엔터프라이즈 서버관리

13. 보안 및 튜닝

SangJun, Im

Department of Computer Science
e_mail : imsangjun@gmail.com

강의계획

- 서버 구성
  - AWS 회원 가입 및 준비
- 실습 서버 설치
  - 래드햇 리눅스 서버 설치
  - 운영환경 기본 구성
  - 사용자 생성 (inhatc)
- 서버 모듈 설치 및 기본 명령 실습
  - 필수 모듈 설치
  - 공용서버 접근 확인
  - 기본명령어 실습
  - 고급 명령어 실습
- 서비스 구성
  - 웹서비스 구성
  - 이메일 서비스 구성
  - 보안 서비스 구성
  - DNS 서비스
  - Database
  - sftp
- 프로그래밍
  - 쉘 프로그래밍
  - 백업 리커버리
  - 시스템 모니터링 & 프로그램
  - 개발 환경 구축 (C/C++ , JAVA, php)
- 서비스 분석
  - 서비스 관리
  - 시스템 서비스 모니터링
- 보안 및 튜닝
  - 네트워크 보안
  - 시스템 보안
  - 어플리케이션 보안

보안

- 시스템 보안
- 네트워크 보안
- 어플리케이션 보안
- 데이터베이스 보안

- 방화벽
- iptables
- 등

- 포트 번호의 중요성
  - 포트 번호
    - 호스트 내의 패킷 목적지 응용 프로그램 구별을 위한 고유 번호
    - 소스 포트와 목적지 포트 : 0 ~ 65535사이의 정수 값.
  - 호스트간 연결 구별 방법
    - 소스 IP주소: 일반적으로 자기 자신 호스트의 IP 주소.
    - 목적지 IP 주소
    - 소스 포트 번호
      - 소스 운영체제가 할당
      - 1024보다 큰 것이 관행(0부터 1023까지의 포트 번호는 시스템이 사용하도록 예약)
    - 목적지 포트 번호
  - 같은 서비스에 여러 클라이언트가 접속할 수 있는 이유
    - 목적지 IP 주소와 목적지 포트 번호는 같지만 소스 포트 번호는 각기 다름
  - *잘 알려진 서비스(well-known services)*
    - 특정한 포트 번호에서 대기하는 프로그램
    - 서비스와 관련된 포트 번호가 승인된 표준
    - 예) 포트 80: HTTP 프로토콜 용으로 잘 알려진 서비스 포트임.

서비스 추적

- **Overview**
  - 네트워크 서비스란?
    - 네트워크 포트에 연결해서 들어오는 요청을 기다리는 프로세스
    - 예) 웹 서버: 포트 80에 연결해서 사이트의 페이지를 다운로드하라는 요청에 응답할 프로세스
  - 네트워크 연결 추적 도구: `netstat` 명령어
    - 네트워크 보안과 일상적인 네트워크 문제들을 해결해 줄 유용한 도구
    - 확실한 디버깅 도구

- **`netstat` 명령어 사용하기**
  - 어떤 포트가 열려 있고 어떤 포트에 대기중인 프로세스가 있는지 추적하는 기능
  - 실행 예
    - TCP (-t) / UDP (-u)를 사용하는 연결 중 대기 중이든 실제로 연결되었든 모든 포트(-a)를 알아보고 있음
    - (-n)을 사용하여 IP 주소로부터 호스트 명을 구하지 (DNS) 말라고 지시

```
[root@ford /root]# netstat -natu
Active Internet connections (servers and
     established)
Proto Recv-Q Send-Q LocalAddress          ForeignAddress   State
tcp     1      0    209.179.251.53:1297   199.184.252.5:80 CLOSE_WAIT
tcp     1      0    209.179.251.53:1296   199.184.252.5:80 CLOSE_WAIT
tcp    57      0    209.179.158.93:1167   199.97.226.1:21  CLOSE_WAIT
tcp     0      0    192.168.1.1:6000      192.168.1.1:1052 ESTABLISHED
tcp     0      0    192.168.1.1:1052      192.168.1.1:6000 ESTABLISHED
tcp     0      0    0.0.0.0:4242          0.0.0.0:*        LISTEN
tcp     0      0    0.0.0.0:1036          0.0.0.0:*        LISTEN
tcp     0      0    0.0.0.0:1035          0.0.0.0:*        LISTEN
tcp     0      0    0.0.0.0:1034          0.0.0.0:*        LISTEN
tcp     0      0    0.0.0.0:1033          0.0.0.0:*        LISTEN
tcp     0      0    0.0.0.0:1032          0.0.0.0:*        LISTEN
tcp     0      0    0.0.0.0:1031          0.0.0.0:*        LISTEN
tcp     0      0    0.0.0.0:1024          0.0.0.0:*        LISTEN
tcp     0      0    0.0.0.0:6000          0.0.0.0:*        LISTEN
tcp     0      0    0.0.0.0:80            0.0.0.0:*        LISTEN
tcp     0      0    0.0.0.0:515           0.0.0.0:*        LISTEN
tcp     0      0    192.168.1.1:53        0.0.0.0:*        LISTEN
tcp     0      0    127.0.0.1:53          0.0.0.0:*        LISTEN
tcp     0      0    0.0.0.0:98            0.0.0.0:*        LISTEN
tcp     0      0    0.0.0.0:113           0.0.0.0:*        LISTEN
tcp     0      0    0.0.0.0:23            0.0.0.0:*        LISTEN
tcp     0      0    0.0.0.0:21            0.0.0.0:*        LISTEN
cp      0      0    0.0.0.0:111           0.0.0.0:*        LISTEN
```

SYSLOGD

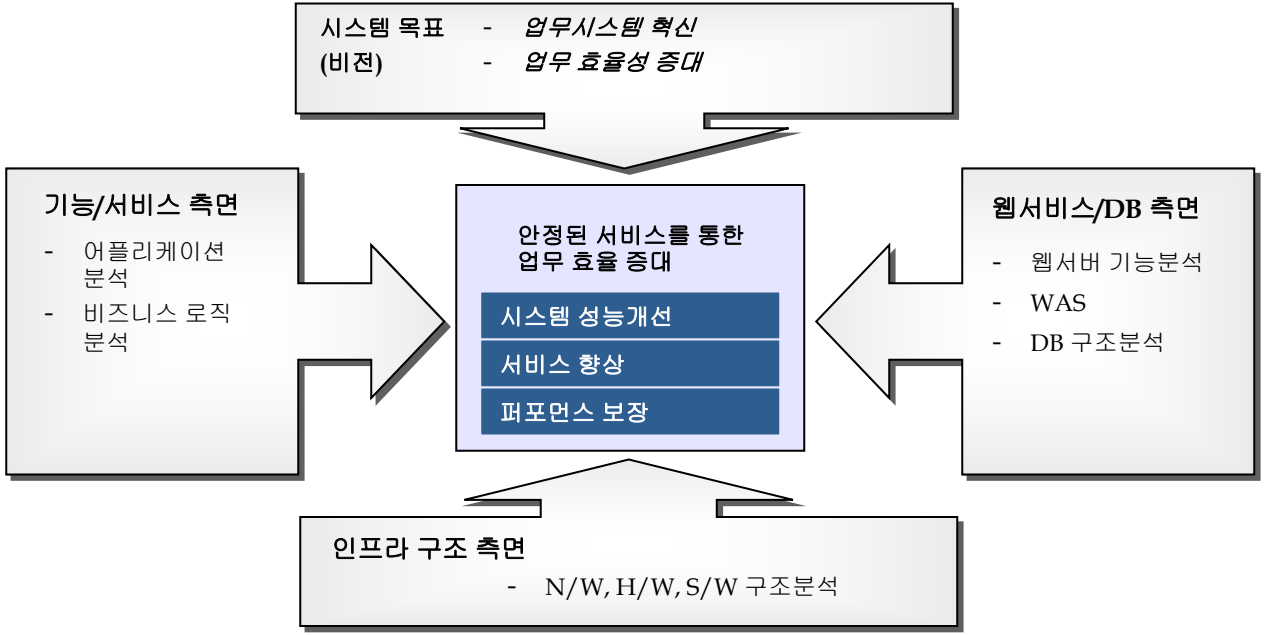
- **Overview**
  - **서비스 데몬들이 출력하는 특별한 사건이나 메시지를 로그할 수 있는 표준 메커니즘**
  - **로깅 수행에 필요한 표준 방법을 제공**
  - **`syslogd`가 사용하는 로그 파일**
    - **/var/log** 디렉터리에 저장됨.
    - 텍스트 파일 포맷
    - 로그 엔트리의 각 줄에는 날짜, 시간, 호스트 이름, 프로세스 이름, 프로세스 PID, 프로세스가 보낸 메시지 등을 기록
    - 인터페이스
      - 표준 C 라이브러리를 사용한 직접 coding 방법
      - **`logger`** 명령어를 사용하는 방법

SYSLOGD

- **syslog 활용하기**
  - **로그 메시지를 분석하여 시간대 별로 시스템 서비스에 대한 사용량을 분석할 수 있음**
  - **이상한 활동 사항도 감지할 수 있음**
    - 예) 호스트 **crackerboy.nothing-better-to-do.net**에서 아주 짧은 시간 동안 왜 그렇게 많은 웹 요청을 보냈는지를 분석해볼 필요가 있을 것임
  - **로그 파싱(parsing)**
    - 주기적으로 로그 메시지를 분석하는 것이 바람직
      - **Perl** 같은 스크립트 언어를 사용하여 로그를 파싱
      - 정상적인 동작은 빼고 나머지 것만 남긴다.

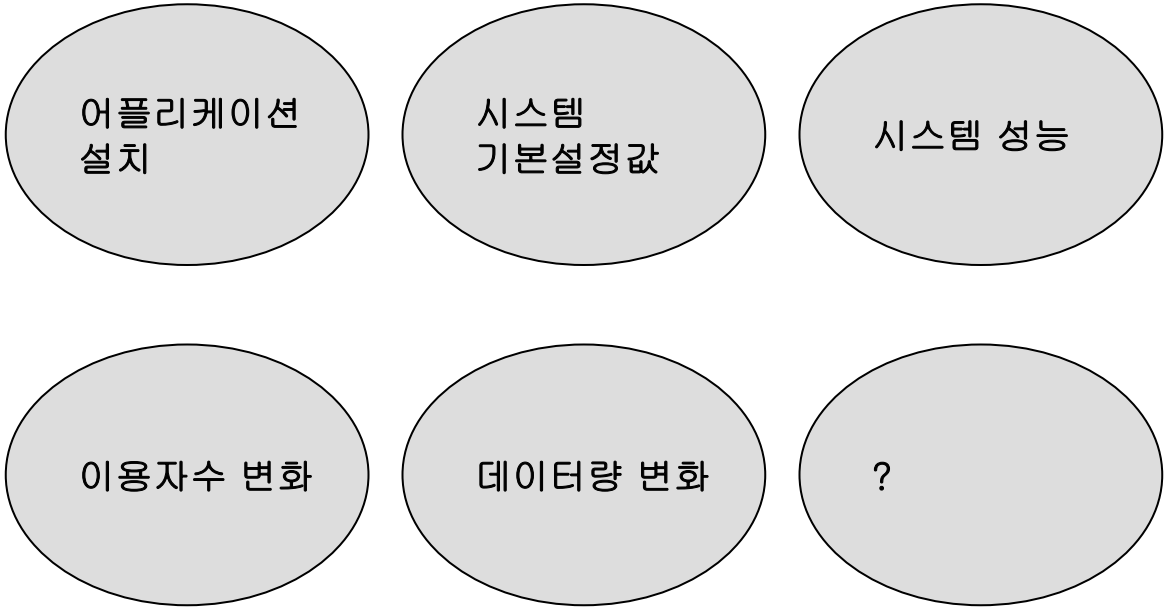
서버 튜닝 개요

- 튜닝의 목표 및 효과

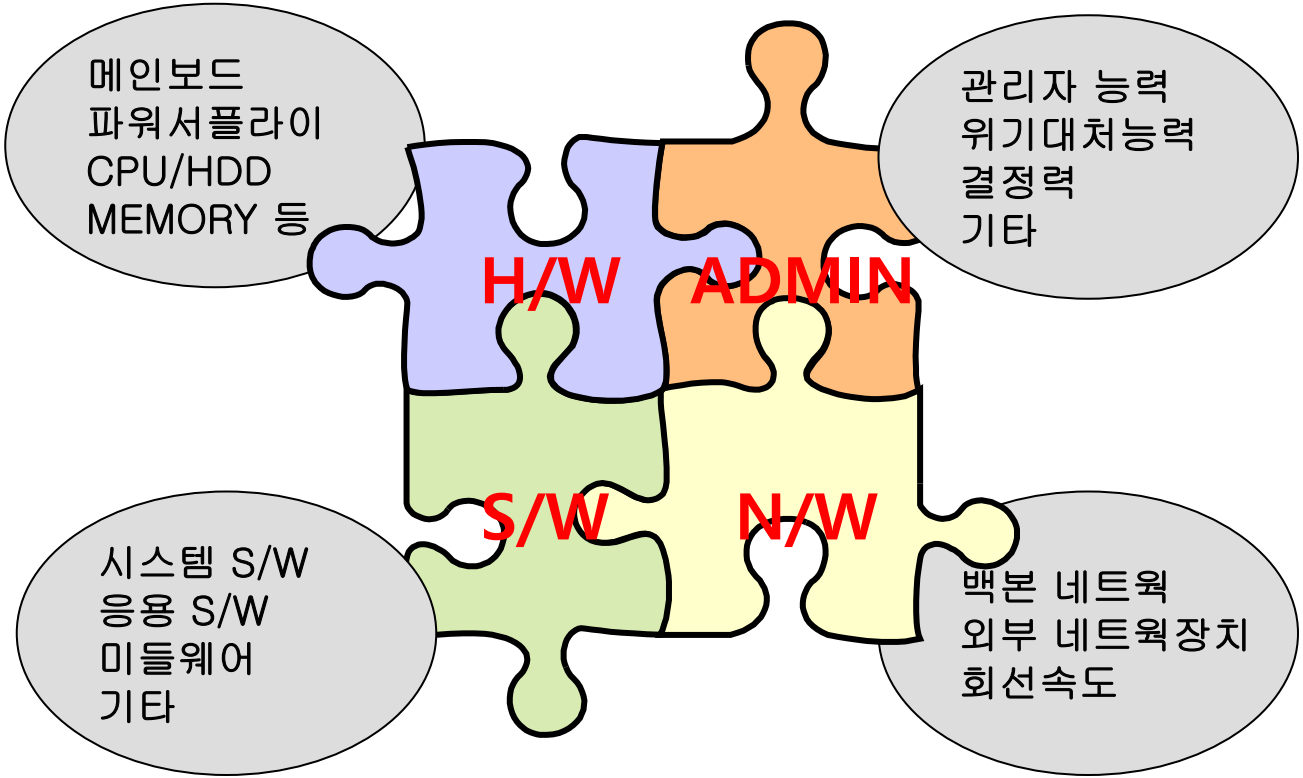


시스템 변화요소

- 튜닝에 영향을 주는요소



튜닝 대상


메인보드
파워서플라이
CPU/HDD
MEMORY 등
관리자 능력
위기대처능력
결정력
기타
H/W
ADMIN
S/W
N/W
시스템 S/W
응용 S/W
미들웨어
기타
백본 네트웍
외부 네트웍장치
회선속도

대상별 튜닝내역

- **Network**
  - 네트워크 시스템 구성상 집중화 현상이 발생 점검
  - 시스템 구성에 대한 적절성 점검
  - 성능 저해 요소인 Garbage packet 발생 포인트 점검
  - 네트워크 장비 트랜잭션 처리 성능 점검
  - 네트워크 취약성 점검

- **웹서버**
  - 운영 시 WEB 서버와 WAS 간의 응답시간 점검
  - 운영 시 로드밸런싱 유무 점검. (L4스위치 동작 및 응답시간 점검)
  - 현재 CPU사용 및 메모리 사용량 점검
  - 웹 서버 구성 (파라미터, 서브 프로세스 구성) 점검

- **WAS (web application server)**
  - 구성 (도메인,튜닝,설정 등) 점검
  - 전체 소프트웨어 구성 및 프레임웍 점검
  - 전체 서비스 구성 및 연관 관계 조사. (WAS단 끼리 연관관계 및 WAS와 기타서비스 연관관계 점검)
  - 단위 모듈별 또는 데이터베이스 쿼리,서비스 수행 응답시간 점검
  - 어플리케이션 구조 점검

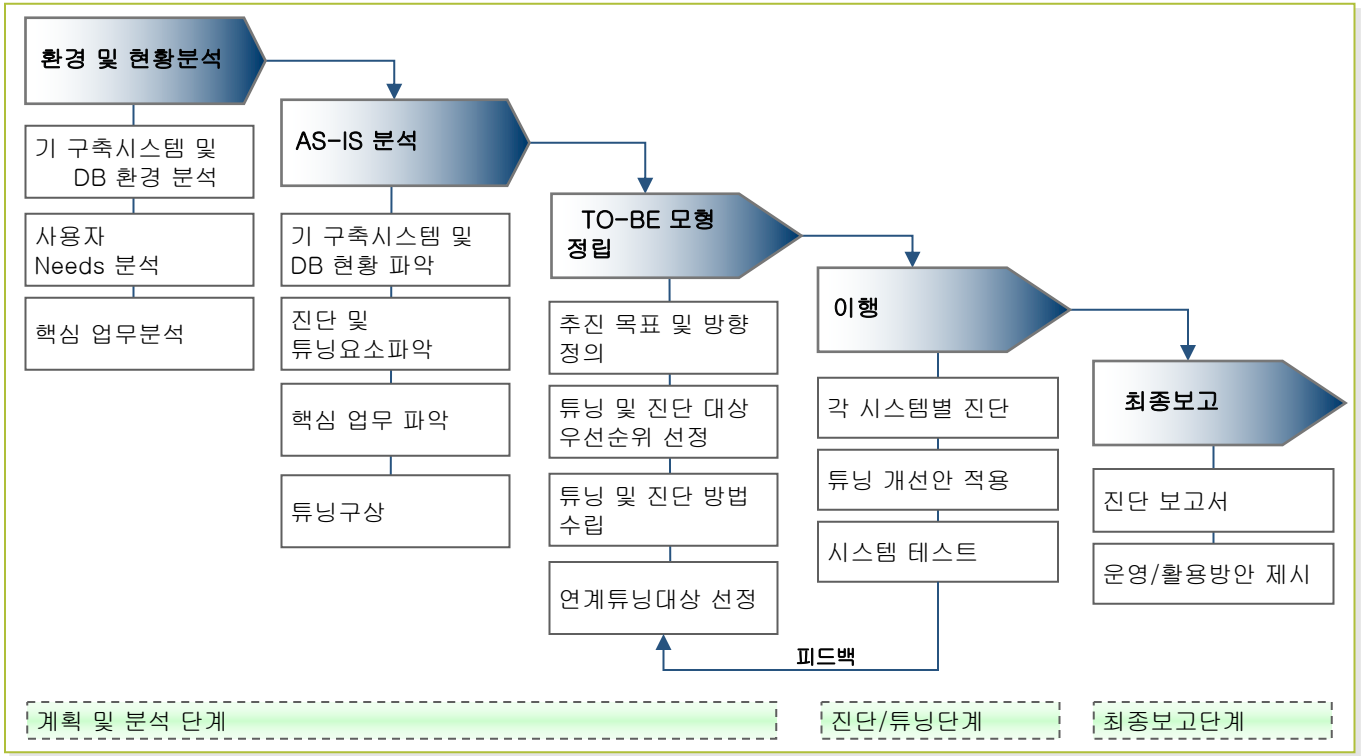
대상별 튜닝내역

- **Database**
  - 인덱스를 사용하지 않는 과도한 부하를 발생시키는 SQL문 파악
  - DB간 과도한 DB LINKS 사용에 따른 네트웍 부하
  - DB Connection Pool을 사용하지 않는 외부 APP 파악
  - 업무시간중 배치작업 유무 파악
  - 연동업무시스템과의 LOCK 발생유무 파악
  - DB서버와 스토리지 분산정책 파악하여 과도한 IO 발생 여부 파악
  - 테이블간 복잡한 Relation(Reference Key) 에 따른 성능 저하 여부 파악
  - 테이블 및 인덱스 스토리지 옵션 적정값 확인
  - DB서버 CPU 및 MEM 사용률 확인

- **기타**
  - 과부하 Application에 대한 분석
  - 배치성 Application 운영 점검 및 분석
  - 각 시스템에 대한 각종 설정값(파라메터) 점검
  - 최적화된 시스템 구성 점검 및 분석
  - 서버에 비중 있는 로드를 발생하는 성능 저해 요소 시스템 별 분석
  - 서버 별로 배치작업 및 크론작업에 대한 시간대별 로드밸런싱 분석

튜닝 절차

■ 진단 프레임웍


환경 및 현황분석
기 구축시스템 및 DB 환경 분석
사용자 Needs 분석
핵심 업무분석
AS-IS 분석
기 구축시스템 및 DB 현황 파악
진단 및 튜닝요소파악
핵심 업무 파악
튜닝구상
TO-BE 모형 정립
추진 목표 및 방향 정의
튜닝 및 진단 대상 우선순위 선정
튜닝 및 진단 방법 수립
연계튜닝대상 선정
이행
각 시스템별 진단
튜닝 개선안 적용
시스템 테스트
최종보고
진단 보고서
운영/활용방안 제시
피드백
계획 및 분석 단계
진단/튜닝단계
최종보고단계

서버 성능관리(튜닝)

- 서버 성능관리 이유?
  - 하드웨어 리소스 증설에 대한 한계 극복
  - 보유한 하드웨어 성능의 충분한 활용
  - 지속적인 서비스 보장

- 시스템 성능 향상방법
  - 시스템 사양 업그레이드
  - 시스템 또는 서비스 튜닝

- 알아야할 지식
  - 시스템
  - OS
  - 네트워크
  - 서비스(어플리케이션)

시스템 관리자

- 시스템 관리자
  - 시스템 관리자 또는 sysadmin은 컴퓨터 시스템이나 네트워크를 운영하고 유지 보수하기 위해 고용된 사람
  - 시스템 관리자는 정보 기술 부서의 구성원
  - 시스템 관리자는 서버나 다른 컴퓨터 운영 체제를 설치하고, 지원하고, 유지 보수하며 서비스 정지나 다른 문제에 대해 응답할 책임.
  - 스크립팅이나 약간의 프로그래밍 실력, 시스템 관련 프로젝트에 대한 프로젝트 관리 실력, 감시, 컴퓨터 운영 기술보유
  - 컴퓨터 문제에 대해 기술적 지원을 통한 상담 역할을 함
  - 시스템 관리자는 기술적인 능력과 책임을 증명해야함

데이터베이스 관리자

- 역할
  - 자료 복구 - 백업
  - 보전 - 데이터 보전
  - 보안 - 접근 제어
  - 성능 유지
  - 개발 및 테스트 지원

- 의무
  - 새로운 소프트웨어 설치
  - 시스템 관리자의 하드웨어 및 소프트웨어 구성
  - 보안 관리
  - 자료 분석
  - 데이터베이스 설계 (예비)
  - 데이터 모델 제작 및 최적화
  - 기존의 엔터프라이즈 데이터베이스의 관리, 새로운 데이터 베이스의 분석, 설계, 작성에 대한 책임

네트워크 관리자

- 역할
  - 네트워크 정상운영 유지
  - 기본네트워크 운용
    - 사용자설정
    - 디렉토리구성 및 파일관리
    - 사용자 인터페이스 작성
    - 성능 모니터링
  - 네트워크 향상
    - 모델링
    - 성능향상
    - 네트워크 확장
    - 인터네트워킹
    - 보안 및 장애관리
  - 사용자교육
  - 네트워크 보호

보안관리자

- 역할
  - 문서/보고서 등의 정보보안 모니터링
  - 방화벽, 침입탐지, 바이러스 모니터링
  - SIM 관리
  - 보안취약점 및 위험분석
  - 보안문제점 해결
  - 보안시스템 설치 및 감리
  - 보안 유지보수

END