

# ACS 5.x : Cisco ACS与NTP服务器同步配置示例

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[Cisco ACS上的NTP配置](#)

[验证](#)

[故障排除](#)

[问题：在VMWare计算机上安装ACS时，时钟漂移过多且NTP发生故障](#)

[解决方案](#)

[更改ACS的接口IP地址后，NTP同步丢失](#)

[解决方案](#)

[相关信息](#)

## 简介

网络时间协议(NTP)是一种用于同步不同网络实体时钟的协议。它使用UDP/123。使用此协议的主要目的是避免数据网络上可变延迟的影响。

本文档提供了Cisco ACS的示例配置，以便将其时钟与NTP服务器同步。ACS 5.x最多可以配置两台NTP服务器。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全ACS版本5.x

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

### 规则

有关文档约定的更多信息，请参考 [Cisco 技术提示约定](#)。

## 配置

本部分提供有关如何配置本文档所述功能的信息。

注意：要获取此部分中所用命令的更多信息，可使用 [命令查找工具](#)（仅限 [已注册客户](#)）。

### Cisco ACS上的NTP配置

要将Cisco ACS的时间与NTP服务器同步，请完成以下步骤：

1. 使用 [clock set <month> <day> <hh : min : ss> <yyyy>](#) 命令手动配置日期和时间。
2. 用 [clock timezone <timezone>](#) 命令指定时区。
3. 使用 [NTP server <IP address of NTP server>](#) 命令指定NTP服务器。

NTP遵循客户端-服务器层次结构。当NTP客户端配置了NTP服务器时，NTP服务器的参考时钟会传递给客户端。从NTP服务器获取准确时间大约需要10-20分钟，具体取决于到达NTP服务器所发生的延迟。

Cisco ACS使用NTP后台程序将其时钟与NTP服务器同步。它不支持简单NTP、SNTP。当NTP守护程序启动时，ACS会向包含其原始时间（本地）的NTP服务器发送数据包。然后，NTP服务器通过插入其参考时钟时间来响应数据包。一旦NTP客户端收到此数据包，它将记录该数据包及其自己的本地时间，以验证数据包所花费的传输时间。为了计算准确的往返延迟时间和偏移值，进行了几次这样的分组交换，最后将NTP客户端的本地时间与NTP服务器的参考时钟同步。

## 验证

使用本部分可确认配置能否正常运行。

要验证配置详细信息，请参阅以下命令输出片段。

```
<#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：层是一种度量，用于指定NTP服务器与主参考时钟的接近程度。与第n层服务器同步的每个NTP客户端被称为第n+1层客户端。

请参阅这些来自ACS的应用日志消息以验证NTP同步详细信息。

<#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--

[命令输出解释程序 \( 仅限注册用户 \) \(OIT\) 支持某些 show 命令。](#) 使用 OIT 可查看对 show 命令输出的分析。

## 故障排除

本部分提供的信息可用于对配置进行故障排除。

**问题：**在VMWare计算机上安装ACS时，时钟漂移过多且NTP发生故障

Cisco ACS配置为使用NTP服务器作为时钟源，但它会不断更改为内部时间源。发生这种情况时，用户不会从Active Directory进行身份验证，因为Kerberos仅支持300秒的时间差。

### 解决方案

如果ESXi主机的CPU利用率很高，则它不会像正常情况那样频繁地为VM提供服务。这会影响虚拟机内的时钟，实际上会导致Windows域控制器的时钟偏移超过五分钟。它导致Kerberos失败。这也会影响没有NTP或主机时钟同步的Windows虚拟机。由于呈现给Cisco ACS的虚拟时钟不够稳定，NTP无法跟上漂移，因此它最终会恢复使用自己作为时间源。

**注意：**NTP后台守护程序会在多个交换中调整时钟，并继续运行，直到客户端获得准确的时间。但是，当NTP服务器和NTP客户端之间的延迟过大时，NTP后台守护程序将终止，您需要手动调整时间并重新启动NTP后台守护程序。

将VMWare工具支持集成到Cisco ACS中时，此问题即被设置为解决，Cisco ACS 5.4版本中提供了此支持，但尚未发布。有关详细信息，请参阅思科漏洞ID [CSCtg50048\(仅限注册客户\)](#)。作为临时解决方法，您可以尝试以下步骤：

- 使用ACS stop命令停止ACS服务（此示例中未提供ACS服务）。
- 删除所有NTP配置并使用write mem命令保存配置。
- 重新启动Cisco ACS。
- 确保所有服务都使用show application status acs命令运行。
- 将时钟设置为尽可能接近实时，在NTP偏移要求之前的第二秒钟。
- 确保时区是正确的。
- 重新添加NTP配置并保存。
- 执行show ntp命令以验证输出是否相同。

**注意：**如果这些步骤无法解决问题，建议您联系[思科TAC](#)。

**更改ACS的接口IP地址后，NTP同步丢失**

如果更改ACS NIC的IP地址，则会使NTP不同步。

## 解决方案

此行为已被发现并记录在思科漏洞ID [CSCtk76151](#)中(仅限于[注册](#)客户)。修改ACS IP地址时，它会重新启动ACS应用程序，但不重新启动NTP守护程序。在ACS版本5.3.0.23中修复了此问题。要在以前的版本中解决此问题，请完成以下步骤：

1. 发出no ntp server命令可停止NTP进程。
2. 再次发出ntp server命令以重新启动NTP进程。

## 相关信息

- [CS ACS 5.X产品支持](#)
- [思科安全访问控制系统5.3用户指南](#)
- [技术支持和文档 - Cisco Systems](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。