windows 계정 로그온 기록하기

HYEONG HWAN, MUN/ 5월 3, 2019/ 미분류/ 0 comments

개발용으로 쓰는 Windows 머신이 있는데, 오늘 갑자기 RDP 연결이 안되더라.

디버그를 위해 콘솔로 접속 후 이벤트 뷰어를 보았다.

이벤트 뷰어에 표시된 에러 메세지는 아래와 같았음.

RD 세션 호스트 서버가 불완전한 연결을 많이 받았습니다. 시스템이 공격을 받을 수 있습니다.

Event ID 는 1006 번.

그런데 이 머신은 방화벽 설정이 잘 되어있고, 나 이외에는 접속하는 사람이 없다.
네트워크 통신을 확인해 보았는데, 이상한 연결도 없었다.

아무튼 내가 취한 조치사항은 아래와 같음.

1) 운영체제 업데이트

2) 윈도우 로그인 기록 남기기. (성공, 실패 모두)

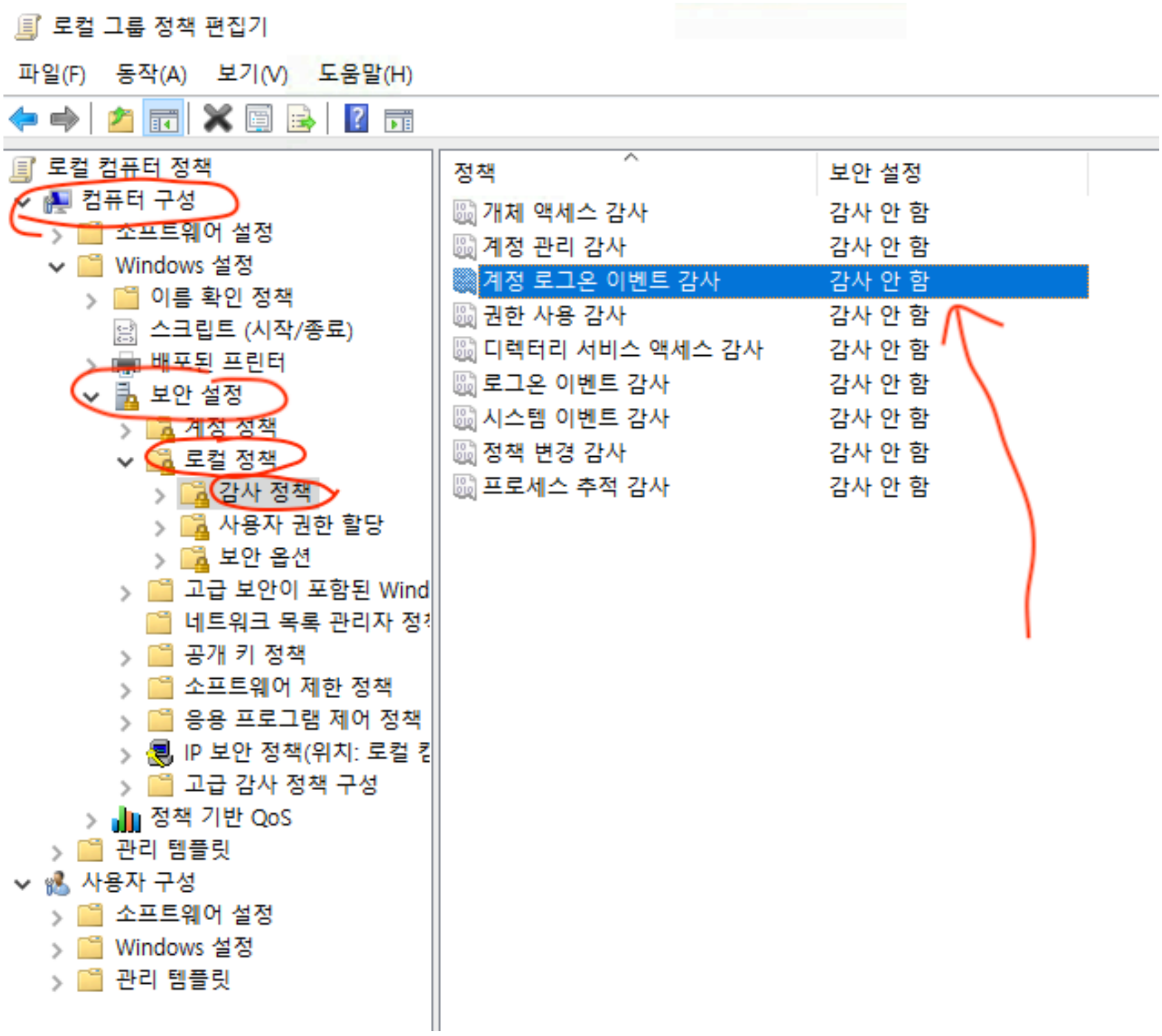
Windows 계정 로그온 기록하는 방법

```
시작 -> 실행 -> gpedit.msc
```

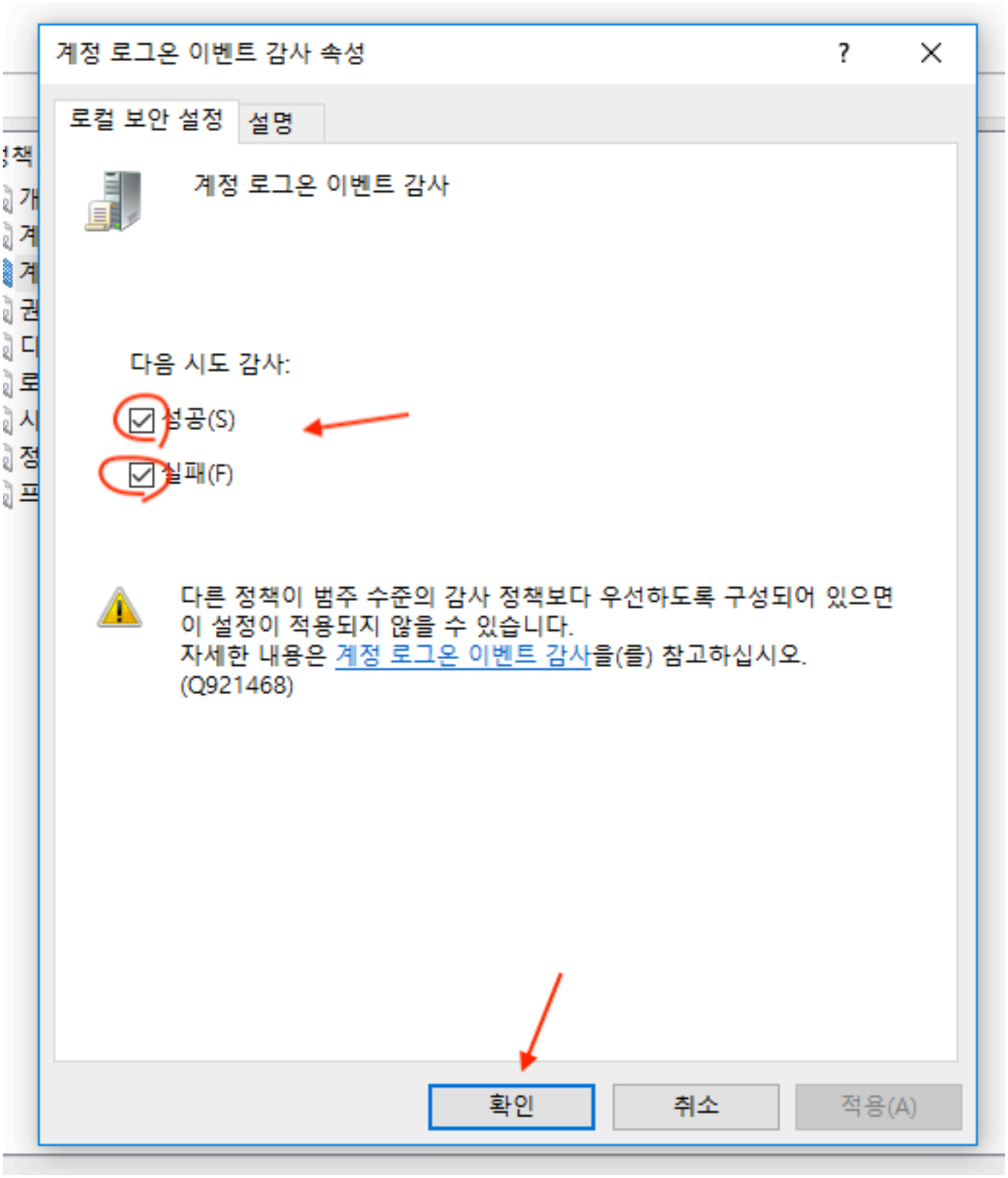
로컬 그룹 정책 편집기가 켜진다.

(이 Group Policy 를 수정해서 윈도우의 많은 부분을 튜닝할 수 있다. 웹서버나 미디어 서버 운영할 때, 통신 속도제한 거는 기능을 설정하면 운영에 도움이 된다.)

아무튼 지금은 로그인 부분만 건드리겠다.



계정 로그온 이벤트 감사 부분을 더블클릭한다.



“성공”, “실패” 체크 후 확인을 클릭한다.

운영 예시

제 Mac 컴퓨터에서 Windows 서버에 원격 접속을 시도함. 제 Mac 컴퓨터의 이름은 NC-IMAC.local 이며, 아이피는 121.***** 이다.
Win 컴퓨터의 이름은 V-WIN10 이며, 로그인 계정은 Lael 이다.

보안 이벤트 수: 24,317 (!) 새 이벤트를 사용할 수 있음

키워드	날짜 및 시간	원본	이벤트 ID	작업 범주	작업 코드
감사 성공	2019-05-03 오후 2:26:26	Microsoft W...	4776	Credential Validation	정보
감사 성공	2019-05-03 오후 2:26:26	Microsoft W...	4798	User Account Management	정보
감사 성공	2019-05-03 오후 2:26:25	Microsoft W...	4624	Logon	정보
감사 성공	2019-05-03 오후 2:26:25	Microsoft W...	4672	Special Logon	정보
감사 성공	2019-05-03 오후 2:26:25	Microsoft W...	4672	Special Logon	정보
감사 성공	2019-05-03 오후 2:26:25	Microsoft W...	4776	Credential Validation	정보
감사 실패	2019-05-03 오후 2:26:20	Microsoft W...	4776	Credential Validation	정보
감사 성공	2019-05-03 오후 2:26:11	Microsoft W...	4798	User Account Management	정보
감사 성공	2019-05-03 오후 2:26:10	Microsoft W...	4634	Logoff	정보
감사 성공	2019-05-03 오후 2:23:24	Microsoft W...	4672	Special Logon	정보
감사 성공	2019-05-03 오후 2:23:24	Microsoft W...	4624	Logon	정보

이벤트 4776, Microsoft Windows security auditing.

일반 자세히

컴퓨터에서 계정의 자격 증명에 대한 유효성 검사를 시도했습니다.

인증 패키지: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
로그온 계정: Lael2
원본 워크스테이션: NC-IMAC.local
오류 코드: 0xC0000064

<로그인 실패>

보안 이벤트 수: 24,317 (!) 새 이벤트를 사용할 수 있음

키워드	날짜 및 시간	원본	이벤트 ID	작업 범주	작업 코드
감사 성공	2019-05-03 오후 2:26:26	Microsoft W...	4776	Credential Validation	정보
감사 성공	2019-05-03 오후 2:26:26	Microsoft W...	4798	User Account Management	정보
감사 성공	2019-05-03 오후 2:26:25	Microsoft W...	4624	Logon	정보
감사 성공	2019-05-03 오후 2:26:25	Microsoft W...	4672	Special Logon	정보
감사 성공	2019-05-03 오후 2:26:25	Microsoft W...	4672	Special Logon	정보
감사 성공	2019-05-03 오후 2:26:25	Microsoft W...	4776	Credential Validation	정보
감사 실패	2019-05-03 오후 2:26:20	Microsoft W...	4776	Credential Validation	정보
감사 성공	2019-05-03 오후 2:26:11	Microsoft W...	4798	User Account Management	정보
감사 성공	2019-05-03 오후 2:26:10	Microsoft W...	4634	Logoff	정보
감사 성공	2019-05-03 오후 2:23:24	Microsoft W...	4672	Special Logon	정보
감사 성공	2019-05-03 오후 2:23:24	Microsoft W...	4624	Logon	정보

이벤트 4776, Microsoft Windows security auditing.

일반 자세히

컴퓨터에서 계정의 자격 증명에 대한 유효성 검사를 시도했습니다.

인증 패키지: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
로그온 계정: Lael
원본 워크스테이션: NC-IMAC.local
오류 코드: 0x0

<로그인 성공>

보안 이벤트 수: 24,317 (!) 새 이벤트를 사용할 수 있음

키워드	날짜 및 시간	원본	이벤트 ID	작업 범주	작업 코드
감사 성공	2019-05-03 오후 2:26:26	Microsoft W...	4776	Credential Validation	정보
감사 성공	2019-05-03 오후 2:26:26	Microsoft W...	4798	User Account Management	정보
감사 성공	2019-05-03 오후 2:26:25	Microsoft W...	4624	Logon	정보
감사 성공	2019-05-03 오후 2:26:25	Microsoft W...	4672	Special Logon	정보
감사 성공	2019-05-03 오후 2:26:25	Microsoft W...	4672	Special Logon	정보
감사 성공	2019-05-03 오후 2:26:25	Microsoft W...	4776	Credential Validation	정보
감사 실패	2019-05-03 오후 2:26:20	Microsoft W...	4776	Credential Validation	정보
감사 성공	2019-05-03 오후 2:26:11	Microsoft W...	4798	User Account Management	정보
감사 성공	2019-05-03 오후 2:26:10	Microsoft W...	4634	Logoff	정보
감사 성공	2019-05-03 오후 2:23:24	Microsoft W...	4672	Special Logon	정보
감사 성공	2019-05-03 오후 2:23:24	Microsoft W...	4624	Logon	정보

이벤트 4624, Microsoft Windows security auditing.

일반 자세히

새 로그온:
- 보안 ID: V-WIN10₩Lael
- 계정 이름: Lael
- 계정 도메인: V-WIN10
- 로그온 ID: 0x33CB44
- 연결된 로그온 ID: 0x0
- 네트워크 계정 이름: -
- 네트워크 계정 도메인: -
- 로그온 GUID: {00000000-0000-0000-0000-000000000000}

프로세스 정보:
- 프로세스 ID: 0x0
- 프로세스 이름: -

네트워크 정보:
- 워크스테이션 이름: NC-IMAC.local
- 원본 네트워크 주소: 121.[redacted]3
- 원본 포트: 0

<로그인 성공>

대응은 잘 한것 같으니, 상황을 좀 더 지켜봐야겠다.

관련

Ubuntu 에 fail2ban 을 설치하여 보안을 강화하기.

2015년 5월 9일

"fail2ban"에서