Loginsearch.ps1을 사용하여 로그온 이벤트 검색

목차

소개

이 문서에서는 PowerShell 스크립트인 Loginsearch.ps1을 사용하여 로그온 이벤트를 검색하는 방법에 대해 설명합니다.

배경 정보

Loginsearch.ps1은 문제 해결을 위해 Umbrella 지원에 유용한 정보를 수집하는 작은 PowerShell 스크립트입니다. 특정 사용자가 OpenDNS Umbrella Dashboard(OpenDNS Umbrella 대시보드)에서 검색 중인 활동 또는 보고서에 올바른 활동을 표시하지 않는 이유를 트러블슈팅할 때는 유용하지만, 다른 유형의 문제를 트러블슈팅하는 데에도 사용할 수 있습니다.

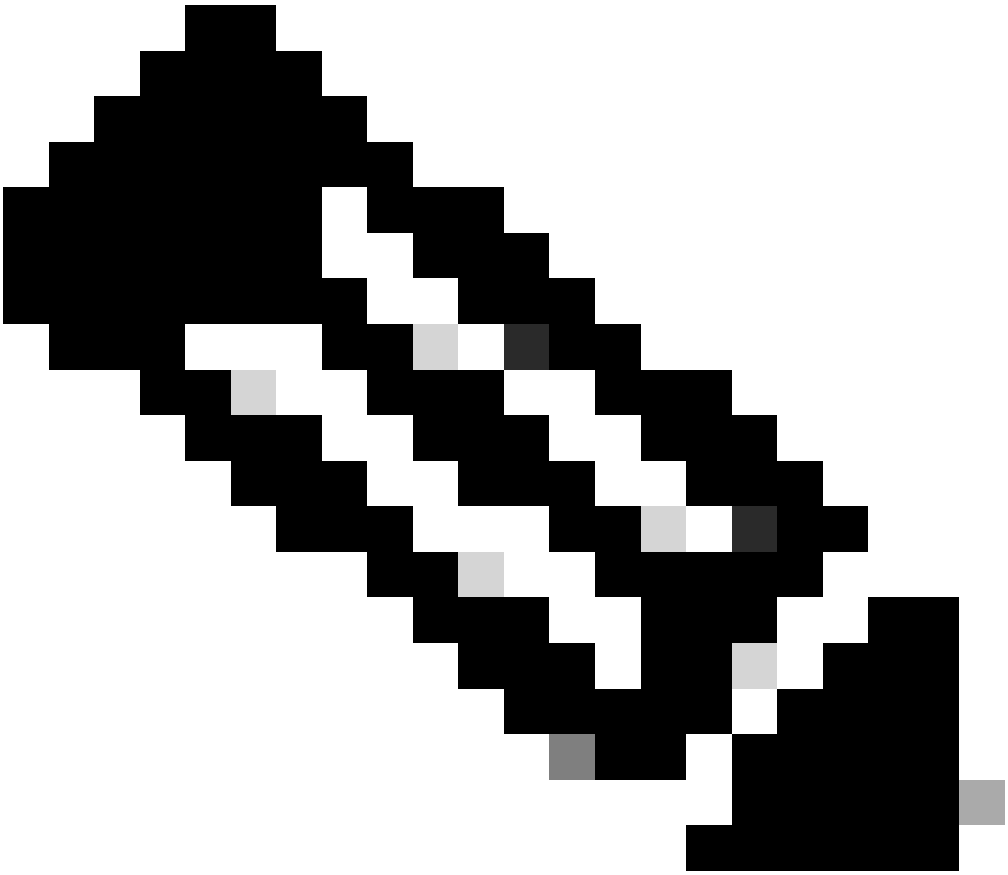
로그인 이벤트가 DC 간에 복제되므로 표준 도메인 컨트롤러에서 이 작업을 실행합니다. 그러나 검색할 때 어떤 이벤트도 표시되지 않고 특정 호스트에서 이벤트를 볼 것으로 예상하는 경우 서버 간에 이벤트 로그를 복제하는 데 문제가 발생할 수 있습니다. 이 경우 해당 호스트에서 사용하는 %LOGONSERVER%을(를) 찾은 다음 구체적으로 표시된 도메인 컨트롤러에서 스크립트를 실행합니다. 그래도 이벤트가 표시되지 않으면 로그온 이벤트가 감사되고 있는지 확인하십시오.

대본은 이 기사의 하단에 첨부되어 있다. 수집된 정보는 직접 또는 OpenDNS Support에서 트러블슈팅에 사용할 수 있습니다.

스크립트 실행

다음 단계를 완료하십시오.

1. 첨부된 텍스트 파일을 다운로드하고 확장명을 '.txt'에서 '.ps1'(으)로 변경합니다.



참고: 이중 확장명을 주의하고 실수로 ".txt.ps1"이라고 명명하지 마십시오.

2. 그런 다음 Windows 서버에서 가 시작한 새 PowerShell 창을 엽니다**'Right-Click -->Run as Administrator'**. 스크립트를 저장한 위치로 이동하여 다음을 **(eg: 'cd C:\Users\admin\Downloads'**입력하여 스크립트를 실행합니다. **.\loginsearch.ps1.**
3. 스크립트는 먼저 Windows 보안 이벤트 로그에서 검색할 사용자 이름을 묻는 메시지를 표시한 다음 IP로 검색하려는 경우 특정 IP 주소를 묻습니다. 화면 프롬프트를 사용합니다. 검색 결과를 특정 사용자 및 IP 주소로 동시에 제한하려는 경우 하나 또는 다른 검색(사용자 이름 또는 IP)을 개별적으로 사용하거나 둘 다 동시에 사용할 수 있습니다.
4. 스크립트가 빨리 실행됩니다. 작업이 완료되면 화면에 모두 시간 스탬프가 포함된 출력이 표시됩니다. 또한 화면에 표시되는 각 이벤트 로그 항목의 내보내기를 완료합니다. **'C:\%hostname%.txt'** 이 기능은 특정 이벤트를 더 자세히 살펴보려는 경우 유용할 수 있습니다.

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.