보안을 위한

KISA | 한눈에 보는 로그설정 노트 (응용프로그램)

설정 방법	권장 설정 값	참고
1. apache 로그 설정		

1. /etc/logrotate.d/httpd 생성
# touch /etc/logrotate.d/httpd 	
 	
2. /etc/logrotate.d/httpd 설정 (아래 항목을 작성)
: /var/log/httpd/*log {
daily
create 0664 root root
missingok
notifempty
sharedscripts
rotate 180
postrotate
/sbin/service httpd reload 〉
/var/log/httpd/rotate 2〉&1 || true
endscript
compress
}
	/var/log/httpd/*log {
	daily
	create 0664 root root
	missingok
	notifempty
	sharedscripts
	rotate 180
	postrotate
	/sbin/service httpd reload 〉
	/var/log/httpd/rotate 2〉&1 || true
	endscript
	compress
	}
		로그 파일은 파일별 하루의 로그 저장
		로그 파일 생성 시, 0664의 권한, root 소유,
		root 그룹으로 설정
		로그 파일은 6개월 분량 보관
		로그 파일이 존재하지 않아도 오류 발생하지 않음
		로그 파일명에 YYYYMMDD 형식의 문자열을 추가
		로그 내용이 없으면 rotation 하지 않음
		로그파일이 로테이트된 후 다음의 커맨드를 실행
		/sbin/service httpd reload 〉 /var/log/httpd/
		rotate 2〉&1 || true

2. nginx 로그 설정		
1. /etc/logrotate.d/nginx 생성 # touch /etc/logrotate.d/nginx 2. /etc/logrotate.d/nginx 설정 (아래 항목을 작성) : /var/log/nginx/*log { create 0644 nginx nginx daily rotate 180 missingok notifempty compress sharedscripts postrotate /bin/kill –USR1 `cat /run/nginx.pid 2〉 /dev/null` 2〉/dev/null || true endscript	/var/log/nginx/*log { create 0644 nginx nginx daily rotate 180 missingok notifempty compress sharedscripts postrotate /bin/kill –USR1 `cat /run/nginx.pid 2〉/dev/null` 2〉/dev/null || true endscript }	로그 파일은 파일별 하루의 로그 저장 로그 파일 생성 시, 0664의 권한, root 소유, root 그룹으로 설정 로그 파일은 6개월 분량 보관 로그 파일이 존재하지 않아도 오류 발생하지 않음 로그 파일명에 YYYYMMDD 형식의 문자열을 추가 로그 내용이 없으면 rotation 하지 않음 로그파일이 로테이트된 후 다음의 커맨드를 실행 /bin/kill –USR1 `cat /run/nginx.pid 2〉/ dev/null` 2〉/dev/null || true
3. IIS 웹 서버 로그 설정 변경		
1. 로그 경로 변경 (추가 볼륨 사용 권장) IIS 관리자(또는 inetmgr.exe 실행) ▶ 로깅 : 로그 저장 옵션은 디폴트(매일 다른 파일로 로그 저장) 유지 권장	다음과 같은 추가 볼륨 경로로 변경 : 〈추가 볼륨〉₩IIS_log	웹 로그는 추가 disk 확보 후 최소 6개월 이상의 분량을 저장 권고 %SystemDrive%₩inetpub₩logs₩LogFiles
4. Snoopy Logger 설치		
1. /etc/snoopy.ini 설정 : 〈권장 설정 값〉 참조 2. 기능 활성화 # sudo snoopy enable 3. 서비스 또는 시스템 재시작 시스템 재시작(권장) 또는 아래와 같이 로깅할 개별 서비스 재시작 # /etc/init.d/ssh restart	다음의 메시지 포맷을 [snoopy] 섹션에 추가 : message_format = "[username:%{username} uid:%{uid} sid:%{sid} tty:%{tty} cwd:%{cwd} filename:%{filename}]: %{cmdline}"	다음 위치에서 로그 확인 가능 R C : /var/log/secure D U : /var/log/auth.log Snoopy는 디폴트로 모든 서비스에 대한 명령어 히스토리를 로깅함 일부 버전의 OS는 /etc/snoopy.ini 파일 생성 후 〈권장 설정 값〉 입력

설정 방법	권장 설정 값	참고
5. Sysmon 설치 (선택)		
1. 로그 크기 설정 이벤트 뷰어 ▶ 응용 프로그램 및 서비스 로그 ▶ Microsoft ▶ Windows ▶ Sysmon ▶ Operational ▶ 속성 ▶ 최대 로그 크기 2. 로그 경로 변경 (추가 볼륨 사용 권장) 이벤트 뷰어 ▶ 응용 프로그램 및 서비스 로그 ▶ Microsoft ▶ Windows ▶ Sysmon ▶ Operational ▶ 속성 ▶ 로그 경로	로깅 : 사용 크기 : 0xFFFF0000 (4194240 KB) (32/64bit) 다음과 같은 추가 볼륨 경로로 변경 : 〈추가 볼륨〉₩EventLogs	%SystemRoot%₩System32₩Winevt₩Logs₩ Microsoft–Windows–Sysmon%4Operational.evtx 반드시 추가 HDD를 장착할 수 있을 경우만 사용 권장

☞ Sysmon은 disk 용량 및 성능 등의 이슈가 있을 수 있으니 충분한 테스트와 상시 관리가 가능한 경우만 사용하십시오.

범례

- OS : 별도 설치, 설정이 필요한 항목
- OS : 사용 불가능한 항목
- : Windows 응용프로그램
- : Linux 응용프로그램
- R : RedHat Enterprise Server 7.6
- C : CentOS 6.9
- D : Debian 9.5.0
- U : Ubuntu 16.04.4 LTS