Active Directory and Security

daehanv

daehanv@gmail.com

목차

Active Directory 개요

Directory

- **개체 정보 저장**
  - 전화번호부 : 성, 이름, 전화번호 등
  - 파일시스템 : 파일 이름, 크기, 생성시간, 변경된 시간 등

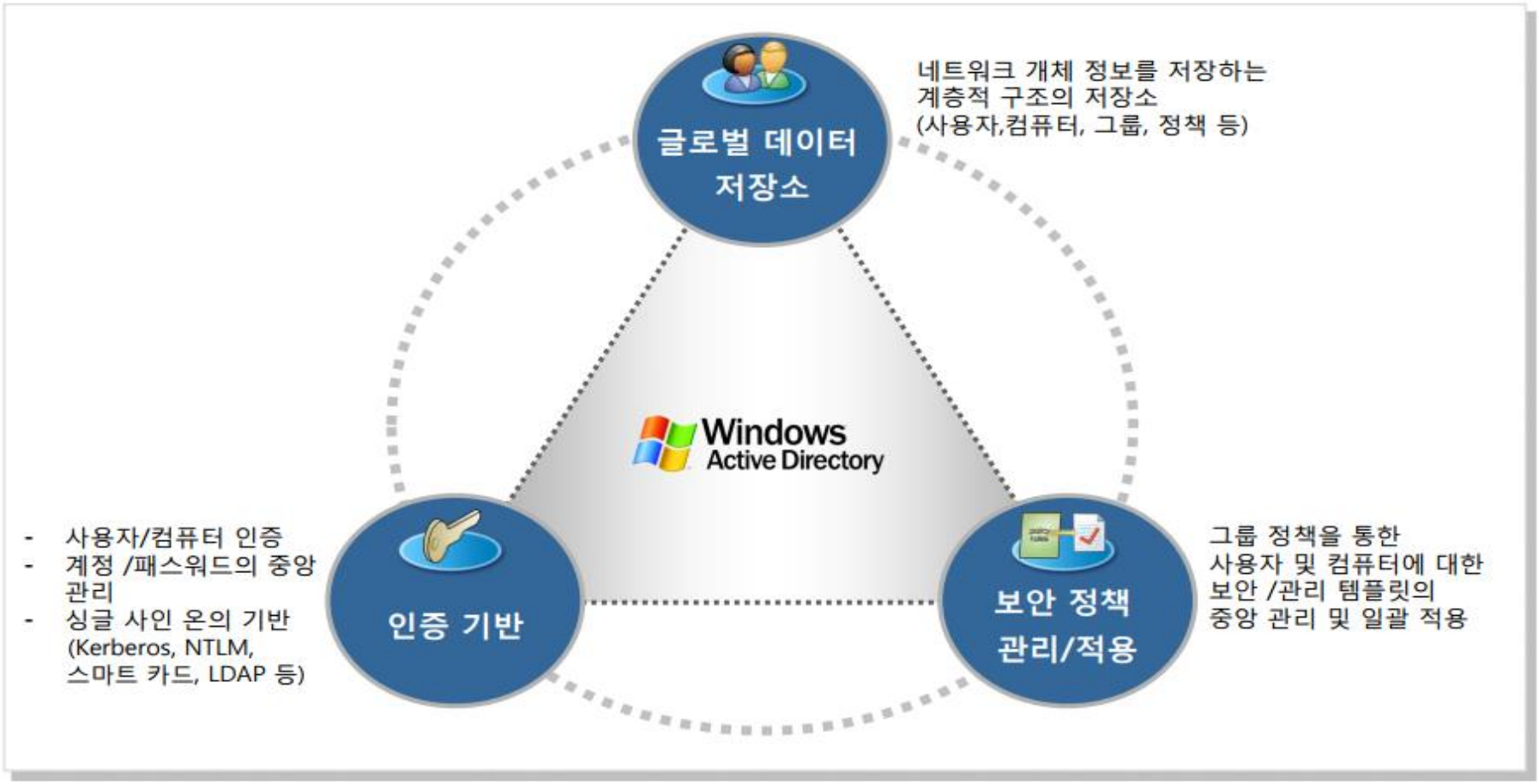
Directory Service

- **분산된 네트워크 자원 정보를 중앙의 저장소에 통합시켜 저장**
  - 네트워크 관련 자원 : 사용자 계정, 그룹 계정, 프린터 등

Active Directory

- **Windows Server OS에서 제공하는 디렉토리 서비스**
- **네트워크 상의 여러가지 자원을 관리자가 모두 통합 관리**
- **디렉토리 서비스의 확장된 개념으로 DNS, 통합, 확장성, 중앙집중관리, 관리위임 등 제공**

Active Directory는 전사 IT 자원의 통합 계정 저장소 개념의 디렉토리 서비스로서 인증, 접근 관리, 및 보안관리 등 중앙 운영을 위한 단일 중심점을 제공합니다.



Source : https://news.microsoft.com/ko-kr/features/active_directory, Active Directory 가치 및 활용(Microsoft)

Active Directory 용어 정리

Active Directory = AD

도메인(Domain)
→ AD의 기본 단위, ex)FIOS.com, FIOS.local

조직 구성 단위(Organization Unit, OU)
→ 도메인 내 세부 단위, ex) FOIS 내 총무팀, 구매팀, 보안팀

도메인 컨트롤러(Domain Controller, DC)
→ 사용자 등록, 암호 변경, 그룹변경, 정책설정 등을 처리하는 서버
→ 모든 AD는 1개 이상의 DC를 보유

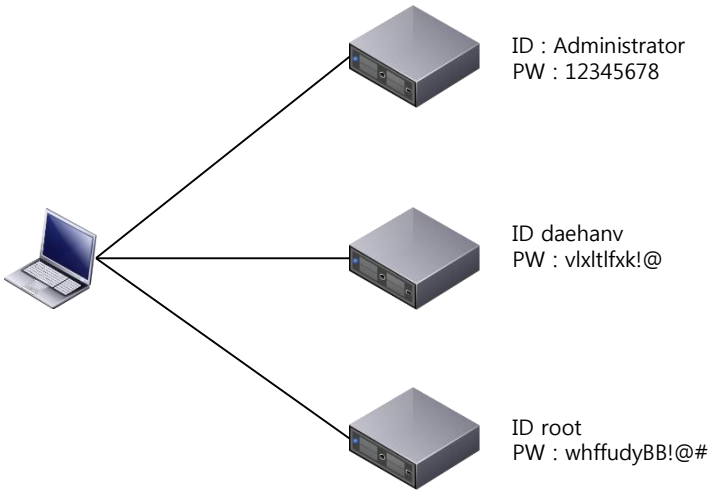
주 도메인 컨트롤러(Primary Domain Controller, PDC)

도메인 관리자(Domain Admin)

Active Directory 특장점

Active Directory 통합 계정으로 효과적인 사용자 관리와 감사가 가능합니다.

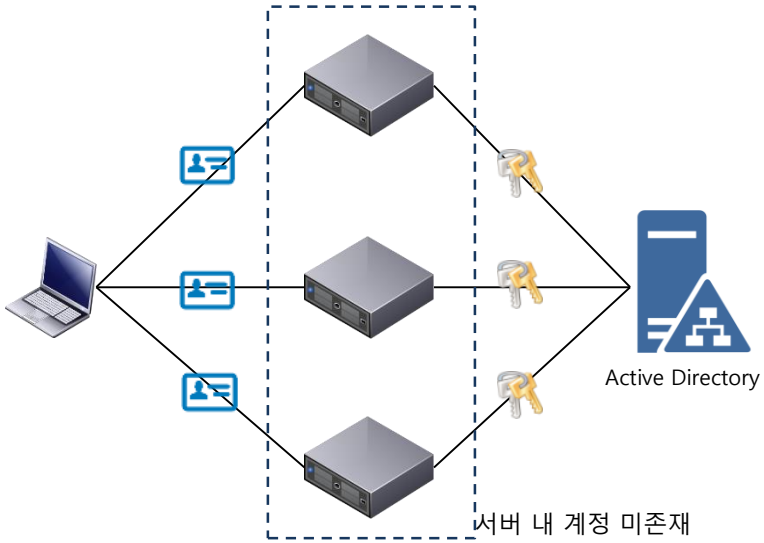
단일 구성



접근 시스템별 개별 계정/암호 사용

- 다수의 관리자 계정 및 암호 존재
- 개별 시스템별 별도의 계정 관리 필요

AD 기반의 계정 통합 관리

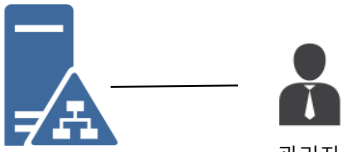


Active Directory 기반의 통합 계정 및 접근관리

- AD기반의 통합 계정(1인 1계정) 사용
- 인증 단일화로 감사기능 강화
- AD에서만 계정관리 필요

Active Directory 특장점(Cont'd)

Active Directory 그룹정책으로 조직 내 사용자 및 컴퓨터의 보안 정책을 수립하고 중앙에서 일괄 적용하여 보안 강화 및 관리 효율을 높일 수 있습니다.



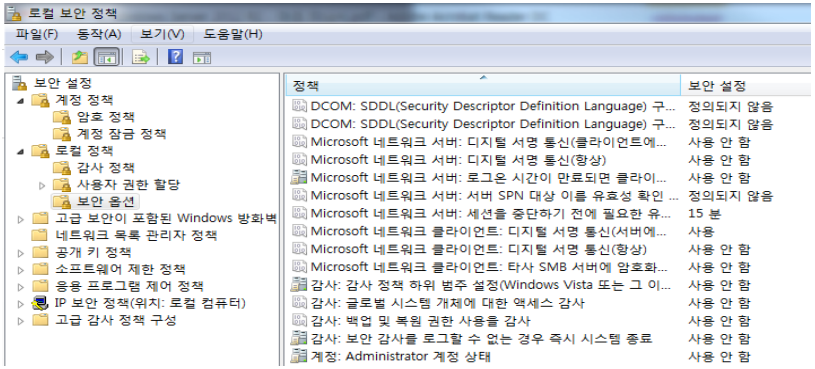
보안 정책 | 구성 및 설정 | 스크립트 /SW

정책 자동 배포
백그라운드 강제 적용

보안 정책
- 계정 및 암호
- 감사정책
- 사용자 권한 통제
- 윈도우 방화벽/화면보호기 설정
- USB, 서비스, 실행파일 통제

구성 및 설정
- 제어판 설정
- 네트워크 설정
- 시스템 설정
- IE 설정
- Windows Update 설정

스크립트/SW
- 소프트웨어 배포/실행
- 스크립트 설정 배포/실행



Active Directory 특장점(Cont'd)

- **다양한 표준 인증 프로토콜 제공(LDAP, Kerberos, RADIUS)**
  - MS Product에 대한 SSO 기능 제공
  - 표준 프로토콜을 지원하는 이기종 시스템들에 대한 동일 계정/암호 사용 가능
  - Linux도 인증 가능

- **보안팀 입장의 장점**
  - 모든 계정 관리(입사, 퇴사, 부서변경, 권한변경 등)는 AD에서만 처리하면 됨
  - 모든 AD에 Join 된 PC된 PC는 PDC와 시간 동기화 진행(추가 설정 시 사용자 시간 변경 불가)
  - 계정, 이벤트 로그, 방화벽 정책, Windows Update 설정/제어 가능
  - Logon Script 등을 이용한 소프트웨어 배포를 통해 긴급 대응 및 별도 설정 가능
  - 로그인 기록 등 다양한 이벤트로그를 통한 감사 가능
  - 이기종 보안장비 내 AD 계정 활용(ex: 계정/그룹기반 접근제어, 802.1x 인증 활용)

Active Directory 보안위협

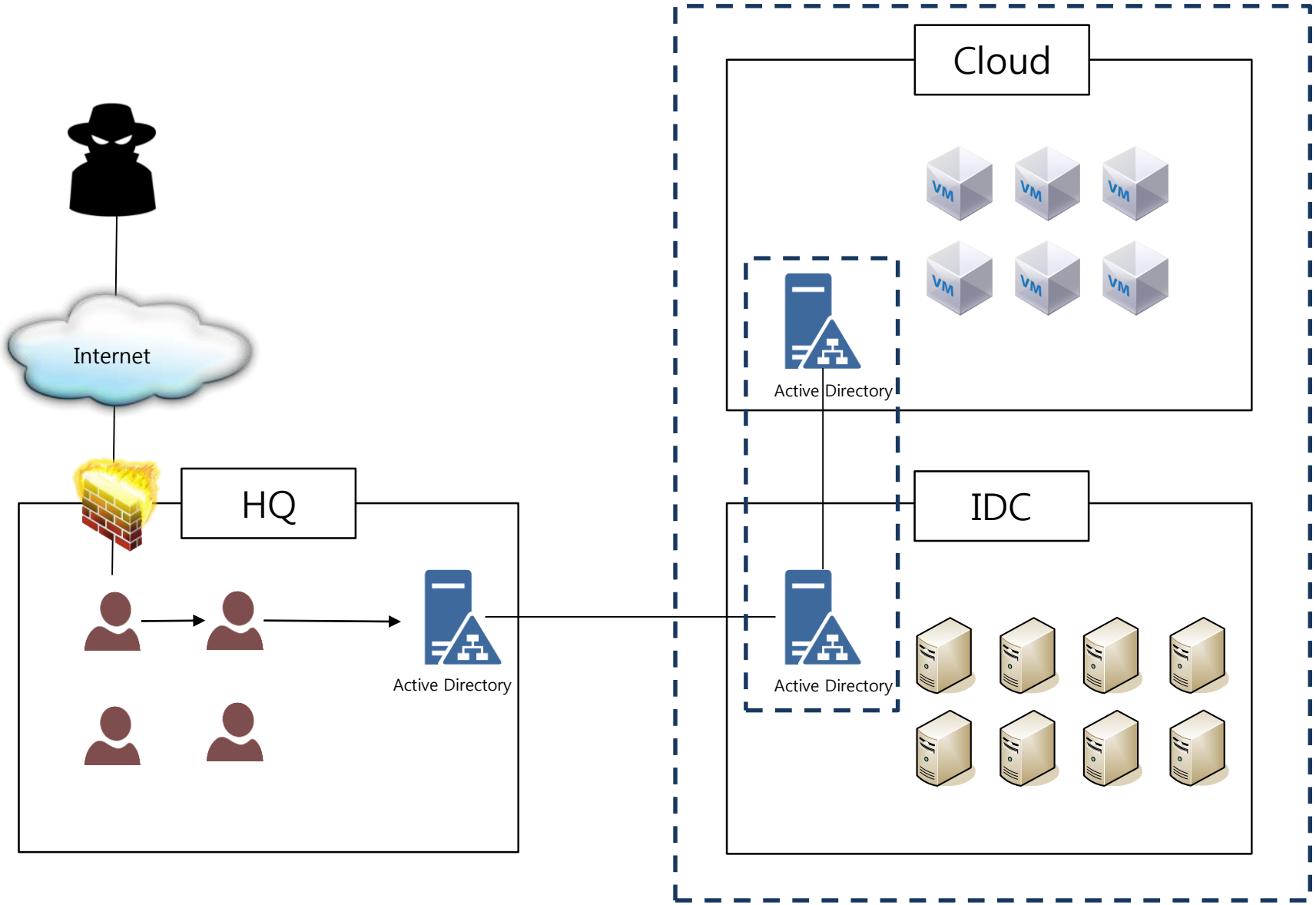
- **AD DC 서버 IP 노출**
  - Domain join을 위해서는 PC/서버의 DNS 설정이 DC의 IP로 변경 필요
  - AD DC의 IP, 정보를 쉽게 확인할 수 있음
  - 사용자 PC↔DC 와의 통신 허용 필요

- **모든 서버/워크스테이션에 접속 가능한 관리자 계정 존재**
  - Domain Join 시, Local Administrators 그룹 내 Domain Admins 그룹 자동 추가
  - Domain Admins에 속한 사용자는 AD 내 모든 자원에 대해 접근 가능

- **모든 정보가 DC(Domain Controller) 내 존재(계정, 패스워드, 컴퓨터 정보 등)**

- **Active Directory 서버의 관리자 권한 획득 시 모든 권한 획득 가능**

Active Directory 보안위협(Cont'd)



Active Directory 보안위협(Cont'd)

- **사용자 PC를 이용한 계정탈취**
  - 사용자 PC를 해킹 후, Lateral Movement를 통해 관리자 권한을 보유한 PC로 접근
  - DC에 접근할 수 있는 권한을 가진 PC와 계정 획득 후 DC 침투
  - Pass the hash, Pass the Ticket

- **DC 직접 공격**
  - 알려지지 않은 취약점 혹은 알려진 취약점(MS 14-068)을 이용한 DC 직접 공격
  - SYSVOL과 같이 접근이 가능한 경로를 통한 정보 획득

- **인증정보 탈취**
  - Kerberos 인증정보 획득을 통한 권한 획득
  - TGS password cracking, Golden Ticket, Silver Ticket

로컬 관리자 계정을 이용한 계정탈취

- 동일한 관리자 패스워드 사용
  - 최초 PC 설정 시, 유지보수 목적 등으로 동일 패스워드 사용(Administrator)
  - 관리자 패스워드 획득 시, Lateral Movement에 사용

- 관리자 계정 제한 기능 구현
  - Administrator/Guest에 대한 계정명 변경 및 사용 불가 설정
    - ✓ PC 유지보수 시 Windows PE 이용
  - 로컬 계정에 대한 원격 접속 차단
    - ✓ https://docs.microsoft.com/en-us/windows/access-protection/access-control/local-accounts
  - LAPS(Local Administrator Password Solution) 사용
    - ✓ https://technet.microsoft.com/en-us/mt227395.aspx

Domain Admins 권한 획득

- 무분별한 Domain Admins 권한 사용
  - Domain Admins은 PC/서버를 관리하기 위한 계정이 아닌 Domain을 관리하기 위한 계정
  - 무분별한 Domain Admins 계정 사용(ex: PC 유지보수실 계정에 Domain Admins 권한 부여)

- Domain Admins 사용제한
  - Domain Admins 대신 Delegate Control(제어위임)을 통한 권한 부여
    - ✓ ex) LDAP 연동용 계정, PC Join용 계정 등
  - 일반 사용자 PC Administrators 그룹 내 Domain Admins 삭제
  - Domain Admins 계정을 이용한 원격 접속(RDP), RunAS 금지
  - Domain Admins에서 DC 접근 시, 망분리 PC 사용

DC 직접 공격

- 모든 사용자는 DC에 접속할 수 있음
  - 하지만 모든 포트가 열려있어야할 필요는 없음
    - ✓ https://technet.microsoft.com/en-us/library/dd772723(v=ws.10).aspx
  - 서비스를 이유로 OS 업그레이드/보안패치 미진행
  - Group Policy, Logon Script 내 주요 정보 노출

- DC 보안 강화
  - NGFW를 이용한 SMB Upload 차단/IDS를 이용한 SMB 업로드 탐지
  - 별도의 그룹 정책 적용(Domain Controller Policy)
  - PsExec, WMIEXEC, wmic, at, 파워셀 등 이벤트 로그를 통한 원격실행 탐지
  - MS Exchange, Sharepoint 등 주요 인증정보를 가지고 있는 서버도 동일한 수준의 보안 유지

인증정보 탈취

- Kerberos
  - 인증 과정이 어려움
  - 탐지는 더더욱 어려움

- Domain Admins 계정 사용 최소화/MSA Account 이용
  - Domain Admins의 인증 정보를 탈취하는 경우가 대다수
  - SPN Scanning 등을 통해 서비스 계정 식별 및 패스워드 확인(Dictionary Attack)
  - Service Account에 대해 25자리 이상의 패스워드 사용 권고(MS)
  - MSA Account를 이용하여 패스워드/SPN 자동 변경 가능
    - ✓ https://technet.microsoft.com/en-us/library/dd560633%28v=ws.10%29.aspx
    - ✓ 제한적 적용 가능(exchange, sharepoint 등)

Active Directory eventlog 모니터링

- AD 환경의 모든 인증은 DC를 통해 처리 됨
  - DC의 로그를 통해 접속 계정/IP 확인 가능
  - Domain Admins 로그인/그룹 내 사용자 추가 등 확인 가능
  - Eventlog→syslog→SIEM/ELK 등으로 모니터링 진행

- 침해사고 모니터링
  - 이벤트로그를 통해 알려진 원격실행도구 탐지 가능
    - ✓ PsExec : Event ID 4656, *C:₩Windows₩PSEXESVC.exe*
    - ✓ Wmiexec : Event ID 5144, ₩₩*₩WMI_SHARE
    - ✓ https://www.jpcert.or.jp/english/pub/sr/ir_research.html
  - Sysmon 사용 시, 대다수의 알려진 도구 탐지 가능 → 하고 싶지만, 해보진 못했어요(유0유)

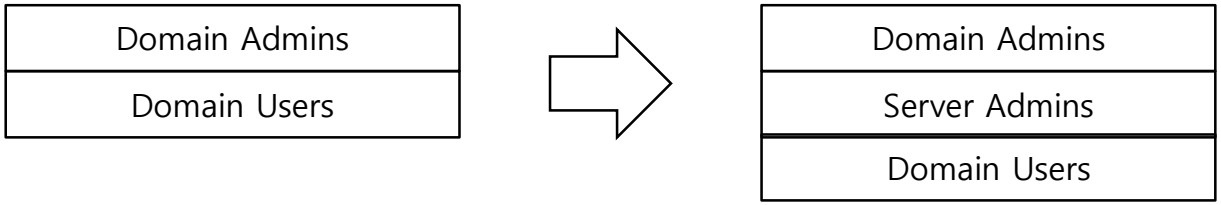
Active Directory 정기 점검

- Built-In Group 주기적 감사
  - Domain Admins/Schema Admins/Enterprise Admins/Account Operator/Local Administrators
  - python-ldap을 이용, 간단한 스크립트로 점검

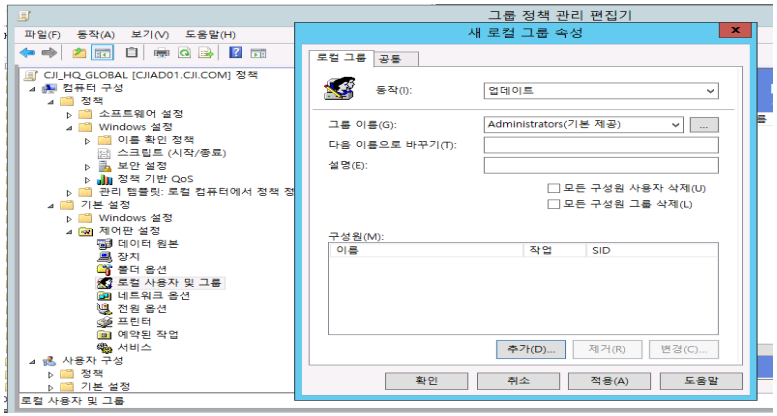
- Windows Server 대상 Prefetch 설정 및 모니터링
  - Windows Server 2012 R2의 경우 기본적으로 Prefetch 미설정
    - ✓ https://truesecdev.wordpress.com/2015/11/25/how-to-enable-prefetch-in-windows-server/
  - Prefetch 설정 및 주기적인 모니터링으로 이상파일 실행 여부 확인
    - ✓ 모니터링 자동화 방안 고민 중

Domain Admins 권한 분리

- Domain Admins 권한을 이용, Windows 서버에 접근하는 경우 다수 존재
  - IDC 인원, 인프라 관리 인원, 대량의 서버 관리자, 보안팀 등
  - 침해 당한 서버에 로그인하는 것만으로도 인증정보를 이용, DC로 침투당할 수 있음
  - 역할에 따라 분리, 서버 로그인은 Server Admins 만 이용

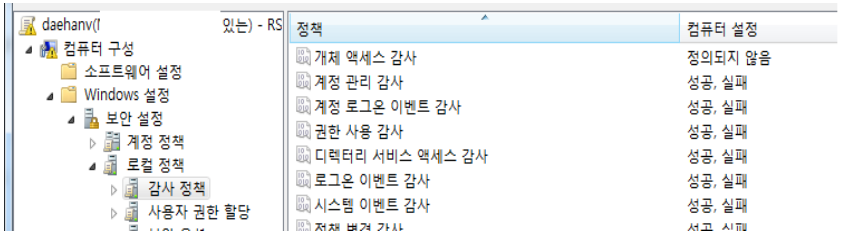


  - GPO를 통해, OU별 관리자 그룹 내 추가 가능
    - ✓ Windows 2008 R2 이상 가능



유용한 Group Policy 사용

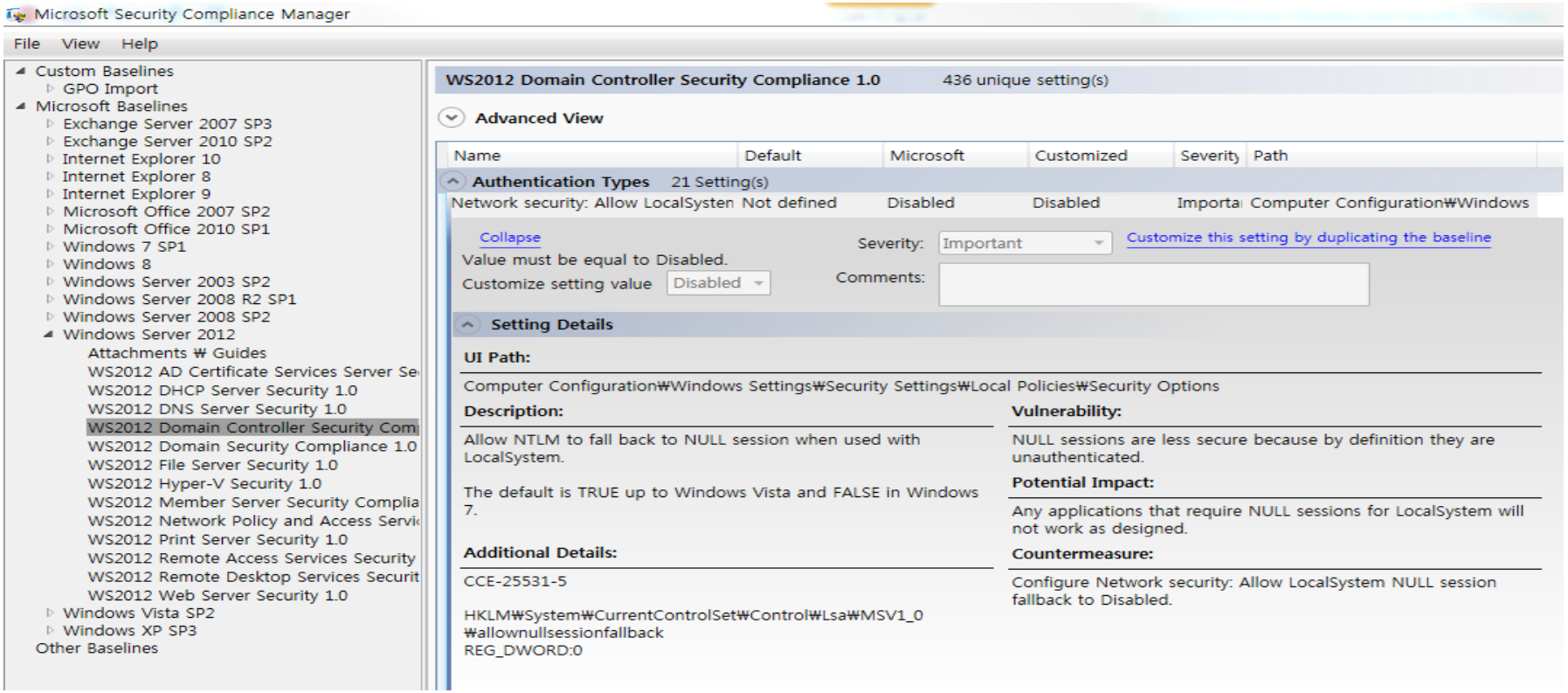
- Eventlog 설정
  - 모든 항목 다 설정(성공, 실패 모두)
  - Eventlog의 최대 크기 설정 변경 필요
    - ✓ **보안로그가 제일 중요!**



- 기타
  - Administrator 계정 이름 바꾸기
  - 원격 데스크톱 서비스를 통한 로그온 거부 <- Local Administrator 계정 등록
  - 네트워크에서 이 컴퓨터 엑세스 거부 <- Local Administrator 계정 등록
  - 시스템 시간 변경

Group Policy의 Best Practice

- Microsoft Security Compliance Manager
  - 각종 서버들의 주요 설정 정보 제공
  - 기존 GPO와 비교 기능 제공



개인적인 Best Practice

Please, don't try this at AD

- 모니터링/정기감사 안함
- 일반 계정에 대충 권한 다 주기
- 암호 외우기 어려우니, 동일한 암호 사용하기
- 암호 일괄 변경 귀찮으니, GPO로 암호 변경하기
- DC 관련 보안패치도 6개월에 한번씩
- DC에서 웹서핑도 하고, 꿀뷰로 만화도 보고
- Domain Admins을 이용해서 모든 서버를 들락날락
- 내 일반(인터넷) PC 이용 DC 접속하기

MS Advanced Threat Analytics

Malicious attacks

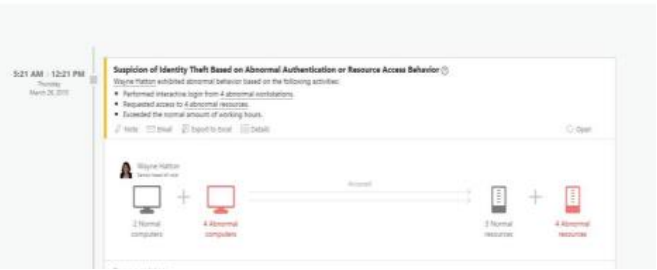
ATA detects known malicious attacks almost as instantly as they occur.

- Pass-the-Ticket (PtT)
- Pass-the-Hash (PtH)
- Overpass-the-Hash
- Forged PAC (MS14-068)
- Golden Ticket
- Malicious replications
- Reconnaissance
- Brute Force
- Remote execution
- Malicious DPAPI

Abnormal behavior

Behavioral analytics leverage Machine Learning to uncover questionable activities and abnormal behavior.

- Anomalous logins
- Unknown threats
- Password sharing
- Lateral movement



Security issues and risks

ATA identifies known security issues using world-class security researchers' work.

- Broken trust
- Weak protocols
- Known protocol vulnerabilities

사용하신 분
어떤지 좀 알려주세요(__)

Source : https://www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics

Question and Answer