Active Drectory 사용자 그룹 조직 구성 단위 모범 사례 분석

정지훈

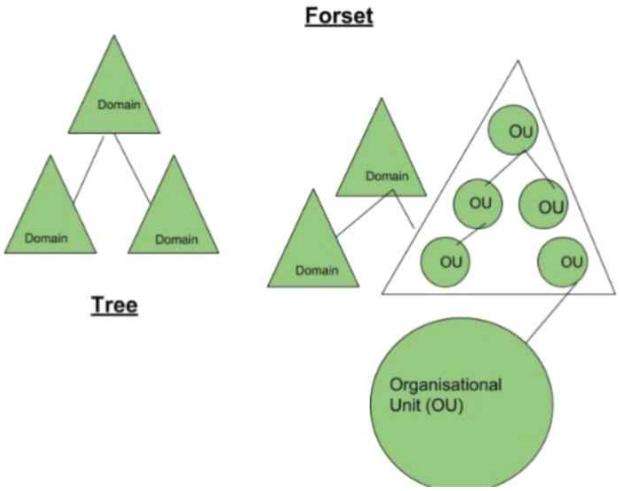
목차

1. Active Directory(AD)란?

: 마이크로소프트가 윈도우용 환경에서 사용하기 위해 개발한 LDAP 디렉터리 서비스이— 기능

목적: 윈도우 기반의 컴퓨터들을 위한 인증 서비스를 제공하는 것

Active Directory는 오래된 윈도우 문서들 안에서 NTDS (NT 디렉터리 서비스) 라고도 불린다.



[AD 용어]

도메인(Domain)
-Acive Directory의 가장 기본의 되는 단위
- 도메인이 여러개 있을 경우 부모 도메인과 자식 도메인으로 구분가능하다.

트리(Tree)와 포리스트(Forest)
-트리는 도메인의 집합, 개념적인 것으로 보면 된다..
-여러개의 트리로 Active Directory가 구성될 경우 이를 포리스트(Forest)

사이트(Site)
-물리적인 범주에 가깝다.
-사이트는 지리적으로 떨어져 있으며, IP 주소 대가 다르다.

트러스트(Trust)
-도메인 또는 포리스트 사이에 신뢰할지 여부에 대한 관계를 나타내는 의미로 사용
-트러스트 안 도메인 사이에는 상호 양방향 전이 트러스트를 갖는다.

조직구성단위(OU)

-도메인 내부에서 사용되는 일종의 폴더와 같은 개념
-권한 위임과 그룹 정책을 적용할 수 있는 최소한의 단위

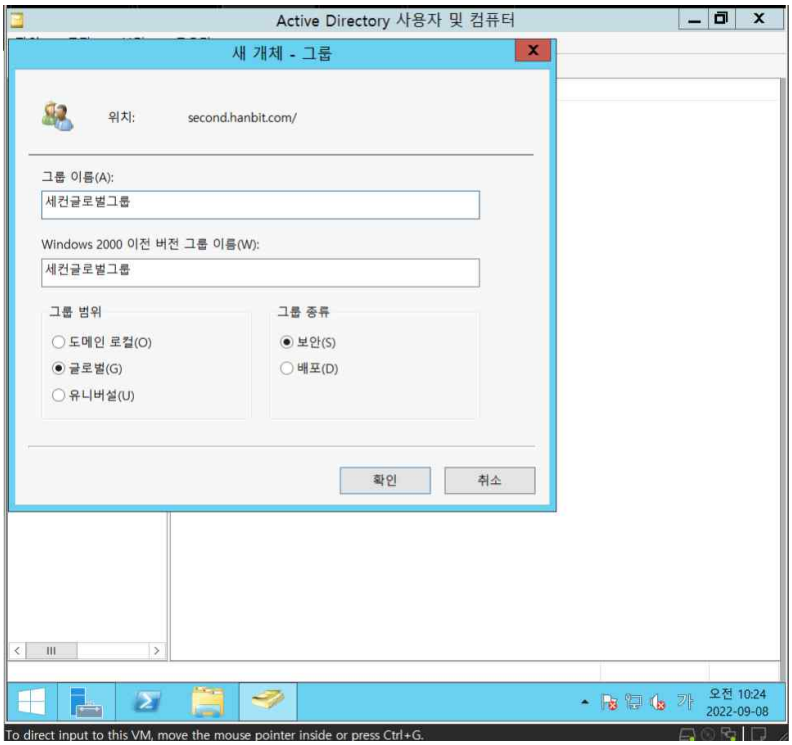
도메인 컨트롤러(Domain Controller)
-로그인, 이용권한 확인, 새로운 사용자 등록, 암호변경 등을 처리하는 기능을 하는 서버 컴퓨터

글로벌 카탈로그(Global catalog)
-AD 트러스트 내의 도메인들에 포함된 개체에 대한 정보를 수집하여 저장되는 통합 저장소
- 사용자의 경우 이름, 아이디, 비밀번호 등의 정보가 글로벌 카탈로그에 저장된다.

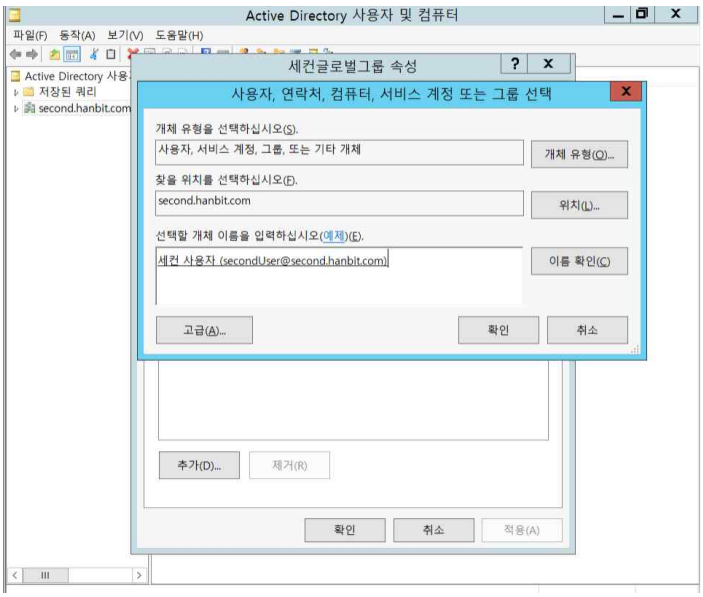
AD의 장점
- 공유 자원에 대한 정보 검색이 편리하다.
- 네트워크 환경에서 Domain 자원을 공유할 수 있다.
- 서버가 많아질수록 인증 절차가 점점 복잡해지지만 AD DS을 이용하면 단일화된 로그인 처리가 가능하다.(하나의 서버에서 모든 인증처리를 할 수 있다.)
- 다른장소에서 자신의 아이디로 로그인만 하면 타인의 PC가 자신의 PC환경과 마찬가지로 변경된다.

AD DS(Active Directory Dmoain Serice)
- Object(객체)에 대한 정보를 네트워크 상에 저장하면 Active Directroy Domain Service는 이러한 정보들을 통합하여 관리하게 된다.

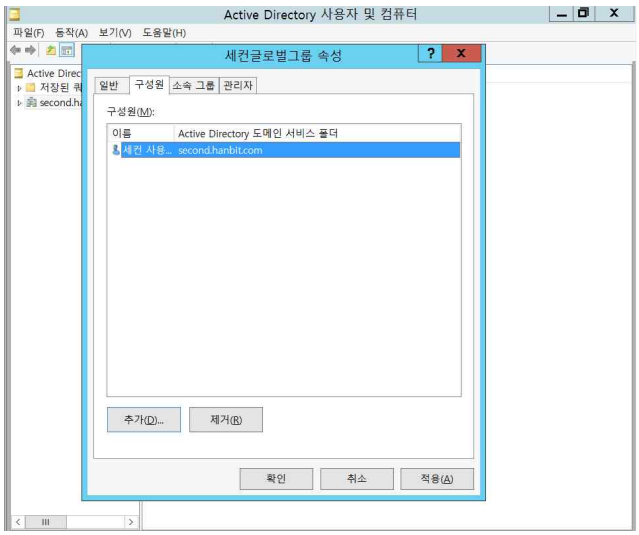
2. AGDLP 구현 실습



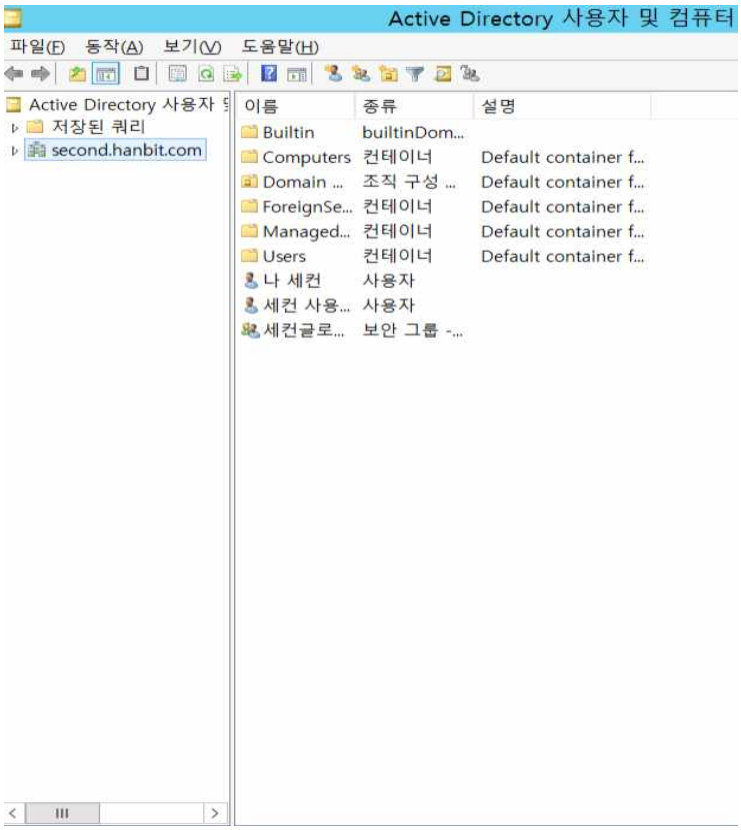
second 서버 > 새로운 글로벌 그룹 생성

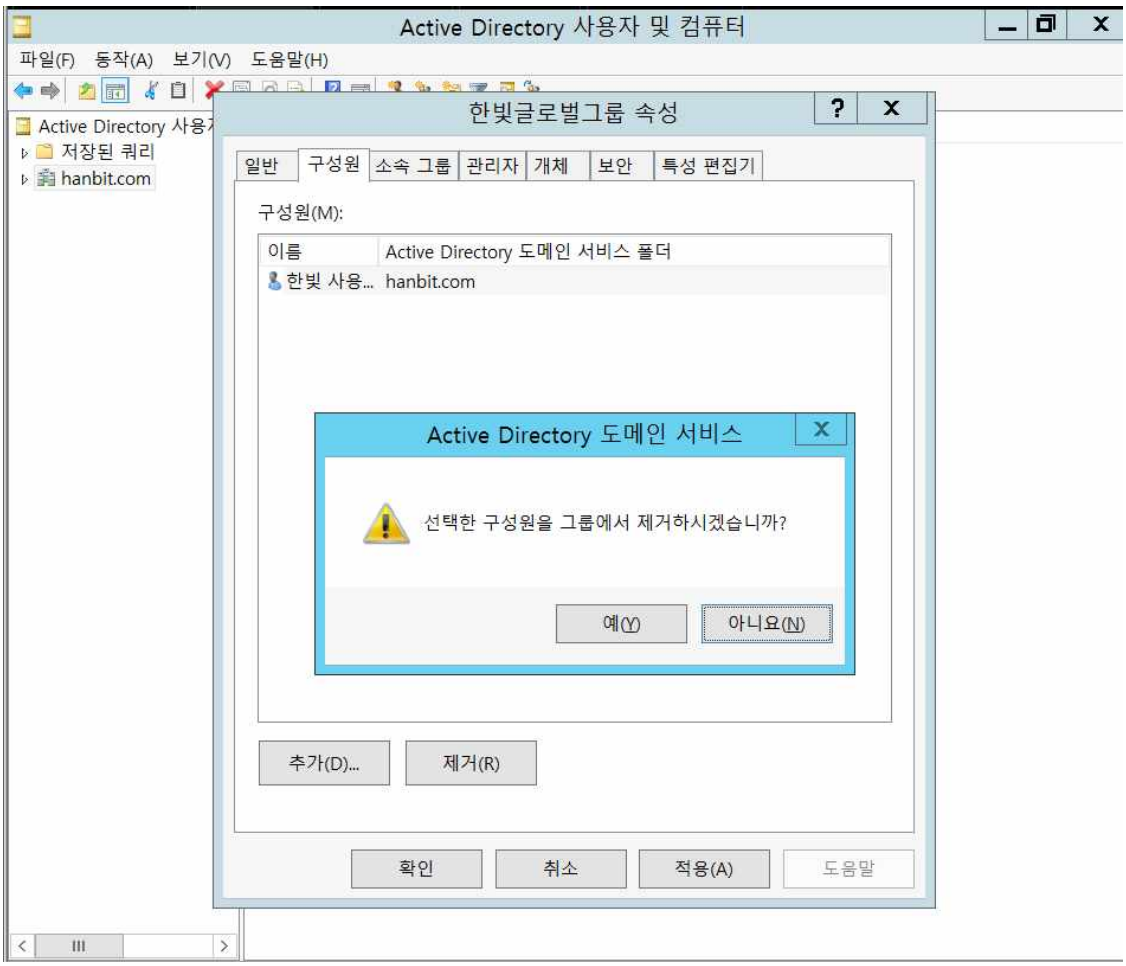


세컨 글로벌그룹 > 세컨 사용자 추가

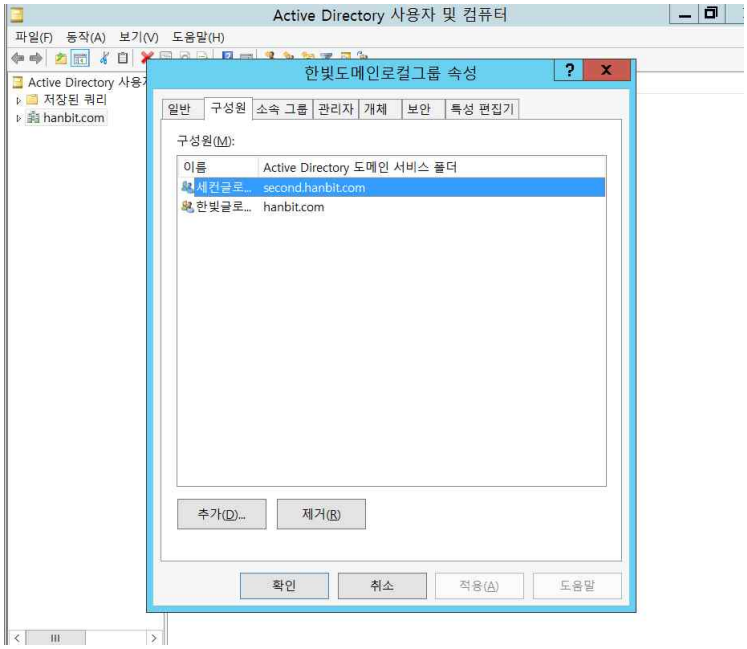


그룹 > 속성 > 구성원 > 선택할 개체 > 세컨 사용자 추가

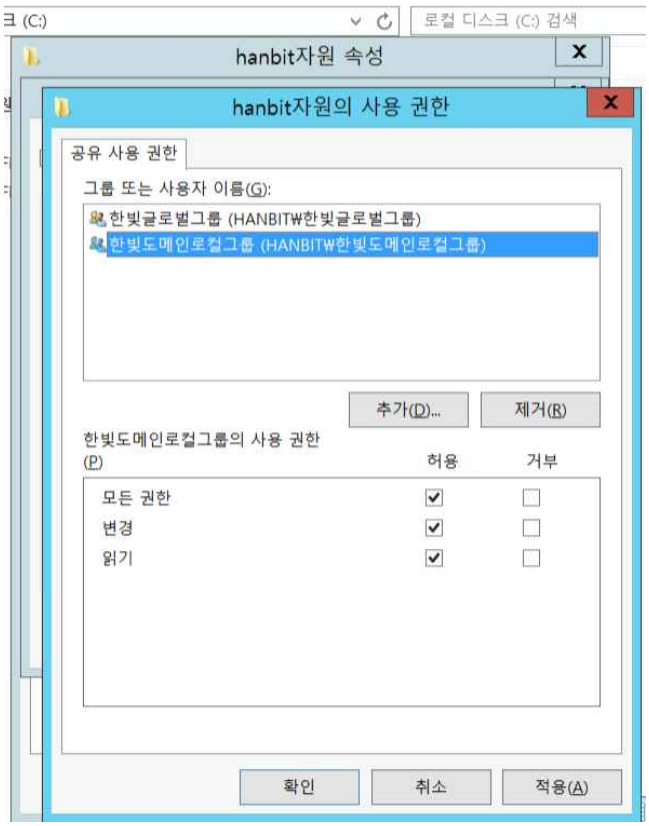




한빛글로벌그룹 속성 > 구성원: 한빛사용자 제거

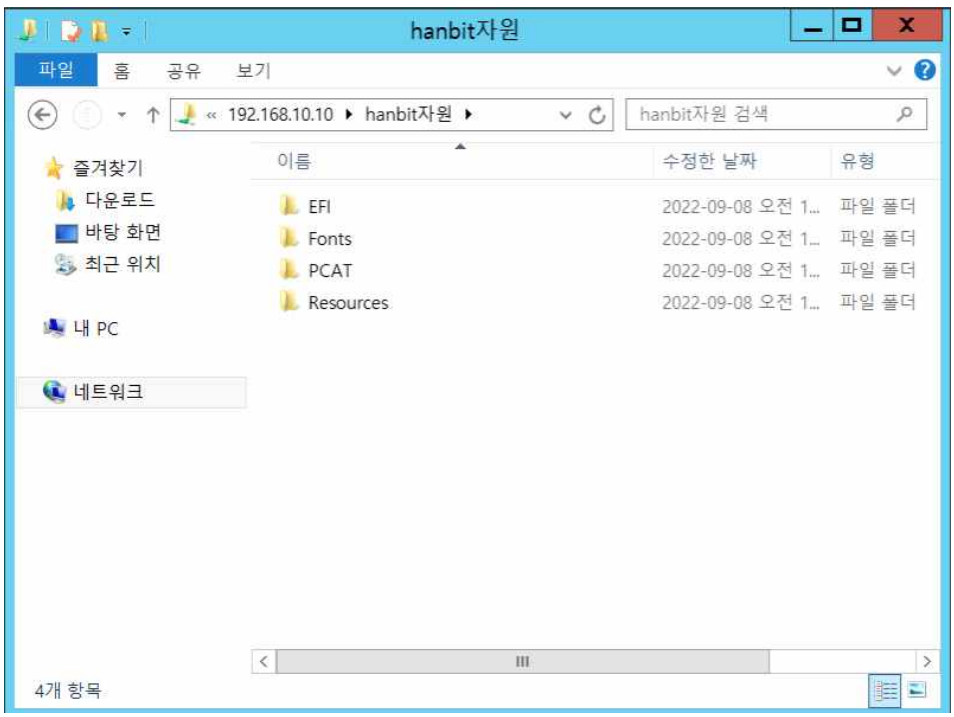


한빛도메인로컬그룹 속성 > 세컨글로벌그룹, 한빛글로벌그룹 추가



hanbit자원 폴더 공유사용권한 (한빛글로벌 그룹, 한빛도메인로컬그룹) 추가

secondUser로 접속



FIRST DNS 서버로 접속했을 때 정상적으로 출력이 된다.