Splunk UF가 도메인 컨트롤러에서 완전히 제거되지 않음

적용 가능성

Splunk Enterprise

설명

SCCM(System Center Configuration Manager)에서 도메인 컨트롤러 구축을 위해 Splunk를 테스트하고 패키징하는 과정에서 https://docs.splunk.com/Documentation/Splunk/7.3.1/Installation/UninstallSplunk에 설명된 대로 Splunk의 제거 부분을 수행하는 동안 Splunk가 시스템에서 완전히 제거되지 않는 것을 발견했습니다. SCCM은 레지스트리에서 남은 Splunk를 설치하고 제거한 DC의 나머지 부분을 감지하고 있습니다.

조사

공식 문서에 따라 Splunk UF를 제거하려고 했습니다.
https://docs.splunk.com/Documentation/Forwarder/7.3.1/Forwarder/Uninstalltheuniversalforwarder#Uninst

하지만 충분하지 않았습니다.
또한 다음 단계에 따라 Splunk UF를 제거하는 것이 좋습니다.
https://support.symantec.com/us/en/article.howto55432.html
https://thesolving.com/server-room/how-to-deploy-remove-software-packages-via-gpo/

해결

Active Directory 그룹 정책 개체가 있는 클라이언트 소프트웨어를 다음 방법으로 제거하는 것이 좋습니다.
1) Windows 작업 표시줄에서 시작 > 모든 프로그램 > 관리 도구 > 그룹 정책 관리를 클릭합니다.
2) 사용하는 Windows 버전에는 시작 메뉴의 모든 프로그램 대신 프로그램이 표시될 수 있습니다.
3) 그룹 정책 관리 창의 콘솔 트리에서 도메인을 확장하고 컴퓨터 구성을 확장한 다음 소프트웨어 설정을 확장하고 소프트웨어 설치를 마우스 오른쪽 단추로 클릭한 다음 속성을 클릭합니다.
4) Advanced(고급) 탭에서 이 응용 프로그램이 관리 범위에 포함되지 않을 때 Uninstall this application(이 응용 프로그램 제거)을 선택한 다음 OK(확인)를 클릭합니다.
5) 오른쪽 창에서 소프트웨어 패키지를 마우스 오른쪽 단추로 클릭한 다음 제거를 클릭합니다.
6) Remove Software(소프트웨어 제거) 대화 상자에서 Immediately uninstall the software from users and computers(사용자 및 컴퓨터에서 소프트웨어 즉시 제거)를 선택한 다음 OK(확인)를 클릭합니다.
7) Group Policy Object Editor(그룹 정책 개체 편집기) 창을 닫고 Group Policy Management(그룹

정책 관리) 창을 닫습니다.

관련 링크

Splunk 설명서

Windows 유니버설 전달자 제거
https://docs.splunk.com/Documentation/Forwarder/7.3.1/Forwarder/Uninstalltheuniversalforwarder#Uninst

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.