ACS 5.x：Cisco ACS與NTP伺服器同步的配置示例

目錄

簡介

網路時間協定(NTP)是一種用於同步不同網路實體時鐘的協定。它使用UDP/123。使用此協定的主要目的是要避免資料網路中可變延遲的影響。

本文檔提供了Cisco ACS與NTP伺服器同步時鐘的示例配置。ACS 5.x最多可以配置兩台NTP伺服器。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco安全ACS 5.x版

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

設定

本節提供用於設定本文件中所述功能的資訊。

注意：使用命令查詢工具(僅限註冊客戶)可獲取有關此部分使用的命令的更多資訊。

Cisco ACS上的NTP配置

為了將Cisco ACS的時間與NTP伺服器同步，請完成以下步驟：

1. 使用clock set <month> <day> <hh：min：ss> <yyyy>命令手動配置日期和時間。
2. 使用clock timezone <timezone>命令指定時區。
3. 使用NTP server <NTP server的IP地址>命令指定NTP伺服器。

   NTP遵循客戶端-伺服器層次結構。當使用NTP伺服器配置NTP客戶端時，NTP伺服器的參考時鐘會傳遞給客戶端。從NTP伺服器獲取準確時間大約需要10-20分鐘，具體取決於到達NTP伺服器的延遲。

   Cisco ACS使用NTP後台程式將其時鐘與NTP伺服器同步。它不支援簡單NTP、SNTP。當NTP後台程式啟動時，ACS會將包含其原始時間（本地）的資料包傳送到NTP伺服器。然後，NTP伺服器透過插入其參考時鐘時間來應答資料包。一旦NTP客戶端收到此資料包，它就會以自己的本地時間記錄該資料包，以驗證資料包所花費的傳輸時間。為了計算精確的往返延遲時間和偏移值，進行了幾次這樣的分組交換，最後將NTP客戶端的本地時間與NTP伺服器的參考時鐘同步。

驗證

使用本節內容，確認您的組態是否正常運作。

若要驗證組態詳細資訊，請參閱以下命令輸出片段。

<#root>

```
acs51/admin#
```

show clock

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

<#root>

```
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)#
```

<#root>

```
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.
```

注意：層是一種度量，用於指定NTP伺服器與主參考時鐘的接近程度。與第n層伺服器同步的每個NTP客戶端被稱為第n+1層客戶端。

請參閱來自ACS的這些應用程式日誌消息以驗證NTP同步詳細資訊。

<#root>

```
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-
```

輸出直譯器工具(僅供註冊客戶使用) (OIT)支援某些show指令。使用OIT檢視對show命令輸出的分析。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

問題：當ACS安裝在VMWare電腦上時，時鐘漂移過多，NTP失敗

Cisco ACS配置為使用NTP伺服器作為時鐘源，但它不斷更改為內部時間源。發生這種情況時，由於Kerberos僅支援300秒的時間差，因此使用者無法從Active Directory進行身份驗證。

解決方案

如果ESXi主機的CPU利用率很高，則它不會像正常情況一樣頻繁地為VM提供服務。這會影響VM內部的時鐘，實際上會導致Windows域控制器上的時鐘偏移超過五分鐘。它導致Kerberos失敗。這也會影響沒有NTP或主機時鐘同步的Windows VM。由於呈現給Cisco ACS的虛擬時鐘不夠穩定，NTP無法跟上這種變化，因此它最終會恢復使用自身作為時間源。

注意：NTP後台程式會在多個交換中調整時鐘，並持續到客戶端獲得準確的時間為止。但是，當NTP伺服器和NTP客戶端之間的延遲變得過大時，NTP守護進程將終止，您需要手動調整時間並重新啟動NTP守護進程。

將VMWare工具支援整合到Cisco ACS中時，此問題即已解決。Cisco ACS 5.4版本提供了此支援，但尚未發佈。如需詳細資訊，請參閱Cisco錯誤ID CSCtg50048(僅限註冊客戶)。暫時解決方法是，您可以嘗試以下步驟：

- 使用ACS stop命令停止ACS服務（ACS啟動時停止）。
- 刪除所有NTP配置並使用write mem命令儲存配置。
- 重新啟動Cisco ACS。
- 確保所有服務都使用show application status acs命令運行。
- 將時鐘設定為儘可能接近即時，在NTP偏移量要求之前的第二秒鐘。
- 確定時區是正確的。
- 重新增加NTP配置並儲存它。
- 執行show ntp命令以驗證輸出是否相同。

注意：如果這些步驟無法解決問題，建議您聯絡思科TAC。

更改ACS的介面IP地址後，NTP同步丟失

如果更改ACS NIC的IP地址，則會使NTP不同步。

解決方案

此行為已被發現並記錄在思科漏洞ID CSCtk76151(僅限註冊客戶)。修改ACS IP地址後，它會重新啟動ACS應用程式，而不是NTP守護程式。已在ACS版本5.3.0.23中修復了此問題。若要在先前版本中解決此問題，請完成以下步驟：

1. 發出no ntp server命令可停止NTP進程。
2. 再次發出ntp server命令，以便重新啟動NTP進程。

相關資訊

- CS ACS 5.X產品支援
- 思科安全訪問控制系統5.3使用手冊
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。