Sourcefire User Agent로 연결 문제 해결

목차

소개

Sourcefire User Agent는 Microsoft Active Directory 서버를 모니터링하고 LDAP를 통해 인증된 로그인 및 로그오프를 보고합니다. FireSIGHT System은 이러한 기록을 관리되는 디바이스에서 직접 네트워크 트래픽 관찰을 통해 수집한 정보와 통합합니다. Sourcefire User Agent로 작업하는 경우 기술적인 문제가 발생할 수 있습니다. 이 문서에서는 Sourcefire User Agent와 관련된 다양한 문제를 해결하기 위한 팁을 제공합니다.

사전 요구 사항

FireSIGHT Management Center, Sourcefire User Agent 및 Active Directory에 대한 지식이 있는 것이 좋습니다.

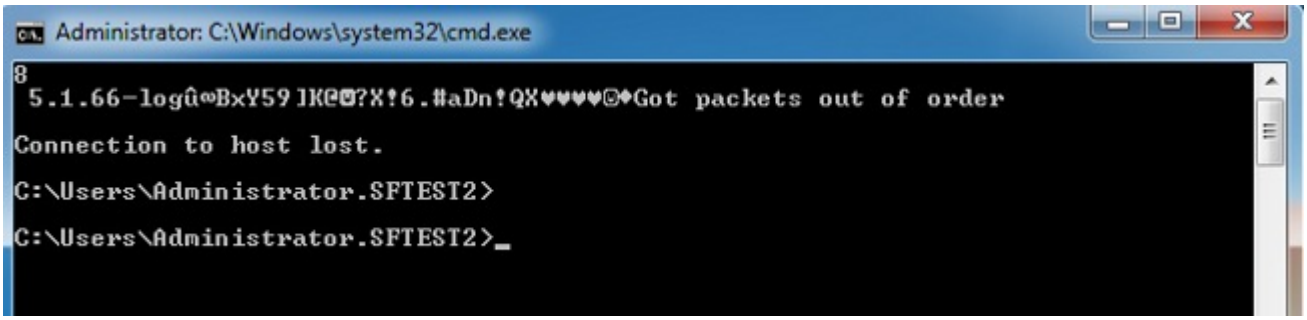
> **팁**: Sourcefire User Agent의 설치 및 제거 단계에 대해 자세히 알아보려면 이 문서를 참조하십시오.

연결 문제

1. User Agent가 FireSIGHT Management Center에 추가되었는지 확인합니다. 이를 확인하려면 Policies(정책) > **Users(사용자) > User Agent(사용자 에이전트)**로 이동하여 구성된 User Agent 호스트의 IP 주소가 올바른지 확인합니다.
2. 포트 3306이 열려 있고 수신 중인지 확인합니다. User Agent와 Defense Center의 통신을 중지하는 방화벽 또는 기타 네트워크 디바이스가 없습니다.
3. FireSIGHT Management Center에서 사용자 에이전트 항목이 구성될 때까지 포트 3306이 열리지 않습니다.
4. User Agent 호스트에 텔넷이 설치되어 있는 경우 User Agent 호스트에서 FireSIGHT

Management Center로 텔넷하여 연결을 확인할 수 있습니다. 5.1.66-log가 표시되고 그 뒤에 ASCII 문자 문자열이 표시됩니다. 연결을 끊으려면 **CTRL+C**를 반복해서 누릅니다.

참고: Got packets out of order 메시지가 표시됩니다.



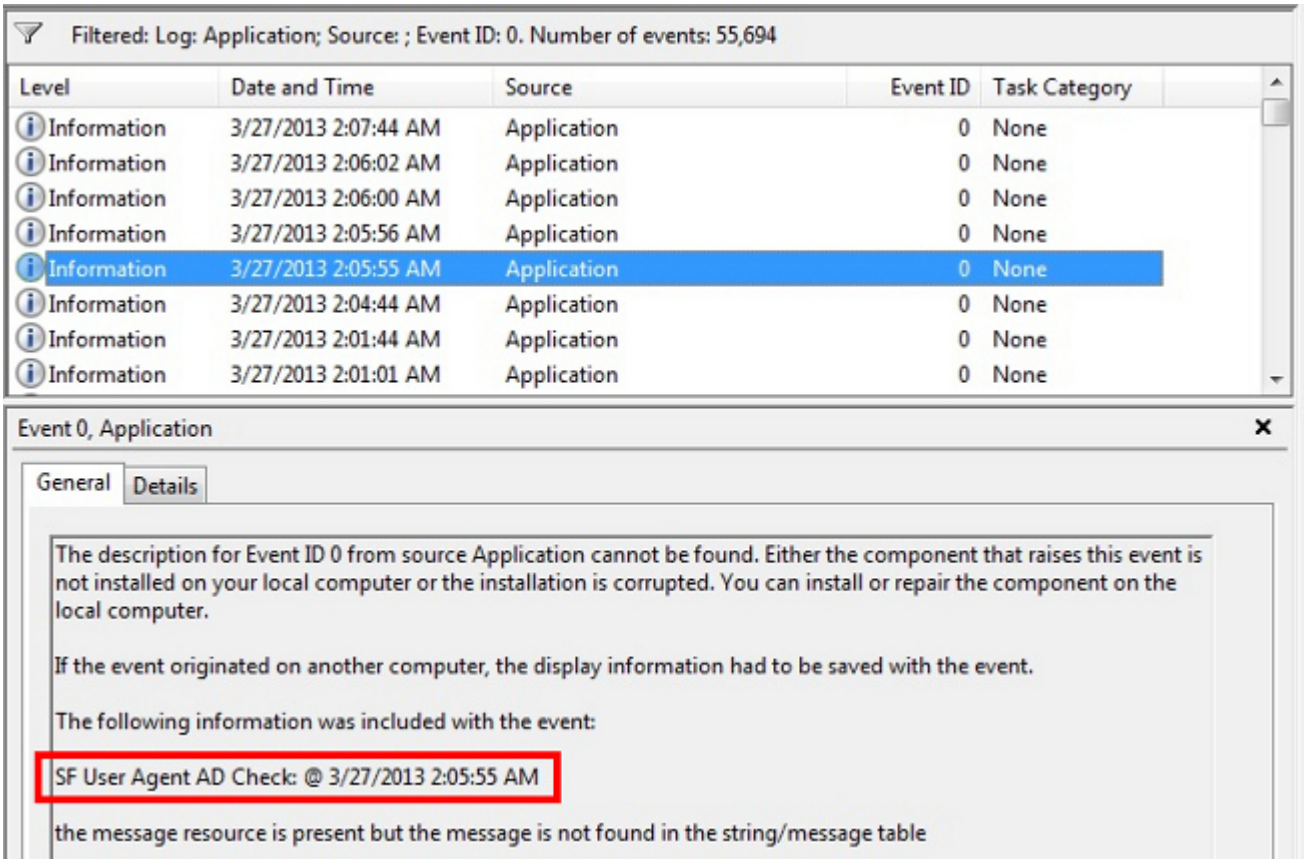
Active Directory 서버에 연결하거나 인증할 때 사용자 에이전트에서 오류가 발생하는 경우 네트워크 또는 사용자 계정 권한 문제가 있을 수 있습니다. 환경에 네트워크 연결 문제가 없는지 확인하고 가능한 경우 테스트하기 위해 Active Directory 서버에 대한 인증에 도메인 관리자 계정을 사용하도록 User Agent를 임시로 구성합니다.

진단 로깅

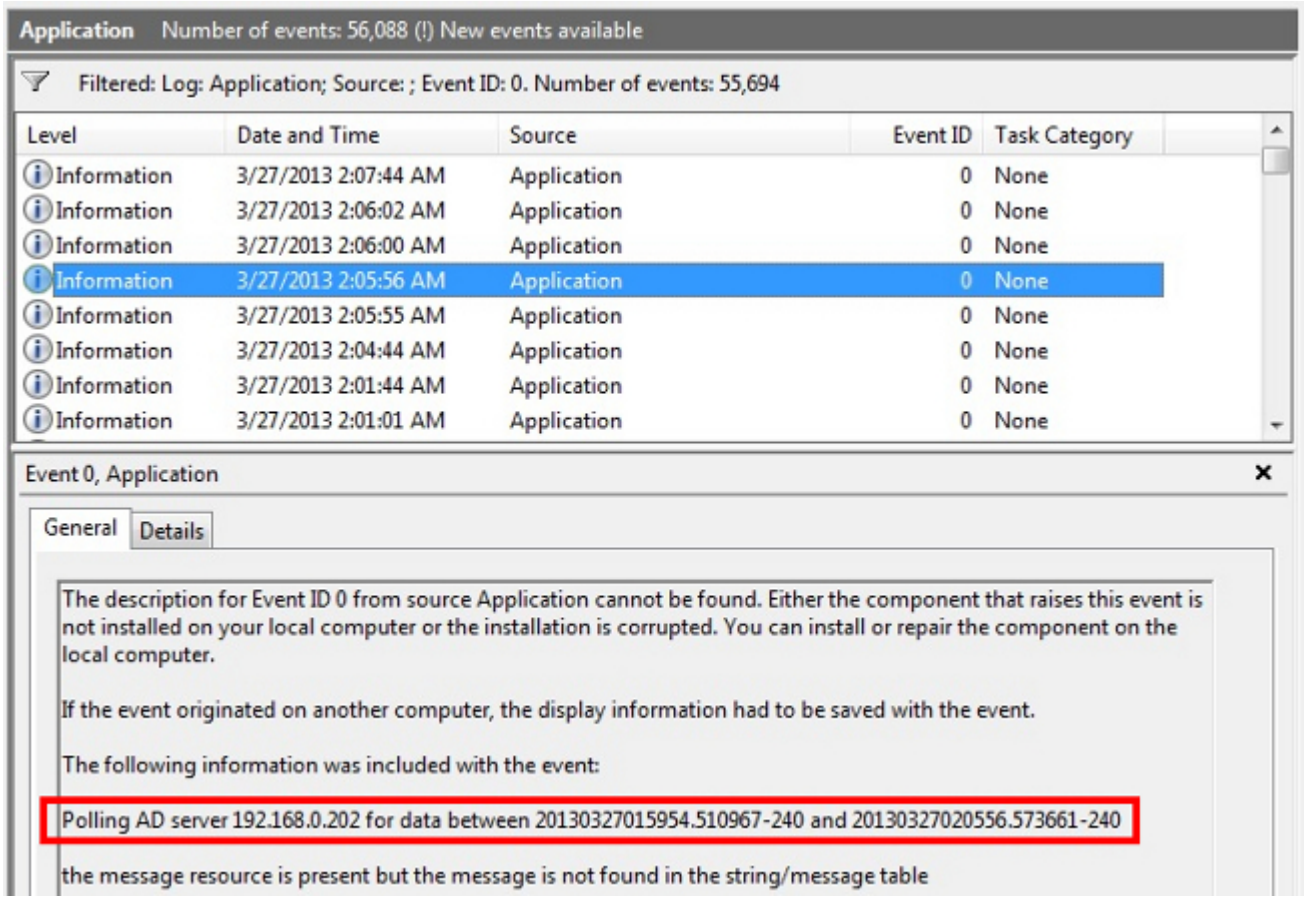
User Agent의 일반적인 문제 해결 방법은 User Agent GUI **클라이언트**에서 **Log to local event log**(로컬 이벤트 로그에 기록)를 선택하고 **Save(저장)**를 클릭합니다. 이렇게 하면 User Agent 호스트 애플리케이션 이벤트 로그에 유용한 운영 메시지가 입력됩니다. 다음 이벤트를 순서대로 검색하여 사용자 에이전트 폴링이 성공적으로 완료되고 있는지 확인할 수 있습니다.

참고: 아래 스크린샷은 User Agent를 실행 중인 호스트의 Microsoft Event Viewer에서 가져온 것입니다.

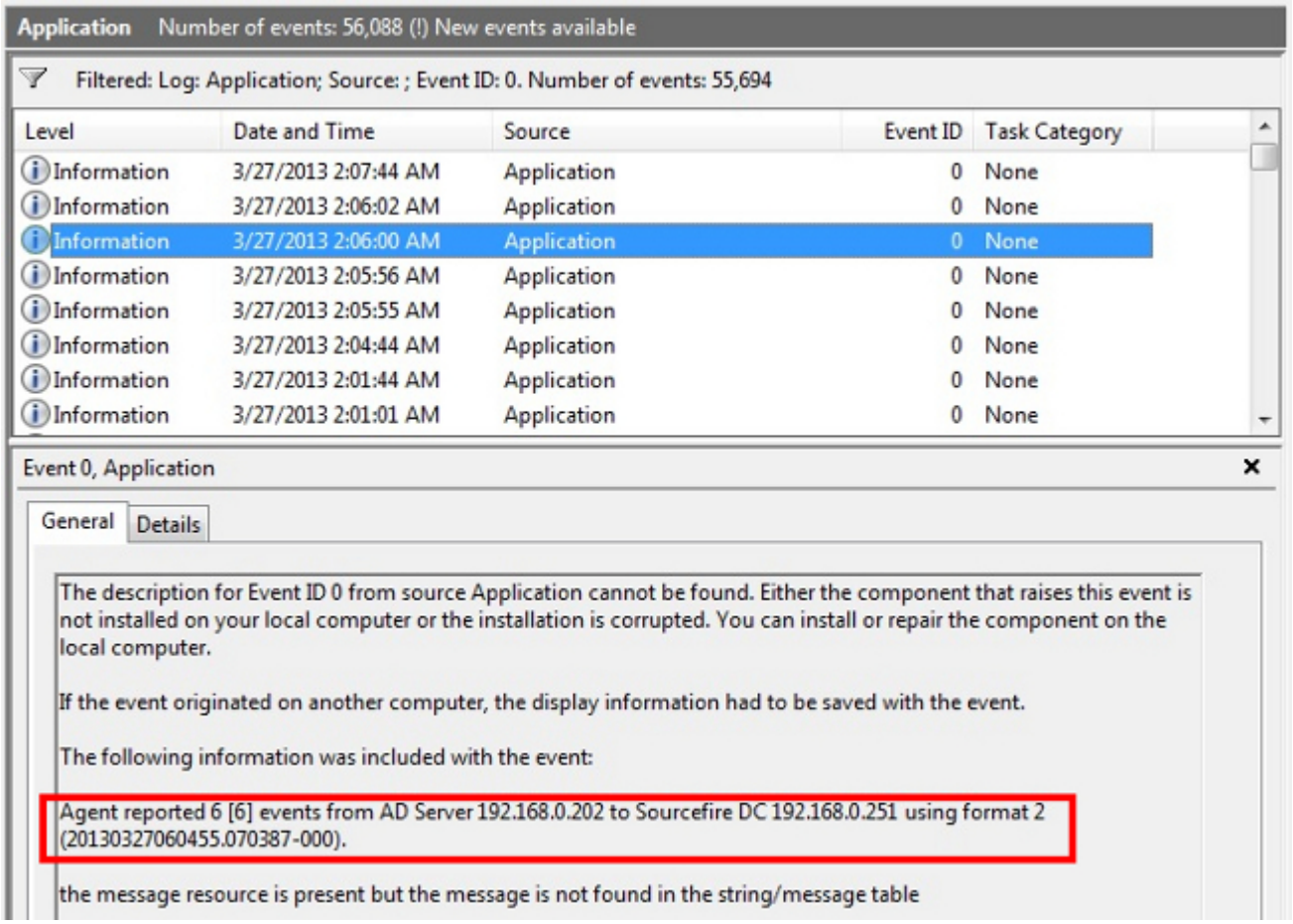
사용자 에이전트 Active Directory 확인



사용자 에이전트 폴링 Active Directory 서버



상담원이 Defense Center에 대해 보고한 번호(#) 이벤트


Application Number of events: 56,088 (!) New events available
Filtered: Log: Application; Source: ; Event ID: 0. Number of events: 55,694
Level Date and Time Source Event ID Task Category
Information 3/27/2013 2:07:44 AM Application 0 None
Information 3/27/2013 2:06:02 AM Application 0 None
Information 3/27/2013 2:06:00 AM Application 0 None
Information 3/27/2013 2:05:56 AM Application 0 None
Information 3/27/2013 2:05:55 AM Application 0 None
Information 3/27/2013 2:04:44 AM Application 0 None
Information 3/27/2013 2:01:44 AM Application 0 None
Information 3/27/2013 2:01:01 AM Application 0 None
Event 0, Application
General Details
The description for Event ID 0 from source Application cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.
If the event originated on another computer, the display information had to be saved with the event.
The following information was included with the event:
Agent reported 6 [6] events from AD Server 192.168.0.202 to Sourcefire DC 192.168.0.251 using format 2 (20130327060455.070387-000).
the message resource is present but the message is not found in the string/message table

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.