit tcp host 10.20.20.1 host 172.22.1.5 eq 161
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 161
access-list 101 permit tcp host 10.20.20.1 host 172.22.1.5 eq 162
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 162
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 514

!--- Define syslog server.
```

```
logging facility 23
logging host outside 172.22.1.5

!--- Define SNMP server.
snmp-server host outside 172.22.1.5 community ***** version 2c
snmp-server community *****
```

Référez-vous à surveiller le Pare-feu Cisco Secure ASA utilisant le SNMP et le Syslog par le tunnel VPN pour plus d'informations sur la façon configurer la version 8.4 ASA

Configuration Syslog avancée

La version 8.4 ASA fournit plusieurs mécanismes qui te permettent de configurer et gérer des messages de Syslog dans les groupes. Ces mécanismes incluent le niveau de gravité du message, la catégorie du message, l'ID du message ou une liste de messages personnalisée que vous créez. Avec l'utilisation de ces mécanismes, vous pouvez saisir une commande unique qui s'applique à de petits ou grands groupes de messages. Quand vous configurez Syslog de cette façon, vous pouvez capturer les messages du groupe de message spécifié, non plus tous messages de la même gravité.

Utilisation de la liste de messages

Utilisez la liste de messages afin d'inclure seulement les messages syslog intéressés par le niveau de gravité et l'ID dans un groupe, puis associez cette liste de messages à la destination souhaitée.

Terminez-vous ces étapes afin de configurer une liste de messages :

1. Saisissez la commande **logging list message_list /** level severity_level [class message_class] afin de créer une liste de messages qui inclut des messages avec un niveau de gravité ou une liste de messages spécifiés.
2. Saisissez la commande **logging list message_list message syslog_id-syslog_id2** afin d'ajouter des messages supplémentaires à la liste de messages que vous venez de créer.
3. Saisissez la commande **logging destination message_list** afin de préciser la destination de la liste de messages créée.

Exemple 2

Sélectionnez ces commandes afin de créer une liste de messages, qui inclut toute la sévérité 2 messages (essentiels) en plus du message 611101 611323, et ayez-également les envoyées à la console :

```
logging list my_critical_messages level 2
logging list my_critical_messages message 611101-611323
logging console my_critical_messages
```

Configuration ASDM

Cette procédure montre une configuration ASDM pour l'exemple 2 avec l'utilisation de la liste de messages.

1. Choisissez **Event Lists** sous Logging et cliquez sur **Add** afin de créer une liste de messages.
2. Saisissez le nom de la liste de messages dans la zone du nom. Dans cet exemple, **my_critical_messages** est utilisé. Cliquez sur **Add** sous Event Class/Severity Filters.
3. Choisissez **tous de la** liste déroulante de classe d'événement. Choisissez **essentiel de la** liste déroulante de sévérité. Cliquez sur **OK** quand vous avez terminé.
4. Cliquez sur **Add** sous les filtres d'ID de message si des messages supplémentaires sont requis. Dans cet exemple, vous devez inclure les messages avec les ID 611101 à 611323.
5. Indiquez la plage d'ID dans la case des ID de message et cliquez sur **OK**.
6. Retournez au menu **Logging Filters** et choisissez **Console** comme destination.
7. Choisissez les **my_critical_messages de la** liste déroulante de **liste d'événements d'utilisation**. Cliquez sur **OK** quand vous avez terminé.
8. Cliquez sur **Apply** après être revenu à la fenêtre des filtres de journalisation.

Ceci se termine les configurations ASDM avec l'utilisation d'une liste de messages suivant les indications de l'exemple 2.

Utilisation de la catégorie de message

Utilisez la catégorie de message afin d'envoyer tous les messages liés à une catégorie à l'emplacement de sortie indiqué. Quand vous précisez un seuil de niveau de gravité, vous pouvez limiter le nombre de messages envoyés à l'emplacement de sortie.

```
logging class message_class destination | severity_level
```

Exemple 3

Saisissez cette commande afin d'envoyer tous les messages de la catégorie ca avec un niveau de gravité urgent ou supérieur vers la console.

```
logging class ca console emergencies
```

Configuration ASDM

Cette procédure affiche les configurations ASDM par exemple 3 avec l'utilisation de la liste de messages.

1. Choisissez le menu **Logging Filters** et choisissez **Console** comme destination.
2. Cliquez sur **Disable logging from all event classes**.
3. Sous les Syslog des catégories d'événement spécifiques, choisissez la catégorie d'événement et la gravité que vous souhaitez ajouter.Cette procédure utilise **ca** et **Emergencies** respectivement.
4. Cliquez sur **Add** afin d'ajouter cela dans la catégorie de message et cliquez sur **OK**.
5. Cliquez sur **Apply** après être revenu à la fenêtre des filtres de journalisation. La console collecte maintenant le message de classe Ca avec des urgences de niveau d'importance comme affiché sur la fenêtre de Logging Filters.

Ceci se termine la configuration par exemple 3. ASDM se rapportent à des messages répertoriés par le niveau d'importance pour une liste des niveaux de gravité du message de log.

Envoyez les messages de log de debug à un serveur de Syslog

Pour le dépannage avancé, la particularité de caractéristique/protocole mettent au point des logs sont exigées. Par défaut, ces messages de log sont affichés sur le terminal (SSH/Telnet). La personne à charge sur le type de mettent au point, et le débit de messages de débogage générés, utilisation du CLI pourrait s'avérer que difficile si met au point sont activés. Sur option, des messages de débogage peuvent être réorientés au processus de Syslog et être générés comme Syslog. Ces Syslog peuvent être envoyés à n'importe quelle destination de Syslog comme n'importe quel autre Syslog. Afin de détourner met au point aux Syslog, sélectionnent la commande **se connectante de debug-suivi**. Cette configuration envoie la sortie de débogage, comme Syslog, à un serveur de Syslog.

```
logging class ca console emergencies
```

Utilisation de se connecter des classes de liste et de message ensemble

Sélectionnez la commande **se connectante de liste** afin de capturer le Syslog pour seuls des messages d'IPsec VPN d'entre réseaux locaux et d'Accès à distance. Cet exemple capture tous les messages du journal système de la catégorie VPN (IKE et IPsec) avec le niveau de débogage ou supérieur.

Exemple

```
hostname(config)#logging enable
hostname(config)#logging timestamp
hostname(config)#logging list my-list level debugging class vpn
hostname(config)#logging trap my-list
hostname(config)#logging host inside 192.168.1.1
```

Hit d'ACL de log

Ajoutez le *log à* chaque élément de liste d'accès (ACE) que vous souhaitez afin de se connecter quand une liste d'accès est frappée. Utilisez cette syntaxe :

```
access-list id {deny | permit protocol} {source_addr source_mask}
{destination_addr destination_mask} {operator port} {log}
```

Exemple

```
ASAfirewall(config)#access-list 101 line 1 extended permit icmp any any log
```

ACLs, par défaut, log chaque paquet refusé. Il n'y a aucun besoin d'ajouter l'option de log **de refuser** ACLs pour générer des Syslog pour les paquets refusés. Quand l'option **log** est précisée, elle génère le message syslog 106100 pour l'ACE auquel elle est appliquée. Le message `106100 de` Syslog est généré pour chaque autorisation assortie ou refuse l'écoulement d'ACE qui traverse le Pare-feu ASA. Le flux de la première correspondance est mis en cache. Les correspondances ultérieures incrémentent le nombre d'occurrences affiché dans la commande **show access-list**. Le comportement de journalisation de liste d'accès par défaut, qui est le **mot-clé de journal** non spécifié, est que si un paquet est refusé, alors le message 106023 est généré, et si le paquet est autorisé, alors aucun message syslog n'est généré.

Un niveau Syslog facultatif (0 - 7) peut être indiqué pour les messages syslog générés (106100). Si aucun niveau n'est précisé, le niveau par défaut est 6 (informatif) pour un nouvel ACE. Si ACE existe déjà, alors son niveau en cours de log demeure sans changement. Si l'option **log disable** est spécifiée, la journalisation de la liste d'accès est complètement désactivée. Aucun message

syslog, notamment le message 106023, n'est généré. L'option par défaut **log** restaure le comportement de journalisation de liste d'accès par défaut.

Réalisez ces étapes afin de permettre au message syslog 106100 de s'afficher dans la sortie de la console :

1. Sélectionnez la commande de **logging enable** afin d'activer la transmission des messages du journal système à tous les emplacements de sortie. Vous devez définir un emplacement de sortie de journalisation afin d'afficher tout journal.
2. Sélectionnez la commande de *<severity_level> de* **niveau de** *<message_number> de* **message de journalisation** afin de placer le niveau d'importance d'un message du journal système spécifique.Dans ce cas, sélectionnez la commande du **message de journalisation 106100** afin d'activer le message `106100`.
3. Entrez dans le **message_list de logging console | severity_level** afin de permettre aux messages du journal système de s'afficher sur la console d'appliance de sécurité (TTY) à mesure qu'ils se produisent. Réglez le severity_level entre 1 et 7, ou utilisez le nom du niveau. Vous pouvez également préciser quels messages sont envoyés avec la variable message_list.
4. Sélectionnez la commande de **message de show logging** afin d'afficher une liste de messages de message du journal système qui ont été modifiés de la valeur par défaut, qui sont des messages qui ont été assignés un niveau d'importance différent et les messages qui ont été désactivés.Voici un exemple de sortie de la commande **show logging message** :`ASAfirewall#`**`show logging message 106100`**
```
syslog 106100: default-level informational (enabled)
ASAfirewall# %ASA-7-111009: User 'enable_15' executed cmd: show logging mess 106
100
```

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Si vous voulez supprimer un message spécifique de Syslog à envoyer au serveur de Syslog, alors vous devez sélectionner la commande comme affichée.

`hostname(config)#`**`no logging message`** *`<syslog_id>`*
Consultez ce document sur la commande logging message pour obtenir plus d'informations.

%ASA-3-201008 : Disallowing new connections

Le message d'erreur %ASA-3-201008: `Disallowing new connections.` le message d'erreur est vu quand une ASA ne peut pas contacter le serveur de Syslog et aucune nouvelle connexion n'est permise.

Solution

Ce message apparaît quand vous avez activé les messages du journal système de TCP et le serveur syslog ne peut pas être atteint, ou quand vous utilisez le serveur syslog Cisco ASA (PFSS) et que le disque du système Windows NT est plein. Procédez comme suit pour résoudre ce message d'erreur :

- Désactivez les messages du journal système de TCP s'ils sont activés.
- Si vous utilisez PFSS, libérez de l'espace sur le système Windows NT où PFSS réside.
- Assurez-vous que le serveur de Syslog est haut et vous peut cingler l'hôte de la console de Cisco ASA.
- Redémarrez la journalisation de messages système de TCP pour autoriser le trafic.

Si le serveur de Syslog descend et se connecter de TCP est configuré, utilisez la commande se connectante d'autorisation-hostdown ou commutez à se connecter d'UDP.

Informations connexes

- Logiciel pare-feu de Cisco ASA
- Références des commandes du pare-feu Cisco Secure PIX
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems