액세스 정책에서 디렉터리 검색을 수행하는 동안 신뢰할 수 있는 도메인에 대한 AD 그룹을 찾을 수 없는 이유는 무엇입니까?

목차

질문:

액세스 정책에서 디렉터리 검색을 수행하는 동안 신뢰할 수 있는 도메인에 대한 AD 그룹을 찾을 수 없는 이유는 무엇입니까?

환경:Cisco WSA(Web Security Appliance), NTLM 인증, 신뢰할 수 있는 도메인

증상:

- 사용자가 자신의 액세스 정책 중 하나에서 *정책 구성원 정의*로 사용할 "Active Directory 그룹 "을 조회하려고 하는데 해당 그룹이 디렉터리 검색에 표시되지 않습니다.
- 그룹은 WSA가 가입한 도메인이 아니라 신뢰할 수 있는 AD 도메인에 속합니다.

이 동작은 설계에 의한 것입니다.액세스 정책에서 그룹을 구성하는 동안 신뢰할 수 있는 도메인의 그룹이 *디렉토리 검색*에 표시되지 않습니다.

모든 AsyncOS 버전에서 WSA는 다른 도메인의 사용자를 인증하고 다른 도메인에 WSA가 가입한 도메인과 양방향 신뢰가 **있는 경우** 해당 AD 그룹과 일치시킬 수 있습니다.

이러한 시나리오에서는 다음 단계를 사용하여 액세스 정책에서 신뢰할 수 있는 도메인의 그룹을 추가할 수 있습니다.

1. GUI —> Web Security Manager —> Access Policies —> *<Policy Name>* —> 선택한 그룹 및 사용자 —> 그룹으로 이동합니다.
2. 도메인 이름과 함께 전체 그룹 이름을 '*Directory Search'* 필드에 수동으로 입력합니다.
3. "Add(추가)" 버튼을 클릭합니다.
4. done(완료)을 클릭한 다음 Submit & commit(제출 및 변경 사항 커밋)

다른 도메인이 WSA에서 가입한 도메인과 양방향 트러스트 관계가 없는 경우 WSA는 수동으로 구성된 그룹과 매칭되지 않습니다

참고: AsyncOS 버전 7.7 이상에서 WSA는 여러 NTLM 영역을 지원하며, 두 도메인 간에 신뢰 관계가 없는 시나리오에서는 두 번째 도메인에 대해 새 NTLM 영역을 생성할 수 있습니다.여러 NTLM 영역을 사용하는 경우 WSA는 액세스 정책 내에서 다른 도메인의 그룹을 조회할 수 있습니다.