

ACS 5.x : Synchronisation de Cisco ACS avec l'exemple de configuration du serveur de NTP

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurez](#)

[Configuration de NTP sur Cisco ACS](#)

[Vérifiez](#)

[Dépannez](#)

[Problème : L'horloge dérive trop et le NTP échoue quand ACS est installé sur un ordinateur de VMware](#)

[Solution](#)

[La synchronisation de NTP perdue après l'adresse IP d'interface d'ACS est changée](#)

[Solution](#)

[Informations connexes](#)

[Introduction](#)

Le Protocole NTP (Network Time Protocol) est un protocole utilisé afin de synchroniser les horloges de différentes entités réseau. Il utilise UDP/123. L'objectif principal pour utiliser ce protocole est d'éviter les effets de la latence variable au-dessus des réseaux de données.

Ce document fournit une configuration d'échantillon pour Cisco ACS pour synchroniser son horloge avec le serveur de NTP. On permet à ACS 5.x pour configurer jusqu'à deux serveurs de NTP.

[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 :

- Version 5.x de Cisco Secure ACS

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.

Conventions

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

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil [Command Lookup Tool](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Configuration de NTP sur Cisco ACS

Afin de synchroniser la période de Cisco ACS avec un serveur de NTP, terminez-vous ces étapes :

1. Configurez manuellement la date et l'heure avec le [<hh de <day> de <month> de clock set : minute : commande de <yyyy> de ss](#).
2. Spécifiez le fuseau horaire avec la commande de [<timezone> de clock timezone](#).
3. Spécifiez le serveur de NTP avec le [serveur de NTP <l'adresse IP de la commande de <server> de NTP](#). Le NTP suit une hiérarchie de client-serveur. Quand un client de NTP est configuré avec un serveur de NTP, l'*horloge de référence* du serveur de NTP est passée au client. Cela prend approximativement 10-20 minutes pour obtenir le temps précis du serveur de NTP et dépend du retard se produit afin d'atteindre le serveur de NTP. Cisco ACS utilise le démon de NTP afin de synchroniser son horloge avec le serveur de NTP. Il ne prend en charge pas le NTP simple, SNTP. Quand les débuts de démon de NTP, ACS envoie un paquet au serveur de NTP qui contient son temps d'origine (gens du pays). Alors le serveur de NTP répond au paquet avec la mise en place de son temps d'horloge de référence. Une fois que le client de NTP reçoit ce paquet, il se connecte le paquet avec sa propre heure locale afin de valider le temps de déplacement pris par le paquet. Plusieurs tels échanges de paquet se produisent afin de calculer le temps précis de délai d'aller-retour et des valeurs excentrées et finalement l'heure locale du client de NTP est synchronisées avec l'horloge de référence du serveur de NTP.

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Afin de vérifier les détails de configuration, référez-vous à ces extraits de sortie de commande.

```
acs51/admin#show clock Wed Jun 13 11:02:00 IST 2012 acs51/admin# acs51/admin(config)#ntp server
192.168.26.55 The NTP server was modified. If this action resulted in a clock modification, you
must restart ACS. acs51/admin(config)# acs51/admin#show ntp Primary NTP : 192.168.26.55
synchronised to NTP server (192.168.26.55) at stratum 2 time correct to within 27 ms polling
server every 64 s remote refid st t when poll reach delay offset jitter
===== 127.127.1.0
LOCAL(0) 10 1 29 64 17 0.000 0.000 0.001 *192.168.26.55 .LOCL. 1 u 33 64 17 0.285 -9.900 2.733
Warning: Output results may conflict during periods of changing synchronization.
```

Remarque: *La strate* est une mesure qui spécifie combien étroit est le serveur de NTP à l'horloge de référence principale. Chaque client de NTP qui est synchronisé avec un serveur de la strate *n* se nomme comme au niveau de la strate *n+1*.

Référez-vous à ces messages de journal d'application d'ACS afin de vérifier les détails de synchronisation de NTP.

```
acs51/admin# show logging application | in ntp
Jun 13 13:51:59 acs51 ntpd[20259]: ntpd 4.2.0a@1.1190-r Mon Jul 28 11:03:50 EDT 2008 (1)
Jun 13 13:51:59 acs51 ntpd[20259]: precision = 1.000 usec
Jun 13 13:51:59 acs51 ntpd[20259]: Listening on interface wildcard, 0.0.0.0#123
Jun 13 13:51:59 acs51 ntpd[20259]: Listening on interface wildcard, ::#123
Jun 13 13:51:59 acs51 ntpd[20259]: Listening on interface lo, 127.0.0.1#123
Jun 13 13:51:59 acs51 ntpd[20259]: Listening on interface eth0, 192.168.26.51#123
Jun 13 13:51:59 acs51 ntpd[20259]: kernel time sync status 0040
Jun 13 13:51:59 acs51 ntpd[20259]: frequency initialized 0.000 PPM from /var/lib/ntp/drift
Jun 13 13:51:59 acs51 ntpd: ntpd startup succeeded Jun 13 13:55:15 acs51 ntpd[20259]:
synchronized to 192.168.26.55, stratum 2 !--- Output suppressed-
```

L'[Outil Interpréteur de sortie](#) (clients [enregistrés](#) uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Problème : L'horloge dérive trop et le NTP échoue quand ACS est installé sur un ordinateur de VMware

Cisco ACS est configuré pour utiliser le serveur de NTP comme clock source mais il change continuellement en la source temporelle interne. Quand ceci se produit, il fait des utilisateurs de notallow pour authentifier à partir du Répertoire actif pendant que le Kerberos prend en charge seulement 300 secondes de différence de temps.

Solution

Quand l'hôte d'ESXi a l'utilisation du CPU élevé, alors il ne sert pas des VMs aussi fréquemment de normale. Ceci affecte les horloges à l'intérieur des VMs et réellement la dérive d'horloge de cause d'un contrôleur de domaine windows qui dépasse cinq minutes. Il fait échouer le Kerberos. Ceci affecterait une VM de Windows sans NTP ou hébergerait le sync d'horloge aussi bien. Comme l'horloge virtuelle a présenté à Cisco ACS n'est pas assez stable pour que le NTP suive la dérive, il retourne par la suite à s'utiliser comme source temporelle.

Remarque: Le démon de NTP ajuste l'horloge dans plusieurs échanges et continue jusqu'à ce que le client obtiennent le temps précis. Cependant, quand le retard entre le serveur de NTP et le client de NTP deviennent trop grand, puis le démon de NTP obtient terminé et vous devez ajuster

le temps manuellement et redémarrer le démon de NTP.

Ce problème est placé pour être résolu quand vous intégrez le support d'outils de VMWare dans Cisco ACS, qui est disponible avec la version 5.4 de Cisco ACS qui doit être relâchée encore. Référez-vous au pour en savoir plus de l'ID de bogue Cisco [CSCtg50048](#) (clients [enregistrés](#) seulement). Comme contournement provisoire, vous pourriez essayer ces étapes :

- Services de l'arrêt ACS avec la commande d'**arrêt ACS**.
- Retirez toute la configuration de NTP et sauvegardez la configuration avec une commande de **mem d'inscription**.
- Réinitialisation Cisco ACS.
- Assurez-vous que tous les services s'exécutent avec la commande d'**acs d'état d'application d'exposition**.
- Réglez l'horloge pour avoir lieu aussi étroitement au temps réel que possible, au deuxième avant de la condition requise excentrée sur le NTP.
- Assurez-vous que le fuseau horaire est le correct.
- Re-ajoutez la configuration de NTP et sauvegardez-la.
- Exécutez la commande de **show ntp** afin de vérifier si la sortie est identique.

Remarque: Si ces étapes ne résolvent pas le problème, vous êtes informé contacter [Cisco TAC](#).

[La synchronisation de NTP perdue après l'adresse IP d'interface d'ACS est changée](#)

Si vous changez l'adresse IP du NIC ACS, ceci fait le NTP sortir du sync.

[Solution](#)

On observe ce comportement et l'ID de bogue Cisco ouvert une session [CSCtk76151](#) (clients [enregistrés](#) seulement). Quand l'adresse IP ACS est modifiée, elle redémarre l'application ACS mais pas le démon de NTP. Il est réparé dans la version 5.3.0.23 ACS. Afin de résoudre ce problème dans des versions antérieures, terminez-vous ces étapes :

1. N'émettez l'**aucun** ordre de **serveur de ntp** afin d'arrêter le processus de NTP.
2. Révissez l'ordre de **serveur de ntp** afin de redémarrer le processus de NTP.

[Informations connexes](#)

- [Support produit du CS ACS 5.X](#)
- [Guide utilisateur pour le Système de contrôle d'accès sécurisé Cisco 5.3](#)
- [Support et documentation techniques - Cisco Systems](#)