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

Exigences

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

- Connaissance de base de la configuration 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 WLC 3504 qui exécute la version de logiciel 8.8.110.0.
- Commutateur de la gamme Cisco Catalyst 3560-CX L3 qui exécute la version de logiciel

15.2(6)E2 de Cisco IOS®.

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.

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 Protocole NTP (Network Time Protocol) est un protocole de réseau pour la synchronisation d'horloge entre les systèmes informatiques au-dessus des réseaux de données de variable-latence pour synchroniser les horloges des ordinateurs à une certaine référence de temps. RFC 1305 et RFC 5905 fournit les informations détaillées sur l'implémentation NTPv3 et NTPv4, respectivement.

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, qui change dynamiquement au fil du temps selon les conditions de réseau entre le serveur de NTP et le client.

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 le toNetwork Time Protocol : Livre Blanc de pratiques recommandées.

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

Configurer

Diagramme du réseau

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

Configurations

En configurant le L3 commutez 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 du serveur de NTP d'exemple sur le commutateur 3560-CX L3. Le commutateur est le ntp master, qui signifie que le routeur agit en tant que serveur bien fondé de NTP mais lui-même obtient le temps d'un autre serveur « pool.ntp.org » de NTP.

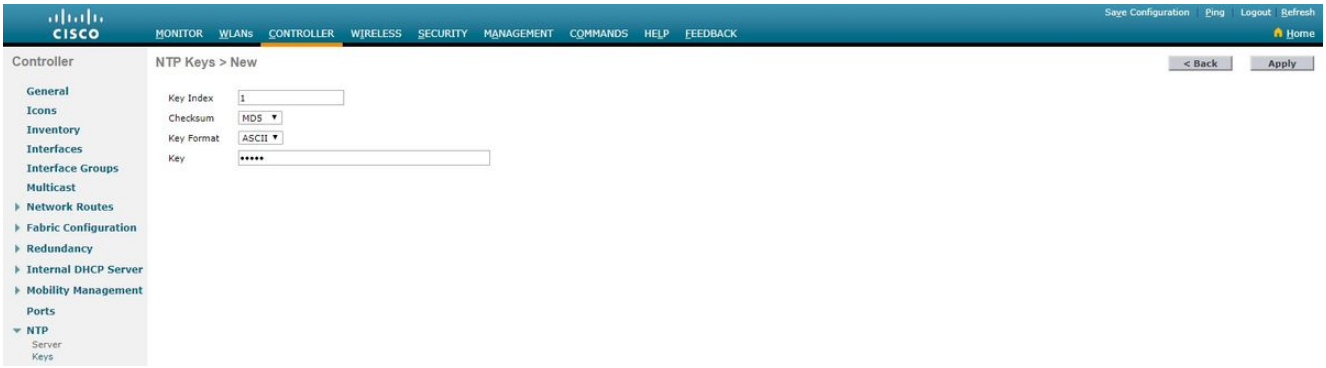
```
(config)#ntp authentication-key 1 md5 1511021F0725 7
(config)#ntp authenticate
(config)#ntp trusted-key 1
(config)#ntp master
(config)#ntp server pool.ntp.org
```

Configurez le WLC pour le serveur de NTP

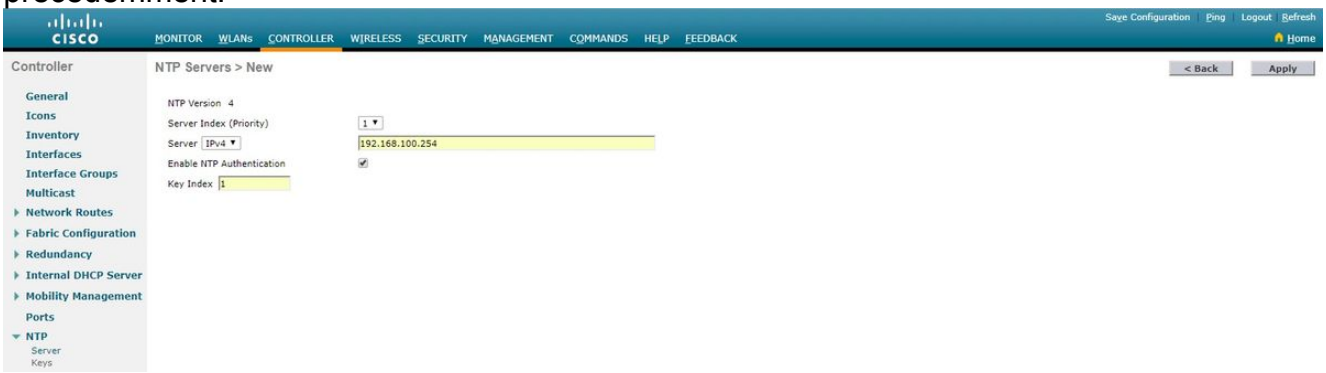
Àpartir de la version 8.6 nous pouvons activer NTPv4. Nous pouvons également configurer un canal d'authentification entre le contrôleur et le serveur de NTP.

Afin de configurer l'authentification de NTP utilisant le GUI de contrôleur, exécutez ces étapes :

1. ChooseController **> NTP > clés**.
2. ClickNewto créent une clé.
3. Écrivez l'index de clé dans la case d'**Indextext de** theKey.
4. Choisissez la **somme de contrôle principale** (MD5 ou SHA1) et la liste de **Formatdrop-down de** theKey.
5. Introduisez la clé dans la case de theKeytext
   :

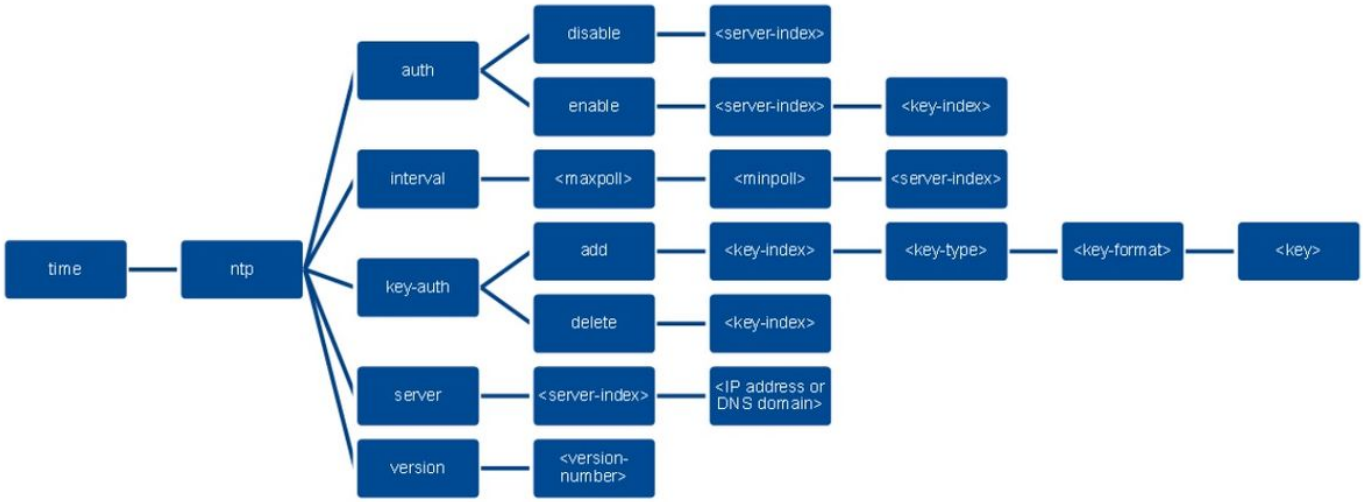


6. ChooseController **> NTP > Serversto** ouvrent la page de serveurs de NTP. La version 3 ou 4 choisie et alors clickNewto ajoutent un serveur de NTP. **Serveurs de** TheNTP **> nouveaux pageappears**.
7. Sélectionnez l'**index de serveur (priorité)**.
8. Entrez dans l'adresse IP du serveur de NTP dans la case **IP Addresstext de** theServer.
9. Activez l'authentification de serveur de NTP en sélectionnant la case d'**authentification de serveur de NTP** et sélectionnez l'**index de clé** configuré précédemment.



10. ClickApply.

Afin de configurer l'authentification de NTP utilisant le contrôleur CLI, followe cette arborescence de commande :




```
>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
```

Vérifiez

Sur le serveur de NTP

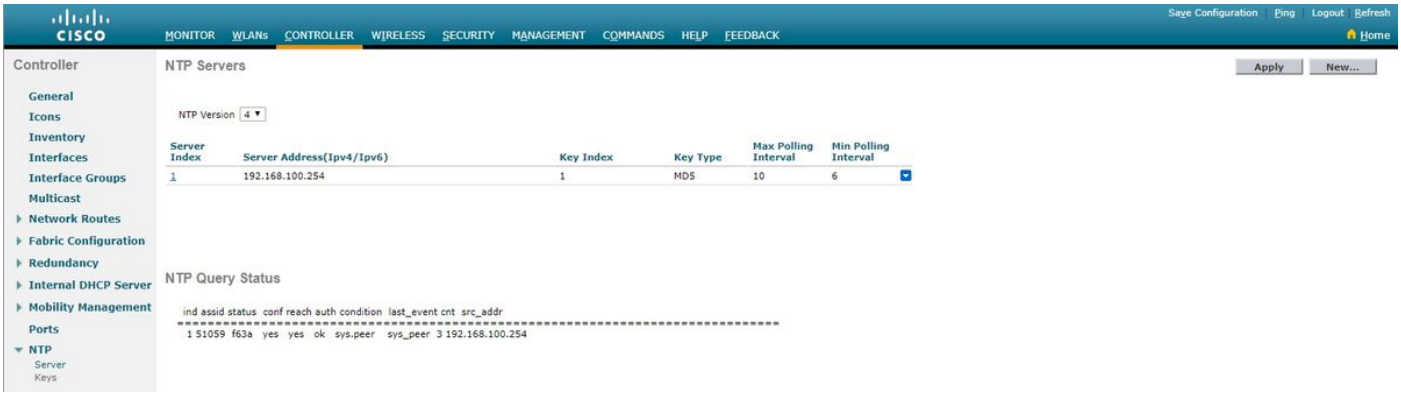
```
#show ntp status
Clock is synchronized, stratum 3, reference is 193.136.152.72
nominal freq is 286.1023 Hz, actual freq is 286.0901 Hz, precision is 2**21
ntp uptime is 6591900 (1/100 of seconds), resolution is 3496
reference time is E007C909.80902653 (09:23:21.502 UTC Fri Feb 8 2019)
clock offset 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
*~193.136.152.72 138.96.64.10 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 le GUI

Pendant l'établissement de la transmission :

Après la connexion établie :



Dans le WLC CLI

```
(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) >
```

Dépanner

Sur le Cisco IOS courant de côté serveur de NTP nous pouvons utiliser le « **debug ntp tout l'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 pool.ntp.org)
Feb 8 09:52:30.563: NTP message sent to 195.22.17.7, from interface 'Vlan1' (192.168.1.81).
Feb 8 09:52:30.577: NTP message received from 195.22.17.7 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 pool.ntp.org)
Feb 8 09:53:37.566: NTP message sent to 195.22.17.7, from interface 'Vlan1' (192.168.1.81).
Feb 8 09:53:37.580: NTP message received from 195.22.17.7 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).
```

Du 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 writting this doc there was a DDTS 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) >
```