Comment automatisez-vous des transferts de log ?

Contenu

Question

Comment automatisez-vous des transferts de log ?

Environnement

Appliance de sécurité du courrier électronique de Cisco (ESA), appliance de sécurité Web (WSA), appliance de Gestion de la sécurité (SMA), et toutes les versions d'AsyncOS.

Beaucoup de différents types de logs sont créés sur les dispositifs de sécurité. Vous pouvez souhaiter faire virer l'appliance automatiquement certains logs sur un autre serveur.

Cette installation peut être faite par l'intermédiaire du GUI ou du CLI utilisant les protocoles de FTP ou SCP. Veuillez lire les particularités ci-dessous :

GUI

1. Allez à l'**administration système - > des abonnements de log**.
2. Cliquez sur le nom de log du log que vous souhaitez modifier sous le champ « de nom de log ».
3. Sous la « méthode de récupération », vous pouvez sélectionner le « FTP sur le serveur distant » ou le « SCP sur le serveur distant ».
4. Écrivez les valeurs correctes dans le scénario approprié que vous choisissez. Si vous n'êtes pas au courant des valeurs correctes, entrez en contact avec s'il vous plaît vos systèmes/administrateur réseau comme ils peuvent vous aider à déterminer quels serveurs sont disponibles dans votre réseau.

CLI (interface de ligne de commande)

Voyez l'ordre suivant CLI :

```
S-Series> logconfig
[]> edit
[]> <appropriate number correlating to the log you wish to modify>

Please enter the name for the log:
[Log_name]> <enter for default>

Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace

[3]> <enter for the default>

Choose the method to retrieve the logs.
1. FTP Poll
2. FTP Push
3. SCP Push
```

Choisissez la méthode que vous désirez installer. De ce point, le CLI marchera vous par les mêmes paramètres de connexion qui sont disponibles dans le GUI.

Ceux-ci sont comme suit :

FTP

- Intervalle de temps maximum entre transférer : 3600 secondes
- Hôte de FTP : Nom d'hôte/adresse IP du ftp server
- Répertoire : Répertoire distant sur le ftp server (relativement à la connexion de FTP. En général « /")
- Nom d'utilisateur : Nom d'utilisateur de FTP
- Mot de passe : Mot de passe FTP

SCP

- Intervalle de temps maximum entre transférer : 3600 secondes
- Protocol : SSH1 ou SSH2
- Hôte SCP : Nom d'hôte/adresse IP du serveur SCP
- Répertoire : Répertoire distant sur le serveur SCP (relativement à la connexion SCP. En général « /")
- Nom d'utilisateur : Nom d'utilisateur SCP
- Vérifier de clé de hôte d'enable
- Automatiquement balayage
- Entrez manuellement

REMARQUE: Le FTP est un protocole de texte brut, signifiant que les données sensibles peuvent être accessibles en lecture par quelqu'un qui renifle le trafic réseau. Le SCP est un protocole chiffré, de ce fait rendant le reniflement inefficace aux données pillantes. Si les données sont sensibles et la Sécurité est un souci, l'il est recommandé que SCP soit utilisé au lieu du FTP.