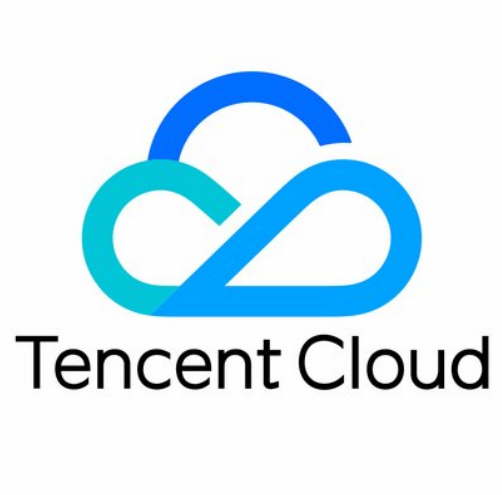
Cloud Virtual Machine

장애처리

제품 문서



목록:

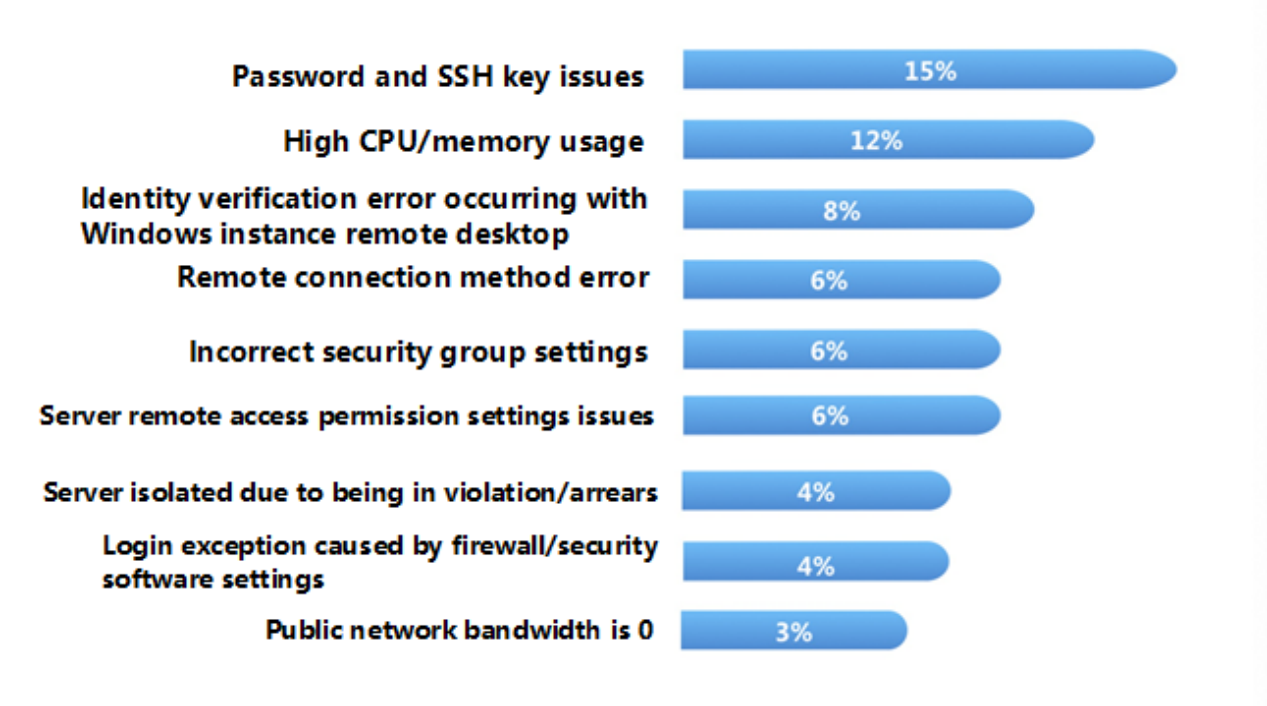
장애처리
인스턴스 관련 장애
CVM에 로그인할 수 없는 문제 처리 방법

최종 업데이트 날짜: : 2024-02-02 11:09:47

본 문서에서는 CVM(Cloud Virtual Machine) 인스턴스를 구매한 후 인스턴스 로그인 오류를 해결하는 방법을 설명합니다.

장애 주요 원인

아래 이미지는 CVM 인스턴스에 연결할 수 없는 주요 원인 및 발생 확률을 보여줍니다. 인스턴스에 연결할 수 없으면, 스마트 진단 툴과 결합해 아래 원인에 따라 문제를 해결하시기 바랍니다.



장애 처리 순서

인스턴스 유형 확인

먼저 구매한 인스턴스 유형이 Windows 시스템 인스턴스인지 Linux 시스템 인스턴스인지 파악합니다. 파악한 다음 각 인스턴스 유형마다 CVM에 로그인할 수 없는 원인이 다르므로 구매한 인스턴스 유형에 맞게 다음 문서를 참조하여 문제를 진단하고 해결합니다.
Windows 인스턴스에 로그인할 수 없는 경우
Linux 인스턴스에 로그인할 수 없는 경우

점검 툴로 원인 진단

Tencent Cloud는 자가 진단과 보안 그룹(포트)검증 툴을 제공하여 로그인할 수 없는 원인을 판단합니다. 약 70%의 로그인 문제는 툴을 통해 점검 및 진단할 수 있습니다.

자가 진단 툴

진단 가능한 문제는 대역폭 이용률이 지나치게 높은 경우, 외부 네트워크 대역폭이 0인 경우, 서버 고부하인 경우, 보안 그룹 규칙이 부적합한 경우, DDoS 공격을 막은 경우, 보안 격리 및 계정 연체 등을 포함합니다.

보안 그룹(포트) 진단 툴

보안 그룹과 포트 관련 장애를 점검합니다. 보안 그룹 설정에 문제가 있으면, 해당 툴의 **원클릭 오픈**기능을 통해 모든 보안 그룹 상용 인터페이스를 오픈할 수 있습니다.
툴을 통해 원인을 진단한 경우, 그에 따라 상응하는 장애 처리를 진행하시기 바랍니다.

인스턴스 재시작

점검 툴을 통해 상응하는 장애를 판단 및 처리한 후, 또는 점검 툴을 통해서도 로그인할 수 없는 원인을 진단할 수 없는 경우 모두 인스턴스 재시작을 통해 원격 연결을 다시 시도해 연결에 성공했는지 조회할 수 있습니다.
인스턴스 재시작 작업은 인스턴스 재시작을 참조할 수 있습니다.

흔히 발생하는 기타 로그인 문제의 원인

위의 처리 단계를 통해서도 문제의 원인을 진단할 수 없거나 CVM에 로그인할 때 사용자가 직접 다음 유형의 오류 메시지를 출력할 경우, 다음 솔루션을 참조할 수 있습니다.

Windows 인스턴스

Windows 인스턴스: 원격 데스크톱 서비스 로그인 권한 없는 경우
Windows 인스턴스: Mac 원격 로그인 비정상
Windows 인스턴스: 인증 오류 발생
Windows 인스턴스: 원격 데스크톱이 원격 컴퓨터로 연결할 수 없는 경우

Linux 인스턴스

Linux 인스턴스: CPU 또는 메모리의 높은 점유율로 인해 로그인할 수 없는 경우

후속 작업

위의 단계를 통해서도 원격 로그인할 수 없는 문제를 해결할 수 없는 경우, 관련 로그와 자가 점검 결과를 저장한 후 Submit Ticket을 통해 피드백 및 해결할 수 있습니다.

Windows 인스턴스 관련
Windows 인스턴스 로그인 불가

최종 업데이트 날짜: : 2024-02-02 11:09:47

본 문서에서는 Windows 인스턴스 로그인 실패의 가능한 원인과 문제 해결 방법에 대해 설명합니다. 지침에 따라 문제의 원인을 식별하고 해결 방법을 배울 수 있습니다.

예상 원인

Windows 인스턴스에 로그인할 수 없는 주요 원인은 다음과 같습니다.
비밀번호 문제
높은 대역폭 이용률
서버 고부하
부적절한 원격 포트 설정
부적절한 보안 그룹 규칙
방화벽 또는 보안 소프트웨어로 인한 예외
원격 데스크톱을 통한 액세스 중 인증 오류

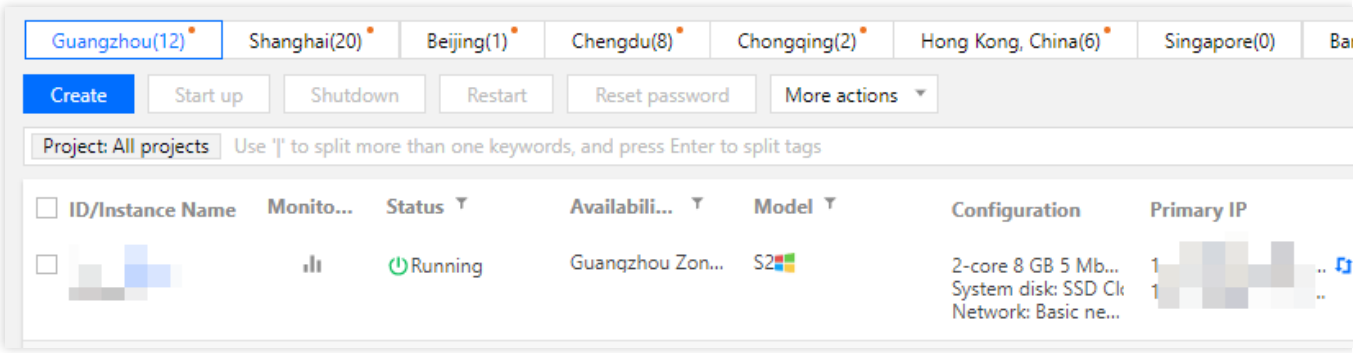
자가 진단 툴 사용

Tencent Cloud는 대역폭, 방화벽 및 보안 그룹 설정 등의 문제로 인해 Windows 인스턴스 연결이 불가능한 것인지 판단할 수 있는 자가 진단 툴을 제공합니다. 70%의 장애는 툴에 의해 위치가 측정되며, 점검된 원인에 따라 로그인 실패를 일으키는 장애 문제의 위치를 측정할 수 있습니다.
1. 자가 진단을 클릭하여 자가 진단 툴을 여십시오.
2. 툴 인터페이스 안내에 따라 진단할 CVM를 선택하고 **점검 시작**을 클릭합니다.
자가 진단 툴로 문제를 진단할 수 없다면 CVM에 VNC 방식을 통해 로그인하여 장애를 진단하시길 권장합니다.

장애 처리

VNC 방식을 통해 로그인

RDP 또는 원격 액세스 소프트웨어를 통해 Windows 인스턴스에 로그인할 수 없는 경우 대신 VNC를 통해 로그인하면 문제의 원인을 식별하는 데 도움이 됩니다.
1. CVM 콘솔에 로그인합니다.
2. 아래 이미지와 같이 인스턴스 관리 페이지에서 액세스할 인스턴스를 선택하고 **로그인**을 클릭합니다.

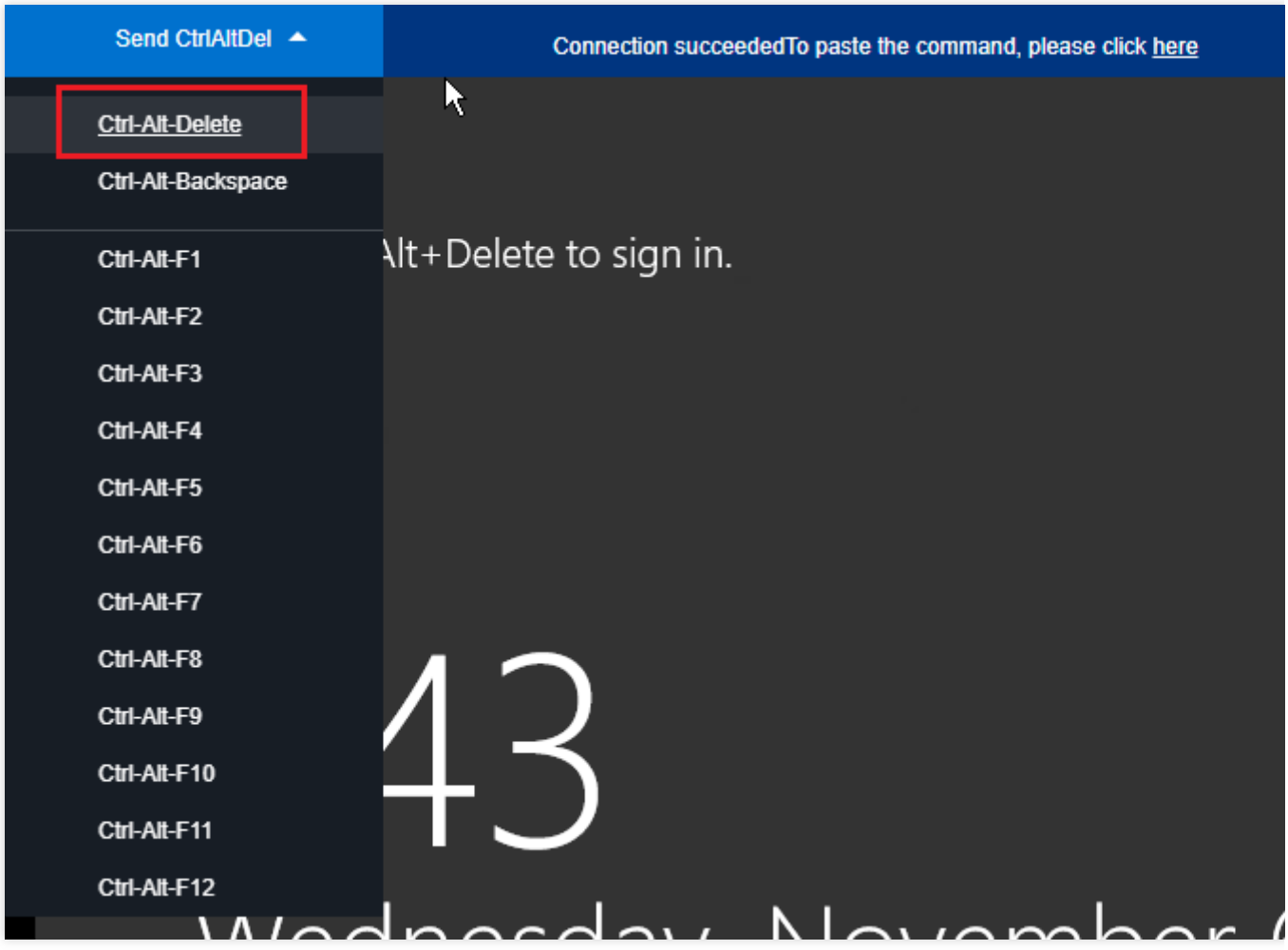


3. '표준 로그인 | Windows 인스턴스' 팝업 창에서 대체 방법(VNC)을 선택하고 **지금 로그인**을 클릭합니다.

설명：

인스턴스의 비밀번호를 잊어버린 경우 콘솔에서 재설정할 수 있습니다. 자세한 내용은 인스턴스 비밀번호 재설정을 참고하십시오.

4. 로그인 팝업 창에서 왼쪽 상단 모서리에 있는 Send CtrlAltDel을 선택하고 Ctrl-Alt-Delete를 눌러 다음 그림과 같이 시스템 로그인 창을 엽니다.



비밀번호 문제

장애 현상: 비밀번호를 잊었거나, 잘못된 비밀번호 입력 또는 비밀번호 재설정에 실패해 로그인할 수 없는 경우입니다.
처리 순서: CVM 콘솔에서 이 인스턴스의 비밀번호를 재설정하고 인스턴스를 다시 시작하십시오. 자세한 내용은 인스턴스 암호 재설정을 참고하십시오.

높은 대역폭 이용률

장애 현상: 자가 진단 툴을 통해 진단한 결과, 대역폭 이용률이 너무 높은 것이 원인인 경우입니다.
처리 순서:
1. VNC 로그인을 통해 인스턴스에 로그인합니다.
2. 높은 대역폭 점유율로 로그인할 수 없을 경우를 참고하여 인스턴스의 대역폭 사용률을 확인하고 그에 따라 문제를 해결합니다.

서버 고부하

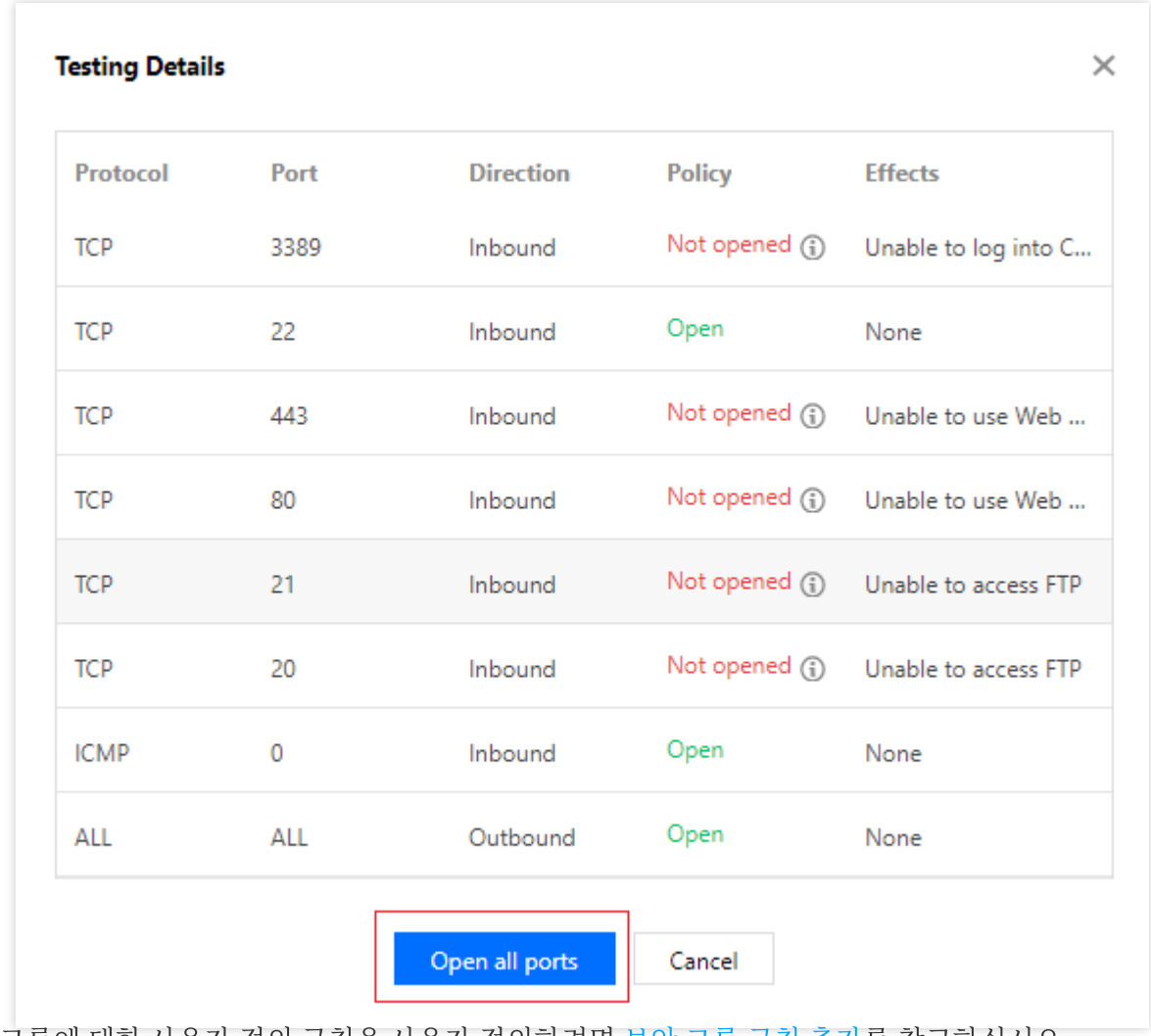
장애 현상: 자가 진단 툴 또는 TCOP 통해 확인한 결과, 서버 CPU의 고부하로 인해 시스템 원격 연결이 불가하거나 액세스 시 심한 랙이 발생하고 있는 경우입니다.
예상 원인: 바이러스, 트로이 목마, 타사 바이러스 백신 소프트웨어, 응용 프로그램 예외, 드라이버 예외 및 백엔드의 소프트웨어 자동 업데이트로 인해 CPU 사용률이 높아져 CVM 로그인 실패 또는 액세스 속도 저하가 발생할 수 있습니다.
처리 순서:
1. VNC 로그인을 통해 인스턴스에 로그인합니다.
2. Windows 인스턴스: CPU 혹은 메모리 점유율이 높아 로그인할 수 없을 경우를 참고하여 '작업 관리자'에서 높은 부하를 일으키는 프로세스를 찾습니다.

부적절한 원격 포트 설정

장애 현상: 인스턴스에 대한 원격 액세스 시도가 실패했거나, 원격 액세스 포트가 기본 포트가 아니거나, 수정되었거나, 포트 3389가 열려 있지 않습니다.
문제 진단: 인스턴스의 공용 IP 주소를 ping하여 네트워크 연결을 확인하고 telnet을 실행하여 포트가 열려 있는지 확인합니다.
처리 순서: 자세한 절차는 포트 문제로 원격 로그인을 할 수 없을 경우를 참고하십시오.

부적절한 보안 그룹 규칙

장애 현상: 자가 진단 툴을 통해 진단한 결과, 보안 그룹 규칙 설정이 적합하지 않아 로그인하지 못하는 경우입니다.
처리 순서: 보안 그룹(포트) 진단 툴을 통해 문제를 해결합니다.
주의사항 :
원격으로 로그인한 Windows 인스턴스의 경우 포트 3389를 개방해야 합니다.



보안 그룹에 대한 사용자 정의 규칙을 사용자 정의하려면 보안 그룹 규칙 추가를 참고하십시오.

방화벽 또는 보안 소프트웨어로 인한 예외

장애 현상: CVM 방화벽 또는 보안 소프트웨어로 인해 로그인 시도가 실패했습니다.

문제 진단: VNC를 통해 Windows 인스턴스에 로그인하여 방화벽이 활성화되어 있는지, 360 Total Security 또는 보안 동글(dongles)과 같은 보안 소프트웨어가 서버에 설치되어 있는지 확인하십시오.

주의사항 :

이 작업에는 CVM 방화벽을 종료하는 작업이 포함됩니다. 이를 수행하려면 해당 권한이 있는지 확인하십시오.

처리 순서: 방화벽 또는 설치된 보안 소프트웨어를 종료한 후 원격으로 다시 액세스를 시도하십시오. 예를 들어 다음과 같이 Windows Server 2016의 방화벽을 종료할 수 있습니다.

1. VNC 로그인을 통해 인스턴스에 로그인합니다.
2. 운영 체제의 바탕 화면에서

을(를) 클릭하고 **제어판**을 선택합니다.

3. 제어판 창에서 **Windows 방화벽**을 클릭합니다.

4. Windows 방화벽 창에서 왼쪽에 있는 **Windows 방화벽 활성화 또는 비활성화**를 클릭하여 '사용자 정의 설정'을 엽니다.
5. **개인 네트워크 설정** 및 **공용 네트워크 설정**을 **Windows 방화벽 비활성화**로 설정하고 **확인**을 클릭합니다.
6. 인스턴스를 재시작하고 원격으로 다시 액세스를 시도하십시오.

원격 데스크톱을 통한 액세스 중 인증 오류

장애 현상: 원격 데스크톱을 통해 Windows 인스턴스에 로그인하려고 하면 '인증 오류입니다. 함수에 잘못된 플래그가 제공되었습니다.'라는 메시지가 표시됩니다. 또는 '인증 오류입니다. 필요한 기능이 지원되지 않습니다.'가 나타납니다.
문제 원인: Microsoft는 2018년 3월에 보안 업데이트를 출시했습니다. 이 업데이트는 자격 증명 보안 지원 프로그램(CredSSP)이 인증 프로세스 중 요청의 유효성을 검사하는 방식을 수정하여 CredSSP의 원격 코드 실행 취약점을 수정합니다. 클라이언트와 서버를 모두 업데이트해야 하며 그렇지 않으면 이전 오류가 발생할 수 있습니다.
처리 순서: 보안 업데이트를 설치합니다(권장). 자세한 내용은 Windows 인스턴스: 신분 인증 오류가 발생할 경우를 참고하십시오.

기타 솔루션

상기 방법을 시도한 후에도 여전히 Window 인스턴스에 로그인할 수 없으면 자가 진단 결과를 저장하고, 지원을 위해 티켓 제출을 통해 피드백을 보내주십시오.

Windows 인스턴스: 신분 인증 오류가 발생할 경우

최종 업데이트 날짜: : 2024-02-02 11:09:47

문제 설명

원격 데스크톱 연결을 통해 Windows 인스턴스에 로그인할 때 다음의 오류 발생.
‘인증 오류입니다. 기능에 제공된 토큰이 잘못되었습니다’.
‘인증 오류입니다. 요청한 기능이 지원되지 않습니다’.

문제 분석

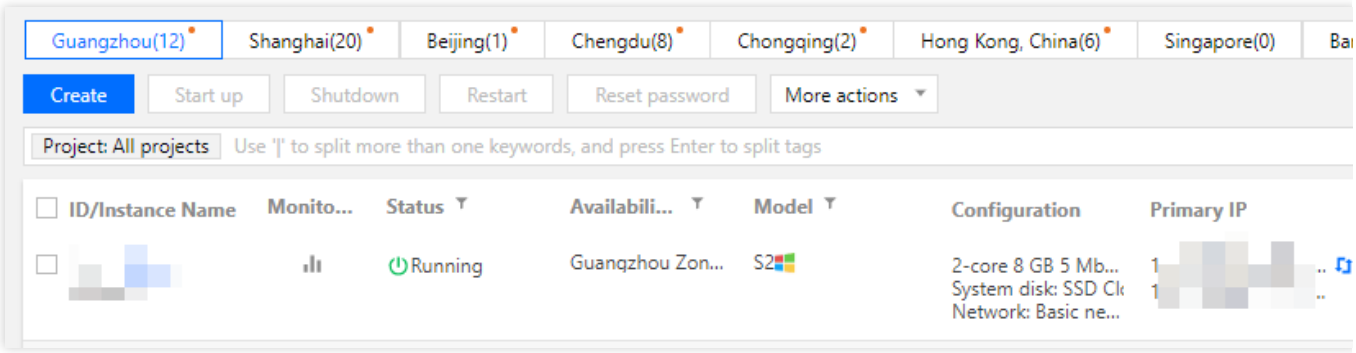
Microsoft에서 2018년 3월에 배포한 보안 업데이트가 CredSSP 프로토콜을 지원함과 동시에, 실명 인증의 인증 요청 방식을 업데이트하여 CredSSP의 원격 코드 실행 취약점이 수정되었습니다. 따라서 클라이언트와 서버 모두 이 업데이트를 설치해야 하며, 그렇지 않으면 문제 설명에서 서술한 상황이 발생할 수 있습니다.
원격 연결에 실패하는 이유는 다음 세 가지 경우가 있습니다.
경우1: 클라이언트 패치 안 함, 서버에 보안 업데이트 설치됨, 정책이 "강제 업데이트된 클라이언트"로 설정됨
경우2: 서버 패치 안 함, 클라이언트에 보안 업데이트 설치됨, 정책이 "강제 업데이트된 클라이언트"로 설정됨
경우3: 서버 패치 안 함, 클라이언트에 보안 업데이트 설치됨, 정책이 "완화"로 설정됨

솔루션

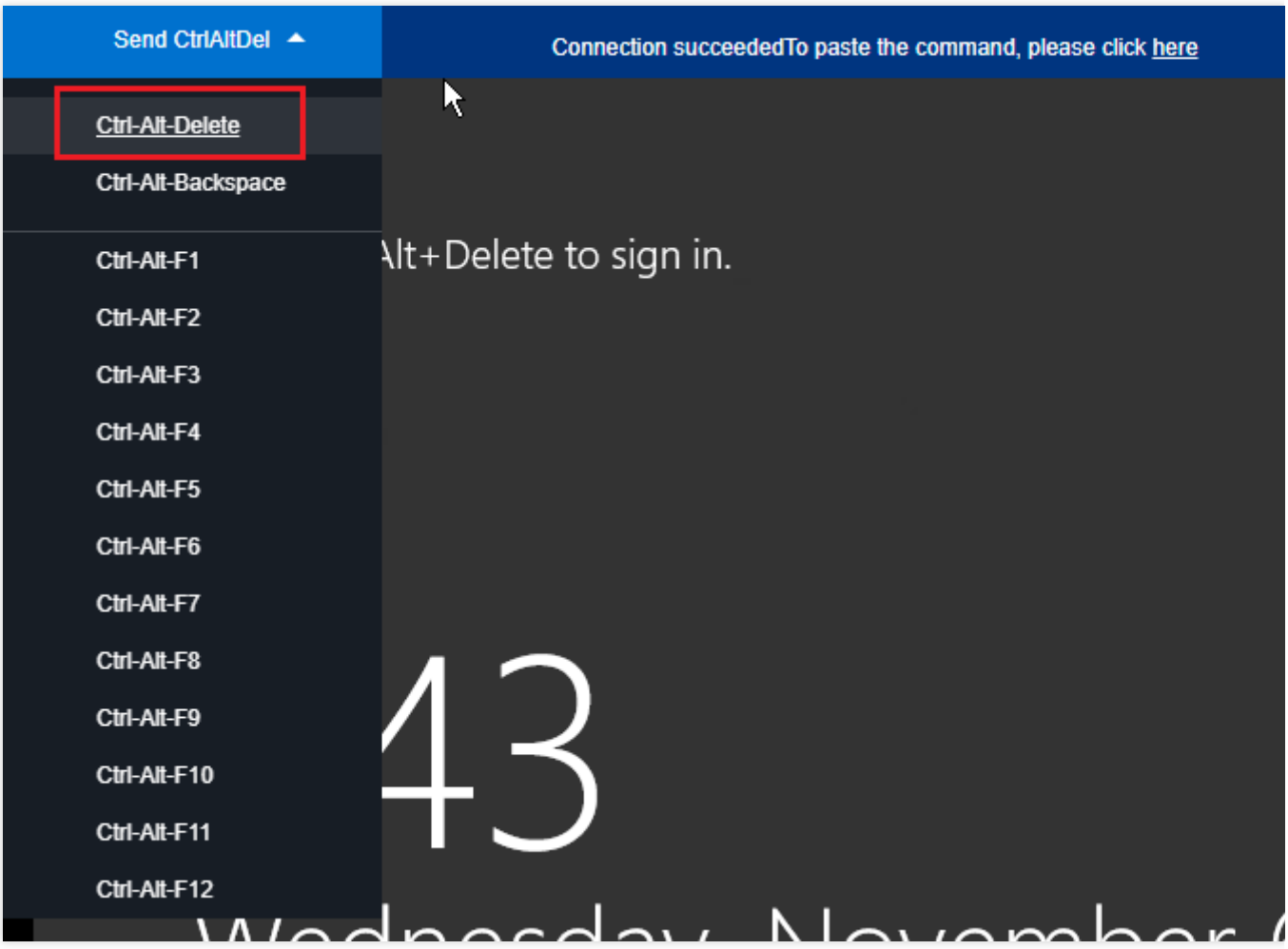
설명 :
클라이언트를 로컬에서만 업그레이드해야 하는 경우 솔루션1: 보안 업데이트 설치(권장)를 사용하십시오.

VNC로 CVM에 로그인

1. CVM 콘솔에 로그인합니다.
2. 아래 이미지와 같이 인스턴스 관리 페이지에서 타깃 CVM 인스턴스를 찾아 **로그인**을 클릭합니다.



3. '표준 로그인 | Windows 인스턴스' 팝업 창에서 **VNC 로그인**을 선택합니다.
4. 아래 이미지와 같이 팝업된 로그인 창 왼쪽 상단의 "원격 명령어 전송"을 선택하고 **Ctrl-Alt-Delete**를 클릭해 시스템 로그인 인터페이스에 진입합니다.



5. 로그인 비밀번호를 입력하고 **Enter**를 눌러 Windows CVM에 로그인합니다.

솔루션1: 보안 업데이트 설치(권장)

보안 업데이트를 설치하여 패치하지 않은 클라이언트/서버를 업데이트합니다. 각 시스템에 따른 업데이트 현황은 CVE-2018-0886 | CredSSP 원격 코드 실행 취약점을 참고 바랍니다. 본 솔루션은 Windows Server 2016을 예로 듭니

다.
기타 운영 체제는 다음 작업을 참고하여 **Windows 업데이트**를 열 수 있습니다.
Windows Server 2012:

> **제어판** > **시스템 및 보안** >**Windows 업데이트**
Windows Server 2008: **시작** > **제어판** > **시스템 및 보안** > **Windows Update**
Windows10:

> **설정** > **업데이트 및 보안**
Windows 7:

> **제어판** > **시스템 및 보안** > **Windows Update**
1. 바탕 화면에서

을(를) 클릭하고 **설정**을 선택합니다.
2. '설정' 창에서 **업데이트 및 보안**을 선택합니다.
3. **업데이트 및 보안** 페이지에서 **Windows 업데이트**를 선택하고 **업데이트 확인**을 클릭합니다.
4. **업데이트 설치**를 클릭합니다.
5. 설치 완료 후 인스턴스를 재시작하여 업데이트를 완료합니다.

솔루션2: 정책 설정 수정

보안 업데이트가 설치된 CVM에서 **암호화 Oracle 수정** 정책을 '취약'으로 설정합니다. 이 솔루션은 Windows Server 2016을 예시로 사용합니다. 다음 단계를 완료하십시오.
주의사항 :
Windows 10 Home 운영 체제에서 그룹 정책 편집기를 사용할 수 없는 경우 레지스트리에서 정책을 수정할 수 있습니다. 자세한 내용은 솔루션3: 레지스트리 수정을 참고하십시오.
1. 바탕 화면에서

을(를) 클릭하고 **gpedit.msc**를 입력하고 **Enter**키를 눌러 '로컬 그룹 정책 편집기'를 엽니다.
설명 :
또는 '**Win+R**' 키를 눌러 실행 대화 상자를 열 수도 있습니다.

2. 왼쪽 탐색 트리에서 **컴퓨터 구성** > **관리 템플릿** > **시스템** > **자격 증명 위임**을 선택하고 **암호화 Oracle 수정**을 더블 클릭합니다.
3. '암호화 Oracle 수정' 창에서 **활성화됨**을 선택하고 **보호 레벨**을 **취약**으로 설정합니다.
4. **확인**을 클릭하여 구성을 마칩니다.

솔루션3: 레지스트리 수정

1. 바탕 화면에서

을(를) 클릭하고 **regedit**를 입력하고 **Enter**키를 눌러 레지스트리 편집기를 엽니다.
설명：
또는 '**Win+R**' 키를 눌러 실행 대화 상자를 열 수도 있습니다.
2. 왼쪽 탐색 트리에서 **컴퓨터** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Microsoft** > **Windows** > **CurrentVersion** > **Policies** > **System** > **CredSSP** > **Parameters**를 선택합니다.
설명：
해당 경로가 없으면 수동으로 생성합니다.
3. **Parameters**를 마우스 우클릭 후 **새로 만들기** > **DWORD(32비트) 값**을 선택하고 파일 이름을 'AllowEncryptionOracle'로 지정합니다.
4. 새로 생성된 'AllowEncryptionOracle' 파일을 더블 클릭하고 '값 데이터'를 '2'로 설정한 후 **확인**을 클릭합니다.
5. 인스턴스를 재시작합니다.

관련 문서

CVE-2018-0886 | CredSSP 원격 코드 실행 취약점
CVE-2018-0886 의 CredSSP 업데이트

CVM 암호 재설정 실패 또는 유효하지 않을 경우

최종 업데이트 날짜: : 2024-02-02 11:09:47

본문은 Windows Server 2012 운영 체제를 예로 들어, 비밀번호 재설정에 실패하거나 재설정한 비밀번호가 적용되지 않는 Window CVM 인스턴스에 대한 문제 진단 방법 및 솔루션을 소개합니다.

현상 설명

CVM 비밀번호를 재설정한 후 '시스템 오류로 인스턴스 비밀번호 재설정에 실패했습니다(7617d94c)' 표시됨
CVM 비밀번호를 재설정한 후 새로운 비밀번호가 적용되지 않아 여전히 변경 전 비밀번호로 로그인됨

예상 원인

다음과 같은 원인으로 CVM 비밀번호 재설정에 실패하거나 재설정한 비밀번호가 적용되지 않을 수 있습니다.
CVM 내 `cloudbase-init` 컴포넌트의 손상, 수정, 비활성화 또는 미실행
CVM에 360 Total Security 또는 Huorong Security와 같은 타사 보안 소프트웨어를 설치한 경우, 타사 보안 소프트웨어가 비밀번호 재설정 컴포넌트 'cloudbase-init'를 차단하여 인스턴스 비밀번호 재설정이 무효화됨

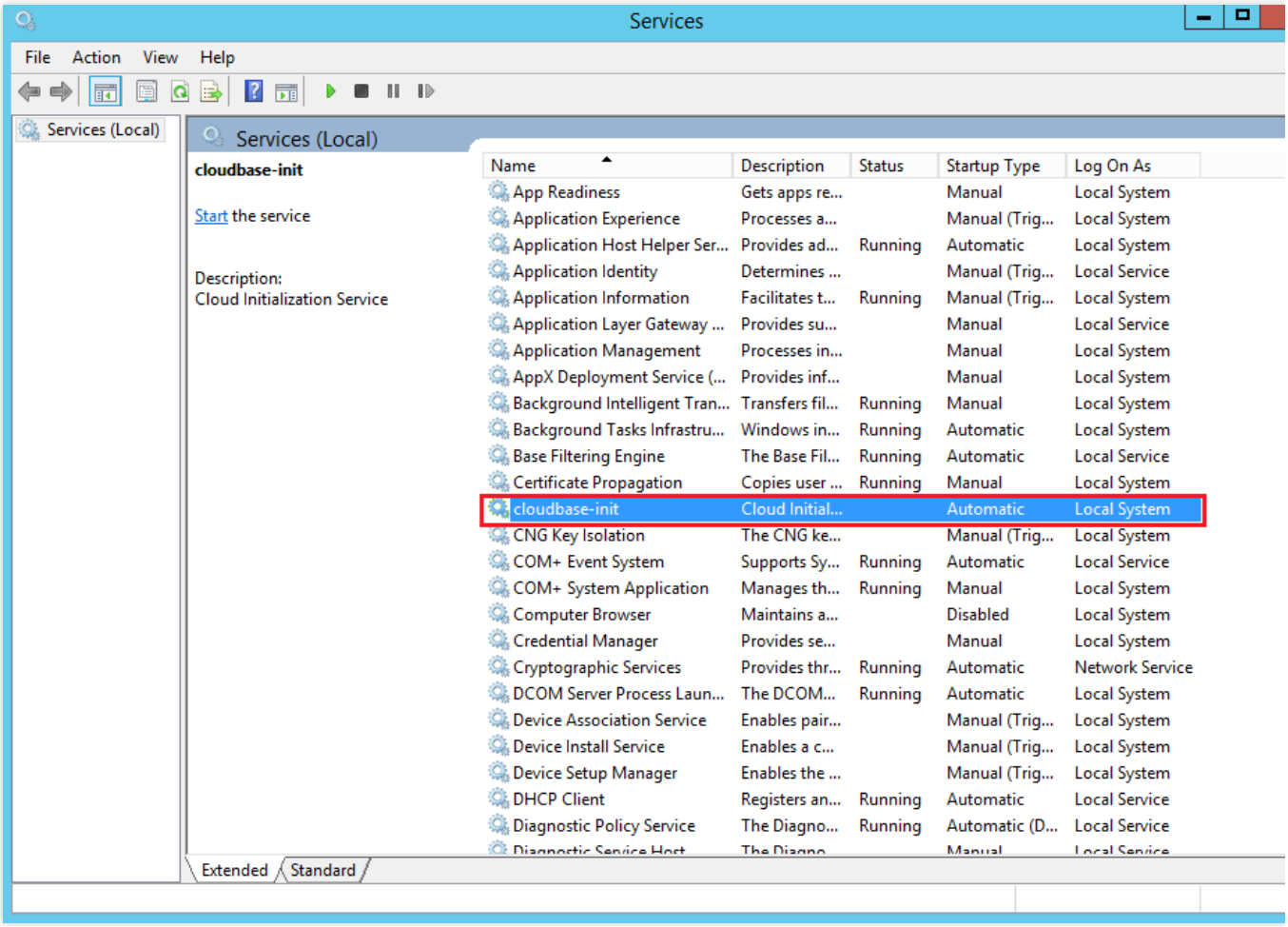
장애 진단 및 프로세스

비밀번호 재설정에 실패하는 문제의 예상 원인에 따라, 다음 두 가지 검사 방법을 제안합니다.

cloudbase-init 서비스 검사

1. 표준 로그인 방식으로 Windows 인스턴스에 로그인(권장)을 참고하여 타깃 Windows 인스턴스에 로그인합니다.
2. 운영 체제 인터페이스에서

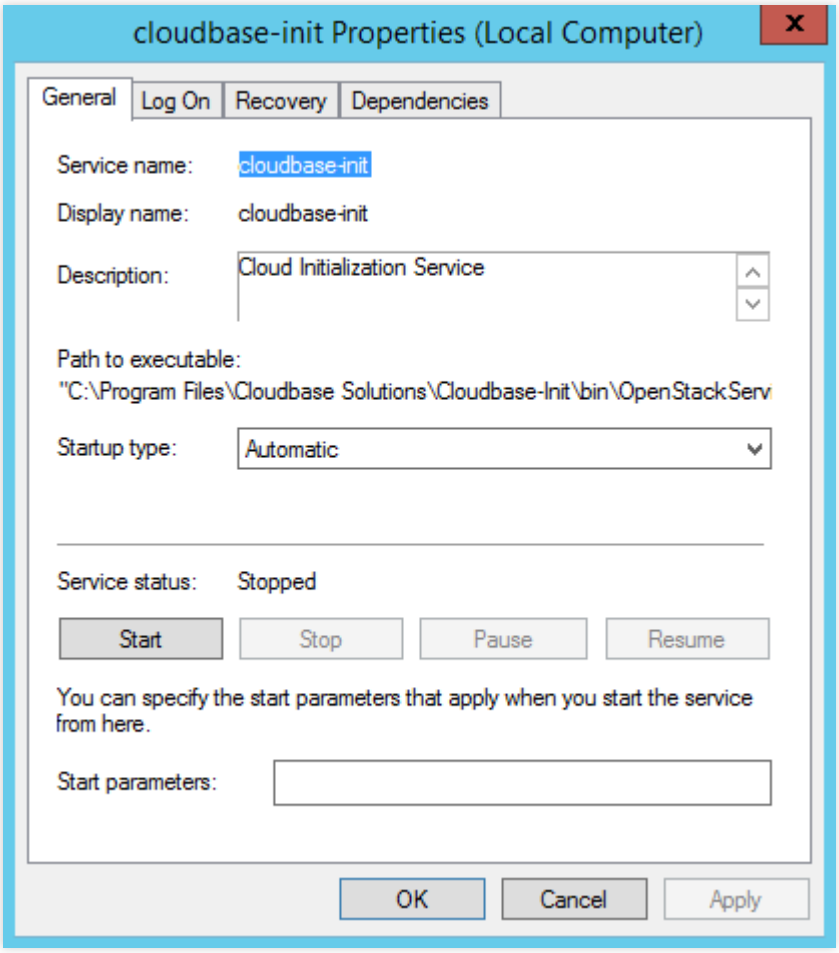
을(를) 우클릭하여 [실행]을 선택하고, [실행] 창에 **services.msc**를 입력한 뒤 **Enter**를 눌러 '서비스' 창을 엽니다.
3. 아래 이미지와 같이 `cloudbase-init` 서비스가 있는지 확인합니다.



서비스가 있으면 다음 단계를 실행합니다.

서비스가 없으면 `cloudbase-init` 서비스를 재설치합니다. 자세한 작업 방법은 Windows 운영 체제에서 Cloudbase-Init 설치를 참고하십시오.

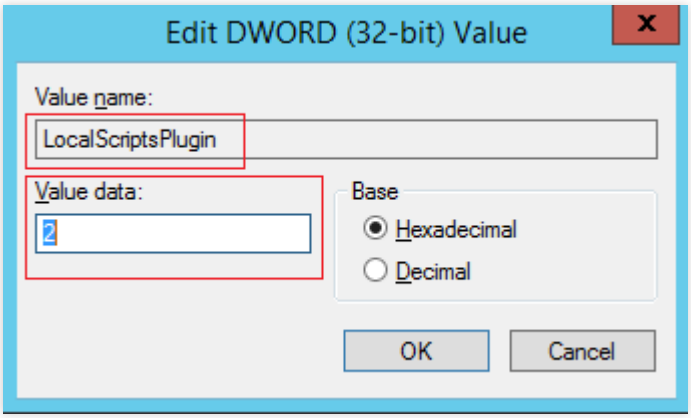
4. 아래 이미지와 같이 더블 클릭하여 `cloudbase-init` 의 속성을 엽니다.



5. [일반] 탭에서 `cloudbase-init` 의 실행 유형이 [자동]으로 설정되어 있는지 확인합니다.
서비스가 있으면 다음 단계를 실행합니다.
자동으로 설정되어 있지 않으면 `cloudbase-init` 의 실행 유형을 [자동]으로 설정합니다.
6. [로그인] 탭으로 이동해 `cloudbase-init` 의 로그인 계정이 [로컬 시스템 계정]으로 설정되어 있는지 확인합니다.
서비스가 있으면 다음 단계를 실행합니다.
로컬 시스템 계정으로 설정되어 있지 않으면 `cloudbase-init` 의 로그인 계정을 [로컬 시스템 계정]으로 설정합니다.
7. [일반] 탭으로 이동해 서비스 상태의 [실행]을 클릭하여 `cloudbase-init` 서비스를 수동 실행한 뒤 오류가 발생하는지 살펴봅니다.
오류가 발생하면 CVM에 설치된 보안 프로그램 검사를 진행합니다.
오류가 발생하지 않으면 다음 단계를 실행합니다.
8. 운영 체제 인터페이스에서

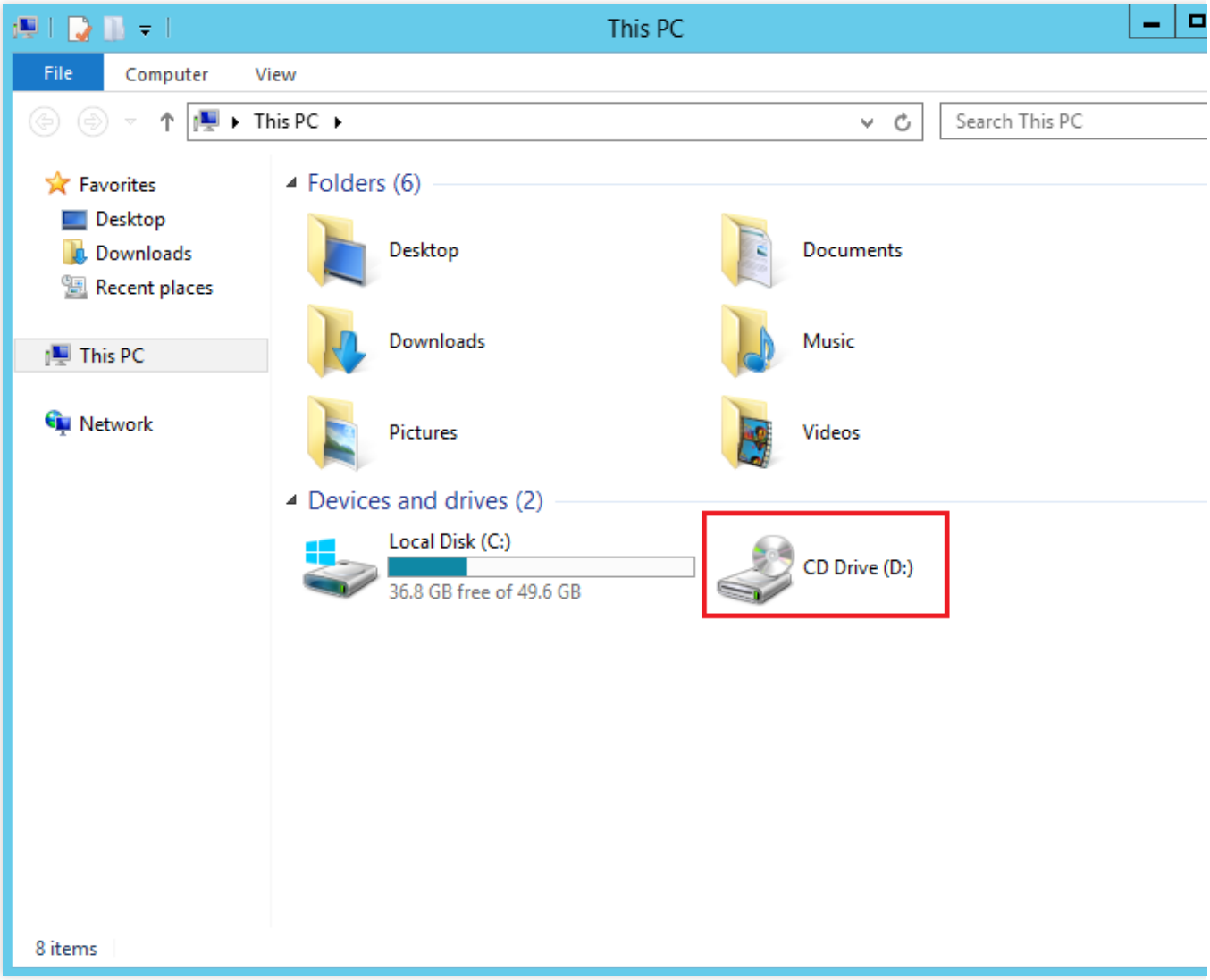
을(를) 우클릭하여 [실행]을 선택하고, [실행] 창에 **regedit**을 입력한 뒤 **Enter**를 눌러 '레지스트리 편집기' 창을 엽니다.

9. 왼쪽의 레지스트리 사이드바에서 [HKEY_LOCAL_MACHINE]>[SOFTWARE]>[Cloudbase Solutions]>[Cloudbase-Init] 디렉터리를 순서대로 펼칩니다.
10. [ins-xxx] 아래의 모든 'LocalScriptsPlugin' 레지스트리를 찾아, LocalScriptsPlugin 값이 2인지 확인합니다.



2가 맞다면, 다음 단계를 실행합니다.
값이 다르면 LocalScriptsPlugin의 값을 2로 설정합니다.
11. 운영 체제 인터페이스에서

을(를) 클릭하여 [내 컴퓨터]를 선택한 뒤, 아래 이미지와 같이 디바이스 및 드라이브에 CD-드라이브를 로딩했는지 확인합니다.



로딩하였다면, CVM에 설치된 보안 프로그램 검사를 진행합니다.
로딩하지 않은 경우 장치 관리자에서 CD-ROM 디스크 드라이버를 실행합니다.

CVM에 설치된 보안 프로그램 검사

설치된 보안 프로그램에서 전체 디스크 스캔을 선택하여, CVM의 취약점과 `cloudbase-init` 의 핵심 컴포넌트 차단 여부를 검사합니다.
CVM의 취약점을 발견했다면 복구해야 합니다.
핵심 컴포넌트가 차단되었다면 차단을 해제해야 합니다.
`cloudbase-init` 모듈 검사 및 설정 단계는 다음과 같습니다.
1. 표준 로그인 방식으로 Windows 인스턴스에 로그인(권장)을 참고하여 타깃 Windows 인스턴스에 로그인합니다.
2. 실제 설치된 타사 보안 프로그램에 'cloudbase-init' 컴포넌트를 복원 및 설정합니다.

Windows 인스턴스: 원격 데스크탑 서비스에 로그인 권한이 없을 경우

최종 업데이트 날짜: : 2024-02-02 11:09:48

장애 현상

상황 설명(1)

Windows가 원격 데스크탑으로 Windows 인스턴스에 연결할 때 "사용자 계정에 원격 로그인 권한이 없기 때문에 연결이 거부되었습니다."라는 메시지가 뜹니다.

상황 설명(2)

Windows가 원격 데스크탑으로 Windows 인스턴스에 연결할 때 "원격 로그인을 하려면 사용자가 원격 데스크탑 서비스로 로그인을 할 수 있는 권한이 필요합니다. 원격 데스크탑 사용자 그룹의 멤버에게는 이 권한이 기본으로 부여되어 있습니다. 단, 사용자가 소속된 그룹에 이 권한이 없거나 원격 데스크탑 사용자 그룹에서 이 권한을 삭제했을 경우엔 수동으로 부여해야 합니다."라고 메시지가 뜹니다.

장애 원인

이 사용자는 원격 데스크탑 연결 방식을 통해 Windows 인스턴스에 로그인이 허용되지 않았습니다.

솔루션

원격 데스크탑을 통해 Windows 인스턴스에 연결할 때 상황 설명(1)의 경우가 발생했을 때 사용자 계정을 Windows 인스턴스가 설정한 원격 데스크탑 서비스를 통한 로그인 허용 리스트에 추가해야 합니다. 자세한 작업 순서는 원격 로그인 권한 허용 설정을 참조하십시오.
사용자가 원격 데스크탑을 통해 Windows 인스턴스에 연결할 때 상황 설명(2)의 경우가 발생했을 때 사용자 계정을 Windows 인스턴스가 설정한 원격 데스크탑 서비스를 통한 로그인 거부 리스트에서 삭제해야 합니다. 자세한 작업 순서는 원격 로그인의 권한 거부 수정을 참조하십시오.

프로세스 순서

VNC 방식을 통해 CVM에 로그인

1. CVM 콘솔에 로그인합니다.
2. 인스턴스의 관리 페이지에서 목표 CVM 인스턴스를 찾은 후 [Log In]을 클릭합니다.
3. 팝업된 "Windows 인스턴스 로그인" 창에서 [Alternative login methods(VNC)]을 선택하고 [Log In Now]을 클릭하여 CVM에 로그인합니다.
4. 팝업된 로그인 창에서 좌측 상단의 "원격 명령어 발송"을 선택하고 **Ctrl-Alt-Delete**를 클릭해 시스템 로그인 인터페이스에 접속합니다.

원격 로그인을 허용하는 권한 설정

설명：

다음 작업은 Windows Server 2016를 예로 듭니다.

1. 운영 체제 인터페이스에서

클릭하고 **gpedit.msc**를 입력한 후 **Enter**를 눌러 "로컬 그룹 정책 에디터"를 엽니다.

2. 왼쪽 메뉴에서 [컴퓨터 설정]>[Windows 설정]>[보안 설정]>[로컬 정책]>[사용자 권한 할당]을 선택하고 [원격 데스크탑 서비스를 통한 로그인 허용]을 더블 클릭하여 엽니다.
3. 열린 "원격 데스크탑 서비스를 통한 로그인 허용 속성" 창에서 원격 데스크탑 서비스를 통한 로그인 허용 사용자 리스트에 로그인해야 하는 계정이 존재하는지 점검합니다.

해당 사용자가 원격 데스크탑 서비스를 통한 로그인 허용 리스트에 없으면 4단계를 실행하십시오.

해당 사용자가 원격 데스크탑 서비스를 통한 로그인 허용 리스트에 있으면 Submit Ticket을 통해 피드백하십시오.

4. [
사용자 또는
그룹 추가]를 클릭하고 “사용자 또는 그룹 선택” 창을 엽니다.
5. 원격 로그인을 해야 하는 계정을 입력하고 [확인]을 클릭합니다.
6. [확인]을 클릭하고 로컬 그룹 정책 에디터를 닫습니다.
7. 인스턴스를 재시작하고 이 계정 원격 데스크탑을 사용해 Windows 인스턴스에 연결을 재시도합니다.

원격 로그인을 거부하는 권한 수정

설명：

다음 작업은 Windows Server 2016를 예로 듭니다.

1. 운영 체제 인터페이스에서

클릭하고 **gpedit.msc**를 입력한 후 **Enter**를 눌러 "로컬 그룹 정책 에디터"를 엽니다.

2. 왼쪽 메뉴에서 [컴퓨터 설정]>[Windows 설정]>[보안 설정]>[로컬 정책]>[사용자 권한 할당]을 선택하고 더블 클릭으로 [원격 데스크탑 서비스를 통한 로그인 거부]를 엽니다.
3. 열린 "원격 데스크탑 서비스를 통한 로그인 거부 속성" 창에서 원격 데스크탑 서비스를 통한 로그인 거부 사용자 리스트에 로그인해야 하는 계정이 존재하는지 점검합니다.

해당 사용자가 원격 데스크탑 서비스를 통한 로그인 거부 리스트에 있으면 로그인해야 하는 계정을 리스트에서 삭제하고 인스턴스를 재시작하십시오.
사용자가 원격 데스크탑 서비스를 통한 로그인 거부 리스트에 없으면 Submit Ticket을 통해 피드백하십시오.

Windows 인스턴스: 네트워크 등급 신분 인증이 필요한 경우

최종 업데이트 날짜: : 2024-02-02 11:09:47

본 문서는 Windows 인스턴스에 원격 연결할 때 "네트워크 수준 인증이 필요합니다" 등의 알림이 표시되는 경우에 대한 처리 방법을 소개합니다.

장애 현상

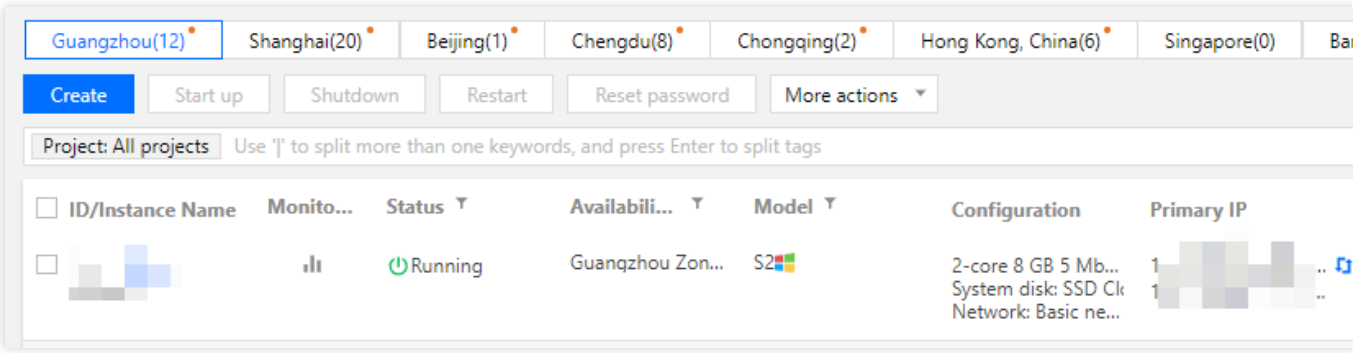
Windows 시스템 자체의 원격 데스크톱 연결을 사용하면, 가끔 원격 컴퓨터에 연결할 수 없는 문제가 나타나며 "네트워크 수준 인증이 필요합니다"와 같은 알림이 표시됩니다.

장애 처리

설명 :
다음 작업은 Windows Server 2016을 예로 듭니다.

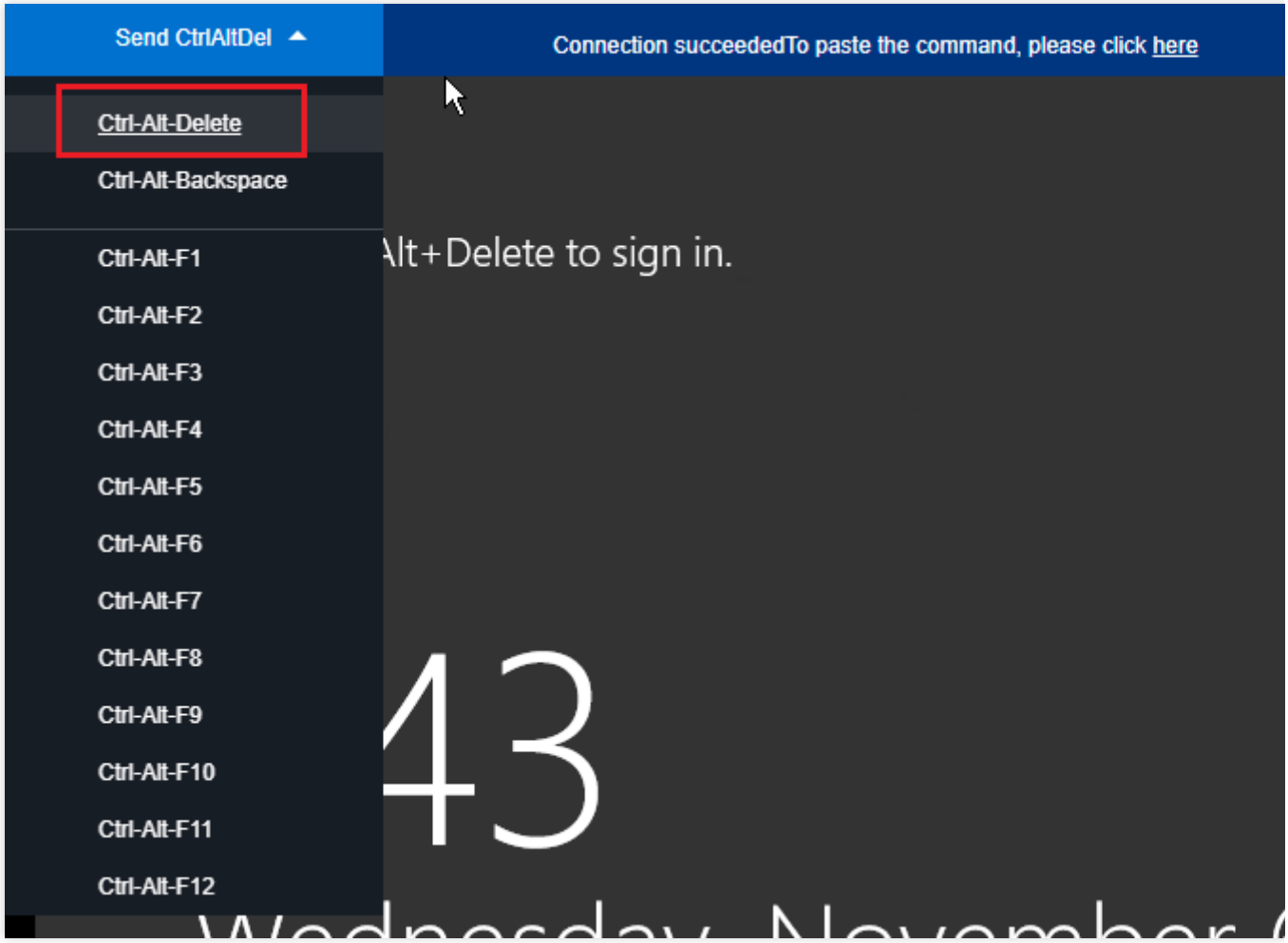
VNC 방식을 통해 CVM에 로그인

1. CVM 콘솔에 로그인합니다.
2. 인스턴스의 관리 페이지에서 타깃 CVM 인스턴스를 찾아 [Log In]을 클릭합니다. 아래 이미지 참조



3. 팝업된 "Windows 인스턴스 로그인" 창에서 [Alternative login methods(VNC)]]을 선택하고 [Log In Now]을 클릭하여 CVM에 로그인합니다.

4. 팝업된 로그인 창 왼쪽 상단의 "원격 명령어 발송"을 선택하고 **Ctrl-Alt-Delete**를 클릭하여 시스템 로그인 인터페이스에 접속합니다. 아래 이미지 참조

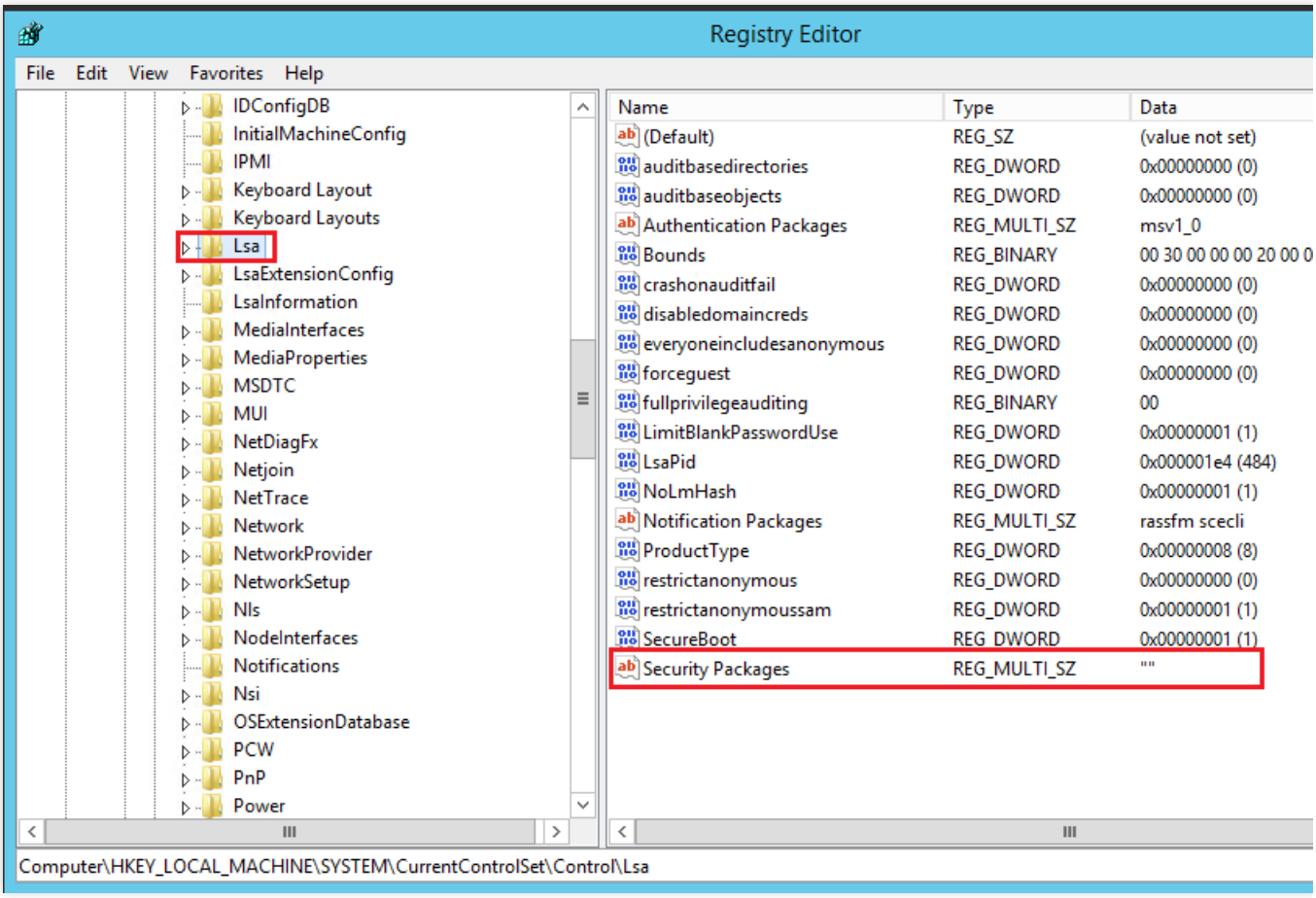


레지스트리 수정

1. 운영 체제 인터페이스에서

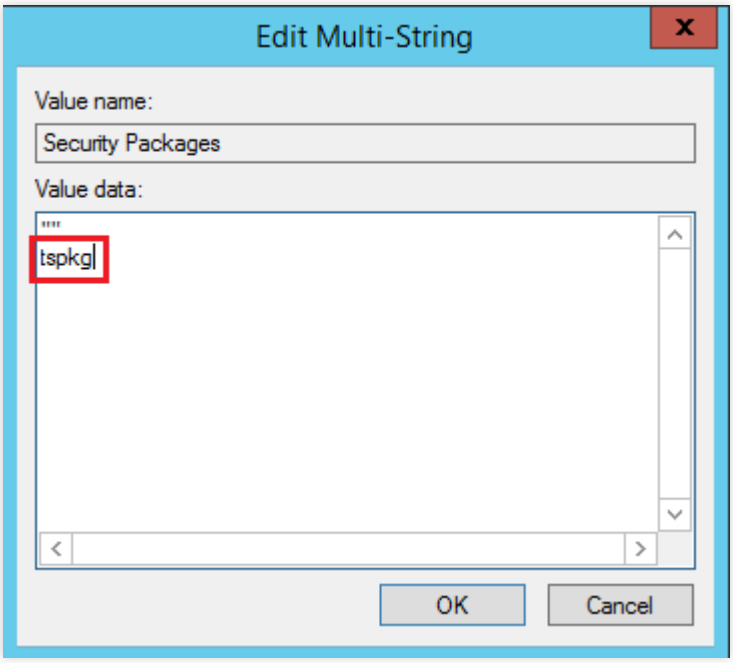
를 클릭하고 **regedit**를 입력한 후 **Enter**를 눌러 레지스트리 편집기를 엽니다.

2. 왼쪽 메뉴에서 차례대로 [컴퓨터]>[HKEY_LOCAL_MACHINE]>[SYSTEM]>[CurrentControlSet]>[Control]>[Lsa] 디렉터리를 열고 오른쪽 창에서 [Security Packages]를 찾습니다. 아래 이미지 참조

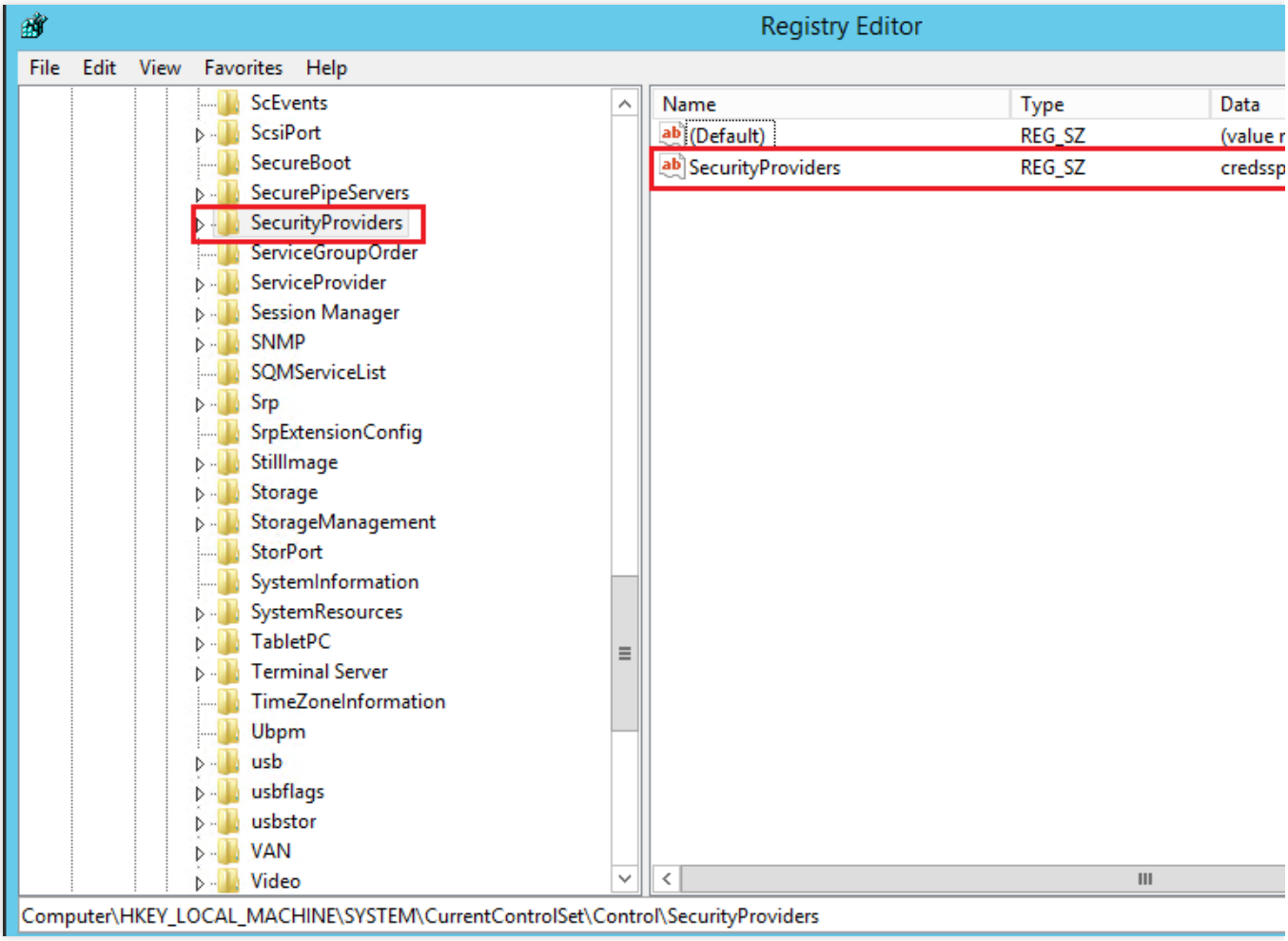


3. [Security Packages]를 더블 클릭하여 [다중 문자열 편집] 창을 엽니다.

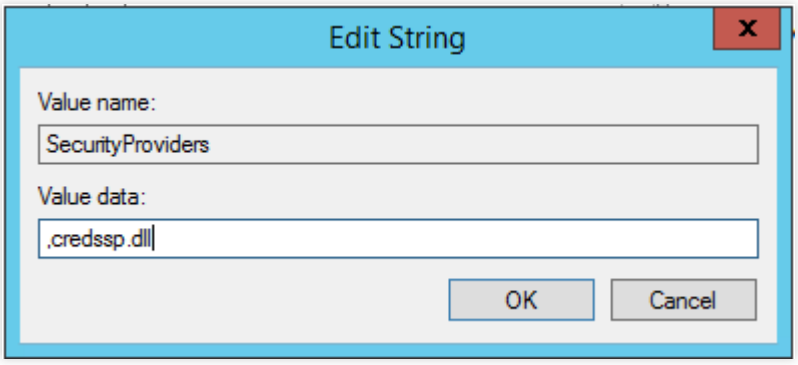
4. "다중 문자열 편집" 창에서 [tspkg] 문자를 추가하고 [확인]을 클릭합니다. 아래 이미지 참조



5. 왼쪽 메뉴에서 차례대로 [컴퓨터]>[HKEY_LOCAL_MACHINE]>[SYSTEM]>[CurrentControlSet]>[Control]>[SecurityProviders] 디렉터리를 열고 우측 창에서 [SecurityProviders]를 찾습니다. 아래 이미지 참조



6. [SecurityProviders]를 더블 클릭하여 [문자열 편집] 창을 엽니다.
7. "문자열 편집" 창의 [값 데이터] 말미에 `, credssp.dll` 을 추가하고 [확인]을 클릭합니다. 아래 이미지 참조



8. 레지스트리 편집기를 닫고 인스턴스를 재시작하면 바로 원격 로그인할 수 있습니다.

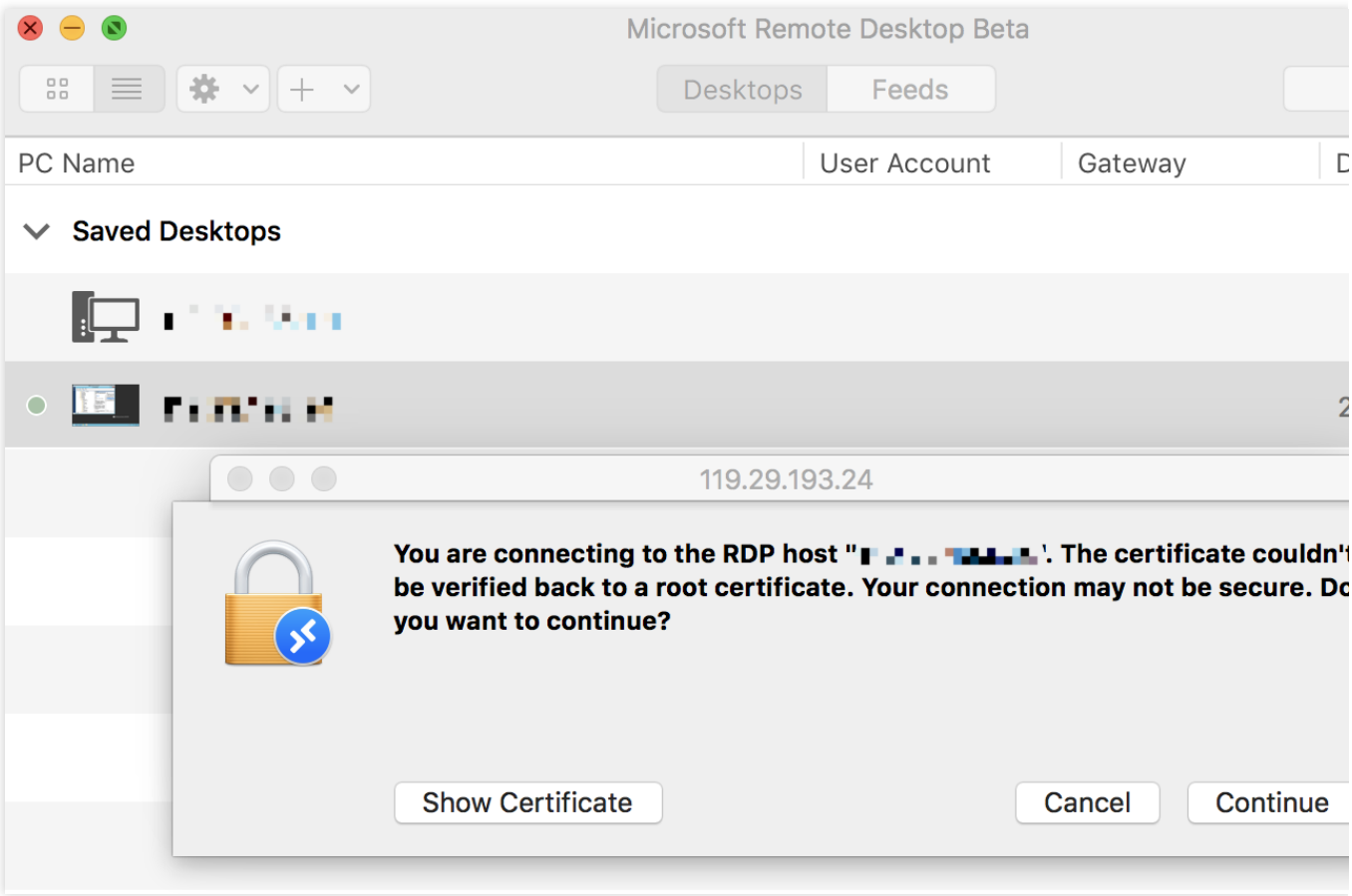
Windows 인스턴스: Mac 원격 로그인에 이상이 발생할 경우

최종 업데이트 날짜: : 2024-02-02 11:09:48

본 문서는 사용자의 Mac이 Microsoft Remote Desktop을 통해 Windows에 원격 로그인 시 흔히 볼 수 있는 장애 현상 및 솔루션을 소개합니다.

장애 현상

Mac이 Microsoft Remote Desktop을 통해 Windows에 원격 로그인 시, "The certificate couldn't be verified back to a root certificate."라는 알림이 뜹니다.



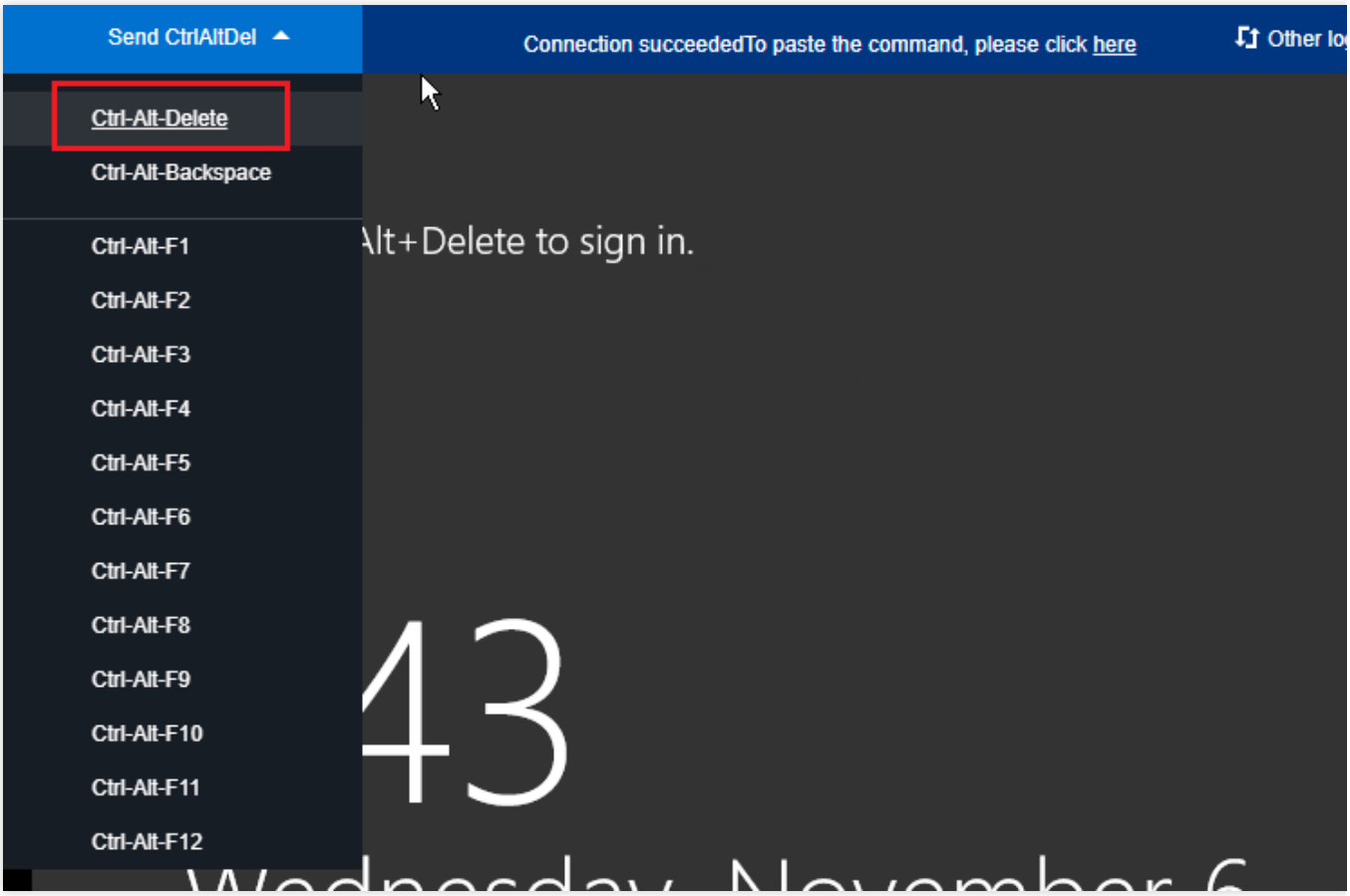
Mac 원격 데스크탑 연결(Remote Desktop Connection) 시, "원격 데스크탑에서 귀하가 연결하고자 하는 컴퓨터를 인증할 수 없습니다"라고 알림이 뜹니다.

장애 처리

설명：
다음 작업은 Windows Server 2016을 예로 듭니다.

VNC 방식을 통해 CVM에 로그인

1. CVM 콘솔에 로그인합니다.
2. "Instances" 페이지에서 목표 CVM 인스턴스를 찾고 [Log In]을 클릭합니다.
3. 팝업된 "Windows 인스턴스 로그인" 창에서 [Alternative login methods(VNC)]을 선택하고 [Log In Now]을 클릭하여 CVM에 로그인합니다.
4. 팝업된 로그인 창 왼쪽 상단의 "원격 명령어 발송"을 선택하고 **Ctrl-Alt-Delete**를 클릭하여 시스템 로그인 인터페이스에 접속합니다. 아래 이미지 참조



인스턴스 로컬 그룹 정책 수정

1. 운영 체제 인터페이스에서

를 클릭하고 **gpedit.msc**를 입력하고 **Enter**를 눌러 “로컬 그룹 정책 에디터”를 엽니다.

설명：

단축키 "Win+R"를 사용하여 실행 인터페이스를 열 수도 있습니다.

2. 왼쪽 메뉴에서 [컴퓨터 설정]>[템플릿 관리]>[Windows 컴포넌트]>[원격 데스크탑 서비스]>[원격 데스크탑 세션 호스트]>[보안]을 선택하고 [원격(RDP) 연결에 지정된 보안 레이어 사용 요청]을 더블클릭합니다.

3. 열린 "원격(RDP)연결에 지정된 보안 레이어 사용 요청" 창에서 [활성화]를 선택하고 [보안 레이어]를 [RDP]로 설정합니다.

4. [확인]을 클릭하여 설정을 완료합니다.

5. 인스턴스를 재시작하여 성공적으로 연결되었는지 다시 시도합니다. 여전히 연결 실패일 경우 Submit Ticket을 통해 피드백해 주시기 바랍니다.

Windows 인스턴스: CPU 혹은 메모리 점유율이 높아 로그인할 수 없을 경우

최종 업데이트 날짜: : 2024-02-02 11:09:48

본 문서는 CPU 혹은 메모리의 이용률이 높아 Windows CVM에 로그인할 수 없을 때의 진단 방법 및 솔루션을 소개합니다.

설명 :

다음 작업 순서는 Windows server 2012 R2를 예로 들며, 운영 체제 버전에 따라 세부 작업 순서에 차이가 있습니다.

예상 원인

CPU 혹은 메모리의 사용률이 지나치게 높으면 서비스 응답 속도가 느려지거나 서버에 로그인할 수 없는 등의 문제가 발생할 수 있습니다. CPU 혹은 메모리의 사용률을 지나치게 높이는 요소에는 하드웨어, 시스템 프로세스, 비즈니스 프로세스, 트로이 목마 바이러스 등이 있습니다. 클라우드 모니터링을 통해 CPU 사용률 임계 값 알림을 생성하여, CPU나 메모리의 사용률이 임계 값을 초과할 경우 즉시 사용자에게 공지하도록 설정할 수 있습니다.

진단 방향

1. CPU 혹은 메모리를 소모하는 세부 프로세스를 진단합니다.
2. CPU 혹은 메모리의 이용률이 높은 프로세스를 분석합니다.

비정상적인 프로세스일 경우 트로이 목마와 같은 바이러스가 원인일 수 있으므로, 사용자는 프로세스를 자체 종료하거나 보안 프로그램을 사용하여 바이러스를 검출할 수 있습니다.

비즈니스 프로세스일 경우 액세스량의 변화가 원인인지, 최적화 공간이 존재하는지 분석해야 합니다.

Tencent Cloud 모듈 프로세스일 경우, 티켓 제출을 통해 당사에 문의하여 진단하시기 바랍니다.

진단 툴

작업 관리자: Windows 자체의 응용 프로그램 및 프로세스 관리 툴로써, 실행 프로세스의 이름, CPU 부하, 메모리 사용, I/O 상태, 로그인된 사용자와 Windows 서비스 정보를 포함한 전반적인 컴퓨터 성능 및 실행 프로그램에 관한 정보를 보여줍니다.

프로세스: 시스템에서 실행 중인 모든 프로세스의 목록입니다.

성능: 전체적인 CPU 사용량과 사용 중인 메모리 등, 시스템 성능에 관한 전체적인 통계 정보입니다.

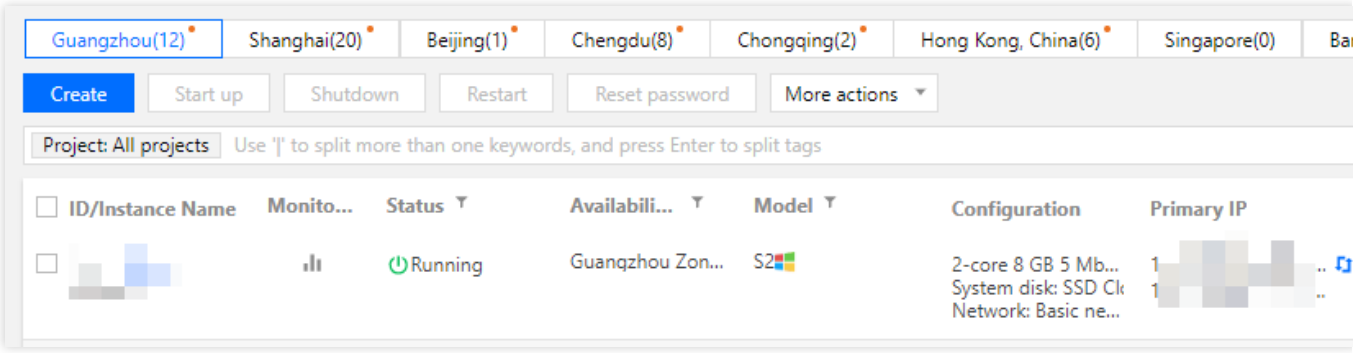
사용자: 현재 시스템에 세션이 있는 모든 사용자입니다.

세부 정보: 프로세스 탭의 상세 내용으로, 프로세스의 PID, 상태, CPU, 메모리 사용 현황 등 프로세스의 상세 정보를 표시합니다.
서비스: 시스템 내의 모든 서비스를 보여줍니다(실행 중지된 서비스 포함).

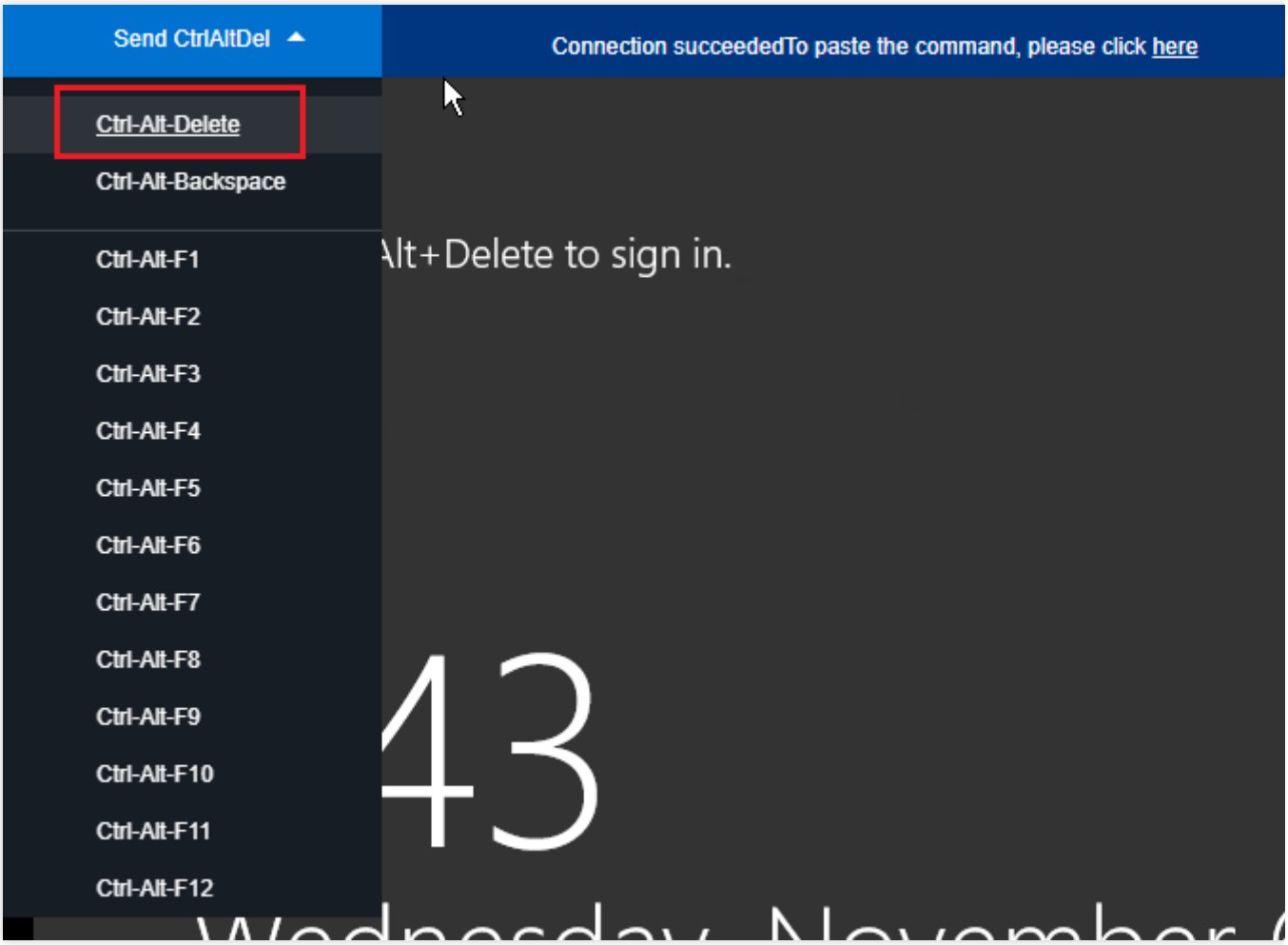
장애 처리

VNC 방식을 사용하여 CVM에 로그인

설명 :
CVM의 부하가 높으면 원격 연결을 구축하기 어려우므로, VNC 방식을 사용하여 Windows 인스턴스에 로그인하시길 권장합니다.
1. CVM 콘솔에 로그인합니다.
2. 아래 이미지와 같이, 인스턴스 관리 페이지에서 타깃 CVM 인스턴스를 찾아 [로그인]을 클릭합니다.

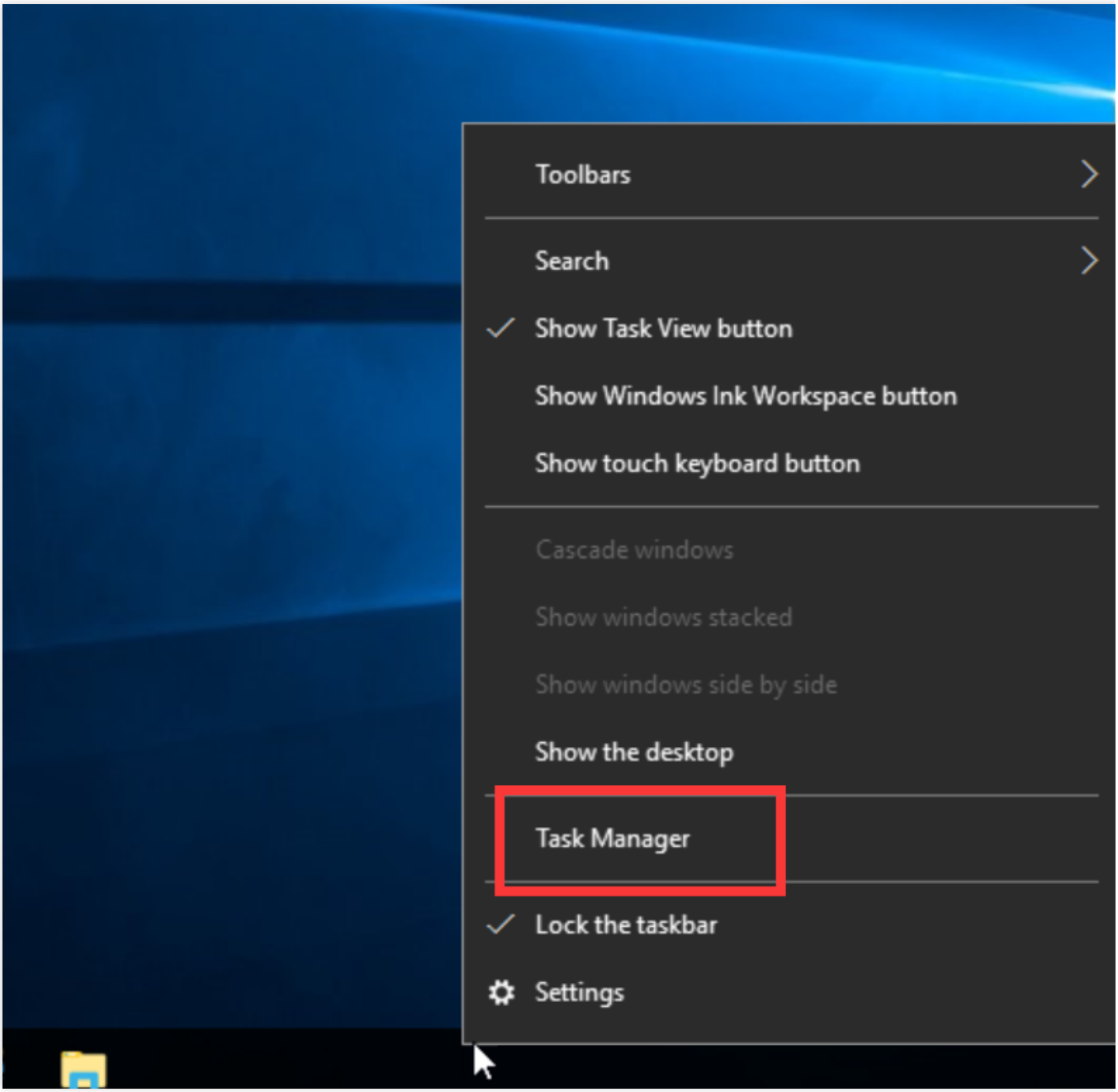


3. 팝업된 'Windows 인스턴스 로그인' 창에서 [기타 방식(VNC)]을 선택하고 [즉시 로그인]를 클릭하여 CVM에 로그인합니다.
4. 아래 이미지와 같이, 팝업된 로그인 창 왼쪽 상단의 '원격 명령어 전송'을 선택하고 **Ctrl-Alt-Delete**를 클릭해 시스템 로그인 인터페이스로 이동합니다.



프로세서 이용률 현황 조회

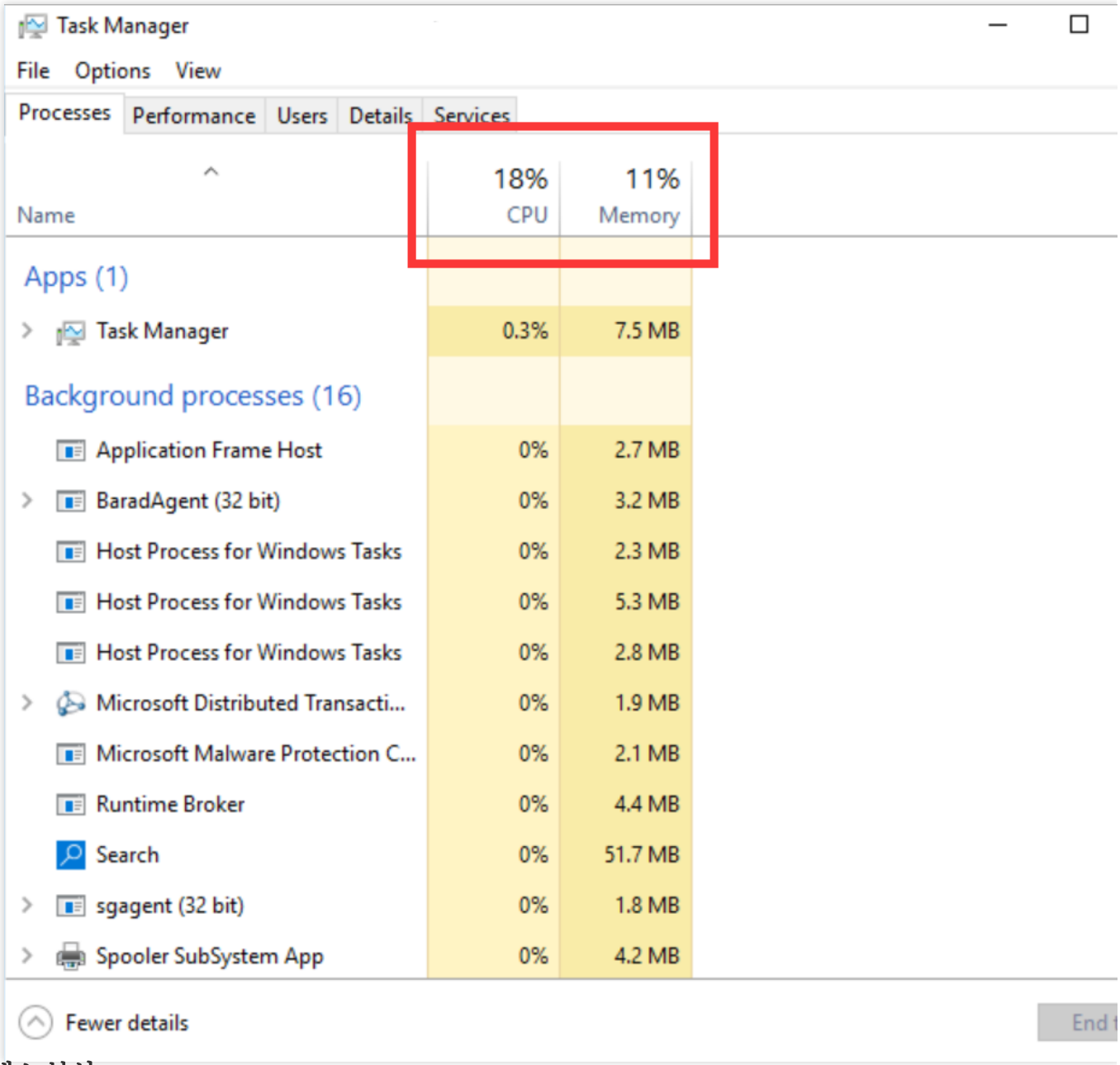
1. 아래 이미지와 같이, CVM에서 '작업 표시줄'을 우클릭한 뒤 [작업 관리자]를 선택합니다.



2. 아래 이미지와 같이, '작업 관리자'에서 리소스 이용률을 바로 확인할 수 있습니다.

설명：

CPU 혹은 메모리를 클릭하여 오름차순/내림차순으로 프로세스를 정렬할 수 있습니다.



프로세스 분석

작업 관리자의 프로세스에 따라 문제를 분석 및 진단하고 적합한 솔루션을 채택합니다.

대량의 CPU 혹은 메모리 리소스를 사용하는 프로세스가 시스템 프로세스일 경우

시스템 프로세스가 대량의 CPU 혹은 메모리 리소스를 사용하고 있을 경우, 아래의 내용을 진단하시기 바랍니다.
1. 프로세스 이름을 검사합니다.
일부 바이러스는 svch0st.exe, explore.exe, iexplorer.exe 등 시스템 프로세스와 유사한 이름을 사용합니다.
2. 프로세스에 대응하는 파일의 위치를 점검합니다.
시스템 프로세스는 일반적으로 `C:\\Windows\\System32` 디렉터리에 위치해 있으며, 완전한 서명 및 설명이 있습니다. 작업 관리자에서 프로세스를 우클릭한 뒤 [파일 위치 열기]를 선택하면 파일이 실행되는 자세한 위치를 조회할 수 있습니다.

프로세스의 위치가 `C:\\Windows\\System32` 디렉터리에 있지 않다면, CVM이 바이러스에 감염되었을 가능성이 있으므로 보안 툴을 사용하거나 수동으로 바이러스를 검출하시기 바랍니다.
프로세스의 위치가 `C:\\Windows\\System32` 디렉터리에 있다면, 시스템을 재시작하거나 안전하지만 불필요한 시스템 프로세스를 종료하시기 바랍니다.
자주 보는 시스템 프로세스는 다음과 같습니다.
System Idle Process: 시스템 유휴 시간 프로세스로, CPU 유휴 시간 백분율을 나타냅니다
system: 메모리 관리 프로세스
explorer: 바탕 화면 및 파일 관리
iexplore: Microsoft 브라우저
csrss: Microsoft 클라이언트/서버 실행 시의 서브 시스템
svchost: 시스템 프로세스로, DLL 실행에 사용됩니다
Taskmgr: 작업 관리자
lsass: 로컬 보안 권한 서비스

대량의 CPU 혹은 메모리 리소스를 사용하는 프로세스가 비정상적인 프로세스일 경우

이름이 이상한 일부 프로세스가 대량의 CPU 혹은 메모리 리소스를 사용하고 있을 경우, xmr64.exe(채굴 바이러스) 등의 트로이 목마 바이러스 프로세스일 수 있습니다. 검색 엔진을 사용하여 해당 프로세스가 트로이 목마 바이러스 프로세스는 아닌지 확인하시기 바랍니다.
트로이 목마 바이러스 프로세스가 맞다면, 보안 툴을 사용하여 바이러스를 검출하고, 필요에 따라 데이터를 백업한 다음 시스템을 재설치하시기 바랍니다.
트로이 목마 바이러스 프로세스가 아니라면, 시스템을 재시작하거나 안전하고 불필요한 프로세스를 종료하시기 바랍니다.

대량의 CPU 혹은 메모리 리소스를 사용하는 프로세스가 비즈니스 프로세스일 경우

대량의 CPU 혹은 메모리 리소스를 사용하는 프로세스가 IIS, HTTPD, PHP, Java 등의 비즈니스 프로세스일 경우 한 단계 더 분석할 것을 권장합니다.
예: 현재 비즈니스 양이 많은지 진단합니다.
비즈니스의 양이 많다면, 서버 구성 업그레이드를 진행하시기 바랍니다. 서버 구성을 업그레이드하지 않으려면 비즈니스 프로세스에 최적화 공간이 있는지 확인하고 최적화하시기 바랍니다.
비즈니스의 양이 많지 않다면, 비즈니스 오류 리포트를 참고하여 잘못된 매개변수로 인해 리소스가 헛되이 소모되는 등의 문제가 생기지 않았는지 분석합니다.

대량의 CPU 혹은 메모리 리소스를 사용하는 프로세스가 Tencent Cloud 모듈 프로세스일 경우

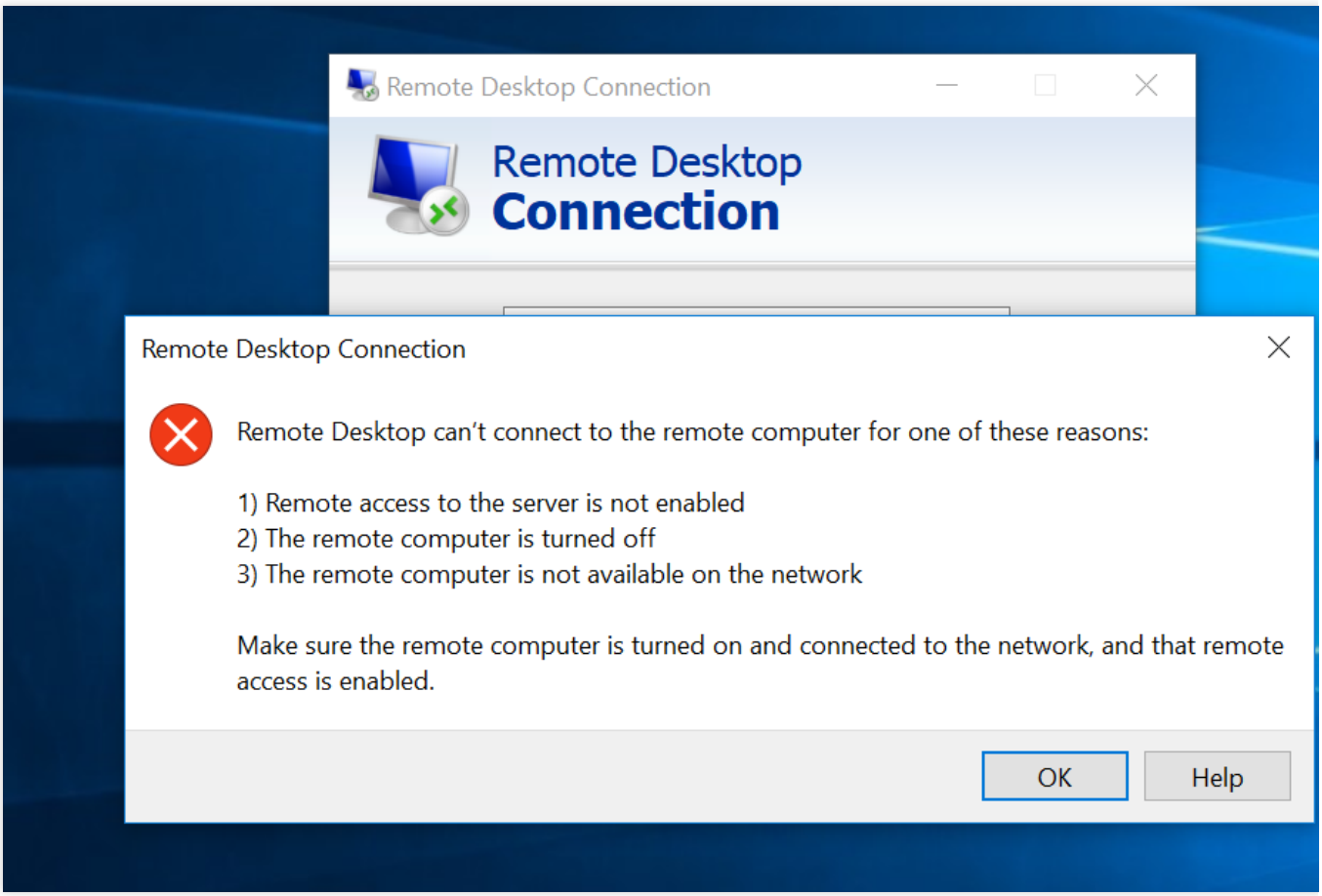
티켓 제출을 통해 당사에 문의하여 더 자세히 진단하시기 바랍니다.

Windows 인스턴스: 원격 데스크탑에서 원격 컴퓨터를 연결할 수 없을 경우

최종 업데이트 날짜: : 2024-02-02 11:09:47

현상 설명

Windows에서 Windows 인스턴스에 원격으로 연결하려고 하면 다음 이미지와 같은 메시지가 표시됩니다.



다음 이유 중 하나로 인해 원격 데스크톱을 사용하여 원격 컴퓨터에 연결할 수 없습니다.

1. 서버에 대한 원격 액세스가 활성화되어 있지 않습니다.
2. 원격 컴퓨터가 꺼져 있습니다.
3. 네트워크에서 원격 컴퓨터를 사용할 수 없습니다.

원격 컴퓨터가 켜져 있고 네트워크에 연결되어 있고 원격 액세스가 활성화되어 있는지 확인하십시오.

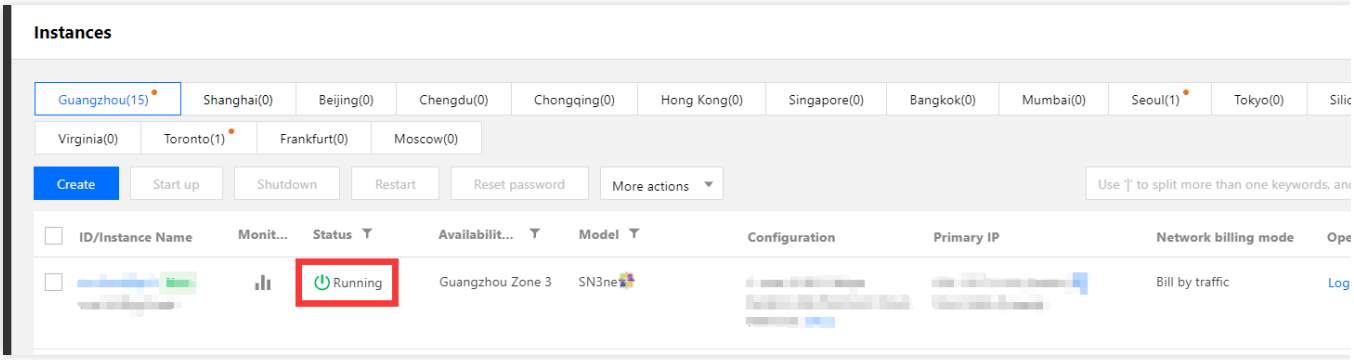
가능한 원인

이 문제의 가능한 원인에는 다음이 포함되지만 이에 국한되지는 않습니다. 실제 상황에 따라 문제를 해결하십시오.
인스턴스가 비정상 상태입니다.
CVM에 공용 IP 주소가 없거나 공중망 대역폭이 0입니다.
인스턴스와 바인딩된 보안 그룹에서 원격 로그인 포트(기본적으로 포트 3389)가 인터넷에 개방되어 있지 않습니다.
원격 데스크톱 서비스가 시작되지 않았습니다.
원격 데스크톱 설정이 올바르지 않습니다.
Windows 방화벽 설정이 올바르지 않습니다.

문제 해결 단계

인스턴스가 실행 중인지 확인

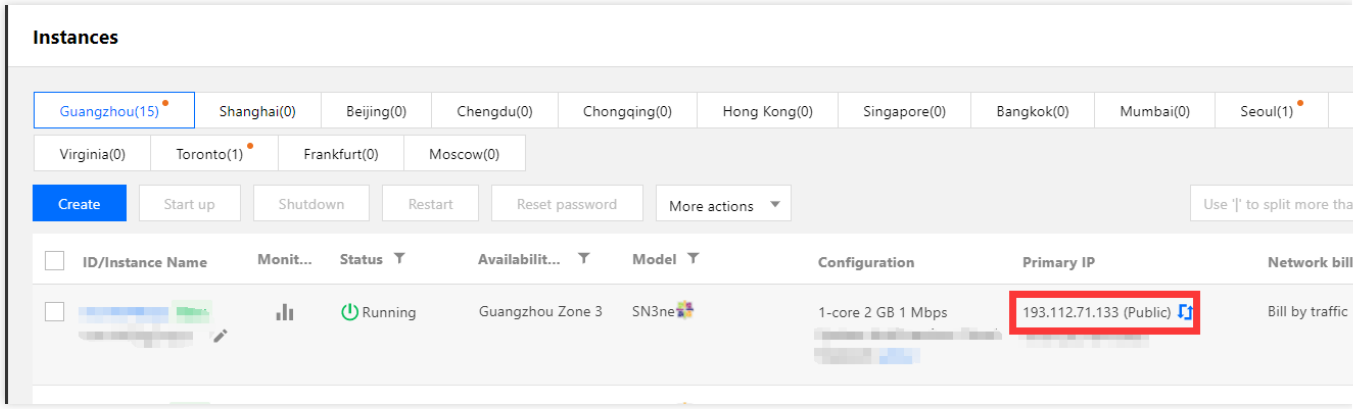
1. CVM 콘솔에 로그인합니다.
2. 인스턴스 관리 페이지에서 다음 이미지와 같이 인스턴스가 '실행 중'인지 확인합니다.



Yes, CVM에 공용 IP 주소가 있는지 확인하십시오.
No, Windows 인스턴스를 시작합니다.

CVM에 공용 IP 주소가 있는지 확인

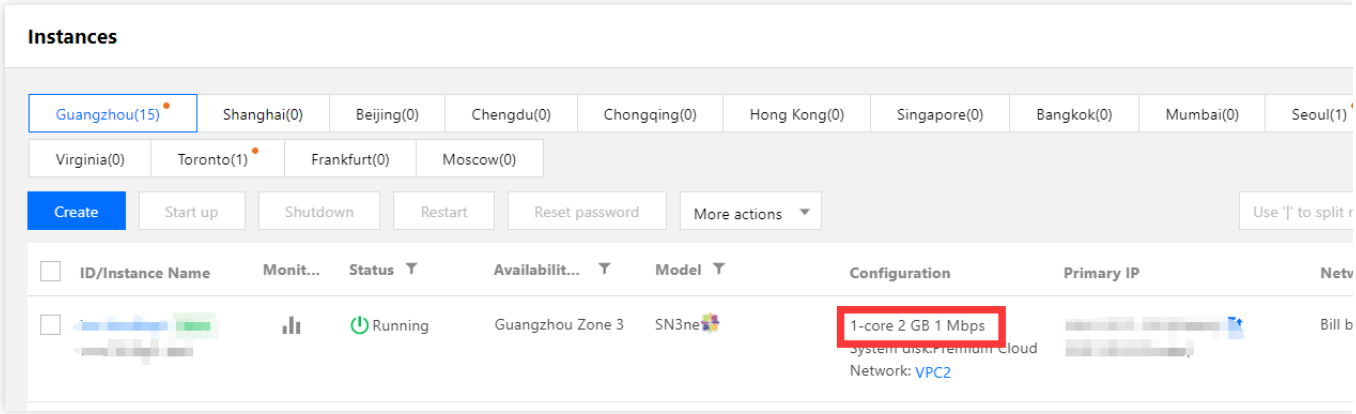
다음 이미지와 같이 CVM 콘솔에서 CVM에 공용 IP 주소가 있는지 확인합니다.



Yes, 공중망 대역폭을 구입했는지 확인하십시오.
No, EIP 신청 및 바인딩합니다.

공중망 대역폭 구입 여부 확인

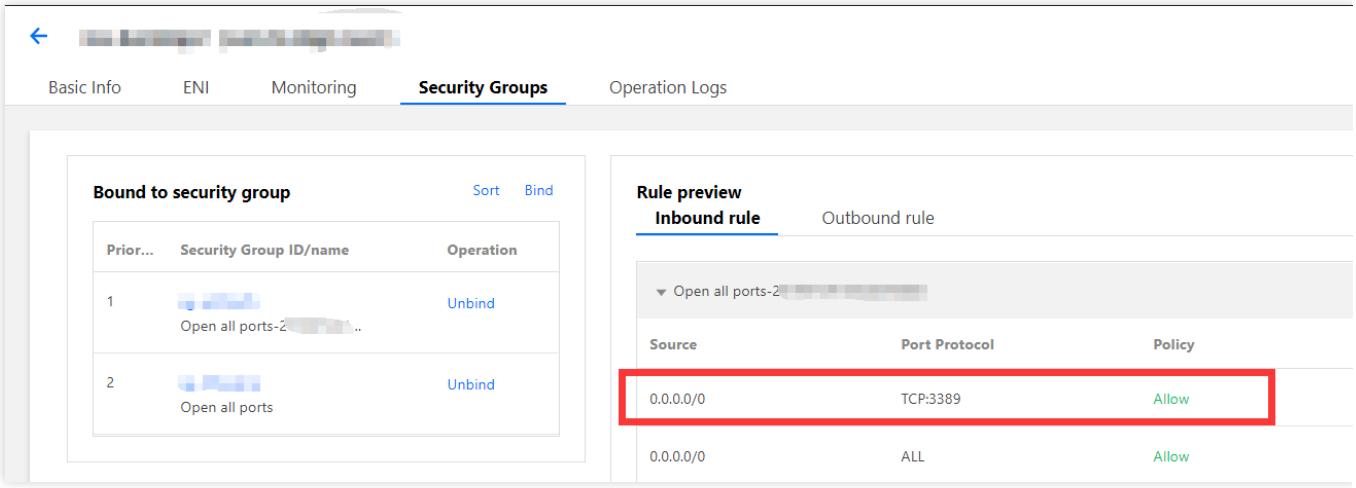
공중망 대역폭이 0Mbps인지 확인합니다. 최소 1Mbps의 공중망 대역폭을 확보해야 합니다.
Yes, 네트워크 구성 변경을 참고하여 대역폭을 5Mbps 이상으로 늘리십시오.



No, 인스턴스의 원격 로그인 포트(3389)가 인터넷에 개방되었는지 확인합니다.

인스턴스의 원격 로그인 포트(3389)가 인터넷에 개방되었는지 확인

1. CVM 콘솔의 인스턴스 관리 페이지에서 로그인할 인스턴스의 ID 또는 이름을 클릭하여 인스턴스 세부 정보 페이지로 이동합니다.
2. **보안 그룹** 탭 페이지에서 다음 이미지와 같이 인스턴스와 바인딩된 보안 그룹의 인터넷에 원격 로그인 포트(기본적으로 포트 3389)가 개방되어 있는지 확인합니다.



Yes, 원격 데스크톱 서비스를 확인하십시오.

No, 해당 보안 그룹 규칙을 편집하여 인터넷에 포트를 개방합니다. 보안 그룹 규칙 추가를 참고하십시오.

원격 데스크톱 서비스 확인

1. VNC를 사용하여 Windows 인스턴스에 로그인하고 Windows 인스턴스용 원격 데스크톱 서비스가 활성화되어 있는지 확인합니다.

설명：

다음 작업은 Windows Server 2016을 예로 들어 설명합니다.

2.

를 우클릭하고 팝업 메뉴에서 **시스템**을 선택합니다.

3. '시스템' 팝업 창에서 **고급 시스템 설정**을 선택합니다.

4. '시스템 속성' 팝업 창에서 **원격** 탭을 선택하고 '이 컴퓨터에 대한 원격 연결 허용'이 선택되었는지 확인합니다.

Yes, 5단계를 실행합니다.

No, 선택하고 **확인**을 클릭합니다.

5.

을(를) 우클릭하고 팝업 메뉴에서 **컴퓨터 관리**를 선택합니다.

6. '컴퓨터 관리' 창의 왼쪽 사이드바에서 **서비스 및 애플리케이션 > 서비스**를 선택합니다.

7. 오른쪽의 서비스 목록에서 **Remote Desktop Services**가 시작되었는지 확인합니다.

Yes, 8단계를 실행합니다.

No, 서비스를 시작합니다.

8.


를 우클릭하고 팝업 메뉴에서 **실행**을 선택합니다.

9. '실행' 팝업 창에서 **msconfig**를 입력하고 **확인**을 클릭합니다.

10. '시스템 구성' 팝업 창에서 **정상 시작**이 선택되어 있는지 확인합니다.

Yes, Windows 인스턴스의 시스템 설정 확인하십시오.

No, 선택하고 **확인**을 클릭합니다.

Windows 인스턴스의 시스템 설정 확인

1. VNC를 사용하여 Windows 인스턴스에 로그인하고 인스턴스의 시스템 설정을 확인합니다.

설명：

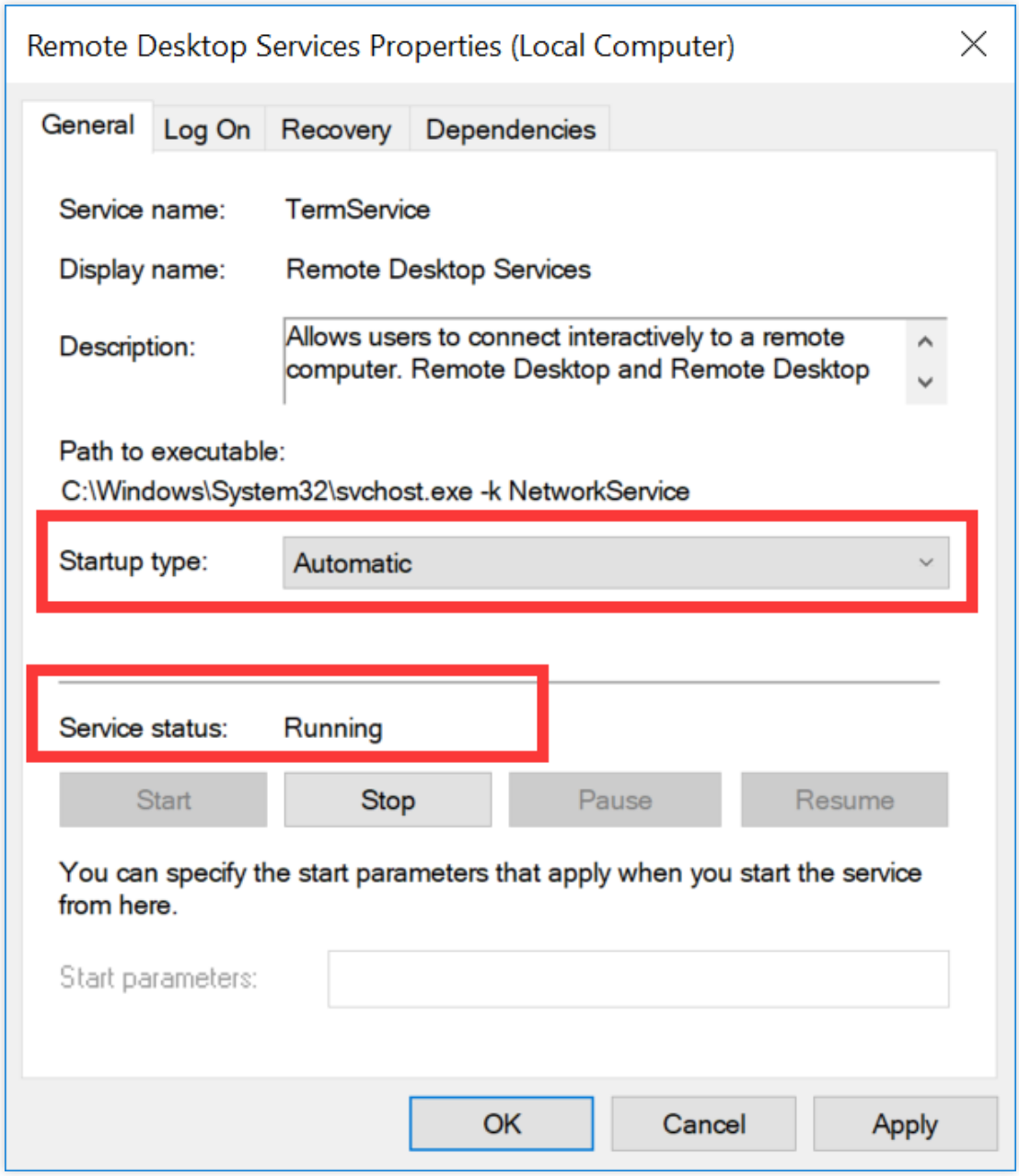
다음 작업에서는 Windows Server 2012의 인스턴스를 예로 사용합니다.

2.


을(를) 우클릭하고 팝업 메뉴에서 **실행**을 선택합니다.

3. '실행' 팝업 창에서 **services.msc**를 입력하고 **Enter**를 눌러 '서비스' 창을 엽니다.

4. 'Remote Desktop Services'를 더블 클릭하여 열고 원격 데스크톱 서비스가 아래와 같이 실행되고 있는지 확인합니다.



Yes, 5단계를 실행합니다.

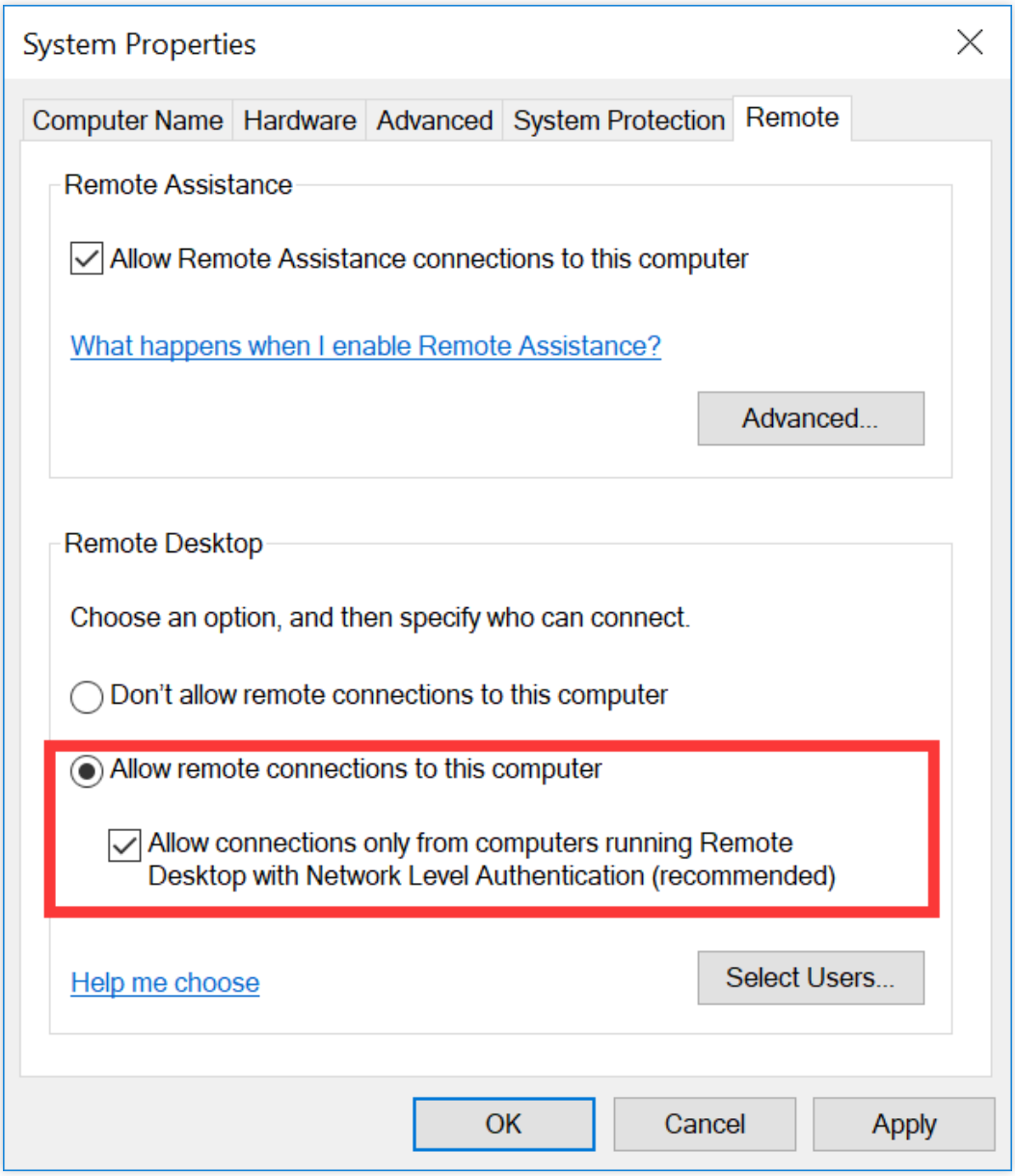
No, '시작 유형'을 '자동'으로, '서비스 상태'를 '실행 중'으로 설정합니다(즉, **시작** 클릭).

5.

을(를) 우클릭하고 팝업 메뉴에서 **실행**을 선택합니다.

6. '실행' 팝업 창에서 **sysdm.cpl**을 입력하고 **Enter** 키를 눌러 '시스템 속성' 창을 엽니다.

7. '원격' 탭에서 아래와 같이 원격 데스크톱이 '이 컴퓨터에 대한 원격 연결 허용(L)'으로 설정되어 있는지 확인합니다.



Yes, 8단계를 실행합니다.

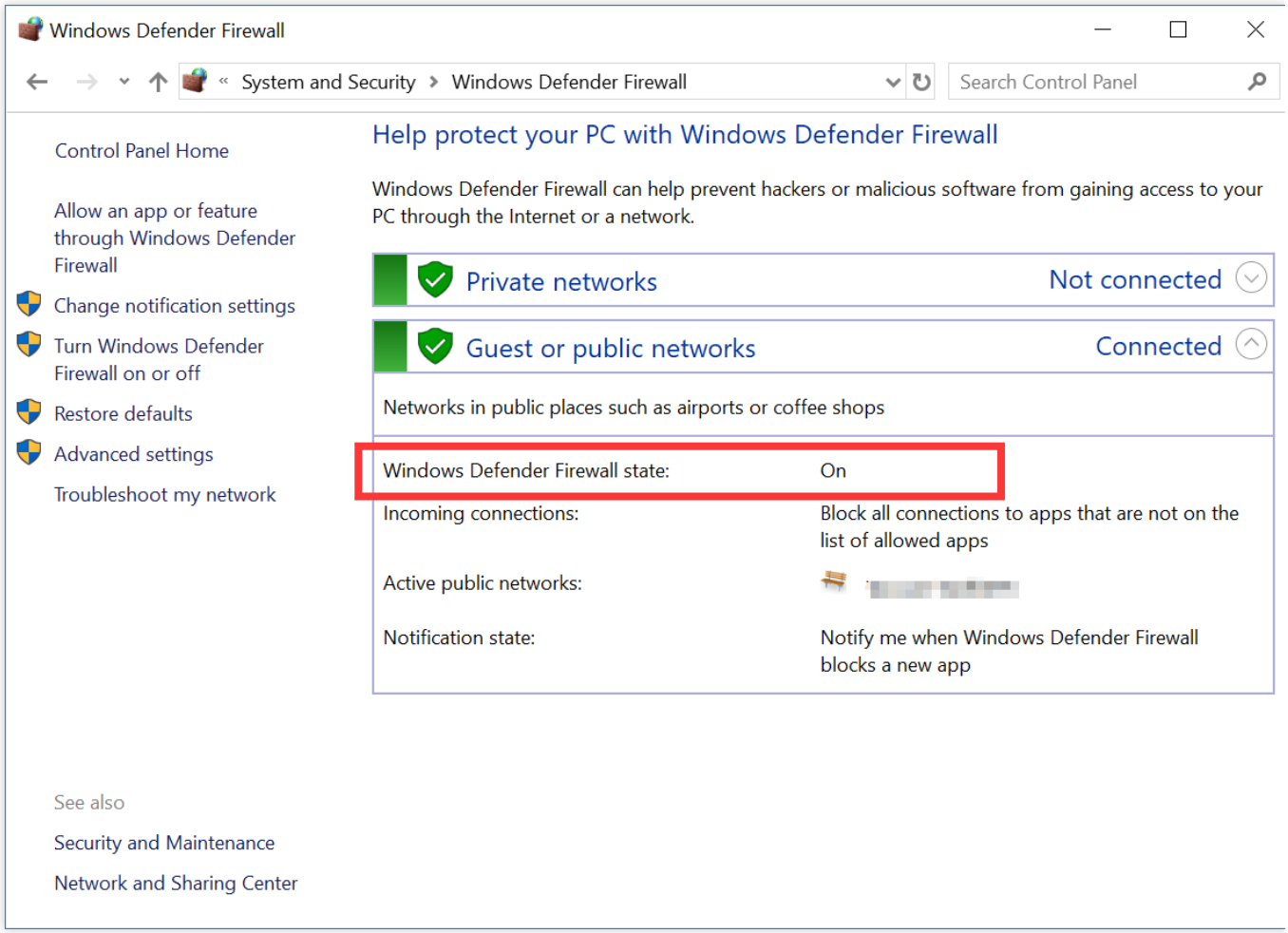
No, 원격 데스크톱을 '이 컴퓨터에 대한 원격 연결 허용(L)'으로 설정합니다.

8.

을 클릭하고 팝업 메뉴에서 **제어판**을 선택합니다.

9. '제어판'에서 **시스템 및 보안** > **Windows Defender 방화벽**을 선택하여 'Windows Defender 방화벽'을 엽니다.

10. "Windows Defender 방화벽"에서 아래와 같이 Windows Defender 방화벽의 상태를 확인합니다.

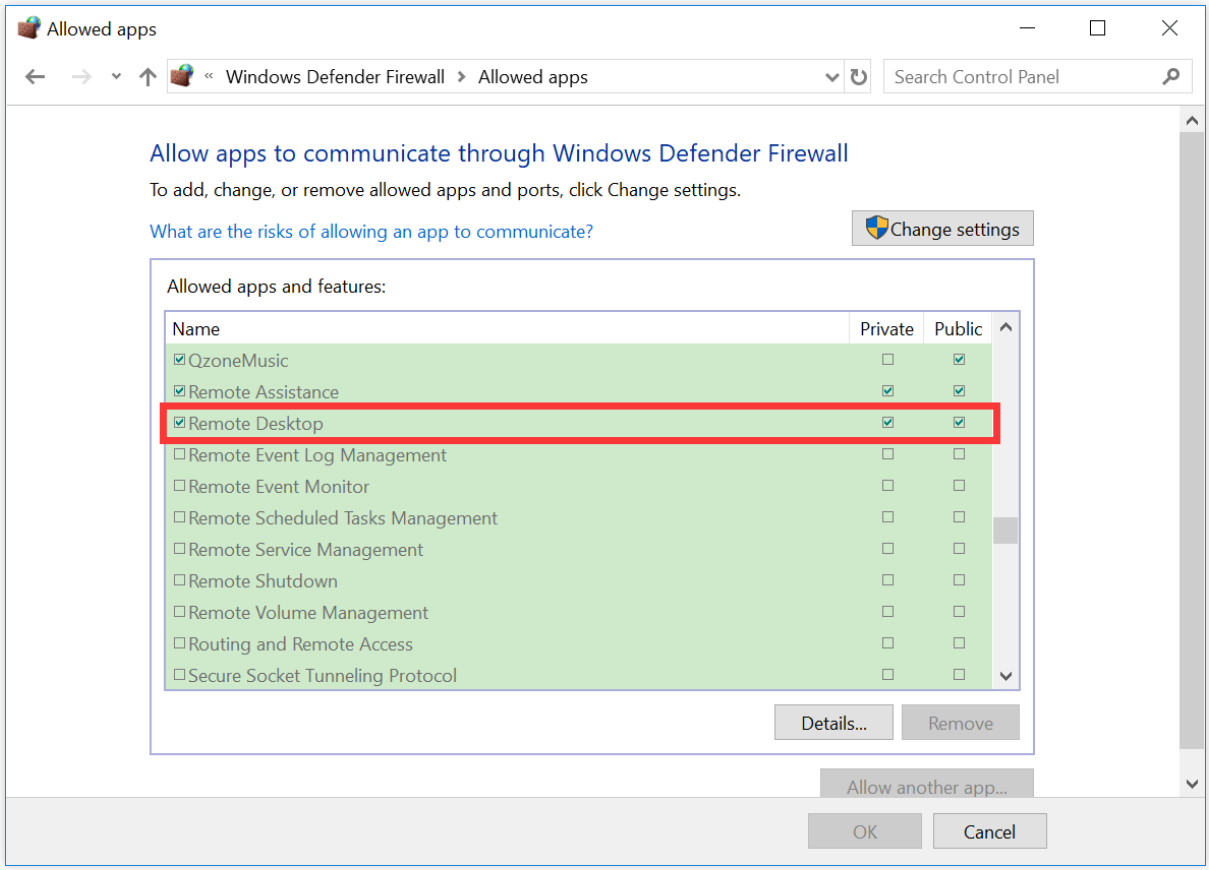


상태가 'On'인 경우 11단계로 진행합니다.

상태가 'Off'인 경우 온라인 지원을 통해 문의해주시기 바랍니다.

11. 'Windows Defender 방화벽'에서 **Windows 방화벽을 통해 앱 또는 기능 허용**을 클릭하여 '허용된 앱' 창을 엽니다.

12. '허용된 앱' 창에서 아래와 같이 '허용된 앱 및 기능'에서 '원격 데스크톱'이 선택되어 있는지 확인합니다.

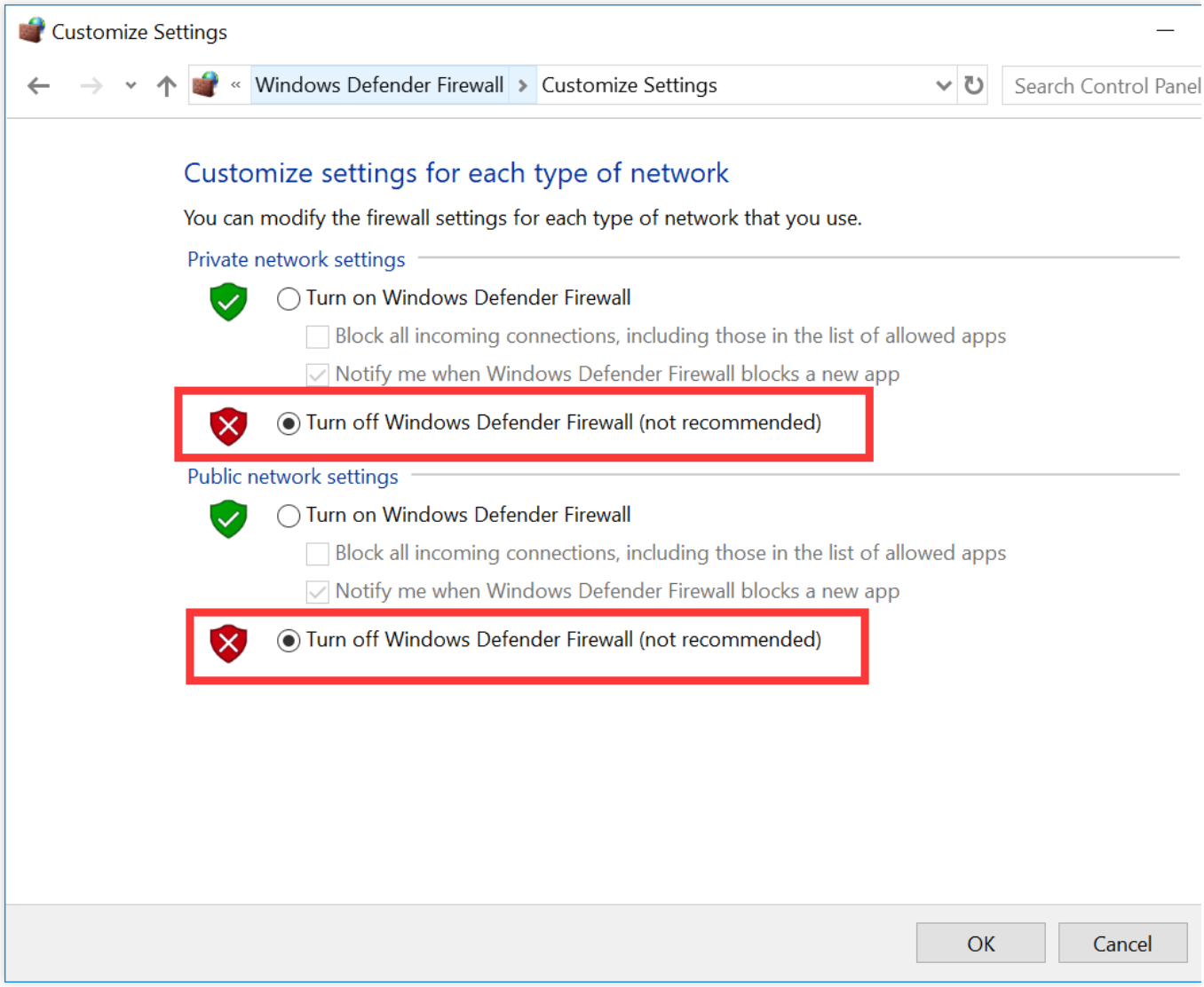


Yes, 13단계를 실행합니다.

No, '원격 데스크톱'을 선택하여 Windows Defender 방화벽을 통한 '원격 데스크톱'을 허용합니다.

13. 'Windows Defender 방화벽'에서 **Windows 방화벽 켜기 또는 끄기**를 선택하여 '설정 사용자 지정' 창을 엽니다.

14. '설정 사용자 지정' 창에서 아래와 같이 '사설망 설정' 및 '공중망 설정'을 'Windows Defender 방화벽 끄기(권장하지 않음)'로 설정합니다.



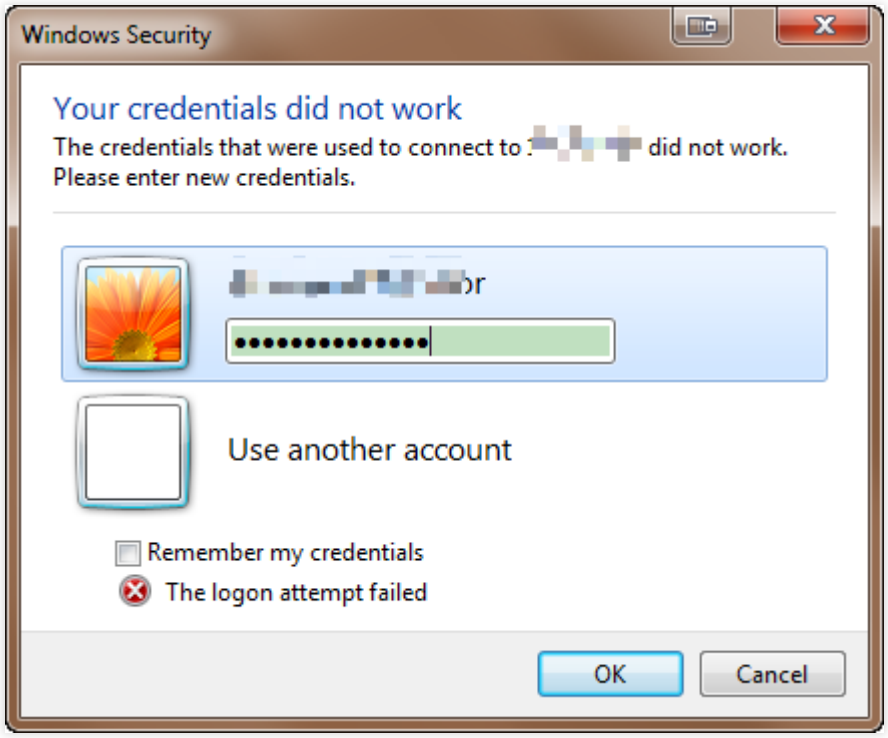
여전히 원격 데스크톱에서 Windows 인스턴스에 연결할 수 없으면 온라인 지원을 통해 문의해주시기 바랍니다.

Windows 인스턴스: 자격 증명이 작동하지 않았습니다.

최종 업데이트 날짜: : 2024-02-02 11:09:47

문제 설명

Windows 운영 체제의 로컬 컴퓨터가 RDP 프로토콜(MSTSC 등)를 통해 원격 데스크톱 접속으로 Windows CVM에 로그인 시, 다음의 에러가 표시됩니다.
자격 증명은 작동할 수 없습니다, `xxx.xxx.xxx.xxx` 접속에 사용된 자격 증명은 작동하지 않았습니다. 새 자격 증명을 입력하세요.



처리 순서

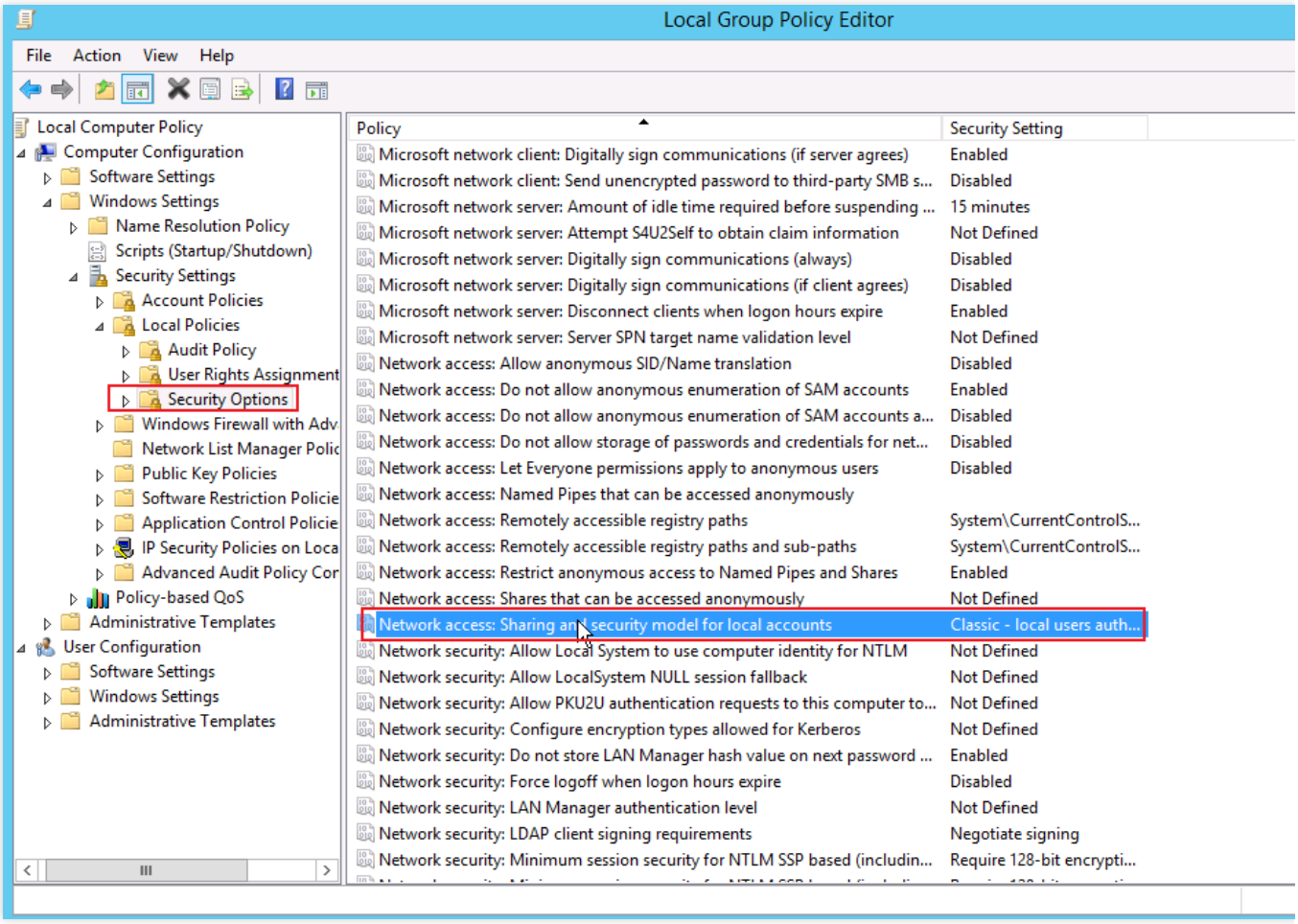
설명 :
Windows Server 2012 운영 체제의 Tencent Cloud CVM를 예로 들면, 운영 체제의 버전이 다르기 때문에, 자세한 조작 절차는 조금 다릅니다.
다음 절차에 따라 문제를 진단하세요, 각 절차를 다 실행한 후, Windows CVM에 재연결해 문제가 해결되었는지 확인합니다. 문제가 해결되지 않은 경우는 다음 절차에 따라 진행하세요.

절차1：네트워크 접근 정책 변경

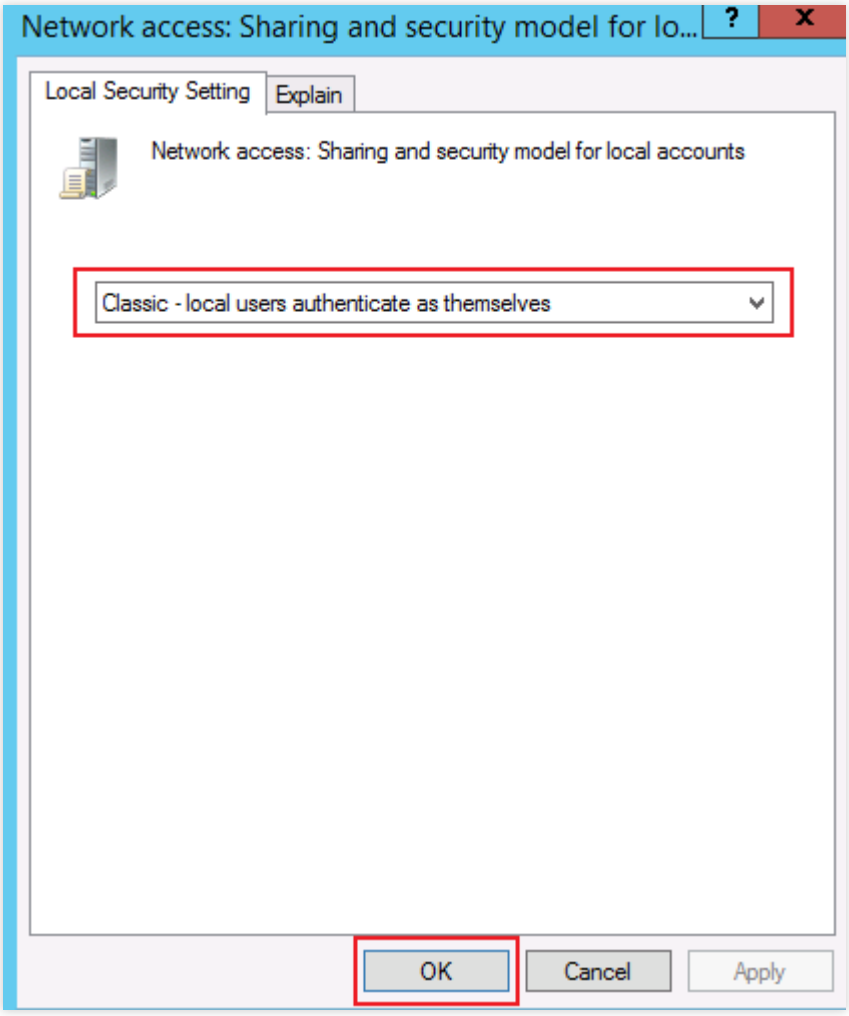
1. VNC를 사용하여 Windows 인스턴스에 로그인합니다.
2. 운영 체제 인터페이스에서

클릭 후,“Windows PowerShell”창을 여십시오.

3. “Windows PowerShell”창에서 **gpedit.msc**를 입력한 후 **Enter**를 눌러 "로컬 그룹 정책 편집기"를 여십시오.
4. 왼쪽 메뉴에서 【컴퓨터 구성】>【Windows 설정】>【보안 설정】>【로컬 정책】>【보안 옵션】 디렉터리를 차례로 클릭해서 여십시오.
5. 【보안 옵션】의 【네트워크 액세스: 로컬 계정의 공유와 보안 모델】을 찾아서 여십시오. 아래 그림과 같습니다.



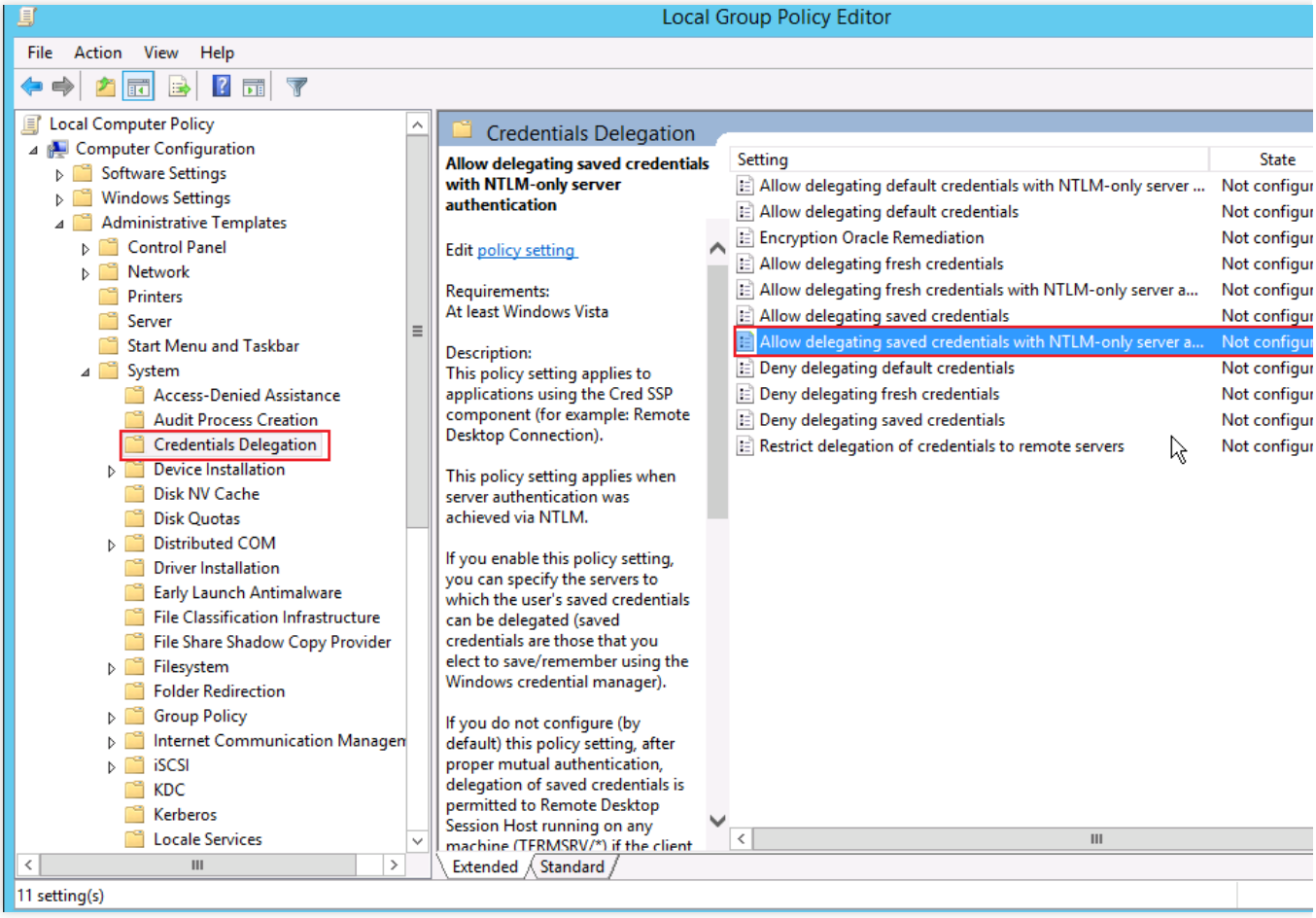
6. 【클래식 - 로컬 사용자 인증 시 원래 신분을 바꾸지 않음】을 선택한 후 【확인】을 클릭하세요. 아래 그림과 같습니다.



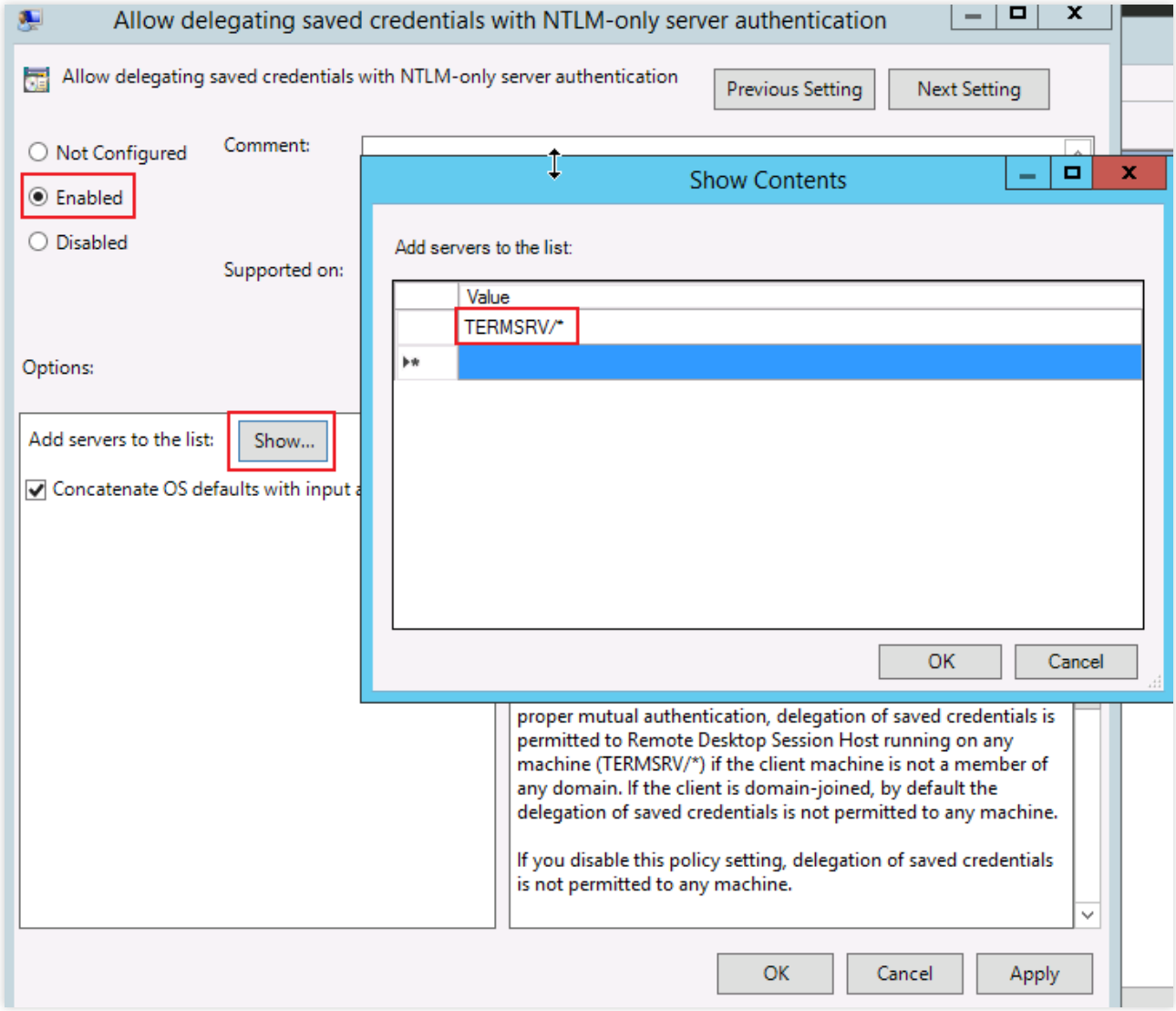
7. Windows CVM에 재연결하여 연결에 성공했는지 확인하세요.
네, 작업이 종료됐습니다.
아니요, 절차2 (자격 증명 위임 변경)을 실행하세요.

절차2 : 자격 증명 위임 변경

1. “로컬 그룹 정책 편집기”의 왼쪽 메뉴에서, 【컴퓨터 구성】 > 【관리 템플릿】 > 【시스템】 > 【자격 증명 위임】 디렉터리를 차례로 클릭해서 여십시오.
2. 【자격 증명 위임】의 【NTLM 서버만의 인증으로 저장된 자격 증명 위임을 허가하기】를 찾아서 여십시오. 아래 그림과 같습니다.

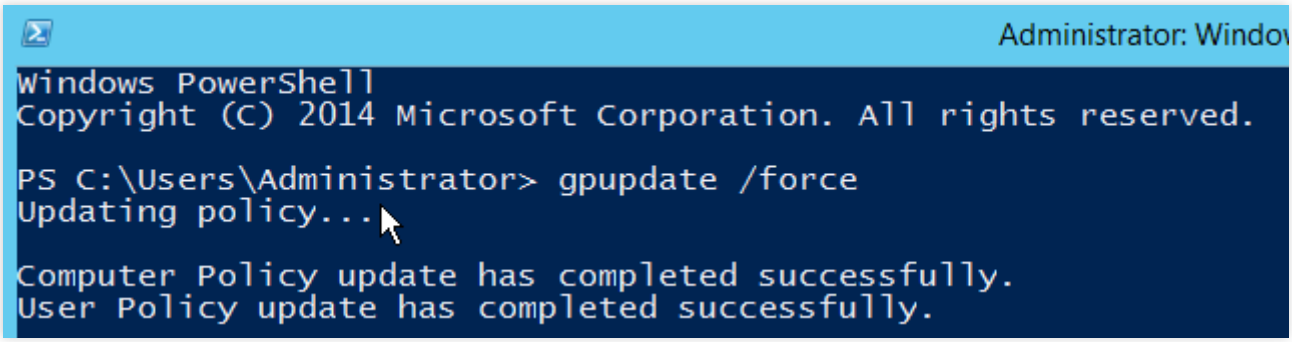


3. 열린 창에서 【활성화됨】을 선택하고 "옵션" 의 【표시】에 `TERMSRV/*` 를 입력하고 【확인】을 클릭하세요. 아래 그림과 같습니다.



4. 【확인】을 클릭하세요.
5. 운영 체제 인터페이스에서

클릭 후,“Windows PowerShell”창을 여십시오.
6. “Windows PowerShell”창에서 **gpupdate /force**를 입력하고 **Enter**키를 눌러 그룹 정책을 새로 고칩니다. 아래 그림과 같습니다.



7. Windows CVM에 재연결하여 연결에 성공했는지 확인하세요.

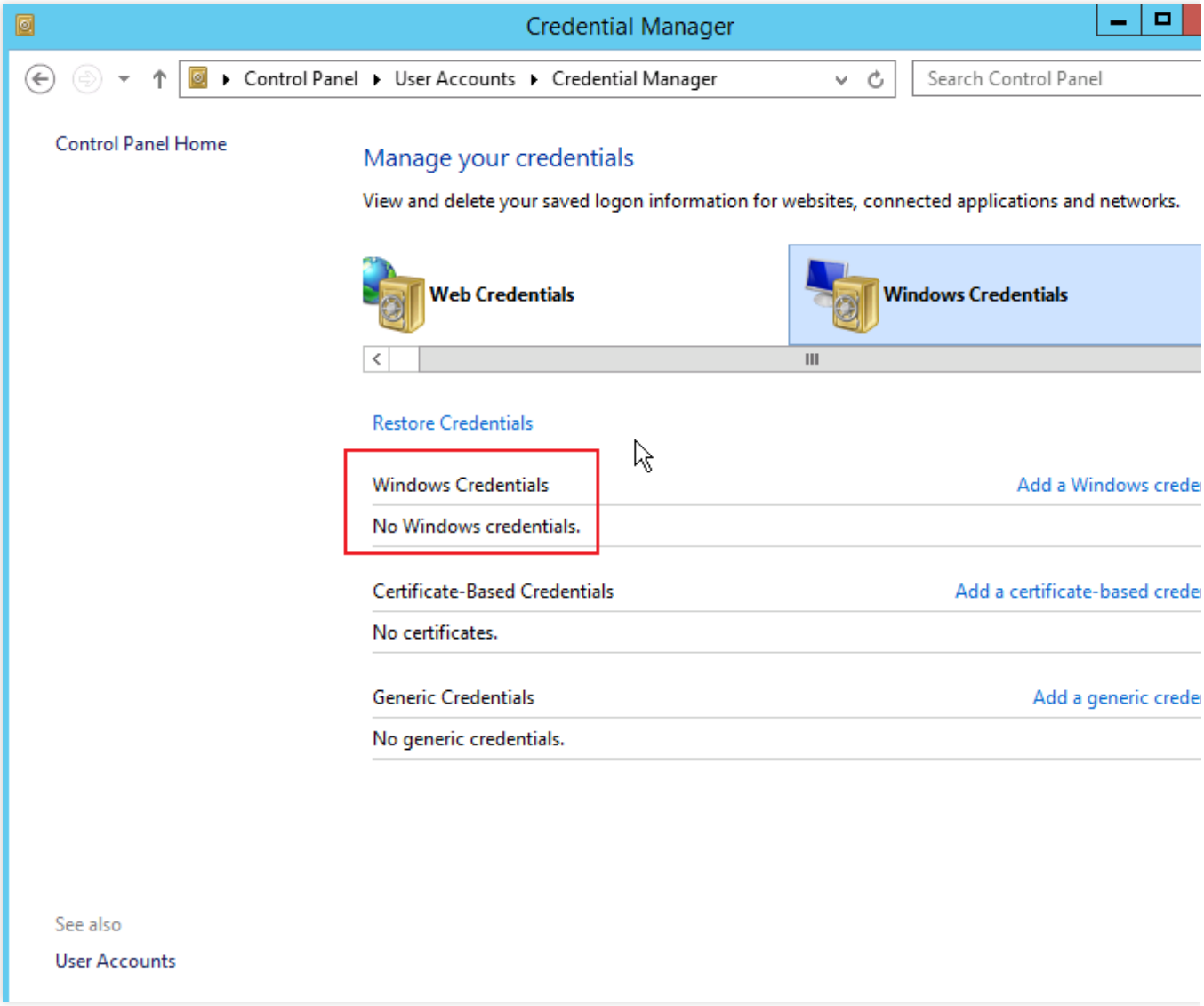
-네, 작업 종료됐습니다.

-아니요, 절차3 (로컬 CVM의 자격 증명 설정)을 실행하세요.

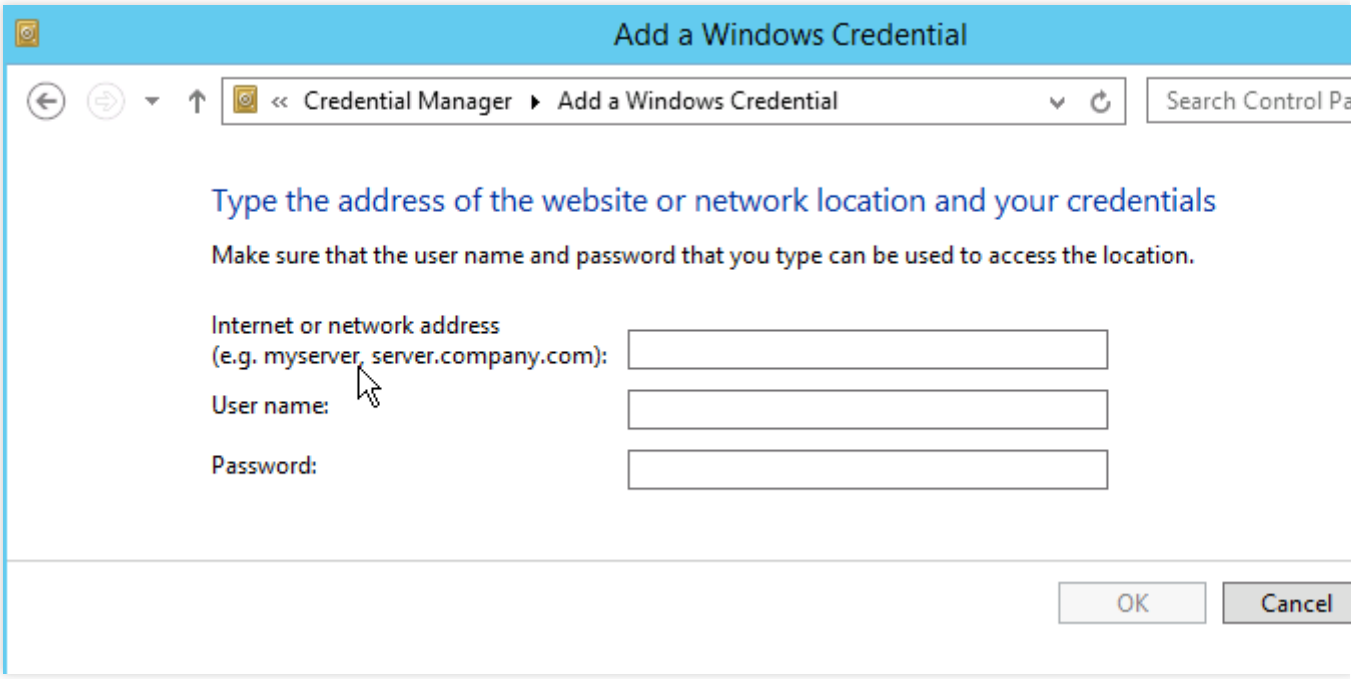
절차3 : 로컬 CVM의 자격 증명 설정

1. 운영 체제 인터페이스에서,

> 【제어판】> 【사용자 계정】을 클릭해, 【자격 증명 관리자】의 【Windows 자격 증명 관리】를 선택하여, Windows 자격 증명 인터페이스에 들어갑니다. 아래 그림과 같습니다.



2. Windows 자격 증명 아래에 현재 로그인하고 있는 CVM의 자격 증명가 있는지 확인하세요.
없으면 다음 단계로 넘어가서 Windows 자격 증명을 추가하세요.
있으면 절차4 (CVM 비밀번호 보호 공유 비활성화)를 실행하세요.
3. 【Windows 자격 증명 추가】를 클릭하고, Windows 자격 증명 추가 인터페이스에 들어갑니다. 아래 그림과 같습니다.



4. 현재 로그인하고 있는 CVM의 IP 주소, 사용자 이름과 비밀번호를 입력하고, 【확인】을 클릭하세요.

설명：

CVM의 IP 주소는 CVM 공인 IP 주소입니다. 상세한 내용은 공인 IP 주소 취득을 참조 바랍니다.

Windows 인스턴스의 기본 사용자 이름은 `Administrator` 이며 비밀번호는 인스턴스 생성 시 설정됩니다. 로그인 비밀번호를 잊어버린 경우 인스턴스 비밀번호 재설정을 참조 바랍니다.

5. Windows CVM에 재연결하여 연결에 성공했는지 확인하세요.

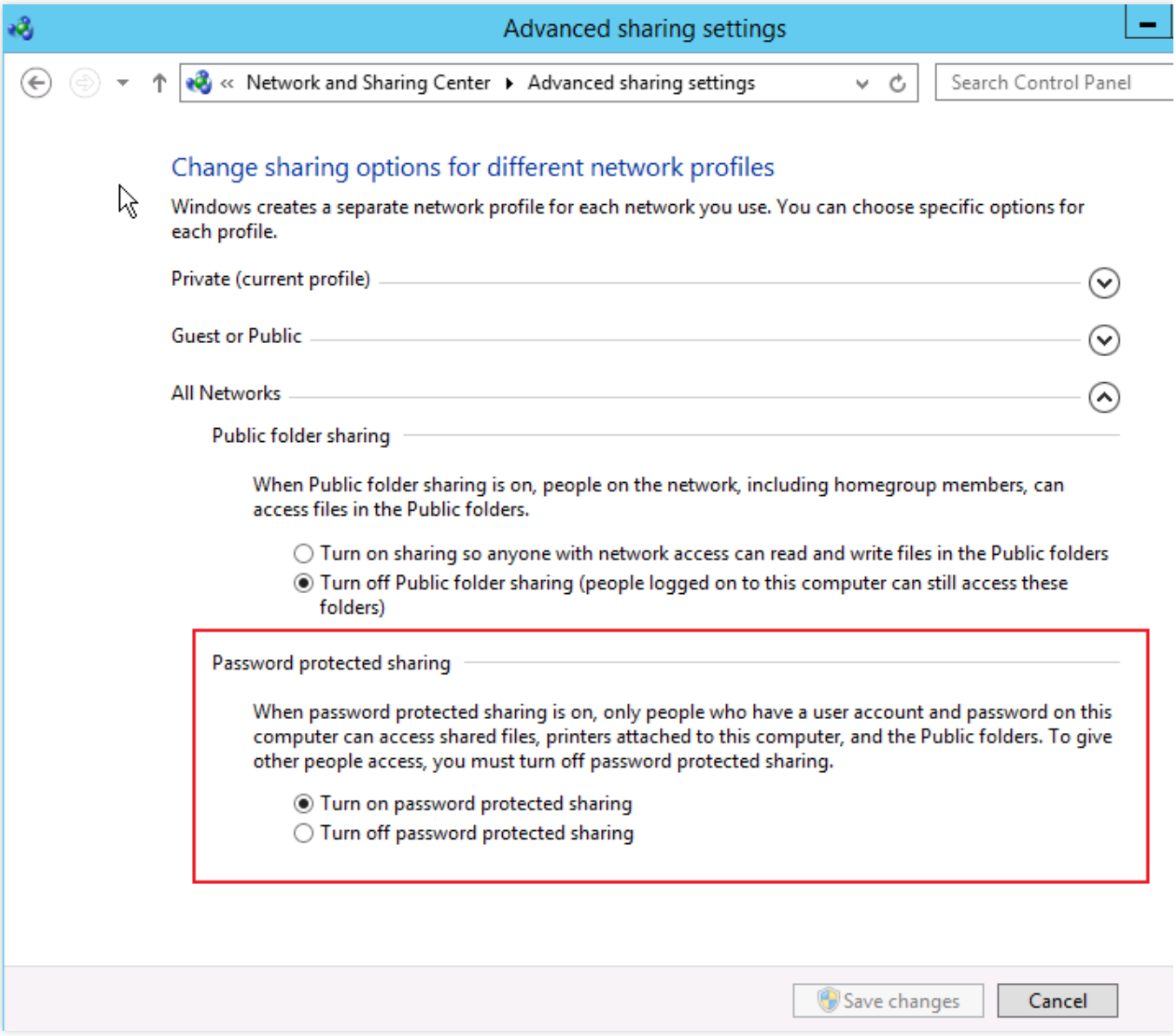
네, 작업 종료됐습니다.

아니요, 절차4 (CVM 비밀번호 보호 공유 비활성화)를 실행하세요.

절차4：CVM 비밀번호 보호 공유 비활성화

1. 운영 체제 인터페이스에서

> 【제어판】> 【네트워크 및 인터넷】> 【네트워크 및 공유 센터】> 【고급 공유 설정 변경】을 클릭하고 고급 공유 설정 변경 인터페이스에 들어갑니다. 아래 그림과 같습니다.



2.【모든 네트워크】탭을 펼치고, 【비밀번호 보호 공유】에서 【비밀번호 보호 공유 비활성화】를 선택하고, 【변경 저장】을 클릭하세요.

2. Windows CVM에 재연결하여 연결에 성공했는지 확인하세요.

네, 작업 종료됐습니다.

아니요, 티켓 제출하고 피드백을 요청하십시오.

Windows 인스턴스: 포트 문제로 원격 로그인을 할 수 없을 경우

최종 업데이트 날짜: : 2024-02-02 11:09:48

본 문서는 CVM이 포트 문제로 인해 원격 로그인할 수 없는 경우의 문제 해결 및 솔루션에 대해 소개합니다.
설명：
다음 작업은 Windows Server 2012 시스템의 CVM을 예로 듭니다.

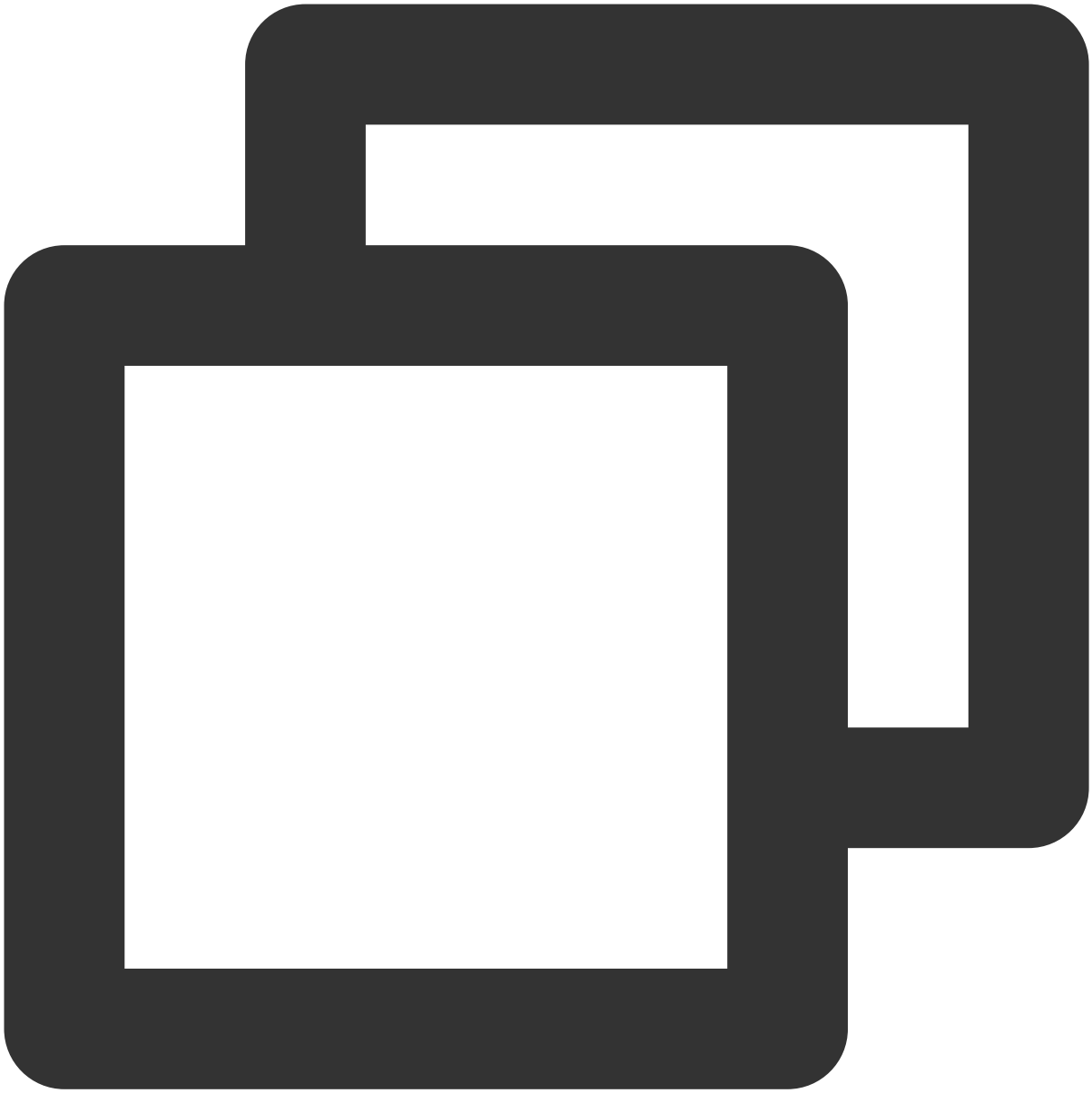
점검 툴

Tencent Cloud가 제공하는 아래의 툴을 통해 로그인할 수 없는 이유가 포트 및 보안 그룹 설정과 연관되어 있는지 판단할 수 있습니다.
자가 진단
보안 그룹(포트) 진단 툴
점검 결과 보안 그룹의 설정 문제로 진단할 경우, 보안 그룹(포트) 진단 툴 의 [원클릭 오픈] 기능을 통해 관련 포트를 오픈하고 로그인을 다시 시도할 수 있습니다. 포트 오픈 후에도 로그인에 실패할 경우 아래 내용을 참조하여 단계적으로 원인을 조사할 수 있습니다.

문제 해결

네트워크 연결성 점검

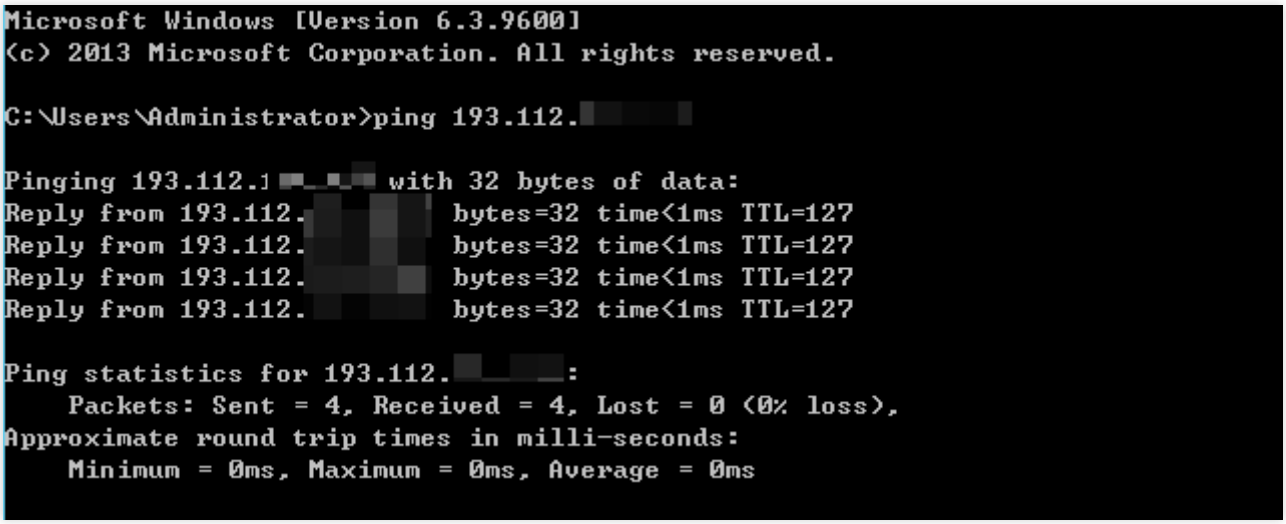
로컬 Ping 명령어를 통해 네트워크의 연결성을 테스트할 수 있습니다. 이와 동시에 서로 다른 네트워크 환경(다른 IP 대역 또는 다른 통신사)의 컴퓨터로 테스트하여 로컬 네트워크 문제인지 서버 문제인지 판단합니다.
1. 로컬 컴퓨터의 각 운영 체제에 따라 명령 툴의 여는 방식을 선택합니다.
Windows 시스템: [시작]>[운행]을 클릭하고 **cmd**을 입력하면 명령 창이 팝업됩니다.
Mac OS 시스템: Terminal 툴을 엽니다.
2. 다음 명령어를 실행하여 네트워크 연결을 테스트합니다.



```
ping + CVM 인스턴스 공인 IP 주소
```

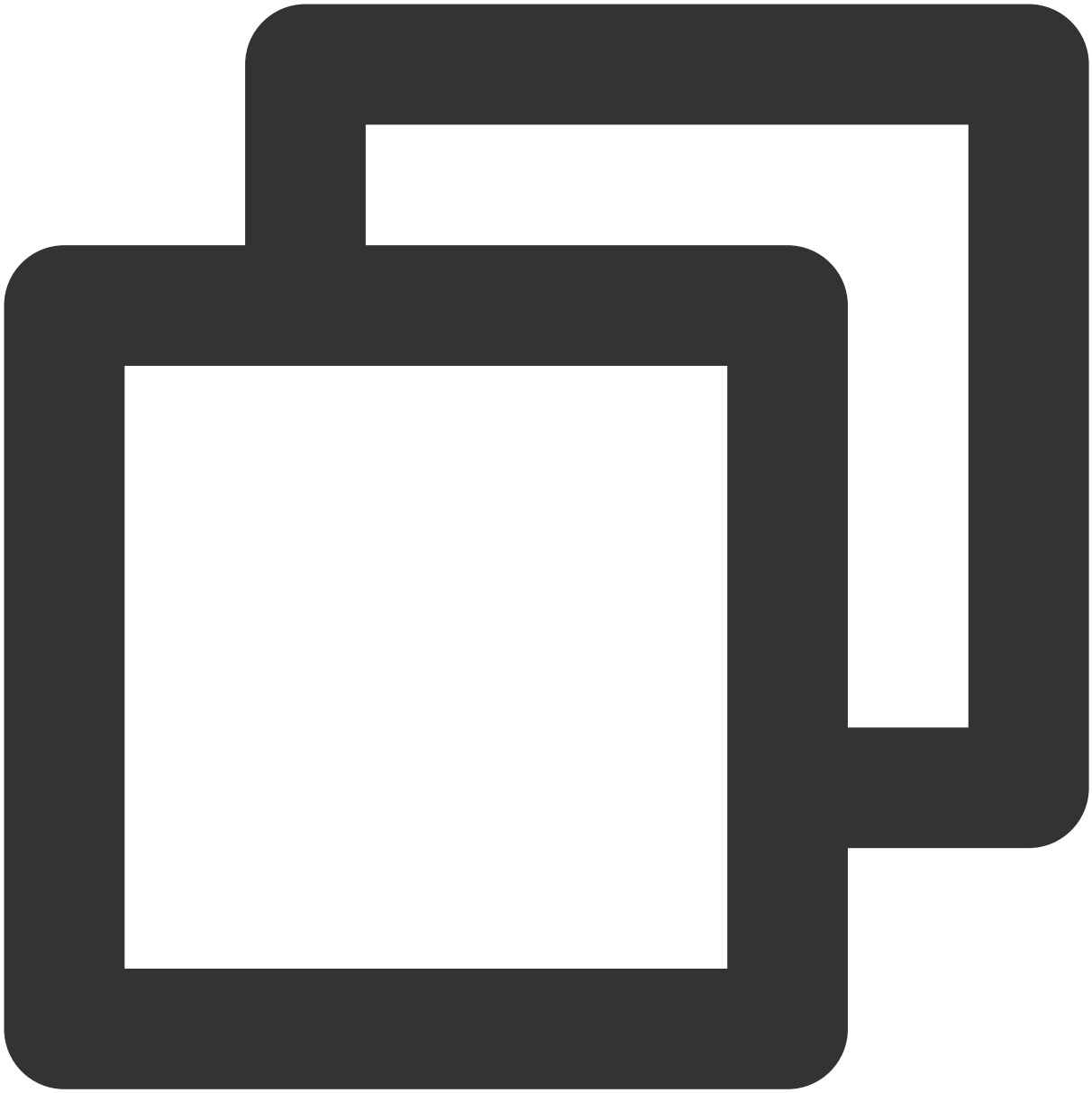
예시, `ping 139.199.XXX.XXX` 명령어를 실행합니다.

네트워크가 정상이면 아래와 같은 결과를 출력합니다. 원격 데스크톱 서비스 설정을 점검하세요.



네트워크가 비정상이면 [요청 시간 초과] 알림이 표시됩니다. 인스턴스 IP 주소 Ping block을 참조하여 문제를 해결하세요.

3. 다음 명령어를 실행하고 **Enter**를 눌러 원격 포트의 오픈 상황을 테스트하여, 포트 액세스 가능 여부를 판단합니다.

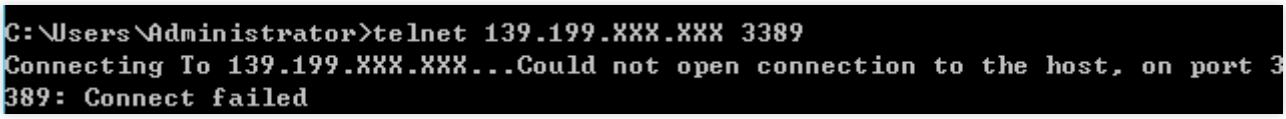


```
telnet + CVM 인스턴스 공인 IP 주소 + 포트 번호
```

예시, `telnet 139.199.XXX.XXX 3389` 명령어를 실행합니다. 아래 이미지 참조

정상 상황: 블랙 스크린에 커서만 나타납니다. 원격 포트(3389) 액세스 가능함을 뜻하므로 인스턴스 원격 데스크톱 서비스 오픈 여부를 점검하세요.

비정상 상황: 연결 실패, 네트워크에 문제 발생했음을 뜻하므로 문제 네트워크의 관련 부분을 점검하세요. 아래 이미지 참조



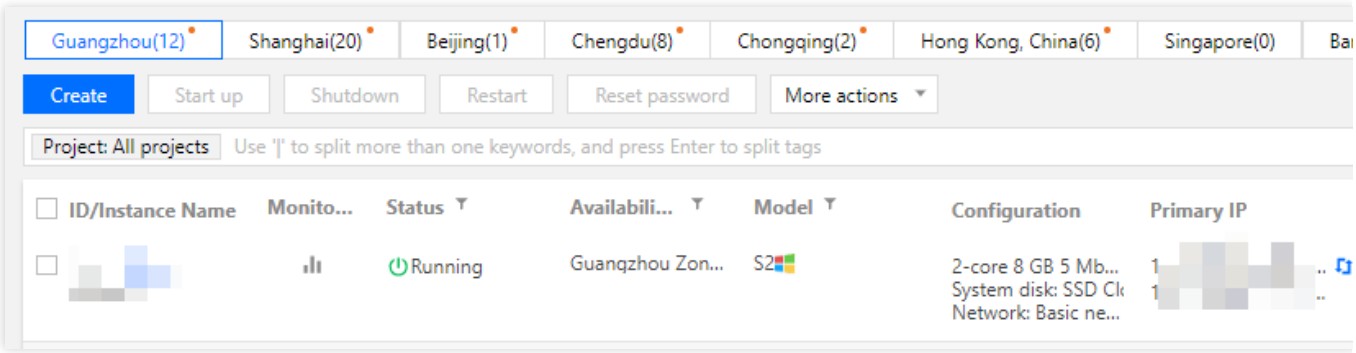
원격 데스크톱 서비스 설정 점검

VNC 방식으로 CVM에 로그인

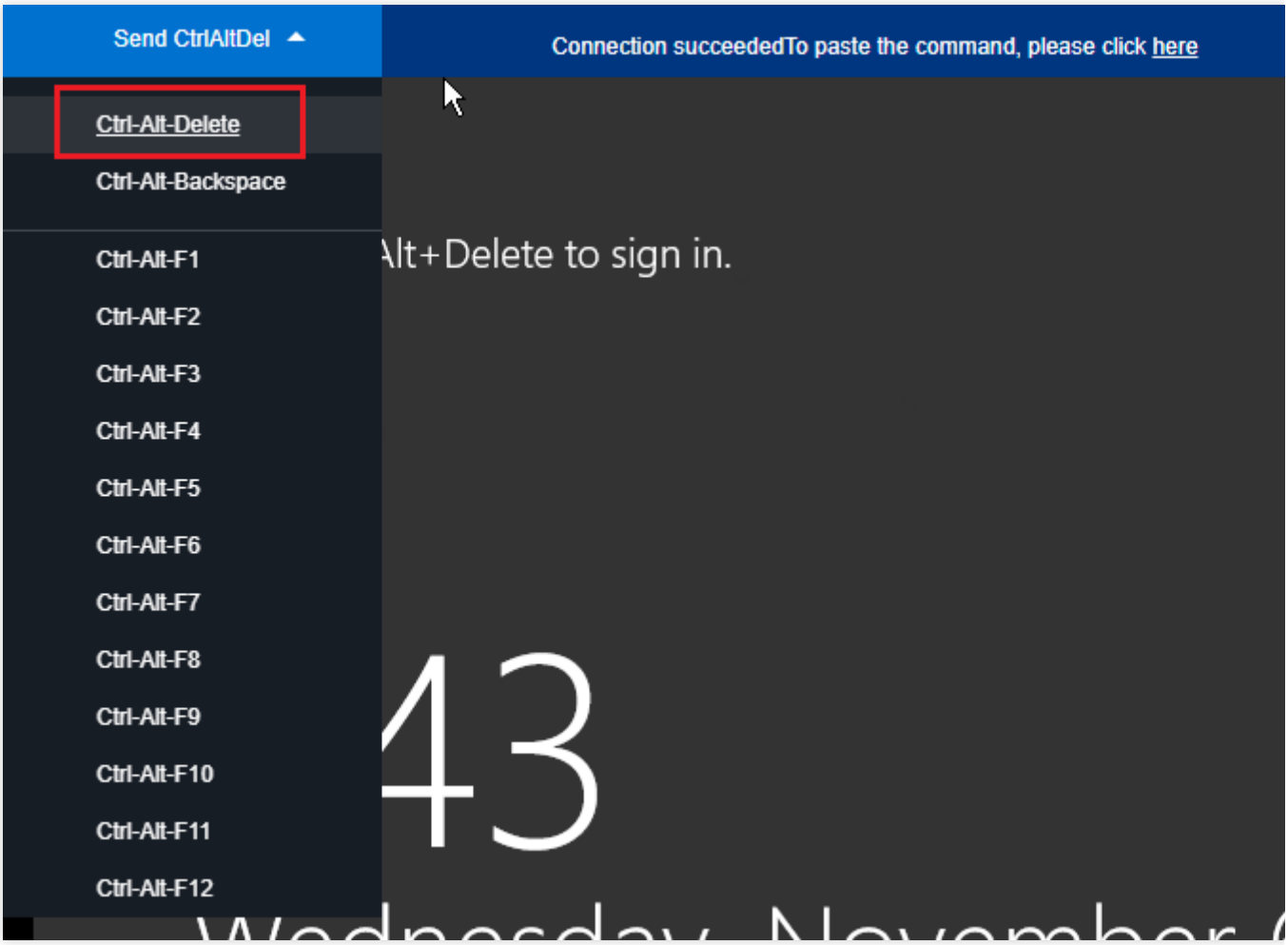
설명：

VNC 방식은 사용자가 표준 방식으로 서버에 로그인할 수 없는 경우 권장하는 로그인 방식입니다.

1. CVM 콘솔에 로그인합니다.
2. 점검 예정인 CVM을 선택하여 [Log In]을 클릭합니다. 아래 이미지 참조

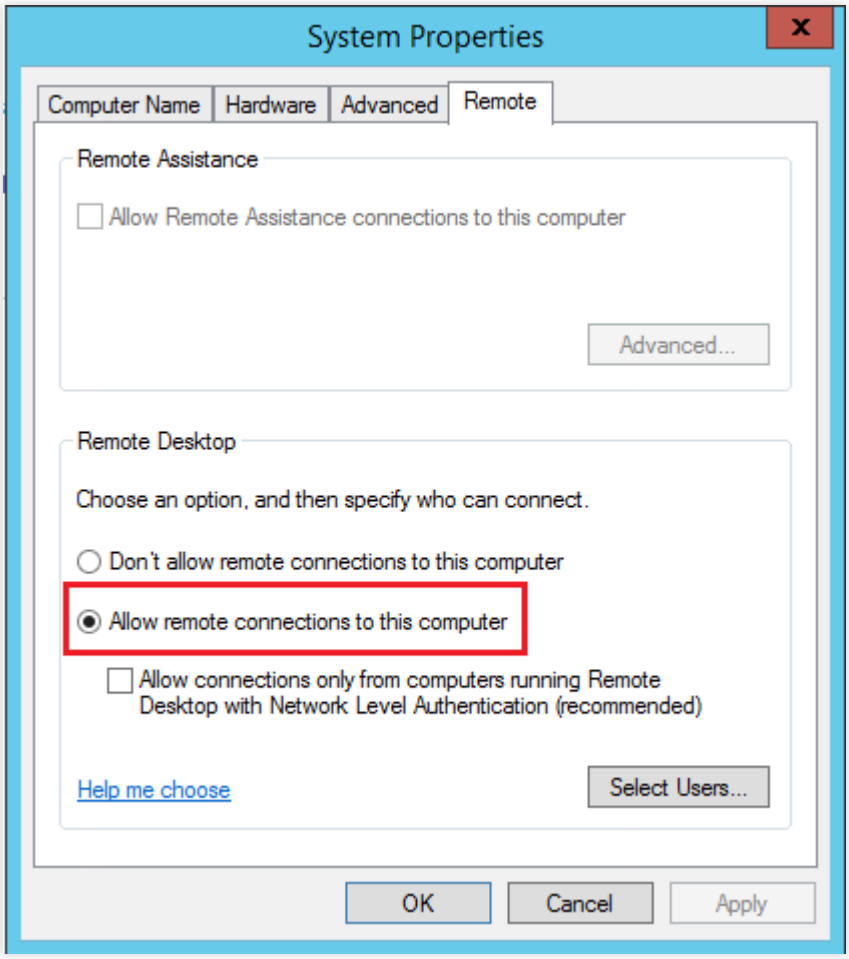


3. 팝업된 "Windows 인스턴스 로그인" 창에서 [Alternative login methods(VNC)]]을 선택하고 [Log In Now]을 클릭하여 CVM에 로그인합니다.
4. 팝업된 로그인 창 왼쪽 상단의 "원격 명령어 발송"을 선택하고 **Ctrl-Alt-Delete**를 클릭하여 시스템 로그인 인터페이스에 접속합니다. 아래 이미지 참조



CVM의 원격 데스크톱 설정 활성화 여부 점검

1. CVM에서 [이 컴퓨터]>[속성]을 우클릭하여 “시스템” 창을 엽니다.
2. “시스템” 창에서 [고급 시스템 설정]을 선택하여 “시스템 속성” 창을 엽니다.
3. "시스템 속성" 창에서 [원격] 탭을 선택하여 "원격 데스크톱" 기능 표시줄에서 [이 컴퓨터로의 원격 연결 허용]을 체크했는지 점검합니다. 아래 이미지 참조

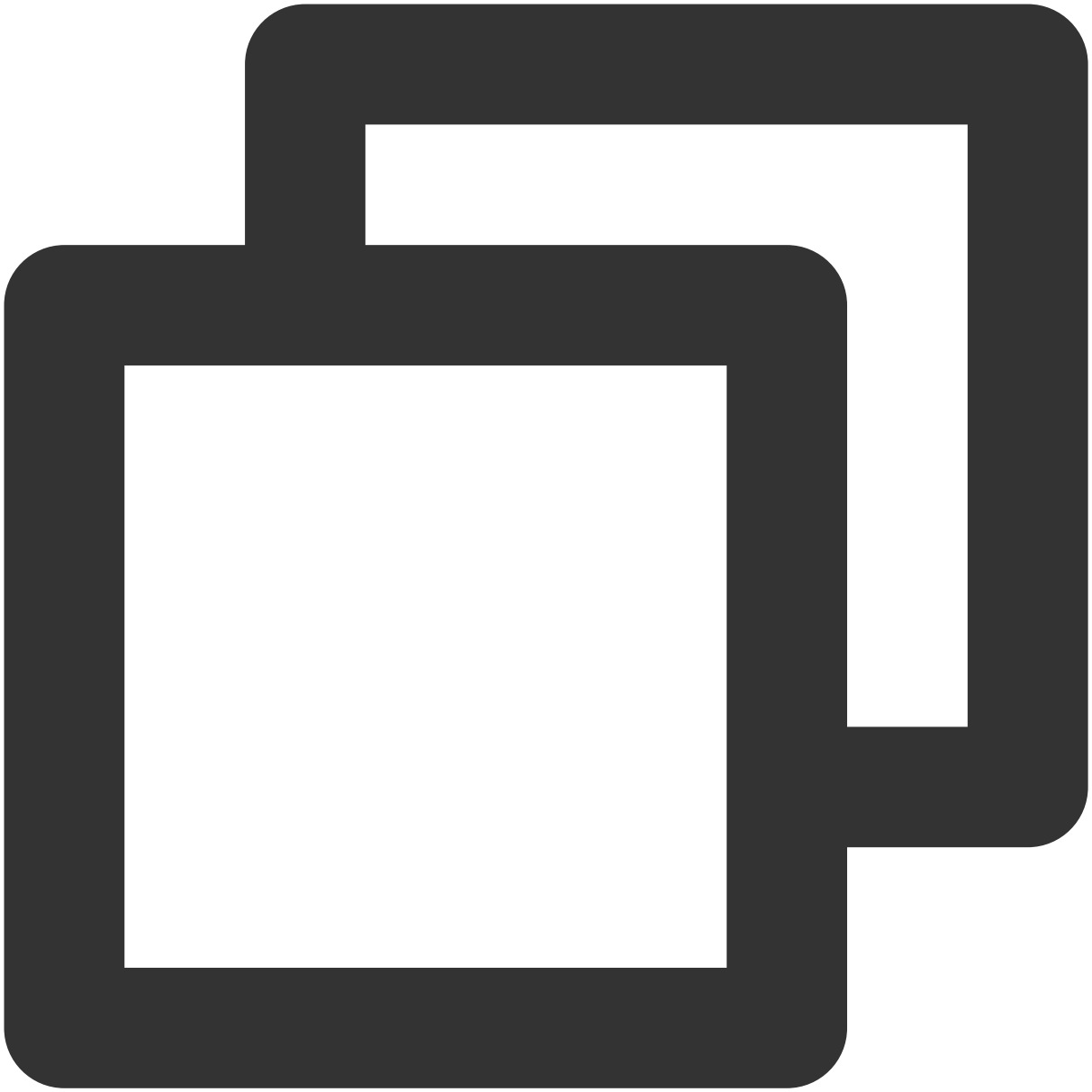


네, 원격 연결 설정 활성화이므로 원격 액세스 포트 오픈 여부를 점검하세요.
아니요, [이 컴퓨터로의 원격 연결 허용]을 체크하고 인스턴스에 다시 원격 연결하여 연결에 성공했는지 조회하세요.

원격 액세스 포트 오픈 여부 점검

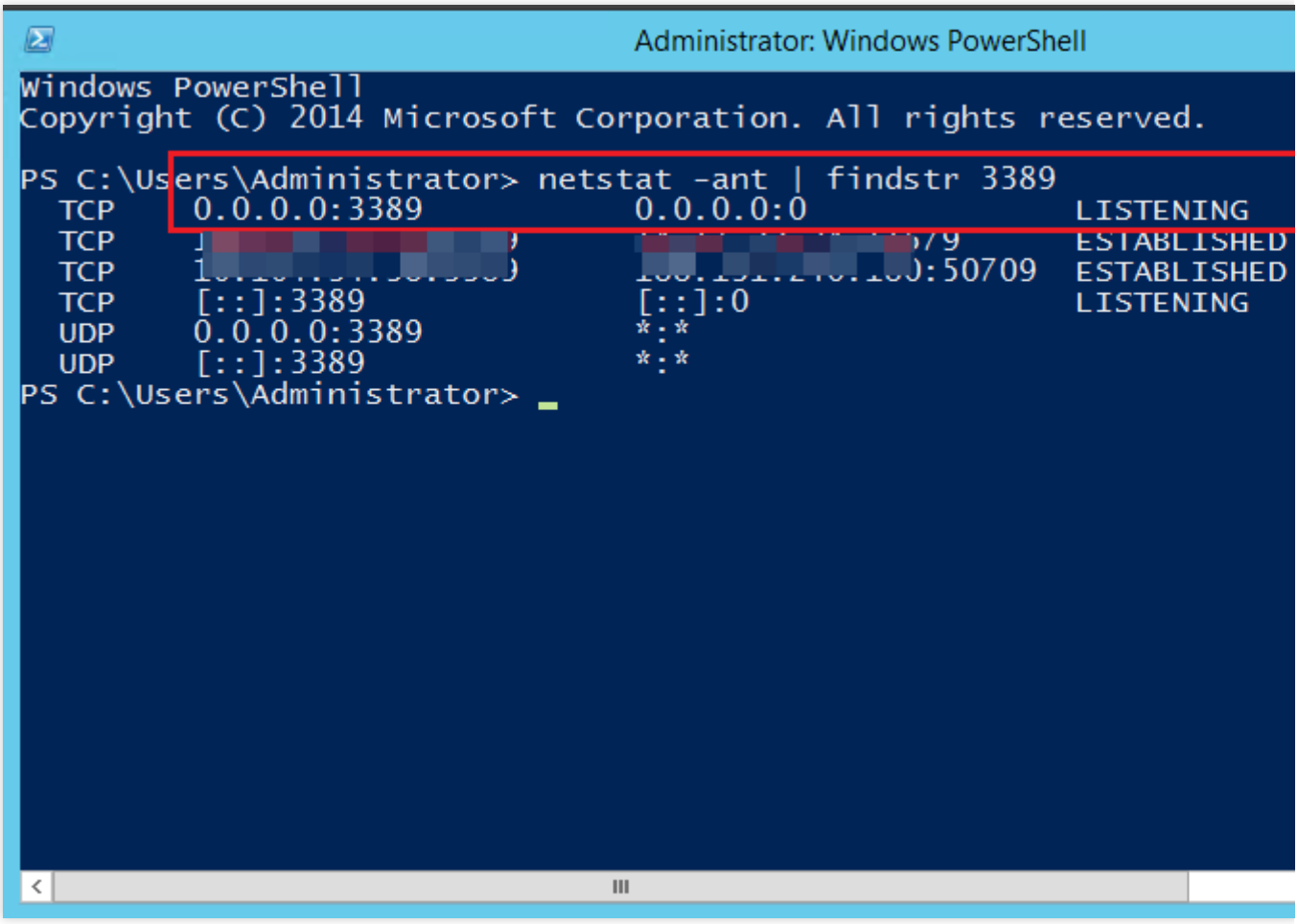
1. CVM에서

을 클릭하여 “Windows PowerShell” 창을 엽니다.
2. “Windows PowerShell” 창에서 아래 명령어를 실행하여 원격 데스크톱 운행 상황(기본 상황에서 원격 데스크톱 서비스 포트 번호는 3389)을 점검합니다.



```
netstat -ant | findstr 3389
```

아래와 같은 결과를 출력하면 정상 상황입니다. 원격 데스크톱을 다시 시작하고 인스턴스에 다시 원격 연결하여 연결에 성공했는지 조회하세요.



아무 연결도 나타나지 않으면 비정상입니다. 레지스트리 원격 포트 일치 여부를 점검하세요.

레지스트리 원격 포트 일치 여부 점검

주의사항 :

해당 단계에서는 **TCP PortNumber** 와 **RDP Tcp PortNumer** 두 곳의 포트 번호를 점검하며, 두 포트 번호가 반드시 일치해야 합니다.

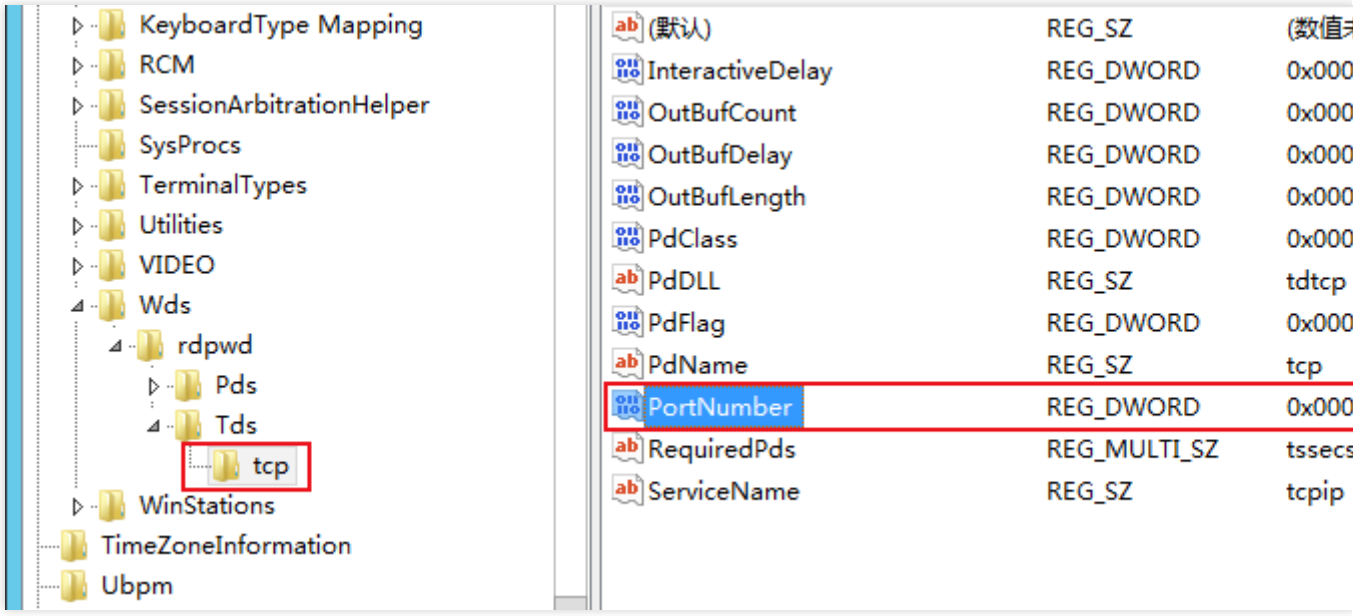
1. CVM에서

을 클릭하고,

을 선택하여 **regedit**를 입력한 다음 **Enter**를 눌러 “레지스트리 편집기” 창을 엽니다.

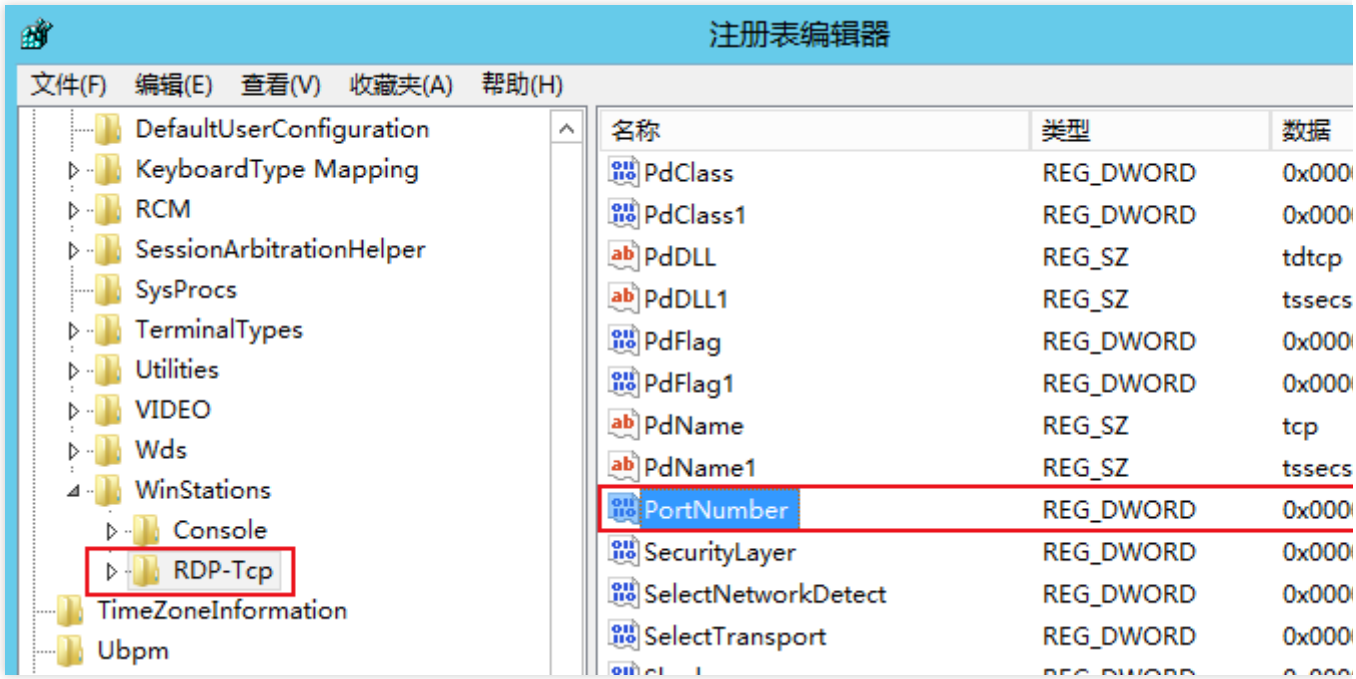
2. 왼쪽 메뉴에서 차례대로 [HKEY_LOCAL_MACHINE]>[SYSTEM]>[CurrentControlSet]>[Control]>[Terminal Server]>[Wds]>[rdpwd]>[Tds]>[tcp] 디렉터리를 엽니다.

3. [tcp] 중에서 PortNumber를 찾아 PortNumber 의 데이터(즉 포트 번호, 기본값 3389)를 기록합니다. 아래 이미지 참조



4. 왼쪽 메뉴에서 차례대로 [HKEY_LOCAL_MACHINE]>[SYSTEM]>[CurrentControlSet]>[Control]>[Terminal Server]>[WinStations]>[RDP-Tcp] 디렉터리를 엽니다.

5. [RDP-Tcp] 중에서 PortNumber를 찾고, [RDP-Tcp] 중의 PortNumber 데이터(포트 번호)와 [tcp] 중의 PortNumber 데이터(포트 번호)가 일치하는지 확인합니다. 아래 이미지 참조



일치하지 않을 경우 6단계를 실행하세요.

일치할 경우 원격 로그인 서비스 재시작하세요.

6. [RDP-Tcp] 중에서 PortNumber를 더블 클릭합니다.

7. 팝업된 창에서 "값 데이터"를 0 - 65535 사이의 사용 중이 아닌 포트로 수정하여 **TCP PortNumber** 와 **RDP Tcp PortNumer** 포트 번호가 일치하도록 한 후 [확인]을 클릭합니다.

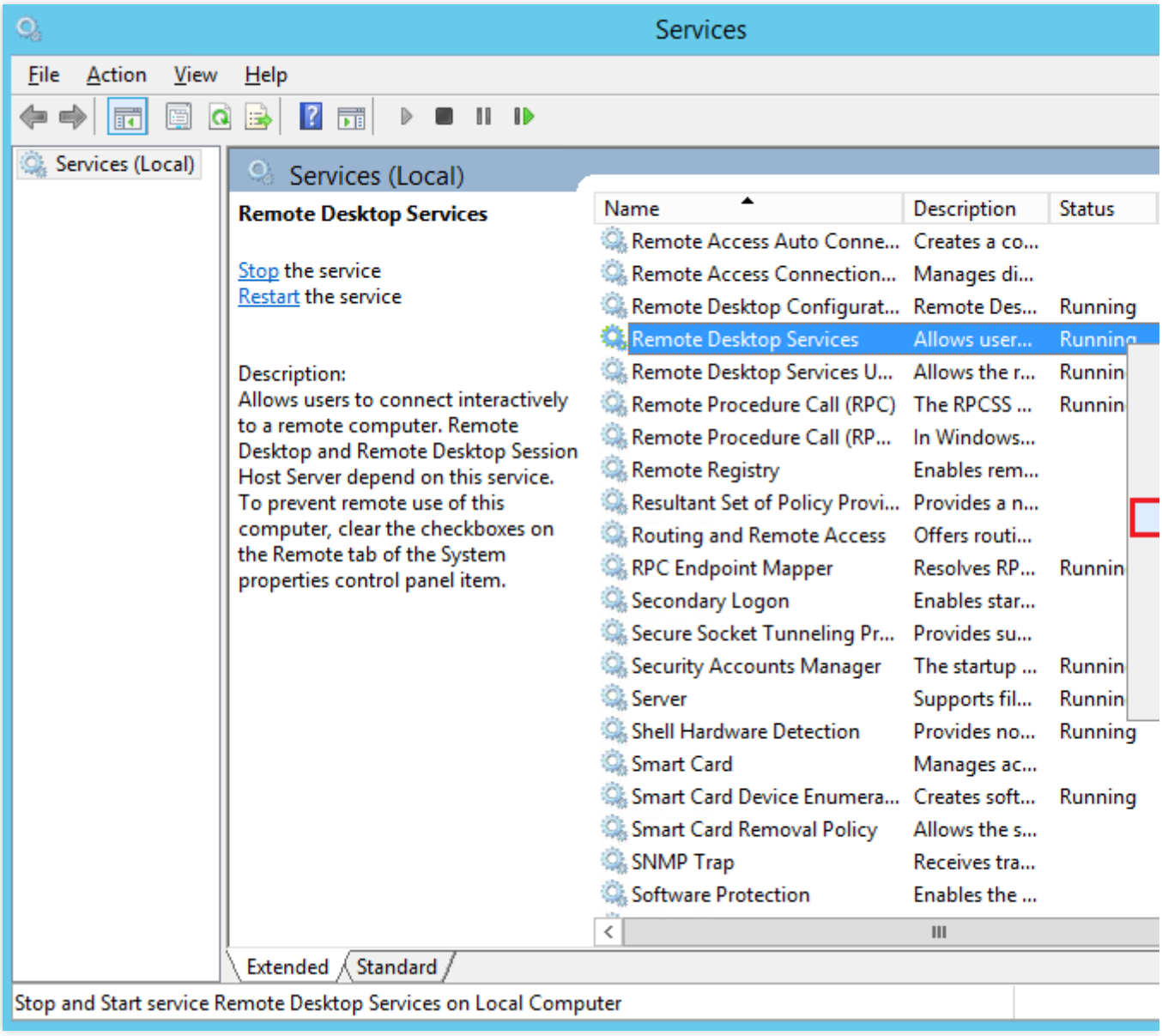
8. 수정 완료 후 CVM 콘솔에서 해당 인스턴스를 재시작하고 인스턴스 원격 연결을 다시 진행하여 연결 여부를 조회합니다.

원격 로그인 서비스 재시작

1. CVM에서

을 클릭하고,

을 선택하여 **services.msc**를 입력한 다음 **Enter**를 눌러 "서비스" 창을 엽니다.
2. "서비스" 창에서 [Remote Desktop Services]를 찾아 [Remote Desktop Services]를 우클릭하고 [재시작]을 선택하여 원격 로그인 서비스를 재시작합니다. 아래 이미지 참조



기타 작업

상기 작업을 실행해도 원격 로그인할 수 없는 문제를 해결하지 못할 경우 Submit Ticket을 통해 피드백 바랍니다.

Linux 인스턴스 로그인 관련 문제
Linux 인스턴스에 로그인할 수 없을 경우

최종 업데이트 날짜: : 2024-02-02 11:09:47

본 문서에서는 Linux 인스턴스 로그인 실패의 가능한 원인과 문제 해결 방법에 대해 설명합니다. 지침에 따라 문제의 원인을 식별하고 해결 방법을 배울 수 있습니다.

문제 파악

자가 진단 툴 사용

Tencent Cloud는 대역폭, 방화벽 및 보안 그룹 설정 등의 문제로 인한 것인지 판단할 수 있는 자가 진단 툴을 제공합니다. 70%의 장애는 툴에 의해 위치가 측정되며, 점검된 원인에 따라 로그인 실패를 일으키는 장애 문제의 위치를 측정할 수 있습니다.
1. 자가 진단을 클릭하여 자가 진단 툴을 엽니다.
2. 메시지가 표시되면 타깃 CVM 인스턴스를 선택하고 **점검 시작**을 클릭합니다.

TAT(TencentCloud Automation Tools)를 사용하여 명령 전송

TAT를 사용하여 문제 해결 및 문제 찾기를 위해 인스턴스에 명령을 보낼 수 있습니다. 순서는 다음과 같습니다.
1. CVM 콘솔에 로그인 한 후 인스턴스 리스트에서 타깃 인스턴스 ID를 클릭합니다.
2. 인스턴스 세부 정보 페이지에서 **명령 실행** 탭을 선택하고 **명령 실행**을 클릭합니다.
3. '실행 명령' 팝업 창에서 필요에 따라 명령을 선택합니다. **명령 실행**을 클릭하고 결과를 확인합니다.
예를 들어 'df -TH'를 입력하고 **명령 실행**을 클릭하면 로그인하지 않고도 인스턴스의 결과를 볼 수 있습니다.
자세한 내용은 Tencent Cloud Automation Tools를 참고하십시오.
설명 :
자가 진단 툴로 문제를 진단할 수 없다면 CVM에 VNC 방식을 통해 로그인하여 장애를 진단하시길 권장합니다.

가능한 원인

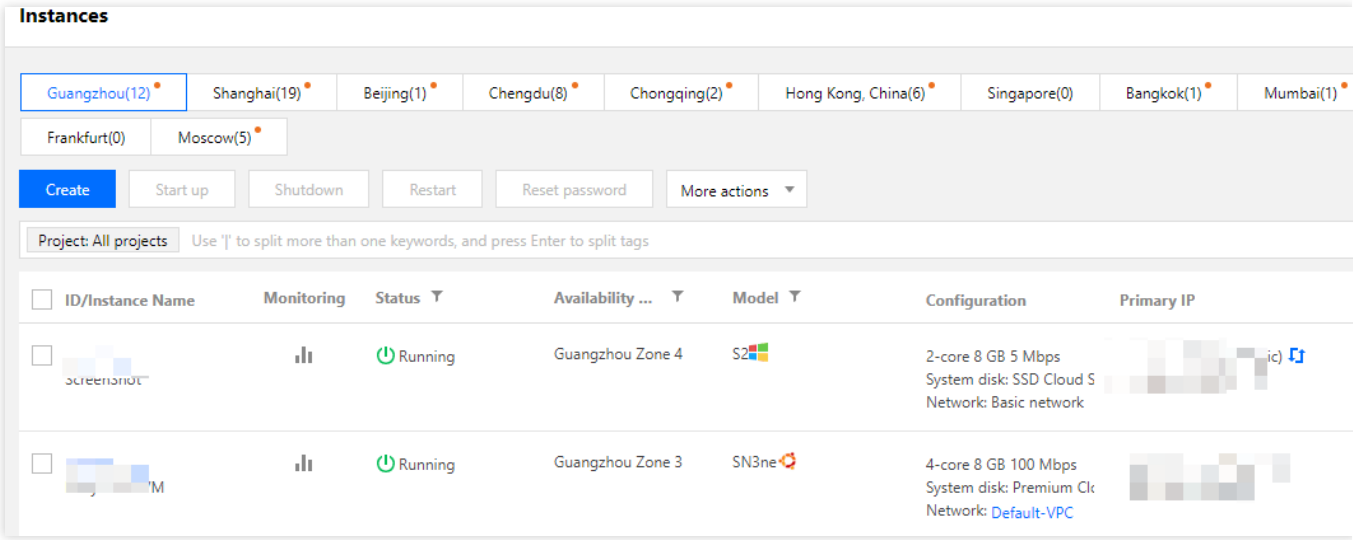
Linux 인스턴스 로그인 실패의 주요 원인은 다음과 같습니다.
SSH 키 문제
비밀번호 문제
높은 대역폭 이용률
서버 고부하
부적절한 보안 그룹 규칙

장애 처리

VNC 방식을 통해 로그인

표준 방법(Orcaterm) 또는 원격 로그인 소프트웨어를 사용하여 Linux 인스턴스에 로그인할 수 없는 경우 Tencent Cloud VNC를 사용하여 로그인하고 문제 원인을 찾을 수 있습니다.

1. CVM 콘솔에 로그인합니다.
2. 인스턴스 관리 페이지에서 아래 이미지와 같이 액세스하려는 인스턴스를 찾고 **로그인**을 클릭합니다.



3. '표준 로그인 | Linux 인스턴스' 팝업 창에서 **VNC 로그인**을 선택합니다.

설명：

인스턴스의 비밀번호를 잊어버린 경우 콘솔에서 재설정할 수 있습니다. 자세한 내용은 인스턴스 비밀번호 재설정을 참고하십시오.

4. 사용자 이름과 비밀번호를 입력하여 로그인 프로세스를 완료합니다.

SSH 키 문제

장애 현상: SSH를 사용하여 Linux 인스턴스에 로그인하는 동안 연결을 사용할 수 없거나 실패했음을 나타내는 메시지가 나타납니다.

처리 순서: SSH 방식으로 Linux 인스턴스에 로그인할 수 없을 경우를 참고하여 문제를 해결합니다.

비밀번호 문제

장애 현상: 비밀번호를 잊었거나, 잘못된 비밀번호 입력 또는 비밀번호 재설정에 실패해 로그인할 수 없는 경우입니다.

솔루션: CVM 콘솔에서 인스턴스의 비밀번호를 재설정하고 인스턴스를 재시작합니다.

처리 순서: 자세한 절차는 인스턴스 비밀번호 재설정을 참고하십시오.

높은 대역폭 이용률

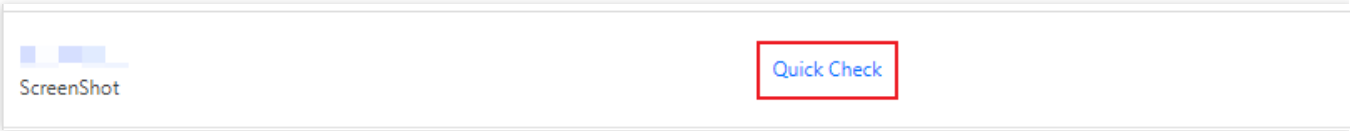
장애 현상: 자가 진단 툴을 통해 진단한 결과, 대역폭 이용률이 너무 높은 것이 원인인 경우입니다.
처리 순서:
1. VNC 로그인을 통해 인스턴스에 로그인합니다.
2. 높은 대역폭 점유율로 로그인할 수 없을 경우를 참고하여 인스턴스의 대역폭 사용률을 확인하고 그에 따라 문제 해결을 수행합니다.

서버 고부하

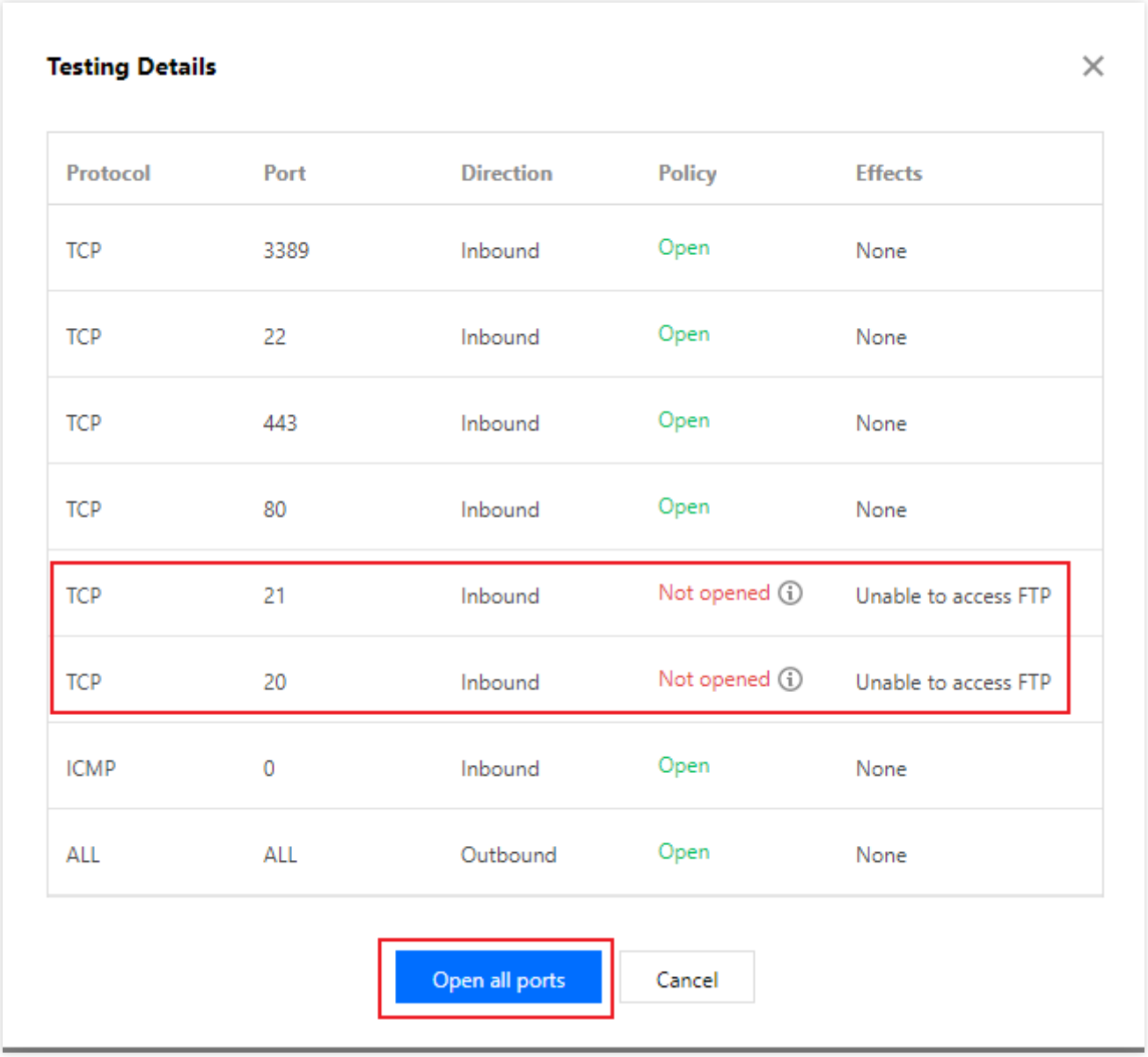
장애 현상: 자가 진단 툴 또는 Tencent Cloud Observability Platform에 서버 CPU 워크로드가 너무 높고 시스템이 원격 연결을 수행할 수 없거나 액세스가 느린 것으로 표시됩니다.
예상 원인: 바이러스, 트로이 목마, 3rd party 바이러스 백신 소프트웨어, 응용 프로그램 예외, 드라이버 예외 및 백엔드의 소프트웨어 자동 업데이트로 인해 CPU 이용률이 높아져 CVM 로그인 실패 또는 액세스 속도 저하가 발생할 수 있습니다.
처리 순서:
1. VNC 로그인을 통해 인스턴스에 로그인합니다.
2. Linux 인스턴스: CPU 혹은 메모리 점유율이 높아 로그인 할 수 없을 경우를 참고하여 '작업 관리자'에서 부하가 높은 프로세스를 찾습니다.

부적절한 보안 그룹 규칙

장애 현상: 자가 진단 툴은 보안 그룹 규칙 구성이 부적절하여 로그인 실패로 이어짐을 보여줍니다.
처리 순서: 보안 그룹(포트) 진단 툴을 통해 문제를 해결하십시오.



보안 그룹의 포트 문제로 인해 문제가 발생한 경우 **모든 포트 열기** 기능을 사용하여 모든 포트를 열 수 있습니다.



보안 그룹에 대한 사용자 정의 규칙을 정의하려면 보안 그룹 규칙 추가를 참고십시오.

기타 솔루션

앞의 문제 해결 방법을 사용하여도 여전히 Linux 인스턴스에 로그인할 수 없으면 자가 진단 결과를 저장하고 티켓 제출을 통해 지원을 받으십시오.

SSH 방식으로 Linux 인스턴스에 로그인할 수 없을 경우

최종 업데이트 날짜: : 2024-02-02 11:09:48

설명 :
본문은 커뮤니티에서 제공한 내용으로, 참고용으로만 제공됩니다. Tencent Cloud 관련 제품과는 무관합니다.
본문에서 언급된 관련 파일 작업은 신중히 진행하시기 바랍니다. 필요한 경우 스냅샷 등 방법을 통해 데이터를 백업할 수 있습니다.

현상 설명

SSH를 사용해 Linux 인스턴스에 로그인 시 연결이 되지 않거나 연결이 실패하여 Linux 인스턴스에 정상적으로 로그인할 수 없다는 메시지가 표시됩니다.

문제 포지셔닝 및 처리

SSH를 사용한 Linux 인스턴스에 로그인에 실패하고 오류 메시지가 반환되면, 오류 메시지를 기록하고, 다음과 같은 일반적인 오류 메시지와의 매칭을 통해 문제를 빠르게 진단하고, 처리 방법을 참고하여 해결하십시오.
SSH 로그인 오류 User root not allowed because not listed in AllowUsers

문제 원인

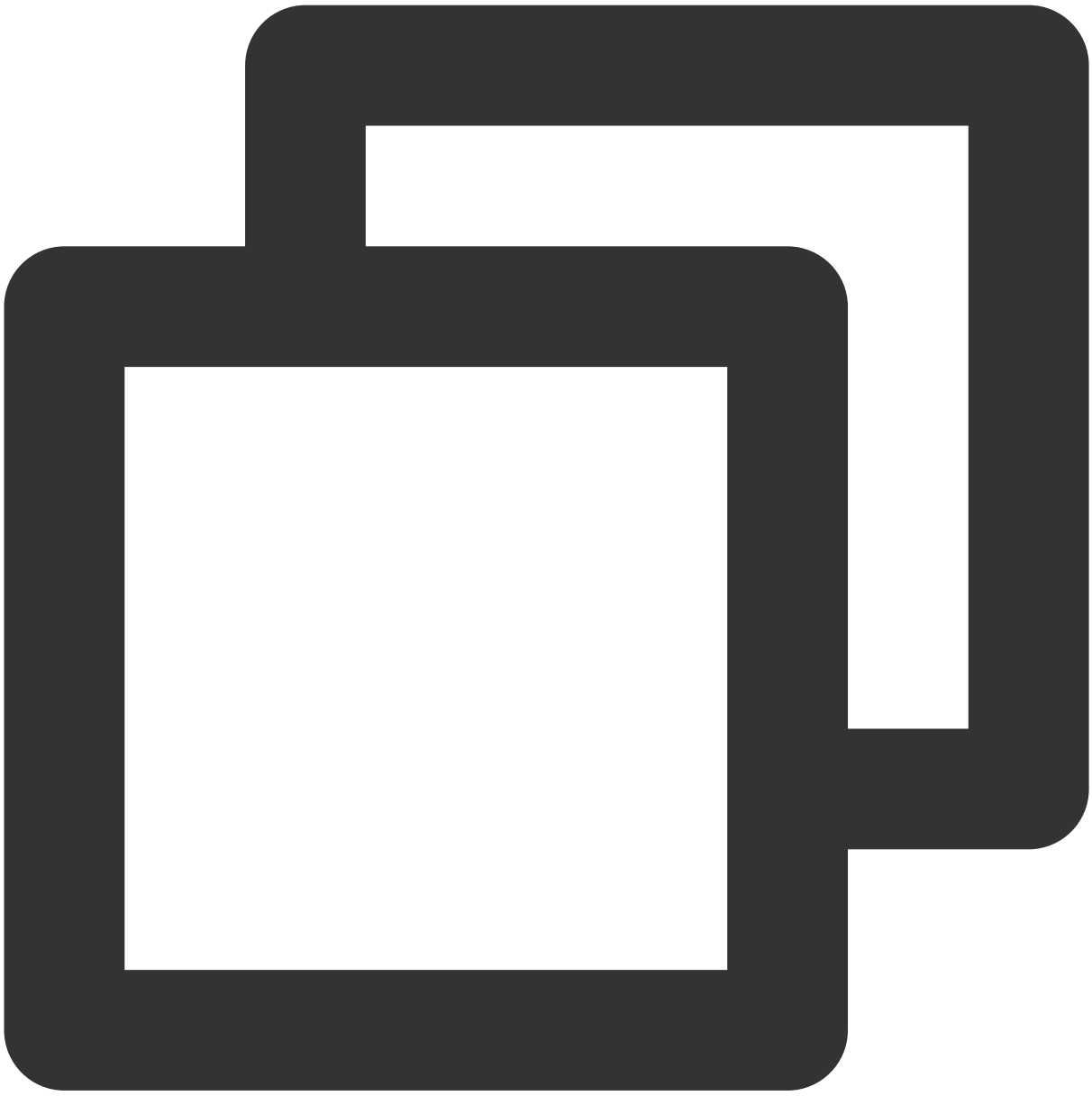
이 문제는 일반적으로 SSH 서비스가 사용자 로그인 제어 매개변수를 실행하여 사용자 로그인을 제한하였을 때 발생합니다. 매개변수 설명은 다음과 같습니다.
AllowUsers: 로그인이 허용된 사용자 화이트리스트로, 이 매개변수가 표시된 사용자만 로그인할 수 있습니다.
DenyUsers: 로그인이 거부된 사용자 블랙리스트로, 이 매개변수가 표시된 모든 사용자는 로그인이 거부됩니다.
AllowGroups: 로그인이 허용된 사용자 그룹의 화이트리스트로, 이 매개변수가 표시된 사용자 그룹만 로그인할 수 있습니다.
DenyGroups: 로그인이 거부된 사용자 그룹의 블랙리스트로, 이 매개변수가 표시된 사용자 그룹은 모두 로그인이 거부됩니다.
설명 :
거부 정책은 허용 정책보다 우선 순위가 높습니다.

해결 방식

1. 처리 순서를 참고하여 SSH 구성 파일 `sshd_config` 로 이동한 후, 설정을 확인합니다.
2. 사용자 로그인 제어 매개변수를 삭제하고 SSH 서비스를 다시 시작합니다.

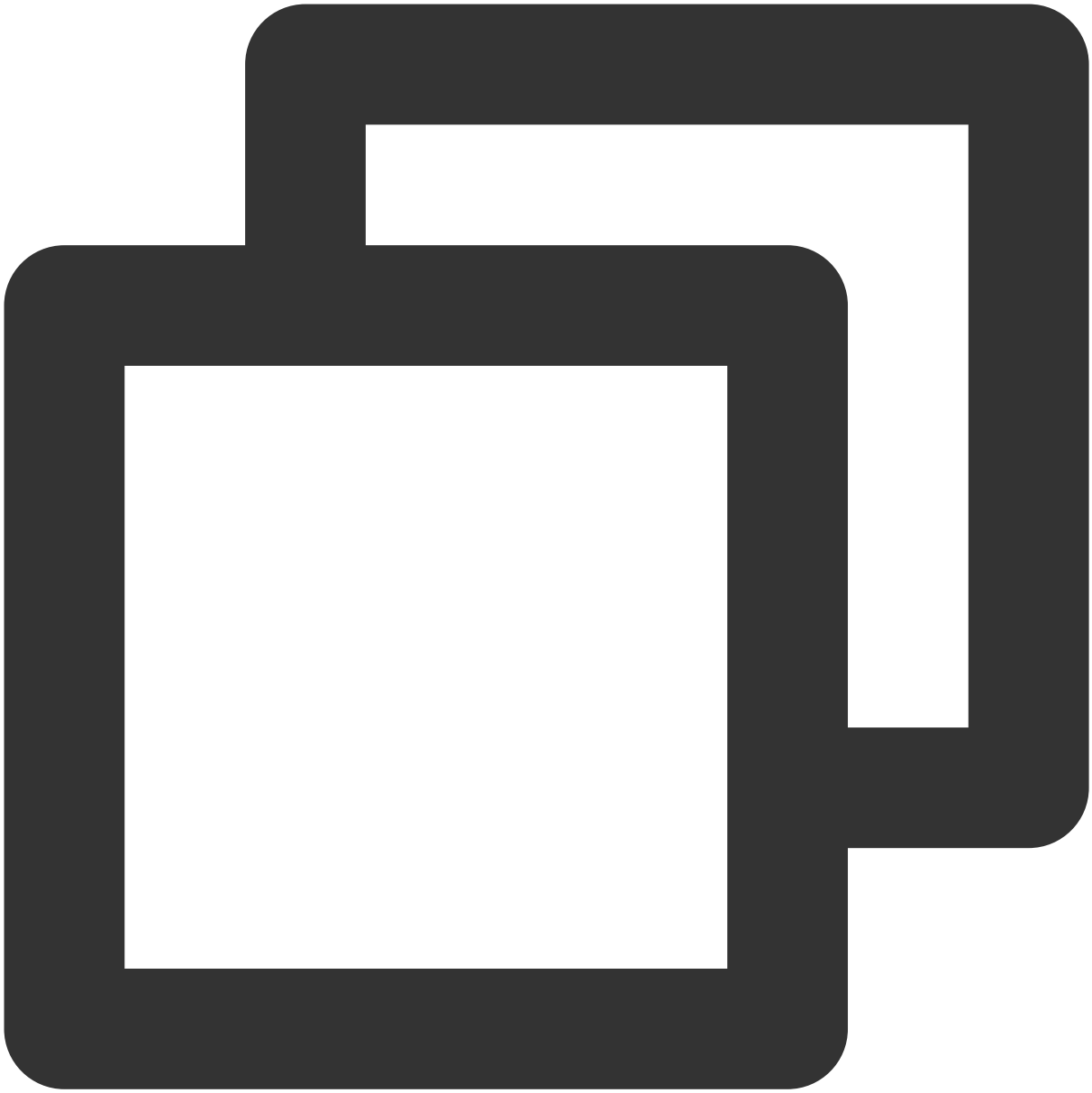
처리 순서

1. VNC 사용하여 Linux 인스턴스에 로그인합니다.
2. 다음 명령을 실행하고 VIM 편집기를 사용하여 `sshd_config` 구성 파일로 이동합니다.



```
vim /etc/ssh/sshd_config
```

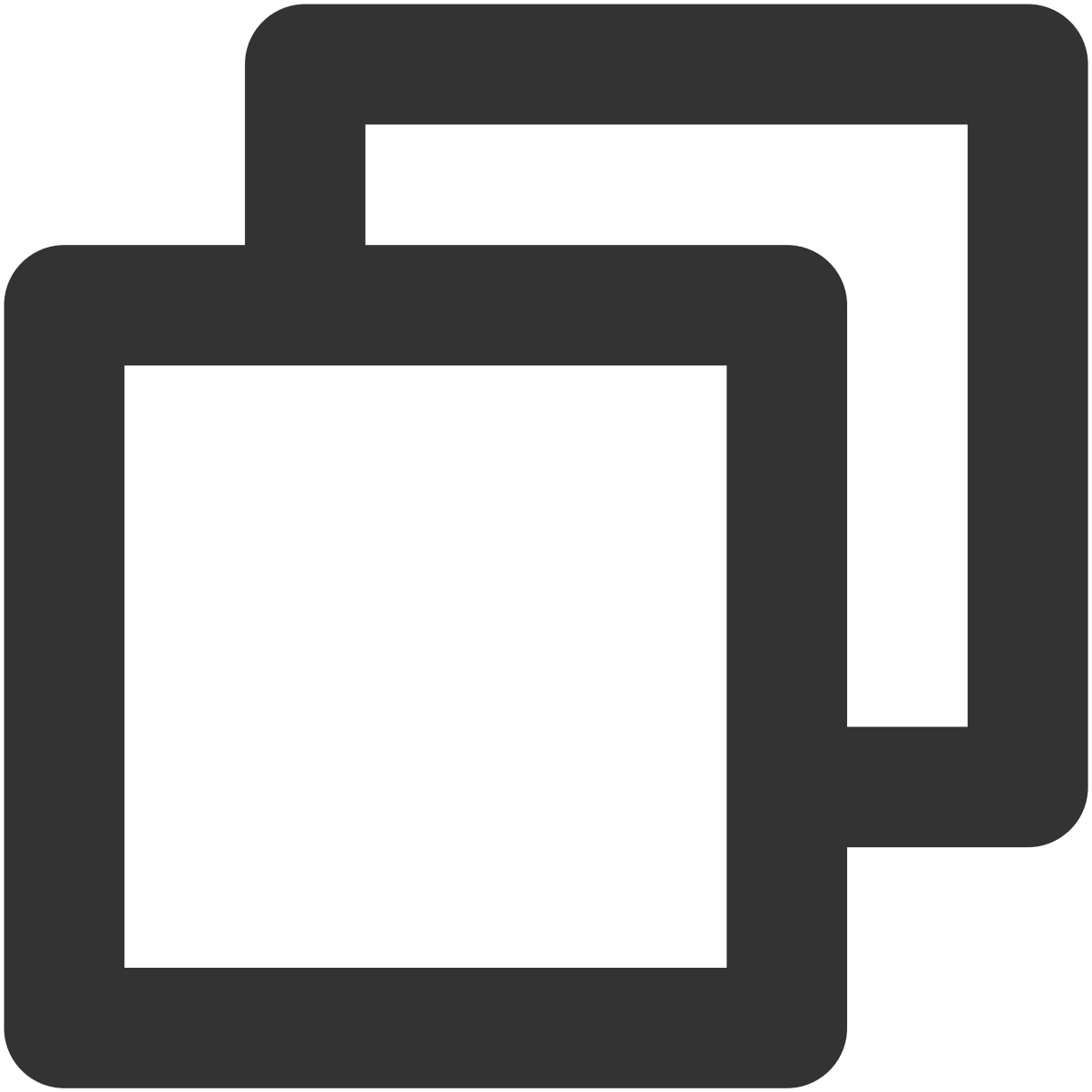
3. **i**를 눌러 편집 모드로 이동하고, 다음 설정을 찾아 삭제하거나, 각 행의 시작 부분에 `#` 을 추가하여 주석을 진행합니다.



```
AllowUsers root test
DenyUsers test
DenyGroups test
AllowGroups root
```

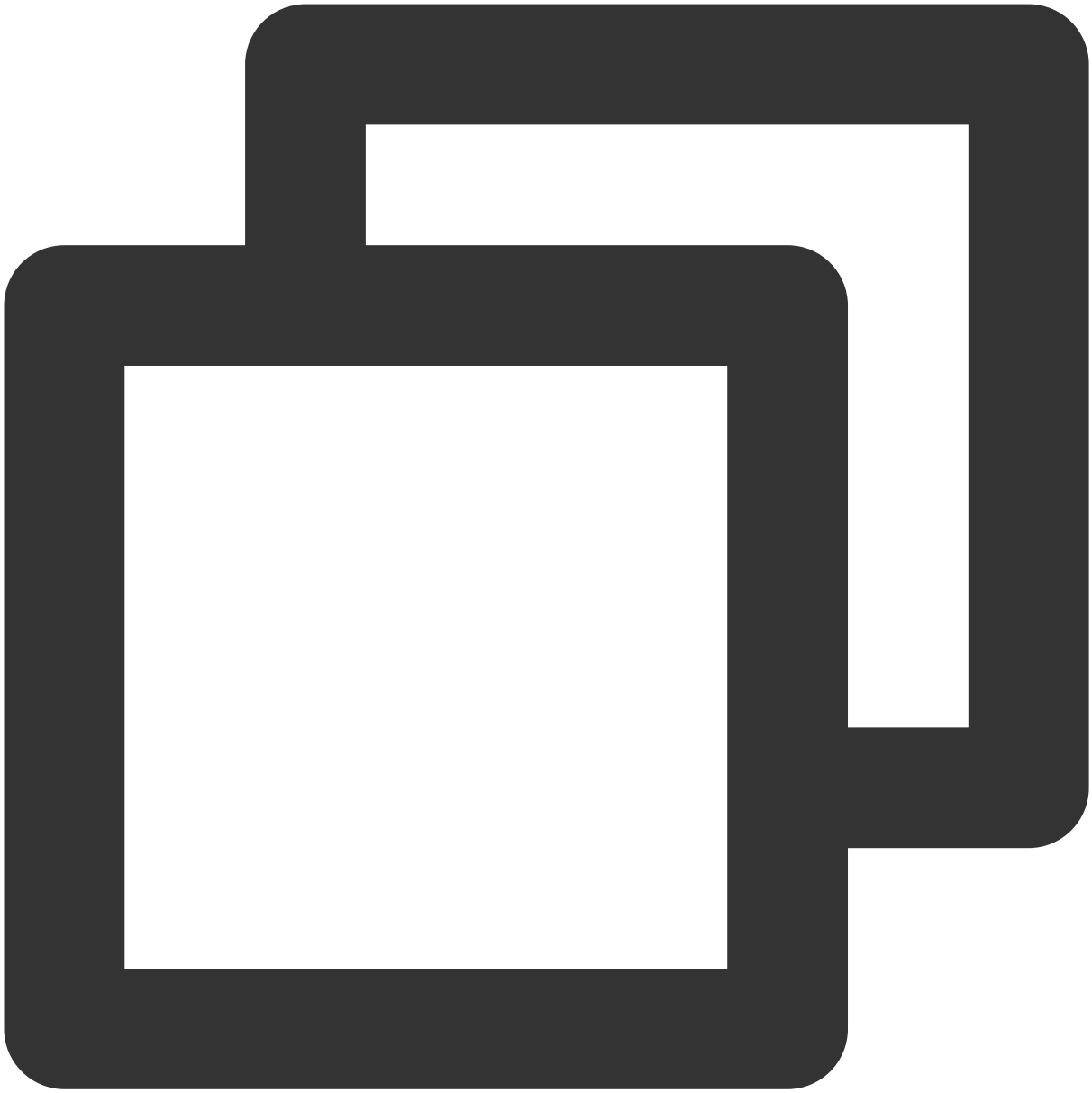
4. **Esc**를 눌러 편집 모드를 종료하고 **:wq**를 입력하여 변경 사항을 저장합니다.
5. 실제 운영 체제에 따라 다음 명령을 실행하여 SSH 서비스를 재시작합니다.

CentOS



```
systemctl restart sshd.service
```

Ubuntu



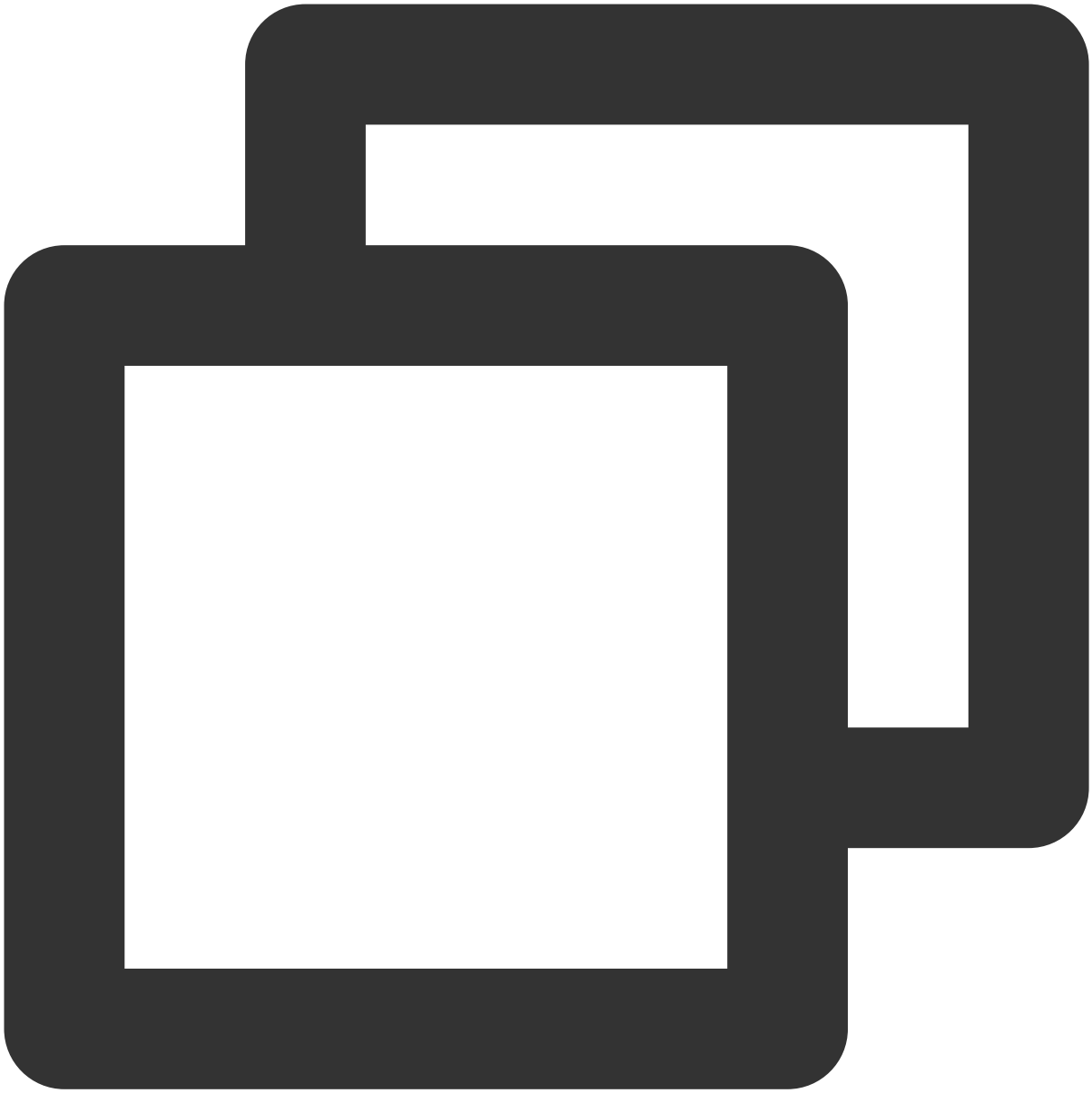
```
service sshd restart
```

SSH 서비스를 재시작한 후 SSH를 사용하여 로그인할 수 있습니다. 상세 내용은 SSH를 사용하여 Linux 인스턴스에 로그인 을 참고하십시오.

SSH 로그인 오류 Disconnected:No supported authentication methods available

현상 설명

SSH를 사용하여 로그인하면 다음 오류 메시지가 나타납니다.



```
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
sshd[10826]: Connection closed by xxx.xxx.xxx.xxx.
Disconnected:No supported authentication methods available.
```

문제 원인

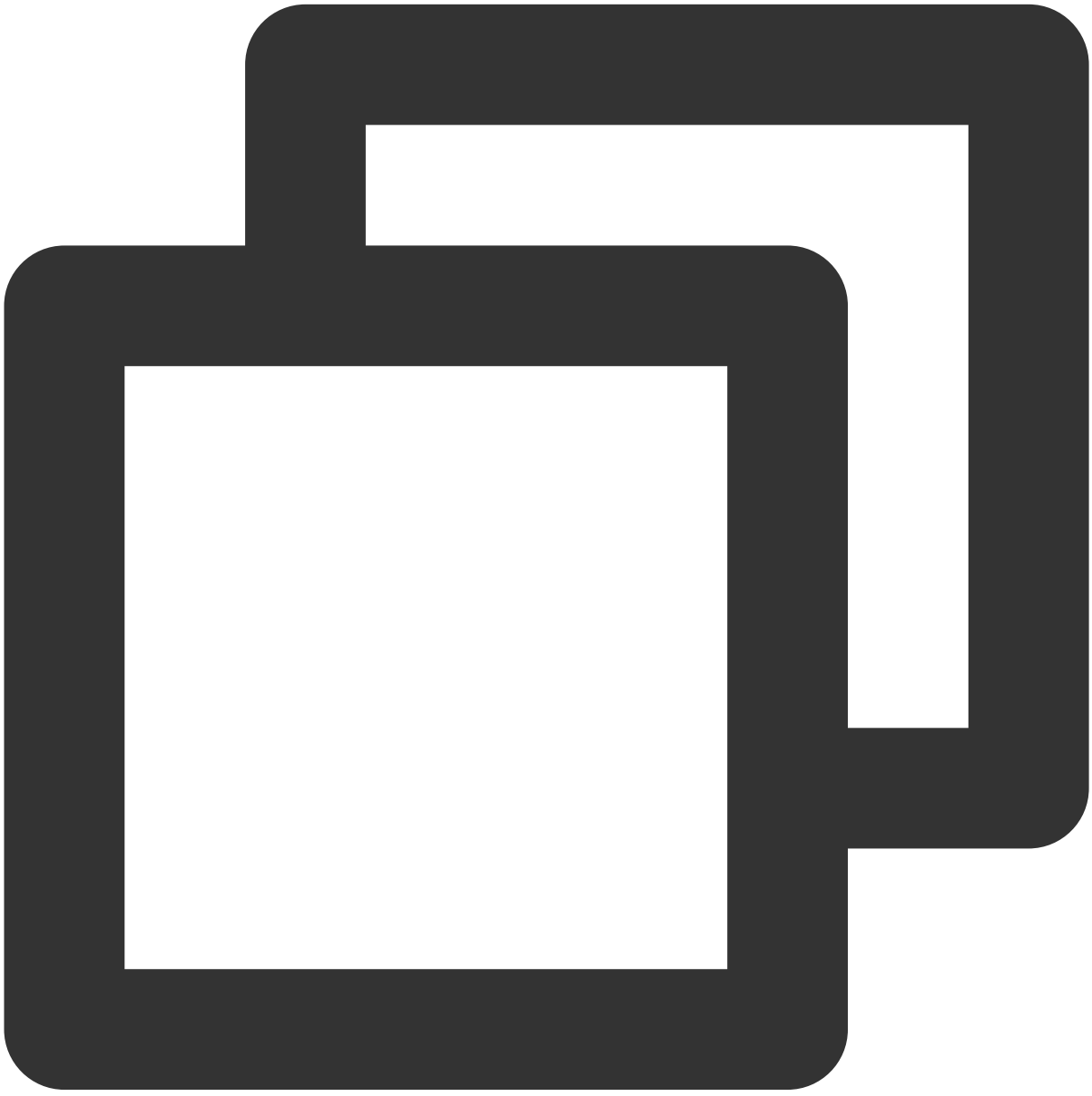
원인은 SSH 서비스가 'PasswordAuthentication' 매개변수를 수정하고 비밀번호 인증 로그인을 비활성화하였기 때문입니다.

해결 방식

1. 처리 순서를 참고하여 SSH 구성 파일 `sshd_config` 로 이동합니다.
2. 'PasswordAuthentication' 매개변수를 수정하고 SSH 서비스를 재시작합니다.

처리 순서

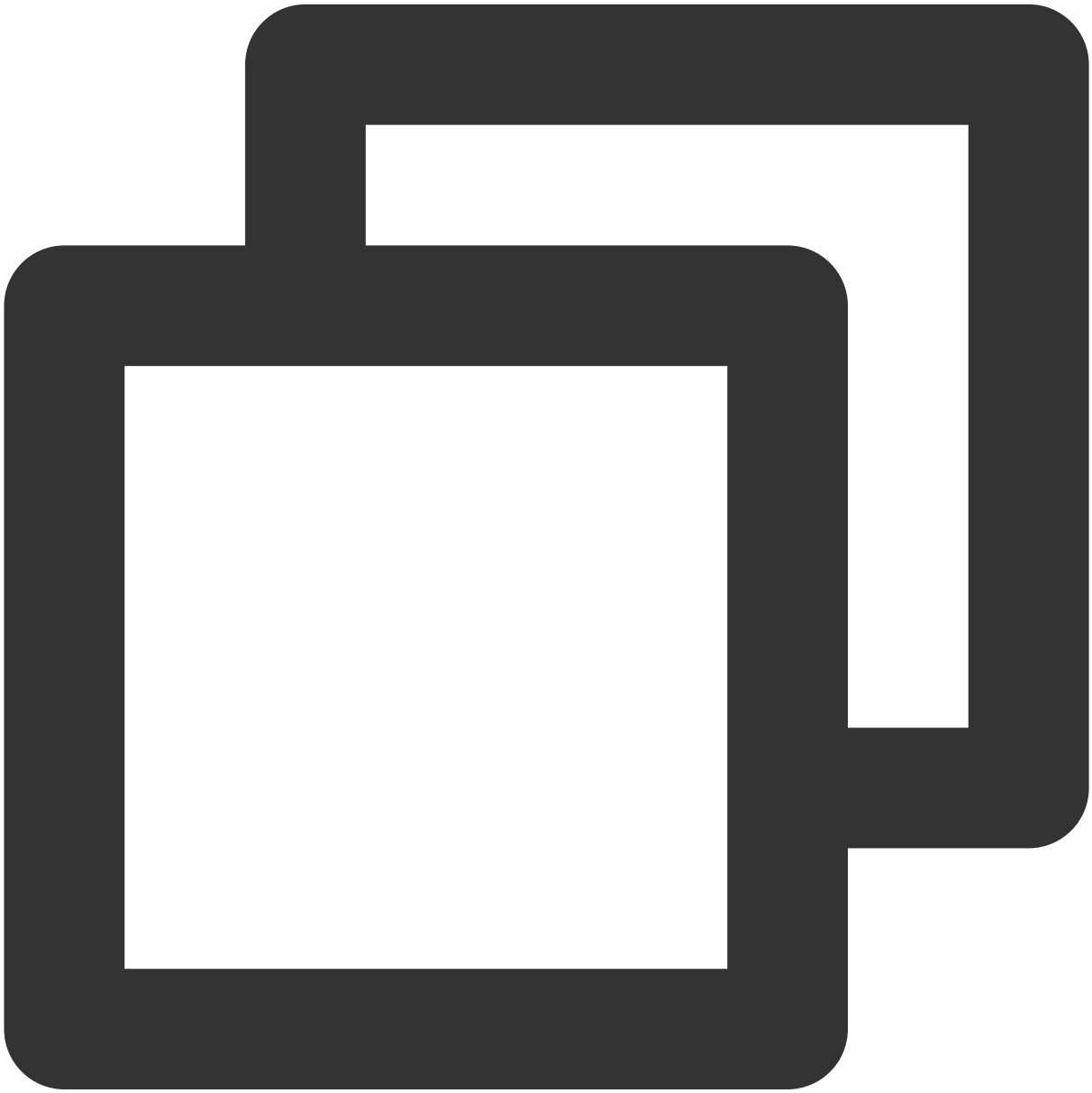
1. VNC 사용하여 Linux 인스턴스에 로그인합니다.
2. 다음 명령을 실행하고 VIM 편집기를 사용하여 `sshd_config` 구성 파일로 이동합니다.



```
vim /etc/ssh/sshd_config
```

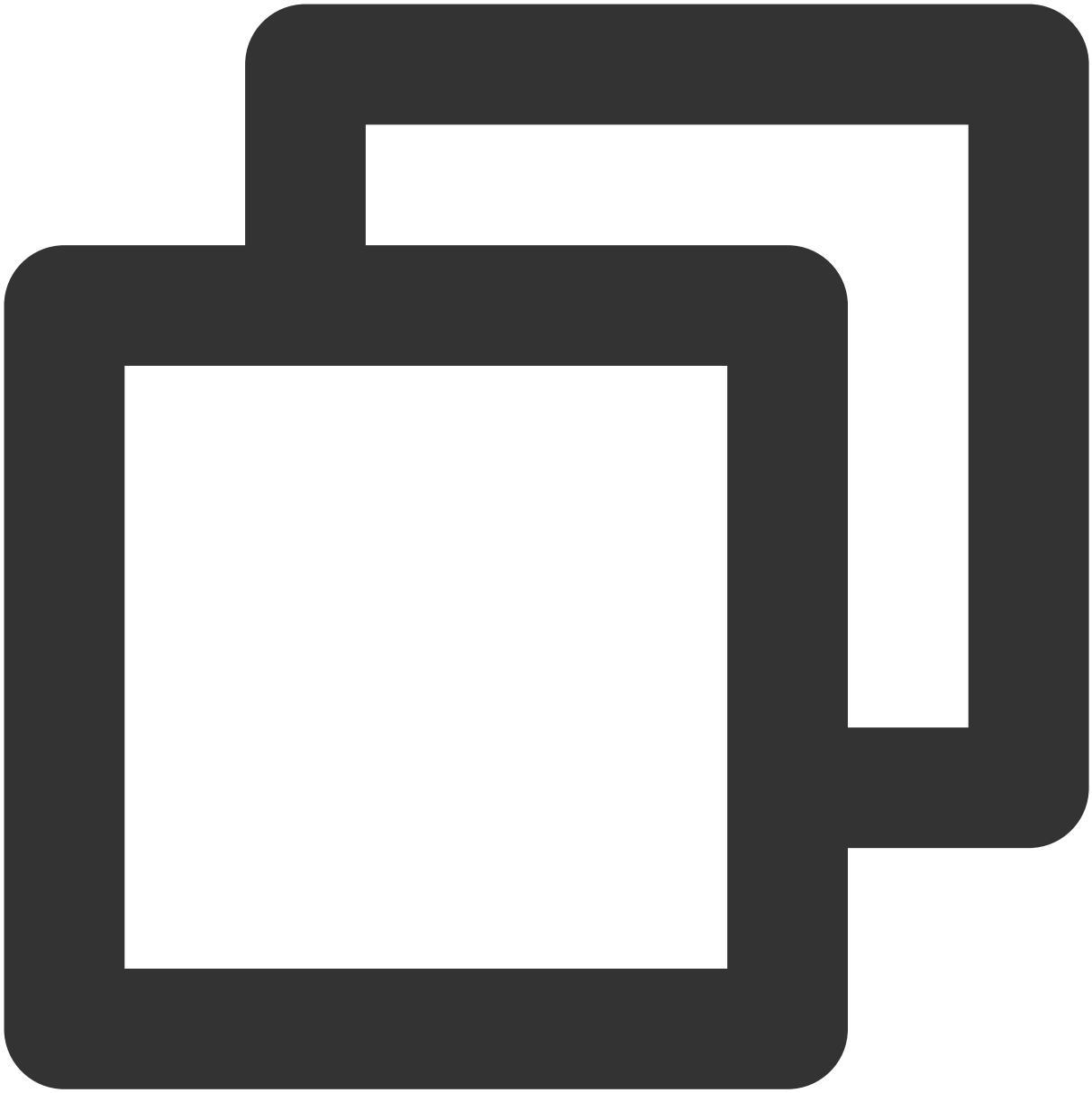
3. **i**를 눌러 편집 모드로 이동한 후, `PasswordAuthentication no` 를 `PasswordAuthentication yes` 로 변경합니다.
4. **Esc**를 눌러 편집 모드를 종료하고 **:wq**를 입력하여 변경 사항을 저장합니다.
5. 실제 운영 체제에 따라 다음 명령을 실행하여 SSH 서비스를 재시작합니다.

CentOS



```
systemctl restart sshd.service
```

Ubuntu



```
service sshd restart
```

SSH 서비스를 재시작한 후 SSH를 사용하여 로그인할 수 있습니다. 상세 내용은 SSH를 사용하여 Linux 인스턴스에 로그인 을 참고하십시오.

SSH 로그인 오류 ssh_exchange_identification: read: Connection reset by peer

현상 설명

SSH를 사용하여 로그인할 때, “ssh_exchange_identification: read: Connection reset by peer” 오류 메시지 또는 다음 오류 메시지가 나타납니다.

“ssh_exchange_identification: Connection closed by remote host”
“kex_exchange_identification: read: Connection reset by peer”
“kex_exchange_identification: Connection closed by remote host”

문제 원인

이러한 유형의 문제에는 여러 가지 원인이 있으며 일반적인 원인은 다음과 같습니다.
로컬 액세스 제어로 인한 연결 제한
일부 침입 방지 소프트웨어가 Fail2ban, denyhost 등과 같은 방화벽 규칙을 변경함
sshd 설정의 최대 연결 수 제한
로컬 네트워크 문제

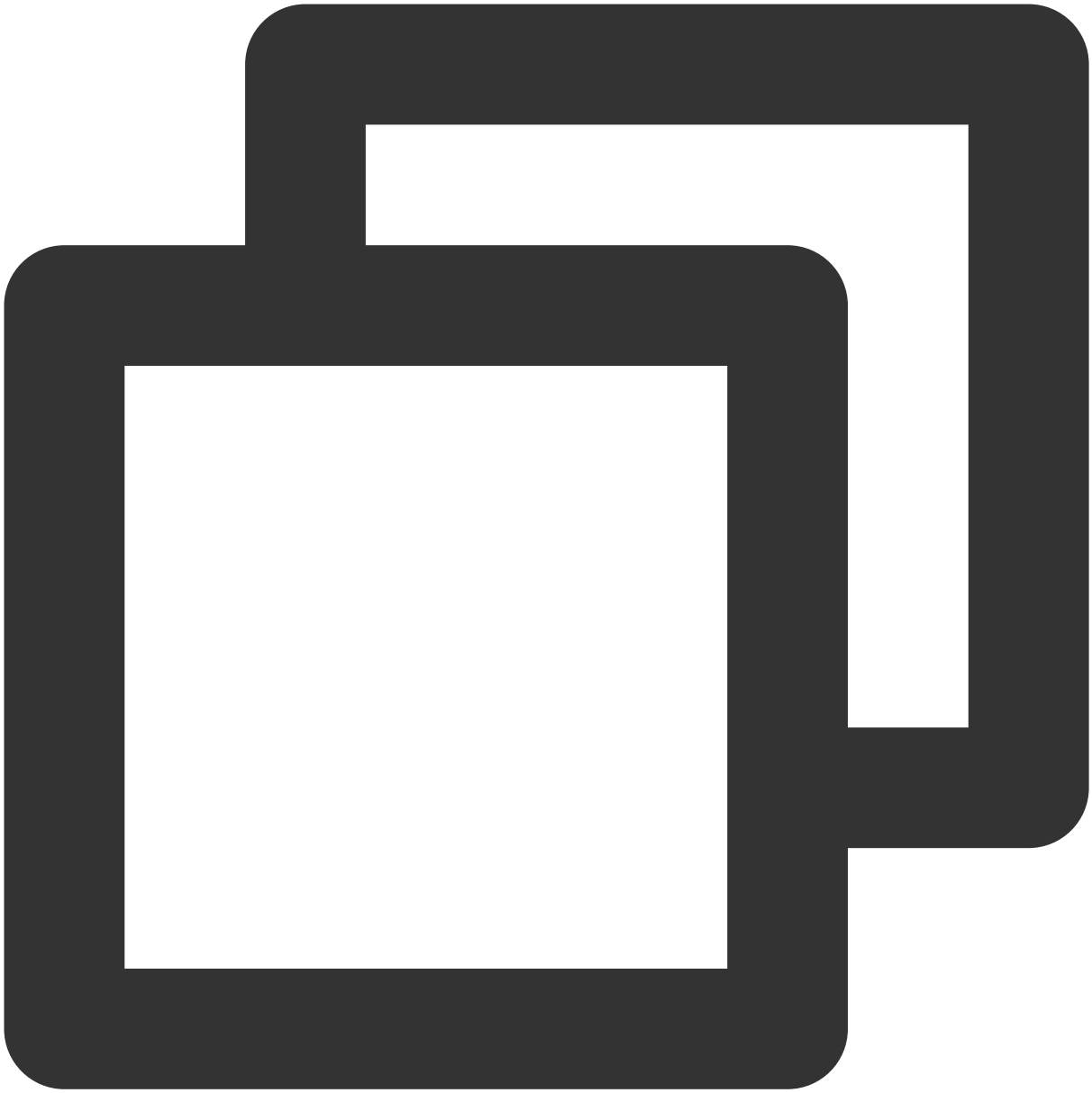
해결 방식

처리 순서를 참고하여 액세스 정책, 방화벽 규칙, sshd 설정 및 네트워크 환경 관련 문제를 진단 및 해결합니다.

처리 순서

액세스 정책 설정 확인 및 조정

Linux에서 `/etc/hosts.allow` 및 `/etc/hosts.deny` 파일을 통해 액세스 정책을 설정할 수 있습니다. 두 파일은 각각 허용 및 차단 정책에 해당됩니다. 예를 들어, `hosts.allow` 파일에 신뢰할 수 있는 호스트 규칙을 설정하고, `hosts.deny` 파일에 다른 모든 호스트를 거부할 수 있습니다. 다음은 'hosts.deny' 차단 정책 구성 예시입니다.



```
in.sshd:ALL# 모든 ssh 연결 차단
in.sshd:218.64.87.0/255.255.255.128# 218.64.87.0--127의 ssh 차단
ALL:ALL# 모든 TCP 연결 차단
```

VNC를 사용하여 Linux 인스턴스 로그인한 후, `/etc/hosts.deny` 파일과 `/etc/hosts.allow` 파일을 확인합니다. 그리고 확인 결과에 따라 다음 처리 방법을 선택합니다.

설정 오류. 필요에 따라 수정합니다. 수정 작업은 즉시 적용됩니다.

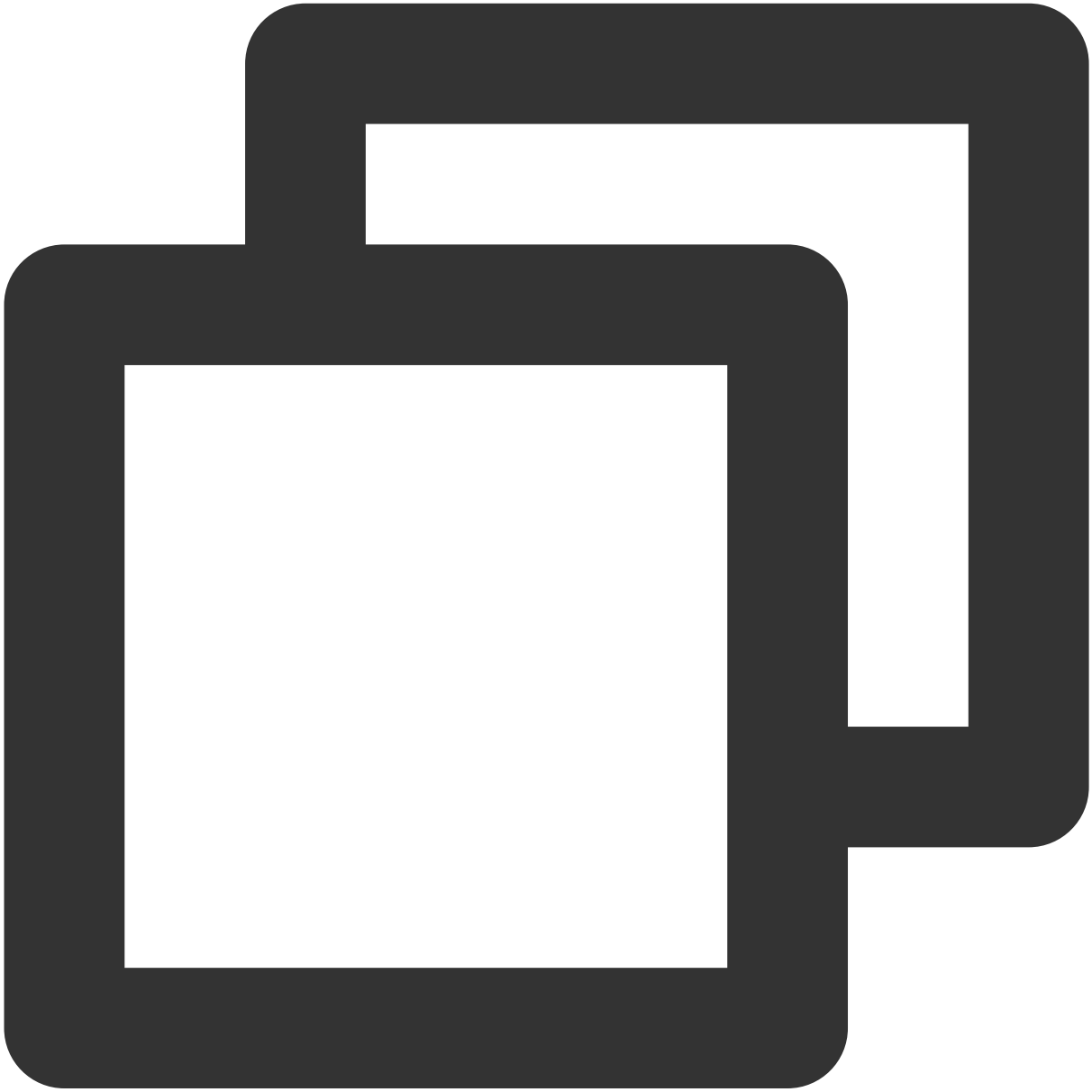
미설정 또는 설정 오류 없음. 다음 단계를 진행합니다.

설명：

액세스 정책 미설정의 경우, 기본 파일이 비어 있고 모든 연결이 허용됩니다.

iptables 방화벽 규칙 확인

Fail2ban 및 denyhost와 같은 일부 침입 방지 소프트웨어 사용으로 인해 iptables 방화벽 규칙이 수정되었는지 확인합니다. 다음 명령어를 실행하여 방화벽이 SSH 연결을 차단했는지 확인합니다.

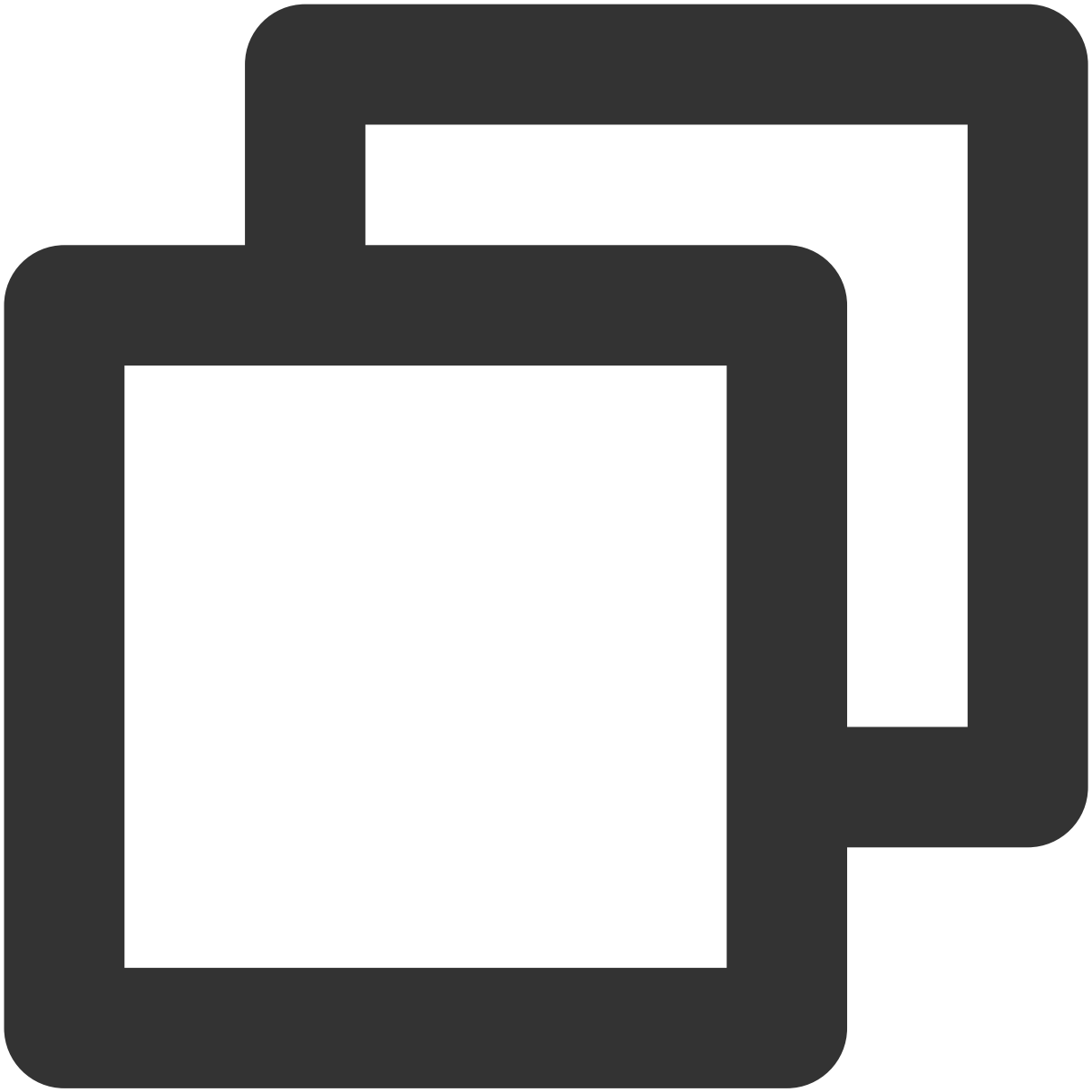


```
sudo iptables -L --line-number
```

SSH 연결이 차단된 경우, 해당 소프트웨어 화이트리스트 및 기타 관련 정책을 통해 직접 설정하시기 바랍니다.
SSH 연결이 차단되지 않은 경우 다음 단계를 진행합니다.

sshd 설정 확인 및 조정

1. 다음 명령을 실행하고 VIM 편집기를 사용하여 `sshd_config` 구성 파일로 이동합니다.



```
vim /etc/ssh/sshd_config
```

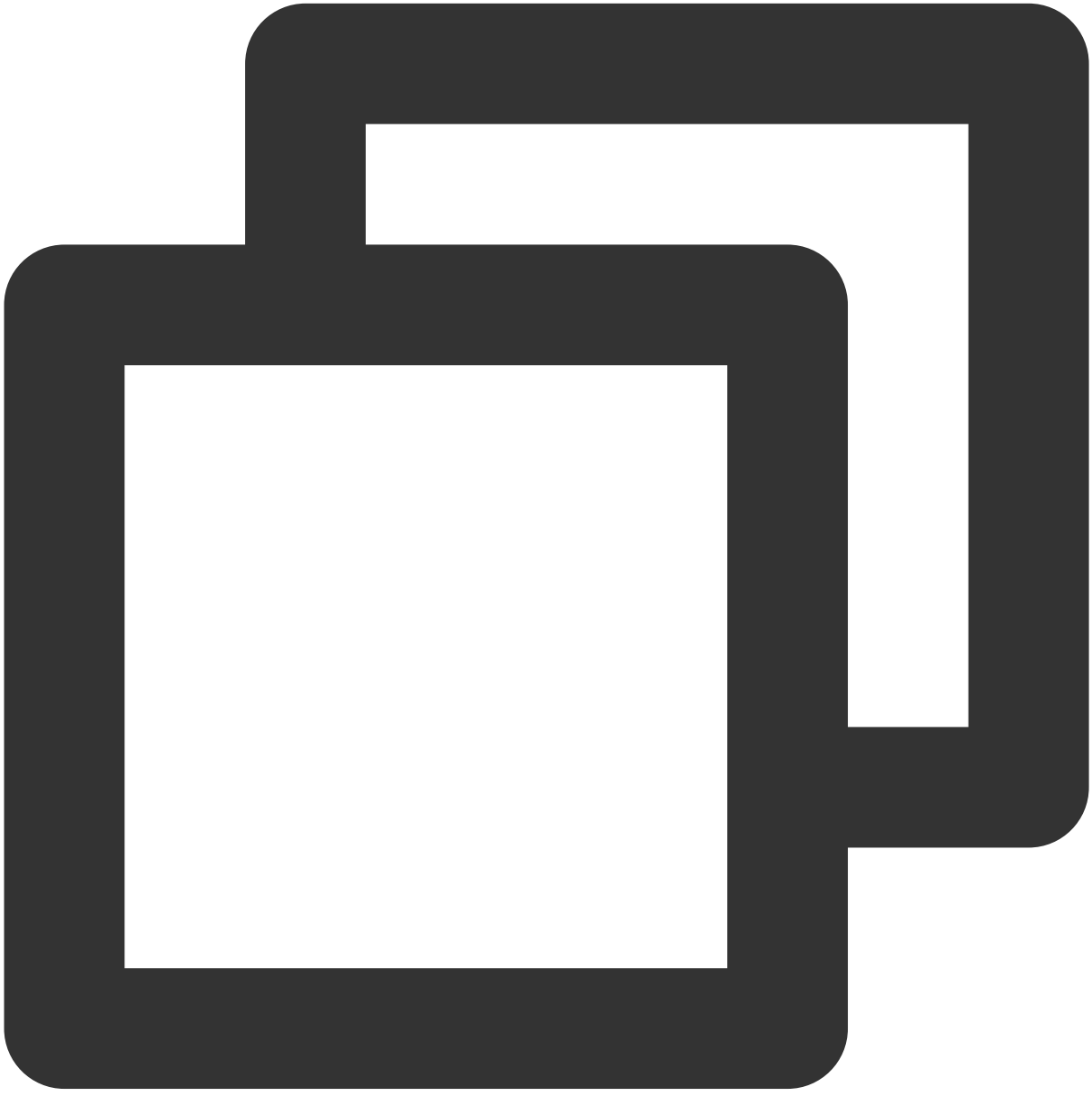
2. 'MaxStartups' 값을 조정해야 하는지 확인합니다. `sshd_config` 구성 파일에서 허용되는 최대 연결 수는 `MaxStartups` 에 의해 설정되며, 짧은 시간에 더 많은 연결을 설정해야 하는 경우 이 값을 적절하게 조정해야 합니다.
조정이 필요한 경우 다음 단계를 참고하여 수정하십시오.

2.1.1 **i**를 눌러 편집 모드로 이동하고, 수정이 완료된 후 **Esc**를 눌러 편집 모드를 종료하고, **:wq**를 입력하여 수정 사항을 저장합니다.

설명：

MaxStartups 10:30:100은 SSH 보호 프로세스의 미인증 최대 접속 수량을 지정하는 기본 설정입니다. 10:30:100은 10번째 연결부터 연결 수가 100개에 도달할 때까지 30% 확률(증분)로 새 연결이 거부됨을 의미합니다.

3. 다음 명령어를 실행하여 sshd 서비스를 재시작합니다.



```
service sshd restart
```

조정이 필요하지 않은 경우 다음 단계를 진행합니다.

네트워크 환경 테스트

1. 개인 IP 사용 여부를 확인합니다.
사용한 경우, 공용 네트워크 IP로 전환한 후 재시도합니다.
사용하지 않은 경우, 다음 단계를 진행합니다.
2. 다른 네트워크 환경을 사용하여 연결이 정상인지 테스트합니다.
정상인 경우, 인스턴스를 재시작하고 VNC를 사용하여 인스턴스에 로그인합니다.
비정상인 경우, 테스트 결과에 따라 네트워크 환경 문제를 해결합니다.
여전히 SSH 로그인 문제가 해결되지 않으면, 시스템 커널 이상 발생 또는 기타 잠재적인 원인을 의심해볼 수 있습니다. 티켓 제출을 통해 고객센터에 연락하여 문제를 해결하시기 바랍니다.

SSH 로그인 오류 Permission denied, please try again

현상 설명

root 사용자가 SSH를 사용하여 Linux 인스턴스에 로그인할 때 “Permission denied, please try again” 이라는 오류 메시지가 나타납니다.

문제 원인

가능한 원인은 시스템의 SELinux 서비스 활성화 또는 SSH 서비스의 `PermitRootLogin` 설정 수정입니다.

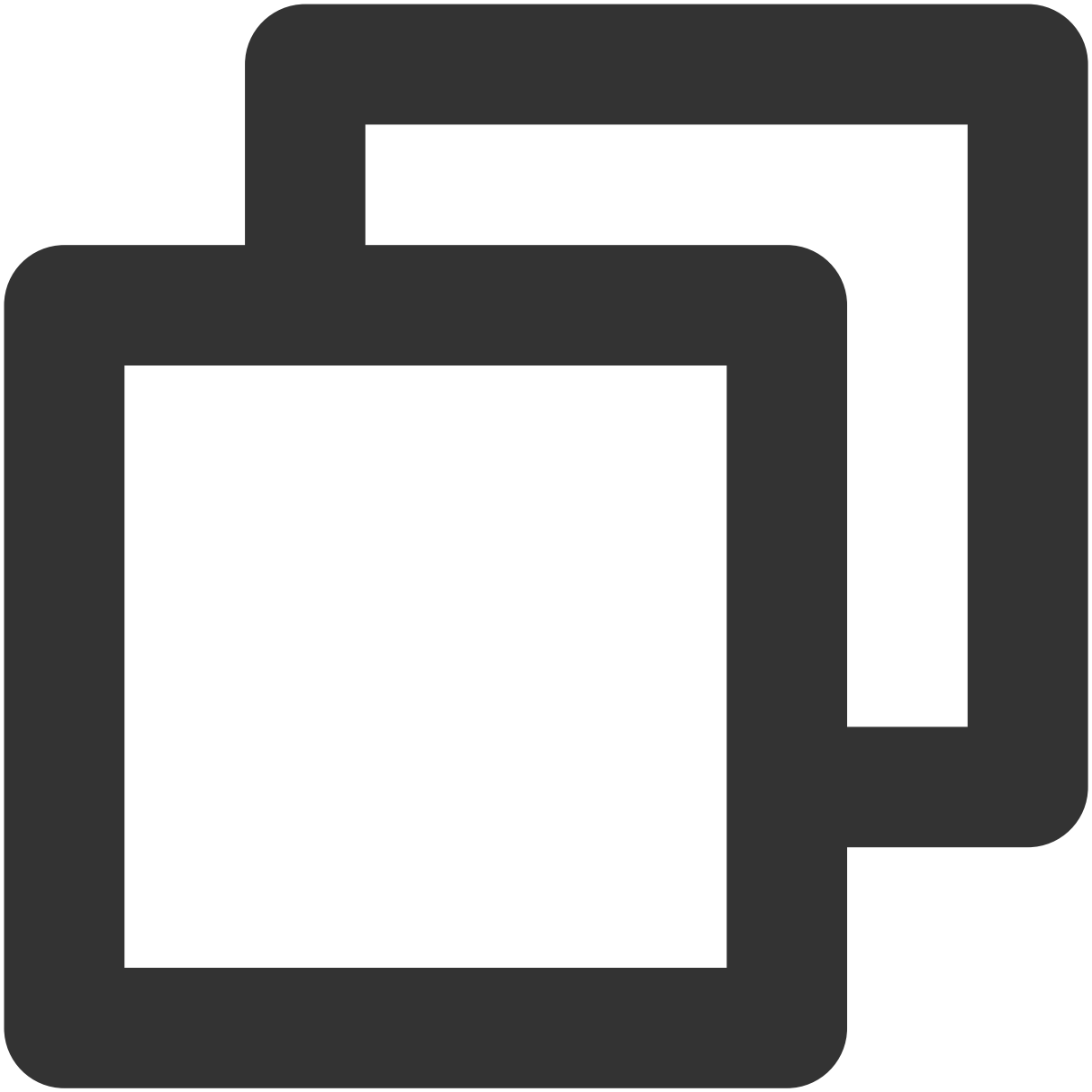
해결 방식

처리 순서를 참고하여 SELinux 서비스와 SSH 구성 파일 `sshd_config` 의 `PermitRootLogin` 매개변수를 확인하여, 문제 원인 파악 및 해결을 진행합니다.

처리 순서

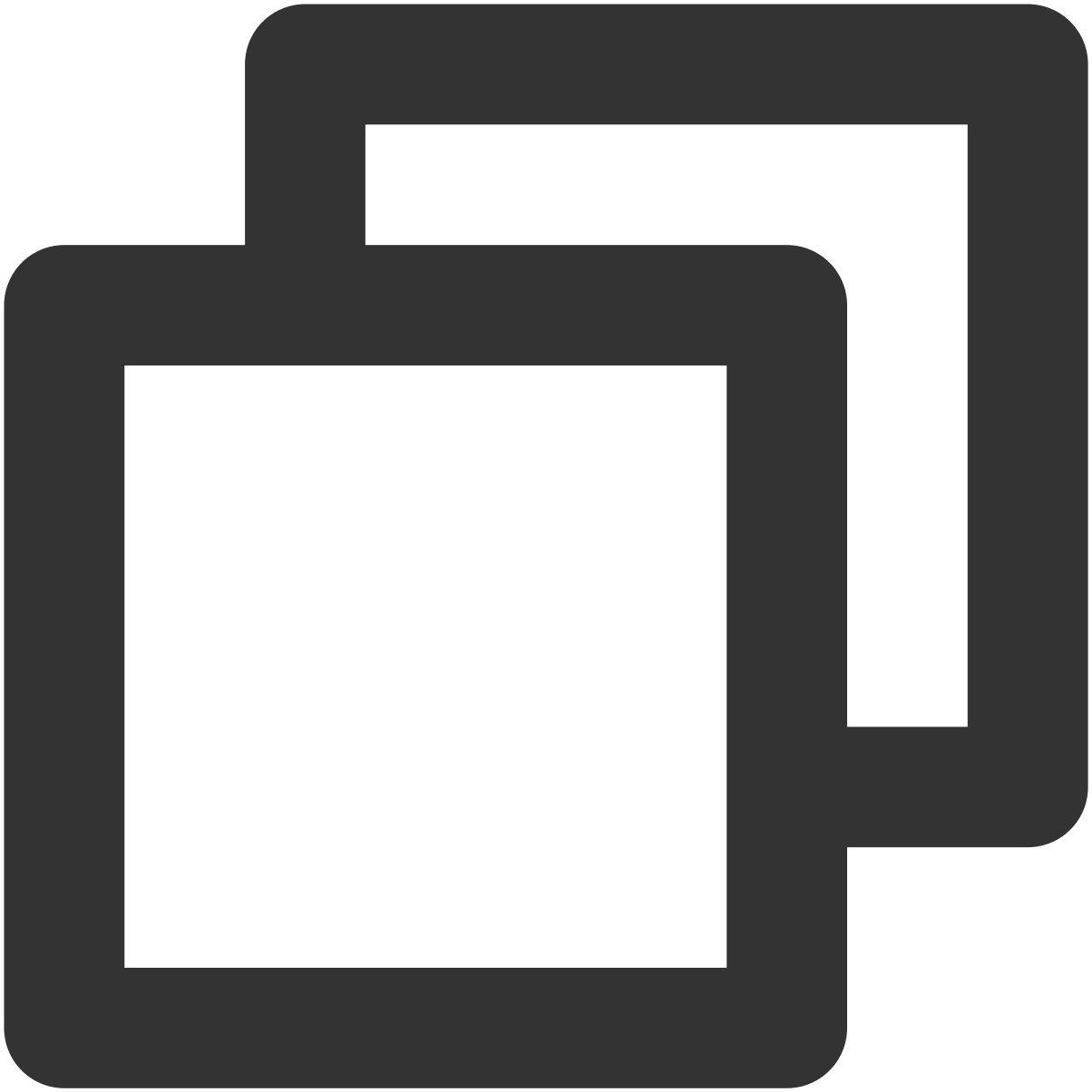
SELinux 서비스 확인 및 비활성화

1. VNC 사용하여 Linux 인스턴스에 로그인합니다.
2. 다음 명령어를 실행하여 현재 SELinux 서비스 상태를 확인합니다.



```
/usr/sbin/sestatus -v
```

반환 매개변수가 'enabled'이면 아래와 같이 활성화 상태이며, 'disabled'이면 비활성화 상태입니다.

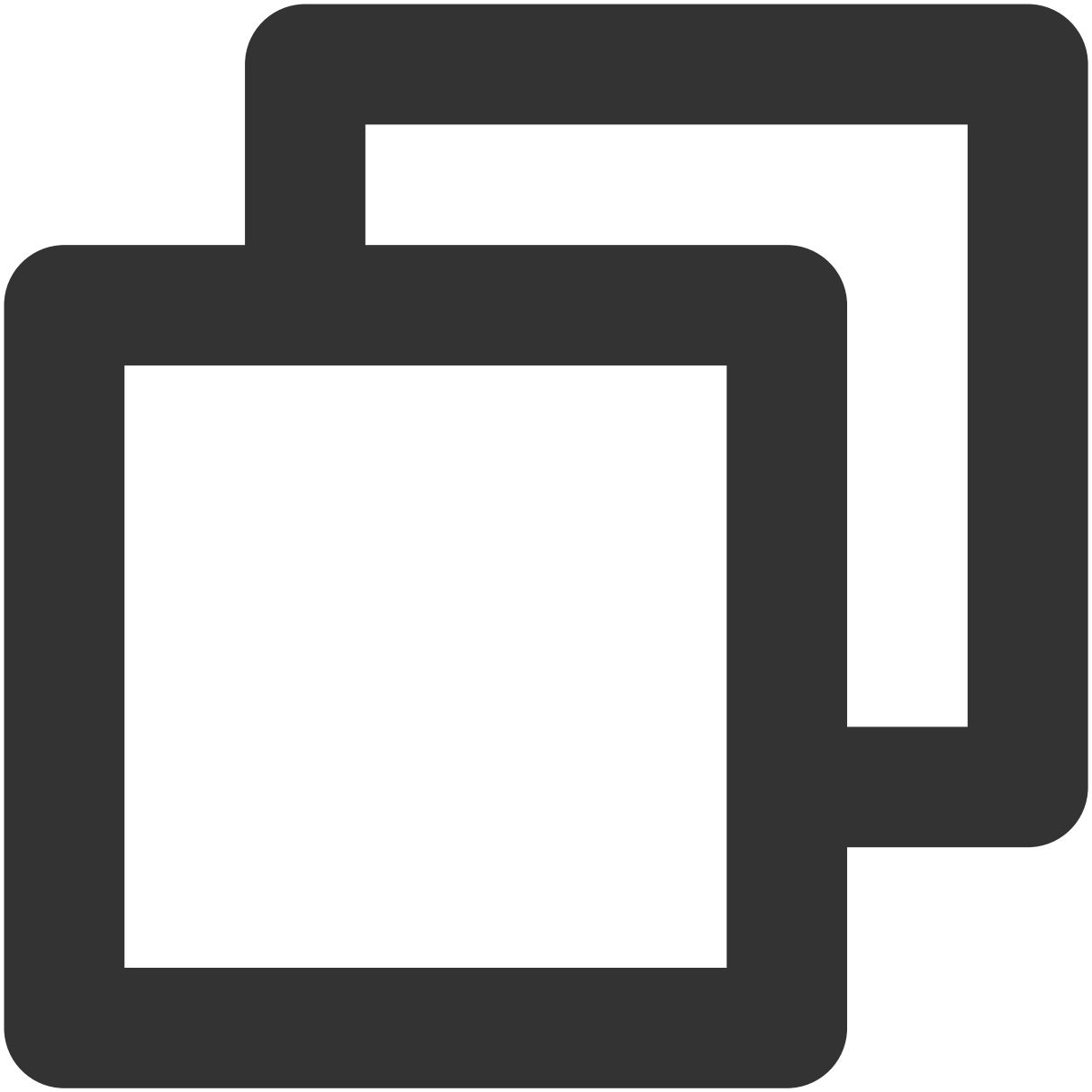


```
SELinux status:       enabled
```

3. 실제 상황에 따라 SELinux 서비스를 일시적 또는 영구적으로 비활성화할 수 있습니다.

SELinux 서비스 일시적인 비활성화

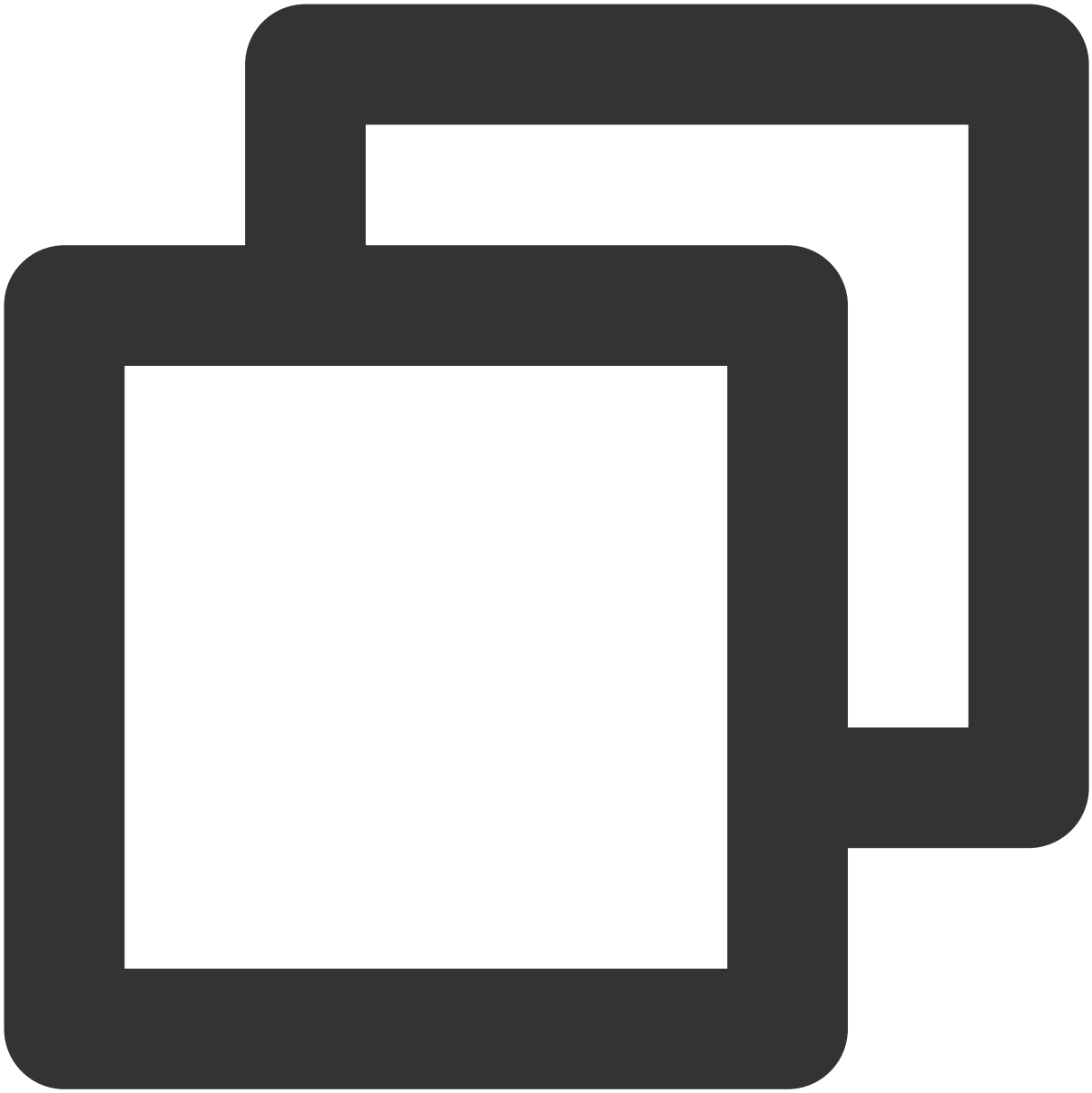
SELinux를 일시적으로 비활성화하려면 다음 명령을 실행합니다. 수정 사항은 시스템이나 인스턴스를 재시작하지 않고도 실시간으로 적용됩니다.



```
setenforce 0
```

SELinux 서비스 영구적인 비활성화

SELinux 서비스를 비활성화 하려면 다음 명령을 실행합니다.



```
sed -i 's/SELINUX=enforcing/SELINUX=disabled/' /etc/selinux/config
```

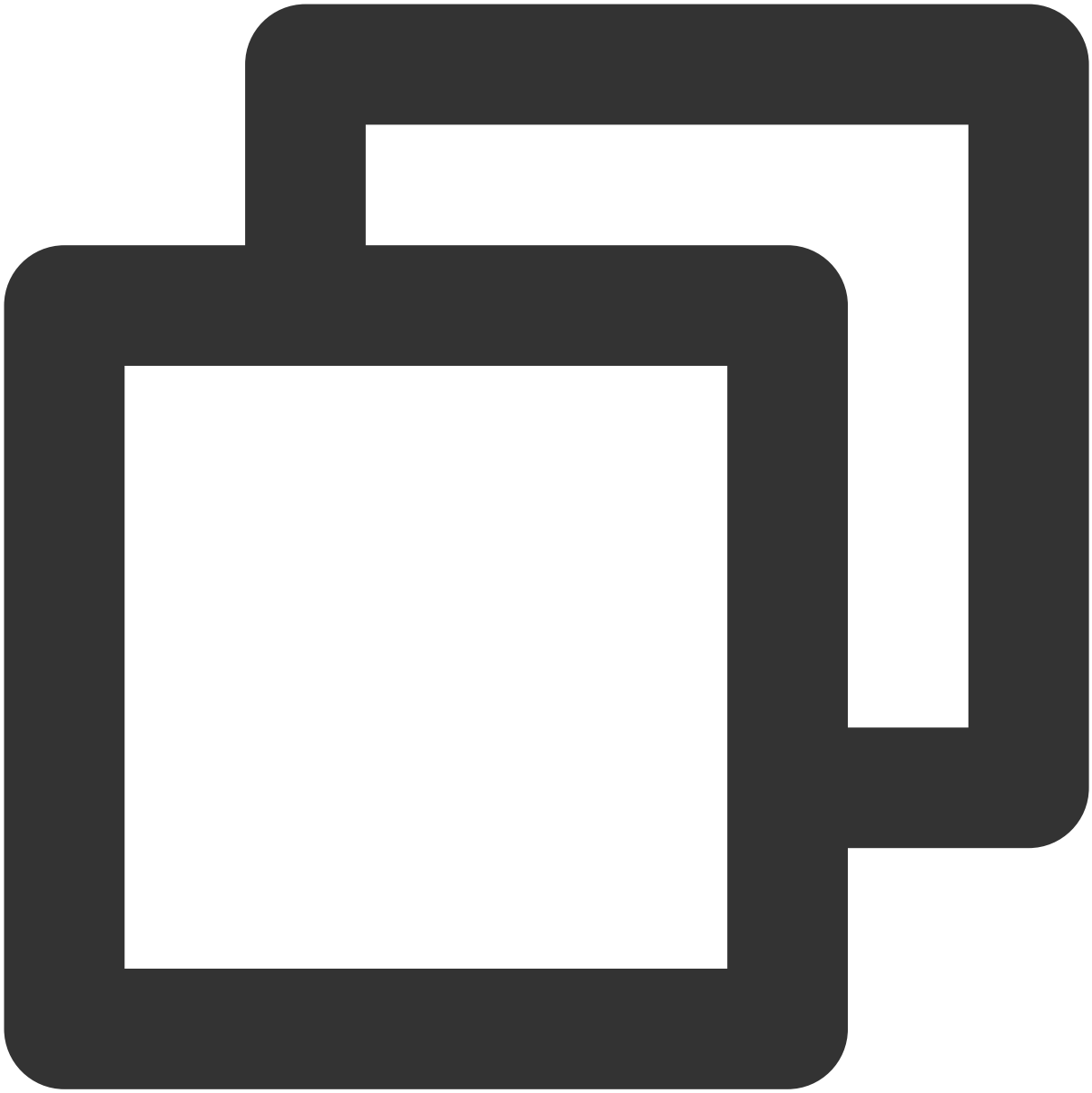
주의사항 :

이 명령은 SELinux 서비스가 enforcing 상태일 때만 적용됩니다.

명령을 실행한 후 수정 사항을 적용하려면 시스템 또는 인스턴스를 재시작해야 합니다.

sshd 설정 확인 및 조정

1. VNC 사용하여 Linux 인스턴스에 로그인합니다.
2. 다음 명령을 실행하고 VIM 편집기를 사용하여 `sshd_config` 구성 파일로 이동합니다.



```
vim /etc/ssh/sshd_config
```

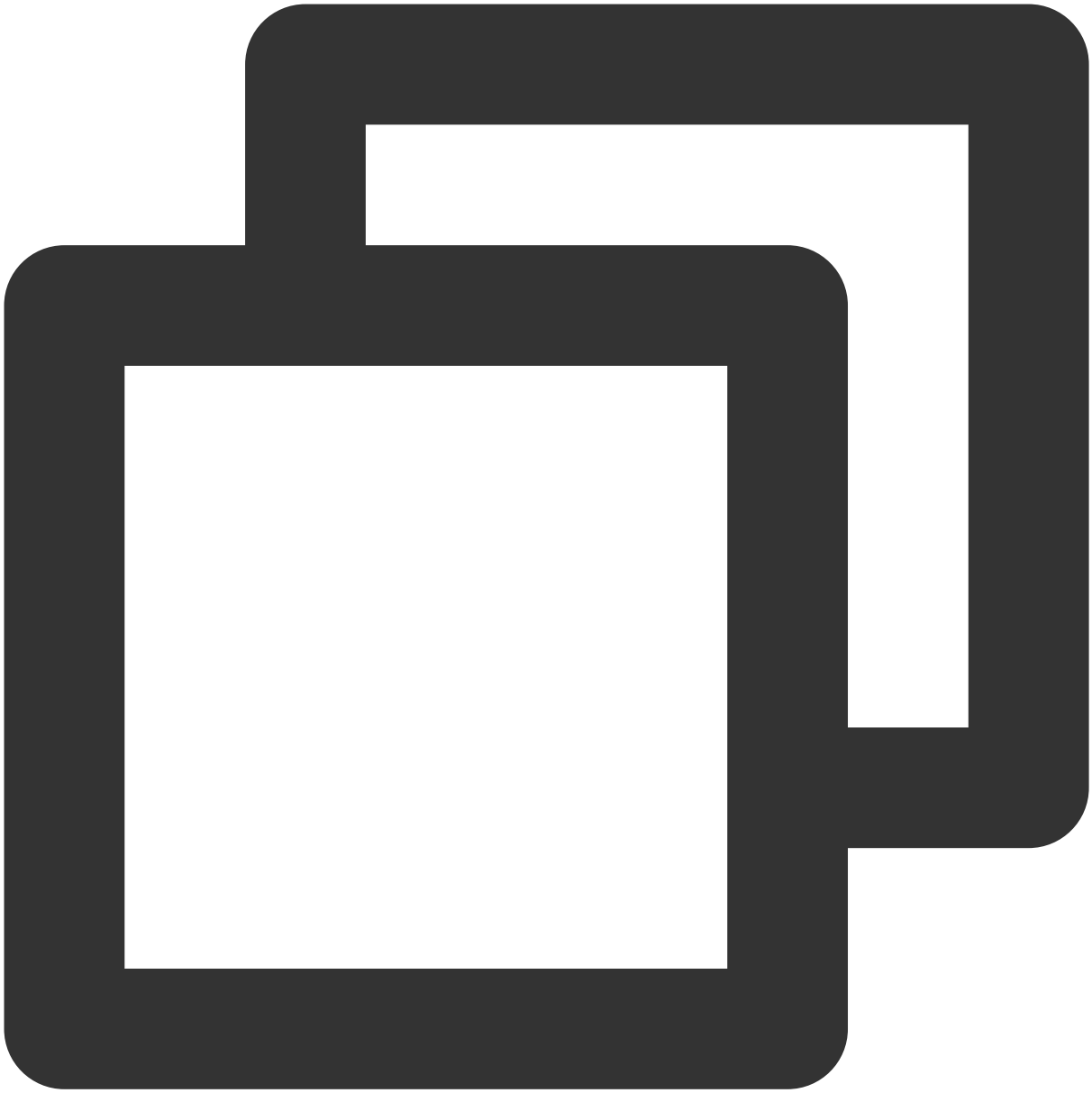
3. **i**를 눌러 편집 모드로 이동한 후, `PermitRootLogin no` 를 `PermitRootLogin yes` 로 변경합니다.

설명：

`sshd_config` 에 이 매개변수가 설정되어 있지 않으면 기본적으로 root 사용자의 로그인을 허용합니다.
이 매개변수는 SSH를 통한 root 사용자의 로그인에만 영향을 미치며, 다른 방법을 통한 root 사용자 인스턴스 로그인에는 영향을 미치지 않습니다.

4. **Esc**를 눌러 편집 모드를 종료하고 **:wq**를 입력하여 변경 사항을 저장합니다.

5. 다음 명령어를 실행하여 SSH 서비스를 재시작합니다.



```
service sshd restart
```

SSH 서비스를 재시작한 후 SSH를 사용하여 로그인할 수 있습니다. 상세 내용은 SSH를 사용하여 Linux 인스턴스에 로그인을 참고하십시오.

SSH 로그인 오류 Too many authentication failures for root

현상 설명

SSH를 사용하여 로그인할 때 비밀번호를 여러 번 입력한 후 “Too many authentication failures for root”라는 오류 메시지가 반환되고 연결이 중단됩니다.

문제 원인

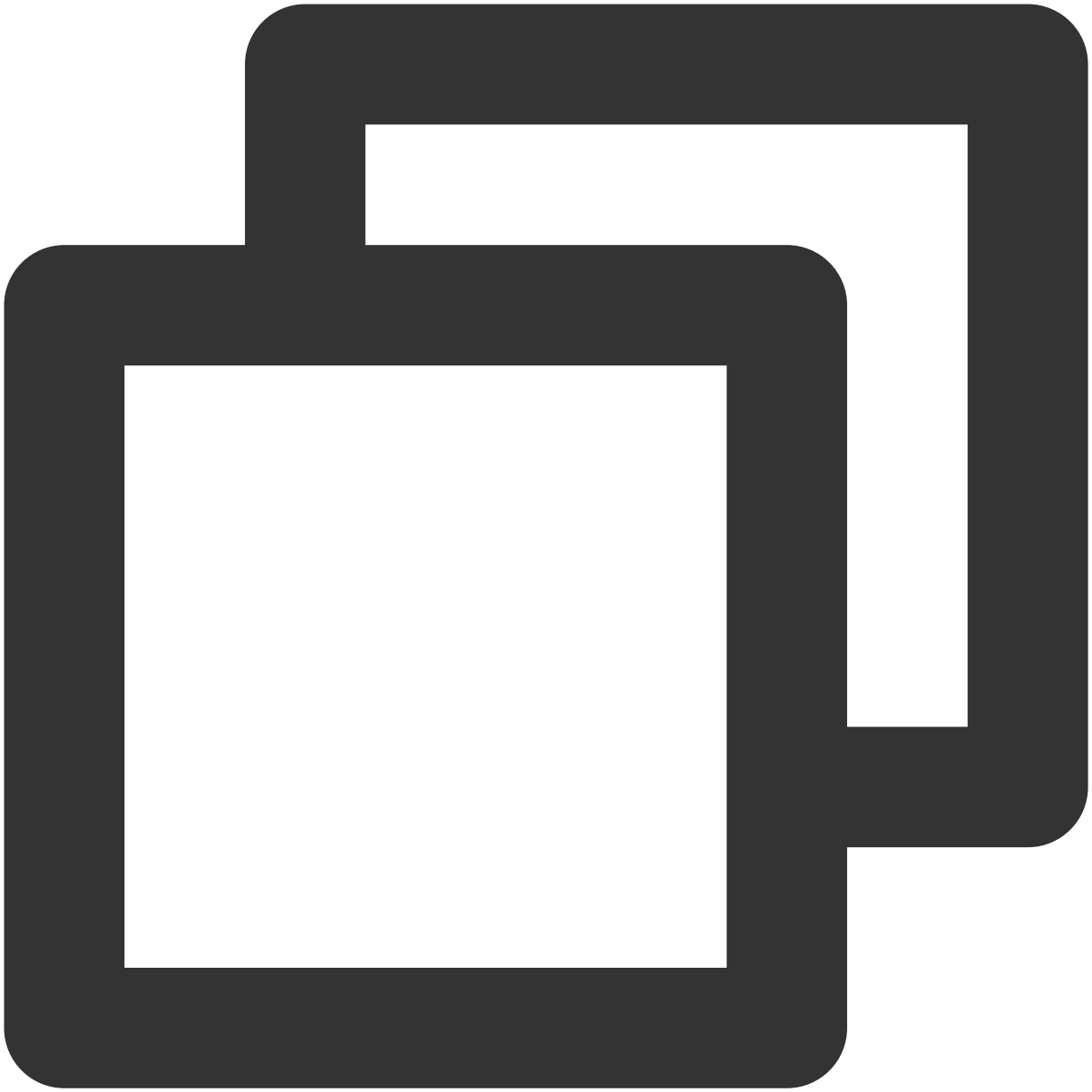
잘못된 비밀번호를 여러 번 반복하여 입력하면 SSH 서비스의 비밀번호 재설정 정책이 트리거됩니다.

해결 방식

1. 처리 순서를 참고하여 SSH 구성 파일 `sshd_config` 로 이동합니다.
2. SSH 서비스 비밀번호 재설정 정책의 'MaxAuthTries' 매개변수 설정을 확인 및 수정하고 SSH 서비스를 다시 시작합니다.

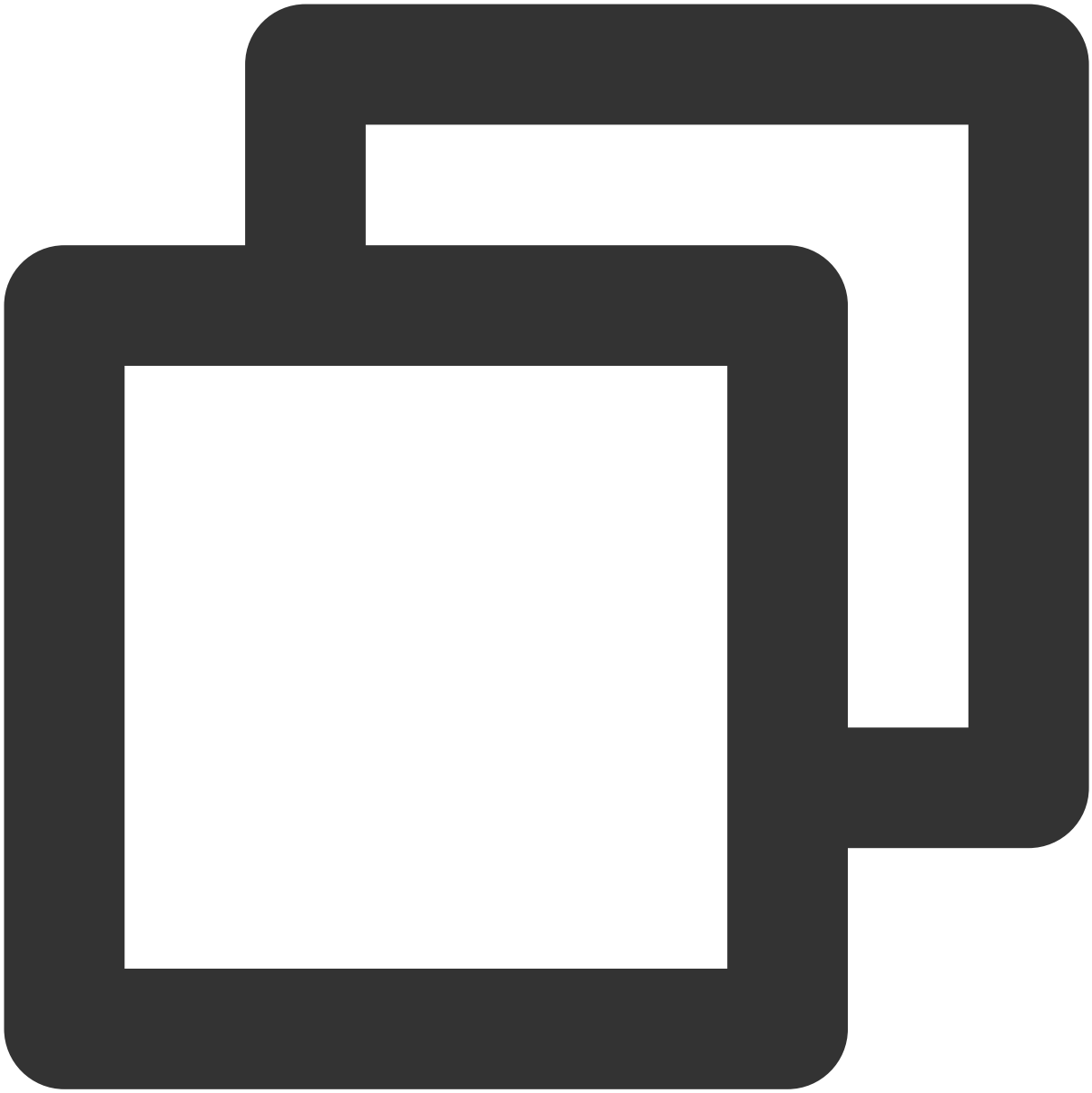
처리 순서

1. VNC 사용하여 Linux 인스턴스에 로그인합니다.
2. 다음 명령을 실행하고 VIM 편집기를 사용하여 `sshd_config` 구성 파일로 이동합니다.



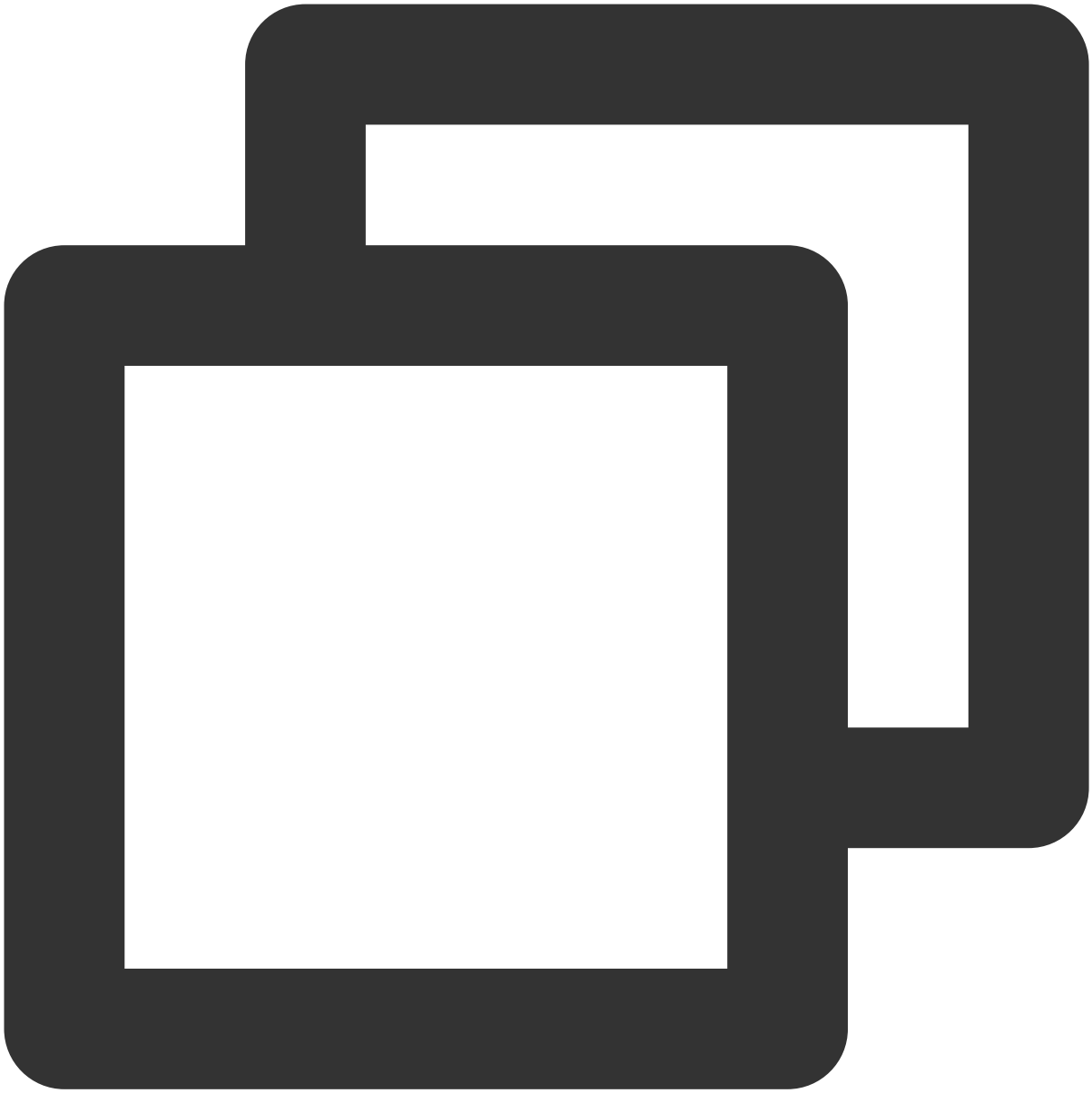
```
vim /etc/ssh/sshd_config
```

3. 다음과 유사한 설정이 포함되어 있는지 확인합니다.



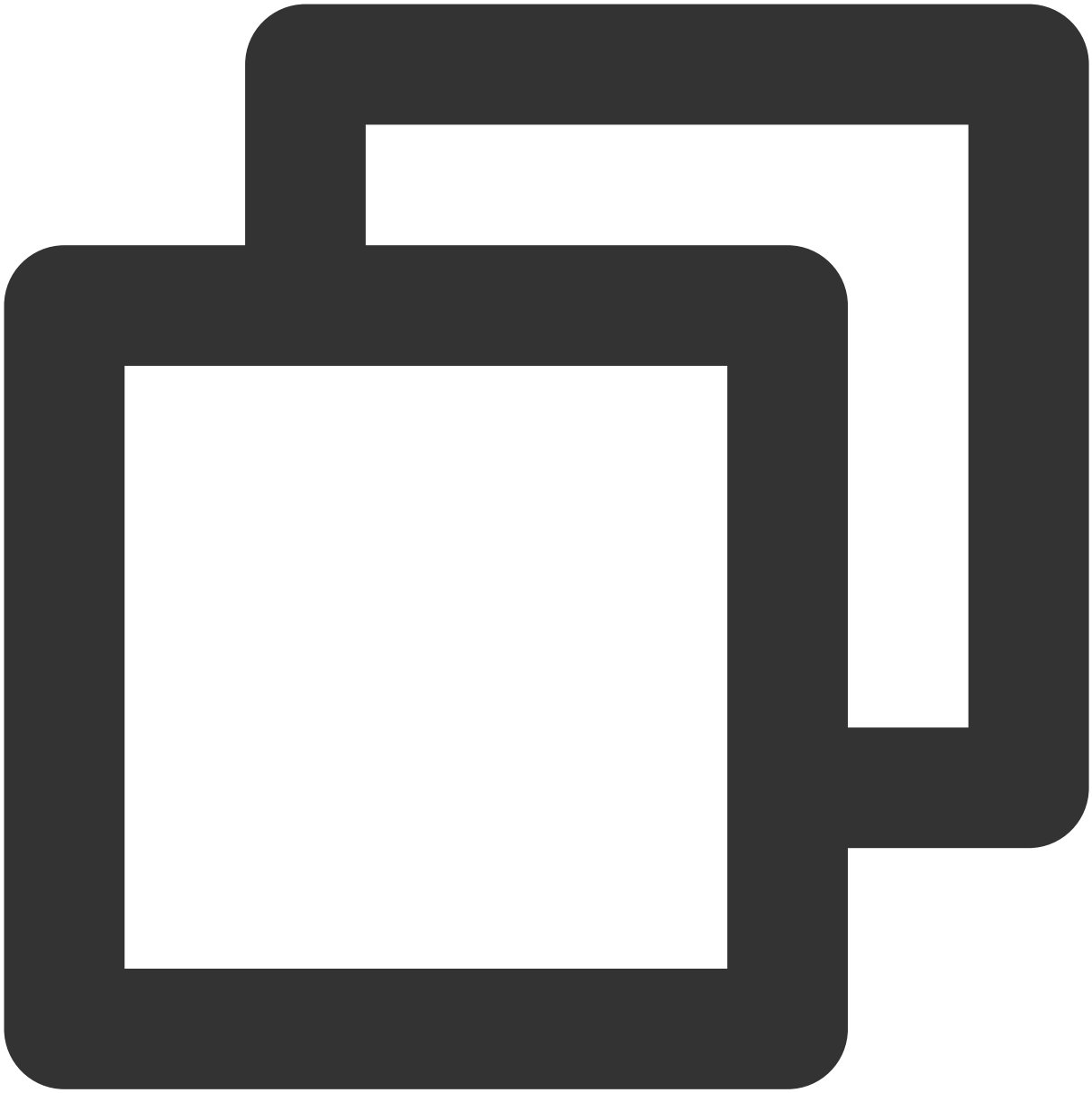
```
MaxAuthTries 5
```

설명：
이 매개변수는 기본적으로 활성화되어 있지 않으며 사용자가 SSH를 사용하여 로그인할 때마다 잘못된 암호를 연속 입력할 수 있는 횟수를 제한하는 데 사용됩니다. 횟수를 초과하면 SSH 연결이 끊어지고 관련 오류 메시지가 표시됩니다. 그러나 해당 계정은 잠기지 않으며 SSH를 사용하여 다시 로그인할 수 있습니다.
실제 상황에 따라 설정 수정 여부를 판단하고 수정이 필요한 경우 `sshd_config` 구성 파일을 백업해 두는 것을 권장합니다.
4. **i**를 눌러 편집 모드로 이동한 후, 다음 설정을 수정하거나, 행 시작 부분에 `#` 을 추가하여 주석을 진행합니다.



```
MaxAuthTries <잘못된 비밀번호를 입력할 수 있는 횟수>
```

5. **Esc**를 눌러 편집 모드를 종료하고 **:wq**를 입력하여 변경 사항을 저장합니다.
6. 다음 명령어를 실행하여 SSH 서비스를 재시작합니다.



```
service sshd restart
```

SSH 서비스를 재시작한 후 SSH를 사용하여 로그인할 수 있습니다. 상세 내용은 SSH를 사용하여 Linux 인스턴스에 로그인을 참고하십시오.

SSH 실행 오류 error while loading shared libraries

현상 설명

Linux 인스턴스가 SSH 서비스를 실행할 때, secure 로그 파일에서 또는 직접적으로 다음과 유사한 오류 메시지가 반환됩니다.

“error while loading shared libraries: libcrypto.so.10: cannot open shared object file: No such file or directory”
“PAM unable to dlopen(/usr/lib64/security/pam_tally.so): /usr/lib64/security/pam_tally.so: cannot open shared object file: No such file or directory”

문제 원인

가능한 원인은 SSH 서비스 실행 관련 시스템 라이브러리 파일 손실이나 권한 설정 등의 예외 발생입니다.

해결 방식

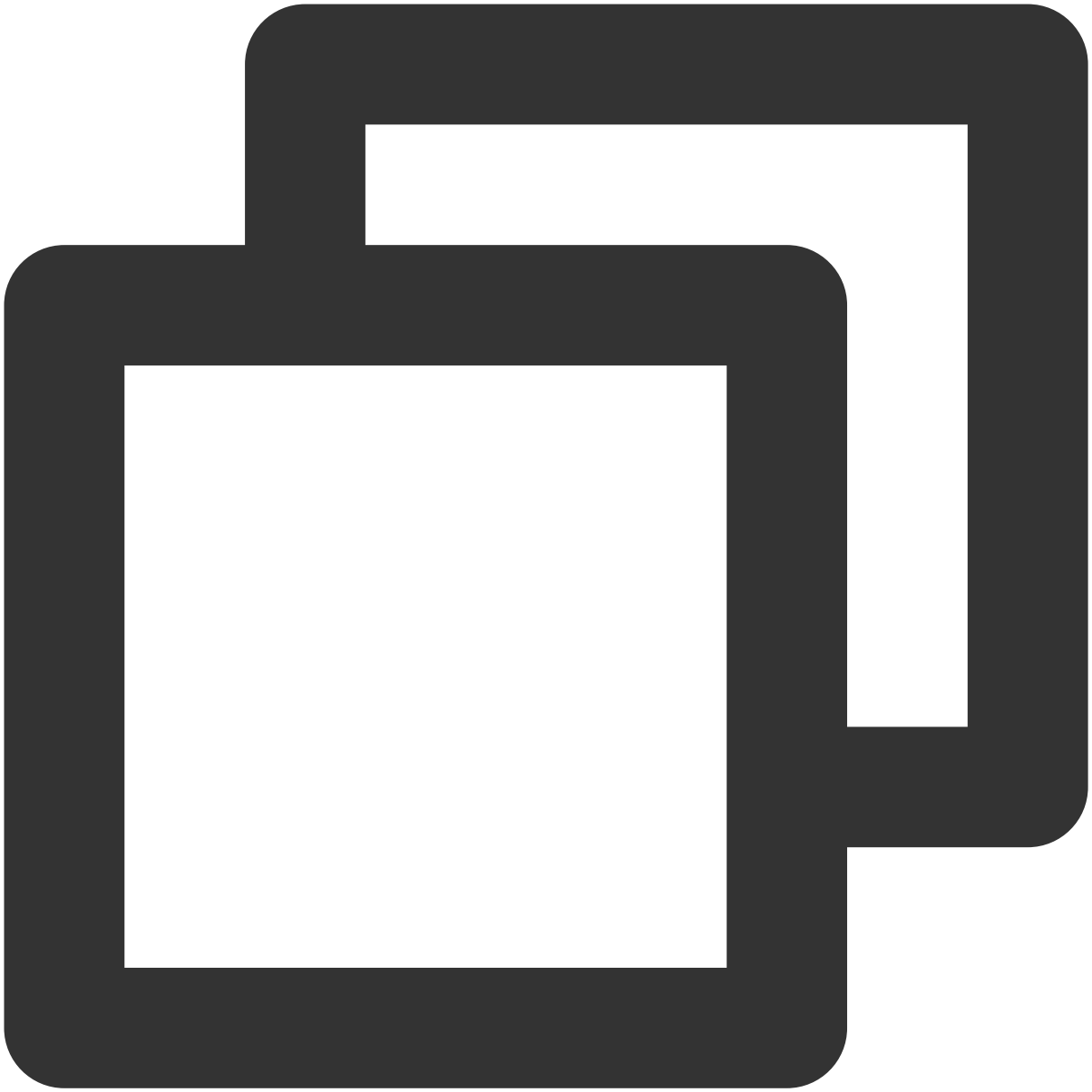
처리 순서를 참고하여 시스템 라이브러리 파일을 확인하고 복구합니다.

처리 순서

설명：
이 글은 libcrypto.so.10 라이브러리 파일 예외 해결을 예로 들어 설명하며, 다른 라이브러리 파일 예외 해결도 이와 유사하므로 실제 상황에 따라 작업하시기 바랍니다.

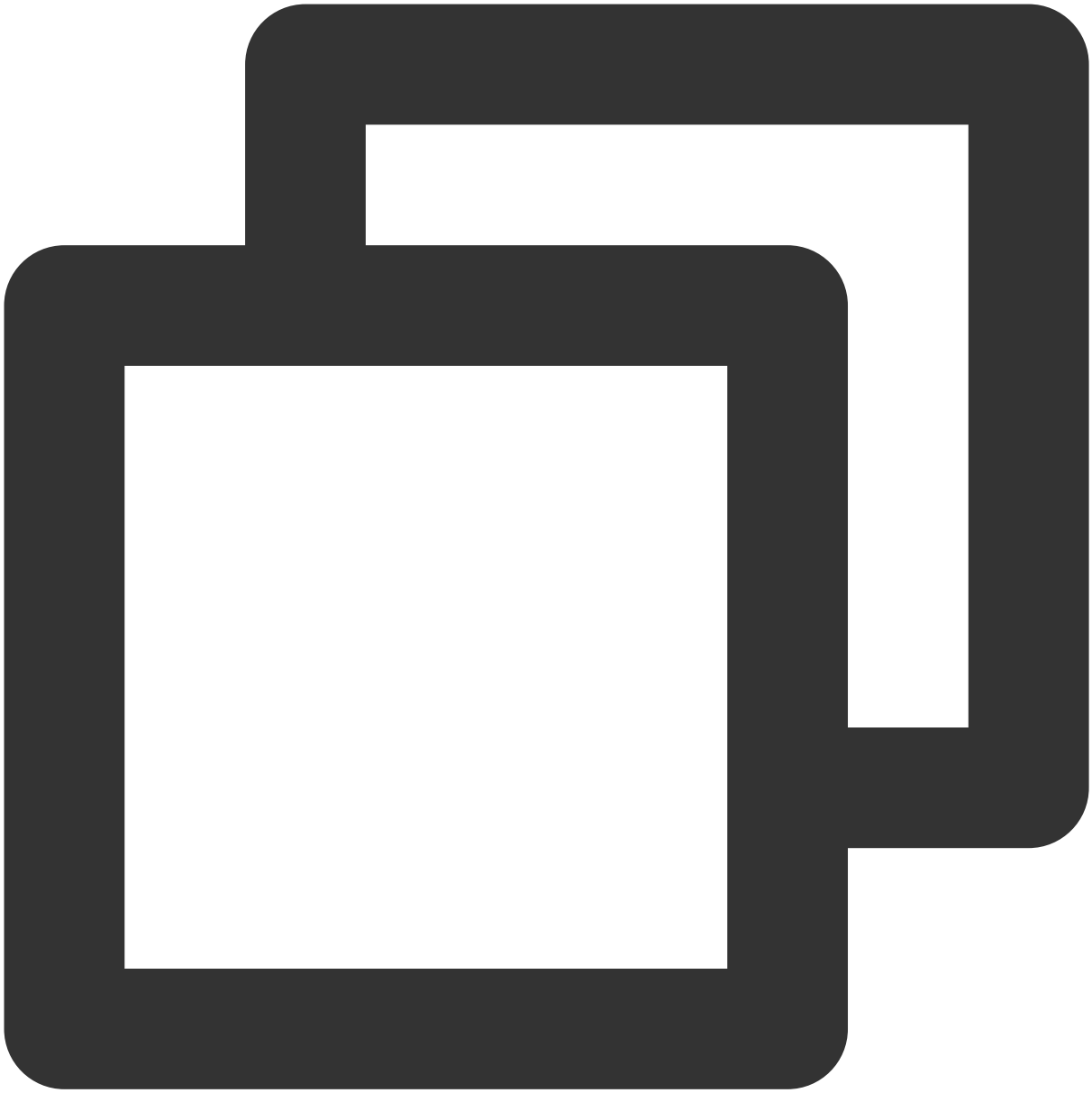
라이브러리 파일 정보 가져오기

1. VNC 사용하여 Linux 인스턴스에 로그인합니다.
2. 다음 명령어를 실행하여 libcrypto.so.10 라이브러리 파일 정보를 확인합니다.



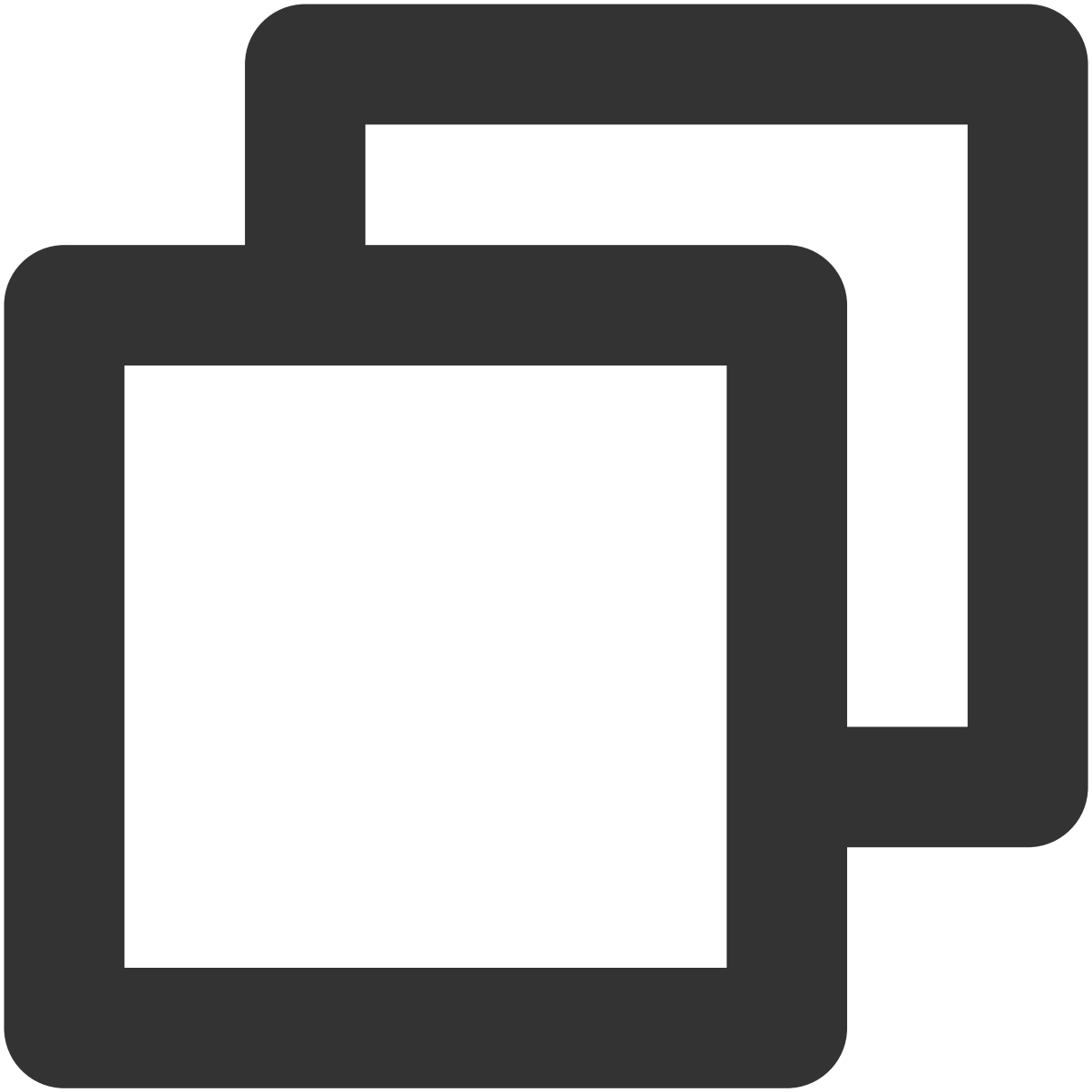
```
ll /usr/lib64/libcrypto.so.10
```

다음과 유사한 정보가 반환되는 경우, `/usr/lib64/libcrypto.so.10` 가 `libcrypto.so.1.0.2k` 라이브러리 파일의 소프트 링크임을 나타냅니다.



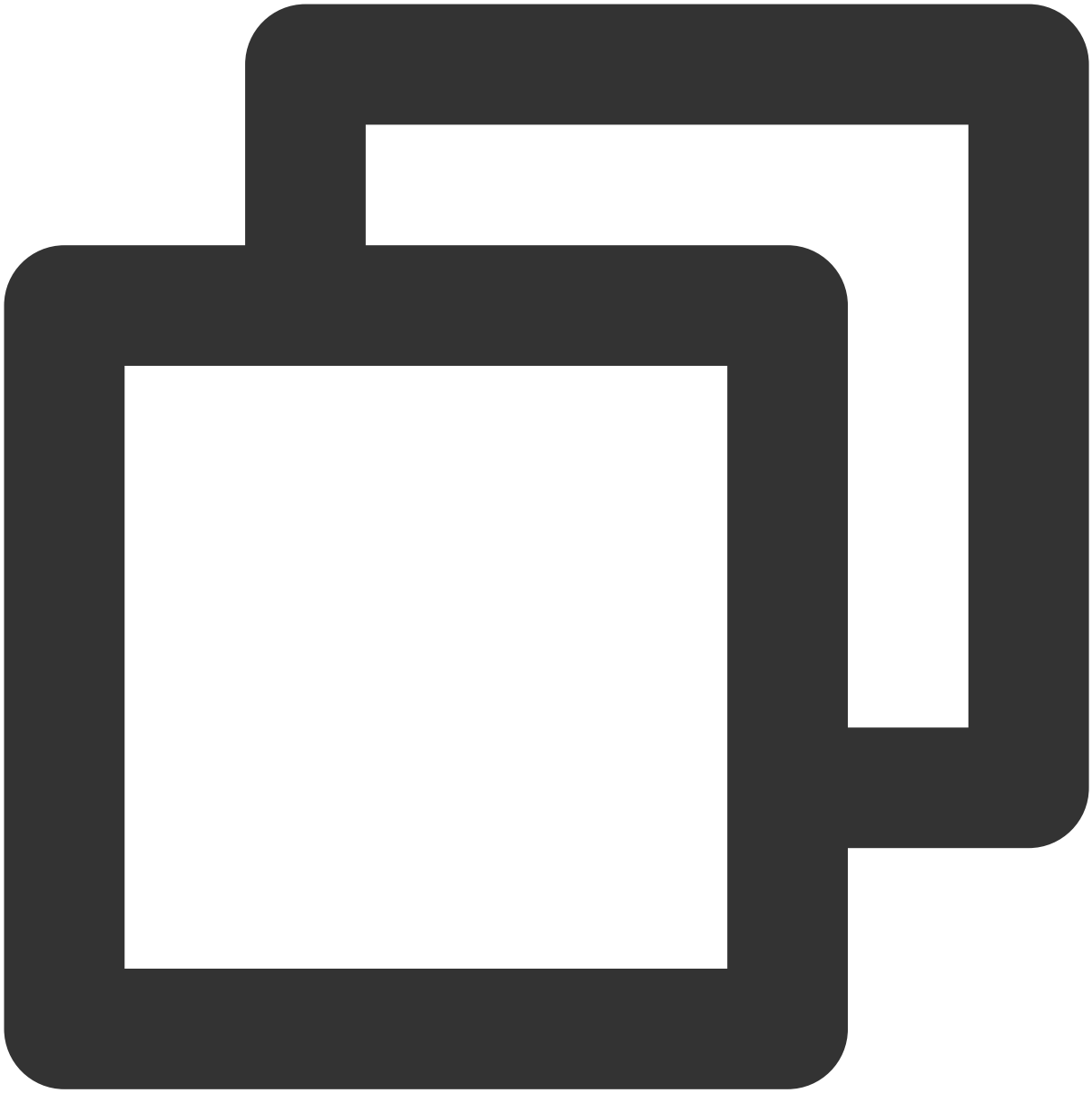
```
lrwxrwxrwx 1 root root 19 Jan 19  2021 /usr/lib64/libcrypto.so.10 -> libcrypto.so.1
```

3. 다음 명령어를 실행하여 `libcrypto.so.1.0.2k` 라이브러리 파일 정보를 확인합니다.



```
ll /usr/lib64/libcrypto.so.1.0.2k
```

다음과 유사한 정보가 반환됩니다.



```
-rwxr-xr-x 1 root root 2520768 Dec 17  2020 /usr/lib64/libcrypto.so.1.0.2k
```

4. 일반 라이브러리 파일의 경로, 권한, 그룹 정보를 기록하고 다음과 같이 처리합니다.

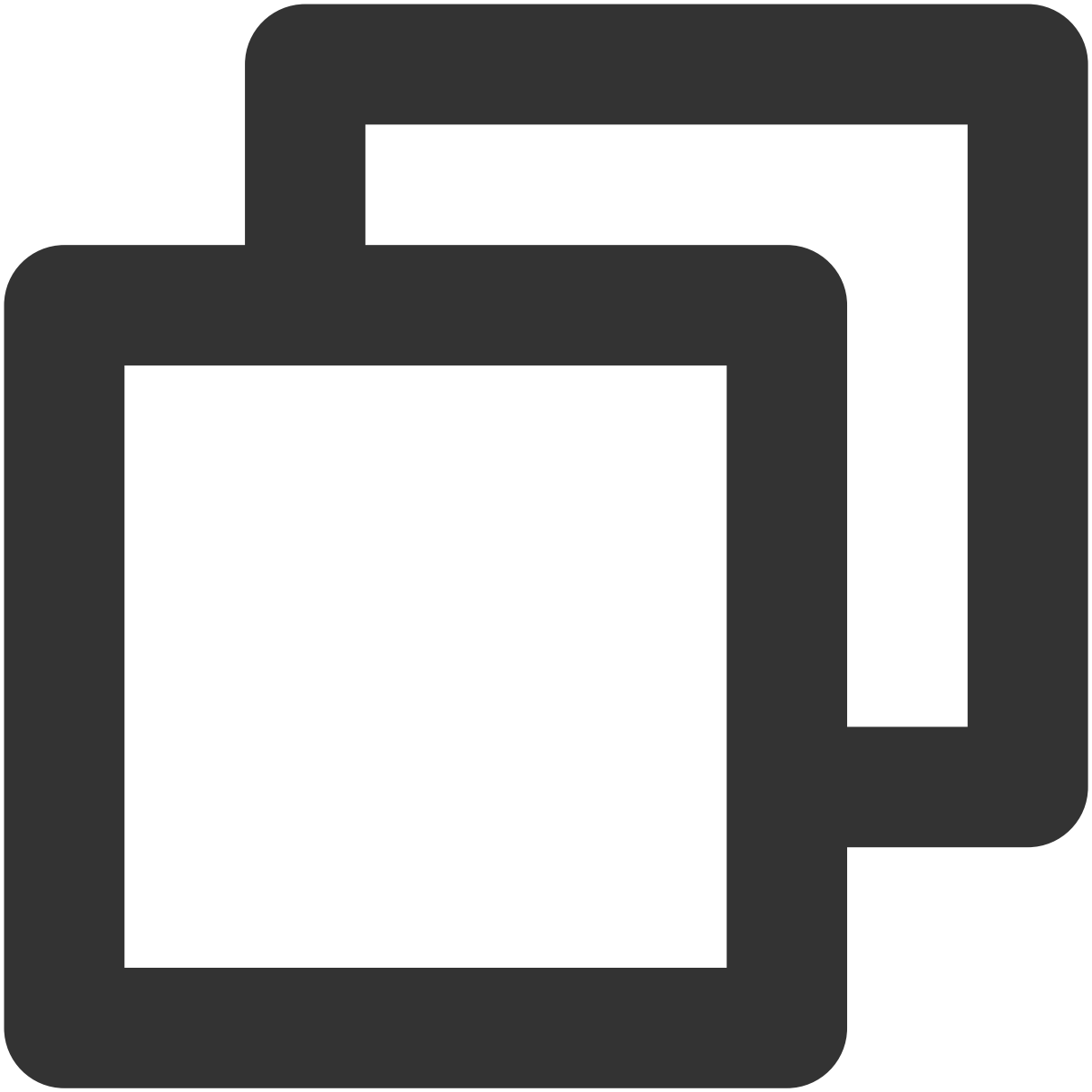
라이브러리 파일 찾기 및 바꾸기

외부 파일 업로드

스냅샷 롤백을 통한 복구

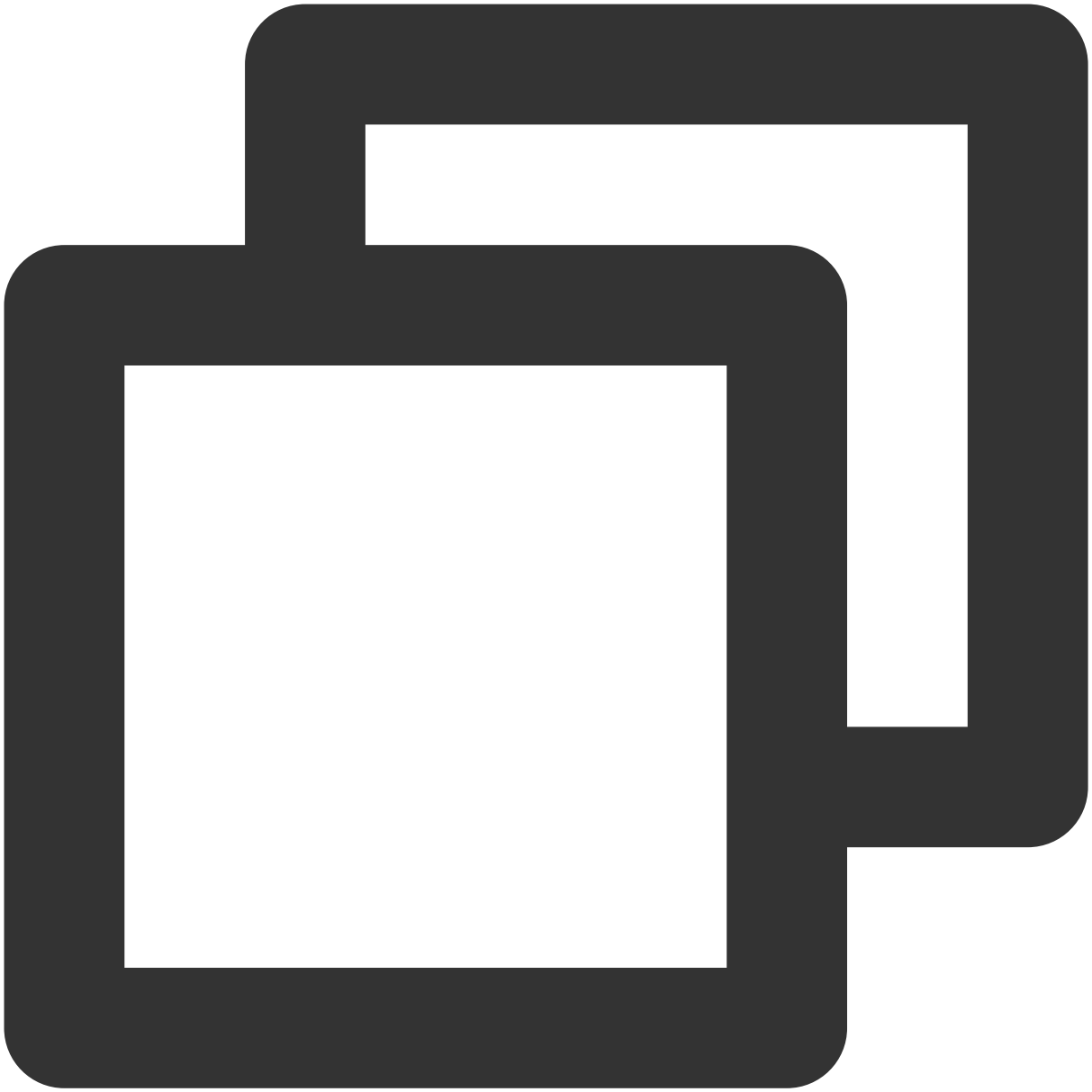
라이브러리 파일 찾기 및 바꾸기

1. 다음 명령어를 실행하여 `libcrypto.so.1.0.2k` 파일을 찾습니다.



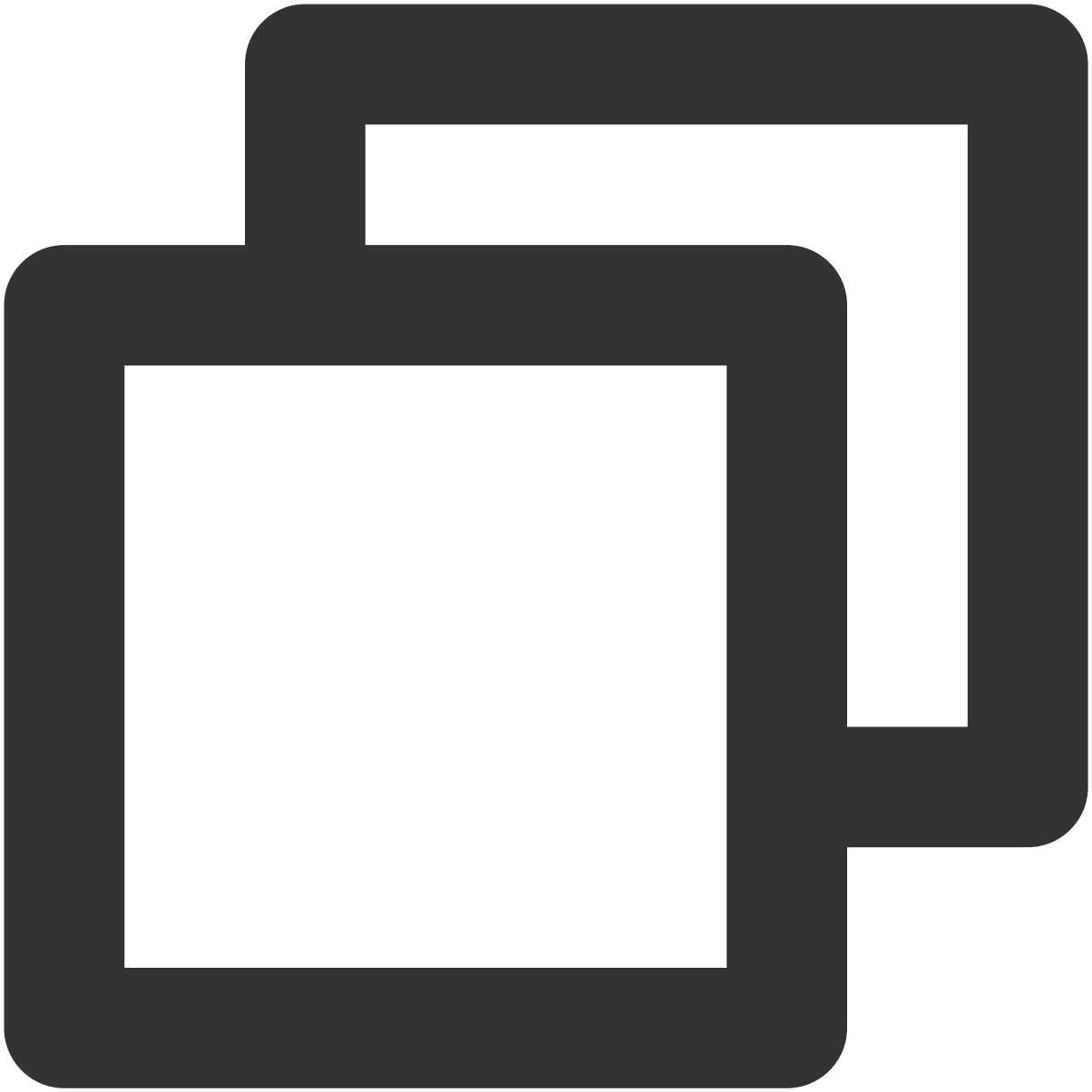
```
find / -name libcrypto.so.1.0.2k
```

2. 반환된 결과에 따라 다음 명령을 실행하여 라이브러리 파일을 일반 디렉터리에 복사합니다.

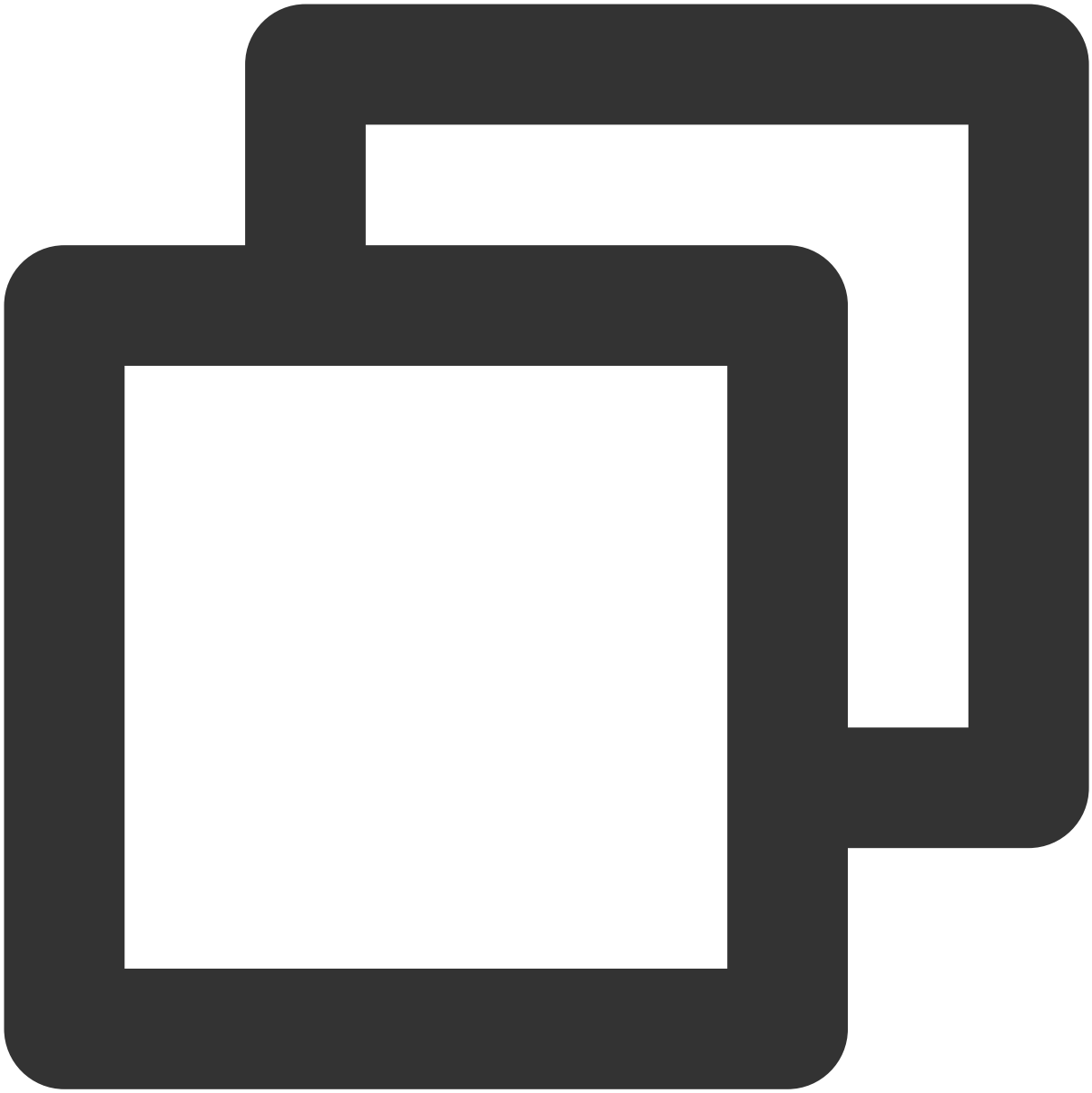


```
cp <1단계에서 얻은 라이브러리 파일의 절대 경로> /usr/lib64/libcrypto.so.1.0.2k
```

3. 다음 명령어를 순서대로 실행하여 파일 권한, 소유자, 그룹을 수정합니다.

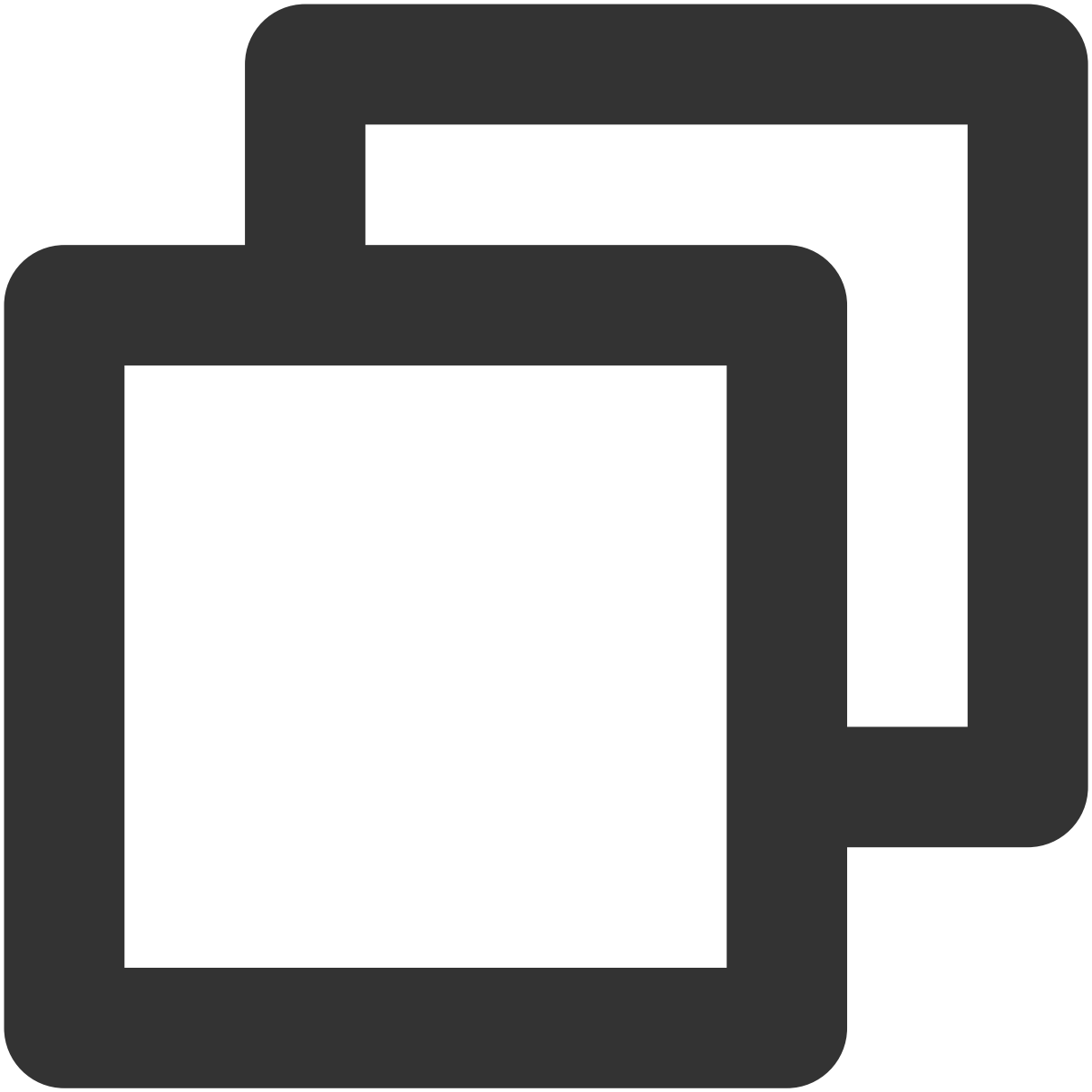


```
chmod 755 /usr/lib64/libcrypto.so.1.0.2k
```



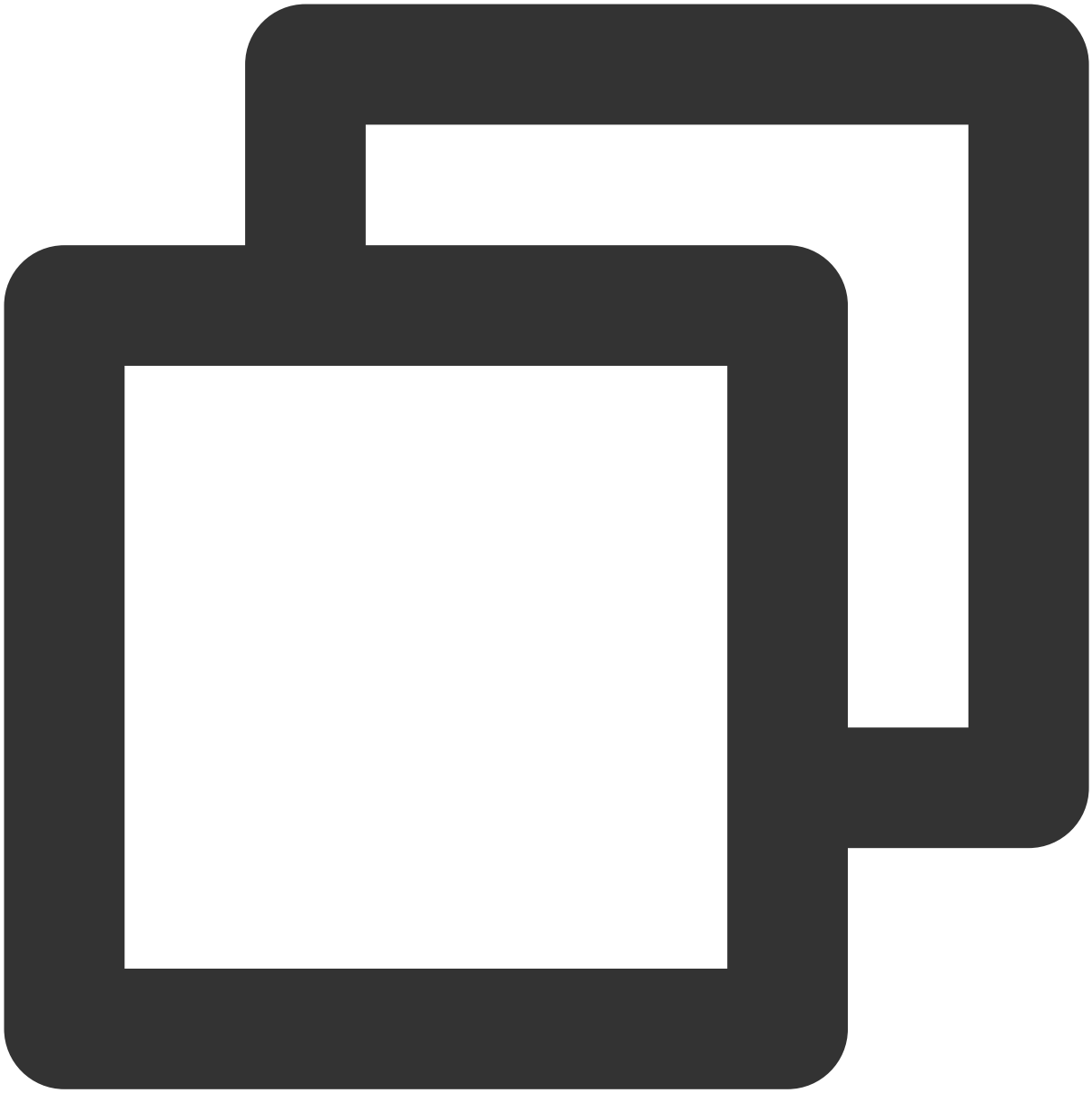
```
chown root:root /usr/lib64/libcrypto.so.1.0.2k
```

4. 다음 명령을 실행하여 소프트 링크를 생성합니다.



```
ln -s /usr/lib64/libcrypto.so.1.0.2k /usr/lib64/libcrypto.so.10
```

5. 다음 명령어를 실행하여 SSH 서비스를 실행합니다.



```
service sshd start
```

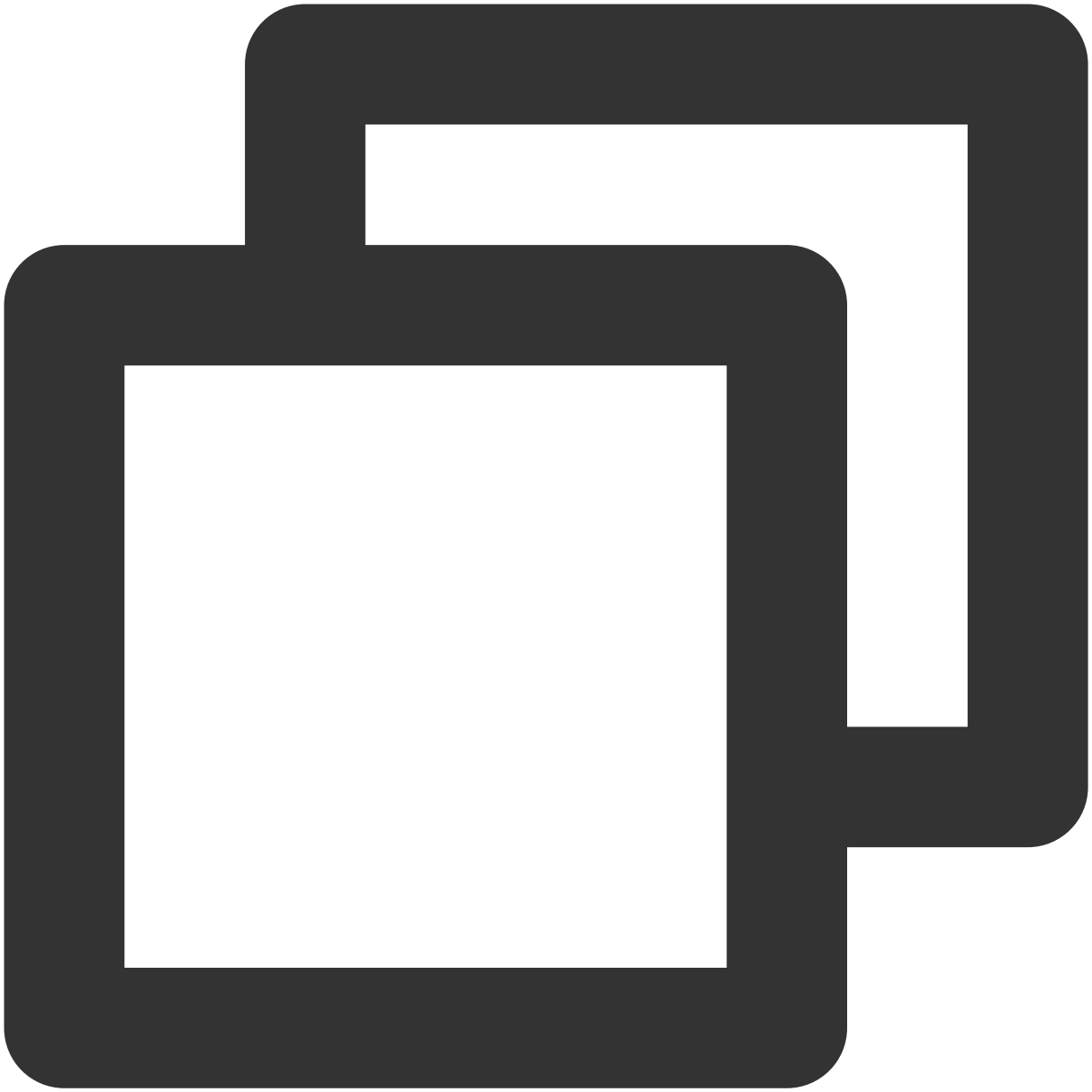
외부 파일 업로드

1. FTP 소프트웨어를 통해 다른 일반 서버의 `libcrypto.so.1.0.2k` 라이브러리 파일을 타깃 서버의 `\\tmp` 디렉터리로 업로드합니다.

설명：

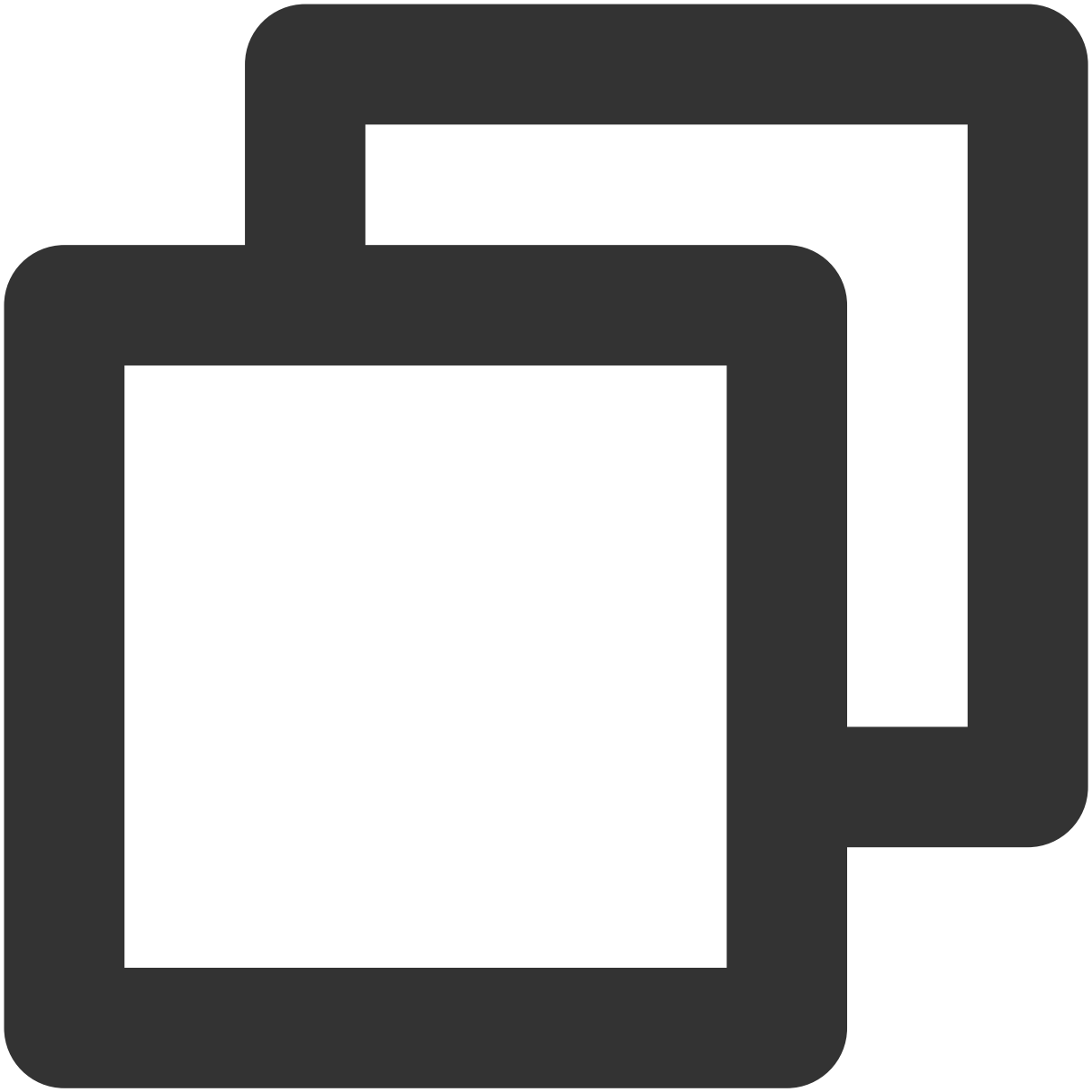
본문은 타깃 서버에 업로드된 `\\tmp` 디렉터리를 예로 들며, 실제 상황에 맞게 수정할 수 있습니다.

2. 다음 명령을 실행하여 라이브러리 파일을 일반 디렉터리에 복사합니다.

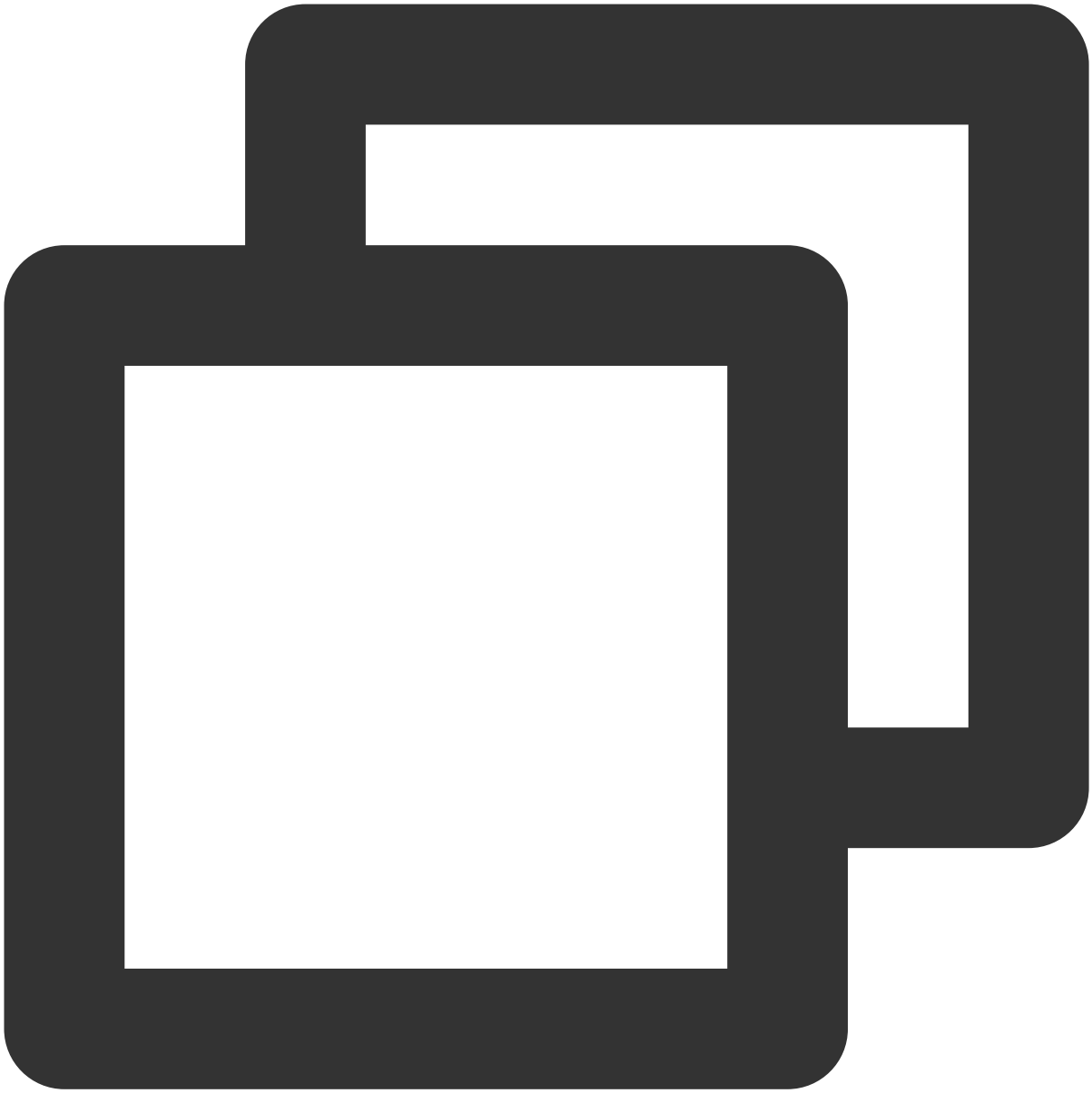


```
cp /tmp/libcrypto.so.1.0.2k /usr/lib64/libcrypto.so.1.0.2k
```

3. 다음 명령어를 순서대로 실행하여 파일 권한, 소유자, 그룹을 수정합니다.

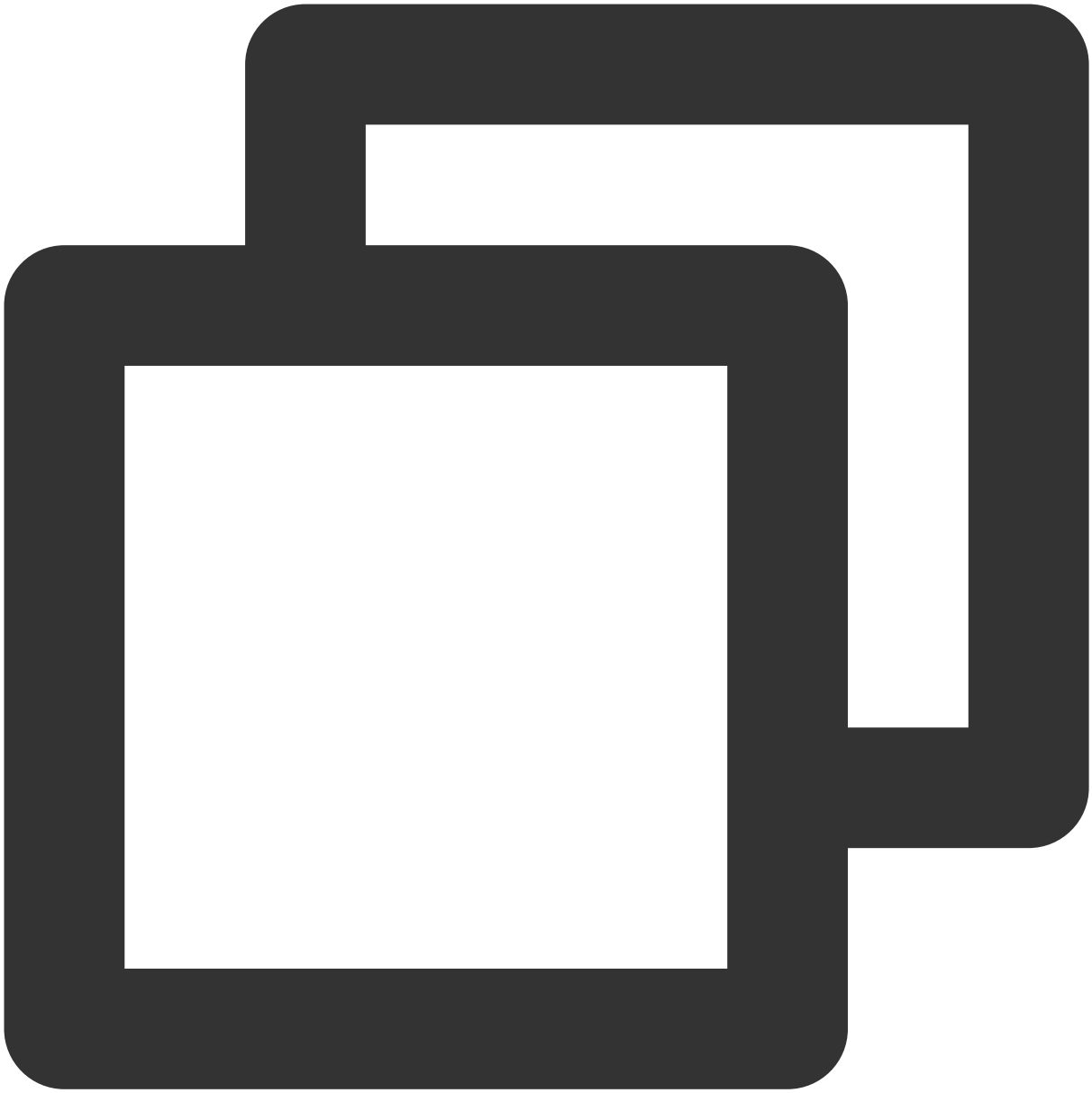


```
chmod 755 /usr/lib64/libcrypto.so.1.0.2k
```



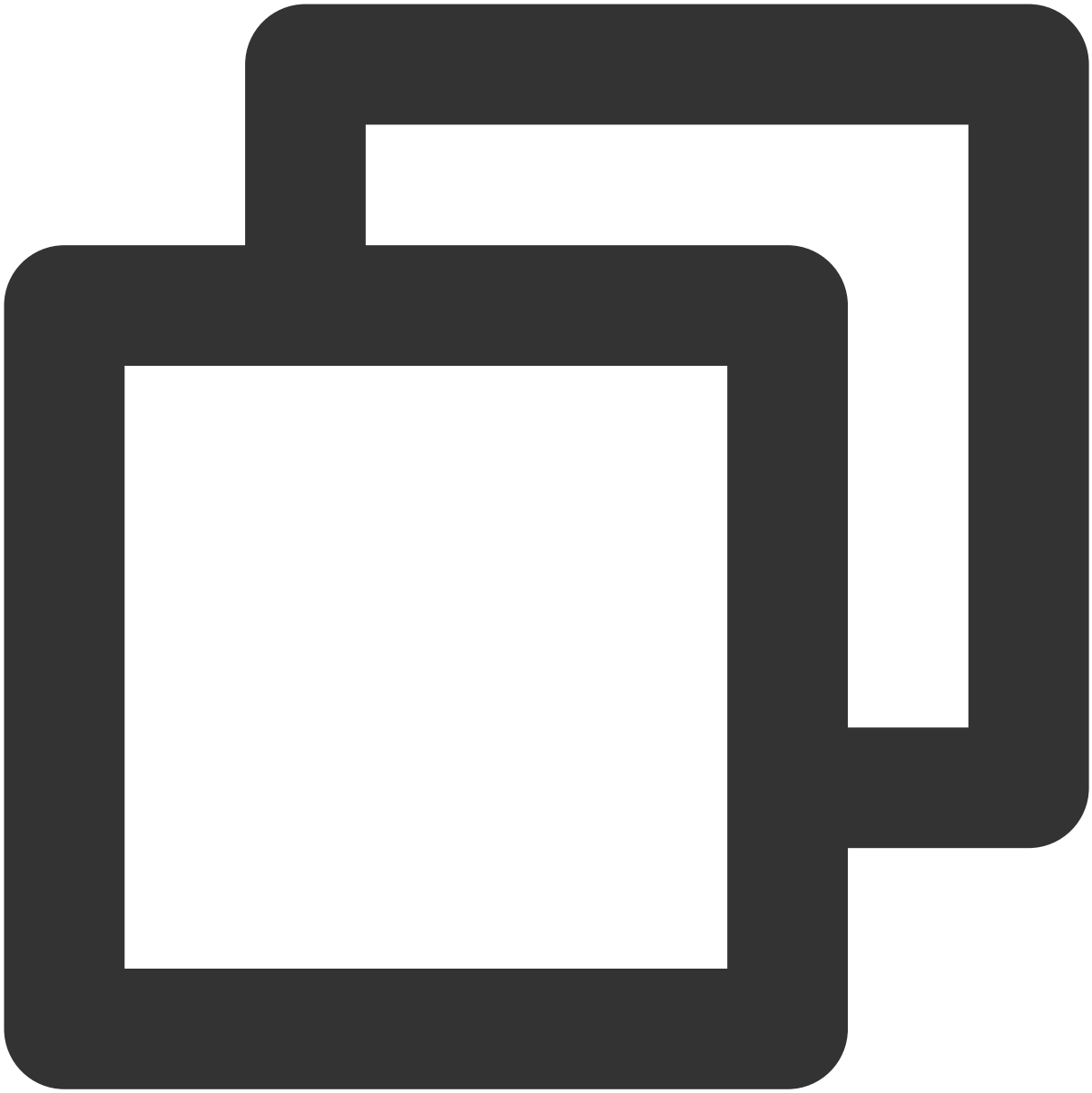
```
chown root:root /usr/lib64/libcrypto.so.1.0.2k
```

4. 다음 명령을 실행하여 소프트 링크를 생성합니다.



```
ln -s /usr/lib64/libcrypto.so.1.0.2k /usr/lib64/libcrypto.so.10
```

5. 다음 명령어를 실행하여 SSH 서비스를 실행합니다.



```
service sshd start
```

스냅샷 롤백을 통한 복구

라이브러리 파일은 인스턴스 시스템 디스크의 과거 스냅샷을 롤백하여 복원할 수 있으며, 자세한 내용은 스냅샷에서 데이터 롤백을 참고하십시오.

주의사항 :

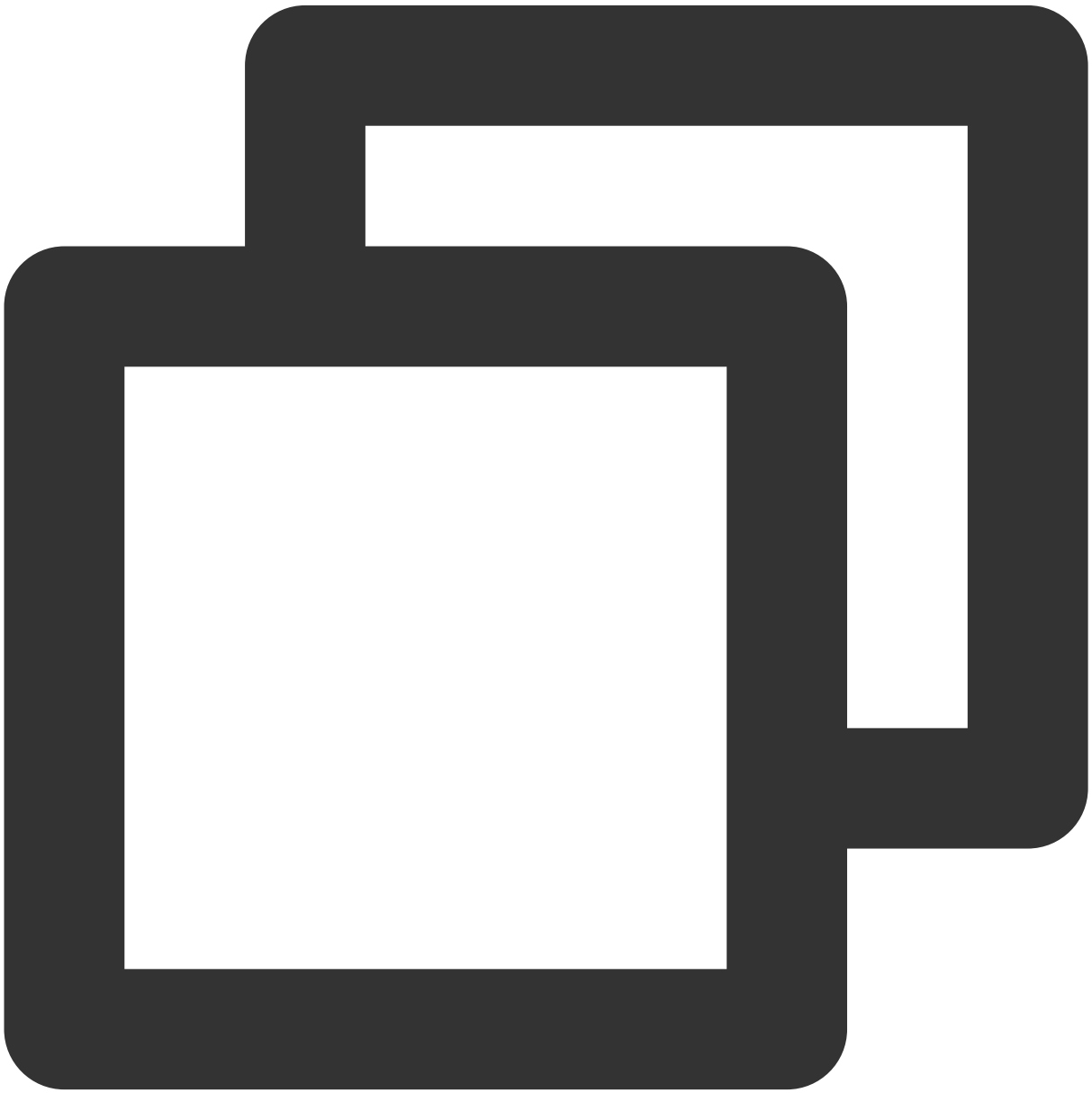
스냅샷 롤백은 스냅샷 생성 후 데이터 손실의 원인이 되므로 주의하시기 바랍니다.

SSH 서비스가 정상적으로 실행될 때까지 스냅샷 생성 시간이 가까운 순으로 롤백을 시도하는 것을 권장합니다. 롤백 후에도 SSH 서비스가 정상적으로 실행되지 않는 경우 해당 시점의 시스템이 비정상적임을 의미합니다.

SSH 서비스 실행 오류 fatal: Cannot bind any address

현상 설명

Linux 인스턴스가 SSH 서비스를 실행할 때, secure 로그 파일에서 또는 직접적으로 다음과 유사한 오류 메시지가 반환됩니다.



```
FAILED.
```

```
fatal: Cannot bind any address.
address family must be specified before ListenAddress.
```

문제 원인

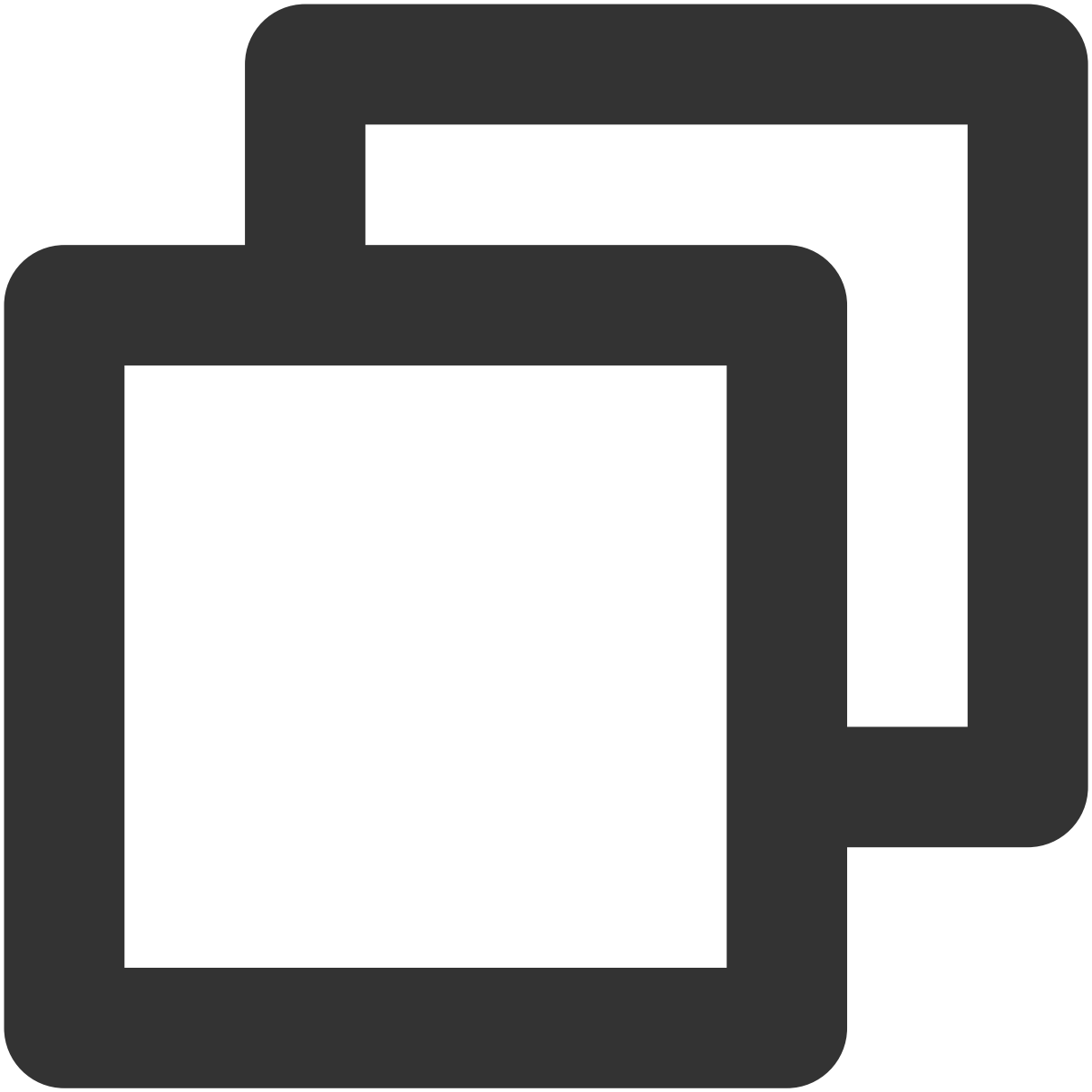
SSH 서비스의 'AddressFamily' 매개변수의 부적절한 설정으로 인해 발생합니다. 'AddressFamily' 매개변수는 실행 시 사용되는 프로토콜군을 지정하는 데 사용됩니다. 매개변수가 IPv6으로만 설정되어 있고 시스템에서 IPv6이 활성화되어 있지 않거나 IPv6 설정이 유효하지 않은 경우 이 문제가 발생할 수 있습니다.

해결 방식

1. 처리 순서를 참고하여 SSH 구성 파일 `sshd_config` 로 이동한 후, 설정을 확인합니다.
2. `AddressFamily` 매개변수를 수정하고 SSH 서비스를 재시작합니다.

처리 순서

1. VNC 사용하여 Linux 인스턴스에 로그인합니다.
2. 다음 명령을 실행하고 VIM 편집기를 사용하여 `sshd_config` 구성 파일로 이동합니다.



```
vim /etc/ssh/sshd_config
```

3. 다음과 유사한 구성이 포함되어 있는지 확인합니다.

```
AddressFamily inet6
```

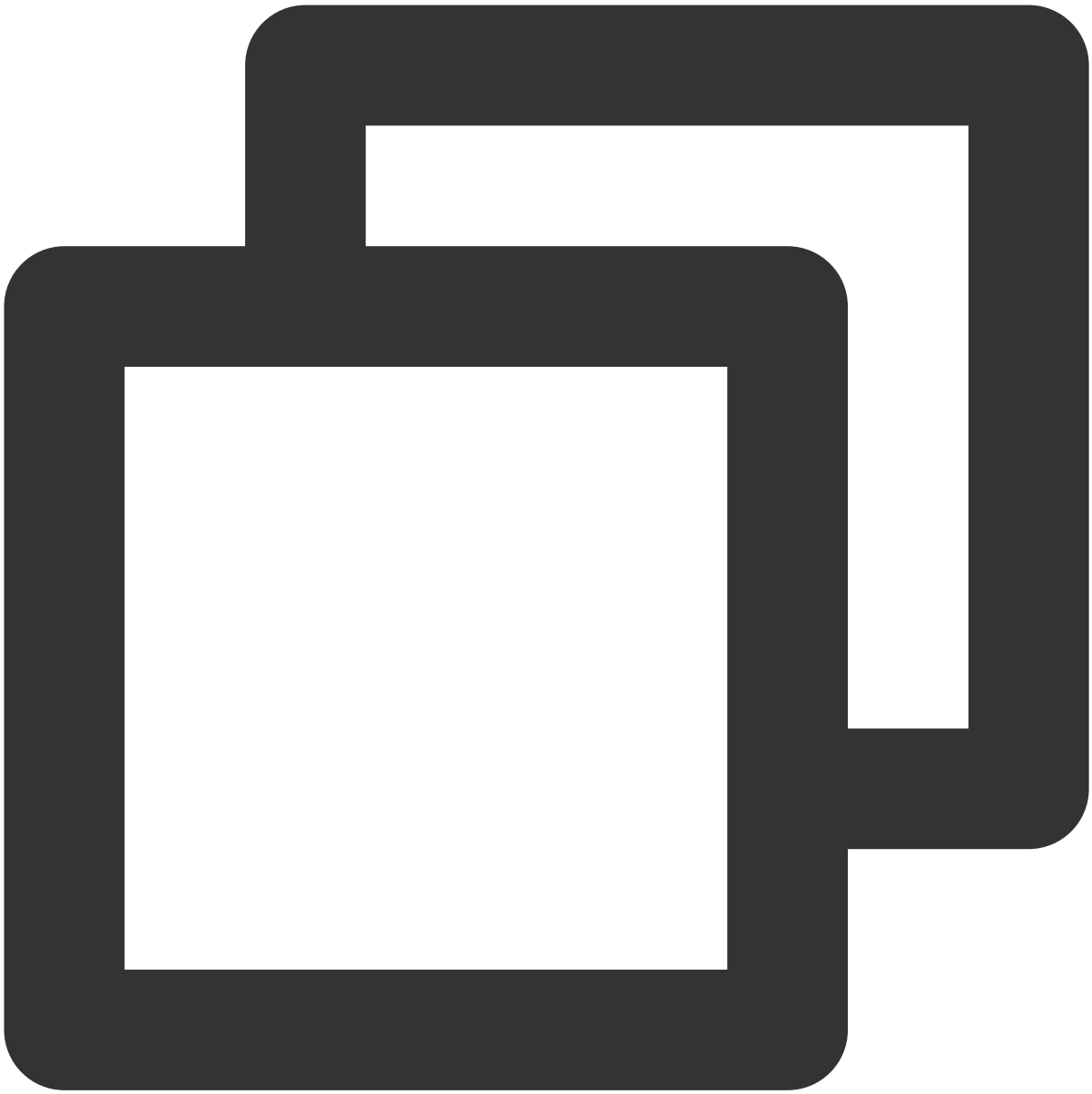
`` 상용 매개변수 관련 설명은 다음과 같습니다.

inet: 기본값인 IPv4 프로토콜군 사용.

inet6: IPv6 프로토콜군 사용.

any: IPv4 및 IPv6 프로토콜군 동시 활성화.

4. **i**를 눌러 편집 모드로 이동한 후, 다음 설정을 수정하거나, 행 시작 부분에 `#` 을 추가하여 주석을 진행합니다.



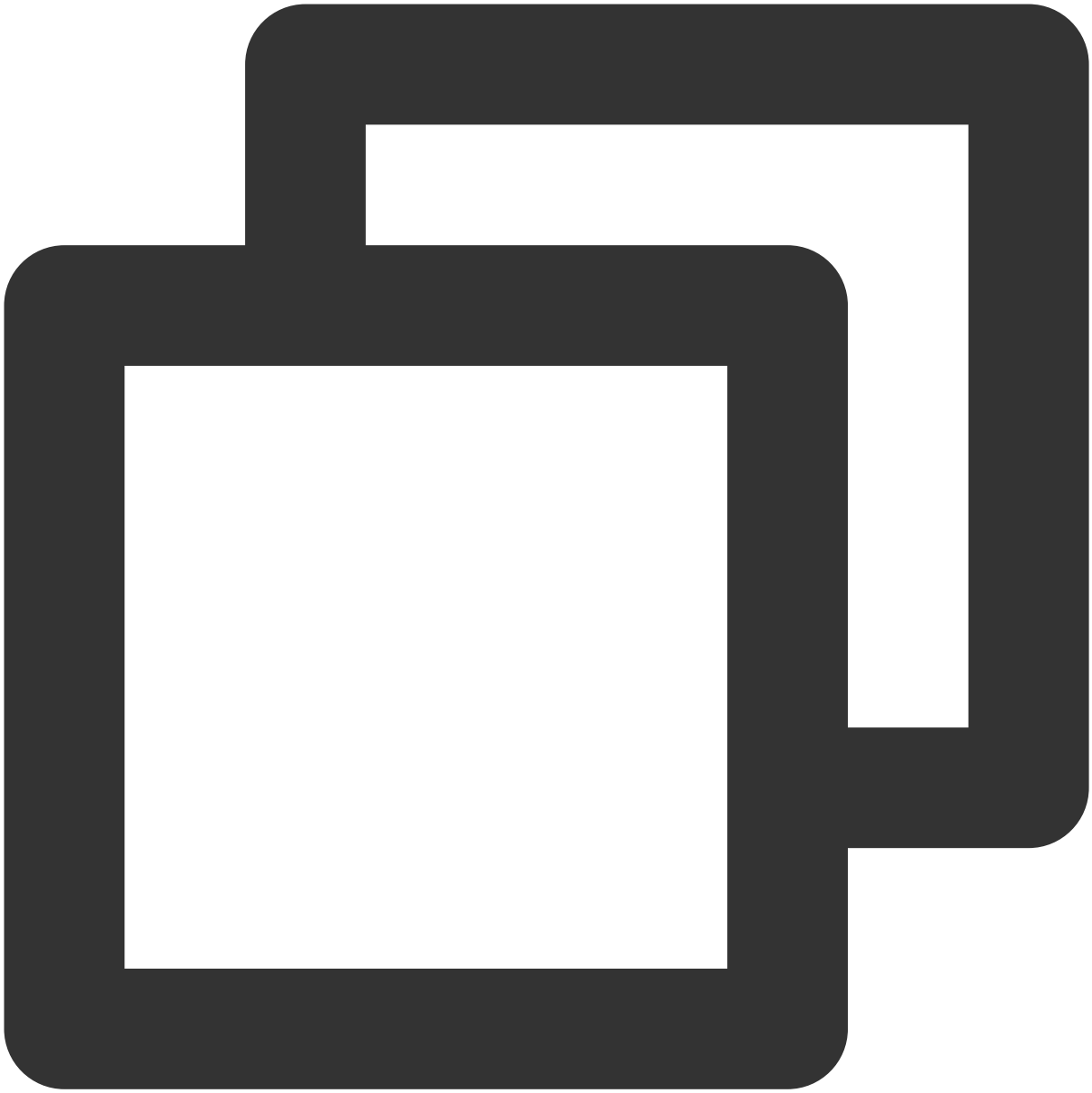
```
AddressFamily inet
```

주의사항 :

'AddressFamily' 매개변수는 'ListenAddress' 이전에 구성해야 적용됩니다.

5. **Esc**를 눌러 편집 모드를 종료하고 **:wq**를 입력하여 변경 사항을 저장합니다.

6. 다음 명령어를 실행하여 SSH 서비스를 재시작합니다.



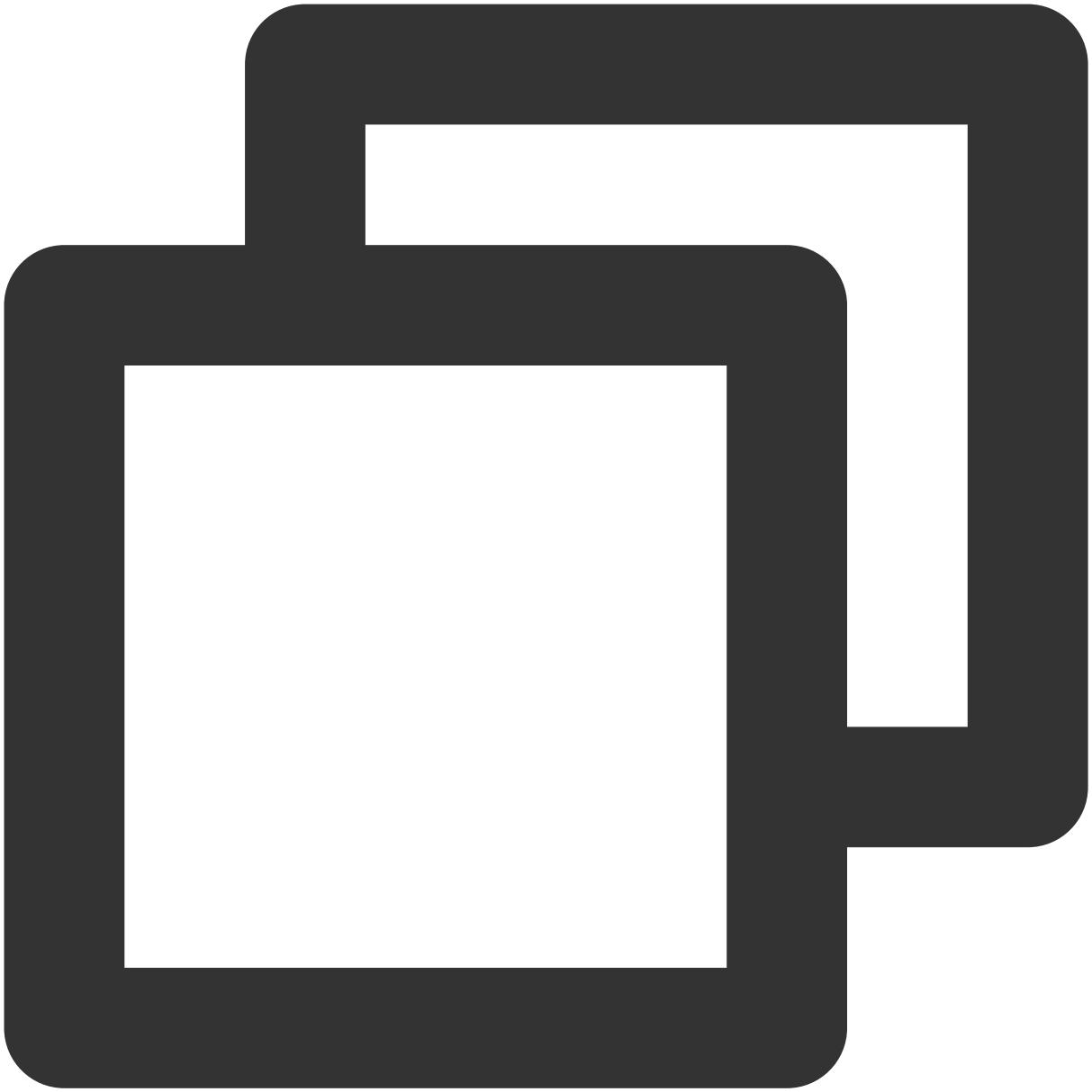
```
service sshd restart
```

SSH 서비스를 재시작한 후 SSH를 사용하여 로그인할 수 있습니다. 상세 내용은 SSH를 사용하여 Linux 인스턴스에 로그인을 참고하십시오.

SSH 서비스 실행 오류 Bad configuration options

현상 설명

Linux 인스턴스가 SSH 서비스를 실행할 때, secure 로그 파일에서 또는 직접적으로 다음과 유사한 오류 메시지가 반환됩니다.



```
/etc/ssh/sshd_config: line 2: Bad configuration options:\\\\
/etc/ssh/sshd_config: terminating, 1 bad configuration options
```

문제 설명

구성 파일은 파일 인코딩이나 구성 오류와 같은 비정상적인 문제로 인해 발생합니다.

해결 방식

다음 처리 항목을 참고하여 `sshd_config` 구성 파일을 복구합니다.

해결 절차

오류 정보에 해당하는 구성 파일 수정

오류 정보에 오류 설정이 명확하게 표시된 경우, VIM 편집기를 통해 `/etc/ssh/sshd_config` 구성 파일을 직접 수정할 수 있습니다. 또한, 다른 인스턴스의 올바른 구성 파일을 참고하여 수정할 수 있습니다.

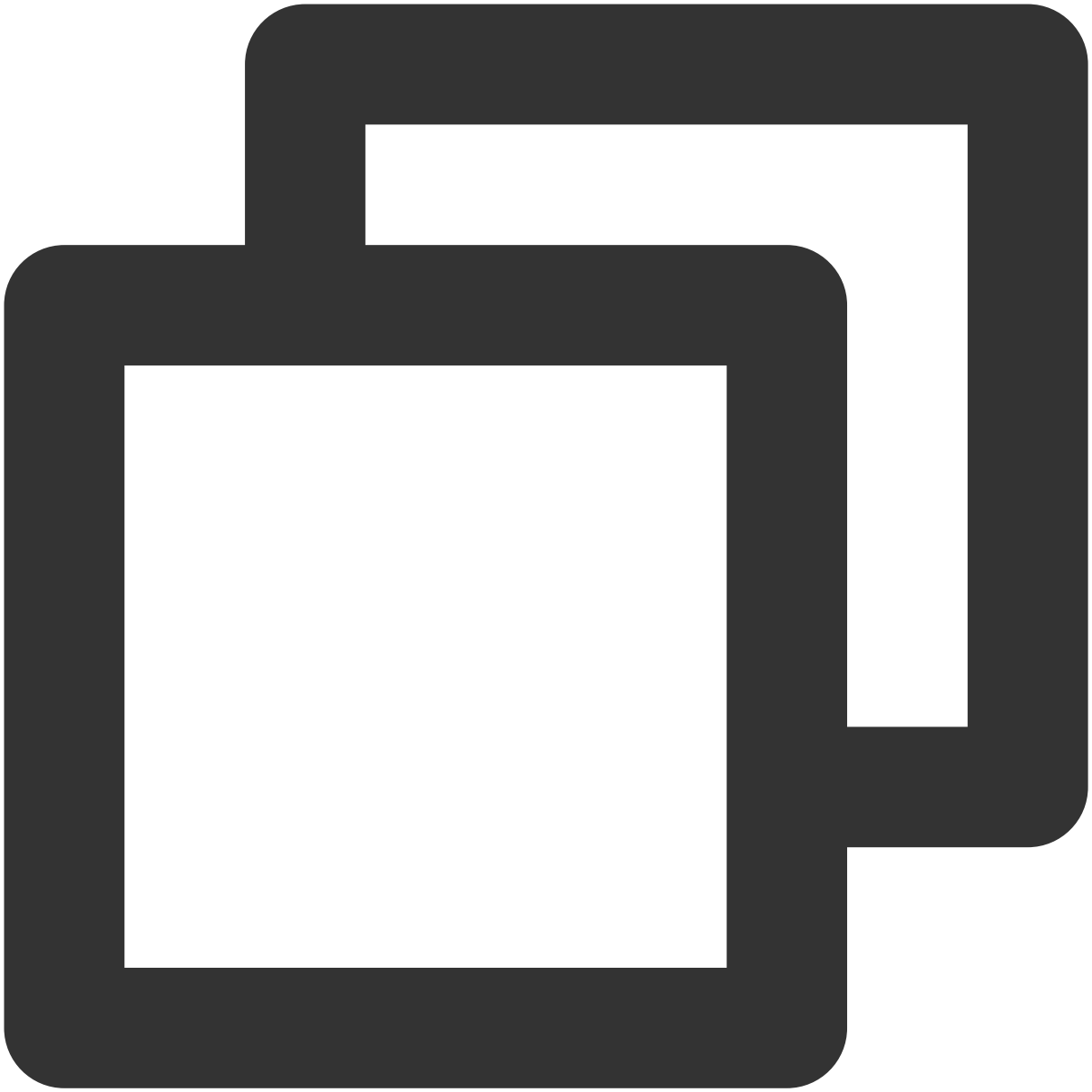
외부 파일 업로드

1. FTP 소프트웨어를 통해 다른 일반 서버의 `/etc/ssh/sshd_config` 라이브러리 파일을 타깃 서버의 `\\tmp` 디렉터리에 업로드합니다.

설명：

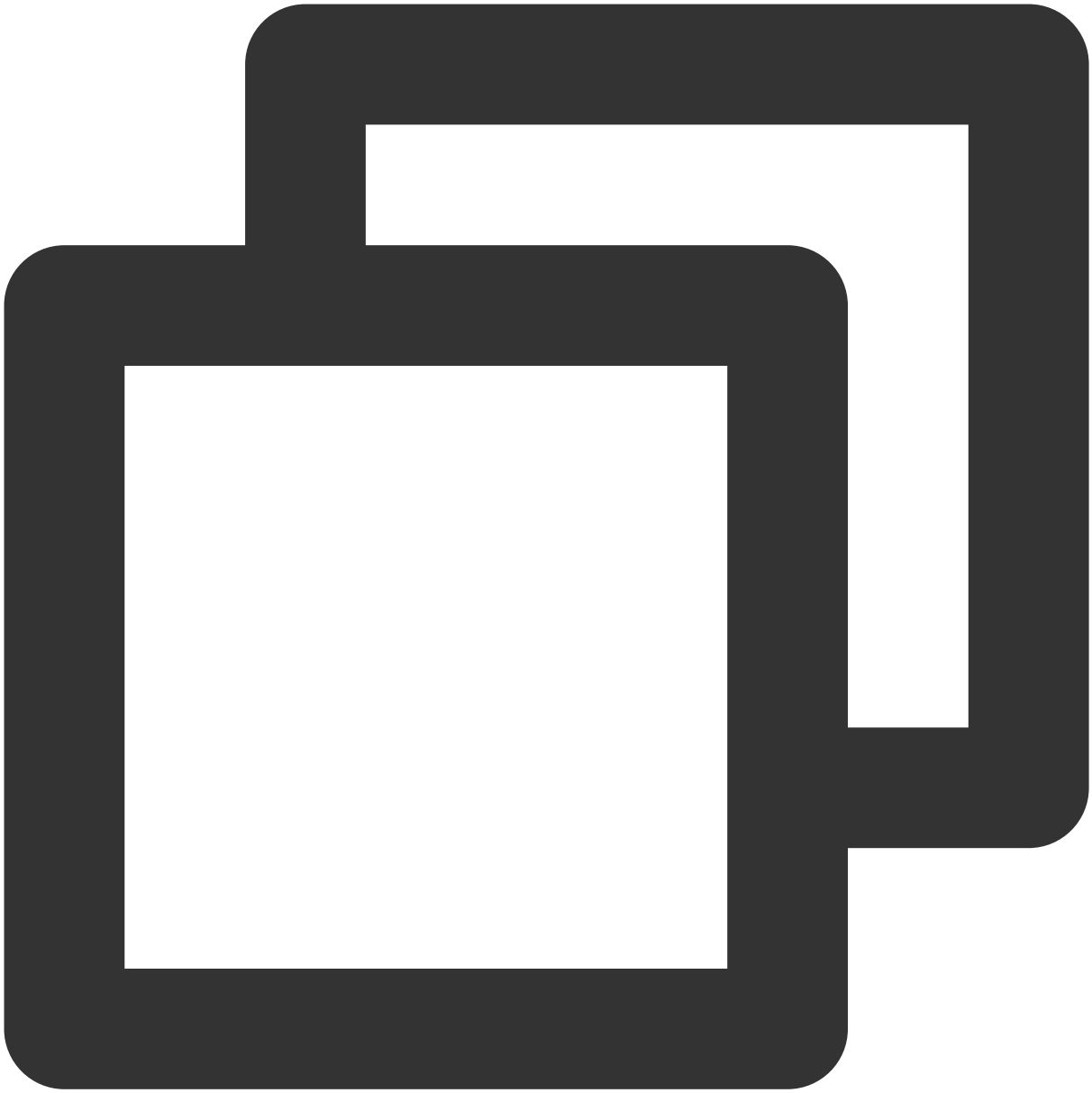
본문은 타깃 서버에 업로드된 `\\tmp` 디렉터리를 예로 들며, 실제 상황에 맞게 수정할 수 있습니다.

2. 다음 명령을 실행하여 라이브러리 파일을 일반 디렉터리에 복사합니다.



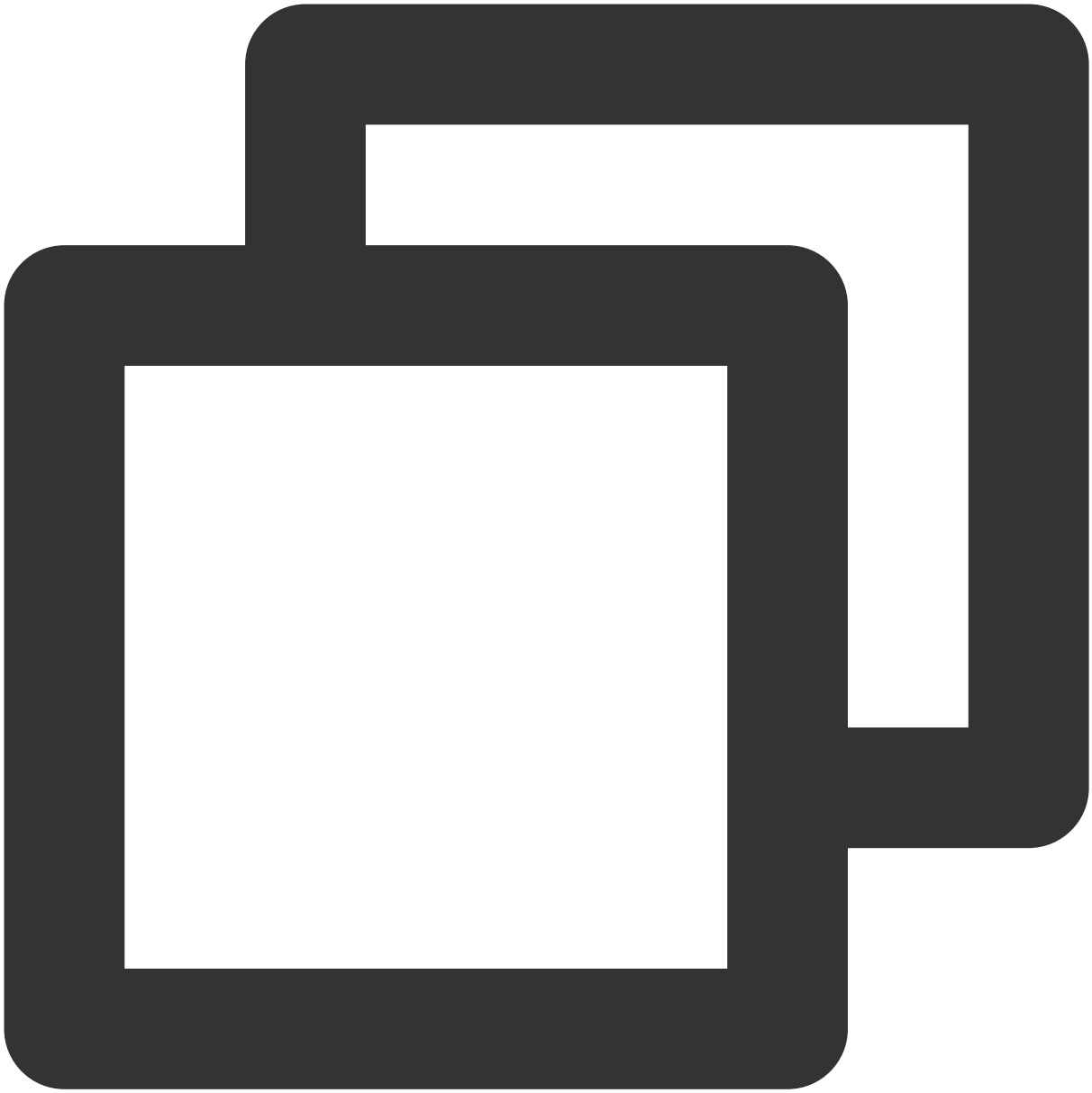
```
cp /tmp/sshd_config /etc/ssh/sshd_config
```

3. 다음 명령어를 순서대로 실행하여 파일 권한, 소유자, 그룹을 수정합니다.



```
chmod 600 /etc/ssh/sshd_config
``` ```
chown root:root /etc/ssh/sshd_config
```

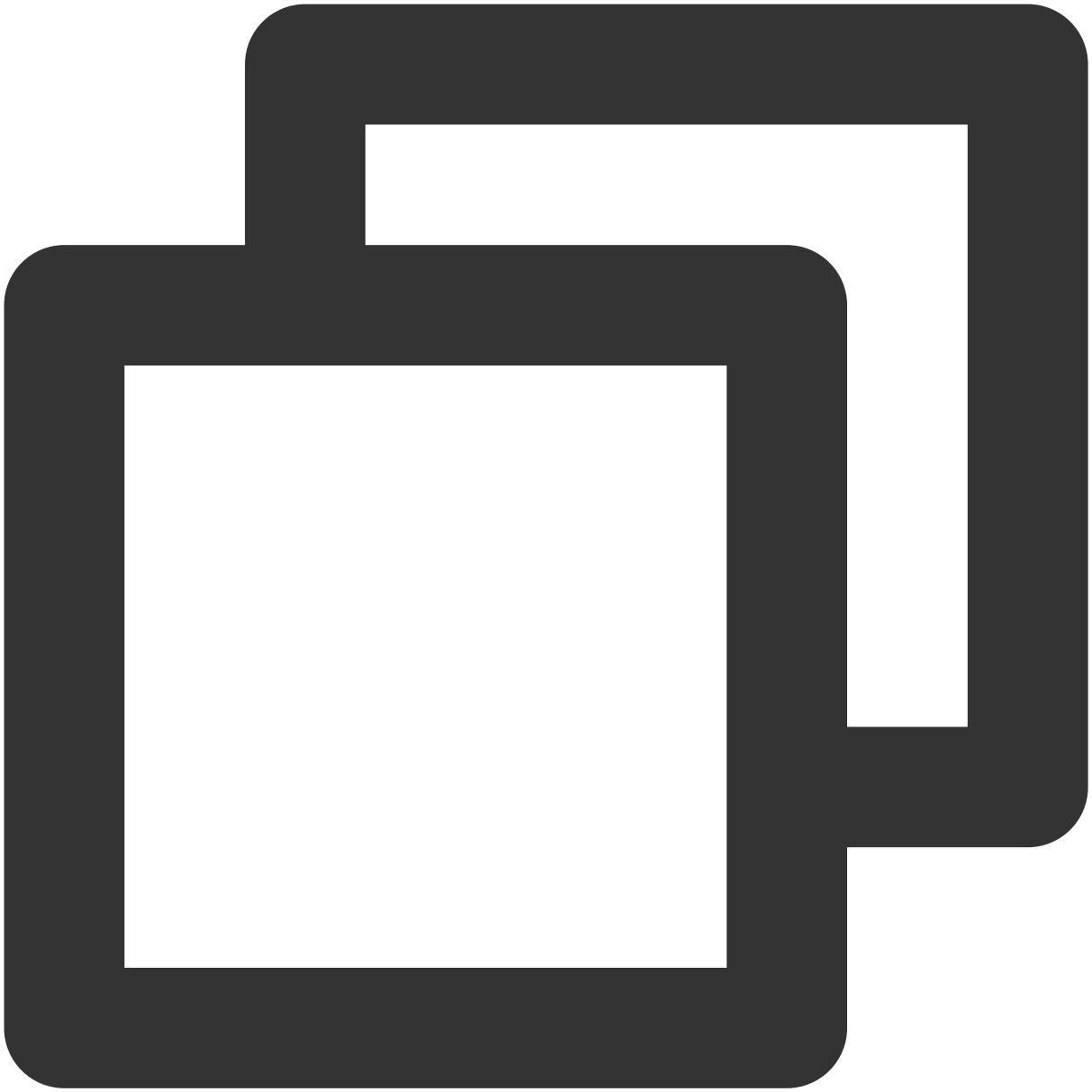
4. 다음 명령어를 실행하여 SSH 서비스를 실행합니다.
```



```
service sshd start
```

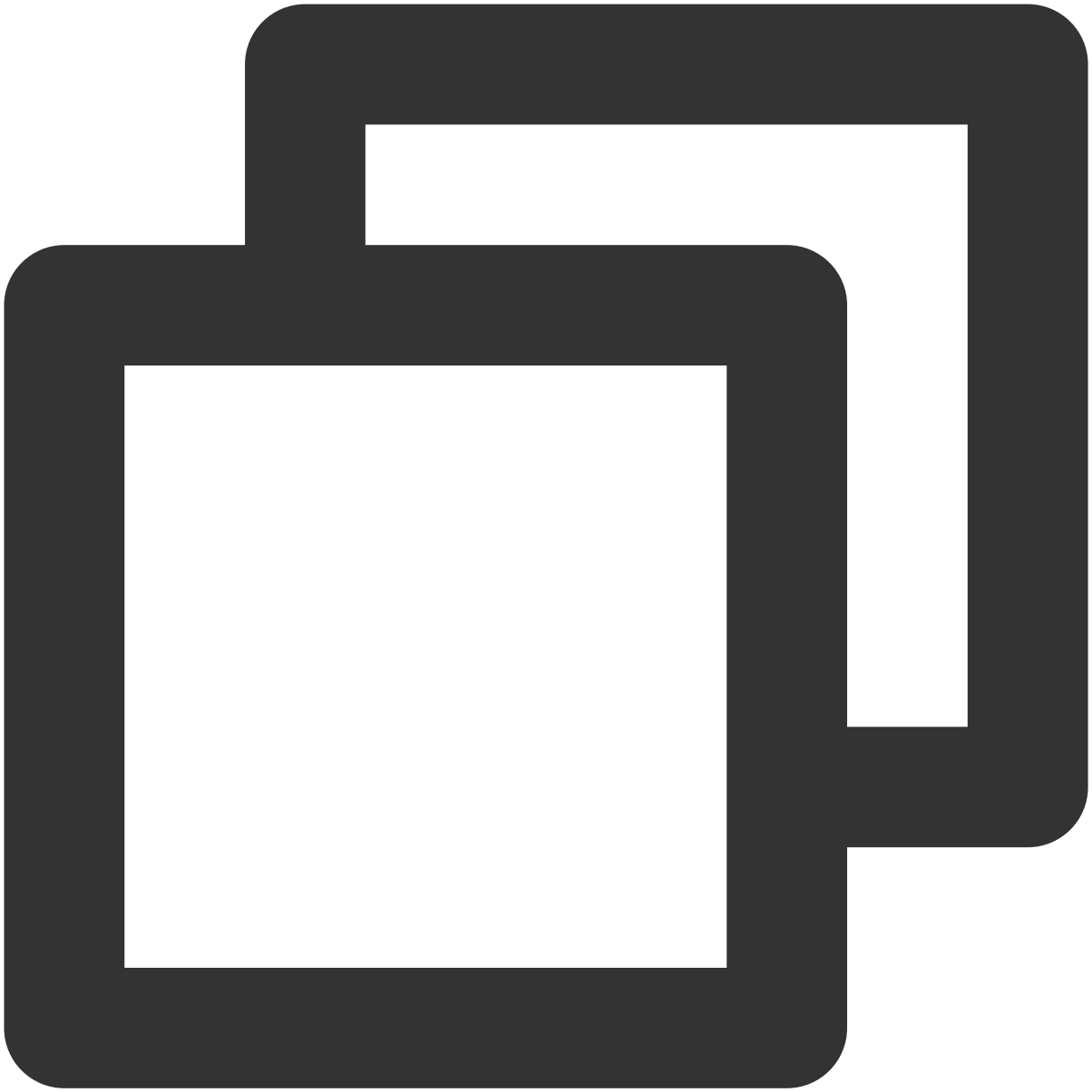
SSH 서비스 재설치

1. VNC 사용하여 Linux 인스턴스에 로그인합니다.
2. 다음 명령어를 실행하여 SSH 서비스를 언마운트 합니다.



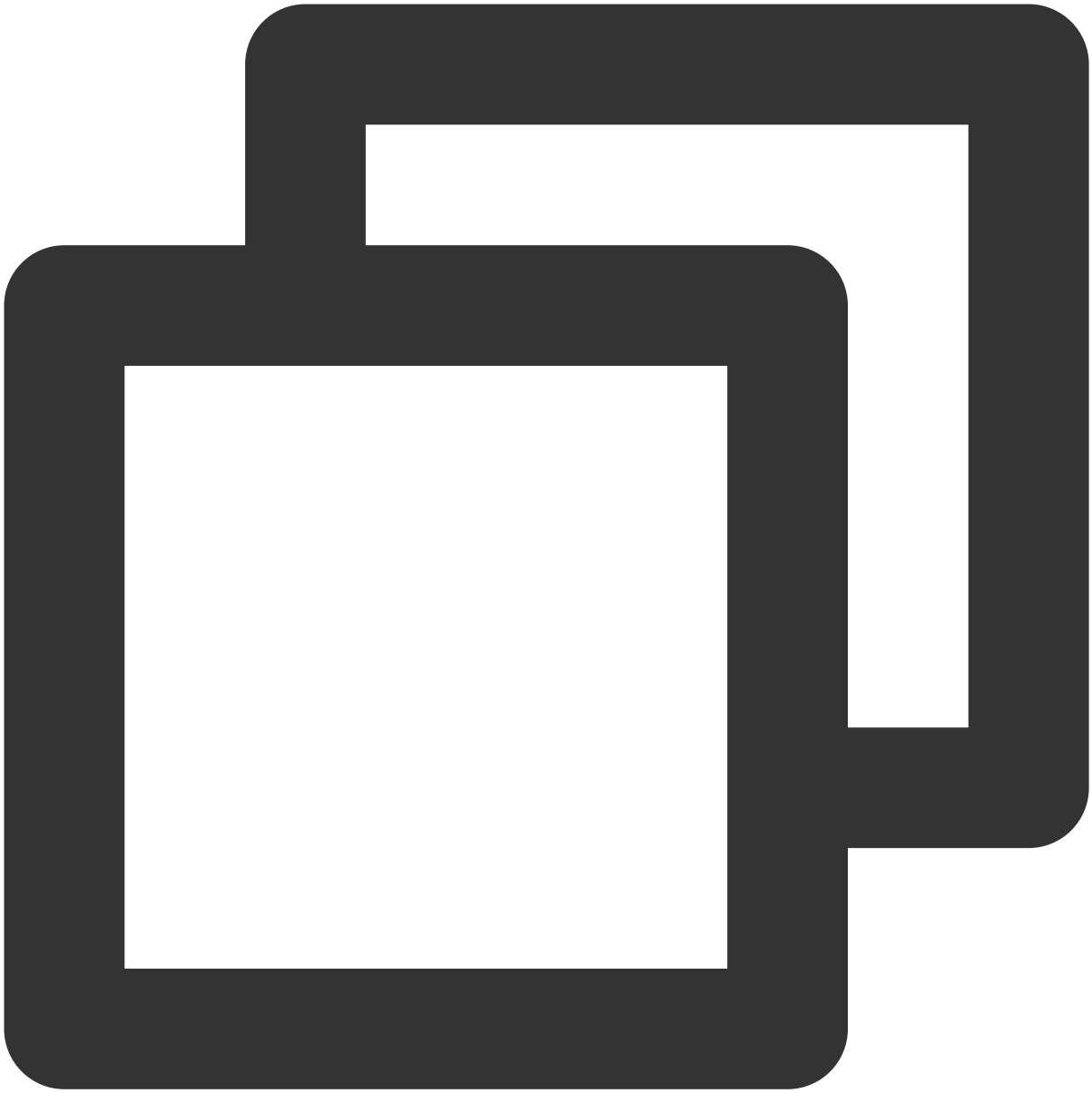
```
rpm -e openssh-server
```

3. 다음 명령어를 실행하여 SSH 서비스를 설치합니다.



```
yum install openssh-server
```

4. 다음 명령어를 실행하여 SSH 서비스를 실행합니다.



```
service sshd start
```

스냅샷 롤백을 통한 복구

라이브러리 파일은 인스턴스 시스템 디스크의 과거 스냅샷을 롤백하여 복원할 수 있으며, 자세한 내용은 스냅샷에서 데이터 롤백을 참고하십시오.

주의사항 :

스냅샷 롤백은 스냅샷 생성 후 데이터 손실의 원인이 되므로 주의하시기 바랍니다.

SSH 서비스가 정상적으로 실행될 때까지 스냅샷 생성 시간이 가까운 순으로 롤백을 시도하는 것을 권장합니다. 롤백 후에도 SSH 서비스가 정상적으로 실행되지 않는 경우 해당 시점의 시스템이 비정상적임을 의미합니다.

문제가 여전히 해결되지 않으면, 티켓 제출을 통해 고객센터에 도움을 요청하십시오.

Linux 인스턴스: CPU 혹은 메모리 점유율이 높아 로그인 할 수 없을 경우

최종 업데이트 날짜: : 2024-02-02 11:09:48

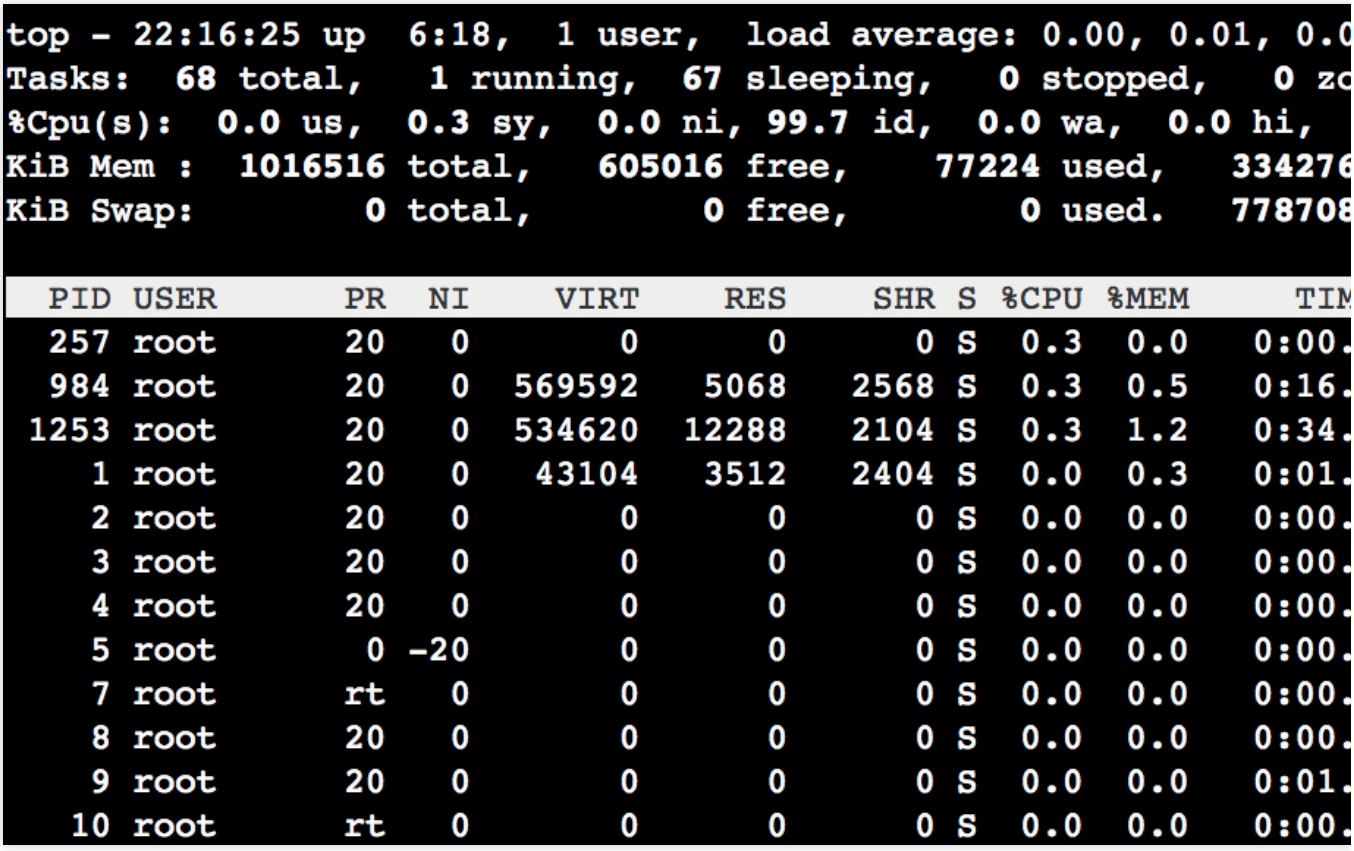
본 문서는 높은 CPU 또는 메모리 사용량으로 인한 Linux CVM 로그인 실패와 같은 문제를 진단하고 해결하는 방법을 설명합니다.

예상 원인

CPU 또는 메모리 사용량이 지나치게 높으면 서비스 응답 속도가 느려지거나 서버에 로그인할 수 없는 등의 문제가 발생할 수 있습니다. CPU 또는 메모리 사용량이 지나치게 높아지는 이유는 하드웨어, 시스템 프로세스, 비즈니스 프로세스 또는 트로이 목마 바이러스 등이 원인일 수 있습니다. 클라우드 모니터링을 사용해 CPU 또는 메모리 사용량 임계 값 알림을 생성함으로써 CPU 또는 메모리 사용량이 임계 값을 초과할 경우, 즉시 사용자에게 공지하도록 설정할 수 있습니다.

진단 툴

Top: 프로세스별 CPU 또는 메모리 사용량을 얻기 위해 일반적으로 사용되는 Linux의 모니터링 도구입니다. top 명령의 출력 정보는 다음과 같습니다.



Top 명령 출력은 두 부분으로 구성됩니다. 상단에는 CPU 및 메모리 리소스의 일반적인 사용량이 표시됩니다.

첫째 줄: 시스템 현재 시간, 현재 로그인 사용자 개수 및 시스템 부하.

둘째 줄: 시스템 전체 프로세스 수, 실행 중인 프로세스 수, 휴면/수면/좀비 프로세스 수입니다.

셋째 줄: 현재 CPU 사용 상황.

넷째 줄: 현재 메모리 사용 상황.

다섯째 줄: 현재 Swap 용량 사용 상황.

하단에는 프로세스별 리소스 사용량 표시:

PID: 프로세스 ID.

USER: 프로세스 소유자.

PR: 프로세스 우선 순위. NI는 NICE 값입니다. NICE 값이 작을수록 우선 순위가 높습니다.

VIRT: 사용하는 버츄얼 메모리 사이즈, 단위 KB.

RES: 현재 사용 중인 메모리 사이즈, 단위 KB.

SHR: 사용하는 공유 메모리의 사이즈, 단위 KB.

S: 프로세스 상태.

%CPU: 업데이트 시간 간격 내 프로세스가 사용하는 CPU 시간의 백분율.

%MEM: 업데이트 시간 간격 내 프로세스가 사용하는 메모리의 백분율.

TIME+: 프로세스가 사용하는 CPU 시간, 0.01s 단위까지 정확합니다.

COMMAND: 프로세스 이름.

장애 처리

CVM 로그인

실제 필요에 따라 CVM 로그인 방법을 선택하십시오.
타사 소프트웨어를 통해 원격으로 Linux CVM 인스턴스에 로그인합니다.

주의사항 :

Linux CVM 인스턴스가 CPU 고부하 상태이면 높으면 로그인에 실패할 수 있습니다.

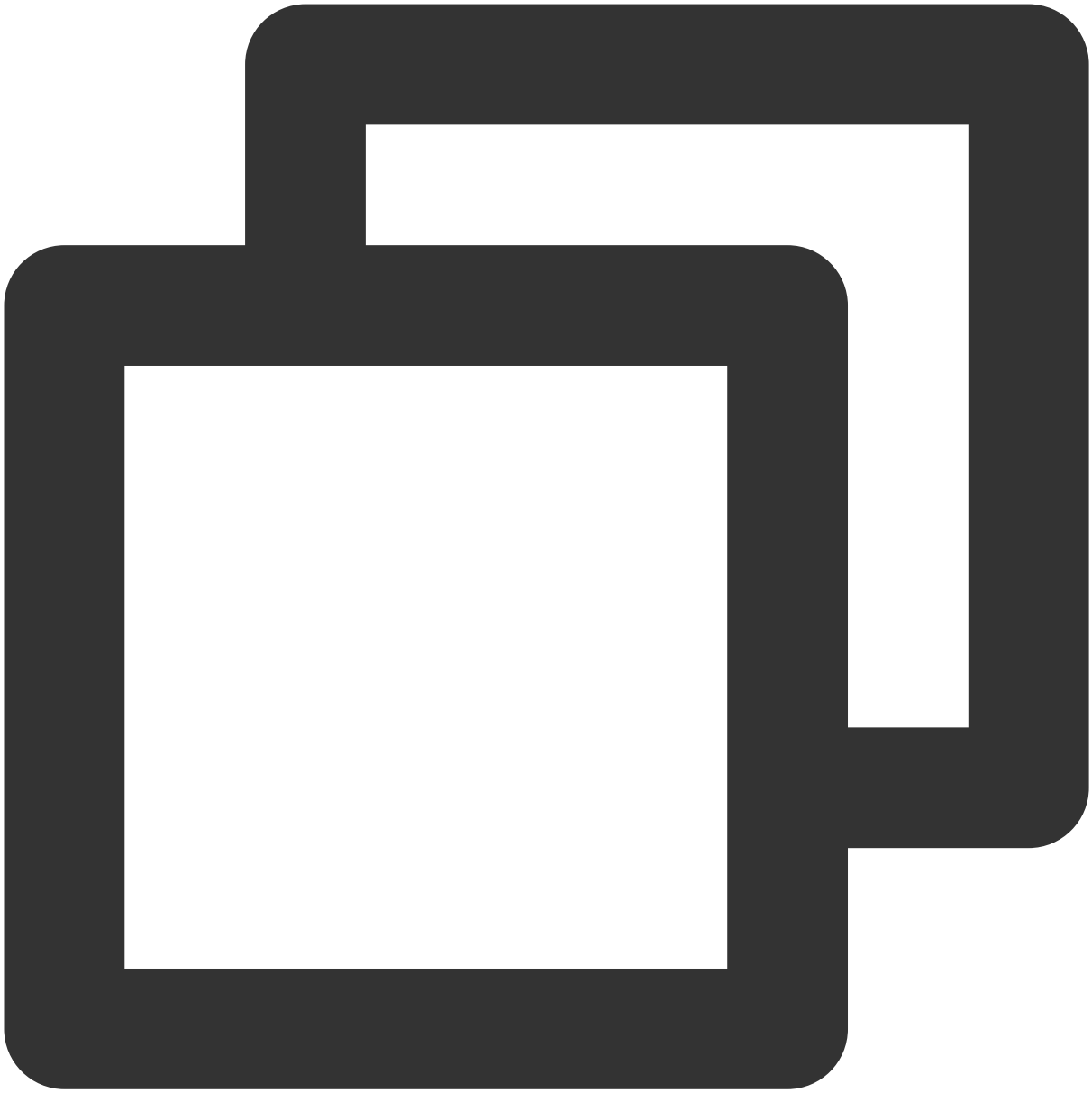
VNC 사용하여 Linux 인스턴스에 로그인합니다.

주의사항 :

Linux CVM 인스턴스가 CPU 고부하 상태이면 콘솔에서 로그인할 수 있습니다.

프로세스의 리소스 사용량 보기

다음 명령을 실행하여 시스템 부하를 확인합니다. '%CPU' 및 '%MEM' 열을 보고 더 많은 리소스를 소비하는 프로세스를 식별합니다.



```
top
```

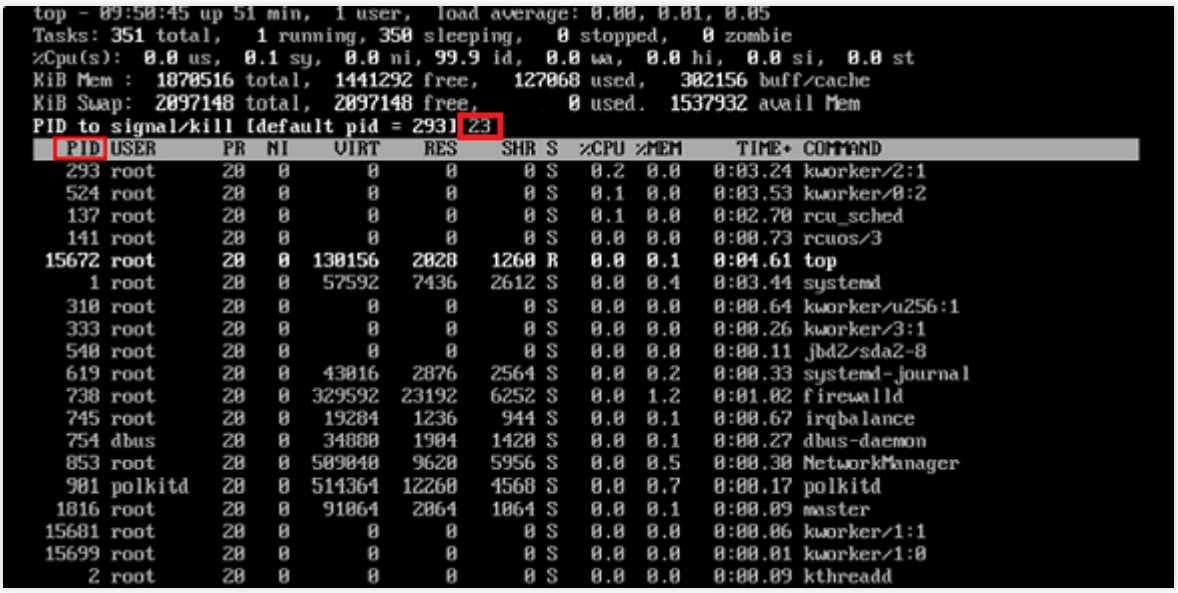
분석 프로세스

작업 관리자 페이지에서 프로세스를 분석하여 문제를 해결합니다.
서비스 프로세스로 인해 문제가 발생한 경우 서비스 프로세스를 최적화할 수 있는지 분석하여 그에 따라 프로세스를 최적화하거나 인스턴스 구성 변경합니다.
예외 프로세스로 의해 문제가 발생한 경우 인스턴스에 바이러스가 있을 수 있습니다. 이 경우 프로세스를 종료하거나 바이러스 백신 프로그램을 사용하여 바이러스를 제거할 수 있습니다. 필요한 경우 데이터를 백업하고 운영 체제를 다

시 설치하십시오.
문제가 Tencent Cloud 컴포넌트 프로세스로 인해 발생한 경우 티켓 제출을 통해 도움을 요청하십시오.
일반적인 Tencent Cloud 컴포넌트는 다음과 같습니다.
sap00x: 보안 컴포넌트
Barad_agent: 모니터링 컴포넌트
secu-tcs-agent: 보안 컴포넌트

종료 프로세스

1. 다른 프로세스의 리소스 소비를 비교하고 종료해야 하는 프로세스의 PID를 기록합니다.
2. 'k'를 입력합니다.
3. 다음 그림과 같이 종료해야 하는 프로세스의 PID를 입력하고 **Enter** 키를 눌러 종료합니다.
PID가 23인 프로세스를 종료해야 한다고 가정합니다.



주의사항 :

Enter 키를 누른 후 `kill PID 23 with signal [15]:` 가 나타나면 **Enter** 키를 다시 눌러 기본 설정을 유지합니다.

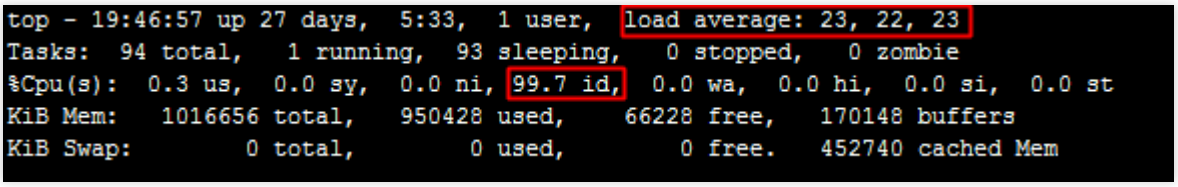
4. 작업이 성공하면 `Send pid 23 signal [15/sigterm]` 메시지가 나타납니다. **Enter**를 눌러 종료를 확인합니다.

기타 관련 문제

CPU 사용량은 낮지만 평균 부하가 높음

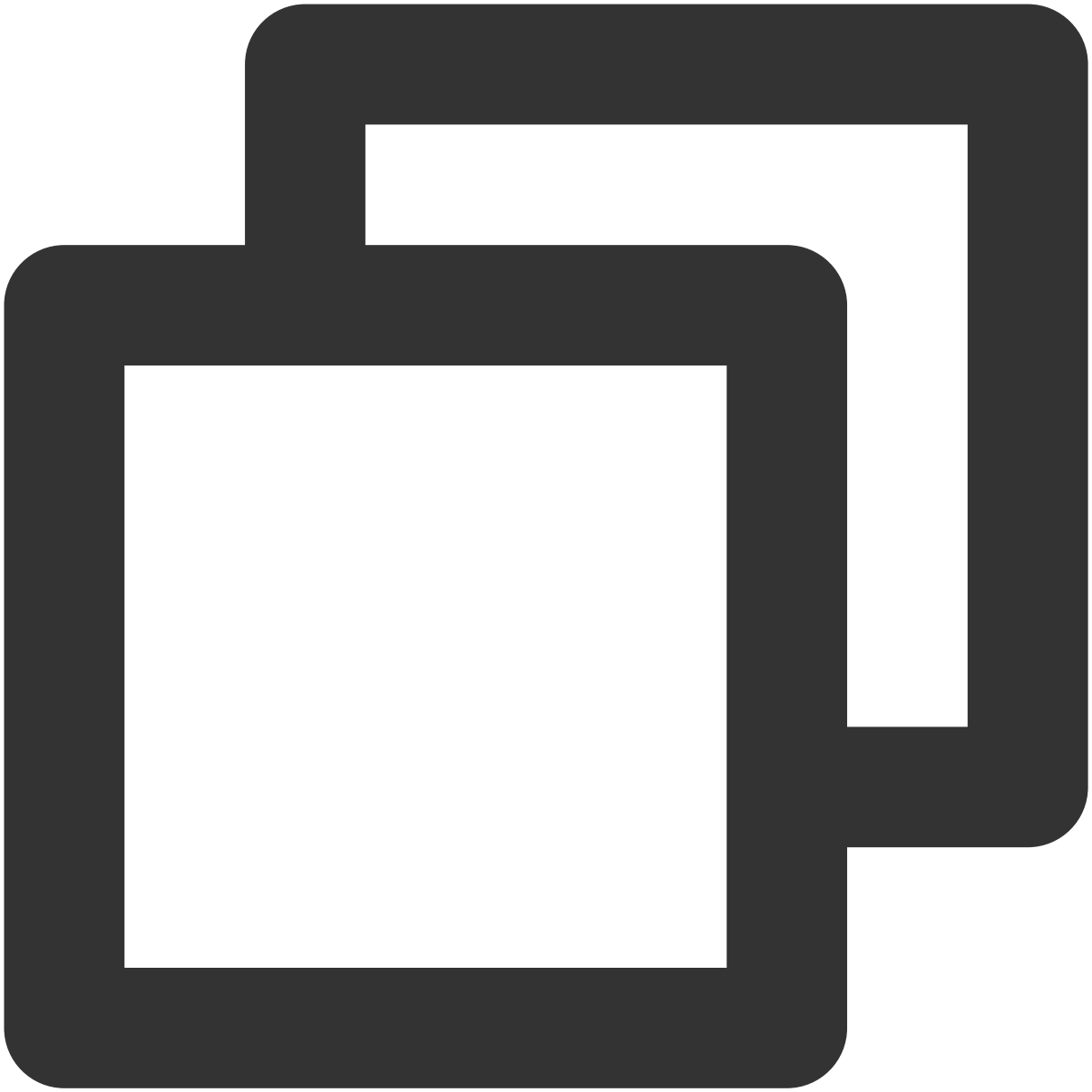
원인

Load average는 CPU 부하의 지표입니다. 평균 부하가 높을수록 보류 중인 프로세스의 큐가 길어집니다.
top 명령이 실행된 후 다음과 유사한 정보가 반환되어 CPU 사용량은 낮지만 load average는 매우 높음을 나타냅니다.

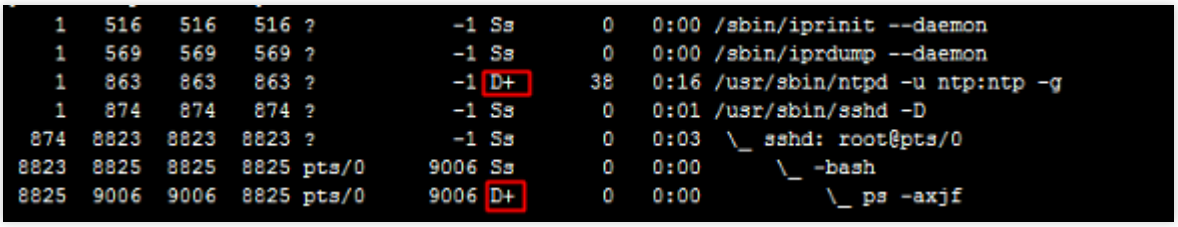


솔루션

다음 명령을 실행하여 아래와 같이 D 상태에 있는 프로세스가 있는지 확인합니다.



```
ps -axjf
```



설명：

D 상태는 중단되지 않은 수면 상태를 나타냅니다. 이 상태의 프로세스는 종료될 수 없으며 자체적으로 종료될 수도 없습니다.

D 상태의 프로세스가 많은 경우 프로세스가 종속된 리소스를 복원하거나 운영 체제를 다시 시작합니다.

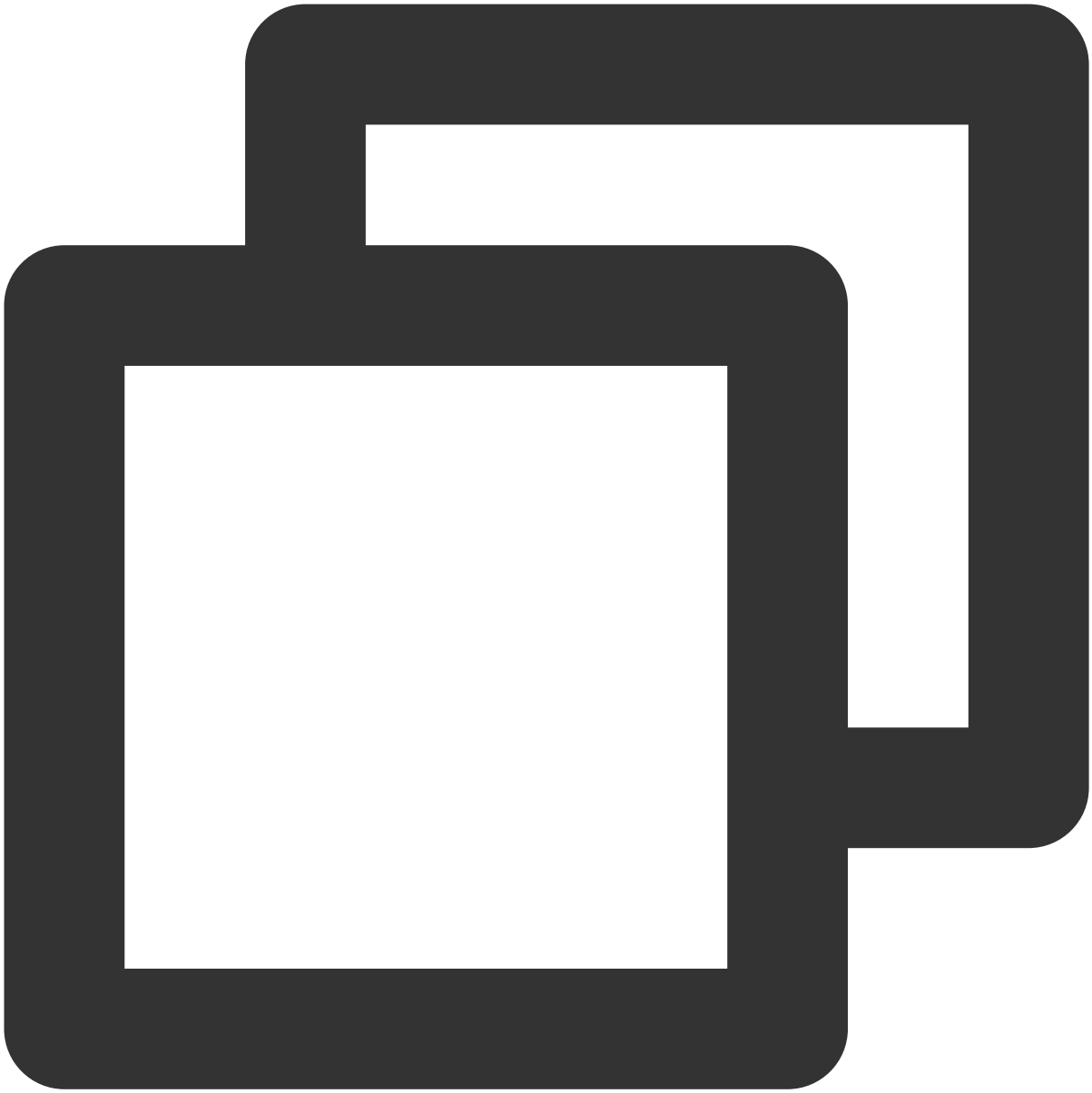
Kswapd0 프로세스의 높은 CPU 사용량

원인

Linux는 페이징 메커니즘을 사용하여 메모리를 관리하고 디스크의 일부를 가상 메모리로 따로 설정합니다. kswapd0은 Linux 시스템의 가상 메모리 관리에서 페이지 교체를 담당하는 프로세스입니다. 시스템 메모리가 부족하면 kswapd0이 페이지를 자주 교체하므로 CPU 사용량이 높아집니다.

솔루션

1. 다음 명령어를 실행하여 kswapd0 프로세스를 찾습니다.



```
top
```

2. kswapd0 프로세스의 상태를 확인합니다.

프로세스가 D 상태가 아니고 오랫동안 실행되어 CPU 리소스를 너무 많이 소모한 경우 3단계을 수행하여 메모리 사용량을 확인합니다.

3. `vmstat` , `free` , `ps` 와 같은 명령을 실행하여 시스템의 프로세스에서 사용하는 메모리 양을 확인합니다. 메모리 사용량에 따라 시스템을 다시 시작하거나 안전하지만 불필요한 프로세스를 종료합니다. si 및 so 값도 높으면 시스템에서 페이지가 자주 교체됩니다. 현재 시스템의 물리적 메모리가 더 이상 요구 사항을 충족할 수 없는 경우 시스템 메모리 업그레이드를 고려하십시오.

Linux 인스턴스: 포트 문제로 로그인을 할 수 없는 경우

최종 업데이트 날짜: : 2024-02-02 11:09:47

본 문서는 CVM이 포트 문제로 인해 원격 로그인이 불가능한 경우의 진단 방법과 솔루션을 소개합니다.
설명 :
아래 작업은 CentOS 7.8 시스템의 CVM을 예로 듭니다.

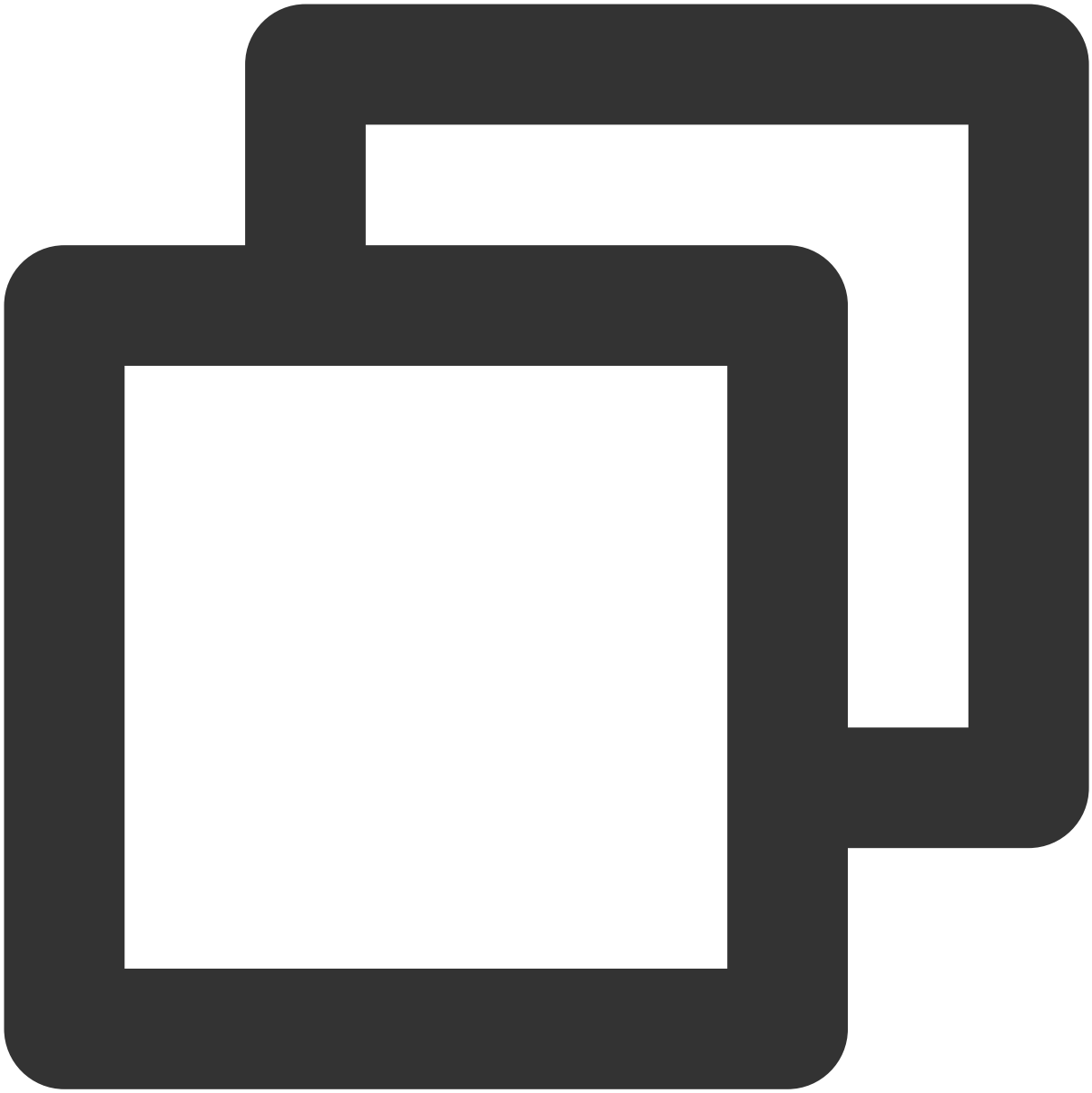
점검 툴

Tencent Cloud가 제공한 아래의 툴을 통해 로그인이 불가능한 문제가 포트 및 보안 그룹 설정과 관련이 있는지 판단할 수 있습니다.
자가 진단
인스턴스 포트 진단 툴
보안 그룹 설정 문제로 진단된 경우, 인스턴스 포트 진단 툴의 [원클릭 오픈] 기능을 통해 관련 포트를 개방한 후 다시 로그인을 시도하십시오. 포트를 개방한 후에도 로그인에 실패한다면 다음 내용을 참조하여 원인을 진단할 수 있습니다.

문제 진단

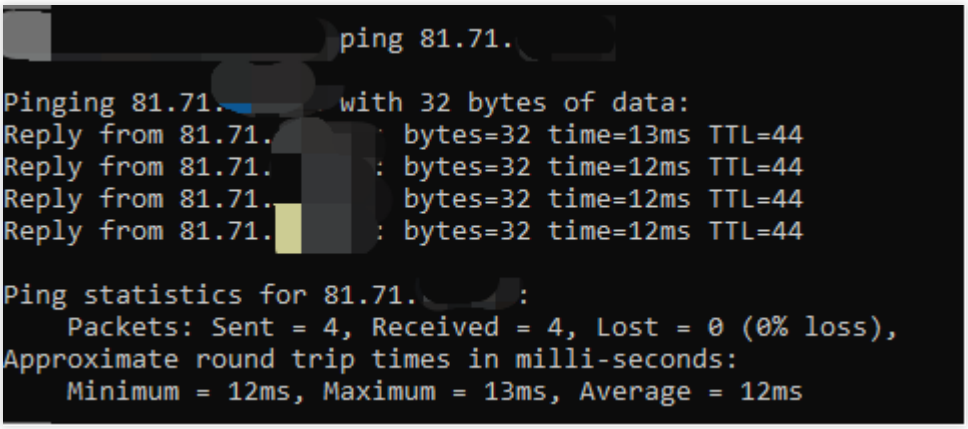
네트워크 연결성 점검

로컬 Ping 명령어를 통해 네트워크 연결성을 테스트할 수 있습니다. 서로 다른 네트워크 환경(IP 대역 또는 ISP)의 컴퓨터를 동시에 사용한 테스트로 로컬 네트워크 문제인지, 서버 문제인지 판단합니다.
1. 로컬 컴퓨터의 운영 체제에 따라 TCCLI를 여는 방식을 선택합니다.
Windows 시스템: [시작]>[실행]을 클릭하고 cmd를 입력하면 명령 라인 대화 상자가 팝업됩니다.
Mac OS 시스템: Terminal 툴을 엽니다.
2. 아래의 명령어를 실행하여 네트워크 연결을 테스트합니다.



```
ping + CVM 인스턴스 공용 IP 주소
```

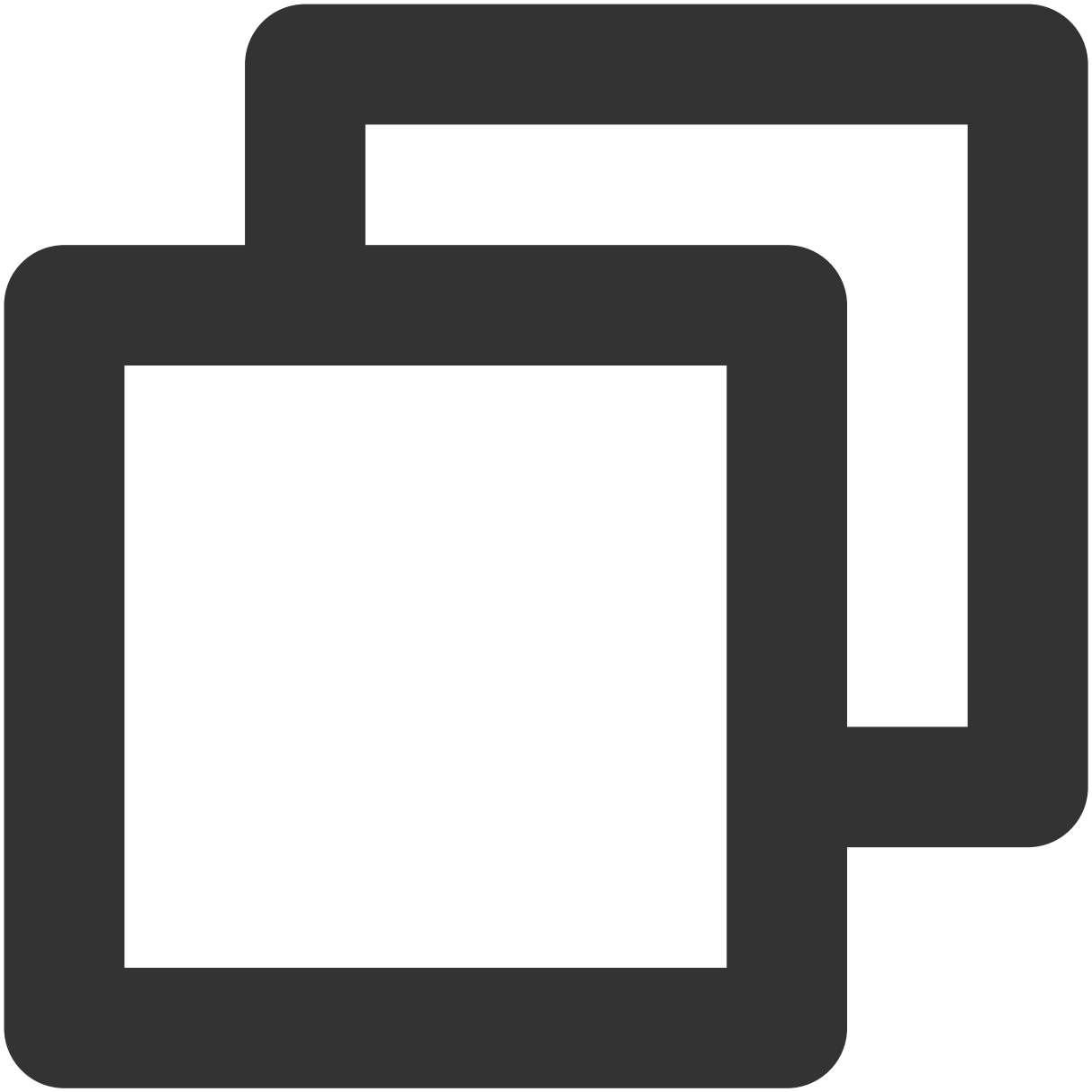
공용 IP 주소 획득을 참조하여 CVM 인스턴스 공용 IP를 획득할 수 있습니다(예: `ping 81.71.XXX.XXX` 실행). 네트워크가 정상인 경우 다음과 유사한 결과를 반환합니다.



네트워크가 비정상인 경우 [요청 시간 초과] 알림이 뜹니다. 인스턴스 IP주소 Ping 연결 불가를 참조하여 진단하십시오.

인스턴스 포트 연결성 점검

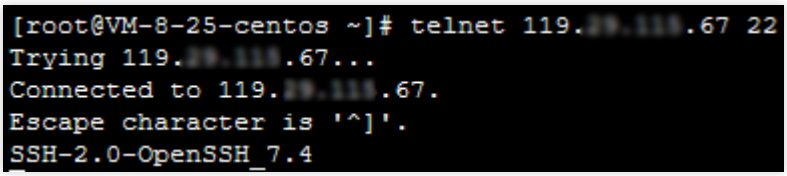
1. VNC로 CVM에 로그인합니다. 자세한 내용은 VNC로 Linux 인스턴스에 로그인을 참조하십시오.
2. 아래의 명령어를 실행하고 **Enter**를 누릅니다. 원격 포트의 활성화 상태를 테스트하여 포트에 액세스가 가능한지 판단합니다.



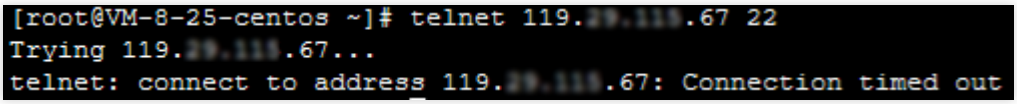
```
telnet + CVM 인스턴스 공용 IP 주소 + 포트 번호
```

예: `telnet 119.XX.XXX.67 22` 명령어를 실행하여 22 포트의 연결성을 테스트합니다.

정상 상태: 아래 이미지와 같은 정보를 반환할 경우 22 포트에 액세스할 수 있습니다.



비정상 상태: 아래 이미지와 같은 정보를 반환할 경우 22 포트에 액세스할 수 없습니다. 문제가 발생한 네트워크에 해당하는 부분을 점검하십시오(예: 인스턴스의 방화벽 또는 보안 그룹의 22 포트 개방 여부).



sshd 서비스 점검

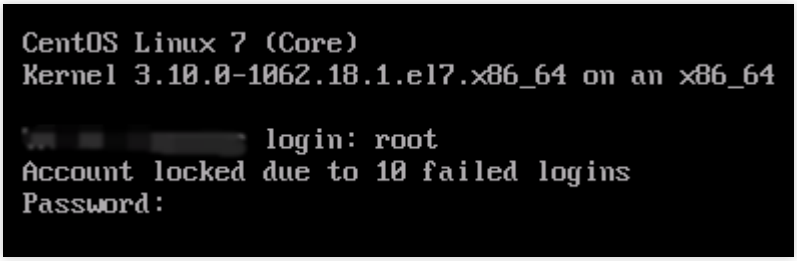
SSH를 사용하여 Linux 인스턴스에 로그인할 때 연결 불가 또는 연결 실패 알림이 뜹니다. sshd 포트가 수신되지 않았거나 sshd 서비스가 실행되지 않은 것이 원인일 수 있습니다. SSH 방식으로 Linux 인스턴스에 로그인할 수 없을 경우를 참조하여 진단하십시오.

Linux 인스턴스:VNC 로그인 오류 알림 Module is unknown

최종 업데이트 날짜: : 2024-02-02 11:09:47

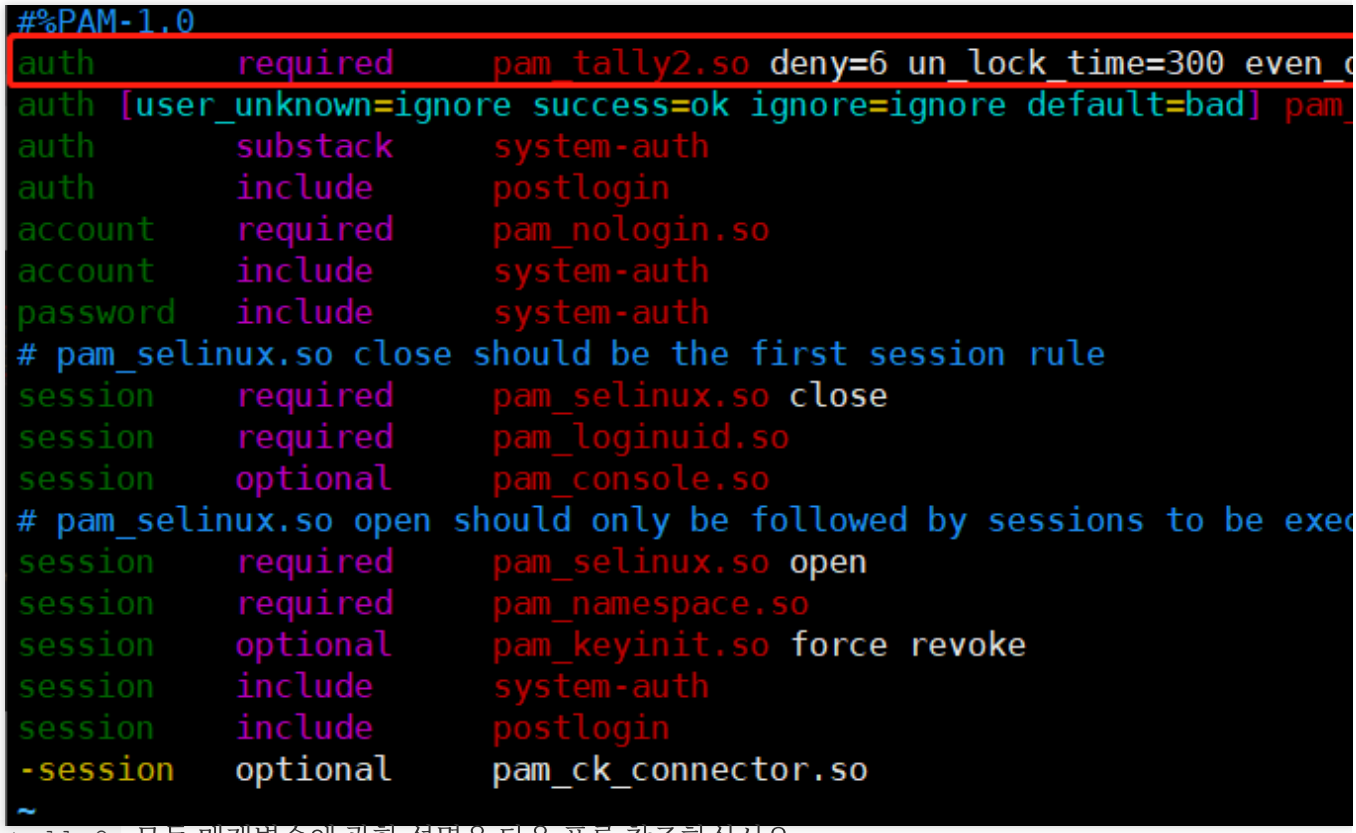
현상 설명

VNC로 CVM에 정상적으로 로그인할 수 없는 경우, 로그인 비밀번호를 입력하기 전에 'Account locked due to XXX failed logins'라는 오류 메시지가 나타납니다. 다음 이미지를 참고하십시오.



예상 원인

VNC로 로그인하면 `/etc/pam.d/login` 이라는 pam 모듈을 호출해 인증을 진행하고 login 구성 파일에 `pam_tally2.so` 모듈의 인증이 구성됩니다. `pam_tally2.so` 모듈의 기능은 Linux 사용자가 로그인 비밀번호를 N번 잘못 입력했을 때 자동으로 X분 동안 또는 영구적으로 잠금되도록 설정하는 것입니다. 그중 영구 잠금은 수동으로 암호를 해제해야 하며, 해제 전까지 잠금 상태가 유지됩니다.
로그인 실패 횟수가 설정 횟수를 초과하여 계정이 일정 시간동안 잠기거나, 무차별 대입 공격으로 계정이 잠기는 경우 로그인할 수 없습니다. 다음 이미지는 설정된 로그인 시도 가능 횟수입니다.



`pam_tally2` 모듈 매개변수에 관한 설명은 다음 표를 참조하십시오.

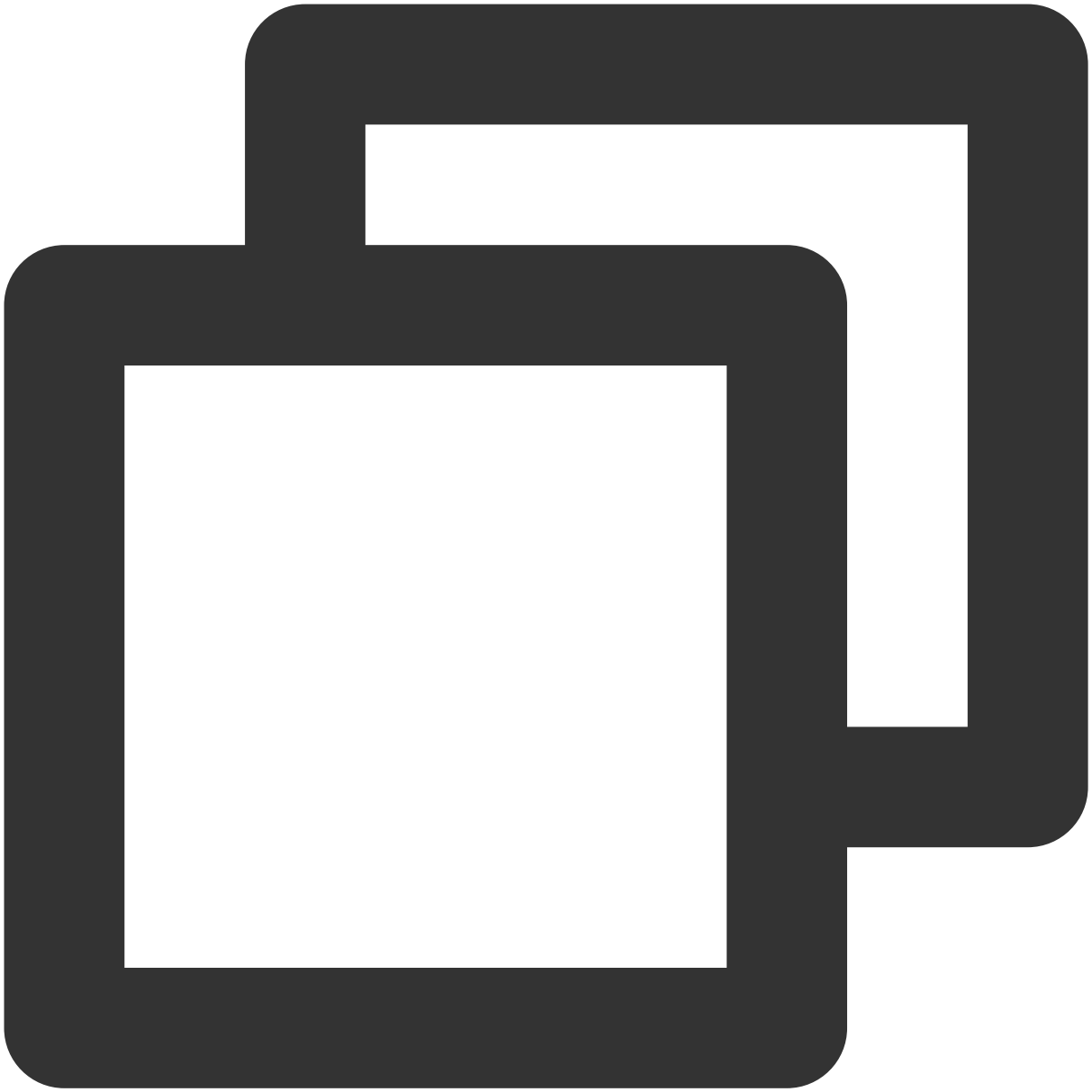
매개변수	설명
deny=n	로그인 실패 횟수가 n회 이상이면 액세스가 거부됩니다.
lock_time=n	로그인 실패 후 계정 잠금 시간(초)입니다.
un lock_time=n	로그인 실패 제한 횟수 초과 후 잠금 해제에 필요한 시간입니다.
no_lock_time	로그 파일/var/log/faillog에.fail_locktime필드를 기록하지 마십시오.
magic_root	root 사용자가(uid=0) 해당 모듈을 호출하면 카운터가 늘어나지 않습니다.
even_deny_root	root 사용자의 로그인 실패 횟수가 deny=n회 이상이면 액세스가 거부됩니다.
root_unlock_time=n	even_deny_root에 상응하는 옵션입니다. 해당 옵션 설정 시, root 사용자의 로그인 실패 횟수가 제한 횟수를 초과했을 때 잠기는 시간.

해결 방법

1. 작업 순서를 참조해 login 설정 파일에서 `pam_limits.so` 모듈 설정을 임시 주석 처리 합니다.
2. 계정이 잠긴 원인을 확인하고 보안 정책을 강화합니다.

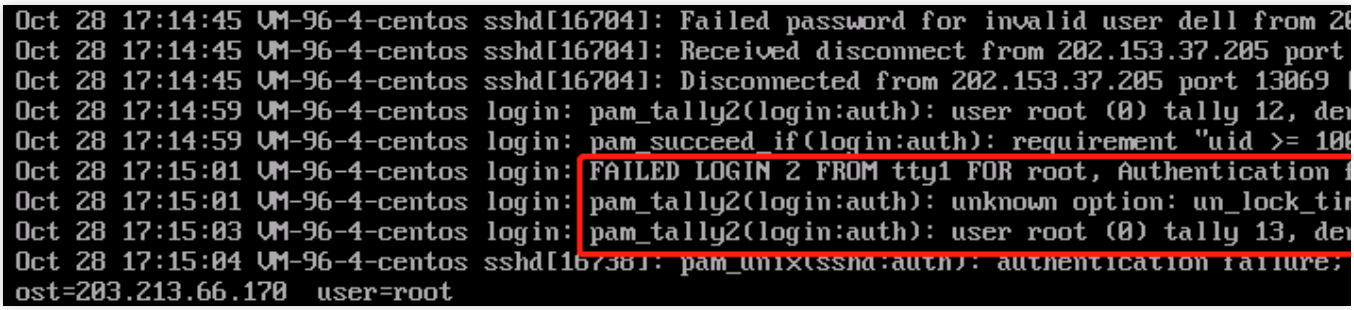
작업 순서

1. SSH를 사용하여 CVM에 로그인합니다. 자세한 내용은 SSH를 사용해 Linux 인스턴스에 로그인을 참조하십시오.
로그인에 성공하면 다음 단계를 실행합니다.
로그인에 실패하면 단독 사용자 모드를 사용해야 합니다.
2. 로그인 성공 후 다음 명령어를 실행하여 로그 정보를 조회하십시오.

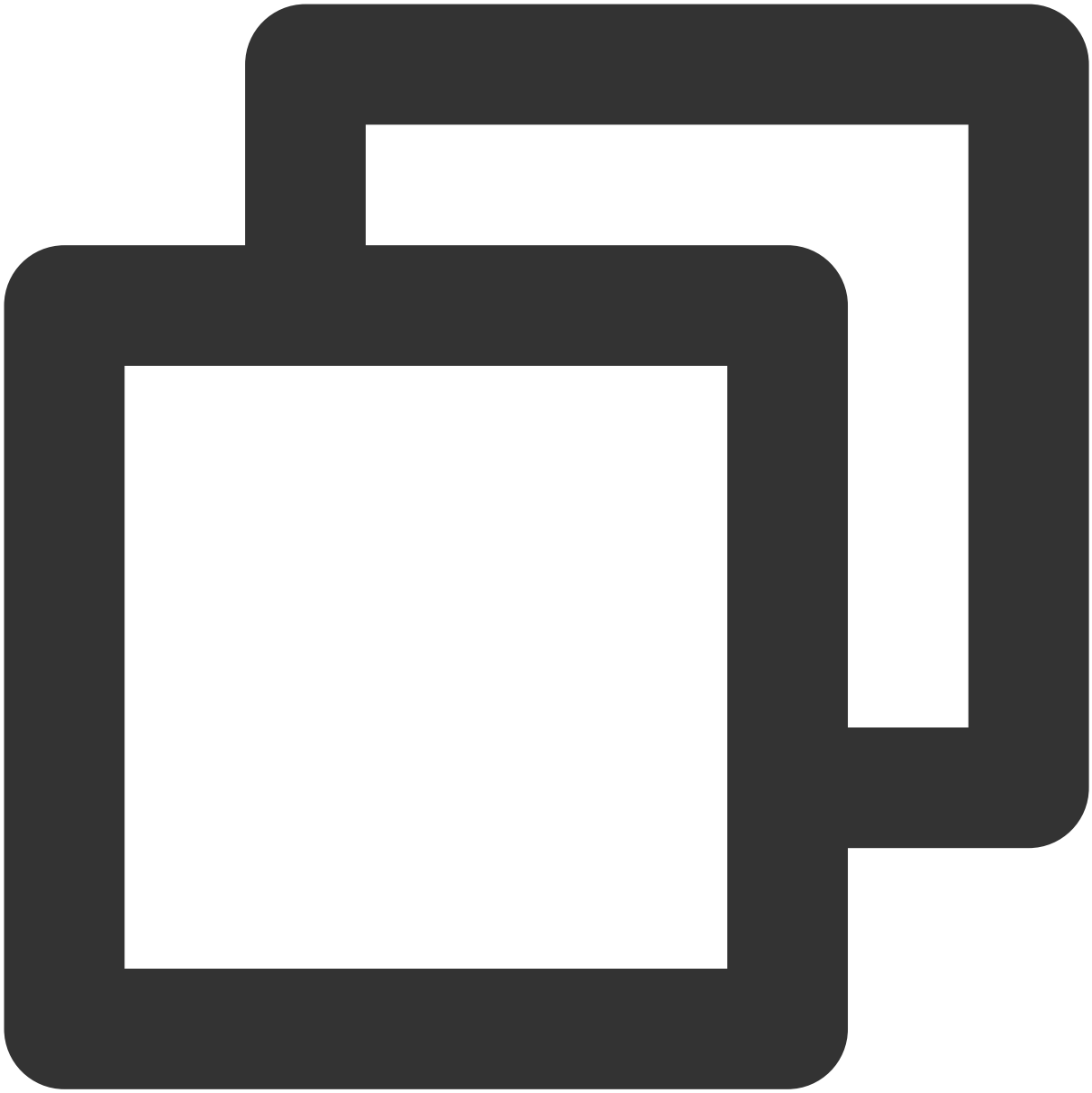


```
vim /var/log/secure
```

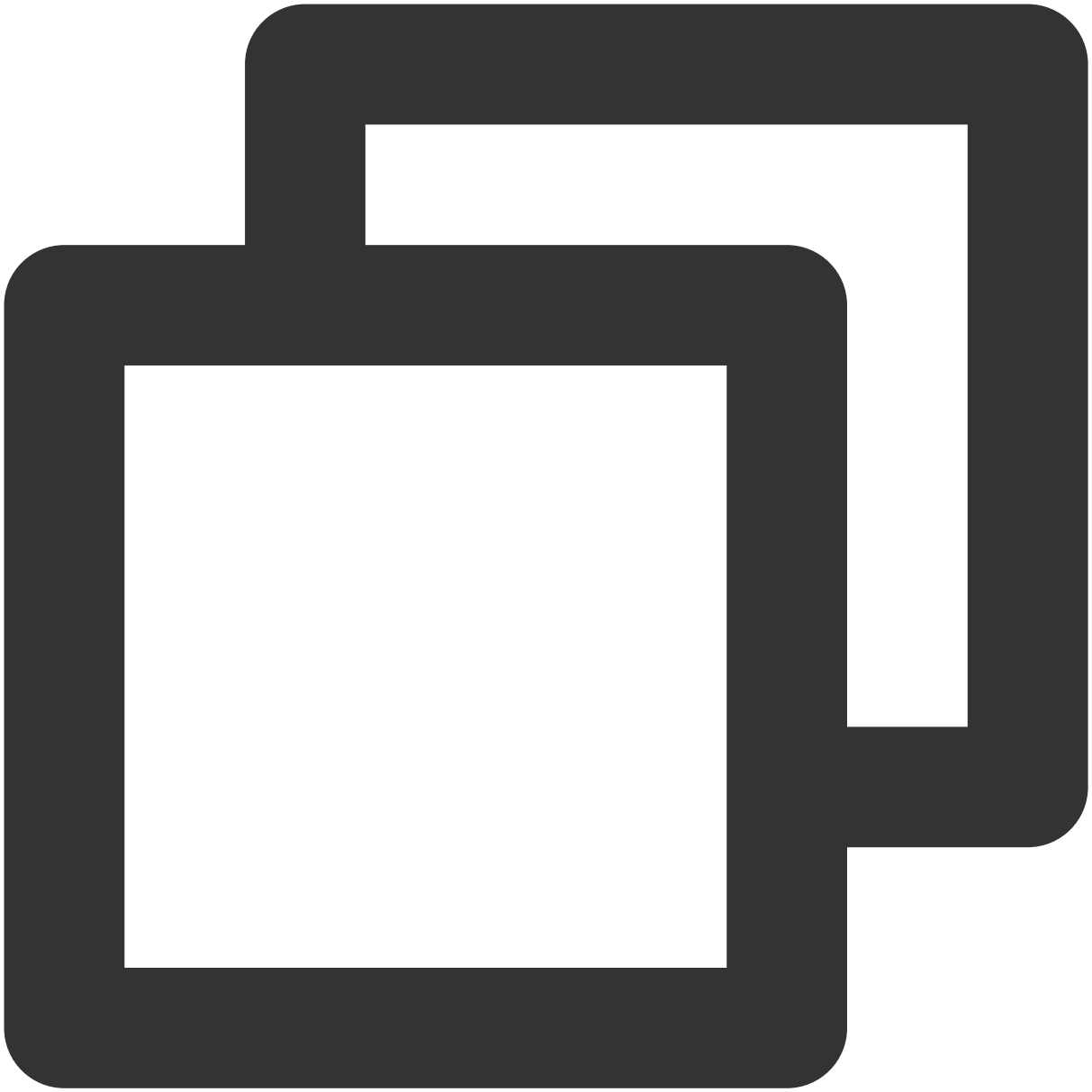
이 파일은 일반적으로 보안 관련 정보 기록에 사용되며, 대부분은 사용자의 CVM 로그인 관련 로그입니다. 다음 이미지와 같이 정보 중에서 `pam_tally2` 가 있는 오류 보고 정보를 가져올 수 있습니다.



3. 다음 명령어를 차례대로 실행하여 `/etc/pam.d` 로 들어간 뒤, 로그에서 오류 보고 pam 모듈의 키워드 `pam_tally2` 를 검색합니다.



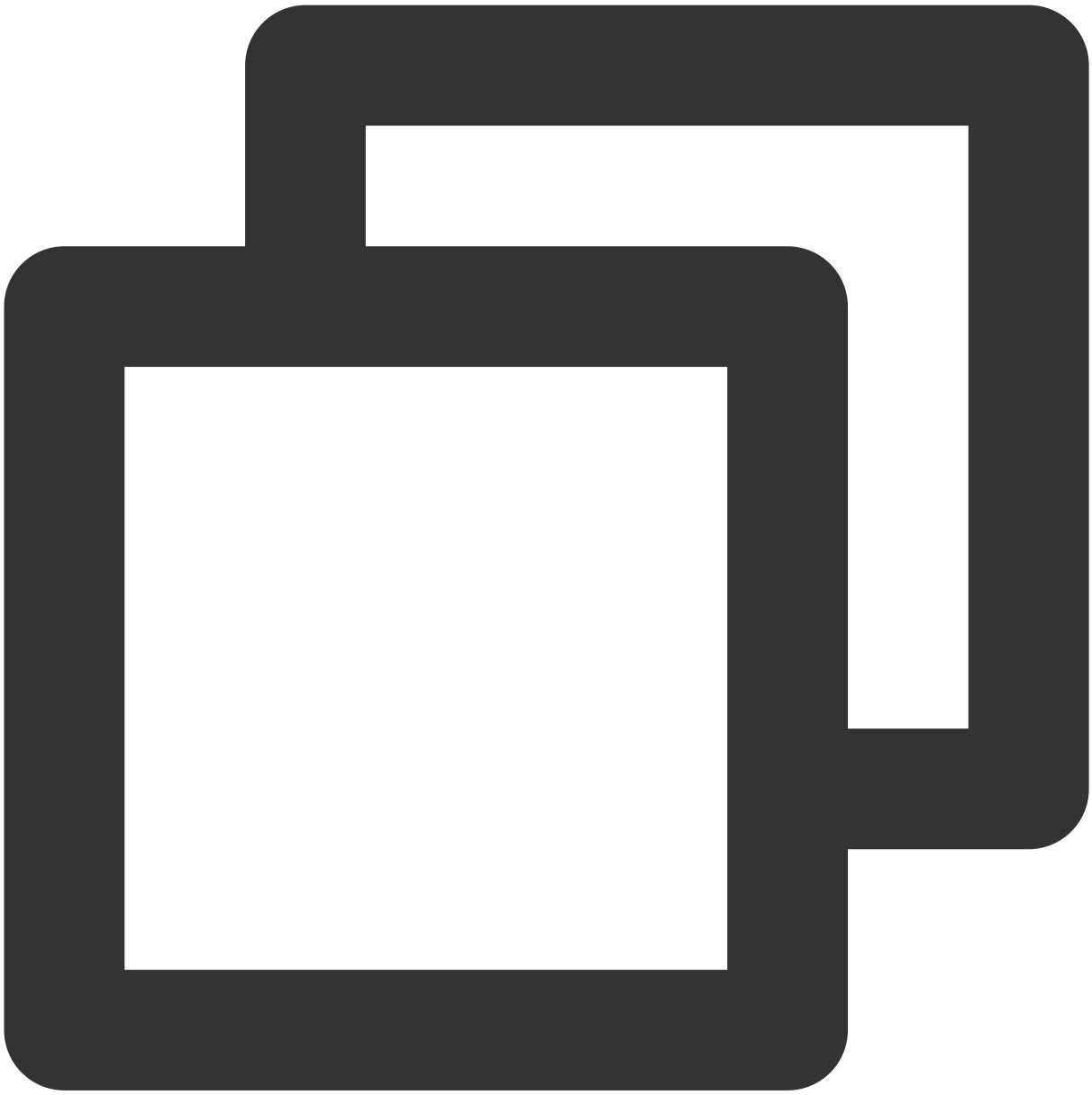
```
cd /etc/pam.d
```



```
find . | xargs grep -ri "pam_tally2" -l
```

다음 이미지와 같은 정보가 반환되면 `login` 파일에 해당 파라미터가 설정되었음을 의미합니다.

4. 다음 명령어를 실행하여 `pam_tally2.so` 모듈 설정을 임시 주석 처리합니다. 설정이 완료되면 다시 로그인이 가능합니다.



```
sed -i "s/.*pam_tally.*/#&/" /etc/pam.d/login
```

5. 계정 잠김이 사용자의 조작 오류 때문인지 무차별 대입 공격 때문인지 확인합니다. 무차별 대입 공격이 원인인 경우 다음과 같은 방법으로 보안 정책을 강화하시기 바랍니다.
CVM 비밀번호를 수정합니다. 비밀번호는 대문자, 소문자, 특수 부호, 숫자로 구성된 12-16자리의 복잡하고 임의적인 비밀번호로 설정하십시오. 자세한 내용은 인스턴스 비밀번호 재설정을 참조하십시오.
CVM에서 사용하지 않는 사용자를 삭제합니다.

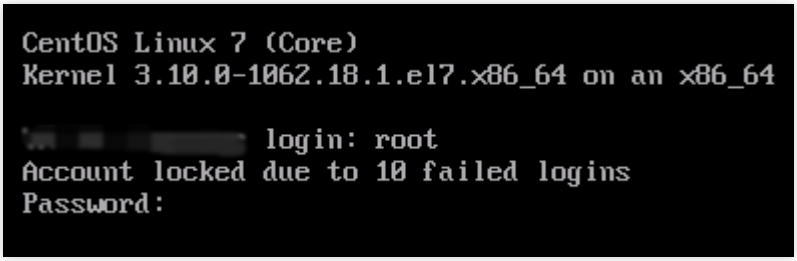
sshd의 기본 포트 22를 1024-65525 사이의 자주 사용하지 않는 포트로 변경합니다. 자세한 방식은 CVM 원격 기본 포트 수정을 참조하십시오.
CVM과 연결된 보안 그룹의 규칙을 관리하기 위해서는 서비스와 프로토콜에 필요한 포트만 개방하면 되며, 모든 프로토콜과 포트를 개방하는 것은 권장하지 않습니다. 자세한 내용은 보안 그룹 규칙 추가를 참조하십시오.
공용 네트워크에 핵심 애플리케이션 서비스 포트의 액세스를 개방하는 것은 권장하지 않습니다. 예시: mysql, redis 등 관련 포트를 로컬 액세스 또는 공인 네트워크 액세스 금지로 변경할 수 있습니다.
HS, yunsuo 등 보안 소프트웨어를 설치하고 실시간 알람을 추가하여 비정상적인 로그인 정보를 즉각적으로 수집할 수 있습니다.

Linux 인스턴스:VNC 로그인 오류 알림 Account locked due to XXX failed logins

최종 업데이트 날짜: : 2024-02-02 11:09:48

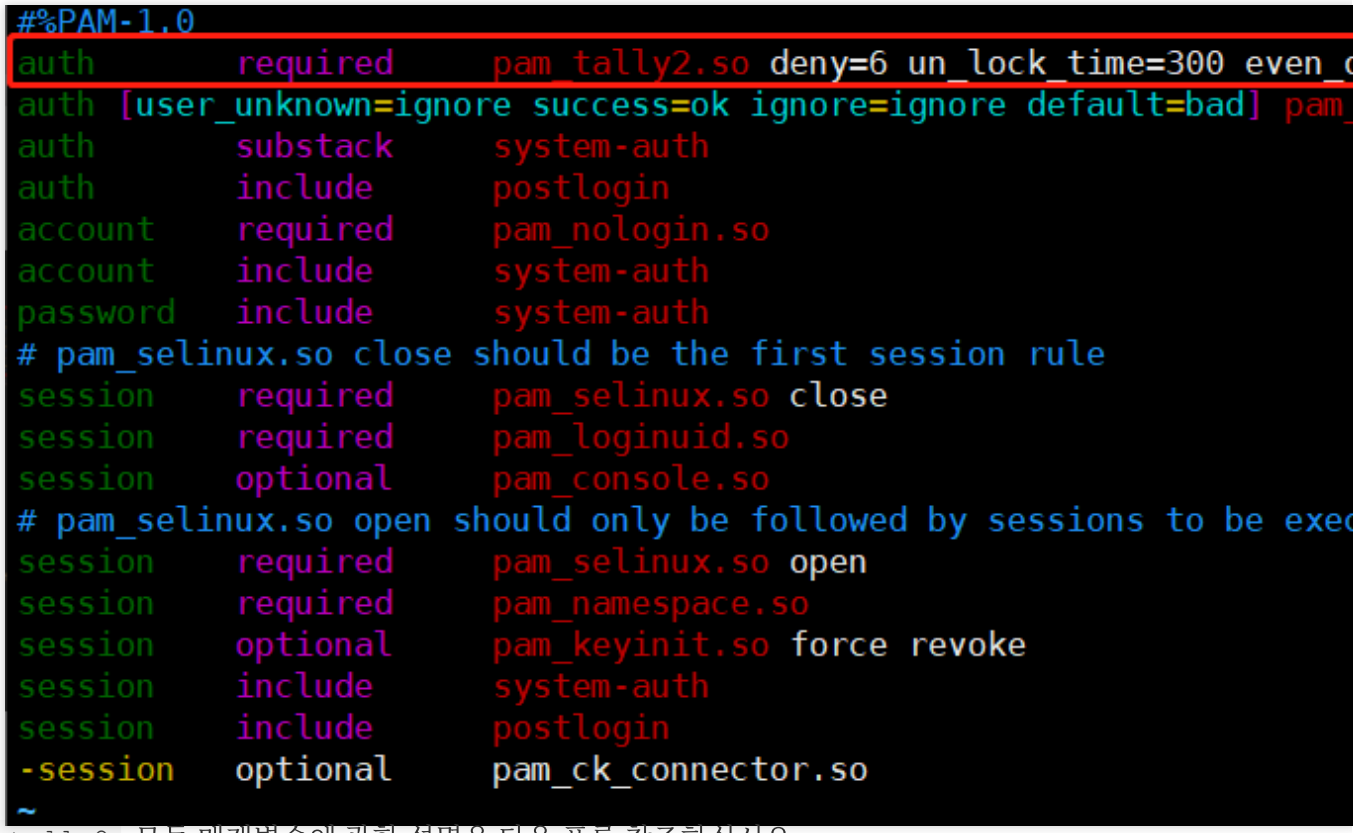
현상 설명

VNC로 CVM에 정상적으로 로그인할 수 없는 경우, 로그인 비밀번호를 입력하기 전에 'Account locked due to XXX failed logins'라는 오류 메시지가 나타납니다. 다음 이미지를 참고하십시오.



예상 원인

VNC로 로그인하면 `/etc/pam.d/login` 이라는 pam 모듈을 호출해 인증을 진행하고 login 구성 파일에 `pam_tally2.so` 모듈의 인증이 구성됩니다. `pam_tally2.so` 모듈의 기능은 Linux 사용자가 로그인 비밀번호를 N번 잘못 입력했을 때 자동으로 X분 동안 또는 영구적으로 잠금되도록 설정하는 것입니다. 그중 영구 잠금은 수동으로 암호를 해제해야 하며, 해제 전까지 잠금 상태가 유지됩니다.
로그인 실패 횟수가 설정 횟수를 초과하여 계정이 일정 시간동안 잠기거나, 무차별 대입 공격으로 계정이 잠기는 경우 로그인할 수 없습니다. 다음 이미지는 설정된 로그인 시도 가능 횟수입니다.



`pam_tally2` 모듈 매개변수에 관한 설명은 다음 표를 참조하십시오.

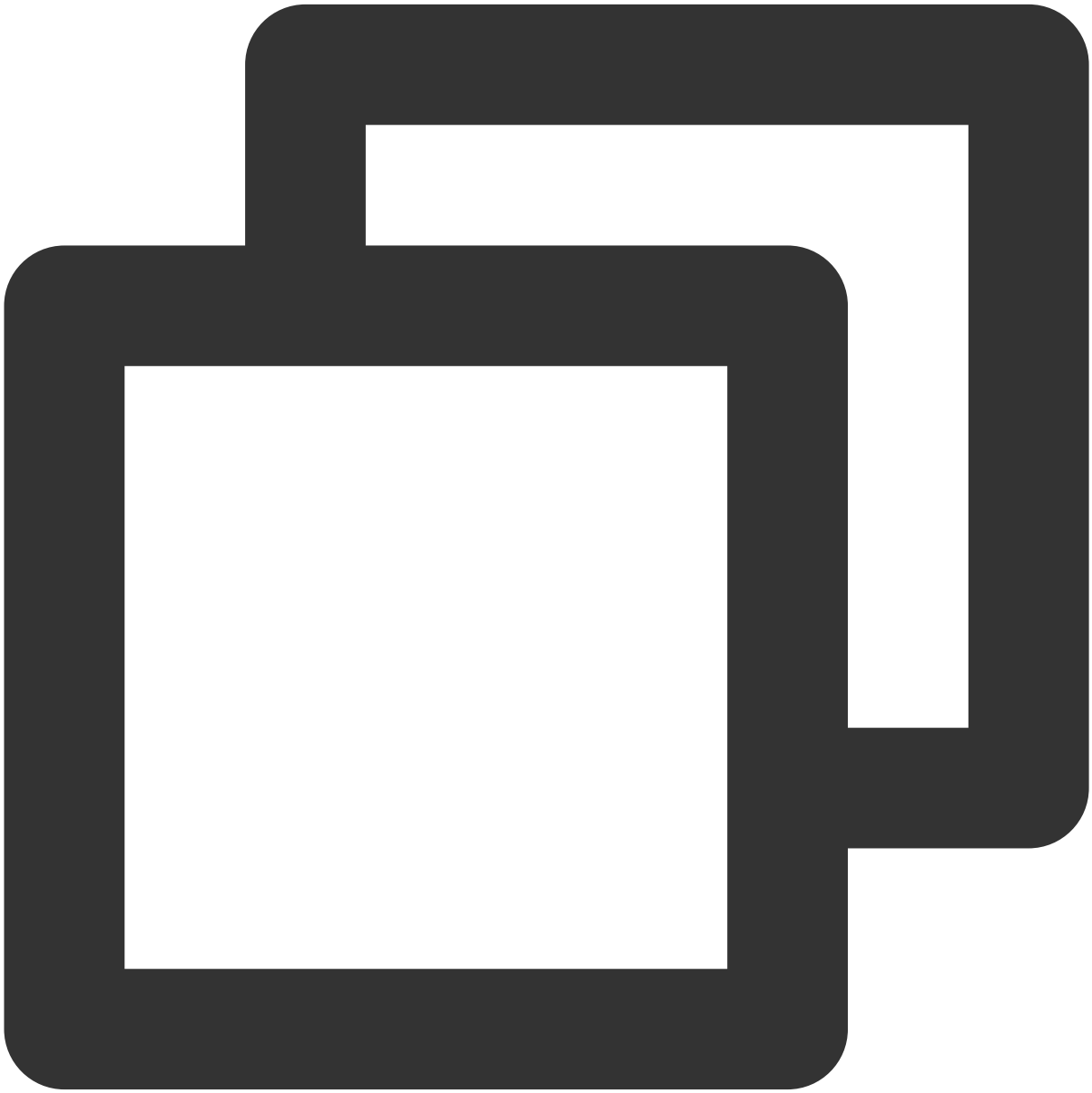
매개변수	설명
deny=n	로그인 실패 횟수가 n회 이상이면 액세스가 거부됩니다.
lock_time=n	로그인 실패 후 계정 잠금 시간(초)입니다.
un lock_time=n	로그인 실패 제한 횟수 초과 후 잠금 해제에 필요한 시간입니다.
no_lock_time	로그 파일/var/log/faillog에.fail_locktime필드를 기록하지 마십시오.
magic_root	root 사용자가(uid=0) 해당 모듈을 호출하면 카운터가 늘어나지 않습니다.
even_deny_root	root 사용자의 로그인 실패 횟수가 deny=n회 이상이면 액세스가 거부됩니다.
root_unlock_time=n	even_deny_root에 상응하는 옵션입니다. 해당 옵션 설정 시, root 사용자의 로그인 실패 횟수가 제한 횟수를 초과했을 때 잠기는 시간.

해결 방법

1. 작업 순서를 참조해 login 설정 파일에서 `pam_limits.so` 모듈 설정을 임시 주석 처리 합니다.
2. 계정이 잠긴 원인을 확인하고 보안 정책을 강화합니다.

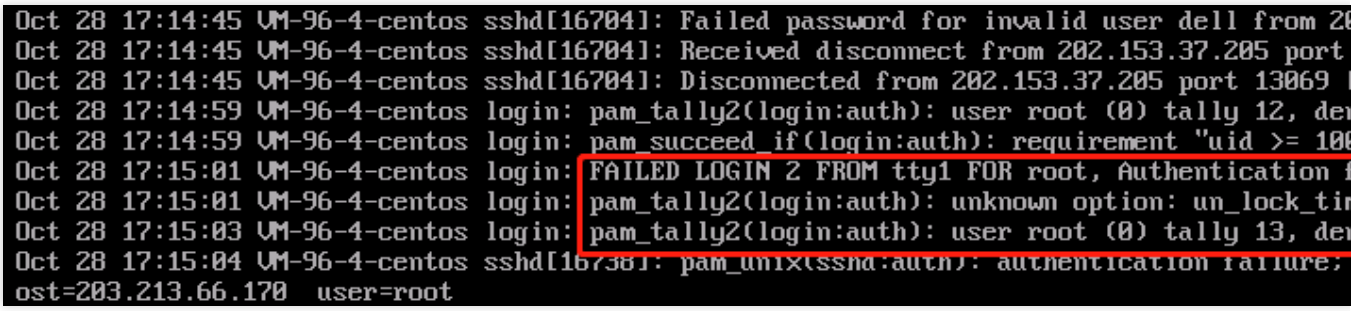
작업 순서

1. SSH를 사용하여 CVM에 로그인합니다. 자세한 내용은 SSH를 사용해 Linux 인스턴스에 로그인을 참조하십시오.
로그인에 성공하면 다음 단계를 실행합니다.
로그인에 실패하면 단독 사용자 모드를 사용해야 합니다.
2. 로그인 성공 후 다음 명령어를 실행하여 로그 정보를 조회하십시오.

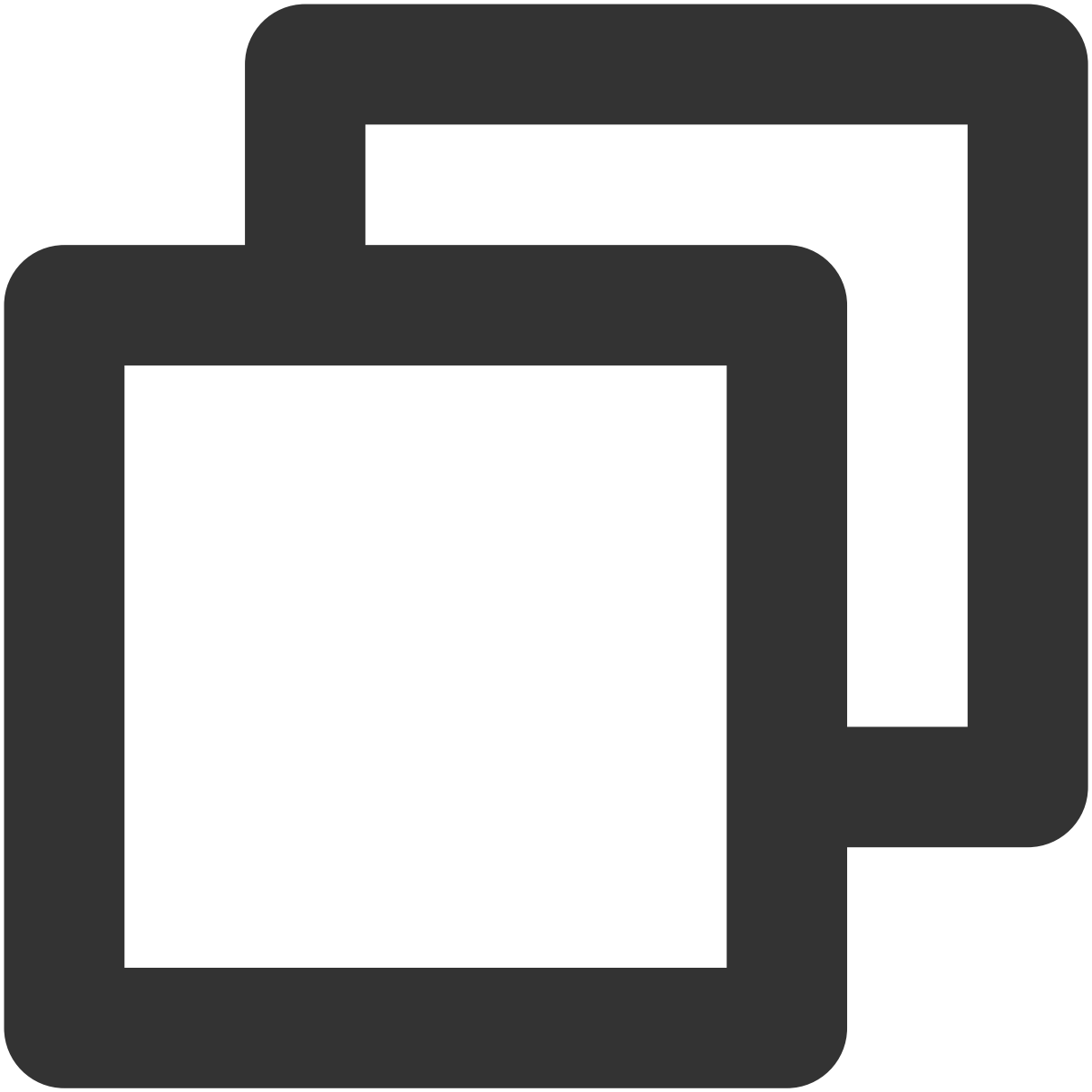


```
vim /var/log/secure
```

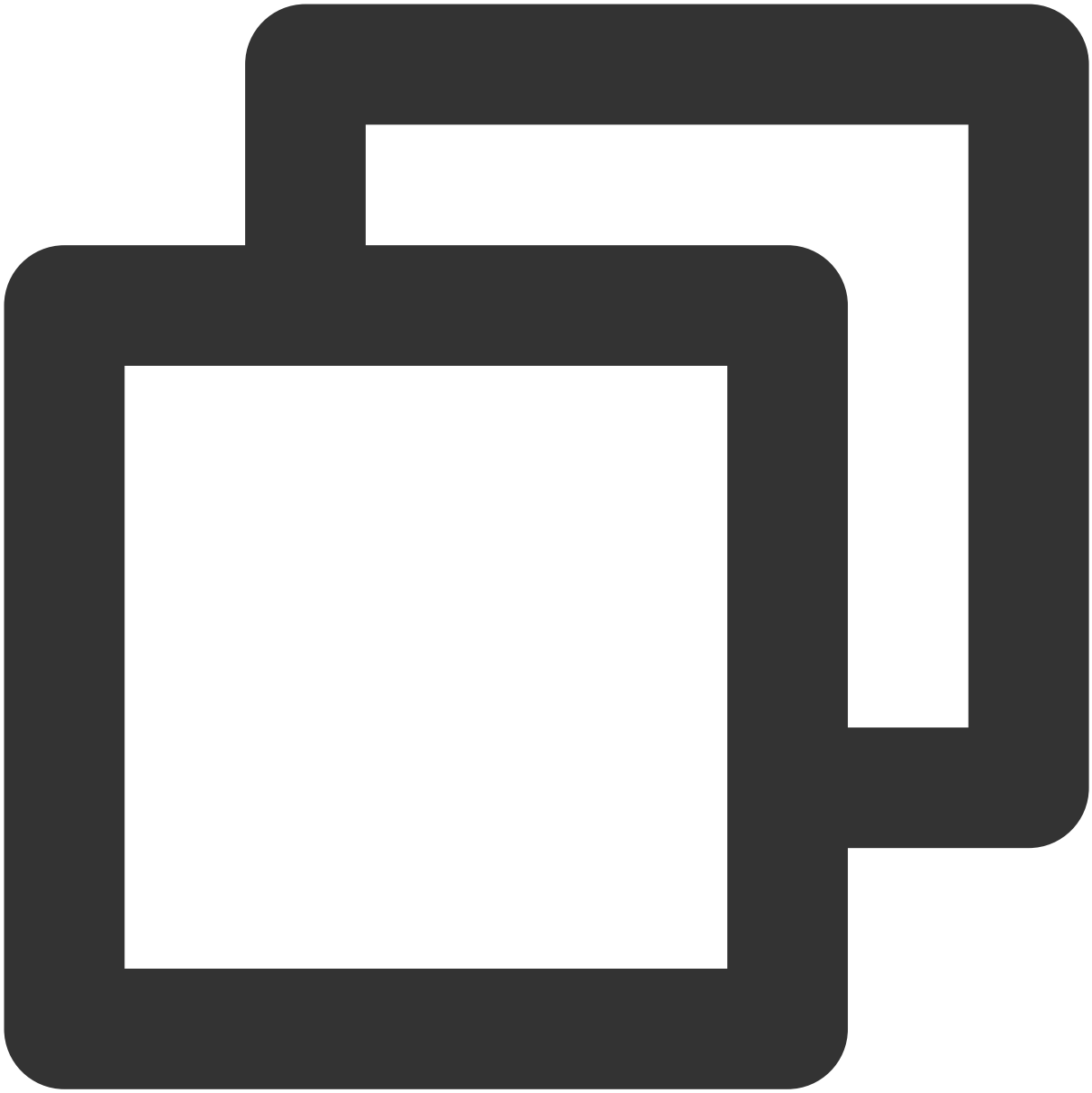
이 파일은 일반적으로 보안 관련 정보 기록에 사용되며, 대부분은 사용자의 CVM 로그인 관련 로그입니다. 다음 이미지와 같이 정보 중에서 `pam_tally2` 가 있는 오류 보고 정보를 가져올 수 있습니다.



3. 다음 명령어를 차례대로 실행하여 `/etc/pam.d` 로 들어간 뒤, 로그에서 오류 보고 pam 모듈의 키워드 `pam_tally2` 를 검색합니다.



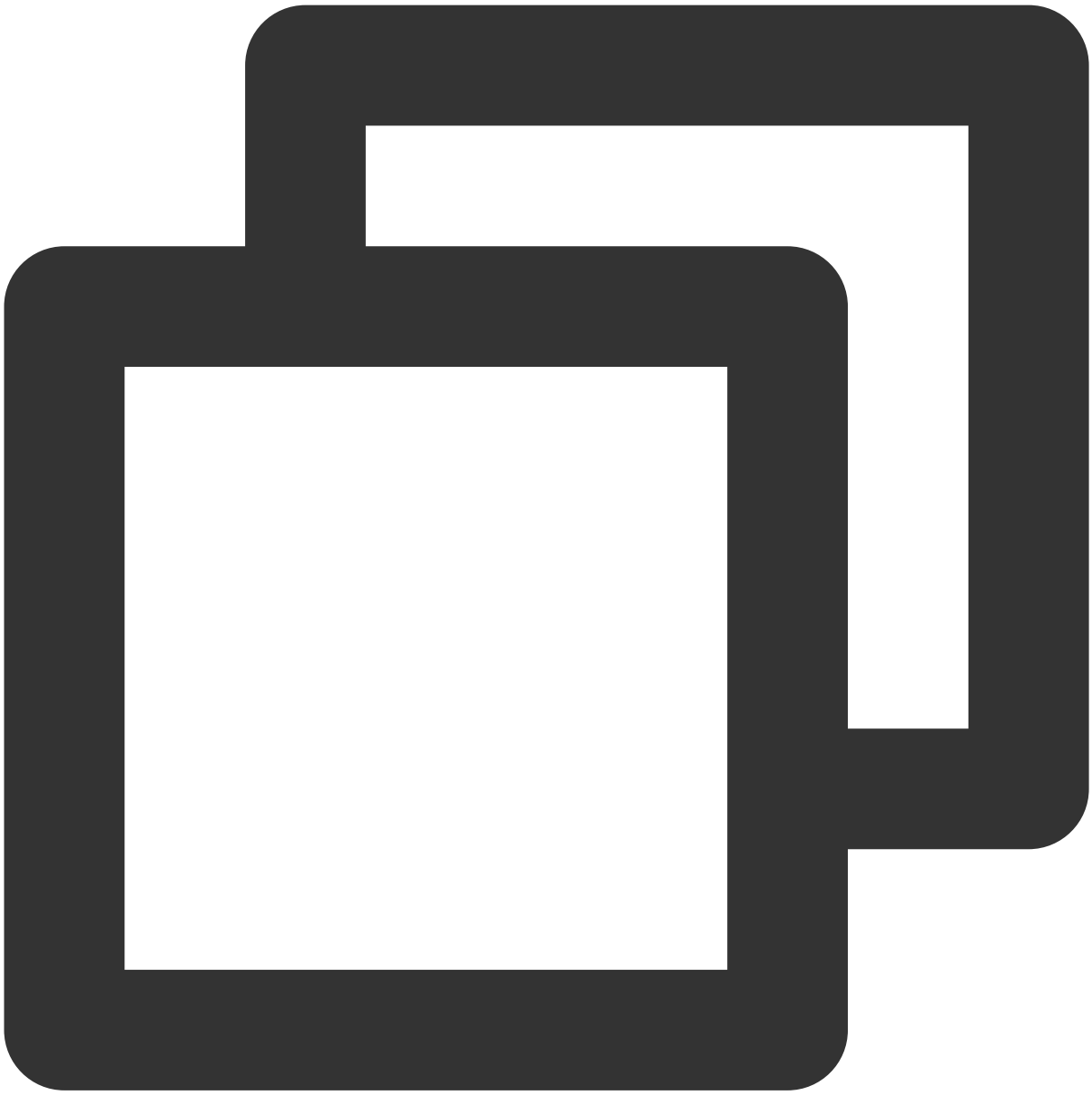
```
cd /etc/pam.d
```



```
find . | xargs grep -ri "pam_tally2" -l
```

다음 이미지와 같은 정보가 반환되면 `login` 파일에 해당 파라미터가 설정되었음을 의미합니다.

4. 다음 명령어를 실행하여 `pam_tally2.so` 모듈 설정을 임시 주석 처리합니다. 설정이 완료되면 다시 로그인이 가능합니다.



```
sed -i "s/.*pam_tally.*/#&/" /etc/pam.d/login
```

5. 계정 잠김이 사용자의 조작 오류 때문인지 무차별 대입 공격 때문인지 확인합니다. 무차별 대입 공격이 원인인 경우 다음과 같은 방법으로 보안 정책을 강화하시기 바랍니다.
CVM 비밀번호를 수정합니다. 비밀번호는 대문자, 소문자, 특수 부호, 숫자로 구성된 12-16자리의 복잡하고 임의적인 비밀번호로 설정하십시오. 자세한 내용은 인스턴스 비밀번호 재설정을 참조하십시오.
CVM에서 사용하지 않는 사용자를 삭제합니다.

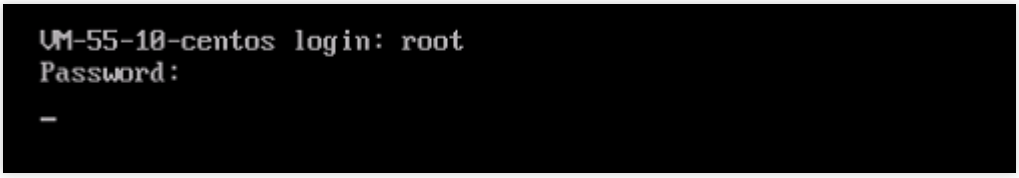
sshd의 기본 포트 22를 1024-65525 사이의 자주 사용하지 않는 포트로 변경합니다. 자세한 방식은 CVM 원격 기본 포트 수정을 참조하십시오.
CVM과 연결된 보안 그룹의 규칙을 관리하기 위해서는 서비스와 프로토콜에 필요한 포트만 개방하면 되며, 모든 프로토콜과 포트를 개방하는 것은 권장하지 않습니다. 자세한 내용은 보안 그룹 규칙 추가를 참조하십시오.
공용 네트워크에 핵심 애플리케이션 서비스 포트의 액세스를 개방하는 것은 권장하지 않습니다. 예시: mysql, redis 등 관련 포트를 로컬 액세스 또는 공인 네트워크 액세스 금지로 변경할 수 있습니다.
HS 등 보안 소프트웨어를 설치하고 실시간 알람을 추가하여 비정상적인 로그인 정보를 즉각적으로 수집할 수 있습니다.

Linux 인스턴스:VNC 로그인 시 정확한 비밀번호 입력 후 응답 없음

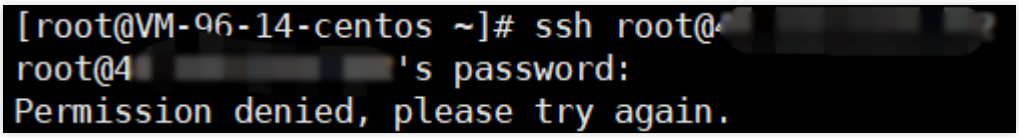
최종 업데이트 날짜: : 2024-02-02 11:09:47

현상 설명

VNC로 CVM에 로그인 시, 정확한 비밀번호를 입력하여도 로그인이 안 되고, 다음 이미지와 같은 인터페이스에서 멈출 수 있습니다. 잠시 후 다시 계정을 입력하라는 안내 메시지가 나타납니다.

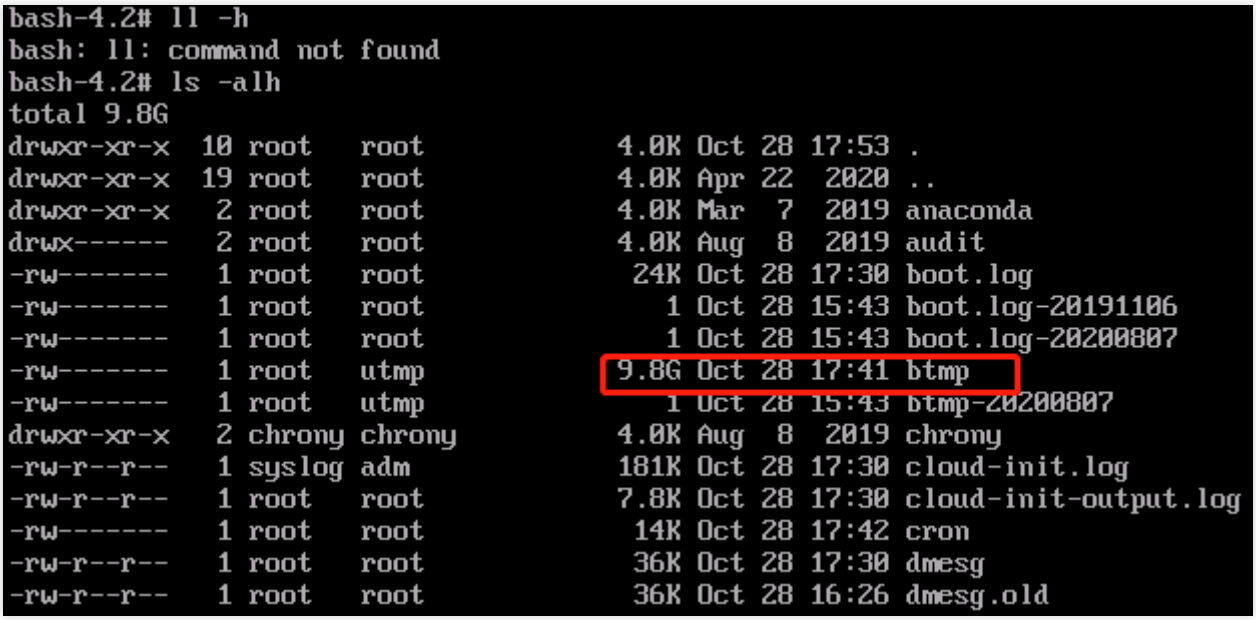


또한 SSH로 원격 로그인 시 “Permission denied, please try again.”이라는 오류 메시지가 나타날 수 있습니다. 다음 이미지를 참고하십시오.



가능한 원인

잦은 무차별 대입 공격으로 인하여 `/var/log/btmp` 로그 용량이 과도하게 늘어났을 가능성이 있습니다. 해당 파일은 로그인 오류 로그를 기록하는 데 사용되며, 용량이 너무 크면 비정상적인 로그인으로 로그에 기록되어 정상적인 로그인이 불가합니다. 다음 이미지를 참고하십시오.

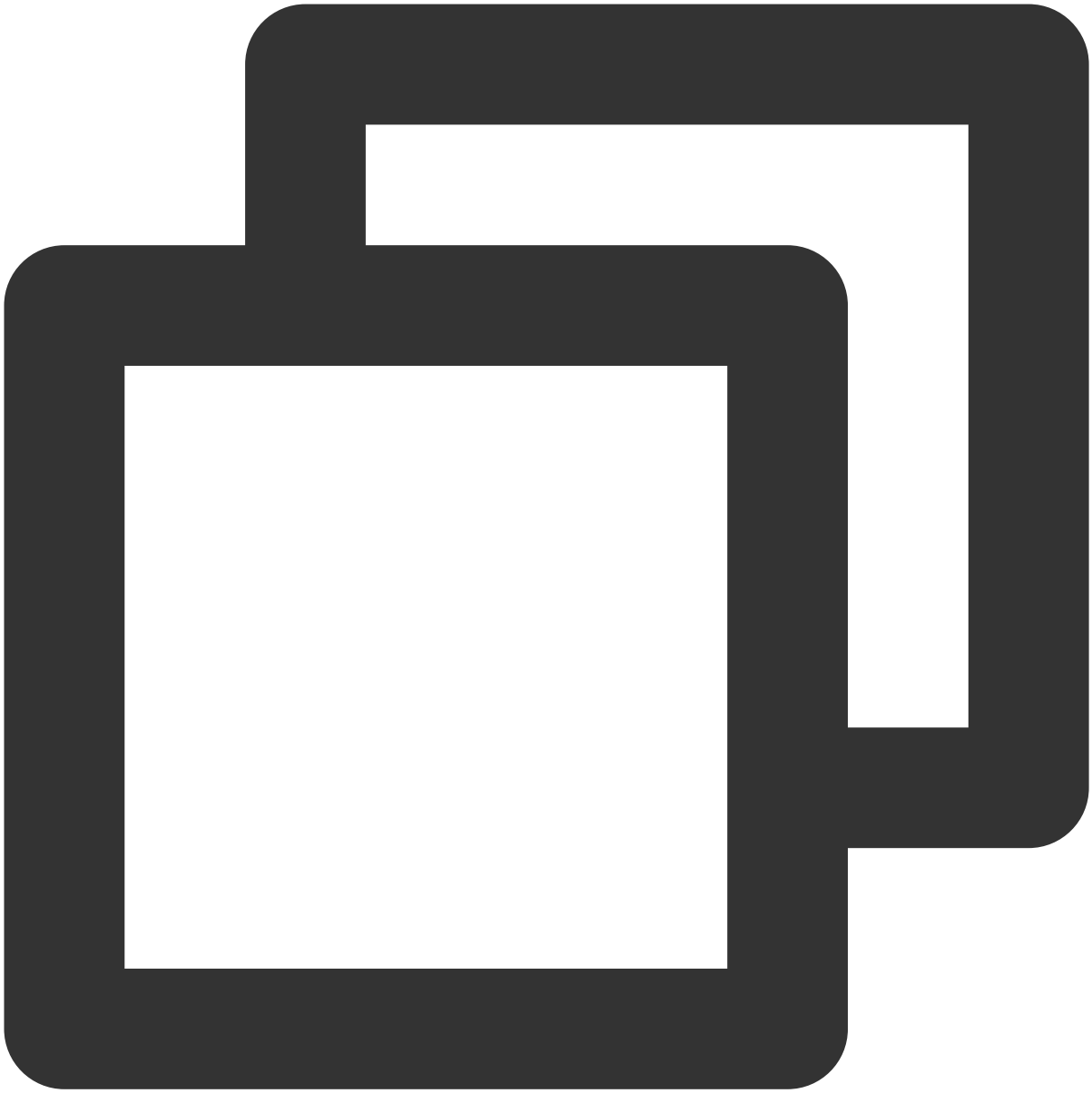


해결 방식

1. 작업 순서를 참조하여 로그 파일 `/var/log/btmp` 의 용량이 너무 크지 않은지 확인합니다.
2. 무차별 대입 공격이 원인인지 확인하고 보안 정책을 강화합니다.

처리 순서

1. SSH를 사용하여 CVM에 로그인해보십시오. 자세한 내용은 SSH를 사용하여 Linux 인스턴스에 로그인을 참조하십시오.
로그인에 성공하면 다음 단계를 실행합니다.
로그인 실패 시, 단일 사용자 모드를 사용해야 합니다. 자세한 내용은 콘솔을 통한 Linux 인스턴스 단일 사용자 모드 진입을 참조하십시오.
2. `/var/log` 로 들어가 로그 파일 `/var/log/btmp` 의 용량을 확인합니다.
3. 로그 파일 `/var/log/btmp` 의 용량이 너무 크면 다음 명령어를 실행하여 btmp 로그 내용을 비웁니다. 로그 파일을 비우고 나면 다시 로그인이 가능합니다.



```
cat /dev/null > /var/log/btmp
```

4. 계정 잠김이 사용자의 조작 오류 때문인지 무차별 대입 공격 때문인지 확인합니다. 무차별 대입 공격이 원인인 경우 다음과 같은 방법으로 보안 정책을 강화하시기 바랍니다.
CVM 비밀번호를 수정합니다. 비밀번호는 대문자, 소문자, 특수 부호, 숫자로 구성된 12-16자리의 복잡하고 임의적인 비밀번호로 설정하십시오. 자세한 내용은 인스턴스 비밀번호 재설정을 참조하십시오.
CVM에서 사용하지 않는 사용자를 삭제합니다.
sshd의 기본 포트 22를 1024-65525 사이의 자주 사용하지 않는 포트로 변경합니다. 자세한 방식은 CVM 원격 기본 포트 수정을 참조하십시오.

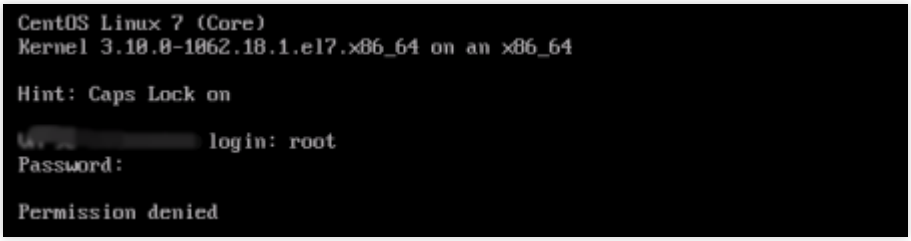
CVM과 연결된 보안 그룹의 규칙을 관리하기 위해서는 서비스와 프로토콜에 필요한 포트만 개방하면 되며, 모든 프로토콜과 포트를 개방하는 것은 권장하지 않습니다. 자세한 내용은 보안 그룹 규칙 추가를 참조하십시오.
공용 네트워크에 핵심 애플리케이션 서비스 포트의 액세스를 개방하는 것은 권장하지 않습니다. 예시: mysql, redis 등 관련 포트를 로컬 액세스 또는 외부 네트워크 액세스 금지로 변경할 수 있습니다.
HS, YUNSUO 등 보안 소프트웨어를 설치하고 실시간 알람을 추가하면 비정상적인 로그인 정보를 즉각적으로 수신할 수 있습니다.

Linux 인스턴스:VNC 또는 SSH 로그인 오류 알림 Permission denied

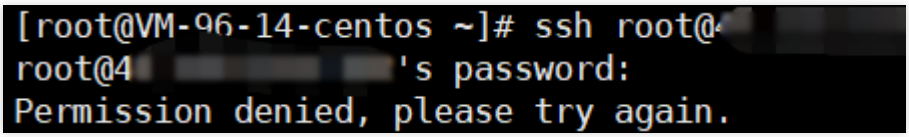
최종 업데이트 날짜: : 2024-02-02 11:09:48

현상 설명

VNC 또는 SSH로 로그인 시 “Permission denied”라는 오류 알림이 나타납니다.
VNC 로그인 오류 알림은 다음 이미지를 참고하십시오.

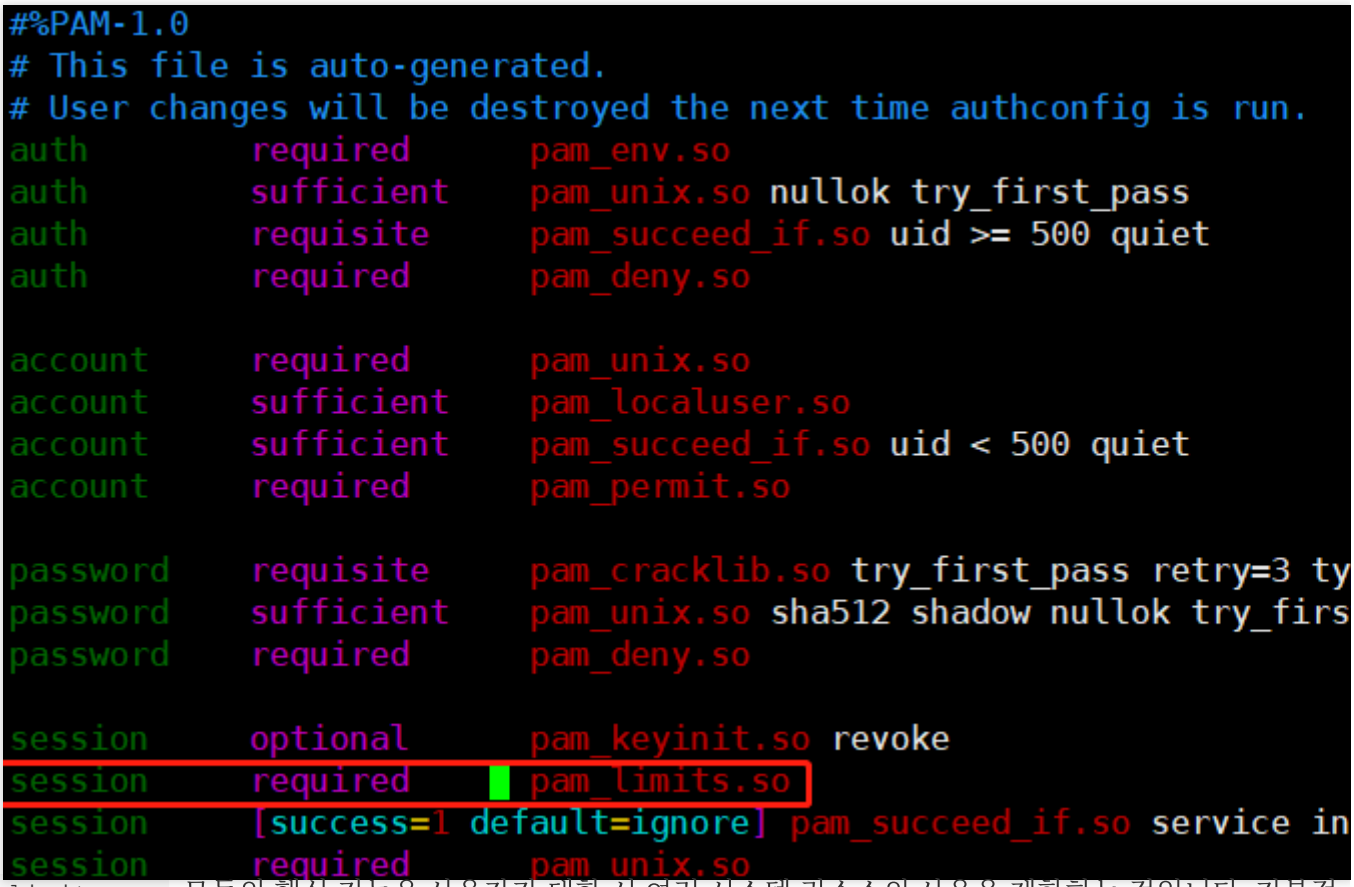


SSH 로그인 오류 알림은 다음 이미지를 참고하십시오.



예상 원인

VNC 또는 SSH로 로그인하면 `/etc/pam.d/login` 이라는 pam 모듈을 호출해 인증을 진행하고, `/etc/pam.d/login` 구성에서 기본적으로 `system-auth` 모듈을 가져와 인증을 진행합니다. 그러면 `system-auth` 모듈은 기본적으로 `pam_limits.so` 모듈을 가져와 인증을 진행합니다. `system-auth` 의 기본 구성은 다음 이미지를 참고하십시오.



`pam_limits.so` 모듈의 핵심 기능은 사용자가 대화 시 여러 시스템 리소스의 사용을 제한하는 것입니다. 기본적으로 해당 모듈의 구성 파일은 `/etc/security/limits.conf` 로, 해당 구성 파일은 사용자가 사용 가능한 최대 파일 갯수, 최대 스레드 수, 최대 메모리 등 리소스 사용량을 규정하고 있습니다. 매개변수에 대한 설명은 다음 표와 같습니다.

매개변수	설명
soft nofile	열 수 있는 최대 파일 기술자 수 입니다(soft limits).
hard nofile	열 수 있는 최대 파일 기술자 수로(hard limits), 해당 설정값을 초과할 수 없습니다.
fs.file-max	시스템 수준에서 열 수 있는 파일 핸들(커널의 struct file)의 수량입니다. 사용자에 대한 제한이 아닌 전체 시스템에 대한 제한입니다.
fs.nr_open	개별 프로세스에서 할당할 수 있는 최대 파일 기술자 수(fd 개수).

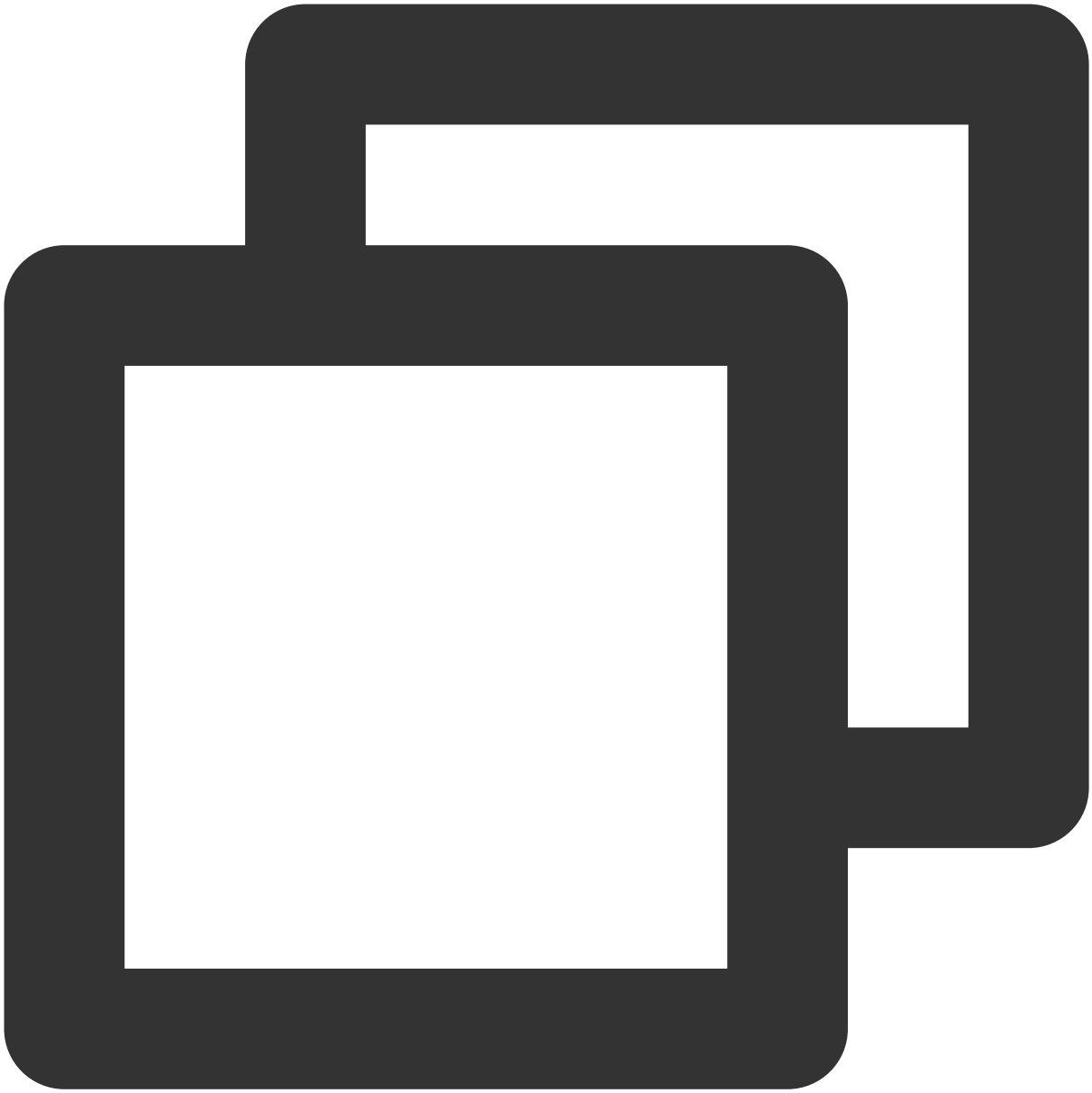
정상적으로 로그인할 수 없는 원인은 구성 파일 `/etc/security/limits.conf` 에서 root 사용자가 열 수 있는 최대 파일 기술자 수의 개수 설정에 오류가 있기 때문일 수 있습니다. 올바른 구성은 `soft nofile ≤ hard nofile ≤ fs.nr_open` 의 관계에 부합해야 합니다.

해결 방법

작업 순서를 참조해 `soft nofile` , `hard nofile` 및 `fs.nr_open` 을 올바른 구성으로 수정합니다.

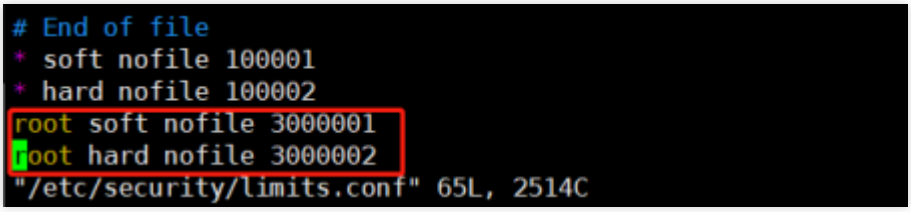
작업 순서

1. SSH를 사용하여 CVM에 로그인합니다. 자세한 내용은 SSH를 사용해 Linux 인스턴스에 로그인을 참조하십시오.
로그인에 성공하면 다음 단계를 실행합니다.
로그인에 실패하면 단독 사용자 모드를 사용해야 합니다.
2. `soft nofile` , `hard nofile` 및 `fs.nr_open` 의 매개변수 값이 `soft nofile ≤ hard nofile ≤ fs.nr_open` 관계에 부합하는지 확인합니다.
다음 명령어를 실행하고 `soft nofile` 및 `hard nofile` 값을 확인합니다.

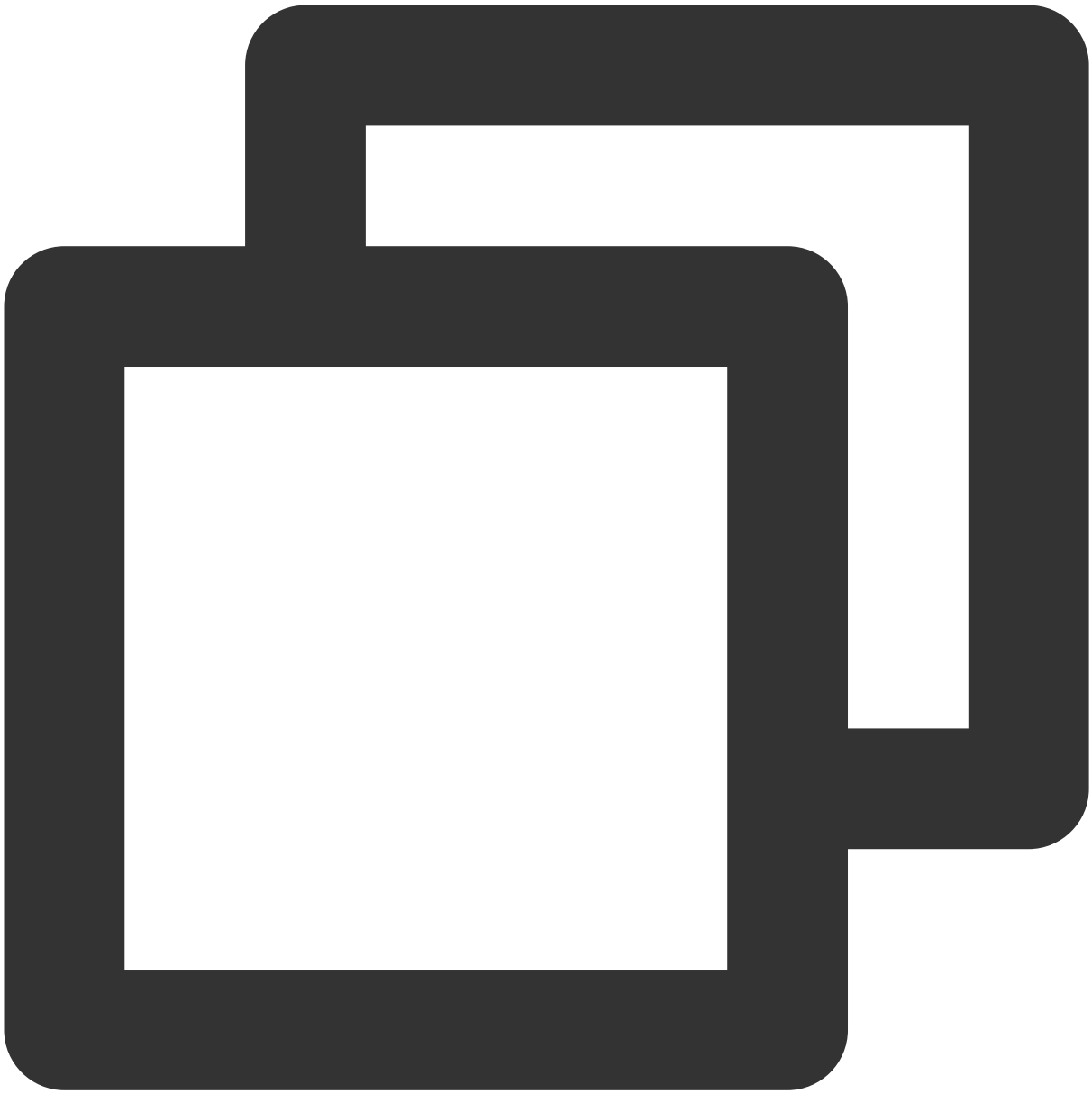


```
/etc/security/limits.conf
```

본 문서에서 도출한 결과값은 3000001과 3000002입니다. 다음 이미지를 참고하십시오.

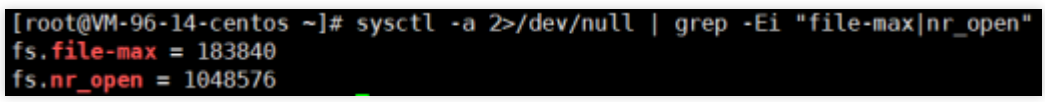


다음 명령어를 실행하여 `fs.nr_open` 값을 조회하십시오.



```
sysctl -a 2>/dev/null | grep -Ei "file-max|nr_open"
```

본 문서에서 도출한 결과값은 1048576입니다. 다음 이미지를 참고하십시오.



3. `/etc/security/limits.conf` 파일을 수정하고, 파일 끝에 다음과 같은 구성을 추가하거나 수정합니다.

`root soft nofile` : 100001

`root hard nofile` : 100002

4. `/etc/sysctl.conf` 파일을 수정하고, 파일 끝에 다음과 같은 구성을 추가하거나 수정합니다.

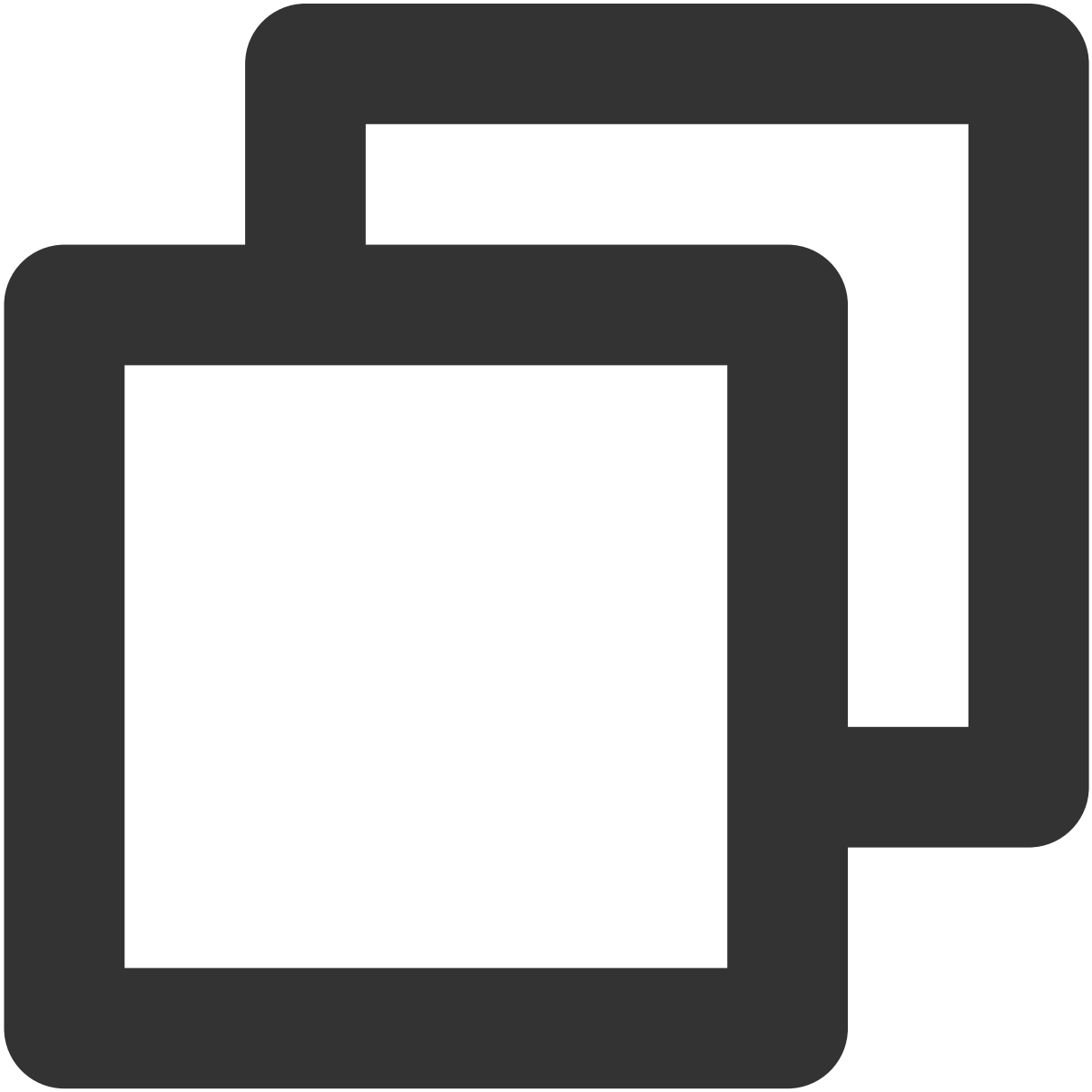
설명 :

`soft nofile ≤ hard nofile ≤ fs.nr_open` 관계에 부합하는 경우, 이 단계를 생략할 수 있으며, 시스템 최대 제한이 부족할 경우 조정할 수 있습니다.

`fs.file-max` = 2000000

`fs.nr_open` = 2000000

5. 다음 명령어를 실행하여 설정을 즉시 적용합니다. 설정이 완료되면 다시 로그인이 가능합니다.



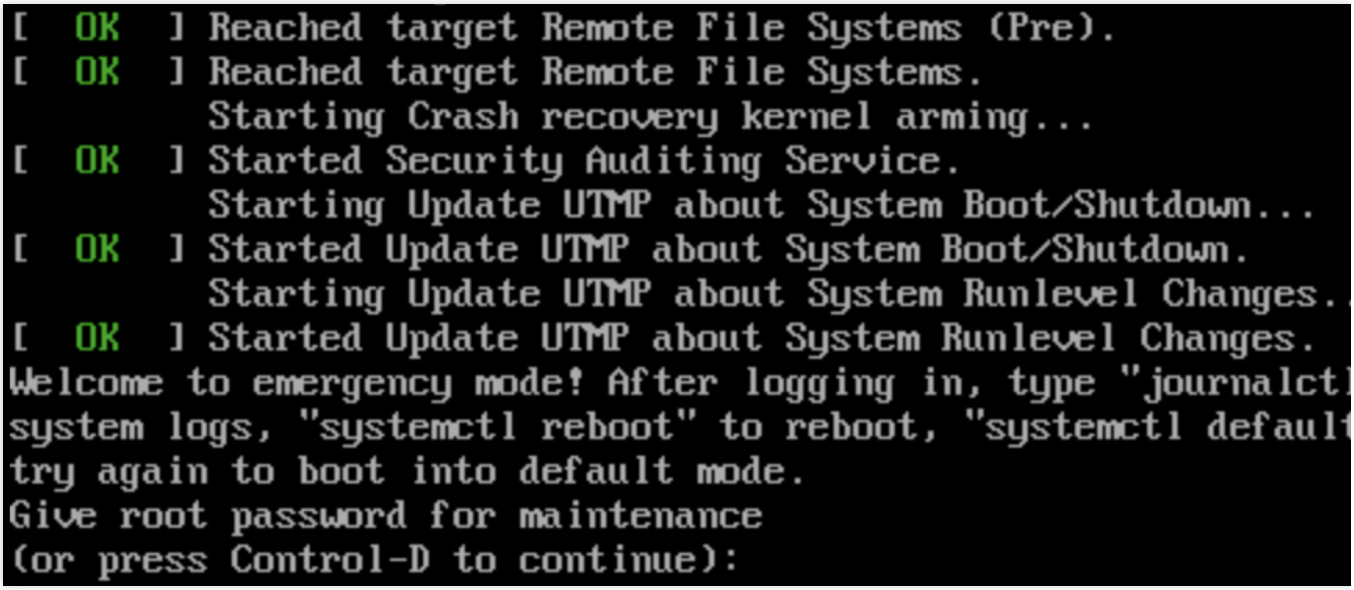
```
sysctl -p
```

Linux 인스턴스:/etc/fstab 구성 오류로 인한 로그인 실패

최종 업데이트 날짜: : 2024-02-02 11:09:48

오류 설명

SSH를 통해 원격으로 Linux CVM에 로그인할 수 없지만 VNC를 통해 CVM에 로그인한 후 시스템 시작 실패를 확인하고 “Welcome to emergency mode”라는 프롬프트 메시지를 볼 수 있습니다.



가능한 원인

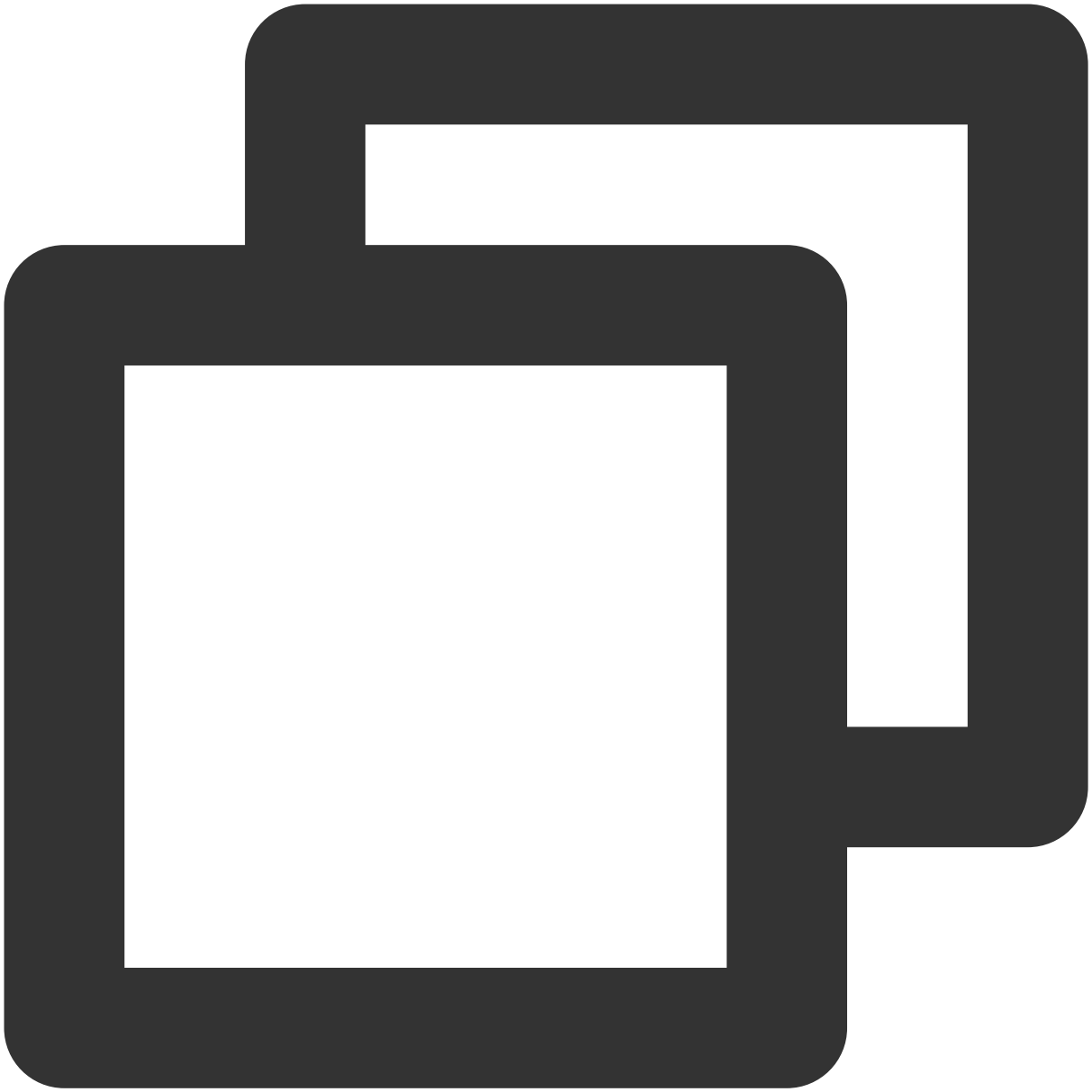
`/etc/fstab` 이 제대로 구성되지 않았습니다.
예를 들어 `/etc/fstab` 파일의 장치 이름을 기반으로 디스크 자동 연결을 구성했습니다. CVM이 다시 시작될 때 장치 이름이 변경되면 이 구성으로 인해 시스템이 정상적으로 시작되지 않습니다.

해결 방법

처리 단계를 참고하여 `/etc/fstab` 구성 파일을 복구하고 CVM을 다시 시작합니다.

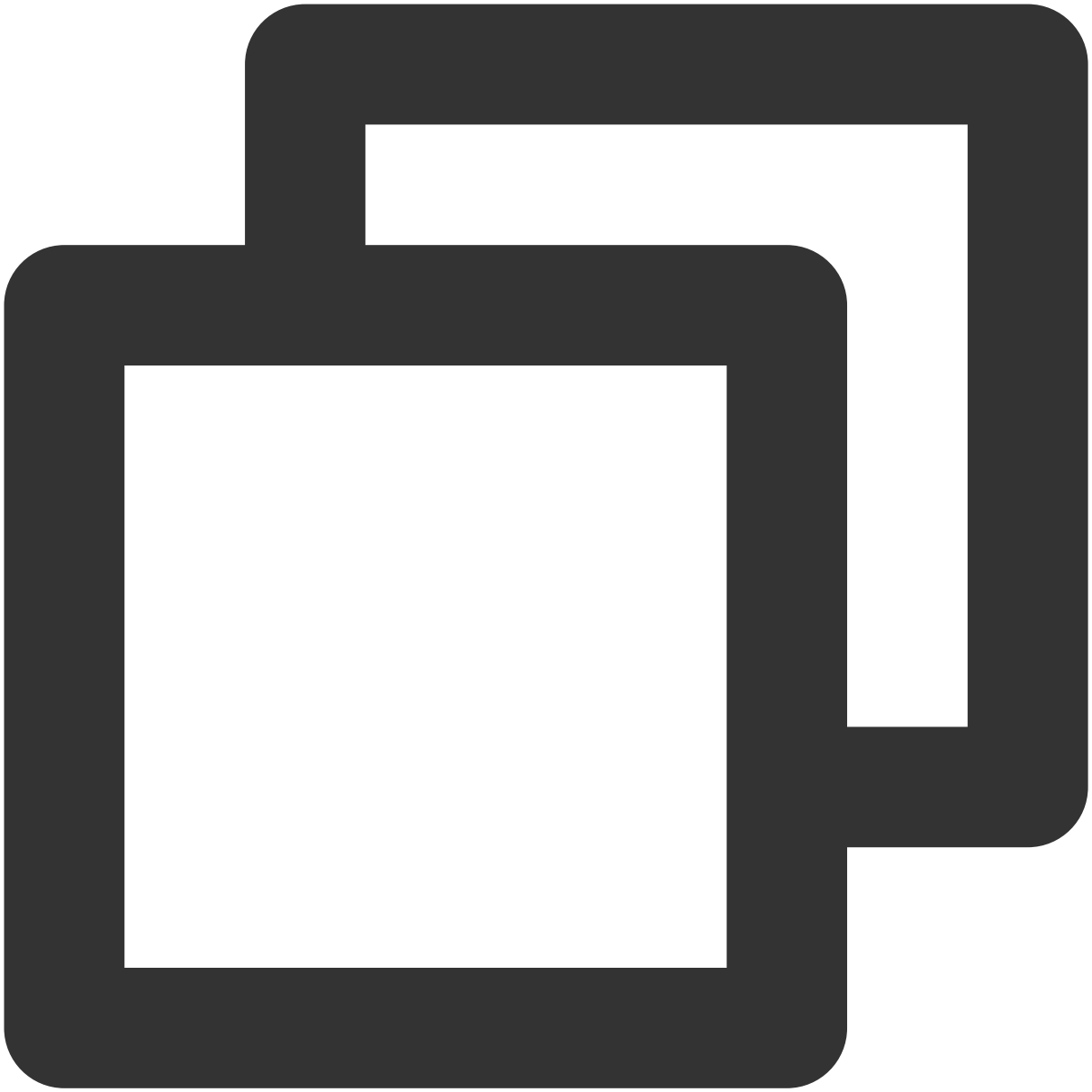
처리 단계

다음 두 가지 방법으로 인스턴스에 액세스할 수 있습니다.
방법1: VNC를 통해 로그인(권장)
방법2: 복구 모드
1. VNC를 사용하여 Linux 인스턴스 로그인합니다.
2. VNC 페이지에서 오류 설명과 같은 현상이 나타나면 root 계정과 비밀번호를 입력하고 **Enter**를 눌러 서버에 로그인하십시오.
비밀번호는 기본적으로 보이지 않습니다.
root 계정과 비밀번호가 없다면 Rescue 모드를 시도해보십시오.
3. 다음 명령어를 실행하여 `/etc/fstab` 파일을 백업합니다. 다음 예시에서 파일은 `/home` 디렉터리에 백업됩니다.



```
cp /etc/fstab /home
```

4. 다음 명령어를 실행하여 VI 편집기를 사용하여 `/etc/fstab` 파일을 엽니다.

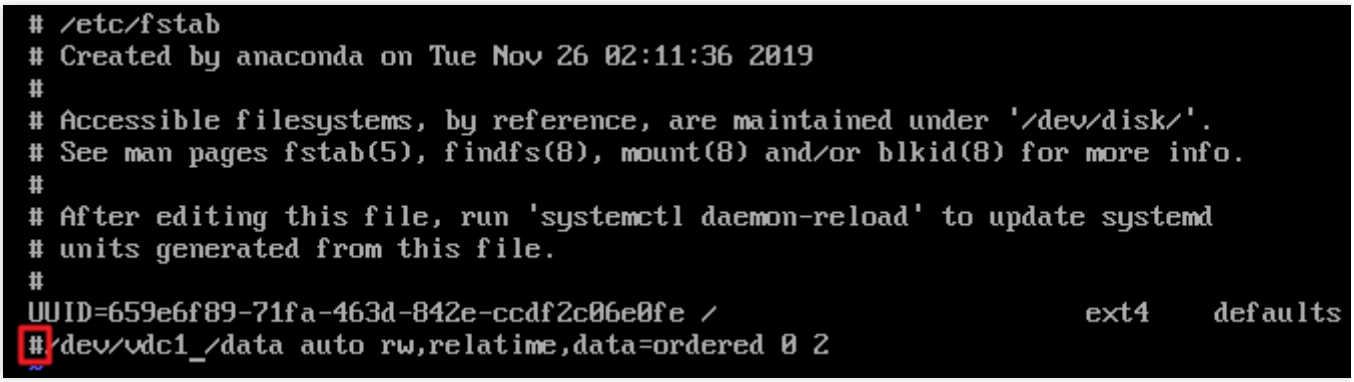


```
vi /etc/fstab
```

5. **i**를 눌러 편집 모드로 들어갑니다. 커서를 오류 줄의 시작 부분으로 이동하고 `#` 을 입력하여 이 구성을 주석 처리합니다.

설명：

오류가 확실하지 않은 경우 시스템 디스크를 제외한 연결된 모든 디스크의 구성을 주석 처리하십시오. 문제를 해결한 후 8단계에서 설명한 대로 이러한 구성을 복구할 수 있습니다.



6. **Esc**를 누르고 **:wq**를 입력한 다음 **Enter**를 눌러 구성을 저장하고 편집기를 종료합니다.
7. 콘솔을 통해 인스턴스를 다시 시작하고 정상적으로 시작 및 로그인할 수 있는지 확인합니다.

설명 :

인스턴스 재시작을 참고하십시오.

8. 로그인 성공 후 디스크 자동 연결 설정이 필요한 경우 Cloud Disk Automount Failed upon Linux CVM Restart를 참고하십시오.

1. 인스턴스 복구 모드로 들어갑니다. 복구 모드 사용을 참고하십시오.

주의사항 :

복구 모드를 사용한 시스템 복구에 설명된 `mount` 및 `chroot` 명령을 실행하고 대상 시스템에 진입했는지 확인합니다.

2. 방법1의 3단계 - 6단계에 따라 `/etc/fstab` 파일을 복구합니다.
3. 복구 모드 종료를 참고하여 인스턴스 복구 모드를 종료합니다.
4. 인스턴스가 복구 모드를 종료한 후에도 여전히 종료됩니다. 인스턴스 스타트업의 설명에 따라 시작합니다. 그런 다음 시스템을 정상적으로 시작하고 로그인할 수 있는지 확인합니다.
5. 로그인 성공 후 디스크의 자동 연결을 구성하려면 Configuring the /etc/fstab file을 참고하십시오.

Linux 인스턴스:sshd 구성 파일 권한 문제

최종 업데이트 날짜: : 2024-02-02 11:09:48

현상 설명

SSH를 사용하여 Linux 인스턴스에 로그인할 때 'ssh_exchange_identification: Connection closed by remote host' 또는 'no hostkey alg'가 표시됩니다.

예상 원인

`/var/empty/sshd` 및 `/etc/ssh/ssh_host_rsa_key` 구성 파일 권한 등 sshd 구성 파일의 권한이 수정되어 SSH를 사용하여 로그인하지 못할 수 있습니다.

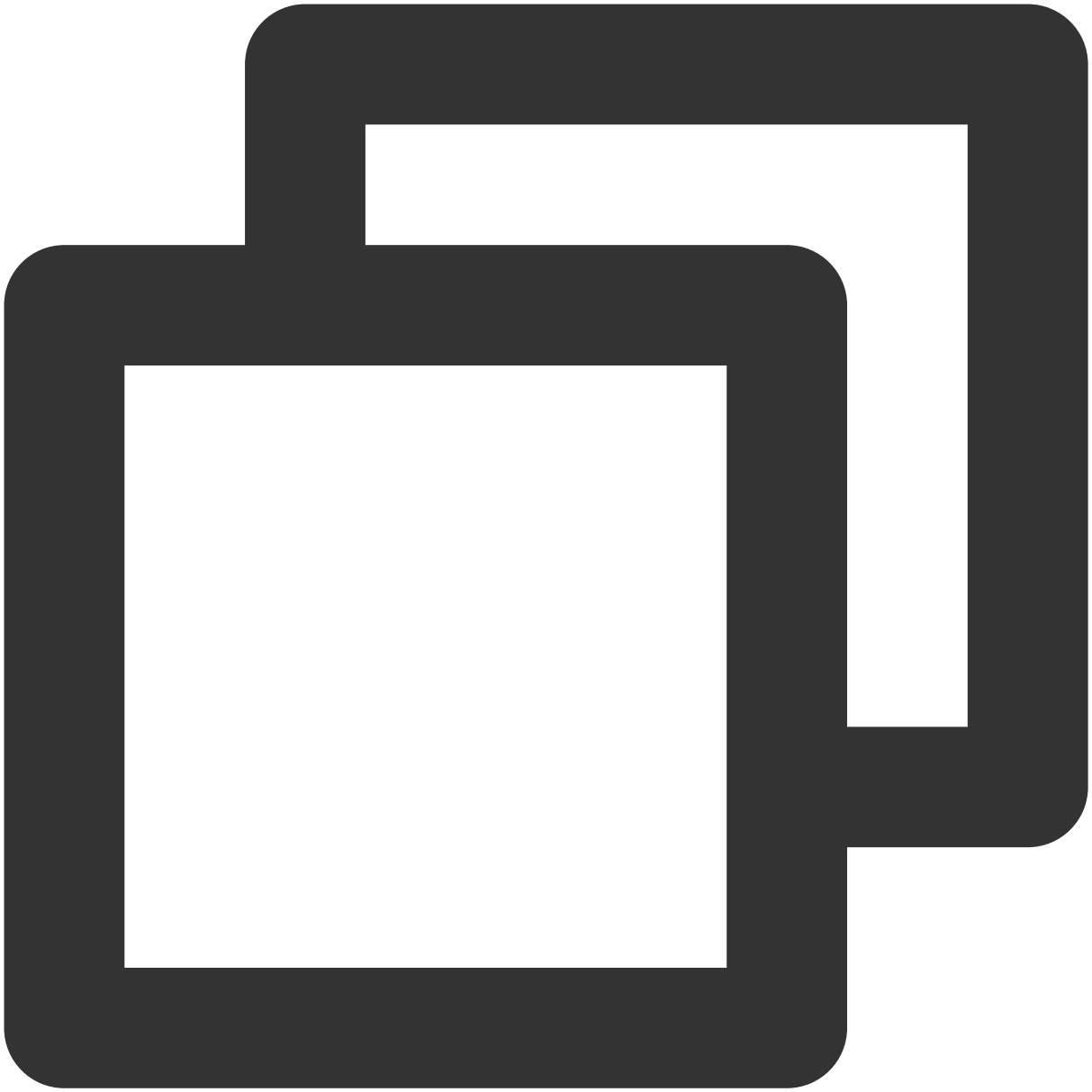
해결 방법

실제 오류 정보와 결합하여 해당 단계를 선택하여 구성 파일 권한을 수정합니다.
오류 메시지가 'ssh_exchange_identification: Connection closed by remote host'인 경우, /var/empty/sshd 파일 권한 수정 단계를 참고하십시오.
오류 메시지가 'no hostkey alg'인 경우, /etc/ssh/ssh_host_rsa_key 파일 권한 수정 단계를 참고하십시오.

처리 단계

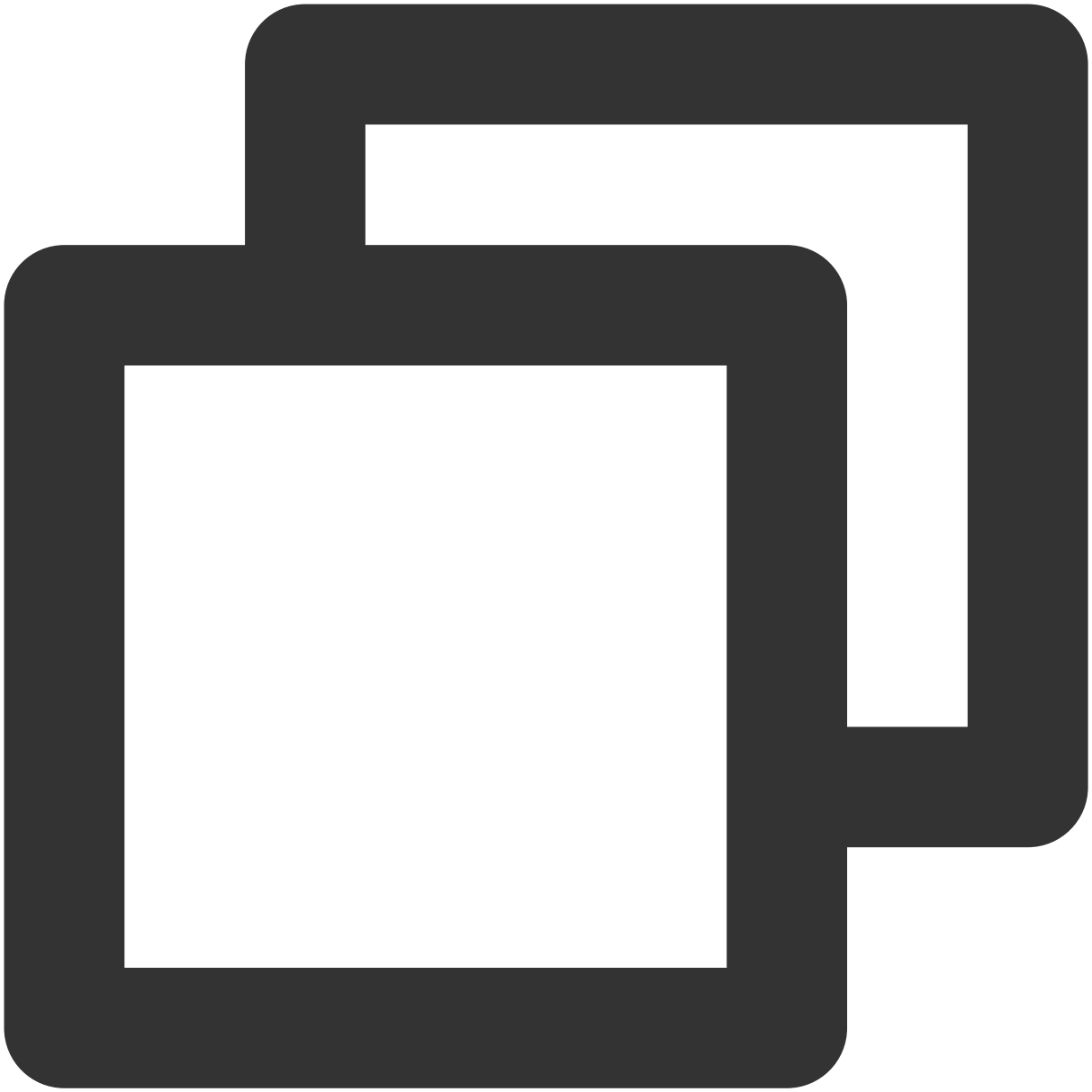
/var/empty/sshd 파일 권한 수정

1. VNC 사용하여 Linux 인스턴스에 로그인합니다.
2. 다음 명령어를 실행하여 오류의 원인을 확인합니다.



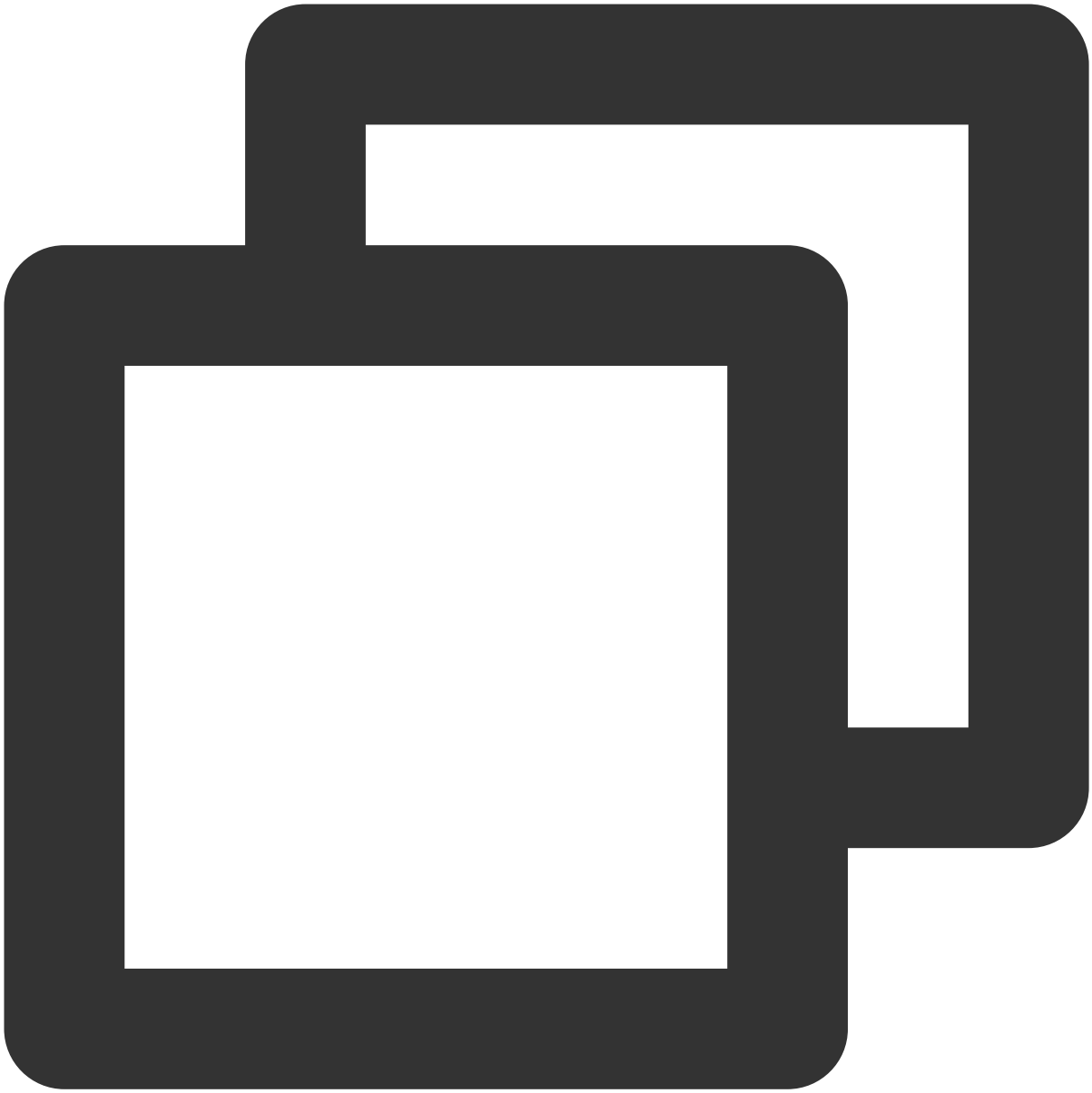
```
sshd -t
```

다음과 유사한 정보가 반환됩니다.



```
“/var/empty/sshd must be owned by root and not group or world-writable.”
```

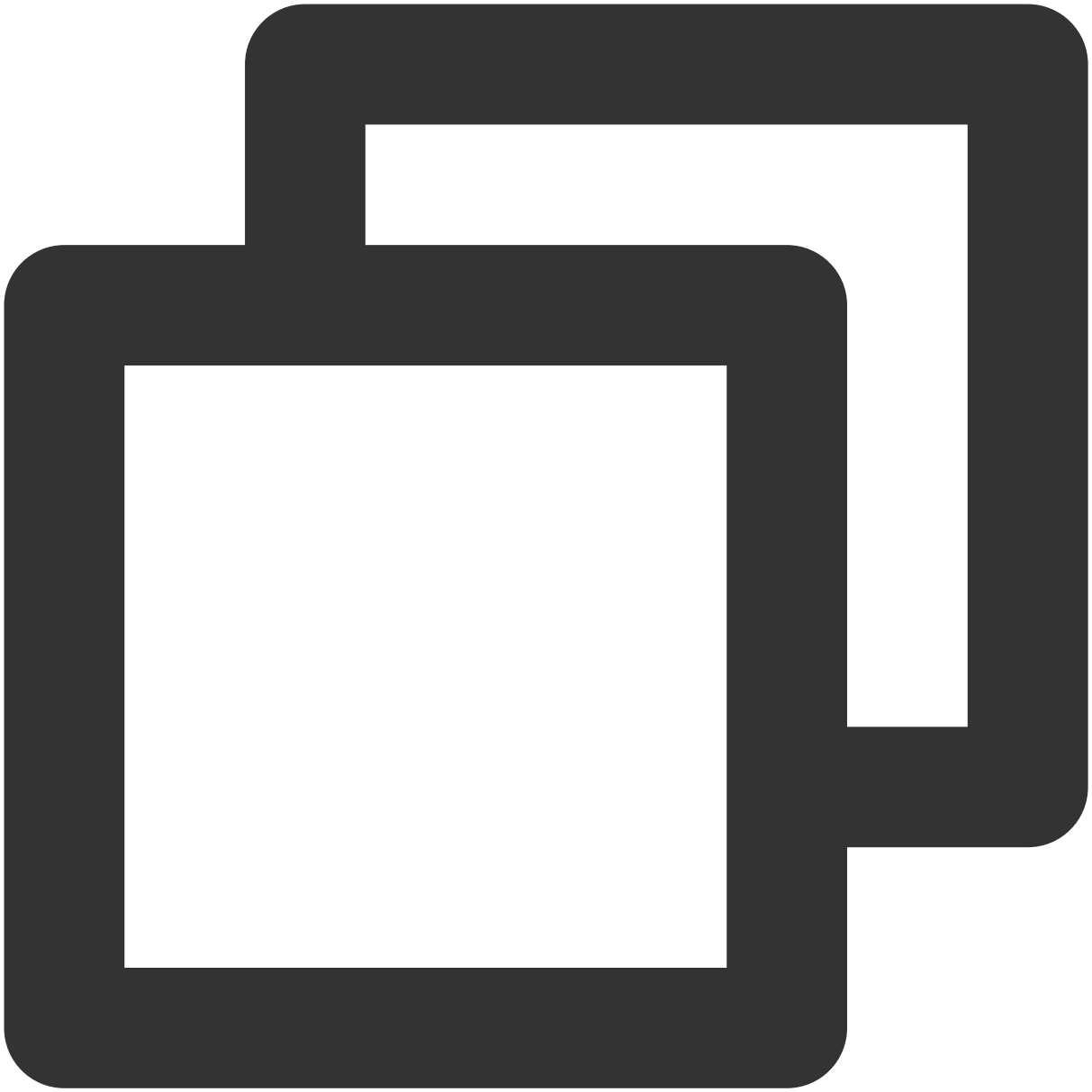
3. 다음 명령을 실행하여 `/var/empty/sshd/` 파일 권한을 수정합니다.



```
chmod 711 /var/empty/sshd/
```

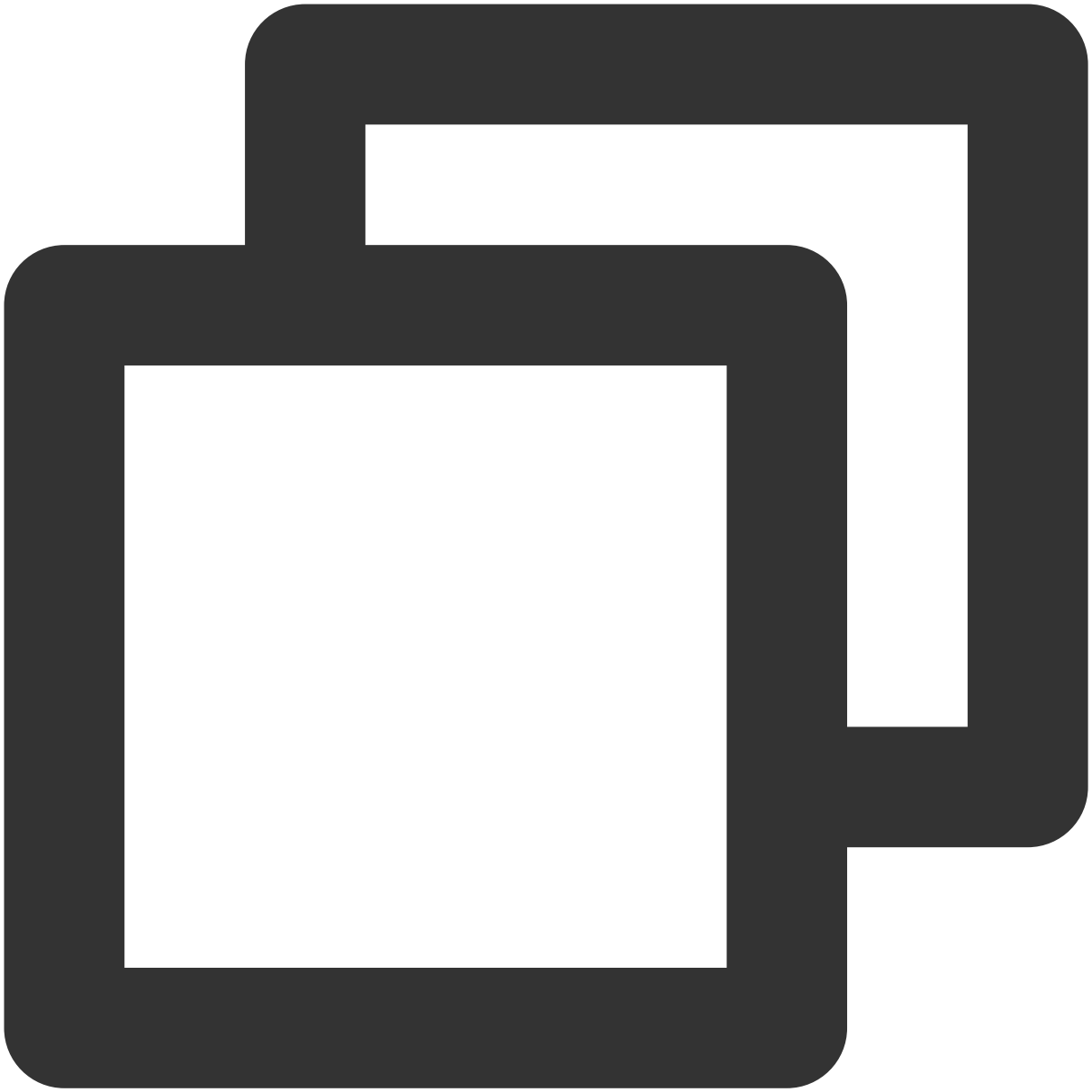
/etc/ssh/ssh_host_rsa_key 파일 권한 수정

1. VNC 사용하여 Linux 인스턴스에 로그인합니다.
2. 다음 명령어를 실행하여 오류의 원인을 확인합니다.



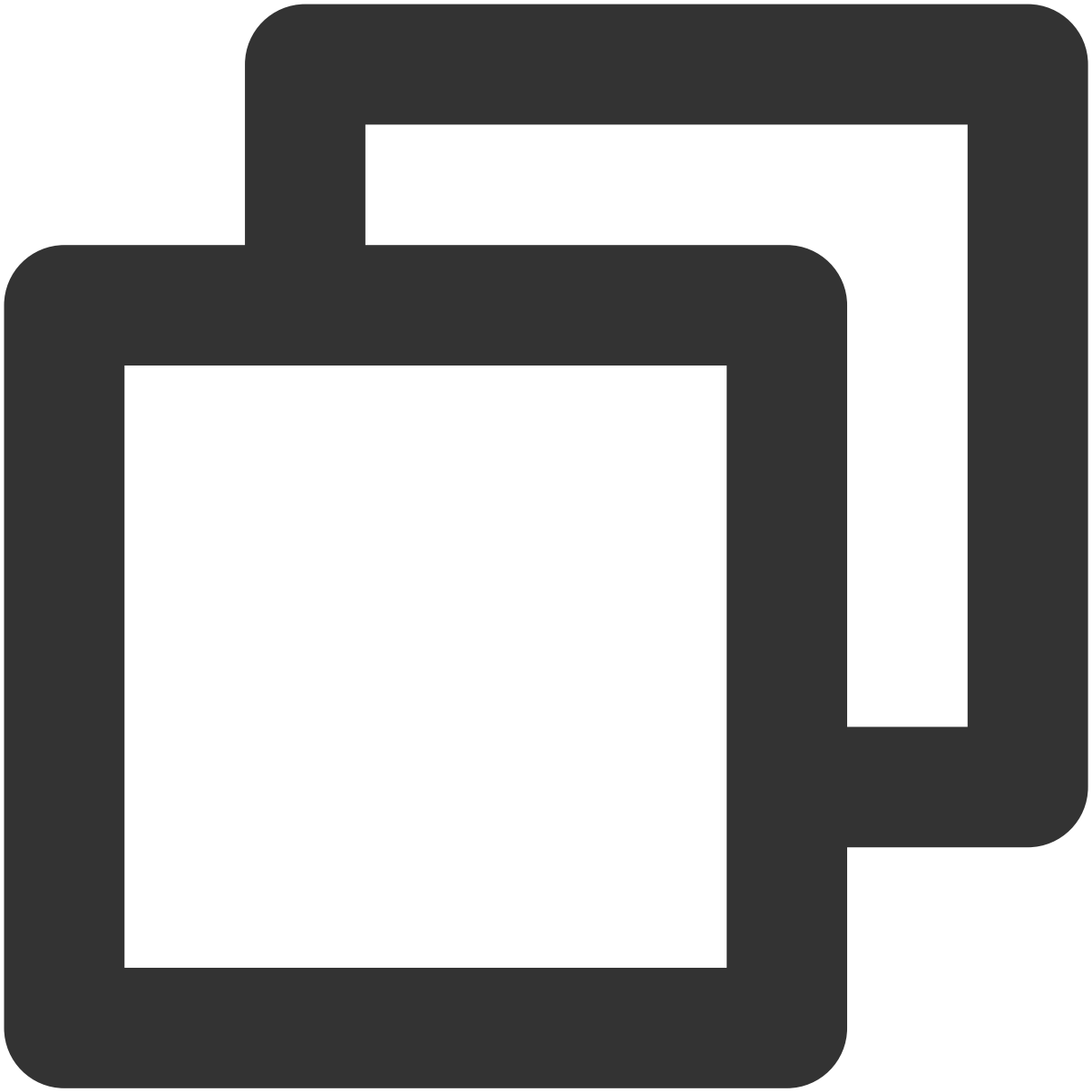
```
sshd -t
```

반환된 정보에는 다음 필드가 포함됩니다.



```
“/etc/ssh/ssh_host_rsa_key are too open”
```

3. 다음 명령을 실행하여 `/etc/ssh/ssh_host_rsa_key` 파일 권한을 수정합니다.



```
chmod 600 /etc/ssh/ssh_host_rsa_key
```

Linux 인스턴스:/etc/profile 무한 루프 호출 문제

최종 업데이트 날짜: : 2024-02-02 11:09:47

현상 설명

SSH를 사용하여 Linux 인스턴스에 로그인할 때 'Last login:' 이라는 관련 정보가 출력되고 SSH 명령이 중지됩니다.

예상 원인

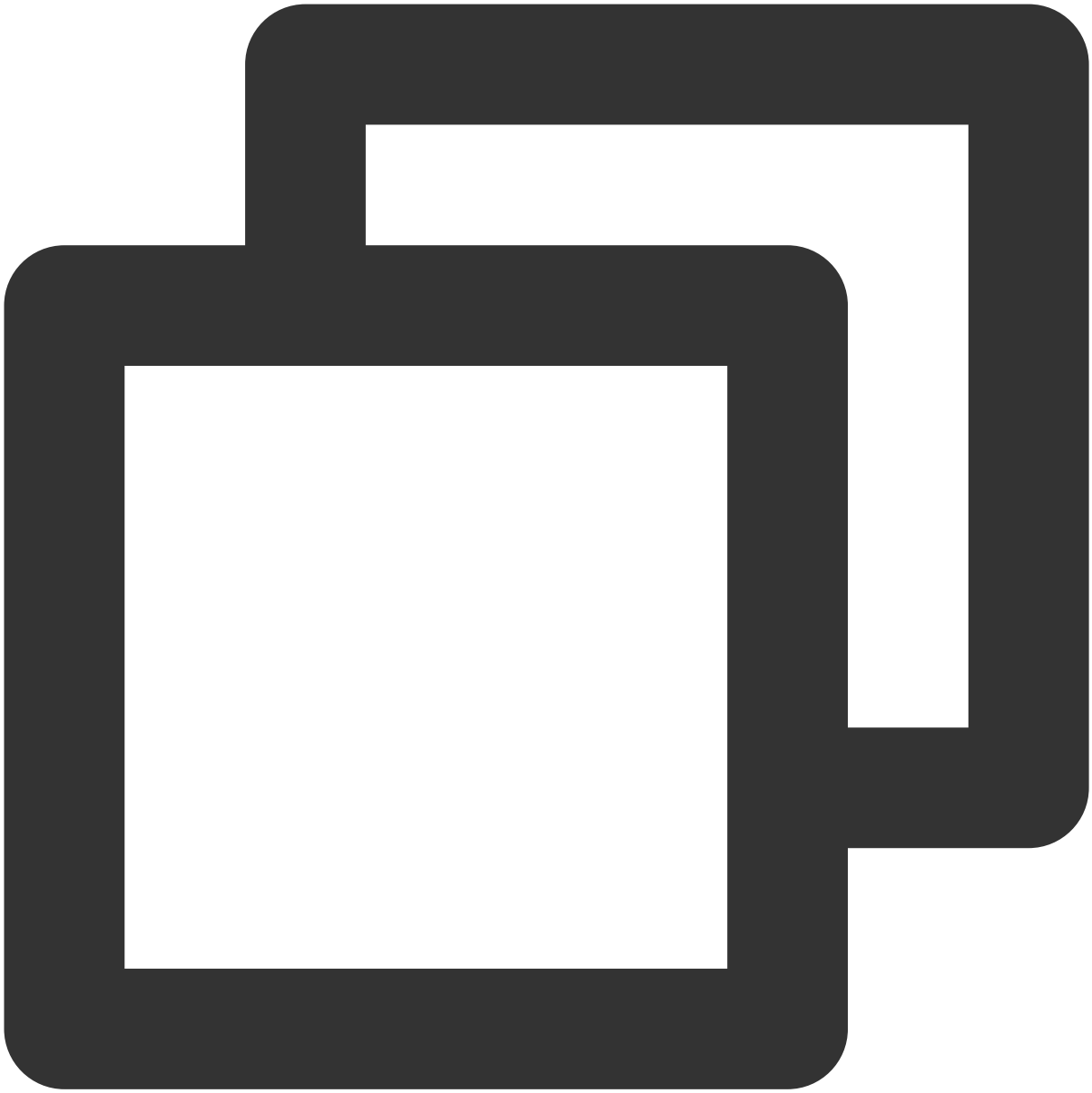
`/etc/profile` 파일이 수정되었기 때문에 `/etc/profile` 에서 `/etc/profile` 호출 현상이 발생하여 무한 루프 호출에 빠져 로그인 실패가 발생하였을 수 있습니다.

해결 방법

처리 단계를 참고하여, `/etc/profile` 파일을 확인 및 복구합니다.

처리 순서

1. VNC 사용하여 Linux 인스턴스에 로그인합니다.
2. 다음 명령을 실행하여 `/etc/profile` 파일을 확인합니다.



```
vim  /etc/profile
```

3. `/etc/profile` 파일에 `/etc/profile` 관련 명령어가 포함되어 있는지 확인합니다.

포함된 경우 다음 단계를 실행합니다.

포함되지 않은 경우 티켓 제출을 통해 고객센터에 도움을 요청하십시오.

4. **i**를 눌러 편집 모드로 들어가고 `/etc/profile` 에서 해당 명령 앞에 `#` 을 추가하여 명령을 주석 처리합니다.

5. **Esc**를 눌러 편집 모드를 종료하고 **:wq**를 입력하여 변경 사항을 저장합니다.

6. 다시 SSH를 사용하여 Linux 인스턴스에 로그인합니다.

서버가 격리되어 로그인할 수 없을 경우

최종 업데이트 날짜: : 2024-02-02 11:09:48

본 문서는 CVM의 외부 네트워크가 격리되어 로그인할 수 없는 문제에 대한 솔루션을 소개합니다.

장애 현상

CVM 격리는 해당 서버가 현재 법률 법규를 위반한 것일 수 있습니다. 아래 방식을 통해 해당 서버의 격리 상태 여부를 조회할 수 있습니다.
CVM 외부 네트워크가 격리될 경우, 콘솔 내부 메시지 또는 SMS 발송 방식을 통해 규정 위반 격리 안내를 사용자에게 공지합니다.
CVM 콘솔 의 "Monitorinig/Status" 표시줄에 해당 CVM 상태: 격리 중이라고 표시됩니다.

문제 원인

CVM에 규정 위반 사항 또는 위험 사항을 발견할 경우, 규정을 위반한 기기에 대해 일부 격리 작업(내부 네트워크의 22, 36000, 3389 로그인 포트를 제외한 나머지 네트워크 액세스가 전부 격리되며, 개발자는 점프 서버 방식으로 서버에 로그인할 수 있음)을 시행합니다.
자세한 내용은 [클라우드 보안 규정 위반 사항의 등급 구분 및 처벌 설명]을 참조 바랍니다.

솔루션

1. 내부 메시지 또는 SMS 알림에 따라 규정 위반 내용을 처리합니다. 보안 취약점을 처리하고, 필요에 따라 시스템을 재설치합니다.
2. 사용자 개인 행위로 인한 규정 위반이 아닌 경우, 서버에 악성 침입이 있을 가능성이 있습니다. 솔루션은 HS를 참조 바랍니다.
3. 보안 취약점을 제거하거나 규정 위반을 중단한 후 Submit Ticket을 통해 고객서비스에 문의하여 격리를 해제하시기 바랍니다.

높은 대역폭 점유율로 로그인할 수 없을 경우

최종 업데이트 날짜: : 2024-02-02 11:09:48

본 문서는 고대역폭 사용으로 인한 Linux 또는 Windows CVM 로그인 문제를 진단하고 해결하는 방법을 설명합니다.

장애 현상

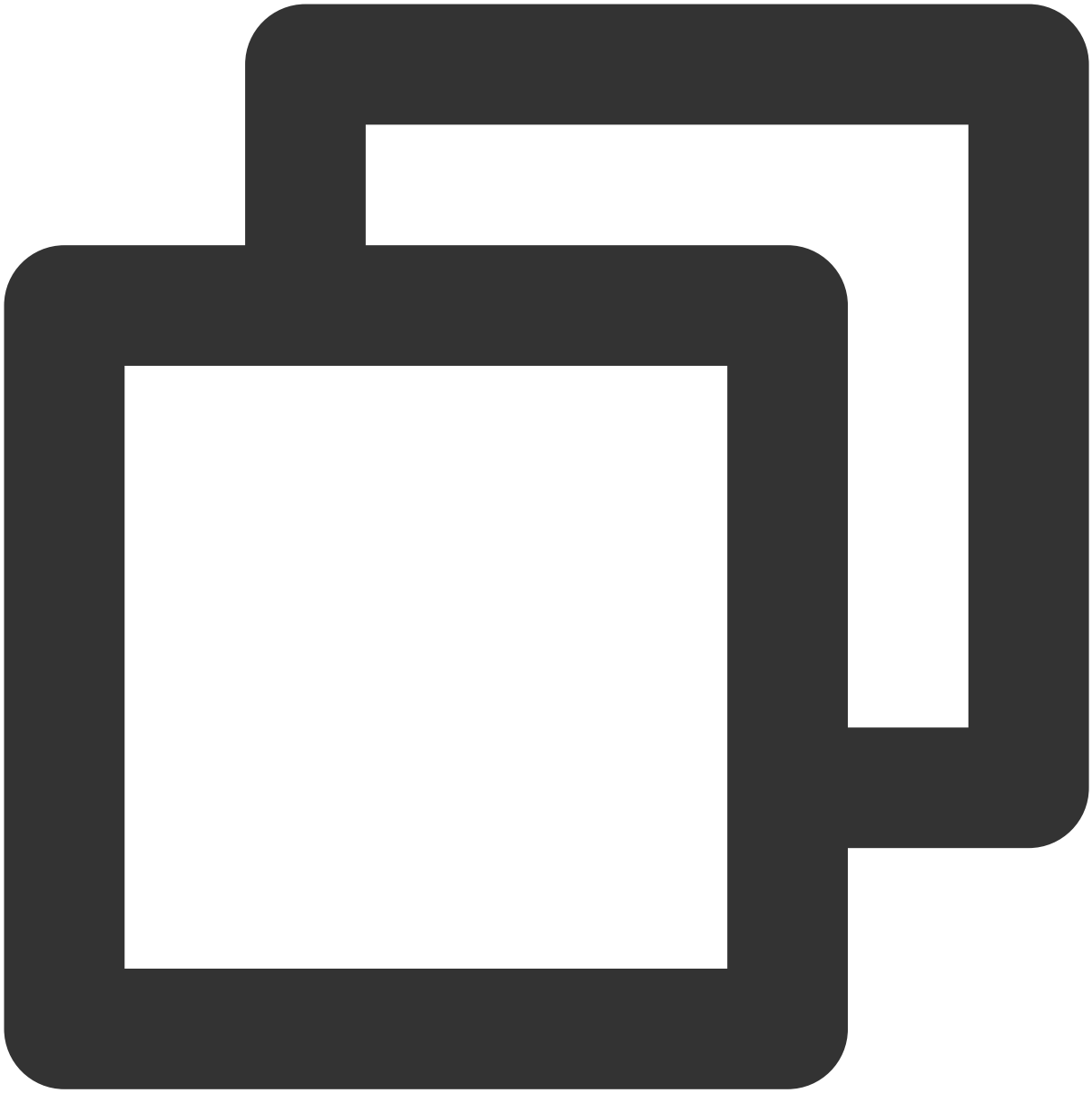
CVM 콘솔에서 CVM의 대역폭 모니터링 데이터는 대역폭 사용량이 너무 높고 CVM에 대한 연결이 실패함을 보여줍니다.
자가 진단 툴을 통한 대역폭 사용량이 너무 높습니다.

장애 진단 및 처리

1. VNC를 사용하여 실제 클라우드 서버 인스턴스에 로그인합니다.
Windows 인스턴스: VNC를 사용하여 Windows 인스턴스에 로그인
Linux 인스턴스: VNC를 사용하여 Linux 인스턴스에 로그인
2. 클라우드 서버 문제 해결:
Windows CVM
Linux CVM
VNC를 사용하여 Windows CVM에 로그인한 후 다음 작업을 수행합니다.
설명 :
다음 작업은 Windows Server 2012 시스템이 있는 CVM을 예로 들어 설명합니다.
1. CVM에서

을(를) 클릭합니다. **작업 관리자**를 선택하여 **작업 관리자** 창을 엽니다.
2. **성능** 탭 페이지를 선택하고 **리소스 모니터 열기**를 클릭합니다.
3. **리소스 모니터**가 열리면 어떤 프로세스가 더 많은 대역폭을 사용하는지 확인합니다. 실제 비즈니스에 따라 프로세스가 정상적인지 확인합니다.
대역폭을 많이 소모하는 프로세스가 정상이라면 접속량의 변화 때문인지, 용량 최적화나 CVM 구성 업그레이드가 필요한지 확인합니다.
대역폭을 많이 소모하는 프로세스가 비정상적인 경우 바이러스나 트로이 목마가 있을 수 있습니다. 프로세스를 직접 종료하거나 보안 소프트웨어를 사용할 수 있습니다. 데이터 백업 후 시스템을 다시 설치할 수도 있습니다.
주의사항 :

Windows 시스템에서 많은 바이러스 프로세스가 시스템 프로세스로 위장합니다. **작업 관리자** > **프로세스**에서 프로세스 정보를 사용하여 예비 검사를 수행할 수 있습니다.
일반 시스템 프로세스에는 완전한 서명과 설명이 있으며 대부분은 C:\\Windows\\System32 디렉터리에 있습니다. 바이러스 프로그램은 시스템 프로세스와 이름이 같을 수 있지만 서명이나 설명이 없습니다. 위치도 비정상적일 것입니다.
대역폭을 많이 사용하는 프로세스가 Tencent Cloud 구성 요소 프로세스인 경우 티켓 제출을 통해 문의하십시오. 문제를 찾고 해결하는 데 도움을 드리겠습니다.
VNC를 사용하여 Linux CVM에 로그인한 후 다음 작업을 수행합니다.
설명：
다음 작업은 CentOS 7.6 시스템이 있는 CVM을 예로 들어 설명합니다.
1. 다음 명령을 실행하여 iftop 툴을 설치합니다. iftop 툴은 Linux CVM용 트래픽 모니터링 가젯입니다.

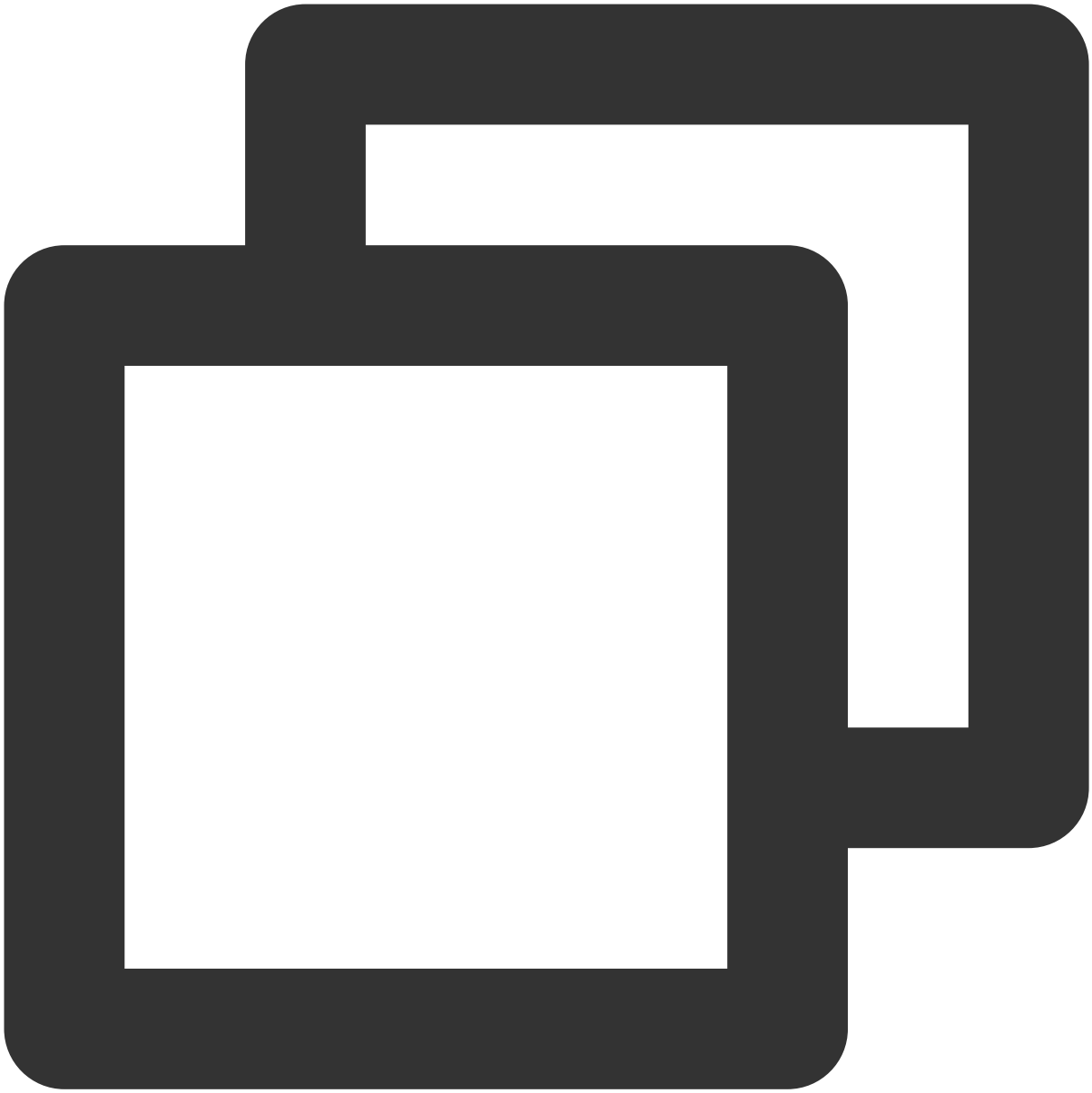


```
yum install iftop -y
```

설명：

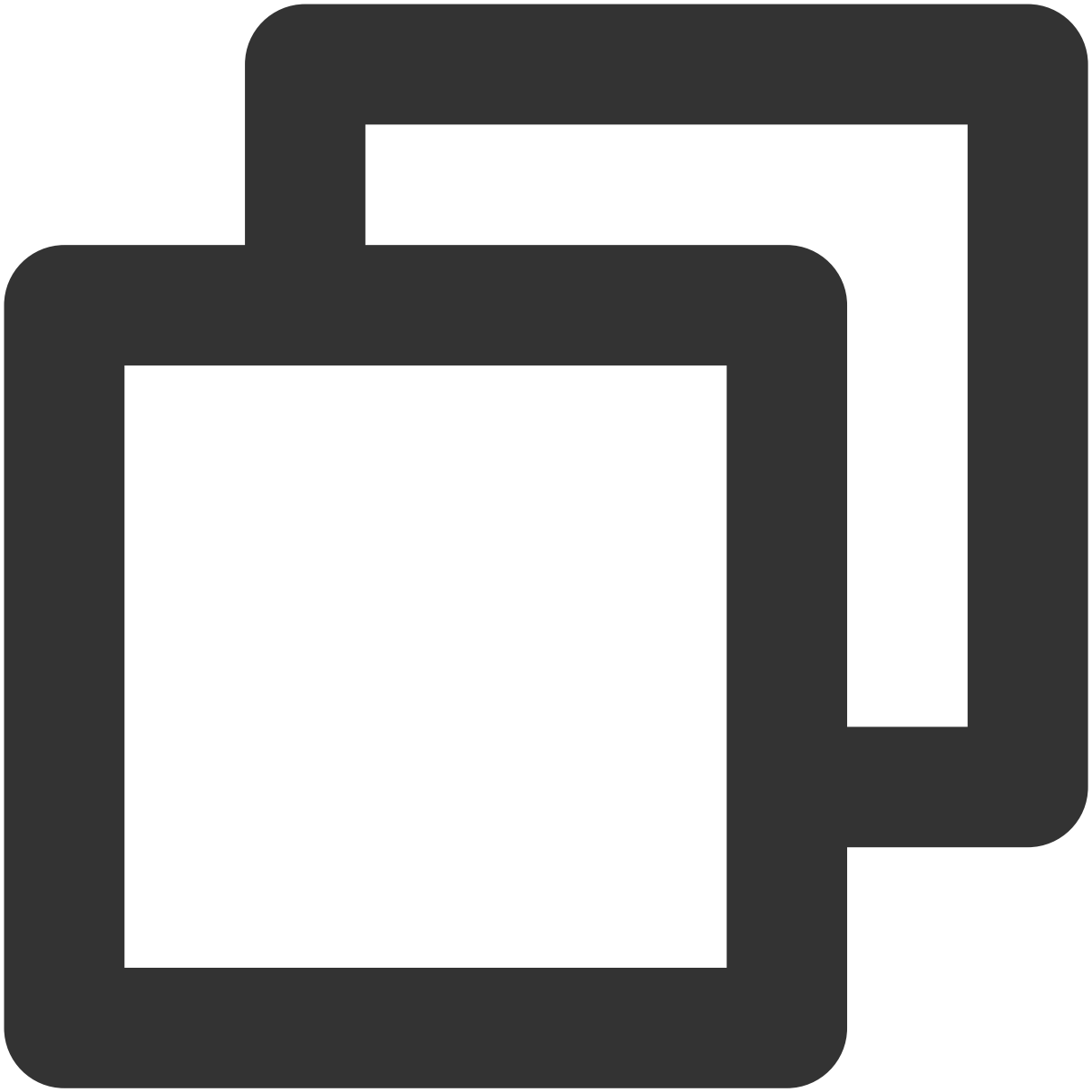
Ubuntu 시스템의 경우 `apt-get install iftop -y` 명령을 실행합니다.

2. 다음 명령을 실행하여 lsof를 설치합니다.

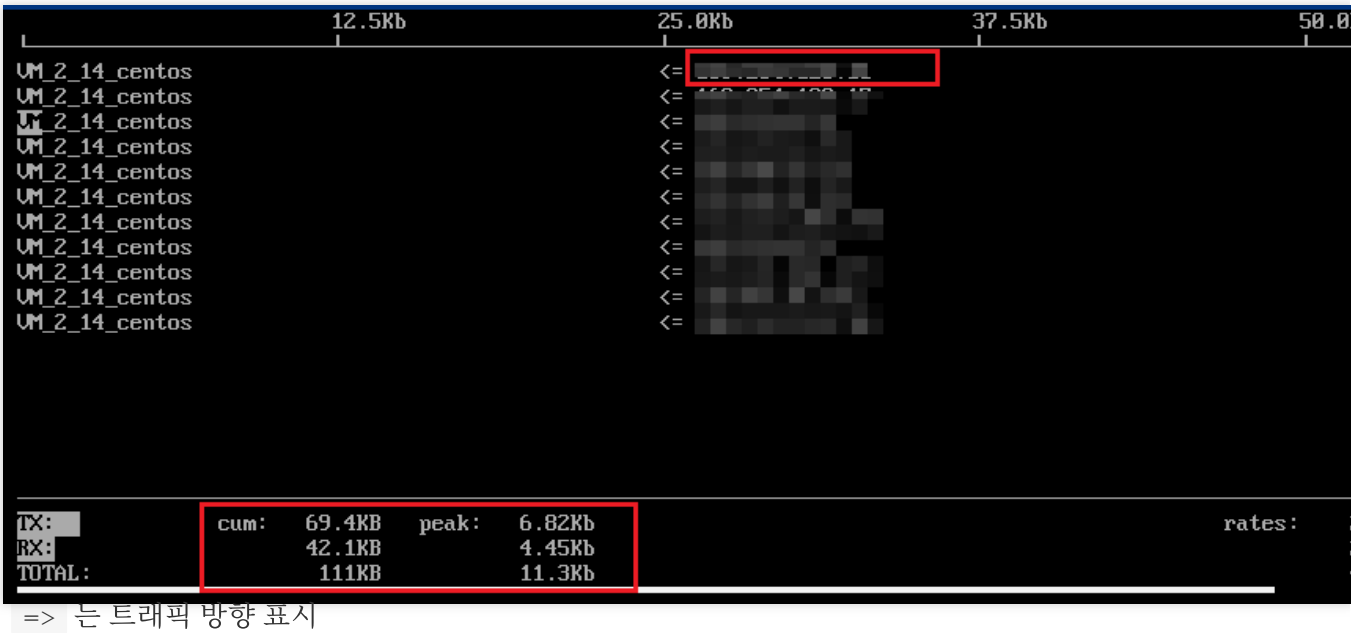


```
yum install lsof -y
```

3. 다음 명령을 실행하여 iftop을 실행합니다. 다음 이미지와 같습니다.



```
iftop
```



`<=` , `=>` 는 트래픽 방향 표시

TX는 발송 트래픽 표시

RX는 수신 트래픽 표시

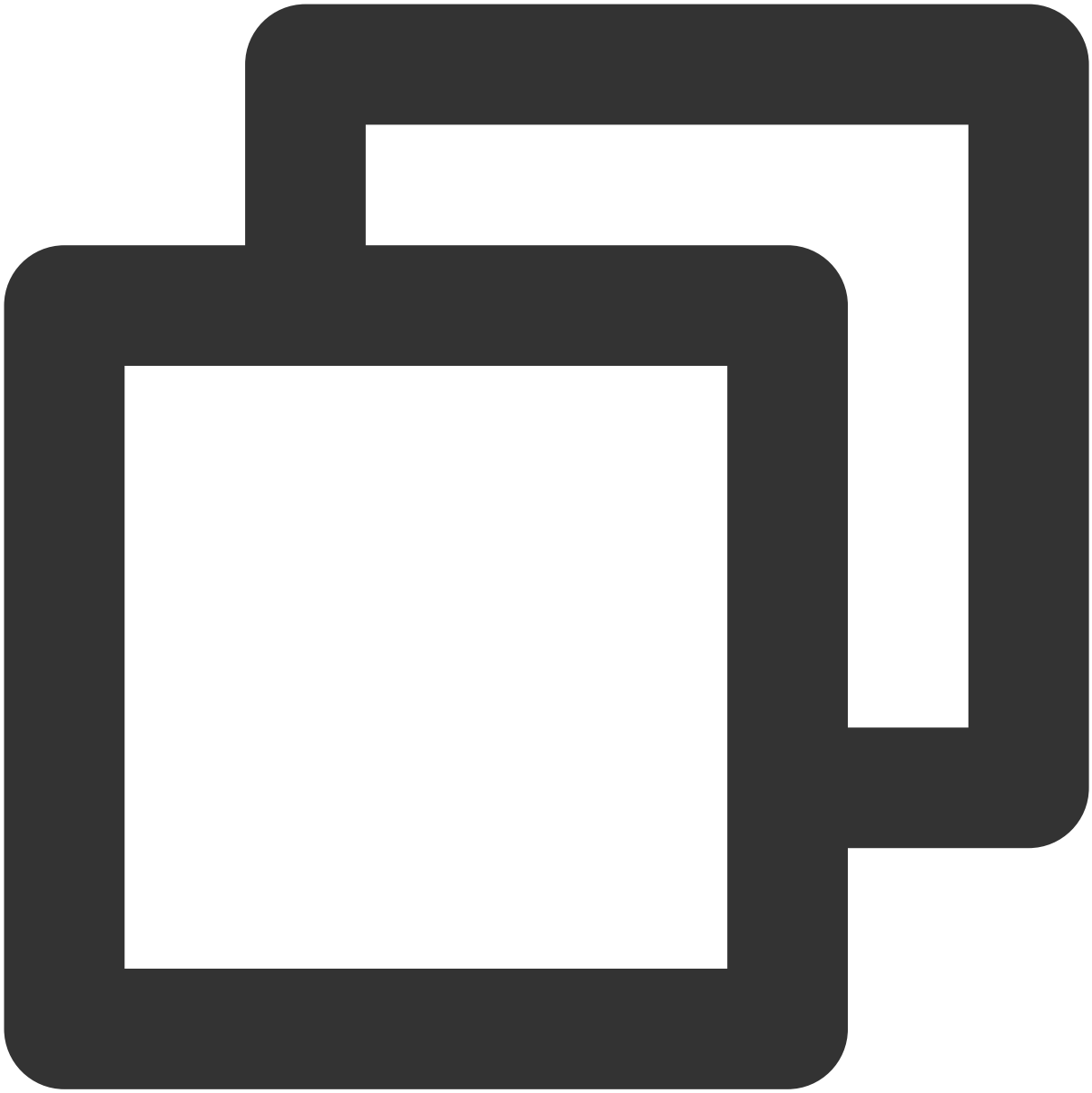
TOTAL은 총 트래픽 표시

Cum은 iftop이 실행되기 시작한 순간부터 지금까지의 총 트래픽 표시

peak는 트래픽 피크 표시

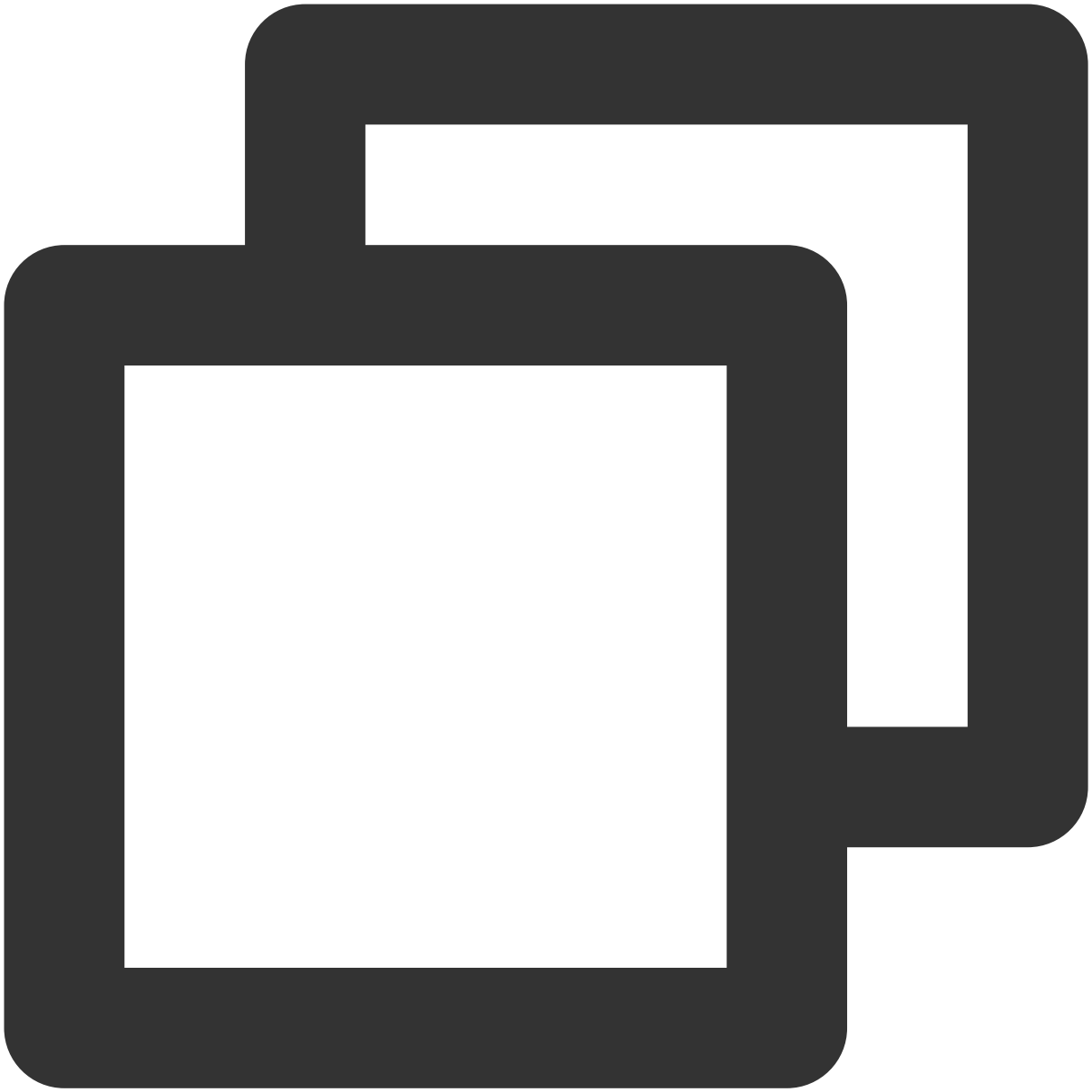
rates는 각각 지난 2초, 10초 및 40초 동안의 평균 트래픽 표시

4. iftop에서 소비된 트래픽의 IP에 따라 다음 명령어를 실행하여 이 IP에 연결된 프로세스를 확인합니다.



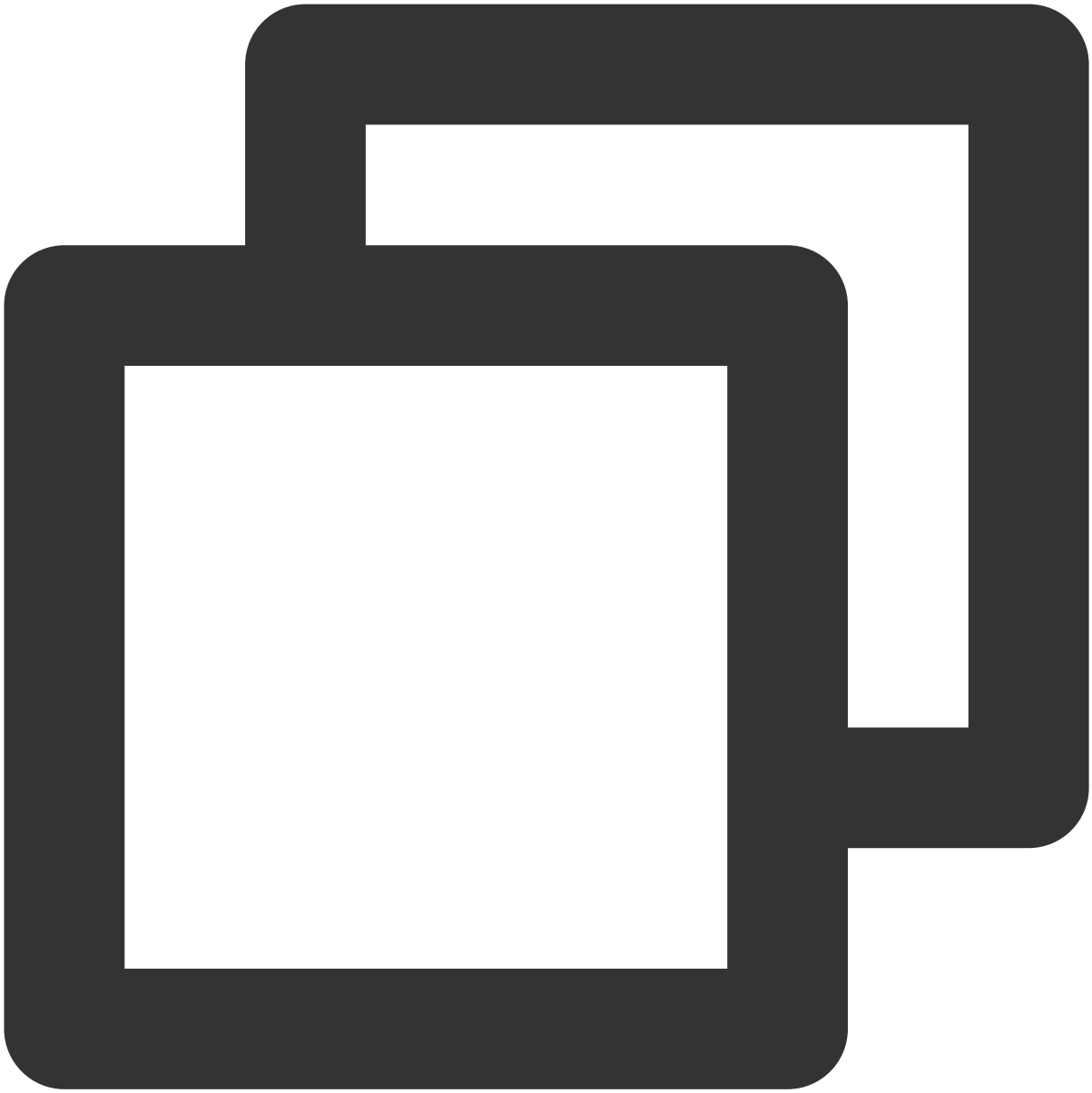
```
lsof -i | grep IP
```

예를 들어 소비된 트래픽의 IP가 201.205.141.123인 경우 다음 명령을 실행합니다.



```
lsof -i | grep 201.205.141.123
```

다음 결과가 반환되면 SSH 프로세스에서 CVM 대역폭을 주로 사용하는 것입니다.



```
sshd       12145    root    3u  IPV4  3294018       0t0   TCP 10.144.90.86:ssh->203
sshd       12179  ubuntu    3u  IPV4  3294018       0t0   TCP 10.144.90.86:ssh->203
```

5. 대역폭을 사용하는 프로세스를 조회하고 프로세스가 정상인지 확인합니다.
대역폭을 많이 소모하는 프로세스가 정상이라면 접속량의 변화 때문인지, 용량 최적화나 CVM 구성 업그레이드가 필요한지 확인합니다.
대역폭을 많이 소모하는 프로세스가 비정상인 경우 바이러스나 트로이 목마가 있을 수 있습니다. 프로세스를 직접 종료하거나 보안 소프트웨어를 사용할 수 있습니다. 데이터 백업 후 시스템을 다시 설치할 수도 있습니다.

대역폭을 많이 사용하는 프로세스가 Tencent Cloud 구성 요소 프로세스인 경우 티켓 제출을 통해 문의하십시오. 문제를 찾고 해결하는 데 도움을 드리겠습니다.
IP138 쿼리 웹 사이트에서 목적지 IP의 위치를 확인하는 것이 좋습니다. IP 위치가 다른 국가/지역에 있는 경우 보안 위험이 더 크니 주의하십시오!

보안 그룹 설정으로 인하여 원격 연결이 안 될 경우

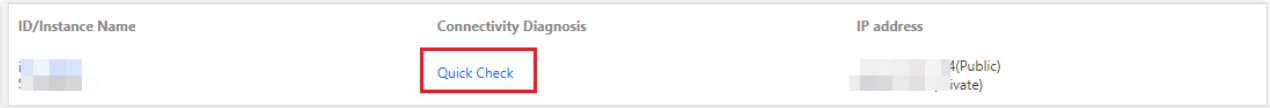
최종 업데이트 날짜: : 2024-02-02 11:09:48

본 문서는 CVM이 보안 그룹 설정 문제로 인해 원격 연결할 수 없는 경우의 문제 해결 및 솔루션을 소개합니다.

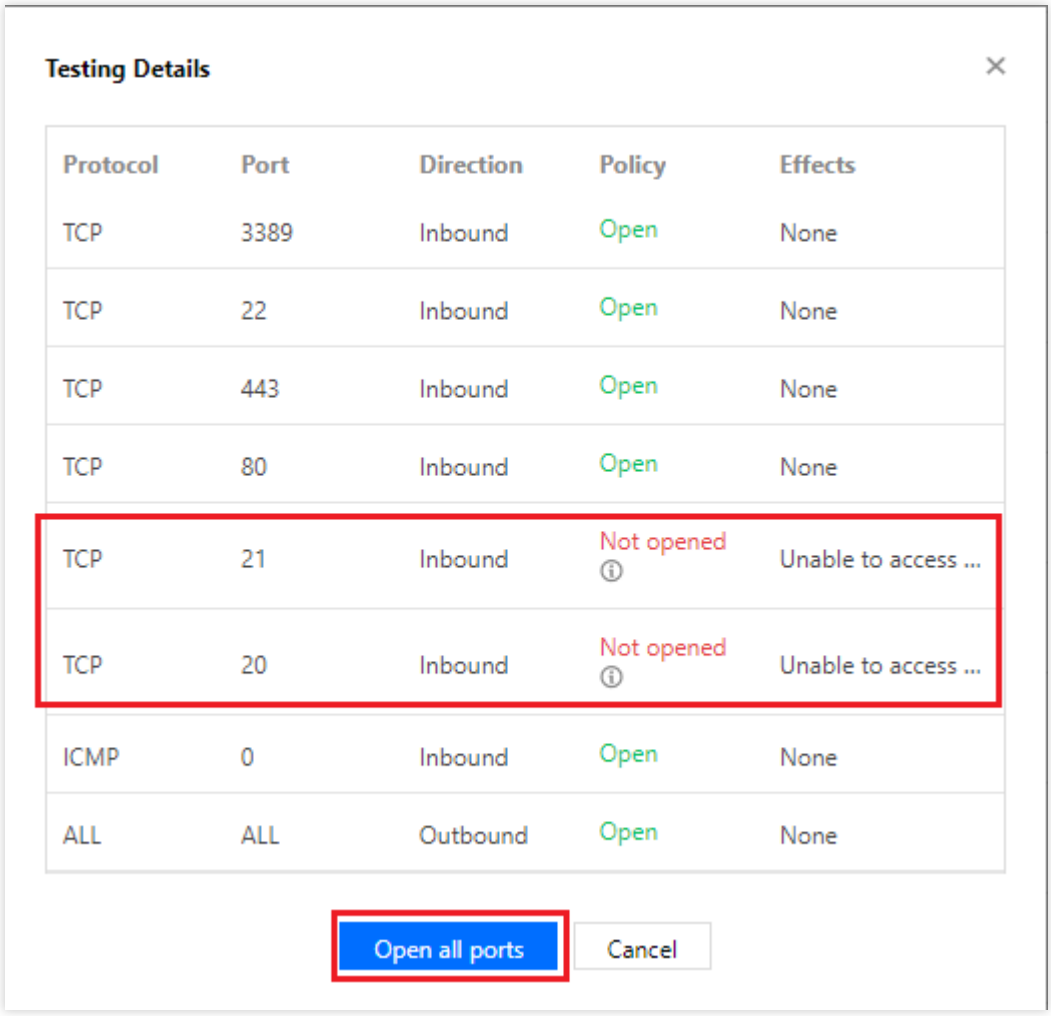
점검 툴

Tencent Cloud가 제공하는 보안 그룹(포트) 진단 툴을 통해 원격 연결할 수 없는 이유가 보안 그룹 설정과 연관되어 있는지 판단할 수 있습니다.

1. 보안 그룹(포트) 진단 툴에 로그인합니다.
2. **인스턴스 포트 진단**페이지에서 점검이 필요한 인스턴스를 선택하고 [Quick Check]을 클릭합니다. 아래 이미지 참조



해당 인스턴스에 개방하지 않은 포트가 있는 것으로 진단한 경우, [Open all ports] 기능을 통해 서버의 상용 포트를 오픈하고 원격 로그인을 다시 시도할 수 있습니다.



보안 그룹 설정 수정

툴을 통해 점검한 결과, 보안 그룹 포트의 설정 문제로 확인되었으나 [원클릭 오픈] 기능을 통한 모든 CVM 상용 포트의 오픈을 원하지 않거나 원격 로그인 포트의 사용자 정의가 필요한 경우, 보안 그룹의 인바운드 및 아웃바운드 규칙을 사용자 정의로 설정하여 원격 연결할 수 없는 문제를 해결할 수도 있습니다. 자세한 작업 내용은 보안 그룹 규칙 수정을 참조 바랍니다.

VNC 및 복구 모드를 통한 Linux 인스턴스 문제 해결

최종 업데이트 날짜: : 2024-02-02 11:09:48

일반적으로 VNC 및 복구 모드를 통해 대부분의 Linux 시스템 문제를 해결할 수 있습니다. 본 문서에서는 SSH 키를 통한 Linux 인스턴스 로그인 실패 및 시스템 오류와 같은 문제를 해결하는 방법을 설명합니다.

문제 해결 도구

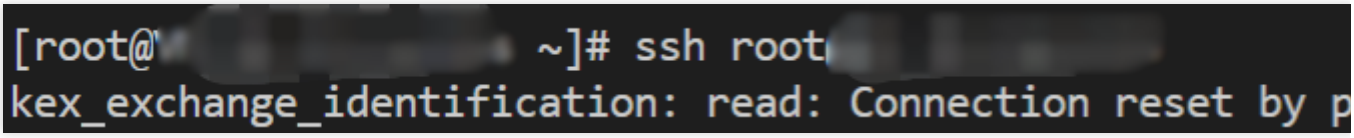
VNC를 통한 로그인은 Web 브라우저를 통해 CVM에 원격으로 연결하는 방법입니다. 이를 통해 CVM 상태를 직접 관찰하거나 시스템의 구성 파일을 수정할 수 있습니다. 일반적으로 SSH 키를 통해 인스턴스에 원격으로 로그인할 수 없는 경우 이 로그인 방법을 사용할 수 있습니다.
복구 모드는 일반적으로 Linux 시스템을 정상적으로 시작할 수 없거나 VNC를 통해 Linux 인스턴스에 로그인할 수 없는 경우에 사용됩니다. 일반적인 사용 사례: 비정상적인 fstab 구성, 주요 시스템 파일 누락, .lib 및 .dll 파일 손상/누락 등.

문제 진단 및 처리

VNC를 사용하여 SSH 키 로그인 실패 문제 해결

오류 설명

SSH 키를 통해 Linux 인스턴스에 로그인하려고 하면 “ssh_exchange_identification: Connection closed by remote host” 오류 메시지가 표시됩니다.



예상 원인

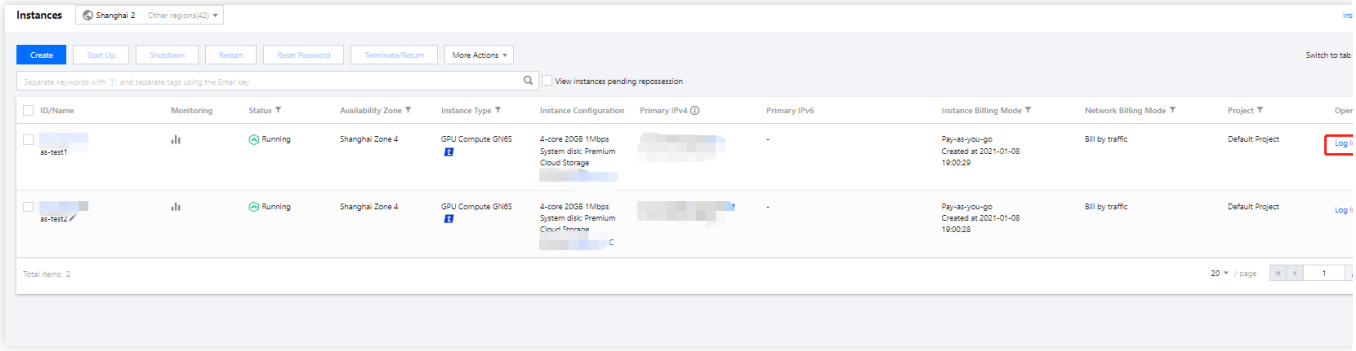
kex_exchange_identification 단계의 connection reset 오류는 일반적으로 ssh 관련 프로세스가 시작되었음을 의미하지만 sshd 구성 파일 권한이 수정되는 등 구성이 비정상적일 수 있습니다.

해결 방식

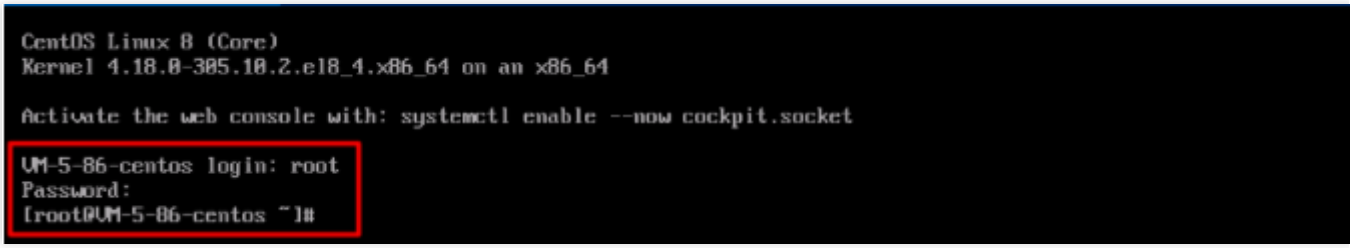
sshd 프로세스를 확인하고 문제를 찾아 수정하려면 처리 단계를 참고하십시오.

처리 단계

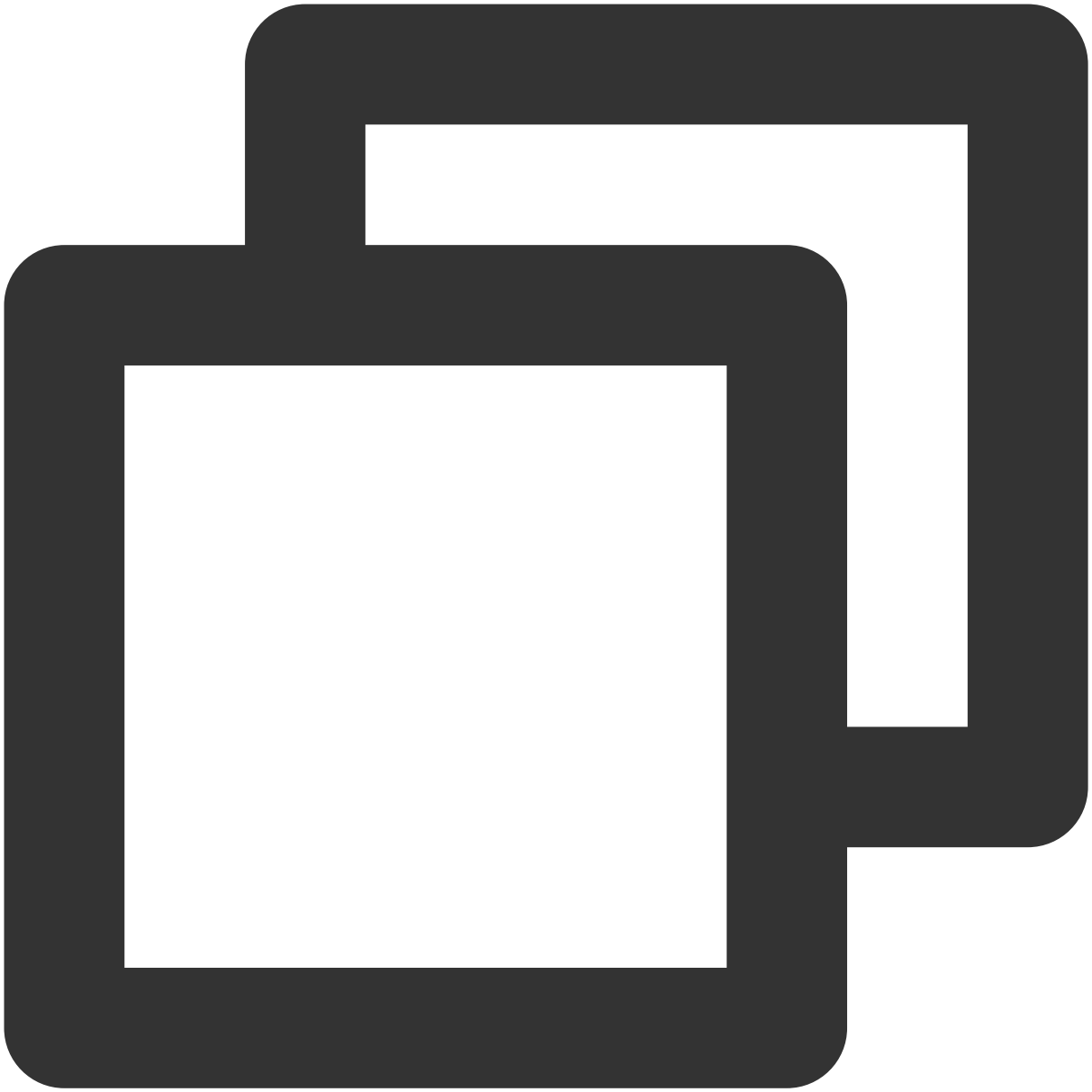
1. 다음 단계에 따라 VNC를 통해 Linux 인스턴스에 로그인합니다.
2. CVM 콘솔에 로그인하여 대상 Linux CVM을 찾은 다음 작업 열에서 **로그인**을 클릭합니다.



3. '표준 로그인 | Linux 인스턴스' 창에서 **VNC를 통해 로그인**을 클릭합니다.
4. 'login' 후 사용자 이름을 입력하고 **Enter**를 누르고, 'Password' 후에 비밀번호를 입력하고 **Enter**를 누릅니다. 다음 정보가 표시되면 로그인이 성공한 것입니다.

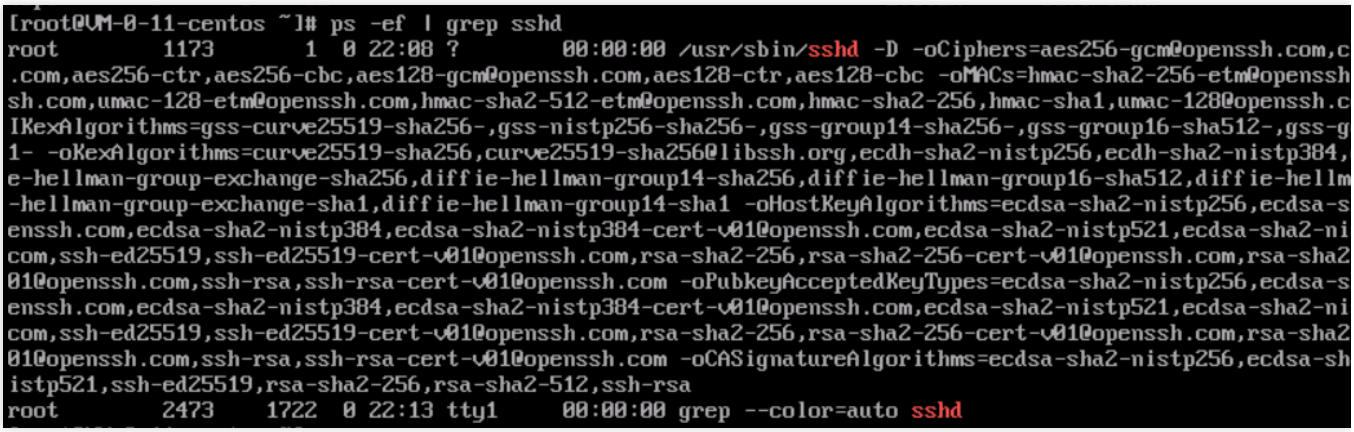


5. 다음 명령어를 실행하여 sshd 프로세스가 정상적으로 실행되고 있는지 확인합니다.

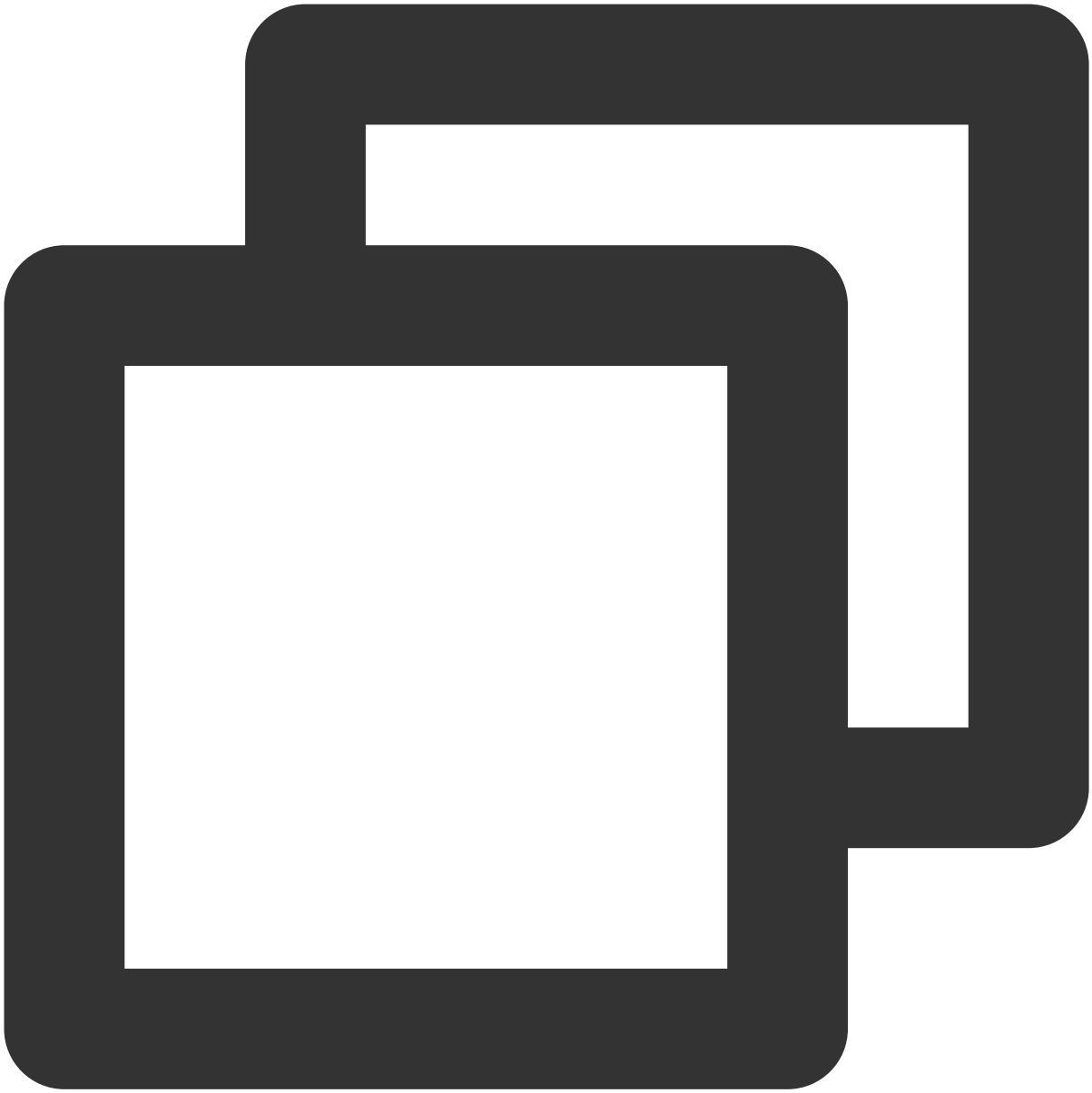


```
ps -ef | grep sshd
```

아래와 같은 결과가 나오면 sshd 프로세스가 정상인 것입니다.

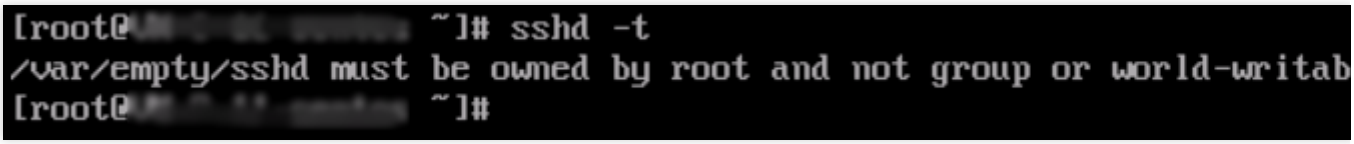


6. 다음 명령어를 실행하여 오류의 원인을 확인합니다.

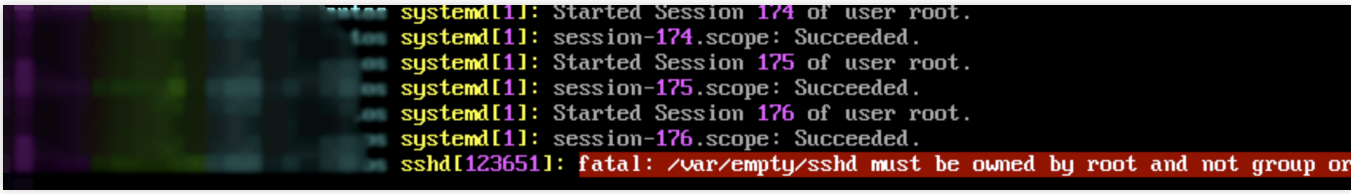


```
sshd -t
```

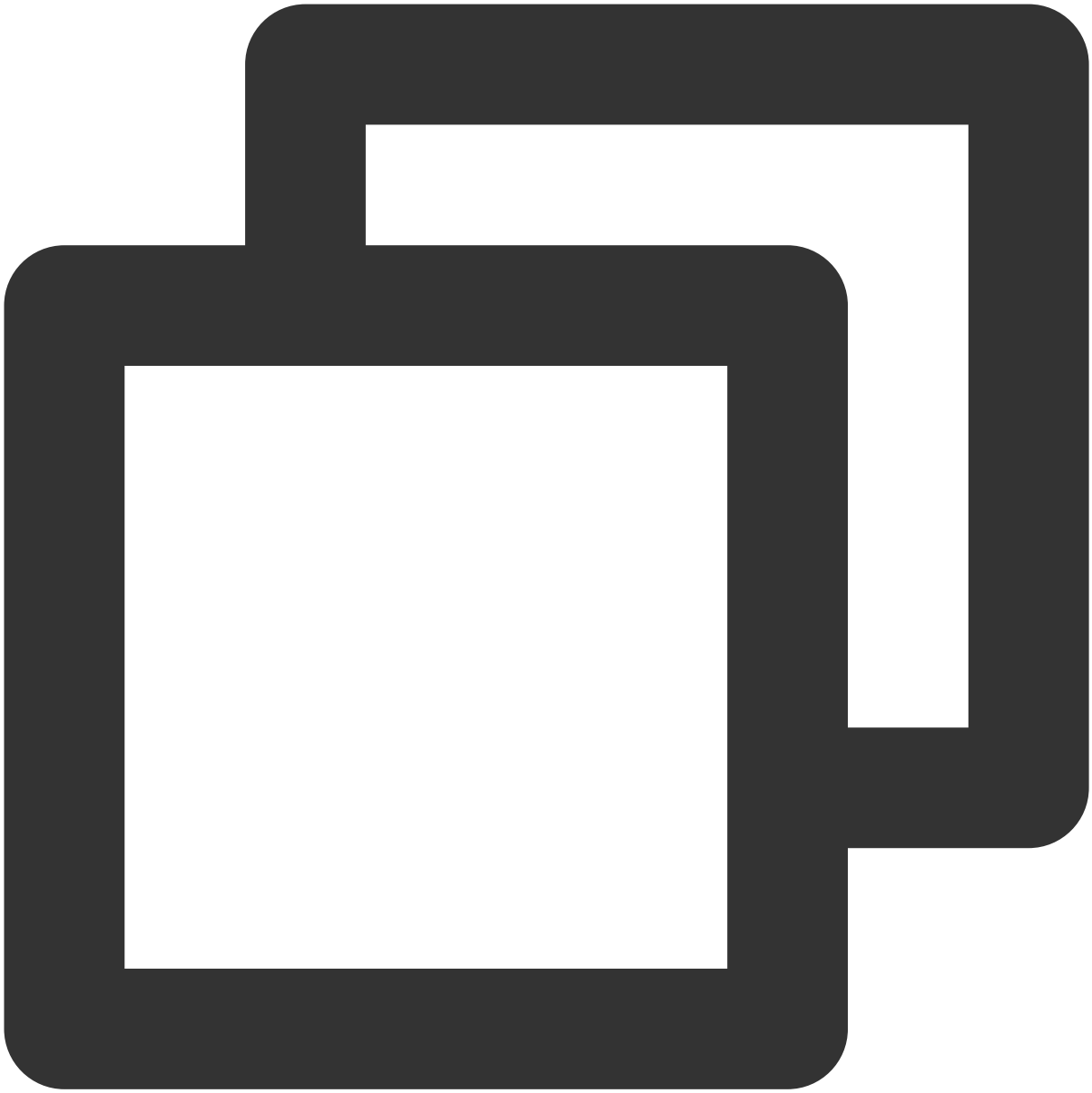
아래에 표시된 '/var/empty/sshd must be owned by root and not group or world-writable.'과 유사한 메시지가 반환되는 경우,
이 오류는 `/var/empty/sshd/` 권한 문제로 인해 발생할 수 있습니다.



문제 해결을 용이하게 하기 위해 `/var/log/secure` 로그에서 오류 메시지를 확인할 수도 있습니다.



7. 다음 명령을 실행하여 `/var/empty/sshd` 디렉터리의 권한을 확인합니다.

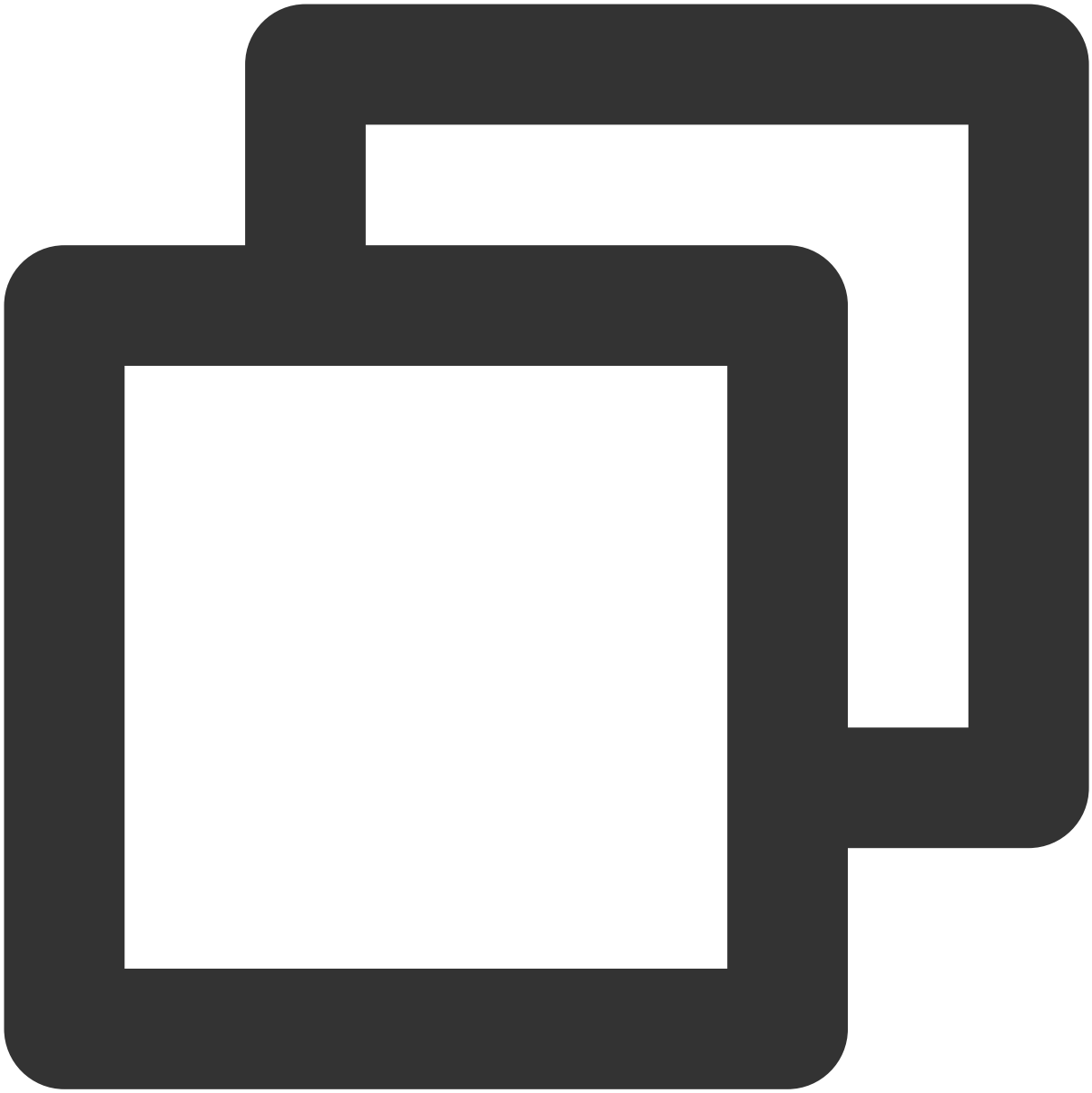


```
ll -d /var/empty/sshd/
```

반환된 결과는 아래와 같습니다. 권한 구성은 777입니다.

```
[root@VM-0-11-centos ~]# ll -d /var/empty/sshd/
drwxrwxrwx. 2 root root 4096 Jul 13  2021 /var/empty/sshd/
```

8. 다음 명령을 실행하여 `/var/empty/sshd/` 파일의 권한을 수정합니다.



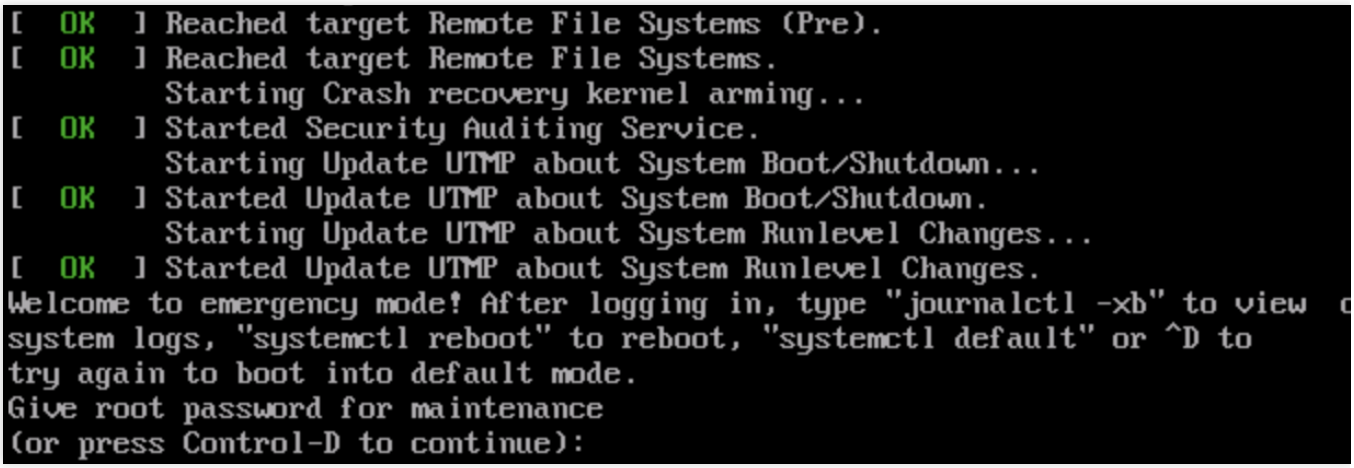
```
chmod 711 /var/empty/sshd/
```

SSH를 사용하여 Linux 인스턴스에 로그인을 참고하여 테스트를 완료한 후, 원격으로 인스턴스에 로그인할 수 있습니다.

VNC를 사용하여 Linux 시스템 시작 실패 문제 해결

오류 설명

SSH를 통해 원격으로 Linux CVM에 로그인할 수 없지만 VNC를 통해 CVM에 로그인한 후 시스템 시작 실패를 확인하고 “Welcome to emergency mode”라는 프롬프트 메시지를 볼 수 있습니다.



예상 원인

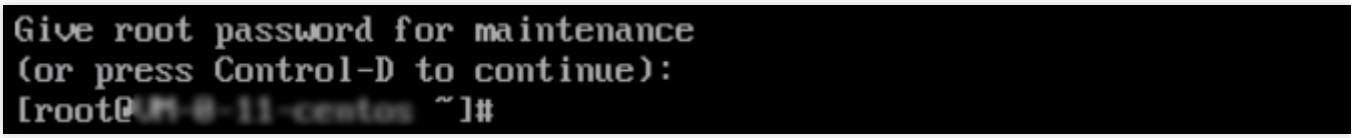
`/etc/fstab` 이 제대로 구성되지 않았습니다.
예를 들어 `/etc/fstab` 파일의 장치 이름을 기반으로 디스크 자동 연결을 구성했습니다. CVM이 다시 시작될 때 장치 이름이 변경되면 이 구성으로 인해 시스템이 정상적으로 시작되지 않습니다.

해결 방식

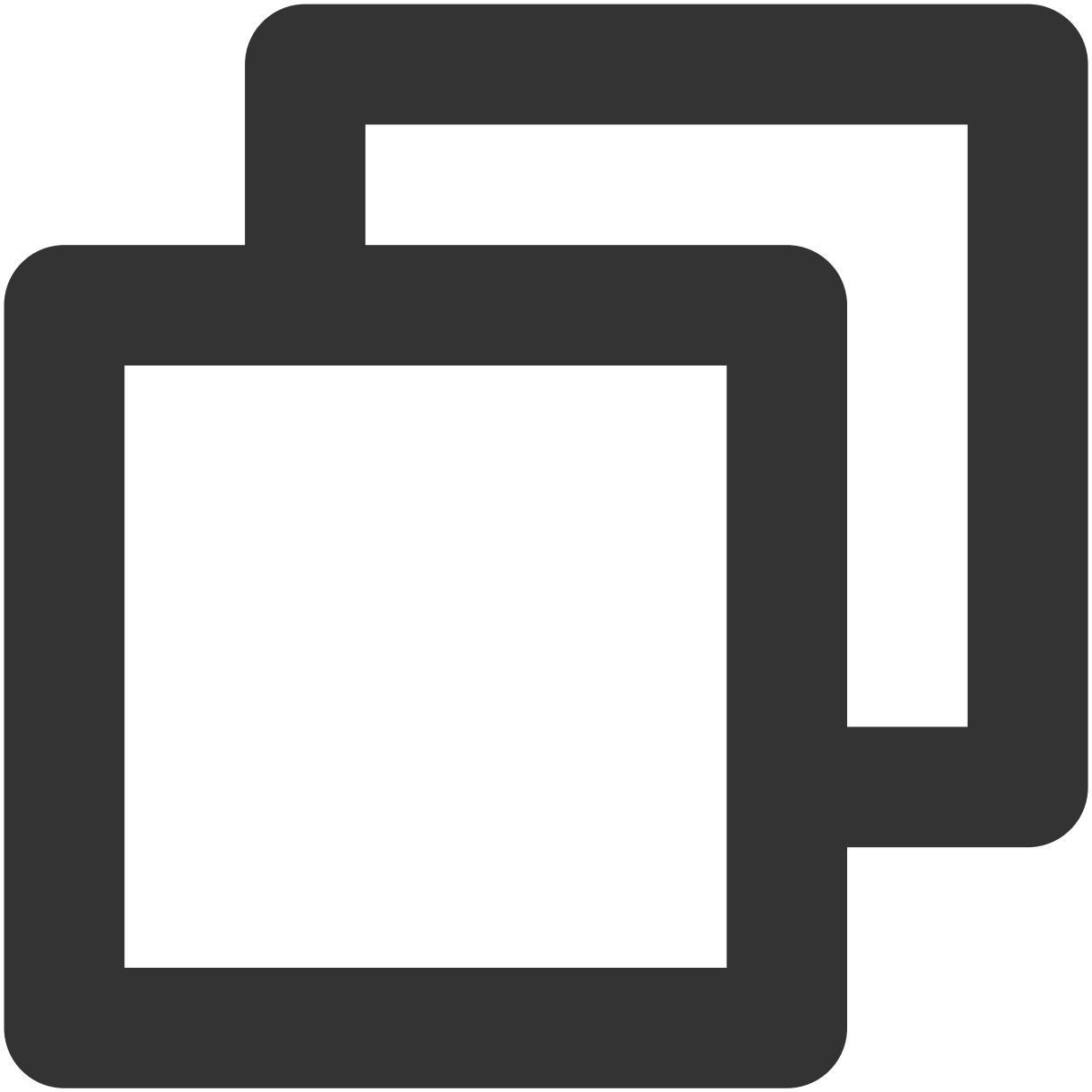
`/etc/fstab` 구성 파일을 복구하려면 처리 단계를 참고하십시오. 그 다음 CVM을 다시 시작하여 복구된 파일을 확인합니다.

처리 단계

1. 처리 1단계에 따라 VNC를 통해 Linux 인스턴스에 로그인합니다.
2. VNC 인터페이스에 진입하면 오류 설명과 같은 인터페이스를 볼 수 있습니다. root 계정 암호(기본적으로 표시되지 않음)를 입력하고 **Enter**를 눌러 서버에 로그인합니다.



3. 시스템 진입 후 다음 명령어를 실행하여 fstab 파일의 드라이브 문자 정보가 올바른지 확인합니다.



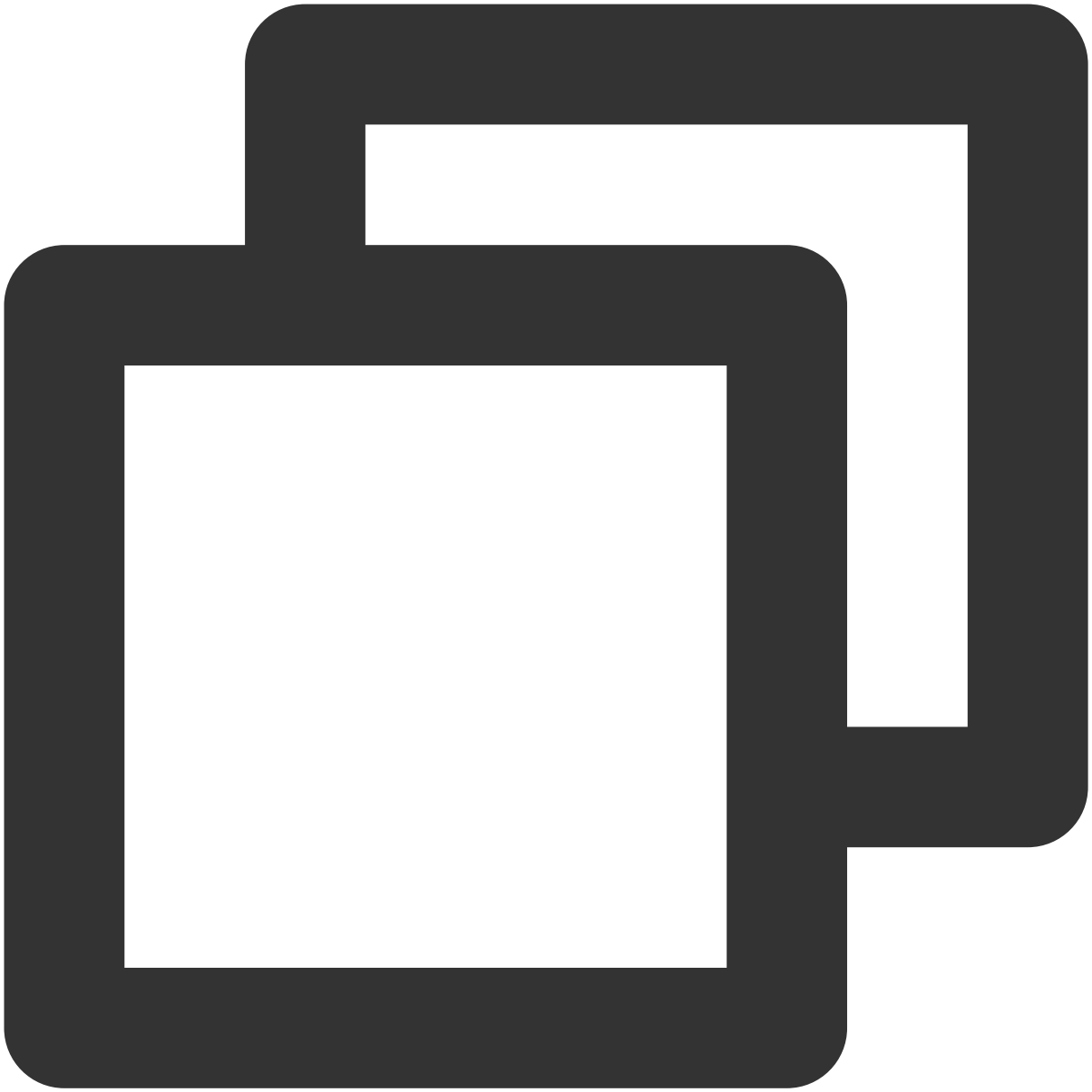
```
lsblk
```

아래 표시된 결과가 반환되면 파일의 드라이브 문자가 잘못된 것입니다.

```
[root@                    ~]# lsblk
NAME    MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sr0      11:0    1 184.1M  0 rom
vda     253:0    0    50G  0 disk
└─vda1  253:1    0    50G  0 part /
[root@                    ~]# cat /etc/fstab

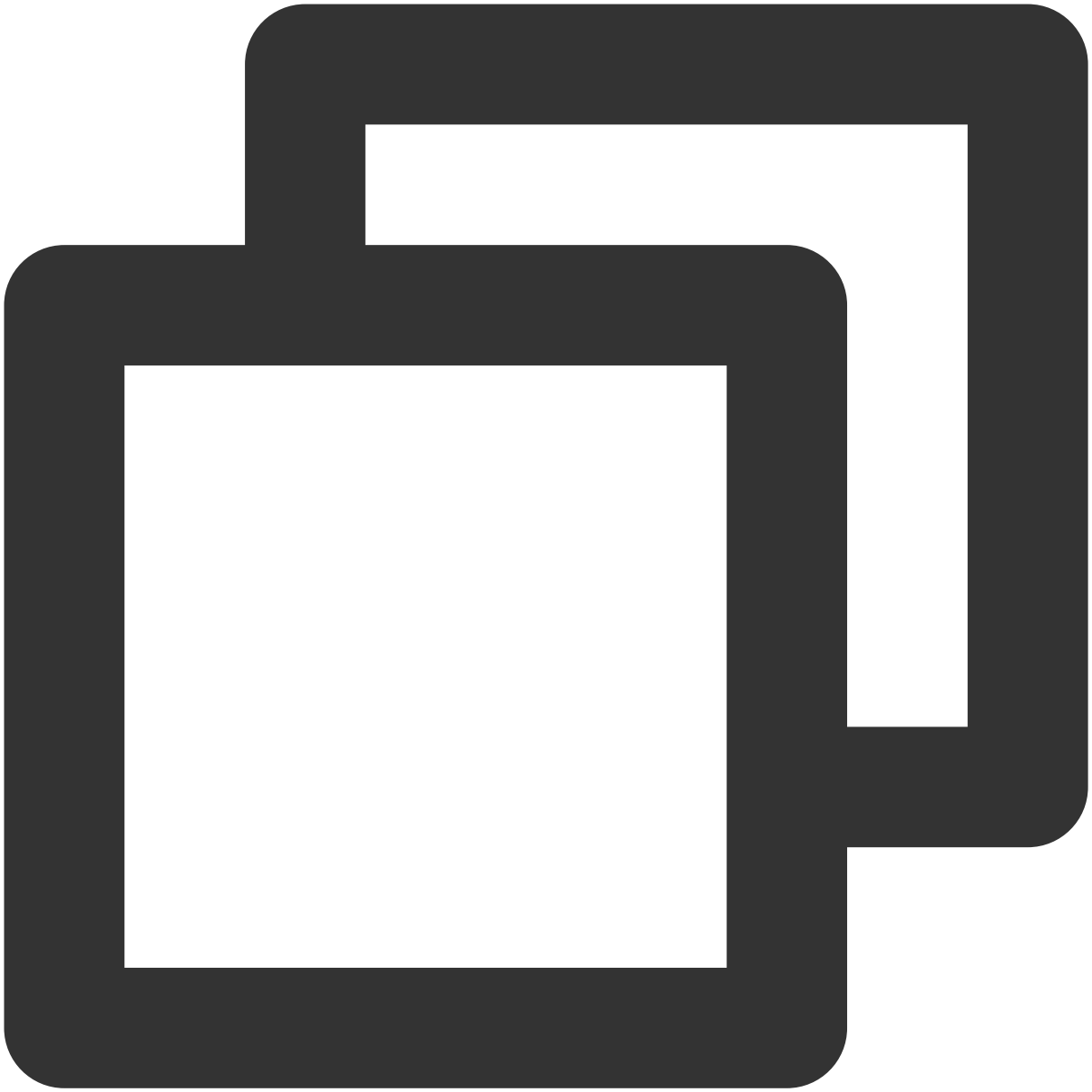
#
# /etc/fstab
# Created by anaconda on Tue Nov 26 02:11:36 2019
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
UUID=659e6f89-71fa-463d-842e-ccdf2c06e0fe /                       ext4    defaul
/dev/vdb1       /data   ext3    defaults        0       0
[root@                    ~]#
```

4. 다음 명령어를 실행하여 fstab 파일을 백업합니다.



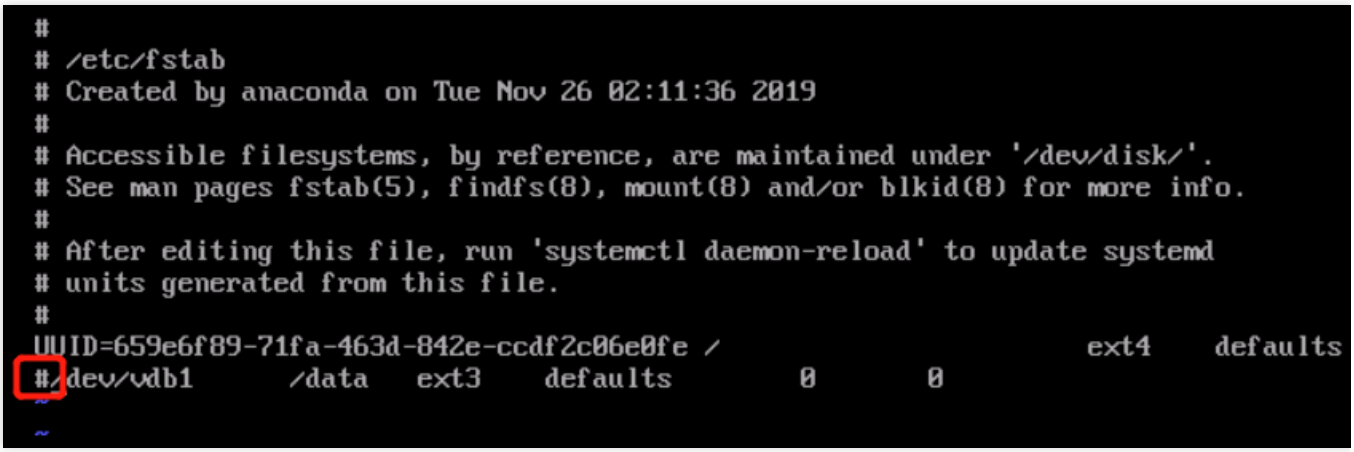
```
cp /etc/fstab /home
```

5. 다음 명령어를 실행하여 VI 편집기를 사용하여 `/etc/fstab` 파일을 엽니다.



```
vi /etc/fstab
```

6. **i**를 눌러 편집 모드로 들어갑니다. 커서를 오류 줄의 시작 부분으로 이동하고 `#` 을 입력하여 이 구성을 주석 처리합니다.



7. **Esc**를 누르고 **:wq**를 입력한 다음 **Enter**를 눌러 구성을 저장하고 편집기를 종료합니다.
8. 콘솔을 통해 인스턴스를 다시 시작합니다. 자세한 내용은 인스턴스 재시작을 참고하십시오.
9. 정상적으로 실행 및 로그인할 수 있는지 확인합니다.

복구 모드를 사용하여 Linux 시스템 시작 실패 문제 해결

오류 설명

Linux 시스템이 다시 시작된 후 인스턴스를 정상적으로 시작할 수 없습니다. 프롬프트 메시지에는 FAILED 시작 실패 항목이 많이 있습니다.

예상 원인

다음과 같은 주요 시스템 파일. .bin 및 .lib 파일이 없습니다.

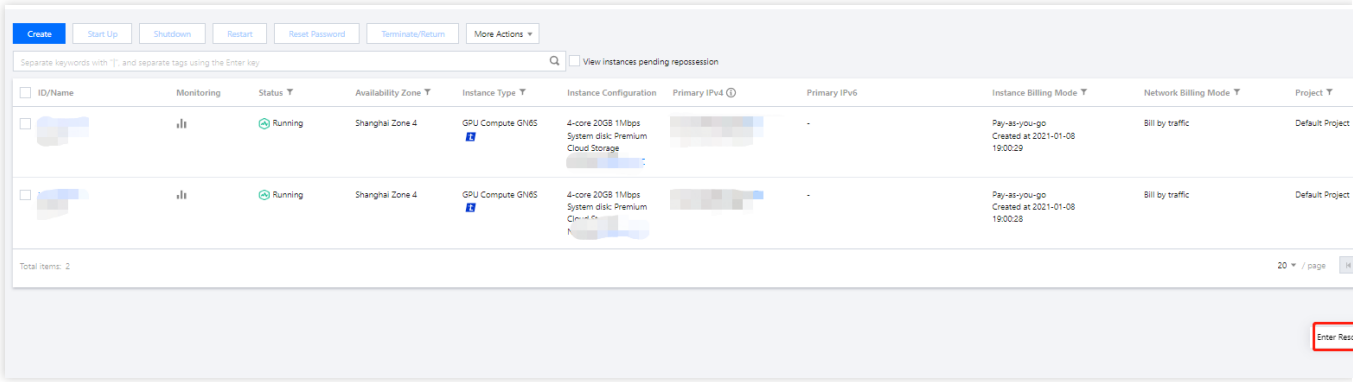
해결 방식

문제 해결을 위해 콘솔을 통해 인스턴스 복구 모드로 들어가려면 처리 단계를 참고하십시오.

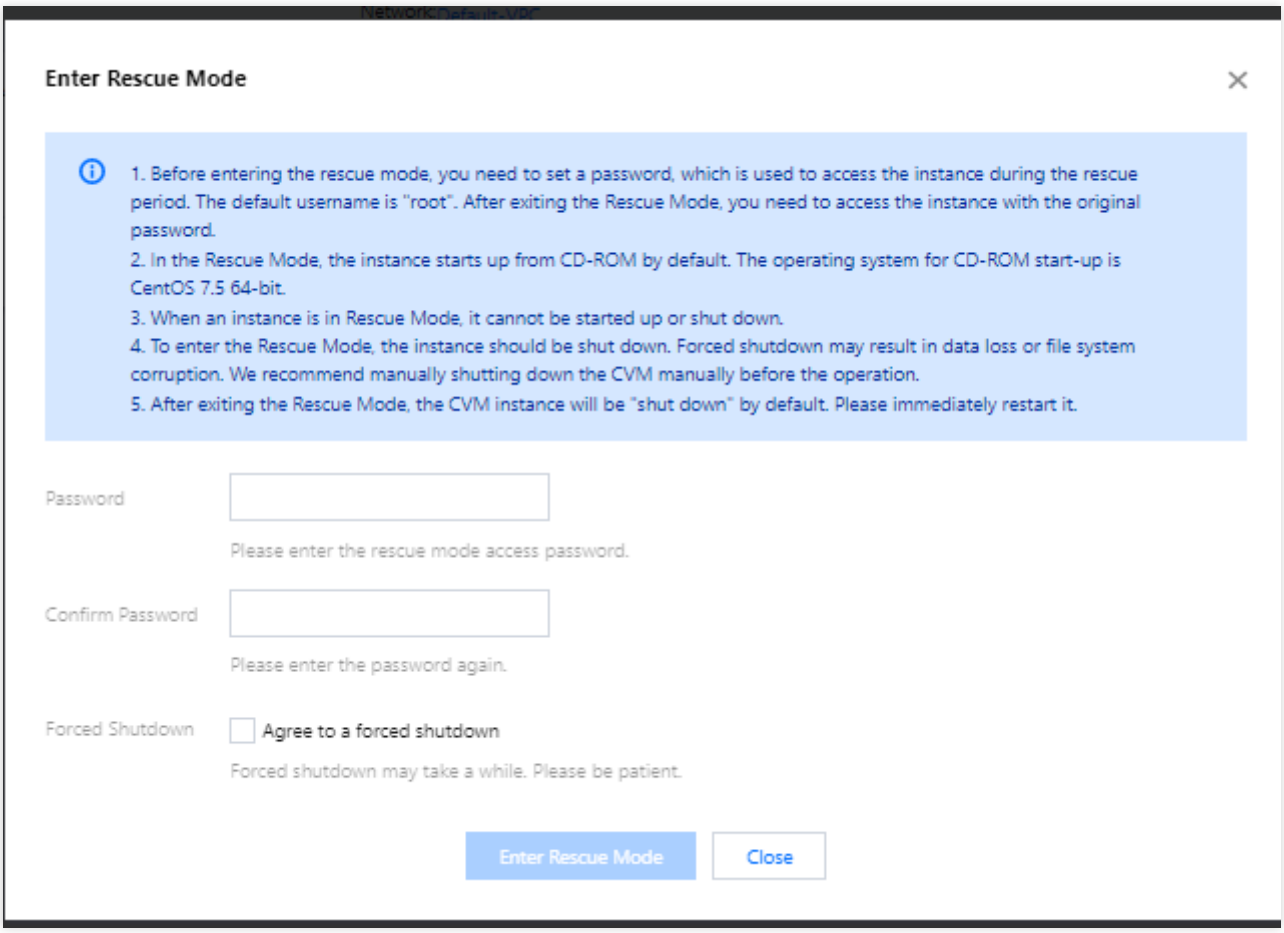
처리 단계

1. 복구 모드로 들어가기 전에 오작동의 영향을 피하기 위해 인스턴스를 백업하는 것이 좋습니다. Creating Snapshots을 통해 클라우드 디스크를 백업하고 커스텀 미러 구축을 통해 로컬 시스템 디스크를 백업합니다.

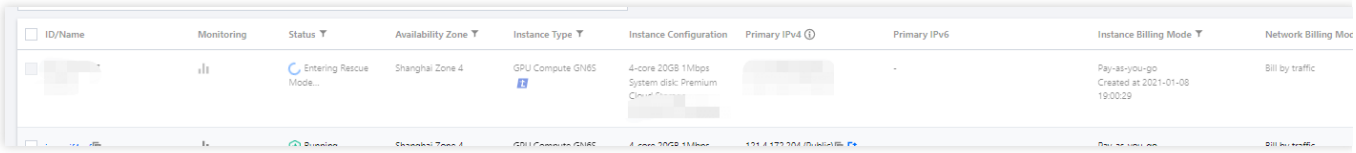
2. CVM 콘솔에 로그인합니다. '인스턴스' 페이지에서 대상 인스턴스를 찾아 **더 보기** > **Ops 및 점검** > **복구 모드 진입**을 선택합니다.



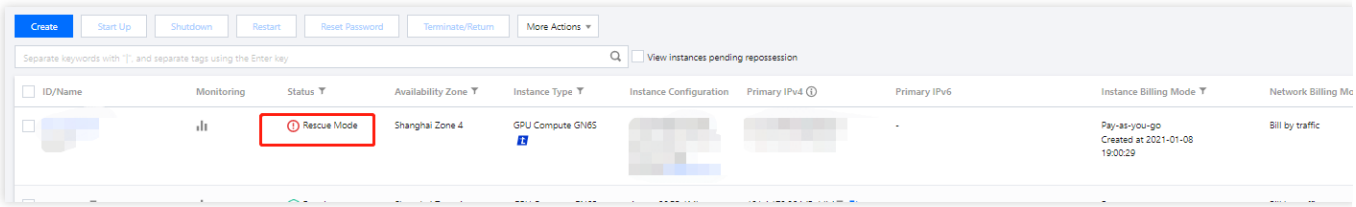
3. '복구 모드 시작' 팝업 창에서 복구 모드에서 인스턴스에 로그인하기 위한 비밀번호를 설정합니다. 아래 이미지와 같습니다.



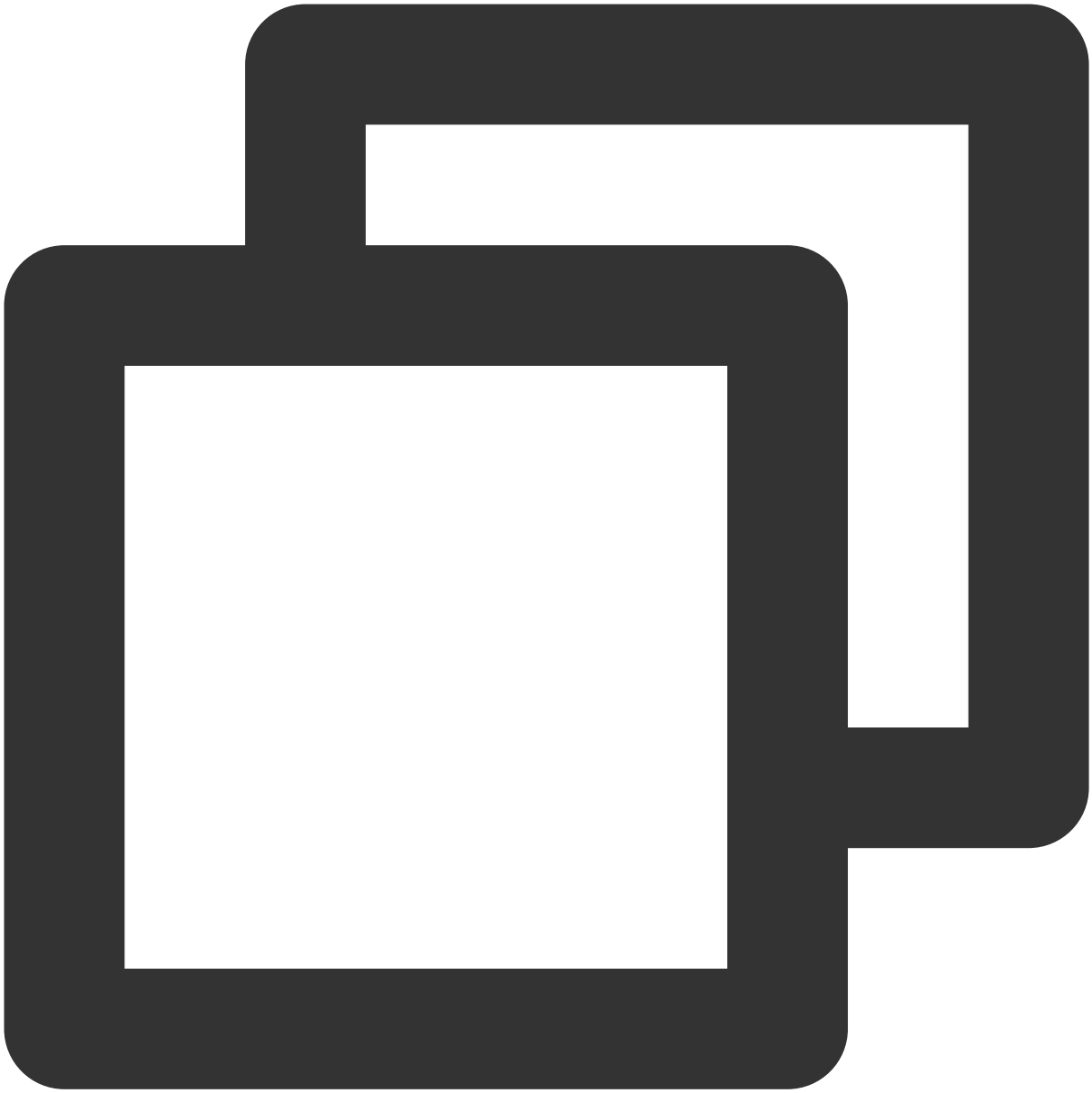
4. **복구 모드 진입**을 클릭하면 인스턴스 상태가 '복구 모드 진입'으로 변경되며 일반적으로 몇 분 안에 완료됩니다.



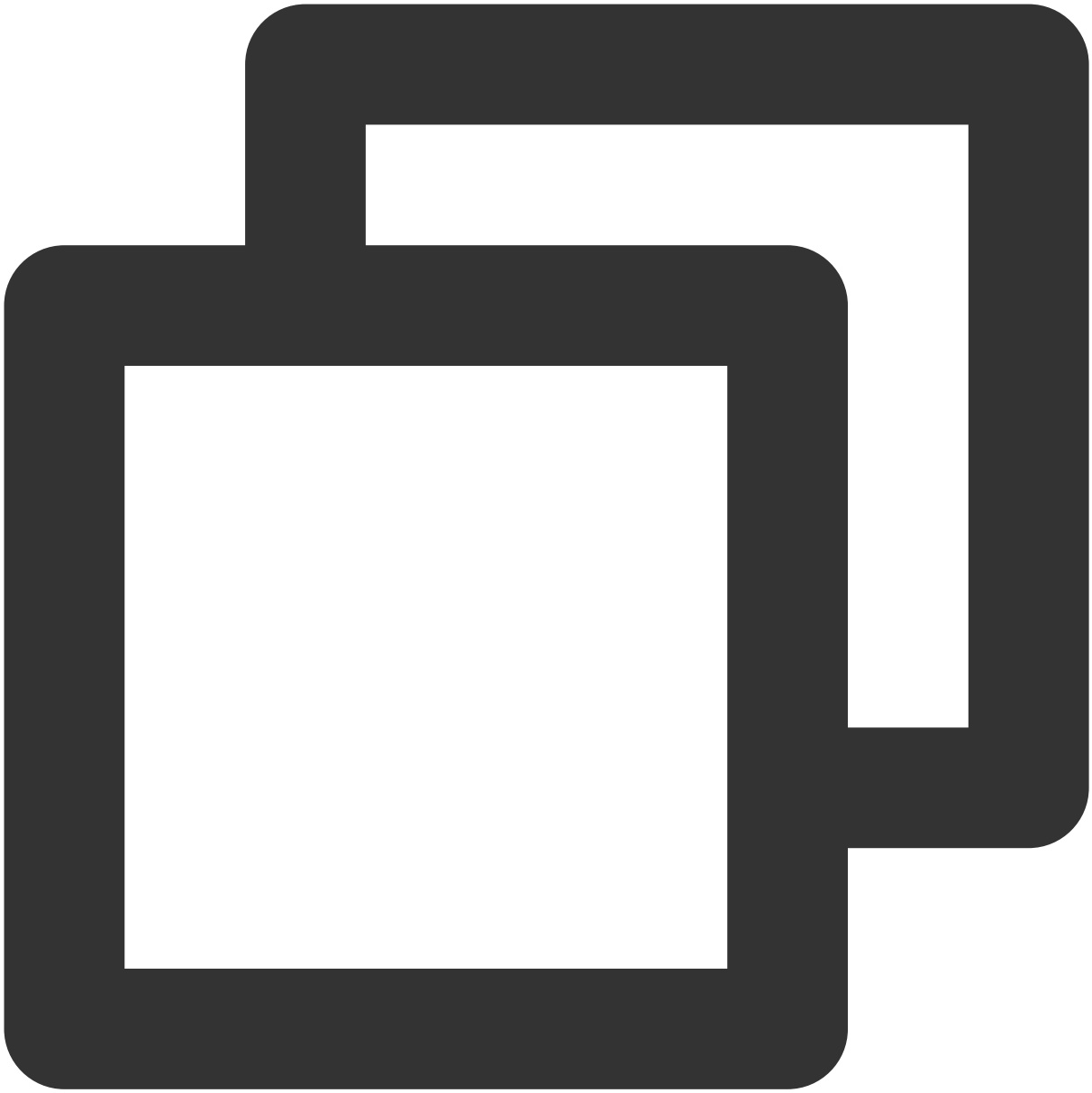
복구 모드에 진입한 인스턴스의 상태가 빨간색 느낌표와 함께 '복구 모드'로 변경됩니다.



5. 3단계에서 설정한 'root' 계정과 비밀번호로 다음과 같이 인스턴스에 로그인합니다.
인스턴스에 공용 IP가 있는 경우 SSH를 사용하여 Linux 인스턴스에 로그인을 참고하십시오.
인스턴스에 공용 IP가 없는 경우 VNC를 사용하여 Linux 인스턴스에 로그인을 참고하십시오.
6. 본 문서는 VNC를 통한 로그인을 예로 들어 설명합니다. 로그인에 성공하면 다음 명령을 순서대로 실행하여 시스템 디스크의 루트 파티션을 마운트합니다.
설명：
복구 모드에서 인스턴스 시스템 디스크의 장치 이름은 vda이고 루트 파티션은 vda1이며 기본적으로 마운트 해제되어 있습니다.

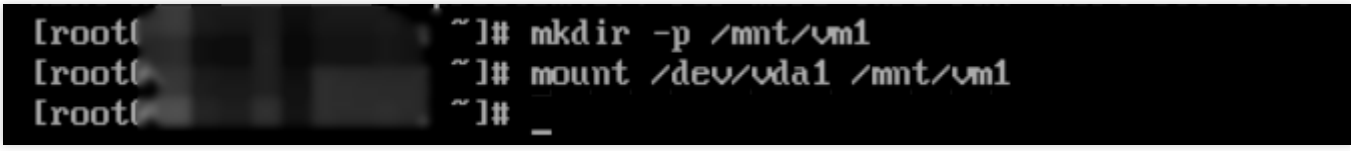


```
mkdir -p /mnt/vm1
```

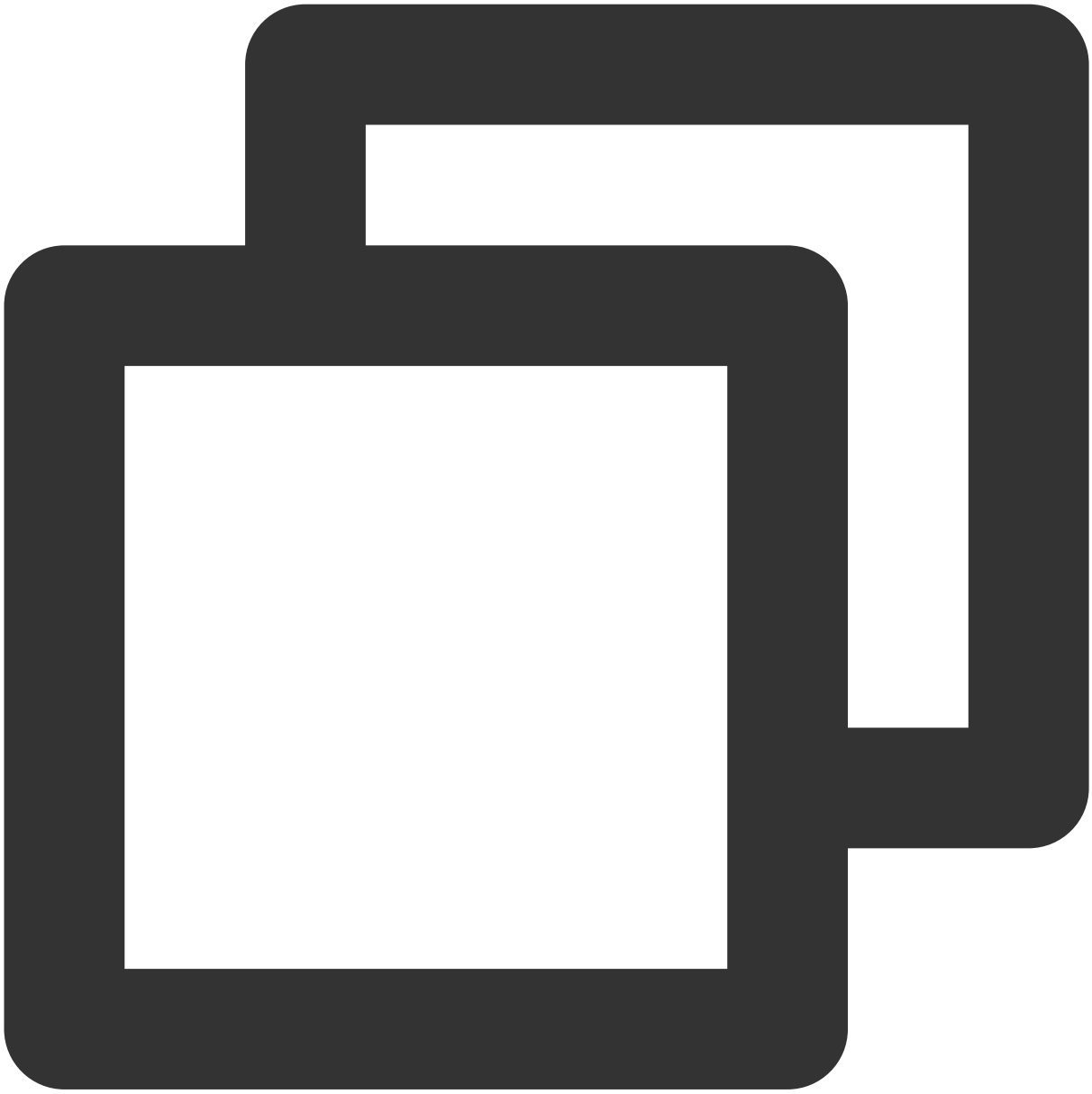


```
mount /dev/vda1 /mnt/vm1
```

실행 완료 후, 반환 결과는 아래와 같습니다.



7. 성공적으로 마운트한 후 원본 시스템의 루트 파티션에 있는 데이터를 조작할 수 있습니다.
또한 `mount -o bind` 명령을 사용하여 원본 파일 시스템의 일부 서브 디렉터리를 마운트하고 `chroot` 명령을 사용하여 지정된 루트 디렉터리에서 명령을 실행할 수도 있습니다. 구체적인 명령은 다음과 같습니다.



```
mount -o bind /dev /mnt/vm1/dev
mount -o bind /dev/pts /mnt/vm1/dev/pts
mount -o bind /proc /mnt/vm1/proc
mount -o bind /run /mnt/vm1/run
mount -o bind /sys /mnt/vm1/sys
chroot /mnt/vm1 /bin/bash
```

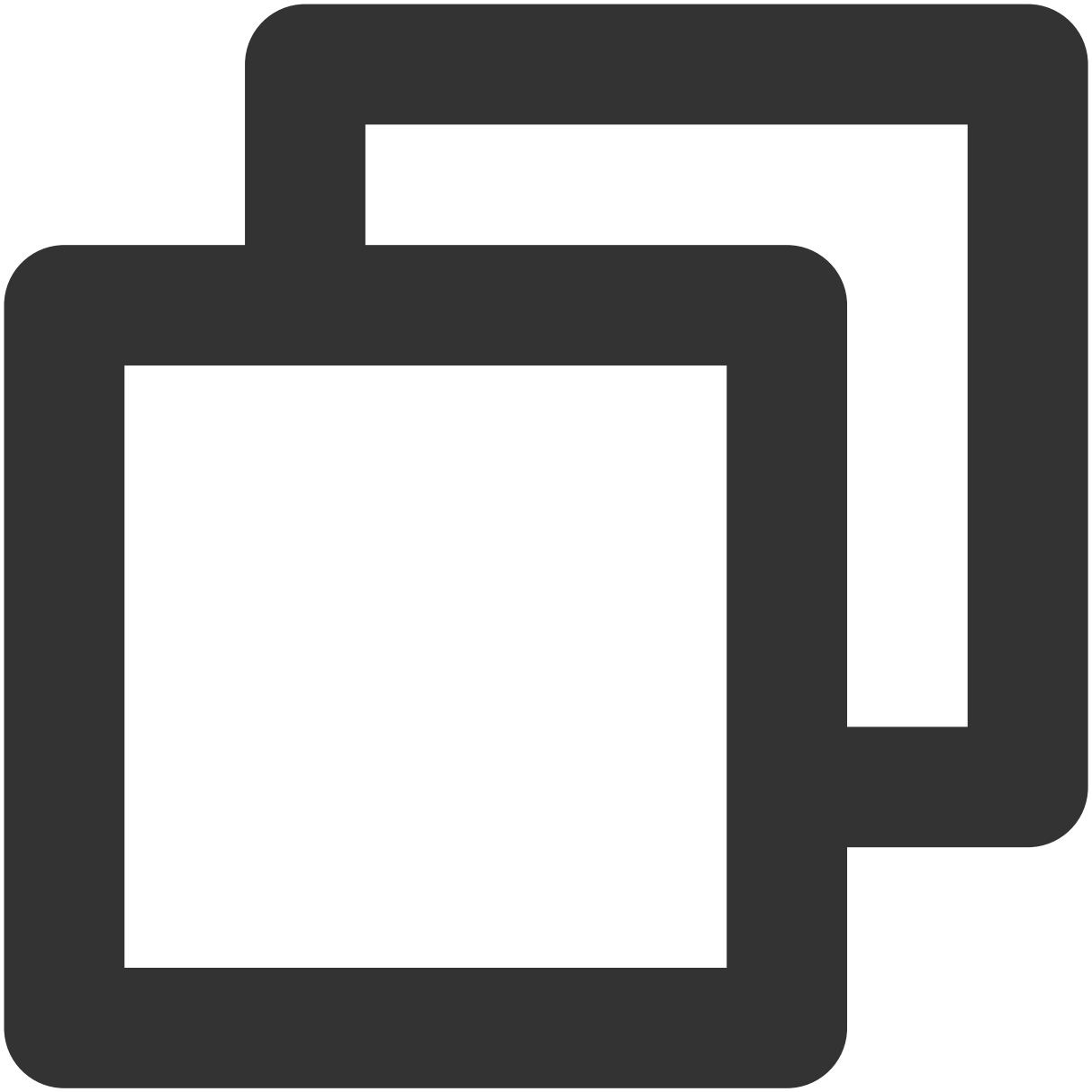
`chroot` 명령을 실행할 때:
오류 메시지가 없으면 `cd /` 명령을 계속 실행할 수 있습니다.
아래와 같은 에러 메시지가 나타나면 루트 디렉터리를 정상적으로 전환할 수 없습니다. 이 경우 `cd /mnt/vm1` 을 실행하여 루트 파티션 데이터를 볼 수 있습니다.

```
[root@VM-0-11-centos ~]# mkdir -p /mnt/vm1
[root@VM-0-11-centos ~]# mount /dev/vda1 /mnt/vm1
[root@VM-0-11-centos ~]# mount -o bind /dev /mnt/vm1/dev
[root@VM-0-11-centos ~]# mount -o bind /dev/pts /mnt/vm1/dev/pts
[root@VM-0-11-centos ~]# mount -o bind /proc /mnt/vm1/proc
[root@VM-0-11-centos ~]# mount -o bind /run /mnt/vm1/run
[root@VM-0-11-centos ~]# mount -o bind /sys /mnt/vm1/sys
[root@VM-0-11-centos ~]# chroot /mnt/vm1 /bin/bash
chroot: failed to run command '/bin/bash': No such file or director
[root@VM-0-11-centos ~]#
```

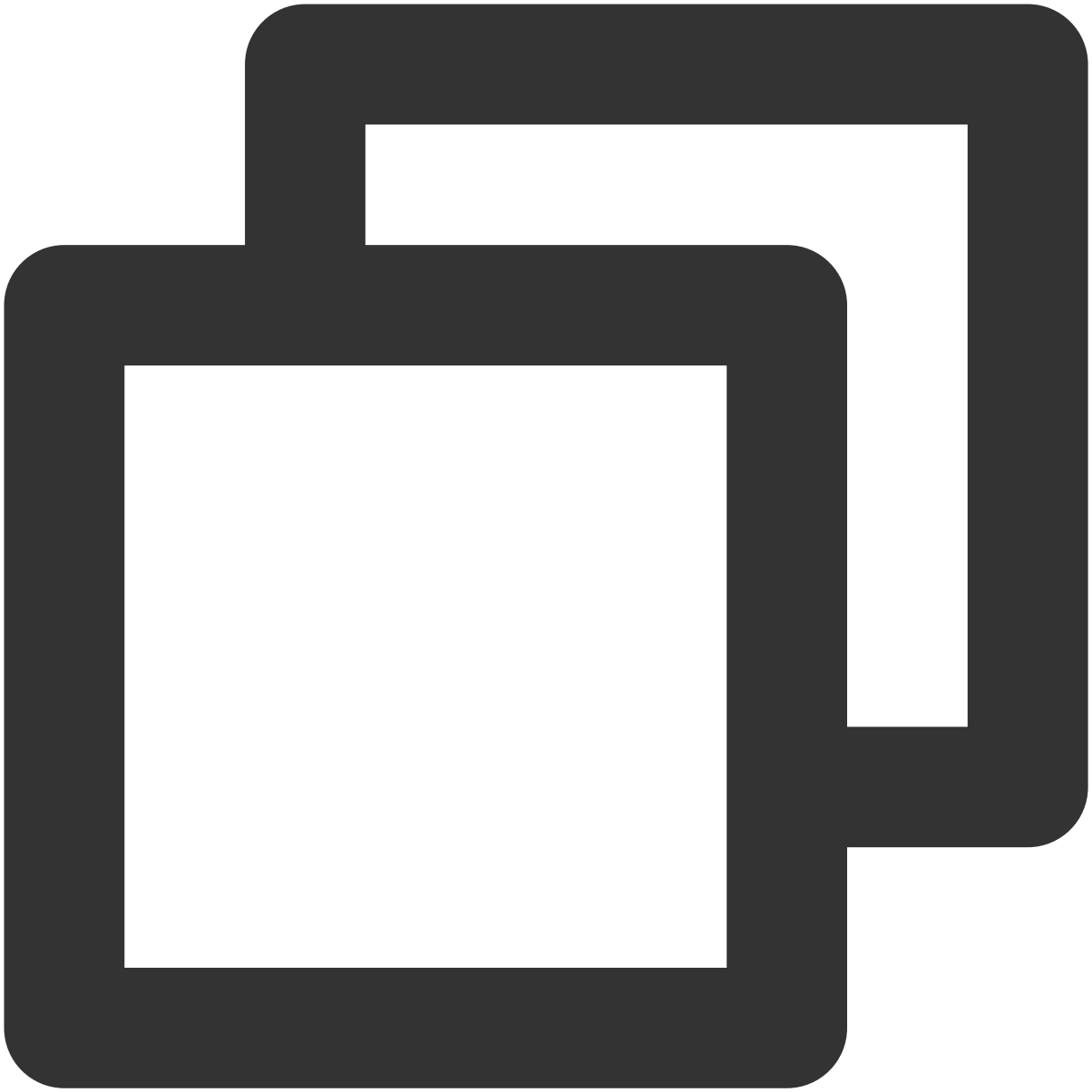
8. 명령을 통해 원래 시스템 루트 파티션의 `/usr/bin` 디렉터리에 있는 모든 파일이 삭제되었는지 확인할 수 있습니다.

```
bin  boot  data  dev  etc  home  lib  lib64  lost+found  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr
[root@VM-0-11-centos vm1]# ll
total 72
lrwxrwxrwx    1 root root     7 Nov  3  2020 bin -> usr/bin
dr-xr-xr-x.   5 root root  4096 Apr 14 17:53 boot
drwxr-xr-x    2 root root  4096 Dec 10  2019 data
drwxr-xr-x   19 root root  3260 Apr 14 18:09 dev
drwxr-xr-x. 100 root root 12288 Apr 14 17:53 etc
drwxr-xr-x.   2 root root  4096 Jun 28  2021 home
lrwxrwxrwx    1 root root     7 Nov  3  2020 lib -> usr/lib
lrwxrwxrwx    1 root root     9 Nov  3  2020 lib64 -> usr/lib64
drwx------.   2 root root 16384 Nov 26  2019 lost+found
drwxr-xr-x.   2 root root  4096 Nov  3  2020 media
drwxr-xr-x.   2 root root  4096 Nov  3  2020 mnt
drwxr-xr-x.   2 root root  4096 Nov  3  2020 opt
dr-xr-xr-x  125 root root     0 Apr 14 18:08 proc
dr-xr-x---.   5 root root  4096 Mar 10 19:24 root
drwxr-xr-x   37 root root  1140 Apr 14 18:10 run
lrwxrwxrwx    1 root root     8 Nov  3  2020 sbin -> usr/sbin
drwxr-xr-x.   2 root root  4096 Nov  3  2020 srv
dr-xr-xr-x   13 root root     0 Apr 14 18:12 sys
drwxrwxrwt.   8 root root  4096 Apr 14 17:56 tmp
drwxr-xr-x.  12 root root  4096 Jun 10  2021 usr
drwxr-xr-x.  20 root root  4096 Jun 10  2021 var
[root@VM-0-11-centos vm1]# cd ./usr/bin/
[root@VM-0-11-centos bin]# pwd
/mnt/vm1/usr/bin
[root@VM-0-11-centos bin]# ls
[root@VM-0-11-centos bin]#
```

9. 이 경우 동일한 운영체제를 사용하여 일반 인스턴스를 생성하고, 다음 명령어를 실행하여 정상 시스템의 `/usr/bin` 디렉터리에 있는 파일을 압축하여 비정상 인스턴스에 원격으로 복사할 수 있습니다.
일반 인스턴스의 경우 다음 명령을 순서대로 실행합니다.



```
cd /usr/bin/ && tar -zcvf bin.tar.gz *
```



```
scp bin.tar.gz root@비정상 인스턴스ip:/mnt/vm1/usr/bin/
```

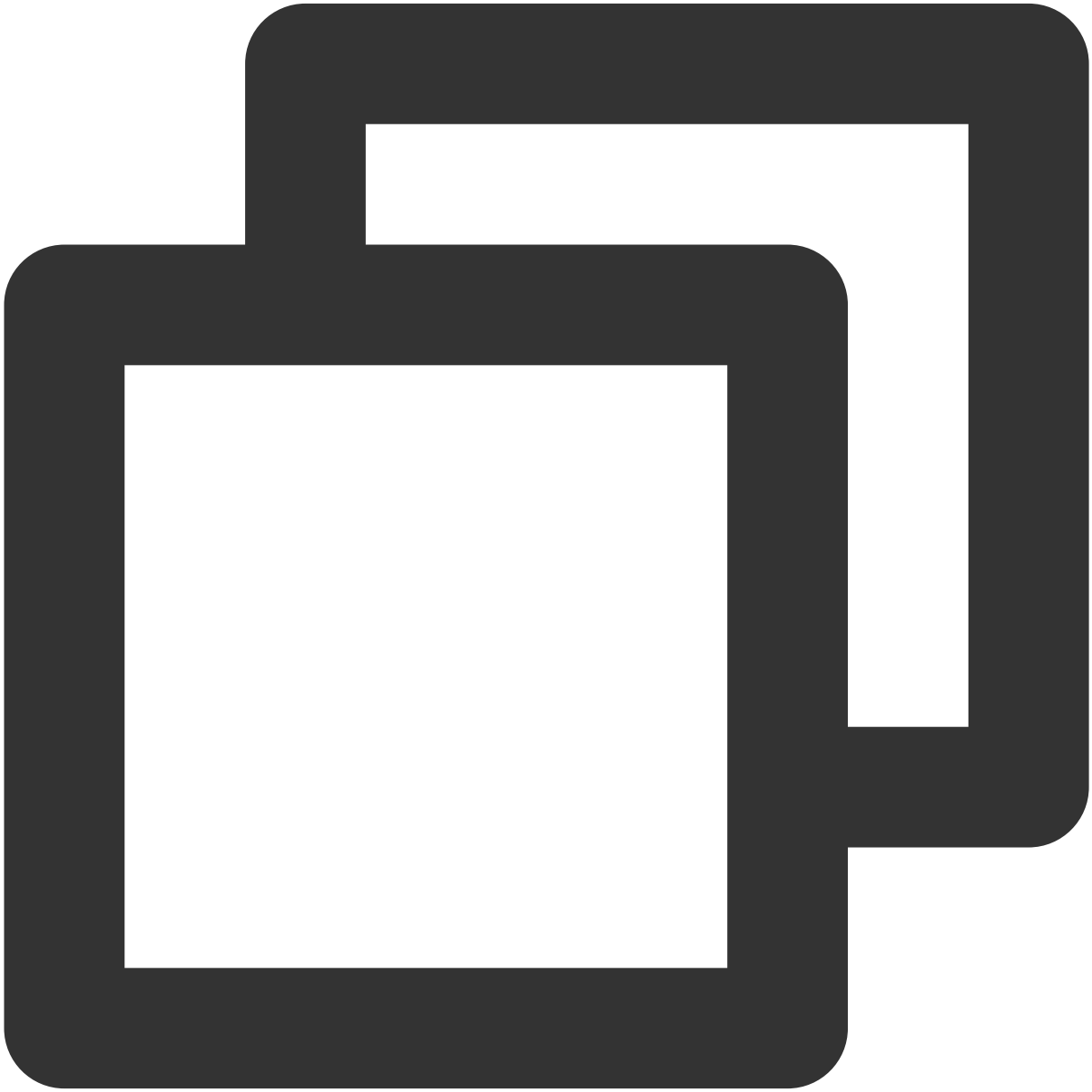
설명：

인스턴스에 공인 IP가 있는 경우 공중망을 통해 복사를 수행할 수 있습니다. 그렇지 않으면 사설망을 통해 복사가 수행됩니다.

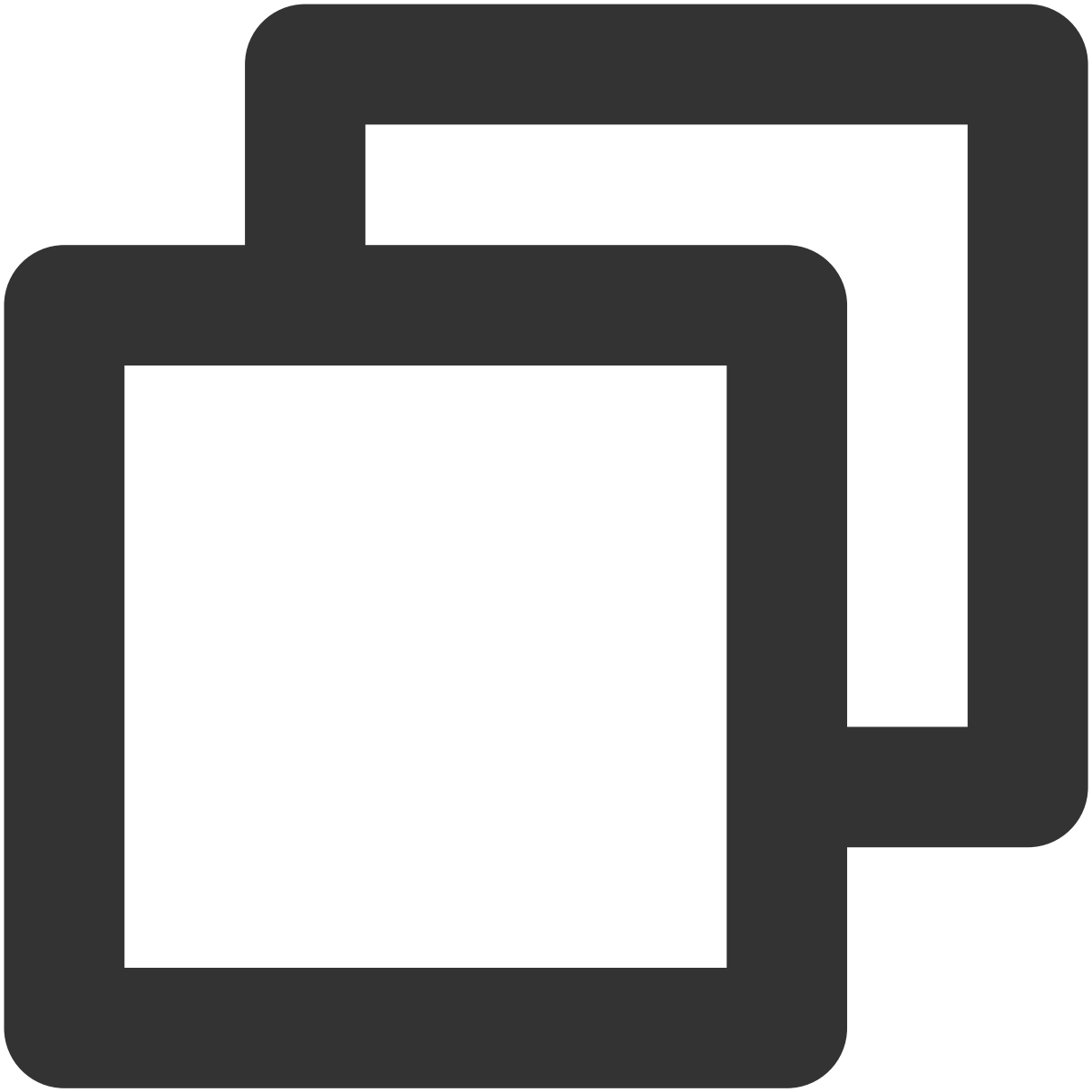
실행 결과는 다음 이미지와 같습니다.

```
[root@VM-10-12-centos bin]# scp bin.tar.gz root@81.70.163.225:/mnt/vm1/usr/bin/
The authenticity of host '81.70.163.225 (81.70.163.225)' can't be established.
ECDSA key fingerprint is SHA256:e+y4JYiXm44pGLmHaVo8ihDvNtbeA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '81.70.163.225' (ECDSA) to the list of known hosts.
root@81.70.163.225's password:
bin.tar.gz                                                    100%   33M
[root@VM-10-12-centos bin]#
```

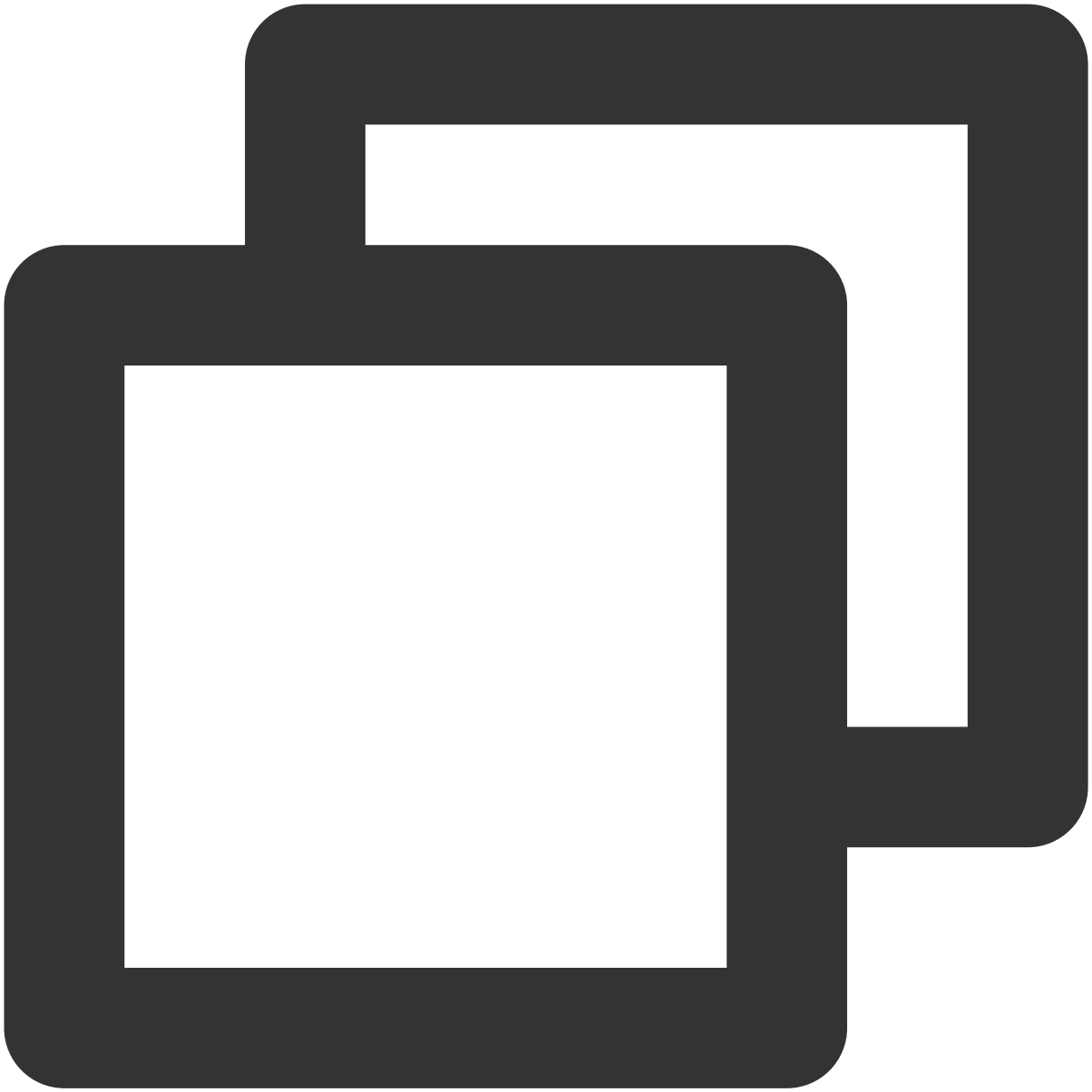
비정상 인스턴스의 경우 복구 모드에서 다음 명령을 순서대로 실행하십시오.



```
cd /mnt/vm1/usr/bin/
```

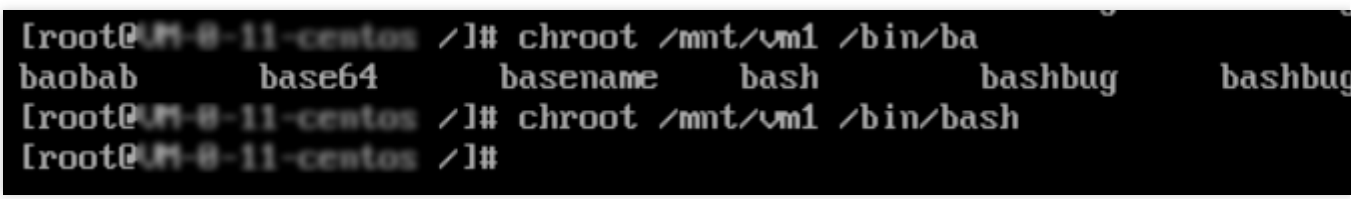


```
tar -zxvf bin.tar.gz
```

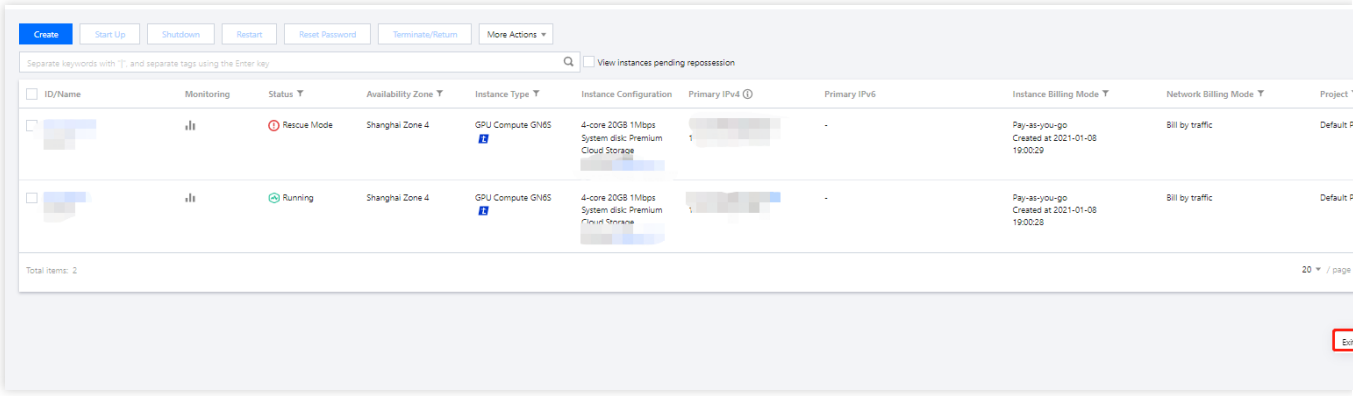


```
chroot /mnt/vm1 /bin/bash
```

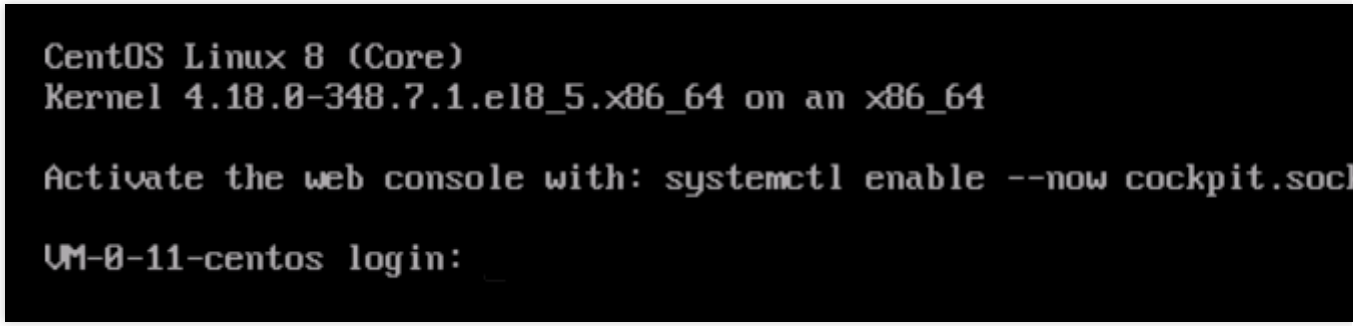
실행 결과는 다음 이미지와 같습니다.



10. 인스턴스를 복구한 후 대상 인스턴스의 작업 열에서 **더 보기** > **Ops 및 점검** > **복구 모드 종료**를 선택합니다. 아래 이미지와 같습니다.



11. 복구 모드를 종료한 후 인스턴스는 종료 상태가 됩니다. 인스턴스를 시작하여 시스템을 확인하십시오. 아래와 같이 시스템이 복구됩니다.



CVM 종료 및 재시작 실패

최종 업데이트 날짜: : 2024-02-02 11:09:48

CVM 종료, 재시작 작업 시 매우 낮은 확률로 종료 실패 또는 재시작 실패의 문제가 발생할 수 있습니다. 이러한 문제가 발생하면 CVM에서 아래와 같이 진단 및 처리할 수 있습니다.

예상 원인

CPU 또는 메모리 사용률이 지나치게 높을 수 있습니다.
Linux 운영 체제의 CVM에 ACPI 관리 프로그램이 설치되어 있지 않을 수 있습니다.
Windows 운영 체제의 CVM에서 시스템 업데이트 시간이 너무 길 경우 문제가 발생할 수 있습니다.
처음 Windows CVM을 구매했을 때, 해당 CVM의 초기화가 미완료 상태일 수 있습니다.
운영 체제에서 일부 소프트웨어를 설치하고 있거나 트로이 목마 바이러스에 감염되어 시스템 자체가 손상되었을 수 있습니다.

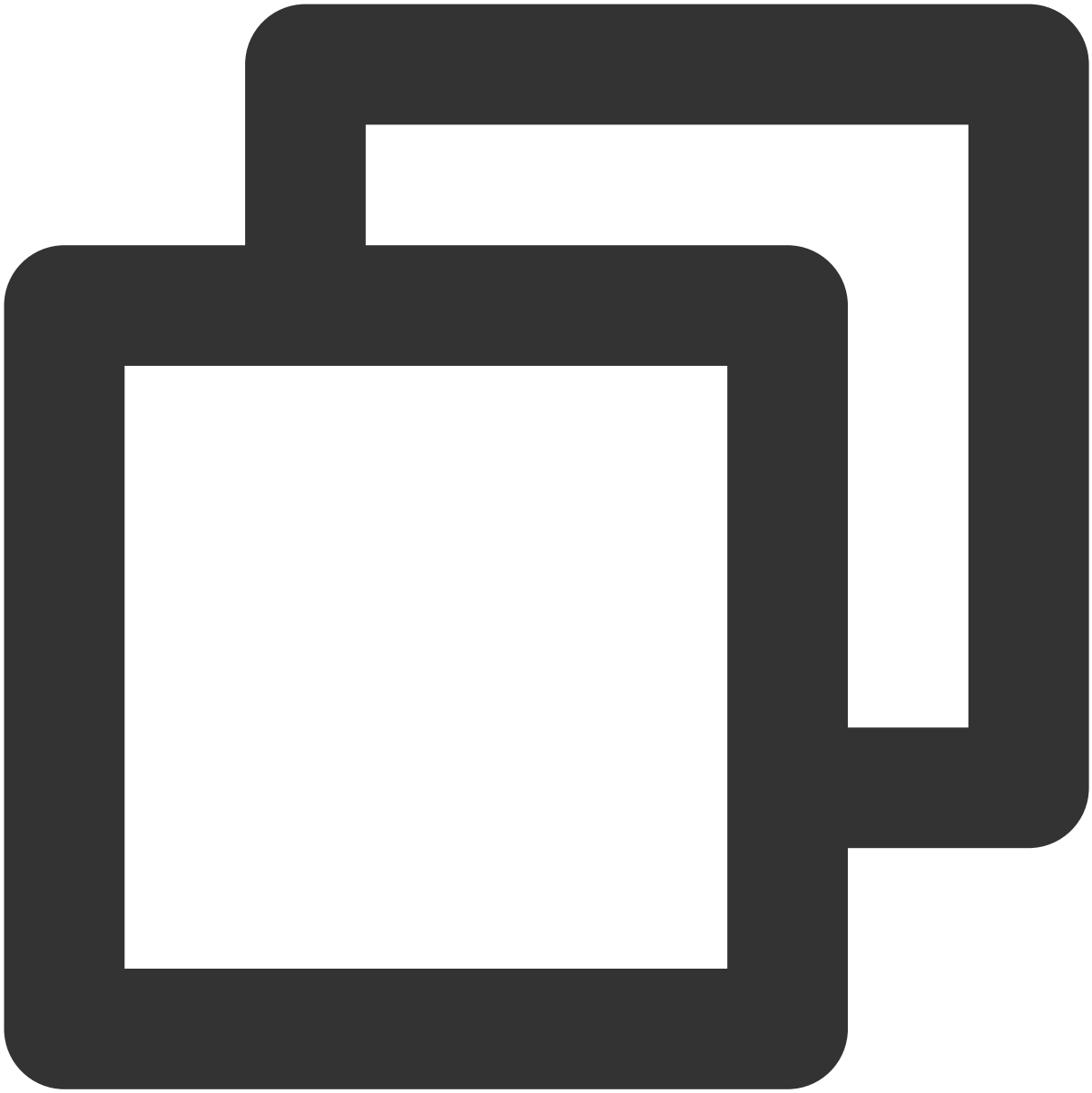
장애 처리

CPU/메모리의 사용 현황 확인

1. CVM 운영 체제의 유형에 따라 CPU/메모리의 사용 현황을 확인합니다.
Windows CVM: CVM에서 마우스 우클릭하여 '작업 표시줄'의 [작업 관리자]를 선택합니다.
Linux CVM: `top` 명령어를 실행하여 `%CPU` 열과 `%MEM` 열의 정보를 확인합니다.
2. 실제 CPU/메모리 사용량에 따라 CPU 또는 메모리 사용량이 지나치게 높은 프로세스를 종료합니다.
그래도 종료/재시작 할 수 없다면 강제 종료/재시작 기능을 실행하시기 바랍니다.

ACPI 관리 프로그램 설치 여부 확인

설명 :
해당 작업은 Linux 운영 체제의 CVM을 대상으로 합니다.
다음 명령어를 실행하여 ACPI 프로세스가 존재하는지 확인합니다.



```
ps -ef | grep -w "acpid" | grep -v "grep"
```

ACPI 프로세스가 존재한다면 강제 종료/재시작 기능을 실행하시기 바랍니다.

ACPI 프로세스가 존재하지 않는다면 ACPI 관리 프로그램을 설치하시기 바랍니다. 자세한 작업 내용은 Linux 전원 관리 구성을 참조 바랍니다.

WindowsUpdate 진행 여부 확인

설명 :

해당 작업은 Windows 운영 체제의 CVM을 대상으로 합니다.

Windows CVM 운영 체제 인터페이스에서 [시작]> [제어판]> [Windows 업데이트]를 클릭하여 현재 업데이트 중인 패치 또는 프로그램이 존재하는지 확인합니다.
Windows가 일부 패치 작업 중에 시스템을 종료할 때 일부 프로세스를 수행합니다. 이 때, 업데이트 시간이 너무 길면 종료/재시작에 실패할 수 있습니다. Windows 업데이트 완료를 기다린 후 다시 CVM의 작업을 종료/재시작 하길 권장합니다.
업데이트 중인 패치 또는 프로그램이 없다면, 강제 종료/재시작 기능을 실행하시기 바랍니다.

CVM의 초기화 완료 여부 확인

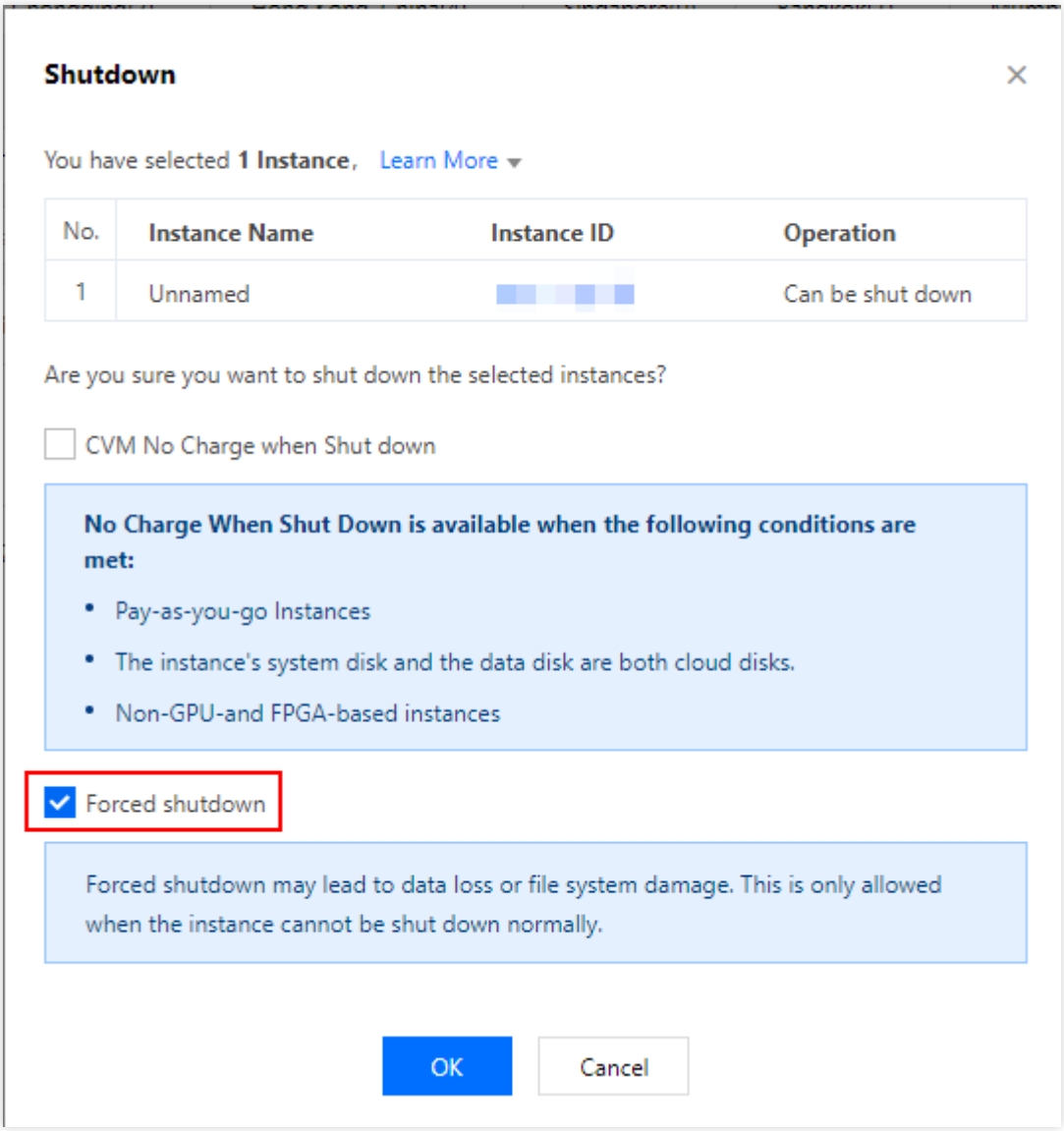
설명 :
해당 작업은 Windows 운영 체제의 CVM을 대상으로 합니다.
처음 Windows CVM을 구매했을 때, 시스템이 Sysprep 방식을 통해 이미지를 전송하기 때문에 초기화 과정에서 비교적 오랜 시간이 소요됩니다. 초기화가 완료되기 전까지 Windows에서 종료/재시작 작업을 생략하므로 작업에 실패할 수 있습니다.
구매한 Windows CVM이 초기화 중이라면, Windows CVM 초기화가 완료될 때까지 기다린 다음, CVM 작업 종료/재시작을 다시 시도하시길 권장합니다.
CVM이 이미 초기화를 완료했다면 강제 종료/재시작 기능을 실행하시기 바랍니다.

소프트웨어 정상 설치 여부 확인

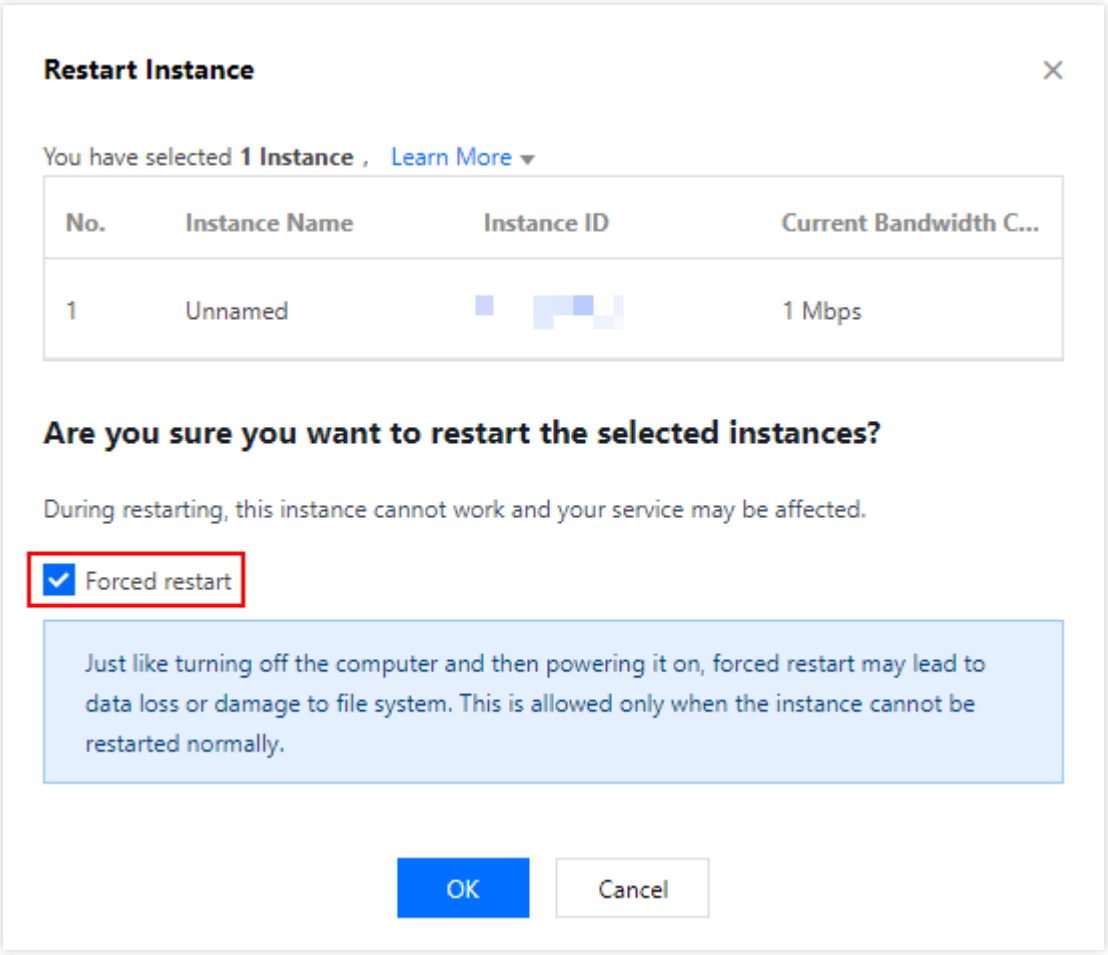
검사 툴 또는 바이러스 백신 소프트웨어를 통해 CVM에 설치된 소프트웨어가 정상적인지, 트로이 목마 등 바이러스에 감염되었는지 등을 확인합니다.
이상이 발견되면 시스템 자체가 손상되어 종료/재시작에 실패한 것일 수 있습니다. 해당 소프트웨어를 제거하고 보안 소프트웨어를 사용하여 바이러스 검출 또는 데이터 백업 후 시스템 재설치를 권장합니다.
이상이 발견되지 않으면 강제 종료/재시작 기능을 실행하시기 바랍니다.

강제 종료/재시작 기능

설명 :
Tencent Cloud는 CVM 종료/재시작에 여러 번 실패했을 때 사용할 수 있도록 강제 종료/재시작 기능을 제공하고 있습니다. 이 작업은 CVM을 강제로 **종료/재시작**하기 때문에, CVM 데이터 손실 또는 파일 시스템 손실을 일으킬 수 있습니다.
1. CVM 콘솔에 로그인합니다.
2. 인스턴스 관리 페이지에서 종료 또는 재시작 대기 중인 CVM을 선택하고 실제 수요에 맞는 작업을 진행합니다.
CVM 종료: [More]> [Instance Status]> [Shutdown]을 클릭합니다.
CVM 재시작: [More]> [Instance Status]> [Restart]를 클릭합니다.
3. 팝업된 'Shutdown' 또는 'Restart Instance' 창에서 [Forced Shutdown] 또는 [Forced Restart]를 체크하고 [확인]을 클릭합니다.
아래 이미지와 같이 [Forced Shutdown]에 체크합니다.



아래 이미지와 같이 [Forced Restart]에 체크합니다.



Network Namespace 생성 불가

최종 업데이트 날짜: : 2024-02-02 11:09:48

문제 설명

새로운 네트워크 네임스페이스(Network Namespace) 생성을 위한 커맨드 실행 시, 커맨드가 멈추며 작업이 진행되지 않습니다. Dmesg 정보 표시: “unregister_netdevice: waiting for lo to become free. Usage count = 1”

문제 원인

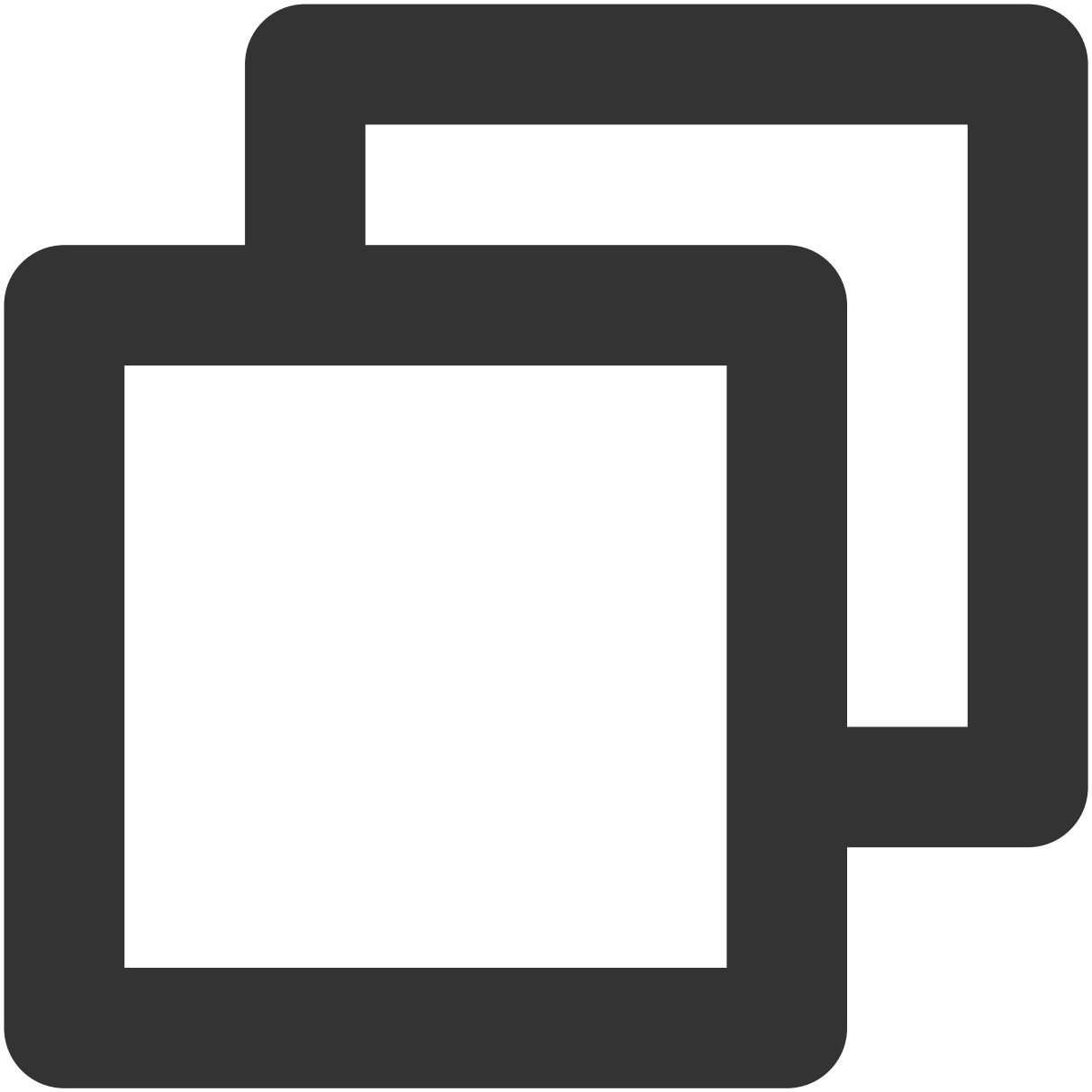
해당 문제는 커널의 bug입니다. 현재 아래의 커널 버전은 모두 bug가 존재합니다.
Ubuntu 16.04 x86_64 커널의 버전은 4.4.0-91-generic입니다.
Ubuntu 16.04 x86_32 커널의 버전은 4.4.0-92-generic입니다.

해결 방법

커널 버전을 4.4.0-98-generic 버전으로 업데이트하면 버전의 bug는 수정됩니다.

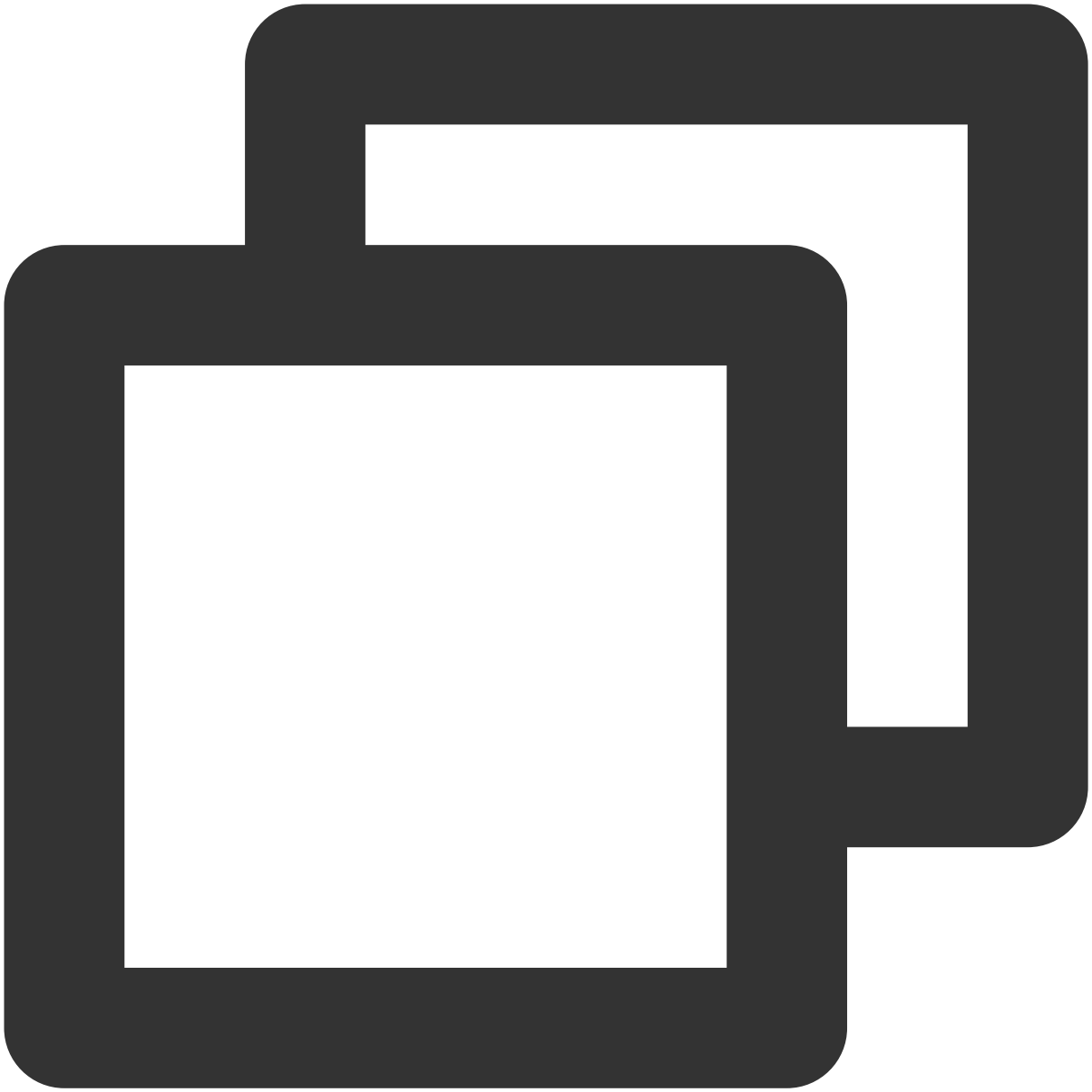
처리 순서

1. 아래의 명령어를 실행하여 현재 커널의 버전을 조회하십시오.



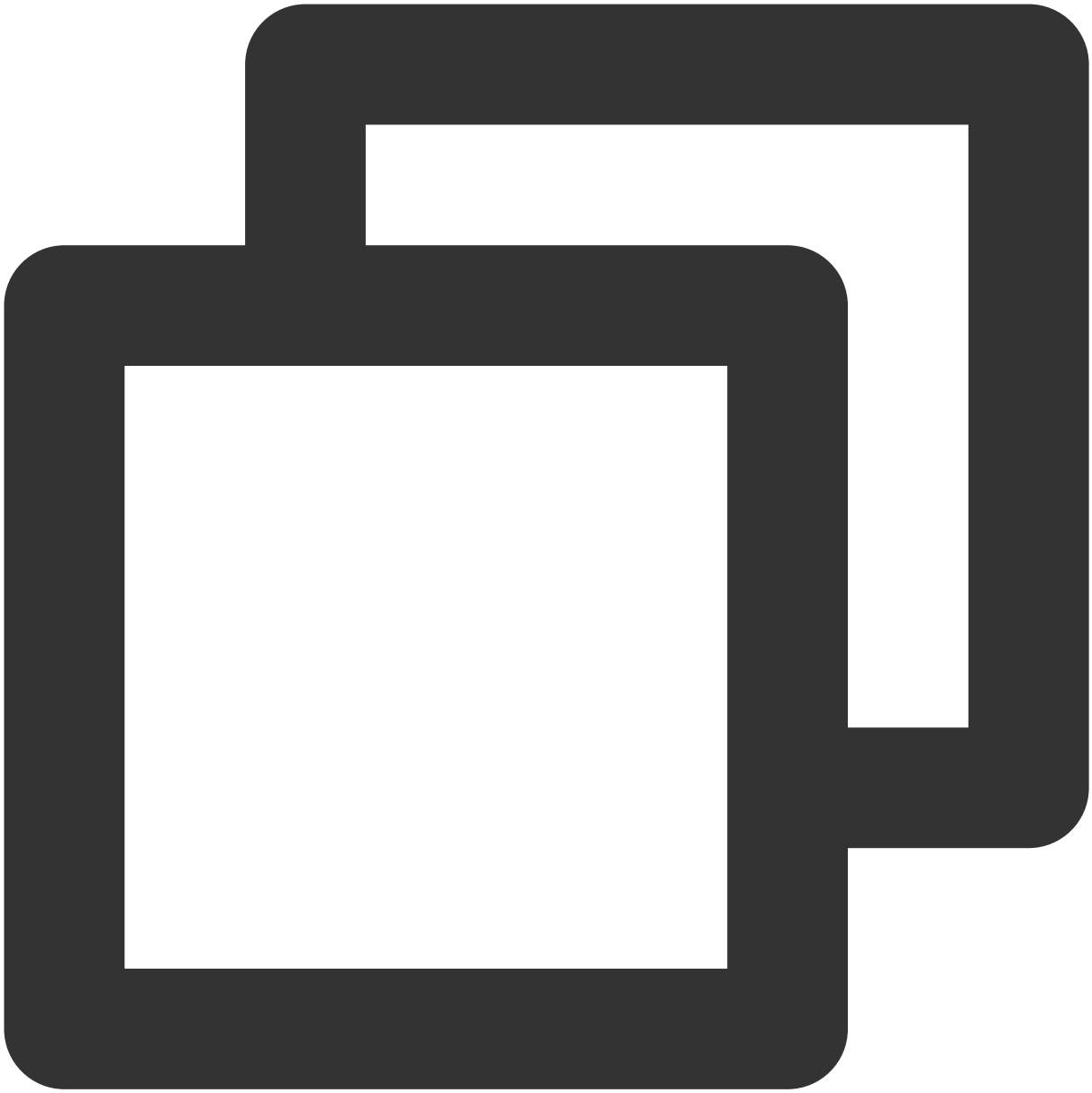
```
uname -r
```

2. 아래의 명령어를 실행하여 4.4.0-98-generic 버전으로 업데이트할 커널이 있는지 조회하십시오.



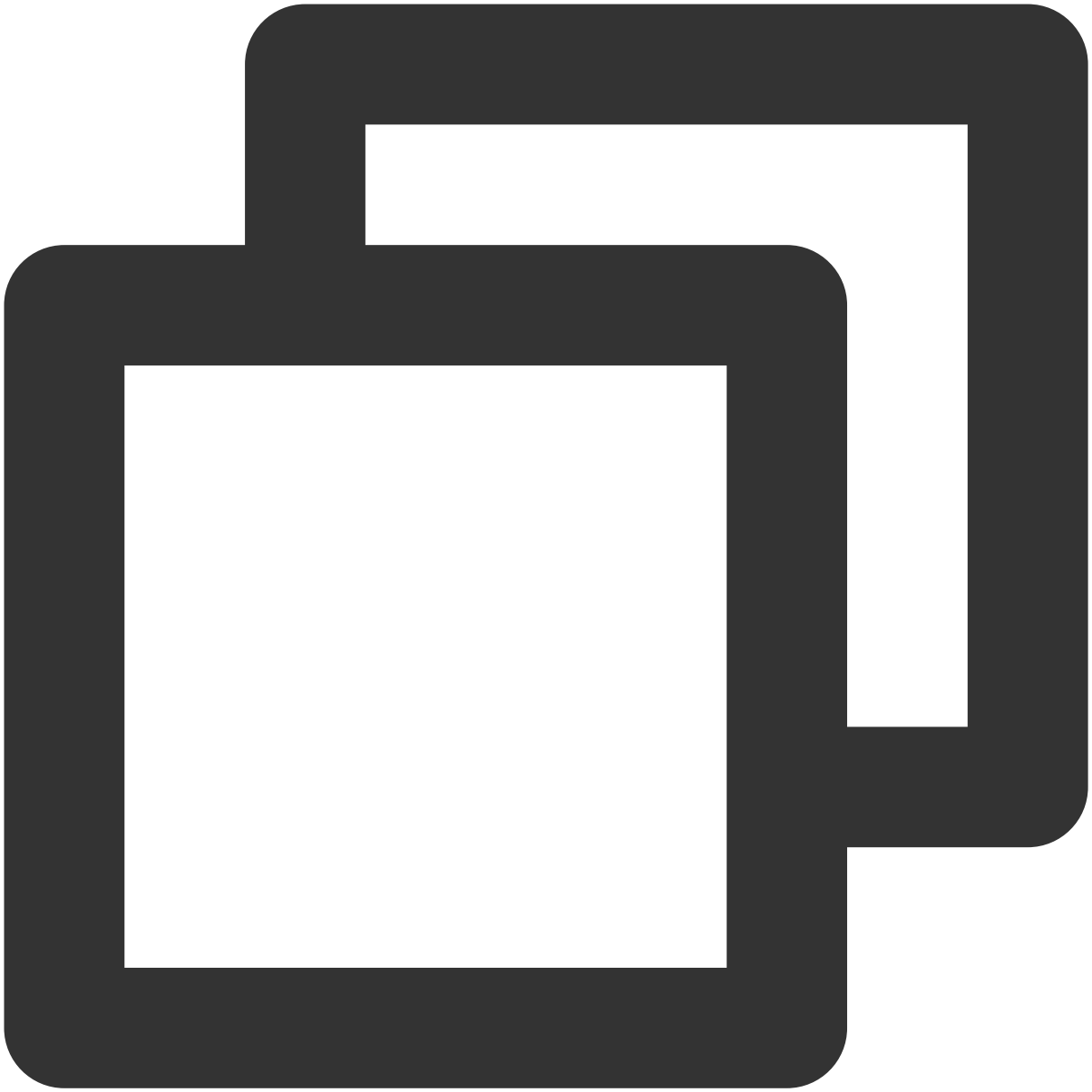
```
sudo apt-get update
sudo apt-cache search linux-image-4.4.0-98-generic
```

다음의 정보가 표시될 경우, 소스에 버전이 존재하며 업데이트를 진행할 수 있음을 나타냅니다.



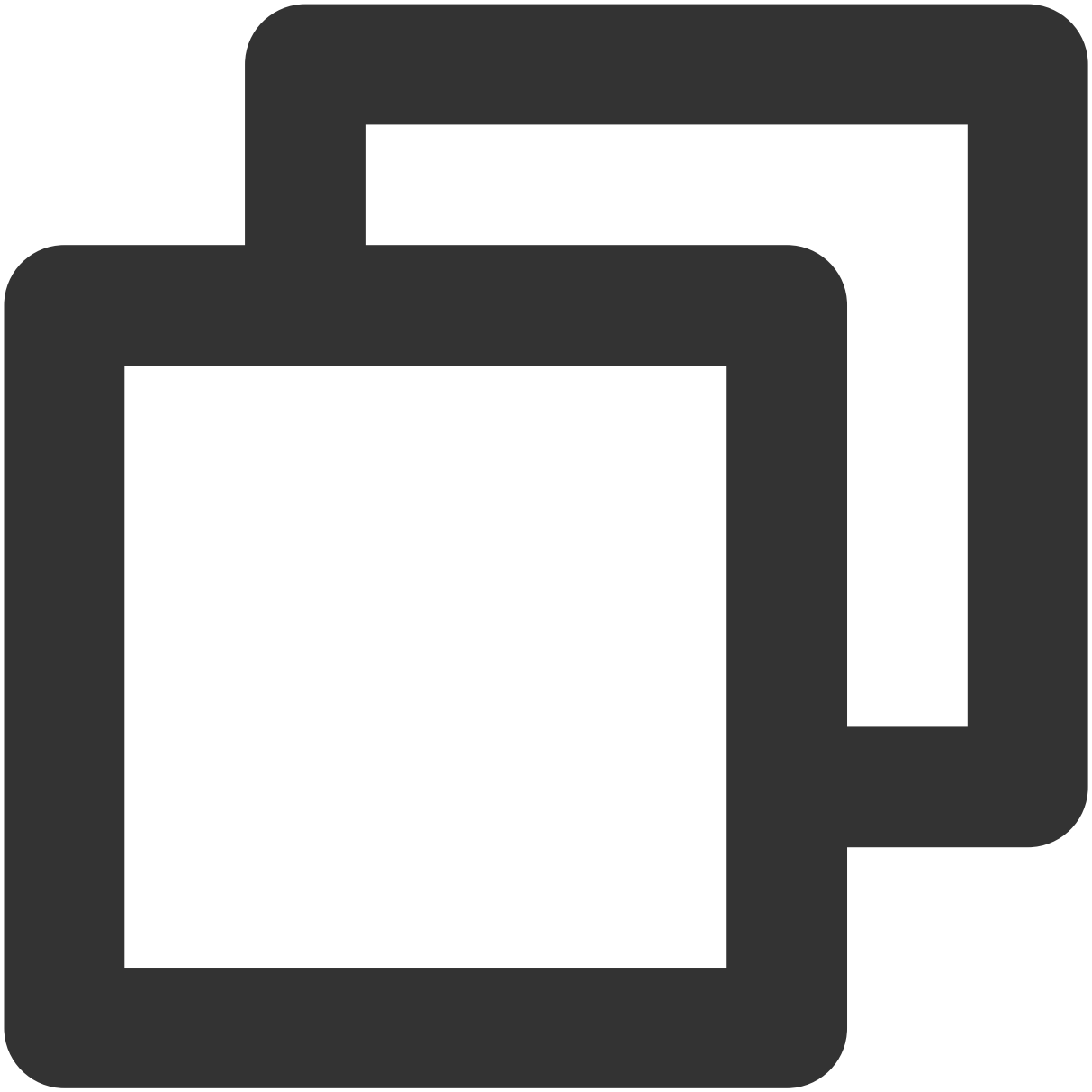
```
linux-image-4.4.0-98-generic - Linux kernel image for version 4.4.0 on 64 bit x86 S
```

3. 아래의 명령어를 실행하여 새로운 버전의 커널과 대응하는 Header 패키지를 설치하십시오.



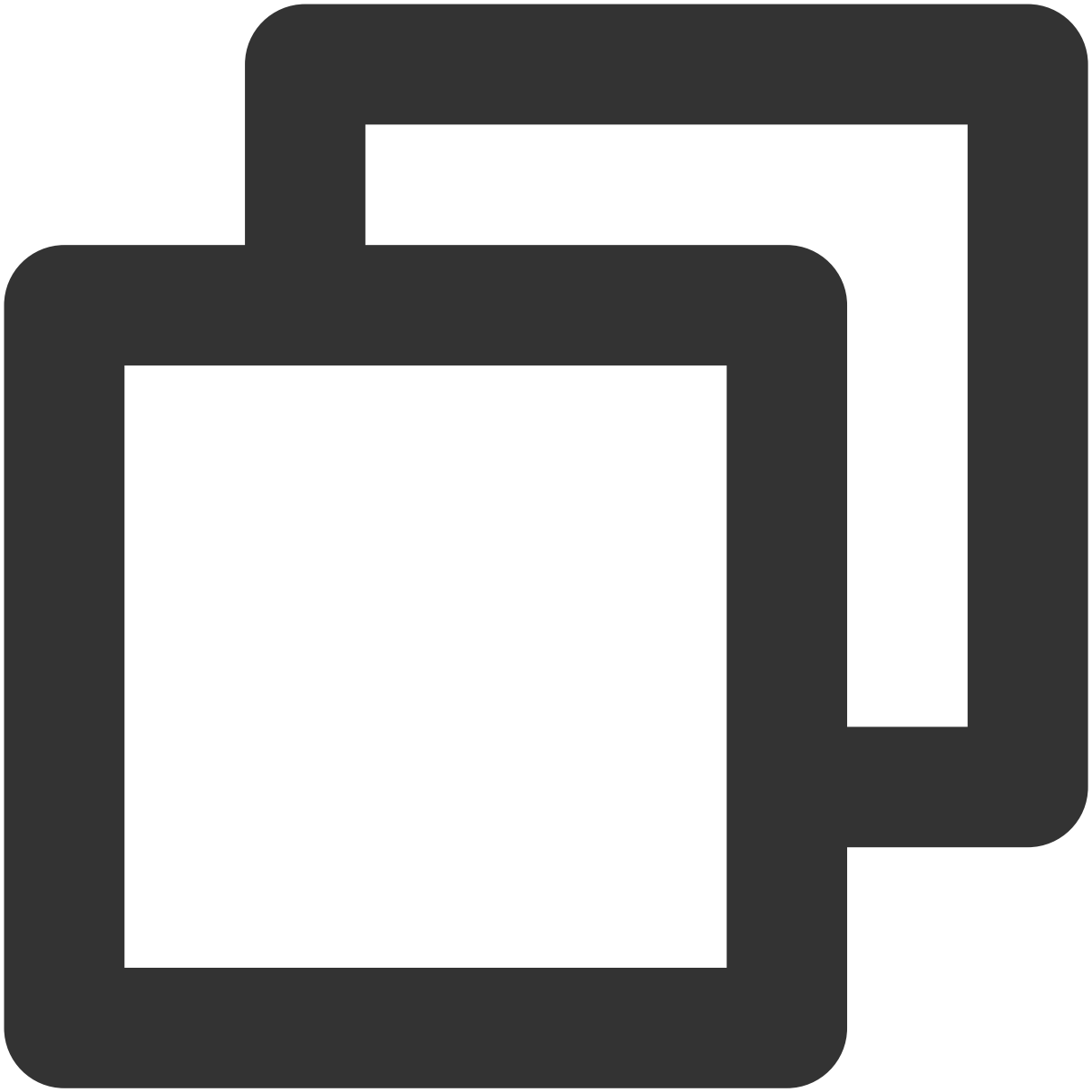
```
sudo apt-get install linux-image-4.4.0-98-generic linux-headers-4.4.0-98-generic
```

4. 아래의 명령어를 실행하여 시스템을 재시작하십시오.



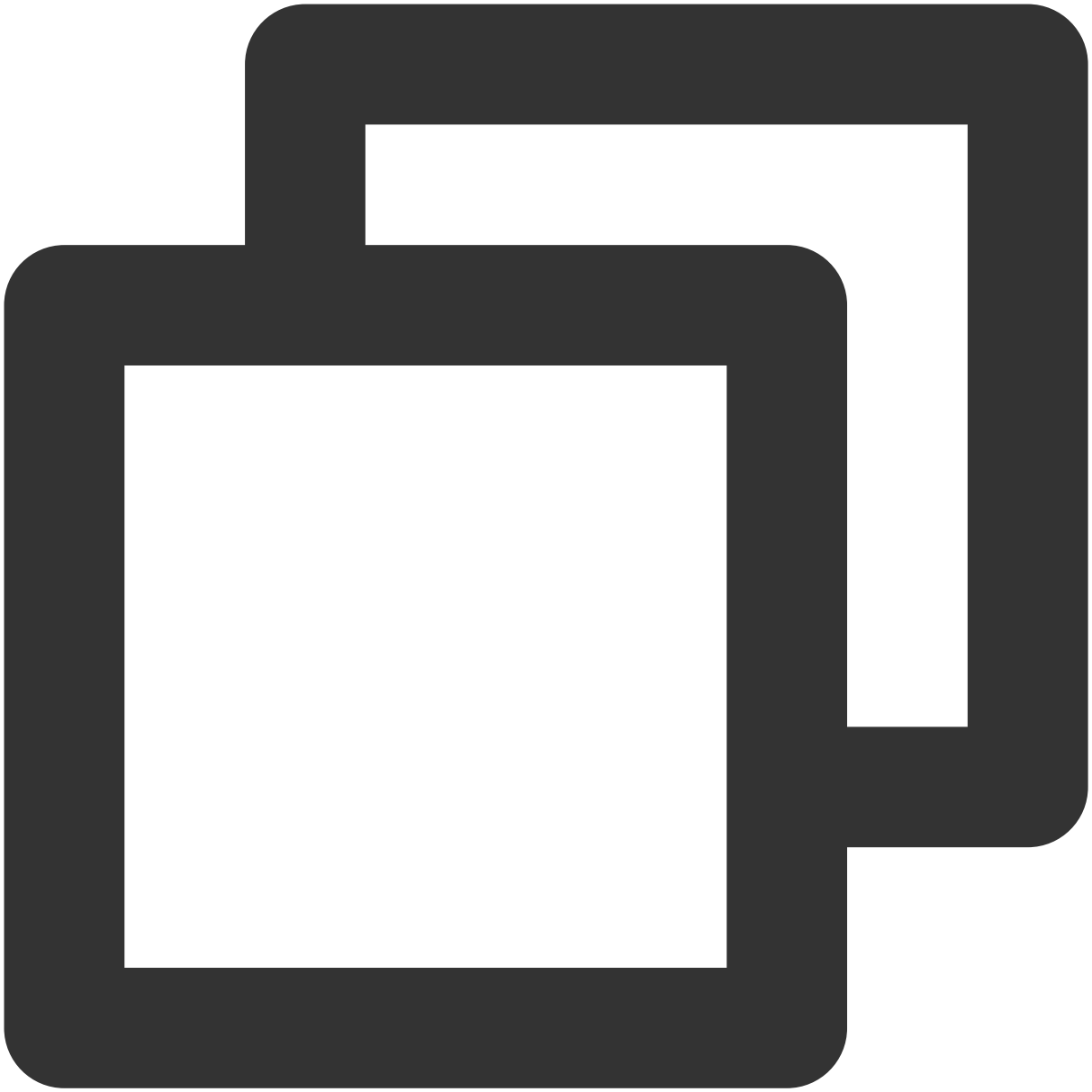
```
sudo reboot
```

5. 아래의 명령어를 실행하여 시스템에 진입한 뒤, 커널 버전을 확인하십시오.



```
uname -r
```

다음의 결과가 표시될 경우 버전 업데이트가 완료되었음을 나타냅니다.



```
4.4.0-98-generic
```

커널 및 IO 관련 문제

최종 업데이트 날짜: : 2024-02-02 11:09:47

인스턴스 자가 점검 사용 시 점검 보고서에서 인스턴스의 오류 상황을 확인할 수 있습니다. 본문에서는 인스턴스 자가 검점 보고서 중 커널 및 IO 관련 문제 현상, 원인 및 해결 절차를 소개합니다.

커널 문제 파악 및 해결

장애 현상

커널 관련 장애로 인한 시스템 로그인 실패 또는 비정상적 재부팅

예상 원인

커넬 hung_task

hung task 메커니즘은 커널 스레드 khungtaskd에 의해 구현되고 khungtaskd는 TASK_UNINTERRUPTIBLE 상태의 프로세스를 모니터링합니다. `kernel.hung_task_timeout_secs` (기본값: 120초) 시간 내에 계속 D 상태라면, hung task 프로세스 스택 정보가 출력됩니다.
`kernel.hung_task_panic=1` 을 구성하면 커널 panic이 트리거되어 기기가 재부팅됩니다.

커널 소프트 락업 soft lockup

soft lockup은 CPU가 커널 코드에 의해 점유되어 다른 프로세스를 실행할 수 없음을 의미합니다. Soft Lockup을 감지하는 원리는 각 CPU에 커널 스레드[watchdog/x] 예약 작업을 할당하고, 해당 스레드가 일정 주기(기본값: `2*kernel.watchdog_thresh` , 3.10 커널 `kernel.watchdog_thresh` , 기본값: 10초) 내에 실행되지 않을 경우 이는 soft lockup 발생을 나타냅니다.
`kernel.softlockup_panic=1` 이 구성된 경우 커널 panic이 트리거되어 기기가 재부팅됩니다.

커널 panic

비정상적인 커널 crash로 인해 기기가 비정상적으로 재부팅됩니다. 일반적인 커널 panic 시나리오는 다음과 같습니다.
커널에 Hung_task가 나타나고 `kernel.hung_task_panic=1` 이 구성됨.
커널에 소프트 락업 soft lockup이 나타나고 `kernel.softlockup_panic=1` 이 구성됨.
커널 bug를 트리거함.

해결 절차

커널 관련 문제 진단 및 해결 절차는 복잡하므로 티켓 제출을 권장합니다.
) 추가 포지셔닝 및 처리.

하드디스크 문제 파악 및 해결

하드디스크 inode 용량 없음

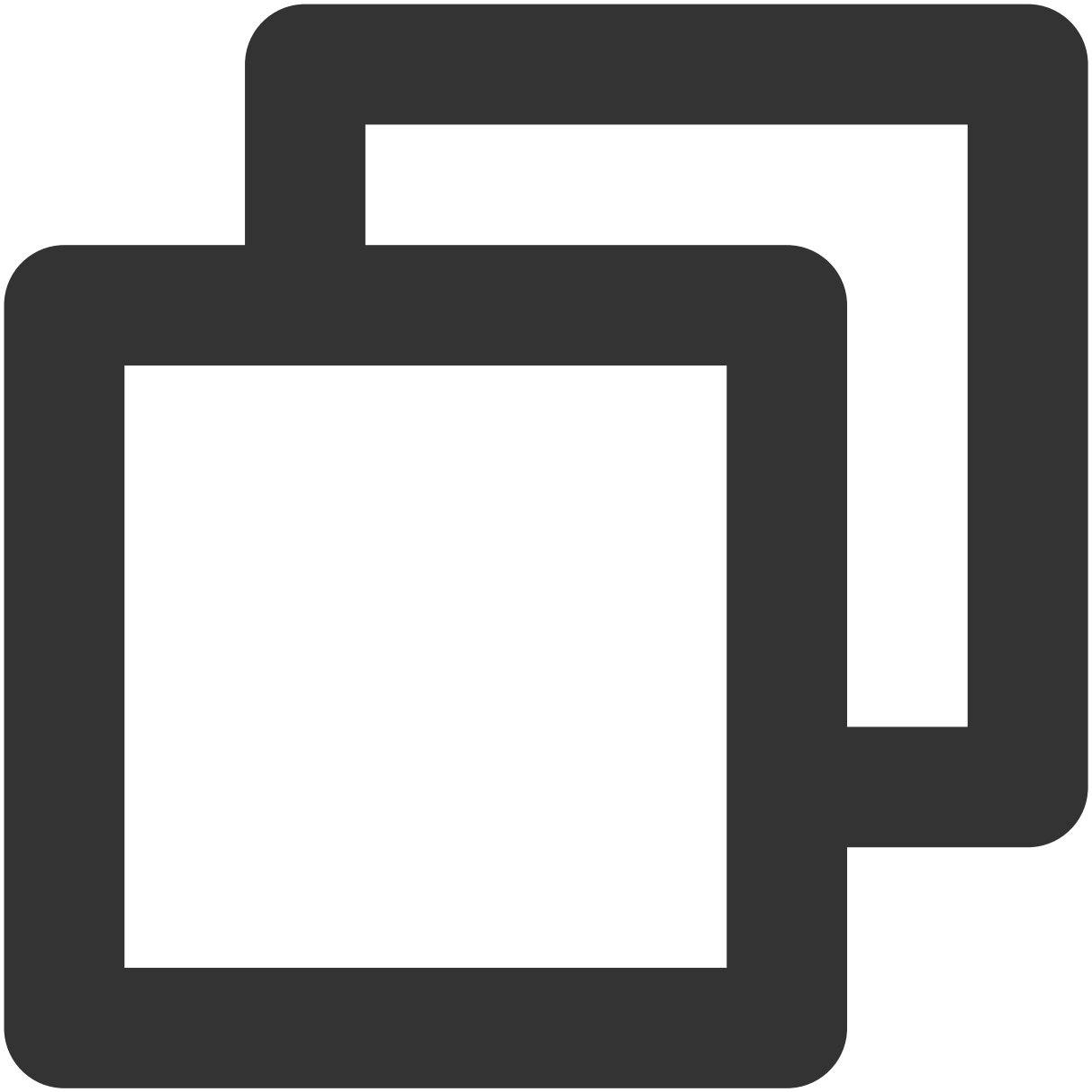
장애 현상: 새 파일을 만들 때 "No space left on device."라는 오류 메시지가 표시되고 `df -i` 명령을 통해 확인한 inode 공간 사용률이 100%임.
가능한 원인: 파일 시스템 inode 소진.
해결 방법: 불필요한 파일 삭제 또는 하드디스크 확장.

하드디스크 용량 없음

장애 현상: 새 파일을 만들 때 "No space left on device."라는 오류 메시지가 표시되고 `df -h` 명령을 통해 확인한 하드디스크 공간 사용률이 100%임.
가능한 원인: 하드디스크 용량 소진.
해결 방법: 불필요한 파일 삭제 또는 하드디스크 확장.

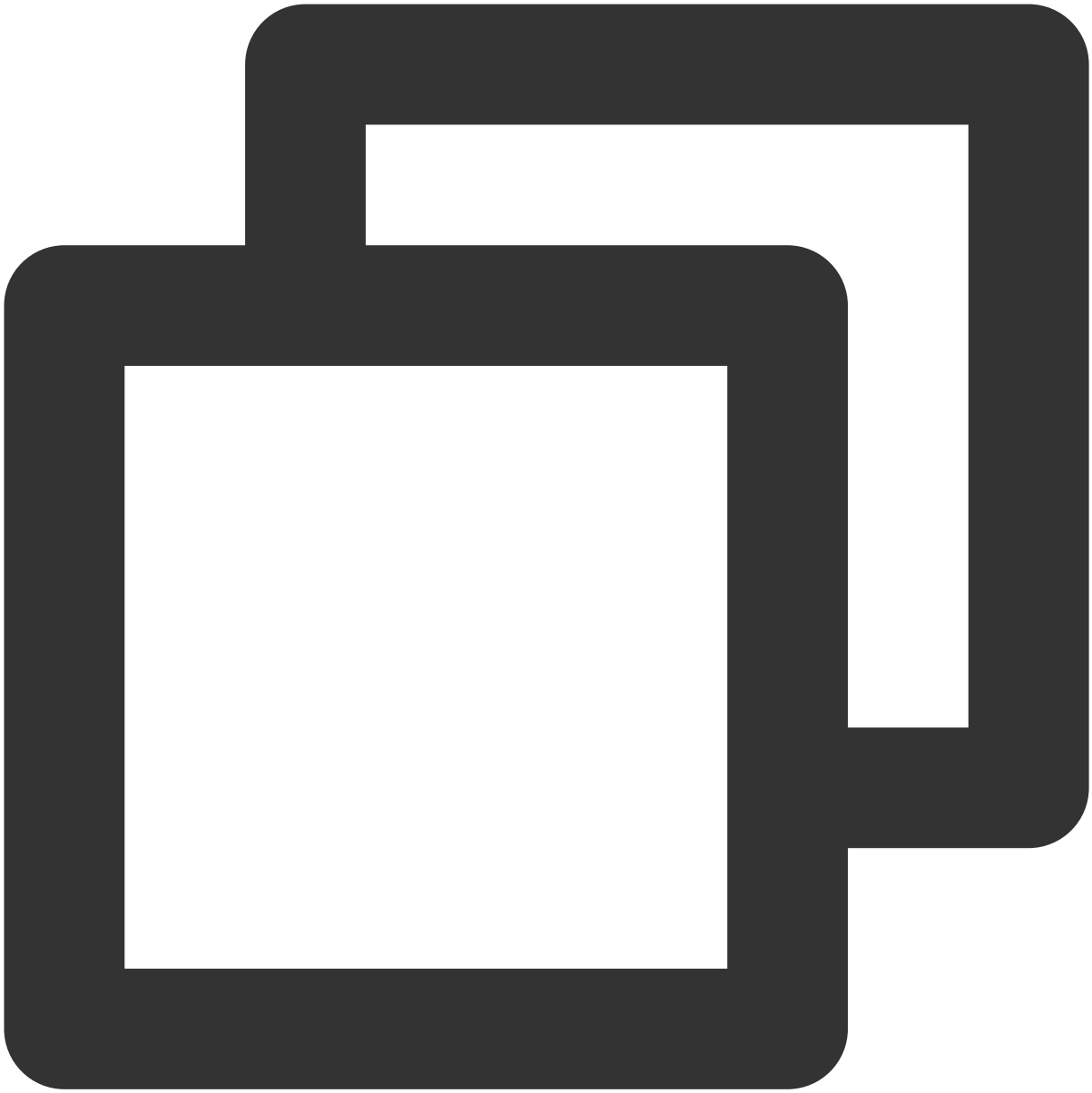
읽기 전용 하드디스크

장애 현상: 파일 읽기만 가능한 파일 시스템. 신규 파일 생성 불가.
가능한 원인: 파일 시스템 손상.
해결 절차:
1. 스냅샷 생성을 통한 하드디스크 데이터 백업. 자세한 내용은 스냅샷 생성을 참고하십시오.
2. 하드디스크 유형에 따른 해결 방법을 실행합니다.
시스템 디스크
데이터 디스크
인스턴스 재부팅을 권장합니다. 자세한 내용은 인스턴스 재부팅을 참고하십시오.
1. 다음 명령어를 실행하여 읽기 전용 디스크 파일 시스템 유형을 확인합니다.



```
lsblk -f
```

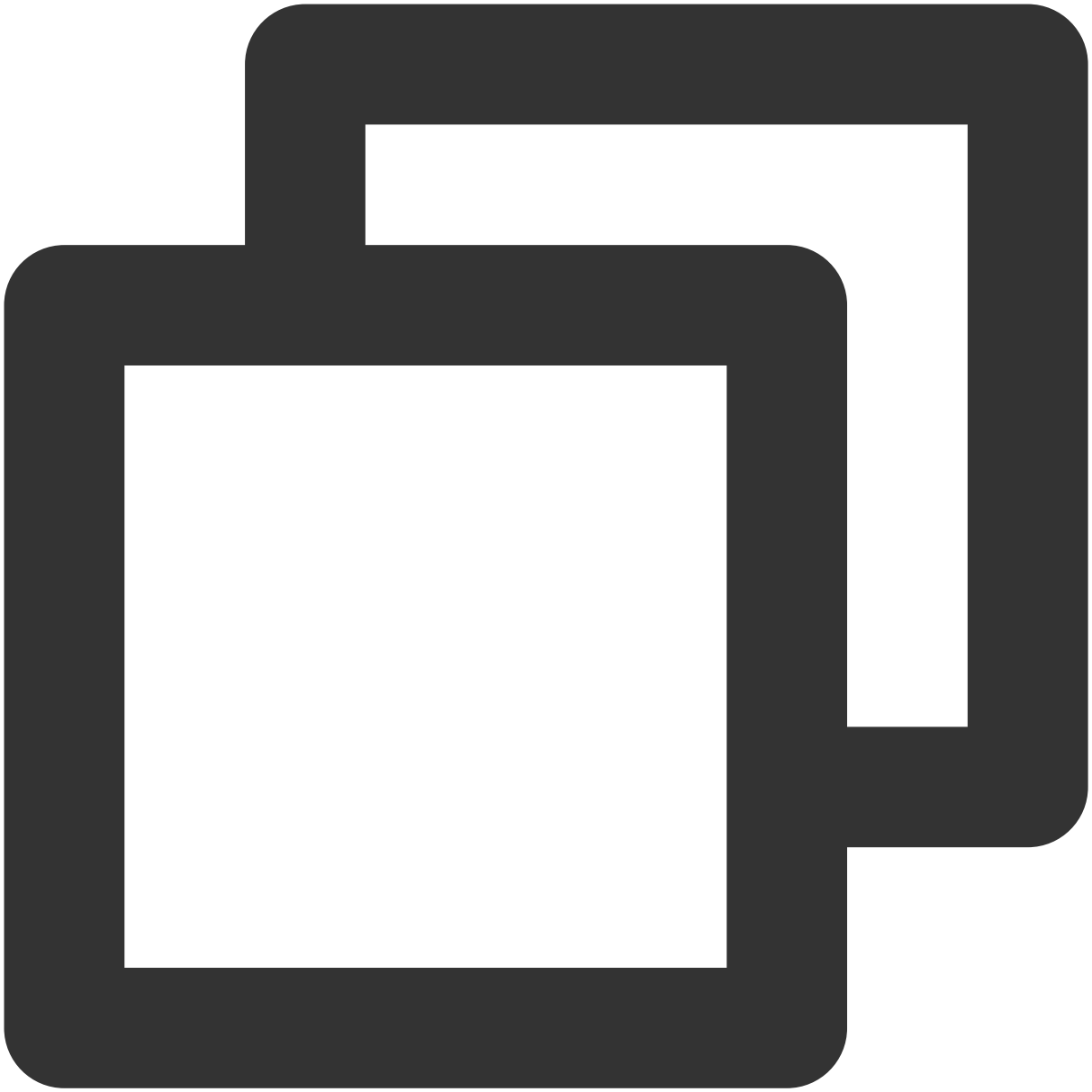
2. 다음 명령어를 실행하여 데이터 디스크를 언마운트합니다.



```
umount <디스크 언마운트 경로>
```

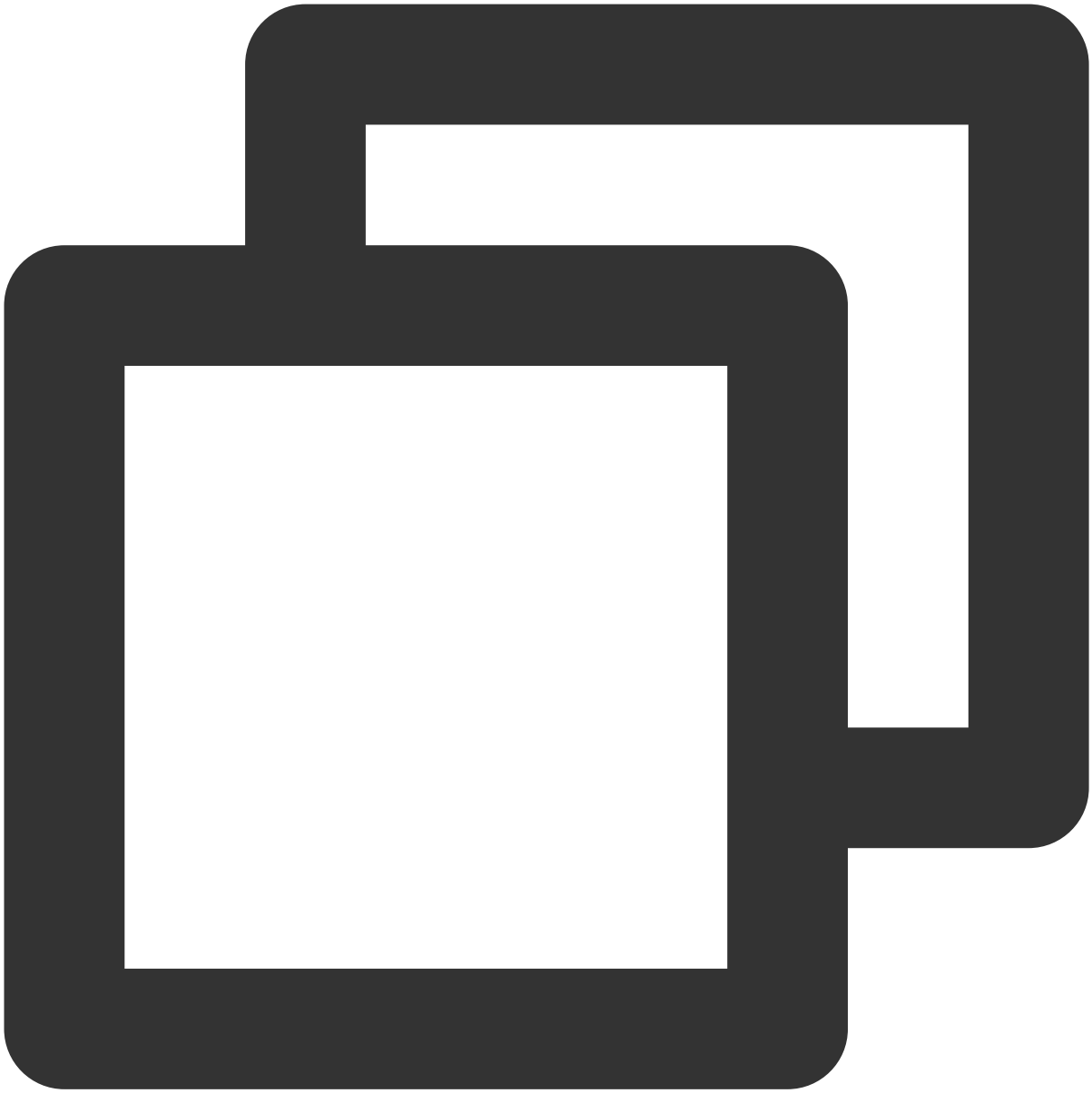
3. 파일 시스템 유형에 따라 다음 명령어를 실행하여 복구합니다.

-**ext3**/**ext4** 파일 시스템에서 다음 명령어 실행.



```
fsck -y /dev/해당 디스크
```

-**xfs** 파일 시스템에서 다음 명령어 실행.



```
xfs_repair /dev/해당 디스크
```

하드디스크 %util 높음

장애 현상: 인스턴스 랙 발생. SSH 또는 VNC 로그인이 느리거나 응답 없음.

가능한 원인: 높은 IO로 인해 하드디스크 %util이 100%에 도달.

해결 방법: IO가 적절한지 확인하고 IO 읽기 및 쓰기 축소 또는 고성능 하드디스크로의 교체 고려.

시스템 bin 또는 lib 소프트 링크 누락

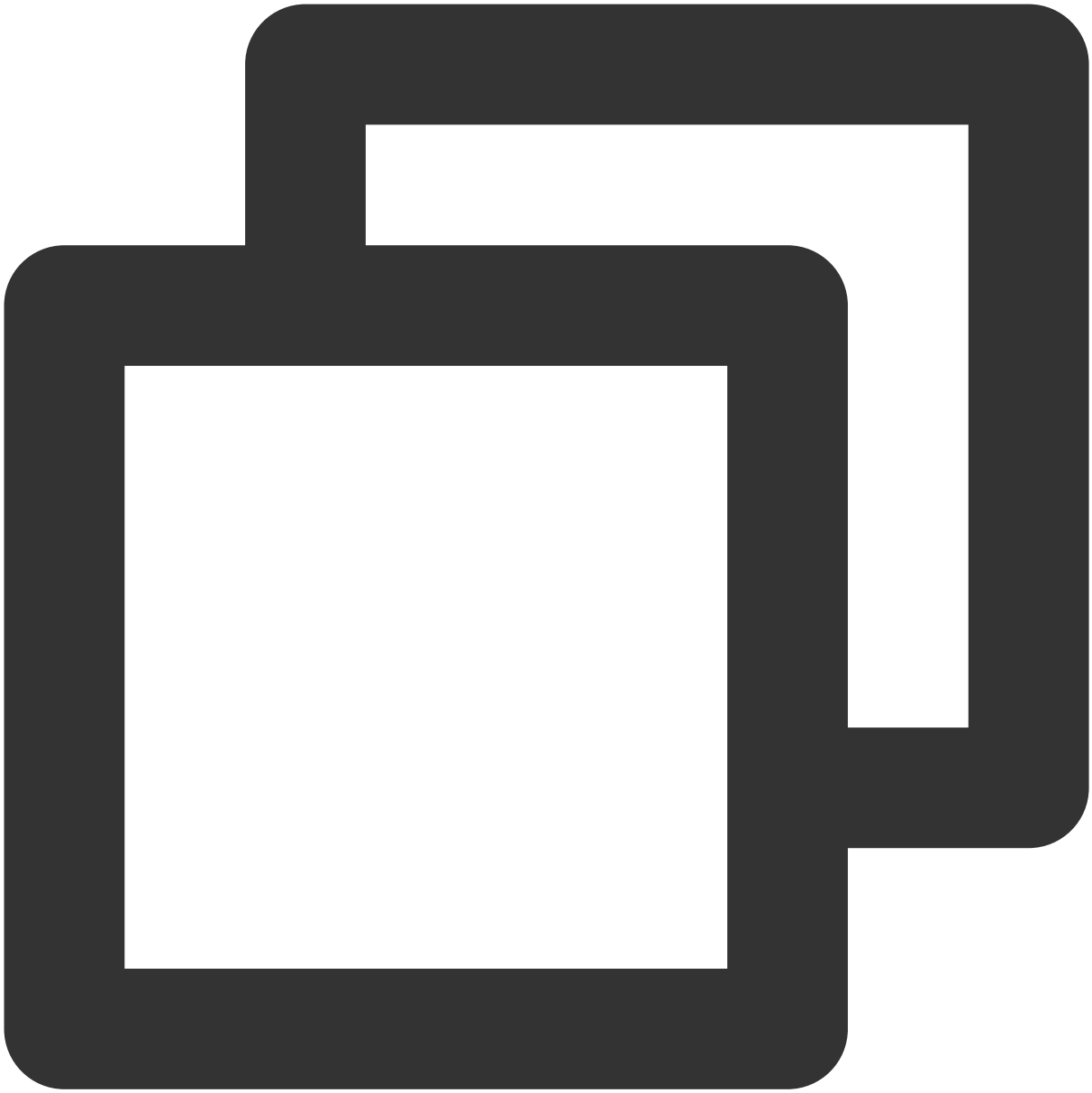
최종 업데이트 날짜: : 2024-02-02 11:09:47

현상 설명

명령 실행 또는 시스템 시작 과정 중 명령 찾을 수 없음 또는 lib 라이브러리 찾을 수 없음 등의 오류 메시지가 표시됩니다.

예상 원인

CentOS 7, CentOS 8, Ubuntu 20 등 시스템의 bin, sbin, lib 및 lib64는 소프트 링크입니다:



```
lrwxrwxrwx   1 root root     7 Jun 19  2018 bin -> usr/bin
lrwxrwxrwx   1 root root     7 Jun 19  2018 lib -> usr/lib
lrwxrwxrwx   1 root root     9 Jun 19  2018 lib64 -> usr/lib64
lrwxrwxrwx   1 root root     8 Jun 19  2018 sbin -> usr/sbin
```

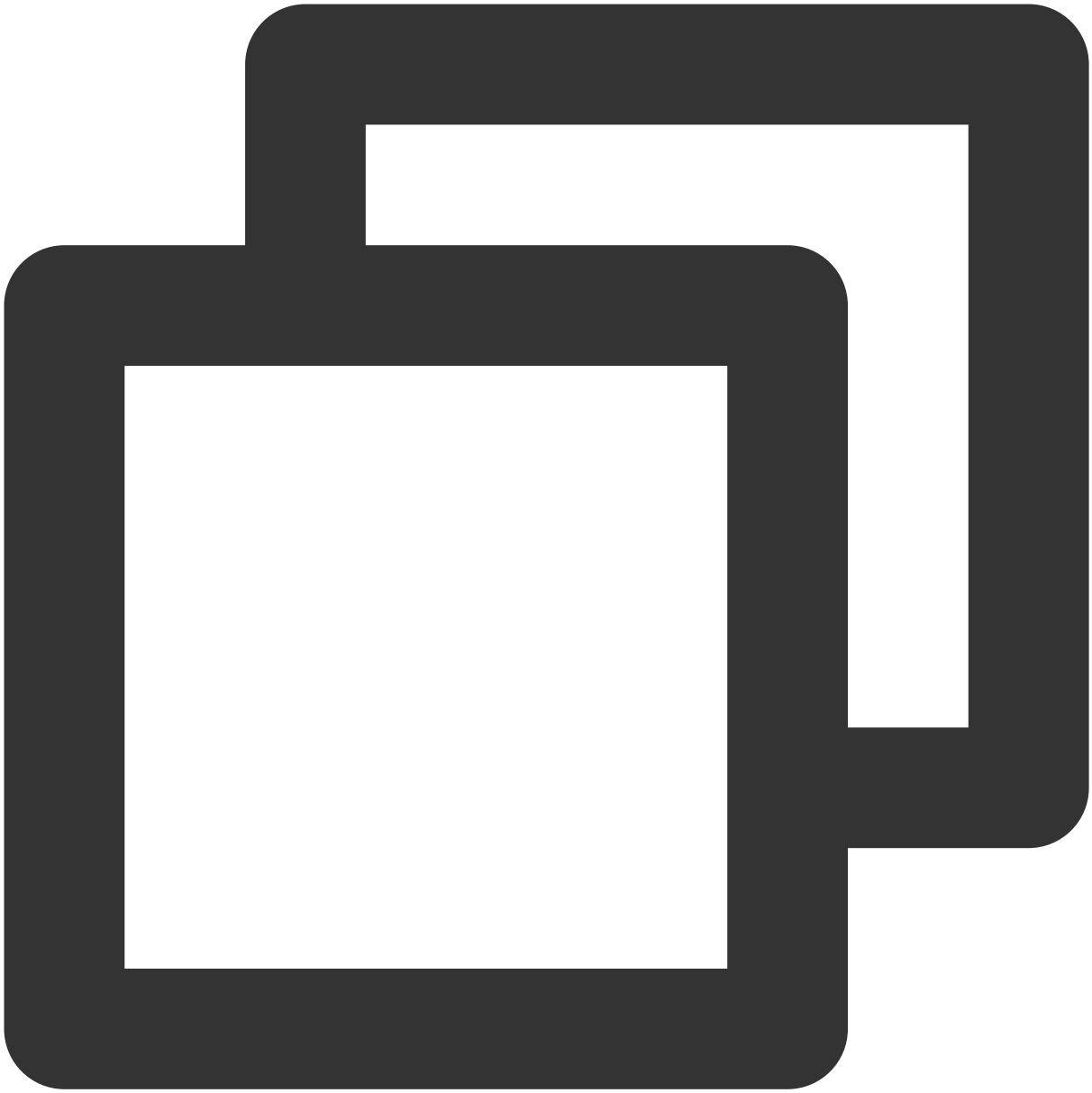
소프트 링크가 삭제되면 명령 실행 또는 시스템 실행 중에 오류가 보고됩니다.

해결 방법

처리 단계를 참고하여 필요한 소프트 링크 확인 및 생성합니다.

처리 단계

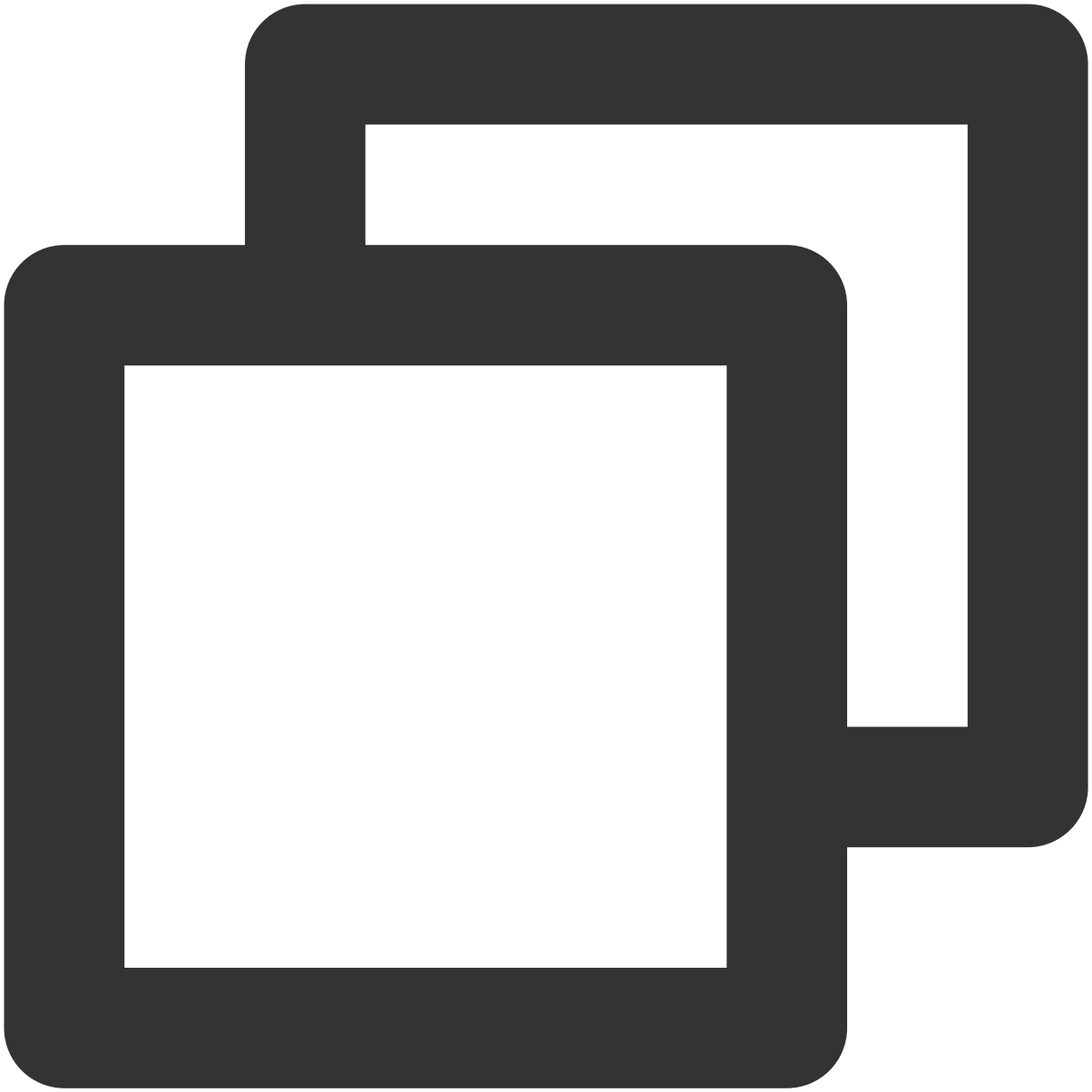
1. 복구 모드를 시작합니다.
2. 'mount' 및 'chroot' 등의 명령을 실행합니다. 그 중 `chroot` 명령 실행 시:
오류 발생 시, `cd /mnt/vm1` 을 실행합니다.
오류 미발생 시, `cd /` 를 실행합니다.
3. 다음 명령을 실행하여 해당 소프트 링크가 존재하는지 확인합니다.



```
ls -al / | grep -E "lib|bin"
```

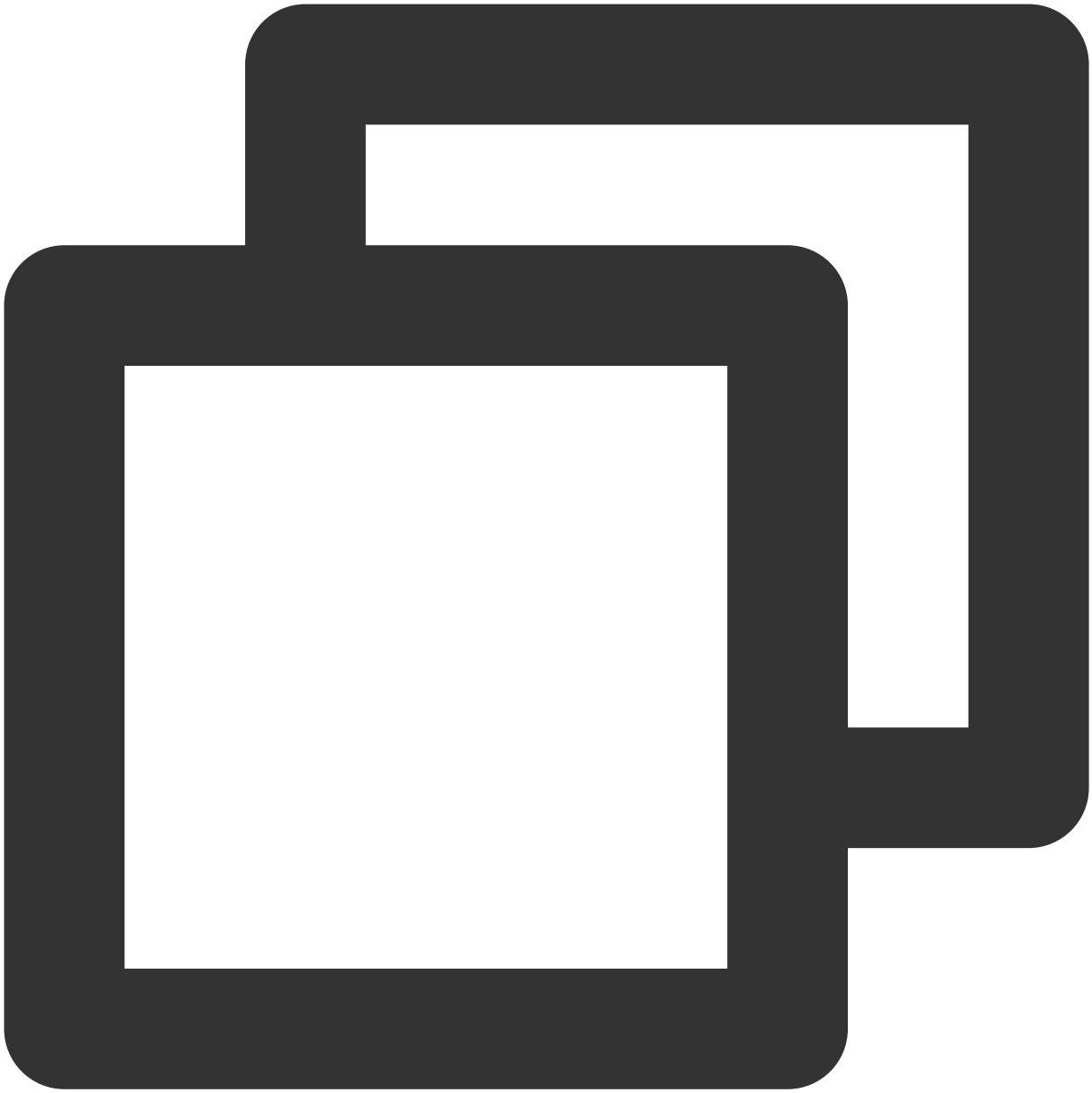
존재하는 경우, 티켓 제출을 통해 고객센터에 도움을 요청하십시오.

존재하지 않는 경우, 필요에 따라 다음 명령을 실행하여 해당 소프트 링크를 생성합니다.



```
ln -s usr/lib64 lib64
ln -s usr/sbin sbin
ln -s usr/bin bin
ln -s usr/lib lib
```

4. 다음 명령을 실행하여 소프트 링크를 확인합니다.



```
chroot /mnt/vm1 /bin/bash
```

오류 메시지가 보고되지 않으면 소프트 링크가 성공적으로 복구된 것입니다.

5. 복구 모드를 종료하고 시스템을 실행합니다.

CVM 바이러스 침입 의심

최종 업데이트 날짜: : 2024-02-02 11:09:48

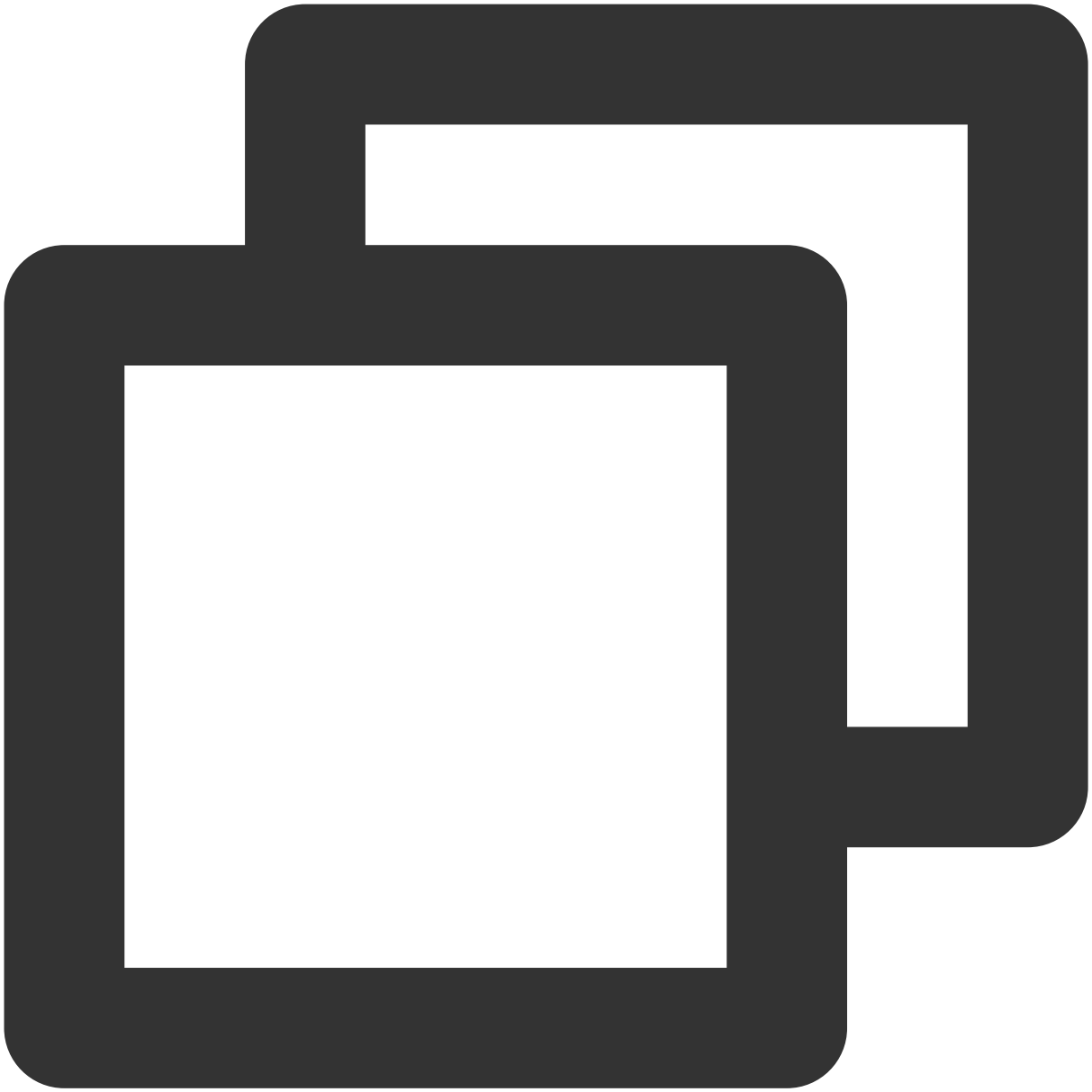
CVM은 취약한 비밀번호와 오픈소스 모듈 취약점으로 인해 해커의 침입을 받을 수 있습니다. 본문은 CVM이 바이러스의 침입을 받았는지 판단 방법과 해결 방법에 대해 설명합니다.

문제 파악

SSH 방식 또는 VNC 방식으로 인스턴스에 로그인한 후 다음 방법을 사용하여 CVM이 바이러스에 감염되었는지 확인합니다.

rc.local에 악성 명령 추가됨

다음 명령을 실행하여 `rc.local` 파일을 확인합니다.

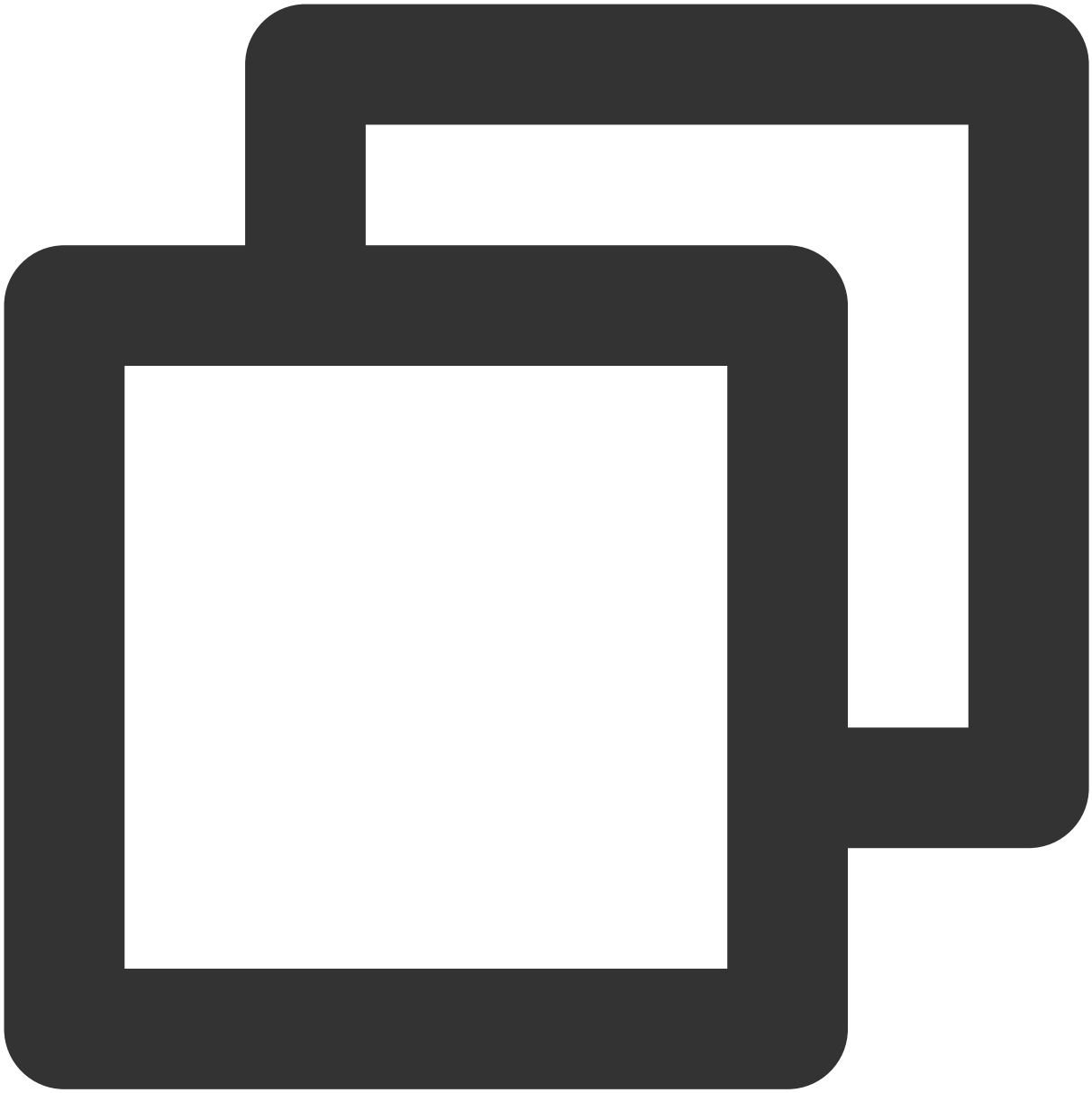


```
cat /etc/rc.local
```

출력 정보가 'wget xx' 및 '/tmp/xx' 등 업무 또는 공지 이미지에 추가된 명령어가 아닌 경우, CVM은 바이러스의 침입을 받았을 가능성이 높습니다.

crontab에 악성 작업 추가됨

다음 명령을 실행하여 현재 일정을 나열합니다.

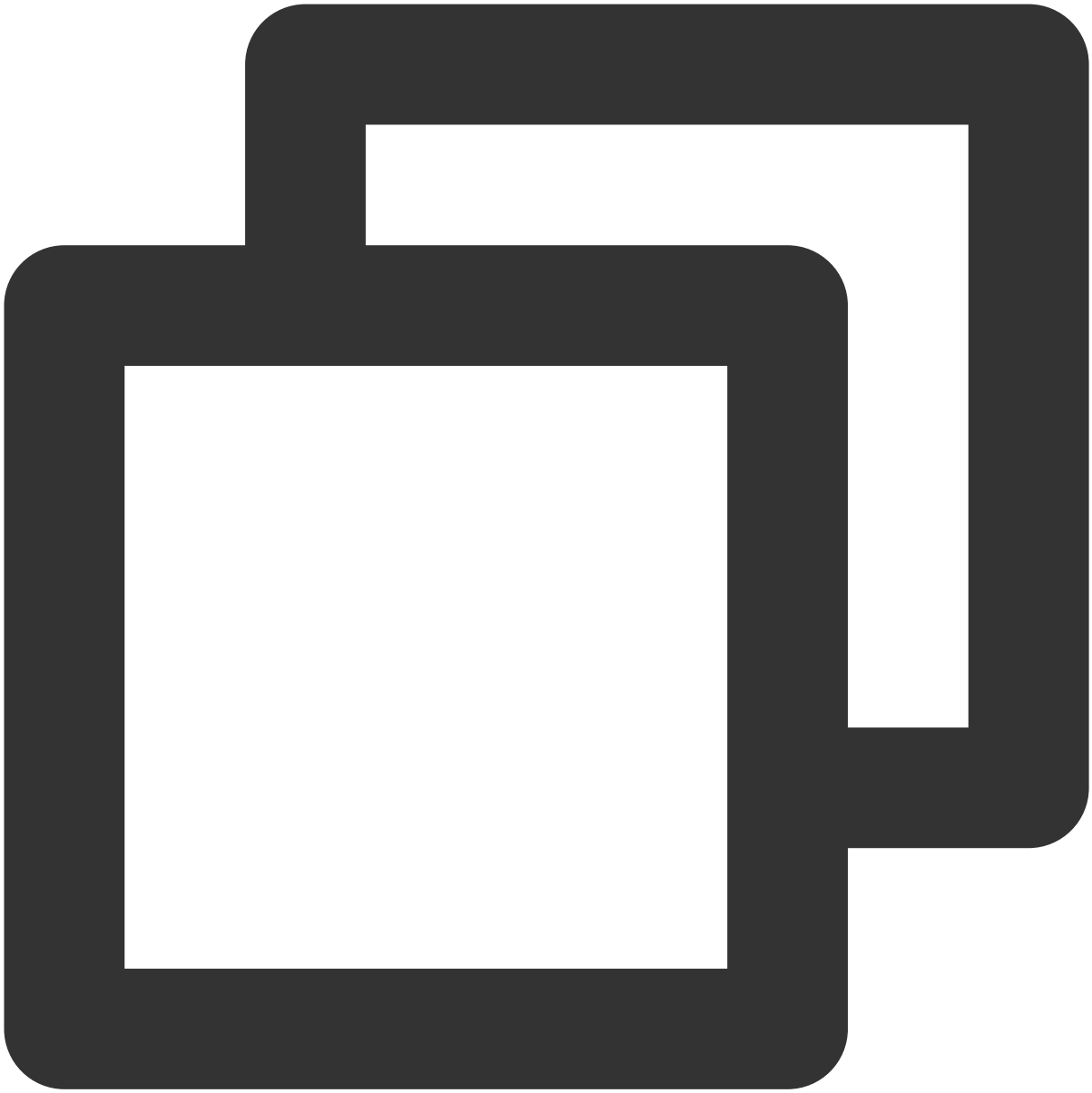


```
crontab -l
```

출력 정보가 'wget xx' 및 '/tmp/xx' 등 업무 또는 공지 이미지에 추가된 명령어가 아닌 경우, CVM은 바이러스의 침입을 받았을 가능성이 높습니다.

ld.so.preload 동적 라이브러리 하이재킹 추가

다음 명령을 실행하여 `/etc/ld.so.preload` 파일을 확인합니다.

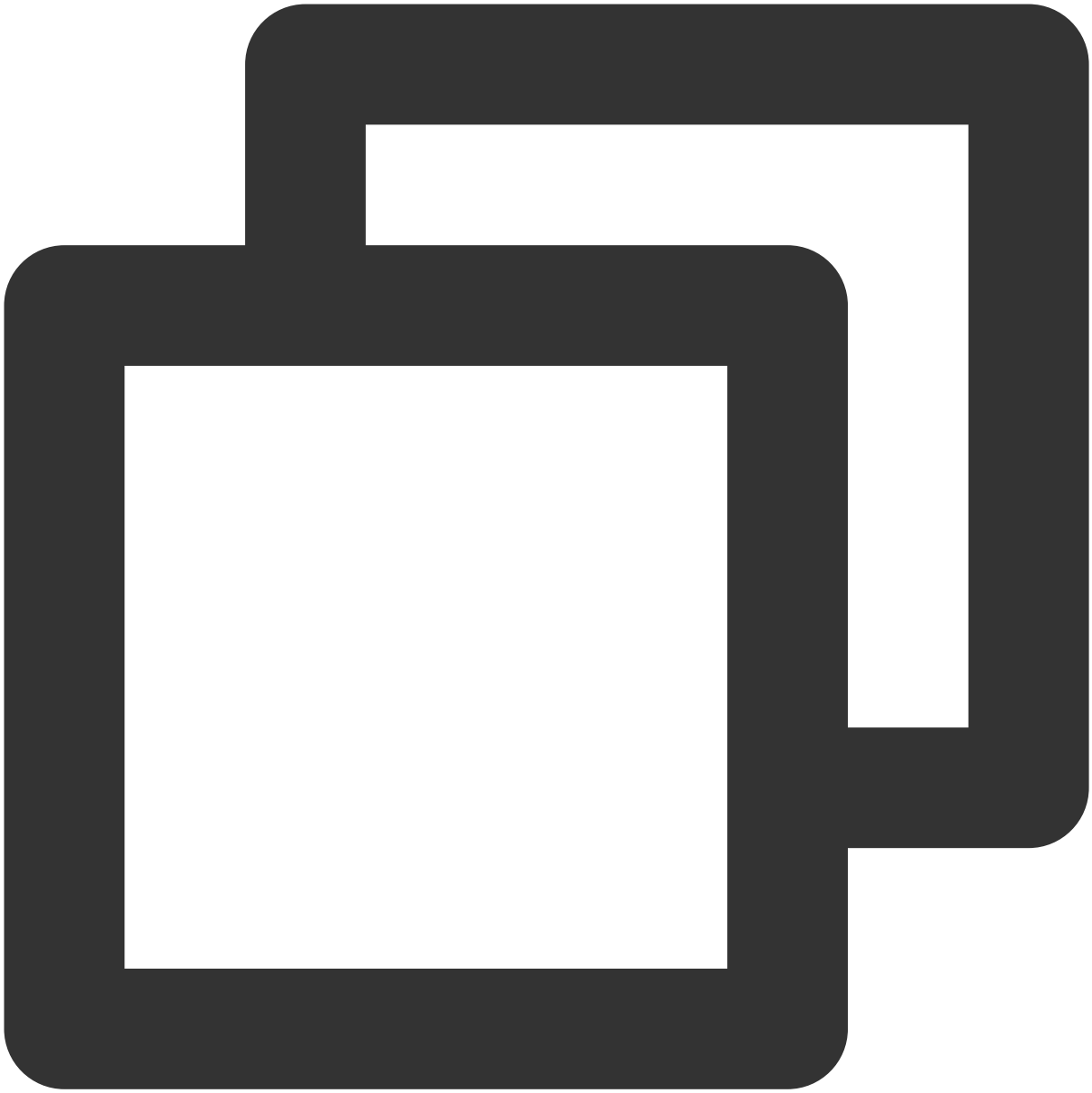


```
cat /etc/ld.so.preload
```

출력 정보가 업무 외 추가된 동적 라이브러리인 경우, CVM은 바이러스의 침입을 받았을 가능성이 높습니다.

sysctl.conf 대용량 페이지 메모리 설정

다음 명령어를 실행하여 대용량 페이지의 메모리 사용량을 확인합니다.



```
sysctl -a | grep "nr_hugepages "
```

출력이 0이 아니고 비즈니스 자체 프로그램이 대용량 페이지 메모리를 사용하지 않는다면 CVM은 바이러스의 침입을 받았을 가능성이 높습니다.

해결 단계

1. 스냅샷 생성을 참고하여 시스템 데이터 백업을 완료하십시오.

2. 시스템 재설치를 참고하여 인스턴스 시스템을 재설치하고, 보안 정책을 강화하기 위해 다음과 같은 조치를 취합니다.
CVM 비밀번호를 수정합니다. 비밀번호는 대문자, 소문자, 특수 부호, 숫자로 구성된 12-16자리의 복잡하고 임의적인 비밀번호로 설정하십시오. 자세한 내용은 인스턴스 비밀번호 재설정을 참조하십시오.
CVM에서 사용하지 않는 사용자를 삭제합니다.
sshd의 기본 포트 22를 1024-65525 사이의 자주 사용하지 않는 포트로 변경합니다. 자세한 방식은 CVM 원격 기본 포트 수정을 참조하십시오.
CVM과 연결된 보안 그룹의 규칙을 관리하기 위해서는 서비스와 프로토콜에 필요한 포트만 개방하면 되며, 모든 프로토콜과 포트를 개방하는 것은 권장하지 않습니다. 자세한 내용은 보안 그룹 규칙 추가를 참조하십시오.
공용 네트워크에 핵심 애플리케이션 서비스 포트의 액세스를 개방하는 것은 권장하지 않습니다. 예시: mysql, redis 등 관련 포트를 로컬 액세스 또는 공인 네트워크 액세스 금지로 변경할 수 있습니다.
HS, yunsuo 등 보안 소프트웨어를 설치하고 실시간 알람을 추가하여 비정상적인 로그인 정보를 즉각적으로 수집할 수 있습니다.

파일 생성 no space left on device 오류

최종 업데이트 날짜: : 2024-02-02 11:09:48

현상 설명

Linux CVM에서 새 파일을 생성할 때 'no space left on device'라는 오류가 나타납니다.

예상 원인

디스크 공간이 가득 참
파일 시스템 `inode` 가 가득 참
df du 불일치
파일이 삭제되었지만 해당 파일 핸들을 보유하고 있는 프로세스가 여전히 있어 하드 디스크 공간이 릴리스되지 않았습니다.
mount 마운트가 중첩됩니다. 예를 들어, 시스템 디스크의 `/data` 디렉터리가 많은 공간을 차지하고, 또한 `/data` 가 다른 데이터 디스크에 마운트하기 위한 마운트 포인트로 사용되어, 시스템 디스크에 df du 불일치가 발생합니다.

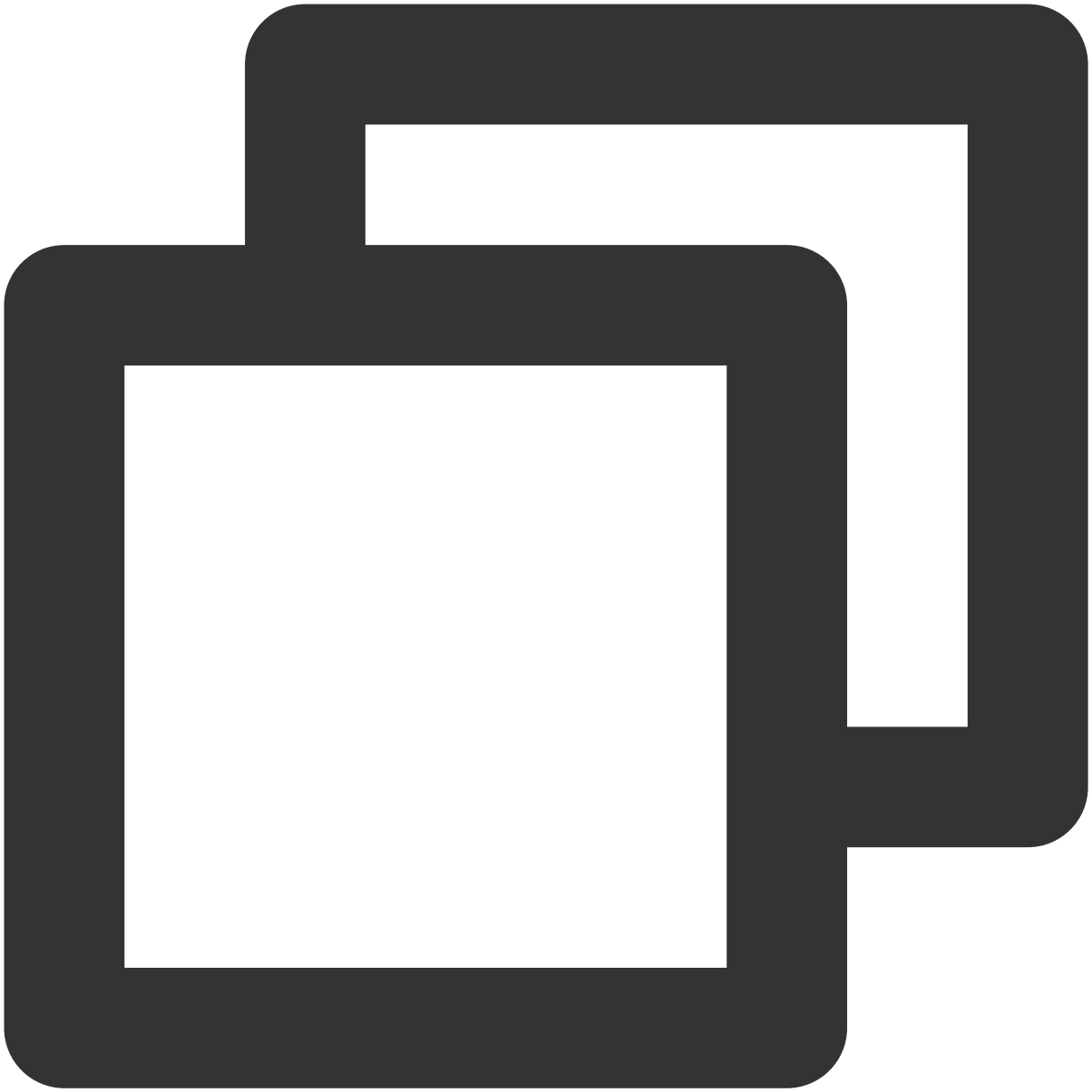
해결 방법

처리 방법을 참고하여 문제를 진단하고 해결합니다.

처리 방법

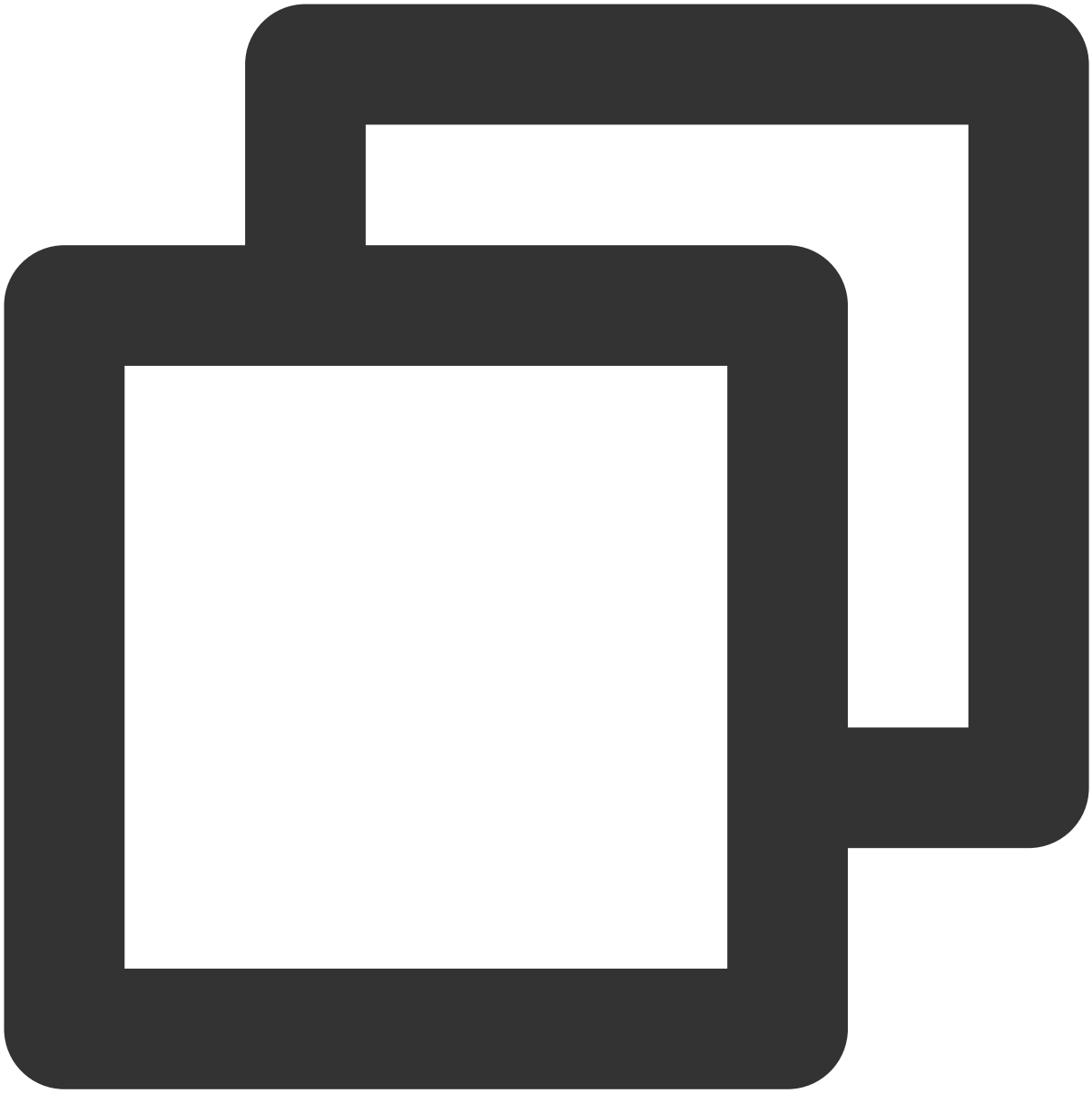
가득 찬 하드 디스크 공간 문제 해결

1. CVM에 로그인합니다. 자세한 내용은 표준 로그인 방식으로 Linux 인스턴스에 로그인을 참고하십시오.
2. 다음 명령어를 실행하여 디스크 사용량을 확인합니다.



```
df -h
```

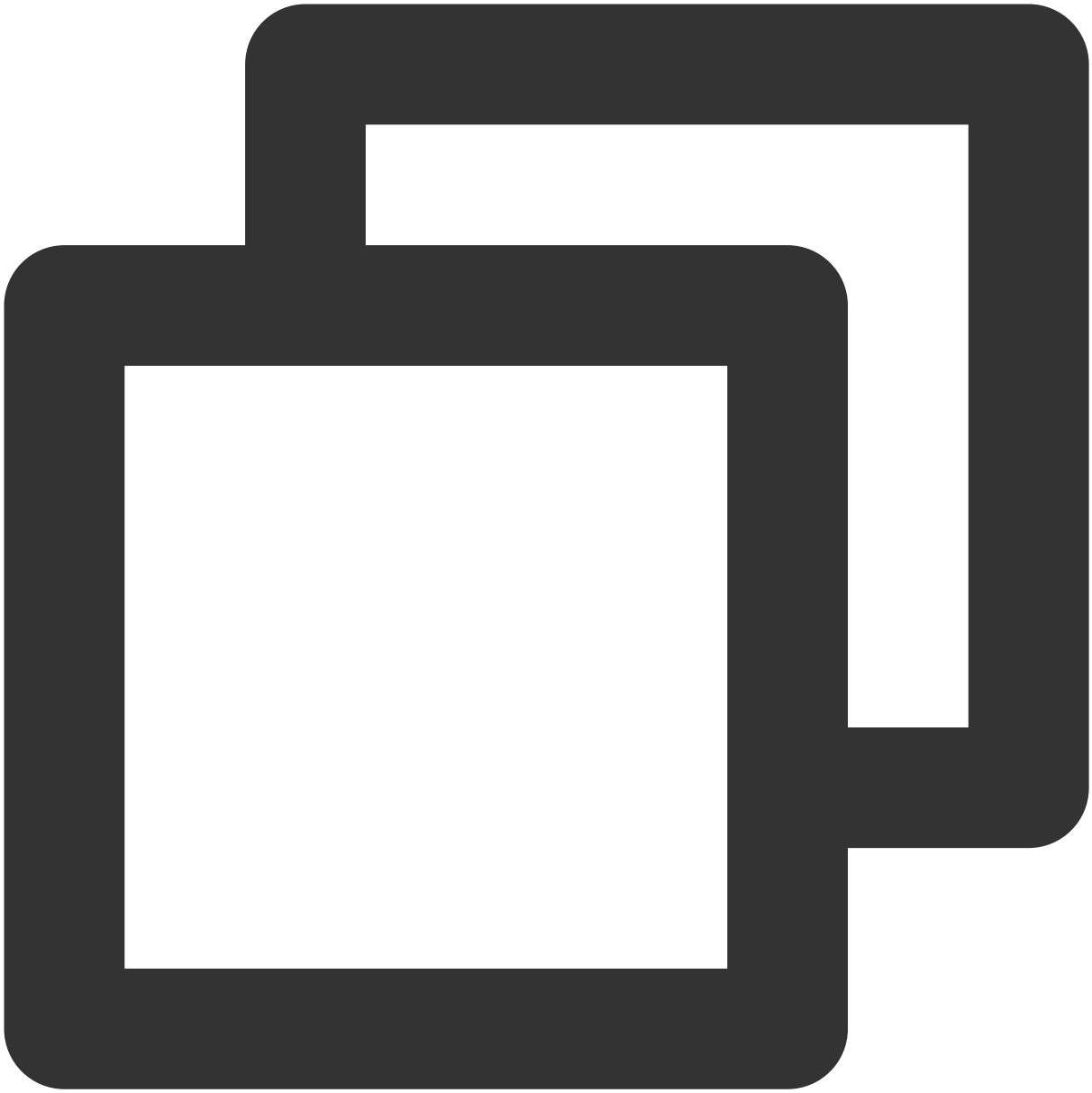
3. 디스크 사용량이 많은 마운트 포인트를 찾고 다음 명령을 실행하여 마운트 포인트로 이동합니다.



```
cd는 마운트 포인트에 해당
```

예를 들어, cd 시스템 디스크 마운트 포인트가 필요한 경우 `cd /` 를 실행합니다.

4. 다음 명령어를 실행하여 많은 공간을 차지하는 디렉터리를 찾습니다.



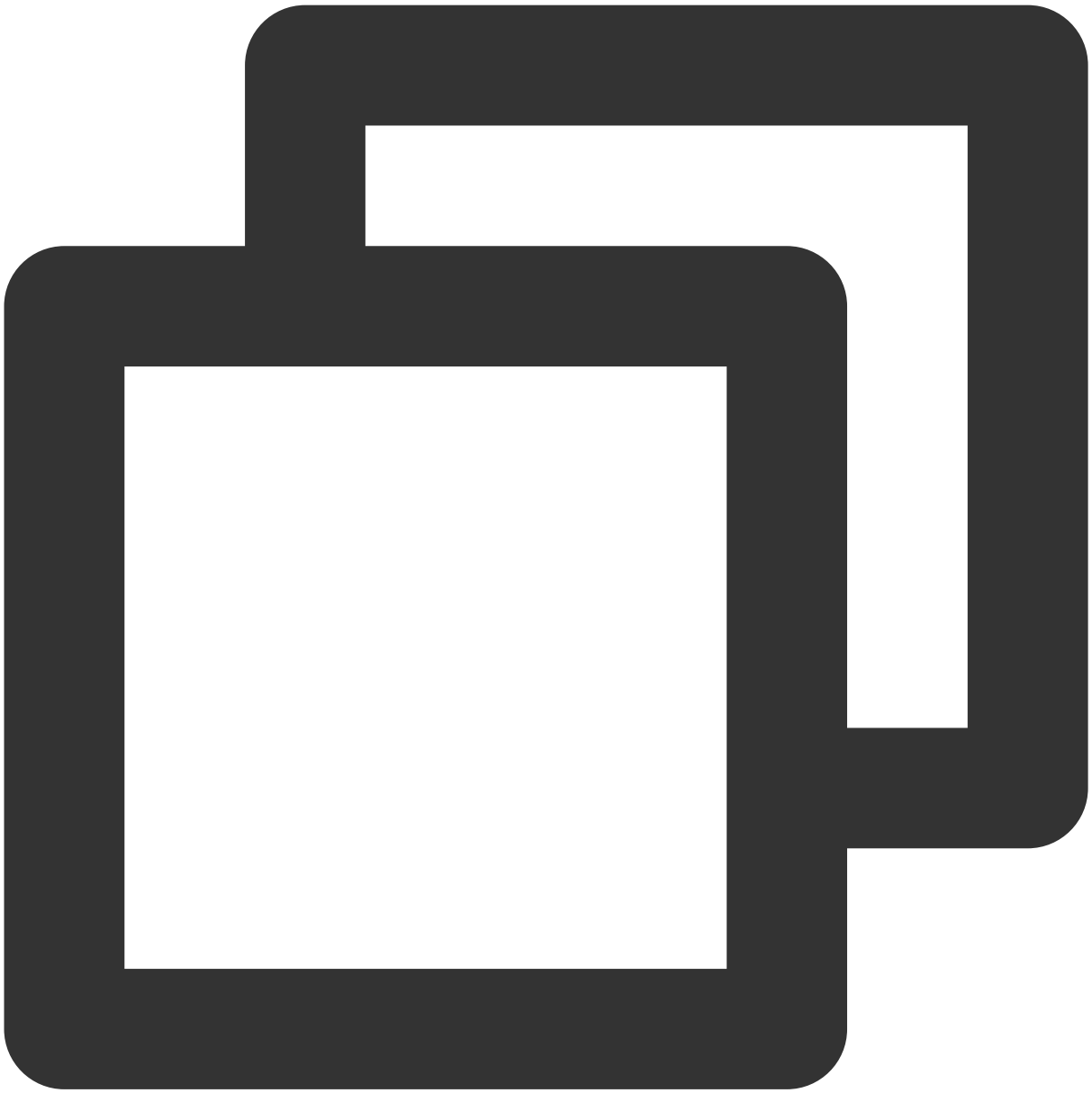
```
du -x --max-depth=1 | sort -n
```

가장 많은 공간을 차지하는 디렉터리를 찾고 용량에 따라 다음 단계를 수행합니다.
디렉터리 용량이 전체 디스크 공간보다 훨씬 작은 경우 df du 불일치 해결 단계를 참고하십시오.
디렉터리 용량이 큰 경우 [2단계](#Step 2)를 실행하여 대용량 파일을 찾아 삭제 여부를 상황에 따라 결정하시기 바랍니다. 삭제할 수 없는 경우 클라우드 디스크 확장을 통해 하드 디스크 스토리지 공간을 확장하십시오.

파일 시스템 inode 가득 찬 문제 해결

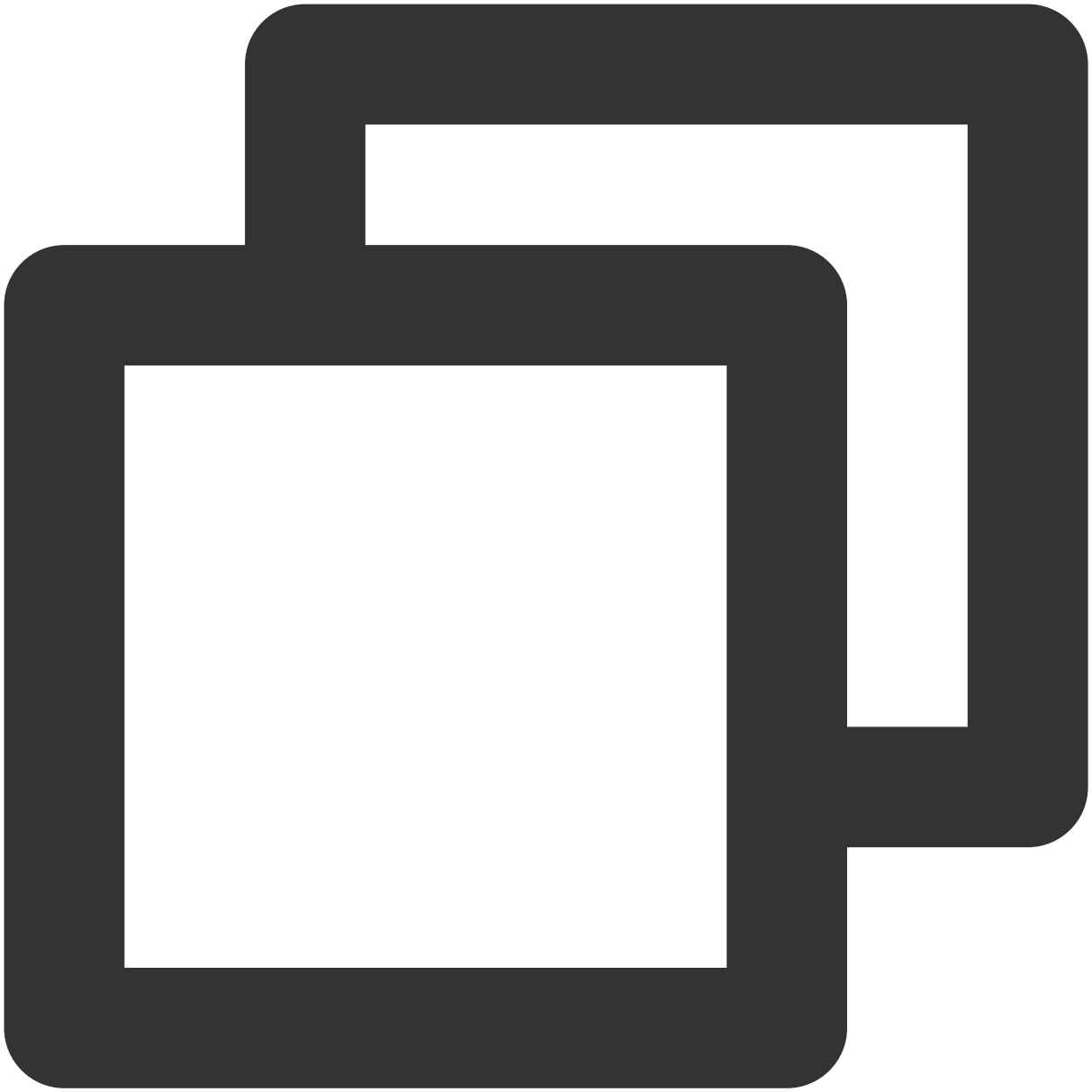
1. CVM에 로그인합니다. 자세한 내용은 표준 로그인 방식으로 Linux 인스턴스에 로그인을 참고하십시오.

2. 다음 명령어를 실행하여 디스크 사용량을 확인합니다.



```
df -h
```

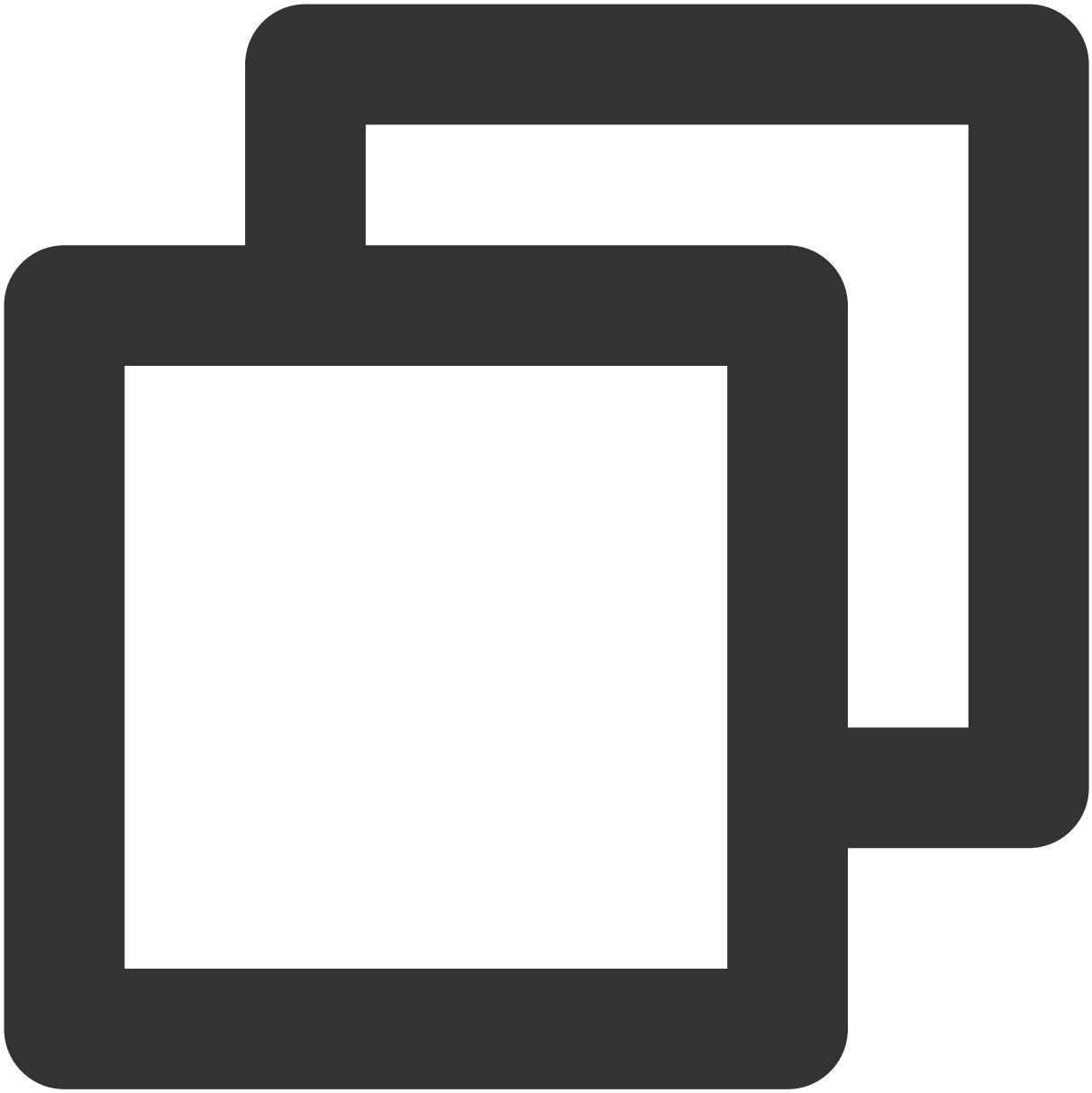
3. 디스크 사용량이 많은 마운트 포인트를 찾고 다음 명령을 실행하여 마운트 포인트로 이동합니다.



```
cd는 마운트 포인트에 해당
```

예를 들어, cd 시스템 디스크 마운트 포인트가 필요한 경우 `cd /` 를 실행합니다.

4. 다음 명령을 실행하여 문제를 해결하기 위해 파일 수가 가장 많은 디렉터리를 찾습니다. 이 명령은 시간이 많이 소요됩니다. 잠시만 기다려 주십시오.

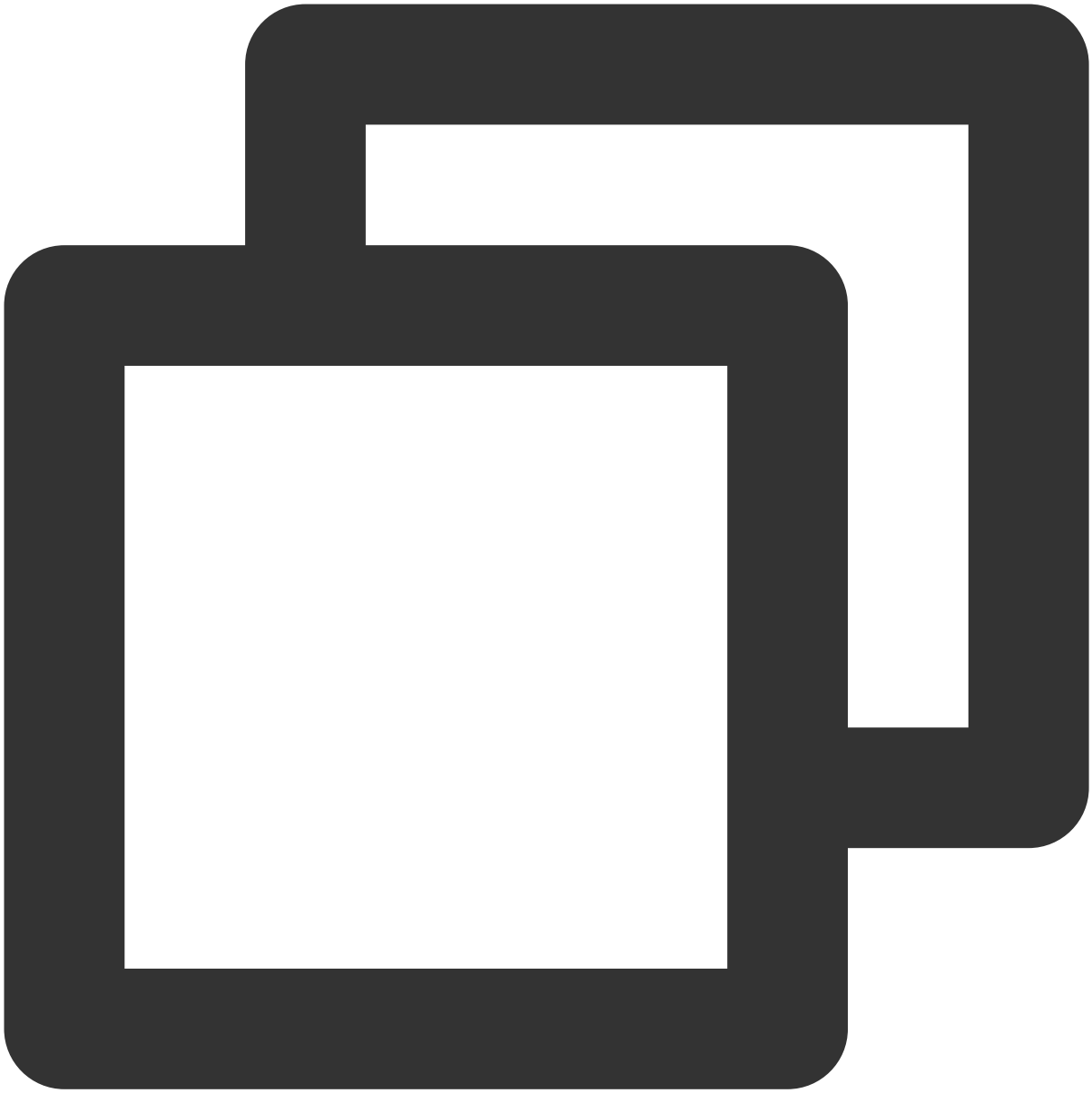


```
find / -type f | awk -F / -v OFS=/ '{$NF="";dir[$0]++}END{for(i in dir)print dir[i]
```

df du의 불일치 문제 해결

프로세스 점유 파일 핸들 문제 해결

다음 명령을 실행하여 파일 점유 프로세스를 조회합니다.



```
lsof | grep delete
```

반환 결과에 따라 다음 단계를 수행하십시오.

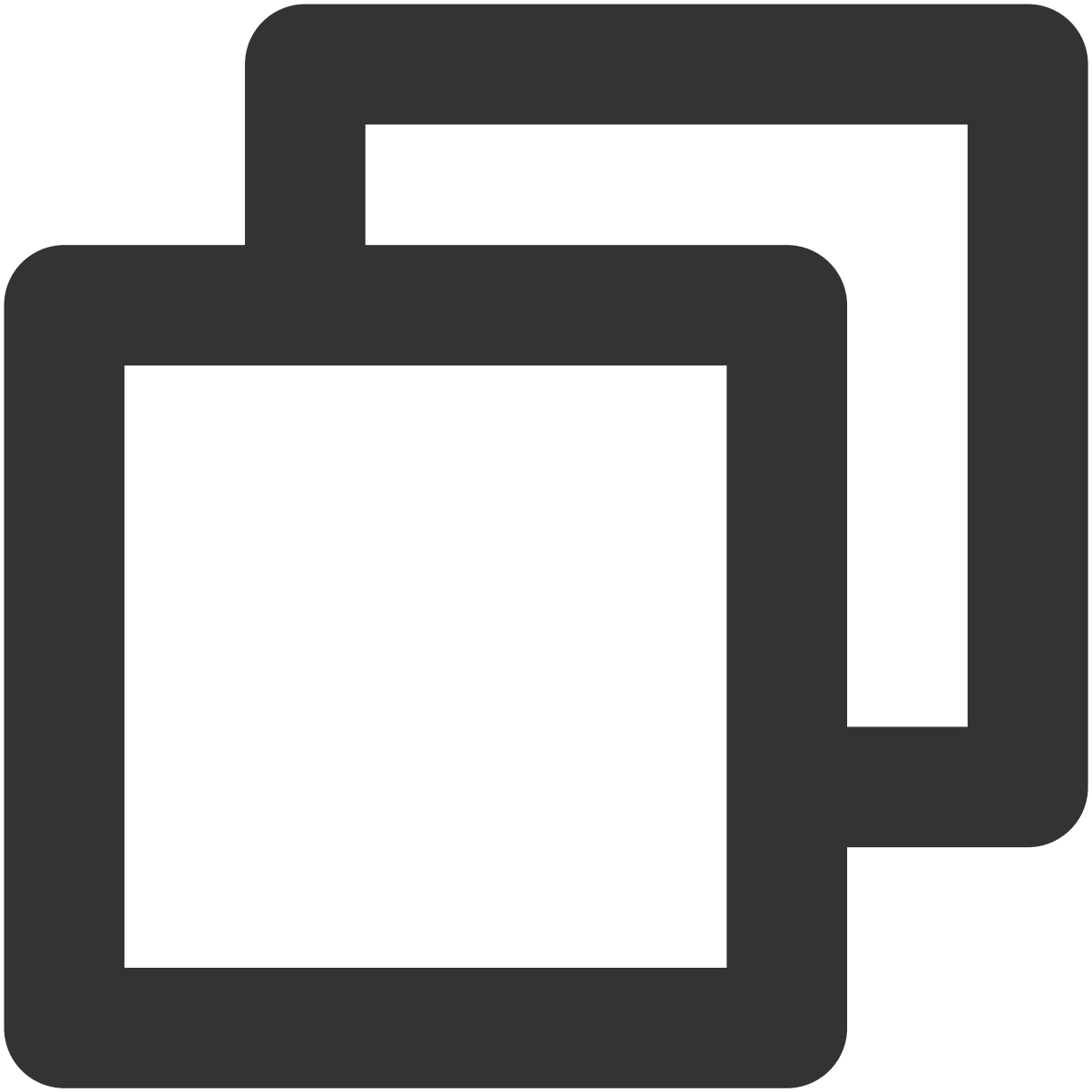
해당 프로세스를 kill 합니다.

서비스를 재시작합니다.

많은 프로세스가 파일 핸들을 점유하는 경우 서버를 재시작합니다.

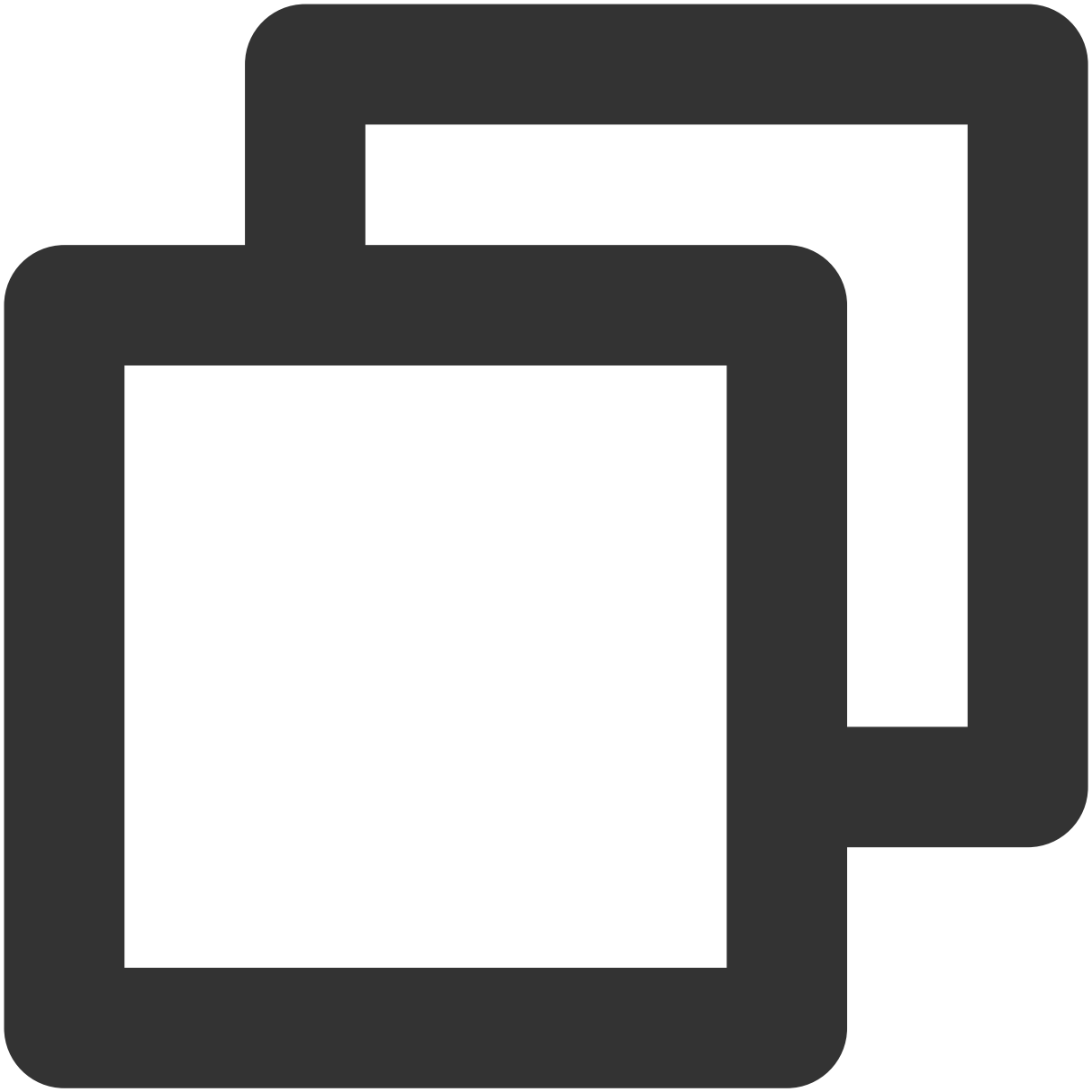
mount 마운트 중첩 문제 해결

1. mount 명령어를 실행하여 `/mnt` 에 공간이 큰 디스크를 mount합니다. 예시:



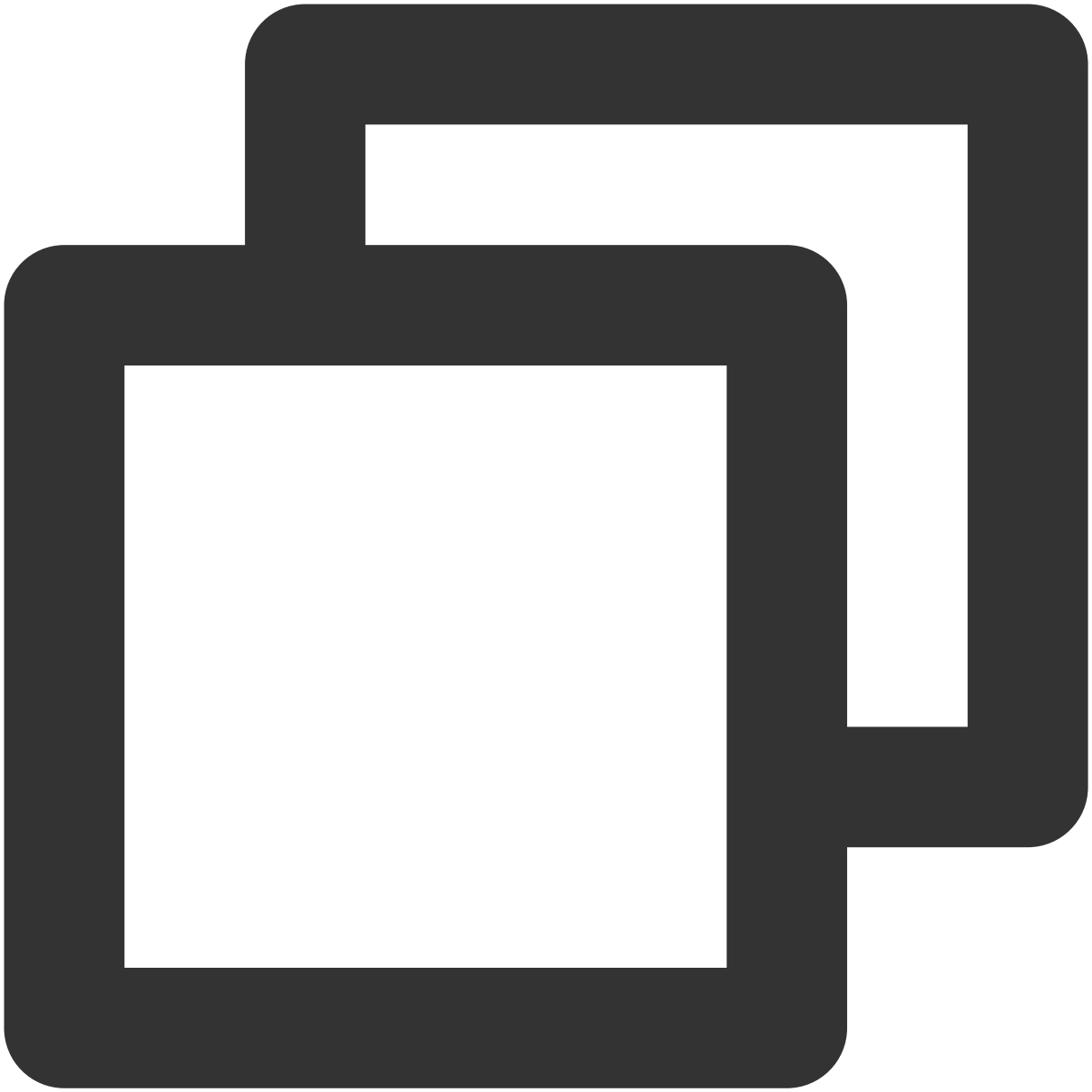
```
mount /dev/vda1 /mnt
```

2. 다음 명령어를 실행하여 `/mnt` 를 입력합니다.



```
cd /mnt
```

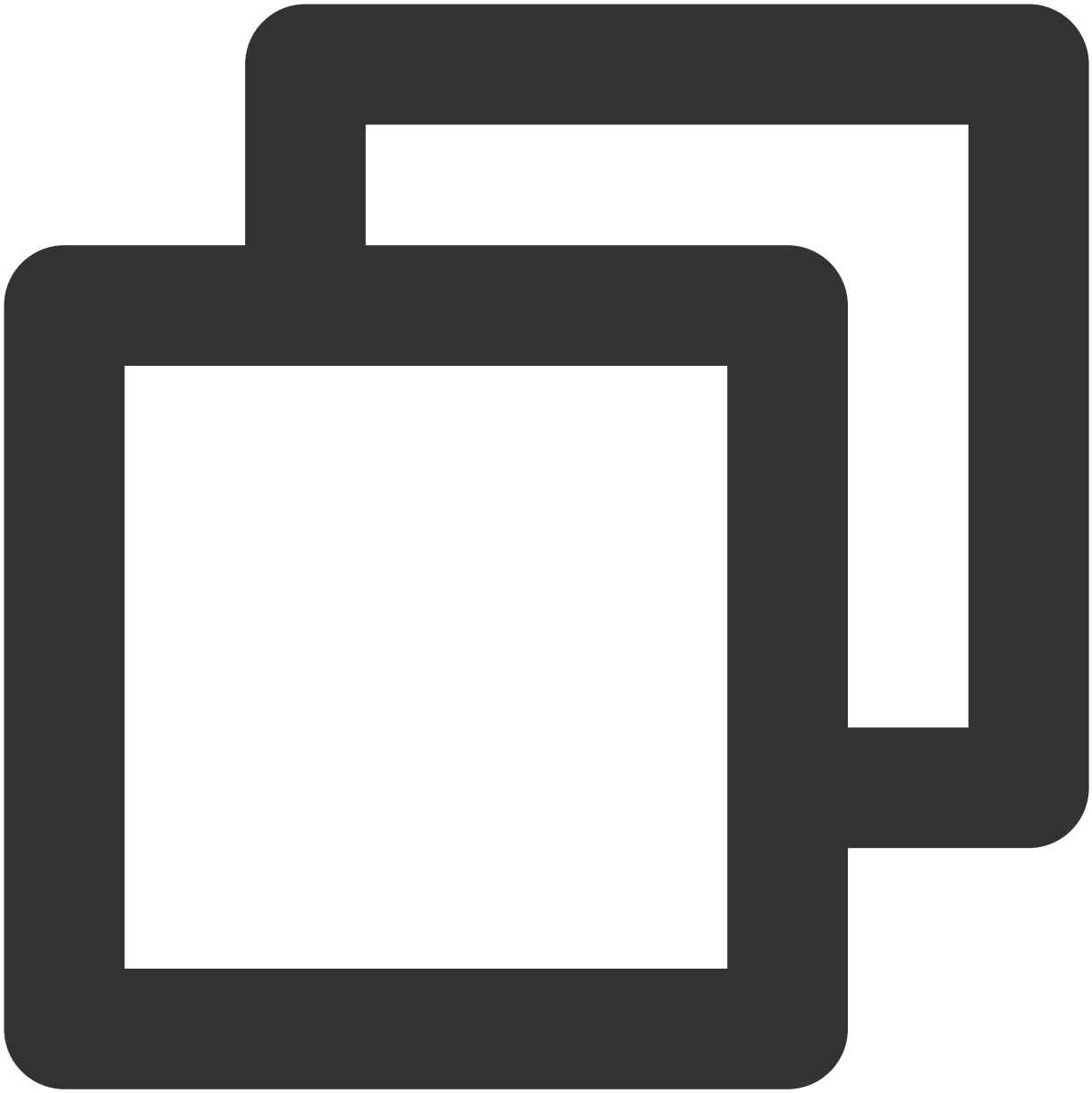
3. 다음 명령어를 실행하여 많은 공간을 차지하는 디렉터리를 찾습니다.



```
du -x --max-depth=1 | sort -n
```

반환 결과를 바탕으로 비즈니스 상황에 따라 디렉터리 또는 파일 삭제 여부를 결정합니다.

4. umount 명령을 실행하여 디스크를 umount합니다. 예시:



```
umount /mnt
```

Linux 인스턴스 메모리 관련 장애
지나치게 높은 인스턴스 메모리 사용률

최종 업데이트 날짜: : 2024-02-02 11:09:48

현상 설명

Linux CVM 인스턴스에 메모리 문제로 장애가 발생했습니다(예시: 시스템 내부 서비스 응답 속도 감소, 서버 로그인 불가, 시스템 OOM 트리거 등).

예상 원인

지나치게 높은 인스턴스 메모리 사용률이 원인인 것으로 보입니다. 보통 인스턴스 메모리 사용률이 지속적으로 90%를 넘을 경우 사용률이 지나치게 높다고 판단합니다.

문제 진단

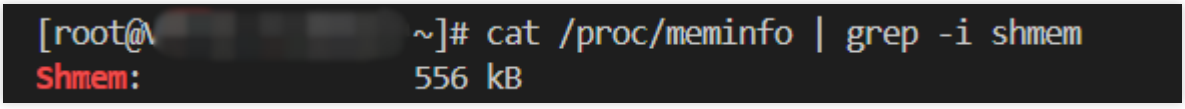
1. 처리 순서를 참조하여 인스턴스 메모리 사용률이 지나치게 높아서 생긴 문제인지 판단합니다.
2. 기타 메모리 문제의 전형적인 사례 분석을 참조하여 문제 원인을 파악합니다.

처리 순서

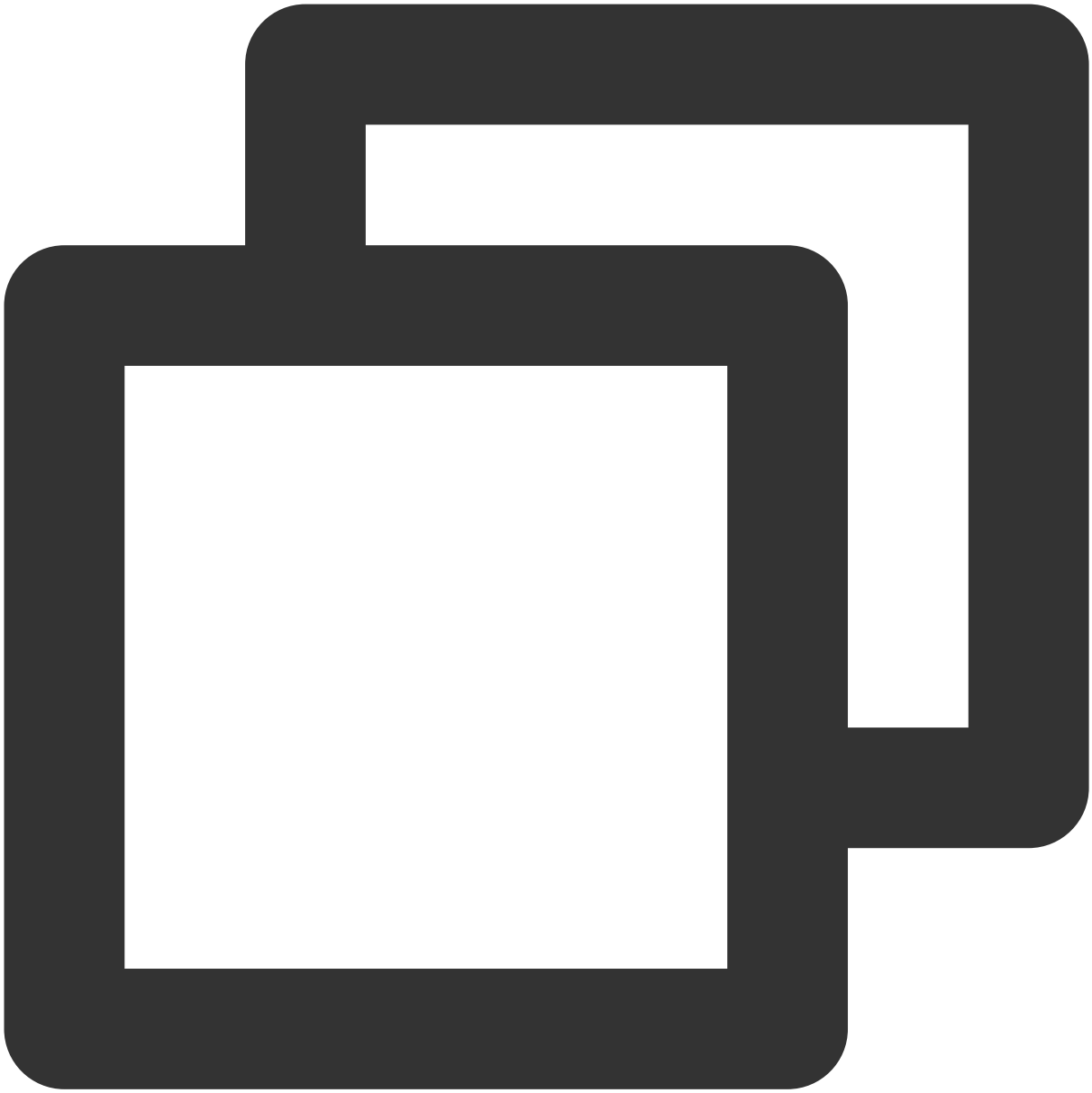
1. 관련 작업을 참조하여 메모리 사용률이 지나치게 높지는 않은지 확인합니다.
메모리 사용률이 지나치게 높다면 다음 단계를 실행합니다.
메모리 사용률이 정상인 경우 기타 메모리 문제의 전형적인 사례 분석을 참조하여 자세한 문제 원인을 파악합니다.
2. 시스템 내부에서 `top` 명령어를 실행한 후 **M**을 눌러 'RES'나 'SHR' 열에 메모리 점유율이 지나치게 높은 프로세스가 있는지 확인합니다.
없는 경우 다음 단계를 실행합니다.
있는 경우 프로세스 유형에 맞춰 작업을 진행합니다. 자세한 내용은 프로세스 분석을 참조하십시오.
3. 다음 명령어를 실행하여 공유 메모리 점유율이 지나치게 높지는 않은지 확인합니다.

```
cat /proc/meminfo | grep -i shmem
```

반환 결과는 다음 이미지와 같습니다.

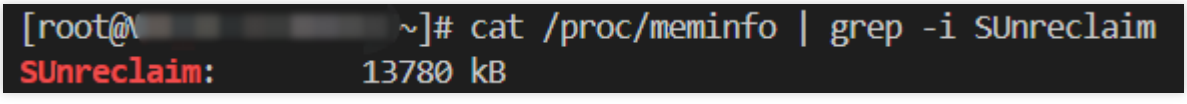


4. 다음 명령어를 실행하여 회수할 수 없는 slab 메모리의 점유율이 지나치게 높지는 않은지 확인합니다.

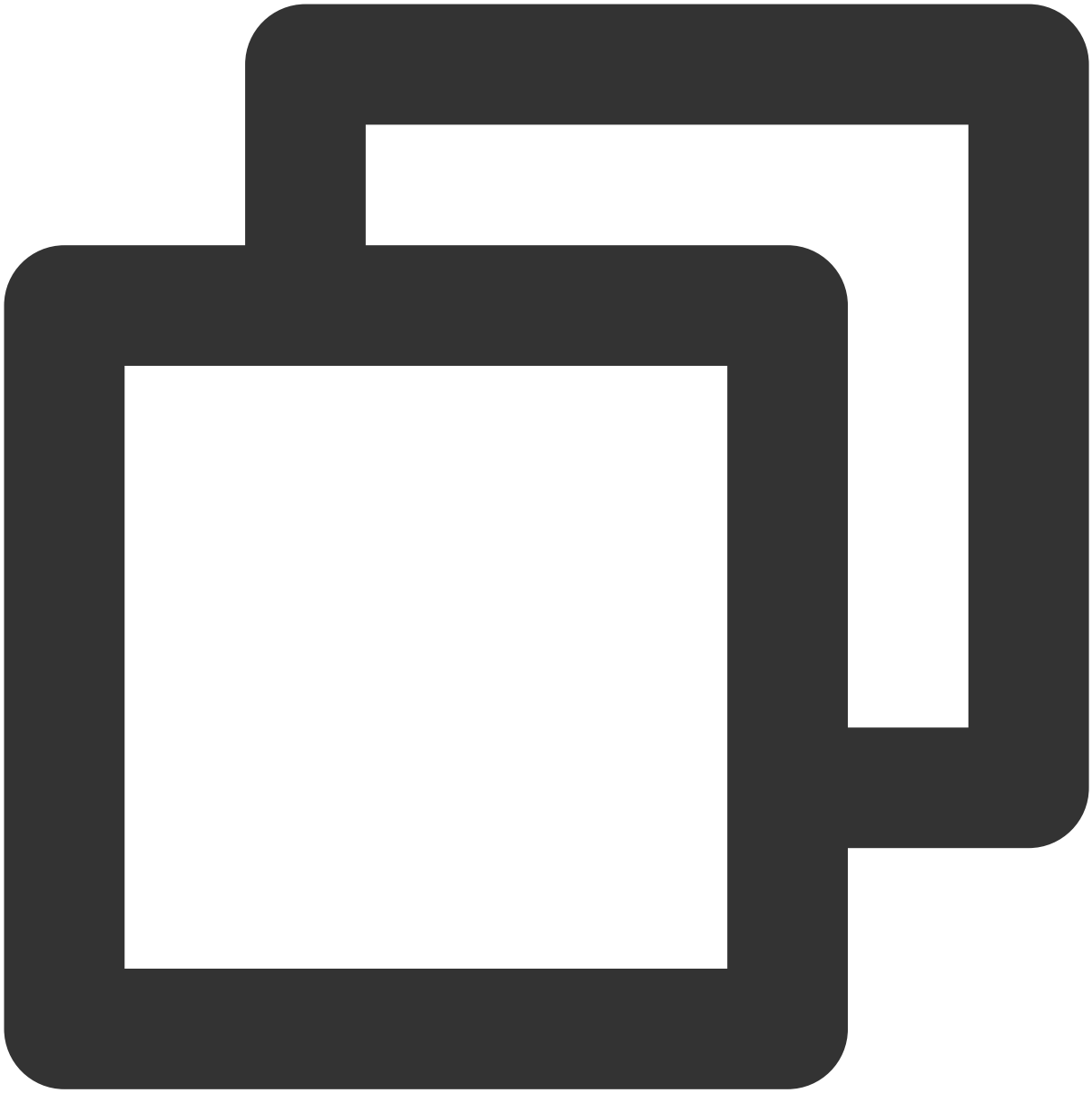


```
cat /proc/meminfo | grep -i SUnreclaim
```

반환 결과는 다음 이미지와 같습니다.

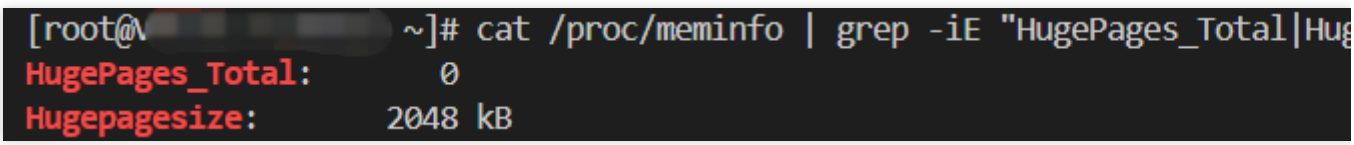


5. 다음 명령어를 실행하여 Hugepage 메모리가 있는지 확인합니다.



```
cat /proc/meminfo | grep -iE "HugePages_Total|Hugepagesize"
```

반환 결과는 다음 이미지와 같습니다.



`HugePages_Total` 의 출력값이 0인 경우 기타 메모리 문제의 전형적인 사례 분석을 참조하여 자세한 문제 원인을 파악합니다.

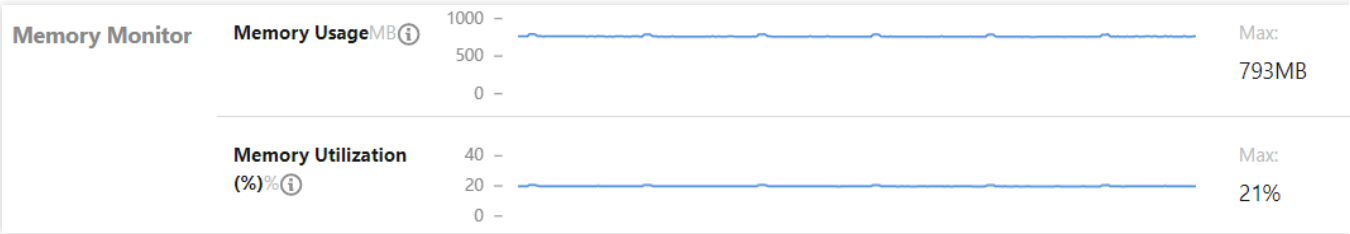
`HugePages_Total` 의 출력값이 0이 아닌 경우 Hugepage 메모리가 설정되어 있다는 의미입니다. Hugepage 메모리의 크기는 `HugePages_Total*Hugepagesize` 이며, Hugepage가 다른 악성 프로그램을 위해 설정된 것은 아닌지 확인해야 합니다. Hugepage 메모리가 필요하지 않다면 `/etc/sysctl.conf` 파일의 `vm.nr_hugepage` 설정 항목에 주석을 달고 `sysctl -p` 명령어를 실행하여 Hugepage 메모리 설정을 해제합니다.

관련 작업

메모리 사용률 조회

Linux 릴리스 버전마다 `free` 명령어 출력의 의미가 다를 수 있기 때문에 `free` 명령어 출력 정보만으로 메모리 사용률을 계산할 수는 없습니다. 그러므로 다음 절차를 따라 Tencent Cloud 모니터링을 통해 메모리 사용률을 확인하시기 바랍니다.

1. CVM 콘솔에 로그인하여 인스턴스 관리 페이지를 클릭합니다.
2. 인스턴스 ID를 선택하고 해당 인스턴스 상세 페이지로 이동하여 [모니터링] 탭을 선택합니다.
3. '메모리 모니터링'에서 다음과 같이 해당 인스턴스의 메모리 사용률을 조회할 수 있습니다.



컴퓨팅 메모리 사용률

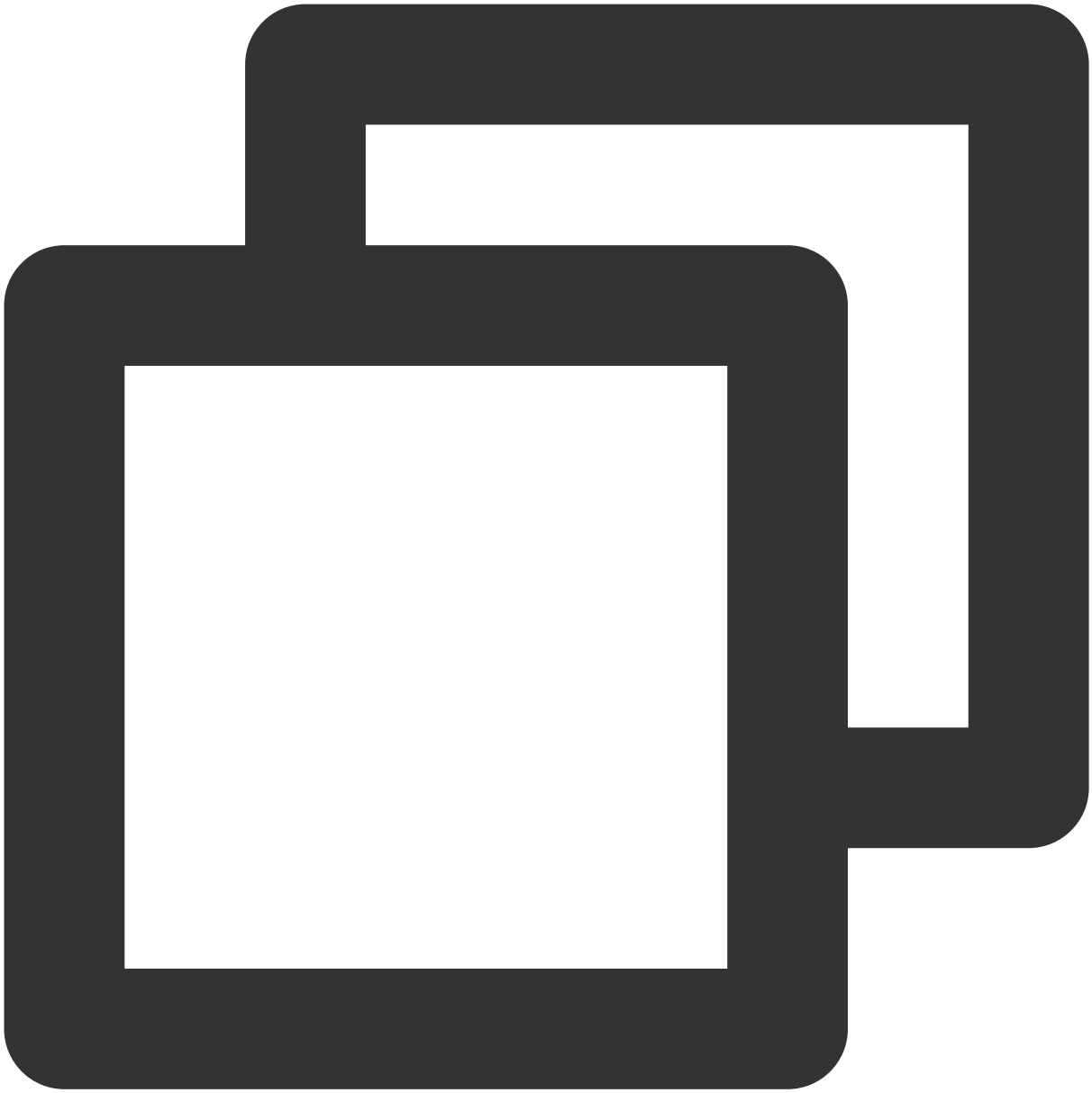
메모리 모니터링에서 메모리 사용률은 총 메모리 중 사용한 메모리의 비율로 계산합니다. 버퍼와 시스템 캐시가 점유하는 콘텐츠는 포함되지 않습니다. 계산 프로세스는 다음과 같습니다.

= `(Total - available)100% / Total`

= `(Total - (Free + Buffers + Cached + SReclaimable - Shmem))100% /Total`

= `(Total - Free - Buffers - Cached - SReclaimable + Shmem) * 100% / Total`

계산 프로세스에서 사용하는 `Total` , `Free` , `Buffer` , `Cached` , `SReclaimable` , `Shmem` 매개변수는 `/proc/meminfo` 에서 획득할 수 있습니다. 다음은 `/proc/meminfo` 예시입니다.



```
[root@VM_0_113_centos test]# cat /proc/meminfo
MemTotal: 16265592 kB
MemFree: 1880084 kB
......
Buffers: 194384 kB
Cached: 13647556 kB
......
Shmem: 7727752 kB
Slab: 328864 kB
SReclaimable: 306500 kB
SUnreclaim: 22364 kB
```

```
12. ......
13. HugePages_Total: 0
14. Hugepagesize: 2048 kB
```

다음은 매개변수에 대한 설명입니다.

매개변수	설명
MemTotal	시스템 총 메모리입니다.
MemFree	시스템 잔여 메모리입니다.
Buffers	블록 디바이스가 점유하는 캐시 페이지입니다. 직접 읽기/쓰기 블록 디바이스와 파일 시스템 메타데이터가 여기에 포함됩니다(예: SuperBlock이 사용하는 캐시 페이지).
Cached	page cache입니다. tmpfs의 파일 POSIX/SysV shared memory 및 shared anonymous mmap이 포함됩니다.
Shmem	tmpfs 등 공유 메모리를 포함합니다.
Slab	커널 slab 할당자가 할당한 메모리는 slabtop로 조회할 수 있습니다.
SReclaimable	회수할 수 있는 slab입니다.
SUnreclaim	회수할 수 없는 slab입니다.
HugePages_Total	Hugepage 메모리의 총 수량입니다.
Hugepagesize	Hugepage 메모리 1페이지의 크기입니다.

기타 메모리 문제의 전형적인 사례 분석

위 절차를 따랐음에도 문제가 처리되지 않거나, CVM 사용 시 아래 유형의 오류 정보가 나타난다면 다음 솔루션을 참조하십시오.

로그 오류 보고 fork: Cannot allocate memory

VNC 로그인 오류 보고 Cannot allocate memory

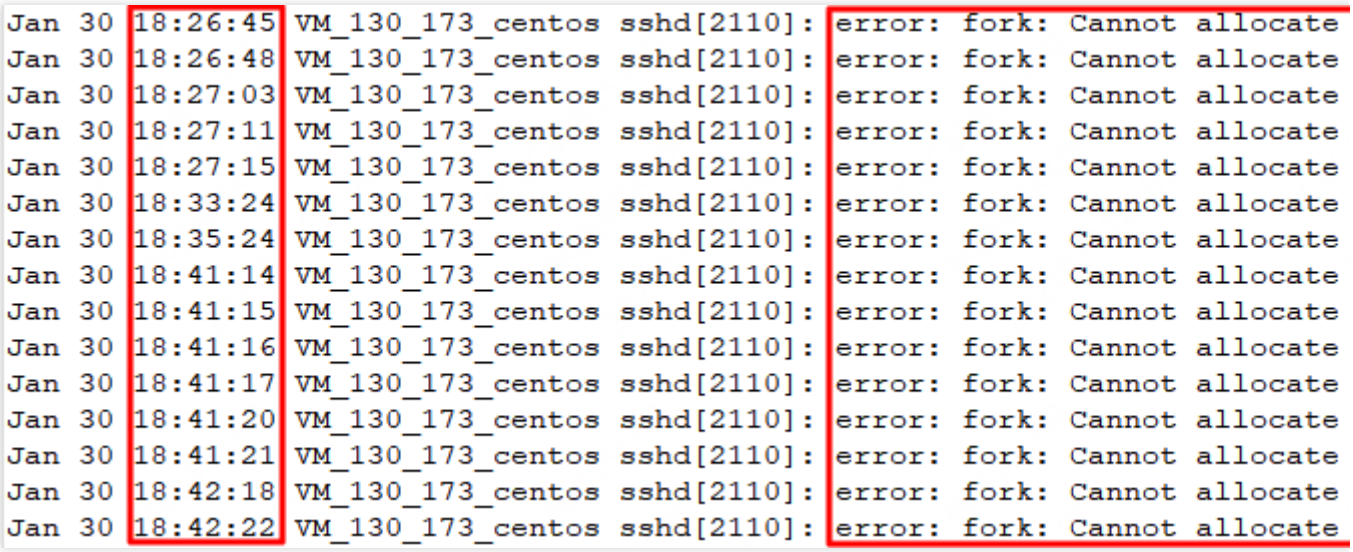
인스턴스 메모리 사용량이 남은 상황에서 Out Of Memory 트리거

로그 오류 보고 fork: Cannot allocate memory

최종 업데이트 날짜: : 2024-02-02 11:09:48

현상 설명

로그에 아래 이미지와 같이 'fork: Cannot allocate memory'. 오류 보고가 나타납니다.



예상 원인

가능한 원인은 프로세스 수 초과입니다. 시스템 내부의 총 프로세스 수가 `pid_max` 에 도달하면 신규 프로세스 생성 시 'fork: Cannot allocate memory' 오류가 보고됩니다.

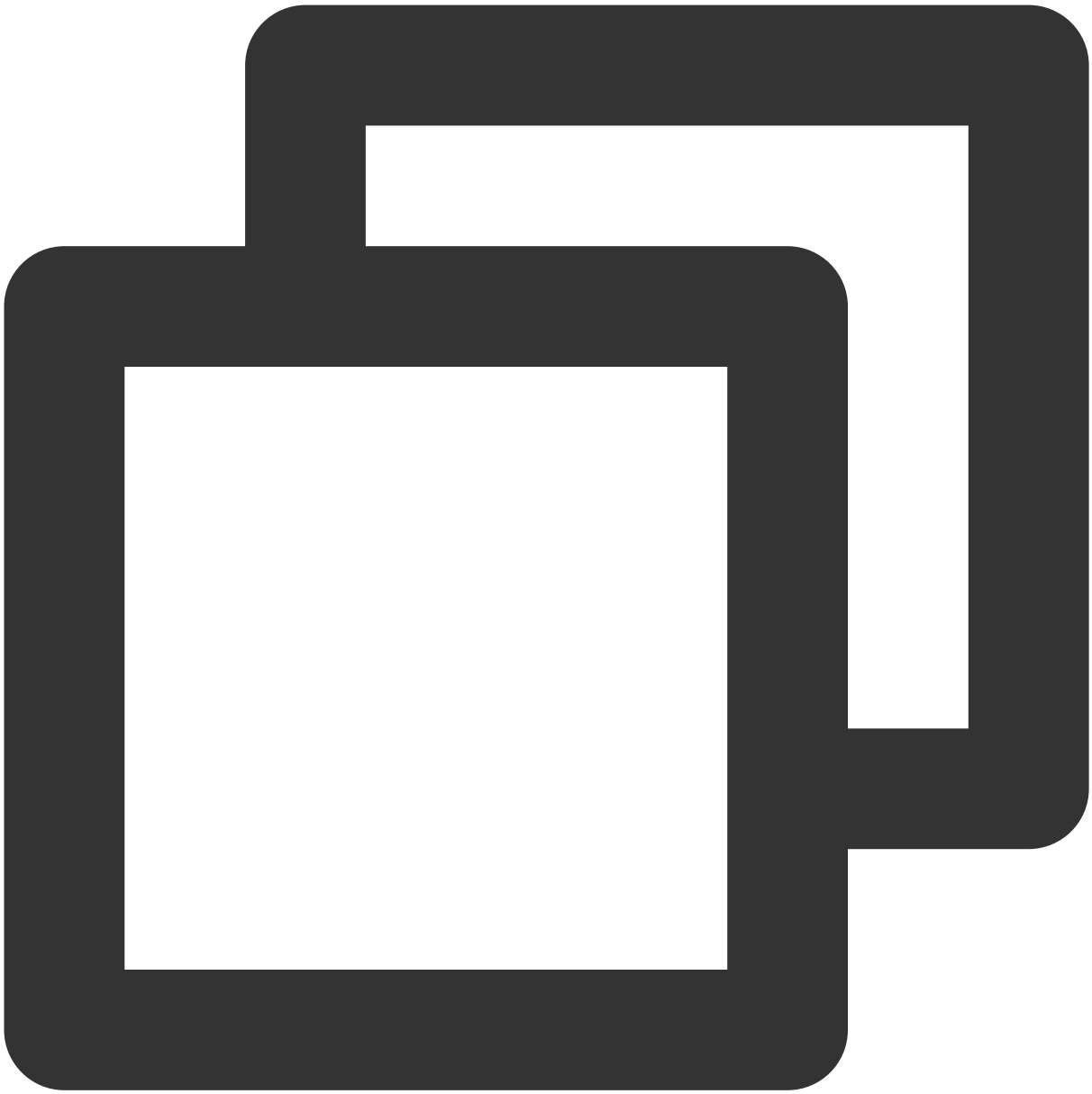
해결 방법

1. 처리 순서를 참고하여 인스턴스 메모리 사용률이 지나치게 높지는 않은지 확인합니다.
2. 총 프로세스 수가 제한을 초과하는지 확인하고 총 프로세스 수 'pid_max'의 설정을 수정합니다.

처리 순서

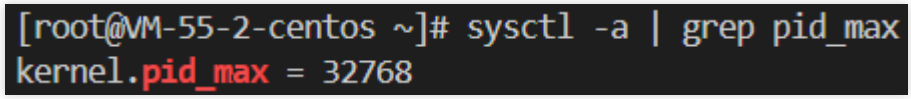
1. 지나치게 높은 인스턴스 메모리 사용률을 참고하여 인스턴스 메모리 사용률을 확인합니다. 인스턴스 메모리 사용률이 정상이라면 다음 단계를 실행합니다.

2. 다음 명령어를 실행하여 시스템의 `pid_max` 값을 조회합니다.

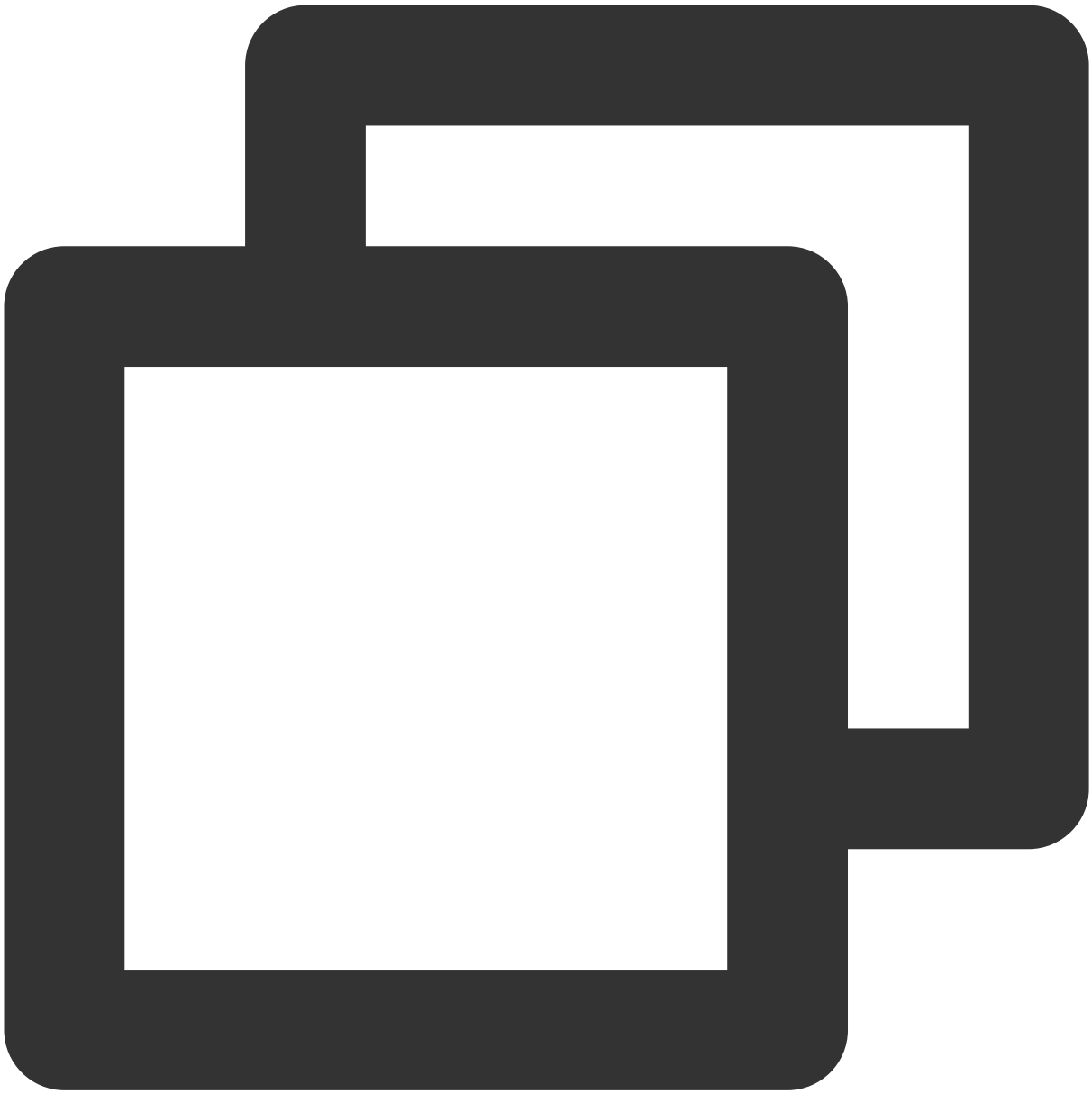


```
sysctl  -a | grep pid_max
```

반환된 결과에 따라 해당 작업을 수행합니다.
반환된 결과는 아래 이미지와 같으며, `pid_max` 의 기본값은 32768입니다. 다음 단계로 이동하십시오.



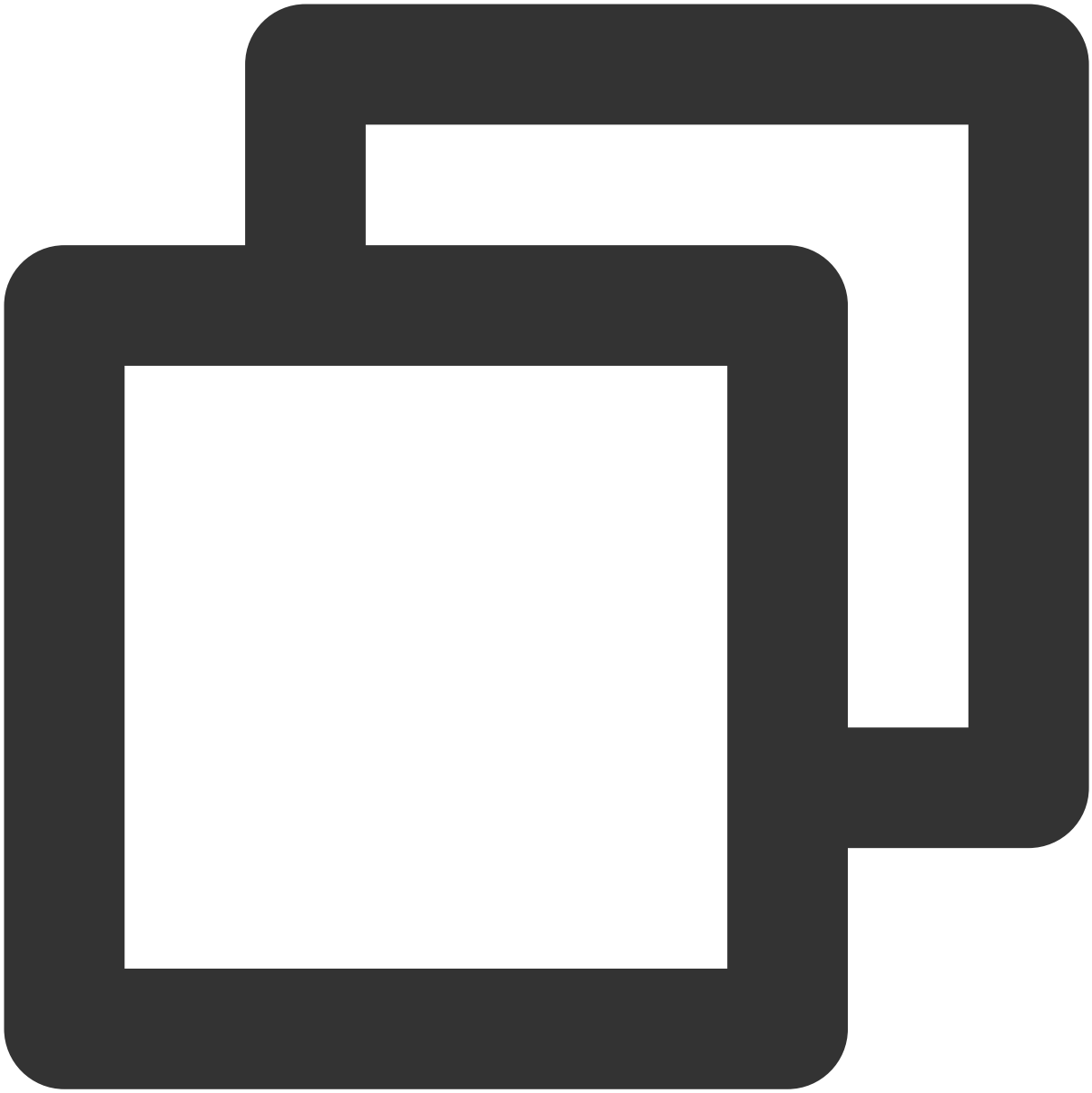
'fork:Cannot assign memory' 오류 메시지가 반환되면 다음 명령어를 실행하여 일시적으로 `pid_max` 를 늘려야 합니다.



```
echo 42768 > /proc/sys/kernel/pid_max
```

명령어를 다시 실행하여 시스템의 `pid_max` 값을 조회할 수 있습니다.

3. 다음 명령어를 실행하여 시스템 내부의 총 프로세스 수를 조회합니다.



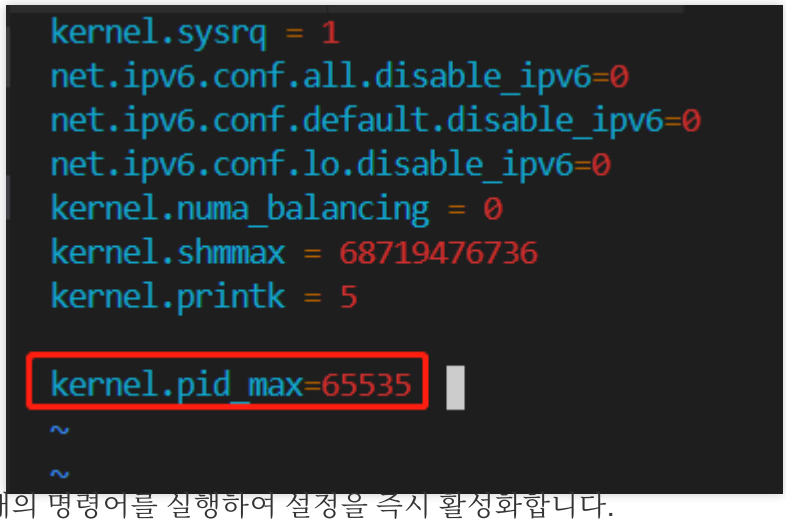
```
pstree -p | wc -l
```

총 프로세스 수가 `pid_max` 에 도달하면 신규 프로세스 생성 시 시스템에서 'fork: Cannot allocate memory' 오류가 보고됩니다.

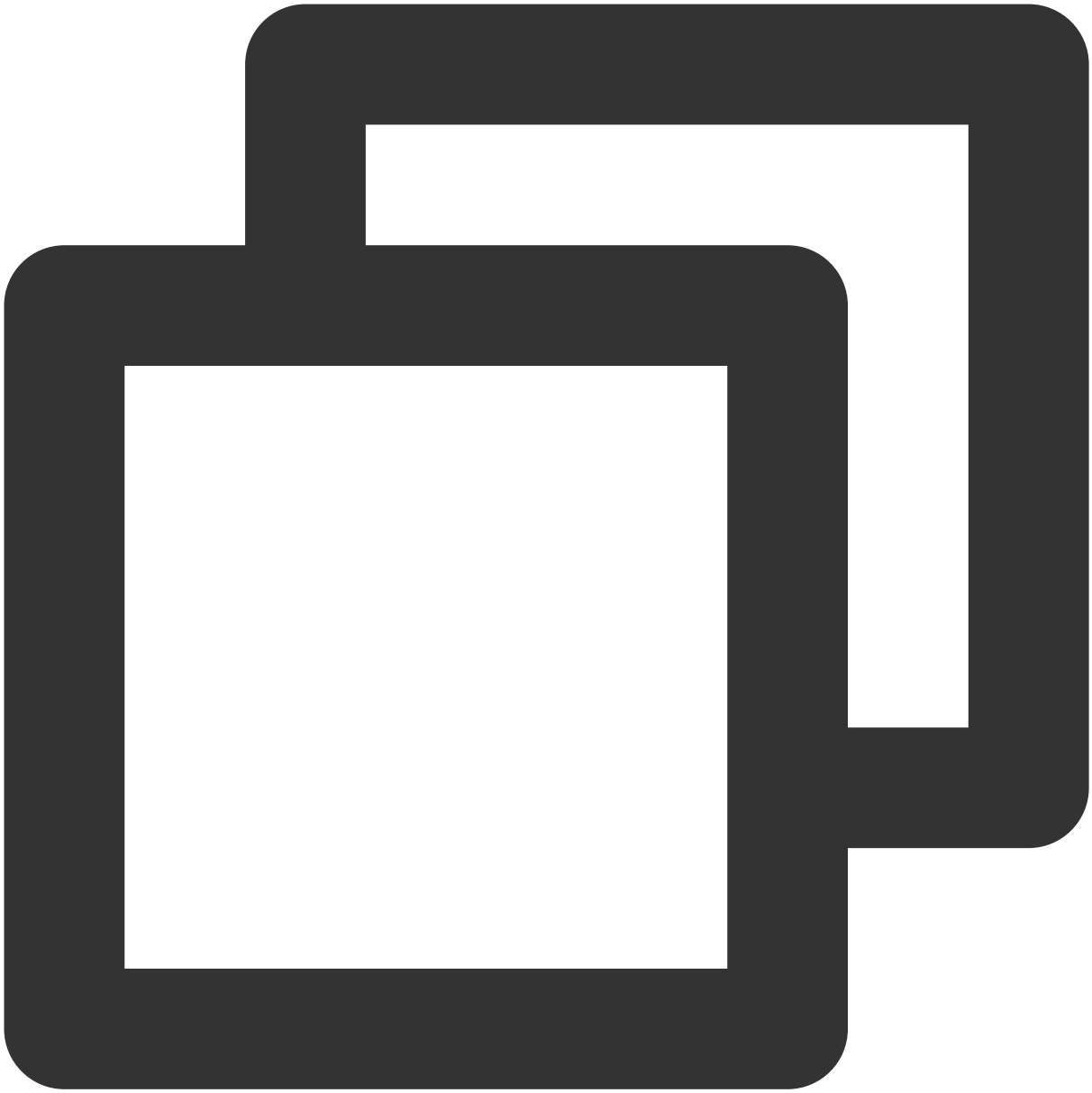
설명：

`ps -efL` 명령어를 실행하여 프로세스 수가 비교적 많은 프로그램을 파악합니다.

4. 프로세스 수를 늘리기 위해 `/etc/sysctl.conf` 설정 파일의 `kernel.pid_max` 값을 65535로 수정합니다. 수정이 완료되면 다음과 같은 화면이 나타납니다.



5. 아래의 명령어를 실행하여 설정을 즉시 활성화합니다.



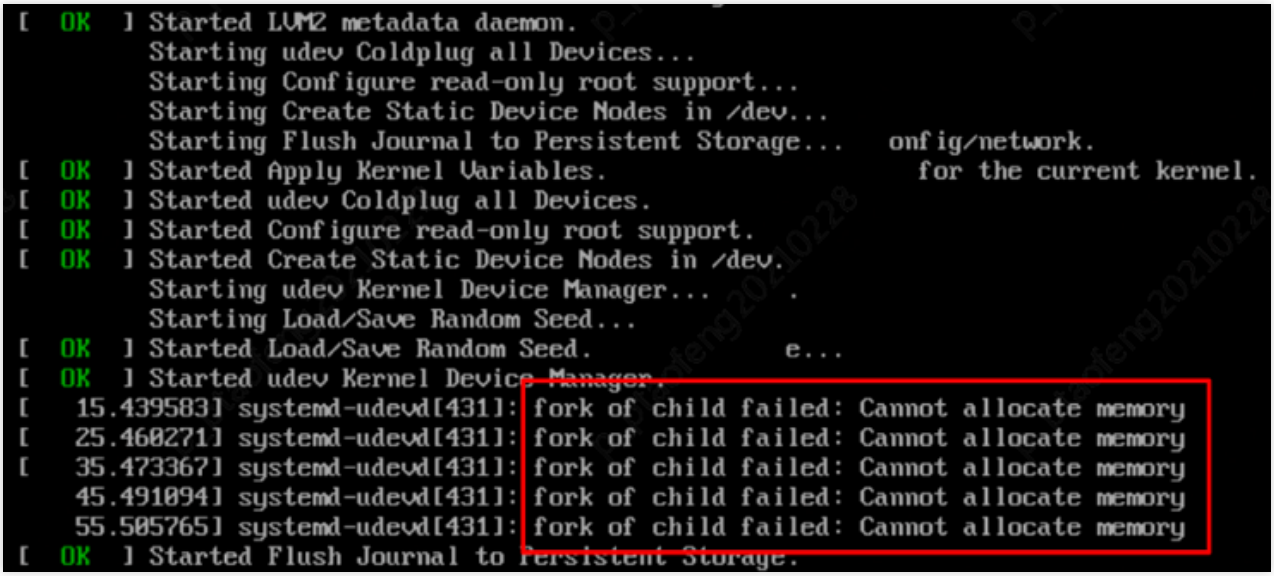
```
sysctl -p
```

VNC 로그인 오류 보고 Cannot allocate memory

최종 업데이트 날짜: : 2024-02-02 11:09:48

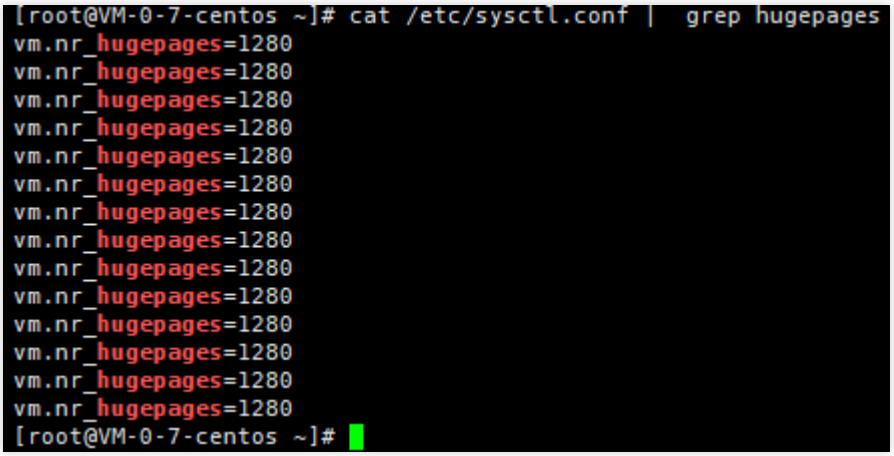
현상 설명

VNC로 CVM에 로그인할 때 시스템에 정상적으로 액세스되지 않고, 다음과 같이 'Cannot allocate memory' 오류 보고 정보가 나타납니다.



예상 원인

시스템 내 다수의 Hugepage 메모리가 원인인 것으로 보입니다. 하나의 Hugepage 메모리는 기본적으로 2048KB를 차지합니다. `/etc/sysctl.conf` 의 Hugepage 개수 계산에 따르면, 아래 예시처럼 1,280개의 Hugepage 메모리는 2.5G에 해당합니다. 인스턴스 설정은 낮은데 Huge pages pool에 2.5G을 할당하게 되면 시스템에 사용 가능한 메모리가 없어 재시작 후 시스템에 액세스할 수 없습니다.

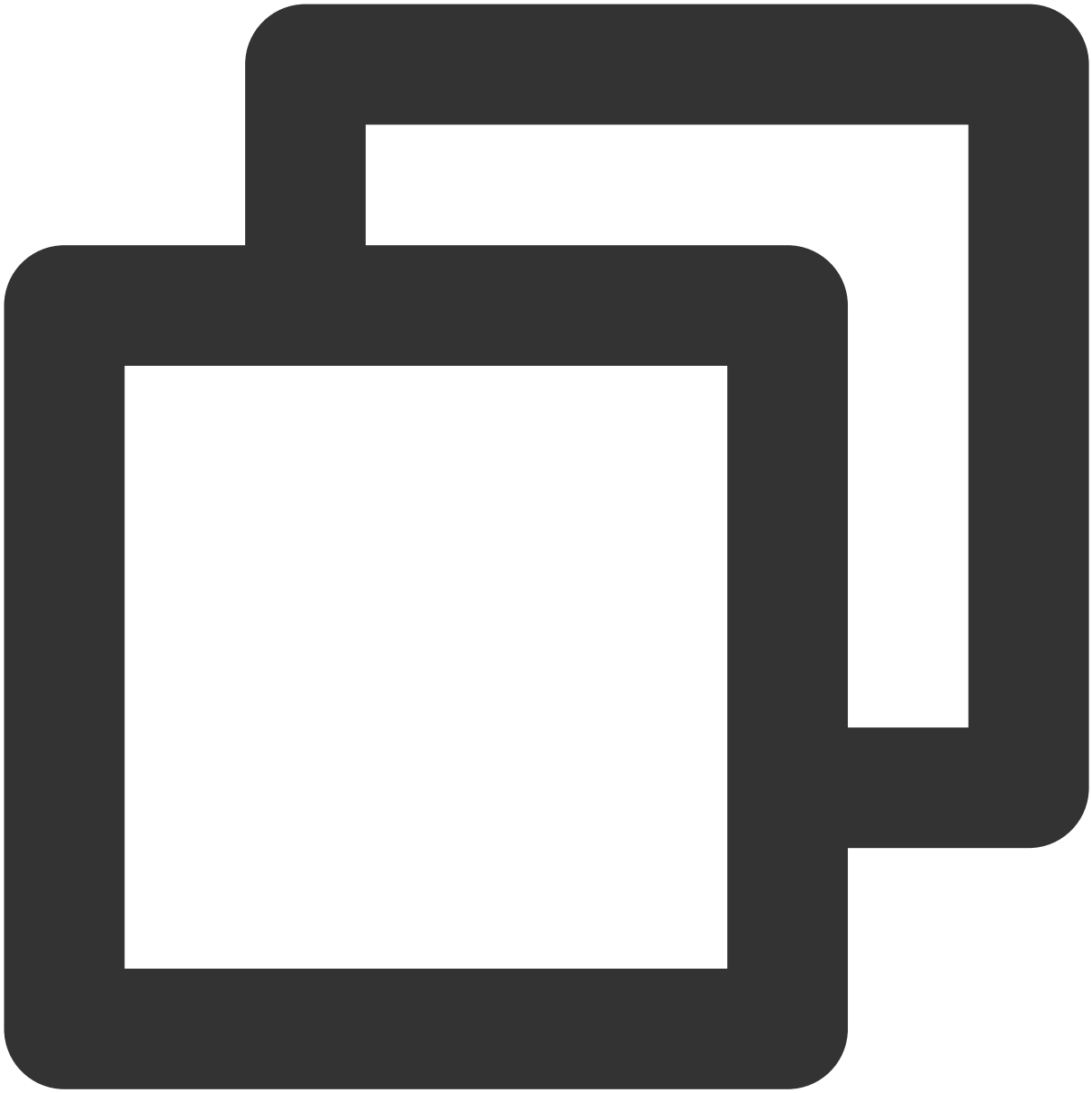


해결 방법

1. 처리 순서를 참고하여 총 프로세스 처리 수 제한 여부를 확인합니다.
2. Hugepage의 메모리 설정을 확인하고 적절하게 수정합니다.

처리 순서

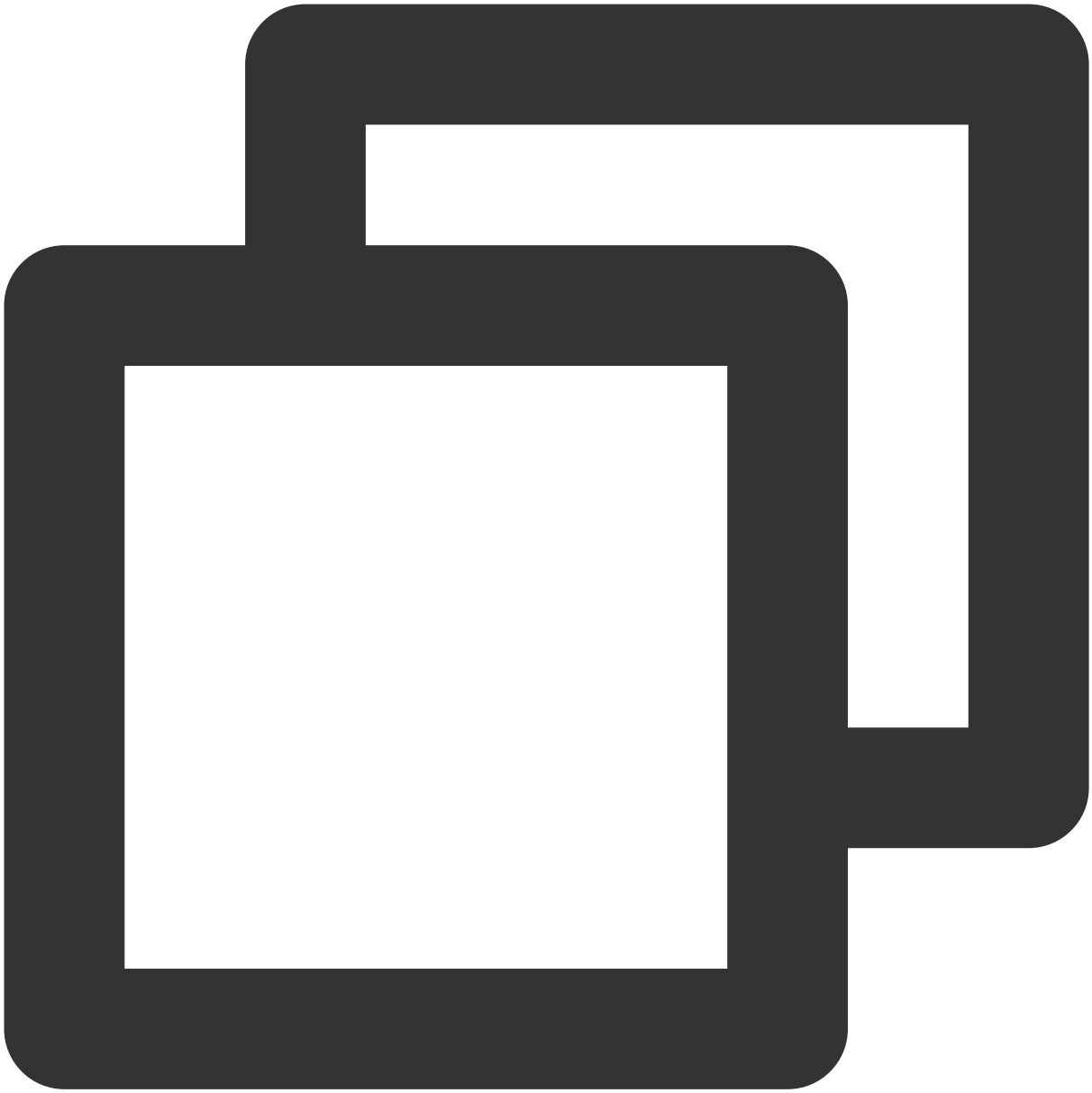
1. 로그 오류 보고 fork: Cannot allocate memory를 참고하여 프로세스 수가 제한을 초과하는지 확인합니다. 초과하지 않는다면 다음 단계를 실행합니다.
2. 단일 사용자 모드로 CVM에 로그인합니다. 자세한 내용은 Linux CVM 단일 사용자 모드 진입 설정을 참고하십시오.
3. 다음 명령어를 실행합니다. 예상 원인을 참고하여 Hugepage 메모리 설정을 확인합니다.



```
cat /etc/sysctl.conf | grep hugepages
```

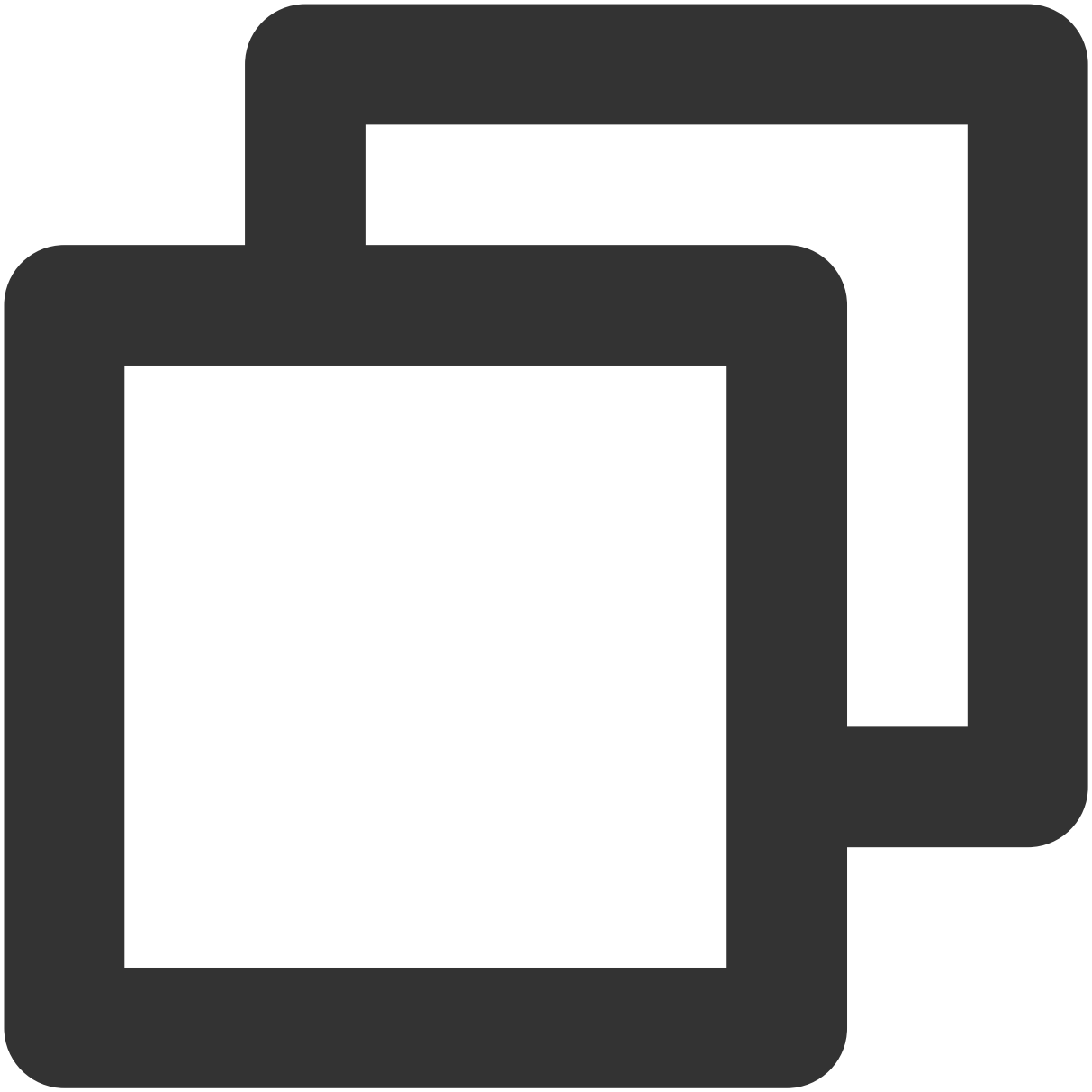
Hugepage 메모리가 여러 개인 경우 아래 순서에 따라 설정을 수정하십시오.

4. 다음 명령어를 실행하여 VIM 편집기로 `/etc/sysctl.conf` 구성 파일을 엽니다.



```
vim /etc/sysctl.conf
```

5. **i**를 눌러 편집 모드로 전환하고, 인스턴스의 실제 설정에 맞춰 `vm.nr_hugepages` 설정 항목을 적정값으로 낮춥니다.
6. **Esc**를 누르고 **:wq**를 입력한 다음, **Enter**를 눌러 저장하고 VIM 편집기를 종료합니다.
7. 아래의 명령어를 실행하여 설정을 즉시 적용합니다.



```
sysctl -p
```

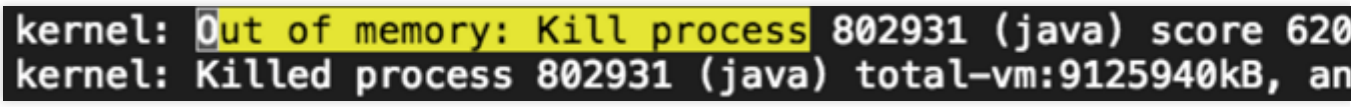
8. 설정 완료 후 CVM을 재시작하면 정상적으로 로그인이 가능합니다.

인스턴스 메모리 사용량이 남은 상황에서 Out Of Memory 트리거

최종 업데이트 날짜: : 2024-02-02 11:09:48

현상 설명

다음과 같이 Linux CVM에 메모리 사용량이 남은 상황에서 OOM(Out Of Memory)이 트리거됩니다.



예상 원인

가능한 원인은 시스템 내 사용 가능한 메모리가 `min_free_kbytes` 값보다 적은 것입니다.
`min_free_kbytes` 값은 Linux 시스템에 강제로 남겨지는 최소 유휴 메모리(Kbytes)입니다. 시스템 내 사용 가능한 메모리가 `min_free_kbytes` 설정 값보다 적은 경우, 시스템은 oom-killer을 실행하거나 강제 재시작되도록 기본 설정되어 있습니다. 구체적인 실행은 커널 매개변수 `vm.panic_on_oom` 값에 의해 결정됩니다.
`vm.panic_on_oom=0` 인 경우 시스템에 OOM 메시지가 나타나고 oom-killer가 실행되어 메모리 점유율이 가장 높은 프로세스를 종료합니다.
`vm.panic_on_oom =1` 인 경우 시스템이 자동으로 재시작됩니다.

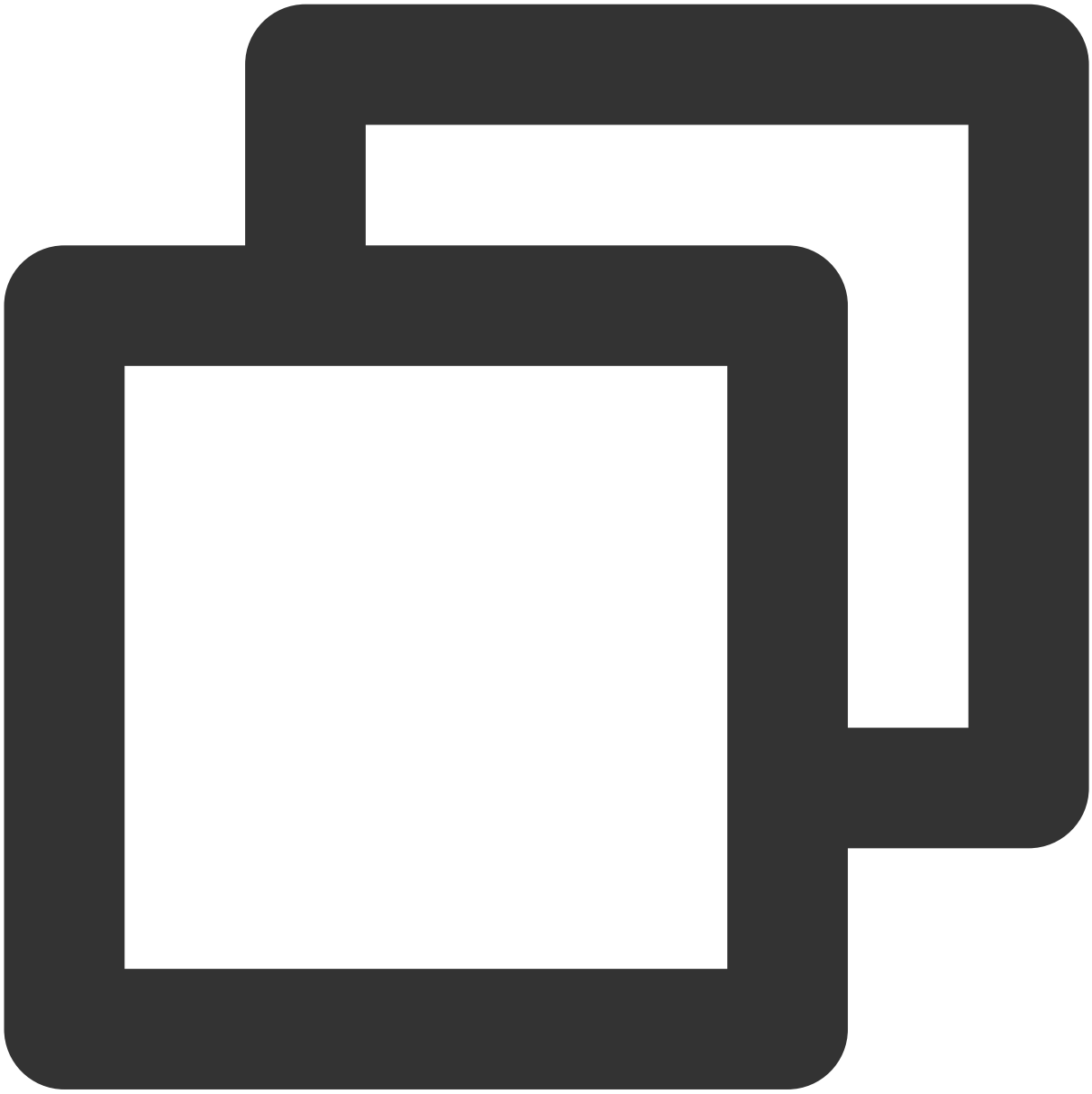
해결 방법

1. 처리 순서를 참고하여 인스턴스 메모리 사용률이 지나치게 높지는 않은지, 프로세스 수에 제한이 있는지 확인합니다.
2. `min_free_kbytes` 값 설정을 확인하고 올바르게 수정합니다.

처리 순서

1. 지나치게 높은 인스턴스 메모리 사용률을 참고하여 인스턴스 메모리 사용률을 확인합니다. 인스턴스 메모리 사용률이 정상이라면 다음 단계를 실행합니다.

2. 로그 오류 보고 fork: Cannot allocate memory를 참고하여 프로세스 수가 제한을 초과하는지 확인합니다. 초과하지 않는다면 다음 단계를 실행합니다.
3. CVM에 로그인한 후 다음 명령어를 실행해 `min_free_kbytes` 값을 조회합니다.

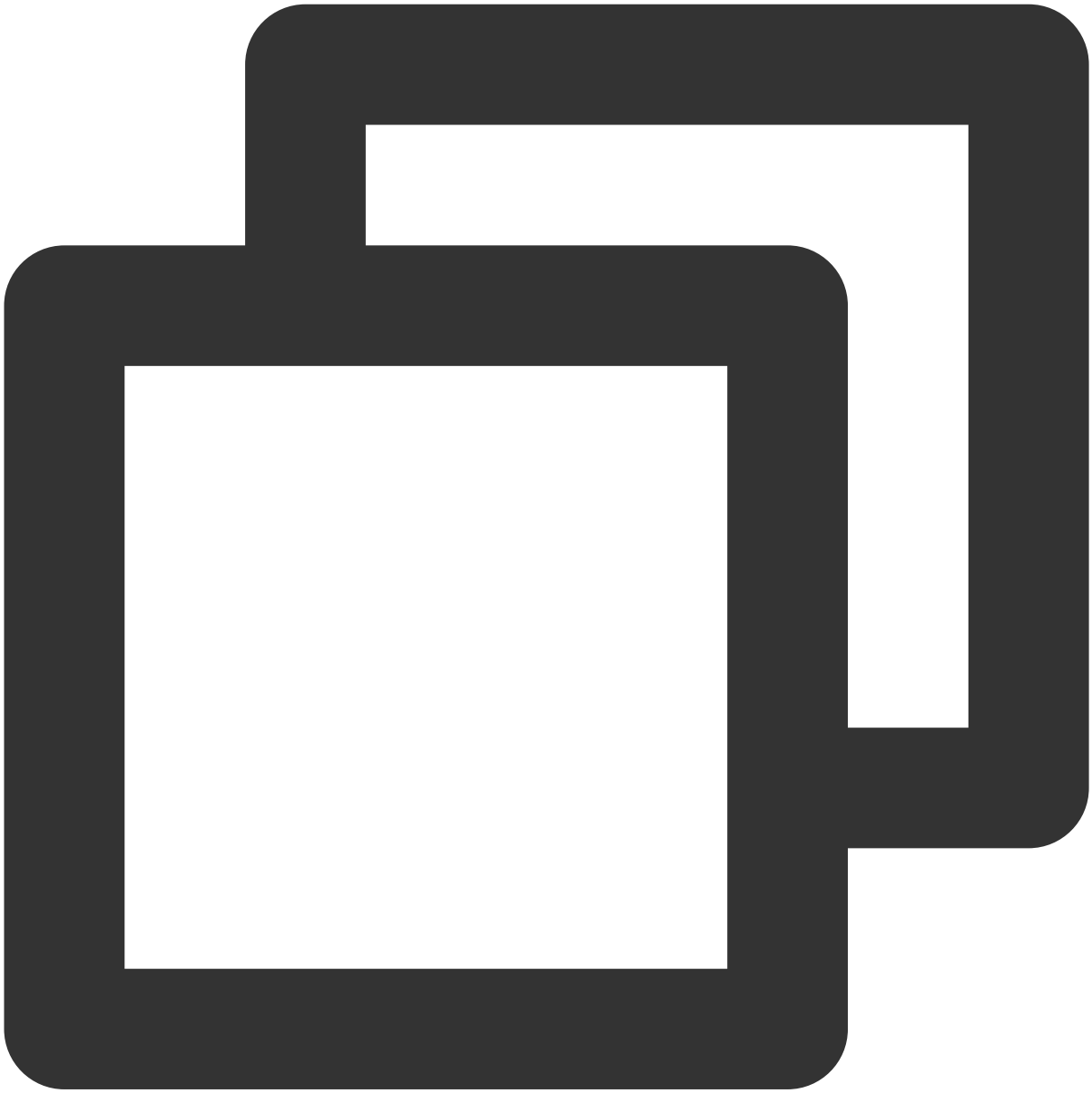


```
sysctl -a | grep min_free
```

`min_free_kbytes` 값의 단위는 kbytes입니다. 다음과 같이 `min_free_kbytes = 1024000` 으로 1GB입니다.

```
[root@ ]# sysctl -a | grep min_free
vm.min_free_kbytes = 1024000
```

4. 다음 명령어를 실행하여 VIM 편집기로 `/etc/sysctl.conf` 구성 파일을 엽니다.

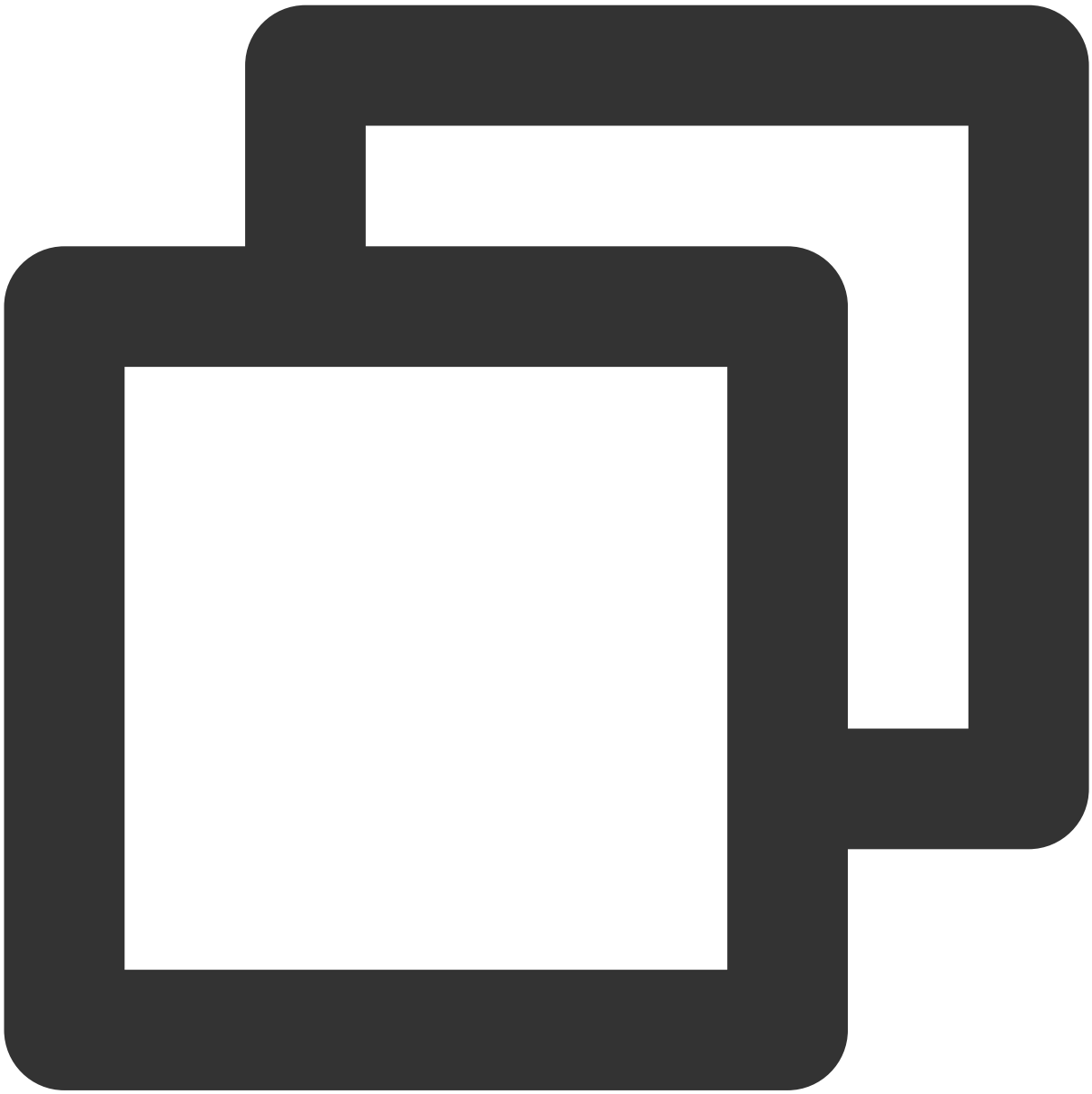


```
vim /etc/sysctl.conf
```

5. **i**를 눌러 편집 모드로 전환한 다음 `vm.min_free_kbytes` 설정 항목을 수정합니다. 해당 설정 항목이 존재하지 않는 경우 구성 파일에 직접 추가할 수 있습니다.

설명： `vm.min_free_kbytes` 값을 전체 메모리의 1% 이하로 수정할 것을 권장합니다.

6. **Esc**를 누르고 **:wq**를 입력한 다음, **Enter**를 눌러 저장하고 VIM 편집기를 종료합니다.
7. 아래의 명령어를 실행하여 설정을 활성화합니다.



```
sysctl -p
```

네트워크 관련 장애
글로벌 링크 딜레이

최종 업데이트 날짜: : 2024-02-02 11:09:47

문제 설명

북미 리전 클라우드 서버 로그인 지연 시간이 너무 깁니다.

문제 분석

전국의 국제 라우팅 엑시트가 적고 그 외 다른 이유로 인하여 동시 발생 횟수가 많을 때, 국제 링크가 꽉 차서 액세스가 불안정하게 됩니다. Tencent Cloud는 이 상황을 ISP에 피드백했습니다.
현재, 북미 리전 클라우드 서버를 구매했을 경우, 국내에서 관리 OPS 진행이 필요하며, 홍콩 리전에서 구매한 클라우드 서버를 사용하여 귀하가 구매한 북미 리전 클라우드 서버에 중계하여 로그인함으로써 이 문제를 해결할 수 있습니다.

해결 솔루션

1. 홍콩 리전의 Windows 클라우드 서버를 구매하여 “점프 서버”로 사용하십시오.
주의사항 :
“사용자 정의 구성” 페이지의 “1. 리전 및 모델 선택”에서 [홍콩] 리전을 선택하십시오.
여기를 클릭하여 구매 진행 >>
Windows 클라우드 서버는 북미 리전의 Windows 및 Linux 클라우드 서버에 로그인을 지원하며 구매를 추천합니다.
홍콩 리전의 Windows 클라우드 서버를 구매할 경우, 최소 1Mbps의 대역폭을 구매해야 하며, 그렇지 않으면 점프 서버 로그인이 불가능합니다.
2. 구매 완료 후, 필요에 따라 중국 리전 Windows 클라우드 서버 로그인 방식을 선택하십시오:
RDP 파일로 Windows 클라우드 서버에 로그인
원격 데스크톱 연결로 Windows 클라우드 서버에 로그인
VNC로 Windows 클라우드 서버에 로그인
3. 홍콩 리전의 Windows 클라우드 서버 내에서 필요에 따라 북미 리전 클라우드 서버 로그인 방식을 선택하십시오.
북미 리전의 Linux 클라우드 서버 로그인하기
표준 로그인 방식으로 Linux 클라우드 서버에 로그인
원격 로그인 소프트웨어로 Linux 클라우드 서버에 로그인
VNC로 Linux 클라우드 서버에 로그인

북미 리전의 Windows 클라우드 서버에 로그인하기
RDP 파일로 Windows 클라우드 서버에 로그인
원격 데스크톱 연결로 Windows 클라우드 서버에 로그인
VNC로 Windows 클라우드 서버에 로그인

사이트 방문 불가

최종 업데이트 날짜: : 2024-02-02 11:09:47

본 문서는 웹 사이트 액세스 오류를 야기하는 문제를 찾아 해결하는 방법에 대해 설명합니다.

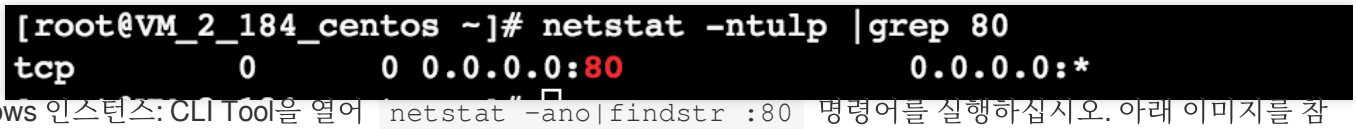
예상 원인

웹 사이트 문제, 방화벽 설치, 서버 과부하 등 원인이 웹 사이트에 액세스하지 못하게 합니다.

장애 처리

서버 관련 문제 점검

서버 종료, 하드웨어 고장, CPU/메모리/대역폭 사용률이 너무 높으면 웹 사이트에 액세스하지 못할 수 있으므로 서버의 작동 상태, CPU/메모리/대역폭 사용을 차례로 조사하는 것을 권장합니다.
1. CVM 콘솔에 로그인하여 인스턴스 관리 페이지에서 인스턴스의 정상 실행 여부를 확인하십시오. 아래 이미지를 참조하십시오.
해당되는 경우 2단계를 실행하십시오.
해당되지 않는 경우 CVM 인스턴스를 재시작하십시오.
2.
인스턴
스의 ID/인스턴스 이름을 클릭해 인스턴스 상세 페이지로 진입하십시오.
3. [모니터링]탭을 선택하여 CPU/메모리/대역폭 사용 현황을 조회하십시오. 아래 이미지를 참조하십시오.
CPU/메모리가 사용량이 너무 많은 경우 Windows 인스턴스: CPU와 메모리의 높은 점유율로 인한 로그인 불가와 Linux 인스턴스: CPU와 메모리의 높은 점유율로 인한 검색 불가를 참조하십시오.
대역폭이 사용량이 너무 많은 경우 대역폭의 높은 점유율로 인한 로그인 불가 를 참조하십시오.
CPU/메모리/대역폭 사용 현황이 정상이라면 4단계를 수행하십시오.
4.
다음
 명령어를 실행하여 웹서비스에 대응하는 포트가 제대로 모니터링되는지 점검합니다.
설명：
다음 작업은 HTTP 서버에 자주 사용하는 80 포트를 예시로 합니다.
Linux 인스턴스: `netstat -ntulp |grep 80` 명령어를 실행하십시오. 아래 이미지를 참조하십시오.



Windows 인스턴스: CLI Tool을 열어 `netstat -ano|findstr :80` 명령어를 실행하십시오. 아래 이미지를 참조하십시오.

포트가 정상적으로 모니터링될 경우 5단계를 실행하십시오.

포트가 정상적으로 모니터링되지 않을 경우 웹서비스 프로세스가 시작하거나 제대로 설정되었는지 점검하십시오.

5.

방화벽

설치를 점검하여 웹서비스 프로세스가 대응하는 포트를 내보내는지 확인하십시오.

Linux 인스턴스: `iptables -vnL` 명령어를 실행하여 iptables가 80 포트를 열 수 있는지 조회하십시오.

80 포트가 이미 열려있는 경우 네트워크 관련 문제 점검 하십시오.

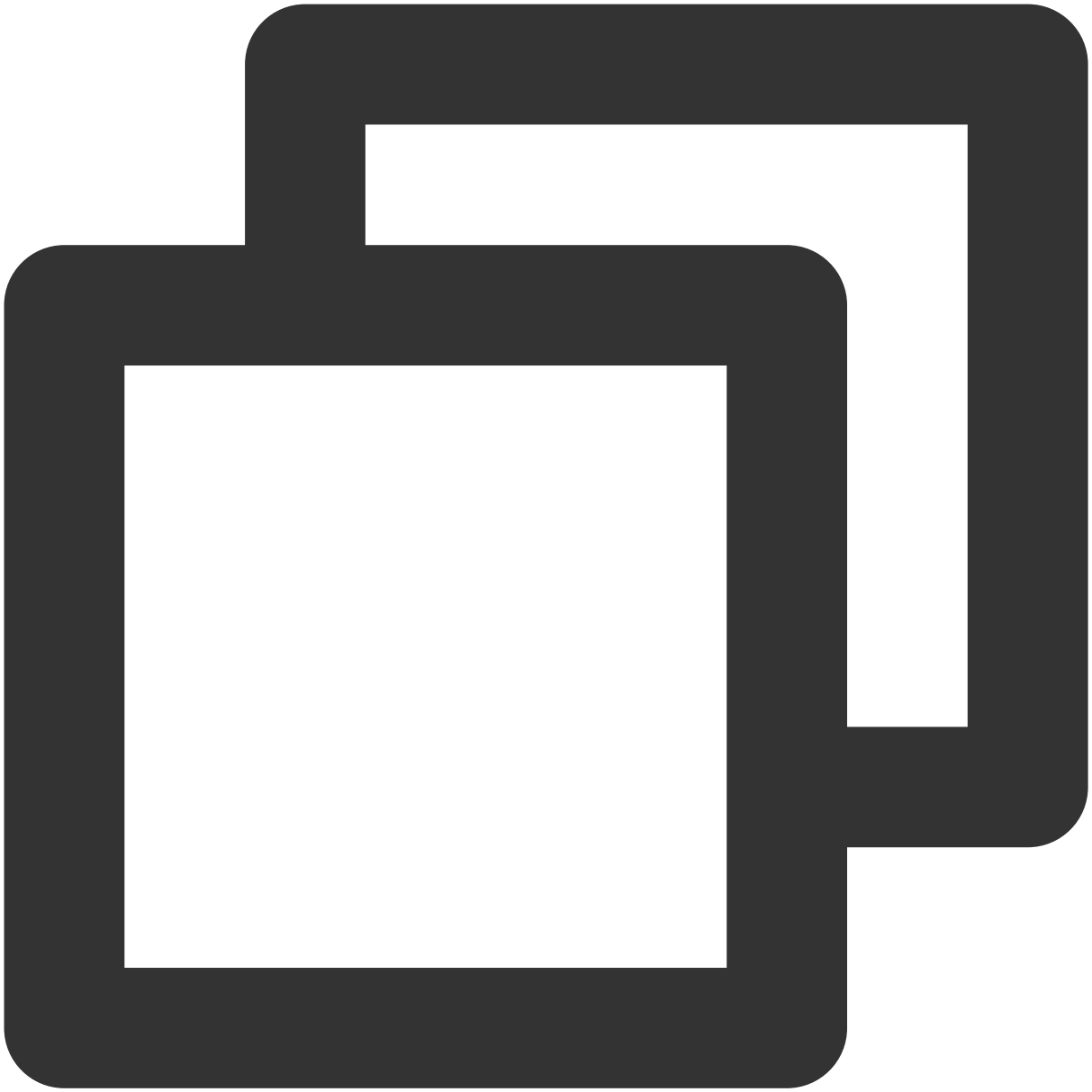
80 포트가 열리지 않은 경우 `iptables -I INPUT 5 -p tcp --dport 80 -j ACCEPT` 명령어를 실행하여 80 포트를 여십시오.

Windows 인스턴스: 운영 체제 인터페이스에서 [시작]>[제어판]>[방화벽 설치]를 클릭하여 Windows 방화벽이 해제되어 있는지 조회하십시오.

- 해제 상태인 경우 네트워크 관련 문제 점검 하십시오.
- 미해제 상태인 경우 방화벽 상태를 해제하십시오.

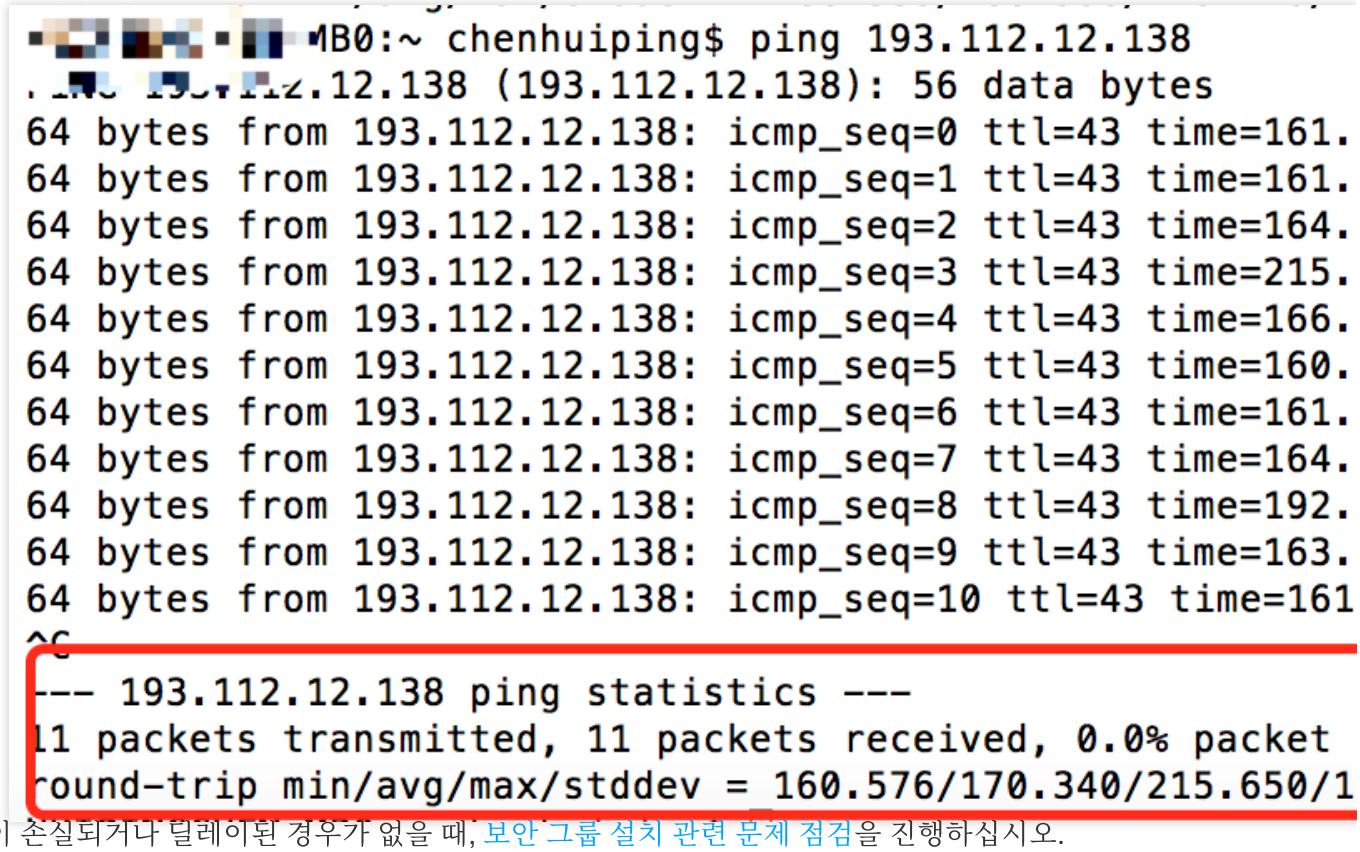
네트워크 관련 문제 점검

네트워크 관련 문제가 웹사이트를 액세스하지 못하게 할 수도 있으므로, 다음 명령어를 실행하여 네트워크가 패킷을 손실하거나 딜레이된 경우가 없는지 점검하십시오.



```
ping 타깃 서버의 공인 IP
```

다음과 유사한 결과로 리턴하면 패킷이 손실되거나 딜레이가 있는 경우가 있음을 나타내므로 MTR을 사용하여 추가적인 점검을 수행하십시오. 자세한 내용은 CVM 네트워크 딜레이와 패킷 손실을 참조하십시오.



패킷이 손실되거나 릴레이된 경우가 없을 때, 보안 그룹 설치 관련 문제 점검을 진행하십시오.

보안 그룹 설정 관련 문제 점검

보안 그룹은 가상 방화벽으로, 연결된 인스턴스의 인바운드 트래픽과 아웃바운드 트래픽을 제어할 수 있습니다. 보안 그룹의 규칙은 프로토콜, 포트, 정책 등을 지정할 수 있습니다. Web 프로세스와 관련된 포트를 열지 않은 경우에도 웹 사이트에 액세스하지 못하게 할 수 있습니다.

1. CVM 콘솔에 로그인하십시오. "인스턴스 리스트" 페이지에서 인스턴스의 ID/인스턴스 이름을 클릭하여 인스턴스 상세 페이지로 진입하십시오.
2. [보안 그룹] 탭을 선택하여 바인딩된 보안 그룹 및 대응 보안 그룹의 아웃바운드와 인바운드 규칙을 조회하고 Web 프로세스와 관련된 포트가 열려 있는지 확인하십시오. 아래 이미지를 참조하십시오.

포트가 열린 경우 도메인, ICP비안 및 분석 관련 문제 점검하십시오.
포트가 닫힌 경우 보안 그룹 설치를 수정하여 Web 프로세스와 관련된 포트를 여십시오.

도메인, ICP비안과 분석 관련 문제 점검

서버 관련 문제, 네트워크 관련 문제 및 보안 그룹 설치 관련 문제를 조회한 뒤, CVM의 공인 IP 주소를 사용하여 액세스를 시도할 수 있습니다. IP 주소를 사용하여 액세스가 가능하지만 도메인 액세스에 실패하면 도메인 ICP비안 또는 분석 관련 문제로 인해 웹 사이트에 액세스하지 못한 것일 수 있습니다.

1. 국가 공업정보부는 허가를 받지 않았거나 ICP비안 절차를 밟지 않은 네트워크에 대해 인터넷 정보 서비스를 제공할 경우 위법 행위로 간주합니다. 네트워크의 정상적인 실행을 위해 먼저 ICP비안을 실행하고 네트워크를 구축하는 것을 권장합니다. ICP비안을 성공적으로 실행한 후 통신관리국에서 전달한 ICP비안 번호를 획득해야 액세스를 활성화할 수 있습니다.

도메인에 ICP비안이 없을 경우 도메인 ICP비안을 실행하십시오.
Tencent Cloud의 도메인 서비스를 사용할 경우 도메인 관리 콘솔에 로그인하여 해당하는 도메인 이름 상황을 조회할 수 있습니다.
도메인이 이미 ICP비안에 등록된 경우 2단계를 실행하십시오.
2.
분석
효과 관련 을 참조하여 분석 관련 문제를 점검하십시오.
웹 사이트 액세스 문제를 해결한 경우 작업을 완료합니다.
여전히 웹 사이트 액세스 문제를 해결할 수 없을 경우 티켓 제출을 통해 피드백하십시오.

사이트 방문 렉걸림

최종 업데이트 날짜: : 2024-02-02 11:09:48

문제 설명

웹 사이트 액세스가 느림

문제 분석

완전한 HTTP 요청은 도메인 이름 확인, TCP 연결 구성, 요청 전송, 서버가 요청을 수신하고 처리하고 처리 결과 리턴하는 것, 브라우저가 HTML 코드를 해석하고 다른 리소스 요청하고 페이지에 렌더링을 진행하는 것도 포함합니다. 이 중 HTTP 요청 프로세스는 사용자의 로컬 클라이언트, 클라이언트에서 액세스 서비스 사이의 네트워크 노드 및 서버를 거칩니다. 3개 링크 중 1개 링크에 문제가 생기면 네트워크 액세스가 느려질 수도 있습니다.

해결 방법

로컬 클라이언트 조회

1. 로컬 클라이언트를 통해 전문가 진단 분석 시스템에 액세스하여 각 도메인의 로컬 액세스 속도를 테스트하십시오.
2. 테스트 결과에 따라 로컬 네트워크에 문제가 있는지 확인하십시오.
예를 들어 테스트 결과가 아래와 같을 경우에 이미지를 참조하십시오.

The following are the test results of Tencent's domain name.	
inews.qq.com	Normal network , 194 milliseconds delay
www.qq.com	Normal network , 128 milliseconds delay
3g.qq.com	Normal network , 140 milliseconds delay
mail.qq.com	Normal network , 99 milliseconds delay
user.qzone.qq.com	Normal network , 98 milliseconds delay
r.qzone.qq.com	Normal network , 203 milliseconds delay
w.qzone.qq.com	Normal network , 188 milliseconds delay
ptlogin2.qq.com	Normal network , 96 milliseconds delay
check.ptlogin2.qq.com	Normal network , 189 milliseconds delay
ui.ptlogin2.qq.com	Normal network , 91 milliseconds delay
i.mail.qq.com	Normal network , 129 milliseconds delay
v.qq.com	Normal network , 129 milliseconds delay

The following are the test results of other's domain name.	
c.3g.163.com	Normal network , 143 milliseconds delay
weibo.com	Normal network , 211 milliseconds delay
www.baidu.com	Normal network , 94 milliseconds delay
www.sina.com.cn	Normal network , 138 milliseconds delay
www.taobao.com	Normal network , 136 milliseconds delay

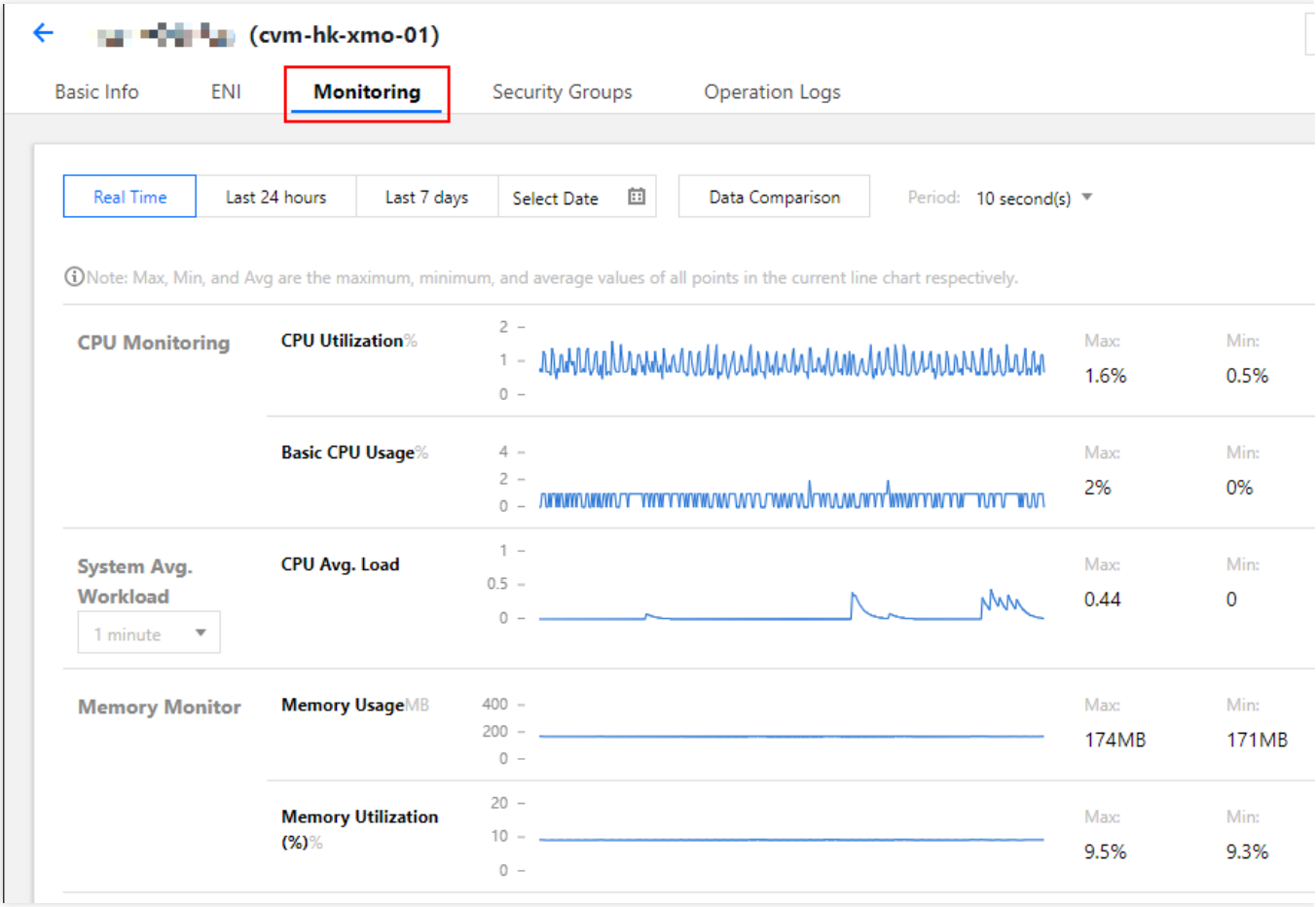
우리는 결과를 통해 각 도메인에 액세스할 때의 딜레이 시간, 네트워크 정상 여부를 확인할 수 있습니다.
비정상일 경우 네트워크 서비스 공급자에 연락하여 해결하십시오.
정상일 경우 네트워크 링크 점검을 진행하십시오.

네트워크 링크 점검

1. 로컬 클라이언트를 ping 서버 공인 IP를 통해 패킷이 손실되거나 딜레이 시간이 긴 경우가 있는지 확인하십시오.
패킷을 분실하거나 딜레이 시간이 길 경우 MTR을 사용해 진단하고, 자세한 내용은 서버 네트워크 지연과 패킷 손실 처리를 참조하십시오.
패킷을 손실하지 않거나 딜레이 시간이 길지 않을 경우 2단계를 실행하십시오.
2. `dig/nslookup` 명령어
를 사용하여 DNS 분석 현황을 점검하고 DNS 분석으로 인한 문제인지 점검하십시오.
공인 IP를 직접 사용하여 해당 페이지에 액세스하여 DNS가 웹 사이트에 액세스가 느려지는 현상을 유발하는지 여부를 확인할 수 있습니다.
해당되는 경우 DNS 분석을 점검하고 자세한 내용은 분석 활성화 관련 을 참조하십시오.
해당되지 않을 경우 서버 점검을 하십시오.

서버 점검

1. CVM 콘솔에 로그인합니다.
2. 점검 대기 중인 인스턴스 ID/인스턴스 이름을 선택하여 해당 인스턴스 상세 페이지로 이동하십시오.
3. 인스턴스 상세 페이지에서 [모니터링]탭을 선택하여 인스턴스 리소스의 사용 현황을 조회하십시오. 아래 이미지를 참조하십시오.



CPU/메모리가 사용량이 너무 많은 경우 Windows 인스턴스: CPU와 메모리의 높은 점유율로 인한 로그인 불가와 Linux 인스턴스: CPU와 메모리의 높은 점유율로 인한 검색 불가를 참조하십시오.
대역폭이 사용량이 너무 많은 경우 대역폭의 높은 점유율로 인한 로그인 불가 를 참조하십시오.
인스턴스 리소스가 정상적으로 사용되고 있다면 기타 문제 점검을 하십시오.

기타 문제 점검

인스턴스 리소스 사용에 따라 서버 부하로 인한 리소스 소모량 증가 여부를 판단하십시오.
소모량이 클 경우 서비스 프로세스를 최적화하거나 서버 구성 업그레이드를 권장합니다. 또한 새로운 서버 구매를 통하여 현재 서버의 부담을 줄일 수 있습니다.
소모량이 적을 경우 로그를 조회하여 문제를 찾아 최적화할 것을 권장합니다.

ENI 다중 큐 설정 오류 문제

최종 업데이트 날짜: : 2024-02-02 11:09:48

현상 설명

CVM ENI의 다중 큐 설정에 오류가 발생합니다.

예상 원인

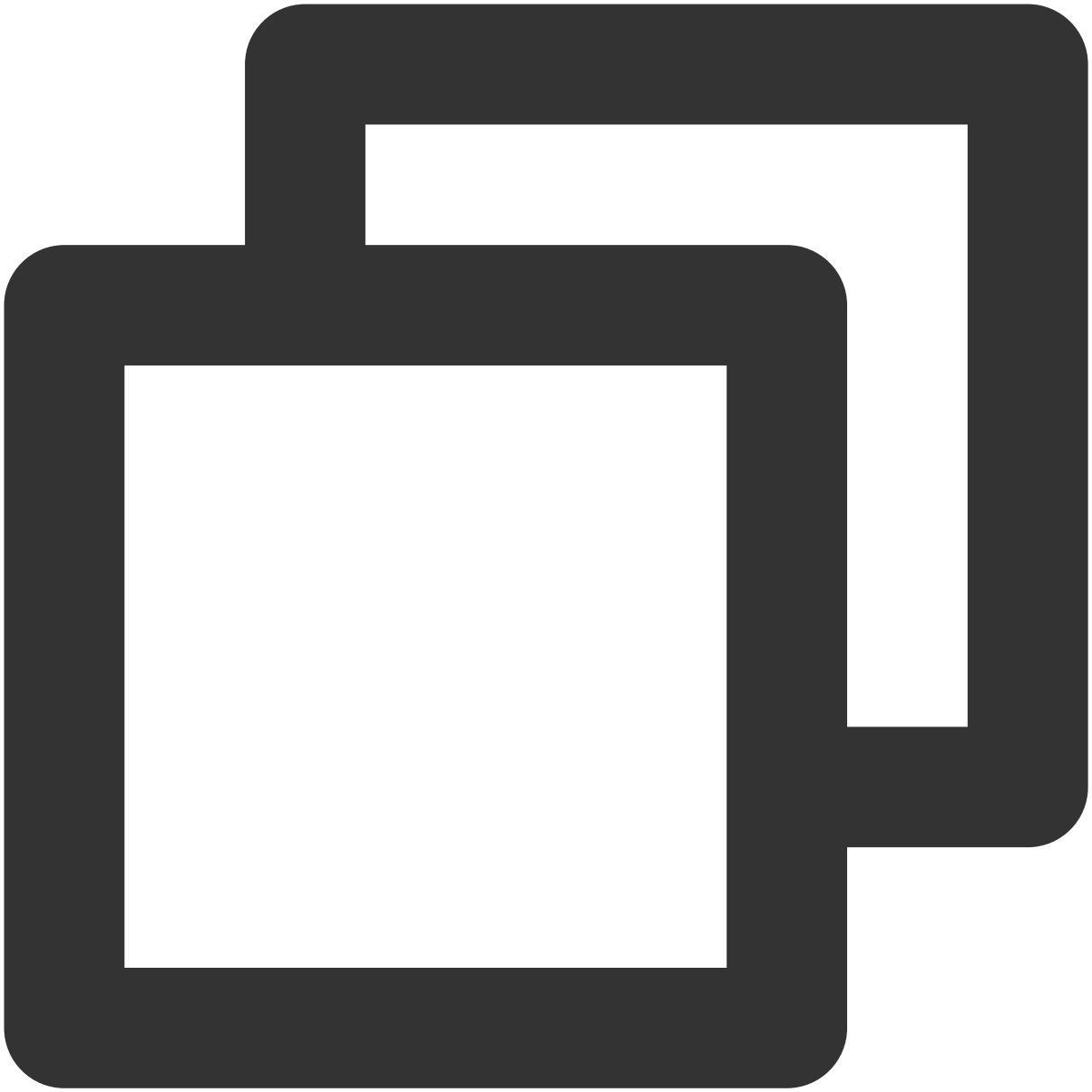
기본적으로 CVM은 ENI에 대한 여러 큐로 설정되며 이 방법은 ENI 중단을 서로 다른 CPU에 분산하여 네트워크 처리 성능을 향상시킬 수 있습니다. 수정 시 ENI의 다중 큐 설정에 오류가 발생할 수 있습니다.

해결 방법

처리 단계를 참고하여 ENI 큐 수를 수정합니다.

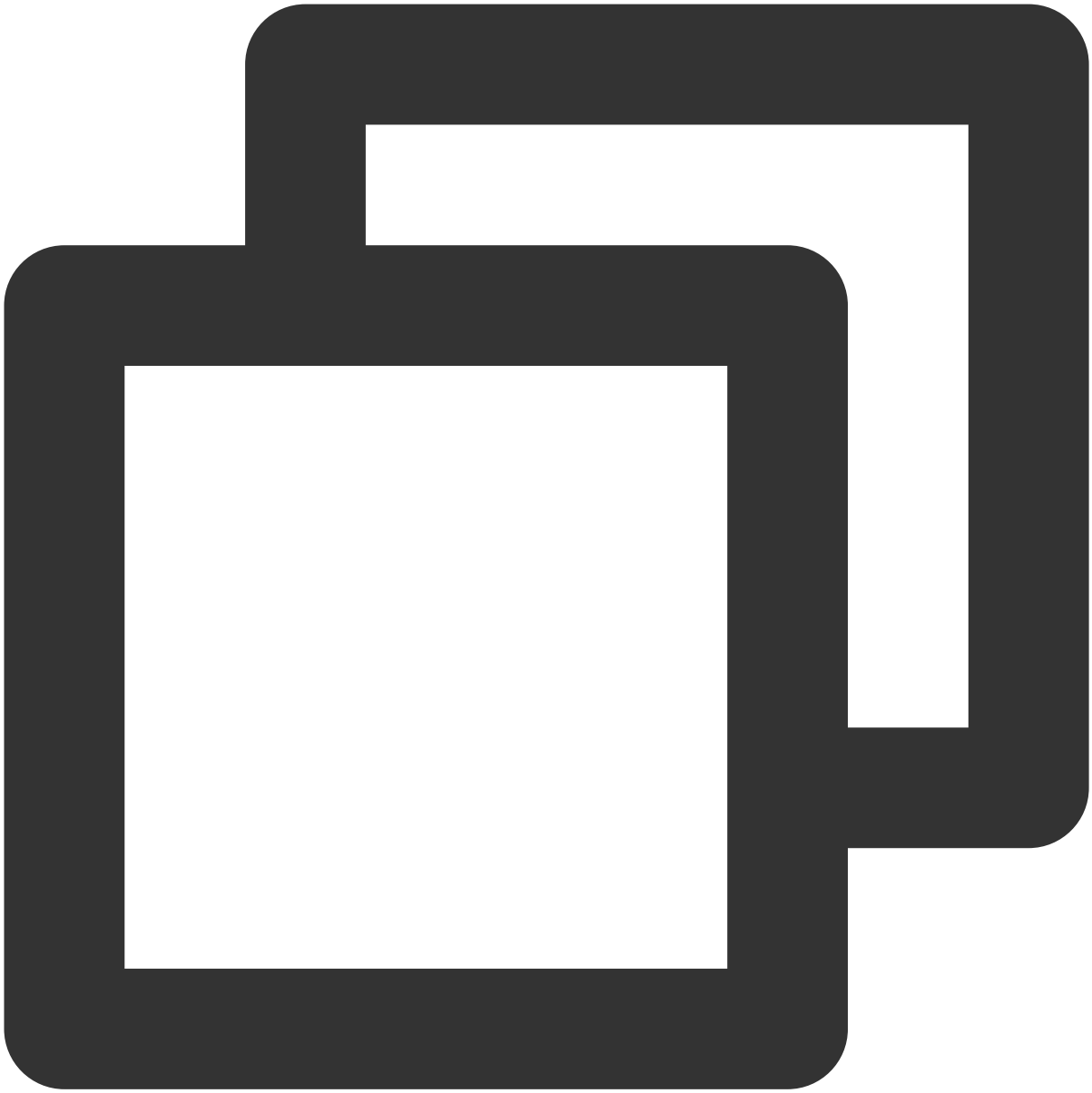
처리 단계

다음 단계에서 CVM의 기본 주 ENI는 'eth0'이고 ENI 큐의 수는 2입니다.
1. 다음 명령을 실행하여 현재 ENI 큐 수를 확인합니다.



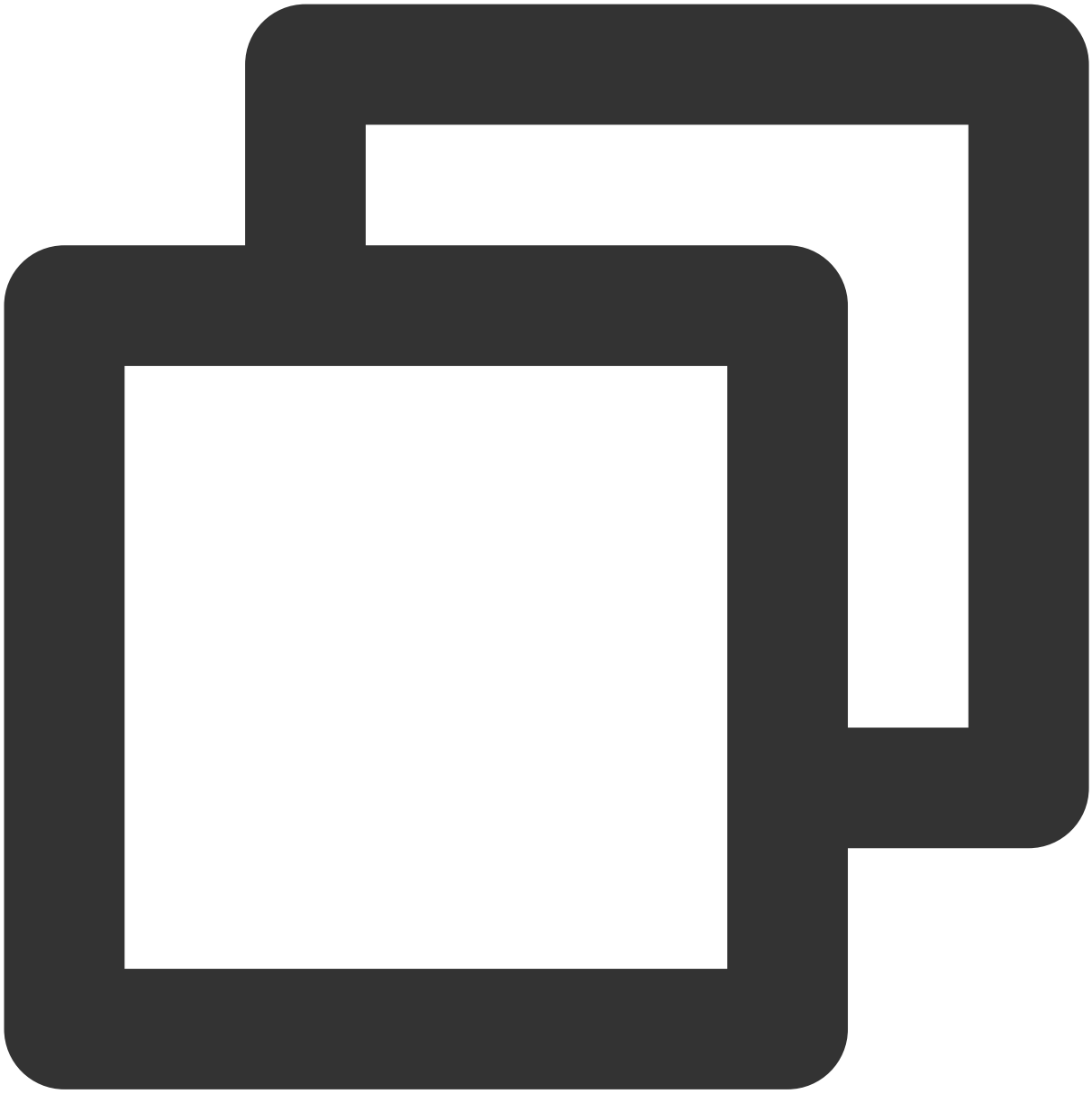
```
ethtool -l eth0
```

다음 결과가 반환되면, 현재 큐 수가 최대 ENI 큐 수보다 작게 설정되어 있는 것입니다. 설정이 비합리적이므로 수정이 필요합니다.



```
Channel parameters for eth0:
Pre-set maximums:
RX:             0
TX:             0
Other:          0
Combined:       2         ### 서버에서 지원하는 최대 ENI 큐 수
Current hardware settings:
RX:             0
TX:             0
Other:          0
Combined:       1        ###현재 설정된 ENI 큐 수
```

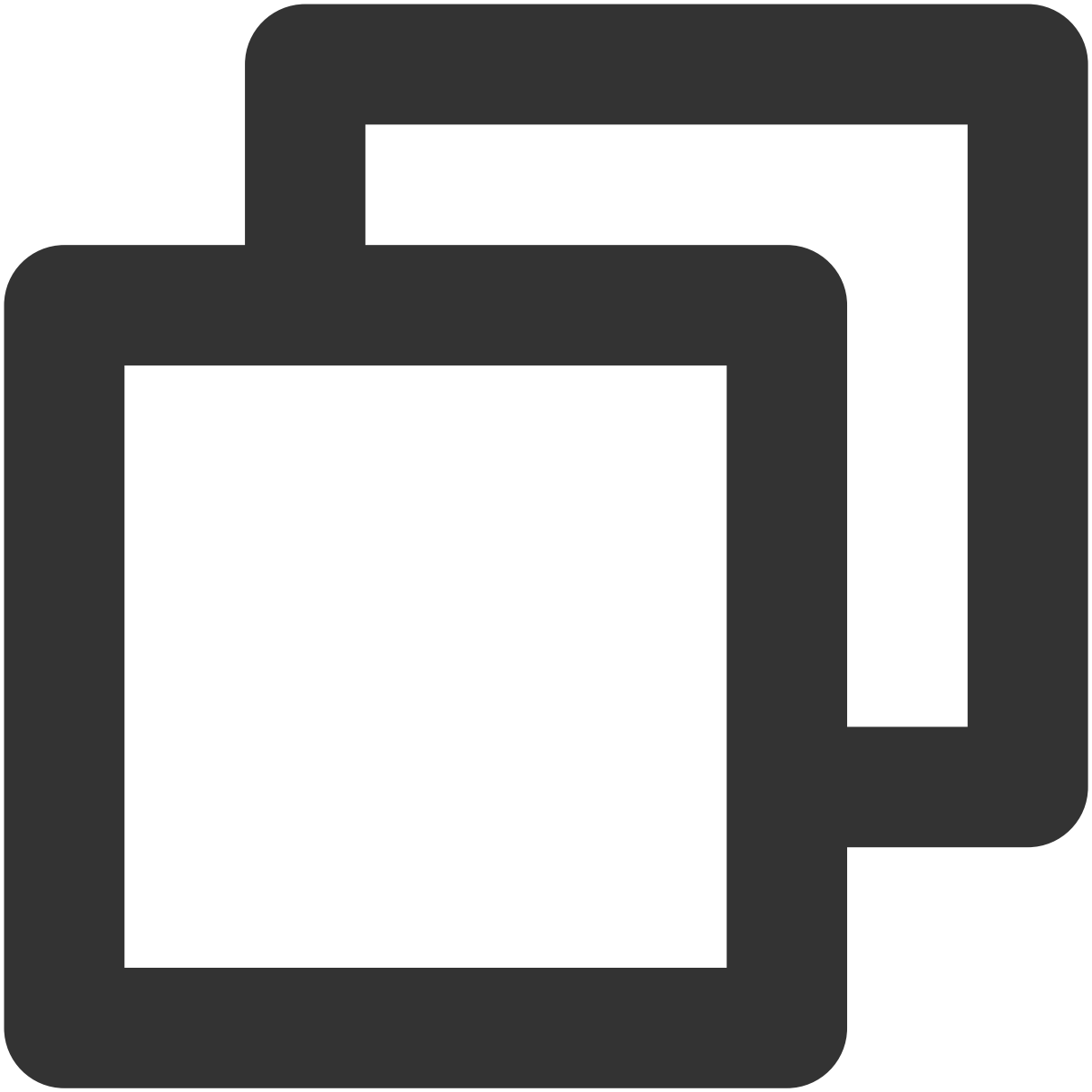
2. 다음 명령을 실행하여 현재 ENI 큐 수를 설정합니다.



```
ethtool -L eth0  combined 2
```

명령어의 큐 개수는 2로 설정하며, 실제 상황에 따라 조정할 수 있습니다. 설정값은 서버에서 지원하는 ENI 큐의 최대 개수입니다.

3. 다음 명령을 실행하여 ENI 큐 수의 현재 설정을 확인합니다.



```
ethtool -l eth
```

서버에서 지원하는 최대 ENI 큐 수는 현재 설정된 ENI 큐 수와 같으므로 설정이 완료됩니다.

CVM 네트워크 대기 시간 및 패킷 손실

최종 업데이트 날짜: : 2024-02-02 11:09:47

문제 설명

로컬 컴퓨터가 CVM에 액세스하거나 CVM에서 기타 네트워크 리소스에 액세스 할 때 네트워크 랙을 발견합니다. `ping` 명령어를 사용하여 네트워크 패킷 존재 또는 비교적 긴 딜레인 시간이 있는지 확인합니다.

문제 분석

패킷 또는 긴 딜레이 시간 문제에는 백본 링크 정체, 링크 노드 장애, CVM 부하, 시스템 설정 문제 등 여러가지 원인이 있을 수 있습니다. CVM 자체 문제를 해결한 후 MTR을 사용하여 추가 진단을 받으실 수 있습니다.
MTR은 네트워크 진단 도구이며 해당 툴이 진단을 완료한 보고서는 사용자가 네트워크 문제의 핵심을 확인할 수 있도록 도와줍니다.

해결 방안

본 문서는 Linux와 Windows CVM을 예로 하며 MTR 사용 방법 및 MTR 보고서 결과에 대한 분석 진행 방법을 소개합니다.
설명 :
로컬 또는 CVM에서 Ping이 비활성화된 경우 MTR에 결과가 없습니다.
실행하는 MTR의 호스트 운영 체제에 따라 MTR 소개 및 사용법을 참고하십시오.
WinMTR 소개 및 사용(Windows 운영 체제)]
MTR 소개 및 사용(Linux 운영 체제)]
WinMTR: Windows 시스템의 무료 네트워크 진단 도구에 사용되며 Ping 과 tracert의 기능을 결합하였습니다. 그래픽 인터페이스는 시각적으로 각각의 노드의 응답 시간과 패킷 상황을 확인할 수 있게 해줍니다.

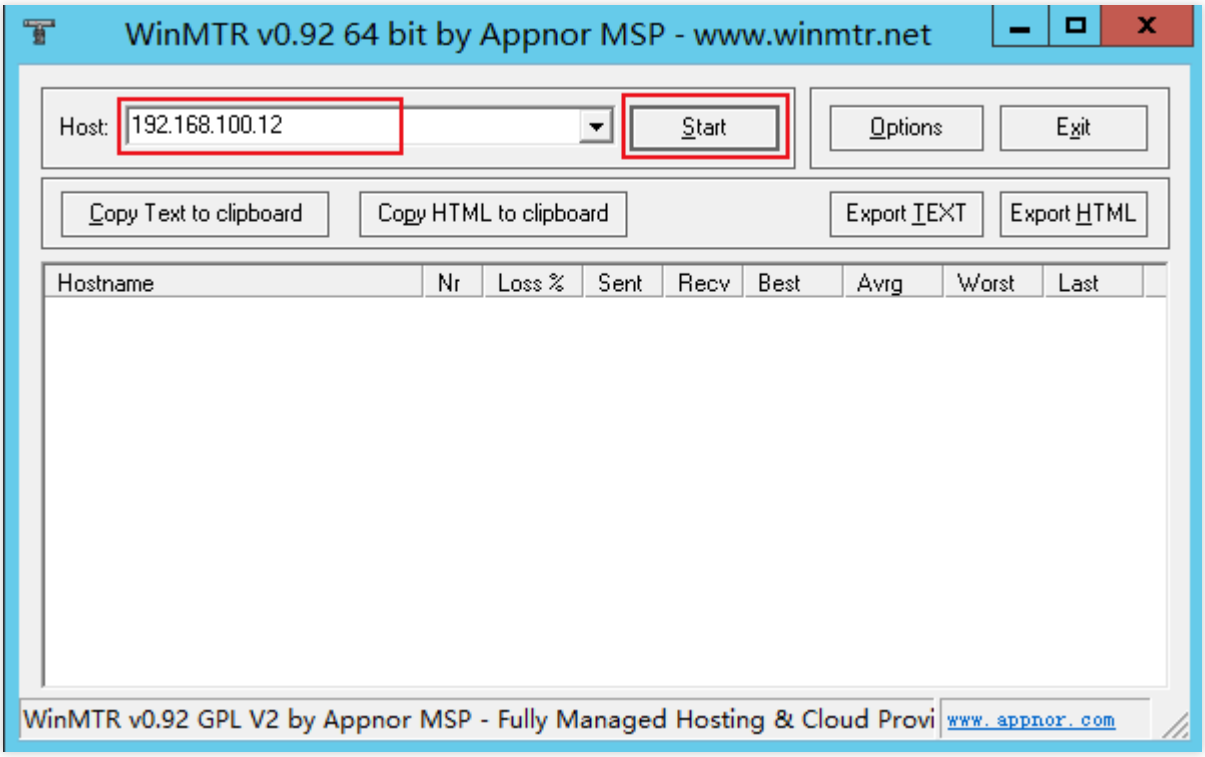
WinMTR 설치

1. Windows CVM에 로그인합니다.
2. 운영 체제 인터페이스에서 공식 웹 사이트 브라우저 액세스를 통해(또는 합법 경로) 대응하는 운영 체제 유형의 WinMTR 설치 패키지를 다운로드하십시오.
3. WinMTR 설치 패키지를 압축 해제하십시오.

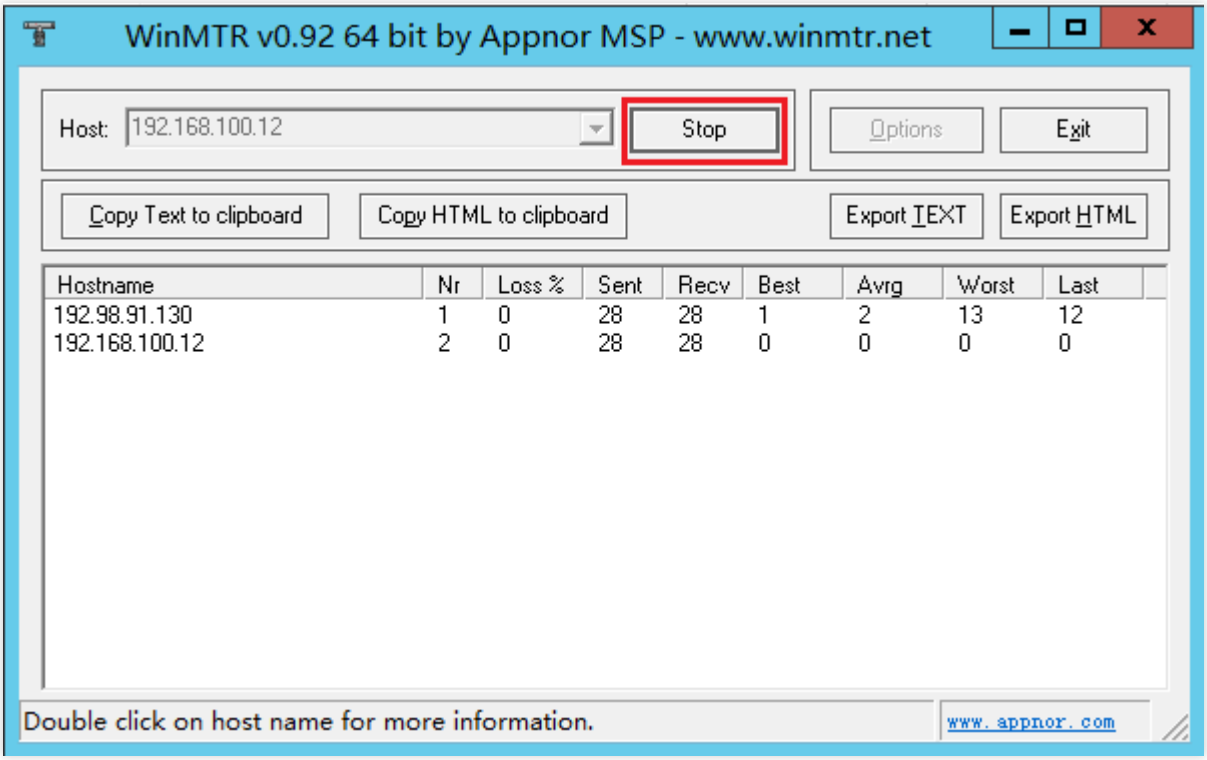
WinMTR 사용

1. WinMTR.exe를 더블 클릭하여 WinMTR 툴을 여십시오.

2. WinMTR 창의 Host에서 타깃 서버 IP 또는 도메인 이름을 입력하고 **Start**를 클릭하십시오. 아래 이미지를 참고하십시오.



3. 실제 상황에 따라 WinMTR이 잠시 실행될 때까지 기다린 뒤 **Stop**을 클릭하여 테스트를 종료하십시오. 아래 이미지를 참고하십시오.



다음은 테스트 결과 주요 정보입니다.

Hostname: 타깃 서버로 통과하는 각 호스트 IP 또는 명칭.

Nr: 노드를 통과하는 수량.

Loss%: 대응하는 노드의 패킷 손실률.

Sent: 전송된 데이터 패키지 수량.

Recv: 응답 받은 수량.

Best: 가장 짧은 응답 시간.

Avrg: 평균 응답 시간.

Worst: 가장 긴 응답 시간.

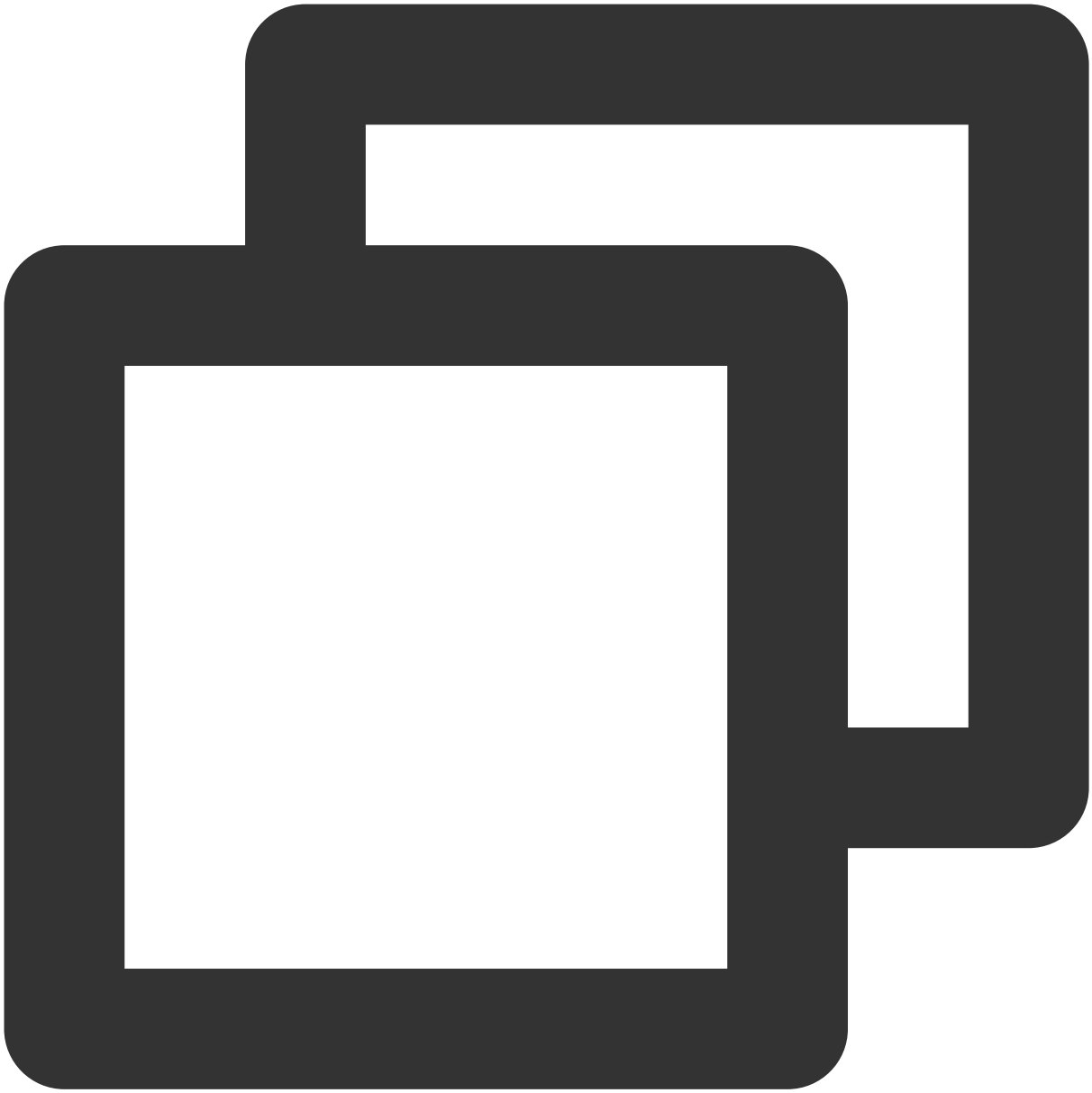
Last: 가장 최근 응답 시간.

MTR: Linux 플랫폼에서 네트워크 상태를 진단하는 도구, Ping, traceroute, nslookup의 기능을 상속하고 일반적으로 ICMP 패키지를 사용하여 두 개의 노드를 테스트하기 전의 네트워크 연결 상태입니다.

MTR 설치

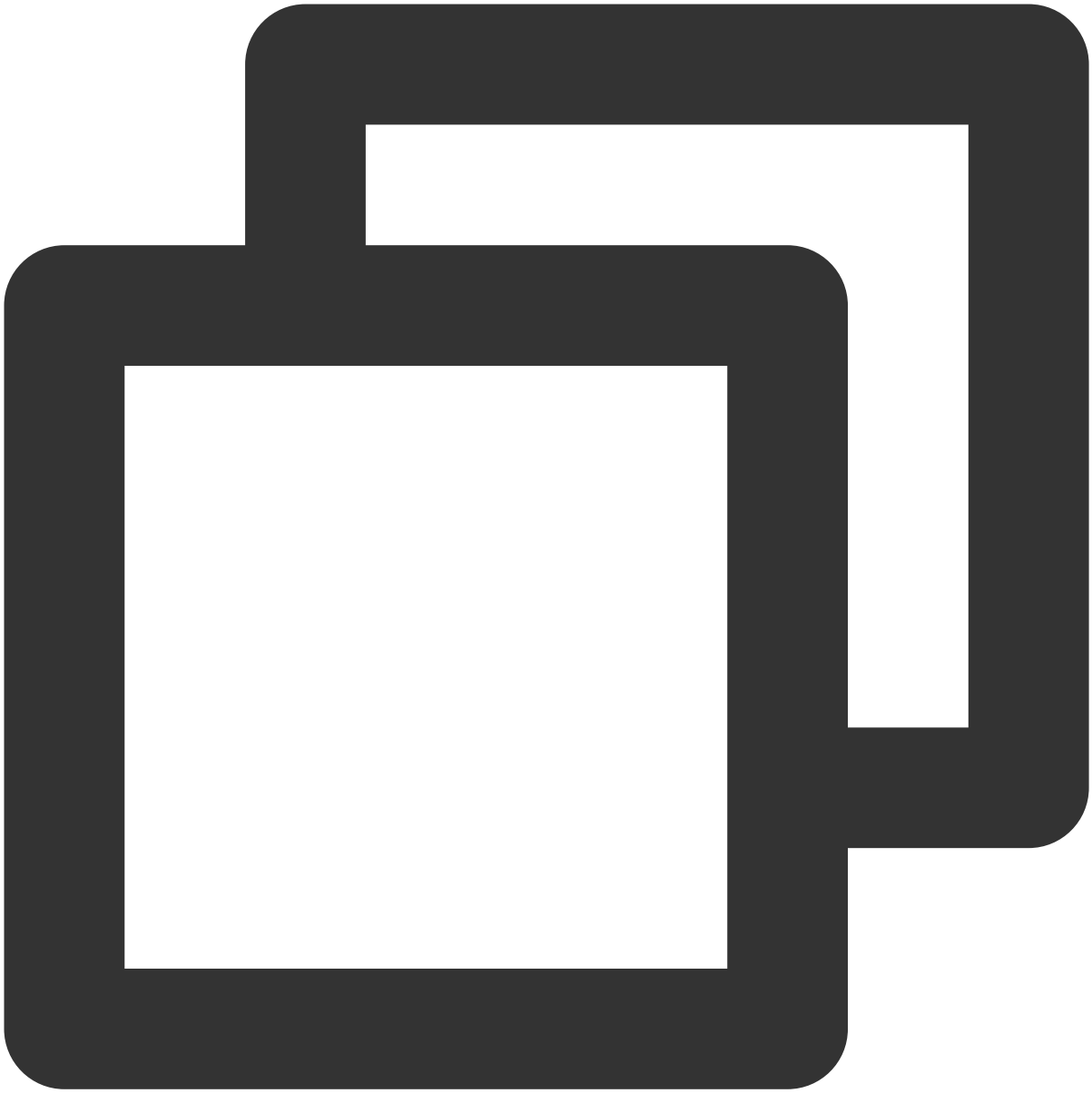
현재 Linux가 배포한 버전은 모두 MTR이 설치되어 있습니다. 사용자의 Linux CVM에 MTR이 설치되어 있지 않다면 다음 명령어를 통해 설치를 진행할 수 있습니다.

CentOS 운영 체제:



```
yum install mtr
```

Ubuntu 운영 체제:



```
sudo apt-get install mtr
```

MTR 관련 파라미터 설명

-h/--help: 도움말 메뉴 표시

-v/--version: MTR 버전 정보 표시

-r/--report: 보고서 형식의 결과 출력

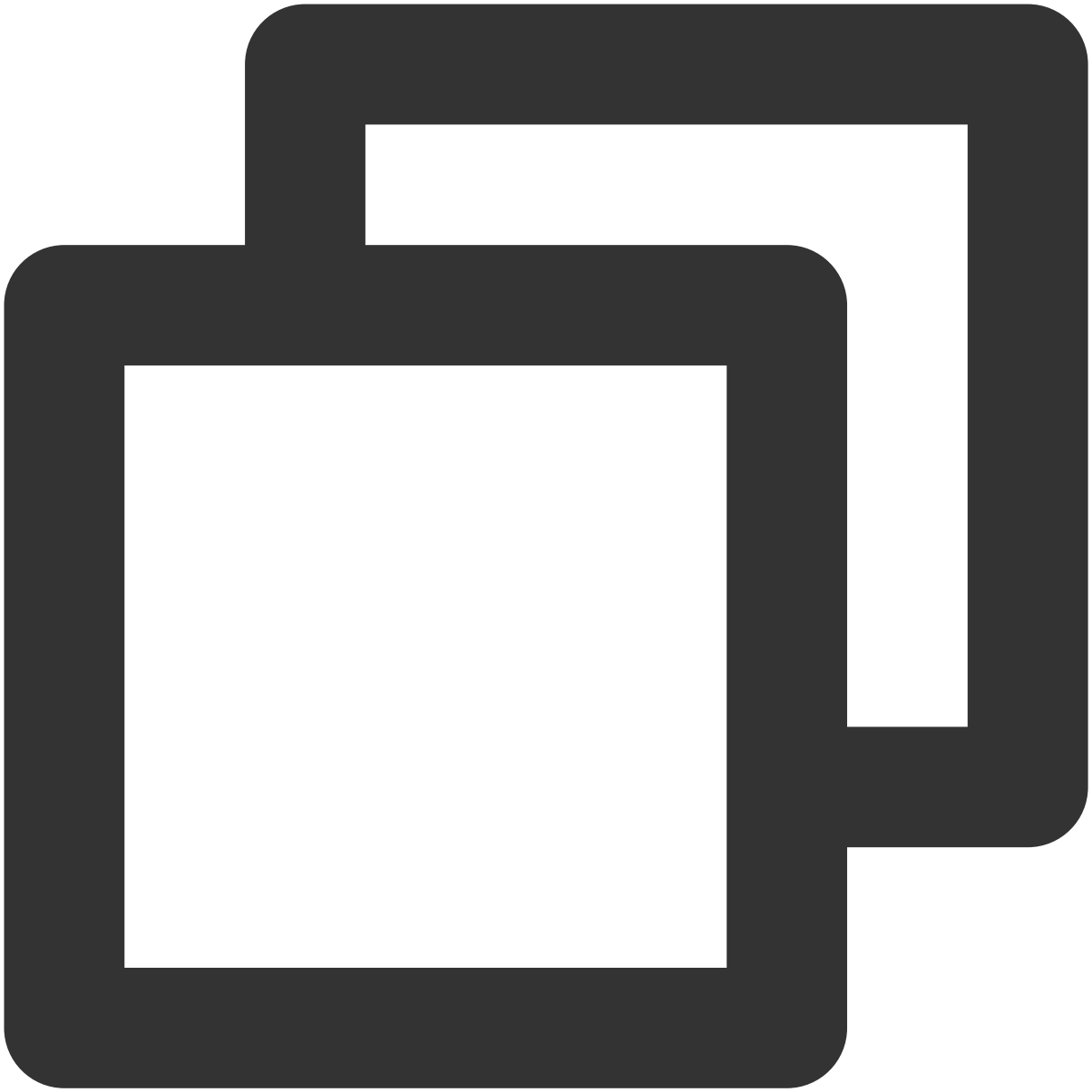
-p/--split: **--report**와 상대적으로 매 회 추적 결과를 각각 나열

-c/--report-cycles: 초당 전송되는 데이터 패키지 수량 설정, 기본값 10

-s/--psize: 데이터 패키지 크기 설정
-n/--no-dns: IP 주소에 대해서 도메인 이름 확인을 진행하지 않음
-a/--address: 사용자가 데이터 패키지의 IP 주소 전송을 설정하고 주요 사용자의 단일 서버에 여러개의 IP 주소가 있는 환경
-4: IPv4
-6: IPv6

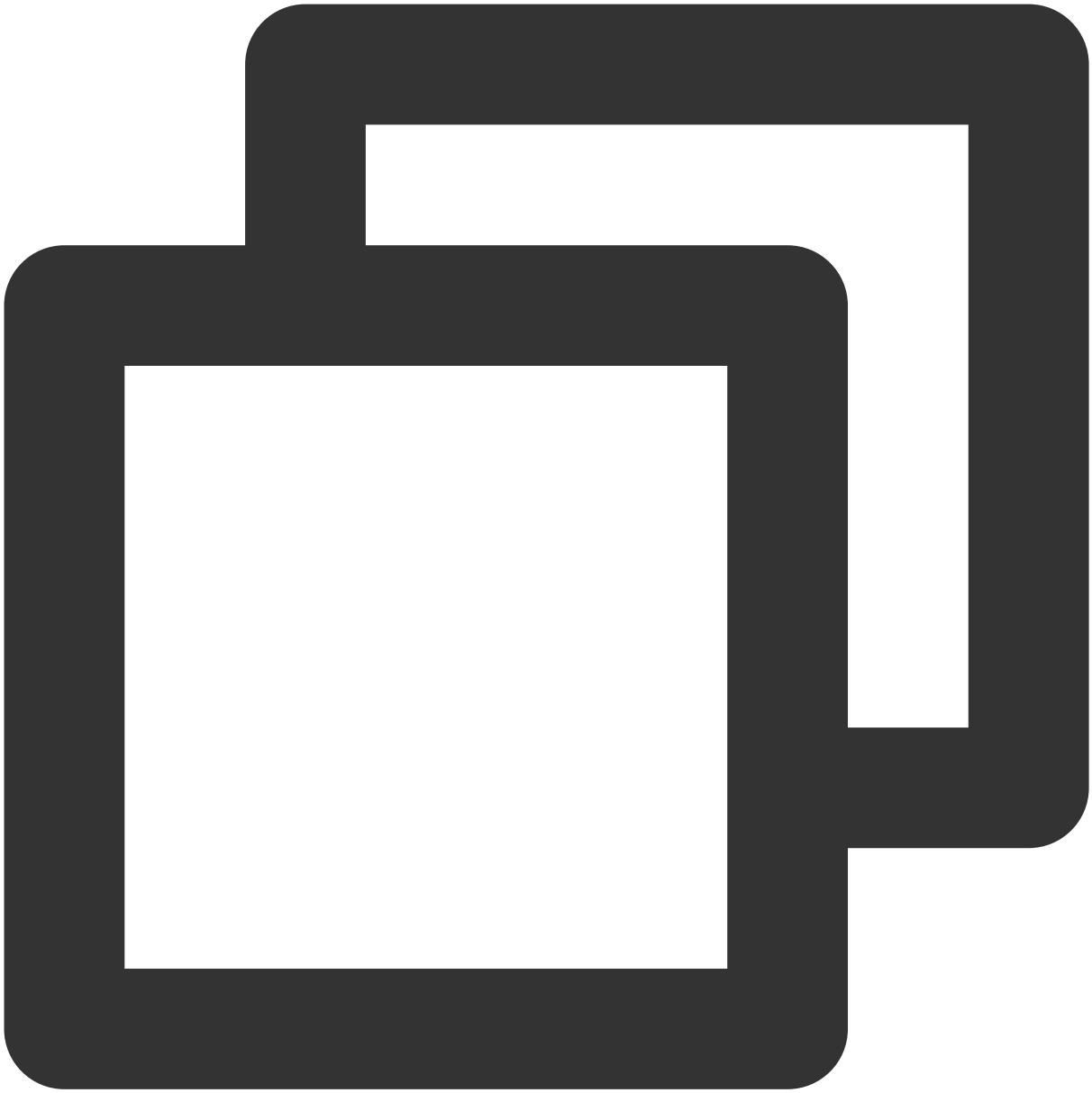
사용 예시

로컬 컴퓨터의 IP가 119.28.98.39인 Virtual Machine을 예로 합니다.
다음 명령어를 실행하여 보고서 형식의 MTR의 진단 보고서를 확인하십시오.



```
mtr 119.28.98.39 --report
```

다음과 유사한 정보가 반환됩니다.



```
[root@VM_103_80_centos ~]# mtr 119.28.98.39 --report
Start: Mon Feb  5 11:33:34 2019
HOST:VM_103_80_centos           Loss%   Snt   Last   Avg  Best  Wrst StD
1.|-- 100.119.162.130            0.0%    10    6.5   8.4   4.6  13.7   2
2.|-- 100.119.170.58             0.0%    10    0.8   8.4   0.6   1.1   0
3.|-- 10.200.135.213             0.0%    10    0.4   8.4   0.4   2.5   0
4.|-- 10.200.16.173              0.0%    10    1.6   8.4   1.4   1.6   0
5.|-- 14.18.199.58               0.0%    10    1.0   8.4   1.0   4.1   0
6.|-- 14.18.199.25               0.0%    10    4.1   8.4   3.3  10.2   1
7.|-- 113.96.7.214               0.0%    10    5.8   8.4   3.1  10.1   2
8.|-- 113.96.0.106               0.0%    10    3.9   8.4   3.9  11.0   2
```

```
 9.|-- 202.97.90.206               30.0%     10    2.4    8.4     2.4     2.5       0
 10.|-- 202.97.94.77                0.0%     10     3.5    4.6     3.5     7.0       1
 11.|-- 202.97.51.142               0.0%     10   164.7    8.4   161.3   165.3       1
 12.|-- 202.97.49.106               0.0%     10   162.3    8.4   161.7   167.8       2
 13.|-- ix-xe-10-2-6-0.tcore2.LVW 10.0%     10   168.4    8.4   161.5   168.9       2
 14.|-- 180.87.15.25               10.0%     10   348.1    8.4   347.7   350.2       0
 15.|-- 180.87.96.21                0.0%     10   345.0    8.4   343.4   345.0       0
 16.|-- 180.87.96.142               0.0%     10   187.4    8.4   187.3   187.6       0
 17.|-- ???                       100.0%     10     0.0    8.4     0.0     0.0       0
 18.|-- 100.78.119.231              0.0%     10   187.7    8.4   187.3   194.0       2
 19.|-- 119.28.98.39                0.0%     10   186.5    8.4   186.4   186.5       0
```

다음은 주요 출력 정보입니다.

HOST: 노드의 IP 주소 또는 도메인 이름.

Loss%: 패킷 손실률.

Snt: 초당 전송된 데이터 패키지의 수량.

Last: 가장 최근 응답 시간.

Avg: 평균 응답 시간.

Best: 가장 짧은 응답 시간.

Wrst: 가장 긴 응답 시간.

StDev: 표준 편차, 편차값이 클수록 각 데이터 패키지가 해당 노드에서의 응답 시간 차이가 큽니다.

보고서 결과 분석 및 프로세스

설명：

네트워크 비대칭으로 인해 로컬 컴퓨터에서 Virtual Machine의 네트워크 문제를 만났을 때, 양방향의 MTR 데이터(로컬 컴퓨터가 CVM로 또는 CVM이 로컬 컴퓨터로)를 수집하길 권장합니다.

1. 보고서 결과에 따라 타깃 서버 IP의 패킷 손실 여부를 확인하십시오.

패킷이 손실되지 않은 경우 네트워크가 정상임을 의미합니다.

패킷이 손실된 경우 2단계를 실행하십시오.

2. 결과 보고서를 조회하고 처음 패킷 손실된 노드를 찾습니다.

타깃 서버의 패킷 손실이 발생하면 대상 서버의 네트워크 구성이 잘못된 것이므로 타깃 서버의 방화벽 구성을 확인하십시오.

패킷 손실이 처음 3개의 홉에서 시작된 경우 일반적으로 로컬 컴퓨터 통신사 네트워크 문제일 수 있으며 기타 웹 사이트에 액세스할 때 동일한 상황의 발생 여부를 확인하십시오. 동일한 상황이 발생할 경우 ISP에 피드백을 보내 진행하십시오.

패킷 손실이 빈번하다면 실제로 네트워크가 불안정한 시나리오입니다. 상담을 위해 티켓 제출을 진행하시고, 엔지니어가 진단할 수 있도록 테스트 화면 캡처를 첨부하십시오.

CVM 네트워크 액세스 패킷 손실

최종 업데이트 날짜: : 2024-02-02 11:09:48

본문은 CVM 네트워크 액세스 패킷 손실 문제를 일으킬 수 있는 주요 원인과 문제 진단 및 솔루션을 소개합니다.

예상 원인

CVM 네트워크 액세스의 패킷 손실 문제에 대한 예상 원인은 다음과 같습니다.
속도 제한 트리거로 인한 TCP 패킷 손실
속도 제한 트리거로 인한 UDP 패킷 손실
소프트웨어 인터럽트 패킷 손실 트리거
UDP 전송 버퍼 가득 참
UDP 수신 버퍼 가득 참
TCP 완전 연결 큐 가득 참
TCP 요청 오버플로
연결 수 상한 도달
iptables policy 설정 관련 규칙

전제 조건

문제 파악 및 해결 전, 인스턴스에 로그인해야 하며, 자세한 내용은 Linux 인스턴스 로그인 및 Windows 인스턴스 로그인을 참고하십시오.

장애 처리

속도 제한 트리거로 인한 TCP 패킷 손실

CVM 인스턴스에는 여러 사양이 있으며 사양마다 네트워크 성능이 다릅니다. 인스턴스의 대역폭 또는 패킷량이 인스턴스 사양 해당 기준을 초과하면 플랫폼 측의 속도 제한이 트리거되어 패킷 손실이 발생합니다. 문제 진단 및 해결 절차는 다음과 같습니다.
1. 인스턴스의 대역폭과 패킷량을 확인합니다.
Linux 인스턴스는 `sar -n DEV 2` 명령을 실행하여 대역폭과 패킷량을 확인할 수 있습니다. 이 중 `rxpck/s` 와 `txpck/s` 지표는 송수신 패킷량이고 `rxkB/s` 와 `txkB/s` 의 지표는 송수신 대역폭입니다.
2. 획득한 대역폭 및 패킷량 데이터를 인스턴스 스펙과 비교하여 인스턴스 사양의 성능 병목 지점에 도달했는지 확인합니다.

확인 결과 맞는 경우, 인스턴스 사양을 업그레이드하거나 서비스량을 조정해야 합니다.
확인 결과 아닌 경우, 티켓 제출을 통해 추가적인 문제 파악 및 해결을 진행하실 수 있습니다.

속도 제한 트리거로 인한 UDP 패킷 손실

속도 제한 트리거로 인한 TCP 패킷 손실 절차를 참고하여 인스턴스 사양 성능 병목 현상으로 인한 패킷 손실인지 확인합니다.
확인 결과 맞는 경우, 인스턴스 사양을 업그레이드하거나 서비스량을 조정해야 합니다.
확인 결과 아닌 경우, DNS 요청에 대한 플랫폼의 추가 주파수 제한이 원인일 수 있습니다. 인스턴스의 전체 대역폭 또는 패킷량이 인스턴스 사양의 성능 병목 지점에 도달하면 DNS 요청 속도 제한이 트리거되어 UDP 패킷 손실이 발생할 수 있습니다. 티켓 제출을 통해 처리하시기 바랍니다.

소프트웨어 인터럽트 패킷 손실 트리거

운영 체제가 `/proc/net/softnet_stat` 의 두 번째 열에 있는 카운트 값이 증가하는 것을 감지하면 "소프트웨어 인터럽트 패킷 손실"로 판단합니다. 인스턴스가 소프트웨어 인터럽트 패킷 손실을 트리거하면 다음 절차를 통해 문제를 진단 및 해결할 수 있습니다.
RPS 활성화 여부 확인:
활성화됨: 커널 매개변수 `net.core.netdev_max_backlog` 가 너무 작으면 패킷 손실이 발생하므로 상향 조정해야 합니다. 커널 매개변수에 대한 자세한 내용은 Linux 인스턴스 상용 커널 매개변수 소개를 참고하십시오.
미활성화: CPU 단일 코어 소프트웨어 인터럽트가 높아서 데이터를 제때 송수신하지 못하는지 확인하십시오. 맞다면 다음을 진행합니다.
RPS를 활성화하여 소프트웨어 인터럽트를 보다 균형적으로 분배합니다.
작업 프로그램으로 인해 소프트웨어 인터럽트 분배가 불균형적인지 확인하십시오.

UDP 전송 버퍼 가득 참

UDP 버퍼가 충분하지 않아 인스턴스에서 패킷이 손실되는 경우 다음 절차에 따라 문제를 진단 및 해결할 수 있습니다.
1. `ss -nump` 명령어를 통해 UDP 전송 버퍼가 가득 찼는지 확인합니다.
2. 확인 결과 맞는 경우, 커널 매개변수 `net.core.wmem_max` 및 `net.core.wmem_default` 를 늘리고 UDP 프로그램을 다시 시작하여 적용하십시오. 커널 매개변수에 대한 자세한 내용은 Linux 인스턴스 상용 커널 매개변수 소개를 참고하십시오.
3. 여전히 패킷 손실 문제가 있는 경우 `ss -nump` 명령어를 통해 전송 버퍼가 예상대로 증가하지 않았는지 확인합니다. 이때 setsockopt를 통해 서비스 코드에 SO_SNDBUF를 설정했는지 확인하고, 맞다면 코드를 수정하여 SO_SNDBUF를 늘리십시오.

UDP 수신 버퍼 가득 참

UDP 버퍼가 충분하지 않아 인스턴스에서 패킷이 손실되면 다음 절차에 따라 처리할 수 있습니다.
1. `ss -nump` 명령어를 통해 UDP 수신 버퍼가 가득 찼는지 확인합니다.

1. 확인 결과 맞는 경우, 커널 매개변수 `net.core.rmem_max` 및 `net.core.rmem_default` 를 늘리고 UDP 프로그램을 다시 시작하여 적용하십시오. 커널 매개변수에 대한 자세한 내용은 Linux 인스턴스 상용 커널 매개변수 소개를 참고하십시오.
2. 패킷 손실 문제가 있는 경우 `ss -nump` 명령어를 통해 수신 버퍼가 예상대로 증가하지 않았는지 확인합니다. 이 때 setsockopt를 통해 서비스 코드에 SO_RCVBUF를 설정했는지 확인하고, 맞다면 코드를 수정하여 SO_RCVBUF를 늘리십시오.

TCP 완전 연결 큐 가득 참

TCP 완전 연결 큐의 길이는 'net.core.somaxconn'와 서비스 프로세스 호출 listen 시 전달되는 backlog 매개변수 중 더 작은 값을 취합니다. 인스턴스의 TCP 완전 연결 큐가 가득 차서 패킷 손실이 발생하면 다음 절차에 따라 해결할 수 있습니다.
1. 커널 매개변수 `net.core.somaxconn` 을 늘립니다. 커널 매개변수에 대한 자세한 내용은 Linux 인스턴스 상용 커널 매개변수 소개를 참고하십시오.
2. backlog 매개변수가 서비스 프로세스에서 전달되는지 확인합니다. 그렇다면 상향 조정하십시오.

TCP 요청 오버플로

TCP가 데이터를 수신할 때 socket이 user에 의해 잠겨 있으면 데이터가 backlog 큐로 전송됩니다. 이 프로세스가 실패하면 TCP 요청 오버플로 및 패킷 손실이 발생합니다. 작업 프로그램 성능이 정상이라면, 다음 절차를 통해 시스템 수준에서 문제를 진단 및 해결할 수 있습니다.
작업 프로그램이 setsockopt를 통해 buffer 크기를 자체 설정했는지 확인합니다.
확인 결과 맞는 경우, 또한 해당 설정 값이 충분히 크지 않은 경우, 더 큰 값으로 수정하여 더 이상 setsockopt를 통해 크기가 지정되지 않도록 합니다.
설명：
setsockopt의 값은 커널 매개변수 `net.core.rmem_max` 및 `net.core.wmem_max` 에 의해 제한됩니다. 작업 프로그램을 조정하면서 `net.core.rmem_max` 와 `net.core.wmem_max` 를 동시에 조정합니다. 조정 후 작업 프로그램을 재부팅하여 설정이 적용되도록 하십시오.
확인 결과 아닌 경우, `net.ipv4.tcp_mem` , `net.ipv4.tcp_rmem` , 및 `net.ipv4.tcp_wmem` 커널 매개변수를 상향 조절하여 TCP socket 수위를 조정합니다.
커널 매개변수 수정에 대한 자세한 내용은 Linux 인스턴스 상용 커널 매개변수 소개를 참고하십시오.

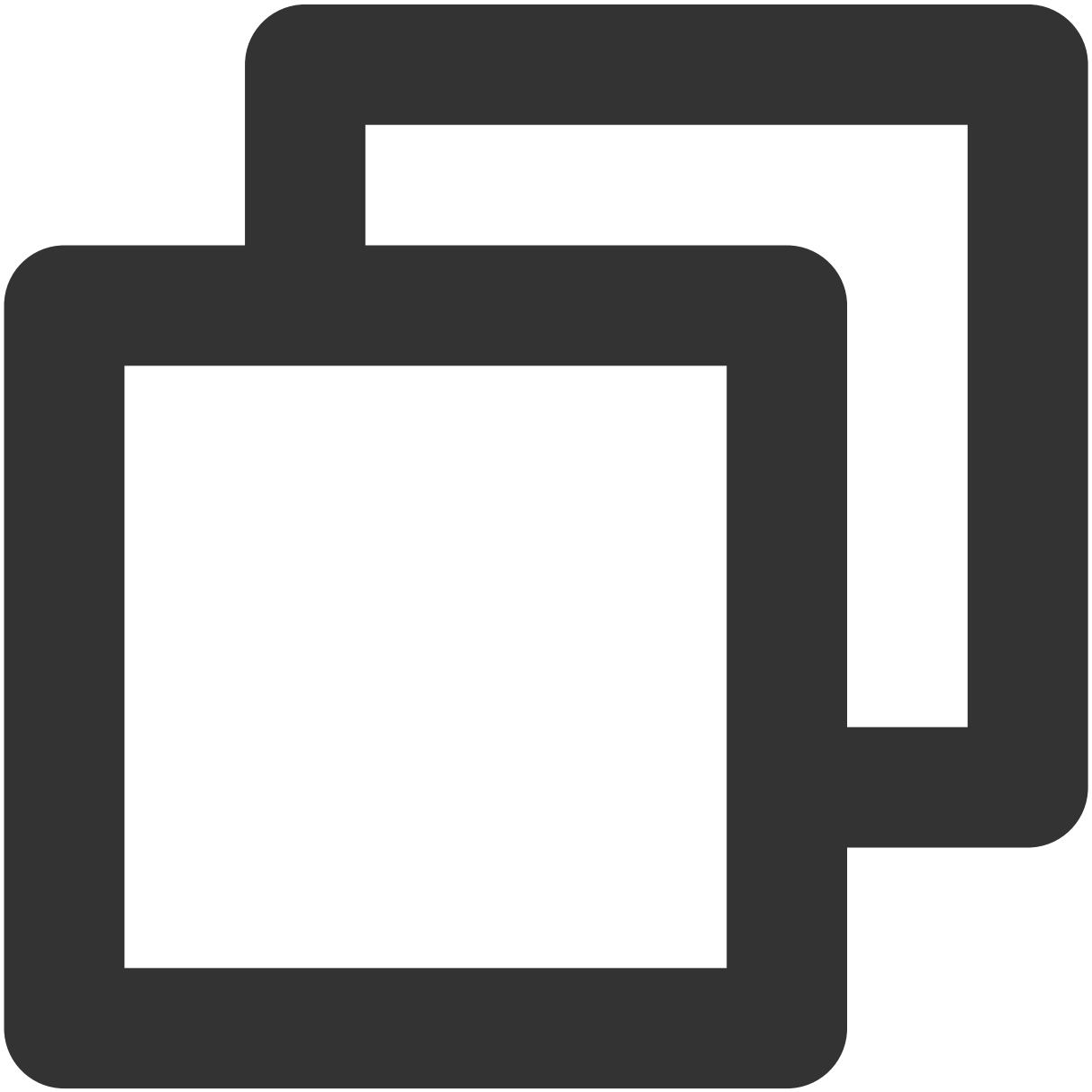
연결 수 상한 도달

CVM 인스턴스에는 다양한 사양이 있으며 각 사양마다 연결 수 성능 지표가 다릅니다. 인스턴스 연결 수가 인스턴스 사양에 해당하는 기준을 초과하면 플랫폼 속도 제한이 트리거되어 패킷 손실이 발생합니다. 해결 절차는 다음과 같습니다.
설명：
연결 수는 호스트에 저장된 CVM 인스턴스의 세션 수를 나타내며, TCP, UDP, ICMP를 포함합니다. 이 값은 CVM 인스턴스에서 `ss` 또는 `netstat` 명령어를 통해 얻은 네트워크 연결 수보다 큽니다.
인스턴스 연결 수를 확인하고, 인스턴스 스펙과 비교하여 인스턴스 사양의 성능 병목 지점에 도달했는지 확인합니다.

확인 결과 맞는 경우, 인스턴스 사양을 업그레이드하거나 서비스량을 조정해야 합니다.
확인 결과 아닌 경우, 인스턴스 사양의 성능 병목 지점에 도달하지 않은 경우 티켓 제출을 통해 처리하시기 바랍니다.

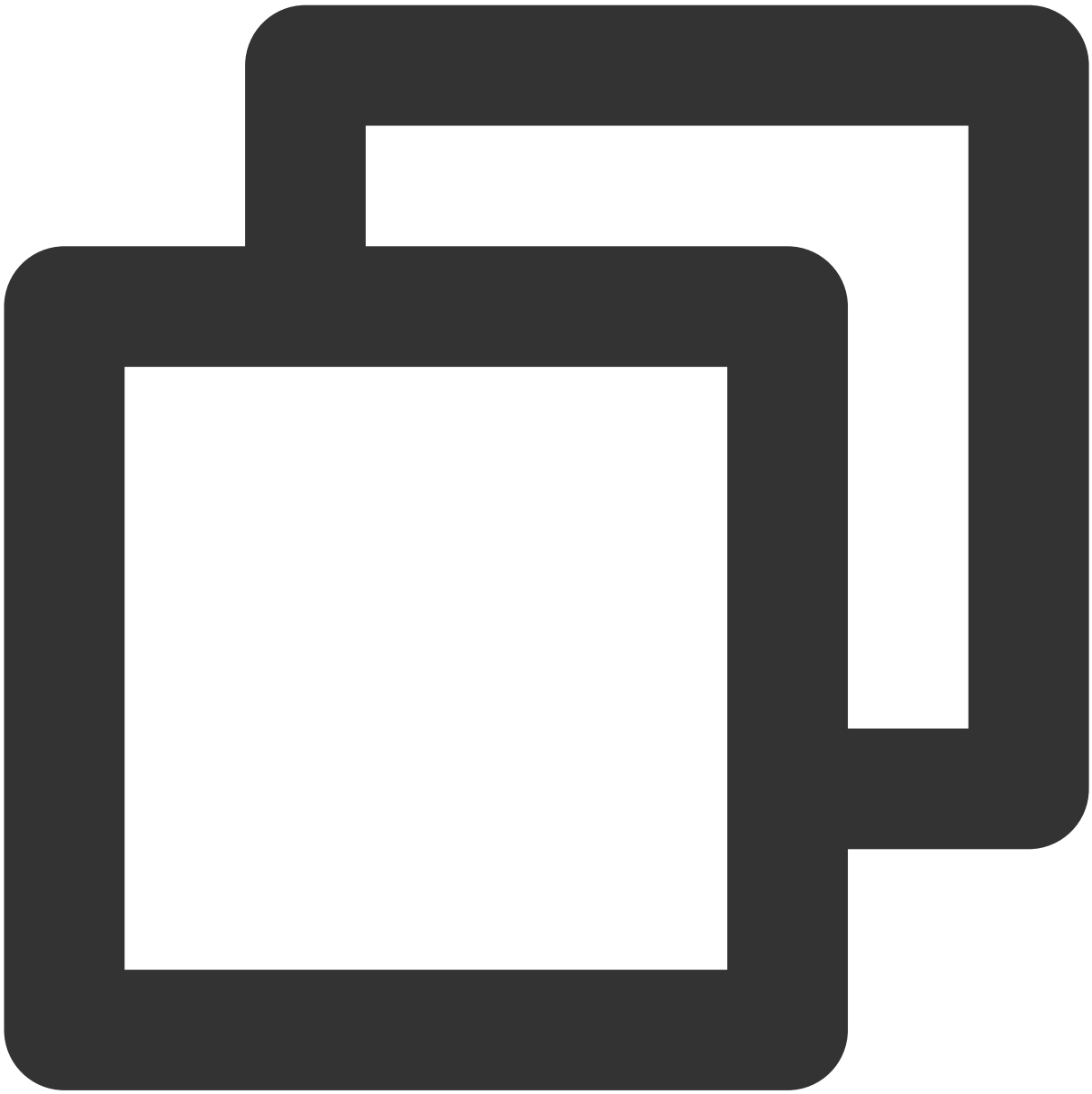
iptables policy 설정 관련 규칙

CVM의 iptables에 관련 규칙이 설정되어 있지 않은 경우, iptables policy 관련 규칙 설정으로 인해 CVM에 도달하는 모든 패킷이 버려질 수 있습니다. 처리 단계는 다음과 같습니다.
1. 다음 명령을 실행하여 iptables policy 규칙을 확인합니다.



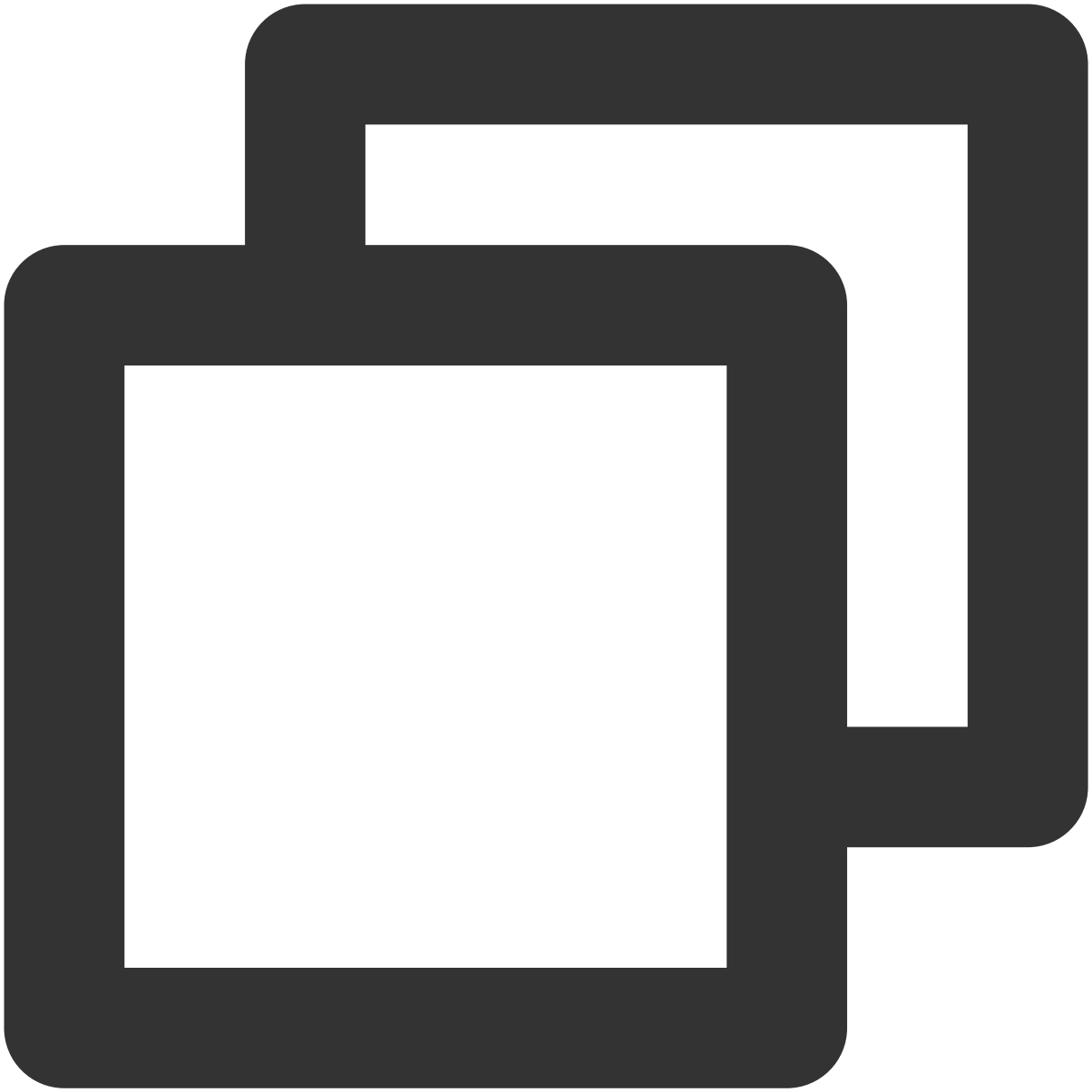
```
iptables -L | grep policy
```

iptables policy 규칙의 기본값은 ACCEPT입니다. INPUT 체인 policy가 ACCEPT가 아니면 서버에 대한 모든 패킷이 버려집니다. 예를 들어 다음 결과가 반환되면 CVM에 들어오는 모든 패킷이 drop된다는 표시입니다.



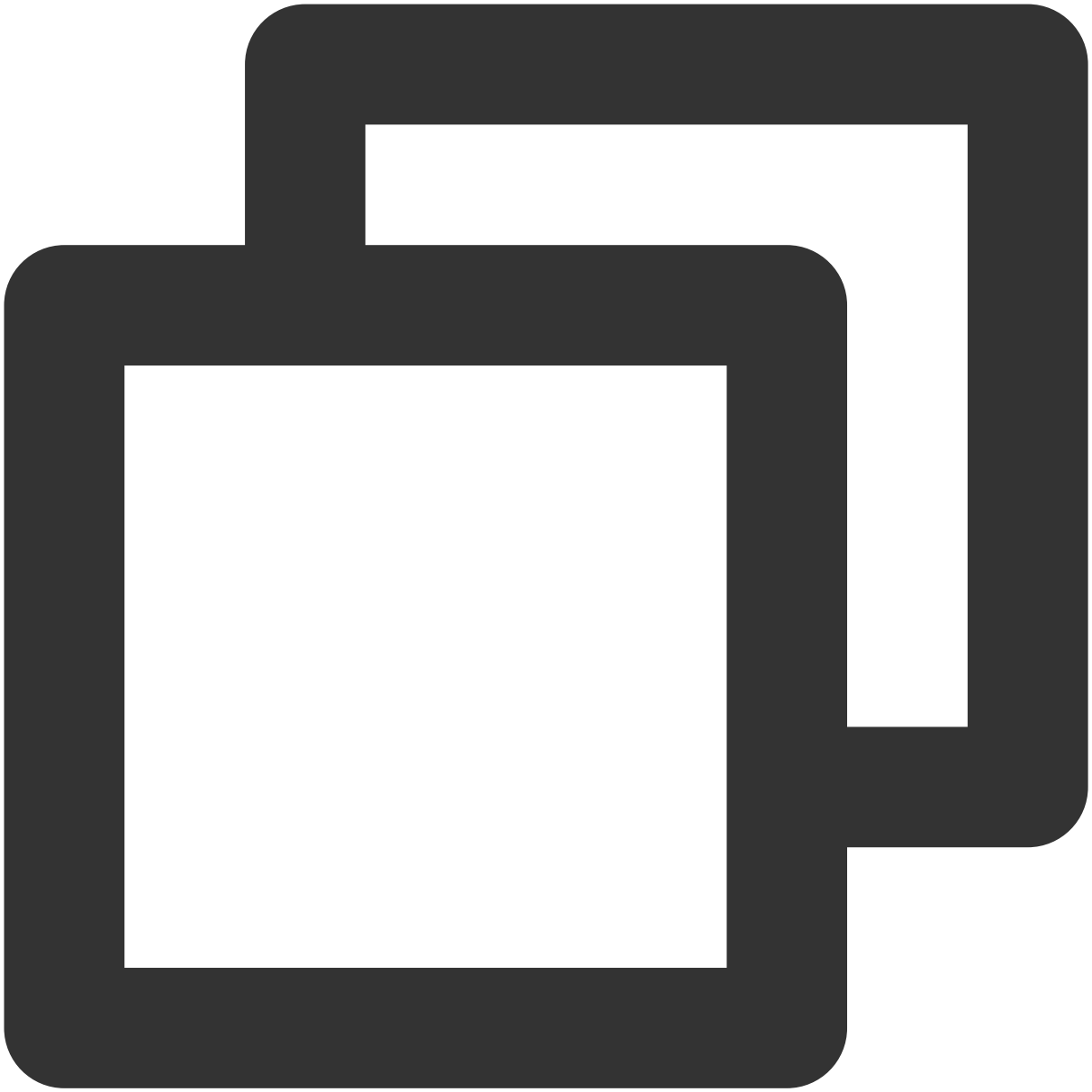
```
Chain INPUT (policy DROP)
Chain FORWARD (policy ACCEPT)
Chain OUTPUT (policy ACCEPT)
```

2. 다음 명령을 실행하여 필요에 따라 `-P` 이후의 값을 조정합니다.



```
iptables -P INPUT ACCEPT
```

조정 후 다시 Step 1 명령을 실행하여 확인할 수 있으며 다음과 같은 결과가 반환되어야 합니다.



```
Chain INPUT (policy ACCEPT)
Chain FORWARD (policy ACCEPT)
Chain OUTPUT (policy ACCEPT)
```

인스턴스IP주소 ping 통하지 않음

최종 업데이트 날짜: : 2024-02-02 11:09:47

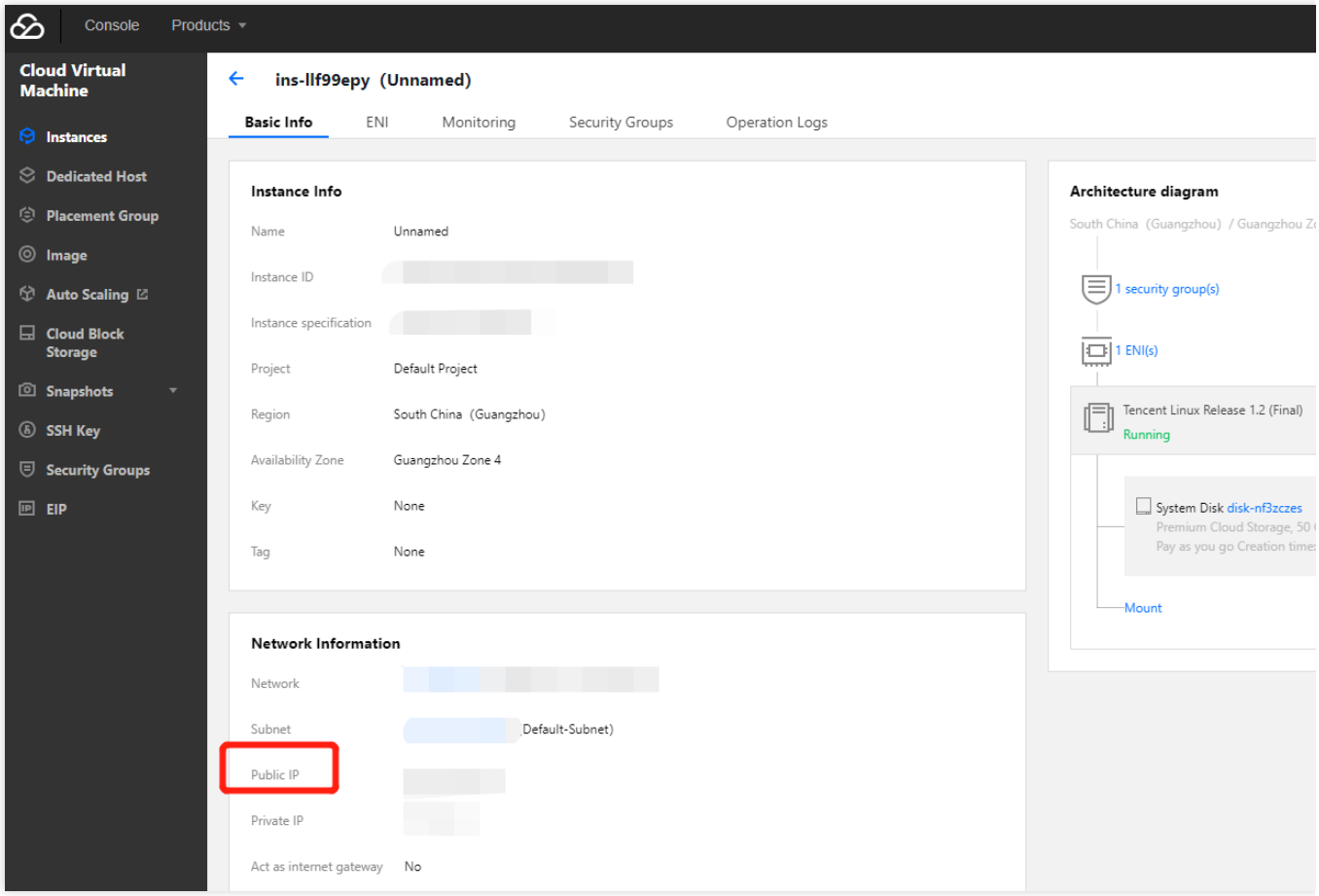
장애 현상

로컬 서버가 인스턴스를 ping하지 못합니다. 가능한 원인은 다음과 같습니다.
잘못된 대상 서버 설정
도메인 이름 확인 실패
연결 오류
로컬 네트워크가 정상이면(로컬 네트워크에서 다른 웹 사이트를 ping할 수 있음) 다음과 같이 문제를 해결하십시오.
인스턴스가 public IP 주소로 구성되었는지 확인
보안 그룹 설정 확인
운영 체제 설정 확인
기타 작업 수행

처리 단계

인스턴스가 public IP 주소로 구성되었는지 확인

설명 :
인스턴스는 public IP 주소가 있는 경우에만 Internet의 다른 컴퓨터에 액세스할 수 있습니다. 그렇지 않으면 사설망 IP 주소 외부를 통해 인스턴스를 ping할 수 없습니다.
1. CVM 콘솔에 로그인합니다.
2. '인스턴스' 페이지에서 다음 그림과 같이 ping할 인스턴스의 ID/이름을 선택하여 인스턴스 세부 정보 페이지로 이동합니다.

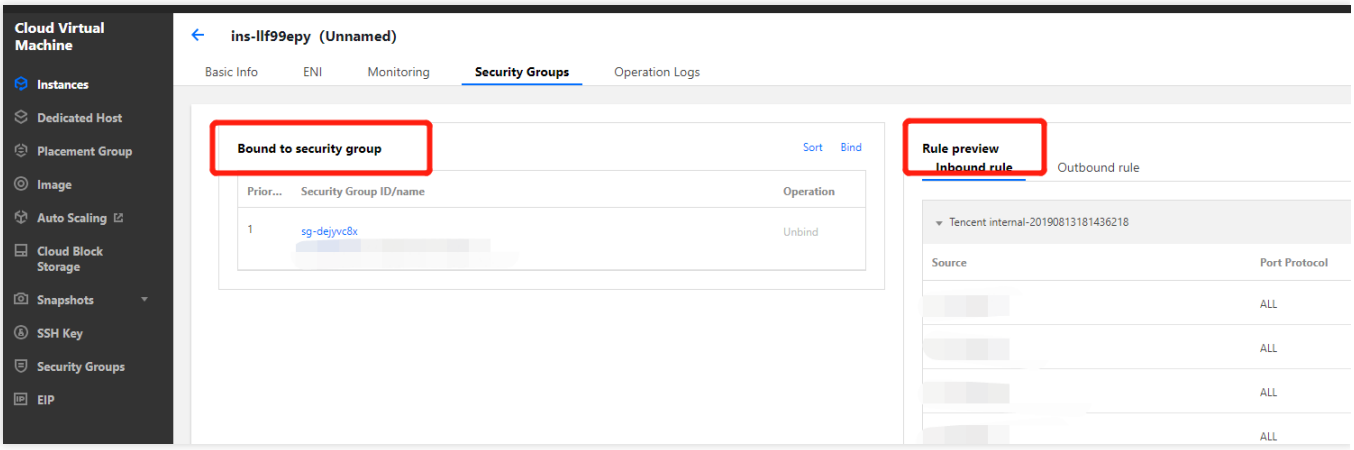


3. '네트워크 정보'에서 인스턴스가 public IP 주소로 구성되어 있는지 확인하십시오.
구성되어 있는 경우, 보안 그룹 설정 확인을 진행하십시오.
구성되어 있지 않은 경우, 클라우드 리소스의 EIP 바인딩을 확인하십시오.

보안 그룹 설정 확인

보안 그룹은 연결된 인스턴스의 인바운드 및 아웃바운드 트래픽을 제어하는 가상 방화벽입니다. 보안 그룹 규칙에서 프로토콜, 포트 및 정책을 지정할 수 있습니다. ping 테스트는 ICMP를 사용하기 때문에 해당 인스턴스와 연결된 보안 그룹에서 해당 프로토콜이 허용되는지 확인해야 합니다. 인스턴스와 해당 인바운드 및 아웃바운드 규칙과 연결된 보안 그룹을 보려면 다음 단계를 수행하십시오.

1. CVM 콘솔에 로그인합니다.
2. '인스턴스' 페이지에서 보안 그룹으로 설정할 인스턴스의 ID/이름을 선택하여 다음 그림과 같이 인스턴스 세부 정보 페이지로 들어갑니다.
3. **보안 그룹** 탭을 클릭하여 다음 이미지와 같이 이 인스턴스의 보안 그룹 관리 페이지로 들어갑니다.



4. 인스턴스와 연결된 보안 그룹과 자세한 인바운드 및 아웃바운드 규칙을 확인하여 이 보안 그룹이 ICMP를 허용하는지 확인합니다.

허용하는 경우, 운영 체제 설정 확인을 진행하십시오.

허용하지 않는 경우, ICMP 프로토콜 정책을 허용으로 설정하십시오.

운영 체제 설정 확인

인스턴스의 운영 체제에 따라 구성을 확인할 방법을 선택합니다.

Linux 운영 체제의 경우 Linux 커널 매개변수 및 방화벽 설정 확인을 진행하십시오.

Windows 운영 체제의 경우 Windows 방화벽 설정 확인을 진행하십시오. 방화벽 설정이 올바르면 Windows 네트워크 설정 재설정을 시도하십시오.

Linux 커널 매개변수 및 방화벽 설정 확인

설명：

Linux 운영 체제에서 ping 테스트가 허용되는지 여부는 커널 및 방화벽 설정에 따라 다릅니다. 둘 중 하나가 ping 테스트를 거부하면 'Request timeout'이 발생합니다.

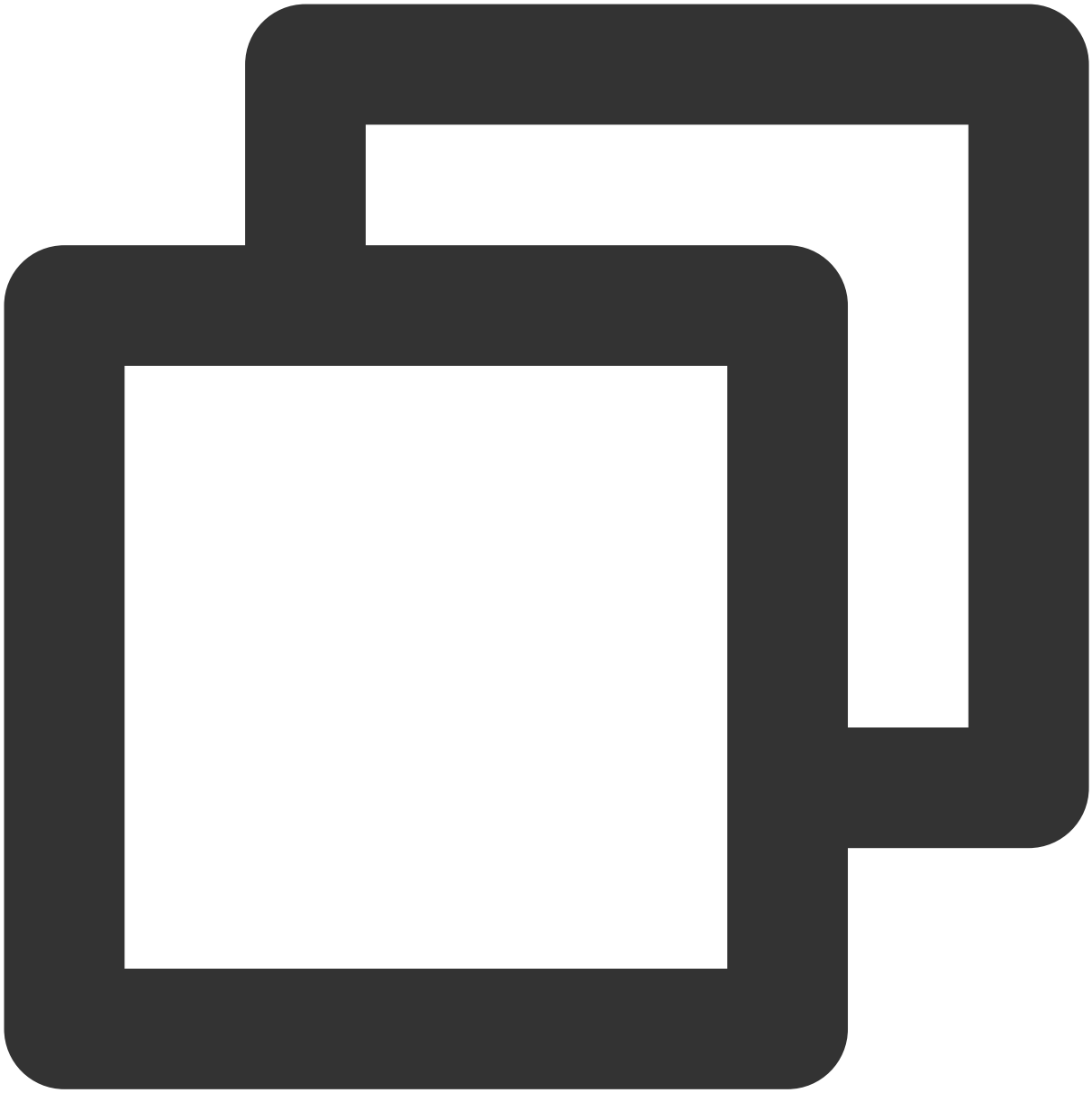
icmp_echo_ignore_all 커널 매개변수 확인

1. VNC를 통해 인스턴스에 로그인합니다. 자세한 내용은 다음을 참고하십시오.

VNC를 사용하여 Linux 인스턴스 로그인합니다.

VNC를 사용하여 Linux 인스턴스 로그인

2. 다음 명령어를 실행하여 시스템의 icmp_echo_ignore_all 설정을 확인합니다.

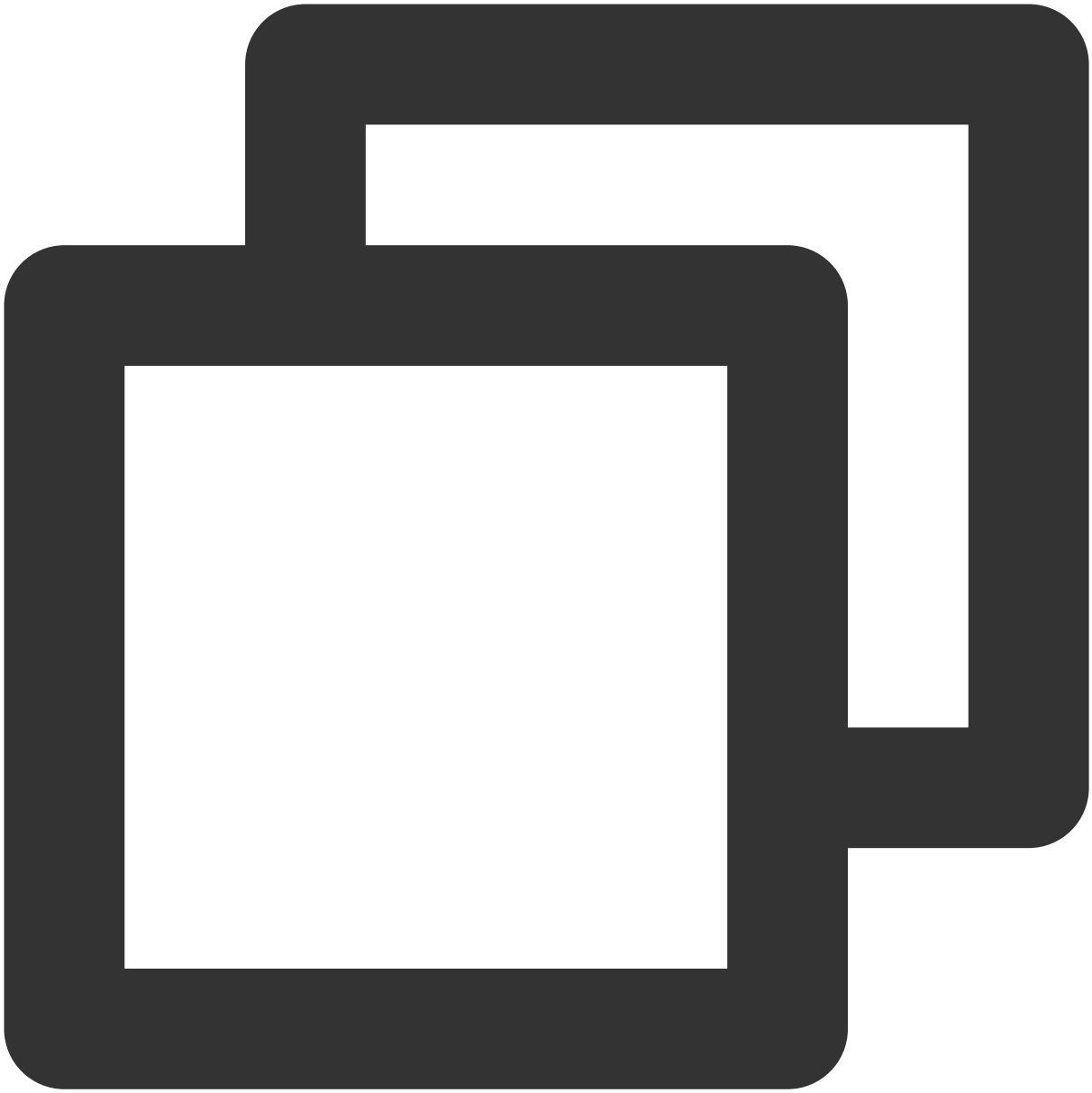


```
cat /proc/sys/net/ipv4/icmp_echo_ignore_all
```

0이 반환되면 모든 ICMP Echo 요청이 시스템에서 허용됩니다. 이 경우 방화벽 설정 확인에서 확인하십시오.

1이 반환되면 모든 ICMP Echo 요청이 시스템에서 거부됩니다. 이 경우 3단계에서 확인하십시오.

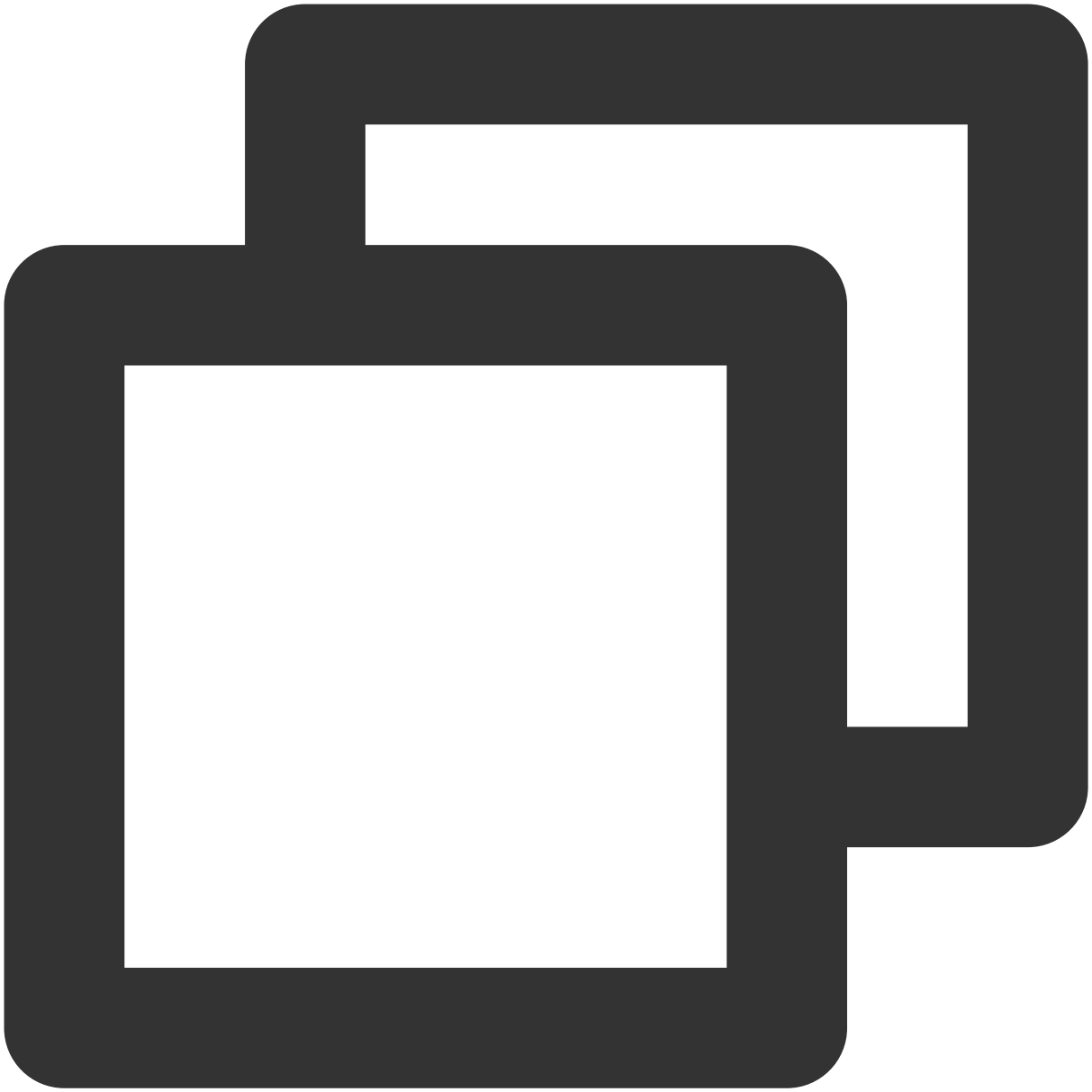
3. 다음 명령을 실행하여 icmp_echo_ignore_all 커널 매개변수의 설정을 수정하십시오.



```
echo "0" >/proc/sys/net/ipv4/icmp_echo_ignore_all
```

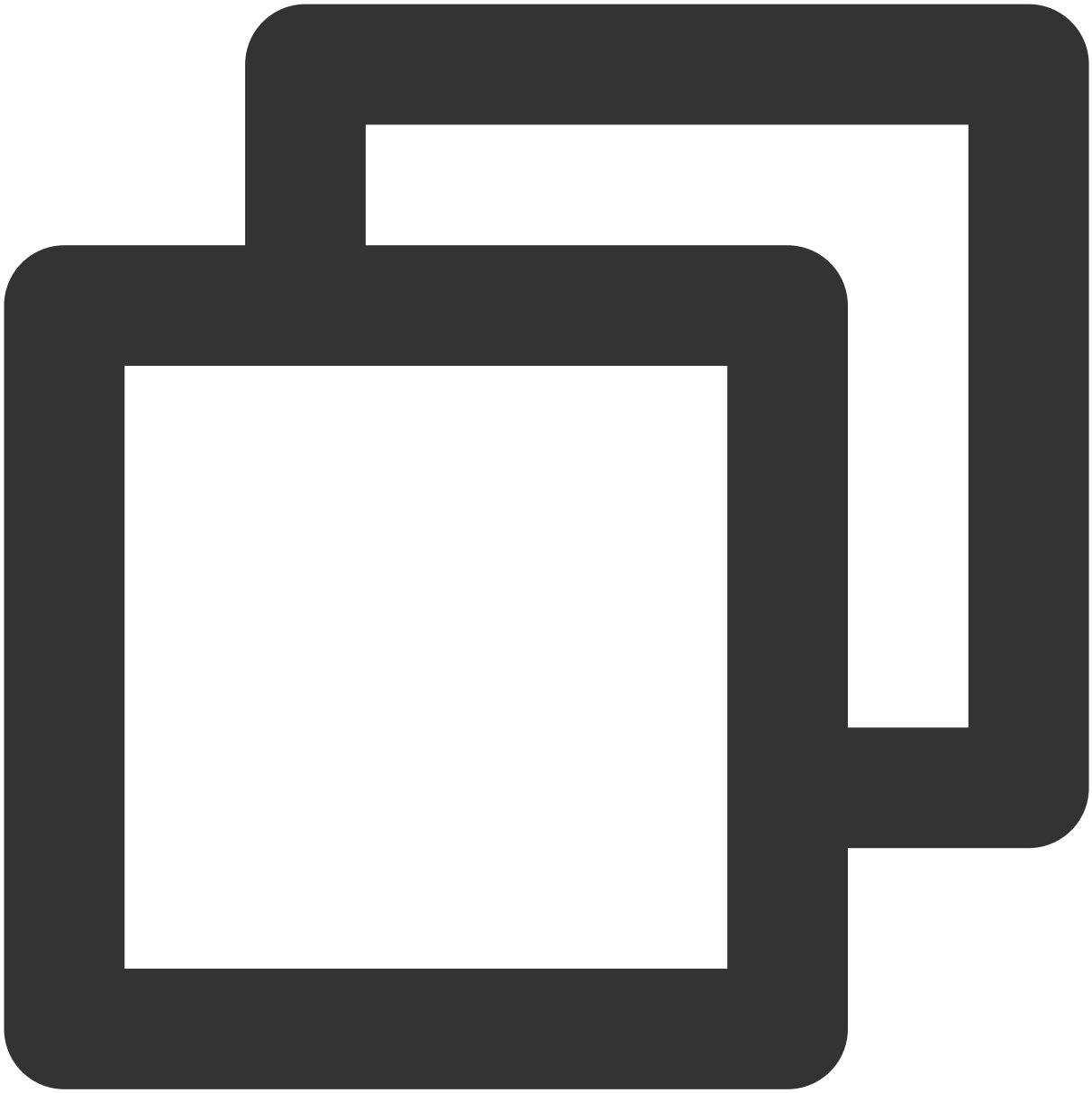
방화벽 설정 확인

다음 명령을 실행하여 방화벽 규칙과 현재 서버의 해당 ICMP 규칙이 비활성화되어 있는지 확인합니다.



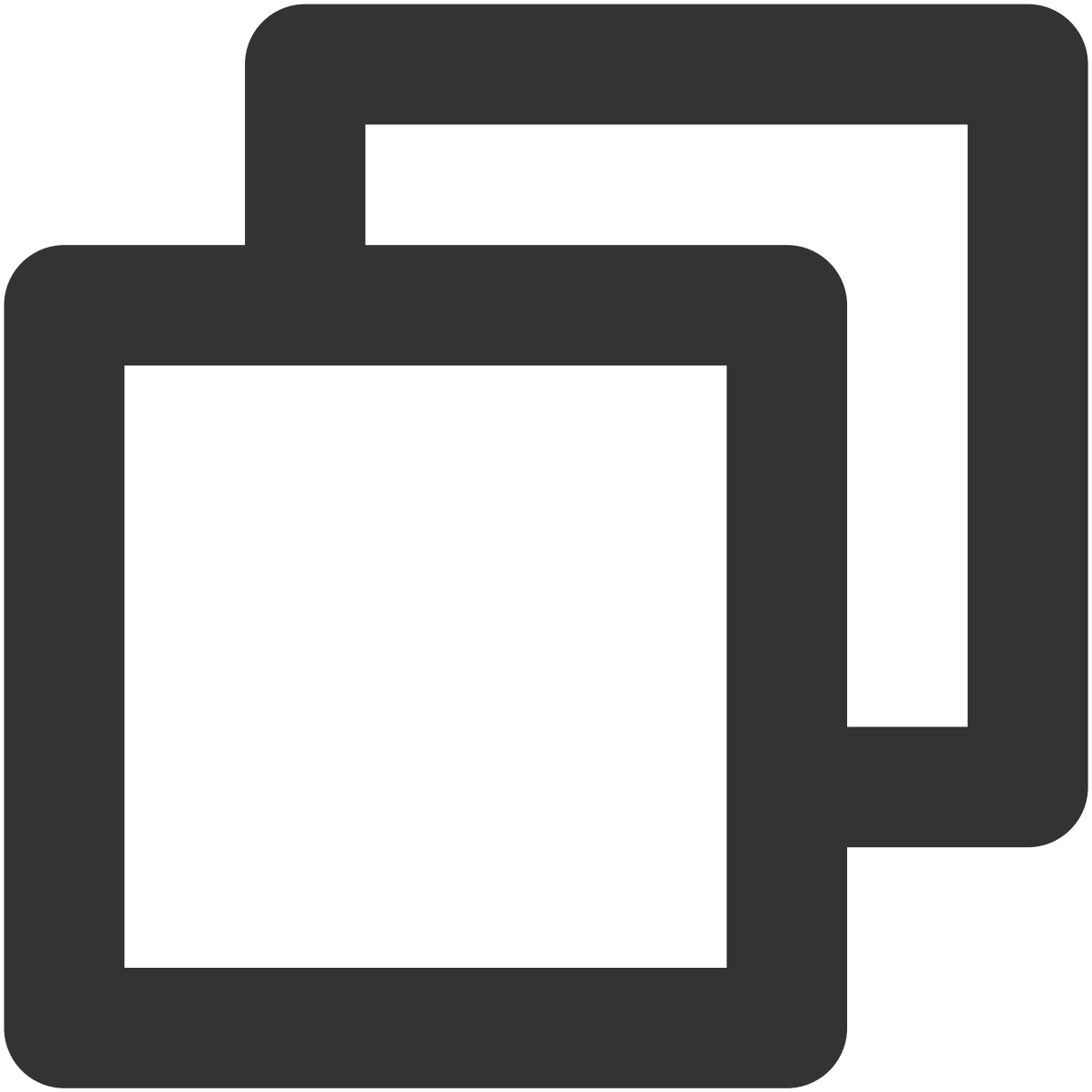
```
iptables -L
```

다음 결과가 반환되면 ICMP 규칙이 비활성화되지 않은 것입니다.



```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
```

반환 결과에 ICMP 규칙이 비활성화되었다고 표시되면 다음 명령을 실행하여 활성화합니다.



```
#Chain INPUT
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
#Chain OUTPUT
iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

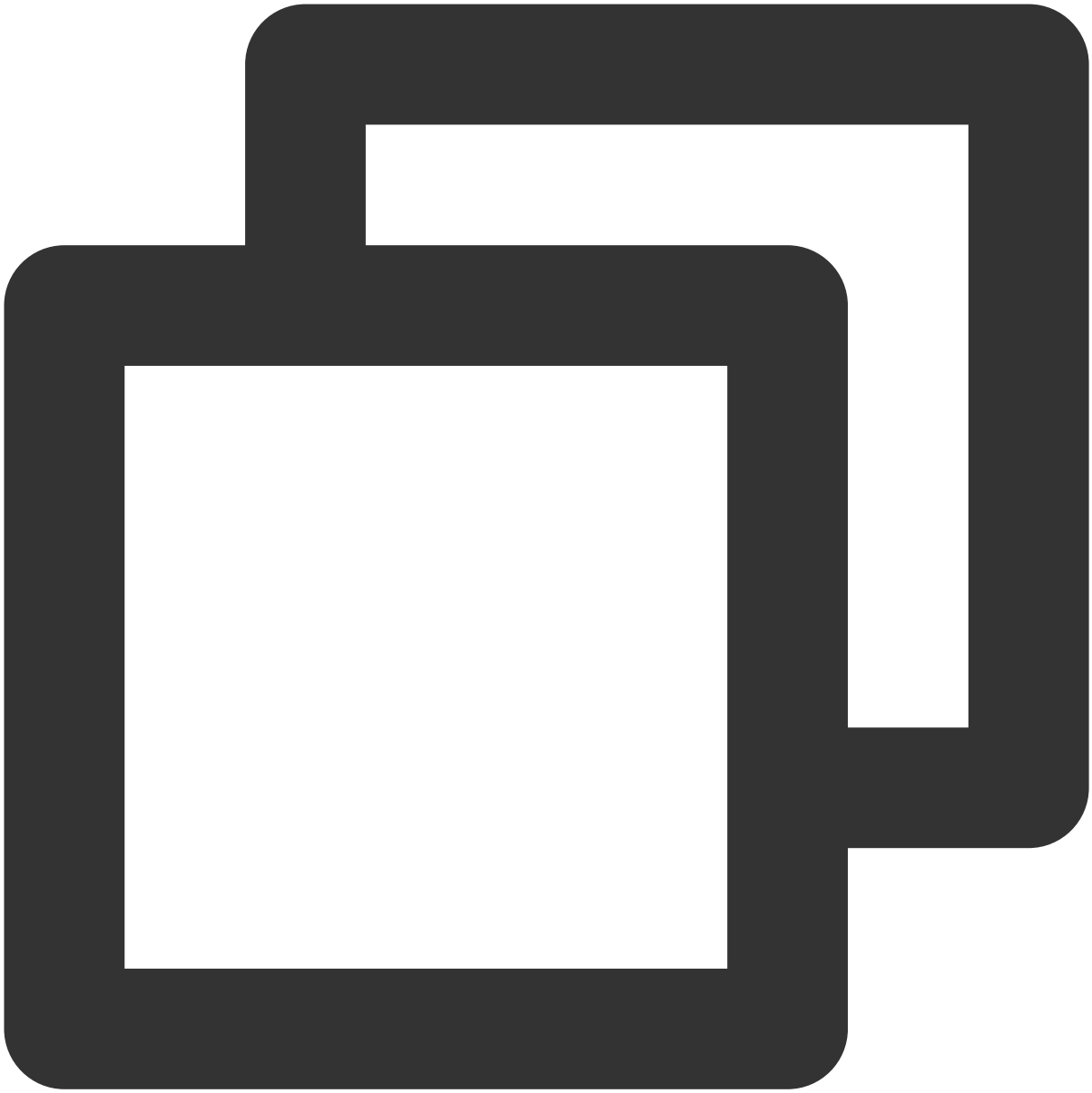
Windows 방화벽 설정 확인

1. 인스턴스에 로그인합니다.
2. **제어판**을 열고 **Windows 방화벽**을 선택합니다.
3. 'Windows 방화벽' 페이지에서 **고급 설정**을 선택합니다.

4. '고급 보안이 포함된 Windows 방화벽' 팝업 창에서 ICMP 인바운드 및 아웃바운드 규칙이 비활성화되어 있는지 확인합니다.
ICMP 인바운드 및 아웃바운드 규칙이 비활성화된 경우 활성화하십시오.

Windows 네트워크 설정 재설정

1. VPC 네트워크가 DHCP를 지원하는지 확인합니다(DHCP는 2018년 6월 이후 생성된 VPC 네트워크에서 지원됨). DHCP를 지원하지 않는 경우 네트워크 설정의 고정 IP가 올바른지 확인하십시오.
2. DHCP를 지원하는 경우 DHCP의 사설망 IP가 맞는지 확인합니다. 올바르지 않은 경우 공식 웹 사이트에서 VNC를 통해 로그인하고 PowerShell을 관리자로 실행하십시오. `ipconfig /release` 및 `ipconfig/renew` (인스턴스를 다시 시작할 필요 없이)를 구현하여 IP를 다시 가져옵니다.
3. DHCP의 IP는 맞지만 여전히 네트워크에 연결할 수 없는 경우 시작 메뉴에서 [실행]을 클릭하고 `ncpa.cpl` 을 입력한 후 확인을 클릭합니다. 로컬 연결을 열고 ENI를 비활성화 및 활성화하십시오.
4. 문제가 지속되면 관리자로 CMD에서 다음 명령을 실행하고 인스턴스를 다시 시작하십시오.



```
reg delete "HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Ne
```

기타 작업

상기 단계를 통해 문제가 해결되지 않을 경우 다음을 참고하십시오.
도메인 이름을 ping할 수 없는 경우 웹사이트 구성을 확인하십시오.
public IP 주소를 ping할 수 없는 경우 인스턴스 및 양방향 MTR 데이터(로컬 서버에서 CVM으로, CVM에서 로컬 서버로)에 대한 정보를 첨부하고 Submit Ticket하여 엔지니어에게 도움을 요청하십시오.
MTR 사용 방법에 대한 자세한 내용은 CVM 네트워크 대기 시간 및 패킷 손실을 참고하십시오.

도메인네임 해석 불가(CentOS 6.x 시스템)

최종 업데이트 날짜: : 2024-02-02 11:09:47

현상 설명

CentOS 6.x 운영 체제의 CVM를 재시작하거나 `service network restart` 명령어를 실행한 후, CVM에서 도메인 이름이 확인되지 않는 상황이 나타날 수 있습니다. 동시에 `/etc/resolv.conf` 구성 파일을 조회할 경우, DNS 정보가 비어 있는 걸 발견할 수 있습니다.

예상 원인

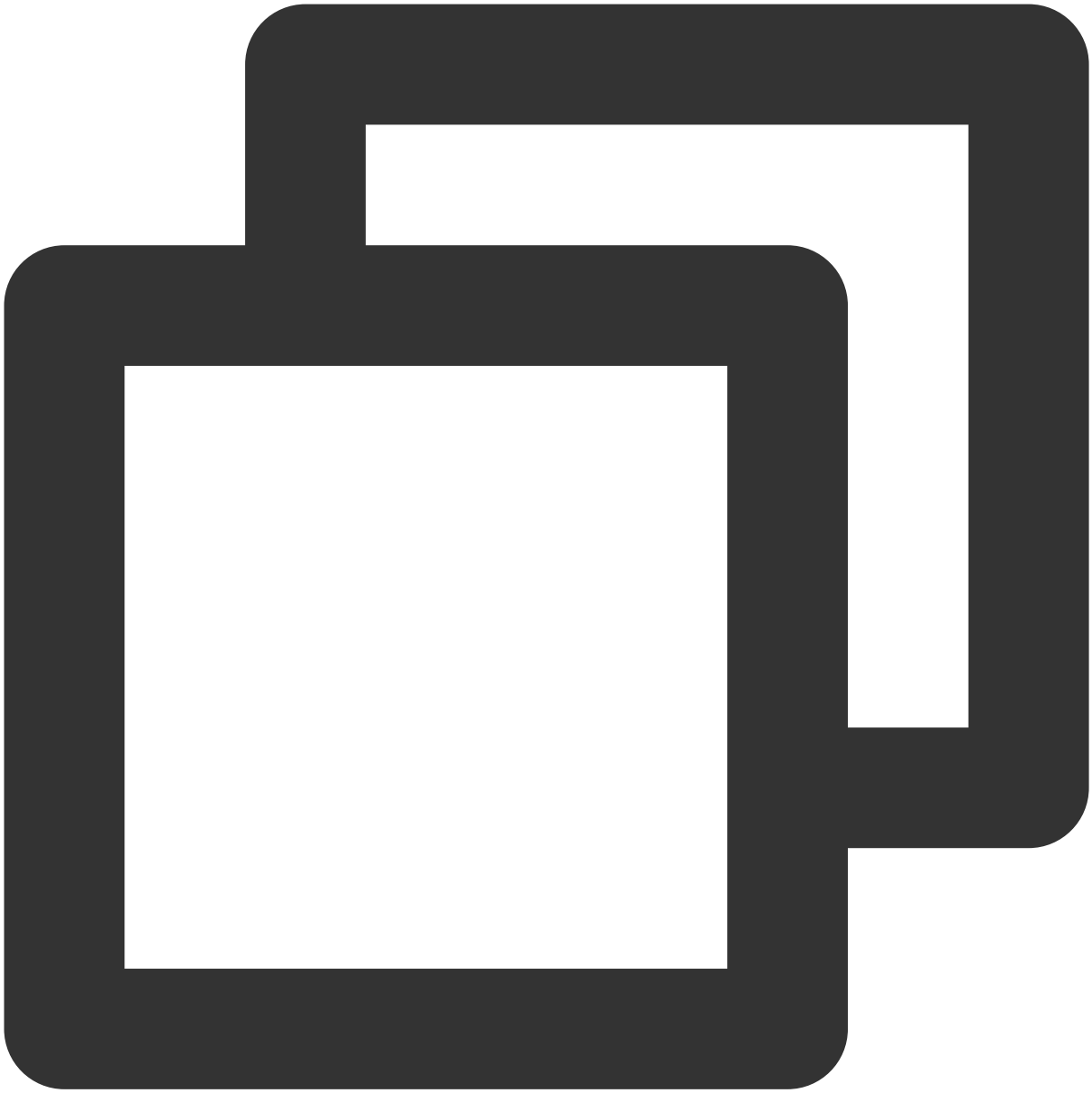
CentOS 6.x 운영 체제에서 grep 버전이 다를 경우, initscripts의 버전이 9.03.49-1보다 낮아 결함이 존재할 수 있습니다.

해결 방식

initscripts의 최신 버전으로 업데이트하고 DNS 정보를 다시 생성하십시오.

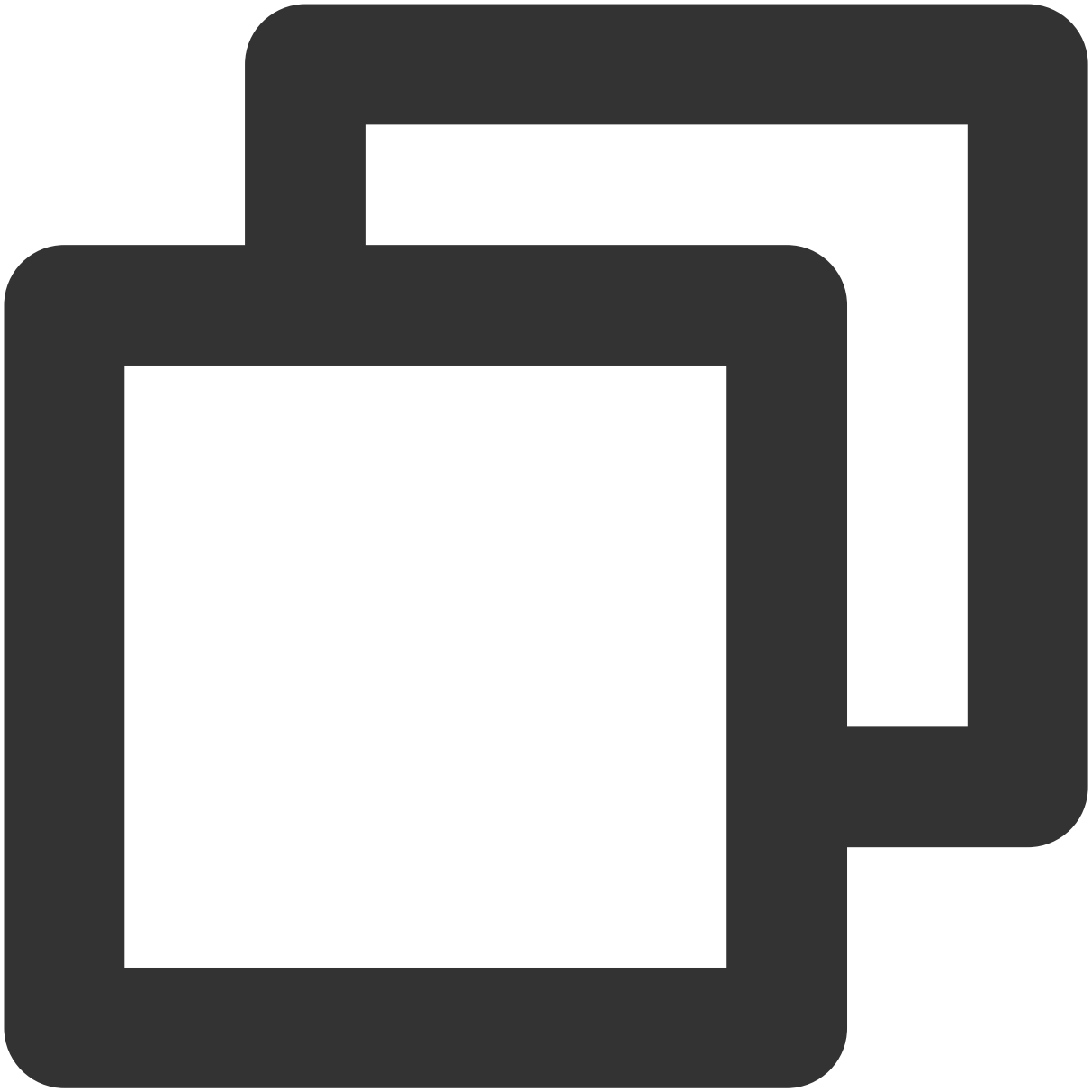
처리 순서

1. CVM에 로그인하십시오.
2. 아래의 명령어를 실행하여 initscripts 의 버전을 확인하고, 9.03.49-1 보다 낮은 버전으로 인해 initscripts에 결함이 있는지 확인하십시오.



```
rpm -q initscripts
```

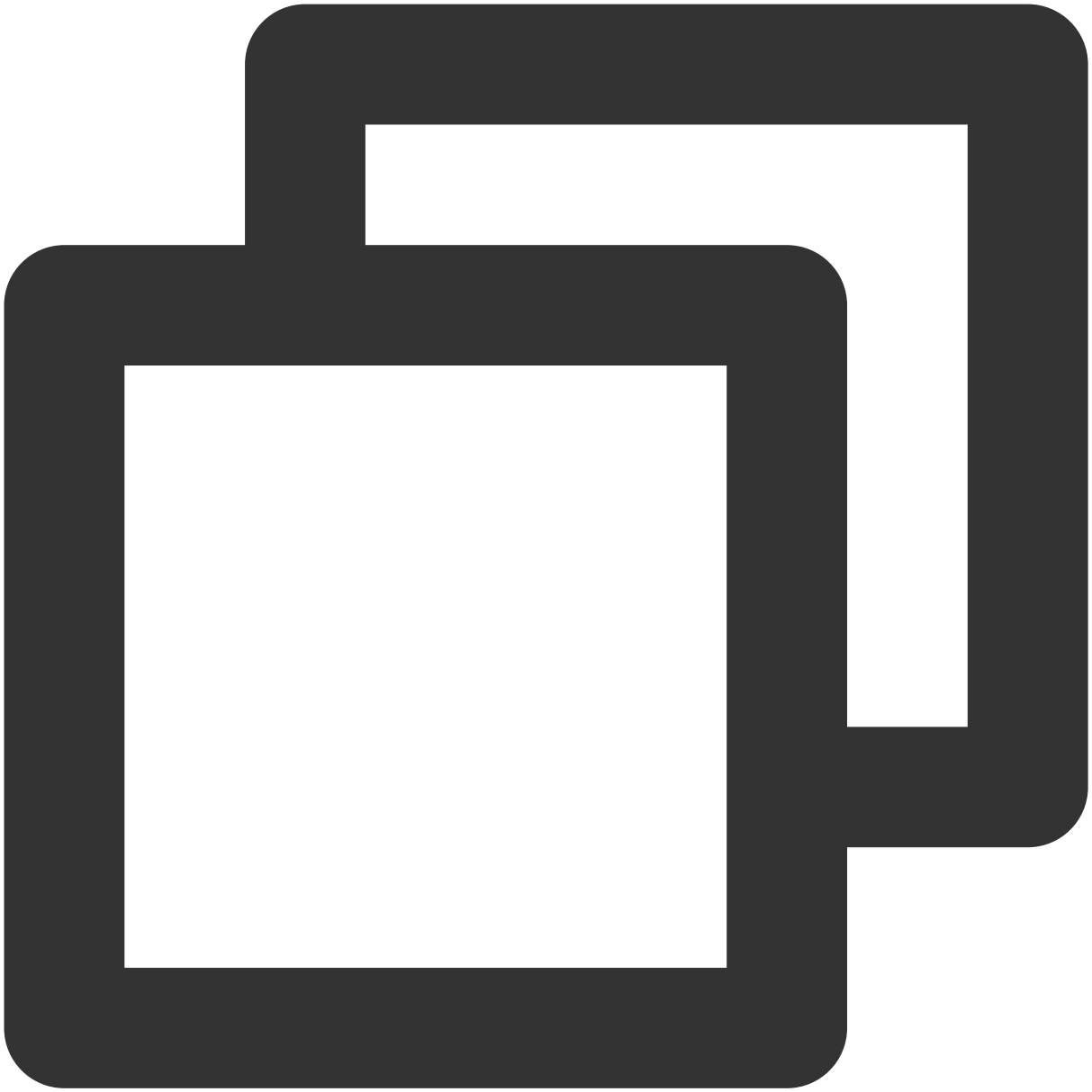
아래와 유사한 정보 리턴



```
initscripts-9.03.40-2.e16.centos.x86_64
```

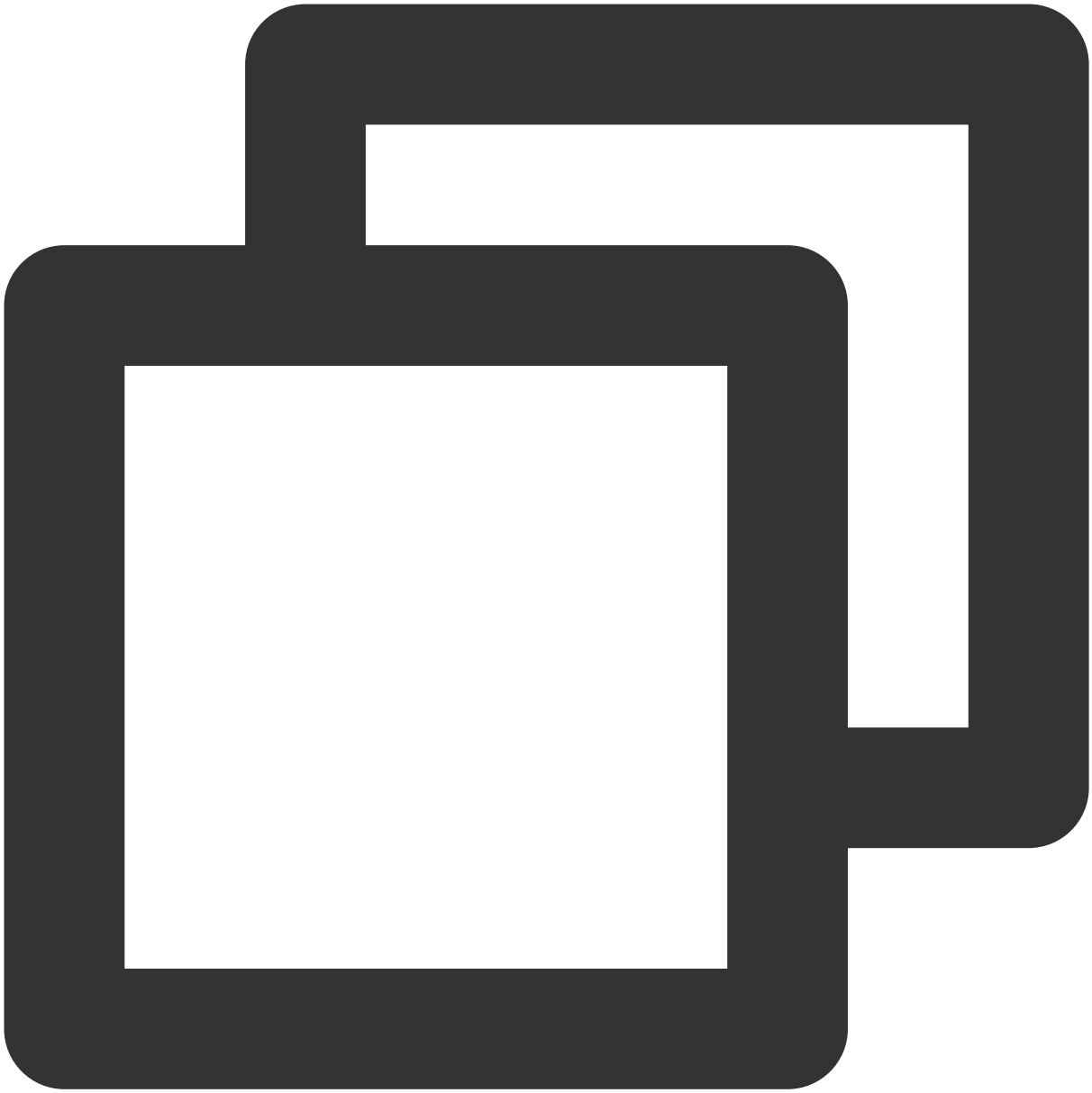
initscripts의 버전이 initscripts-9.03.40-2보다 낮은 버전이라서(initscripts-9.03.49-1) DNS 삭제 위험이 있다는 것을 알 수 있습니다.

3. 아래의 명령어를 순서에 따라 실행하여 initscripts를 최신 버전으로 업데이트하고 DNS 정보를 다시 생성하십시오.



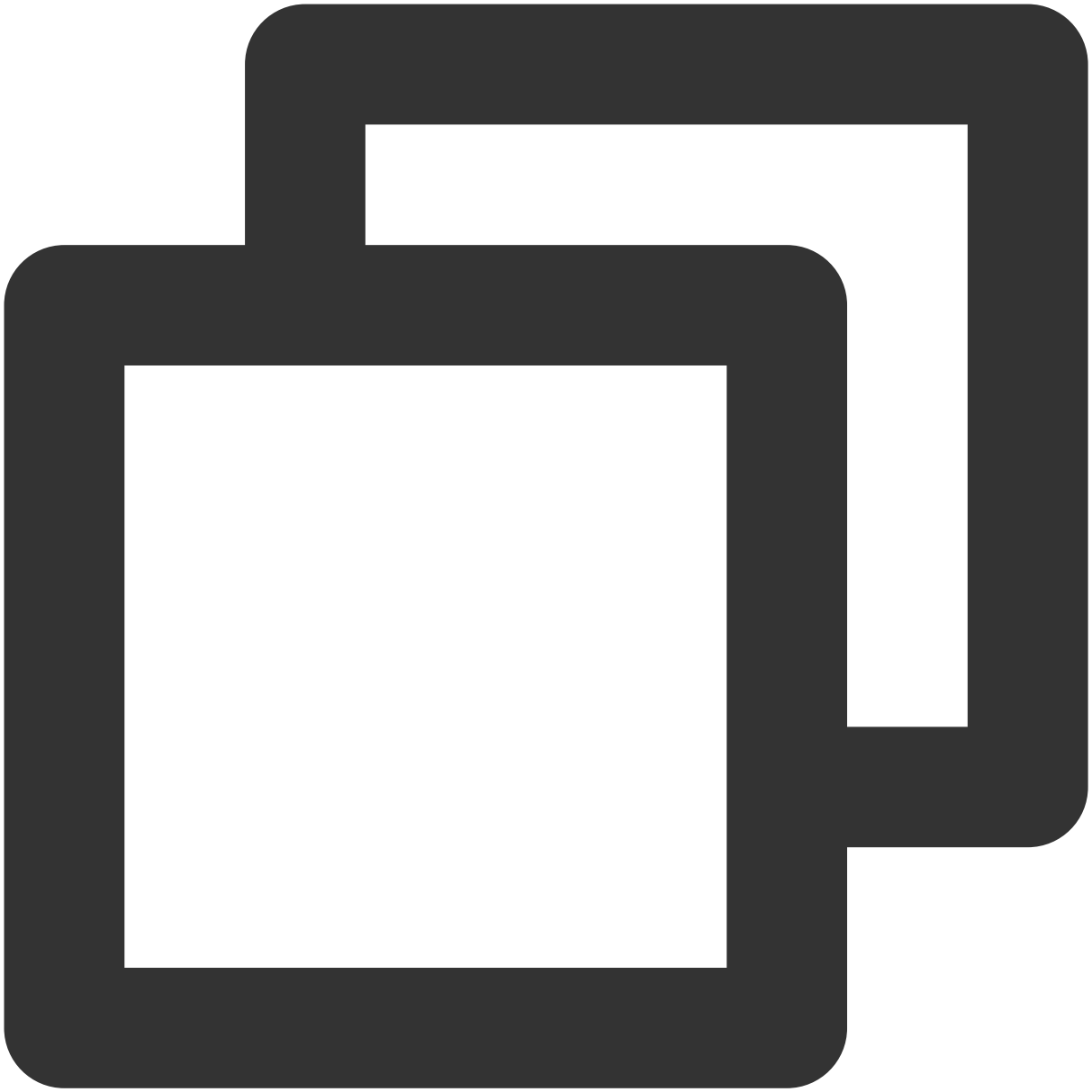
```
yum makecache
yum -y update initscripts
service network restart
```

4. 업데이트 완료 후, 아래의 명령어를 실행해 initscripts의 버전 정보를 조회하여 업데이트 성공 여부를 확인하십시오.



```
rpm -q initscripts
```

아래와 유사한 정보 리턴



```
initscripts-9.03.58-1.el6.centos.2.x86_64
```

표시되는 버전이 이전의 버전과 다르며, initscripts-9.03.49-1보다 높아 업데이트 작업이 성공했다는 것을 알 수 있습니다.