커넥터에서 읽는 Window 이벤트/EventID 이해

목차

[소개](#)
[개요](#)

소개

이 문서에서는 커넥터가 기본적으로 읽는 창 이벤트/이벤트 ID에 대해 설명합니다.

개요

Umbrella VA(Virtual Appliance)는 기술적으로 어떤 소스 IP 주소에서 DNS 쿼리를 수신하는지에 대한 가시성만 제공합니다. 사용자가 DNS 요청과 연결되기 위해 VA는 커넥터와 함께 작동하며, 그 결과 사용자-IP 매핑이 이루어집니다.

커넥터는 도메인 컨트롤러의 보안 이벤트 로그에서 특정 이벤트 ID가 있는 이벤트를 읽습니다. 그런 다음 이러한 이벤트가 구문 분석되고 사용자 이름과 소스 IP 주소가 VA로 전송되며, 이 VA는 소스 IP와 사용자 간의 매핑을 생성합니다.

도메인 컨트롤러에서 이러한 이벤트를 감사하지 않으면 VA 매핑 프로세스가 제대로 수행되지 않습니다. 이 문서에서는 커넥터가 기본적으로 감시하는 이벤트 ID 유형에 대해 간략하게 설명합니다.

이벤트 ID	설명
4624	이벤트 4624는 로그온 유형, 사용자의 위치 또는 계정 유형과 상관없이 로컬 컴퓨터에 로그온하는 모든 시도를 문서화합니다.
528	이벤트(528)는 네트워크 로그온 이벤트의 경우를 제외하고 계정이 로컬 컴퓨터에 로그온할 때마다 로깅됩니다. 이벤트 528은 로그온에 사용된 계정이 로컬 SAM 계정인지 또는 도메인 계정인지 로깅됩니다.
540	네트워크 상의 다른 곳에 있는 사용자가 이 컴퓨터의 서버 서비스에서 제공하는 리소스(예: 공유 폴더)에 연결할 때 이벤트 540이 로깅됩니다.
4768	이 이벤트는 도메인 컨트롤러에만 로깅되며 이 이벤트의 성공 및 실패 인스턴스가 모두 로깅됩니다.

4769	Windows에서는 이 이벤트 ID를 성공한 서비스 티켓 요청과 실패한 서비스 티켓 요청 모두에 사용합니다.

커넥터가 도메인 컨트롤러의 보안 이벤트 로그에서 직접 이벤트를 읽을 수 없는 경우 Umbrella를 사용하여 지원 티켓을 생성하여 이 항목을 WMI 구독으로 변경할 수 있습니다. WMI 구독의 경우 커넥터는 위에 나열된 모든 이벤트에 구독합니다. 또한 커넥터는 아래에 언급 된 바와 같이 EventID로 로그오프 이벤트를 서브스크립션합니다. 기본적으로 커넥터는 보안 이벤트 로그에서 이러한 로그오프 이벤트를 읽지 않습니다.

이벤트 ID	설명
538	이벤트(538)는 사용자가 네트워크 연결, 대화형 로그온 또는 기타 로그온 유형으로부터 로그오프할 때마다 로깅됩니다(로그온 유형의 차트는 이벤트(528) 참조).
4647	이 이벤트는 로그온 세션의 종료를 신호하고 로그온 ID를 사용하여 로그온 이벤트(4624)로 다시 상관될 수 있다.
4634	이 이벤트는 또한 로그온 세션의 종료를 신호하고 로그온 ID를 사용하여 로그온 이벤트(4624)와 다시 상관될 수 있다.

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.