Windows Server

■ EFS(Encrypt File System) 파일 암호화
암호화 = 파일의 내용을 보더라도 내용을 알 수 없도록 하는 것
암호 = Password
예) D가 암호라고 할 때 A에서 +3이라는 규칙을 아는 사람이 D라는 암호를 풀수 있음
이같이 암호키 +3 이라는 규칙을 아는 사람 및 장비만 해석 가능

<암호화 키의 방식>

단일키 = 개인키 = 비밀키 : 암호화/복호화(암/복호화)의 속도가 빠르다. : 키 관리가 어려움.
이중키 = 공개키 : 공개키로 암호화하여 개인키로 복호화하는 방식 = RSA(소수, 인수분해 형식으로 만듬)

상황1) 특정서버(tokyo)에 김정국 사원이 담당하는 2022년 하반기 신규 프로젝트 파일이 저장되어 있다. 8/16일에 발표 전까지는 자신 외에 아무도 볼 수 없기를 바란다.
비밀 유지를 위해 김정국은 EFS를 사용하였다.

tokyo에서 C:₩기밀자료를 생성 → 프로젝트.txt 만들기
폴더 속성에서 고급특성 → 압축 또는 암호화 특성에서 암호화 데이터 보호를 위해 내용을 암호화 체크 → 확인하기 → 적용 여부 물어보면 확인하고 확인하기
초록색으로 파일과 폴더가 바뀌어 있는 것 확인할 것
다른 계정으로 파일 확인 해보기 → administrator와 일반 유저 모두 액세스 거부가 발생함

상황2) 김정국이 퇴사하게 되었다. 관리자가 이 계정을 삭제 했다.
삭제된 계정은 동일하게 생성은 할 수 있으나, SID는 재 사용이 안 됨
이같은 경우에는 별도로 개인키를 백업하여야 함
파일 복구 에이전트
외장장치에 암호화를 한 사용자에게 자신의 인증서(키)를 백업하도록 지시 한다.
C:₩외장하드 폴더 생성 → 시작에서 액자모양 클릭해서 사용자 계정 → 파일 암호화 인증서관리 메뉴 클릭 → 다음 → 인증서 보기 클릭해서 인증서 확인 자세히에서 RSA키 확인 → 다음 → 백업위치(C:₩외장하드)지정 key.pfx로하고 암호 지정 → C:₩기밀자료 체크 → 업데이트 확인 문구 C:₩외장하드 폴더에 key.pfx키있는 것 확인

관리자 계정으로 로그인 후 시작 → 실행 (시작+실행 = Win+R) → mmc(management console)를 열기
파일 → 스냅인 추가/제거 → 인증서 → 추가 → 내사용자 계정 → 마침&확인
개인용 마우스 오른쪽 가져오기 → 인증서 저장된 위치에서 인증서 가져오기 → 확장자

<실습>
boston서버에 user3의 홈폴더(home)를 생성
user3의 홈폴더 user3의 파일 암호화를 적용
C:₩USB 폴더를 만들어서 여기에 자신의 개인키를 백업하세요.

■ Privilege와 Permission의 차이점
권한(특권) - 관리자만이 해야하는 작업들
시스템에 치명적인 문제를 발생시킬 수 있는 항목들
관리도구 → 로컬보안정책 → 로컬정책 → 사용자 권한 할당

사용권한
일반 사용자에게 관리자가 어떠한 공유자원에 대한 사용을 승인해 주는 것
파일, 폴더, 프린터 등의 속성 → 보안 탭에서 설정

<Q>
파일 사용권한에 대한 문제 Access Control
★ 공유 설정, 사용권한 할당 등의 작업은 관리자만이 할 수 있다.
london [자료] 공유폴더 생성 파일 1,2,3을 만들자.(공유 사용권한 : 모든 권한)
해당 폴더 속성 – 보안에서 user1(읽기), user2(쓰기), user3(수정)으로 할당하자.

boston or tokyo에서 각 사용자로 로그인하여 위의 파일들에 대해 아래의 작업을 실행해보자.
1. 파일을 열고, 복사를 할 수 있다. user1 user2 user3
2. 파일을 열어 내용을 수정한 후 저장 user2 user3
3. 파일 삭제 user3
4. 새 파일 만들기 user1 user2 user3
5. 소유권 가져오기
₩₩london₩₩자료에서 user1 파일을 user1에서 생성
₩₩london₩자료 user1파일 속성에서 보안 → 고급 → 소유자탭 → 소유권변경
남의 것이라 소유권 액세스 거부됨
administrator는 관리자여서 소유권 변경이 가능함

● 공유 권한
공유 폴더에 적용, 운격지에서 공유경로를 사용하여 ₩₩london 연결할 때 적용을 받음. 1차필터

● 보안
공유 연결이든 로컬 작업이든 모두 적용이 됨.
단 공유 연결은 먼저 공유 권한을 적용받는다.
공유는 모든권한으로 주고 보안에서 상세한 설정을 한다.

<실습1>
AD 사용자 및 컴퓨터 → 영업부 오른쪽 클릭 → 새로 만들기→ 그룹(A,B생성)
user 오른쪽 마우스 클릭 그룹추가 → 그룹쓰고 이름확인 후 선택
그룹 → 오른쪽 클릭 → 구성원 탭 클릭으로 그룹 속해있는 것 확인

user1은 그룹A와 B의 구성원이다
폴더 A에 대해 user1은 읽기 그룹B에게는 쓰기 권한이 할당된다.
user1은 해당 폴더에 대해 어떤 사용 권한을 갖는가?

C:₩폴더A생성 하고 공유
보안에서 추가 user1;그룹B
읽기 + 쓰기 = 사용권한은 누적이 됨.

폴더 설정 → 파일에게 상속된다.
파일에서 폴더와 다르게 설정한다면 파일이 폴더보다 우선순위가 높아짐.

<실습2>
파일2에 대해 그룹A에게 쓰기 거부를 설정했다면 user1은 파일2에 대해 어떤 권한을 갖는가?
★ 거부
일반적으로 사용권한 설정은 폴더 수준에서 한다.

폴더 안에 있는 파일은 그 사용권한을 상속받음(즉, 폴더로부터 사용권한을 상속)으로 일일이 설정할 필요가 없다.
예외적으로 특정 파일에 대해 상이하게 설정해야 할 필요가 있을 때만 거부를 사용한다.

★ 상속 차단
폴더A₩폴더B₩폴더C₩파일 생성
상속받은 계정은 보안 제거가 불가함
- 추가
- 제거

★ Permission 적용방법
- 사용권한은 상위의 설정이 하위로 상속된다.
  상속된 사용권한은 차단을 하기 전까지는 변경할 수 없다.
- 사용권한은 누적된다.
- 모든 파일에 대해 공통적으로 적용할 것은 폴더 단계에서 설정을 하고 각각의 파일에 대해 추가적인 권한은 별개로 설정을 한다.

<TEST>
영업부 OU(조직)에서 HR, Sales 그룹 생성
HR ← user1 user2 user3 추가
Sales ← user1 user4 user5 추가

FolderA1 HR : 쓰기만 Sales : 읽기만 – 두파일에 대해 어떤 작업을 할 수 있는가?
  File1.txt
  FolderA2
    File2.txt

FolderB1 HR : 읽기 Sales : 읽기만 – 두파일에 대해 어떤 작업을 할 수 있는가?
  File1.txt
  FolderB2 Sales : 쓰기
    File2.txt

FolderC1 HR : 수정
  File1.txt
  FolderC2
    File2.txt Sales만이 읽기가 되어야 합니다.