

Windows Troubleshooting Guide

- Windows 장애 유형.....2
 - 1. 유형1) 블루스크린(BSOD) 발생 후 재부팅.....2
 - 2. 유형2) 동작 중 시스템 멈춤(Hang) 발생.....2
 - 3. 유형3) 사용 중 느려지는 문제 (CPU Usage 증가).....3
 - 4. 유형4) 사용 중 메모리 증가 문제 (메모리 누수).....3
 - 5. 유형5) 부팅 중 시스템 멈춤(Hang).....3
- 커널 메모리 덤프(Kernel Memory Dump) 수집 가이드.....4
- 키보드를 이용한 강제 메모리 덤프 생성.....8
 - 1. Regedit(레지스트리 편집기)를 실행.....8
 - 2. USB 키보드 설정 방법.....9
 - 3. PS2 키보드 설정 방법.....10
 - 4. 덤프 생성.....10
- 성능모니터 데이터수집.....11

Windows Troubleshooting Guide

● Windows 장애 유형

유형1)~4)는 대표적인 디버깅 방법입니다. 마지막 유형5는 Rare한 유형입니다.

유형 1)~4)에 대한 디버깅 방법을 이용해 1차 원인 분석을 진행합니다.

추가 분석이 필요한 경우 세부 내용에 따라 추가 로그 수집이 필요합니다

한번에 모든 로그를 수집하는 방법은 없습니다. 1차 원인 분석으로 원인을 파악할 수도 있고 추가 디버깅이 필요할 수 있습니다. 이유는 Windows 서버는 넉넉한 자원으로 많은 프로세스가 동작하는 시스템입니다. 모든 프로세스에 대한 디버깅 로그를 남기는 것은 불가능합니다. 로그는 시스템 성능에 영향을 줍니다. Windows 디버깅은 분석에 따라 디버깅 계획이 변경됨을 이해 부탁드립니다.

1. 유형1) 블루스크린(BSOD) 발생 후 재부팅

블루스크린 발생시 메모리 덤프를 통해서 디버깅을 합니다. 메모리 덤프 유형에는 전체 메모리 덤프, 커널 메모리 덤프, 활성 메모리 덤프 등이 존재합니다. 서버에는 커널 메모리 덤프를 설정을 추천 드립니다. 커널 메모리 덤프는 커널 영역 메모리를 MEMORY.DMP로 압축하게 됩니다.

블루스크린 발생후 재부팅 이슈는 95%이상이 커널 드라이버에서 문제가 발생합니다. 커널 메모리 덤프로 원인 분석이 가능합니다.

아래 [커널 메모리 덤프 설정]방법으로 설정하기를 추천 드립니다.

2. 유형2) 동작 중 시스템 멈춤(Hang) 발생

동작 중 시스템 멈춤 발생시 메모리 덤프를 통해서 디버깅을 합니다.

시스템 멈춤의 경우 Windows logon수행중 Hang될 수 있는데 이때는 전체 메모리 덤프가 필요할 수 있습니다. 그 외 시스템 멈춤의 경우 커널 메모리 덤프로 가능합니다.

시스템 멈춤 발생시 강제 메모리 덤프를 생성할 수 있습니다.

아래 [커널 메모리 덤프 설정]방법으로 설정하기를 추천 드립니다.

오른쪽 Ctrl 키를 누른 상태에서 Scroll Lock 키 두번 입력 시 강제 메모리 덤프가 생성됩니다.

3. 유형3) 사용 중 느려지는 문제 (CPU Usage 증가)

사용 중 느려지는 문제의 경우 성능모니터 로그를 수집 필요합니다.

성능모니터는 Runtime에 Process가 사용하는 성능로그를 실시간 수집합니다.

성능모니터 수집 시작하고 느려지는 문제가 재연된 후 수집 종료된 로그가 필요합니다.

수집되는 동안 반드시 문제가 재연되어야 합니다.

문제가 발생하면 **[성능모니터 수집]** 대로 수집하기를 추천 드립니다.

4. 유형4) 사용 중 메모리 증가 문제 (메모리 누수)

사용 중 메모리 증가하는 문제의 경우 성능모니터 로그를 수집 필요합니다.

성능모니터 수집을 시작하고 메모리 증가하는 문제가 재연된 후 수집 종료된 로그가 필요합니다.

메모리 증가 패턴을 확인해야함으로 24시간에서 120시간정도 수집이 필요합니다.

수집되는 동안 반드시 문제가 재연되어야 합니다.

문제가 보인다면 **[성능모니터 수집]** 대로 수집하기를 추천 드립니다.

5. 유형5) 부팅 중 시스템 멈춤(Hang)

부팅 중 시스템 멈춤 유형은 흔하지 않은 케이스입니다. 디버깅 방법이 까다롭습니다.

이 경우 먼저 멈춰 있는 화면 사진을 공유주시면 좋습니다. 재연조건이 있다면 찾는 것이 중요합니다. 재연빈도가 얼마나 되는지 확인 필요합니다.

[커널 메모리 덤프 설정]이 되어 있다면 강제 메모리 덤프 생성 시도하여 메모리 덤프가 생성되는지 확인 필요합니다. 메모리 덤프가 생성 안 된 경우 설치된 3rd party 드라이버를 삭제하고 문제가 나오는지 확인 필요합니다.

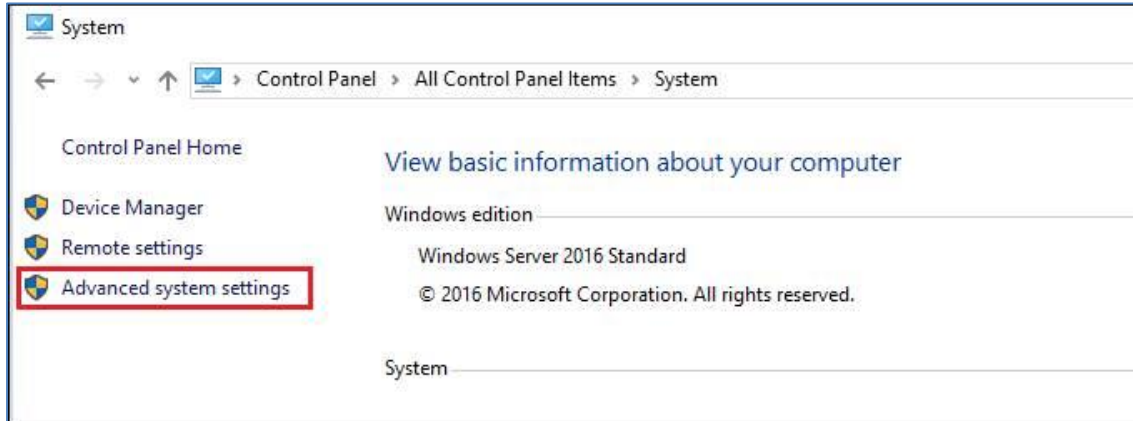
라이브 디버깅을 활성화하고 재연하여 디버깅이 필요합니다.

아래 **[커널 메모리 덤프 설정]** 방법으로 설정하기를 추천 드립니다. 멈춰진 화면의 사진이 필요합니다.

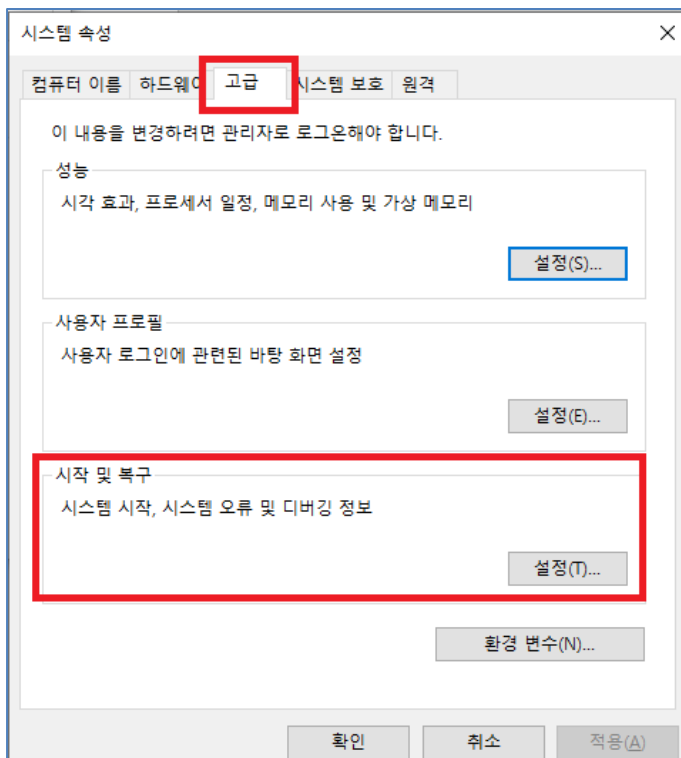
오른쪽 Ctrl 키를 누른 상태에서 Scroll Lock 키 두 번 입력시 강제 메모리 덤프 생성 시도해주세요.

● 커널 메모리 덤프(Kernel Memory Dump) 수집 가이드

1. 제어판(Control panel) – 시스템(System) - 시스템 고급 설정(Advanced system settings)을 클릭
(또는 실행 - **sysdm.cpl**)

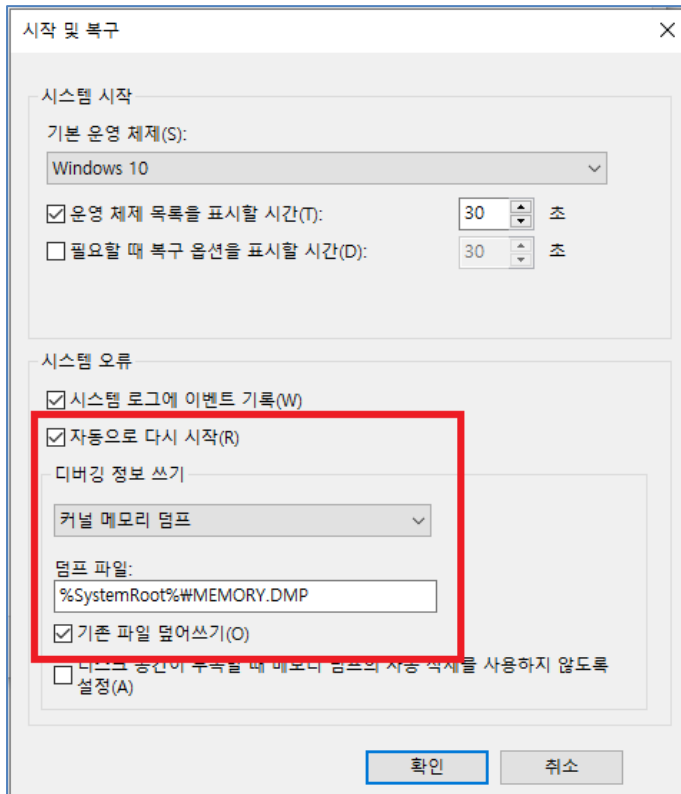


2. 고급(Advanced) 탭 – 시작 및 복구 설정(Startup and Recovery) - 설정(Settings)버튼 클릭

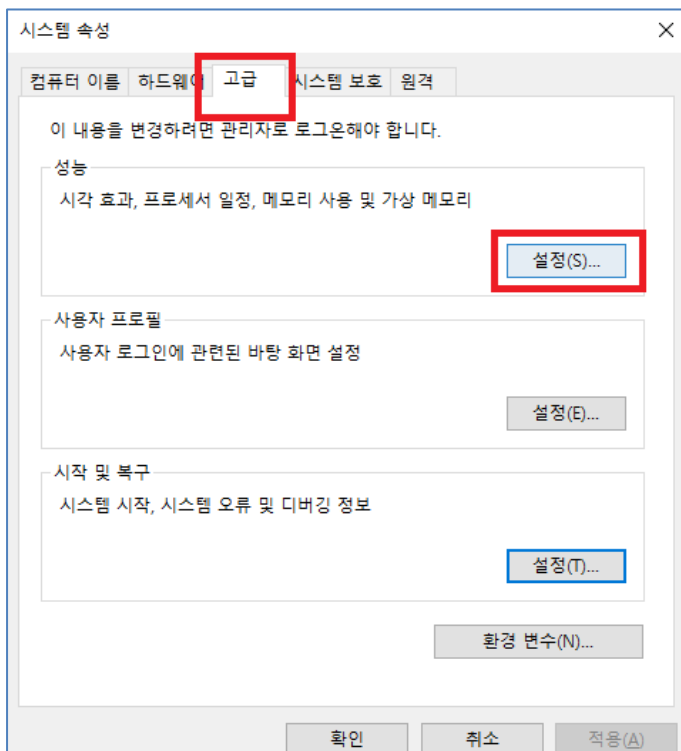


3. "자동으로 다시 시작 옵션(Automatically restart)"은 check 합니다.
4. "디버깅 정보 쓰기(Write debugging information)"는 "커널 메모리 덤프(Kernel memory dump)"로 설정합니다.

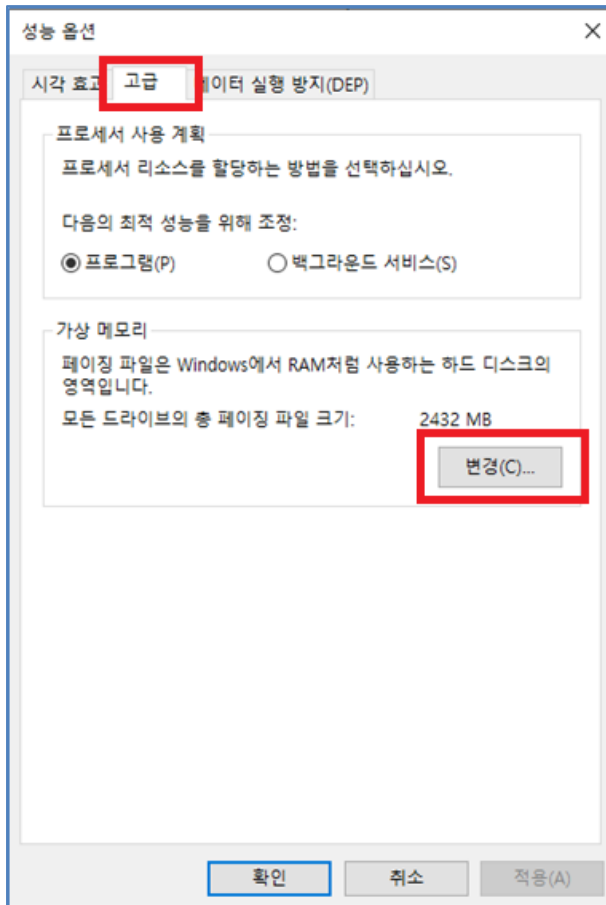
5. "기존 파일 덮어쓰기(Overwrite any existing file)"는 check 합니다.



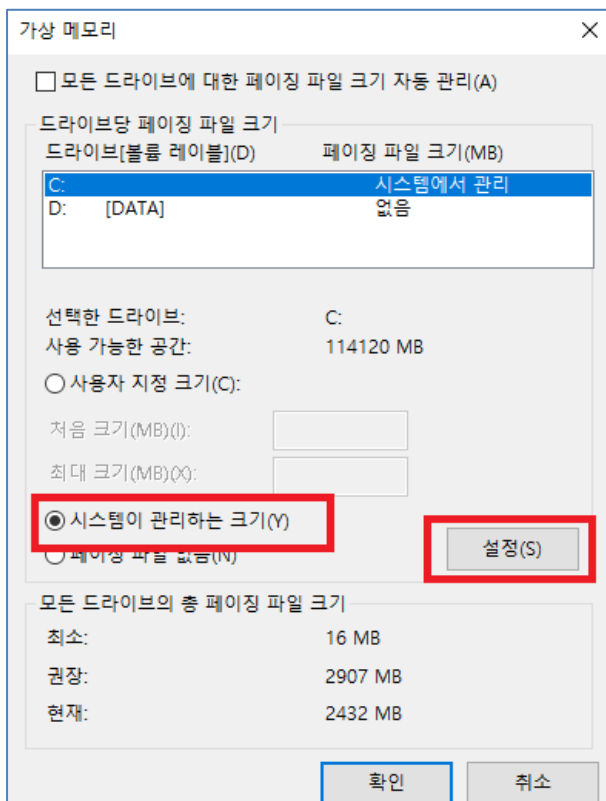
6. 제어판(Control panel) – 시스템(System) - 시스템 고급 설정(Advanced system settings) – 고급 (Advanced) 탭 – 성능(Performance) – 설정(Settings) 버튼을 클릭합니다.



7. 성능 옵션 - 고급(Advanced) 탭 - 가상 메모리(Virtual memory)에서 변경을 클릭합니다.

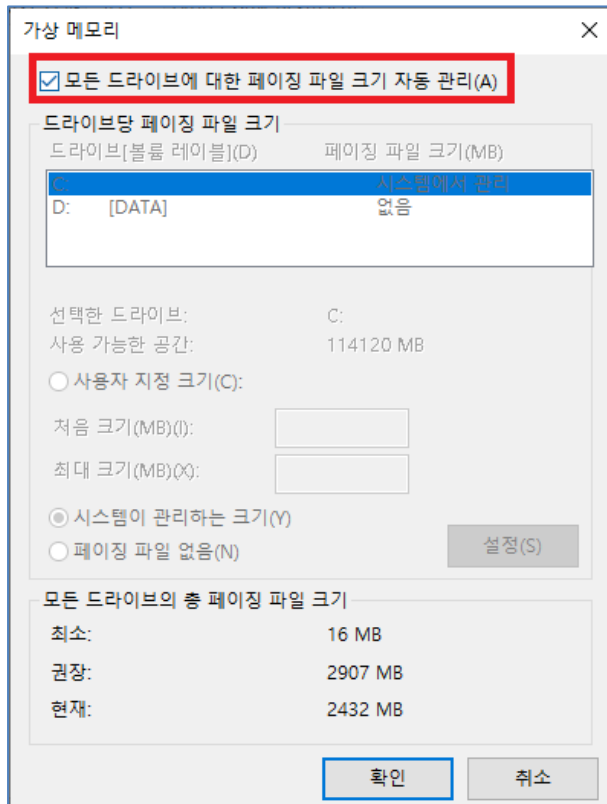


8. 시스템이 관리하는 크기(System managed size) check - "설정(Set)"



9. 모든 드라이브에 대한 페이징 파일 크기 자동 관리를 check – 확인(OK)

(Automatically manage paging file size for all drivers)



10. (Option) 8번의 페이징 파일을 사용자 지정 크기로 사용하려면,

최소 크기 – 물리 메모리 보다 크게 설정

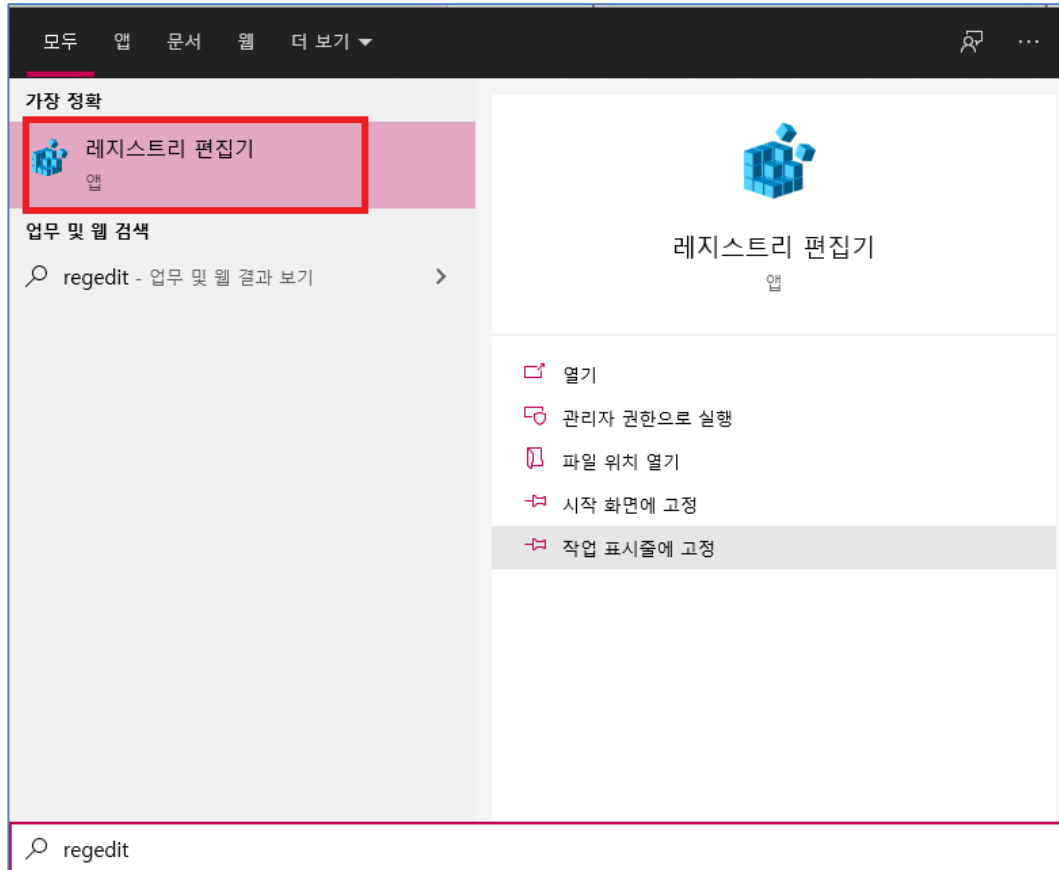
Ex) 실제 4G RAM이 장착된 경우, 최소 크기는 4096MB 이상 설정

11. 시스템을 재시작 합니다.

12. 하드웨어 제조사에서 제공하는 Automatic System Recovery (ASR) 기능이 Enable 되어 있다면 이 기능을 Disable 해 주세요. 이 설정에 대한 가이드가 필요하시다면 사용하고 계시는 하드웨어 제조사에 문의해 주세요.

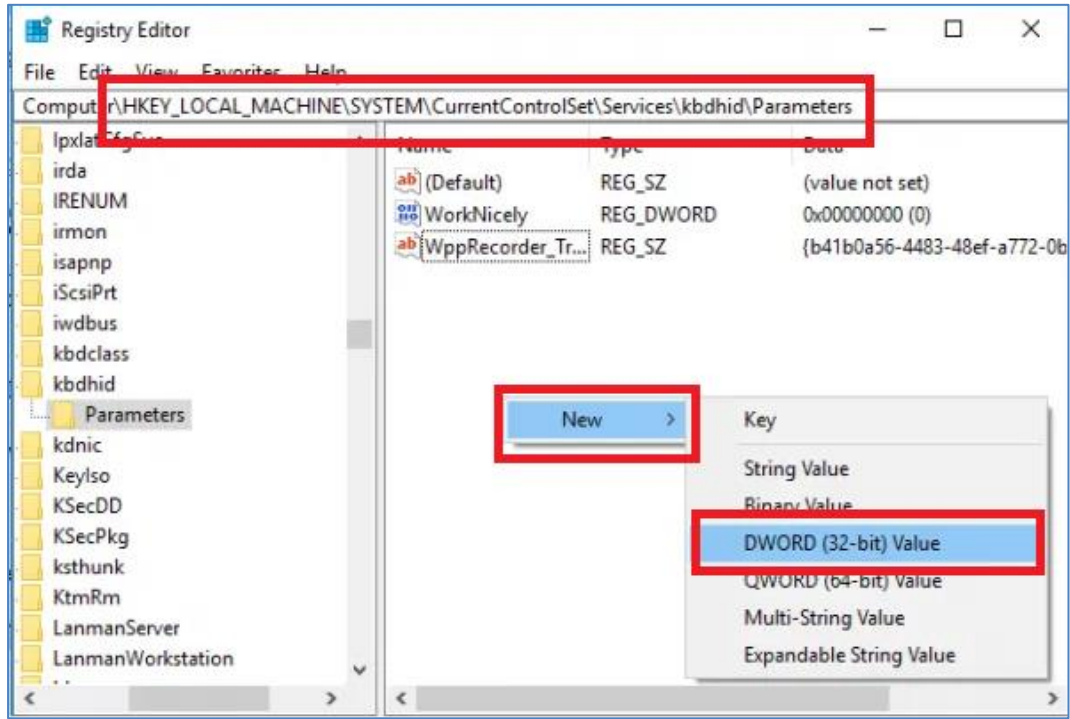
● 키보드를 이용한 강제 메모리 덤프 생성

1. Regedit(레지스트리 편집기)를 실행

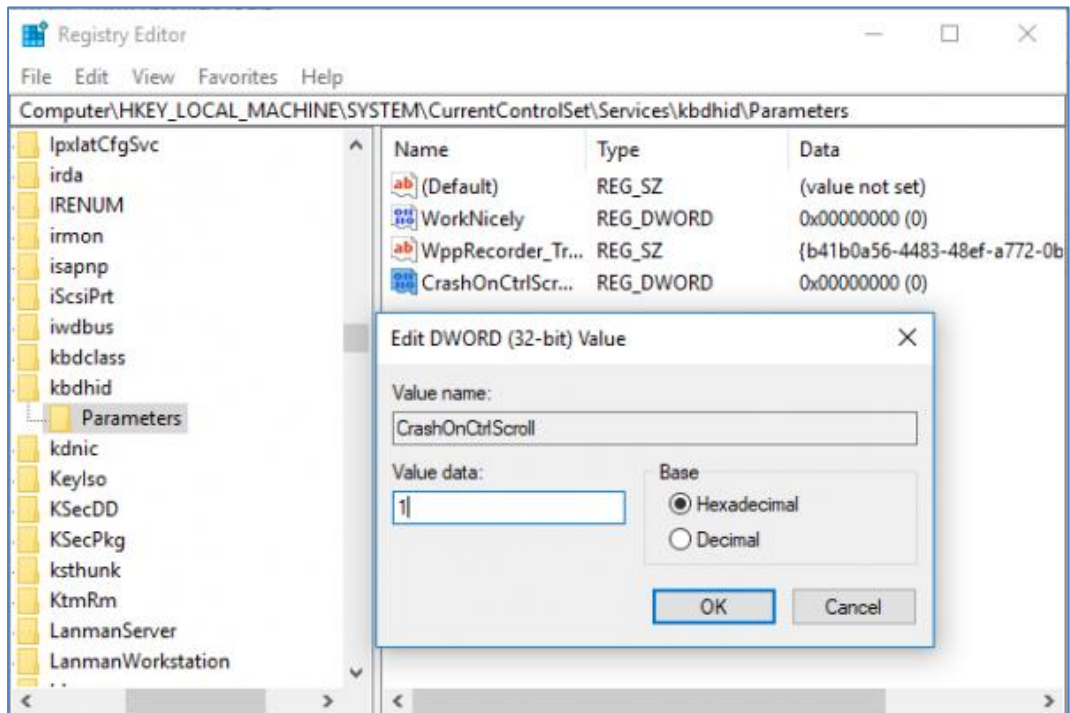


2. USB 키보드 설정 방법

- A. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kbdhid\Parameters 이동
- B. 새로 만들기 - DWORD(32비트) 값 생성



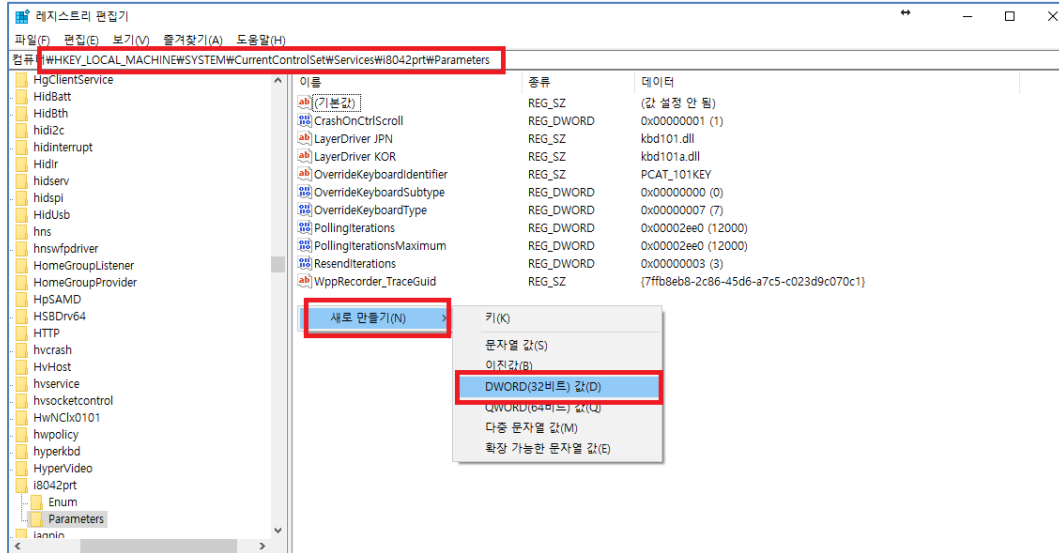
- C. "CrashOnCtrlScroll" 값을 "1"로 설정



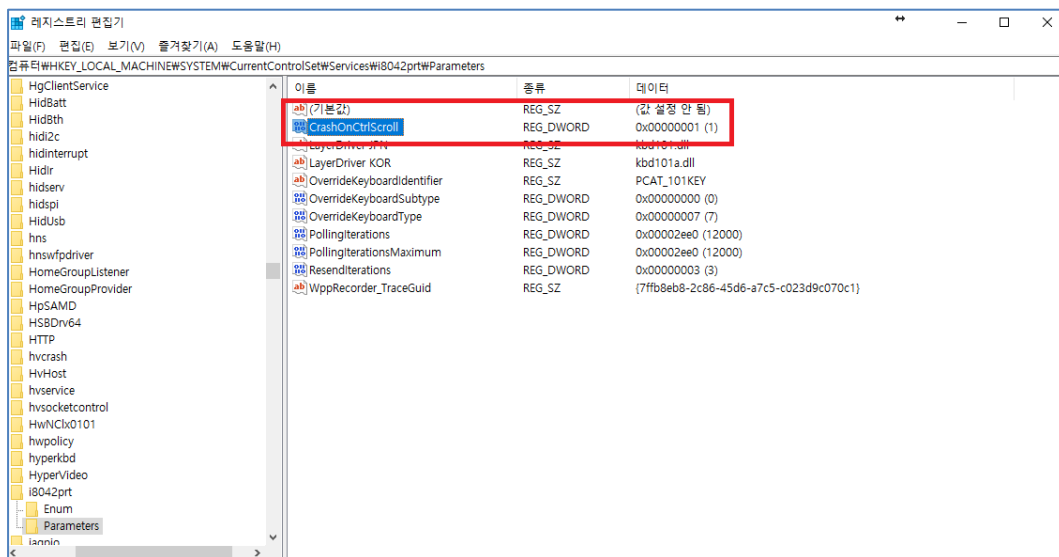
3. PS2 키보드 설정 방법

A. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W8042prt\Parameters

B. 새로 만들기 - DWORD(32비트) 값 생성



C. "CrashOnCtrlScroll" 값을 "1"로 설정



Note:

문제 발생시 덤프를 생성하기 위해 오른쪽 Ctrl 키가 있는 PS/2 키보드나 USB 키보드를 컴퓨터에 직접 연결해 놓아야 합니다

4. 덤프 생성

덤프 수집이 필요할 때 해당 연결된 키보드의 **오른쪽 Ctrl 키를 누른 상태에서 Scroll Lock 키를 두 번 눌러 덤프를 강제 수집**합니다. 덤프 파일은 기본적으로 C:\Windows\MEMORY.DMP로 생성됩니다.

● 성능모니터 데이터수집

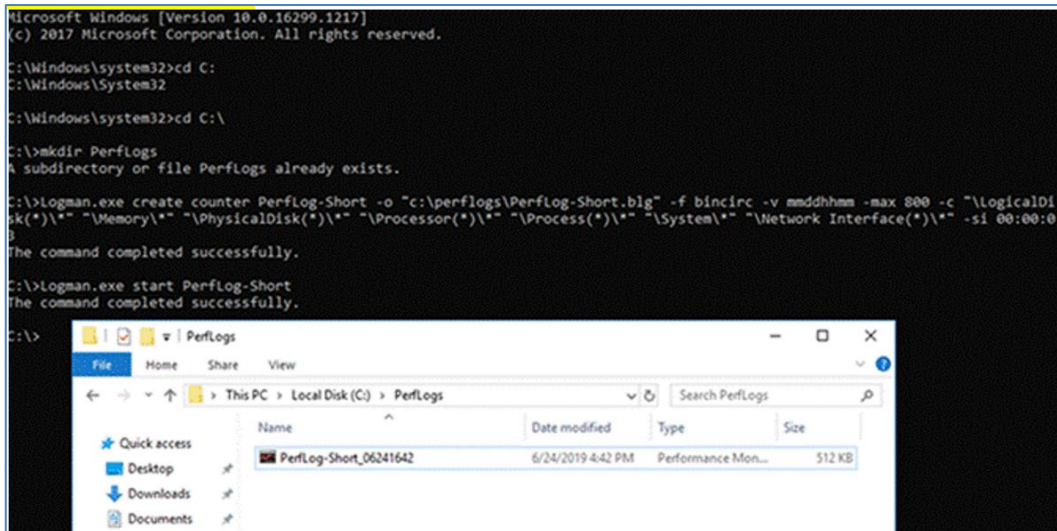
1. 명령창(cmd.exe)를 실행 (관리자 권한으로 실행합니다)
2. C:\W 드라이브에 C:\WPerfLogs폴더를 생성합니다.
3. 현재 서버 상태에서 다음 명령을 Copy and Paste하여 명령 실행창에 실행합니다. 그러면 Perfmon에PerfLog-Short라는 Counter를 생성합니다. Success메시지가 출력 안되면 **Logman.exe delete PerfLog-Short**를입력하고 다음 명령을 다시 Copy and Paste해주세요.

[명령어]

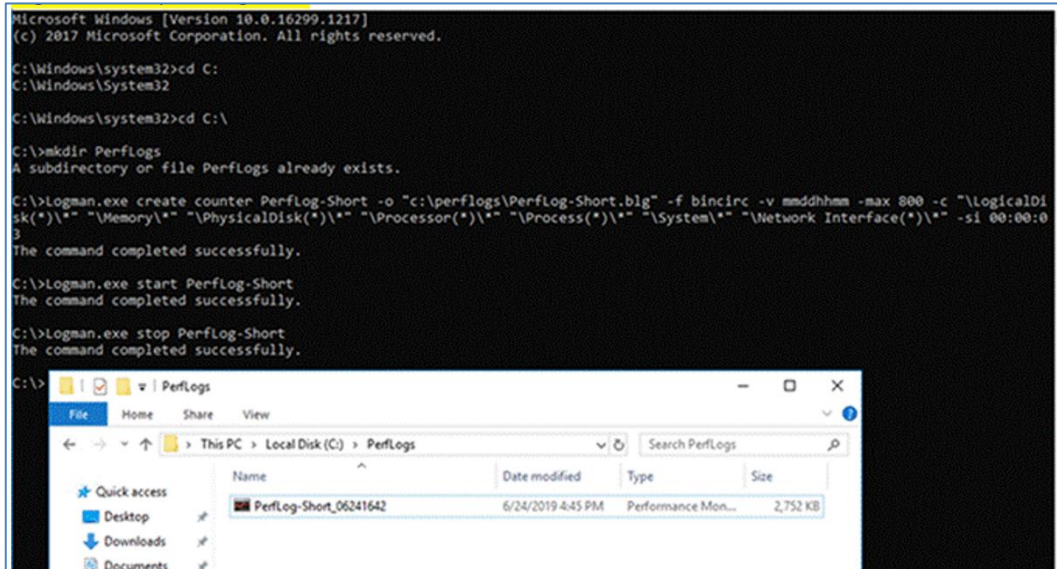
```
Logman.exe create counter PerfLog-Short -o "c:\perflogs\PerfLog-Short.blg" -f bincirc -v mmdhmm -max 950 -c "\\LogicalDisk(*)\\*" "\\Memory\\*" "\\PhysicalDisk(*)\\*" "\\Processor(*)\\*" "\\Process(*)\\*" "\\System\\*" "\\Network Interface(*)\\*" -si 00:01:00
```

4. Log 수집을 시작하기 위해서는 다음을 실행합니다.

A. **Logman.exe start PerfLog-Short**



- B. 24시간 이상 수집 후 수집을 종료하기 위해서 다음을 명령 실행창(관리자권한)에서 실행합니다. Logman.exe stop PerfLog-Short



The screenshot shows a Windows command prompt window with the following commands and output:

```
Microsoft Windows [Version 10.0.16299.1217]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:
C:\Windows\System32>
C:\Windows\system32>cd C:\
C:\>mkdir Perflogs
A subdirectory or file Perflogs already exists.
C:\>Logman.exe create counter PerfLog-Short -o "c:\perflogs\Perflog-Short.blg" -f bincirc -v mdddhmm -max 800 -c "\LogicalDisk(*)\*" "\Memory\*" "\PhysicalDisk(*)\*" "\Processor(*)\*" "\Process(*)\*" "\System\*" "\Network Interface(*)\*" -si 00:00:03
The command completed successfully.
C:\>Logman.exe start PerfLog-Short
The command completed successfully.
C:\>Logman.exe stop PerfLog-Short
The command completed successfully.
```

Below the command prompt, a File Explorer window shows the contents of the C:\Perflogs directory:

Name	Date modified	Type	Size
PerfLog-Short_06241642	6/24/2019 4:45 PM	Performance Mon...	2,752 KB

- C. Log수집 종료 후 C:\PerfLogs에 로그가 생성됨을 확인할 수 있습니다.