

ACS 5.x:NTP 서버와의 Cisco ACS 동기화 컨피그레이션 예

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[구성](#)

[Cisco ACS의 NTP 컨피그레이션](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[문제/장애:클럭이 너무 많이 분산되고 VMWare 시스템에 ACS가 설치된 경우 NTP가 실패합니다.](#)

[솔루션](#)

[ACS의 인터페이스 IP 주소가 변경된 후 NTP 동기화 손실](#)

[솔루션](#)

[관련 정보](#)

소개

NTP(Network Time Protocol)는 서로 다른 네트워크 엔티티의 클럭을 동기화하는 데 사용되는 프로토콜입니다. 이 프로토콜은 UDP/123을 사용합니다. 이 프로토콜을 사용하는 주된 목적은 데이터 네트워크에 대한 가변 레이턴시의 영향을 방지하는 것입니다.

이 문서에서는 Cisco ACS에서 시계를 NTP 서버와 동기화하기 위한 샘플 컨피그레이션을 제공합니다. ACS 5.x는 최대 2개의 NTP 서버를 구성할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure ACS 버전 5.x

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

[표기 규칙](#)

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 규칙](#)을 참조하십시오.

[구성](#)

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고: [명령 조회 도구](#) (등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

[Cisco ACS의 NTP 컨피그레이션](#)

Cisco ACS의 시간을 NTP 서버와 동기화하려면 다음 단계를 완료하십시오.

1. [<month> <day> <hh:min:ss> <yyyy>](#) 명령을 사용하여 날짜 및 시간을 [수동으로](#) 구성합니다.
2. [clock timezone <timezone>](#) 명령을 사용하여 표준 시간대를 지정합니다.
3. NTP server <IP address of NTP server> [명령을 사용하여 NTP 서버를 지정합니다.](#) NTP는 클라이언트-서버 계층 구조를 따릅니다. NTP 클라이언트가 NTP 서버로 구성되면 NTP 서버의 참조 시계가 클라이언트에 전달됩니다. NTP 서버에서 정확한 시간을 얻는 데 약 10-20분이 소요되며 NTP 서버에 연결하기 위해 지연이 발생하는 경우에 따라 달라집니다. Cisco ACS는 NTP 데몬을 사용하여 시계를 NTP 서버와 동기화합니다. Simple NTP, SNTP는 지원하지 않습니다. NTP 데몬이 시작되면 ACS는 원래 시간(로컬)을 포함하는 NTP 서버로 패킷을 전송합니다. 그런 다음 NTP 서버는 참조 클럭 시간을 삽입하여 패킷에 응답합니다. NTP 클라이언트가 이 패킷을 수신하면 패킷이 소요된 이동 시간을 확인하기 위해 고유한 로컬 시간으로 패킷을 로깅합니다. 정확한 왕복 지연 시간 및 오프셋 값을 계산하고 마지막으로 NTP 클라이언트의 로컬 시간이 NTP 서버의 참조 시계와 동기화되기 위해 이러한 패킷 교환이 몇 가지 발생합니다.

[다음을 확인합니다.](#)

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

컨피그레이션 세부사항을 확인하려면 다음 명령 출력 조각을 참조하십시오.

```
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	1	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.

참고: Stratum은 NTP 서버가 기본 참조 클럭에 얼마나 근접한지를 지정하는 측정값입니다.stratum n 서버와 동기화된 각 NTP 클라이언트를 stratum n+1 레벨이라고 합니다.

NTP 동기화 세부 정보를 확인하려면 ACS에서 보낸 애플리케이션 로그 메시지를 참조하십시오.

```
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 도구\(등록된 고객만 해당\)](#)(OIT)는 특정 show 명령을 지원합니다.OIT를 사용하여 show 명령 출력의 분석을 보니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제/장애:클럭이 너무 많이 분산되고 VMWare 시스템에 ACS가 설치된 경우 NTP가 실패합니다.

Cisco ACS는 NTP 서버를 클럭 소스로 사용하도록 구성되었지만 내부 시간 소스로 계속 변경됩니다.이 경우 Kerberos는 300초의 시간차만 지원하므로 사용자가 Active Directory에서 인증하지 못합니다.

솔루션

ESXi 호스트의 CPU 사용률이 높으면 VM이 정상만큼 자주 사용되지 않습니다.이는 VM 내부의 클럭에 영향을 미치며, 실제로 Windows 도메인 컨트롤러로부터 5분 이상의 클럭 차이가 발생합니다.이로 인해 Kerberos가 실패합니다.이는 NTP 또는 호스트 클럭 동기화가 없는 Windows VM에도 영향을 미칩니다.Cisco ACS에 제시된 가상 시계가 NTP가 드리프트에 맞출 수 있을 만큼 안정적이지 않기 때문에 결국 자신을 시간 소스로 사용하는 것으로 돌아갑니다.

참고: NTP 데몬은 여러 교환에서 시계를 조정하고 클라이언트가 정확한 시간을 얻을 때까지 계속 진행합니다.그러나 NTP 서버와 NTP 클라이언트 간의 지연 시간이 너무 커지면 NTP 데몬이 종료되고 시간을 수동으로 조정하고 NTP 데몬을 다시 시작해야 합니다.

이 문제는 아직 릴리스되지 않은 Cisco ACS 릴리스 5.4에서 사용 가능한 VMWare 툴 지원을 Cisco ACS에 통합할 때 해결되도록 설정됩니다. 자세한 내용은 Cisco 버그 ID [CSCtg50048](#)([등록된](#) 고객만 해당)을 참조하십시오. 임시 해결 방법으로 다음 단계를 시도할 수 있습니다.

- **ACS stop** 명령을 사용하여 ACS 서비스를 중지합니다.
- 모든 NTP 컨피그레이션을 제거하고 **write mem** 명령을 사용하여 컨피그레이션을 저장합니다.
- Cisco ACS를 재부팅합니다.
- 모든 서비스가 **show application status acs** 명령으로 실행 중인지 확인합니다.
- 가능한 한 실시간으로 시계를 NTP의 오프셋 요구 사항 이전의 두 번째 시간으로 설정합니다.
- 표준 시간대가 1이어야 합니다.
- NTP 컨피그레이션을 다시 추가하고 저장합니다.
- 출력이 **동일한지** 확인하려면 **show ntp** 명령을 수행합니다.

참고: 이러한 단계에서 문제가 해결되지 않으면 [Cisco TAC](#)에 문의하는 것이 좋습니다.

[ACS의 인터페이스 IP 주소가 변경된 후 NTP 동기화 손실](#)

ACS NIC의 IP 주소를 변경하면 NTP가 동기화되지 않습니다.

[솔루션](#)

이 동작은 Cisco 버그 ID [CSCtk76151](#)([등록된](#) 고객만 해당)에서 관찰되고 기록됩니다. ACS IP 주소가 수정되면 ACS 애플리케이션을 재시작하지만 NTP 데몬은 재시작하지 않습니다. ACS 버전 5.3.0.23에서 수정되었습니다. 이전 버전에서 이 문제를 해결하려면 다음 단계를 완료하십시오.

1. NTP 프로세스를 중지하려면 **no ntp server** 명령을 실행합니다.
2. NTP 프로세스를 다시 시작하려면 **ntp server** 명령을 다시 실행합니다.

[관련 정보](#)

- [CS ACS 5.X 제품 지원](#)
- [Cisco Secure Access Control System 5.3 사용 설명서](#)
- [기술 지원 및 문서 - Cisco Systems](#)