Configurez un ESA pour les mises à jour de présentation

Contenu

Introduction

Ce document décrit le processus pour de bêtas clients, et les appliances preprovisioned utilisées pour le test, qui doit être les mises à jour configurées de traction d'utiliser-et des serveurs de mise à jour de mise en place pour l'appliance de sécurité du courrier électronique de Cisco (ESA) et l'appliance de Gestion de la sécurité (SMA). Maintenez dans l'esprit, les serveurs de mise en place ne doivent pas être utilisés par des clients de production en série pour la production ESA ou SMA.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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.

Configurez

Remarque: Les clients devraient être seulement utilisation le serveur URLs de mise à jour de mise en place s'ils ont accédé à preprovisioning par Cisco pour la bêta utilisation seulement. Si vous n'avez pas un permis valide appliqué pour le bêta usage, votre appliance ne recevra pas des mises à jour des serveurs de mise à jour de mise en place. Ces instructions devraient seulement être utilisées pour de bêtas clients ou par les administrateurs qui participent aux essais pilotes.

Afin de recevoir des mises à jour de mise en place :

GUI

1. Choisissez les **Services de sécurité > les mises à jour de services > éditent des configurations de mise à jour…**
2. Confirmez que tous les services sont configurés pour utiliser des serveurs de mise à jour d'IronPort Cisco.

CLI

1. Écrivez l'**updateconfig de** commande.
2. Écrivez le **dynamichost** masqué de commande secondaire.
3. Sélectionnez une de ces commandes : Pour le matériel ESA/SMA : **stage-update-manifests.ironport.com:443**Pour ESA/SMA virtuel : **stage-stg-updates.ironport.com:443**
4. La presse entrent jusqu'à ce que vous soyez retourné à l'invite principale.
5. Entrez dans la **validation** afin de sauvegarder toutes les modifications.

Vérifiez

La vérification peut être vue dans les *updater_logs* avec la transmission réussissant pour l'URL approprié d'étape. Du CLI sur l'appliance, écrivez les **updater_logs d'étape de grep** :

```
9.9.5-033.local (SERVICE)>  grep stage updater_logs

Wed Mar 16 18:16:17 2016 Info: internal_cert beginning download of remote file "http://stage-
updates.ironport.com/internal_cert/1.0.0/internal_ca.pem/default/100101"
Wed Mar 16 18:16:17 2016 Info: content_scanner beginning download of remote file "http://stage-
updates.ironport.com/content_scanner/1.1/content_scanner/default/1132001"
Wed Mar 16 18:16:17 2016 Info: enrollment_client beginning download of remote file
"http://stage-updates.ironport.com/enrollment_client/1.0/enrollment_client/default/102057"
Wed Mar 16 18:16:18 2016 Info: support_request beginning download of remote file "http://stage-
updates.ironport.com/support_request/1.0/support_request/default/100002"
Wed Mar 16 18:16:18 2016 Info: timezones beginning download of remote file "http://stage-
updates.ironport.com/timezones/2.0/zoneinfo/default/2015100"
Wed Mar 16 18:26:19 2016 Info: repeng beginning download of remote file "http://stage-
updates.ironport.com/repeng/1.2/repeng_tools/default/1392120079"
```

S'il y a des erreurs de communication inattendues, entrez dans l'**URL> de <stage de fouille** afin de vérifier le Domain Name Server (DN).

```
9.9.5-033.local (SERVICE)>  dig stage-updates.ironport.com


; <<>> DiG 9.8.4-P2 <<>> stage-updates.ironport.com A
;; global options: +cmd
```

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52577
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;stage-updates.ironport.com. IN A

;; ANSWER SECTION:
stage-updates.ironport.com. 275 IN A 208.90.58.21

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Mar 22 14:31:10 2016
;; MSG SIZE rcvd: 60
```

Afin de vérifier l'appliance peut au telnet au-dessus du port 80, sélectionnent la commande de l'**URL> 80 de <stage de telnet**.

```
9.9.5-033.local (SERVICE)>  telnet stage-updates.ironport.com 80

Trying 208.90.58.21...
Connected to origin-stage-updates.ironport.com.
Escape character is '^]'.
```

Retournez

Afin de revenir aux serveurs de mise à jour de production en série, terminez-vous ces étapes :

1. Écrivez l'**updateconfig de** commande.
2. Écrivez le **dynamichost** masqué de commande secondaire.
3. Sélectionnez une de ces commandes : Pour le matériel ESA/SMA : **update-manifests.ironport.com:443**Pour ESA/SMA virtuel : **update-manifests.sco.cisco.com:443**
4. La presse entrent jusqu'à ce que vous soyez retourné à l'invite principale.
5. Exécutez la **validation** afin de sauvegarder toutes les modifications.

   Remarque: Les appliances de matériel (C1x0, C3x0, C6x0, et X10x0) devraient SEULEMENT utiliser l'hôte dynamique URLs de *stage-update-manifests.ironport.com:443* ou d'*update-manifests.ironport.com:443*. S'il y a une configuration du cluster avec l'ESA et le vESA, l'**updateconfig** doit être configuré au niveau d'ordinateur et confirmer que le **dynamichost** est alors placé en conséquence.

Filtrage des URL

Si le Filtrage URL est configuré et en service sur l'appliance, une fois qu'une appliance a été réorientée pour utiliser l'URL d'étape pour des mises à jour, l'appliance devra également être configurée pour utiliser le serveur de mise en place pour le Filtrage URL :

1. Accédez à l'appliance par l'intermédiaire du CLI
2. Écrivez le **websecurityadvancedconfig de** commande.
   L'étape par la configuration et changent la valeur pour l'option *entrent dans l'adresse Internet de service de sécurité Web* à : **v2.beta.sds.cisco.com**
3. Changez la valeur pour l'option écrivent la valeur seuil pour les demandes en attente à : **5.** (le par défaut est 50.)
4. Recevez les par défaut pour toutes autres options.
5. La presse entrent jusqu'à ce que vous soyez retourné à l'invite principale.

6. Entrez dans la **validation** afin de sauvegarder toutes les modifications.

Cheminement d'interaction de Web

Si le cheminement d'interaction de Web est configuré et en service sur l'appliance, une fois qu'une appliance a été réorientée pour utiliser l'URL d'étape pour des mises à jour, l'appliance devra également être configurée pour utiliser le serveur d'agrégateur de mise en place :

1. Accédez à l'appliance par l'intermédiaire du CLI
2. Écrivez l'**aggregatorconfig de** commande.
3. Utilisez la commande d'ÉDITER et écrivez cette valeur : **stage.aggregator.sco.cisco.com**
4. La presse entrent jusqu'à ce que vous soyez retourné à l'invite principale.
5. Exécutez la **validation** afin de sauvegarder toutes les modifications.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- le vESA ne peut pas télécharger et appliquer des mises à jour pour le courrier indésirable ou l'antivirus
- Support et documentation techniques - Cisco Systems