

ASA 8.x: Cisco ASA im Multiple-Context-Modus Synchronisiert mit NTP-Server - Konfigurationsbeispiel

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[ASDM-Konfiguration](#)

[FWSM im Multiple-Context-Modus als NTP-Client](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Fehler: Peer/Server-Uhr nicht synchronisiert](#)

[Problem: Die Uhr kann nicht mit dem NTP-Server synchronisiert werden.](#)

[Befehle zur Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

Dieses Dokument enthält eine Beispielkonfiguration, wie die Uhr der Cisco Adaptive Security Appliance (ASA) im Multiple-Context-Modus mit der des NTP-Servers (Network Time Protocol) synchronisiert wird.

NTP ist ein Protokoll zur Synchronisierung der Uhren verschiedener Netzwerkeinheiten. Er verwendet UDP/123. Der Hauptgrund für die Verwendung dieses Protokolls besteht darin, die Auswirkungen variabler Latenz über die Datennetze zu vermeiden.

In diesem Szenario befindet sich die Cisco ASA im Multiple-Context-Modus. Admin und Test1 sind die beiden unterschiedlichen Kontexte. Um die Cisco ASA als NTP-Client zu konfigurieren, müssen Sie den **Befehl [NTP-Server](#)** nur im Bereich der Systemausführung angeben, da dieser Befehl den Kontextmodus nicht unterstützt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

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

- Cisco ASA mit Softwareversion 8.2 oder höher
- Cisco Adaptive Security Device Manager (ASDM) mit Softwareversion 6.3 und höher

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).

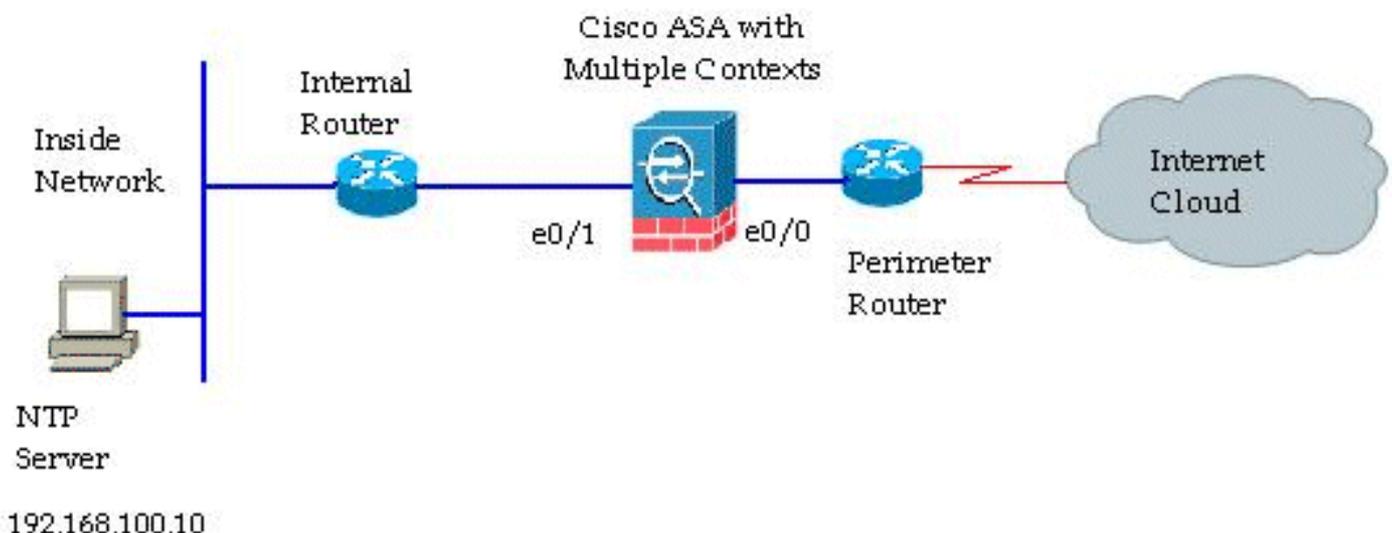
Konfigurieren

In diesem Abschnitt werden die Informationen angezeigt, die zum Konfigurieren der in diesem Dokument beschriebenen Funktionen erforderlich sind.

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

Netzwerkdiagramm

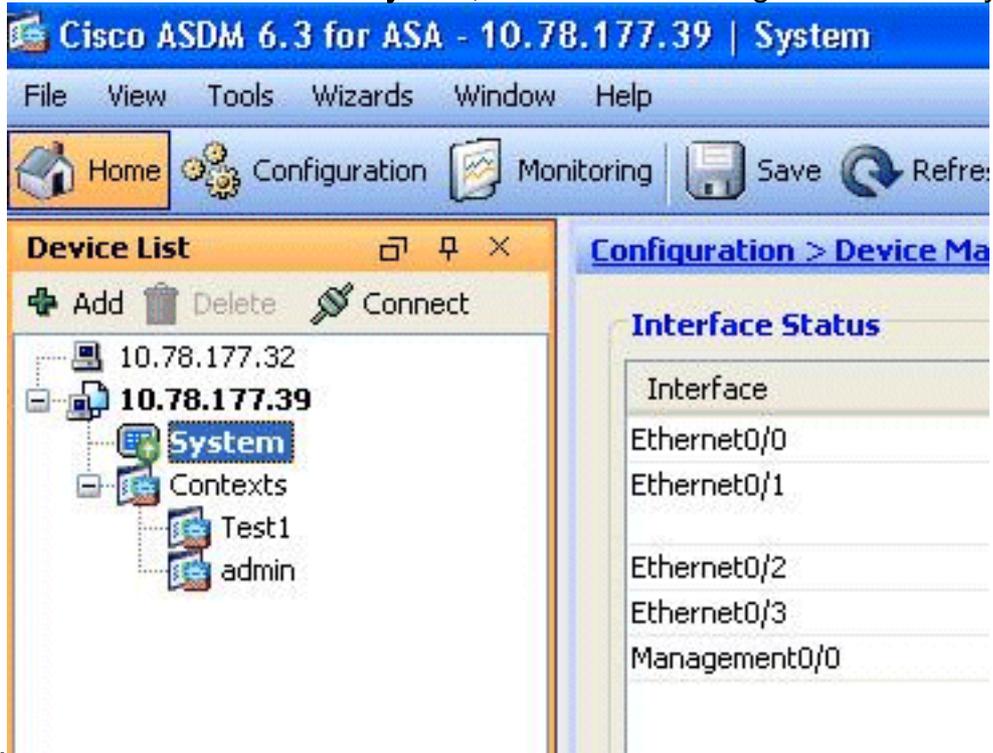
In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



ASDM-Konfiguration

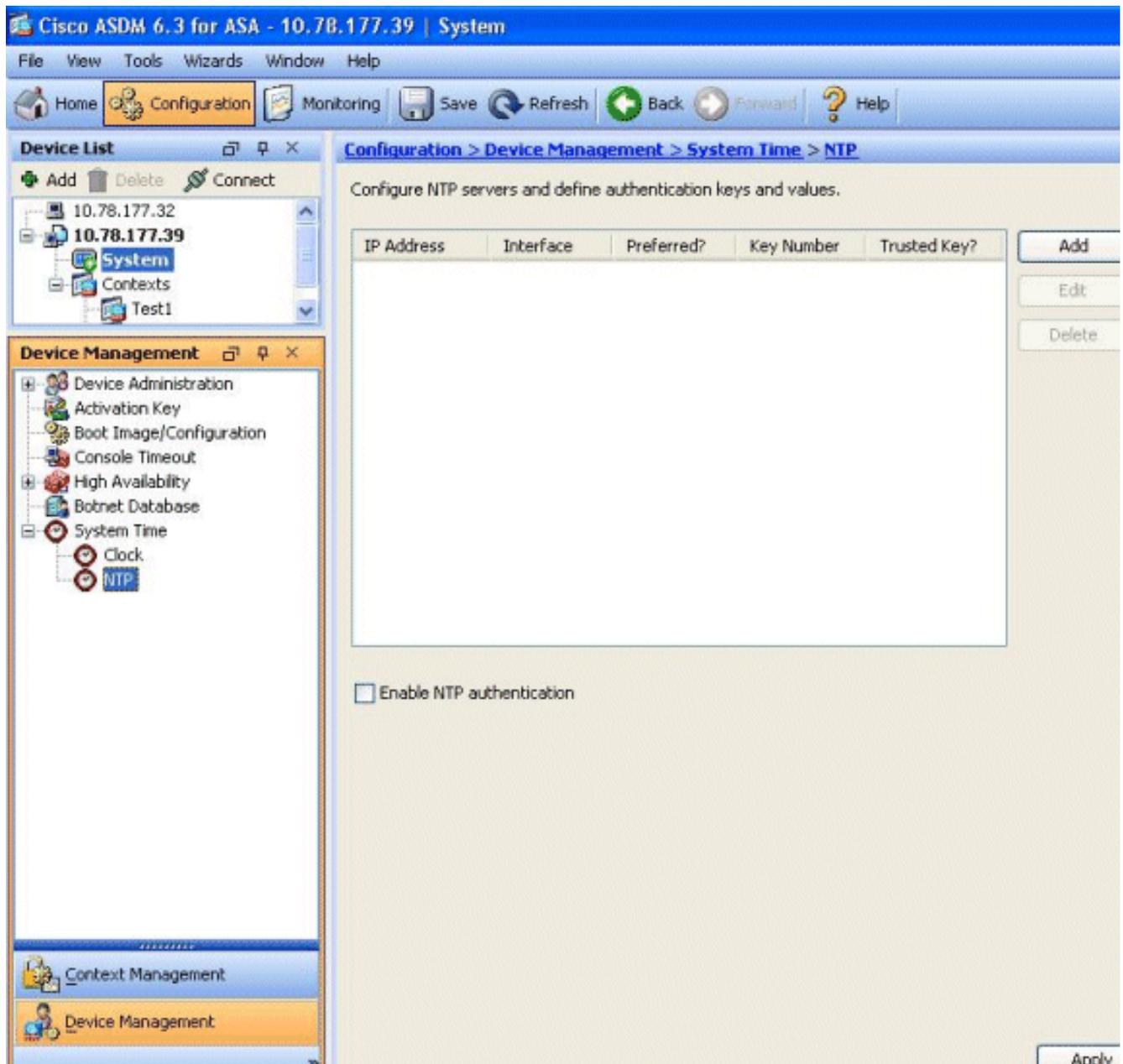
Gehen Sie wie folgt vor, um das ASDM zu konfigurieren:

1. Klicken Sie unter der Cisco ASA auf **System**, um den Ausführungsbereich des Systems zu



überprüfen.

2. Gehen Sie zu **Konfiguration > Gerätemanagement > Systemzeit > NTP**, und klicken Sie auf **Hinzufügen**.



3. Das Fenster NTP-Serverkonfiguration hinzufügen wird angezeigt. Geben Sie die IP-Adresse der Schnittstelle an, die dem NTP-Server zugeordnet ist, und geben Sie die Details des Authentifizierungsschlüssels an. Klicken Sie auf

Add NTP Server Configuration

IP Address: 192.168.100.10 Preferred

Interface: inside

Authentication Key

Key Number: 10 Trusted

Key Value: ●●●●●

Re-enter Key Value: ●●●●●

OK Cancel Help

OK. **Hinweis:** NTP-

Serverdetails sollten im Kontext-System angegeben werden. Da der Systemausführungsbereich jedoch keine Schnittstellen im Multiple-Context-Modus enthält, müssen Sie einen Schnittstellennamen angeben (d. h., dieser wird im Admin-Kontext definiert).

4. Hier sehen Sie die Details zum NTP-Server:

Configuration > Device Management > System Time > NTP

Configure NTP servers and define authentication keys and values.

IP Address	Interface	Preferred?	Key Number	Trusted Key?
192.168.100.10	inside	No	10	No

Add Edit Delete

Enable NTP authentication

Dies ist die entsprechende CLI-Konfiguration der Cisco ASA, zu Ihrer Referenz:

Cisco ASA

```
ciscoasa# show run
: Saved
:
ASA Version 8.2(1) <system>
!
terminal width 511
hostname ciscoasa
enable password 2KFQnbNIdI.2KYOU encrypted
no mac-address auto
!
interface Ethernet0/0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
 shutdown
!
interface Management0/0
 shutdown
!
class default
  limit-resource All 0
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
!
ftp mode passive
clock timezone GMT 0
pager lines 10
no failover
asdm image disk0:/asdm-635.bin
asdm history enable
arp timeout 14400
console timeout 0

admin-context admin
context admin
  allocate-interface Ethernet0/0
  allocate-interface Ethernet0/1
  allocate-interface Ethernet0/2
  allocate-interface Ethernet0/3
  config-url disk0:/admin.cfg
!

context Test1
  allocate-interface Ethernet0/1
  allocate-interface Ethernet0/3
  config-url disk0:/Test1.cfg
!
!--- This command is used to set a key to !---
authenticate with an NTP server. ntp authentication-key
10 md5 *
!--- This command is used to configure the !--- NTP
server IP address and the interface associated. ntp
server 192.168.100.10 source inside
username Test password I2xAvC8b372aLGtP encrypted
privilege 15
username Cisco password dDFIeex1zkFMaVXs encrypted
privilege 15
!--- Output suppressed. ! prompt hostname context
Cryptochecksum:ae65e1f96123ea351ca1086c22f3ebc7 : end
```

[FWSM im Multiple-Context-Modus als NTP-Client](#)

Das Cisco Firewall Service Module (FWSM) unterstützt die NTP-Konfiguration nicht separat. Die FWSM-Uhr wird beim Hochfahren des Moduls automatisch mit der Uhr des Catalyst Switches synchronisiert. Wenn der Catalyst Switch selbst mit einem NTP-Server synchronisiert wird, übernimmt das FWSM diese Uhr.

[Überprüfen](#)

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

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.

- [show ntp status](#) - Zeigt den Status jeder NTP-Zuordnung an.

```
ciscoasa# show ntp status
Clock is synchronized, stratum 10, reference is 192.168.100.10
nominal freq is 99.9984 Hz, actual freq is 99.9984 Hz, precision is 2**6
reference time is d3a93668.7b6b6155 (11:41:28.482 GMT Thu Jul 12 2012)
clock offset is -2.0439 msec, root delay is 1.48 msec
root dispersion is 3894.03 msec, peer dispersion is 3891.95 msec
```

- [NTP-Zuordnungen anzeigen](#) - Zeigt die Informationen zur NTP-Zuordnung an.

```
ciscoasa# show ntp associations
address          ref clock      st  when  poll reach  delay  offset  disp
*~192.168.100.10 127.127.7.1    9   7     64   7     1.5  -2.04 3892.0
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

```
ciscoasa# show ntp associations detail
```

```
192.168.100.10 configured, our_master, sane, valid, stratum 9
ref ID 127.127.7.1, time d3aa5d7a.d8cf2704 (08:40:26.846 GMT Fri Jul 13 2012)
our mode client, peer mode server, our poll intvl 1024, peer poll intvl 1024
root delay 0.00 msec, root disp 0.03, reach 377, sync dist 16.602
delay 1.71 msec, offset 1.3664 msec, dispersion 15.72
precision 2**16, version 3
org time d3aa5d8a.68391cb8 (08:40:42.407 GMT Fri Jul 13 2012)
rcv time d3aa5d8a.6817b624 (08:40:42.406 GMT Fri Jul 13 2012)
xmt time d3aa5d8a.67a3f2da (08:40:42.404 GMT Fri Jul 13 2012)
filtdelay =      1.71    1.60    1.57    1.68    1.59    1.66    1.65    1.65
filtoffset =     1.37    1.41    1.50    1.52    1.63    1.61    1.56    1.53
filterror =     15.63   31.25   46.88   62.50   78.13   93.75  109.38  125.00
```

[Fehlerbehebung](#)

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

[Fehler: Peer/Server-Uhr nicht synchronisiert](#)

Die Cisco ASA wird nicht mit dem NTP-Server synchronisiert, und diese Fehlermeldung wird angezeigt:

```
NTP: packet from 192.168.1.1 failed validity tests 20
Peer/Server Clock unsynchronized
```

Lösung:

Aktivieren Sie die NTP-Debug, und überprüfen Sie diese Ausgabe im Detail:

```
ciscoasa(config)# NTP: xmit packet to 192.168.1.1:
  leap 3, mode 3, version 3, stratum 0, ppoll 64
```

Es sieht so aus, als ob der NTP-Server mit einer Schicht 0 konfiguriert ist, die gemäß [RFC 1305](#) als "Unspecified" (Nicht festgelegt) angegeben wird.

Um diesen Fehler zu beheben, definieren Sie die Stratum-Nummer des NTP-Servers zwischen 6 und 10.

Problem: Die Uhr kann nicht mit dem NTP-Server synchronisiert werden.

Die Cisco ASA wurde als NTP-Client konfiguriert, die Synchronisierung funktioniert jedoch nicht, und diese Ausgabe wird empfangen:

```
ciscoasa# show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 99.9984 Hz, actual freq is 99.9984 Hz, precision is 2**6
reference time is d3a93395.388e423c (11:29:25.220 GMT Thu Jul 12 2012)
clock offset is -4050.4142 msec, root delay is 1.21 msec
root dispersion is 19941.07 msec, peer dispersion is 16000.00 msec
```

Lösung:

Um dieses Problem zu beheben, überprüfen Sie folgende Punkte:

- Überprüfen Sie, ob der NTP-Server von der Cisco ASA erreichbar ist. Führen Sie den Ping-Test durch, und überprüfen Sie das Routing.
- Stellen Sie sicher, dass die Cisco ASA-Konfiguration intakt ist und mit den Parametern des NTP-Servers übereinstimmt.
- Aktivieren Sie die **NTP-Debugbefehle**, um weitere Details zu erhalten.

Befehle zur Fehlerbehebung

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.

Hinweis: Beachten Sie [vor der](#) Verwendung von **Debug**-Befehlen die [Informationen](#) zu [Debug-Befehlen](#).

- [debug ntp paket](#) - Zeigt Meldungen über NTP-Pakete an.
- [debug ntp event](#) - Zeigt Meldungen über NTP-Ereignisse.

Zugehörige Informationen

- [Produkt-Support für Cisco Adaptive Security Appliances der Serie ASA 5500](#)
- [NTP-Beispielkonfiguration für einen Catalyst 6000-Switch mit hoher Verfügbarkeit](#)
- [NTPv3 RFC 1305](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)