

컴퓨터 역할

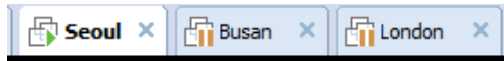
2018년 9월 12일 수요일 오후 12:34

Windows server 2008이 설치된 컴퓨터의 역할

1. Print Services(프린터 공유)
ip를 통해서 공유를 시킨다.
서버에는 비효율적으로 세팅하지 않는다.
2. File Services(ex. 공유폴더) => 50% (서버 1)
공유를 하면서 부가적인 역할도 있다.
EX) DFS : 여러 컴퓨터의 공유폴더를 하나의 공간에 보관
- ★ 3. Active Directory Domain Services(ADDS or AD) => 50% (서버1)
다중 컴퓨터 제어 기능
중앙 집중식 관리(서버 하나로 여러 컴퓨터 제어가 가능)
windows 서버를 사용하는 이유!!
4. DNS Server(서버2)
도메인을 ip로 변환시켜준다.
5. Web Server IIS
client의 요청과 server의 응답한다.
이런 과정으로 web page 접속이 가능하다.
6. Terminal Services(원격접속 서비스)
프로그램 설치만으로 접속이 가능해진다.

ADDS

2018년 9월 13일 목요일 오후 12:30



서울 = 메인 컴퓨터(DC)

부산 = 제어받는 컴퓨터(Member)

DC - 제어하는 디바이스

Member - 제어 받는 디바이스

멤버는 윈도우서버가 아니여도 client os도 가능하다.

! ★ AD환경 구성하는 법

1. 도메인을 먼저 만들어야 한다.(DC를 지정할 computer에서 만듦)
2. DC를 만든다
3. Member를 만든다.(알아서 DC와 연결된다)
4. DC와 Member 연결

• DC만드는 법

1. 서버관리자 로 이동



2. 역할 및 기능 추가

2 역할 및 기능 추가

3. 설치 유형은 역할 기반 또는 기능 기반 설치

● 역할 기반 또는 기능 기반 설치

역할, 역할 서비스 및 기능을 추가하여 단일 서버를 구성합니다.

○ 원격 데스크톱 서비스 설치

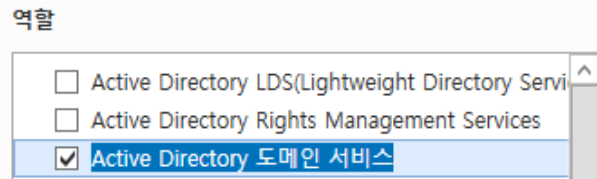
VDI(가상 데스크톱 인프라)에 필요한 역할 서비스를 설치하여 가상 컴퓨터 기반 또는 세션 기반 데스크톱 배포를 만듭니다.

4. 서버 선택

● 서버 풀에서 서버 선택

○ 가상 하드 디스크 선택

5. 서버 역할 선택(필요한 기능들은 자체적으로 선별)



6. 기능(역할을 서포터용으로 사용할 수 있는 목록)

=> 통과

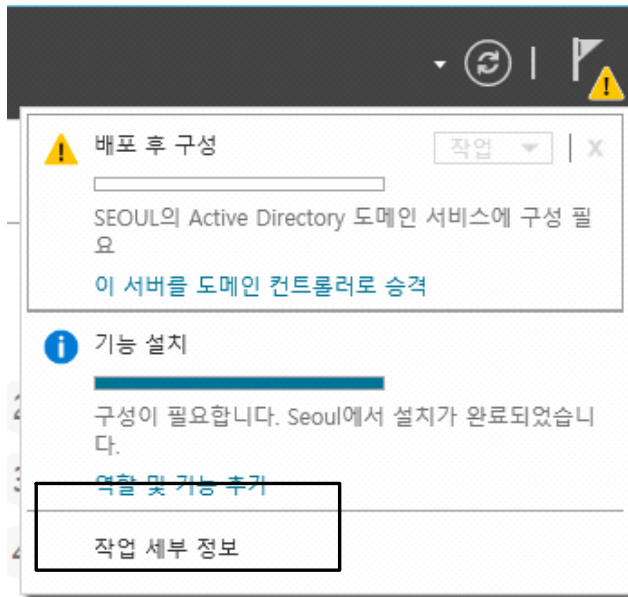
7. 도메인 컨트롤러로 승격

Active Directory 도메인 서비스

이 컴퓨터를 도메인 컨트롤러로 설정하려면 추가 단계가 필요합니다.

이 서버를 도메인 컨트롤러로 승격

* 창을 닫았을 경우 해당 아이콘을 누르면 들어갈 수 있다.



8. 배포작업을 선택

기존 도메인에 도메인 컨트롤러를 추가합니다(D).

=> **도메인이 이미** 구성되어 있을 경우 추가적인 DC를 만들어 줄 때 하나의 도메인에 여러개의 DC를 운용할 수 있다.

기존 포리스트에 새 도메인을 추가합니다(E).

=> 포리스트는 이미 구성되어 있을 경우 도메인을 추가할 때

새 포리스트를 추가합니다(F).

=> 아무것도 없는 초기 상태

※ 포리스트 ??

포리스트 > 도메인 > DC, Member

포리스트 안에 여러 도메인이 운용할 수 있고 각 도메인마다 독립적이다.

※ 루트 도메인 ??

포리스트에서 최상위에 있는 도메인

다른 도메인과 연결해서 사용할 수 있다.

최고 권한을 가진 도메인

배포 작업을 선택합니다.

- ☐ 기존 도메인에 도메인 컨트롤러를 추가합니다(D).
- ☐ 기존 포리스트에 새 도메인을 추가합니다(E).
- ☒ 새 포리스트를 추가합니다(F).

이 작업에 대한 도메인 정보를 지정합니다.

루트 도메인 이름(R):

루트 도메인 이름은 DNS를 구매한 것으로 설정해야 한다.

9. 도메인 컨트롤러 옵션

※ 기능 수준 ??

서버의 버전이 다를 때 기능 수준을 맞춰야 한다.

버전을 높일 수는 있지만 높은 버전을 낮출 수는 없다.

포리스트 기능 수준:

도메인 기능 수준:

포리스트 기능 수준 = 포리스트 구성할 때만 나오며 알아서 적용된다.

도메인 기능 수준 =

상위에 있는 도메인이 버전이 낮을 경우 높은 버전을 낮은 버전으로 맞춰야한다.

도메인 컨트롤러 기능을 지정합니다.

- ☒ DNS(Domain Name System) 서버(O)
- ☒ GC(글로벌 카탈로그)(G)
- ☐ RODC(읽기 전용 도메인 컨트롤러)(R)

DSRM(디렉터리 서비스 복원 모드) 암호를 입력합니다.

암호(D):

암호 확인(C):

PW : P@\$w0rd

10. DNS 옵션

⚠ 권한 있는 부모 영역이 없거나 권한 있는 부모 영역에서 Windows DNS 서버가 실행되고 있지 않으므로... 더 많이 표시 ✕

도메인 네임이 잘못 되서 나오는 오류

11. 추가옵션

도메인에 할당된 NetBIOS 이름을 확인하고 필요한 경우 변경합니다.

NetBIOS 도메인 이름:

도메인의 이름을 줄여서 사용할 수 있다. 자동으로 변경, '.'을 기준으로 제일 왼쪽에 있는 부분이 적용된다.

12. 경로

기본 default값 설정

설정 끝 재부팅후

ITBANK\Administrator

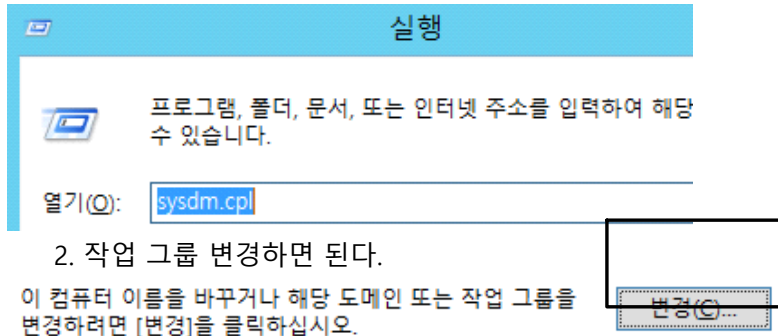
이렇게 바뀐다.

=>AD로 구성되면 DC가 ID를 통합 관리한다. 컴퓨터 이름이랑 그룹이 바뀐다.

※ DC는 항상 켜져 있어야 한다!!

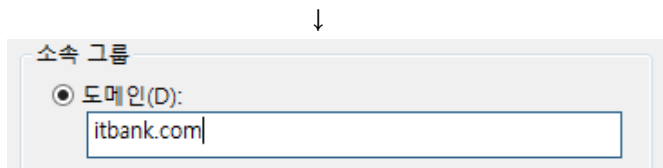
• Member 만드는 법

1. 실행창(window+R)에서 sysdm.cpl로 시스템 속성



2. 작업 그룹 변경하면 된다.

이 컴퓨터 이름을 바꾸거나 해당 도메인 또는 작업 그룹을 변경하려면 [변경]을 클릭하십시오.



※ DNS 서버는 DC IP주소로 설정해야한다.

● 다음 DNS 서버 주소 사용(E):

기본 설정 DNS 서버(P):

10 . 0 . 0 . 110

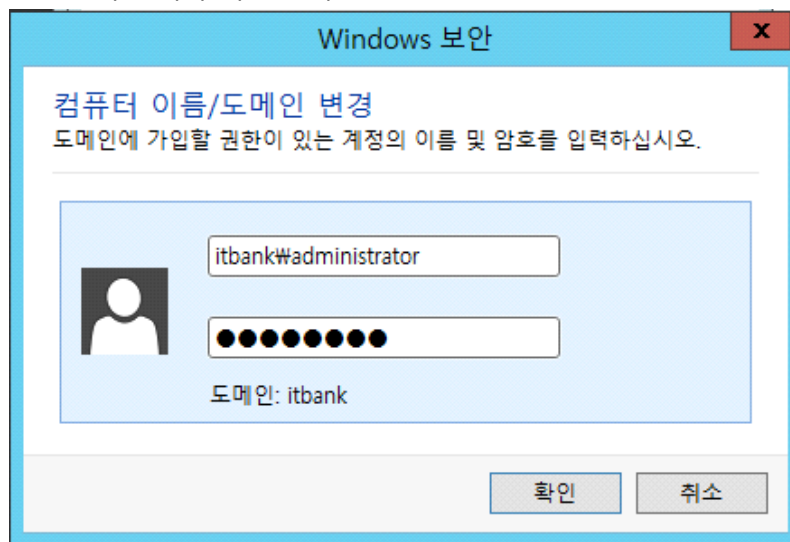
보조 DNS 서버(A):

. . .

IP 주소를 세팅하는 이유??

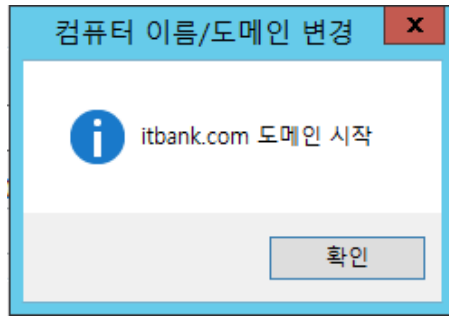
=> 해당 도메인으로 가기 위해서는 DNS서버에 물어봐야 하기 때문

3. DC의 관리자 계정 입력



PW : P@\$w0rd

4. 완료



*** 도메인 탈퇴하는 방법 : workgroup으로 변경하면 된다.**

로컬 로그인 : member computer가 member로 가입되기 전에 가지고 있던 계정(admin)으로 login하는 방식
관리자 계정, 특정 컴퓨터에 다른 세팅을 하기 위해서 관리자가 직접 가서 관리자 계정을 통해 설정한다.

↑
BUSAN#Administrator
↓

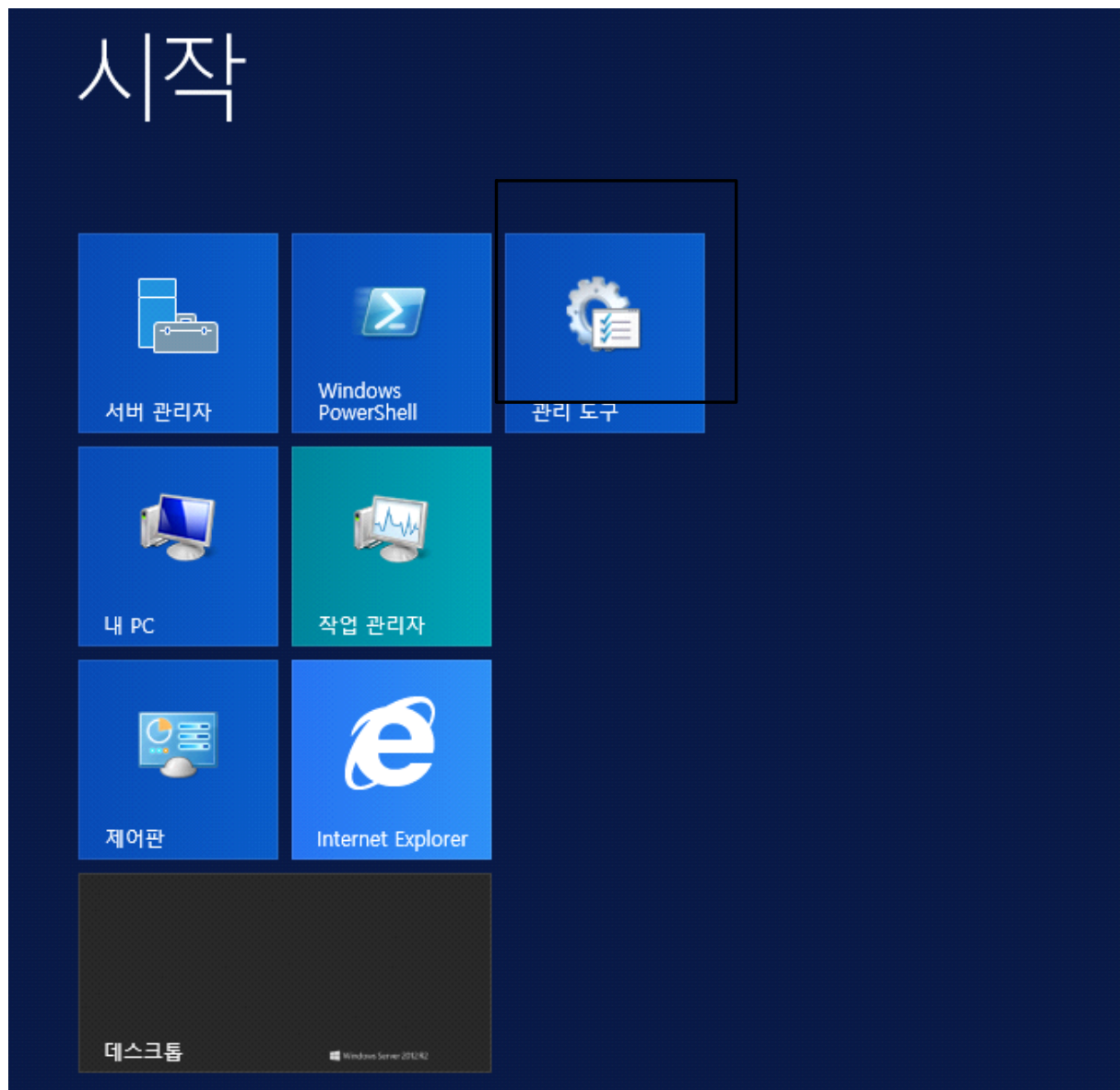
도메인 로그인 : DC가 계정을 관리,도메인에서 통합된 계정으로 Member computer 에서 Login하는 방식
앞에 컴퓨터 이름이 있다면 로컬 로그인/netbios가 있다면 도메인 로그인

itbank#administrator

=> DC(서울)로 접속

○ 사용자 만드는 법

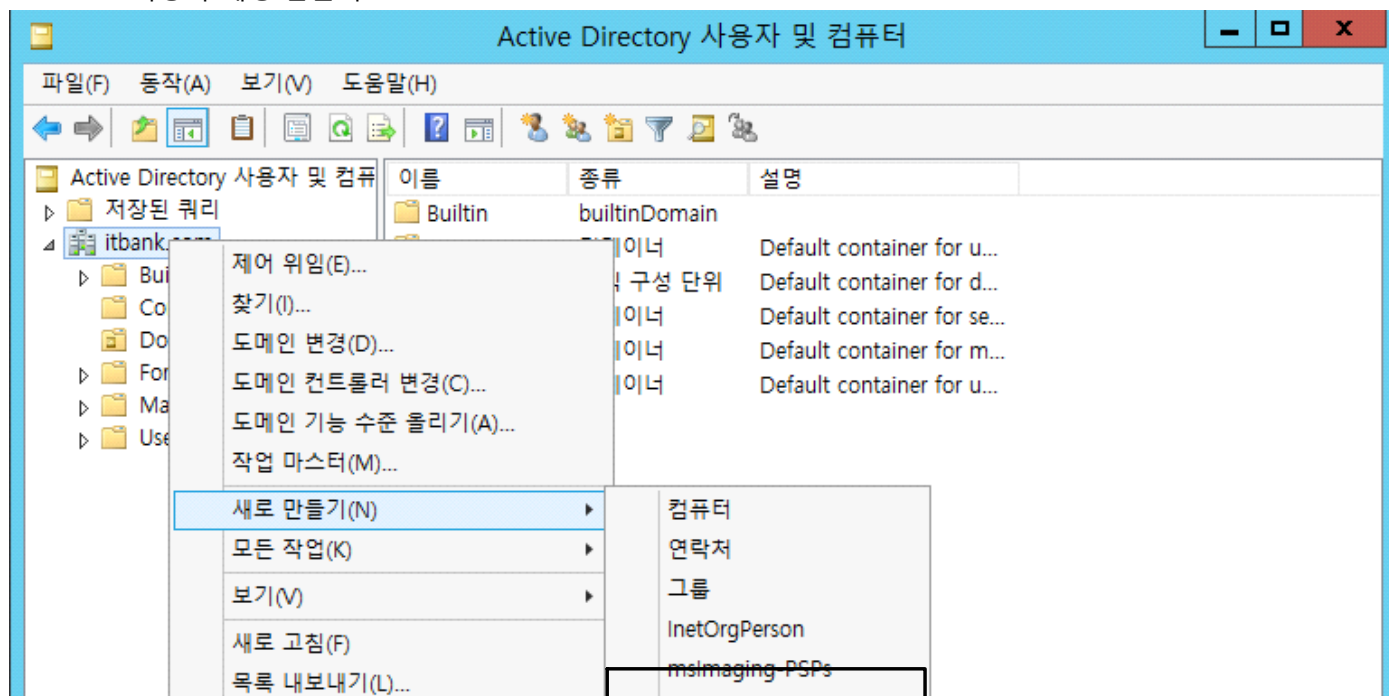
1. 관리도구로 이동(Window키 누르고)

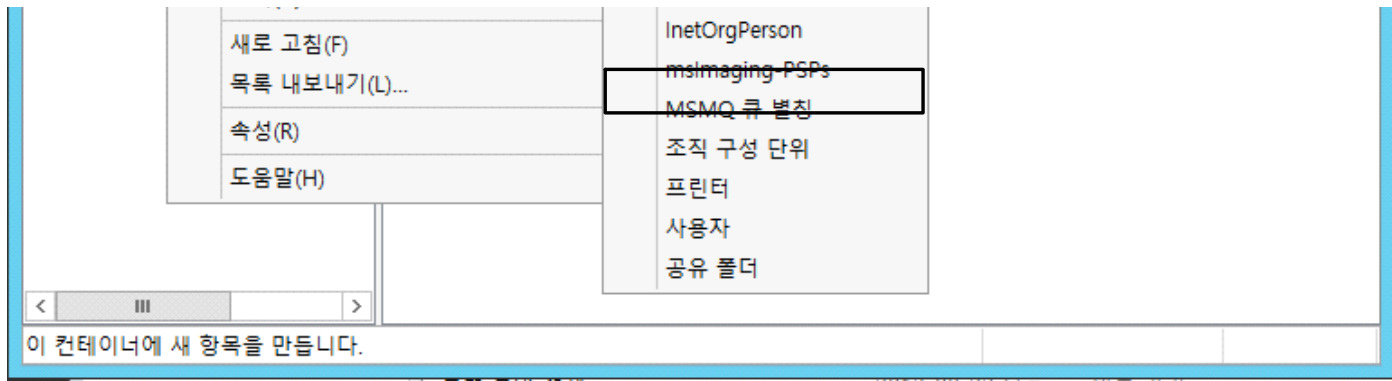


2. 계정 생성/그룹생성/그룹에 계정 삽입/계체 분류 할 수 있는 곳

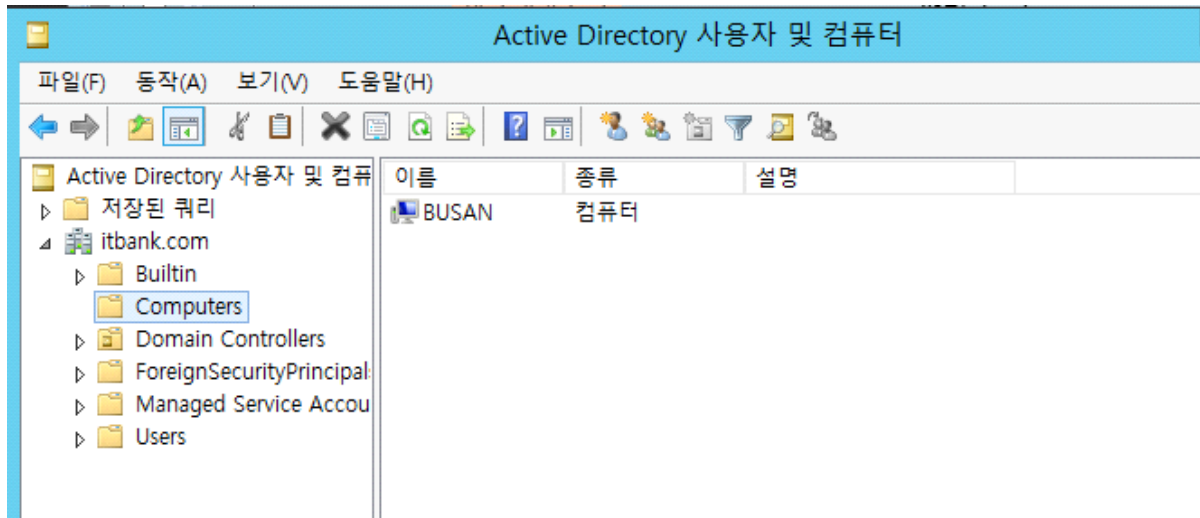
Active Directory 사용자 및 컴퓨터 2013-08-22 오후... 바로 가기

3. 사용자 계정 만들기

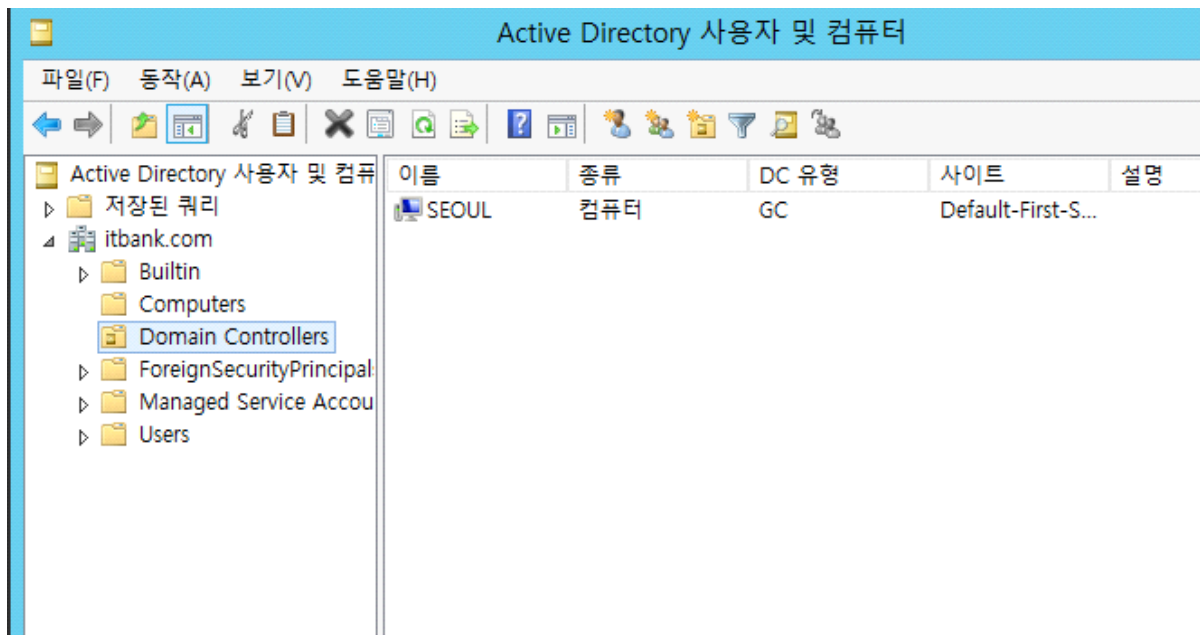




- 도메인에 멤버를 가입하면 DC에 멤버 컴퓨터가 등록된다.



- DC 컴퓨터만 저장되는 공간



○ 자식 도메인 만드는법

- ex)본사-지사와 같은 개념, 부모 도메인과 연결이 된다. 자원 공유가 가능하다.
 아이디 공유가 가능하다. 부모 도메인도 도메인 이름을 받아서 같이 사용한다.
 단, 혼동 방지를 위해 부모 도메인 이름 앞에 자신의 도메인 이름을 붙인다.
1. DNS서버는 부모 도메인의 DC IP로 설정해야한다.

☒ 다음 DNS 서버 주소 사용(E):
 기본 설정 DNS 서버(P): 10 . 0 . 0 . 110
 보조 DNS 서버(A): . . .

2. 자식 도메인을 만들때 에도 DC는 필요하다(도메인당 1개이상의 DC가 있어야한다)

3. DC만드는 법과 동일

4. 배포 작업 선택

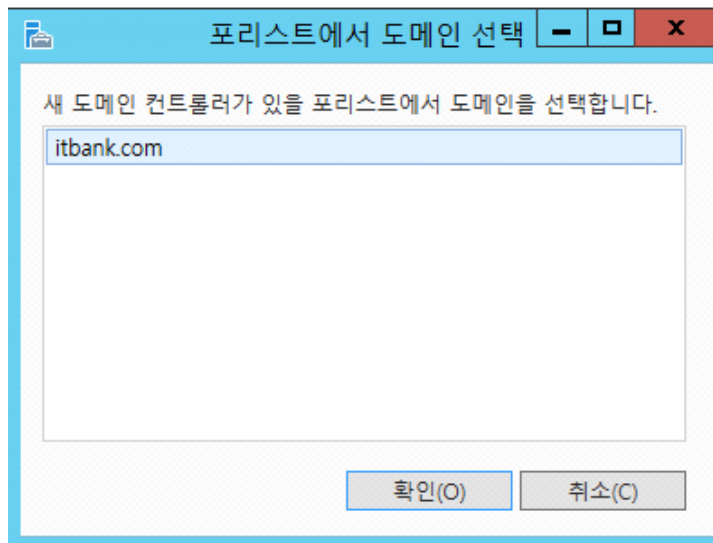
배포 작업을 선택합니다.

- ☐ 기존 도메인에 도메인 컨트롤러를 추가합니다(D).
- ☒ 기존 포리스트에 새 도메인을 추가합니다(E).
- ☐ 새 포리스트를 추가합니다(F).

이 작업에 대한 도메인 정보를 지정합니다.

도메인 유형 선택(T): 자식 도메인
 부모 도메인 이름(M): itbank.com
 새 도메인 이름(W): eu

5. 포리스트에서 도메인 선택



6. 도메인 컨트롤러 옵션

도메인 기능수준은 부모 도메인 기능 수준과 동일하거나 낮게 해주면 된다.

글로벌 카탈로그(GC) : ADDS환경에서 사용되는 각종 DB파일을 만들어서 상호 교환 및 유지 처리속도가 빨라진다.

7. 다른 설정 변경없이 설치

EUWAdministrator

8.설치 끝

부모도메인으로 자식도메인에 접속 가능 ↓

기타 사용자

●●●●●●●●
👁️ →

자식도메인의 관리자 계정으로 부모도메인 접속 불가(주종관계)

기타 사용자

사용하려는 로그인 방법이 허용되지 않습니다.
자세한 내용은 네트워크 관리자에게 문의하세요.

확인

❖ 트리도메인 : 연결되지 않는 독립적인 도메인

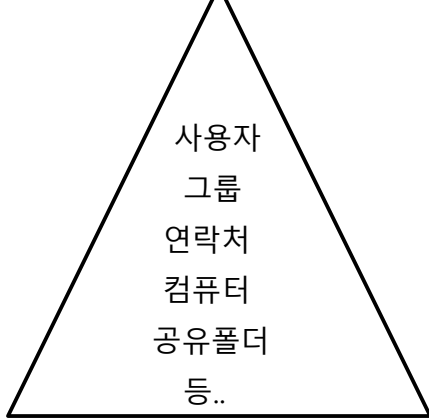
로컬 로그인은 MEMBER에서만 가능하다. DC에서는 불가능!
DC에서는 일반 사용자 계정으로 접속 불가, 관리자 계정만 가능

Domain

2018년 9월 14일 금요일 오후 12:36

Domain

- 네트워크 관리를 위한 논리적인 단위



- Windows 개체들이 포함됨
- 조직의 자원을 중앙에서 효율적으로 관리하기 위한 것
- 중앙집중식 관리 = DC(Domain controller)

DC??

- 계정이 아니라 시스템 즉, 컴퓨터

SAM(File) ??

- windows os 설치 시 기본적으로 자동으로 생성되는 파일
- 모든 사용자의 정보가 담겨있다. 관리자 계정 포함
- 삭제, 열람, 수정 불가(특별관리대상)
- 백그라운드 상에 항상 열려 있다.
- 부팅하자마자 파일이 실행된다.
- 듀얼 부팅하면 수정이 가능하다.
- 로컬 로그인과 연관있다

NTDS.dit ??

- AD환경에서의 사용자 관리 파일
- member는 보유할 수 없다.
- DC로 변경되는 순간 SAM 파일은 비활성화, 데이터는 NTDS.dit로 포워딩
- 각 도메인별로 생성된다.
- member는 sam파일은 유지(로컬 로그인 가능)

Domain 이름 표현시 주소 2가지

1. 터넷 이름 주소(DNS) itbank.edu
2. 컴퓨터 이름 구조(NetBios) ITBANK

개체관리

2018년 9월 17일 월요일 오후 12:36

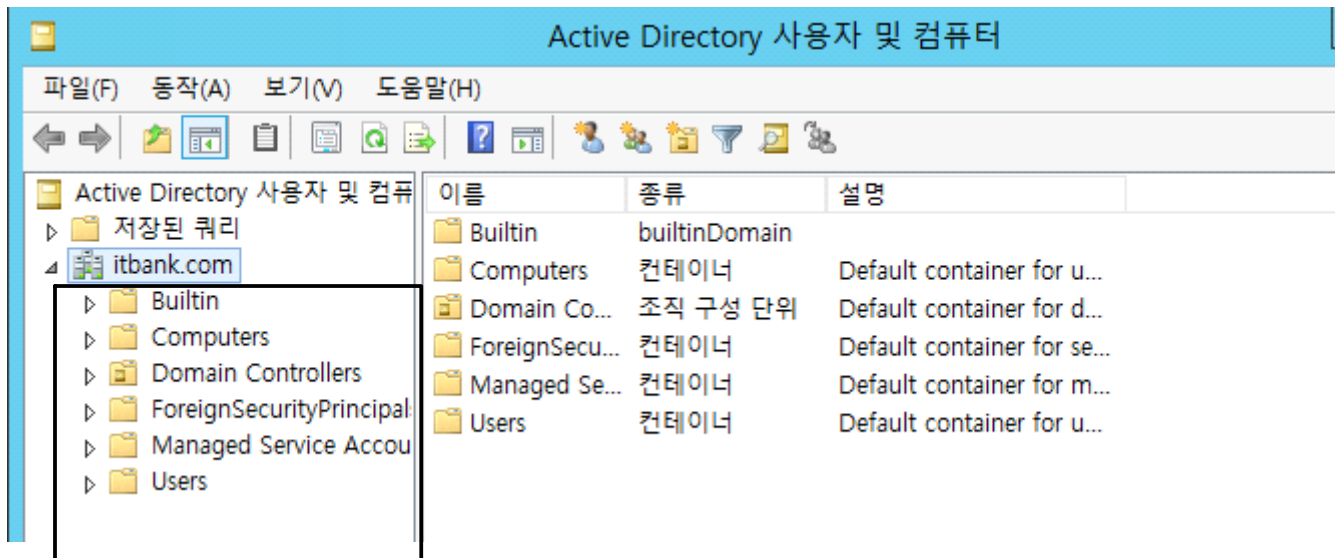
개체관리 = 사용자 관리(사용자 계정, 사용자 그룹, 컴퓨터 등..)

• 개체 관리 폴더 위치

시작 → 관리도구 → Active Directory로 시작하는 폴더, ADSI 편집

❖ 파일 속성에 대상이 있는데 마지막 부분이 원본

대상(T): %SystemRoot%\system32\dsa.msc



↑ Container(컨테이너)와 Organization Unit로 구성

- Container(컨테이너)
 - AD의 개체를 담을 수 있는 바구니/폴더
 - 새로 생성 불가능하며, 별다른 기능은 없음
 - 하위 구조 불가
 - 폴더모양
- Organization Unit(조직 구성 단위, 컨테이너의 일종)
 - AD의 관리 단위(도메인, OU)
 - 제어 위임, 정책 적용의 최소단위
 - 개체를 담을 수 있는 컨테이너 기능 + 하위 구조 가능
 - 조직의 구조를 표현이 가능(하위 구조)
 - 삭제하려면 보호체크 해제
 - 원하면 언제든지 생성 가능
 - 폴더모양 안에 다른 것이 있는게 OU

※ OU를 체계적인 관리를 위해 회사 구조와 동일하게 만들어서 관리한다.

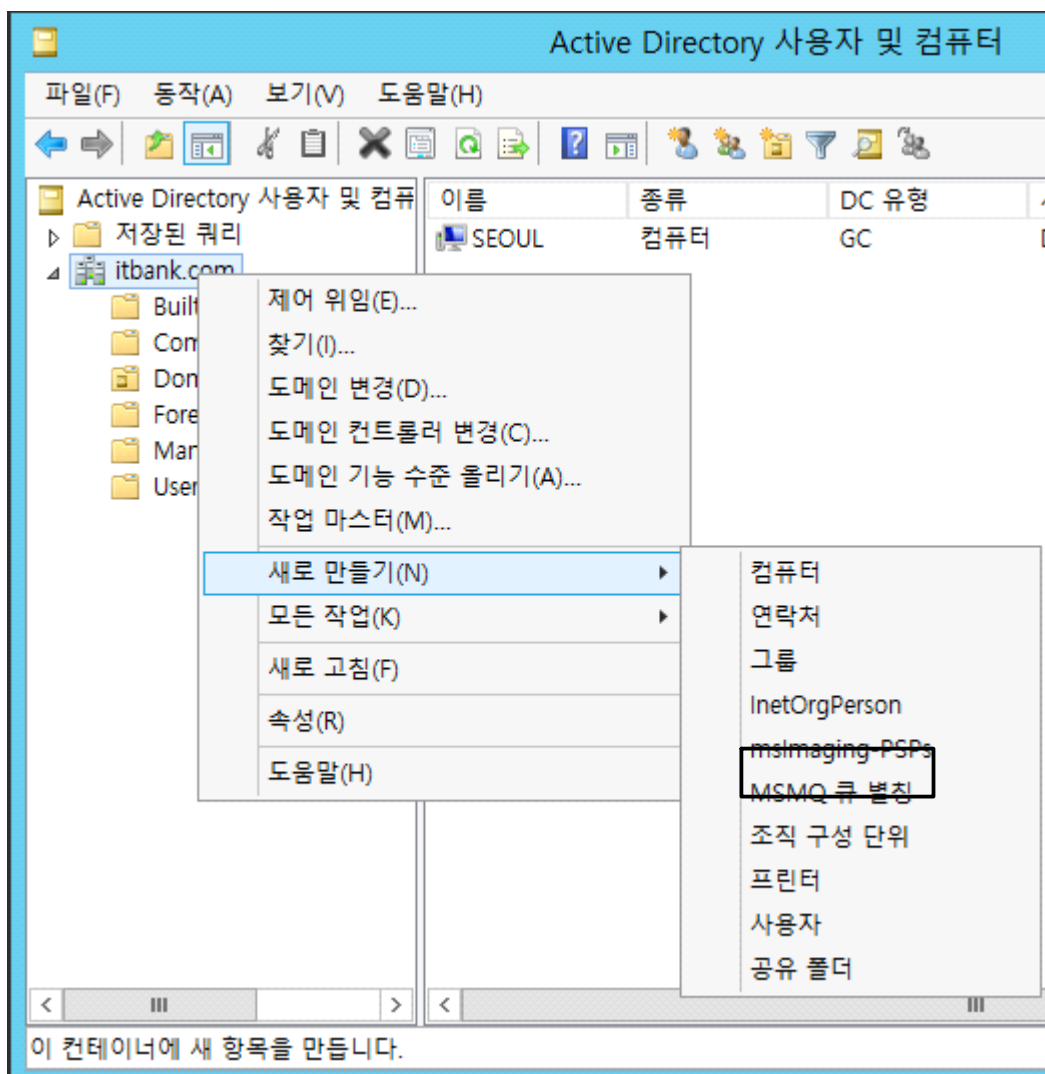
공통점 : 어떠한 개체들을 저장하는 역할

차이점 :

컨테이너		컨테이너			OU
생성유무		X			O
정책적용		X			O
하위구조		X			O

- Builtin
- Computers
- Domain Controllers
- ForeignSecurityPrincipals
- Managed Service Accounts
- Users

• OU생성 하는법



❖ OU안에 하위 OU를 만들때는 항상 어디에 만들것인지 지정을 해줘야 한다

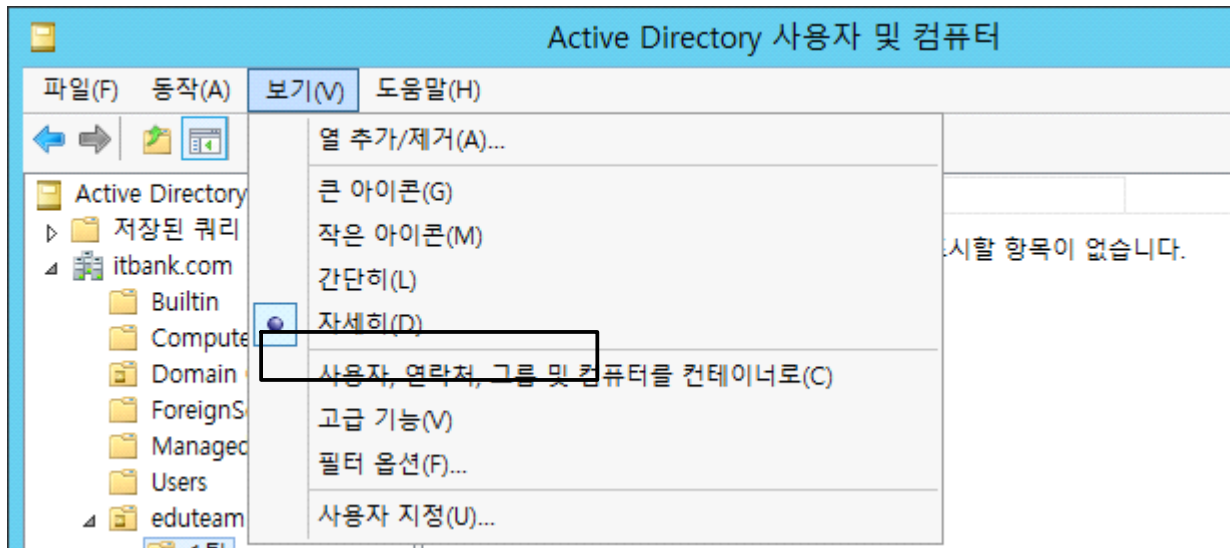
● OU삭제하는 방법

! 주의사항

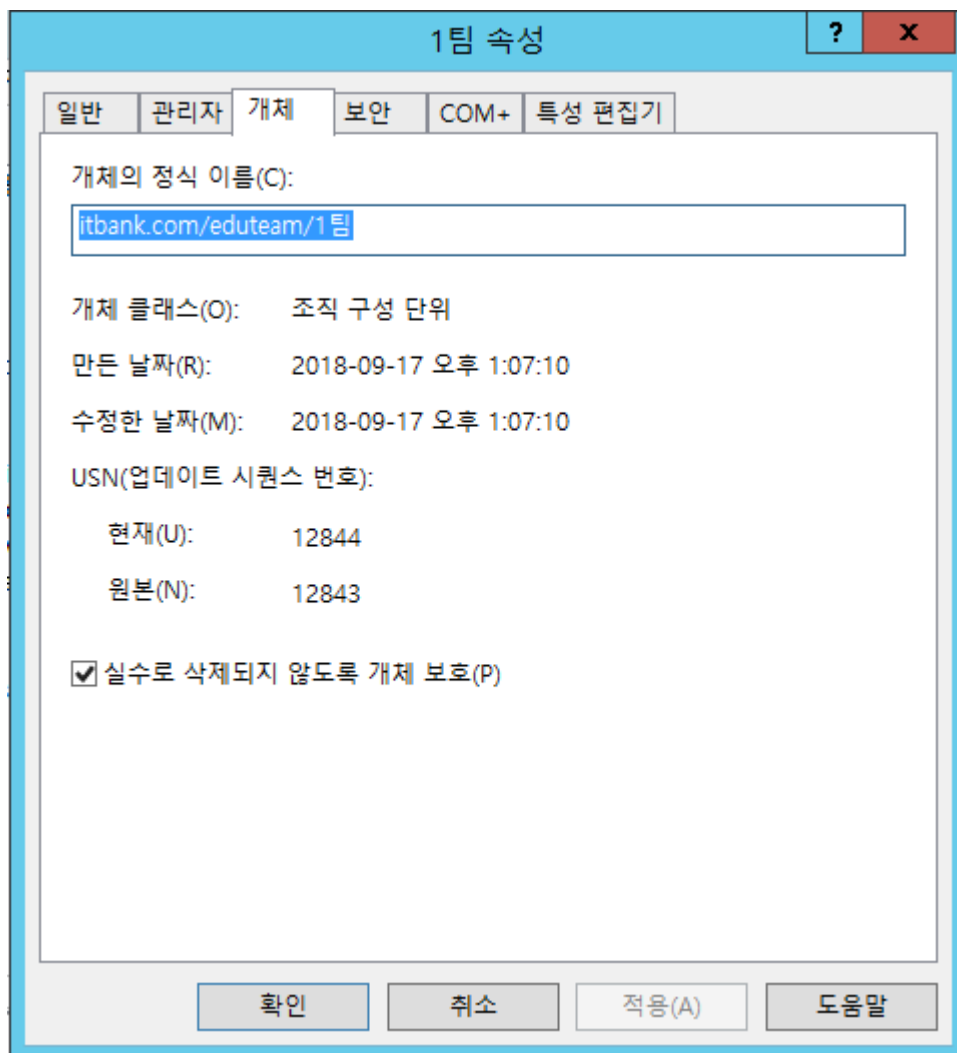
☒ 실수로 삭제되지 않도록 컨테이너 보호(P)

OU생성시 체크하면 삭제가 되지 않는다.

만약 체크하고 생성 했다면 ??

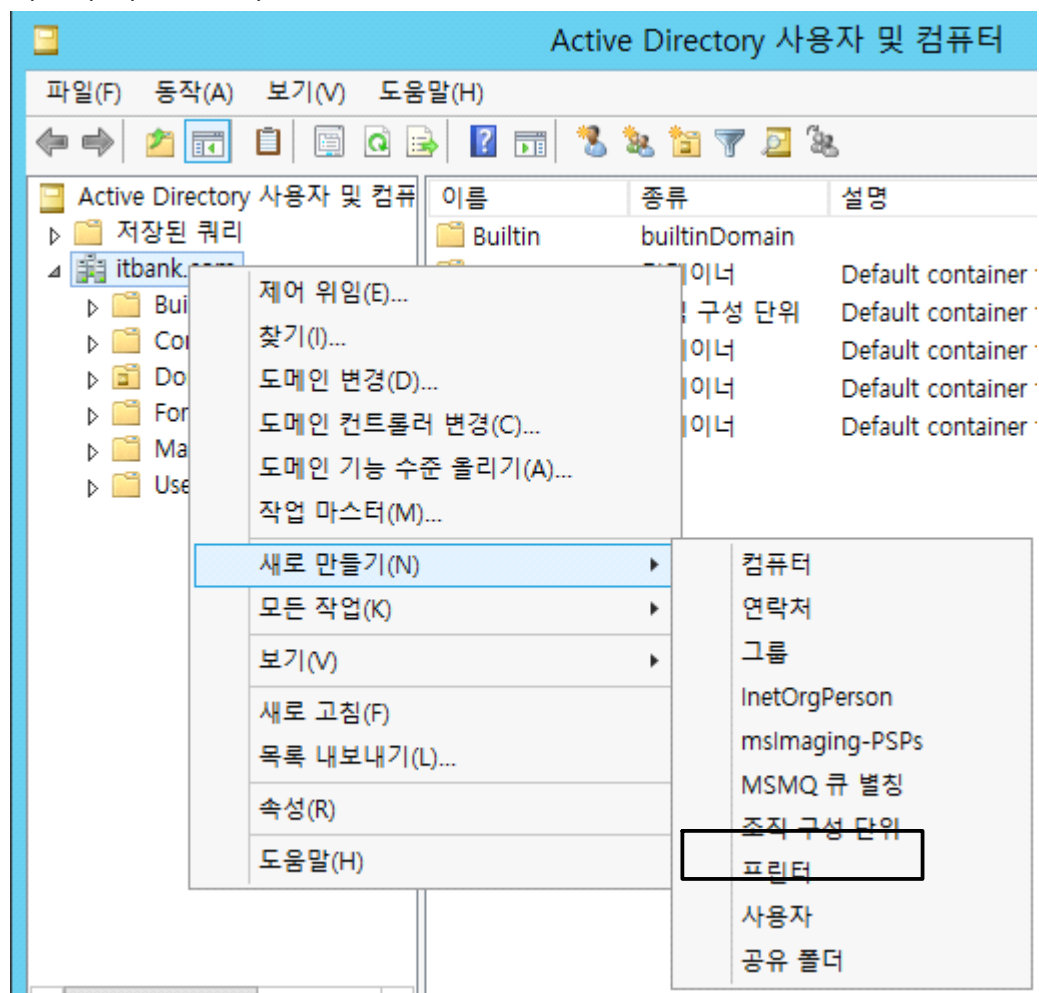


고급 기능을 누르고 삭제할 OU의 속성을 보면



이렇게 뜨니 체크 해제하고 삭제하면 삭제가 된다.

사용자 계정 생성하는 법



새 개체 - 사용자

위치: itbank.com/

성(L):

이름(F): 이니셜(I):

전체 이름(A):

사용자 로그인 이름(U): @itbank.com

Windows 2000 이전 버전 사용자 로그인 이름(W): ITBANK#

< 뒤로(B) 다음(N) > 취소

- 성
- 이름
- 이니셜

❖ 계정의 이름일 뿐 아이디는 아니다

- 사용자 로그인 이름 -> 로그인 할때 아이디

사용자 로그인 이름(U):

s1 @itbank.com

Windows 2000 이전 버전 사용자 로그인 이름(W):

ITBANK# s1

← UPN방식

← Windows 2000이전

사원들에게는 UPM방식으로 알려주는게 편하다.

ii) itbankws1 : 도메인의 NetBios Name 사용 (도메인 유일 이름)

iii) s1@itbank.edu : UPN **User Principal Name**
s1@itbank.com

집중적으로 연습하라

- ☒ 다음 로그인 시 사용자가 반드시 암호를 변경해야 함(M)
- ☐ 사용자가 암호를 변경할 수 없음(S)
- ☐ 암호 사용 기간 제한 없음(W)
- ☐ 계정 사용 안 함(O)

☒ 다음 로그인 시 사용자가 반드시 암호를 변경해야 함(M)

-> 초기에는 관리자가 지정, 이후에는 사용자가 변경

☐ 사용자가 암호를 변경할 수 없음(S)

-> 사용X, 영구적으로 변경 불가, 공용계정시 사용

☐ 암호 사용 기간 제한 없음(W)

-> 사용 X, 적정 사용기간은 3달, 공용계정시 사용

☐ 계정 사용 안 함(O)

-> 당장 사용하지 않을 경우

공용계정은 사용하지 않는다.

❖ 사용자 계정 로그인 시간 설정

ST 속성

환경	세션	원격 제어	원격 데스크톱 서비스 프로필
일반	주소	계정	프로필
주소	계정	프로필	전화
계정	프로필	전화	조직
프로필	전화	조직	소속 그룹
전화	조직	소속 그룹	전화 접수

사용자 로그인 이름(U):
s1 @itbank.com

Windows 2000 이전 버전 사용자 로그인 이름(W):
ITBANKW s1

로그온 시간(L)... 로그인 대상(T)...

ST에 대한 로그인 시간

12 · 2 · 4 · 6 · 8 · 10 · 12 · 2 · 4 · 6 · 8 · 10 · 12

모두	일요일	월요일	화요일	수요일	목요일	금요일	토요일
일요일	●	●	●	●	●	●	●
월요일	●	●	●	●	●	●	●
화요일	●	●	●	●	●	●	●
수요일	●	●	●	●	●	●	●
목요일	●	●	●	●	●	●	●
금요일	●	●	●	●	●	●	●
토요일	●	●	●	●	●	●	●

일요일부터 토요일, 오전 12:00부터 오전 12:00까지

확인 취소

● 허용된 로그인(P)
○ 거부된 로그인(D)

계정의 로그인 시간대를 정할 수 있다.

지정 컴퓨터 설정

ST 속성

환경	세션	원격 제어	원격 데스크톱 서비스 프로파일	
일반	주소	계정	프로필	전화
			조직	소속 그룹
			전화 접	

사용자 로그인 이름(U):

Windows 2000 이전 버전 사용자 로그인 이름(W):

로그인 워크스테이션 ? X

컴퓨터 이름에 컴퓨터의 NetBIOS 또는 DNS(Domain Name System) 이름을 입력하십시오.

이 사용자의 로그인 대상:

☐ 모든 컴퓨터(C)

☒ 다음 컴퓨터(T)

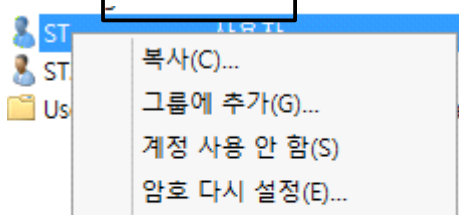
컴퓨터 이름(O):

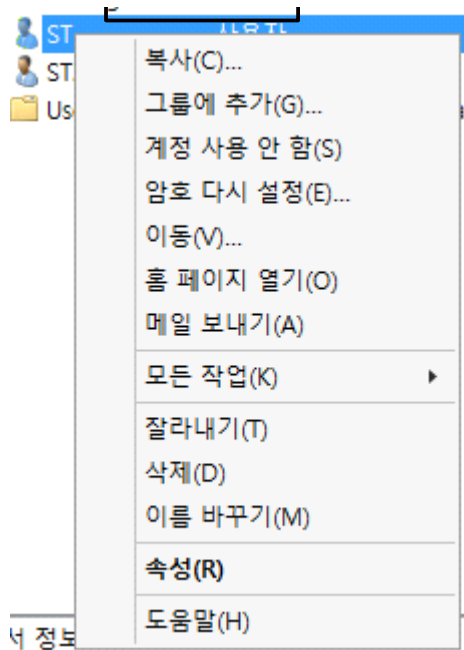
해당 컴퓨터에만 설정가능
컴퓨터 계정명을 입력하면 된다.

● 계정 복사

템플릿??

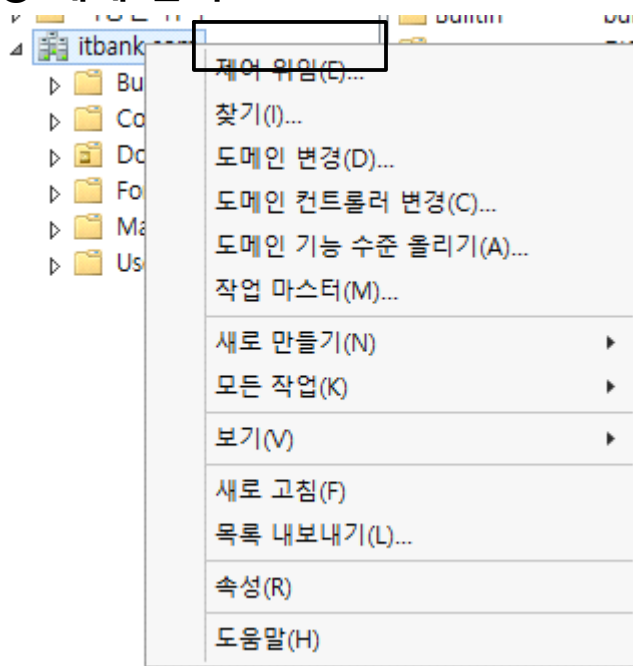
A라는 정보를 토대로 새로운 것을 만드는 것(단, A는 그대로 유지)





사용 중인 계정을 복사하지 않고 템플릿 계정을 만들어서 그 계정을 템플릿 한다.

● 개체 검색



사용자, 연락처, 그룹 찾기

파일(F) 편집(E) 보기(V)

찾기(D): 사용자, 연락처, 그룹 위치(N): itbank.com

찾아보기(B)...

사용자, 연락처, 그룹 고급


이름(A):

설명(R):

지금 찾기(I)

중지(P)

모두 지우기(C)



OR

사용자, 연락처, 그룹 찾기

파일(F) 편집(E) 보기(V)

찾기(D): 사용자, 연락처, 그룹 위치(N): itbank.com

찾아보기(B)...

사용자, 연락처, 그룹 고급

필드(L) 조건(T): 값(U):

조건 목록(O):


추가(A) 제거(R)

<위의 조건을 이 목록에 추가>

지금 찾기(I)

중지(P)

모두 지우기(C)



필드를 통해 조건을 입력하고 해당 조건에 부합하는 것들만 찾을 수 있다.

사용자, 연락처, 그룹 찾기

파일(F) 편집(E) 보기(V)

찾기(D): 사용자, 연락처, 그룹 위치(N): eu.itbank.com

찾아보기(B)...

사용자, 연락처, 그룹 고급

이름(A):

설명(R):

지금 찾기(I)

중지(P)

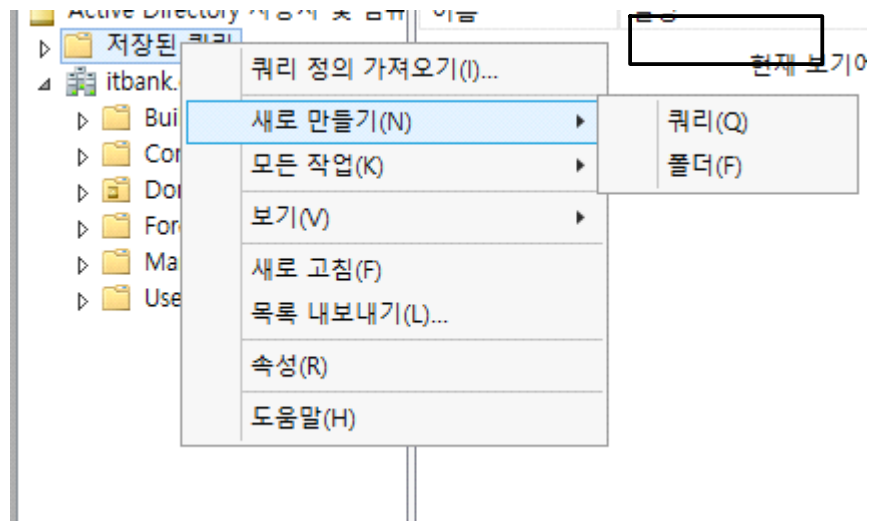
모두 지우기(C)

위치만 변경하면 자식 도메인의 파일들도 찾을 수 있다.

● 저장된 쿼리

조건 검색한 결과를 저장할 수 있는 곳

동일한 조건으로 수시로 검색 할경우 쿼리를 활용하면 편하다



쿼리 활용 법

새 쿼리

?

x

이름(N):

계정 사용 안함 찾기 쿼리

설명(D):

비활성화 계정 찾는 쿼리

쿼리 루트(Q):

...Witbank

찾아보기(B)...

☒ 하위 컨테이너 포함(S)

쿼리 문자열(U):

쿼리 정의(E)...

일반 쿼리 찾기

찾기(D): 일반 쿼리

사용자

컴퓨터

그룹

쿼리의 변수를 정의하십시오.

이름(A):

설명(R):

☒ 계정 사용 안 함(U)

☐ 암호 사용 기간 제한 없음(O)

마지막 로그인한 후 지난 시간(일)(T):

확인

↑ 쿼리 정의를 통한 검색설정

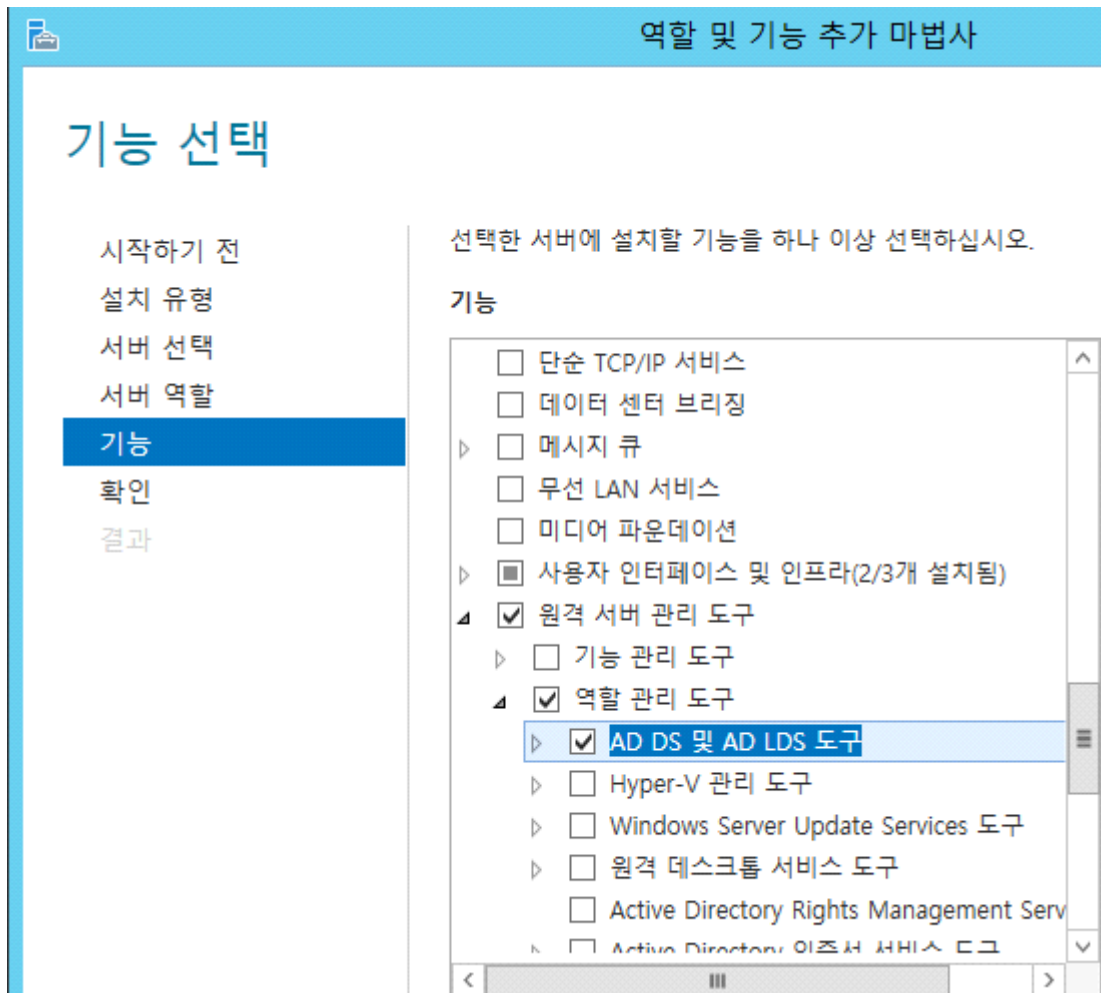
AD 관리도구는 DC가 아닌 다른 곳에서도 활용할 수 있다.

1. DC에서 사용자의 계정을 만들고 member에서 해당 계정으로 로그인을 한다.
2. DC의 관리자 계정으로 member에 접속
3. 역할 및 기능 추가를 열어서 기능 탭에 보면 원격서버 관리도구를 열어서 adds 및 ad lds 도구만 체크

빠른 시작(Q)

1 이 로컬 서버 구성

2 역할 및 기능 추가



• 일반사용자계정에서 사용자 생성/관리하게 만드는 법

1. DC에서 Builtin에 들어가서 Account Operators(특수 그룹)

계정을 Account Operators에 저장하면 사용자계정에도 사용자계정관리를 할 수 있다.

이 방법은 권한까지 주는 방법

2. OU를 만들고 우클릭하면 제어 위임 선택

해당 OU에 제어 위임할 계정을 선택

해당 계정에 어떤 작업 권한을 위임할 것인지 선택

제어위임???

-> Account Operators에 저장된 계정은 모든 권한이 생기지만 제어위임을 활용하면 해당 OU에서만 작업을 할 수 있다.

커맨드 작업(개체관리)

2018년 9월 18일 화요일 오후 12:40

LDAP DN

- cn : Common Name
OU도 아니고 Domain이 아닌 모든 것
ex) 사용자계정,그룹,컨테이너 등...
itbank.com-test(OU)-s1(계정)
=> cn=s1,ou=test,dc=itbank,dc=com
- dc : Domain Component(도메인 이름)
'.'을 기점으로 분할 해야 한다.
ex) itbank.com : dc=itbank, dc=com
eu.itbank.com : dc=eu,dc=itbank,dc=com
띄어쓰기하면 안된다.(명령어가 끝난 것으로 인식)
- ou : Organization unit
ex) itbank.com - TEST(OU)
=> ou=TEST,dc=itbank,dc=com

처음부터 끝까지 경로를 다 적어 줘야한다.

Ex)cn=s1,dc=itbank,dc=edu
=> s1의 계정은 itbank.edu에 존재

• AD 개체 생성 및 삭제 명령어

dsadd : 생성

```
dsadd computer - 디렉터리에 컴퓨터를 추가합니다.  
dsadd contact - 디렉터리에 연락처를 추가합니다.  
dsadd group - 디렉터리에 그룹을 추가합니다.  
dsadd ou - 디렉터리에 조직 구성 단위를 추가합니다.  
dsadd user - 디렉터리에 사용자를 추가합니다.  
dsadd quota - 디렉터리 파티션에 할당량 사양을 추가합니다.
```

dsmove : 이동 및 이름변경

dsrm : 개체 삭제

dsmod : 개체 속성값 변경할 때, 수정

dsquery : 호출

명령어 보는 방법 : 명령어 /?(단계별 도움말을 제공)

구문 : 명령어의 사용 형식

```
구문: dsadd ou <조직 구성 단위 DN> [-desc <설명>]  
      [ <-s <서버> | -d <도메인>> ] [ -u <사용자 이름> ]  
      [ -p <<암호> | * > ] [ -q ] [ <-uc | -uco | -uci> ]
```

- <> : 필수적으로 입력

- [] : 옵션

- { } : 선택

Cmd 창 삭제 : cls

1. OU생성 : eduteam

```
C:\Users\Administrator>dsadd ou ou=eduteam,dc=itbank,dc=com -desc "test OU"  
dsadd 성공:ou=eduteam,dc=itbank,dc=com
```

2. 사용자 생성

Cn=s1 / UPN s1@itbank.com / 암호 P@\$w0rd

Cn=s2 / UPN s2@itbank.com / 암호 P@\$w0rd

```
C:\WUsers\Administrator>dsadd user cn=s1,dc=itbank,dc=com -upn s1@itbank.com -pwd
P@$w0rd
dsadd 성공:cn=s1,dc=itbank,dc=com

C:\WUsers\Administrator>dsadd user cn=s2,dc=itbank,dc=com -upn s2@itbank.com -pwd
P@$w0rd
dsadd 성공:cn=s2,dc=itbank,dc=com
```

3. 개체 이동

s1 > users

s2 > eduteam

```
C:\WUsers\Administrator>dsmove "cn=s1,dc=itbank,dc=com" -newparent cn=users,dc=it
bank,dc=com
dsmove 성공:cn=s1,dc=itbank,dc=com

C:\WUsers\Administrator>dsmove "cn=s2,dc=itbank,dc=com" -newparent ou=eduteam,dc=
itbank,dc=com"
dsmove 성공:cn=s2,dc=itbank,dc=com
```

4. 개체 이름 변경

s1 > s3

```
C:\WUsers\Administrator>dsmove "cn=s1,cn=users,dc=itbank,dc=com" -newname "s3"
dsmove 성공:cn=s1,cn=users,dc=itbank,dc=com
```

5. 계정 삭제

s3,s2삭제

```
C:\WUsers\Administrator>dsrcm cn=s3,cn=users,dc=itbank,dc=com
cn=s3,cn=users,dc=itbank,dc=com을<를> 삭제하시겠습니까<Y/N>? y
dsrcm 성공:cn=s3,cn=users,dc=itbank,dc=com

C:\WUsers\Administrator>dsrcm cn=s2,ou=eduteam,dc=itbank,dc=com
cn=s2,ou=eduteam,dc=itbank,dc=com을<를> 삭제하시겠습니까<Y/N>? y
dsrcm 성공:cn=s2,ou=eduteam,dc=itbank,dc=com
```

- noprompt(자동삭제모드) 적극 활용할 것!

삭제시 삭제여부를 물어보지만 커맨드 작성시 noprompt를 옵션으로 넣으면 물어보지 않는다.

6. 연속된 계정 생성하기

- eduteam(OU) > 1. test(OU) > 2. p10~20생성

1. test(OU) 생성

```
C:\WUsers\Administrator>dsadd ou ou=test,ou=eduteam,dc=itbank,dc=com
dsadd 성공:ou=test,ou=eduteam,dc=itbank,dc=com
```

2. p10~20생성

```
C:\WUsers\Administrator>for /L %N in (10,1,20) do dsadd user cn=p%N,ou=test,ou=ed
uteam,dc=itbank,dc=com -upn p%N@itbank.com -pwd P@$w0rd
```

For : 지정한 회수 만큼 반복

/L : for와 세트

%n : 변수(%는 반드시 붙이되 n은 임의값),(메모리에 공간을 만들어 데이터를 입력하고 사용)

in (10,1,20) : (초기값,증가값,최종값),(일정 공간에 10을 넣어 실행)

do : 실행하라

7. 연속된 계정 삭제하기

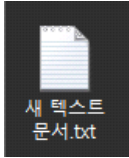
- eduteam(OU) > 1. test(OU) > 2. p10~20삭제

```
C:\WUsers\Administrator>for /L %N in (10,1,20) do dsrcm cn=p%N,ou=test,ou=eduteam,
dc=itbank,dc=com -noprompt
```

※dsrcm user cn= -> 삭제할때 user를 사용하지 않는다.

• 배치파일(=실행파일)

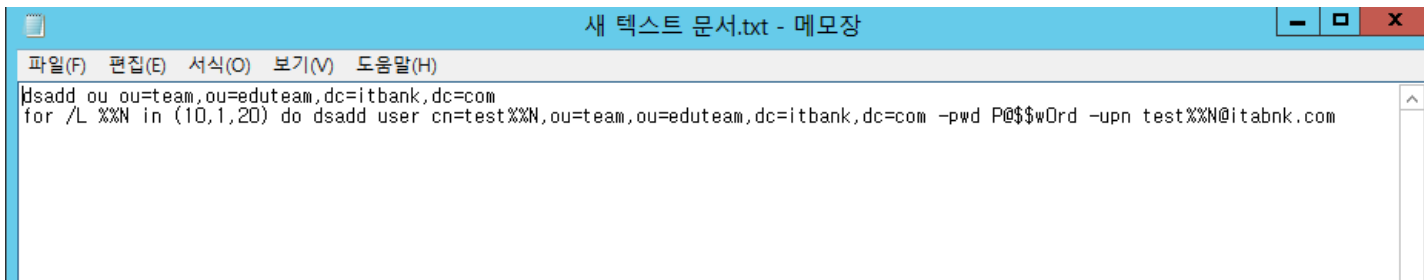
- 명령어 자체를 실행파일로 만들 수 있다.
- 확장자만 변경해주면 된다.
- 특히 배치할 때 자주 사용한다.
- 순차적으로 명령어를 파일로 만든 것이기 때문에 파일 실행만하면 해당 명령어가 실행된다.
- 반드시 확장자가 보여야 한다. 보이지 않으면 제대로 설정 할 수 가 없다.



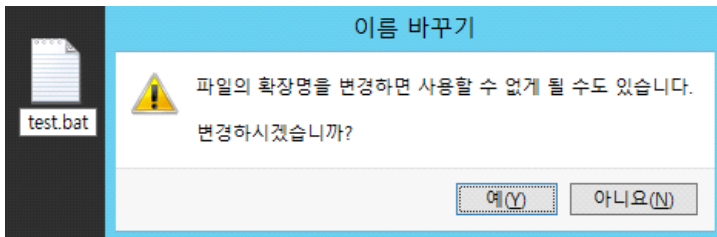
- 배치파일 만들 때는 %사용시에는 반드시 두개(%%)를 붙여줘야 한다.
for /L %%N in (10,1,20) do dsadd user cn=test%%N,

- 만드는 법 -

1. 메모장에 원하는 결과가 나오도록 순서대로 적어준다.



2. 확장자를 변경해준다



- 실행 결과 확인 방법 -

명령어 사이에 pause를 입력해준다.

```
dsadd ou ou=team,ou=eduteam,dc=itbank,dc=com
pause
for /L %%N in (10,1,20) do dsadd user cn=test:
pause
```

<실습>

Dsadd이용, for문이용, bat파일이용

Eduteam > x10~20 사용자생성
y10~20
z10~20

[옵션]

Upn > 계정이름 같게 >x10@itbank.com

암호 > P@\$\$w0rd

계정생성.bat

```
for /L %%N in (10,1,20) do dsadd user cn=%%N,ou=eduteam,dc=itbank,dc=com -upn x%%N@itbank.com -pwd P@$$w0rd
pause
for /L %%N in (10,1,20) do dsadd user cn=y%%N,ou=eduteam,dc=itbank,dc=com -upn y%%N@itbank.com -pwd P@$$w0rd
pause
for /L %%N in (10,1,20) do dsadd user cn=z%%N,ou=eduteam,dc=itbank,dc=com -upn z%%N@itbank.com -pwd P@$$w0rd
pause
```

itbank.com

└ 동대문

- └ 501 OU 생성 a10~a20 계정 생성, samid / upn 지정, 암호 P@\$w0rd
- └ 502 OU 생성 a10~a20 계정 생성, samid / upn 지정, 암호 P@\$w0rd
- └ 503 OU 생성 a10~a20 계정 생성, samid / upn 지정, 암호 P@\$w0rd
- └ 504 OU 생성 a10~a20 계정 생성, samid / upn 지정, 암호 P@\$w0rd
- └ 505 OU 생성 a10~a20 계정 생성, samid / upn 지정, 암호 P@\$w0rd

동대문.bat

```
dsadd ou ou=동대문,dc=itbank,dc=com
pause
dsadd ou ou=501,ou=동대문,dc=itbank,dc=com
dsadd ou ou=502,ou=동대문,dc=itbank,dc=com
dsadd ou ou=503,ou=동대문,dc=itbank,dc=com
dsadd ou ou=504,ou=동대문,dc=itbank,dc=com
dsadd ou ou=505,ou=동대문,dc=itbank,dc=com
pause
for /L %%N in (10,1,20) do dsadd user cn=a%%N,ou=501,ou=동대문,dc=itbank,dc=com -upn a%%N@itbank.com -pwd P@$w0rd -samid a%%N
pause
for /L %%N in (10,1,20) do dsadd user cn=b%%N,ou=502,ou=동대문,dc=itbank,dc=com -upn b%%N@itbank.com -pwd P@$w0rd -samid b%%N
pause
for /L %%N in (10,1,20) do dsadd user cn=c%%N,ou=503,ou=동대문,dc=itbank,dc=com -upn c%%N@itbank.com -pwd P@$w0rd -samid c%%N
pause
for /L %%N in (10,1,20) do dsadd user cn=d%%N,ou=504,ou=동대문,dc=itbank,dc=com -upn d%%N@itbank.com -pwd P@$w0rd -samid d%%N
pause
for /L %%N in (10,1,20) do dsadd user cn=e%%N,ou=505,ou=동대문,dc=itbank,dc=com -upn e%%N@itbank.com -pwd P@$w0rd -samid e%%N
pause
```

※이중 for문도 가능하다

Group

- 구성원, 소속 그룹
- 그룹 중이 가능(nesting)
- 사용자,컴퓨터의 연락처의 집합, 권한(permission) 부여의 대상(그룹을 사용하는 목적)
- 다른 그룹의 구성원(memberof)이 될 수 있으며 다른 그룹을 구성원으로(members) 받아들일 수 있다.
- 조직도에 맞게 그룹을 만든다

GroupA(소속원 B)

Group B

S1

그룹A의 소속원은 그룹B, 그룹B의 소속원은 S1

S1의 그룹은 그룹B, 그룹B의 그룹은 그룹A

1. Domain Local

- 자기 도메인 내에서만 존재하는 그룹
- 절대로 다른 도메인으로 이동할 수 없다.
- 단일 도메인에서는 사용할 필요가 없다, 다중 도메인에서만 사용
- 같은 크기의 DL은 서로 이동할 수 있다.
- 구성원(members) : 사용자 계정(본인 도메인, 트러스트된 도메인)

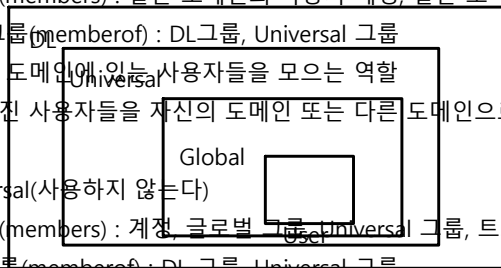
- 소속 그룹(memberof) : 같은 도메인의 다른 DL 그룹
 - > 리소스에 권한을 부여하는 용도로 사용
 - > 자기 도메인의 사용자, 다른 도메인의 사용자, 글로벌 그룹을 받아들이는 역할

2. Global

- 다른 도메인으로 갈 수 있는 그룹(자기 도메인과 트러스트된 도메인에서 조회 가능)
- 같은 도메인에 있는 Global은 넣을 수 있지만 다른 도메인에 있는 Global은 넣을 수 없다.
- 다중 도메인 환경에서는 정보를 가져오는 역할
- 단일 도메인에서는 Global을 활용하는게 편하다.
- 구성원(members) : 같은 도메인의 사용자 계정, 같은 도메인의 글로벌 그룹
- 소속 그룹(memberof) : DL그룹, Universal 그룹
 - > 자기 도메인에 있는 사용자들을 모으는 역할
 - > 모여진 사용자들을 자신의 도메인 또는 다른 도메인으로 데려가는 역할

3. Universal(사용하지 않는다)

- 구성원(members) : 계정, 글로벌 그룹, Universal 그룹, 트러스트된 도메인
- 소속그룹(memberof) : DL 그룹, Universal 그룹
- 장점 : 사용자의 로그인 향상
- 단점 : 복제 트래픽 증가, 보안 문제 야기



[Group 전략]

A >> G >> P

Account > Group > Permission(권한)

(계정) (G,U,DL)

1. A DL P : A > DL < P

- 단일 도메인 환경
- 다중 도메인 모델 등이 섞여 있는 트러스트된 도메인
- 비권장
- 사용자 계정을 DL에 소속 시켜 권한을 주겠다.

2. A G P : A > G < P

- 단일 도메인
- 사용자 계정을 Global그룹에 소속시켜 권한을 주겠다.

3. A G DL P : A > G > DL < P

- 다중 도메인
- MS 권장
- 사용자 계정을 Global그룹에 모아서 DL에 소속시켜 권한을 준다.

4. A G U D L P : A > G > U > D L < P

- 다중도메인
- global catalog로 인해 비권장

[실습]

- 계정 생성

AGP@itbank.com

ADLP@itbank.com

AGDLP@itbank.com

AGUDLP@itbank.com

- 그룹 생성

AGP-G	글로벌 그룹 생성	AGP 계정 그룹 가입
ADLP-DL	도메인 로컬 그룹 생성	ADLP 계정 그룹 가입
AGDLP-G	글로벌 그룹 생성	AGDLP 계정 그룹 가입
AGDLP-DL	도메인 로컬 그룹 생성	AGDLP-G 그룹 가입
AGUDLP-G	글로벌 그룹 생성	AGUDLP 구성원 추가
AGUDLP-U	유니버설 그룹 생성	AGUDLP-G 그룹 가입
AGUDLP-DL	도메인 로컬 그룹 생성	AGUDLP-U 그룹 가입

그룹생성시 그룹 종류는 보안으로 사용

그룹 종류

☒ 보안(S)

☐ 배포(D)

※ 그룹 범위를 잘못 지정했다면 > U > DL 순으로 변경할 수 있다.

1. 그룹에 구성원 추가 하는 법

AGP-G 속성

일반 구성원 소속 그룹 관리자

사용자, 연락처, 컴퓨터, 서비스 계정 또는 그룹 선택

개체 유형을 선택하십시오(S).

사용자, 서비스 계정, 그룹, 또는 기타 개체

개체 유형(O)...

찾을 위치를 선택하십시오(F).

itbank.com

위치(L)...

선택할 개체 이름을 입력하십시오(예제)(E).

AGP

이름 확인(C)

고급(A)...

확인

취소

추가(D)...

제거(R)

확인

취소

적용(A)

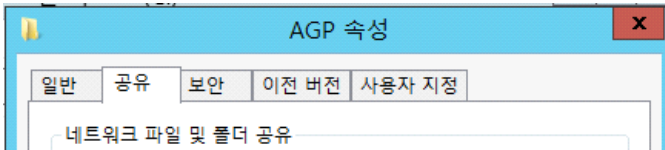
그룹 속성에 들어가서 구성원 탭으로 이동
구성원으로 등록할 계정을 입력하고 이름확인을 통해 설정

2. C드라이브에 폴더 4개 생성

ADLP	2018-09-20 오후...	파일 폴더
AGDLP	2018-09-20 오후...	파일 폴더
AGUDLP	2018-09-20 오후...	파일 폴더

※ 상위 그룹에 권한을 주면 하위 그룹도 동일하게 권한을 부여 받는다.

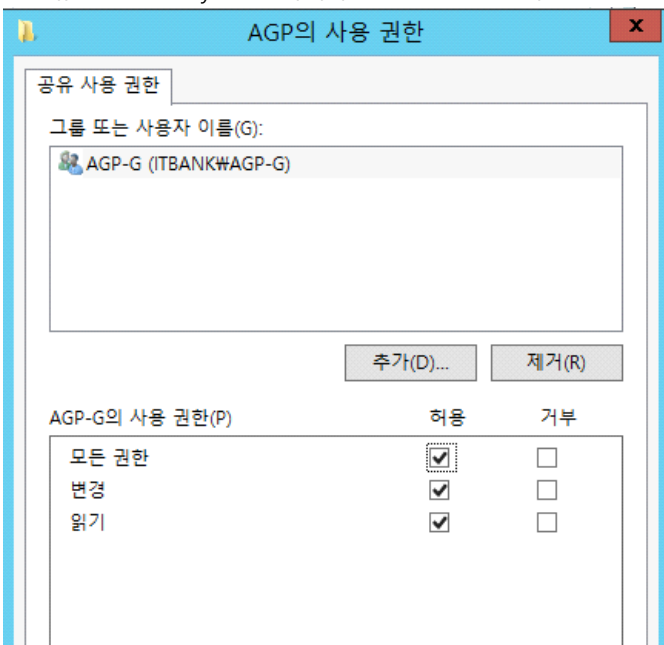
3. 각 폴더의 속성에 들어가면 공유 탭으로 이동한다.



4. 고급 공유를 누르고 선택한 폴더 공유 클릭



5. 공유 권한을 everyone을 삭제하고 AGP그룹을 선택



커맨드로 하는 실습

OU 생성 : eduteam

dsadd ou ou=eduteam,dc=itbank,dc=com

- 사용자 생성

- cn : ava

- 계정 생성 위치 : ou=eduteam

- SAM 이름 : ava

- UPN : ava@itbank.com

- 암호 : P@\$w0rd

- 다음 로그인 시 암호 변경

- 직함 : student

dsadd user cn=ava,ou=eduteam,dc=itbank,dc=com -samid ava -upn ava@itbank.edu -pwd P@\$w0rd -mustchpwd yes -title student

- eduadmins 그룹 생성
 - sam이름 : edu-admins
 - 위치 : eduteam 아래
 - 설명 : 교육팀관리자

dsadd group cn=eduadmins,ou=eduteam,dc=itbank,dc=com -samid edu-admins -desc 교육팀관리자

- ouadmins 그룹 생성
 - sam이름 : ou-admins
 - 위치 : itbank.com 아래
 - 설명 : 전체관리자

dsadd group cn=ouadmins,dc=itbank,dc=com -samid ou-admins -desc 전체관리자

itbank.com

└ eduteam (OU)
 └ eduadmins (그룹)
 └ ava (계정)
 └ ouadmins (그룹)

- 그룹에 구성원(사용자) 추가

dsmod group cn=eduadmins,ou=eduteam,dc=itbank,dc=com -addmbr cn=ava,ou=eduteam,dc=itbank,dc=com

= dsquery group -name eduadmins | dsmod group -addmbr cn=ava,ou=eduteam,dc=itbank,dc=com
 > 그룹(eduadmins)을 요청해서 사용자계정(ava)을 추가할 때는 옵션이 바로 뒤에 붙는다

= dsquery user -name ava | dsmod group cn=eduadmins,ou=eduteam,dc=itbank,dc=com -addmbr
 > 계정(ava)을 요청해서 그룹(eduadmins)에 추가할 때는 마지막에 옵션이 붙는다.

- 그룹에 구성원(사용자) 삭제

dsmod group cn=eduadmins,ou=eduteam,dc=itbank,dc=com -rmmbr cn=ava,ou=eduteam,dc=itbank,dc=com
 > Dsmod로 원하는 그룹으로 이동해 -rmmbr로 사용자 계정(계정의 위치 입력) 삭제

- 그룹에 구성원(그룹) 추가

itbank.com

└ ouadmins (그룹)
 └ eduadmins (그룹)

dsquery group -name eduadmins | dsmod group cn=ouadmins,dc=itbank,dc=com -addmbr
 > Eduadmins를 요청해서 ouadmins에 추가할 때는 마지막에 옵션이 붙는다.

**※ A를 B에 추가할 때 dsquery로 A를 요청하면 -addmbr은 마지막에 붙는다
 dsquery로 B를 요청하면 -addmbr은 앞쪽에 붙는다**

- 사용자의 소속그룹 확인 -memberof

dsquery user -name ava | dsget user -memberof

- 그룹의 구성원 확인 -members

dsquery group -name ouadmins | dsget group -members
 dsget : cmd창에 표시

- 그룹 삭제

dsquery group -name eduadmins | dsrm -noprompt
 dsquery group -name ouadmins | dsrm -noprompt

- 계정 삭제

dsquery user -name ava | dsrm -noprompt

※ 명령어 옵션을 넣을때 띄어쓰기가 들어갈때 조심할 것!!

명령어를 구분할 때 띄어쓰기가 기준, 필요할 시 " " 을 활용할 것.

그룹생성시 default는 Global

권한

2018년 9월 27일 목요일 오후 12:38


리소스 권한 ex)파일이나 폴더에 보여
라이트 권한 - 어떤 시스템을 다루는데 필요한 권한 설정
정책 속에 라이트 권한도 속해 있다.


• 리소스 권한


- 네트워크 권한 : Shared Permission
- 공유 권한
- 로컬 권한 ex)NTPS

• 공유의 종류

- 단순 공유 폴더(Simple shared folder)
- 고급 공유 (Advanced shared folder)
ACL, ACE
속성 > 공유 > 고급 공유
공유 이름 변경 가능
정확한 공유 권한 편집 가능
- 숨김 공유(Hide a shared folder)
공유명 뒤에 \$를 붙이면 숨김 공유
접근시에 네트워크 장비 목록이나 폴더 목록 X
직접 접근만 가능 \ \ 컴퓨터 \ 공유이름\$ 방식
실제 폴더 위치나 공유 폴더의 존재를 보안상 숨김
관리 공유라는 관리 먹적의 공유도 존재
- 관리 공유
윈도우가 부팅되는 순간 공유
기본적으로 사용하고 있는 드라이브는 모두 공유

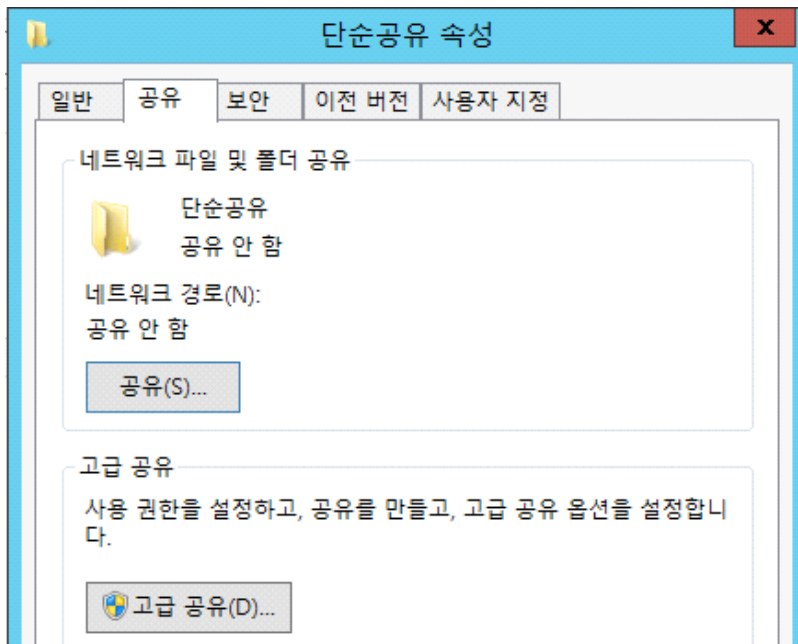
 단순공유

 고급공유

 숨김공유

단순 공유와 고급공유의 차이는 클릭으로 결정된다!

1. 단순공유



↓ - 공유폴더의 기본값-

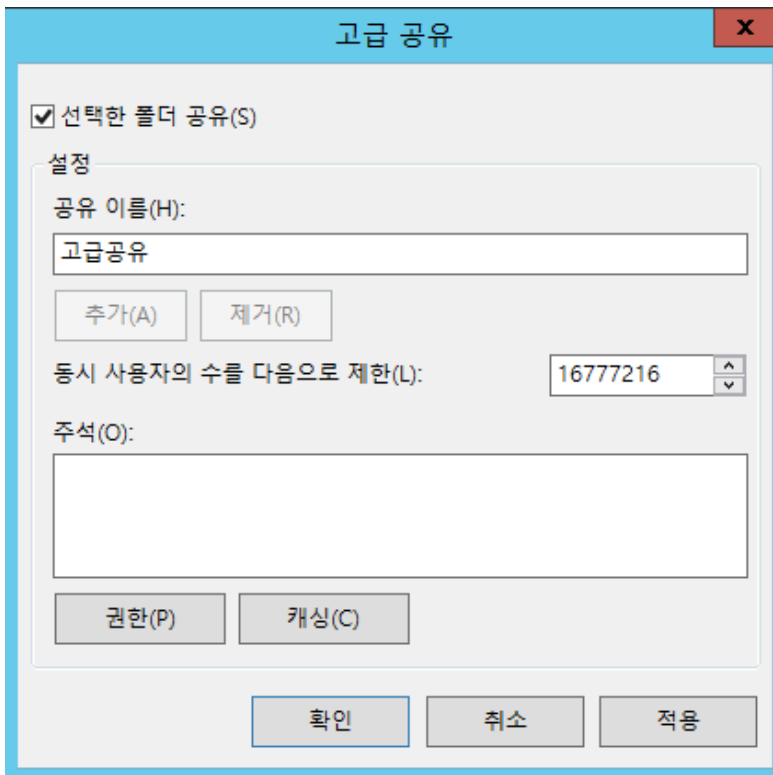
이름	사용 권한 수준
Administrator	읽기/쓰기 ▼
Administrators	소유자

소유자 : 권한설정, 다른계정의 권한설정, 생성,수정 등 모든 권한을 가지고 있다

▼
추가(A)

공유계정을 추가할 때 사용자 계정을 입력하고 추가하면 된다.

2. 고급공유



공유 이름 : Client가 접속할 때 알려줄 이름, 실제이름과 동일하게 할 필요는 없다.

동시 사용자의 수를 다음으로 제한 : 접속 할 인원을 제한 할 수 있다. 윈도우7은 20명으로 제한

주석

권한탭

ACL : Access control list

그룹 또는 사용자 이름(G):

Everyone

추가(D)...

제거(R)

ACE : Access control entree

Everyone의 사용 권한(P)

허용

거부

모든 권한	<input type="checkbox"/>	<input type="checkbox"/>
변경	<input type="checkbox"/>	<input type="checkbox"/>
읽기	<input checked="" type="checkbox"/>	<input type="checkbox"/>

※ ACL에 등록된 계정마다 ACE가 다르다

SID : Security identifier 보안 식별자

- 시스템이 계정/그룹을 식별 할 때 사용, **시스템은 계정과 그룹을 이름으로 구분하지 못한다.**
- windows 각 사용자나 작업그룹에 부여되는 고유 번호
- 계정에 대한 핵심 식별자는 SID이다.
계정 생성 > 삭제 > 같은 이름으로 다시 생성해도 SID는 같지 않다.

C: \>whoami /user

```
사용자 정보
-----
사용자 이름      SID
=====
itbank\administrator S-1-5-21-3659561364-2908046465-1821834938-500
```

사용자 정보

사용자 이름

SID

=====

itbank\administrator	S-1-5-21-3659561364-2908046465-1821834938-500	관리자
Windows domian domain domain	1000 ~	일반사용자
	501	guest(비활성화상태로 생성)
	RID	

SID 확인

- 1) Cmd창에서 whoami /user

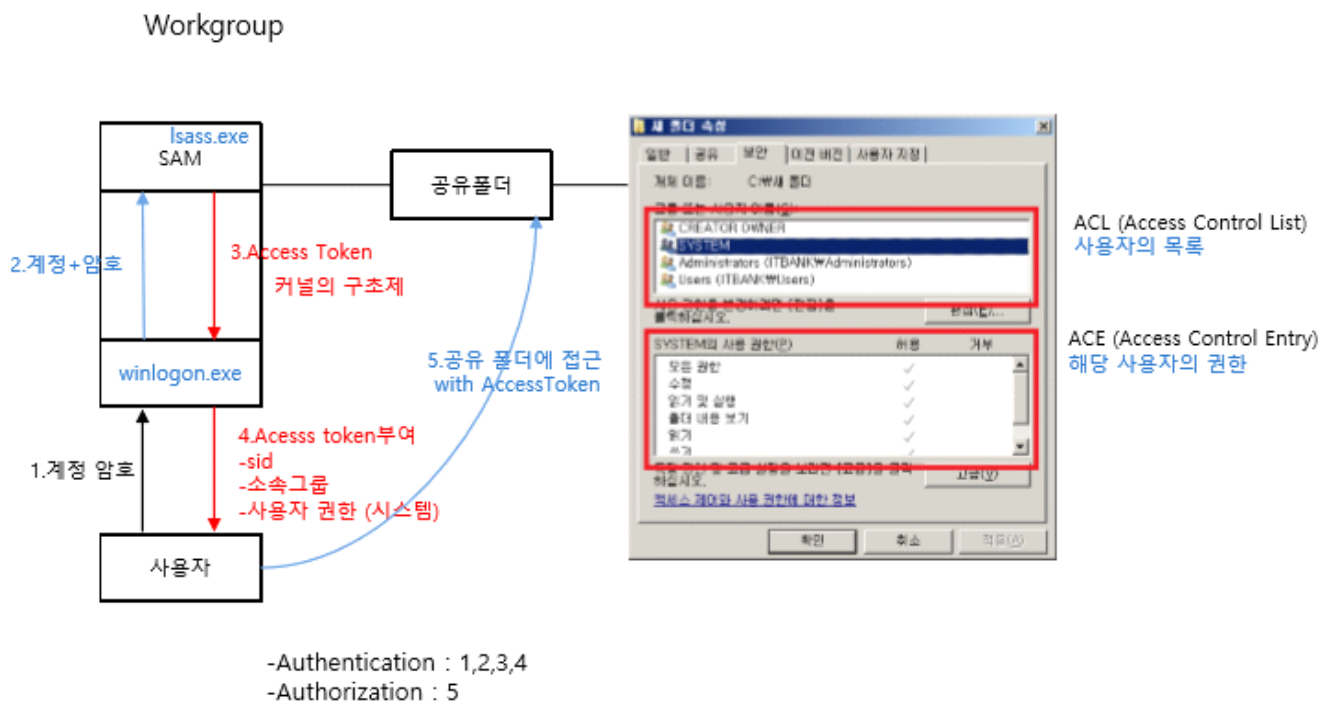
- 2) AD 사용자 및 컴퓨터(dsa.msc) > 보기 -고급 체크 > 계정속성 > 특성 편집기 탭 > objectSid
- 3) 레지스트리 HKLM \ SOFTWARE \ Microsoft \ WindowsNT \ Currentversion \ ProfileList

[Access Token]

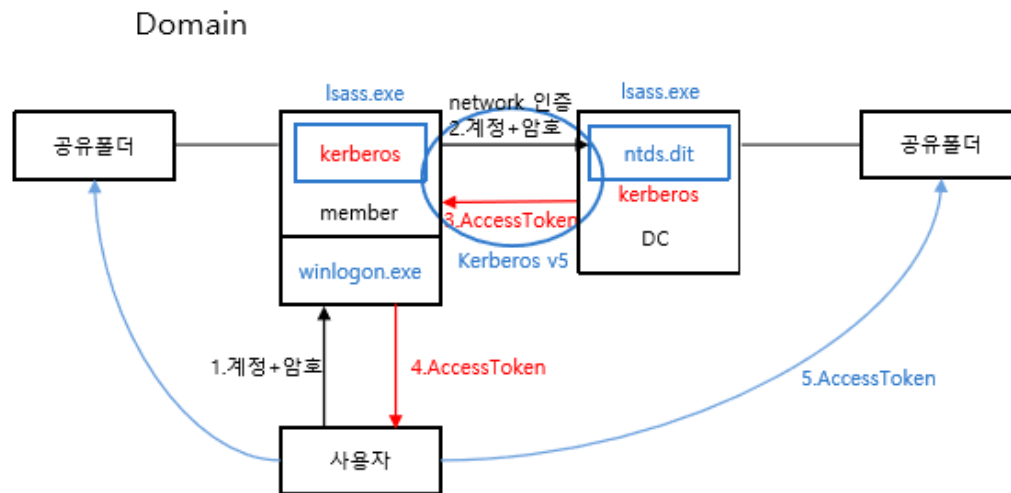
- SID 적용
- 사용자가 로그인 성공시 생성됨
- 사용자가 개체에 접근하거나 시스템 기능을 사용할 때 자격증명을 위하여 요구됨
- 도메인 : 한번의 Access Token으로 도메인의 모든 자원에 접속 가능
- 독립실행형 : 각 서버 접속시마다 Access Token 생성
- 자원들 ACL 목록이 SID와 Access Token의 SID를 비교하여 사용허가를 하게 된다.

Authentication(인증) : 정당한 사용자인가

Authorization(권한 부여) : authenticated된 사용자가 resource(폴더, 프린터)에 접근 가능/불가능



1. 로그인할때 입력한 winlogon.exe파일은 sam으로 전송
2. 일치 할 경우 Access Token 생성(로그인 되자마자 발급)
3. Access Token에는 계정의 **SID값,소속그룹**,사용자권한(시스템)이 있다.
4. 사용자 계정으로 공유폴더,폴더,파일 등 접근할 때 Access Token을 사용
5. 계정에 부여된 SID값과 파일이나 폴더에 등록된 ACL의 SID값을 비교해서 ACE에 설정된 권한을 부여
6. 계정에 부여된 SID값과 파일이나 폴더에 등록된 ACL의 SID값이 다를 경우 접근 불가
7. 예외사항으로 소속그룹에 소속되어 있을 경우 계정의 SID값이 ACL에 없더라도 소속 그룹의 SID값이 ACL에 있을 경우 해당 ACL의 권한을 계정에 부여한다



1. 로그인할때 입력한 member의 winlogon.exe파일은 kerberos에 의해 DC로 이동
2. DC의 ntds.dit에 해당 정보가 있다면 AccessToken을 member로 전달

차이점

- workgroup의 경우 각 컴퓨터마다 AccessToken이 독립적이다.
- domain의 경우 AccessToken이 공유?가 되기때문에 다른 컴퓨터에도 접근이 가능하다.

3. 숨김 공유

공유 폴더 목록에 안뜨게 하기 위해서 사용
공유 이름뒤에 \$를 붙이면 공유는 하되 숨김

공유 이름(H):

숨김공유\$

Member에서 DC의 공유폴더 보는 법

1. 실행창에 DC의 IP를 치는법

열기(O): \\10.0.0.110

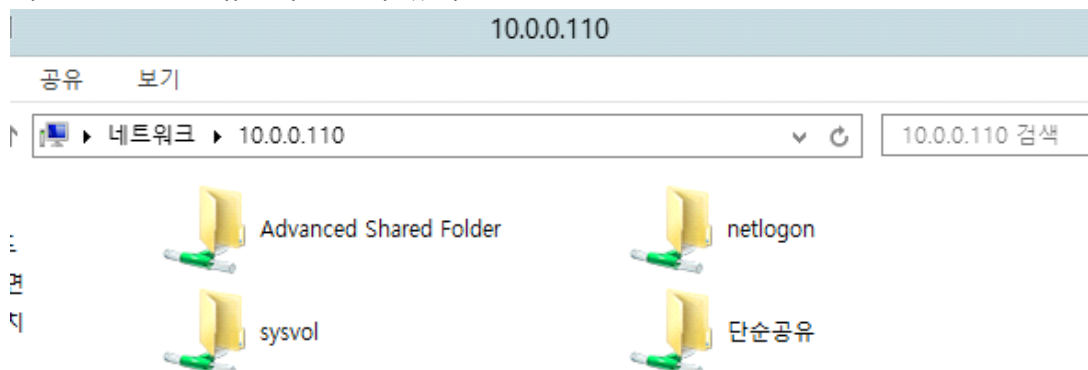
2. 실행창에 DC의 이름으로 치는법

열기(O): \\WSeoul

3. DC의 숨김폴더로 이동하는 법

열기(O): \\WSeoul\숨김공유\$

해당 방법으로 공유폴더를 볼 수 있다.



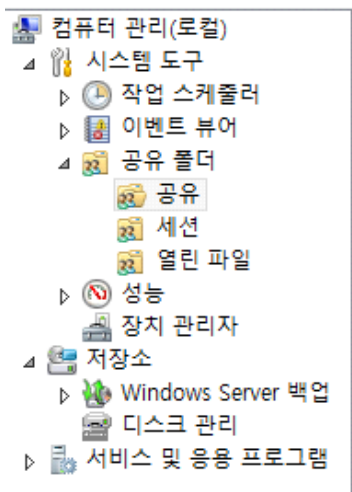
Netlogon,sysvol : 관리공유폴더

관리공유폴더 보는 법

DC에서 실행창에 compmgmt.msc 검색

열기(O):

- Workgroup환경에서 많이 쓰인다.
- 공유폴더,로컬 사용자 및 그룹을 활용하기 위해 사용한다.



세션 : 공유폴더에 누가 들어 와있는지 확인

열린파일 : 공유폴더에서 어떤작업을 하고 있는지 확인

공유로 : 공유폴더 list를 볼수 있다.

공유 이름	폴더 경로	종류	클라이언트 연결 수
ADMIN\$	C:\Windows	Windows	0
Advanc...	C:\고급공유	Windows	1
C\$	C:\	Windows	0
IPC\$		Windows	0
NETLOG...	C:\Windows\SYS...	Windows	0
SYSVOL	C:\Windows\SYS...	Windows	0
단순공유	C:\단순공유	Windows	0
숨김공...	C:\숨김공유	Windows	0

Admin\$,IPC\$: 서버나 시스템을 원격지에서 접속할 때 필요하다.원격관리용도로 활용

C\$: C드라이브를 자동으로 관리공유형태로 공유,공유 해지시 각종 공유서비스를 활용 못할 수 있다.

NETLOGON\$: 도메인 로그인 요청처리를 할때 반드시 필요

SYSVOL : 여러대의 DC가 있을 때 DC들간 데이터 복제를 할 때

커맨드 창으로 공유폴더 만드는 법

Mkdir : 폴더생성

```
C:\>mkdir sharecli_
```

명령어는 linux와 동일

Cd : 이동

Net share : 공유작업

```
C:\W>net share
```

공유 이름	리소스	설명
숨김공유\$	C:\W\숨김 공유	
C\$	C:\W	기본 공유
IPC\$		원격 IPC
ADMIN\$	C:\W\Windows	원격 관리
Advanced Shared Folder	C:\W\고급공유	
NETLOGON	C:\W\Windows\SYSTEM32\sysvol\withbank.edu\SCRIPTS	Logon server share
SYSTEM	C:\W\Windows\SYSTEM32\sysvol	Logon server share
단순공유	C:\W\단순공유	

명령을 잘 실행했습니다.

Net share clitest=c:\Wsharecli

```
C:\W>net share clitest=c:\Wsharecli
```

=을 기준으로 오른쪽에는 실제폴더 위치(이름) 왼쪽에는 공유 이름
/grant 권한 부여할 그룹or계정 : 권한설정(read:읽기,full:모든권한,change:변경)

```
C:\W>net share clitest=c:\Wsharecli /grant:everyone,read
```

여러 사용자or그룹에 설정할 경우 한칸 띄우고 추가 입력

```
C:\W>net share clitest=c:\Wsharecli /grant:everyone,read /grant:
```

Net share 공유폴더 : 공유폴더의 상세 정보

```
C:\W>net share clitest
```

공유 이름	clitest
경로	c:\Wsharecli
설명	
최대 사용자 수	제한 없음
사용자	
캐싱	문서의 수동 캐시
사용 권한	Everyone, READ
	ITBANK\Administrator, CHANGE

/delete : 공유제거

```
C:\W>net share clitest /delete
```

Rmdir : 폴더 삭제

```
C:\W>rmdir sharecli
```

실습

배치 파일로 작성

Share11~15 계정 생성 > samid 지정, upn 지정, 암호 P@\$w0rd 설정

Sharegroup 그룹 생성 > share11~13 구성원으로 가입

공유폴더 생성

C:\Wshare11 폴더 생성 후

- 공유 이름 share11으로 공유
- Share 11 사용자 읽기 권한

C:\Wshare12 폴더 생성 후

- 공유이름 share12으로 공유
- Share12 사용자 변경 권한

C:\Wshare13 폴더 생성후

- 공유이름 share13으로 공유
- Share13 사용자 모든 권한

C:\sharegroup 폴더 생성 후

- 공유 이름 sharegroup으로 공유
- Sharegroup 읽기 권한
- Share14는 변경 권한
- Share15는 모든 권한

공유권한

2018년 9월 28일 금요일 오후 12:35

DFS : 분산 파일 시스템(distribute file system)

Client가 여러곳의 공유폴더를 접속 할때 여러곳에 접속 하는 것을 편리하기 만들기 위함

Hosting server를 결정하고 그곳에 name space(논리적 경로)를 설정

Client가 접근할 때 이용하는 경로임

● 접근방법

도메인형식 - 도메인이름을 활용 ex) wwitbank.edu

로컬형식

Name space dataroom으로 지정하면 접속하기 위해서는 wwitbank.eduWdataroom으로 접속

같은 서버의 공유 폴더 뿐만 아니라 다른 곳의 공유폴더도 name space에 모을 수 있다.

같은 네트워크에 존재하는 모든 트라이언트들이 접속할 수 있게 만들 수 있다.

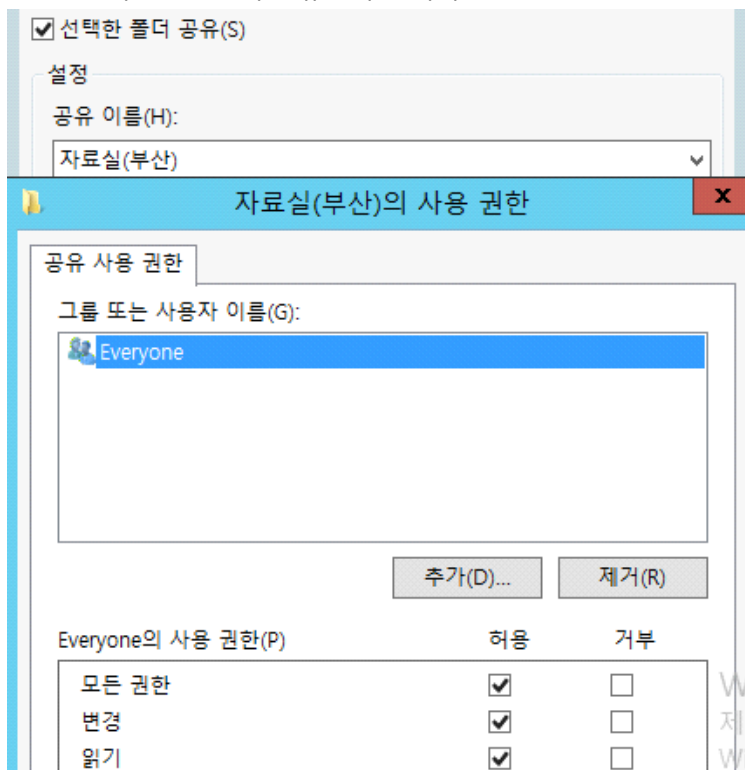
설정 간 준비사항

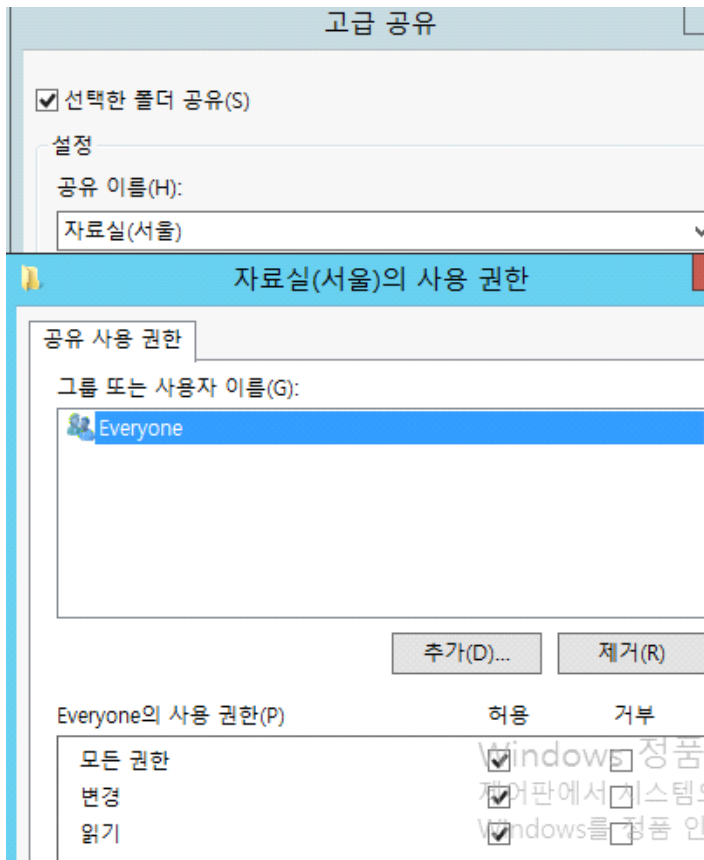
권한 : everyone,읽기 필수

=> 모든 공유폴더들을 한 곳으로 모으는게 목적.

• 설정 방법

1. DC와 member에 공유폴더 한개씩 설정

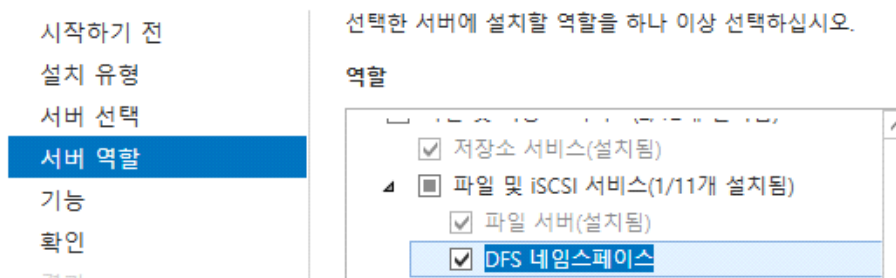




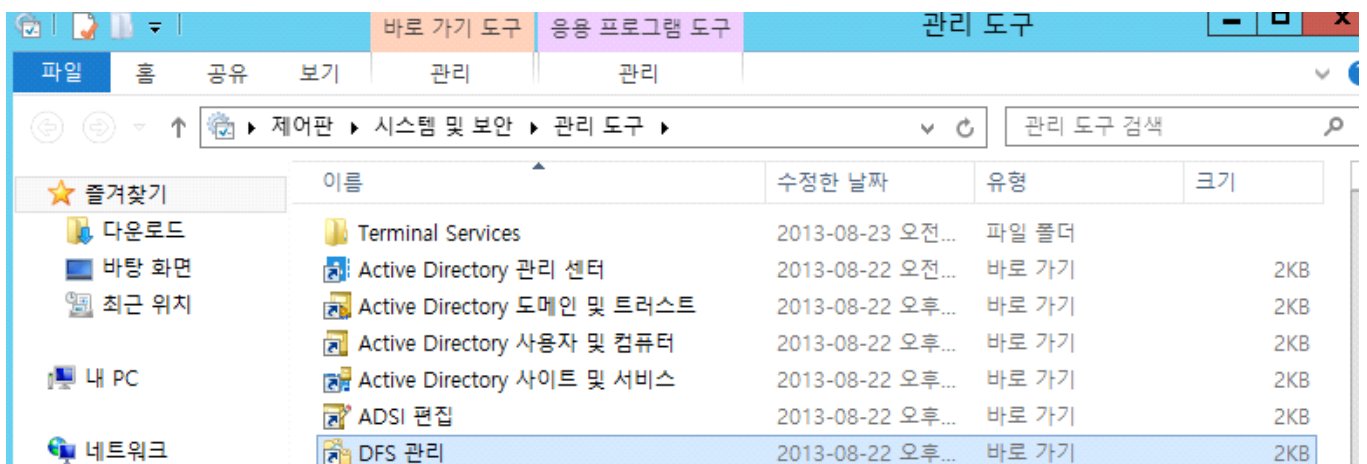
DC를 Hosting server로 활용 -> DFS 기능을 추가해야함.

2. 서버역할에 파일 및 iscsi 서비스를 확장하면 DFS네임스페이스 설정

서버 역할 선택



3. 시작 -> 관리도구 -> DFS관리



4. 새 네임스페이스 생성

DFS 관리

네임스페이스

새 네임스페이스(N)...

DC(서울)로 생성

네임스페이스를 호스트할 서버의 이름을 입력하십시오. 여기서 지정하는 서버가 네임스페이스 서버가 됩니다.

서버(S):

seoul

찾아보기(B)...

네임스페이스의 이름을 입력합니다. 이 이름은 네임스페이스 경로에서 서버 또는 도메인 이름 다음에 표시됩니다(예: \\Server\\Name 또는 \\Domain\\Name).

이름(A):

dataroom

예: 공용

DFS기능이 SERVER 자체 기능이므로 도메인이 있을 경우 도메인 기반 네임스페이스 활용, 없을 경우 독립형 네임스페이스 활용

도메인 기반 네임스페이스(D)

도메인 기반 네임스페이스는 하나 이상의 네임스페이스 서버와 Active Directory 도메인 서비스에 저장됩니다. 여러 개의 서버를 사용하여 도메인 기반 네임스페이스의 가용성을 높일 수 있습니다. Windows Server 2008 모드에서 만들어진 네임스페이스는 향상된 확장성 및 액세스 기반 열거를 지원합니다.

☒ Windows Server 2008 모드 사용(E)

도메인 기반 네임스페이스 미리 보기(R):

\\Witbank.edu\\dataroom

네임스페이스에 공유폴더를 등록만 하면 클라이언트가 접근하여 활용할 수 있다.

\\Witbank.edu\\dataroom

폴더를 생성하는것이 아니라 기존 공유폴더를 등록하는 것.

DFS 관리

네임스페이스

\\Witbank.edu\\dataroom

새 폴더(O)...

이름(N):

자료실(서울)

공유폴더의 이름과 같지 않아도 된다. 네임스페이스에서 이름을 어떻게 사용할 것인지 정하는 것.

폴더 대상 경로(P):

\\Wseoul\\자료실(서울)

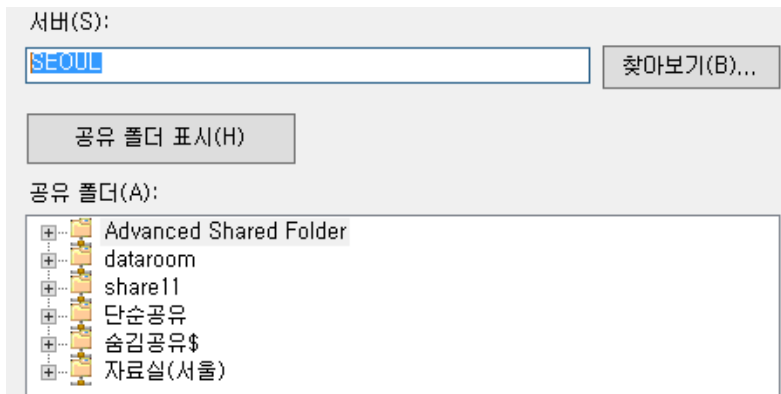
찾아보기(B)...

공유폴더의 원본파일 경로, 찾아보기로 파일의 경로를 지정할 수 있다.

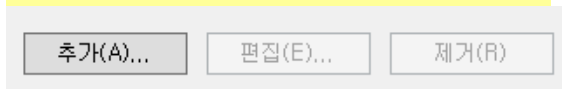
폴더 대상 경로(P):

\\Wseoul\\자료실(서울)

찾아보기(B)...



※ 추가를 눌러 폴더를 지정하면 지정한 폴더를 네임스페이스 상 지정한 공유폴더에 데이터가 모이게 되어 원하는 작업을 할 수 없다.



네임스페이스 완성

네임스페이스		네임스페이스 서버	위임	검색
2개 항목				
종류	이름			
	자료실(부산)			
	자료실(서울)			

• 확인방법

Member(busan)에서 실행창에 [₩witbank.edu₩dataroom](http://witbank.edu₩dataroom) 을 검색한다.

※ CWDFSRoots₩dataroom 그 속에 공유폴더가 있는데 탐색기를 통한 접근은 안되고 실행창으로 접근해야 사용가능하다.

네트워크드라이브

네트워크적으로 만들어진 드라이브

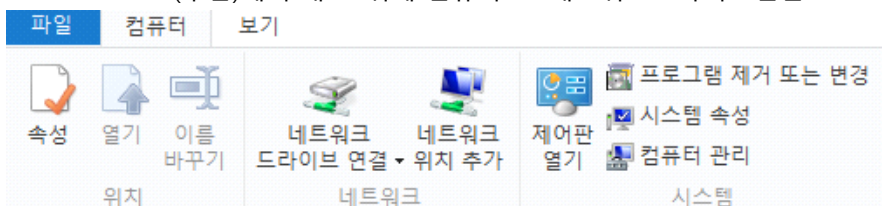
해당 드라이브를 활용하기 위해서는 공유폴더를 활용해야한다.

설정방법

1. DC(서울) C:₩에 공유폴더를 생성(everyone,full)




2. MEMBER(부산)에서 내PC 위에 컴퓨터 -> 네트워크드라이브연결




- ### 3. 연결할 폴더경로 지정(정확하게)

연결할 네트워크 폴더를 선택하십시오.

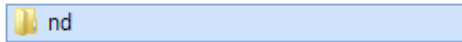
연결에 사용할 드라이브 문자와 연결할 폴더를 지정하십시오.

드라이브(D): Z: 

폴더(O): \\wseoul\네트워크드라이브  [찾아보기\(B\)...](#)

- 커맨드작업

- ### 1. DC(서울)C:\wnd 공유폴더 생성(everyone,full)



- ## 2. Member(부산) cmd 창

```
>net use y: \\wseoul\nd
```

Y: 드라이브라는 이름으로 wwseoulwnd를 연결하겠다. Y: 와 경로 사이에는 **띄어쓰기 반드시** 필요

- ### 3. 생성 완료 Z:



- #### 4. 삭제방법

```
C:\Users\administrator.ITBANK>net use z: /del
z:이<가> 제거되었습니다.

C:\Users\administrator.ITBANK>net use y: /del
y:이<가> 제거되었습니다.
```

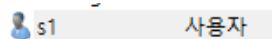
Del이나 delete나 상관없다.

네트워크 드라이버를 활용한 홈폴더

계정을 기준으로 해당 계정이 도메인상에 다른 member에 접속해도 해당 계정에 따라 다닌다.

- 설정방법


- ## 1. S1 계정 생성



- ## 2. Homefolder 공유폴더에 s1계정 공유 설정(권한 : full)

공유 사용 권한

그룹 또는 사용자 이름(G):

 s1 (s1@itbank.edu)

3. S1계정의 속성창 -> 프로파일 권한부여가 제대로 이루어지지 않으면 액세스 거부가 뜬다.

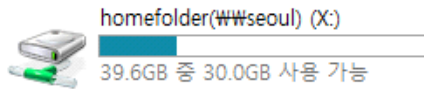
홈 폴더

☐ 로컬 경로(L):

☒ 연결(C): X: 대상(T): \\₩₩seoul₩₩homefolder

4. Member(부산)에 S1으로 로그인하면 홈폴더가 생성된것을 확인할 수 있다.

네트워크 위치 (1)



폴더 리디렉션

DC와 member에 도메인관리자 계정으로 로그인한 상태 => itbank₩₩administrator

같은계정면 바탕화면이 같아야한다???

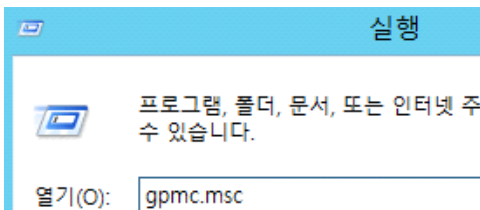
- ↳ 기본적으로 window운영체제에 C:₩₩사용자 폴더에 계정마다 전용공간을 형성한다.
그 전용공간에 바탕화면이 있다.

Member에 두 계정의 있는데 차이점을 알아보자

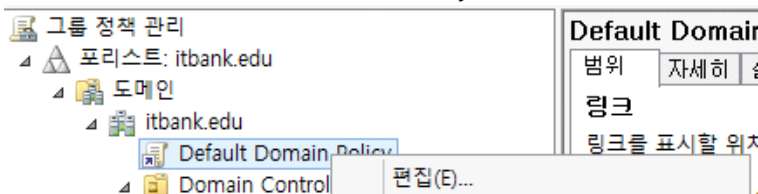
	Administrator	2018-09-11 오후...	파일 폴더
	administrator.ITBANK	2018-09-28 오후...	파일 폴더

도메인로그인(~.itbank)과 로컬로그인의 차이

1. 그룹 정책 관리 => 도메인에서 사용할 정책을 설정

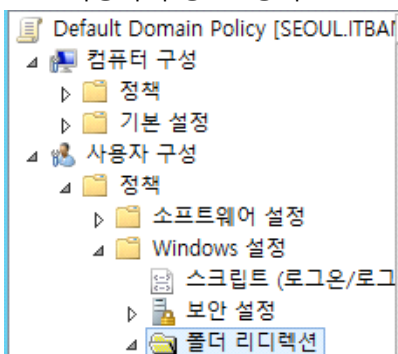


2. 도메인 하위 Default Domain Policy

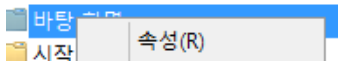


※ Domain Controllers 하위 Default Domain Controllers Policy와 헷갈리지 말것

3. 사용자 구성 -> 정책 -> windows설정 -> 폴더리디렉션

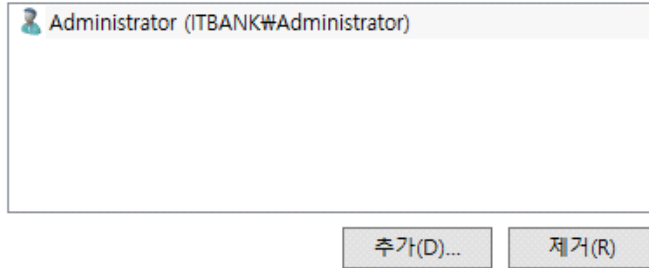


4. 폴더리디렉션 -> 바탕화면 속성



5. DC(서울) C:₩에 공유파일 권한설정(administrator, full)

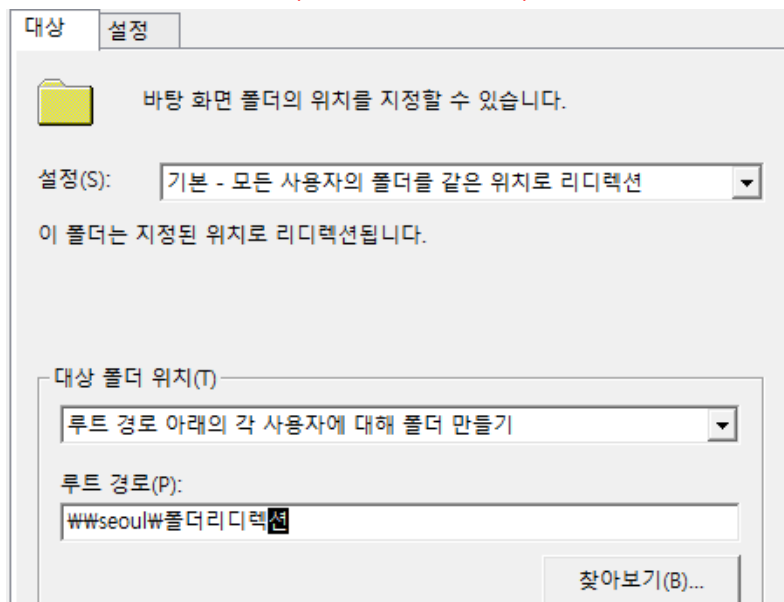
그룹 또는 사용자 이름(G):



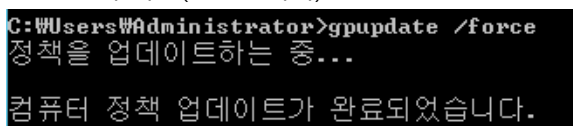
Administrator의 사용 권한(P)	허용	거부
모든 권한	<input checked="" type="checkbox"/>	<input type="checkbox"/>
변경	<input checked="" type="checkbox"/>	<input type="checkbox"/>
읽기	<input checked="" type="checkbox"/>	<input type="checkbox"/>

관리자 계정만 설정해야 관리자 계정만 통합된다.

6. 바탕화면 속성 설정(오타있는지 확인)



7. 정책 적용(cmd창에서)



어떤 조건에 의해 동일한 바탕화면을 사용할 수 있는가???

↳ 사용자의 바탕화면이 공유폴더(폴더리디렉션)으로 이동

실습

1.네트워크드라이브

GUI 환경으로 네트워크 드라이브연결 1번 문자레이블은 z:

CLI 환경으로 네트워크 드라이브연결 1번 문자레이블은 y:

2.Seoul에서 HomeFolder를 공유 한 뒤 s1 계정의 홈폴더로 지정해주세요

문자 레이블은 x 드라이브로 해주세요 !!

3.서울 , 부산 server에서 각각 공유폴더 2개씩 생성 후 공유권한 설정 (Everyone , change)

서울 : test_seoul1 , test_seoul2

부산 : test_busan1 , test_busan2

* 서울은 DFS_hosting_server가 되며 서울 부산에 있는 모든 공유폴더를 VM이라는 네임스페이스에 통합 관리 한다.

부산에서 접근시 모든 공유폴더 목록이 보이게 되면 성공

4.Folder Redirection

Administrator의 바탕화면을 폴더리디렉션 하여 Seoul,busan 컴퓨터 어디서나 항상 같은 바탕화면을 받을 수 있도록 서비스를 제공하세요.

로컬 권한

2018년 10월 1일 월요일 오후 12:33

NTFS(New Technology File System)

- 권한을 지칭하는 것이 아니라 파일 시스템
- MS에서 만듦
- Windows는 기본값으로 NTFS를 사용함

파일시스템?

운영체제에서 데이터가 생성되면 데이터들이 중구난방 생성되면 관리하기 힘들어
파일시스템을 통해 계층구조로 관리

NTFS 권한 : NTFS를 써야지만 사용할 수 있는 권한

1. Permission : 리소스에 대한 접근권한, Action on Object
 - 파일,폴더,프린터와 같은 개체에 적용되는 속성
 - 개체 속성 -> 보안 탭에서 설정
 - 특정 폴더들 보안탭에 존재하는것, 특정 개체에 대한 접근 권한
2. Right : 시스템에 대한 변경권한, Action on System
 - 도메인이나 로컬컴퓨터에 적용되는 속성
 - 그룹정책(gpedit.msc, gpmmc.msc) -> 컴퓨터 구성 -> 정책 -> windows 설정 -> 보안설정 -> 로컬 정책 -> 사용자 권한 할당,보안 옵션 항목에서 구성
 - 시스템 전체에 대한 권한

암시적인 퍼미션

vs

명시적인 퍼미션

Implicitly Permission

Explicitly Permission

Allow+Revoke

Allow+Deny

회색 : 수정 불가

검정색 : 수정 가능

권한을 주지 않았는데 권한설정

직접 권한 부여

- 1) Allow : 권한을 준 경우(grant)
- 2) Deny : 권한을 거부한 경우
- 3) Revoke : 권한 설정을 하지 않은 경우

소유권이란??

소유자는 개체에 대해서 어떻게 사용권한을 설정할 것인지 누구에게 권한을 부여할 것인지 제어가능
소유자는 접근거부여도 개체에 대해 사용권한을 변경가능(ACL, ACE편집가능)

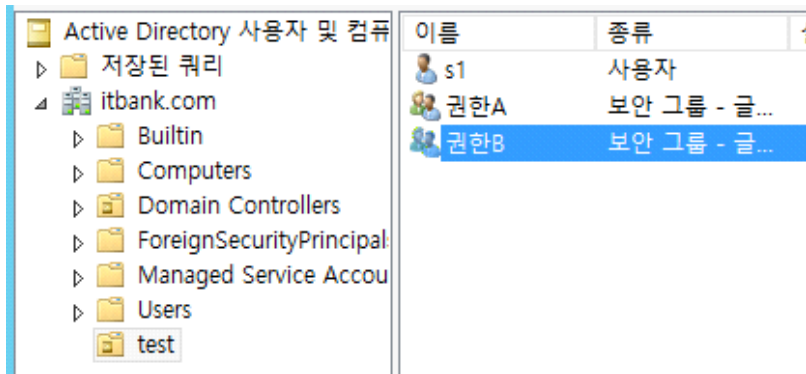
- Administrators => 그룹(administrator계정이 들어가 있다)
 - 모든 권한이 부여된 구성원
 - NTFS볼륨상에 생성되는 폴더나 파일들에 대해 기본적으로 모든권한
- CREATOR OWNER
 - 해당 폴더나 파일을 만든 소유주를 자동으로 포함하는 그룹이다.
EX) userA가 Data 폴더를 만들었다면 userA는 Data 폴더를 만든 소유주 -> CREATOR OWNER의 구성원
 - 폴더의 소유주는 자신의 폴더에 대해 모든 권한을 가지게 된다.
 - 특정 권한은 특수 NTFS 사용 권한의 모음이다.
 - 상황마다 속하는 계정이 달라진다.
 - 폴더별로 파일별로 구성원이 달라진다.
- System
 - Windows Server 2012이 내부적으로 사용하는 계정이다. 모든 권한이 부여되어 있다.
 - Windows Server 2012이 NTFS 볼륨 상의 모든 폴더나 파일에 액세스 할 수 있도록 하기 위해 사용된다.
- Users
 - 일반 사용자 계정을 포함하고 있는 User 로컬 그룹에게는 읽기 및 실행, 폴더 내용보기, 읽기, 특정 권한 부여
 - 특정 권한에는 폴더 생성 및 파일 생성 권한이 설정되어 있다.
 - 일반사용자들은 기본적으로 NTFS 볼륨상에 생성된 폴더에 하위 폴더나 파일을 생성할 수 있다
 - 특정 사용자만이 액세스하도록 하기 위해서는 Users를 제거하고 사용자나 그룹에게 NTFS 권한을 부여
 - 권한 설정할때 반드시 확인하고 생각해야한다

[퍼미션의 규칙]

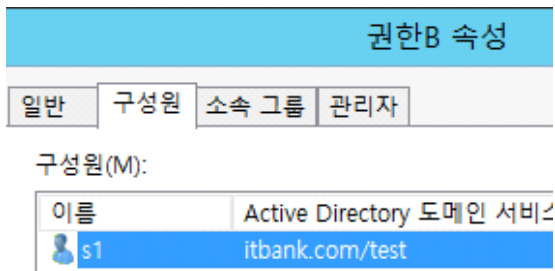
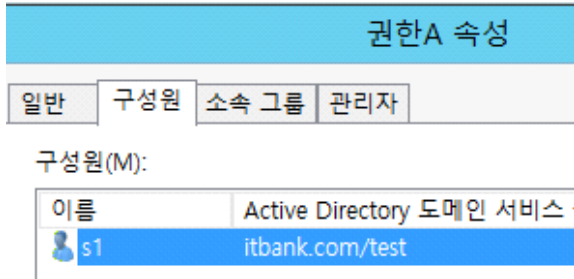
1. NTFS 권한은 각 드라이브의 루트에서 시작된다.
2. 권한은 누적(cumulative), 상속(inheritance)된다.
상속은 포기할 수으며 할줄 알아야 NTFS작업을 할 수 있다.
3. 거부 권한이 우선된다
4. 직접 적용한 권한이 우선된다

● 설정방법

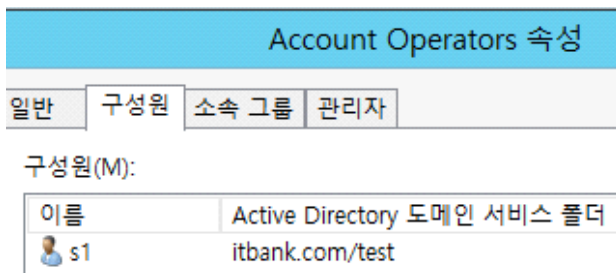
1. Test ou에 s1계정,권한a,권한b그룹 생성



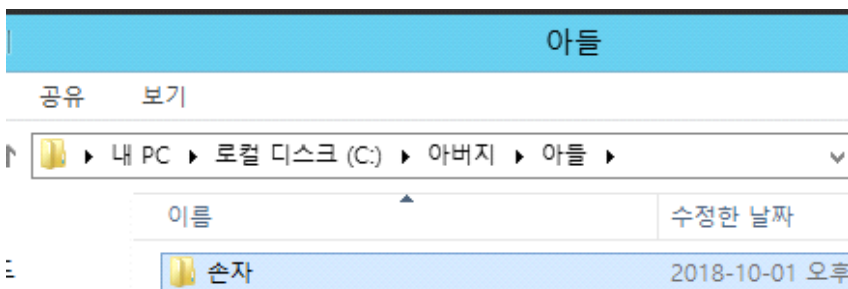
2. 각 그룹에 s1 추가



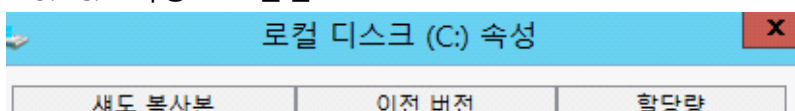
3. Builtin -> Account Operators에 s1 구성원 추가(로컬권한을 보기 위함) => s1사용자는 일반사용자계정이다보니 DC에 접속할 수 있게 하기 위함

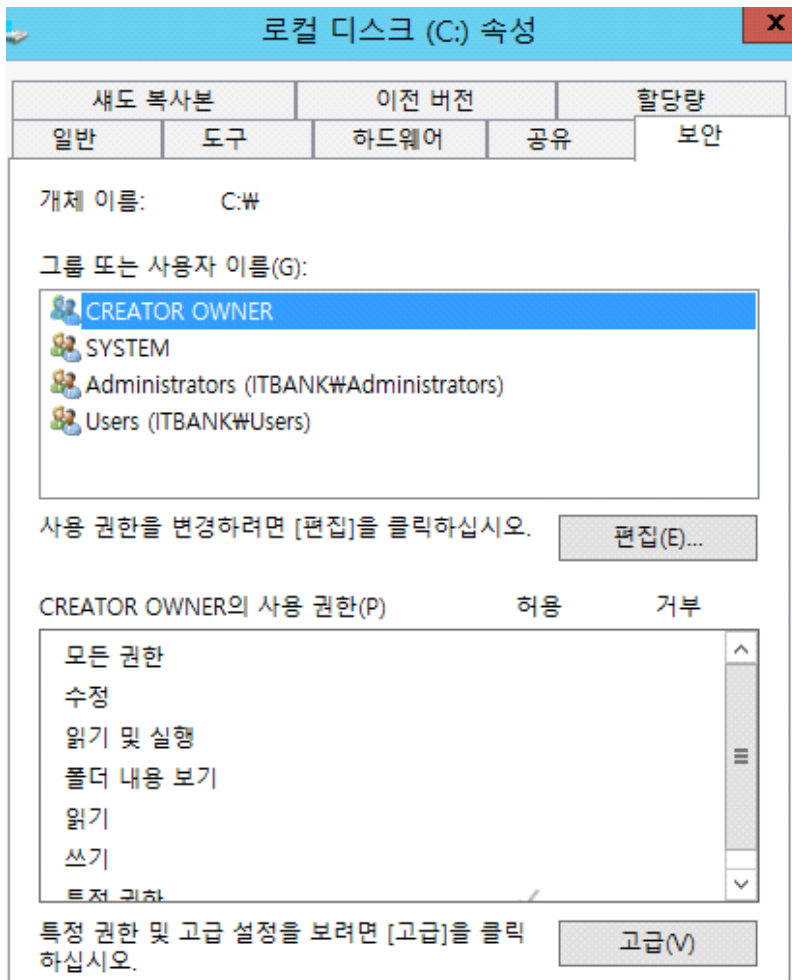


4. C:\ 아버지\아들\손자 폴더 생성



5. C:\ 속성 > 보안탭





드라이브 루트에서 권한을 설정하면 하위는 자동으로 권한을 부여받는다.
 드라이브 루트가 다르면 권한이 달라진다.
 하위 폴더를 다른 드라이브루트로 옮기면 옮긴 드라이브루트의 권한을 부여받는다.
 드라이브가 옮겨지면 무조건 권한 세팅을 다시 해야한다.

상속포기하는 법

폴더의 보안탭 -> 고급 -> 상속 사용안함

아버지 고급 보안 설정

이름: C:\아버지

소유자: Administrators (ITBANK\Administrators) 변경(C)

사용 권한

감사

유효한 액세스

자세한 내용을 보려면 사용 권한 항목을 두 번 클릭하십시오. 사용 권한 항목을 수정하려면 항목을 선택하고 [편집] 버튼을 클릭하십시오.

사용 권한 항목:

유형	보안 주제	액세스	다음에서 상속됨
허용	SYSTEM	모든 권한	C:\
허용	Administrators (ITBANK\Administr...	모든 권한	C:\
허용	Users (ITBANK\Users)	읽기 및 실행	C:\
허용	Users (ITBANK\Users)	옵션	C:\
허용	CREATOR OWNER	모든 권한	C:\

추가(D)

제거(R)

보기(V)

상속 사용 안 함(I)

상속 차단 X

현재 상속된 사용 권한을 어떻게 하시겠습니까?

이 개체의 상속을 차단하려고 합니다. 이렇게 하면 부모 개체로부터 상속된 사용 권한이 이 개체에 더 이상 적용되지 않습니다.

➔ 상속된 사용 권한을 이 개체에 대한 명시적 사용 권한으로 변환합니다.

➔ 이 개체에서 상속된 사용 권한을 모두 제거합니다.

취소

1. 상속된 권한을 유지하되 명시적 사용 권한으로 변환
2. 모두 제거(불편해서 활용X)

6. USERS는 삭제, 권한A는 읽기, 권한B는 쓰기만

CREATOR OWNER

SYSTEM

Administrators (ITBANK\Administrators)

권한A (ITBANK\권한A)

권한B (ITBANK\권한B)

권한A (ITBANK\권한A)

권한B (ITBANK\권한B)

추가(D)...

제거(R)

권한A의 사용 권한(P)

허용

거부

읽기 및 실행	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<div>^</div> <div></div> <div></div> <div>≡</div>
폴더 내용 보기	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
읽기	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

권한B (ITBANK\권한B)

추가(D)...

제거(R)

권한B의 사용 권한(P)

허용

거부

읽기 및 실행	<input type="checkbox"/>	<input type="checkbox"/>	<div>^</div> <div></div> <div></div> <div>≡</div>
폴더 내용 보기	<input type="checkbox"/>	<input type="checkbox"/>	
읽기	<input type="checkbox"/>	<input type="checkbox"/>	
쓰기	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

[네트워크 권한 VS NTFS 권한]

- 허용과 거부가 만나면 무조건 거부가 우선된다.
- 허용 및 거부 권한 VS Revoke = 허용 및 거부 권한이 설정
- 네트워크 권한 전부 허용(읽기,쓰기), NTFS권한으로 세부조정

GPO(Group Policy Object) : 그룹 정책 개체

도메인, OU에 적용할 정책과 설정 정보를 담고있는 일종의 컨테이너
OU별로 다른 정책 적용해서 OU를 통해 부서 관리

[그룹정책]

관리자들이 사용자/컴퓨터 사용 권한을 중앙에서 제어할 수 있도록 관리작업을 단순화하는 규칙의 집합
Workgroup,도메인환경에 따라 정책설정방법이 달라진다.
도메인환경에서는 DC에 정책설정하면 member에게 배포

Permission	right
권한	권한
Action on object	action on system

- right는 GPO를 이용해서 세팅한다.

[그룹 정책의 기능]

- 사용자/컴퓨터의 권한을 중앙에서 제어할 수 있도록 관리 작업 단순화
- Windows 구성 요소, 시스템 리소스, 네트워크 리소스, 제어판 유틸리티, 데스크톱, 시작메뉴 환경구성
- 사용자의 내 문서와 같은 특수 폴더에 대한 중앙집중화된 관리 디렉터리 생성 ---> 폴더리디렉션
- 지정된 시점(컴퓨터 부팅, 사용자 로그인)에 실행되는 사용자 및 컴퓨터 스크립트를 정의
- 계정 잠금, 암호 감사, 사용자 권한 할당, 보안에 관련된 정책 구성
- **GPO 적용될 사용자 지정불가, 도메인 혹은 OU에 적용시킨다.**

로컬 그룹 정책	도메인 그룹 정책
LGPO	GPO
Gpedit.msc	gpmmc.msc
독립실행형	도메인 컨트롤러 (DC)
정책 예외 불가	정책 적용 시 분리, 예외처리 가능

[컴퓨터 구성]	[사용자 구성]
컴퓨터 기준 정책	사용자 계정 기준 정책
로그온 계정 무관	로그온 컴퓨터 무관
시스템 시작 시	로그온 시

Default Domain Policy

- 도메인과 연결된 GPO가 중요하다
- 도메인 전체를 위해 자동 생성, 연결된 GPO
- 기본 계정 정책을 구성
- 보안설정은 도메인과 연결된 GPO에서 설정해야 한다.

Default Domain Controllers Policy

- DC를 위해 자동 생성, 연결된 GPO
- 도메인 컨트롤러가 Domain Controllers OU에서 제거되지 않는 이상 도메인 내의 모든 컨트롤러에 적용
- 사용자 권한이나 감사 정책 설정을 변경해야하는 도메인 컨트롤러에서 응용 프로그램을 설치할 경우 수정

GPO편집이 가능한 그룹

- Domain Admins, Enterprise Admins, Group Policy, Creator Owner

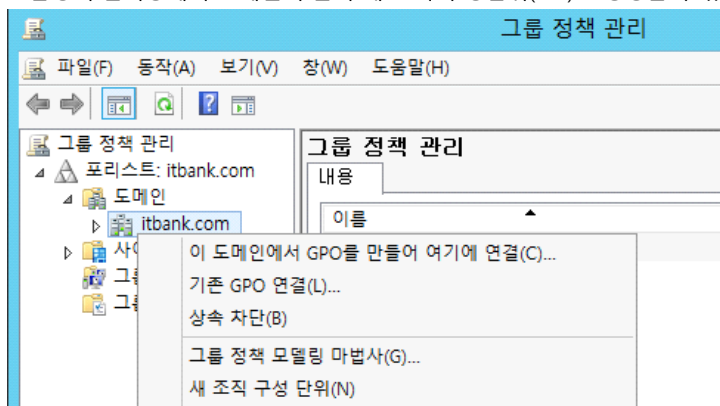
[GPO 생성, 연결]

- 기본적으로 그룹 정책 적용은 GPO를 도메인, OU에 연결하여 사용
- 연결된 개체없이 GPO만 단독으로 생성 가능하며 그룹정책 편집기의 생성된 GPO는 그룹정책개체 하위 생성된다.
- 미리 생성된 GPO를 정책을 적용할 대상에 불러와 연결해 사용
- 적용 대상 개체에서 GPO를 생성하여 직접 연결해 사용
- GPO와 개체의 연결을 삭제할 경우 GPO는 삭제되지 않음
- GPO를 적용 받은 개체를 삭제해도 GPO는 삭제되지 않음
- GPO를 삭제할 경우 연결된 모든 연결이 해제됨

[정책 상속]

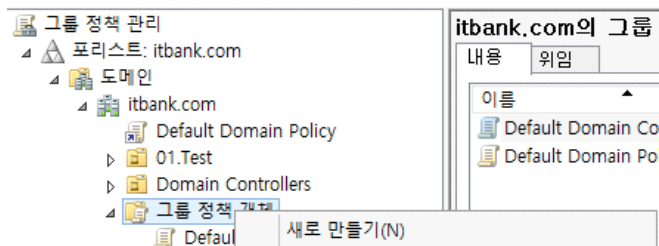
- 정책은 상위 컨테이너에서 하위 컨테이너로 상속된다.
- 상속은 거부하거나 강제 상속할 수 있다. 강제상속이 우선순위가 높다
- 강제 상속되는 GPO는 자물쇠 GPO아이콘이 Overlap됨
- 상속을 거부하면 컨테이너의 아이콘에 파란색 느낌표 추가
- 강제 상속은 상속 거부 불가

그룹정책 관리창에서 도메인 우클릭 새 조직 구성단위(OU)로 생성할 수 있다.

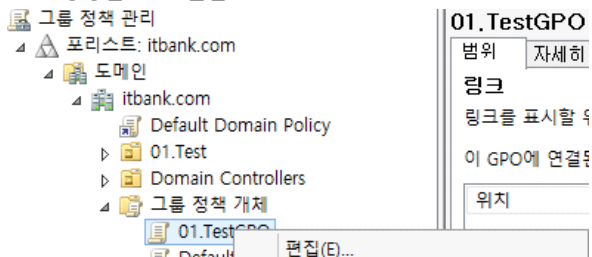


GPO 생성

1. 그룹정책 개체에서 새로만들기

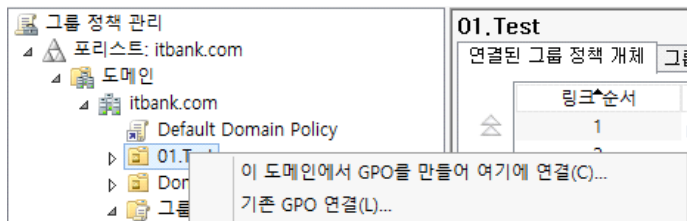


2. 생성한 GPO 편집

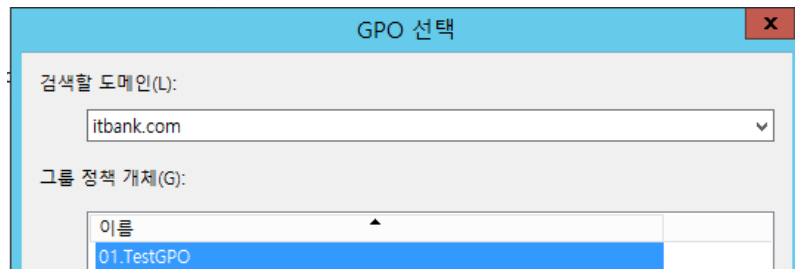


GPO 연결하는법

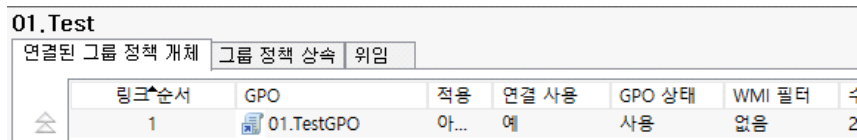
1. OU에서 기존GPO연결



2. 연결한 GPO선택

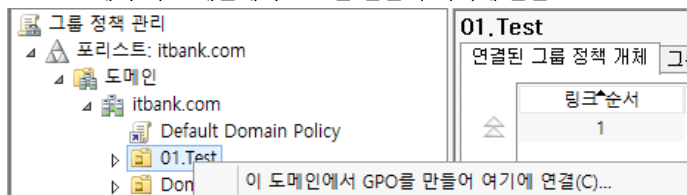


3. 연결완료



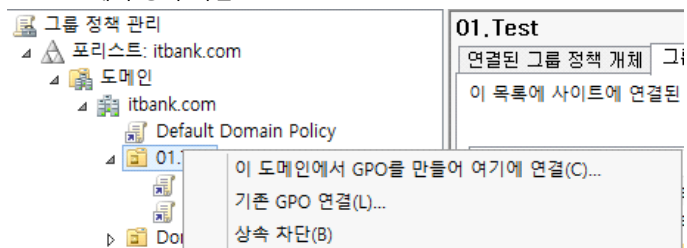
OR

1. OU에서 이 도메인에서 GPO를 만들어 여기에 연결



상속 차단하는법

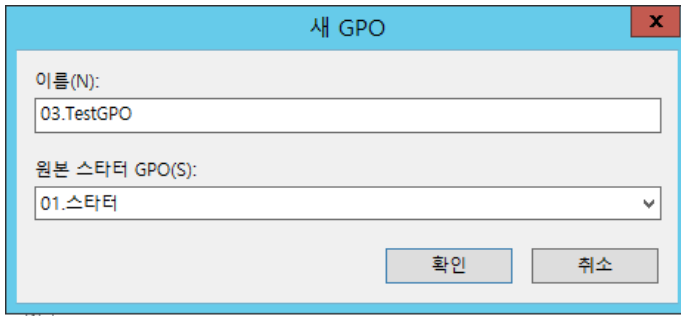
• Ou에서 상속 차단



강제 상속

상속 차단이여도 우선순위1순위로 적용

• GPO에서 적용



=> 새로만든 GPO에 스타터GPO의 정책이 반영되는 것을 알 수 있다.

[계정정책]

- 암호 정책, 계정 잠금 정책, Kerberos정책(인증정책) 등은 도메인 루트와 연결되는 정책만 설정 가능
- 기본 도메인 정책, 도메인이 연결되는 새로 만든 정책에서만 설정
- 도메인 계정 정책은 해당 도메인의 모든 구성원 컴퓨터들의 기본 계정 정책이됨
- 도메인과 연결된 GPO에서만 작업해야함

[정책적용시기]

- 사용자 컴터 시작/종료, 로그인/로그오프
- DC: 5분에 한번씩 적용
- Member : 기본 90분(정책에서 수정 가능)
- Gpupdate / force : 정책 수동 적용
- 정책설정은 정확하게 되었는데 적용이 안되면 컴퓨터 재부팅도 방법

=====

실습1. 컴퓨터 구성 : 01. 암호 정책

seoul >

그룹 정책 관리 (gpmc.msc) >

포리스트 >

도메인 >

itbank.edu >

default domain policy : 편집 >

그룹정책편집기 >

컴퓨터 구성 >

정책 >

windows 설정 >

보안 설정>

계정 정책>

계정 잠금 정책>

계정 잠금 임계값 : 5 >

계정 잠금 기간, 잠금 수 초기화 시간 : 기본 설정 > 확인

gpupdate /force

s1 계정 생성

busan >

s1 로그인 5회 실패 시도 >

seoul>

그룹 정책 관리 >

default domain policy : 편집 >

그룹정책편집기 >

컴퓨터 구성 >

정책 >

windows 설정 >

보안 설정>
계정 정책>
암호 정책>
암호는 복잡성을 만족해야 함 : 사용함 > 확인

그룹 정책 관리 >
그룹 정책 개체 >
정책 만들기 : 01. 암호 정책 >
그룹정책편집기 >
컴퓨터 구성 >
정책 >
windows 설정 >
보안 설정>
계정 정책>
암호 정책>
암호는 복잡성을 만족해야 함 : 사용안함

인사팀 ou 생성>
s1 > 인사팀 이동
01. 암호 정책 > 인사팀에 연결

gpupdate /force
dsa.msc >
s1 > 암호 다시 설정 >
password 설정 가능한지 확인 => 설정 가능

seoul>
그룹 정책 관리 >
default domain policy : 편집 >

그룹정책편집기 >
컴퓨터 구성 >
정책 >
windows 설정 >
보안 설정>
계정 정책>
암호 정책>
암호는 복잡성을 만족해야 함 : 사용안함
gpupdate /force
dsa.msc >
s1 > 암호 다시 설정 >
쉬운 암호 설정 가능한지 확인

실습2. 사용자 구성 : ou 제어판 액세스 금지(해당 정책적용 ou는 제어판 사용금지)
seoul >
인사팀 OU >
gp1@itbank.edu 생성

busan >
gp1 로그인 >
제어판 정상 실행 확인
시작 > 실행 > control.exe 실행 확인

seoul >
그룹 정책 관리
포리스트 >
도메인 >
itbank.edu >
인사팀 >
이 도메인에서 GPO를 만들어서 여기에 연결 : 02. 제어판 제한 >

그룹 정책 개체 >

02. 제어판 제한 : 편집 >

그룹 정책 관리 편집기 (02. 제어판 제한)

사용자 구성 >

정책 >

관리 템플릿 >

제어판 >

제어판의 액세스 금지 : 사용 >

busan >

gp1 재로그인 >

시작 메뉴 > 제어판 사라짐 확인

시작 > 검색 : 제어판 > 실행 불가 확인

시작 > 실행 > control.exe 실행 불가 확인

시작 > 실행 > sysdm.cpl, ncpa.cpl, appwiz.cpl 등 실행 불가 확인

실습3. 사용자 구성 : 홈페이지 설정 변경 제한

OU, 계정 생성

seoul >

인사팀 (OU)

계약직관리 (OU)

gp2@itbank.edu

정규직관리 (OU)

gp3@itbank.edu

그룹 정책 관리

그룹 정책 개체 >

새로 만들기 : 03. 홈페이지 설정 변경 제한 >

03. 홈페이지 설정 변경 제한 : 편집 >

그룹 정책 관리 편집기 (03. 홈페이지 설정 변경 제한)

사용자구성>

정책>

관리템플릿>

Windows 구성 요소 >

internet explorer >

홈페이지 설정 변경할 수 없음> <http://www.naver.com> 으로 고정

그룹 정책 관리

인사팀 >

03. 홈페이지 설정 변경 제한 GPO 연결 >

정규직 관리 >

(우클릭) 상속 차단 체크 >

busan >

gp2 로그인 >

실행 > inetcp.cpl > 제한됨 >

internet explorer 실행 > 도구 >

인터넷 옵션 실행 >

www.naver.com 수정 불가 설정됨 확인 >

gp3 로그인 >

실행 > inetcp.cpl > 실행됨 확인

실습4. 사용자 구성 : 바탕 화면에서 휴지통 아이콘 제거

seoul >

인사팀 OU에 GPO 생성 : 04. 바탕 화면에서 휴지통 아이콘 제거 > 편집

그룹 정책 관리 편집기 (04. 바탕 화면에서 휴지통 아이콘 제거)

사용자구성>
정책>
관리템플릿>
바탕화면>
바탕 화면에서 휴지통 아이콘 제거 : 사용>

busan >
gp2 > 휴지통 제거 확인

실습5. 사용자 구성 : 명령 프롬프트 사용 안 함
seoul >
인사팀 OU에 GPO 생성 : 05. 명령 프롬프트 사용 안 함 > 편집

그룹 정책 관리 편집기 (05. 명령 프롬프트 사용 안 함)
사용자구성 >
정책 >
관리템플릿 >
시스템 >
명령 프롬프트 사용 안 함 : 사용

busan >
gp1 로그인 >
실행 : cmd > 차단되는 것 확인

실습6. 컴퓨터 구성 : 사용자가 로그인 할 때 다음 프로그램 실행
seoul >
서버1 OU 생성 >
busan 컴퓨터 이동 >
서버1 OU에 GPO 생성 : 06. 사용자가 로그인 할 때 다음 프로그램 실행

그룹 정책 관리 편집 (06. 사용자가 로그인 할 때 다음 프로그램 실행)
컴퓨터 구성 >
정책 >
관리템플릿 >
시스템 >
로그온 >

사용자가 로그인 할 때 다음 프로그램 실행 : 사용 >
로그온 할 때 실행할 항목 >
"c:\program files\internet explorer\iexplore.exe" www.nate.com
(수정 기능 없으니 메모장에 옮겨 붙일 것)

busan >
아무 계정 로그인
gpupdate /force (컴퓨터 구성 정책이므로 안될 경우 리부팅)
gp1 로그인 > iexplore 실행 확인

[\\seoul\로그온스크립트\\$](#)

실습8. 컴퓨터 구성 : 시작 스크립트(bat파일을 정책으로 설정해서 부팅시 자동 실행)

busan >

c:\start 폴더 생성 >

문서 파일 생성 >

test 폴더 생성 >

test 폴더 아래 test.txt 문서 파일 생성 >

seoul >

바탕 화면에 시작.bat 작성 >

rmdir /s /q c:\start

서버1 OU에 GPO 생성 : 08. 시작 스크립트

그룹 정책 관리 편집 (08. 시작 스크립트)

컴퓨터 구성 >

windows 설정 >

스크립트 (시작/종료) >

시작프로그램 속성 >

파일 표시 : 시작.bat 붙여 넣기 >

추가 : 찾아보기 > 시작.bat 선택

busan >

재부팅 >

탐색기에서 start 폴더 삭제 확인

실습9. 사용자 구성 : 드라이브 맵

seoul >

c:\드라이브맵 폴더 생성 >

드라이브맵\$ 숨김 공유 >

everyone, 읽기+변경 >

인사팀 OU에 GPO 생성 : 9. 드라이브 맵

그룹 정책 관리 편집 (9.드라이브 맵)

사용자 구성 >

기본 설정 >

Windows 설정 >

드라이브 맵 >

새로 만들기 : 매핑된 드라이브 >

동작 : 업데이트 >

위치 : [\\itbank.edu](http://itbank.edu)\드라이브맵\$

지정할 레이블 : 매핑된 드라이브

드라이브 문자 > 사용 : x 선택

busan >
gp1 재로그온 >
탐색기에서 확인

실습10. 컴퓨터 구성 : 사용자 권한 할당 - 로컬 로그인 거부(원하는 계정 접근 차단 가능)
seoul >
gp4@itbank.edu 계정 생성

busan >
gp4 로그인 > 확인

seoul >
그룹 정책 관리 편집 (default domain policy)
컴퓨터 구성 >
정책 >
windows 설정 >
보안 설정 >
로컬 정책 >
사용자 권한 할당 >
로컬 로그인 거부 : 이 정책 설정 정의 체크 >
사용자 또는 그룹 추가 >
gp4 추가 > (찾아보기로 추가할 것)

busan >
gpupdate /force >
gp4 로그오프 > 로그인 > 로그인 불가

실습11. 컴퓨터 구성 : 사용자 권한 할당 - 시간대 변경, 시간 변경
seoul >
gp5@itbank.edu 계정 생성

그룹 정책 관리 편집 (default domain policy)
컴퓨터 구성 >
정책 >
windows 설정 >
보안 설정 >
로컬 정책 >
사용자 권한 할당 >
시간대 변경 : 이 정책 설정 정의 체크 >
사용자 또는 그룹 추가 >
gp5 추가 >
시스템 시간 변경 : 이 정책 설정 정의 체크 >
사용자 또는 그룹 추가 >
gp5 추가 >

busan >
gpupdate /force >
administrator@itbank.edu 로그인 >
시간대 변경, 날짜 및 시간 변경 가능 확인 >

gp5 로그인 >
시간대 변경, 날짜 및 시간 변경 가능 확인

다른 gp들 로그인하면 시간대 변경 불가 확인

실습12. 컴퓨터 구성 : DC에 일반 계정 로그인
seoul >
itbank.edu >
domain controllers >

default domain controllers policy : 편집 >

컴퓨터 구성 >

정책 >

windows 설정 >

보안 설정 >

로컬 정책 >

사용자 권한 >

로컬 로그인 허용 >

관리자 그룹들만 허용되도록 되어 있음

gp5 추가 >

gpupdate /force >

gp5로 로그인

실습13. 컴퓨터 구성 : 보안 옵션 - administrator 이름 바꾸기

seoul >

그룹 정책 관리 편집 (default domain policy)

컴퓨터 구성 >

정책 >

windows 설정 >

보안 설정 >

로컬 정책 >

보안 옵션 >

계정 : Administrator 계정 이름 바꾸기 >

이 정책 설정 정의 : root >

gpupdate /force >

administrator 로그오프 >

administrator 로그인 > (로그온 불가)

root@itbank.edu 로그인 >

root를 다시 administrator로 설정 >

> 반드시 재로그인!

실습14. 컴퓨터 구성 : 보안 옵션 - 로그인 시 메시지 보이게 하기

seoul >

그룹 정책 관리 편집 (default domain policy)

컴퓨터 구성 >

정책 >

windows 설정 >

보안 설정 >

로컬 정책 >

보안 옵션 >

대화형 로그인 : 로그온을 시도하는 사용자에게 대한 메시지 제목

이 정책 설정 정의 : 공지 제목 입력 (제목 반드시 설정 해야 함)

대화형 로그인 : 로그온을 시도하는 사용자에게 대한 메시지 텍스트

템플릿에 이 정책 설정 정의 : 공지 내용 입력

busan >

gpupdate /force >

로그오프시 공지 팝업 확인

실습15. 보안템플릿(템플릿을 만들어놓으면 일일이 설정할 필요가 없다)

- 그룹 정책 중 보안 설정만 별도로 샘플을 만들어 적용하기 전에 분석(비교)후 적용할 수 있는 도구

- 보안 설정을 저장하거나 불러오고 다른 내용과 비교 가능

mmc.exe >

파일 >

스냅인 추가/제거 >

보안 템플릿 추가 >

보안 구성 및 분석 추가 >

바탕화면에 '보안 템플릿'으로 저장 (보안 템플릿 도구 완성)

보안 템플릿.msc 실행 >

보안 템플릿 > (템플릿)

c:\users\administrator\documents\security\templates 우클릭 : 새 템플릿 >

'계정 정책 적용'으로 생성 >

계정 정책 >

계정 정책 > 암호 정책 수정

계정 정책 적용 : 저장 (우클릭) > (저장 비활성화 될 때까지 저장)

보안 구성 및 분석 > (데이터베이스)

데이터베이스 열기 : DB1 (데이터베이스 이름 지정) > (저장한 db가 없으면 이름지어서 만들면 된다)

C:\User\사용자\document\security\database

템플릿 가져오기 : 계정 정책 적용.inf 선택 >

C:\User\사용자\document\security\templates

지금 컴퓨터 분석 > (db상 정한 정책과 컴퓨터에 설정된 정책을 비교)

계정 정책 >

암호 정책 > 항목들 체크 표시 생긴 것 확인 (x : 일치하지 않음 v 일치)

내용 수정 >

보안 구성 및 분석 : 저장 (우클릭) >

템플릿 내보내기 > 계정 정책 적용 - 최종

그룹 정책 관리

default domain policy : 편집 >

컴퓨터 구성 >

정책 >

windows 설정 >

보안 설정 : 정책 가져오기 (우클릭) >

계정 정책 적용 - 최종.inf 열기 >

16. 그룹정책 백업 & 복원

그룹 정책 관리 >

그룹 정책 개체 >

모두 백업 >

모두 백업 > (1회 더)

백업 관리 >

정책 선택 > 복원 > 확인

01. 암호 정책 선택 >

백업에서 복원 > (자신의 백업을 자동으로 인식하여 보여줌)

정책 선택 >

설정 가져오기 > (다른 백업에서 설정을 가져옴)

17. 실습 스타터 GPO

그룹정책에서 관리 템플릿을 미리 설정하여 사용

그룹 정책 관리 >

스타터 GPO >

새로 만들기 >

스타터GPO 샘플 : 편집 >

그룹 정책 편집기 >

그룹 정책 개체 >

새로 만들기 >

원본 스타터 GPO

18. 그룹 정책 모델링

도메인 컨트롤러와 사용자와 컴퓨터, 컨테이너, ou를 조합하여 그룹 정책 적용을 시뮬레이션한 결과를 출력

그룹 정책 관리 >

그룹 정책 모델링 (우클릭) >

그룹 정책 모델링 마법사 >

도메인 컨트롤러 선택 >

사용자 (컨테이너) 선택 >

컴퓨터 (컨테이너) 선택 >

사이트 : default-first-site-name >

추가 데이터를 수집하지 않고 마법사의 마지막 페이지로 이동 : 체크 >

결과 확인 >

19. 그룹 정책 결과

컴퓨터와 사용자를 조합하여 적용되는 정책의 결과 출력

그룹 정책 관리 >

그룹 정책 결과 >

그룹 정책 결과 마법사 >

컴퓨터 선택 >

사용자 선택 >

결과 확인

20. 그룹 정책 관리 위임

도메인, 사이트, ou에 대해 정책 관리를 위임

그룹 정책 관리 >

인사팀 >

우측 위임 탭 >

권한 : GPO 연결 선택 >

gp5 추가

gp5로 사용자 전환

그룹 정책 관리 >

서버1 > 그룹 정책 관련 메뉴 비활성화

인사팀 > 권한 정책 연결, 삭제 가능

21. 정책 새로 고침 간격 설정

도메인 컨트롤러는 기본 적으로 5분마다 정책 변경을 체크

그룹 정책 관리 >

default domain policy : 편집 >

컴퓨터 구성 >

정책 >

관리 템플릿 >

시스템 >

그룹 정책 >

컴퓨터에 대한 그룹 정책 새로 고침 간격 : 사용 >

기본 적용 빈도 : 90분

추가 임의 시간 : 30분

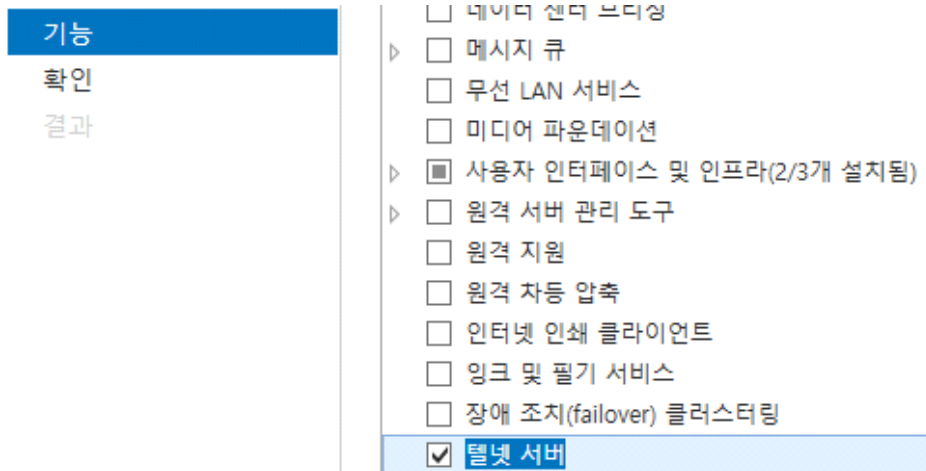
원격접속

2018년 10월 4일 목요일 오후 2:29

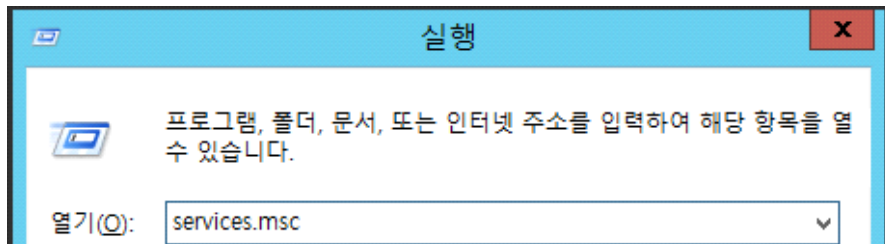
Telnet

• 사용방법

1. 역할 및 기능 추가 마법사의 기능탭에 한곳(seoul)은 텔넷 서버,한곳(busan)은 텔넷 클라이언트



2. 텔넷 서비스 설치 후 활성화 시켜줘야 한다.



3. telnet을 찾아서 시작유형을 자동으로 변경/시작버튼까지 누를것

이름	설명	상태	시작 유형
Task Scheduler	사용...	실행 ...	자동
TCP/IP NetBIOS Helper	NetB...	실행 ...	자동(트리...
Telephony	로컬 ...		수동
Telnet	원격 ...		자동

속도가 빨라 내부통신할때는 텔넷이 좋다.

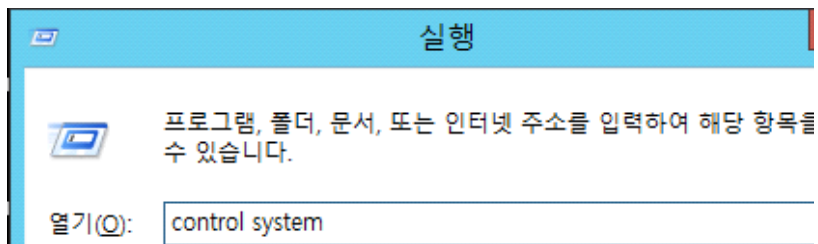
암호화를 거치면 리소스 소모량이 높다.

같은 네트워크 영역 내에서만 사용할 것.

원격데스크톱




• 사용방법

1. cmd창에 control system



2. 원격 설정으로 이동

제어판 홈

-  장치 관리자
-  원격 설정
-  고급 시스템 설정

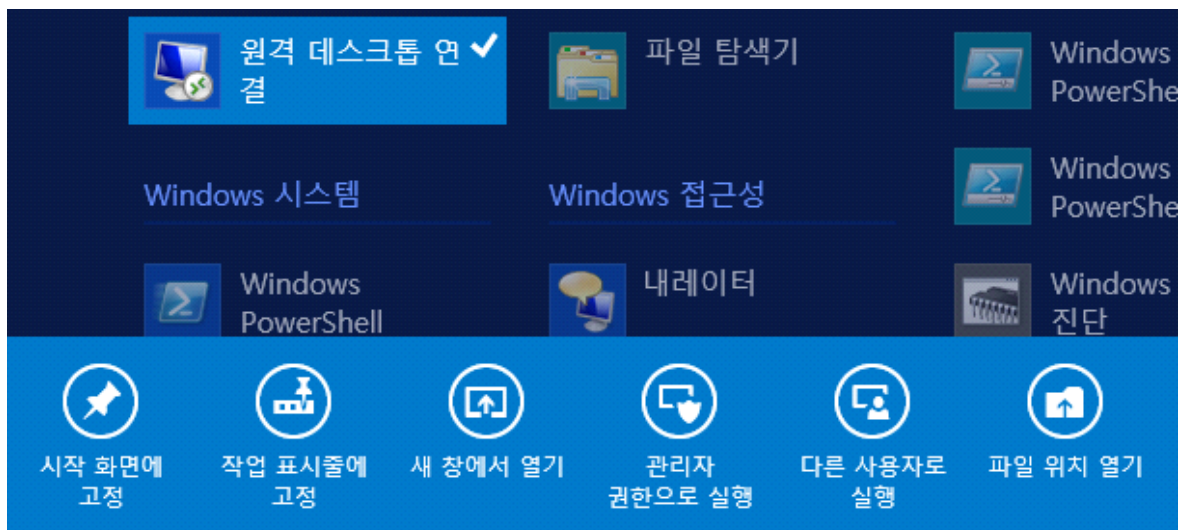
3. 원격 연결 허용으로 변경

원격 데스크톱

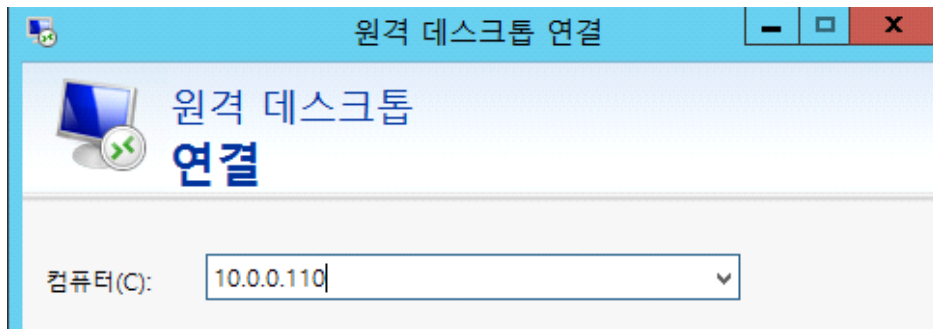
옵션을 선택한 다음 연결할 수 있는 사용자를 지정합니다.

- ☐ 이 컴퓨터에 대한 원격 연결 허용 안 함(D)
- ☒ 이 컴퓨터에 대한 원격 연결 허용(L)
- ☒ 네트워크 수준 인증을 사용하여 원격 데스크톱을 실행하는 컴퓨터에서만 연결 허용(권장)(N)

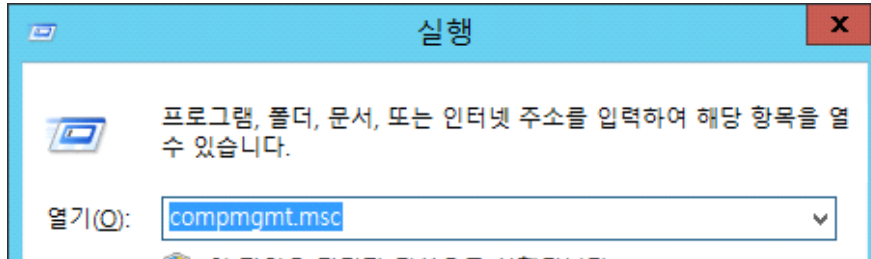
4. 시작탭에 원격데스크톱 우클릭 해서 작업 표시줄에 연결



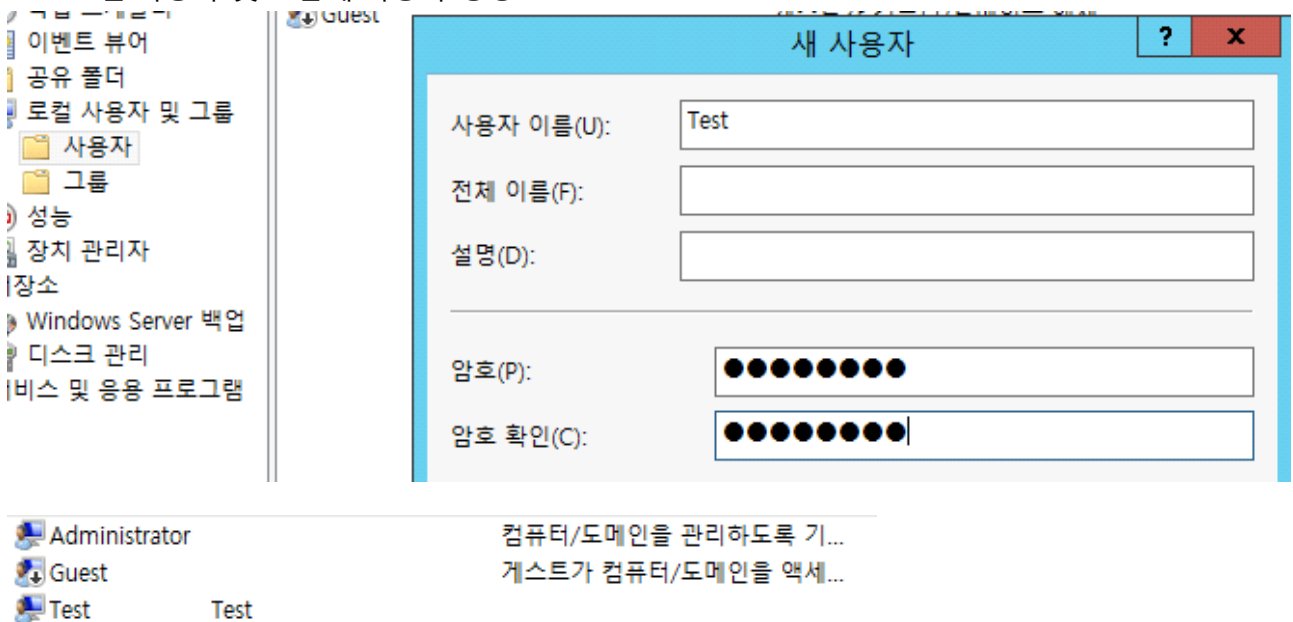
5. 원격 연결할 컴퓨터 ip 입력



- 일반 사용자 계정으로 원격 접속 하는법
1. Cmd 창에 Compmgmt.msc

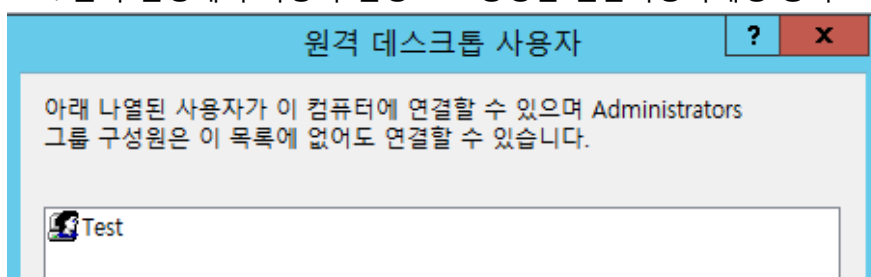


2. 로컬 사용자 및 그룹에 사용자 생성



3. cmd창에 control system

4. 원격 설정에서 사용자 설정으로 생성한 일반사용자계정 등록



5. remote desktop users의 구성원이여야 원격 데스크톱으로 접속할수 있는 계정이 된다.

6. 원격 데스크톱 연결할때 사용자 이름을 test로 변경



연결설정에서 다른이름으로 저장을 통해 접속파일을 생성하면 그 파일을 통해 바로 원격접속이 가능

디스크 관리하는 법

2018년 10월 8일 월요일 오후 12:36

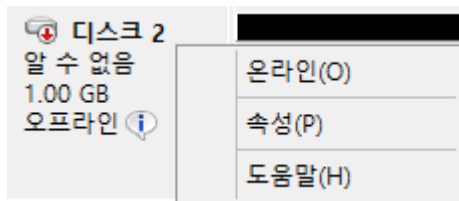
엔진 세팅가서 HDD 1GB 13개 추가 > diskmgmt.msc로 확인

디스크 관리 하는 방법

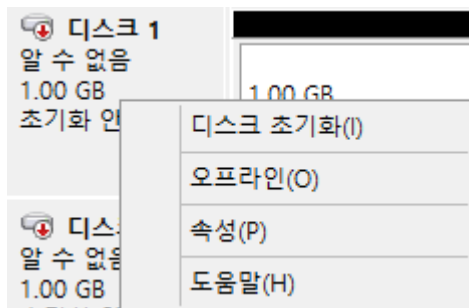
- 일반적인 형태 관리
 - 파티션나누는 것
- 동적 형태 관리
 - 레이드,

단순 볼륨

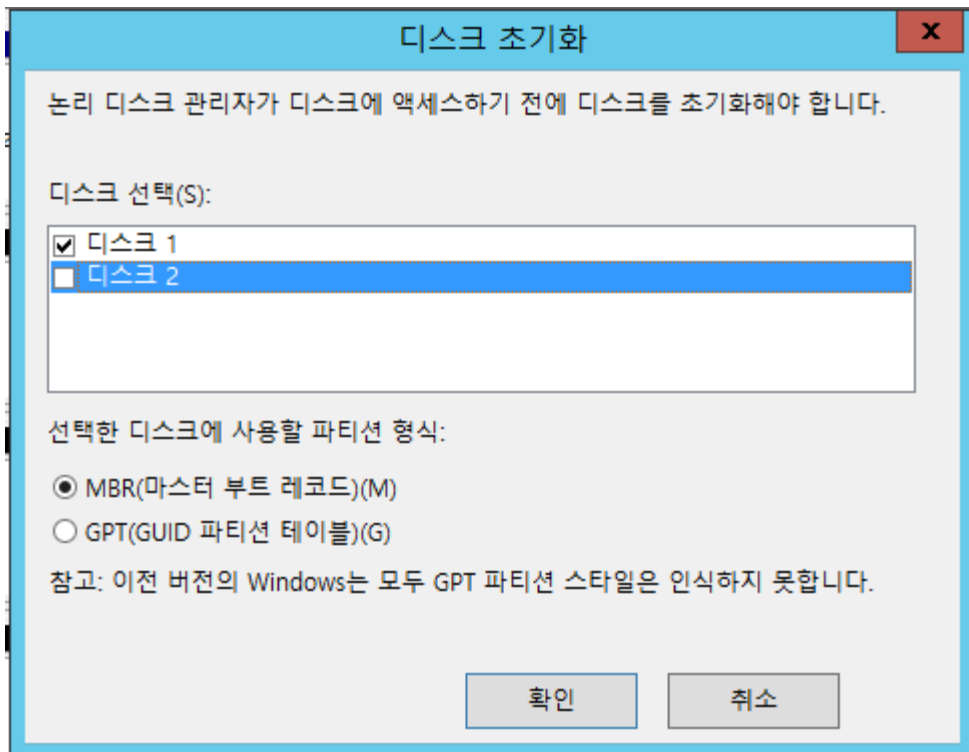
디스크 1번,2번을 온라인 상태로 변경 -> 디스크 선택후 우클릭으로 온라인 선택



초기화 안됨이라고 나오는건 초기화가 안된 것, 초기화 해야함



디스크1번은 MBR, 디스크2번은 GPT, 나머지는 MBR로 초기화



MBR : 파티션 공간이 4개(=primary를 4개), 각 공간마다 16Byte,
 마지막은 확장파티션(EXTENDED)이 자동으로 생성, 2.3TB이하만 단일 디스크로 인식
 primary로 만들려면 커맨드작업을 해야한다.

GPT : 최대 128개까지(=primary를 128개), 2.3TB이상

디스크1번을 새 단순 볼륨 선택



단순 볼륨 크기(파티션 크기) 100MB

최대 디스크 공간(MB):	1021
최소 디스크 공간(MB):	8
단순 볼륨 크기(MB)(S):	<input type="text" value="1021"/>

드라이브 문자 할당이나 마운트 작업을 해야지 경로설정및 사용이 가능하다

☒ 드라이브 문자 할당(A):

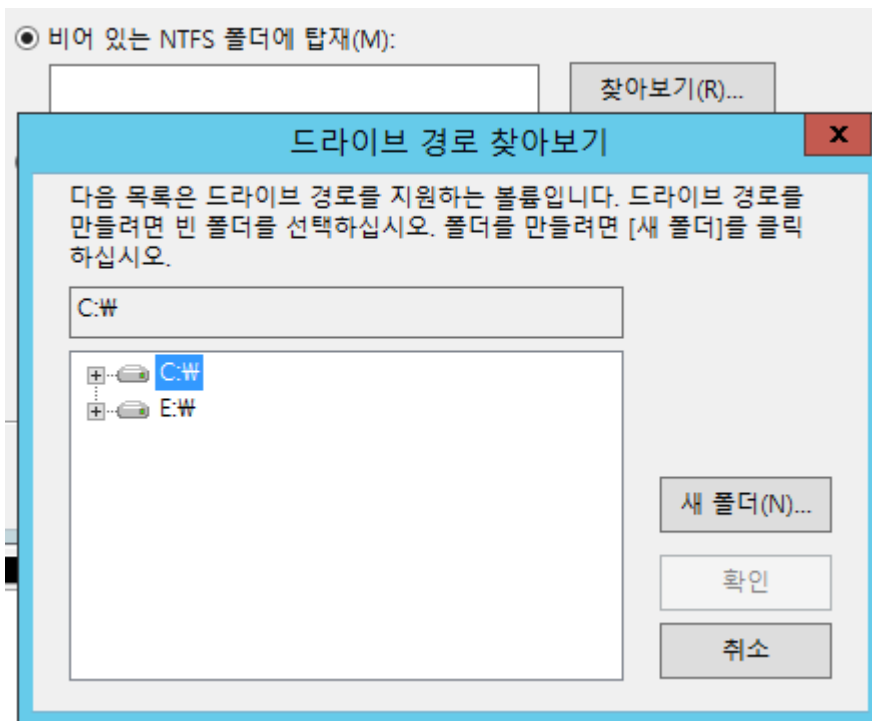
☐ 비어 있는 NTFS 폴더에 탑재(M):

☐ 드라이브 문자 또는 드라이브 경로를 할당하지 않음(D)

파일시스템은 NTFS로 해야 로컬권한을 사용할 수 있다.

할당 단위 크기는 클러스터값 지정, 기본값은 4KB
파일 및 폴더 압축 사용 선택하면 하드가 절반 사용된다

C:\에 Mount 폴더 생성하고 디스크 1번 빈공간에 단순 볼륨 만들기
볼륨크기는 100MB설정하고 비어있는 NTFS 폴더에 탑재 선택해서 생성



파티션을 여러 개 나눠야 할 경우 마운트를 많이 활용 한다.

디스크 1번,2번에 100MB 파티션 4개 생성 (단,문자할당 및 마운트 x)

디스크 1 기본 1023 MB 온라인	새 볼륨 (E) 100 MB NTFS 정상 (주 파티션)	새 볼륨 100 MB NTFS 정상 (주 파티션)	새 볼륨 100 MB NTFS 정상 (주 파티션)	새 볼륨 100 MB NTFS 정상 (논리 드라이브)	622 MB 사용 가능한 공간
	새 볼륨 100 MB NTFS 정상 (주 파티션)	새 볼륨 100 MB NTFS 정상 (주 파티션)	새 볼륨 100 MB NTFS 정상 (주 파티션)	새 볼륨 100 MB NTFS 정상 (주 파티션)	592 MB 할당되지 않음

마지막 볼륨은 확장 및 줄이기가 가능하다. 하지만 앞에 있는 볼륨들은 자유롭지 못하다.
=> 기존 가지고 있던 공간 내에서만 가능하다.
=> 확장 축소를 하다보면 기록을 남겨야하는데 그 기록 1MB이 사용된다.

동적 디스크

레이드 : 디스크 성능을 향상 할 수 있다.

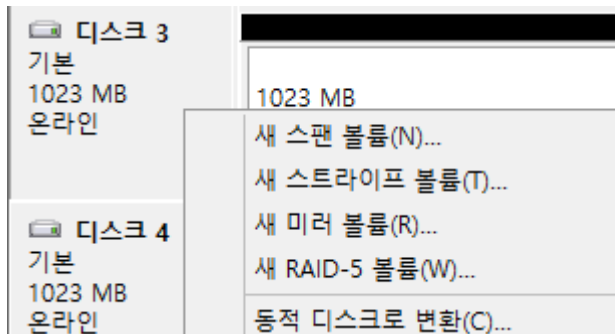
하드웨어적 레이드 : 레이드 장치를 활용하여 하드웨어를 연결

소프트웨어적인 레이드 : 논리적으로 OS에서 지원, 하드웨어적 레이드보다 성능이 떨어진다.

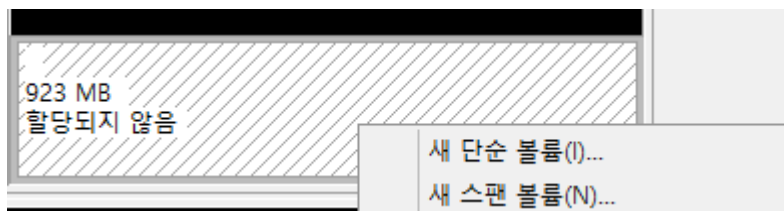
스팬볼륨

편리성이 뛰어난 반면 위험가능성이 있다.(만약 4번이 고장나면 3번도 같이 고장난다)

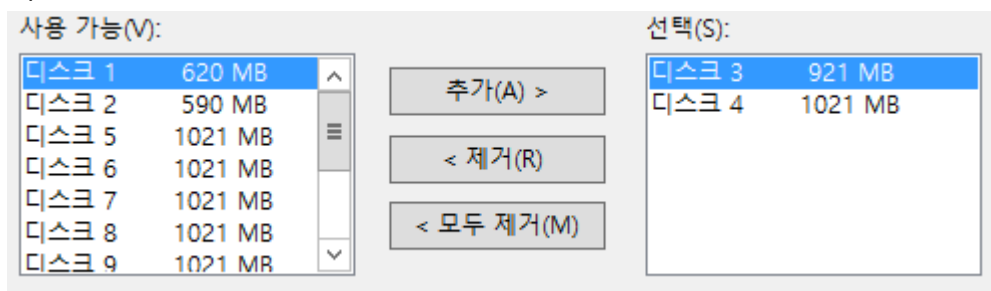
디스크 3번부터 싹다 동적디스크로 변환



디스크 공간 우클릭하여 새 스펠 볼륨 선택



디스크4번을 결합



스트라이프 볼륨

- RAID(레이드)
 - 0,1,5번까지 2,3,4는 사용하지 않는다.
 - 0번은 스트라이프 볼륨, 디스크의 속도를 높이는게 목적, 여러개가 동시에 저장
저가형 레이드는 0번만 지원,
 - 1번 레이드
미러 볼륨, 디스크의 개수를 짝수로 잡아야한다.
속도 안빨라지고 데이터의 안정성만 우선
 - 5번 레이드
하드가 최소 3개이상 있어야 한다.
패리티(복구)비트가 있으며 복구비트를 제외하고 두개씩 저장한다.
패리티(복구)비트에는 같으면 0, 다르면 1이 저장된다.

용량을 10GB 3개를 묶어도 패리티(복구)비트로 인해 20GB만 사용할 수 있다.

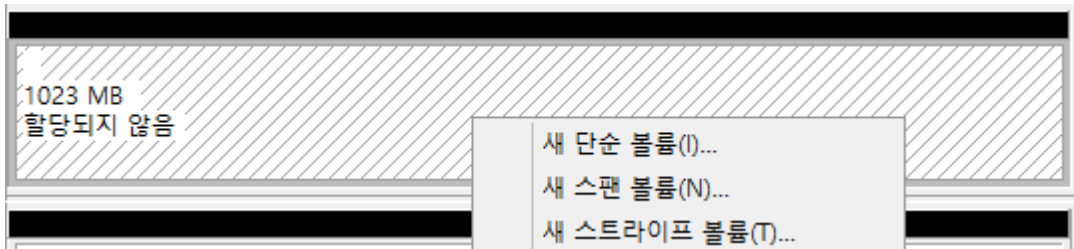
- 6번 레이드

하드가 최소 4개 이상 있어야 한다.

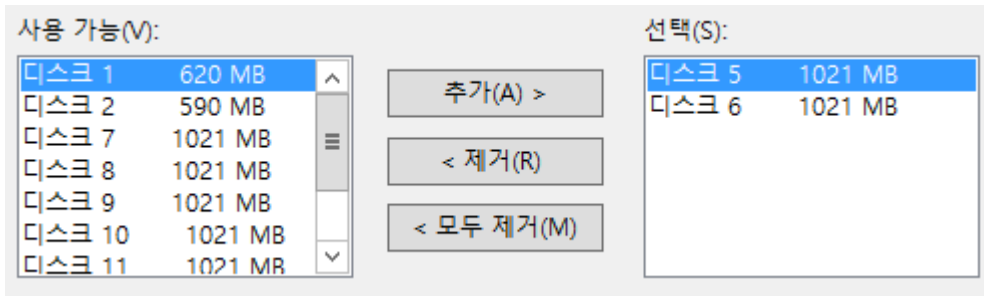
패리티(복구)비트를 이중으로 저장한다.

레이드 0번 만들기

디스크 5번 우클릭 새 스트라이프 볼륨 선택

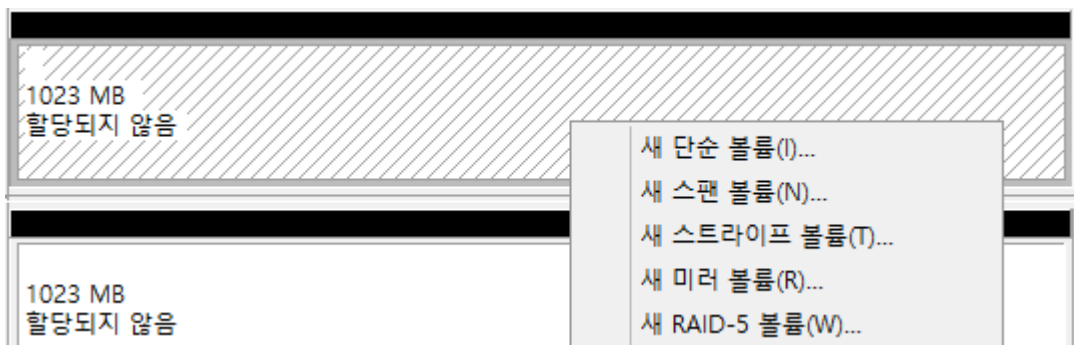


디스크 6번 추가 후 빠른 포맷

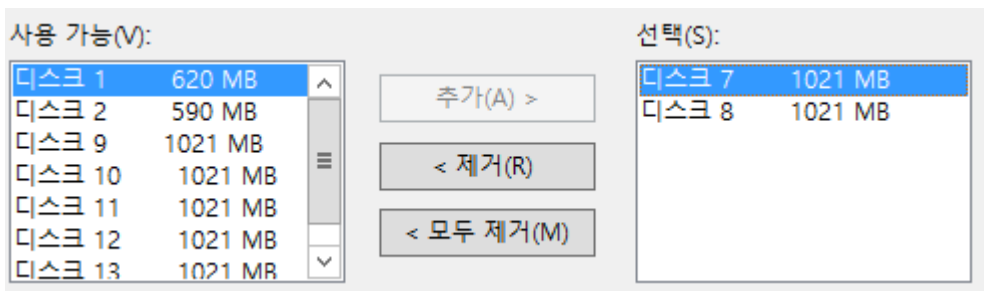


레이드 1번 만들기

디스크 7번 우클릭 새 미러볼륨 마법사 선택

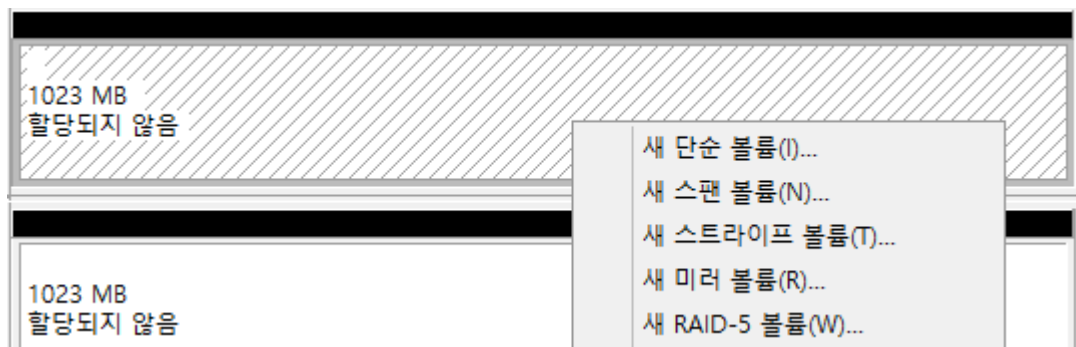


디스크 8번 추가 후 빠른 포맷

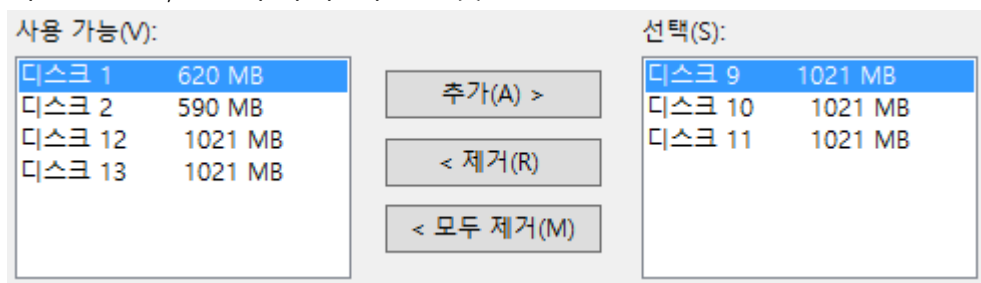


레이드 5번 만들기

디스크 9번 우클릭 새 RAID-5볼륨 선택



디스크 10번,11번 추가 후 빠른 포맷



디스크 12번,13번은 복구 용도

하드디스크 9번, 하드디스크 11번 삭제

=> VMWARE setting 들어가서 지워야함. 40G하드가 1번이니 +1번해서 해당 디스크 삭제

디스크7번 우클릭해서 미러삭제를 통해 일반 디스크로 복구하고 새로운 디스크(12번)와 미러를 맺는다.
디스크9번 우클릭해서 볼륨복구를 통해 새로운 디스크 13번을 선택하면 RAID 구성

=====

커맨드 작업(항상 디스크를 지정하고 작업)

- diskpart: disk online 하기

시작> cmd> diskpart

DISKPART>list disk

DISKPART>select disk 1

DISKPART>list disk 선택된디스크는* 표시가생긴다

DISKPART>online disk

DISKPART>attributes disk clear readonly

- diskpart : partition 생성

```
DISKPART>create partition primary size 100
DISKPART>create partition extended size 100
DISKPART>create partition logical size 50
DISKPART>list partition
DISKPART>select partition 3
DISKPART>delete partition
DISKPART>select partition 0
DISKPART>delete partition
Primary 는 지우지 말 것 바로 다음에 사용할 거니까
```

- diskpart : 드라이브에 경로 할당

드라이브 경로 할당(알파벳)

```
DISKPART>list partition
DISKPART>Select partition 1
DISKPART>Assign letter=G
DISKPART>remove letter=G
DISKPART>exit
```

드라이브 경로 할당(특정 폴더에 마운트)

```
cd\
c:\mkdir mount
c:\diskpart
DISKPART>select disk 1
DISKPART>list partition
DISKPART>select partition 2
DISKPART>assign mount=c:\mount
DISKPART>remove mount=c:\mount
```

※ 할당한 경로 삭제 = remove

- diskpart : partition 확장 축소

파티션 확장(확장 파티션 없는 상태에서 실행)

```
DISKPART>list disk
DISKPART>select disk 1
DISKPART>create partition primary size 100
DISKPART>list partition
DISKPART>select partition 3
DISKPART>extend size 100
DISKPART>list partition
```

파티션 축소

```
DISKPART>select partition 3
DISKPART>shrink querymax
=> 사용 가능한 바이트 수 확인
DISKPART>shrink desired 40
=> 40바이트만큼 축소
```


DISKPART>list partition

- diskpart : 동적디스크변환, 단순볼륨생성

동적디스크변환

DISKPART>list disk

DISKPART>select disk 1

DISKPART>convert dynamic

11번까지모두반복해서실행해보도록한다.

동적디스크변환후단순볼륨생성

DISKPART>list disk

DISKPART>select disk 2

DISKPART>create volume simple size 100

- diskpart : volume 확장축소

동적디스크변환후볼륨확장축소

DISKPART>detail volume

DISKPART>list volume

DISKPART>select volume 5

DISKPART>extend size 100

DISKPART>list volume

DISKPART>select volume

DISKPART>shrink querymax

DISKPART>shrink desired 100

- diskpart : span volume

DISKPART>list disk

DISKPART>select disk 3

DISKPART>create volume simple size 1000

DISKPART>extend size 1000 disk 4

- diskpart : stripe volume (RAID-0)

DISKPART>list disk

DISKPART>create volume stripe size 1000 disk 5,6

DISKPART>format fs=ntfs quick

- diskpart : Mirror(RAID-1) Volume

DISKPART>list disk

DISKPART>select disk 7

DISKPART>detail disk

DISKPART>create volume simple size 1000

DISKPART>add disk 8

- diskpart : Stripe with parrity (RAID-5) Volume

DISKPART>list disk

DISKPART>select disk 9

DISKPART>create volume raid size 1000 disk 9,10,11

※ 스크립트 만드는법(C:\diskpart.txt)

배치파일처럼 메모장에 커맨드를 작성하면 된다.

.txt로 그대로 뒤야 한다.

Clean = diskprt에서 해당 디스크를 초기화

Diskpart /s 경로 (c:\diskpart.txt)

백업

2018년 10월 10일 수요일 오후 2:45

백업은 선택이 아니라 필수 !!

백업의 종류		백업 시작전 data	1회차		2회차		3회차		4회차	
			추가	백업된 데이터	추가	백업된 데이터	추가	백업된 데이터	추가	백업된 데이터
Full	전체	A	A	A	B	A+B	C	A+B+C	D	A+B+C+D
incremental	증분		A	A	B'	B	C'	C	D'	D
diffrential	차등		A		B'		B'+C'		B'+C'+D'	
update -daily -weekly	업데이트		A		B		New B		N.New B	
- archive bit : 새로 생성된 파일에 자동으로 구성되는 체크비트 - 증분: 백업 후 아카이브 비트 제거										

FULL(전체) 백업 : 존재하는 모든 데이터를 백업, 기존 백업 데이터에 추가 데이터를 합해 백업
archive bit를 사용 하지 않는다.

- 장점 : 백업의 신뢰도 ↑, 안정성 ↑
- 단점 : 백업된 데이터 크기 ↑, 백업 속도 ↓

Incremental 백업 : 증가된 데이터들만 백업, 변경된 데이터들만 백업

Archive bit : 백업데이터인지 아닌지 확인할 수 있는 비트(1 : 생성, 0 : 백업)

Diffrential 백업 : 1회차때 0으로 변경, 2회차때부터 1을 유지, 3회차때 유지
즉, 1회차때만 archive bit를 변경, 2회차부터 변경X

UPDATE 백업 : 백업 이미지를 하나만 만들어서 데이터를 추가하는 형식

실습

1. 40G 하드 2개 추가 생성
2. 단순 볼 생성



3. 서버관리자에 역할 및 기능추가의 기능탭에 Windows Server 백업 선택



기능 선택

시작하기 전	선택한 서버에 설치할 기능을 하나 이상 선택하십시오. 기능 <input type="checkbox"/> Windows Search 서비스 <input type="checkbox"/> Windows Server 마이그레이션 도구 <input checked="" type="checkbox"/> Windows Server 백업
설치 유형	
서버 선택	
서버 역할	
기능	

4. 제어판 → 시스템 및 보안 → 관리도구 → windows server 백업

5. 로컬 백업 하위에 한번 백업 선택

6. 다른 옵션 선택

백업 옵션	다음을 사용하여 지금 백업 만들기: <input type="radio"/> 예약된 백업 옵션(S) 예약된 백업을 만들었거나 이 백업에 같은 설정 <input checked="" type="radio"/> 다른 옵션(D) 예약된 백업을 만들지 않았거나 예약된 백업과 지정하려면 이 옵션을 선택합니다.
백업 구성 선택	
대상 형식 지정	
확인	
백업 진행률	

예약된 백업 옵션 : 사전에 백업을 만들었거나 예약

다른 옵션 : 예약된 백업이 없거나 다른 위치에 백업을 지정

7. 사용자 지정

백업 옵션	예약할 구성 형식을 선택하십시오. <input type="radio"/> 전체 서버(권장)(U) 모든 서버 데이터, 응용 프로그램 및 시스템 백업 크기: 9.15GB <input checked="" type="radio"/> 사용자 지정(C) 백업할 파일, 사용자 지정 볼륨을 선택하십시오.
백업 구성 선택	
백업할 항목 선택	
대상 형식 지정	
확인	
백업 진행률	

전체 서버 : 모든 data를 백업

사용자 지정 : 지정한 data만 백업

8. 항목 추가로 c:\w 추가

백업 옵션	백업할 항목을 선택하십시오. 완전 복구 옵션을 사용할 수 있습니다. 이름 로컬 디스크(C:)
백업 구성 선택	
백업할 항목 선택	
대상 형식 지정	
확인	
백업 진행률	

항목 추가 탭을 활용해서 백업할 대상 지정

9. E:\w에 저장

백업 옵션	백업을 저장할 볼륨을 선택하십시오. 이 컴퓨터에 연결된 외부 디스크는 볼륨으로 나열됩니다. 백업 대상(B): 새 볼륨 (F:)
백업 구성 선택	
백업할 항목 선택	

백업 옵션	백업을 저장할 볼륨을 선택하십시오. 이 컴퓨터에 연결된 외부 디스크는 볼륨으로 나열됩니다.	
백업 구성 선택	백업 대상(B):	새 볼륨 (E:)
백업할 항목 선택	백업 대상의 전체 공간:	40.00GB
대상 형식 지정	백업 대상의 사용 가능한 공간:	39.90GB
백업 대상 선택		
확인		
백업 진행률		

로컬드라이브도 속도가 느리지만 원격 공유 폴더를 선택하면 백업 이미지를 백업하는데 속도가 너무 느리다.

10. 백업 진행하면 끝

백업 옵션	상태: 완료되었습니다.							
백업 구성 선택								
백업할 항목 선택	상태 정보							
대상 형식 지정	백업 위치: E:							
백업 대상 선택	전송된 데이터: 7.72GB							
확인								
백업 진행률	<table border="1"> <thead> <tr> <th>항목</th> <th>상태</th> <th>전송된 데이터</th> </tr> </thead> <tbody> <tr> <td>로컬 디스크(C:)</td> <td>완료되었습니다.</td> <td>7.72GB 중 7.72GB</td> </tr> </tbody> </table>		항목	상태	전송된 데이터	로컬 디스크(C:)	완료되었습니다.	7.72GB 중 7.72GB
항목	상태	전송된 데이터						
로컬 디스크(C:)	완료되었습니다.	7.72GB 중 7.72GB						

11. E:\ 들어가면 백업 이미지를 확인할 수 있다.

<< 새 볼륨 (E:) >> WindowsImageBackup > Seoul >

이름	수정일
Backup 2018-10-11 034405	2018-
Catalog	2018-
Logs	2018-
SPPMetadataCache	2018-
MediaId	2018-

복구 하는법

1. 로컬백업의 복구 선택

작업
로컬 백업
백업 일정... 한 번 백업... 복구...

2. 이 서버 선택

시작	이 마법사를 사용하여 파일, 응용 프로그램 및 설정을 복구합니다.
백업 날짜 선택	복구에 사용하기 위해 저장된 백업
복구 유형 선택	<input checked="" type="radio"/> 이 서버(SEOUL)(T) <input type="radio"/> 다른 위치에 저장된 백업(A)
복구할 항목 선택	
복구 옵션 지정	

다른 위치에 백업이미지를 보관하고 있다면 다른 위치에 저장된 백업 선택

3. 사용할 백업 선택

사용 가능한 백업(A)
복구에 사용할 백업 날짜를 선택하십시오. 굵게 표시된 날짜의 백업을 사용할 수 있습니다.

2018년 10월						
일	월	화	수	목	금	토
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

백업 날짜: 2018-10-11
 시간(T): 오후 12:44
 위치: 새 볼륨 (E:)
 상태: 사용 가능한 온라인
 복구 가능한 항목: 로컬 디스크(C:), R...

백업한 날에는 달력에 박스로 표시되어 있다. 시간 탭을 활용해서 복구할 백업 파일 선택

4. 파일 및 폴더 선택

복구할 대상을 선택하십시오.

☒ 파일 및 폴더(F)
이 백업에 포함된 볼륨을 찾아보고 파일 및 폴더를 선택할 수 있습니다.

☐ Hyper-V(H)
가상 컴퓨터를 원래 위치 또는 다른 위치로 복원하거나 가상 컴퓨터의 가...
사할 수 있습니다.

☐ 볼륨(V)
C:에 저장된 모든 데이터와 같이 전체 볼륨을 복원할 수 있습니다.

☐ 응용 프로그램(A)
Windows Server 백업에 등록된 응용 프로그램을 복구할 수 있습니다.

5. C:\ 선택

사용 가능한 항목(A):

- Seoul
- 로컬 디스크(C:)

6. 복구 대상은 원래 위치

복구 대상

☒ 원래 위치(I)
☐ 다른 위치(A)

원래 위치 : 기존 위치에 복구할때

다른 위치 : 이미지에 있던 데이터를 특정 장소에 복구하고 싶을때

7. A파일을 보유하고 있는데 백업 이미지에 a파일이 있을경우

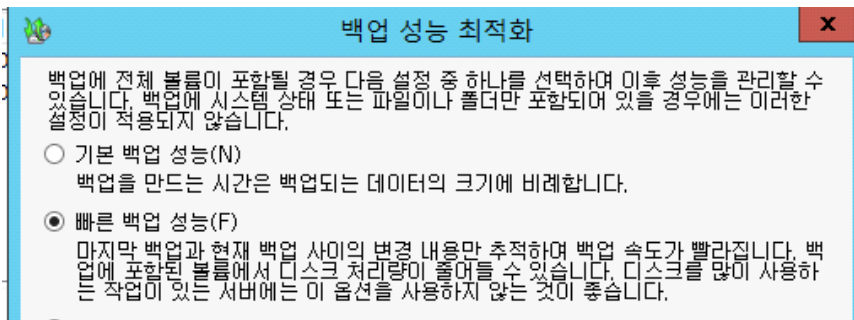
☒ 복사본을 만들어 두 버전 모두 유지(C)
=> 두개 다 유지하겠다. 부팅시 부팅프로그램에 문제가 생길 수 있다.

☐ 기존 버전을 복구된 버전으로 덮어쓰기(O)
=> 백업이미지에 있던 파일로 덮어쓰겠다.

☐ 복구 대상에 이미 있는 항목 복구 안 함(D)
=> 하나씩 비교를 해서 있는 data는 복구x, 없는 data는 백업

증분 백업

1. 로컬백업 우클릭해서 성능 설정 구성으로 이동 -> 빠른 백업 성능 선택

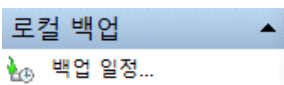


2. 전체 백업과 동일하게 백업 진행

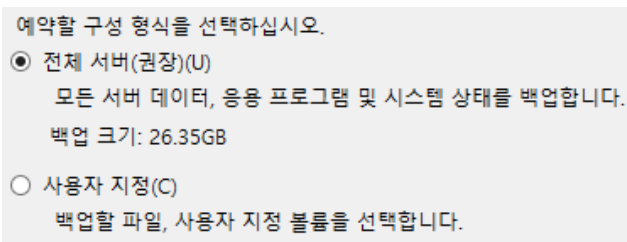
3. C:\에 빈 텍스트 파일 생성후 동일하게 백업진행하면 추가 생성된 파일만 백업하는 것을 알수있다

백업 일정

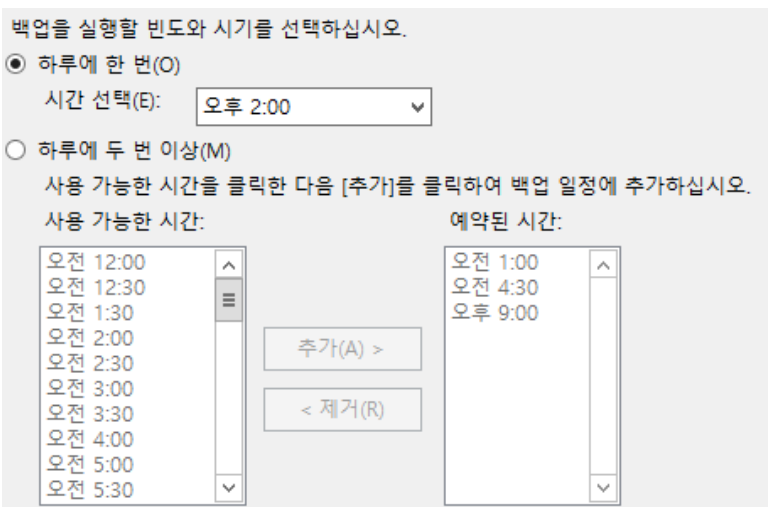
1. 백업 일정 선택



2. 전체 서버 선택



3. 백업 빈도와 시간 선택



4. 위치 선택

백업을 저장할 위치를 지정하십시오.

☐ 백업 전용 하드 디스크에 백업(권장)(B)

백업을 가장 안전하게 저장하려면 이 옵션을 선택합니다. 사용하는 하드 디스크가 포맷되어 백업 저장 전용 디스크가 됩니다.

☒ 볼륨에 백업(V)

전체 디스크를 백업 전용으로 사용할 수 없는 경우 이 옵션을 선택합니다. 백업을 저장하는 데 사용되는 동안 볼륨의 성능은 200퍼센트까지 줄어든 수 있습니다. 동일한 볼륨에 다른 서버 데이터는 저장하지 않는 것이 좋습니다.

☐ 공유 네트워크 폴더에 백업(E)

서버에 로컬로 백업을 저장하지 않으려는 경우 이 옵션을 선택합니다. 새 백업을 만들 경우 이전 백업을 덮어쓰므로 한 번에 하나의 백업만 사용할 수 있습니다.

5. 백업 전용 하드 디스크에 백업 선택

백업을 저장할 위치를 지정하십시오.

☒ 백업 전용 하드 디스크에 백업(권장)(B)

백업을 가장 안전하게 저장하려면 이 옵션을 선택합니다. 사용하는 하드 디스크가 포맷되어 백업 저장 전용 디스크가 됩니다.

☐ 볼륨에 백업(V)

전체 디스크를 백업 전용으로 사용할 수 없는 경우 이 옵션을 선택합니다. 백업을 저장하는 데 사용되는 동안 볼륨의 성능은 200퍼센트까지 줄어든 수 있습니다. 동일한 볼륨에 다른 서버 데이터는 저장하지 않는 것이 좋습니다.

☐ 공유 네트워크 폴더에 백업(E)

서버에 로컬로 백업을 저장하지 않으려는 경우 이 옵션을 선택합니다. 새 백업을 만들 경우 이전 백업을 덮어쓰므로 한 번에 하나의 백업만 사용할 수 있습니다.

6. 백업 전용 하드로 사용할 디스크 선택

백업을 저장할 디스크를 하나 이상 선택하십시오. 디스크를 오프사이트에 저장하는 경우 백업 디스크를 여러 개 사용할 수 있습니다.

사용 가능한 디스크(A):

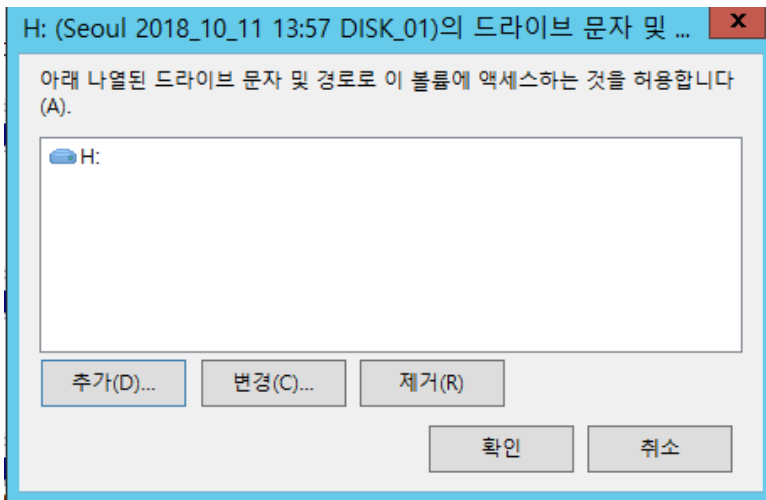
디스크	이름	크기	사용 중인...	디스크 볼륨
<input checked="" type="checkbox"/> 2	VMware, ...	40.00GB	8.68GB	G:₩

사용 가능한 모든 디스크 표시(S)...

7. 디스크 관리 들어가면 백업전용 하드 가 파티션이 이루어진것을 알 수 있다.

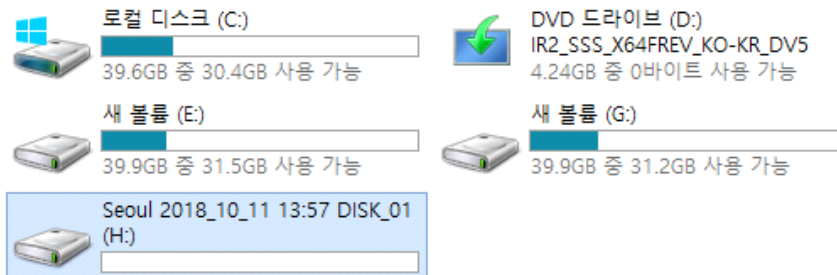
 디스크 3 기본 39.88 GB 온라인	Seoul 2018_10_11 13:57 DISK_01 (H:) 39.86 GB NTFS 정상 (주 파티션)
--	---

8. 해당 디스크를 우클릭 하면 드라이브 문자 및 경로 변경 선택



1. 문자열 선택해서 내컴퓨터에서 확인 할수 있다.

장치 및 드라이브 (5)



디스크 쿼터

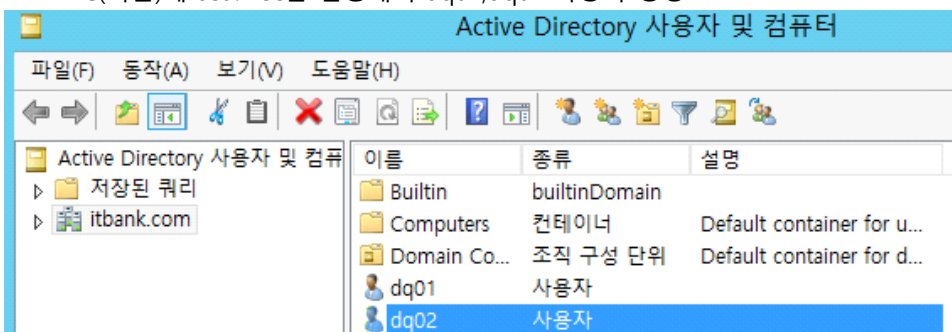
사용자 별로 디스크를 할당 해주는것.

관리자 계정은 할당 용량 제한을 받지 않는다.

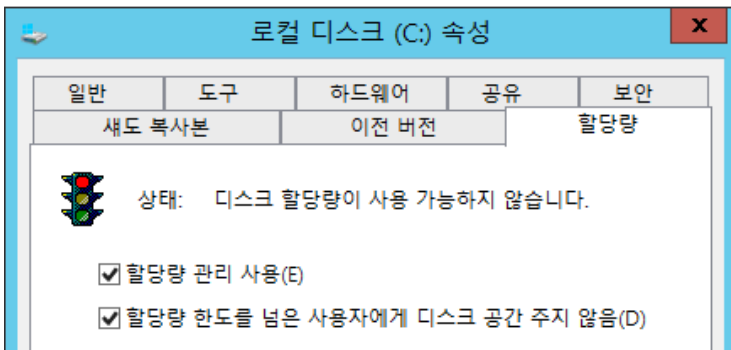
일반 사용자 및 시스템계정(OS가 사용하는 계정)도 제한을 받는다.

각 드라이브별로 제한을 받는다.

1. 서울과 부산을 스텝샷을 통해 AD로 변경
2. DC(서울)에 dsa.msc를 실행해서 dq01,dq02 사용자 생성



3. C:\w 속성에 할당량



4. 제한 용량과 경고수준의 용량 설정

이 볼륨의 새 사용자에게 대한 기본 할당량 한도 선택:

- ☐ 디스크 사용 제한 안 함(O)
- ☒ 디스크 공간을 다음
으로 제한(L) MB
- 경고 수준을 다음으
로 설정 MB

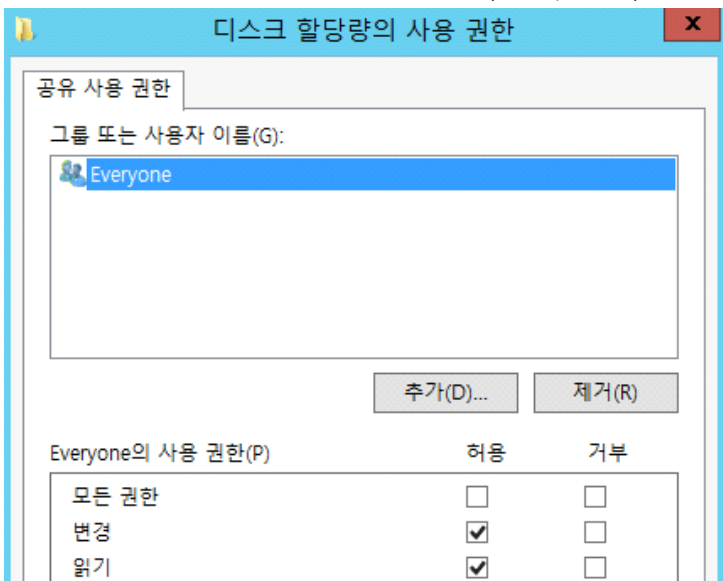
5. 기록 설정

이 볼륨에 대한 할당량 기록 옵션 선택:

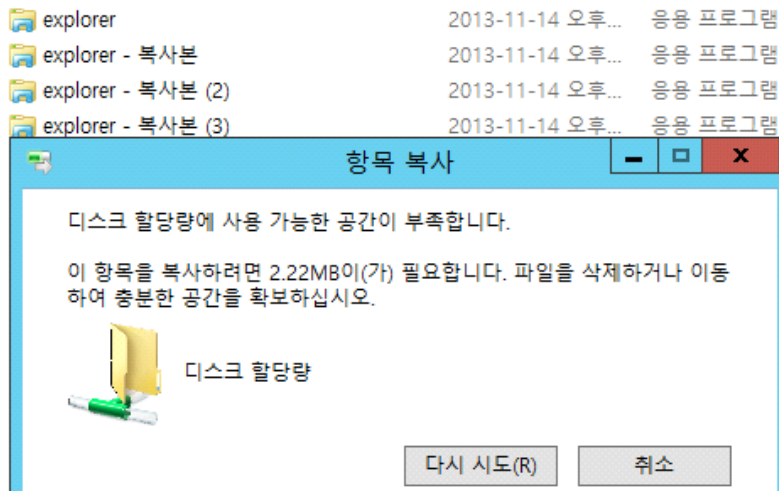
- ☒ 사용자가 할당량 한도를 넘었을 때 이벤트 기록(G)
- ☒ 사용자가 경고 수준을 넘었을 때 이벤트 기록(V)

기록을 해야만 확인을 할 수 있다.

1. C:\W 디스크 할당량 폴더 생성 및 공유 (READ,WRITE)



7. C:\W Windows\Explorer가 디스크 할당량 폴더에 몇개가 저장되는지 확인



용량 제한으로 4개만 저장된다.

※ 할당량 항목 -> 시스템 계정 -> 더블클릭 -> 제한안함으로 기존에 제한한것을 풀수 있다.

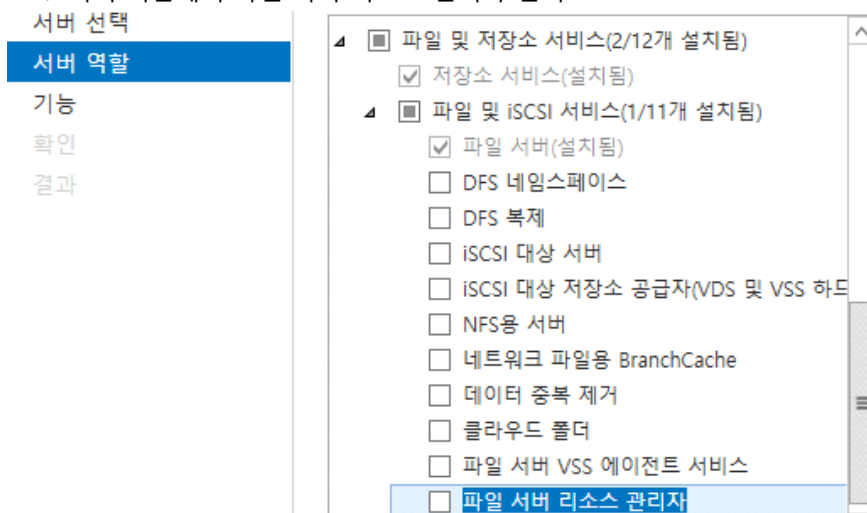
8. 할당량 -> 새할당량 항목 -> dq02 추가 -> 디스크 제한(20mb)을 다르게 할 수 있다.

explorer - 복사본 (4)	2013-11-14 오후...	응용 프로그램	2,275KB
explorer - 복사본 (5)	2013-11-14 오후...	응용 프로그램	2,275KB
explorer - 복사본 (6)	2013-11-14 오후...	응용 프로그램	2,275KB
explorer - 복사본 (7)	2013-11-14 오후...	응용 프로그램	2,275KB
explorer - 복사본 (8)	2013-11-14 오후...	응용 프로그램	2,275KB
explorer - 복사본 (9)	2013-11-14 오후...	응용 프로그램	2,275KB
explorer - 복사본 (10)	2013-11-14 오후...	응용 프로그램	2,275KB
explorer - 복사본 (11)	2013-11-14 오후...	응용 프로그램	2,275KB

용량 제한으로 8개만 저장된다.

※ NTFS기능 중 하나이다. NTFS기능을 사용해야지 활용할 수 있다.

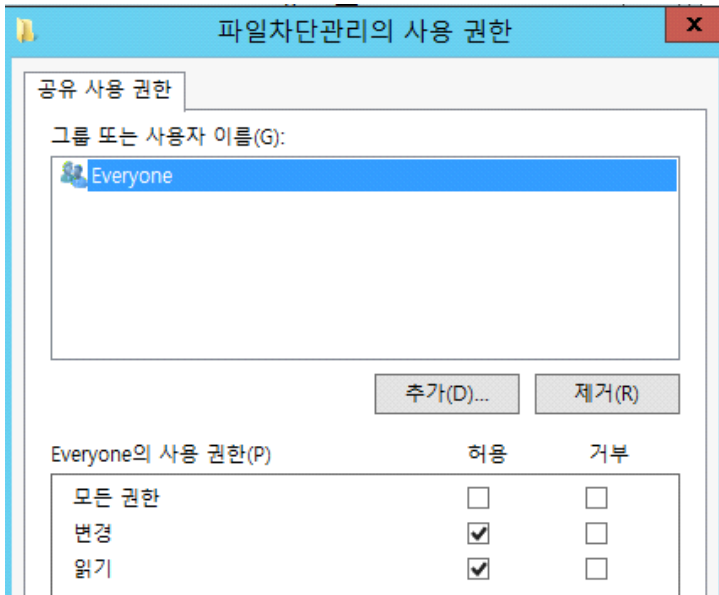
1. 서버관리자에서 역할 및 기능 추가
2. 서버 역할에서 파일 서버 리소스 관리자 선택



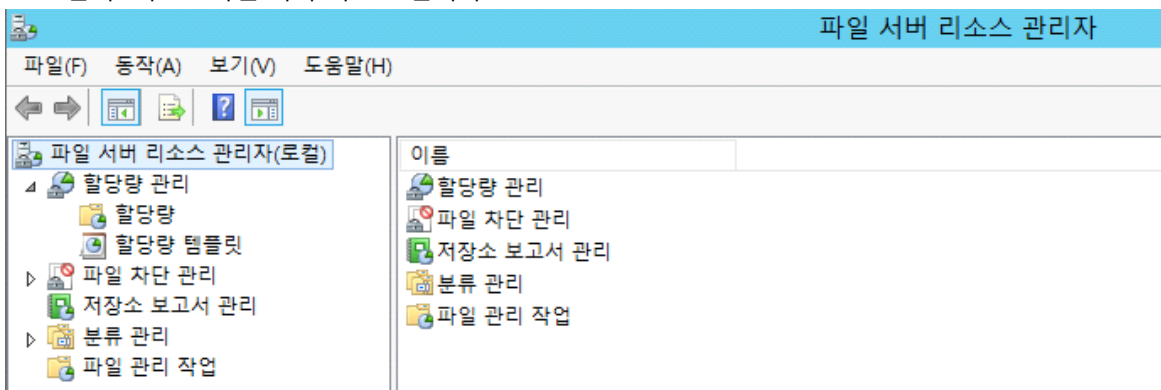
=> 디스크 쿼터는 디스크에 제한을 걸지만 파일 서버 리소스는 파일에 제한을 건다.
관리자 계정도 제한을 건다. 특정 확장자도 제한이 가능

3. C:\W에 할당량관리,파일차단관리 폴더 생성 및 공유 (READ,WRITE)

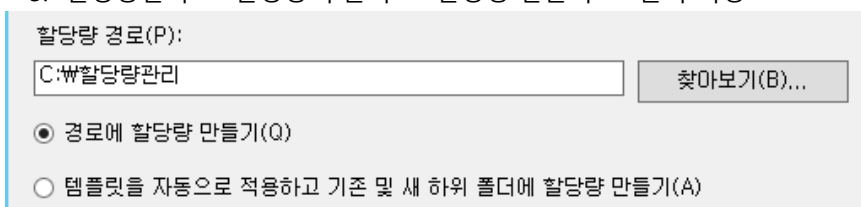
할당량관리	2018-10-11 오후...	파일 폴더
파일차단관리	2018-10-11 오후...	파일 폴더



4. 관리도구 -> 파일 서버 리소스 관리자



5. 할당량관리 -> 할당량 우클릭 -> 할당량 만들기 -> 폴더 지정



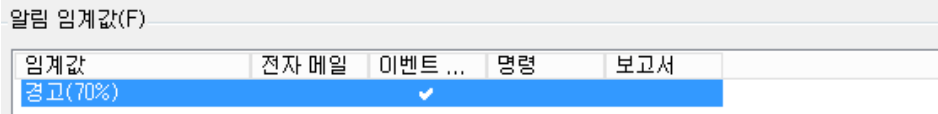
6. 할당량 속성 방법 선택



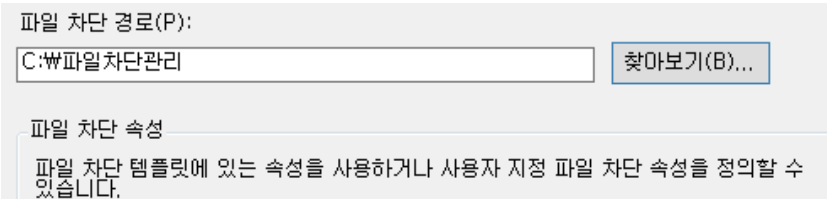
하드할당량 : 차단

소프트 할당량 : 모니터링 목적, 확인하기 위함

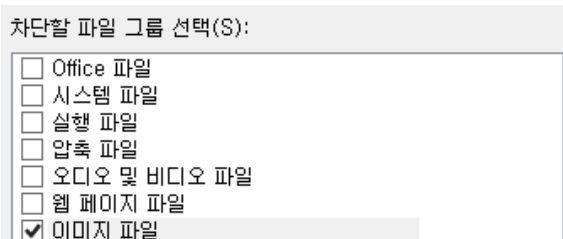
7. 알림 임계값 설정, 이벤트로그 설정



8. 파일차단 관리 -> 파일차단 우클릭 -> 파일차단 만들기 -> 파일 경로 설정



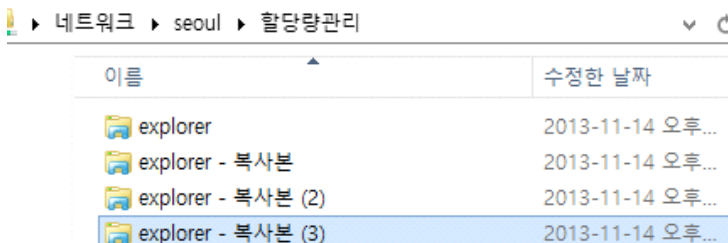
9. 파일 차단 속성 선택, 이벤트로그 선택



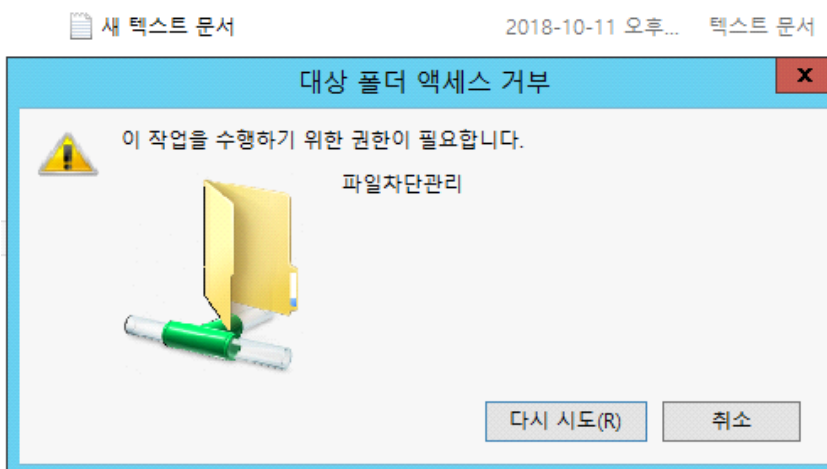
파일 그룹 : 확장자를 모아놓은 그룹,

10. Member(부산)에서 관리자계정(administrator)로 접속해서 설정 확인

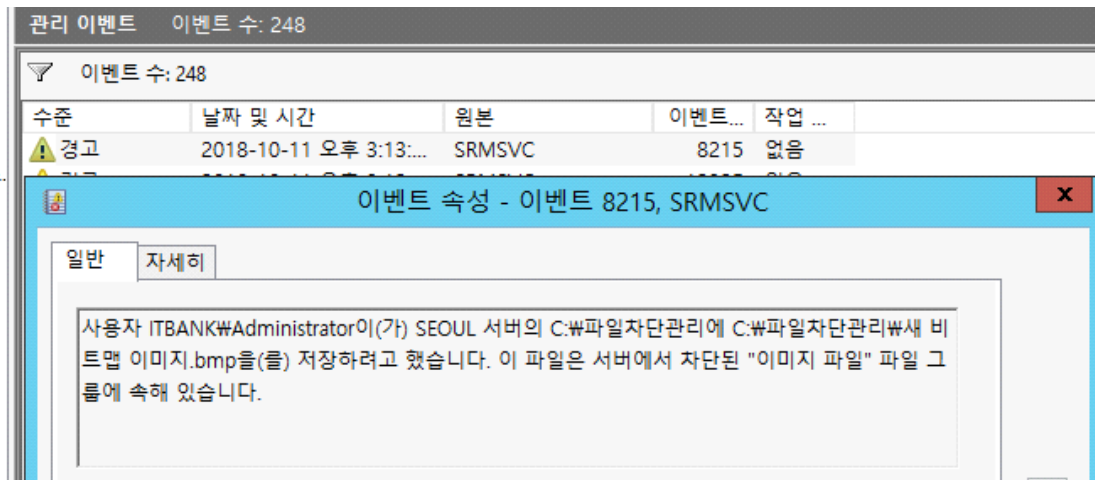
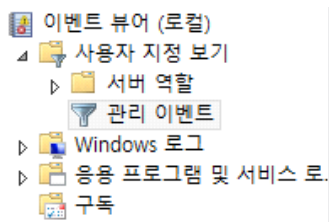
11. 할당량 관리폴더에 4개이상 생성 불가



12. 파일차단 관리 폴더에 텍스트문서는 생성되나 이미지파일은 생성 불가



13. DC(서울)에서 관리도구 -> 이벤트 뷰어 -> 관리 이벤트



이곳에서 로그메시지를 확인할 수 있다.

IIS

2018년 10월 12일 금요일 오후 12:37

IIS (Internet Information Service)

- Web Server
 - 클라이언트/서버 모델
 - 클라이언트가 HTTP를 이용하여 웹서버에 들어있는 웹페이지를 요청
 - 서버는 요청 받은 웹페이지를 클라이언트에게 전달
 - IIS : Windows 전용, 다른 OS에는 사용 불가 -> 비용 발생, 호환성 제로
 - Apache : Windows, Linux, Unix, Mac -> 무료, 호환성 좋음

EX)

Apache + PHP + MySQL(DB) => 전부 무료 (개인용 플랫폼)

Apache + Tomcat + jsp + oracle(DB) => 기업용

IIS + ASP + ms-SQL => 기업용

※ Apache = static(정해진 작업만 할 수 있다)

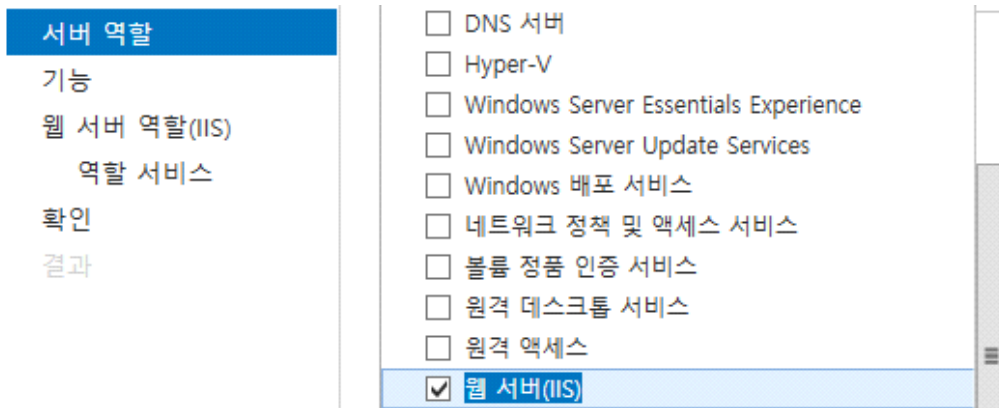
※ DB와 웹은 항상 같이 붙어있다.

※ 트래픽 분산을 위해 동적처리와 정적처리를 나눠서 진행한다.

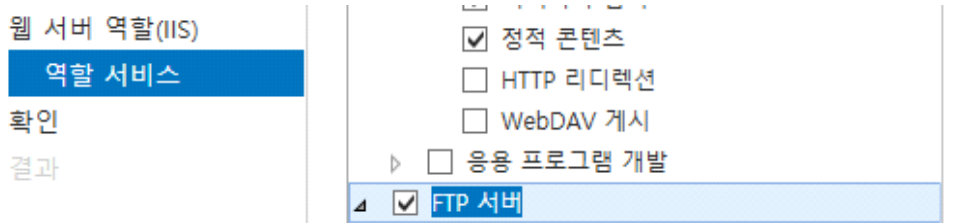
- FTP Server
- HTTP(HyperText Transfer Protocol)
 - 인터넷 상에서는 데이터를 송수신하는 프로토콜, 통신규약
 - hypertext는 link(페이지간 이동) 제공
 - client/sever model protocol 기반
 - TCP 80
 - Application Level Protocol 기반
 - 어떤 종류의 데이터든지 전송할 수 있도록 구현
(image,video,audio,text...)
- HyperText Markup Language(HTML)
 - HTTP 프로토콜을 이용하여 전송된다
 - 웹서버 : 클라이언트의 요청 시 보유한 HTML 파일을 웹클라이언트(IE,크롬,파이어폭스)에 전송
 - 웹서버의 문서전송 형태 : 텍스트 형태의 코드를 전송
- Browser
 - HTML 코드를 해석하여 출력

웹서버

1. 서버 관리자 -> 역할 및 기능추가 > IIS 선택

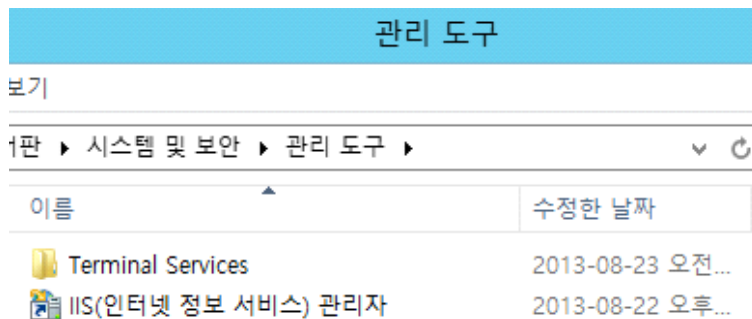


2. 역할 서비스에서 FTP 서버 선택

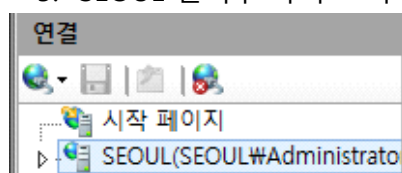


3. 설치 완료

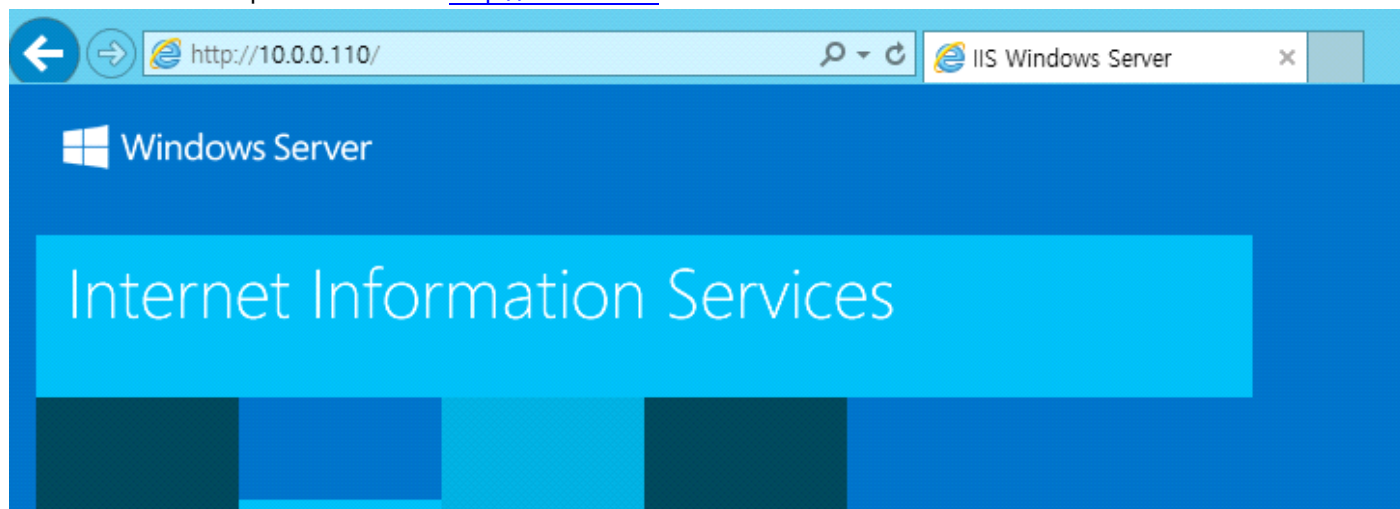
4. 관리도구에서 IIS관리자 실행

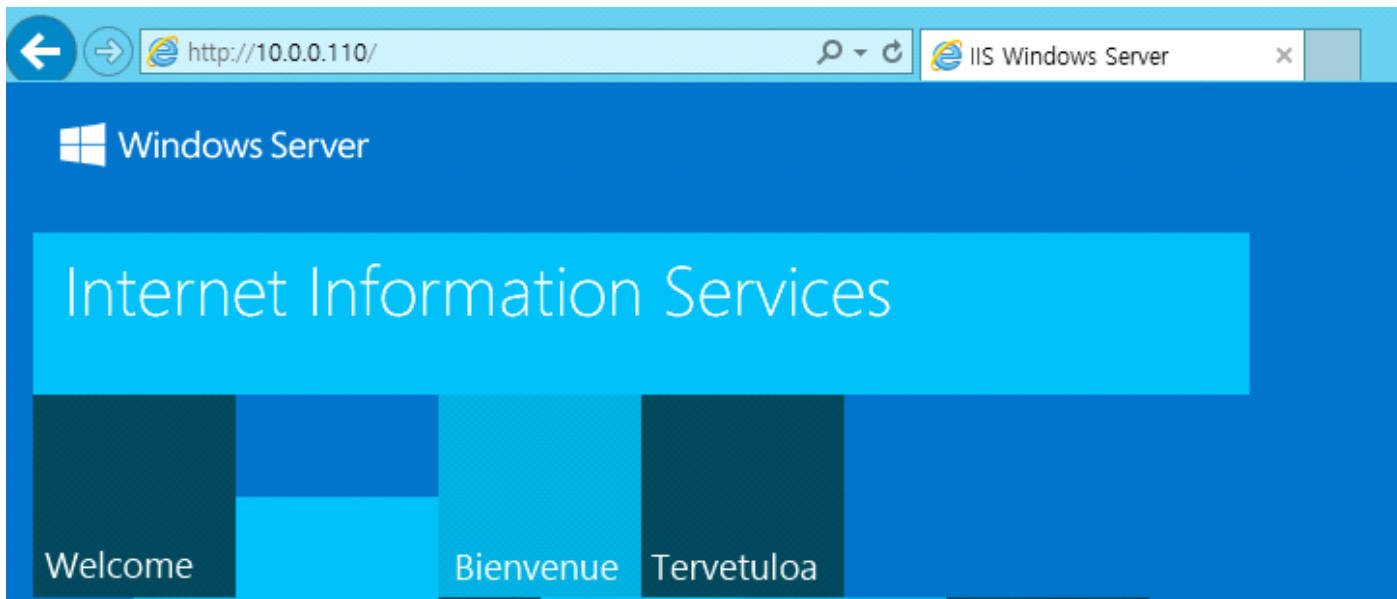


5. SEOUL 선택후 다시 표시하지않음 클릭후 아니오



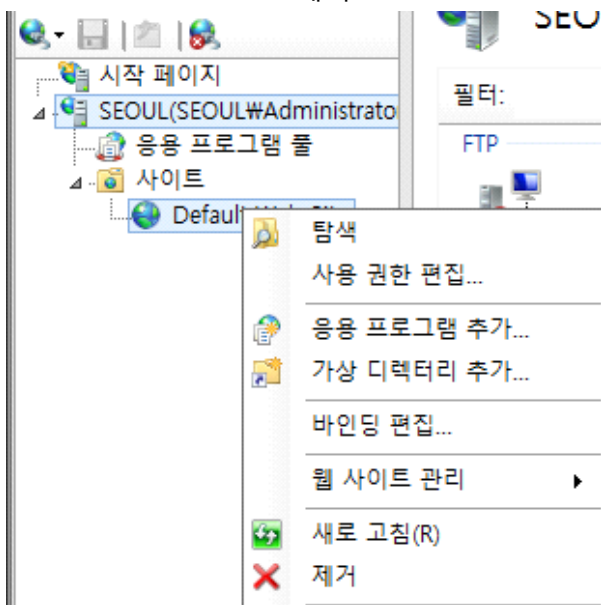
6. Busan에서 exploar 실행해서 <http://10.0.0.110> 접속하면 접속 된다.





7. IIS설치하면 C:\inetpub\wwwroot\iis-85.png를 실행하면 busan에서 본 페이지 화면이 실행된다.
컨텐츠 디렉토리가 필요하고 그 속에 페이지(wwwroot)가 들어 있다.

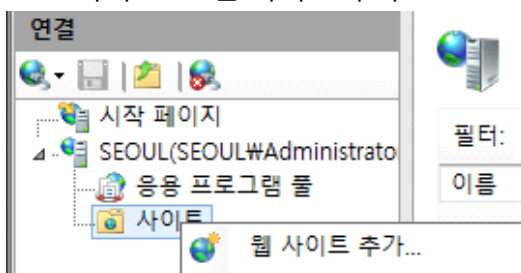
8. Default web site 제거



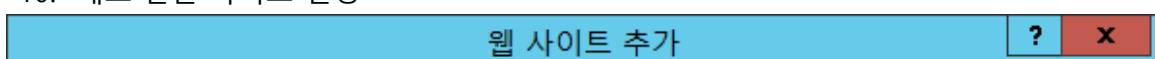
why???

=> web site를 새로 만들어보기 위함

9. 사이트 -> 웹 사이트 추가



10. 새로 만들 사이트 설정



- C:\W80 폴더 생성
- 사이트 이름 : MyWeb
- 실제 경로 : C:\W80
- IP주소 : 접속 할 수 있는 ip 설정
- 포트 : 포트를 지정할 수 있다.
- 호스트 이름 : Web server 이름

11. C:\W80에 index.text파일 생성후 확장자를 html로 변경하고 busan에서 다시 접속
12. index.text를 aaa.text로 변경하면 busan에서 403오류가 뜬다
=> 디렉토리를 확인할 수 없게 설정했기 때문
13. Soul에서 myweb의 기본 문서들어가면 index.html이 상속 설정이 되어 있어 메인페이지로 나온다.
=> 메인페이지를 자동으로 인식한다
14. 기본페이지 추가하는 방법은 작업탭에 추가를 눌러서 이름을 넣어주면 된다.

15. 디렉토리 검색 기능은 비활성화하는 것이 좋다.
16. 오류페이지 코드를 활용해서 점검시간 등 전파할 수 있다.

17. C:\W80WTEST\index.text 생성
18. Busan가서 <http://10.0.0.110/test> 접속



19. C:\WS1\index.html 생성
20. Myweb우클릭 -> 가상디렉터리 추가 -> 별칭 -> 실제 경로 지정 -> 부산에서 확인
21. 웹 서버 생성시 포트번호를 8080으로 변경
22. C:\W8080\index.html 생성
23. Busan에서 접속할 때는 <http://10.0.0.110:8080/으로> 접속해야 한다.
=> 10.0.0.110 뒤에 " : "을 붙이면서 접속할 포트번호를 입력한다.

실습

Web site 추가
Web server 이름 : MyWeb
컨텐츠 디렉터리 : C:\WMyweb
바인딩 : http / 지정하지 않은 모든 ip / 547 포트
기본문서 : abcd.html
하위 디렉터리 : c:\WMyweb\WS2
접속 시 페이지에 S2가 나오게
가상 디렉터리 : C:\WS1 > 별칭은 MYS1
접속시 페이지에 S1이 나오게