IPS 5.x et version ultérieure : Exemple de configuration NTP sur IPS

Contenu

Introduction

Ce document fournit à une configuration d'échantillon pour synchroniser l'horloge Cisco Secure de Système de prévention d'intrusion (IPS) un Serveur de synchronisation de réseau utilisant le Protocole NTP (Network Time Protocol). Le routeur de Cisco est configuré pendant qu'un serveur de NTP et le capteur IPS est configuré pour utiliser le serveur de NTP (routeur de Cisco) comme source temporelle.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Le serveur de NTP doit être accessible du capteur de Cisco IPS avant que vous commenciez cette configuration de NTP.

Composants utilisés

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

- Périphérique IPS de gamme Cisco 4200 qui exécute la version de logiciel 7.0 et plus tard
- Version 7.0.1 et ultérieures du Cisco IPS Manager Express (IME)**Remarque:** Tandis qu'IME

peut être utilisé pour surveiller les périphériques de capteur qui exécutent le Cisco IPS 5.0 et plus tard, certaines des nouvelles fonctionnalités et caractéristiques fournies dans IME sont seulement prises en charge sur les capteurs qui exécutent le Cisco IPS 6.1 ou plus tard.

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.

Produits connexes

Vous pouvez également utiliser ce document avec des ces matériel et versions de logiciel :

- Périphérique IPS de gamme Cisco 4200 qui exécute les versions de logiciel 6.0 et plus tôt
- Version 6.1.1 du Cisco IPS Manager Express (IME)

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configuration

Configurez un routeur de Cisco pour être un serveur de NTP

Le capteur exige une connexion authentifiée avec un serveur de NTP s'il va utiliser le serveur de NTP comme source temporelle. Le capteur prend en charge seulement l'algorithme de hachage de MD5 pour le chiffrement à clé. Employez la procédure suivante pour lancer un routeur de Cisco pour agir en tant que serveur de NTP et pour utiliser son horloge interne comme source temporelle.

Terminez-vous ces étapes pour installer un routeur de Cisco pour agir en tant que serveur de NTP :

1. Procédure de connexion au routeur.
2. Écrivez le mode de configuration.`router#` **`configure terminal`**
3. Créez la valeur d'ID de clé et principale.`router(config)#` **`ntp authentication-key key_ID md5 key_value`** L'ID de clé peut être un nombre entre 1 et 65535. La valeur principale est texte (numérique ou caractère). Il est chiffré plus tard. Exemple :`router(config)#` **`ntp authentication-key 12345 md5 123`** **Remarque:** Le capteur prend en charge seulement des clés de MD5. Les clés pourraient déjà exister sur le routeur. Utilisez la commande de **configuration en cours d'exposition** de vérifier d'autres clés. Vous pouvez utiliser ces valeurs pour la clé de confiance dans l'étape 4.
4. Indiquez la clé que vous avez juste créée dans l'étape 3 comme la clé de confiance (ou utilisez une clé existante).`router(config)#` **`ntp trusted-key key_ID`** L'ID de clé de confiance est le même nombre que l'ID de clé dans l'étape 3. par exemple :`router(config)#` **`ntp trusted-key 12345`**
5. Spécifiez l'interface sur le routeur avec lequel le capteur communiquera.`router(config)#` **`ntp source interface_name`** Exemple :`router(config)#` **`ntp source FastEthernet 1/0`**

6. Spécifiez le nombre de strate de ntp master à assigner au capteur comme affiché ici :`router(config)#` **`ntp master stratum_number`** Exemple :`router(config)#` **`ntp master 6`**
   Remarque: Le nombre de strate de ntp master identifie la position relative du serveur dans la hiérarchie de NTP. Vous pouvez choisir un nombre entre 1 et 15. Il n'est pas important pour le capteur qui vous numérotent choisissent.

Configurez le capteur pour utiliser une source temporelle de NTP

Terminez-vous les étapes dans cette section afin de configurer le capteur pour utiliser la source temporelle de NTP (le routeur de Cisco est la source temporelle de NTP dans cet exemple).

Le capteur exige une source temporelle cohérente. Il est recommandé pour utiliser un serveur de NTP. Employez la procédure suivante pour configurer le capteur pour utiliser le serveur de NTP en tant que sa source temporelle. Vous pouvez utiliser le NTP authentifié ou Unauthenticated.

Remarque: Pour le NTP Authenticated, vous devez obtenir l'ID d'adresse IP du serveur de NTP, de clé de serveur de NTP, et la valeur principale du serveur de NTP.

Terminez-vous ces étapes afin de configurer le capteur pour utiliser un serveur de NTP en tant que sa source temporelle :

1. Ouvrez une session au CLI utilisant un compte avec des privilèges d'administrateur.
2. Écrivez le mode de configuration comme affiché ici :`sensor#` **`configure terminal`**
3. Entrez le mode d'hôte de service.`sensor(config)# service host`
4. Le NTP peut être configuré en tant que NTP authentifié et Unauthenticated.Terminez-vous ces étapes afin de configurer le NTP Unauthenticated :Écrivez le mode de configuration de NTP.`sensor(config-hos)#` **`ntp-option enabled-ntp-unauthenticated`** Spécifiez l'adresse IP du serveur de NTP.`sensor(config-hos-ena)#` **`ntp-server ip_address`** Dans cet exemple l'adresse IP du serveur de NTP est 10.1.1.1.`sensor(config-hos-ena)#` **`ntp-server 10.1.1.1`** C'est la procédure pour configurer le NTP Unauthenticated utilisant le Cisco IPS Manager Express :Choisissez la **configuration > le Corp.-IPS > le capteur installé > temps**. Puis, cliquez sur la case d'option à côté du **NTP Unauthenticated** après que vous fournissiez l'adresse IP du serveur de NTP suivant les indications du tir d'écran.Cliquez sur **Apply**.Ceci se termine la configuration Unauthenticated de NTP.Terminez-vous ces étapes afin de configurer le NTP authentifié :Écrivez le mode de configuration de NTP.`sensor(config-hos)#` **`ntp-option enable`** Spécifiez l'adresse IP du serveur et l'ID de clé de NTP. L'ID de clé est un nombre entre 1 et 65535. C'est l'ID de clé ce vous a déjà installé sur le serveur de NTP.`sensor(config-hos-ena)#` **`ntp-servers ip_address key-id key_ID`** Dans cet exemple l'adresse IP du serveur de NTP est 10.1.1.1.`sensor(config-hos-ena)#` **`ntp-server 10.1.1.1 key-id 12345`** Spécifiez le serveur de NTP de valeur principale.`sensor(config-hos-ena)#` **`ntp-keys key_ID md5-key key_value`** La valeur principale est texte (numérique ou caractère). C'est la valeur principale cette vous a déjà installé sur le serveur de NTP. Exemple :`sensor(config-hos-ena)#` **`ntp-keys 12345 md5-key 123`** C'est la procédure pour configurer le NTP authentifié utilisant le Cisco IPS Manager Express :Choisissez la **configuration > le Corp.-IPS > le capteur installé > temps**. Puis, cliquez sur la case d'option à côté du **NTP authentifié** après que vous fournissiez l'adresse IP du serveur de NTP suivant les indications du tir d'écran.Fournissez la clé et l'ID de clé qui doivent être identique que mentionnés dans le serveur de NTP.Dans cet exemple la clé est 123 et l'ID de clé est 12345.Cliquez sur **Apply**.Ceci se termine la configuration authentifiée de NTP.
5. Annulez le mode de configuration de NTP.`sensor(config-hos-ena)# exit`

```
sensor(config-hos)# exit

Apply Changes:?[yes]
```

6. Appuyez sur **entrent** pour appliquer les modifications ou pour entrer **non** pour les jeter.Ceci se termine la tâche de configuration.

Vérifiez

Cette section fournit des informations qui vous permettront de vérifier que votre configuration fonctionne correctement.

Vérifiez les configurations authentifiées de NTP. Ceci veille que la configuration authentifiée de NTP est faite correctement.

```
sensor(config-hos-ena)#show settings enabled ----------------------------------------------
ntp-keys (min: 1, max: 1, current: 1) ---------------------------------------------- key-id:
12345 ---------------------------------------------- md5-key: 123 ----------------------------
----------------- ---------------------------------------------- ntp-servers (min: 1, max: 1,
current: 1) ---------------------------------------------- ip-address: 10.1.1.1 key-id: 12345 -
------------------------------------------- ----------------------------------------------
sensor(config-hos-ena)#
```

Afin d'afficher le contenu de la configuration contenue dans le sous-mode en cours, utilisez les configurations d'exposition commandent dans n'importe quel mode de commande de service. Ceci vérifie que la configuration Unauthenticated de NTP est faite correctement.

```
sensor(config-hos-ena)#show settings enabled-ntp-unauthenticated ------------------------------
--------------- ntp-server: 10.1.1.1 ---------------------------------------------
sensor(config-hos-ena)#
```

Afin d'afficher l'horloge système, utilisez la commande de show clock dans le mode d'exécution comme affiché. Cet exemple affiche le NTP configuré et synchronisé :

```
sensor#show clock detail 11:45:02 CST Tues Jul 20 2011 Time source is NTP sensor#
```

Dépannez

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

Informations connexes

- Page de support de Système de protection contre les intrusions Cisco
- Page de support de Cisco IPS Manager Express
- Protocole NTP (Network Time Protocol)
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems