프로그램 이름 확장자에 다른 분류

.cpl : control panel >> 제어판 콘솔

.msc : microsoft console >> MMC 틀을 이용하여 만든 콘솔

MMC

- Microsoft Management Console

- 관리자 도구들을 개발하기 위해 제공된 틀

- 여러 기능들을 스냅인으로 제공 받아 필요한 콘솔들을 원하는 대로 구성하여 사용할 수 있

도록 제공하는 도구

> .msc 확장자를 갖고 있는 모든 콘솔들 중 필요한 콘솔들은 mmc를 이용하여 불러오는

것이 가능

OU

- Organizational Unit, 조직 단위

- 도메인 내부의 디렉토리 객체

- 사용자/컴퓨터 계정, 그룹, 공유 프린터, 다른 조직 단위 등을 포함할 수 있음

- 그룹 정책 설정을 부여하거나 관리 권한을 위임할 수 있는 가장 작은 범위(혹은 구성 단위)

> 권한의 위임을 통해 도메인 안에서 관리 범위를 설정

- 생성 시 이름은 관리자가 마음대로 지정

> 가장 많이 사용되는 방식 : 회사의 조직도를 참조하여 부서명으로 구성

- OU 간의 객체 이동이 가능하다

> 단, 복사는 불가능

사용자 계정

- 인증을 받거나 로컬/네트워크의 자원에 접근하는 것을 가능하게 해주는 객체

- 사용자 계정은 사람들에게 하나씩 만들어 준다.

사용자 식별

인증/접근 > 권한

> 관리자 입장에서 위의 작업들을 편하게 하기 위해 사용

- 사용자 계정 저장 위치

로컬 계정 : SAM ( C:\windows\system32\config\SAM )

> 단일 컴퓨터에 로그온하여 그 컴퓨터 내부의 자언을 사용

도메인 계정 : ntds.dit ( C:\windows\ntds\ntds.dit )

> 컴퓨터가 가입된 도메인에 로그온하여 도메인 전체 컴퓨터의 자원을 사용

- 사용자 계정을 생성하면 Security ID (SID)도 같이 생성된다.

- 사용자 계정 관리 도구

로컬 계정 : CLI - net user

GUI - 로컬 사용자 및 그룹(lusrmgr.msc)

컴퓨터 관리 - 로컬 사용자 및 그룹 (compmgmt.msc)

도메인 계정 : CLI - dsadd user

GUI - AD 사용자 및 컴퓨터 (dsa.msc)

- 계정 표현 방식

user logon name

> 계정명

user logon name(windows 2000 이전 버전) ; 2000 이전부터 사용하던 방식

> NetBIOS\계정명

UPN(User Principal Name)

> 계정명@도메인주소

LDAP-DN

> CN = 계정명, OU = OU 이름, DC = 도메인, DC = 주소

LDAP-RDN

> CN = 계정명

\* LDAP 방식에서의 표현

CN : 사용자/그룹/컴퓨터 계정, 컨테이너

OU : 조직 단위(OU) >> 내부 OU부터 바깥쪽으로 나가는 순서대로 작성

DC : 도메인 주소를 . 단위로 분할하여 입력

사용자 암호 정책

- 사용자 계정의 암호는 보안에 있어서 가장 기초가 되는 항목

> 그렇기 때문에 여러가지 정책을 시용하여 암호를 관리

- windows는 다음 다섯 가지의 암호 정책이 있음

1. 암호의 복잡도

암호의 복잡도는 다음 네 가지의 복잡도 범주중 세가지 이상을 만족해야 함

> 복잡도 종류

1) 영어 대문자 (A ~ Z)

2) 영어 소문자 (a ~ z)

3) 숫자 (0 ~ 9)

4) 특수문자(알파벳 이외의 문자)

2. 최근 암호 기억

이전에 사용했던 암호를 정해진 개수 만큼 기억

> 기억하고 있는 암호로 변경을 할 수 없다.

3. 최대 암호 사용 기간

암호의 최대 사용 기간

> windows 에서는 기본 42일 사용(broot force 공격으로 암호를 찾아내는

기간이 평균 42일 소요)

4. 최소 암호 사용기간

암호의 최소 사용 기간

> 암호 변경 후 해당 암호를 최소 몇 일 동안 사용하도록 만들어서

암호 변경 후에 다시 원래 암호로 변경하는 것을 방지

5. 최소 암호 길이

암호를 몇 글자 이상 입력하도록 지정