KISA | 보안을 위한 한눈에 보는 로그설정 노트 (Window)

설정 방법	권장 설정 값	참고
1. 이벤트 로그 감사 설정 7 | 10 | 08 | 12 | 16		
1. 제어판을 이용한 설정 08 : gpedit.msc ▶ 컴퓨터 구성 ▶ Windows 설정 ▶ 보안 설정 ▶ 로컬 정책 ▶ 감사 정책 12 16 7 10 : gpedit.msc ▶ 컴퓨터 구성 ▶ Windows 설정 ▶ 보안 설정 ▶ 고급 감사 정책 구성 ▶ 시스템 감사 정책 ▶ 계정 로그온, 계정 관리, 세부 추적, 로그온/로그오프, 개체 액세스, 시스템	자격 증명 유효성 검사 감사 (성공, 실패) 기타 계정 로그온 이벤트 감사 (성공, 실패) 컴퓨터 계정 관리 감사 (성공, 실패) 사용자 계정 관리 감사 (성공, 실패) 프로세스 만들기 감사 (성공, 실패) RPC 이벤트 감사 (성공, 실패) 로그오프 감사 (성공, 실패) 로그온 감사 (성공, 실패) 기타 로그온/로그오프 이벤트 감사 (성공, 실패) 특수 로그온 감사 (성공, 실패) 파일 공유 감사 (성공, 실패) 기타 개체 액세스 이벤트 감사 (성공, 실패) 보안 상태 변경 감사 (성공, 실패)	고급 감사정책 구성 GUI는 쓸 수 없으며 auditpol.exe를 통한 수동 설정만 가능
2. 이벤트 로그 크기 설정 7 | 10 | 08 | 12 | 16		
1. 레지스트리를 이용한 설정 : HKLM₩SYSTEM₩CurrentControlSet₩services₩eventlog₩Security₩MaxSize (REG_DWORD) : HKLM₩SYSTEM₩CurrentControlSet₩services₩eventlog₩System₩MaxSize (REG_DWORD) : HKLM₩SYSTEM₩CurrentControlSet₩services₩eventlog₩Application₩MaxSize (REG_DWORD) : HKLM₩SYSTEM₩CurrentControlSet₩services₩eventlog₩Windows PowerShell₩MaxSize (REG_DWORD)	보안, 시스템, 애플리케이션 : 0xFFFF0000 (4194240 KB) (4GB 이상) 파워쉘 : 0x06400000 (102400 KB) (100MB 이상)	Security, System, Application 이벤트 로그는 여유 공간 확보 후 저장 log Security.evtx log System.evtx log Application.evtx log Windows PowerShell.evtx
3. 이벤트 로그 경로 변경 7 | 10 | 08 | 12 | 16		
1. 로그 경로 변경 (추가 볼륨이 있을 경우) 이벤트 뷰어 ▶ Windows 로그 ▶ 시스템, 응용 프로그램, 보안 ▶ 속성 ▶ 로그 경로	다음과 같은 추가 볼륨 경로로 변경 : 〈추가 볼륨〉₩EventLogs	보안, 시스템, 응용프로그램 이벤트 로그는 추가 disk 사용 권고 〈추가볼륨〉₩EventLogs₩System.evtx 〈추가볼륨〉₩EventLogs₩Application.evtx 〈추가볼륨〉₩EventLogs₩Security.evtx
4. 이벤트 로그 설정 (시간 변경) 7 | 10 | 08 | 12 | 16		
1. 로그 크기 설정 이벤트 뷰어 ▶ 응용 프로그램 및 서비스 로그 ▶ Microsoft ▶ Windows ▶ DateTimeControlPanel ▶ Operational ▶ 속성	로깅 : 사용 크기 : 0x06400000 (102400 KB) (100MB 이상)	log Microsoft-Windows-DateTimeControlPanel%4Operational.evtx
5. 이벤트 로그 설정 (저장매체 연결) 7 | 10 | 08 | 12 | 16		
1. 로그 크기 설정 이벤트 뷰어 ▶ 응용 프로그램 및 서비스 로그 ▶ Microsoft ▶ Windows ▶ DriverFrameworks-UserMode ▶ Operational ▶ 속성	로깅 : 사용 크기 : 0x06400000 (102400 KB) (100MB 이상)	log Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx
6. 이벤트 로그 설정 (윈도우 방화벽) 7 | 10 | 08 | 12 | 16		
1. 로그 크기 설정 이벤트 뷰어 ▶ 응용 프로그램 및 서비스 로그 ▶ Microsoft ▶ Windows ▶ Windows Defender ▶ Operational ▶ 속성	로깅 : 사용 크기 : 0x06400000 (102400 KB) (100MB 이상)	log Microsoft-Windows-Windows Defender%4Operational.evtx 08 은 Desktop Experience 설치 후 기능 활성화 가능 12 는 Microsoft Security Essentials in Windows Server 2012 설치 후 활성화 가능
7. 이벤트 로그 설정 (원격 데스크톱) 7 | 10 | 08 | 12 | 16		
1. 로그 크기 설정 이벤트 뷰어 ▶ 응용 프로그램 및 서비스 로그 ▶ Microsoft ▶ Windows : RemoteDesktopServices-RdpCoreTS ▶ Operational ▶ 속성 : TerminalServices-LocalSessionManager ▶ Operational ▶ 속성 : TerminalService-RemoteConnectionManager ▶ Operational ▶ 속성	로깅 : 사용 크기 : 0x06400000 (102400 KB) (100MB 이상)	log Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational.evtx, log Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx, log Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx 08 에서는 RdpCoreTS 사용 금지 권장

설정 방법	권장 설정 값	참고
8. 이벤트 로그 설정 (네트워크 연결) 7 | 10 | 08 | 12 | 16		
1. 로그 크기 설정 이벤트 뷰어 ▶ 응용 프로그램 및 서비스 로그 ▶ Microsoft ▶ Windows ▶ NetworkProfile ▶ Operational ▶ 속성	로깅 : 사용 크기 : 0x06400000 (102400 KB) (100MB 이상)	log Microsoft-Windows-NetworkProfile%4Operational.evtx
9. 로컬 방화벽 로그 설정 7 | 10 | 08 | 12 | 16		
1. 제어판을 이용한 설정 08 : 시작 프로그램, 관리 도구 ▶ 고급 보안이 설정된 Windows 방화벽 ▶ 속성 ▶ 로깅, 사용자 지정 12 16 7 10 : 제어판 ▶ Windows 방화벽 ▶ 고급 설정 ▶ 속성 ▶ 로깅, 사용자 지정	손실된 패킷을 로그에 기록: 활성화 성공한 연결을 로그에 기록: 활성화 LogFileSize: 0x19000 (102400 KB)(100 MB 이상)	%SystemRoot%₩System32₩LogFiles₩Firewall₩pfirewall.log
10. 프리패치 활성화 7 | 10 | 08 | 12 | 16		
1. 레지스트리를 이용한 설정 HKLM₩SYSTEM₩CurrentControlSet₩Control₩Session Manager₩Memory Management₩PrefetchParameters₩EnablePrefetcher (REG_DWORD) : 0x00: 비활성화 : 0x01: 응용프로그램 프리패칭 활성화 : 0x02: 부트 프리패칭 활성화 : 0x03: 응용프로그램과 부트 프리패칭 활성화 (권장)	EnablePrefetcher : 0x03	%SystemRoot%₩Prefetch₩*.pf SSD 사용시 기능 본 항목 설정 금지 권장
11.NTFS 트랜잭션 로그 크기 설정 7 | 10 | 08 | 12 | 16		
1. 현재 로그 크기 확인 # chkdsk /L 2. 로그 크기 설정 # chkdsk /F /L:〈size〉 (size는 KB 단위)	# chkdsk /F /L:1048576 (1 GB 이상)	%SystemDrive%₩$LogFile
12. NTFS 변경 로그 크기 설정 7 | 10 | 08 | 12 | 16		
1. 현재 로그 크기 확인 # fsutil usn queryjournal 〈volume〉 2. 로그 크기 설정 # fsutil usn createjournal m=〈maxsize〉 a=〈allocationdelta〉 〈volume〉	# fsutil usn createjournal m=4294967296 a=4194304 c: (4 GB 이상, 모든 볼륨에 적용)	%SystemDrive%₩$Extend₩$UsnJrnl:$J
13. 시스템 복원 설정 7 | 10 | 08 | 12 | 16		
1. 제어판을 이용한 설정 08 12 16 : 시작 프로그램, 관리 도구 ▶ Windows Server 백업 ▶ 백업 일정 (윈도우 서버는 다음 위치에서 기능 설치후 설정 가능 : 시작 프로그램 ▶ 서버 관리자 ▶ 기능 추가 ▶ Windows Server 백업 기능) 7 10 : 제어판 ▶ 시스템 속성 ▶ 시스템 보호 ▶ 볼륨 선택, 구성 ▶ 복원 설정, 디스크 공간 사용	시스템 설정 및 이전 버전 파일 복원 (체크) 디스크 공간 사용 : 20GB 이상으로 설정	%SystemDrive%₩System Volume Information

☞ 상기 설정은 각 윈도우 순정버전에서 테스트되었으며 OS 세부 버전에 따라 달라질 수 있습니다.

범례

OS : 별도 설치, 설정이 필요없는 항목
OS : 별도 설치, 설정이 필요한 항목

: 윈도우 제품군
: 윈도우 서버 제품군

7 : Windows 7 Ultimate K 6.1.7601
10 : Windows 10 Enterprise K 10.0.10240
08 : Windows Server 2008 SP2 Datacenter 6.0.6002
12 : Windows Server 2012 R2 Standard 6.3.9600
16 : Windows Server 2016 Standard 10.0.14393
log : %SystemRoot%₩System32₩Winevt₩Logs₩