

ACS 5.x: Konfigurationsbeispiel für die Cisco ACS-Synchronisierung mit NTP-Server

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[NTP-Konfiguration auf Cisco ACS](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Problem: Die Uhr drift zu viel und NTP schlägt fehl, wenn ACS auf einem VMWare-Rechner installiert ist](#)

[Lösung](#)

[NTP-Synchronisierung verloren, nachdem die IP-Adresse der Schnittstelle von ACS geändert wurde](#)

[Lösung](#)

[Zugehörige Informationen](#)

Einführung

Network Time Protocol (NTP) ist ein Protokoll zur Synchronisierung der Uhren verschiedener Netzwerkeinheiten. Er verwendet UDP/123. Das Hauptziel bei der Verwendung dieses Protokolls besteht darin, die Auswirkungen einer variablen Latenz über die Datennetze zu vermeiden.

Dieses Dokument enthält eine Beispielkonfiguration für den Cisco ACS zur Synchronisierung der Uhr mit dem NTP-Server. ACS 5.x kann bis zu zwei NTP-Server konfigurieren.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Secure ACS Version 5.x

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

NTP-Konfiguration auf Cisco ACS

Gehen Sie wie folgt vor, um die Uhrzeit des Cisco ACS mit einem NTP-Server zu synchronisieren:

1. Konfigurieren Sie Datum und Uhrzeit manuell mit dem Befehl [clock set <month> <hh:min:ss> <yyyy>](#).
2. Geben Sie die Zeitzone mit dem Befehl [clock timezone <timezone> an](#).
3. Geben Sie den NTP-Server mit dem Befehl [<IP-Adresse des NTP-Servers> an](#). NTP folgt einer Client-Server-Hierarchie. Wenn ein NTP-Client mit einem NTP-Server konfiguriert ist, wird die *Referenzzeit* des NTP-Servers an den Client übergeben. Die genaue Zeitangabe vom NTP-Server dauert ca. 10-20 Minuten, abhängig von der Verzögerung beim Erreichen des NTP-Servers. Cisco ACS verwendet den NTP-Daemon, um seine Uhr mit dem NTP-Server zu synchronisieren. Es unterstützt kein Simple NTP, SNTP. Wenn der NTP-Daemon startet, sendet der ACS ein Paket an den NTP-Server, das die ursprüngliche Uhrzeit (Lokal) enthält. Anschließend antwortet der NTP-Server mit dem Einfügen der Referenzzeit auf das Paket. Sobald der NTP-Client dieses Paket empfängt, protokolliert er das Paket mit seiner eigenen lokalen Uhrzeit, um die vom Paket benötigte Reisezeit zu validieren. Mehrere solche Paketaustauschvorgänge dienen zur Berechnung der genauen Round-Trip-Verzögerungszeit und der Offset-Werte. Schließlich wird die lokale Zeit des NTP-Clients mit der Referenzzeit des NTP-Servers synchronisiert.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Weitere Informationen zum Überprüfen der Konfigurationsdetails finden Sie in diesen Ausgabeschnitten.

```
acs51/admin#show clock
Wed Jun 13 11:02:00 IST 2012
acs51/admin#
```

```
acs51/admin(config)#ntp server 192.168.26.55
The NTP server was modified.
If this action resulted in a clock modification, you must restart ACS.
acs51/admin(config)#
```

```
acs51/admin#show ntp
Primary NTP      : 192.168.26.55
```

```
synchronised to NTP server (192.168.26.55) at stratum 2
  time correct to within 27 ms
  polling server every 64 s
```

remote	refid	st	t	when	poll	reach	delay	offset	jitter
127.127.1.0	LOCAL(0)	10	l	29	64	17	0.000	0.000	0.001
*192.168.26.55	.LOCL.	1	u	33	64	17	0.285	-9.900	2.733

Warning: Output results may conflict during periods of changing synchronization.

Hinweis: *Stratum* ist eine Maßnahme, die angibt, wie nah der NTP-Server an die primäre Referenzzeit ist. Jeder NTP-Client, der mit einem Schicht-*n*-Server synchronisiert wird, wird als Schicht-*n*+1-Client bezeichnet.

Überprüfen Sie anhand dieser Anwendungsprotokollmeldungen des ACS die NTP-Synchronisierungsdetails.

```
acs51/admin# show logging application | in ntp
Jun 13 13:51:59 acs51 ntpd[20259]: ntpd 4.2.0a@1.1190-r Mon Jul 28 11:03:50 EDT 2008 (1)
Jun 13 13:51:59 acs51 ntpd[20259]: precision = 1.000 usec
Jun 13 13:51:59 acs51 ntpd[20259]: Listening on interface wildcard, 0.0.0.0#123
Jun 13 13:51:59 acs51 ntpd[20259]: Listening on interface wildcard, ::#123
Jun 13 13:51:59 acs51 ntpd[20259]: Listening on interface lo, 127.0.0.1#123
Jun 13 13:51:59 acs51 ntpd[20259]: Listening on interface eth0, 192.168.26.51#123
Jun 13 13:51:59 acs51 ntpd[20259]: kernel time sync status 0040
Jun 13 13:51:59 acs51 ntpd[20259]: frequency initialized 0.000 PPM from /var/lib/ntp/drift
Jun 13 13:51:59 acs51 ntpd: ntpd startup succeeded
Jun 13 13:55:15 acs51 ntpd[20259]: synchronized to 192.168.26.55, stratum 2
```

!--- Output suppressed--

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des Befehls show** anzuzeigen.

[Fehlerbehebung](#)

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

[Problem: Die Uhr drift zu viel und NTP schlägt fehl, wenn ACS auf einem VMWare-Rechner installiert ist](#)

Der Cisco ACS ist so konfiguriert, dass er den NTP-Server als Taktquelle verwendet, er wechselt jedoch kontinuierlich zur internen Zeitquelle. In diesem Fall können Benutzer sich nicht über Active Directory authentifizieren, da Kerberos nur 300 Sekunden Zeitdifferenz unterstützt.

Lösung

Wenn der ESXi-Host über eine hohe CPU-Auslastung verfügt, werden VMs nicht so häufig unterstützt wie normal. Dies wirkt sich auf die Uhren in VMs aus und führt dazu, dass die Taktzyklen von einem Windows Domain Controller über fünf Minuten hinweg abweichen. Es verursacht den Ausfall des Kerberos. Dies würde sich auch auf eine Windows VM ohne NTP- oder Host-Uhrensynchronisierung auswirken. Da die virtuelle Uhr, die dem Cisco ACS präsentiert wird, für NTP nicht stabil genug ist, um mit der Abweichung Schritt zu halten, wird sie letztendlich wieder als Zeitquelle verwendet.

Hinweis: Der NTP-Daemon passt die Uhr an mehreren Exchange an und fährt fort, bis der Client die genaue Zeit erhält. Wenn die Verzögerung zwischen dem NTP-Server und dem NTP-Client jedoch zu groß wird, wird der NTP-Daemon beendet. Sie müssen die Zeit manuell anpassen und den NTP-Daemon neu starten.

Dieses Problem kann behoben werden, wenn Sie die Unterstützung für VMWare-Tools in das Cisco ACS integrieren, das mit Cisco ACS Version 5.4 verfügbar ist und noch nicht veröffentlicht wird. Weitere Informationen finden Sie unter Cisco Bug ID [CSCtg50048](#) (nur [registrierte](#) Kunden). Als temporäre Lösung können Sie die folgenden Schritte ausführen:

- Beenden Sie ACS-Dienste mit dem Befehl **ACS stop**.
- Entfernen Sie alle NTP-Konfigurationen, und speichern Sie die Konfiguration mit einem Befehl **write mem**.
- Starten Sie den Cisco ACS neu.
- Stellen Sie sicher, dass alle Dienste mit dem Befehl **show application status acs** ausgeführt werden.
- Stellen Sie die Uhr so nahe wie möglich an der Echtzeit ein, bis zur zweiten vor der Offset-Anforderung für NTP.
- Stellen Sie sicher, dass die Zeitzone die richtige ist.
- NTP-Konfiguration erneut hinzufügen und speichern
- Führen Sie den Befehl **show ntp** aus, um zu überprüfen, ob die Ausgabe identisch ist.

Hinweis: Wenn das Problem mit diesen Schritten nicht behoben werden kann, sollten Sie sich an das [Cisco TAC](#) wenden.

NTP-Synchronisierung verloren, nachdem die IP-Adresse der Schnittstelle von ACS geändert wurde

Wenn Sie die IP-Adresse der ACS-Netzwerkkarte ändern, führt dies dazu, dass das NTP nicht mehr synchronisiert wird.

Lösung

Dieses Verhalten wird beobachtet und in der Cisco Bug-ID [CSCtk76151](#) protokolliert (nur [registrierte](#) Kunden). Wenn die ACS-IP-Adresse geändert wird, wird die ACS-Anwendung neu gestartet, jedoch nicht der NTP-Daemon. Es wurde in ACS Version 5.3.0.23 behoben. Gehen Sie wie folgt vor, um dieses Problem in früheren Versionen zu beheben:

1. Geben Sie den Befehl **no ntp server** ein, um den NTP-Prozess zu beenden.
2. Führen Sie den Befehl **ntp server** erneut aus, um den NTP-Prozess neu zu starten.

Zugehörige Informationen

- [Produkt-Support für CS ACS 5.X](#)
- [Benutzerhandbuch zum Cisco Secure Access Control System 5.3](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)