ASA 8.x： ASA 8.x：NTP のサーバと同期されているマルチ コンテキスト モードの Cisco ASA の設定例

目次

概要

このドキュメントでは、マルチ コンテキスト モードの Cisco 適応型セキュリティ アプライアンス（ASA）のクロックとネットワーク タイム プロトコル（NTP）サーバのクロックとの同期方法の設定例を示します。

NTP は異なるネットワーク エンティティのクロックの同期に使用されるプロトコルです。 UDP/123 を使用します。 このプロトコルを使用する主な目的は、データ ネットワーク上の変数の遅延による影響を回避することです。

このシナリオでは、Cisco ASA はマルチ コンテキスト モードです。 Admin と Test1 は、2 種類のコンテキストです。 Cisco ASA を NTP クライアントとして設定するには、システム実行スペースで NTP サーバ コマンドを指定する必要があります。その理由はこのコマンドがコンテキスト モードをサポートしていないことにあります。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco ASA ソフトウェア リリース バージョン 8.2 以降
- Cisco Adaptive Security Device Manager（ASDM）ソフトウェア リリース バージョン 6.3 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

このセクションでは、このドキュメントで説明されている機能を設定するために必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

ASDM の設定

ASDM を設定するには、次の手順を実行します：

1. システム実行スペースを確認するには、Cisco ASA で [System] をクリックします。
2. [Configuration] > [Device Management] > [System Time] > [NTP] に移動し、[Add] をクリックします。
3. [Add NTP Server Configuration] ウィンドウが表示されます。 NTP サーバに関連付けられたインターフェイスの IP アドレスを指定し、認証キーの詳細を指定します。 [OK] をクリックします。**注:** NTP サーバの詳細は、コンテキスト システム内で指定する必要があります。ただし、システム実行スペースがマルチ コンテキスト モードのインターフェイスを含めないため、インターフェイス名を指定する必要があります（つまり、管理コンテキスト内で定義されます）。
4. 次のウィンドウで NTP サーバの詳細を参照してください：

以下に、参照用に Cisco ASA の同様の CLI 設定を示します：

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
ciscoasa#
```

NTP クライアントとしてのマルチ コンテキスト モードの FWSM

Cisco Firewall Service Module（FWSM）は NTP コンフィギュレーションを個別にサポートしません。 FWSM のクロックは、起動したときに Catalyst スイッチのクロックと自動的に同期します。 Catalyst スイッチ自体が NTP サーバと同期する場合、FWSM がそのクロックを継承します。

確認

このセクションでは、設定が正常に機能していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show ntp status** - 各 NTP アソシエーションの状態を表示します。`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`
- **show ntp associations** - NTP アソシエーションに関する情報を表示します。`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`

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

エラー： 同期されていないピア/サーバ クロック

Cisco ASA は NTP サーバと同期していないため、このエラー メッセージが表示されます：

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

解決策：

NTP のデバッグをイネーブルにして、この出力を詳細に確認してください：

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

NTP サーバがストラタム値 0 で設定されているように見えます。RFC 1305 によると「詳細不明」と指定されています 。

このエラーを解決するには、6 から 10 の間で NTP サーバのストラタム番号を定義します。

問題： NTP サーバとのクロック同期不可

Cisco ASA は NTP のクライアントとして設定されていますが、同期が完了しなかったため次の出力が表示されます：

```
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
```

解決策：

この問題を解決するには、次の項目を確認してください：

- NTP サーバが Cisco ASA から到達可能であるかどうかを確認します。 ping テストを行い、ルーティングを確認します。
- Cisco ASA 設定を変更せずに、NTP サーバのパラメータと一致することを確認します。
- さらに調べるために NTP **デバッグ コマンド**を有効にします。

トラブルシューティングのためのコマンド

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- debug ntp packet - NTP パケットに関するメッセージを表示します。
- debug ntp event - NTP イベントに関するメッセージを表示します。

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス製品のサポート
- High Availability Catalyst 6000 スイッチのための NTP 設定例
- NTPv3 RFC 1305
- テクニカルサポートとドキュメント - Cisco Systems