

LDAP 인증 그룹 정책을 수행하도록 WSA를 구성하려면 어떻게 합니까?

목차

[질문:](#)

질문:

환경: Cisco WSA(Web Security Appliance), 모든 버전의 AsyncOS

이 기술 자료 문서는 Cisco에서 유지 관리하거나 지원하지 않는 소프트웨어를 참조합니다. 이 정보는 귀하의 편의를 위해 제공됩니다. 자세한 내용은 소프트웨어 공급업체에 문의하십시오.

"인증 그룹"이 작동하려면 먼저 "GUI > 네트워크 > 인증"에서 인증 영역을 구성해야 합니다.

1. 먼저 "Authentication Protocol(인증 프로토콜)"을 'LDAP'로 설정하고 "Group Authorization(그룹 권한 부여)"으로 이동합니다(다른 섹션이 올바르게 구성되어 있음).
2. "그룹 이름 특성"을 지정합니다. "Web Security Manager" > "Web Access Policies" > "Click Group" > "Select Group Type to Authentication Group" > "Directory Lookup" 테이블에 표시되는 값을 포함하는 특성입니다. 이 속성은 고유해야 하며 이 속성으로 표시되는 리프 노드에 그룹의 사용자 목록이 있어야 합니다.
3. 다음으로 "Group Filter Query(그룹 필터 쿼리)"를 지정합니다. LDAP 디렉터리에서 모든 GROUP을 찾는 데 WSA가 사용하는 검색 필터입니다.
4. 이제, 구성원 고유 값을 보유할 리프 노드의 특성인 "그룹 구성원 특성"을 지정합니다. 이 속성은 이 GROUP의 멤버를 보유하므로 여러 항목이 표시됩니다. 이 특성에 포함된 값이 동일한 페이지에 있는 "사용자 이름 특성"에 포함된 값과 일치하는지 확인하십시오.

다음은 WSA에서 LDAP 영역 컨피그레이션을 사용하여 LDAP 그룹에 대한 사용자 이름을 매칭하는 방법의 예입니다.

1. "Group Filter Query"를 "objectClass=group"으로 설정했다고 가정하겠습니다.
2. WSA는 먼저 이 필터를 사용하여 LDAP 디렉토리를 검색하고 결과를 찾습니다.
3. 그런 다음 결과를 사용하여 WSA는 "Group Membership Attribute"에 지정된 특성을 찾습니다. "member"라는 속성이라고 합니다.
4. 이제 사용자가 WSA 프록시를 통해 'USERNAME_A'로 로그인하면 WSA는 LDAP 서버에서 사용자 계정을 조회하고 일치하는 항목이 있으면 "User Name Attribute(사용자 이름 특성)"에 지정된 특성을 사용합니다(예:uid)를 확인하고 "uid"가 위에서 수집한 "member" 속성에 나열된 사용자와 일치하는지 확인합니다.
5. 일치하는 항목이 있는 경우 사용자는 구성된 정책을 사용하고, 그렇지 않은 경우 WSA는 다음 정책을 라인 평가합니다.

LDAP 서버를 사용하여 구성해야 하는 특성을 보려면 "Softerra LDAP Browser"
<http://www.ldapbrowser.com>을 참조하십시오.