Comprensión de los códigos de asociación NTP en los controladores SD-WAN

Contenido

Introducción

Prerequisites

- Componentes Utilizados

Antecedentes

Problema

Solución

- Interpretación de código

Conclusiones

Comandos útiles

Introducción

Este documento describe cómo entender los códigos de estado de asociación NTP en los controladores SD-WAN.

Prerequisites

- El servicio NTP debe permitir allow-service ntp dentro de las interfaces de túnel VPN 0 de todos los controladores. Si el servicio no está permitido, utilice este procedimiento para activarlo.

<#root>

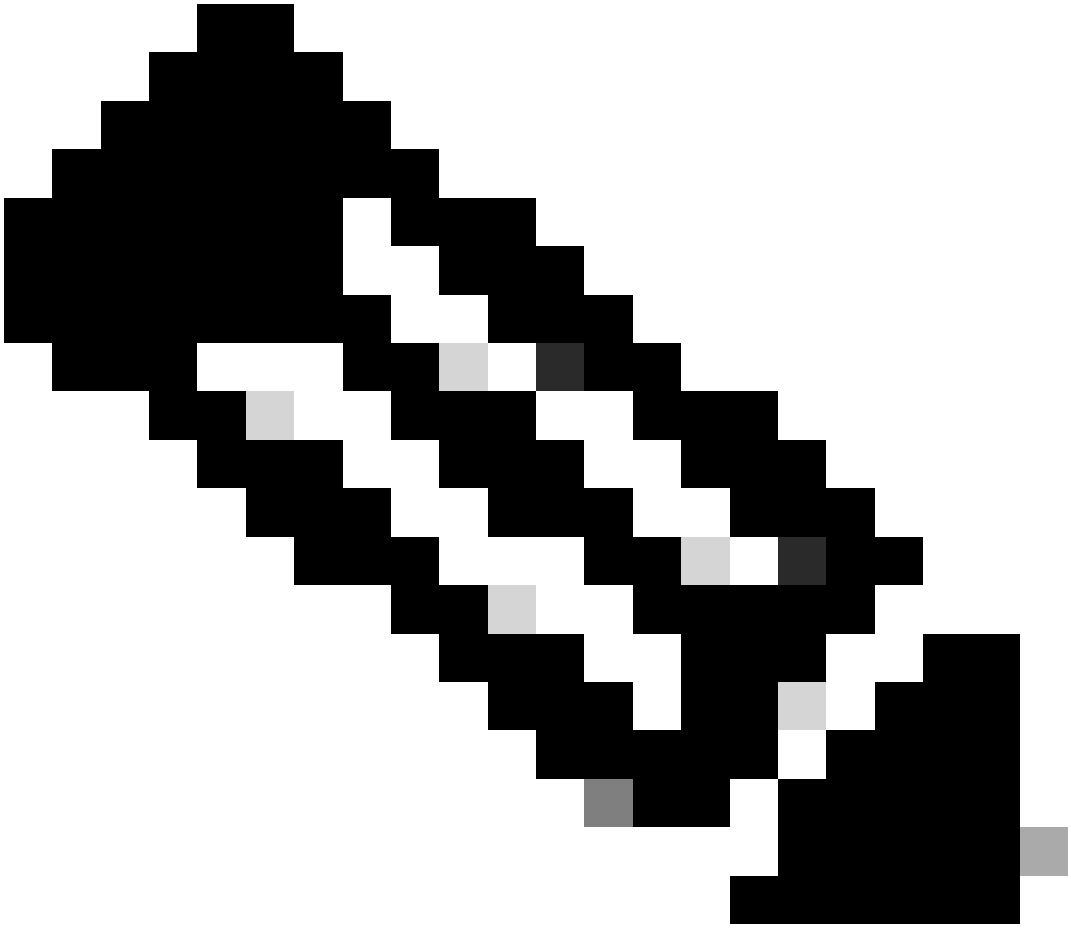
```
config t
vpn 0
!
interface eth1
tunnel-interface
```

allow-service ntp

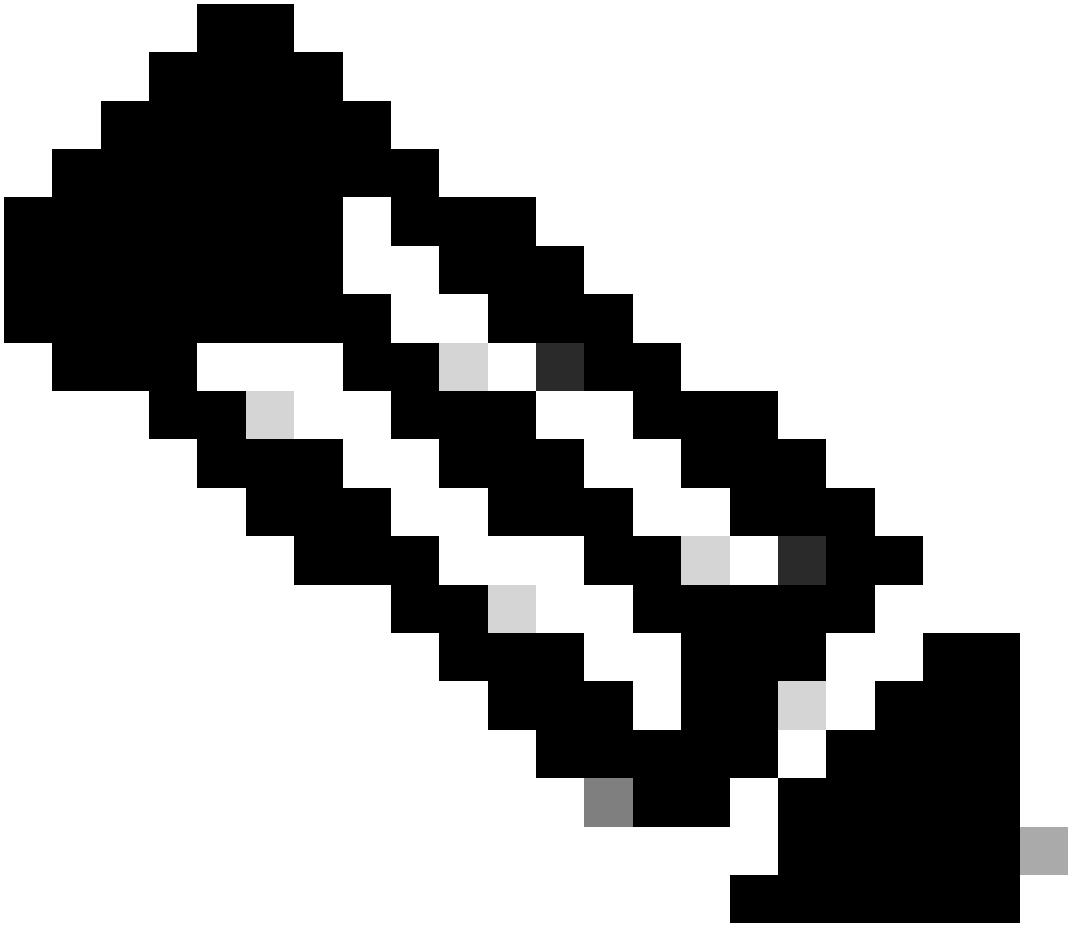
```
!
commit
```

- Todos los controladores también deben tener NTP configurado. Consulte la documentación oficial para configurar NTP a través de CLI o de la plantilla vManage.
- Todos los controladores y todos los nodos de la superposición deben configurarse con el

mismo servidor NTP para que tengan la misma fecha/hora. Un conjunto diferente de fecha/hora puede causar problemas en el establecimiento de la conexión de control.



Nota: para obtener información sobre la configuración de NTP, consulte Configuración de servidores NTP mediante Cisco Vmanage y Configuración de NTP mediante CLI.



Nota: Para obtener más información sobre los problemas de establecimiento de conexión de control, consulte Resolución de Problemas de Conexiones de Control SD-WAN.

Componentes Utilizados

Este documento se basa en las siguientes versiones de software y hardware:

- Controladores SD-WAN versión 20.9.3

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Los controladores SD-WAN se pueden asociar a un servidor de protocolo de tiempo de la red (NTP) para la sincronización del reloj de la red. NTP se basa en el puerto 13 del protocolo de datagramas de usuario (UDP), que proporciona un método de transporte sin conexión.

En Viptela OS, el comando show ntp associations muestra diferentes códigos durante el proceso de conexión que proporcionan información sobre la etapa en la que se encuentra la sincronización. que se puede utilizar para conocer el estado o solucionar posibles problemas.

Problema

El estado de asociación de NTP puede mostrar diferentes valores que ayudan a encontrar la causa raíz de los problemas de NTP, pero aún así necesitan una interpretación legible por las personas.

Situación 1: la conectividad NTP se ha establecido correctamente, el código es 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

Situación 2: no se ha establecido la conectividad NTP, el código es 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

Solución

Interpretación de código

Con estos códigos obtenidos de los escenarios 1 y 2, la información puede traducirse en información legible para el ser humano.

- Descodificar primer byte:
    - Escenario 1: Del código obtenido 961a, el primer byte 9 significa 10+80 (alcanzable y configurado en ntp.conf).
    - Escenario 2: Desde el código 8023 obtenido, el primer byte 8 significa que el servidor NTP está configurado pero no es alcanzable.

Code	Mensaje	Descripción
08	bcst	asociación de broadcast
10	reach (alcance)	host alcanzable
20	autentificar	autenticación habilitada
40	autenticación	ok
80	config	asociación persistente

- Descodificar segundo byte:
    - Escenario 1: Del código obtenido 961a, el segundo byte 6 significa que es el peer del sistema.
    - Escenario 2: Desde el código obtenido 8023, el segundo byte 0 significa que se descarta como no válido.

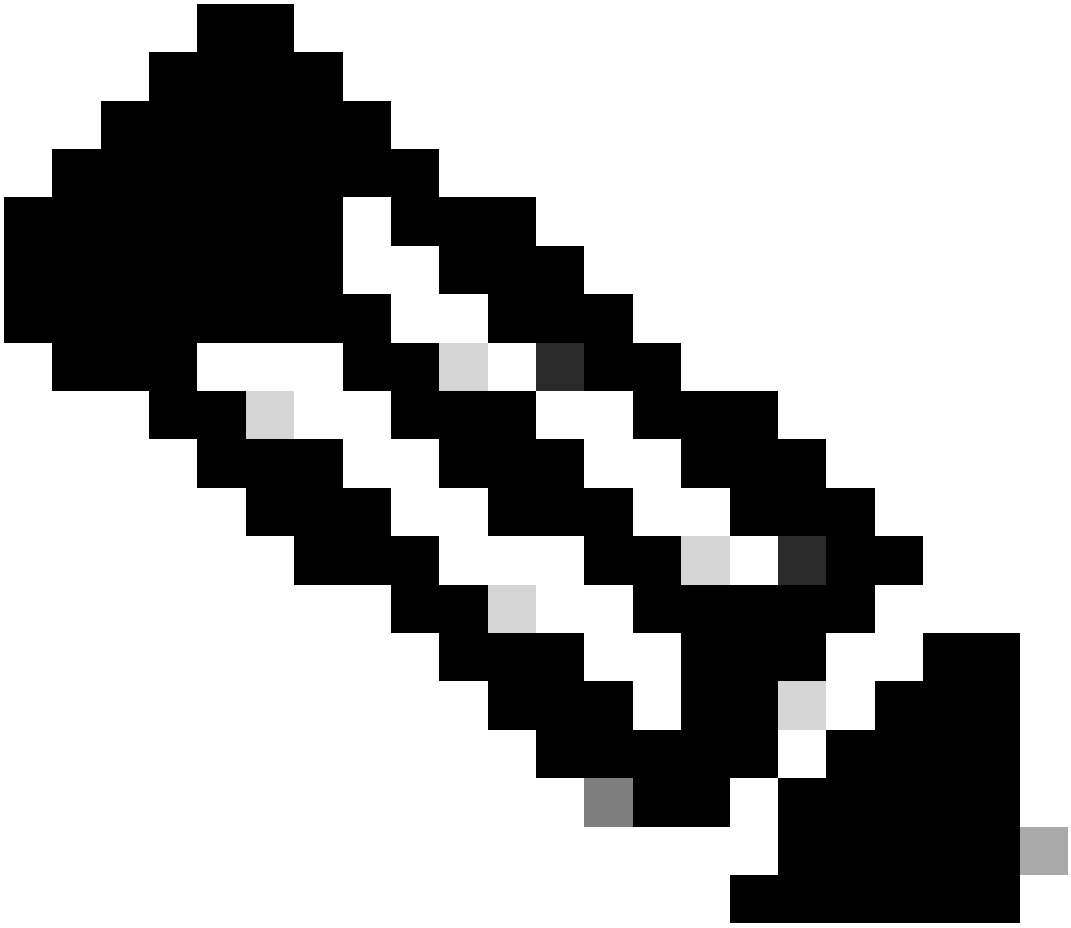
Code	Mensaje	T	Descripción
0	sel_reject		descartado como no válido (TEST10-TEST13)
1	sel_falsetick	X	descartado por el algoritmo de intersección
2	sel_exceso	.	descartado por desbordamiento de tabla (no utilizado)
3	sel_outlyer	-	descartado por el algoritmo de clúster
4	sel_candidate	+	incluido por el algoritmo de combinación
5	sel_backup	#	copia de seguridad (más de dos fuentes maxclock)
6	sel_sys.peer	*	peer del sistema
7	sel_pps.peer	o	PPS peer (cuando el peer

			preferido es válido)

- Descodificar tercer y cuarto byte: El tercer byte es la cuenta de veces que se ha producido el cuarto byte.

    - Escenario 1: Del código obtenido 961a, los bytes tercero y cuarto 1a significan que el dispositivo se ha convertido en peer del sistema una vez.
    - Escenario 2: Del código obtenido 8023 , el tercer y cuarto bytes 23 significan que el NTP está configurado, no es alcanzable, descartado como no válido y ha habido dos intentos de alcanzarlo sin éxito.

Code	Mensaje	Descripción
01	movilizar	asociación movilizada
02	desmovilizar	asociación desmovilizada
03	inalcanzable	Servidor inalcanzable
04	alcanzable	accesible al servidor
05	reiniciar	reinicio de asociación
06	no_reply	no se encontró ningún servidor (modo ntpdate)
07	rate_exceeded	velocidad superada (tasa de código de beso)
08	access_denied	acceso denegado (código de beso DENY)
09	leap_armed	salto armado desde el código LI del servidor
0 a	sys_peer	convertirse en peer del sistema
0 ter	clock_event	consulte clock status word
0 quater	bad_auth	falla de autenticación
0 d	palomitas de maíz	supresor de pico de palomitas
0e	interleave_mode	entrar en modo entrelazado
0f	interleave_error	error de entrelazado (recuperado)



Nota: Para obtener más información sobre los códigos de asociación NTP, consulte RFC5905.

Conclusiones

- El código 961a de la situación 1 significa que:
  - El servidor NTP es accesible y está configurado en ntp.conf (byte 9).
  - Es un par del sistema (byte 6).
  - Se ha convertido en par del sistema una vez (byte 1 y byte a).
- El código 8023 de la situación 2 significa que:
  - El servidor NTP está configurado pero no es alcanzable (byte 8).
  - Esto significa que se descarta como no válido (byte 0).
  - Esto significa que el NTP está configurado, no es accesible, se descarta como no

válido y ha habido dos intentos de alcanzarlo sin éxito. (byte 2 y byte 3).

Comandos útiles

Estos comandos se pueden utilizar para solucionar problemas de NTP, además de show ntp associations.

- show ntp peer: muestra información sobre los peers NTP con los que el software Cisco SD-WAN está sincronizando sus relojes.
- tcpdump test: La prueba de tcpdump es útil para confirmar que hay paquetes que se envían y reciben entre los controladores y el servidor NTP.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).