[Windows] [오류] 윈도우 원격 데스크톱 연결 인증 오류 CredSSP 암호화 Oracle 수정 때문일 수 있습니다.

원인

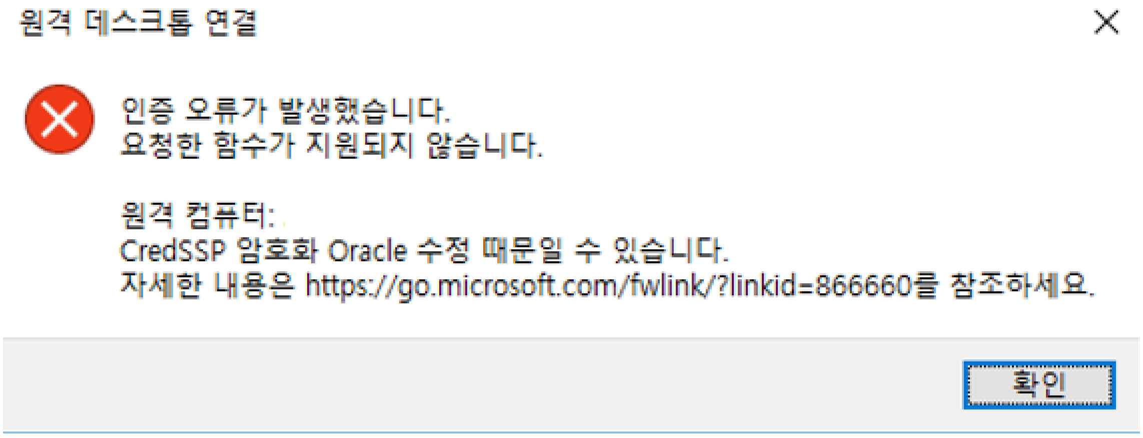
최근 마이크로소프트에서 배포한 보안 업데이트 적용으로 Windows Server에 원격 접근 이슈가 발생
보안 업데이트의 내용은 CredSSP버전에서 원격 코드 실행 취약성이 발견되어 배포되는 부분으로 클라이언트와 서버간의 인증 프로토콜이 강화되는 내용

오류화면

[Window Title]
원격 데스크톱 연결

[Content]
인증 오류가 발생했습니다.
요청한 함수가 지원되지 않습니다.

원격 컴퓨터:
CredSSP 암호화 오라클 수정 때문일 수 있습니다.
자세한 내용은 https://go.microsoft.com/fwlink/?linkid=866660를 참조하세요.



원격 데스크톱 연결

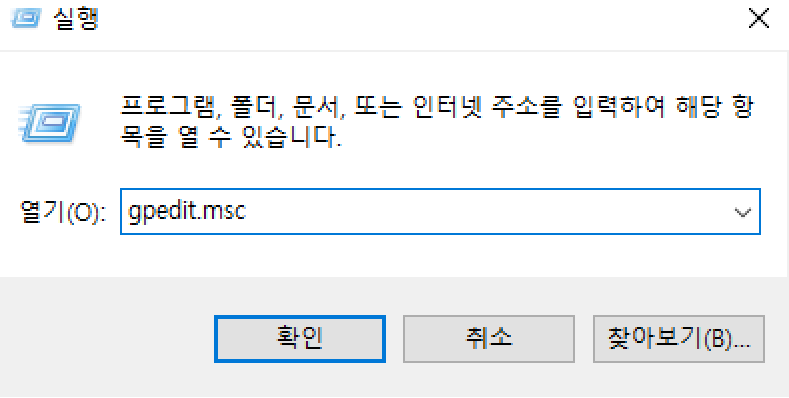
인증 오류가 발생했습니다.
요청한 함수가 지원되지 않습니다.

원격 컴퓨터:
CredSSP 암호화 Oracle 수정 때문일 수 있습니다.
자세한 내용은 https://go.microsoft.com/fwlink/?linkid=866660를 참조하세요.

원격 CredSSP 인증 오류 해결 방법 1

접속하는 Client PC 의 그룹정책 수정으로 강제 적용 방법

Wins + R 단축키를 사용하여 실행 창을 열고 "gpedit.msc"을 입력 후 확인



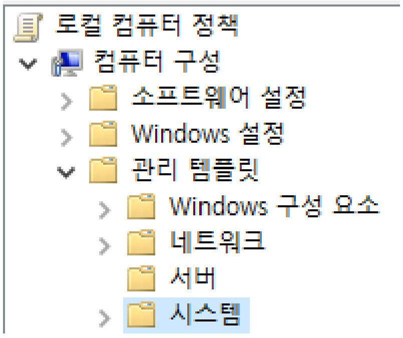
실행

프로그램, 폴더, 문서, 또는 인터넷 주소를 입력하여 해당 항목을 열 수 있습니다.

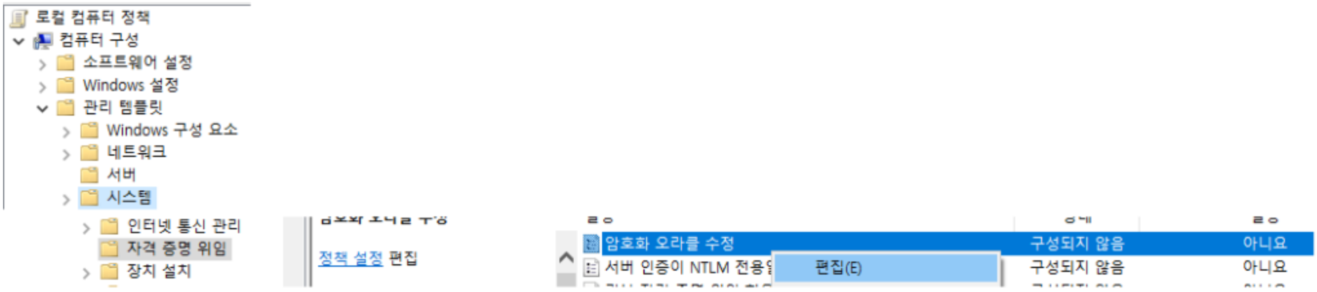
열기(O): gpedit.msc

확인
취소
찾아보기(B)...

컴퓨터 구성 -> 관리 템플릿 -> 시스템 -> 자격 증명 위임 -> Oracle 수정 암호화 편집 클릭

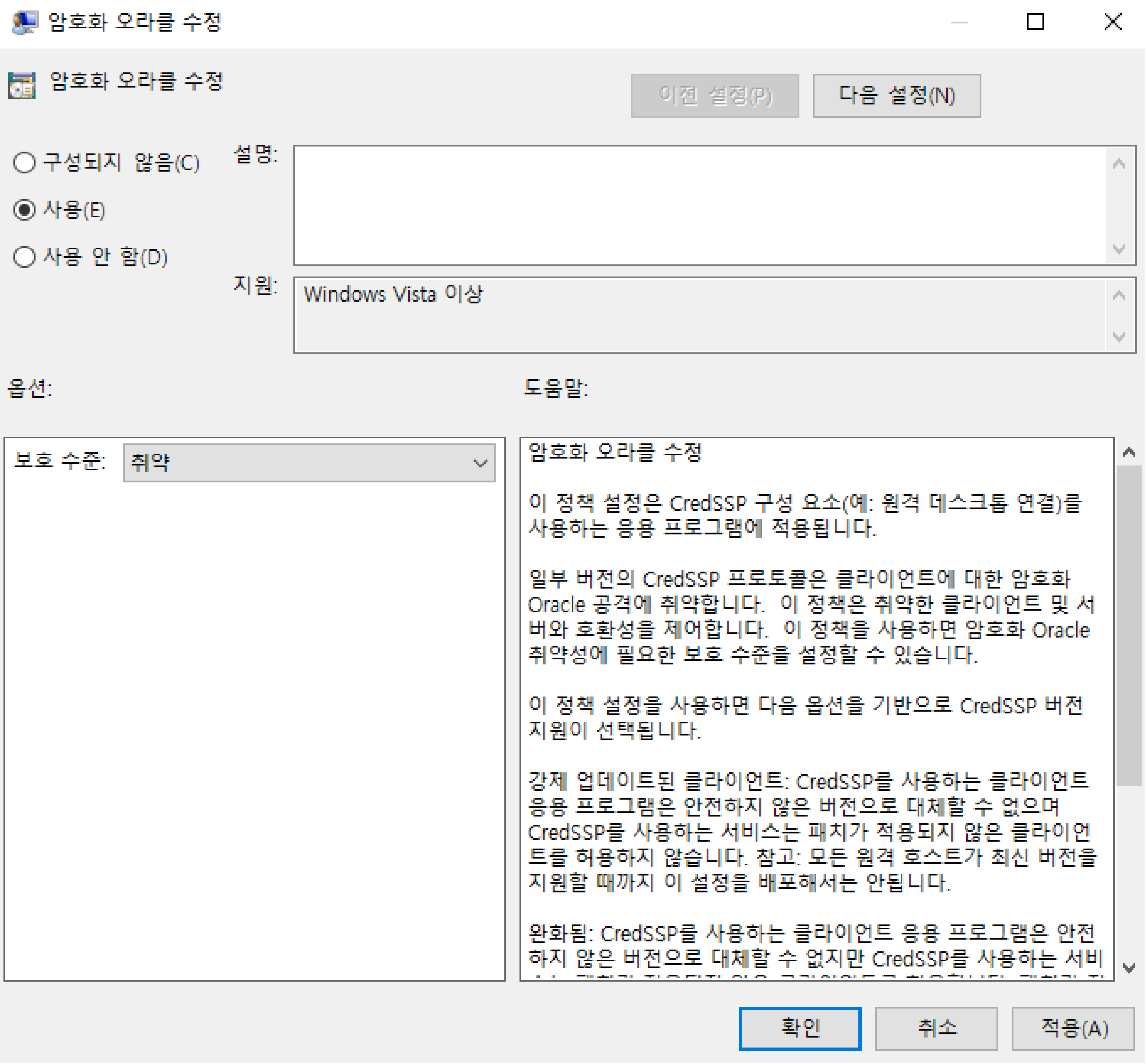


로컬 컴퓨터 정책
컴퓨터 구성
소프트웨어 설정
Windows 설정
관리 템플릿
Windows 구성 요소
네트워크
서버
시스템



로컬 컴퓨터 정책
컴퓨터 구성
소프트웨어 설정
Windows 설정
관리 템플릿
Windows 구성 요소
네트워크
서버
시스템
인터넷 통신 관리
자격 증명 위임
장치 설치
정책 설정 편집
암호화 오라클 수정
구성되지 않음
아니요
서버 인증이 NTLM 전용
구성되지 않음
아니요
편집(E)

사용 - 보호 수준: "취약" 선택후 확인 클릭



암호화 오라클 수정

○ 구성되지 않음(C)
● 사용(E)
○ 사용 안 함(D)

설명:

지원: Windows Vista 이상

옵션:

보호 수준: 취약

도움말:

암호화 오라클 수정

이 정책 설정은 CredSSP 구성 요소(예: 원격 데스크톱 연결)를 사용하는 응용 프로그램에 적용됩니다.

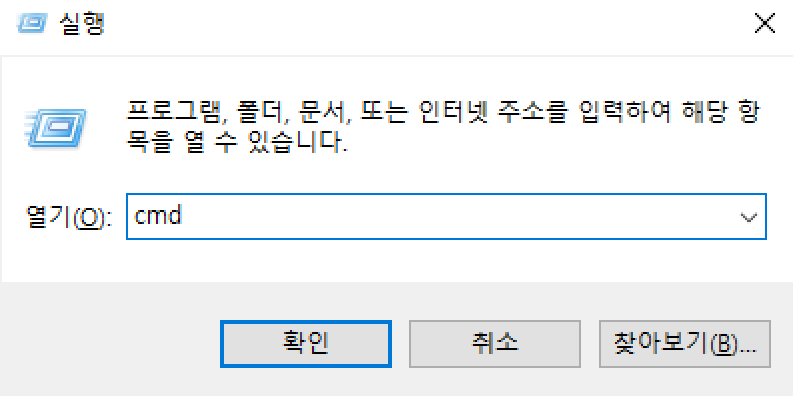
일부 버전의 CredSSP 프로토콜은 클라이언트에 대한 암호화 Oracle 공격에 취약합니다. 이 정책은 취약한 클라이언트 및 서버와 호환성을 제어합니다. 이 정책을 사용하면 암호화 Oracle 취약성에 필요한 보호 수준을 설정할 수 있습니다.

이 정책 설정을 사용하면 다음 옵션을 기반으로 CredSSP 버전 지원이 선택됩니다.

강제 업데이트된 클라이언트: CredSSP를 사용하는 클라이언트 응용 프로그램은 안전하지 않은 버전으로 대체할 수 없으며 CredSSP를 사용하는 서비스는 패치가 적용되지 않은 클라이언트를 허용하지 않습니다. 참고: 모든 원격 호스트가 최신 버전을 지원할 때까지 이 설정을 배포해서는 안됩니다.

완화됨: CredSSP를 사용하는 클라이언트 응용 프로그램은 안전하지 않은 버전으로 대체할 수 없지만 CredSSP를 사용하는 서비

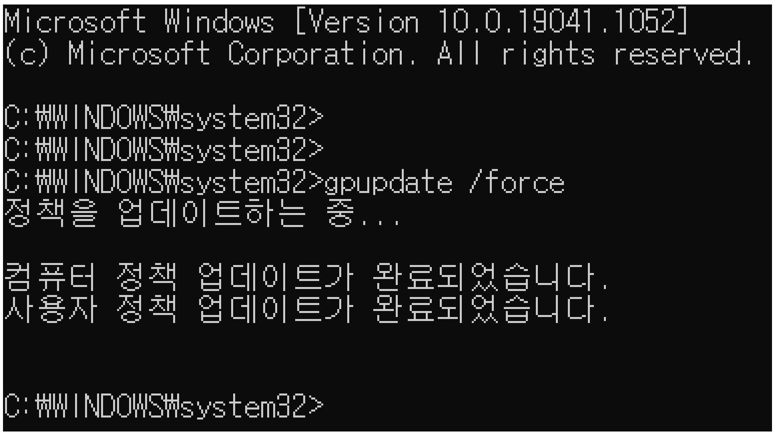
로컬 그룹 정책 편집기 창 종료
윈도우 키 + R 키를 이용하여 실행 창 활성화 => "cmd" 입력 후 엔터



프로그램, 폴더, 문서, 또는 인터넷 주소를 입력하여 해당 항목을 열 수 있습니다.

열기(O): cmd

gpupdate /force 입력 후 엔터



```
Microsoft Windows [Version 10.0.19041.1052]
(c) Microsoft Corporation. All rights reserved.

C:₩WINDOWS₩system32>
C:₩WINDOWS₩system32>
C:₩WINDOWS₩system32>gpupdate /force
정책을 업데이트하는 중...

컴퓨터 정책 업데이트가 완료되었습니다.
사용자 정책 업데이트가 완료되었습니다.


C:₩WINDOWS₩system32>
```

원격 데스크톱 연결 접속 확인

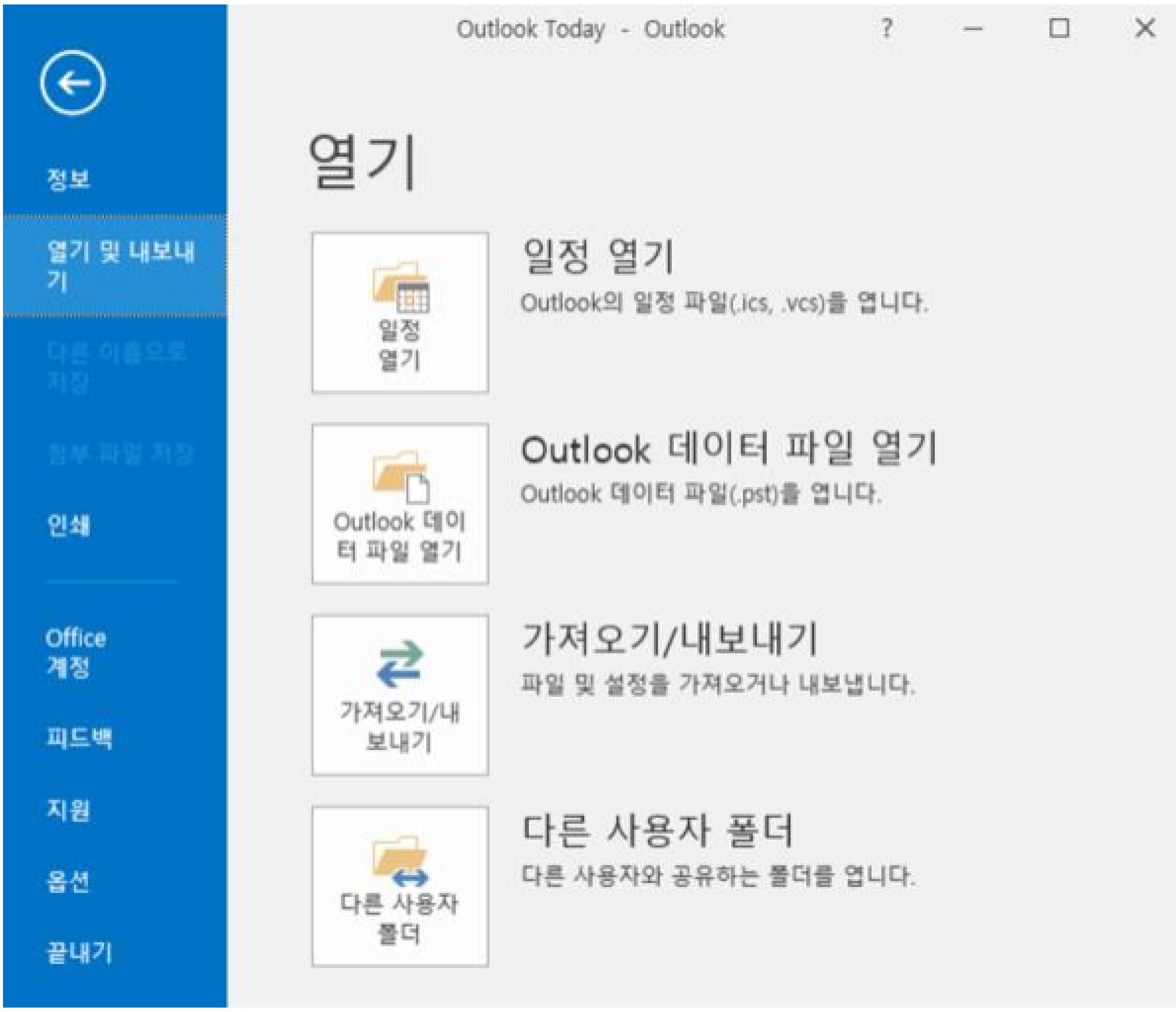
원격 CredSSP 인증 오류 해결 방법 2

Client: 사용하는 PC 및 노트북 최신 Windows Update 적용
Server: 최신 Windows Update 적용
원격 데스크톱 연결 접속 확인

Outlook 2016 PST 백업 및 복원 가이드

Outlook PST 백업하기

1. Outlook 파일 -> 열기 및 내보내기를 클릭합니다.


Outlook Today - Outlook
?
정보
열기 및 내보내기
다른 이름으로 저장
첨부 파일 저장
인쇄
Office 계정
피드백
지원
옵션
끝내기
열기
일정 열기
Outlook 데이터 파일 열기
가져오기/내보내기
다른 사용자 폴더

일정 열기

Outlook의 일정 파일(.ics, .vcs)을 엽니다.

Outlook 데이터 파일 열기

Outlook 데이터 파일(.pst)을 엽니다.

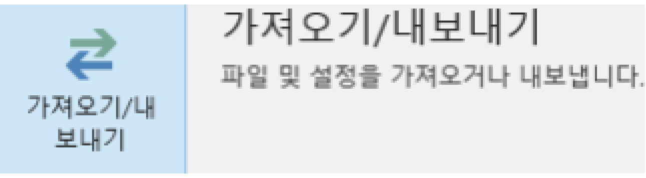
가져오기/내보내기

파일 및 설정을 가져오거나 내보냅니다.

다른 사용자 폴더

다른 사용자와 공유하는 폴더를 엽니다.

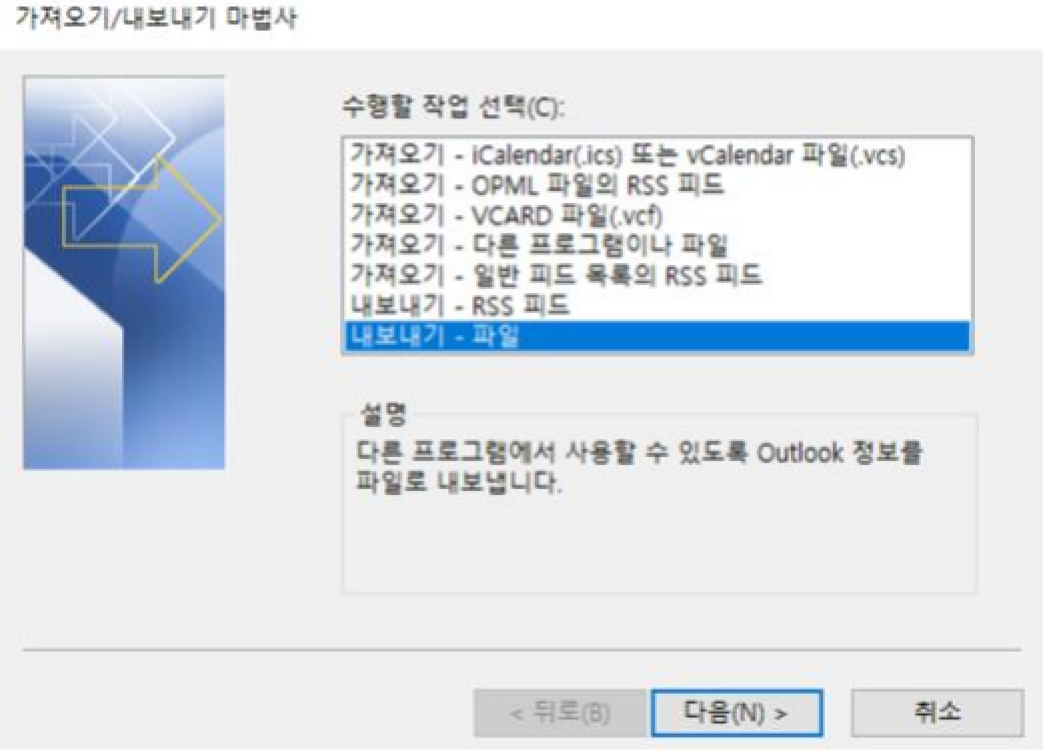
2. 가져오기/내보내기를 클릭합니다.



가져오기/내보내기

파일 및 설정을 가져오거나 내보냅니다.

3. 내보내기 – 파일을 선택하고 다음(N)을 클릭합니다.


가져오기/내보내기 마법사

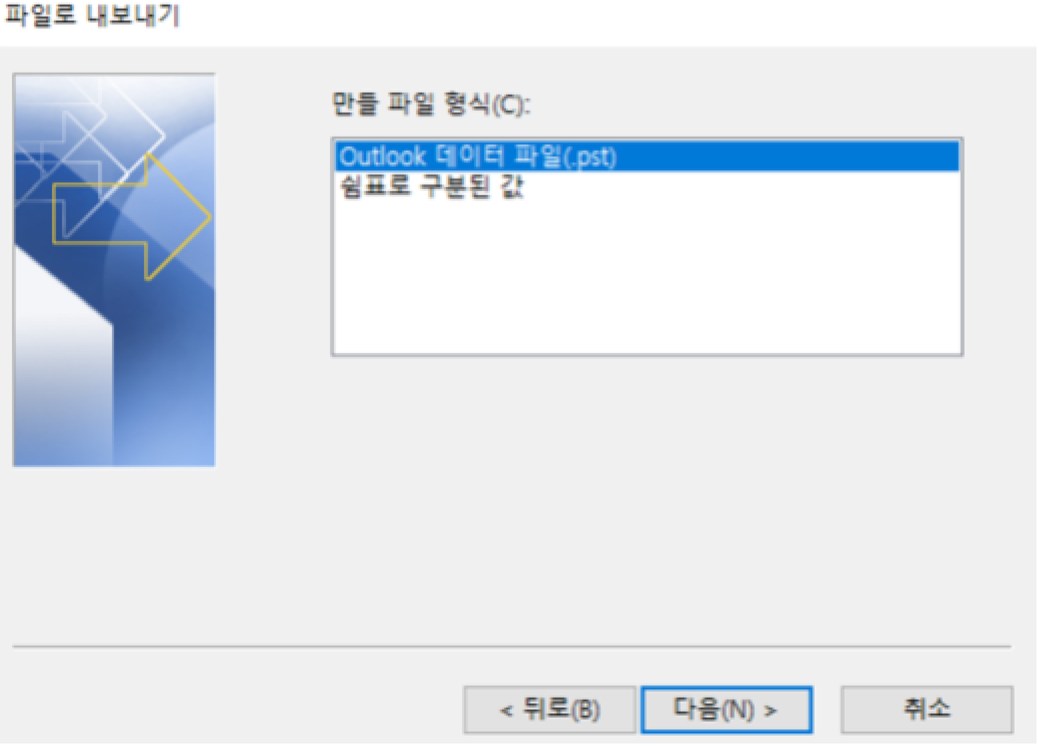
수행할 작업 선택(C):

- 가져오기 - iCalendar(.ics) 또는 vCalendar 파일(.vcs)
- 가져오기 - OPML 파일의 RSS 피드
- 가져오기 - VCARD 파일(.vcf)
- 가져오기 - 다른 프로그램이나 파일
- 가져오기 - 일반 피드 목록의 RSS 피드
- 내보내기 - RSS 피드
- 내보내기 - 파일

설명

다른 프로그램에서 사용할 수 있도록 Outlook 정보를 파일로 내보냅니다.

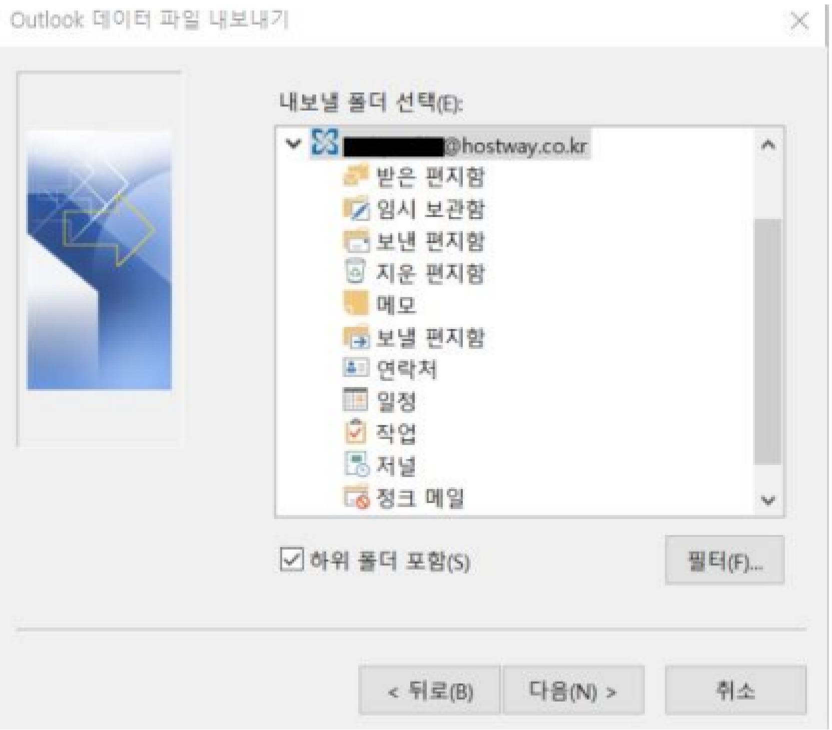
4. Outlook 데이터 파일(.pst)를 선택하고 다음(N)을 클릭합니다.


파일로 내보내기

만들 파일 형식(C):

- Outlook 데이터 파일(.pst)
- 쉼표로 구분된 값

5. 백업하고 싶은 상위 디렉토리를 선택하고 다음(N)을 클릭합니다.
(하위 폴더 포함(S)을 체크하도록 하며, 메일 계정을 선택해야 계정의 전체 데이터가 백업됩니다.)



Outlook 데이터 파일 내보내기

내보낼 폴더 선택(E):

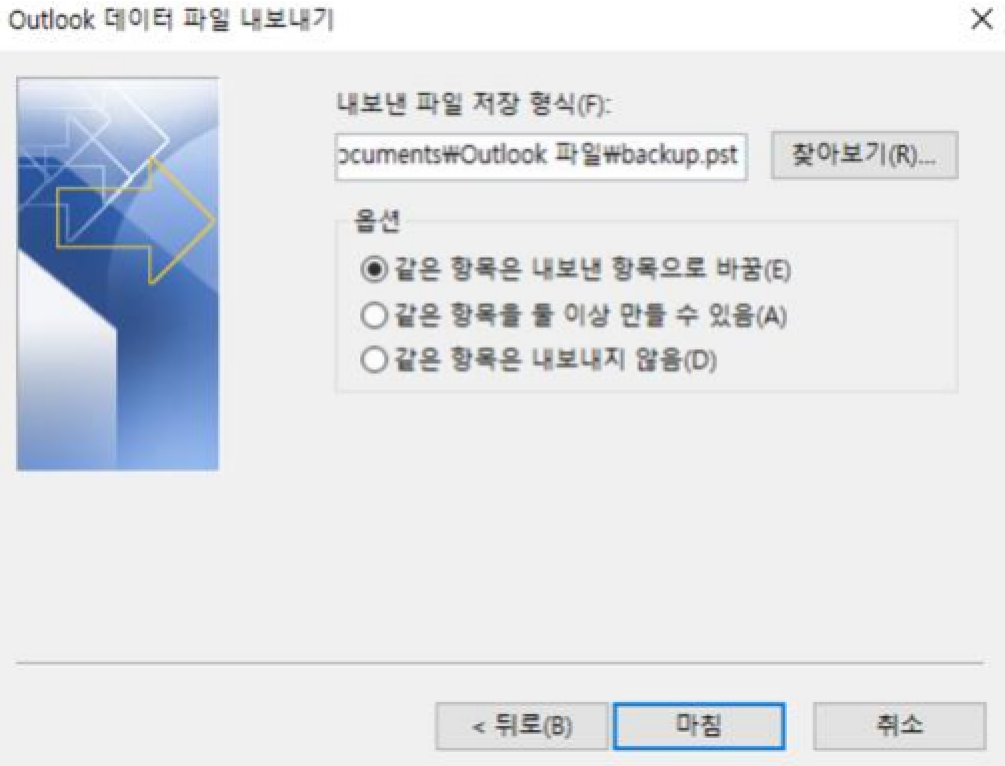
[redacted]@hostway.co.kr

받은 편지함
임시 보관함
보낸 편지함
지운 편지함
메모
보낼 편지함
연락처
일정
작업
저널
정크 메일

☑ 하위 폴더 포함(S)

필터(F)...
< 뒤로(B)
다음(N) >
취소

6. 저장할 위치를 선택하고 마침을 클릭합니다.



Outlook 데이터 파일 내보내기

내보낸 파일 저장 형식(F):

ɔcuments₩Outlook 파일₩backup.pst

찾아보기(R)...

옵션

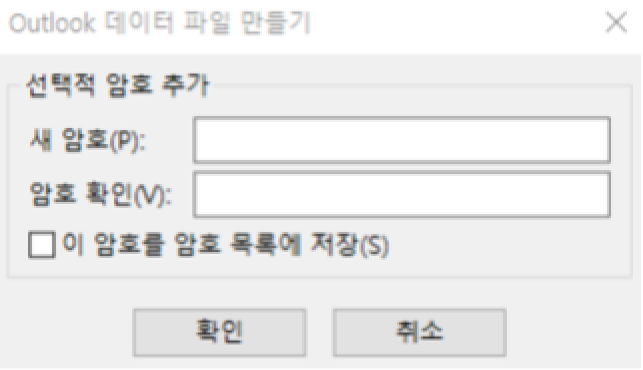
● 같은 항목은 내보낸 항목으로 바꿈(E)

○ 같은 항목을 둘 이상 만들 수 있음(A)

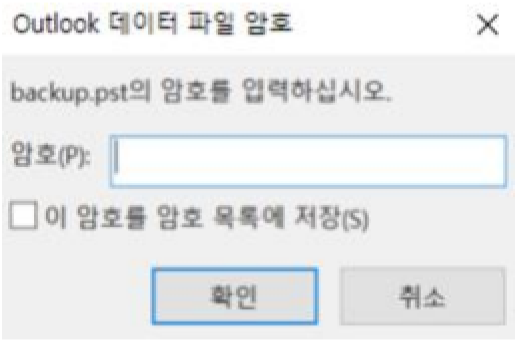
○ 같은 항목은 내보내지 않음(D)

< 뒤로(B)
마침
취소

7. 저장할 파일의 암호를 지정하거나 필요 없다면 미 입력 후 확인을 클릭합니다.


Outlook 데이터 파일 만들기
선택적 암호 추가
새 암호(P):
암호 확인(V):
☐ 이 암호를 암호 목록에 저장(S)
확인
취소

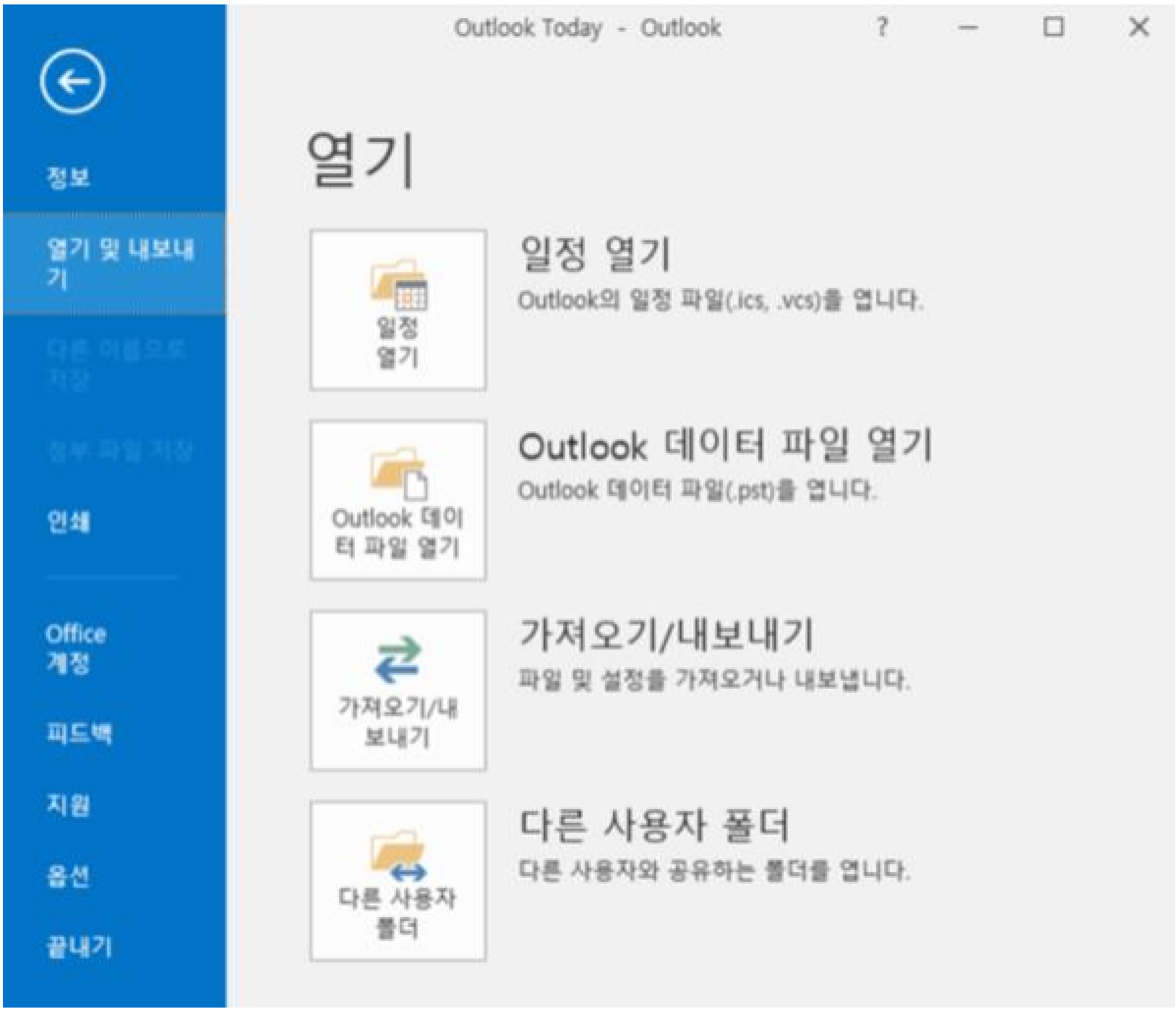
8. 암호를 입력하였다면 한번 더 입력하여 줍니다.


Outlook 데이터 파일 암호
암호(P):
☐ 이 암호를 암호 목록에 저장(S)
확인
취소

backup.pst의 암호를 입력하십시오.

Outlook PST 복원하기

1. Outlook 파일 -> 열기 및 내보내기를 클릭합니다.


Outlook Today - Outlook
정보
열기 및 내보내기
다른 이름으로 저장
첨부 파일 저장
인쇄
Office 계정
피드백
지원
옵션
끝내기
열기
일정 열기
Outlook 데이터 파일 열기
가져오기/내보내기
다른 사용자 폴더

일정 열기

Outlook의 일정 파일(.ics, .vcs)을 엽니다.

Outlook 데이터 파일 열기

Outlook 데이터 파일(.pst)을 엽니다.

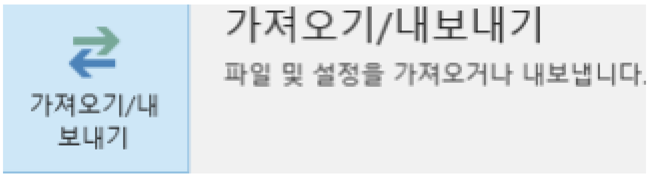
가져오기/내보내기

파일 및 설정을 가져오거나 내보냅니다.

다른 사용자 폴더

다른 사용자와 공유하는 폴더를 엽니다.

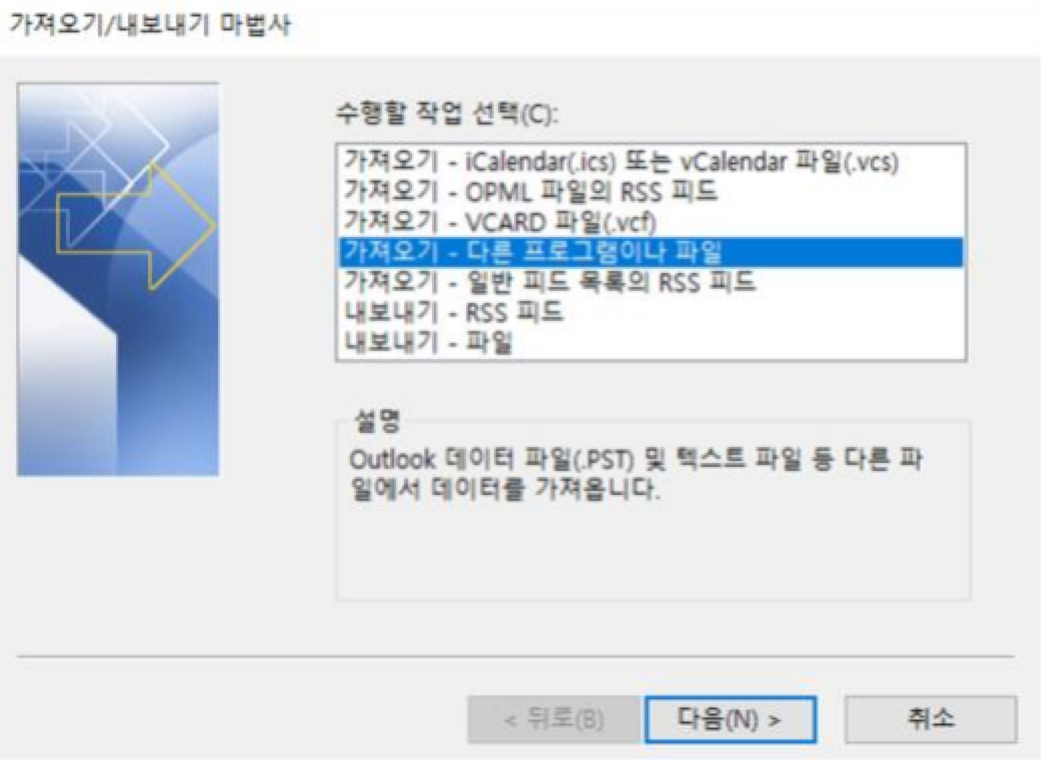
2. 가져오기/내보내기를 클릭합니다.



가져오기/내보내기

파일 및 설정을 가져오거나 내보냅니다.

3. 가져오기 – 다른 프로그램이나 파일을 선택하고 다음(N)을 클릭합니다.


가져오기/내보내기 마법사

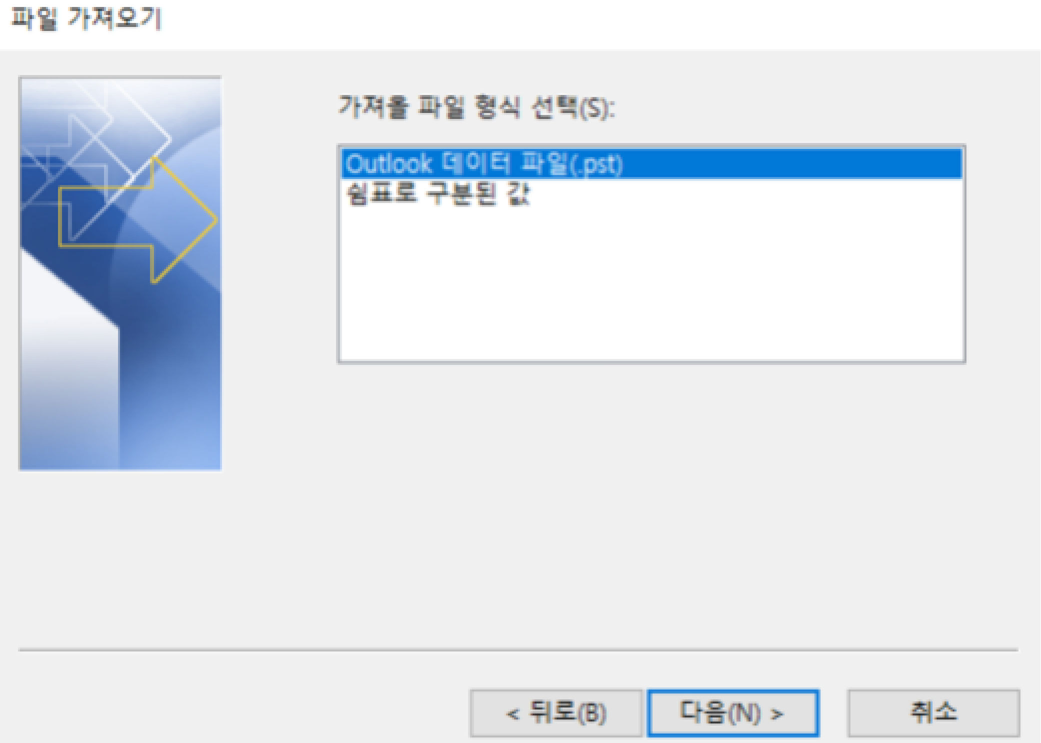
수행할 작업 선택(C):

- 가져오기 - iCalendar(.ics) 또는 vCalendar 파일(.vcs)
- 가져오기 - OPML 파일의 RSS 피드
- 가져오기 - VCARD 파일(.vcf)
- 가져오기 - 다른 프로그램이나 파일
- 가져오기 - 일반 피드 목록의 RSS 피드
- 내보내기 - RSS 피드
- 내보내기 - 파일

설명

Outlook 데이터 파일(.PST) 및 텍스트 파일 등 다른 파일에서 데이터를 가져옵니다.

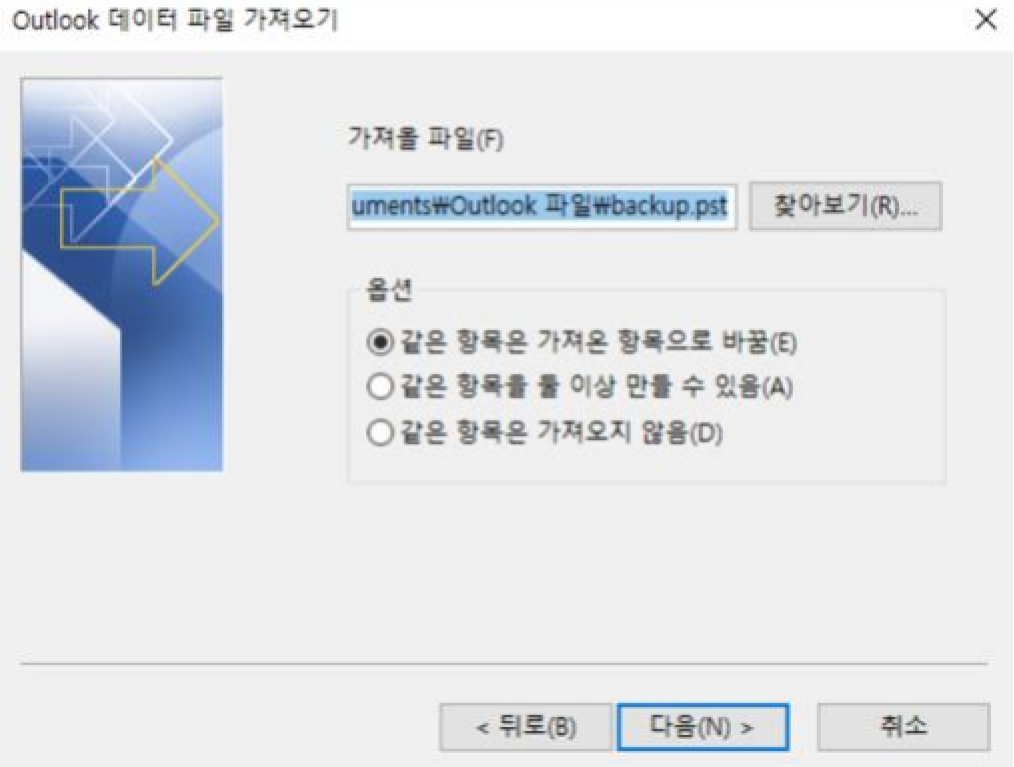
4. Outlook 데이터 파일(.pst)를 선택하고 다음(N)을 클릭합니다.


파일 가져오기

가져올 파일 형식 선택(S):

- Outlook 데이터 파일(.pst)
- 쉼표로 구분된 값

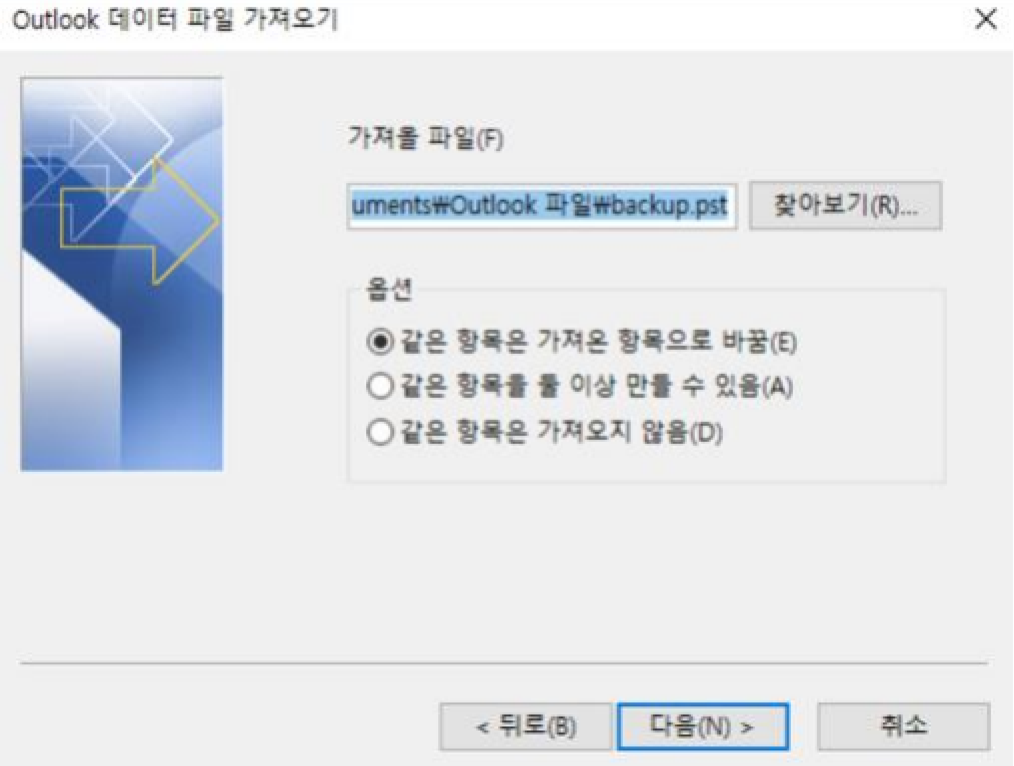
5. 백업 받았던 파일(.pst)을 지정하고 다음(N)을 클릭합니다.


Outlook 데이터 파일 가져오기
가져올 파일(F)
찾아보기(R)...
옵션
< 뒤로(B)
다음(N) >
취소

uments₩Outlook 파일₩backup.pst

● 같은 항목은 가져온 항목으로 바꿈(E)
○ 같은 항목을 둘 이상 만들 수 있음(A)
○ 같은 항목은 가져오지 않음(D)

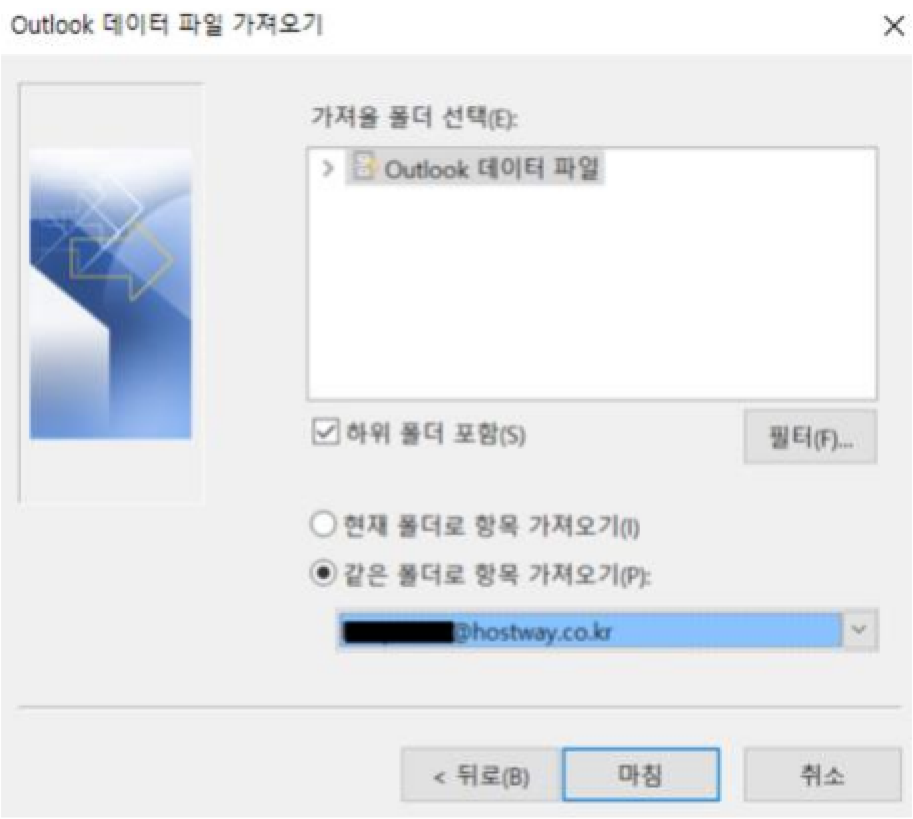
6. 가져올 계정 및 폴더를 선택하고 마침을 클릭합니다.


Outlook 데이터 파일 가져오기
가져올 파일(F)
찾아보기(R)...
옵션
< 뒤로(B)
다음(N) >
취소

uments₩Outlook 파일₩backup.pst

● 같은 항목은 가져온 항목으로 바꿈(E)
○ 같은 항목을 둘 이상 만들 수 있음(A)
○ 같은 항목은 가져오지 않음(D)

7. 백업 시 암호를 지정하였다면 암호를 입력합니다.


Outlook 데이터 파일 가져오기

가져올 폴더 선택(E):

Outlook 데이터 파일

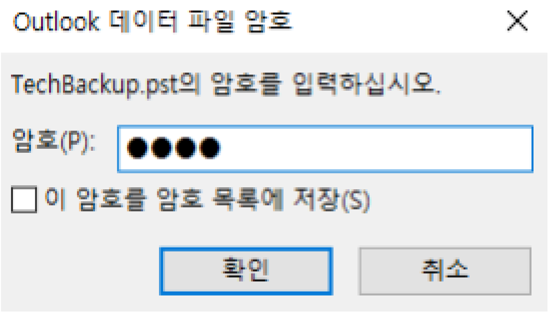
☑ 하위 폴더 포함(S)

○ 현재 폴더로 항목 가져오기(I)

● 같은 폴더로 항목 가져오기(P):

[redacted]@hostway.co.kr

8. Outlook에서 복원된 데이터를 확인합니다.


Outlook 데이터 파일 암호

TechBackup.pst의 암호를 입력하십시오.

암호(P): ●●●●

☐ 이 암호를 암호 목록에 저장(S)

기타

※ 해당 문서는 Outlook 2016을 기준으로 작성 되었으며
Outlook 하위 버전에서도 백업 및 복원 방법이 크게 다르지 않습니다.

[Windows] Windows 랜섬웨어 &

SMB 취약점 포트 차단

[Windows] Windows 랜섬웨어 & SMB 취약점 포트 차단

SMB

네트워크에 연결된 컴퓨터끼리 파일, 프린터, 포트 또는 기타 메시지를 전달하는데 사용된다.
SMB 프로토콜 원격코드 실행 취약점은 랜섬웨어 공격으로 많이 사용되고 있다.

OS 최신 보안 패치

MS에서 SMB 관련 취약점에 대한 패치는 보안 업데이트로 제공된다.
업데이트가 어려운 서버는 아래 SMB 포트 차단으로 조치 가능하다.

SMB 포트 차단

```
Powershell ISE에서 아래 내용 복사 후 실행
# updated by Hostway System Team

$Language = Get-WinUserLanguageList
$Lang = $Language.LanguageTag

Switch($Lang)
{
‘ko’
{
Write ‘OS Version’
[Environment]::OSVersion
Write-Verbose -Message “취약점 포트 제거 UDP 137, UDP 138, TCP 139, TCP 445″ -Verbose

netsh advfirewall firewall set rule name=”네트워크 검색(NB-Name-In)” profile=public dir=in localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”네트워크 검색(NB-Name-In)” profile=private dir=in localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”네트워크 검색(NB-Name-In)” profile=public,domain dir=in localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”네트워크 검색(NB-Name-In)” profile=private,domain dir=in localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”네트워크 검색(NB-Name-In)” profile=private,public dir=in localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”네트워크 검색(NB-Name-In)” profile=any dir=in localport=137 protocol=udp new enable=no

netsh advfirewall firewall set rule name=”파일 및 프린터 공유(NB-Name-In)” profile=public dir=in localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”파일 및 프린터 공유(NB-Name-In)” profile=private dir=in localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”파일 및 프린터 공유(NB-Name-In)” profile=public,domain dir=in localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”파일 및 프린터 공유(NB-Name-In)” profile=private,domain dir=in localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”파일 및 프린터 공유(NB-Name-In)” profile=private,public dir=in localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”파일 및 프린터 공유(NB-Name-In)” profile=any dir=in localport=137 protocol=udp new enable=no

netsh advfirewall firewall set rule name=”네트워크 검색(NB-Datagram-In)” profile=public dir=in localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”네트워크 검색(NB-Datagram-In)” profile=private dir=in localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”네트워크 검색(NB-Datagram-In)” profile=public,domain dir=in localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”네트워크 검색(NB-Datagram-In)” profile=private,domain dir=in localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”네트워크 검색(NB-Datagram-In)” profile=private,public dir=in localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”네트워크 검색(NB-Datagram-In)” profile=any dir=in localport=137 protocol=udp new enable=no

netsh advfirewall firewall set rule name=”파일 및 프린터 공유(NB-Datagram-In)” profile=public dir=in localport=138 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”파일 및 프린터 공유(NB-Datagram-In)” profile=private dir=in localport=138 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”파일 및 프린터 공유(NB-Datagram-In)” profile=public,domain dir=in localport=138 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”파일 및 프린터 공유(NB-Datagram-In)” profile=private,domain dir=in localport=138 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”파일 및 프린터 공유(NB-Datagram-In)” profile=private,public dir=in localport=138 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”파일 및 프린터 공유(NB-Datagram-In)” profile=any dir=in localport=138 protocol=udp new enable=no

netsh advfirewall firewall set rule name=”네트워크 검색(NB-Datagram-In)” profile=public dir=in localport=138 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”네트워크 검색(NB-Datagram-In)” profile=private dir=in localport=138 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”네트워크 검색(NB-Datagram-In)” profile=public,domain dir=in localport=138 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”네트워크 검색(NB-Datagram-In)” profile=private,domain dir=in localport=138 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”네트워크 검색(NB-Datagram-In)” profile=private,public dir=in localport=138 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”네트워크 검색(NB-Datagram-In)” profile=any dir=in localport=138 protocol=udp new enable=no

netsh advfirewall firewall set rule name=”가상 컴퓨터 모니터링(NB-Session-In)” profile=public dir=in localport=139 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”가상 컴퓨터 모니터링(NB-Session-In)” profile=private dir=in localport=139 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”가상 컴퓨터 모니터링(NB-Session-In)” profile=public,domain dir=in localport=139 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”가상 컴퓨터 모니터링(NB-Session-In)” profile=private,domain dir=in localport=139 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”가상 컴퓨터 모니터링(NB-Session-In)” profile=private,public dir=in localport=139 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”가상 컴퓨터 모니터링(NB-Session-In)” profile=any dir=in localport=139 protocol=tcp new enable=no

netsh advfirewall firewall set rule name=”파일 및 프린터 공유(NB-Session-In)” profile=public dir=in localport=139 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”파일 및 프린터 공유(NB-Session-In)” profile=private dir=in localport=139 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”파일 및 프린터 공유(NB-Session-In)” profile=public,domain dir=in localport=139 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”파일 및 프린터 공유(NB-Session-In)” profile=private,domain dir=in localport=139 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”파일 및 프린터 공유(NB-Session-In)” profile=private,public dir=in localport=139 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”파일 및 프린터 공유(NB-Session-In)” profile=any dir=in localport=139 protocol=tcp new enable=no

netsh advfirewall firewall set rule name=”파일 및 프린터 공유(SMB-In)” profile=public dir=in localport=445 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”파일 및 프린터 공유(SMB-In)” profile=private dir=in localport=445 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”파일 및 프린터 공유(SMB-In)” profile=public,domain dir=in localport=445 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”파일 및 프린터 공유(SMB-In)” profile=private,domain dir=in localport=445 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”파일 및 프린터 공유(SMB-In)” profile=private,public dir=in localport=445 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”파일 및 프린터 공유(SMB-In)” profile=any dir=in localport=445 protocol=tcp new enable=no
}
‘en-US’
{
Write ‘OS Version’
[Environment]::OSVersion
Write-Verbose -Message “Vulnerability Port Removal UDP 137, UDP 138, TCP 139, TCP 445″ -Verbose

netsh advfirewall firewall set rule name=”Network Discovery (NB-Name-In)” profile=public dir=in localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”Network Discovery (NB-Name-In)” profile=private dir=in localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”Network Discovery (NB-Name-In)” profile=public,domain dir=in localport=137
```

```
protocol=udp new enable=no
netsh advfirewall firewall set rule name=”Network Discovery
(NB-Name-In)” profile=private,domain dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name=”Network Discovery
(NB-Name-In)” profile=private,public dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name=”Network Discovery
(NB-Name-In)” profile=any dir=in localport=137 protocol=udp
new enable=no

netsh advfirewall firewall set rule name=”File and Printer
Sharing (NB-Name-In)” profile=public dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name=”File and Printer
Sharing (NB-Name-In)” profile=private dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name=”File and Printer
Sharing (NB-Name-In)” profile=public,domain dir=in
localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”File and Printer
Sharing (NB-Name-In)” profile=private,domain dir=in
localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”File and Printer
Sharing (NB-Name-In)” profile=private,public dir=in
localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”File and Printer
Sharing (NB-Name-In)” profile=any dir=in localport=137
protocol=udp new enable=no

netsh advfirewall firewall set rule name=”Network Discovery
(NB-Datagram-In)” profile=public dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name=”Network Discovery
(NB-Datagram-In)” profile=private dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name=”Network Discovery
(NB-Datagram-In)” profile=public,domain dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name=”Network Discovery
(NB-Datagram-In)” profile=private,domain dir=in localport=137
```

```
protocol=udp new enable=no
netsh advfirewall firewall set rule name=”Network Discovery
(NB-Datagram-In)” profile=private,public dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name=”Network Discovery
(NB-Datagram-In)” profile=any dir=in localport=137
protocol=udp new enable=no

netsh advfirewall firewall set rule name=”File and Printer
Sharing (NB-Datagram-In)” profile=public dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name=”File and Printer
Sharing (NB-Datagram-In)” profile=private dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name=”File and Printer
Sharing (NB-Datagram-In)” profile=public,domain dir=in
localport=138 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”File and Printer
Sharing (NB-Datagram-In)” profile=private,domain dir=in
localport=138 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”File and Printer
Sharing (NB-Datagram-In)” profile=private,public dir=in
localport=138 protocol=udp new enable=no
netsh advfirewall firewall set rule name=”File and Printer
Sharing (NB-Datagram-In)” profile=any dir=in localport=138
protocol=udp new enable=no

netsh advfirewall firewall set rule name=”Network Discovery
(NB-Datagram-In)” profile=public dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name=”Network Discovery
(NB-Datagram-In)” profile=private dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name=”Network Discovery
(NB-Datagram-In)” profile=public,domain dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name=”Network Discovery
(NB-Datagram-In)” profile=private,domain dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name=”Network Discovery
(NB-Datagram-In)” profile=private,public dir=in localport=138
```

```
protocol=udp new enable=no
netsh advfirewall firewall set rule name=”Network Discovery
(NB-Datagram-In)” profile=any dir=in localport=138
protocol=udp new enable=no

netsh advfirewall firewall set rule name=”Virtual Machine
Monitoring (NB-Session-In)” profile=public dir=in
localport=139 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”Virtual Machine
Monitoring (NB-Session-In)” profile=private dir=in
localport=139 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”Virtual Machine
Monitoring (NB-Session-In)” profile=public,domain dir=in
localport=139 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”Virtual Machine
Monitoring (NB-Session-In)” profile=private,domain dir=in
localport=139 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”Virtual Machine
Monitoring (NB-Session-In)” profile=private,public dir=in
localport=139 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”Virtual Machine
Monitoring (NB-Session-In)” profile=any dir=in localport=139
protocol=tcp new enable=no

netsh advfirewall firewall set rule name=”File and Printer
Sharing (NB-Session-In)” profile=public dir=in localport=139
protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”File and Printer
Sharing (NB-Session-In)” profile=private dir=in localport=139
protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”File and Printer
Sharing (NB-Session-In)” profile=public,domain dir=in
localport=139 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”File and Printer
Sharing (NB-Session-In)” profile=private,domain dir=in
localport=139 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”File and Printer
Sharing (NB-Session-In)” profile=private,public dir=in
localport=139 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”File and Printer
Sharing (NB-Session-In)” profile=any dir=in localport=139
```

```
protocol=tcp new enable=no

netsh advfirewall firewall set rule name=”File Server Remote Management (SMB-In)” profile=public dir=in localport=445 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”File Server Remote Management (SMB-In)” profile=private dir=in localport=445 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”File Server Remote Management (SMB-In)” profile=public,domain dir=in localport=445 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”File Server Remote Management (SMB-In)” profile=private,domain dir=in localport=445 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”File Server Remote Management (SMB-In)” profile=private,public dir=in localport=445 protocol=tcp new enable=no
netsh advfirewall firewall set rule name=”File Server Remote Management (SMB-In)” profile=any dir=in localport=445 protocol=tcp new enable=no
}
}
```

Windows 2012 원격 세션 늘리기

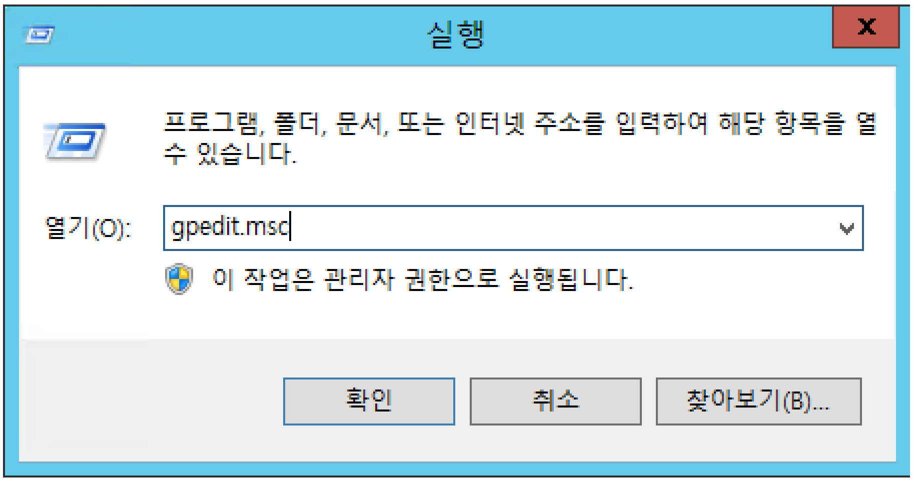
Windows Server 2012 설치 이후 고객사에서 원격 접속으로 접속하여 작업시 다른 세션의 접속으로 인하여 세션이 끊기며 서로 뺏어가는 경우가 자주 발생하게 됩니다.

Windows 2012의 경우 1개의 세션만을 공유하도록 기본으로 설정되어 있어 발생하는 문제입니다.

이에 Windows Server 2012에서 세션 설정을 변경하는 방법을 안내드리도록 하겠습니다.

Windows Server 2012의 경우 세션 설정에 대하여 로컬 컴퓨터 정책에서 설정해야 합니다.

실행창에서 gpedit.msc 를 입력하여 실행합니다.

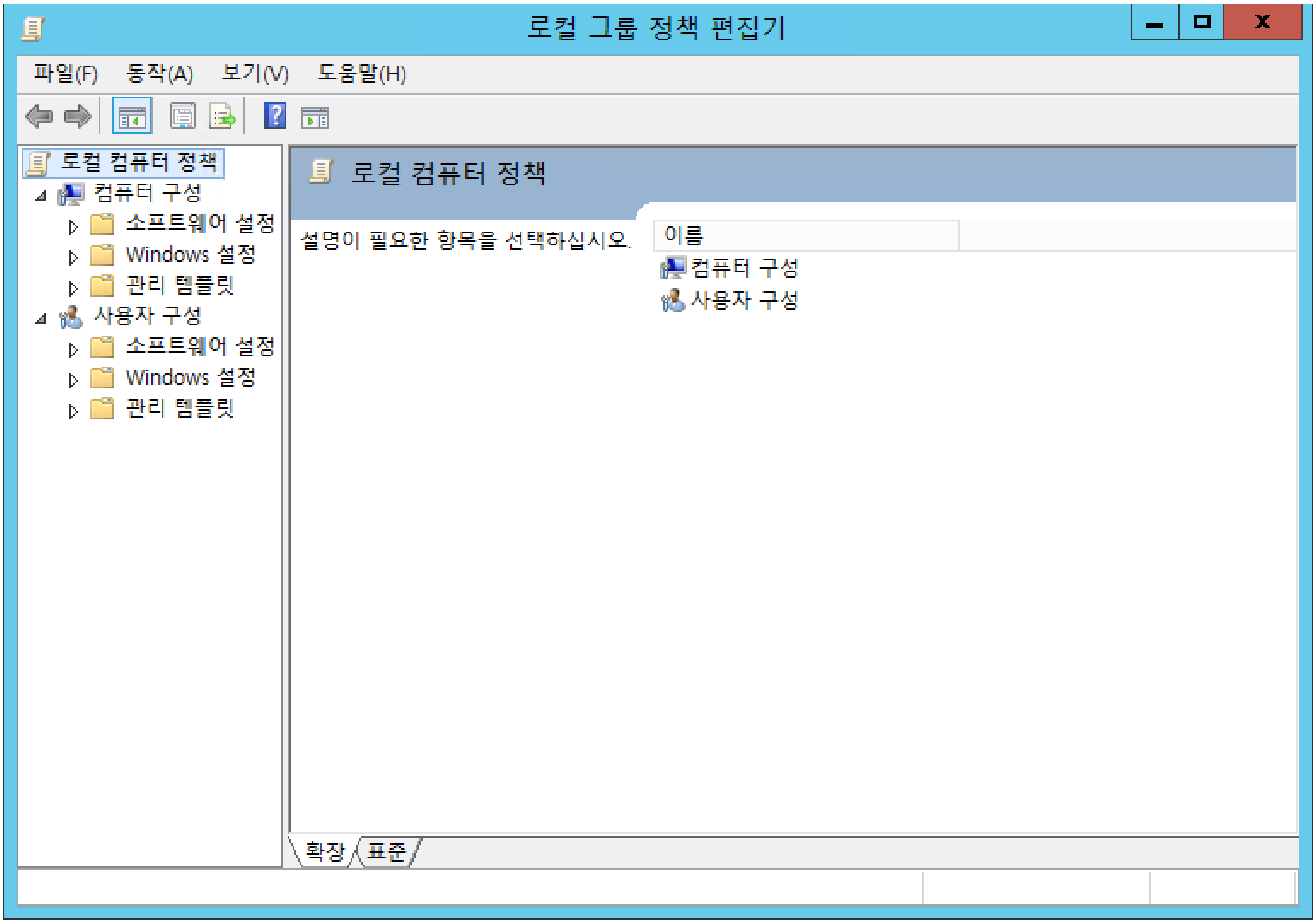

실행
확인
취소
찾아보기(B)...

프로그램, 폴더, 문서, 또는 인터넷 주소를 입력하여 해당 항목을 열 수 있습니다.

열기(O): gpedit.msc

이 작업은 관리자 권한으로 실행됩니다.

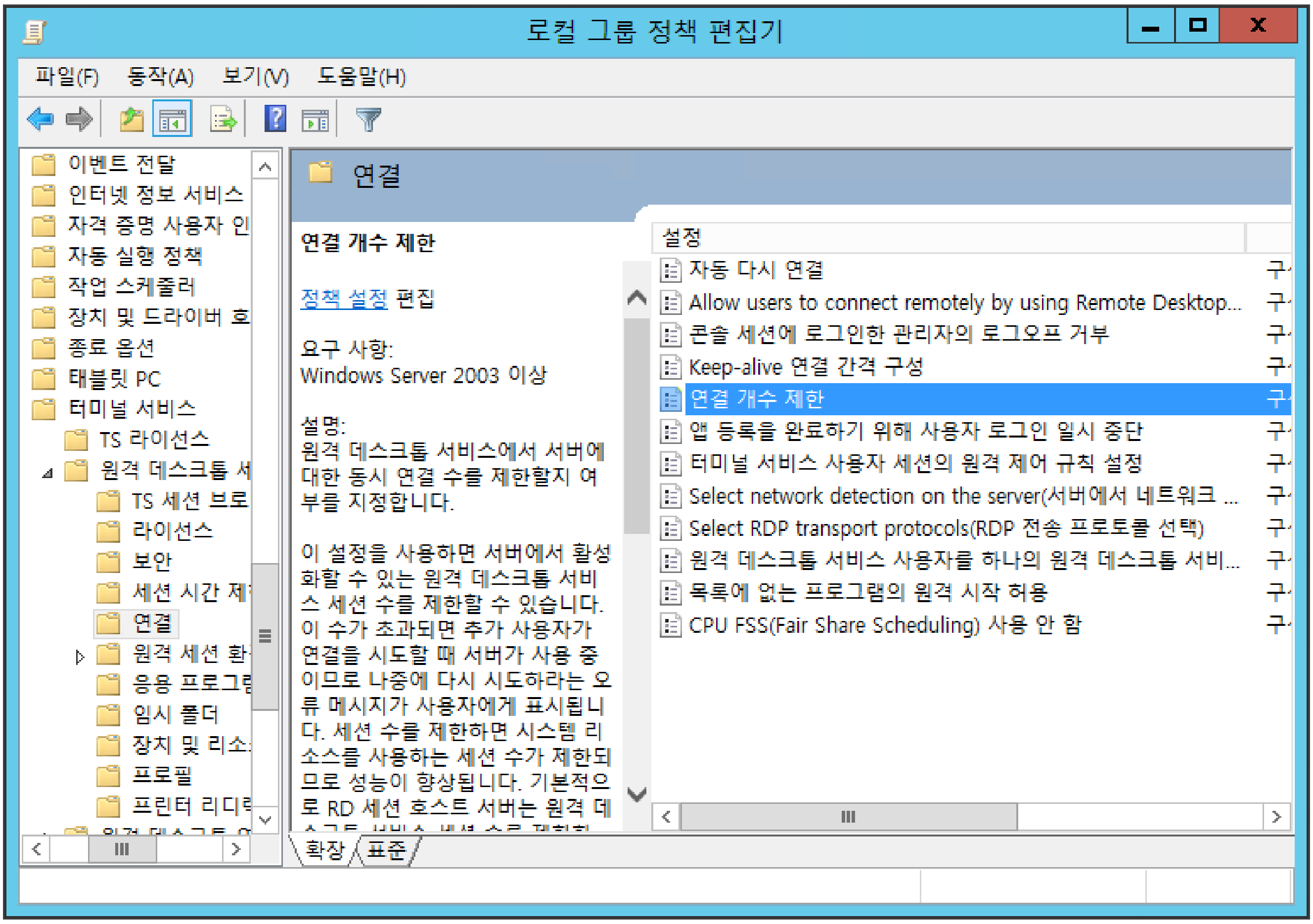
로컬 그룹 정책 편집기가 나타납니다.


로컬 그룹 정책 편집기
파일(F)
동작(A)
보기(V)
도움말(H)
로컬 컴퓨터 정책
컴퓨터 구성
소프트웨어 설정
Windows 설정
관리 템플릿
사용자 구성
소프트웨어 설정
Windows 설정
관리 템플릿
로컬 컴퓨터 정책
이름
컴퓨터 구성
사용자 구성
확장
표준

설명이 필요한 항목을 선택하십시오.

원격 세션 연결 설정 변경을 위하여 [컴퓨터 구성] – [관리 템플릿] - [Windows 구성 요소] – [터미널 서비스] – [원격 데스크톱 세션 호스트] – [연결] 메뉴를 선택 한후

[연결 개수 제한]을 항목을 선택합니다.


로컬 그룹 정책 편집기
파일(F)
동작(A)
보기(V)
도움말(H)
이벤트 전달
인터넷 정보 서비스
자격 증명 사용자 인
자동 실행 정책
작업 스케줄러
장치 및 드라이버 호
종료 옵션
태블릿 PC
터미널 서비스
TS 라이선스
원격 데스크톱 서
TS 세션 브로
라이선스
보안
세션 시간 제
연결
원격 세션 환
응용 프로그
임시 폴더
장치 및 리소
프로필
프린터 리디
연결
설정
확장
표준

연결 개수 제한

정책 설정 편집

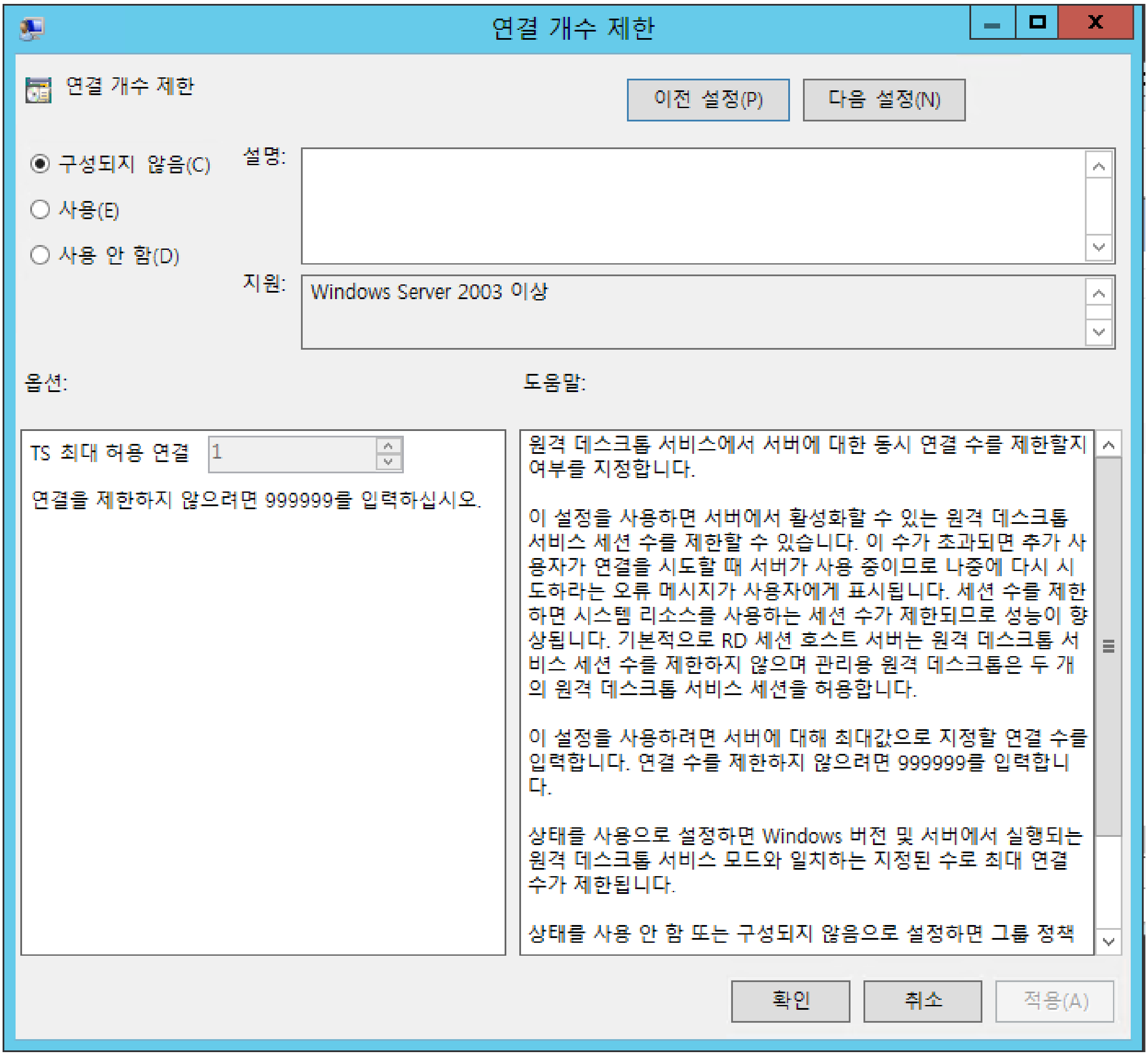
요구 사항:
Windows Server 2003 이상

설명:
원격 데스크톱 서비스에서 서버에 대한 동시 연결 수를 제한할지 여부를 지정합니다.

이 설정을 사용하면 서버에서 활성화할 수 있는 원격 데스크톱 서비스 세션 수를 제한할 수 있습니다. 이 수가 초과되면 추가 사용자가 연결을 시도할 때 서버가 사용 중이므로 나중에 다시 시도하라는 오류 메시지가 사용자에게 표시됩니다. 세션 수를 제한하면 시스템 리소스를 사용하는 세션 수가 제한되므로 성능이 향상됩니다. 기본적으로 RD 세션 호스트 서버는 원격 데

- 자동 다시 연결
- Allow users to connect remotely by using Remote Desktop...
- 콘솔 세션에 로그인한 관리자의 로그오프 거부
- Keep-alive 연결 간격 구성
- 연결 개수 제한
- 앱 등록을 완료하기 위해 사용자 로그인 일시 중단
- 터미널 서비스 사용자 세션의 원격 제어 규칙 설정
- Select network detection on the server(서버에서 네트워크 ...
- Select RDP transport protocols(RDP 전송 프로토콜 선택)
- 원격 데스크톱 서비스 사용자를 하나의 원격 데스크톱 서비...
- 목록에 없는 프로그램의 원격 시작 허용
- CPU FSS(Fair Share Scheduling) 사용 안 함

기본적인 [연결 개수 제한]은 구성되지 않음으로 설정되어 있습니다.



● 구성되지 않음(C)

○ 사용(E)

○ 사용 안 함(D)

지원: Windows Server 2003 이상

TS 최대 허용 연결 1

연결을 제한하지 않으려면 999999를 입력하십시오.

원격 데스크톱 서비스에서 서버에 대한 동시 연결 수를 제한할지 여부를 지정합니다.

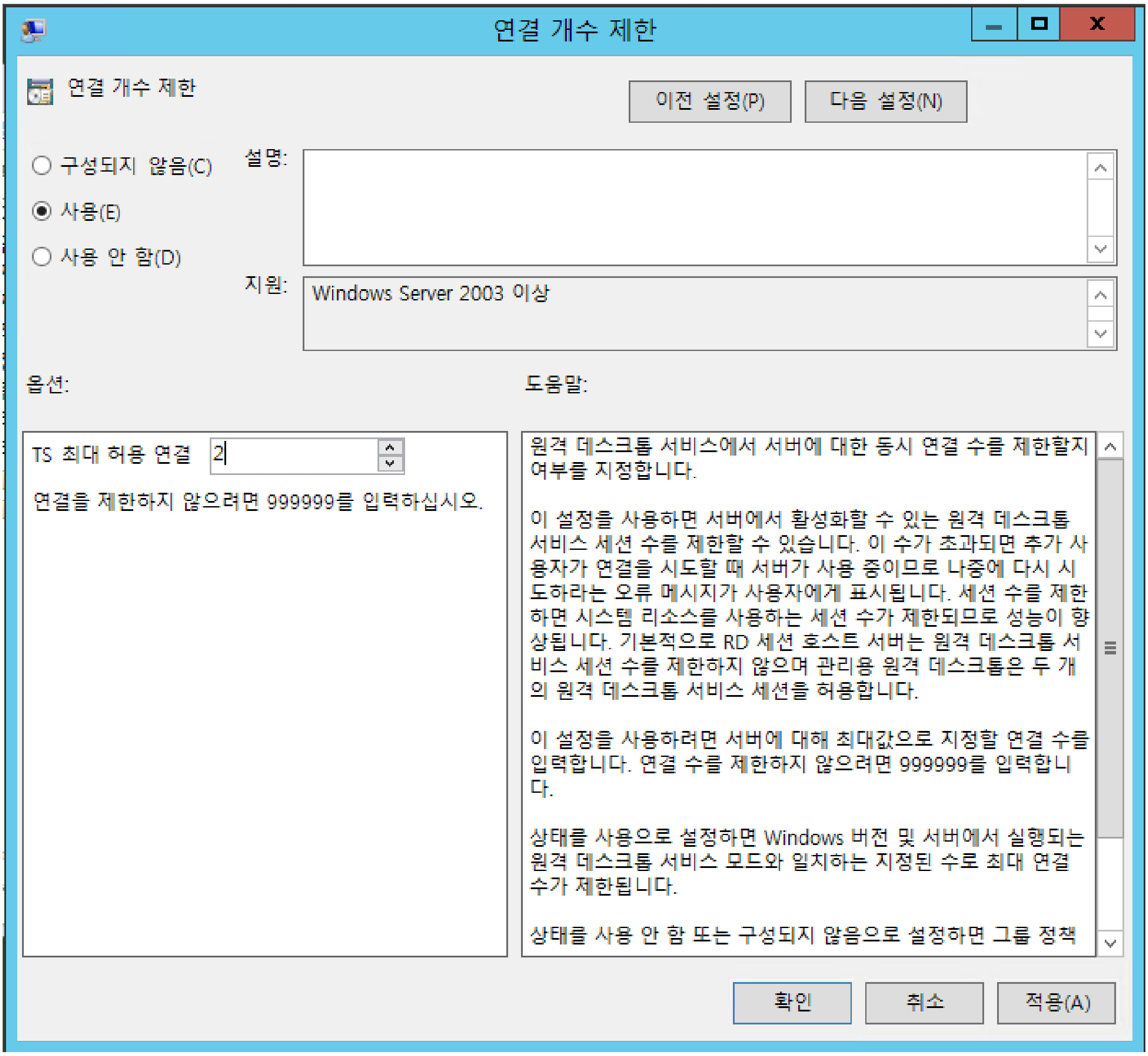
이 설정을 사용하면 서버에서 활성화할 수 있는 원격 데스크톱 서비스 세션 수를 제한할 수 있습니다. 이 수가 초과되면 추가 사용자가 연결을 시도할 때 서버가 사용 중이므로 나중에 다시 시도하라는 오류 메시지가 사용자에게 표시됩니다. 세션 수를 제한하면 시스템 리소스를 사용하는 세션 수가 제한되므로 성능이 향상됩니다. 기본적으로 RD 세션 호스트 서버는 원격 데스크톱 서비스 세션 수를 제한하지 않으며 관리용 원격 데스크톱은 두 개의 원격 데스크톱 서비스 세션을 허용합니다.

이 설정을 사용하려면 서버에 대해 최대값으로 지정할 연결 수를 입력합니다. 연결 수를 제한하지 않으려면 999999를 입력합니다.

상태를 사용으로 설정하면 Windows 버전 및 서버에서 실행되는 원격 데스크톱 서비스 모드와 일치하는 지정된 수로 최대 연결 수가 제한됩니다.

상태를 사용 안 함 또는 구성되지 않음으로 설정하면 그룹 정책

[연결 개수 제한]을 사용으로 선택하며, 옵션에서 TS 최대 허용 연결을 임의의 값으로 설정한 후 확인을 클릭 합니다.(여기서는 2개 선택)



○ 구성되지 않음(C)
● 사용(E)
○ 사용 안 함(D)

지원: Windows Server 2003 이상

TS 최대 허용 연결: 2

연결을 제한하지 않으려면 999999를 입력하십시오.

원격 데스크톱 서비스에서 서버에 대한 동시 연결 수를 제한할지 여부를 지정합니다.

이 설정을 사용하면 서버에서 활성화할 수 있는 원격 데스크톱 서비스 세션 수를 제한할 수 있습니다. 이 수가 초과되면 추가 사용자가 연결을 시도할 때 서버가 사용 중이므로 나중에 다시 시도하라는 오류 메시지가 사용자에게 표시됩니다. 세션 수를 제한하면 시스템 리소스를 사용하는 세션 수가 제한되므로 성능이 향상됩니다. 기본적으로 RD 세션 호스트 서버는 원격 데스크톱 서비스 세션 수를 제한하지 않으며 관리용 원격 데스크톱은 두 개의 원격 데스크톱 서비스 세션을 허용합니다.

이 설정을 사용하려면 서버에 대해 최대값으로 지정할 연결 수를 입력합니다. 연결 수를 제한하지 않으려면 999999를 입력합니다.

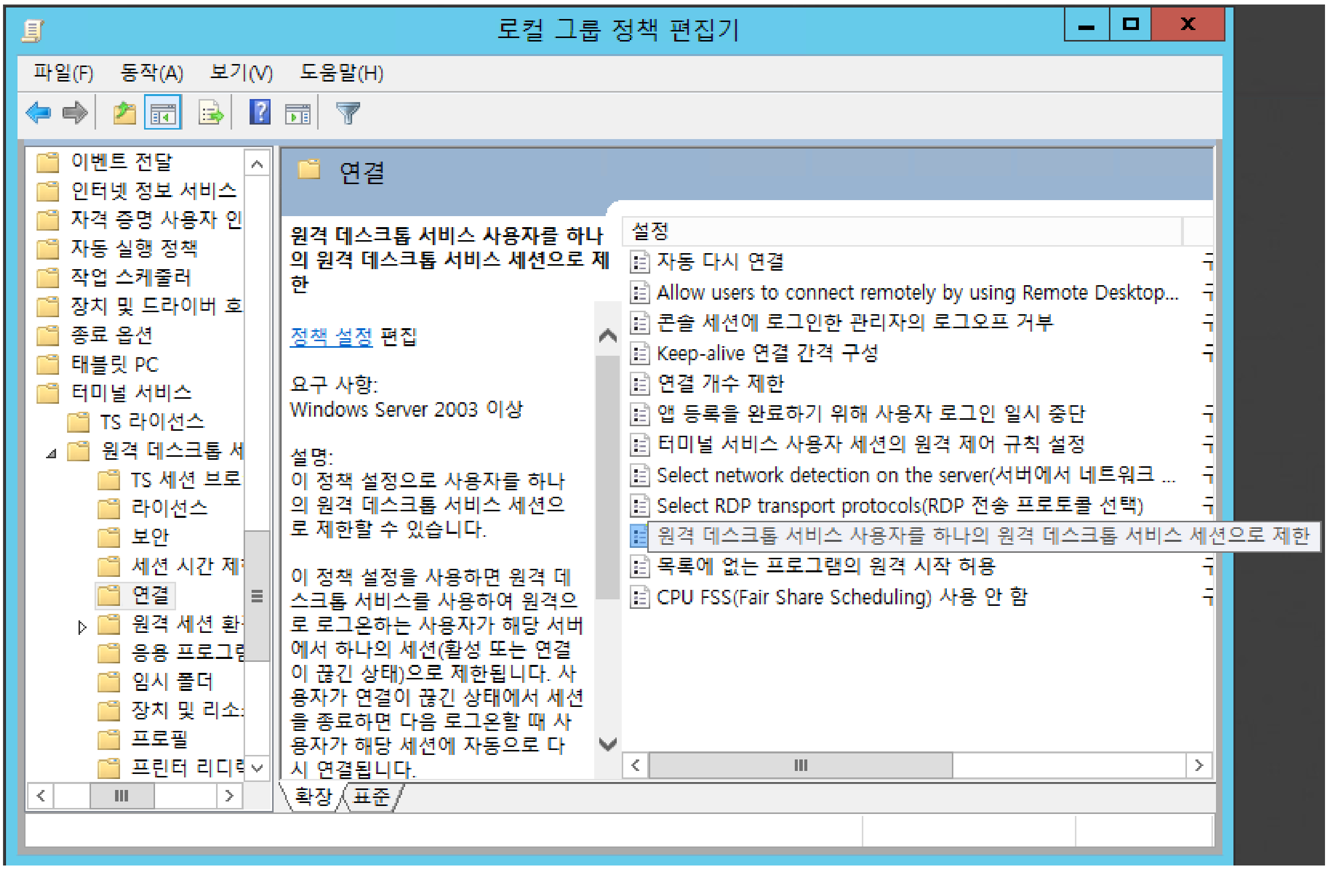
상태를 사용으로 설정하면 Windows 버전 및 서버에서 실행되는 원격 데스크톱 서비스 모드와 일치하는 지정된 수로 최대 연결 수가 제한됩니다.

상태를 사용 안 함 또는 구성되지 않음으로 설정하면 그룹 정책

여기 까지의 설정으로 세션 연결은 2개로 늘어났지만, 아직까지는 하나의 세션으로 접속이 됩니다.

이에 각자 별도의 세션으로 접속하기 위한 작업을 다음과 같이 추가적으로 적용해 줍니다.

[원격 데스크톱 서비스 사용자를 하나의 원격 데스크톱 서비스 세션으로 제한] 을 선택합니다.


로컬 그룹 정책 편집기
파일(F)
동작(A)
보기(V)
도움말(H)
이벤트 전달
인터넷 정보 서비스
자격 증명 사용자 인
자동 실행 정책
작업 스케줄러
장치 및 드라이버 호
종료 옵션
태블릿 PC
터미널 서비스
TS 라이선스
원격 데스크톱 서
TS 세션 브로
라이선스
보안
세션 시간 제
연결
원격 세션 환
응용 프로그
임시 폴더
장치 및 리소
프로필
프린터 리디
연결
확장
표준

원격 데스크톱 서비스 사용자를 하나의 원격 데스크톱 서비스 세션으로 제한

정책 설정 편집

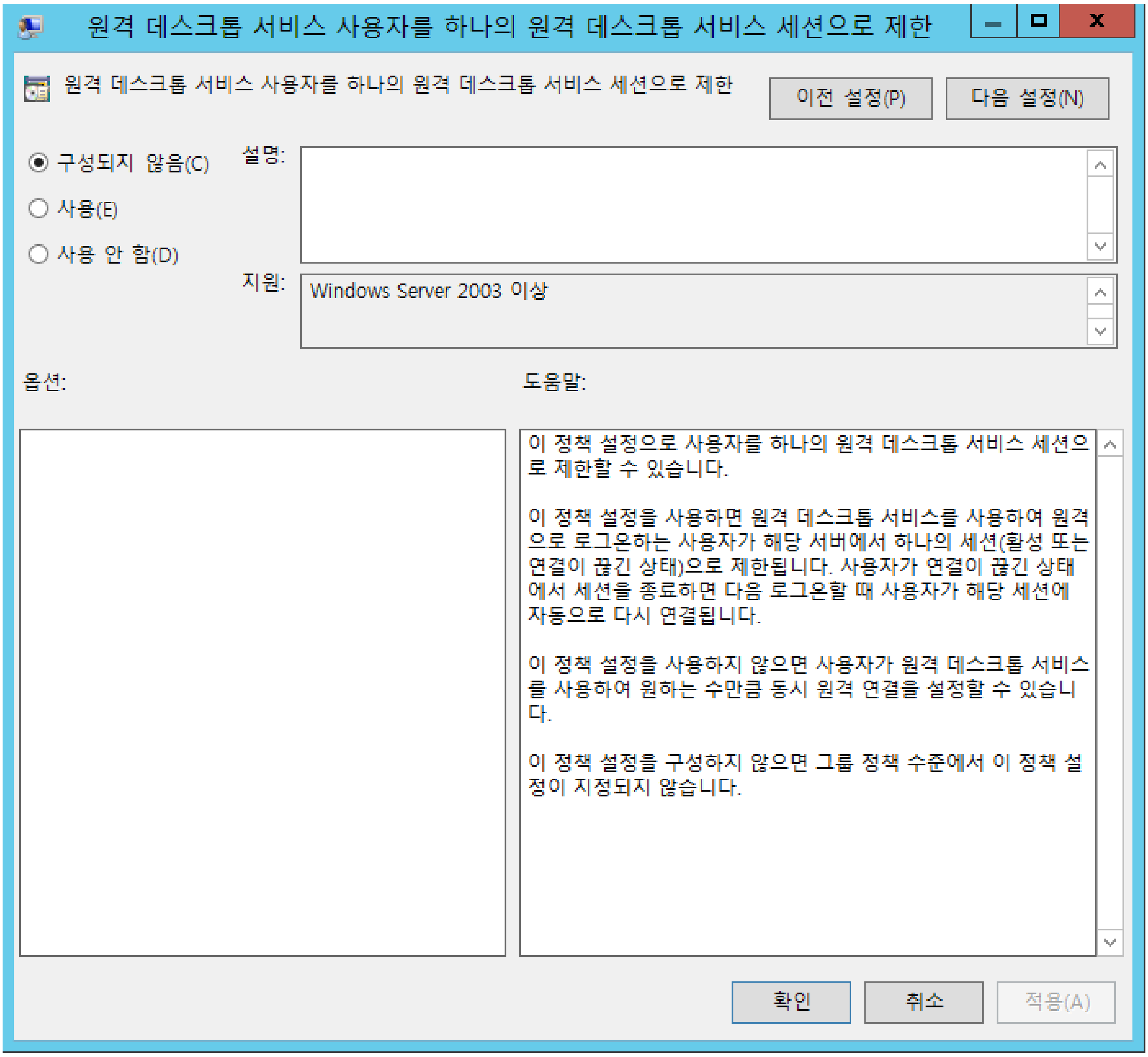
요구 사항:
Windows Server 2003 이상

설명:
이 정책 설정으로 사용자를 하나의 원격 데스크톱 서비스 세션으로 제한할 수 있습니다.

이 정책 설정을 사용하면 원격 데스크톱 서비스를 사용하여 원격으로 로그온하는 사용자가 해당 서버에서 하나의 세션(활성 또는 연결이 끊긴 상태)으로 제한됩니다. 사용자가 연결이 끊긴 상태에서 세션을 종료하면 다음 로그온할 때 사용자가 해당 세션에 자동으로 다시 연결됩니다.

설정
- 자동 다시 연결
- Allow users to connect remotely by using Remote Desktop...
- 콘솔 세션에 로그인한 관리자의 로그오프 거부
- Keep-alive 연결 간격 구성
- 연결 개수 제한
- 앱 등록을 완료하기 위해 사용자 로그인 일시 중단
- 터미널 서비스 사용자 세션의 원격 제어 규칙 설정
- Select network detection on the server(서버에서 네트워크 ...
- Select RDP transport protocols(RDP 전송 프로토콜 선택)
- 원격 데스크톱 서비스 사용자를 하나의 원격 데스크톱 서비스 세션으로 제한
- 목록에 없는 프로그램의 원격 시작 허용
- CPU FSS(Fair Share Scheduling) 사용 안 함

기본적인 메뉴는 다음과 같습니다.


원격 데스크톱 서비스 사용자를 하나의 원격 데스크톱 서비스 세션으로 제한
이전 설정(P)
다음 설정(N)
확인
취소
적용(A)

원격 데스크톱 서비스 사용자를 하나의 원격 데스크톱 서비스 세션으로 제한

● 구성되지 않음(C)
○ 사용(E)
○ 사용 안 함(D)

설명:

지원: Windows Server 2003 이상

옵션:

도움말:

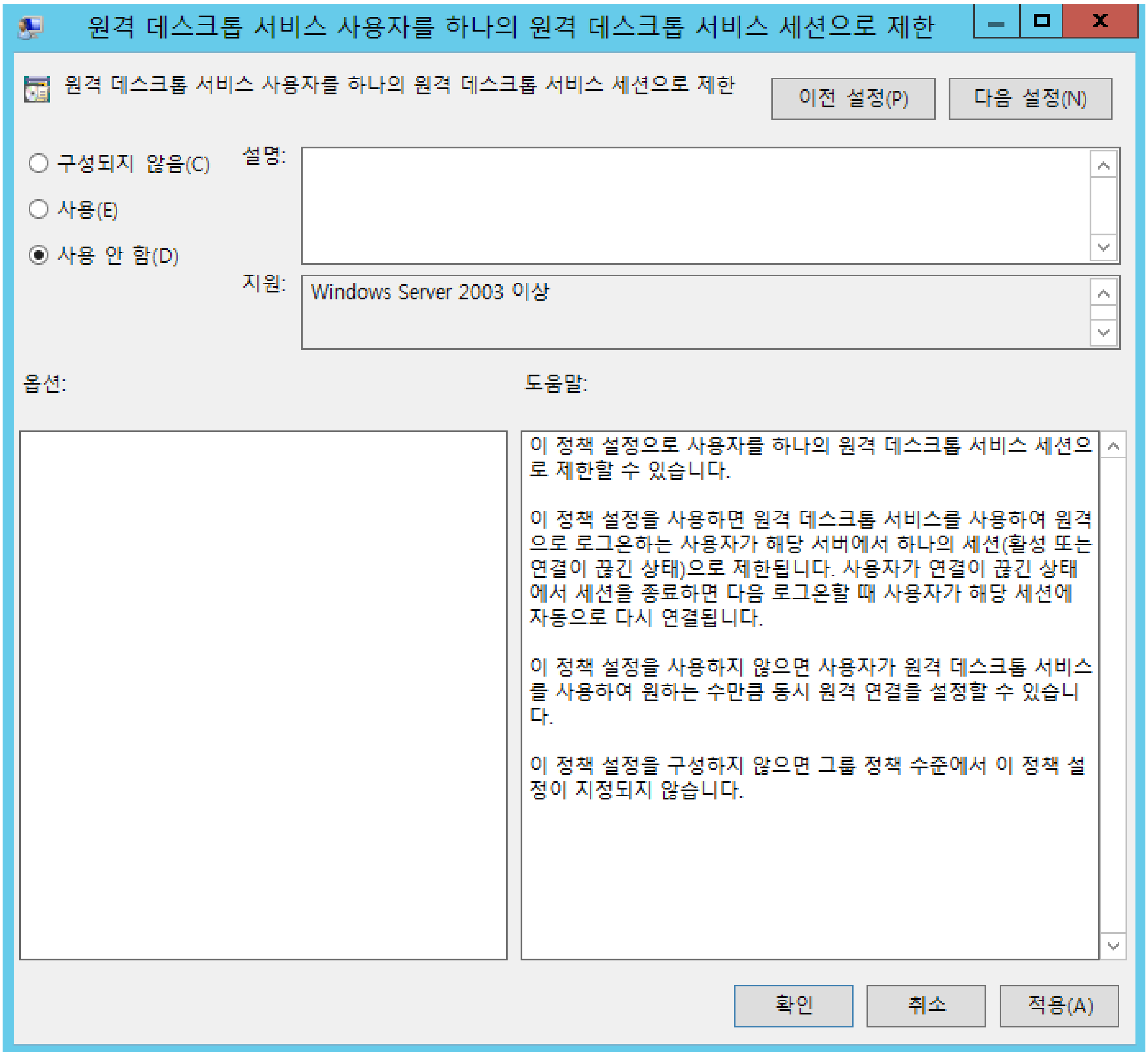
이 정책 설정으로 사용자를 하나의 원격 데스크톱 서비스 세션으로 제한할 수 있습니다.

이 정책 설정을 사용하면 원격 데스크톱 서비스를 사용하여 원격으로 로그온하는 사용자가 해당 서버에서 하나의 세션(활성 또는 연결이 끊긴 상태)으로 제한됩니다. 사용자가 연결이 끊긴 상태에서 세션을 종료하면 다음 로그온할 때 사용자가 해당 세션에 자동으로 다시 연결됩니다.

이 정책 설정을 사용하지 않으면 사용자가 원격 데스크톱 서비스를 사용하여 원하는 수만큼 동시 원격 연결을 설정할 수 있습니다.

이 정책 설정을 구성하지 않으면 그룹 정책 수준에서 이 정책 설정이 지정되지 않습니다.

각각의 세션에서 작업을 하기 위하여 사용 안 함 으로 선택 후 확인을 클릭합니다.



원격 데스크톱 서비스 사용자를 하나의 원격 데스크톱 서비스 세션으로 제한

원격 데스크톱 서비스 사용자를 하나의 원격 데스크톱 서비스 세션으로 제한

○ 구성되지 않음(C)
○ 사용(E)
● 사용 안 함(D)

설명:

지원: Windows Server 2003 이상

옵션:

도움말:

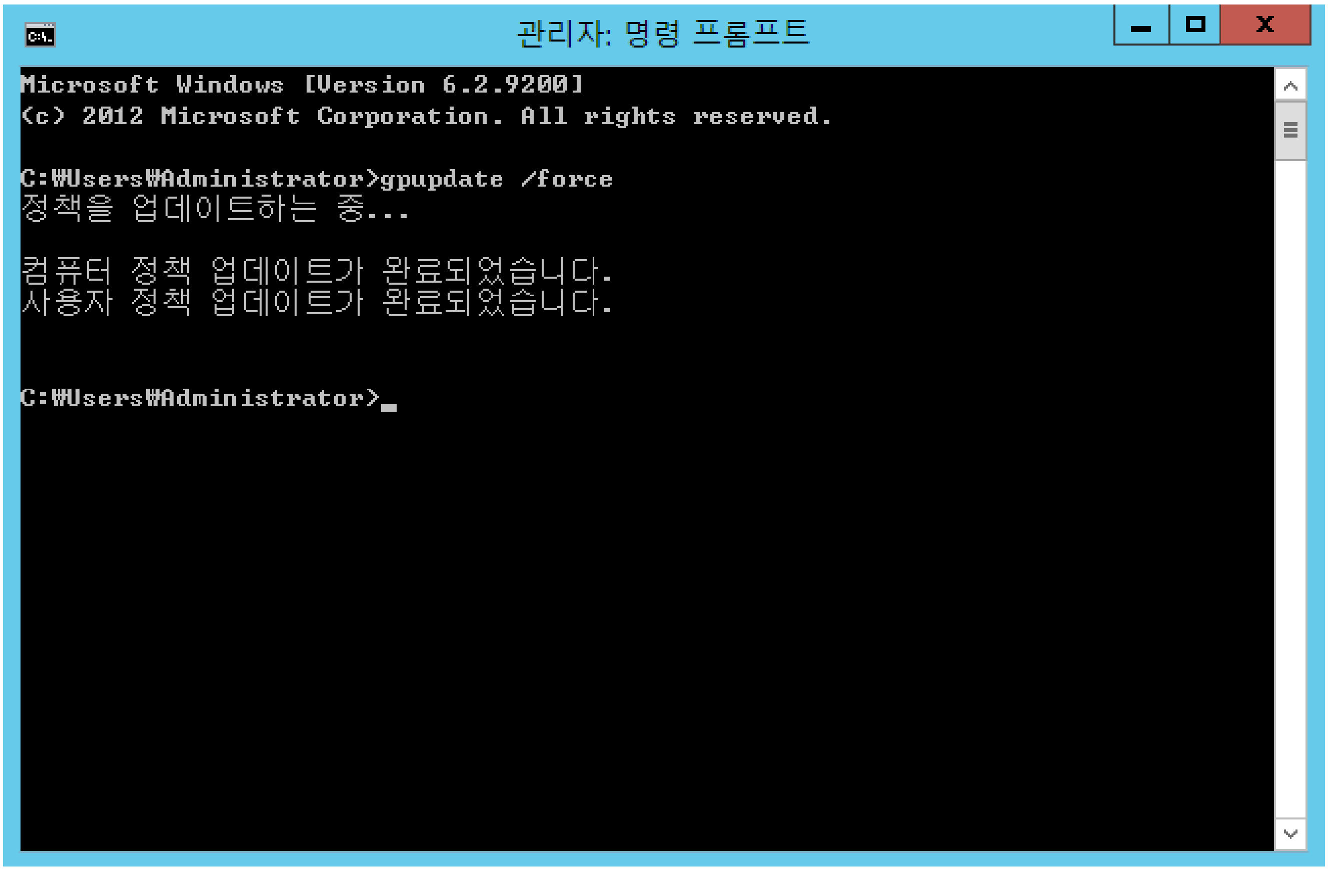
이 정책 설정으로 사용자를 하나의 원격 데스크톱 서비스 세션으로 제한할 수 있습니다.

이 정책 설정을 사용하면 원격 데스크톱 서비스를 사용하여 원격으로 로그온하는 사용자가 해당 서버에서 하나의 세션(활성 또는 연결이 끊긴 상태)으로 제한됩니다. 사용자가 연결이 끊긴 상태에서 세션을 종료하면 다음 로그온할 때 사용자가 해당 세션에 자동으로 다시 연결됩니다.

이 정책 설정을 사용하지 않으면 사용자가 원격 데스크톱 서비스를 사용하여 원하는 수만큼 동시 원격 연결을 설정할 수 있습니다.

이 정책 설정을 구성하지 않으면 그룹 정책 수준에서 이 정책 설정이 지정되지 않습니다.

변경된 정책이 적용 될 수 있도록 정책 업데이트를 적용 해줍니다.



```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
정책을 업데이트하는 중...

컴퓨터 정책 업데이트가 완료되었습니다.
사용자 정책 업데이트가 완료되었습니다.


C:\Users\Administrator>_
```