Secure Access 가상 어플라이언스 구축 후 Active Directory 오프라인 통합

목차

문제

두 개의 VA(Secure Access Virtual Appliance)를 배포한 후 AD(Active Directory) 통합이 Secure Access 대시보드 내에서 작동을 중지했습니다. 이전에는 AD 통합이 작동했지만 VA를 배포한 후 AD 커넥터가 Secure Access 대시보드에 오프라인으로 표시됩니다. AD 연결을 복원하려면 지원이 필요합니다.

환경

- 기술: 솔루션 지원(SSPT - 계약 필요)
- 하위 기술: 보안 액세스
- 소프트웨어 버전: 모두
- 보안 액세스(DNS-Advantage/Umbrella)
- 본사에 2개의 Secure Access VA(Virtual Appliance) 구축
- 이벤트 변경: AD 커넥터 장애 직전의 VA 설치
- AD 커넥터가 이전에 작동했으며 이제 Secure Access 포털에 오프라인으로 표시됩니다.

해결

VA 구축 후 Secure Access 포털에서 오프라인으로 표시되는 AD 통합 문제를 해결하려면 다음 세부 문제 해결 단계를 수행합니다.

커넥터 재시작 중 네트워크 트래픽 캡처

커넥터 서비스를 다시 시작하는 동안 AD 커넥터/도메인 컨트롤러의 모든 인터페이스에서 Wireshark 캡처를 실행합니다. 이렇게 하면 커넥터 초기화 중에 네트워크 통신 실패나 무단 액세스 시도를 식별할 수 있습니다.

1단계: 모든 관련 인터페이스에서 Wireshark 캡처 시작

Wireshark를 시작하고 모든 AD 커넥터/도메인 컨트롤러 인터페이스에서 캡처를 시작합니다.

2단계: Windows 서비스 관리자를 통해 Connector 서비스 다시 시작

services.msc를 열고 OpenDNS Connector 서비스를 찾은 다음 Restart를 클릭합니다.

3단계: 추가 분석을 위해 캡처 파일 저장

캡처를 중지하고 .pcap 파일을 내보냅니다.

커넥터 로그 수집

AD 커넥터에서 로그를 수집하여 오류 또는 인증 문제를 심층적으로 파악합니다.

1. 로그 디렉토리로 이동합니다.

```
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\vX.X.X
```

1. 관련 로그 파일을 수집하고 검토할 수 있도록 준비합니다. 앞서 언급한 디렉터리의 모든 로그 파일을 안전한 위치로 복사하십시오.

AD 커넥터 계정 권한 확인

가상 어플라이언스를 도입한 후 AD 커넥터 계정이 올바르게 작동하려면 특정 권한이 필요합니다. 계정에 이벤트 로그 판독기 역할이 없으면 무단 액세스 예외가 발생할 수 있습니다.

1. AD Connector 계정에 이벤트 로그 판독기 권한을 할당합니다. ADUC(Active Directory 사용자 및 컴퓨터) 또는 그룹 정책을 사용하여 AD 커넥터 계정을 이벤트 로그 판독기 그룹에 추가하십시오.
2. 계정에 새 권한이 있는지 확인하십시오. AD 커넥터 계정에 대한 그룹 구성원 자격을 확인하여 이벤트 로그 판독기 포함 여부를 확인하십시오.

공통 예외 발견

트러블슈팅 중에 로그 또는 커넥터 상태 출력에서 이 예외를 관찰할 수 있습니다.

```
* Exception type: system.unauthorizedaccessexception
message: Attempted to perform an unauthorized operation.
```

이는 AD 커넥터 계정에 충분한 권한이 없음을 나타냅니다. 특히 이벤트 로그 판독기 역할은 VA가 도입된 후 필수입니다.

오프라인에서 AD 커넥터 상태를 온라인으로 변경하는 CLI 명령을 찾을 수 없습니다.

원인

근본적인 원인은 Secure Access Virtual Appliance를 배포한 후 AD 커넥터 계정에 대한 권한이 충분하지 않기 때문입니다. 계정에 적절한 AD 커넥터 기능에 필요한 이벤트 로그 판독기 권한이 없습

니다. 이로 인해 "system.unauthorizedaccessexception" 오류가 발생하여 커넥터가 Secure Access 포털 내에서 온라인으로 작동하지 않습니다.

관련 콘텐츠

- Cisco 기술 지원 및 다운로드

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.