Comprendre les codes d'association NTP dans les contrôleurs SD-WAN

Table des matières

Introduction

Ce document décrit comment comprendre les codes d'état d'association NTP sur les contrôleurs SD-WAN.

Conditions préalables

- Le service NTP doit être autorisé à autoriser le service ntp à l'intérieur des interfaces de tunnel VPN 0 de tous les contrôleurs. Si le service n'est pas autorisé, utilisez cette procédure pour l'activer.

<#root>

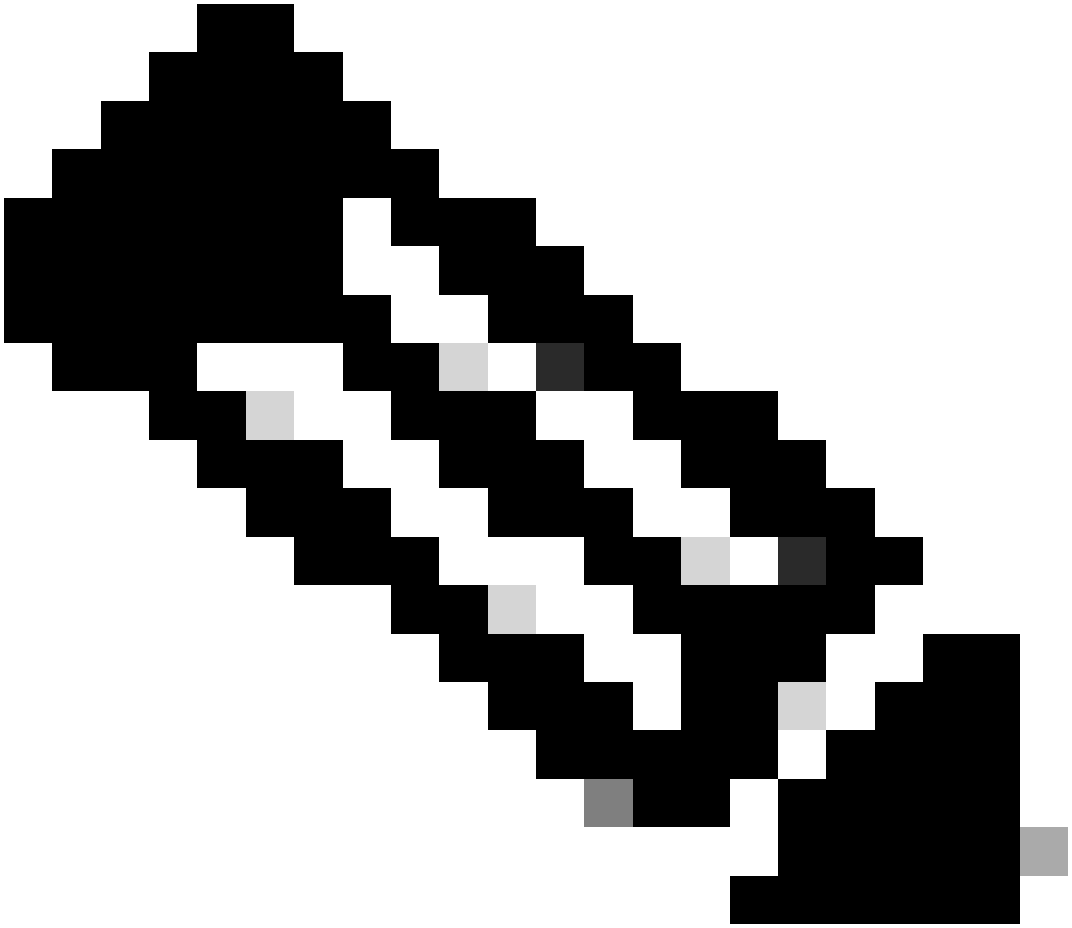
```
config t
vpn 0
!
interface eth1
tunnel-interface
```

allow-service ntp

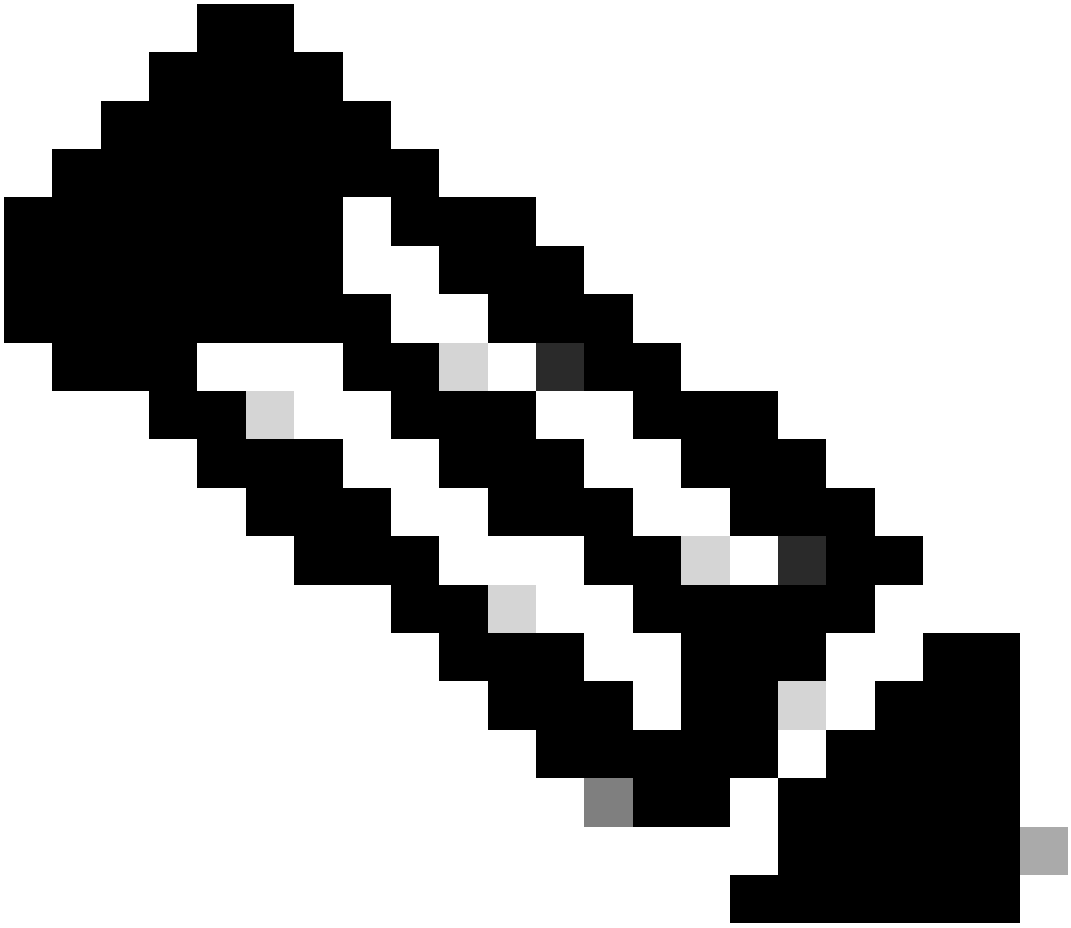
```
!
commit
```

- NTP doit également être configuré sur tous les contrôleurs. Consultez la documentation officielle pour configurer NTP via l'interface de ligne de commande ou le modèle vManage.
- Tous les contrôleurs et tous les noeuds de la superposition doivent être configurés avec le

même serveur NTP pour avoir la même date/heure. Un jeu de dates/heures différent peut entraîner des problèmes dans l'établissement de la connexion de contrôle.



Remarque : pour la configuration NTP, reportez-vous à la section Configure NTP servers Using Cisco Vmanage and Configure NTP using CLI.



Remarque : pour plus d'informations sur les problèmes d'établissement de connexion de contrôle, reportez-vous à Dépannage des connexions de contrôle SD-WAN.

Composants utilisés

Ce document est basé sur les versions logicielles et matérielles suivantes :

- Contrôleurs SD-WAN version 20.9.3

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.

Informations générales

Les contrôleurs SD-WAN peuvent être associés à un serveur NTP (Network Time Protocol) pour la synchronisation de l'horloge réseau. Le protocole NTP repose sur le port 13 du protocole UDP (User Datagram Protocol), qui fournit une méthode de transport sans connexion.

Dans Viptela OS, la commande show ntp associations affiche différents codes pendant le processus de connexion qui fournit des informations sur l'étape de la synchronisation. Il peut être utilisé pour connaître l'état ou dépanner des problèmes potentiels.

Problème

L'état de l'association NTP peut afficher différentes valeurs qui aident à trouver la cause première des problèmes NTP, mais qui ont toujours besoin d'une interprétation lisible par l'homme.

Scénario 1 : la connectivité NTP est correctement établie, le code est 961a.

<#root>

vBond1#

show ntp associations

LAST

IDX ASSOCID

STATUS

 CONF

REACHABILITY

 AUTH

CONDITION

EVENT

 COUNT
----
1   42171

961a

    yes

yes

          none

sys.peer

reachable

```
 1
```

Scénario 2 : la connectivité NTP n'est pas établie, le code est 8023.

```
<#root>
vManage#
show ntp associations

                                                    LAST
IDX ASSOCID
STATUS

CONF

REACHABILITY
 AUTH
CONDITION
 EVENT COUNT
-------------------------------------------------------------------------------
1   14598
  8023

yes

no
          none
reject

mobilize
 1
```

Solution

Interprétation Du Code

Avec ces codes obtenus à partir des scénarios 1 et 2, les informations peuvent être traduites en informations lisibles par l'homme.

- Décoder le premier octet :
    - Scénario 1 : à partir du code obtenu 961a, le premier octet 9 signifie 10+80 (accessible et configuré dans ntp.conf).
    - Scénario 2 : à partir du code 8023 obtenu, le premier octet 8 signifie que le serveur NTP est configuré mais inaccessible.

Code	Message	Description
08	bcst	association de radiodiffusion
10	section droite	hôte joignable
20	authenb	authentification activée
40	authentification	ok
80	configuration	association persistante

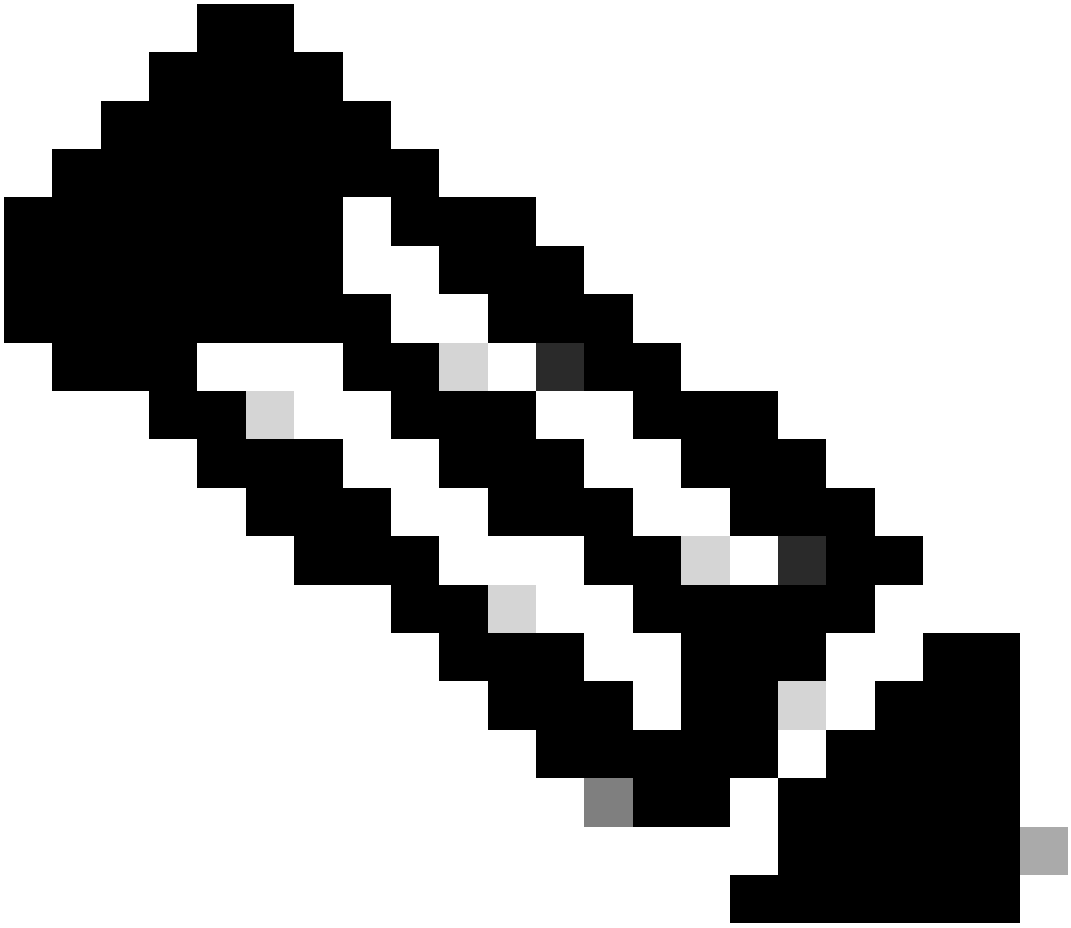
- Décoder le deuxième octet :
    - Scénario 1 : A partir du code obtenu 961a, le deuxième octet 6 signifie qu'il est l'homologue du système.
    - Scénario 2 : à partir du code obtenu 8023, le deuxième octet 0 signifie que le code est rejeté comme non valide.

Code	Message	T	Description
0	sel_reject		ignoré comme non valide (TEST10-TEST13)
1	auto_falsetick	X	abandonné par l'algorithme de croisement
2	auto_excès	.	rejeté par débordement de table (non utilisé)
3	Sel_outlyer	-	ignoré par l'algorithme de cluster
4	sel_candidate	+	inclus dans l'algorithme de combinaison
5	sel_backup	#	sauvegarde (plus de sources tos maxclock)
6	sel_sys.peer	*	homologue système
7	sel_pps.peer	o	homologue PPS (lorsque l'homologue préféré est valide)

- Décoder le troisième et le quatrième octets : le troisième octet est le nombre de fois que le quatrième octet s'est produit.

- Scénario 1 : à partir du code 961a obtenu, les troisième et quatrième octets 1a signifient que le périphérique est devenu homologue système une fois.
- Scénario 2 : à partir du code obtenu 8023, les troisième et quatrième octets 23 signifient que NTP est configuré, inaccessible, rejeté comme non valide et qu'il y a eu deux tentatives pour l'atteindre sans succès.

Code	Message	Description
01	mobiliser	association mobilisée
02	démobilisation	association démobilisée
03	inaccessible	serveur inaccessible
04	accessible	serveur joignable
05	redémarrage	reprise d'association
06	no_reply	aucun serveur trouvé (mode ntpdate)
07	débit_dépassé	taux dépassé (code de baiser TAUX)
08	accès_refusé	accès refusé (code d'embrassement REFUSÉ)
09	saut_armé	saut armé depuis le code LI du serveur
0 bis	sys_peer	devenir homologue système
0b	événement_horloge	voir le mot d'état d'horloge
0 quater	mauvaise_auth	échec de l‘authentification
0d	maïs éclaté	suppresseur d'épi de maïs soufflé
0e	mode_entrelacement	passage en mode entrelacement
0f	erreur_entrelacement	erreur d'entrelacement (récupérée)



Remarque : pour plus d'informations sur les codes d'association NTP, reportez-vous à la RFC5905.

Conclusions

- Le code 961a du scénario 1 signifie que :
  - Le serveur NTP est accessible et configuré dans ntp.conf (octet 9).
  - Il s'agit d'un homologue système (octet 6).
  - Est devenu homologue système une fois (octet 1 et octet a).
- Le code 8023 du scénario 2 signifie que :
  - Le serveur NTP est configuré mais il n'est pas accessible (octet 8).
  - Cela signifie que est rejeté comme non valide (octet 0).
  - Cela signifie que NTP est configuré, inaccessible, rejeté comme non valide et qu'il y a

eu deux tentatives pour l'atteindre sans succès. (octets 2 et 3).

Commandes utiles

Ces commandes peuvent être utilisées à des fins de dépannage NTP en plus de show ntp associations.

- show ntp peer : affiche des informations sur les homologues NTP avec lesquels le logiciel Cisco SD-WAN synchronise ses horloges.
- tcpdump test : le test tcpdump est utile pour confirmer que des paquets sont envoyés et reçus entre les contrôleurs et le serveur NTP.

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.