

[Windows Event Log]

목차

01

Event Log

02

Event 유형

03

Log 설정

04

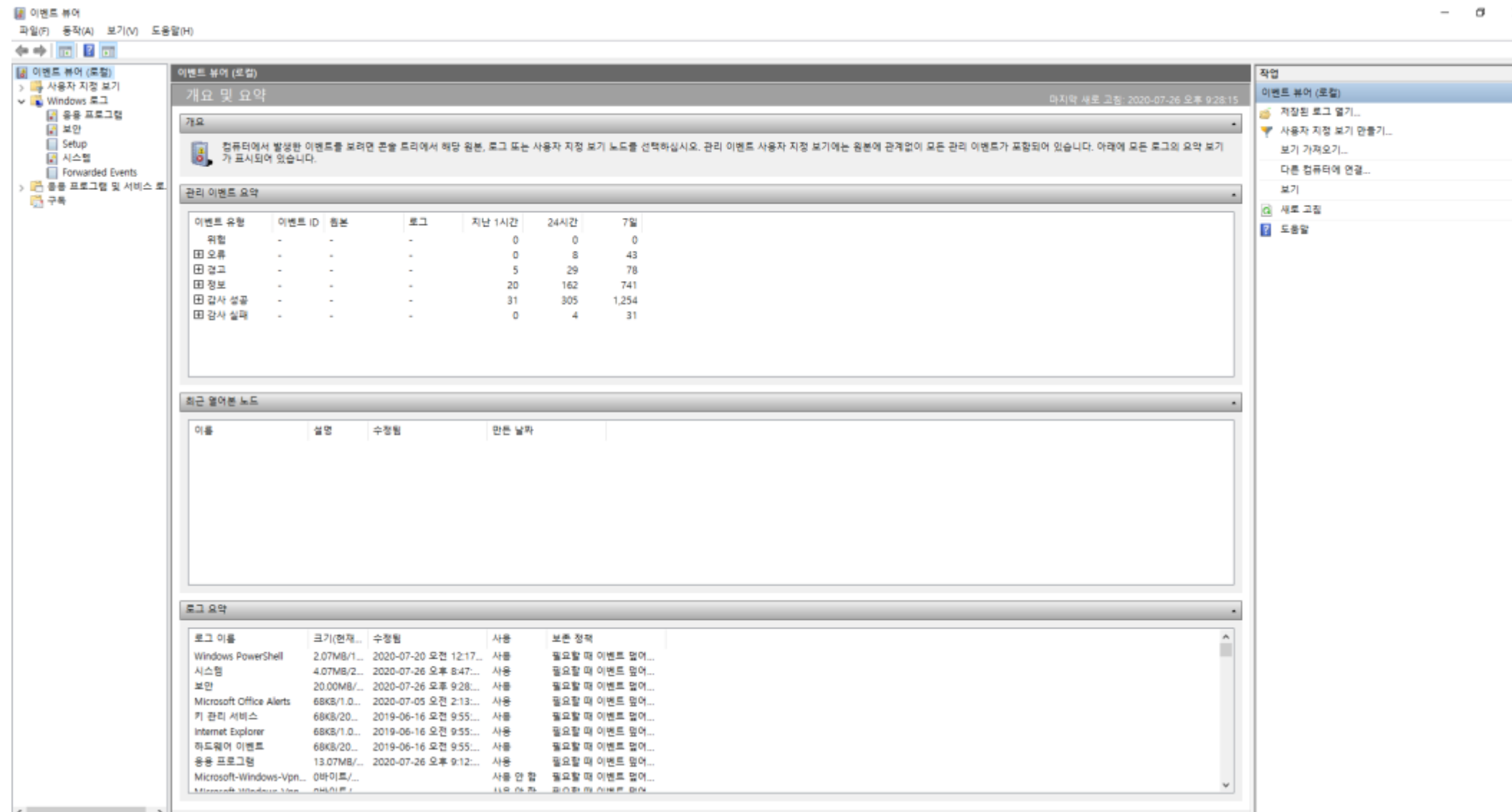
Event Log
감사 정책

01

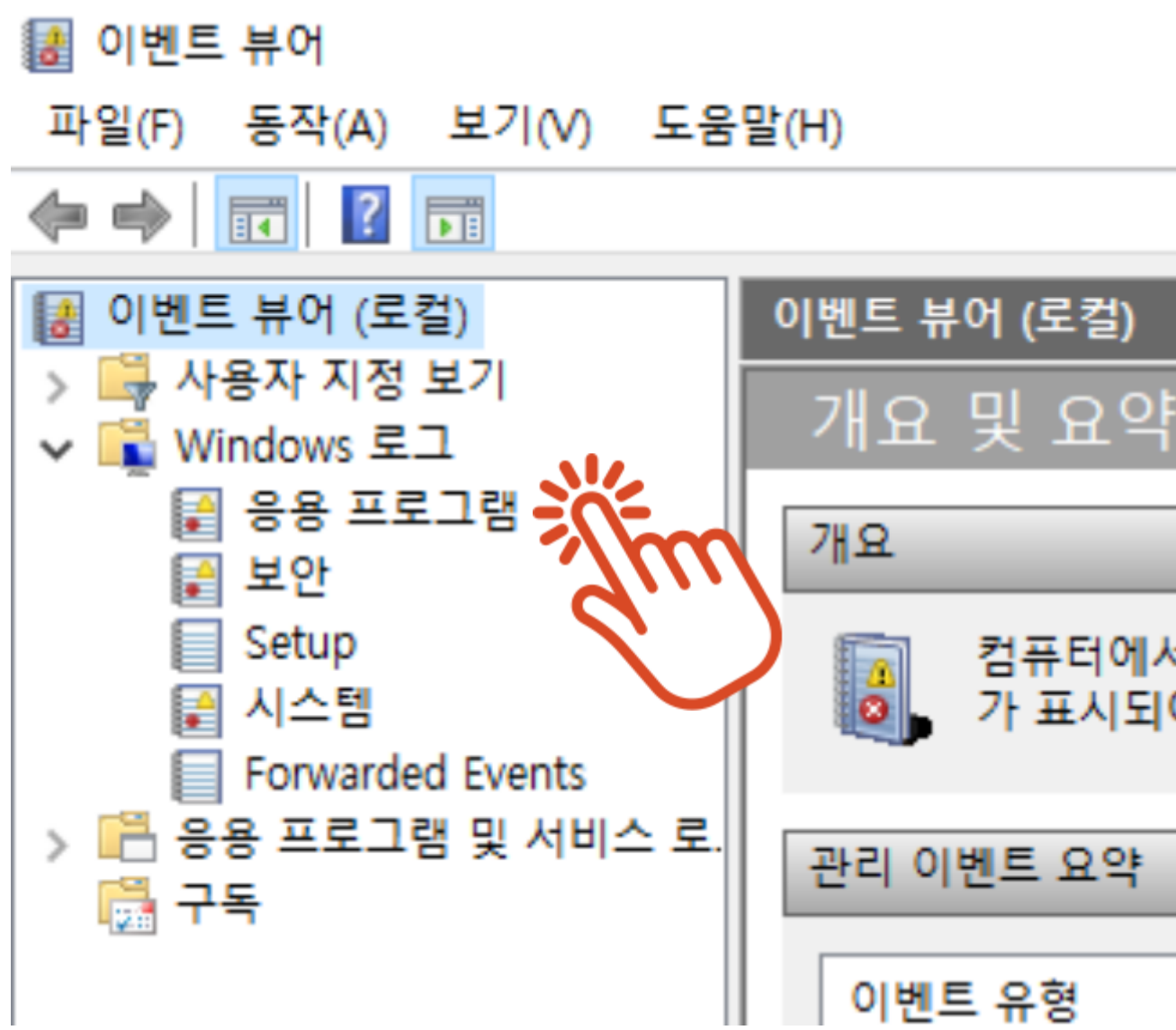
Event Log

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



정보



경고



오류



감사 성공



감사 실패

수준	날짜 및 시간	원본	이벤트 ID	작업 범주
정보	2020-07-26 오후 7:35:36	ESSENT	300	로그인/복구
정보	2020-07-26 오후 7:35:36	ESSENT	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
정보	2020-07-26 오후 7:34:07	Security-SPP	8230	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-908QA7Q#admi 컴퓨터(R): DESKTOP-908QA7Q
 Opcode(O): 정보
 추가 정보(I): [이벤트 로그 도움말](#)

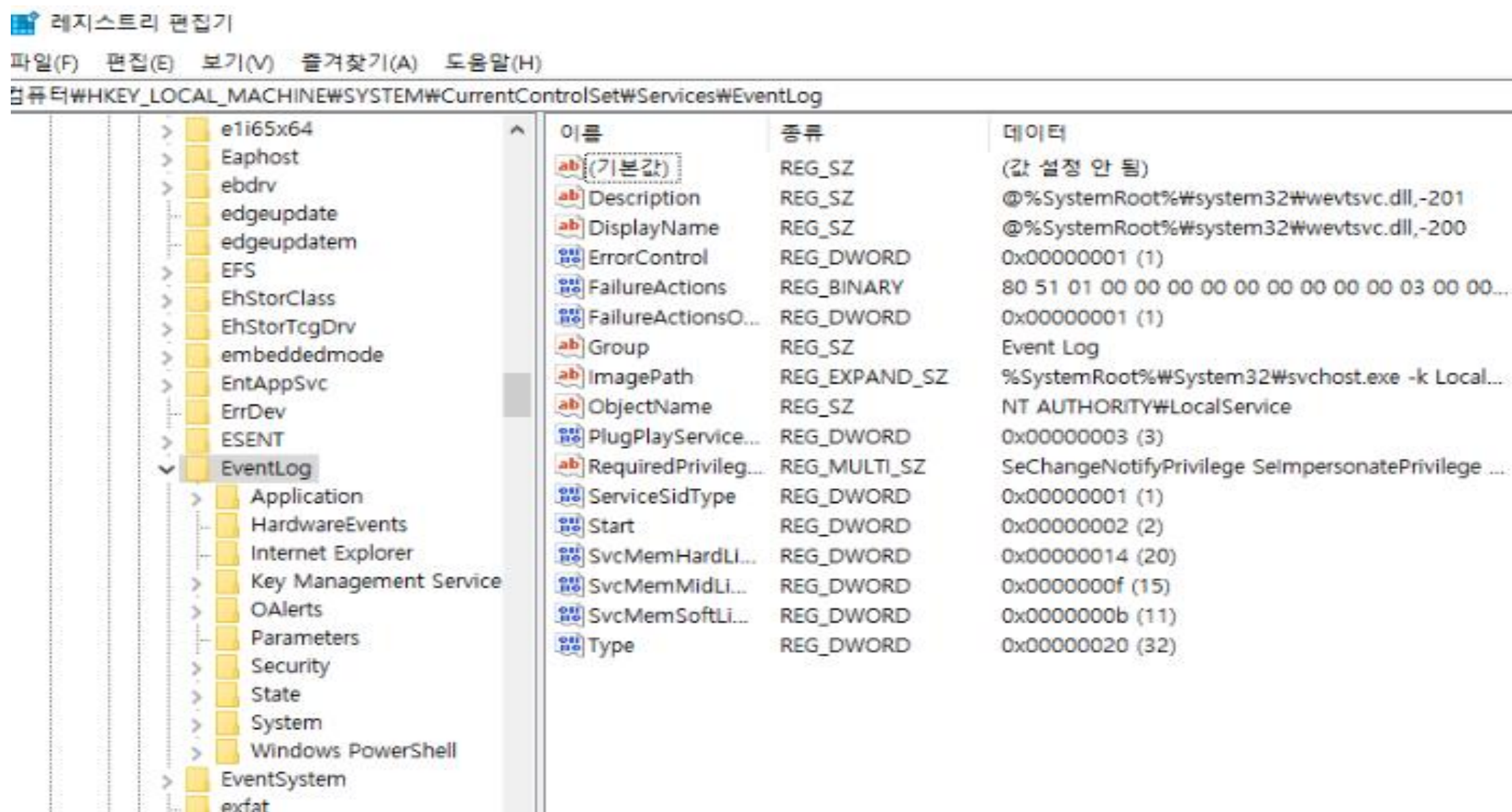
03

로그 설정



레지스트리 이용

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



03

로그 설정



이벤트 뷰어 이용

로그 우클릭 => 속성

로그 속성 - 응용 프로그램 (유형: 관리)

일반

구독

전체 이름(F): Application

로그 경로(L): %SystemRoot%\System32\Winevt\Logs\Application.evtx

로그 크기: 13.07MB(13,701,120 바이트)

만든 날짜: 2019년 6월 16일 일요일 오전 9:54:16

수정한 날짜: 2020년 7월 27일 월요일 오전 11:16:22

액세스한 날짜: 2020년 7월 27일 월요일 오전 11:16:22

☒ 로깅 사용(E)

최대 로그 크기(KB)(X): 20480

최대 이벤트 로그 크기에 도달할 때:

- ☒ 필요한 경우 이벤트 덮어쓰기(가장 오래된 이벤트 먼저)
- ☐ 로그가 꽉 차면 로그 보관. 이벤트를 덮어쓰지 않음(A)
- ☐ 이벤트 덮어쓰지 않음(수동으로 로그 지우기)(N)

로그 지우기(R)

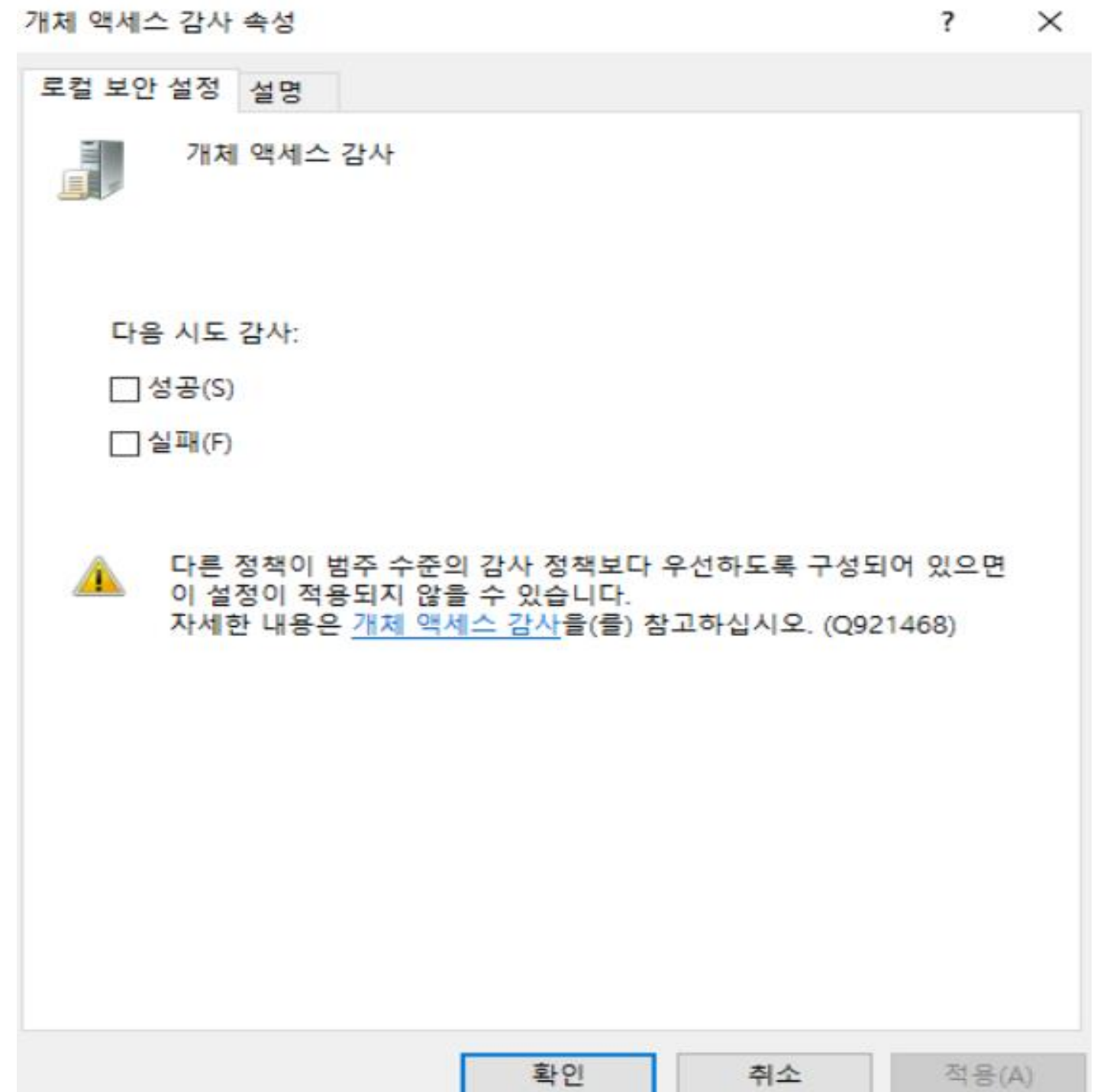
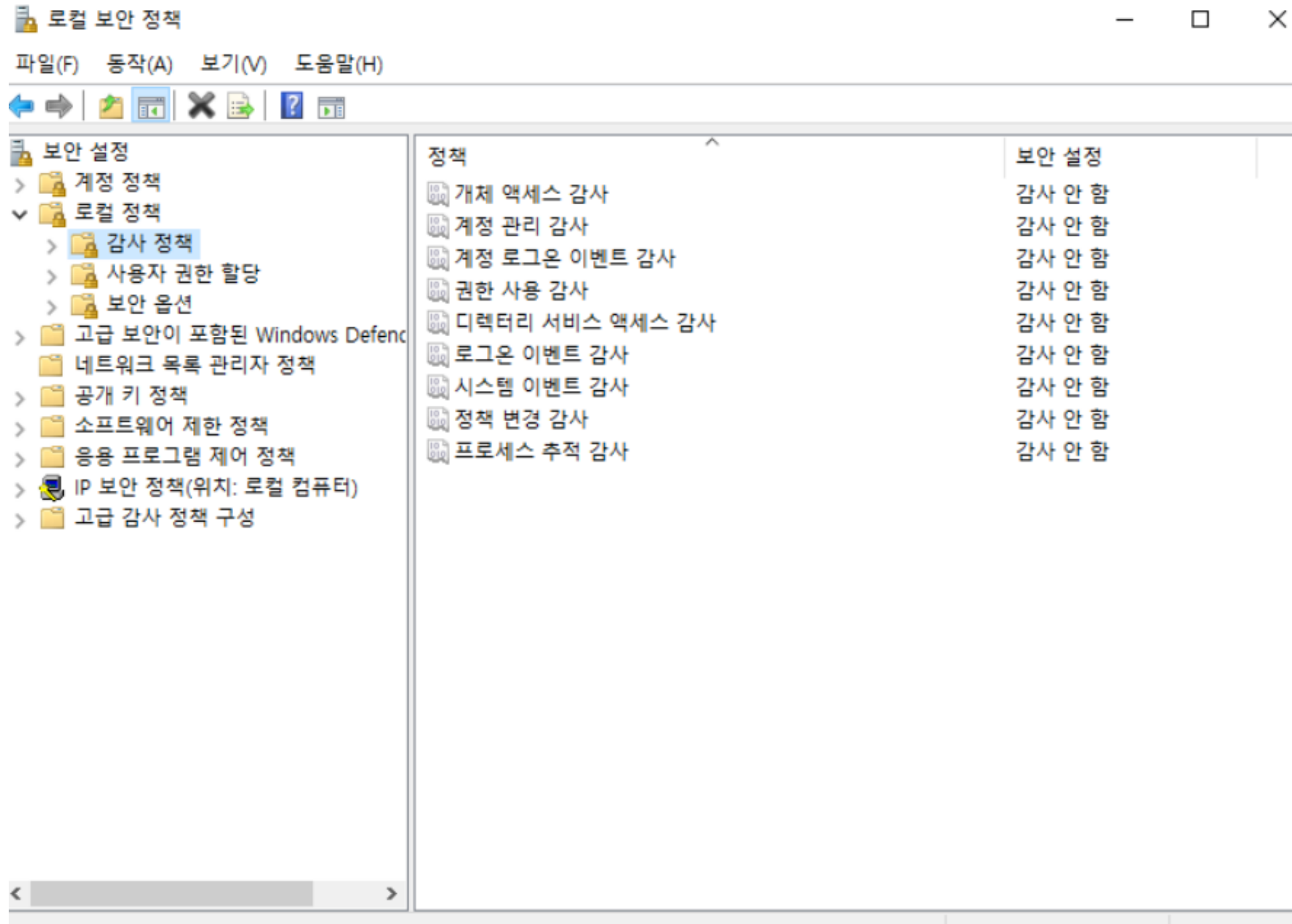
확인

취소

적용(P)

04 이벤트 로그 감사 정책

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



감사합니다.