Active Directory Connector 성능 이해

목차

소개

이 문서에서는 Umbrella DNS의 Active Directory 커넥터 성능에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Umbrella DNS를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

Umbrella 커넥터 서비스는 Umbrella의 Active Directory 통합의 일부로 사용자/컴퓨터 로그인 이벤트를 모니터링하는 데 사용됩니다. OpenDNS 커넥터 서비스는 사이트에 있는 각 AD 도메인 컨트롤러의 보안 이벤트 로그에서 로그인 정보를 읽습니다.

사용자 로그인 이벤트의 빈도가 높은 환경에서는 이러한 성능 지침을 검토하는 것이 중요합니다. 정확한 사용자 식별을 위해서는 커넥터 서비스가 로그인 정보를 신속하게 검색할 수 있어야 합니다
.

최대 이벤트/초

처리할 수 있는 이벤트의 수에는 제한이 없습니다. Umbrella Connector 서비스는 "사이트"의 모든 도메인 컨트롤러에서 초당 연속 850개의 이벤트를 지원하도록 테스트되었습니다. 이는 실행 중인 타사 소프트웨어가 없는 전용 랩 환경을 기반으로 합니다. 실제 결과는 네트워크 레이턴시 및 기타 병목 현상에 따라 달라질 수 있습니다.

고객은 이 문서의 뒷부분에 나오는 "Events Per Second" 섹션을 참조하여 대략적인 이벤트 수를 확인할 수 있습니다.

새로운 기능

로그인 이벤트의 빈도가 높은 대규모 구축 고객의 경우 Umbrella는 새로운 성능 중심 기능을 제공합니다. 일반적인 성능 권장 사항 외에 로드 밸런싱, 병렬 통신 및 직접 이벤트 로그 판독기 연결에 대한 지침을 이 문서의 뒷부분에서 읽어 주십시오.

성능 권장 사항

커넥터 크기 조정

Active Directory Connector 서비스를 실행하는 서버에는 Umbrella 설명서의 크기 조정 가이드에 지정된 대로 CPU 및 메모리 리소스가 있어야 합니다.

전용 커넥터

커넥터 서비스를 도메인 컨트롤러에 직접 설치할 수 있지만 Cisco Umbrella에서는 커넥터 서비스 전용 멤버 서버에 커넥터를 설치하는 것이 좋습니다. 이 구성원 서버에는 다른 타사 소프트웨어가 설치되어 있지 않아야 합니다. Umbrella 설명서에서 설치 프로세스에 대한 자세한 내용을 읽으십시오.

Umbrella 사이트

가능한 경우 Umbrella 구축은 네트워크 전체에서 통신하는 구성 요소를 제한하는 "사이트"로 분리해야 합니다. 커넥터 서비스는 동일한 Umbrella 사이트의 구성 요소와만 통신할 수 있습니다. 이 기능은 사용자가 대규모 지역에 배포된 배포를 가지고 있을 때 항상 사용해야 합니다.

일반적으로 Umbrella 사이트는 각 물리적 위치에 대해 생성됩니다. Umbrella 사이트에서는 Umbrella 설명서에서 이러한 규칙을 반드시 확인해야 합니다.

Umbrella 사이트를 적절하게 사용하면 구축을 크게 개선하고 WAN을 통해 통신하는 구성 요소를 방지할 수 있습니다.

네트워크 레이턴시

로그인 이벤트는 네트워크를 통해 커넥터로 전송할 수 있습니다. 커넥터와 각 도메인 컨트롤러 간에 고속 연결이 있어야 네트워크 관련 지연을 줄일 수 있습니다. 커넥터는 도메인 컨트롤러 및 가상 어플라이언스에 최대한 가깝게 배치할 수 있습니다.

커넥터 수

각 Umbrella 사이트에는 하나의 커넥터가 필요합니다. Umbrella 사이트에는 여러 개의 커넥터가 있을 수 있지만 이중화를 위해서만 필요합니다. 추가 커넥터가 있으면 첫 번째 커넥터와 동일한 기능을 복제하므로 도메인 컨트롤러에 추가 로드가 발생합니다. Umbrella는 각 Umbrella 사이트에 대해 최대 2개의 커넥터를 권장합니다.

이벤트 로그 크기

Windows 보안 이벤트 로그가 크면 이 WMI 작업의 성능에 부정적인 영향을 줄 수 있습니다. Umbrella에서는 이벤트 로그 크기를 제한할 것을 권장합니다. 가장 좋은 성능은 512MB 미만의 로그 파일을 사용하지만, 이는 로그 보존 요구 사항에 따라 조정될 수 있습니다. 로그 파일 크기는 다음 지침을 사용하여 조정할 수 있습니다.

1. 이벤트 뷰어 애플리케이션(eventvwr.msc)을 엽니다.

2. Windows 로그 > 시스템으로 이동

3. 시스템 로그를 마우스 오른쪽 버튼으로 클릭하고 속성을 선택합니다.

4. 원하는 대로 최대 로그 파일 크기를 조정하고 확인을 선택합니다.

서드파티 소프트웨어

다른 많은 소프트웨어 제품에서도 WMI를 사용하므로 도메인 컨트롤러의 WMI에 병목 현상이 발생할 수 있습니다. 여기에는 다음이 포함될 수 있습니다.

- 이벤트 로그를 모니터링하는 서드파티 보안/분석 소프트웨어
- Windows 이벤트 로그 전달
- SIEM 통합 및 이벤트 로그를 모니터링하는 기타 소프트웨어

이 소프트웨어가 더 이상 필요하지 않으면 비활성화하는 것이 좋습니다. 또는 부록에 설명된 '직접 이벤트 로그 판독기 연결' 방법을 사용하여 이 문제를 완화할 수 있습니다.

안티바이러스 소프트웨어

안티바이러스 검사에서 이 폴더 및 다음 실행 파일 제외:

```
C:\Program Files (x86)\OpenDNS\OpenDNS Connector
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\OpenDNSAuditService.exe
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\<VERSION>OpenDNSAuditClient.exe
```

추가 도메인 컨트롤러

도메인 컨트롤러의 WMI 알림 시스템은 각 이벤트 로그 항목을 큐잉하고 처리하여 WMI 가입자에게 전송합니다. 이것은 효과적으로 DC에 의해 이벤트가 전송되는 푸시 메커니즘입니다. 따라서 이벤트를 전송하는 속도에 영향을 주는 성능 병목 현상이 도메인 컨트롤러 자체에 발생할 수 있습니다.

AD 환경에 도메인 컨트롤러를 추가하여 이러한 병목 현상을 완화할 수 있습니다. Umbrella는 단일 도메인 컨트롤러를 최대 850개/s의 이벤트를 테스트했습니다.

서비스 계정 예외

서비스 계정을 제외하여 Umbrella에서 탐지한 AD 로그인 수를 줄입니다. 올바른 정책 적용을 위해 이러한 어카운트는 제외해야 합니다. 또한 AD 사용자 정책을 사용하지 않지만 많은 사용자 로그온을 할 수 있는 서버 및 기타 디바이스를 제외할 수 있습니다.

WMI 패치

도메인 컨트롤러 및 커넥터 서버가 최신 Microsoft 패치로 최신 상태인지 확인하십시오. 다음은 알려진 WMI 성능 문제를 해결하는 핫픽스의 예입니다.

WMI 메모리 및 핸들 제한

WMI에 병목 현상을 만들 수 있는 자체 내부 제한이 있습니다. 특히 다른 소프트웨어에서 집중적인 WMI 작업을 수행하는 경우에는 더욱 그렇습니다. 이러한 제한을 늘리는 방법의 예는 Microsoft 설명서에서 찾을 수 있습니다.

Umbrella 지원에서는 환경에 대한 올바른 제한을 조언할 수 없습니다. Microsoft에 도움을 요청하십시오.

DC 로드 밸런싱

Umbrella는 이제 사이트에 여러 도메인 컨트롤러 및 많은 로그온 이벤트가 있을 때 유용한 로드 밸런싱 기능을 지원합니다. 이 시나리오에서는 추가 커넥터가 설치되고 도메인 컨트롤러가 로드 밸런

싱 그룹을 통해 커넥터에 할당됩니다.

간단한 환경에서는 로드 밸런싱이 다음과 같이 작동합니다.

- DC_A 및 DC_B는 Connector_1에 의해 처리되는 로드 밸런싱 그룹_1에 할당됩니다.
- DC_C 및 DC_D는 Connector_2에서 처리하는 로드 밸런싱 그룹_2에 할당됩니다.
- 가상 어플라이언스는 두 커넥터에서 이벤트를 계속 수신하므로 모든 로그온 이벤트를 계속 인식합니다.
- 이중화가 필요한 경우 각 로드 밸런싱 그룹에 추가 커넥터를 설치할 수 있습니다.

이 기능은 다음과 같은 이점을 제공합니다.

- 각 커넥터의 업무량이 크게 감소합니다. 각 커넥터가 더 적은 수의 도메인 컨트롤러를 처리하고 있습니다.
- 이는 일반적으로 DC에서 이벤트를 수신하는 데 지연이 많은 시나리오에서 도움이 됩니다.

로드 밸런싱은 도메인 컨트롤러가 많은 복잡한 멀티 사이트 환경에서 사용하도록 확장할 수 있습니다. 추가 커넥터를 설치하는 것 외에 로드 밸런싱을 사용하는 데에는 단점이 없습니다.

이때 로드 밸런싱 기능은 Umbrella 지원에 의해 활성화되어야 합니다. Umbrella 지원에 문의하여 요구 사항에 대해 논의하십시오.

가상 어플라이언스 병렬 통신

이제 커넥터는 기본 직렬 방법을 사용하지 않고 여러 가상 어플라이언스에 로그인 이벤트를 동시에 전송할 수 있습니다. 이 기능은 사이트에 여러 가상 어플라이언스가 있고 로그온 이벤트가 많은 경우 유용합니다.

이 기능은 다음과 같은 이점을 제공합니다.

- 여러 어플라이언스가 있는 경우 로그인 정보 전송 지연을 최소화합니다. 이벤트는 한 번에 모든 어플라이언스로 전송될 수 있습니다.
- 한 어플라이언스에서 다른 어플라이언스에 대한 Knock-on 효과가 있는 통신 문제 또는 중단을 방지합니다. 각각에 대해 별도의 이벤트 대기열이 유지됩니다.

이 기능은 이제 자동으로 활성화되지만, 서버가 CPU 및 메모리 권장 사항을 충족하는 경우에만 활성화됩니다.

사용자 로그인 이벤트 전송 가속화

커넥터는 이제 사용자 로그인 이벤트를 일괄 처리로 전송할 수 있으므로 가상 어플라이언스로 전송할 수 있는 초당 이벤트 수(초당)가 크게 증가합니다. 이는 특히 커넥터가 원격 위치에서 가상 어플라이언스와 통신하는 데 중요합니다.

이제 이 기능을 자동으로 활성화할 수 있지만 다음과 같은 요구 사항이 있습니다.

- 위의 병렬 통신을 활성화해야 합니다. 서버는 CPU 및 메모리 권장 사항을 충족해야 합니다.
- ADC 버전 1.8 이상 필요

- 커넥터 버전 3.2.0 이상 필요

직접 이벤트 로그 판독기 연결

Active Directory 커넥터 버전 1.4 이상에서는 WMI 쿼리를 사용하지 않고 도메인 컨트롤러의 보안 이벤트 로그에 직접 연결하는 새로운 방법을 지원합니다. 이렇게 하면 WMI가 "중간 사용자"로 제거되고 WMI에 병목 현상이 발생하는 경우 성능이 크게 향상됩니다. 이는 개별 도메인 컨트롤러가 많은 로그인 이벤트를 처리하는 시나리오에서 특히 유용합니다.

이 기능은 올바른 사용자가 식별될 때 짧은(예: 5초) 지연이 발생하기 때문에 커넥터가 5초마다 새 이벤트를 가져오는 끌어오기 메커니즘을 사용하여 작동합니다.

이제 이 최적화가 기본적으로 활성화됩니다. 이 기능에 대한 자세한 내용은 Umbrella 지원에 문의하십시오.

초당 이벤트 수

초당 이벤트를 추정하기 위해 도메인 컨트롤러에서 최근 이벤트의 수를 계산할 수 있습니다. Umbrella는 다음과 같이 피크 시간에 이 작업을 수행할 것을 권장합니다.

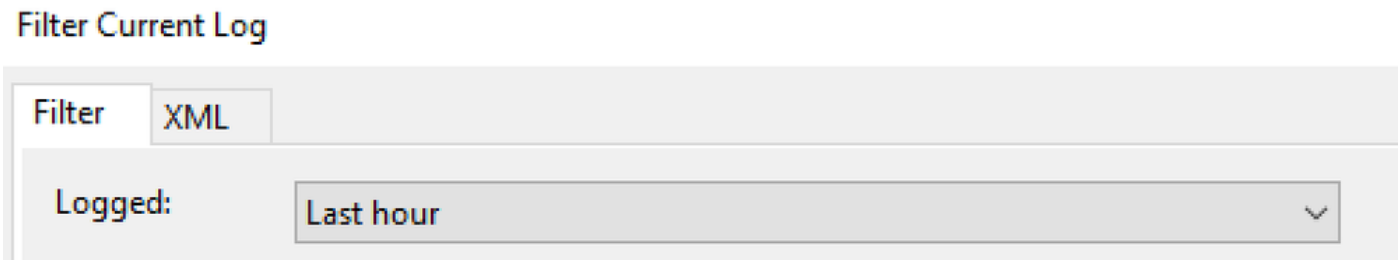
1. 이벤트 뷰어 애플리케이션(eventvwr.msc)을 엽니다.

2. Windows 로그 > 시스템으로 이동합니다.

3. 현재 로그 필터링을 선택하고 지난 시간에 로그인한 이벤트를 선택합니다.

4. 확인을 선택합니다.

필터가 로드되면 이벤트 로그에 지난 1시간 동안의 이벤트 수가 표시될 수 있습니다. 이 값은 초당 이벤트를 추정하기 위해 3600으로 나눌 수 있습니다.



360024901511

360024894112

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.