

Entender códigos de associação NTP em controladores SD-WAN

Contents

[Introdução](#)

[Pré-requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Problema](#)

[Solução](#)

[Interpretação de código](#)

[Conclusões](#)

[Comandos úteis](#)

Introdução

Este documento descreve como entender os códigos de status de associação NTP em controladores SD-WAN.

Pré-requisitos

- O serviço NTP deve ter permissão de `allow-service ntp` dentro das interfaces de túnel VPN 0 de todos os controladores. Se o serviço não for permitido, use este procedimento para ativá-lo.

<#root>

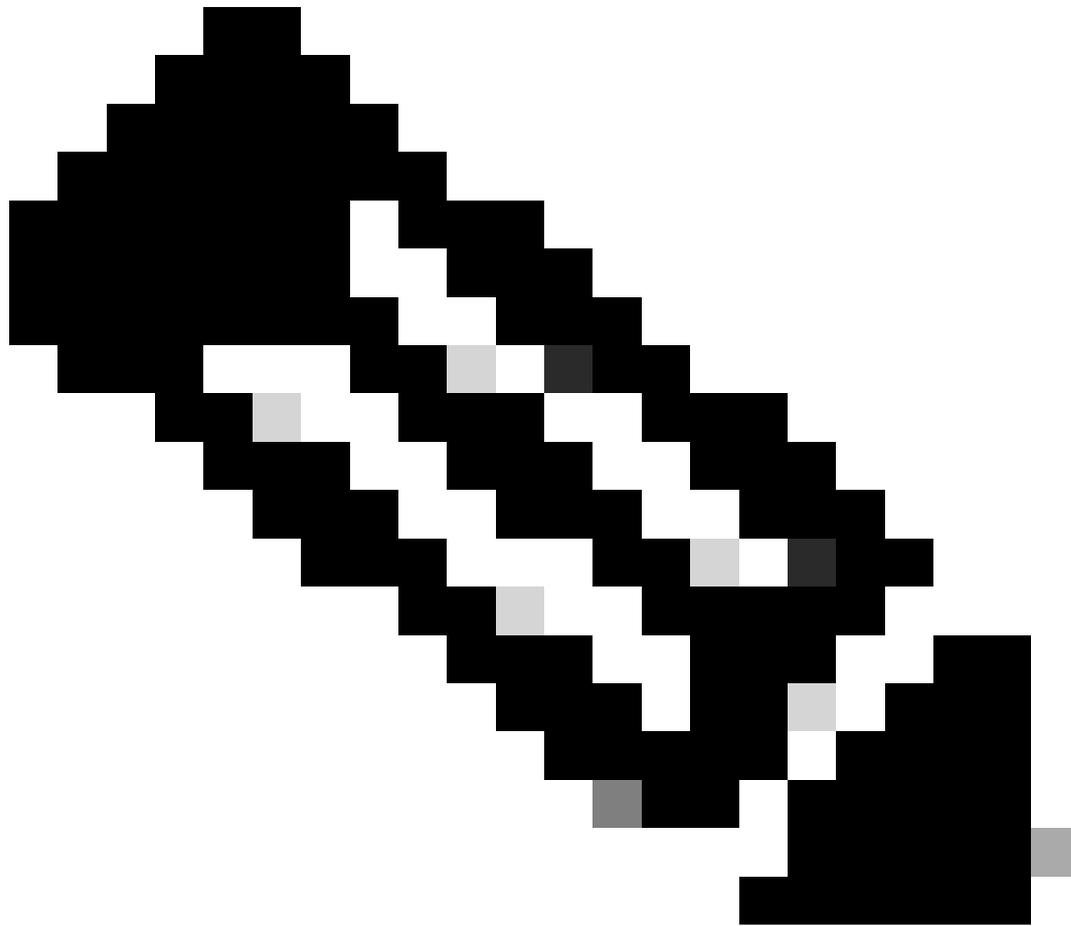
```
config t
vpn 0
!
interface eth1
tunnel-interface

allow-service ntp

!
commit
```

- Todos os controladores também devem ter o NTP configurado. Consulte a documentação oficial para configurar o NTP via CLI ou Modelo vManage.
- Todos os controladores e todos os nós na sobreposição devem ser configurados com o

mesmo servidor NTP para terem a mesma data/hora. Um conjunto diferente de data/hora pode causar problemas no estabelecimento da conexão de controle.



Observação: para a configuração NTP, consulte [Configurar servidores NTP usando o Cisco Vmanage e Configurar NTP usando CLI.](#)



Observação: para obter referência adicional sobre problemas de estabelecimento de conexão de controle, consulte [Troubleshooting de Conexões de Controle SD-WAN](#).

Componentes Utilizados

Este documento é baseado nestas versões de software e hardware:

- Controladores SD-WAN versão 20.9.3

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Os controladores SD-WAN podem ser associados a um servidor Network Time Protocol (NTP) para a sincronização do relógio da rede. O NTP é construído na porta 13 do Protocolo de Datagrama de Usuário (UDP - User Datagram Protocol) que fornece um método de transporte sem conexão.

No Viptela OS, o comando `show ntp associations` exibe diferentes códigos durante o processo de conexão que fornecem informações sobre o estágio em que a sincronização está. Pode ser usado para saber o status ou solucionar possíveis problemas.

Problema

O status da associação NTP pode mostrar valores diferentes que ajudam a encontrar a causa raiz dos problemas de NTP, mas ainda precisam de uma interpretação legível por humanos.

Cenário 1: a conectividade NTP foi estabelecida com êxito, o código é 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
```

Cenário 2: a conectividade NTP não está estabelecida; o código é 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
```

Solução

Interpretação de código

Com esses códigos obtidos nos cenários 1 e 2, as informações podem ser traduzidas em informações legíveis por humanos.

- Decodificar primeiro byte:
 - Cenário 1: A partir do código 961a obtido, o primeiro byte 9 significa 10+80 (alcançável e configurado em ntp.conf).
 - Cenário 2: A partir do código 8023 obtido, o primeiro byte 8 significa que o servidor NTP está configurado, mas não está acessível.

Code	Mensagem	Descrição
08	bcst	associação de transmissão
10	alcance	host alcançável
20	authenb	autenticação habilitada
40	Autenticação	ok
80	config	associação persistente

- Decodificar segundo byte:
 - Cenário 1: a partir do código 961a obtido, o segundo byte 6 significa que é o peer do sistema.
 - Cenário 2: A partir do código obtido 8023, o segundo byte 0 significa que não é válido.

Code	Mensagem	T	Descrição
0	sel_reject		descartado como inválido (TEST10-TEST13)
1	sel_falsetick	X	descartado pelo algoritmo de interseção
2	sel_excess	.	descartado pelo estouro de tabela (não usado)
3	sel_outlier	-	descartado pelo algoritmo de cluster
4	sel_candidate	+	incluído pelo algoritmo de combinação
5	sel_backup	#	backup (mais do que origens do tos maxclock)
6	sel_sys.peer	*	peer de sistema
7	sel_pps.peer	o	PPS peer (quando o peer de preferência é válido)

- Decodificar terceiro e quarto bytes: Terceiro byte é a contagem de vezes que o quarto byte ocorreu.
 - Cenário 1: a partir do código 961a obtido, o terceiro e o quarto bytes 1a significam que o dispositivo se tornou o peer do sistema uma vez.
 - Cenário 2: Do código obtido 8023 , o terceiro e o quarto bytes 23 significam que o NTP está configurado, não alcançável, descartado como inválido e houve duas tentativas de alcançá-lo sem sucesso.

Code	Mensagem	Descrição
01	mobilizar	associação mobilizada
02	desmobilizar	associação desmobilizada
03	Não Acessível	Servidor inalcançável
04	alcançável	servidor alcançável
05	reiniciar	reinicialização de associação
06	no_reply	nenhum servidor encontrado (modo ntpdate)
07	taxa_excedida	taxa excedida (código de beijo TAXA)
08	acesso_negado	acesso negado (código de beijo DENY)
09	leap_armed	salto armado a partir do código LI do servidor
0a	sys_peer	tornar-se peer do sistema
0b	evento_relógio	ver palavra de status do relógio
0c	bad_auth	falha na autenticação
0d	pipoca	protetor antispico de pipoca
0e	interleave_mode	entrando no modo interleave
0f	erro_intercalação	erro de intercalação (recuperado)



Observação: para obter mais referências sobre códigos de associação NTP, consulte [RFC5905](#).

Conclusões

- O código 961a do cenário 1 significa que:
 - O servidor NTP está acessível e configurado em ntp.conf (byte 9).
 - É um peer de sistema (byte 6).
 - Tornou-se peer do sistema uma vez (byte 1 e byte a).
- O código 8023 do cenário 2 significa que:
 - O servidor NTP está configurado, mas não está acessível (byte 8).
 - Isso significa que é descartado como inválido (byte 0).
 - Isso significa que o NTP está configurado, inalcançável, descartado como inválido, e

houve duas tentativas de alcançá-lo sem sucesso. (byte 2 e byte 3)

Comandos úteis

Esses comandos podem ser usados para fins de identificação e solução de problemas do NTP, além de mostrar associações ntp.

- `show ntp peer`: Exibe informações sobre os peers NTP com os quais o software Cisco SD-WAN está sincronizando seus relógios.
- `tcpdump test`: O teste `Tcpdump` é útil para confirmar que há pacotes sendo enviados e recebidos entre os controladores e o servidor NTP.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.