Configuration du protocole NTP sur les contrôleurs LAN sans fil

Table des matières

Introduction

Ce document décrit comment configurer les contrôleurs LAN sans fil (WLC) AireOS pour synchroniser la date et l'heure avec un serveur NTP (Network Time Protocol).

Conditions préalables

Exigences

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

- Connaissance de base de la configuration de Cisco WLC.
- Connaissances de base du protocole NTP.

Composants utilisés

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

- Cisco WLC 3504 qui exécute le logiciel version 8.8.110.
- Commutateur de couche 3 de la gamme Cisco Catalyst 3560-CX qui exécute le logiciel Cisco IOS® version 15.2(6)E2.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Gérer la date et l'heure système sur le contrôleur LAN sans fil

Sur un WLC, la date et l'heure système peuvent être configurées manuellement à partir du WLC ou configurées pour obtenir la date et l'heure d'un serveur NTP.

La date et l'heure du système peuvent être configurées manuellement dans l'assistant de configuration CLI ou dans l'interface graphique utilisateur/CLI du WLC.

Ce document fournit un exemple de configuration pour synchroniser la date et l'heure du système WLC via un serveur NTP.

NTP est un protocole réseau de synchronisation d'horloge entre des systèmes informatiques sur des réseaux de données à latence variable, qui permet de synchroniser les horloges des ordinateurs avec une référence temporelle. Les documents RFC 1305 et RFC 5905 fournissent des informations détaillées sur l'implémentation de NTPv3 et NTPv4, respectivement.

Un réseau NTP reçoit généralement son heure d'une source de temps faisant autorité, telle qu'une horloge radio ou une horloge atomique connectée à un serveur de temps. Le protocole NTP distribue ensuite cette heure sur le réseau.

Un client NTP effectue une transaction avec son serveur au cours de l'intervalle d'interrogation, qui change dynamiquement au fil du temps et dépend des conditions réseau entre le serveur NTP et le client.

NTP utilise le concept de strate pour décrire le nombre de sauts NTP à partir d'une source temporelle faisant autorité. Par exemple, un serveur de temps de strate 1 est directement relié à une horloge radio ou atomique. Il envoie ensuite son temps à un serveur de temps de strate 2 via NTP, et ainsi de suite.

Pour plus d'informations sur les meilleures pratiques pour le déploiement NTP, référez-vous à Utilisation des meilleures pratiques pour le protocole NTP.

L'exemple de ce document utilise un commutateur L3 de la gamme Cisco Catalyst 3560-CX comme serveur NTP. Le WLC est configuré pour synchroniser sa date et son heure avec ce serveur NTP.

Configurer

Diagramme du réseau

WLC ---- 3560-CX Commutateur L3 ---- Serveur NTP

Configurations

Configurer le commutateur L3 en tant que serveur NTP faisant autorité

Utilisez cette commande en mode de configuration globale si vous voulez que le système soit un serveur NTP faisant autorité, même si le système n'est pas synchronisé avec une source temporelle externe :

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

Configuration de l'authentification NTP

Si vous souhaitez authentifier les associations avec d'autres systèmes à des fins de sécurité, utilisez les commandes suivantes. La première commande active la fonctionnalité d'authentification NTP.

La deuxième commande définit chacune des clés d'authentification. Chaque clé possède un numéro de clé, un type et une valeur. Actuellement, le seul type de clé pris en charge est md5.

Troisièmement, une liste de clés d'authentification approuvées est définie. Si une clé est approuvée, ce système est prêt à se synchroniser avec un système qui utilise cette clé dans ses paquets NTP. Afin de configurer l'authentification 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 un exemple de configuration de serveur NTP sur le commutateur 3560-CX L3. Le commutateur est le NTP master, ce qui signifie que le routeur agit comme le serveur NTP faisant autorité, mais lui-même obtient l'heure d'un autre serveur NTP xxxx.xxx.

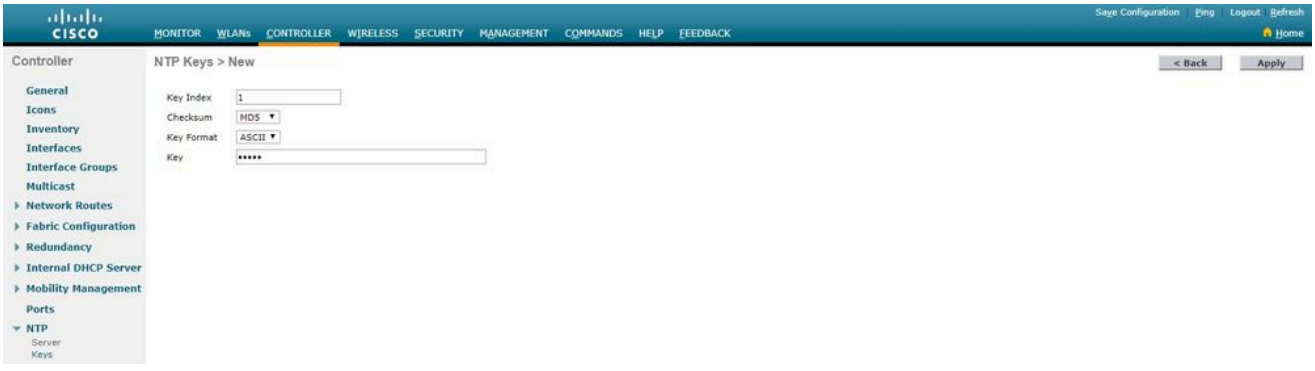
```
(config)#ntp authentication-key 1 md5 1511021F0725 7
(config)#ntp authenticate
(config)#ntp trusted-key 1
(config)#ntp master
(config)#ntp server xxxx.xxx
```

Configurer le WLC pour le serveur NTP

Depuis la version 8.6, vous pouvez activer NTPv4. Vous pouvez également configurer un canal d'authentification entre le contrôleur et le serveur NTP.

Afin de configurer l'authentification NTP dans l'interface graphique du contrôleur, effectuez ces étapes :

- Choisissez **Controller > NTP > Keys**.
- Cliquez sur **New** pour créer une clé.
- Entrez l'index de la clé dans la zone de texte **Index de la clé**.
- Sélectionnez la **somme de contrôle de clé** (MD5 ou SHA1) et la liste déroulante **Key Format**.
- Entrez la clé dans la zone de texte **Clé** :



- Choisissez **Controller > NTP > Servers** pour ouvrir la page NTP Servers. Sélectionnez la version 3 ou 4, puis cliquez sur **New** pour

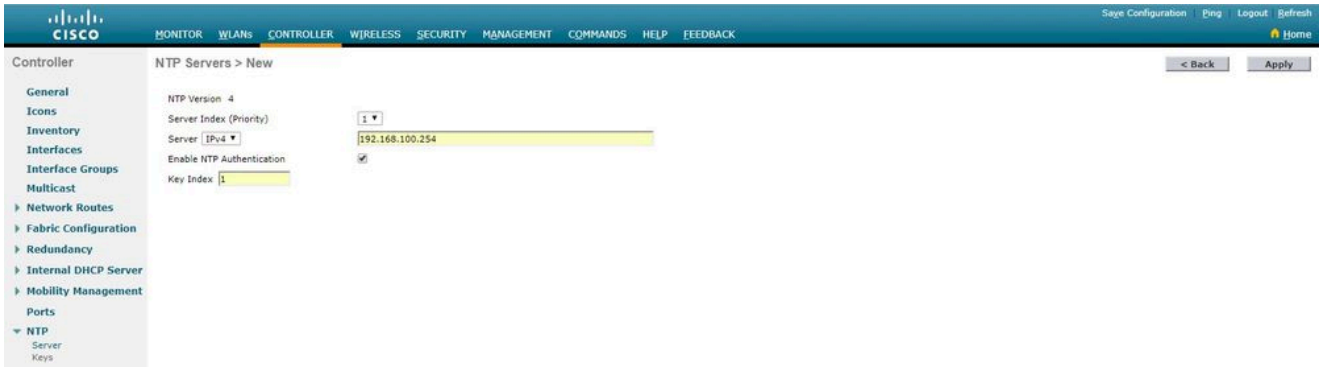
ajouter un serveur NTP. La **page NTP Servers > New** s'affiche.

- Sélectionnez l'**index du serveur (priorité)**.
-

Entrez l'adresse IP du serveur NTP dans la zone de texte **Server IP Address**.

-

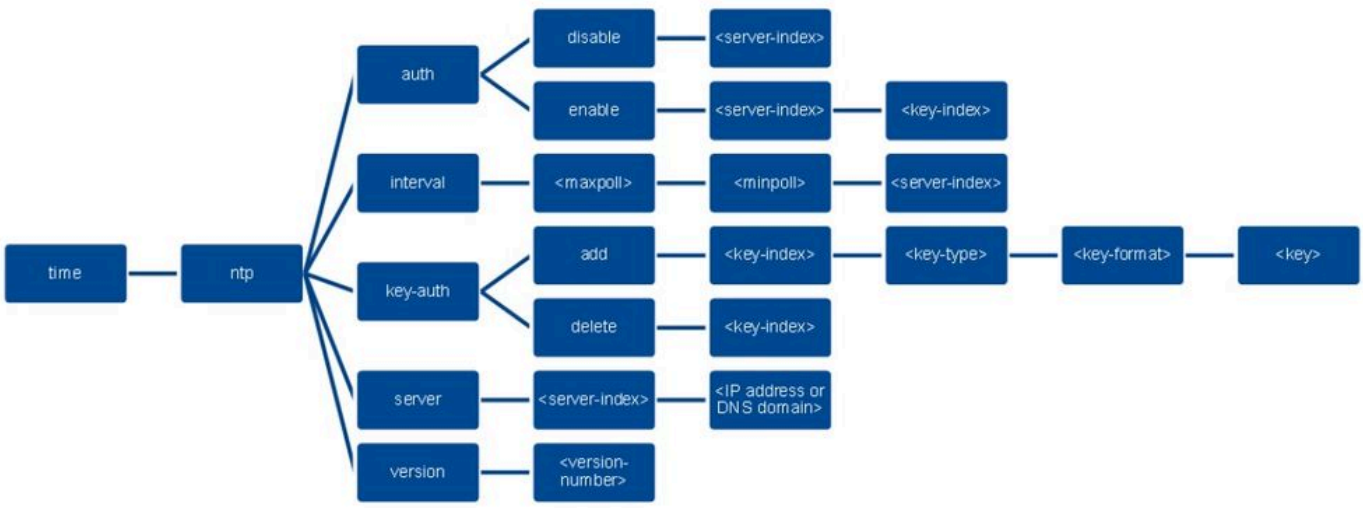
Activez l'authentification du serveur NTP, activez la case à cocher **NTP Server Authentication** et sélectionnez l'**index de clé** configuré précédemment.



-

Cliquez sur Apply.

Afin de configurer l'authentification NTP via l'interface de ligne de commande du contrôleur, suivez cette arborescence de commandes :



>config time ntp version 4
>config time ntp key-auth add 1 md5 ascii cisco
>config time ntp server 1 192.168.100.254
>config time ntp auth enable 1 1

Vérifier

Sur le serveur NTP

#show ntp status
Clock is synchronized, stratum 3, reference is x.x.x.x
nominal freq is 286.1023 Hz, actual freq is 286.0901 Hz, precision is 2**21
ntp uptime is 6591900 (1/100 of seconds), resolution is 3496
reference time is E007C909.80902653 (09:23:21.502 UTC Fri Feb 8 2019)
clock offset is 0.3406 msec, root delay is 59.97 msec
root dispersion is 25.98 msec, peer dispersion is 1.47 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000042509 s/s
system poll interval is 128, last update was 7 sec ago.

#show ntp associations

 address ref clock st when poll reach delay offset disp
*~x.x.x.x y.y.y.y 2 20 1024 17 13.634 0.024 1.626
 ~127.127.1.1 .LOCL. 7 9 16 377 0.000 0.000 0.232
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

#show ntp information
Ntp Software Name : Cisco-ntpv4
Ntp Software Version : Cisco-ntpv4-1.0
Ntp Software Vendor : CISCO
Ntp System Type : Cisco IOS / APM86XXX

Sur le WLC

Dans l'interface graphique

Pendant que le WLC établit la communication :

Une fois la connexion établie :

Dans la CLI WLC

(Cisco Controller) >show time

Time..... Fri Feb 8 10:14:47 2019

Timezone delta..... 0:0
Timezone location.....

NTP Servers
NTP Version..... 4

Index NTP Key NTP Server NTP Key Polling Intervals
Index Type Max Min
---
1 1 192.168.100.254 MD5 10 6

NTPQ status list of NTP associations

assoc
ind assid status conf reach auth condition last_event cnt src_addr
==========
1 1385 f63a yes yes ok sys.peer sys_peer 3 192.168.100.254

(Cisco Controller) >

Dépannage

Du côté du serveur NTP qui exécute Cisco IOS, vous pouvez utiliser la commande debug ntp all enable :

#debug ntp all
NTP events debugging is on
NTP core messages debugging is on
NTP clock adjustments debugging is on
NTP reference clocks debugging is on

NTP packets debugging is on
#
(communication between SW and NTP server xxxx.xxx)
Feb 8 09:52:30.563: NTP message sent to x.x.x.x, from interface 'Vlan1' (192.168.1.81).
Feb 8 09:52:30.577: NTP message received from x.x.x.x on interface 'Vlan1' (192.168.1.81).
Feb 8 09:52:30.577: NTP Core(DEBUG): ntp_receive: message received
Feb 8 09:52:30.577: NTP Core(DEBUG): ntp_receive: peer is 0x0D284B34, next action is 1.

(communication between SW and WLC)
Feb 8 09:53:10.421: NTP message received from 192.168.100.253 on interface 'Vlan100' (192.168.100.254).
Feb 8 09:53:10.421: NTP Core(DEBUG): ntp_receive: message received
Feb 8 09:53:10.421: NTP Core(DEBUG): ntp_receive: peer is 0x00000000, next action is 3.
Feb 8 09:53:10.421: NTP message sent to 192.168.100.253, from interface 'Vlan100' (192.168.100.254).

(communication between SW and NTP server xxxx.xxx)
Feb 8 09:53:37.566: NTP message sent to x.x.x.x, from interface 'Vlan1' (192.168.1.81).
Feb 8 09:53:37.580: NTP message received from x.x.x.x on interface 'Vlan1' (192.168.1.81).
Feb 8 09:53:37.580: NTP Core(DEBUG): ntp_receive: message received
Feb 8 09:53:37.580: NTP Core(DEBUG): ntp_receive: peer is 0x0D284B34, next action is 1.

(communication between SW and WLC)
Feb 8 09:54:17.421: NTP message received from 192.168.100.253 on interface 'Vlan100' (192.168.100.254).
Feb 8 09:54:17.421: NTP Core(DEBUG): ntp_receive: message received
Feb 8 09:54:17.421: NTP Core(DEBUG): ntp_receive: peer is 0x00000000, next action is 3.
Feb 8 09:54:17.421: NTP message sent to 192.168.100.253, from interface 'Vlan100' (192.168.100.254).

Côté WLC :

>debug ntp ?

detail Configures debug of detailed NTP messages.
low Configures debug of NTP messages.
packet Configures debug of NTP packets.

(at the time of writte this doc there was Cisco bug ID CSCvo29660
on which the debugs of ntpv4 are not printed in the CLI. The below debugs are using NTPv3.)
(Cisco Controller) >debug ntp detail enable
(Cisco Controller) >debug ntp packet enable
(Cisco Controller) >*emWeb: Feb 08 11:26:53.896: ntp Auth key Info = -1

*emWeb: Feb 08 11:26:58.143: ntp Auth key Info = -1

*emWeb: Feb 08 11:26:58.143: ntp Auth key Info = -1

*emWeb: Feb 08 11:26:58.143: Key Id = 1 found at Local Index = 0

*sntpReceiveTask: Feb 08 11:26:58.143: Initiating time sequence

*sntpReceiveTask: Feb 08 11:26:58.143: Fetching time from:192.168.100.254

*sntpReceiveTask: Feb 08 11:26:58.143: Started=3758614018.143350 2019 Feb 08 11:26:58.143

*sntpReceiveTask: Feb 08 11:26:58.143: hostname=192.168.100.254 hostIdx=1 hostNum=0
*sntpReceiveTask: Feb 08 11:26:58.143: Looking for the socket addresses

*sntpReceiveTask: Feb 08 11:26:58.143: NTP Polling cycle: accepts=0, count=5, attempts=1,
retriesPerHost=6. Outgoing packet on NTP Server on socket 0:

*sntpReceiveTask: Feb 08 11:26:58.143: sta=0 ver=3 mod=3 str=15 pol=8 dis=0.000000 ref=0.000000

*sntpReceiveTask: Feb 08 11:26:58.143: ori=0.000000 rec=0.000000
*sntpReceiveTask: Feb 08 11:26:58.143: tra=3758614018.143422 cur=3758614018.143422

*sntpReceiveTask: Feb 08 11:26:58.143: Host Supports NTP authentication with Key Id = 1

*sntpReceiveTask: Feb 08 11:26:58.143: NTP Auth Key Id = 1 Key Length = 5

*sntpReceiveTask: Feb 08 11:26:58.143: MD5 Hash and Key Id added in NTP Tx packet

*sntpReceiveTask: Feb 08 11:26:58.143: 00000000: 1b 0f 08 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
*sntpReceiveTask: Feb 08 11:26:58.143: 00000010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
*sntpReceiveTask: Feb 08 11:26:58.143: 00000020: 00 00 00 00 00 00 00 00 e0 07 e6 02 24 b7 50 00 ....$.P.
*sntpReceiveTask: Feb 08 11:26:58.143: 00000030: 00 00 00 01 e4 35 f3 1a 89 f0 93 c5 51 c7 c5 23 .....5......Q..#
*sntpReceiveTask: Feb 08 11:26:58.143: 00000040: 01 dd 67 e0 ..g.
*sntpReceiveTask: Feb 08 11:26:58.143: Flushing outstanding packets

*sntpReceiveTask: Feb 08 11:26:58.143: Flushed 0 packets totalling 0 bytes

*sntpReceiveTask: Feb 08 11:26:58.143: Packet of length 68 sent to ::ffff:192.168.100.254 UDPport=123
*emWeb: Feb 08 11:26:58.143: ntp Auth key Info = 0

*emWeb: Feb 08 11:26:58.143: idx != 0 : ntp key Id = 1 Msg auth Status = 66

*sntpReceiveTask: Feb 08 11:26:58.146: Packet of length 68 received from ::ffff:192.168.100.254 UDPport=123
*sntpReceiveTask: Feb 08 11:26:58.146: Incoming packet on socket 0: has Authentication Enabled
*sntpReceiveTask: Feb 08 11:26:58.146: 00000000: 1c 04 08 eb 00 00 0e a0 00 00 0b 2e c3 16 11 07 ....
*sntpReceiveTask: Feb 08 11:26:58.146: 00000010: e0 07 e5 f8 d3 21 bf 57 e0 07 e6 02 24 b7 50 00 .....!.W....$.P.
*sntpReceiveTask: Feb 08 11:26:58.146: 00000020: e0 07 e6 02 24 e5 e3 b4 e0 07 e6 02 24 f3 c7 5a ....$.......$..Z
*sntpReceiveTask: Feb 08 11:26:58.146: 00000030: 00 00 00 01 32 e4 26 47 33 16 50 bd d1 37 63 b7 ....2.&G3.P..7c.
*sntpReceiveTask: Feb 08 11:26:58.146: KeyId In Recieved NTP Packet 1

*sntpReceiveTask: Feb 08 11:26:58.146: KeyId 1 found in recieved NTP packet exists as part of the trusted Key/s

*sntpReceiveTask: Feb 08 11:26:58.146: The NTP trusted Key Id 1 length = 5

*sntpReceiveTask: Feb 08 11:26:58.146: NTP Message Authentication - SUCCESS

*sntpReceiveTask: Feb 08 11:26:58.146: sta=0 ver=3 mod=4 str=4 pol=8 dis=0.043671 ref=3758614008.824734

*sntpReceiveTask: Feb 08 11:26:58.146: ori=3758614018.143422 rec=3758614018.144133
*sntpReceiveTask: Feb 08 11:26:58.146: Offset=-0.000683+/-0.002787 disp=1.937698

*sntpReceiveTask: Feb 08 11:26:58.146: best=-0.000683+/-0.002787

*sntpReceiveTask: Feb 08 11:26:58.146: accepts=1 rejects=0 flushes=0

*sntpReceiveTask: Feb 08 11:26:58.146: Correction: -0.000683 +/- 0.002787 disp=1.937698

*sntpReceiveTask: Feb 08 11:26:58.146: Setting clock to 2019 Feb 08 11:26:58.145 + 0.001 +/- 1.940 secs
*sntpReceiveTask: Feb 08 11:26:58.146: correction -0.001 +/- 1.938+0.003 secs - ignored

(Cisco Controller) >

Informations connexes

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.