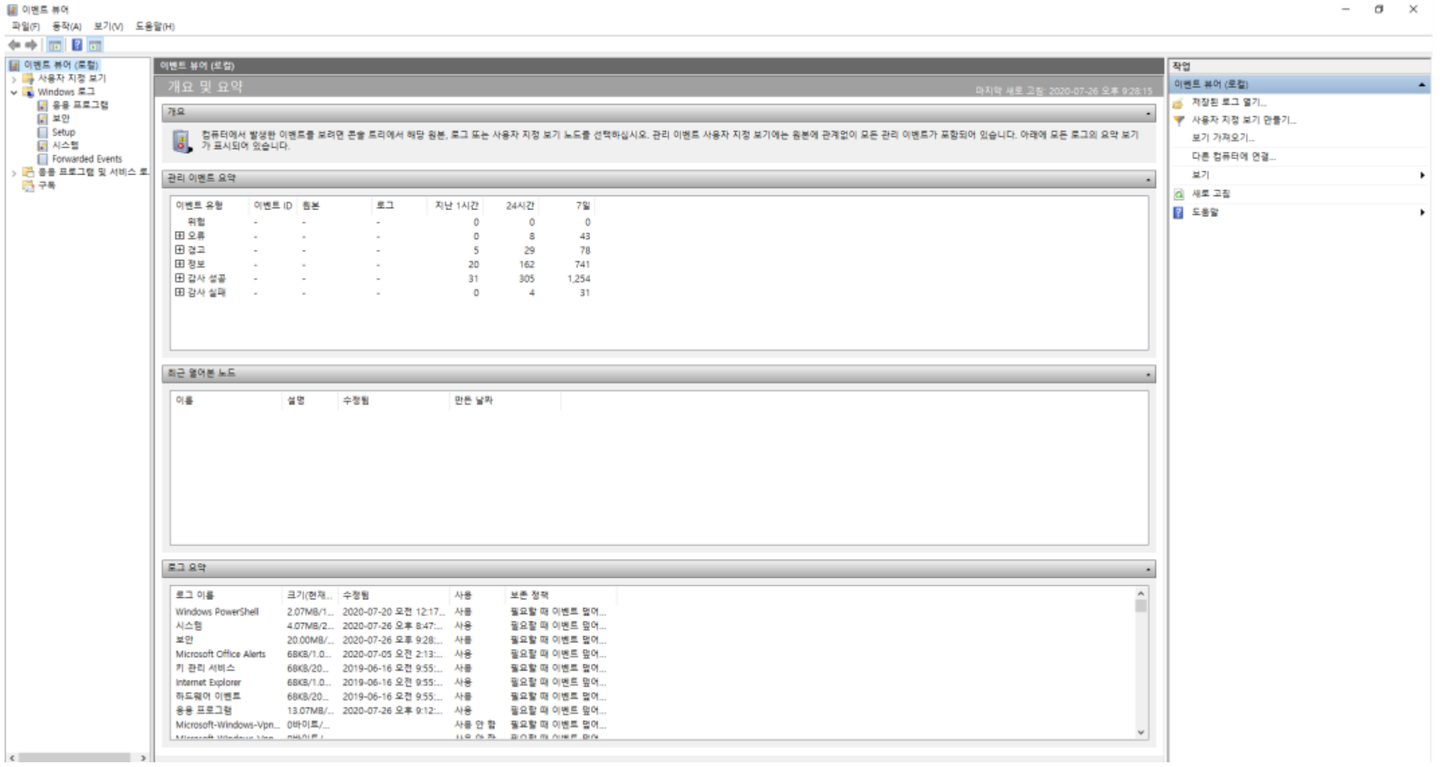
[Windows Event Log]

목차

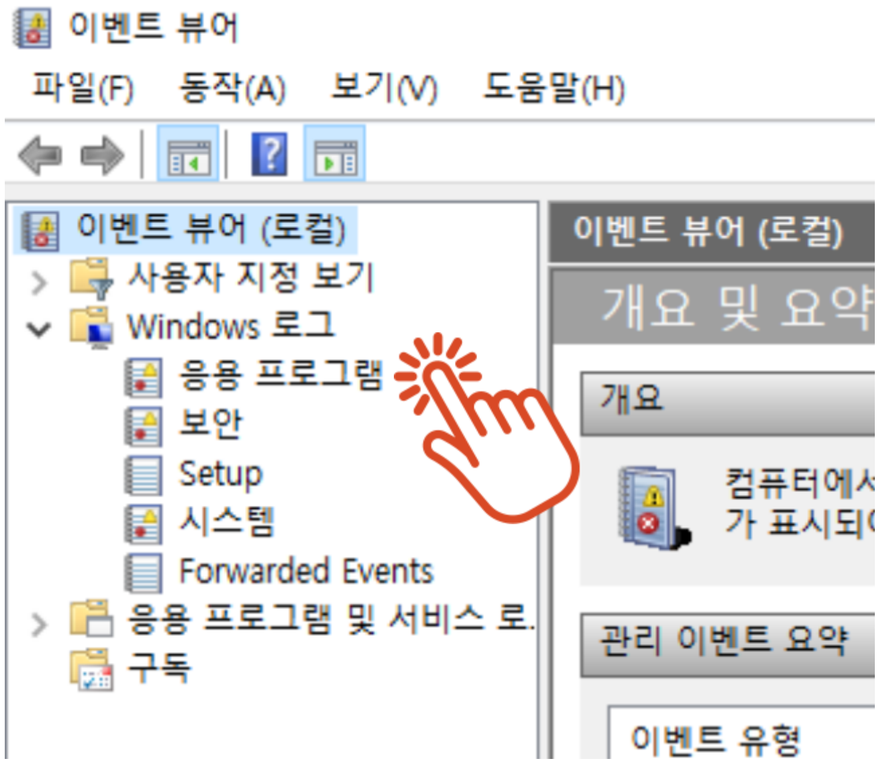
01 Event Log

이벤트 로그에는 윈도우에서 발생하는 다양한 이벤트들이 기록된다.

이벤트 로그를 확인하기 위해서는 이벤트 뷰어를 이용해야 한다.

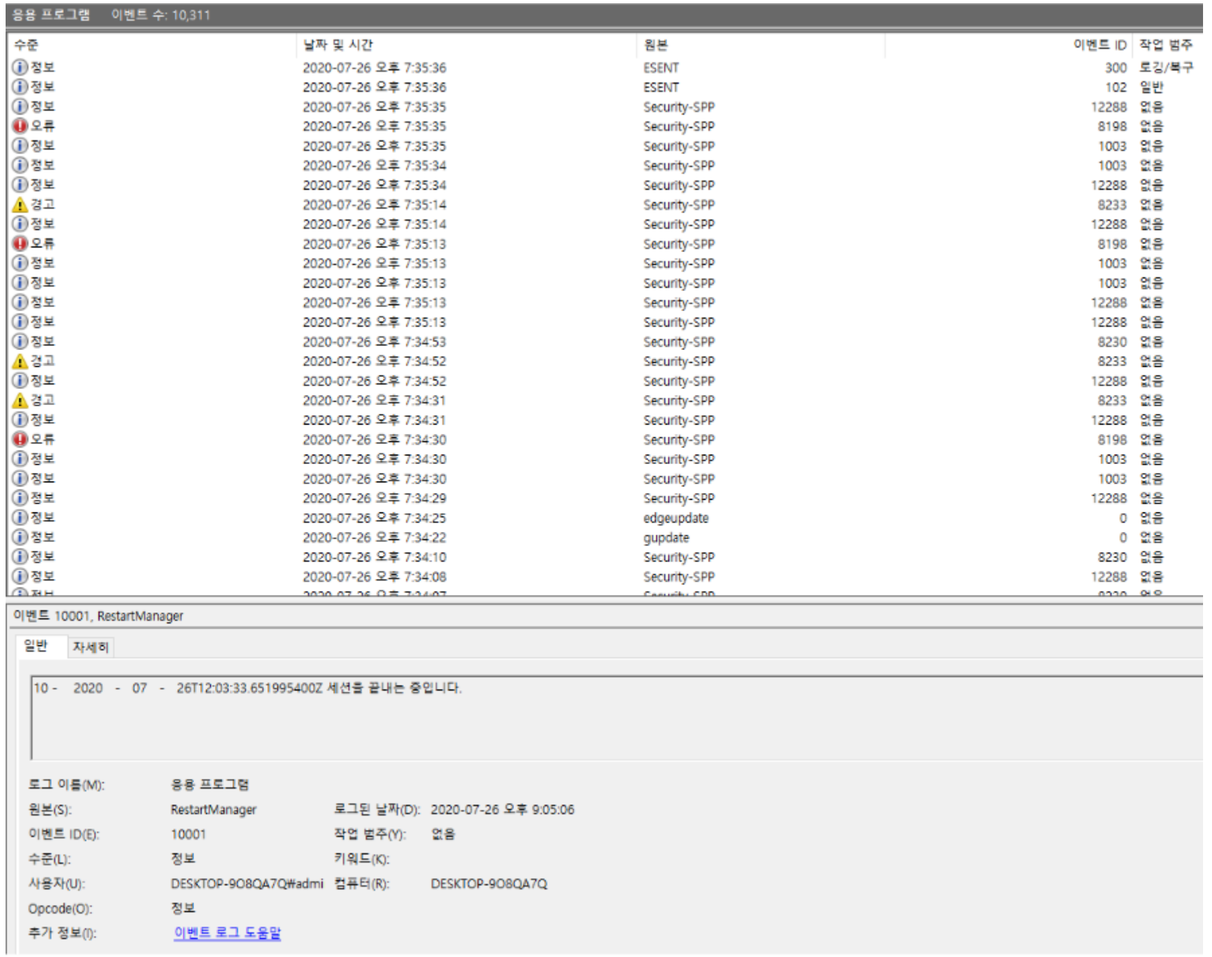


Event Log



- 응용 프로그램
- 보안
- Setup
- 시스템
- Forwarded Events

02 Event 유형


응용 프로그램 이벤트 수: 10,311

수준	날짜 및 시간	원본	이벤트 ID	작업 범주
정보	2020-07-26 오후 7:35:36	ESENT	300	로깅/복구
정보	2020-07-26 오후 7:35:36	ESENT	102	일반
정보	2020-07-26 오후 7:35:35	Security-SPP	12288	없음
오류	2020-07-26 오후 7:35:35	Security-SPP	8198	없음
정보	2020-07-26 오후 7:35:35	Security-SPP	1003	없음
정보	2020-07-26 오후 7:35:34	Security-SPP	1003	없음
정보	2020-07-26 오후 7:35:34	Security-SPP	12288	없음
경고	2020-07-26 오후 7:35:14	Security-SPP	8233	없음
정보	2020-07-26 오후 7:35:14	Security-SPP	12288	없음
오류	2020-07-26 오후 7:35:13	Security-SPP	8198	없음
정보	2020-07-26 오후 7:35:13	Security-SPP	1003	없음
정보	2020-07-26 오후 7:35:13	Security-SPP	1003	없음
정보	2020-07-26 오후 7:35:13	Security-SPP	12288	없음
정보	2020-07-26 오후 7:35:13	Security-SPP	12288	없음
정보	2020-07-26 오후 7:34:53	Security-SPP	8230	없음
경고	2020-07-26 오후 7:34:52	Security-SPP	8233	없음
정보	2020-07-26 오후 7:34:52	Security-SPP	12288	없음
경고	2020-07-26 오후 7:34:31	Security-SPP	8233	없음
정보	2020-07-26 오후 7:34:31	Security-SPP	12288	없음
오류	2020-07-26 오후 7:34:30	Security-SPP	8198	없음
정보	2020-07-26 오후 7:34:30	Security-SPP	1003	없음
정보	2020-07-26 오후 7:34:30	Security-SPP	1003	없음
정보	2020-07-26 오후 7:34:29	Security-SPP	12288	없음
정보	2020-07-26 오후 7:34:25	edgeupdate	0	없음
정보	2020-07-26 오후 7:34:22	gupdate	0	없음
정보	2020-07-26 오후 7:34:10	Security-SPP	8230	없음
정보	2020-07-26 오후 7:34:08	Security-SPP	12288	없음

이벤트 10001, RestartManager

일반 자세히

10 - 2020 - 07 - 26T12:03:33.651995400Z 세션을 끝내는 중입니다.

로그 이름(M): 응용 프로그램
원본(S): RestartManager 로그된 날짜(D): 2020-07-26 오후 9:05:06
이벤트 ID(E): 10001 작업 범주(Y): 없음
수준(L): 정보 키워드(K):
사용자(U): DESKTOP-9O8QA7Q\#admi 컴퓨터(R): DESKTOP-9O8QA7Q
Opcode(O): 정보
추가 정보(I): 이벤트 로그 도움말


정보


경고


오류

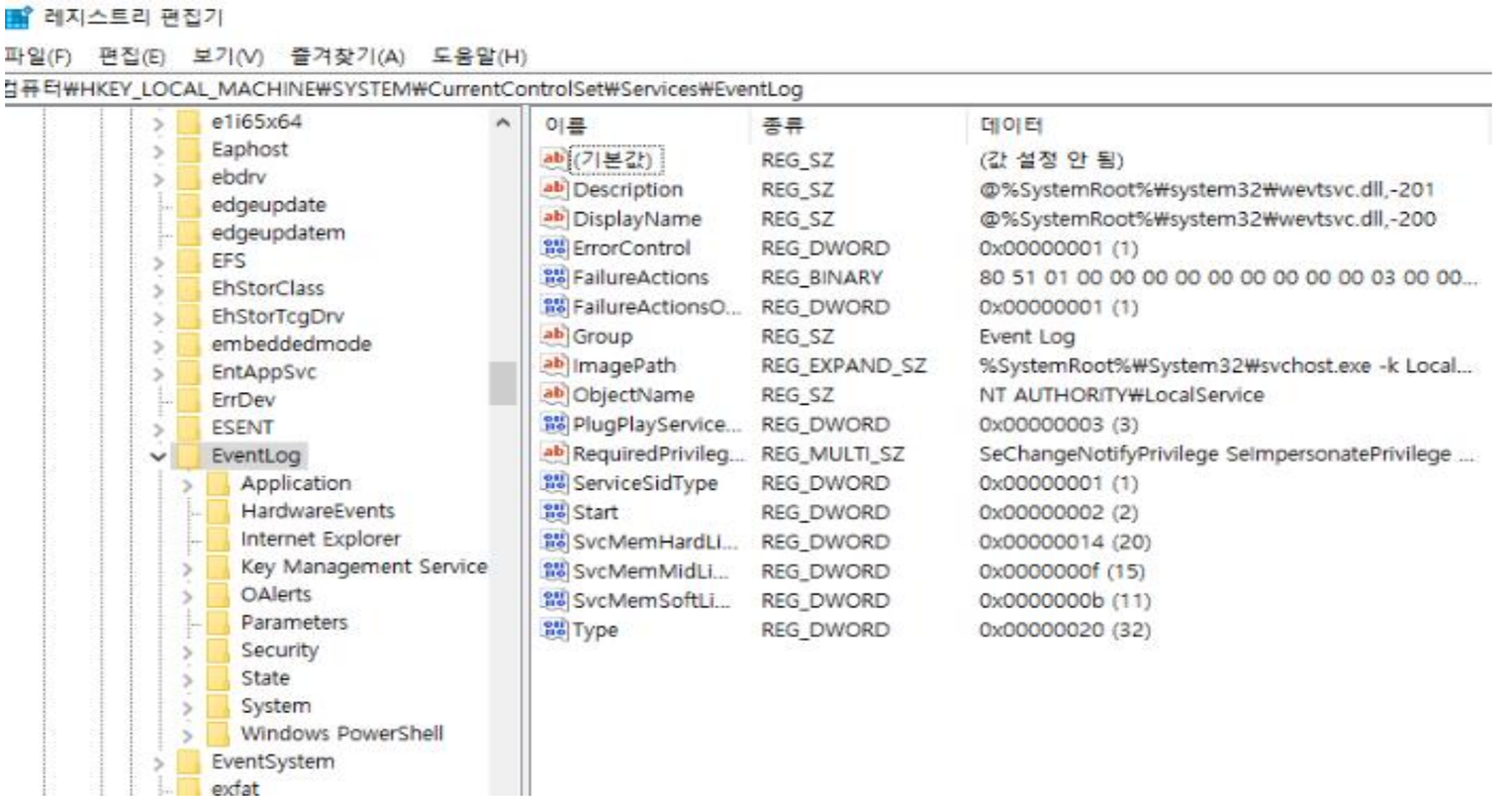
감사 성공


감사 실패

03 로그 설정

레지스트리 이용

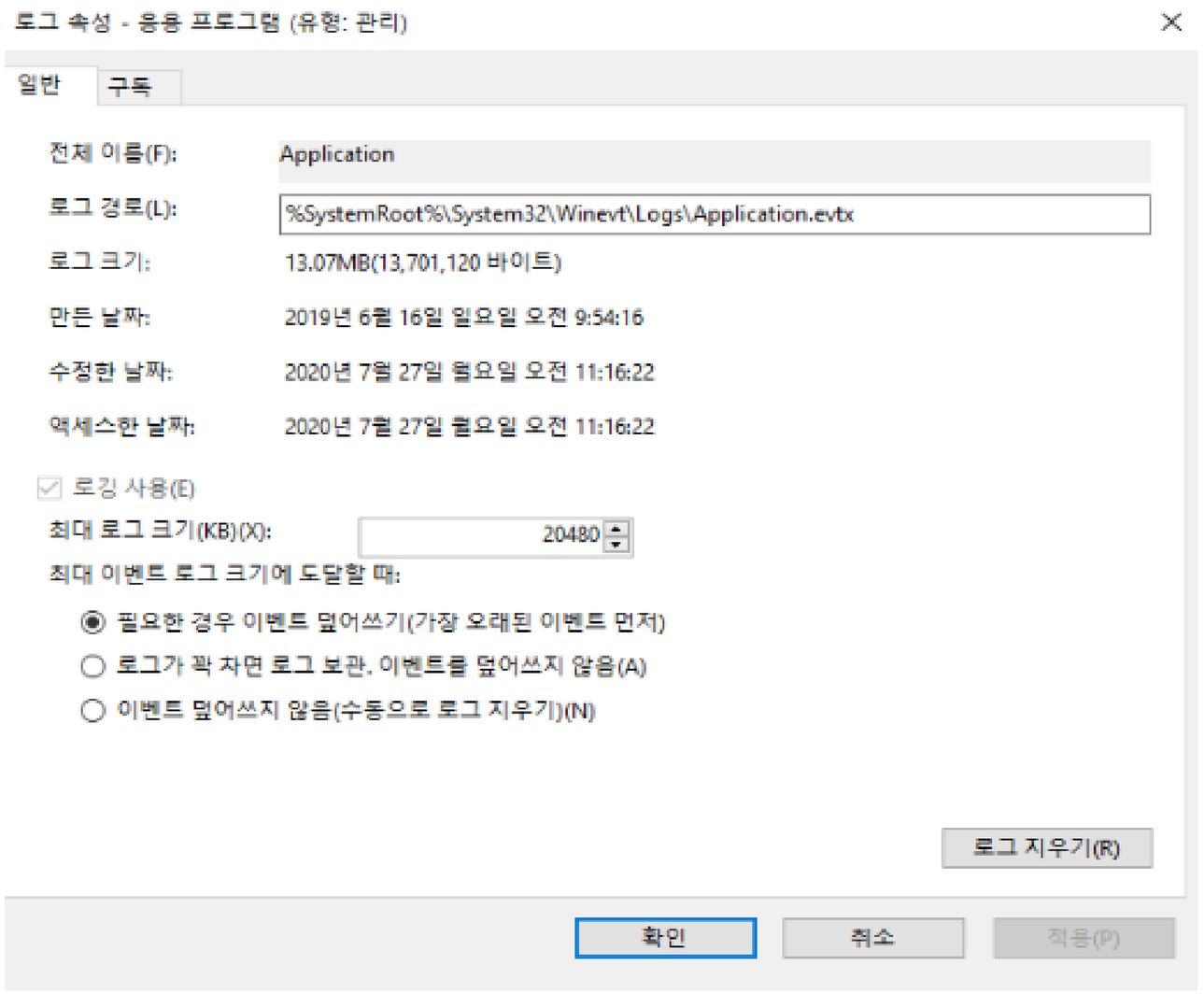
[실행] => regedit 입력 => HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩EventLog



03 로그 설정

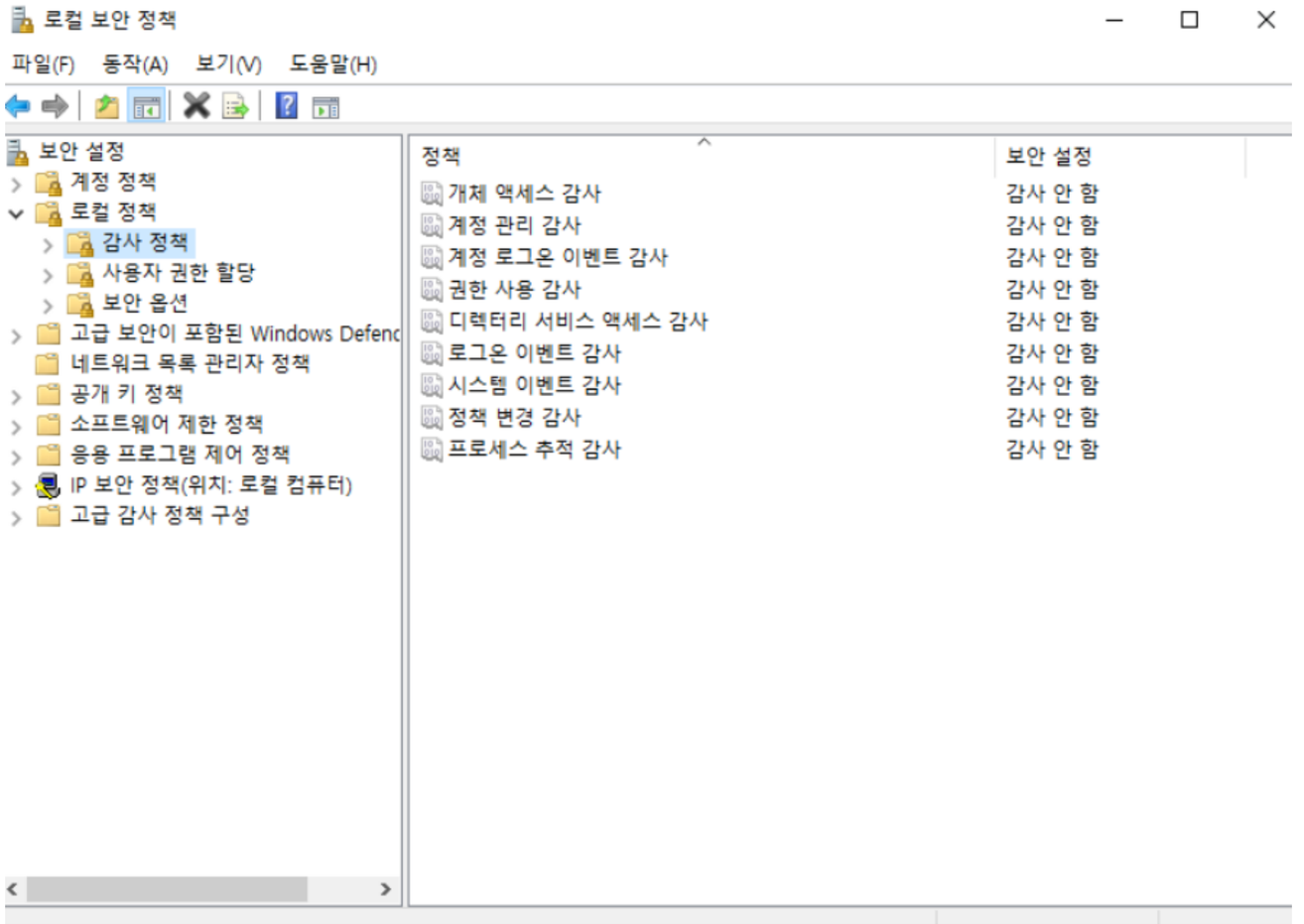
이벤트 뷰어 이용

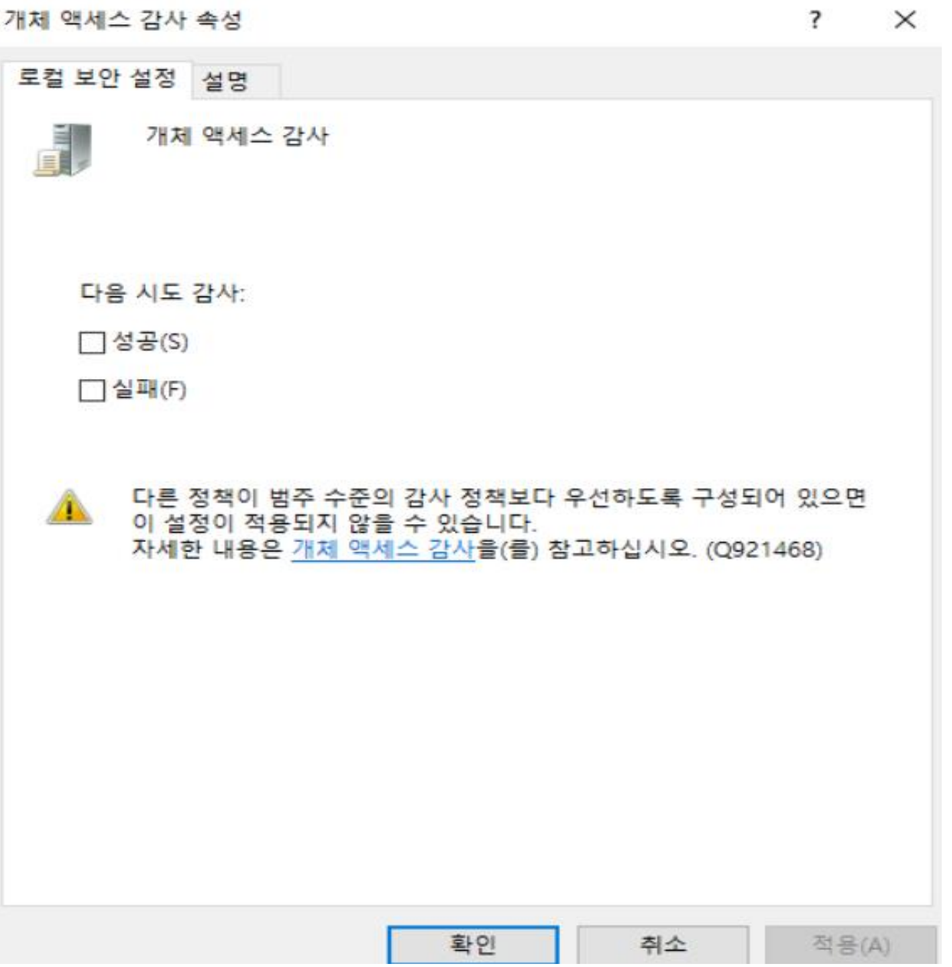
로그 우클릭 => 속성



04 이벤트 로그 감사 정책

[로컬 보안 정책] => [로컬 정책] => [감시 정책] => 감사 클릭 => 성공/실패 감사 설정





감사합니다.