Active Directory의 개념 및 효율과 필요성

㈜엑셈 컨설팅본부/SQL Server팀 양 동환

개요

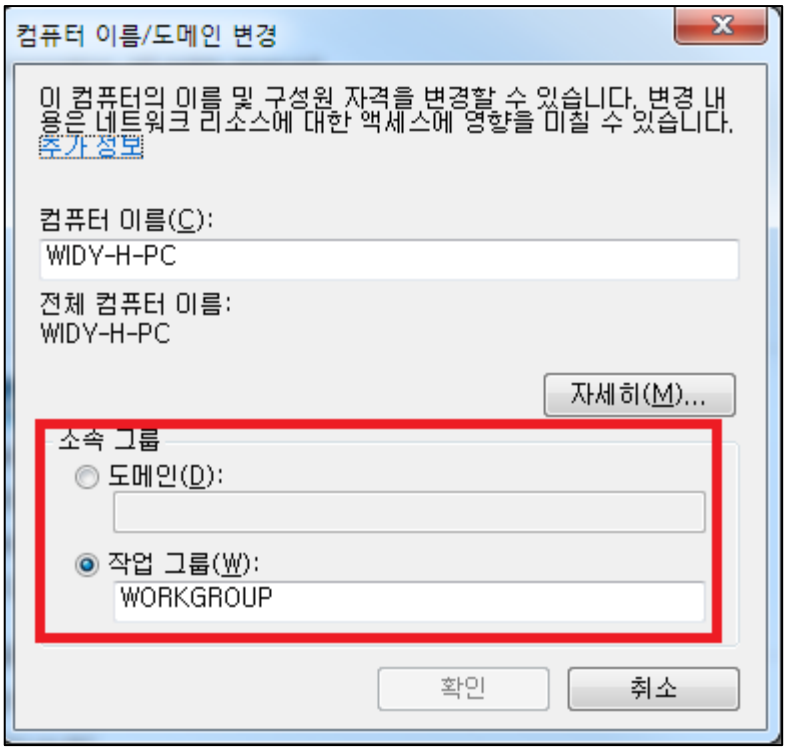
MicroSoft(MS)에서 Windows Server 2000 을 출시하면서 가장 크게 내세운 기능이 있다면 그건 바로 Active Directory(AD)일 것이다.

점점 더 다양하고 복잡해지는 IT 인프라에 체계성을 갖춰 관리, 보안, 상호 운영성의 이익을 갖도록 하는 것이 AD 가 도입 된 가장 큰 이유이고 MS 에서 Windows Server 새로운 버전이 나올 때마다 가장 중점을 둬서 발전시킨 것 또한 AD 이다. 그렇다면 이 문서를 통해 AD 에 대해 좀 더 자세히 살펴보고 기업에서 AD 가 얼마나 효율적으로 사용가능하고 왜 필요한지 알아보도록 하자.

AD란 무엇인가

Active Directory 에 대해 설명하기 앞서 우선 MicroSoft 의 네트워크 환경에 대해 간단히 설명하겠다. MS 의 OS 인 Windows 는 크게 두 가지 모델이 있다. Windows 9X 계열, XP, 7,8 등과 같은 가정용이 있고, Windows NT 계열인 Server 2000, 2003, 2008, 2012 등과 같은 기업용이 있다. 이 두 가지의 OS 모델은 개발환경 및 코드가 다르며 시장에서의 쓰임새도 다르다. 기업용이라고 하는 NT 계열은 가정용과 달리 개인 혼자서 사용하기 위한 것이 아니다. 기본적으로 네트워킹 이라는 요소가 포함되어 기업환경과 같이 많은 사람들이 정보 및 자원을 서로 공유할 수 있어야 한다. 이렇듯 네트워크에서 컴퓨터가 자원을 공유하는 용도로 사용된다면 역시 보안(Security)부분은 빼놓을 수가 없다. 적절한 사용자에게만 서비스를 제공해야 하고 그렇지 못한 사용자는 접근을 통제해야 한다. NT 는 이러한 기능을 제공하기 위해 자신의 자원에 접근하게 할 사용자를 생성하고 이것을 DB 화 시켜 리스트를 유지한다. 이 리스트를 Directory 라고 부르고 이 Directory 를 저장하는 공간을 Directory Database 라고 부른다. 이 Directory Database 에 저장되는 개체(Object)을 가리켜 계정(Account)라고 부른다. 예를 들면 사용자 계정, 컴퓨

터 계정 등이 있을 수 있다. 결국 한 컴퓨터에서 서버에 있는 파일에 접근을 하고자 한다면, 그 컴퓨터를 사용하는 사용자계정이 서버의 Directory Database 에 등록이 되어 있어야 접근이 가능하다는 것을 의미한다. 이러한 Directory 를 효율적으로 관리하기 위해 MS 에서는 네트워크 관리모델을 두 가지 제공한다.



[그림1]내 컴퓨터 – 속성 – 컴퓨터 이름/도메인 변경 창

내 컴퓨터 속성에 들어가서 위 그림과 같은 창을 본 적이 있을 것이다. 그림과 같이 MS 에서는 WORKGROUP 과 DOMAIN 이라는 모델을 제공한다. 두 모델의 가장 큰 차이점은 앞서 말한 Directory Database 의 위치라고 할 수 있다. 그렇다면 두 모델의 차이점을 표를 통해 알아보도록 하겠다.

	WORKGROUP	DOMAIN
Directory Database 위치	` 각각의 컴퓨터 내	` 하나 이상의 마스터 서버(DC) 내
장점	` 작은 규모의 네트워크 환경이라면 전체 서버를 관리할 강력한 시스템이 필요 없고 따로 관리자가 없이 각각 자신들의 시스템을 스스로 관리하는 게 방침인 게 회사의 방침인 곳에서는 적절하다.	` 회사 내 모든 컴퓨터 및 사용자 계정을 서버마다 생성하지 않고 하나의 마스터 서버(DC)에서만 생성하여 중앙 관리 할 수 있다.
단점	` 한 사용자가 자원을 가진 서버마다 별도의 사용자 계정을 가지고 있어야 한다. ` 하나의 사용자를 위해서 서버마다 계정을 만들어야 한다. ` 중앙집중적인 관리의 어려움	` 전체 Directory Database 를 관리할 강력한 마스터 서버가 있어야 한다. ` 굳이 중앙관리를 할 필요가 없을 정도의 소규모 네트워크 환경일 경우 오히려 불편할 수 있다.

[표1]MS 네트워크 모델 비교

이 중 AD 는 Domain 모델을 사용하는 기능이다. 이제 MS 의 네트워크모델을 알았으니 AD 에 대해 설명하겠다.

AD 는 MS 에서 개발한 Windows 환경에서 사용하기 위한 LDAP(LightWeight Directory Access Protocol) 디렉터리 서비스(Directory Service)이다. 디렉터리 서비스라는 용어자체가 조금 생소할 수 있는데 사전적 의미로는 다음과 같다.

> 디렉터리 서비스 – 네트워크 내에 분산되어 있는 디렉터리를 일원적으로 관리하여, 디렉터리에 수용되어 있는 정보의 검색, 변경, 추가, 삭제 등 디렉터리 사용자나 사용자 프로그램이 요구하는 서비스를 제공하는 기능 단위

쉽게 말해 네트워크 내에 여러 디렉터리(사용자에 관한 데이터, 프린터, 서버, 데이터베이스, 그룹, 컴퓨터, 보안 정책등과 같은 Object)들을 모아 중앙에서 관리할 수 있고 동시에 여러 사용자들이 디렉터리에 접근하여 사용할 수 있게 서비스를 제공해 주는 것을 말한다. 이런 디렉터리 서비스가 하는 일은 다음과 같다.

- 조직이나 회사의 확장에 따라 같이 확장할 수 있는 정보 소스의 역할
- 관리자가 한 컴퓨터에서 전체 네트워크의 정보를 입력하고 관리할 수 있는 기능
- 외부에서 접근하는 허가 받지 않은 사용자로부터 정보를 안전하게 보관하기 위해 관리자가 정의하는 보안 강화
- 네트워크의 많은 컴퓨터 간에 디렉터리 분산
- 더 많은 사용자들이 사용할 수 있고, 에러 발생을 줄이기 위해 복제 사용
- 많은 수의 개체를 저장할 수 있도록 여러 개의 저장소로 디렉터리를 분할

디렉터리 서비스는 AD 이외에도 많이 있지만 AD 는 위와 같은 디렉터리 서비스의 기본 기능에 충실할 뿐만 아니라 그룹 정책(Group Policy)와 개발 인증에 대해 뛰어나 큰 기업의 네트워크 환경을 관리할 수 있다.

AD의 기본기능

확장가능 Directory(Extensible Directory)

AD 가 적게는 수십에서 많게는 수만 개 수준의 Object 를 관리 할 수 있는 것은 기본적으로 AD 가 섹션을 나누어 관리될 수 있도록 하는 파티션 개념을 도입했기 때문이다. 그에 따라 기업의 확장에 따라 얼마든지 AD 영역도 확장될 수 있다.

스키마(Schema) 사용

Directory Service 를 하기 위해선 각 Object 들을 구분할 수 있는 일종의 Rule 이 필요하다. AD 는 스키마를 이용하여 각 Object 들을 구분하고 관리한다.

DNS 사용

AD 는 Internet Name Space 개념인 DNS 를 도입하여 사용한다. 이는 숫자로 이루어진 IP 주소를 사람이 쉽게 기억하고 인지할 수 있게 이름으로 풀이하는 방법인데 AD 에서는 이 DNS 를 이용하여 Internet 에 있는 Source 나 Object 를 찾는다. 이는 네트워크 상에 물리적 위치에 상관없이 Object 를 쉽게 찾을 수 있는 방법을 제공한다.

LDAP 지원

AD 를 검색하고 Directory 와 응용 프로그램간의 정보 교환을 할 때 LDAP 프로토콜을 사용한다.

한곳에서 관리(Single Point of Administration)

Directory 를 관리한다는 것은 네트워크 상의 Object 들을 추가, 변경, 삭제하는 작업을 말한다. AD 는 이런 작업들을 한 컴퓨터(DC)에서 액세스하여 관리할 수 있도록 한다. 이는 비용과 시간을 절약할 수 있는 것을 의미한다.

AD의 추가기능

향상된 질의(Enhanced Queries)

AD 에는 Global Catalog Server 에 전체 Directory 에 대한 Index 를 만들어 둔다. 이 Global Catalog Server 에 사용자는 질의를 함으로서, Object 를 찾을 수 있다. Global Catalog Server 는 AD 가 복제될 때에 자동으로 생성되기 때문에 복제된 정보를 이중화로 가지고 있다.

결함 허용(Fault Tolerance)

AD 가 복제 되기 때문에 어느 한쪽에 장애가 발생하더라도 복제된 정보를 이용해 계속 디렉터리 서비스를 할 수 있다.

보안 통제(Security Controls)

사용자나 관리자가 AD 를 사용하고 관리하는 것은 보안 정책(Security Policy)으로 규정된다. AD 는 ACL(Access Control List)가 있어서 권한이 부여된 사용자만이 해당 Object 를 읽거나 쓸 수 있도록 통제할 수 있다. 그리고 여러 책임 있는 그룹에게 관리 권한과 책임을 분산하여 관리할 수도 있다.

AD의 동작원리

AD 의 동작원리를 이해하기 위해서는 다음과 같은 4 가지의 개념을 이해하고 있어야 된다.

- 표준 이름 명명 법(Name Standard)
- 논리적 구조 요소와 Organization 그리고 그 둘의 상관관계
- 각 컴포넌트의 물리적 구조와 동작
- AD 의 보안 특징

그럼 4 가지의 개념을 하나하나 살펴보도록 하겠다.

표준 이름 명명 법

AD 는 아래와 같이 업계 표준인 2 가지의 이름 명명 법(Naming Conventions)을 사용하기 때문에 사용자나 응용프로그램이 AD 를 액세스 할 때에 비슷한 포맷으로 사용할 수 있다.

- DNS(Domain Name System)

- Internet 의 표준 이름 영역(namespace) 방식이 DNS 이다. AD 는 이 DNS 와 같은 이름 영역 표시법을 사용하고 이를 이용해서 이름을 주소로 풀이해서 그 자원이 있는 장소를 찾을 수 있는 서비스를 제공한다.

- LDAP(Lightweight Directory Access Protocol)

  - AD 가 directory database 와 응용 프로그램 간의 핵심 프로토콜로 사용된다.

AD 는 각 Object 를 기준으로 하여 동작하는데 이 Object 는 AD 내에서 각각 고유한 이름을 갖게 되며 이것으로 서로 구분하게 된다. 이를 이름영역(Namespace)라고 하고 이름을 Object 나 그 이름이 나타내는 정보로 번역하는 과정을 이름 풀이(Name Resolution)이라고 한다.

관리자가 AD 구조를 생성할 때, 그 Contents 는 논리적 계층적 구조로 만들어져서 보관된다.

예를 들면, EXEM 이 EX-EM.com 으로 되어 있다면, SQLServer 팀은 SQLServer.EX-EM.com 으로, Consulting 팀은 Consulting.EX-EM.com 으로 만들어 지는 것이 바로 AD 내에서 논리적 계층 구조로 이름이 명명된다는 의미하는 것이다.

AD 내의 각 Object 의 이름에는 다음과 같은 3 가지 타입이 있다.

- DN(Distinguished Name)

  - AD 내의 모든 object 는 DN 을 가진다. 예를 들어 필자(YDH)의 DN 은 YDH@SQLServer.EX-EM.com 이다.

- YDH : AD 에 정의된 user object 의 실제 이름이다.
- SQLServer : EXEM 의 SQLServer 팀을 나타내는 컨테이너(Container)이다.
- EX-EM : AD 내의 EXEM 사의 이름 영역(Namespace)이다.
- Com : Internet 에서 일반 회사임을 나타내는 컨테이너(Container)이다.
- RDN(Relative Distinguished Name)

- Object 의 Attribute(속성)을 나타내는 이름의 한 부분을 의미한다. YDH 라는 user object 의 RDN 은 YDH 이다. 이 YDH 라는 object 의 부모(Parent) object 의 RDN 은 Users 이다.

- UPN(User Principal Name)

  - 사용자의 로그온 이름이다. Object 가 있는 컨테이너의 DNS 이름이나 user object 를 대신하는 줄인 이름인 것이다.

AD의 논리 구조와 요소

AD 를 구성하는 각 요소들은 논리적인 구조로 엮어져 있다. 사용하는 용도에 따라 논리적으로 그룹화 되어 있으며, 각 object 들의 물리적 위치에 관계없이 이름만으로 쉽게 검색 할 수 있는 것이다. 이러한 AD 의 기본 구성 요소와 논리 구조에 대해 알아보겠다.

- Objects

  - 공통된 속성을 가지며 class 별로 구성된다. Users, computers, application 등이 object 이다.

- Object Attributes

  - 각 object 가 가지고 있는 특징을 정의하는 정보의 카테고리이다. 같은 타입의 object 는 동일한 attribute 를 가지고 그 attribute 의 값이 서로 다르기 때문에 해당 object 들은 unique 하게 되는 것이다.

- Object Classes

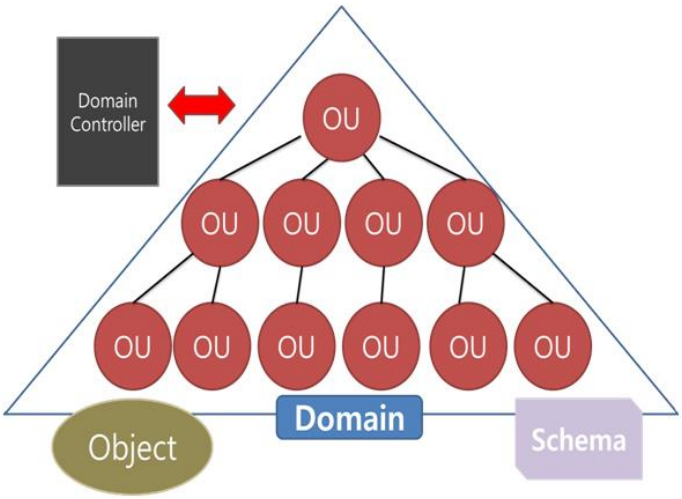
  - Object 의 논리적 그룹이다. 이 클래스의 특징을 기술하는 것을 properties 라고 부른다.

- Ex) users, groups, computers, domains, organizational units(OU), security policies 등

- Schema

- AD 의 object 를 정의한다. 이는 각 object 의 attributes, classes, classes properties 등을 규정한다.

AD 의 논리구조



[그림2]AD의 object는 containers, domains 그리고 OUs를 구성한다.

- Container

  - 다른 object 를 포함하고 있는 일종의 directory object 이다.

- Domains

  - AD 의 논리 구조의 단위가 domain 이다. 사용자 계정정보와 DNS 이름을 바탕으로 서로를 구별하고 보안 정보를 공유하는 object 의 논리적 container 이다.

  - Domain 은 보안 관리 체계를 이루는 최소 단위이자 복제가 일어나는 단위이다.

-

- DC(Domain Controller)

  - AD 의 물리적 구조를 살펴보면 DC 서버가 domain 의 directory 를 한 벌 저장하고 있다. 한 domain 에 여러 개의 DC 가 있을 수 있으며, 각기 해당 domain 의 directory 정보의 복제 본을 한 벌씩 가지고 있다.

- OU(Organizational Units)

  - 일종의 container object 로서 domain 내의 object 들을 관리할 수 있는 그룹으로 묶어 놓은 것을 말한다.

AD 논리구조의 상관관계

- 그림

- Trees

  - 연속되는 이름영역을 가진 하나 이상의 domain 으로 구성된 계층적 조직을 tree 라고 한다. 이 연속된 이름영역(Contiguous namespace)이라는 것은 parent container 의 이름이 child object 의 이름의 뒤에 붙는다는 것을 말한다. AD 내에서 tree 내의 domain 끼리는 서로 trust relationship 을 가지면서 공통된 schema, configuration, global catalog server 를 사용한다. 여기서 trust relationship 이라고 하는 것은 두 개 이상의 domain 을 논리적으로 연결하여 하나의 관리 단위로 이용하는 것을 의미하기 때문에 각 object 는 domain 에 상관없이 서로 공유된다.

- Forests

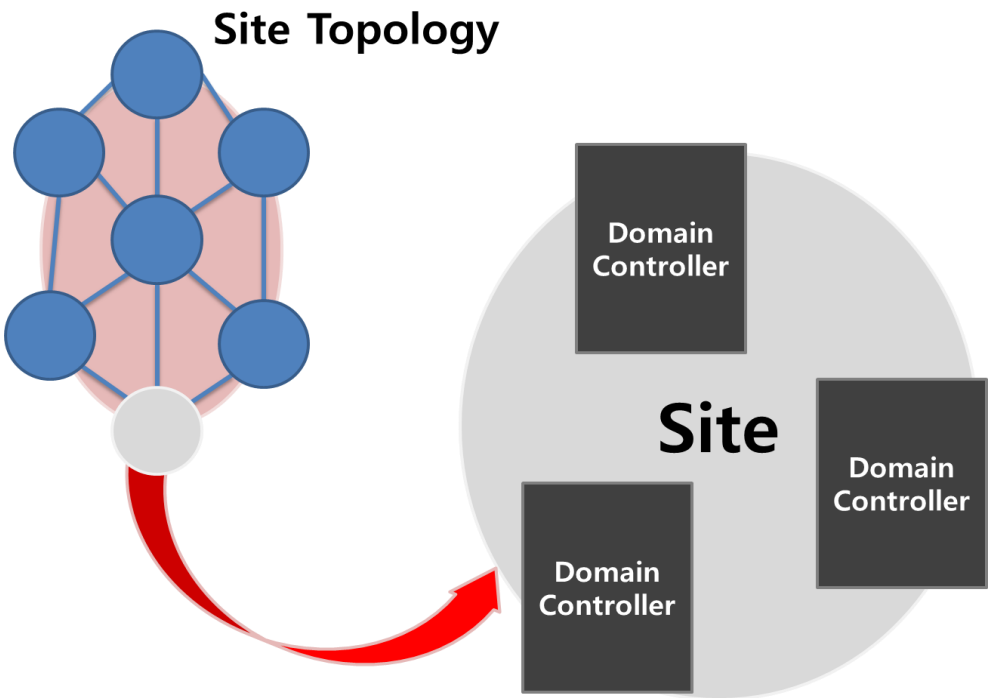
  - Forest 는 연속되지 않는 이름영역을 가진 하나 이상의 tree 로 이루어진다. forest 내의 각 tree 는 독립적인 이름영역을 가지는데, 이들 tree 간에 각기 다른 이름영역을 disjointed namespace 라고 부른다. Default 로 root tree 나 forest 내에서 제일 먼저 만들어 지는 tree 의 이름이 forest 의 이름으로 사용된다.
    이름이 서로 공유되지 않더라도 forest 내의 tree 들은 schema, configuration, global catalog server 는 공유한다.

- Global Catalog Server

  - 전체 directory 의 모든 구성 요소와 그 상관 관계를 한눈에 알아 볼 수 있도록 한다. 이것은 AD 가 복제 될 때에 만들어 지며, 전체 directory 의 복제 본을 저장하고 있다. 이것을 통해 사용자나 관리자가 해당 object 를 물리적 위치에 상관없이 찾을 수 있다.

  - Global Catalog Server 는 모든 directory object 를 담고 있지만 AD 의 각 object 와 attribute 의 일부분만 복제하고 저장하고 있다.

AD의 물리적 구조



[그림3]AD는 Site내에서 DC(Domain Controller)를 포함하는 site topology를 구성하여 하나의 물리적 디렉터리 구조를 이룬다.

- Sites

  - AD server 가 물리적으로 위치하는 장소 정도로 이해하면 된다. 관리자 (Administrators)는 신뢰성 있고 빠른(Site 내의 서버끼리 일어나는 복제 작업에 따른 네트워크 트래픽을 감당) LAN 네트워크 망에 있는 여러 서버들을 묶어서 Site 를 만든다. Site 에는 서버, 컴퓨터, 프린터, 팩스 등과 같은 하드웨어를 포함한다. Site 는 이름 영역에 속하지 않는다. Site topology 정보나 그 구조에 관한 사항은 directory 에 별개로 저장된다.

  - Site 를 만들 때 고려사항으로는

    - 복제 트래픽이 원할 하게 전송될 것

    - 사용자가 DC 에 신뢰성 있고 빠른 LAN 망으로 접속할 수 있게 할 것

    - 한 Site 는 여러 domain 에 여러 DC 를 포함할 수 있고, 한 domain 의 여러 DC 에는 여러 site 가 포함될 수 있음

- Site Topology

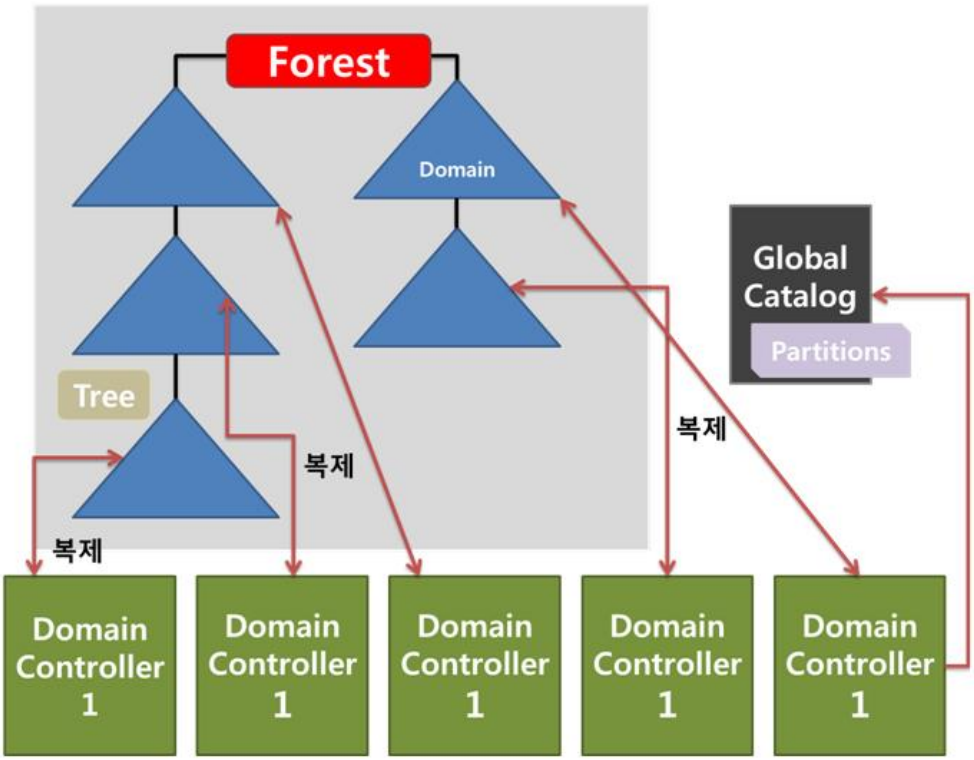
  - 기업의 전 네트워크에 site 를 어떻게 분산 배치 할 것인지를 기술하고 있다. 한 site 에 최소 하나의 DC 를 두도록 설계하는 것을 권장한다.

- Domain Controllers

  - Domain directory 를 업데이트 할 수 있는 복사본을 가지고 있는 서버를 말한다. 모든 DC 는 계층적 구조가 아닌 동등한 관계를 유지하기 때문에 NT4.0 이전 버전에 있던 primary 나 backup domain controller 라는 개념은 더 이상 사용하지 않는다.

  - DC 가 없는 site 에서는 복제가 일어나지 않는다.

AD의 물리적 구조 내에서의 동작



[그림4]Site를 이루는 물리적 구성 요소와 DC가 구성되면 이는 AD운용과 함께 어울려 동작한다. 이 동작에는 디렉터리 복제, Global Catalog server업데이트, Directory확장과 성능최적화를 위한 directory 저장 조직의 개편 등이 포함된다.

- 복제(Replication)

  - Directory 에 변경(새로운 서버의 추가, 삭제 포함)이 생기면 바로 다른 DC 에게도 복제가 일어난다. 복제를 함으로써 장애로 인해 디렉터리 데이터에 손상이 가더라도 다른 서버를 통해 읽을 수 있고 복제된 디렉터리가 네트워크 전반에 걸쳐 있어 각 사용자의 액세스가 분산되어 로드를 줄일 수 있다.

  - AD 는 multi-master replication 을 한다.

  - 복제가 일어나면 해당 변경사항이 Global Catalog server 에도 복제가 된다.

- 물리 구조에서의 Global Catalog server(GCS)의 역할

  - GCS 는 DC 가 생성될 때 자동으로 생성된다. AD 의 부분 복제 본이 DC 에 있게 된다. 이것은 AD 가 정보와 자원을 저장하기 위해 partition 을 사용하기 때문이다.

- Partitions

  - 디렉터리 데이터의 서브 셋을 담고 잇는 물리적 저장 컨테이너 이다 AD 는 partition 에 각 domain 의 디렉터리 정보를 DN 별로 분리 저장한다. GCS 는 DN 을 보면 해당 object 가 있는 partition 의 복제 본이 어디 있는지를 알 수 있기 때문에 쉽게 object 를 찾을 수 있다.

- Naming Context

  - 디렉터리의 연속되는 Sub-Tree 이며 복제의 단위가 된다. 한 partition 이 하나의 naming context 이다. 복제가 일어날 때 마다 이들 naming context 도 복제된다.

  - AD 에서는 하나의 서버가 최소 3 개의 naming context 를 가진다.

    - Configuration : Site, services, partition 과 schema 에 대한 물리적 데이터 저장

    - Domain naming : domain directory 데이터를 포함하는 복제의 기본 단위

    - Schema : 전 AD 에 대한 Schema 를 저장

AD Security 특징

AD 를 관리하고 액세스하는 것은 엄격한 보안 관리를 통해서 제어된다. 보안관리를 위해 다음과 같은 4 가지 기능이 있다.

- ACL(Access Control List)

- AD 내의 각 object 에는 누가 어떤 권한(permission)으로 액세스 할 수 있는지 통제할 수 있는 ACL 이 있다. 적용대상은 object 뿐만 아니라, object attribute 와 object classes 도 액세스 하는 것을 통제한다.

- Delegation(권한 위임)

  - 관리자가 특정 개인이나 그룹에게 container 나 sub-tree 에 대한 특정 권한을 주어서 이를 관리하게 할 수 있는 것을 말한다.

- Inheritance(상속)

  - Container object 에 대한 ACE(Access Control Entry)를 child container 에 있는 object 에게도 그대로 상속하여 적용하는 것을 말한다.

- Trust Relationships

  - Schema, configuration, global catalog server 를 공유한다는 것을 의미한다.

  - 한 domain 에 있는 사용자가 다른 domain 에 있는 자원을 액세스 하려면 해당 domain 사이에는 trust relationship 이 이루어져야 한다.

  - Trust relationship 에는 다음과 같이 2 종류가 있다.

    - Transitive Trusts

      - 다른 용어로는 implicit trust 라고도 하며 domain 간에 서로 양방향 신뢰관계(trust relationship)가 설립되는 것을 말한다. 이는 forest 에서도 일정한 권한이 주어진다면 사용자는 어떤 자원에도 액세스할 수 있도록 하기 위함이다.

      - Domain 이 만들어져서 tree 에 포함될 때 자동으로 설정된다.

- Ex) domain A -> domain B, domain B- > domain C = domain A -> domain C

■ Explicit Trusts

- 단 방향으로 신뢰가 설정되는 경우이다. Domain A 가 domain B 를 trust 할 때에는 domain B 의 사용자가 domain A 의 자원을 액세스 할 수 있고 그 반대의 경우에는 안 된다.

- forest 간에는 explicit trust 가 설정된다.

지금까지 AD 란 무엇인지를 알아보았고 다음은 AD 설계, 구축 및 운영 Tip 에 대해 설명하겠다.

AD 설계

AD 를 구축하기에 앞서 먼저 AD 를 설계해야 한다. AD 설계는 6 가지의 단계가 있다. 1 단계부터 차근차근 알아보도록 하자.

요구분석

안정적인 AD 구축 및 운영을 위한 가장 중요한 단계는 요구분석 단계이다. 요구조건을 최대한 도출하고 분석을 통하여 올바른 설계의 방향을 결정하는 것은 아무리 강조해도 지나치지 않다. AD 설계에 정답이 있는 것은 아니다. AD 를 구축하고자 하는 회사의 요구사항이 있고 AD 에서 수용할 범위가 결정되었다면 설계된 내용을 토대로 AD 를 구축하였을 때 요건이 모두 해결될 수 있다면 최적의 설계를 한 것이라고 할 수 있다.

도메인 구조 결정

요구분석을 끝내면 먼저 도메인구조를 결정할 필요가 있다. 몇 개의 도메인으로 AD 를 구축할 것인지를 고려해야 한다. AD 는 Windows NT4.0 의 도메인 구조와는 분명히 달라질 수 있다.

NT4.0 의 도메인은 계층적인 관리구조를 지원하지 못하였다. 그런 이유로 지사, 본사, 부서별 관리 등을 회사가 원하는 대로 지원하기 위해서 복수도메인 구조가 불가피했던 경우가 생겼다. 하지만 AD 는 조직단위(OU)라는 관리구조가 도입됨에 따라 계층적인 관리가 가능하고 Windows NT4.0 이라면 복수도메인으로 구축되어야 할 경우라도, 대부분의 경우 AD 는 단일 도메인으로써 지원할 수 있는 토대가 마련되었다. MS 는 도메인 모델을 결정할 때 먼저 '단일 도메인 모델'을 검토하고, 회사의 요구사항이 단일 도메인 모델로써 해결될 수 없는 상황일 경우에만 복수 도메인 모델을 도입할 것을 권장하고 있다. 컴퓨터가 100 대 이상의 중소규모 환경보다 더 큰 규모의 회사 환경이라도 반드시 복수 도메인으로 가야 할 이유는 많지 않다고 판단된다. 복수 도메인이 필요한 경우는 조직간에 보안상의 이유로 계정/암호정책 등이 차별적인 설정을 가져야 하는 경우, 회사의 조직간에 IT 관리에 대한 책임과 역할이 명확하게 구분되어야 하는 경우 등이 일반적인 이유이다.

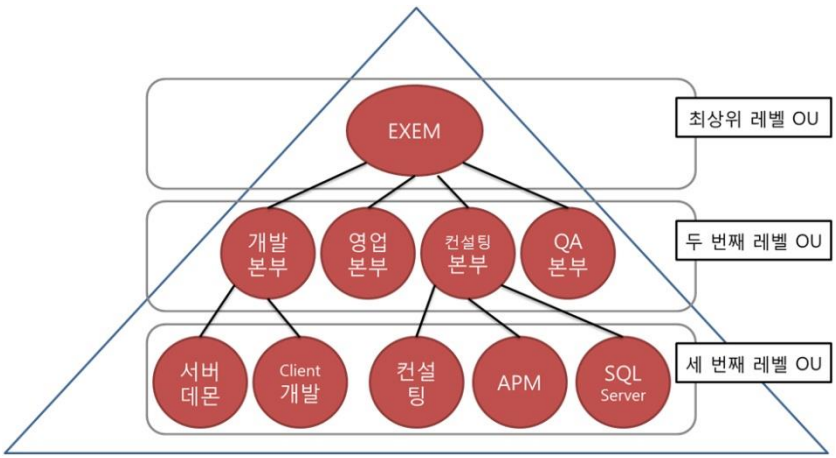
도메인 이름 결정

도메인의 이름은 회사를 대표할 수 있는 이름을 선택하는 것이 좋다. 예를 들어 '엑셈'은 ex-em.com 이라는 도메인을 가지고 있다. 이 이름을 그대로 AD 도메인 이름으로 사용하기로 한다. 만일 회사가 인터넷에 등록한 도메인 이름이 없는 상태라면 먼저 회사를 대표할 수 있는 이름 하나를 등록할 것을 권장한다. 당장 인터넷에 연결 자체는 할 필요가 없더라도 도메인 이름을 확보해 두는 것이 안정적인 도메인 구축을 할 수 있는 방법이다. 이 도메인 이름은 두 가지 용도로 사용된다. 하나는 인터넷상의 다수의 클라이언트들이 회사의 웹 서버, 메일 서버 등의 자원에 접근하기 위한 용도이고, 둘째는 회사 내부의 클라이언트가 도메인을 식별하고 디렉터리 서비스를 받기 위한 용도이다. 이들은 사용용도가 다르지만 동일한 이름체계를 사용하고 있기에 하나의 DNS 서버를 통해서 얼마든지 서비스될 수 있지만, 보안을 고려한 좋은 모델은 이 두 가지 용도별로 DNS 서버를 분리시키는 방법이다. 내부 DNS 서버와 외부 DNS 서버로 구분하는 것을 의미한다.

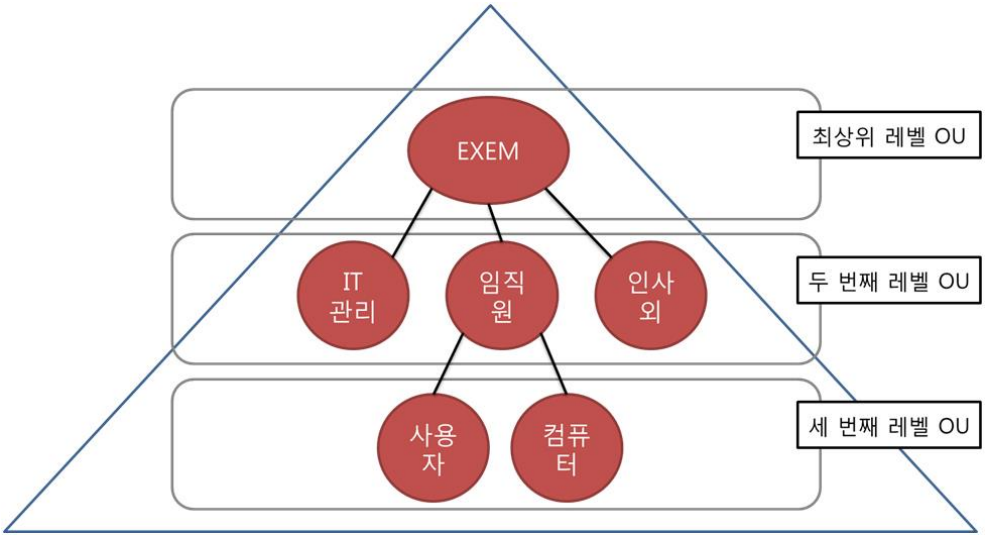
관리구조 결정(OU)

AD 구조에서 OU 는 큰 의미를 가진다. 관리권한의 위임, 그룹정책 적용의 최소단위가 OU 이기 때문에 IT 관리 요구사항을 그대로 반영하여 OU 구조를 만들어 낼 필요가 있다. OU 의 가장 큰 용도는 그룹정책구성을 위한 최소단위, 관리권한 위임의 최소단위로 사용되어 IT 관리자가 개체들을 보다 쉽고 유연하게 관리하도록 한다. 그렇지만 OU 구조가 조직구조와 같을 필요는 없다. OU 라는 단위는 사용자들에게는 투명하다. 사용자들은 자신이 어떤 OU 에 속해 있는지 몰라도 되고, 알 필요도 없다는 것이다.

방법은 2 가지가 있다. 첫 번째 방법은 부서별로 OU 를 구분하여 조직도 형태의 OU 를 만드는 것이고, 두 번째 방법은 하나의 OU 에 개체를 모두 담고 Filtering 을 통해서 그룹별로 지정된 프로그램을 배포하는 방법이다.



[그림5] 조직 도를 반영한 계층적 OU 구조 디자인



[그림6] 기능적 측면을 고려한 계층적 OU 구조 디자인

명명규칙

AD 인프라와 관련된 서버/PC/로그온 이름 등 다양한 개체에 대한 명명규칙을 정의한다.

구분	고려사항	비고
서버 명	‘도입된 서비스 유형 등이 파악될 수 있는 이름을 고려하는 것이 좋음	‘운영서버/개발서버 ‘도입된 시스템 분류
클라이언트 PC 명	‘효율적인 관리를 위해 단말 명은 변경되지 않는 고유 값을 설정하는 것이 좋음	‘공유자원에 접근이 용이하도록 단말의 ‘설명’항목에 부서명/사용자 이름 등을 표기함으로써 접근이 용이하도록 구성
사용자계정	‘기존 어플리케이션에서 사용하던 로그온 ID 와의 편의성 측면을 고려해야 함 ‘로그온 ID 가 보안이 유지되어야 할 대상인지	‘암호정책 고려 ‘암호 길이 ‘최소암호사용기간 ‘최대암호사용기간

	판단	암호 잘못 입력 시 동작 등
그룹계정	‘조직, 직무, 직군, 직급 등의 다양한 그룹이 통합디렉터리에서는 하나의 ‘그룹’카테고리로 분류됨 ‘사용자가 통합디렉터리에서 검색이 용이하도록 이름 선택	

디렉터리 구성 테이블 작성

구현을 위해서 필요한 디렉터리의 내용들을 테이블로 작성해 보았다. 이건 하나의 예시로 작성해 본 것이다. OU 구조 중 기능적 측면을 고려한 계층적 OU 구조 일 경우의 예이다.

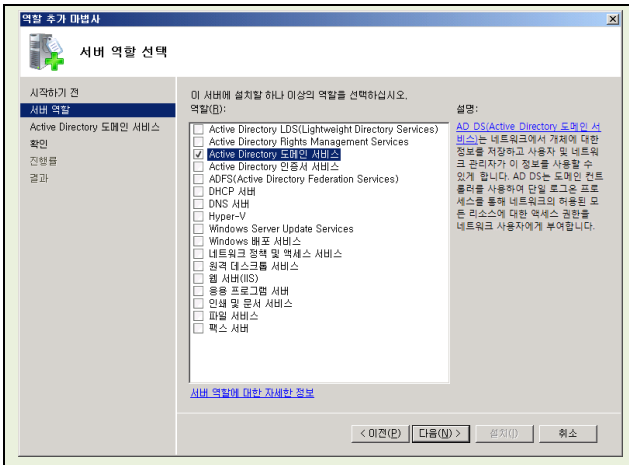
단위	그룹, 사용자, 컴퓨터	권한위임	그룹정책(GPO)	옵션
도메인			‘암호정책(8 자리) ‘계정잠금정책(5 번) ‘감사정책 구현	‘무시안함 ‘무시안함 ‘무시안함
Domain Controller	‘도메인 컨트롤러 배치			
Computers	‘파일, 프린트, DNS 서버			
윈도우 네트웍스 OU		‘인사담당자에게 사용자 계정 생성권한위임	‘전사적인 업무프로그램 배포정책 ‘인터넷옵션 설정	
IT 관리 OU	관리자 계정	‘없음(상속)		‘정책상속

			거부
임직원 OU		‘없음(상속)	‘My Documents 폴더 지정 ‘공유폴더 매핑 로그온 스크립트
인사 외 OU	‘인사시스템에 등재되지 않은 외부사용자	‘없음(상속)	‘없음(상속)
임직원/ 사용자 OU	‘회사의 모든 임직원	‘없음(상속)	‘없음(상속)
임직원/ 컴퓨터 OU	‘회사의 모든 PC	‘없음(상속)	‘없음(상속)

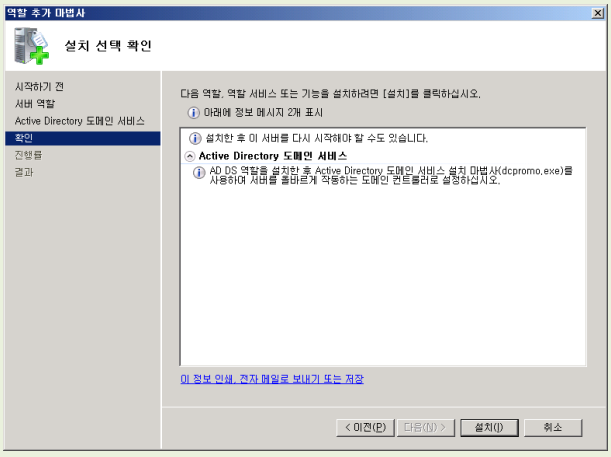
이것으로 AD 설계가 끝나면 다음은 AD 를 구축해야 한다.

AD 설치 및 운영TIP

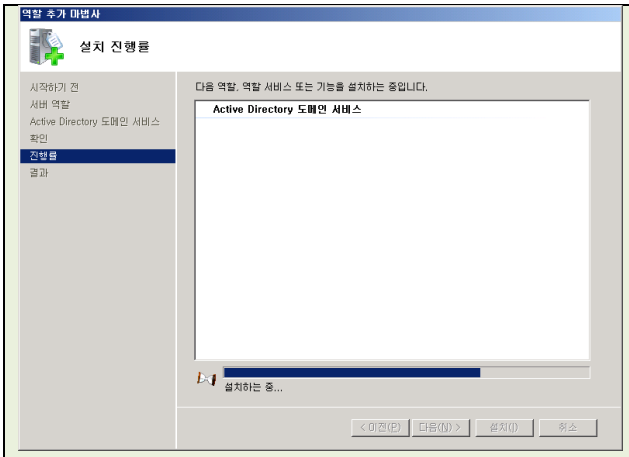
AD 서버 구축 (Windows Server 2008 R2 기준)



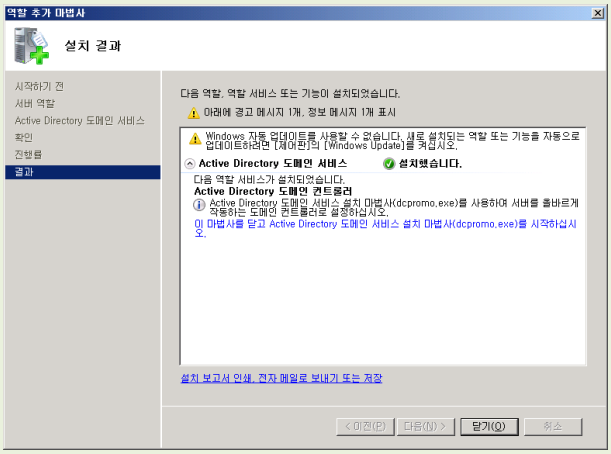
<서버 관리자>에서 <역할 추가>를 선택한 후 추가할 서버 역할 항목에서 <Active Directory 도메인 서비스>를 선택한다.



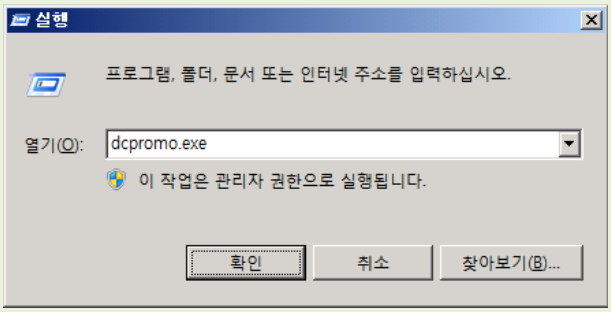
필요한 기능 추가 탭이 나오면 확인을 누른 후 다음(N) 버튼을 클릭 한 후 설치(I)를 선택한다.



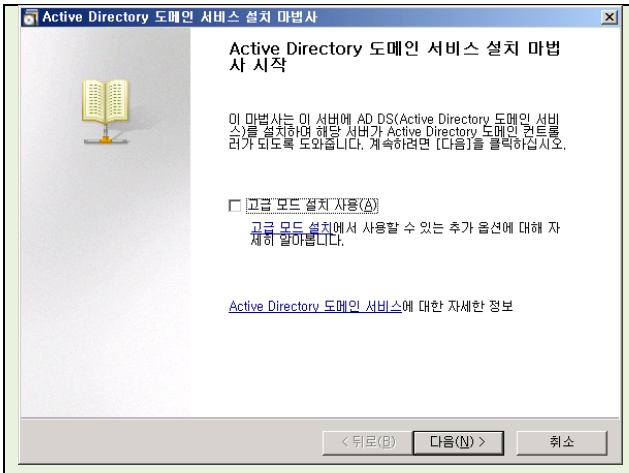
<Active Directory 도메인 서비스> 역할 설치가 진행된다.



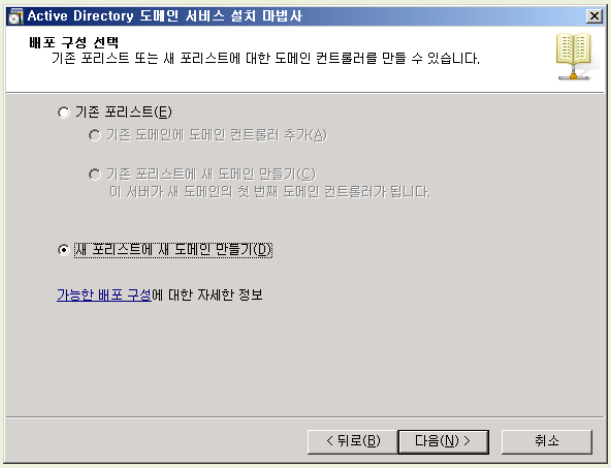
설치가 완료되면 닫기(O)를 선택한다.



<시작>-<실행>을 클릭한 후 dcpromo.exe 를 실행시킨다.

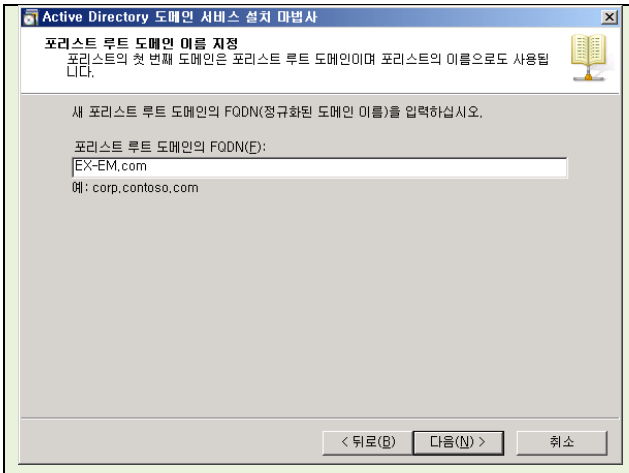


Active Directory 도메인 서비스 설치 마법사 가 시작되면 다음(N)을 선택한다.

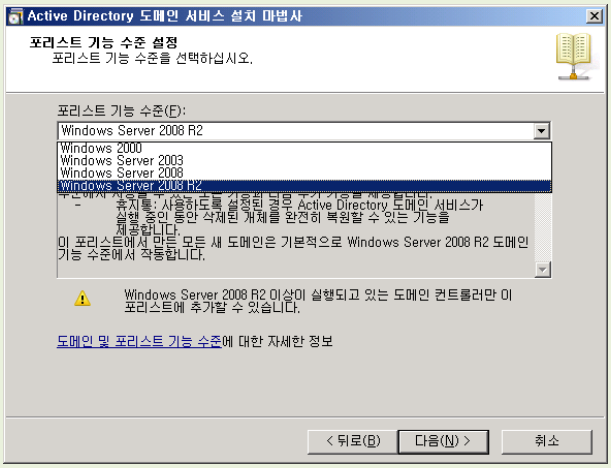


AD 초기구성이므로 <새 포리스트에 새 도메인 만들기>를 선택한 후 다음(N)을 선택한다.

AD 초기 구성이 아니고 기존에 포리스트가 존재할 경우 위에 <기존 포리스트> 선택



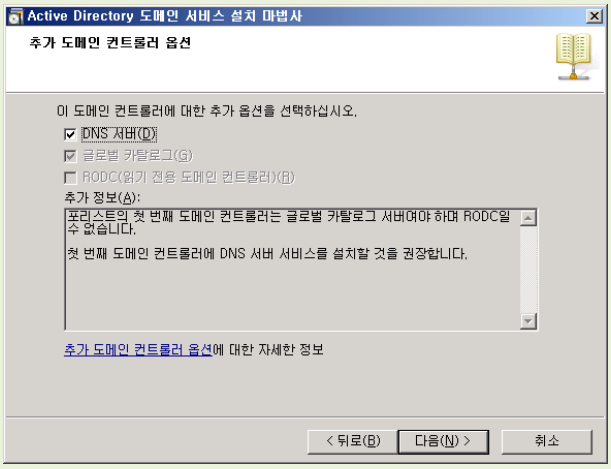
새 포리스트의 루트 도메인의 도메인이름을 지정해준다.



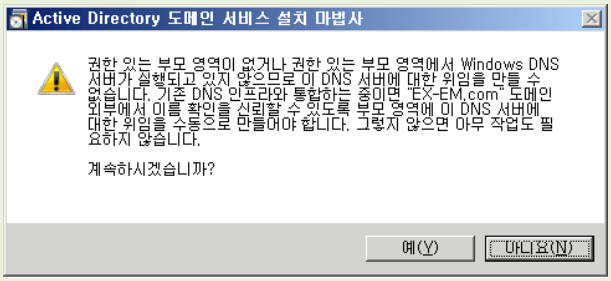
포리스트 기능 수준을 선택해 준다.

Windows 2000 부터 현재 AD 구축하고 있는 OS 의 버전까지 지정가능

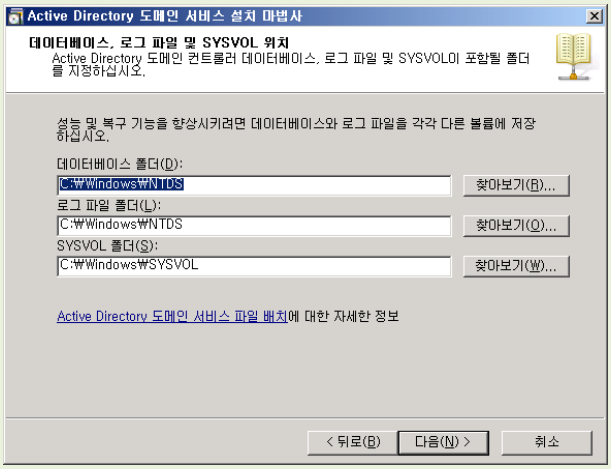
DC(Domain Controller)로 사용할 서버 OS 중 최하버전을 기준으로 설정하는 것이 바람직함.



기본적으로 AD 서버는 DNS 서버 기능도 필요하므로 DNS 서버도 옵션으로 선택해 준 후 다음(N)을 선택한다.

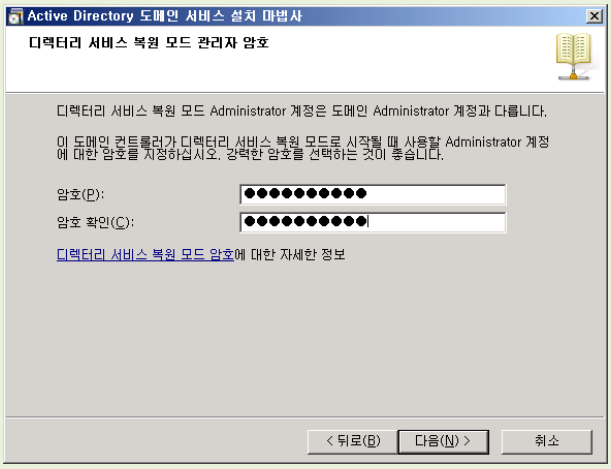


AD 초기 구축이므로 기존에 DNS 서버가 존재하지 않으므로 예(Y)를 선택한다.

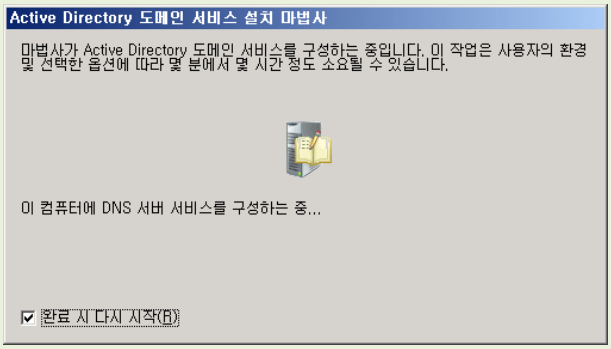


데이터베이스, 로그 파일 및 SYSVOL 위치를 지정해주고 다음(N)을 선택한다.

추후 위치는 변경가능



추후에 AD 서버에 문제가 생겼을 경우에 대비해 AD 서버 복원 시에 필요한 암호를 설정해준다.



설치가 완료될 때까지 대기한다.

AD 설치가 완료되면 필수적으로 서버를 재 시작 해야 한다.

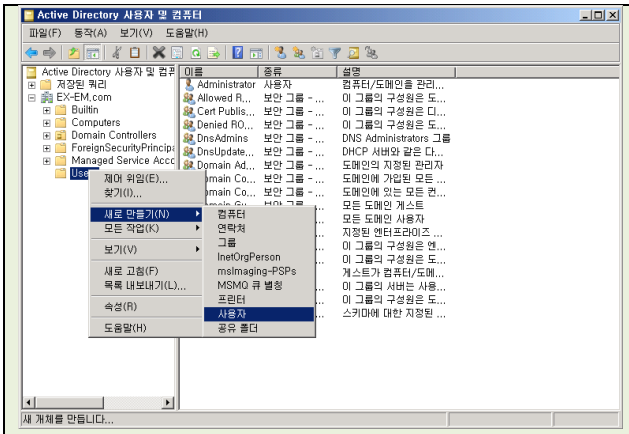
재 부팅 후 서버의 OS 계정정보가 변경되어 있는 것을 확인할 수 있다.

- 도메인 명\계정

계정의 패스워드는 기존과 동일하다.

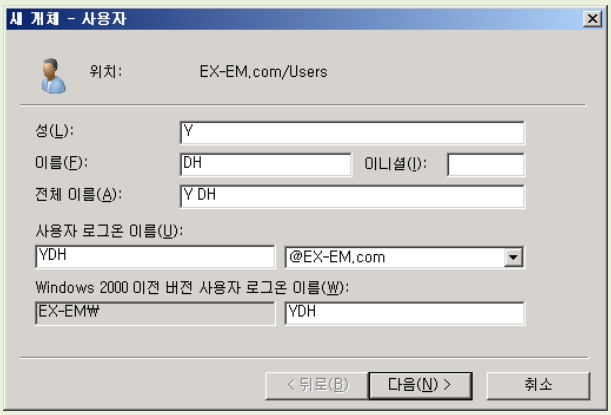
<시작> - <컴퓨터> - <속성> 에서 도메인계정으로 로그인 되어 있다는 것을 확인할 수 있다.

AD에 Join

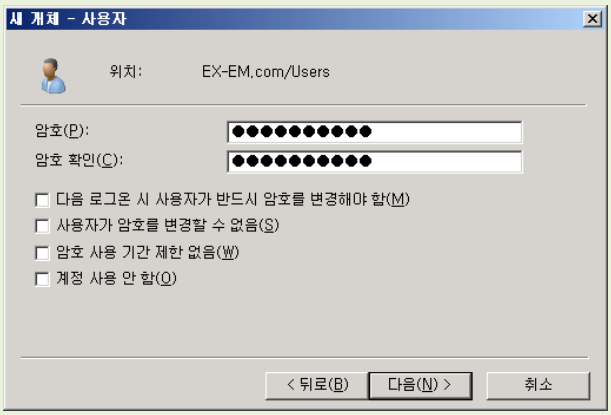


앞서 구축한 AD 서버에서 새로운 사용자를 생성한다.

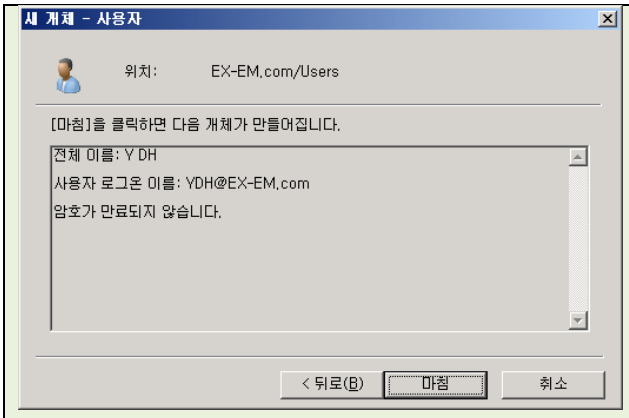
<시작> – <관리도구> – <Active Directory 사용자 및 컴퓨터>에서 왼쪽의 User 탭에서 우 클릭 후 새로 만들기 → 사용자를 선택한다.



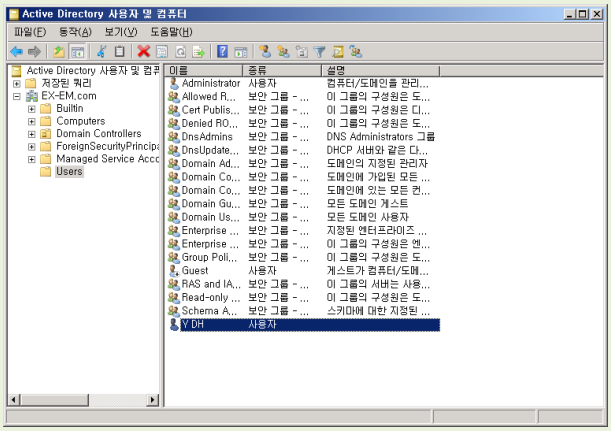
이름과 로그온 이름을 적절하게 지정해 준 후 다음(N)을 선택한다.



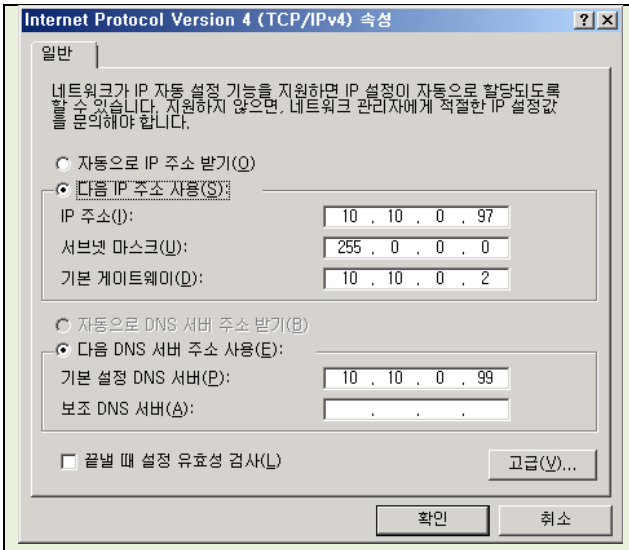
해당 사용자의 로그온 패스워드를 지정해 준 후 다음(N)을 선택한다.



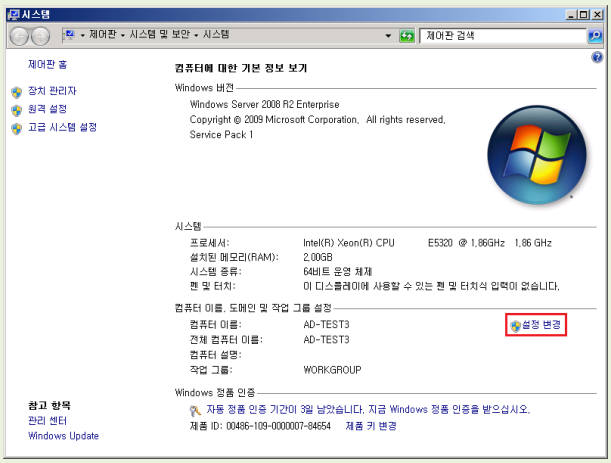
새로운 사용자가 만들어지면 마침을 선택한다.



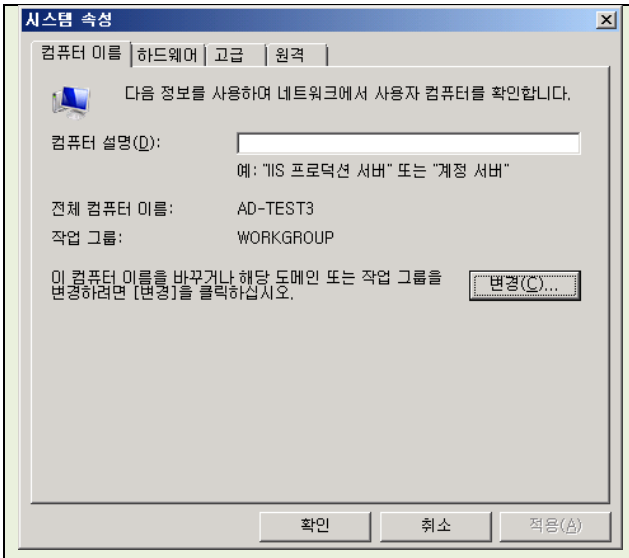
User 탭에서 가장 아래에 새로운 사용자가 생성된 것을 확인할 수 있다.



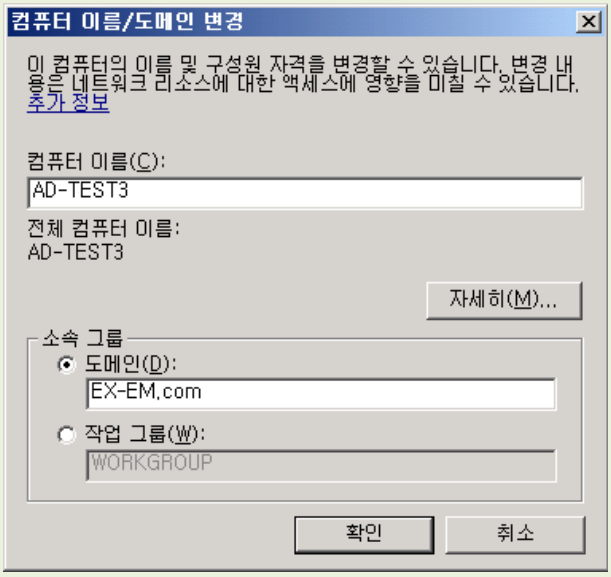
AD 에 Join 할 서버에 <제어판> - <네트워크 및 인터넷> - <네트워크 연결>에서 IP 속성을 들어간 후 DNS 서버를 지정해 주는 곳에 AD 서버의 IP 주소를 지정해준다.



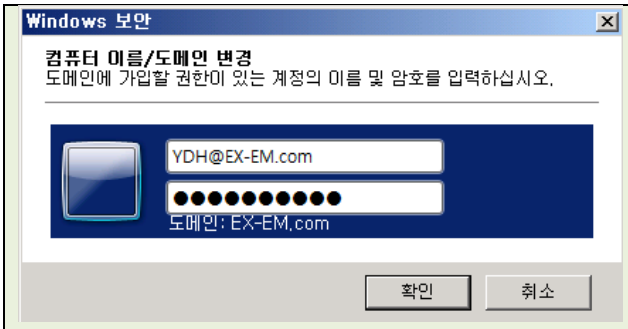
<시작> - <컴퓨터> 에서 우클릭 후 속성을 선택한 후 설정 변경을 선택한다.



컴퓨터 이름 탭에서 변경을 선택한다.

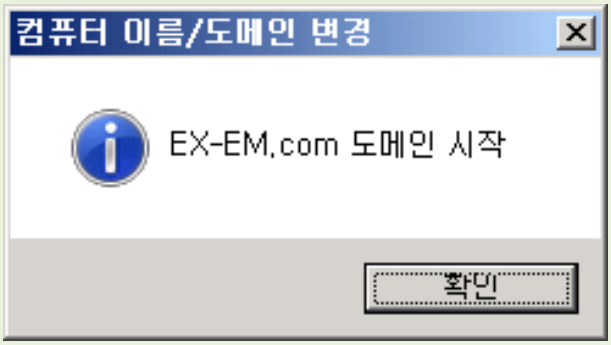


소속 그룹을 도메인(D)으로 선택한 후 AD 서버에서 생성한 도메인이름을 적어준다.

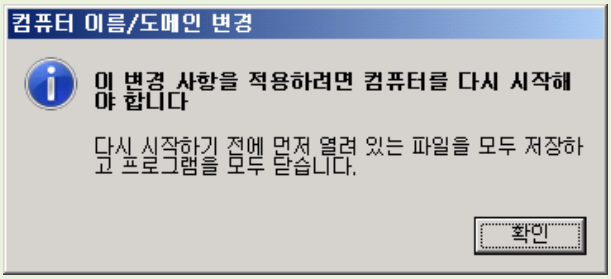


이전에 생성한 사용자와 패스워드를 지정해준다.

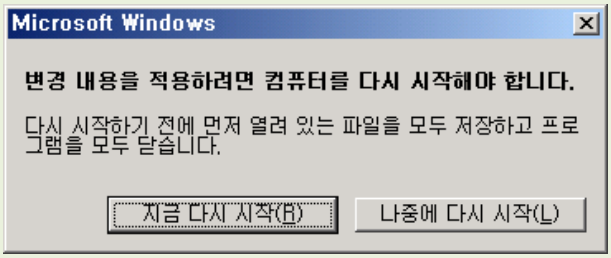
사용자명@도메인



정상적으로 확인이 되면 도메인이 변경된다.

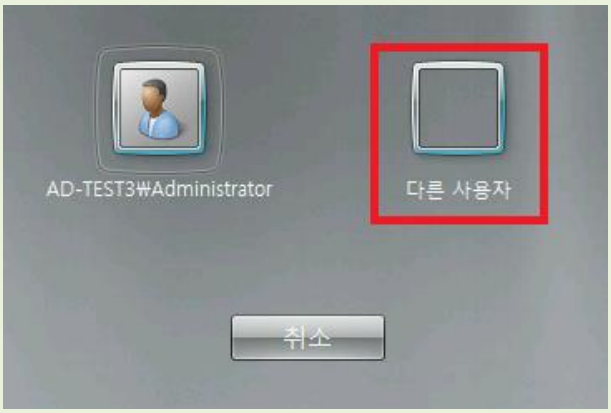


AD 서버에 조인을 하려면 서버는 재 부팅을 필수적으로 해야 한다.



지금 다시 시작(R)을 선택한다.

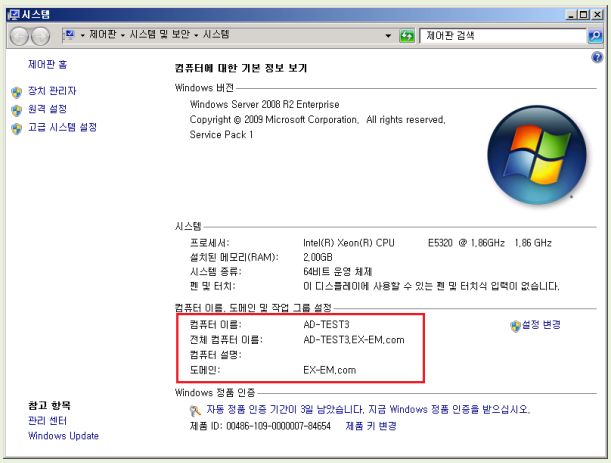
재 부팅 후 OS 로그인 화면이 나오면 아래에 사용자 전환(W)을 선택한다.



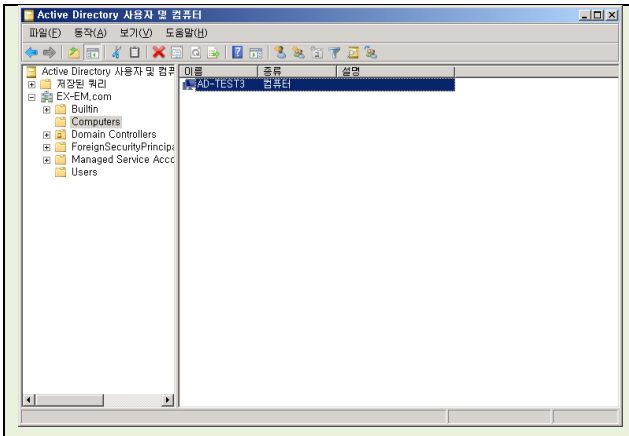
다른 사용자를 선택한다.

지정된 도메인 계정과 패스워드를 입력한다.

사용자명@도메인

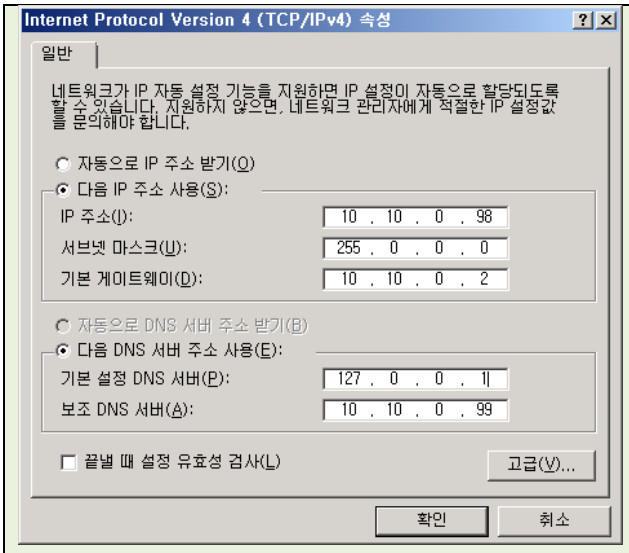


컴퓨터 속성에서 확인 할 수 있다.

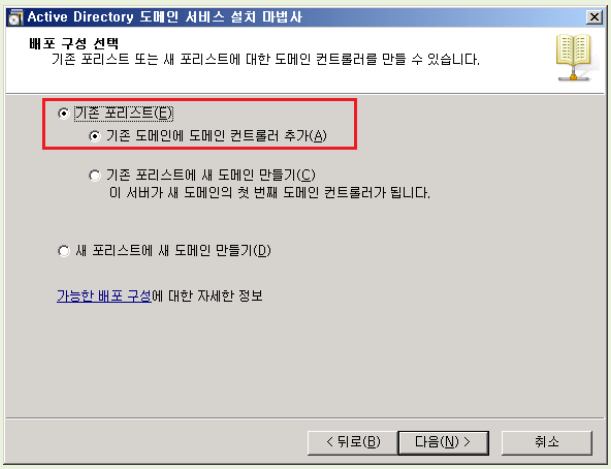


AD 서버에서 <Active Directory 사용자 및 컴퓨터> 에서 Computers 탭에서 Join 된 서버(컴퓨터)목록을 확인할 수 있다.

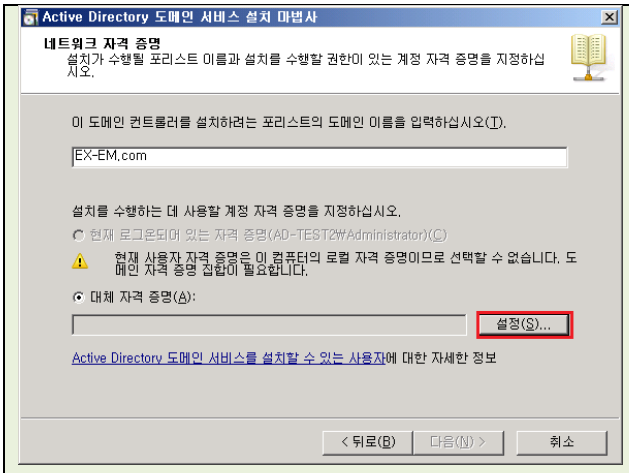
AD 이중화(DC 서버 추가)



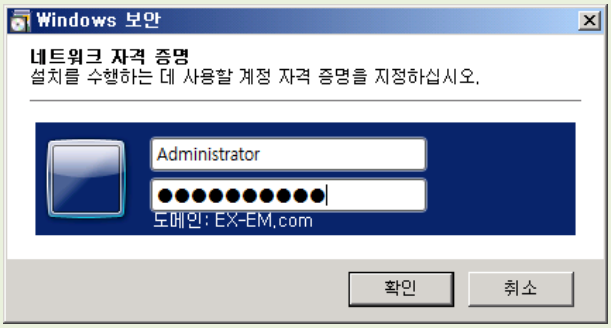
AD 이중화 할 서버의 IP 속성을 들어가서 기본 설정 DNS 서버에 자기 자신을 입력하고 보조 DNS 서버에 기존 AD 서버를 입력한다. (기존 AD 에는 반대로 입력)



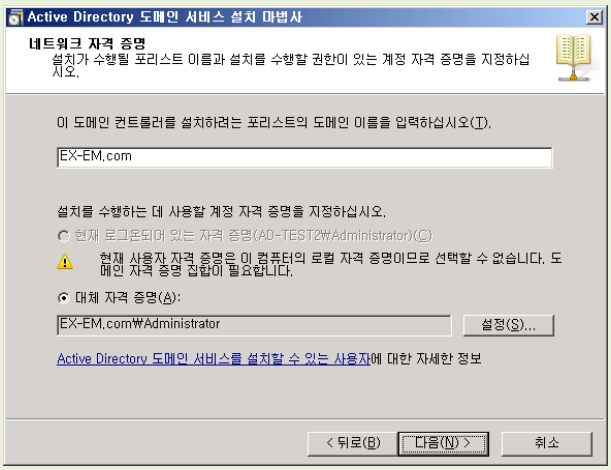
기존 AD 설치와 동일하게 서버에서 역할 추가로 Active Directory 도메인 서비스를 설치하고 dcpromo.exe 를 실행시킨 후 기존 포리스트(E)를 선택하고 기존 도메인에 도메인 컨트롤러 추가(A)를 선택한다.



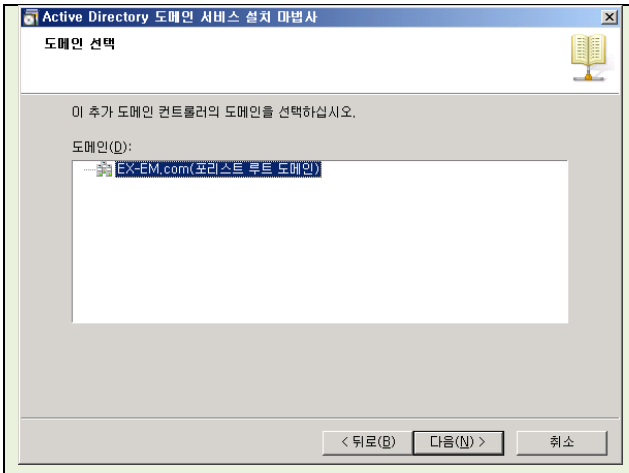
상단에 기존 도메인 이름을 입력하고 대체 자격 증명(A)에 설정(S)을 선택한다.



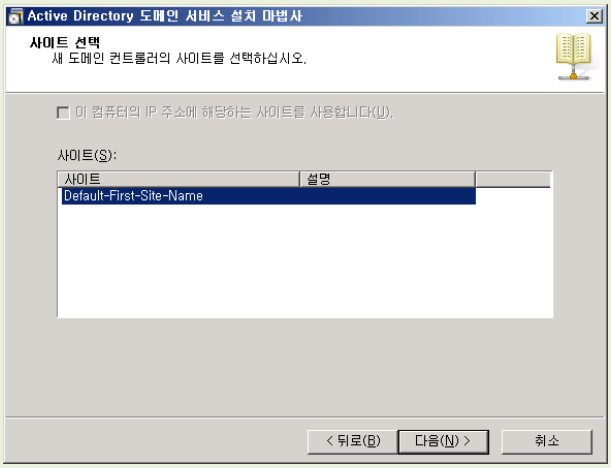
네트워크 자격 증명 창이 뜨면 기존 AD 서버의 Administrator 계정 및 패스워드를 입력한다.



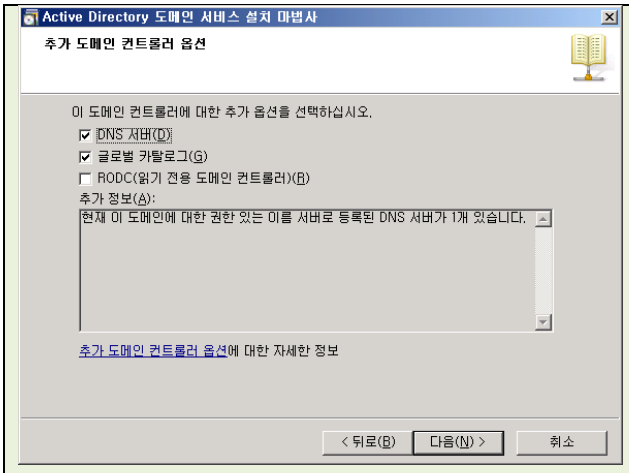
자격 증명이 완료되면 다음(N)을 선택한다.



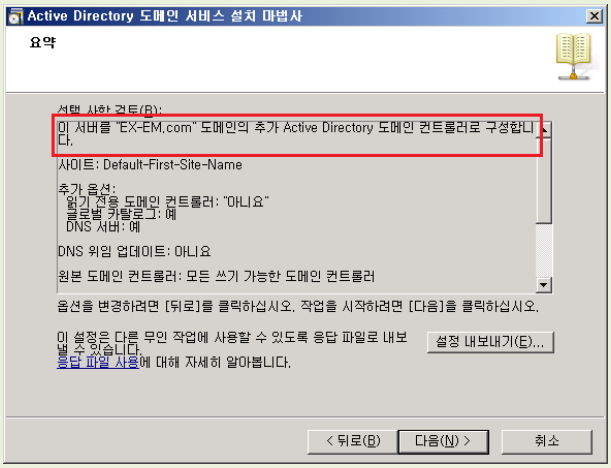
기존의 도메인이 맞는지 확인하고 다음(N)을 선택한다.



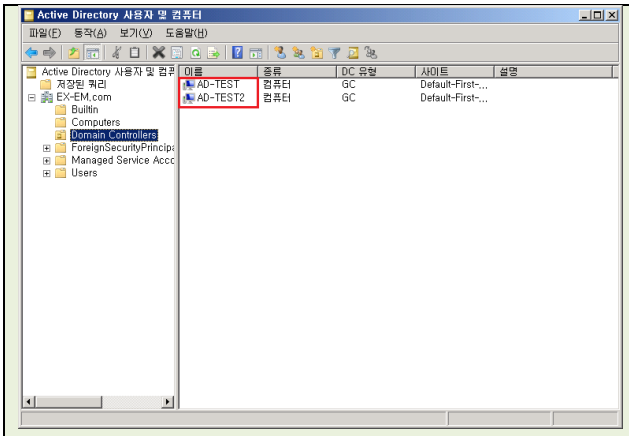
다음(N)을 선택한다.



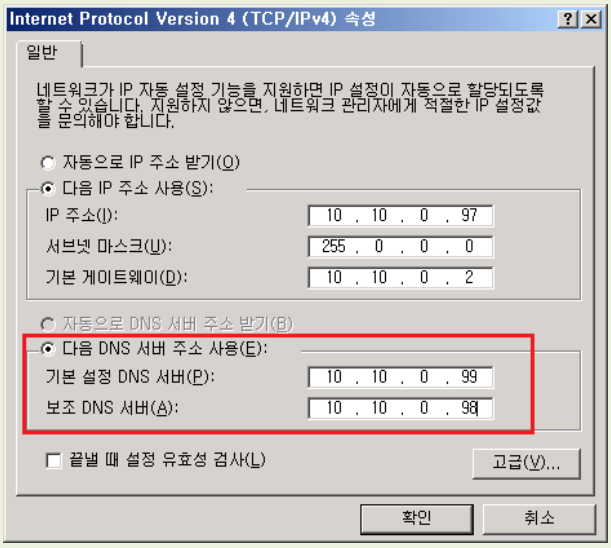
DNS 서버(D) 와 글로벌 카탈로그(G)가 체크 되어 있는지 확인한 후 다음(N)을 선택한다.



그 이후엔 기존 AD 구축방법과 동일하게 진행하면 된다.

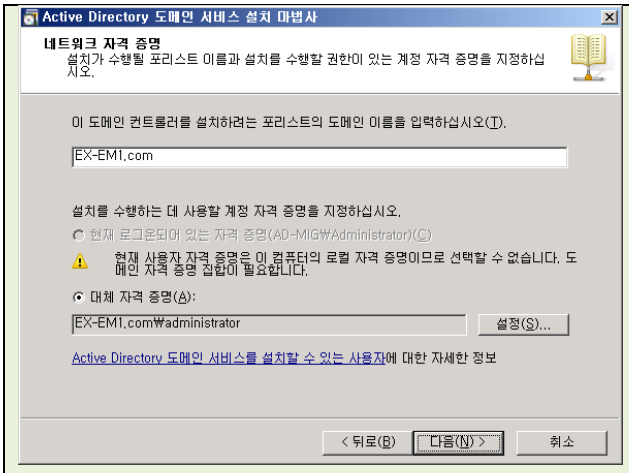


AD 이중화가 끝나면 <Active Directory 사용자 및 컴퓨터> 에서 좌측의 Domain Controllers 탭에서 AD 서버가 2 개(=DC 가 2 개)가 된 것을 확인할 수 있다.

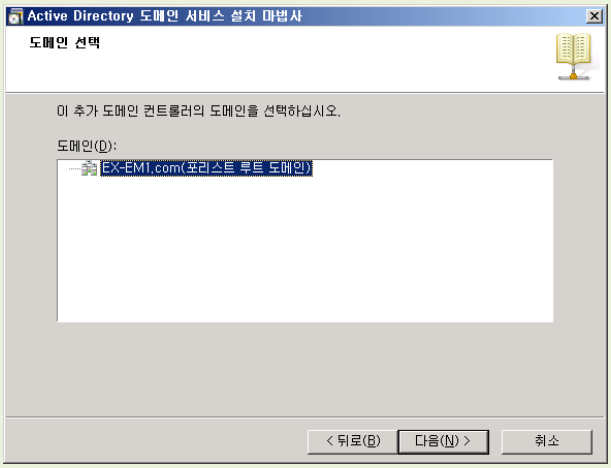


해당 AD 도메인에 JOIN 한 멤버서버의 IP 속성에 들어가서 DNS 서버란에 각각의 AD 서버 IP 를 입력해주면 된다.

AD서버 Migration(Windows Server 2003r2 → Windows Server 2008r2)

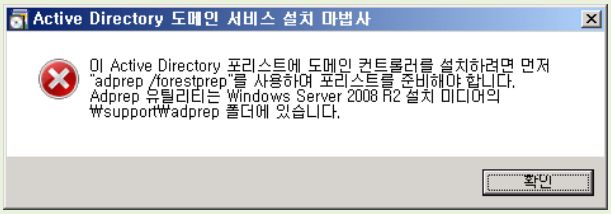


Windows Server 2003 r2 서버에 EX-EM1.com 도메인 이름으로 AD 서버가 미리 구성되어 있다.

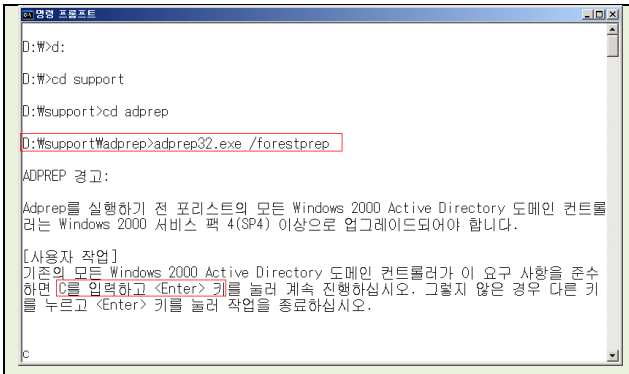


Windows Server 2008r2 서버에 Active Directory 도메인 서비스 역할을 추가하고 dcpromo.exe 를 실행시킨다.

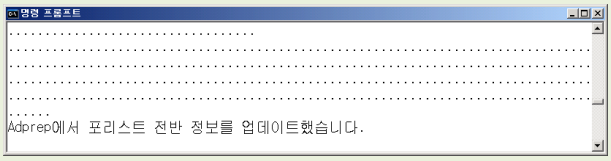
기존에 존재하는 도메인(EX-EM1.com)이 맞는지 확인한다.



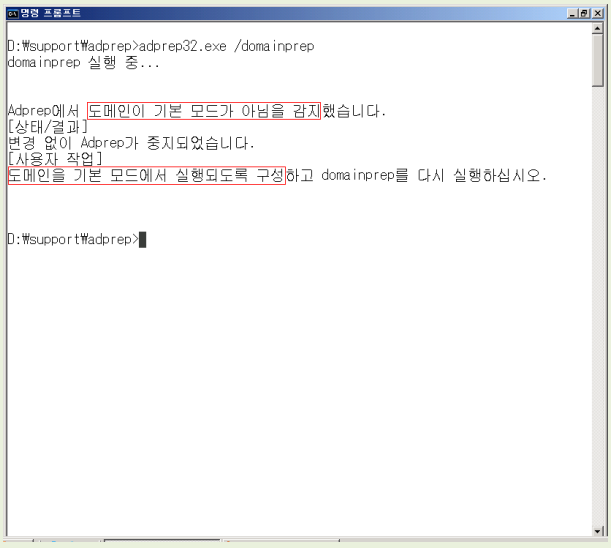
다음(N)을 선택하면 기존의 AD 서버의 도메인 컨트롤러 수준이 2003 이여서 2008r2 서버에서는 도메인 컨트롤러로 기능 수준을 올릴 수 없다는 경고 창과 함께 더 이상 진행이 불가해진다.



기존 AD 서버(2003)에서 2008r2 Media 를 삽입하고 CMD 창을 연 후 D:\support\adprep 경로로 들어가 adprep32.exe /forestprep 명령어를 입력한다.



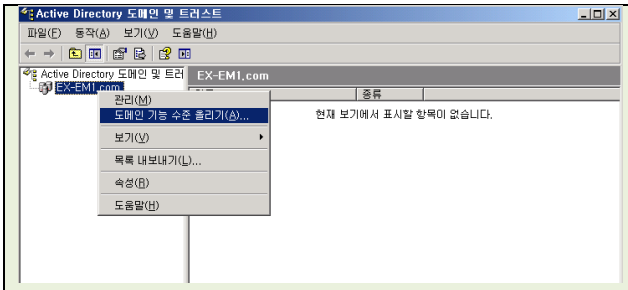
포리스트 전반 정보를 2003 에서 2008 수준으로 업데이트가 진행된다.



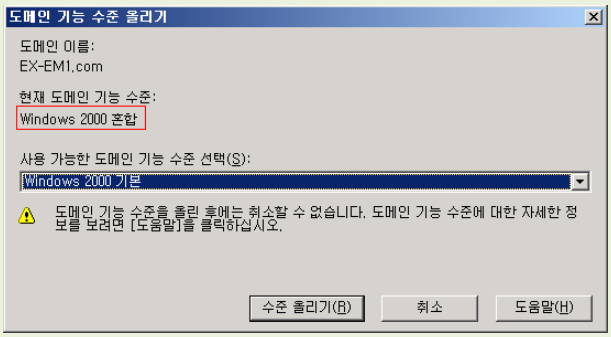
도메인 관련 정보도 2008 로 업데이트를 진행하기 위해

Adprep32.exe /domainprep 명령어를 실행시킨다.

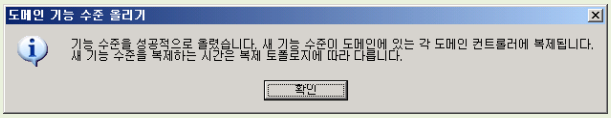
왼쪽 화면과 같은 오류가 발생할 시엔 아래 진행과정 참조



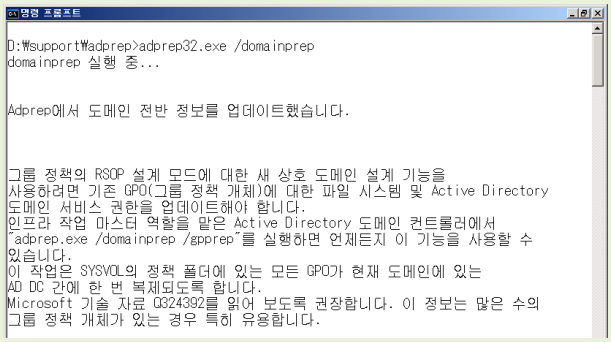
<시작> - <관리도구> - <Active Directory 도메인 및 트러스트> 에서 좌측에 해당 도메인 이름에 우 클릭 후 도메인 기능 수준 올리기(A) 를 선택한다.



도메인 기능 수준이 혼합으로 되어 있다면 사용 가능한 도메인 기능 수준 선택(S)에서 기본모드로 변경해준다.



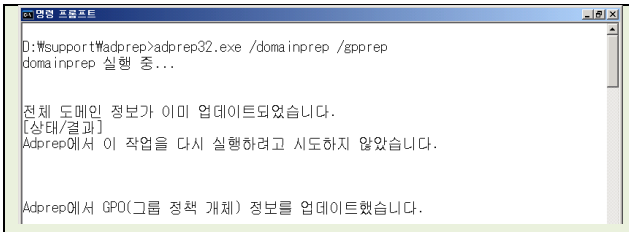
기능 수준 올리기가 성공적으로 완료되면 다시 진행한다.



명령 창에

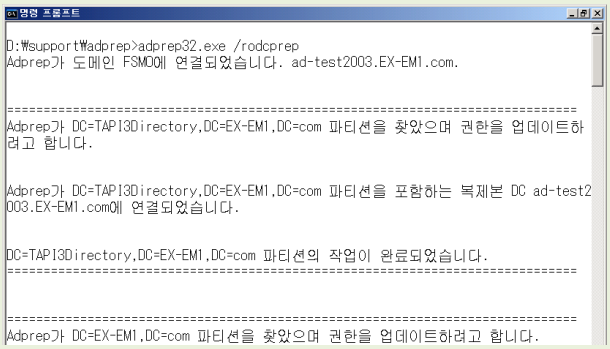
adprep32.exe /domainprep

를 입력하여 도메인 전반 정보를 업데이트 한다.



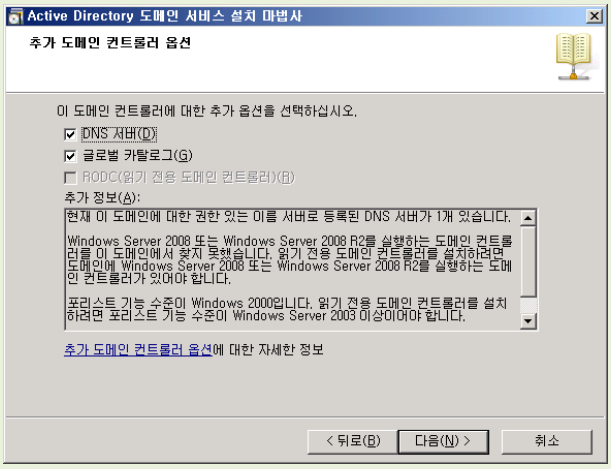
명령 창에

adprep32.exe /domainprep /gpprep 를 입력하여 도메인 그룹 정책을 업데이트 한다.

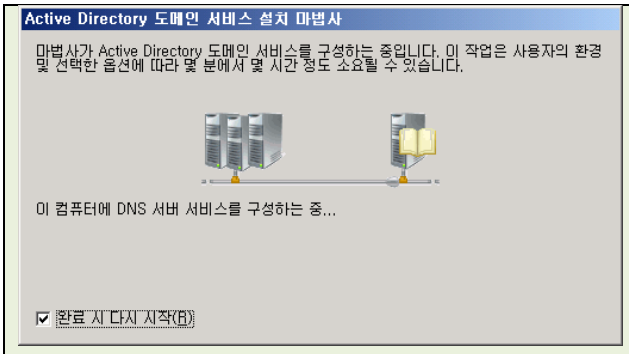


명령 창에

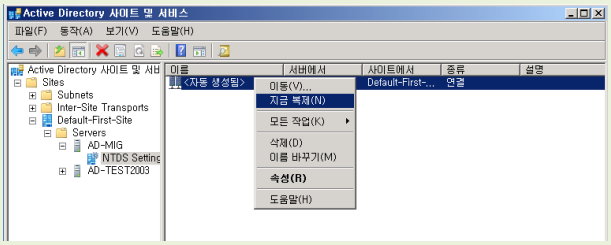
adprep32.exe /rodcprep 를 입력한다.



위와 같이 모든 업데이트를 진행한 후 다시 2008r2 서버로 돌아와 다시 dcpromo.exe 를 실행시켜 도메인 서비스 설치 마법사를 진행한다.



문제 없이 DC 구성되는 것을 확인할 수 있다.



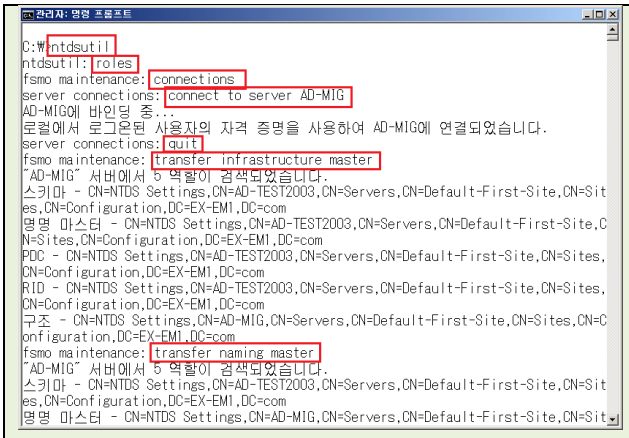
Active Directory 사이트 및 서비스 에서 좌측에

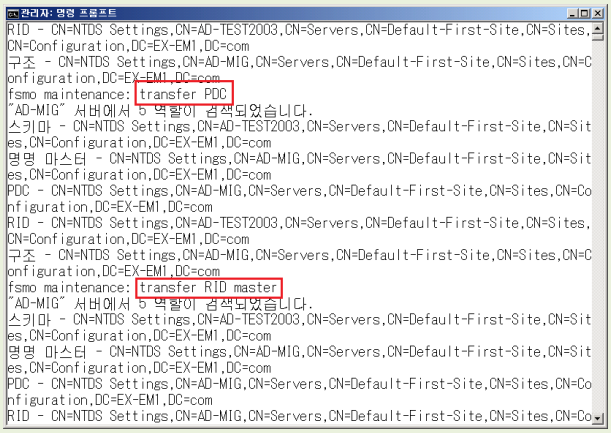
Sites – Default-First-Site – Servers – 신규 DC 명 – NTDS Settings 에서 우 클릭 후 지금 복제(N)를 선택하여 복제를 마무리 한다.

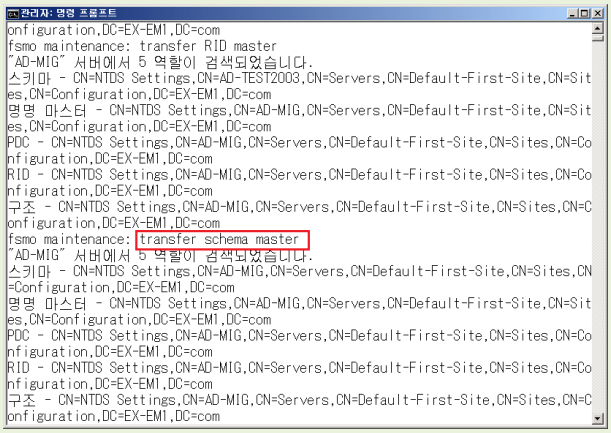
작업마스터 변경

(Windows 2003 → Windows 2008)

2008 서버 명령 프롬프트에서 netdom query fsmo 라고 입력하여 현재 작업마스터 정보를 파악한다.







명령 창에

Ntdsutil – roles – connections – connect to server '변경할 서버 명' – quit

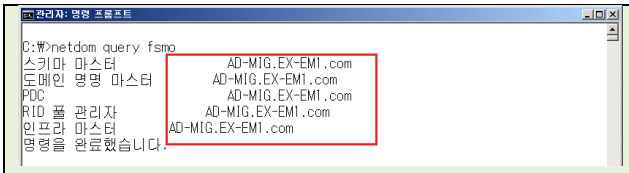
Transfer infrastructure master

Transfer naming master

Transfer PDC

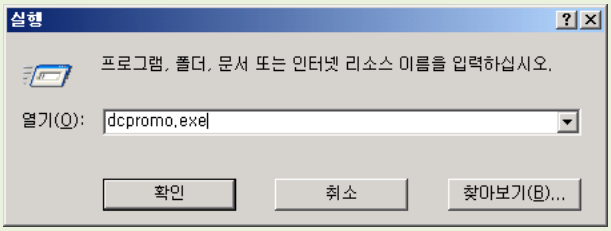
Transfer RID master

Transfer schema master 를 차례로 입력한다.



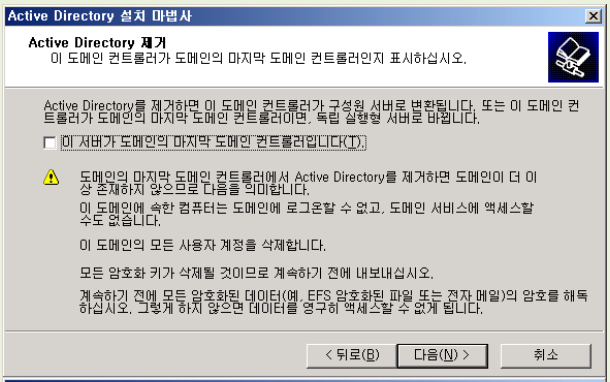
명령어에 netdom query fsmo 를 다시 입력하여

변경이 제대로 됐는지 확인한다.

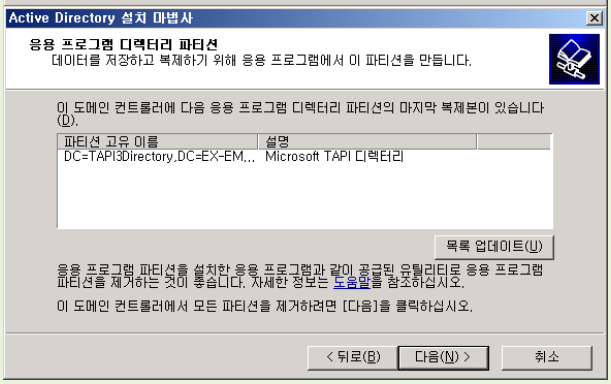


기존 AD 서버인 2003 서버에서 DC 기능 제거

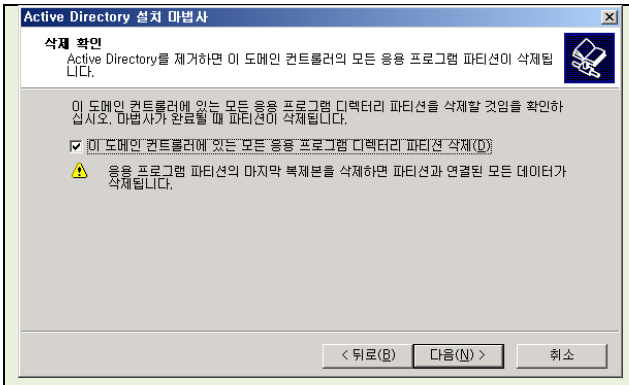
Dcpromo.exe 실행한다.



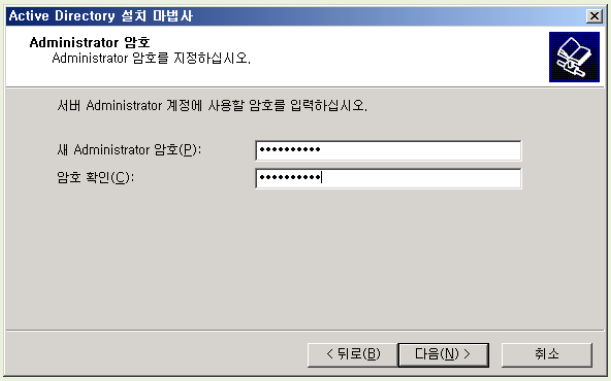
Active Directory 제거 마법사 시작한다.



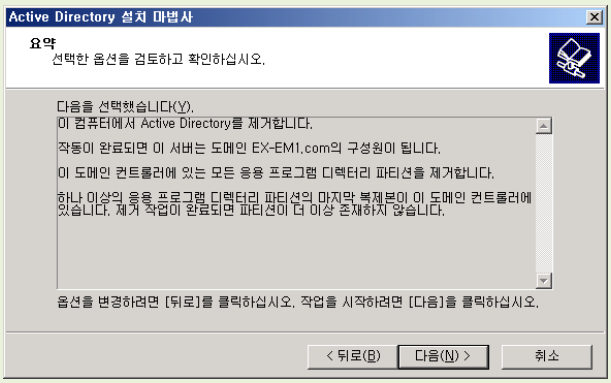
확인 후 다음(N)을 선택한다.



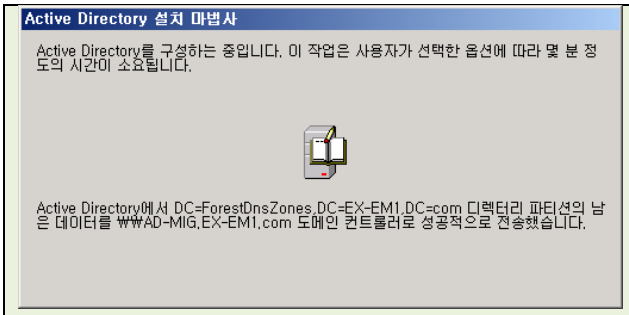
이 도메인 컨트롤러에 있는 모든 응용 프로그램 디렉터리 파티션 삭제(D)를 체크하고 다음(N)을 선택한다.



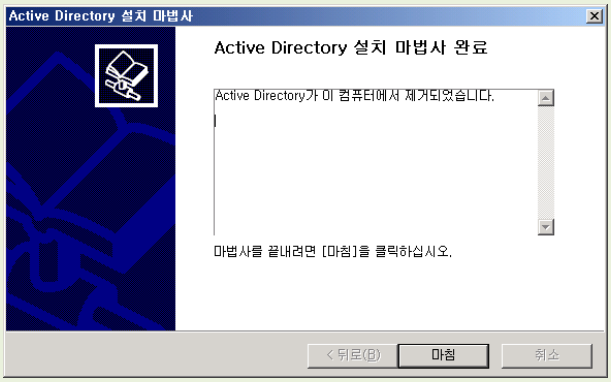
Administrator 암호를 입력한 후 다음(N)을 선택한다.



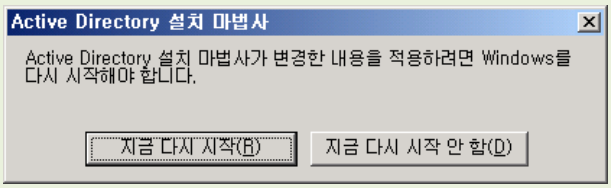
내용을 확인 후 다음(N)을 선택한다.



제거를 진행한다.



제거가 정상적으로 완료됐다.



서버를 재 시작해주면 마무리 된다.

Windows Server 2008 이상은 Windows 도메인 정보 업데이트 없이도 진행이 된다.

AD 운영 TIP

AD 를 구축해 운영하는데 있어 유용한 TIP 을 몇 가지 알려주도록 하겠다.

- 최상의 보안을 위해 컴퓨터에 관리 자격 증명으로 로그온 하지 않는다.
- AD 의 보안을 한층 더 강화하기 위해 다음 보안 지침을 구현 하는 것이 좋다.

- 각 도메인에서 Administrator 및 Guest 계정의 이름을 바꾸거나, 사용을 금지하여 도메인에 대한 공격을 방지한다.

- 모든 DC 를 잠금 장치된 방에 넣어 보호한다.

- 두 Forest 간 보안 관계를 관리하고 Forest 를 통한 보안 관리와 인증을 간소화한다.

- AD 스키마를 더 안전하게 보호하려면 Schema Admins 그룹에서 모든 사용자를 제거하고 스키마를 변경해야 할 때만 사용자를 그룹에 추가한다. 변경이 완료되면 다시 그룹에서 제거한다.

- 사용자, 그룹, 컴퓨터의 공유 리소스에 대한 액세스와 그룹 정책 필터 링을 제한한다.

- AD 관리 도구에 대해 서명이 있거나 암호화된 LDAP 트래픽 사용이 해제되지 않도록 예방한다.

- 특정 기본 그룹에 할당된 일부 기본 사용자 권한은 해당 그룹의 구성원이 도메인에서 관리자 권한을 포함한 추가 권한을 획득하게 할 수 있다. 따라서 한 조직 안에서 Enterprise Admin, Domain Admins, Account Operators, Server Operators, Print Operators 및 Backup Operators 그룹의 구성원인 사용자는 모두 동등하게 신뢰되어야 한다.

    - 최신 디렉터리 정보에 빠르게 액세스할 필요가 있는 모든 특정 영역은 Site 로 구성한다.

- 최신 AD 정보에 즉시 액세스해야 하는 영역을 별도의 Site 로 만들면 필요에 맞는 리소스를 제공 받을 수 있다.

    - 모든 Site 에 DC 를 하나 이상 배치하고 각 Site 에서 하나 이상의 DC 를 Global Catalog 로 만든다.

- 자체 DC 와 하나 이상의 Global Catalog 를 가지고 있지 않은 Site 는 다른 Site 를 통해 디렉터리 정보를 사용해야 하기 때문에 비효율적이다.

- Domain 내의 모든 트러스트 관계를 보존할 수 있도록 DC 에 대한 정기적 백업을 수행한다.

결론

지금까지 AD 에 대해 알아보는 시간을 가졌다. 아직까지는 국내 대부분의 기업에서 사내컴퓨터의 OS 로 Microsoft 사의 Windows 를 사용한다. 그러므로 AD 와 같은 디렉터리 서비스는 기업에서 정말 효과적으로 사용한다면 얼마든지 사용할 수 있고 그만큼의 장점들이 분명히 있다고 생각한다. 하지만 역시 Microsoft 의 폐쇄적인 정책으로 인해 각 각의 기업에 특성에 맞게 바꾸어 사용하지 못하고 정해진 틀에 맞추어 사용할 수 밖에 없다는 단점도 분명히 존재한다. 그렇지만 앞서 설명한대로 AD 는 기본기능에 충실한 뿐만 아니라 확장 성 및 보안정책에 큰 장점을 가지고 있기에 기업에서는 사내에서 AD 의 사용을 한번쯤 검토해보길 바라며 이 글을 마친다.