

Windows Server Active Directory

AD 개요

- Microsoft사에서 제공하는 대규모 네트워크 관리 및 운영을 위한 기술
 - 대규모 회사는 지역적으로 분산된 환경에서 많은 수의 컴퓨터를 운영
 - 이러한 네트워크 환경에서 ‘단일 서버’은 한계가 있음
- 네트워크 상으로 나눠져 있는 여러 자원(Resource)을 중앙 관리자가 통합 관리
 - 직원들은 자신의 PC에 모든 정보를 보관할 필요가 없어짐
 - PC가 있는 장소와 무관하게 회사의 어디서든 자신의 ID로 회사 전체 자원을 편리하게 사용
- 통합 관리를 위해 AD에서 지원되는 기술은 굉장히 많음
 - 주로 윈도우 사용자 및 윈도우 단말의 일괄 관리를 위해 사용
- 생소한 용어 및 구성이 어려워 진입 장벽이 높음

AD 용어

- Directory Service
 - 분산된 네트워크 관련 자원 정보를 중앙 저장소에 통합시켜 관리 가능하게 해주는 서비스
 - 즉. 사용자는 중앙의 저장소를 통해 원하는 네트워크 자원에 대한 정보를 ‘자동으로’ 취득/접근
- Active Directory (AD)
 - Directory Service를 Windows Server에서 구현한 것
- Active Directory Domain Service (AD DS)
 - AD를 통해 컴퓨터 사용자, 기타 주변 장치에 대한 정보를 네트워크상에 저장하고 이 정보를 관리자가 통합 관리
 - Domain Controller 필요 (= DNS)
- Domain Controller (= DNS)
 - 로그온, 이용 권한 확인, 새로운 사용자 등록, 암호 변경, 그룹 등을 처리하는 서버 컴퓨터
 - 각 도메인마다 하나 이상의 DC 설치
- 읽기 전용 Domain Controller (RODC)
 - 주 DC로부터 AD 관련 데이터를 전송 받아 저장 후 사용 (데이터 추가/변경 불가)
 - 본사와 멀리 떨어진 지사에 사용
 - DC는 필요 하지만 규모가 크지 않아 관리자를 두기 어려운 경우 또는 주 컨트롤러의 부하를 분담 위해 사용

AD 용어

- Domain (= Group)

- AD의 가장 기본 단위로 서울본사, 부산 지사 등이 각각 하나의 도메인
- 즉. 관리 범위를 표현

- 트리(Tree)

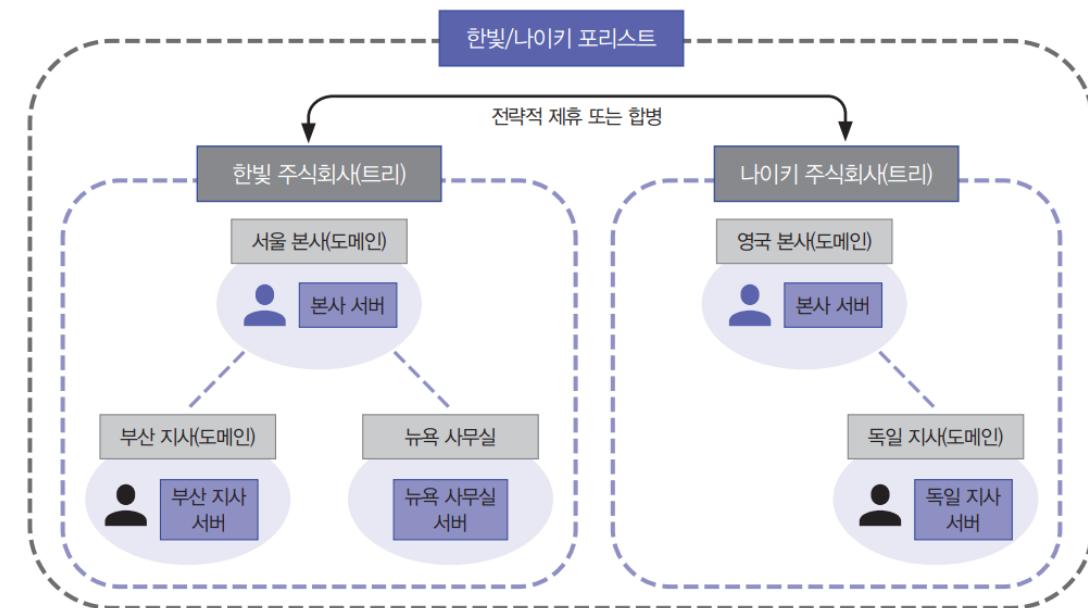
- 도메인의 집합
- RAPA.com = 서울지사, 부산지사, 광주지사
 - RAPA Tree
 - » 서울지사 = rapa.com = 부모 도메인
 - » 부산지사 = bs.rapa.com = 자식 도메인
 - » 광주지사 = gj.rapa.com = 자식 도메인

- 포리스트 (Forest)

- 서로 다른 Tree의 묶음

* 도메인 < 트리 < 포리스트

* 도메인 < 트리 ≤ 포리스트



AD 용어

- 조직 구성 단위 (Organizational Unit , OU)
 - 도메인을 세부적으로 나눈 단위
 - RAPA 서울 지사 (= RAPA 서울 도메인)
 - 인사팀 (OU)
 - 관리팀 (OU)
 - 운영팀 (OU)
- 글로벌 카탈로그 (Global Catalog , GC) [트리내에 1개 이상의 GC 필수](#)
 - AD 도메인 안에 포함된 개체에 대한 정보를 수집해 저장하는 통합 저장소
 - 사용자의 정보 , 전체 이름 , 아이디 , 암호 등..
 - 가장 먼저 설치하는 Domain Controller가 GC 서버로 지정 됨
 - 필요시 모든 DC는 GC로 동작 가능
 - 각 지사에 관리해야 하는 정보가 방대한 경우 부하 분산 용도 (AD 성능 향상)
 - 서울 DC = 서울 GC / 부산 DC = 부산 GC / 광주 DC = 광주 GC

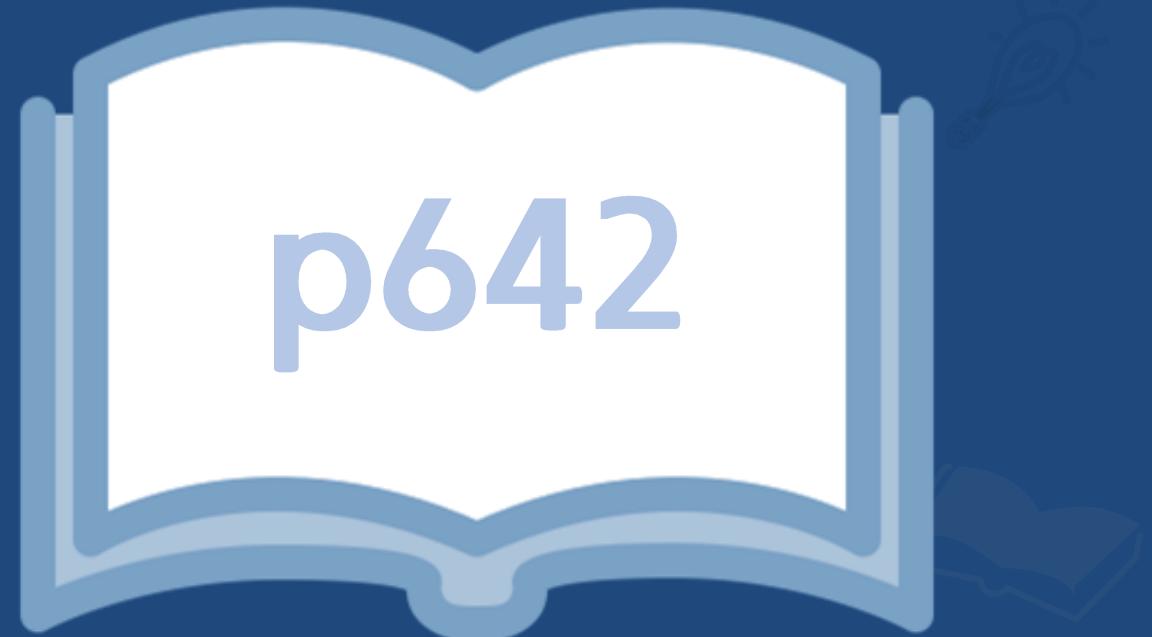
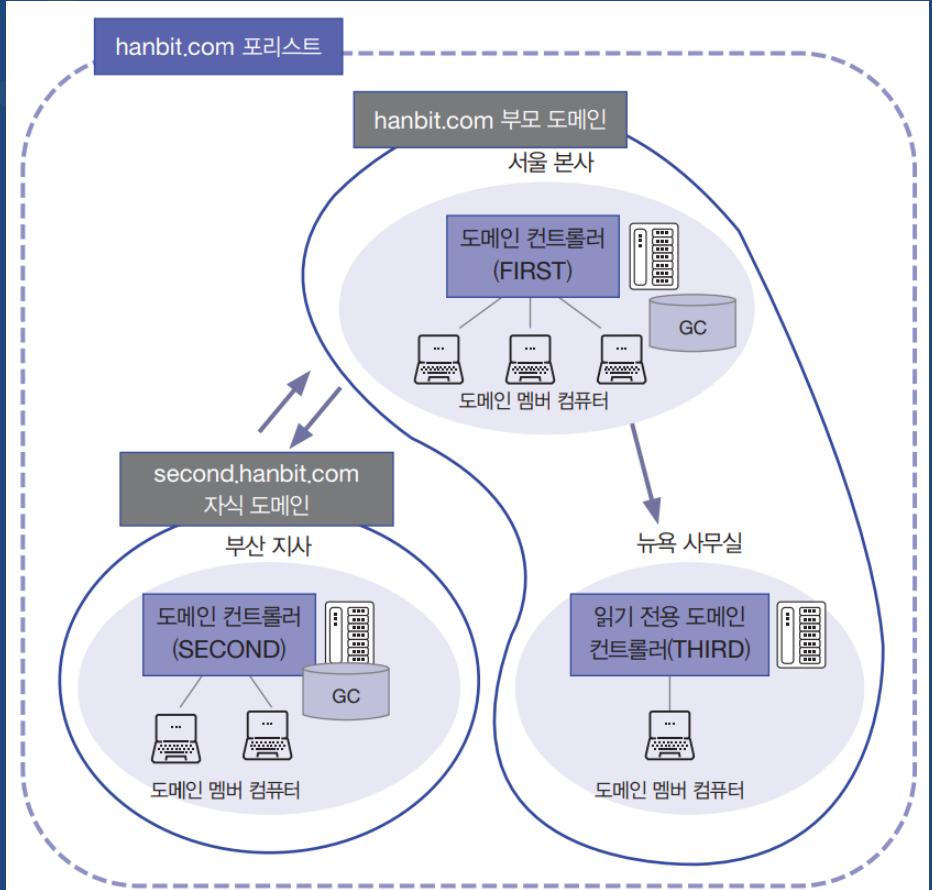
AD 필요성

- 회사 사용자의 정보 관리 일원화
- 그룹정책을 통해 사용자의 관리 및 정책 관리
 - 사용자 그룹 정책
 - 특정 계정은 ESXi 서버의 VM 생성 불가 ...
 - 컴퓨터 그룹 정책
 - 사용권한 제어 , 계정 및 암호정책 , 네트워크 정책 , 소프트웨어 제한 ...
- 소프트웨어 라이센스 관리 일원화
- 개별 운영/관리 되던 전산자원 (PC , PDA ..) 논리적으로 조직화 → 중앙 통합관리

Active Directory Domain Service



Q. hanbit.com AD 환경 구성 하세요.



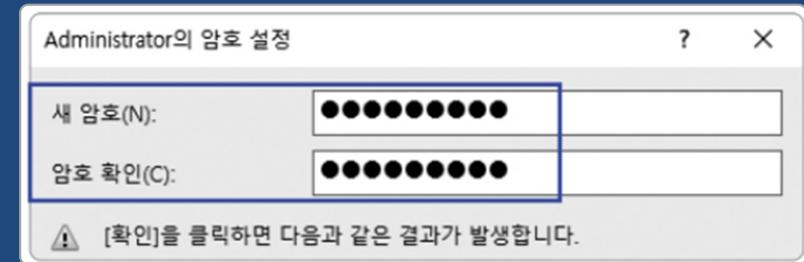
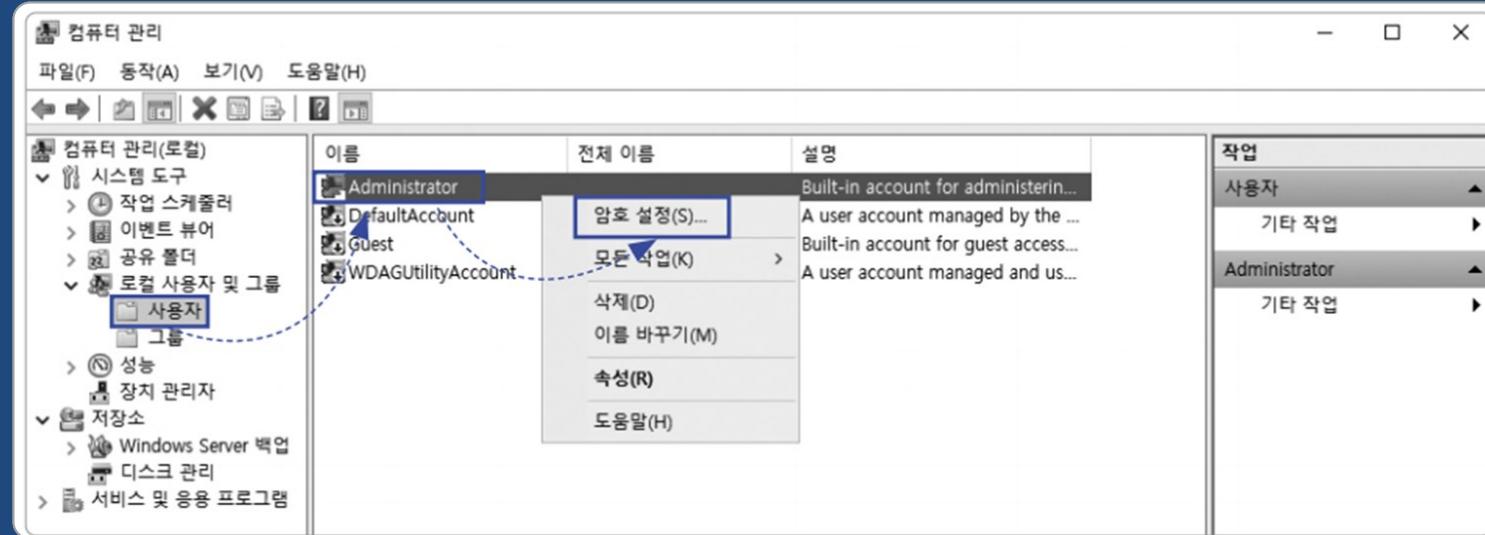
Active Directory Domain Service



Q. hanbit.com AD 환경 구성 하세요. [FIRST , SECOND , THIRD , WINCLIENT]

1) 모든 VM의 로그인 암호 변경 (초기화)

- VMware1! / VMware2! / VMware3! / VMwareC!
- 컴퓨터 관리 → 로컬 사용자 및 그룹 / 사용자 → Administrator (우클릭) → 암호 설정



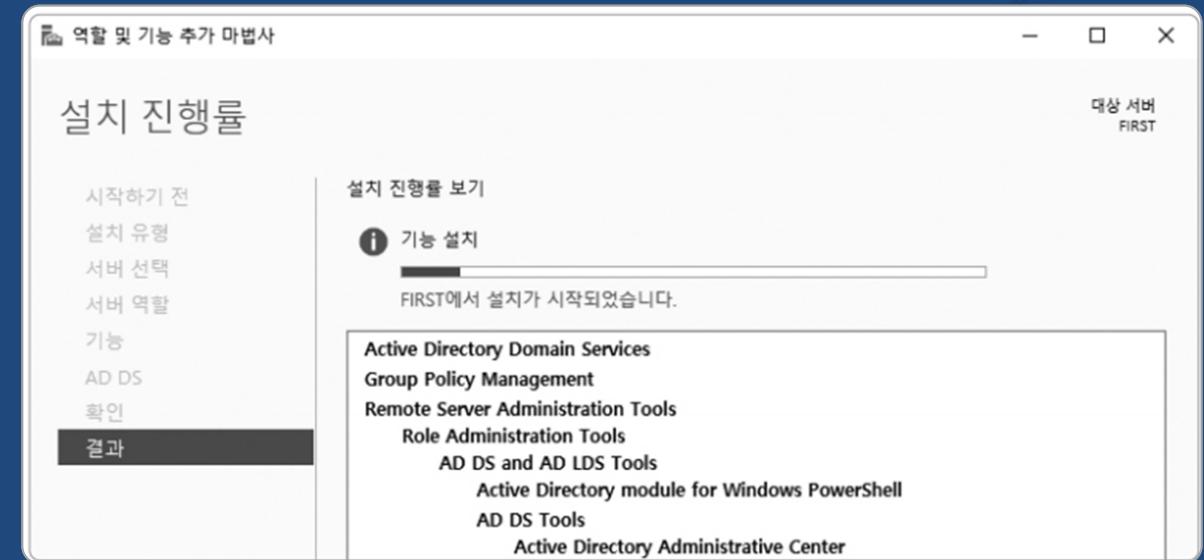
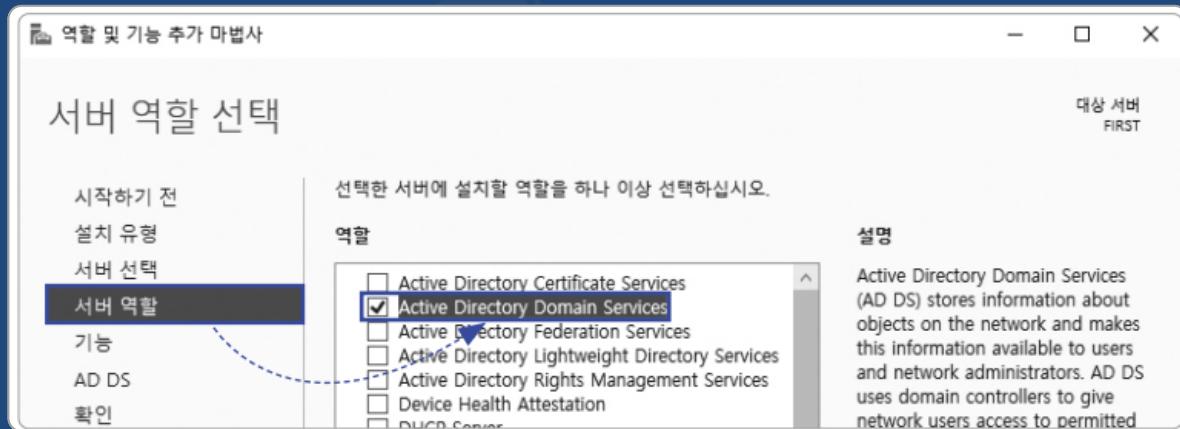
Active Directory Domain Service



Q. hanbit.com AD 환경 구성 하세요. [FIRST]

2) Active Directory Domain Service 설치

- 서버관리자 → 관리 → 역할 및 기능 추가 → 서버 역할 선택 / **Active Directory Domain Service** → 기능 설치



Active Directory Domain Service



Q. hanbit.com AD 환경 구성 하세요. [FIRST]

3) Domain Controller 구성

- 서버관리자 → 알림 → [이 서버를 도메인 컨트롤러로 승격]



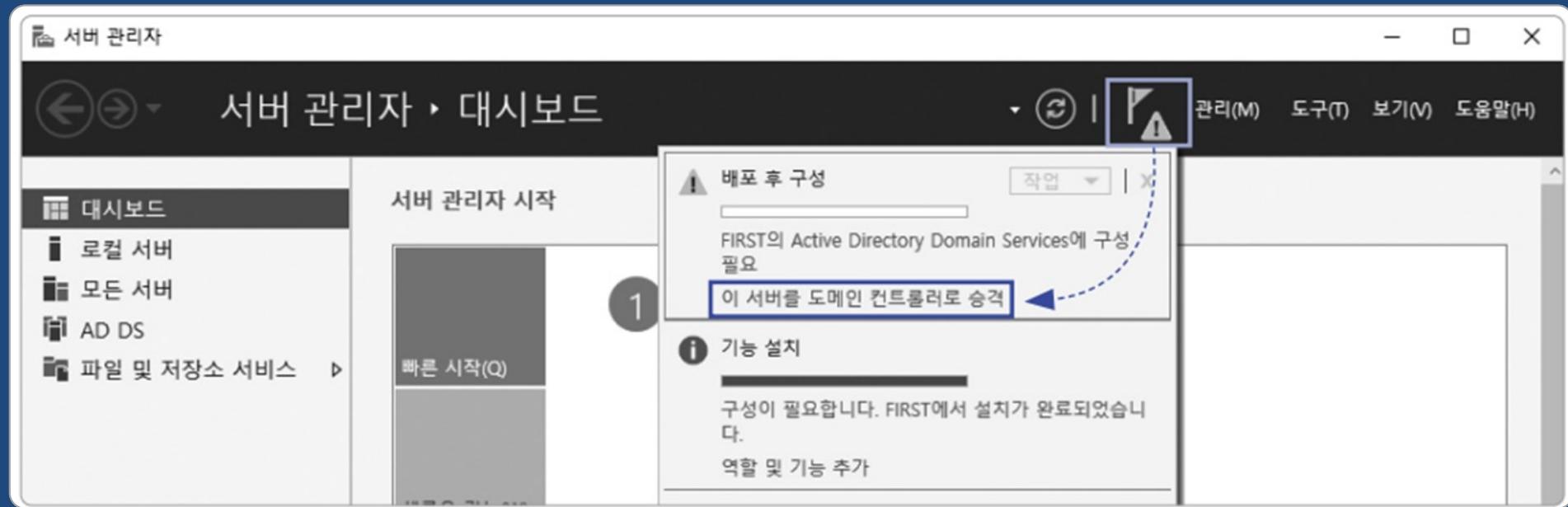
Active Directory Domain Service



Q. hanbit.com AD 환경 구성 하세요. [FIRST]

4-1) hanbit.com 포리스트 구성

- 서버관리자 → 알림 → [이 서버를 도메인 컨트롤러로 승격] → Active Directory 도메인 서비스 구성 마법사



Active Directory Domain Service

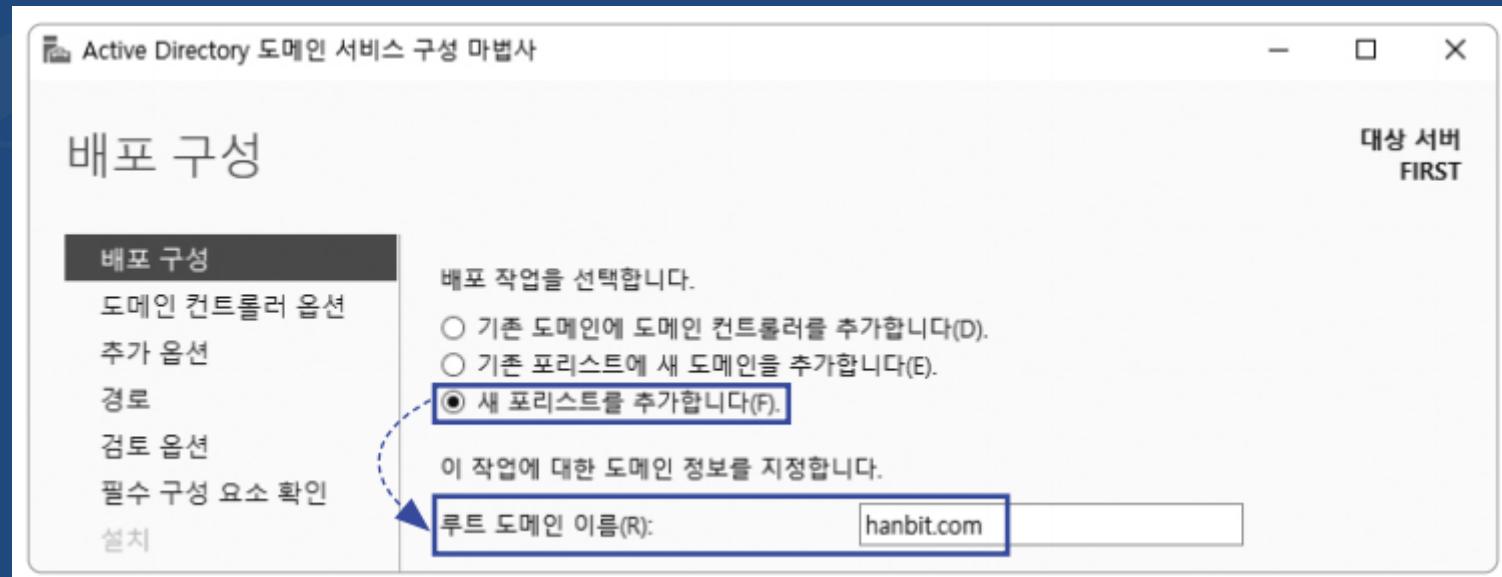


Q. hanbit.com AD 환경 구성 하세요. [FIRST]

4-2) hanbit.com 포리스트 구성

- 배포 구성

- 새 포트리스를 추가합니다.
- 루트 도메인 이름 : hanbit.com



Active Directory Domain Service



Q. hanbit.com AD 환경 구성 하세요. [FIRST]

4-3) hanbit.com 포리스트 구성

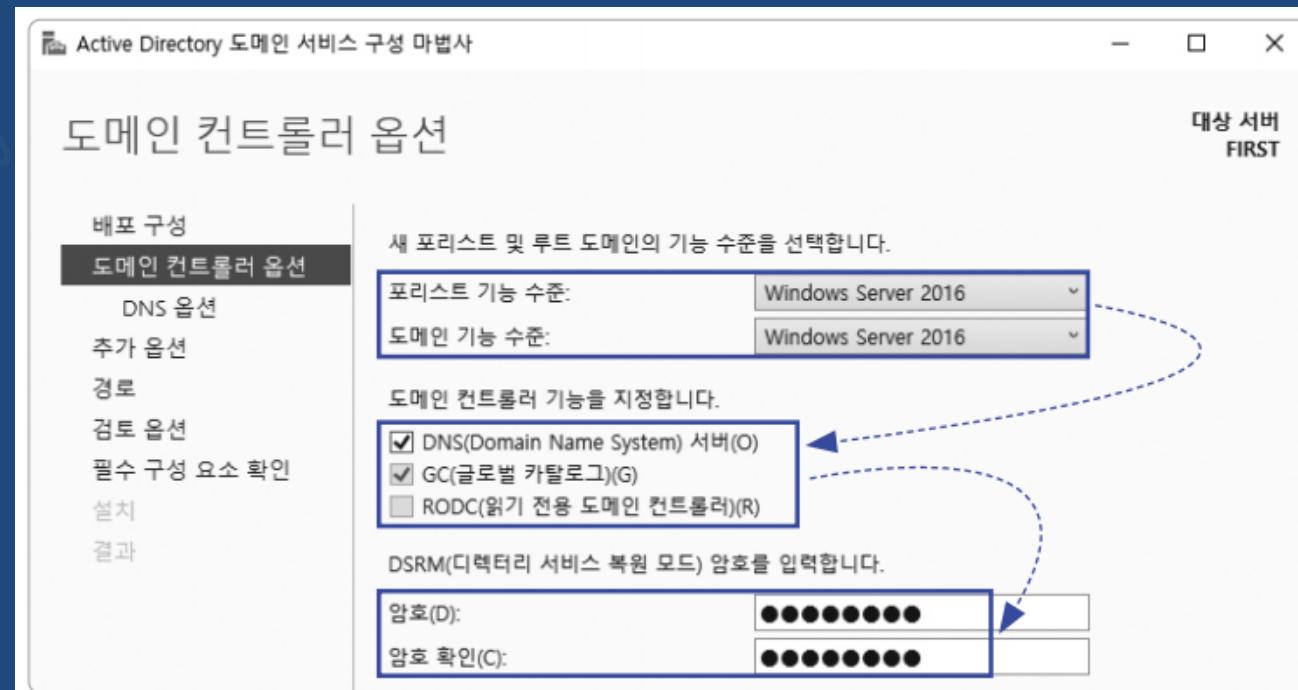
- 도메인 컨트롤러 옵션

- 포트리스 기능 수준 / 도메인 기능 수준 : Windows Server 2016 (최신 AD 기능)
- 도메인 컨트롤러 기능 지정

- ✓ DNS
- ✓ GC

- DSRM 암호

- ✓ VMware!



Active Directory Domain Service

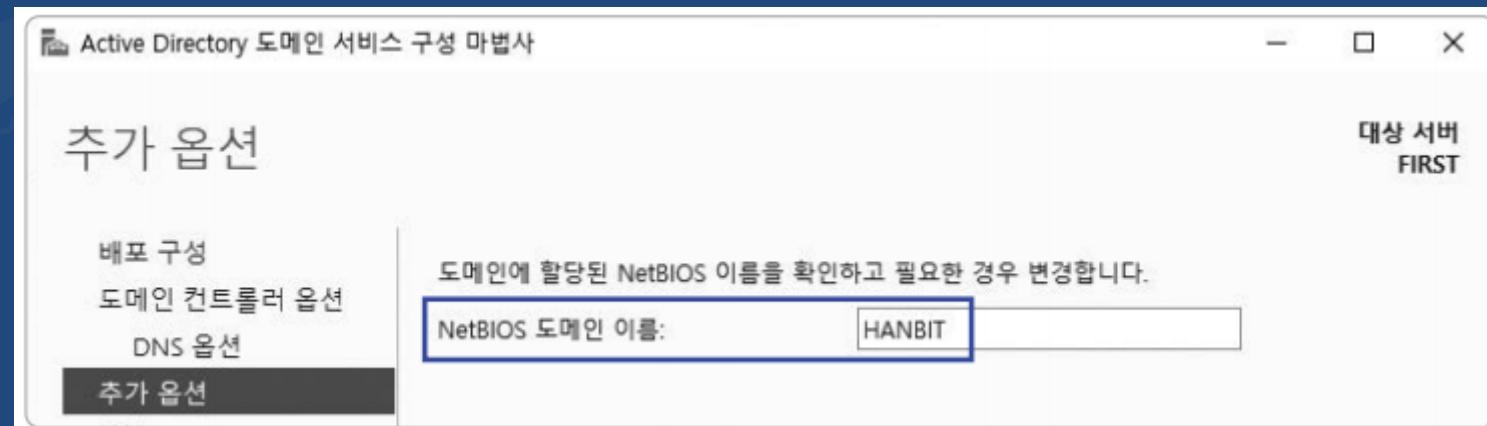


Q. hanbit.com AD 환경 구성 하세요. [FIRST]

4-4) hanbit.com 포리스트 구성

- 추가 옵션

- NetBIOS 도메인 이름 : HANBIT



Active Directory Domain Service

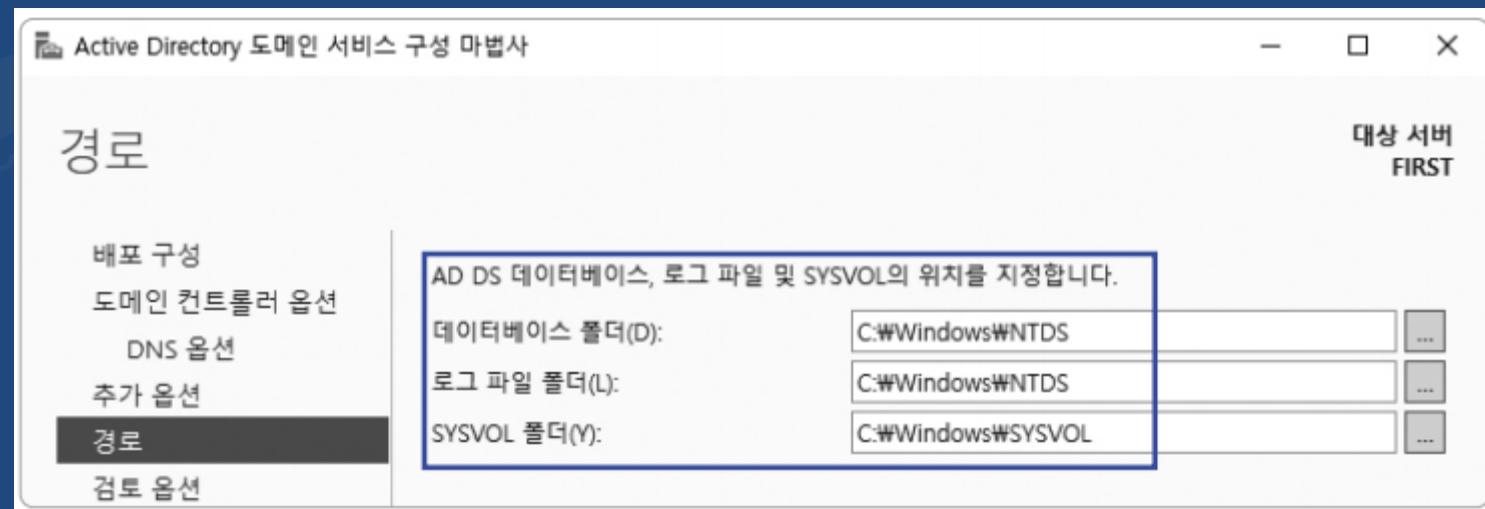


Q. hanbit.com AD 환경 구성 하세요. [FIRST]

4-5) hanbit.com 포리스트 구성

- 경로

- 데이터베이스 , 로그 파일 , SYSVOL 위치 지정 (기본값)



Active Directory Domain Service

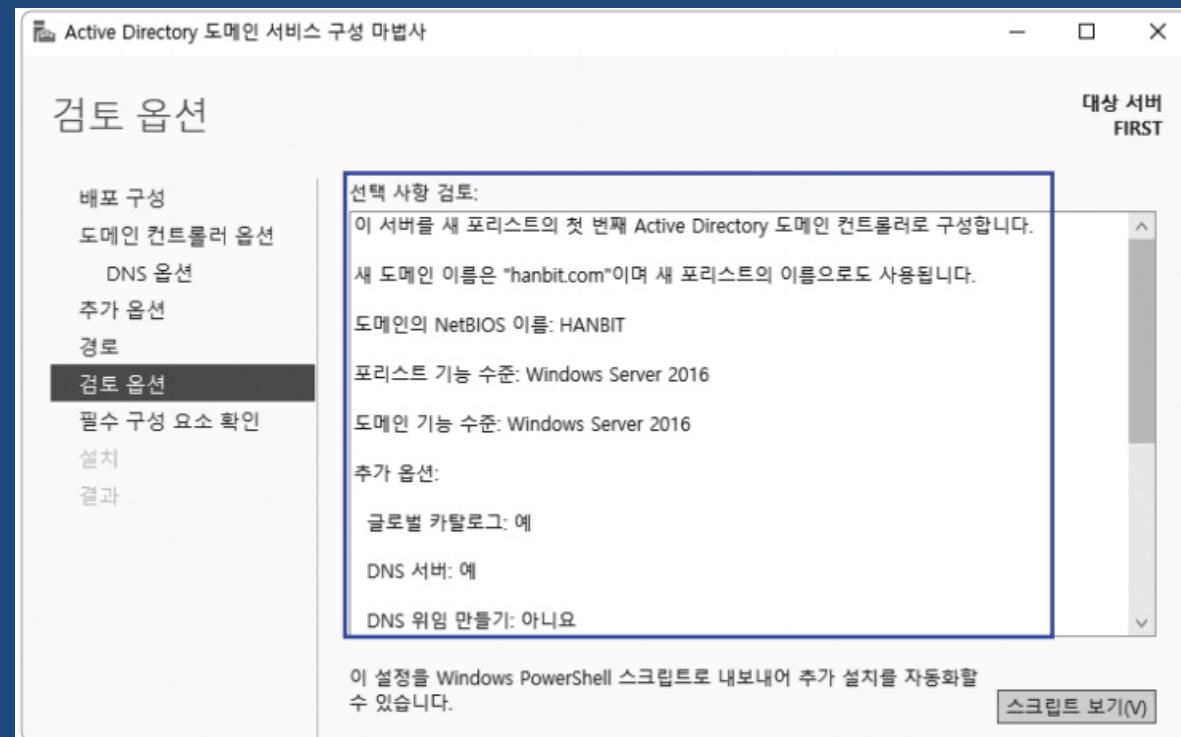


Q. hanbit.com AD 환경 구성 하세요. [FIRST]

4-6) hanbit.com 포리스트 구성

- 검토 옵션

- ## • 앞서 설정한 내용 확인



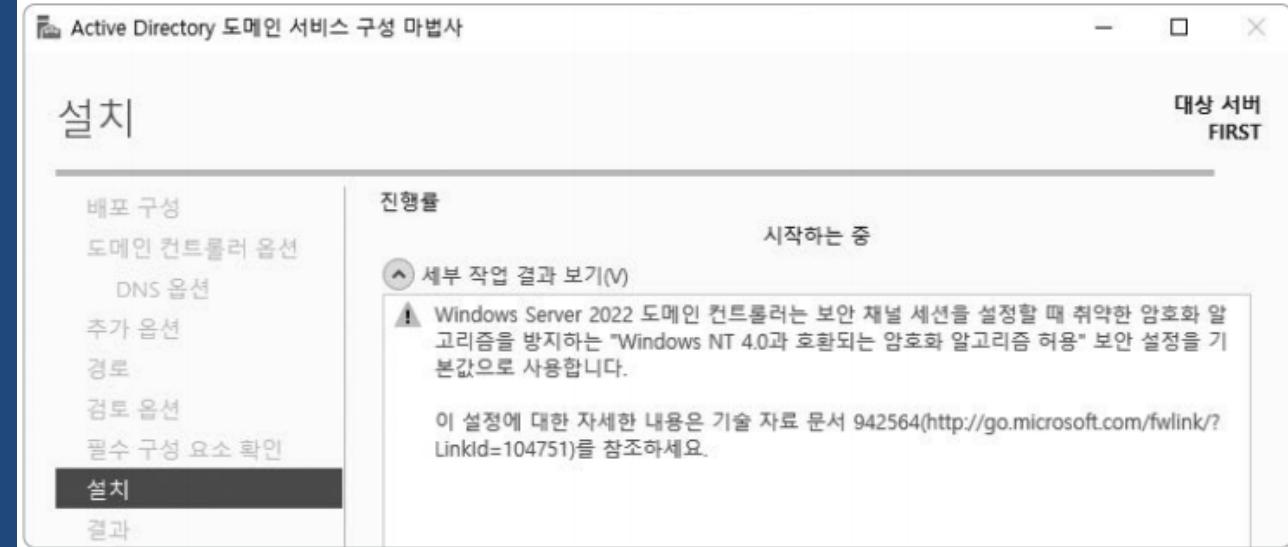
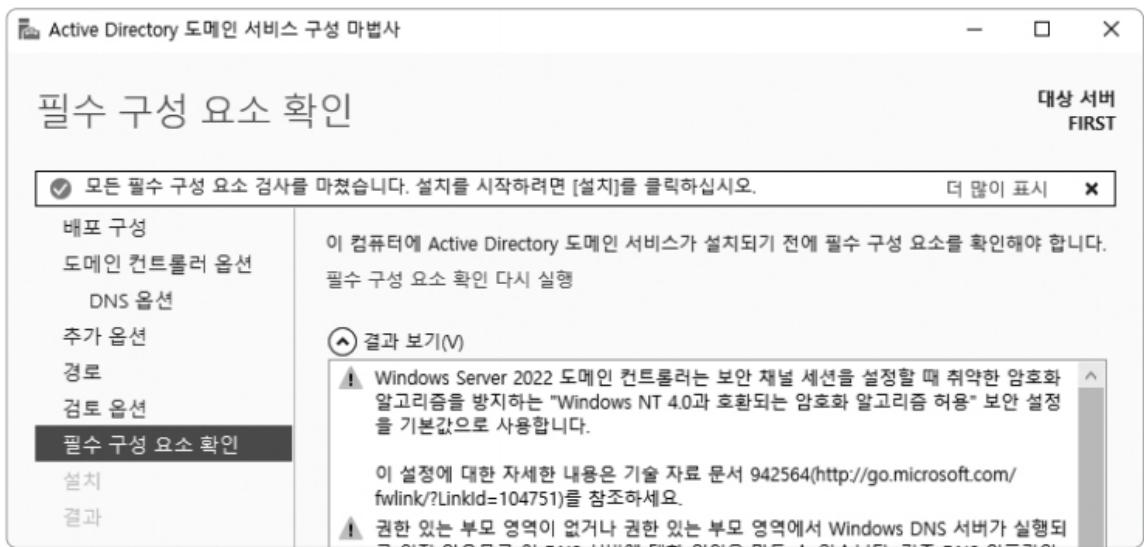
Active Directory Domain Service



Q. hanbit.com AD 환경 구성 하세요. [FIRST]

4-7) hanbit.com 포리스트 구성

- 필수 구성 요소 확인 → 설치 (경고무시)



Active Directory Domain Service



Q. hanbit.com AD 환경 구성 하세요. [FIRST]

5) hanbit.com 포리스트 구성

- 재부팅 후 로그온 화면

- VMware!



* NetBIOS : HANBIT\... [Windows 환경]

* UPN : administrator@... [Windows 및 기타 OS 환경]

Active Directory Domain Service



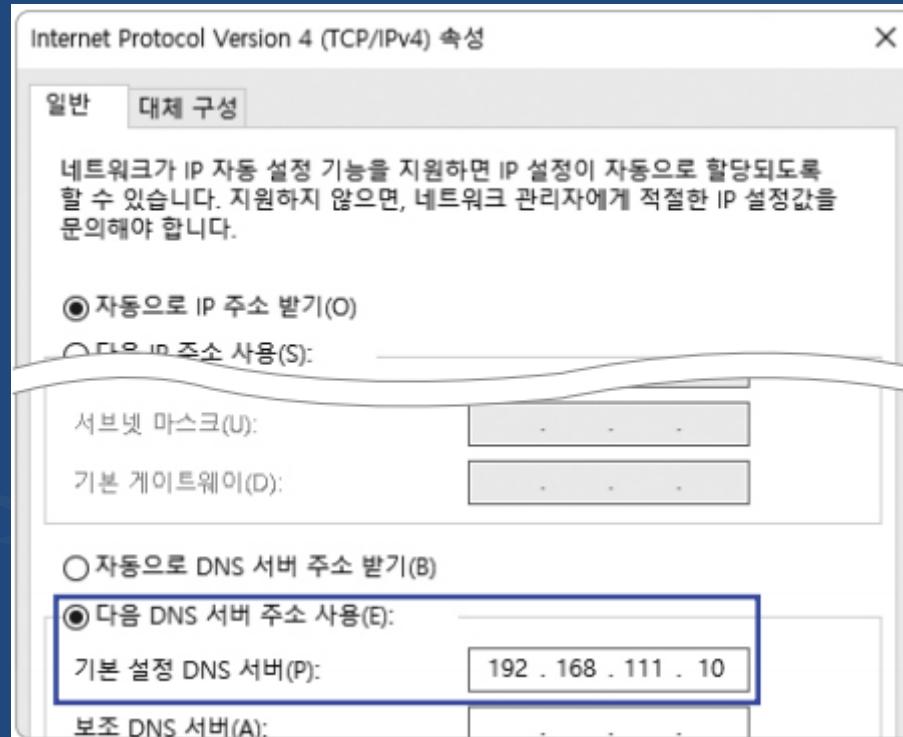
Q. hanbit.com AD 환경 구성 하세요. [WINCLIENT]

* 컴퓨터 이름 변경 → WINCLIENT

1) WINCLIENT의 Domain Join

- DNS 변경

- 192.168.111.10



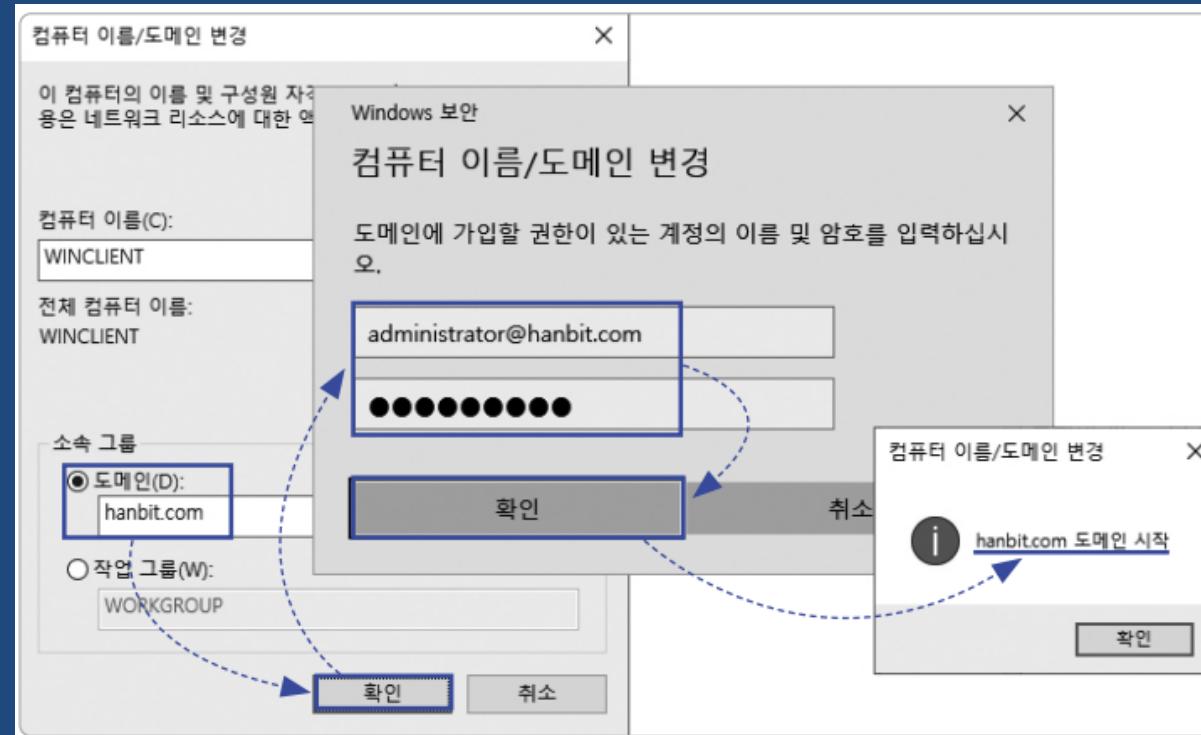
Active Directory Domain Service



Q. hanbit.com AD 환경 구성 하세요. [WINCLIENT]

2) WINCLIENT의 Domain Join

- 시작(우클릭) → 시스템 → 이 PC의 이름 바꾸기 [고급] → 컴퓨터 이름 / 변경 → 소속 그룹 [도메인] → hanbit.com → 가입 권한 계정
- 가입 권한 계정 = 도메인 관리자 계정 (FIRST)
 - administrator@hanbit.com / VMware!



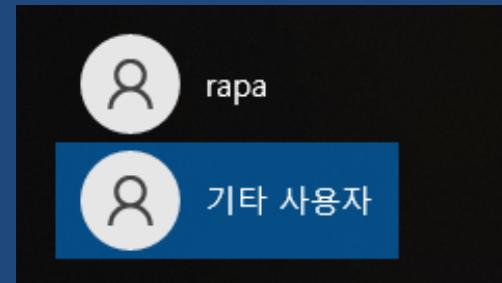
Active Directory Domain Service



Q. hanbit.com AD 환경 구성 하세요. [WINCLIENT]

3) WINCLIENT의 hanbit.com Domain 사용

- 재부팅 → rapa → WINCLIENT PC의 Local 계정 접속
- 로그아웃 → Other user → administrator@hanbit.com 접속
 - WINCLIENT PC 관리자가 아닌 FIRST 관리자(Domain 관리자)가 WINCLIENT PC를 이용해 접속
 - Active Director 도메인에 가입된 컴퓨터라면 어디서든 도메인의 다른 사용자로 접속 가능



Active Directory Domain Service



Q. hanbit.com AD 환경 구성 하세요. [WINCLIENT]

4) WINCLIENT의 도메인 확인

- 시스템 → 정보 → WINCLIENT.hanbit.com

The screenshot shows two windows side-by-side. The left window is the 'System' control panel, and the right window is a 'Properties' dialog box.

System Control Panel (Left):

- Home
- 설정 검색
- 시스템
- 디스플레이
- 소리
- 알림 및 작업
- 집중 지원
- 전원 및 절전
- 저장소

Properties Dialog Box (Right):

제목: 정보
PC가 모니터링되고 보호됩니다.
자세한 내용은 Windows 보안을 참조하세요.

장치 사양

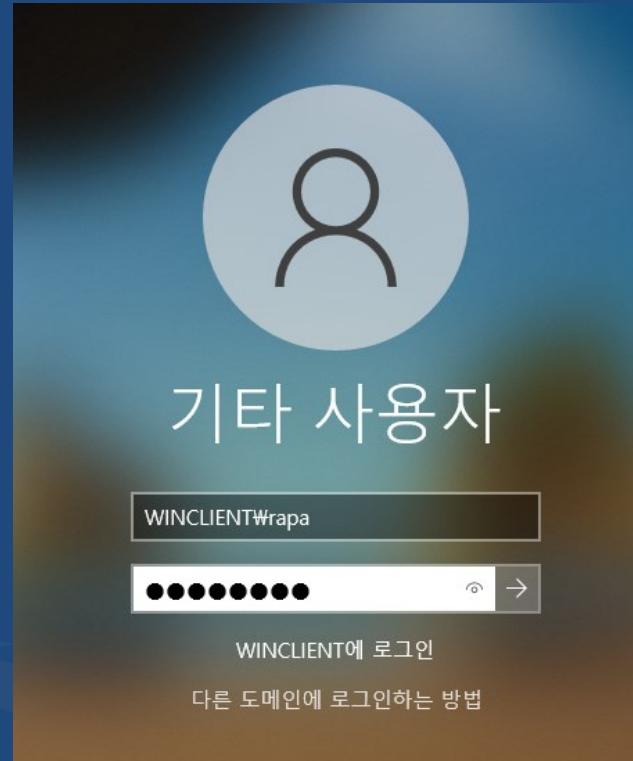
디바이스 이름	WINCLIENT
전체 디바이스 이름	WINCLIENT.hanbit.com
프로세서	AMD Ryzen 7 7800X3D 8-Core Processor 4.19 GHz(2 프로세서)
설치된 RAM	2.00GB
장치 ID	2638C18D-0E76-42C8-B2E1-F61C853DB0CC
제품 ID	00329-20000-00001-AA945
시스템 종류	64비트 운영 체제, x64 기반 프로세서
펜 및 터치	이 디스플레이에 사용할 수 있는 펜 또는 터치식 입력이 없습니다.

Active Directory Domain Service



Q. hanbit.com AD 환경 구성 하세요. [WINCLIENT]

- 5) WINCLIENT의 Local 계정 접속
 - WINCLIENT\rapa / VMwareC!



* 도메인에 가입된 PC는 언제든 도메인의 다른 사용자로 접속 및 기존 로컬 사용자 접속 가능

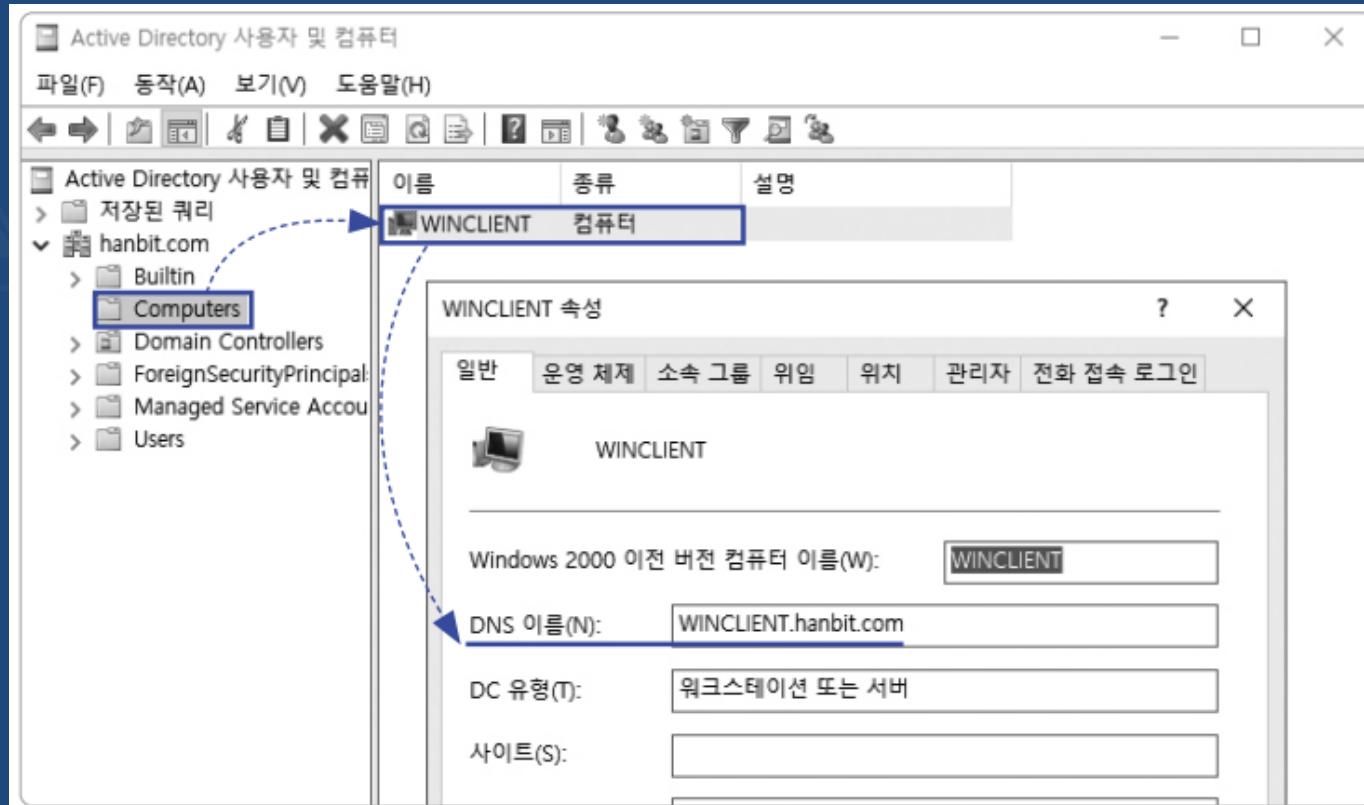
Active Directory Domain Service



Q. hanbit.com AD 환경 확인 하세요. [FIRST]

1) Domain 소속 컴퓨터 확인

– 서버 관리자 → 도구 → Active Directory 사용자 및 컴퓨터 → hanbit.com / Computers

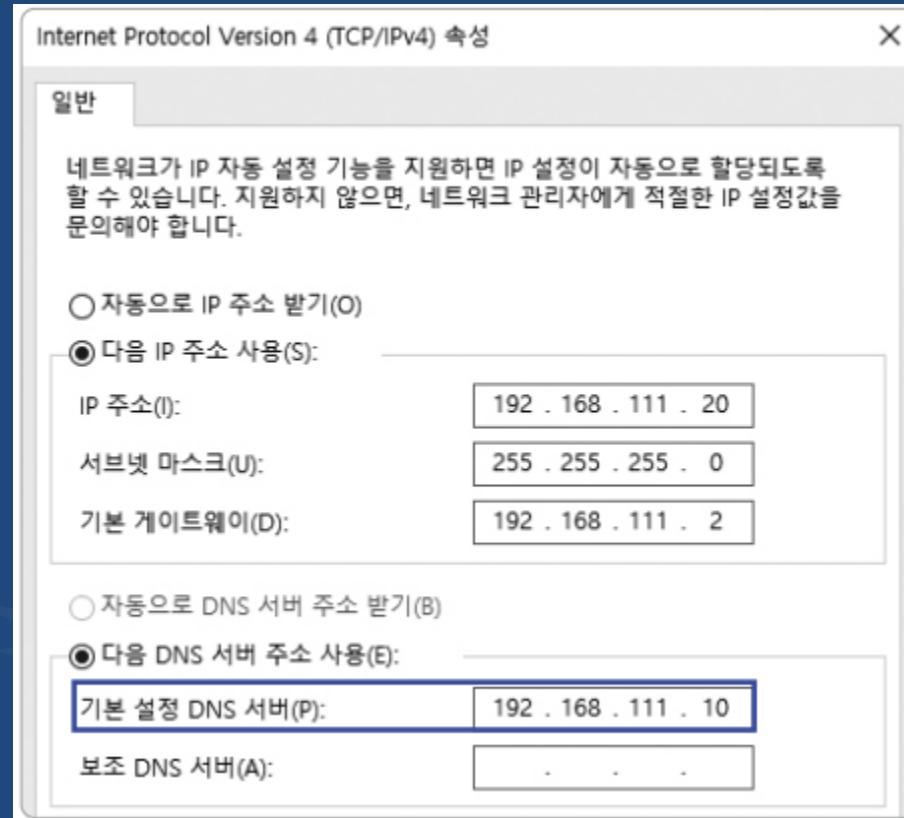


Active Directory Domain Service



Q. second.hanbit.com AD 환경 구성 하세요. [SECOND]

1) SECOND 서버의 DNS를 FIRST로 변경



Active Directory Domain Service



Q. second.hanbit.com AD 환경 구성 하세요. [SECOND]

2) Active Directory Domain Service 설치

– 서버관리자 → 관리 → 역할 및 기능 추가 → 서버 역할 선택 / Active Directory Domain Service → 기능 설치

3) Domain Controller 구성

– 서버관리자 → 알림 → [이 서버를 도메인 컨트롤러로 승격]

4-1) 자식 도메인 구성

– 서버관리자 → 알림 → [이 서버를 도메인 컨트롤러로 승격] → Active Directory 도메인 서비스 구성 마법사

Active Directory Domain Service

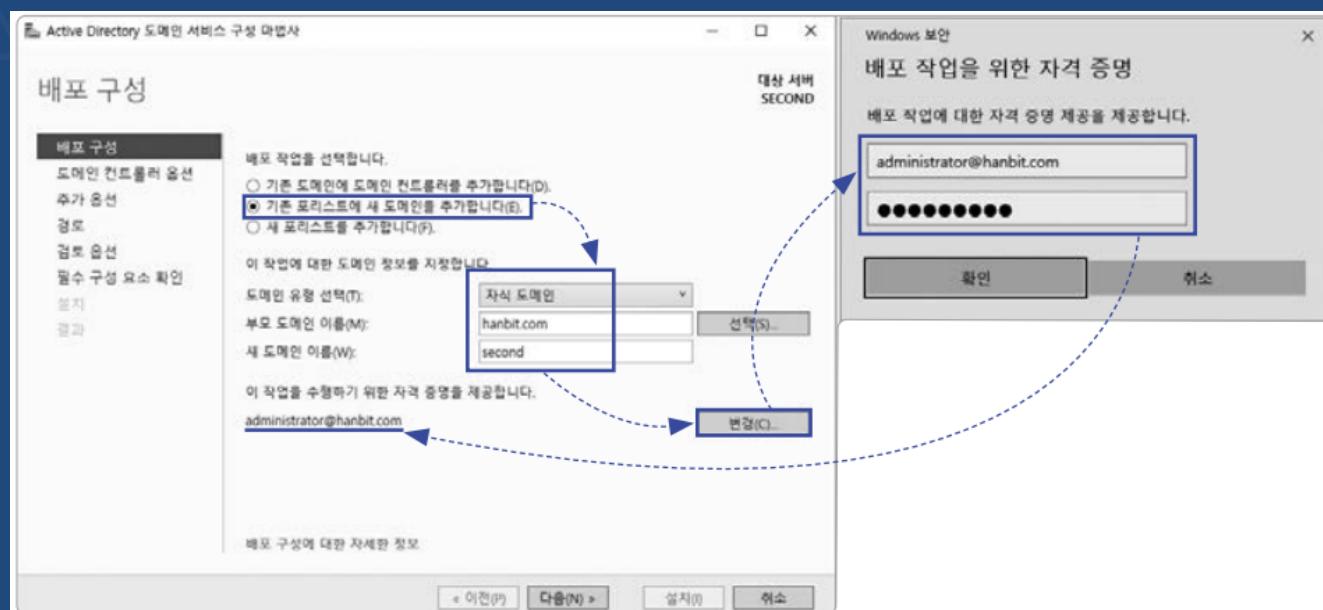


Q. second.hanbit.com AD 환경 구성 하세요. [SECOND]

4-2) 자식 도메인 구성

- 배포 구성

- 기존 포리스트에 새 도메인을 추가합니다
- 도메인 유형 선택 : 자식 도메인
- 부모 도메인 이름 : hanbit.com
- 새 도메인 이름 : second
- 배포 작업 자격 증명 : 도메인 관리자의 사용자명과 암호 (administrator@hanbit.com / VMware1!)



Active Directory Domain Service

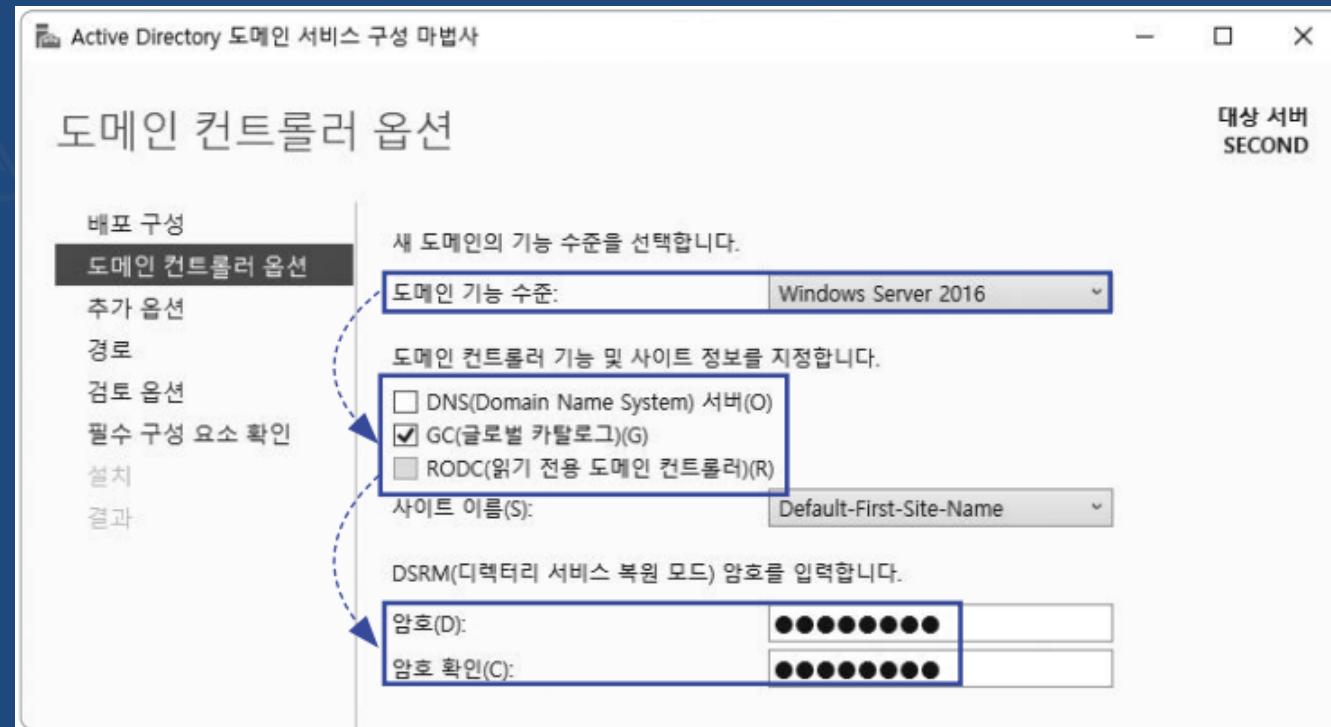


Q. second.hanbit.com AD 환경 구성 하세요. [SECOND]

4-3) 자식 도메인 구성

- 도메인 컨트롤러 옵션

- 도메인 기능 수준 : Windows Server 2016
- 도메인 컨트롤러 기능 및 사이트 정보를 지정
 - ✓ GC
- DSRM 암호
- ✓ VMware!



Active Directory Domain Service

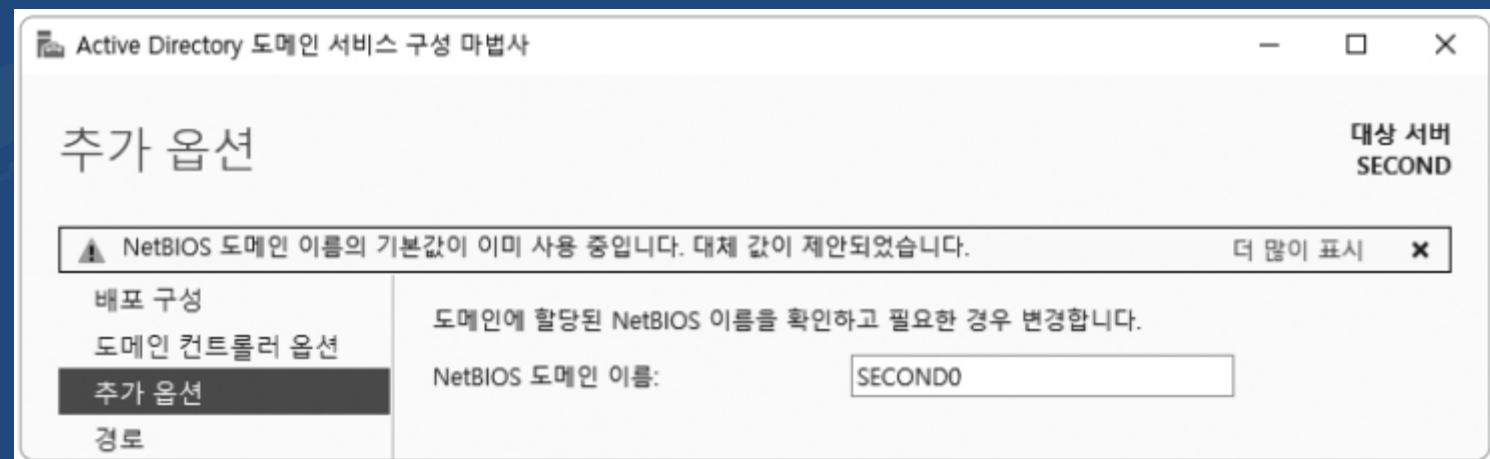


Q. second.hanbit.com AD 환경 구성 하세요. [SECOND]

4-4) 자식 도메인 구성

- 추가 옵션

- NetBIOS 도메인 이름 : SECOND0



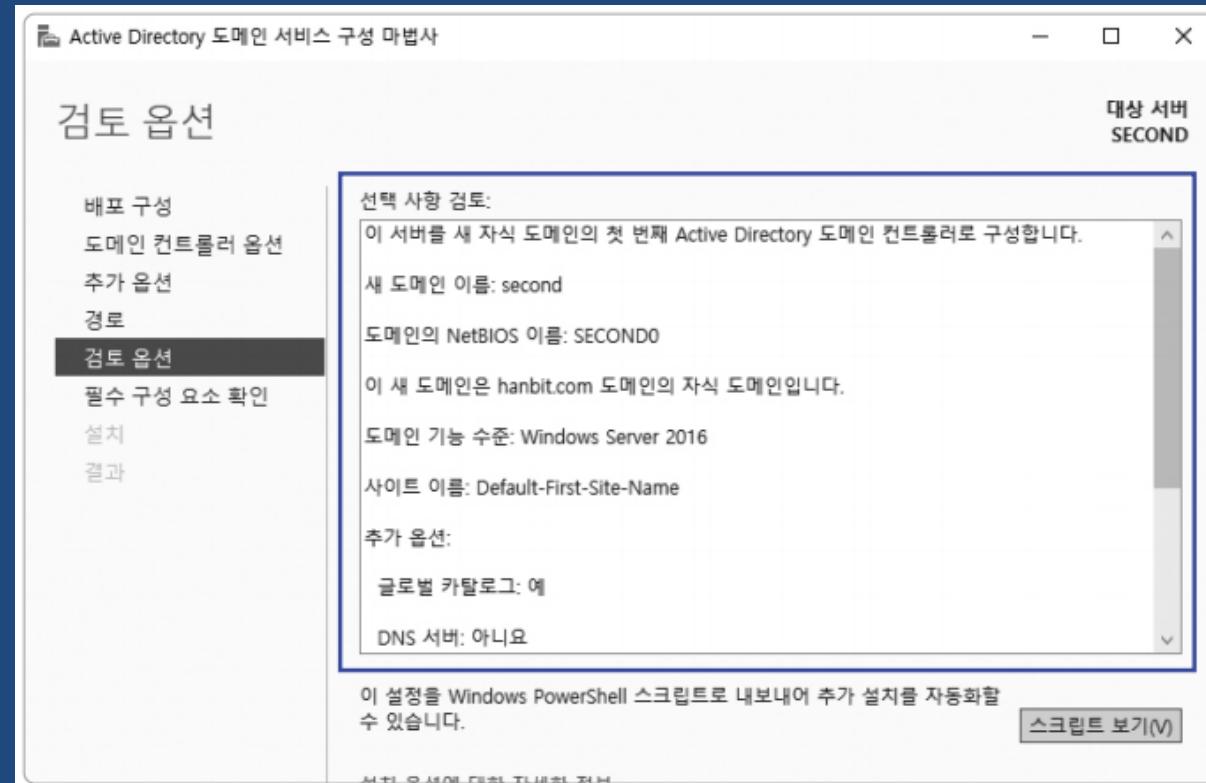
Active Directory Domain Service



Q. second.hanbit.com AD 환경 구성 하세요. [SECOND]

4-5) 자식 도메인 구성

- 경로 → 기본값
- 검토 옵션 → 내용 확인
- 설치 (경고 무시)



Active Directory Domain Service



Q. second.hanbit.com AD 환경 구성 하세요. [SECOND]

5) 자식 도메인 구성

- 재부팅 → Other user → UPN 접속



* NetBIOS : HANBITW... [Windows 환경]

* UPN : administrator@... [Windows 및 기타 OS 환경]

Active Directory Domain Service



Q. second.hanbit.com AD 환경 확인 하세요. [SECOND]

1) 부모 도메인, 자식 도메인 확인

– 서버 관리자 → 도구 → Active Directory 도메인 및 트러스트 → hanbit.com / second.hanbit.com



Active Directory Domain Service



Q. RODC AD 환경 구성 하세요. [THIRD]

1) THIRD 서버의 DNS를 FIRST로 변경

2) Active Directory Domain Service 설치

– 서버관리자 → 관리 → 역할 및 기능 추가 → 서버 역할 선택 / **Active Directory Domain Service** → 기능 설치

3) Domain Controller 구성

– 서버관리자 → 알림 → [이 서버를 도메인 컨트롤러로 승격]

4-1) RODC 구성

– 서버관리자 → 알림 → [이 서버를 도메인 컨트롤러로 승격] → Active Directory 도메인 서비스 구성 마법사

Active Directory Domain Service

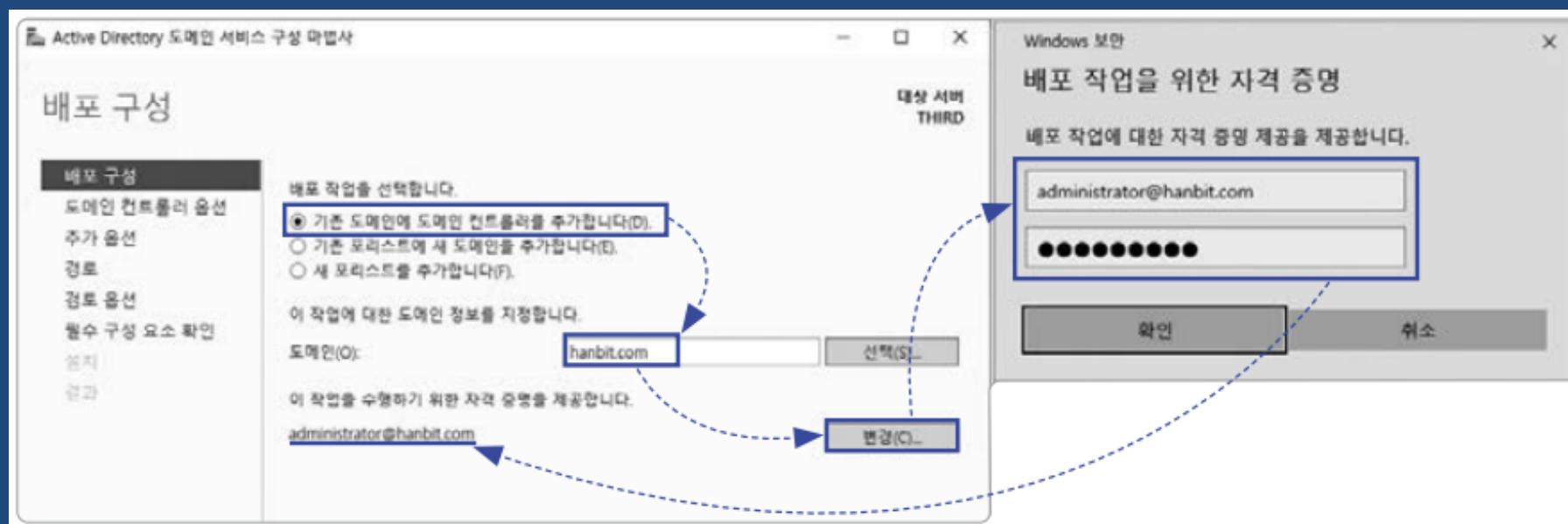


Q. RODC AD 환경 구성 하세요. [THIRD]

4-2) RODC 구성

- 배포 구성

- 기존 도메인에 도메인 컨트롤러를 추가합니다
- 도메인 : hnabit.com



Active Directory Domain Service

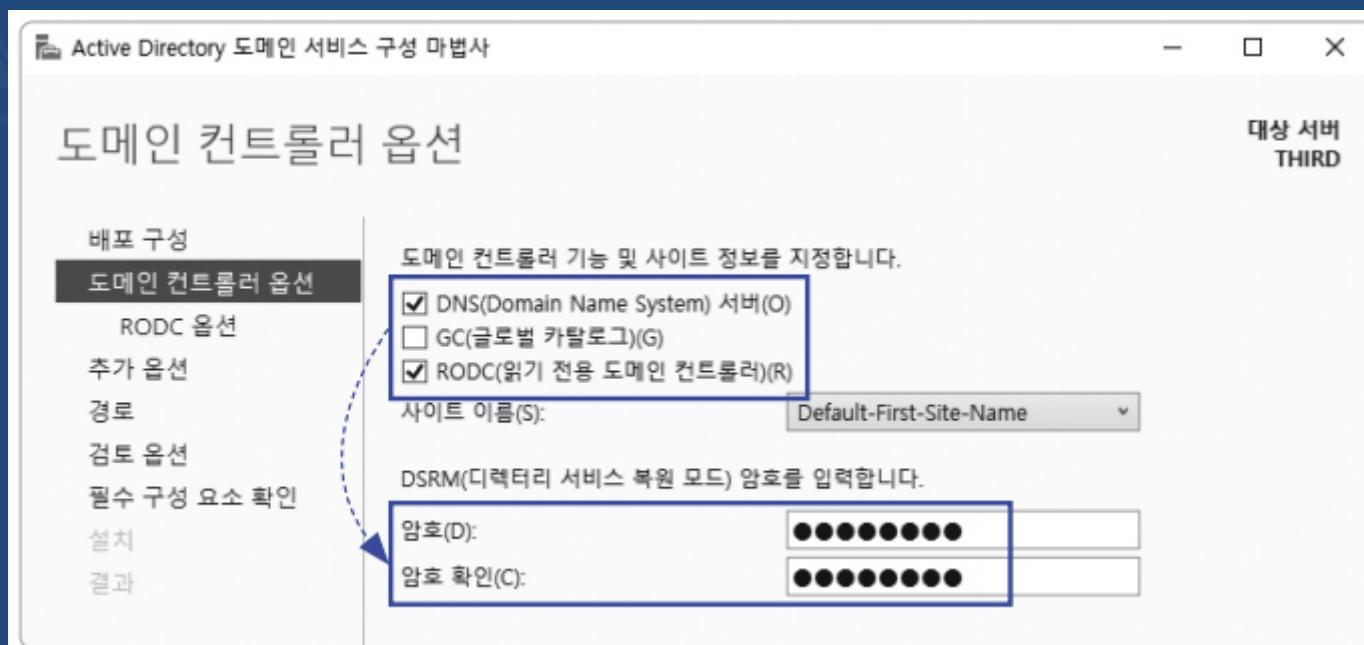


Q. RODC AD 환경 구성 하세요. [THIRD]

4-3) RODC 구성

- 도메인 컨트롤러 옵션

- 도메인 기능 수준 : Windows Server 2016
- 도메인 컨트롤러 기능 및 사이트 정보를 지정
 - ✓ DNS 서버
 - ✓ RODC
- DSRM 암호
 - ✓ VMware!



Active Directory Domain Service

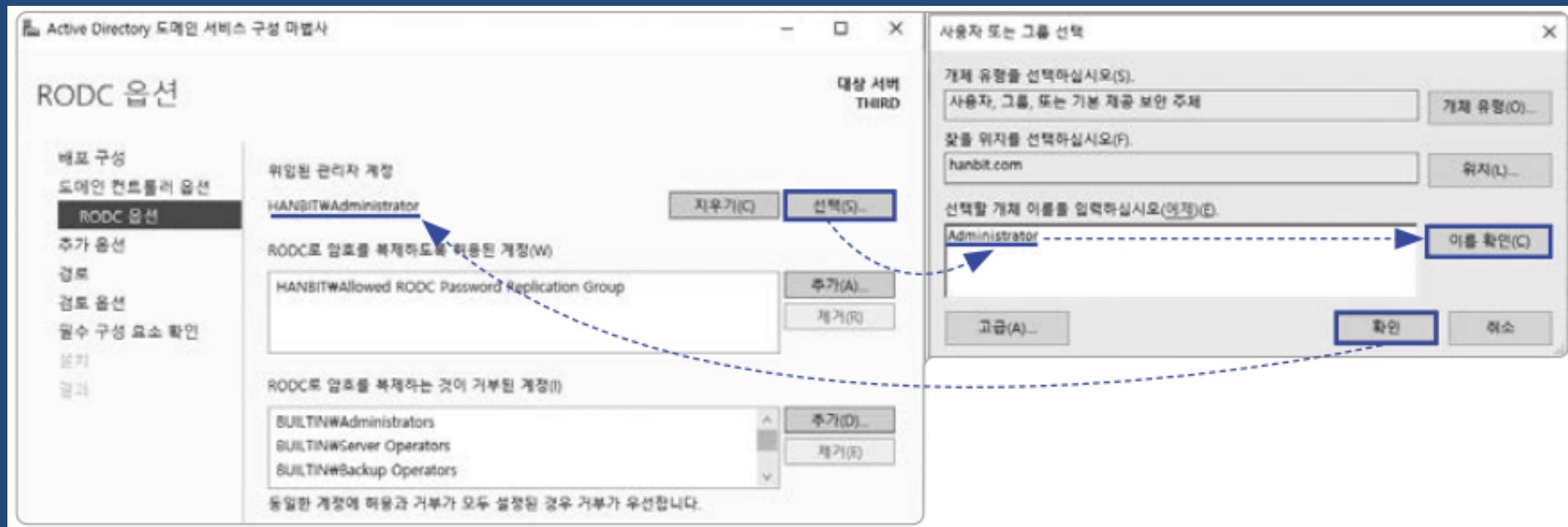


Q. RODC AD 환경 구성 하세요. [THIRD]

4-4) RODC 구성

- RODC 옵션

- 위임된 관리자 계정 : 선택 → Administrator → 이름 확인 → Administrator 선택 → HANBIT\Administrator



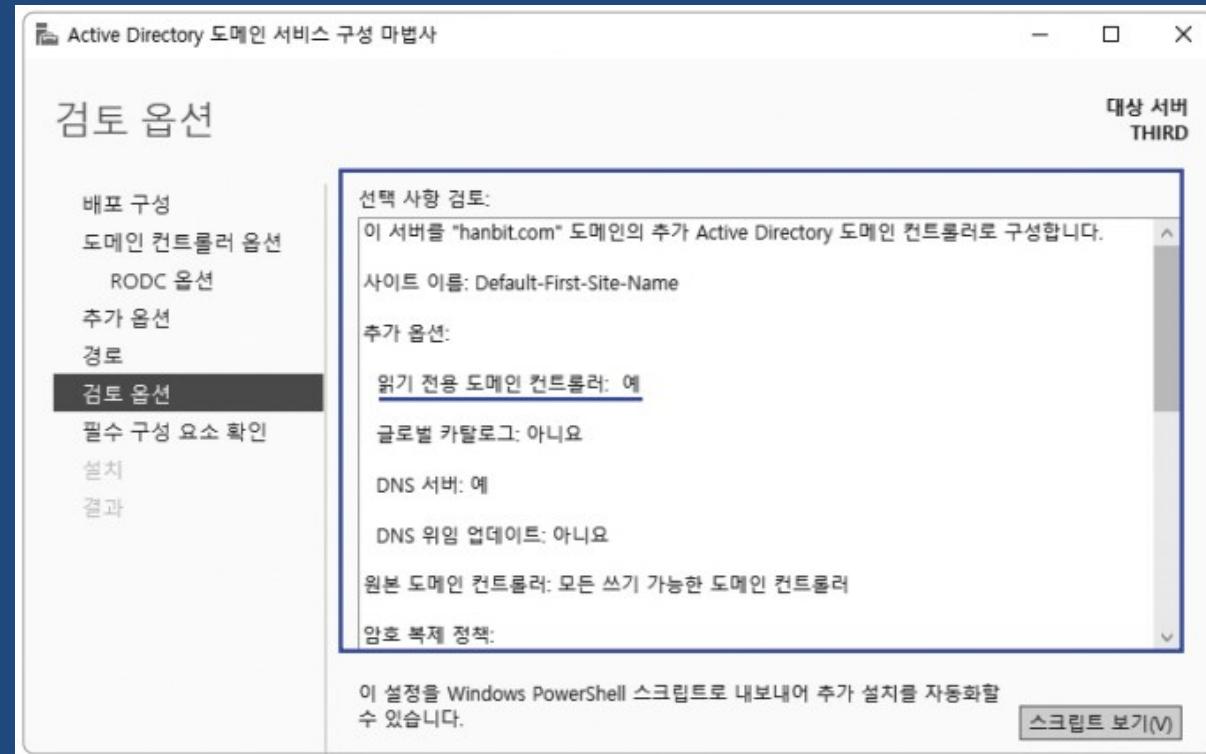
Active Directory Domain Service



Q. RODC AD 환경 구성 하세요. [THIRD]

4-5) RODC 구성

- 경로 → 기본값
- 검토 옵션 → 내용 확인
- 설치 (경고 무시)



Active Directory Domain Service



Q. RODC AD 환경 구성 하세요. [THIRD]

5) RODC 구성

- 재부팅 → Other user → 도메인 관리자 UPN 접속



* NetBIOS : HANBITW... [Windows 환경]

* UPN : administrator@... [Windows 및 기타 OS 환경]

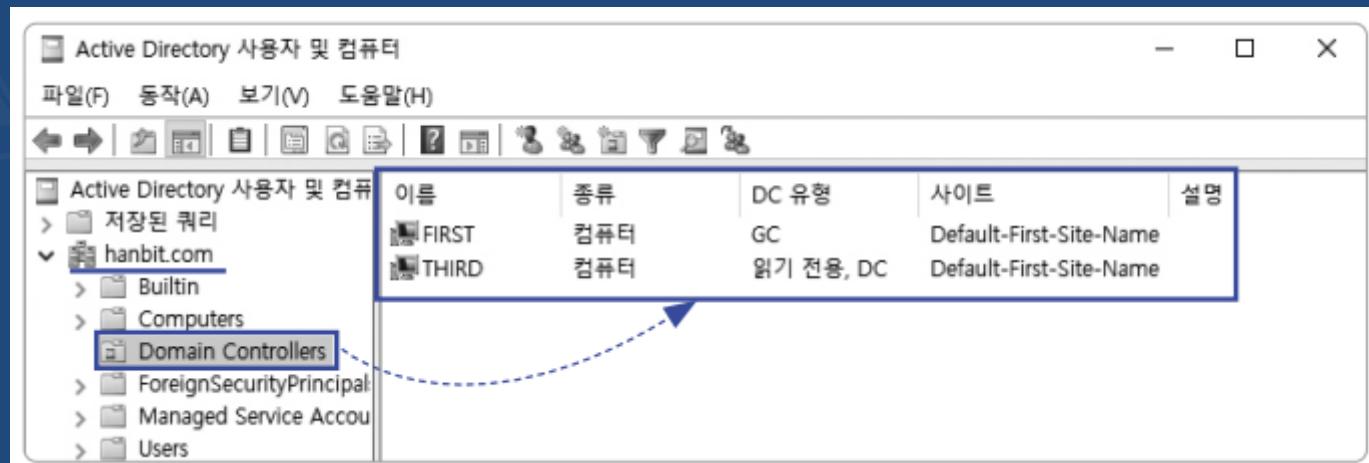
Active Directory Domain Service



Q. RODC AD 환경 확인 하세요. [THIRD]

1) 도메인 컨트롤러 확인

- 시작 → Settings → Windows Settings → Time & Language → Language / Windows display language → 한국어
- 서버 관리자 → 도구 → Active Directory 사용자 및 컴퓨터 → hanbit.com / Domain Controller



Active Directory Domain Service



Q. 서버 관리자를 사용해 서울에서 부산, 뉴욕의 AD 도메인 컨트롤러 통합 관리 되도록 설정 하세요.



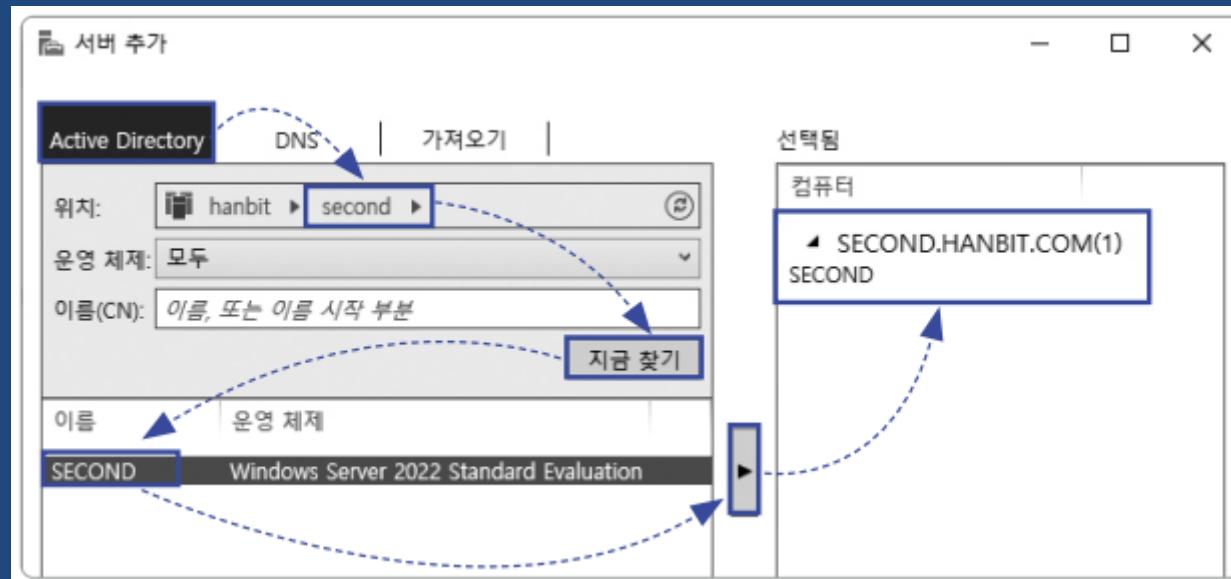
Active Directory Domain Service



Q. 다른 도메인 컨트롤러 등록해 관리 하세요. [FIRST]

1) 서울 본사에 부산 지사 AD 도메인 컨트롤러 추가

- 서버 관리자 → 관리 → 서버 추가 → 서버 추가 / Active Directory → 위치 : hanbit ▶ second → 지금 찾기
→ 이름 / SECOND → ►



Active Directory Domain Service



Q. 다른 도메인 컨트롤러 등록해 관리 하세요. [FIRST]

2) 서울 본사 서버에 부산 지사 AD 도메인 컨트롤러 추가 확인

- 서버 관리자 → 모든 서버

The screenshot shows the Windows Server Manager interface. The left navigation pane is titled '서버 관리자' and lists several service icons: 대시보드, 로컬 서버, 모든 서버 (which is selected and highlighted in blue), AD DS, DNS, and 파일 및 저장소 서비스. The main pane is titled '서버' and shows a list of two servers: 'FIRST' and 'SECOND'. The table columns are '서버 이름', 'IPv4 주소', '관리 효율성', '마지막 업데이트', and 'Windows 정품 인증'. The 'FIRST' server is listed with the IP 192.168.111.10, status '온라인 - 성능 카운터가 시작되지 않았습니다.', last updated on 2022-03-26 at 11:45:39, and Windows Product Activation code 00455-50000-00001-AA483. The 'SECOND' server is listed with the IP 192.168.111.20, status '온라인 - 성능 카운터가 시작되지 않았습니다.', last updated on 2022-03-26 at 11:47:43, and Windows Product Activation code 00454-40000-00001-AA089.

서버 이름	IPv4 주소	관리 효율성	마지막 업데이트	Windows 정품 인증
FIRST	192.168.111.10	온라인 - 성능 카운터가 시작되지 않았습니다.	2022-03-26 오전 11:45:39	00455-50000-00001-AA483
SECOND	192.168.111.20	온라인 - 성능 카운터가 시작되지 않았습니다.	2022-03-26 오전 11:47:43	00454-40000-00001-AA089

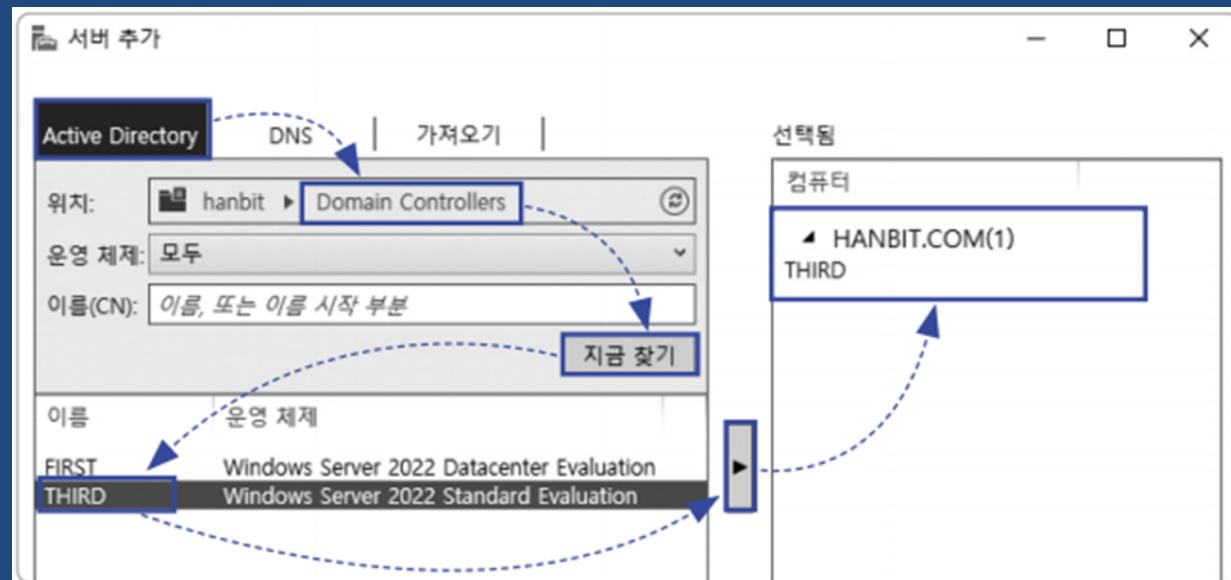
Active Directory Domain Service



Q. 다른 도메인 컨트롤러 등록해 관리 하세요. [FIRST]

3) 서울 본사 서버에 뉴욕 지사 AD 도메인 컨트롤러 추가

- 서버 관리자 → 관리 → 서버 추가 → 서버 추가 / Active Directory → 위치 : hanbit ► Domain Controller → 지금 찾기 → 이름 / THIRD ► ►



Active Directory Domain Service



Q. 다른 도메인 컨트롤러 등록해 관리 하세요. [FIRST]

4) 서울 본사 서버에 뉴욕 지사 AD 도메인 컨트롤러 추가 확인

- 서버 관리자 → 모든 서버

The screenshot shows the Windows Server Manager interface. On the left, the navigation pane is visible with options like '대시보드', '로컬 서버', '모든 서버' (which is selected and highlighted in blue), 'AD DS', 'DNS', and '파일 및 저장소 서비스'. A dashed arrow points from the '모든 서버' option to the main content area. The main area displays a table titled '서버' with three entries: FIRST, SECOND, and THIRD. The columns include '서버 이름', 'IPv4 주소', '관리 효율성', '마지막 업데이트', and 'Windows 정품 인증'. The 'FIRST' entry is highlighted.

서버 이름	IPv4 주소	관리 효율성	마지막 업데이트	Windows 정품 인증
FIRST	192.168.111.10	온라인 - 성능 카운터가 시작되지 않았습니다.	2022-03-26 오전 11:55:39	00455-50000-00001-AA483(
SECOND	192.168.111.20	온라인 - 성능 카운터가 시작되지 않았습니다.	2022-03-26 오전 11:55:36	00454-40000-00001-AA089(
THIRD	192.168.111.30	온라인 - 성능 카운터가 시작되지 않았습니다.	2022-03-26 오후 12:01:30	00454-40000-00001-AA232(

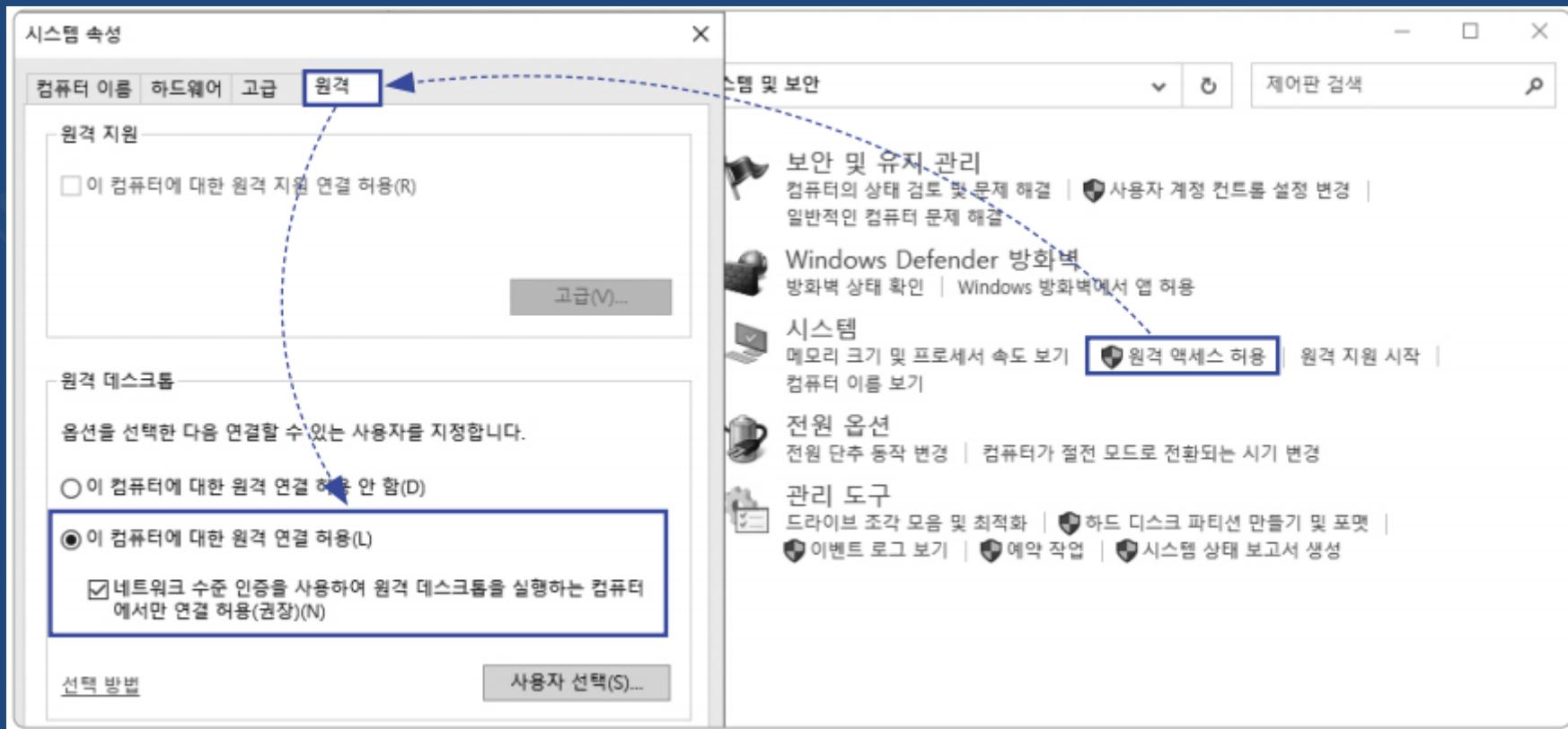
Active Directory Domain Service



Q. 외부에서 SECOND 서버 관리 가능하도록 설정 하세요. [SECOND]

1-1) 외부에서 RDP 접속 가능하도록 설정

- 관리자 계정 접속 (administrator@second.hanbit.com) → 제어판 → 시스템 및 보안 → 시스템 / 원격 액세스 허용
→ 시스템 속성 / 원격 / 이 컴퓨터에 대한 원격 연결 허용



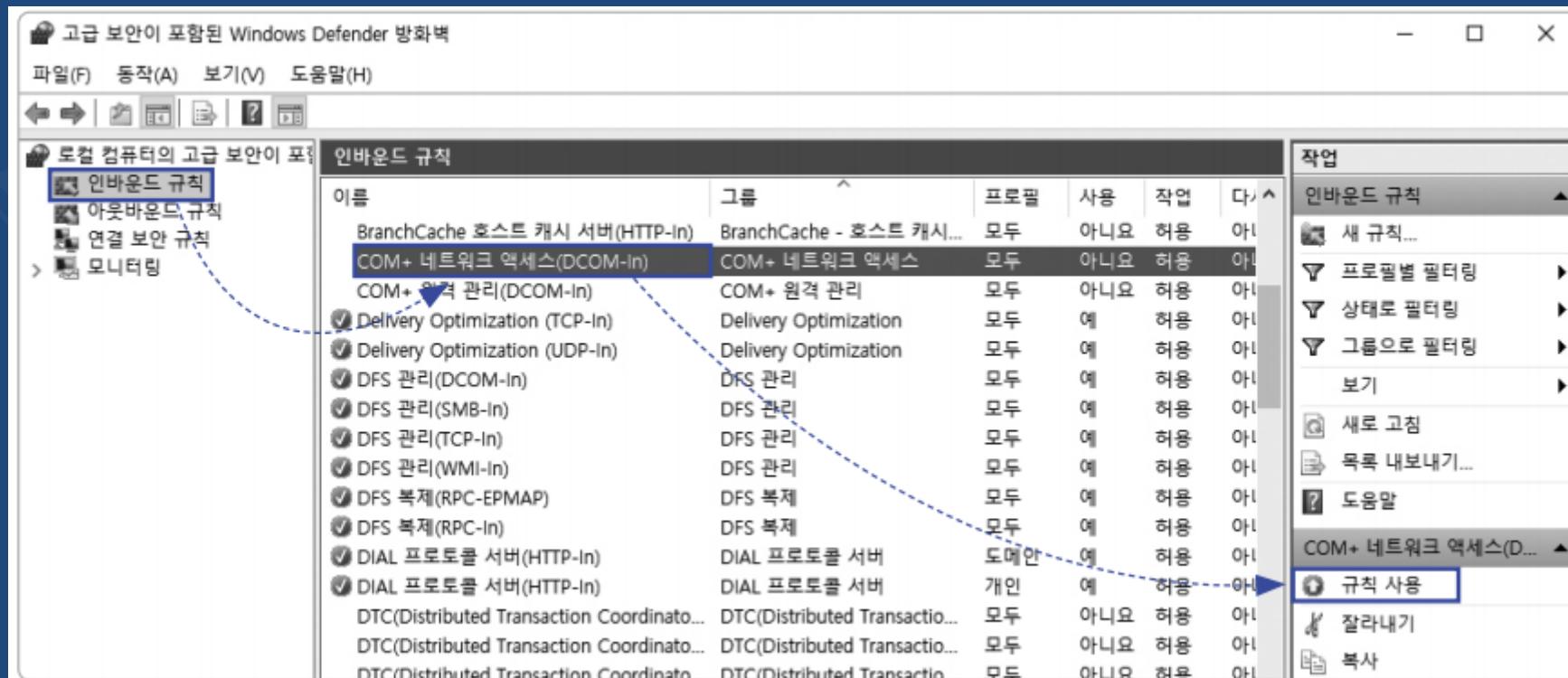
Active Directory Domain Service



Q. 외부에서 SECOND 서버 관리 가능하도록 설정 하세요. [SECOND]

1-2) 외부에서 RDP 접속 가능하도록 설정

- 서버 관리자 → 로컬 서버 → Microsoft Defender 방화벽 / 도메인, 개인, 공개 → 프로그램 설정 / 방화벽 설정:네트워크 보호 설정 → 인바운드 규칙 → COM+ 네트워크 액세스 (DCOM-In) → 규칙 사용



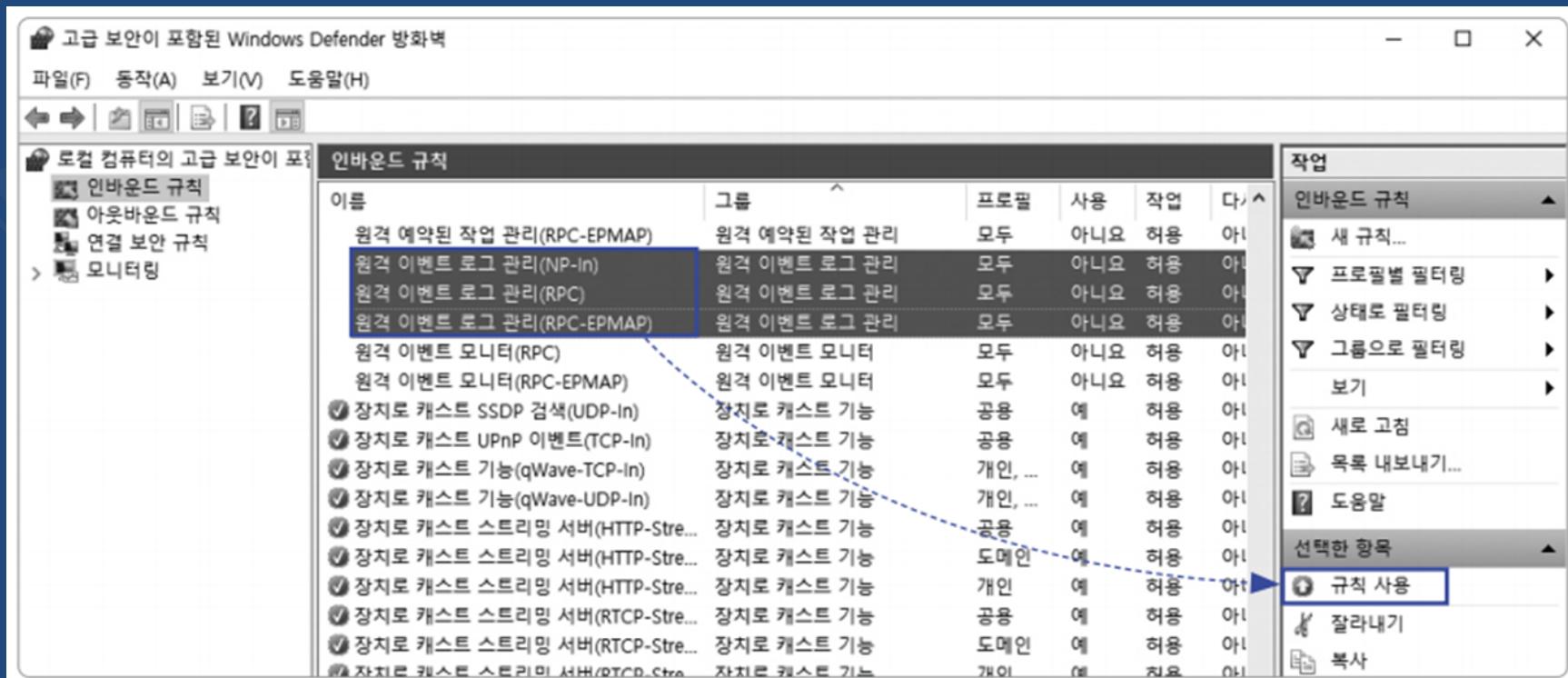
Active Directory Domain Service



Q. 외부에서 SECOND 서버 관리 가능하도록 설정 하세요. [SECOND]

1-3) 외부에서 RDP 접속 가능하도록 설정

- 서버 관리자 → 로컬 서버 → Microsoft Defender 방화벽 / 도메인, 개인, 공개 → 프로그램 설정 / 방화벽 설정:네트워크 보호 설정 → 인바운드 규칙 → 원격 이벤트 로그 관리 (NP-In) (RPC) (PRC-EPMAP) → 규칙 사용 → 로그 아웃



Active Directory Domain Service



Q. 외부에서 THIRD 서버 관리 가능하도록 설정 하세요. [THIRD]

1-1) 외부에서 RDP 접속 가능하도록 설정

- 관리자 계정 접속 (administrator@hanbit.com) → 제어판 → 시스템 및 보안 → 시스템 / 원격 액세스 허용
→ 시스템 속성 / 원격 / 이 컴퓨터에 대한 원격 연결 허용

1-2) 외부에서 RDP 접속 가능하도록 설정

- 서버 관리자 → 로컬 서버 → Microsoft Defender 방화벽 / 도메인, 개인, 공개 → 프로그램 설정 / 방화벽 설정:네트워크 보호 설정 → 인바운드 규칙 → COM+ 네트워크 액세스 (DCOM-In) → 규칙 사용

1-3) 외부에서 RDP 접속 가능하도록 설정

- 서버 관리자 → 로컬 서버 → Microsoft Defender 방화벽 / 도메인, 개인, 공개 → 프로그램 설정 / 방화벽 설정:네트워크 보호 설정 → 인바운드 규칙 → 원격 이벤트 로그 관리 (NP-In) (RPC) (PRC-EPMAP) → 규칙 사용 → 로그 아웃

Active Directory Domain Service



Q. FIRST 서버에서 SECOND , THIRD 서버 관리를 위해 원격 접속 해보세요. [FIRST]

1) 서버 관리자 → 모든 서버 → SECOND 우클릭 → 원격 데스크톱 연결

- SECOND.second.hanbit.com
- SECOND@administrator
- administrator@second.hanbit.com

2) 서버 관리자 → 모든 서버 → THIRD 우클릭 → 원격 데스크톱 연결

- THIRD.hanbit.com
- HANBIT@administrator
- administrator@hanbit.com

Active Directory Domain Service



Q. 현재 상태를 스냅숏으로 저장하세요.

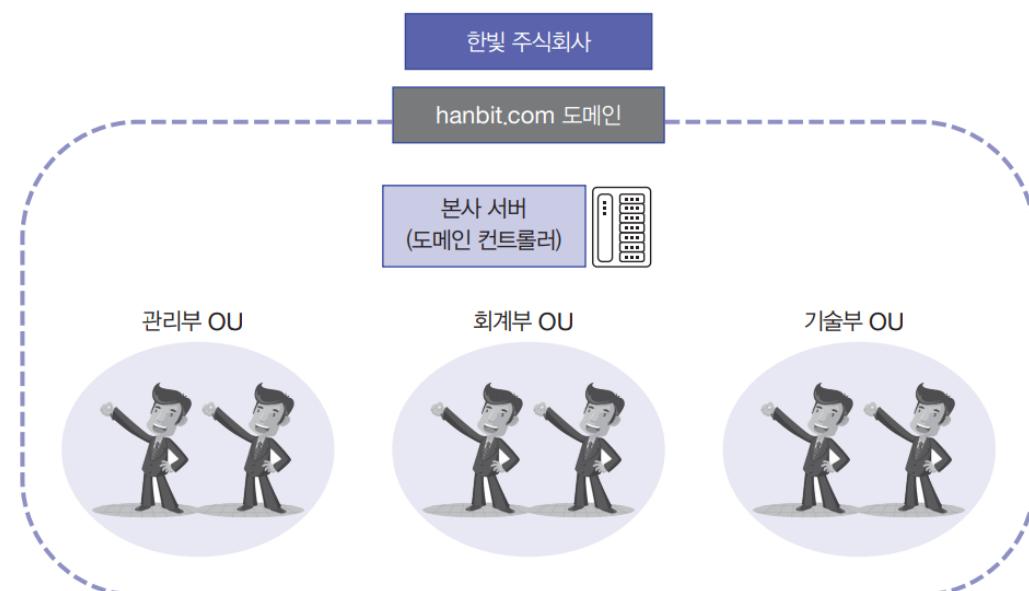
- FIRST , SECOND , THIRD 컴퓨터 종료
- 스냅숏 이름 : AD 구성 완료
- 부팅 순서 : FIRST , SECOND , THIRD , WINCLIENT

AD 사용자 계정과 조직 구성 단위

- 사용자 계정
 - ‘로컬 사용자 계정’과 AD 도메인에 접근 가능한 ‘도메인 사용자 계정’이 있음
- 도메인 사용자 계정 표현 (ex. hanbit.com 의 thisUser)
 - 기본 도메인 로그온 이름 : HANBIT\thisUser
 - UPN(User Principal Name) : thisUser@hanbit.com
 - Distinguished name : CN=thisUser , OU=조직구성단위이름 , DC=hanbit , DC=com
 - Relative Distinguished name : CN=thisUser

AD 사용자 계정과 조직 구성 단위

- 조직 구성 단위 (Organizational Unit , OU)
 - 사용자 , 그룹 , 컴퓨터를 포함할 수 있는 Active Directory 컨테이너
 - 즉. 회사의 내부의 조직 , 도메인의 작은 개념
 - 사용자 뿐만 아니라 컴퓨터, 프린터, 그룹, 다른 OU등 모두 포함 가능



Active Directory Domain Service



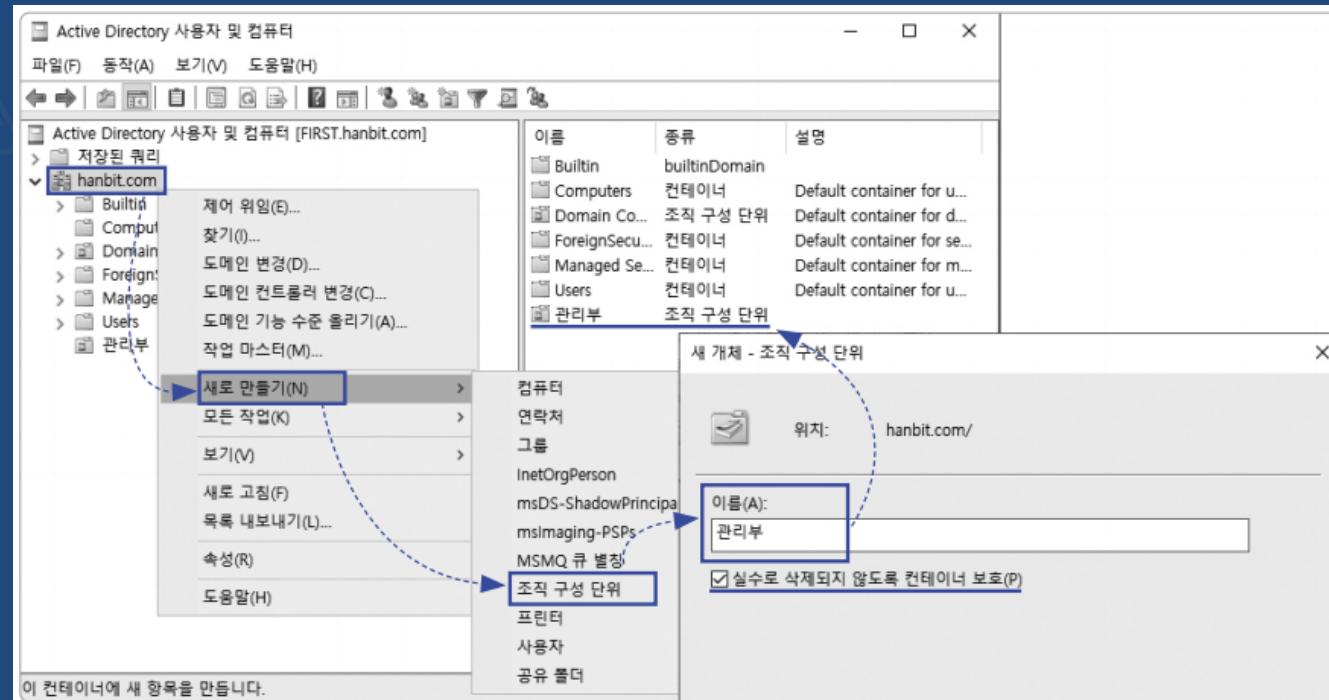
Q. OU를 생성하고 운영 하세요. [FIRST]

준비. FIRST , SECOND , WINCLIENT 사용

준비. FIRST의 AD 구성 동작 확인 후 SECOND , WINCLIENT 부팅

1) OU 생성

- 서버 관리자 → 도구 → Active Directory 사용자 및 컴퓨터 → hanbit.com 우클릭 → 새로 만들기 → 조직 구성 단위
→ 이름 : 관리부



Active Directory Domain Service



Q. OU를 생성하고 운영 하세요. [FIRST]

2) OU 추가

- 회계부 , 기술부 추가

The screenshot shows the Windows Server Management Console with the title bar "Active Directory 사용자 및 컴퓨터". The left pane displays a tree view of the domain structure under "Active Directory 사용자 및 컴퓨터 [FIRST.hanbit.com]". The "hanbit.com" node is expanded, showing subcontainers like Builtin, Computers, Domain Controllers, ForeignSecurityPrincipals, Managed Service Accounts, and Users. Below these, three new containers are being added: 관리부 (Management), 회계부 (Accounting), and 기술부 (Technology). The right pane is a table listing existing containers with their types and descriptions. The newly created containers are listed at the bottom of the table.

이름	종류	설명
Builtin	builtinDomain	
Computers	컨테이너	Default container for upgraded com...
Domain Co...	조직 구성 단위	Default container for domain control...
ForeignSecu...	컨테이너	Default container for security identifi...
Managed Se...	컨테이너	Default container for managed servic...
Users	컨테이너	Default container for upgraded user ...
관리부	조직 구성 단위	
회계부	조직 구성 단위	
기술부	조직 구성 단위	

Active Directory Domain Service



Q. OU를 생성하고 운영 하세요. [FIRST]

1) OU 안에 OU 생성

- 관리부 우클릭 → 새로 만들기 → 조직 구성 단위 → 이름 : 공정팀
- 관리부 우클릭 → 새로 만들기 → 조직 구성 단위 → 이름 : 인사팀

이름	종류	설명
공정팀	조직 구성 단위	조직 구성 단위
인사팀	조직 구성 단위	조직 구성 단위

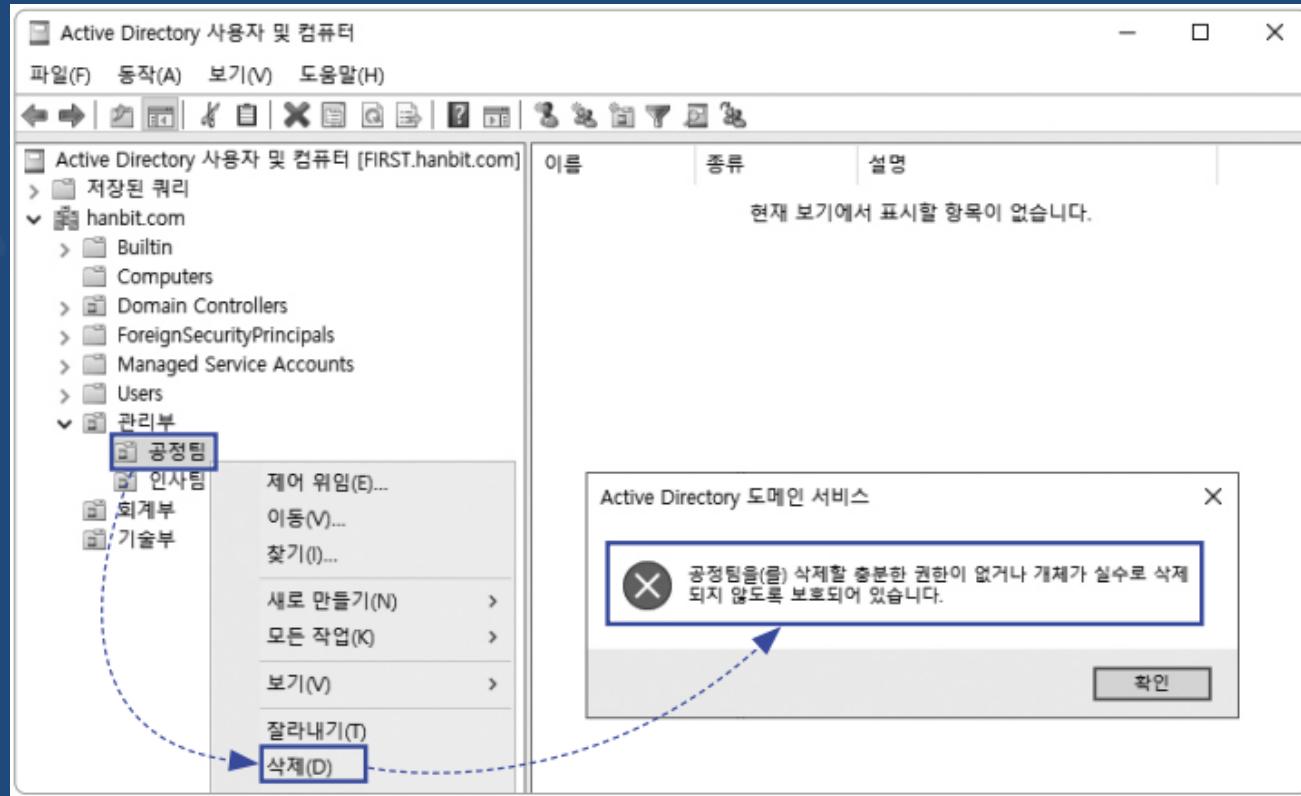
Active Directory Domain Service



Q. OU를 생성하고 운영 하세요. [FIRST]

1) OU 삭제

- 공정팀 우클릭 → 삭제
- 실수 방지를 위해 ‘컨테이너 보호’



Active Directory Domain Service



Q. OU를 생성하고 운영 하세요. [FIRST]

2) OU 삭제

- 보기 → 고급 기능 → 개체 → 개체의 정식 이름 : hanbit.com/관리부/공정팀 → 실수로 삭제되지 않도록 개체 보호
 - 공정팀 우클릭 → 삭제
-
- 보기 → 고급 기능 → 개체 → 개체의 정식 이름 : hanbit.com/관리부/인사팀 → 실수로 삭제되지 않도록 개체 보호
 - 인사팀 우클릭 → 삭제

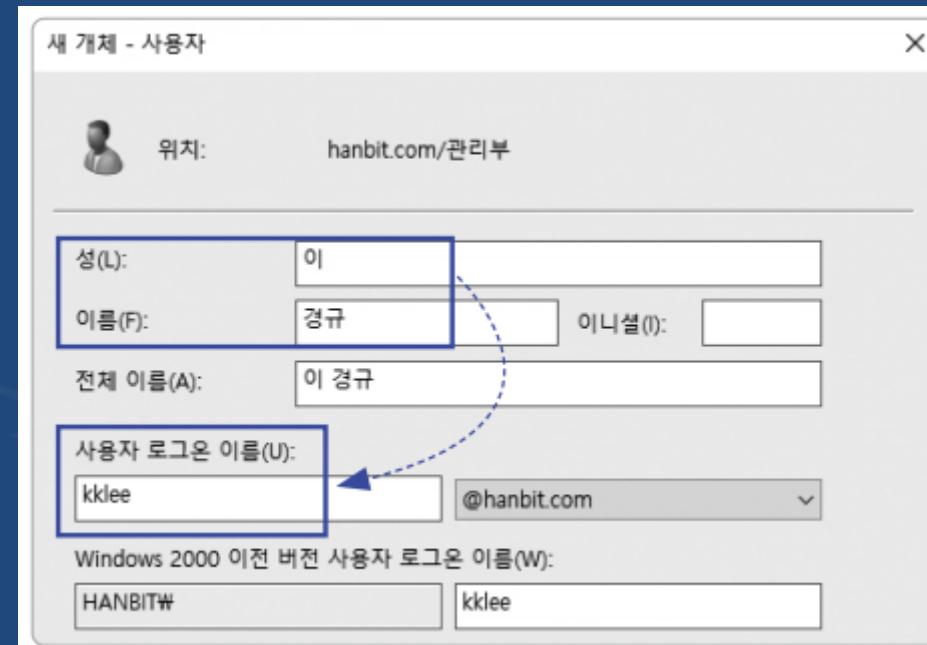
Active Directory Domain Service



Q. hanbit.com 도메인 사용자 계정을 생성하고 OU에 소속시켜 운영 하세요. [FIRST]

1-1) 사용자 계정 생성

- Active Directory 사용자 및 컴퓨터 → 관리부 우클릭 → 새로 만들기 / 사용자
- 새 개체 - 사용자
 - 성 : 이
 - 이름 : 경규
 - 사용자 로그온 이름 : kklee
= kklee@hnabit.com



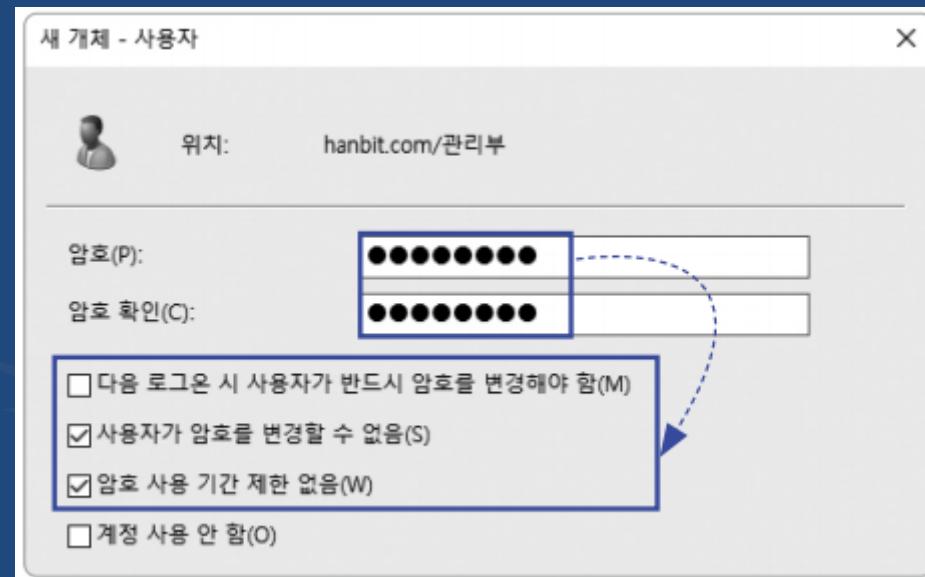
Active Directory Domain Service



Q. hanbit.com 도메인 사용자 계정을 생성하고 OU에 소속시켜 운영 하세요. [FIRST]

1-2) 사용자 계정 생성

- Active Directory 사용자 및 컴퓨터 → 관리부 우클릭 → 새로 만들기 / 사용자
- 새 개체 - 사용자
 - 암호 : p@ssw0rd
 - ✗ 다음 로그온 시 사용자가 반드시 암호를 변경해야 함
 - ✗ 암호 사용 기간 제한 없음



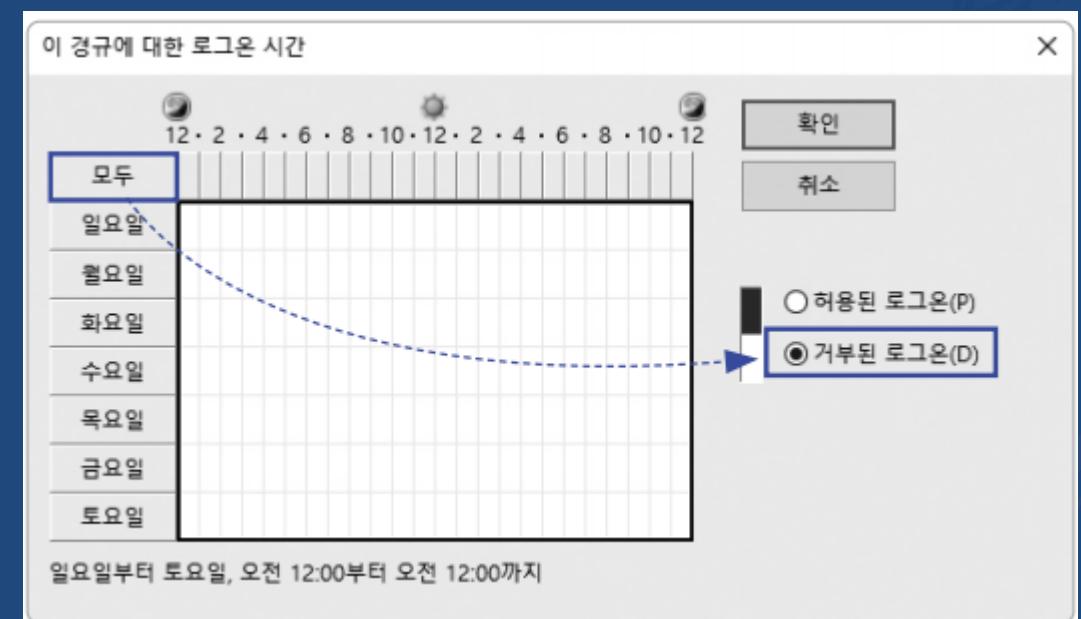
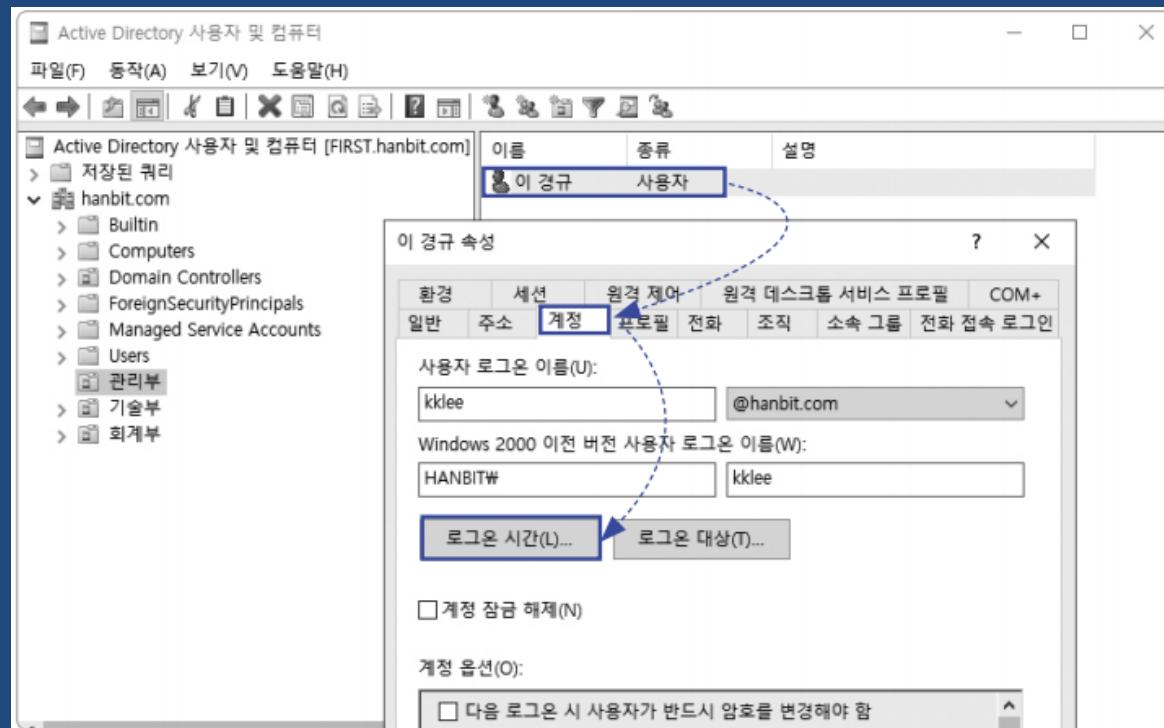
Active Directory Domain Service



Q. hanbit.com 도메인 사용자 계정을 생성하고 OU에 소속시켜 운영 하세요. [FIRST]

2-1) 접속 가능 시간 설정

- 관리부 → 이 경규 더블클릭 → 속성 / 계정 → 로그온 시간 → 모두 → 거부된 로그온
- 모든 요일 / 모든 시간 / 로그온 거부



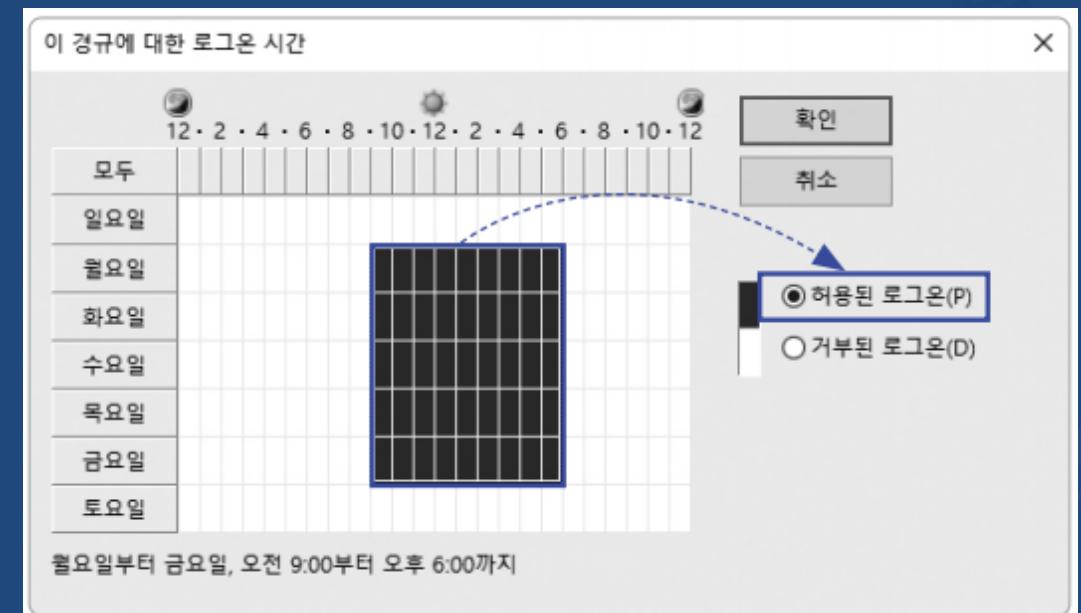
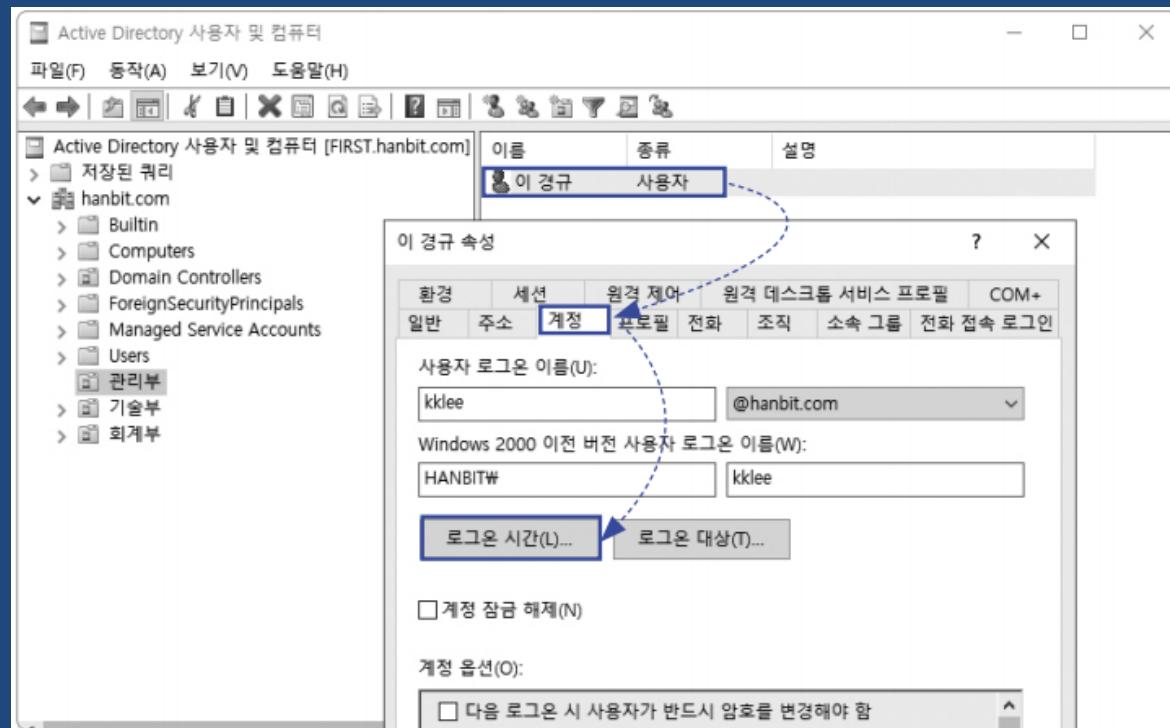
Active Directory Domain Service



Q. hanbit.com 도메인 사용자 계정을 생성하고 OU에 소속시켜 운영 하세요. [FIRST]

2-2) 접속 가능 시간 설정

- 월요일 ~ 금요일 / 오전 9시 ~ 오후 6시 / 로그온 허용



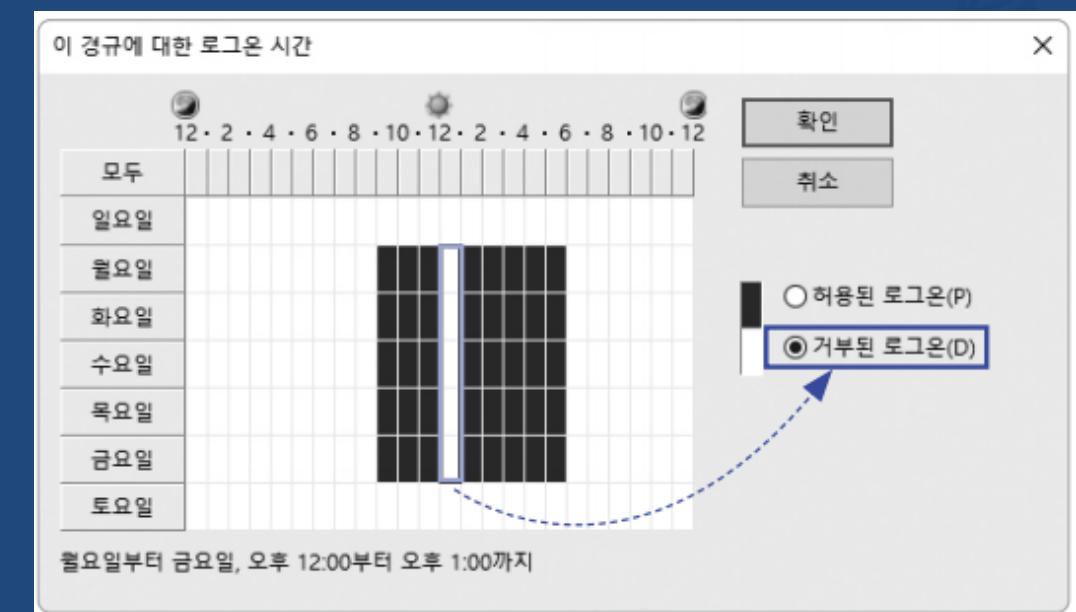
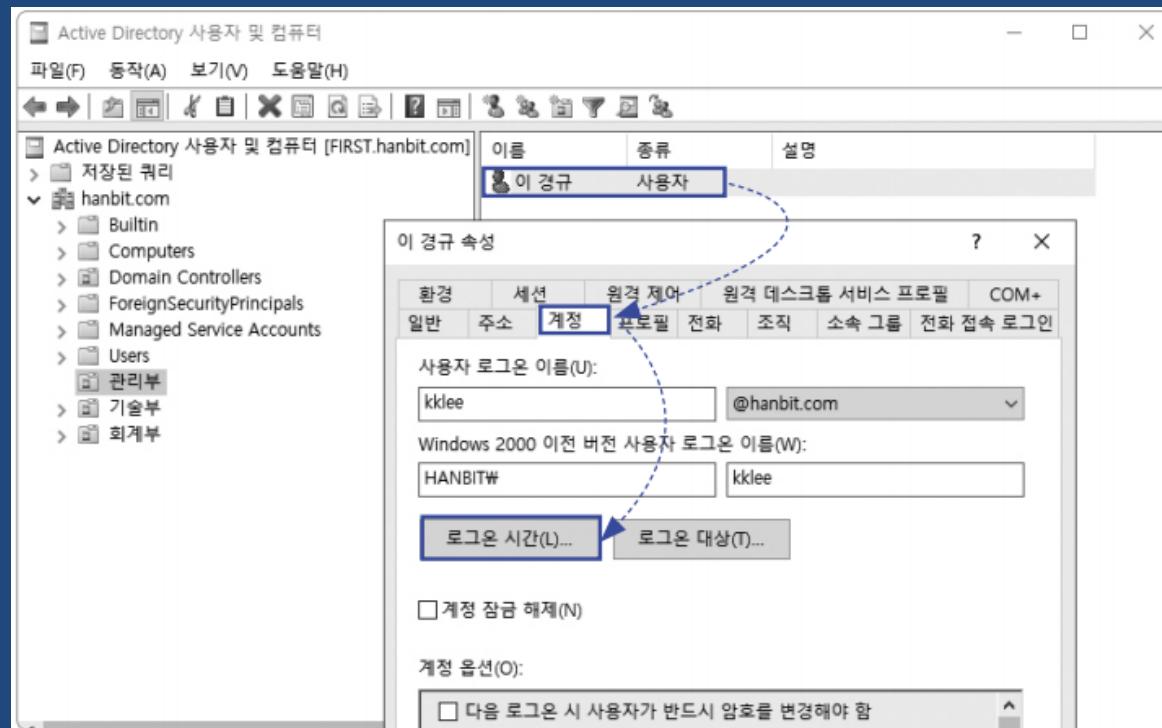
Active Directory Domain Service



Q. hanbit.com 도메인 사용자 계정을 생성하고 OU에 소속시켜 운영 하세요. [FIRST]

2-3) 접속 가능 시간 설정

- 월요일 ~ 금요일 / 오전 9시 ~ 오후 12시, 오후 1시 ~ 오후 6시 / 로그온 허용
- 월요일 ~ 금요일 / 오전 12시 ~ 오후 1시 / 로그온 거부



Active Directory Domain Service

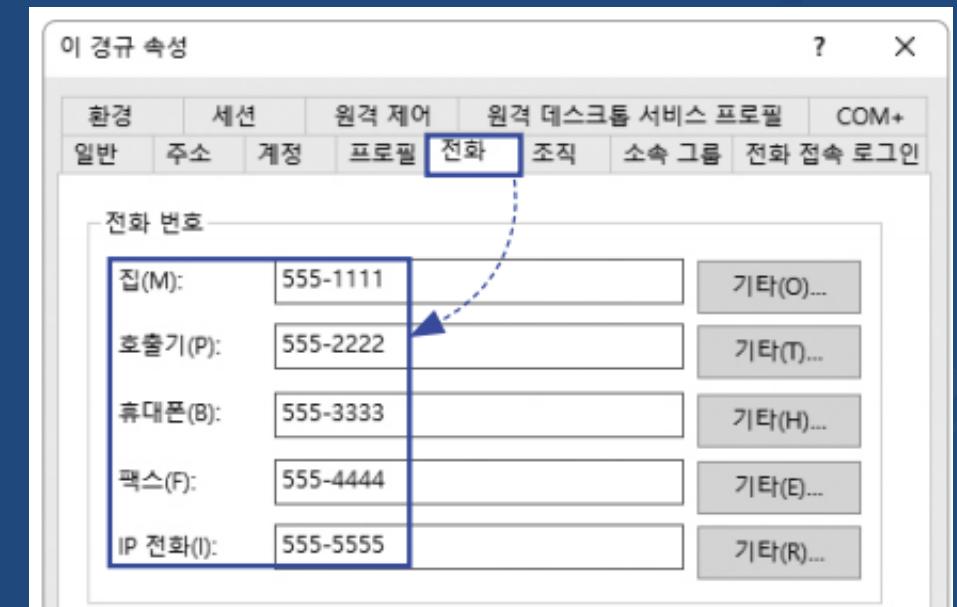
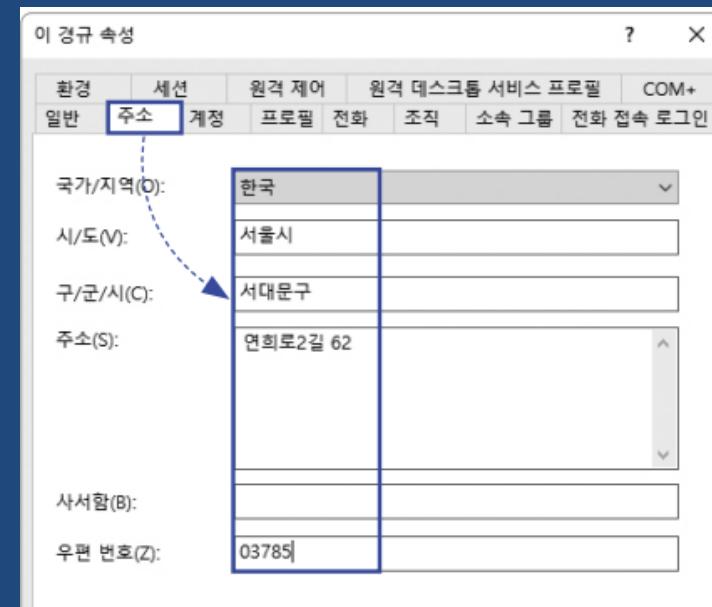


Q. hanbit.com 도메인 사용자 계정을 생성하고 OU에 소속시켜 운영 하세요. [FIRST]

3-1) 사용자 주소/전화 설정

- 관리부 → 이 경규 더블클릭 → 속성 / 주소

- 시/도 : 서울시
- 구/군/시 : 양천구
- 주소 : 목동 124-1 한국전파진흥협회
- 우편번호 : 07969



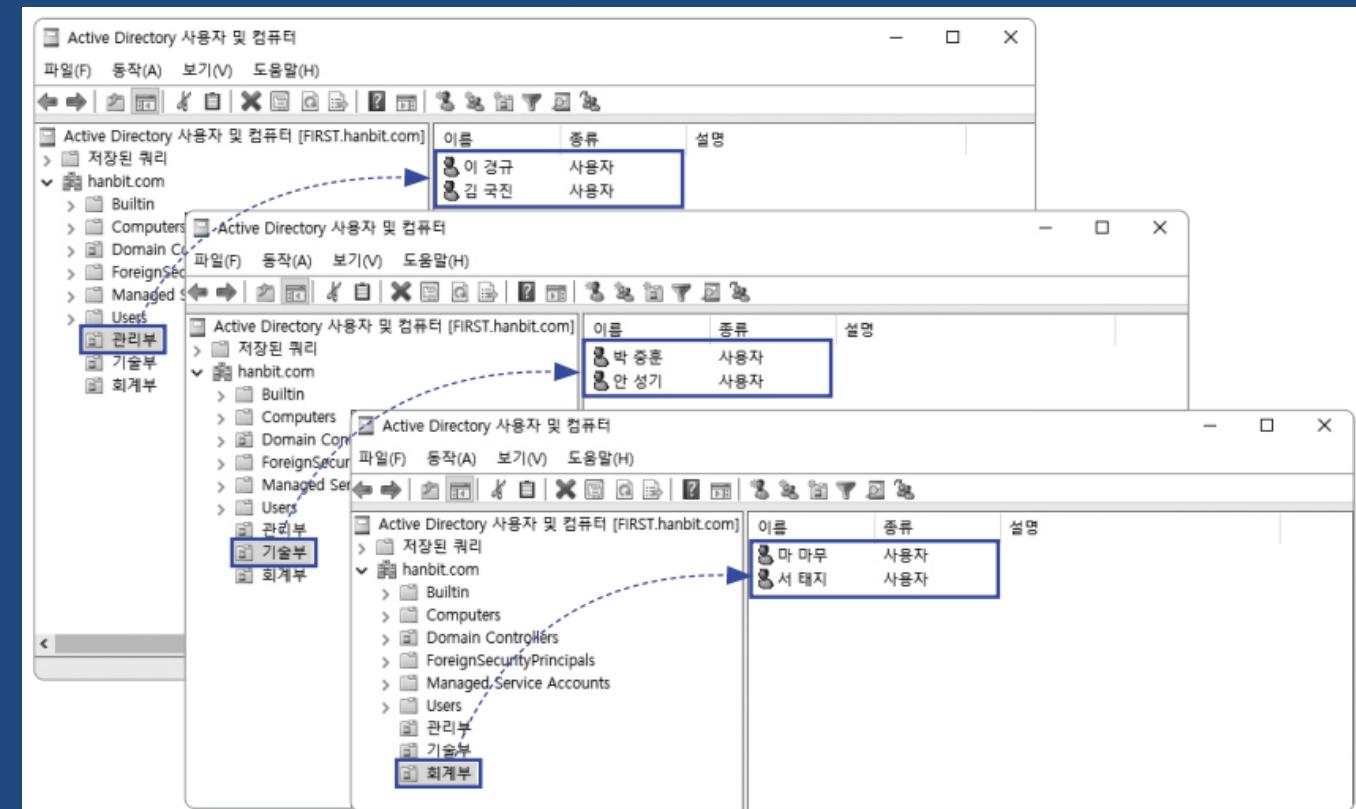
Active Directory Domain Service



Q. hanbit.com 도메인 사용자 계정을 생성하고 OU에 소속시켜 운영 하세요. [FIRST]

1) 템플릿 만들어 사용자 생성

- 관리부 OU : 김 국진 (kjkim) / p@ssw0rd / 사용자 암호 변경 불가 / 암호 사용 기간 없음
- 기술부 OU : 안성기 (skann) , 박중훈 (jhpark)
- 회계부 OU : 서태지 (tgseo) , 마마무 (mmma)



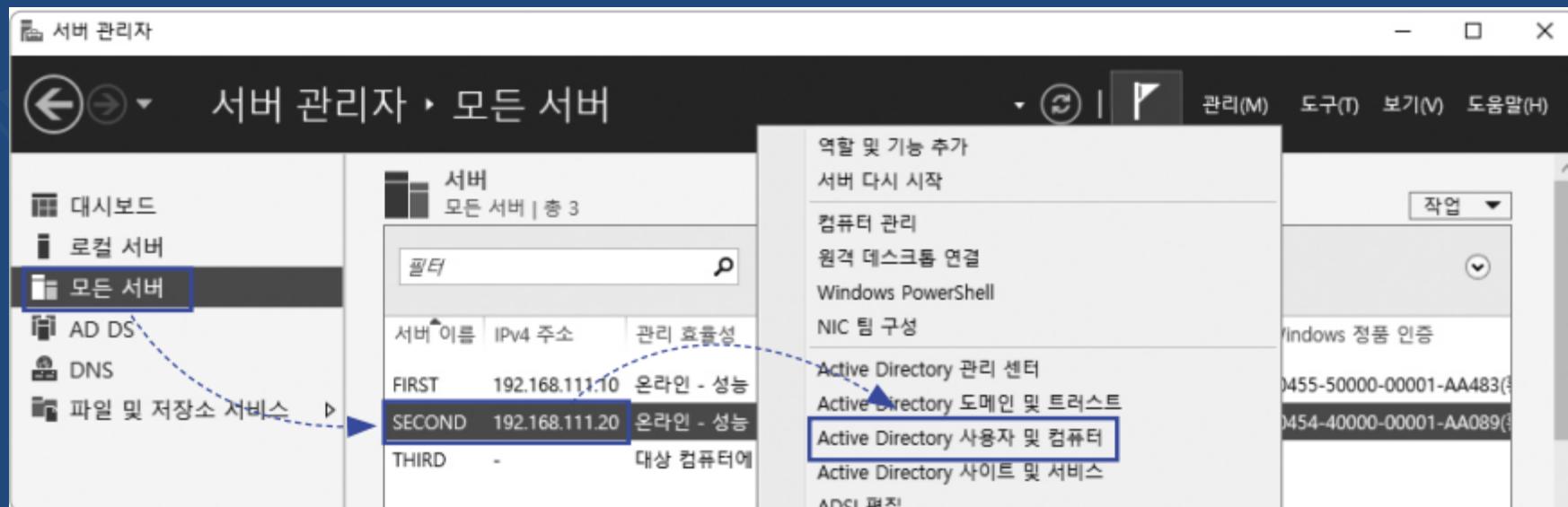
Active Directory Domain Service



Q. FIRST 서버에서 second.hanbit.com 도메인에 사용자 생성하고 운영 하세요. [FIRST]

1) FIRST 서버에서 second.hanbit.com AD 도메인 컨트롤러 접근

- 서버 관리자 → 모든 서버 → SECOND 우클릭 → Active Directory 사용자 및 컴퓨터



Active Directory Domain Service

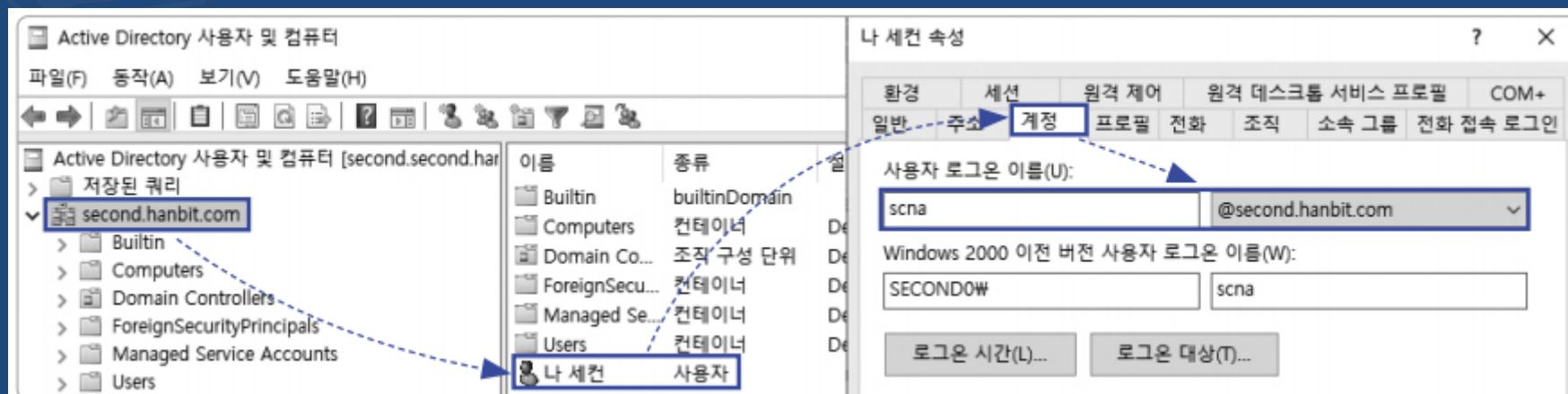


Q. FIRST 서버에서 second.hanbit.com 도메인에 사용자 생성하고 운영 하세요. [FIRST]

2) FIRST 서버에서 second.hanbit.com 도메인 사용자 생성

– Active Directory 사용자 및 컴퓨터 → second.hanbit.com 우클릭 → 새로 만들기 / 사용자

- 성 : 나
 - 이름 : 세컨
 - 사용자 로그온 이름 : scna
- = scna@second.hanbit.com



Active Directory Domain Service



Q. 새로 생성된 도메인 사용자로 로그온 하세요. [WINCLIENT]

- 1) WINCLIENT 컴퓨터에서 hanbit.com 도메인 사용자 이경규(kklee@hanbit.com) 로그온 확인



Active Directory Domain Service



Q. 새로 생성된 도메인 사용자로 로그온 하세요. [WINCLIENT]

2) WINCLIENT 컴퓨터에서 second.hanbit.com 도메인 사용자 나세컨(scna@second.hanbit.com) 로그온 확인



AD 그룹 개요

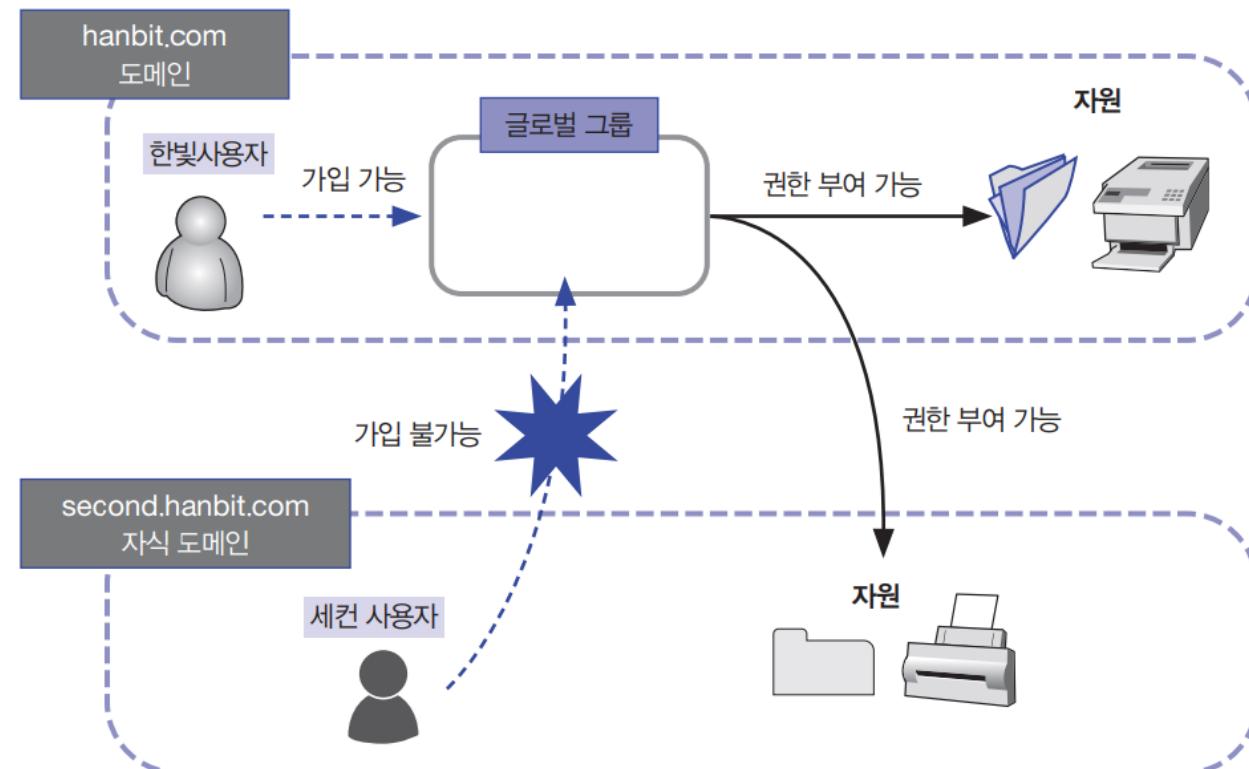
- 사용자 또는 컴퓨터의 집합
- 그룹은 다른 그룹을 포함 가능
- 그룹을 구성하는 컴퓨터 및 사용자의 편리한 권한 부여가 목적
- AD가 운영되는 회사의 사원이 100명 이라면?
 - 각 직원마다 권한 부여 위해서는 많은 시간과 노력 필요
 - 운영 및 관리 불편
- ‘사원 그룹’ 생성 후 그룹에만 권한 부여 후 100명의 사원을 그룹에 소속
 - 그룹에 소속된 사원은 그룹의 권한을 갖게 됨
- 그룹 종류
 - 배포 그룹
 - 보안 그룹
 - 글로벌 그룹
 - 도메인 로컬 그룹
 - 유니버설 그룹

AD 그룹 종류

▪ 보안 그룹 (Security Group)

- 글로벌 그룹

- 모든 도메인에 위치한 자원의 권한 할당 가능 (공유풀더, 프린터 등...)
- 글로벌 그룹을 생성한 도메인의 구성원만 소속이 가능

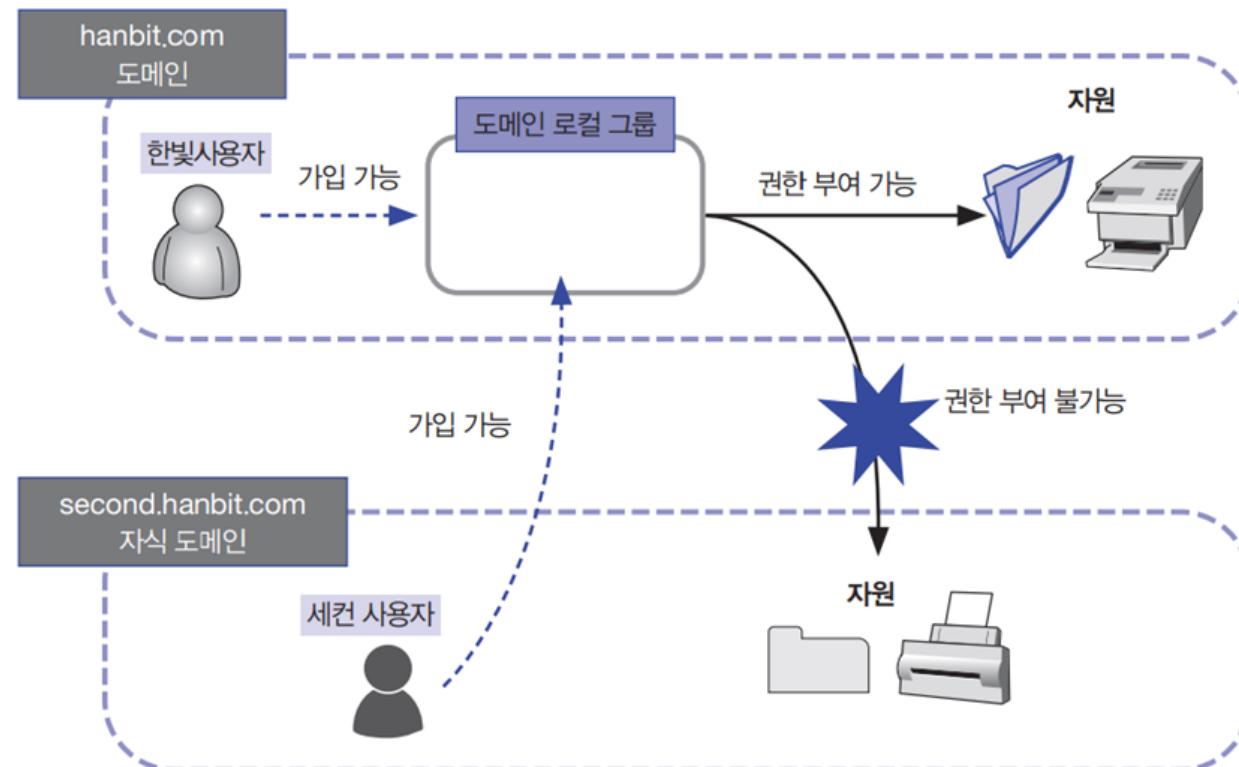


AD 그룹 종류

▪ 보안 그룹 (Security Group)

- 도메인 로컬 그룹

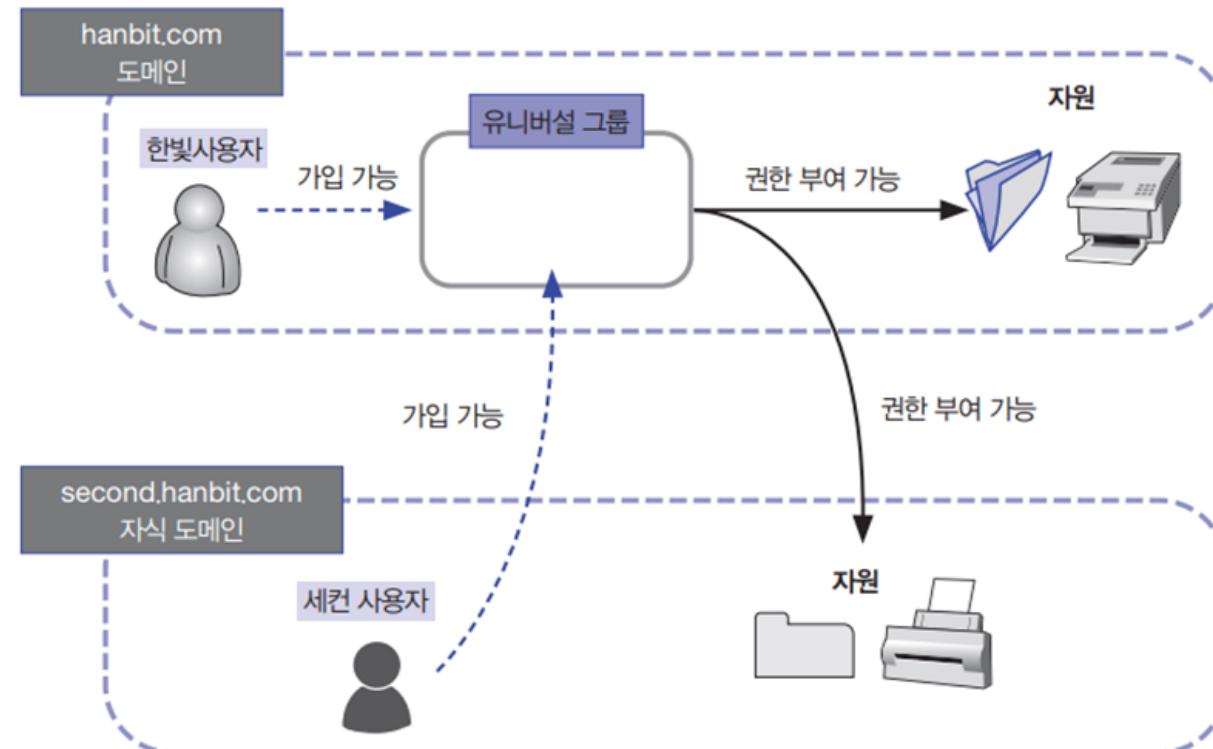
- 다른 도메인에 있는 사용자도 구성원 가능
- 도메인 로컬 그룹을 생성한 도메인의 자원만 권한 할당 가능



AD 그룹 종류

▪ 보안 그룹 (Security Group)

- 유니버설 그룹 유니버설 그룹의 정보는 GC 모두 저장해야하는 정보
포리스트의 AD 성능이 전반적으로 하락, 따라서 유니버설 그룹 최소화
 - 글로벌 그룹 + 도메인 로컬 그룹
 - 모든 도메인의 자원에 대한 권한 할당 가능 / 모든 도메인의 사용자 소속 가능



Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요. [FIRST]

1) 사용자 생성

- 한빛 사용자 : hanbitUser@hanbit.com / VMware1!

The screenshot shows the Windows Active Directory User and Computer Management console. On the left, the navigation pane shows the domain structure under 'Active Directory 사용자 및 컴퓨터 [FIRST.hanbit.com]'. A blue box highlights the 'hanbit.com' node. On the right, the 'New User Properties' dialog box is open, showing the 'General' tab selected. The 'User logon name (U):' field contains 'hanbitUser' and the 'Domain (W):' dropdown shows '@hanbit.com'. The 'User' object class is selected in the list of object types. At the bottom of the dialog, several checkboxes are checked, including 'The user must change the password at next logon', 'The user cannot change the password', and 'The password never expires'.

Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요. [FIRST]

2-1) 그룹 생성

- Active Directory 사용자 및 컴퓨터 → hanbit.com 우클릭 → 새로 만들기/그룹 → 새 개체/그룹
- 이름 : **한빛글로벌그룹**
- 그룹 범위 : **글로벌**



Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요. [FIRST]

2-2) 그룹 생성

- 한빛도메인로컬그룹 / 보안그룹 - 도메인 로컬
- 한빛유니버설그룹 / 보안그룹 - 유니버설

이름	종류	설명
Builtin	builtinDomain	
Computers	컨테이너	Default container for upgraded com...
Domain Controllers	조직 구성 단위	Default container for domain control...
ForeignSecurityPrincipals	컨테이너	Default container for security identifi...
Managed Service Accounts	컨테이너	Default container for managed servic...
Users	컨테이너	Default container for upgraded user ...
관리부	조직 구성 단위	
기술부	조직 구성 단위	
직원 템플릿	사용자	
한빛 사용자	사용자	
한빛글로벌그룹	보안 그룹 - 글로벌	
한빛도메인로컬그룹	보안 그룹 - 도메인 로컬	
한빛유니버설그룹	보안 그룹 - 유니버설	
회계부	조직 구성 단위	

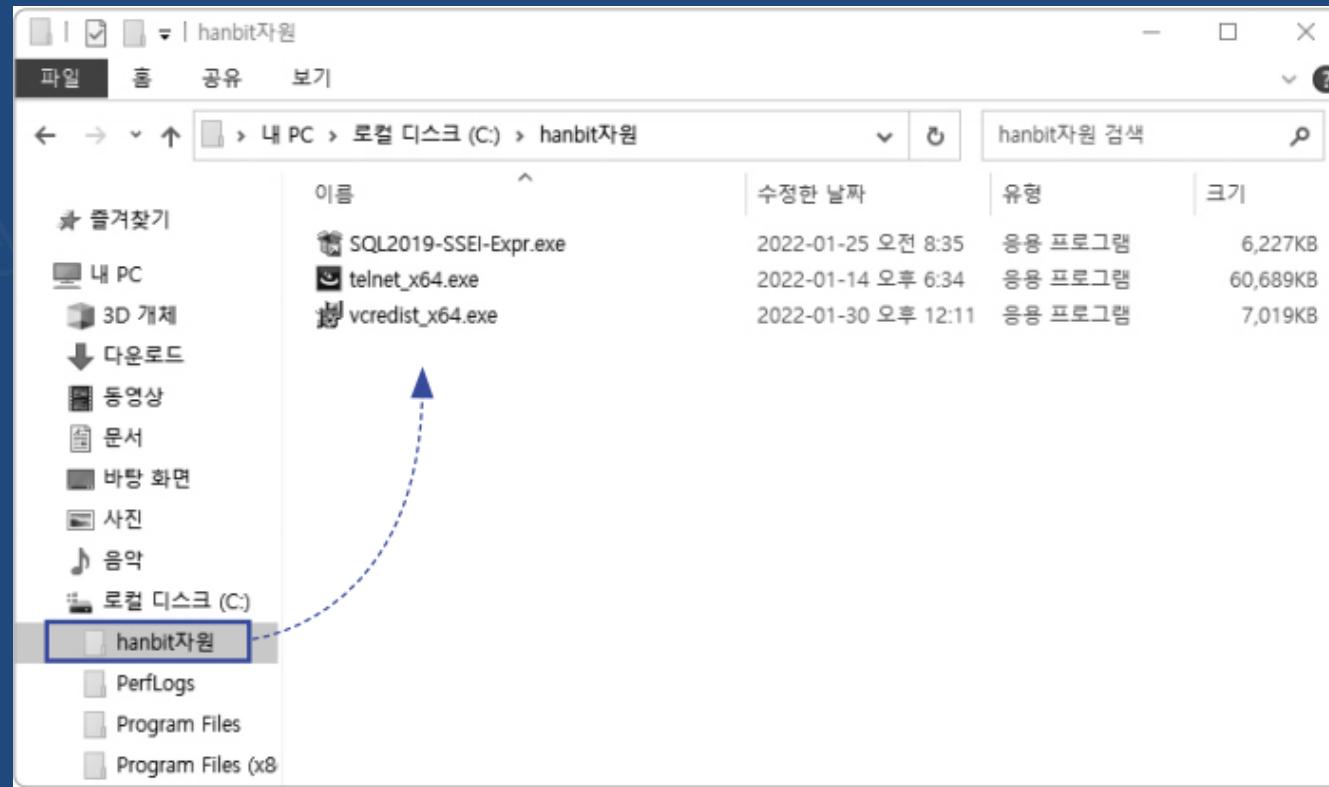
Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요. [FIRST]

3) hanbit.com 준비

- C:\hanbit자원



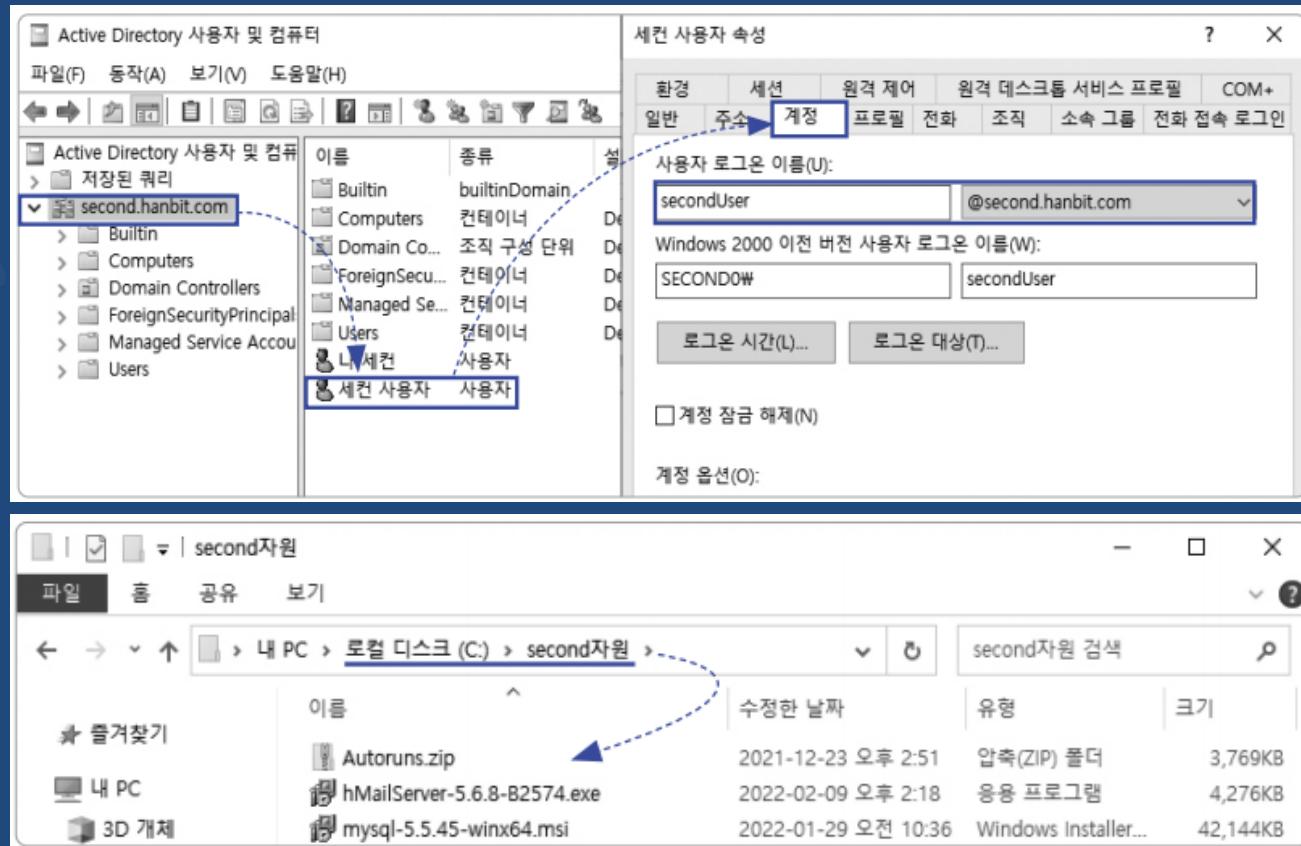
Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요. [SECOND]

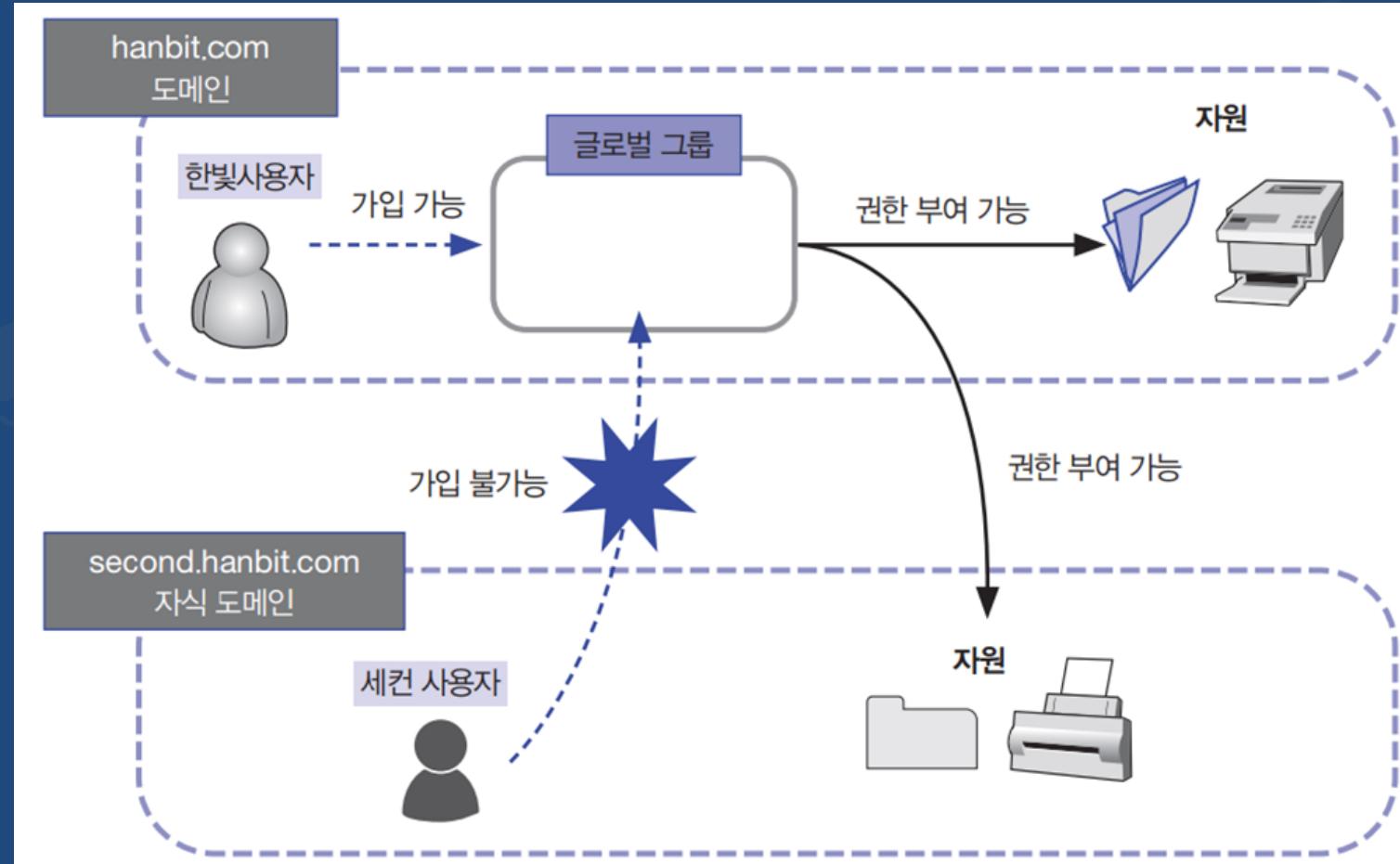
4) second.hanbit.com 준비

- 세컨 사용자 : secondUser@second.hanbit.com / VMware!
- C:\second자원\



Active Directory Domain Service

Q. 그룹을 생성해 권한을 주고 운영 하세요.



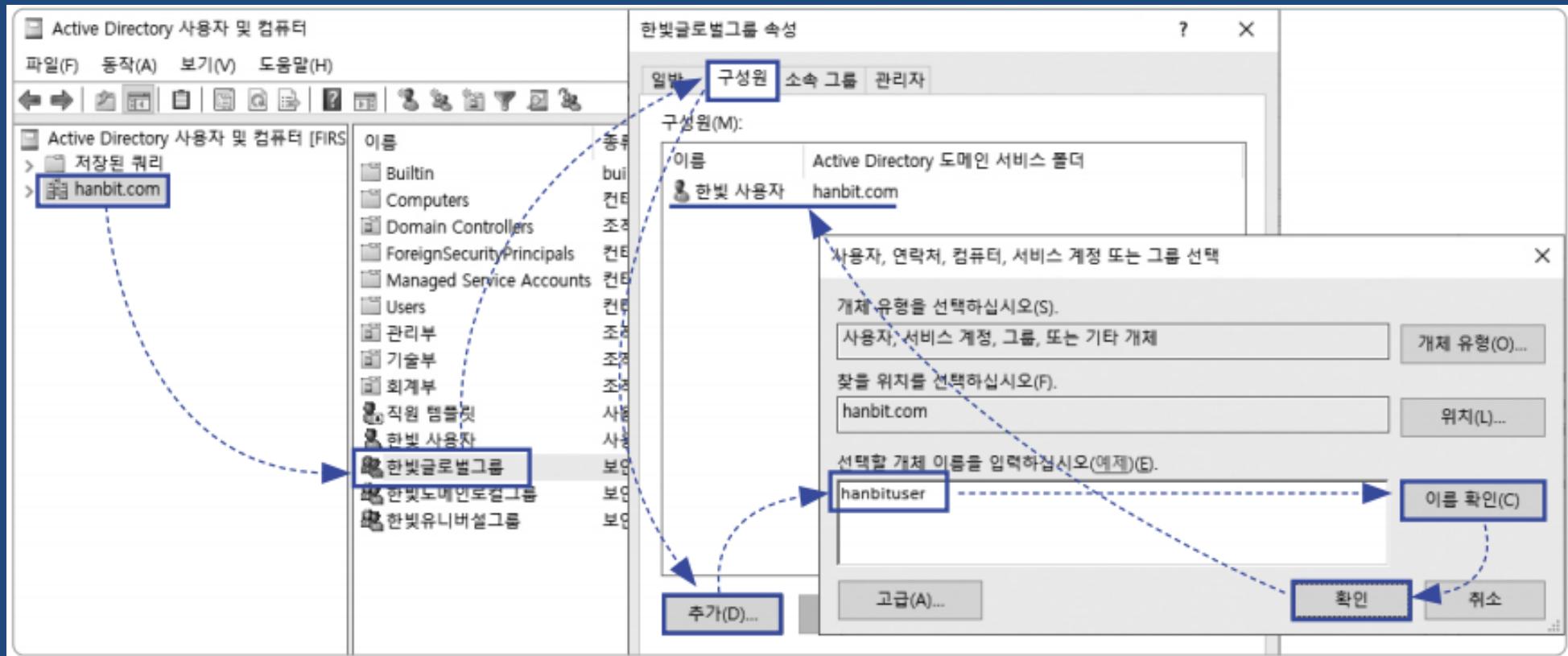
Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요. [FIRST]

5-1) 글로벌 그룹 가입

- hanbit.com → 한빛글로벌그룹 더블클릭 → 구성원/추가 → 선택할 개체 이름 : hanbitUser



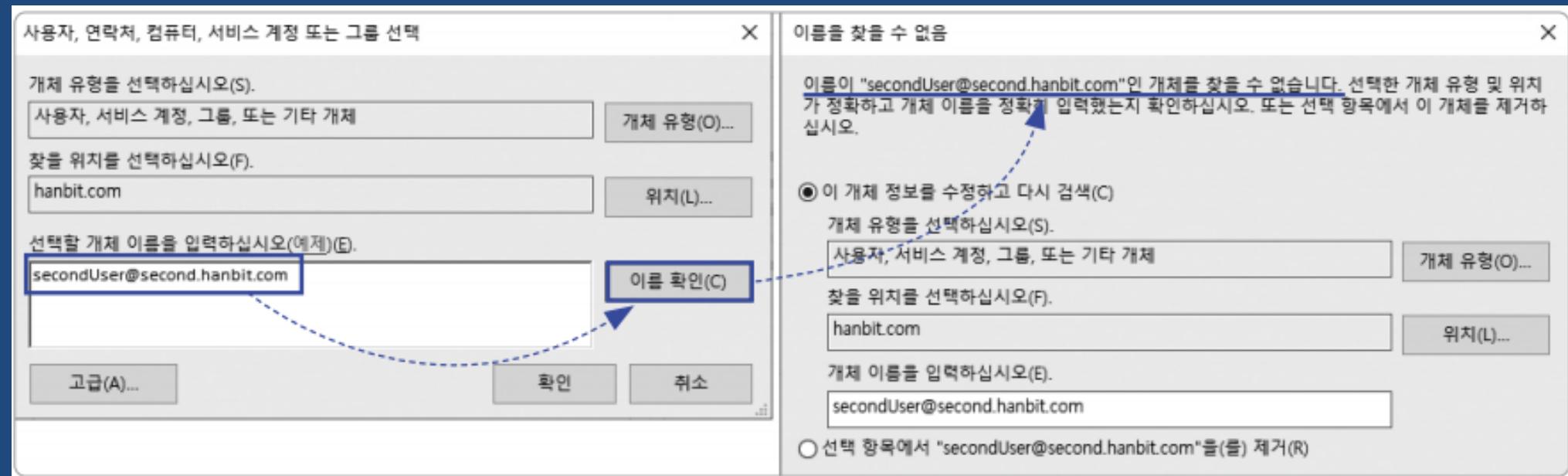
Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요. [FIRST]

5-2) 글로벌 그룹 가입

- hanbit.com → 한빛글로벌그룹 더블클릭 → 구성원/추가 → 선택할 개체 이름 : secondUser@second.hanbit.com



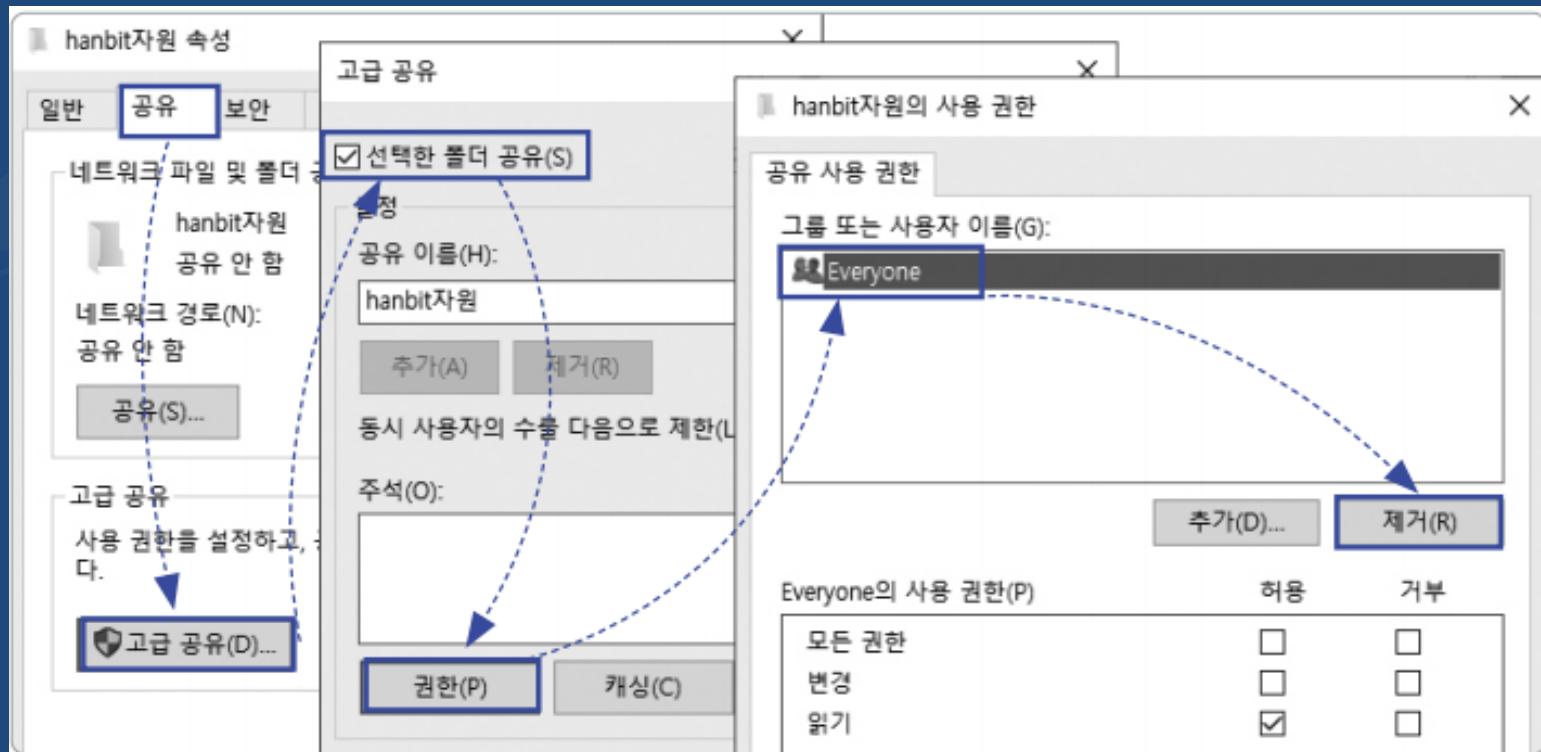
Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요. [FIRST]

6-1) hanbit.com 자원 글로벌 그룹 공유

- 'C:\hanbit자원' 우클릭 → 속성/공유/고급공유/선택한 폴더 공유 → 권한 → Everyone 제거



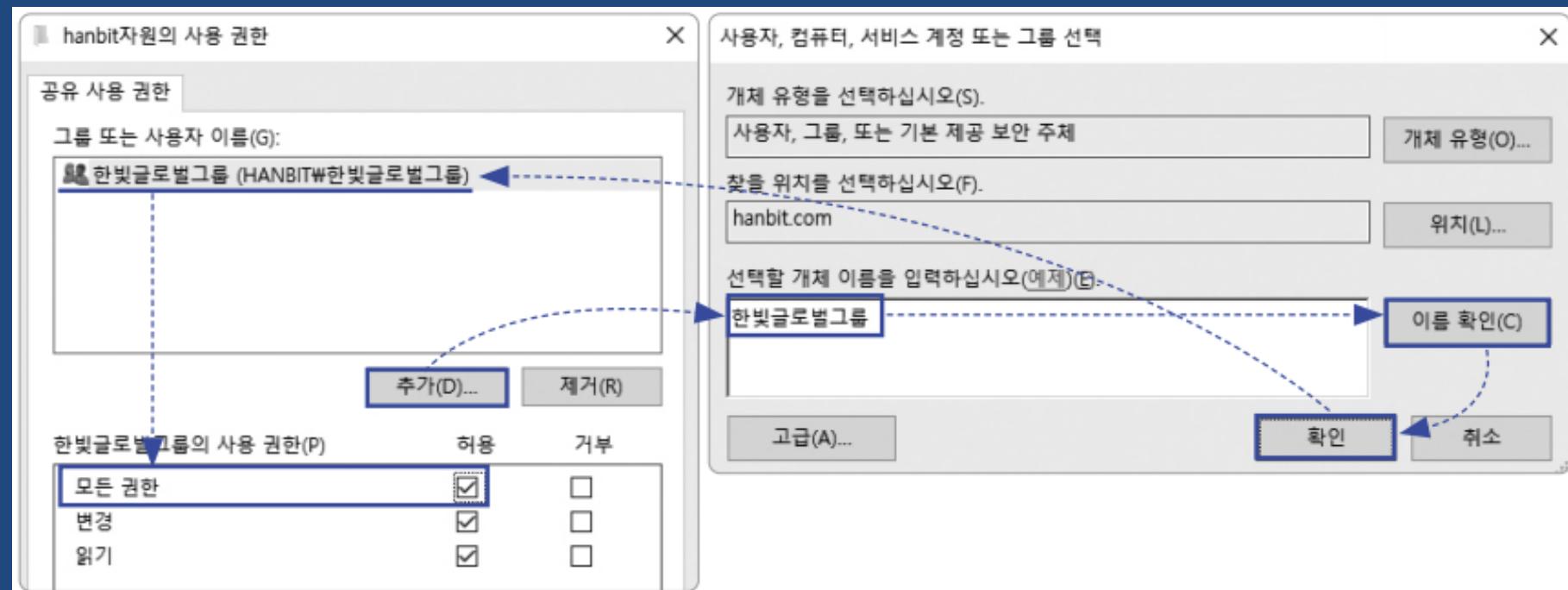
Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요. [FIRST]

6-2) hanbit.com 자원 글로벌 그룹 공유

- 'C:\hanbit자원' 우클릭 → 속성/공유/고급공유/선택한 폴더 공유 → 권한 → 추가 → 한빛글로벌그룹 (모든권한)



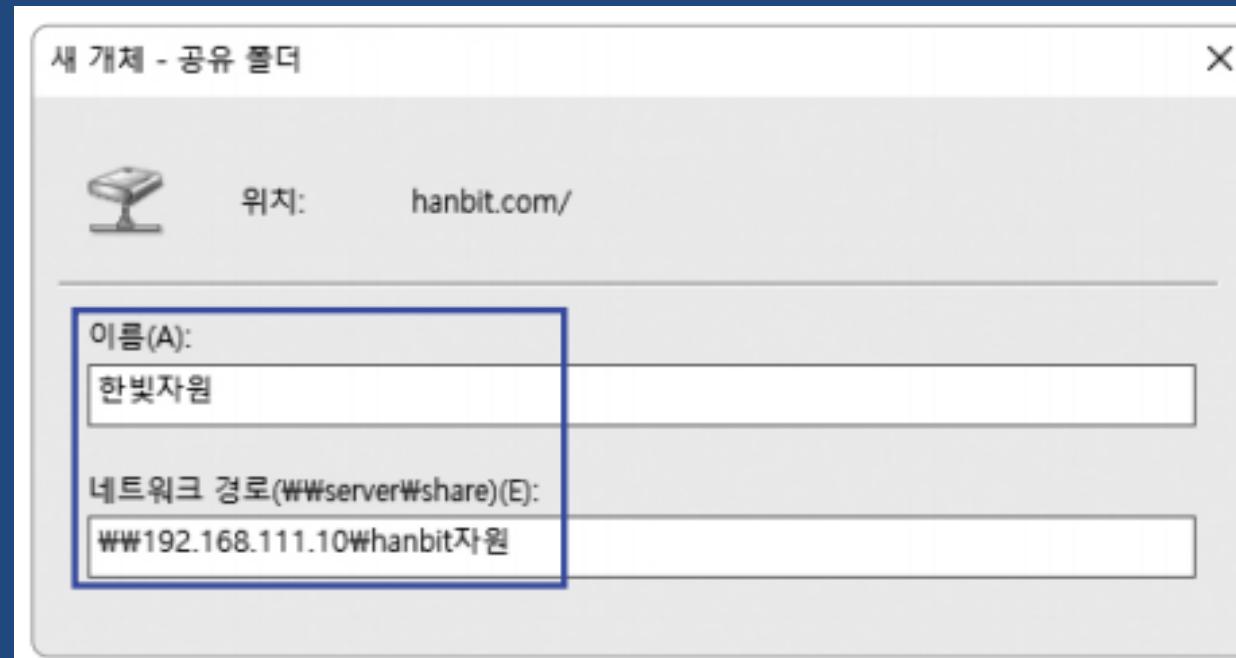
Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요. [FIRST]

7-1) hanbit.com 자원 AD검색 등록

- Active Directory 사용자 및 컴퓨터 → hanbit.com 우클릭 → 새로 만들기/공유 폴더 → 새 개체/공유 폴더
- 이름 : **한빛자원**
- 네트워크 경로 : **\192.168.111.10\hanbit자원**



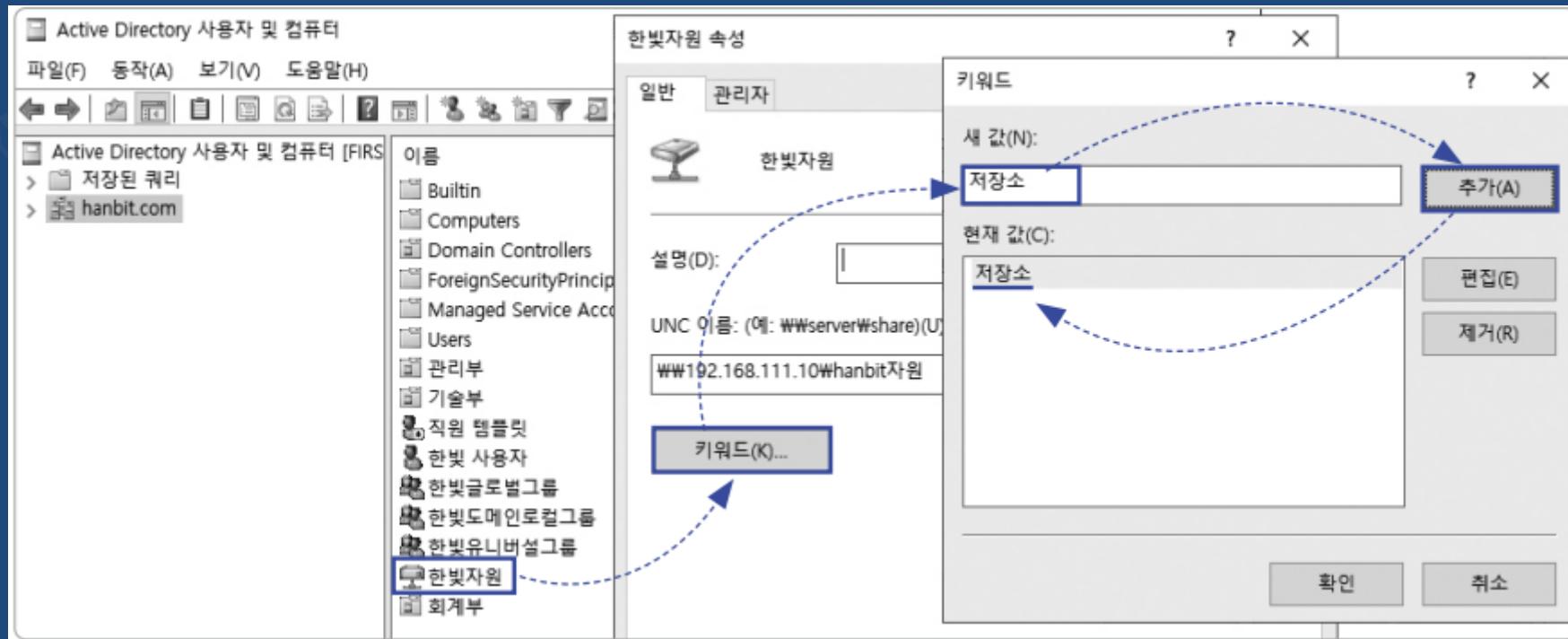
Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요. [FIRST]

7-1) hanbit.com 자원 AD검색 등록

- Active Directory 사용자 및 컴퓨터 → hanbit.com 우클릭 → 새로 만들기/공유 폴더 → 새 개체/공유 폴더 → 키워드
- 새 값: 저장소



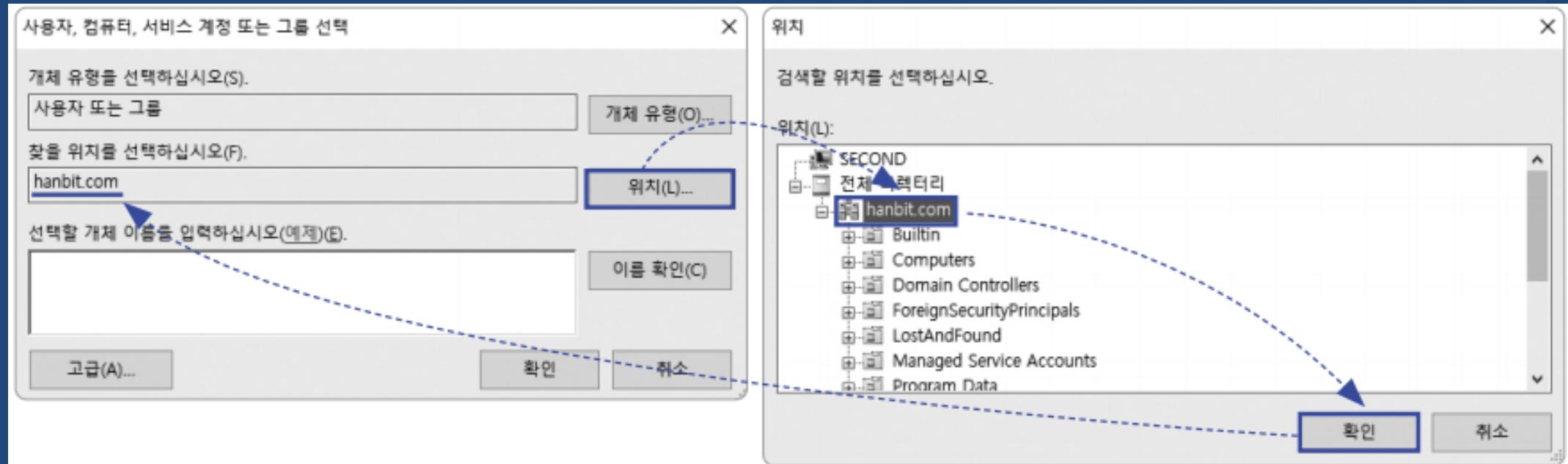
Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요. [SECOND]

8-1) second.hanbit.com 자원 글로벌 그룹 공유

- 'C:\second\자원' 우클릭 → 속성/공유/고급공유/선택한 폴더 공유 → 권한 → Everyone 제거
- 'C:\second\자원' 우클릭 → 속성/공유/고급공유/선택한 폴더 공유 → 권한 → 추가 → 위치 → hanbit.com



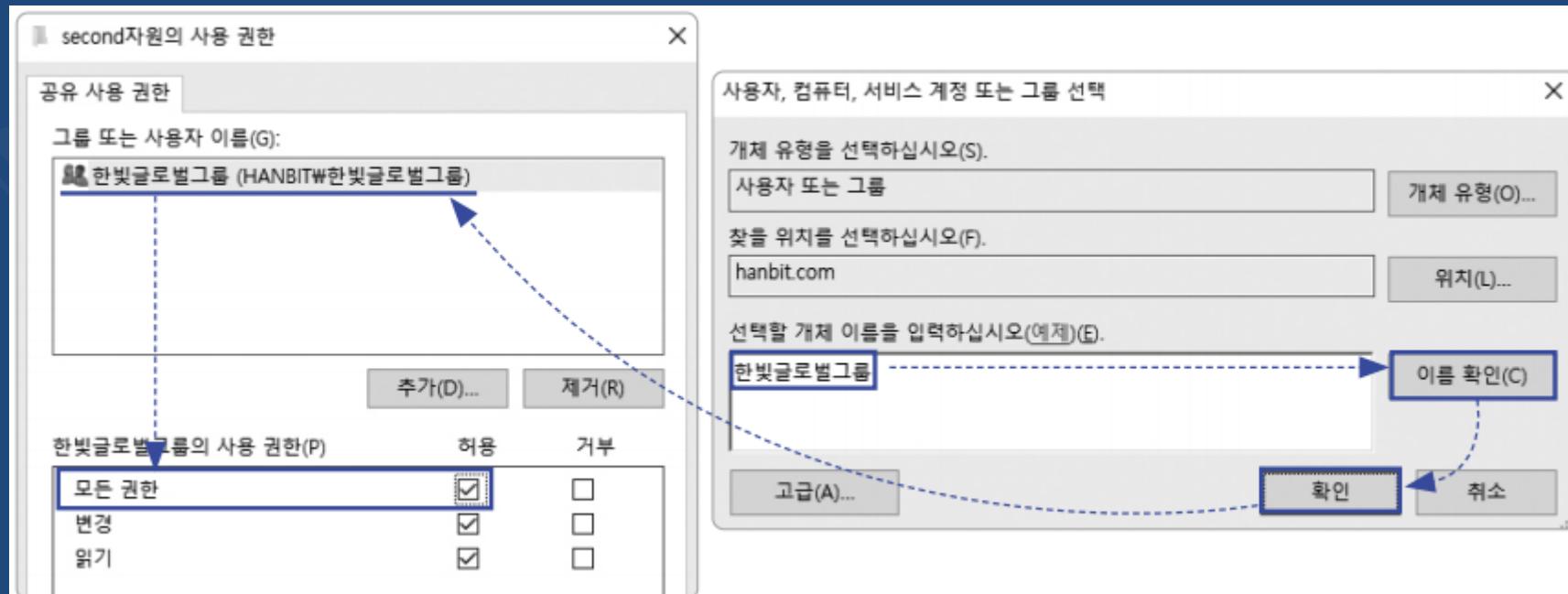
Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요. [SECOND]

8-2) second.hanbit.com 자원 글로벌 그룹 공유

- 'C:\second자원' 우클릭 → 속성/공유/고급공유/선택한 폴더 공유 → 권한 → 추가 → 한빛글로벌그룹 (모든권한)



Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요. [SECOND]

8-1) second.hanbit.com 자원 AD검색 등록

- 이름 : 세컨자원
- 네트워크 경로 : \\192.168.111.20\second자원
- 키워드 : 저장소

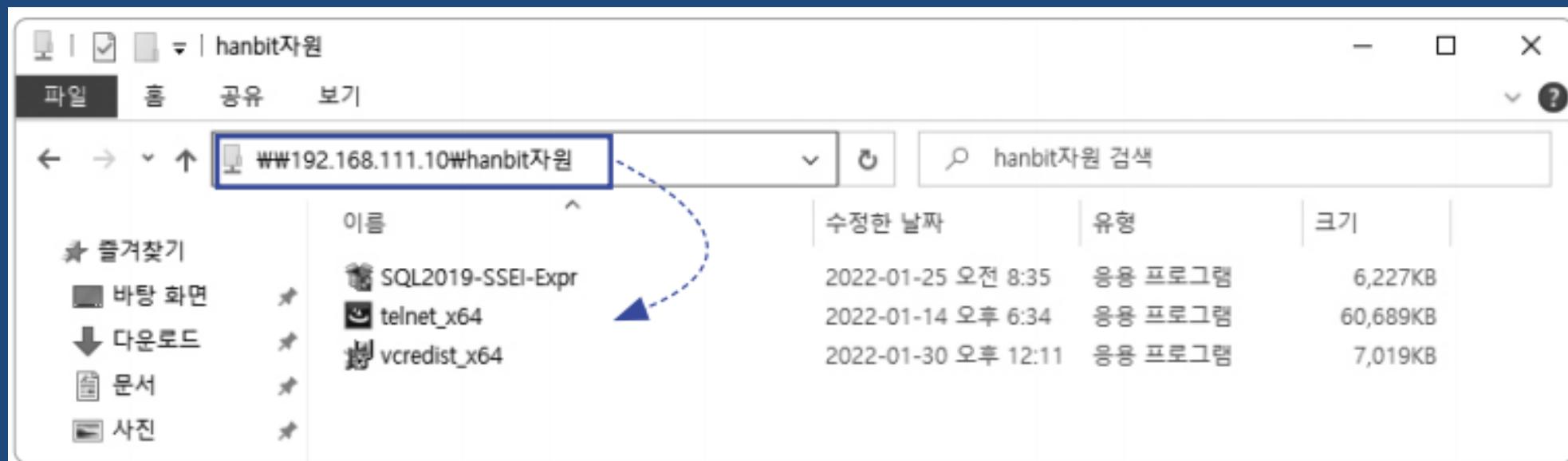
Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요. [WINCLIENT]

9-1) hanbit.com / second.hanbit.com 도메인 자원 사용 확인

- hanbitUser@hanbit.com / VMwaare1!
- 파일탐색기 → \\192.168.111.10\hanbit자원
- 파일탐색기 → \\192.168.111.20\second자원



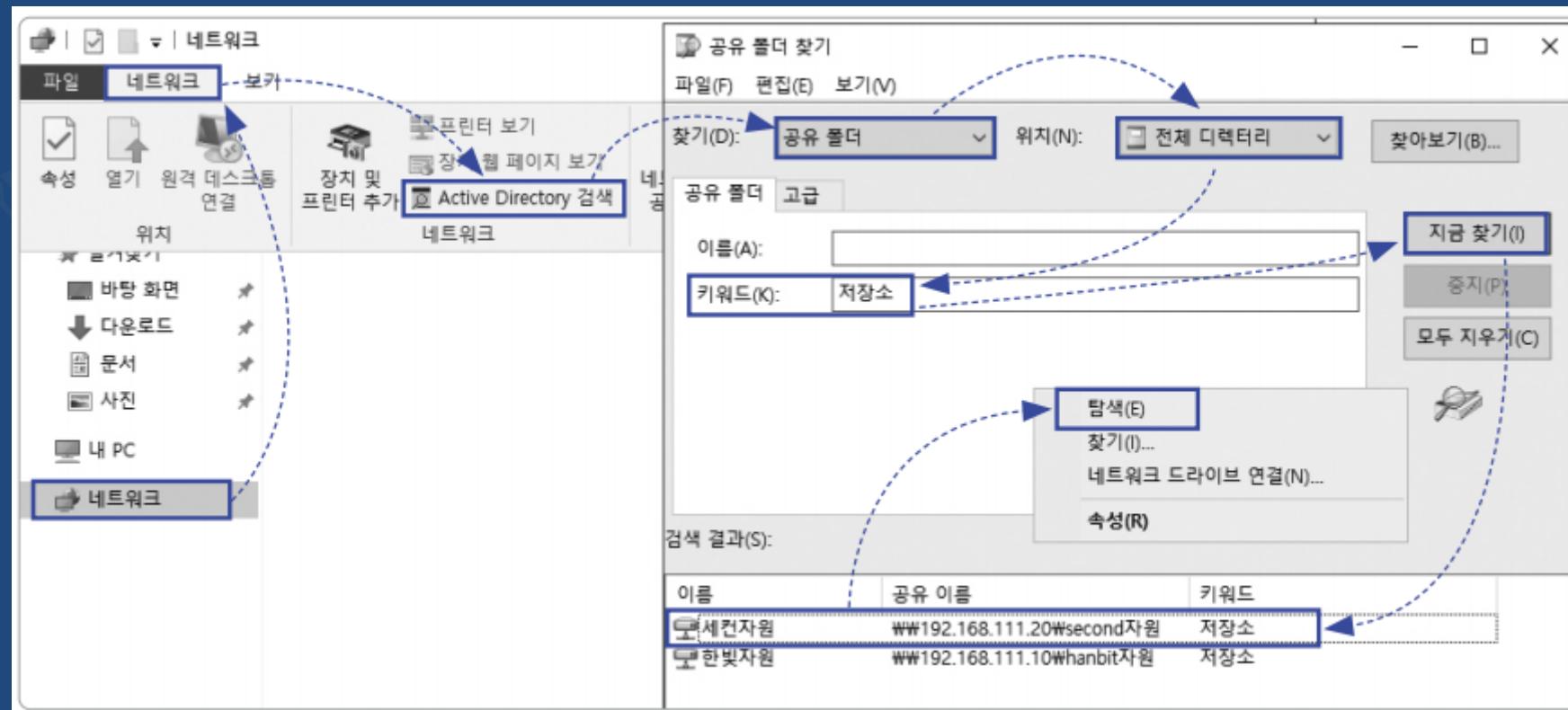
Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요. [WINCLIENT]

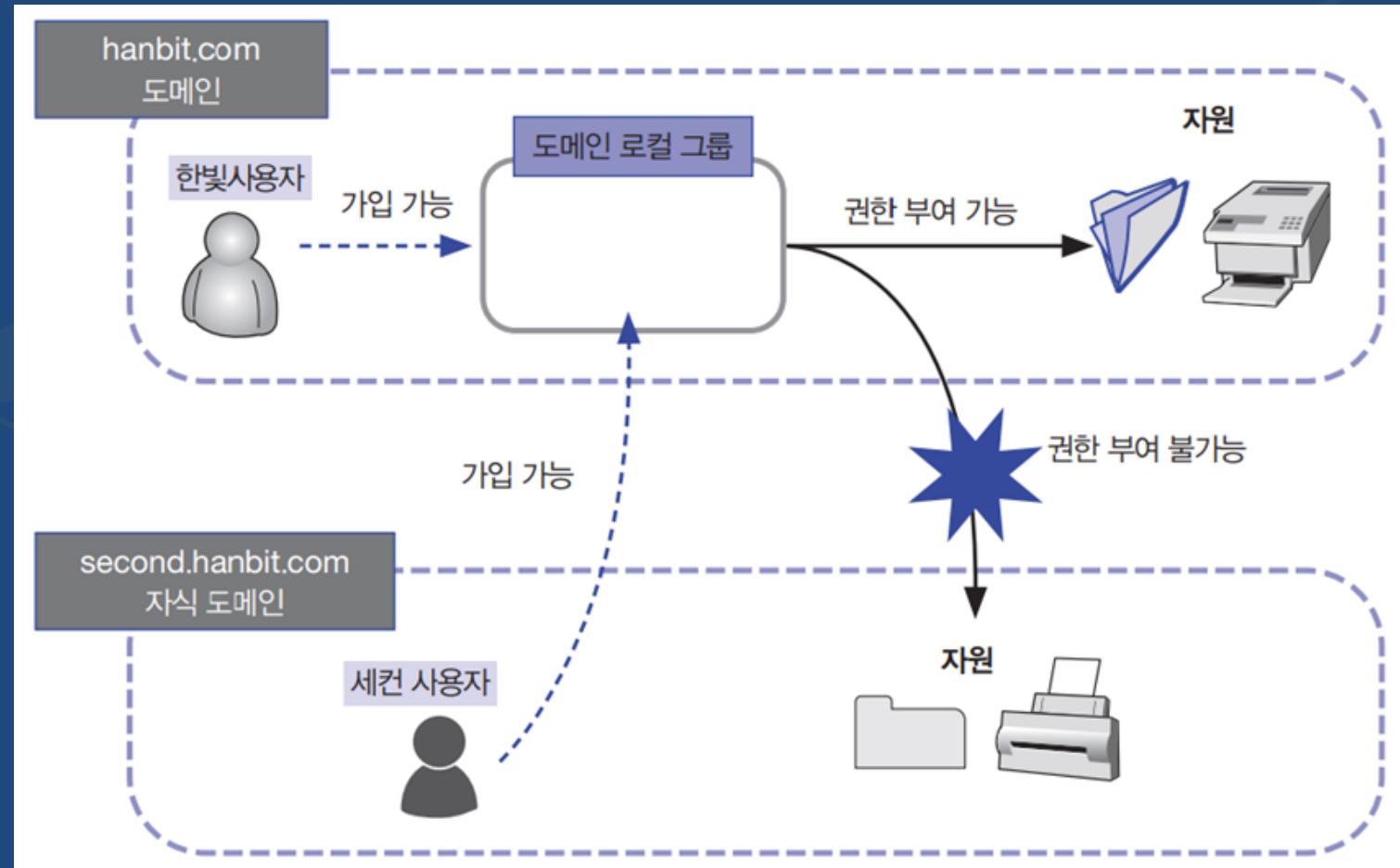
9-2) hanbit.com / second.hanbit.com 도메인 자원 사용 확인

- 파일탐색기 → 네트워크 → Active Directory 검색 → 공유 폴더 찾기 → 공유 폴더/전체/키워드:저장소 → 지금 찾기



Active Directory Domain Service

Q. 그룹을 생성해 권한을 주고 운영 하세요.



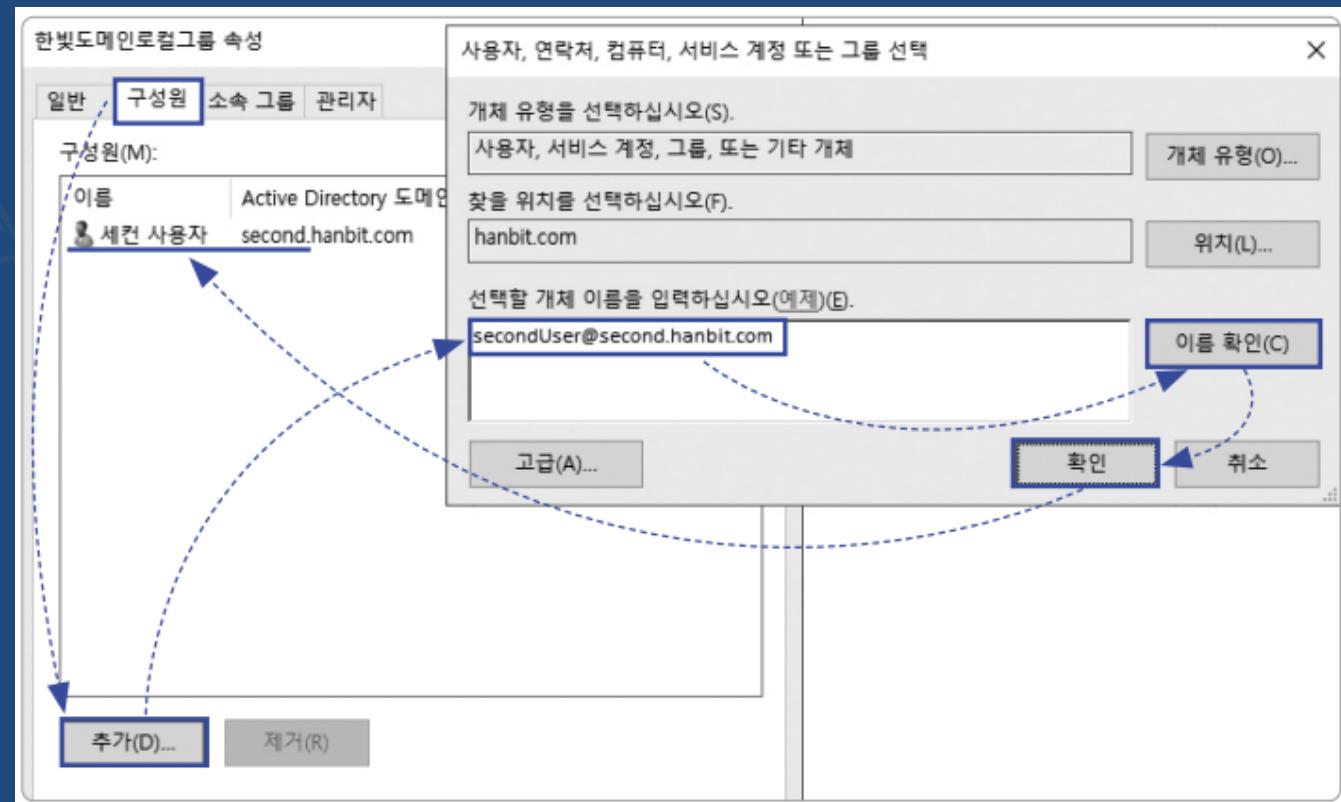
Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요. [FIRST]

1) 도메인 로컬 그룹 가입

- 서버관리자 → Active Directory 사용자 및 컴퓨터 → hanbit.com → 한빛도메인로컬그룹 더블클릭 → 구성원/추가 → 선택할 개체 이름 : secondUser@second.hanbit.com



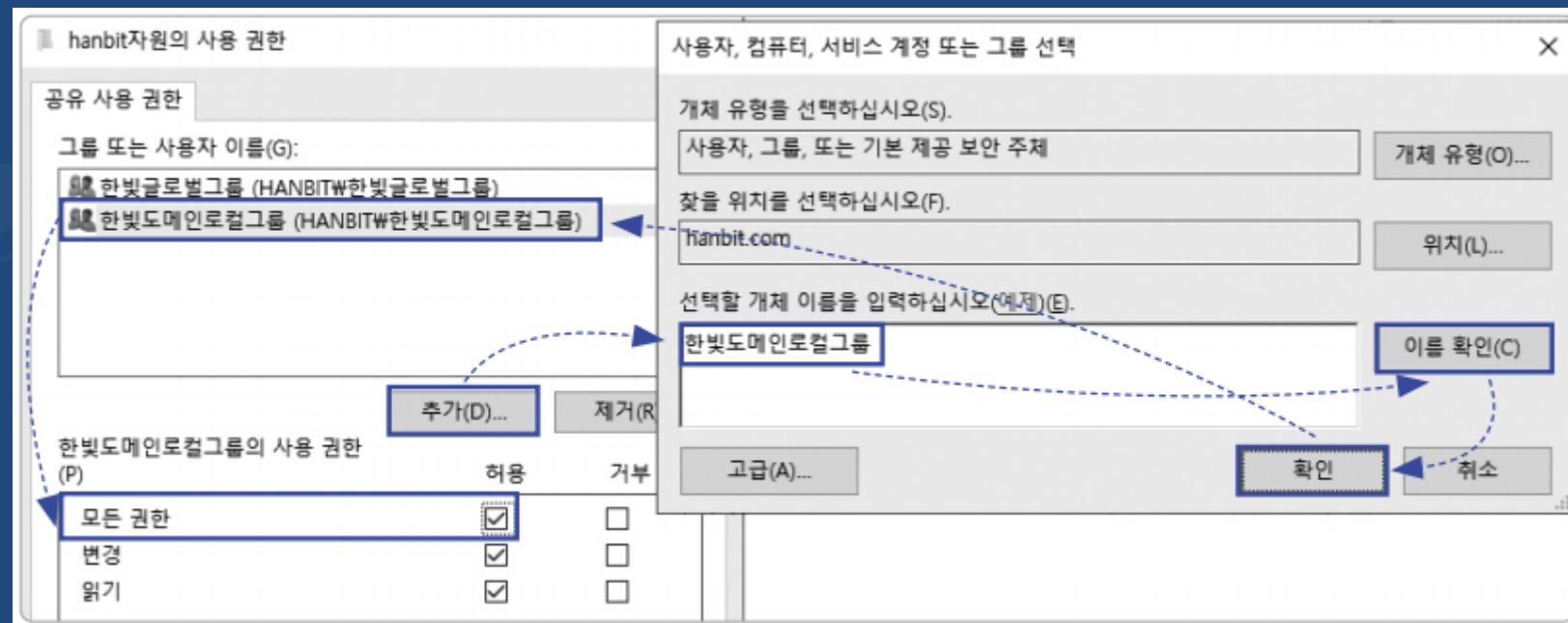
Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요. [FIRST]

2) hanbit.com 자원 도메인 로컬 그룹 공유

- 'C:\hanbit자원' 우클릭 → 속성/공유/고급공유/선택한 폴더 공유 → 권한 → 추가 → 한빛도메인로컬그룹(모든권한)



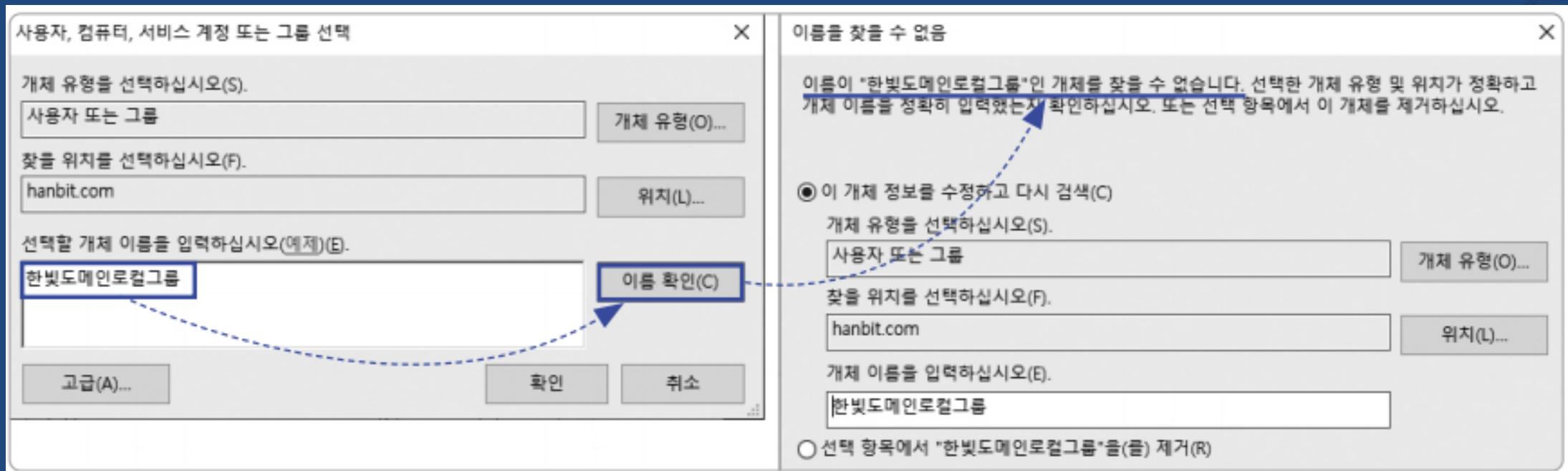
Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요. [SECOND]

2) second.hanbit.com 자원 도메인 로컬 그룹 공유

- 'C:\second자원' 우클릭 → 속성/공유/고급공유/선택한 폴더 공유 → 권한 → 추가 → 사용자, 컴퓨터, 서비스 계정 또는 그룹 선택/위치 → hanbit.com
- 사용자, 컴퓨터, 서비스 계정 또는 그룹 선택 → 한빛도메인로컬그룹 → 이름 확인



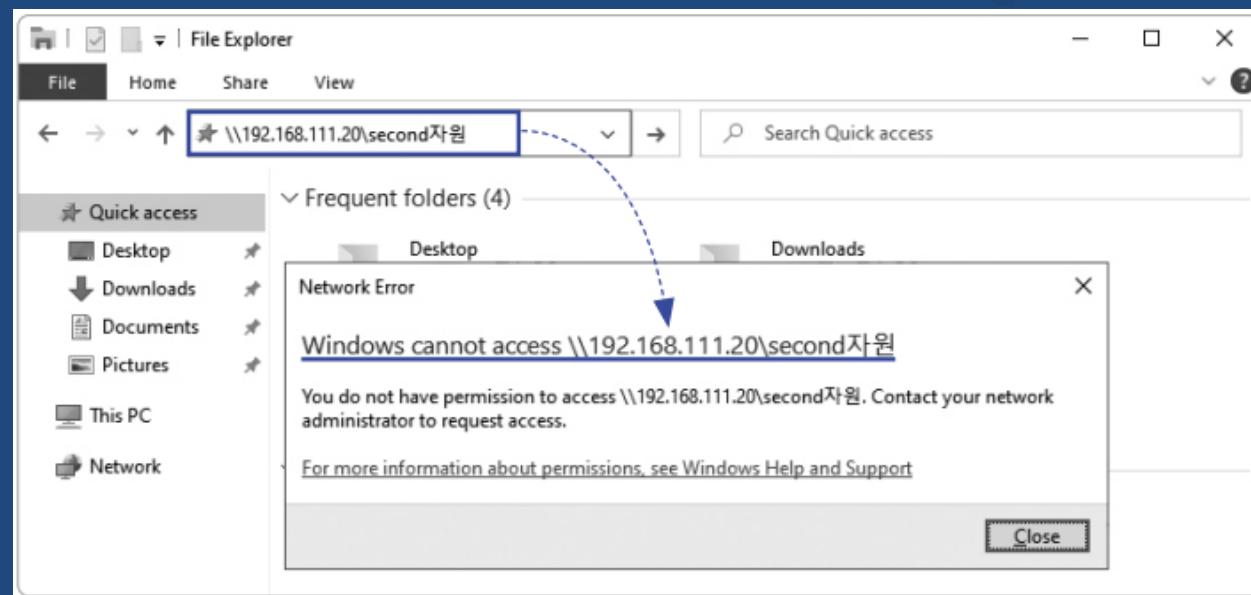
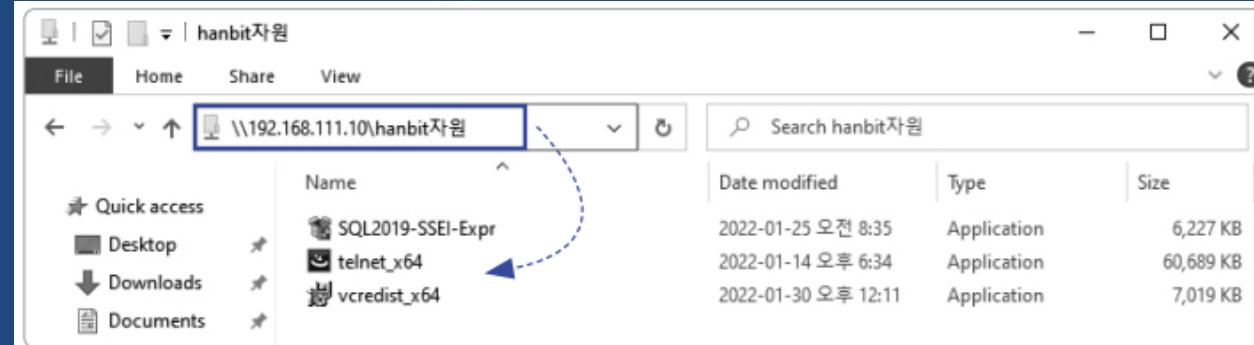
Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요. [WINCLIENT]

3) 도메인 자원 사용 확인

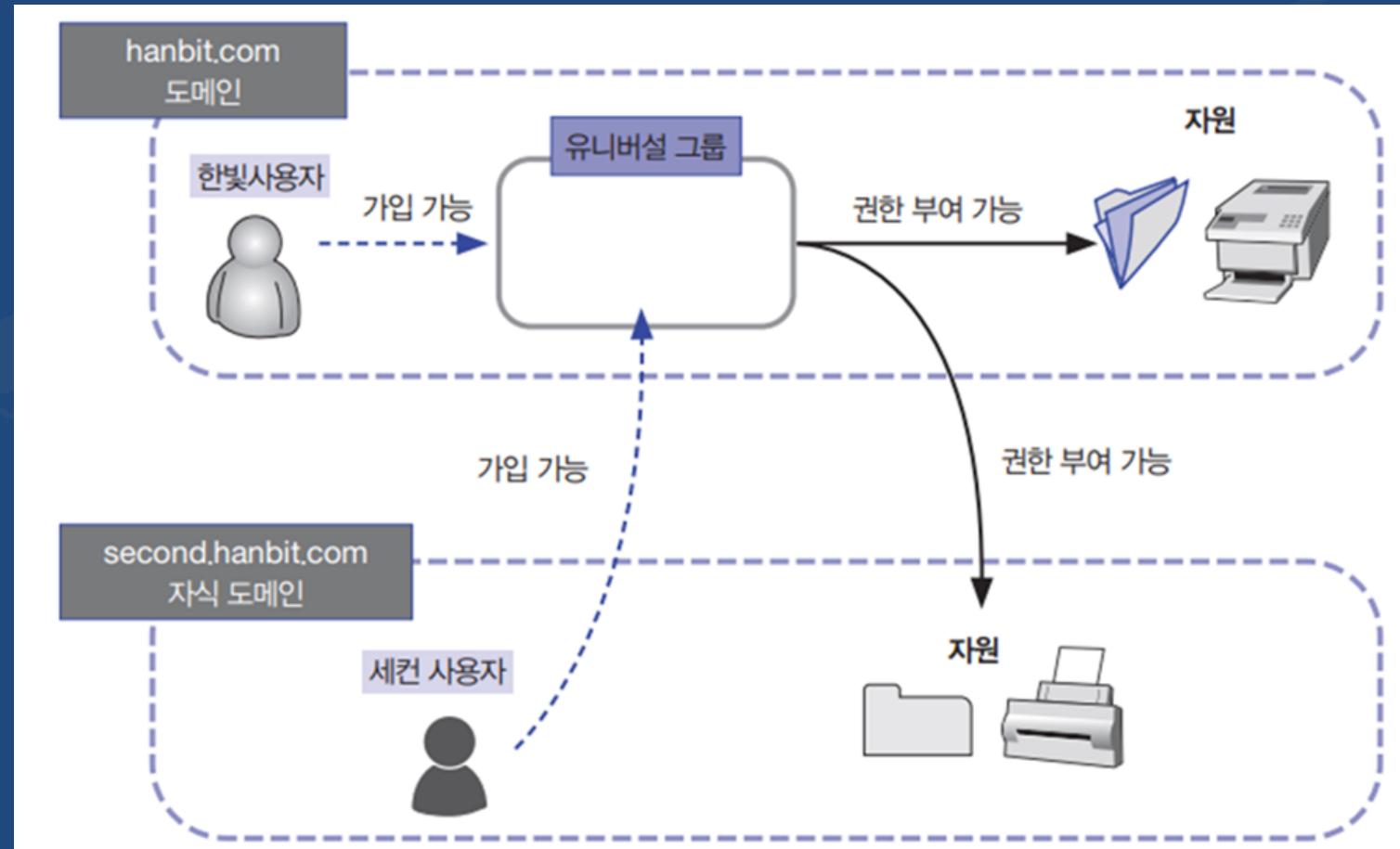
- secondUser@second.hanbit.com / VMware!
- 파일탐색기 → \\192.168.111.10\hanbit자원
- 파일탐색기 → \\192.168.111.20\second자원



Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요.



Active Directory Domain Service



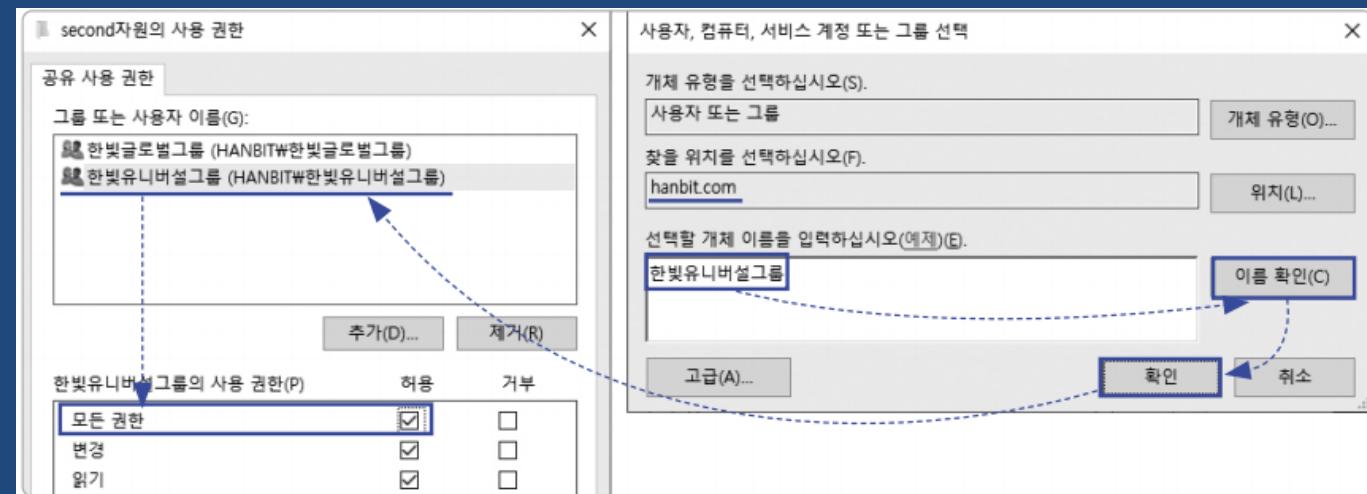
Q. 그룹을 생성해 권한을 주고 운영 하세요. [SECOND]

1) 유니버설 그룹 가입

- 서버관리자 → Active Directory 사용자 및 컴퓨터 → hanbit.com → 한빛유니버설그룹 더블클릭 → 구성원/추가 → 선택할 개체 이름 : secondUser@second.hanbit.com

2) second.hanbit.com 자원 도메인 로컬 그룹 공유

- 'C:\second자원' 우클릭 → 속성/공유/고급공유/선택한 폴더 공유 → 권한 → 추가 → 사용자,컴퓨터,서비스 계정 또는 그룹 선택/위치 → hanbit.com
- 사용자,컴퓨터,서비스 계정 또는 그룹 선택 → 한빛유니버설그룹 → 이름 확인 → 모든 권한/허용



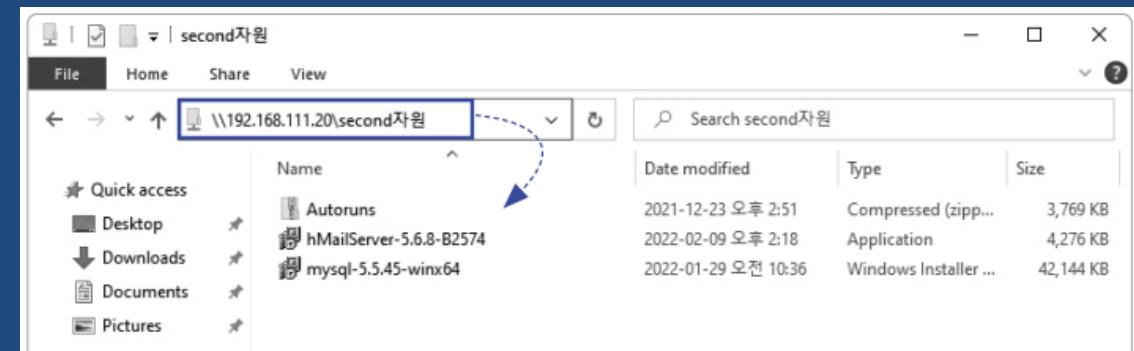
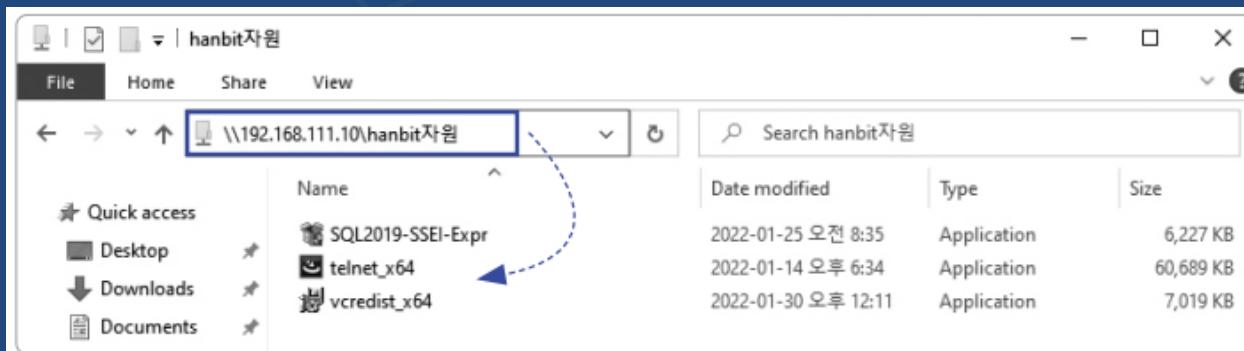
Active Directory Domain Service



Q. 그룹을 생성해 권한을 주고 운영 하세요. [WINCLIENT]

3) 도메인 자원 사용 확인

- secondUser@second.hanbit.com / VMware!
- 파일탐색기 → \\192.168.111.10\hanbit자원
- 파일탐색기 → \\192.168.111.20\second자원

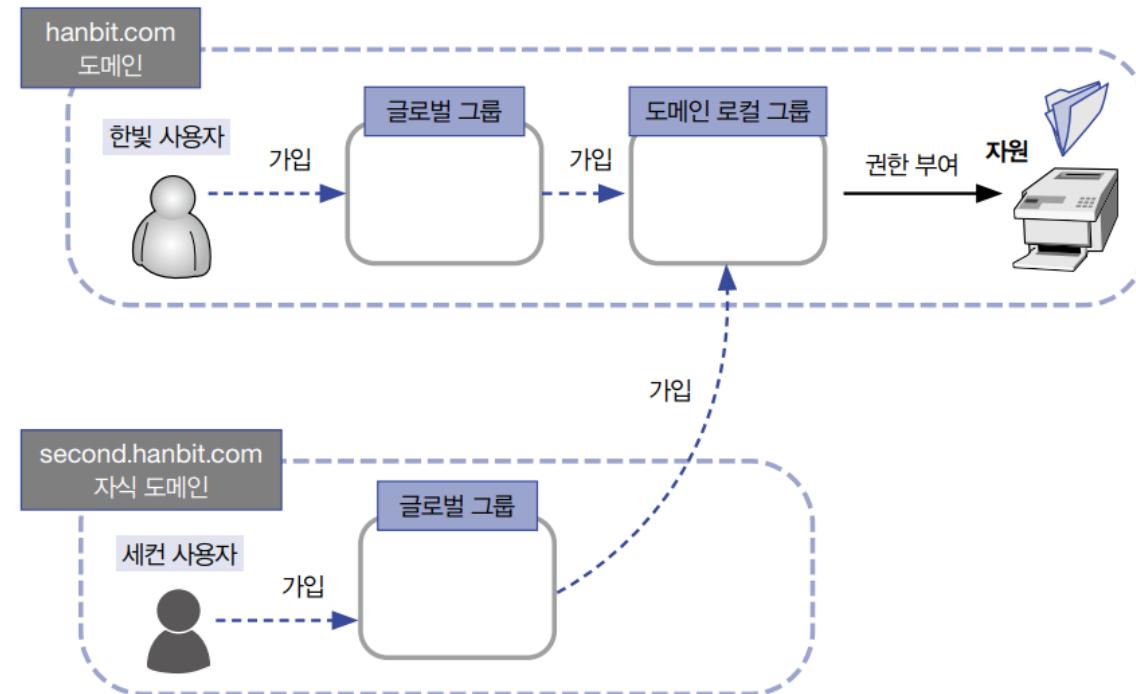


AD 그룹 & 권한 권장

- Microsoft사는 Active Directory를 설계할 때 ‘AGDLP’ 순서 권장
- 관리의 일관성, 명확한 권한 구조, 확장성 및 유연성 측면에서 유리
 - 자원을 직접 컨트롤 하는 방법 보다는 그룹의 권한 및 계층에 의한 종속성을 이용한 관리가 효율적

Account (사용자 계정) → Global group (글로벌 그룹) → Domain Local group (도메인 로컬 그룹) → Permission (권한)

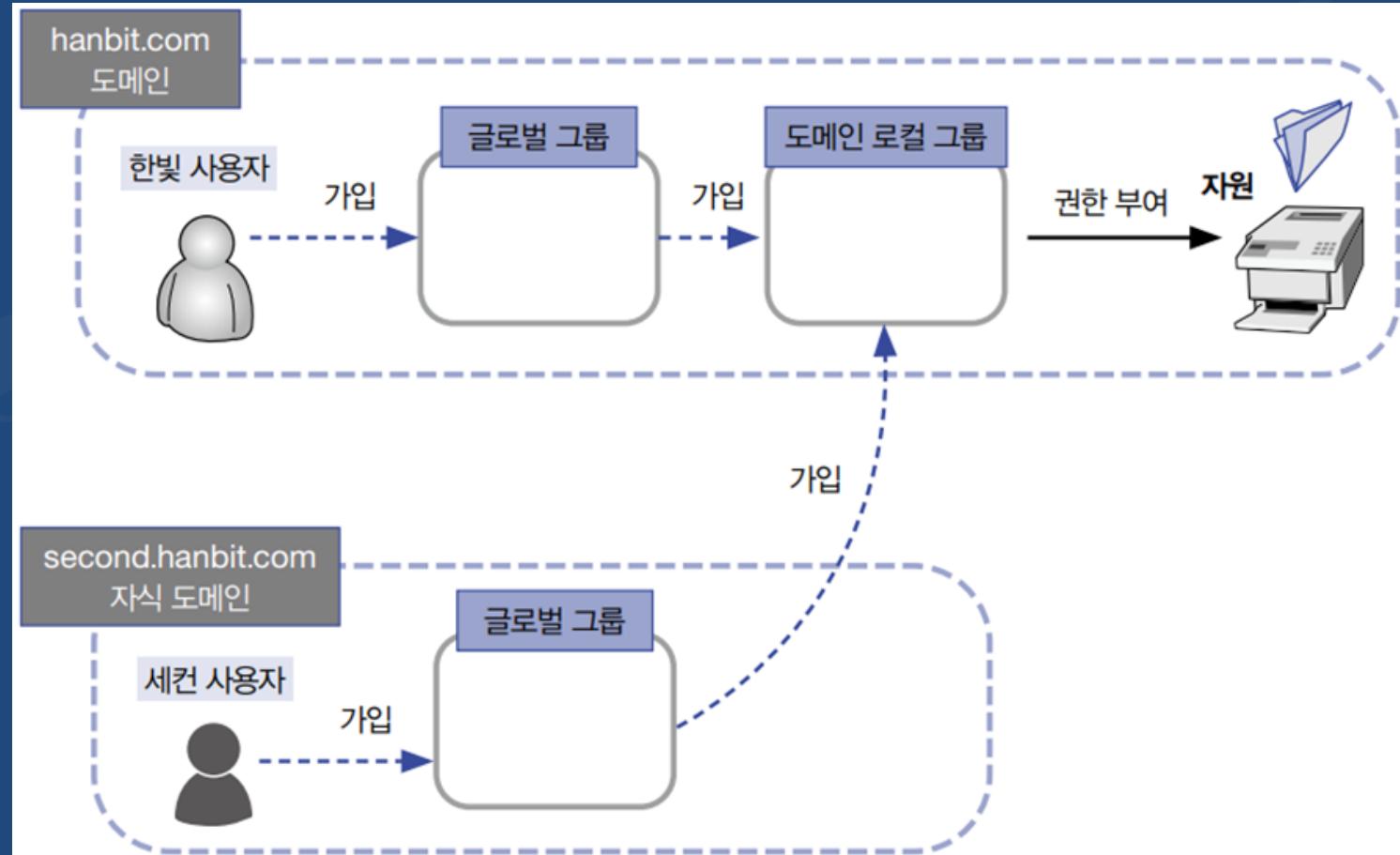
AD 그룹 & 권한 권장



- 각 도메인 사용자는 자신의 도메인에 생성된 **글로벌 그룹**에 가입
- 이 **글로벌 그룹**은 도메인 로컬 그룹에 가입
- 도메인 로컬 그룹에 자원에 대한 권한 부여
 - hanbit.com 도메인 사용자, second.hanbit.com 도메인 사용자 모두 자원에 접근 가능

Active Directory Domain Service

Q. AGDLP를 구현해 그룹과 자원을 운영 하세요.



Active Directory Domain Service



Q. AGDLP를 구현해 그룹과 자원을 운영 하세요. [SECOND]

1) 글로벌 그룹 생성

- 서버관리자 → Active Directory 사용자 및 컴퓨터 → second.hanbit.com 우클릭 → 새로 만들기/그룹
- 그룹 이름 : 세컨글로벌그룹
- 그룹 범위 : 글로벌



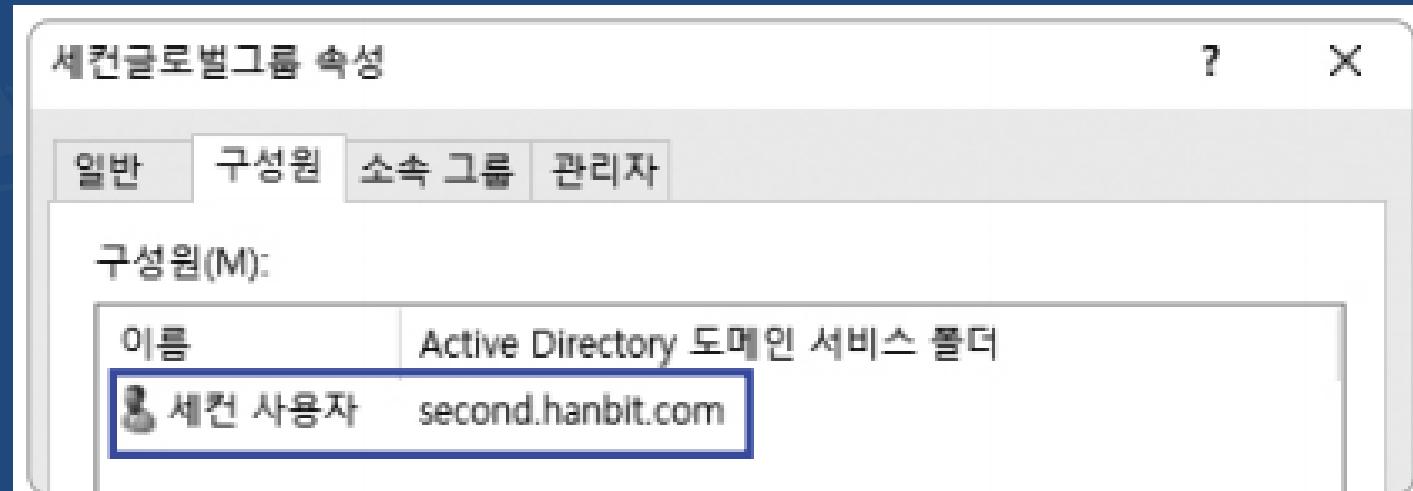
Active Directory Domain Service



Q. AGDLP를 구현해 그룹과 자원을 운영 하세요. [SECOND]

2) 구성원 추가

– secondUser@second.hanbit.com



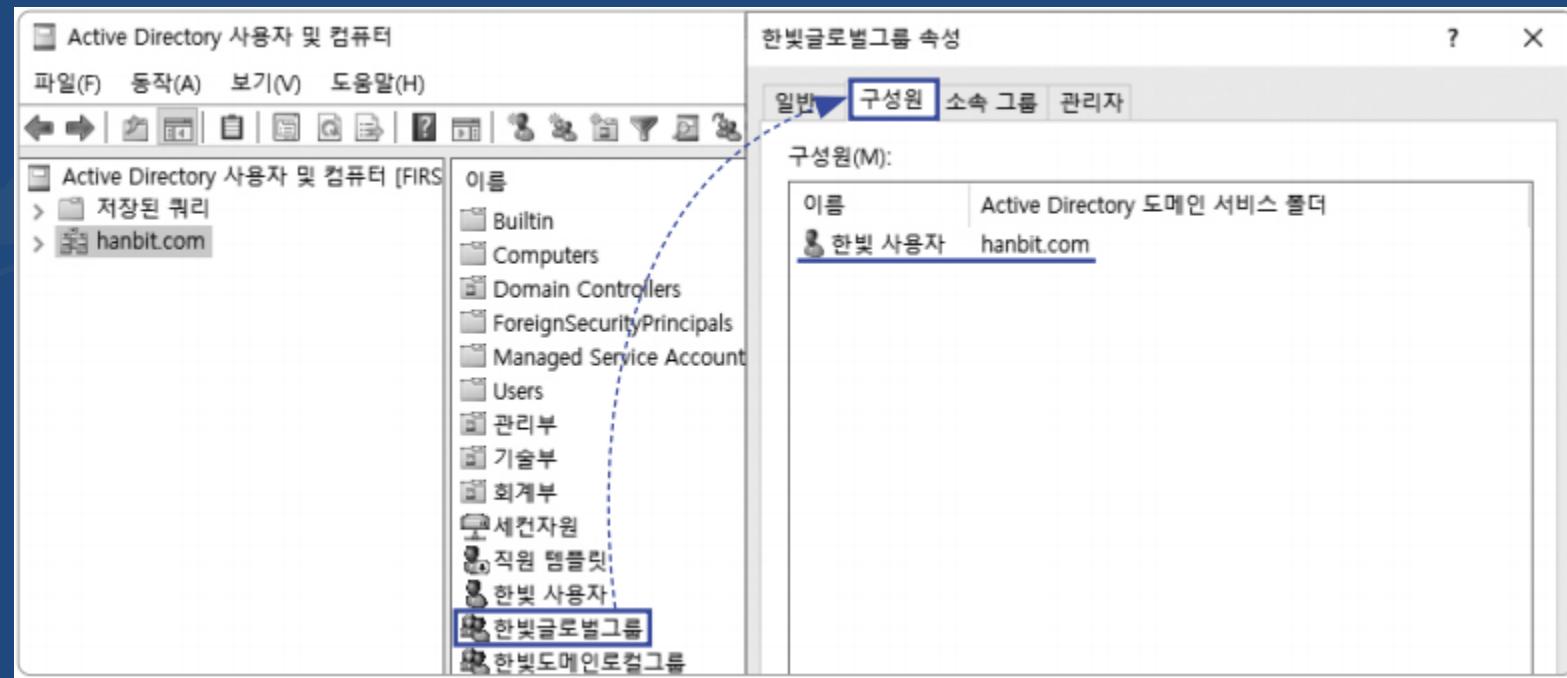
Active Directory Domain Service



Q. AGDLP를 구현해 그룹과 자원을 운영 하세요. [FIRST]

3) 글로벌그룹 구성원 확인

– hanbitUser@hanbit.com



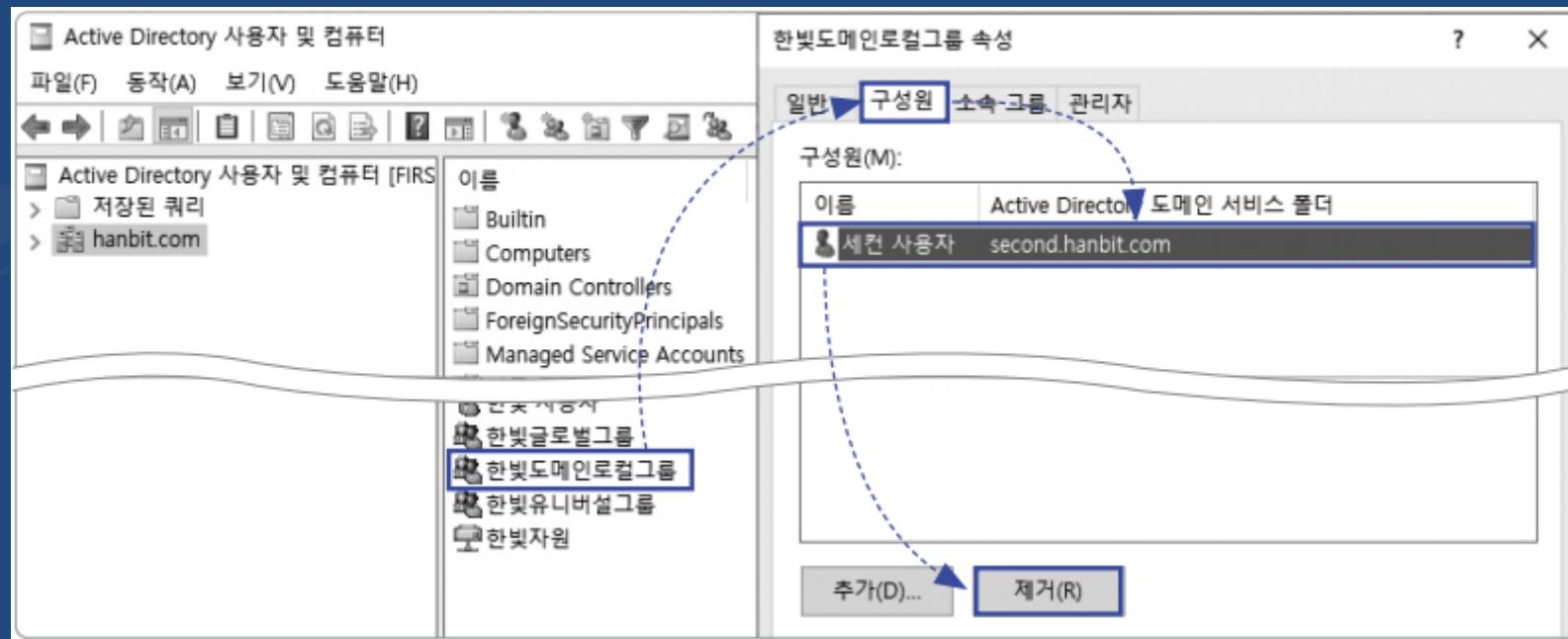
Active Directory Domain Service



Q. AGDLP를 구현해 그룹과 자원을 운영 하세요. [FIRST]

3-1) 도메인로컬그룹 구성

- 세컨 사용자 / second.hanbit.com → 제거



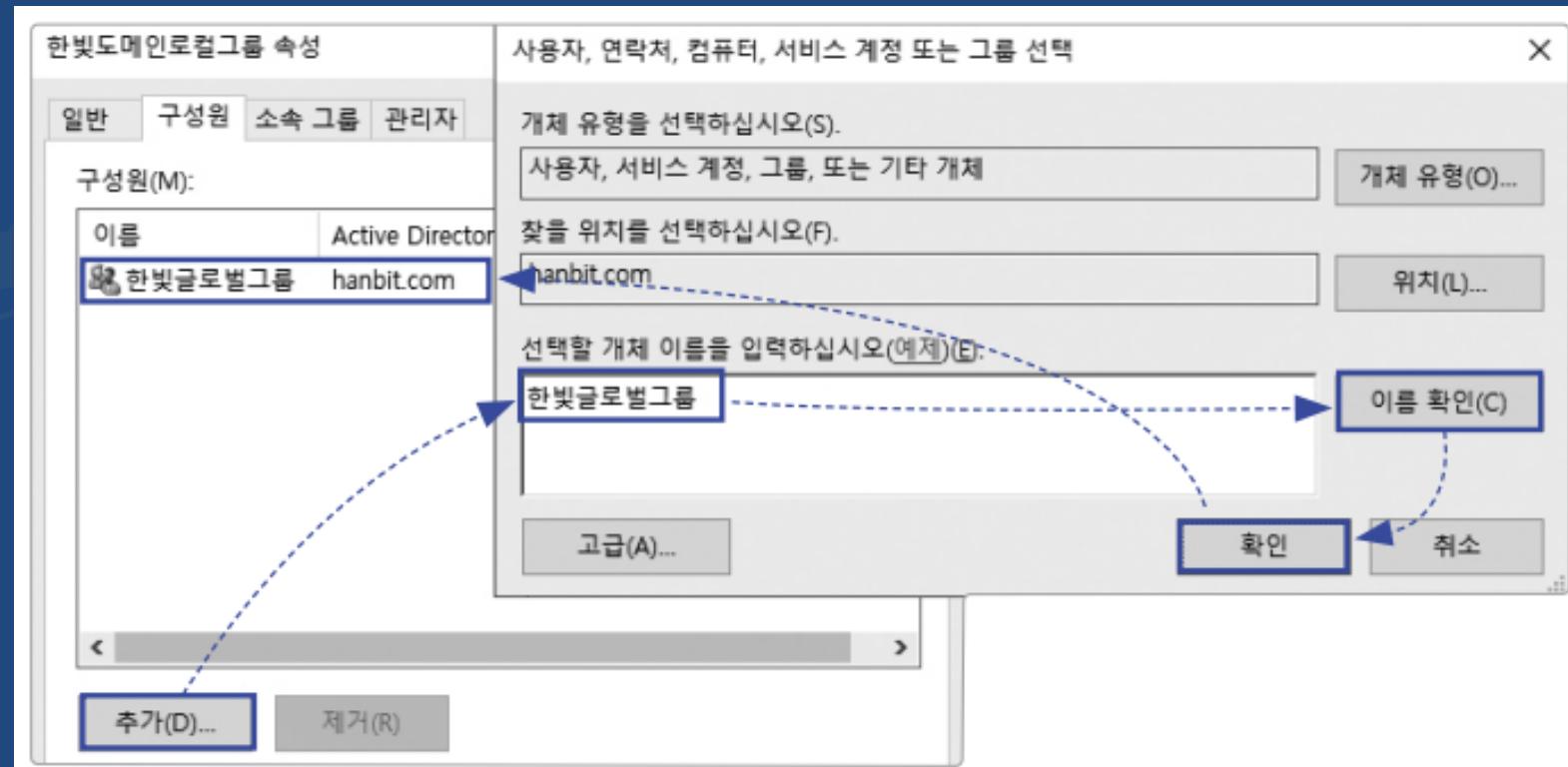
Active Directory Domain Service



Q. AGDLP를 구현해 그룹과 자원을 운영 하세요. [FIRST]

3-2) 도메인로컬그룹 구성

- 한빛글로벌그룹 → 추가



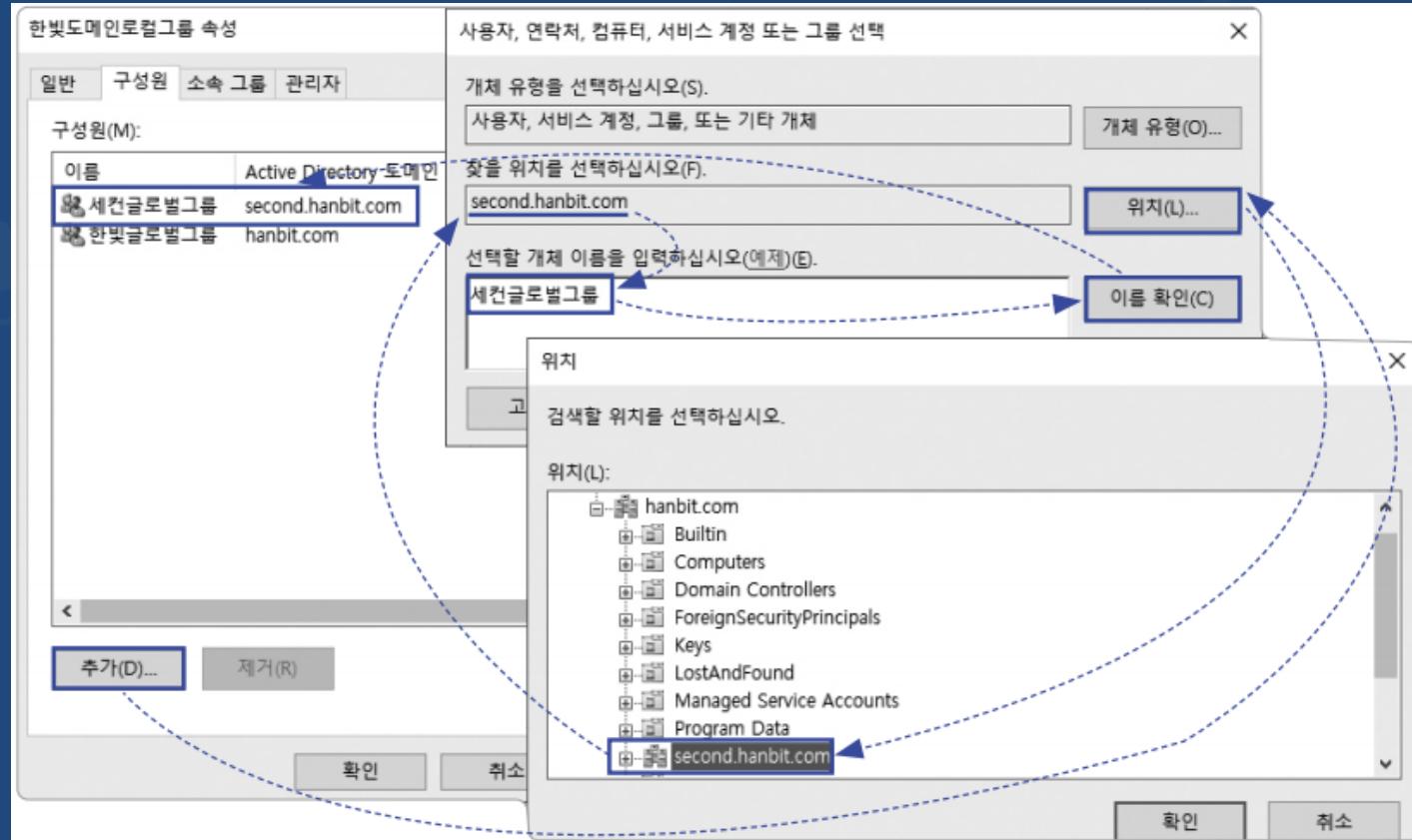
Active Directory Domain Service



Q. AGDLP를 구현해 그룹과 자원을 운영 하세요. [FIRST]

3-3) 도메인로컬그룹 구성

- 세컨글로벌그룹 → 추가



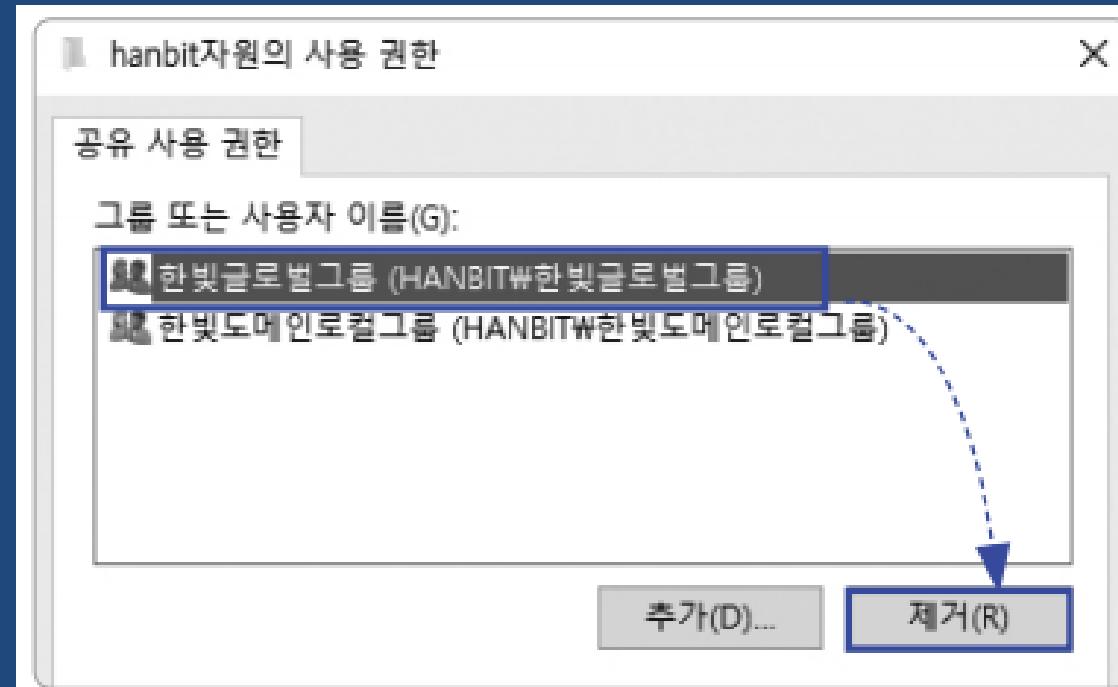
Active Directory Domain Service



Q. AGDLP를 구현해 그룹과 자원을 운영 하세요. [FIRST]

4) 도메인 자원 권한 부여

– ‘C:\hanbit자원’ → 한빛글로벌그룹 권한 제거



Active Directory Domain Service



Q. AGDLP를 구현해 그룹과 자원을 운영 하세요. [WINCLIENT]

3) 도메인 자원 사용 확인

- hanbitUser@hanbit.com / VMware1!
- secondUser@second.hanbit.com / VMware1!
- 파일탐색기 → \\192.168.111.10\hanbit자원

Active Directory Domain Service



Q. AGDLP를 구현해 second자원을 도메인에 공유 하세요.

- 세컨로컬도메인그룹 → 'C:\second자원' (모든 권한)

- 한빛글로벌그룹
- 세컨글로벌그룹

- 확인 [WINCLIENT]

- hanbitUser@hanbit.com / VMware1!
- secondUser@second.hanbit.com / VMware1!
- 파일탐색기 → \\192.168.111.20\hanbit자원

AD 계정 / OU / 그룹 Summary

- 그룹은 작업을 하는 계정을 관리하거나 권한을 부여하기 위한 단위
- OU는 사용자, 그룹, 컴퓨터 등을 배치할 수 있는 컨테이너 (= 폴더, 부서)
- OU는 그룹 정책을 적용하기 위한 최소 단위로 사용
 - OU에는 권한을 줄 수 없음
- 사용자 계정은 하나의 OU에만 가입 가능
- 사용자 계정은 여러 개의 그룹에 가입 가능

AD 그룹 정책 개념

- AD 통해 도메인 안의 많은 컴퓨터나 사용자에게 다양한 사용 제한 구성 가능
 - 특정 사용자에게만 동작하는 프로그램 지정
 - 시작 메뉴 사용 옵션
 - USB 및 CD/DVD 사용 제한
 - 잘못된 사용자의 시스템 구성 변경이나 네트워크 바이러스 침투 등의 사고 예방
- 그룹 정책을 통해 각 컴퓨터 및 사용자에 대한 일괄된 관리 가능
- 그룹 정책 개체 (Group Policy Object , GPO)
 - 그룹 정책을 묶은 개체
 - GOP는 도메인 단위에 저장
 - 글로벌 카탈로그에 해당 정보가 저장
 - GPO를 적용하기 위한 가장 작은 단위 : OU
 - 종류
 - 로컬 GPO : 4순위
 - 사이트 GPO : 3순위
 - 도메인 GPO : 2순위
 - OU GPO : 1순위

AD 그룹 정책 개념

- 그룹 정책은 상속 가능
 - 부모 컨테이너 → 자식 컨테이너
 - 자식 컨테이너는 필요시 상속 내용 재정의, 상속 차단 가능
 - 부모 컨테이너는 차단 하지 못하도록 강제 상속 가능

Ex) hanbit.com 도메인 → 기술부 OU → 기술1팀/2팀 OU 상속

hanbit.com

- 기술부 OU
 - 기술1팀 OU
 - 기술2팀 OU

AD 그룹 정책의 가능한 작업

- 보안 설정
 - 보안 강화를 위한 사용자의 암호 및 계정 잠금 등에 대해 도메인의 모든 사용자에게 강제로 적용
- 스크립트 설정
 - 사용자 로그온/로그아웃 시 또는 컴퓨터의 부팅과 종료 시에 자동으로 실행될 작업을 스크립트에 지정
- 폴더 리디렉션
 - 사용자가 도메인 내의 어느 컴퓨터에서 로그온하더라도 자신의 문서 등에 대한 폴더를 동일한 환경으로 제공
- 소프트웨어 설정
 - 사용자가 사용할 소프트웨어에 대해 설치, 삭제, 업데이트 제어