**SYSTEM진단 역량강화 – 환경분석**

**대상 기본정보**

OS : CentOS 6.9

DBMS : MySQL 5.1.73-8

Web server : APACHE 2.2.15-69

WAS : N/A (/root/apache-tomcat-9.0.0.M19 설치 디렉터리만 존재함)

**포트 분석**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Proto** | **Local Address** | **Well Known 여부** | **Foreign Address** | **Program name** | **비고** |
| tcp | 0.0.0.0:39939 | N (rpcbind) | 0.0.0.0:\* | rpc.statd | RPC 클라이언트와 서버의 상태 모니터링 |
| tcp | 0.0.0.0:3306 | Y (mysql) | 0.0.0.0:\* | mysqld | DBMS(mysql) 서비스 Port |
| tcp | 0.0.0.0:111 | Y (rpcbind) | 0.0.0.0:\* | rpcbind | RPC Address 분배 |
| tcp | 0.0.0.0:22 | Y (ssh) | 0.0.0.0:\* | sshd | SSH 연결 Port |
| tcp | 127.0.0.1:631 | Y (IPP) | 0.0.0.0:\* | cupsd | 프린터 사용을 위한 서비스 |
| tcp | 127.0.0.1:25 | Y (SMTP) | 0.0.0.0:\* | master | Postfix 메일 전송 서비스 포트 |
| tcp | :::80 | Y (ssh) | :::\* | httpd | WEB Server(Apache) 서비스 포트 |

**데몬 분석**

|  |  |  |  |
| --- | --- | --- | --- |
| **RUSER** | **COMMAND** | **목적** | **비고** |
| root | init | 시스템 커널 부팅 프로그램 | /sbin/ |
| root | udevd | 리눅스 커널 장치 관리자 | /sbin/ |
| root | auditd | 시스템 정보 감사 | /sbin/ |
| root | portreserve | 포트 예약 관리 | /sbin/ |
| root | rsyslogd, syslogd | 시스템 로그 관리 | /sbin/ |
| rpc | rpcbind | 원격 호출 관련(NFS, 포트 매핑 등) 서비스 관리 | /sbin/rpcbind |
| dbus | dbus-daemon | IPC와 같은 dbus관련 서비스 관리 | /bin/ |
| root | NetworkManager | 네트워크 변경 사항 탐지 및 설정 | /usr/sbin/ |
| root | modem-manager | 모뎀 관리 | /usr/sbin/ |
| rpcuser | rpc.statd | 클라이언트와 서버의 상태 모니터링 | /sbin/rpc.statd |
| root | dhclient | IP 동적 할당 관리 | /sbin/ |
| root | wpa\_supplicant | 무선랜(wi-fi) 설정 | /usr/sbin/ |
| root | cupsd | 프린터 사용 관리 | /etc/  /usr/lib/  /usr/share/ |
| root | acpid | ACPI 방식의 시스템 전력 관리 | /usr/sbin/ |
| 68 | hald | 디바이스 장치 자동 인식 | /usr/sbin/ |
| Root | hald-runner | /usr/libexec/ |
| Root | hald-addon-input | /usr/libexec/ |
| 68 | hald-addon-acpi | /usr/libexec/ |
| root | automount | 파일시스템 사용 관련 자동 마운트 | /usr/sbin/ |
| root | sshd | SSH 서비스 | /usr/sbin/ |
| root | mysqld\_safe | MySQL\_safe 서비스 실행 관련 | /usr/bin/  datadir=/var/lib/mysql |
| mysql | mysqld | MySQL 서비스 실행 관련 | /usr/libexec/  datadir=/var/lib/mysql |
| root | master | Postfix 메일 서버 마스터 프로세스 | /usr/libexec/postfix/ |
| postfix | qmgr | Postfix 메일 서버 큐 관리 |  |
| root | abrtd | 자동 버그 보고 도구 | /usr/sbin/ |
| apache | httpd | 아파치 웹 서버 실행 | /usr/sbin/ |
| root | crond | 정기 작업 예약 스케줄러 | /usr/sbin/ |
| root | at | 단일 예약 작업 관리 | /usr/sbin/ |
| root | certmonger | PKI(인증서) 모니터링 및 갱신 | /usr/sbin/ |
| root | gdm-binary | GNOME(GUI) 디스플레이 매니저 | /usr/sbin/ |
| root | mingetty | 가상 터미널 관리 / 콘솔 로그인 입력 대기 | /sbin/ |
| root | gdm-simple-slave | GUI(GNOME) 환경 실행 관리 | /usr/libexec/ |
| root | Xorg | GUI(GNOME) 환경 실행 관리 | /usr/bin/ |
| root | console-kit-daemon | GUI(GNOME) 환경에서의 콘솔 로그인 관리 | /usr/sbin/ |
| gdm | dbus-launch | IPC와 같은 dbus관련 서비스 관리 | /usr/bin/ |
| root | devkit-power-daemon | 장치 전원 관리 기능 | /usr/libexec/ |
| root | polkitd | 시스템 전반에서 인증 단계 관리 및 통제 | /usr/libexec/polkit-1/ |
| rtkit | rtkit-daemon | 실시간 프로세스 스케줄링 관리 | /usr/libexec/ |
| root | pam.d | 리눅스 사용자 인증 및 접근 권한 설정 관리 | /etc/ |
| root | gnome-keyring-daemon | 세션 키링, 패스워드 및 암호문 저장 및 관리 | /usr/bin/ |
| root | gnome-session | 시스템 GUI 환경 접속 | /usr/bin/ |
| root | dbus-launch | IPC와 같은 dbus관련 서비스 관리 | /usr/bin/ |
| root | dbus-daemon | IPC와 같은 dbus관련 서비스 관리 | /bin/ |
| root | gconfd-2 | GNOME(GUI) 시스템 관리 및 설정 도구 | /usr/libexec/ |
| root | gnome-settings-daemon | GNOME(GUI) 설정 도구 | /usr/libexec/ |
| root | seahorse-daemon | GUI(GNOME) 환경에서 암호화된 키값(패스워드) 관리 | /usr/bin/ |
| root | gvfsd | GNOME 가상 파일 시스템 관리 | /usr/libexec/ |
| root | gvfs-fuse-daemon | gvfs를 FUSE 파일 시스템으로 마운트 | /usr/libexec/ |
| root | metacity | GUI 환경 제공 | /usr/bin/ |
| root | gnome-panel | GUI 환경 제공 | /usr/bin/ |
| root | nautilus | 파일 관리자 | /usr/bin/ |
| root | bonobo-activation-server | 구성 요소 컴포넌트 추적기 | /usr/libexec/ |
| root | gvfs-gdu-volume-monitor | Gvfs 디스크 볼륨 사용량 모니터링 | /usr/libexec/ |
| root | wnck-applet | GUI(GNOME) 환경 패널 / 윈도우 창 리스트 관리 | /usr/libexec/ |
| root | trashapplet | GUI(GNOME) 환경 휴지통 관리 | /usr/libexec/ |
| root | udisks-daemon | 디스크 저장소 관리 | /usr/libexec/ |
| root | udisks-daemon | 디스크 저장소 관리 |  |
| root | gvfsd-trash | Gvfs 휴지통 (불필요한 파일 시스템 정리) | /usr/libexec/ |
| root | gvfs-afc-volume-monitor | Gvfs afc 볼륨 모니터링 (afc : apple file conduit) | /usr/libexec/ |
| root | gvfs-gphoto2-volume-monitor | Gvfs gphoto2 볼륨 모니터링 (gphoto2 : 사진 관리 프로그램) | /usr/libexec/ |
| root | gnote | GUI(GNOME) 환경에서 메모장, 텍스트 편집기 | /usr/bin/ |
| root | clock-applet | GUI(GNOME)시간 관련 도구 (시간 설정) | /usr/libexec/ |
| root | gdm-user-switch-applet | GUI(GNOME) 환경에서 사용자 변경 관리 | /usr/libexec/ |
| root | notification-area-applet | GUI(GNOME) 환경에서 NOTI(알람) 발생 관리 | /usr/libexec/ |
| root | gnome-power-manager | GUI 환경 제공 | /usr/bin/ |
| root | gdu-notification-daemon | GUI(GNOME) 디스크 관련 NOTI(알람) | /usr/libexec/ |
| root | polkit-gnome-authentication-agent-1 | GUI(GNOME) 환경 시스템 전반에서 인증 단계 관리 및 통제 | /usr/libexec/polkit-gnome-authentication-agent-1 |
| root | evolution-alarm-notify | Evolution (이메일 클라이언트) 이벤트 알림 | /usr/libexec/evolution/2.32/ |
| root | nm-applet --sm-disable | 네트워크 설정 및 관리 (GUI, GNOME) | /usr/bin/ |
| root | gnome-volume-control-applet | GUI(GNOME) 환경에서 사운드 볼륨 관리 | /usr/bin/ |
| root | pulseaudio | 사운드 관리 | /usr/bin/ |
| root | abrt-applet | 자동 버그 리포팅 도구 | /usr/bin/ |
| root | bluetooth-applet | GUI(GNOME) 환경에서 블루투스 설정 및 관리 | /usr/bin/ |
| root | restorecond | SELinux 관련, 파일 생성 감시 | /usr/sbin/ |
| root | im-settings-daemon | 키보드 등 입력기 설정 | /usr/libexec/ |
| root | gpk-update-icon | GNOME 소프트웨어 업데이트 알림 및 관리 | /usr/bin/ |
| root | /usr/libexec/pulse/gconf-helper | GUI(GNOME) 환경에서 pulseaudio 관리 헬퍼 | /usr/libexec/pulse/ |
| root | gnome-screensaver | GUI(GNOME) 환경 스크린세이버 설정 및 관리 | /usr/bin/ |
| root | ibus-daemon | 입력(키보드) 버스 관리 | /usr/bin/ |
| root | gconf-im-settings-daemon | GUI(GNOME) 환경에서 키보드 등 입력기 설정 | /usr/libexec/ |
| root | ibus-gconf | GUI(GNOME) 환경에서 입력 버스 설정 | /usr/libexec/ |
| root | ibus-x11 | X11 환경 입력 버스 관리 | /usr/libexec/ |
| root | ibus-engine-hangul | 한글 입력 버스 엔진 | /usr/libexec/ |
| root | gvfsd-burn | CD 굽기 위치 제공 | /usr/libexec/ |
| root | gvfsd-metadata | 내부 gvfs 메타데이터 저장소 관리 | /usr/libexec/ |
| root | sshd | SSH 접속 프로세스 |  |
| root | bash | bash 쉘 실행 | /bin/ |
| root | top | 실시간 CPU 사용률 체크 | /usr/bin/ |
| postfix | pickup | Postfix 메일 서버 관리 |  |

**계정 분석**

/etc/passwd 파일 내용:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Username** | **Info** | **Home directory** | **Command/shell** | **비고** |
| root | root | /root | /bin/bash | 최고관리자 |
| bin | bin | /bin | /sbin/nologin | 명령어 실행 |
| daemon | daemon | /sbin | /sbin/nologin | 데몬 프로세스 실행 |
| adm | adm | /var/adm | /sbin/nologin | 시스템 관리자 별도 계정 |
| lp | lp | /var/spool/lpd | /sbin/nologin | 로컬 프린트 서버 |
| sync | sync | /sbin | /bin/sync | 원격지 서버 동기화 |
| shutdown | shutdown | /sbin | /sbin/shutdown | 시스템 종료 |
| halt | halt | /sbin | /sbin/halt | 시스템 강제 종료 |
| mail | mail | /var/spool/mail | /sbin/nologin | 메일 서비스 |
| uucp | uucp | /var/spool/uucp | /sbin/nologin | 유닉스 시스템 파일 복사 |
| operator | operator | /root | /sbin/nologin | 특수 목적용(시스템 백업 등), 여러 사용자가 시스템 공통관리를 위해 사용 |
| games | games | /usr/games | /sbin/nologin | GUI 환경에서 게임 실행 |
| gopher | gopher | /var/gopher | /sbin/nologin | 웹(www) 이전에 사용하던 서비스 |
| ftp | FTP User | /var/ftp | /sbin/nologin | FTP 서비스 |
| nobody | Nobody | / | /sbin/nologin | 웹 서비스 등 외부 오픈 서비스에서 사용하는 익명 연결 계정 |
| dbus | System message bus | / | /sbin/nologin | 시스템 메시지 출력 |
| usbmuxd | usbmuxd user | / | /sbin/nologin | USB 연결 및 마운트 관련 |
| rpc | Rpcbind Daemon | /var/lib/rpcbind | /sbin/nologin | 원격 호출 관련(NFS, 포트 매핑 등) 서비스 |
| rtkit | RealtimeKit | /proc | /sbin/nologin | 실시간 프로세스 스케줄링 정책 관련 서비스 |
| avahi-autoipd | Avahi IPv4LL Stack | /var/lib/avahi-autoipd | /sbin/nologin | IPv4 자동 할당 서비스 |
| vcsa | virtual console memory owner | /dev | /sbin/nologin | 가상메모리 생성 시 계정 |
| abrt | - | /etc/abrt | /sbin/nologin | 프로그램 버그 리포팅 서비스 |
| rpcuser | RPC Service User | /var/lib/nfs | /sbin/nologin | RPC(NFS 등) 사용자 |
| nfsnobody | Anonymous NFS User | /var/lib/nfs | /sbin/nologin | NFS 서비스 이용 기본 계정 |
| haldaemon | HAL daemon | / | /sbin/nologin | 디바이스 장치 인식 |
| ntp | - | /etc/ntp | /sbin/nologin | 시간 동기화 |
| apache | Apache | /var/www | /sbin/nologin | 아파치 웹 서버 |
| saslauth | Saslauthd user | /var/empty/saslauth | /sbin/nologin | Postfix 등 메일 서버에서 SASL 보안 프로토콜을 이용한 사용자 인증 서비스 |
| postfix | - | /var/spool/postfix | /sbin/nologin | 메일 전송 서버 |
| gdm | - | /var/lib/gdm | /sbin/nologin | GUI 사용 관련 |
| pulse | PulseAudio System Daemon | /var/run/pulse | /sbin/nologin | 사운드(오디오) 서버 프로그램 |
| sshd | Privilege-separated SSH | /var/empty/sshd | /sbin/nologin | SSH 서비스 |
| tcpdump | - | / | /sbin/nologin | tcpdump 프로그램 |
| adiosl | Adiosl | /home/adiosl | /bin/bash | 일반 사용자 로그인 계정 |
| mysql | MySQL Server | /var/lib/mysql | /bin/bash | MySQL 서비스 |
| cubrid | - | /home/cubrid | /bin/bash | 일반 사용자 로그인 계정 |
| named | Named | /var/named | /sbin/nologin | DNS 서비스 |