ACS 5.x： NTP のサーバとの Cisco ACS の同期の設定例

目次

概要

ネットワーク タイム プロトコル (NTP) は、異なるネットワーク エンティティのクロックを同期するため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 ネットワーク上の可変の遅延による影響を回避することです。

このドキュメントでは、NTP サーバとクロックを同期するための、Cisco ACS の設定例を示します。 ACS 5.x では、2 台までの NTP サーバを設定できます。

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 Secure ACS バージョン 5.x

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

この項では、このドキュメントで説明する機能の設定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。

Cisco ACS の NTP 設定

Cisco ACS の時間を NTP サーバと同期するには、次の手順を実行します。

1. 日時を手動で、clock set <month> <day> <hh: min: ss> <yyyy> コマンドを使用して設定します。
2. clock timezone <timezone> コマンドで時間帯を指定します。
3. NTP server <IP address of NTP server> コマンドで NTP サーバを指定します。NTP は、クライアント サーバ階層に従います。 NTP クライアントが NTP サーバで設定されると、NTP サーバの*基準クロック*がクライアントに渡されます。 NTP サーバから正確な時刻を取得するには、約 10 ~ 20 分かかり、これは、NTP サーバに到達するために発生する遅延により異なります。Cisco ACS は、NTP デーモンを使用して、NTP サーバとクロックを同期します。 Cisco ACS は Simple NTP（SNTP）をサポートしていません。 NTP デーモンが開始されると、ACS は、元の時間（ローカル）を含む NTP サーバにパケットを送信します。次に、NTP サーバは、基準クロックの時間を挿入してパケットに応答します。 NTP クライアントは、このパケットを受信すると、それ自体のローカル時間でパケットをログに記録し、パケットが移動にかかった時間を検証します。 このような複数のパケット交換は、正確な往復遅延時間とオフセット値を計算するために発生し、最終的に、NTP クライアントのローカル時間が、NTP サーバの基準クロックと同期されます。

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。

設定の詳細を確認するには、次のコマンド出力の抜粋を参照してください。

```
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.
```
注: *Stratum* は、プライマリ基準クロックへの NTP サーバの近さを指定する手段です。 stratum *n* サーバと同期されている各 NTP クライアントは、stratum n+1 レベルと呼ばれます。

ACS からの次のアプリケーション ログ メッセージを参照して、NTP 同期の詳細を確認してください。

```
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-
```
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。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

問題： ACS が VMWare マシンにインストールされていると、クロックのドリフトが大きすぎて NTP で障害が発生する

Cisco ACS が、クロック ソースとして NTP サーバを使用するように設定されていますが、頻繁に、内部の時間ソースに変更されます。 これが発生すると、ユーザが Active Directory から認証できなくなります。これは、Kerberos がサポートしている時差は 300 秒だけであるためです。

解決策

ESXi ホストで CPU 使用率が高くなると、通常どおりには VM で機能しません。 これは、VM 内部のクロックに影響し、実際に、Windows のドメイン コントローラからの、5 分を超えるクロック ドリフトを引き起こします。 これにより、Kerberos に障害が発生します。 これは、NTP を使用しない Windows VM だけでなく、ホストのクロック同期にも影響を与えます。 Cisco ACS に示される仮想クロックが不安定になり、NTP がドリフトに対応できなくなると、この仮想クロックは最終的に、それ自体を時刻ソースとして再び使用します。

注: NTP デーモンは、複数の交換でクロックを調整し、クライアントが正確な時刻を取得するまで続行します。 ただし、NTP サーバと NTP クライアント間の遅延が大きくなりすぎると、NTP デーモンが終了するため、時間を手動で調整し、NTP デーモンを再起動する必要があります。

この問題は、Cisco ACS に VMWare ツールのサポートを統合すると解決されるように設定されています。これは、今後リリースされる Cisco ACS リリース 5.4 で提供されます。 詳細は、Cisco Bug ID CSCtg50048（登録ユーザ専用）を参照してください。 一時的な回避策として、次の手順を試すことができます。

- **ACS stop** コマンドをで ACS サービスを停止します。
- すべての NTP 設定を削除し、**write mem** コマンドで設定を保存します。

- Cisco ACS をリブートします。
- **show application status acs** コマンドで、すべてのサービスが動作していることを確認します。
- クロックを実際の時刻にできるだけ近い時刻、つまり、NTP のオフセット要件の 1 秒前に設定します。
- 時間帯が正しいことを確認します。
- NTP 設定を再度追加し、保存します。
- **show ntp** コマンドを実行して、出力が同じであるかどうかを確認します。

注: これらの手順で問題が解決しない場合は、Cisco TAC に連絡してください。

ACS のインターフェイス IP アドレスの変更後に NTP 同期が失われる

ACS NIC の IP アドレスを変更すると、NTP が同期されなくなります。

解決策

この動作は確認済みであり、Cisco Bug ID CSCtk76151（登録ユーザ専用）に記載されています。 ACS の IP アドレスが変更されると、ACS アプリケーションが再起動されますが、NTP デーモンは再起動されません。 これは、ACS バージョン 5.3.0.23 で修正されています。 以前のバージョンでこの問題を解決するには、次の手順を実行してください。

1. **ntp server** コマンドを実行して、NTP プロセスを停止します。
2. **ntp server** コマンドを再実行して、NTP プロセスを再起動します。

関連情報

- CS ACS 5.X 製品サポート
- Cisco Secure Access Control System 5.3 ユーザ ガイド
- テクニカルサポートとドキュメント - Cisco Systems