iTEASY

[Windows Server 보안 설정 5가지 팁]

아이티이지
서비스 운영팀

- 목 차 -

♧ **문서 작성간에 테스트된 환경**

- Windows 2003 R2 Stendard 32bit / Windows 2008 R2 Enterprise 64bit

♧ **개요**

- 최근 게임 사이트, 포털 사이트 등 개인정보 유출사고가 빈번하게 일어나는 것을 알 수 있습니다. 이와 같은 보안사고는 주요 사이트뿐만 아니라 네트워크가 연결된 모든 서버는 공격 대상이 될 수 있습니다. 서버 보안에 각별한 관심이 필요합니다.

- 해당 문서는 OS 상에서 설정 가능한 보안 설정에 대한 내용을 기술하고 있으며, 서버 관리자 분들께서 서버 운영에 참고해 주시기 바랍니다.

1. 서버에서 실행되는 서비스 확인

- 서버에서 실행되는 서비스를 확인하고, 사용하지 않는 서비스는 사용하지 않는 것이 좋습니다. 서버 자원 소모뿐만 아니라, 사용하지 않는 서비스들을 통해 해킹의 위협에 노출될 수 있기 때문입니다.

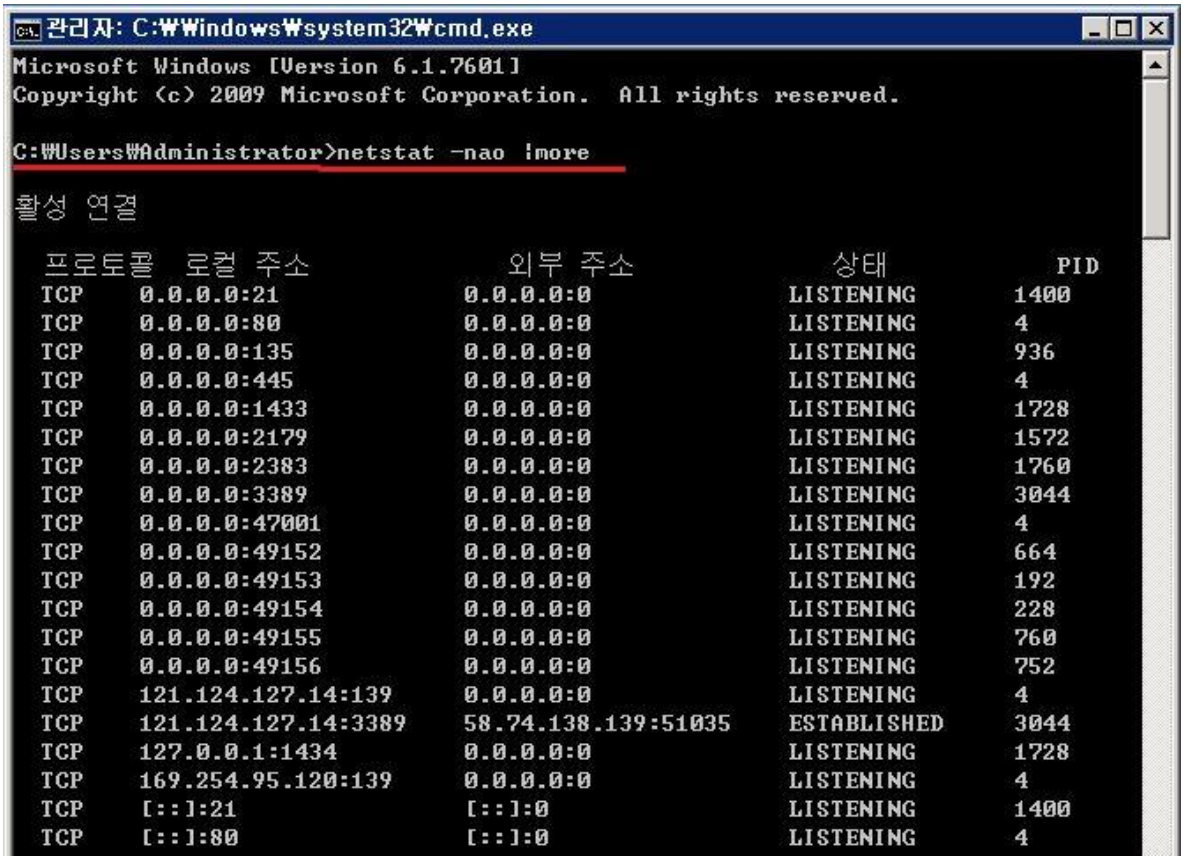
① 서비스 확인
: 아래 명령어를 통해 현재 서버에 Open 되어 있는 Port 확인

시작 > 모든 프로그램 > 보조 프로그램 > 명령 프롬프트 실행

또는
시작 > cmd [엔터]

※ Windows 2003 server 의 경우,
시작 > 실행 > cmd [엔터]

c:₩> netstat -nao



※ Open 되어있는 포트가 많을 경우, more를 이용하여 한 페이지씩 출력하여 볼 수 있습니다.

예시) c:₩> netstat -nao | more

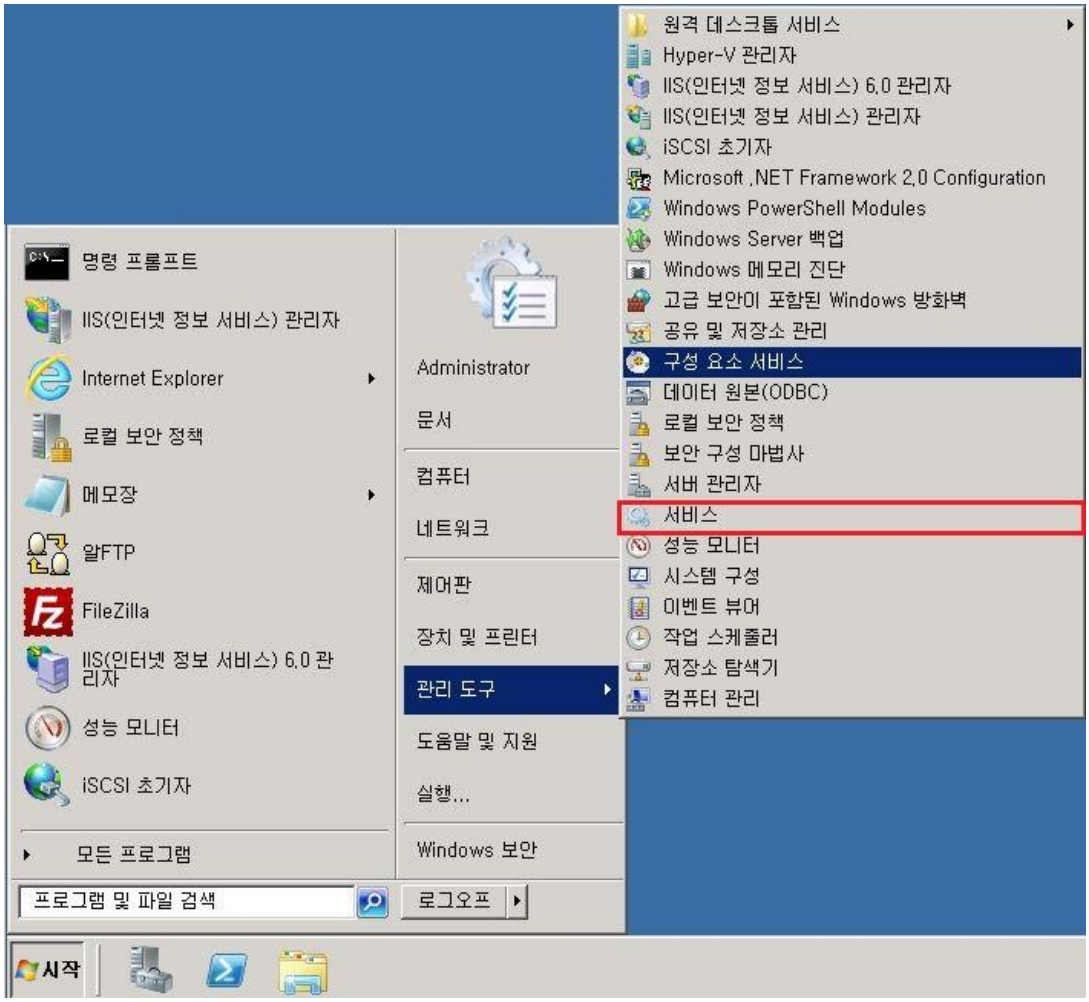
※ 서비스 별 포트 목록

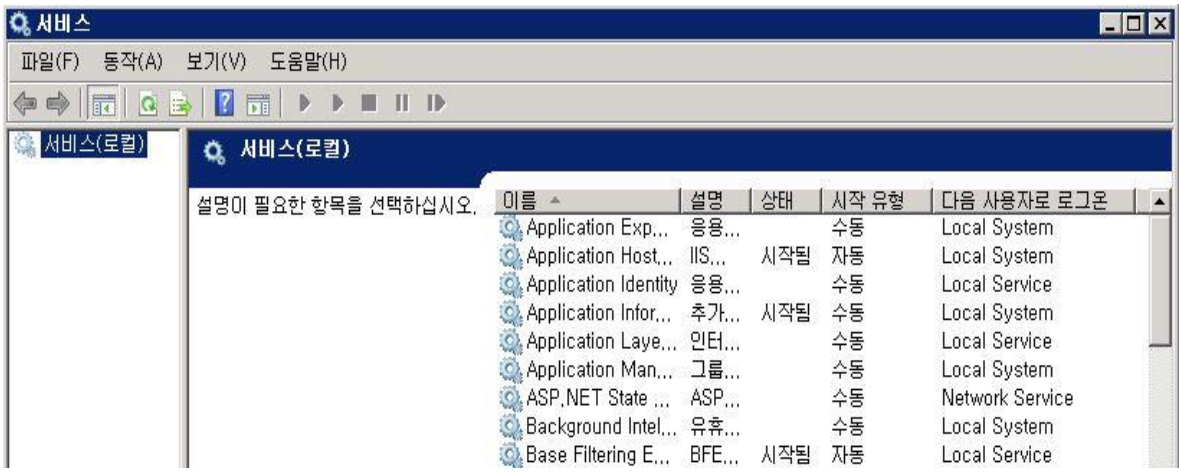
서비스명	기본 포트	서비스명	기본 포트
FTP	21	IMAP	143
SSH	22	MMS	554
TELNET	23	MSSQL	1433
SMTP	25 / 587	ORACLE	1521
DNS	53	MYSQL	3306
HTTP	80	RDP	3389
POP3	110	TOMCAT	8080
HTTPS	443		

② 부팅시 불필요 서비스 실행 방지

: 사용하지 않는 서비스가 있으실 경우, 서버가 부팅될 때 실행되지 않도록 하는 것이 좋습니다.

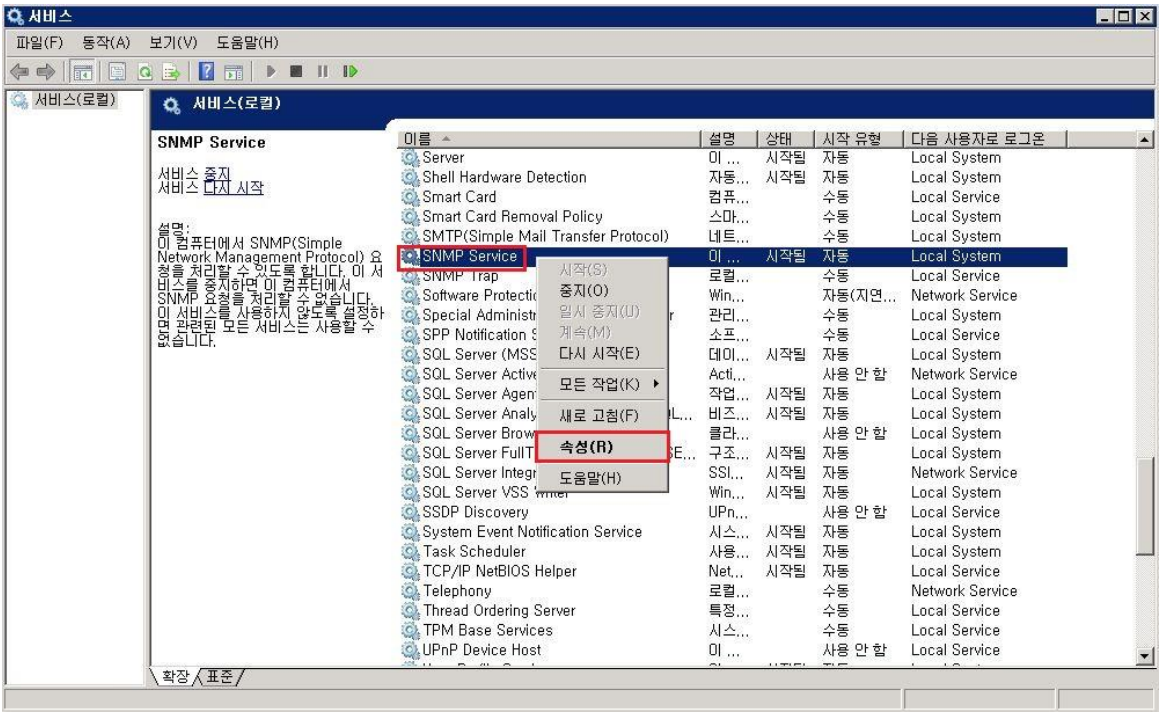
시작 > 모든 프로그램 > 관리 도구 > 서비스



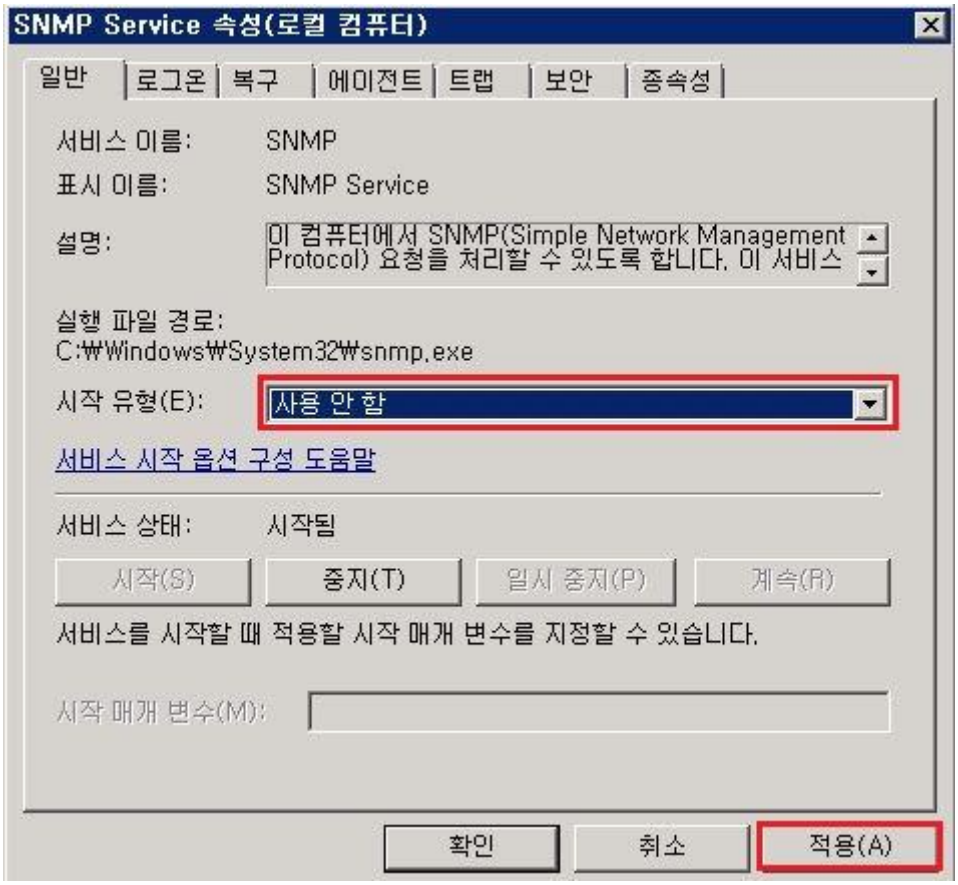


예시) snmp 서비스 중지

서비스 > snmp services [마우스 우클릭] > 속성



Snmp 서비스 속성 > 일반 > 시작 유형 > "사용 안 함"으로 변경

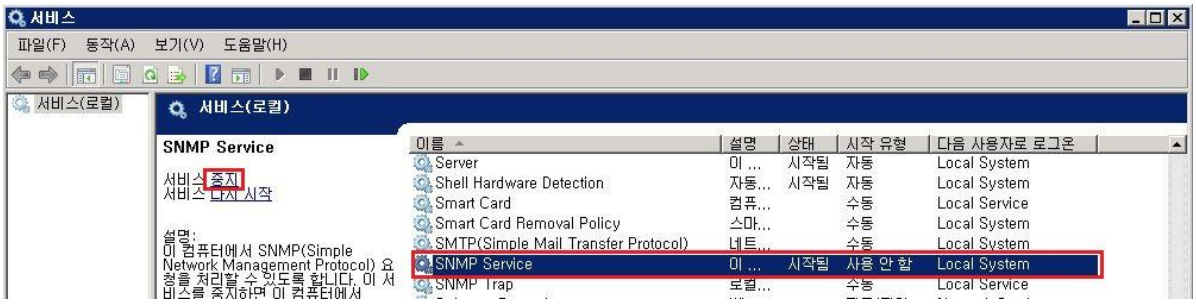


③ 서비스 종료

: 사용하지 않는 프로그램 종료

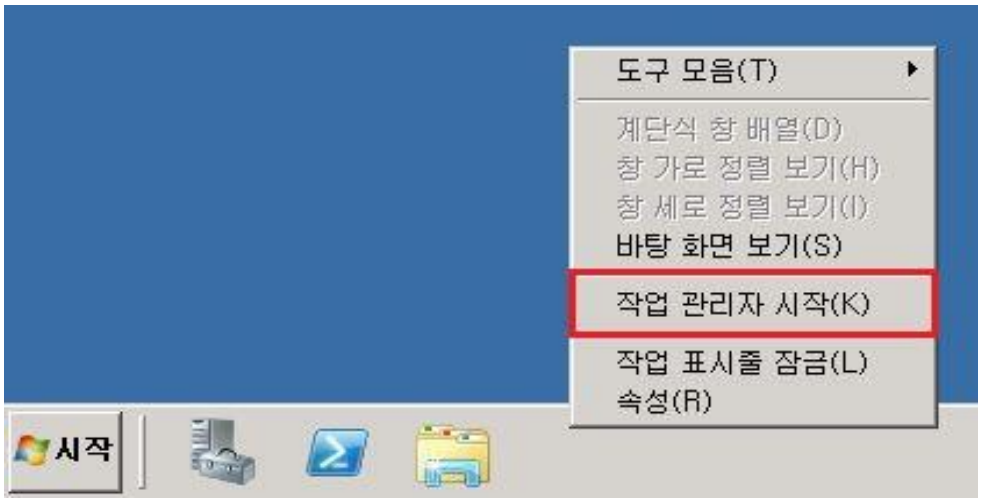
서비스 > [서비스 명] > 중지

예시) 서비스 > snmp services > 중지

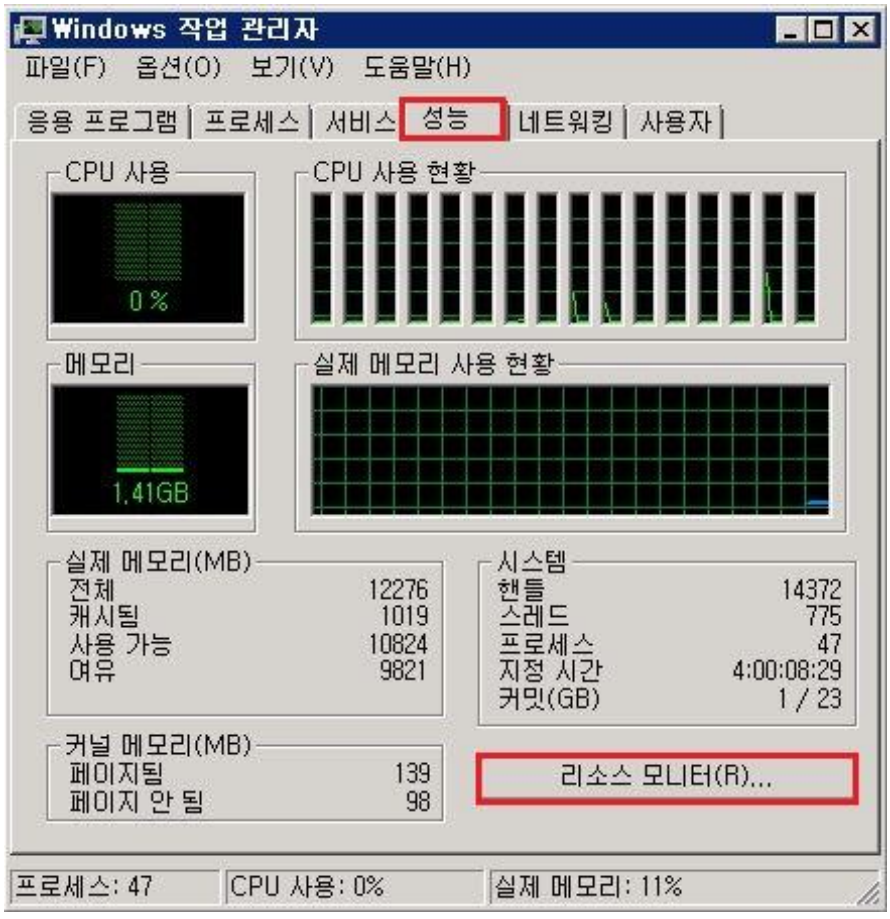


[TIP] 시스템 성능 부하 및 리소스 모니터링

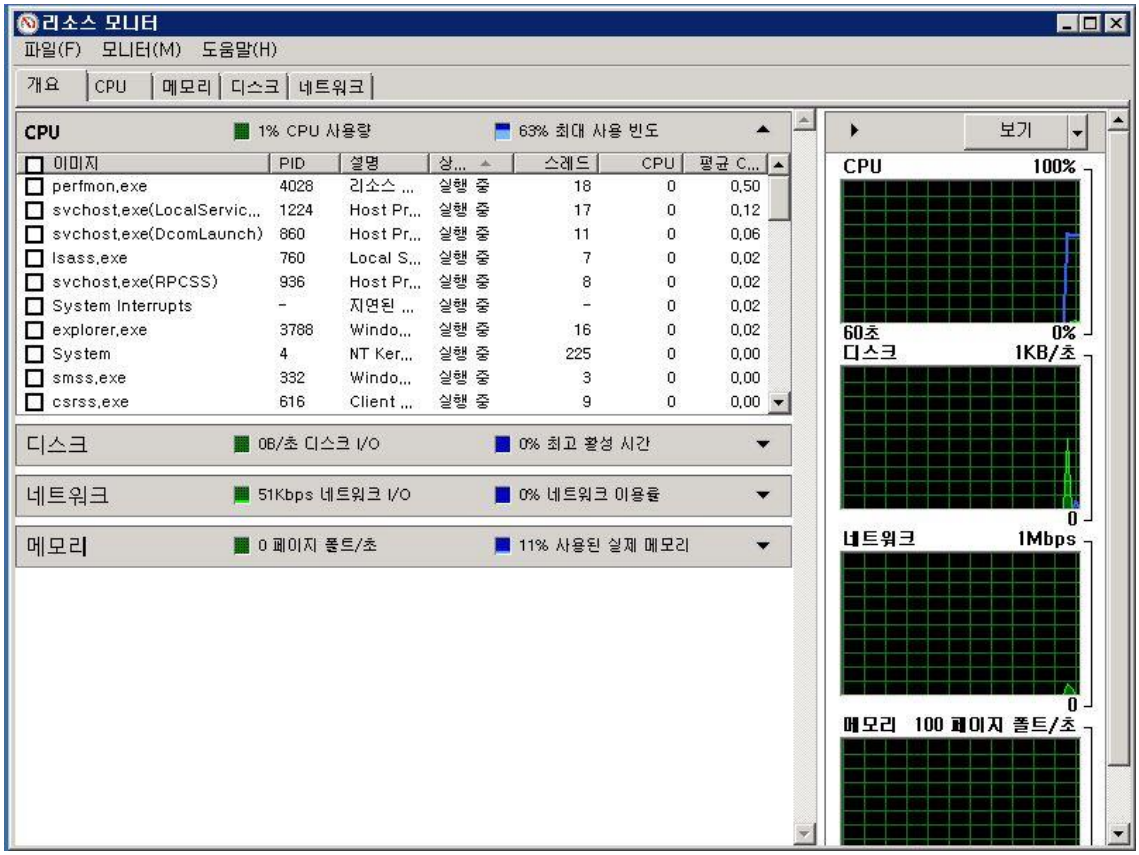
작업 창 [마우스 우클릭] >작업관리자 시작



Windows 작업 관리자 > 성능



Windows 작업관리자 > 성능 > 리소스 모니터



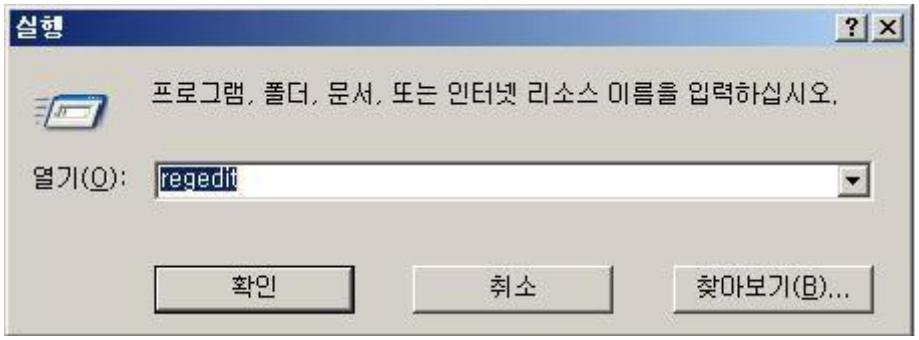
2. 원격 터미널 접속(RDP) 보안

- RDP(Remote Desktop Protocol) 이란, 마이크로소프트 (Microsoft)에서 Windows NT와 Windows CE가 서로 통신하기 위해 만든 프로토콜 입니다.

① 원격 터미널 포트 변경
: 기본적인 원격 터미널 포트는 3389이지만, 반드시 해당 포트를 사용할 필요는 없습니다. 기본 포트로 무차별 대입법 등을 통해 접속 시도가 발생할 수 있기 때문에 포트를 변경하여 임의 포트로 변경하여, 포트 노출을 예방하는 것이 좋습니다.
: 레지스트리 파일을 변경하는 부분으로 설정 후, 시스템을 재부팅 해야 만 적용됩니다.

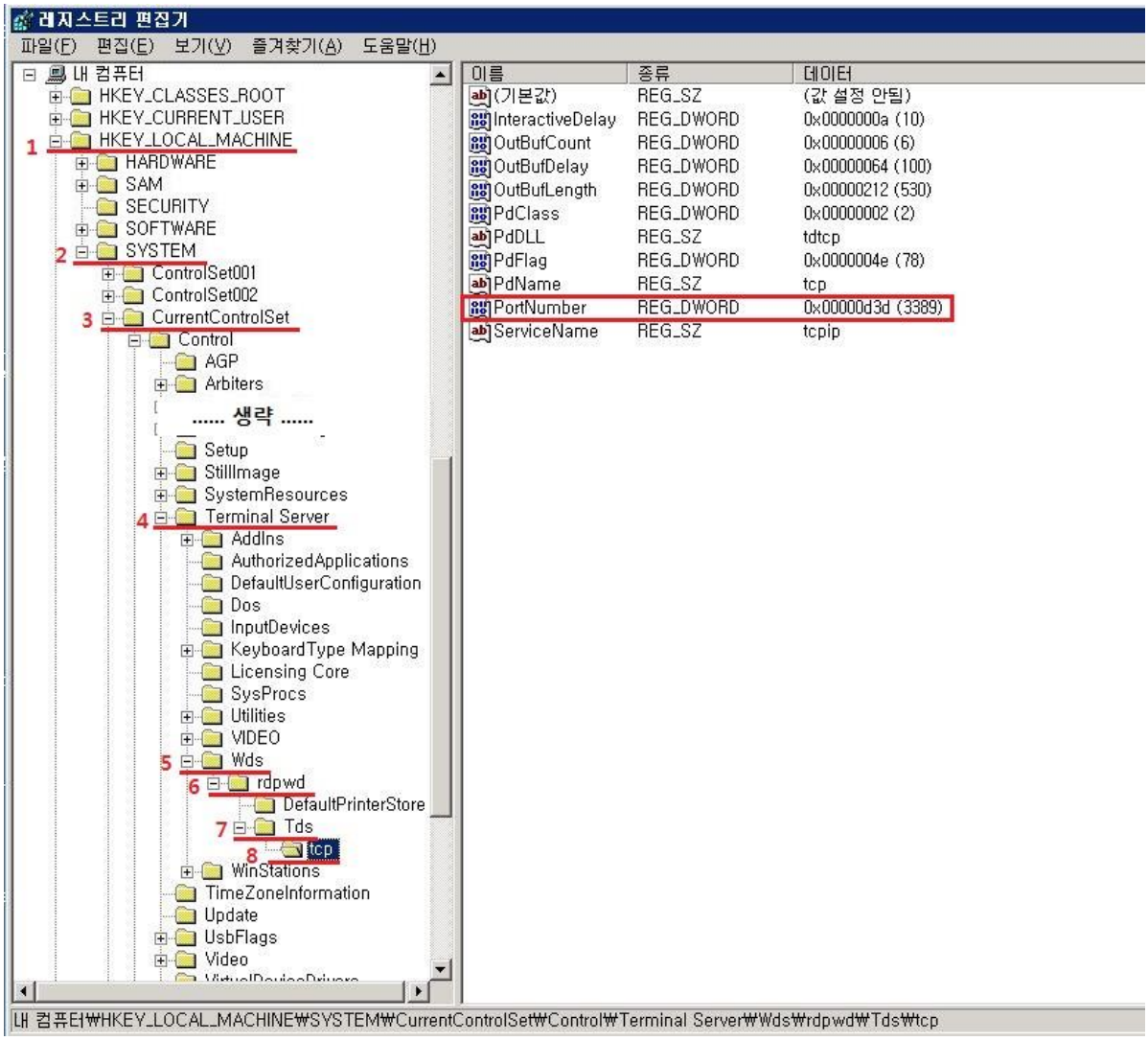
< Windows Server 2003 >

시작 > 실행 > regedit

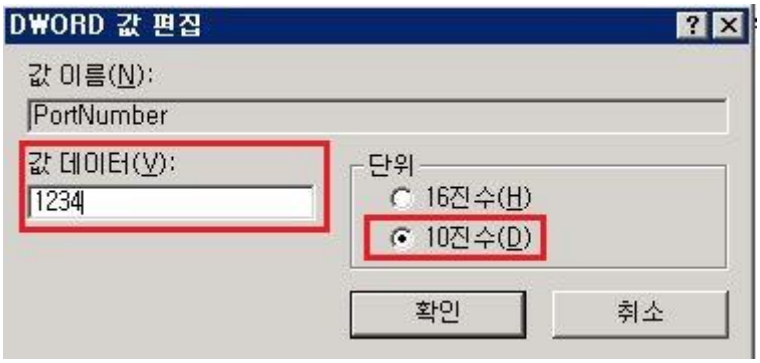


레지스트리 편집기에서 아래 경로의 PortNumber값을 3389에서 임의 값을 변경합니다. Windows 2003 Server에서는 두 개의 레지스트리 값을 변경하셔야 합니다.

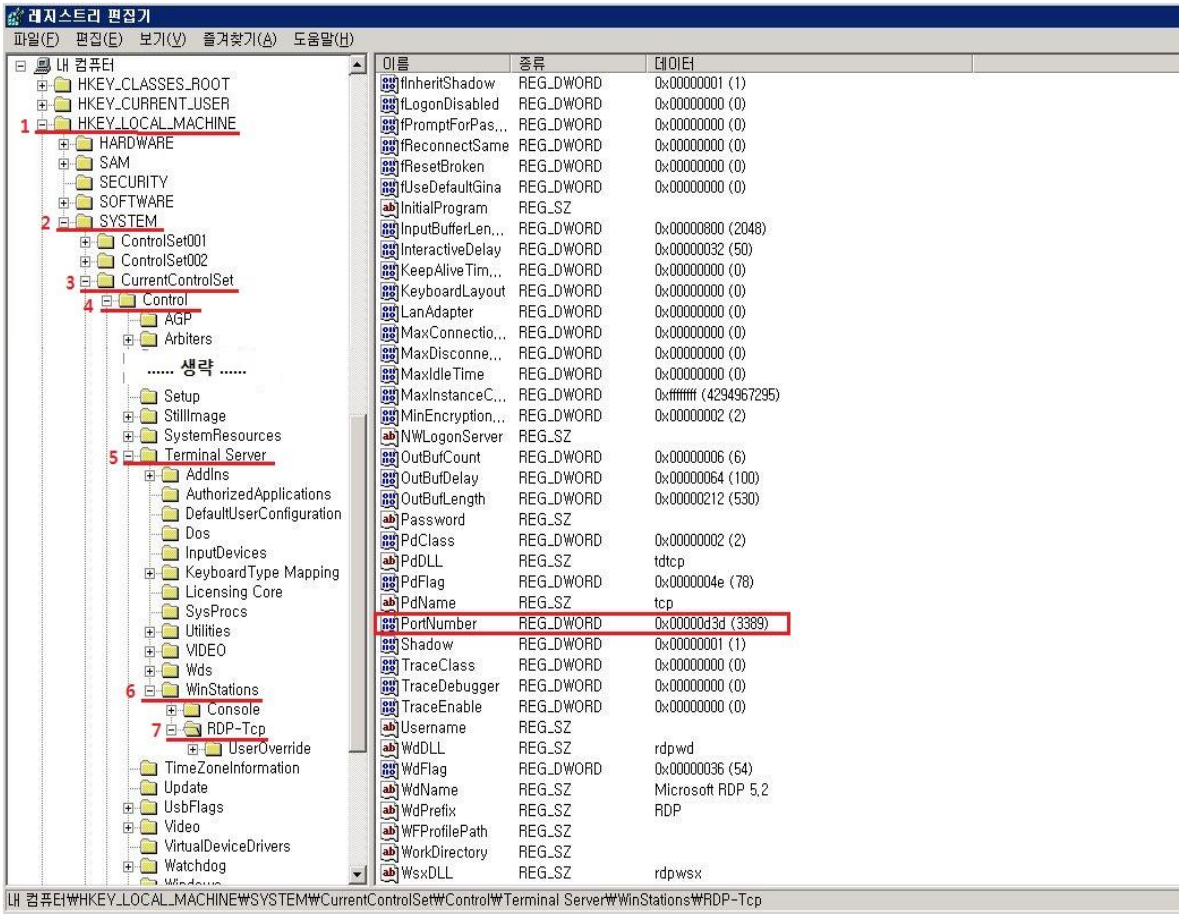
➢ HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩Terminal Server₩Wds₩rdpwd₩Tds₩tcp



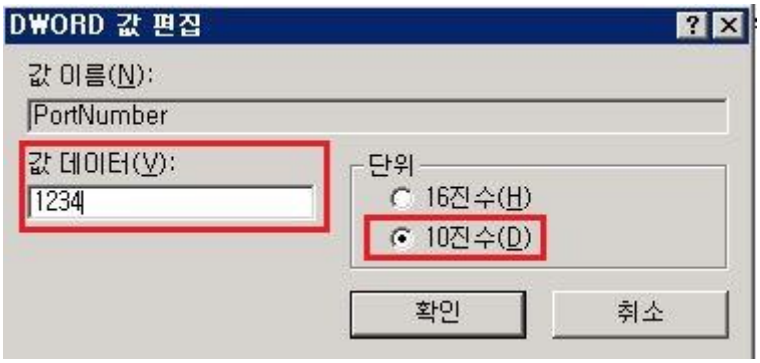
PortNumber 의 단위를 10진수로 변경한 뒤 임의 값으로 지정합니다.



➢ HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩Terminal Server₩WinStations₩RDP-Tcp



PortNumber 의 단위를 10진수로 변경한 뒤 임의 값으로 지정합니다.

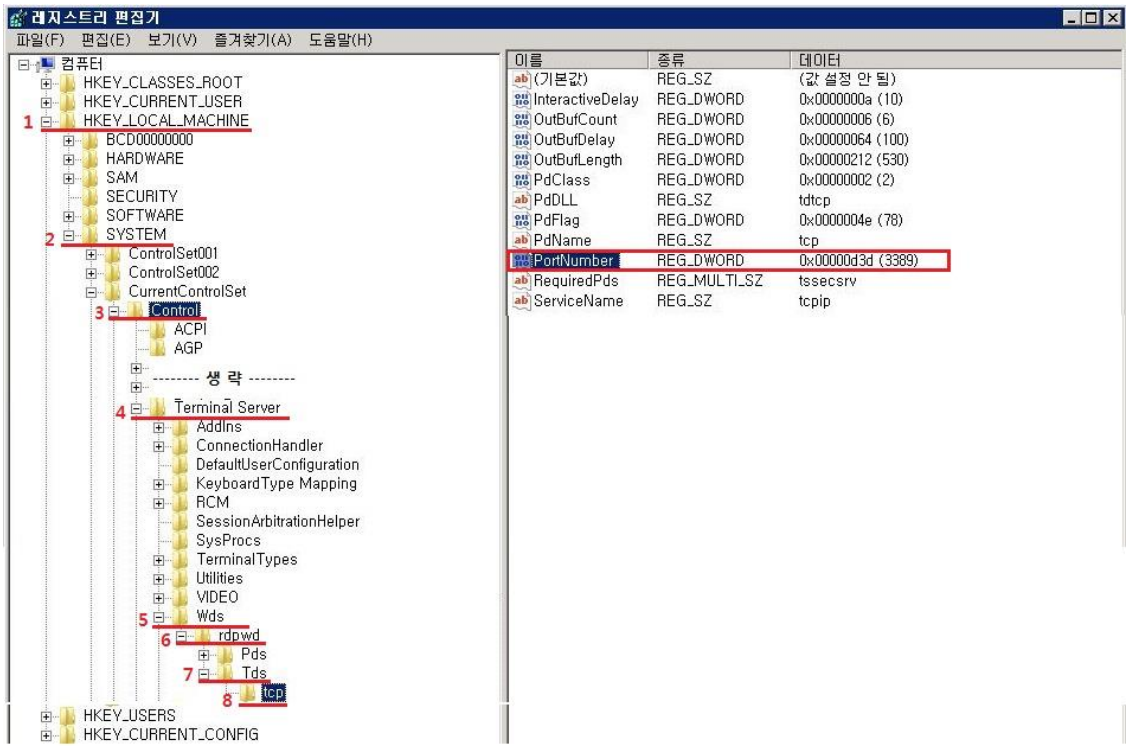


< Windows Server 2008 >

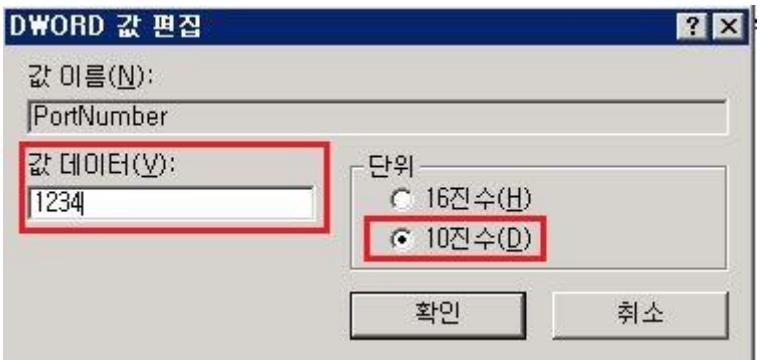
시작 > regedit

레지스트리 편집기에서 아래 경로의 PortNumber 값을 3389에서 임의 값으로 변경합니다.

➢ HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩Terminal Server₩Wds₩rdpwd₩Tds₩tcp

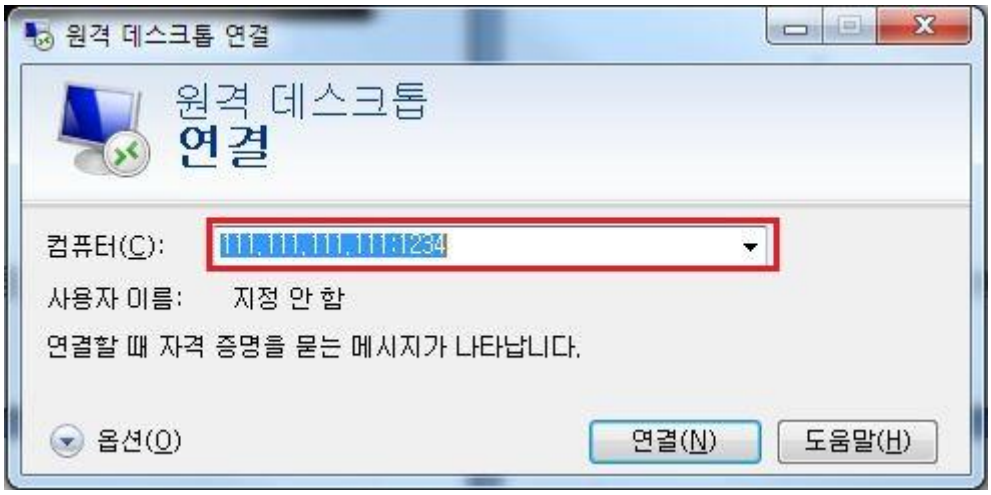


PortNumber 의 단위를 10진수로 변경한 뒤 임의 값으로 지정합니다.



원격 터미널 접속 포트를 임의 값으로 변경하셨을 경우, PC에서 원격 접속 시 아래와 같이 IP 뒤에 임의 포트를 지정하여 연결하셔야 합니다.

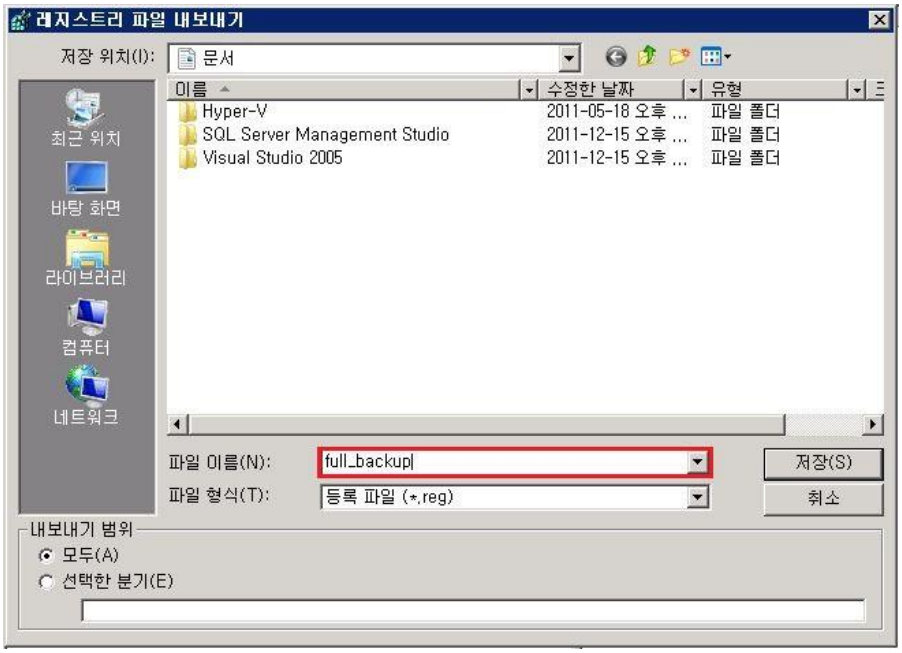
예시) 111.111.111.111:1234



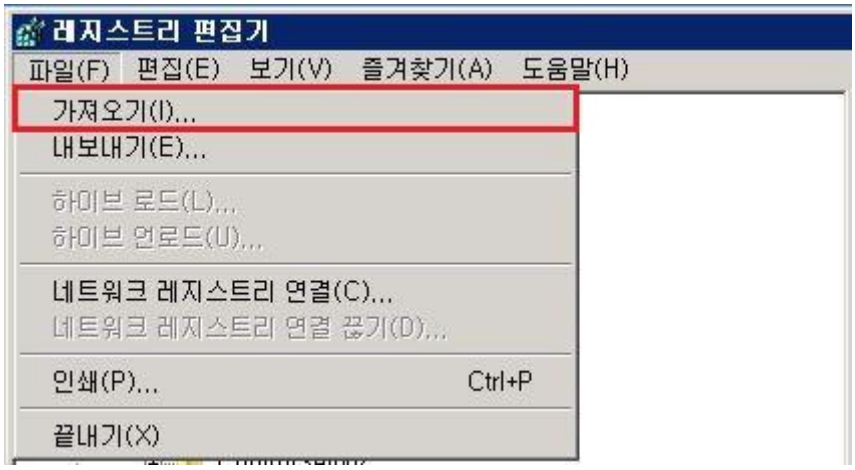
[TIP 레지스트리 백업]

레지스트리 편집기 > 파일 > 내보내기

레지스트리를 백업할 경로 및 파일 명을 지정한 뒤 저장 버튼을 클릭합니다.



※ 레지스트리 복구는 반대로 백업된 파일을 "가져오기" 하시면 되십니다.



※ 레지스트리 변경 작업의 경우, 잘못 편집 시 시스템에 심각한 손상을 줄 수 있이 때문에 작업 전 반드시 백업을 하셔야 하십니다.

※ 변경된 설정을 적용시키기 위해서는 시스템을 재시작을 하셔야 적용됩니다.

※ 서버 방화벽에서 변경한 임의 포트를 등록하셔야 방화벽에서 차단되지 않습니다.

※ 위 예시의 임의 Port 1234는 임의 값으로 절대 똑같이 설정하시지 마시기 바랍니다.

3. 사용자 계정 보안 설정

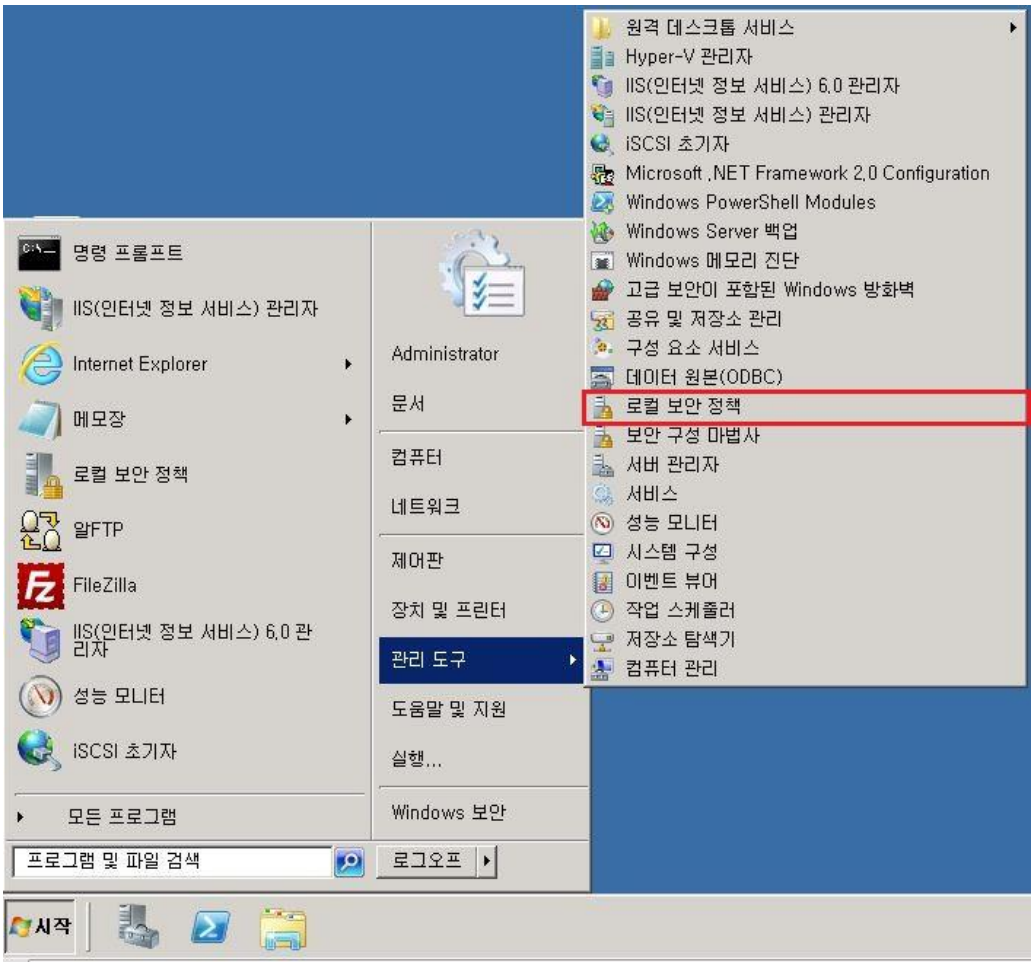
- Server 에서는 관리자 계정, FTP 접속을 위한 일반 사용자 계정 등 편의에 따라 각기 계정을 생성하여 사용하게 됩니다. 이렇게 생성한 사용자 계정들에 대한 기본적인 보안 설정을 하지 않을 경우 무차별적인 패스워드 대입 등을 통해 시스템으로 접근할 수 있습니다.

- 또, 일반 사용자 계정이 해킹 등으로 인해 불법적인 접속이 되었다 하더라도 시스템 파일로 접속할 수 없도록 해야만 더 큰 피해를 방지할 수 있습니다.

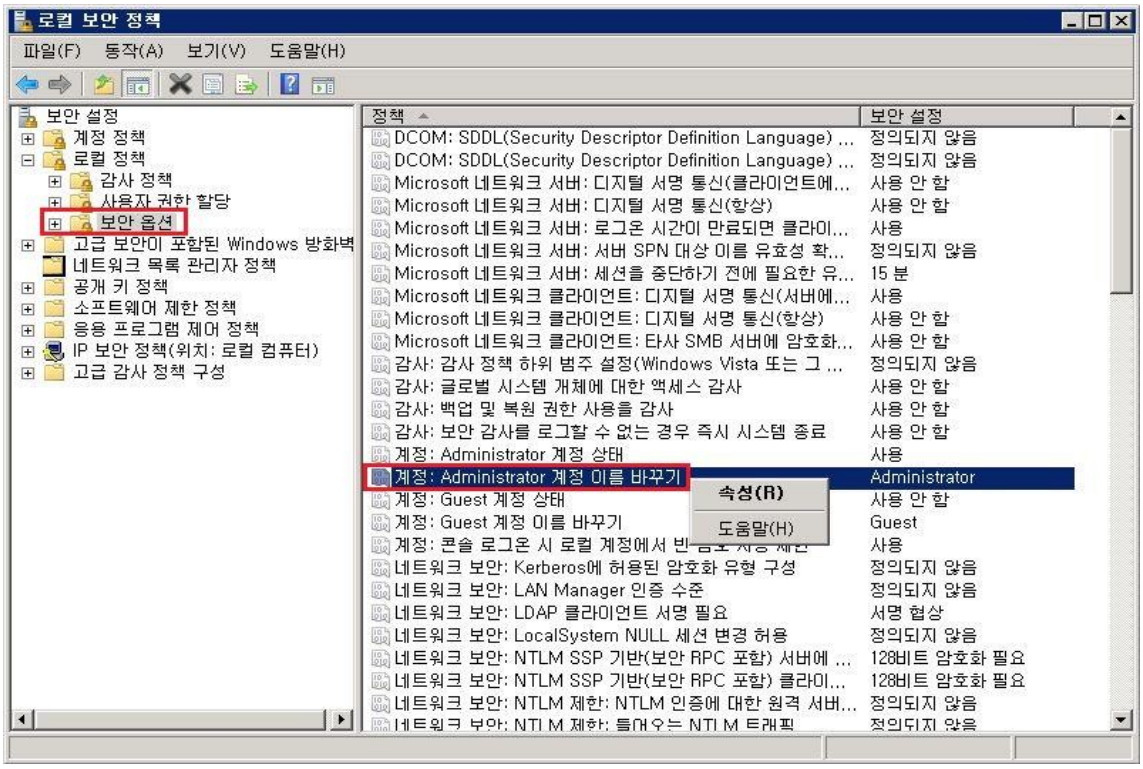
① Administrator 계정 명 변경

: Windows에서 기본적으로 제공되는 관리자 계정 명은 "administrator" 입니다. 이 계정 기본적으로 제공되는 계정으로 해당 계정에 패스워드를 계속 대입시키게 되면 아무리 복잡도가 높은 패스워드로 설정하셔도 침해사고가 발생할 수 있습니다.

시작 > 모든 프로그램 > 관리 도구 > 로컬 보안 정책



로컬 보안 정책 > 로컬 보안 정책 > 보안 옵션 > 계정 : Administrator 계정 이름 바꾸기 > [마우스 우클릭] > 속성

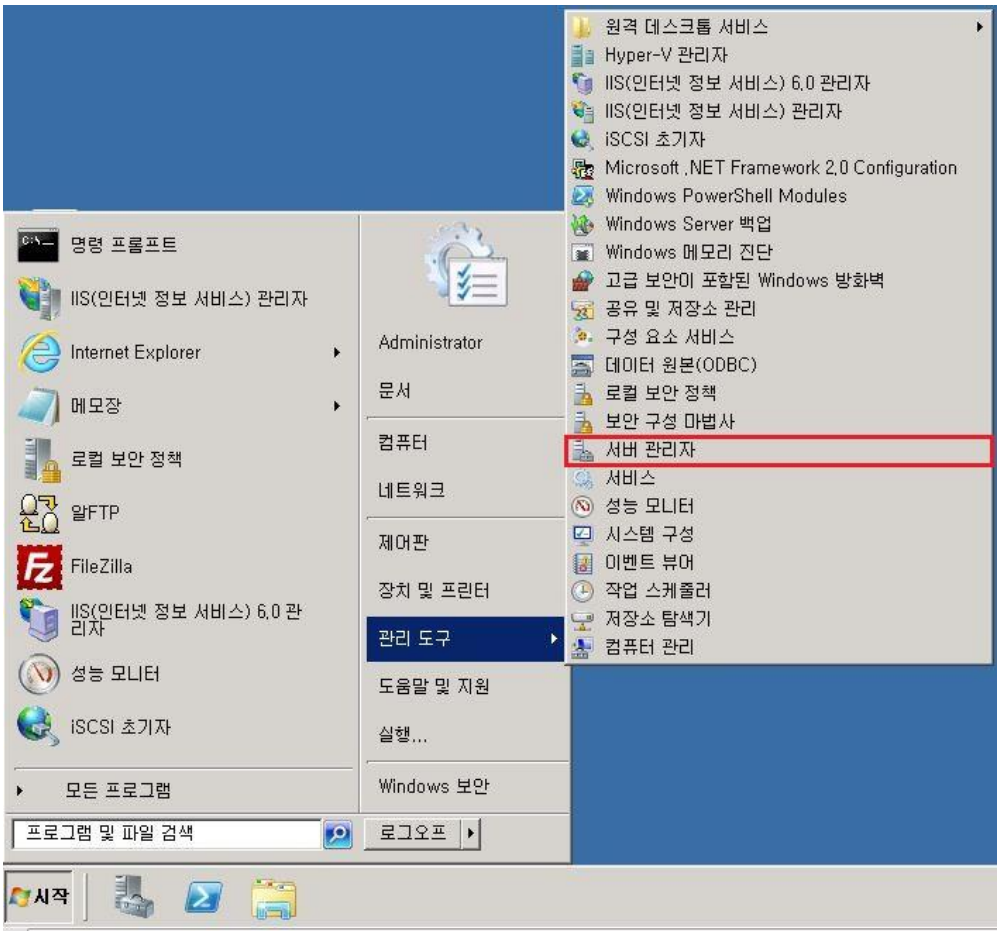


계정 : Administrator 계정 이름 바꾸기 속성 > administrator 부분을 임의 계정으로 변경

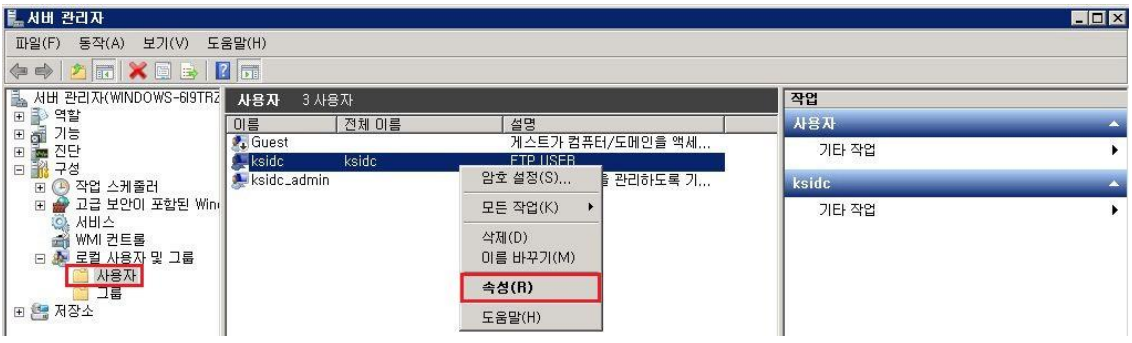
② 일반 사용자 계정 원격 터미널 접속 제한

: 일반적으로 서버로 사용하는 시스템의 경우 일반 사용자 계정을 통해 원격 터미널 접속을 하여 작업하는 경우가 매우 적습니다. 일반 사용자 계정을 통해 시스템으로의 직접적인 접근을 제한하는 것이 좋습니다.

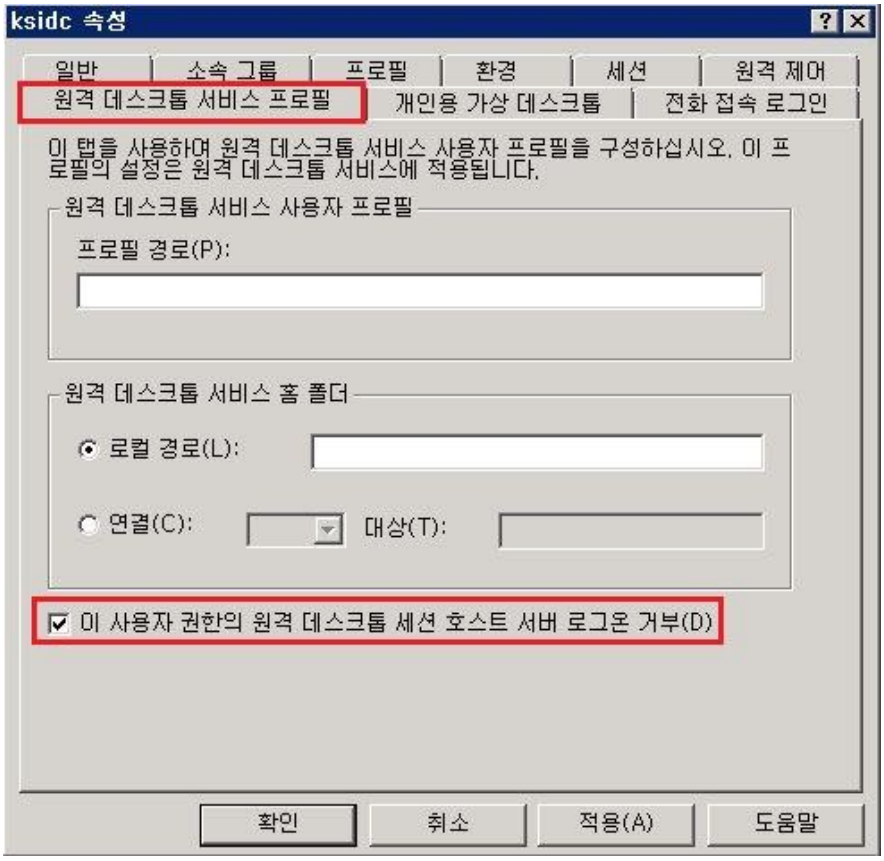
시작 > 모든 프로그램 > 관리 도구 > 서버 관리자



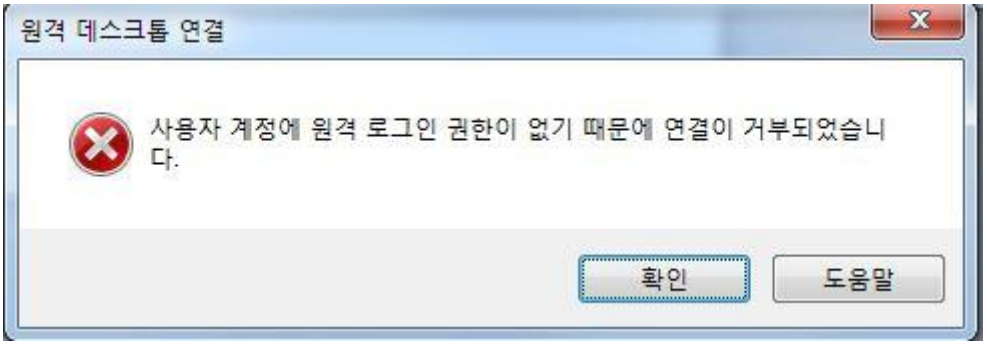
서버 관리자 > 구성 > 로컬 사용자 및 그룹 > 사용자 > 일반 사용자 계정 [마우스 우클릭] > 속성



일반 사용자 계정의 속성 > 원격 데스크톱 서비스 프로필 > "이 사용자 권한의 원격 데스크톱 세션 호스트 서버 로그온 거부" 체크 > 적용



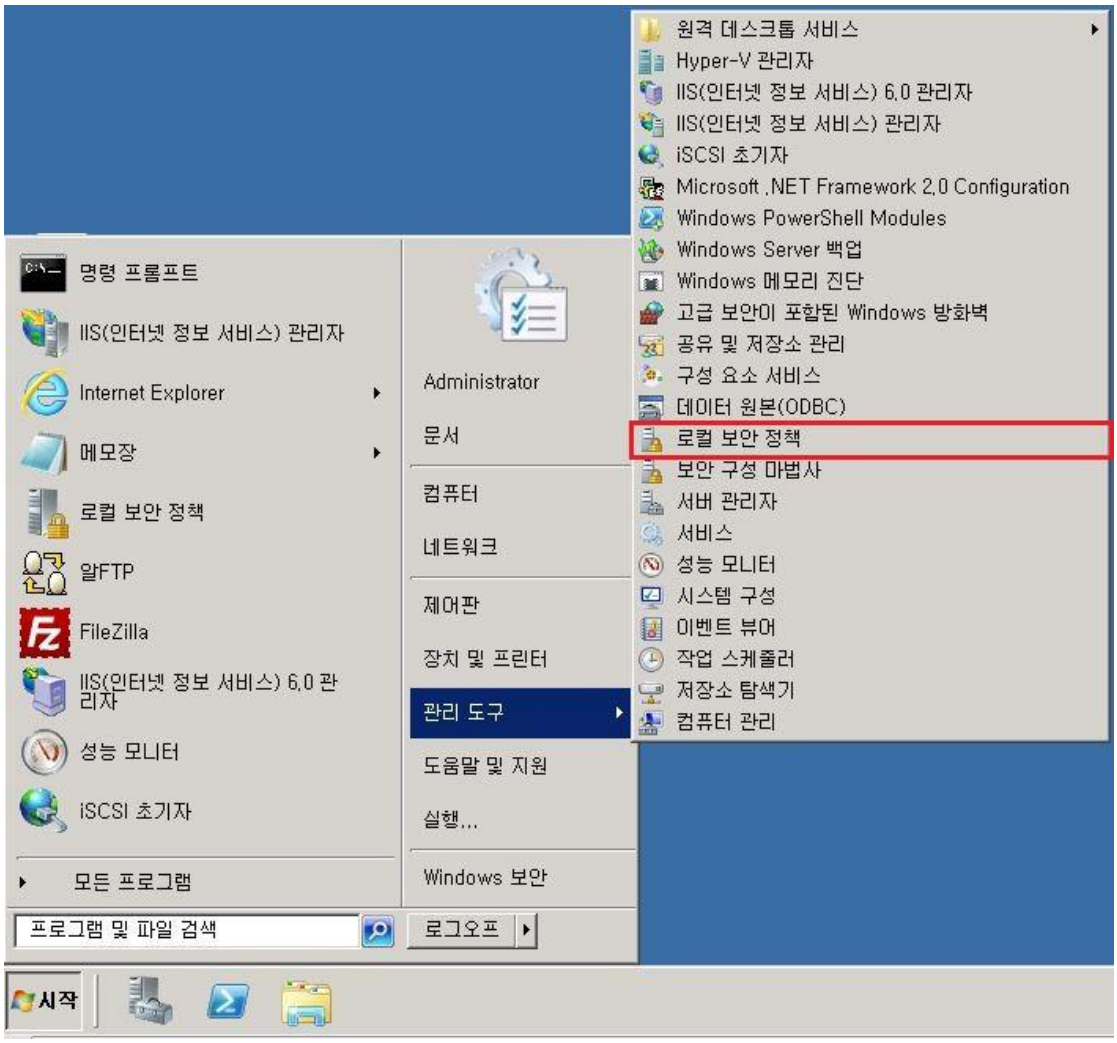
※ 원격 접속을 제한한 사용자로 접속을 할 경우 아래와 같이 차단되는 부분은 확인 할 수 있습니다.



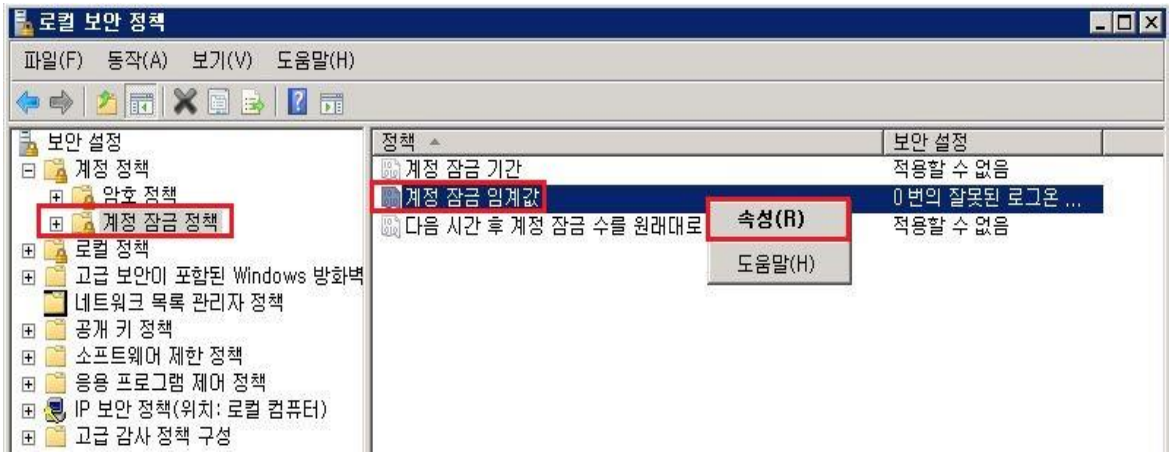
③ 계정 잠금 설정

: 계정의 보안을 더욱 강화하기 위해서는 계정 잠금 정책을 활성화 하여 특정 횟수 이상의 로그인 실패가 발생할 경우 계정을 지정한 시간만큼 접속 차단하여, 외부에서의 Brute force 공격으로부터 방어해야 합니다.

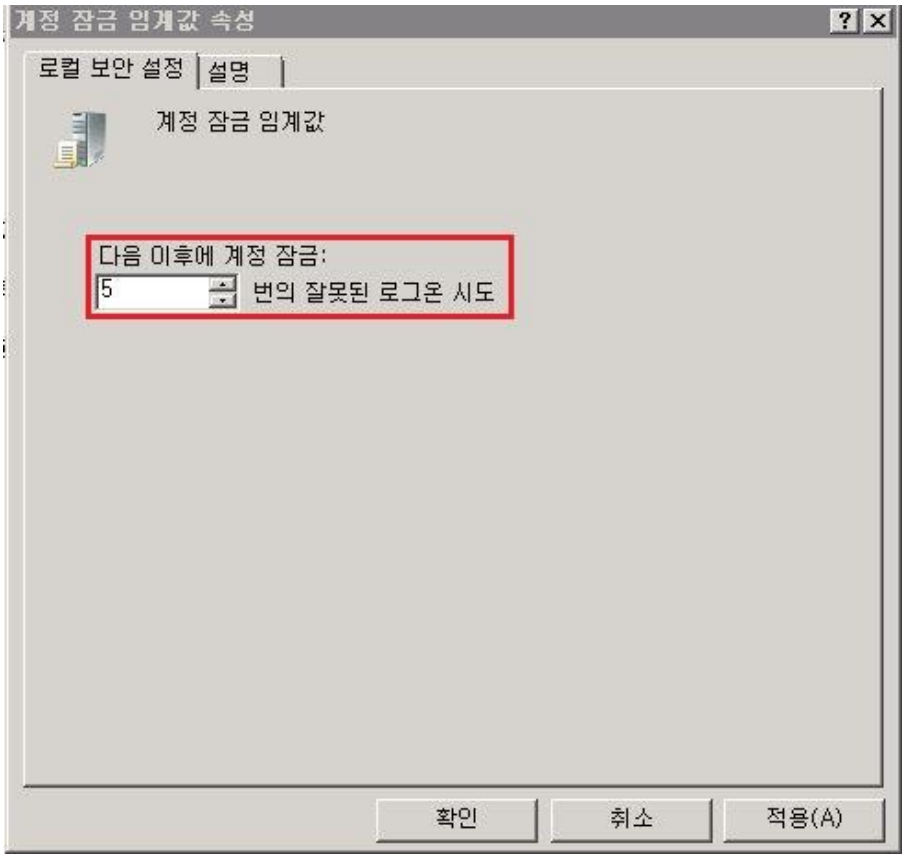
시작 > 모든 프로그램 > 관리 도구 > 로컬 보안 정책



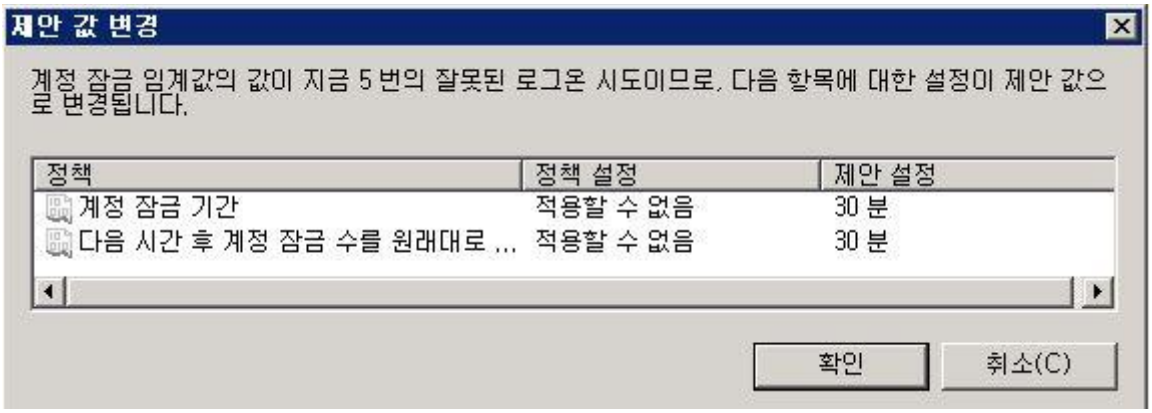
로컬 보안 정책 > 로컬 보안 정책 > 보안 설정 > 계정 정책 > 계정 잠금 정책 > 계정 잠금 임계값 [마우스 우클릭] > 속성



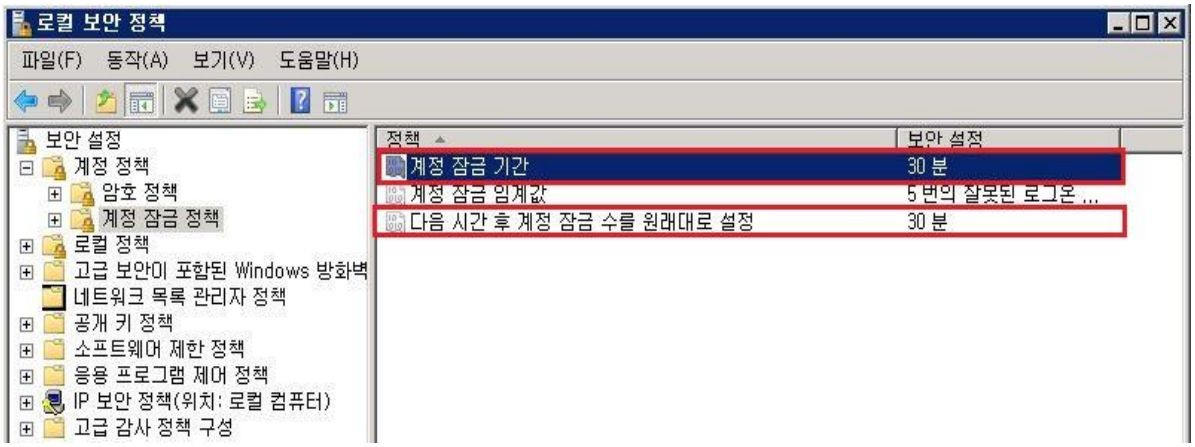
계정 잠금 임계값 속성 > 잘못된 로그온 시도 횟수 지정 > 적용



해당 로그온 실패 임계 값을 지정하실 경우, 자동적으로 계정 잠금 기간이 30분으로 설정됩니다.



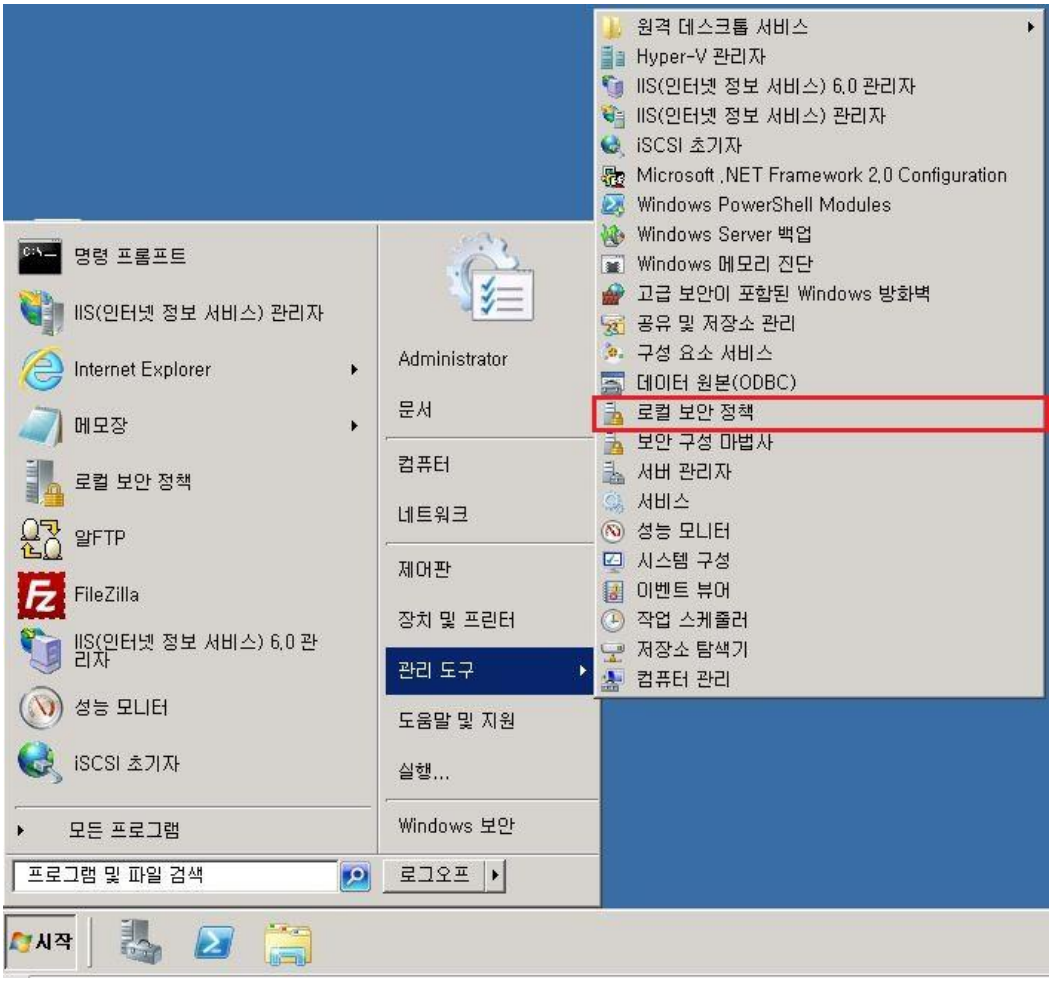
위와 같은 계정 잠금 기간은 서버 관리자 분께서 임의로 변경 가능하십니다.



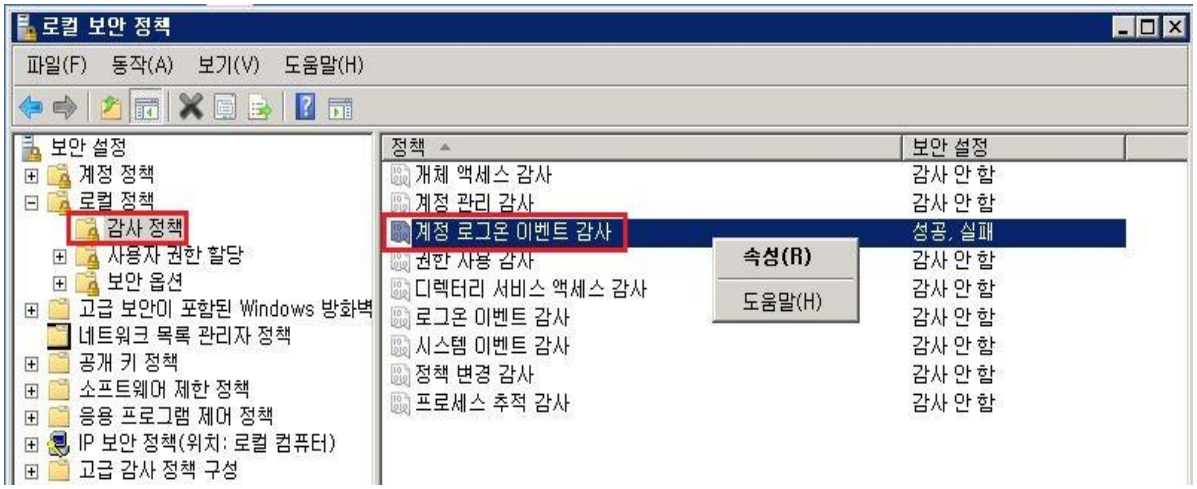
④ 보안 로그 활성화

: 보안 감사 정책을 사용하여 계정의 접속 정보를 이벤트 뷰어에 남기도록 설정합니다.

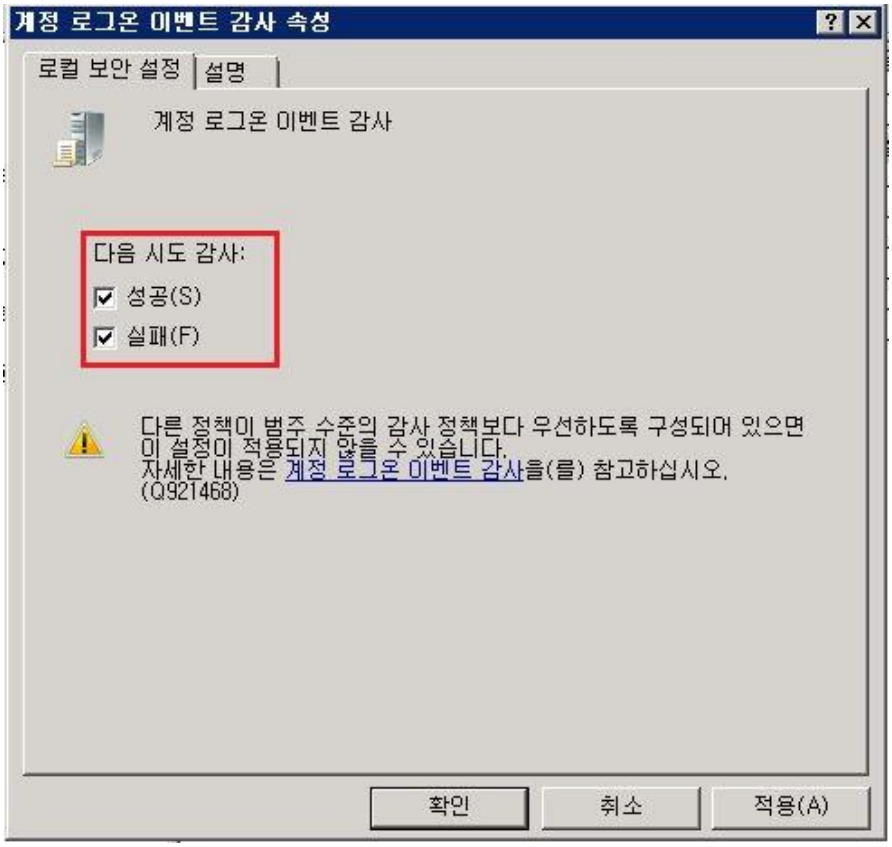
시작 > 모든 프로그램 > 관리 도구 > 로컬 보안 정책



로컬 보안 정책 > 로컬 보안 정책 > 보안 설정 > 로컬 정책 > 감사 정책 > 계정 잠금 임계값 [마우스 우클릭] > 속성



계정 로그온 이벤트 감사 속성 > 성공, 실패 체크 > 적용

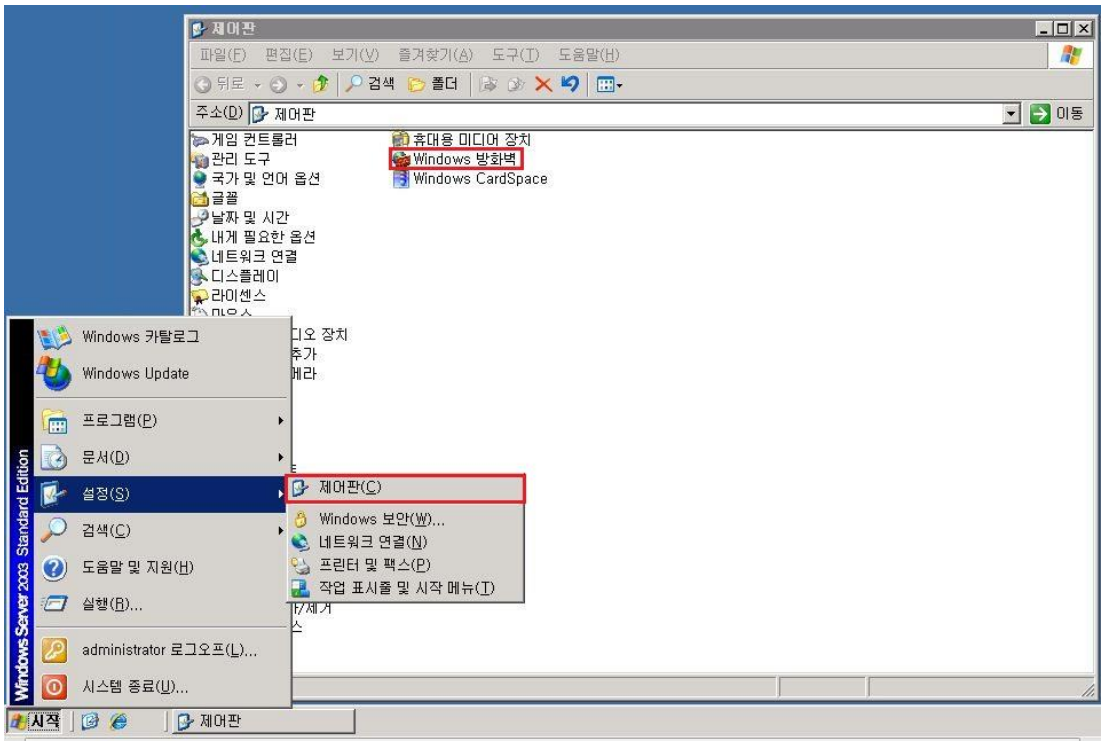


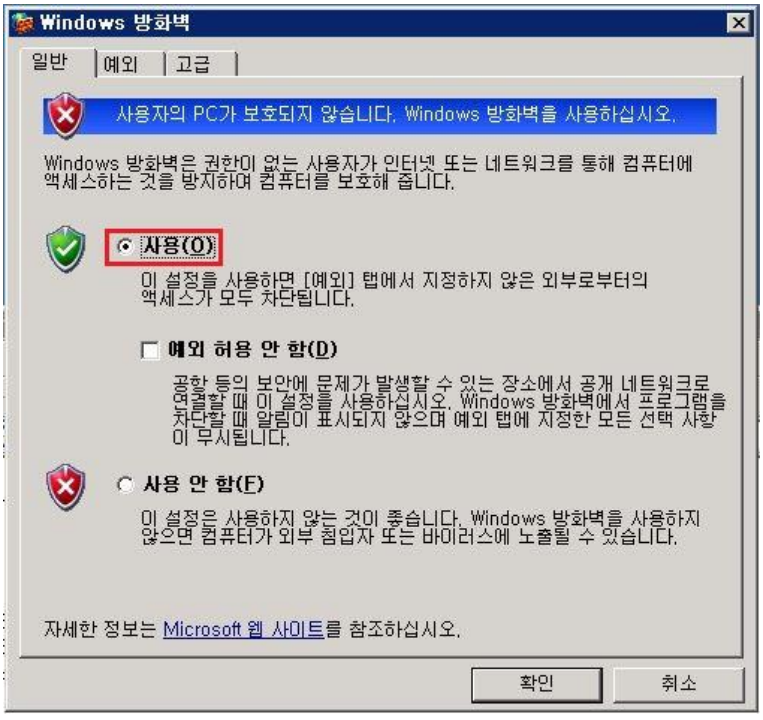
4. Windows 방화벽

① Windows 방화벽 상태 확인

< Windows Server 2003 >

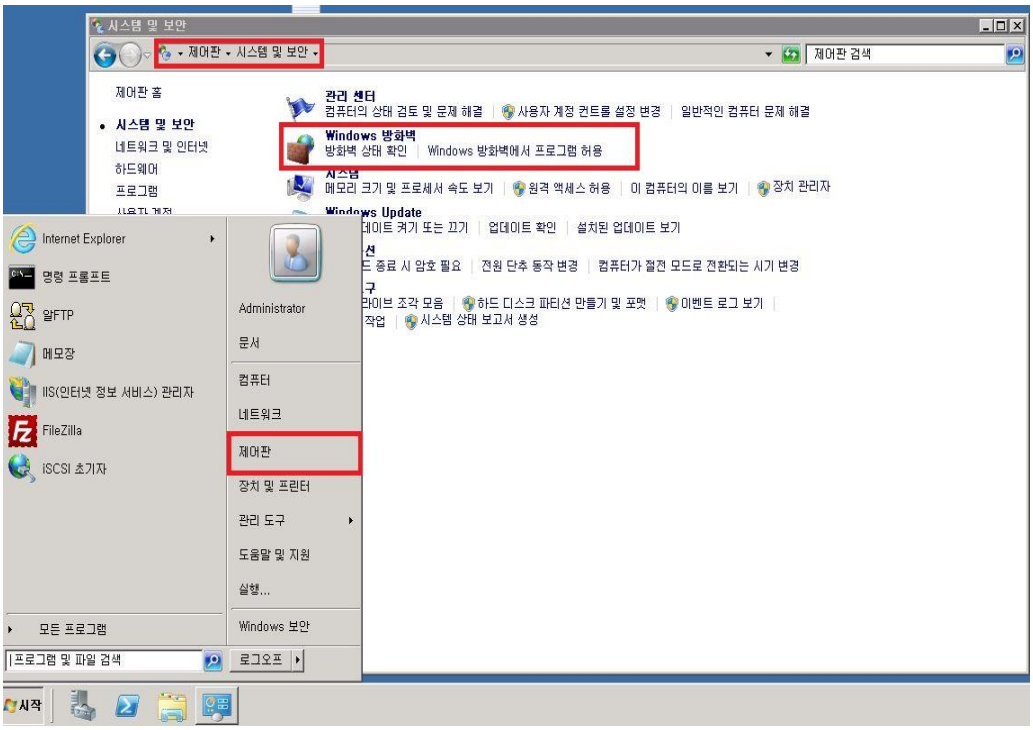
시작 > 설정 > 제어판 > Windows 방화벽



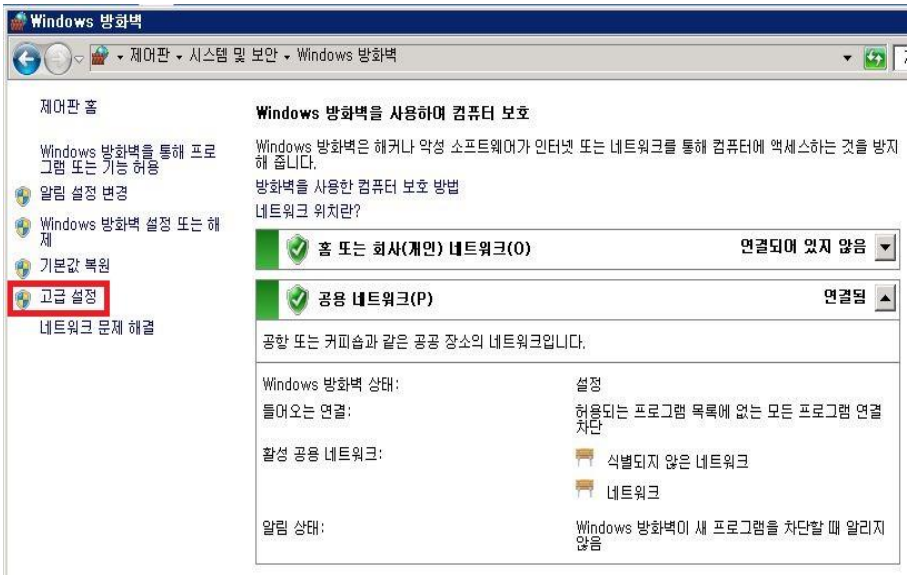


< Windows Server 2008 >

시작 > 모든 프로그램 > 제어판 > 시스템 및 보안 > Windows 방화벽 > 방화벽 상태 확인



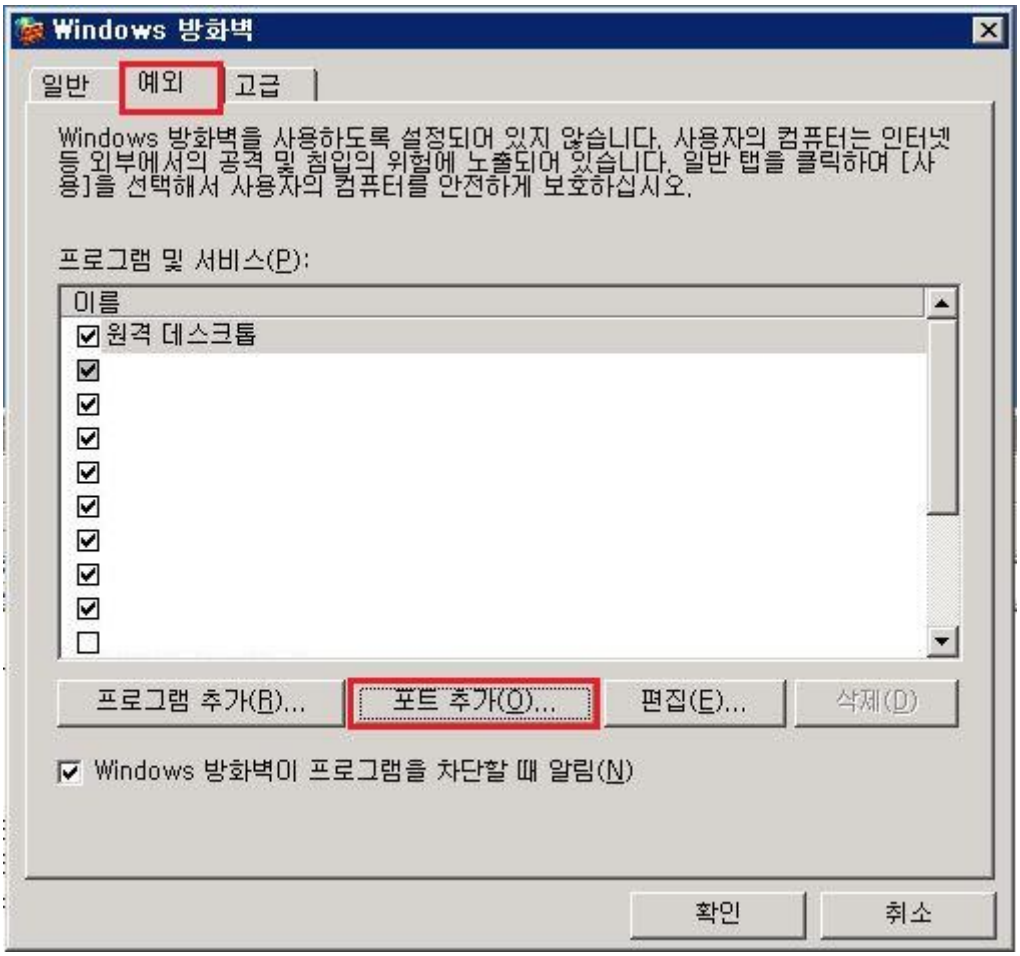
방화벽이 활성화 되어 있을 경우 아래와 같은 화면이 나오며, 고급 설정에서 설정을 추가합니다.



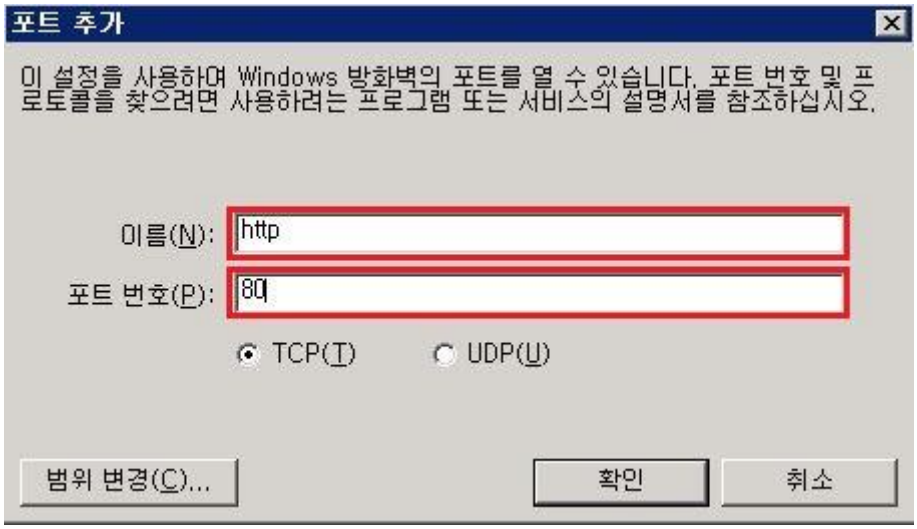
② 접근 허용할 Port 등록

< Windows Server 2003 >

Windows 방화벽 > 예외 탭 > 포트 추가

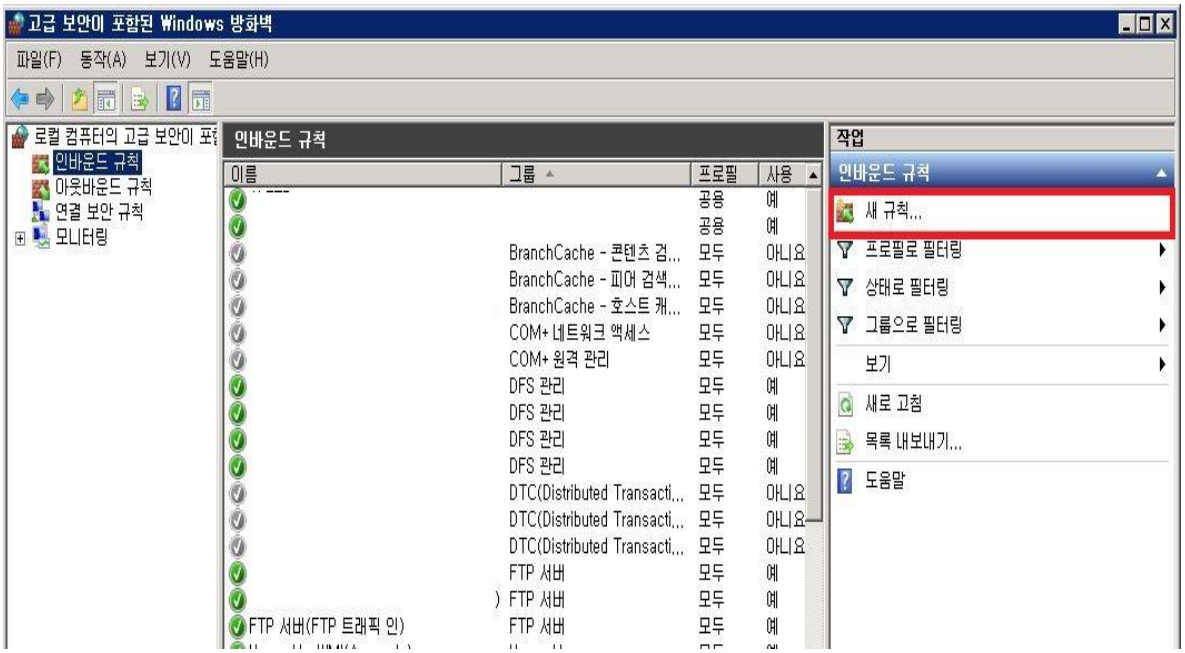


접근 허용할 포트를 추가 합니다.

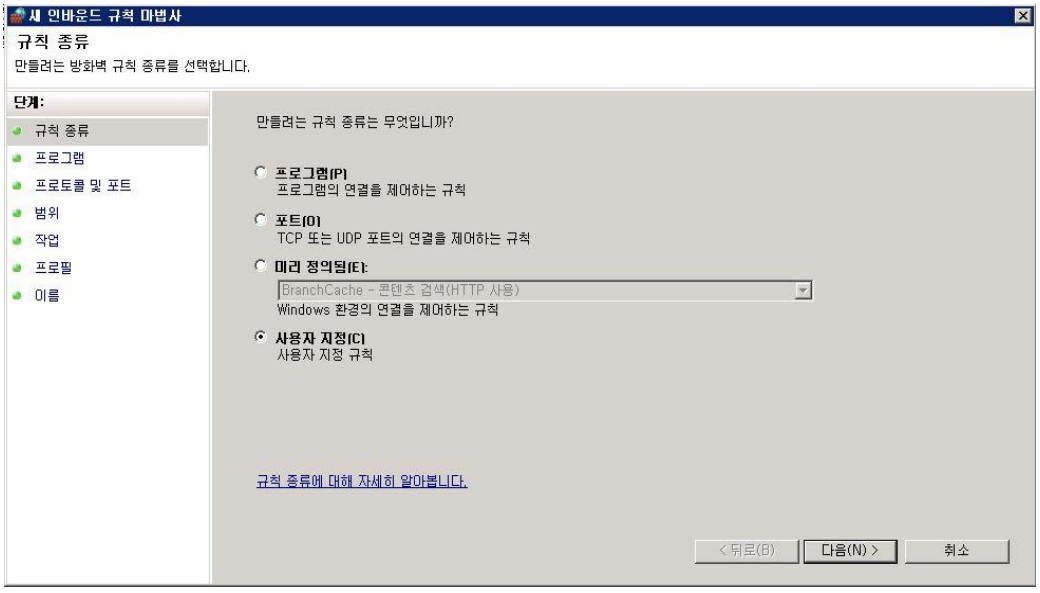


< Windows Server 2008 >

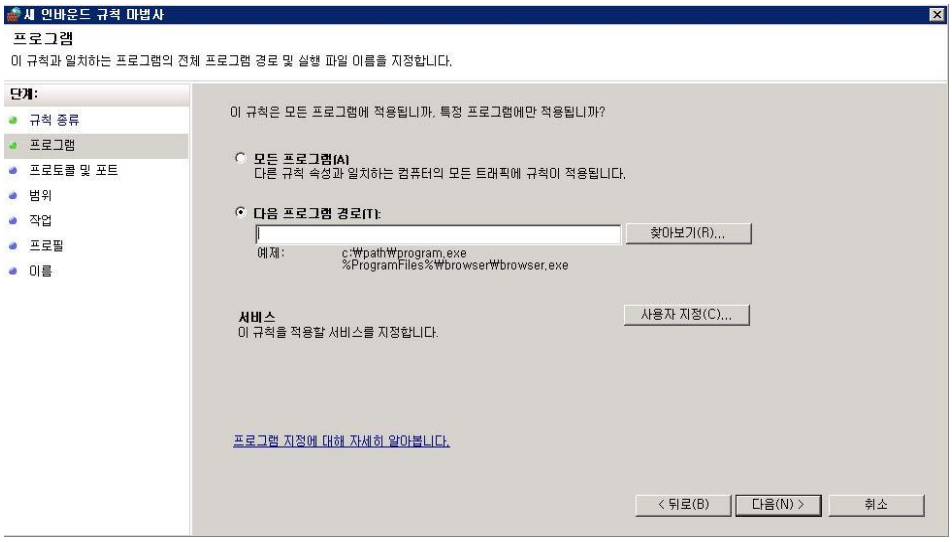
접근을 허용할 서비스를 인바운드 규칙에 새로운 규칙을 등록합니다.



사용자 지정 > 다음

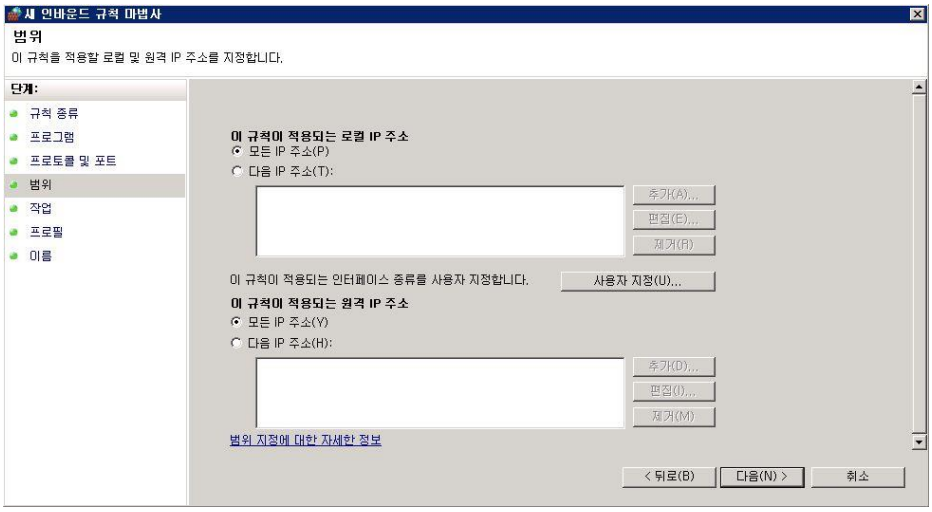


프로그램 > 다음

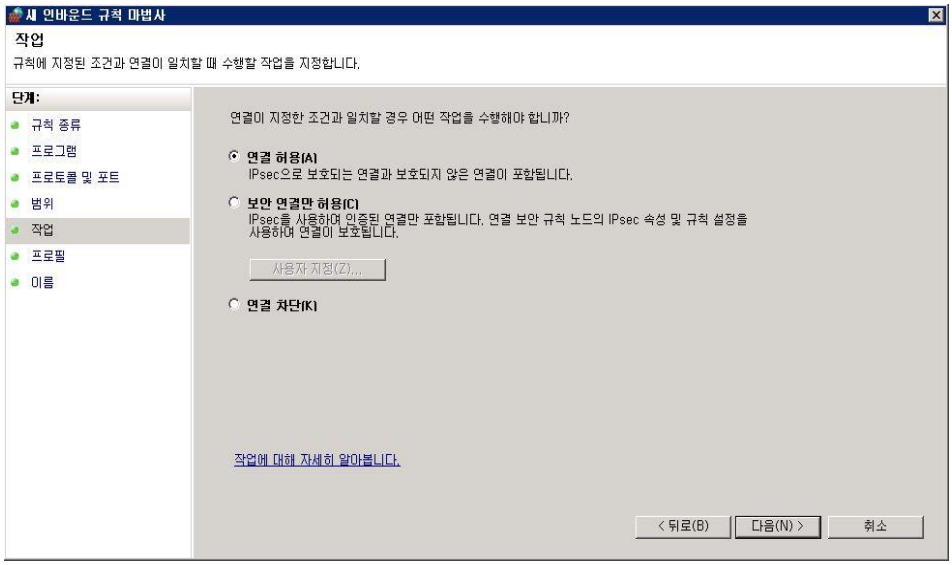


프로토콜 및 포트 > 프로토콜 종류 : TCP 지정 > 로컬 포트에 특정 Port 및 대역 설정

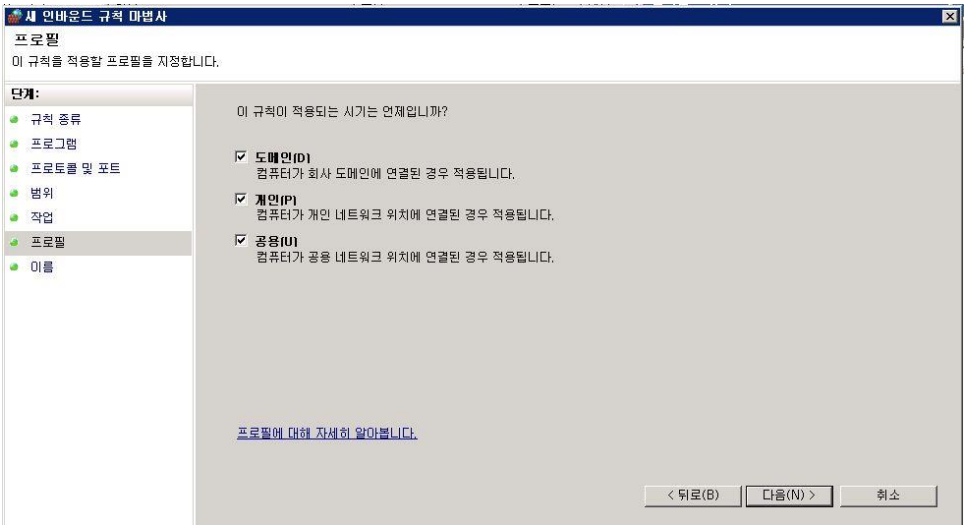
범위 > 다음



작업 > 연결 허용 > 다음



프로필 > 다음



정책 명을 임의로 지정 후 마침

5. 메모리 덤프 분석

- 메모리 덤프란? 시스템 중지 오류(ex. 블루스크린, 시스템 충돌)가 발생하여 윈도우 서버가 예기치 않게 종료될 경우 시스템에서 파일 형식으로 디버깅 정보를 시스템에 남기게 되는데 이때 생성되는 파일을 메모리 덤프라고 합니다.

- 메모리 덤프를 분석하기 위해서는 메모리 덤프 파일을 분석하기 위해서는 분석 프로그램인 WinDbg과 i386 폴더가 필요합니다.

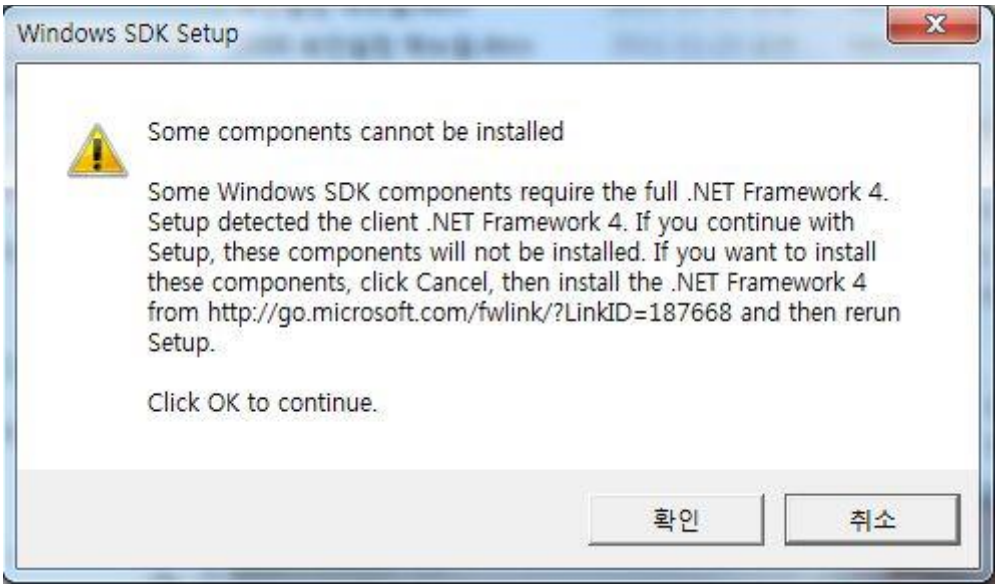
  ※ 메모리 덤프 파일을 개인 PC으로 다운로드 하여 분석하여도 무방합니다.

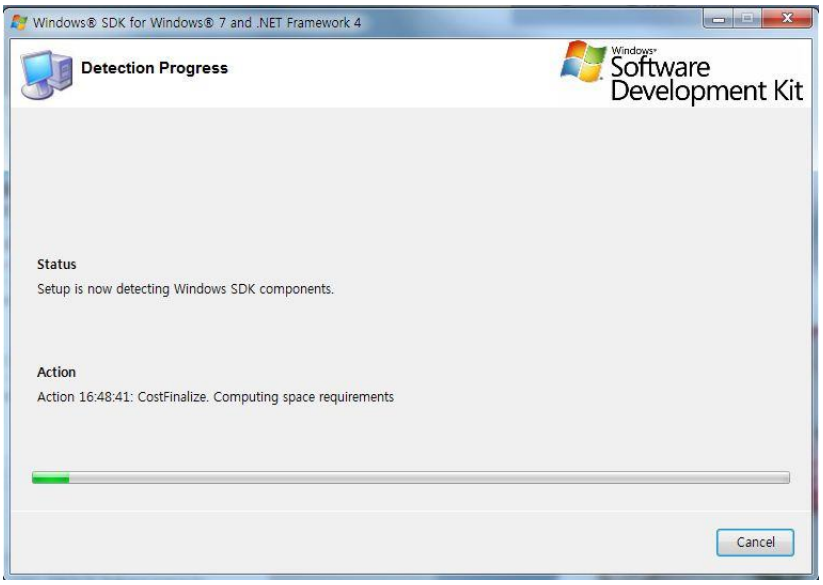
  ※ WinDbg 다운로드 경로
  - 32비트 버전 : http://www.microsoft.com/whdc/devtools/debugging/installx86.mspx
  - 64비트 버전 : http://www.microsoft.com/whdc/devtools/debugging/install64bit.mspx

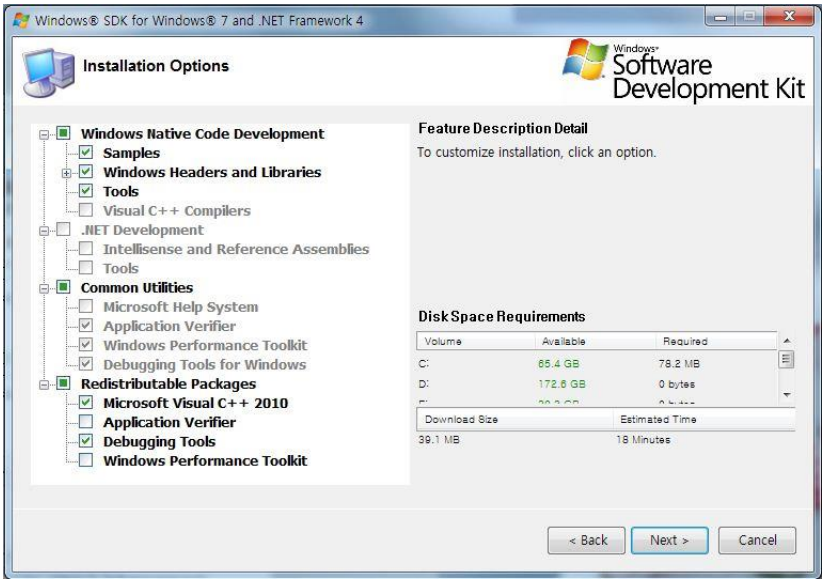
  ※ Symbols 다운로드 경로
  - http://msdn.microsoft.com/en-us/windows/hardware/gg463028.aspx

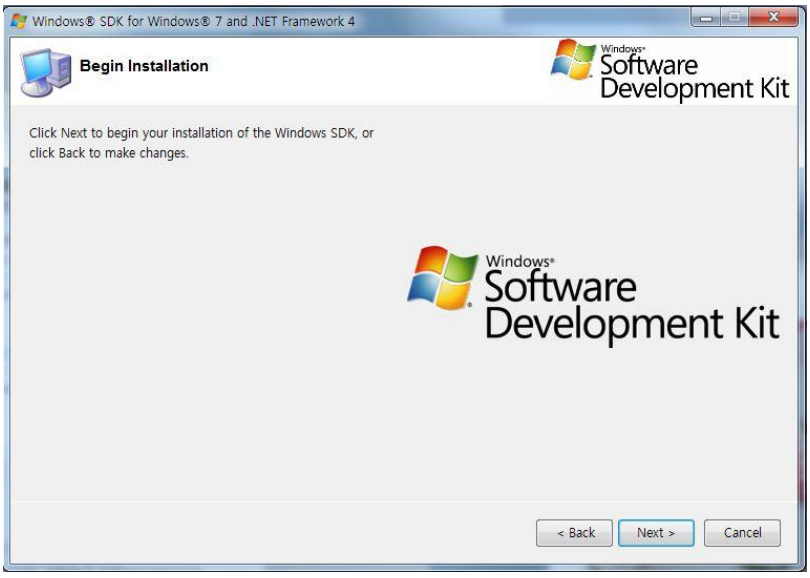
  ※ 생성 경로 : c:₩windows₩Memory.dmp

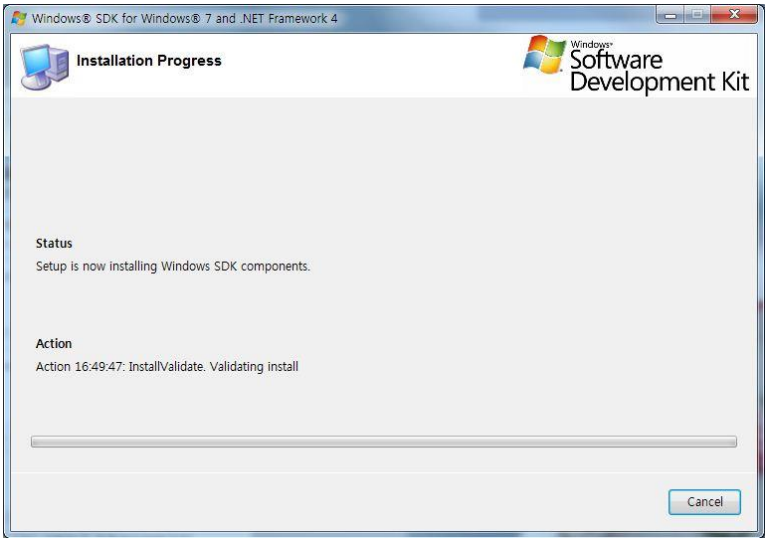
  ① WinDbg 설치
  : 다운로드 받은 설치 파일을 실행시킵니다.




Windows® SDK for Windows® 7 and .NET Framework 4
Detection Progress
Windows Software Development Kit
Status
Setup is now detecting Windows SDK components.
Action
Action 16:48:41: CostFinalize. Computing space requirements
Cancel

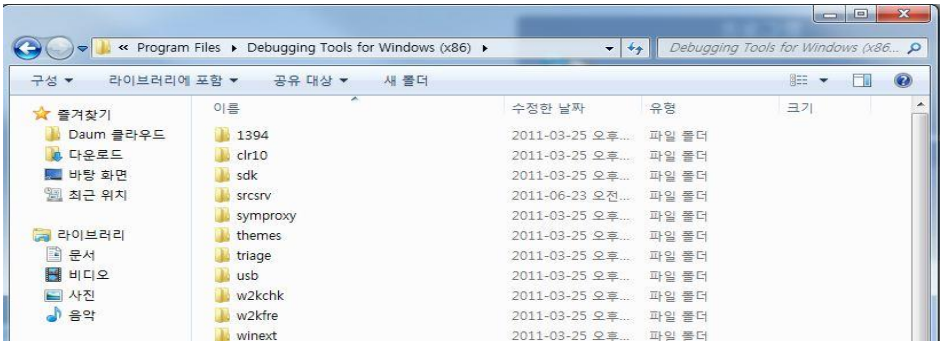

Windows® SDK for Windows® 7 and .NET Framework 4
Installation Options
Windows Software Development Kit
Windows Native Code Development
Samples
Windows Headers and Libraries
Tools
Visual C++ Compilers
.NET Development
Intellisense and Reference Assemblies
Tools
Common Utilities
Microsoft Help System
Application Verifier
Windows Performance Toolkit
Debugging Tools for Windows
Redistributable Packages
Microsoft Visual C++ 2010
Application Verifier
Debugging Tools
Windows Performance Toolkit
Feature Description Detail
To customize installation, click an option.
Disk Space Requirements
Volume
Available
Required
C:
65.4 GB
78.2 MB
D:
172.6 GB
0 bytes
Download Size
Estimated Time
39.1 MB
18 Minutes
< Back
Next >
Cancel


Windows® SDK for Windows® 7 and .NET Framework 4
Begin Installation
Windows Software Development Kit
Click Next to begin your installation of the Windows SDK, or click Back to make changes.
Windows Software Development Kit
< Back
Next >
Cancel



설치된 경로를 확인합니다.

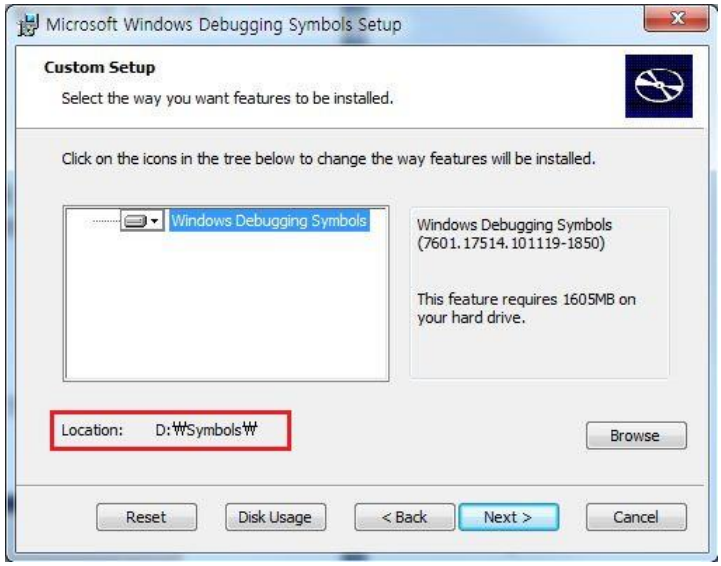
(기본 설치 경로 : C:₩Program Files₩ Debugging Tools for Windows (x86))

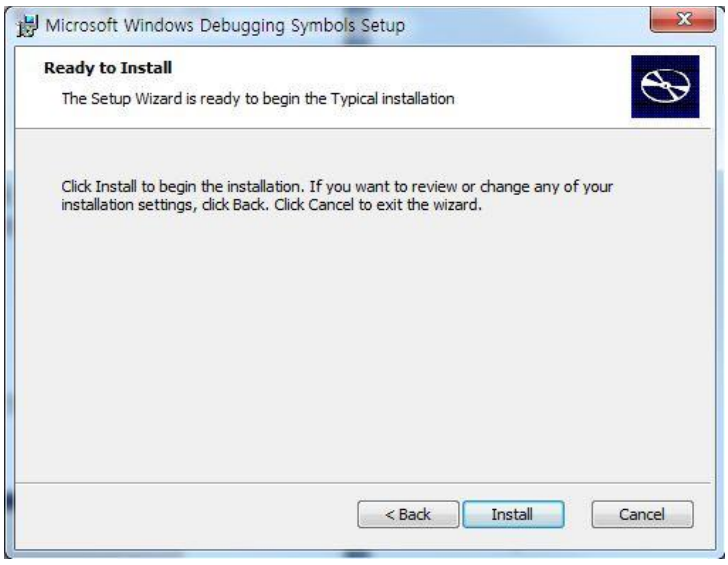


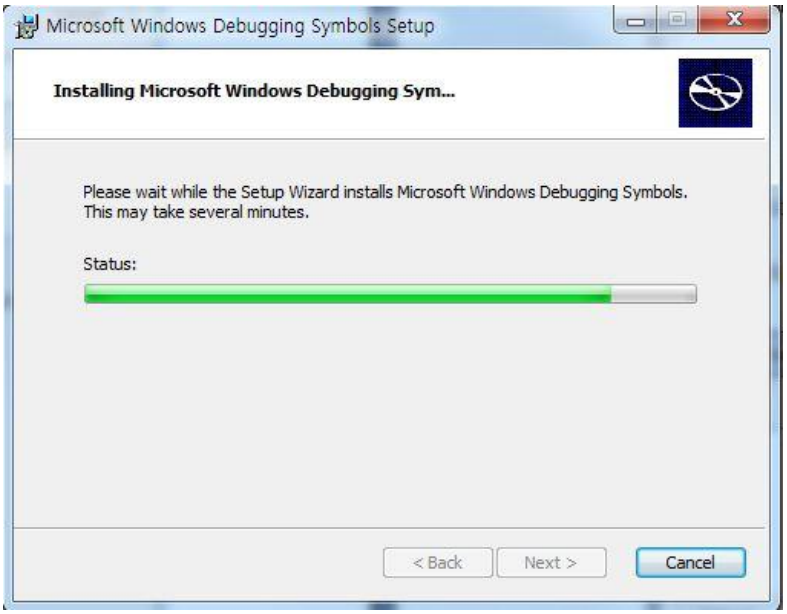
② Symbols 설치

: 다운로드 받은 설치 파일을 실행시킵니다.


Microsoft Windows Debugging Symbols License Agreement
End-User License Agreement
Please read the following license agreement carefully
MICROSOFT SOFTWARE LICENSE TERMS
MICROSOFT DEBUGGING SYMBOLS AND EXECUTABLES
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the
I accept the terms in the License Agreement
I do not accept the terms in the License Agreement
< Back
Next >
Cancel

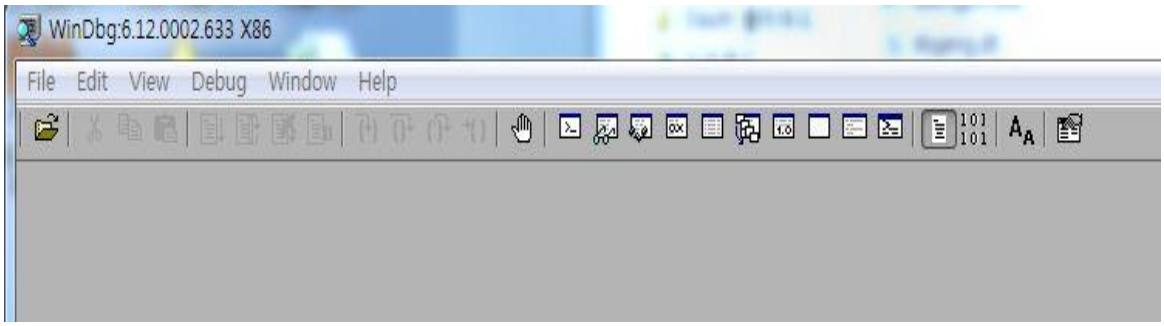

Microsoft Windows Debugging Symbols Setup
Custom Setup
Select the way you want features to be installed.
Click on the icons in the tree below to change the way features will be installed.
Windows Debugging Symbols
Windows Debugging Symbols (7601.17514.101119-1850)
This feature requires 1605MB on your hard drive.
Location: D:₩Symbols₩
Browse
Reset
Disk Usage
< Back
Next >
Cancel


Microsoft Windows Debugging Symbols Setup
Ready to Install
The Setup Wizard is ready to begin the Typical installation
Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
< Back
Install
Cancel



③ 분석 방법

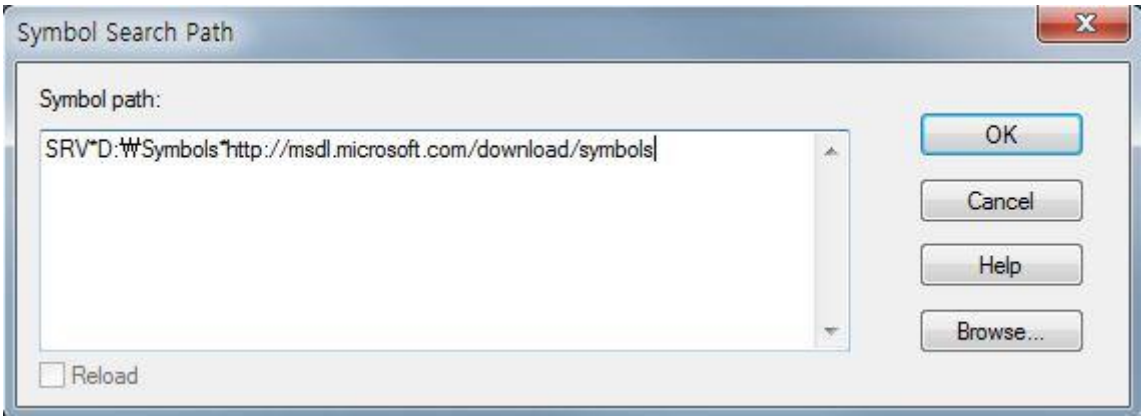
설치된 경로에서 WinDdg.exe를 실행합니다.



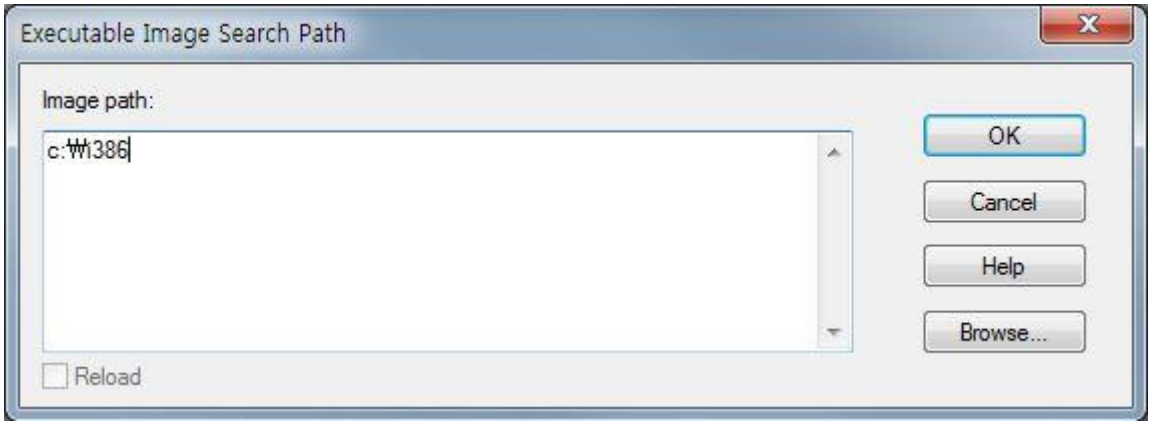
File > Symbol File Path를 지정해 줍니다.

: Symbols 경로는 SRV*[설치폴더] *http://msdl.microsoft.com/download/symbols 으로 지정하시면 되십니다.

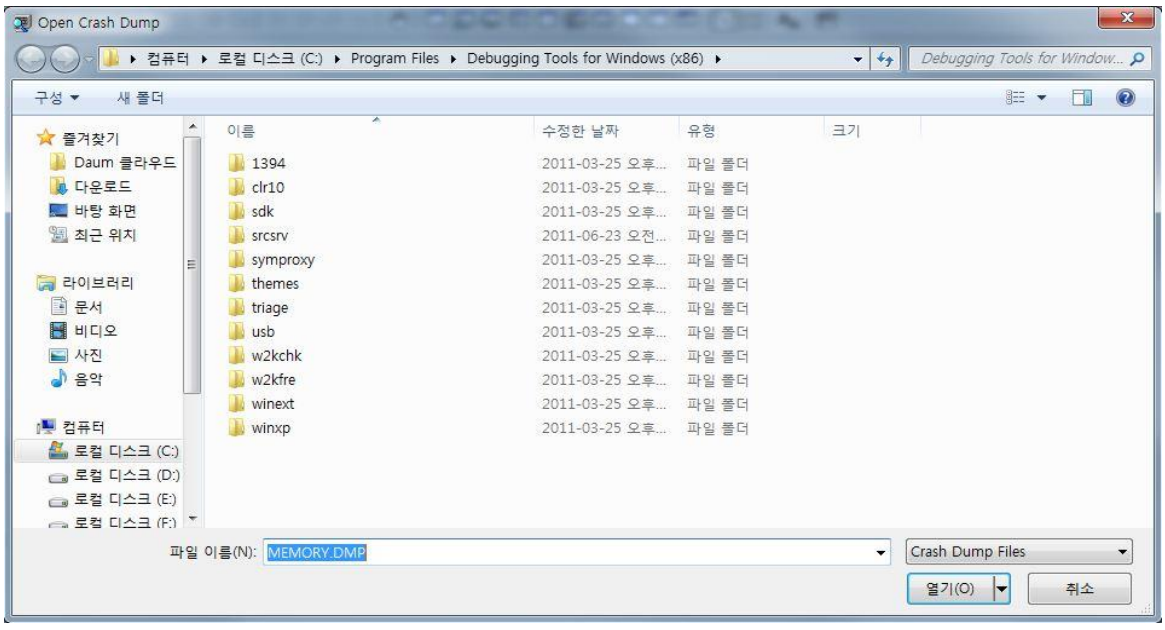
ex) SRV*D:₩Symbols*http://msdl.microsoft.com/download/symbols



File > Image File Path 에서 i386 경로를 지정해 줍니다.

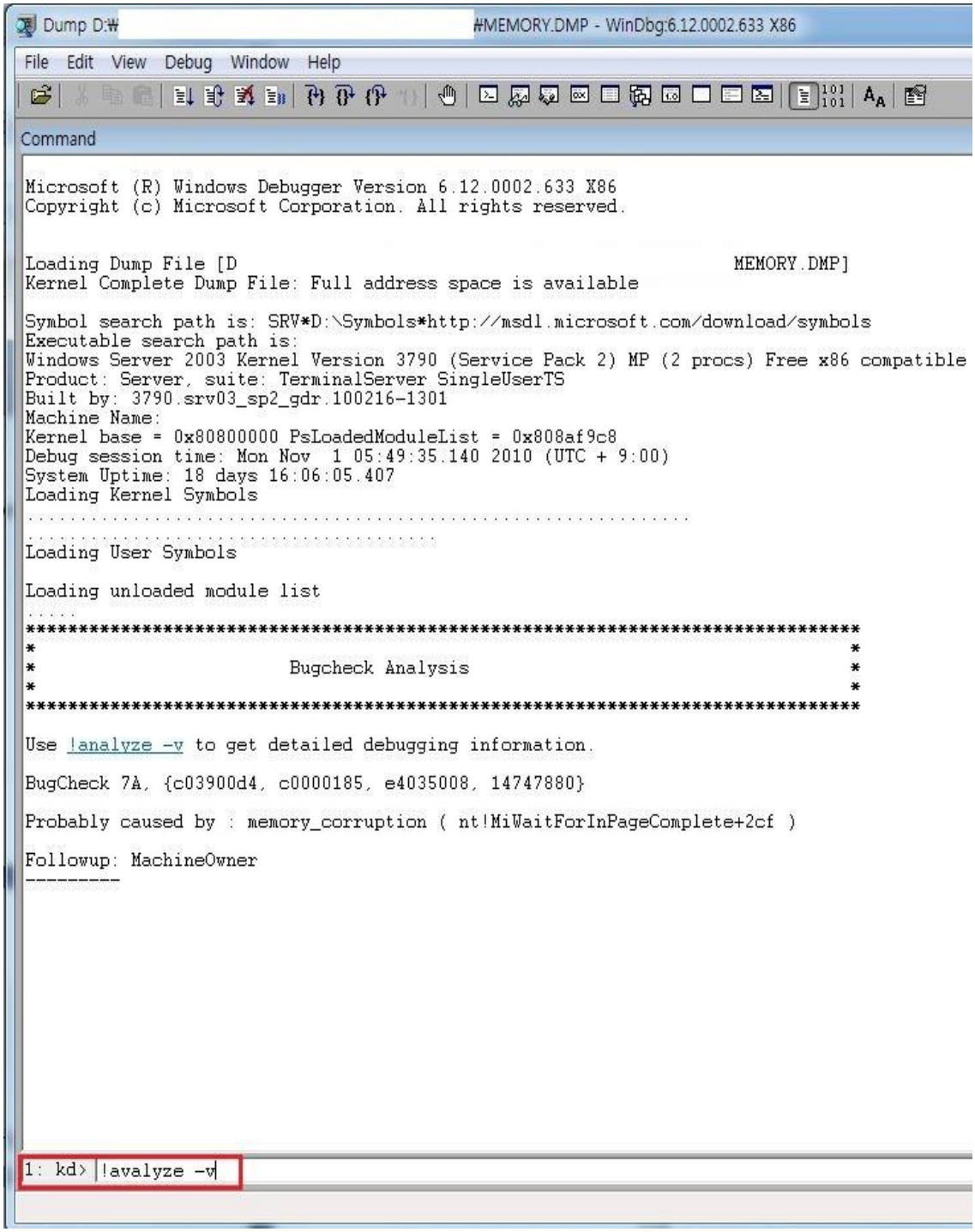


File > Open Crash Dump 를 실행하여 덤프 파일을 가져 옵니다.



!analyze -v 명령어를 이용하여, Dump 내용 중 오류 내용을 확인하시면 되십니다.

kb> !analyze -v

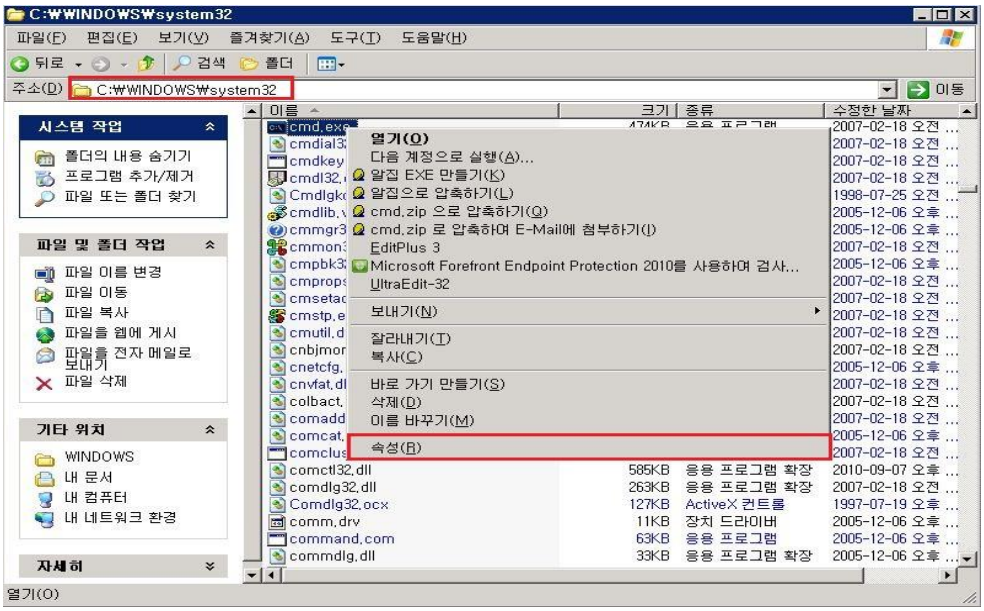


[Windows 2003 cmd.exe 보안 설정 TIP]

: cmd란 명령 프롬프트으로 도스 창입니다. 즉, "도스(DOS) 명령" 을 실행하는 부분입니다. 일반적으로 서버의 경우 외부에서 cmd를 요청하는 경우가 없기 때문에 외부에서 접근하여 사용하는 부분을 제한하는 것이 좋습니다.

※ cmd.exe 파일 경로 : C:₩windows₩system32

① cmd.exe [마우스 우클릭] > 속성



② cmd 속성 > 보안

: 접근이 불필요한 계정들은 모두 삭제하여 내부 관리자가 접속을 한 후에만 사용할 수 있도록 합니다.