

NTP-Zuordnungs-codes in SD-WAN-Controllern verstehen

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Problem](#)

[Lösung](#)

[Code-Interpretation](#)

[Schlussfolgerungen](#)

[Nützliche Befehle](#)

Einleitung

In diesem Dokument wird erläutert, wie Sie NTP-Zuordnungsstatuscodes auf SD-WAN-Controllern verstehen.

Voraussetzungen

- Der NTP-Dienst muss "allow-service ntp" innerhalb der VPN 0-Tunnelschnittstellen aller Controller zugelassen sein. Wenn der Dienst nicht zulässig ist, verwenden Sie dieses Verfahren, um ihn zu aktivieren.

```
<#root>
```

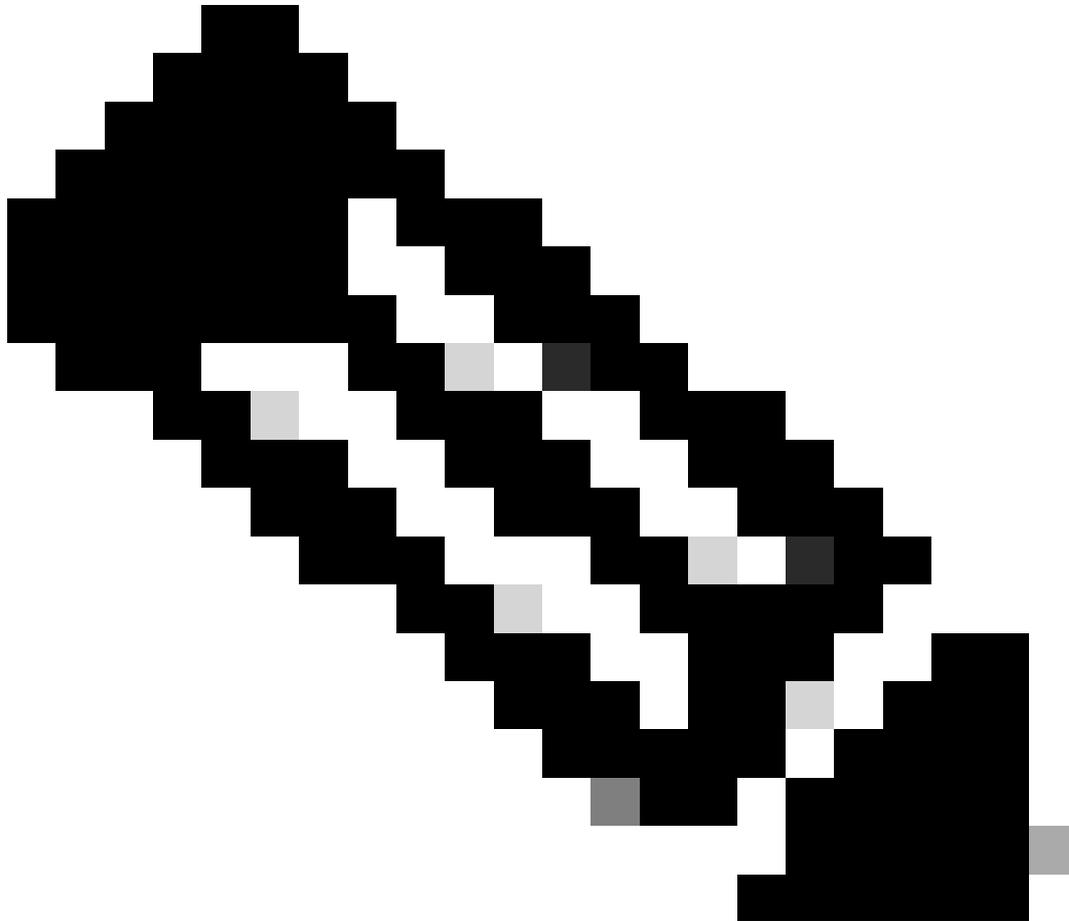
```
config t
vpn 0
!
interface eth1
tunnel-interface

allow-service ntp

!
commit
```

- Auf allen Controllern muss außerdem NTP konfiguriert sein. Informationen zur NTP-Konfiguration über die CLI oder die vManage-Vorlage finden Sie in der offiziellen Dokumentation.

- Alle Controller und alle Knoten im Overlay müssen mit demselben NTP-Server konfiguriert werden, damit das Datum/die Stunde identisch ist. Ein anderes Datum/eine andere Stunde kann zu Problemen beim Herstellen der Steuerverbindung führen.
-



Hinweis: Weitere Informationen zur NTP-Konfiguration finden Sie unter [Konfigurieren von NTP-Servern mit Cisco Vmanage und Konfigurieren von NTP mit CLI.](#)



Hinweis: Weitere Informationen zum Herstellen der Steuerverbindung finden Sie unter [Problembehandlung bei SD-WAN-Steuerverbindungen](#).

Verwendete Komponenten

Dieses Dokument basiert auf den folgenden Software- und Hardwareversionen:

- SD-WAN-Controller Version 20.9.3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

SD-WAN-Controller können einem NTP-Server (Network Time Protocol) zur Synchronisierung der Netzwerkuhr zugeordnet werden. NTP basiert auf dem User Datagram Protocol (UDP)-Port 13, der eine verbindungslose Transportmethode bereitstellt.

In Viptela OS zeigt der Befehl `show ntp associations` während des Verbindungsprozesses verschiedene Codes an, die Informationen über die Phase liefern, in der die Synchronisierung läuft. Damit können Sie den Status ermitteln oder potenzielle Probleme beheben.

Problem

Der NTP-Zuordnungsstatus kann verschiedene Werte anzeigen, mit denen die Ursache von NTP-Problemen leichter ermittelt werden kann, die aber dennoch eine für Menschen lesbare Interpretation erfordern.

Szenario 1: NTP-Verbindung wurde erfolgreich hergestellt, Code lautet 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

Szenario 2: Keine NTP-Verbindung hergestellt, Code 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

Lösung

Code-Interpretation

Mithilfe dieser aus Szenario 1 und 2 gewonnenen Codes können Informationen in für Menschen lesbare Informationen übersetzt werden.

- Erstes Byte decodieren:
 - Szenario 1: Aus dem erhaltenen Code 961a bedeutet das erste Byte 9 10+80 (erreichbar und konfiguriert in ntp.conf).
 - Szenario 2: Aus dem erhaltenen Code 8023 bedeutet das erste Byte 8, dass der NTP-Server konfiguriert, aber nicht erreichbar ist.

Code	Nachricht	Beschreibung
08	BCST	Rundfunkgesellschaft
10	erreichen	Host erreichbar
20	authentisch	Authentifizierung aktiviert
40	authentifizierung	OK
80	konfig.	beständige Assoziation

- Zweites Byte decodieren:
 - Szenario 1: Aus dem erhaltenen Code 961a bedeutet das zweite Byte 6, dass es sich um den System-Peer handelt.
 - Szenario 2: Aus dem erhaltenen Code 8023 bedeutet das zweite Byte 0, dass als ungültig verworfen wird.

Code	Nachricht	T	Beschreibung
0	sel_reject		verworfen als ungültig (TEST10-TEST13)
1	sel_falsetick	X	durch Kreuzungsalgorithmus verworfen
2	Selbstüberschuss.		durch Tabellenüberlauf verworfen (nicht verwendet)
3	Selbstauser	-	vom Clusteralgorithmus verworfen
4	sel-Kandidat	+	vom Kombinationsalgorithmus eingeschlossen
5	sel_backup	Nr.	Backup (mehr als tos maxclock sources)
6	sel_sys.peer	*	System-Peer
7	sel_pps.peer	o	PPS-Peer (wenn bevorzugter)

			Peer gültig ist)
--	--	--	------------------

- Decodiertes drittes und viertes Byte: Das dritte Byte ist die Anzahl der Male, die das vierte Byte aufgetreten ist.
 - Szenario 1: Aus dem erhaltenen Code 961a bedeuten drittes und viertes Byte 1a, dass das Gerät einmal zum System-Peer geworden ist.
 - Szenario 2: Aus dem erhaltenen Code 8023 bedeuten drittes und viertes Byte 23, dass das NTP konfiguriert ist, nicht erreichbar ist, als ungültig verworfen wurde und dass zwei Versuche unternommen wurden, es ohne Erfolg zu erreichen.

Code	Nachricht	Beschreibung
01	mobilisieren	Verband mobilisiert
02	demobilisieren	Verein demobilisiert
03	unerreichbar	Server nicht erreichbar
04	erreichbar	Server erreichbar
05	Neustart	Assoziationsneustart
06	Keine Antwort	Kein Server gefunden (ntpdate-Modus)
07	Rate überschritten	Rate überschritten (Kiss-Code RATE)
08	Zugriff verweigert	Zugriff verweigert (Kusscode DENY)
09	sprunghaft	Sprung vom Server-LI-Code
0a	sys_peer	zu System-Peer
0 b	Uhrenereignis	siehe Taktstatuswort
0c	schlecht_auth	authentifizierungsfehler.
0 d	Popcorn	Popcornspitzenunterdrücker
0e	Verschachtelungsmodus	Eintritt in den Interleaving-Modus
0f	interleave_error	Verschachtelungsfehler (wiederhergestellt)



Hinweis: Weitere Informationen zu NTP-Zuordnungs-codes finden Sie unter [RFC5905](https://www.rfc-editor.org/rfc/rfc5905).

Schlussfolgerungen

- Code 961a aus Szenario 1 bedeutet, dass
 - Der NTP-Server ist erreichbar und in ntp.conf (Byte 9) konfiguriert.
 - Es ist ein System-Peer (Byte 6).
 - Wurde einmal zu einem System-Peer (Byte 1 und Byte a).
- Code 8023 aus Szenario 2 bedeutet, dass
 - Der NTP-Server ist konfiguriert, aber nicht erreichbar (Byte 8).
 - Dies bedeutet, dass als ungültig verworfen wird (Byte 0).
 - Das bedeutet, dass das NTP konfiguriert, nicht erreichbar und als ungültig verworfen wurde. Es wurden zwei erfolglose Versuche unternommen, das NTP zu erreichen.

(Byte 2 und Byte 3).

Nützliche Befehle

Diese Befehle können für die NTP-Fehlerbehebung verwendet werden und zusätzlich NTP-Zuordnungen anzeigen.

- `show ntp peer`: Zeigt Informationen zu den NTP-Peers an, mit denen die Uhren der Cisco SD-WAN-Software synchronisiert werden.
- `tcpdump test`: Der Tcpcmdump-Test ist nützlich, um zu bestätigen, dass Pakete zwischen den Controllern und dem NTP-Server gesendet und empfangen werden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.