NTP sur l'exemple Sans fil de configuration de contrôleurs LAN

Contenu

Introduction

Ce document explique comment configurer les contrôleurs LAN Sans fil (WLCs) pour synchroniser la date et l'heure avec un serveur de Protocole NTP (Network Time Protocol).

Conditions préalables

Conditions requises

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

- Connaissance de base de la configuration du Point d'accès léger (recouvrements) et des Cisco WLC
- Connaissance de base de NTP

Composants utilisés

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

- Cisco 4400 WLC qui exécute la version de logiciel 7.0.116.0
- Recouvrements de gamme de Cisco 1230AG
- Routeur de gamme Cisco 2800 qui exécute la version de logiciel 12.4(11)T de Cisco IOS®

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

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.

Gérer la date du système et le temps sur le contrôleur LAN Sans fil

Sur un WLC, la date du système et le temps peuvent être manuellement configurés du WLC ou être configurés pour obtenir la date et l'heure d'un serveur de NTP.

La date du système et le temps peuvent être manuellement configurés utilisant l'assistant ou le WLC GUI/CLI de configuration CLI. Ce document fournit un exemple de configuration pour synchroniser la date du système et le temps WLC par un serveur de NTP.

Le NTP est un Internet Protocol utilisé pour synchroniser les horloges des ordinateurs à une certaine référence de temps. RFC 1305 fournit les informations détaillées sur l'implémentation du NTP v3. Un réseau de NTP reçoit habituellement son temps d'une source temporelle bien fondée, telle qu'une horloge radio ou une horloge atomique reliée à un Serveur de synchronisation. Le NTP distribue alors cette fois à travers le réseau. Un client de NTP effectue une transaction avec son serveur pendant l'intervalle de sondage (de 64 à 1024 secondes), qui change dynamiquement au fil du temps selon les conditions de réseau entre le serveur de NTP et le client. L'autre situation se produit quand le routeur communique à un mauvais serveur de NTP (par exemple, serveur de NTP avec la grande dispersion). Le routeur augmente également l'intervalle entre deux invitations à émettre. Pas plus d'une transaction de NTP par minute est nécessaire pour synchroniser deux ordinateurs. Il n'est pas possible d'ajuster l'intervalle entre deux invitations à émettre de NTP sur un routeur.

Le NTP emploie le concept d'une strate pour décrire combien de sauts de NTP loin un ordinateur est d'une source temporelle bien fondée. Par exemple, un Serveur de synchronisation de la strate 1 a une radio ou une horloge atomique directement reliée à elle. Il envoie alors son temps à un Serveur de synchronisation de strate 2 par le NTP, et ainsi de suite.

Pour plus d'informations sur les pratiques recommandées pour le déploiement de NTP, référez-vous au Network Time Protocol : Livre Blanc de pratiques recommandées. L'exemple dans ce document utilise un routeur de Cisco 2800 en tant que serveur de NTP. Le WLC est configuré pour synchroniser sa date et heure avec ce serveur de NTP.

Configurez

Configuration du routeur de gamme Cisco 2800 en tant que serveur de NTP

Configurer le routeur en tant que serveur bien fondé de NTP

Utilisez cette commande en mode de configuration globale si vous voulez que le système soit un

serveur bien fondé de NTP, même si le système n'est pas synchronisé à une source temporelle extérieure :

```
ntp master
!--- Makes the system an authoritative NTP server
```

Configurer l'authentification de NTP

Si vous voulez authentifier les associations avec d'autres systèmes pour des raisons de sécurité, utilisez les commandes qui suivent. Les premières commandes enables la fonction d'authentification de NTP. La deuxième commande définit chacune des clés d'authentification. Chaque clé a un nombre principal, un type, et une valeur. Actuellement, le seul type pris en charge principal est MD5. Troisièmement, une liste de clés « de confiance » d'authentification est définie. Si une clé est de confiance, ce système sera prêt à synchroniser à un système qui utilise cette clé en ses paquets de NTP. Afin de configurer l'authentification de NTP, utilisez ces commandes en mode de configuration globale :

```
ntp authenticate
!--- Enables the NTP authentication feature ntp authentication-key number md5 value !--- Defines
the authentication keys ntp trusted-key key-number !--- Defines trusted authentication keys
```

Voici une configuration de serveur de NTP d'exemple sur le routeur de gamme 2800. Le routeur est le ntp master, qui veut dire que le routeur agit en tant que serveur bien fondé de NTP.

```
ntp master
ntp authenticate
ntp authentication-key 1 md5 0305480F0008 7
ntp trusted-key 1
```

Configurer le WLC pour le serveur de NTP

Commençant par la release de 7.0.116.0, vous pouvez également configurer un canal d'authentification entre le contrôleur et le serveur de NTP. Afin de configurer l'authentification de NTP utilisant le GUI de contrôleur, exécutez ces étapes :

1. Choisissez le **contrôleur > le NTP > les serveurs** pour ouvrir la page de serveurs de NTP. Cliquez sur New pour ajouter un serveur de NTP.**Les serveurs de NTP > nouvelle page** apparaît.
2. Choisissez une priorité de serveur de la liste déroulante d'**index de serveur (priorité)**.
3. Entrez dans l'adresse IP du serveur de NTP dans la zone de texte d'**IP address de serveur**.
4. Activez l'authentification de serveur de NTP en sélectionnant la case d'authentification de serveur de NTP.
5. Cliquez sur **Apply**.
6. Choisissez le **contrôleur > le NTP > les clés**.
7. Cliquez sur New pour créer une clé.
8. Écrivez l'index de clé dans la zone de texte d'**index de clé**.
9. Choisissez le format principal de la liste déroulante **principale de format**.
10. Introduisez la clé dans la zone de texte **principale**.

Vérifiez

Vous pouvez utiliser ces commandes du WLC CLI de vérifier la configuration :

```
(Cisco Controller) >show time Time..................................... Wed Nov 23
```

```
15:31:27 2011 Timezone delta..................................... 0:0 Timezone
location.............................. (GMT -6:00) Central Time (US and Canada) NTP Servers
NTP Polling Interval......................... 86400 Index NTP Key Index NTP Server NTP Msg Auth
Status ------- ------------------------------------------------------------- 1 1 10.78.177.30
AUTH SUCCESS
```

Dépannez

Vous pouvez utiliser la commande d'**enable de détail de debug ntp** de visualiser la séquence d'opérations qui se produisent une fois la configuration du serveur de NTP sont faites sur le WLC.

```
*sntpReceiveTask: Nov 23 15:08:24.360: Started=3531049704.360568 2011 Nov 23 15:08:24.360

*sntpReceiveTask: Nov 23 15:08:24.360: Looking for the socket addresses

*sntpReceiveTask: Nov 23 15:08:24.360: NTP Polling cycle: accepts=0, count=5, attempts=1,
retriesPerHost=6.
 Outgoing packet on NTP Server on socket 0:

*sntpReceiveTask: Nov 23 15:08:24.360: sta=0 ver=3 mod=3 str=15 pol=8 dis=0.000000 ref=0.000000

*sntpReceiveTask: Nov 23 15:08:24.361: ori=0.000000 rec=0.000000
*sntpReceiveTask: Nov 23 15:08:24.361: tra=3531049704.360889 cur=3531049704.360889

*sntpReceiveTask: Nov 23 15:08:24.361: Host Supports NTP authentication with Key Id = 1

*sntpReceiveTask: Nov 23 15:08:24.361: NTP Auth Key Id = 1 Key Length = 5

*sntpReceiveTask: Nov 23 15:08:24.361: MD5 Hash and Key Id added in NTP Tx packet

*sntpReceiveTask: Nov 23 15:08:24.361: Flushing outstanding packets

*sntpReceiveTask: Nov 23 15:08:24.361: Flushed 0 packets totalling 0 bytes

*sntpReceiveTask: Nov 23 15:08:24.361: Packet of length 68 sent to 10.78.177.30 UDPport=123
*sntpReceiveTask: Nov 23 15:08:24.363: Packet of length 68 received from 10.78.177.30
UDPport=123
*sntpReceiveTask: Nov 23 15:08:24.363: KeyId In Recieved NTP Packet 1

*sntpReceiveTask: Nov 23 15:08:24.363: KeyId 1 found in recieved NTP packet exists as part of
the trusted Key/s

*sntpReceiveTask: Nov 23 15:08:24.363: The NTP trusted Key Id  1 length = 5

*sntpReceiveTask: Nov 23 15:08:24.363: NTP Message Authentication - SUCCESS *sntpReceiveTask:
Nov 23 15:08:24.363: sta=0 ver=3 mod=4 str=8 pol=8 dis=3.875031 ref=3531071269.384065
*sntpReceiveTask: Nov 23 15:08:24.363: ori=3531049704.360889 rec=3531071270.103183
*sntpReceiveTask: Nov 23 15:08:24.363: tra=3531071270.103387 cur=3531049704.363251
```

Informations connexes

- Protocole d'Heure Réseau : Livre blanc sur les pratiques recommandées
- Guide de configuration Sans fil de contrôleur LAN de Cisco, release 7.0.116.0
- Support et documentation techniques - Cisco Systems