# 감사정책 적용을 통한 외부 접속 로그 생성 및 확인

윈도우 2000 및 2003 서버 제품군을 초기 설치 하였을 경우 보안감사 정책이 자동 설정 되지 않습니다.

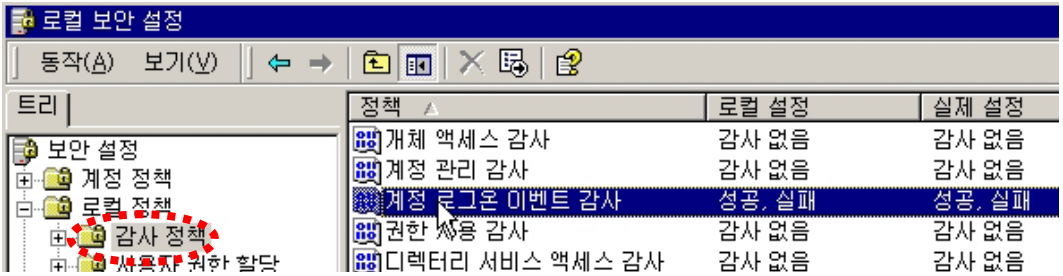
그로 인하여 윈도우 터미널서비스로 서버의 접속을 시도할 경우 해당 접속에 대한 성공/실패에 대한 로그가 생성 되지 않습니다.

윈도우 서버 제품군은 리눅스와 달리 외부접속에 대한 로그를 별도로 정책을 할당하지 않을 경우 생성되지 않습니다.

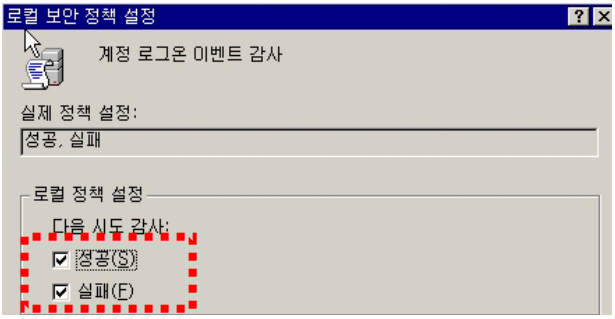
다음은 서버의 보안감사 정책을 통한 터미널 서비스 접속 시도에 대한 성공/실패의 로그를 확인하는 방법을 설명하도록 하겠습니다.

1) [시작]-[프로그램]-[관리도구]-[로컬보안 정책]을 실행 합니다.

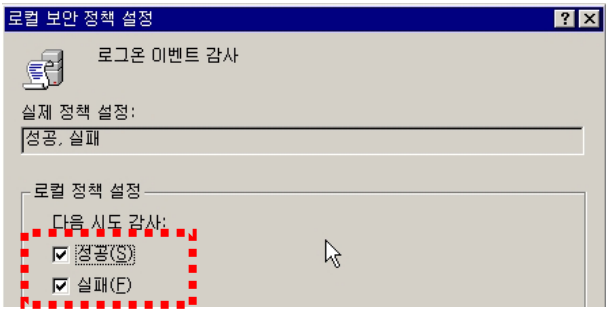
   다음 그림과 같이 [로컬 정책]-[감사 정책] 메뉴로 이동 합니다.




2) 우측 메뉴의 정책 중 [계정 로그온 이벤트 감사]를 더블클릭 한 후 [성공/실패]에 모두 체크 합니다.




3) 다음은 [로그온 이벤트 감사]를 선택한 후 [성공/실패]에 모두 체크 합니다.

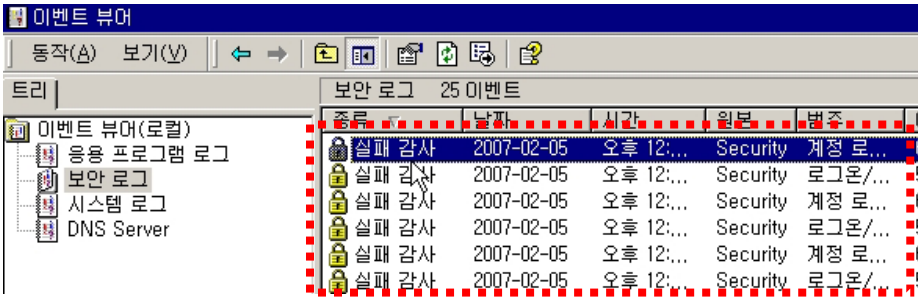


4) 위와 같이 설정한 후 터미널 서비스 클라이언트를 이용하여 로그인 대상 서버에 잘못된 로그인 시도를 2~3회 실행 합니다.

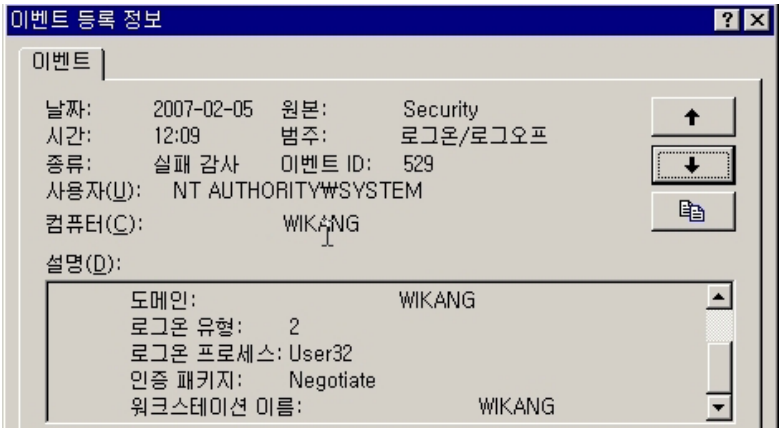
5) 잘못된 접속에 대한 로그를 확인하기 위하여 [시작]-[프로그램]-[관리도구]-[이벤트뷰어]를 실행 합니다.

좌측의 메뉴 중 [보안로그] 항목을 선택합니다.

다음 그림과 같이 [실패 감사]된 로그들이 남겨진 것을 확인할 수 있습니다.




6) [실패 감사]된 로그를 더블클릭 하시면 다음그림과 같은 상세 정보를 확인할 수 있습니다.

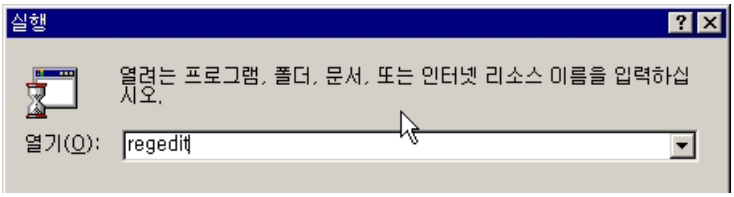



※ 위의 그림은 WIKANG의 컴퓨터명을 가진 워크스테이션에서 터미널서비스로 잘못된 로그인을 수행한 결과로 확인하실 수 있습니다.

7) 위의 설정만으로 잘못된 접속을 시도하는 로그를 확인할 수는 있으나 해당 접속자의 IP주소를 확인할 수는 없습니다.

다음 내용에서는 터미널서비스로 잘못된 접속시도가 발생할 때 접속자의 IP주소를 로그에 포함하는 방법을 설명하도록 하겠습니다.

[시작]-[실행]-[regedit]를 입력하여 레지스트리 편집기를 실행합니다.

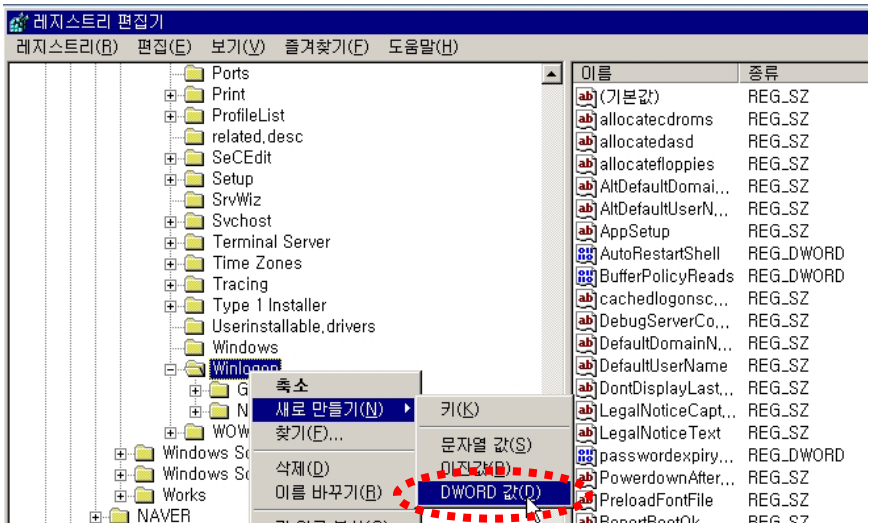


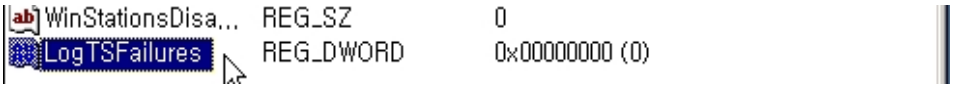
8) 다음 그림과 같이 레지스트리 값을 만들어 1로 설정 합니다.

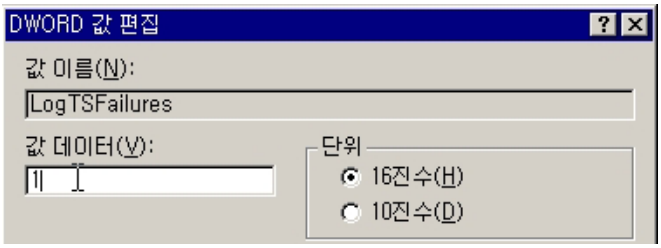
값 이름 : LogTSFailures

값 종류 : REG_DWORD

값 데이터 : 1



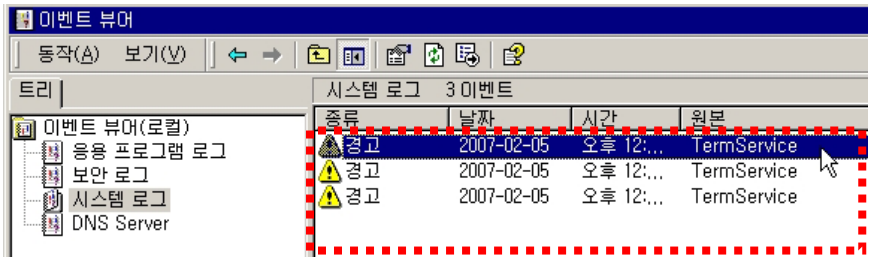




9) 위와 같이 설정한 후 터미널 서비스 클라이언트를 이용하여 로그인 대상 서버에 잘못된 로그인 시도를 2~3회 실행 합니다

10) 잘못된 접속에 대한 로그를 확인하기 위하여 [시작]-[프로그램]-[관리도구]-[이벤트뷰어]를 실행 합니다.

좌측의 메뉴 중 [시스템 로그] 항목을 선택합니다.

다음 그림과 같이 잘못된 접속에 대한 [경고] 로그들이 남겨진 것을 확인할 수 있습니다.




11) 우측 메뉴의 [경고] 로그를 더블클릭 하시면 다음그림과 같이 접속시도자의 IP주소를 확인 하실 수 있습니다.


※ 위의 그림중 [원본 네트워크 주소] 항목이 IP주소가 남겨지는 항목이며 넥스트라인의 보안정책으로 인하여 IP주소는 편집하였습니다.