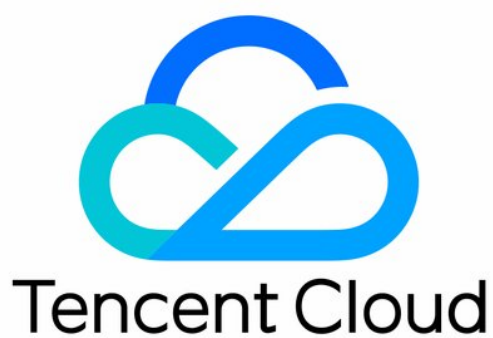


Cloud Virtual Machine

모범 사례

제품 문서



Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

목록:

모범 사례

- CVM 모범 사례

- CVM 유형 모범 사례

- 웹사이트 구축 방법

- 환경 구축

 - 환경 개요 구축

 - IIS 서비스 설치

- 웹 사이트 구축

 - 웹 사이트 개요 구축

 - WordPress 개인 사이트 구축

 - WordPress 개인사이트 매뉴얼 구축

 - WordPress 웹 사이트 수동 구축(Windows)

 - Discuz! 포럼 구축

 - Discuz! 포럼 수동 구축

 - Ghost 블로그 수동 구축

- 애플리케이션 구축

 - FTP 서비스 구축

 - Linux CVM에서 FTP 서비스 구축

 - Windows CVM에서 FTP 서비스 구축

 - NTP 서비스

 - NTP 서비스 개요

 - Linux 인스턴스에서 NTP 서비스 설정

 - Linux 인스턴스: NTPDate를 NTPD로 전환

 - Windows 인스턴스에서 NTP 서비스 설정

 - PostgreSQL 프라이머리/세컨더리 아키텍처 구축

 - Microsoft SharePoint 2016 구축

 - aaPanel-BT Windows 설치

 - Docker 구축

 - GitLab 구축

 - RabbitMQ 구축

- 시각화 인터페이스 구축

 - Ubuntu 시각화 인터페이스 구축

 - CentOS 시각화 인터페이스 구축

- 데이터 백업

- CVM에 로컬 파일 업로드

로컬 파일을 CVM에 복사

Windows 시스템에서 MSTSC를 통해 Windows CVM에 파일 업로드

MacOS 시스템에서 MRD를 사용하여 Windows CVM에 파일 업로드

Linux 시스템에서 RDP를 사용하여 Windows CVM에 파일 업로드

Windows 시스템에서 WinSCP를 사용하여 Linux CVM에 파일 업로드

Linux 또는 MacOS 시스템에서 SCP를 사용하여 Linux CVM에 파일 업로드

Linux 시스템에서 FTP를 사용하여 CVM에 파일 업로드

Windows 시스템에서 FTP를 사용하여 CVM에 파일 업로드

기타 시나리오 관련 작업

CVM의 내부 네트워크를 통한 COS 액세스

Linux 인스턴스 데이터 복구

Windows 인스턴스 디스크 용량 관리

Linux 인스턴스에서 수동으로 커널 변경

CVM에서 Windows 기반 AD 도메인 설정

네트워크 성능 테스트

네트워크 처리량 성능 테스트

개요

netperf 테스트 방법

DPDK 테스트 방법

Linux 시스템에서 USB/IP를 사용하여 USB 장치 원격 공유

Windows 시스템에서 RemoteFx를 사용하여 USB 장치 리디렉션

AVX512를 통한 CVM에서의 AI 애플리케이션 가속

Tencent SGX 보안 컴퓨팅 환경 구축

M6p 인스턴스 영구 메모리 설정

모범 사례

CVM 모범 사례

최종 업데이트 날짜: : 2024-02-02 10:56:28

본 문서는 사용자가 최대한 안전하고 신뢰적인 클라우드 서버를 활용할 수 있도록 도와줍니다.

보안 및 네트워크

액세스 제한: 방화벽 ([보안 그룹](#)) 사용을 통해 신뢰하는 주소의 액세스 인스턴스를 허용하여 액세스를 제한하고 보안 그룹에 가장 엄격한 규칙을 구성합니다. 예를 들면 포트 액세스 및 IP 주소 액세스를 제한합니다.

보안 레벨: 다양한 보안 그룹 규칙을 생성하여 다양한 보안 레벨의 인스턴스 그룹에 적용함으로써 중요한 서비스를 실행하는 인스턴스가 외부에 쉽게 접촉하지 않도록 합니다.

네트워크 논리 격리: [사설 네트워크](#) 사용을 통해 논리 영역을 구분합니다.

계정 권한 관리: 동일한 그룹의 클라우드 리소스가 여러 개의 다양한 계정을 컨트롤할 경우 [정책 시스템](#) 을 사용해 클라우드 리소스에 대한 액세스 권한을 제어합니다.

안전한 로그인: [SSH 키](#) 방식을 사용해 사용자의 Linux류의 인스턴스에 로그인하십시오. [비밀번호 로그인](#)을 사용하는 인스턴스는 불규칙적으로 암호를 수정해야 합니다.

스토리지

하드웨어 스토리지: 신뢰성 요구가 매우 높은 데이터에 대해 Tencent Cloud Cloud Block Storage (CBS) 를 사용해 데이터의 지속적인 스토리지 신뢰성을 확보하십시오. [로컬 디스크](#)는 가능한 선택하지 마십시오. 자세한 내용은 [CBS 제품 설명서](#)를 참조하십시오.

백업 및 복구

동일 리전 인스턴스 백업: 사용자 정의 미러 이미지 및 클라우드 드라이브 스냅샷 방식을 사용해 사용자의 인스턴스 및 서비스 데이터를 백업할 수 있습니다. [CBS 스냅샷](#) 및 [사용자 정의 이미지 생성](#)을 참조하십시오.

리전 간 인스턴스 백업: [미러 이미지 복사](#)를 사용해 리전 간 복제 및 인스턴스 백업을 실행할 수 있습니다.

인스턴스 장애 차단: [EIP](#)를 통한 도메인 이름 매핑은 서버를 사용할 수 없는 경우 서비스 IP를 다른 클라우드 서버 인스턴스로 빠르게 재지정하여 인스턴스 장애를 차단합니다.

모니터링과 알람

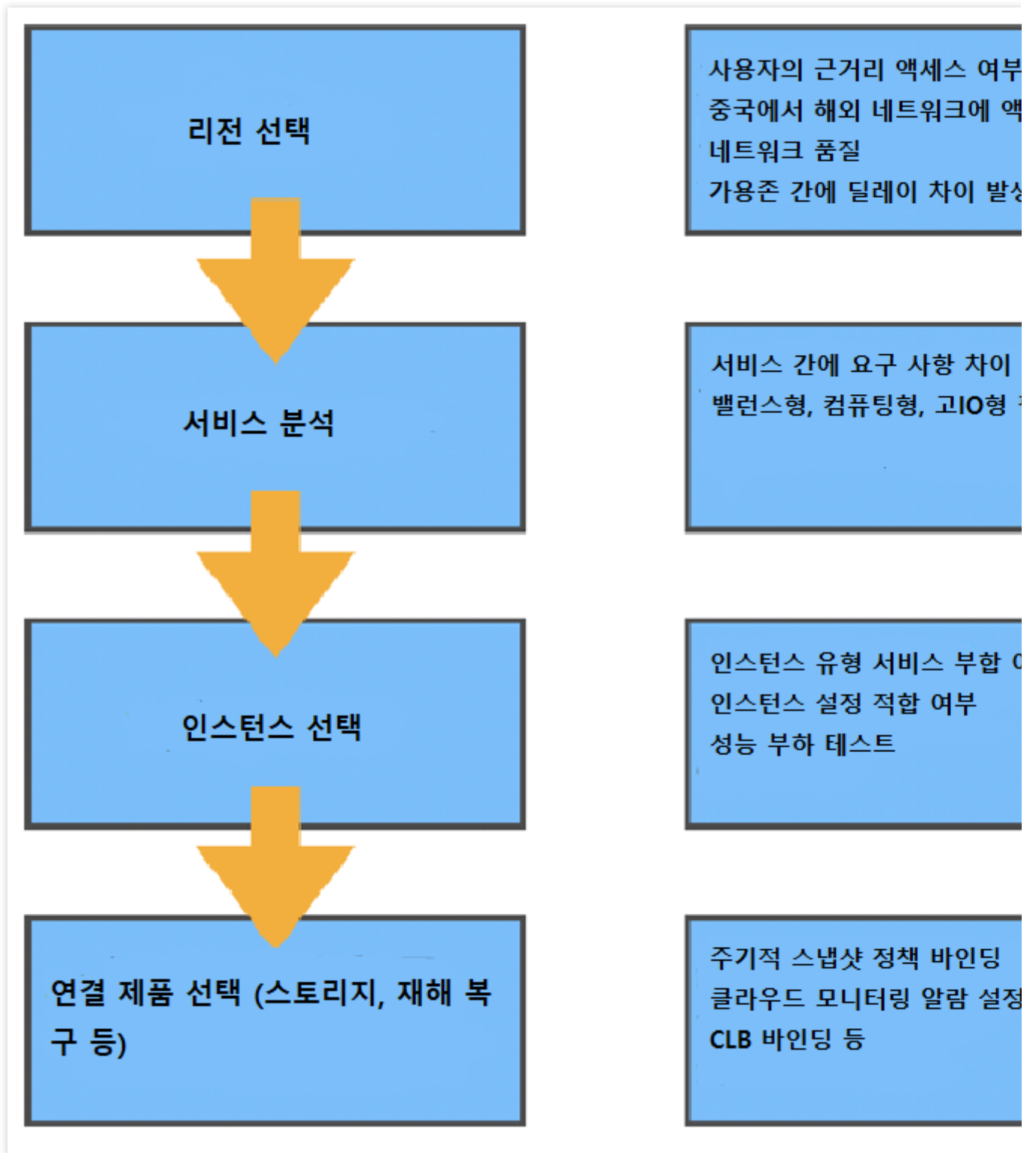
모니터링과 응답 이벤트: 정기적으로 데이터를 모니터링하고 적절한 알람을 설정합니다. 자세한 내용은 [TCOP 제품 설명서](#)를 참조하십시오.

돌발 요청 처리: [오토 스케일링](#)을 사용해 서비스 피크에 있는 클라우드 서버 안정성을 보장하고 비정상 인스턴스를 자동으로 교체할 수 있습니다.

CVM 유형 모범 사례

최종 업데이트 날짜: : 2024-02-02 10:56:28

본 문서는 Cloud Virtual Machine(CVM) 인스턴스 기능, 자주 사용되는 서비스 시나리오, 주의 사항 및 모범 사례 등을 통해 인스턴스 선택 방법을 소개하여 사용자가 실제 서비스 시나리오에 맞춰 CVM을 구매할 수 있도록 도와줍니다. 인스턴스 선택 분석 과정은 다음 이미지와 같습니다.



리전 및 가용존

리전

리전(Region)은 구매한 클라우드 컴퓨팅 리소스가 존재하는 지역 위치를 규정하며 귀하와 귀하의 고객이 해당 리소스에 액세스할 때의 네트워크 상태를 결정합니다.

중국 외 리전 구매의 경우, 네트워크 품질, 관련 컴플라이언스 정책 및 일부 이미지 사용 제한 규정(예: Windows 시스템과 Linux 시스템은 중국 외 리전에서 상호 전환이 불가함 등)을 확인하십시오.

가용존

하나의 리전은 하나 혹은 다수의 가용존(Zone)을 포함하며 동일 리전의 가용존 별로 판매하는 CVM 인스턴스 유형이 다를 수 있습니다. 또한 가용존 간에 리소스 상호 액세스 시, 네트워크 딜레이가 다르게 나타날 수 있습니다.

리전과 가용존에 대한 자세한 내용은 [리전 및 가용존](#)을 참고하십시오.

인스턴스 유형

Tencent Cloud는 여러 종류의 인스턴스 스펙을 포함한 다양한 유형의 인스턴스를 제공합니다. 아키텍처 기준으로 x86 컴퓨팅, ARM 컴퓨팅, 베어 메탈 컴퓨팅, 이중 컴퓨팅(GPU/FPGA), Batch Compute로 구분할 수 있습니다. 특징 기능을 기준으로 표준형, 컴퓨팅형, 메모리형, 고IO형, 빅 데이터형 등으로 구분할 수 있습니다. 본 문서는 인스턴스 특징 기능을 기준으로 구분하였으며 자세한 정보는 다음 내용을 참고하십시오.

표준형

표준형 인스턴스 각 항목의 성능 파라미터는 밸런스가 맞추어져 있으며 web 사이트나 미들웨어 등 대부분의 일반적인 서비스에 적용됩니다. 표준형 인스턴스의 주요 시리즈는 다음과 같습니다.

S 및 SA 시리즈: S와 SA 시리즈는 각각 Intel과 AMD의 핵심입니다. 동일 세대와 설정의 S 시리즈는 SA 시리즈보다 더욱 강력한 싱글 코어 성능을 자랑하는 반면 SA 시리즈는 가성비가 높습니다.

스토리지 최적화형 S5se 시리즈: 최신 가상화 기술 SPDK를 기반으로 스토리지 프로토콜 스택을 최적화하고 CBS 성능을 대폭 향상시켜 대형 데이터베이스, NoSQL 데이터베이스 같은 IO 집약형 서비스에 적합합니다.

네트워크 최적화형 SN3ne 시리즈: 내부 네트워크 송수신 능력이 최고 600만 pps에 달하며 표준형 S3 인스턴스보다 성능이 8배 향상되었습니다. 내부 네트워크 대역폭은 최고 25Gbps까지 지원 가능해져 표준형 S3보다 2.5배 향상되었습니다. 영상 댓글 자막, 라이브 방송, 게임 등 네트워크 패킷 송수신량이 많은 시나리오에 적합합니다.

컴퓨팅형

컴퓨팅형 C 시리즈는 최고의 싱글 코어 컴퓨팅 성능을 자랑하며 트래픽이 많은 Web 프론트 엔드 서버, 대규모 다중 사용자 온라인(MMO) 게임 서버 같은 일괄 처리, 고성능 컴퓨팅, 대형 게임 서버 등 컴퓨팅 집약형 애플리케이션에 적합합니다.

메모리형

메모리형 M 시리즈 인스턴스는 CPU와 메모리 비율이 1:8에 이를 정도로 큰 메모리 공간과 저렴한 메모리 단위 가격을 자랑합니다. MySQL, Redis 같은 고성능 데이터베이스, 분산형 메모리 캐시 등 메모리 작업, 조회, 컴퓨팅이 많이 필요한 애플리케이션에 적합합니다.

고 IO 형

고IO형 IT 시리즈 인스턴스 데이터 디스크는 로컬 디스크 스토리지로 최신 NVME SSD 스토리지 탑재, 높은 랜덤 IOPS, 많은 처리량, 짧은 액세스 딜레이 등 특징을 고루 갖춘 제품입니다. 저렴한 비용으로 최고의 IOPS를 경험할 수

있으며 고성능 관계형 데이터베이스, Elasticsearch 등 강력한 디스크 읽기/쓰기 기능과 짧은 딜레이 시간을 요구하는 고성능 데이터베이스 같은 IO 집약형 서비스에 적합합니다.

설명 :

IT 시리즈 인스턴스의 데이터 디스크는 로컬 스토리지로, 데이터 손실의 위험이 있습니다(예: 호스트 다운 시). 사용자의 애플리케이션이 데이터 신뢰성이 높은 아키텍처가 아니라면 CBS를 데이터 디스크로 선택할 수 있는 인스턴스 사용을 권장합니다.

빅 데이터형

빅 데이터형 D 시리즈 인스턴스는 대량의 스토리지 리소스를 탑재하고 있어, 많은 양을 처리할 수 있습니다. Hadoop 분산형 컴퓨팅, 대량의 로그 처리, 분산형 파일 시스템과 대형 데이터 웨어하우스 등 처리 집약형 애플리케이션에 적합합니다.

설명 :

빅 데이터 모델 D 시리즈 인스턴스의 데이터 디스크는 로컬 디스크로, 데이터 손실의 위험이 있습니다(예: 호스트 다운 시). 사용자의 애플리케이션이 데이터 신뢰성이 높은 아키텍처가 아니라면 CBS를 데이터 디스크로 선택할 수 있는 인스턴스 사용을 권장합니다.

이종 컴퓨팅

이종 컴퓨팅 인스턴스는 GPU, FPGA 등 이종 하드웨어를 탑재하여 실시간 고속 병렬 컴퓨팅과 부동 소수점 컴퓨팅이 가능합니다. 딥러닝, 과학 컴퓨팅, 비디오 코딩/디코딩과 그래픽 워크스테이션 등 고성능 애플리케이션에 적합합니다.

NVIDIA GPU 시리즈 인스턴스는 현재 메이저인 T4/V100 및 최신 세대 A100을 포괄하는 NVIDIA Tesla 시리즈 GPU를 탑재해 뛰어난 범용 컴퓨팅 성능을 제공합니다. 딥러닝 트레이닝/추리, 과학 컴퓨팅 등의 애플리케이션 시나리오에 가장 적합합니다.

CPM 2.0

CPM 2.0은 Tencent Cloud 최신 가상화 기술을 기반으로 연구 개발한 고성능의 베어 메탈 CVM입니다. 가상 컴퓨터의 유연성과 탄력성, 베어 메탈의 안정성을 모두 갖추었으며 네트워크, 데이터베이스 등 Tencent Cloud 전 제품과 손쉽게 결합하여 사용할 수 있습니다. CPM 2.0 인스턴스 제품군은 표준형, 고IO형, 빅 데이터와 이종 컴퓨팅 시나리오를 모두 커버하며 클라우드 전용의 보안 격리된 고성능 물리 서버 클러스터를 분 단위로 구축할 수 있습니다. 또한 3rd party 가상화 플랫폼을 지원하며 내포된 가상화 기술을 사용하여 AnyStack 하이브리드 배포를 구현하고 우수하고 효율적인 하이브리드 클라우드 솔루션을 구현할 수 있습니다.

고성능 컴퓨팅 클러스터

고성능 컴퓨팅 클러스터는 CPM 2.0을 컴퓨팅 노드로 하여 고속 RDMA 인터넷 네트워크가 지원하는 클라우드 컴퓨팅 클러스터를 제공합니다. 자동차 시뮬레이션, 유체역학, 분자동력 같은 대규모 컴퓨팅 시나리오를 폭넓게 지원할 수 있으며 고성능의 이종 리소스를 제공하여 대규모 머신러닝 트레이닝 등의 시나리오를 지원할 수 있습니다.

CVM 인스턴스 유형에 대한 더 자세한 내용은 [인스턴스 스펙](#)을 참고하십시오.

자주 쓰는 서비스 시나리오 모델 추천

서비스 시나리오	상용 소프트웨어	시나리오 소개	권장 모델
Web 서비스	NginxApache	Web 서비스는 일반적으로 개인 웹 사이트, 블로그 및 대형 이커머스 웹 사이트 등을 포함합니다. 이러한 사용 사례에는 컴퓨팅, 스토리지 및 메모리 리소스의 균형이 필요하므로 표준형 인스턴스를 권장합니다.	표준형 S 및 SA 시리즈
미들웨어	Kafka MQ	메시지 큐 서비스는 컴퓨팅과 메모리 리소스에 대한 수요가 상대적으로 균일하여 CBS를 탑재한 표준형 모델을 스토리지로 추천합니다.	표준형 S 시리즈 컴퓨팅형 C 시리즈
데이터베이스	MySQL	데이터베이스는 IO 성능에 대한 요구 사항이 높아 SSD CBS 및 로컬 디스크를 사용할 것을 추천합니다. (로컬 디스크 모델은 데이터 백업이 필요하며 데이터 손실의 리스크가 있습니다).	고IO형 IT 시리즈 메모리형 M 시리즈
캐시	RedisMemcache	캐시형 서비스는 메모리와 컴퓨팅에 대한 요구 사항이 높아 메모리 비율이 높은 메모리형 인스턴스를 추천합니다.	메모리형 M 시리즈
빅 데이터	HadoopES	빅 데이터 서비스는 대량의 스토리지가 필요하고 IO 처리량에 대한 요구 사항도 어느 정도 있기 때문에 전용 빅 데이터형 D 시리즈를 추천합니다. (로컬 디스크 모델은 데이터 백업이 필요하며 데이터 손실의 리스크가 있습니다).	빅 데이터형 D 시리즈
고성능 컴퓨팅	StarCCMWRF-Chem	고성능 컴퓨팅 서비스는 뛰어난 단일 머신 컴퓨팅 성능과 고효율의 멀티 머신 확장 능력이 필요합니다. 고속 RDMA 네트워크의 고성능 컴퓨팅 클러스터 또는 컴퓨팅형 인스턴스 패밀리를 조합하여 사용할 것을 권장합니다.	고성능 컴퓨팅 클러스터컴퓨팅형 C 시리즈
가상화	KvmOpenStack	가상화 애플리케이션은 클라우드 서버에 가상화 기능이 내포되어 있어야 하며, 성능 부하 추가 없이도 기존 베어 머신과 동일한 성능을 유지해야 합니다. CPM 2.0 제품을 추천합니다.	고성능 컴퓨팅 클러스터CPM 2.0
비디오 렌더링	UnityUE4	비디오 렌더링 시나리오는 DirectX와 OpenGL 등 그래픽 및 이미지 처리 API 지원이 필요하기 때문에 GPU 렌더링형 GN7vw를 추천합니다.	GPU 렌더링형 GN7vw
AI 컴퓨팅	TensorFlowCUDA	AI 컴퓨팅 서비스는 프로세싱 기능과 병행되어야 하며 GPU 연산 기능, 비디오 메모리에 대해 명확한 요구 사항이 있습니다.	GPU 컴퓨팅형고성능 컴퓨팅 클러스터

관련 제품

상용 클라우드 서비스 조합 추천

실제 서비스 시나리오와 결합하여 다른 Tencent Cloud 제품과 함께 사용할 수 있습니다. 본 문서는 전형적인 Web 사이트 구축 아키텍처를 예로 들어 다음 이미지와 같이 클라우드 서비스를 결합하여 사용할 것을 권장합니다.



기타 클라우드 서비스

실제 니즈에 따라 다른 클라우드 서비스를 선택할 수 있습니다. 예를 들어 기본 서비스 구축이 완료된 후, 견고한 시스템 아키텍처와 안전한 데이터를 보장하기 위해 일정한 재해 복구 조치를 취할 수 있습니다. 또한 다음 Tencent Cloud 제품과 결합하여 재해 복구 솔루션을 구현할 수 있습니다.

스냅샷

스냅샷은 빠르고 효율적인 데이터 보호 서비스이자 매우 중요하고 유효한 데이터 재해 복구 조치입니다. 일상적인 데이터 백업, 빠른 복구, 데이터를 생성하는 복제 애플리케이션, 빠른 환경 구축 등이 필요한 서비스 시나리오에 사용할 것을 권장합니다. 스냅샷 제작에 약간의 비용이 발생할 수 있습니다. 자세한 내용은 [스냅샷 과금 개요](#)를 참고하십시오.

TCOP

클라우드 리소스에 대한 정보 규칙을 설정하는 것도 비즈니스 운영에 필수적입니다. TCOP에서 텐센트 클라우드 서비스의 리소스 활용도, 애플리케이션 성능, 운영 현황 등 종합적인 정보를 볼 수 있다. 이 플랫폼은 또한 다중 메트릭 모니터링, 사용자 지정 경고, 교차 지역 및 교차 프로젝트 인스턴스 그룹화, 시각적 모니터링을 위한 Dashboard, Prometheus 호스팅과 같은 기능을 제공합니다. TCOP은 Tencent Cloud 서비스의 긴급 상황 감지 및 처리를 도와 시스템 안정성을 향상하고 OPS 효율성을 개선하며 OPS 비용을 절감할 수 있습니다.

CLB

CLB 서비스를 사용하여 단일 장애 지점으로부터 비즈니스를 보호할 수 있습니다. CLB 서비스는 버추얼 서비스 주소 (VIP)를 설정하여 같은 리전의 다수의 CVM 인스턴스를 성능과 가용성이 우수한 애플리케이션 서비스 풀로 가상화하는 것입니다. 애플리케이션에서 지정한 방식에 따라 클라이언트의 네트워크 요청을 CVM 풀로 배포할 수 있습니다. CLB 서비스는 CVM 풀의 CVM 인스턴스 상태를 확인하고 비정상 상태의 인스턴스를 자동으로 격리하여 CVM의 단일 실패 지점 문제를 해결하고 애플리케이션의 전반적인 서비스 성능을 향상시킵니다.

관련 문서

[리전 및 가용존](#)

[인스턴스 스펙](#)

웹사이트 구축 방법

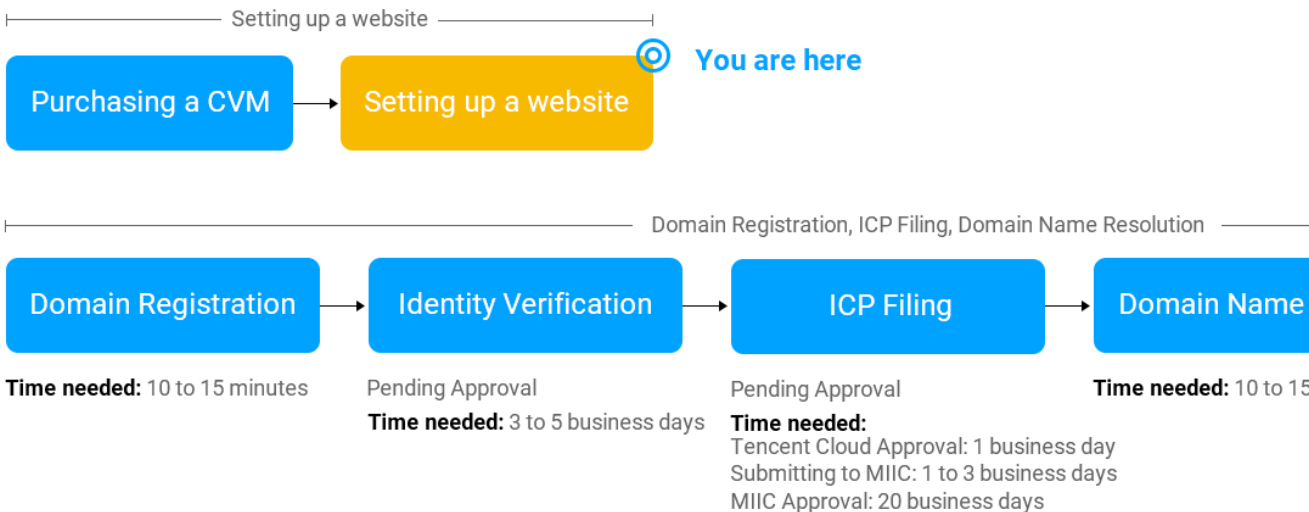
최종 업데이트 날짜: : 2024-02-02 10:56:29

CVM 구입 후 구입한 서버에서 자신만의 웹 사이트나 포럼을 구축할 수 있습니다.

설명 :

또한 Lighthouse를 통해 ‘원클릭 구축’이 가능하며, 직접 설정할 필요가 없습니다. 생성 시 필요한 애플리케이션 이미지를 선택하기만 하면 개인 웹 사이트 구축을 완료할 수 있습니다. 자세한 내용은 [Lighthouse 구입 방법](#)을 참고하십시오.

How to setup a website



구축 방법

Tencent Cloud는 주요 웹 사이트 시스템을 위한 다양한 유형의 튜토리얼을 제공합니다. 구축 방식은 미리 이미지 배포와 수동 구축의 두 종류이며, 그 특징은 다음과 같습니다.

비교 항목	미리 이미지 배포	수동 구축
구축 방식	Tencent 클라우드 마켓의 시스템 이미지 직접 설치 및 배포를 선택합니다.	필요한 소프트웨어를 수동으로 설치합니다. 사용자 정의할 수 있습니다.
특징	패키지 소프트웨어 버전은 비교적 고정되어 있습니다.	패키지 버전을 유연하게 선택할 수 있습니다.

소요 시간	비교적 짧음. 원클릭 배포.	비교적 김. 관련 소프트웨어 직접 설치.
난이도	비교적 쉬움.	소프트웨어 패키지 버전과 설치 방법에 대해 어느 정도 이해하고 있어야 합니다.

웹 사이트 구축

실제 필요에 따라 다양한 시스템의 개인 웹 사이트 구축을 시작할 수 있습니다.

웹 사이트 유형	구축 방법	설명
WordPress	WordPress(Linux) 수동 구축	WordPress 는 PHP 언어를 사용해 개발된 블로그 플랫폼입니다. 사용자는 PHP와 MySQL 데이터베이스를 지원하는 서버에 개인 웹 사이트를 구축할 수 있습니다. WordPress를 콘텐츠 관리 시스템(CMS)으로 사용할 수도 있습니다.
	WordPress(Linux) 수동 구축	
Discuz!	Discuz! 수동 구축	Discuz!는 PHP+MySQL 아키텍처로 개발된 범용 커뮤니티 포럼입니다. 사용자는 서버에서 간단한 설치 구성을 통해 완전한 포럼 서비스를 배포할 수 있습니다.
LNMP 환경	LNMP 환경 수동 구축 (CentOS 7)	LNMP 환경은 Linux 시스템에서 Nginx + MySQL/MariaDB + PHP로 구성된 웹 사이트 서버 아키텍처를 나타냅니다.
	LNMP 환경 수동 구축 (CentOS 6)	
	LNMP 환경 수동 구축 (openSUSE)	
LAMP 환경	LAMP 수동 구축	LAMP 환경은 Linux 시스템에서 Apache + MySQL/MariaDB + PHP로 구성된 웹 사이트 서버 아키텍처를 나타냅니다.
WIPM 환경	WIPM 수동 구축	WIPM 환경은 Windows 시스템에서 IIS + PHP + MySQL 로 구성된 웹 사이트 서버 아키텍처를 나타냅니다.
Drupal	Drupal 수동 구축	Drupal은 PHP 언어로 작성된 오픈 소스 콘텐츠 관리 프레임워크(CMF)로, 콘텐츠 관리 시스템(CMS)과 PHP 개발 프레임워크(Framework)로 공동 구성됩니다. 사용자는 Drupal을 개인 또는 그룹 웹 사이트 개발 플랫폼으로 사용할 수 있습니다.
Ghost	Ghost 수동 구축	Ghost는 Node.js 기반의 오픈 소스 블로그 플랫폼입니다. 신속한 배포 및 간소화된 온라인 출판물 프로세스 등 기능 특징을 통해, 사용자는 Ghost로 개인 블로그를 빠르게 구축할 수 있습니다.

Microsoft SharePoint 2016	Microsoft SharePoint 2016 구축	Microsoft SharePoint는 Microsoft SharePoint Portal Server 의 약칭으로 기업이 지능형 포털 사이트를 개발할 수 있는 포털 사이트입니다. 이 사이트는 사용자가 비즈니스 프로세스에서 관련 정보를 더 잘 이용하고 더 효율적으로 작업할 수 있도록 합니다.
---------------------------	--	--

관련 작업

개인 웹 사이트는 도메인 가입, 웹 사이트 ICP 비안, 리졸브 등의 작업을 거친 후에야 외부 액세스가 가능합니다. 개인 웹 사이트를 CVM에 배치 완료했으며, 웹 사이트를 인터넷에 배포할 계획인 경우, 사용 가능한 도메인을 준비합니다.

환경 구축

환경 개요 구축

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

본 문서를 참고하여 CVM에 다양한 개발 환경을 구축할 수 있습니다. CVM이 없다면 [CVM 구매 페이지](#)에서 구매할 수 있습니다.

작업 순서

다음 문서를 참고하여 다양한 개발 환경을 수동 배포하거나 Tencent Cloud 서비스 마켓플레이스의 이미지를 사용하여 원클릭으로 배포할 수 있습니다.

- [LNMP 환경 구축](#)
- [LAMP 환경 구축](#)
- [Java Web 환경 구축](#)
- [WIPM 환경 구축](#)
- [Node.js 환경 구축](#)

환경 구축에 문제가 발생한 경우 [환경 구축 FAQ](#)를 참조하십시오.

IIS 서비스 설치

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

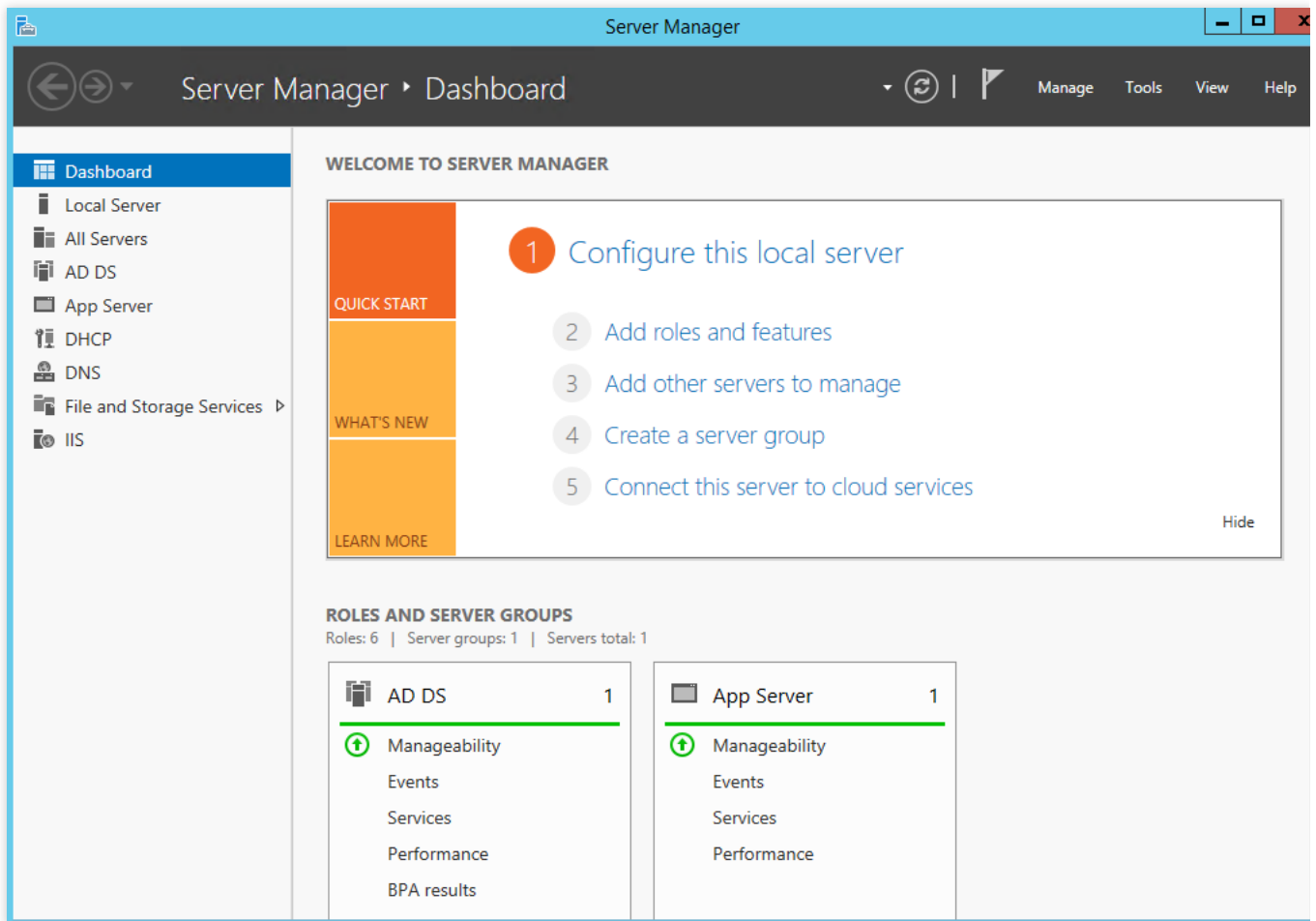
본 문서는 Windows Server 2012 R2 운영 체제와 Windows Server 2008 운영 체제를 예로, Windows CVM에서 IIS 역할 추가 및 설치 방법에 대해 소개합니다.

작업 순서

Windows Server 2012 R2 운영 체제

1. Windows CVM에 로그인합니다.
2. 아래 이미지와 같이 운영 체제 인터페이스에서

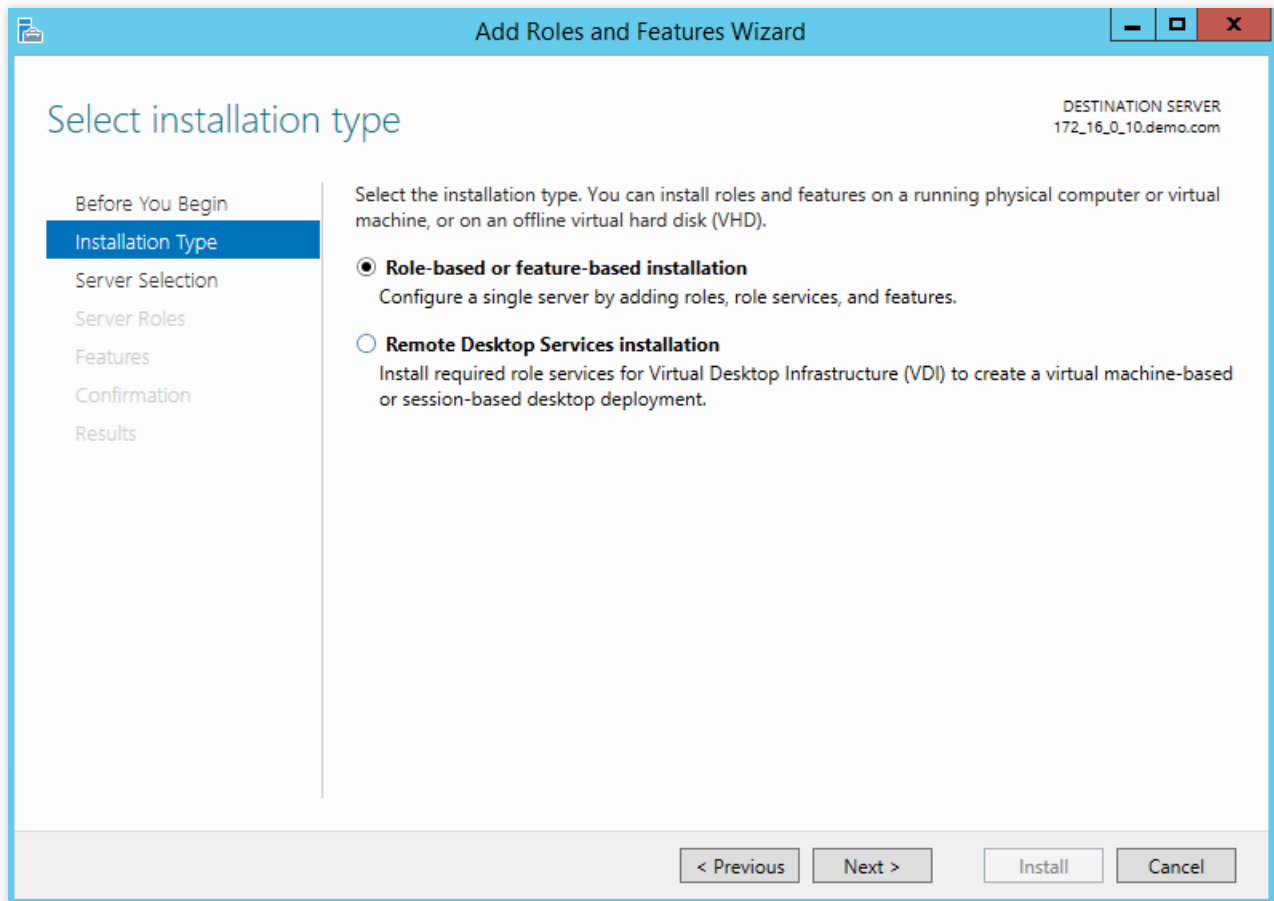
를 클릭하여 서버 관리자를 엽니다.



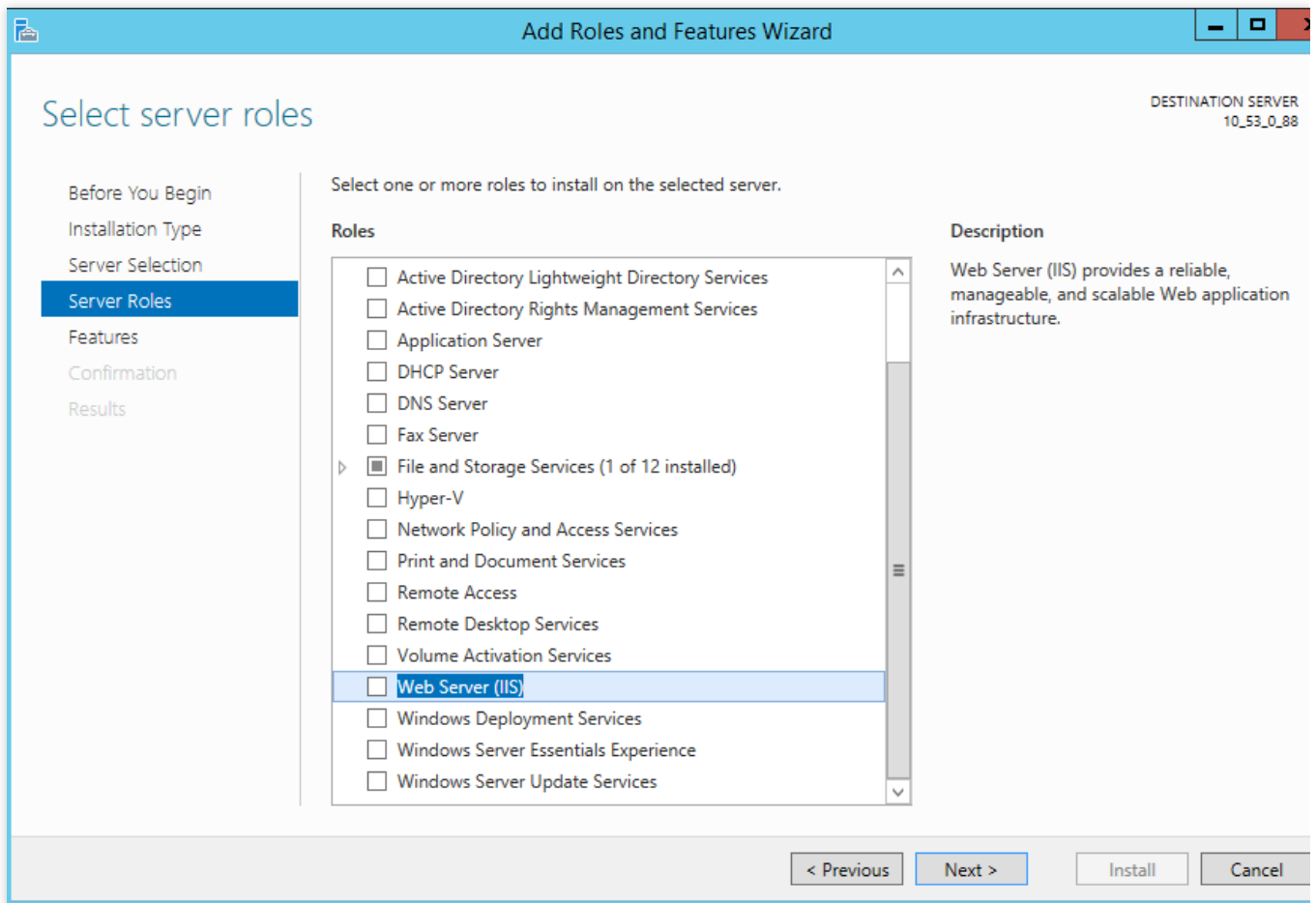
3. [역할 및 기능 추가]를 클릭하면 '역할 및 기능 추가 마법사' 창이 팝업됩니다.

4. '역할 및 기능 추가 마법사' 창에서 [다음]을 클릭합니다.

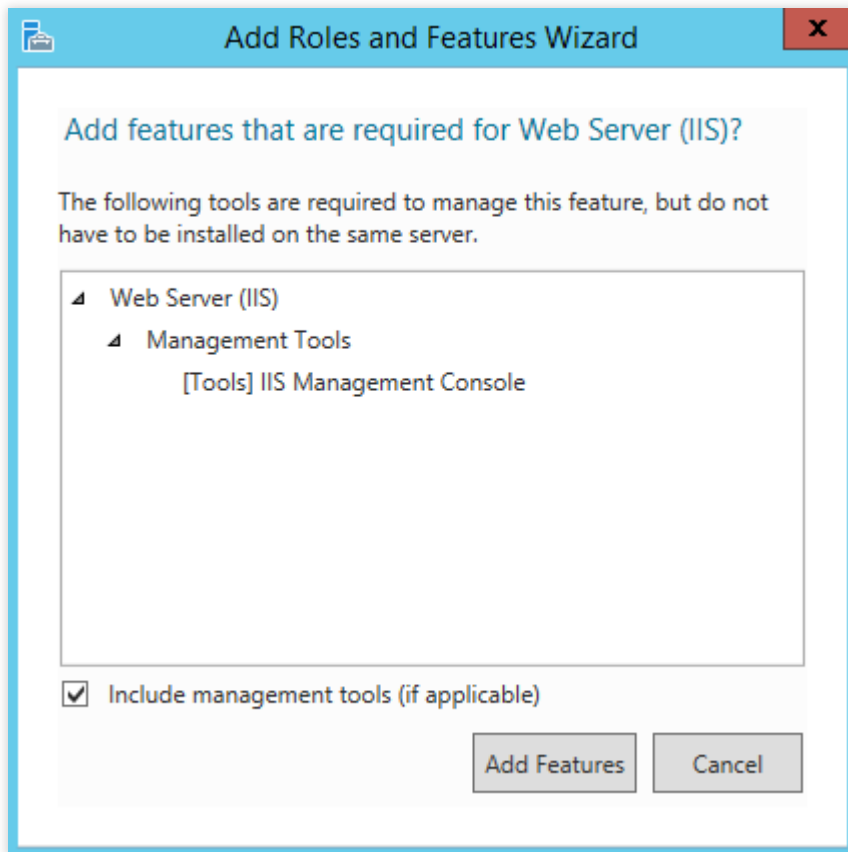
5. 아래 이미지와 같이 '설치 유형 선택' 인터페이스에서 [역할 기반 또는 기능 기반 설치]를 선택하고, [다음]을 2회 연속 클릭합니다.



6. 아래 이미지와 같이, '서버 역할 선택' 인터페이스에서 [웹 서버(IIS)]를 선택하고 [다음]을 클릭합니다.
'Web 서버(IIS)에 필요한 기능 추가' 대화 상자가 팝업됩니다.

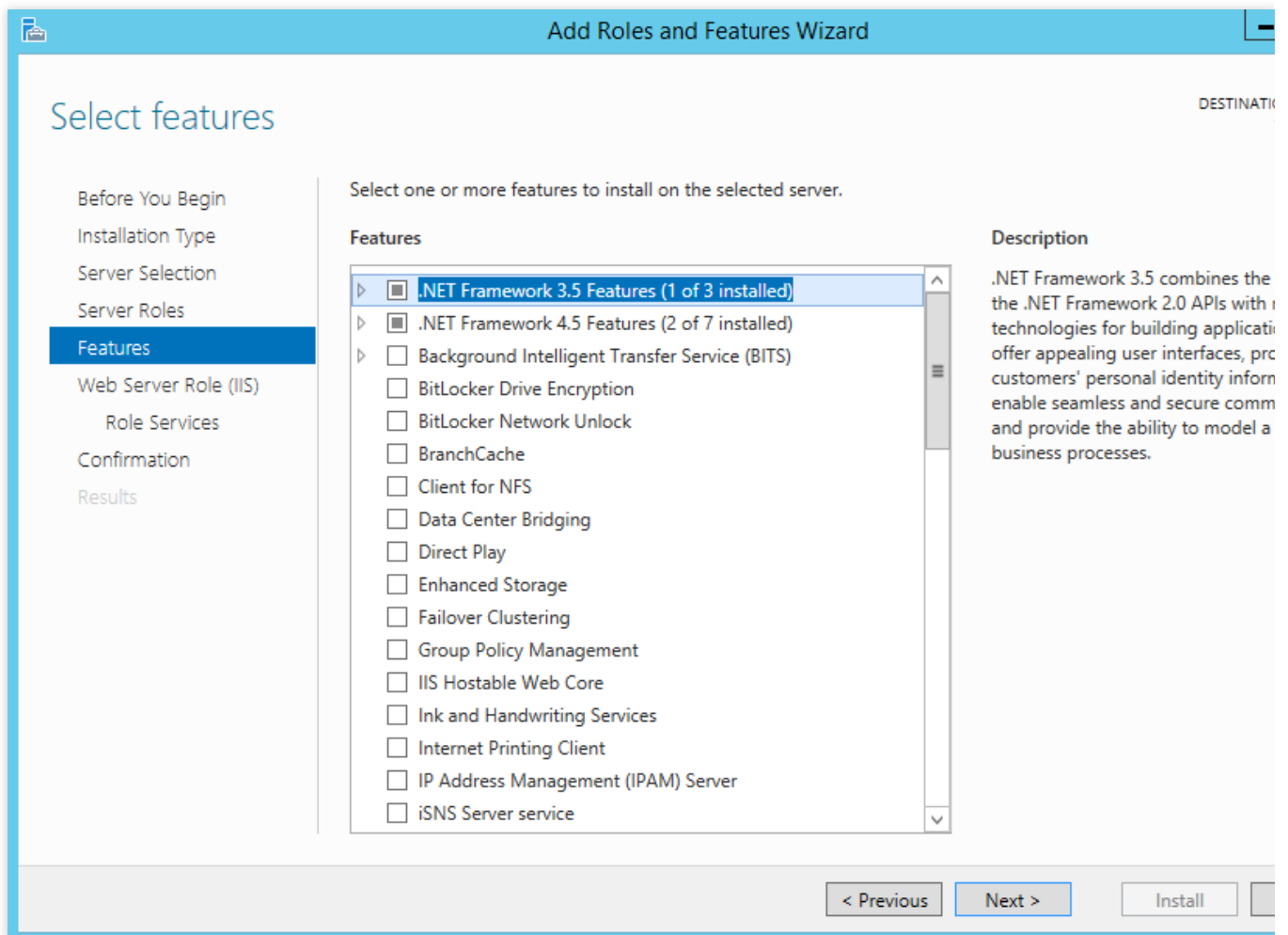


7. 아래 이미지와 같이 'Web 서버(IIS)에 필요한 기능 추가' 대화 상자가 팝업되면 [기능 추가]를 클릭합니다.

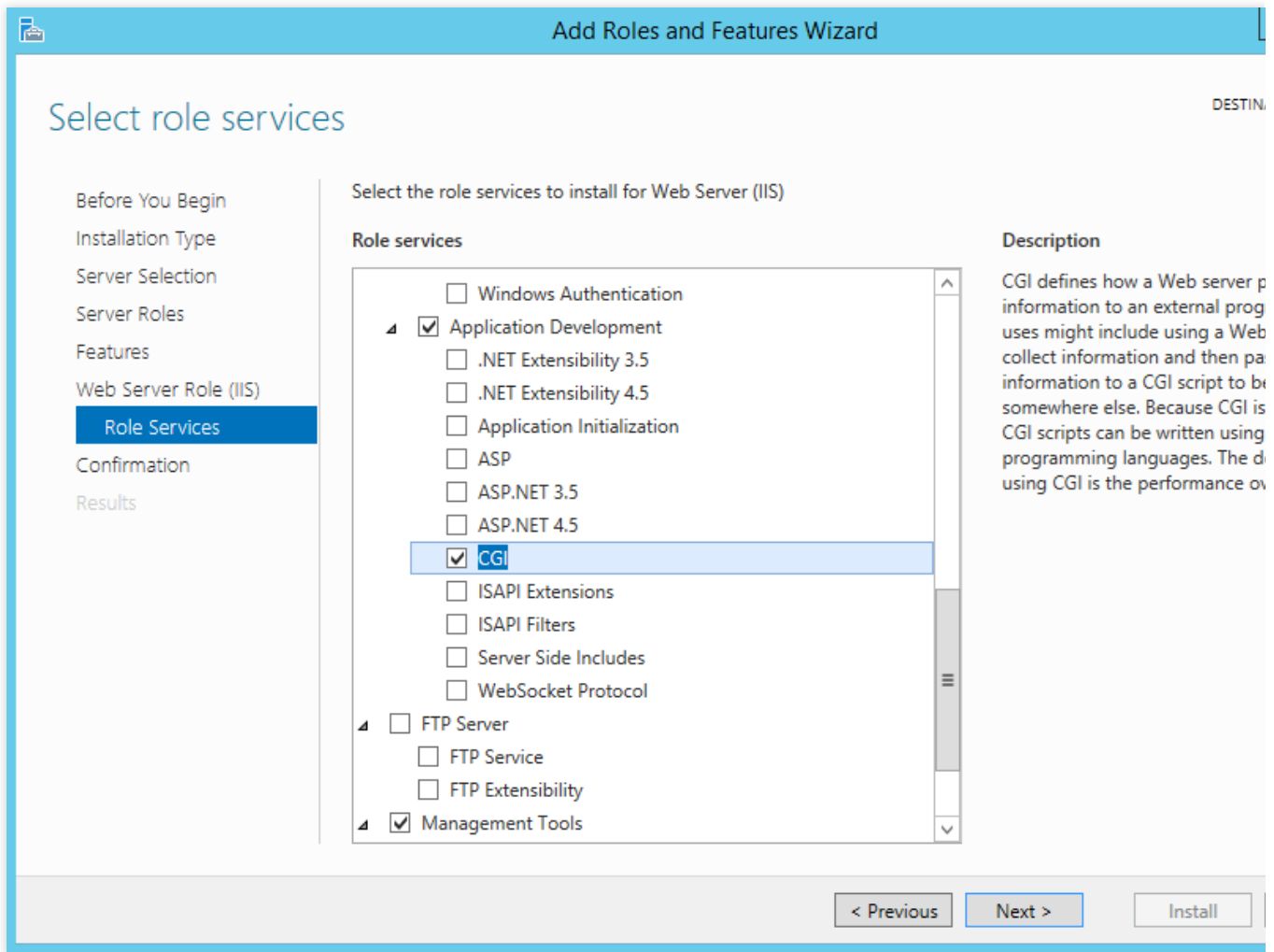


8. [다음]을 클릭합니다.

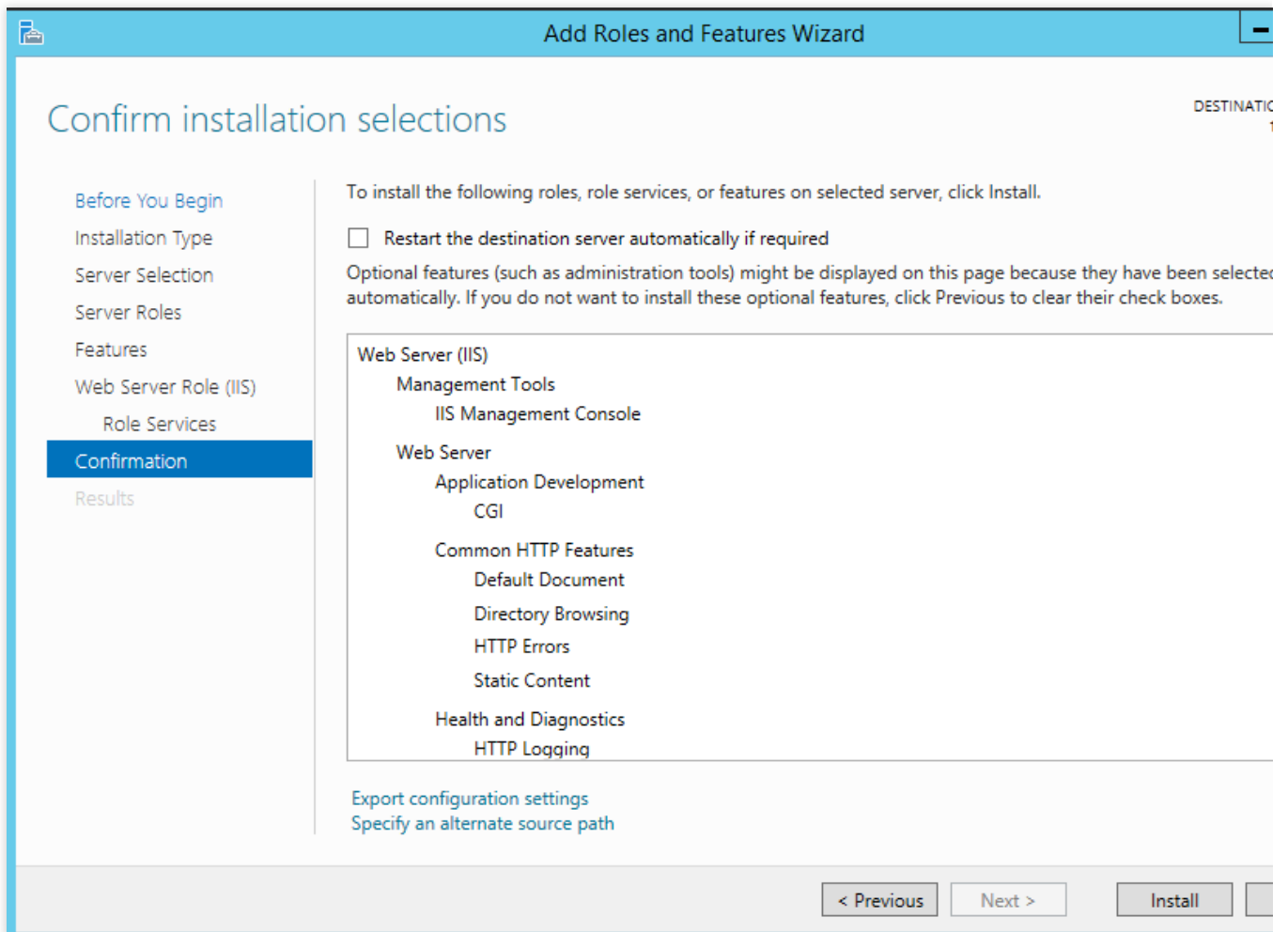
9. 아래 이미지와 같이 '기능 선택' 인터페이스에서 [.NET Framework 3.5 기능]을 선택하고 [다음]을 2회 연속 클릭합니다.



10. 아래 이미지와 같이, '역할 서비스 선택' 인터페이스에서 [CGI]를 선택하고 [다음]을 클릭합니다.

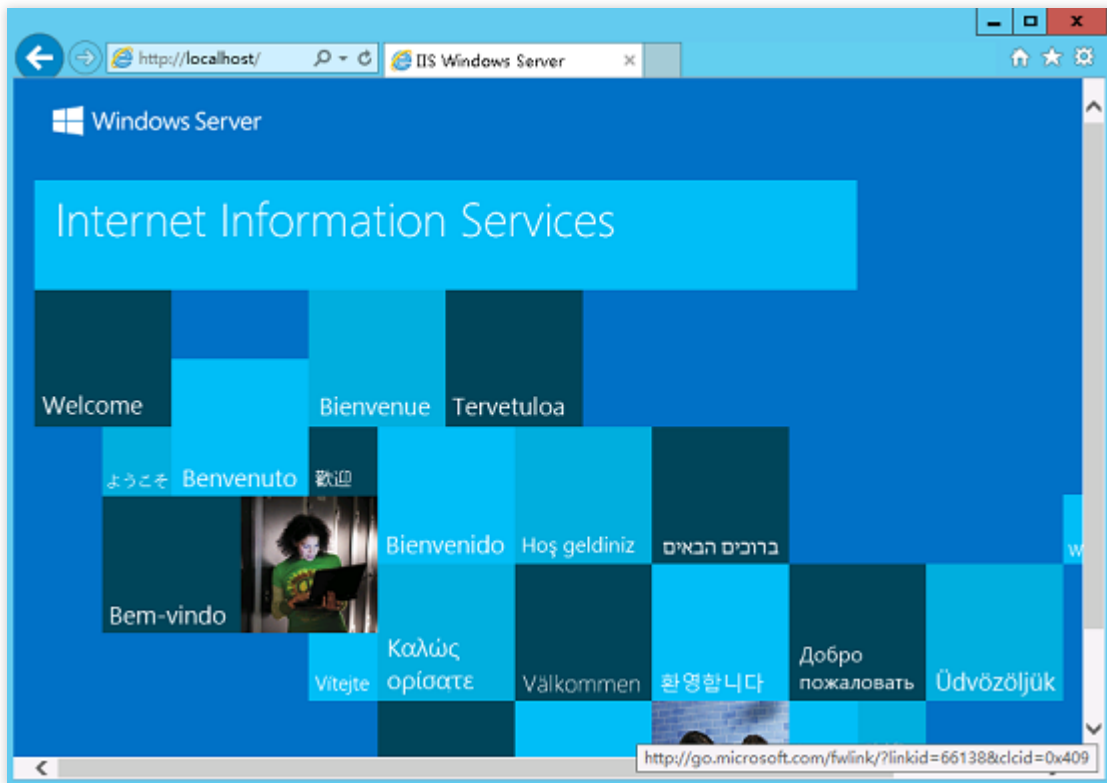


11. 아래 이미지와 같이 설치 정보를 확인한 후 [설치]를 클릭하고 설치가 완료될 때까지 기다립니다.



12. 설치 완료 후 CVM의 브라우저에서 `http://localhost/` 에 액세스하여 IIS가 성공적으로 설치되었는지 확인합니다.

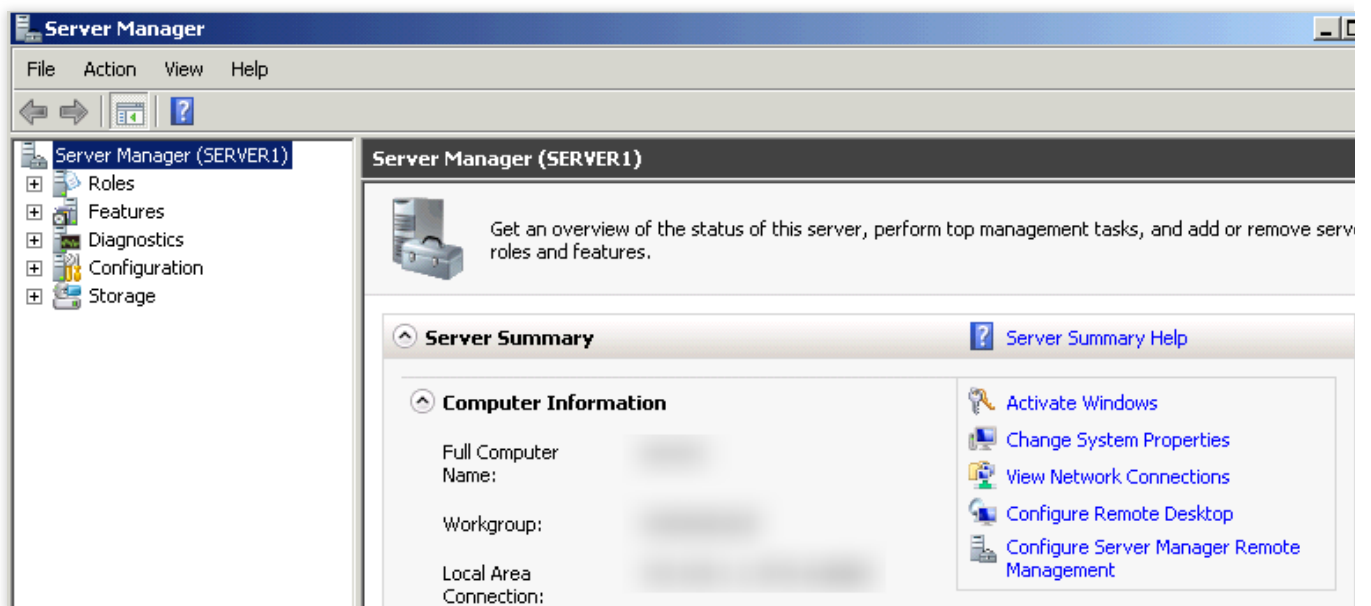
다음과 같은 인터페이스가 나타나면 설치 성공입니다.



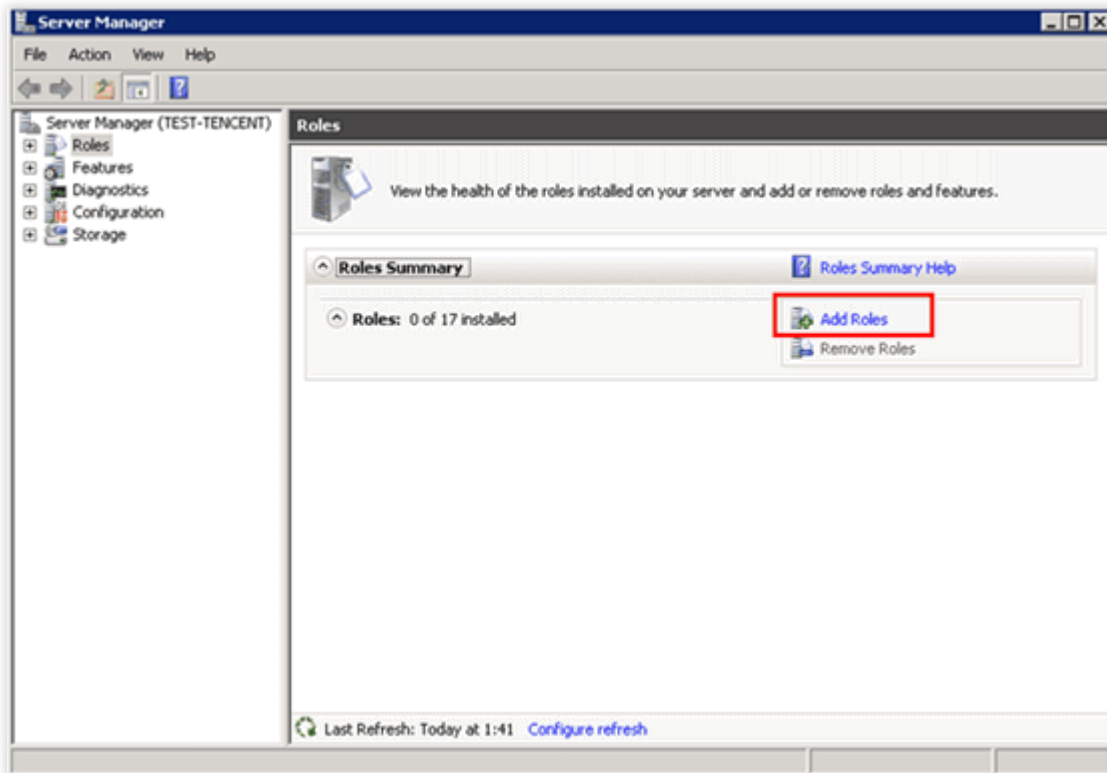
Windows Server 2008 운영 체제

1. Windows CVM에 로그인합니다.
2. 아래 이미지와 같이 운영 체제 인터페이스에서

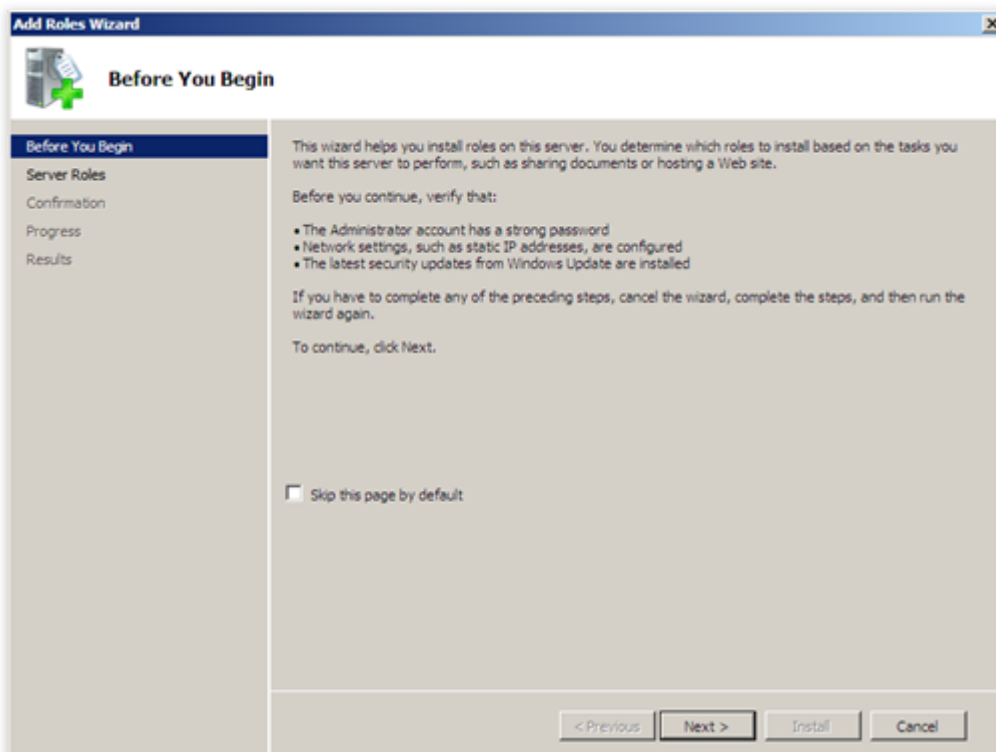
를 클릭하여 서버 관리자를 엽니다.



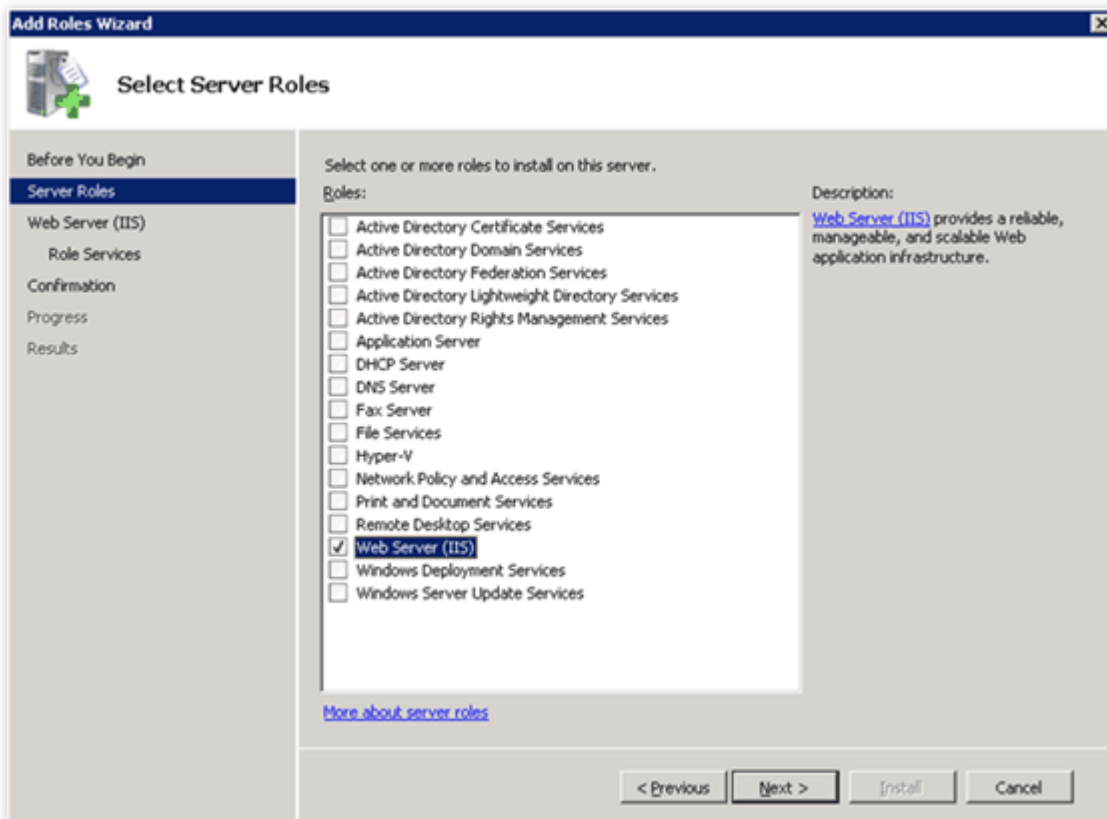
3. 아래 이미지와 같이 왼쪽 사이드바에서 [역할]을 선택하고, 오른쪽 창에서 [역할 추가]를 클릭합니다.



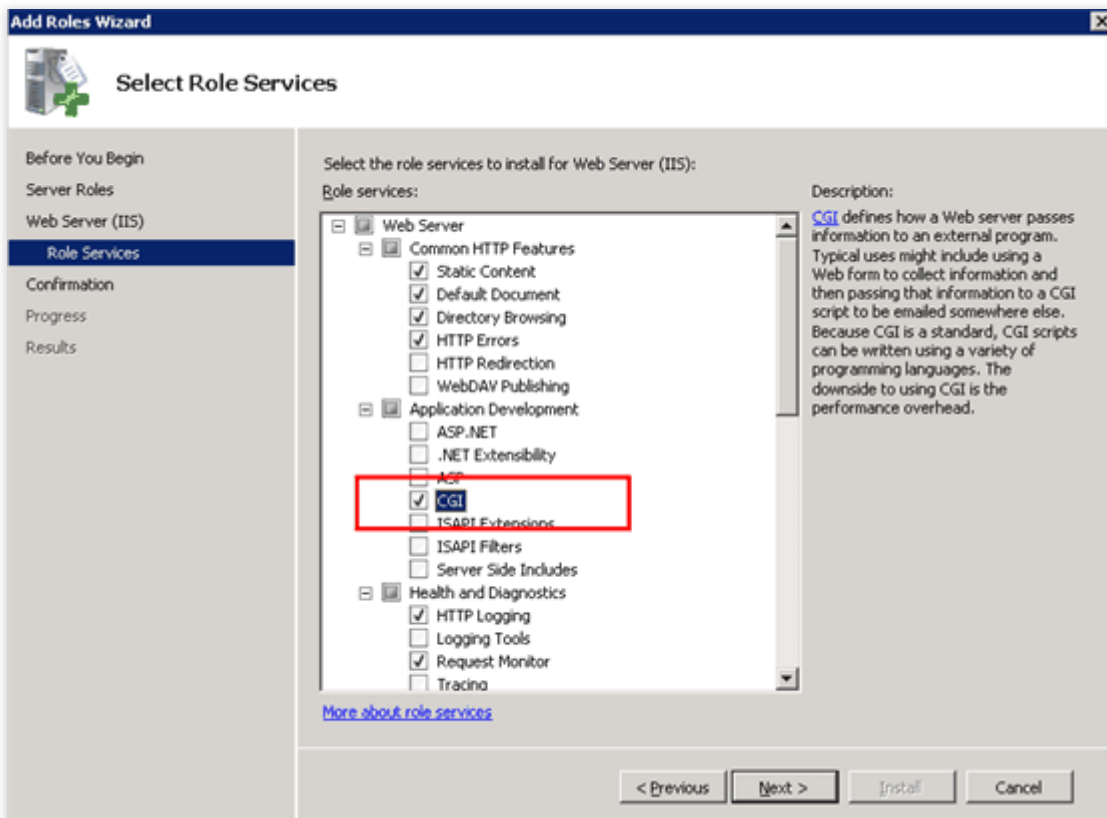
4. 아래 이미지와 같이 '역할 추가 마법사' 창에서 [다음]을 클릭합니다.



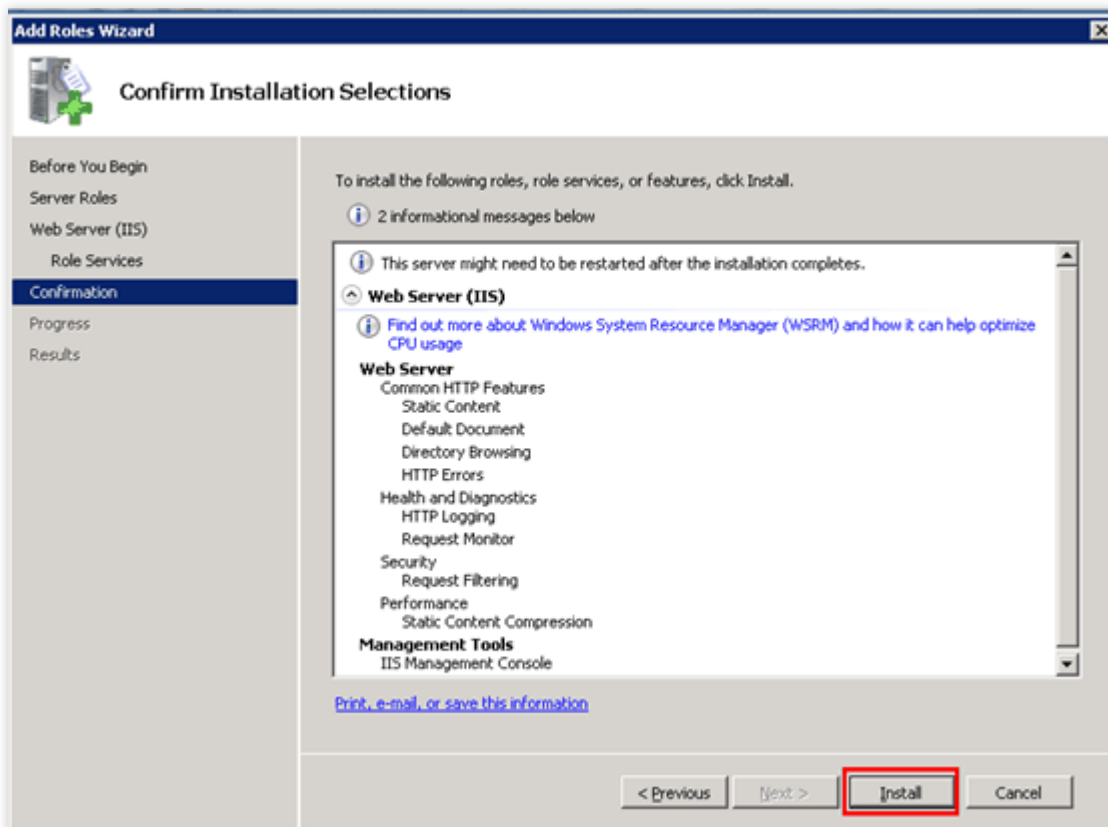
5. 아래 이미지와 같이 '서버 역할 선택' 인터페이스에서 [Web 서버(IIS)]를 선택하고 [다음]을 2회 연속 클릭합니다.



6. 아래 이미지와 같이, '역할 서비스 선택' 인터페이스에서 [CGI]를 선택하고 [다음]을 클릭합니다.



7. 아래 이미지와 같이 설치 정보를 확인한 후 [설치]를 클릭하고 설치가 완료될 때까지 기다립니다.



8. 설치 완료 후 CVM의 브라우저에서 `http://localhost/` 에 액세스하여 IIS가 성공적으로 설치되었는지 확인합니다.

다음과 같은 인터페이스가 나타나면 설치 성공입니다.



웹 사이트 구축

웹 사이트 개요 구축

최종 업데이트 날짜: : 2024-02-02 10:56:28

본 문서를 참고하여 CVM에 웹 사이트를 구축할 수 있습니다. CVM이 없다면 [CVM 구매 페이지](#)에서 구매할 수 있습니다.

1단계: 웹 사이트 배포

다음 문서를 참고하여 웹 사이트를 수동으로 만들어 배포할 수 있습니다.

- [웹 사이트 구축 방법](#)
- [WordPress 개인 사이트 구축](#)
- [Discuz! 포럼 구축](#)
- [Drupal 개인 사이트 구축](#)
- [Ghost 블로그 구축](#)

웹 사이트 구축에 문제가 발생한 경우 [웹 사이트 구축 FAQ](#)를 참조하십시오.

2단계: 웹 사이트 배포

사이트 배포 및 구축 완료 후 웹 사이트를 인터넷에 배포하고 액세스 서비스를 제공해야 하는 경우, 도메인 등록, 웹 사이트 ICP비안, 도메인 리졸브가 필요합니다.

WordPress 개인 사이트 구축

WordPress 개인사이트 매뉴얼 구축

최종 업데이트 날짜: : 2024-02-02 10:56:29

작업 시나리오

워드프레스는 PHP로 개발된 블로그 플랫폼입니다. 이 문서에서는 CentOS 7.6이 설치된 Tencent Cloud CVM에서 비공개 WordPress 사이트를 수동으로 구축하는 방법을 설명합니다.

WordPress 사이트를 구축하려면 [CentOS 환경에서 YUM을 통해 소프트웨어 설치](#) 등 일반적인 Linux 명령에 익숙해야 합니다. 또한 관련 소프트웨어 프로그램의 사용법과 버전 호환성 정보를 알아야 합니다.

주의사항 :

Tencent Cloud는 클라우드 마켓의 이미지 환경을 통해 WordPress 사이트를 배포할 것을 권장하며, 수동 구축 과정이 오래 걸릴 수 있습니다.

소프트웨어

다음 소프트웨어 프로그램은 WordPress 사이트를 구축하는 데 사용됩니다.

Linux: Linux 운영 체제, 본 문서는 CentOS 7.6을 예시로 사용합니다.

Nginx: Web 서버, 본 문서는 Nginx 1.17.5을 예시로 사용합니다.

MariaDB: 데이터베이스, 본 문서는 MariaDB 10.4.8을 예시로 사용합니다.

PHP: 스크립트 언어, 본 문서는 PHP 7.2.22를 예시로 사용합니다.

WordPress: 블로그 플랫폼, 본 문서는 WordPress 5.0.4를 예시로 사용합니다.

작업 단계

1단계: CVM(Cloud Virtual Machine) 로그인

[Linux 인스턴스에 로그인](#)합니다. 실제 작업 스타일에 따라 다른 로그인 방식을 선택할 수도 있습니다.

원격 로그인 소프트웨어를 사용하여 [Linux 인스턴스 로그인](#)

SSH를 사용하여 [Linux 인스턴스에 로그인](#)

2단계: LNMP 환경 수동 구축

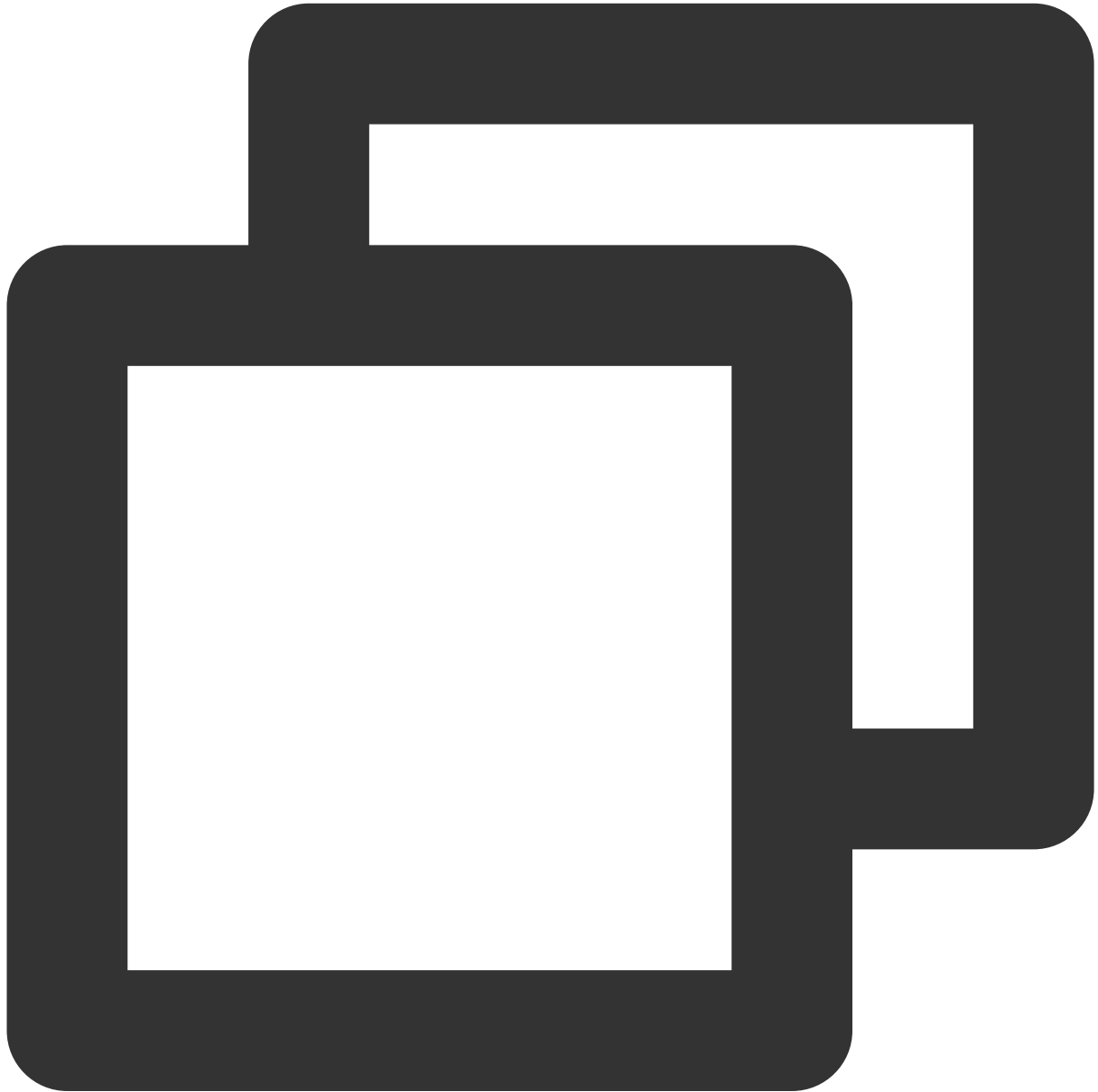
LNMP는 Linux, Nginx, MariaDB 및 PHP의 약칭입니다. 웹 서버를 위한 가장 일반적인 실행 환경 중 하나입니다. CVM 인스턴스를 생성하고 로그인한 후 [LNMP 환경 수동 구축](#)을 참고하여 LNMP 환경을 구축할 수 있습니다.

3단계: WordPress 데이터베이스 구성

주의사항 :

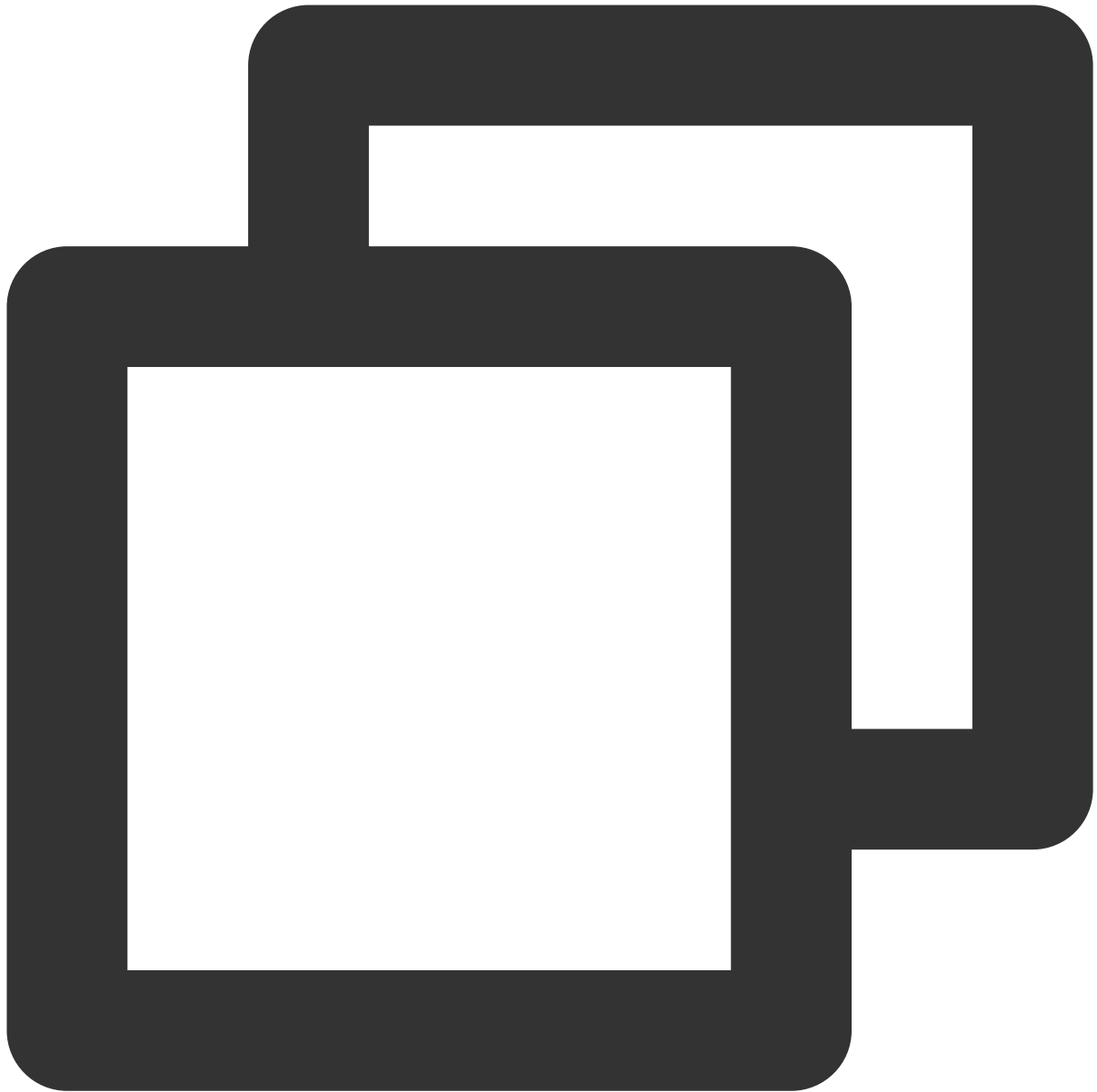
사용자 인증 방법은 MariaDB 버전에 따라 다릅니다. 자세한 내용은 MariaDB 공식 웹 사이트를 참고하십시오.

1. 아래의 명령어를 실행하여 MariaDB에 진입하십시오.



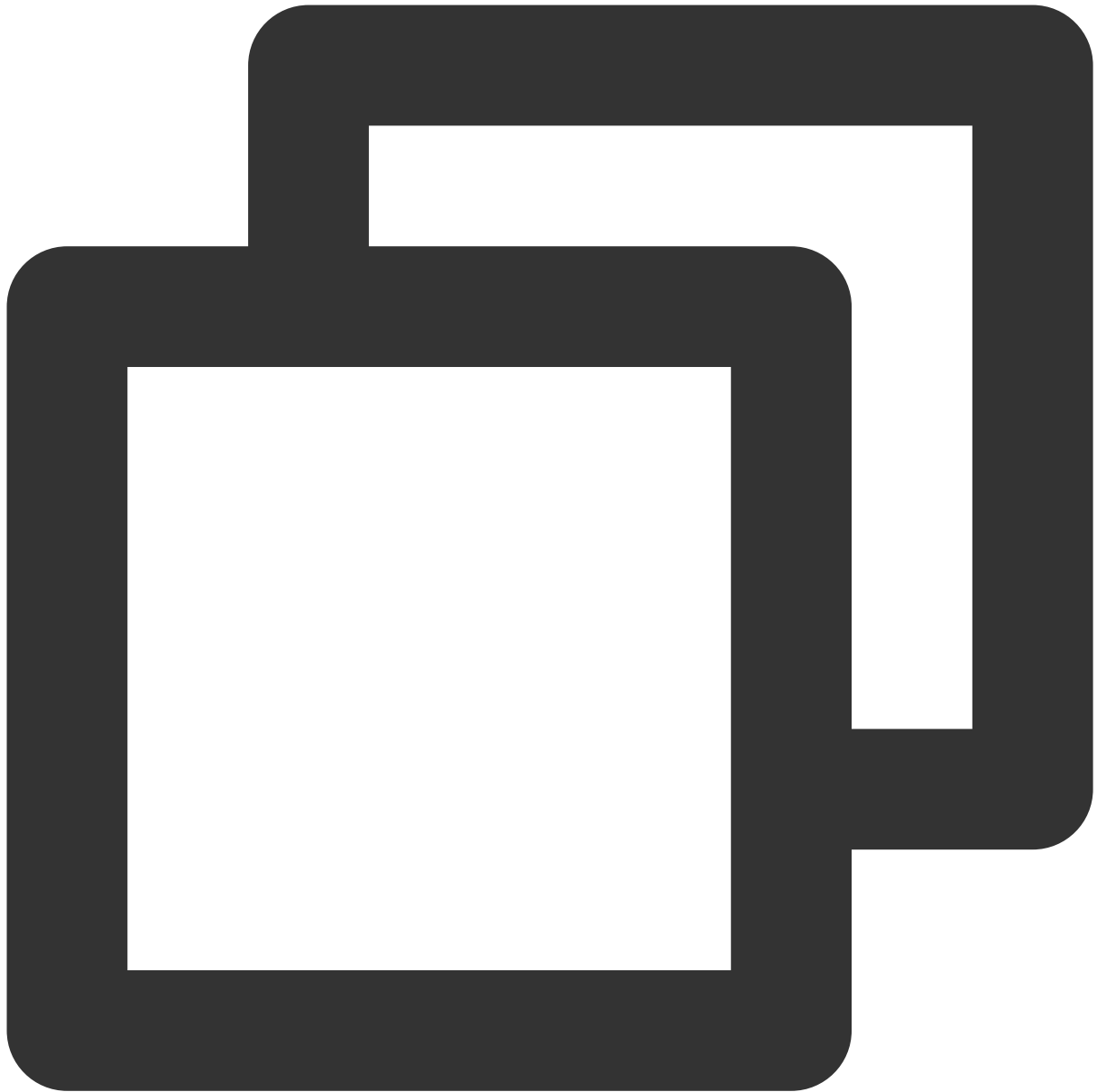
```
mysql
```

2. 아래의 명령어를 실행하여 “wordpress”와 같은 MariaDB 데이터베이스를 생성하십시오.



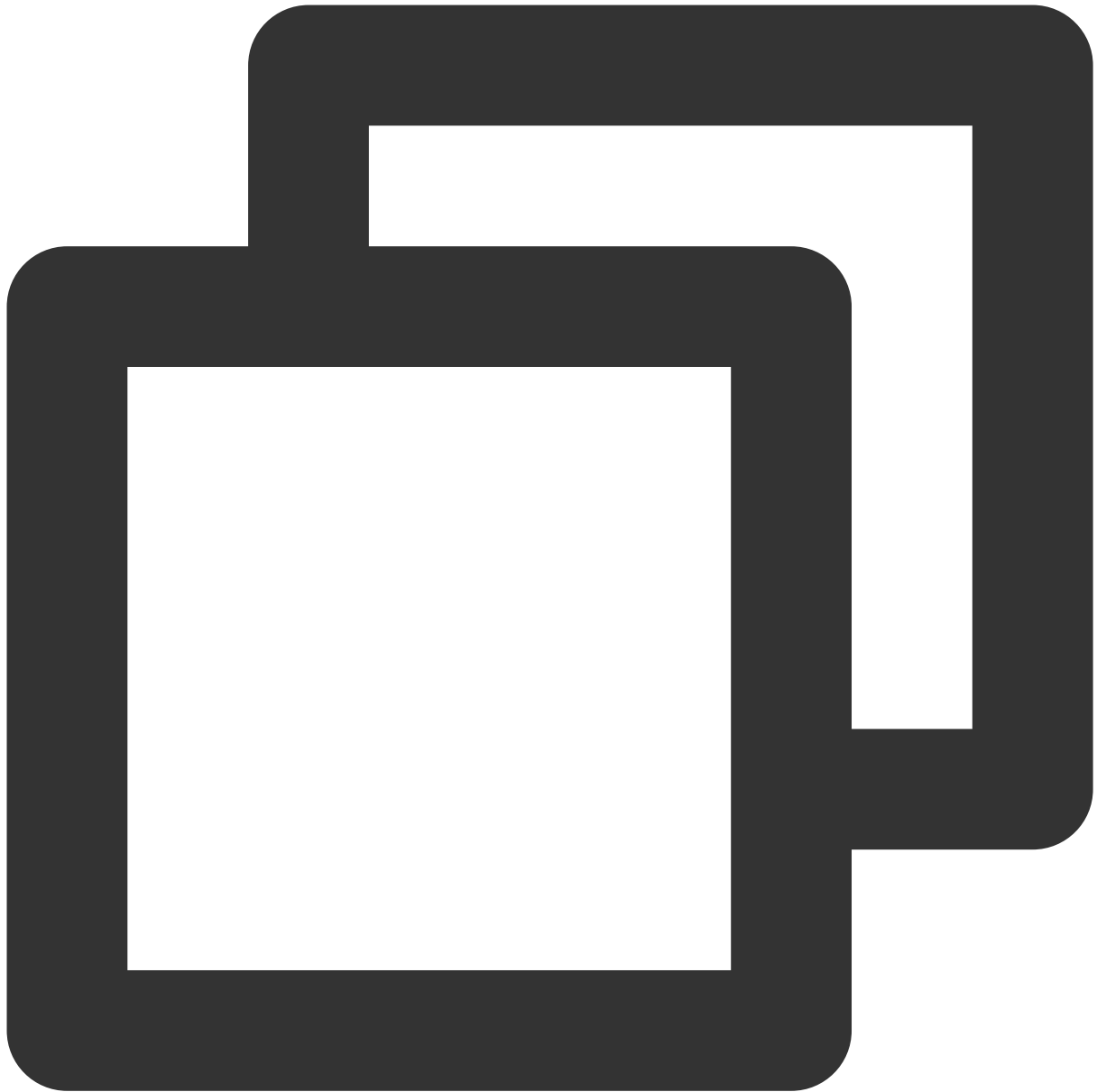
```
CREATE DATABASE wordpress;
```

3. 아래의 명령어를 실행하여 “user”와 같은 새로운 사용자를 추가하십시오. 로그인 비밀번호는 ‘123456’입니다.



```
CREATE USER 'user'@'localhost' IDENTIFIED BY '123456';
```

4. 아래의 명령어를 실행하여 사용자에게 “wordpress” 데이터베이스의 모든 권한을 부여하십시오.

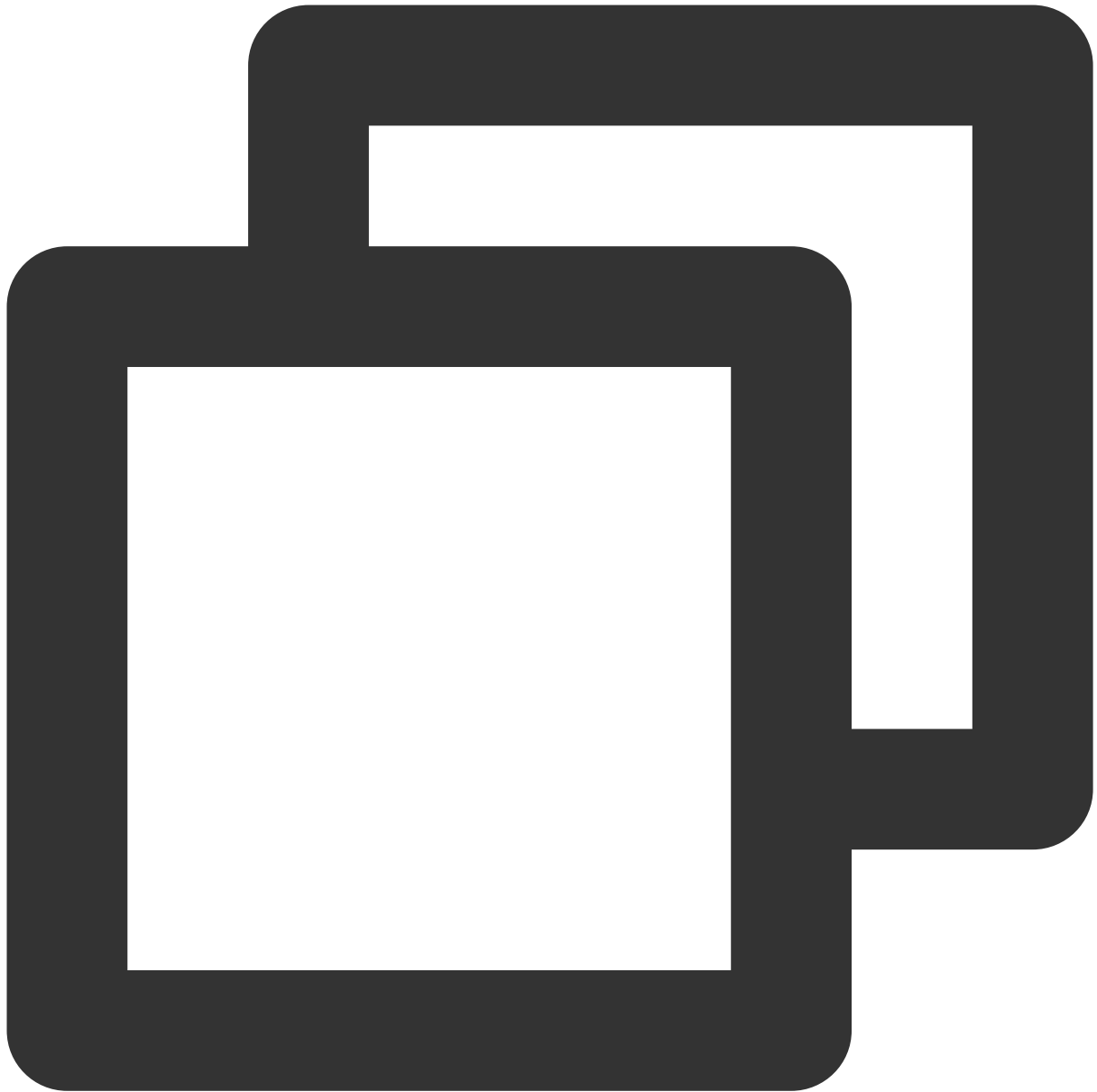


```
GRANT ALL PRIVILEGES ON wordpress.* TO 'user'@'localhost' IDENTIFIED BY '123456';
```

5. 아래의 명령어를 실행하여 root 계정 비밀번호를 설정하십시오.

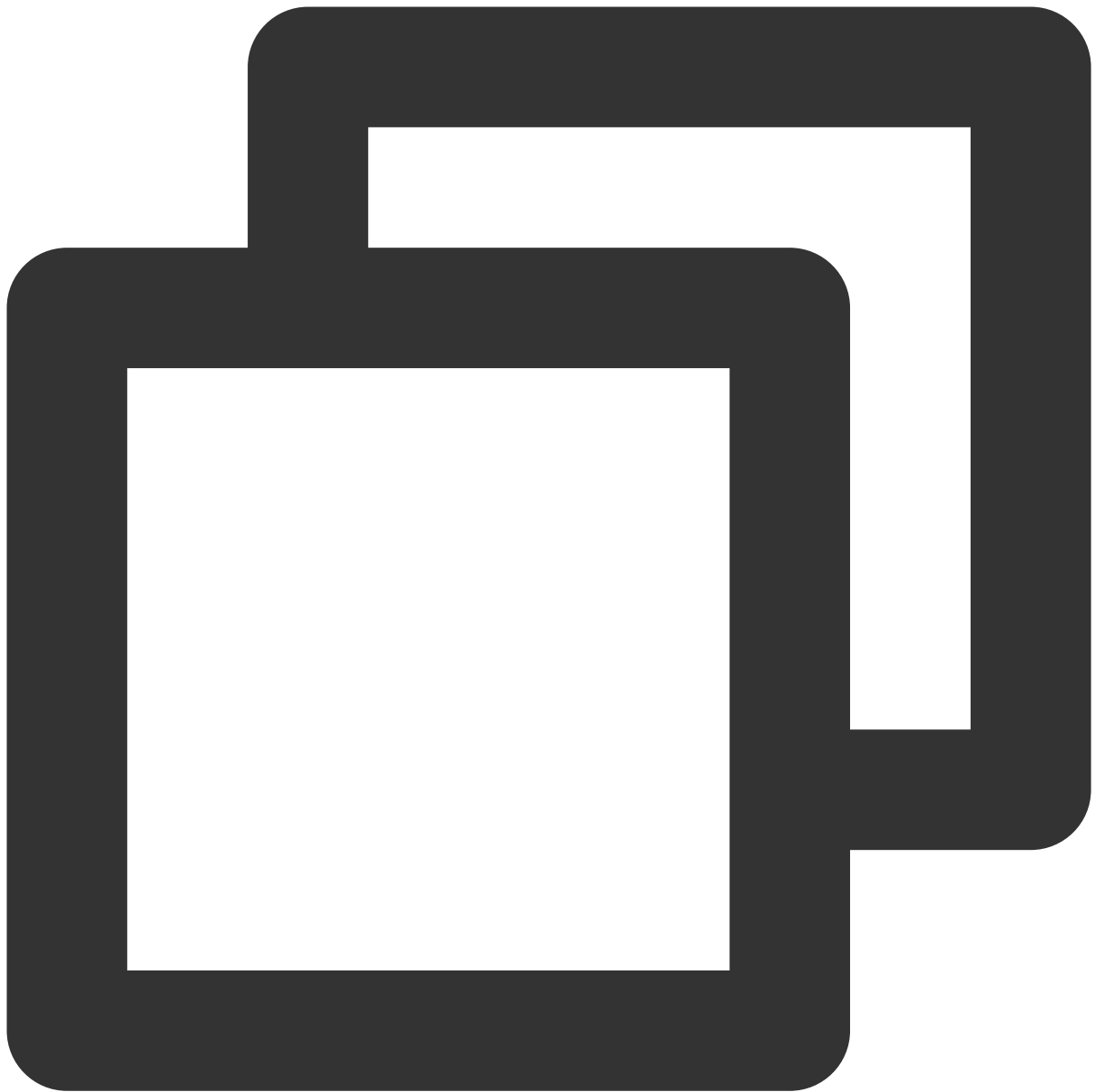
설명 :

CentOS 시스템의 MariaDB 10.4에 root 계정 ‘비밀번호 없이 로그인’ 기능이 추가되었습니다. 아래의 순서대로 root 계정 비밀번호를 설정하고 기억하십시오.



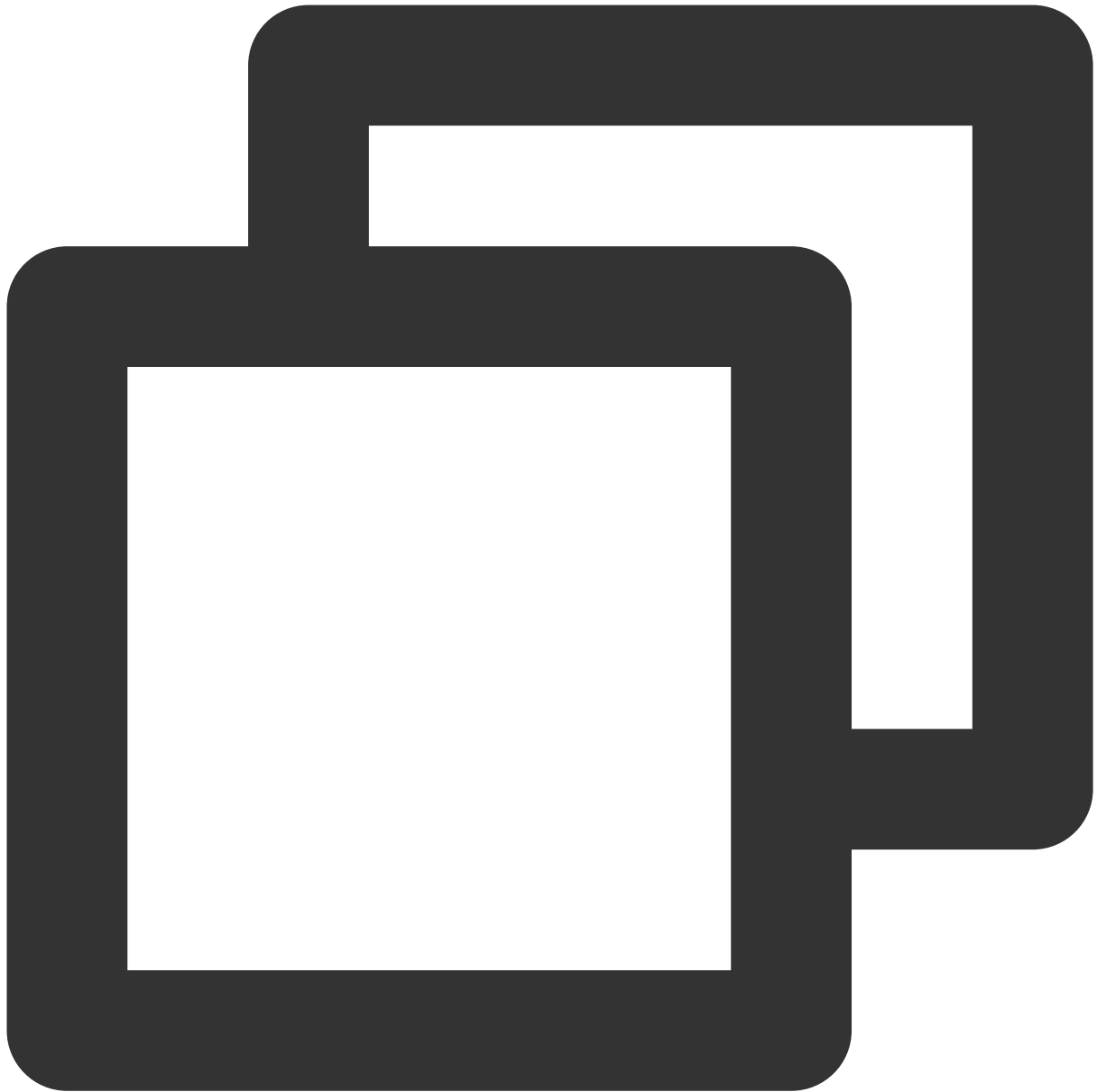
```
ALTER USER root@localhost IDENTIFIED VIA mysql_native_password USING PASSWORD('비밀번호');
```

6. 아래의 명령어를 실행하여 모든 구성을 활성화하십시오.



```
FLUSH PRIVILEGES;
```

7. 아래의 명령어를 실행하여 MariaDB를 종료하십시오.



\\q

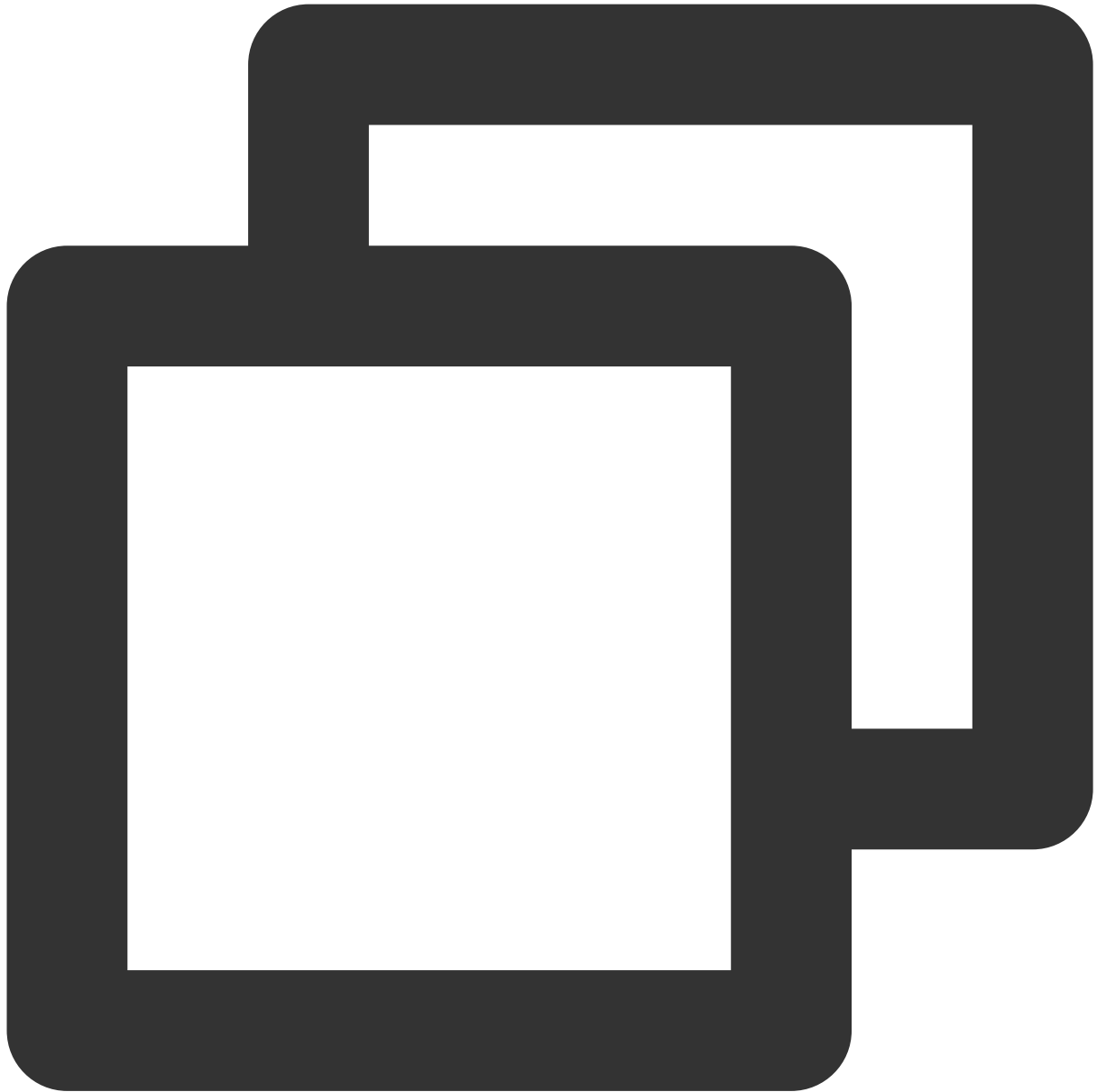
4단계: WordPress 설치 및 설정

WordPress 다운로드

설명 :

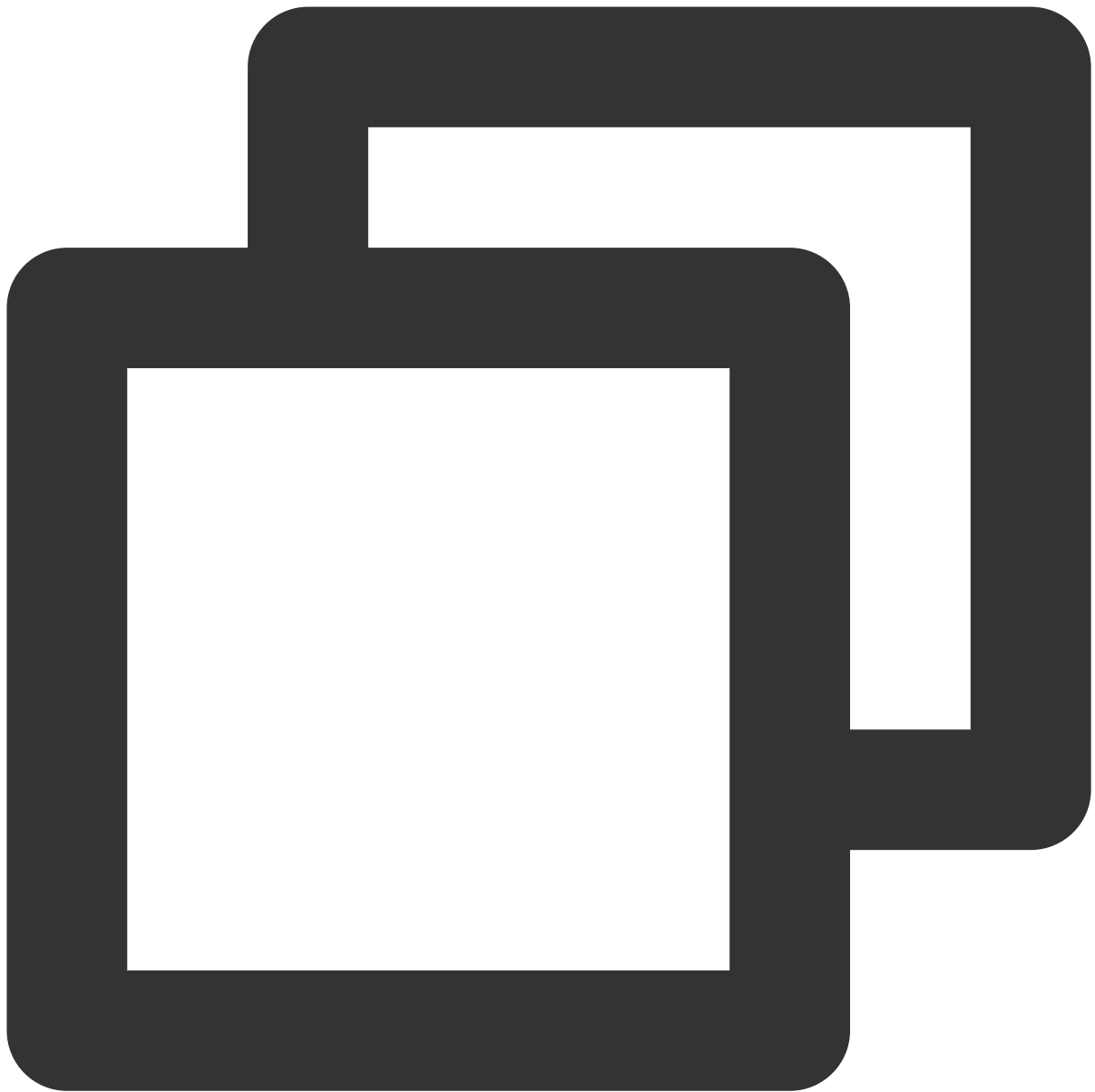
WordPress는 WordPress 공식 홈페이지에서 최신 중국어 버전의 WordPress를 다운로드하여 설치할 수 있으며, 이 튜토리얼에서는 WordPress 중국어 버전을 사용합니다.

1. 아래의 명령어를 실행하여 웹 사이트 디렉터리에서 PHP-Nginx 구성 테스트에 사용하는 'index.php' 파일을 삭제하십시오.

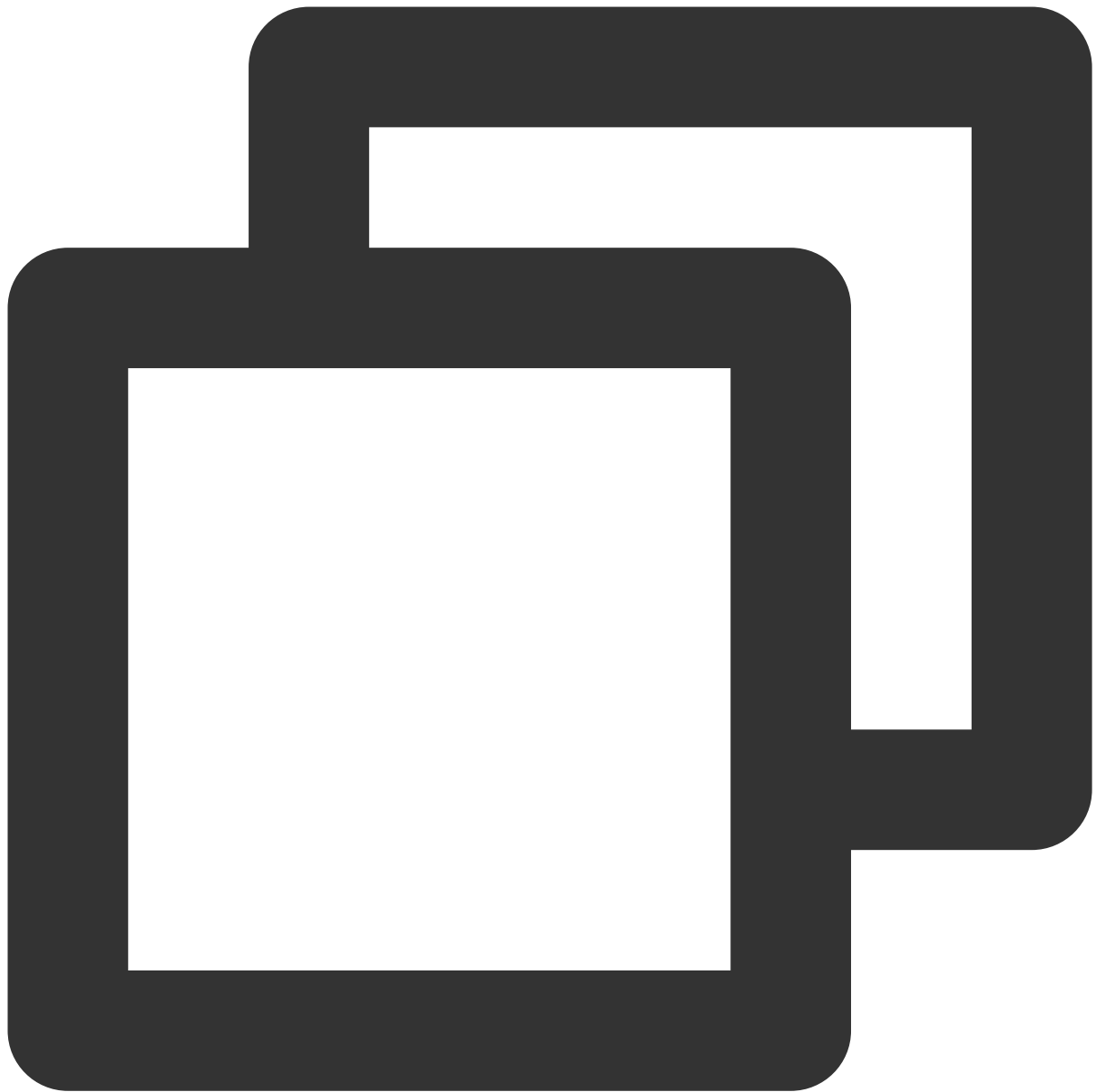


```
rm -rf /usr/share/nginx/html/index.php
```

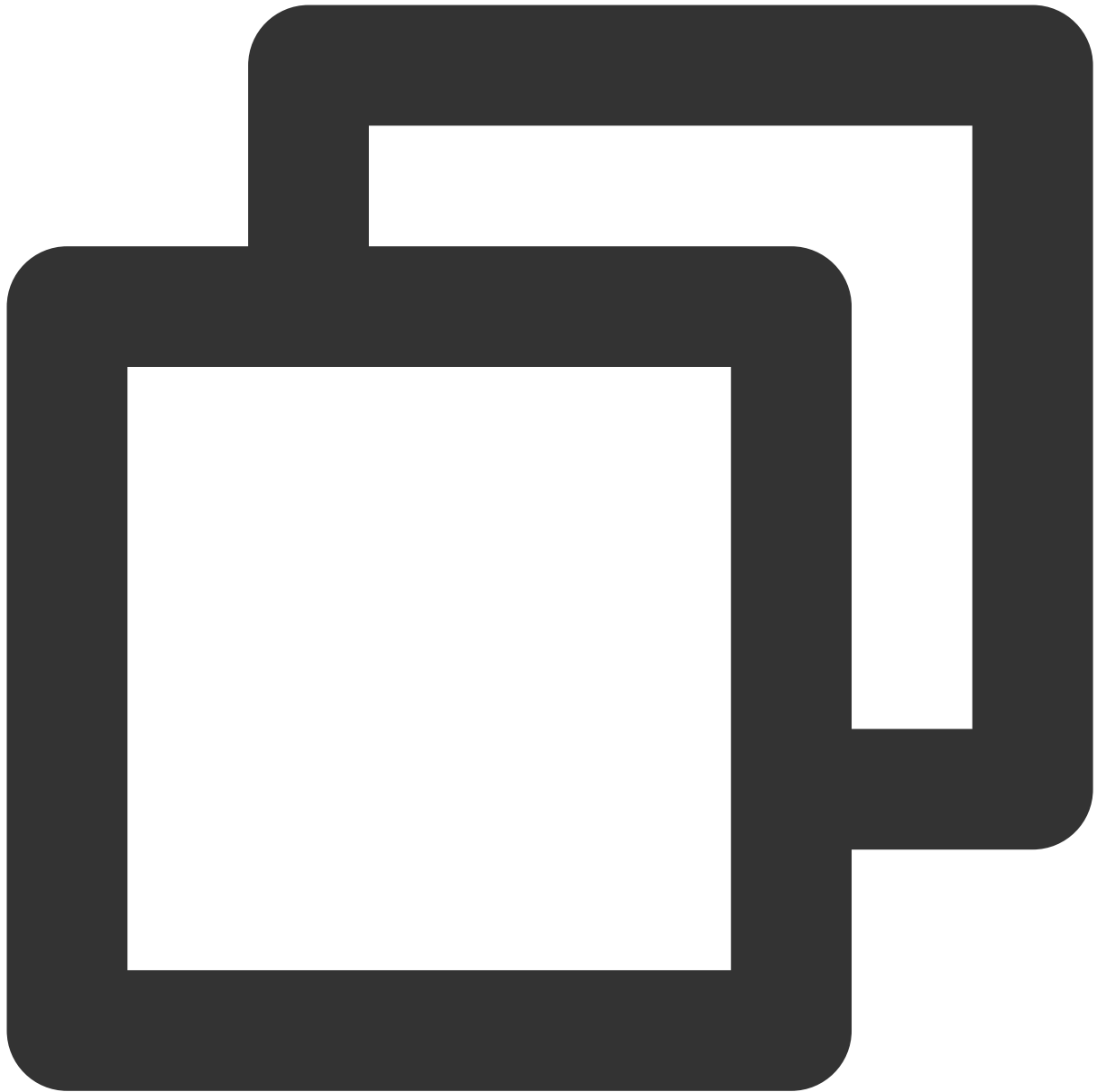
2. 아래의 명령어를 차례대로 실행하여 '/usr/share/nginx/html/' 디렉터리에 진입한 뒤 WordPress를 다운로드 및 압축 해제 하십시오.



```
cd /usr/share/nginx/html
```



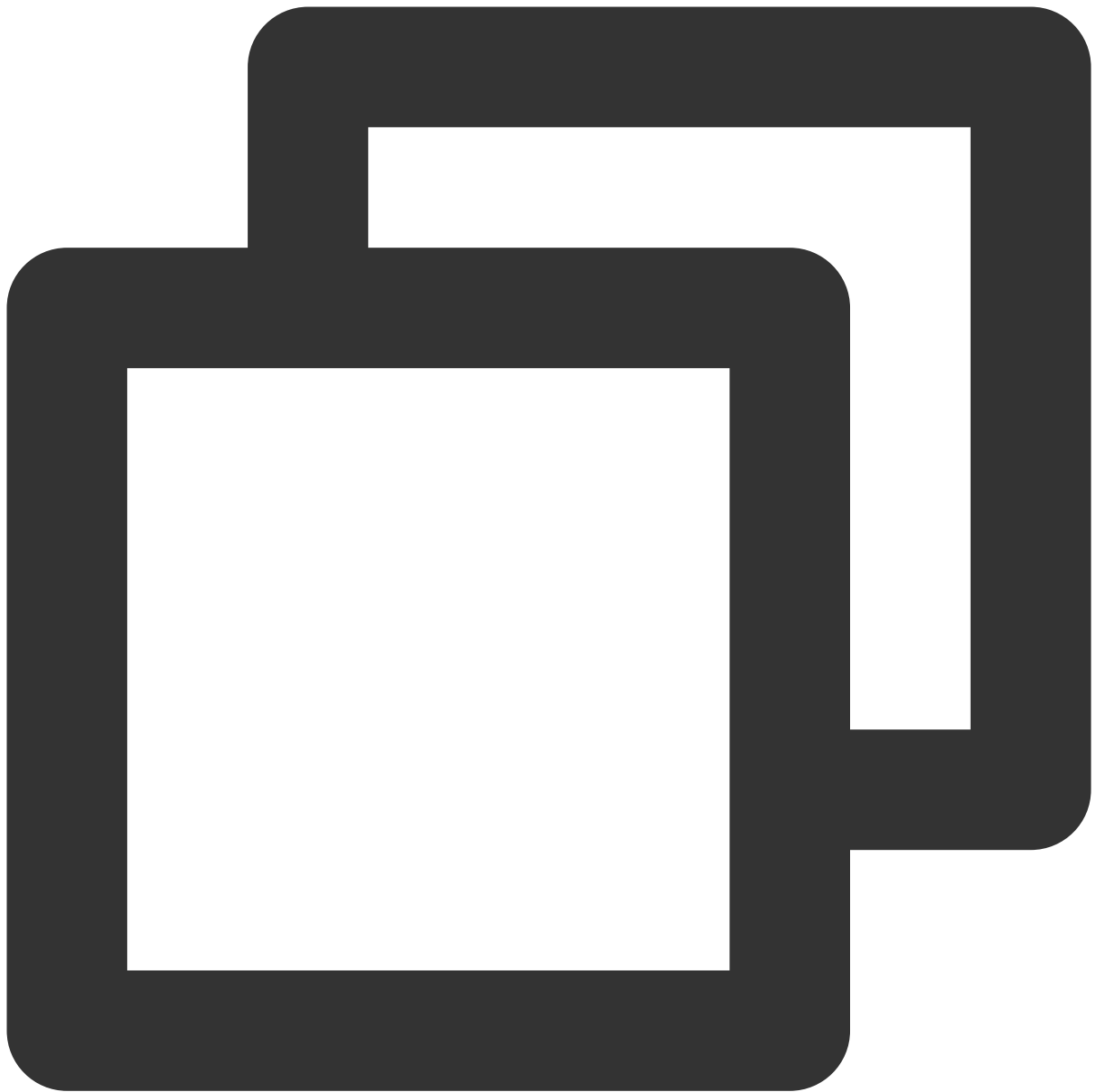
```
wget https://cn.wordpress.org/wordpress-5.0.4-zh_CN.tar.gz
```



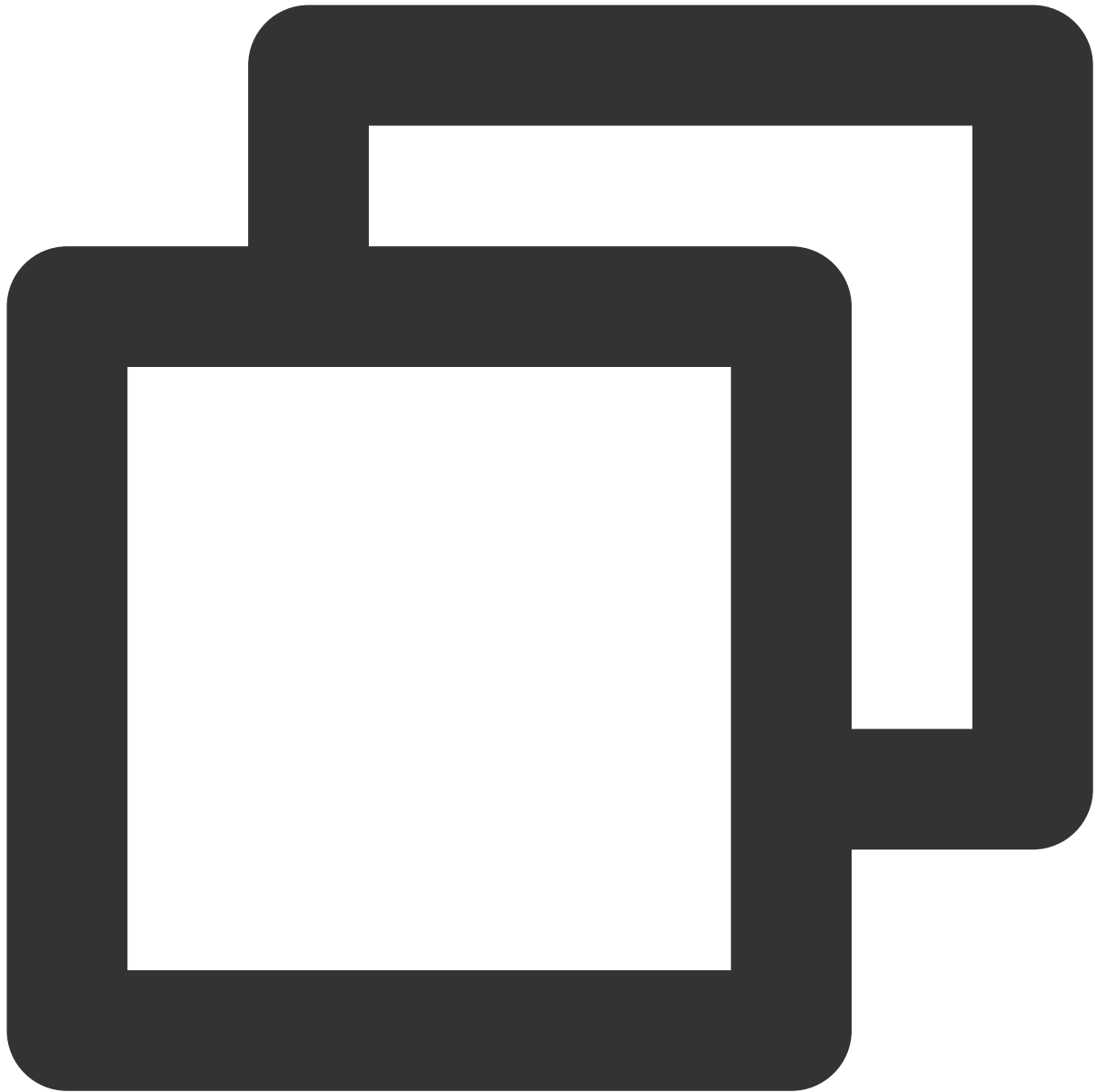
```
tar zxvf wordpress-5.0.4-zh_CN.tar.gz
```

WordPress 구성 파일 수정

1. 아래의 명령어를 차례대로 실행하여 WordPress 설치 디렉터리에 진입한 뒤 'wp-config-sample.php' 파일을 'wp-config.php' 파일로 복제하십시오. 본래의 예시 구성 파일은 백업되어 보존됩니다.

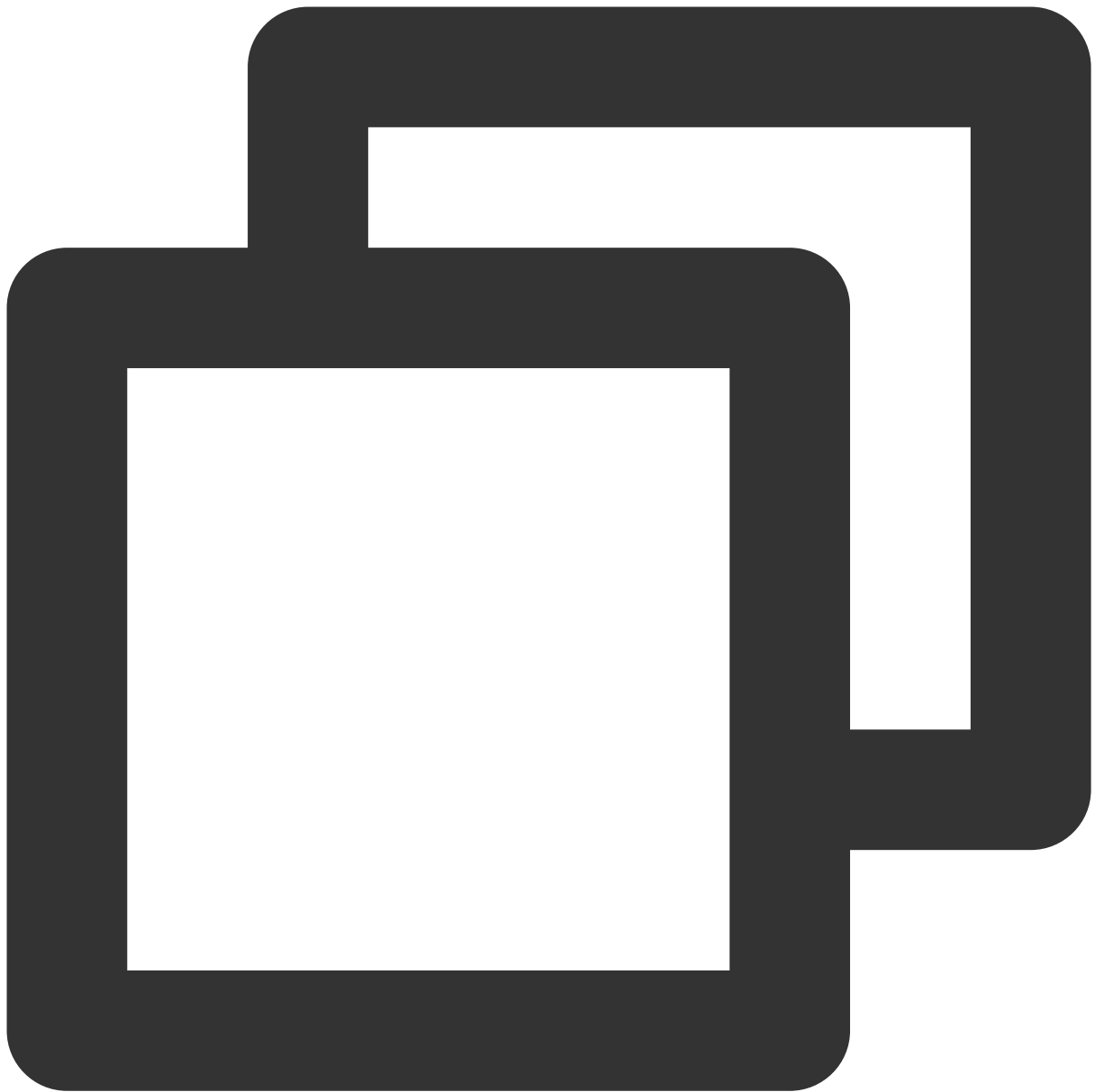


```
cd /usr/share/nginx/html/wordpress
```

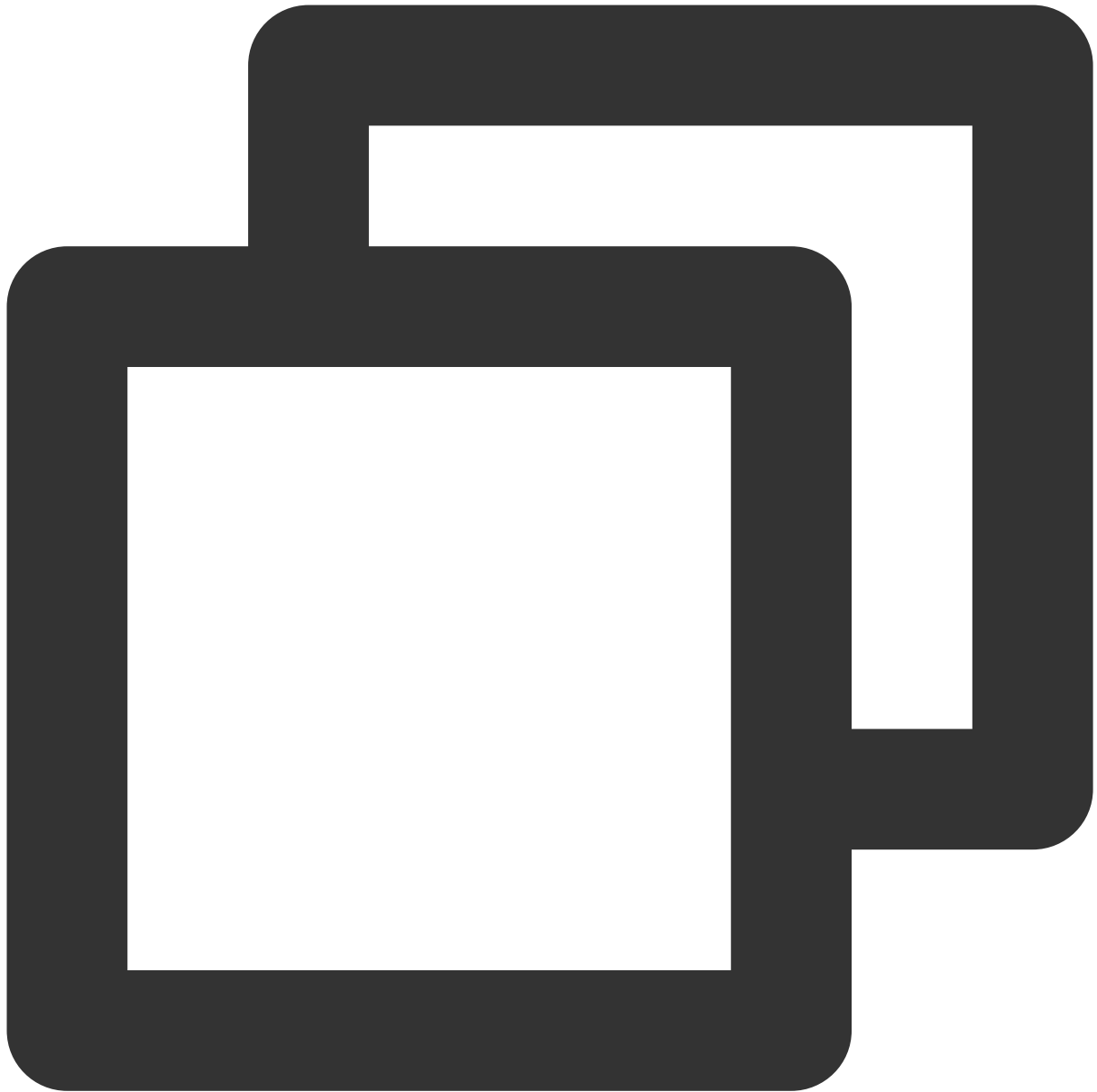
```
cp wp-config-sample.php wp-config.php
```

2. 아래의 명령어를 실행하여 새로 생성된 구성 파일을 연 뒤 편집하십시오.



```
vim wp-config.php
```

3. **i**를 눌러 편집 모드로 들어갑니다. 파일에서 MySQL 섹션을 찾아 [WordPress 데이터베이스 구성](#)에 설명된 대로 설정을 수정합니다.

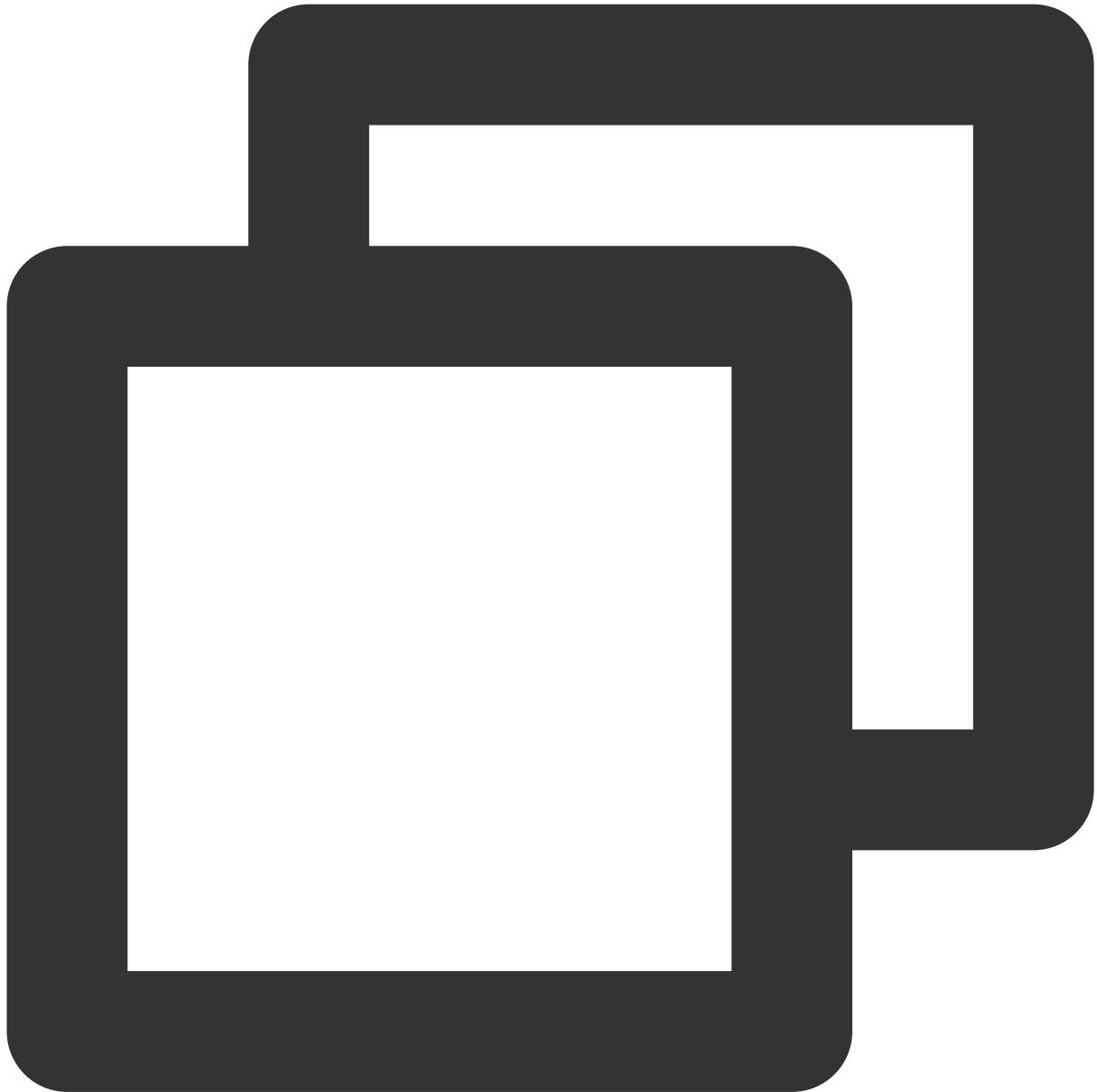


```
// ** MySQL settings - You can get this info from your web host ** //  
/** The name of the database for WordPress */  
define('DB_NAME', 'wordpress');  
/** MySQL database username */  
define('DB_USER', 'user');  
/** MySQL database password */  
define('DB_PASSWORD', '123456');  
/** MySQL hostname */  
define('DB_HOST', 'localhost');
```

4. 수정 완료 후, **Esc**키를 누르고 **:wq**를 입력합니다. 그런 다음 변경 사항을 저장하고 파일을 닫습니다.

5단계: WordPress 설치 확인

1. 브라우저 주소란에 `http://도메인 이름 또는 CVM 인스턴스 공용 IP/wordpress 폴더` 를 예시처럼 입력 하십시오.



`http://192.xxx.xxx.xx/wordpress`

WordPress 설치 페이지로 이동하여 WordPress 구성을 시작하십시오.

2. WordPress 설치 마법사에 따라 아래의 설치 정보를 입력하고 **WordPress 설치**를 클릭해 설치를 완료합니다.

필요 정보	설명

웹 사이트 제목	WordPress 웹 사이트 명칭
사용자 이름	WordPress 관리자 이름. 보안을 위해 크랙되기 쉬운 admin 이 아닌 다른 이름을 사용하십시오.
비밀번호	기본 강력한 암호 또는 사용자 정의 암호를 사용합니다. 이전 비밀번호를 사용하지 마시고 비밀번호를 안전한 곳에 보관하십시오.
이메일 주소	알림을 수신할 이메일 주소입니다.

이제 WordPress 사이트에 로그인하여 블로그를 게시할 수 있습니다.

관련 작업

WordPress 사이트의 도메인 이름을 설정할 수 있습니다. 이러한 방식으로 사용자는 복잡한 IP 주소 대신 도메인 이름을 사용하여 사이트를 방문할 수 있습니다. 학습 목적으로 사이트를 구축하는 경우 사이트에 대한 IP 주소를 설정할 수 있습니다. 그러나 이 방법은 다른 경우에는 권장되지 않습니다.

FAQ

CVM 사용 도중 문제가 생겼을 경우, 아래의 문서를 참고하여 실제 상황에 따라 문제를 분석 및 해결할 수 있습니다.

CVM 로그인 문제는 [키 관련 문제](#), [로그인 및 원격 연결](#)을 참고하십시오.

CVM 네트워크 문제는 [IP 주소 문제](#), [포트 관련 문제](#)를 참고하십시오.

CVM 디스크 문제는 [시스템 디스크와 데이터 디스크](#)를 참고하십시오.

WordPress 웹 사이트 수동 구축(Windows)

최종 업데이트 날짜: : 2024-02-02 10:56:29

작업 시나리오

WordPress는 PHP 언어를 사용해 개발한 블로그 플랫폼입니다. WordPress를 통해 개인의 블로그 플랫폼을 구축해 사용할 수 있습니다. 본 문서는 Windows Server 2012 운영 체제의 Tencent Cloud 서버를 예시로 하며, WordPress 개인 웹 사이트를 수동으로 구축합니다.

주의사항 :

Tencent Cloud는 클라우드 마켓의 이미지 환경을 통해 WordPress 개인 블로그를 배포할 것을 권장하며, 수동 구축 과정이 오래 걸릴 수 있습니다.

소프트웨어

WordPress 개인 사이트는 PHP 5.6.20 이상 및 MySQL 5.0 이상에서 구축할 수 있습니다. 보안성 강화를 위해 WordPress 개인 사이트 구축 시 PHP 7.3 이상, MySQL 5.6 이상 버전 설치를 권장합니다.

본 문서에서 구축한 WordPress 개인 사이트의 구성 버전과 설명은 다음과 같습니다.

Windows: Windows 운영 체제, 본 문은 Windows Server 2012 R2 데이터센터 Edition의 64비트 중국어 버전을 예로 들어 설명합니다.

IIS: Web 서버의 경우, 본 문은 IIS 8.5를 예시로 사용합니다.

MySQL: 본 문은 데이터베이스 MySQL 8.0.19를 예시로 사용합니다.

PHP: 스크립트 언어의 경우, 본 문은 PHP 7.1.30를 예시로 사용합니다.

WordPress: 블로그 플랫폼, 본 문은 WordPress 5.9를 예시로 사용합니다.

작업 단계

1단계: CVM(Cloud Virtual Machine) 로그인

RDP 파일을 사용하여 [Windows 인스턴스에 로그인](#)(권장).

실제 작업 스타일에 따라 [데스크탑에 원격 연결하여 Windows 인스턴스에 로그인](#)할 수 있습니다.

2단계: WIPM 환경 구축

[WIPM 환경 수동 구축](#)을 참고하여 다음을 수행합니다.

1. IIS 서비스를 설치합니다.
2. PHP 5.6.20 이상 버전 환경을 배포합니다.

3. MySQL 5.6 이상 버전 데이터베이스를 설치합니다.

3단계: WordPress 설치 및 설정

설명 :

WordPress는 WordPress 공식 홈페이지에서 최신 중국어 버전의 WordPress를 다운로드하여 설치할 수 있으며, 이 튜토리얼에서는 WordPress 중국어 버전을 사용합니다.

1. WordPress를 다운로드하고 WordPress 설치 패키지를 CVM에 압축 해제합니다.

예를 들어, WordPress 설치 패키지의 압축을 'C:\\wordpress' 디렉터리에 해제합니다.

2.



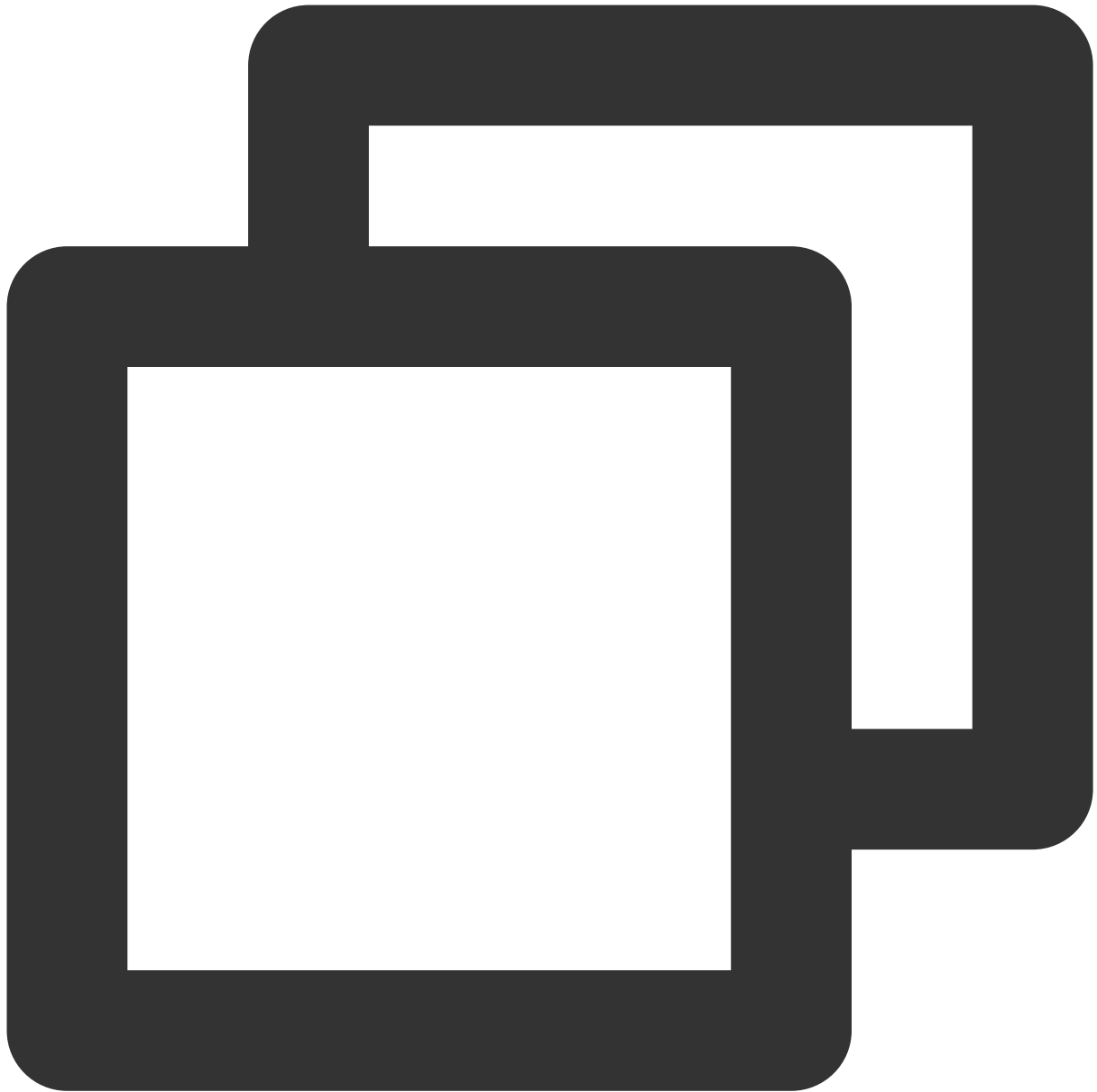
>



> **MySQL 5.6 Command Line Client**를 클릭하여, MySQL 명령 라인 클라이언트를 엽니다.

3. MySQL 명령 라인 클라이언트에서 다음 명령을 실행하여 WordPress 데이터베이스를 생성합니다.

예를 들어 'wordpress' 데이터베이스를 생성합니다.



```
create database wordpress;
```

4. WordPress의 압축 해제 설치 경로에서 `wp-config-sample.php` 파일을 찾아 복사하고, 파일 이름을 `wp-config.php` 로 변경합니다.

5. 'wp-config.php' 파일을 텍스트 편집기로 열고 관련 설정 정보를 [3단계: MySQL 데이터베이스 설치](#)의 내용으로 수정합니다. 아래 이미지와 같습니다.


```
// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'root' );

/** Database password */
define( 'DB_PASSWORD', '123456' );

/** Database hostname */
define( 'DB_HOST', 'localhost' );

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The database collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

6. wp-config.php 파일을 저장합니다.

7.



을(를) 클릭하여 서버 관리자를 엽니다.

8. 서버 관리자의 왼쪽 사이드바에서 **IIS**를 선택하고 오른쪽 IIS 관리 창의 **서버** 열에서 서버 이름을 우클릭하고 **Internet Information Services(IIS) 관리자**를 선택합니다.

9. 열려 있는 'Internet Information Services (IIS) 관리자' 창의 왼쪽 사이드바에서 서버 이름을 차례로 펼쳐 **웹사이트**를 클릭하여 '웹사이트' 관리 페이지로 이동합니다.

10. **웹사이트**에서 80번 포트에 바인딩된 웹사이트를 삭제합니다.

웹 사이트의 바인딩 포트를 점유되어 있지 않는 다른 포트 번호로 수정할 수도 있습니다. 예를 들어 포트 8080으로 수정합니다.

11. 오른쪽의 **작업** 열에서 **웹 사이트 추가**를 클릭합니다.

12. 팝업 창에서 다음 정보를 입력하고 **확인**을 클릭합니다.

웹 사이트 이름: 사용자 정의합니다. 예: wordpress.

응용 프로그램 풀: **DefaultAppPool**로 선택합니다.

물리적 경로: C:\wordpress 와 같이 WordPress가 압축 해제된 경로를 선택합니다.

13. PHP의 압축 해제 설치 경로에서 **php.ini** 파일을 열고 다음 콘텐츠를 수정합니다.

13.1 PHP 버전에 따라 해당 설정 매개변수를 수정합니다.

PHP 버전 5.X의 경우 `extension=php_mysql.dll` 을 찾아 앞의 `;` 을 삭제합니다.

PHP 버전 7.X의 경우 `extension=php_mysql.dll` 또는 `extension=mysqli` 를 찾아 앞의 `;` 을 삭제합니다.

13.2 `extension_dir = "ext"` 를 찾아 앞의 `;` 을 삭제합니다.

14. `php.ini` 파일을 저장합니다.

4단계: WordPress 설정 인증

1. 브라우저를 이용하여 `http://localhost/wp-admin/install.php` 에 액세스하여 WordPress 설치 페이지로 이동하여 WordPress 설정을 시작합니다.

2. WordPress 설치 마법사에 따라 아래의 설치 정보를 입력하고 **WordPress 설치**를 클릭해 설치를 완료합니다.

필수 정보	설명
웹 사이트 제목	WordPress 웹 사이트 이름.
사용자 이름	WordPress 관리자 명칭. 보안상의 이유로 admin 명칭과 다르게 설정하길 권장합니다. 기본 사용자 이름이 admin과 비교하여 크래킹이 더 어렵기 때문입니다.
비밀번호	강력한 기본 비밀번호 또는 사용자 정의 비밀번호를 사용할 수 있습니다. 기존 비밀번호는 재사용하지 마시고 비밀번호는 안전한 곳에 보관하시기 바랍니다.
귀하의 이메일	공지를 받을 이메일 주소입니다.

이제 WordPress 블로그에 로그인할 수 있으며, 블로그에 게시글을 업로드할 수 있습니다.

FAQ

CVM 사용 도중 문제가 생겼을 경우, 아래의 문서를 참고하여 실제 상황에 따라 문제를 분석 및 해결할 수 있습니다.

CVM 로그인 문제는 [키 관련 문제](#), [로그인 및 원격 연결](#)을 참고하십시오.

CVM 네트워크 문제는 [IP 주소 문제](#), [포트 관련 문제](#)를 참고하십시오.

CVM 디스크 문제는 [시스템 디스크와 데이터 디스크](#)를 참고하십시오.

Discuz! 포럼 구축

Discuz! 포럼 수동 구축

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

Discuz!는 전 세계에서 완성도 및 커버율이 가장 높은 포럼 웹 사이트 소프트웨어 시스템 중 하나로, 200여만 명의 웹 사이트 사용자를 보유하고 있으며, 귀하도 Discuz!를 통해 포럼을 구축할 수 있습니다. 본 문서는 Tencent Cloud CVM에서 Discuz! 포럼 구축 및 그에 필요한 LAMP(Linux + Apache + MariaDB + PHP)환경 구축에 대해 소개합니다.

Discuz! 포럼 수동 구축을 위해 자주 사용하는 커맨드인 [CentOS 환경에서 YUM을 통해 소프트웨어 설치](#) 등의 Linux 커맨드에 익숙해져야 하며, 설치된 소프트웨어의 사용 및 버전 호환성에 대한 이해도가 있어야 합니다.

소프트웨어

본 문서 중 구축한 Discuz! 포럼 소프트웨어의 구성 버전 및 설명은 다음과 같습니다.

Linux: Linux 운영 체제의 경우, 본 문서는 CentOS 7.6을 예시로 사용합니다.

Apache: Web 서버의 경우, 본 문서는 Apache 2.4.15를 예시로 사용합니다.

MariaDB: 데이터베이스의 경우, 본 문서는 MariaDB 5.5.60를 예시로 사용합니다.

PHP: 스크립트 언어의 경우, 본 문서는 PHP 5.4.16을 예시로 사용합니다.

Discuz!: 포럼 웹 사이트 소프트웨어의 경우, 본 문서는 Discuz! X3.4를 예시로 사용합니다.

작업 순서

1단계: CVM(Cloud Virtual Machine) 로그인

[Linux 인스턴스에 로그인](#)합니다. 실제 작업 스타일에 따라 다른 로그인 방식을 선택할 수도 있습니다.

[원격 로그인 소프트웨어를 사용하여 Linux 인스턴스 로그인](#)

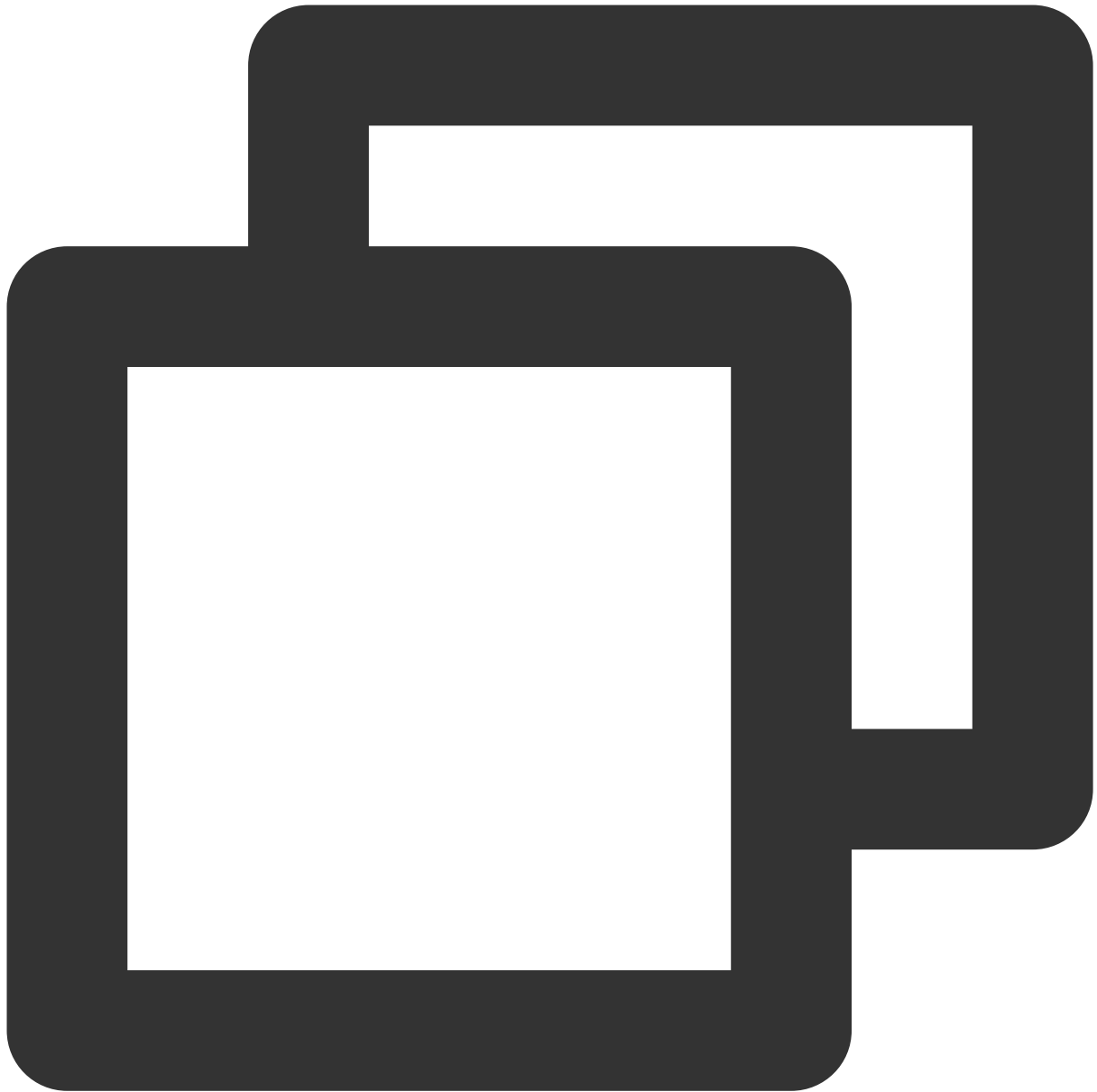
[SSH를 사용하여 Linux 인스턴스에 로그인](#)

2단계: LAMP 환경 구축

CentOS 시스템에 대해 Tencent Cloud는 CentOS와 동기화된 소프트웨어 설치 소스를 제공하고 있어, 포함되어 있는 소프트웨어 모두 현재로써 가장 안정적인 버전으로, 직접 Yum을 통해 빠르게 설치할 수 있습니다.

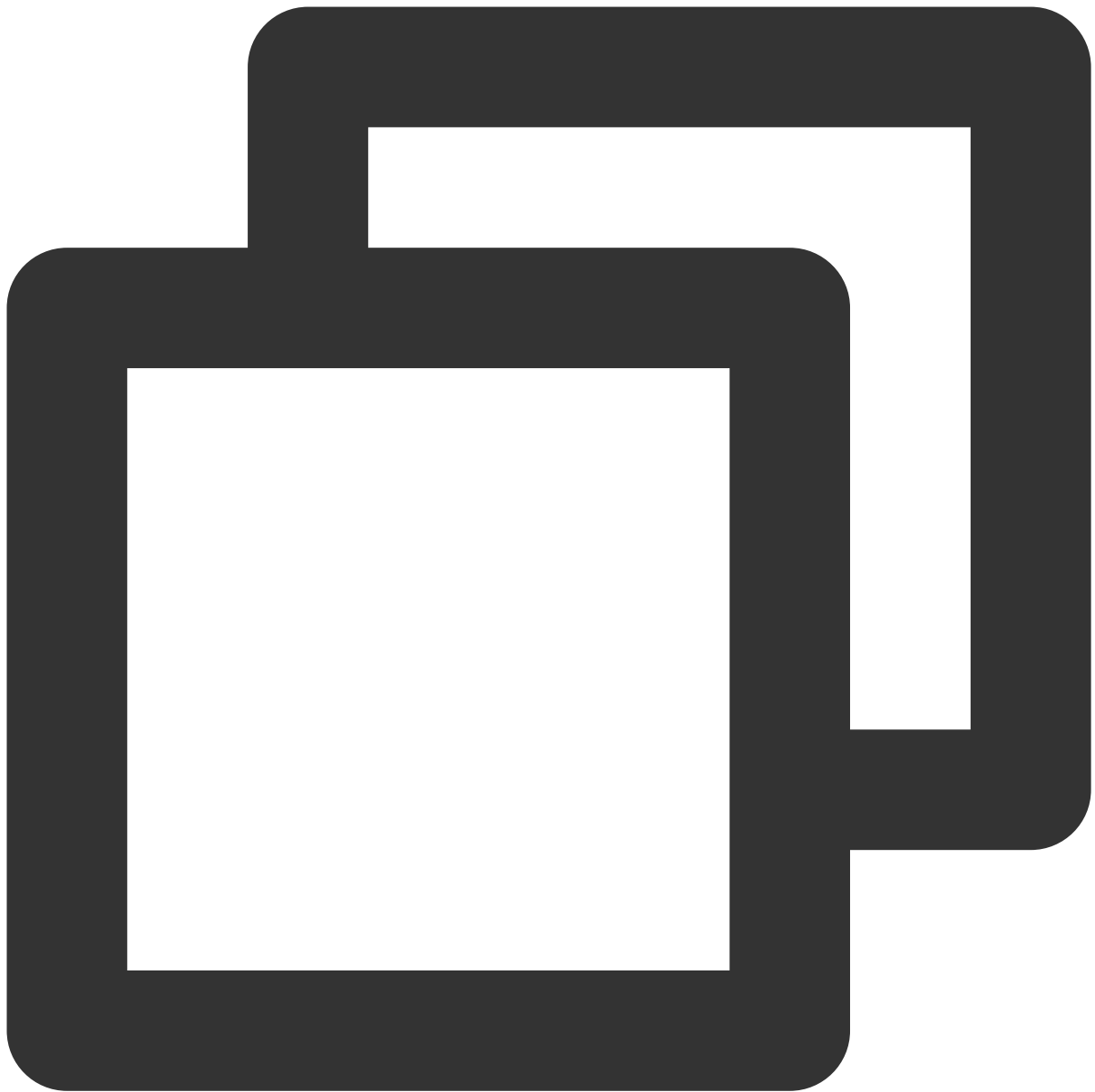
필요한 소프트웨어 설치 및 설정

1. 다음 명령어를 실행하여 필수 소프트웨어(Apache, MariaDB, PHP, Git)를 설치합니다.

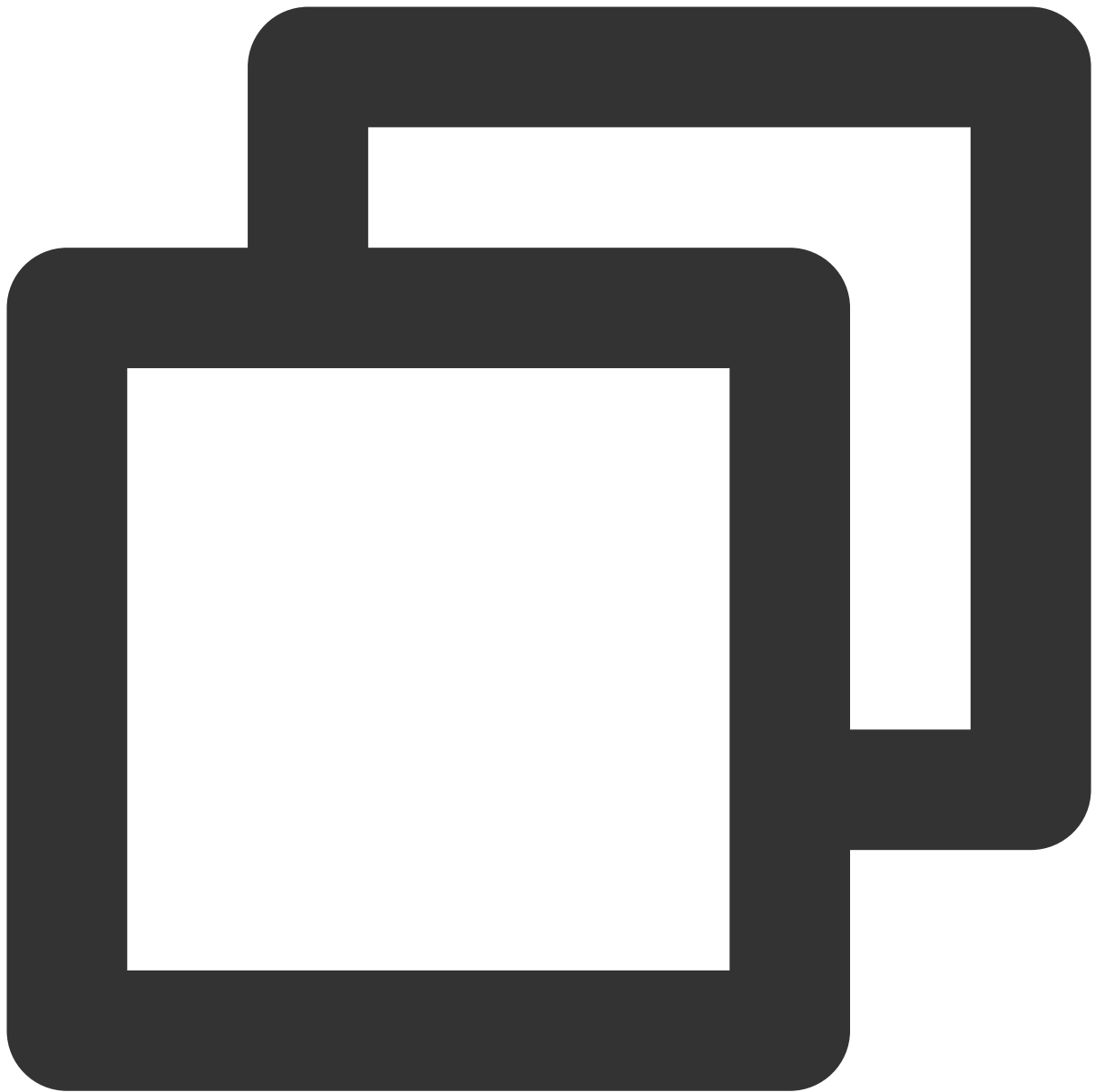


```
yum install httpd php php-fpm php-mysql mariadb mariadb-server git -y
```

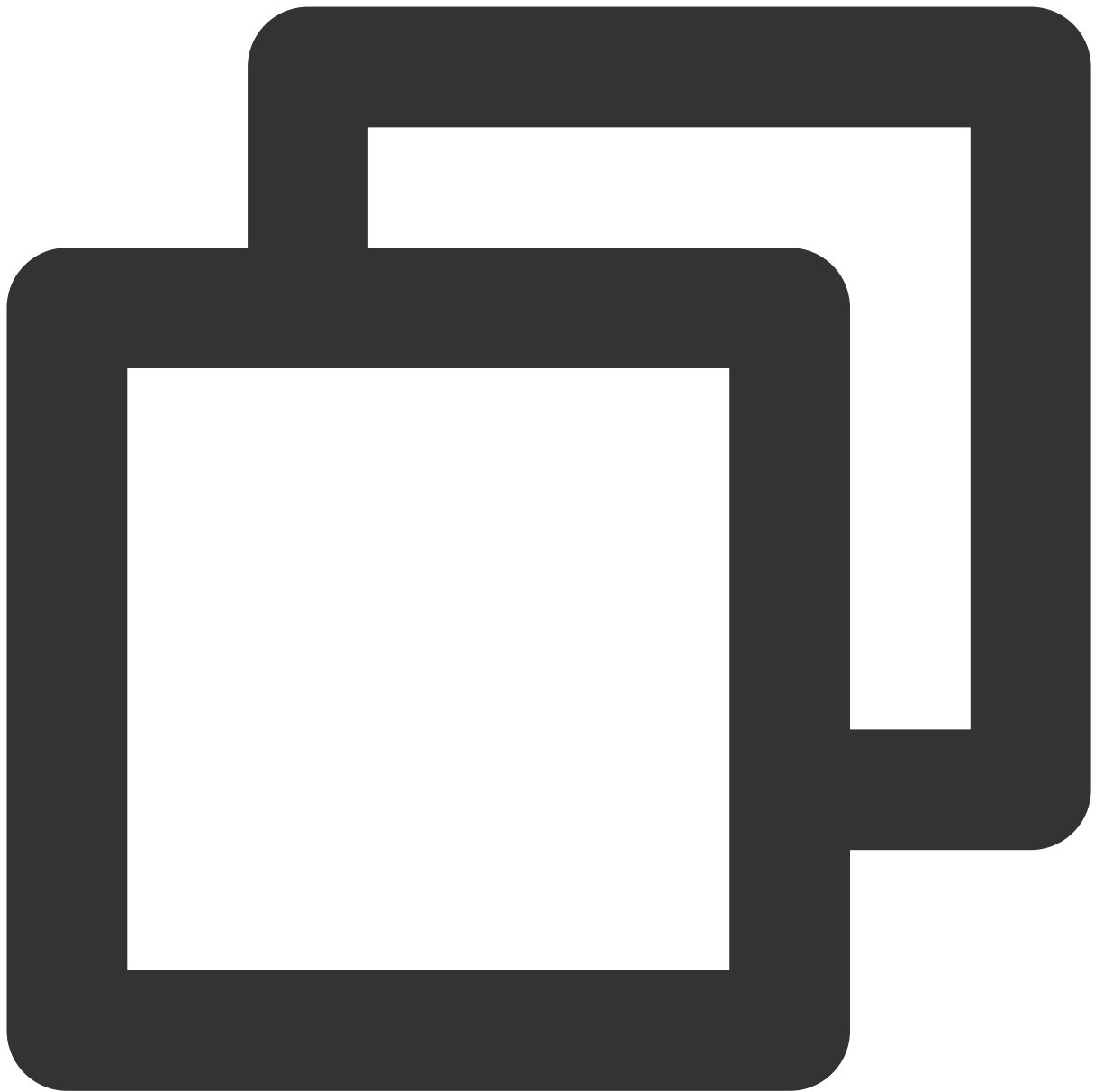
2. 다음 명령어를 차례대로 실행하여 서비스를 시작합니다.



```
systemctl start httpd
```



```
systemctl start mariadb
```



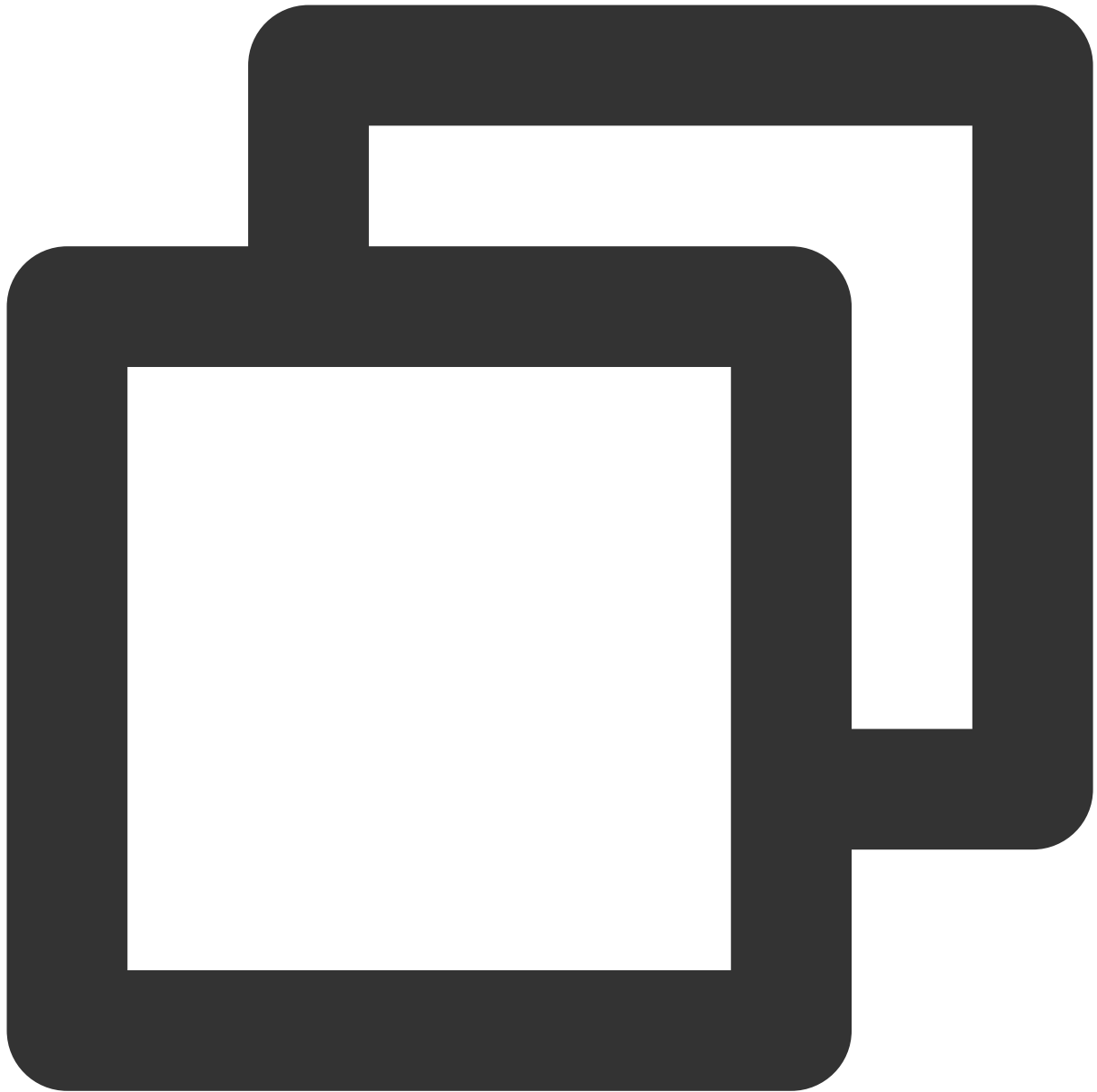
```
systemctl start php-fpm
```

3. root 사용자가 데이터베이스에 액세스할 수 있도록 다음 명령어를 실행하여 root 계정 비밀번호 및 기본 환경을 설정합니다.

주의사항 :

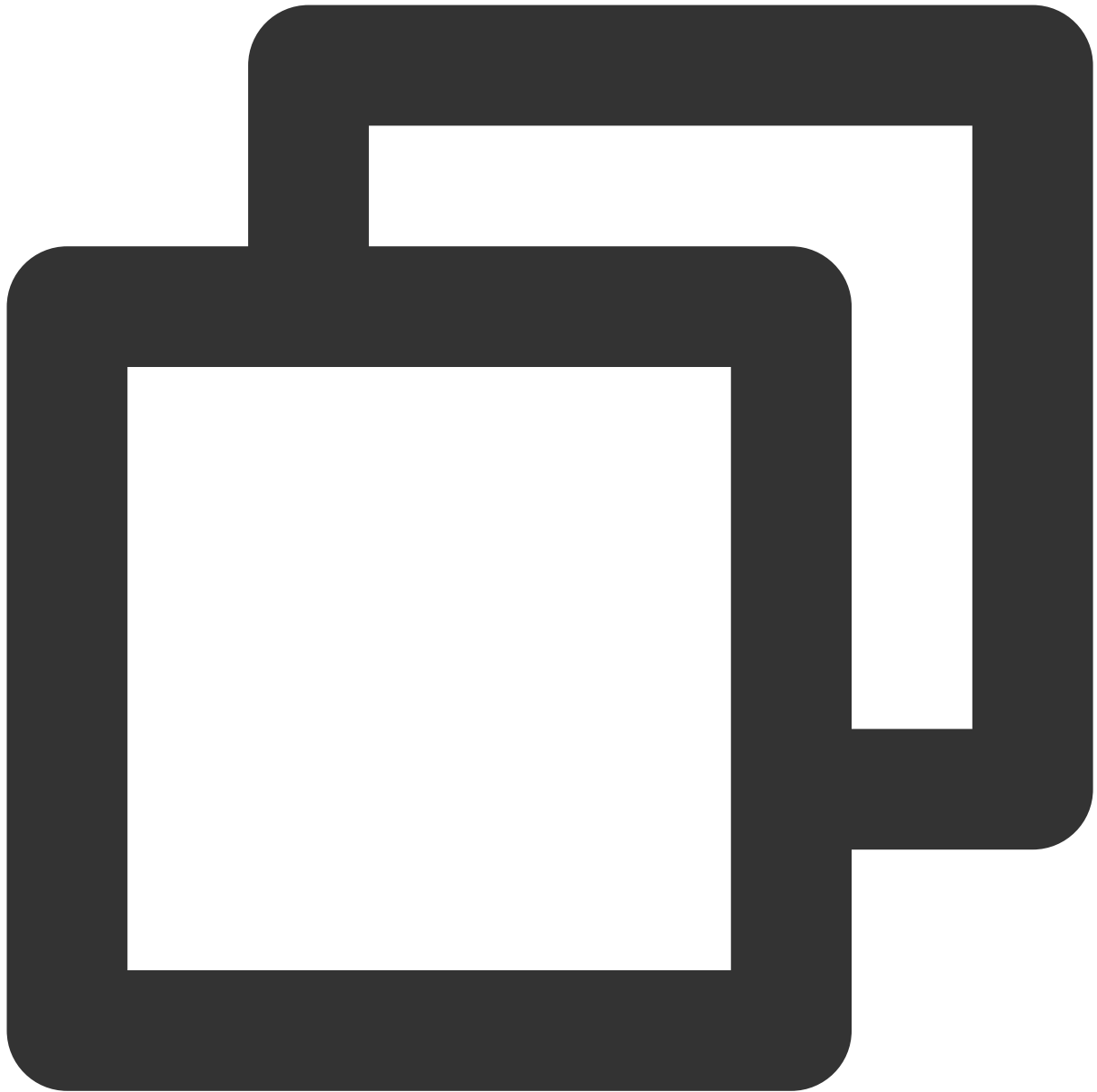
MariaDB 에 처음 로그인 하기 전, 다음 명령어를 실행하여 사용자 비밀번호 및 기본 설정으로 이동합니다.

처음으로 root 비밀번호를 입력하라는 메시지가 뜨면 **Enter**를 눌러 바로 root 비밀번호 설정 단계로 진입합니다. root 비밀번호 설정 시 인터페이스는 나타나지 않도록 기본 설정되어 있습니다. 인터페이스의 알림에 따라 순서대로 다른 기본 구성을 완료하십시오.



```
mysql_secure_installation
```

4. 다음 명령어를 실행하여 MariaDB에 로그인하고 [3단계](#)에서 설정한 비밀번호를 입력한 후 **"Enter"**를 누릅니다.



```
mysql -u root -p
```

방금 설정한 비밀번호를 입력하여 MariaDB 에 로그인 되면 제대로 설정되었음을 뜻합니다. 아래 그림 참고.

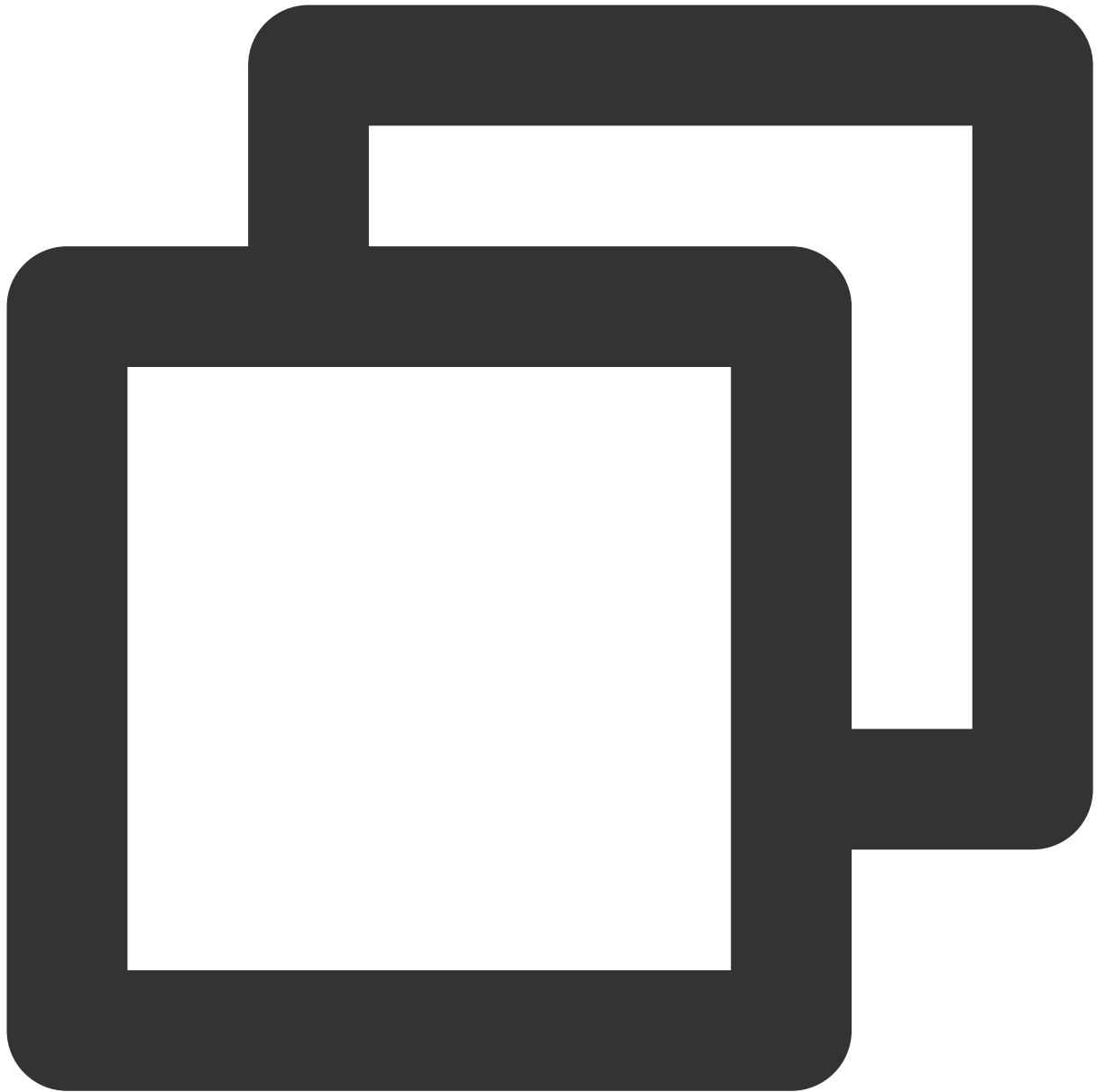
```
[root@VM_149_104_centos ~]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 27
Server version: 5.5.60-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

5. 다음 명령어를 실행하여 MariaDB 데이터베이스를 종료합니다.

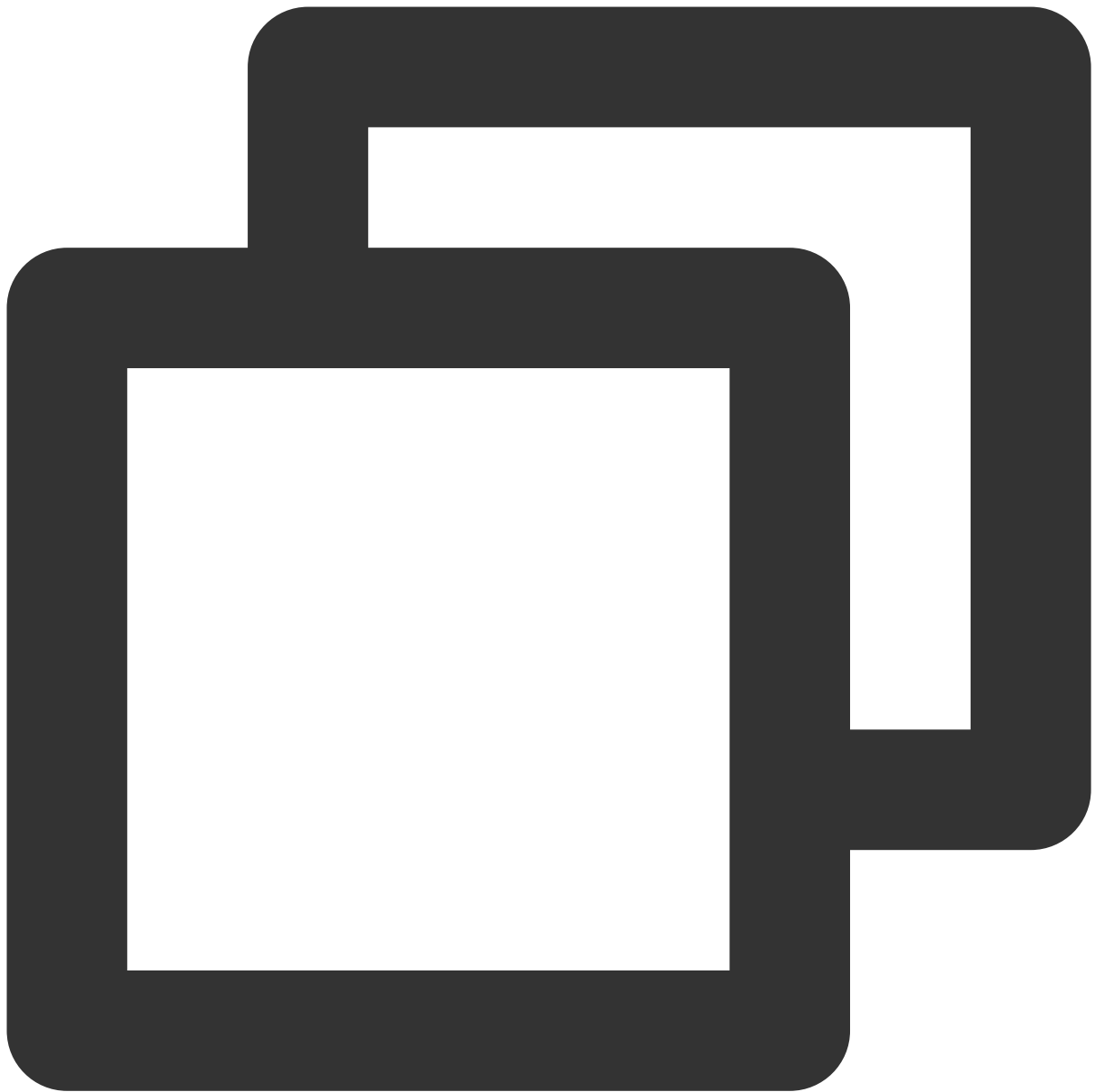


```
\\q
```

환경 설정 검증

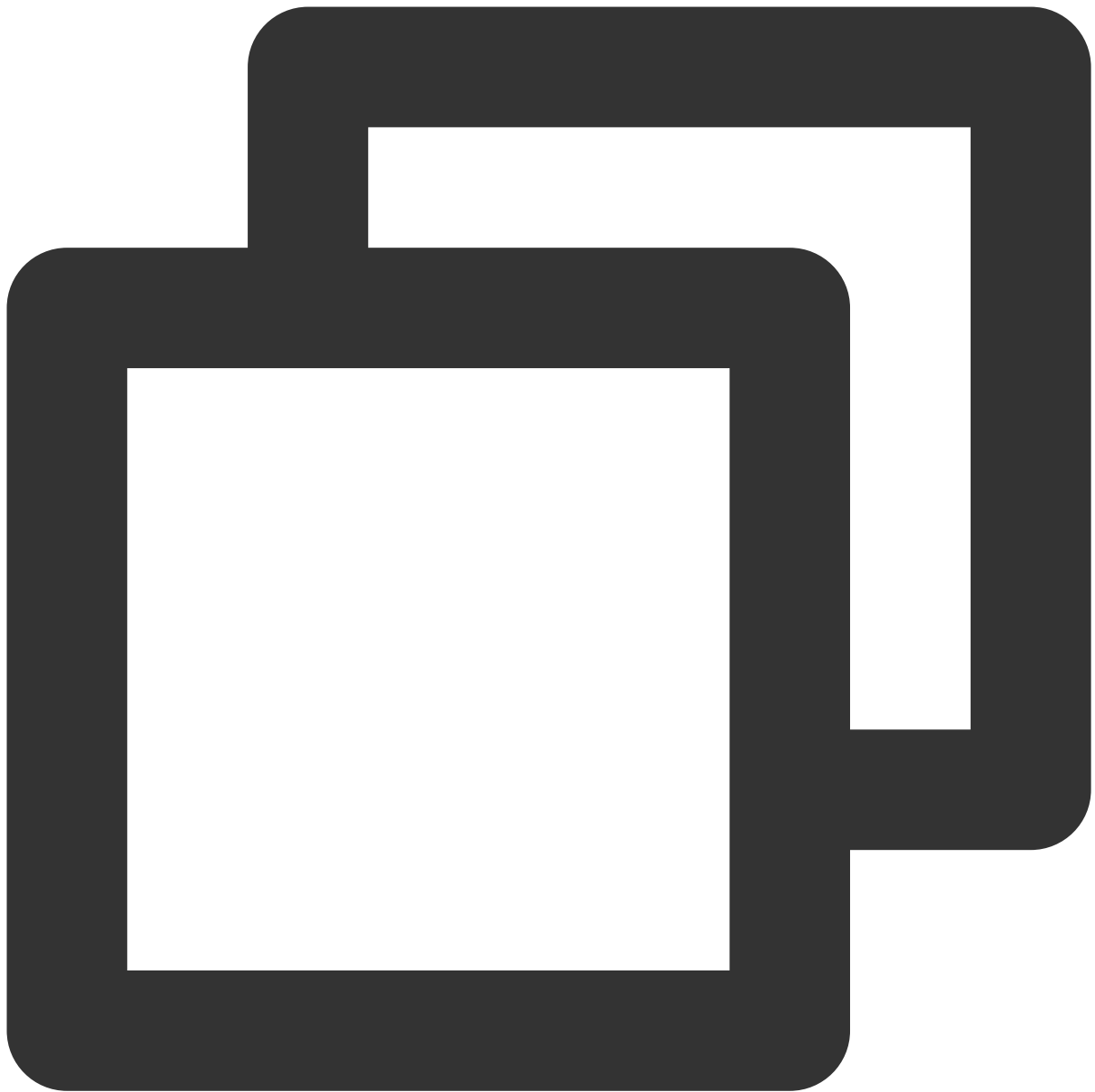
환경 구축 성공 여부를 확인 및 보장하기 위해 아래의 작업을 통해 검증할 수 있습니다.

1. 다음 명령어를 실행하여 Apache의 기본 루트 디렉터리 `/var/www/html` 에서 `test.php` 테스트 파일을 생성합니다.



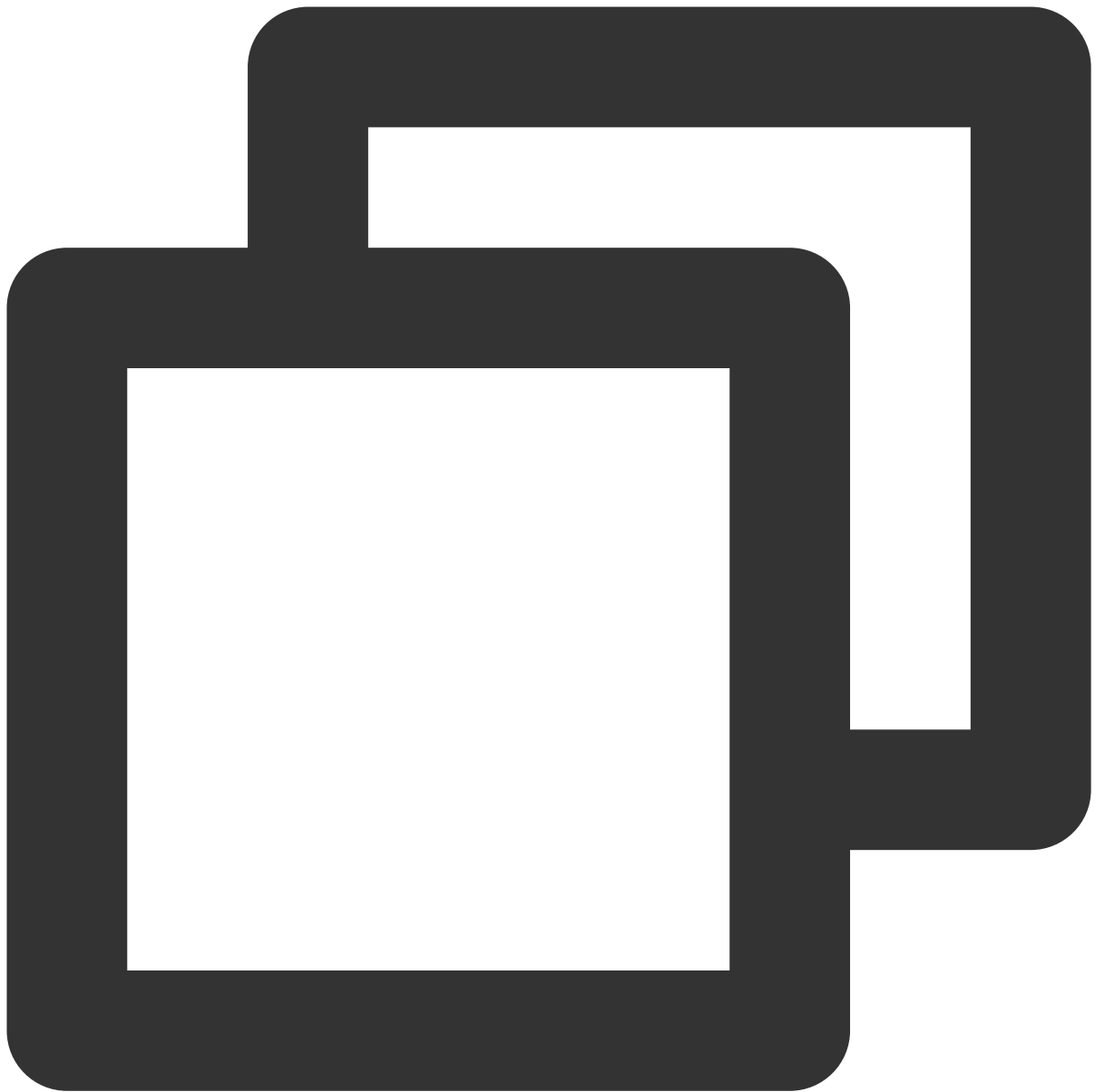
```
vim /var/www/html/test.php
```

2. **i**를 눌러 편집 모드로 바꾸고 다음 내용을 입력합니다.



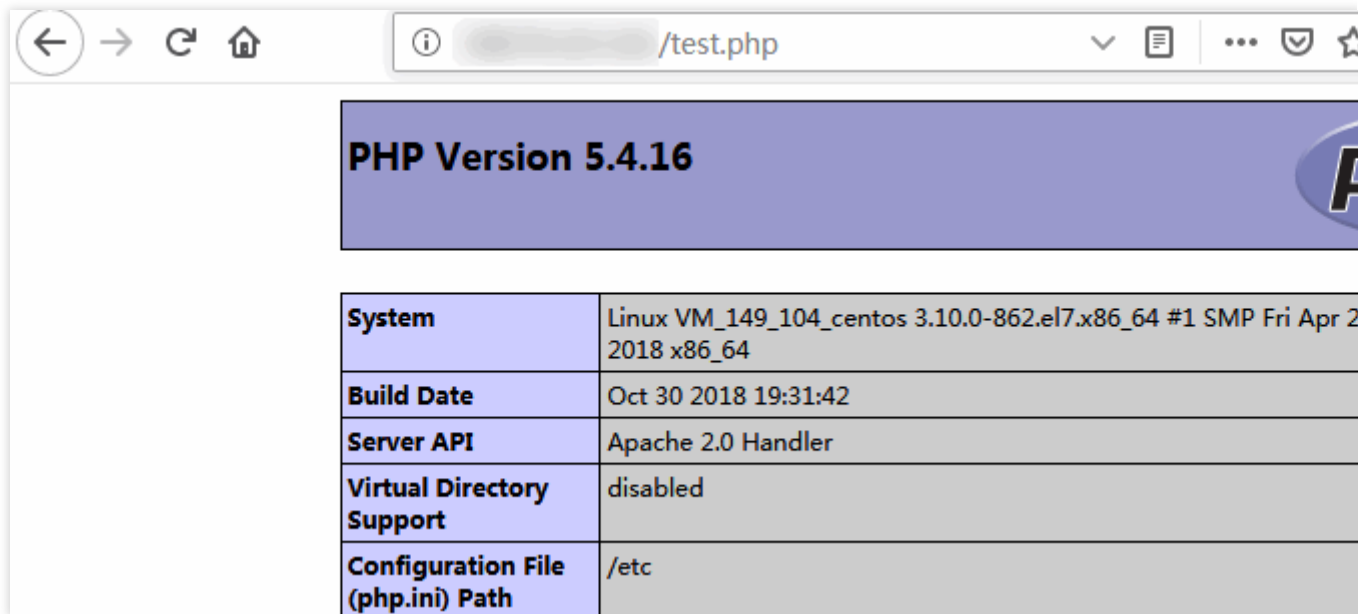
```
<?php
echo '<title>Test Page</title>';
phpinfo()
?>
```

3. **Esc**를 누르고 **:wq**를 입력하여 파일을 저장하고 뒤로 돌아갑니다.
4. 브라우저에서 해당 `test.php` 파일에 액세스하고 환경 설정 성공 여부를 조회합니다.



`http://CVM의 공인 IP/test.php`

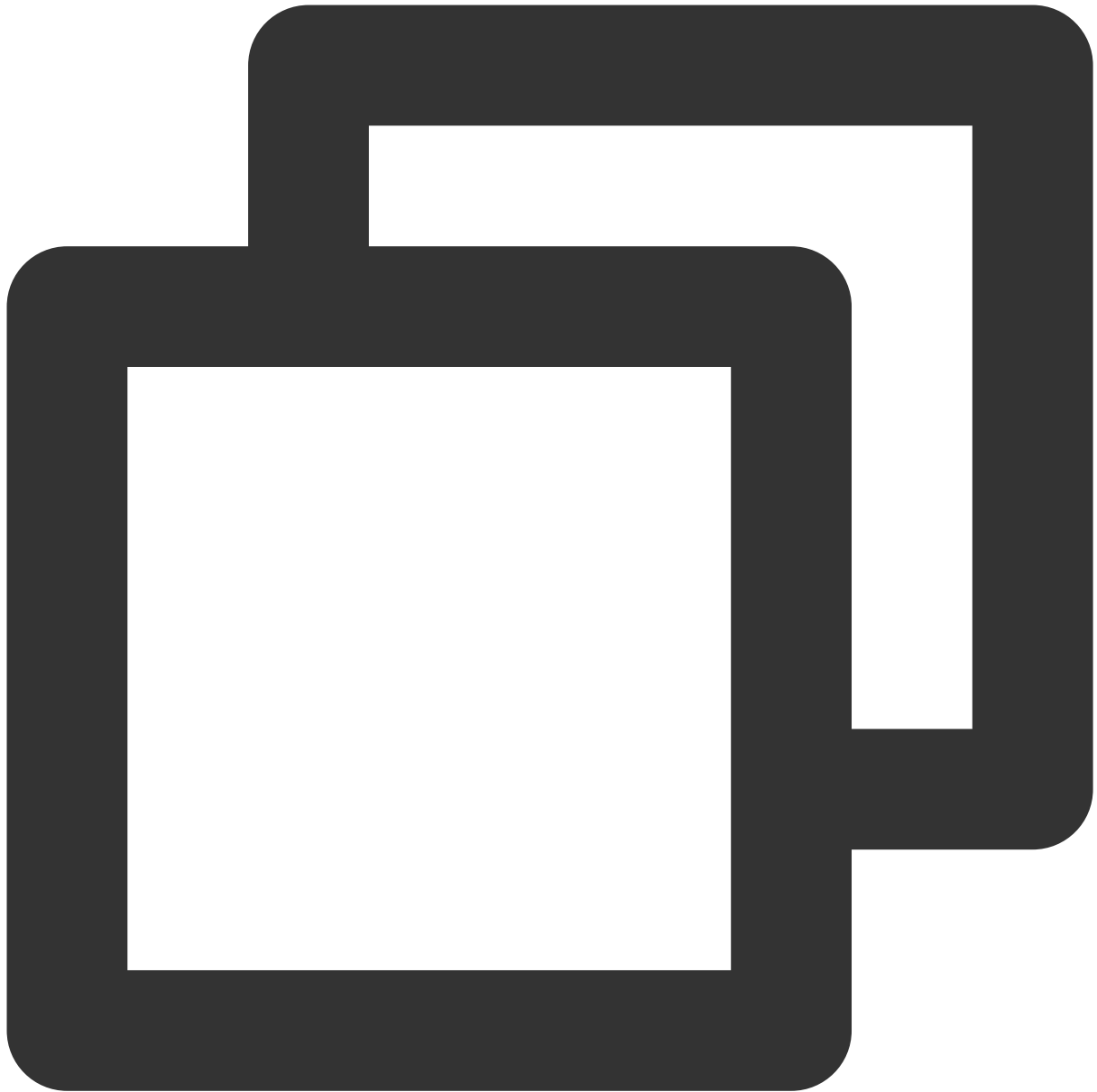
다음 페이지가 나타나면 LAMP 환경 설정 성공을 의미합니다.



3단계: Discuz! 설치 및 설정

Discuz! 다운로드

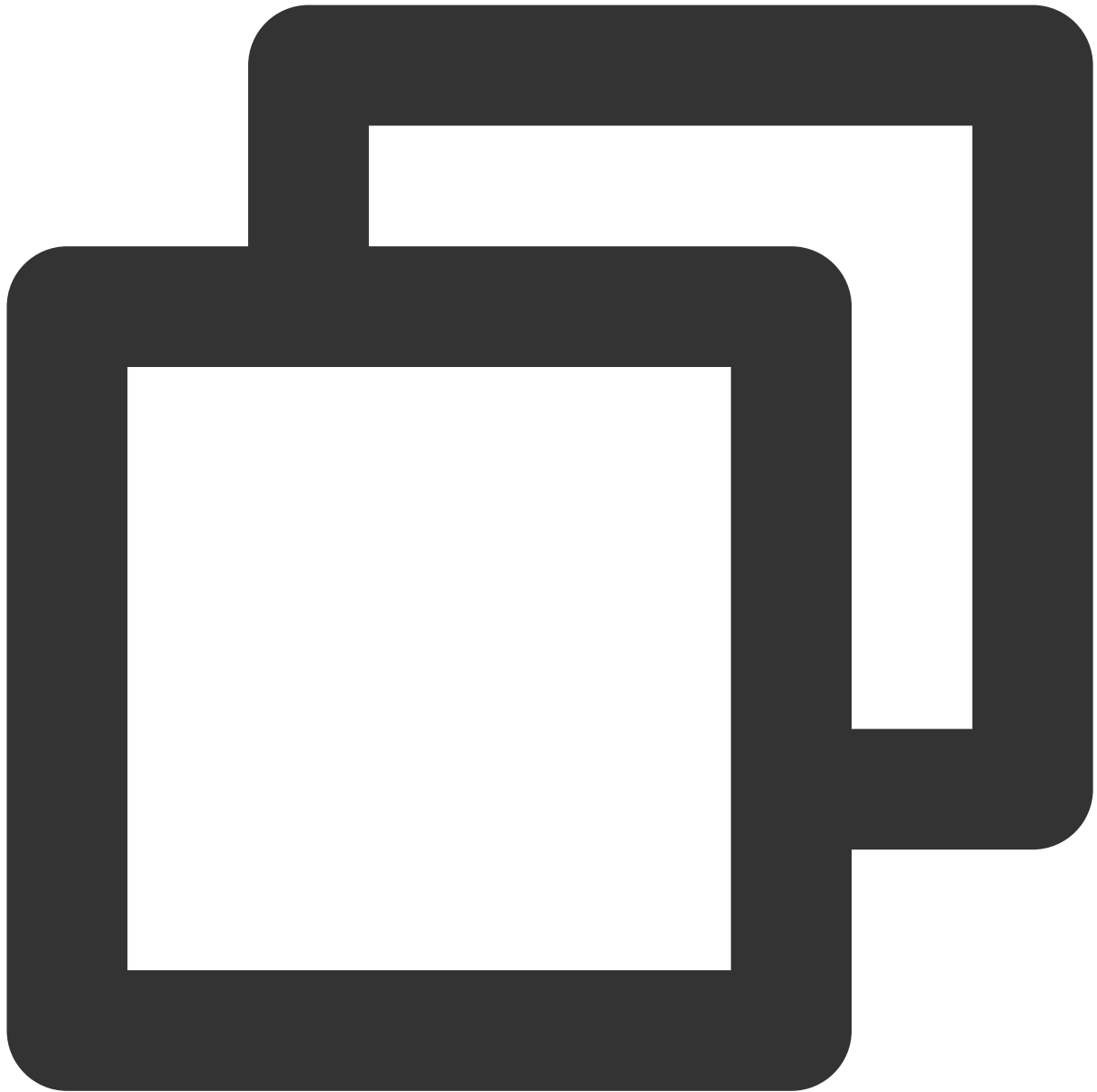
다음 명령어를 실행하여 설치 패키지를 다운로드 합니다.



```
git clone https://gitee.com/Discuz/DiscuzX.git
```

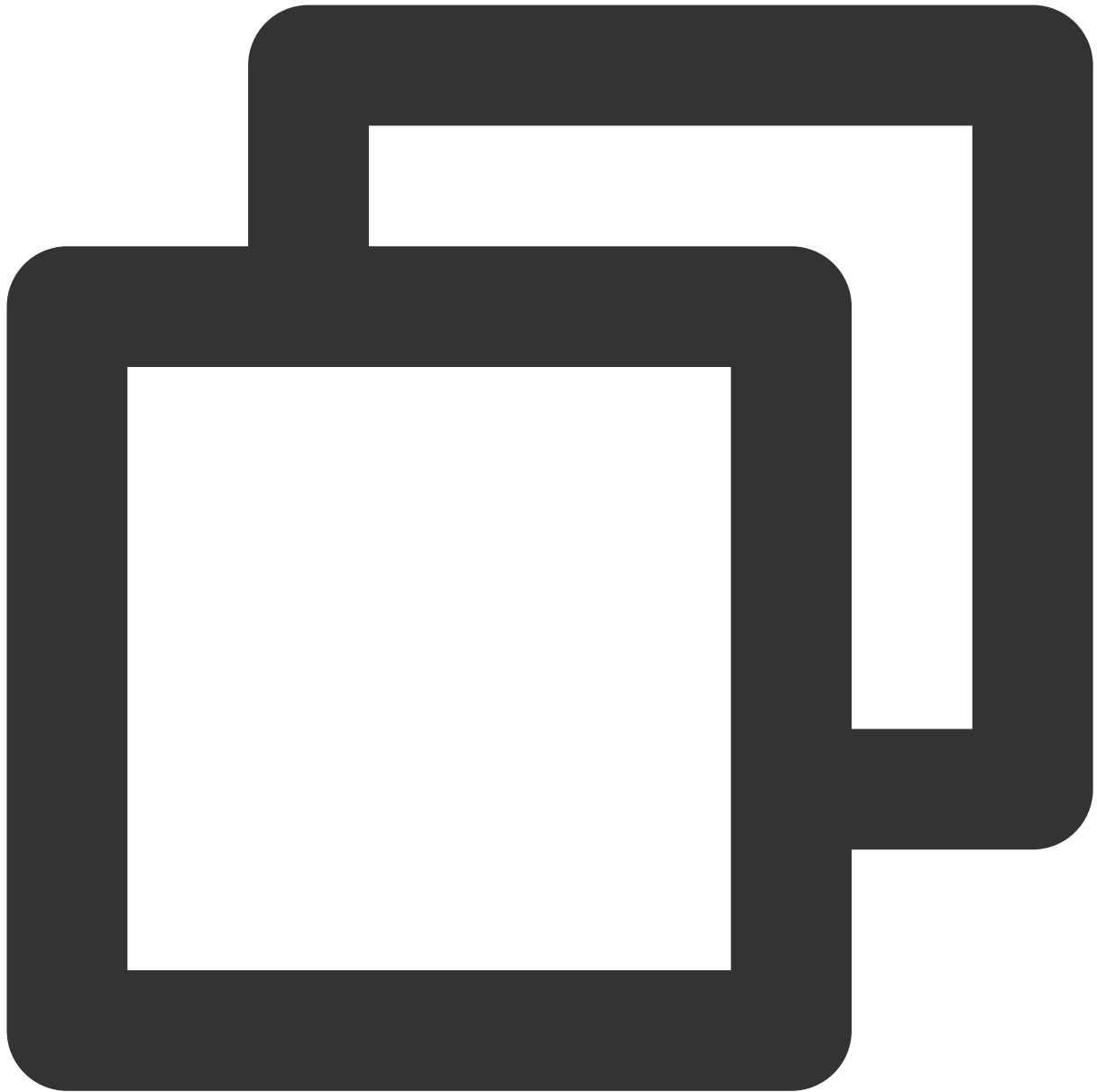
설치 준비 작업

1. 다음 명령어를 실행하여 다운로드 완료한 설치 디렉터리로 이동합니다.



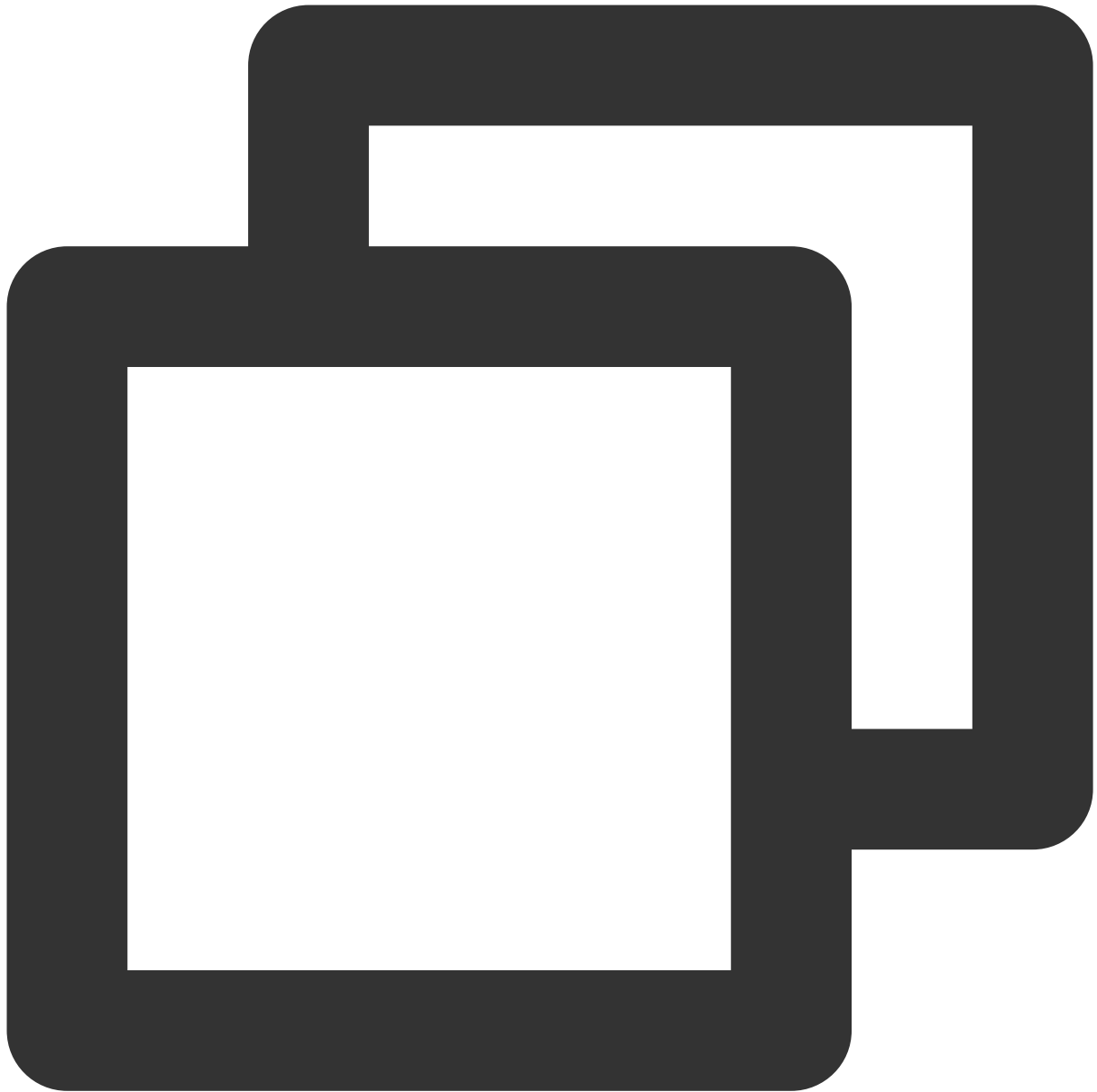
```
cd DiscuzX
```

2. 다음 명령어를 실행하여 "upload" 폴더 내의 모든 파일을 `/var/www/html/` 로 복사합니다.



```
cp -r upload/* /var/www/html/
```

3. 다음 명령어를 실행하여 쓰기 권한을 기타 사용자에게 부여합니다.



```
chmod -R 777 /var/www/html
```

Discuz! 설치

1. Web 브라우저 주소창에 Discuz! 사이트의 IP 주소(즉, CVM 인스턴스의 공용 IP 주소) 또는 [관련 작업](#)을 통해 획득한 가용 도메인을 입력하면 바로 Discuz! 설치 인터페이스를 확인할 수 있습니다.

설명 :

본문은 설치 단계만 안내합니다. 버전이 너무 낮다는 보안 경고가 있을 경우 더 높은 버전의 이미지를 사용하는 것이 좋습니다.

2. 동의를 클릭하여 설치 환경 확인 페이지로 이동합니다.
3. 현재 상태가 정상임을 확인한 후, **다음 단계**를 클릭하여 실행 환경 설정 페이지로 이동합니다.
4. 새로 설치를 선택하고 **다음 단계**를 클릭하여 데이터베이스 생성 페이지로 이동합니다.
5. 페이지 알림에 따라 정보를 작성하여 Discuz!를 위한 1개의 데이터베이스를 생성합니다.

주의사항 :

[필수 소프트웨어 설치](#)에서 설정한 root 계정과 비밀번호를 이용해 데이터베이스에 연결하고 시스템 메일함, 관리자 계정, 비밀번호와 Email을 설정하십시오.

자신의 관리자 아이디와 비밀번호를 기억하십시오.

6. **다음 단계**를 클릭하여 설치를 시작합니다.

7. 설치 완료 후 **포럼 설치가 완료되었습니다. 여기를 클릭해 액세스하세요**를 클릭하면 바로 포럼에 액세스할 수 있습니다.

관련 작업

사용자의 Discuz! 포럼 웹 사이트에 별도의 도메인을 설정할 수 있습니다. 사용자는 복잡한 IP 주소를 사용할 필요 없이 기억하기 쉬운 도메인으로 웹 사이트에 액세스할 수 있습니다. 포럼을 구축하여 학습용으로만 사용하는 일부 사용자의 경우, IP를 사용해 직접 설치 및 임시 사용이 가능하지만 이를 권장하지는 않습니다.

FAQ

CVM 사용 도중 문제가 생겼을 경우, 아래의 문서를 참고하여 실제 상황에 따라 문제를 분석 및 해결할 수 있습니다.

CVM 로그인 문제는 [키 관련 문제](#), [로그인 및 원격 연결](#)을 참고하십시오.

CVM 네트워크 문제는 [IP 주소 문제](#), [포트 관련 문제](#)를 참고하십시오.

CVM 디스크 문제는 [시스템 디스크와 데이터 디스크](#)를 참고하십시오.

Ghost 블로그 수동 구축

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

Ghost는 Node.js 언어로 작성된 오픈 소스 블로그 플랫폼으로, Ghost를 사용하여 블로그를 빠르게 구축하고 온라인 게시 프로세스를 간소화할 수 있습니다. 이 문서는 Tencent Cloud CVM에서 Ghost 개인 웹사이트를 수동으로 구축하는 방법을 설명합니다.

Ghost 웹 사이트 구축을 위해 자주 사용하는 명령어인 [Ubuntu 환경에서 Apt-get을 통해 소프트웨어 설치](#)등의 Linux 운영 체제와 명령어를 숙지해야 합니다.

소프트웨어

본문에서 Ghost 블로그를 구축하는 데 사용된 운영 체제 및 소프트웨어 버전은 다음과 같습니다.

운영체제: Ubuntu 20.04.

Nginx: 본 문서는 Web 서버 Nginx 1.18.0을 예시로 사용합니다.

MySQL: 본 문서는 데이터베이스 MySQL 8.0.25를 예시로 사용합니다.

Node.js: 본 문서는 런타임 환경 Node.js 14.17.0 버전을 예시로 사용합니다.

Ghost : Ghost 4.6.4

전제 조건

Linux CVM을 구비해야 합니다. CVM을 구매하지 않았다면, [Linux CVM 커스텀 설정](#)을 참고하시기 바랍니다.

Ghost 블로그 설정에는 이미 ICP비안이 완료되고, CVM 리졸브가 완료된 도메인을 사용해야 합니다.

작업 순서

1단계: Linux 인스턴스 로그인

[Linux 인스턴스에 로그인](#)합니다. 실제 작업 스타일에 따라 다른 로그인 방식을 선택할 수도 있습니다.

[원격 로그인 소프트웨어를 사용하여 Linux 인스턴스 로그인](#)

[SSH를 사용하여 Linux 인스턴스에 로그인](#)

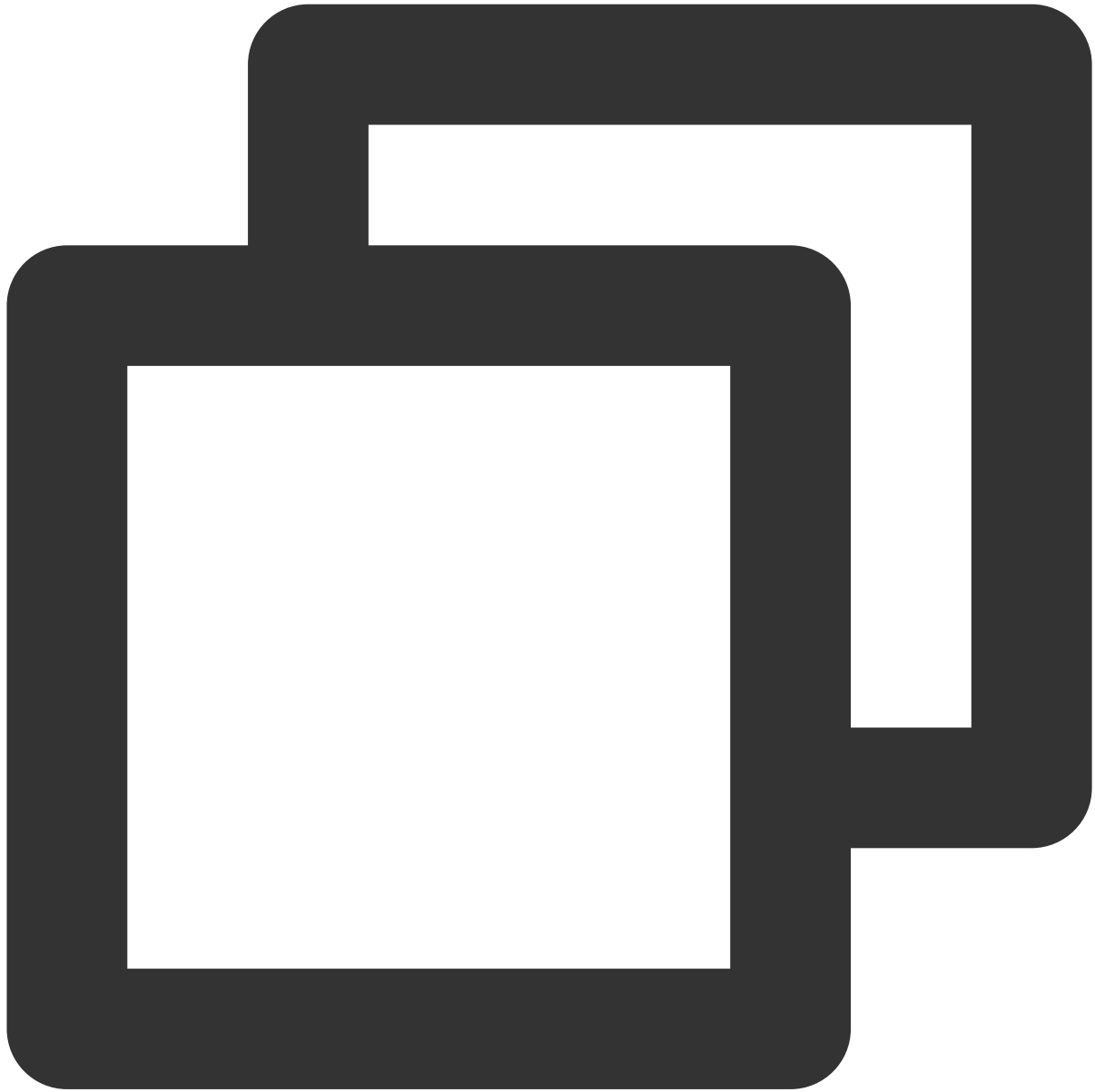
2단계: 신규 사용자 생성

1. Ubuntu 운영 체제의 CVM에 로그인한 후, [로그인](#), [원격 연결](#)을 참고하여 root 사용자로 전환하십시오.

2. 다음 명령어를 실행하여 신규 사용자를 생성하십시오. 본 문서는 'user'를 예시로 사용합니다.

주의사항 :

사용자 이름으로 'ghost'를 사용하지 마십시오. Ghost-CLI와 충돌할 수 있습니다.



```
adduser user
```

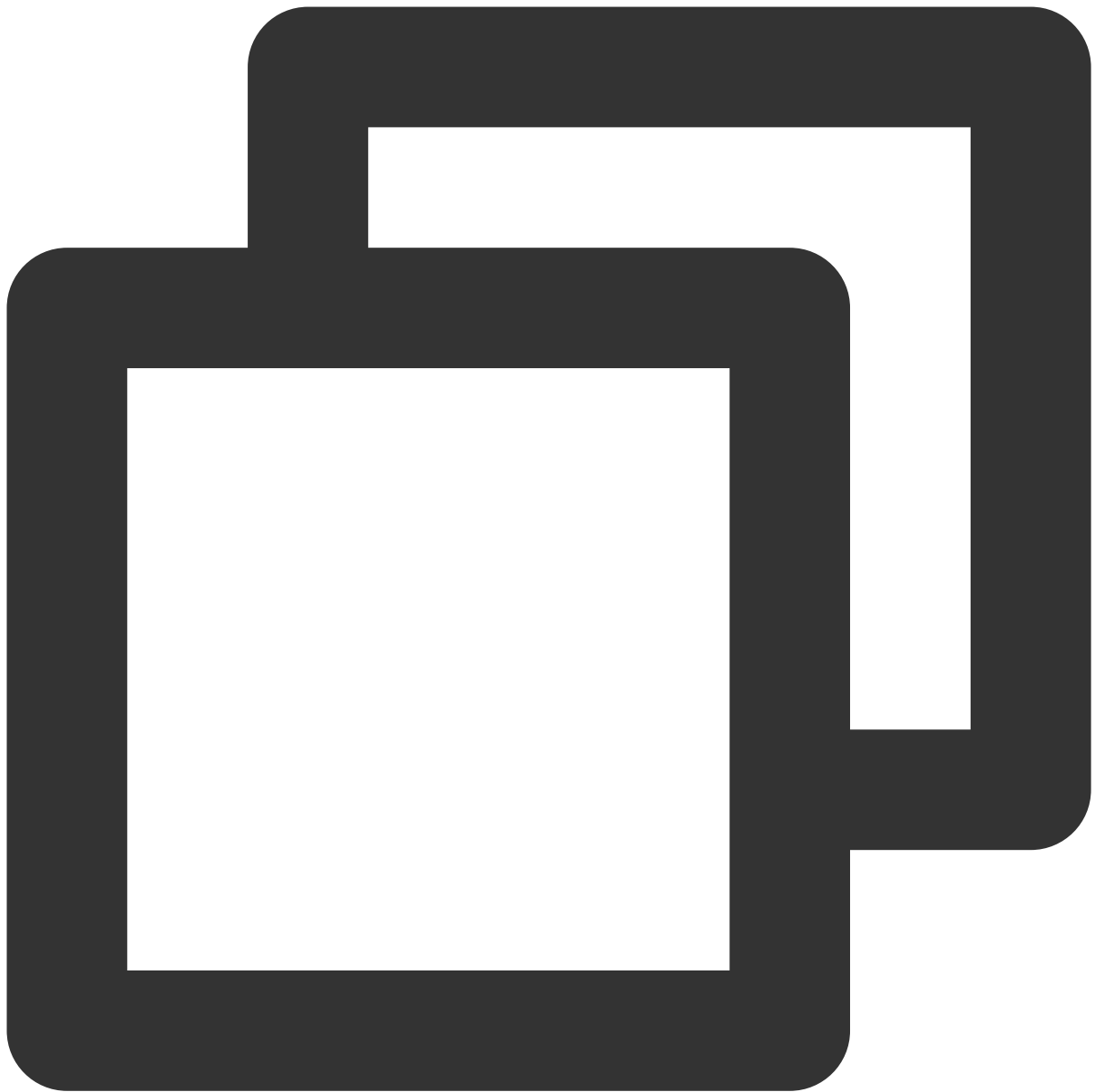
3. 안내에 따라 사용자 비밀번호를 입력 및 확인합니다. 비밀번호는 표시 안 함으로 기본 설정되어 있으며 입력 후 **Enter**를 누르면 다음 단계로 넘어갑니다.

4. 실제 상황에 따라 사용자 관련 정보를 입력합니다. 입력하지 않아도 **Enter**를 눌러 다음 단계를 진행할 수 있습니다.

5. **Y**를 입력하여 정보를 확인한 후, **Enter**를 눌러 설정을 완료하면 다음과 같이 표시됩니다.

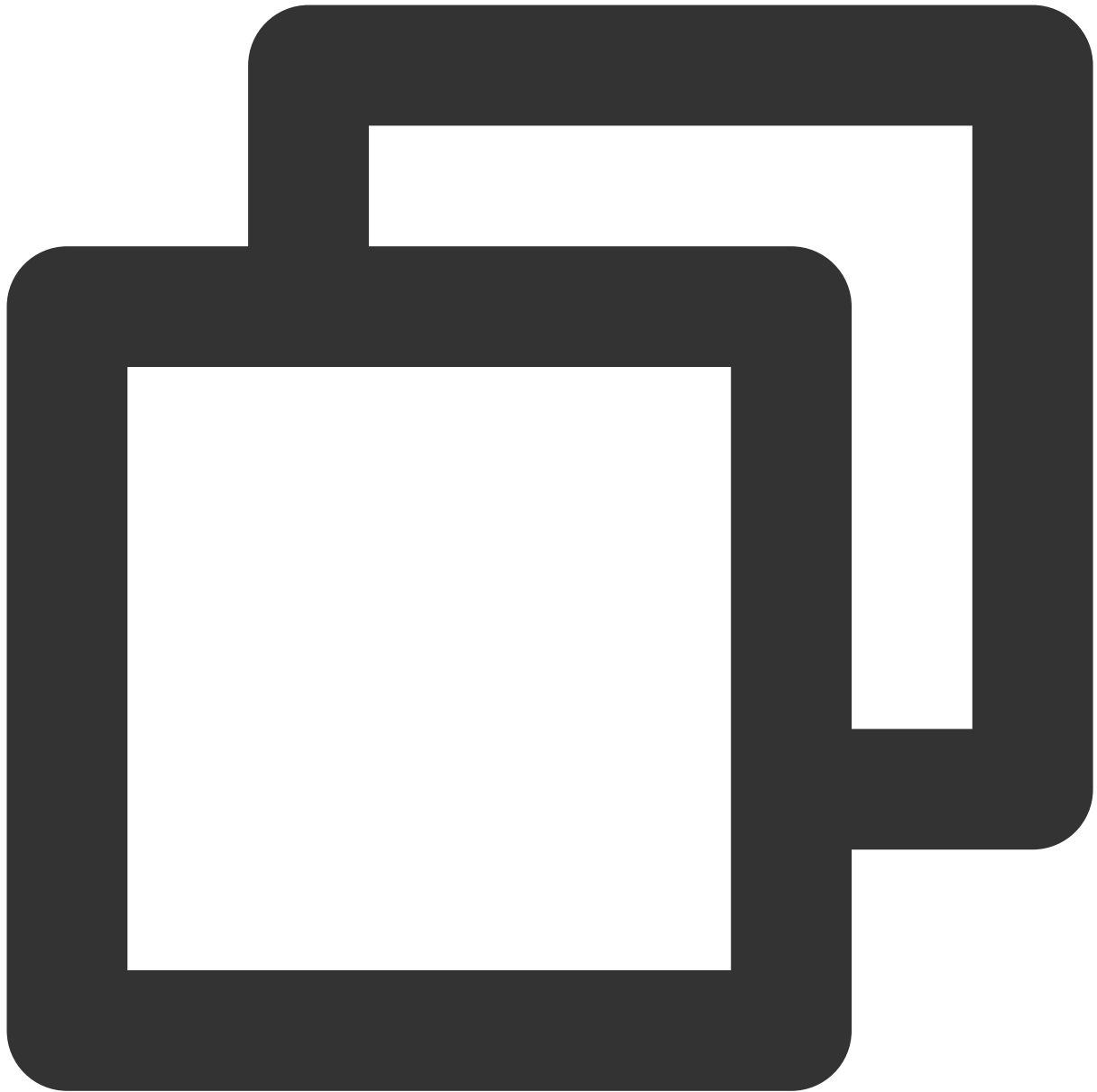
```
root@VM-0-22-ubuntu:/home/ubuntu# adduser user
Adding user `user' ...
Adding new group `user' (1000) ...
Adding new user `user' (1000) with group `user' ...
Creating home directory `/home/user' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for user
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] Y
root@VM-0-22-ubuntu:/home/ubuntu#
```

6. 다음 명령어를 실행하여 사용자 권한을 추가합니다.



```
usermod -aG sudo user
```

7. 다음 명령어를 실행하여 'user'로 전환합니다.



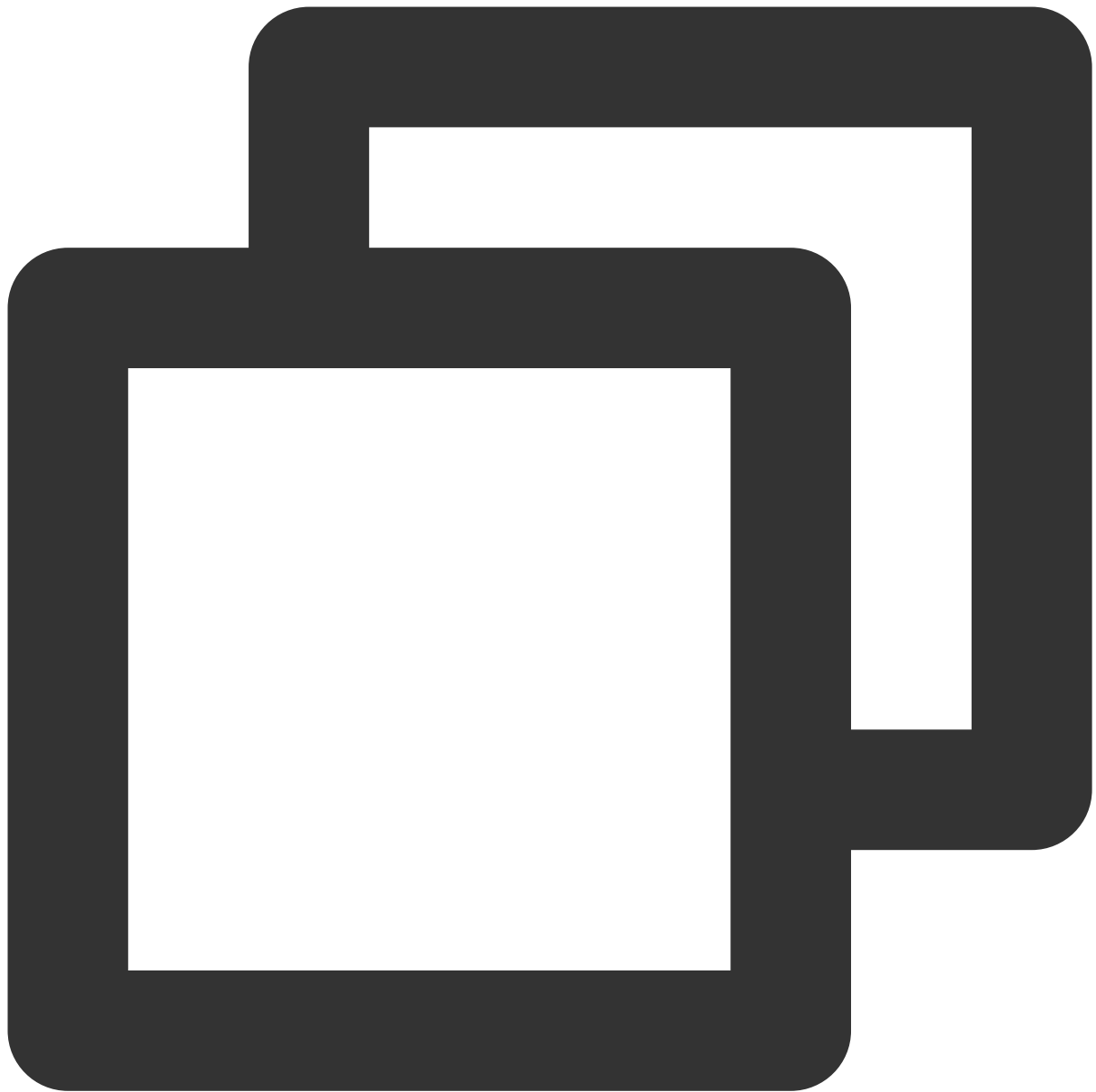
```
su - user
```

3단계: 설치 패키지 업데이트

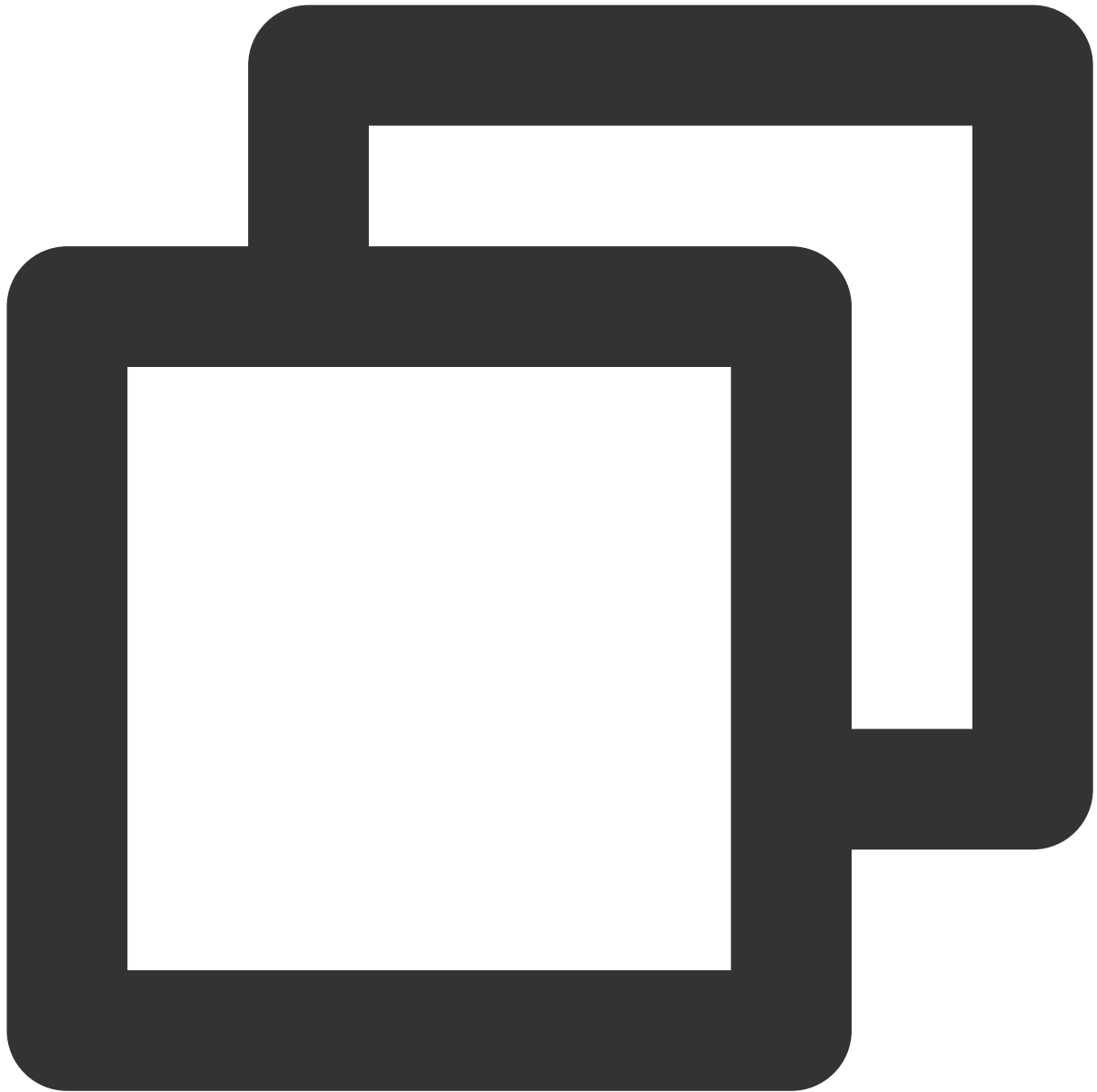
다음 명령어를 순서대로 실행하여 설치 패키지를 업데이트합니다.

설명 :

인터페이스의 안내에 따라 'user'의 비밀번호를 입력하고 **Enter**를 눌러 업데이트를 시작합니다.



```
sudo apt-get update
```

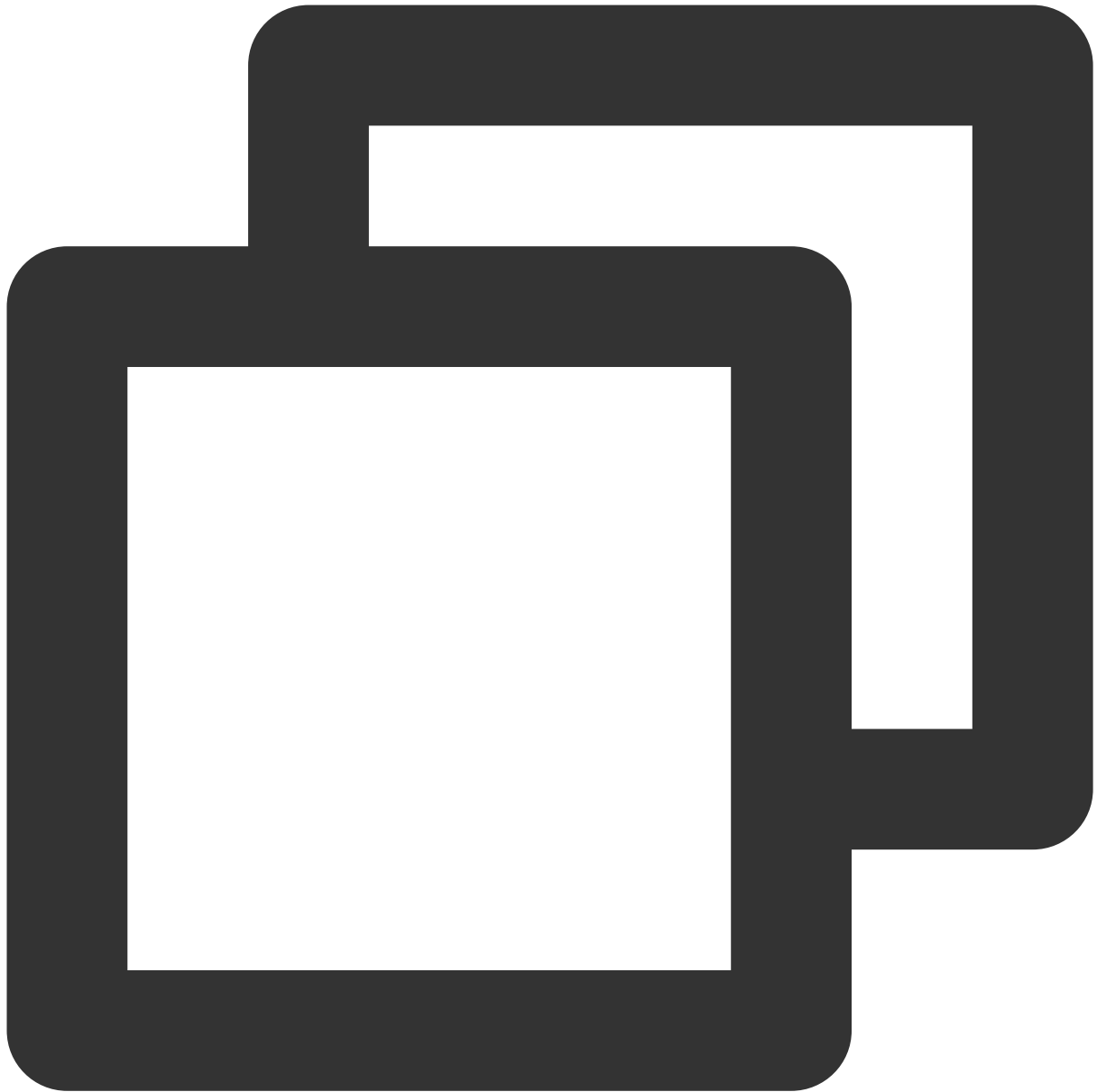


```
sudo apt-get upgrade -y
```

4단계: 환경 설정

Nginx 설치 및 설정

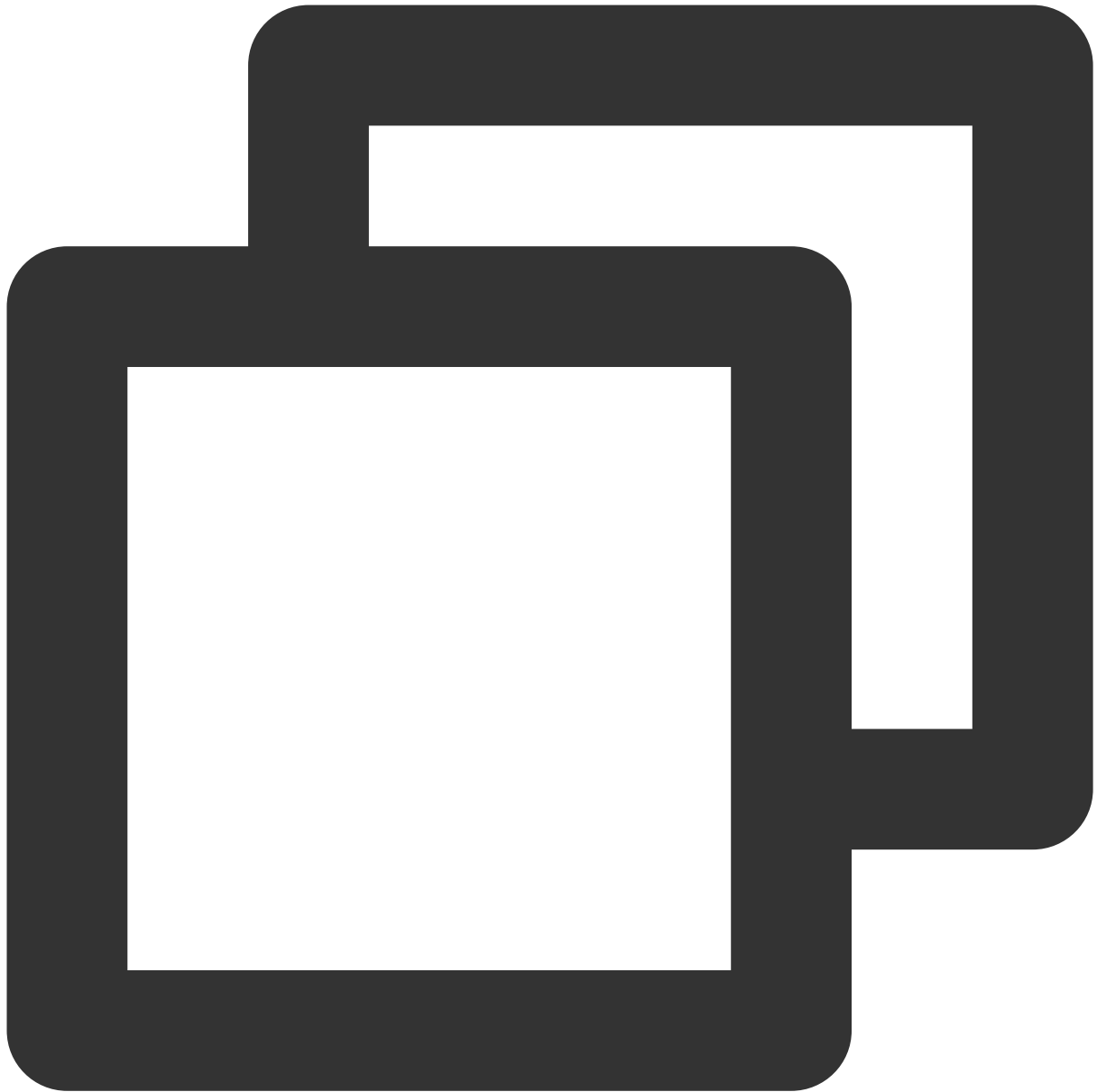
다음 명령어를 실행하여 Nginx를 설치합니다.



```
sudo apt-get install -y nginx
```

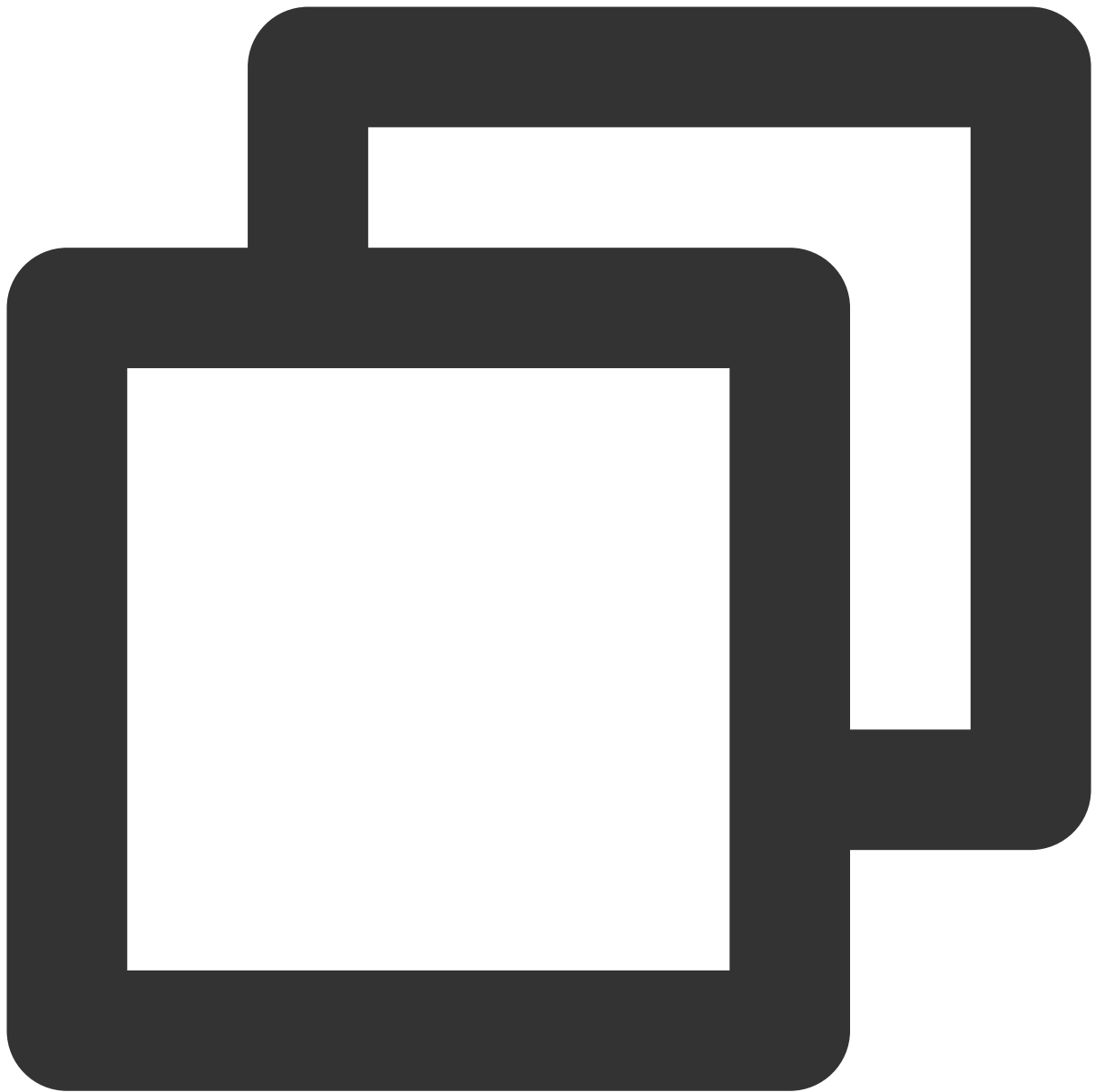
MySQL 설치 및 설정

1. 다음 명령어를 실행하여 MySQL을 설치합니다.



```
sudo apt-get install -y mysql-server
```

2. 다음 명령어를 실행하여 MySQL을 연결합니다.

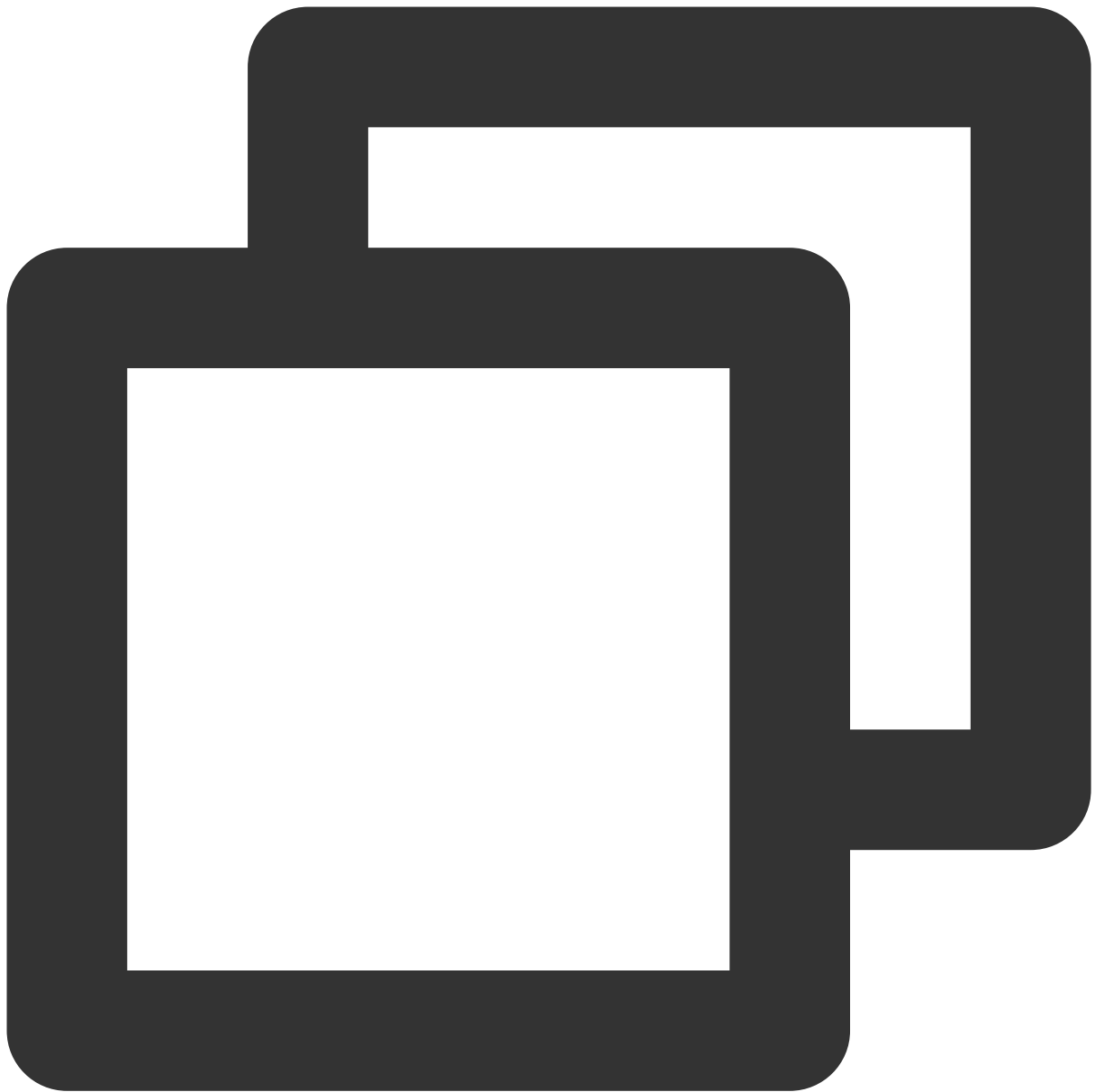


```
sudo mysql
```

3.

다음

명령어를 실행하여 Ghost가 사용할 데이터베이스를 생성합니다. 본문은 'ghost_data'를 예시로 사용합니다.

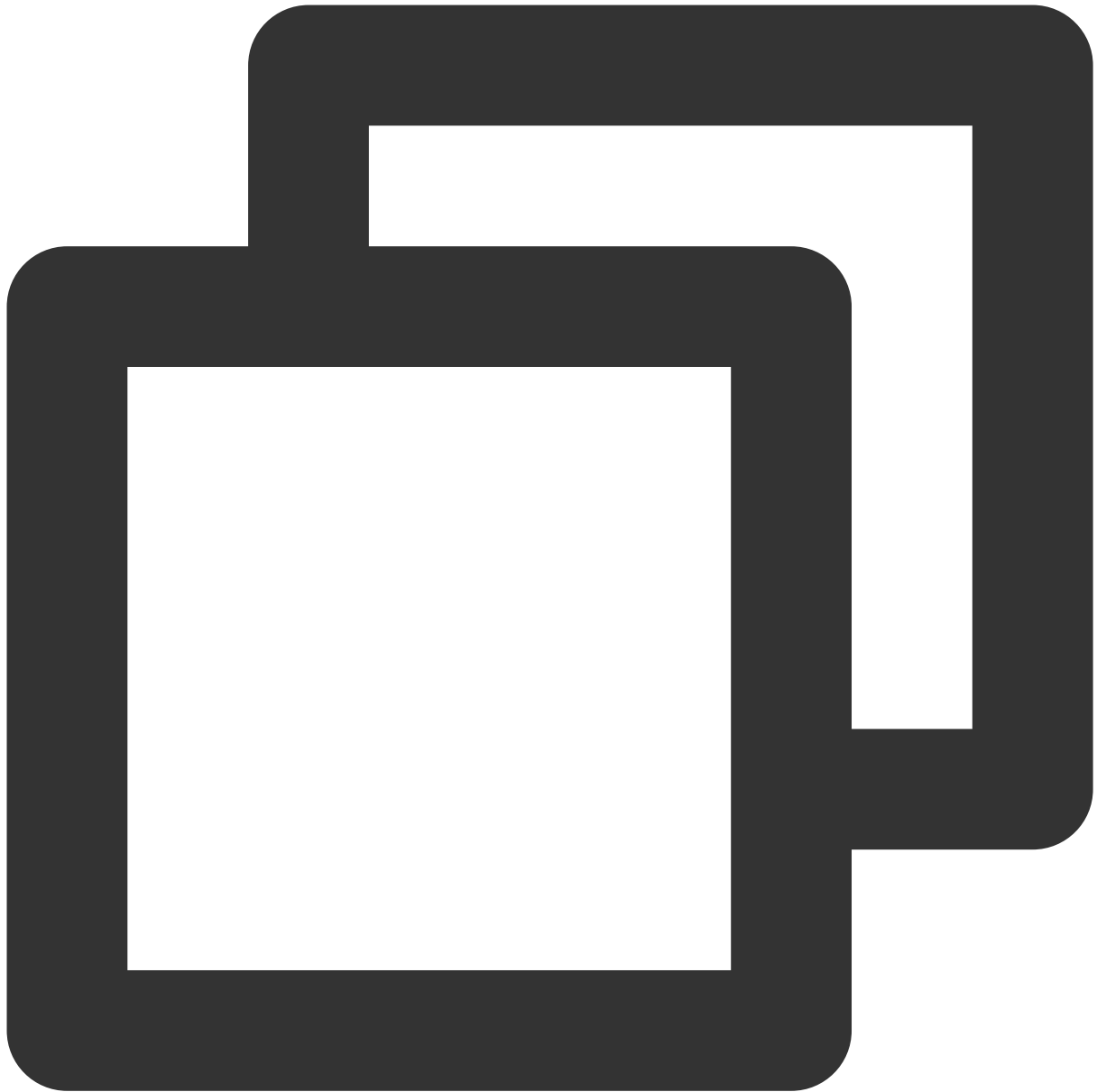


```
CREATE DATABASE ghost_data;
```

4.

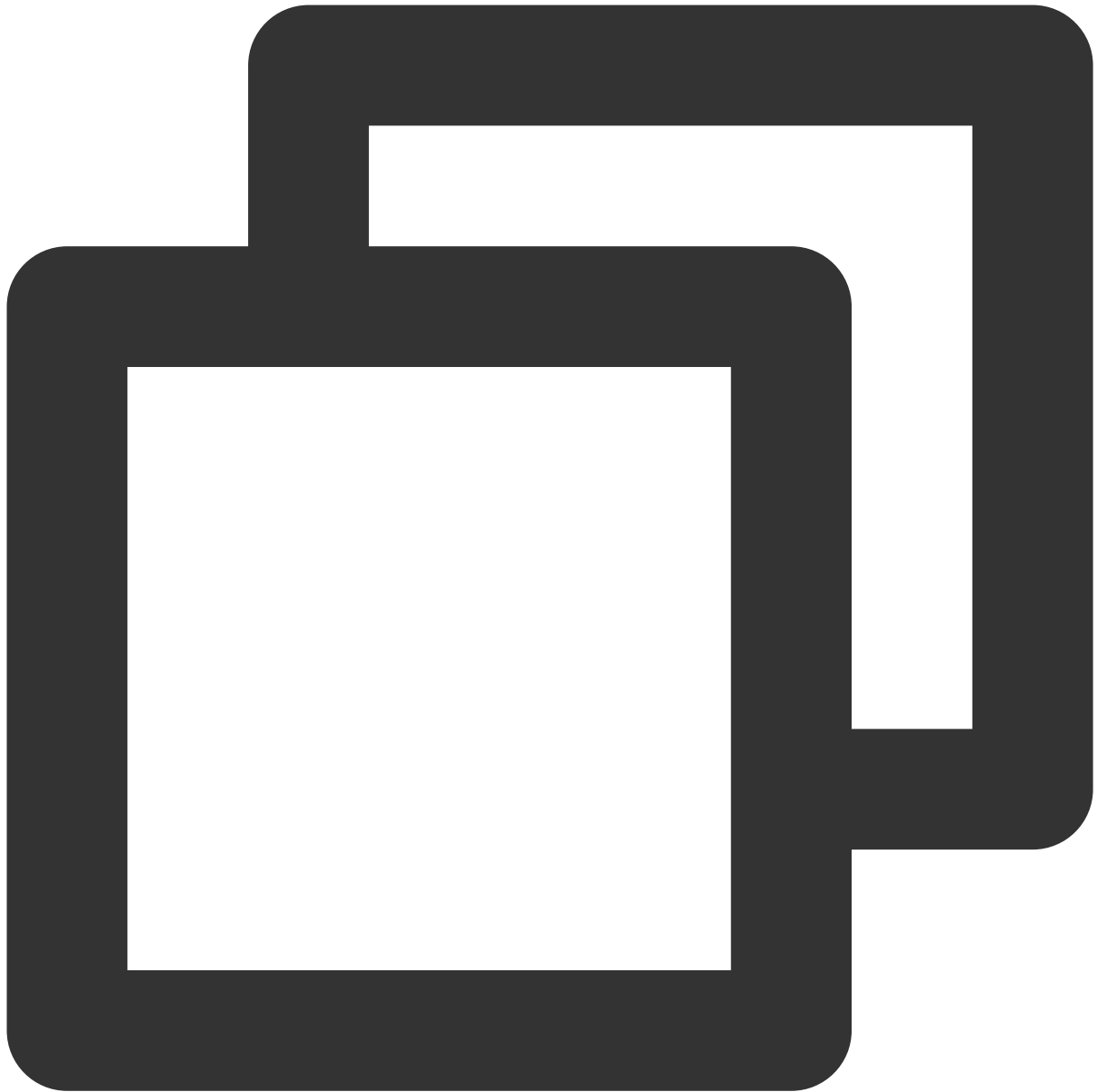
다음

명령어를 실행하여 root 계정 비밀번호를 설정합니다.



```
ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'root' 계정
```

5. 다음 명령어를 실행하여 MySQL을 종료합니다.



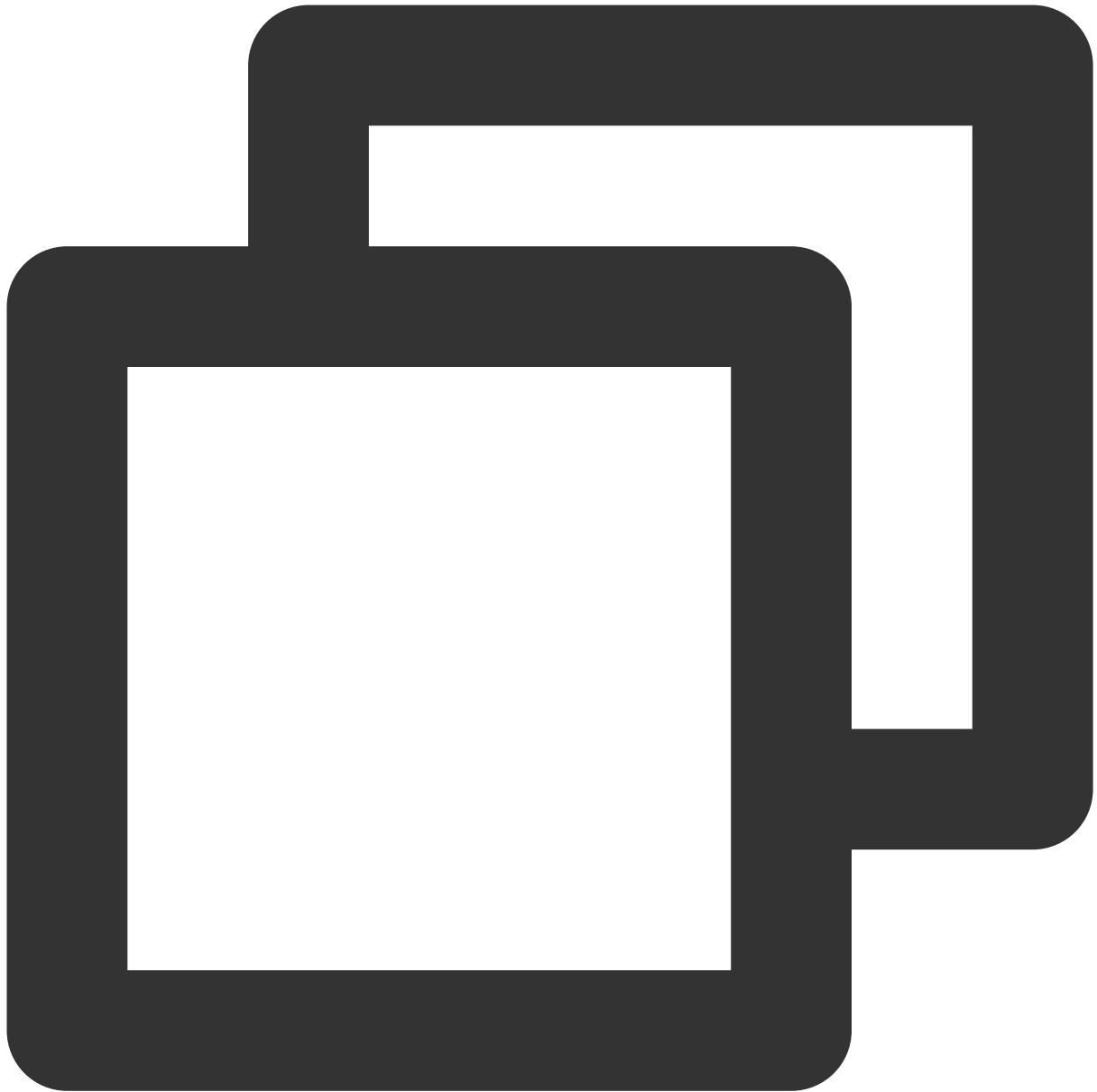
```
\\q
```

Node.js 설치 및 설정

1. 다음 명령어를 실행하여 Node.js가 지원하는 설치 버전을 추가합니다.

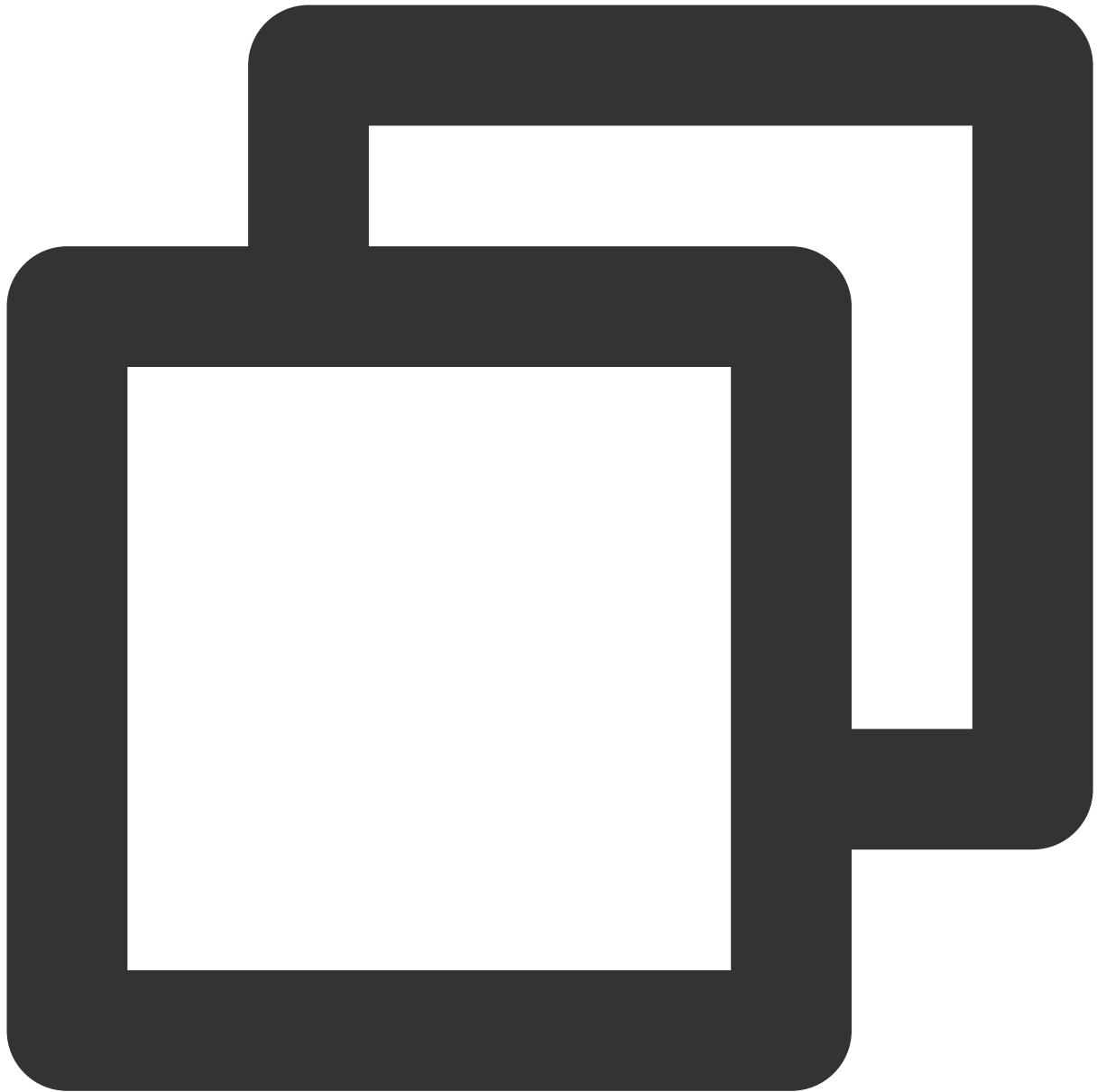
설명 :

Ghost 각 버전마다 Node.js에 대한 버전 요구 사항이 다르므로 [supported Node versions](#) 및 다음 명령어를 참고하여 해당 명령어를 실행합니다.



```
curl -sL https://deb.nodesource.com/setup_14.x | sudo -E bash
```

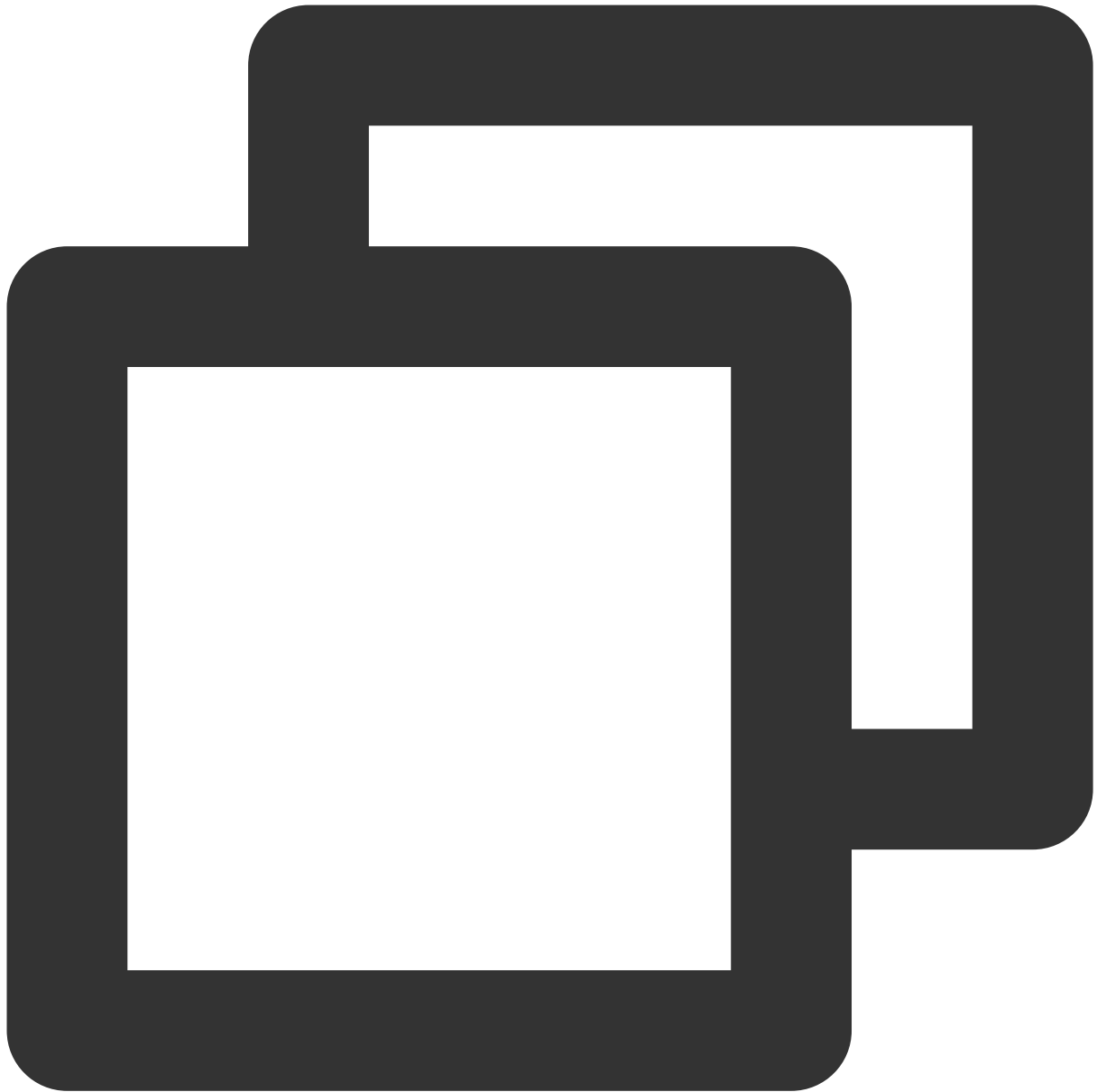
2. 다음 명령어를 실행하여 Node.js를 설치합니다.



```
sudo apt-get install -y nodejs
```

Ghost-CLI 설치

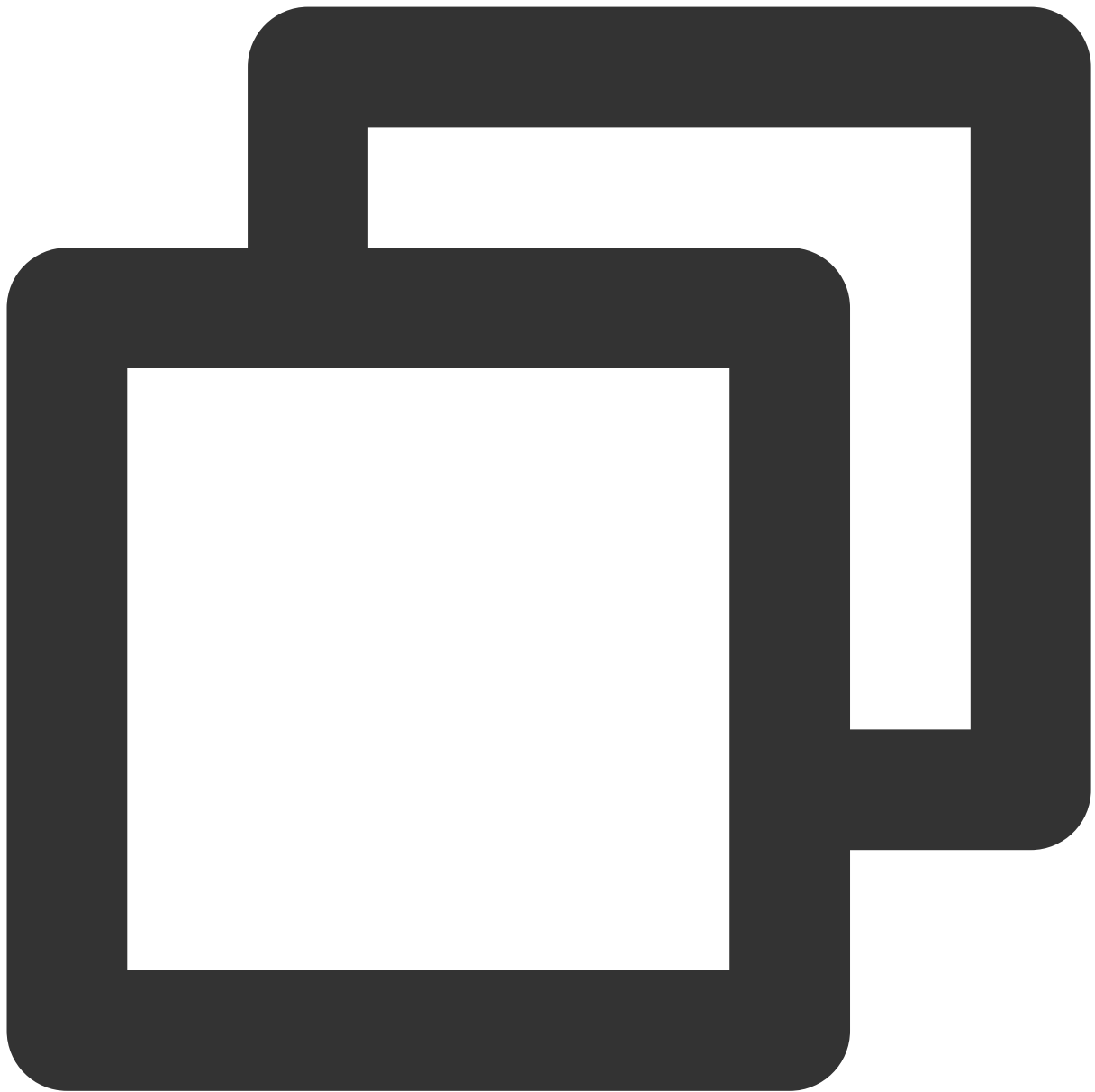
다음 명령어를 실행하여 Ghost-CLI을 설치하여 Ghost를 빠르게 설정합니다.



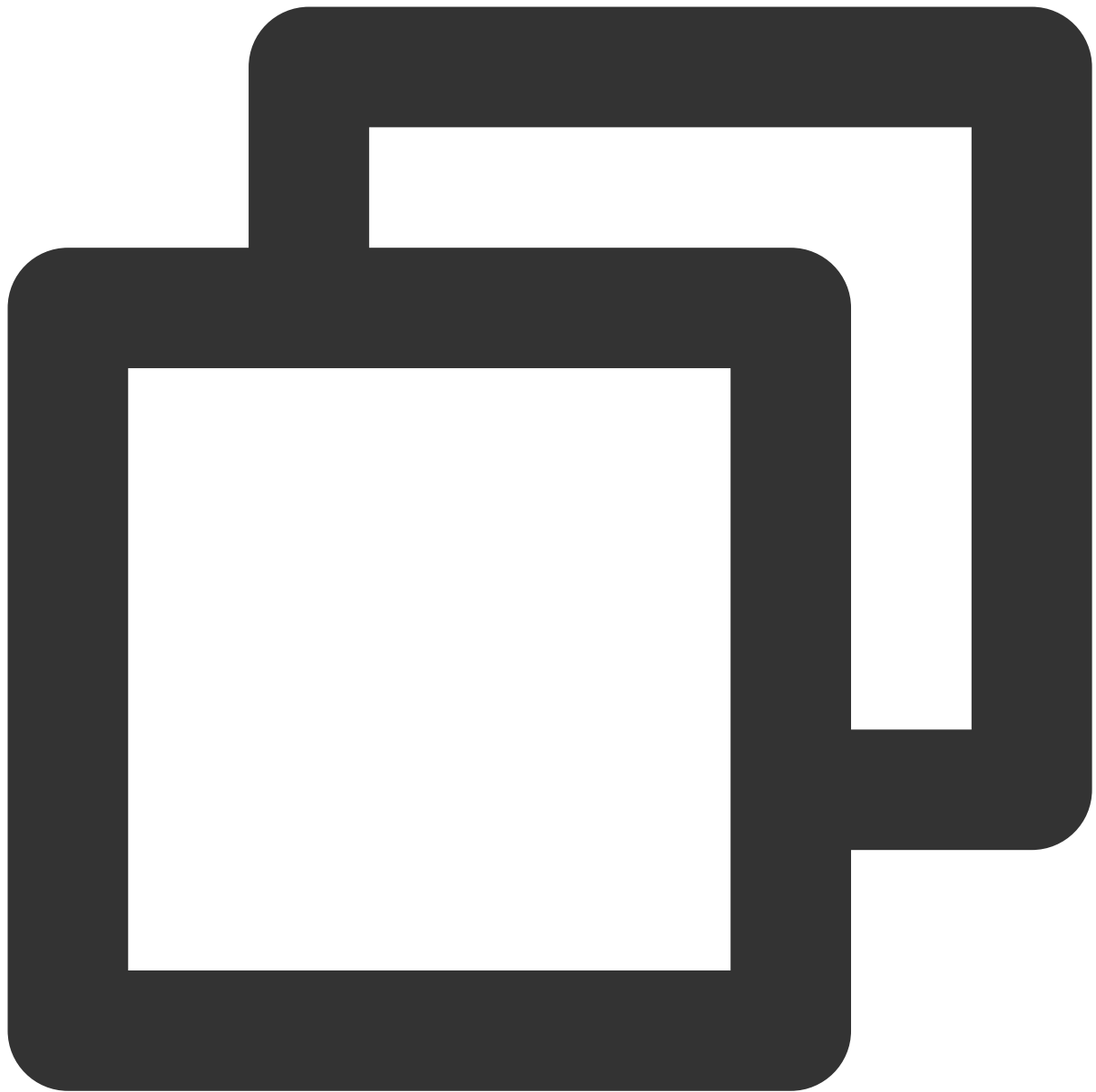
```
sudo npm install ghost-cli@latest -g
```

5단계: Ghost 설치 및 설정

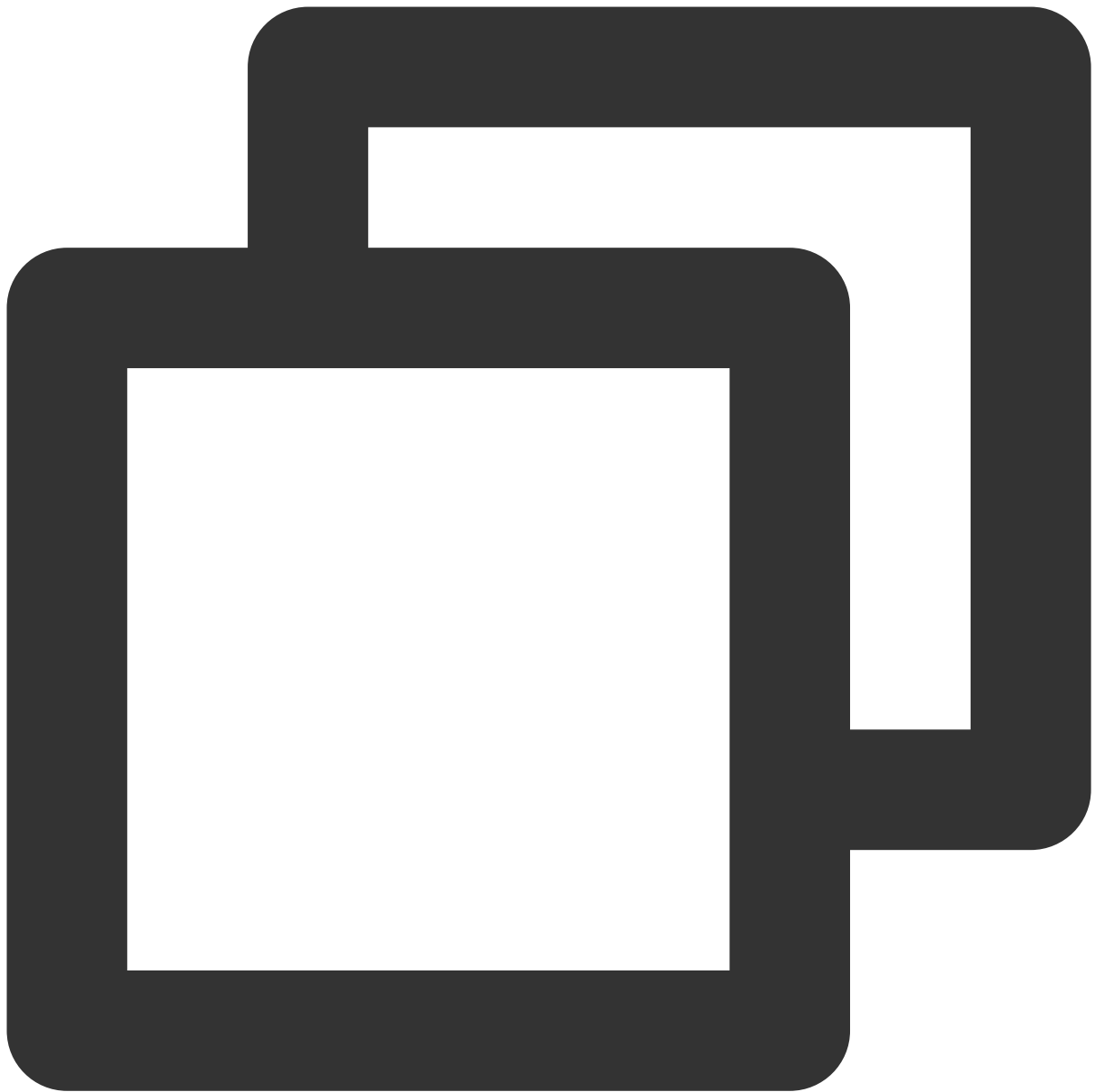
1. 다음 명령어를 순서대로 실행하여 Ghost 설치 디렉터리를 설정 및 이동합니다.



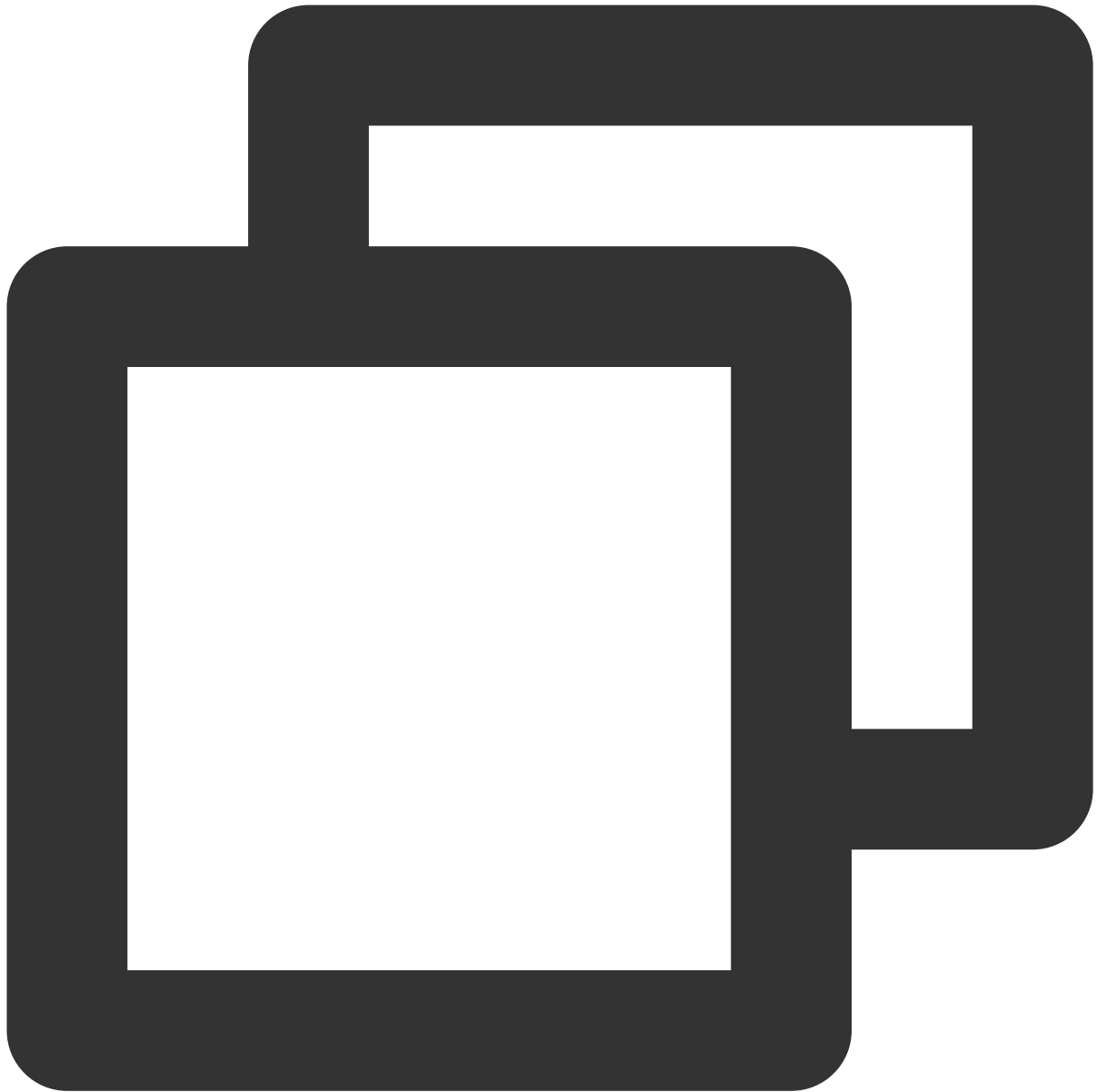
```
sudo mkdir -p /var/www/ghost
```



```
sudo chown user:user /var/www/ghost
```

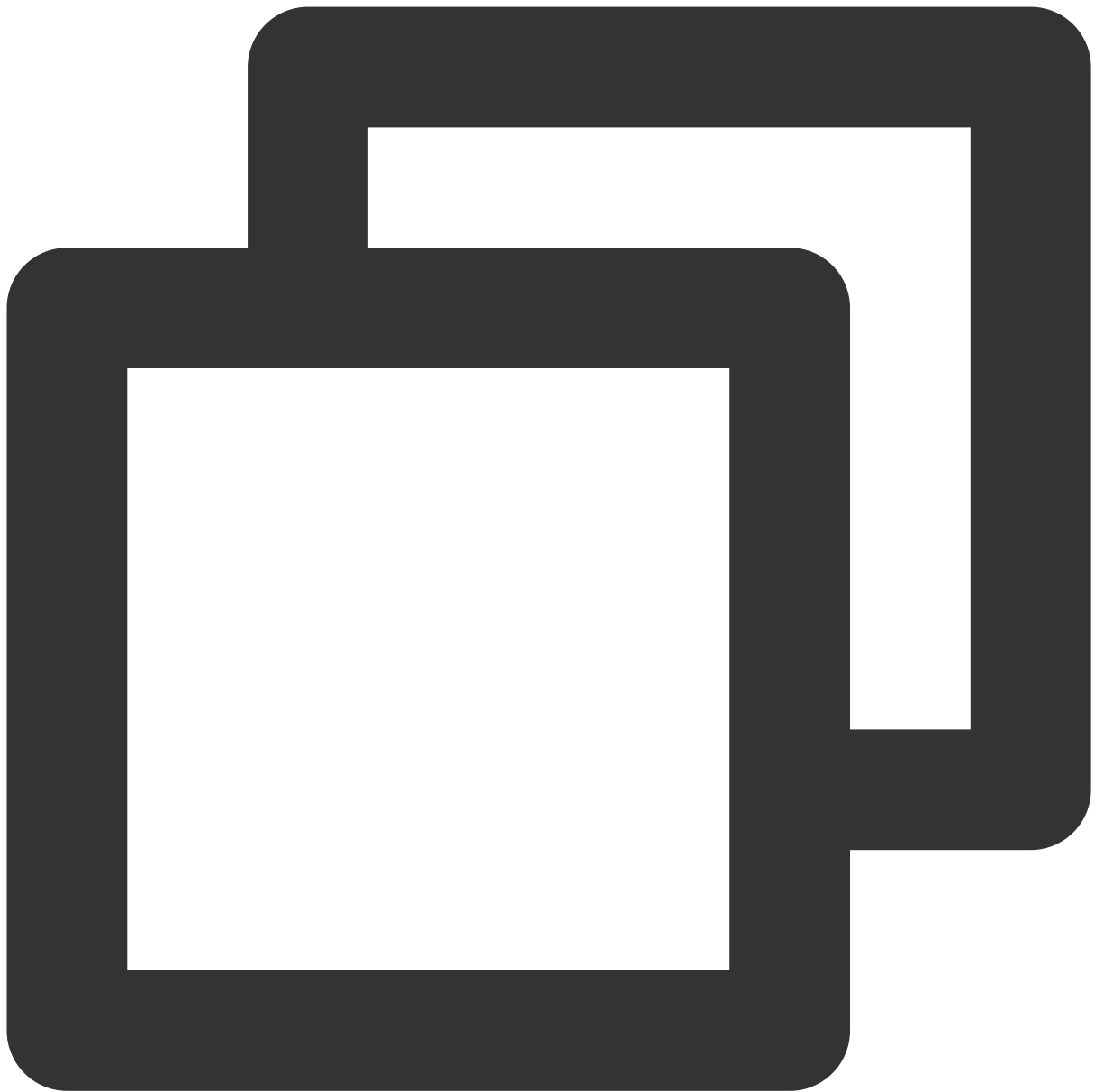


```
sudo chmod 775 /var/www/ghost
```



```
cd /var/www/ghost
```

2. 다음 명령어를 실행하여 Ghost를 설치합니다.



```
ghost install
```

3. 다음 이미지를 참고하여 설치 프로세스를 완료합니다.

```

✓ Finishing install process
? Enter your blog URL: http://www.qcloudnewshow.com
? Enter your MySQL hostname: localhost
? Enter your MySQL username: root
? Enter your MySQL password: [hidden]
? Enter your Ghost database name: ghost_data
✓ Configuring Ghost
✓ Setting up instance
+ sudo useradd --system --user-group ghost
+ sudo chown -R ghost:ghost /var/www/ghost/content
✓ Setting up "ghost" system user
? Do you wish to set up "ghost" mysql user? Yes
✓ Setting up "ghost" mysql user
? Do you wish to set up Nginx? Yes
+ sudo mv /tmp/www-qcloudnewshow-com/www.qcloudnewshow.com.conf /etc/nginx
+ sudo ln -sf /etc/nginx/sites-available/www.qcloudnewshow.com.conf /etc/n
+ sudo nginx -s reload
✓ Setting up Nginx
? Do you wish to set up SSL? Yes
? Enter your email (For SSL Certificate) azhengyx@sina.cn
+ sudo mkdir -p /etc/letsencrypt
+ sudo ./acme.sh --install --home /etc/letsencrypt
+ sudo /etc/letsencrypt/acme.sh --issue --home /etc/letsencrypt --domain w
load" --accountemail azhengyx@sina.cn
+ sudo openssl dhparam -dsaparam -out /etc/nginx/snippets/dhparam.pem 2048
+ sudo mv /tmp/ssl-params.conf /etc/nginx/snippets/ssl-params.conf
+ sudo mv /tmp/www-qcloudnewshow-com/www.qcloudnewshow.com-ssl.conf /etc/n
+ sudo ln -sf /etc/nginx/sites-available/www.qcloudnewshow.com-ssl.conf /e
+ sudo nginx -s reload
✓ Setting up SSL
? Do you wish to set up Systemd? Yes
+ sudo mv /tmp/www-qcloudnewshow-com/ghost_www-qcloudnewshow-com.service /
+ sudo systemctl daemon-reload
✓ Setting up Systemd
+ sudo systemctl is-active ghost_www-qcloudnewshow-com
? Do you want to start Ghost? Yes
+ sudo systemctl start ghost_www-qcloudnewshow-com
+ sudo systemctl is-enabled ghost_www-qcloudnewshow-com
+ sudo systemctl enable ghost_www-qcloudnewshow-com --quiet
✓ Starting Ghost

Ghost uses direct mail by default. To set up an alternative email method r
-----

Ghost was installed successfully! To complete setup of your publication, v
http://www.qcloudnewshow.com/ghost/

```

주요 설정은 다음과 같습니다.

3.1 Enter your blog URL: http://(도메인 이름) 형식의 도메인을 입력합니다.

3.2 Enter your MySQL hostname: 데이터베이스 연결 주소를 입력합니다. `localhost` 를 입력한 다음 **Enter**를 누릅니다.

3.3 Enter your MySQL username: 데이터베이스 사용자 이름을 입력합니다. `root` 를 입력한 다음 **Enter**를 누릅니다.

3.4 Enter your MySQL password: 데이터베이스 비밀번호를 입력하고 [root 계정 비밀번호 설정](#)에서 설정한 비밀번호를 입력한 다음 **Enter**를 누릅니다.

3.5 Enter your database name: Ghost가 사용할 데이터베이스를 입력합니다. [데이터베이스 생성](#)에서 생성한 `ghost_data` 를 입력한 다음 **Enter**를 누릅니다.

3.6 Do you wish to set up SSL?: HTTPS 액세스를 활성화하려면 **Y**를 입력한 다음 **Enter**를 누릅니다.

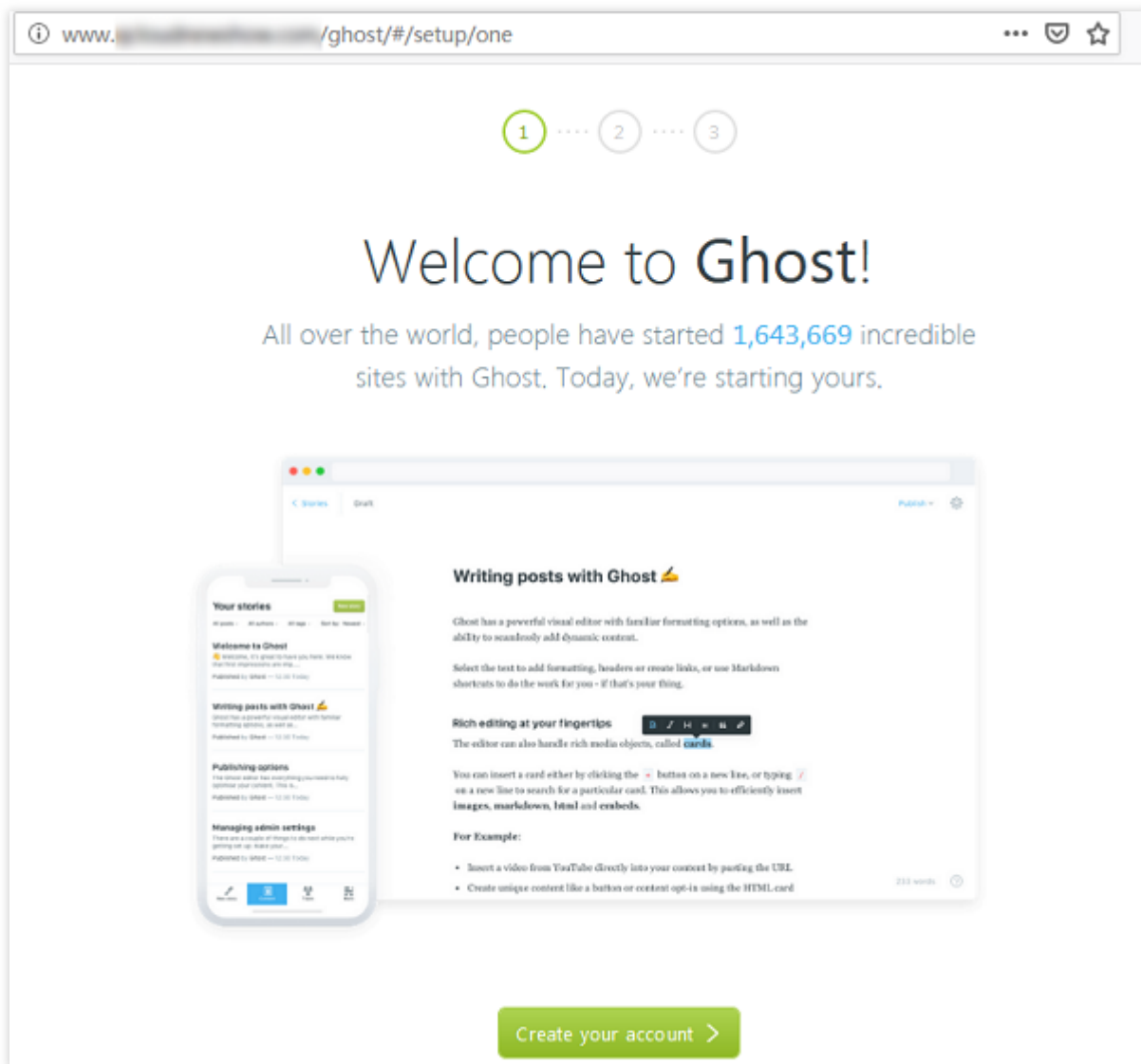
실제 상황과 페이지 안내에 따라 나머지 설정을 완료합니다. 설정을 완료하면 인터페이스 하단에 Ghost 관리자 액세스 주소가 출력됩니다.

4. 다음 이미지와 같이 로컬 브라우저를 통해 Ghost의 관리자 액세스 주소에 액세스한 후, 개인 블로그 설정을 시작합니다.

설명 :

HTTPS 액세스를 활성화한 경우, 'https://'를 사용하여 액세스 또는 블로그 설정 등의 작업을 할 수 있습니다.

[Create your account]를 클릭하여 관리자 계정을 생성합니다.



5. 다음 이미지와 같이 관련 정보를 입력한 후, [Last step]을 클릭합니다.

www.ghost.org/ghost/#/setup/two

1 2 3

Create your account

Site title

ghost

Full name

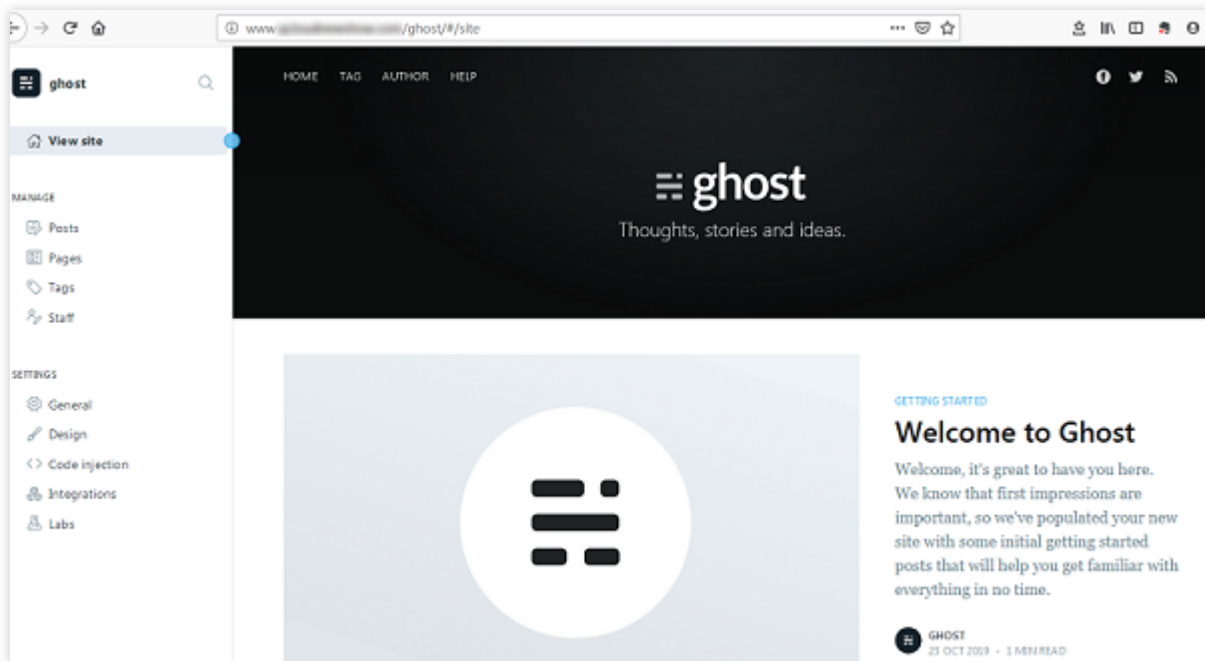
Email address

Password

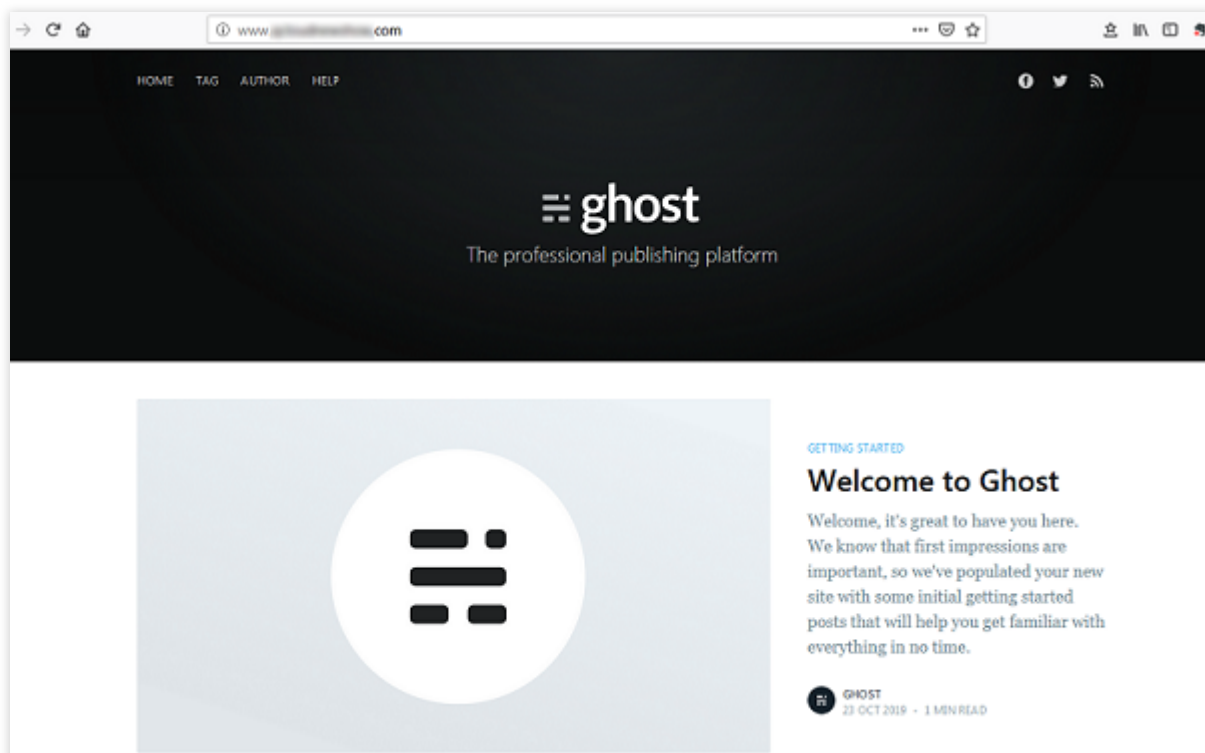
Last step: Invite staff users >

6. 블로그 생성에 다른 사람을 초대할 수 있으며, 이 단계는 생략 가능합니다.

7. 다음 이미지와 같이 관리 인터페이스에 들어가서 블로그를 관리합니다.



다음 이미지와 같이 설정이 끝나면 로컬 브라우저를 사용하여 설정된 'www.xxxxxxxx.xx' 도메인을 액세스하여 블로그를 확인합니다.



FAQ

CVM 사용 도중 문제가 생겼을 경우, 아래의 문서를 참고하여 실제 상황에 따라 문제를 분석 및 해결할 수 있습니다.

CVM 로그인 문제는 [키 관련 문제](#), [로그인](#), [원격 연결](#)을 참고하십시오.

CVM 네트워크 문제는 [IP 주소 문제](#), [포트 관련 문제](#)를 참고하십시오.

CVM 디스크 문제는 [시스템 디스크와 데이터 디스크](#)를 참고하십시오.

애플리케이션 구축

FTP 서비스 구축

Linux CVM에서 FTP 서비스 구축

최종 업데이트 날짜: : 2024-02-02 10:56:29

작업 시나리오

Vsftpd(very secure FTP daemon)는 수많은 Linux 릴리스 버전의 기본 FTP 서버입니다. 본문은 CentOS 7.6 64비트 운영 체제의 Tencent Cloud Virtual Machine(CVM)을 예시로, vsftpd 소프트웨어를 사용하여 Linux CVM의 FTP 서비스를 구축하는 방법을 설명합니다.

소프트웨어

본 문서에 구축한 FTP 서비스 구성 버전은 아래와 같습니다.

Linux 운영 체제: 본 문서는 공용 이미지 CentOS 7.6을 예로 듭니다.

Vsftpd: 본 문서는 vsftpd 3.0.2를 예로 듭니다.

작업 단계

1단계: CVM(Cloud Virtual Machine) 로그인

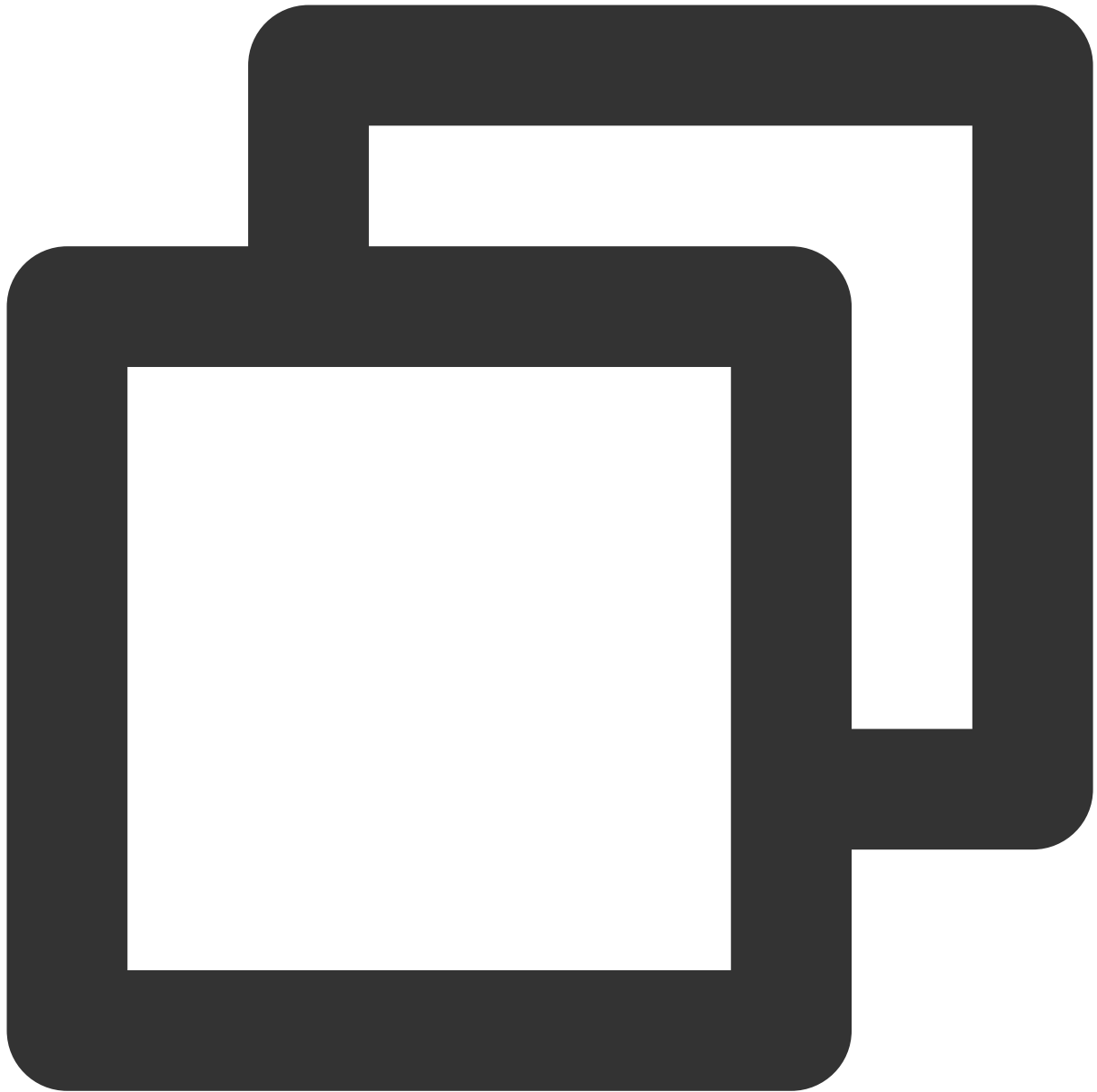
[Linux 인스턴스에 로그인](#)합니다. 실제 작업 스타일에 따라 다른 로그인 방식을 선택할 수도 있습니다.

[원격 로그인 소프트웨어를 사용하여 Linux 인스턴스 로그인](#)

[SSH를 사용하여 Linux 인스턴스에 로그인](#)

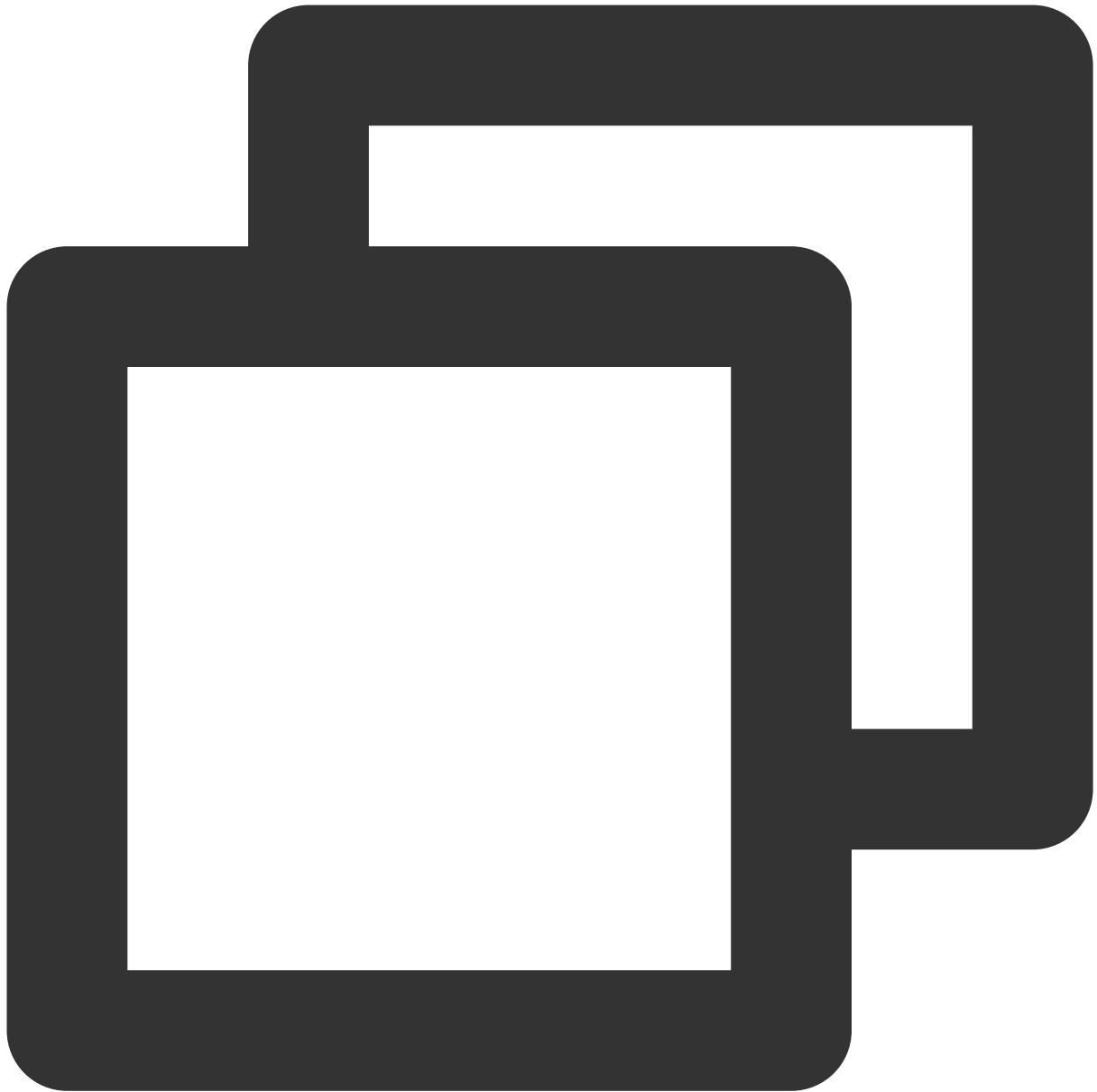
2단계: vsftpd 설치

1. 다음 명령어를 실행하여 vsftpd를 설치합니다.



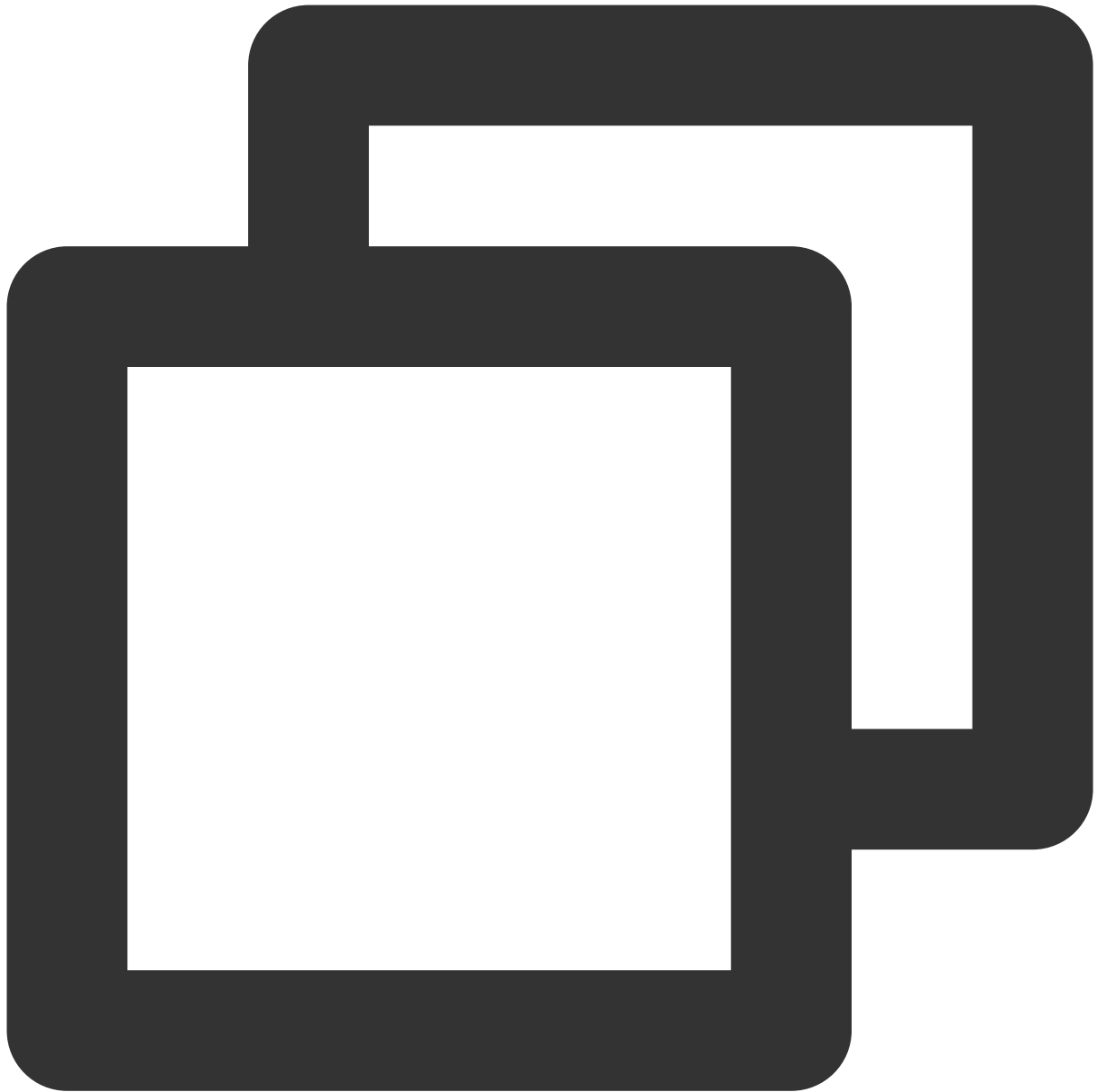
```
yum install -y vsftpd
```

2. 다음 명령어를 실행하여 부팅 시 **vsftpd** 자동 실행으로 설정합니다.



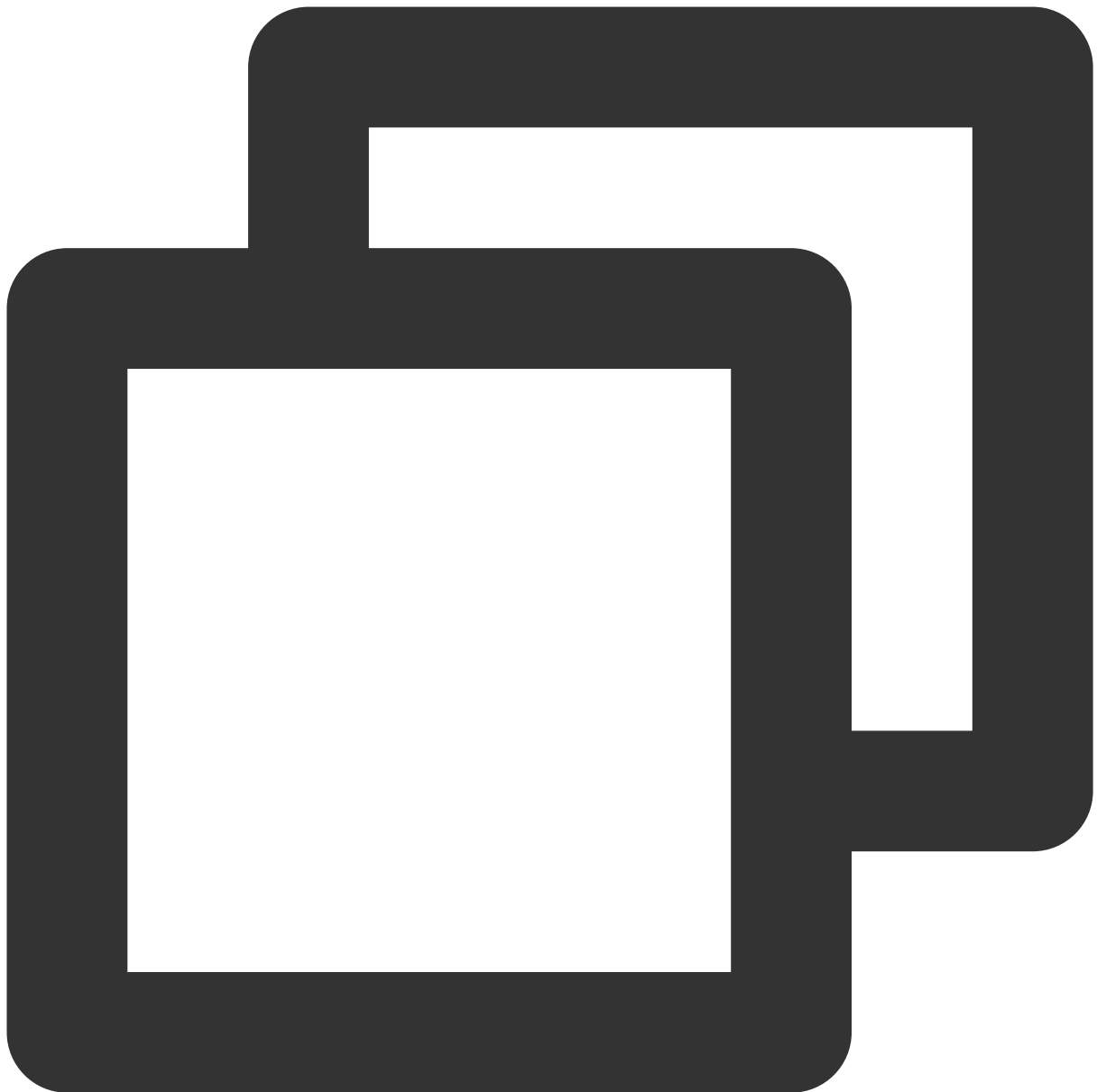
```
systemctl enable vsftpd
```

3. 다음 명령어를 실행하여 FTP 서비스를 실행합니다.



```
systemctl start vsftpd
```

4. 다음 명령어를 실행하여 서비스가 실행되었는지 확인합니다.



```
netstat -antup | grep ftp
```

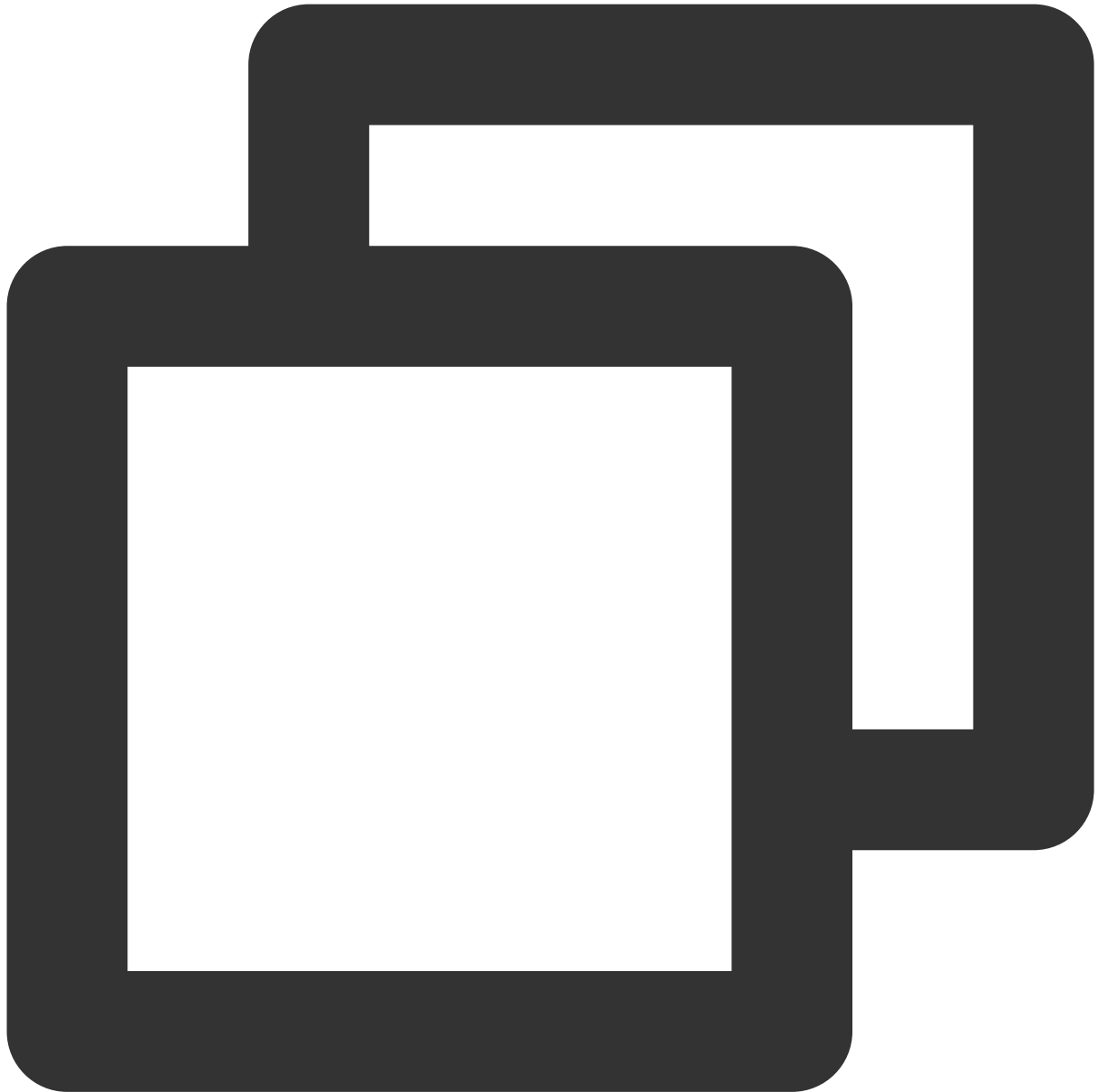
아래와 같은 결과가 표시되면 FTP 서비스가 실행된 것입니다.

```
[root@VM_0_117_centos ~]# systemctl start vsftpd
[root@VM_0_117_centos ~]# netstat -antup | grep ftp
tcp6      0      0 :::21          :::*           LISTEN
```

이때 vsftpd가 익명 액세스 모드를 기본값으로 설정하므로 사용자 이름, 비밀번호 없이도 바로 FTP 서버에 로그인할 수 있습니다. 이 방식으로 FTP 서버에 로그인한 사용자는 수정 및 파일 업로드 권한이 없습니다.

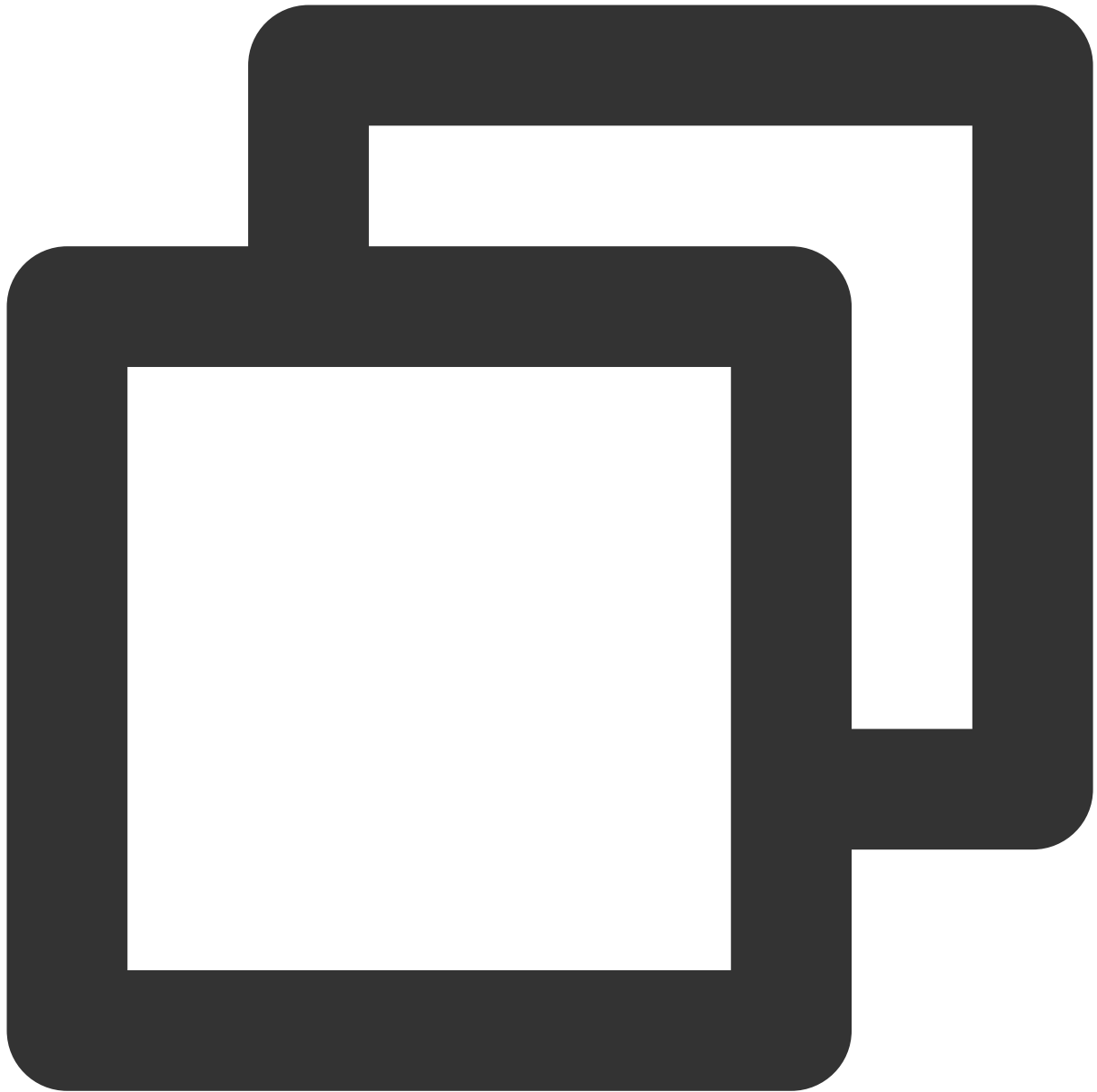
3단계: vsftpd 설정

1. 다음 명령어를 실행하여 FTP 서비스 사용을 위해 사용자 ID를 생성합니다. 본 문서는 ftpuser를 예로 듭니다.



```
useradd ftpuser
```

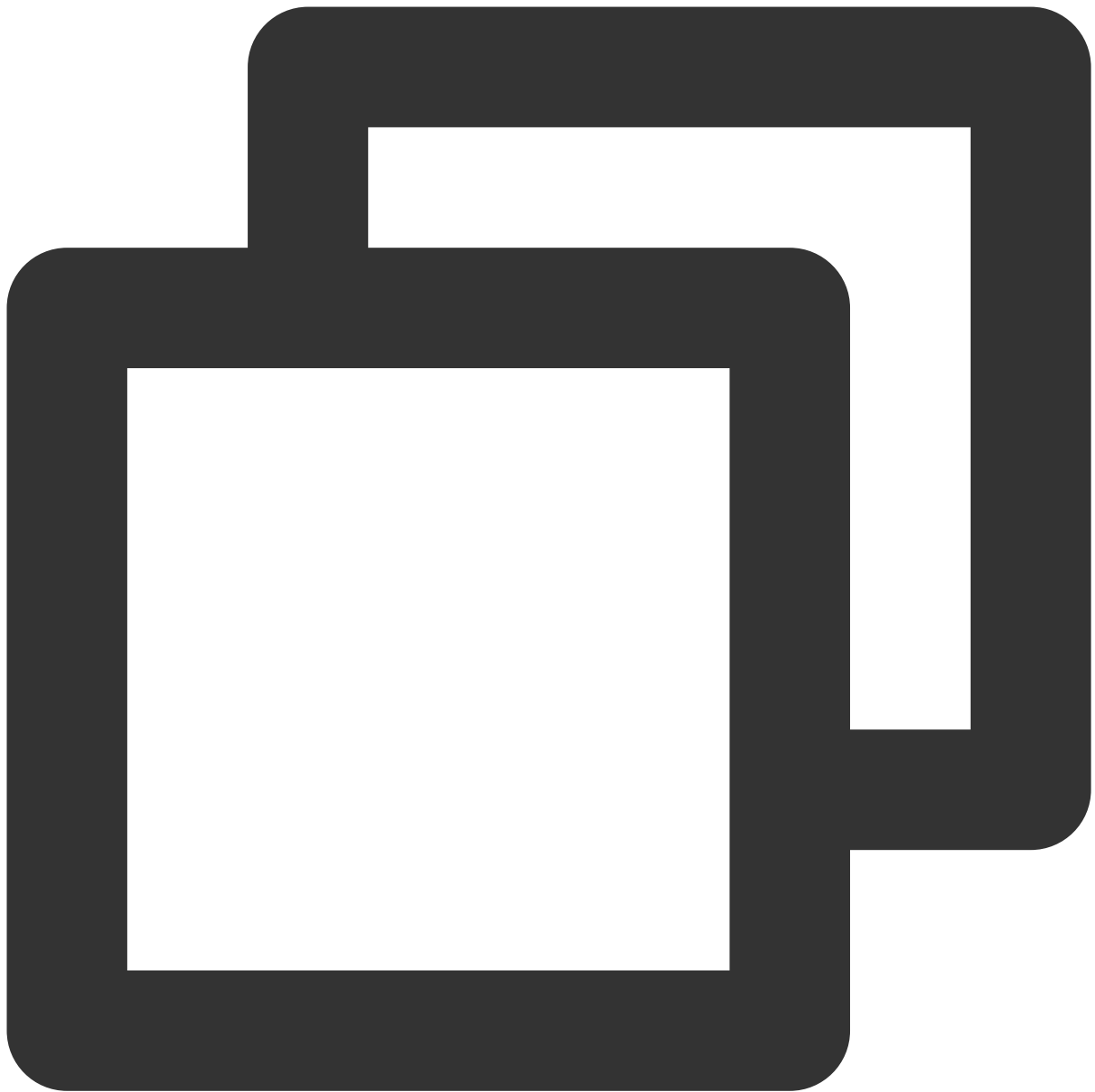
2. 다음 명령어를 실행하여 사용자 ftpuser의 비밀번호를 설정합니다.



```
passwd ftpuser
```

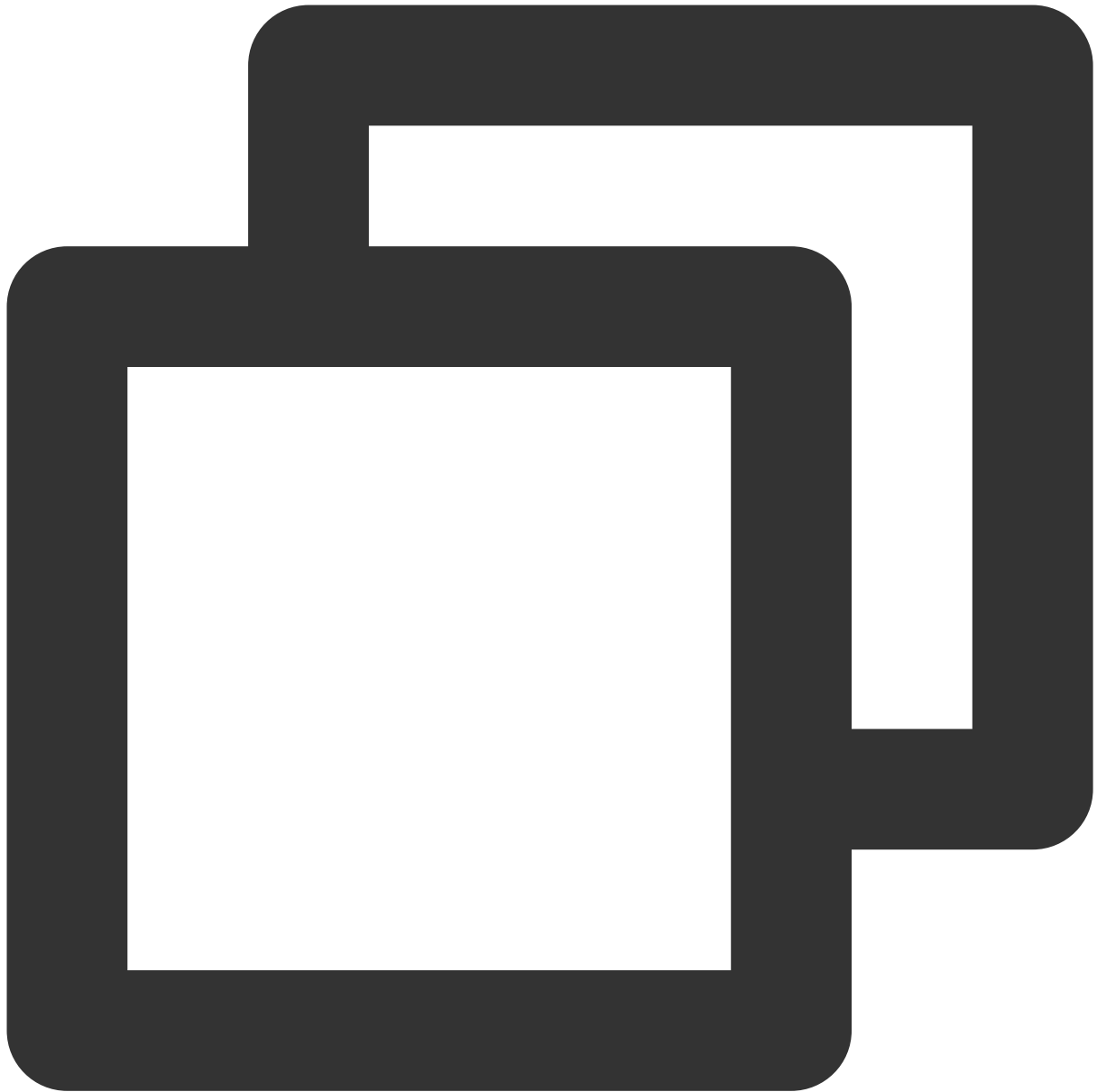
비밀번호를 입력한 후 **Enter**를 눌러 설정을 확인합니다. 비밀번호는 표시 안 함으로 기본 설정되어 있으며, 본 문서는 `tf7295TFY` 를 예로 듭니다.

3. 다음 명령어를 실행하여 FTP 서비스에 사용할 파일 디렉터리를 생성합니다. 본 문서는 `/var/ftp/test` 를 예로 듭니다.



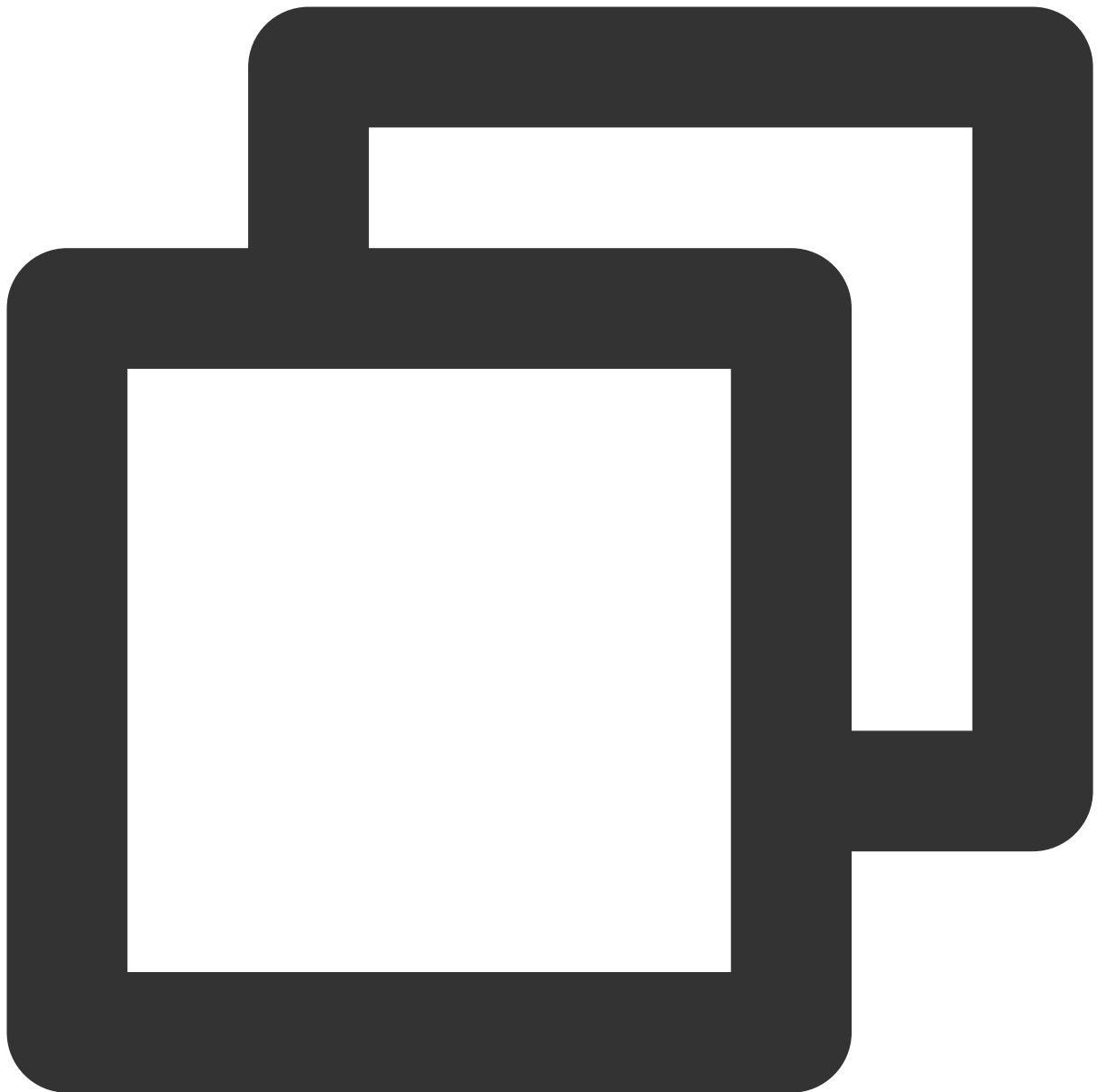
```
mkdir /var/ftp/test
```

4. 다음 명령어를 실행하여 디렉터리 권한을 수정합니다.



```
chown -R ftpuser:ftpuser /var/ftp/test
```

5. 다음 명령어를 실행하여 `vsftpd.conf` 파일을 엽니다.



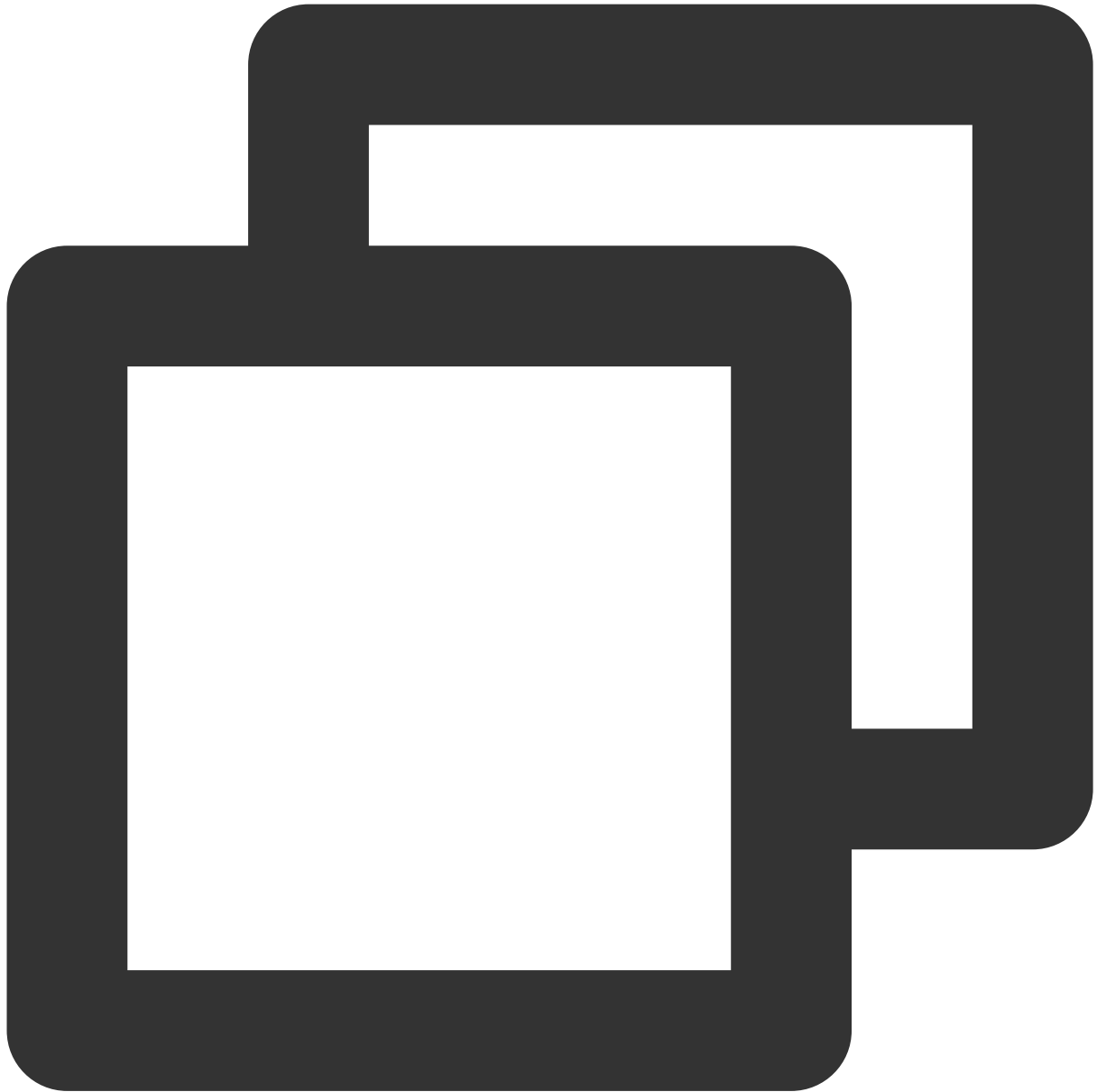
```
vim /etc/vsftpd/vsftpd.conf
```

6. **i**를 눌러 편집 모드로 전환하고 실제 수요에 따라 FTP 모드를 선택한 후 구성 파일 `vsftpd.conf` 을 수정합니다.

주의사항 :

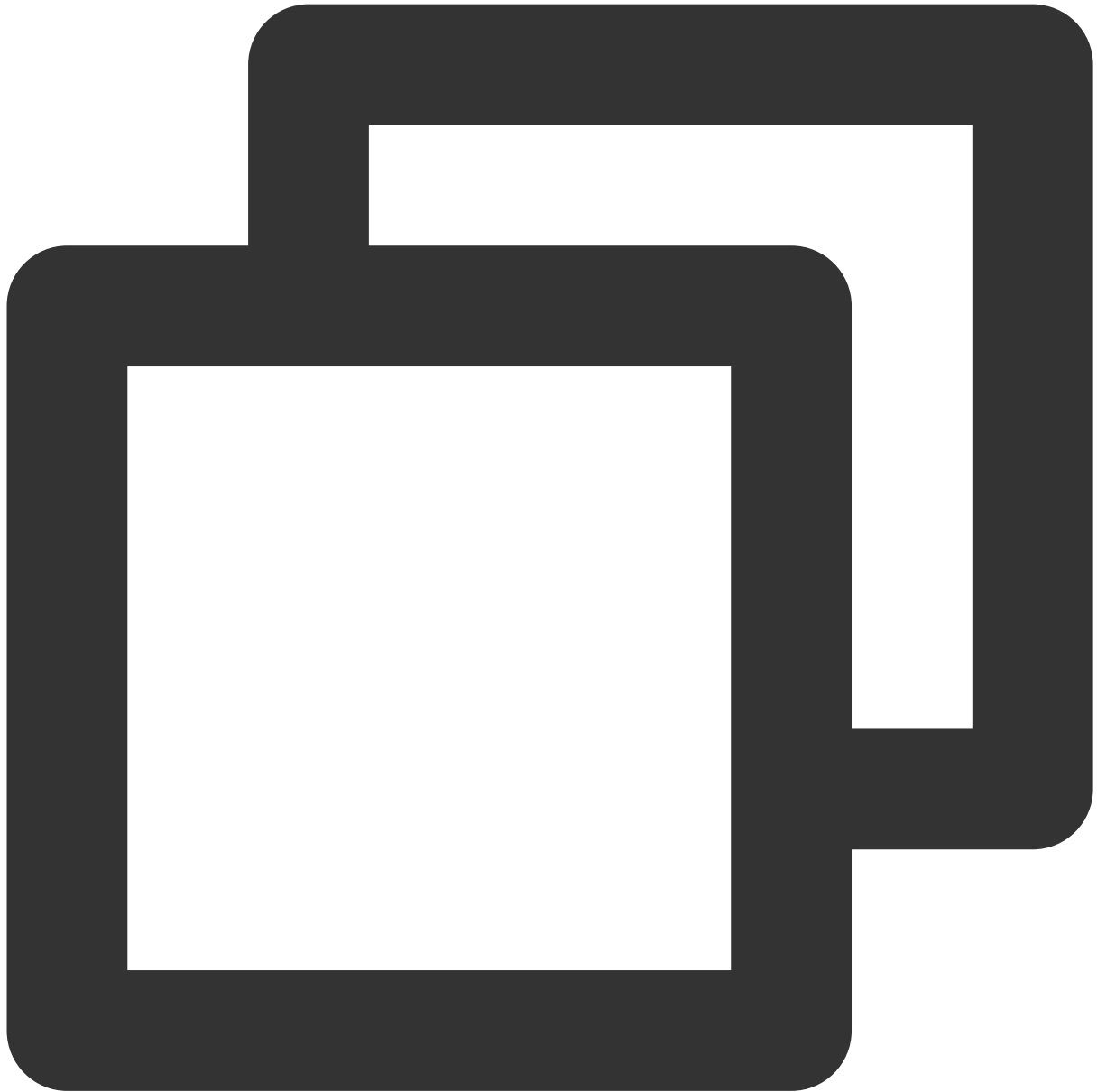
FTP는 능동 모드와 수동 모드를 통해 클라이언트 컴퓨터와 연결하고 데이터를 전송할 수 있습니다. 대다수 클라이언트 컴퓨터의 방화벽 설정과 리얼 IP를 획득할 수 없는 등의 이유로 **수동 모드**를 선택하여 FTP 서비스를 구축할 것을 권장합니다. 아래의 수정 예시는 수동 모드 설정이므로, 능동 모드를 선택해야 한다면 **FTP 능동 모드 설정**으로 이동하십시오.

6.1 다음의 설정 매개변수를 수정하여 익명 사용자와 로컬 사용자의 로그인 권한을 설정하고, 예외 사용자 리스트 파일을 지정하는 경로를 설정한 후 IPv4 sockets 리슨을 시작합니다.



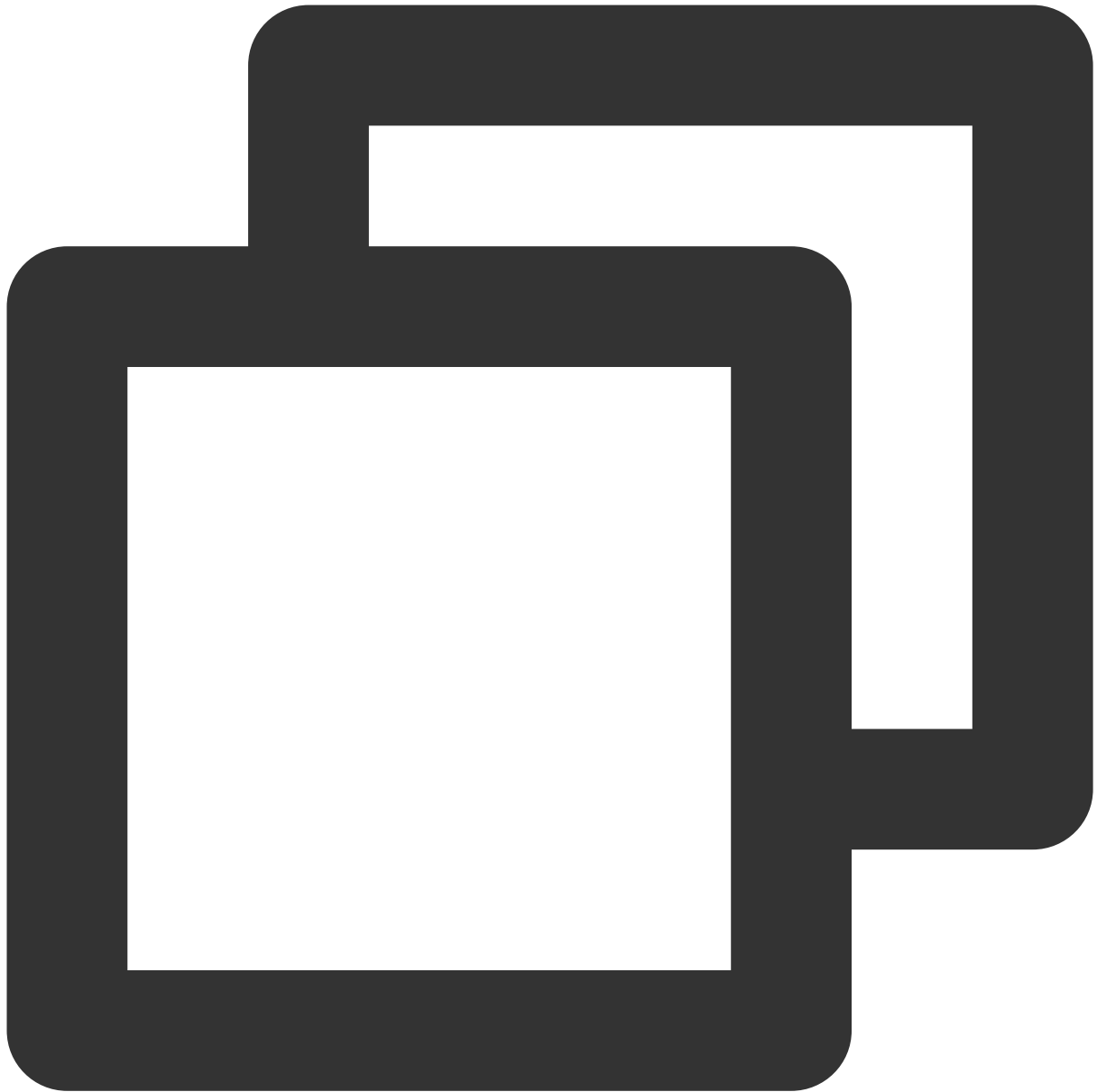
```
anonymous_enable=NO
local_enable=YES
write_enable=YES
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
listen=YES
```

6.2 줄 맨 앞에 # 을 추가하여 `listen_ipv6=YES` 설정 매개변수를 주석 처리하고, IPv6 sockets 리슨을 종료합니다.



```
#listen_ipv6=YES
```

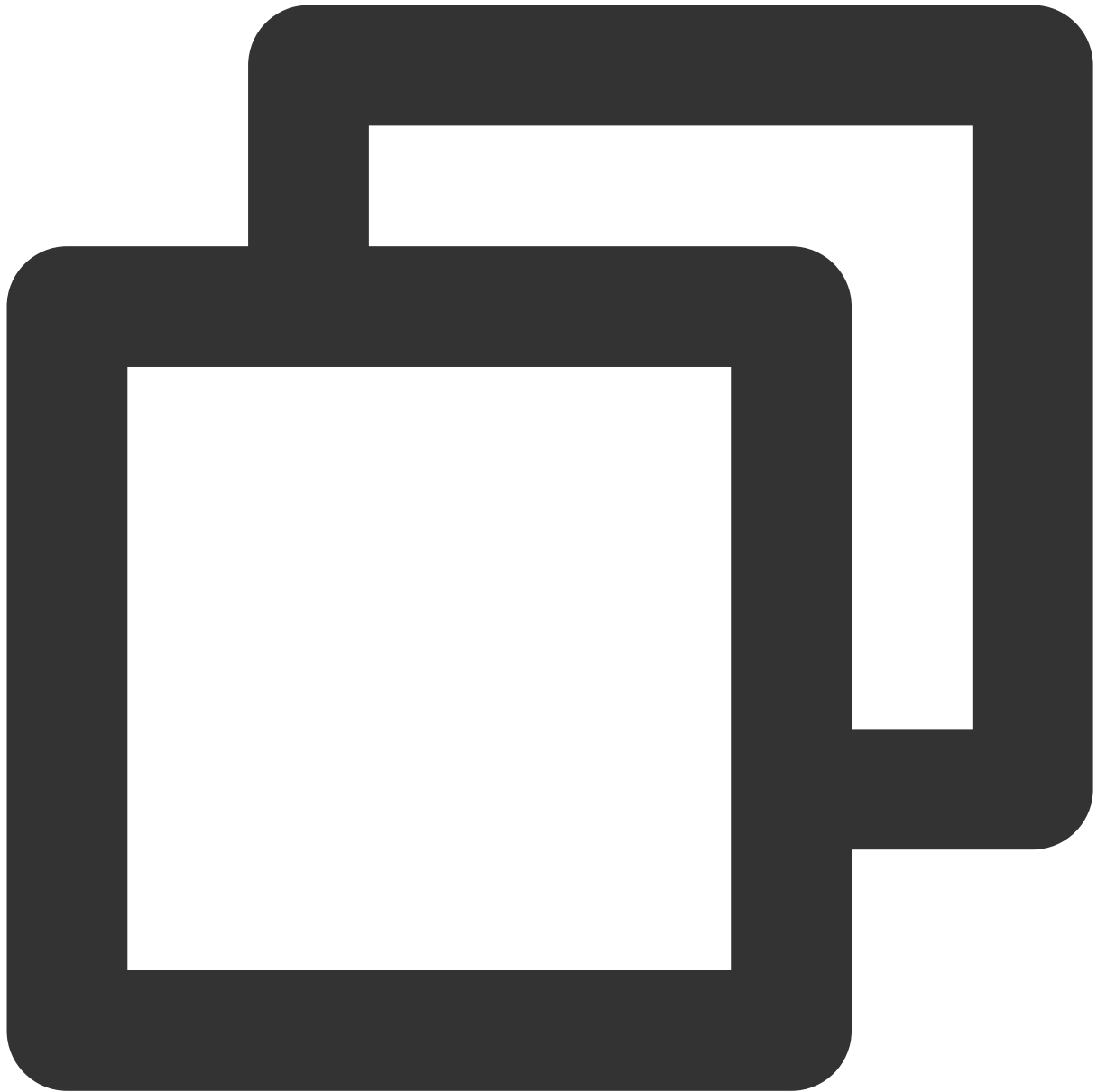
6.3 다음 설정 매개변수를 추가하고 수동 모드를 활성화하여, 로컬 사용자가 로그인한 후 위치한 디렉터리와 CVM이 데이터 전송에 사용할 포트 범위 값을 설정합니다.



```
local_root=/var/ftp/test
allow_writeable_chroot=YES
pasv_enable=YES
pasv_address=xxx.xx.xxx.xx #사용자의 Linux CVM의 공인 IP로 수정
pasv_min_port=40000
pasv_max_port=45000
```

7. **Esc**를 누르고 **:wq**를 입력하여 저장한 후 종료합니다.

8. 다음 명령어를 실행하여 `chroot_list` 파일을 생성 및 편집합니다.

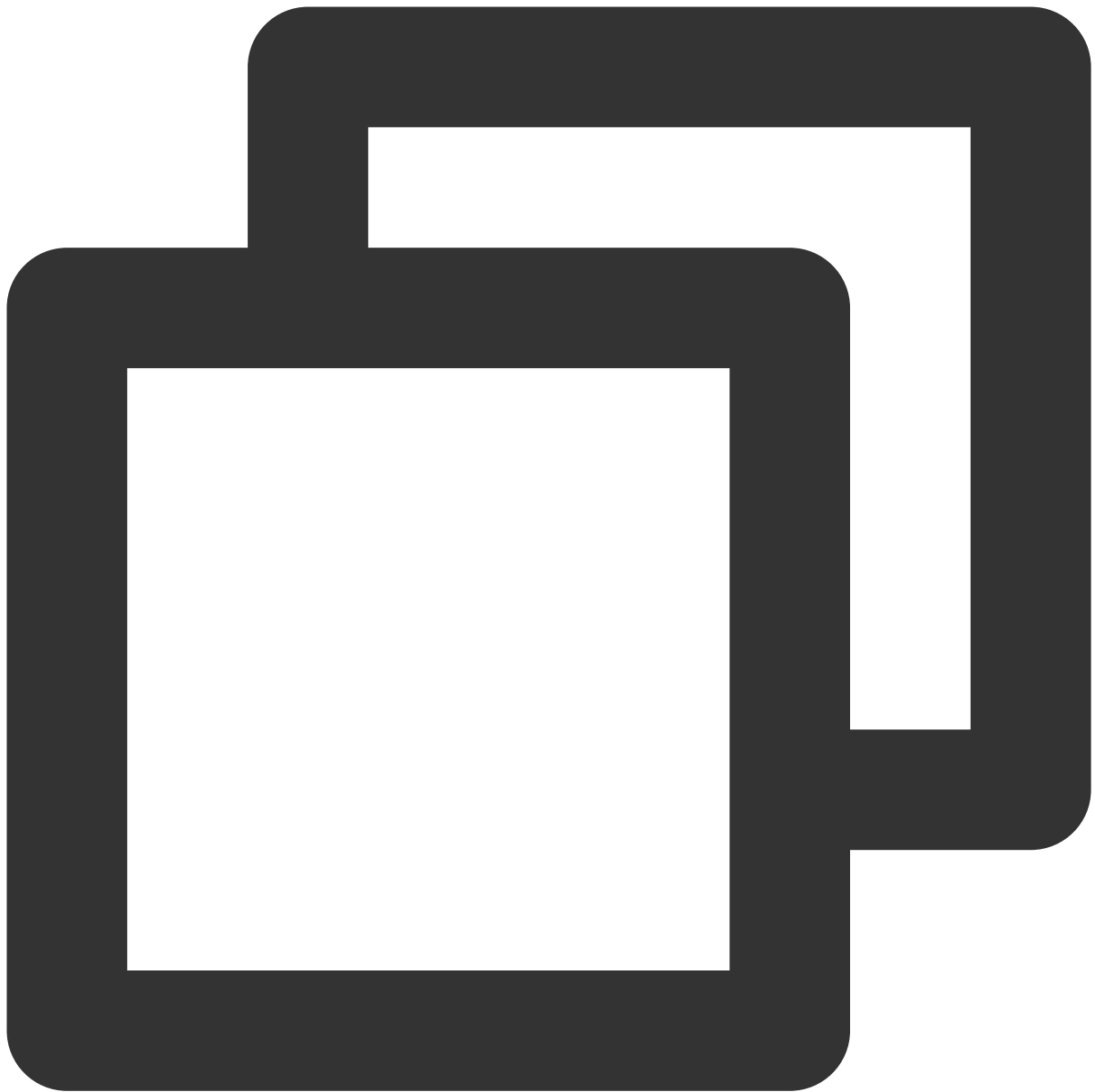


```
vim /etc/vsftpd/chroot_list
```

9. **i**를 눌러 편집 모드로 전환하여 사용자 이름을 한 줄에 하나씩 입력합니다. 설정을 완료하면 **Esc**를 누르고 **:wq**를 입력하여 저장한 후 종료합니다.

설정된 사용자는 홈 디렉터리에 잠겨 있지 않게 됩니다. 예외 사용자를 설정할 필요가 없다면 이 단계를 건너뛸 수 있으며, **:wq**를 입력하여 파일을 종료합니다.

10. 다음 명령어를 실행하여 FTP 서비스를 재시작합니다.



```
systemctl restart vsftpd
```

4단계: 보안 그룹 설정

FTP 서비스를 구축한 후 실제 사용하는 FTP 모드에 따라 Linux CVM에 **인바운드 규칙**을 열어줘야 합니다. 자세한 사항은 [보안 그룹 규칙 추가](#)를 참고하십시오.

대다수의 클라이언트 컴퓨터는 LAN에서 IP 주소 전환을 거칩니다. 따라서 FTP 능동 모드를 선택했다면 클라이언트 컴퓨터가 획득한 리얼 IP 주소를 확인하십시오. 그렇지 않으면 클라이언트가 FTP 서버에 로그인할 수 없게 됩니다.
능동 모드: 포트 21 개방.

수동 모드: 포트 21 개방 및 구성 파일 수정에서 설정한 `pasv_min_port` 와 `pasv_max_port` 사이의 모든 포트를 개방합니다. 본 문서는 40000 ~ 45000 범위의 포트를 개방합니다.

5단계: FTP 서비스 인증

FTP 클라이언트 소프트웨어, 브라우저 또는 파일 리소스 관리자 등의 툴을 통해 FTP 서비스를 인증할 수 있습니다.

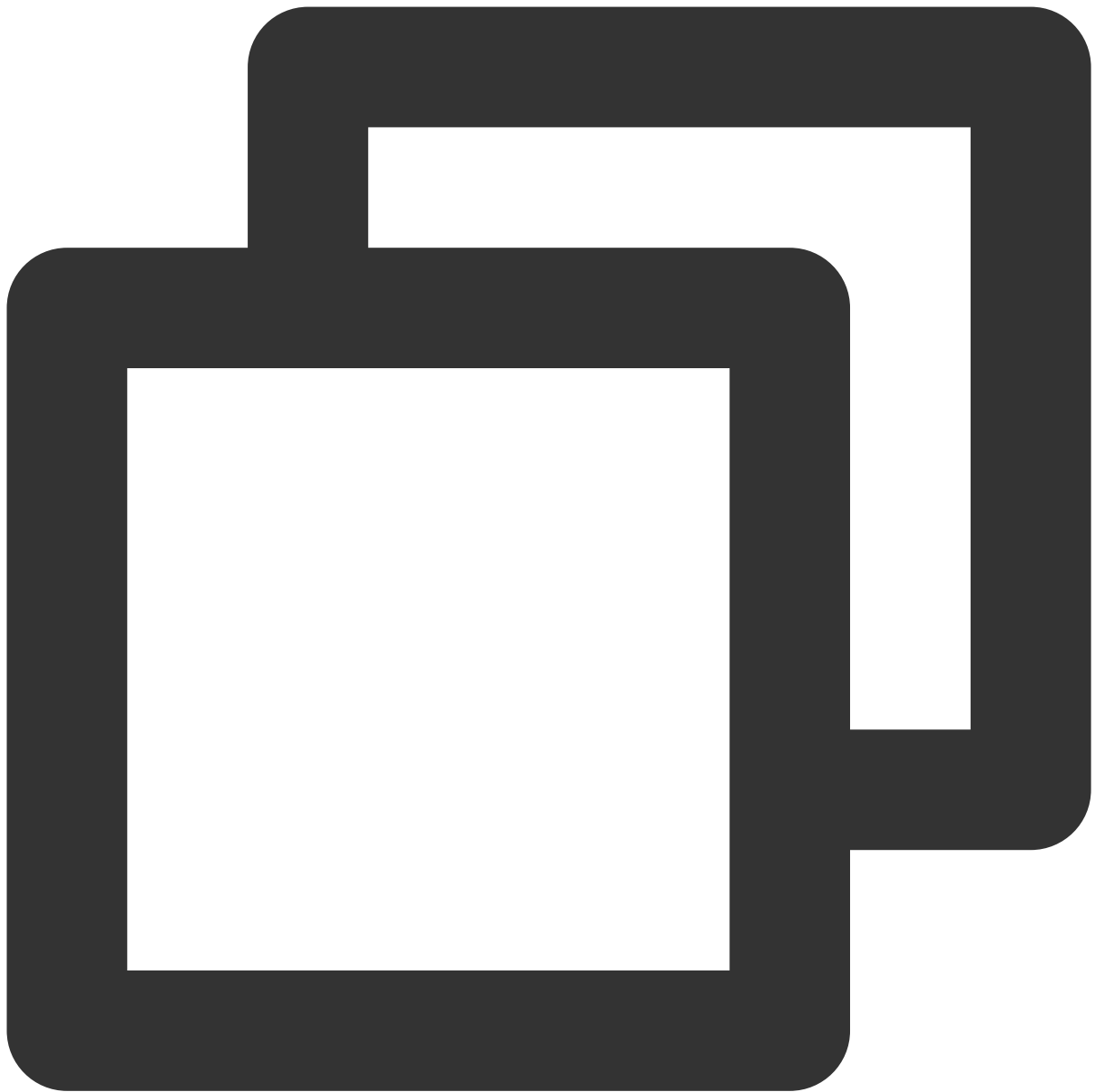
본 문서는 클라이언트의 파일 리소스 관리자를 예로 듭니다.

1. 클라이언트의 IE 브라우저를 열어 **툴 > Internet 옵션 > 고급**을 클릭하고, 선택한 FTP 모드에 따라 수정합니다.

능동 모드: '수동 FTP 사용' 선택 취소.

수동 모드: '수동 FTP 사용' 선택.

2. 클라이언트의 컴퓨터를 열어 경로 입력란에 아래 주소를 입력하여 액세스합니다.



ftp://CVM 공인 IP:21

3. '로그인 정보' 팝업 창에 [vsftpd 구성](#)에서 설정한 사용자 이름과 비밀번호를 입력합니다.

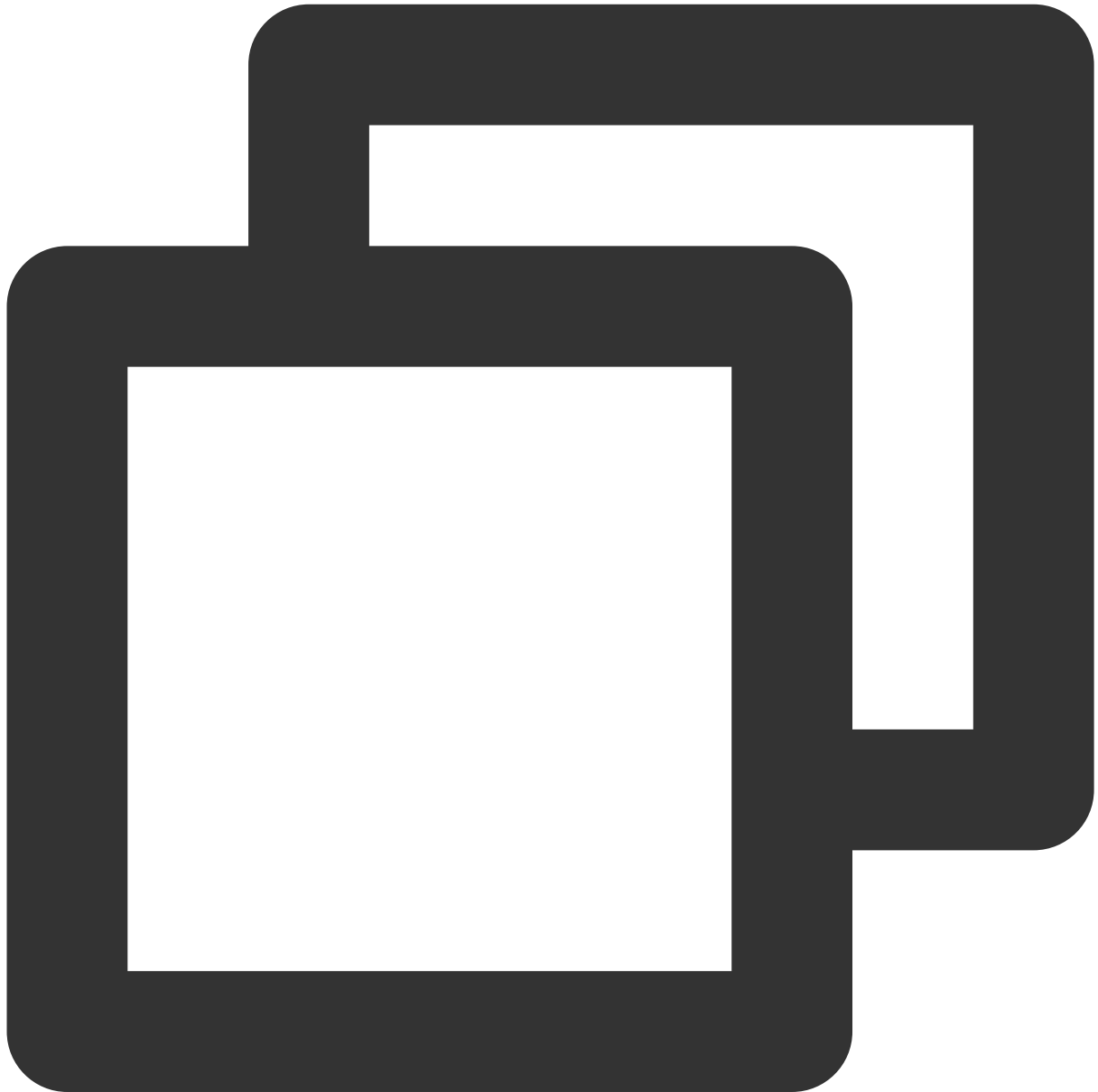
본 문서에서 사용한 사용자 이름은 `ftpuser` 이고, 비밀번호는 `tf7295TFY` 입니다.

4. 로그인에 성공한 후 파일을 업로드하거나 다운로드할 수 있습니다.

부록

FTP 능동 모드 설정

능동 모드에서 수정해야 하는 설정은 다음과 같으며, 나머지 구성은 기본 설정을 유지합니다.



```
anonymous_enable=NO      #익명 사용자의 로그인 차단
local_enable=YES          #로컬 사용자 로그인 허용
chroot_local_user=YES     #전체 사용자를 홈 디렉터리로 제한
chroot_list_enable=YES    #예외 사용자 리스트 활성화
chroot_list_file=/etc/vsftpd/chroot_list  #사용자 리스트 파일 지정, 해당 리스트에 포함된
```

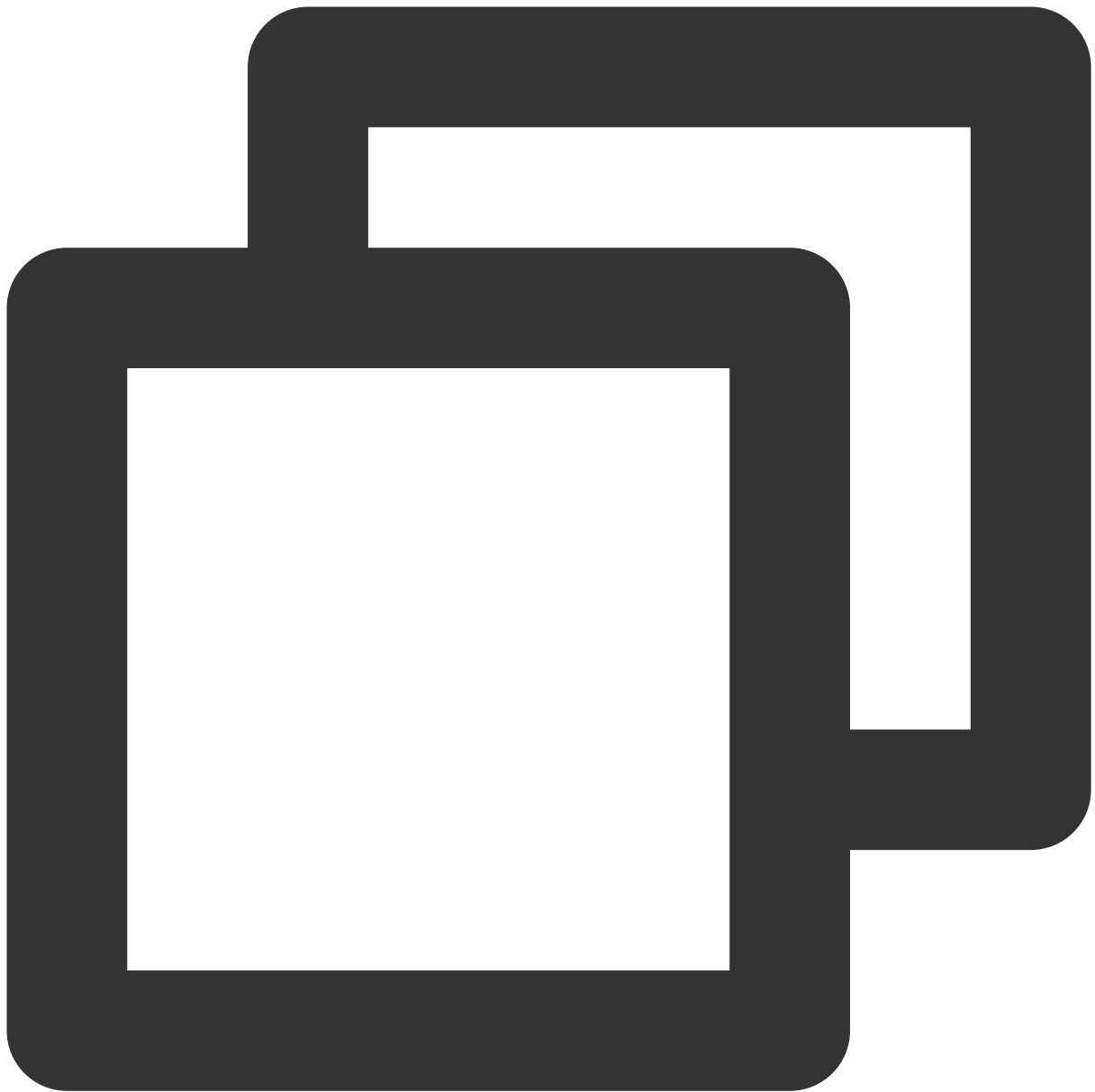
```
listen=YES                #IPv4 sockets 리스  
#줄 맨 앞에 #을 추가하여 다음 매개변수 주석 처리  
#listen_ipv6=YES          #IPv6 sockets 리스 닫기  
#다음 매개변수 추가  
allow_writeable_chroot=YES  
local_root=/var/ftp/test  #로컬 사용자가 로그인 후 위치한 디렉터리 설정
```

Esc를 누르고 **:wq**를 입력하여 저장한 후 종료하고, **8단계**로 이동하여 **vsftpd** 설정을 완료합니다.

FTP 클라이언트의 파일 업로드 실패

문제 설명

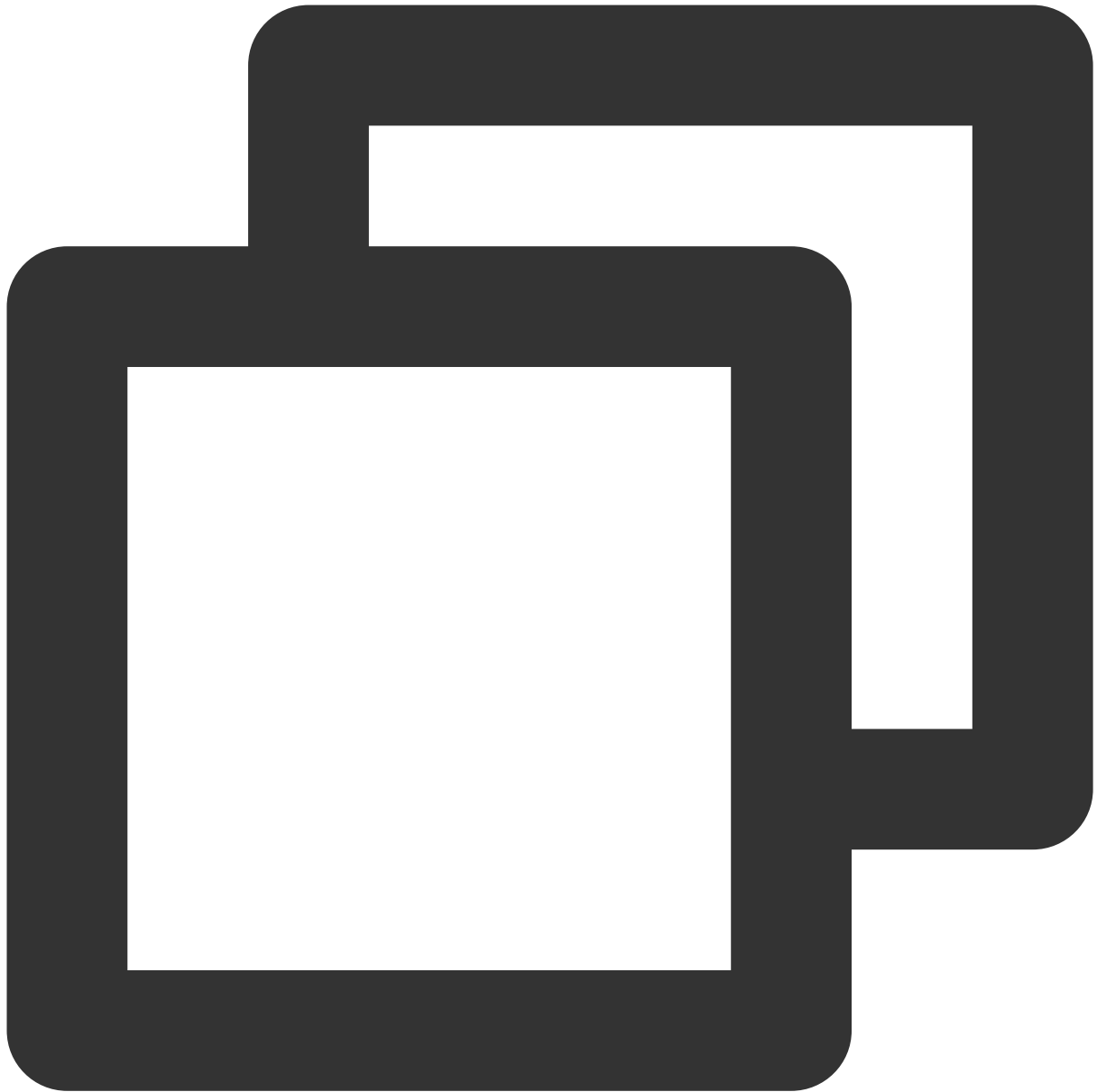
Linux 시스템 환경에서 **vsftp**를 통해 파일을 업로드할 경우 아래와 같은 오류 정보를 표시합니다.



```
553 Could not create file
```

솔루션

1. 다음 명령어를 실행하여 서버 디스크 용량을 점검합니다.

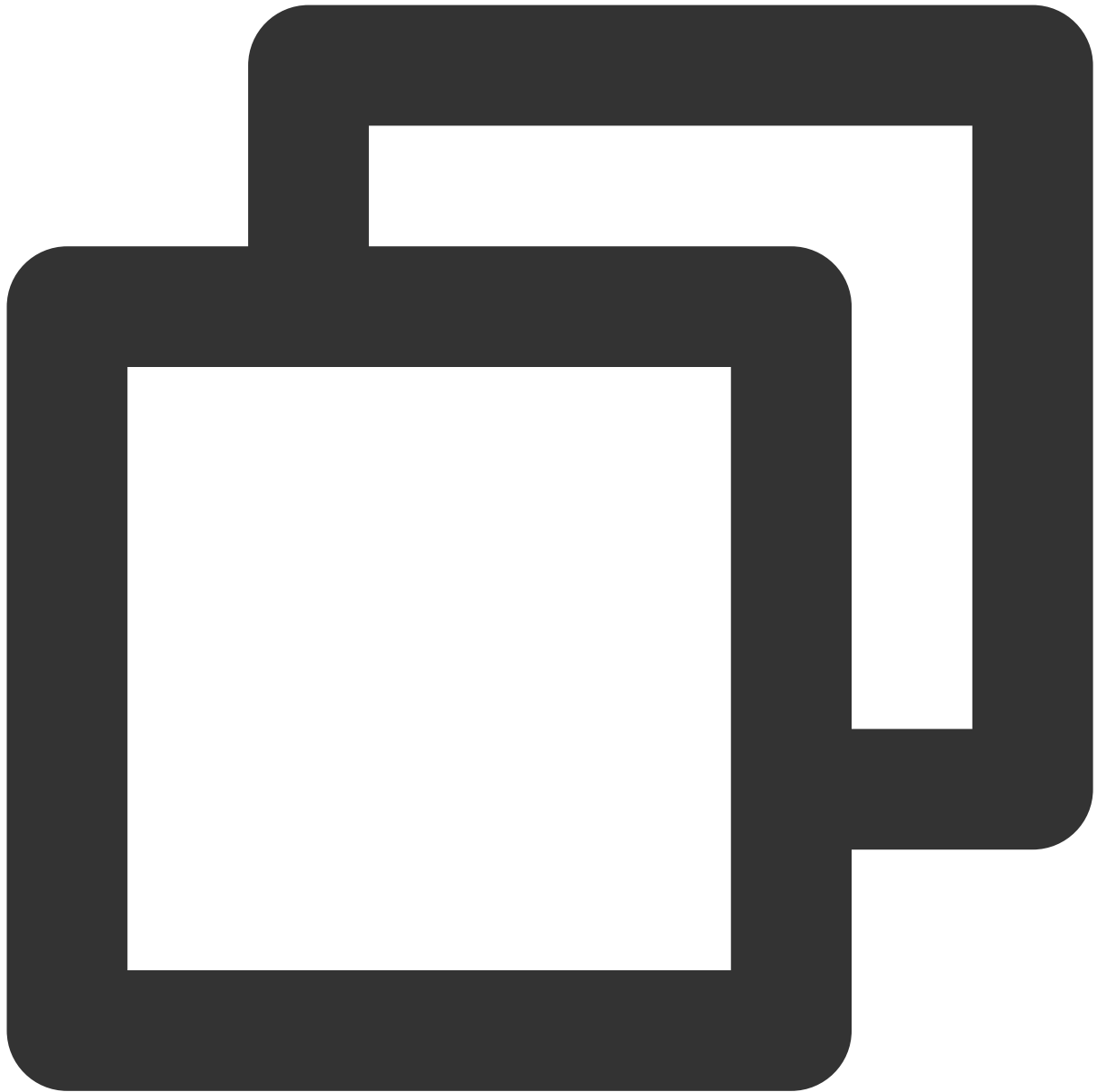


```
df -h
```

디스크 용량이 부족할 경우 파일을 업로드할 수 없게 됩니다. 디스크 용량이 큰 파일을 삭제하십시오.

디스크 용량이 정상일 경우 다음 단계를 진행하십시오.

2. 다음 명령어를 실행하여 FTP 디렉터리에 쓰기 권한이 있는지 확인합니다.



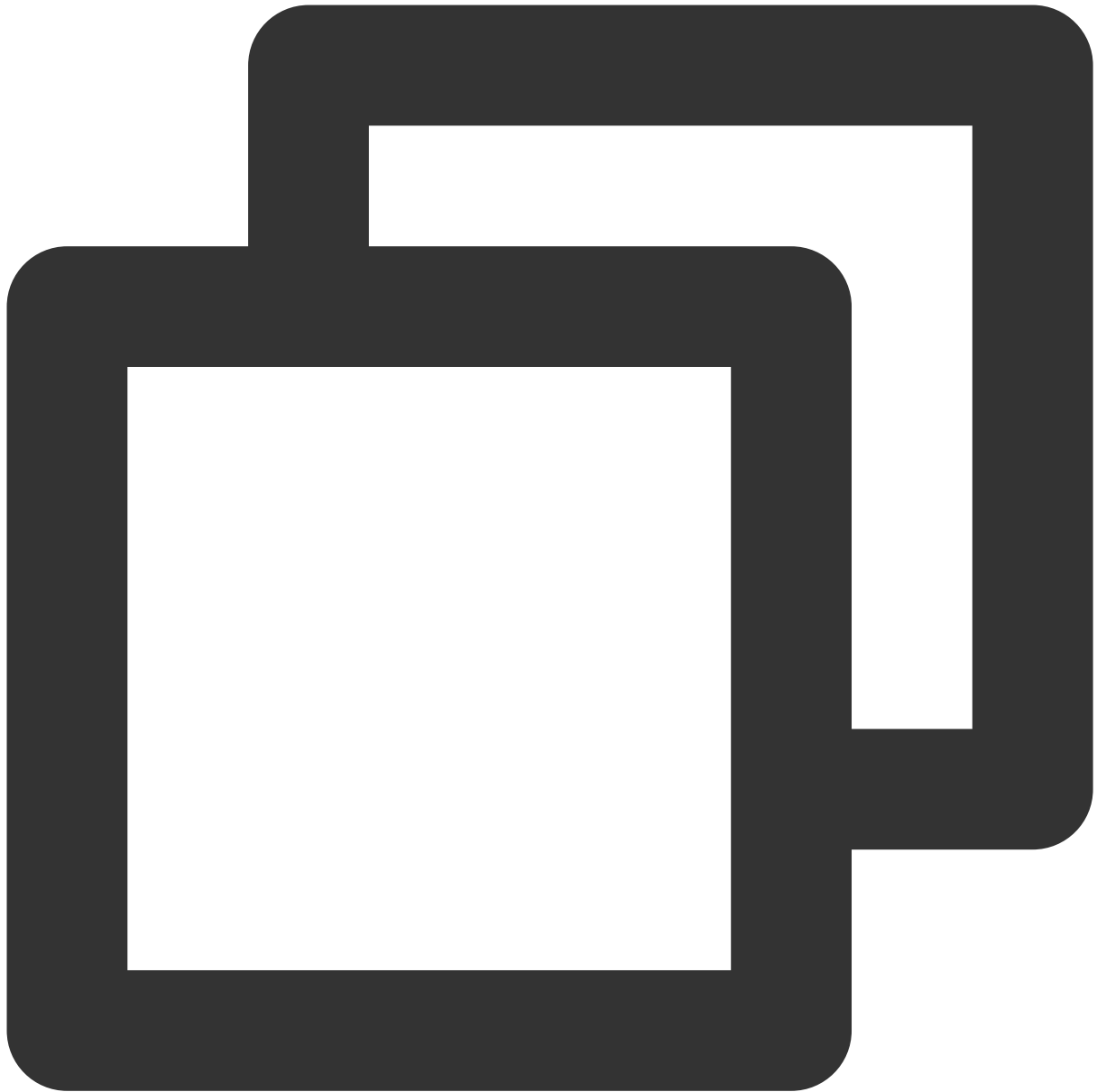
```
ls -l /home/test
```

/home/test가 FTP 디렉터리입니다. 실제 FTP 디렉터리로 수정하십시오.

반환 결과에 'w'가 없으면 사용자에게 쓰기 권한이 없음을 의미합니다. 다음 단계를 진행하십시오.

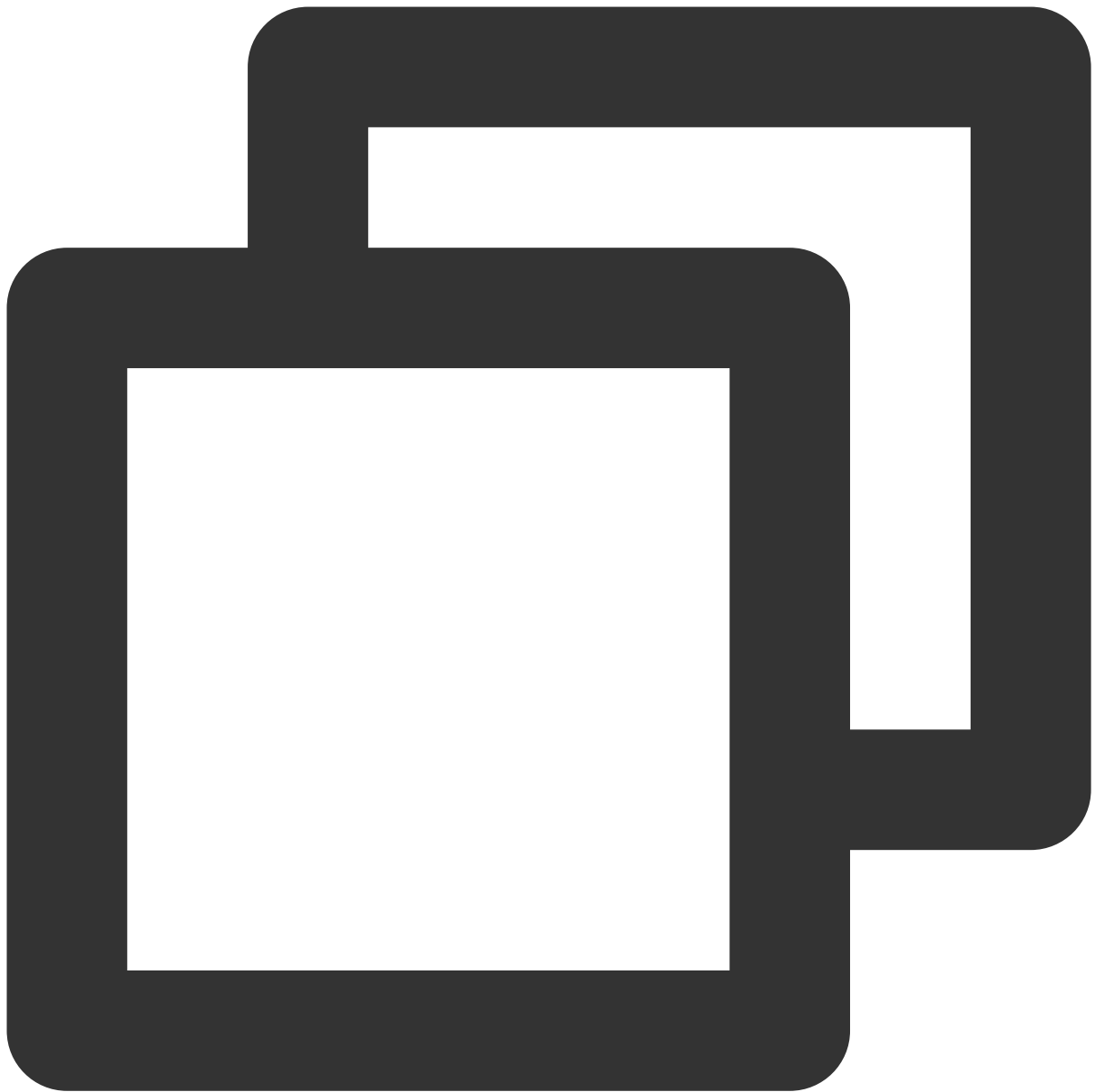
반환 결과에 'w'가 있으면 [티켓 제출](#)을 통해 문의해주시기 바랍니다.

3. 다음 명령어를 실행하여 FTP 디렉터리에 쓰기 권한을 추가합니다.



```
chmod +w /home/test  
# /home/test가 FTP 디렉터리입니다. 실제 FTP 디렉터리로 수정하십시오.
```

4. 다음 명령어를 실행하여 쓰기 권한 설정에 성공했는지 다시 확인합니다.



```
ls -l /home/test
```

```
# /home/test가 FTP 디렉터리입니다. 실제 FTP 디렉터리로 수정하십시오.
```

Windows CVM에서 FTP 서비스 구축

최종 업데이트 날짜: : 2024-02-02 10:56:29

작업 시나리오

본 문서는 Windows 운영 체제의 Tencent Cloud CVM에서 IIS를 통해 FTP 사이트를 구축하는 방법을 소개합니다.

소프트웨어 버전 예시

본 문서에 나오는 FTP 서비스 구성 버전은 다음과 같습니다.

Windows 운영 체제의 경우, 본 문서는 Windows Server 2012를 예시로 사용합니다.

IIS: Web 서버입니다. 본 문서는 IIS 8.5를 예시로 사용합니다.

작업 순서

1단계: CVM 로그인

[RDP 파일을 사용하여 Windows 인스턴스에 로그인\(권장\)](#)합니다.

실제 작업 스타일에 따라 [원격 데스크톱을 사용하여 Windows 인스턴스 로그인](#)할 수 있습니다.

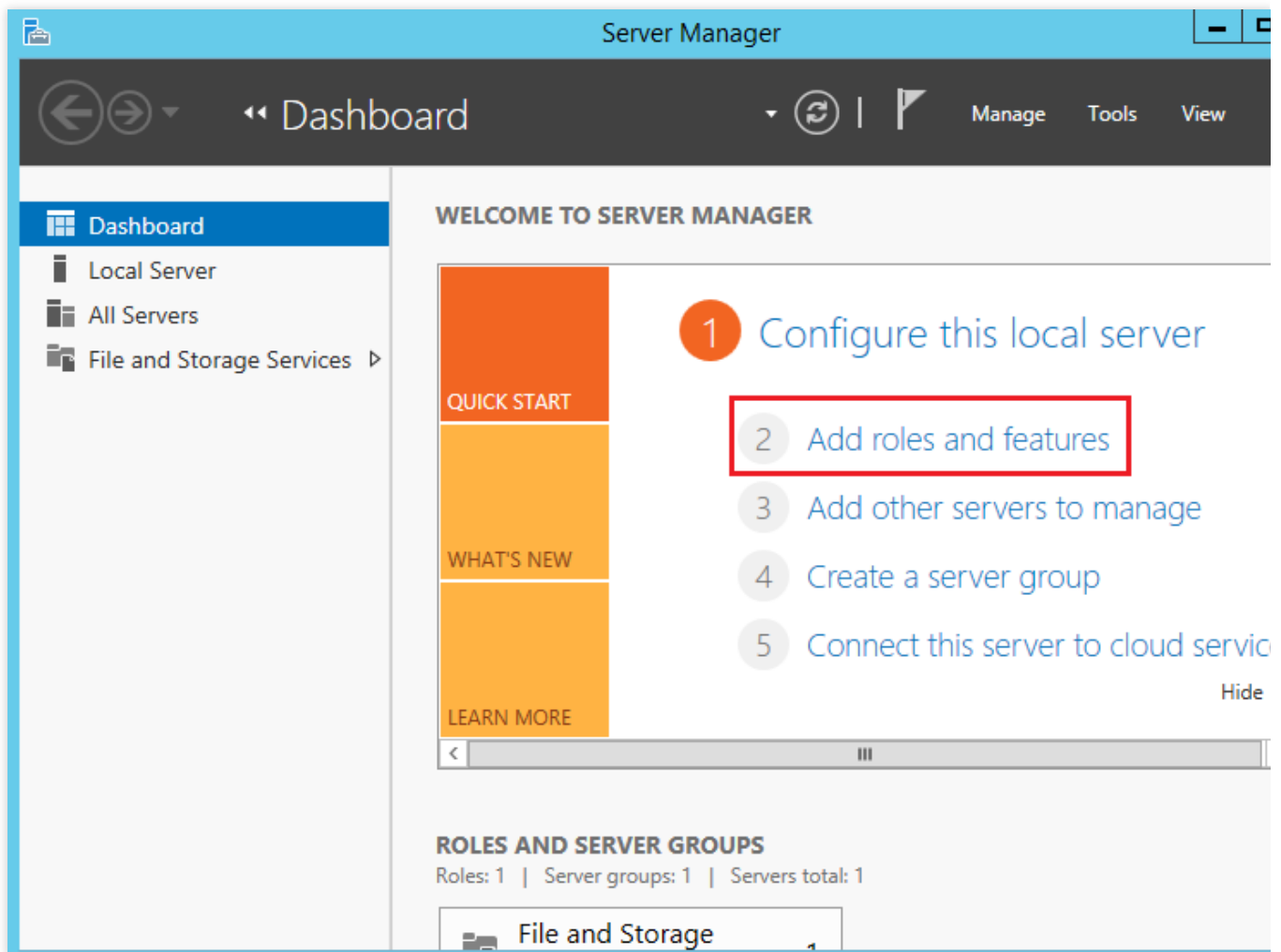
2단계: IIS에서 FTP 서비스 설치

1. 운영 체제 인터페이스에서

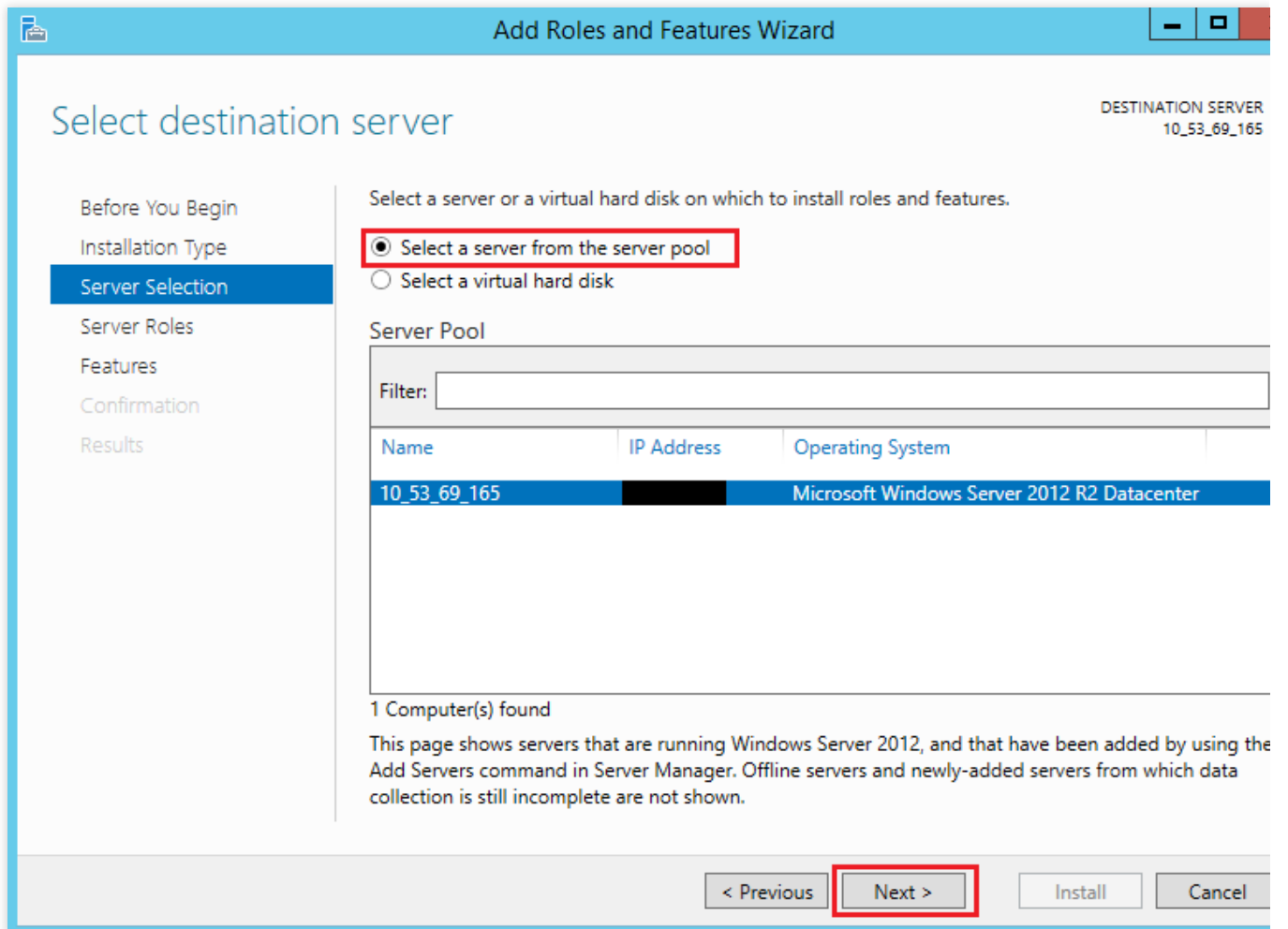


를 클릭하여 서버 관리자를 엽니다.

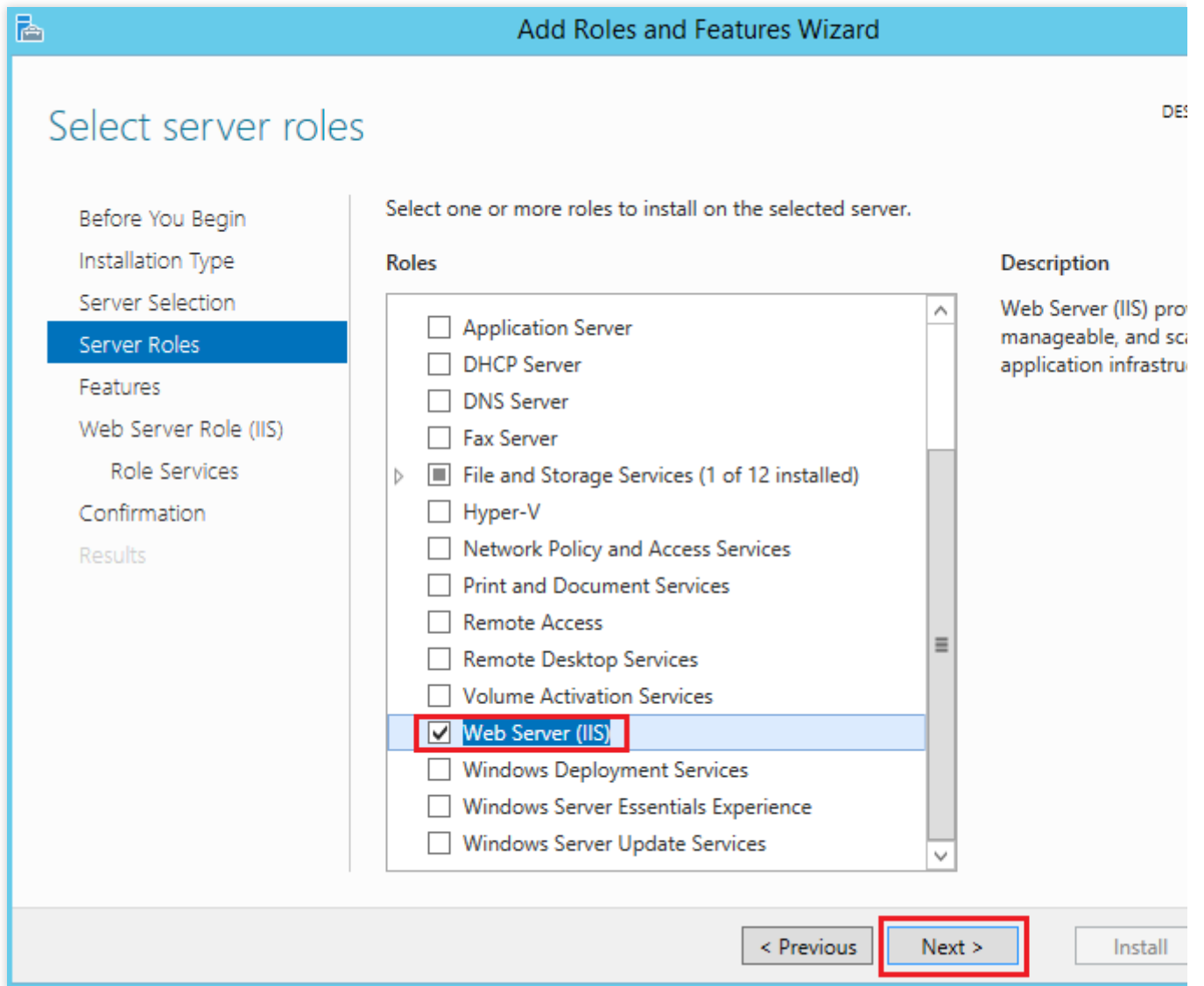
2. 다음 이미지와 같이 '서버 관리자' 창에서 [역할 및 기능 추가]를 클릭합니다.



3. '역할 및 기능 추가 마법사' 팝업 창에서 [다음 단계]를 클릭하여 '설치 유형 선택' 인터페이스로 이동합니다.
4. '설치 유형 선택' 인터페이스에서 [역할 또는 기능에 기반한 설치]를 선택하고 [다음 단계]를 클릭합니다.
5. 다음 이미지와 같이 '타깃 서버 선택' 인터페이스에서 기본 설정을 유지하고 [다음 단계]를 클릭합니다.

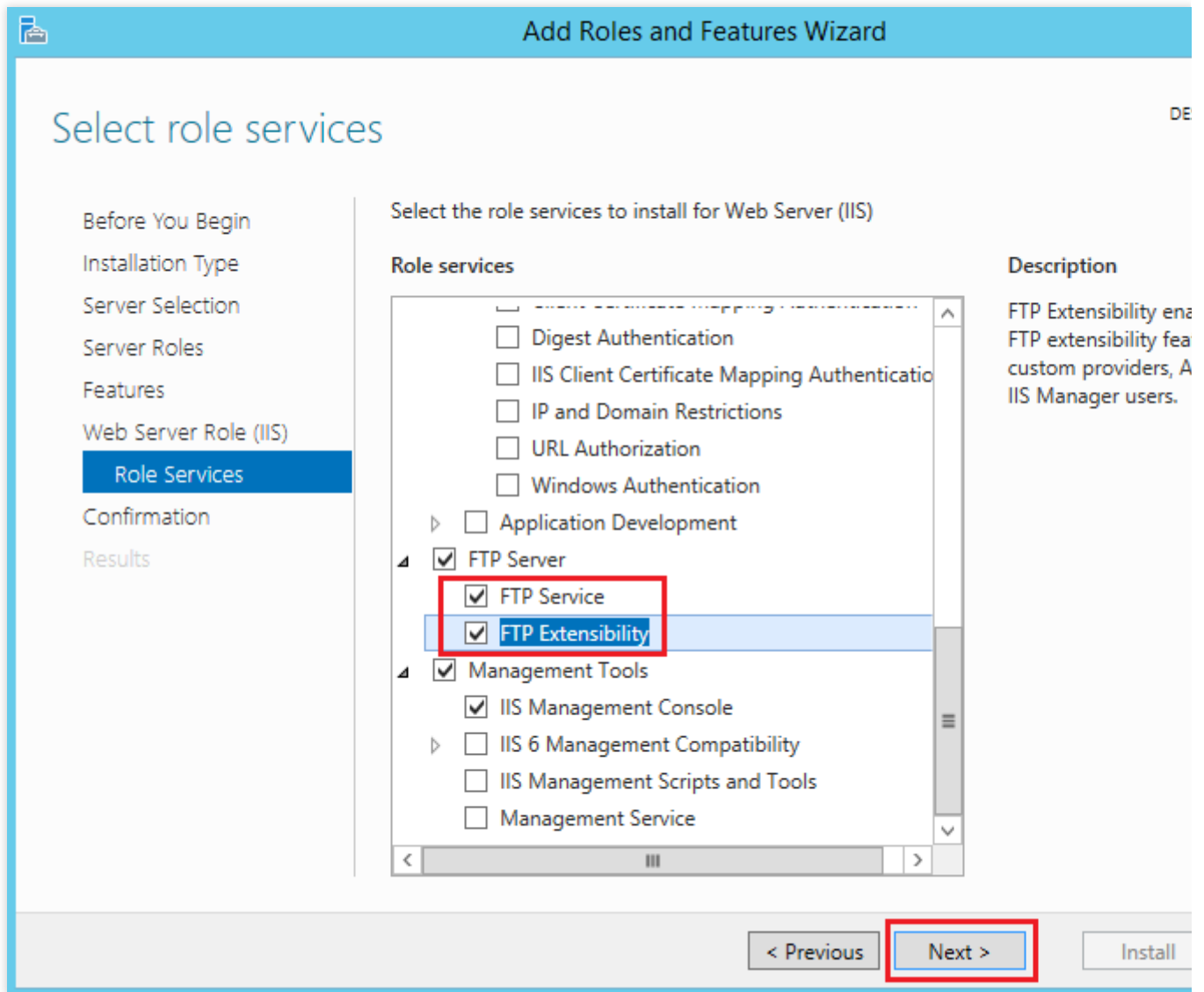


6. 다음 이미지와 같이 '서버 역할 선택' 인터페이스에서 [Web 서버(IIS)]를 선택하고 팝업 창에서 [기능 추가]를 클릭합니다.



7. [다음 단계]를 3번 연속 클릭한 후, '역할 서비스 선택' 인터페이스로 이동합니다.

8. 다음 이미지와 같이 '역할 서비스 선택' 인터페이스에서 [FTP 서비스] 및 [FTP 확장]을 선택하고 [다음 단계]를 클릭합니다.



9. [설치]를 클릭하여 FTP 서비스 설치를 시작합니다.

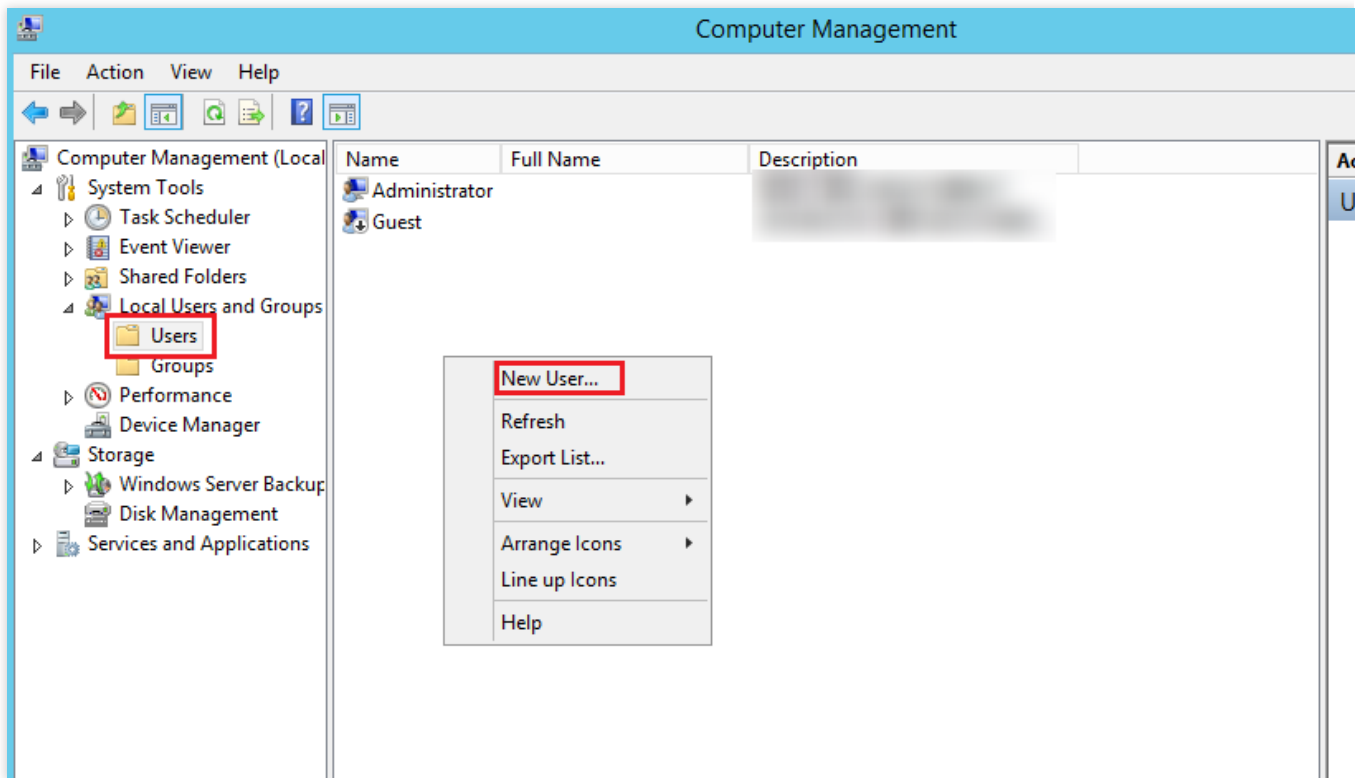
10. 설치 완료 후 [종료]를 클릭합니다.

3단계: FTP 사용자 이름 및 비밀번호 생성

설명 :

다음 순서에 따라 FTP 사용자 이름 및 비밀번호를 설정하십시오. 익명 사용자로 FTP 서비스에 액세스하려면 이 단계를 건너뛰세요.

1. '서버 관리자' 창에서 오른쪽 상단 메뉴의 [툴]>[컴퓨터 관리]를 선택하여 컴퓨터 관리 창을 엽니다.
2. '컴퓨터 관리' 인터페이스에서 왼쪽 메뉴의 [시스템 툴]>[로컬 사용자 및 그룹]>[사용자]를 선택합니다.
3. 다음 이미지와 같이 [사용자]의 오른쪽 인터페이스 빈 공간에서 우클릭하여 [신규 사용자]를 선택합니다.



4. '신규 사용자' 인터페이스에서 다음 알림에 따라 사용자 이름 및 비밀번호를 설정하고 [생성]을 클릭합니다.

The 'New User' dialog box contains the following fields and options:

- User name: ftpuser
- Full name: (empty)
- Description: (empty)
- Password: (masked with dots)
- Confirm password: (masked with dots)
- ☐ User must change password at next logon
- ☐ User cannot change password
- ☒ Password never expires
- ☐ Account is disabled
- Buttons: Help, Create, Close

주요 매개변수는 다음과 같습니다.

사용자 이름: 사용자 정의합니다. 본 문서는 ftpuser 를 예시로 사용합니다.

비밀번호 및 비밀번호 확인: 사용자 정의합니다. 비밀번호는 대문자, 소문자 및 숫자를 포함해야 합니다. 본 문서는 `tf7295TFY` 를 예시로 사용합니다.

[다음 로그인 시 비밀번호 변경 필요] 선택을 해제하고 [비밀번호 무기한 유효]를 선택합니다.

실제 수요에 맞게 선택하십시오. 본 문서는 비밀번호 무기한 유효를 예시로 사용합니다.

5. [닫기]를 클릭하여 '신규 사용자' 창을 닫으면 생성된 `ftpuser` 사용자를 리스트에서 즉시 조회할 수 있습니다.

4단계: 공유 폴더 권한 설정

설명 :

본 문서는 `C:\\test` 폴더를 예시로 사용하여 FTP 사이트의 공유 폴더를 설정하였으며 폴더는 공유해야 할 `test.txt` 파일을 포함하고 있습니다. 본 예시를 참조하여 하나의 `C:\\test` 폴더 및 `test.txt` 파일을 생성할 수 있습니다. 실제 수요에 따라 다른 폴더를 FTP 사이트의 공유 폴더로 설정할 수도 있습니다.

1. 운영 체제 인터페이스에서



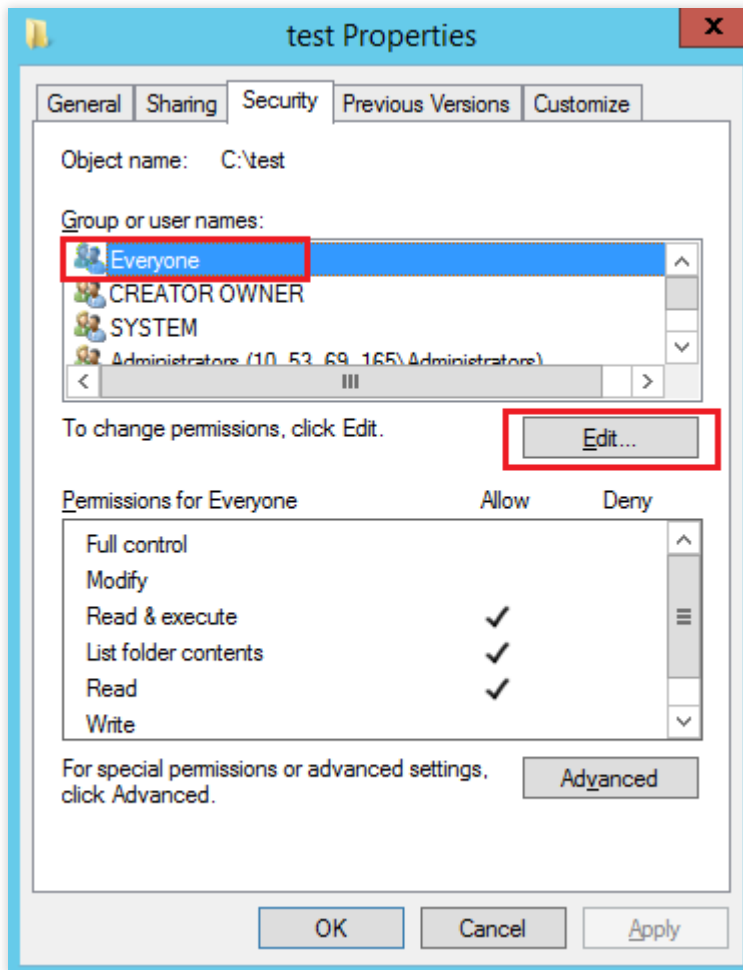
를 클릭하여 '내 PC' 창을 엽니다.

2. C 드라이브에서 `test` 폴더를 선택하고 우클릭 후, [속성]을 선택합니다.

3. 'test 속성' 창에서 [보안] 태그를 선택합니다.

4. 다음 이미지와 같이 `Everyone` 사용자를 선택하고 [편집]을 클릭합니다.

'그룹 또는 사용자 이름'에 `Everyone` 이 없는 경우 [Everyone 사용자 추가](#)를 참조하여 추가하십시오.

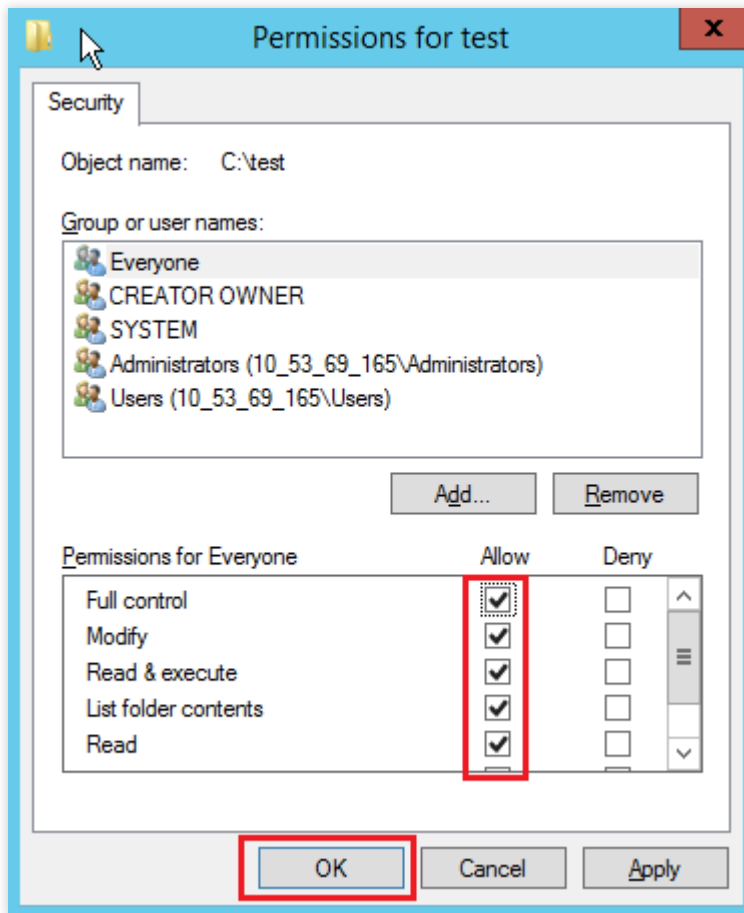


5.

다음

이미지와 같이 'test의 권한' 인터페이스에서 수요에 따라 `Everyone` 사용자의 권한을 설정하고 [확인]을 클릭합니다.

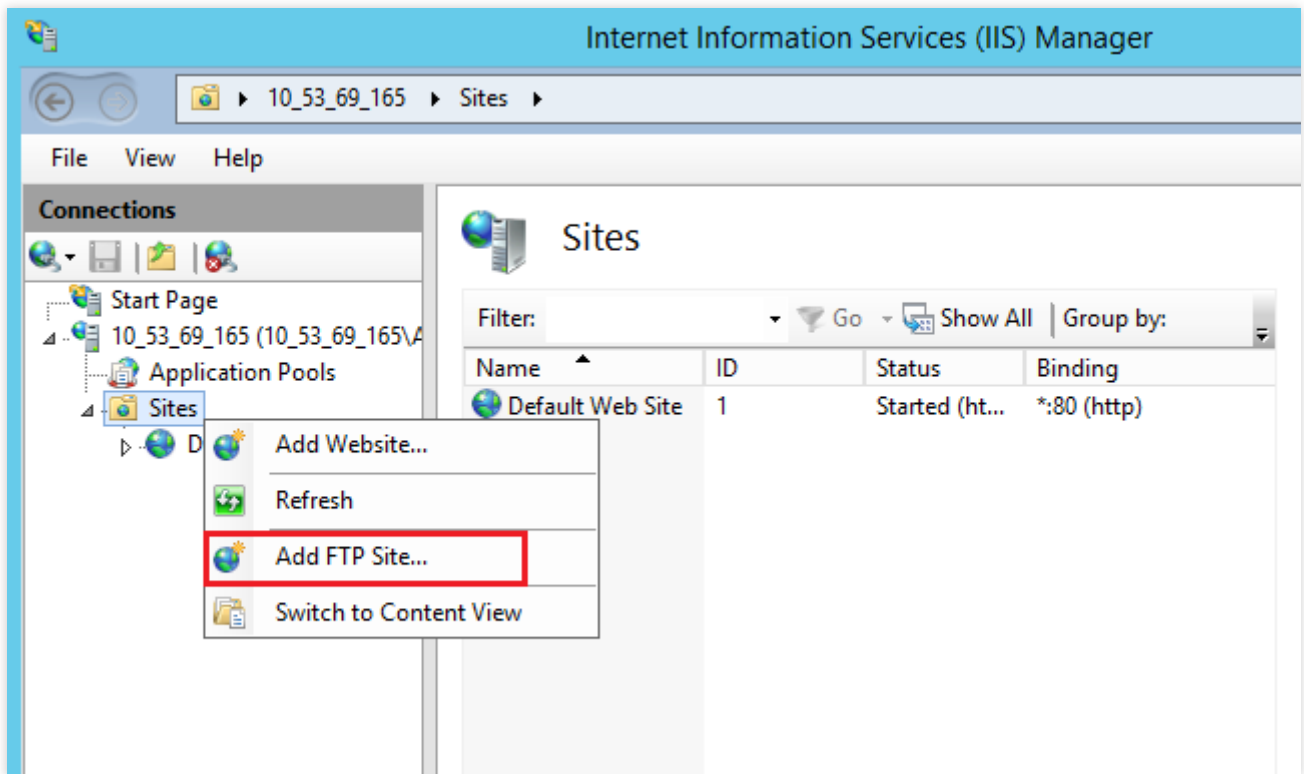
본 문서는 `Everyone` 사용자에게 모든 권한을 부여하는 것을 예시로 사용합니다.



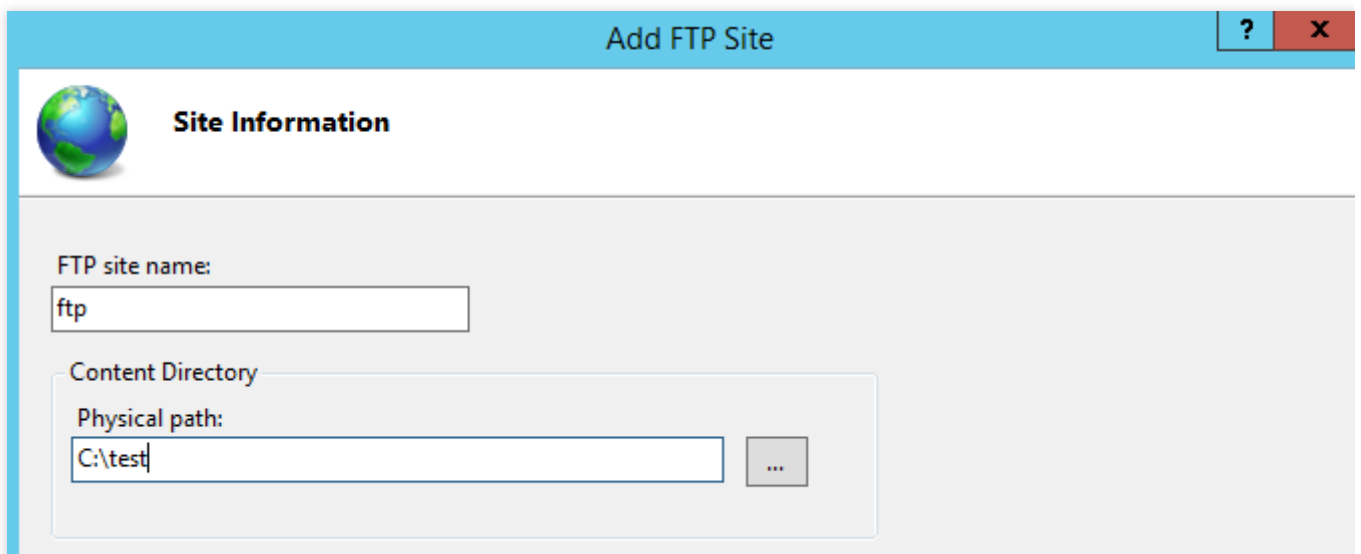
6. **test** 속성 창에서 [확인]을 클릭하여 설정을 완료합니다.

5단계: FTP 사이트 추가

1. '서버 관리자' 창에서 오른쪽 상단 메뉴의 [툴]>[Internet Information Services (IIS) 관리자]를 선택합니다.
2. 다음 이미지와 같이 열린 **Internet Information Services (IIS) 관리자** 창에서 왼쪽 메뉴의 서버 이름을 차례대로 펼치고 [웹 사이트]를 우클릭한 후, [FTP 사이트 추가]를 선택합니다.



3. '사이트 정보' 인터페이스에서 다음 정보를 참조하여 설정하고 [다음 단계]를 클릭합니다.



FTP 사이트 이름: FTP 사이트 이름을 입력합니다. 본 문서는 ftp 를 예시로 사용합니다.

물리 경로: 권한 설정을 완료한 공유 폴더의 경로를 선택하십시오. 본 문서는 C:\test 를 예시로 사용합니다.

4. '바인딩 및 SSL 설정' 인터페이스에서 다음 정보를 참조하여 설정하고 [다음 단계]를 클릭합니다.

Add FTP Site

Binding and SSL Settings

Binding

IP Address: All Unassigned Port: 21

☐ Enable Virtual Host Names:

Virtual Host (example: ftp.contoso.com):

☒ Start FTP site automatically

SSL

☒ No SSL

☐ Allow SSL

☐ Require SSL

SSL Certificate: Not Selected

Select... View...

Previous Next Finish Cancel

설정한 주요 매개변수 정보는 다음과 같습니다.

바인딩: IP 주소는 [전부 미할당]을 기본 선택하고 포트는 기본값 21(FTP 기본 포트 번호)입니다. 포트를 직접 설정할 수도 있습니다.

SSL: 수요에 따라 선택하십시오. 본 문서는 [SSL 없음]을 예시로 사용합니다.

SSL 없음: SSL 암호화가 필요하지 않습니다.

SSL 허용: FTP 서버가 클라이언트와의 비 SSL 및 SSL 연결을 지원하도록 허용합니다.

SSL 요구: SSL을 암호화해야만 FTP 서버와 클라이언트 사이에서 통신할 수 있습니다.

[SSL 허용] 또는 [SSL 필요]를 선택한 경우, 'SSL 인증서'에서 기존 SSL 인증서를 선택할 수 있습니다. [서버 인증서 제작](#) 순서를 참조하여 하나의 SSL 인증서를 만들 수도 있습니다.

5. '인증 및 라이선스 정보' 인터페이스에서 다음 정보를 참조하여 설정하고 [다음 단계]를 클릭합니다.

Add FTP Site

Authentication and Authorization Information

Authentication

☐ Anonymous

☒ Basic

Authorization

Allow access to:

Specified users

ftpuuser

Permissions

☒ Read

☒ Write

Previous Next Finish Cancel

인증: 인증 방법 중 하나를 선택합니다. 본 문서는 [기본]을 예시로 사용합니다.

익명: 모든 사용자가 익명 또는 FTP 사용자 이름만 제공하는 콘텐츠에 액세스하도록 허용합니다.

기본: 사용자가 유효한 사용자 이름과 비밀번호를 제공해야만 콘텐츠에 액세스할 수 있도록 요구합니다. 기본 인증은 네트워크를 통해 암호화되지 않은 비밀번호를 전송하기 때문에, 사용자가 클라이언트와 FTP 서버 간 연결이 안전하다고 인지할 때만(예: SSL 사용) 이 인증 방법을 사용할 수 있습니다.

라이선스: 액세스가 허용되는 풀다운 리스트에서 한 가지 방식을 선택합니다. 본 문서는 지정 사용자 `ftpuuser` 를 예시로 사용합니다.

모든 사용자: 익명 사용자나 신원이 표시된 사용자에게 관계 없이 모든 사용자는 해당 콘텐츠에 액세스할 수 있습니다.

익명 사용자: 익명 사용자는 콘텐츠에 액세스할 수 있습니다.

지정한 역할 또는 사용자 그룹: 일부 역할 또는 사용자 그룹의 멤버만 콘텐츠에 액세스할 수 있습니다. 이 항목을 선택하면 역할 또는 사용자 그룹을 지정해야 합니다.

지정한 사용자: 지정한 사용자만 콘텐츠에 액세스할 수 있습니다. 이 항목을 선택하면 사용자 이름을 지정해야 합니다.

권한: 필요에 따라 권한을 설정합니다. 본 문서는 [읽기] 및 [쓰기] 권한 설정을 예시로 사용합니다.

읽기: 권한이 부여된 사용자의 디렉터리로부터 콘텐츠 읽기를 허용합니다.

쓰기: 권한이 부여된 사용자의 디렉터리 쓰기를 허용합니다.

6. [완료]를 클릭하면 즉시 FTP 사이트 생성이 완료됩니다.

6단계: 보안 그룹 및 방화벽 설정

1. FTP 사이트 구축 완료 후 FTP 액세스 모드에 따라 FTP 사이트 추가 시 포트를 바인딩하는 인바운드 규칙을 개방하십시오.

능동 모드: 20 및 21 포트를 개방합니다.

수동 모드: 21 포트 및 1024 ~ 65535 사이의 포트(예: 5000 ~ 6000 개방)를 개방합니다.

해당 인바운드 규칙을 추가하는 방법은 [보안 그룹 규칙 추가](#)를 참조하십시오.

2. (옵션) FTP 서버가 방화벽으로부터의 수동 연결을 수락할 수 있도록 [Microsoft 공식 홈페이지 문서](#)를 참조하여 FTP 사이트의 방화벽 지원을 설정합니다.

7단계: FTP 사이트 테스트

FTP 클라이언트 소프트웨어와 브라우저 또는 파일 리소스 관리자 등의 툴을 통해 FTP 서비스를 인증할 수 있습니다. 본 문서는 클라이언트의 파일 리소스 관리자를 예시로 사용합니다.

1. 실제 상황에 따라 IE 브라우저를 설정하세요.

FTP 사이트 방화벽이 설정된 경우(능동 모드):

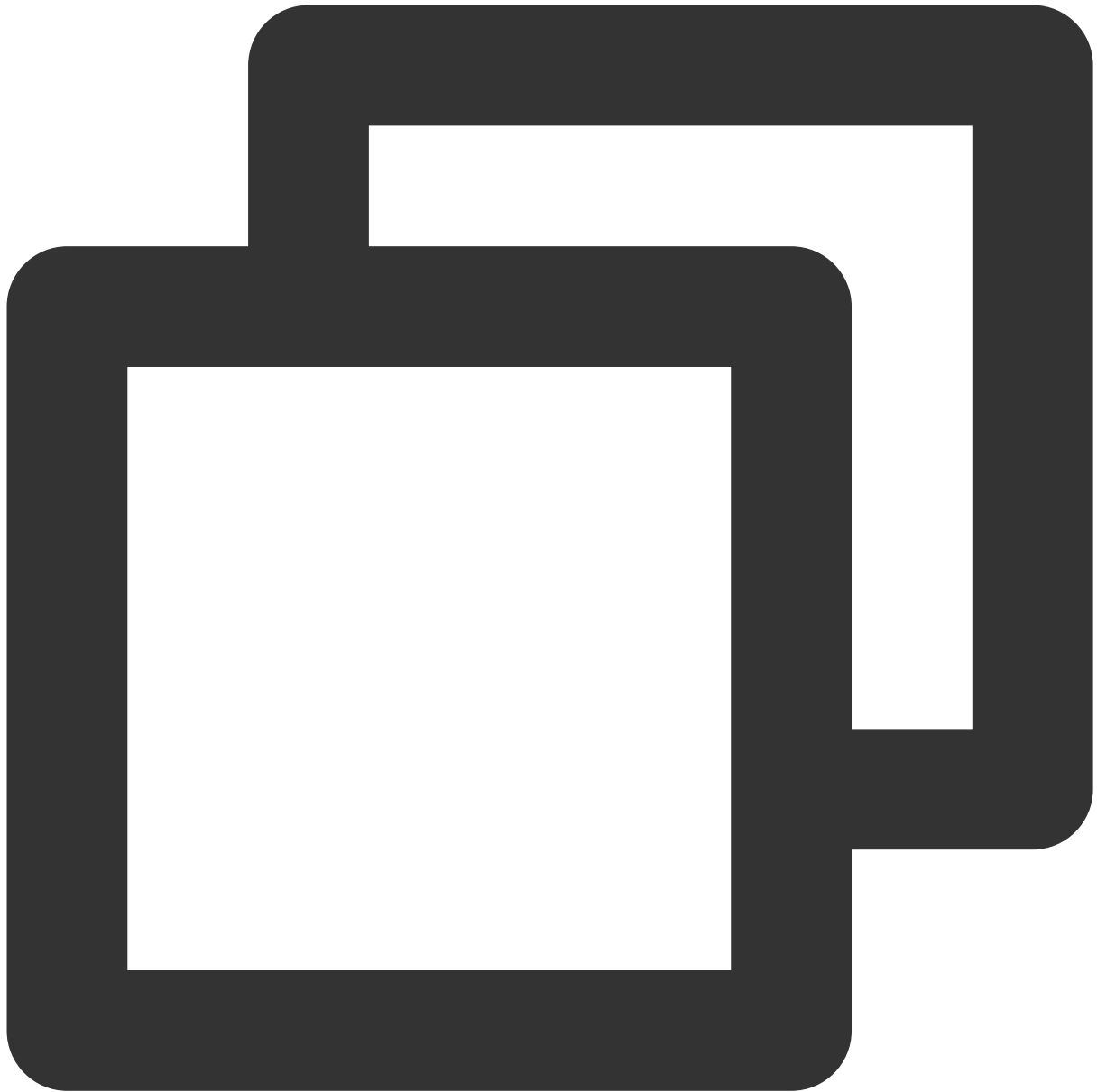
클라이언트의 IE 브라우저를 열어 [도구]>[Internet 옵션]>[고급]을 선택합니다. [방화벽 및 DSL 모뎀과 호환되는 수동 FTP 사용] 선택을 해제하고 [확인]을 클릭합니다.

FTP 사이트 방화벽이 설정되지 않은 경우(수동 모드):

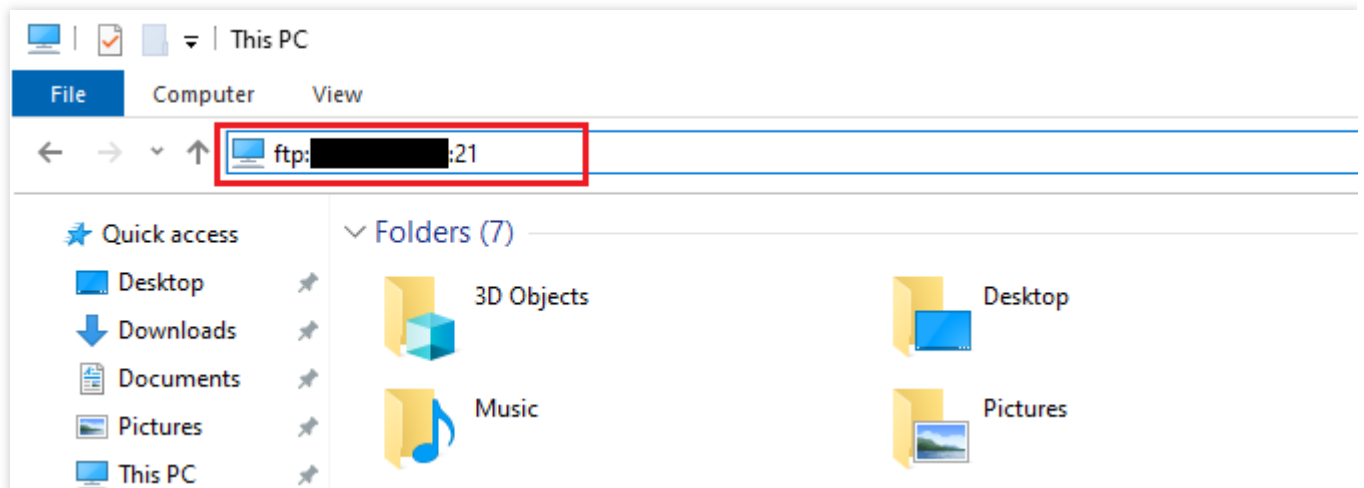
1.1.1 FTP 서버의 IE 브라우저를 열어 [도구]>[Internet 옵션]>[고급]을 선택합니다. [방화벽 및 DSL 모뎀과 호환되는 수동 FTP 사용] 선택을 해제하고 [확인]을 클릭합니다.

1.1.2 클라이언트의 IE 브라우저를 열어 [도구]>[Internet 옵션]>[고급]을 선택하고 [방화벽 및 DSL 모뎀과 호환되는 수동 FTP 사용] 선택을 해제하고 [확인]을 클릭합니다.

2. 클라이언트의 컴퓨터를 열어 경로 창에서 다음 주소에 액세스합니다.



ftp://CVM 공용 네트워크 IP:21

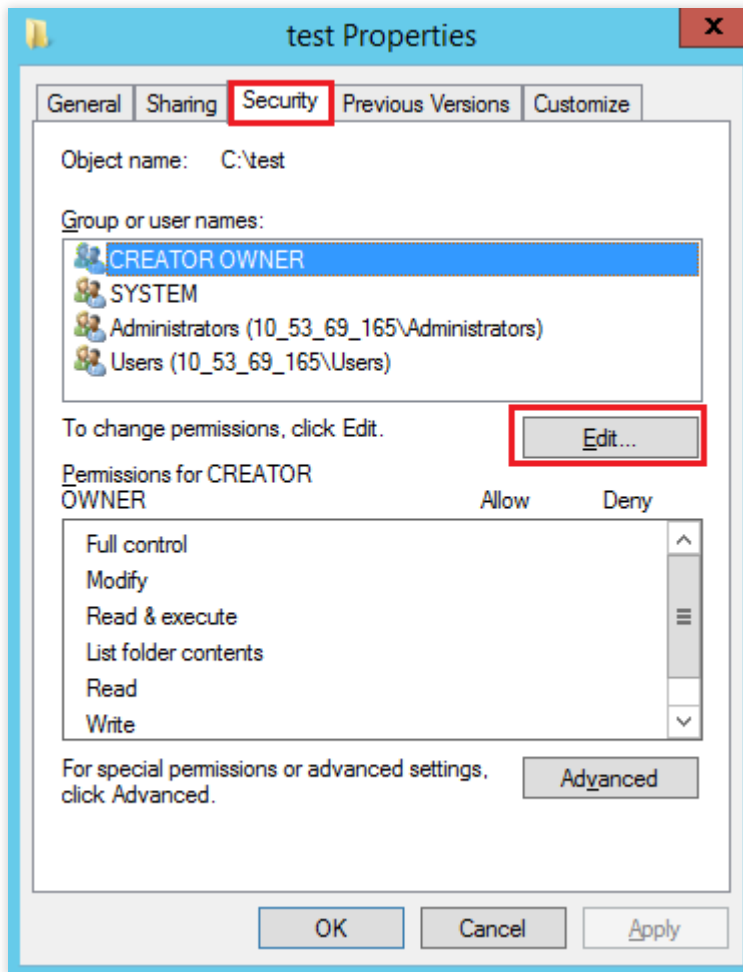


3. '로그인 정보' 팝업 창에 [FTP 사용자 이름 및 비밀번호 생성](#)에서 설정된 사용자 이름 및 비밀번호를 입력합니다.
본 문서에서 사용하는 사용자 이름은 `ftpuser` 이고 비밀번호는 `tf7295TFY` 입니다.
4. 로그인 성공 후 즉시 파일을 업로드 및 다운로드할 수 있습니다.

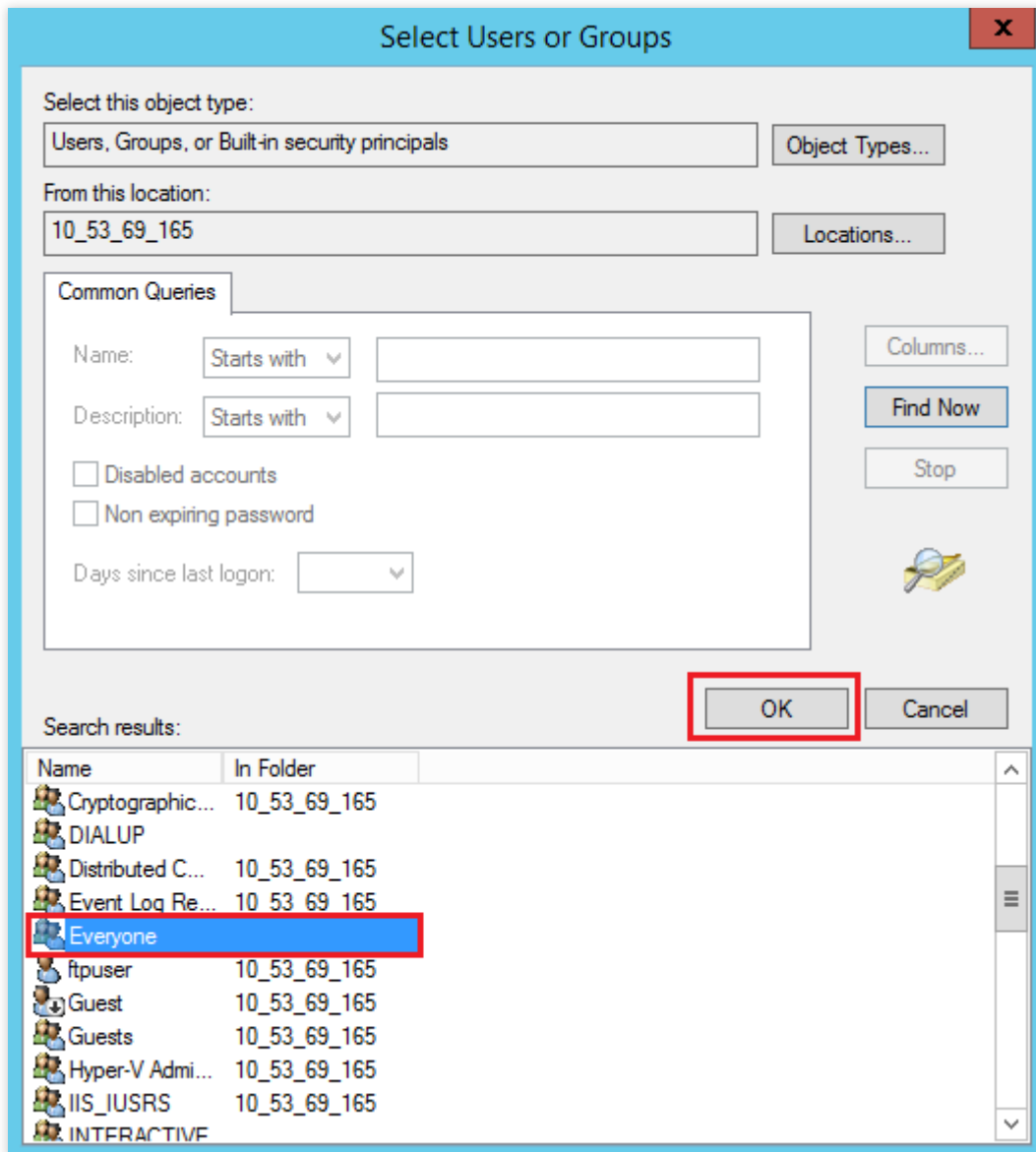
부록

Everyone 사용자 추가

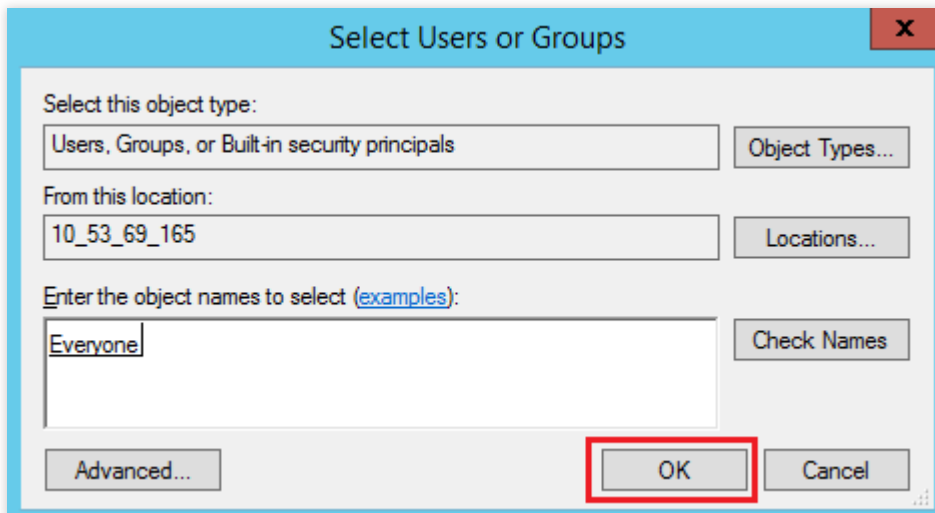
1. 다음 이미지와 같이 'test 속성' 창에서 [보안] 태그를 선택하고 [편집]을 클릭합니다.



2. 'test의 권한' 인터페이스에서 [추가]를 클릭합니다.
3. '사용자 또는 그룹 선택' 인터페이스에서 [고급]을 클릭합니다.
4. 팝업된 '사용자 또는 그룹 선택' 인터페이스에서 [바로 찾기]를 클릭합니다.
5. 다음 이미지와 같이 검색 결과에서 `Everyone` 을 선택하고 [확인]을 클릭합니다.



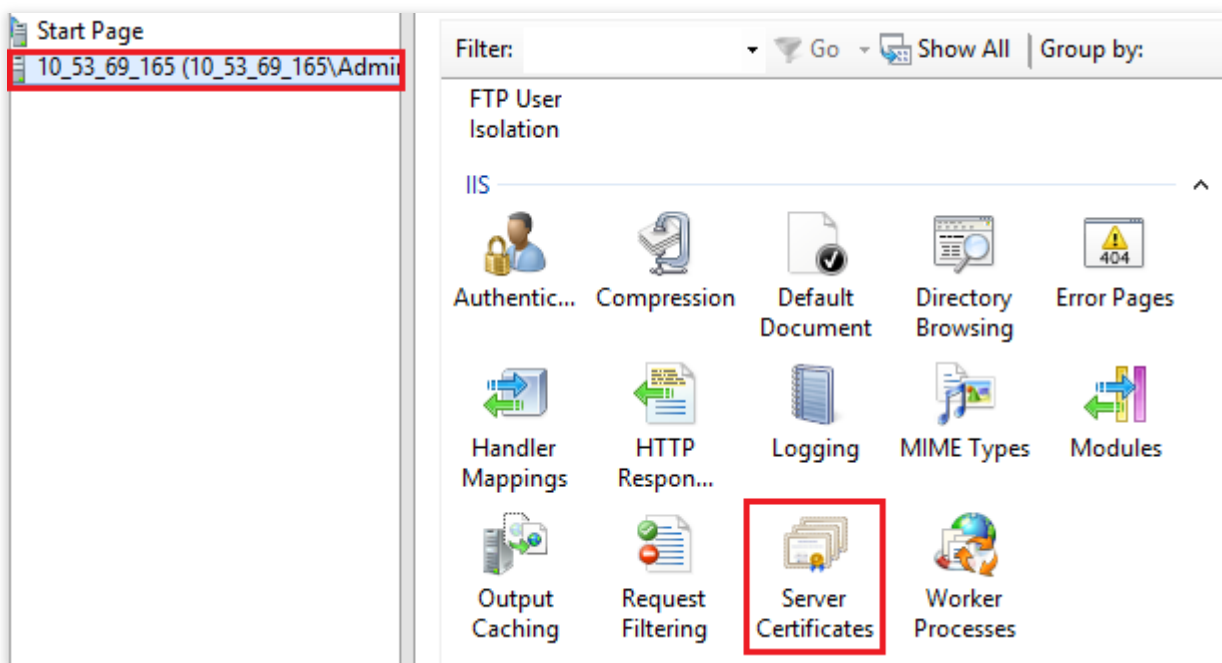
6. 다음 이미지와 같이 '사용자 또는 그룹 선택' 인터페이스에서 [확인]을 클릭하면 즉시 추가할 수 있습니다.



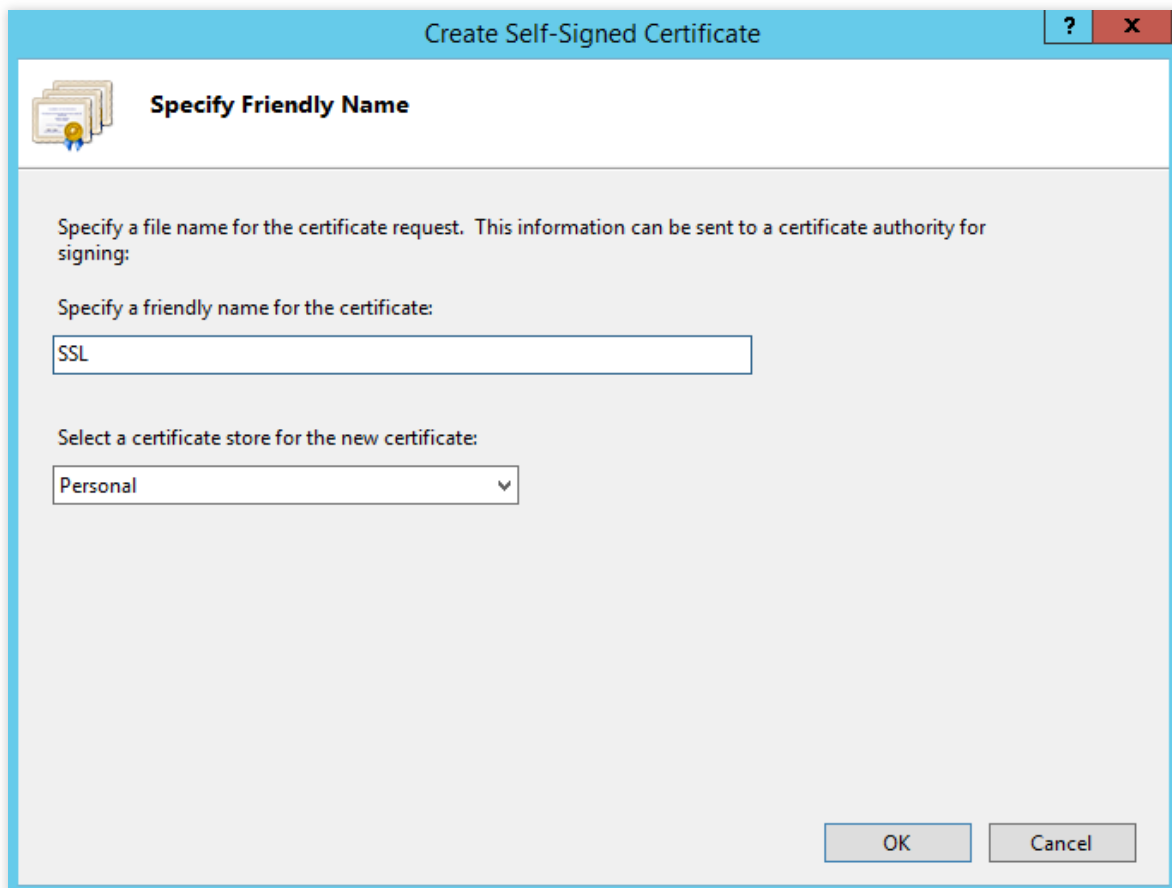
5단계로 이동하여 Everyone 사용자 권한을 설정합니다.

서버 인증서 제작

1. '서버 관리자' 창에서 오른쪽 상단 메뉴의 [툴]>[Internet Information Services (IIS) 관리자]를 선택합니다.
2. 다음 이미지와 같이 **Internet Information Services(IIS) 관리자** 팝업 창에서 왼쪽 메뉴의 서버를 선택하고 오른쪽 인터페이스의 [서버 인증서]를 더블 클릭합니다.



3. 오른쪽 작업 열에서 [자체 서명 인증서 생성]을 선택합니다.
4. 다음 이미지와 같이 '자체 서명 인증서 생성' 팝업 창에서 인증서 이름 및 스토리지 유형을 설정합니다. 본 문서는 개인 스토리지 유형의 SSL 인증서 생성을 예시로 사용합니다.



5. [확인]을 클릭하면 즉시 생성이 완료됩니다.

NTP 서비스

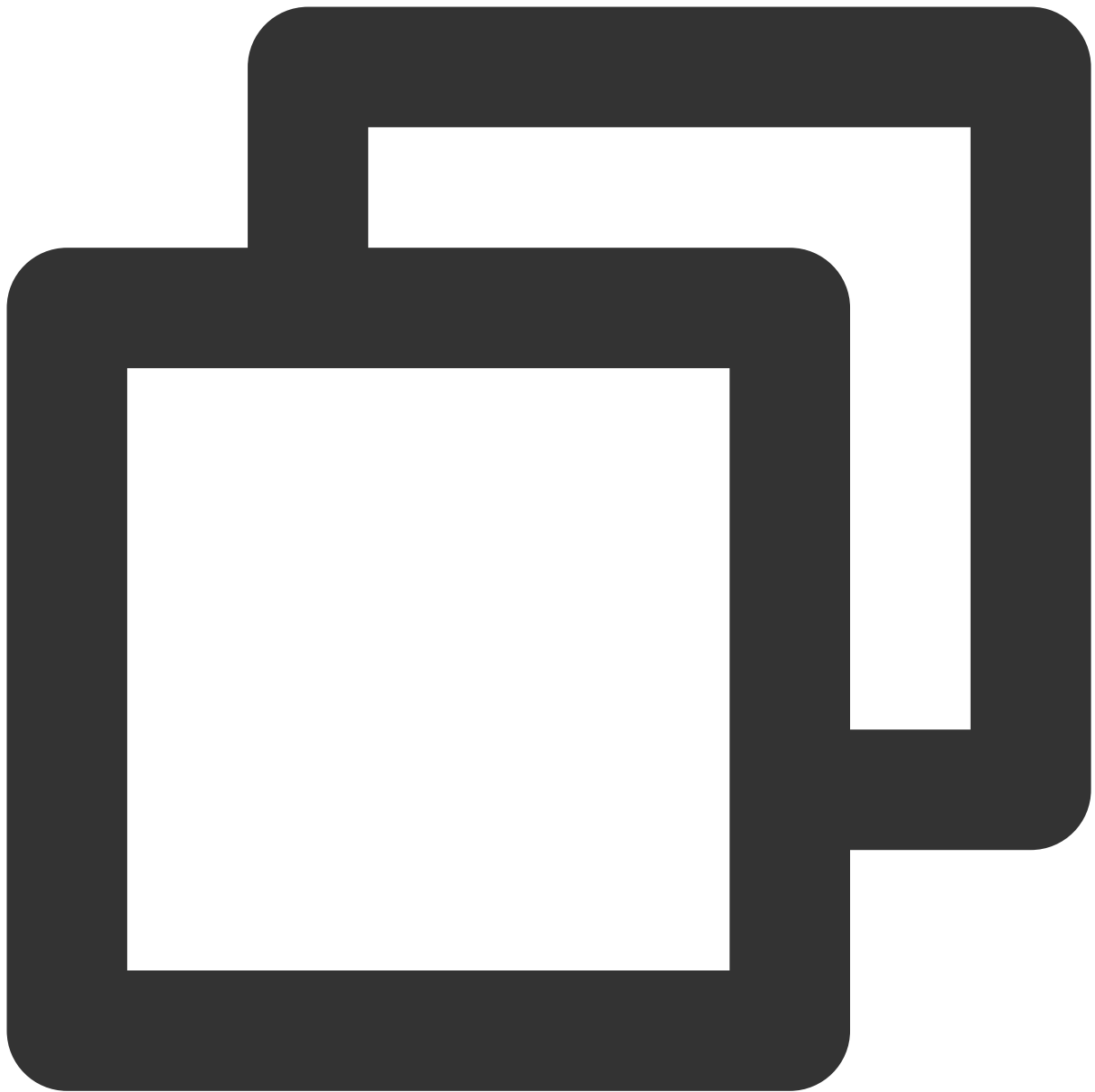
NTP 서비스 개요

최종 업데이트 날짜: : 2024-02-02 10:56:28

네트워크 타임 프로토콜(Network Time Protocol, NTP)은 네트워크에서 각 컴퓨터의 시간을 동기화하는 데 사용되는 프로토콜입니다. 그 용도는 컴퓨터의 시계를 협정 세계시 UTC로 동기화하는 것입니다.

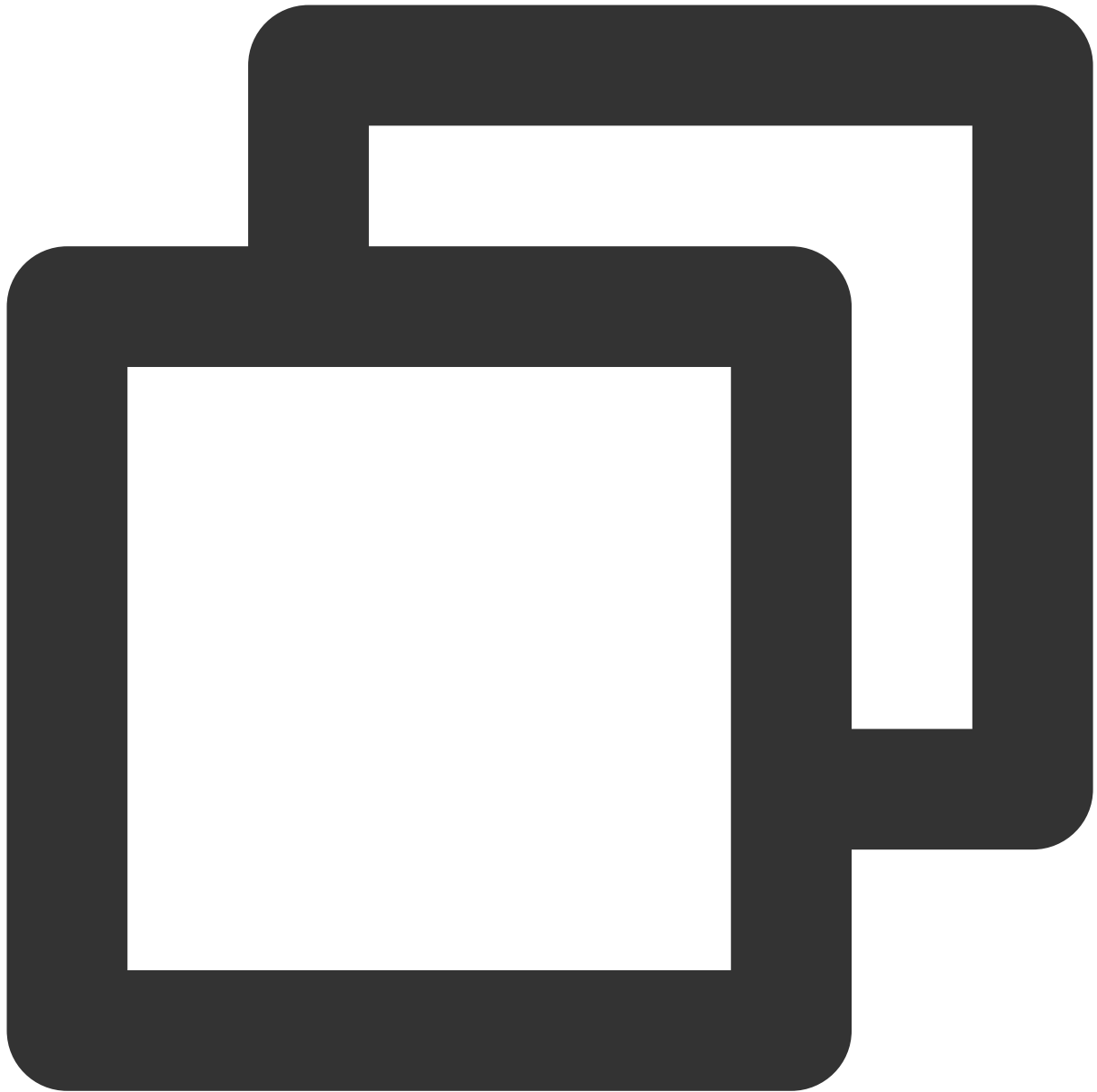
Tencent Cloud는 Tencent Cloud 내부 네트워크 디바이스용으로 내부 네트워크 NTP 서버를 제공하며 비 Tencent Cloud 디바이스일 경우, Tencent Cloud가 제공하는 공용 네트워크 NTP 서버를 사용할 수 있습니다.

내부 네트워크 NTP 서버



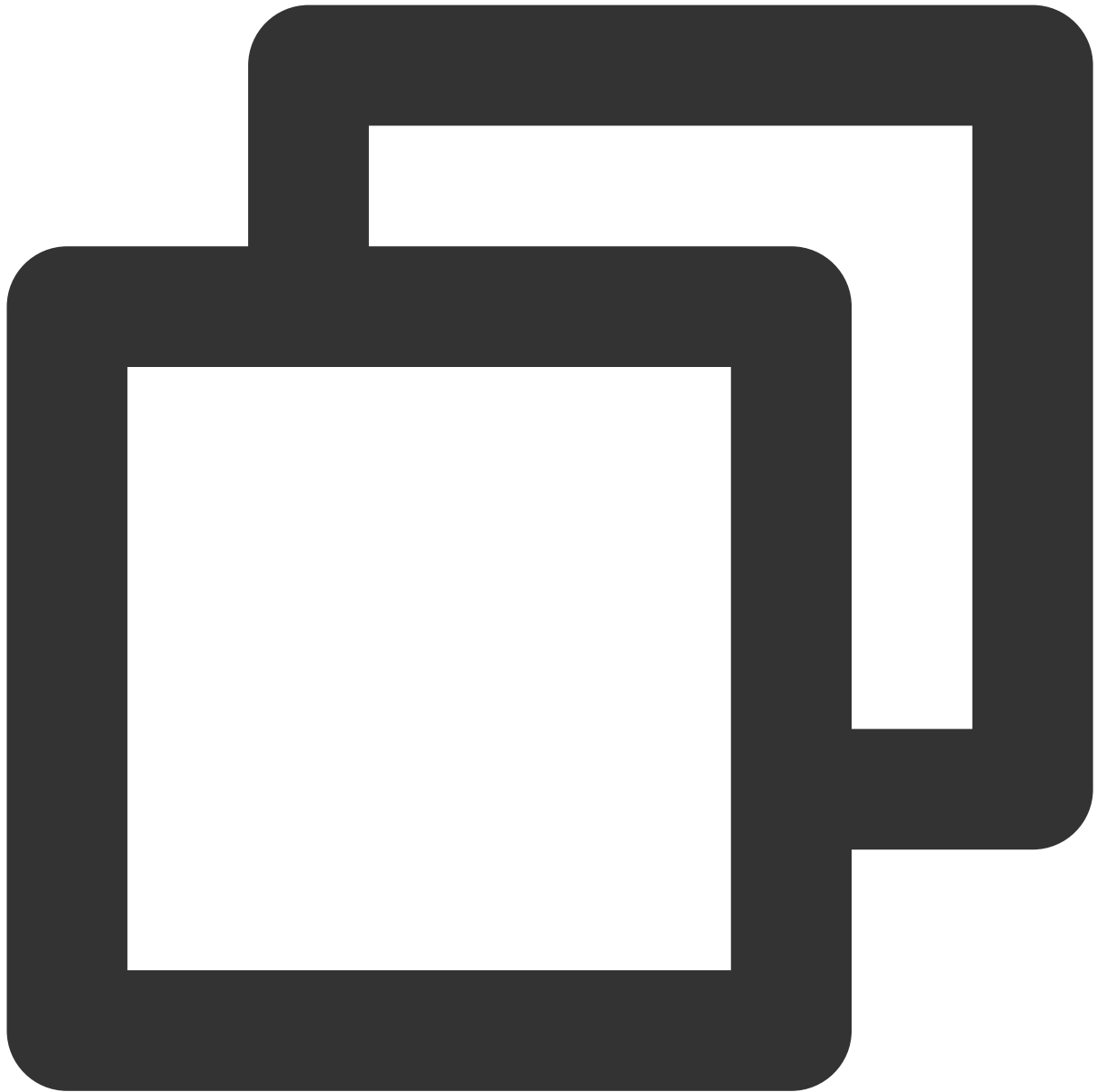
```
time1.tencentyun.com  
time2.tencentyun.com  
time3.tencentyun.com  
time4.tencentyun.com  
time5.tencentyun.com
```

외부 네트워크 NTP 서버



```
ntp.tencent.com  
ntp1.tencent.com  
ntp2.tencent.com  
ntp3.tencent.com  
ntp4.tencent.com  
ntp5.tencent.com
```

다음은 이전 외부 네트워크 NTP 서버 주소이며 이전 주소를 계속 사용할 수 있지만 새 외부 네트워크 NTP 서버 주소를 설정하여 사용하는 것이 좋습니다.



```
time.cloud.tencent.com  
time1.cloud.tencent.com  
time2.cloud.tencent.com  
time3.cloud.tencent.com  
time4.cloud.tencent.com  
time5.cloud.tencent.com
```

Linux 시스템의 NTP 타임 원본 서버 설정 관련 자세한 내용은 <[Linux 인스턴스에서 NTP 서비스 설정](#)>을 참고하십시오.

Windows 시스템의 NTP 타임 원본 서버 설정 관련 자세한 내용은 <[Windows 인스턴스에서 NTP 서비스 설정](#)>을 참고하십시오.

Linux 인스턴스에서 NTP 서비스 설정

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

Network Time Protocol daemon(NTPD)은 Linux 운영 체제의 데몬 프로세스 중 하나로, NTP 프로토콜을 완벽히 구현하였으며 로컬 시스템과 시계 원본 서버 간의 시간을 교정하는 데 사용됩니다. NTPD는 중단점 업데이트를 사용하는 NTPDate와 달리 스테핑식의 점진적인 시간 교정을 사용하므로 시간 점프 현상이 발생하지 않습니다. 본 문서는 CentOS 7.5 운영 체제의 CVM을 예로 들어 NTPD의 설치 및 설정 방법에 대해 소개합니다.

주의 사항

일부 운영 체제는 chrony를 기본 NTP 서비스로 사용하고 있으므로, NTPD가 실행 중인지와 부팅 시 자동 실행으로 되어 있는지 확인해야 합니다.

`systemctl is-active ntpd.service` 명령어를 사용하여 NTPD가 실행 중인지 확인할 수 있습니다.

`systemctl is-enabled ntpd.service` 명령어를 사용하여 NTPD가 부팅 시 자동 실행으로 되어 있는지 확인할 수 있습니다.

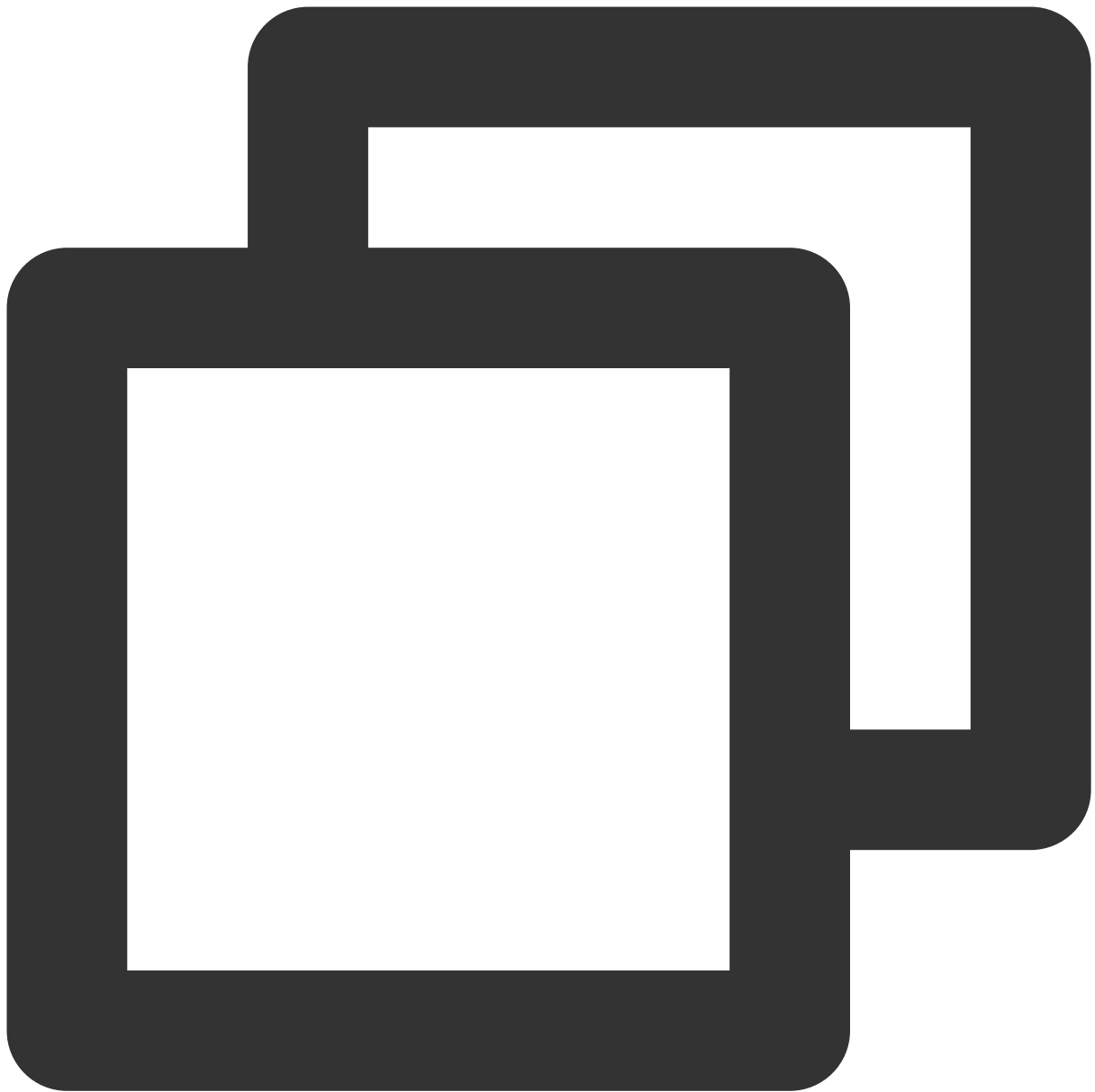
NTP 서비스의 통신 포트는 UDP 123으로, NTP 서비스를 설정하기 전에 UDP 123 포트가 개방된 상태를 유지해야 합니다.

해당 포트를 개방하지 않았다면 [보안 그룹 규칙 추가](#)를 참조하여 개방하시기 바랍니다.

작업 순서

NTPD 설치

다음 명령어를 실행하여 NTPD가 설치되어 있는지 확인합니다.

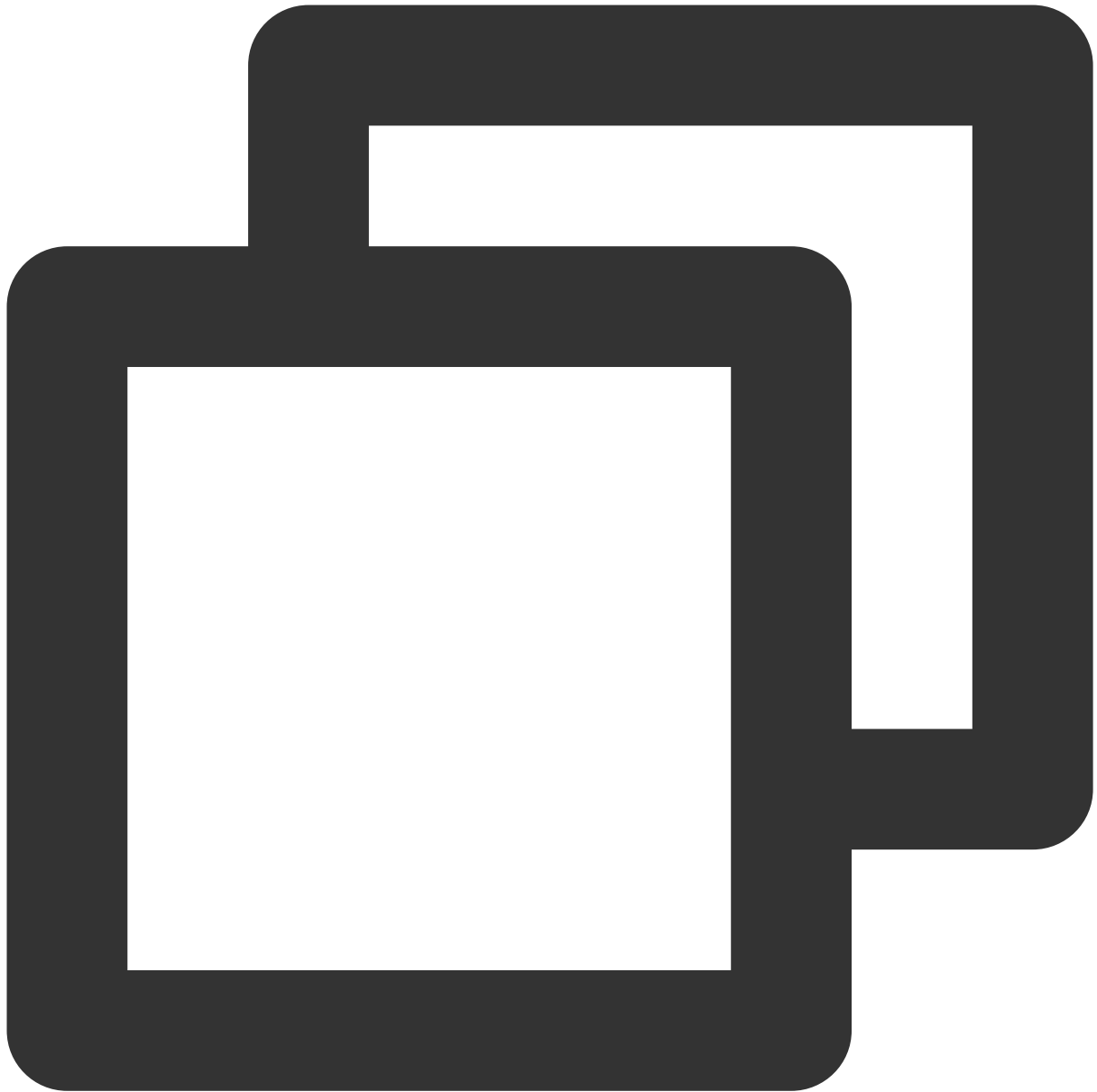


```
rpm -qa | grep ntp
```

아래와 같은 결과가 출력된다면 NTPD가 설치되어 있음을 의미합니다.

```
[root@VM_16_2_centos ~]# rpm -qa | grep ntp
ntpdate-4.2.6p5-28.el7.centos.x86_64
ntp-4.2.6p5-28.el7.centos.x86_64
fontpackages-filesystem-1.44-8.el7.noarch
```

NTPD가 설치되어 있지 않다면 `yum install ntp` 를 통해 NTPD를 설치합니다.

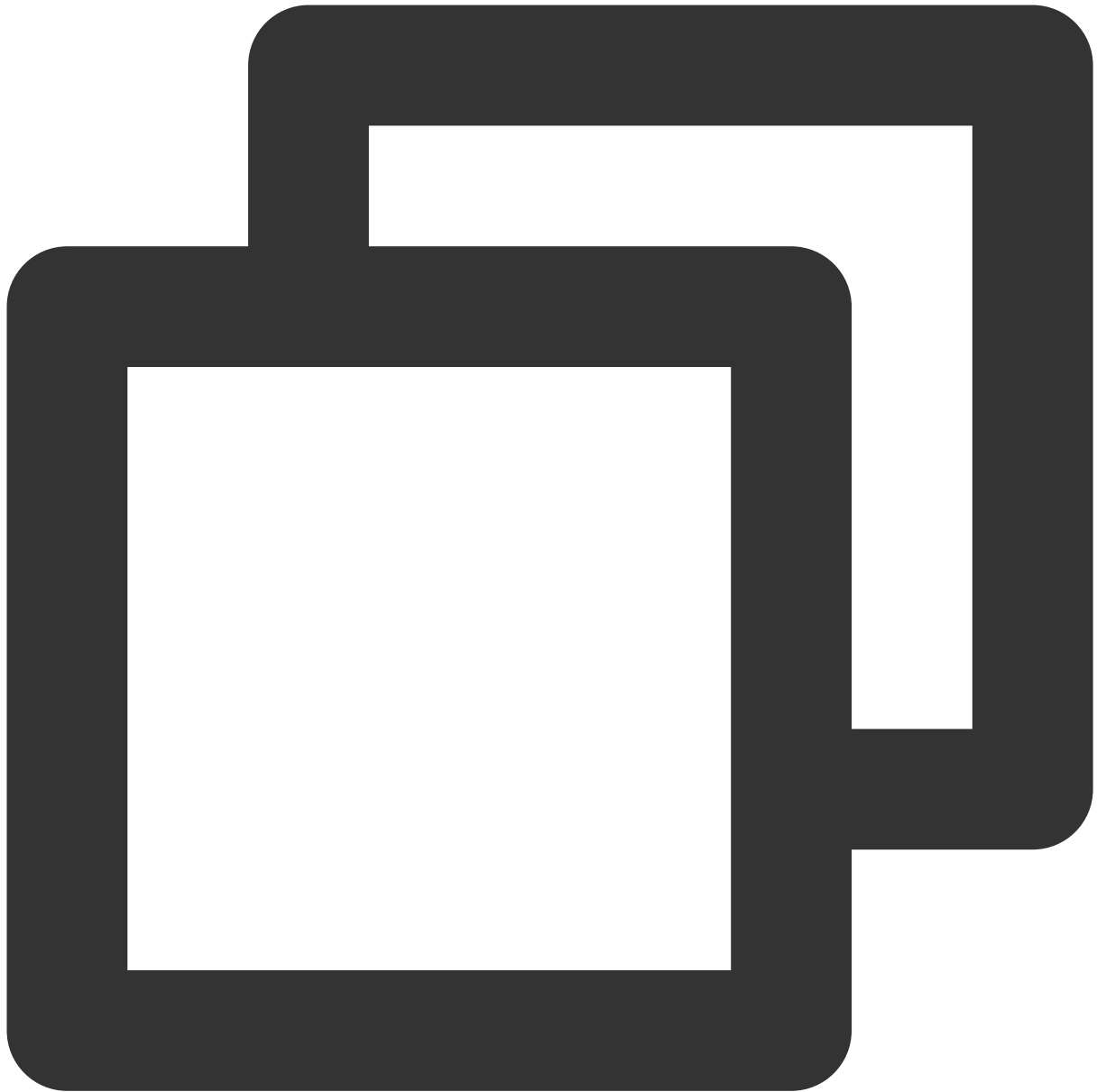


```
yum -y install ntp
```

NTPD는 기본적으로 클라이언트 실행 방식을 사용합니다.

NTP 설정

1. 다음 명령어를 실행하여 NTP 서비스 구성 파일을 엽니다.



```
vi /etc/ntp.conf
```

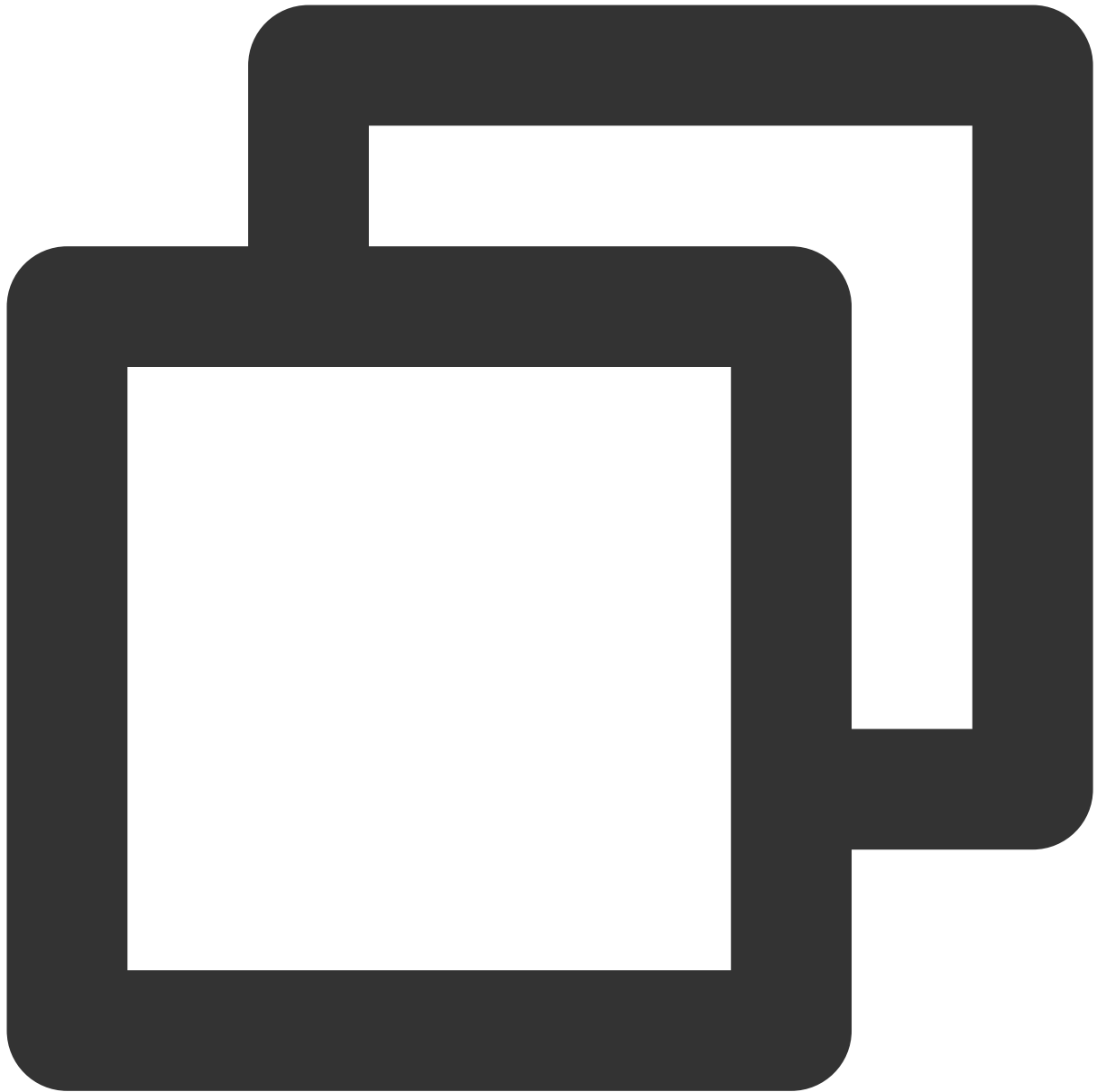
2. 아래 이미지와 같이 **i**를 눌러 편집 모드로 바꾸고, **server** 관련 설정을 찾아 설정하고자 하는 타깃 **NTP**의 시계 원본 서버(예: `time1.tencentyun.com`)로 **server**를 수정한 다음, 불필요한 **NTP** 시계 원본 서버를 삭제합니다.

```
# Use public servers from the pool.ntp.org project.  
# Please consider joining the pool (http://www.pool.ntp.org/join.html).  
server 0.centos.pool.ntp.org iburst  
server 1.centos.pool.ntp.org iburst  
server 2.centos.pool.ntp.org iburst  
server 3.centos.pool.ntp.org iburst
```

3. **Esc**를 누르고 **:wq**를 입력하여 파일을 저장한 뒤 리턴합니다.

NTPD 실행

다음 명령어를 실행하여 NTPD 서비스를 재시작합니다.

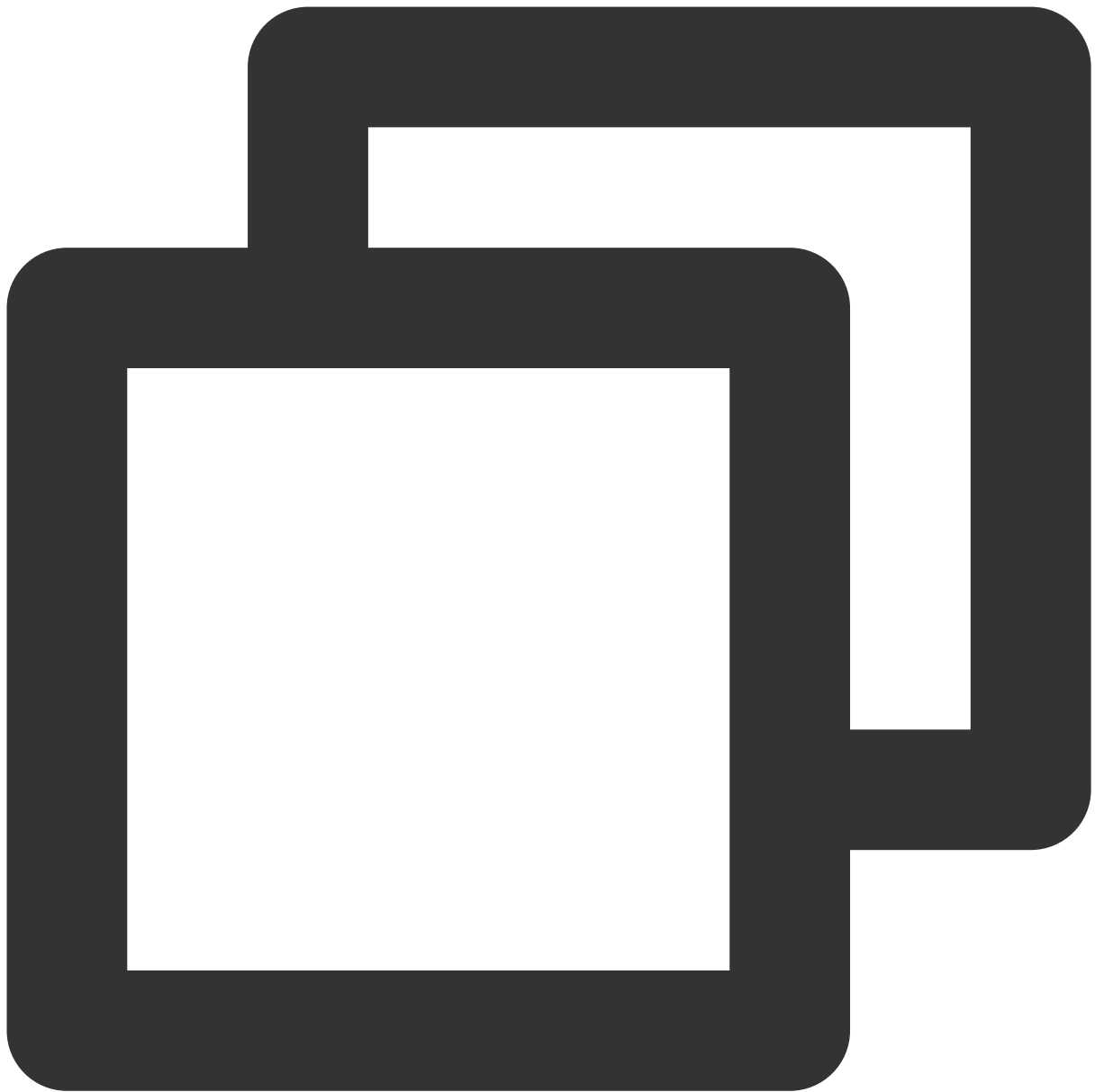


```
systemctl restart ntpd.service
```

NTPD 상태 확인

다음 명령어를 실제 수요에 맞게 실행하여 NTPD의 상태를 확인합니다.

다음 명령어를 실행하여, NTP 서비스 포트인 UDP 123 포트가 정상적으로 리스되고 있는지 확인합니다.

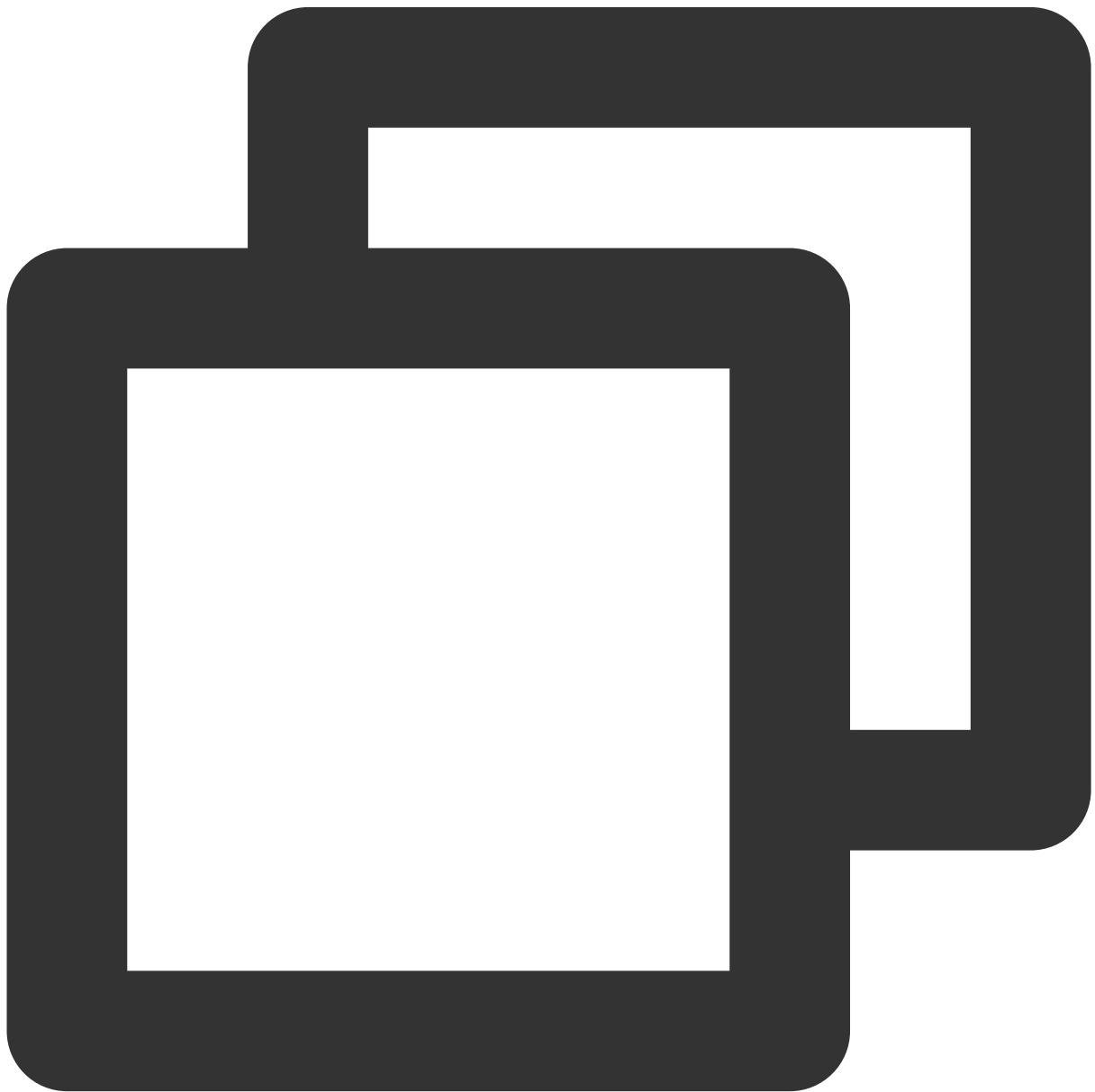


```
netstat -nupl
```

아래와 같은 결과가 출력된다면 정상적으로 리스되고 있음을 의미합니다.

```
[root@VM_0_136_centos ~]# netstat -nupl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 172.30.0.136:123        0.0.0.0:*
udp        0      0 127.0.0.1:123           0.0.0.0:*
udp6       0      0 fe80::5054:ff:fec2::123 :::*
udp6       0      0 ::1:123                 :::*
[root@VM_0_136_centos ~]#
```

다음 명령어를 실행하여 NTPD의 상태가 정상인지 확인합니다.



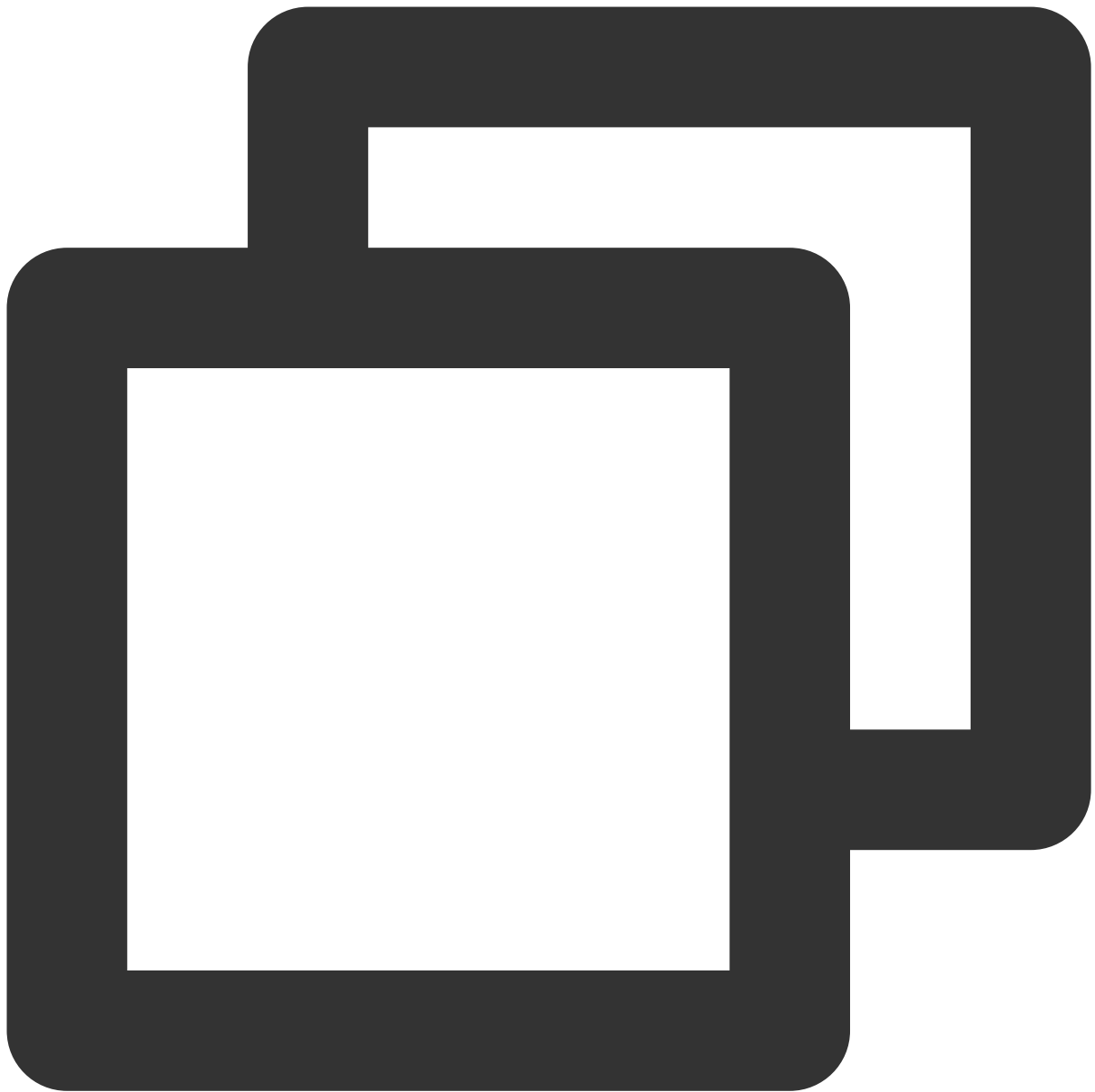
```
service ntpd status
```

아래와 같은 결과가 출력된다면 NTPD의 상태가 정상임을 의미합니다.

```
[root@VM_0_136_centos ~]# service ntpd status
Redirecting to /bin/systemctl status ntpd.service
• ntpd.service - Network Time Service
   Loaded: loaded (/usr/lib/systemd/system/ntpd.service; enabled; vendor p
   Active: active (running) since Wed 2019-08-07 15:23:25 CST; 5min ago
   Process: 997 ExecStart=/usr/sbin/ntpd -u ntp:ntp $OPTIONS (code=exited,
   Main PID: 999 (ntpd)
   CGroup: /system.slice/ntpd.service
           └─999 /usr/sbin/ntpd -u ntp:ntp -g

Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c01d 0d kern kernel tim
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: ntp_io: estimated max descripto
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 0 lo 127.0.0
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 1 eth0 172.3
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 2 lo ::1 UDP
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 3 eth0 fe80:
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listening on routing socket on
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c016 06 restart
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c012 02 freq_set kernel
Aug 07 15:23:34 VM_0_136_centos ntpd[999]: 0.0.0.0 c615 05 clock_sync
Hint: Some lines were ellipsized, use -l to show in full.
[root@VM_0_136_centos ~]#
```

다음 명령어를 실행하여 더 자세한 NTP 서비스 정보를 받을 수 있습니다.



```
ntpq -p
```

다음과 유사한 결과를 리턴합니다.

```
[root@VM_0_136_centos ~]# ntpq -p
=====
      remote               refid              st t when poll reach   delay   offset  jitter
=====
  108.55.2.24             .INIT.              16 u    -   64    0    0.000   0.000   0.000
  193.228.143.22         194.59.202.20       2 u    6   64   17  277.831   3.940   5.000
 *185.253.55.26          194.59.202.20       2 u   68   64   16  201.280   1.729   0.000
  193.228.143.14         194.59.202.20       2 u   69   64   16  293.382   1.003   0.000
  169.229.8.3            100.122.36.4        2 u    3   64   17    6.607   9.897   0.000
[root@VM_0_136_centos ~]#
```

remote: 이 요청에 응답하는 NTP 서버의 이름.

refid: NTP 서버가 사용하는 상위 레벨의 NTP 서버.

st: remote 원격 서버의 레벨. 서버는 1-16 사이의 숫자로 레벨의 높고 낮음을 설정하며, 부하 및 네트워크 혼잡을 완화하기 위해 원칙상으로는 레벨 1의 서버에는 직접적으로 연결하지 않도록 권장합니다.

when: 지난번 요청 성공 이후부터 지금까지의 시간(초).

poll: 로컬 기기와 원격 서버가 얼마의 시간에 한 번 동기화(단위는 초)하는지 의미합니다. 초기에 NTP를 실행할 때의 poll 값은 비교적 낮으므로, 서버와의 동기화 빈도수가 늘어날 수 있습니다. 가능한 빨리 올바른 시간 범위로 변경하시기 바랍니다. 변경한 후에는 poll 값이 점점 늘어나며 동기화 빈도수는 상대적으로 줄어들게 됩니다.

reach: 8진수 값으로, 서버와 연결할 수 있는지 테스트하는 데 사용합니다. 한 번 연결에 성공할 때마다 reach의 값이 늘어납니다.

delay: 로컬 기기에서 NTP 서버로 동기화 요청을 보낼 때의 round trip time입니다.

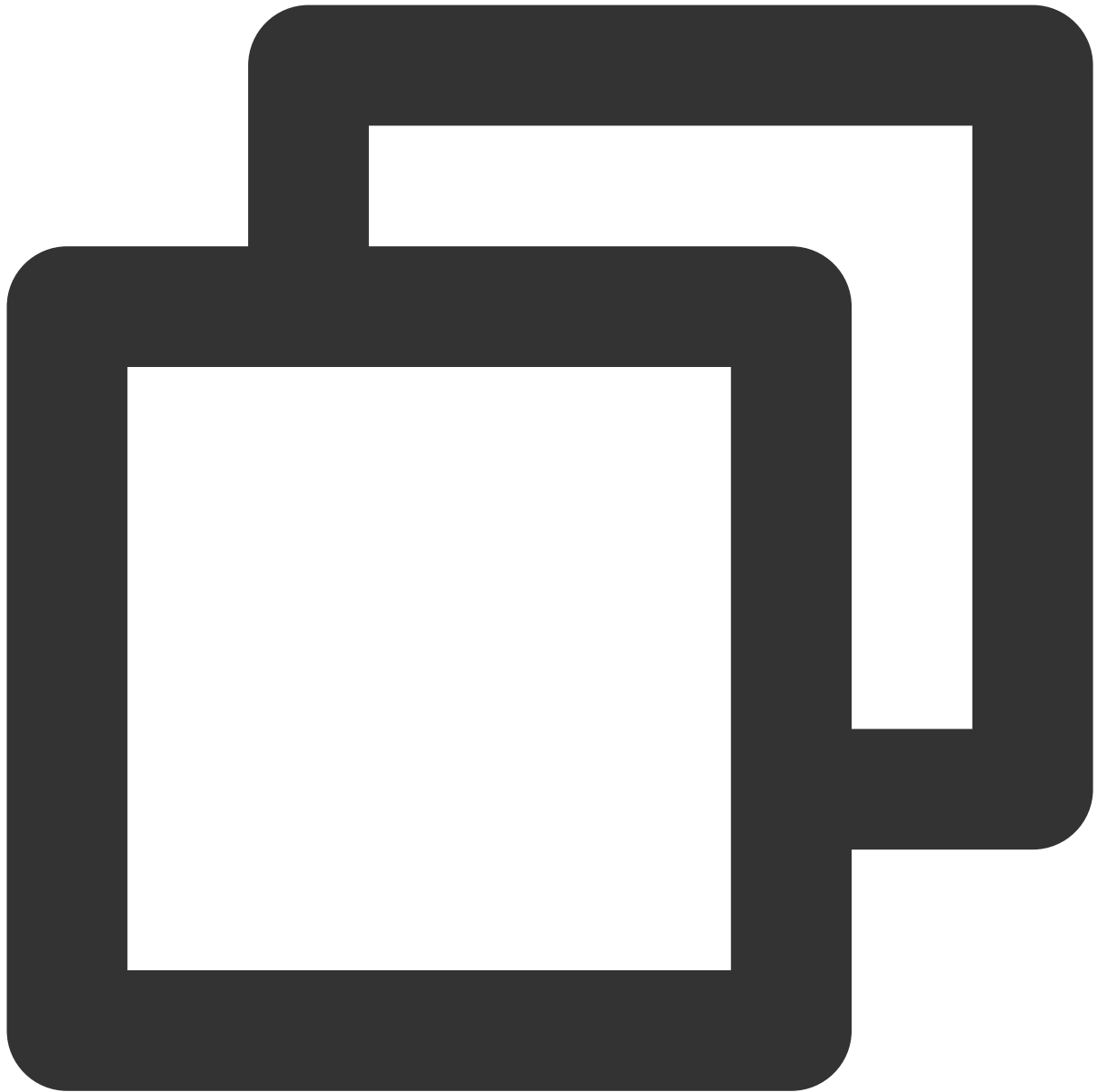
offset: 호스트는 NTP 시계를 통해 동기화할 타임 소스의 시간 오프셋을 동기화하며 단위는 밀리세컨드(ms)입니다.

offset이 0에 가까울수록 호스트와 NTP 서버의 시간이 더 가깝습니다.

jitter: 통계에 사용하는 값. 특정 기준으로 연속하는 숫자 내 offset의 분포 현황을 통계합니다. 즉 jitter 값의 절댓값이 작을수록 CVM의 시간이 더 정확합니다.

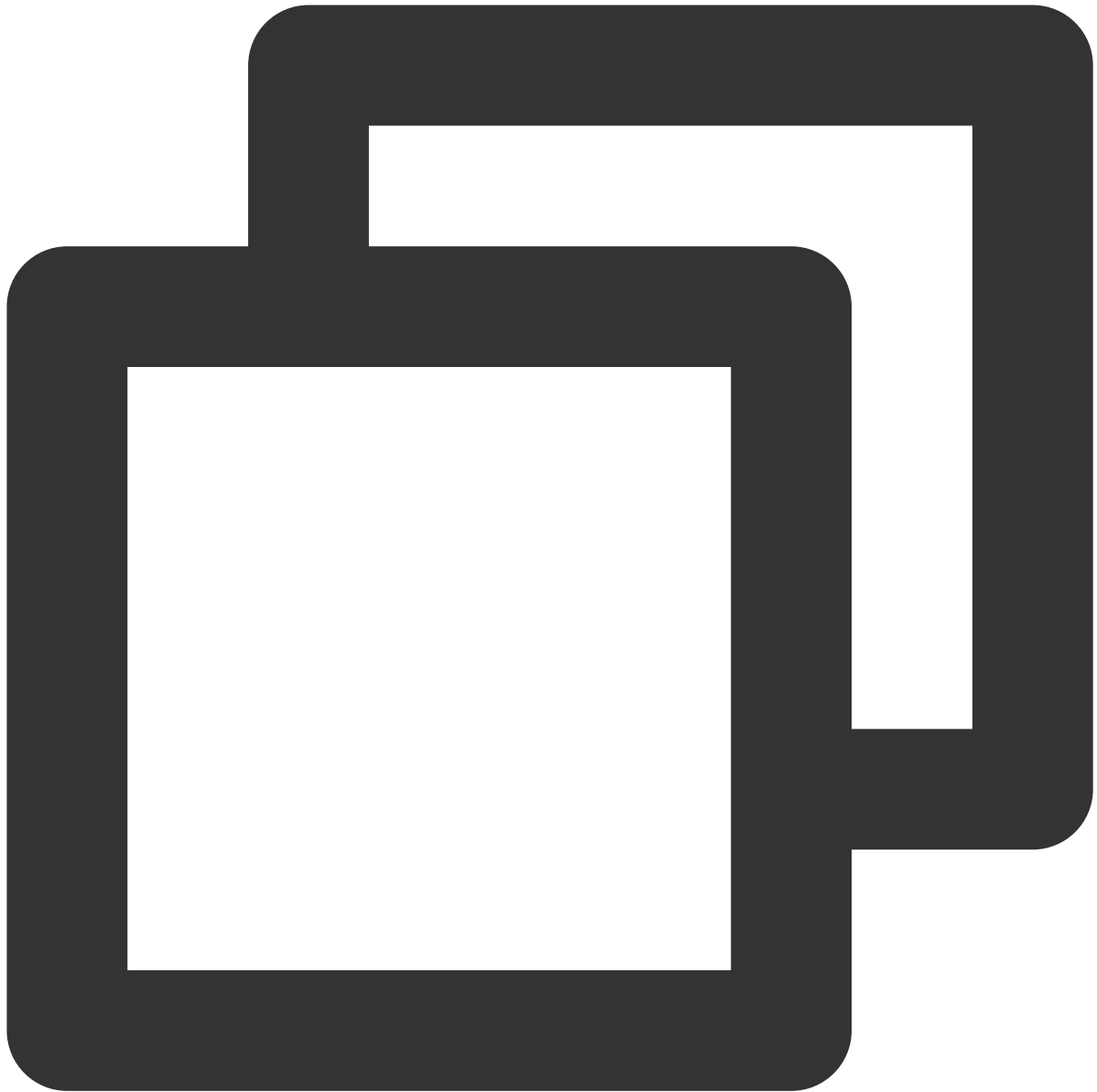
NTPD를 부팅 시 실행되도록 설정

1. 다음 명령어를 실행하여 NTPD를 부팅 시 자동 실행으로 설정합니다.



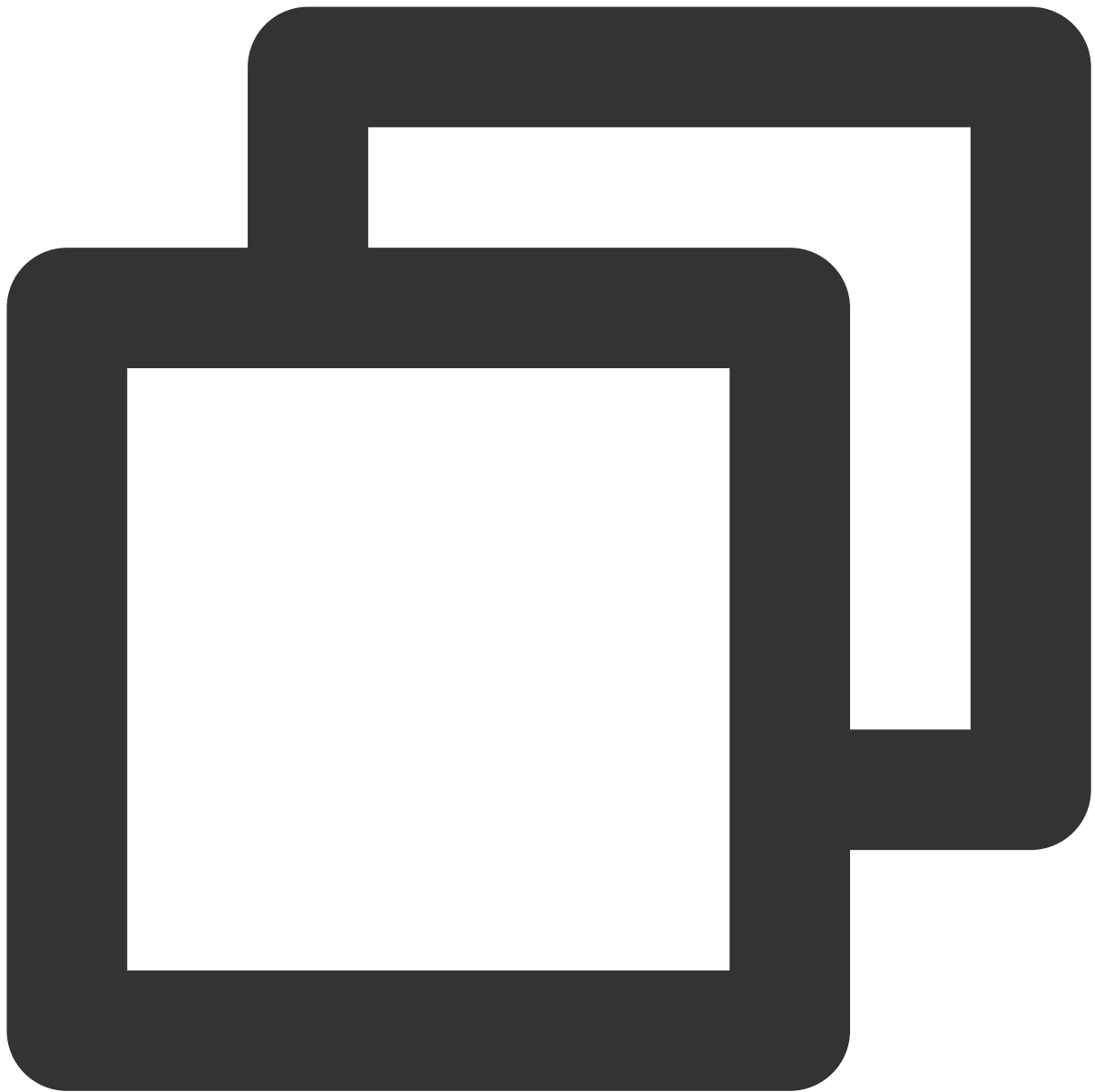
```
systemctl enable ntpd.service
```

2. 다음 명령어를 실행하여 chrony가 부팅 시 실행으로 설정되었는지 확인합니다.



```
systemctl is-enabled chronyd.service
```

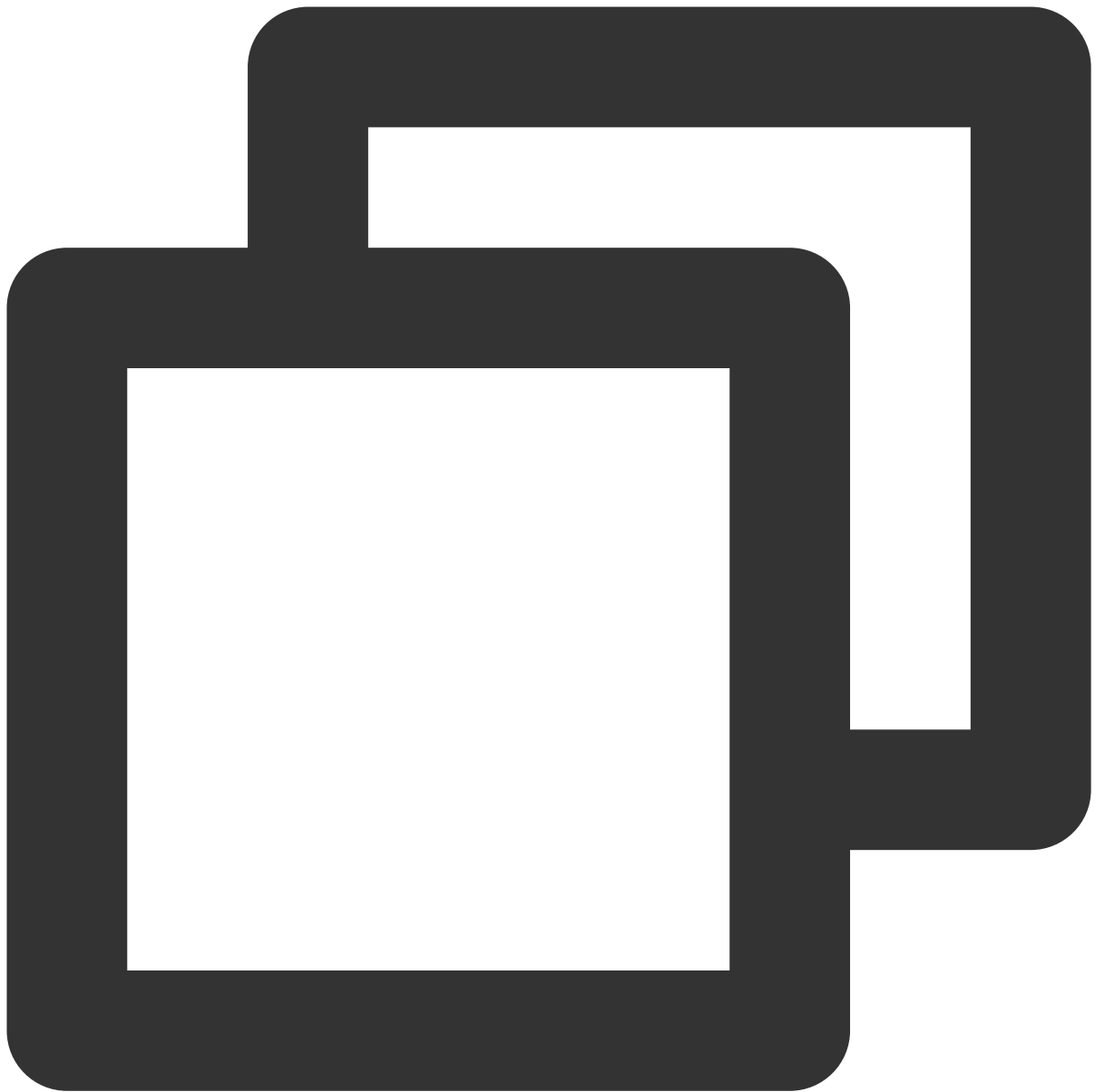
chrony가 부팅 시 실행으로 설정되었다면, 다음 명령어를 실행하여 chrony를 부팅 시 자동 실행에서 삭제합니다. chrony와 NTPD가 충돌하여 NTPD의 부팅 시 실행이 실패할 수 있습니다.



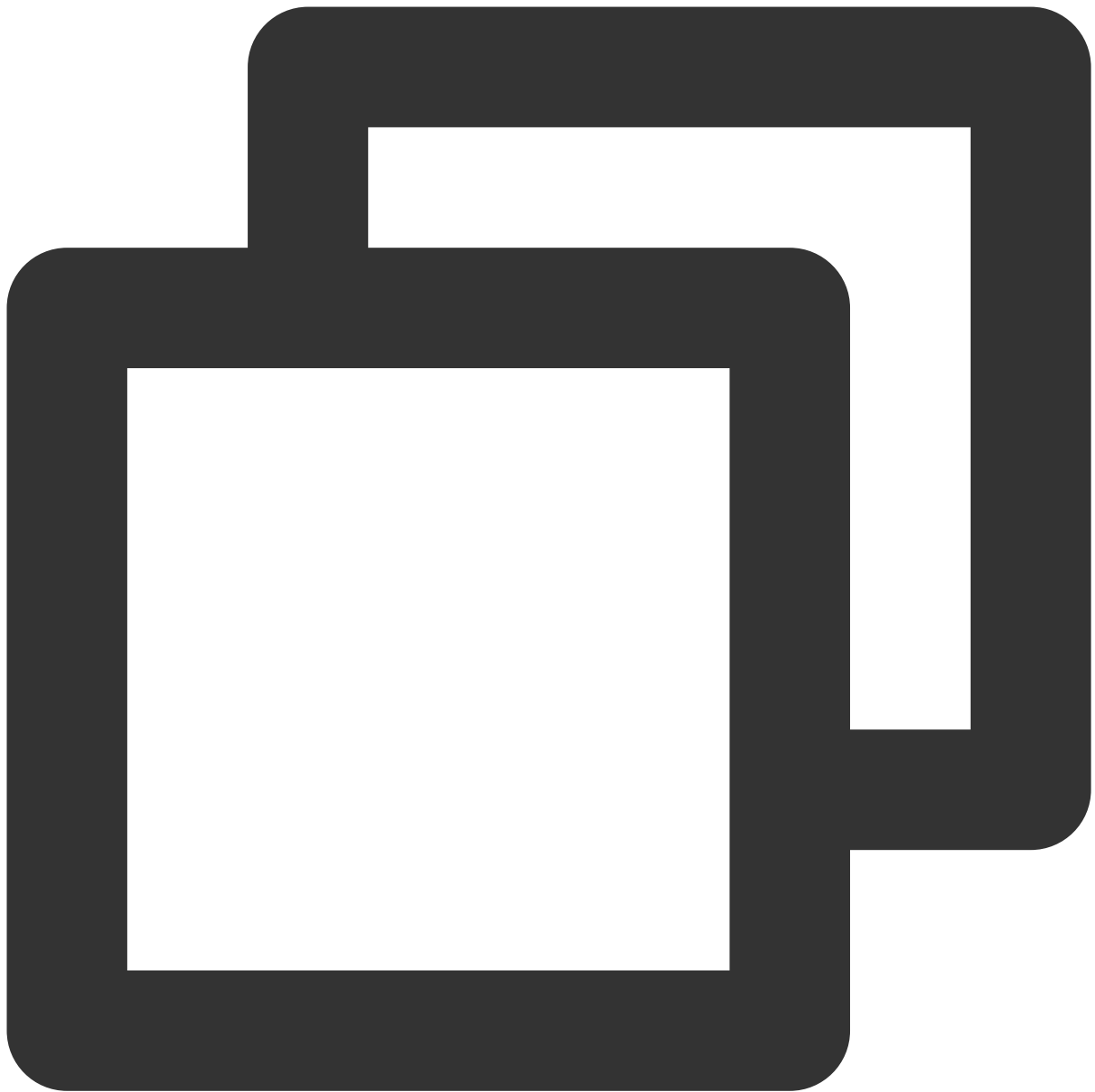
```
systemctl disable chronyd.service
```

NTPD의 보안성 향상

다음 명령어를 차례대로 실행하여 `/etc/ntp.conf` 구성 파일의 보안성을 향상합니다.



```
interface ignore wildcard
```



```
interface listen eth0
```

Linux 인스턴스: NTPDate를 NTPD로 전환

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

NTPDate는 중단점 업데이트를 사용하며, NTPD는 스테핑식의 점진적 시간 교정을 사용합니다. NTPDate 시간 동기화를 사용하고 있다면, 이미 탑재 및 실행 중인 서비스의 인스턴스에 대해 NTPD 시간 동기화를 사용하시기를 권장합니다. 본 문서는 CentOS 7.5 운영 체제의 CVM을 예로 들어 NTPDate를 NTPD로 전환하는 방법에 대해 소개합니다.

전제 조건

NTP 서비스의 통신 포트는 UDP 123으로, NTP 서비스를 설정하기 전에 UDP 123 포트가 개방된 상태를 유지해야 합니다.

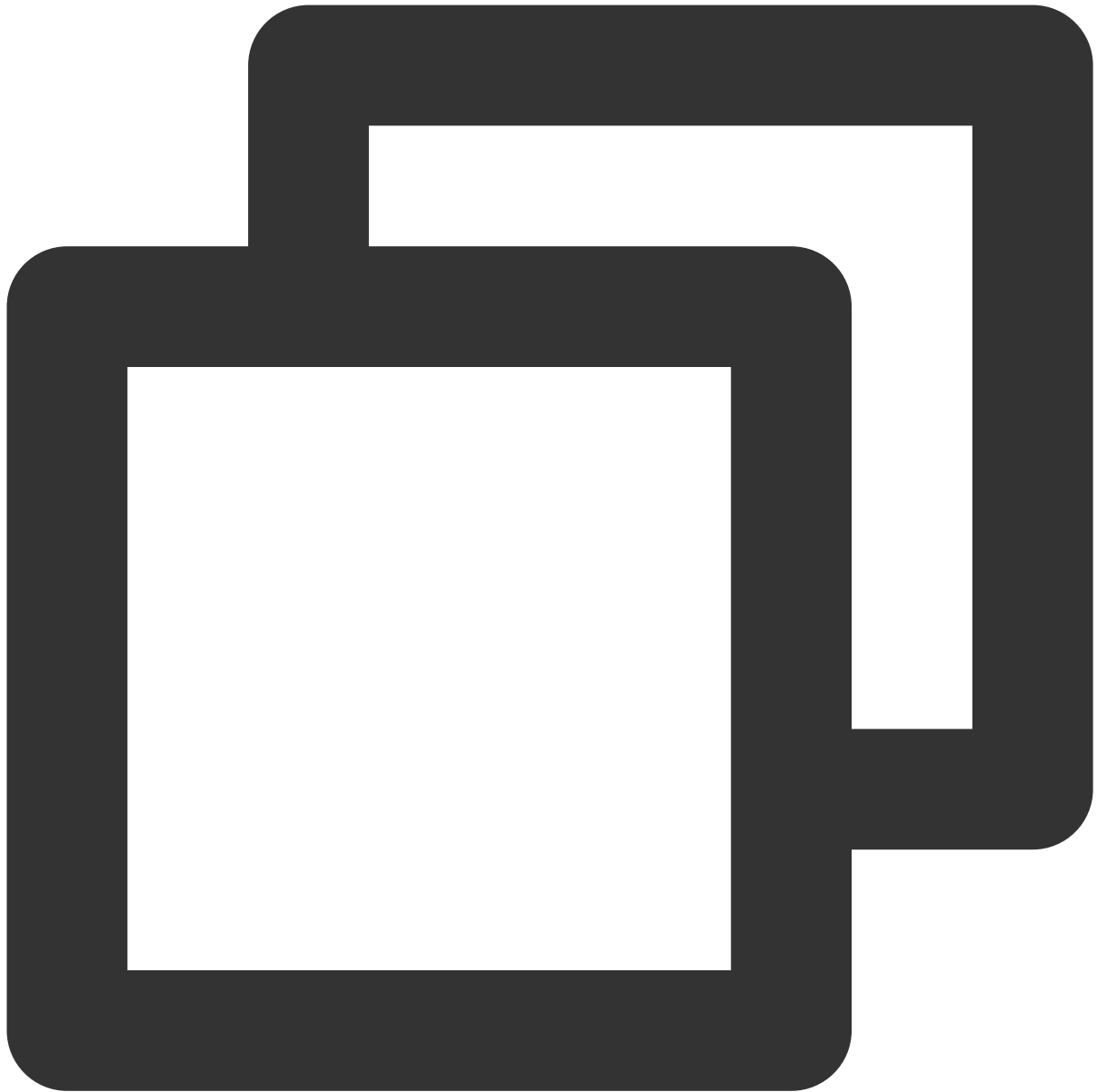
해당 포트를 개방하지 않았다면 [보안 그룹 규칙 추가](#)를 참조하여 개방하시기 바랍니다.

작업 순서

NTPDate를 NTPD로 수동 전환

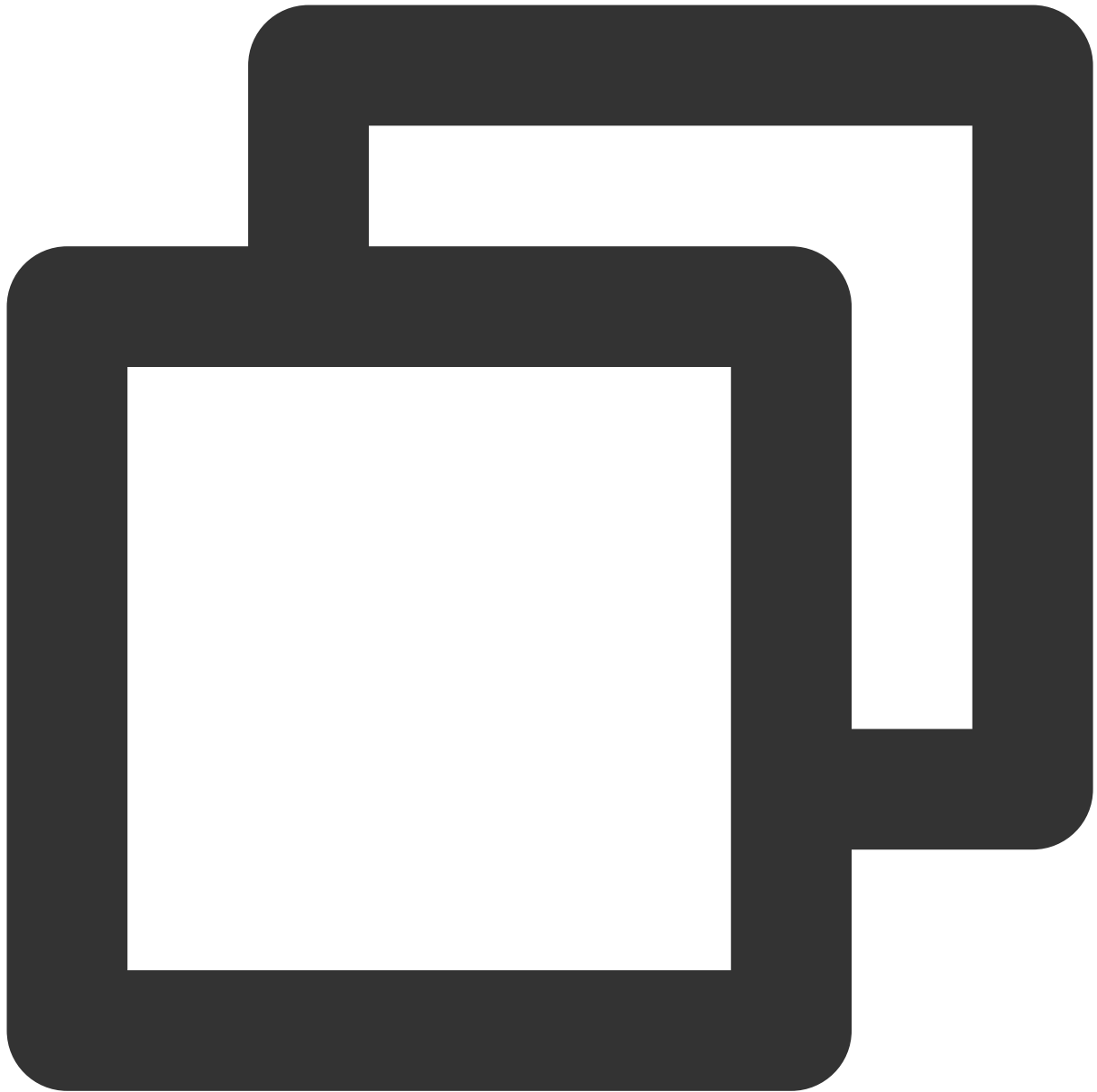
NTPDate 비활성화

1. 다음 명령어를 실행하여 crontab 설정을 내보낸 다음 NTPDate를 필터링합니다.



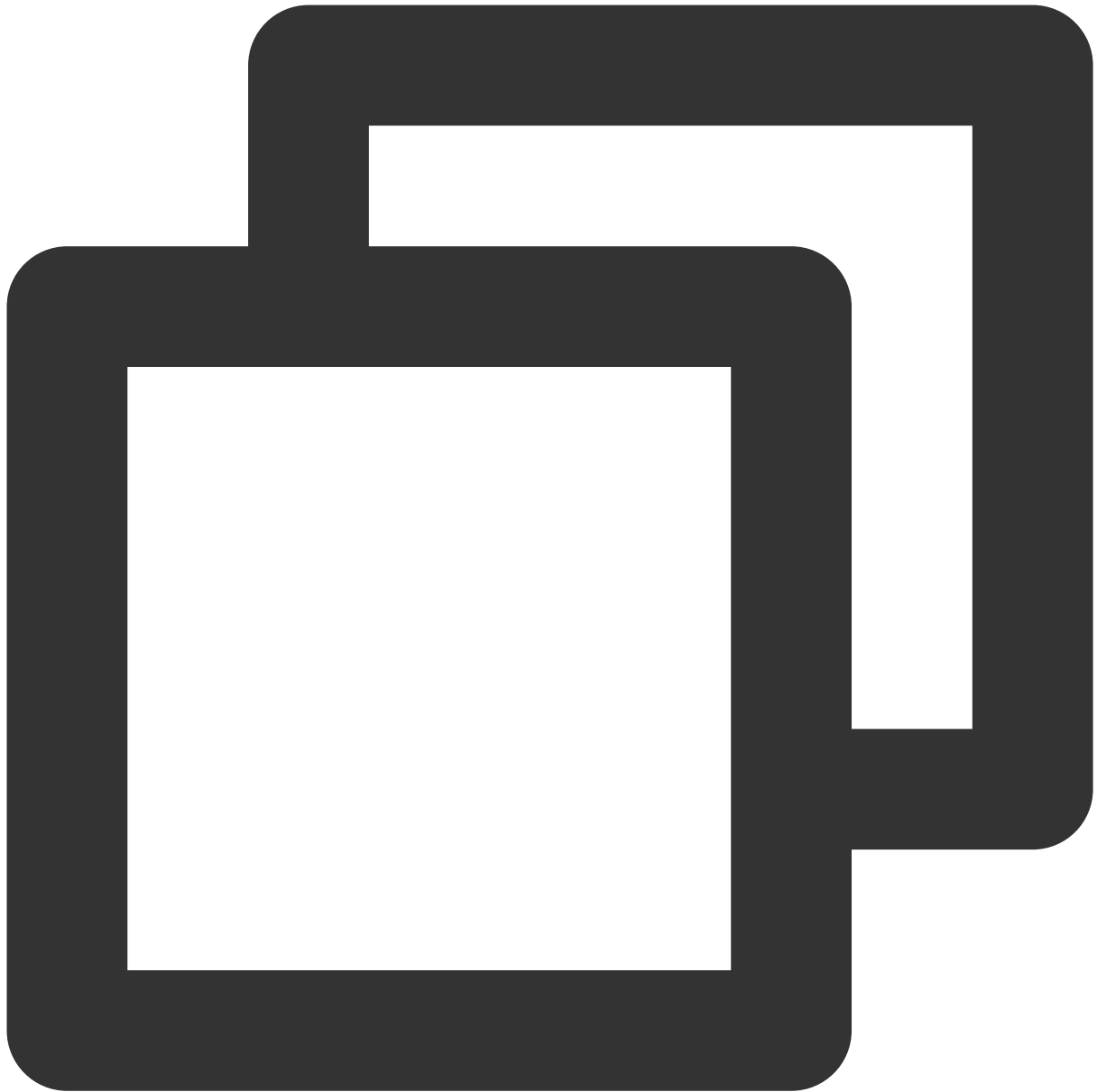
```
crontab -l |grep -v ntpupdate > /tmp/cronfile
```

2. 다음 명령어를 실행하여 NTPDate 설정을 업데이트합니다.



```
crontab /tmp/cronfile
```

3. 다음 명령어를 실행하여 `rc.local` 파일을 수정합니다.

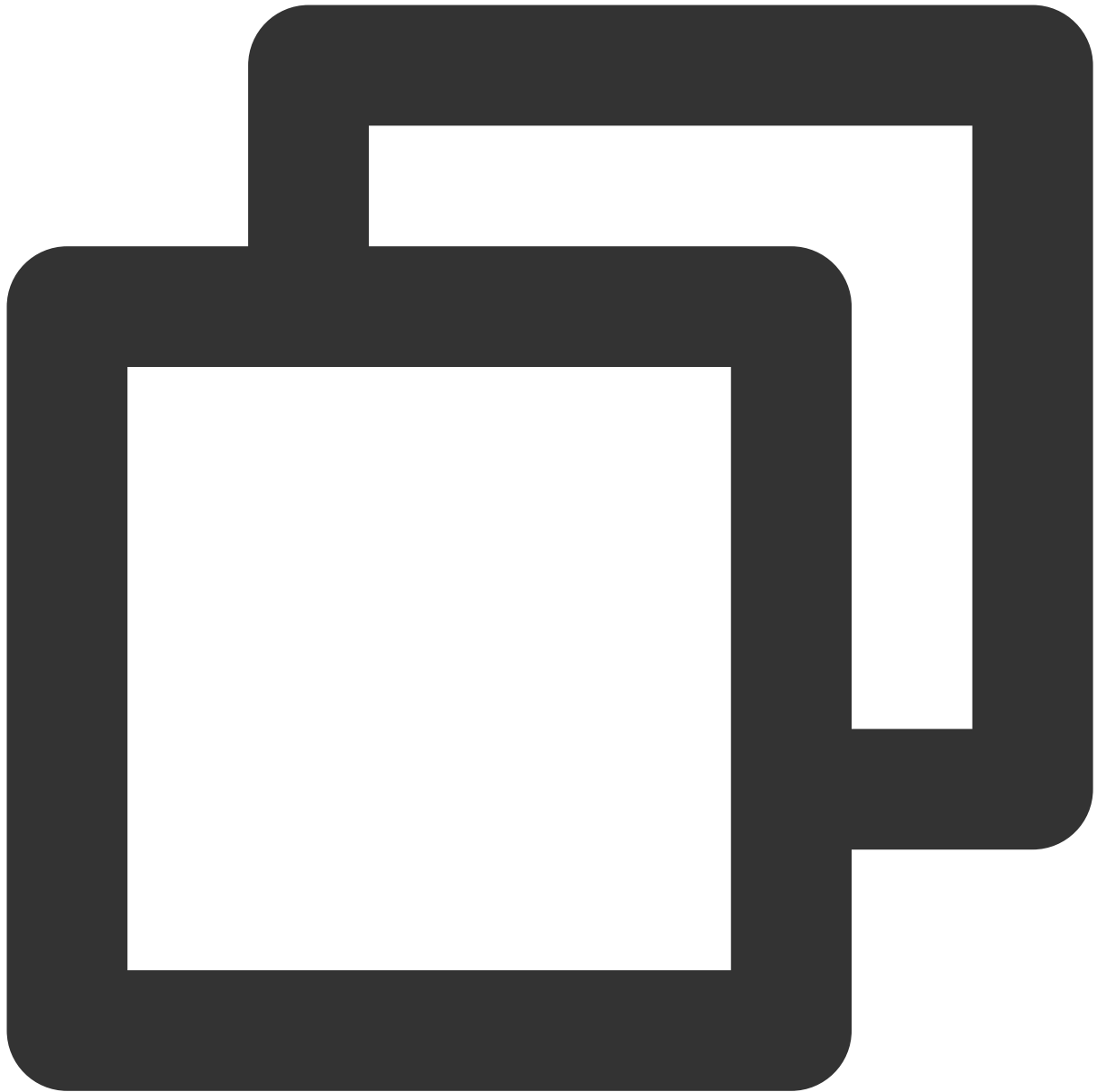


```
vim rc.local
```

4. **i**를 눌러 편집 모드로 바꾸고, `ntpupdate` 설정 행을 삭제합니다.
5. "**Esc**"를 누르고 "**:wq**"를 입력하여 파일을 저장한 후 돌아갑니다.

NTPD 설정

1. 다음 명령어를 실행하여 NTP 서비스 구성 파일을 엽니다.



```
vi /etc/ntp.conf
```

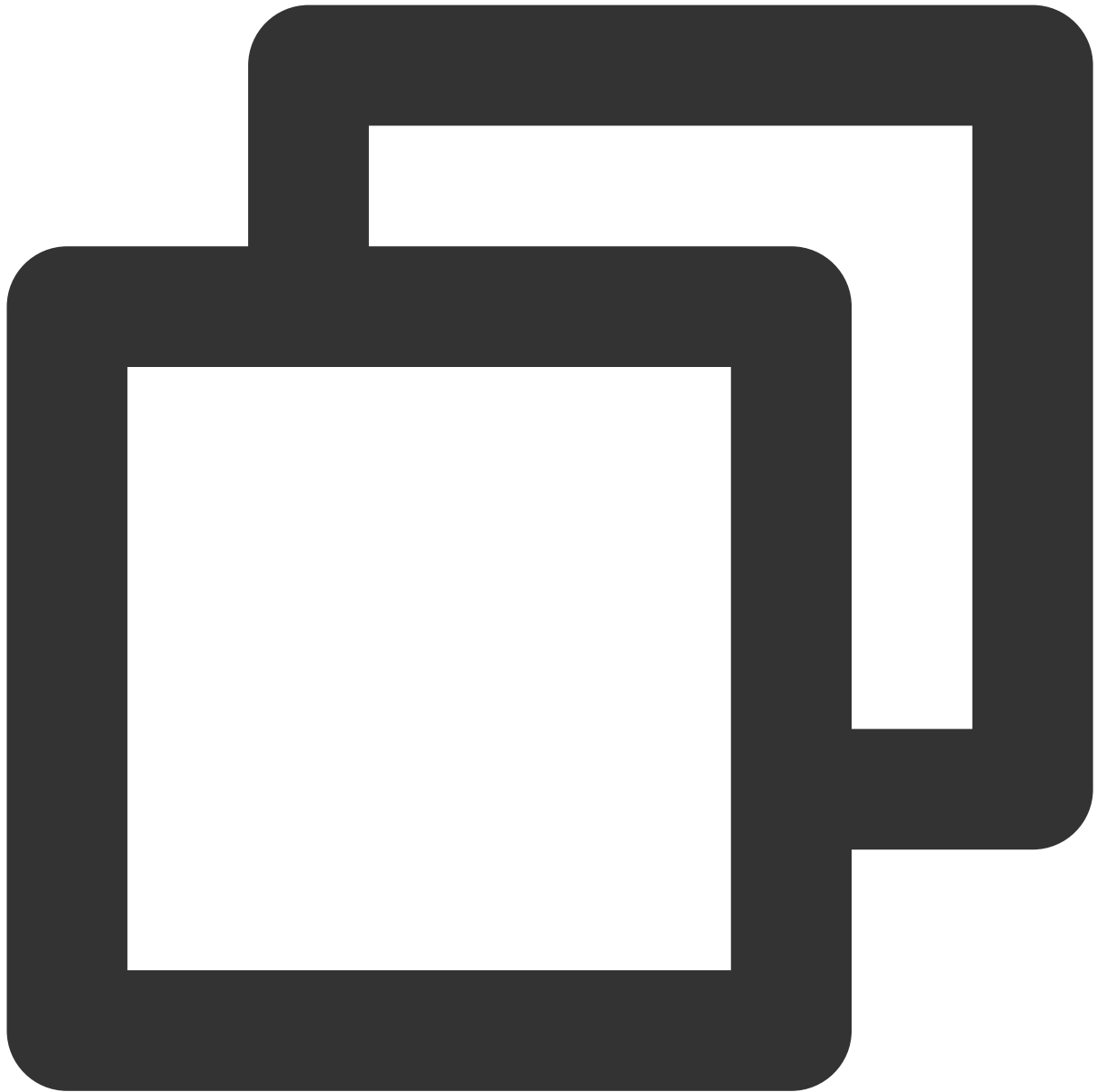
2. 아래 이미지와 같이 **i**를 눌러 편집 모드로 바꾸고, **server** 관련 설정을 찾아 설정하고자 하는 타깃 **NTP**의 시계 원본 서버(예: `time1.tencentyun.com`)로 **server**를 수정한 다음, 불필요한 **NTP** 시계 원본 서버를 삭제합니다.

```
# Use public servers from the pool.ntp.org project.  
# Please consider joining the pool (http://www.pool.ntp.org/join.html).  
server 0.centos.pool.ntp.org iburst  
server 1.centos.pool.ntp.org iburst  
server 2.centos.pool.ntp.org iburst  
server 3.centos.pool.ntp.org iburst
```

3. **Esc**를 누르고 **:wq**를 입력하여 파일을 저장한 뒤 리턴합니다.

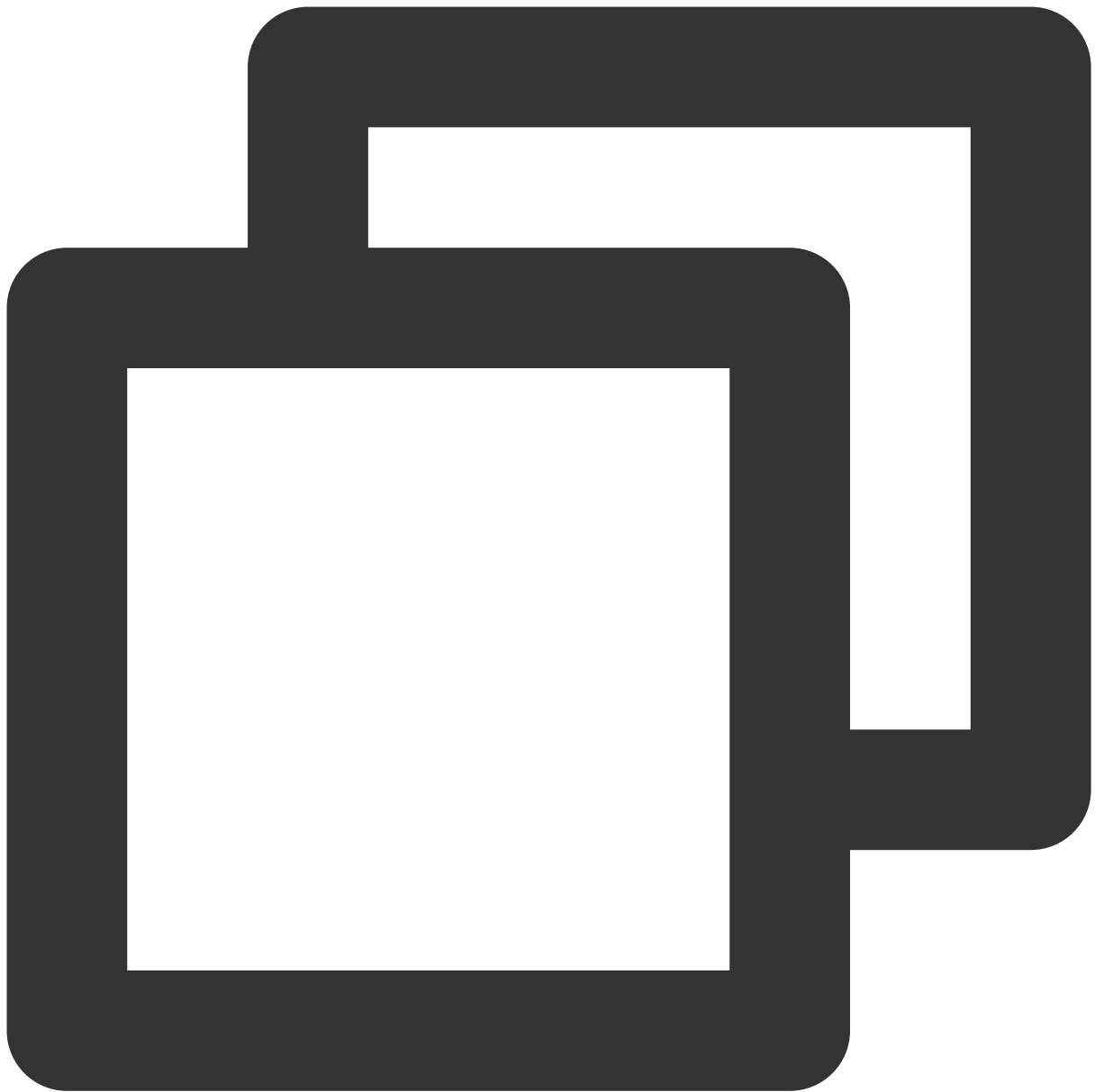
Linux 인스턴스: NTPDate를 NTPD로 자동 전환

1. `ntpd_enable.sh` 스크립트를 다운로드 합니다.



```
wget https://image-10023284.cos.ap-shanghai.myqcloud.com/ntpd_enable.sh
```

2. 다음 명령어를 실행하여 `ntpd_enable.sh` 스크립트로 NTPDate를 NTPD로 전환합니다.



```
sh ntpd_enable.sh
```

Windows 인스턴스에서 NTP 서비스 설정

최종 업데이트 날짜: : 2024-02-02 10:56:29

작업 시나리오

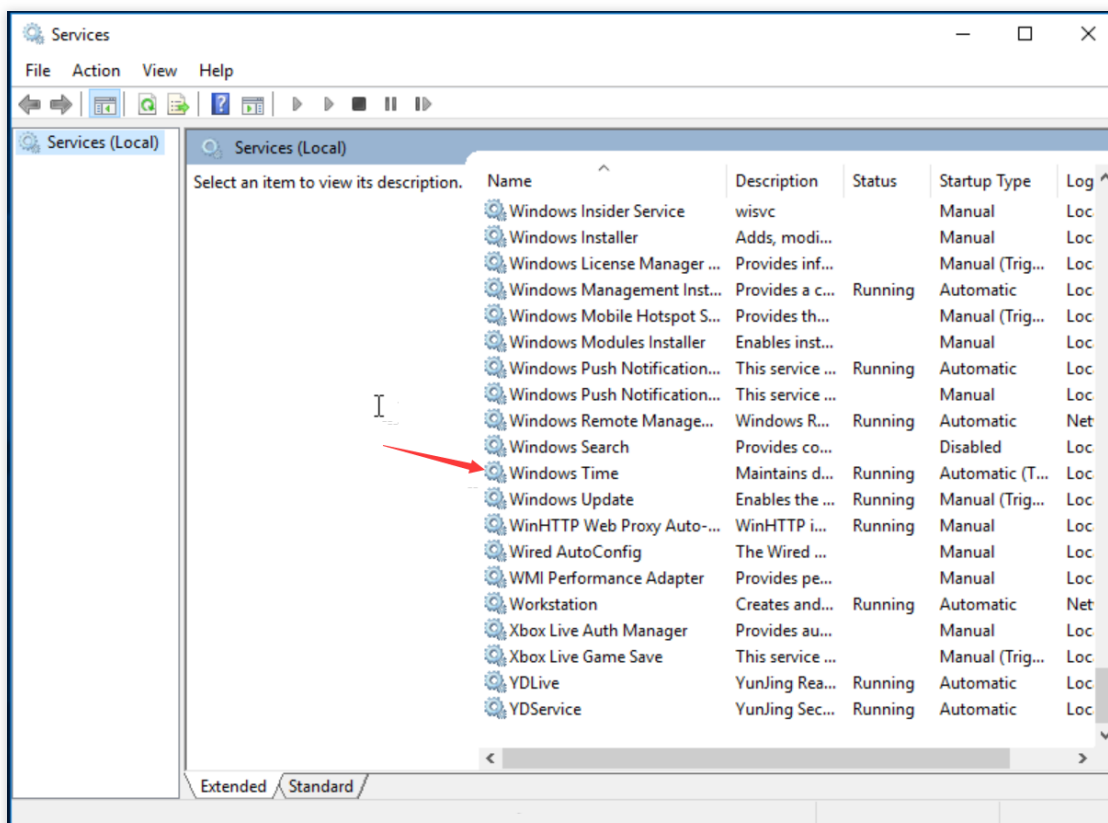
Windows 타임 서비스(Windows Time service, W32Time)는 로컬 시스템과 클럭 소스 서버 간의 시간 동기화에 사용됩니다. 네트워크 타임 프로토콜(NTP)을 사용하여 네트워크상의 컴퓨터 시계를 동기화합니다. 본 문서는 Windows Server 2012 운영 체제의 CVM을 예로 NTP 서비스 실행 및 클럭 소스 서버 주소 수정 방법에 대해 설명합니다.

작업 순서

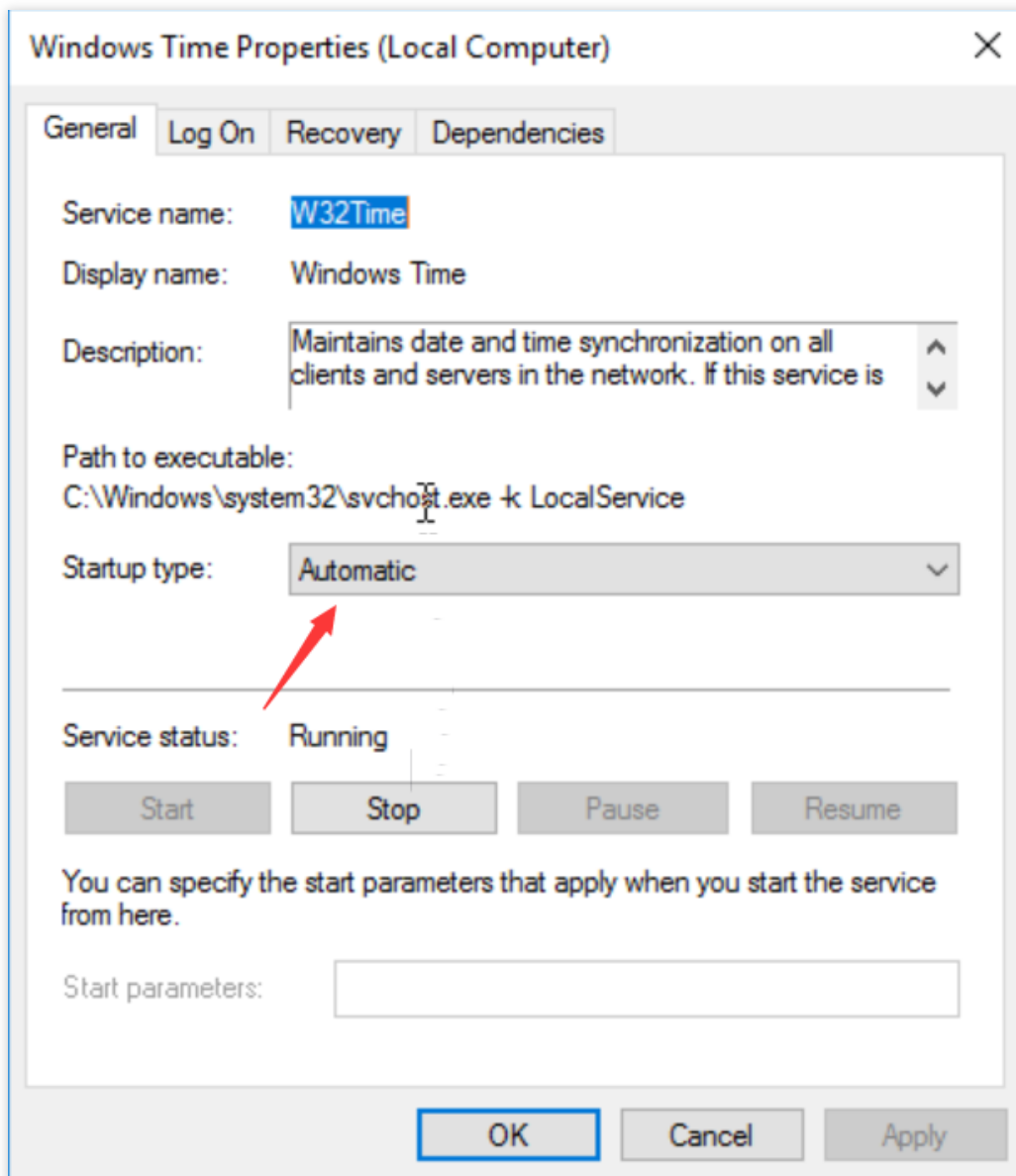
1. Windows CVM에 로그인합니다.
2. 시작에서

> [관리 도구]>[서비스]를 클릭하여 서비스 창을 엽니다.

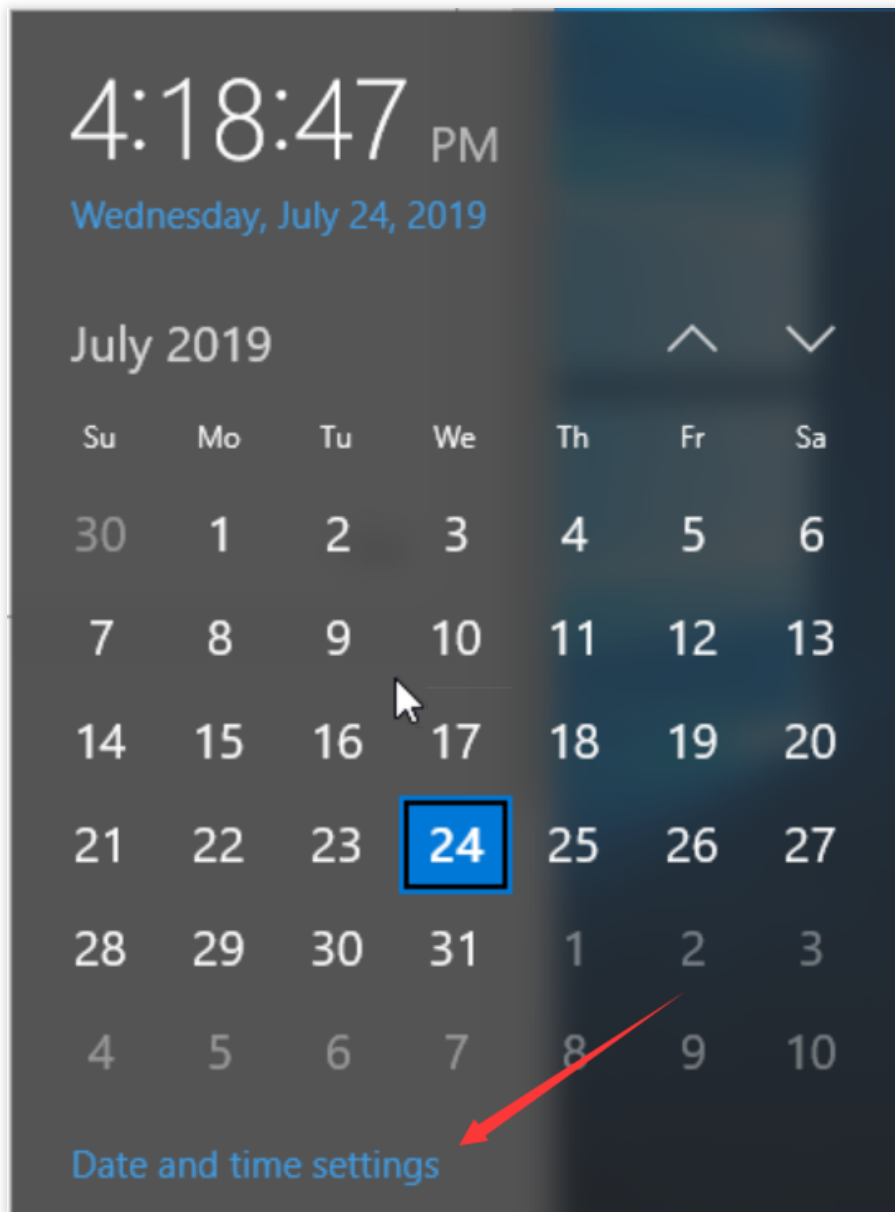
3. 아래 이미지와 같이 "서비스" 창에서 [Windows Time]을 더블 클릭하여 창을 엽니다.



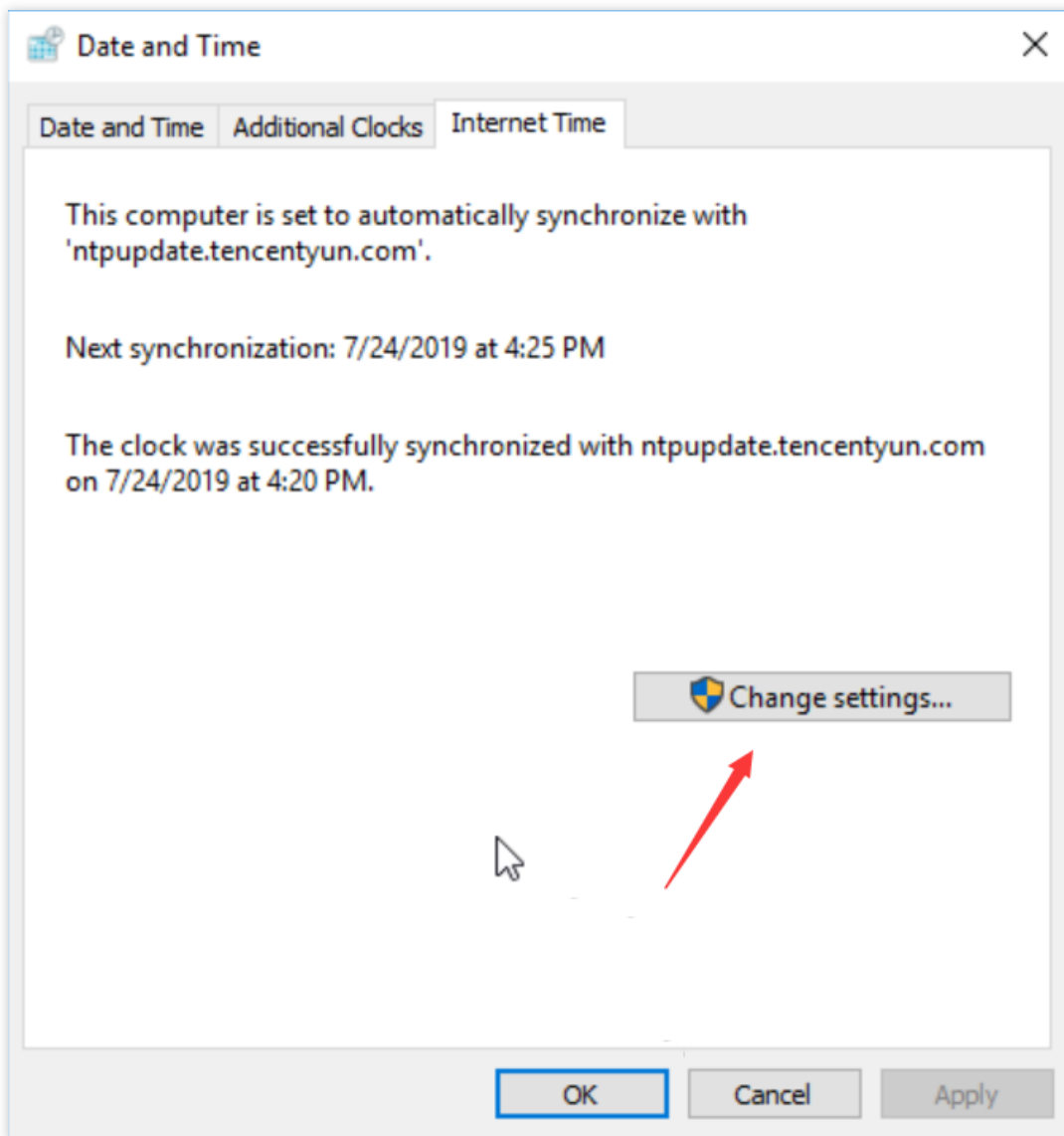
4. 아래 이미지와 같이 열린 "Windows Time 속성(로컬 컴퓨터)" 창에서 [시작 유형]을 [자동]으로 설정하고, [서비스 상태]를 [시작]으로 설정한 다음 [확인]을 누릅니다.



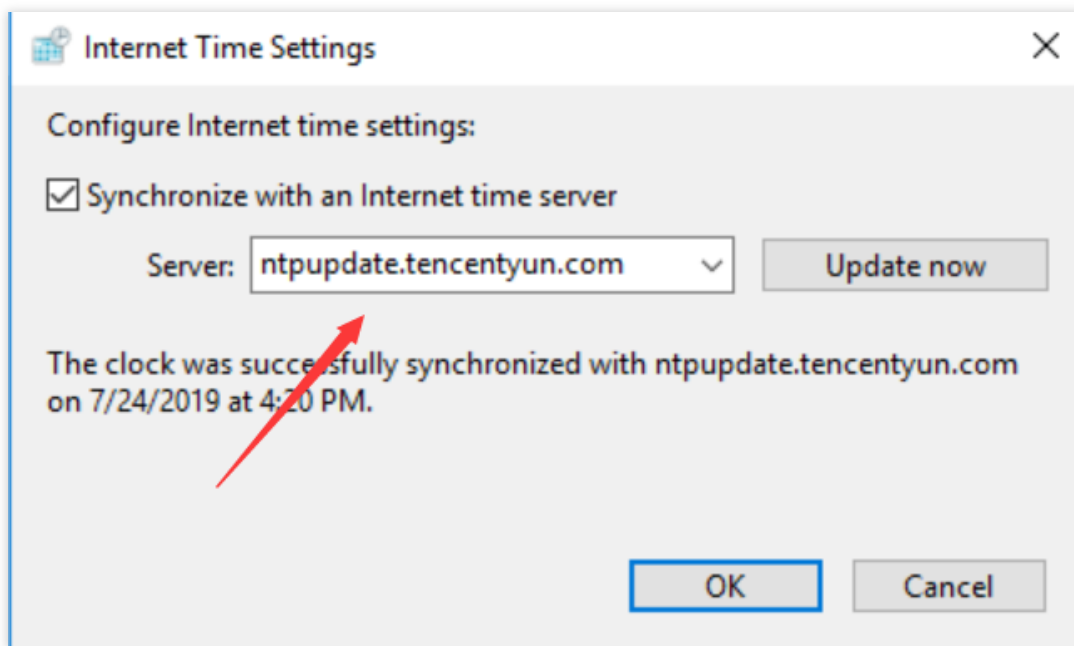
5. 아래 이미지와 같이 운영 체제 인터페이스 작업 표시란에서, 우측 하단의 시간 >[날짜 및 시간 설정]을 클릭합니다.



6. 아래 이미지와 같이 팝업된 “날짜 및 시간” 창에서 [인터넷 시간] 탭을 선택하고 [설정 변경]을 클릭합니다.



7. 아래 이미지와 같이 팝업된 "인터넷 시간 설정" 창에서 [서버]를 타깃 클럭 소스 서버의 도메인 또는 IP 주소로 설정하고, [확인]을 눌러 설정을 완료합니다.



PostgreSQL 프라이머리/세컨더리 아키텍처 구축

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

PostgreSQL은 확장성과 표준 준수에 중점을 둔 오픈 소스 관계형 데이터베이스 관리 시스템입니다. PostgreSQL은 엔터프라이즈 수준의 복잡한 온라인 트랜잭션 처리(OLTP) 시스템에 이상적입니다. NoSQL(JSON/XML/hstore) 및 지리 정보 시스템(GIS, Geographic Information System 또는 Geo-Information system) 데이터 유형을 지원합니다. 강력한 안정성과 데이터 무결성을 특징으로 하는 PostgreSQL은 웹사이트, 위치 애플리케이션 시스템, 복잡한 데이터 객체 처리 및 기타 사용 사례에 적합합니다.

본 문서는 CentOS 7을 실행하는 CVM 인스턴스에서 PostgreSQL 시스템을 구축하는 방법을 설명합니다.

소프트웨어

본 문서는 PostgreSQL을 구축하기 위해 다음 소프트웨어를 예로 사용합니다.

Linux: Linux 운영 체제의 경우, 본 문서는 CentOS 7.6을 예시로 사용합니다.

PostgreSQL: 관계형 데이터베이스 관리 시스템. 본 문서에서는 PostgreSQL 12을 예시로 사용합니다.

전제 조건

두 개의 CVM 인스턴스가 생성되어 있어야 합니다. 하나의 CVM 인스턴스는 기본 노드로 작동하고 다른 하나는 보조 노드로 작동합니다.

구체적인 단계는 [구매 페이지를 통한 인스턴스 생성](#)을 참고하십시오.

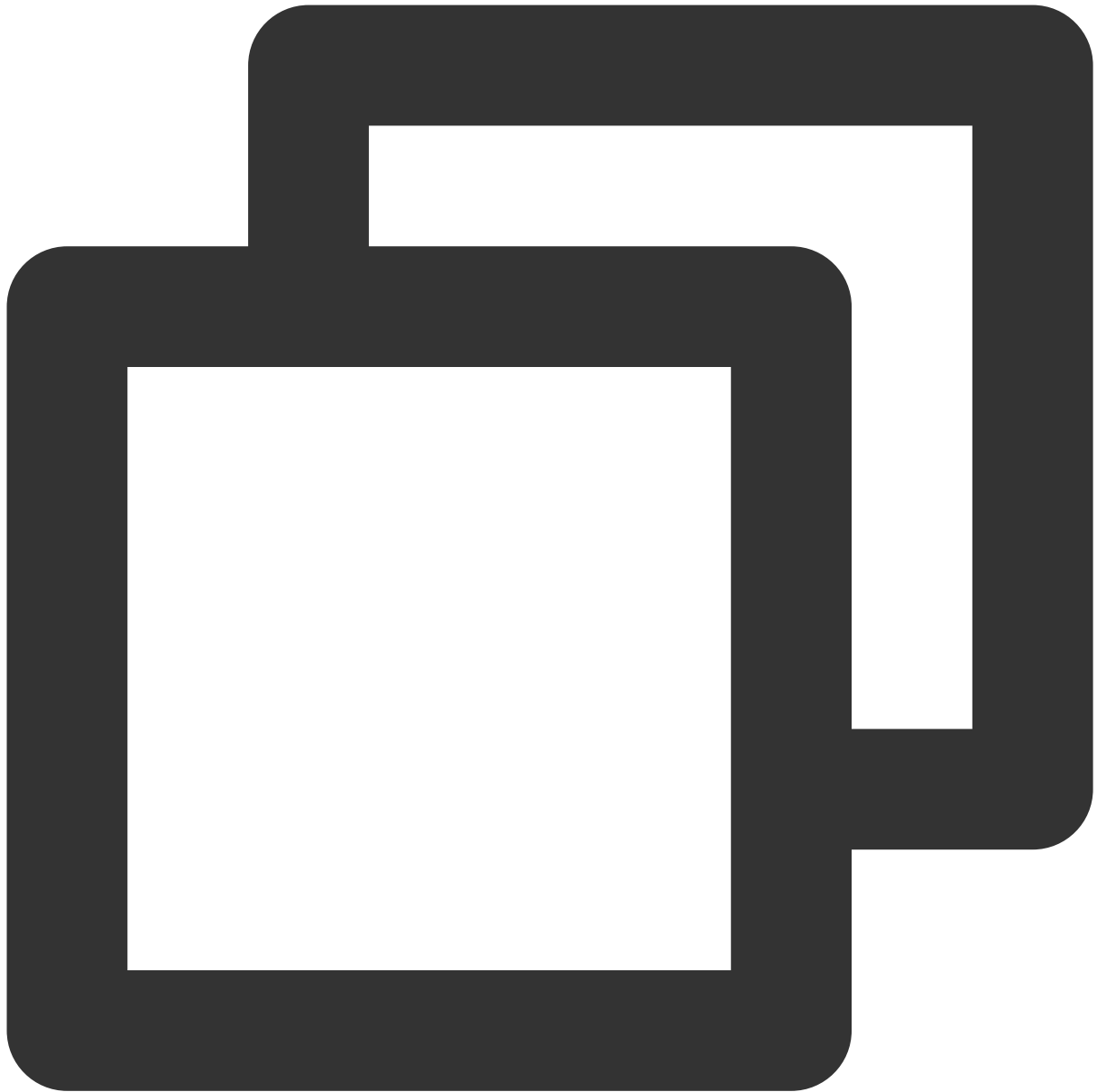
두 CVM 인스턴스에 보안 그룹 규칙(5432 포트 개방)이 설정되어있어야 합니다.

구체적인 단계는 [보안 그룹 규칙 추가](#)를 참고하십시오.

작업 단계

프라이머리 노드 설정

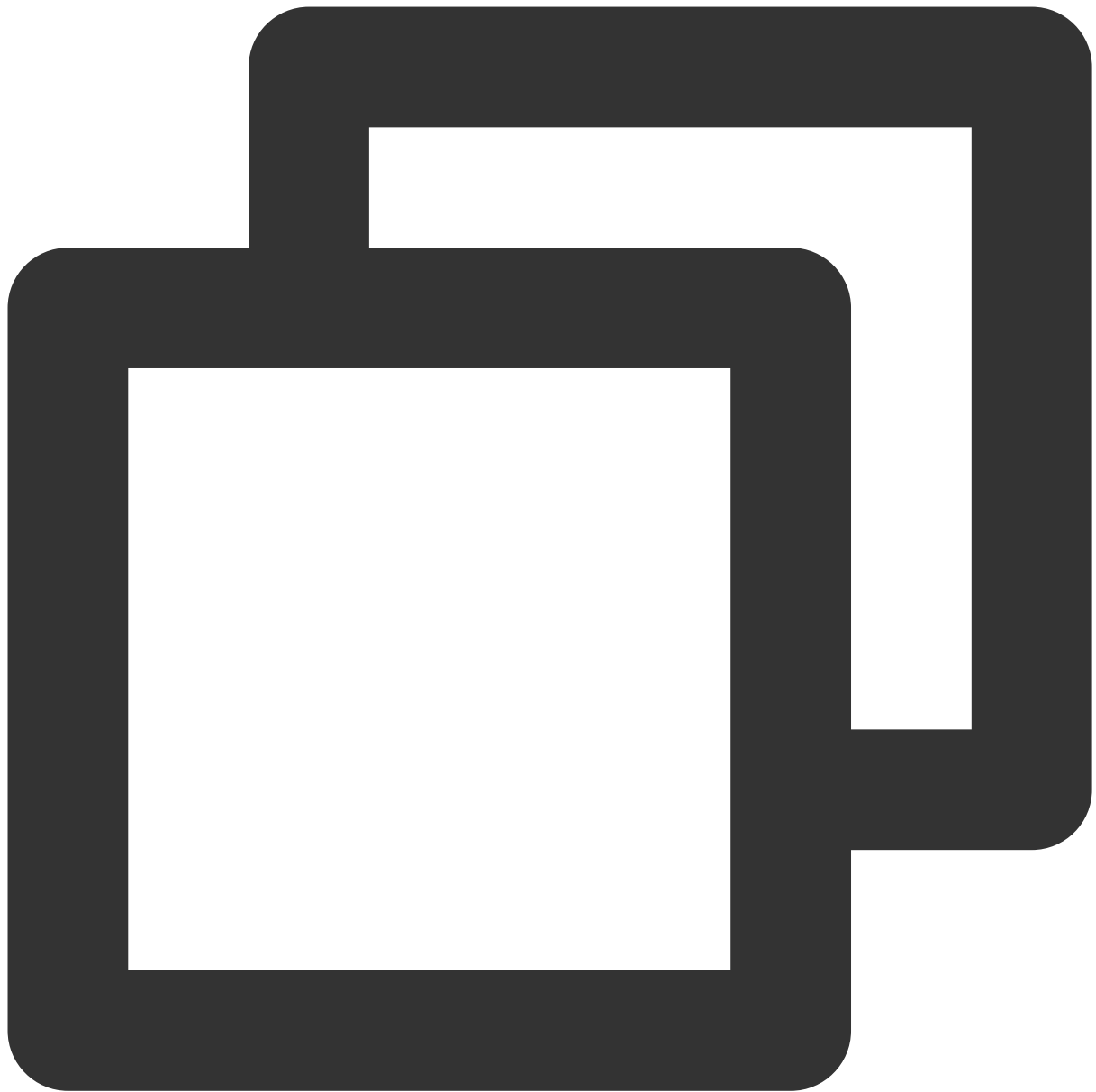
1. 프라이머리 노드 인스턴스에 로그인합니다.
2. 다음 명령을 실행하여 모든 패키지, 시스템 버전 및 커널을 업그레이드합니다.



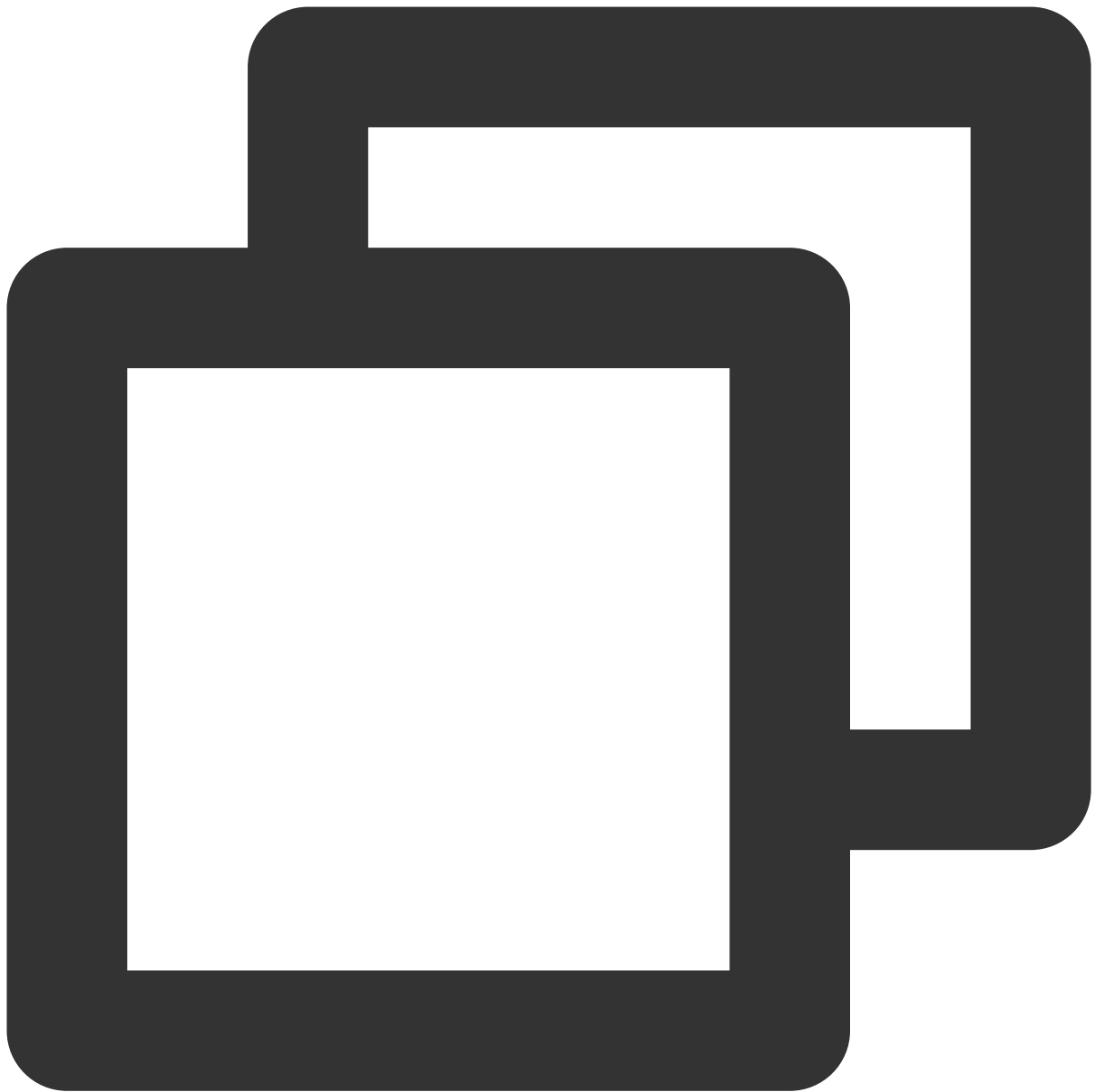
```
yum update -y
```

3. 다음 명령어를 순서대로 실행하여 PostgreSQL을 설치합니다.

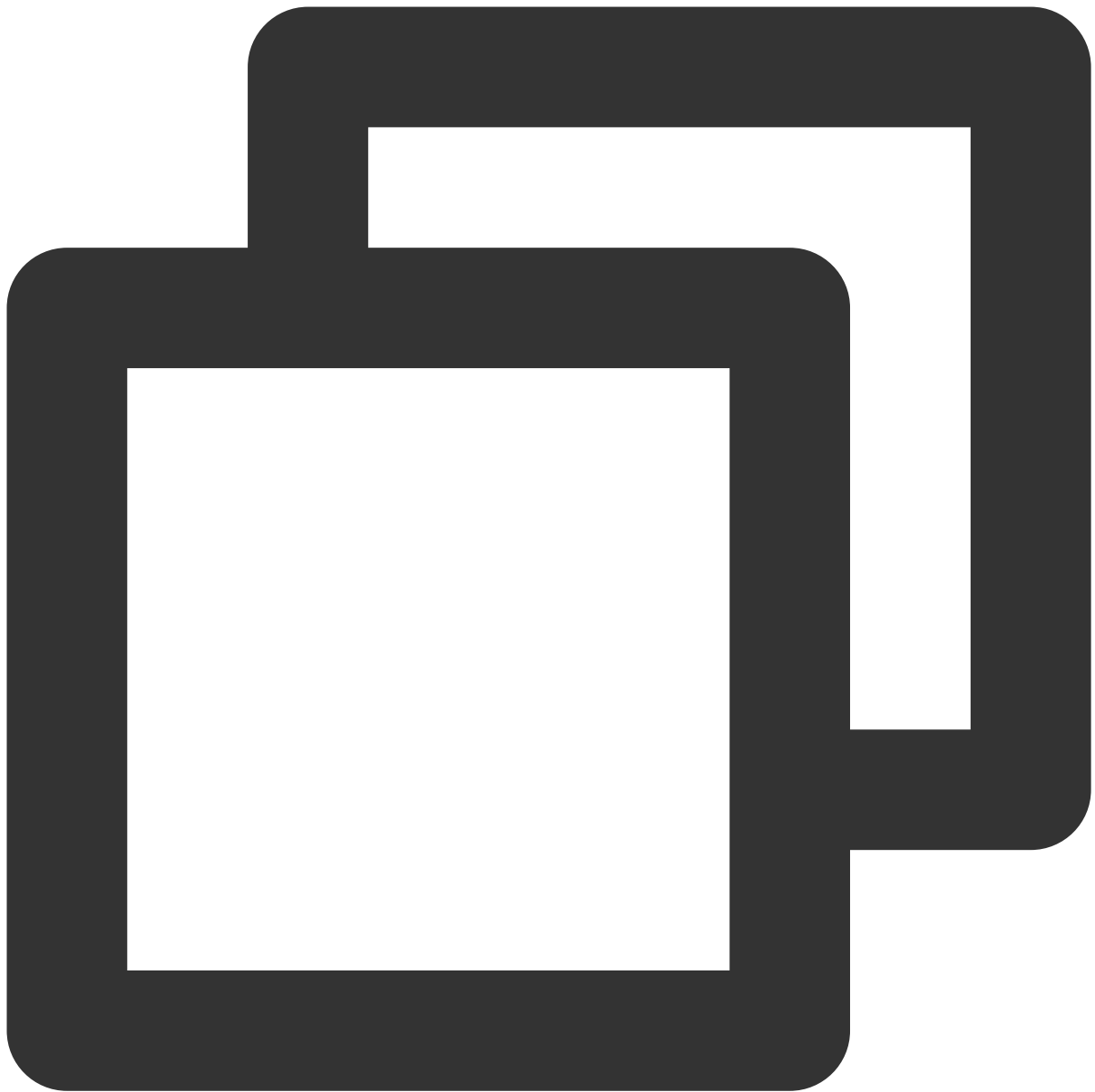
본 문서에서는 PostgreSQL 버전 12을 예시로 사용하며 필요에 따라 다른 버전을 선택할 수 있습니다.



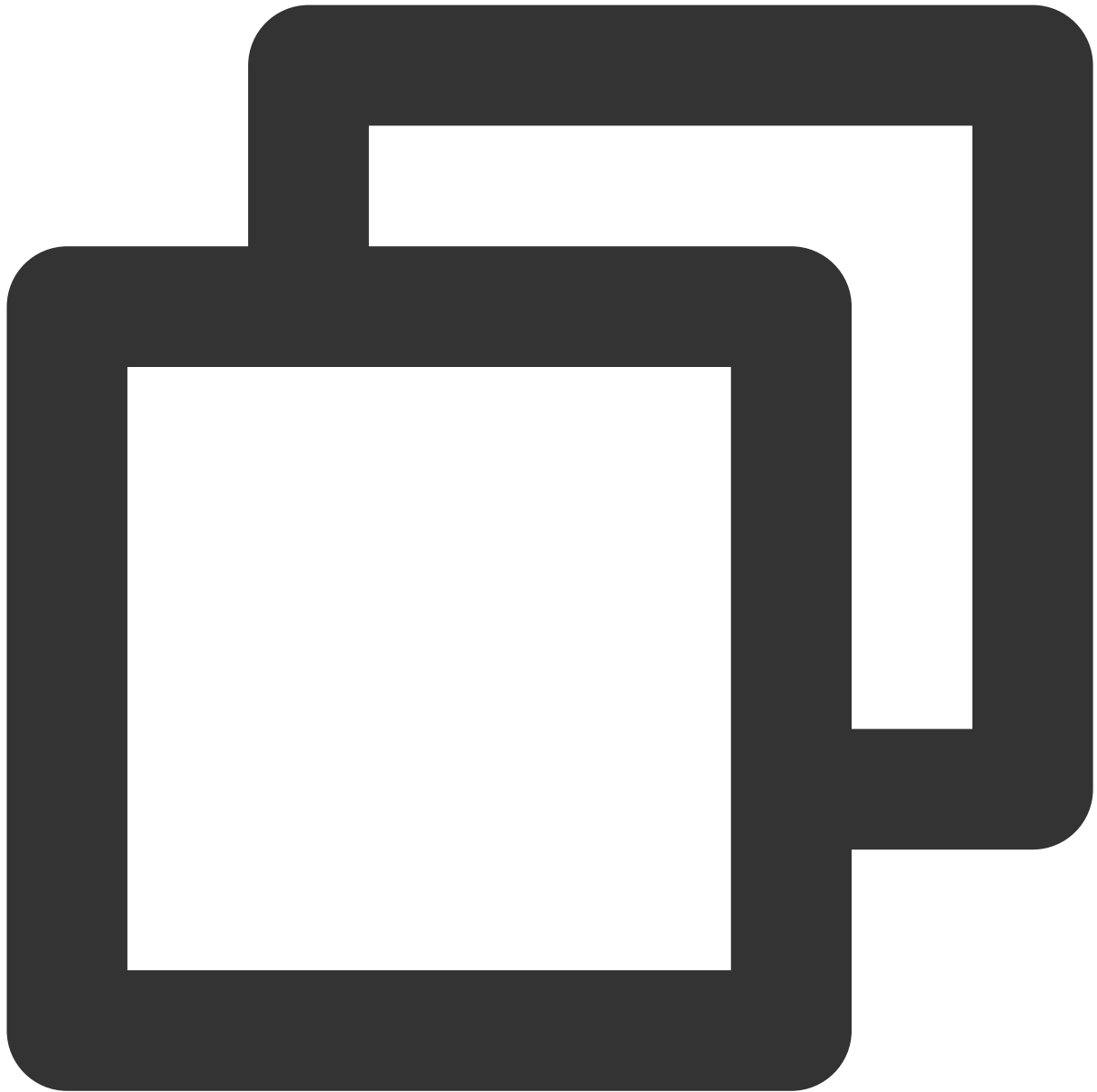
```
wget --no-check-certificate https://download.postgresql.org/pub/repos/yum/repорpms/
```



```
rpm -ivh pgdg-redhat-repo-latest.noarch.rpm
```

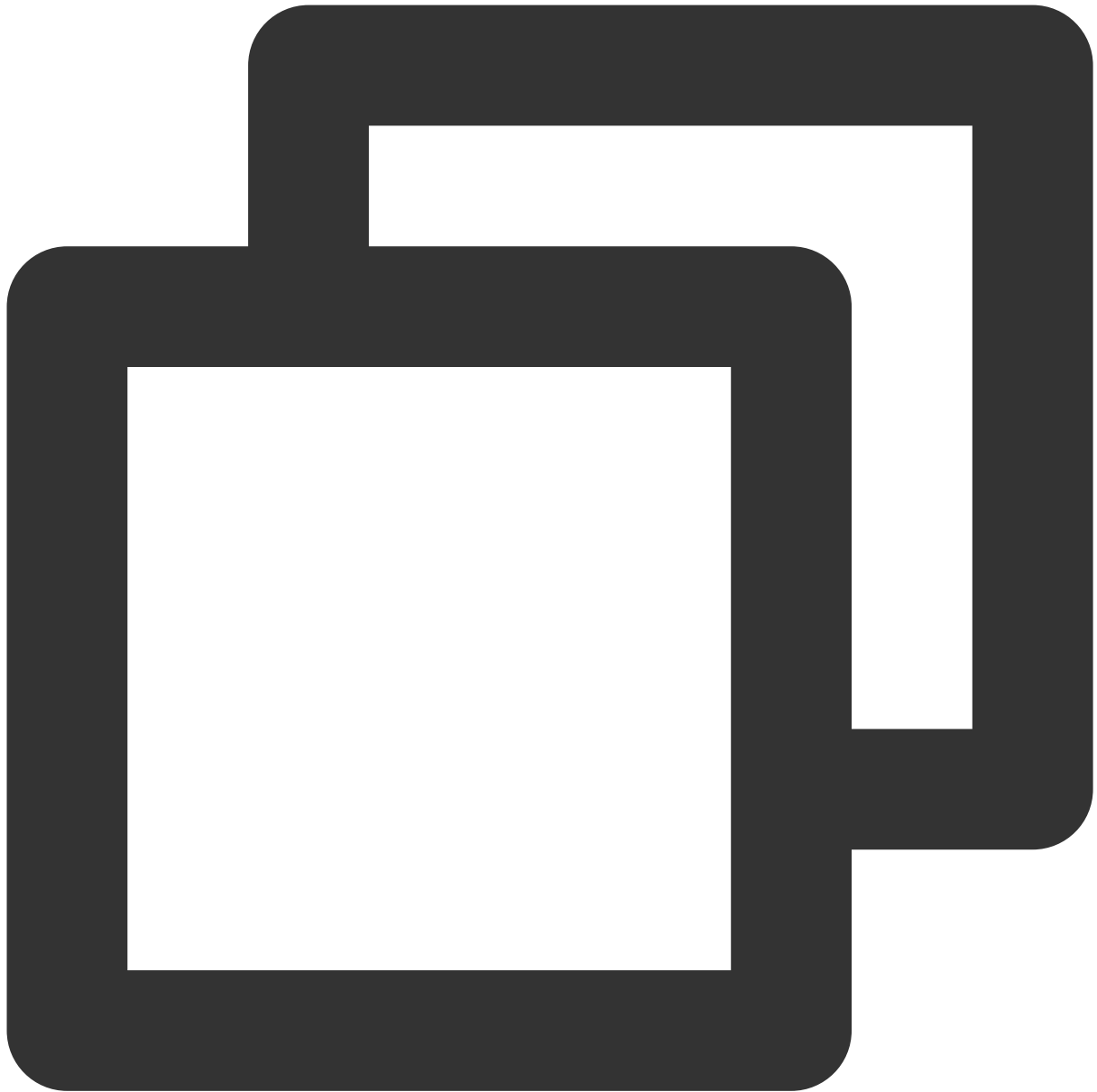



```
yum install postgresql12-server postgresql12-contrib -y
```



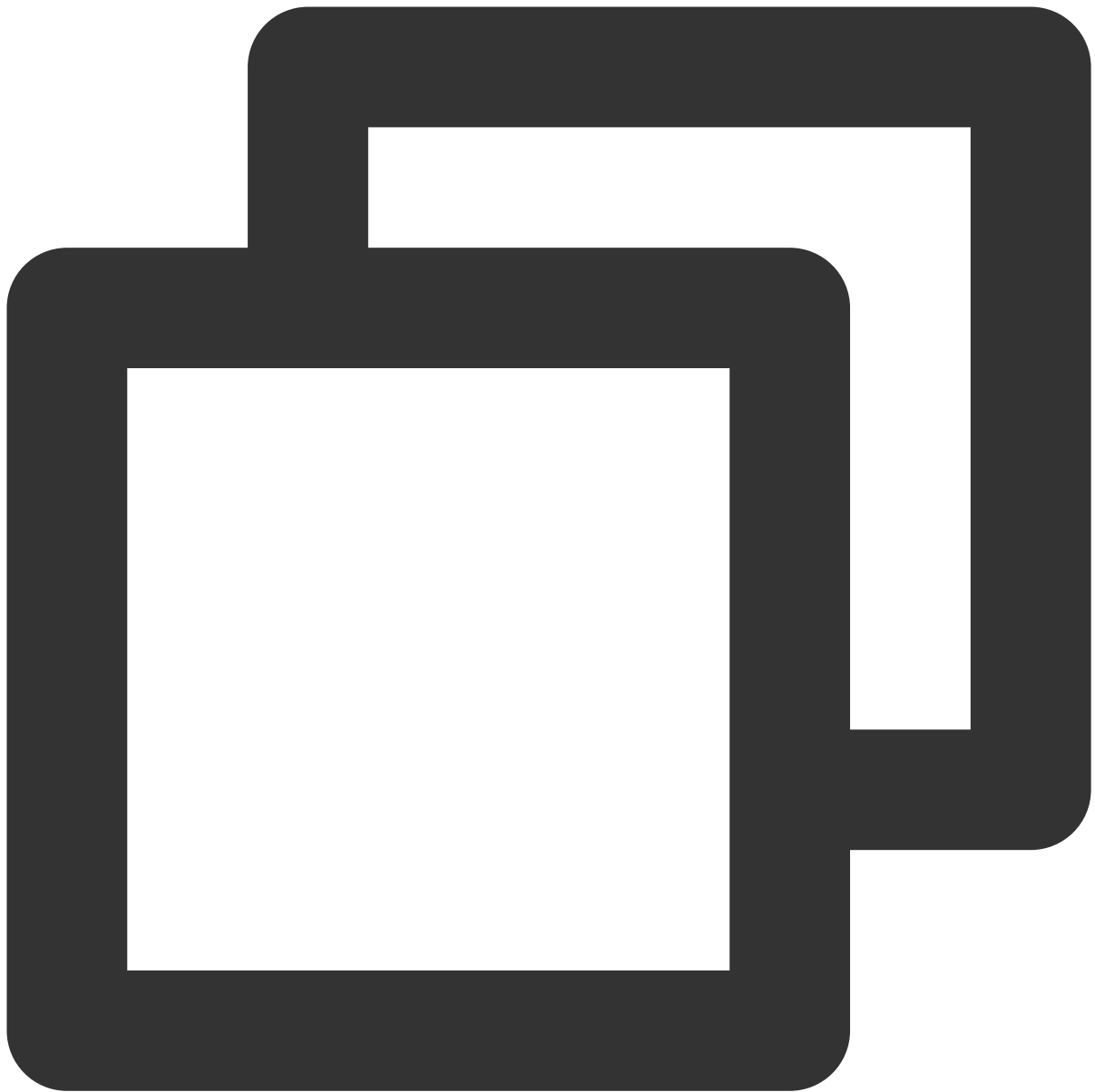
```
/usr/pgsql-12/bin/postgresql12-setup initdb
```

4. 아래의 명령어를 실행하여 서비스를 시작하십시오.



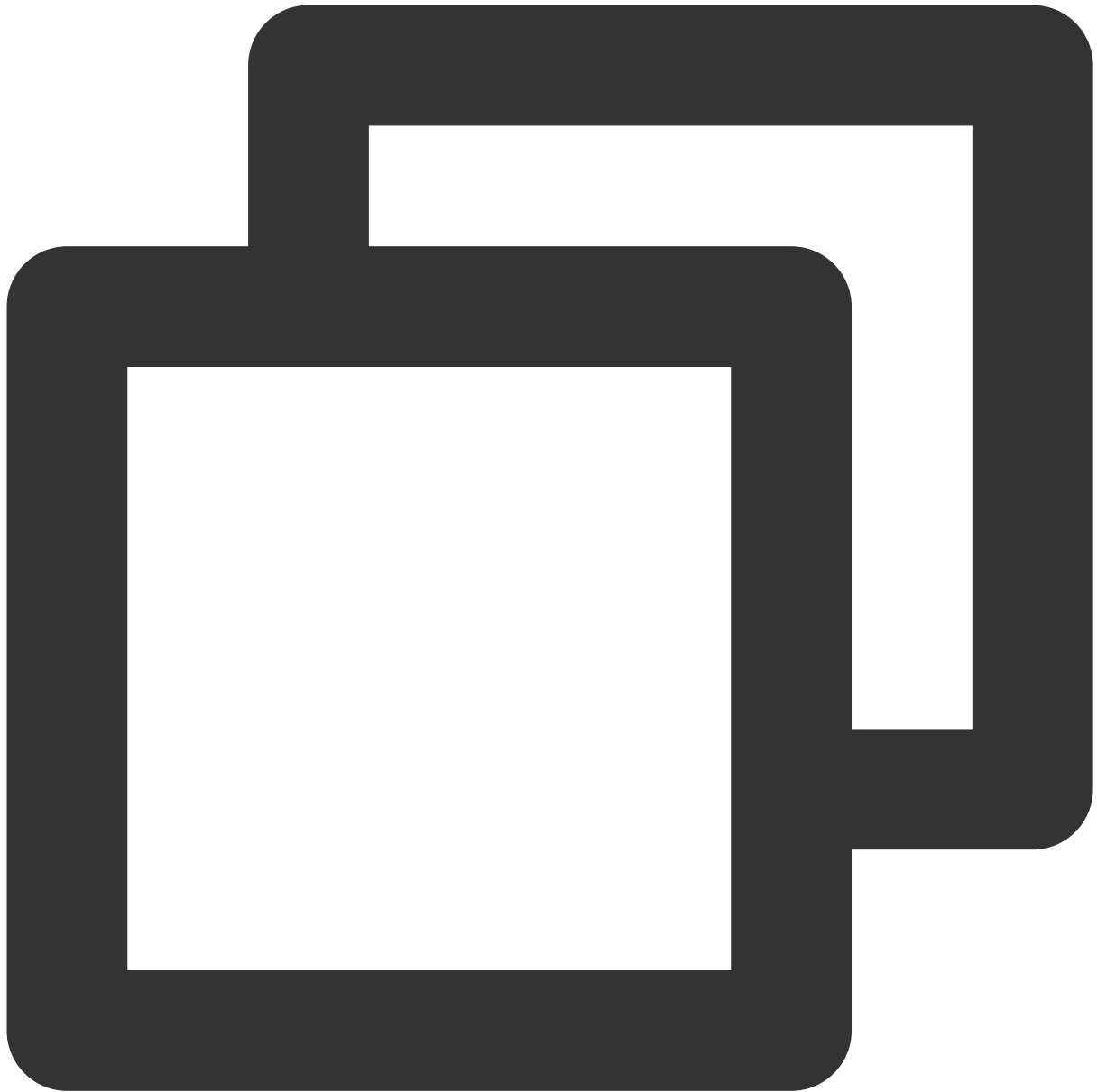
```
systemctl start postgresql-12.service
```

5. 다음 명령을 실행하여 시작 시 서비스가 자동으로 실행되도록 설정합니다.



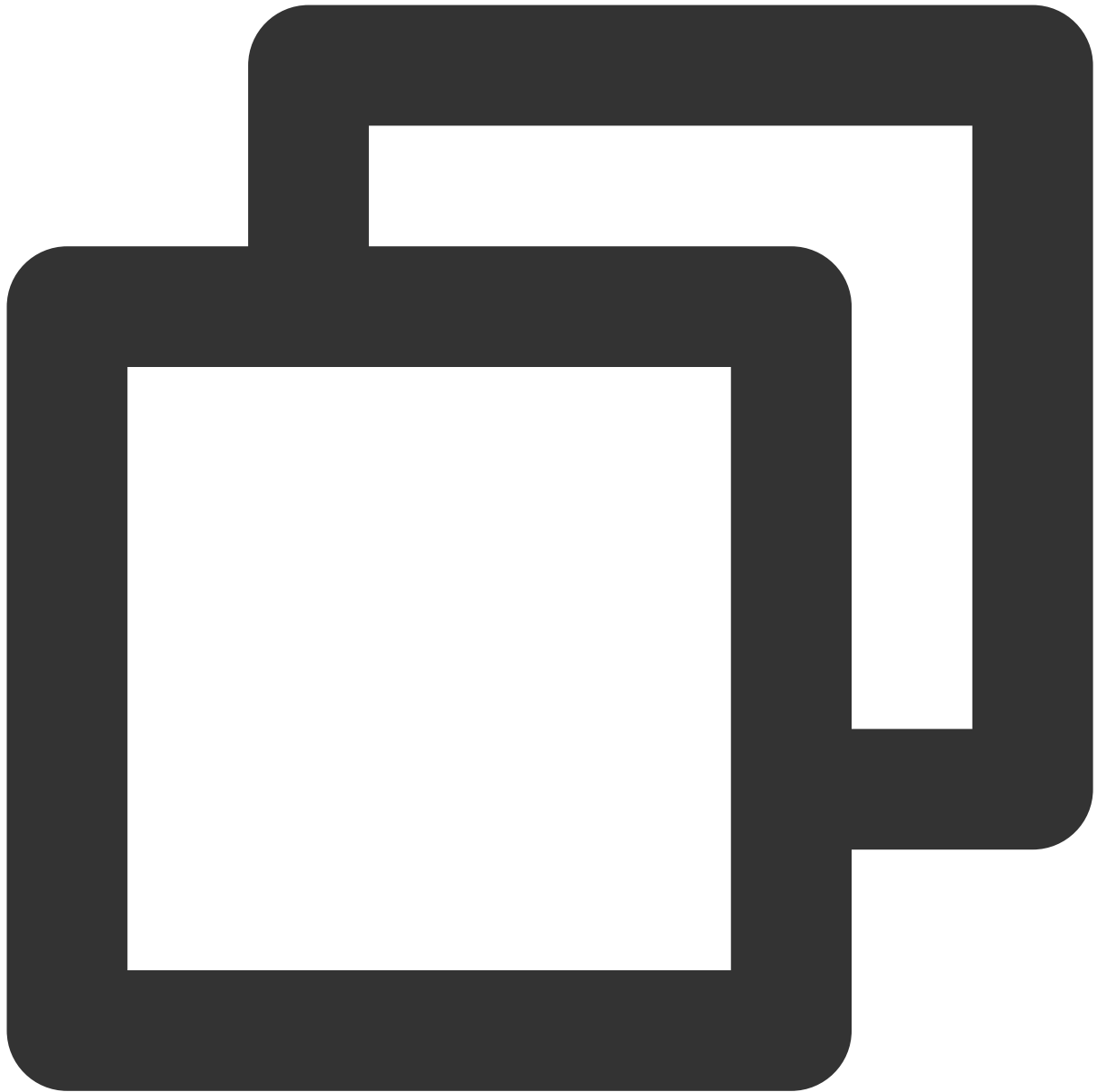
```
systemctl enable postgresql-12.service
```

6. 다음 명령을 실행하여 postgres 사용자로 로그인합니다.



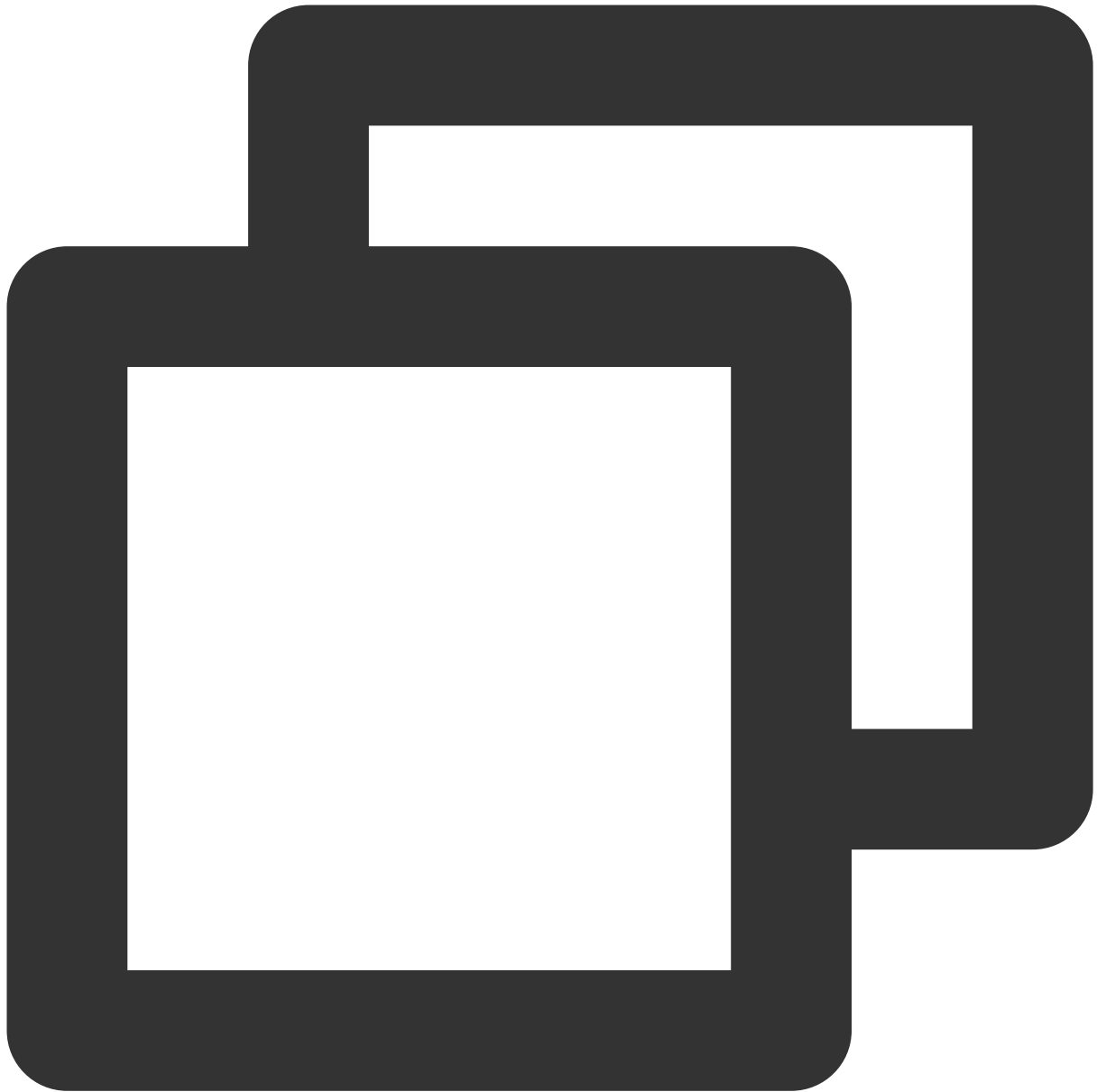
```
su - postgres
```

7. 다음 명령을 실행하여 PostgreSQL 인터랙티브 터미널로 이동합니다.



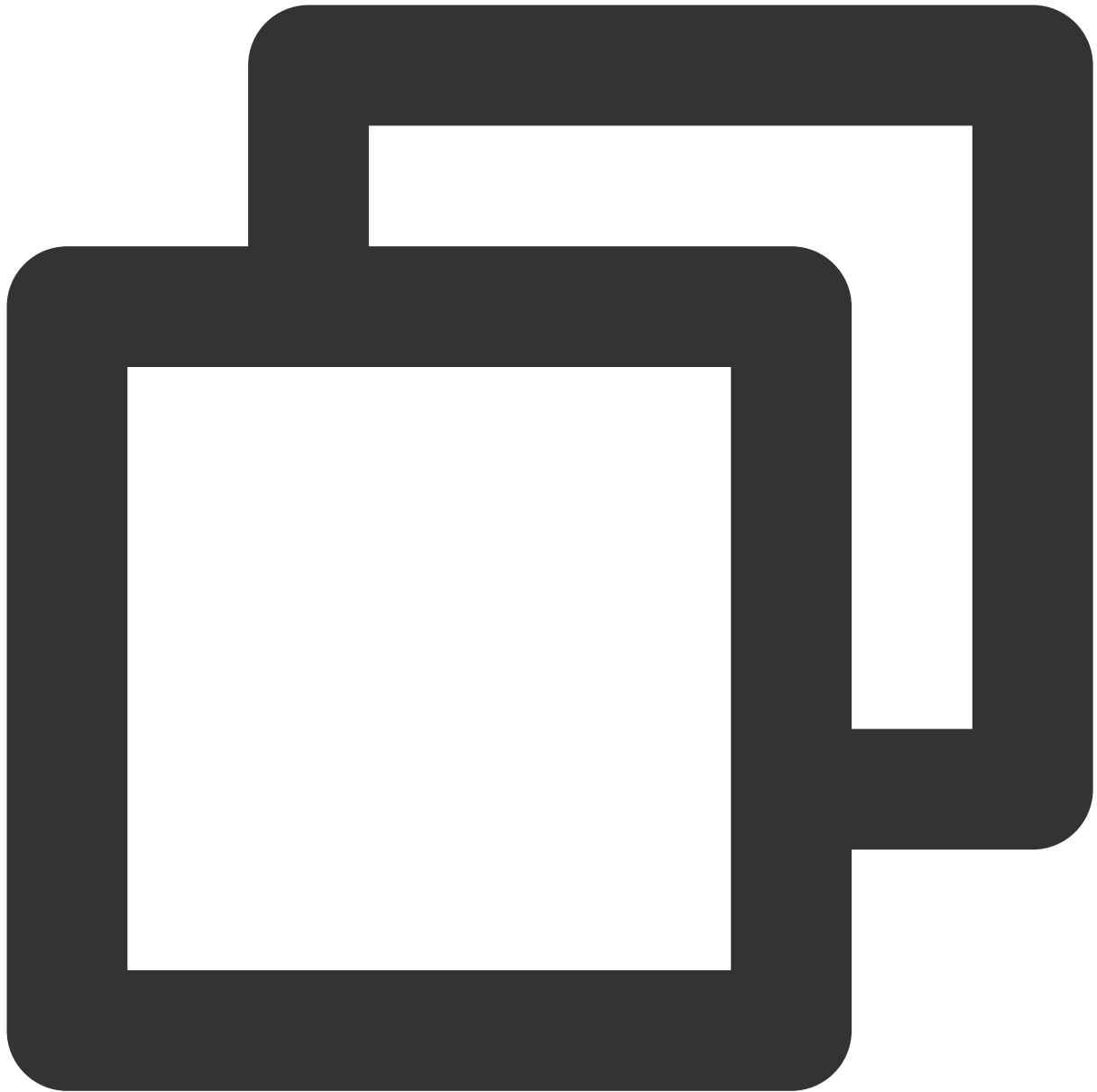
```
psql
```

8. 다음 명령을 실행하여 보안성 향상을 위해 사용자 `postgres`의 비밀번호를 설정합니다.



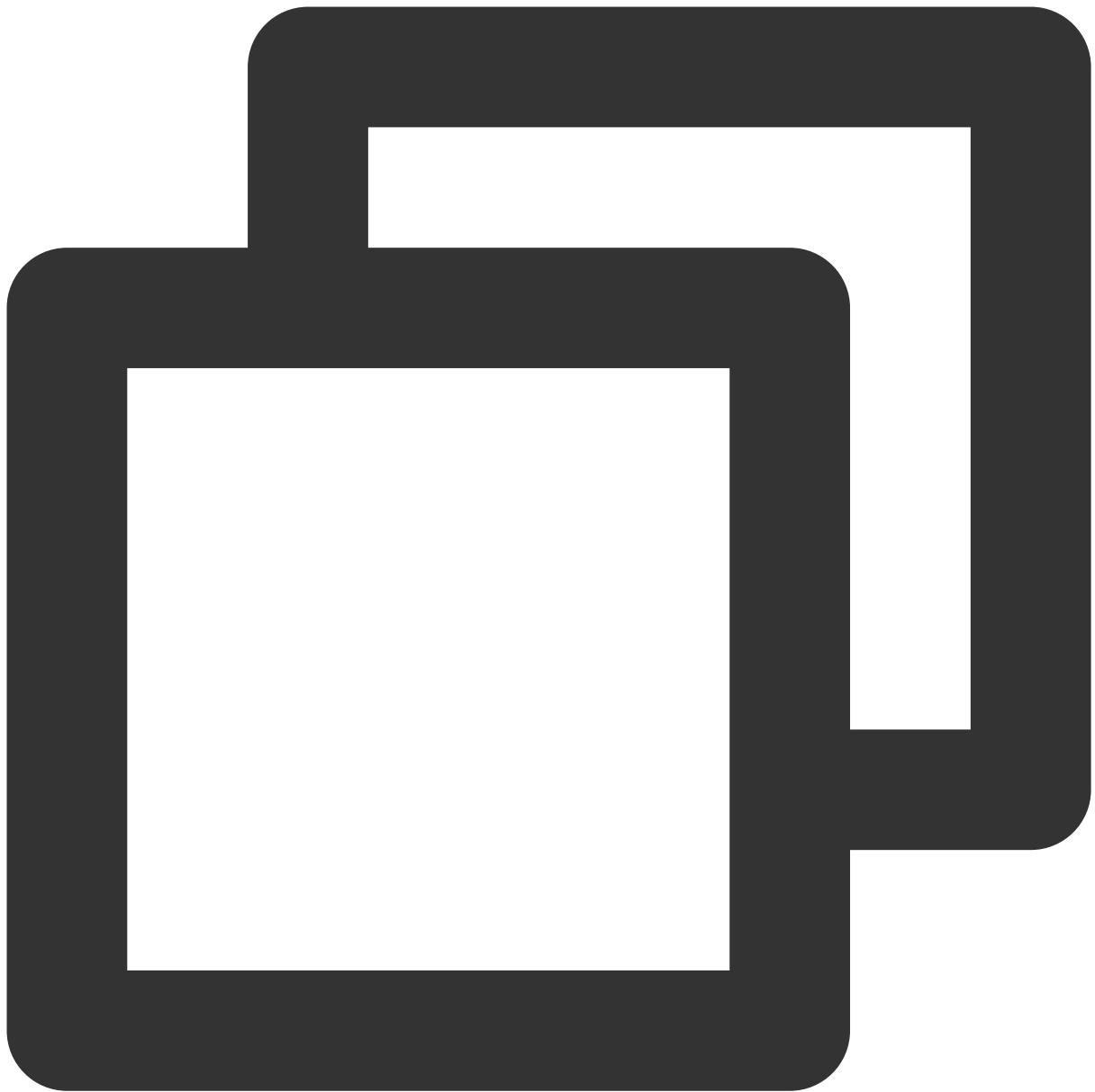
```
ALTER USER postgres WITH PASSWORD '사용자 정의 비밀번호';
```

9. 다음 명령어를 실행하여 데이터베이스 계정을 생성하고 비밀번호, 로그인 권한, 백업 권한을 설정합니다.



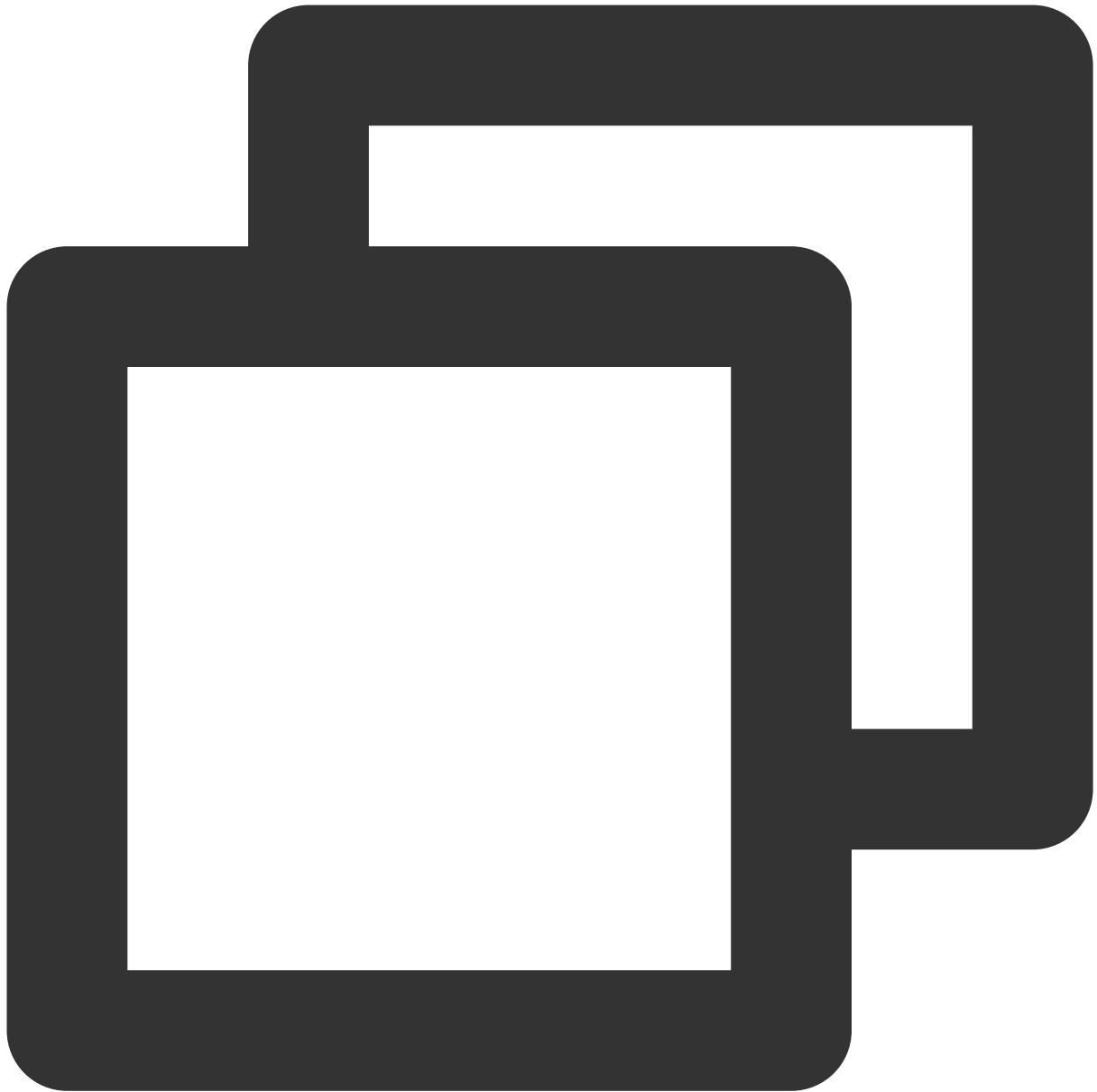
```
create role 계정 이름 login replication encrypted password '사용자 정의 비밀번호';
```

본 문에서는 데이터베이스 계정 'replica'와 비밀번호 '123456'을 생성하는 것을 예로 들어 다음 명령을 실행합니다.



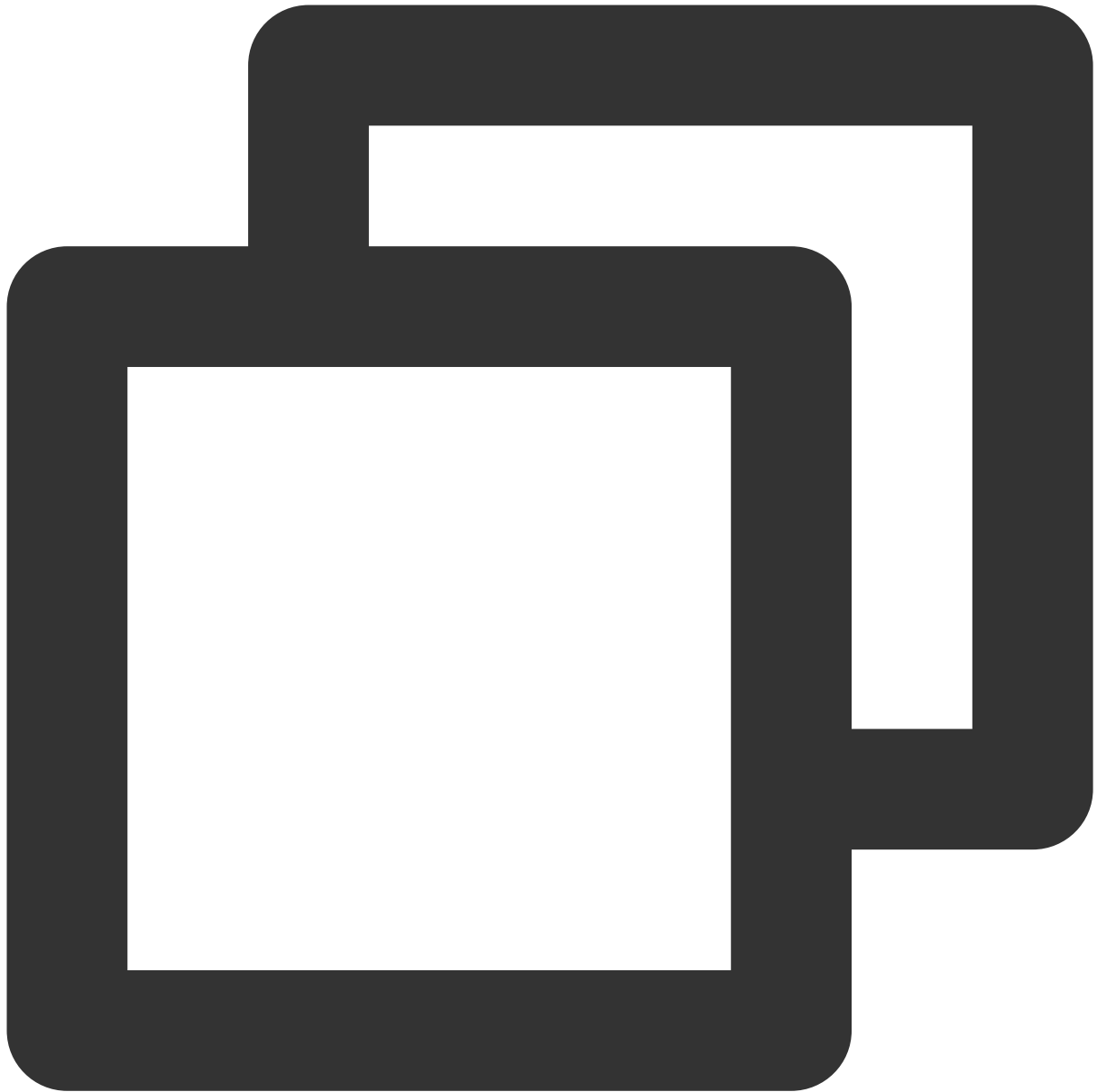
```
create role replica login replication encrypted password '123456';
```

10. 다음 명령어를 실행하여 계정이 성공적으로 생성되었는지 쿼리합니다.



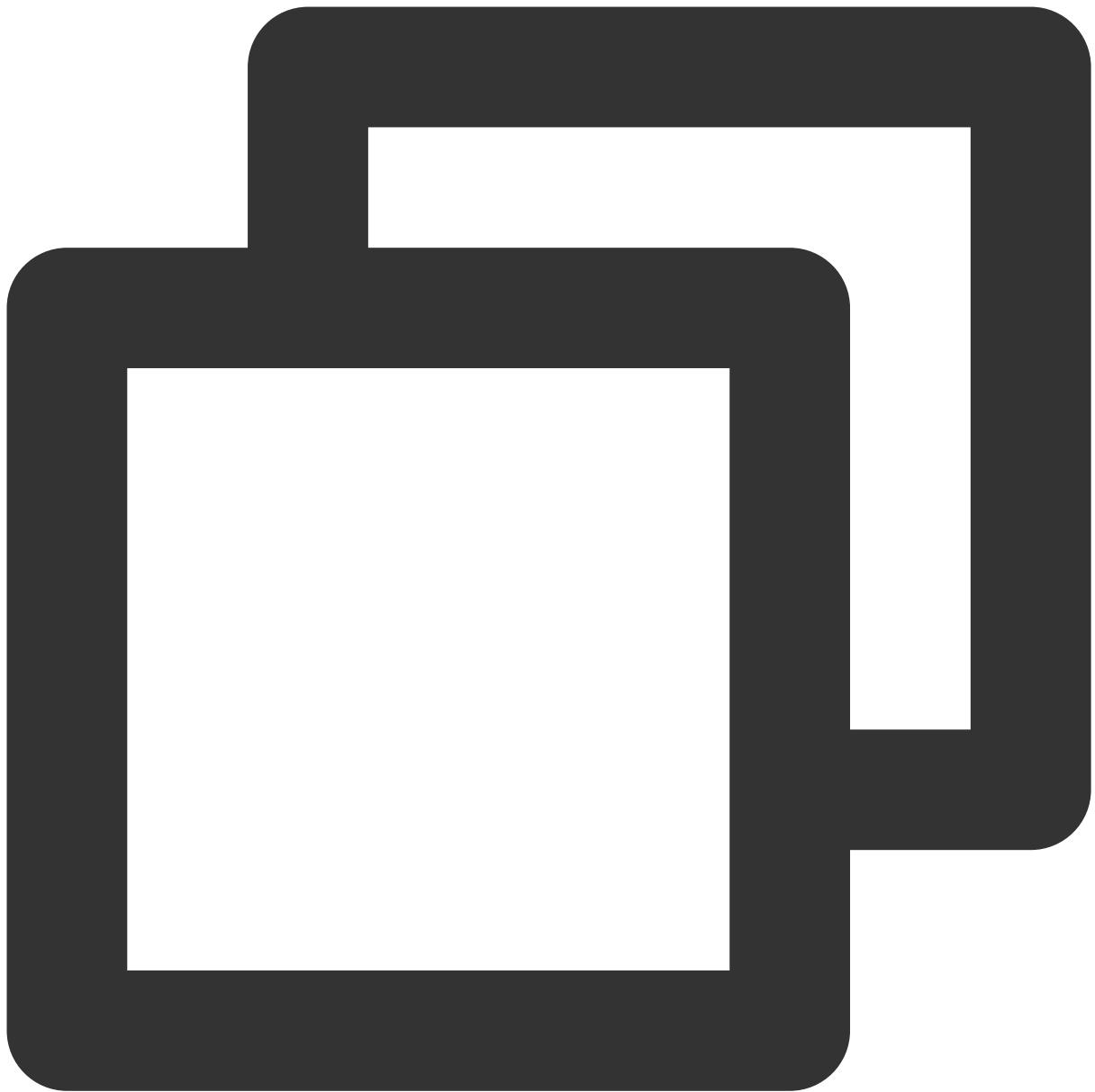
```
SELECT username from pg_user;
```

다음 결과가 반환되면 생성이 완료된 것입니다.



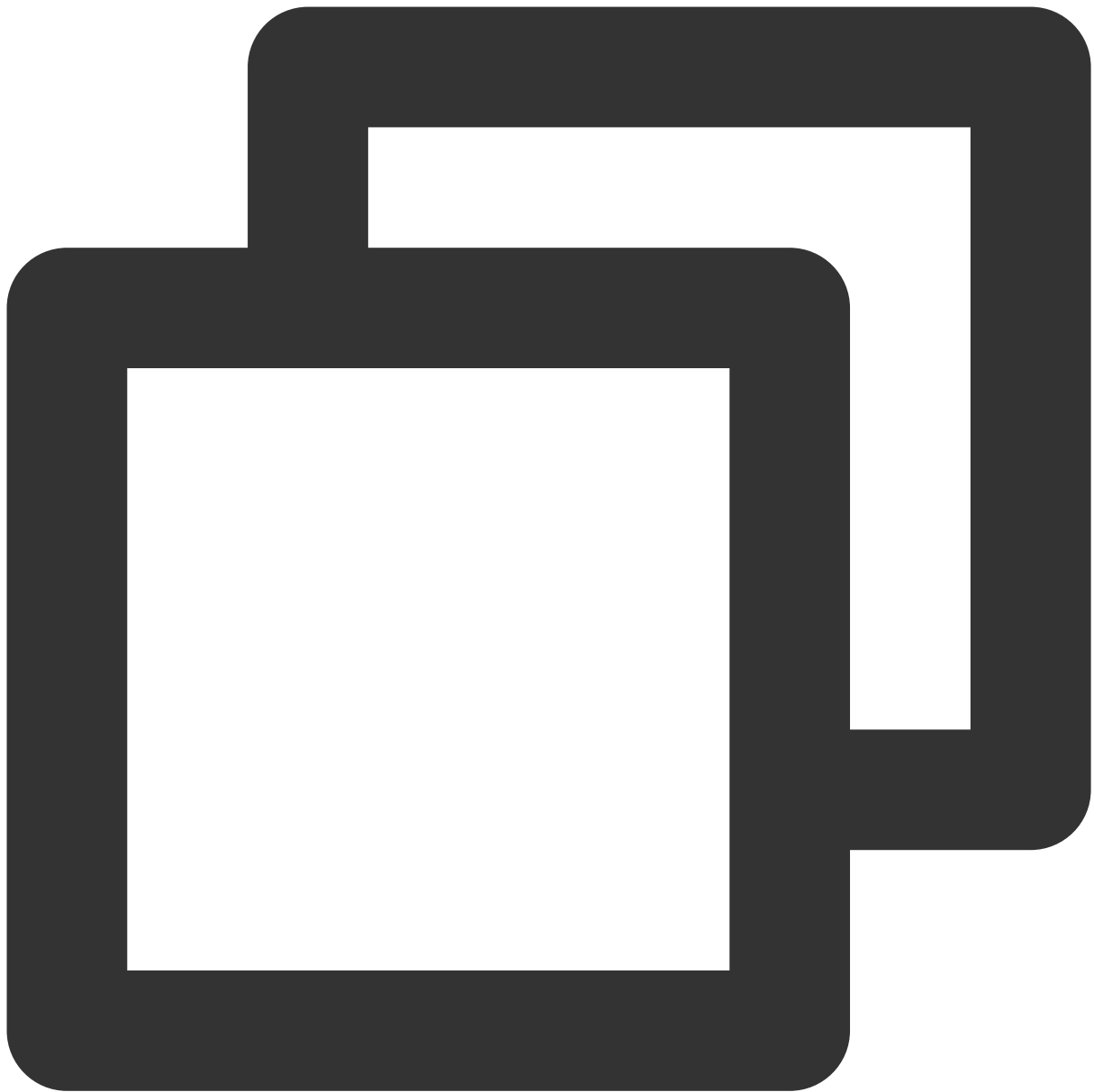
```
username
-----
postgres
replica
(2 rows)
```

11. 다음 명령어를 실행하여 권한이 성공적으로 생성되었는지 쿼리합니다.



```
SELECT rolname from pg_roles;
```

다음 결과가 반환되면 생성이 완료된 것입니다.

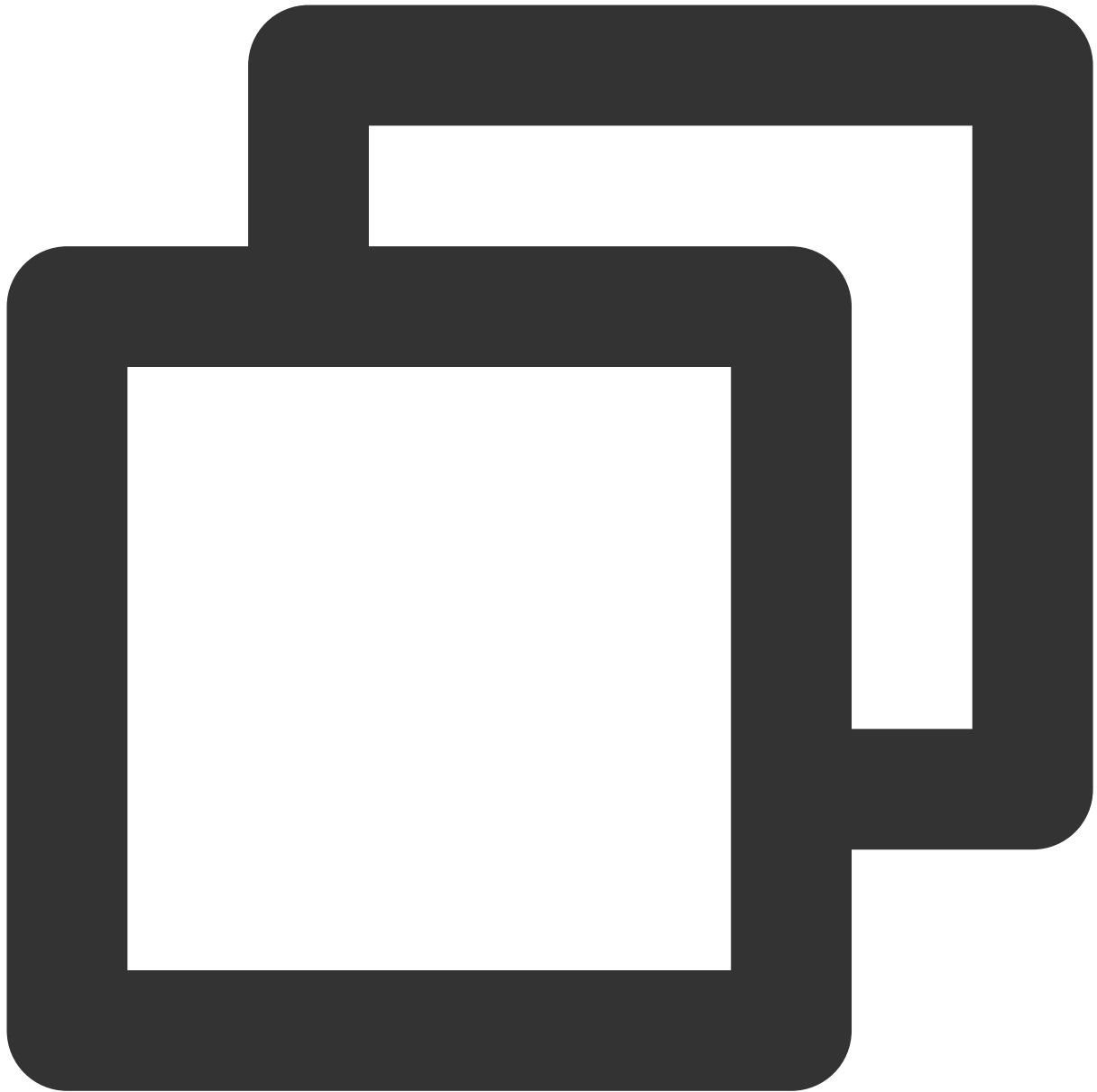


```
rolname
-----
pg_signal_backend
postgres
replica
(3 rows)
```

12. **\q**를 입력하고 **Enter**를 눌러 SQL 터미널을 종료합니다.

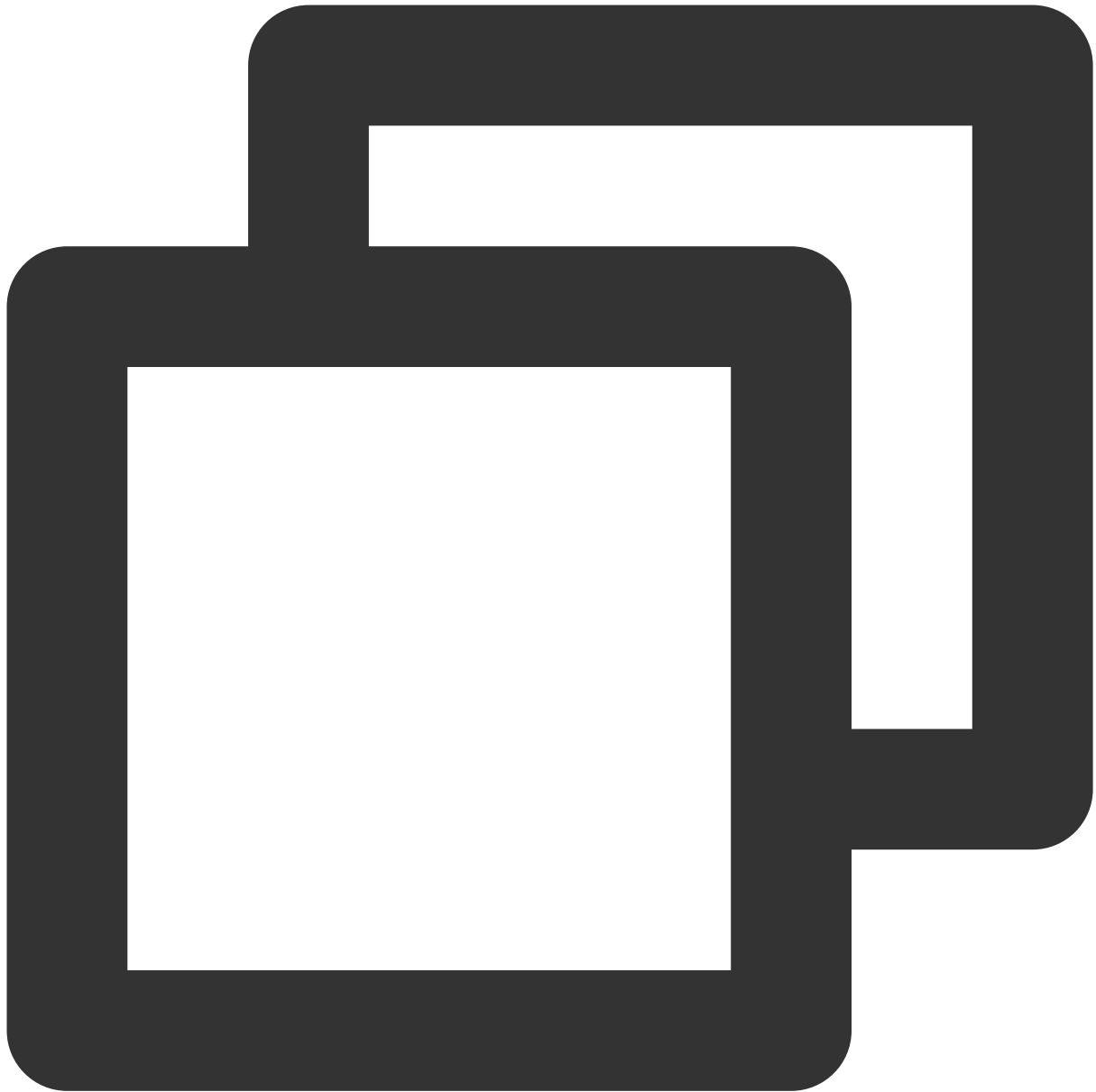
13. **exit** 를 입력하고 **Enter**를 눌러 PostgreSQL을 종료합니다.

14. 다음 명령을 실행하여 **pg_hba.conf** 구성 파일을 열고 **replica** 사용자 얼로우리스트를 설정합니다.



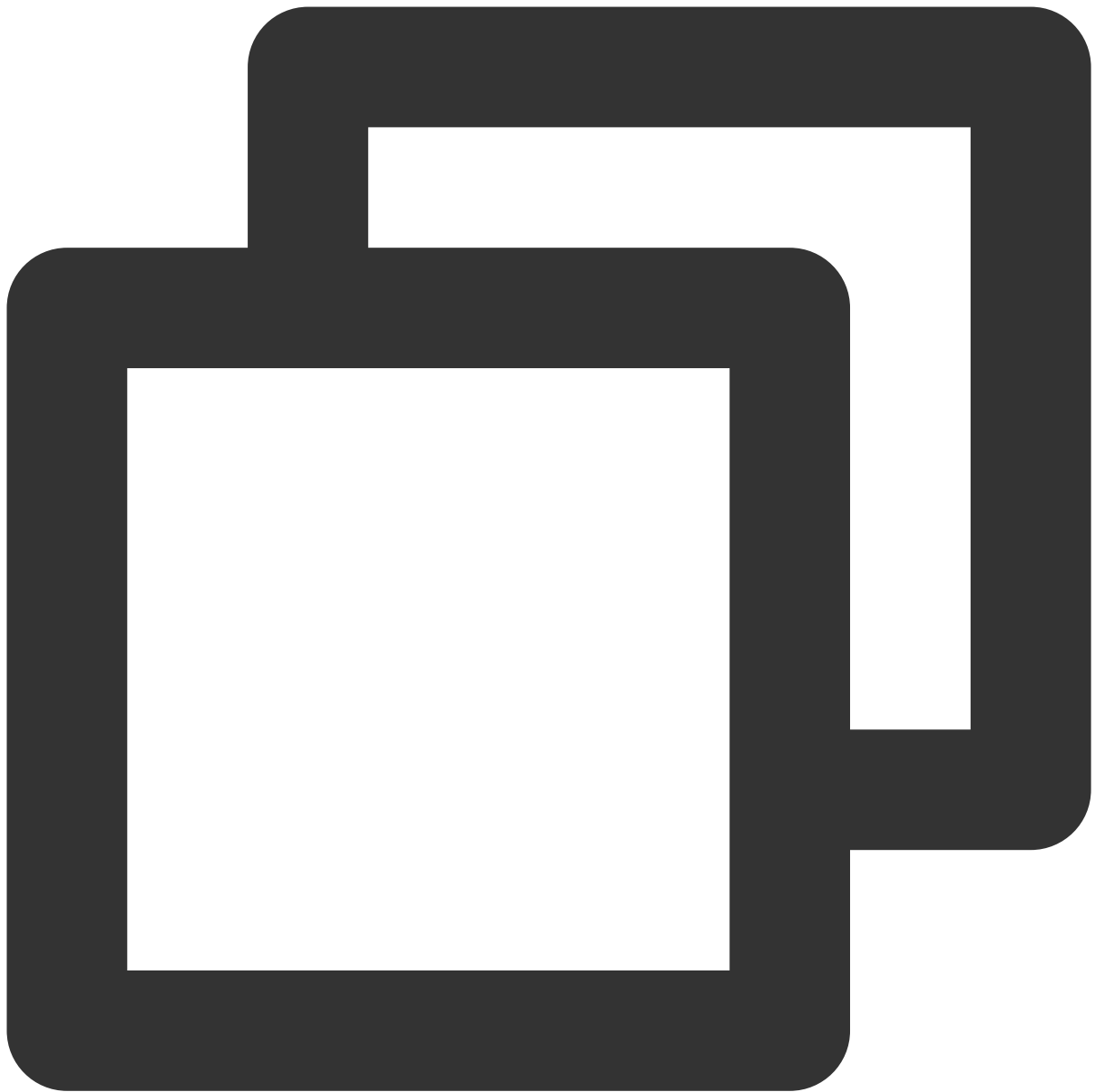
```
vim /var/lib/pgsql/12/data/pg_hba.conf
```

15.i를 눌러 편집 모드로 전환하고 'IPv4 local connections' 섹션에 다음 두 줄의 내용을 추가합니다.



host	all	all	<세컨더리 노드의 VPC IPv4 IP 대역>	md
host	replication	replica	<세컨더리 노드의 VPC IPv4 IP 대역>	md

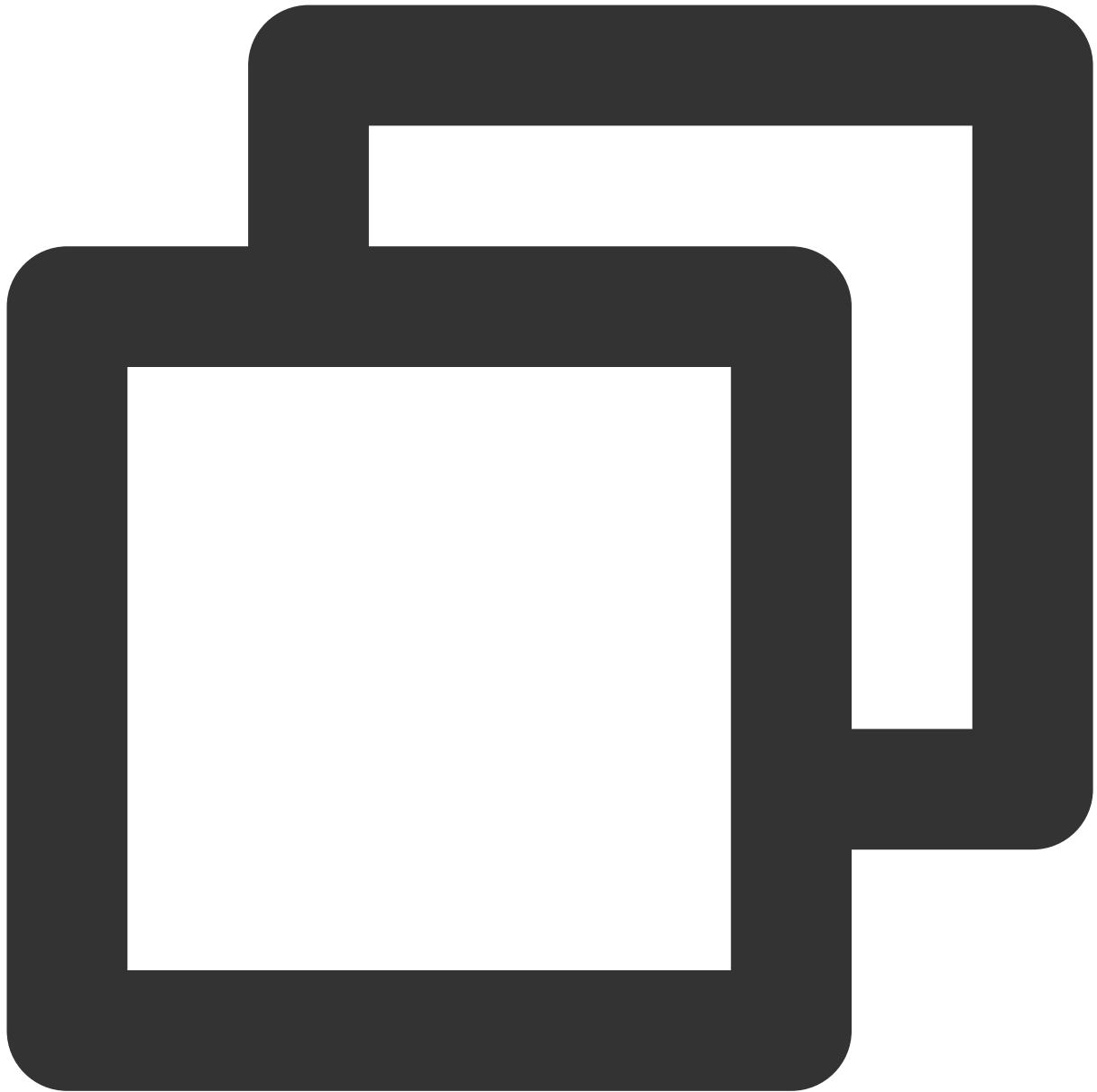
예를 들어 데이터베이스 계정이 'replica'이고 세컨더리 노드의 VPC IPv4 IP 대역이 'xx.xx.xx.xx/16'인 경우 'IPv4 local connections' 섹션에 다음 콘텐츠를 추가합니다.



host	all	all	xx.xx.xx.xx/16	md5
host	replication	replica	xx.xx.xx.xx/16	md5

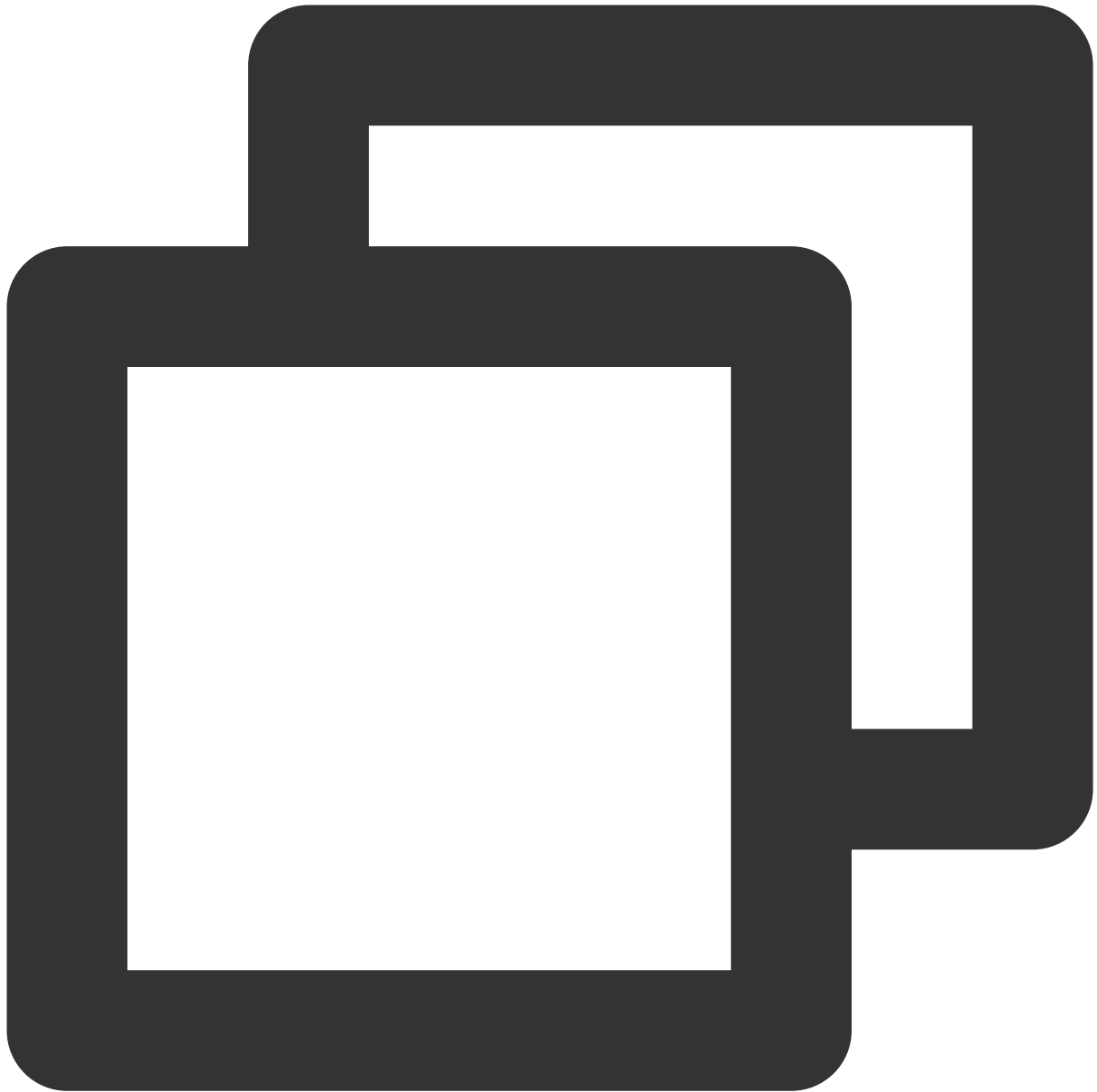
16. **Esc** 를 누르고 **:wq** 를 입력하여 파일을 저장하고 뒤로 돌아갑니다.

17. 다음 명령어를 실행하여 postgresql.conf 파일을 엽니다.



```
vim /var/lib/pgsql/12/data/postgresql.conf
```

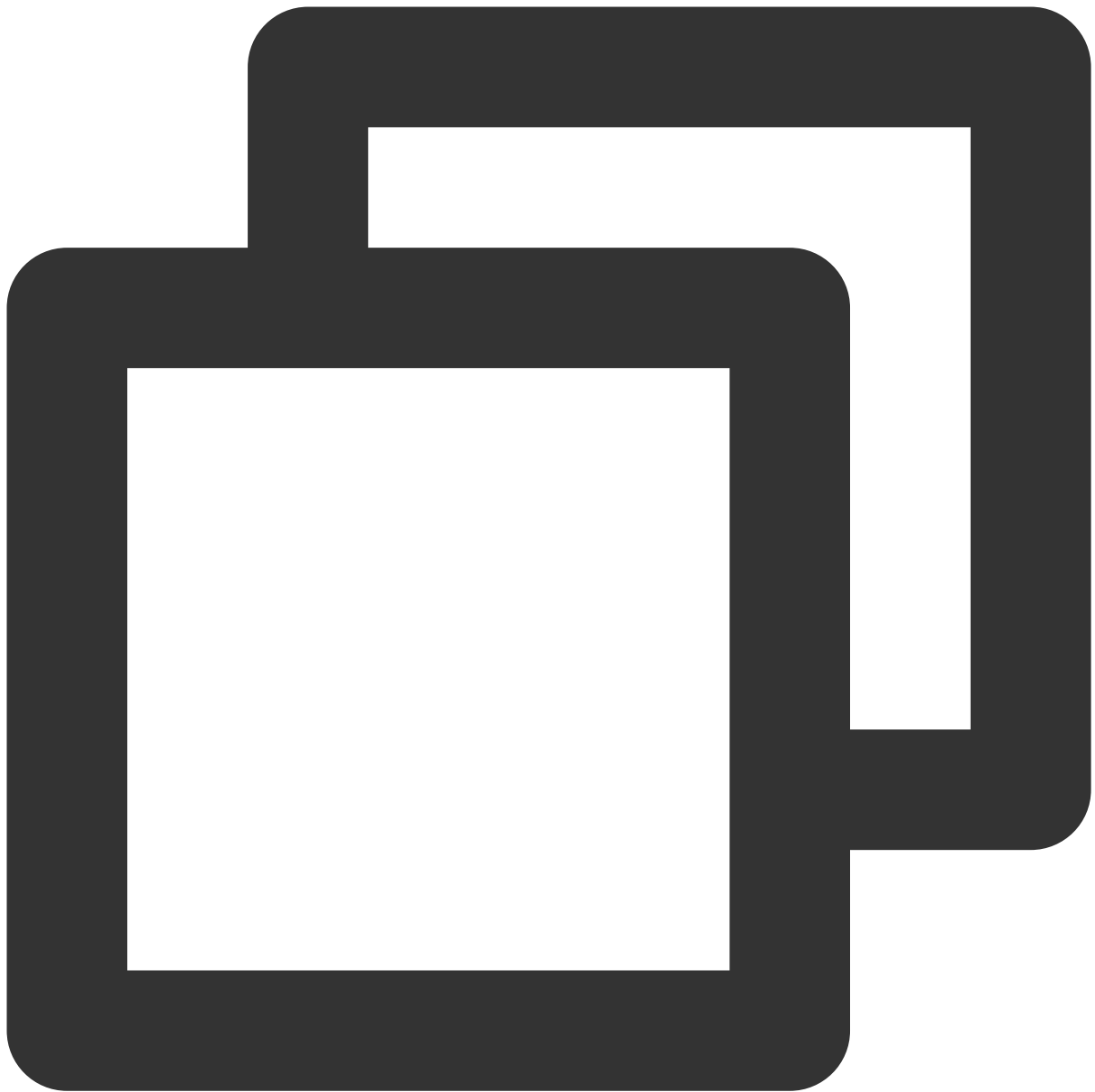
18.i를 눌러 편집 모드로 이동하고 다음 매개변수를 각각 찾은 다음 매개변수를 다음 콘텐츠로 수정합니다.



```
listen_addresses = '*'      #수신되는 내부 IP 주소
max_connections = 100 #최대 연결 수, 세컨더리 데이터베이스의 max_connections는 프라이머리
wal_level = hot_standby     #핫 백업 모드 활성화
synchronous_commit = on    #동기화 복사 활성화
max_wal_senders = 32        #동기화할 최대 프로세스 수
wal_sender_timeout = 60s    #스트리밍 복사 호스트가 데이터를 보내는 시간 초과 시간
```

19. **Esc** 를 누르고 **:wq** 를 입력하여 파일을 저장하고 뒤로 돌아갑니다.

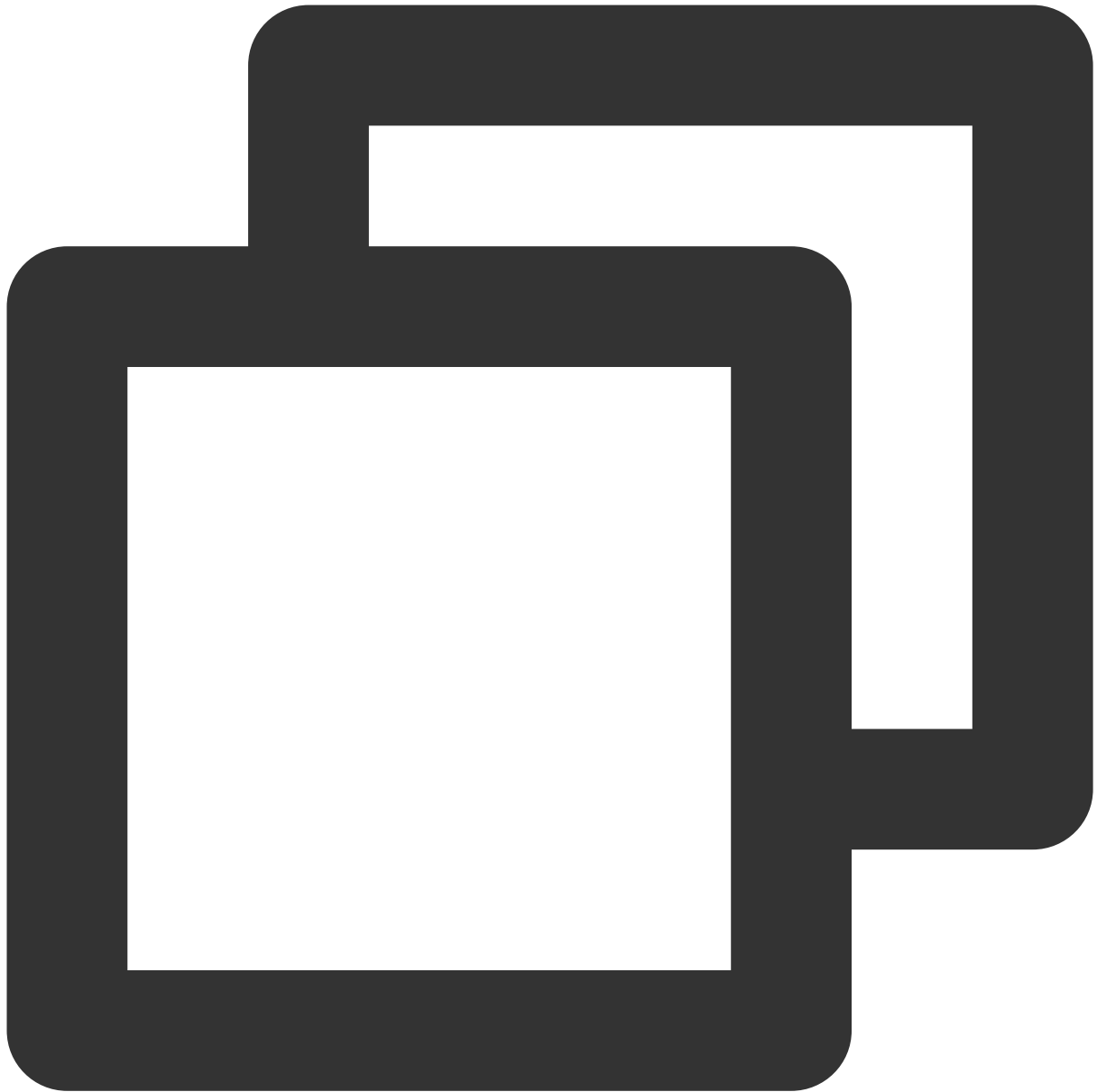
20. 아래의 명령어를 실행하여 서비스를 재시작합니다.



```
systemctl restart postgresql-12.service
```

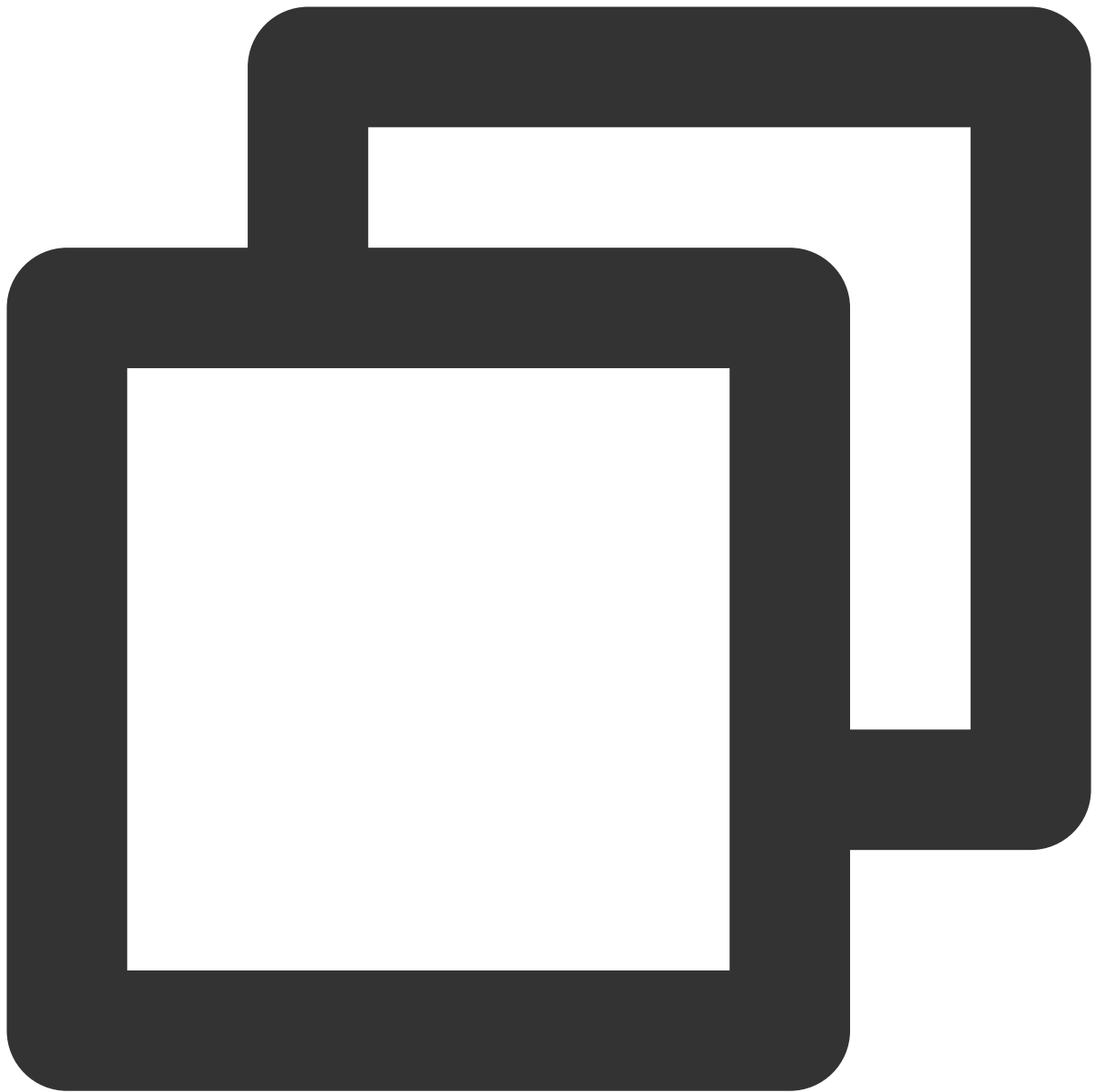
세컨더리 노드 설정

1. 세컨더리 노드 인스턴스에 로그인합니다.
2. 다음 명령을 실행하여 모든 패키지, 시스템 버전 및 커널을 업그레이드합니다.

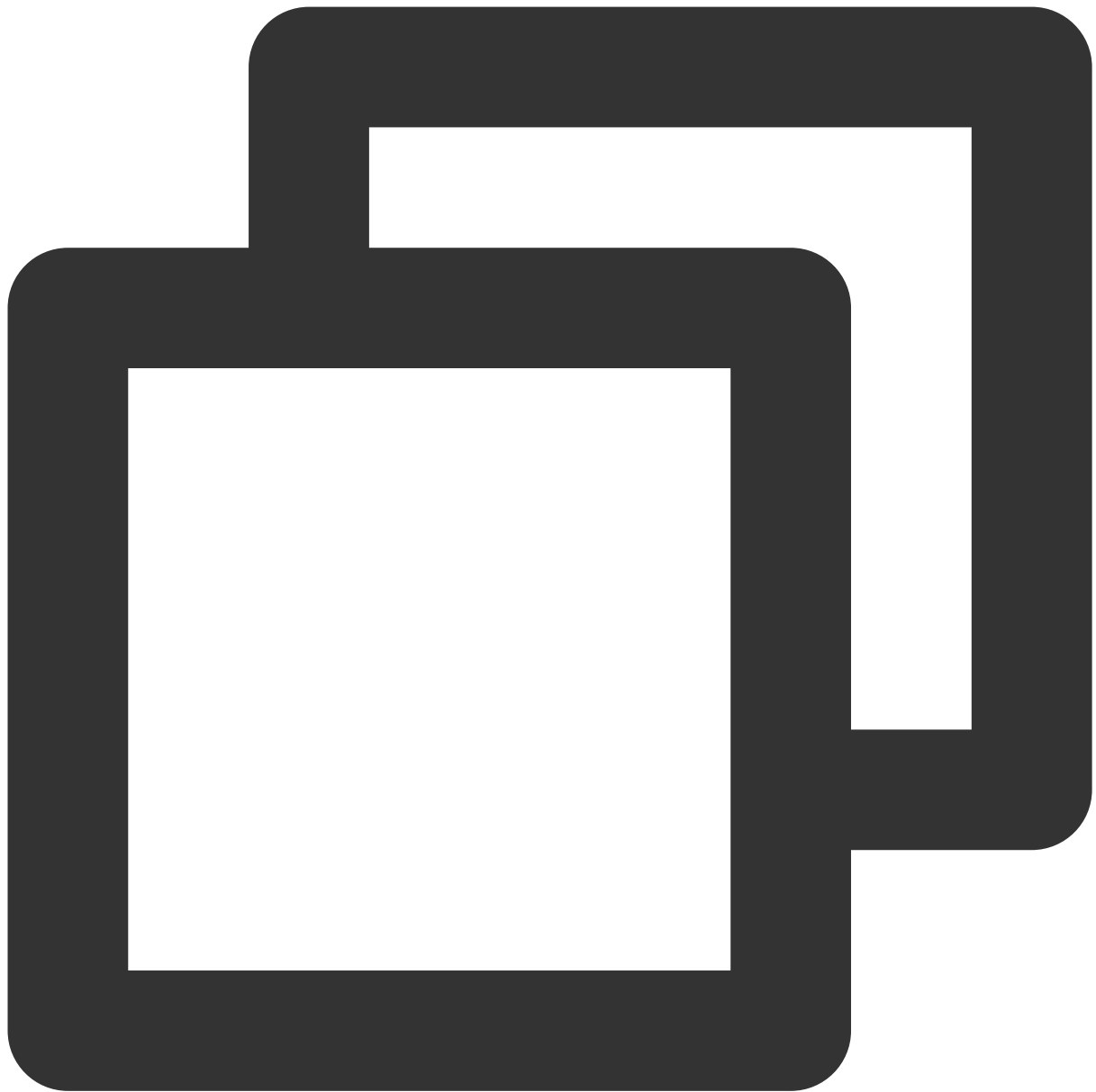


```
yum update -y
```

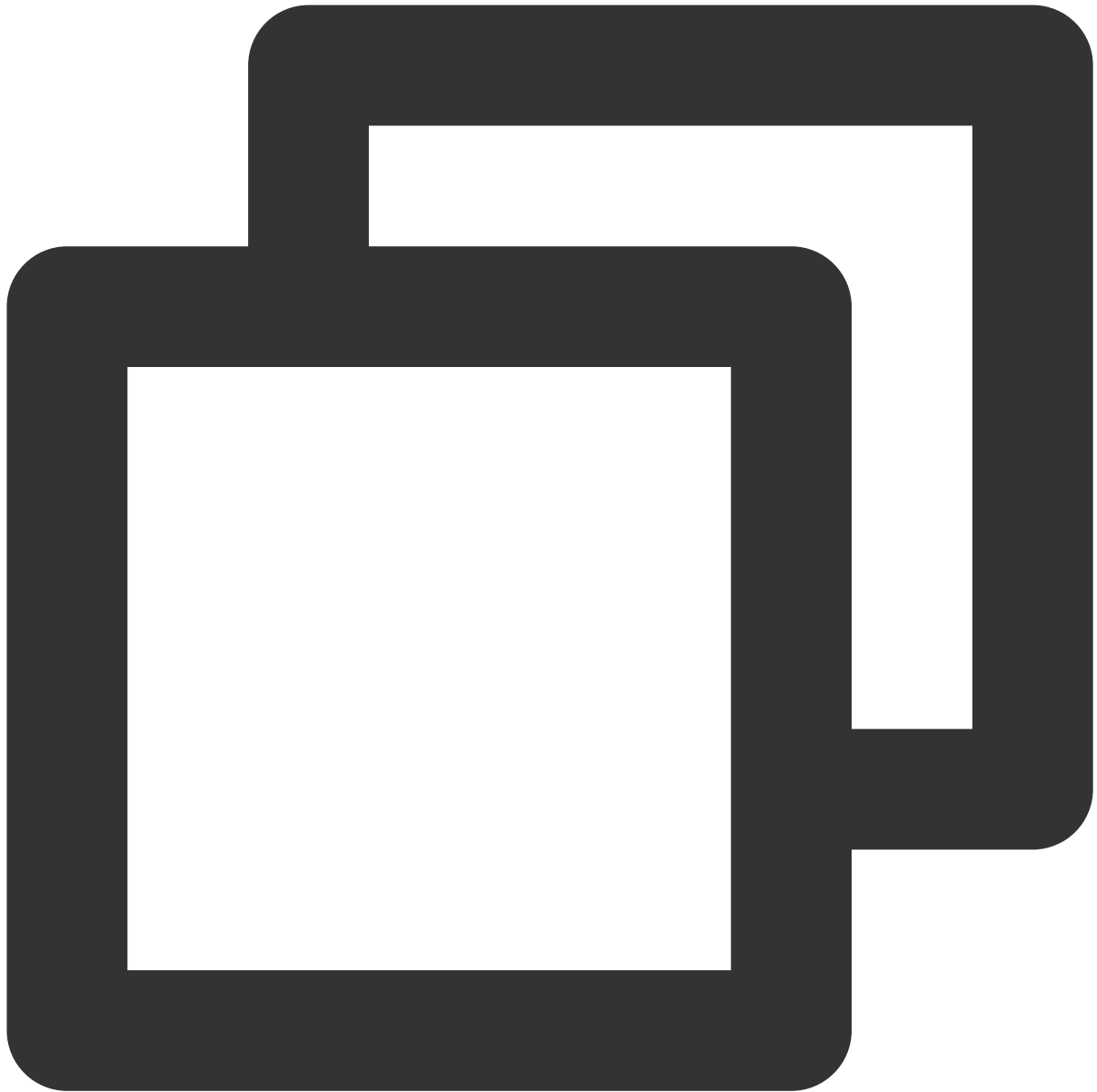
3. 다음 명령어를 순서대로 실행하여 PostgreSQL을 설치합니다.



```
wget --no-check-certificate https://download.postgresql.org/pub/repos/yum/repорpms/
```

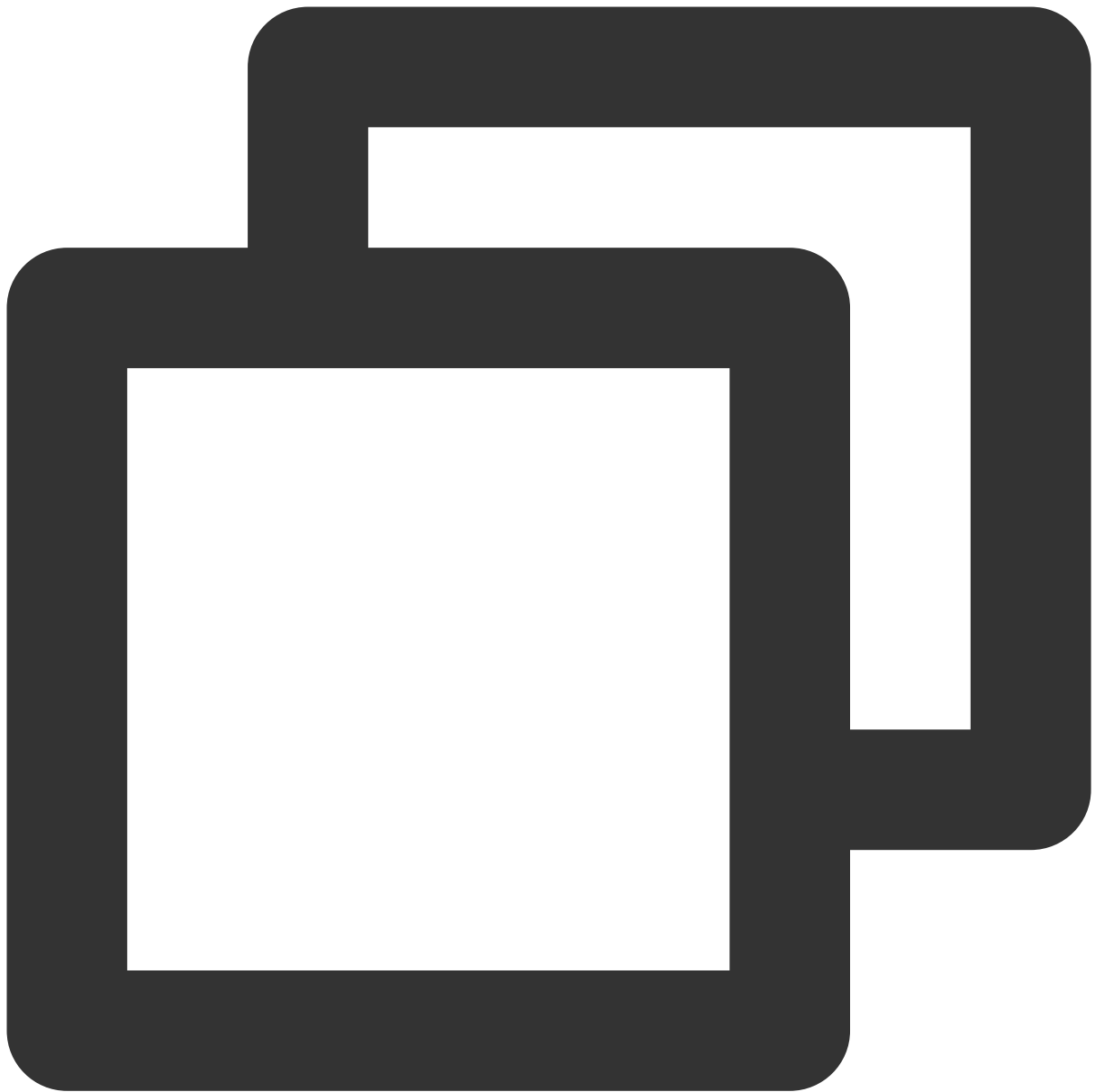


```
rpm -ivh pgdg-redhat-repo-latest.noarch.rpm
```



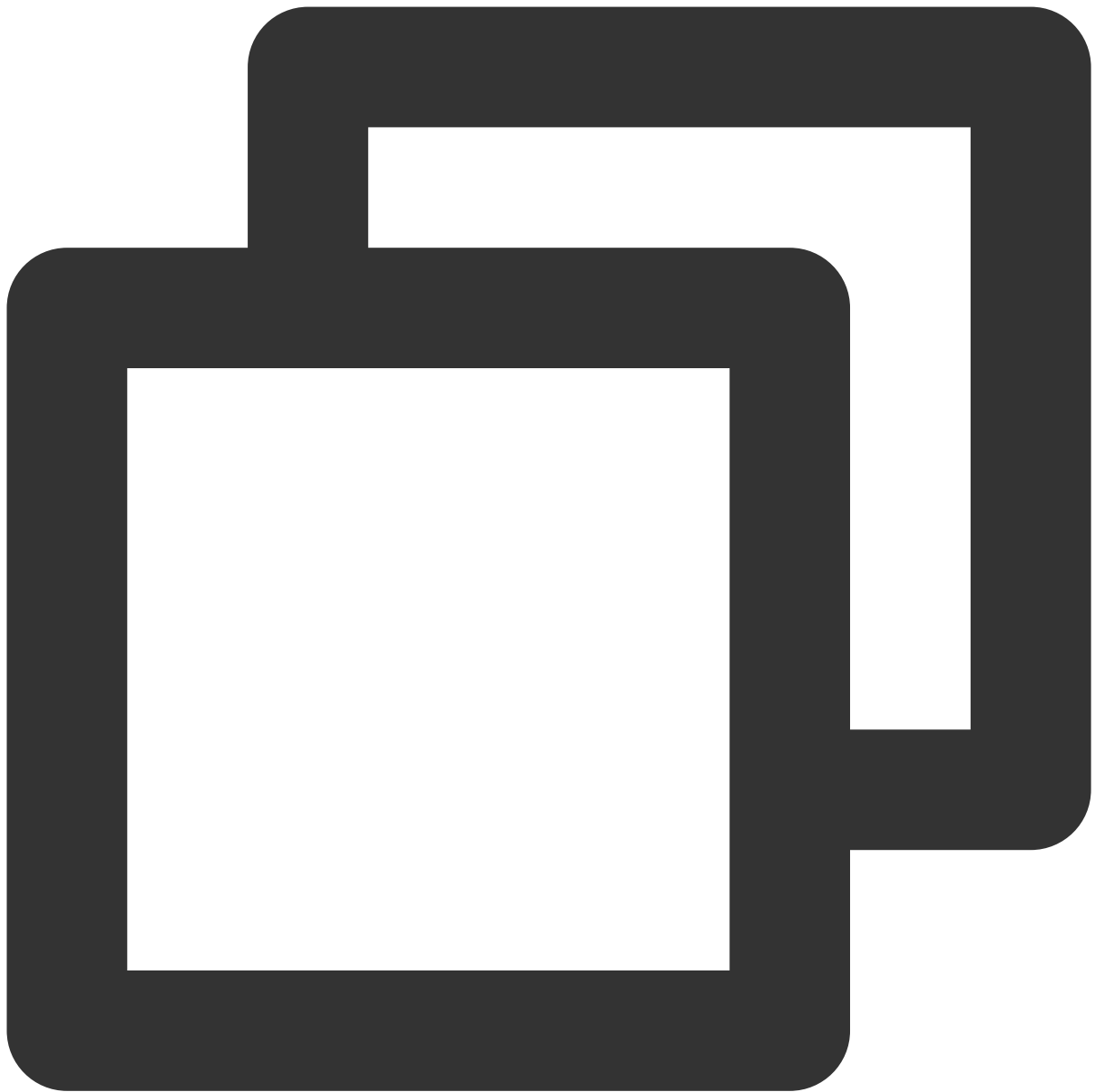
```
yum install postgresql12-server postgresql12-contrib -y
```

4. 다음 명령을 실행하여 `pg_basebackup` 기본 백업 툴을 사용하여 백업 디렉터리를 지정합니다.



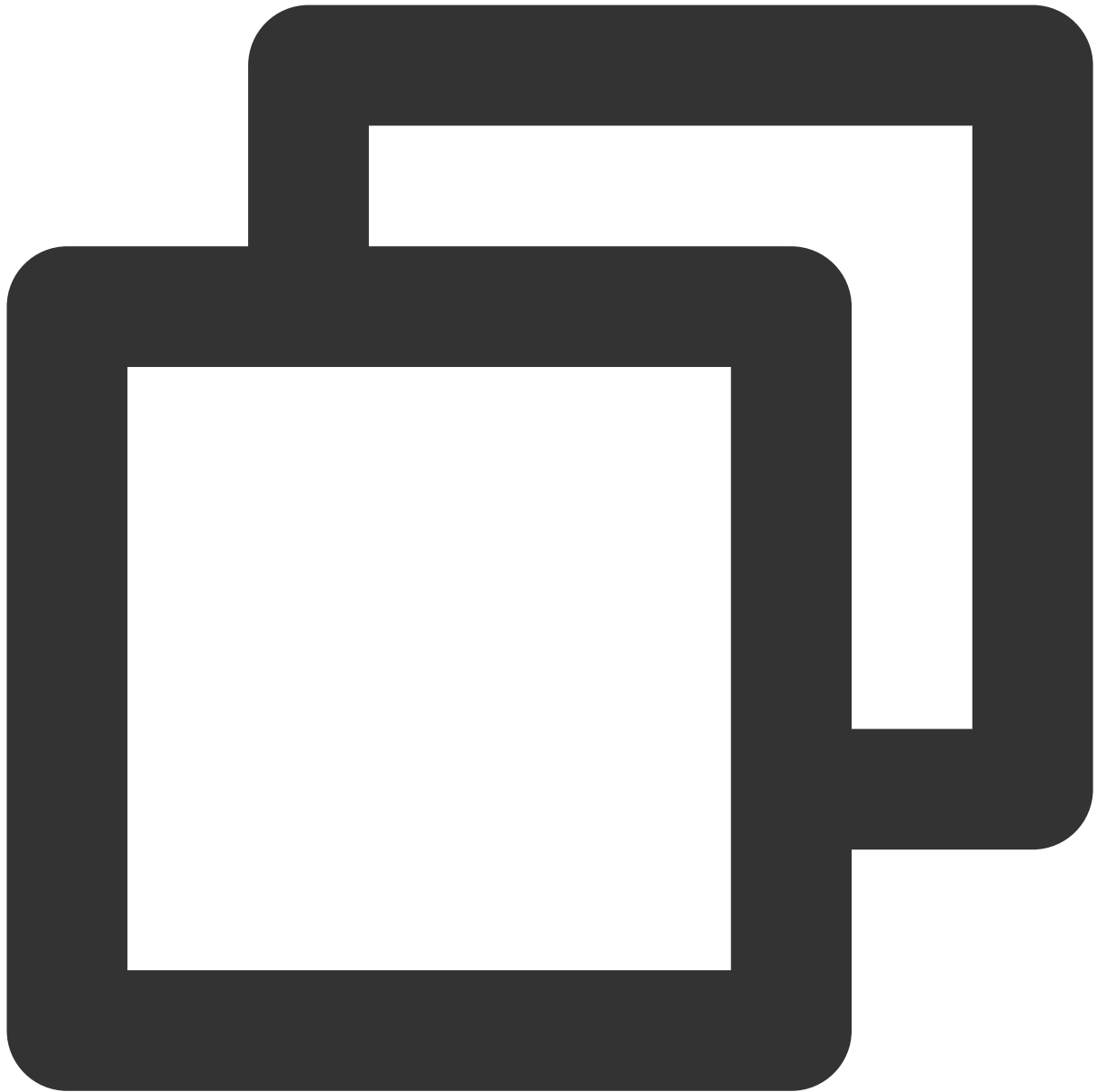
```
pg_basebackup -D /var/lib/pgsql/12/data -h <프라이머리 노드 공용 IP> -p 5432 -U replic
```

다음 지시에 따라 데이터베이스 계정에 해당하는 비밀번호를 입력하고 Enter를 누릅니다. 다음 결과가 반환되면 백업이 성공한 것입니다.



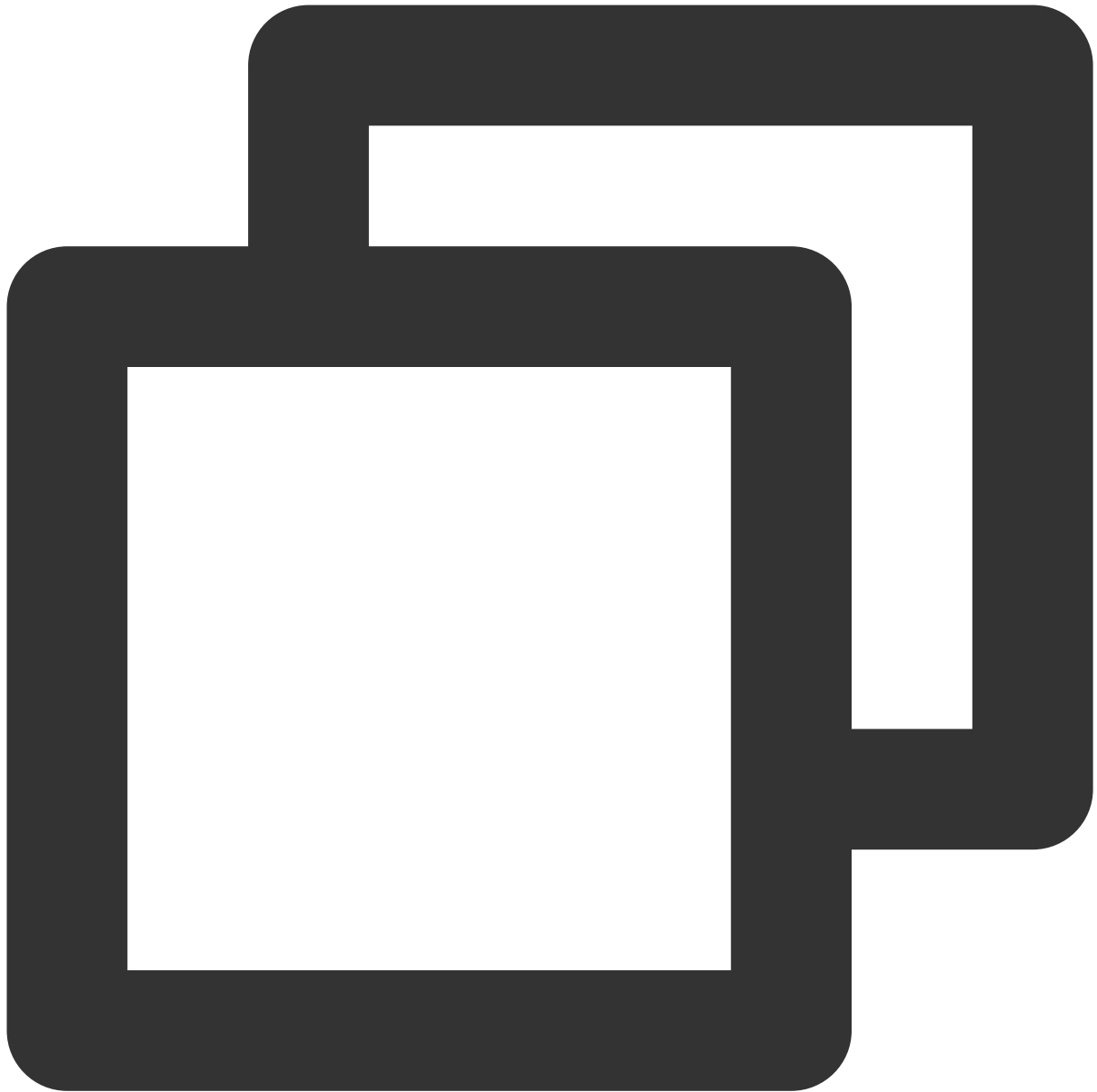
```
Password:  
24526/24526 kB (100%), 1/1 tablespace
```

5. 다음 명령을 실행하여 **master** 설정 파일을 복사합니다.



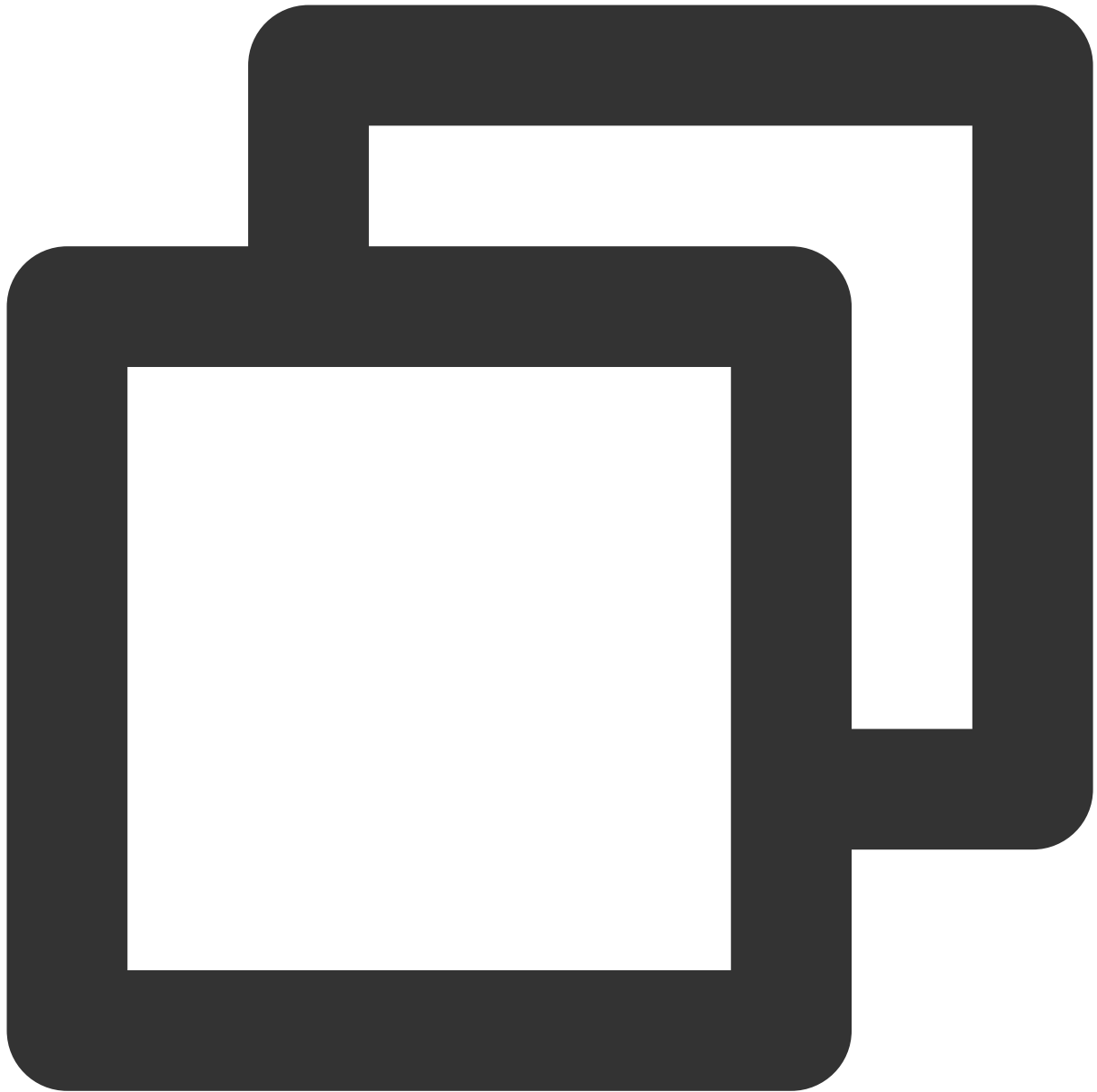
```
cp /usr/pgsql-12/share/recovery.conf.sample /var/lib/pgsql/12/data/recovery.conf
```

6. 다음 명령어를 실행하여 `recovery.conf` 파일을 엽니다.



```
vim /var/lib/pgsql/12/data/recovery.conf
```

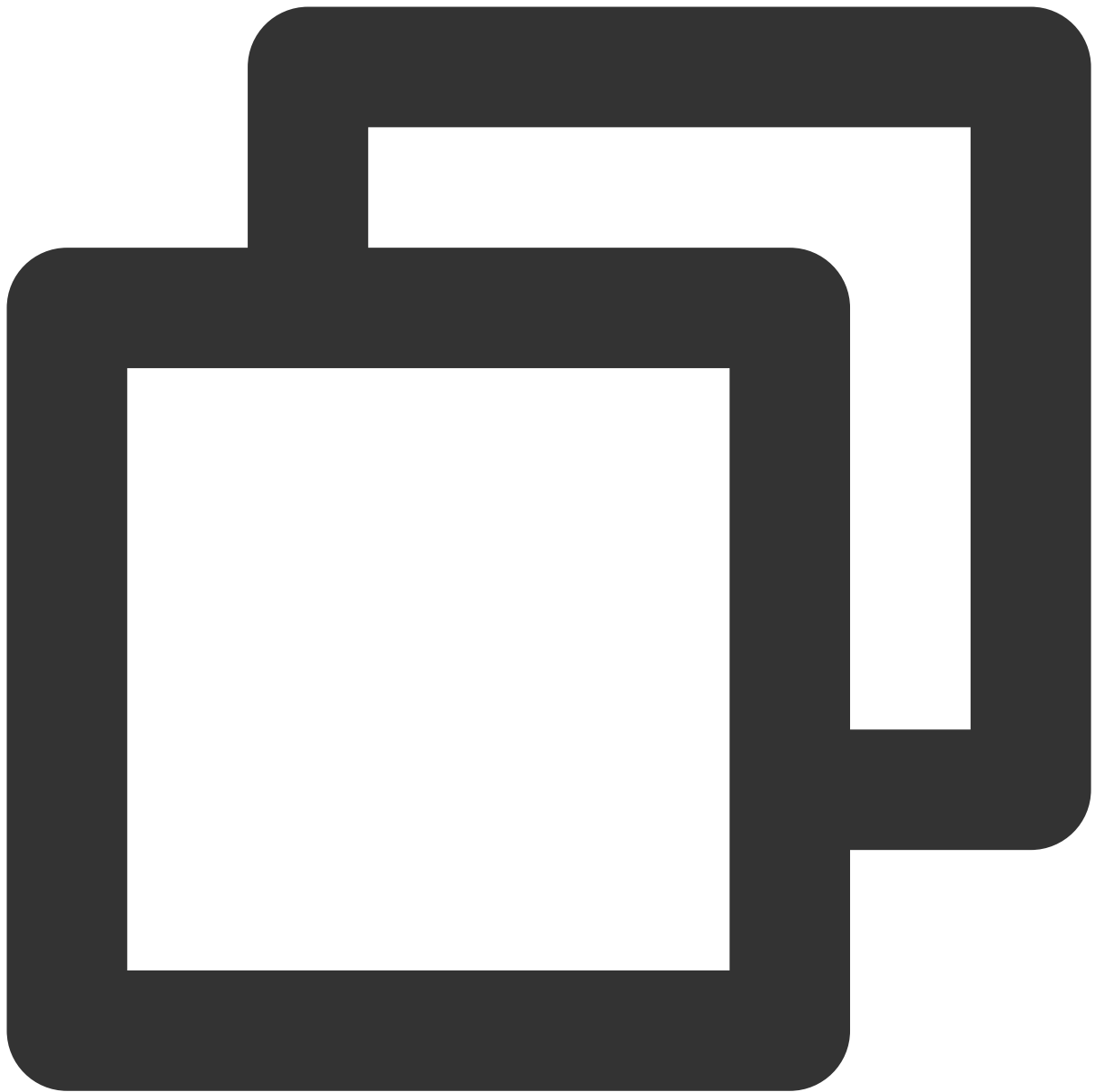
7.i를 눌러 편집 모드로 전환하고 각각 다음 매개변수를 찾아 다음 콘텐츠와 같이 수정합니다.



```
standby_mode = on      #이 노드를 세컨더리 데이터베이스로 성명
primary_conninfo = 'host=<프라이머리 노드 공용 IP> port=5432 user=데이터베이스 계정 passw
recovery_target_timeline = 'latest' #스트림 복사를 최신 데이터와 동기화
```

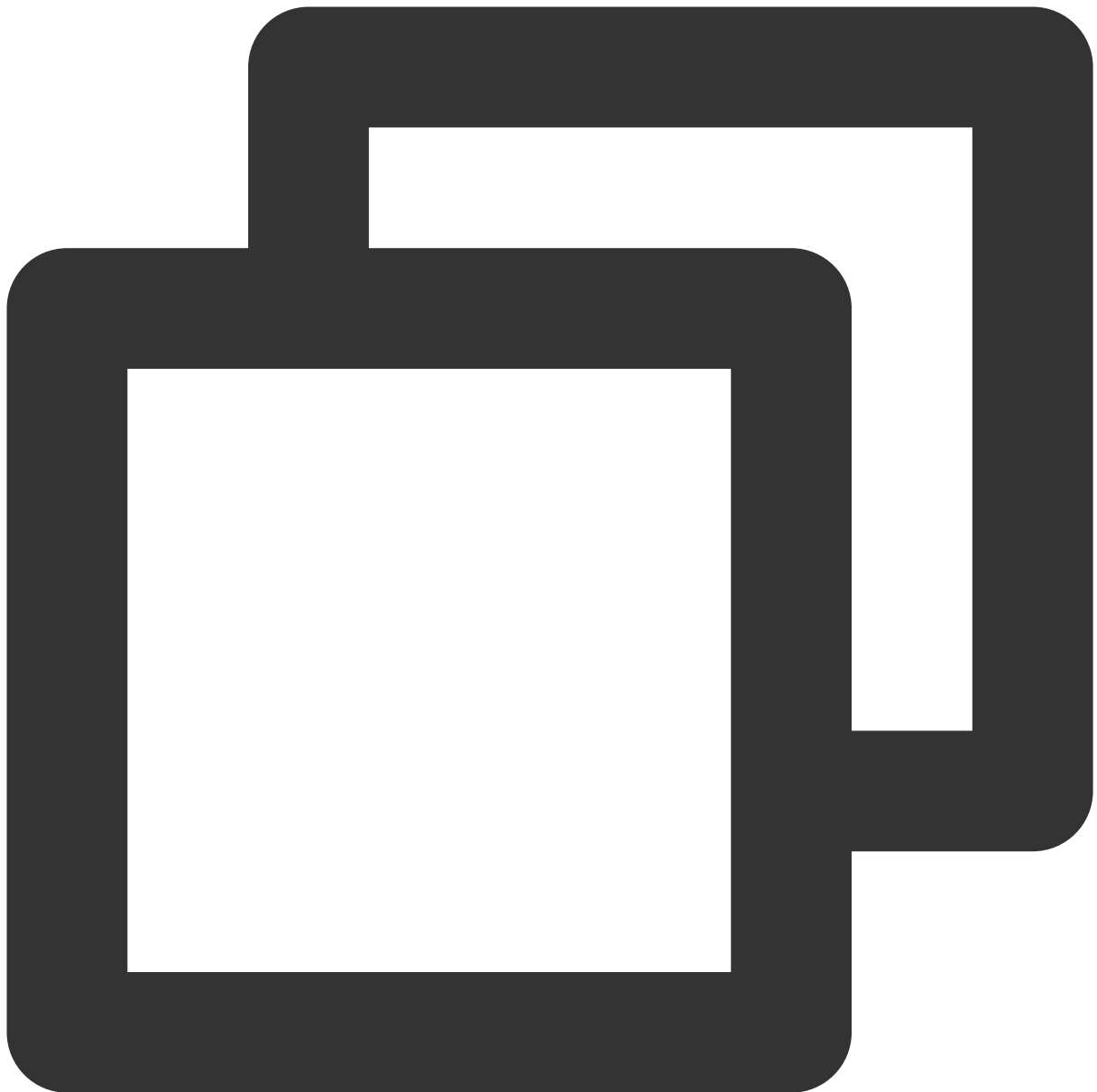
8. **Esc** 를 누르고 **:wq** 를 입력하여 파일을 저장하고 뒤로 돌아갑니다.

9. 다음 명령어를 실행하여 `postgresql.conf` 파일을 엽니다.



```
vim /var/lib/pgsql/12/data/postgresql.conf
```

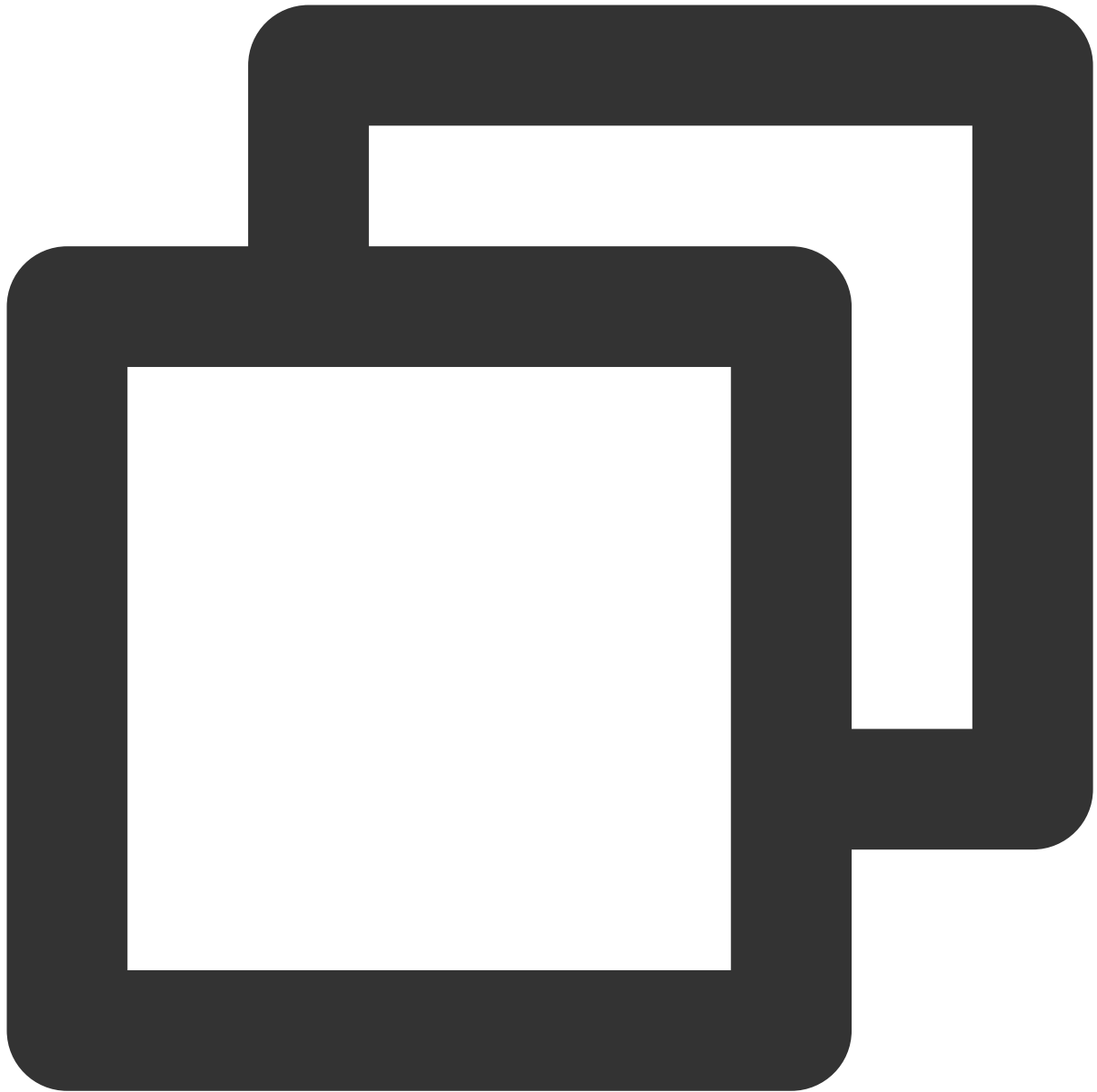
10.i를 눌러 편집 모드로 전환하고 다음 매개변수를 각각 찾아 다음과 같이 수정합니다.



```
max_connections = 1000          # 최대 연결 수, 세컨더리 데이터베이스의 max_connections
hot_standby = on                 # 핫 백업 활성화
max_standby_streaming_delay = 30s # 스트림 백업의 최대 딜레이 시간
wal_receiver_status_interval = 1s # 세컨더리 노드가 프라이머리 노드에 상태를 보고하는 최대
hot_standby_feedback = on       # 데이터 복사에 오류가 있는 경우 프라이머리에게 피드백
```

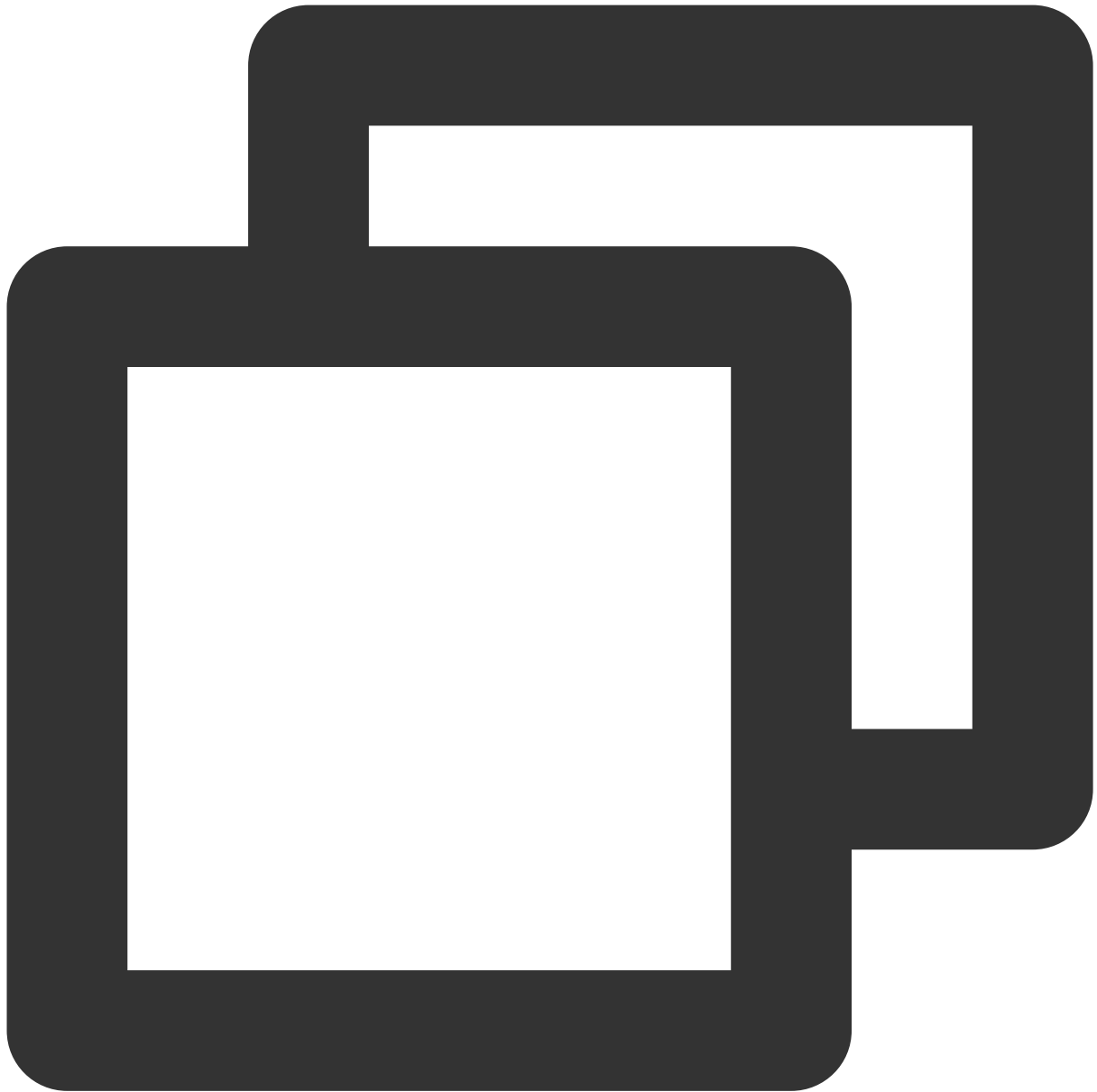
11. **Esc** 를 누르고 **:wq** 를 입력하여 파일을 저장하고 뒤로 돌아갑니다.

12. 다음 명령을 실행하여 데이터 디렉터리의 그룹 및 소유자를 수정합니다.



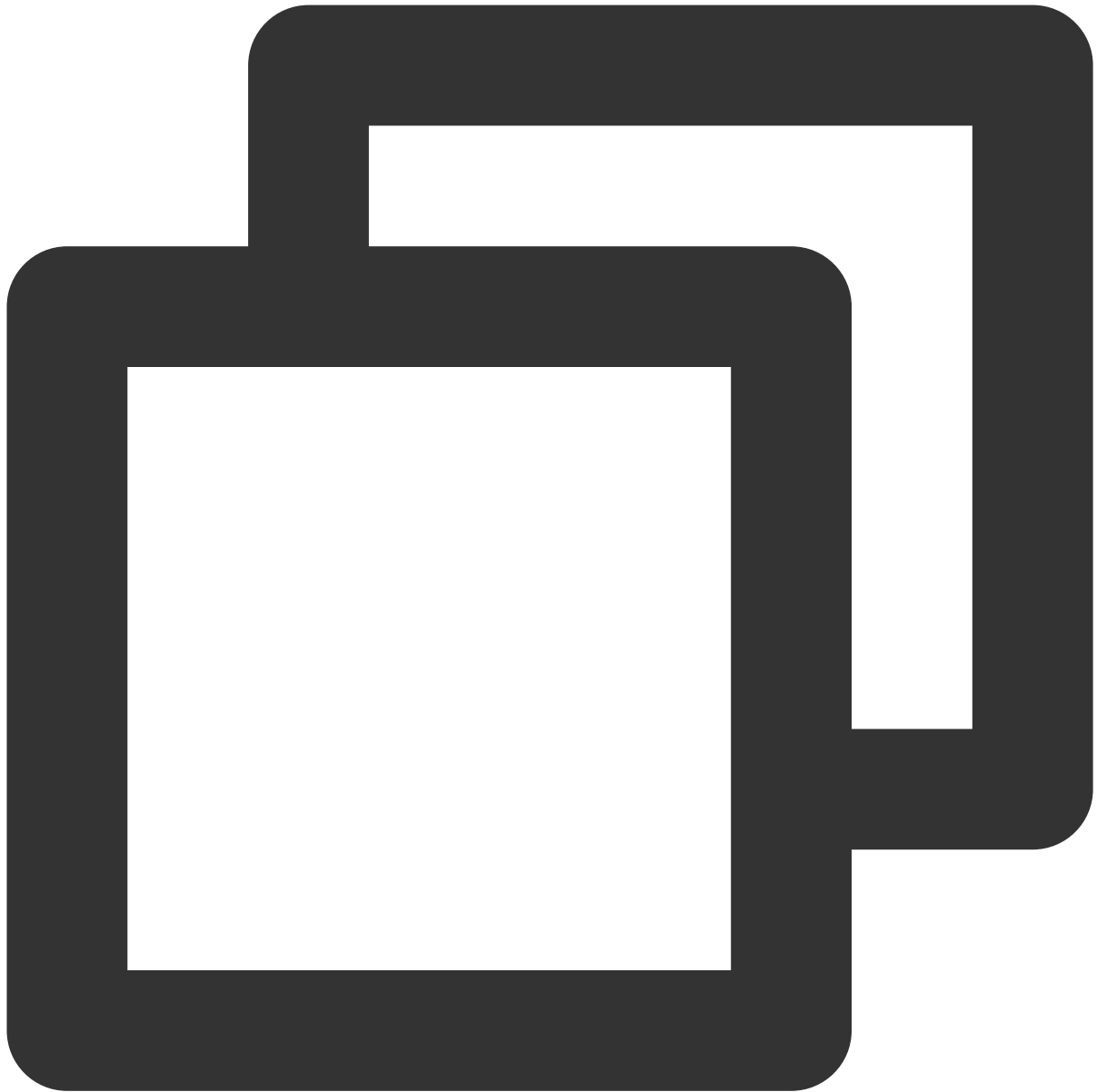
```
chown -R postgres.postgres /var/lib/pgsql/12/data
```

13. 아래의 명령어를 실행하여 서비스를 시작하십시오.



```
systemctl start postgresql-12.service
```

14. 다음 명령을 실행하여 시작 시 서비스가 자동으로 실행되도록 설정합니다.

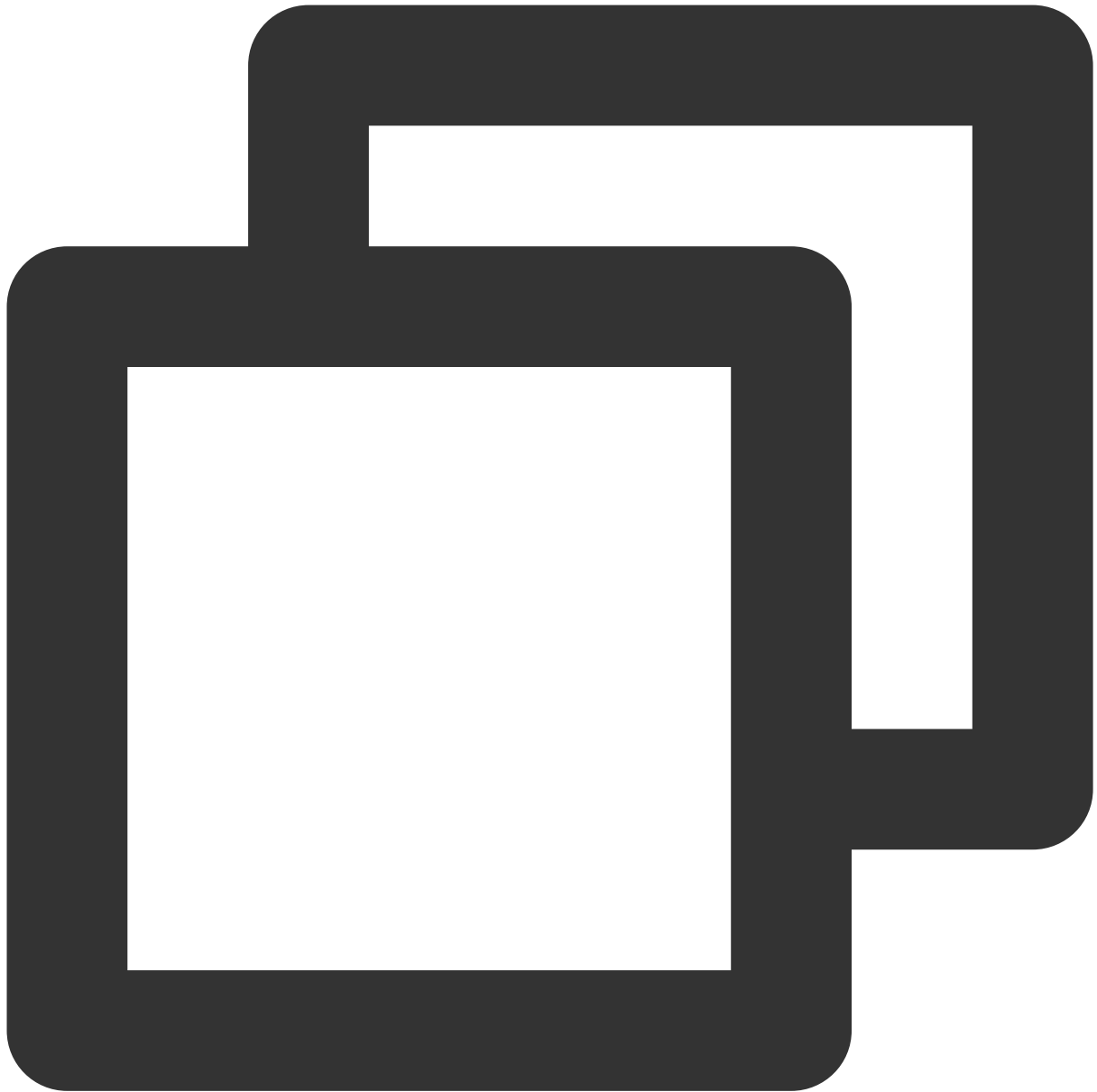


```
systemctl enable postgresql-12.service
```

배포 인증

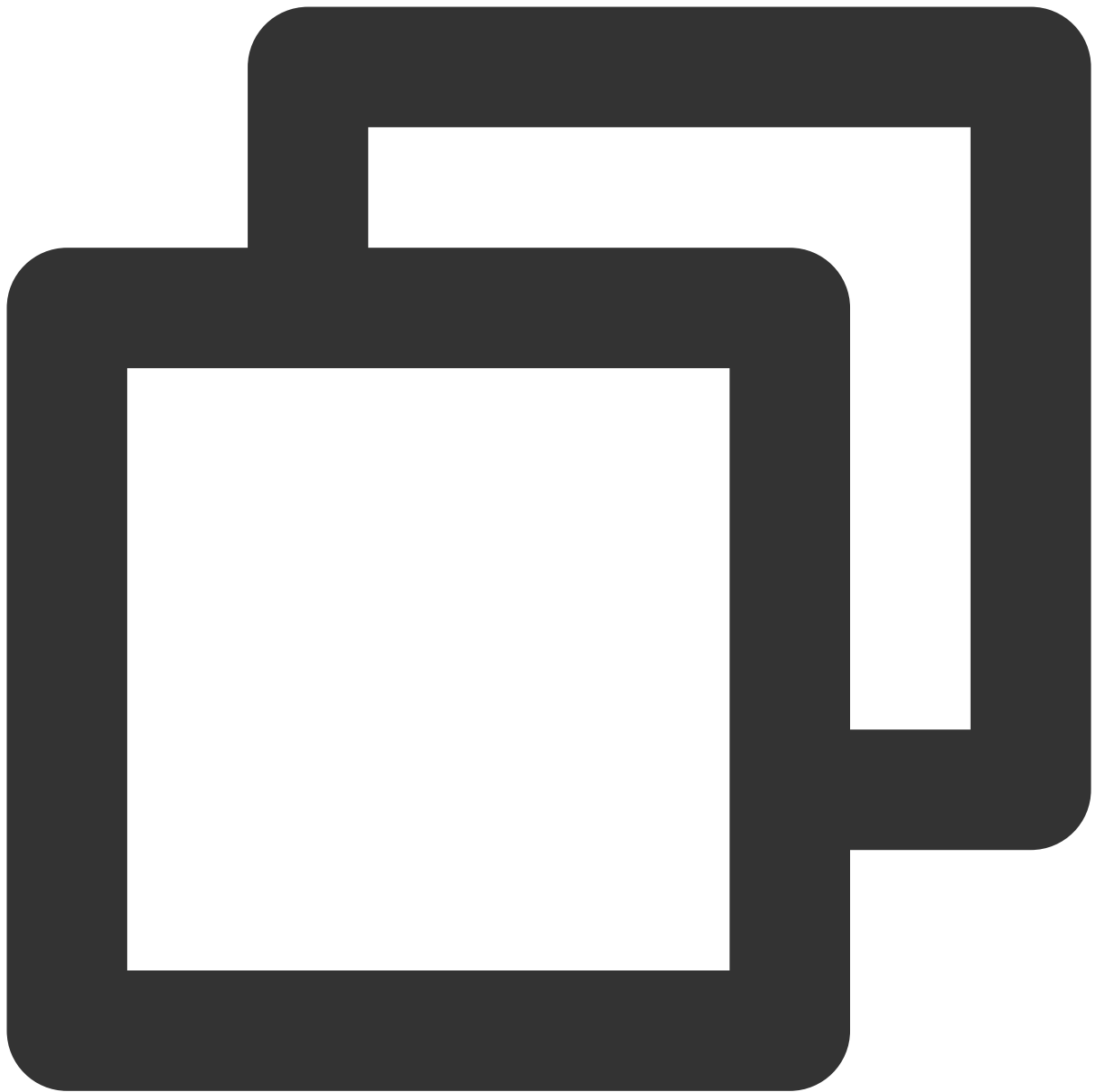
다음을 수행하여 배포 성공 여부를 인증할 수 있습니다.

1. 다음 명령어를 실행하여 노드에서 디렉터리를 백업합니다.



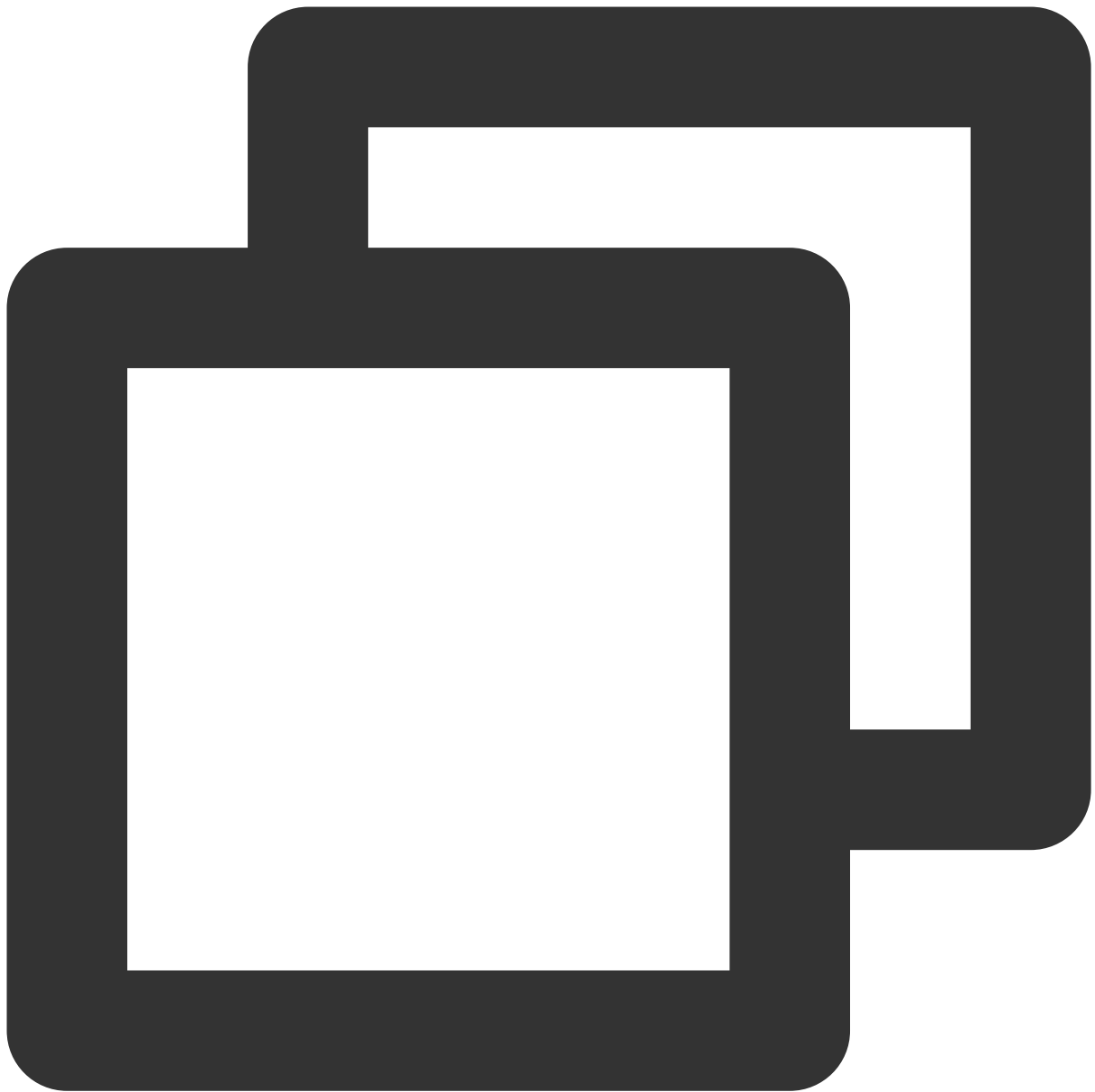
```
pg_basebackup -D /var/lib/pgsql/12/data -h <프라이머리 노드 공용 IP> -p 5432 -U replic
```

데이터베이스 비밀번호를 입력하고 **Enter** 키를 눌러 다음 결과가 반환되면 백업이 성공한 것입니다.



```
Password:  
24526/24526 kB (100%), 1/1 tablespace
```

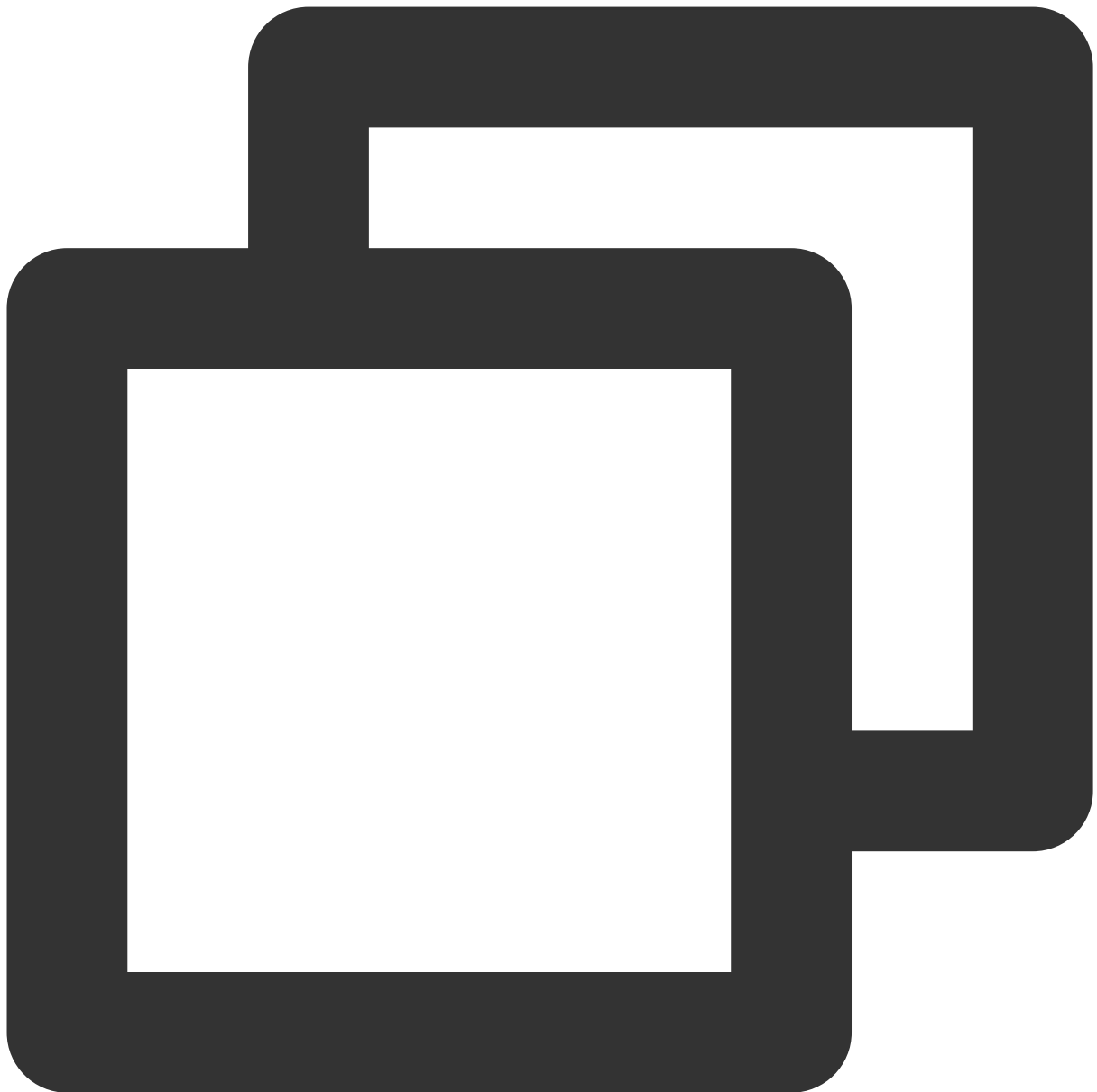
2. 프라이머리 노드에서 다음 명령을 실행하여 **sender** 프로세스를 조회합니다.



```
ps aux |grep sender
```

```
[root@VM-5-7-centos ~]# ps aux |grep sender
postgres  3875  0.0  0.0 363128  3068 ?        Ss   11:53   0:00 postgres: wal sender process re
00CA0
root      19724  0.0  0.0 112812   972 pts/0    S+   13:00   0:00 grep --color=auto sender
```

3. 세컨더리 노드에서 다음 명령을 실행하여 receiver 프로세스를 조회합니다.

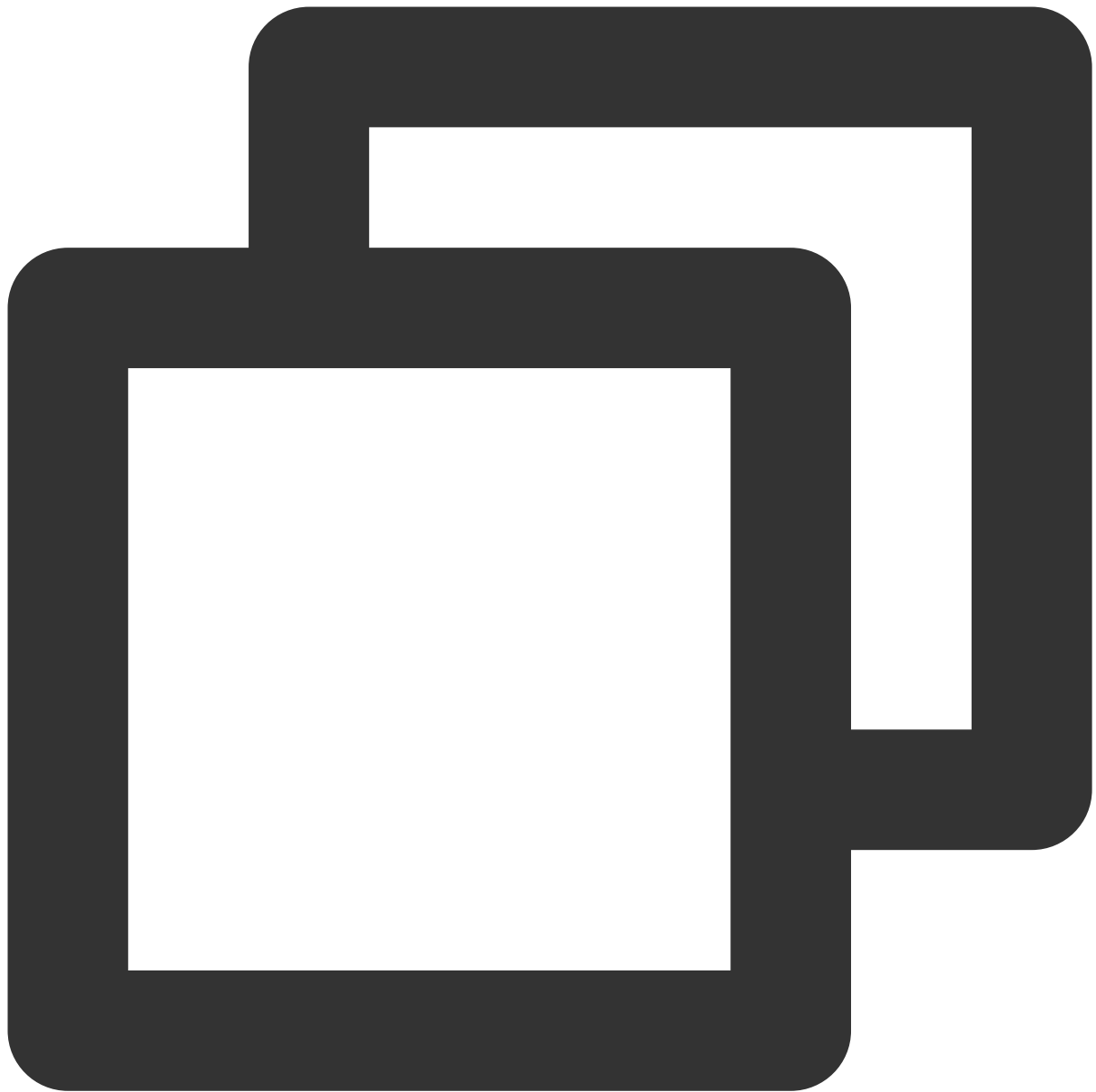


```
ps aux |grep receiver
```

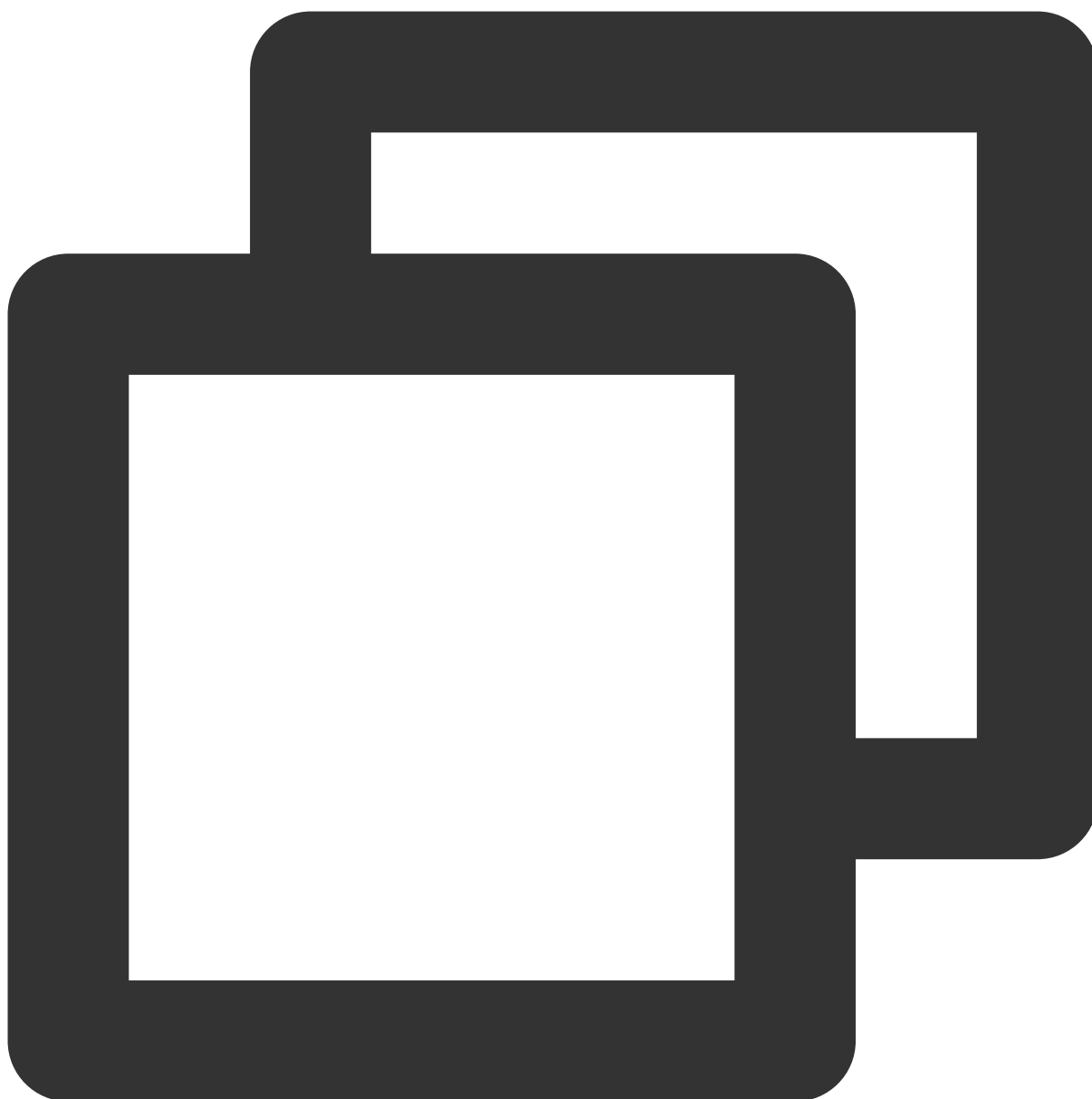
다음 결과가 반환되면 receiver 프로세스를 성공적으로 조회 가능함을 의미합니다.

```
[root@VM-5-88-centos ~]# ps aux | grep receiver
postgres  4688  0.0  0.0 369492  3272 ?        Ss   11:53   0:00 postgres: wal re
root      4789  0.0  0.0 112812   972 pts/0    S+   11:54   0:00 grep --color=aut
```

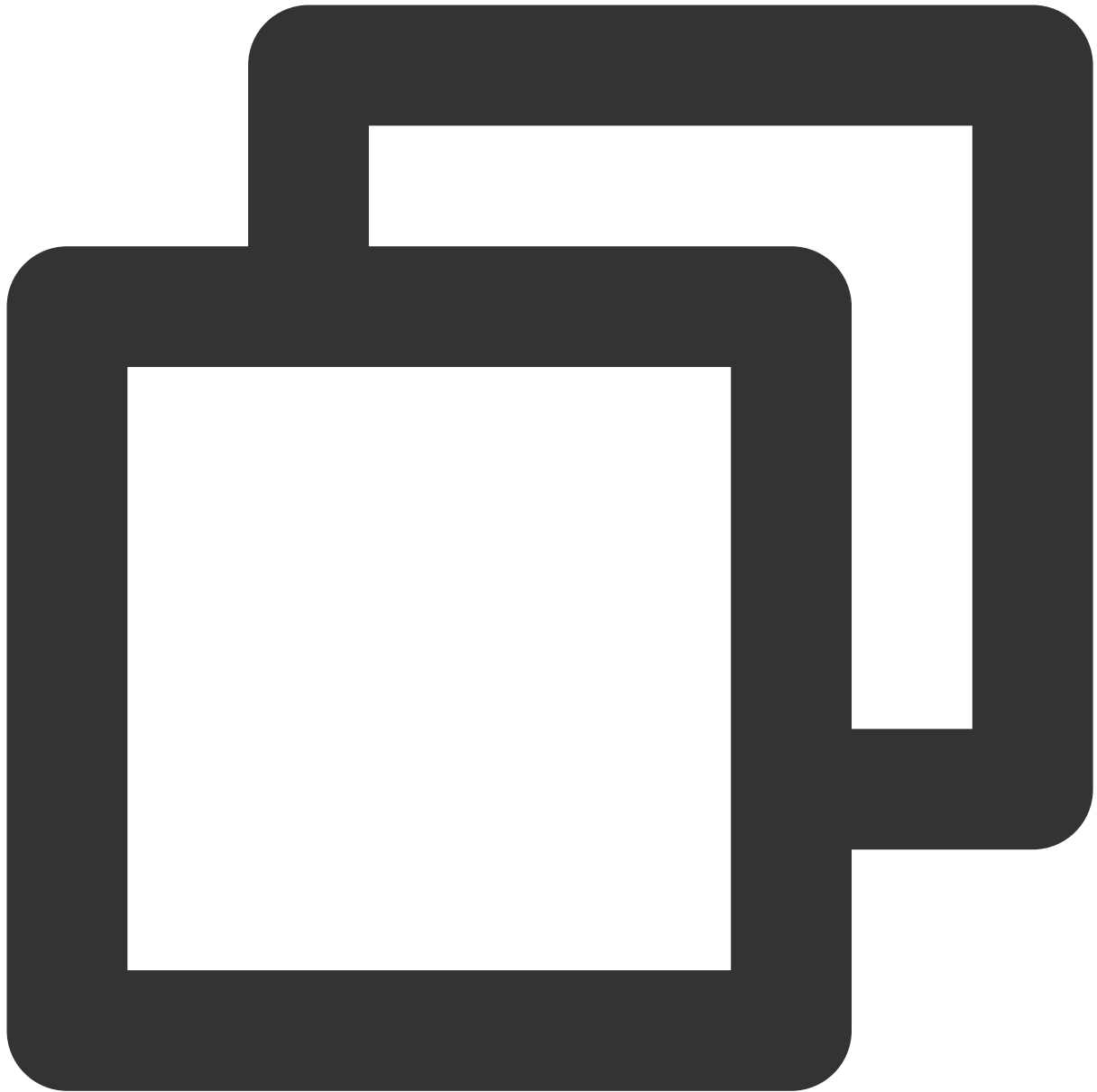
4. 프라이머리 노트에서 다음 명령을 순서대로 실행하여 PostgreSQL 인터랙티브 터미널로 이동하여 프라이머리 데이터베이스에서 세컨더리 데이터베이스 상태를 조회합니다.



```
su - postgres
```



```
psql
```



```
select * from pg_stat_replication;
```

다음 결과가 반환되면 세컨더리 데이터베이스 상태를 성공적으로 조회 가능함을 의미합니다.


```
postgres=# select * from pg_stat_replication;
 pid | usesysid | username | application_name | client_addr | client_hostname | client_port |
-----+-----+-----+-----+-----+-----+-----+
 3875 |    16384 | replica | walreceiver      | 114.117.197.144 |                |    44724   |
 76  |          |         |                  |              |                |           |
 2   | streaming | 0/3000AE0 | 0/3000AE0        | 0/3000AE0    | 0/3000AE0      |           |
(1 row)
```

Microsoft SharePoint 2016 구축

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

본 문서에서는 CVM 인스턴스에서 Microsoft SharePoint 2016을 구축하는 방법을 소개합니다.

소프트웨어

본 문서에서는 다음 하드웨어 사양의 CVM 인스턴스를 예시로 사용합니다.

vCPU: 4코어

메모리: 8GB

본 문서에서는 다음 소프트웨어 버전을 예시로 사용합니다.

운영 체제: Windows Server 2012 R2 데이터센터 64비트(영어)

데이터베이스: SQL Server 2014

전제 조건

Windows CVM을 구입했습니다. 아직 설정하지 않은 경우 [Windows CVM 커스텀 설정](#)을 참고하십시오.

작업 단계

1단계: Windows 인스턴스에 로그인

[RDP](#) 파일을 통한 [Windows](#) 인스턴스 로그인하거나 원격 데스크톱을 사용하여 [Windows](#) 인스턴스 로그인할 수 있습니다.

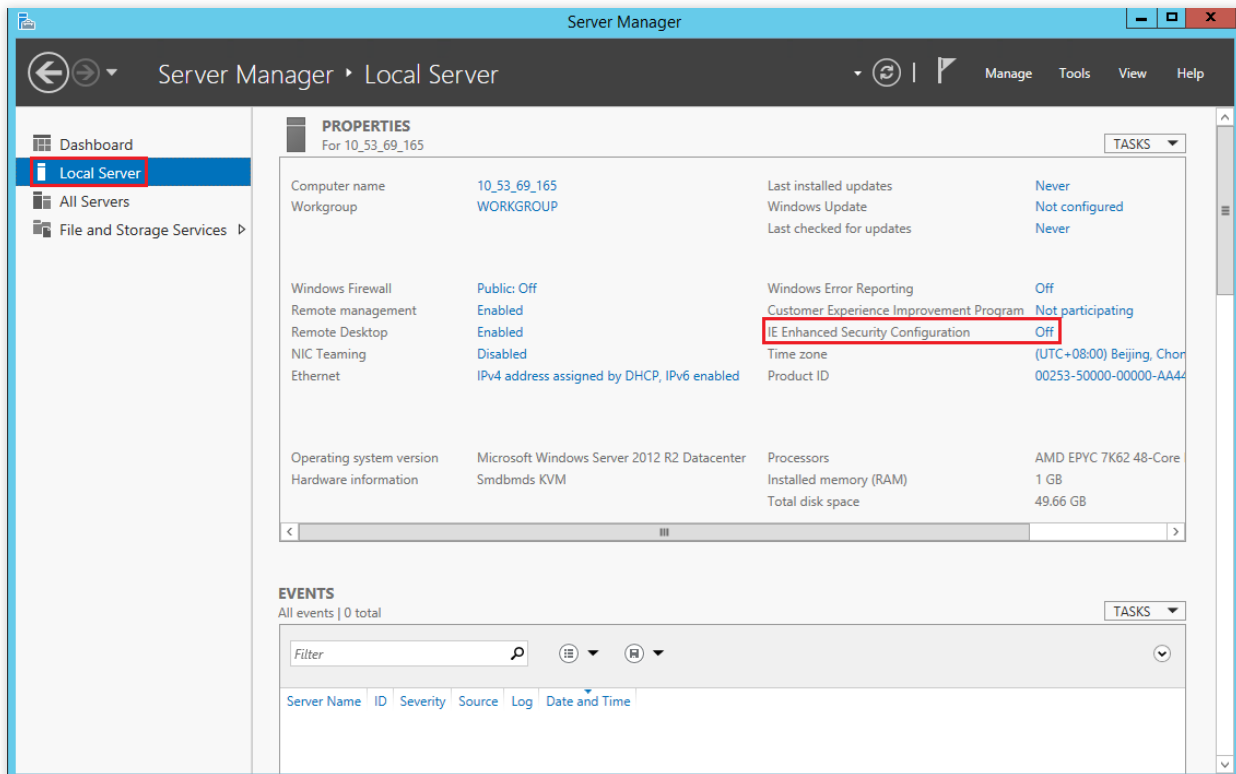
2단계: AD, DHCP, DNS 및 IIS 서비스 추가

1. 바탕 화면에서

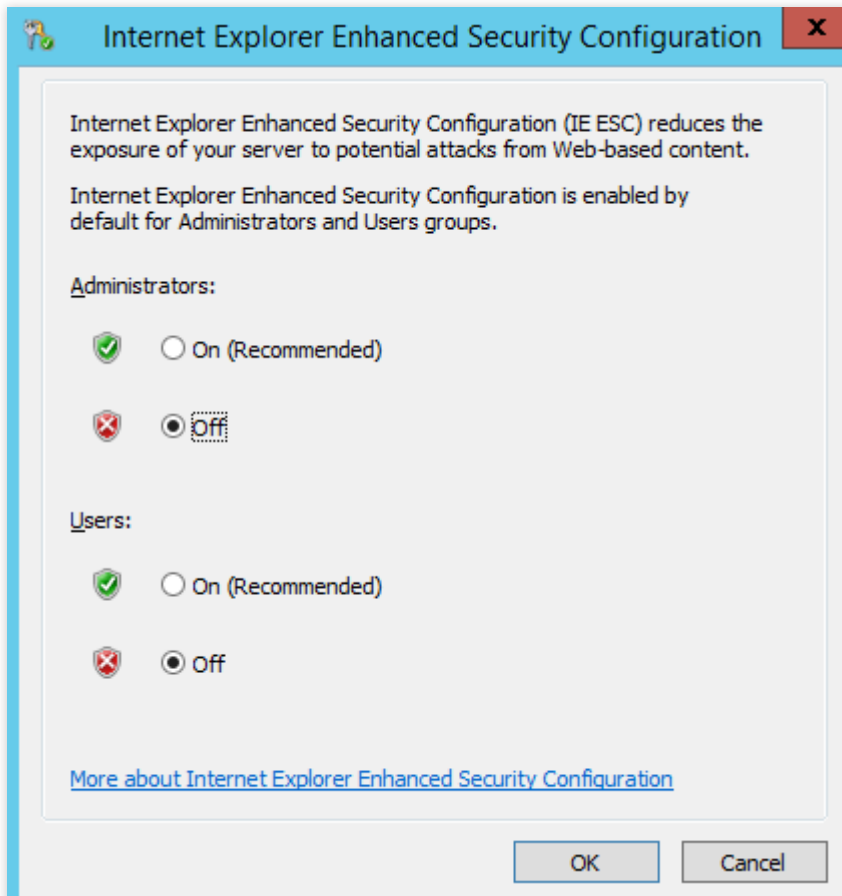


을(를) 클릭하여 서버 관리자를 엽니다.

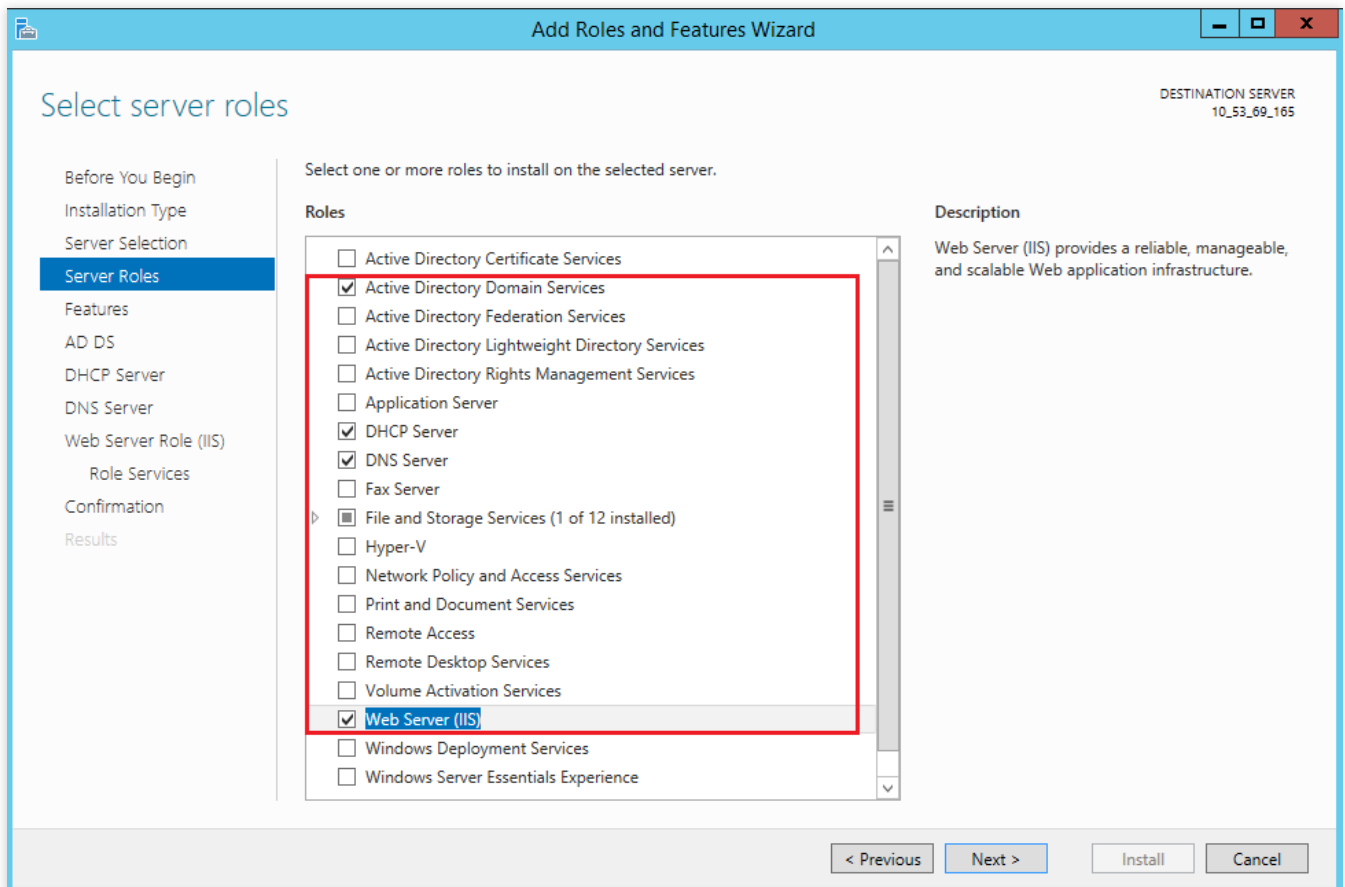
2. 왼쪽 사이드바에서 **로컬 서버**를 선택하고 아래와 같이 **IE 보안 강화 구성**을 찾습니다.



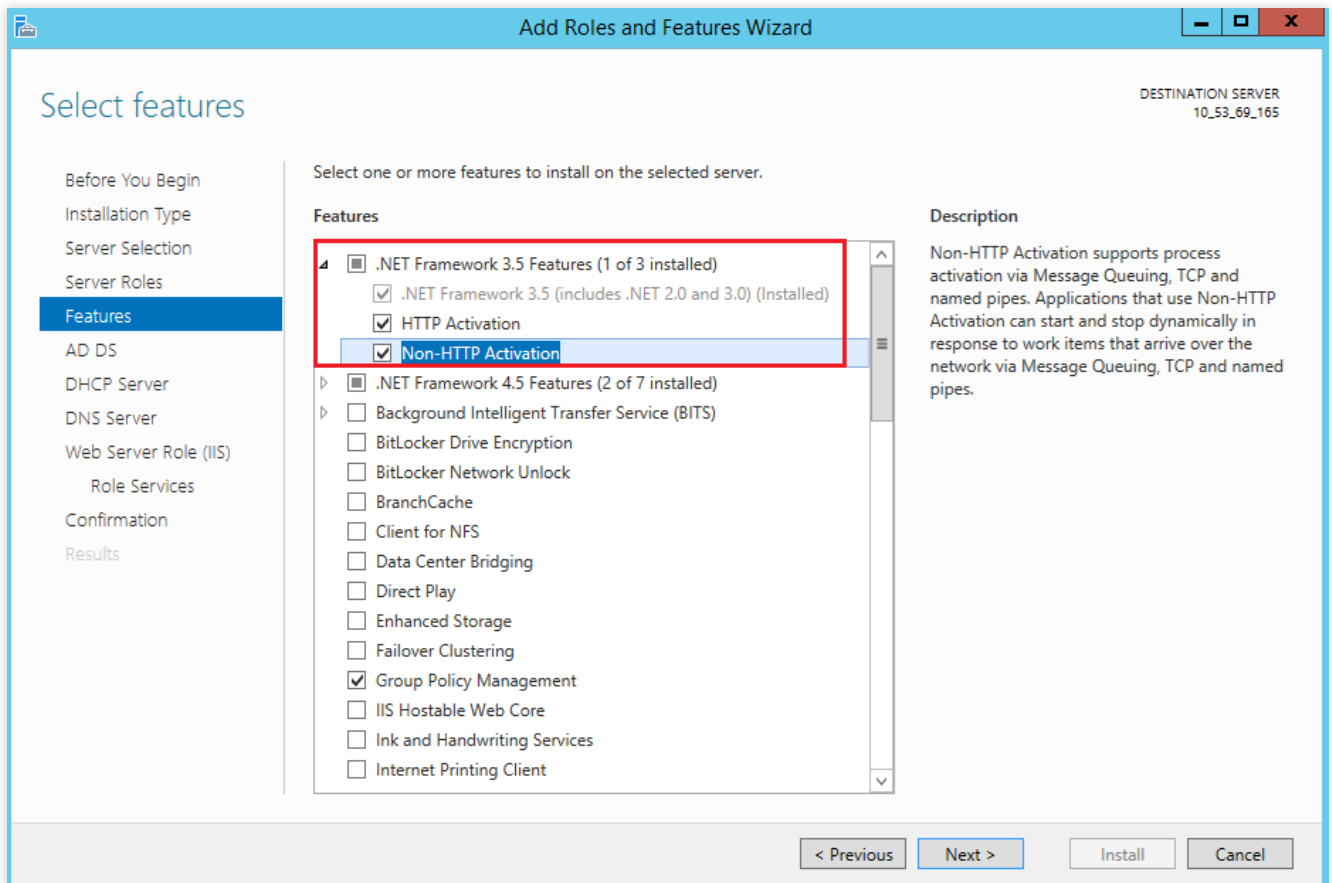
3. 아래와 같이 **IE 보안 강화 구성**을 비활성화합니다.



4. 왼쪽 사이드바에서 **대시보드**를 선택하고 **역할 및 기능 추가**를 클릭합니다.
5. '역할 및 기능 추가 마법사' 창에서 기본 구성을 유지하고 **다음**을 3번 클릭합니다.
6. '서버 역할' 페이지에서 **Active Directory 도메인 서비스**, **DHCP 서버**, **DNS 서버**, ****Web 서버(IIS)****를 선택하고 아래와 같이 팝업 창에서 **기능 추가**를 클릭합니다.



7. **다음**을 클릭합니다.
8. '기능' 페이지에서 '.NET Framework 3.5 기능'을 선택하여 아래와 같이 **기능 추가**를 클릭합니다.



9. 기본 구성을 유지하고 확인 페이지가 나타날 때까지 **다음**을 클릭합니다.

10. 설치를 확인하고 **설치**를 클릭합니다.

11. 설치가 완료되면 CVM을 다시 시작합니다.

3단계: AD 서비스 구성

1. 바탕 화면에서

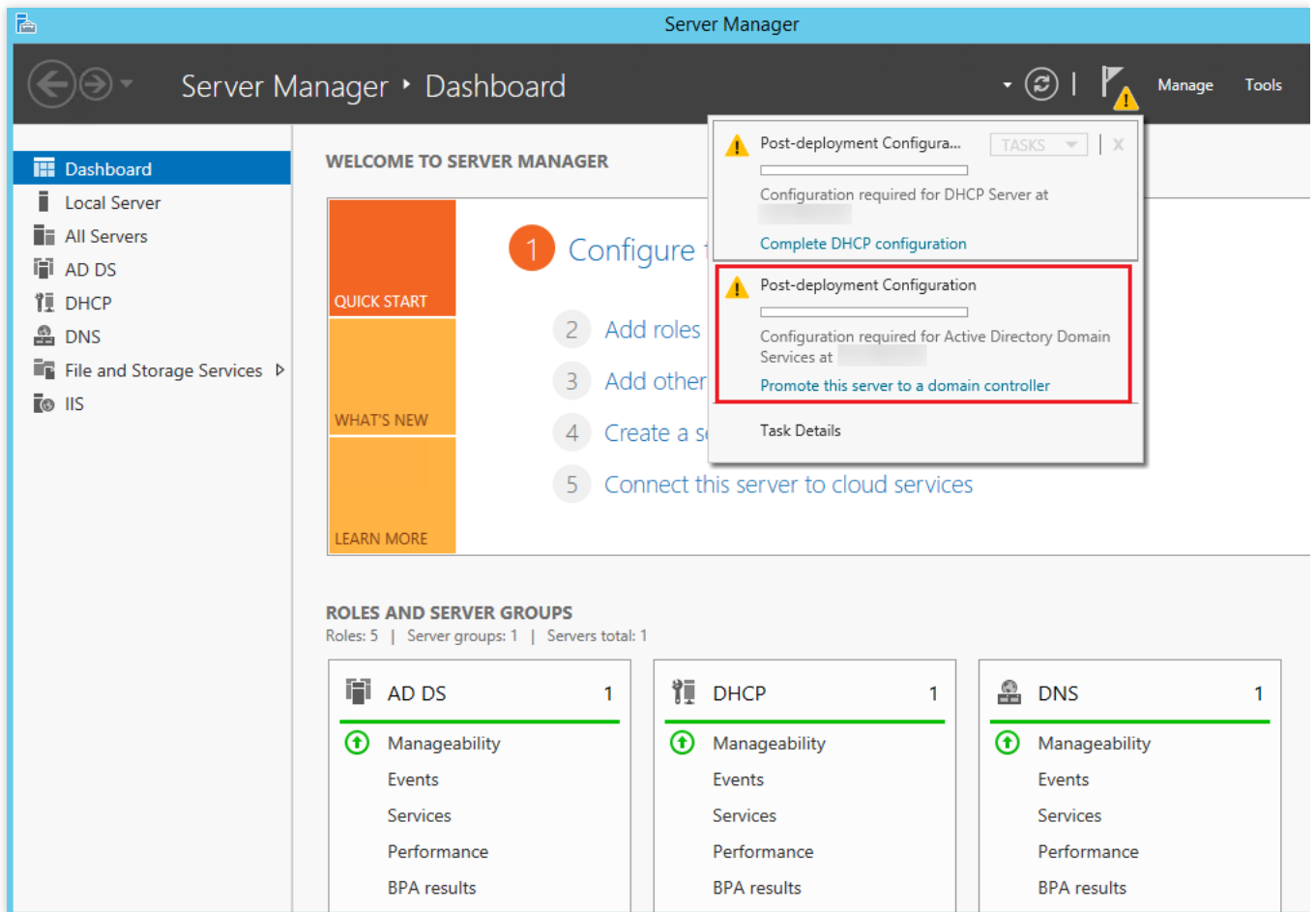


을(를) 클릭하여 서버 관리자를 엽니다.

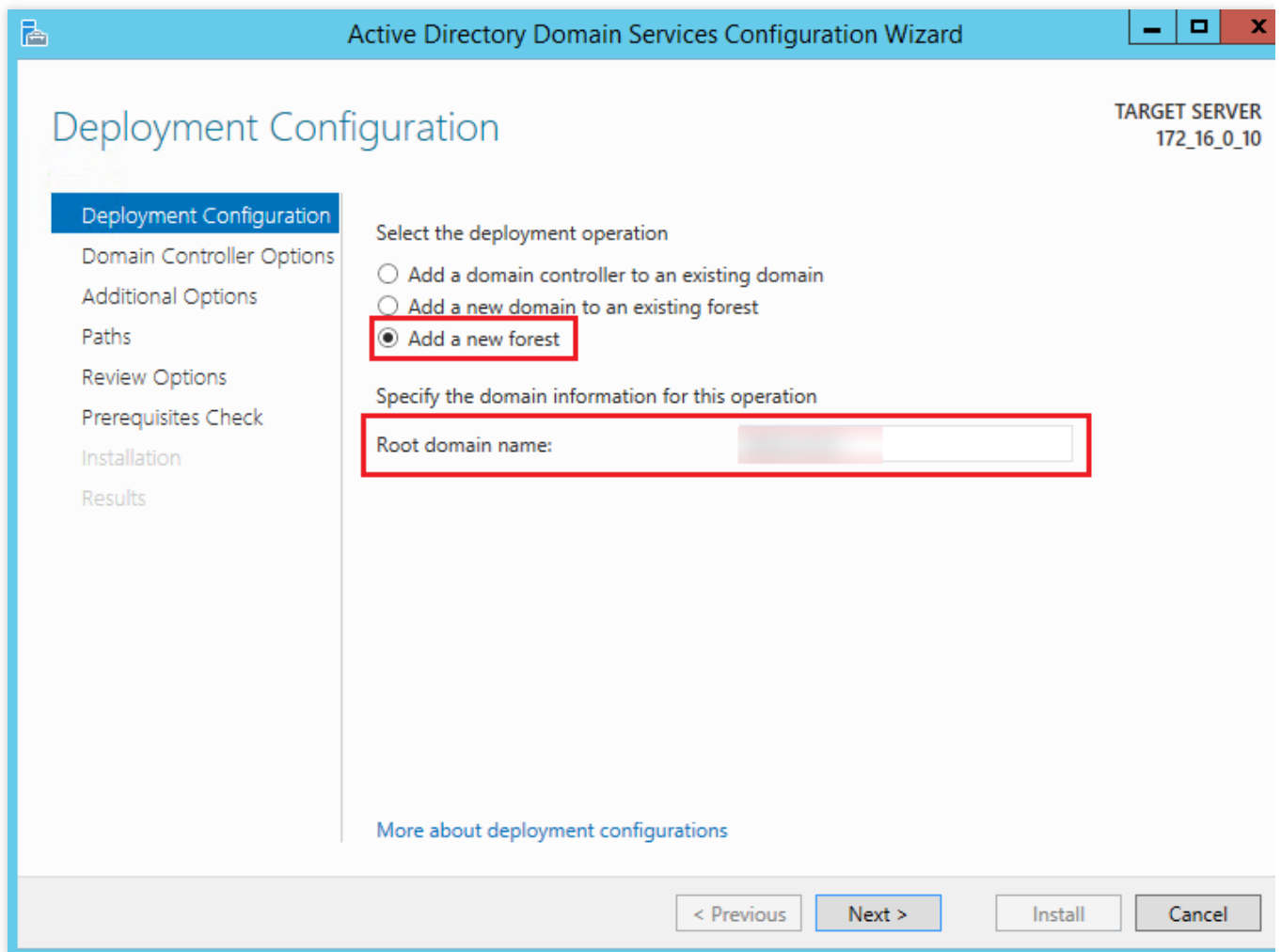
2.



을(를) 클릭하여 아래와 같이 이 서버를 도메인 컨트롤러로 승격을 선택합니다.



3. 열린 'Active Directory 도메인 서비스 설정 마법사' 창에서 **새 포리스트 추가**를 선택하고 루트 도메인 이름 필드에 도메인 이름을 입력한 후 **다음**을 클릭합니다.



4. DSRM(디렉터리 서비스 복원 모드) 암호를 설정하고 다음을 클릭합니다.

5. 기본 구성을 유지하고 구성이 완료될 때까지 **다음**을 클릭합니다.

6. **설치**를 클릭합니다.

4단계: DHCP 서비스 구성

1. 바탕 화면에서

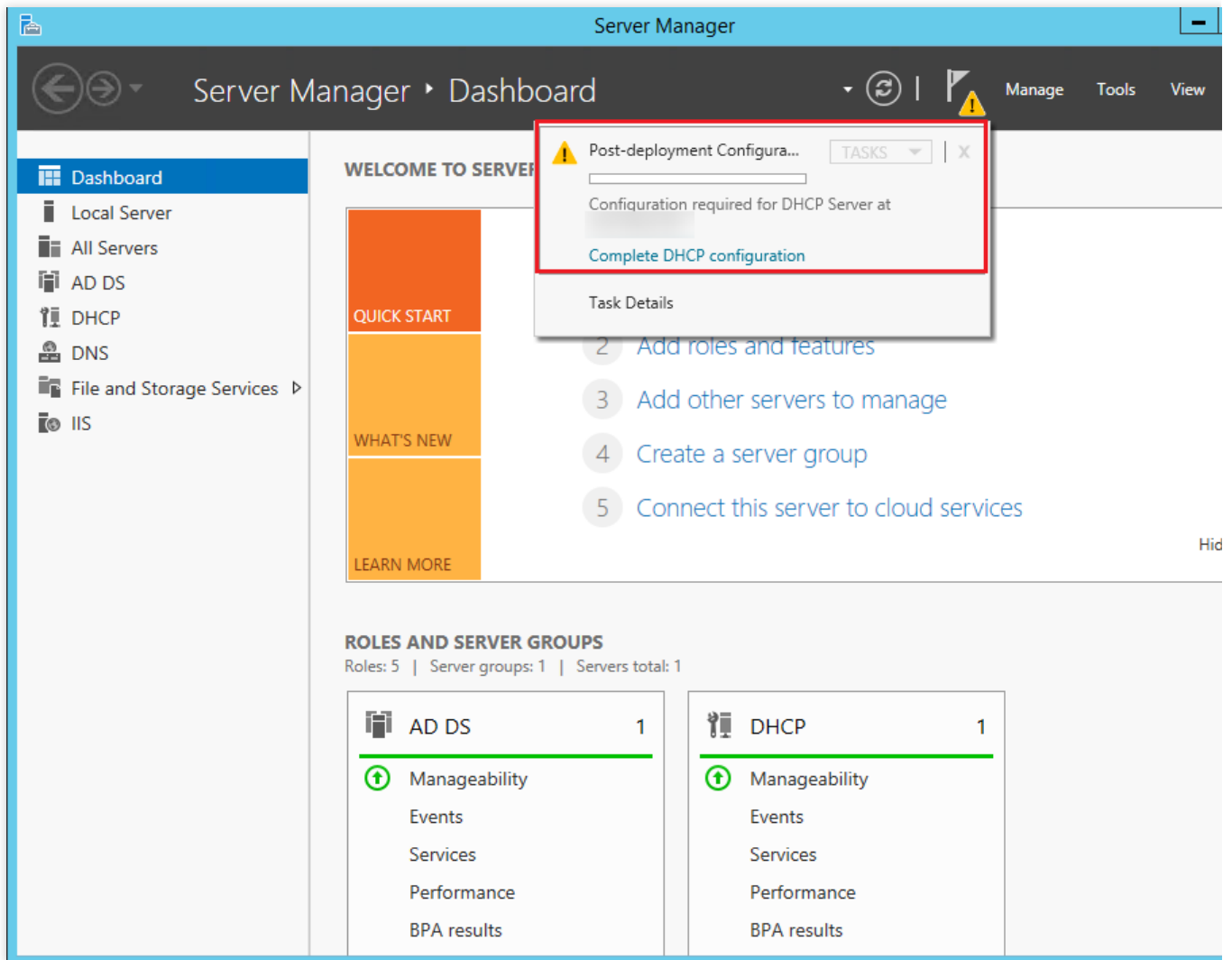


을(를) 클릭하여 서버 관리자를 엽니다.

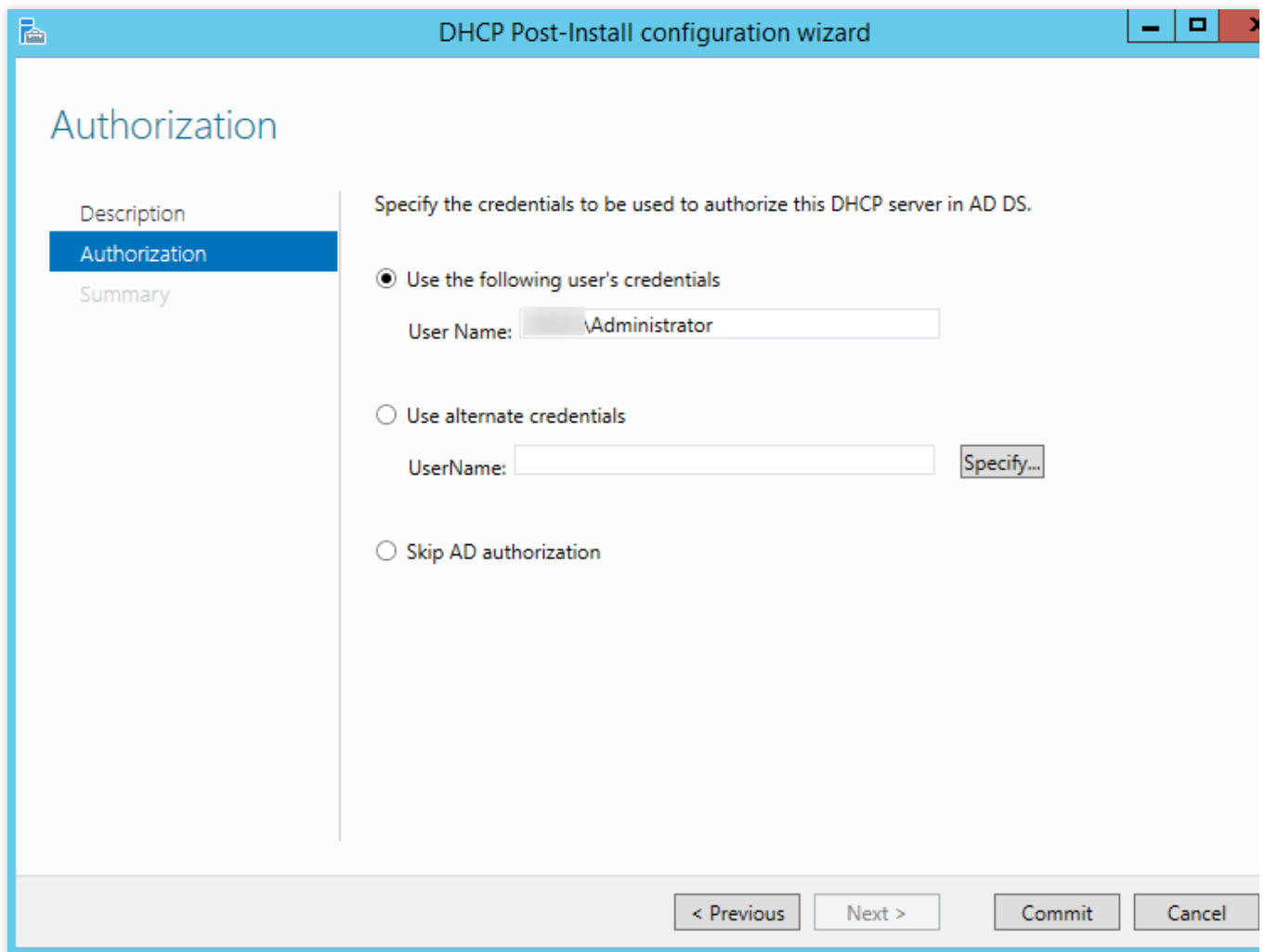
2.



을(를) 클릭하여 아래와 같이 **DHCP 구성 완료**를 선택합니다.



3. 'DHCP 설치 후 설정 마법사' 창에서 다음을 클릭합니다.
4. 기본 구성을 유지하고 커밋을 클릭하여 설치를 완료합니다.



5. 닫기를 클릭합니다.

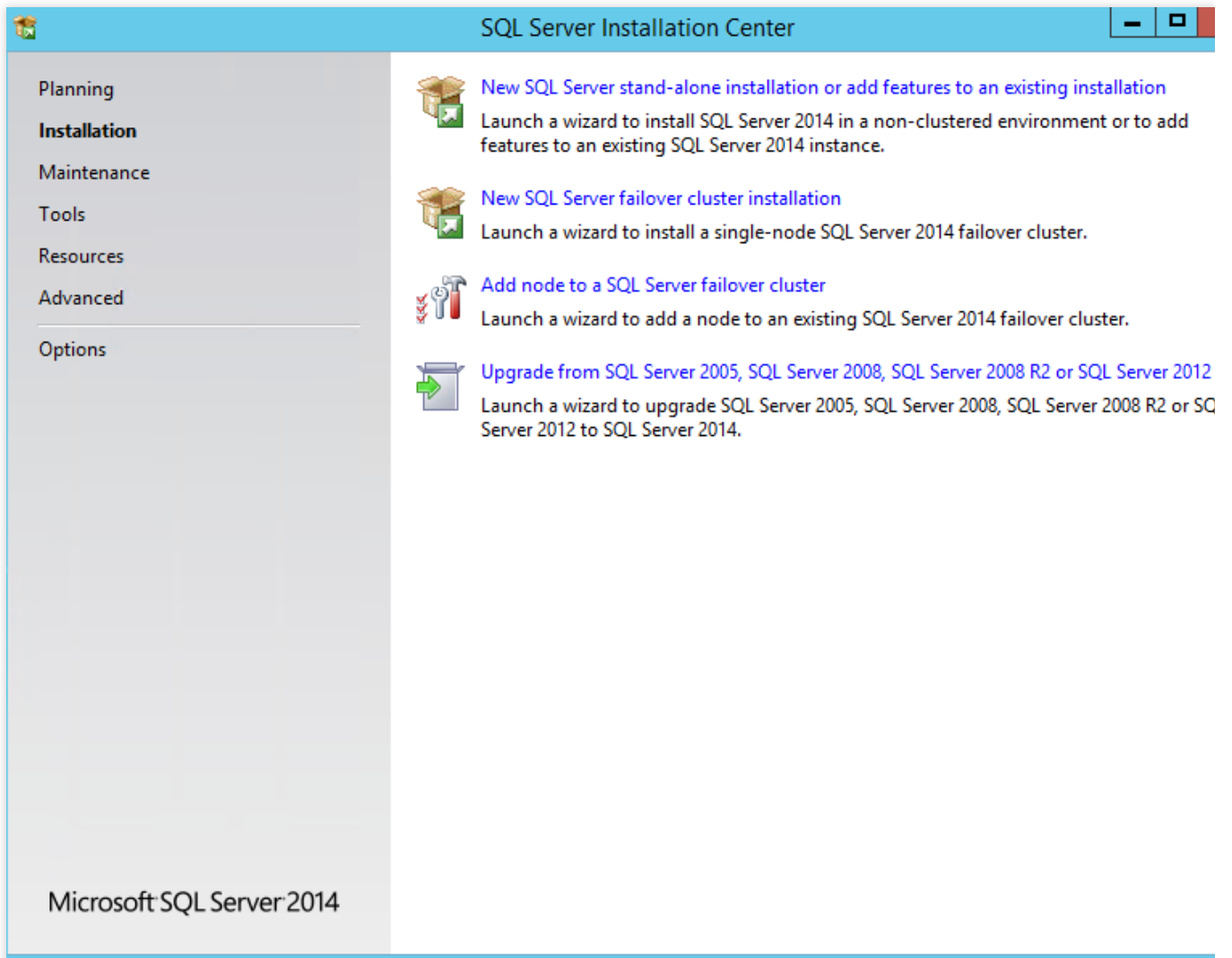
5단계: SQL Server 2014 데이터베이스 설치

1. CVM에서 브라우저를 열고 SQL Server 2014 공식 사이트에서 SQL Server 2014 설치 패키지를 다운로드합니다.

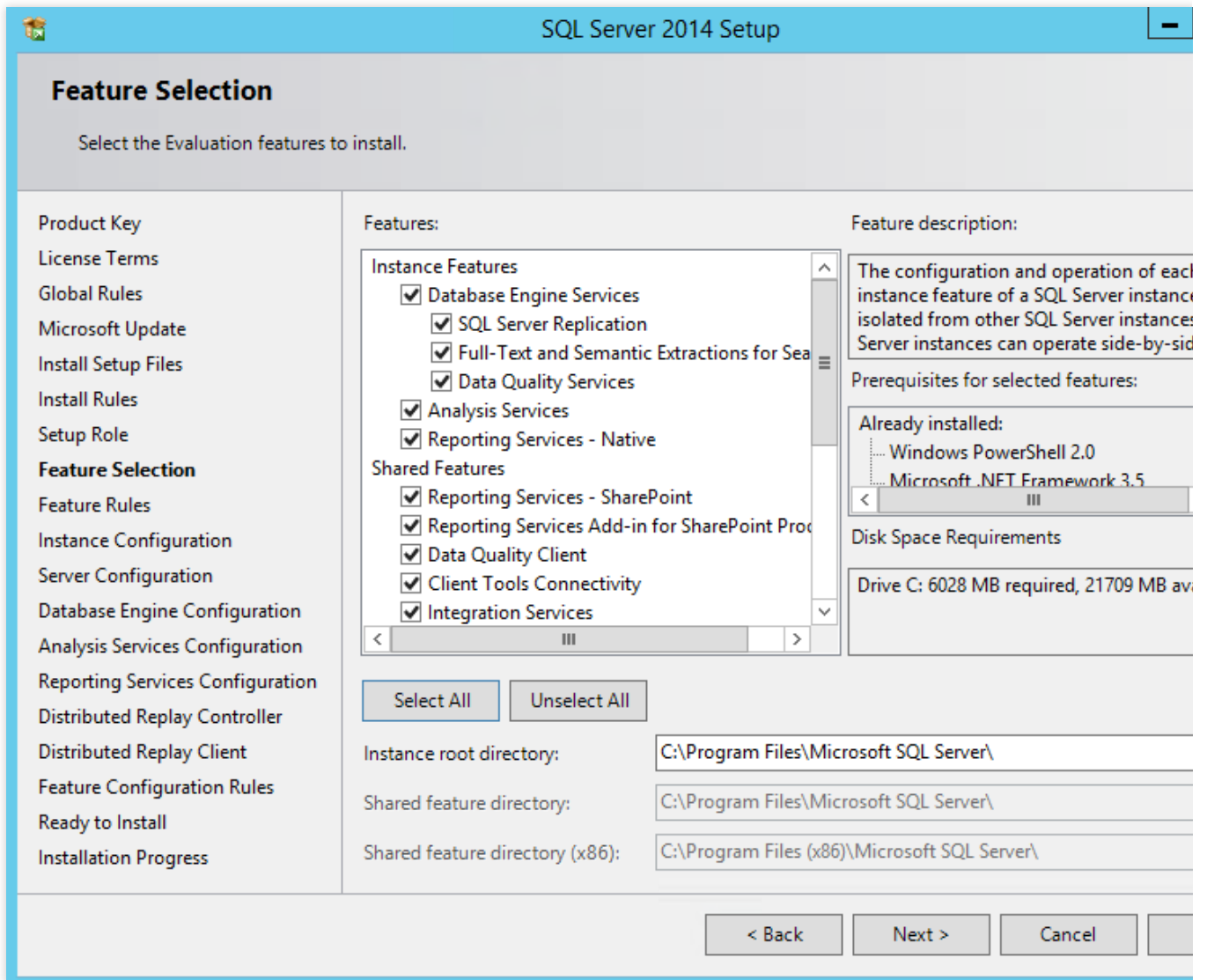
설명 :

3rd party 웹 사이트 또는 기타 유효한 채널에서 SQL Server 2014 설치 패키지를 얻을 수도 있습니다.

2. 아래와 같이 'Setup.exe' 파일을 더블클릭하여 설치 마법사를 시작하여 새 SQL Server 독립 실행형 설치 또는 기능 추가를 클릭합니다.



3. 제품 키 페이지에서 제품 키를 입력하고 **다음**을 클릭합니다.
4. '사용 조건에 동의합니다'를 선택하고 **다음**을 클릭합니다.
5. 기본 구성을 유지하고 **다음**을 클릭합니다.
6. 설치 확인이 완료되면 **다음**을 클릭합니다.
7. 기본 구성을 유지하고 **다음**을 클릭합니다.
8. '기능 선택' 페이지에서 **모두 선택**을 클릭하여 모든 기능을 선택하고 **다음**을 클릭합니다.



9. '인스턴스 구성' 페이지에서 기본 인스턴스를 선택하고 다음을 클릭합니다.

SQL Server 2014 Setup

Instance Configuration

Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.

Product Key
License Terms
Global Rules
Microsoft Update
Install Setup Files
Install Rules
Setup Role
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Analysis Services Configuration
Reporting Services Configuration
Distributed Replay Controller
Distributed Replay Client
Feature Configuration Rules
Ready to Install
Installation Progress

☒ **Default instance**

☐ Named instance:

Instance ID:

SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL12.MSSC

Analysis Services directory: C:\Program Files\Microsoft SQL Server\MSAS12.MSSQL

Reporting Services directory: C:\Program Files\Microsoft SQL Server\MSRS12.MSSQL

Installed instances:

Instance Name	Instance ID	Features	Edition
---------------	-------------	----------	---------

< Back
Next >
Cancel

10. '서버 구성' -> 서비스 계정 페이지에서 SQL Server 데이터베이스 엔진 및 SQL Server Analysis Services에 대한 계정과 암호를 구성하고 **다음**을 클릭합니다.

SQL Server 2014 Setup

Server Configuration

Specify the service accounts and collation configuration.

Product Key
License Terms
Global Rules
Microsoft Update
Install Setup Files
Install Rules
Setup Role
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Analysis Services Configuration
Reporting Services Configuration
Distributed Replay Controller
Distributed Replay Client
Feature Configuration Rules
Ready to Install
Installation Progress

Service Accounts Collation

Microsoft recommends that you use a separate account for each SQL Server service.

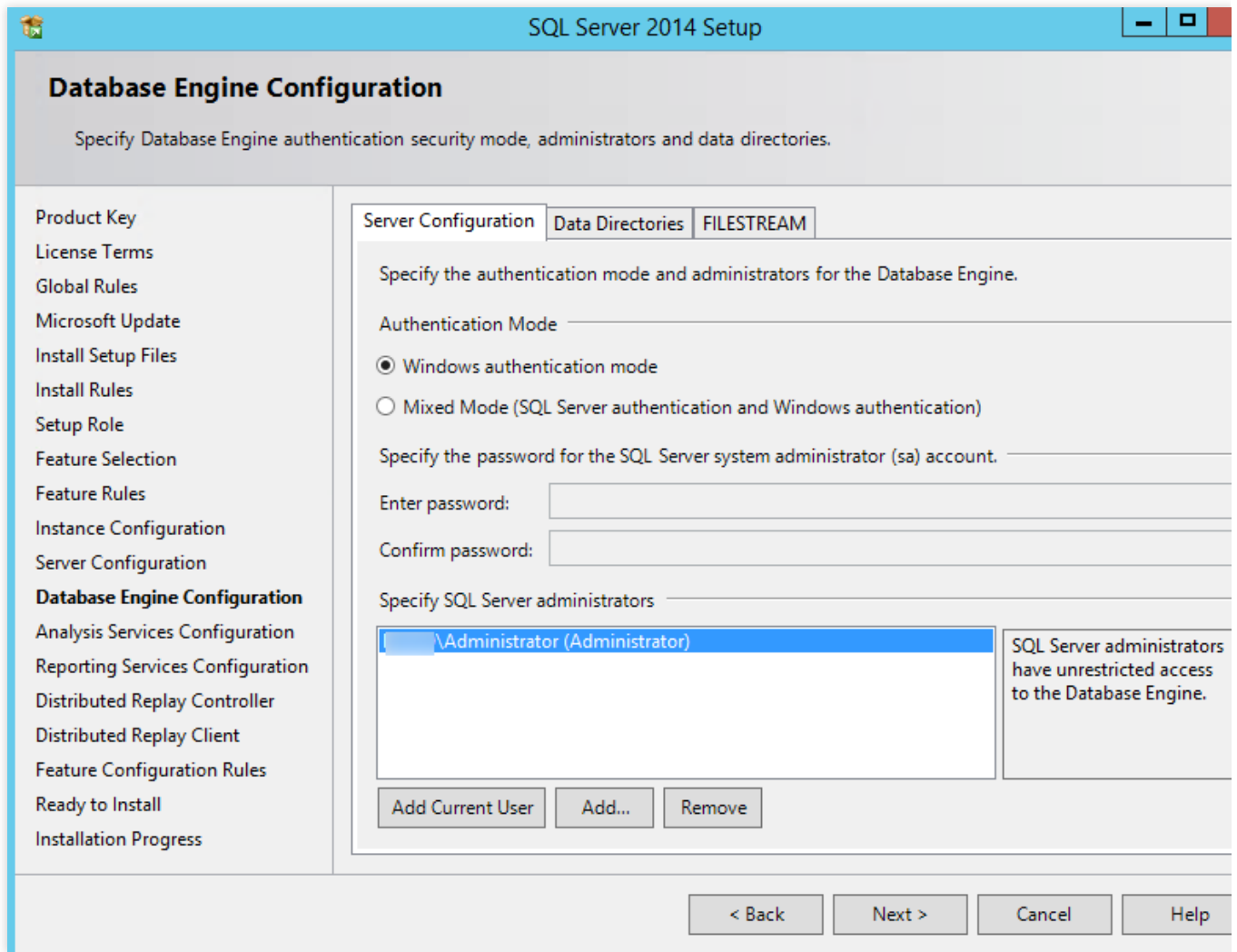
Service	Account Name	Password
SQL Server Agent	NT Service\SQLSERVERA...	
SQL Server Database Engine	NT Service\MSSQLSERVER	
SQL Server Analysis Services		
SQL Server Reporting Services	NT Service\ReportServer	
SQL Server Integration Services 12.0	NT Service\MsDtsServer...	
SQL Server Distributed Replay Client	NT Service\SQL Server D...	
SQL Server Distributed Replay Con...	NT Service\SQL Server D...	
SQL Full-text Filter Daemon Launc...	NT Service\MSSQLFDLa...	
SQL Server Browser	NT AUTHORITY\LOCAL ...	

< Back Next > Cancel

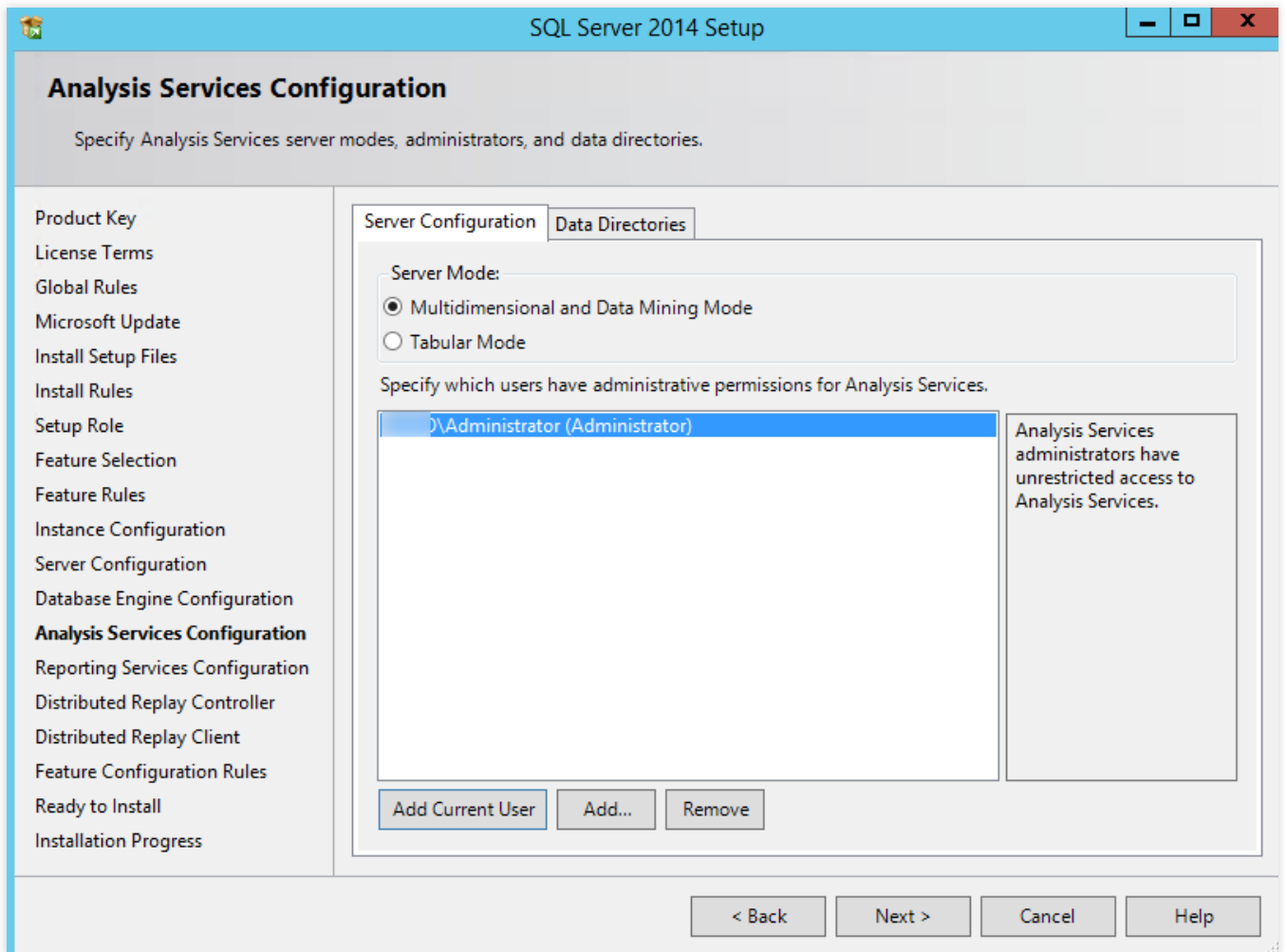
'SQL Server 데이터베이스 엔진'의 계정 이름을 'NT AUTHORITY\NETWORK SERVICE'로 설정합니다.

'SQL Server Analysis Services'의 계정 이름과 암호를 2단계: AD, DHCP, DNS 및 IIS 서비스 추가에서 14 - 15에서 구성한 도메인 이름과 암호로 설정합니다.

11. '데이터베이스 엔진 구성' -> 서버 구성 페이지에서 **현재 사용자 추가**를 선택하여 현재 계정을 SQL Server의 관리자 계정으로 사용하고 **다음**을 클릭합니다.

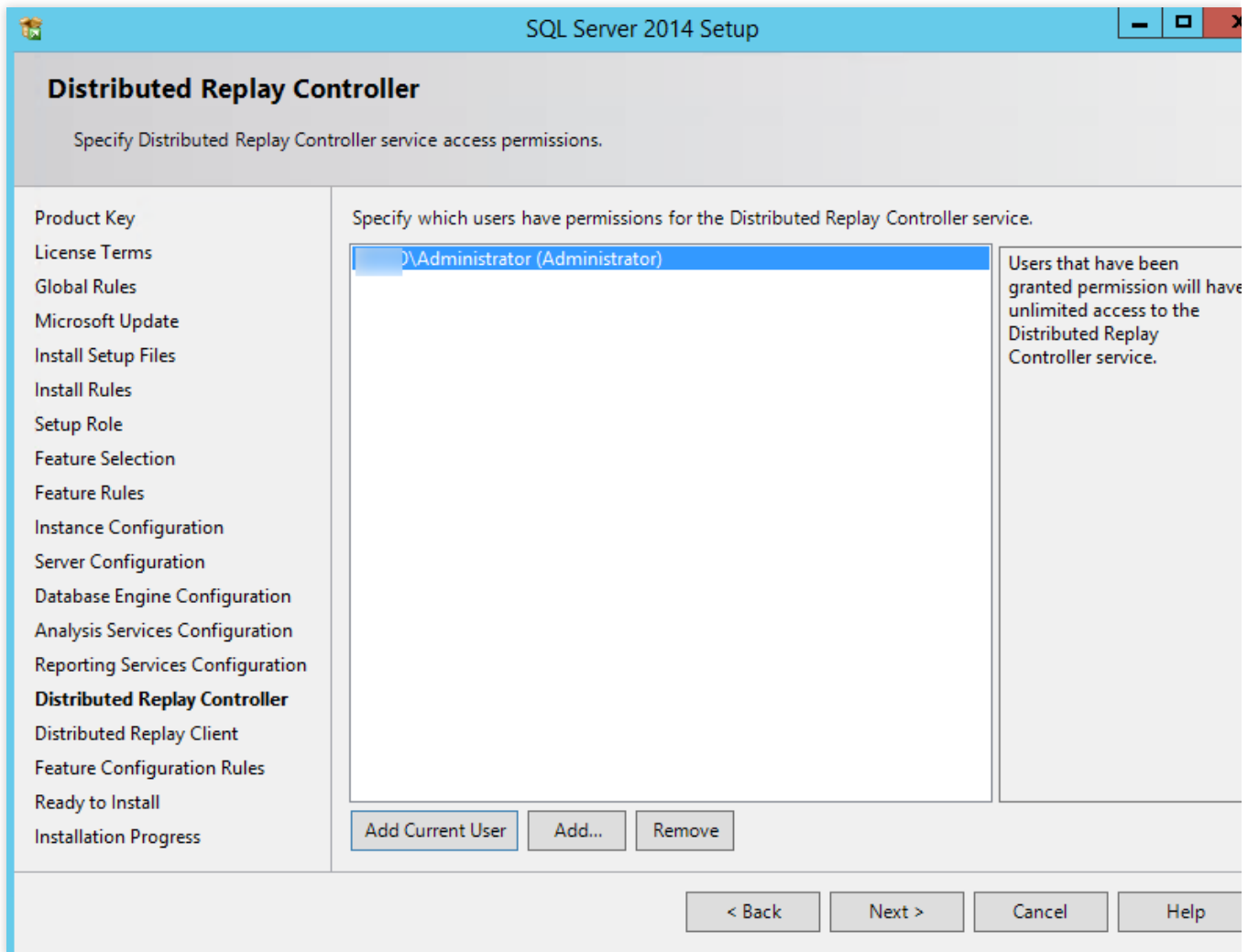


12. 'Analysis Services 구성' -> 계정 프로비저닝 페이지에서 **현재 사용자 추가**를 선택하여 현재 계정에 Analysis Services에 대한 관리자 권한을 부여하고 **다음**을 클릭합니다.



13. 기본 구성을 유지하고 **다음**을 클릭합니다.

14. 아래와 같이 'Distributed Replay Controller' 페이지에서 **현재 사용자 추가**를 클릭하여 현재 계정에 Distributed Replay 컨트롤러 서비스에 대한 액세스 권한을 부여합니다. **다음**을 클릭합니다.



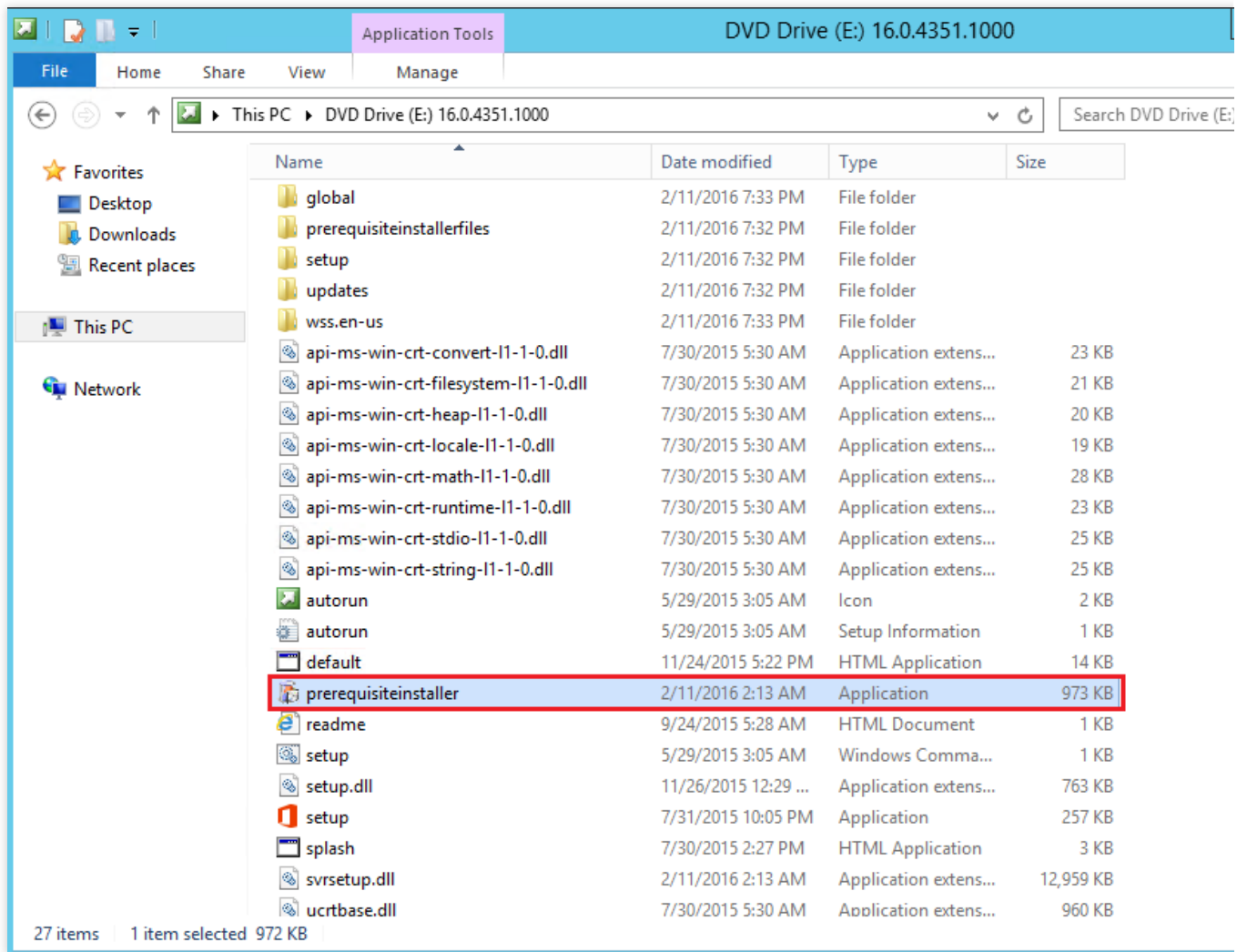
15. 기본 구성을 유지하고 설치가 완료될 때까지 **다음**을 클릭합니다.

4단계: SharePoint 2016 설치

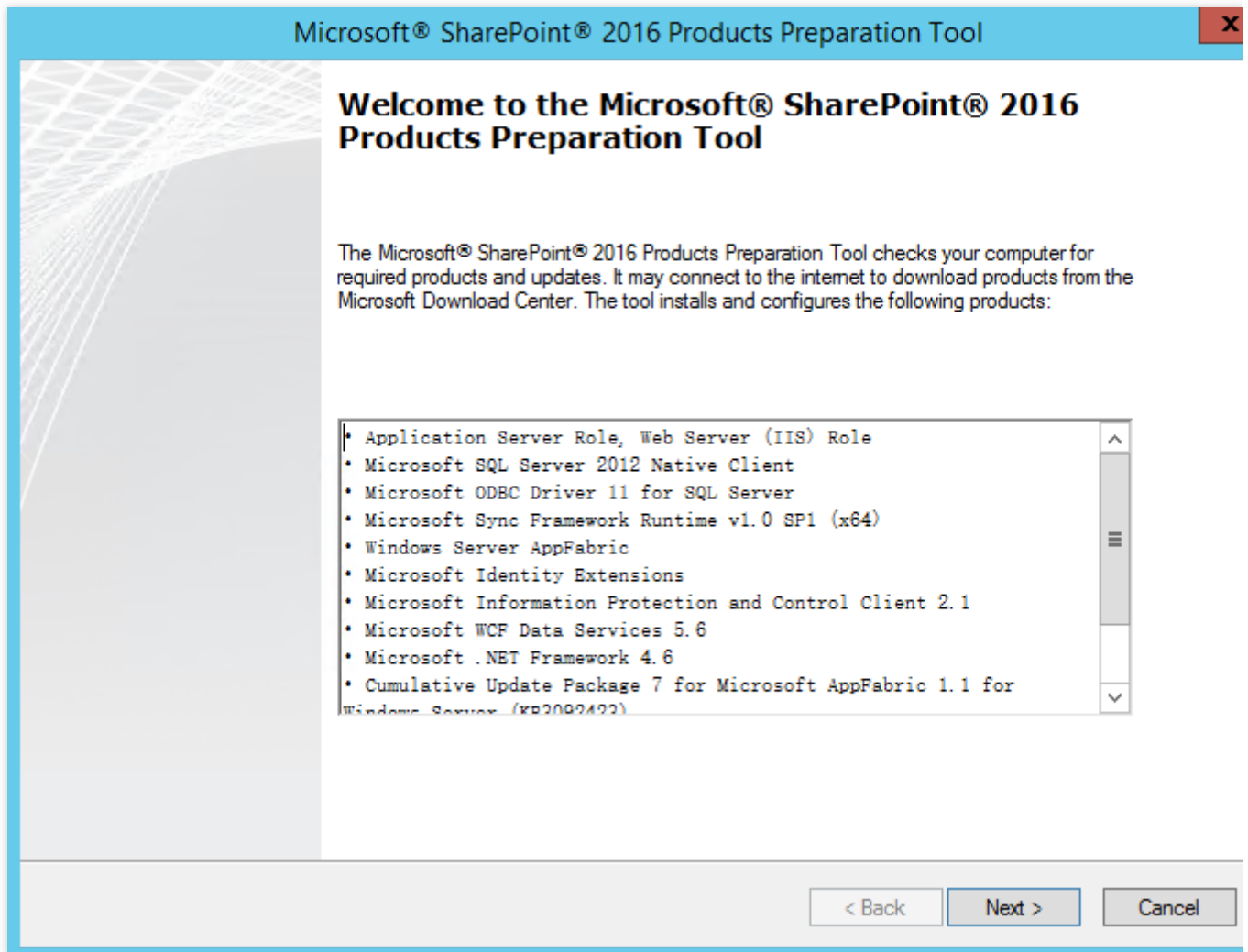
1. CVM에서 브라우저를 열고 Microsoft SharePoint 2016 공식 사이트에서 Microsoft SharePoint 2016 설치 패키지를 다운로드합니다.

2. Microsoft SharePoint 2016 이미지 파일을 열고 아래와 같이 준비 도구의 실행 파일

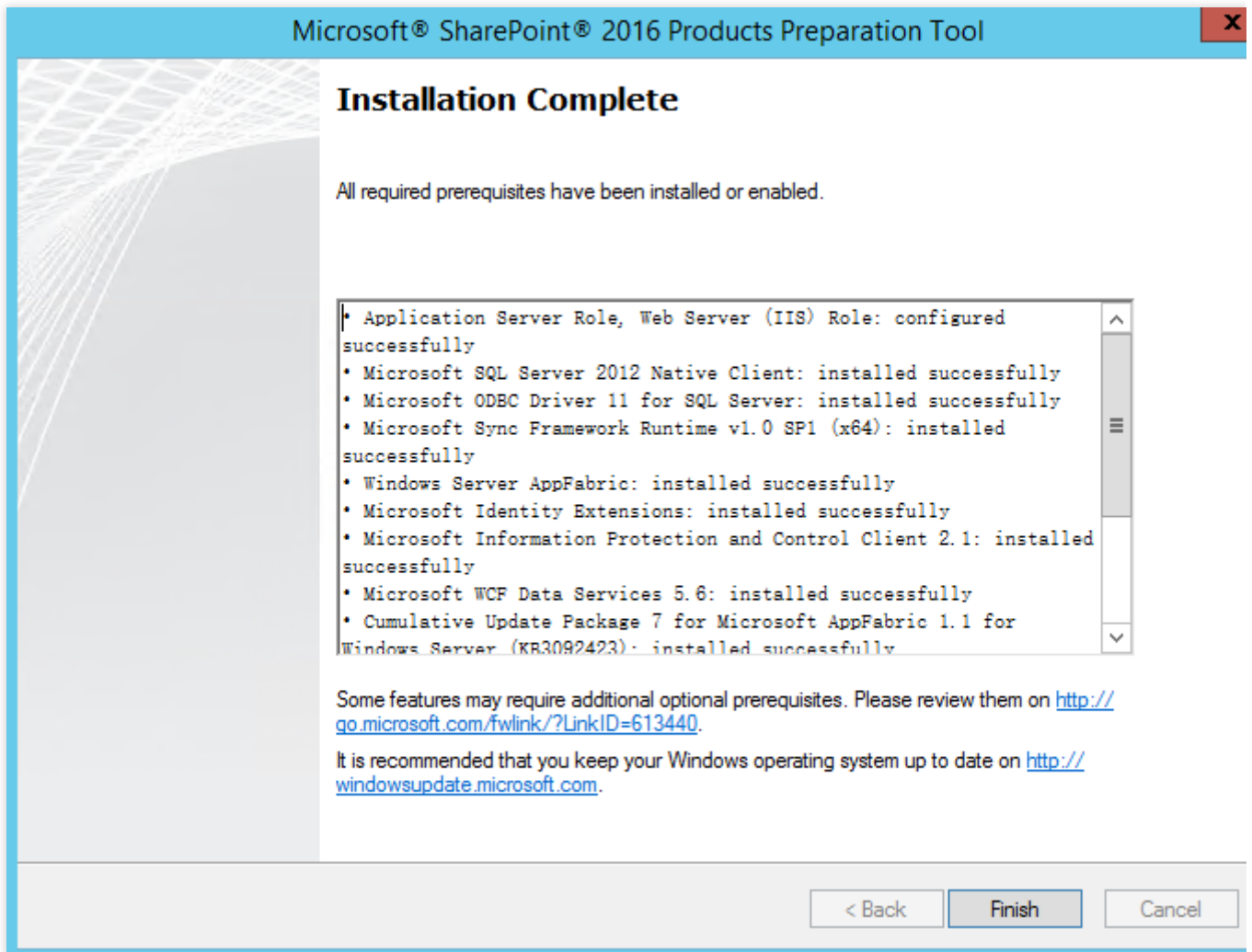
`prerequisiteinstaller.exe` 를 더블클릭하여 Microsoft SharePoint 2016 준비 도구를 설치합니다.



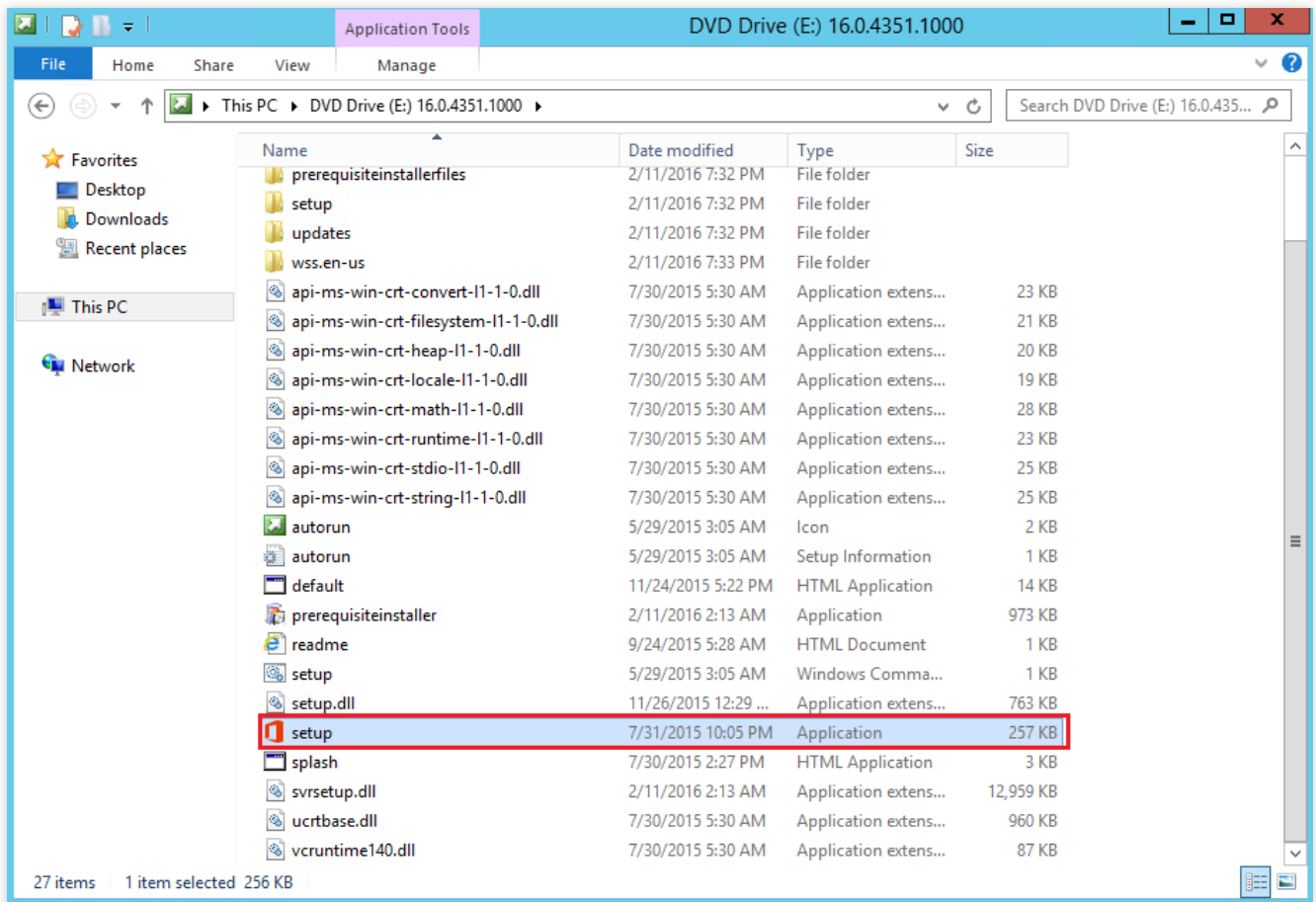
3. Microsoft SharePoint 2016 준비 도구의 설치 마법사를 열고 다음을 클릭합니다.



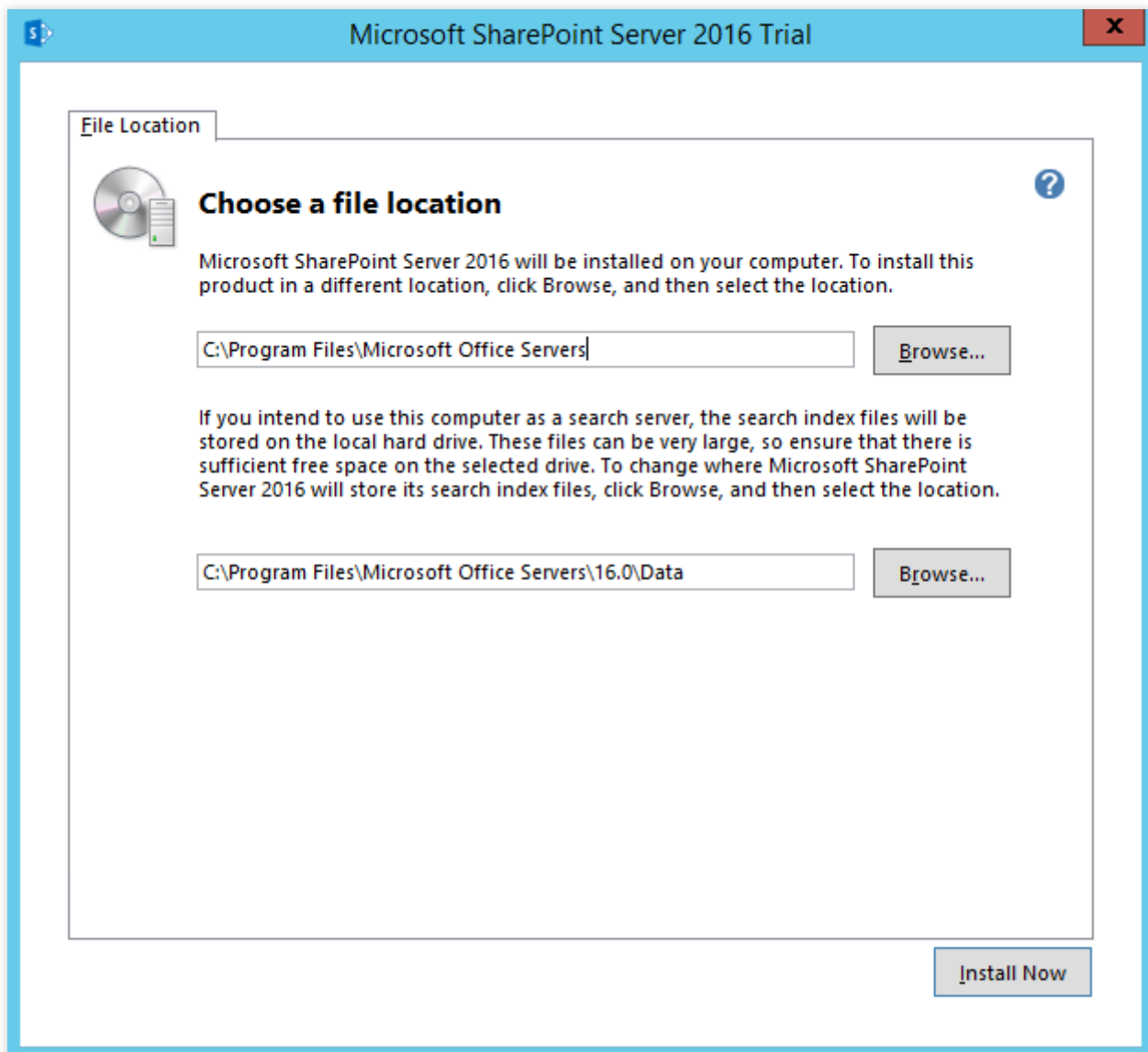
4. '사용권 계약 조건에 동의합니다'를 선택하고 **다음**을 클릭합니다.
5. 준비 도구가 설치된 후 **완료**를 클릭하여 CVM을 다시 시작합니다.



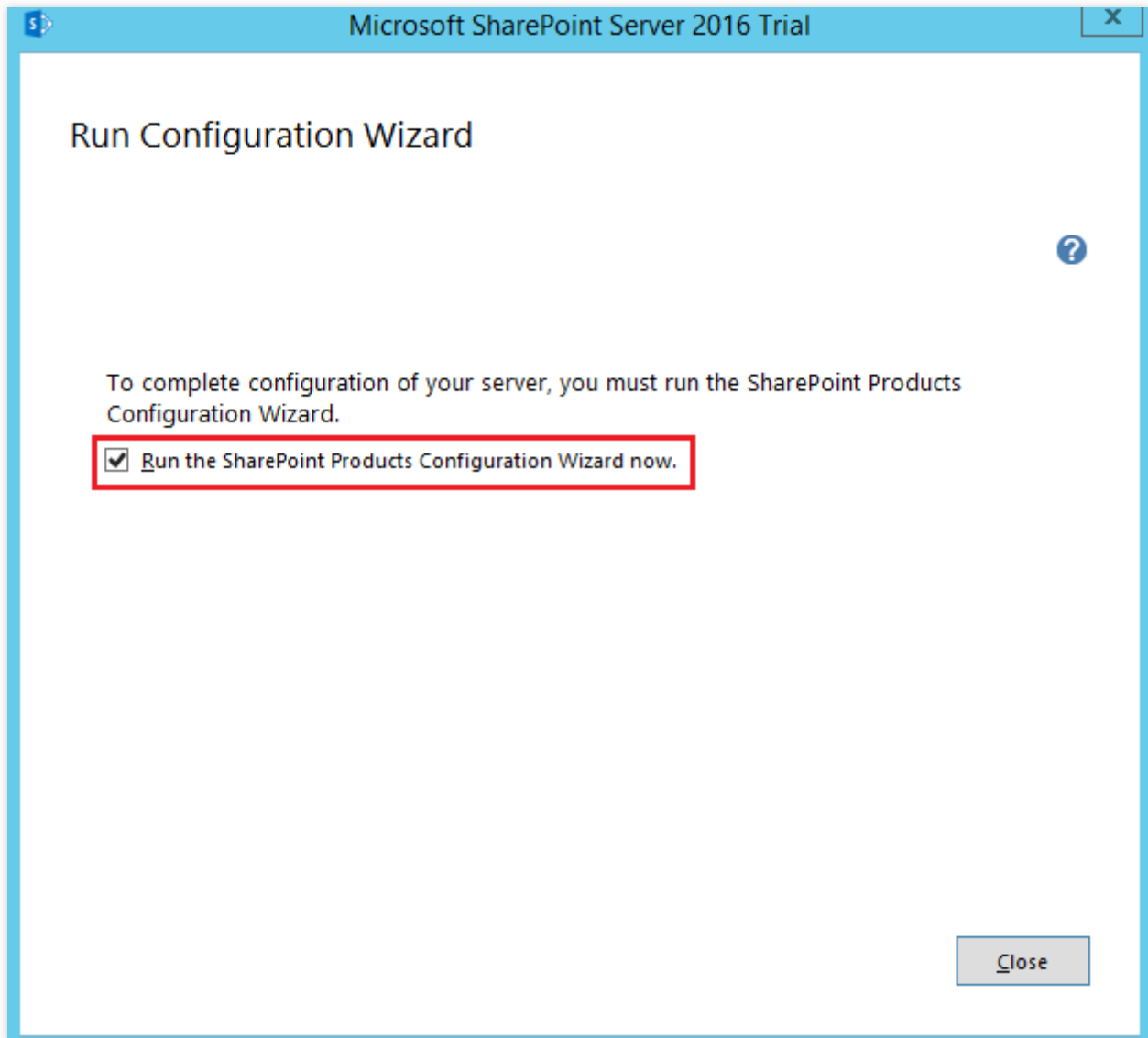
6. Microsoft SharePoint 2016 이미지 파일을 열고 설치 파일 `setup.exe` 를 더블클릭하여 Microsoft SharePoint 2016을 설치합니다.



7. 제품 키를 입력하고 **계속**을 클릭합니다.
8. '이 계약 조건에 동의합니다'를 선택하고 **계속**을 클릭합니다.
9. 설치 디렉터리를 선택하고(이 예시에서는 기본 구성을 유지하지만 필요에 따라 디렉터리를 지정할 수 있음) **지금 설치**를 클릭합니다.

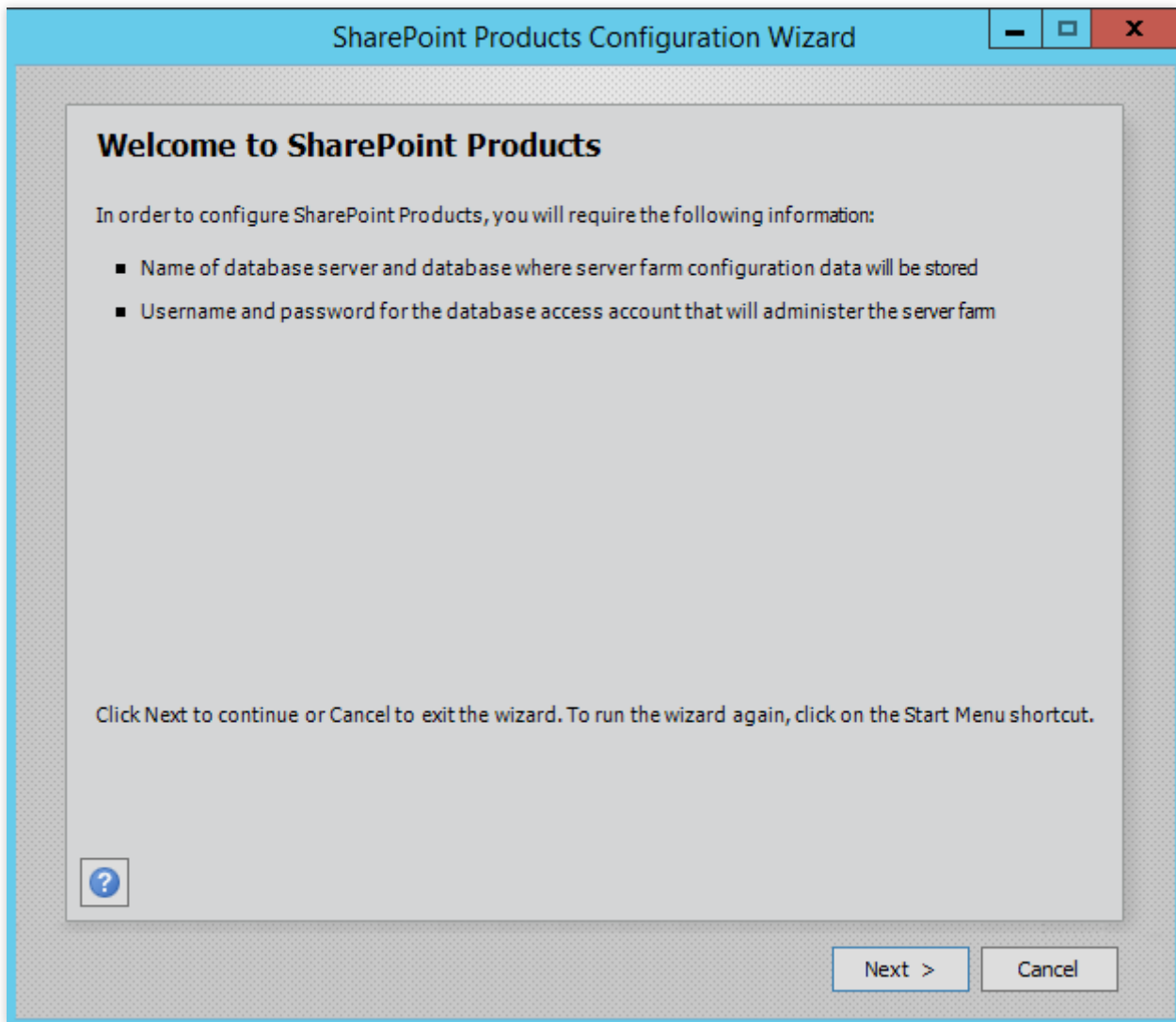


10. 설치가 완료되면 '지금 SharePoint 제품 구성 마법사 실행'을 선택하고 **닫기**를 클릭합니다.



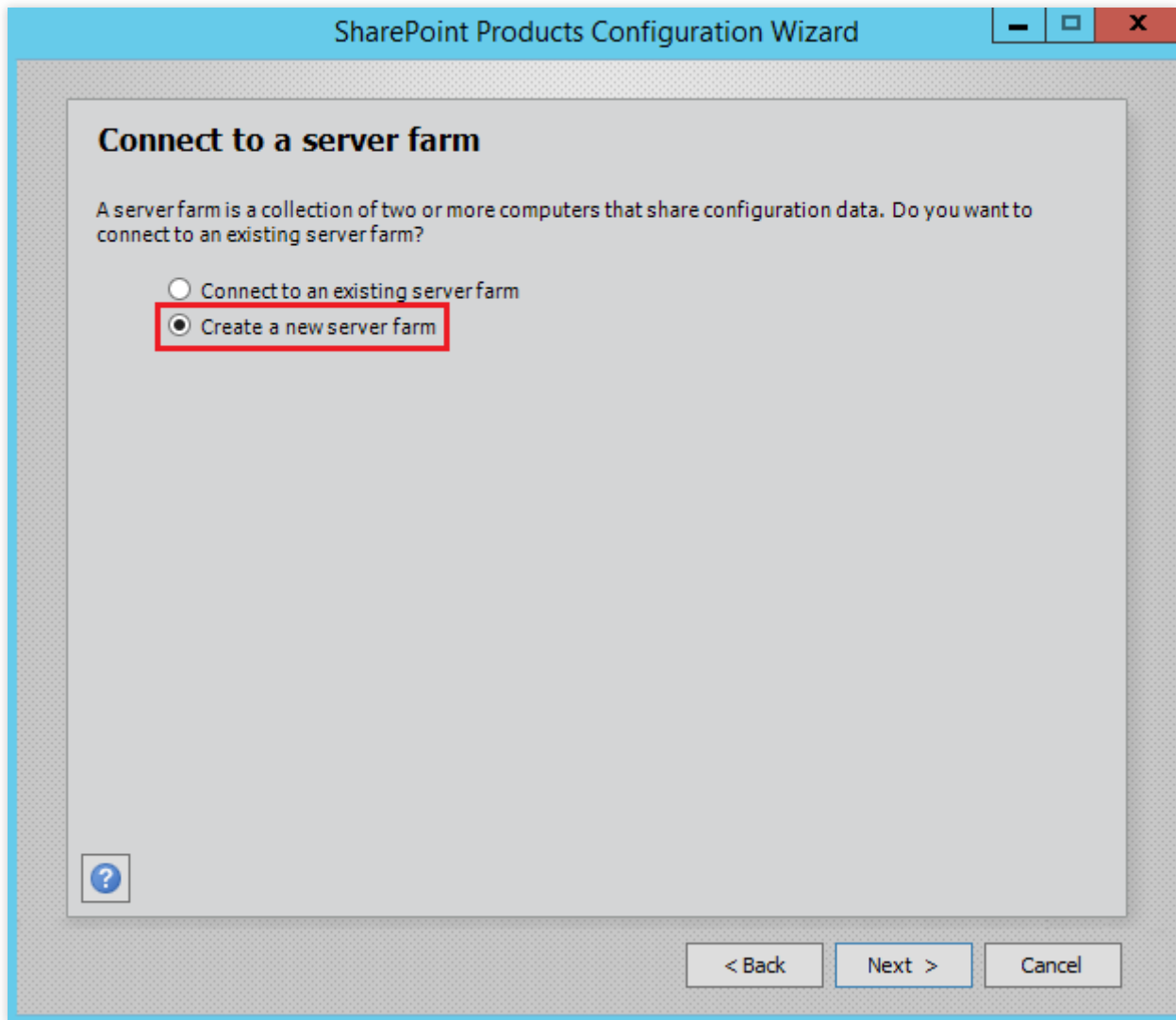
5단계: SharePoint 2016 구성

1. SharePoint 제품 구성 마법사 창에서 다음을 클릭합니다.



2. 팝업 대화 상자에서 **예**를 클릭하면 구성 중에 서비스를 다시 시작할 수 있습니다.

3. 새 서버 **팜** 만들기를 선택하고 **다음**을 클릭합니다.



4. 아래와 같이 구성 데이터베이스 설정 지정 페이지에서 구성 데이터베이스와 액세스 계정을 설정하고 **다음**을 클릭합니다.

SharePoint 데이터베이스는 로컬 호스트에 있으므로 로컬 데이터베이스와 계정을 입력합니다.

SharePoint Products Configuration Wizard

Specify Configuration Database Settings

All servers in a server farm must share a configuration database. Type the database server and database name. If the database does not exist, it will be created. To reuse an existing database, the database must be empty. For additional information regarding database server security configuration and network access please see [help](#).

Database server: .

Database name: SharePoint_Config

Specify Database Access Account

Select an existing Windows account that this machine will always use to connect to the configuration database. If your configuration database is hosted on another server, you must specify a domain account.

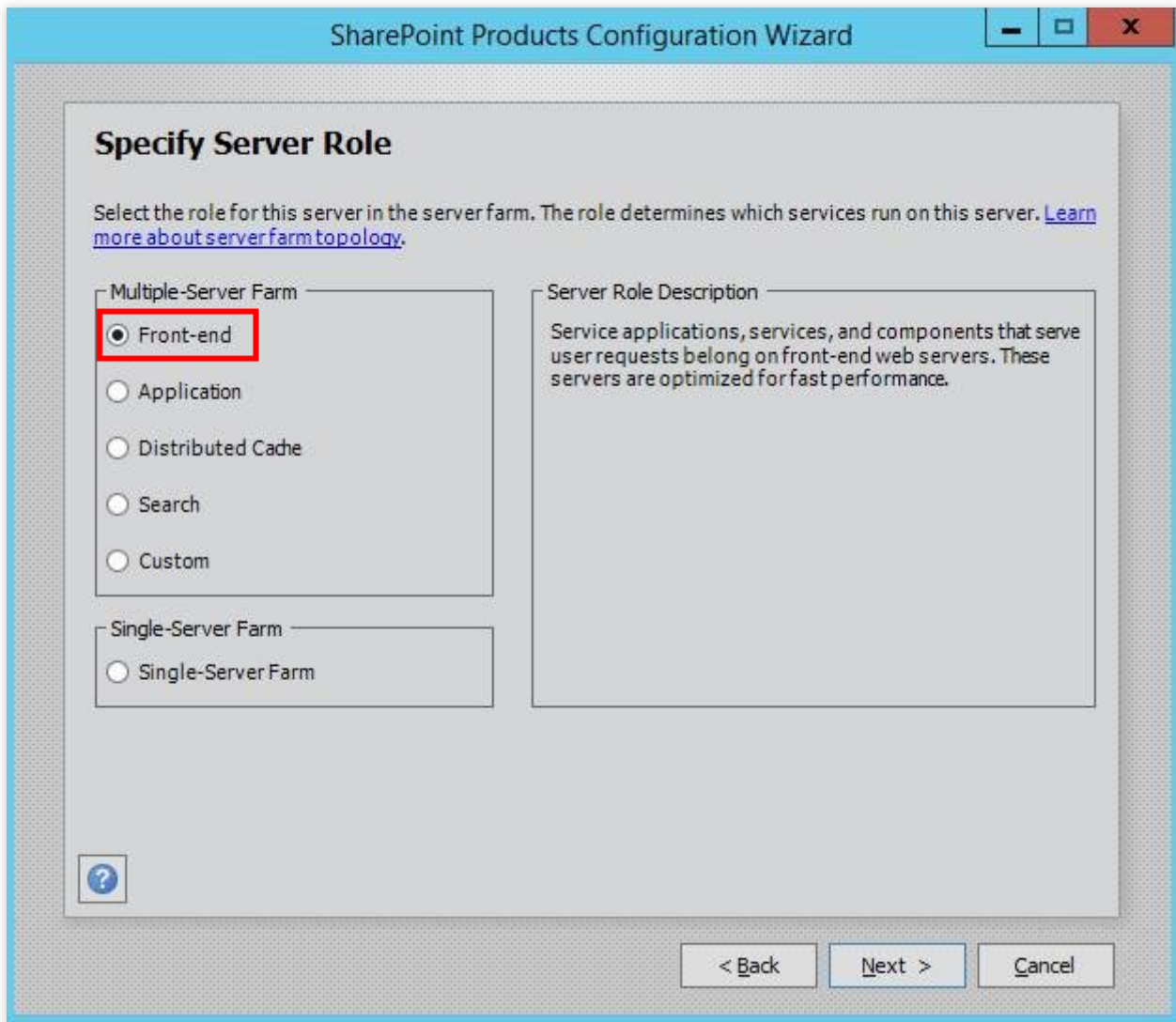
Type the username in the form DOMAIN\User_Name and password for the account.

Username: Administrator

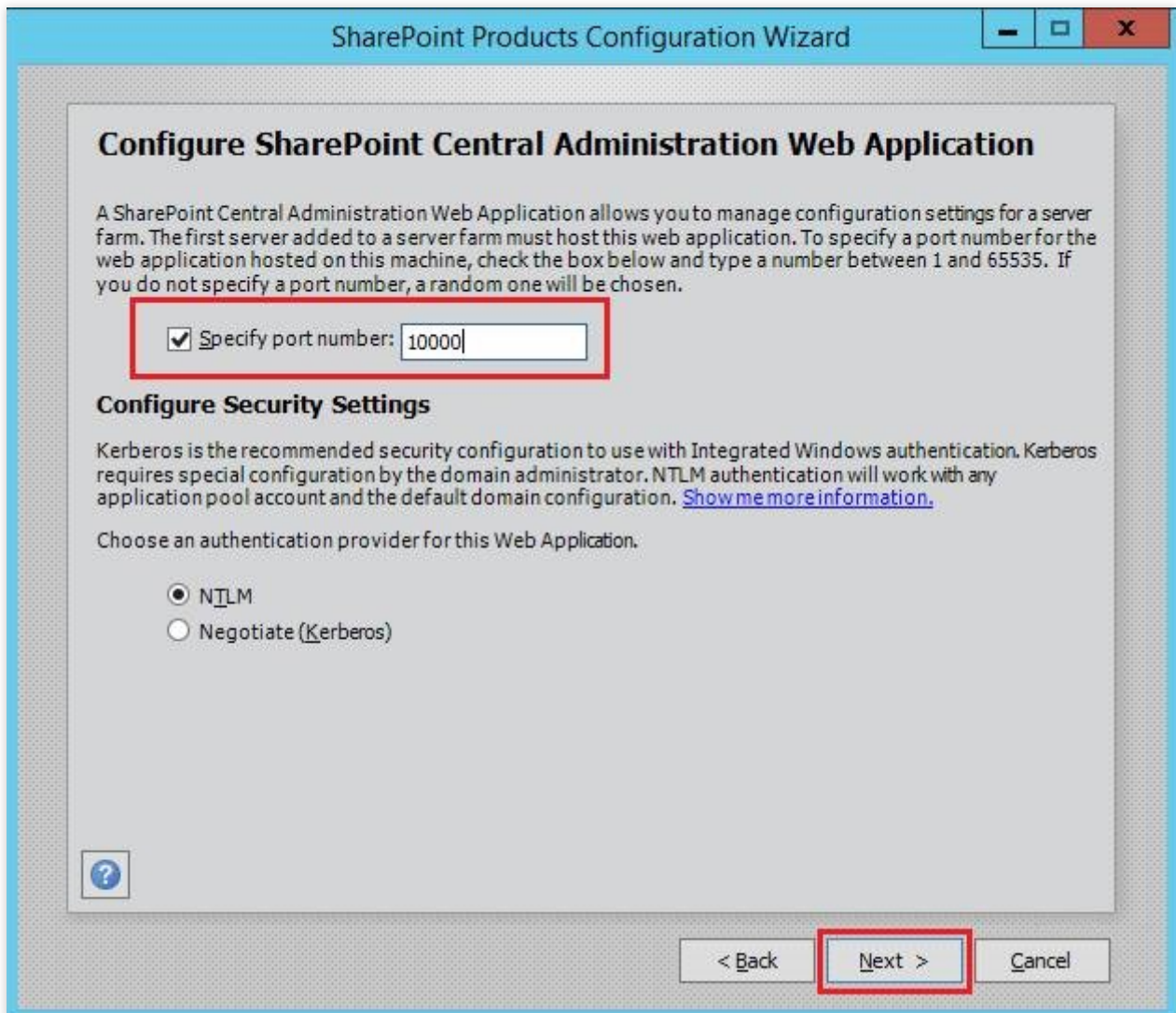
Password:

< Back Next > Cancel

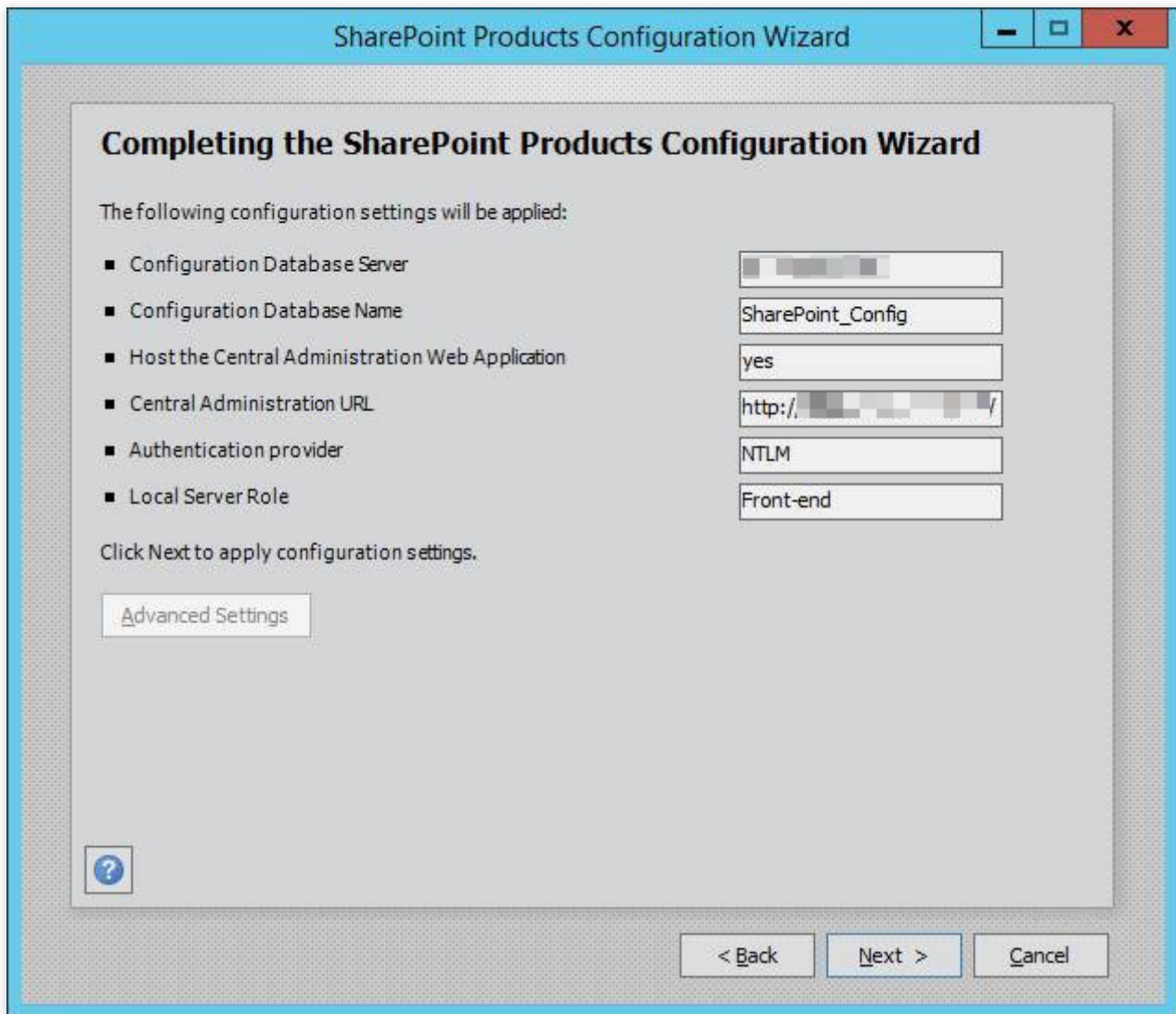
5. 서버 팜의 암호를 입력하고 다음을 클릭합니다.
6. '다중 서버 팜'에 대해 프론트 엔드를 선택하고 다음을 클릭합니다.



7. SharePoint 관리 센터의 포트 번호를 지정하고(이 예시에서는 10000을 사용하지만 필요에 따라 포트 번호를 구성할 수 있음) 다음을 클릭합니다.



8. 아래와 같이 SharePoint 구성을 확인하고 다음을 클릭합니다.



9. Sharepoint 구성이 완료되면 **마침**을 클릭합니다.

aaPanel-BT Windows 설치

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

Pagoda Panel은 사용하기 쉽고 강력하며 평생 무료로 제공되는 서버 관리 소프트웨어이며 Linux 및 Windows 시스템을 지원합니다. Pagoda Panel에서는 LAMP, LNMP, 웹 사이트, 데이터베이스, FTP, SSL을 원클릭으로 설정할 수 있으며 Web을 통해 서버를 쉽게 관리할 수 있습니다.

본 문서는 Tencent Cloud Market 이미지를 통해 Windows 운영 체제의 CVM에 Pagoda Panel을 빠르게 설치하는 방법에 대해 설명합니다.

작업 단계

CVM 생성 시 Pagoda Panel 설치

주의사항 :

구매한 CVM 부서를 이용하여 Pagoda Panel을 설치하고자 하는 경우 [시스템 재설치](#)를 통해 해당 이미지를 어워드 마켓에서 선택하여 환경 구축을 완료할 수 있습니다. 현재 중국 외 일부 리전의 CVM은 이미지 마켓을 통한 시스템 재설치를 지원하지 않으니 타 리전의 클라우드 서버를 이용하여 구축하거나 [Pagoda Panel 공식 홈페이지](#)에서 자세한 설치 정보를 확인하시기 바랍니다.

1. [CVM 콘솔](#)에 로그인 한 후 인스턴스 관리 페이지에서 **생성**을 클릭합니다.
2. 페이지의 프롬프트에 따라 모델을 선택하고 '이미지'에서 **이미지 마켓 > 이미지 마켓에서 선택**을 아래 이미지와 같이 선택합니다.

주의사항 :

현재 일부 중국 외 리전은 이미지 마켓을 통한 CVM 생성을 지원하지 않습니다. 선택한 리전에 **이미지 마켓**이 없는 경우 이미지 마켓을 지원하는 다른 리전을 선택하십시오.

메모리가 2GB 이상이고 시스템 디스크 용량이 40GB 이상인 인스턴스 설정을 선택하는 것이 좋습니다.

3. **이미지 Market** 창의 검색 창에서 **유지보수 툴**을 선택하고 'pagoda'를 입력한 후



을(를) 클릭합니다.

4. 필요에 따라 이미지를 선택합니다. 본 문서는 ****Pagoda Windows Panel Official Version (WAMP/WNMP/Tomcat/Node.js)****을 예로 듭니다. 클릭 **무료 사용**.

5. 인스턴스와 연결된 보안 그룹에서 포트 8888을 개방하는 인바운드 규칙을 추가해야 합니다. 자세한 내용은 [보안 그룹 규칙 추가](#)를 참고하십시오.

실제 필요에 따라 스토리지 미디어 및 대역폭과 같은 기타 설정을 구성하고 구매를 선택하여 Pagoda Panel 구축을 완료합니다.

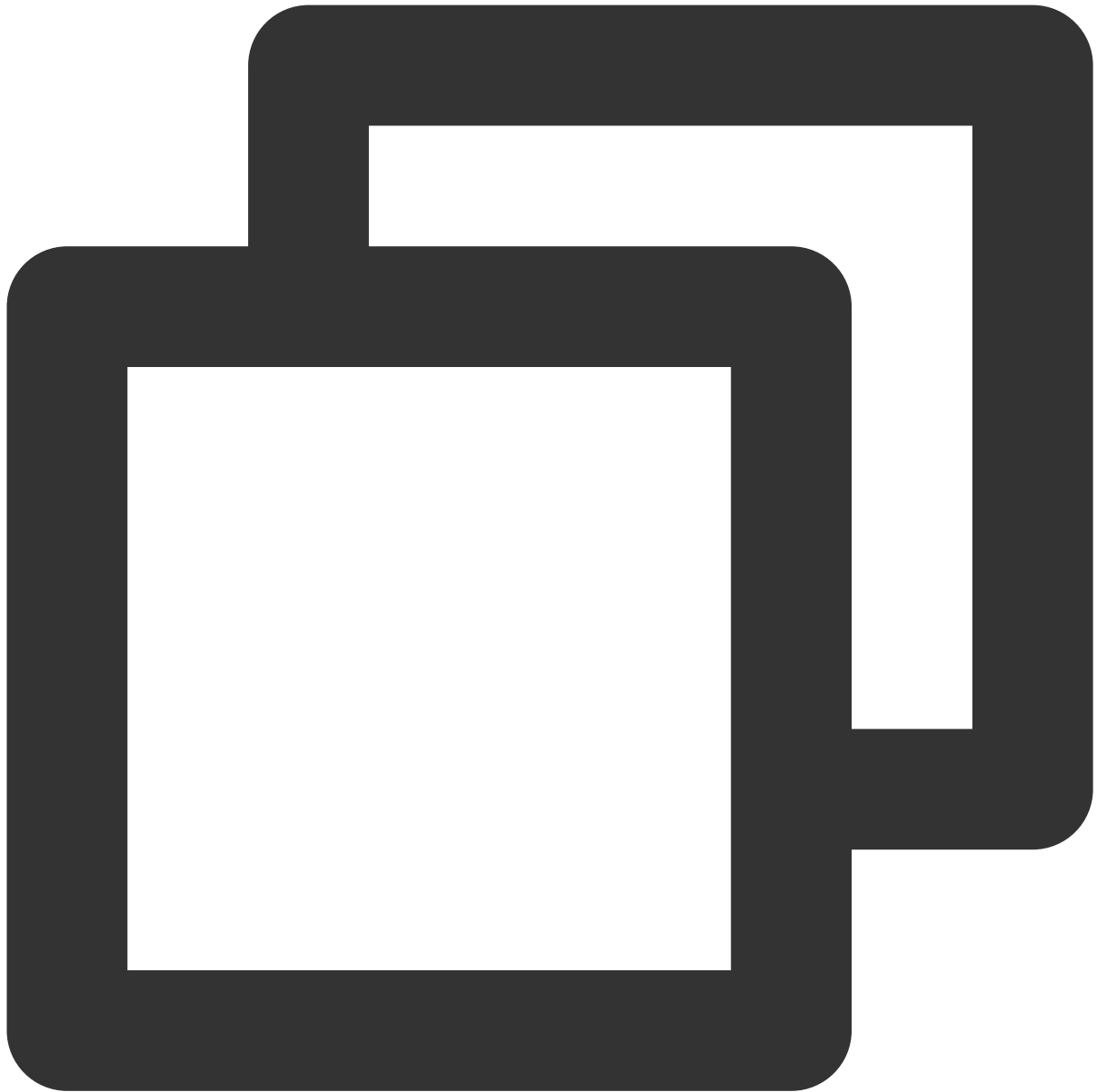
패널 로그인 정보 가져오기

1. CVM에 로그인합니다. 자세한 내용은 [표준 방식으로 Windows 인스턴스에 로그인](#)을 참고하십시오.
2. 운영 체제 인터페이스에서 왼쪽 하단의



을(를) 우클릭하고 팝업 메뉴에서 **실행**을 클릭합니다.

3. cmd 창에서 다음 명령을 실행하여 로그인 정보를 가져옵니다.

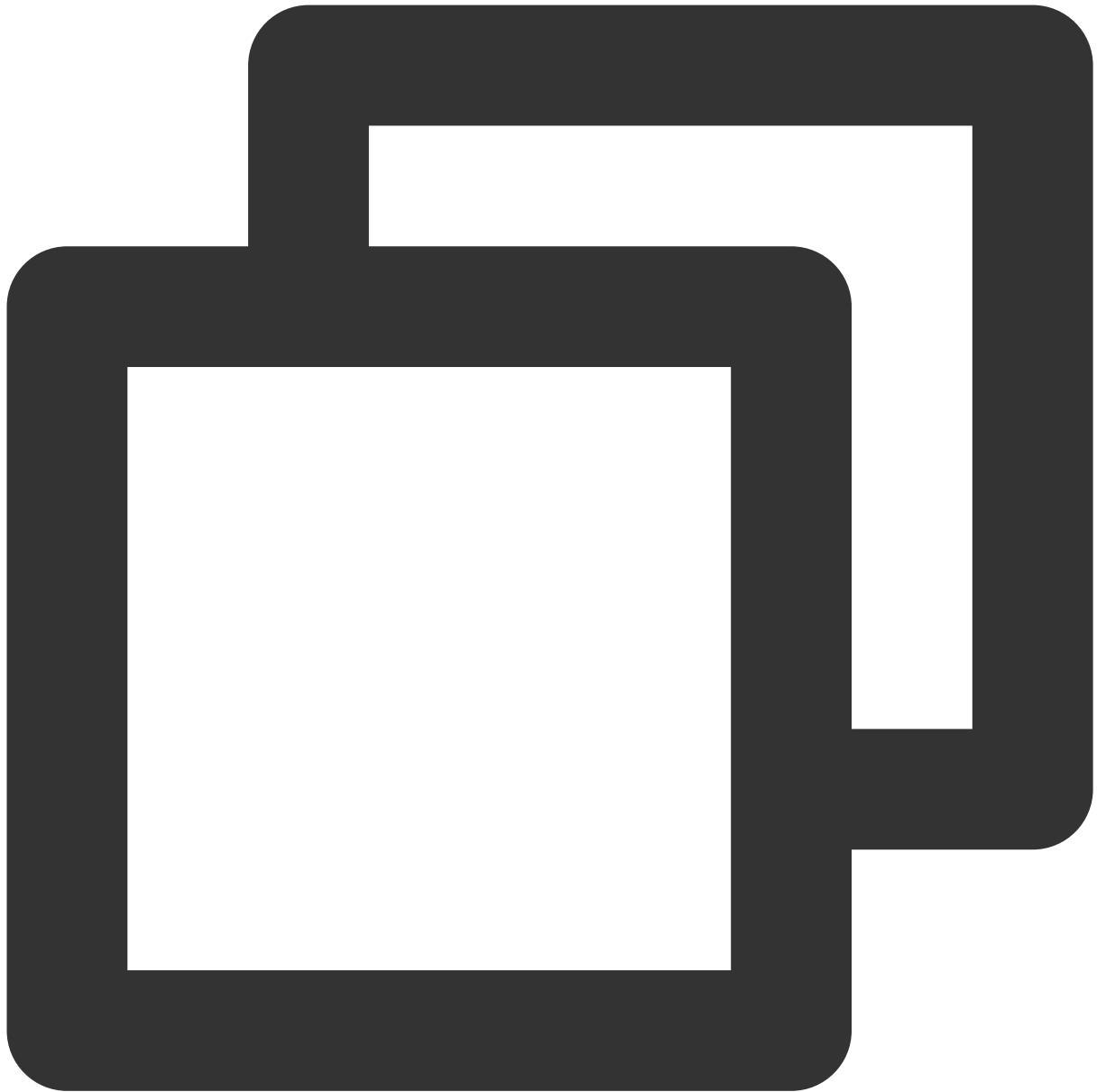


```
bt default
```

결과가 반환되면 탭 패널의 주소와 로그인 정보를 기록합니다.

Pagoda Panel에 로그인

1. 로컬 컴퓨터에서 브라우저를 열고 가져온 Pagoda Panel 주소에 액세스합니다.



`http://CVM 공용 IP:8888/xxxx`

2. 기록된 사용자 이름과 암호를 입력하고 로그인을 클릭합니다.
3. '<이용약관>에 동의합니다'를 선택하고 **패널로 이동하기**를 클릭합니다.
4. 실제 필요에 따라 패널에서 관련 패키지 설치 및 배포 웹 사이트를 선택하십시오.

Docker 구축

최종 업데이트 날짜: : 2024-03-04 15:59:16

작업 시나리오

본문은 Tencent Cloud 클라우드 서비스에서 Docker를 구축하고 사용하는 방법을 소개합니다. 본문의 내용은 Linux 운영 체제에 익숙하고 Tencent Cloud 클라우드 서비스를 사용하기 시작한 개발자에게 적합합니다. Docker에 대한 자세한 내용은 [Docker 공식 홈페이지 문서](#)를 참고하십시오.

설명 :

Windows 운영 체제의 CVM에서 Docker를 빌드 및 사용하려면 [Windows에 Docker 데스크톱 설치](#)를 참고하십시오.

예시 운영 체제

본 문서에서는 CVM 인스턴스 운영 체제 CentOS 8.2 을 예시로 사용합니다.

TencentOS Server 운영 체제를 사용하는 경우 실제 버전에 해당하는 작업 수행:

TencentOS Server 2.4: 이미지가 Docker로 미리 구성되어 있으므로 다시 설치할 필요가 없습니다. [Docker 사용하기](#)를 참고하여 직접 사용을 시작할 수 있습니다.

TencentOS Server 3.1 (TK4): 문서를 참고하여 구축하십시오.

전제 조건

구매한 Linux CVM이 있어야 합니다.

설명 :

Docker를 빌드하려면 64비트 시스템을 사용해야 하며 커널 버전은 3.10 이상이어야 합니다.

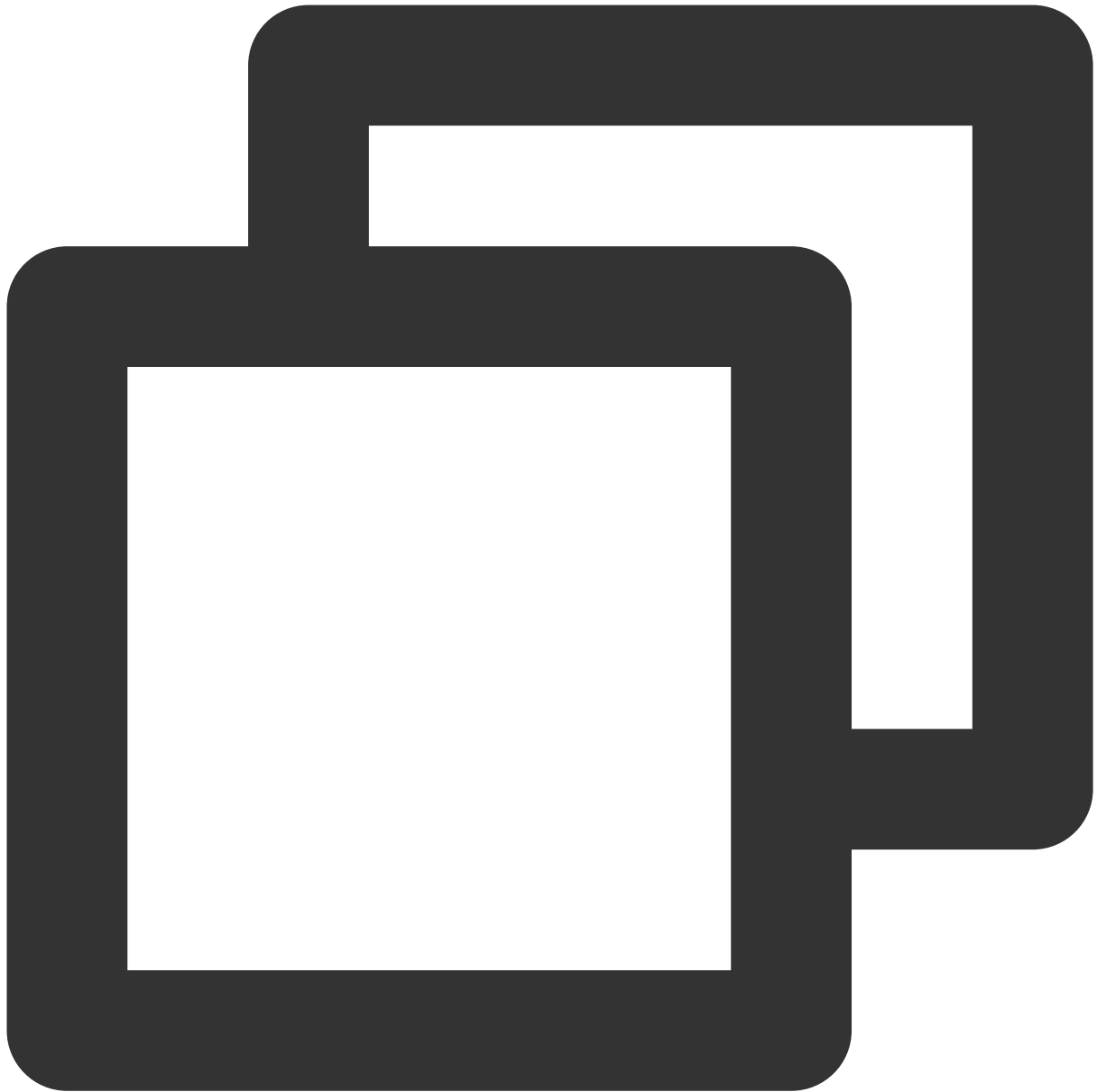
작업 단계

Docker 설치

실제 운영 체제 버전에 따라 다음 단계를 수행합니다.

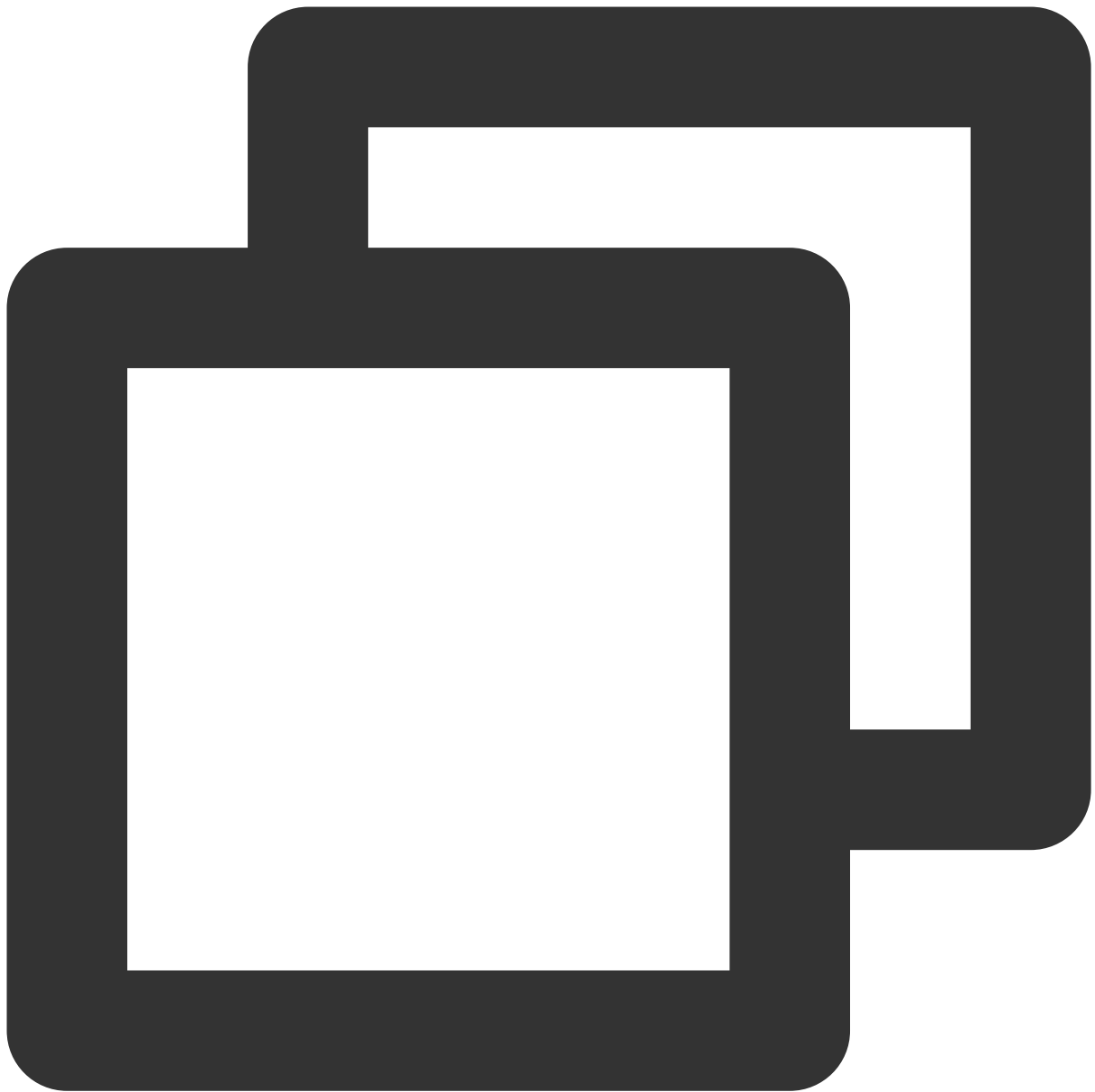
CentOS 8.2

1. [표준 방식으로 Linux 인스턴스에 로그인\(권장\)](#)합니다.
2. 다음 명령어를 실행하여 Docker 소프트웨어 보관소를 추가합니다.



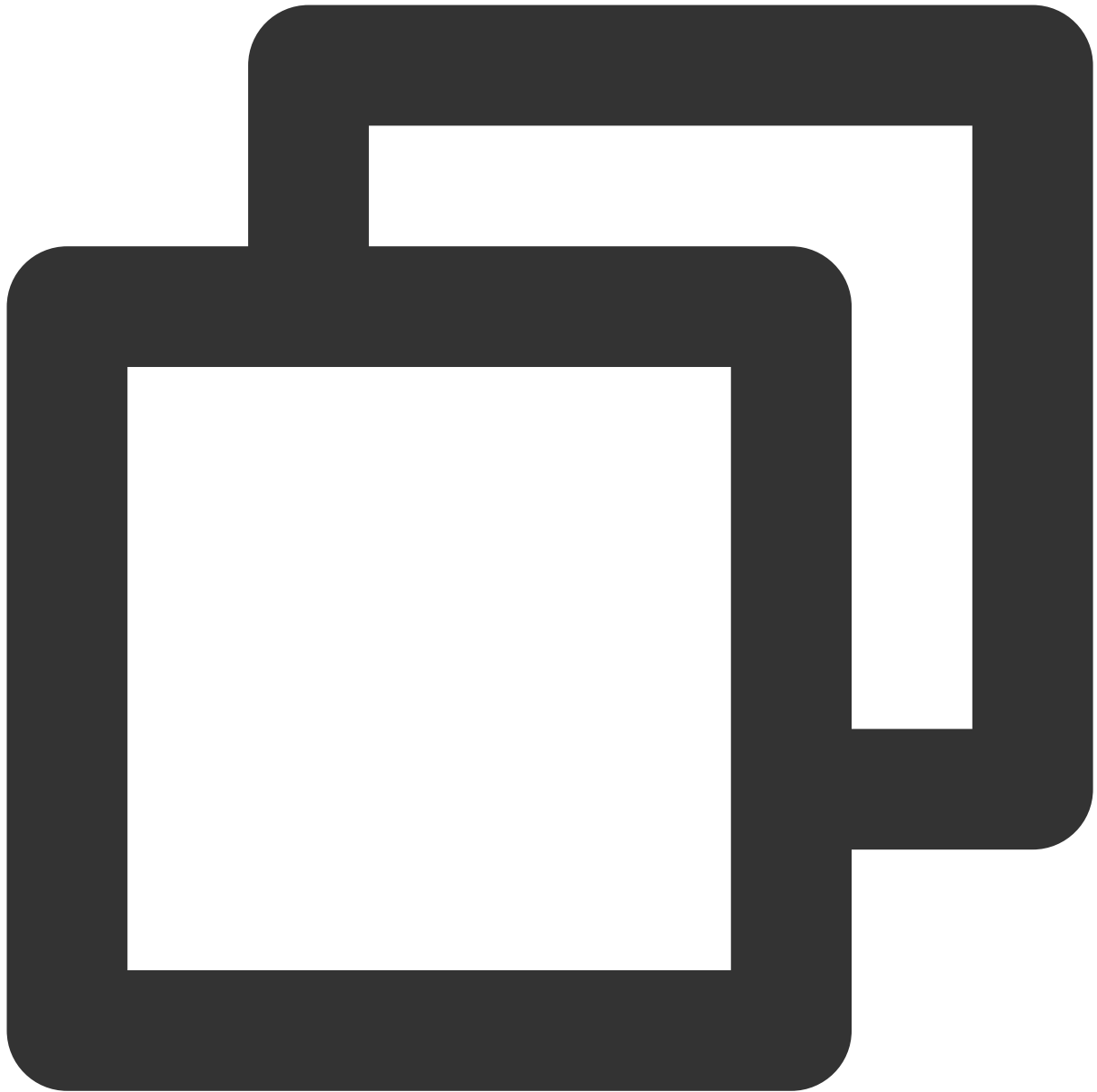
```
dnf config-manager --add-repo=http://mirrors.tencent.com/docker-ce/linux/centos/doc
```

3. 다음 명령어를 실행하여 추가된 Docker 소프트웨어 보관소를 확인합니다.



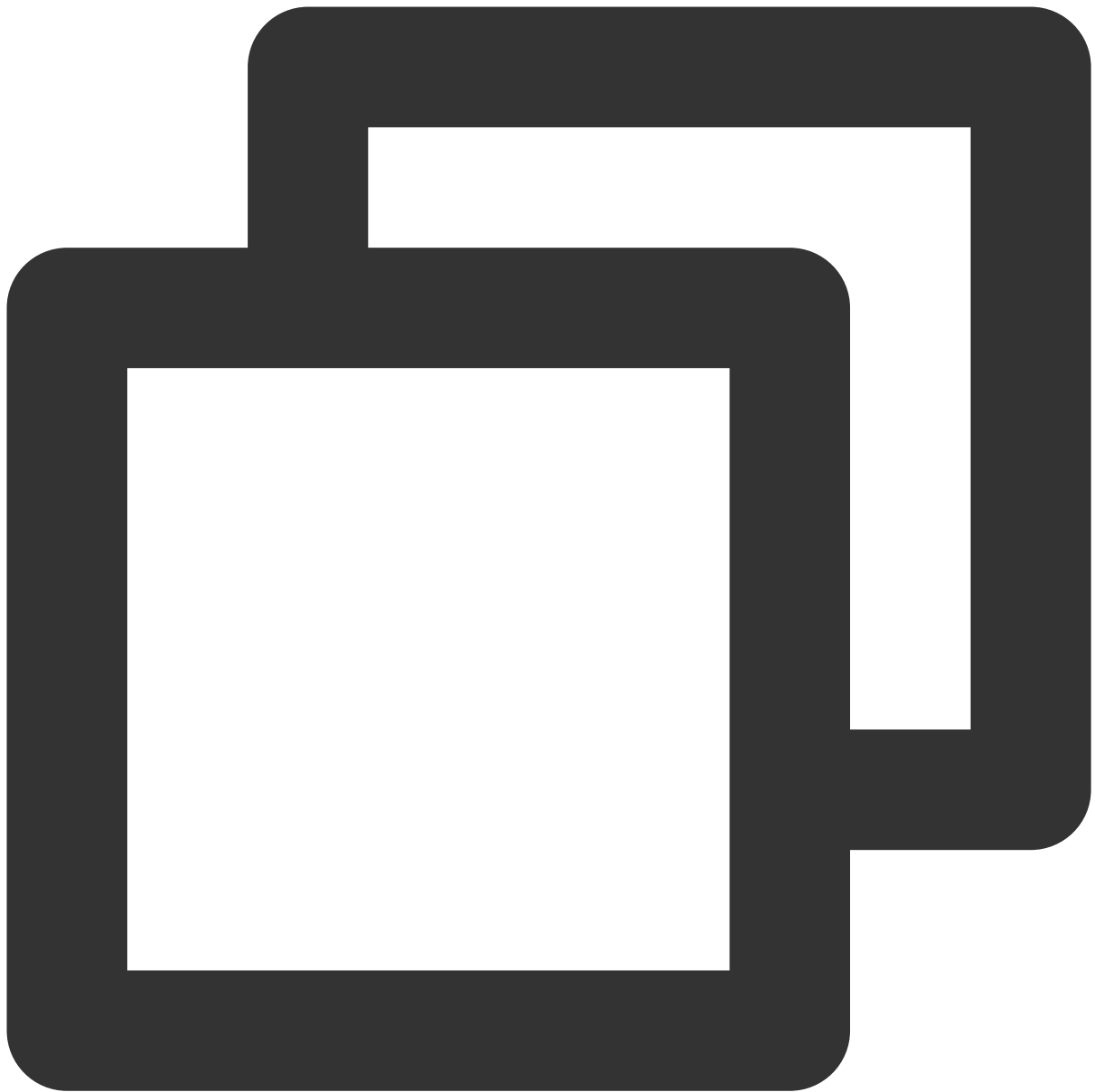
```
dnf list docker-ce
```

4. 다음 명령어를 실행하여 Docker를 설치합니다.



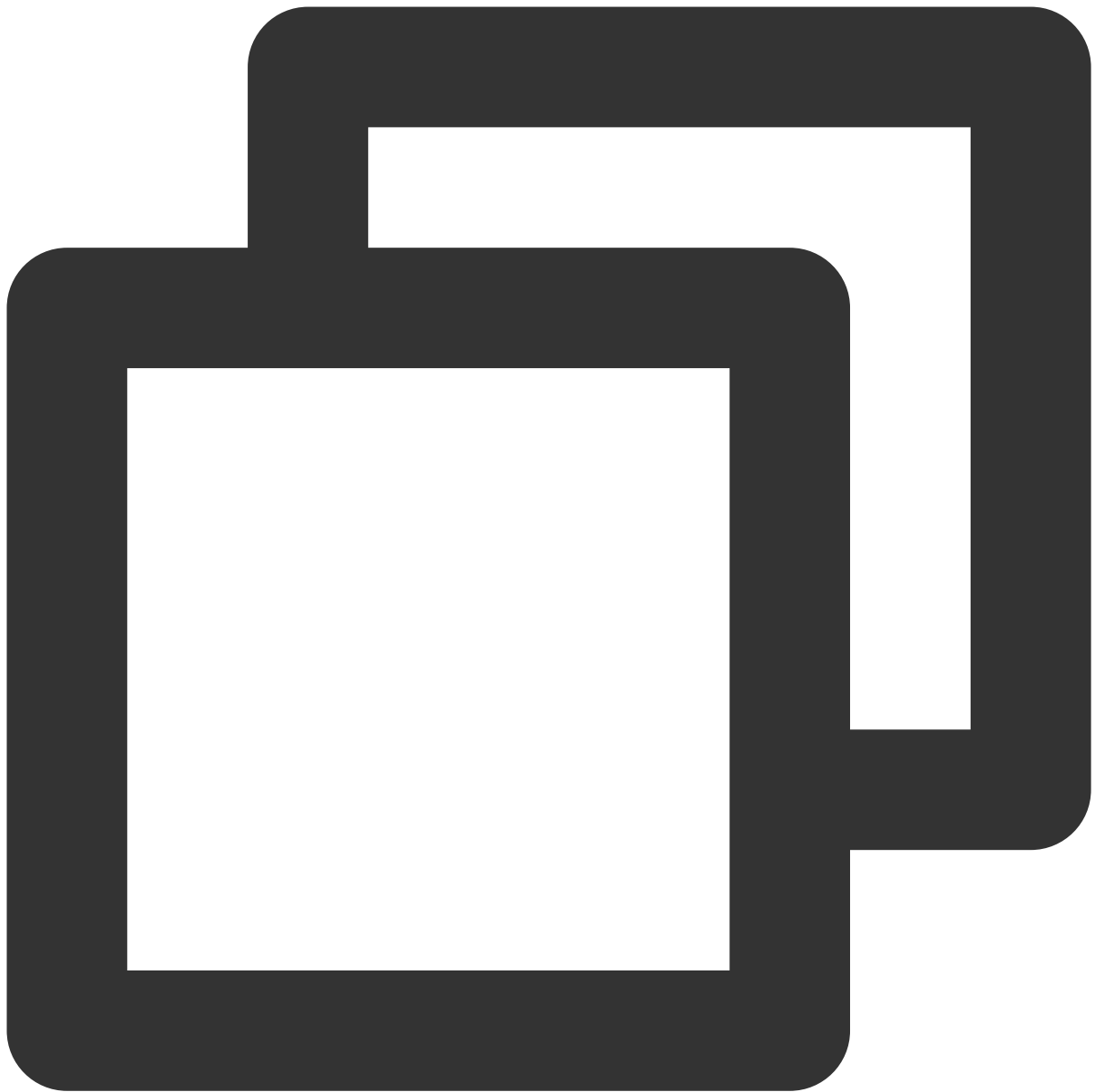
```
dnf install -y docker-ce --nobest
```

5. 다음 명령어를 실행하여 Docker를 실행합니다.



```
systemctl start docker
```

6. 다음 명령어를 실행하여 설치 결과를 확인합니다.



```
docker info
```

다음 정보가 반환되면 설치가 완료된 것입니다.

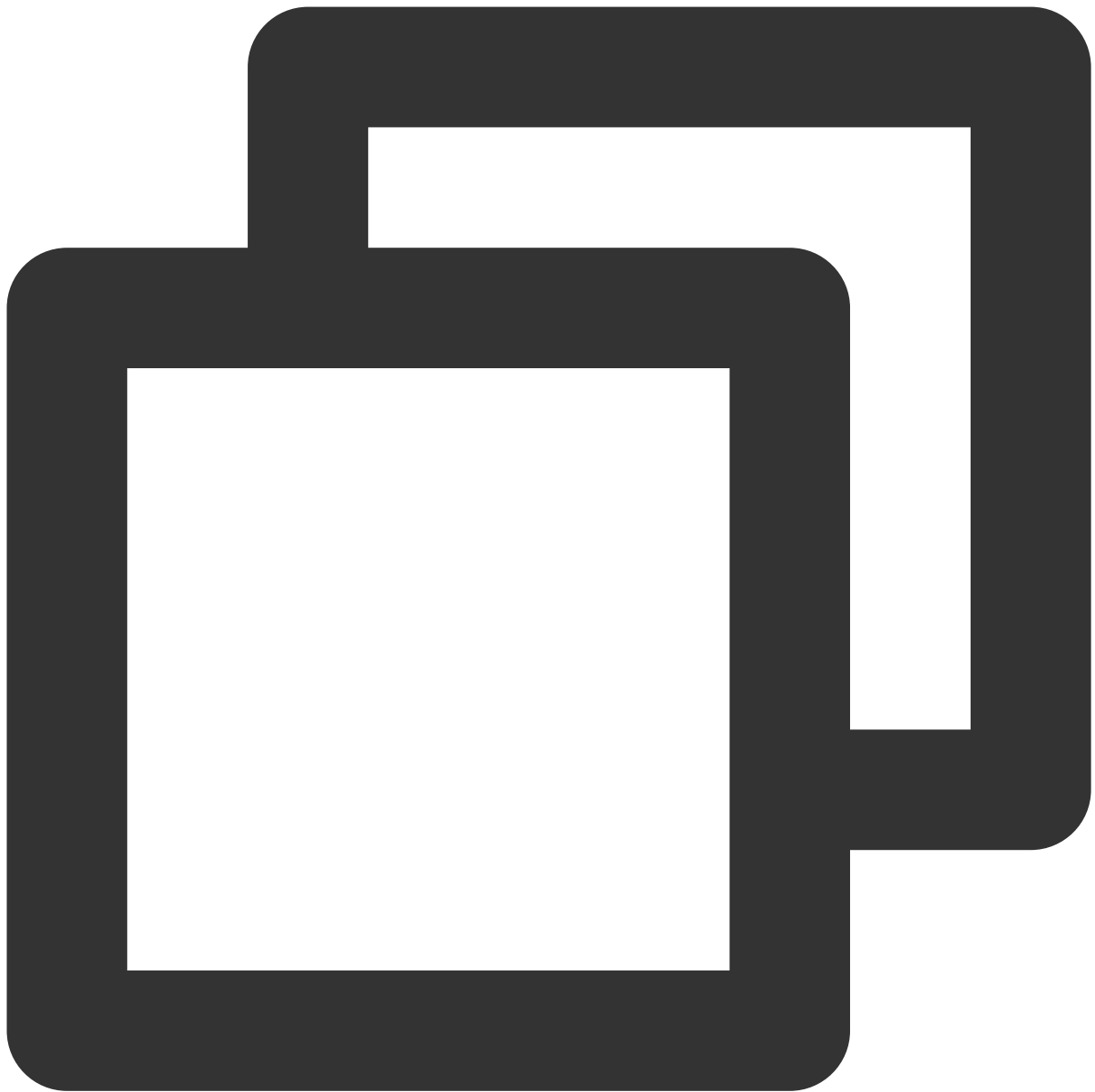
```
Kernel Version: 4.18.0-305.3.1.el8.x86_64
Operating System: CentOS Linux 8 (Core)
OSType: linux
Architecture: x86_64
CPUs: 2
Total Memory: 3.587GiB
Name: vm-2-143-centos
ID: 7GLW:CZKW:POYY:
Docker Root Dir: /var/lib/docker
Debug Mode: false
Registry: https://index.docker.io/v1/
Labels:
Experimental: false
Insecure Registries:
  127.0.0.0/8
Live Restore Enabled: false
```

Docker 사용

Docker의 기본 사용 명령어는 다음과 같습니다.

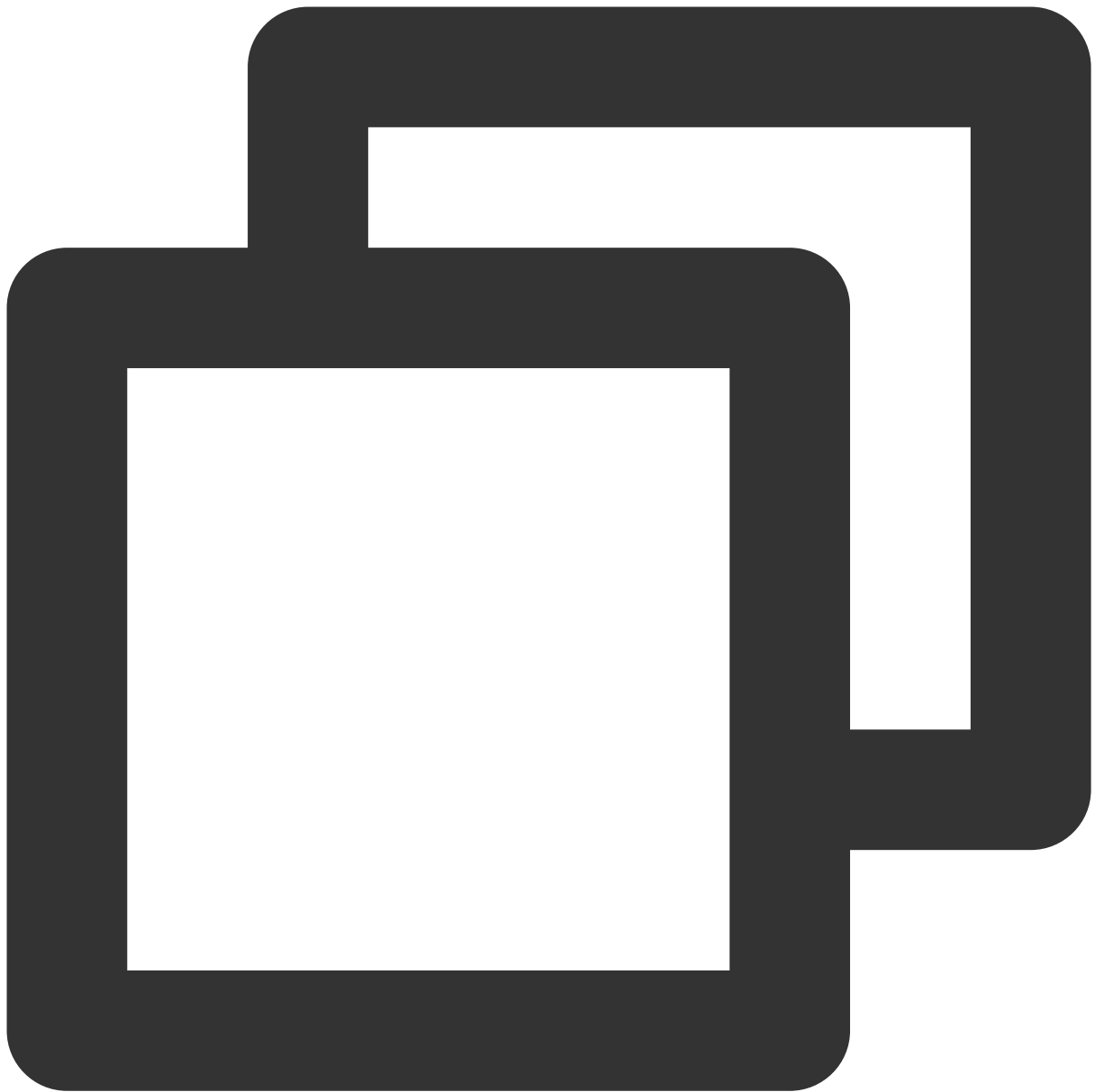
Docker 데몬을 관리합니다.

Docker 데몬을 실행합니다.



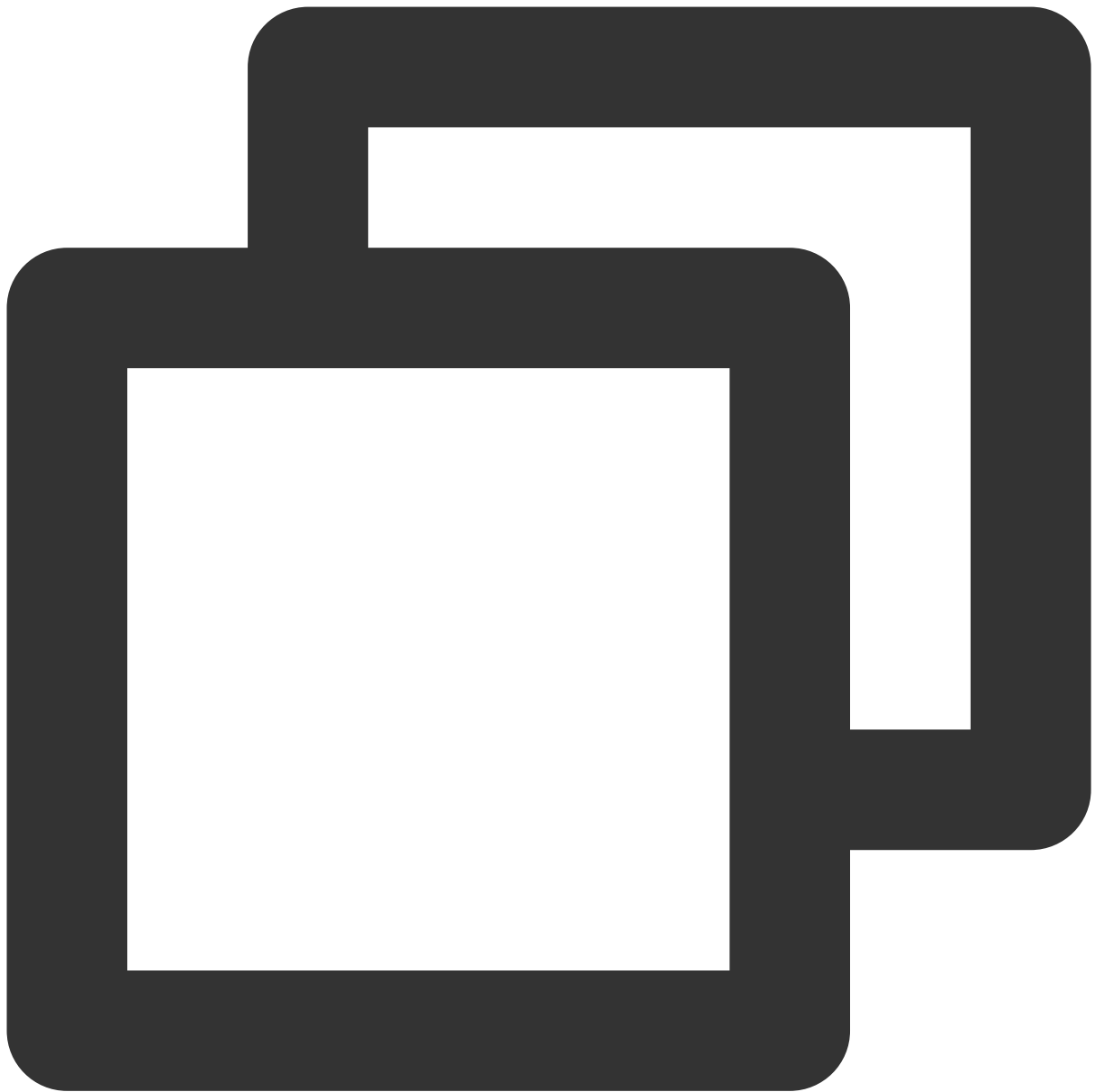
```
systemctl start docker
```

Docker 데몬을 중지합니다.



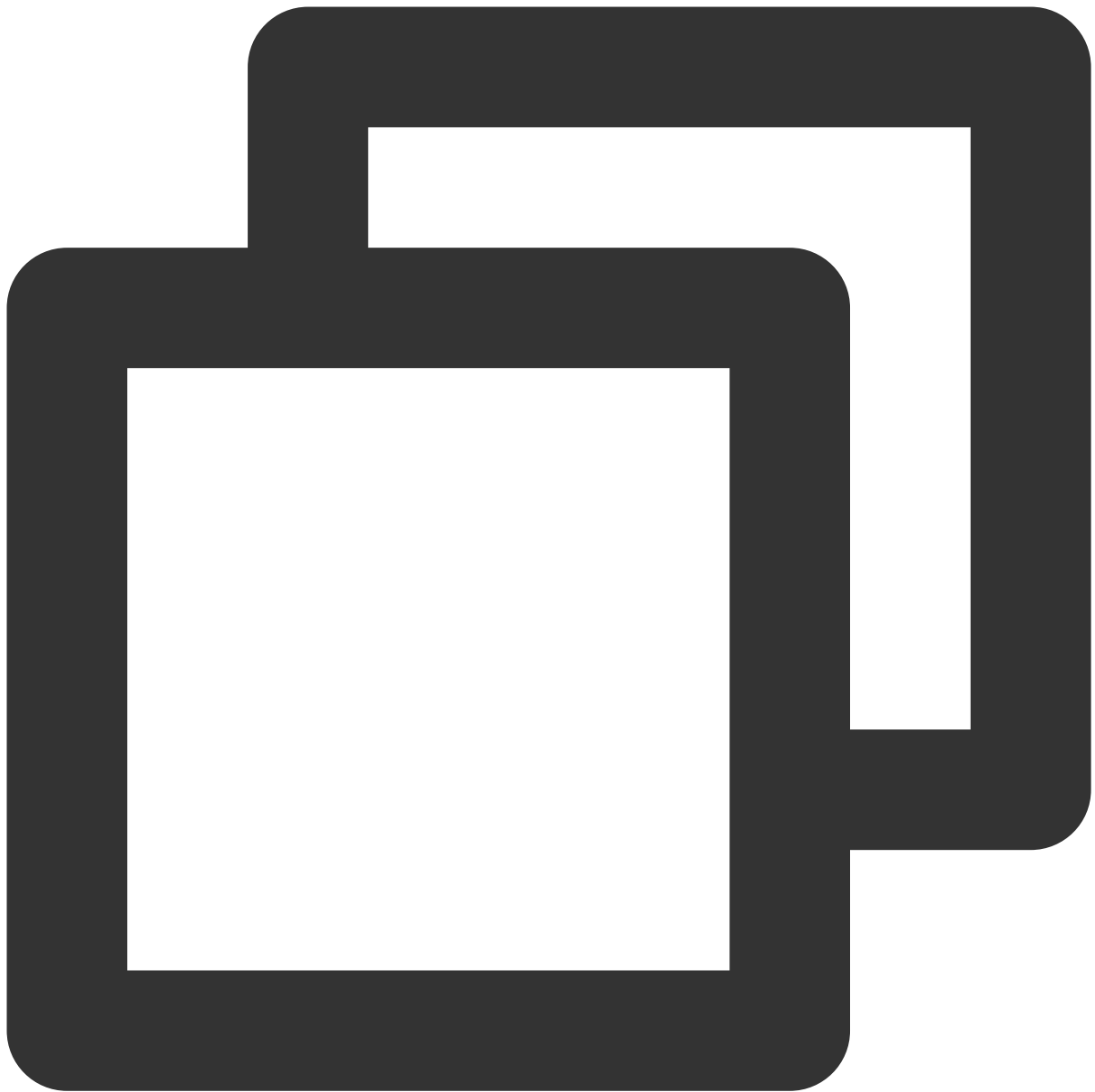
```
systemctl stop docker
```

Docker 데몬을 재시작합니다.



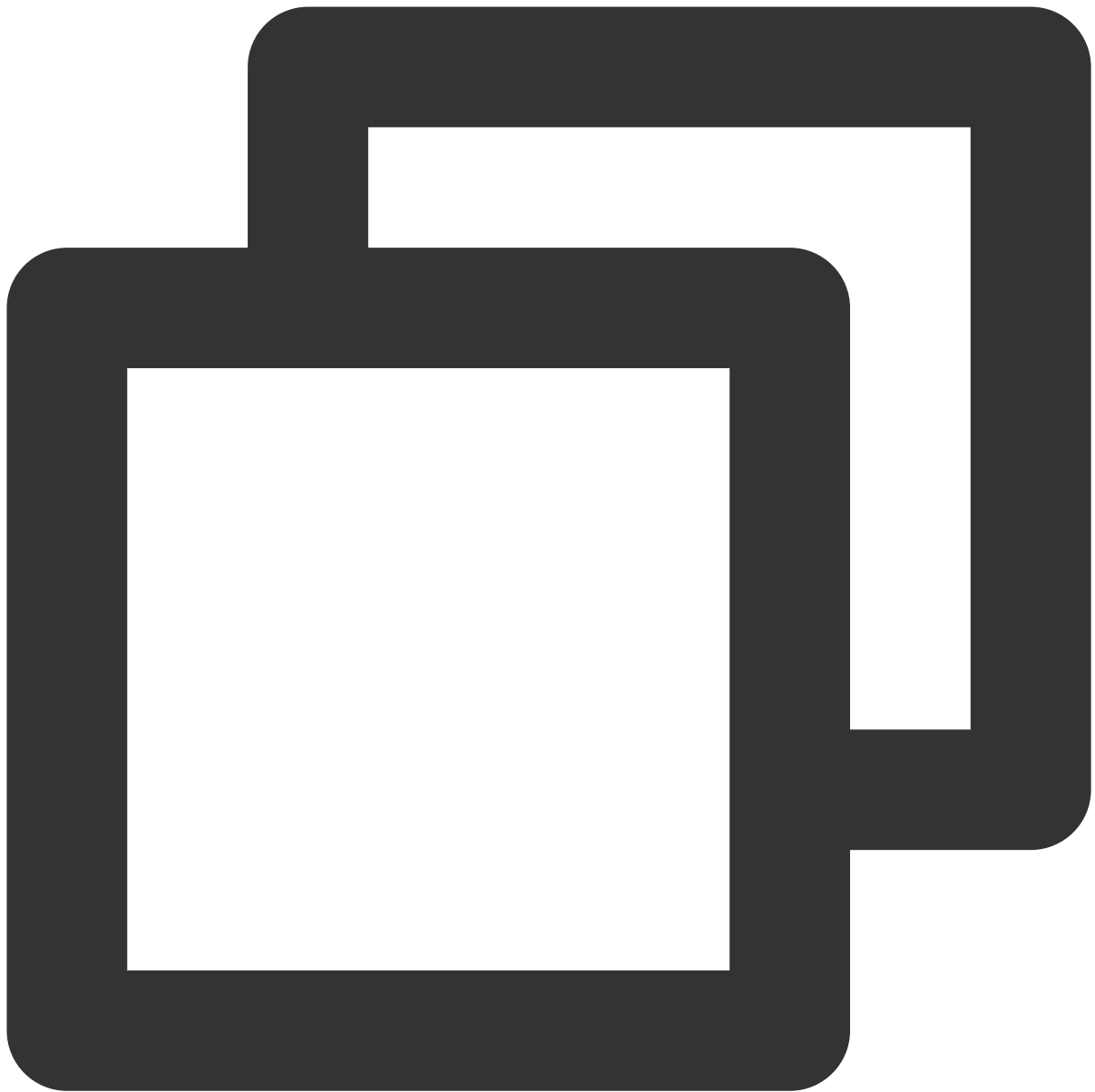
```
systemctl restart docker
```

이미지를 관리합니다. 본문은 Docker Hub의 Nginx 이미지를 예시로 사용합니다.



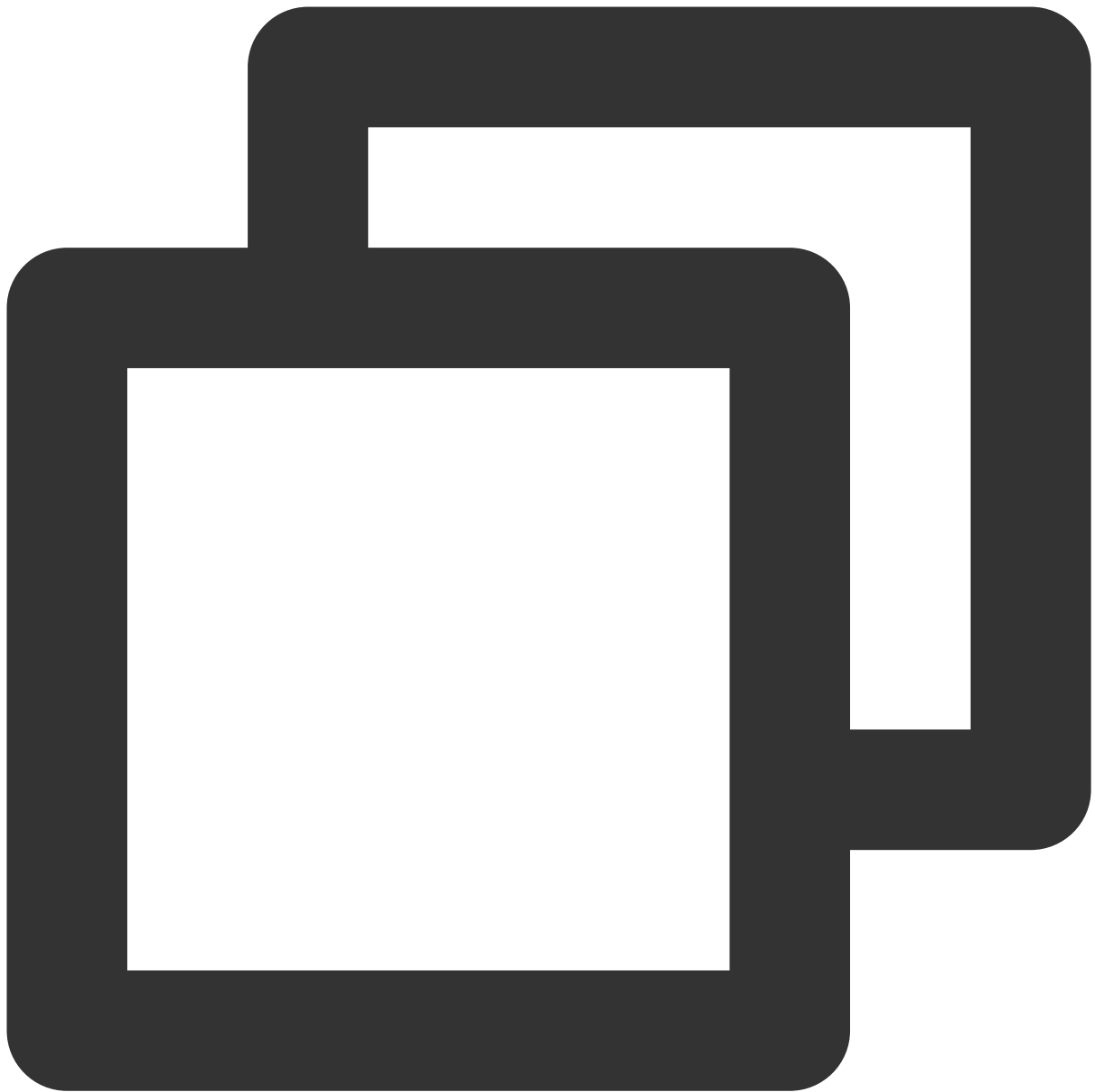
```
docker pull nginx
```

태그 수정 : 이미지 태그를 수정하여 구분을 기억할 수 있습니다.



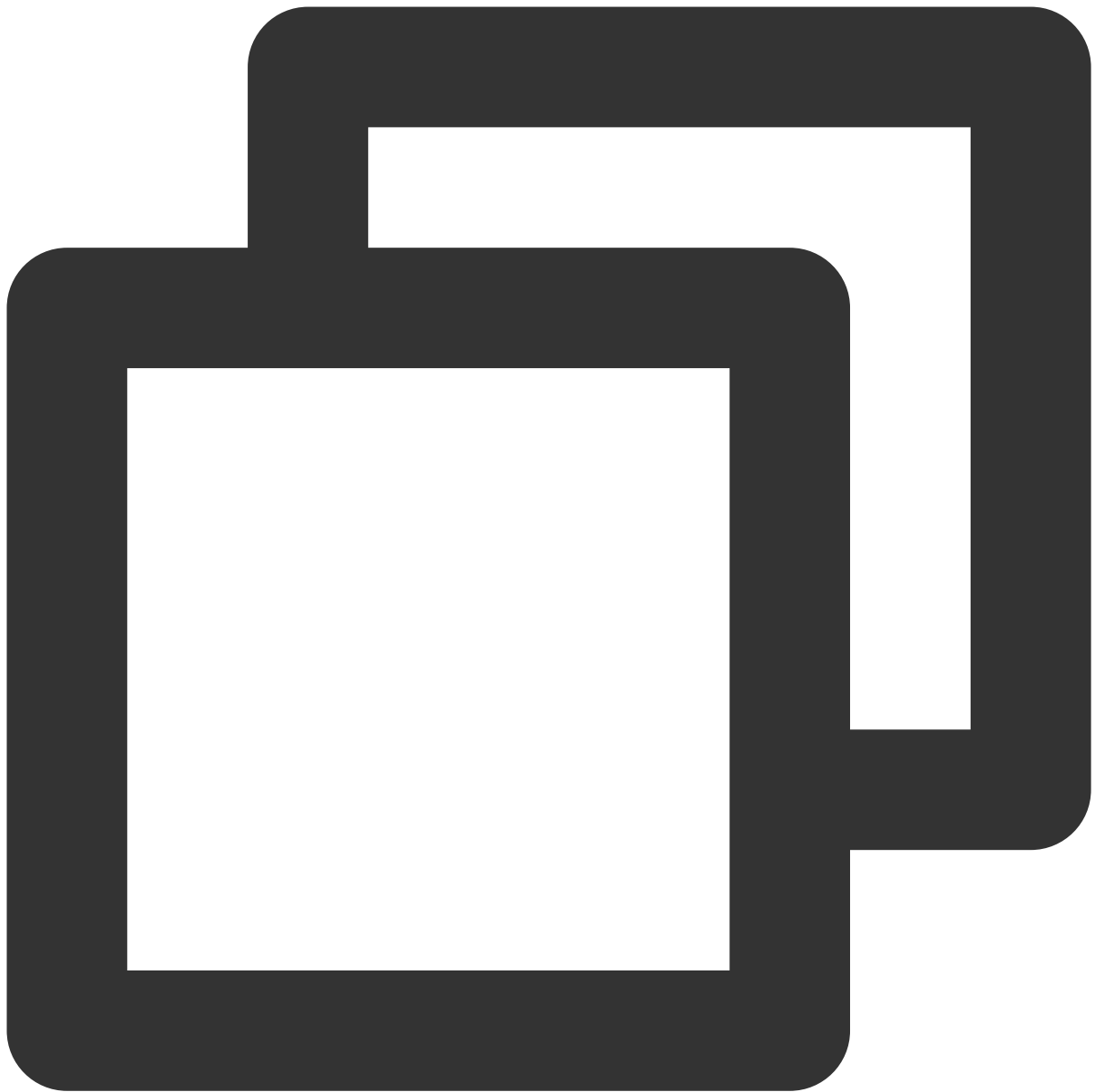
```
docker tag docker.io/nginx:latest tencentyun/nginx:v1
```

기존 이미지 보기:



`docker images`

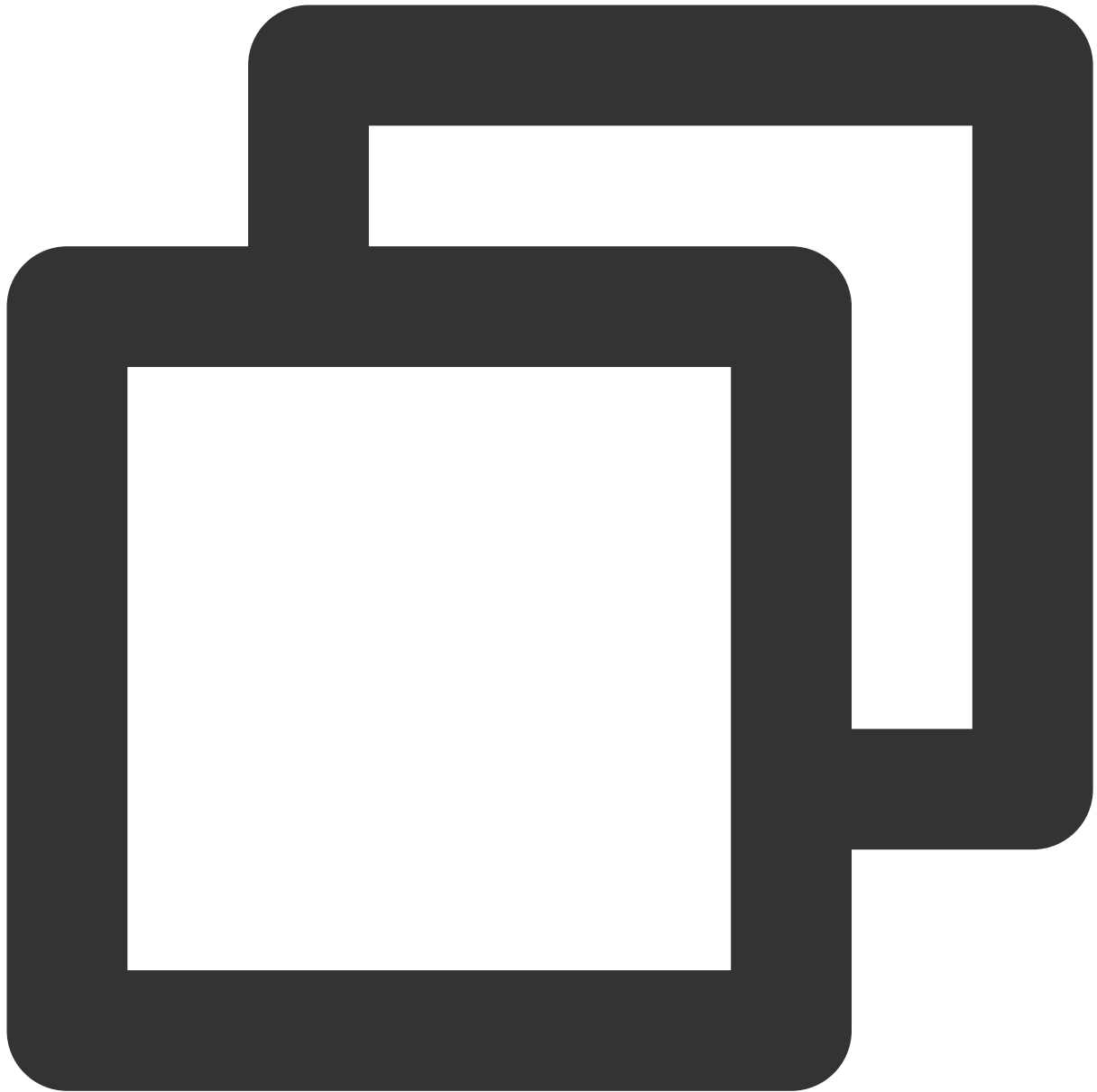
이미지 강제 삭제:



```
docker rmi -f tencentyun/nginx:v1
```

컨테이너 관리.

컨테이너 입력:

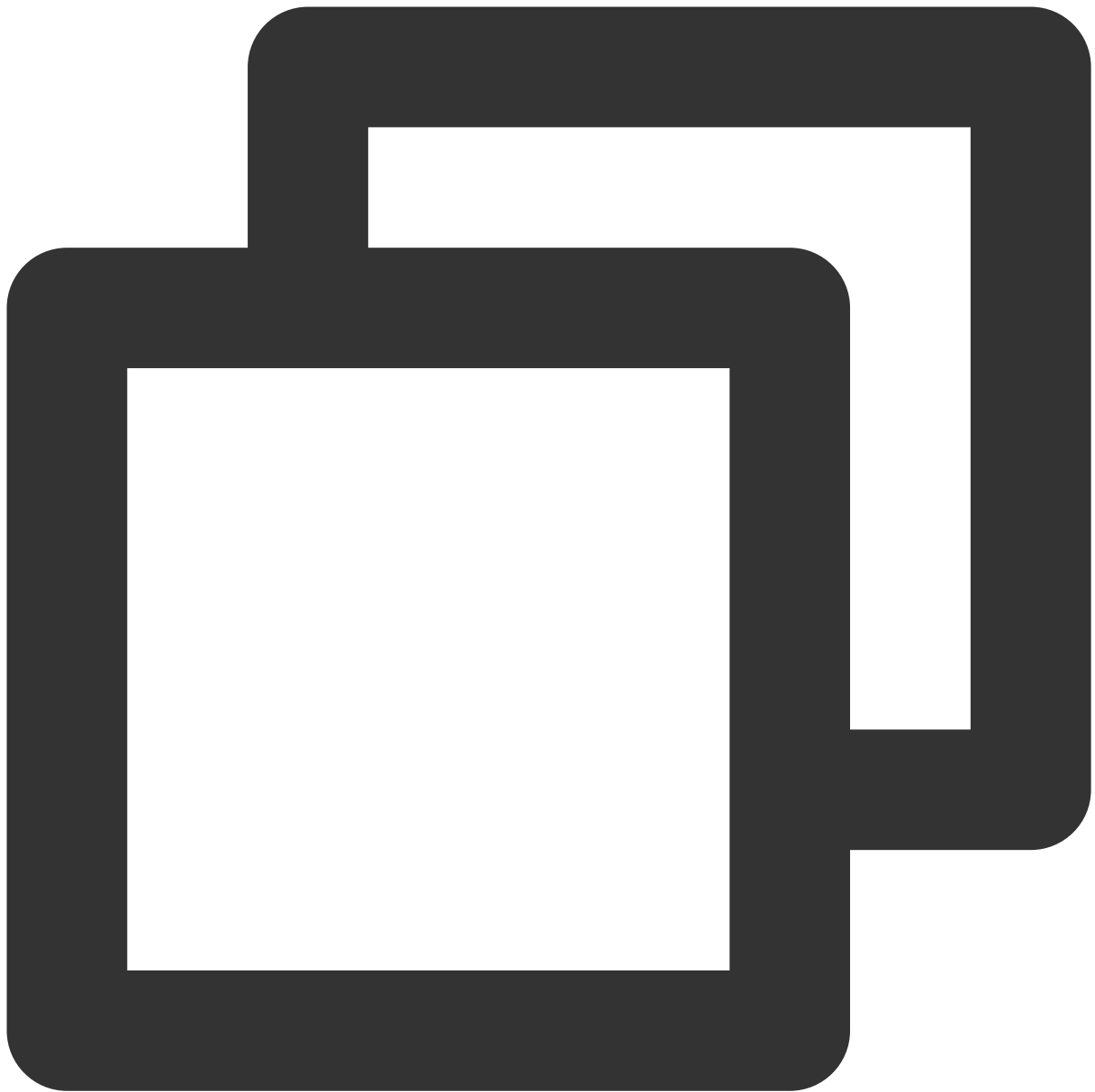


```
docker run -it ImageId /bin/bash
```

이 중 `ImageId` 는 `docker images` 명령어를 실행하여 얻을 수 있습니다.

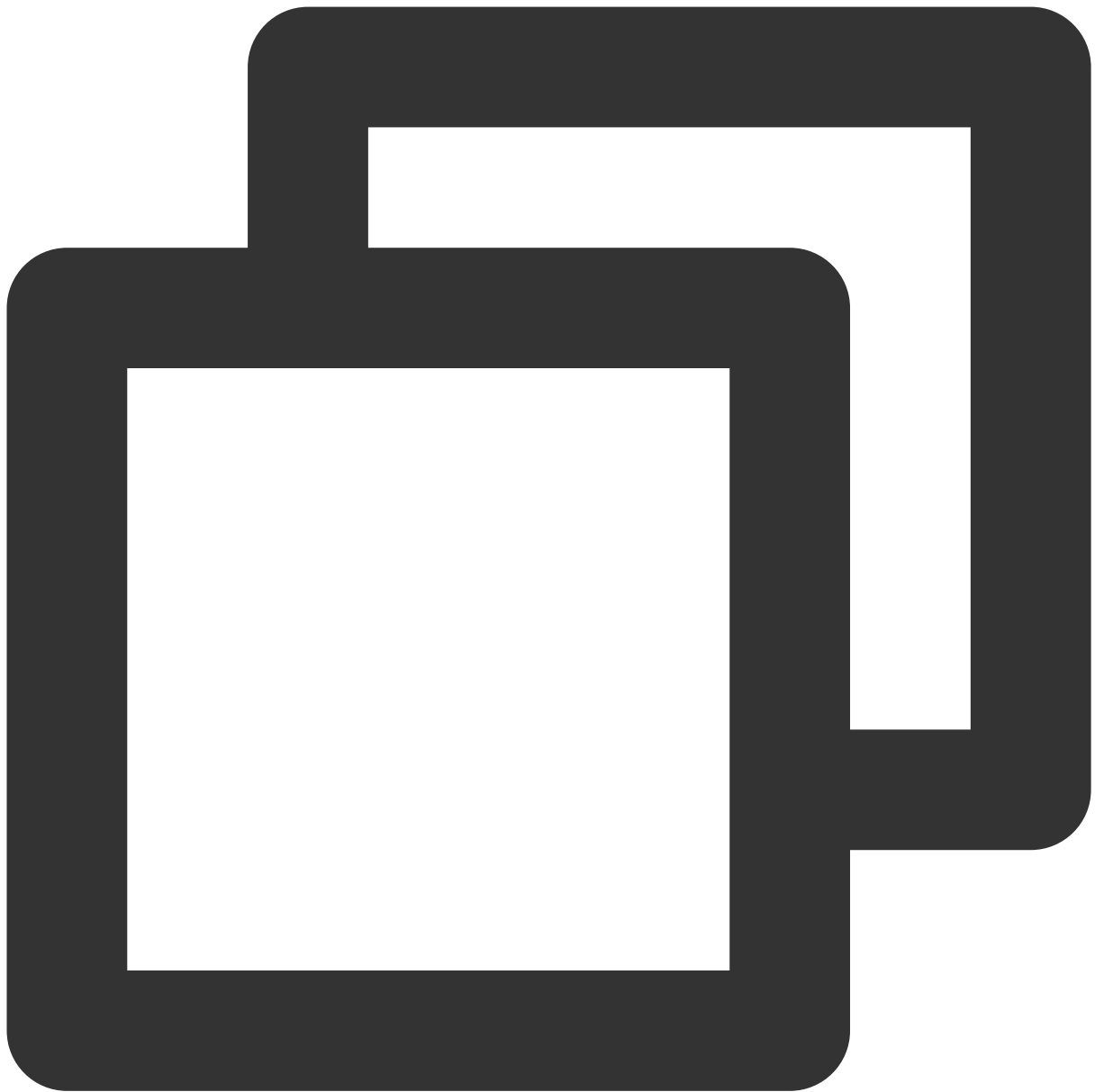
컨테이너 종료: 'exit' 명령어를 실행하여 현재 컨테이너를 종료합니다.

백그라운드에서 실행 중인 컨테이너 입력:



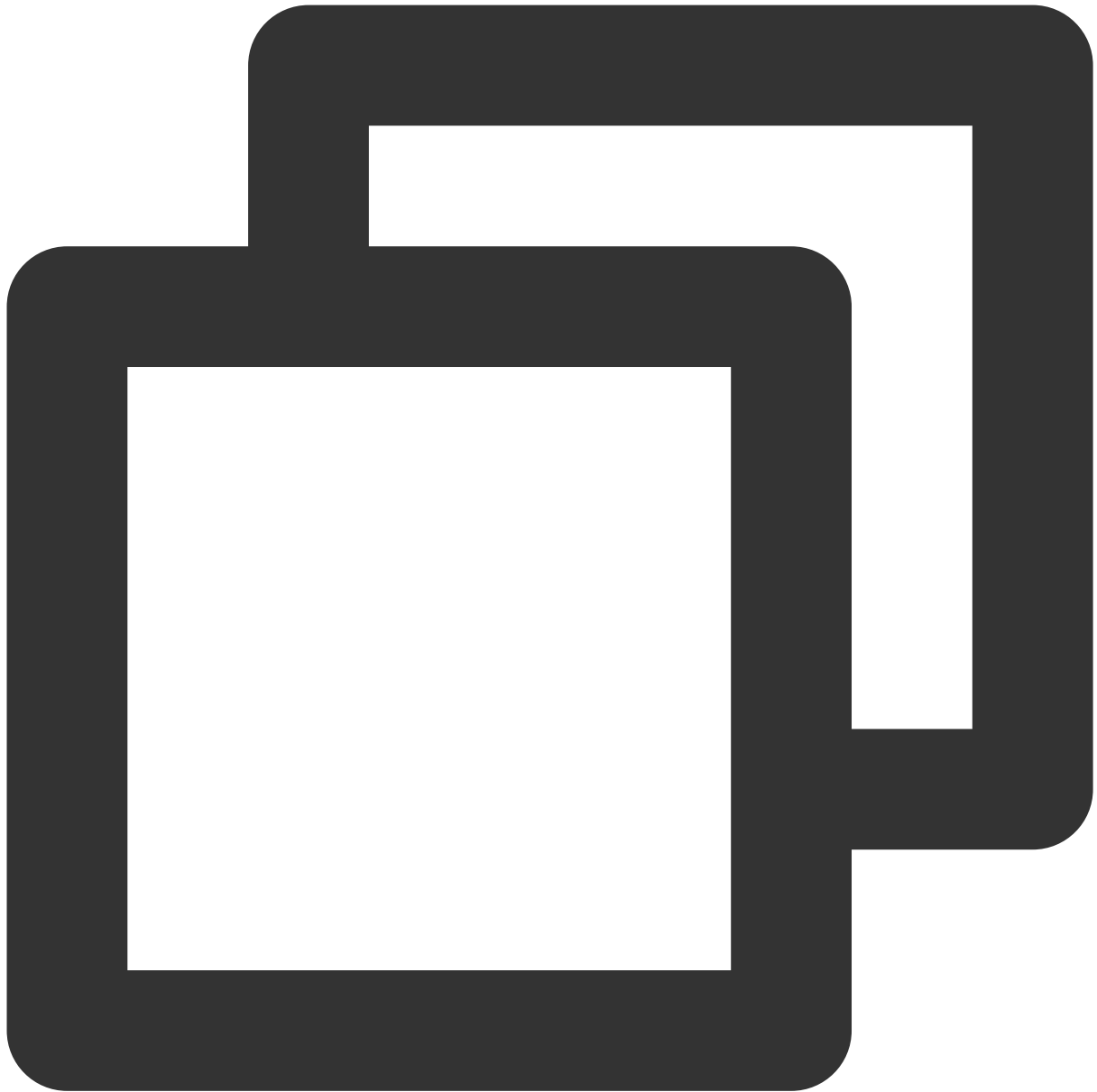
```
docker exec -it 컨테이너 ID /bin/bash
```

컨테이너를 이미지로 만듭니다.



```
docker commit <컨테이너 ID 또는 컨테이너 이름> [<레지스트리 이름>[:<태그>]]
```

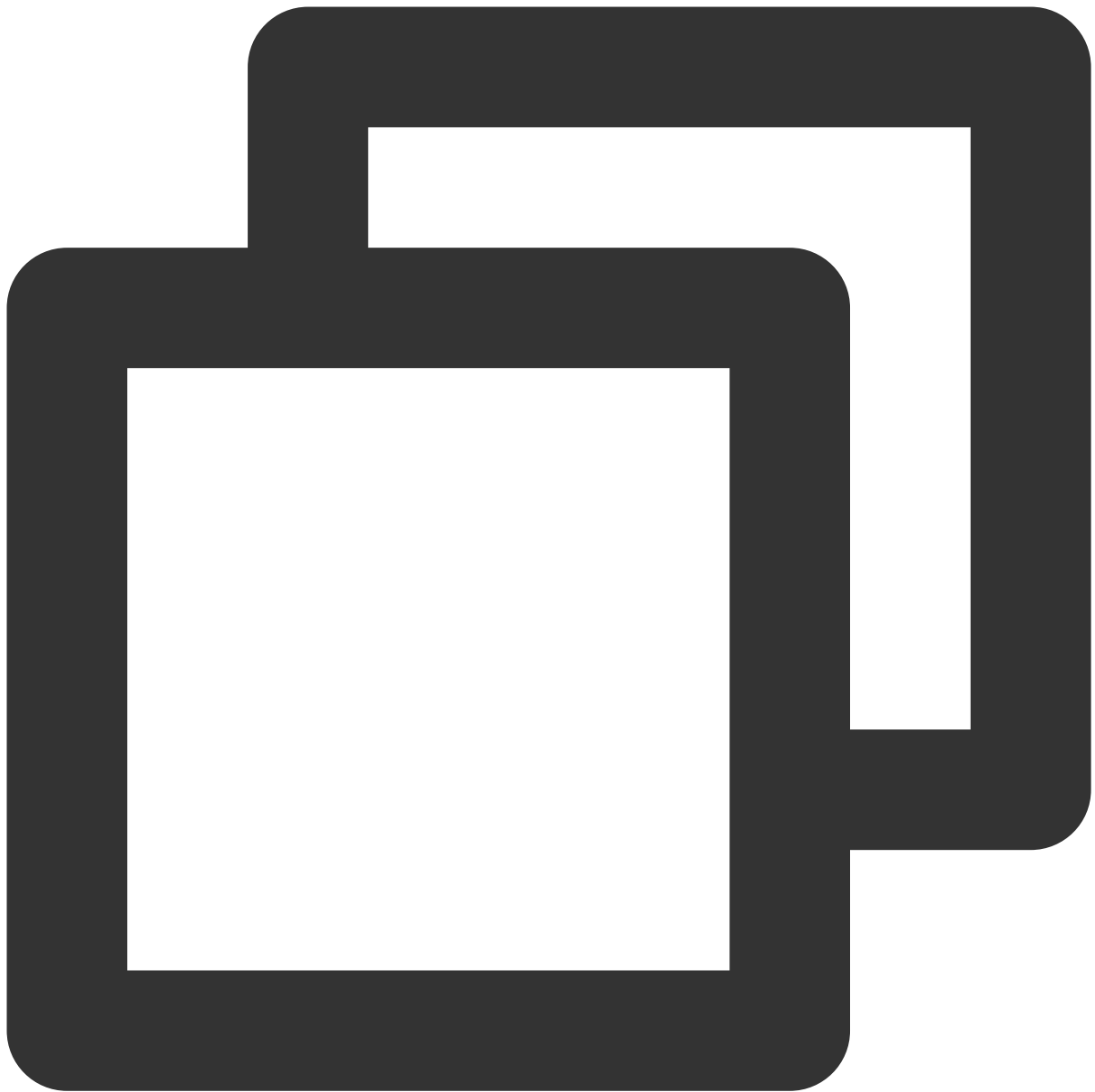
예시:



```
docker commit 1c23456cd7**** tencentyun/nginx:v2
```

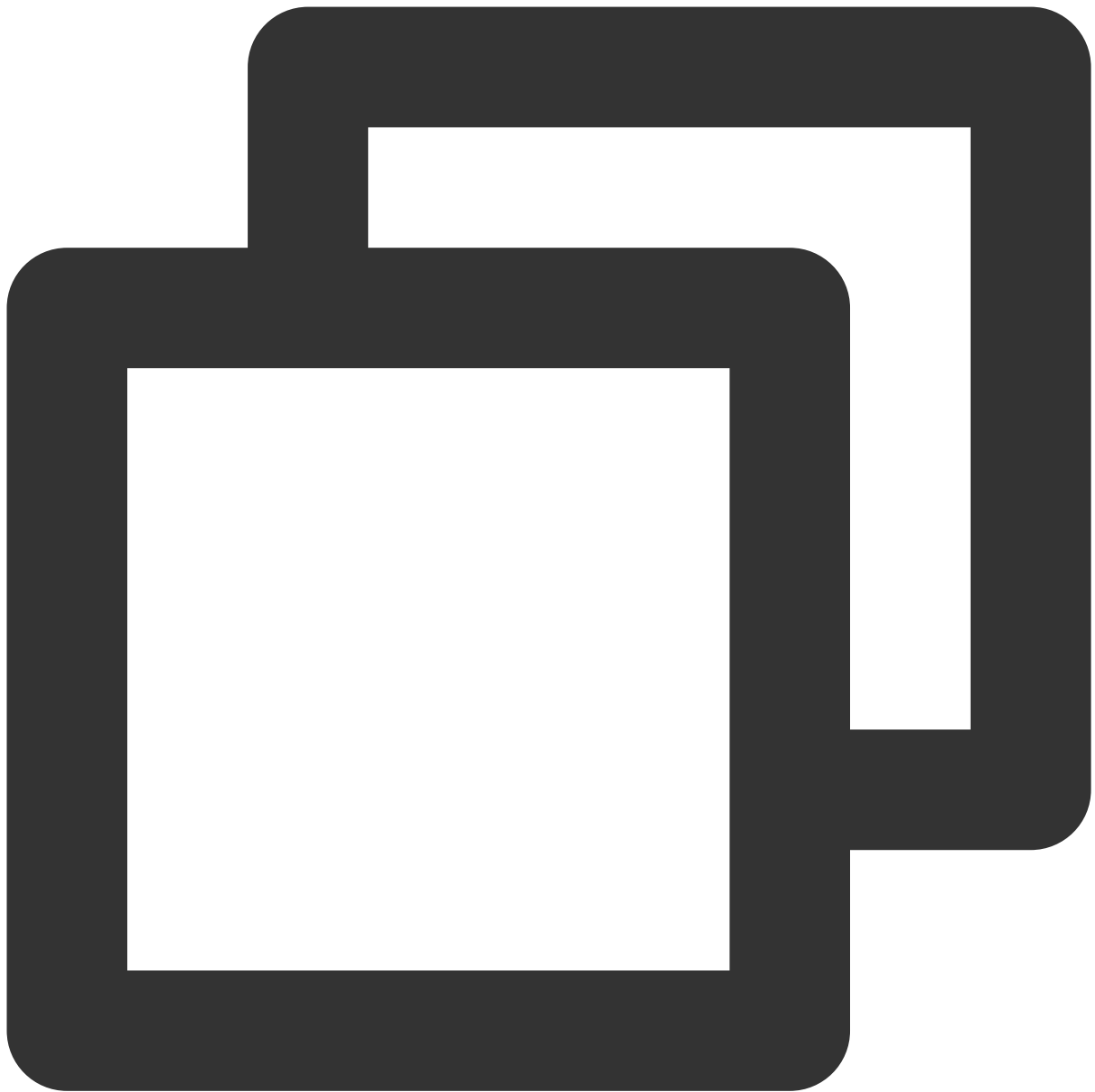
이미지 생성

1. 다음 명령어를 실행하여 Dockerfile 파일을 엽니다.



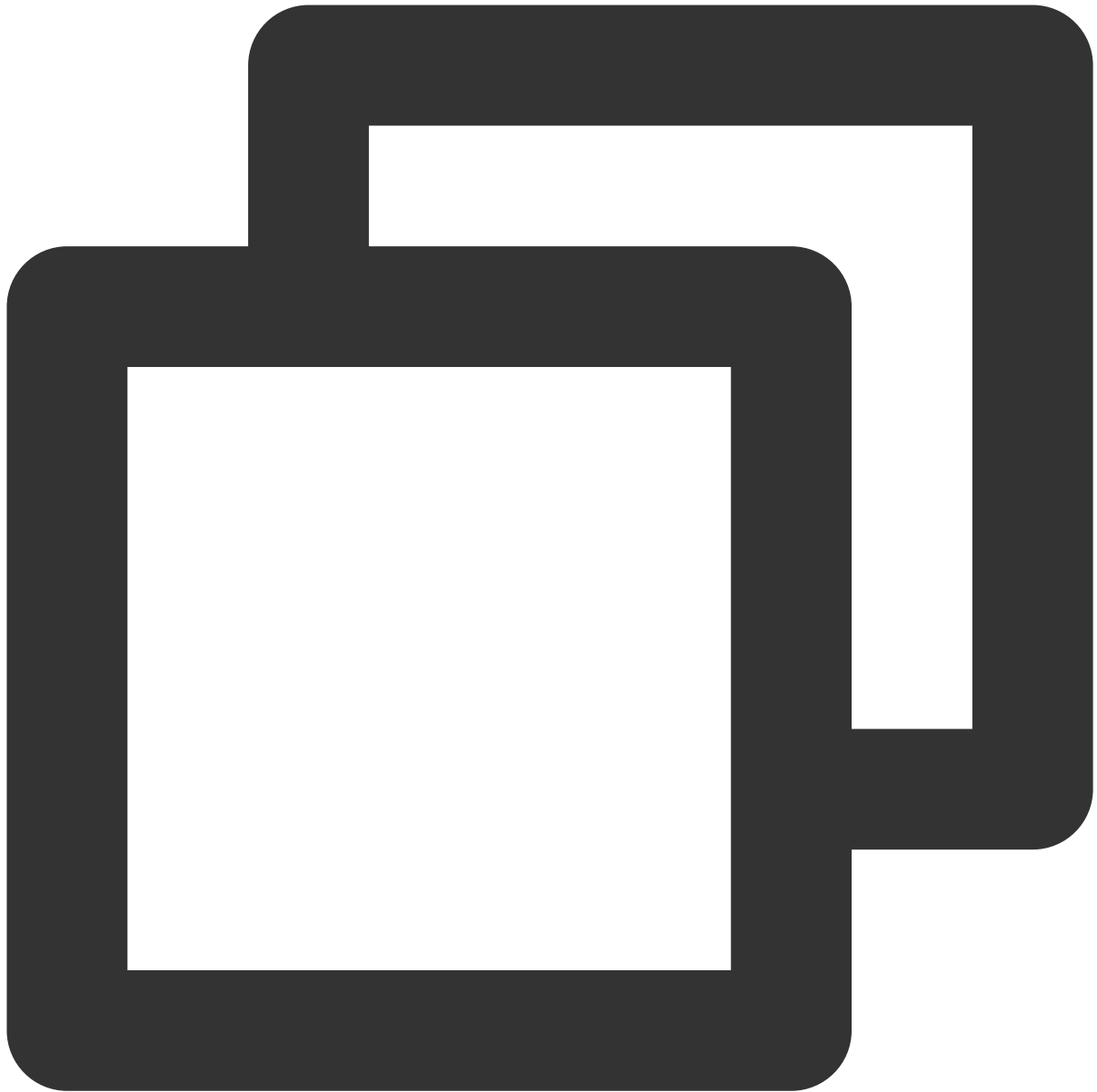
```
vim Dockerfile
```

2. **i**를 눌러 편집 모드로 전환하고 다음을 추가합니다.



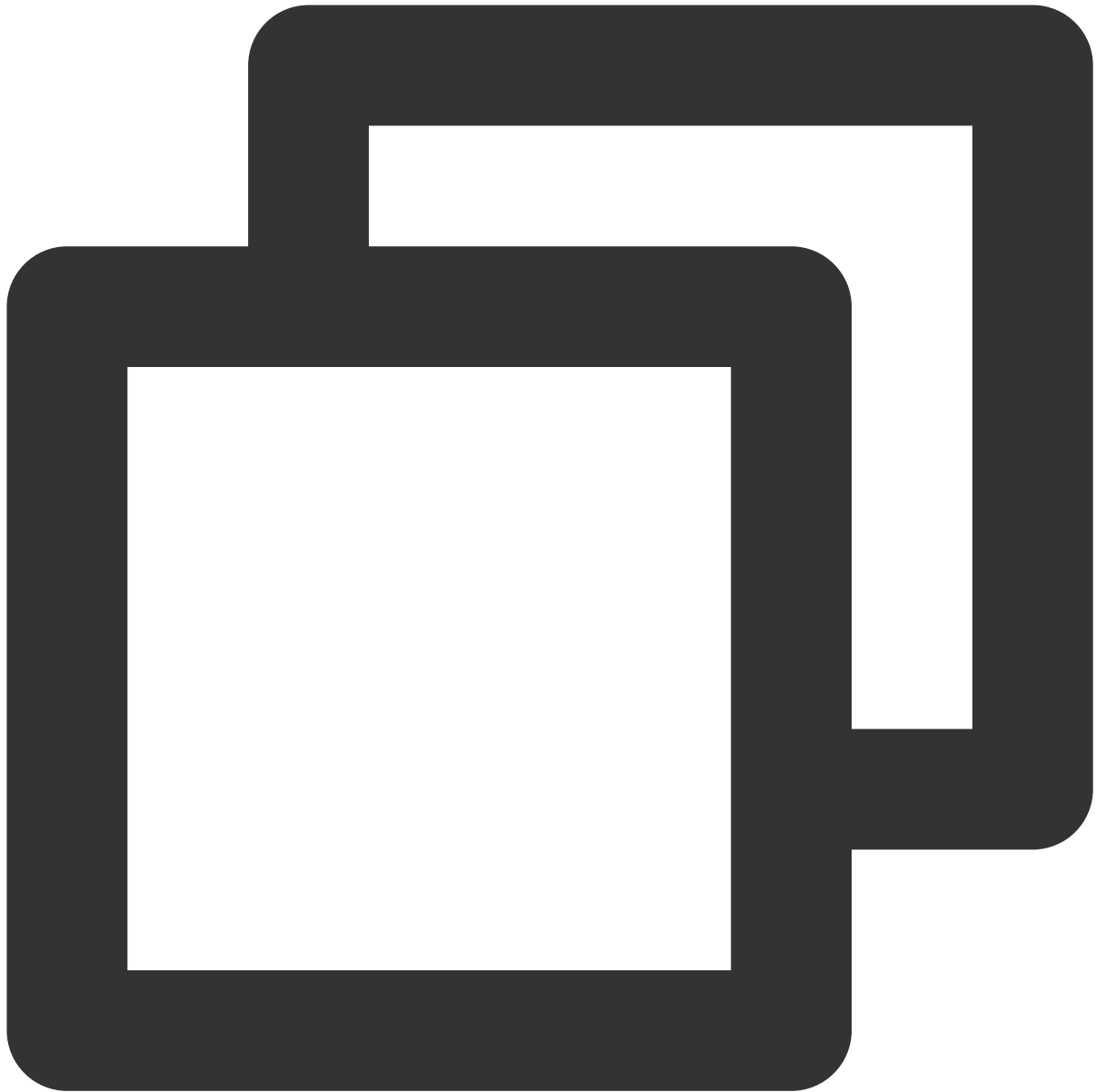
```
FROM tencentyun/nginx:v2 #기본 이미지 출처 성명.  
MAINTAINER DTSTACK #이미지 소유자 성명.  
RUN mkdir /dtstack # RUN 뒤에는 컨테이너가 실행되기 전에 실행해야 하는 명령어를 입력합니다. D  
ENTRYPOINT ping https://cloud.tencent.com/ #시작 실행 명령어. 여기서 마지막 명령어는 포그i
```

3. **Esc**를 누르고 **:wq**를 입력하여 파일을 저장하고 뒤로 돌아갑니다.
4. 다음 명령어를 실행하여 이미지를 빌드합니다.



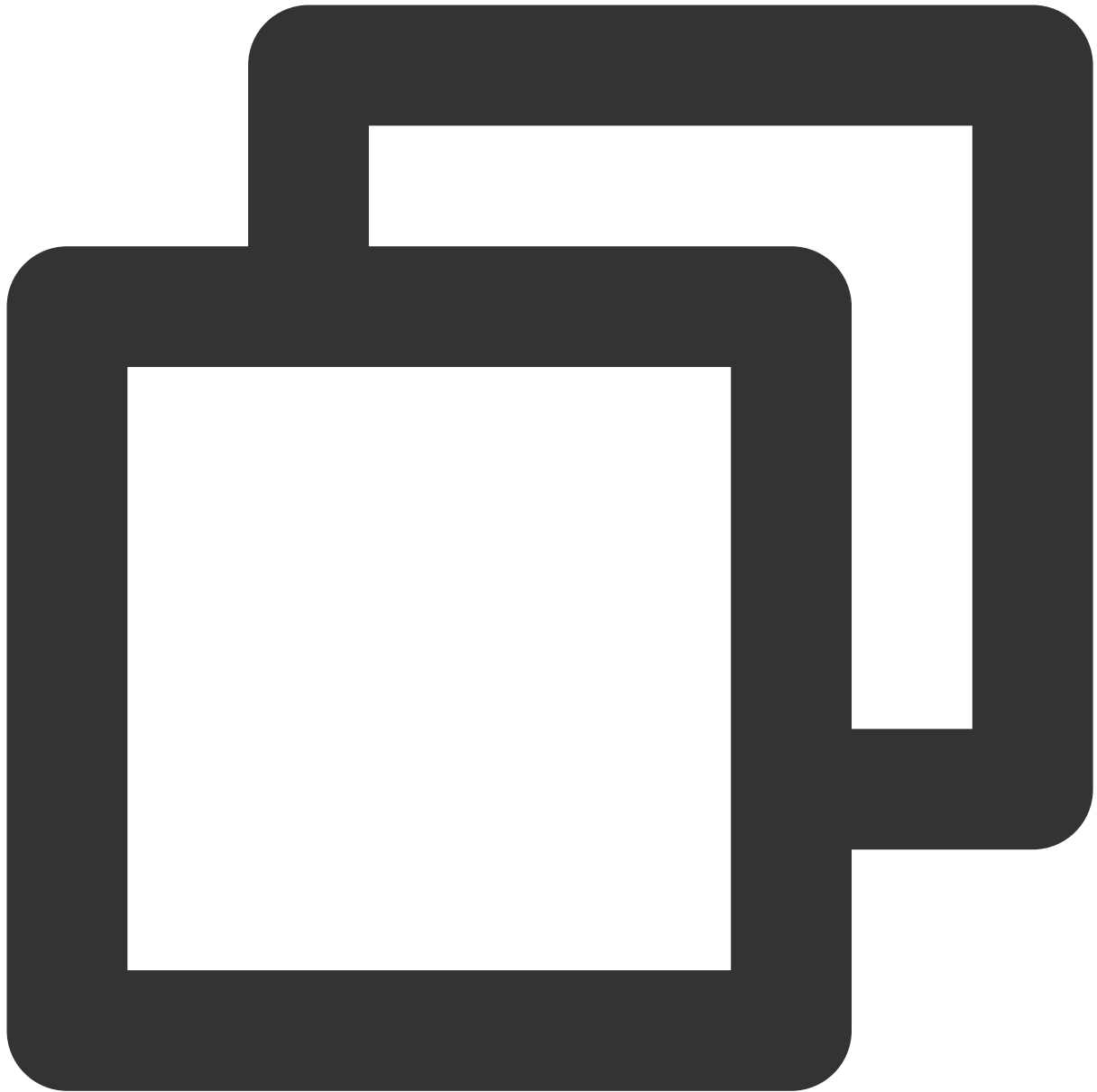
```
docker build -t nginxos:v1 . #. Dockerfile 파일의 경로이며 무시할 수 없습니다.
```

5. 다음 명령어를 실행하여 이미지가 성공적으로 생성되었는지 확인합니다.



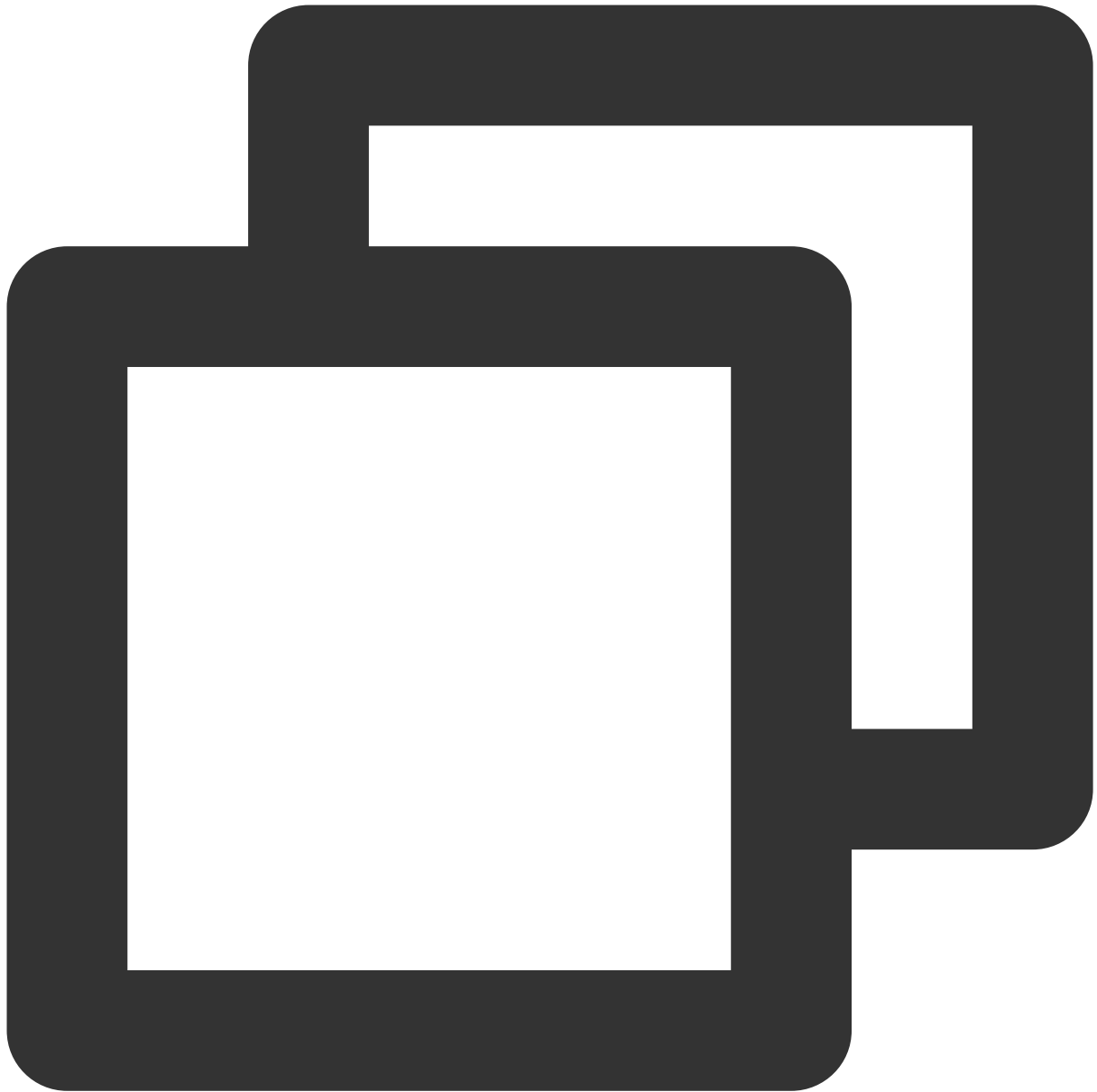
```
docker images
```

6. 다음 명령어를 순서대로 실행하여 컨테이너를 실행 및 확인합니다.



```
docker run -d nginxos:v1      #백그라운드에서 컨테이너를 실행합니다.  
docker ps                    #현재 실행 중인 컨테이너를 확인합니다.  
docker ps -a                 #실행되지 않는 컨테이너를 포함한 모든 컨테이너를 확인합니다.  
docker logs CONTAINER ID/IMAGE #방금 실행한 컨테이너가 표시되지 않으면 컨테이너 ID 또는 c
```

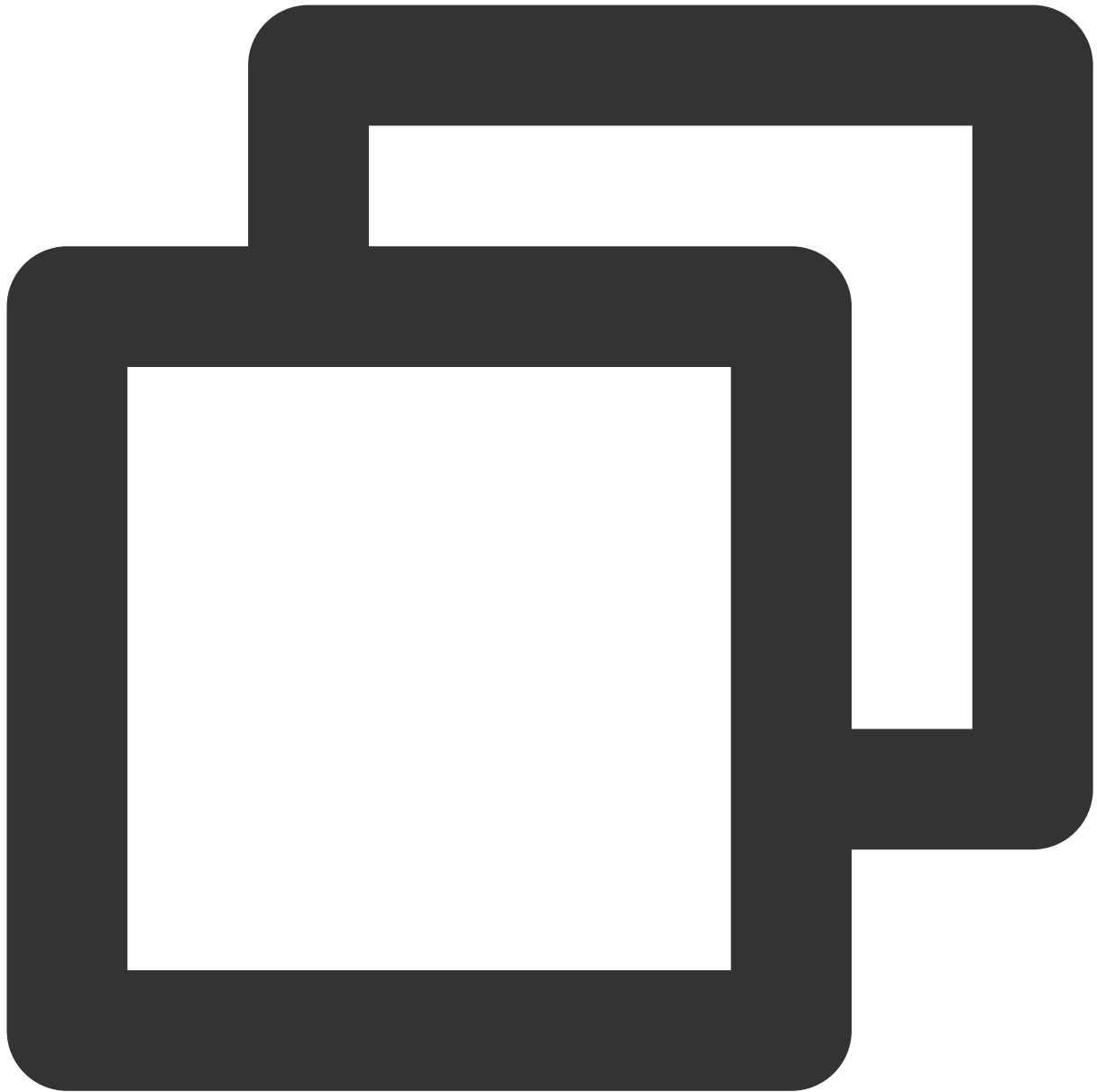
7. 다음 명령어를 순서대로 실행하여 이미지를 생성합니다.



```
docker commit fb2844b6**** nginxweb:v2 #commit 매개변수 뒤에 빌드할 새 이미지의 컨테이너  
docker images #로컬 (다운로드 및 로컬 생성) 이미지를 나열합니다.
```

8. 다음 명령어를 실행하여 이미지를 원격 웨어하우스로 푸시합니다.

기본적으로 Docker Hub에 푸시합니다. 먼저 Docker에 로그인하고 이미지에 연결을 바인딩하고 'Docker 사용자 이름/이미지 이름:태그' 형식으로 이미지 이름을 생성한 후 마지막으로 푸시를 완료해야 합니다.



```
docker login #실행 후 이미지 레지스트리의 사용자 이름과 비밀번호 입력
docker tag [이미지 이름]:[태그] [사용자 이름]:[태그]
docker push [사용자 이름]:[태그]
```

푸시가 완료되면 브라우저로 **Docker Hub** 공식 홈페이지에 로그인하여 볼 수 있습니다.

GitLab 구축

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

GitLab은 Ruby를 사용하여 개발한 오픈 소스 버전의 관리 시스템으로, Git를 소스 관리 툴로 삼아, 자가 호스팅 Git 프로젝트 리포지토리를 구현할 수 있으며, Web 인터페이스를 통해 오픈 또는 개인 프로젝트에 액세스할 수 있습니다. 본 문서에서는 Tencent Cloud CVM에 GitLab을 설치하고 또한 이를 사용하는 방법에 대해 소개합니다.

예시 버전

본 문서에서 사용하는 CVM 설정은 다음과 같습니다.

vCPU: 듀얼코어

메모리: 4GB

Linux 운영 체제: 본 문서는 CentOS 7.7을 예로 듭니다.

전제 조건

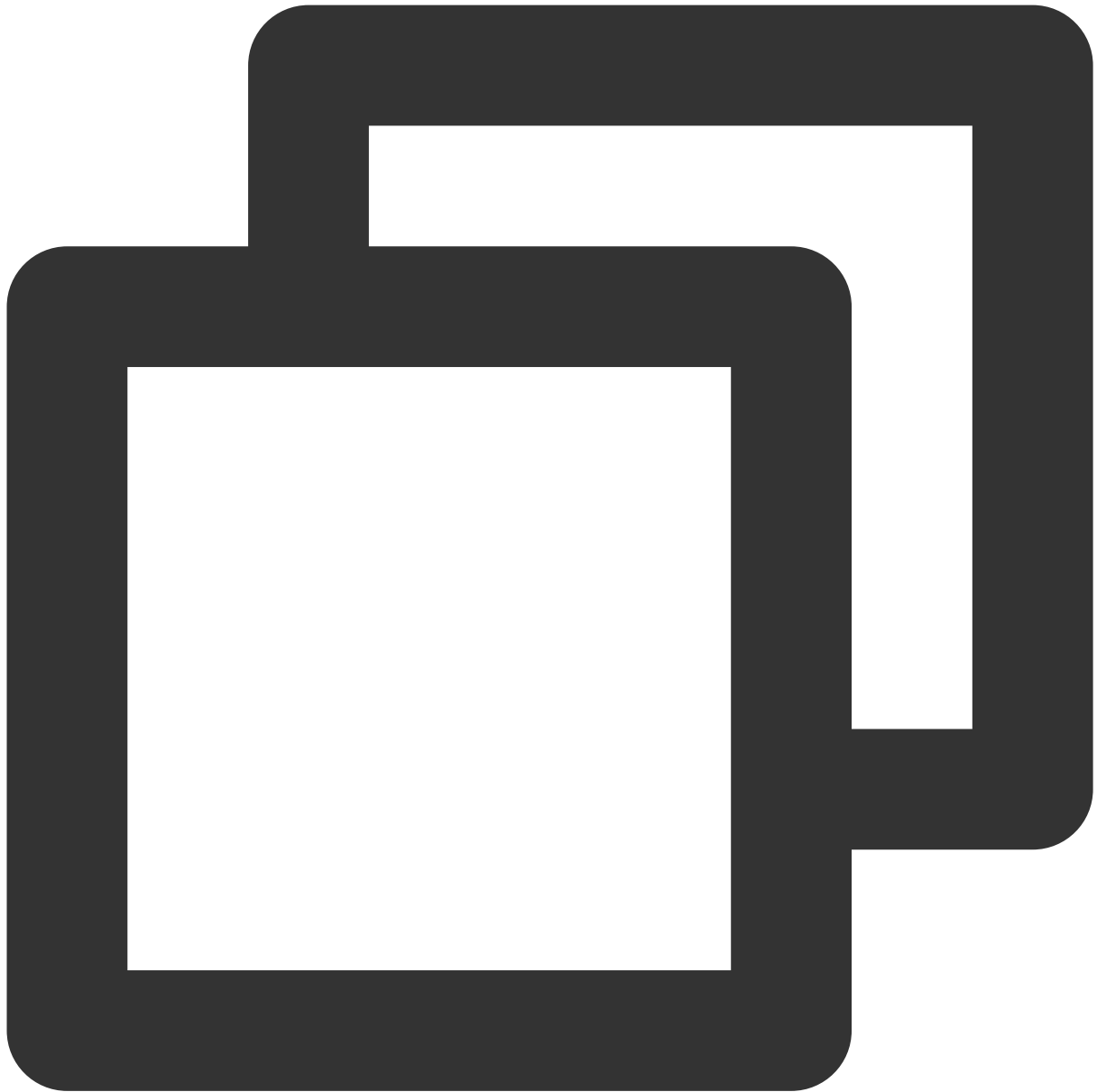
Linux CVM을 구비해야 합니다. CVM을 구매하지 않았다면, [Linux CVM 사용자 정의 설정](#)을 참조 바랍니다.

Linux 인스턴스에 보안 그룹 규칙(80 포트 개방)이 설정되어 있어야 합니다. 자세한 내용은 [보안 그룹 규칙 추가](#)를 참조 바랍니다.

작업 순서

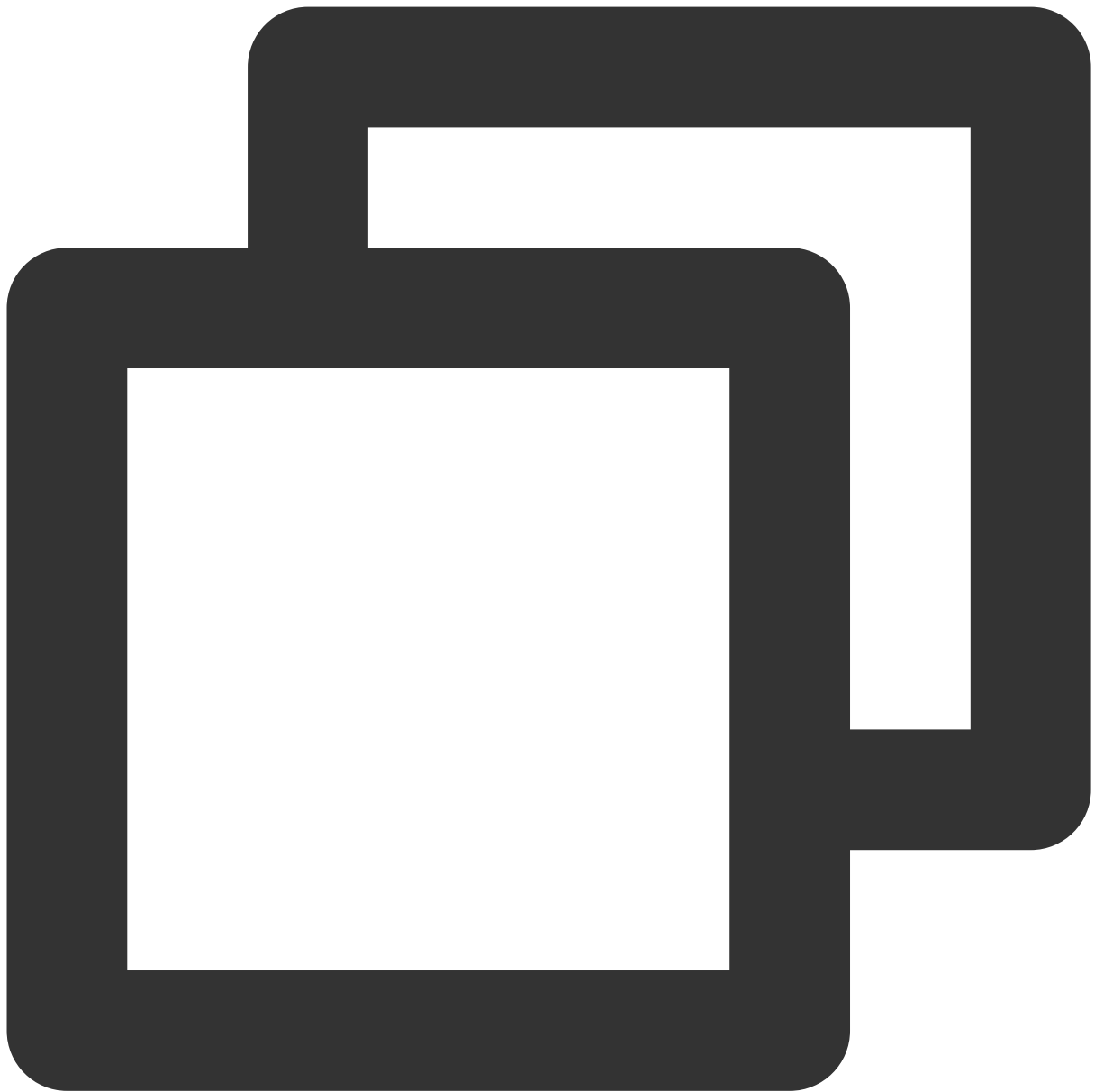
GitLab 설치

1. [표준 방식으로 Linux 인스턴스에 로그인\(권장\)](#). 실제 작업 스타일에 따라 다른 로그인 방식을 선택할 수 있습니다. [원격 로그인 소프트웨어를 사용하여 Linux 인스턴스에 로그인](#)
[SSH를 사용하여 Linux 인스턴스에 로그인](#)
2. 다음 명령어를 실행하여 종속 패키지를 설치합니다.

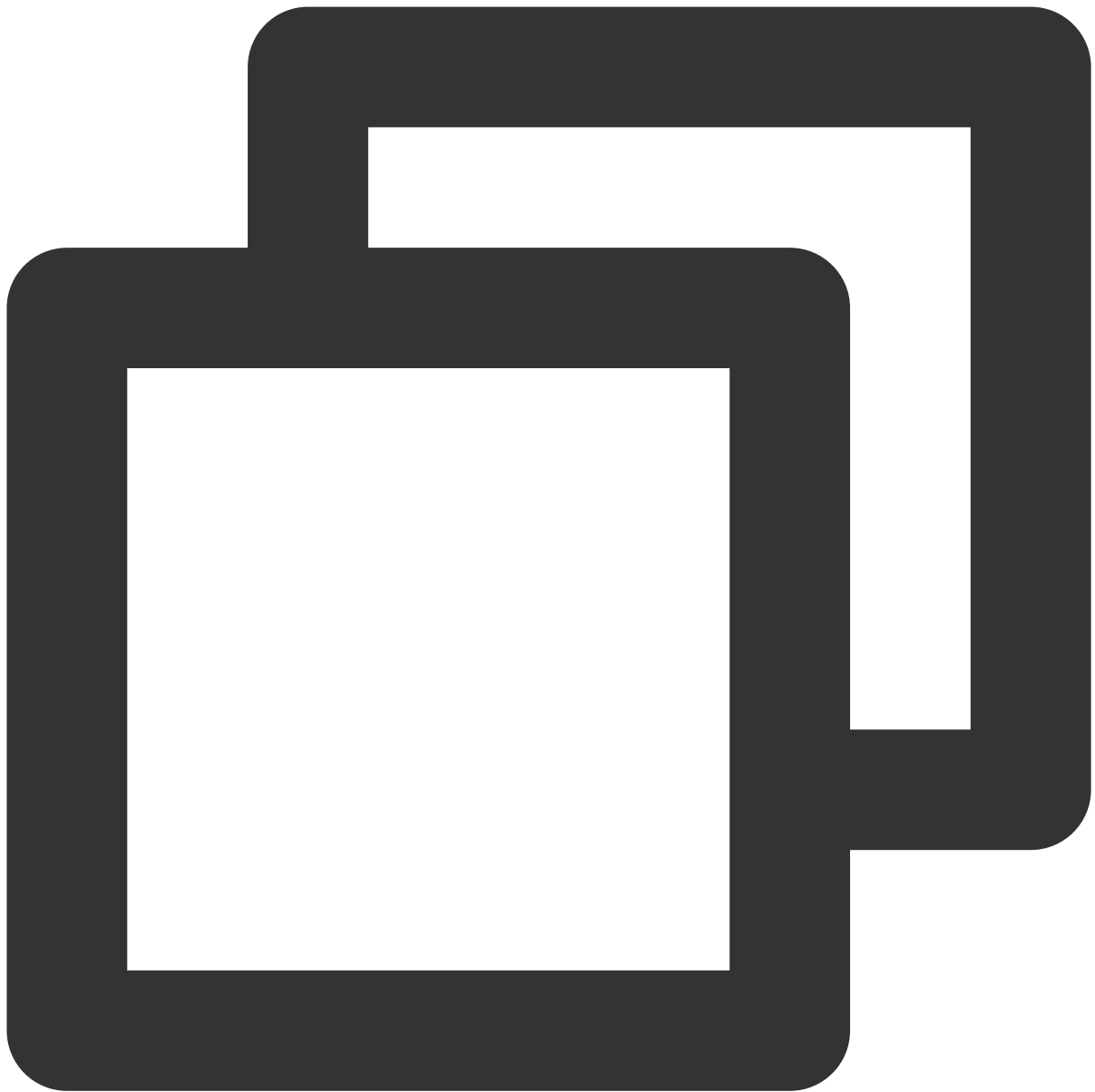


```
yum install -y curl policycoreutils-python openssh-server
```

3. 다음 명령어를 순서대로 실행하여 부팅 시 SSH 자동 실행으로 설정하고 SSH 서비스를 실행합니다.

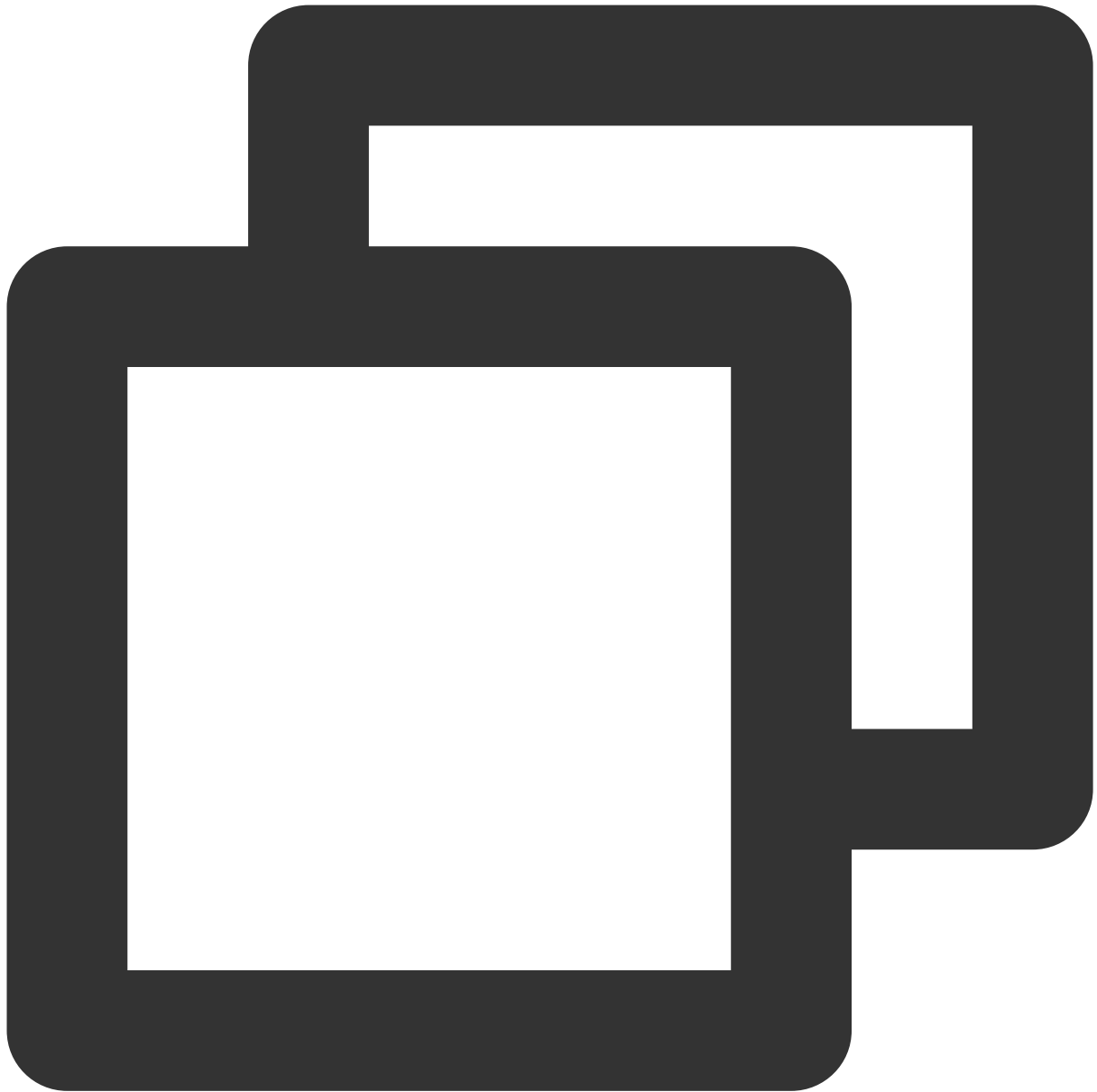


```
systemctl enable sshd
```



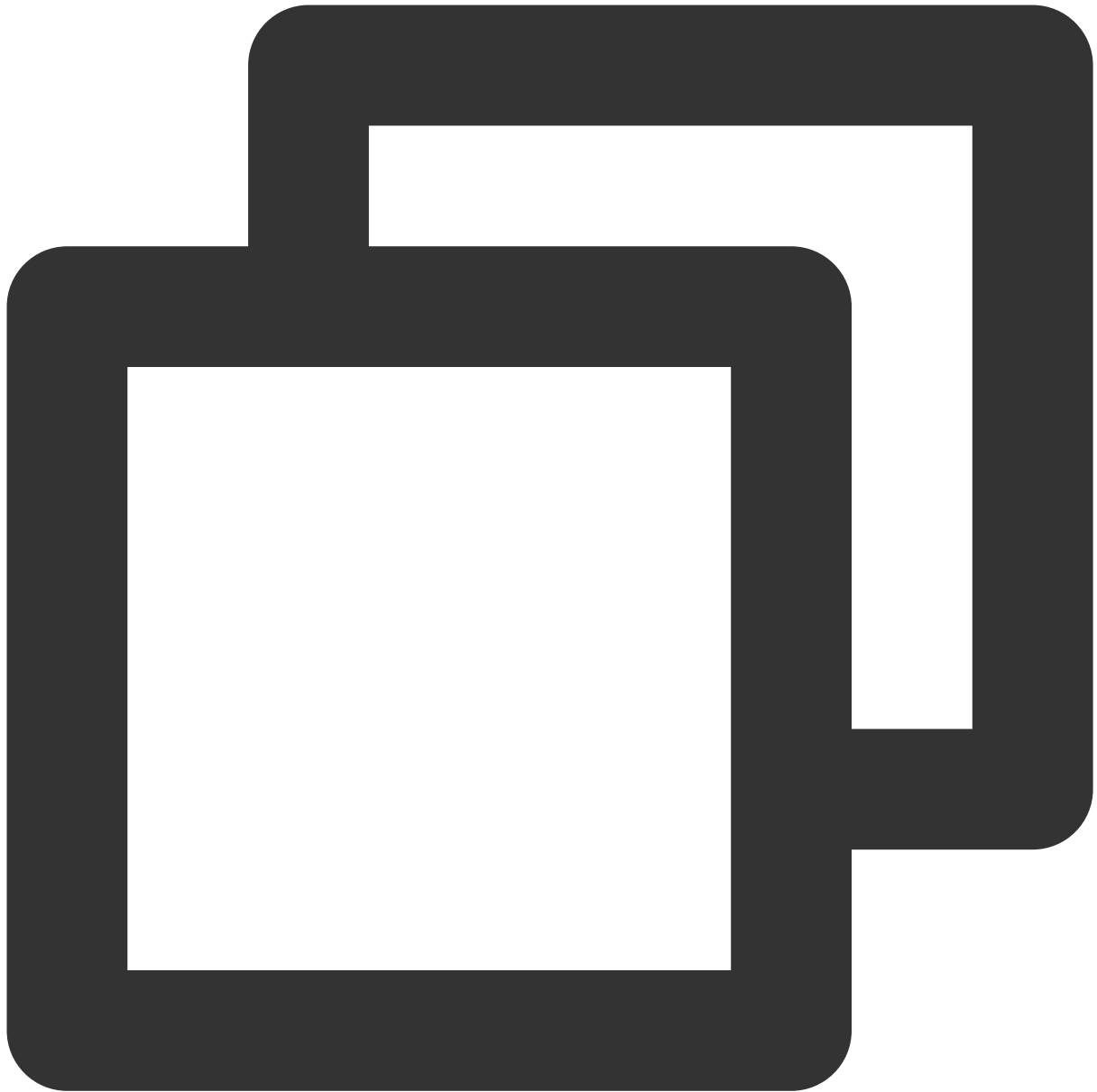
```
systemctl start sshd
```

4. 다음 명령어를 실행하여 Postfix를 설치합니다.



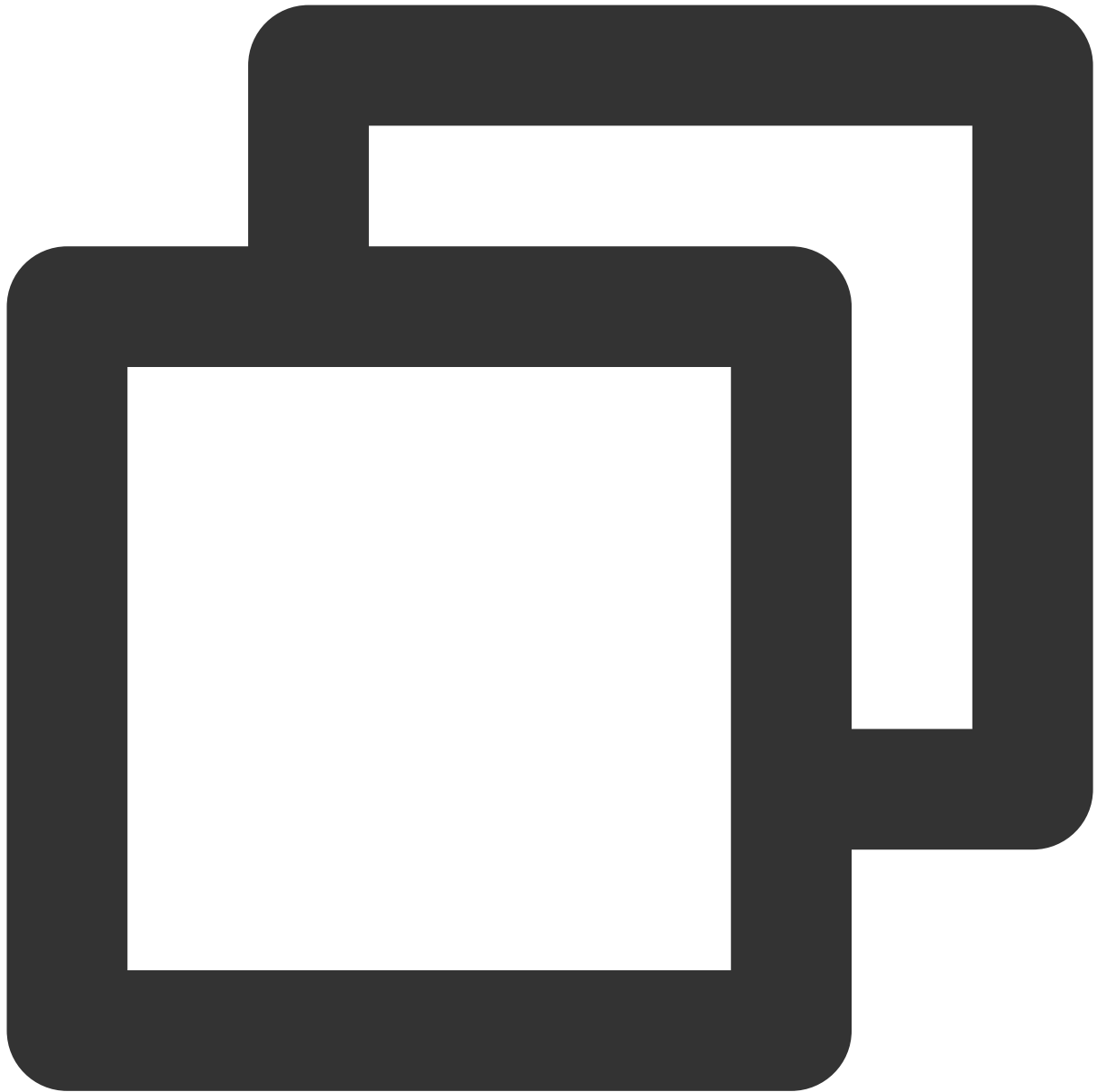
```
yum install -y postfix
```

5. 다음 명령어를 실행하여 부팅 시 **Postfix** 자동 실행으로 설정합니다.



```
systemctl enable postfix
```

6. 다음 명령어를 실행하여 Postfix의 구성 파일 main.cf를 엽니다.



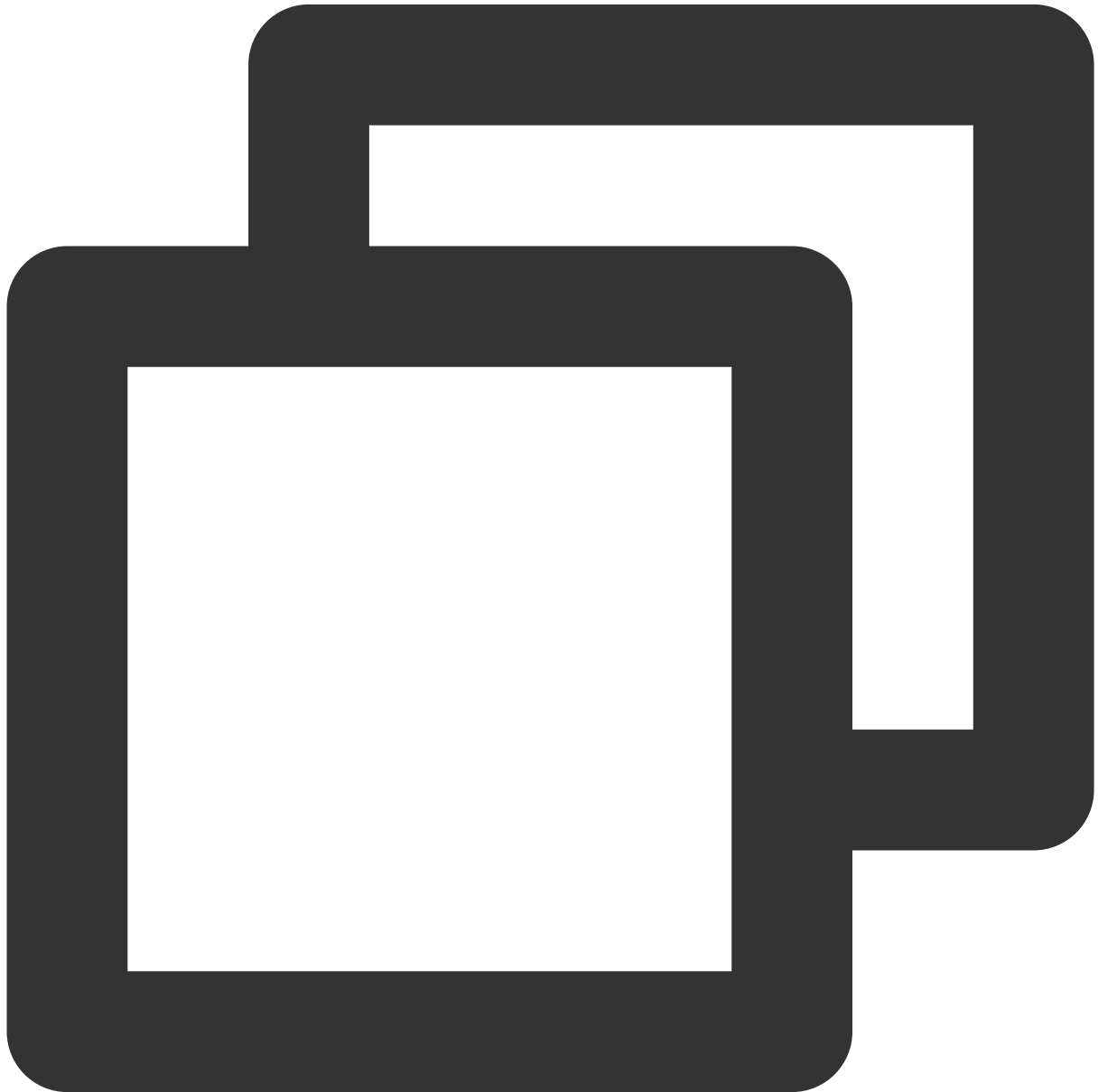
```
vim /etc/postfix/main.cf
```

7. **i**를 눌러 편집 모드로 이동하고, `inet_interfaces = all` 앞의 `#` 을 삭제한 다음, `inet_interfaces = localhost` 앞에 `#` 을 추가합니다. 수정이 완료되면 아래 이미지와 같습니다.

```
inet_interfaces = all
#inet_interfaces = $myhostname
#inet_interfaces = $myhostname, localhost
#inet_interfaces = localhost
```

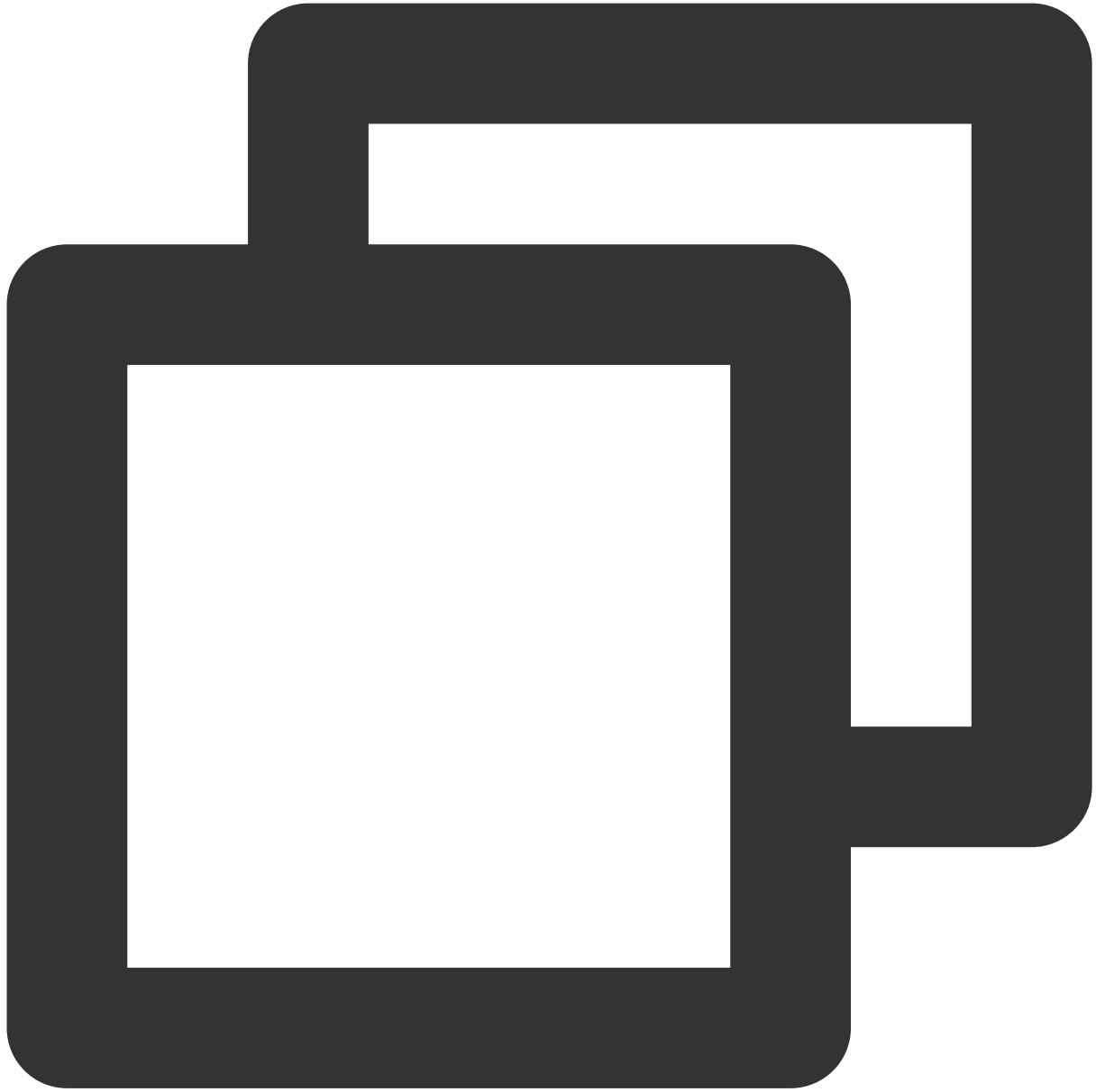
8. **Esc**를 누르고 **:wq**를 입력하여 수정된 내용을 저장하고 종료합니다.

9. 다음 명령어를 실행하여 Postfix를 실행합니다.



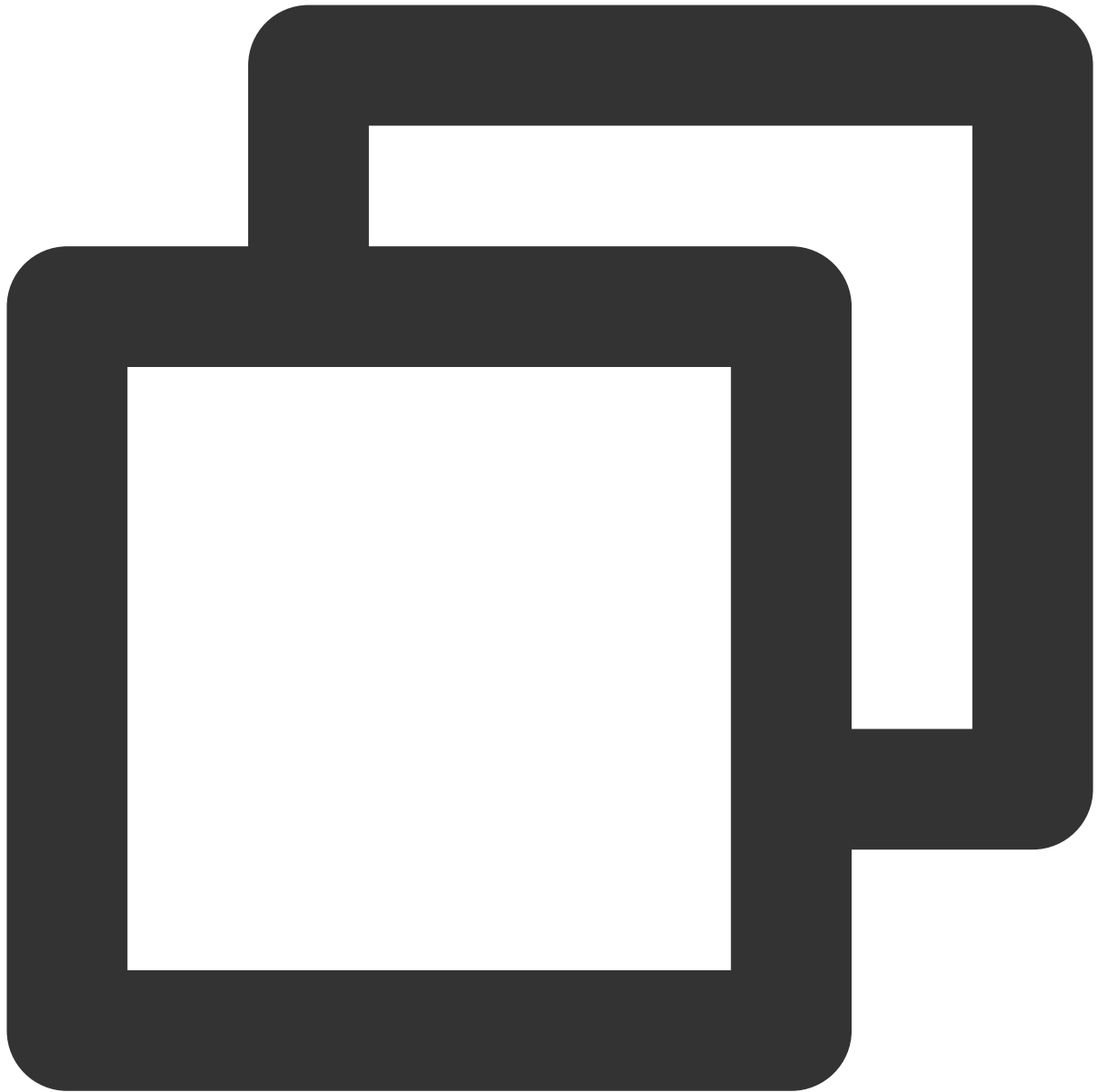
```
systemctl start postfix
```

10. 다음 명령어를 실행하여 GitLab 소프트웨어 패키지의 리포지토리를 추가합니다.



```
curl https://packages.gitlab.com/install/repositories/gitlab/gitlab-ce/script.rpm.
```

11. 다음 명령어를 실행하여 GitLab을 설치합니다.



```
sudo EXTERNAL_URL="인스턴스 공인 IP 주소" yum install -y gitlab-ce
```

인스턴스의 공인 IP 획득 방법은 [공인 IP 주소 획득](#)을 참조 바랍니다.

12. 로컬 브라우저에서 획득한 공인 IP에 액세스하여 반환되는 페이지가 아래 이미지와 같다면, GitLab 설치에 성공했음을 의미합니다.

주의사항 :

해당 페이지에서 GitLab 로그인 계정의 비밀번호를 설정하시기 바랍니다.



 Please create a password for your new account.

GitLab Community Edition

A complete DevOps platform

GitLab is a single application for the entire software development lifecycle. From project planning and source code management to CI/CD, monitoring, and security.

Change your password

New password

Confirm new password

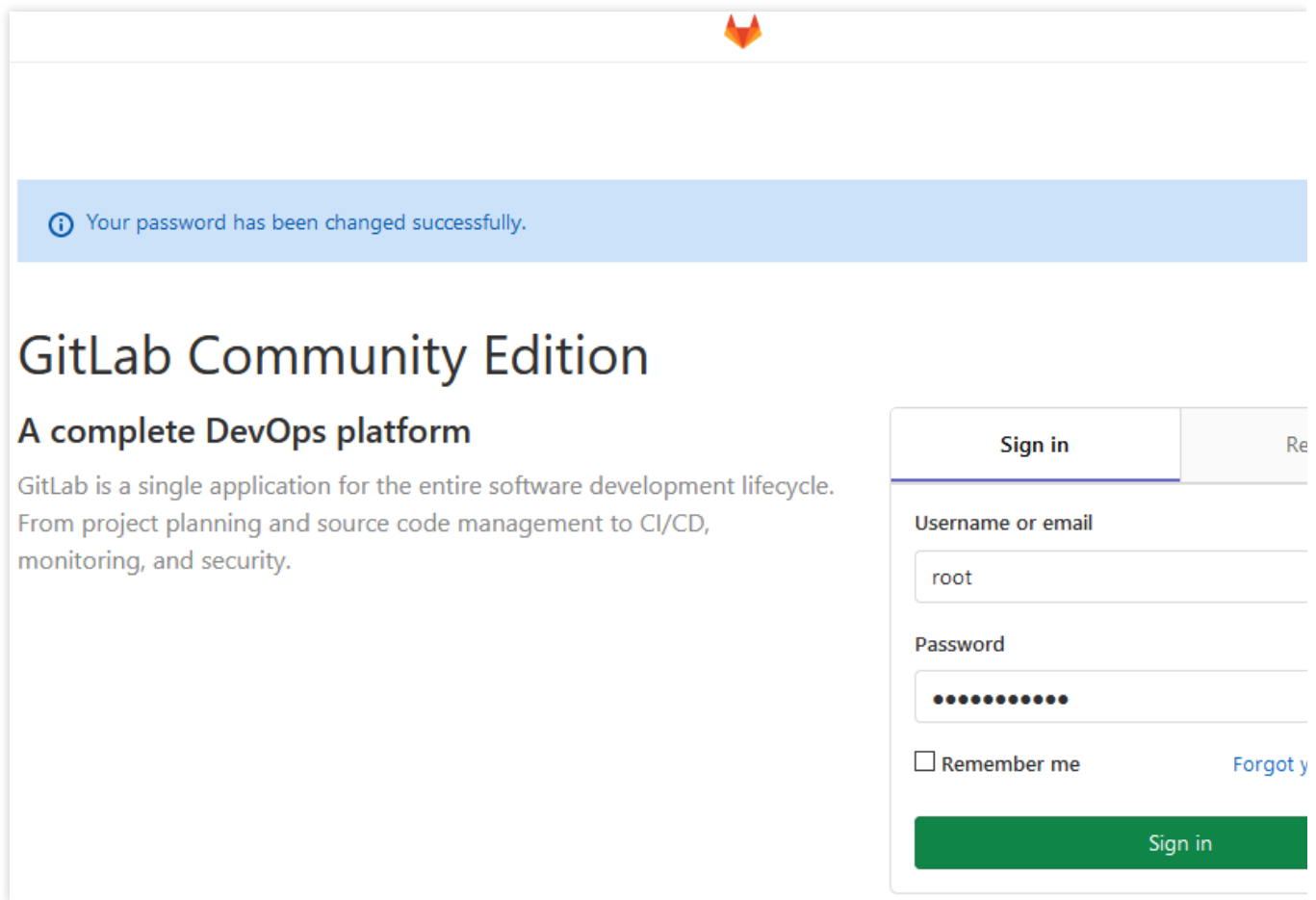
Change your password

[Didn't receive a confirmation email?](#)

[Already have login access?](#)

프로젝트 생성

1. 아래 이미지와 같이 로컬 브라우저에서 CVM의 공인 IP를 액세스하여 GitLab 로그인 인터페이스로 이동한 다음, `root` 계정 및 설정한 로그인 비밀번호로 로그인합니다.



2. 아래 이미지와 같이 페이지 안내에 따라 개인 프로젝트를 생성하며, 본 문서는 `test` 를 예로 듭니다.

Project name

Project URL

Project slug

Want to house several dependent projects under the same namespace? [Create a group.](#)

Project description (optional)

Description format

Visibility Level

☒ **Private**
Project access must be granted explicitly to each user. If this project is part of a group, access will be granted to members of the group.

☐ **Internal**
The project can be accessed by any logged in user.

☐ **Public**
The project can be accessed without any authentication.

☐ **Initialize repository with a README**
Allows you to immediately clone this project's repository. Skip this if you plan to push up an existing repository.

Create project

Cancel

3. 프로젝트 생성을 완료하면 페이지 상단의 [Add SSH Key]를 클릭합니다.
4. 'SSH Keys' 페이지로 이동하여 아래의 순서에 따라 SSH Keys를 추가합니다.
 - 4.1 키 획득을 통해 프로젝트 관리에 들어갈 PC의 키 정보를 획득하고 'Key'에 붙여넣습니다.
 - 4.2 Title 에 해당 키의 이름을 사용자가 지정합니다.
 - 4.3 아래 이미지와 같이 [Add key]를 클릭하고 키를 추가합니다.

SSH Keys

Add an SSH key

Key

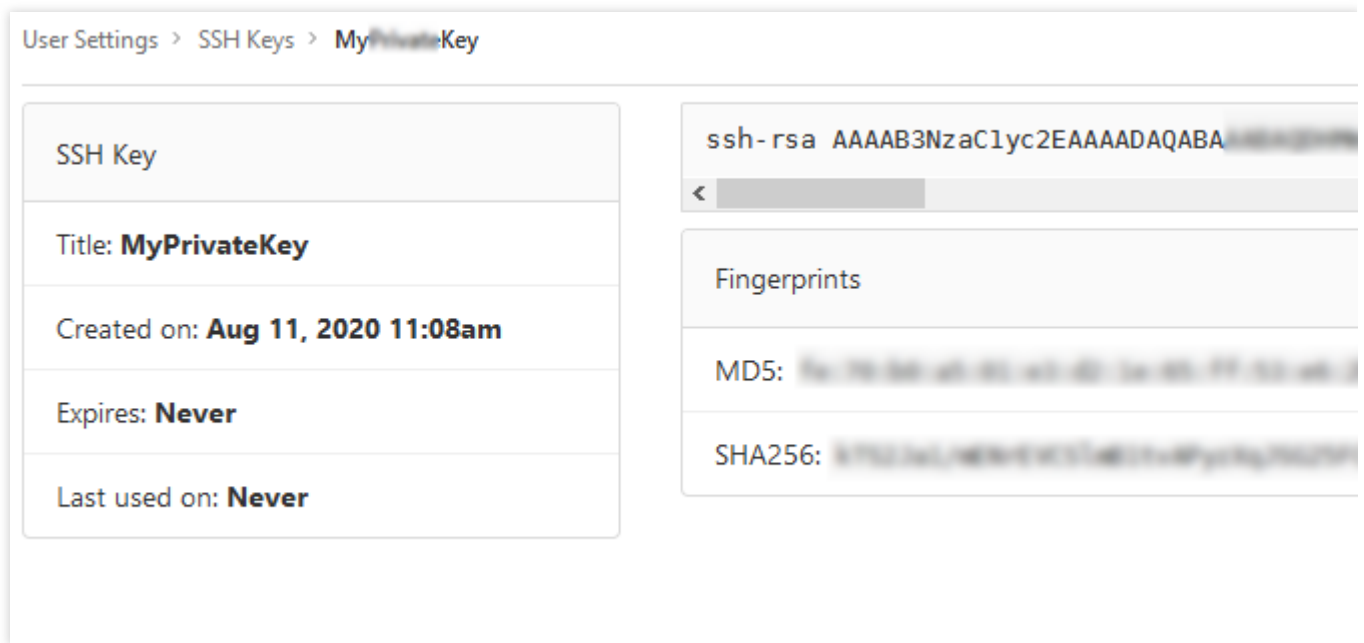
```
ssh-rsa  
AAAAB3NzaC1yc2EAAAADAQABAAQDHMmy2G  
9A=H7ZyT0R8LwOBBW=BX  
J2QH2y6ALu2QFHQzUdY=BBB02.BWwg2OPVd)=  
D4X3w1Thuwj2TB8-u4UC3uKQNCu2u3PVWPydw  
JBBY)=u1achumAMuygWQB=QeOCUHYTHGLu21u  
ly82wg13HWkYn2u2B82=uPQFygAuPMKDCwg5u  
JWC=BAAwPFC3=PC5yBLAwAB
```

Exp

My Private Key

Add key

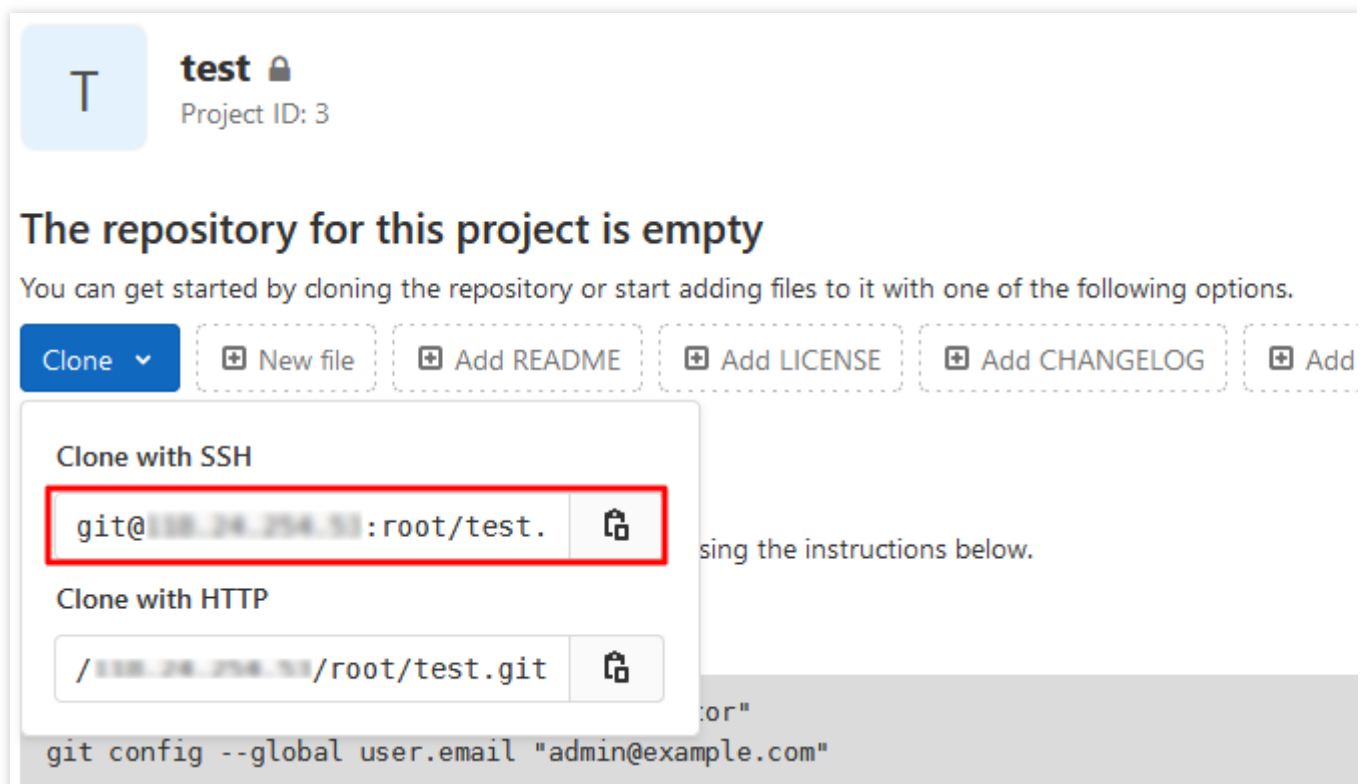
©2013-2022 Tencent Cloud. All rights reserved.



5.

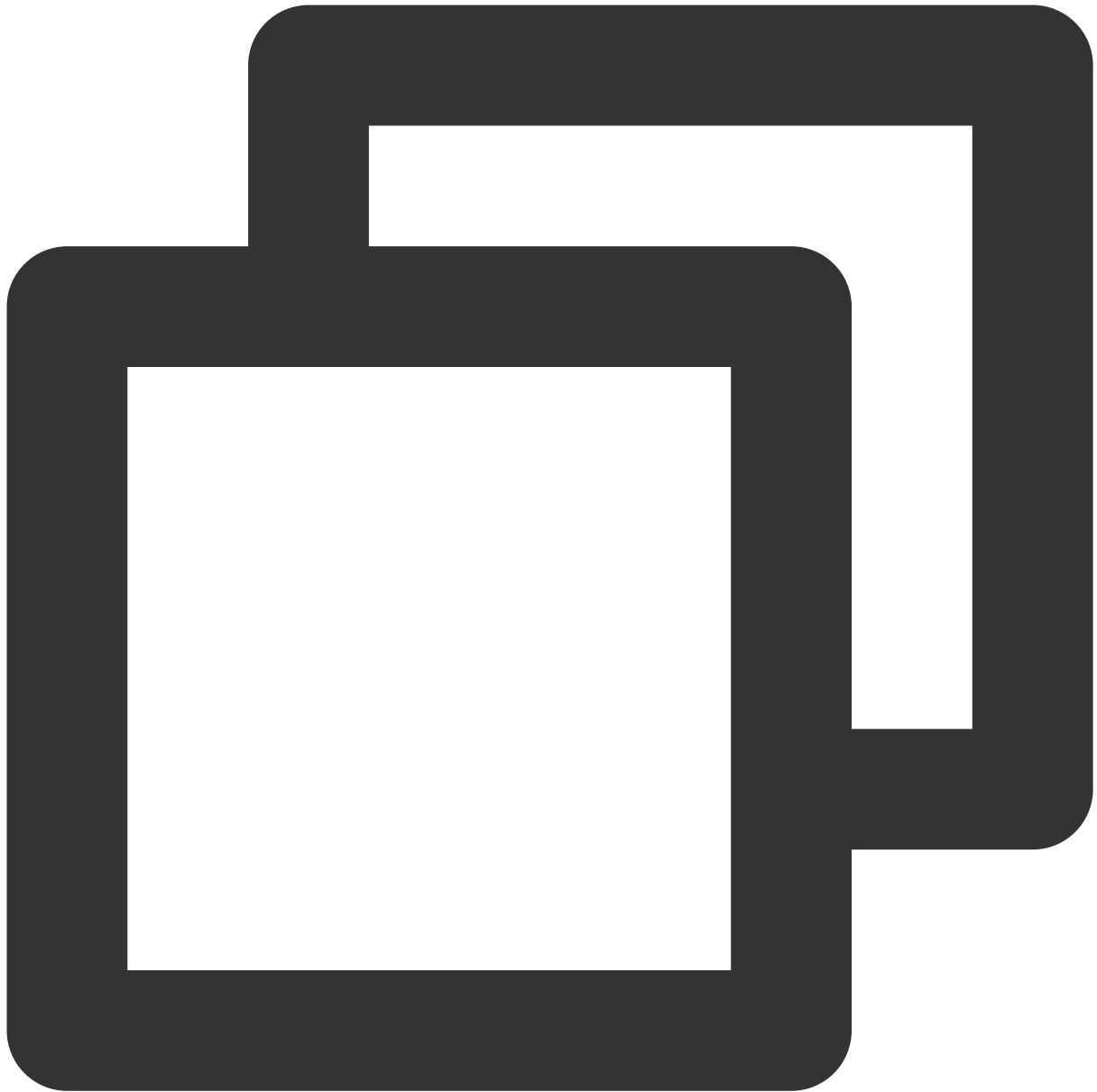
아래

이미지와 같이 프로젝트 메인 페이지로 돌아가 [clone]을 클릭하여 프로젝트 주소를 기록합니다.



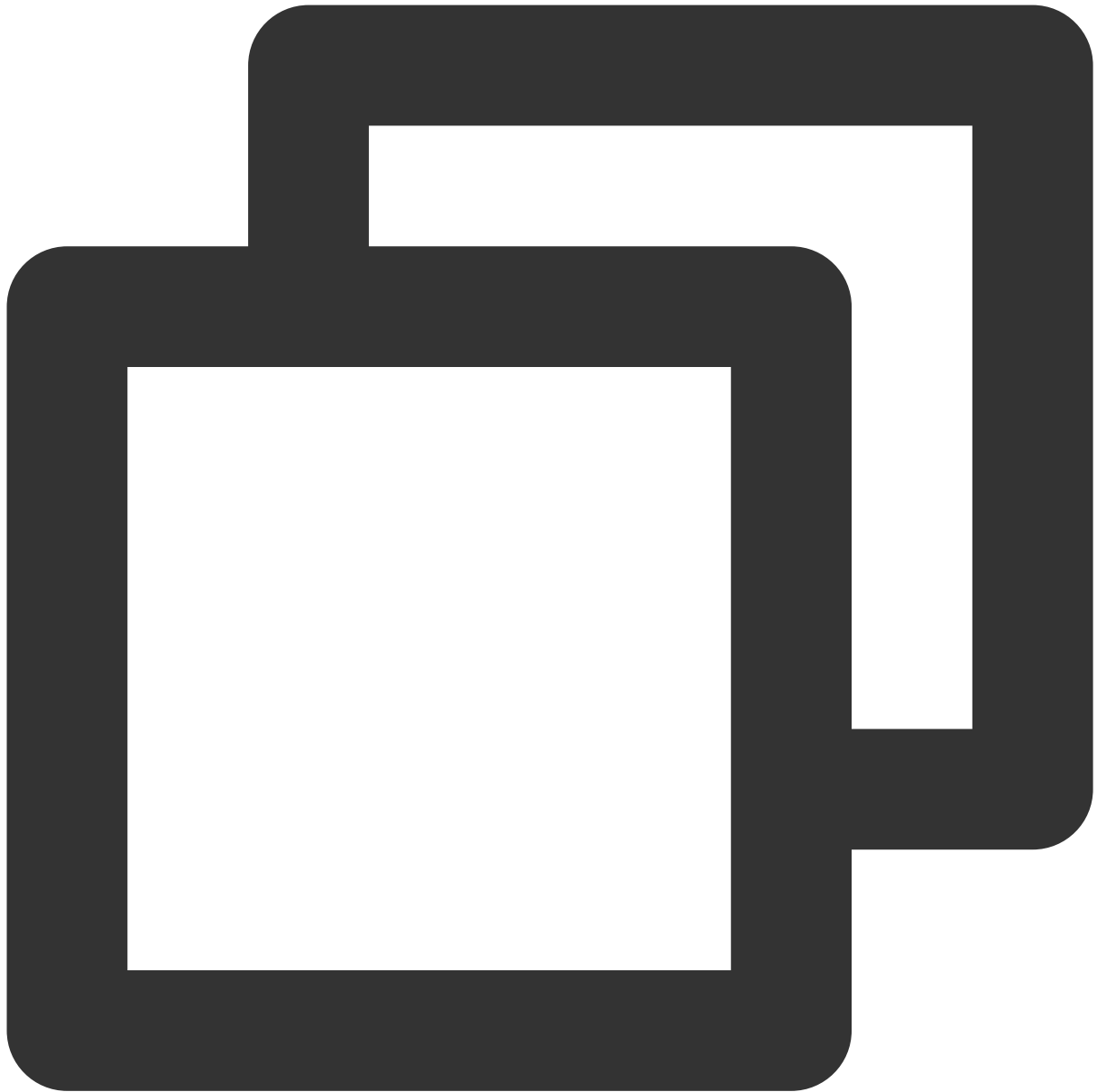
프로젝트 클론

1. 관리에 들어간 PC에서 다음 명령어를 실행하여 git 리포지토리를 사용할 사용자 이름을 설정합니다.



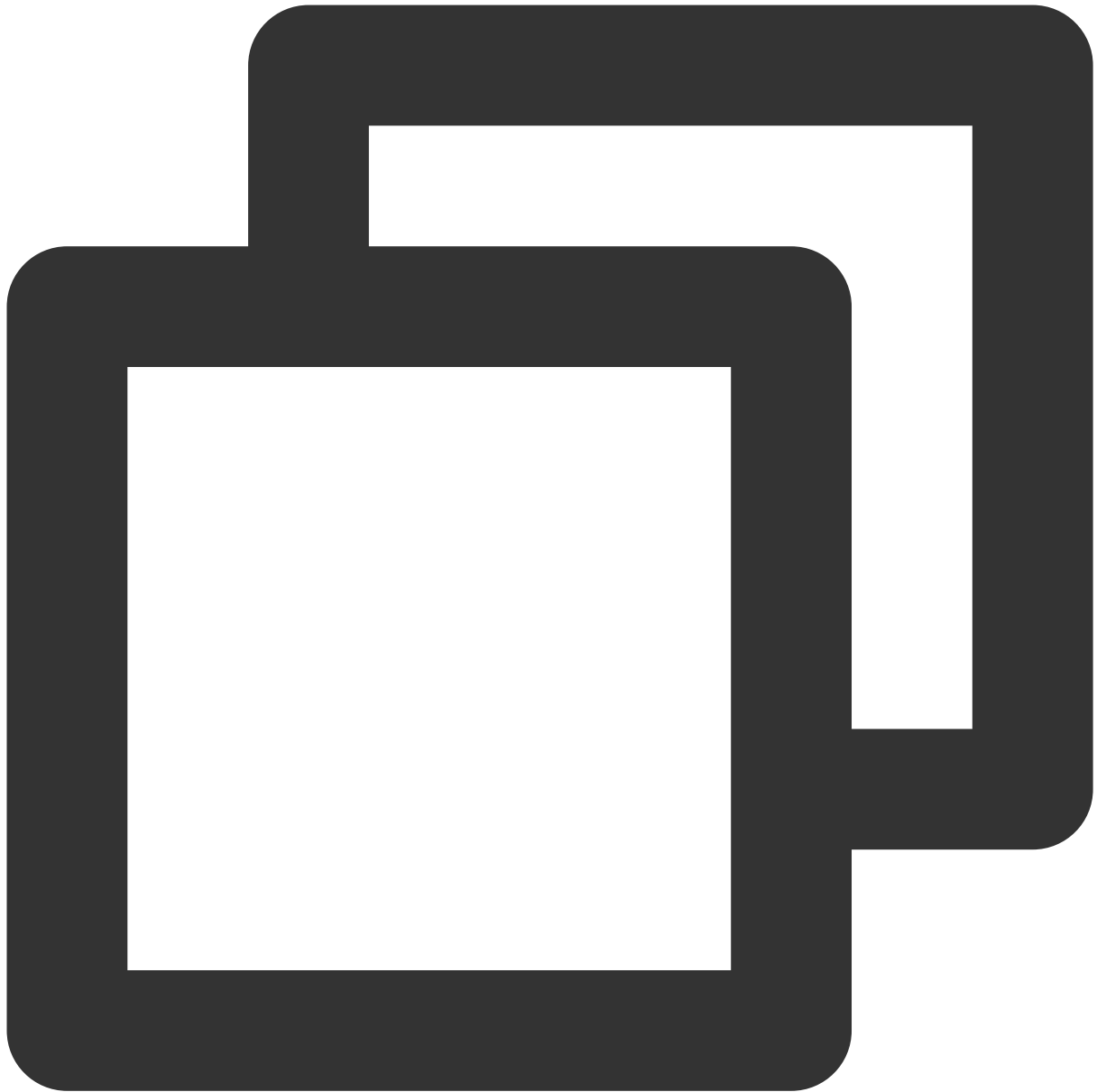
```
git config --global user.name "username"
```

2. 다음 명령어를 실행하여 git 리포지토리를 사용할 사용자의 메일을 설정합니다.



```
git config --global user.email "xxx@example.com"
```

3. 다음 명령어를 실행하여 프로젝트를 클론합니다. 그중에서 '프로젝트 주소'를 [5단계](#)에서 획득한 프로젝트 주소로 변경합니다.

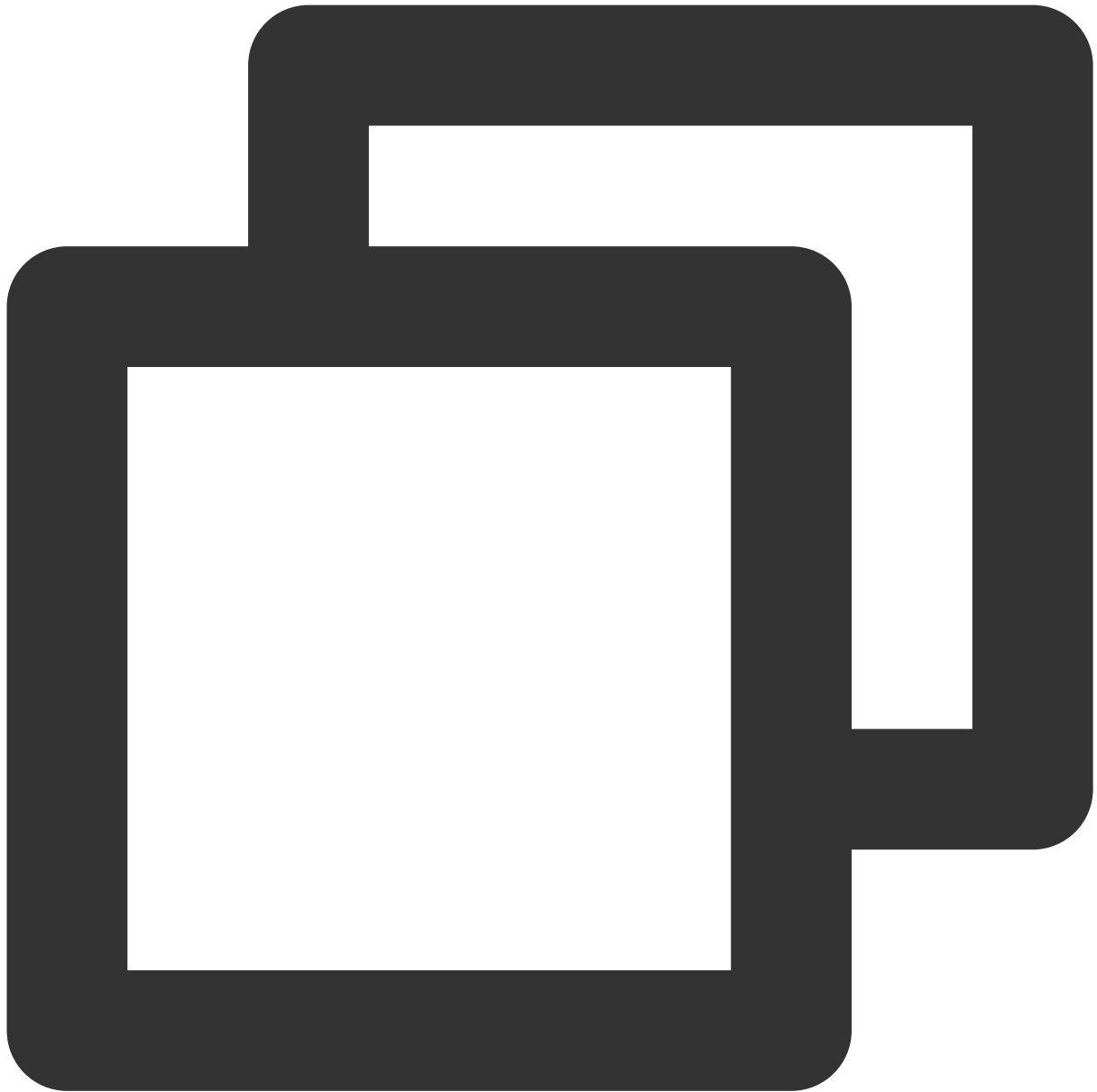


```
git clone '프로젝트 주소'
```

프로젝트 클론을 완료하면 로컬에 동일한 이름의 디렉터리가 생성되며 프로젝트 안에 있는 모든 파일이 포함됩니다.

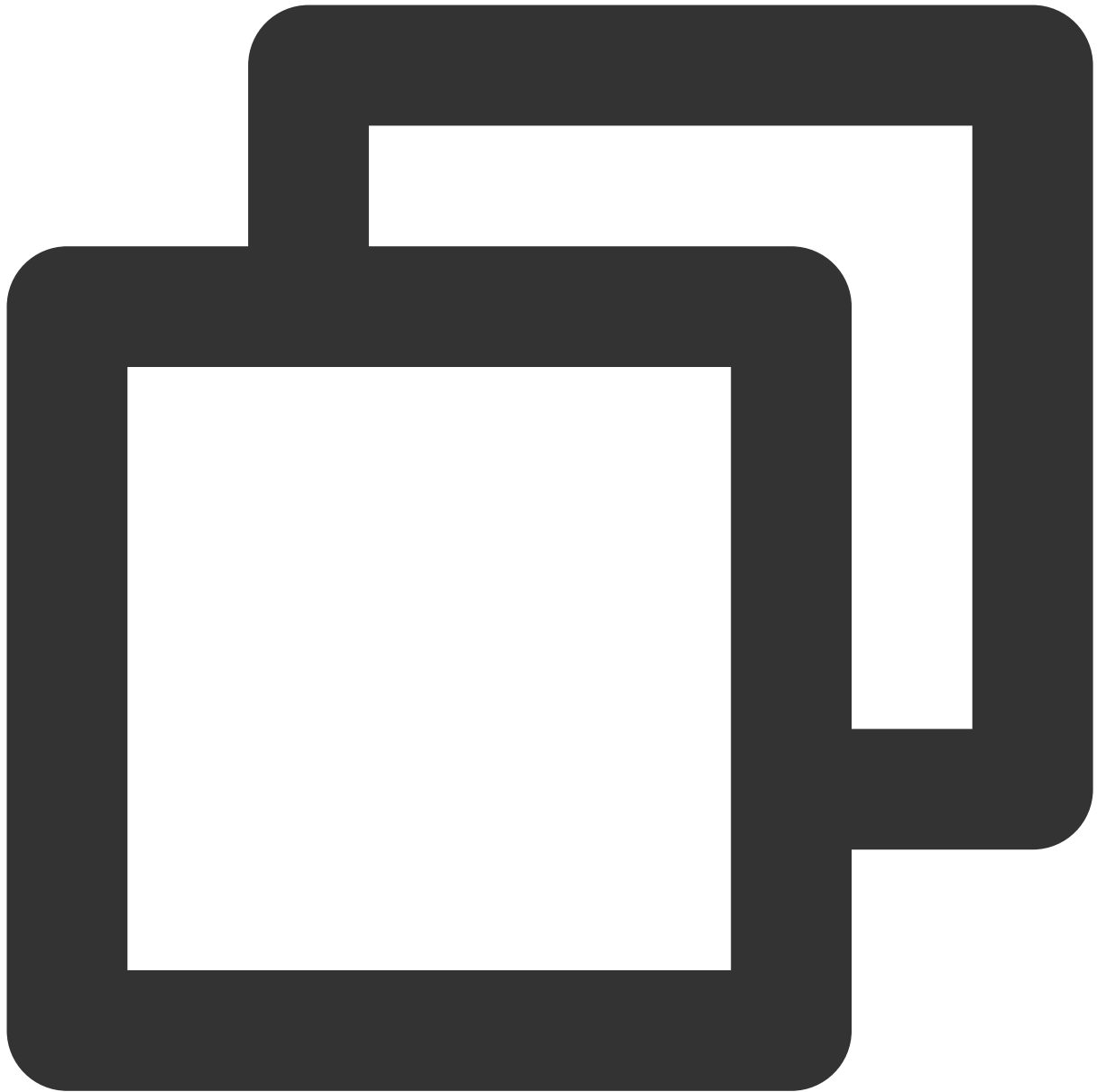
파일 업로드

1. 다음 명령어를 실행하여 프로젝트 디렉터리로 이동합니다.



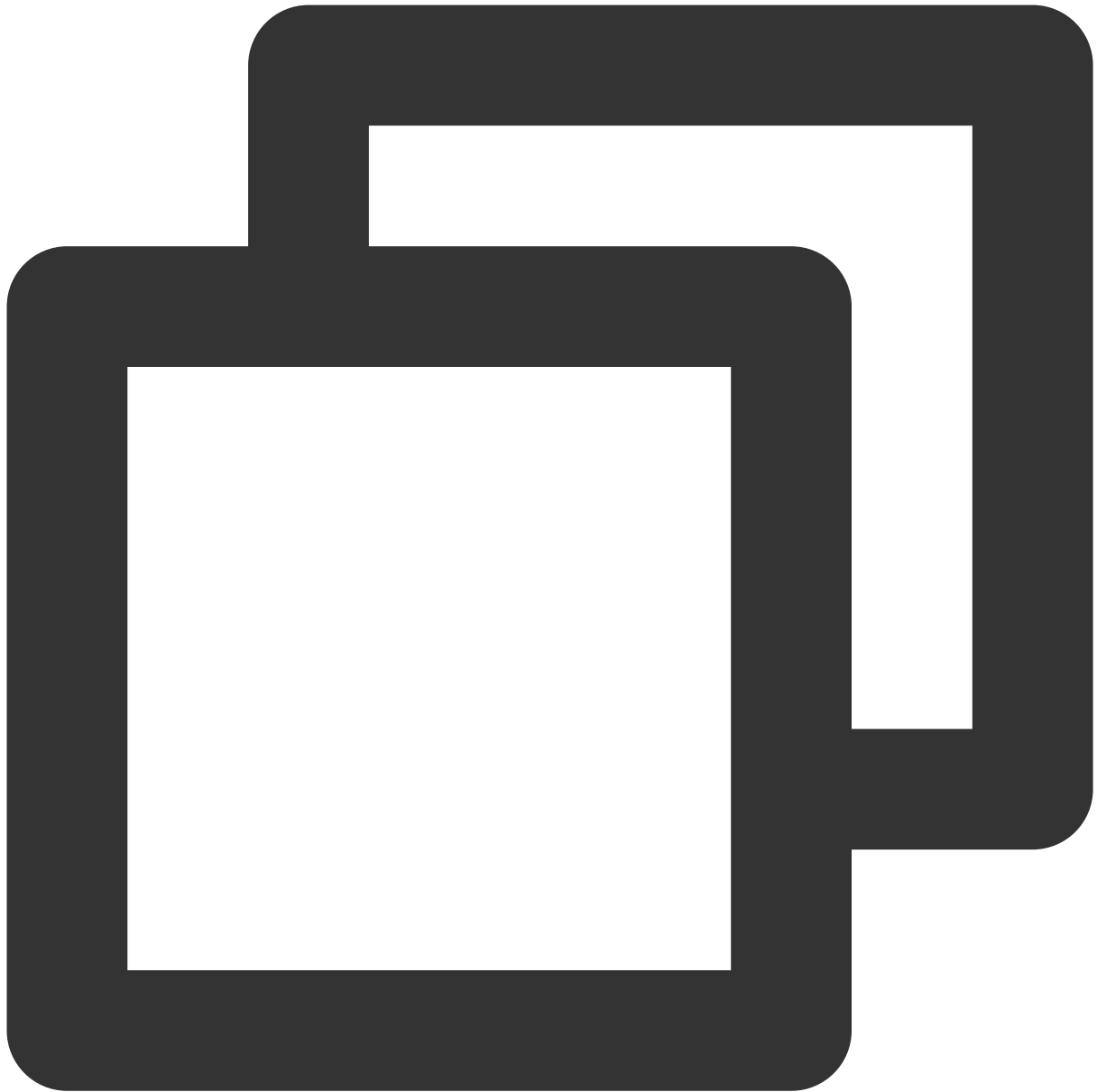
```
cd test/
```

2. 다음 명령어를 실행하여 GitLab에 업로드할 타깃 파일을 생성합니다. 본 문서는 `test.sh`를 예로 듭니다.



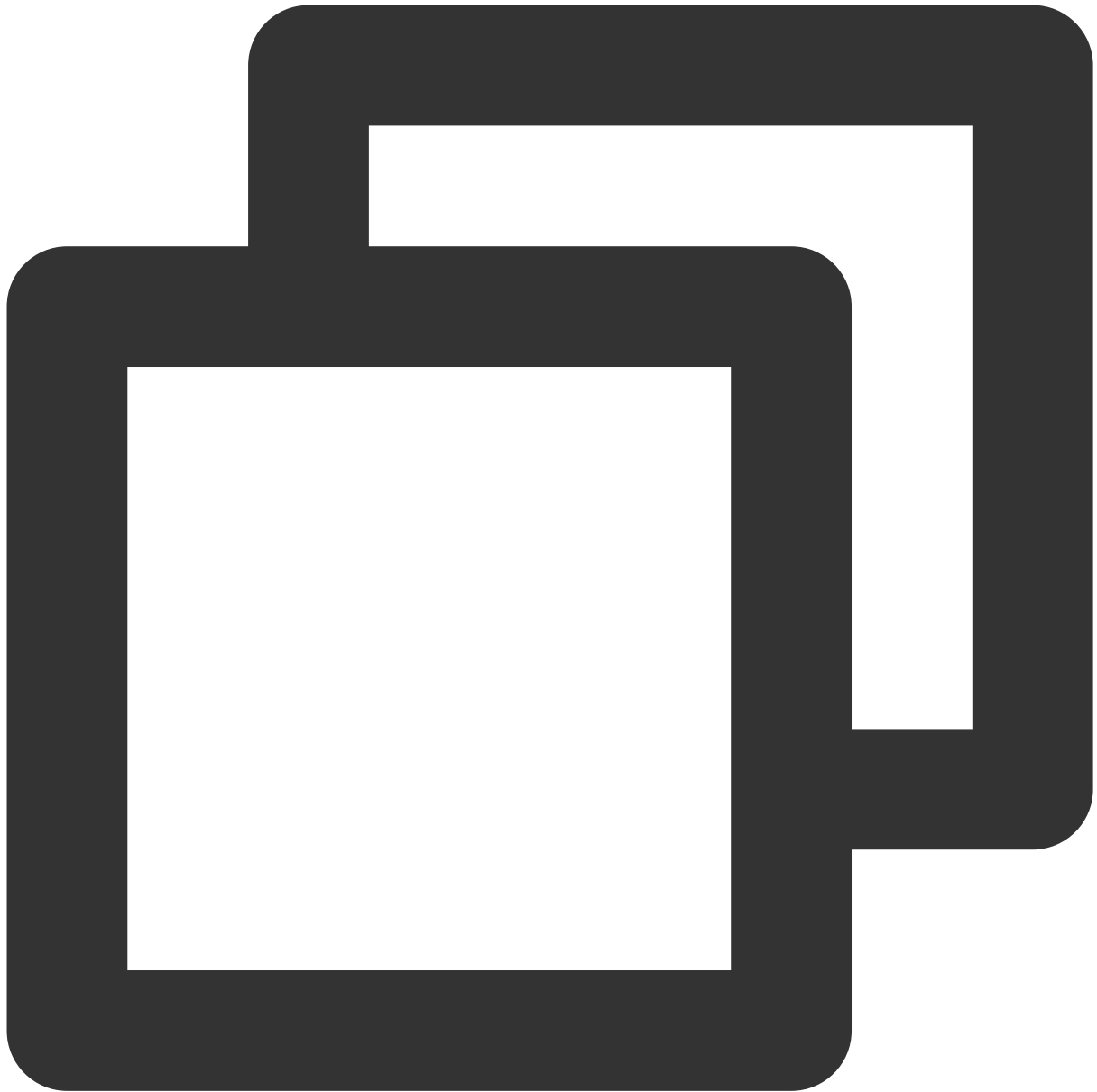
```
echo "test" > test.sh
```

3. 다음 명령어를 실행하여 `test.sh` 파일을 인덱스에 추가합니다.



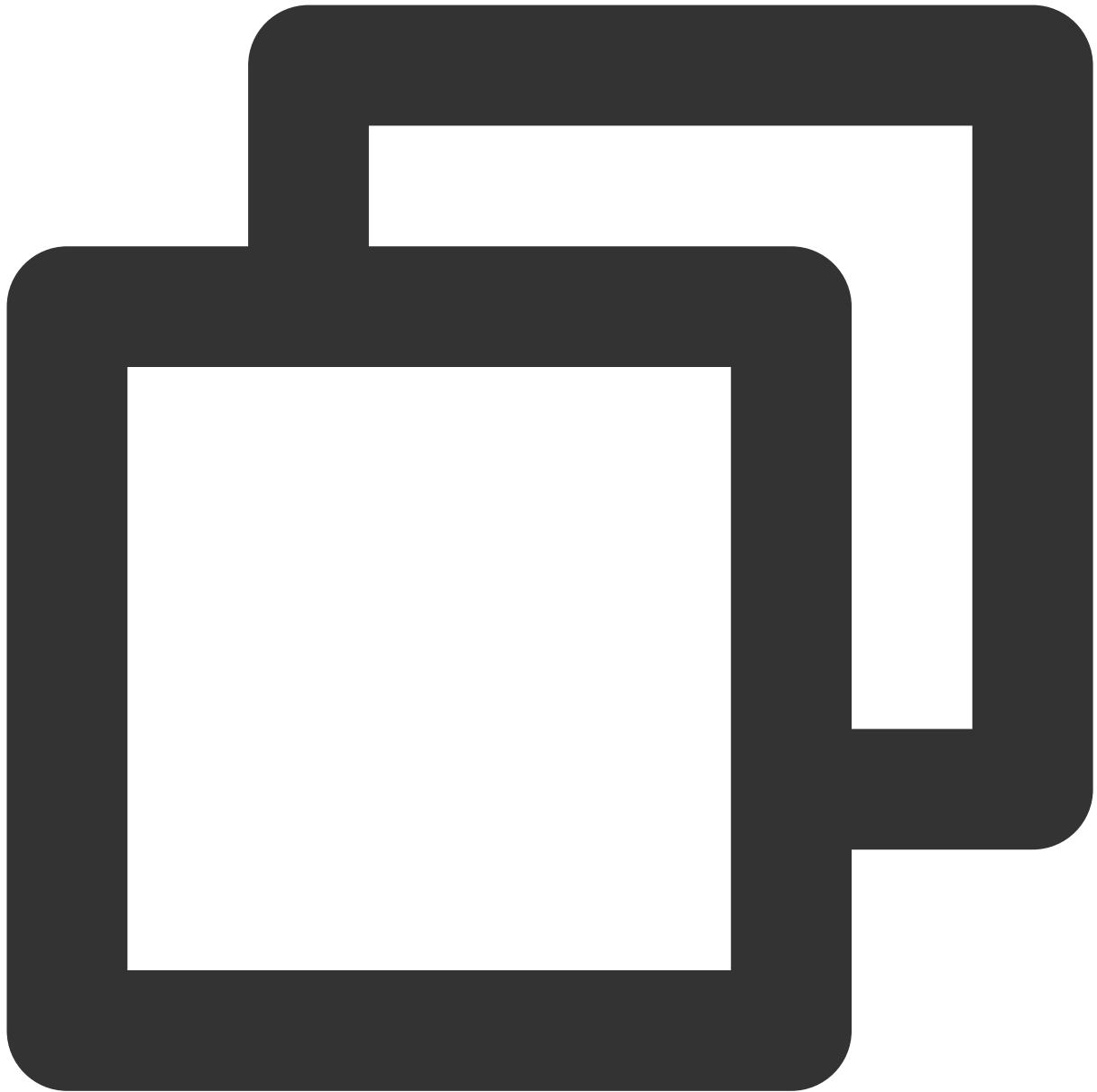
```
git add test.sh
```

4. 다음 명령어를 실행하여 **test.sh**를 로컬 리포지토리에 제출합니다.



```
git commit -m "test.sh"
```

5. 다음 명령어를 실행하여 `test.sh`를 GitLab 서버에 동기화합니다.



```
git push -u origin master
```

아래 이미지와 같이 **test** 프로젝트 페이지로 돌아가면 파일 업로드에 성공했음을 바로 확인할 수 있습니다.

Administrator > test > Details

**test** 
Project ID: 3

 1 Commit  1 Branch  0 Tags  143 KB Files  143 KB Storage

master  test /   History F

 **test.sh**
username authored 1 minute ago

 Auto DevOps enabled  Add README  Add LICENSE  Add CHANGELOG  Add

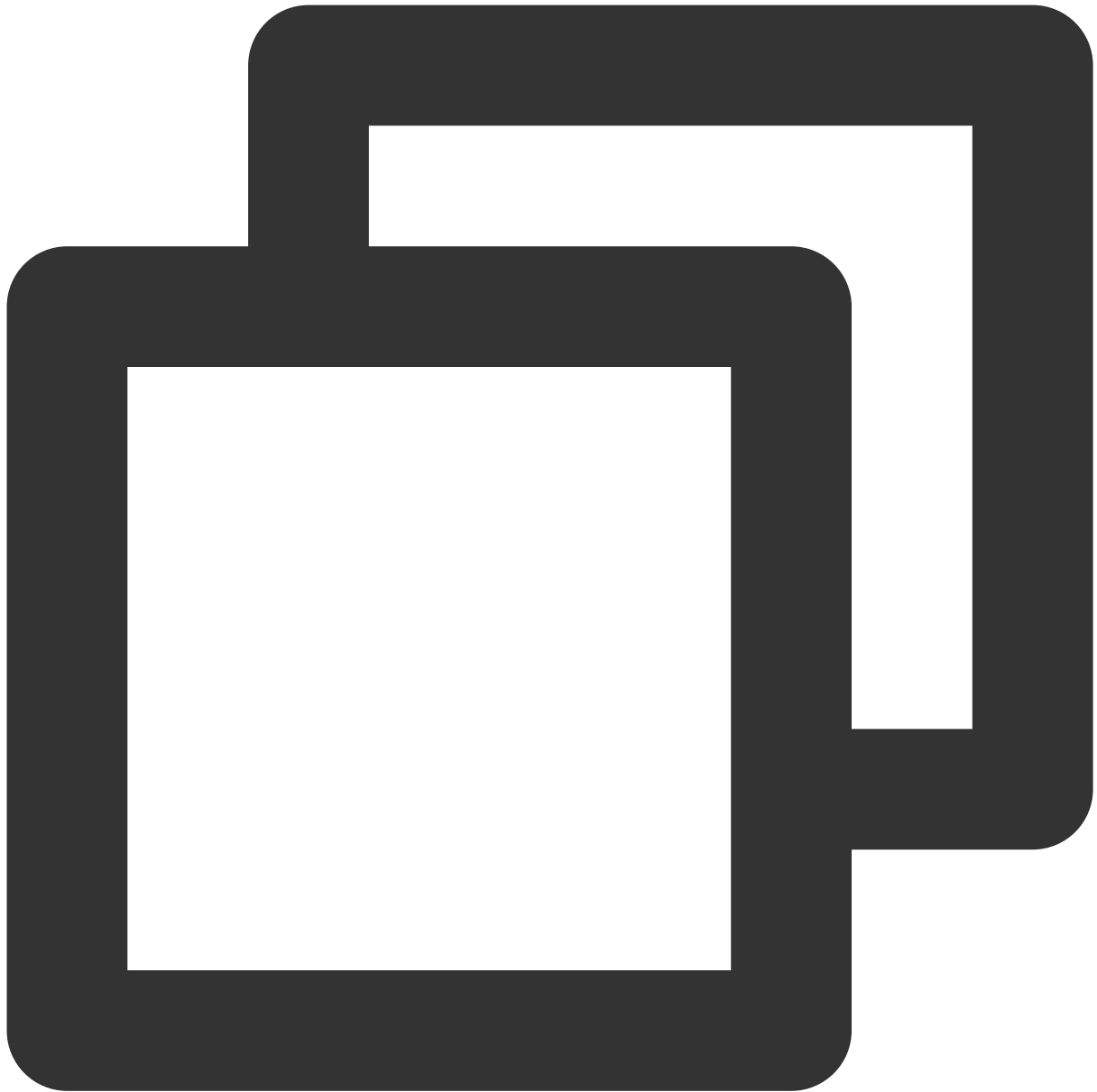
 Add Kubernetes cluster

Name	Last commit
 test.sh	test.sh

관련 작업

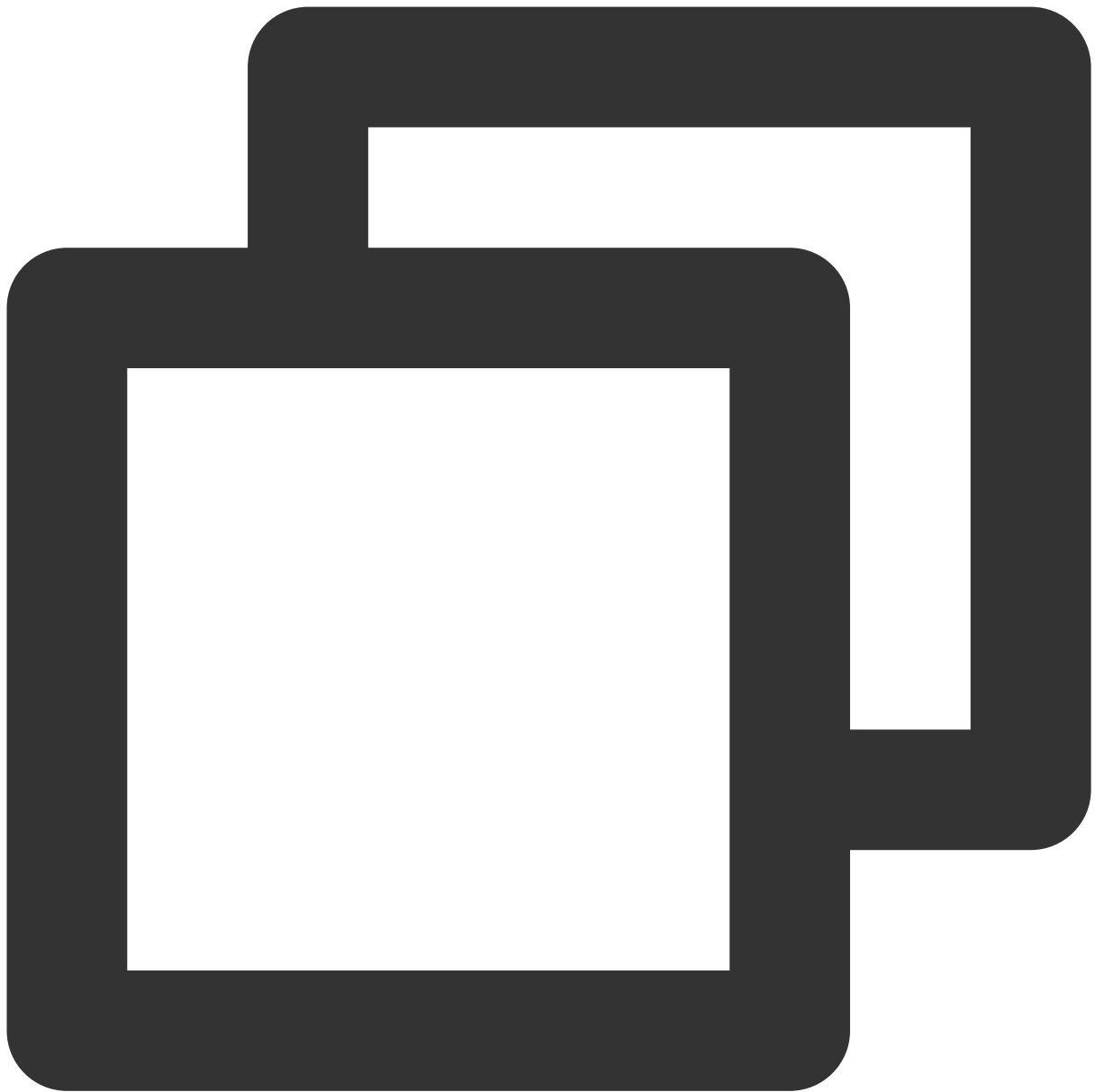
키 획득

1. 프로젝트 관리에 들어갈 PC에서 다음 명령어를 실행하여 Git를 설치합니다.



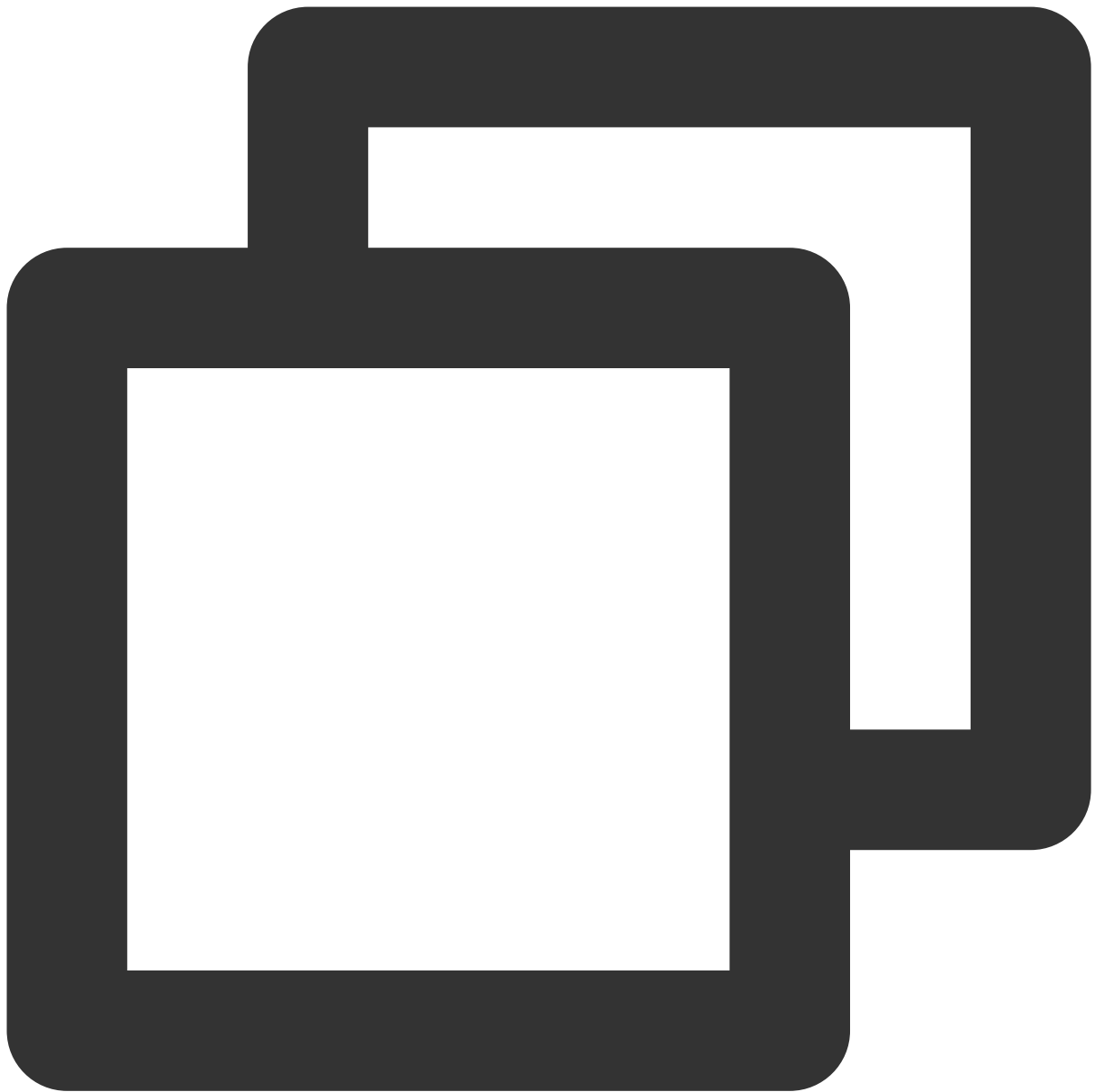
```
yum install -y git
```

2. 다음 명령어를 실행하여 키 파일 `.ssh/id_rsa`를 생성합니다. 키 파일을 생성하는 과정에서 **Enter**를 눌러 기본 설정을 유지합니다.



```
ssh-keygen
```

3. 다음 명령어를 실행하여 키 정보를 조회 및 기록합니다.



```
cat .ssh/id_rsa.pub
```

RabbitMQ 구축

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

RabbitMQ는 Advanced Message Queuing Protocol(AMQP)의 오픈 소스 메시지 브로커 소프트웨어를 구현한 것으로, 서버에서 Erlang 언어 입력을 사용하며 Python, Ruby, .NET, Java, JMS, C, PHP, ActionScript, XMPP, STOMP, AJAX 등 다양한 클라이언트를 지원합니다. 편의성, 확장성 및 고가용성 등의 장점을 갖춘 RabbitMQ를 본 문서를 참조하여 Tencent Cloud CVM에 배포할 수 있습니다.

예시 버전

본문의 예시 작업에서 사용하는 소프트웨어의 버전 및 구성은 다음과 같습니다.

Linux: Linux 운영 체제의 경우, 본 문서는 CentOS 7.7를 예시로 사용합니다.

RabbitMQ Server: 오픈 소스 메시지 브로커 소프트웨어의 경우, 본 문서는 RabbitMQ Server 3.6.9를 예로 듭니다.

Erlang: 프로그래밍 언어의 경우, 본 문서는 Erlang 19.3을 예로 듭니다.

전제 조건

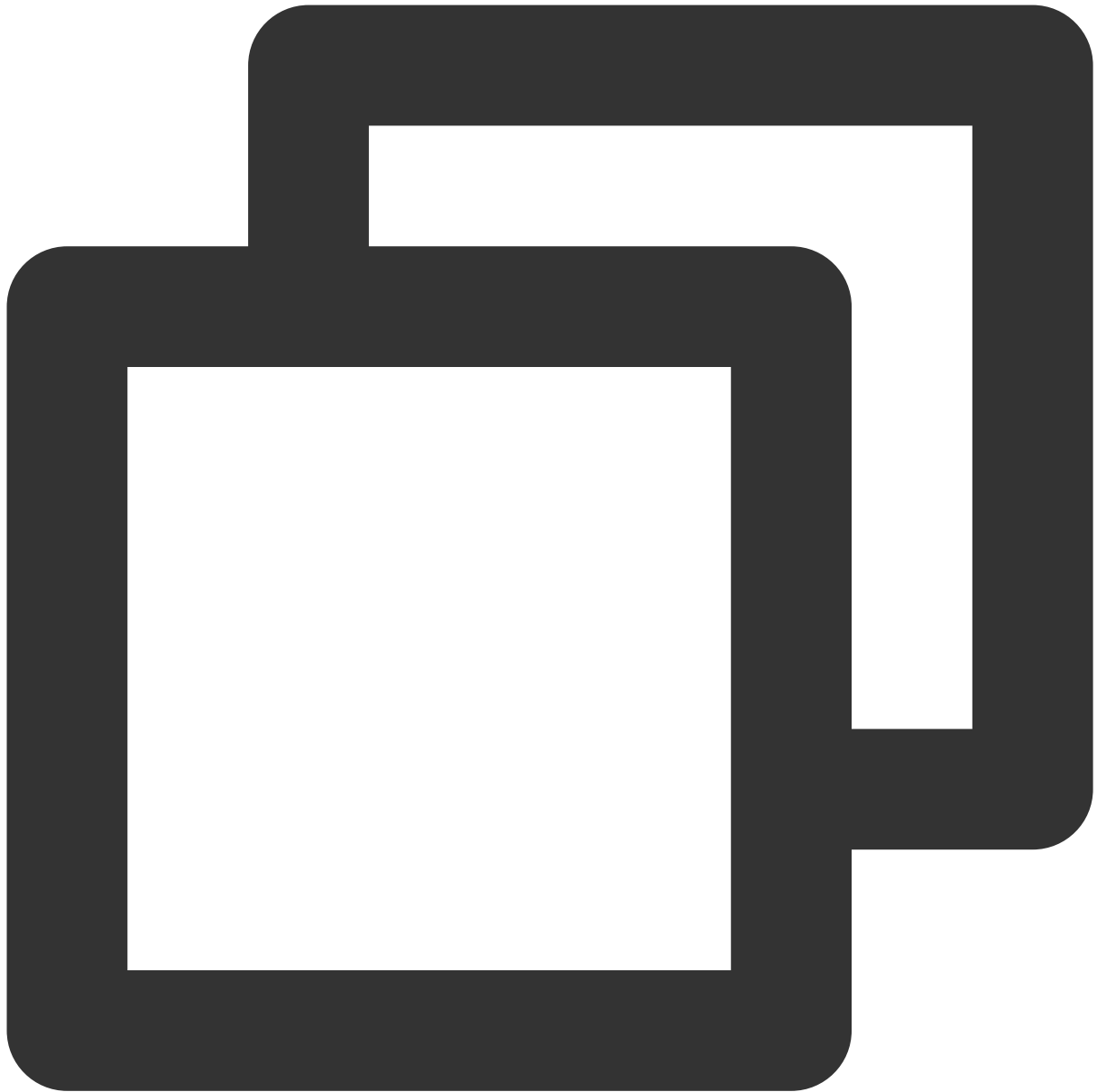
Linux CVM을 구입 완료해야 합니다.

Linux 인스턴스에 보안 그룹 규칙(80, 5672 및 15672 포트 개방)이 설정되어 있어야 합니다. 자세한 내용은 [보안 그룹 규칙 추가](#)를 참조 바랍니다.

작업 단계

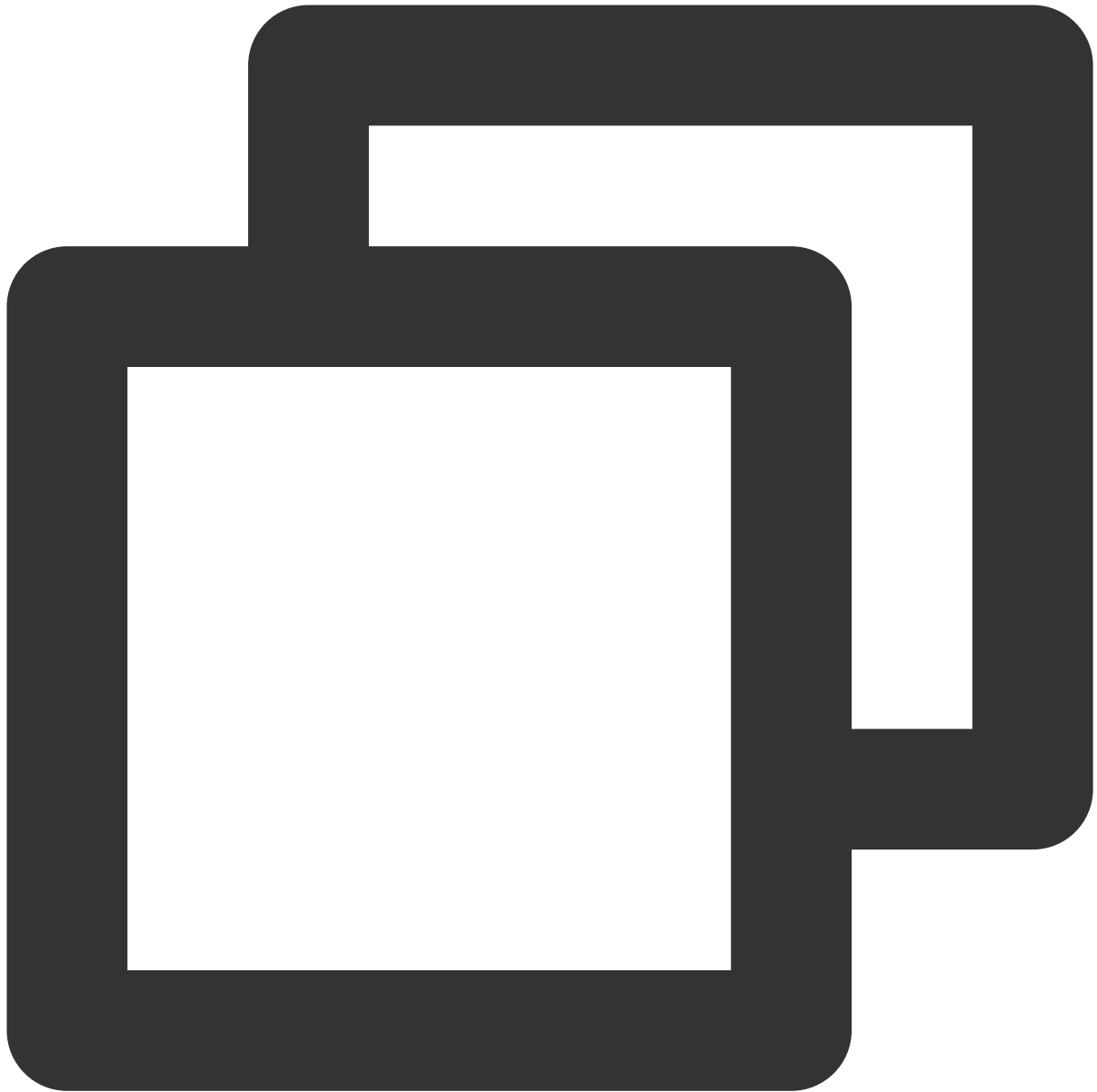
Erlang 설치

- 표준 방식으로 [Linux 인스턴스에 로그인\(권장\)](#). 실제 작업 스타일에 따라 다른 로그인 방식을 선택할 수 있습니다.
[원격 로그인 소프트웨어를 사용하여 Linux 인스턴스 로그인](#)
[SSH를 사용하여 Linux 인스턴스에 로그인](#)
- 다음 명령어를 실행하여 종속 패키지를 설치합니다.



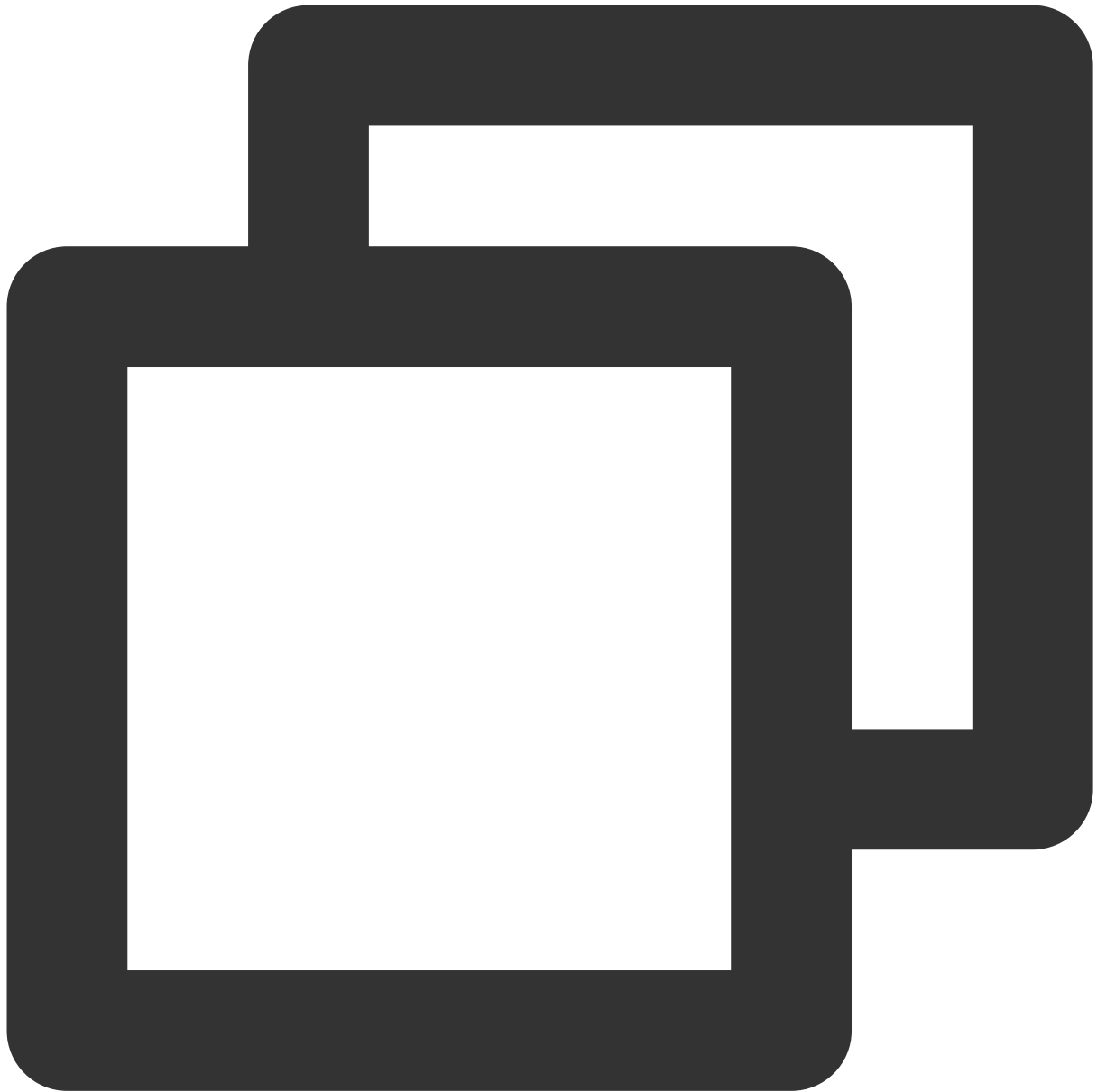
```
yum -y install make gcc gcc-c++ m4 ncurses-devel openssl-devel unixODBC-devel
```

3. 다음 명령어를 실행하여 Erlang 설치 패키지를 다운로드합니다.



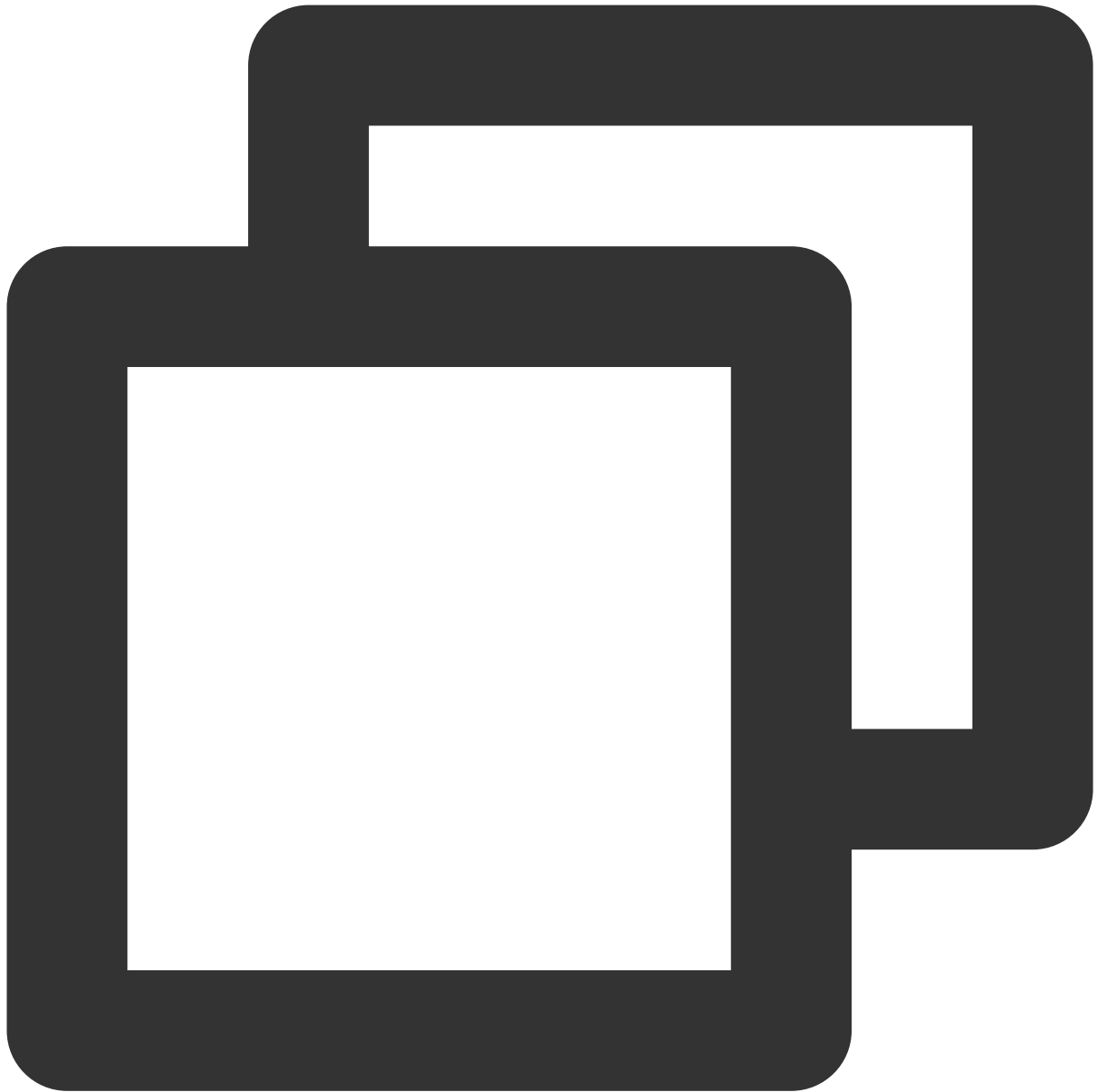
```
wget http://erlang.org/download/otp_src_19.3.tar.gz
```

4. 다음 명령어를 실행하여 Erlang 설치 패키지를 압축 해제합니다.



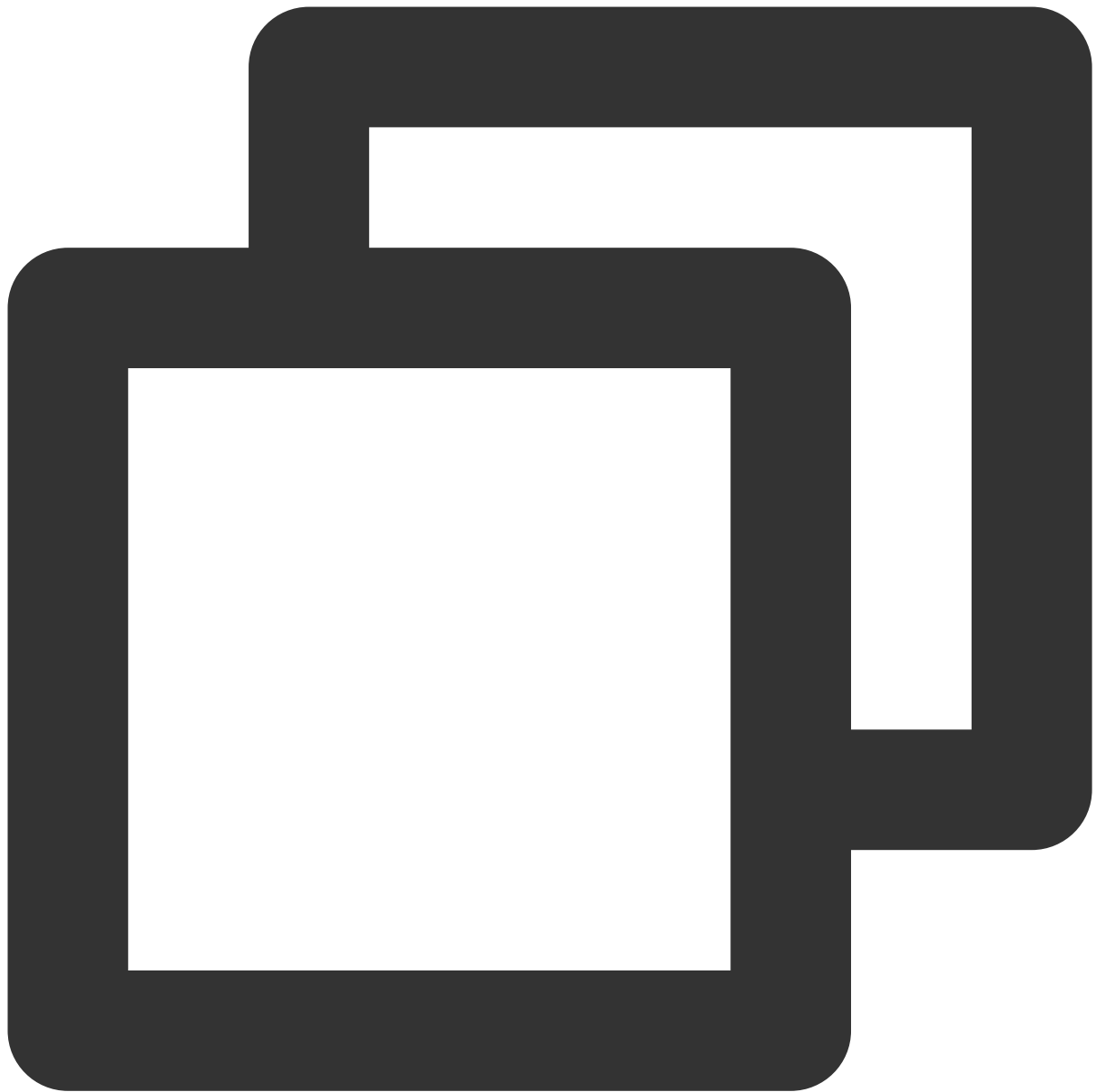
```
tar xzf otp_src_19.3.tar.gz
```

5. 다음 명령어를 실행하여 **erlang** 폴더를 생성합니다.

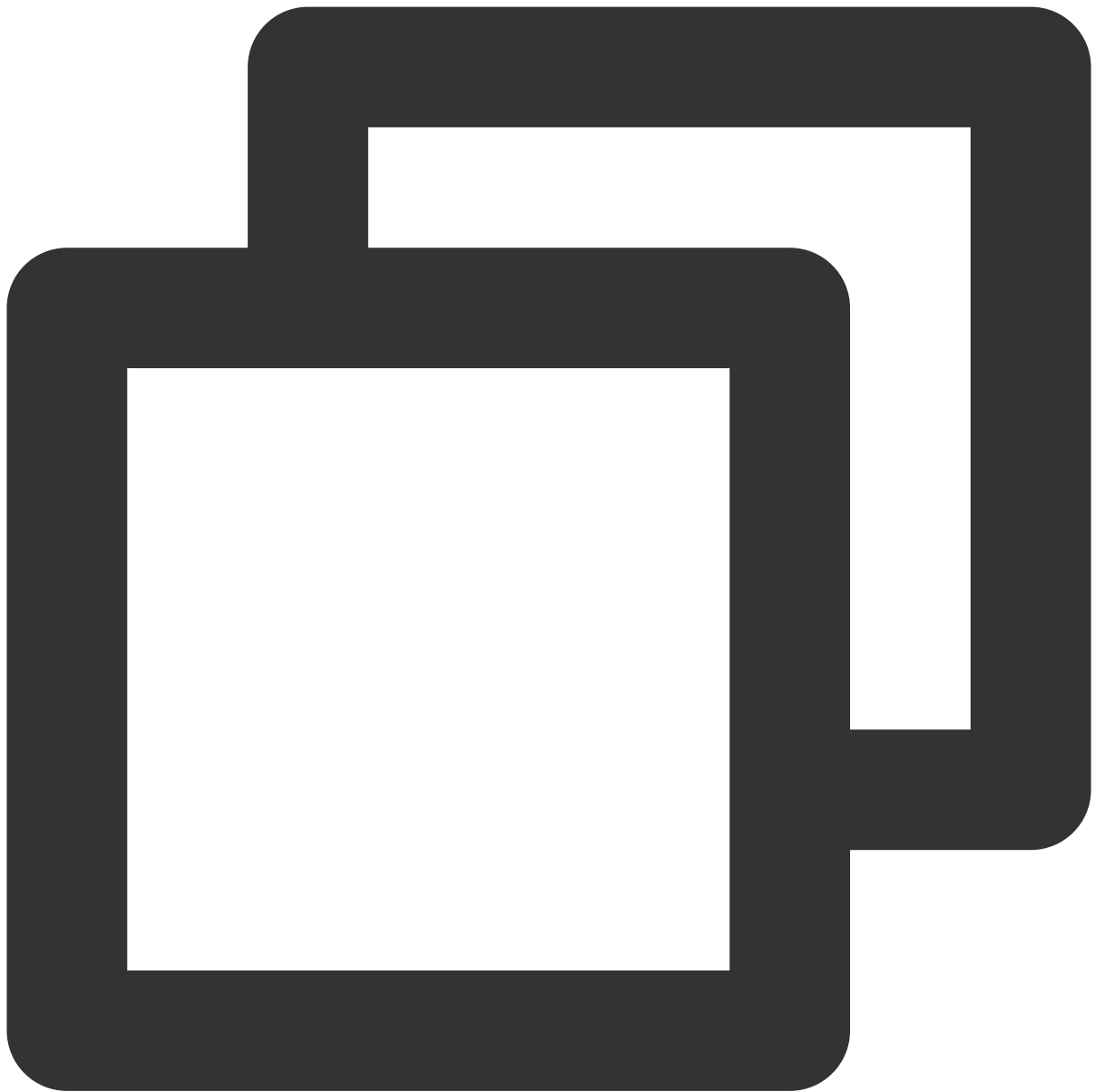


```
mkdir /usr/local/erlang
```

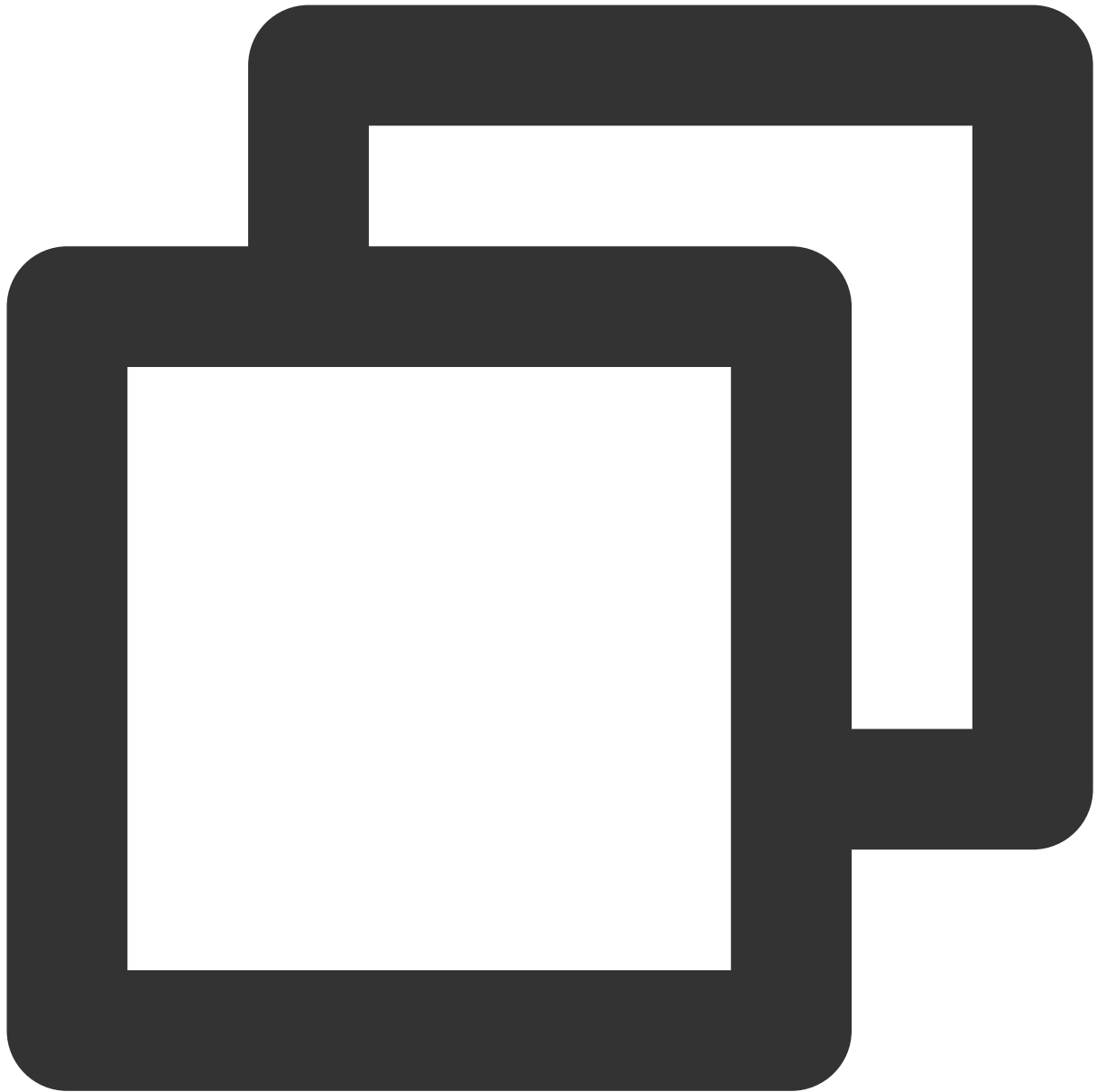
6. 다음 명령어를 순서대로 실행하여 Erlang 설치를 컴파일합니다.



```
cd otp_src_19.3
```

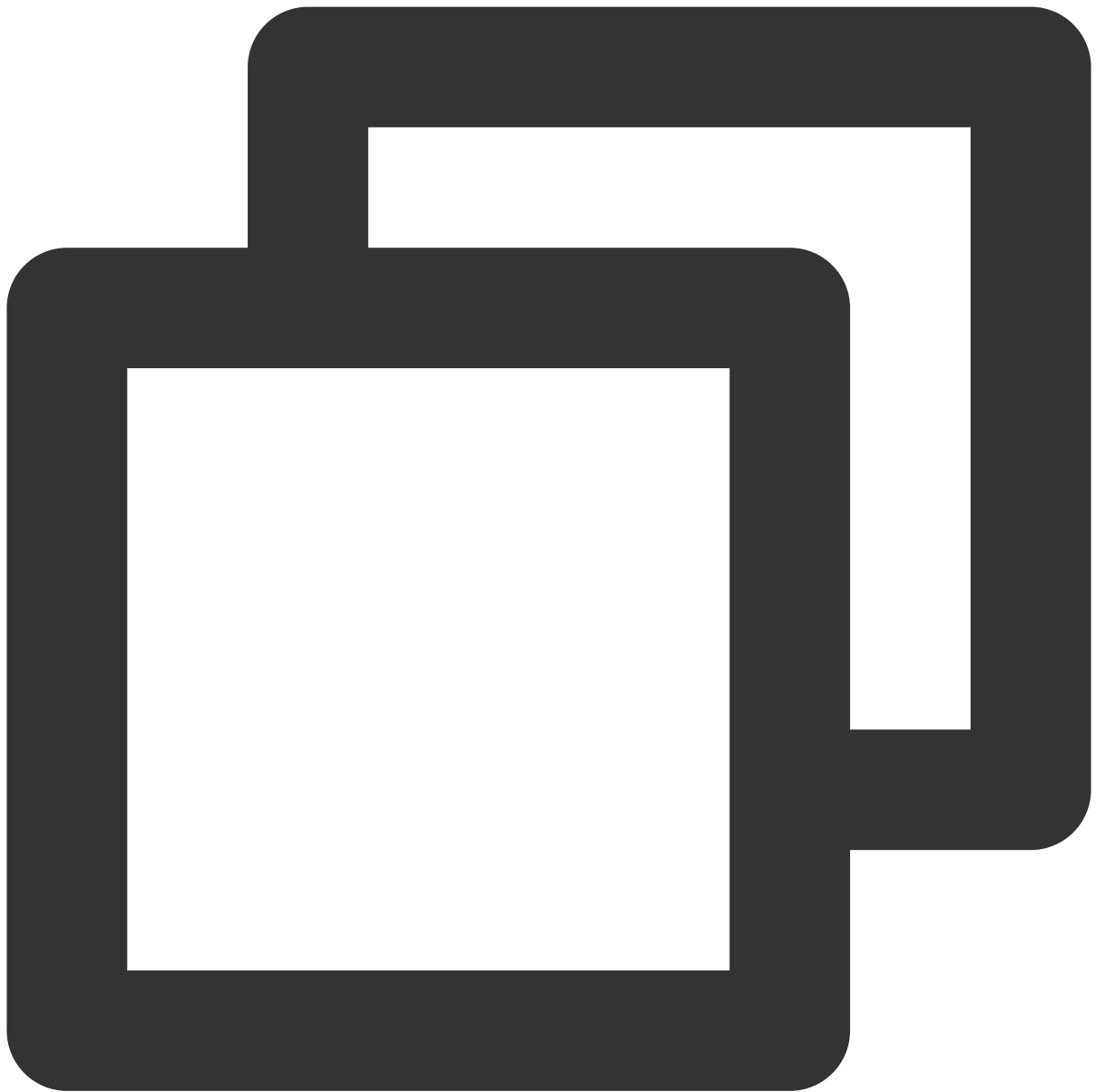


```
./configure --prefix=/usr/local/erlang --without-javac
```



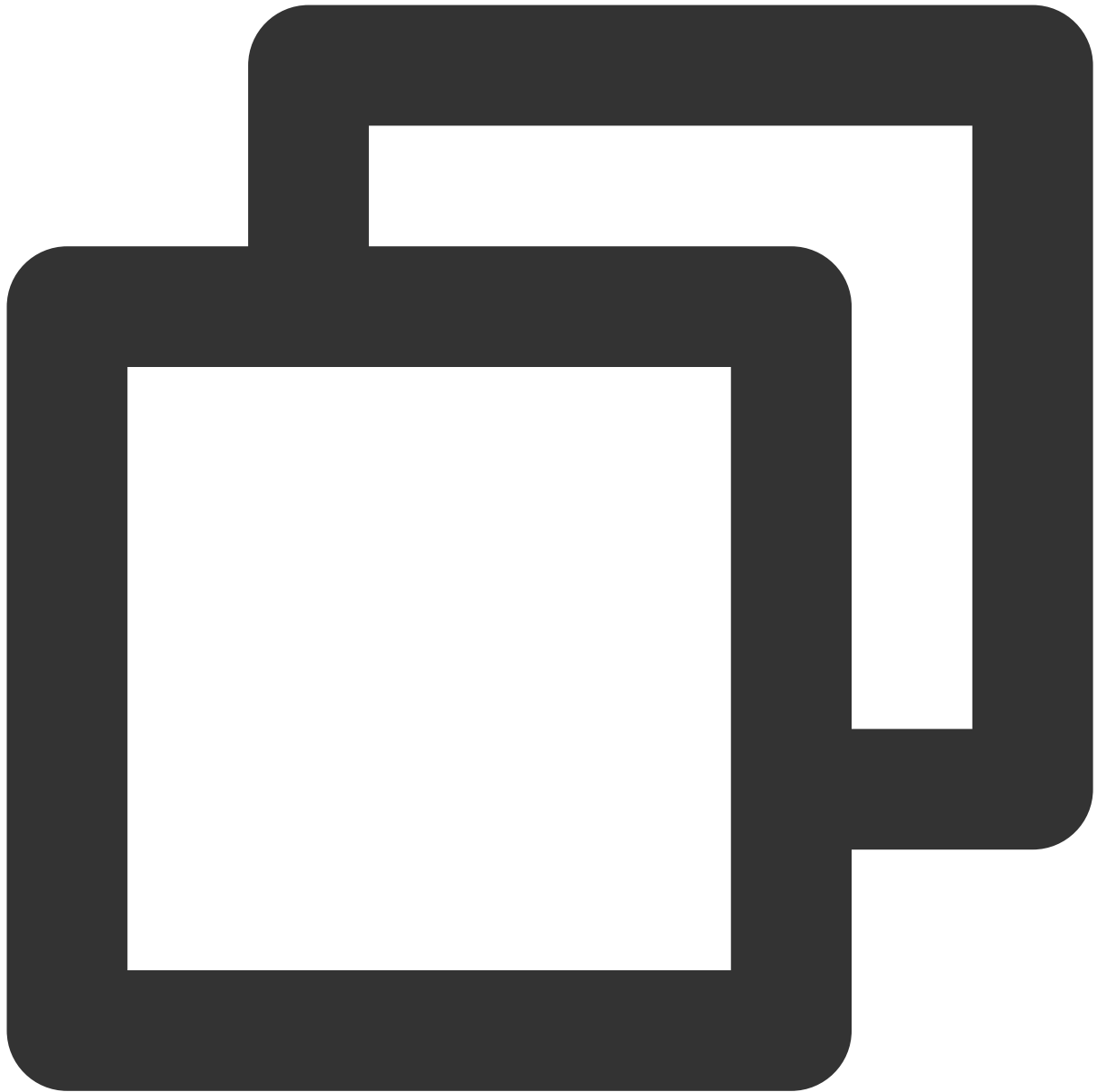
```
make && make install
```

7. 다음 명령어를 실행하여 **profile** 구성 파일을 엽니다.



```
vi /etc/profile
```

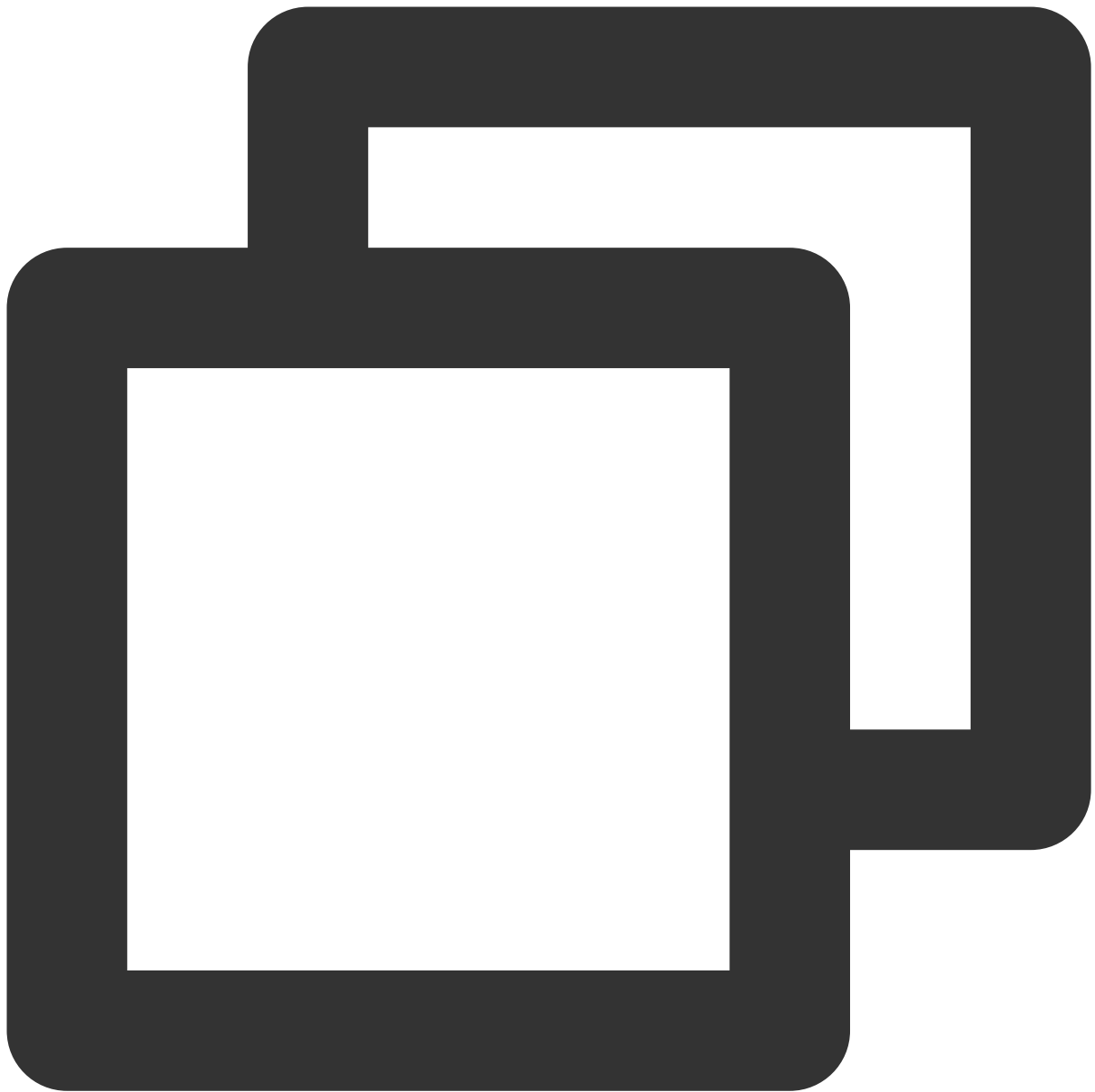
8. **i**를 눌러 편집 모드로 이동하고 파일 끝에 아래의 내용을 입력합니다.



```
export PATH=$PATH:/usr/local/erlang/bin
```

9. **Esc**를 누르고 **:wq**를 입력하여 파일을 저장하고 종료합니다.

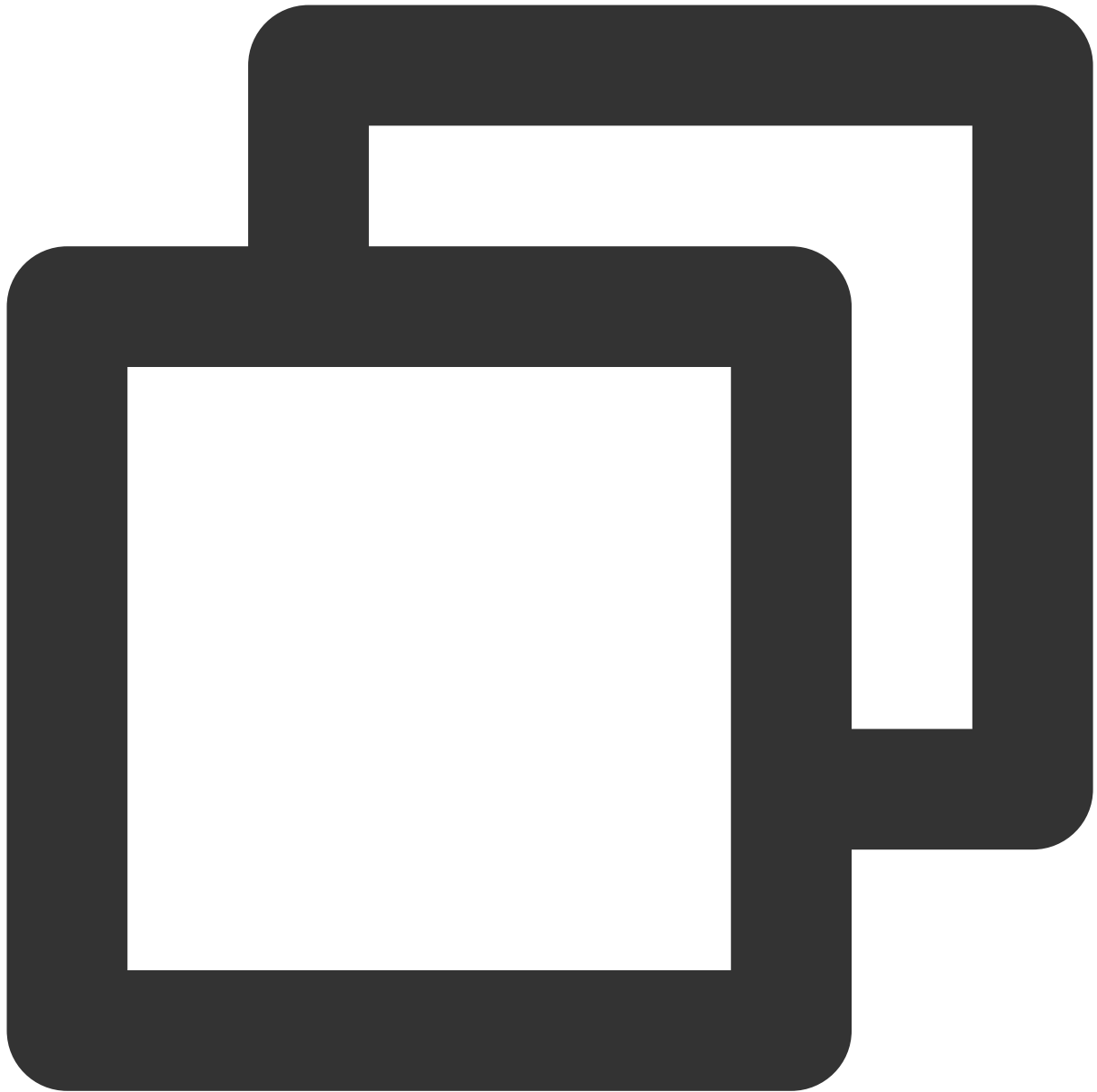
10. 아래의 명령어를 실행하여 환경 변수가 즉시 적용되도록 합니다.



```
source /etc/profile
```

RabbitMQ Server 설치

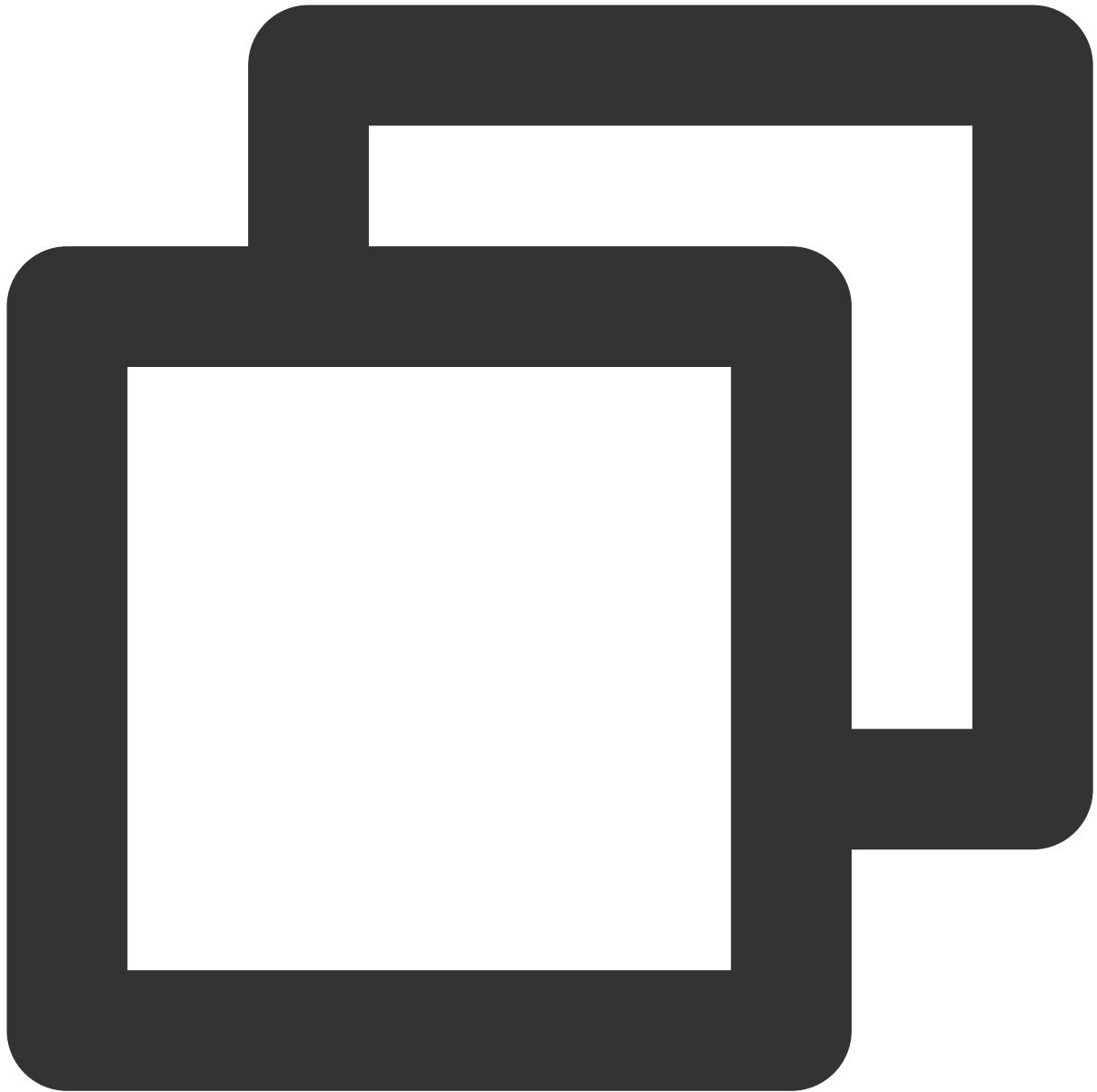
1. 다음 명령어를 실행하여 RabbitMQ Server 설치 패키지를 다운로드합니다.



```
wget https://github.com/rabbitmq/rabbitmq-server/releases/download/rabbitmq_v3_6_9/
```

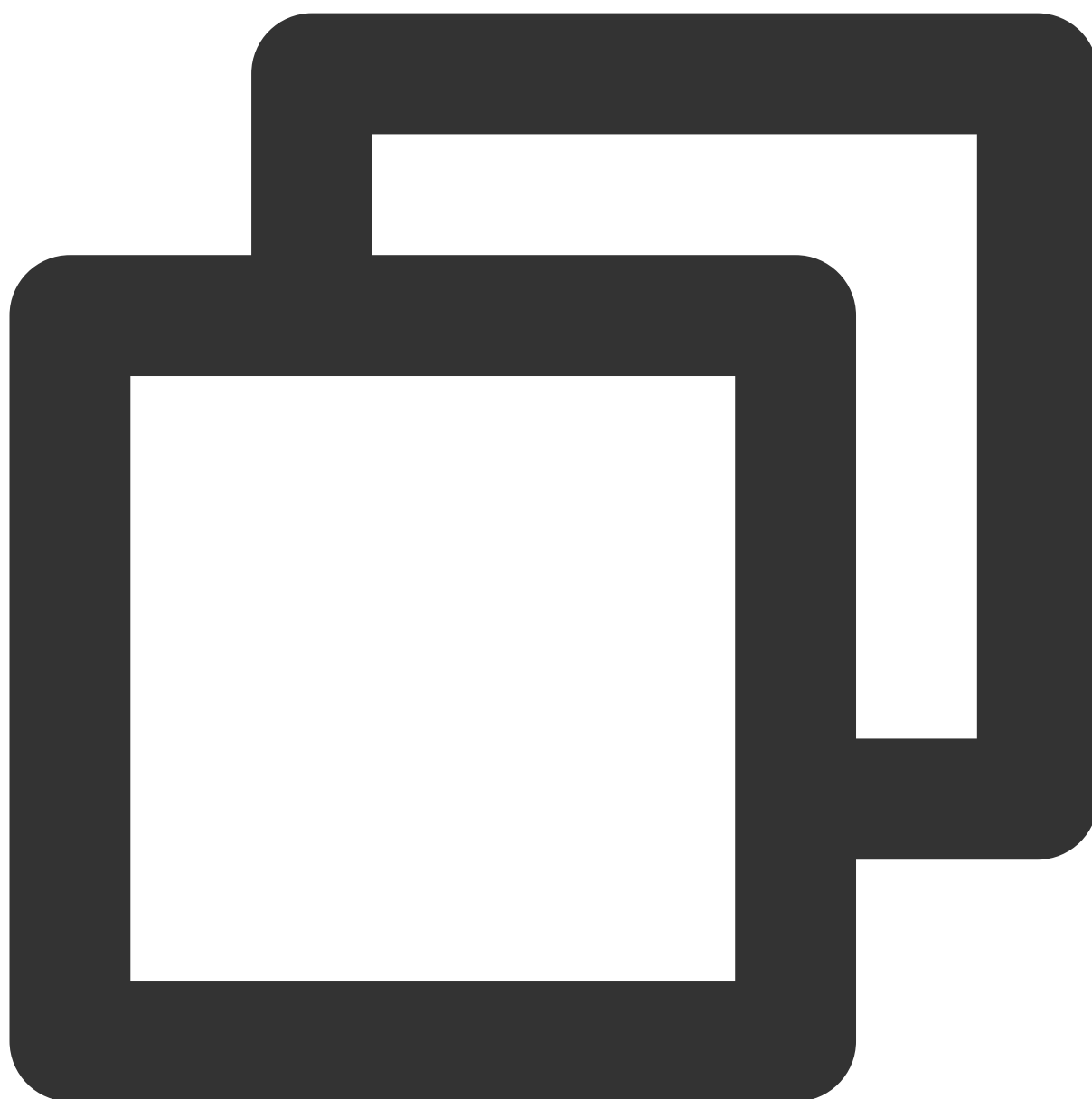
본문은 RabbitMQ 3.6.9 버전을 예시로 하며, RabbitMQ 공식 홈페이지에서 제공하는 다운로드 주소를 사용합니다. 다운로드 링크가 유효하지 않는 등 오류가 발생하거나 다른 RabbitMQ 버전이 필요한 경우 [rabbitmq-server](#)에서 더 자세한 설치 관련 정보를 얻을 수 있습니다.

2. 다음 명령어를 실행하여 서명 키를 가져옵니다.

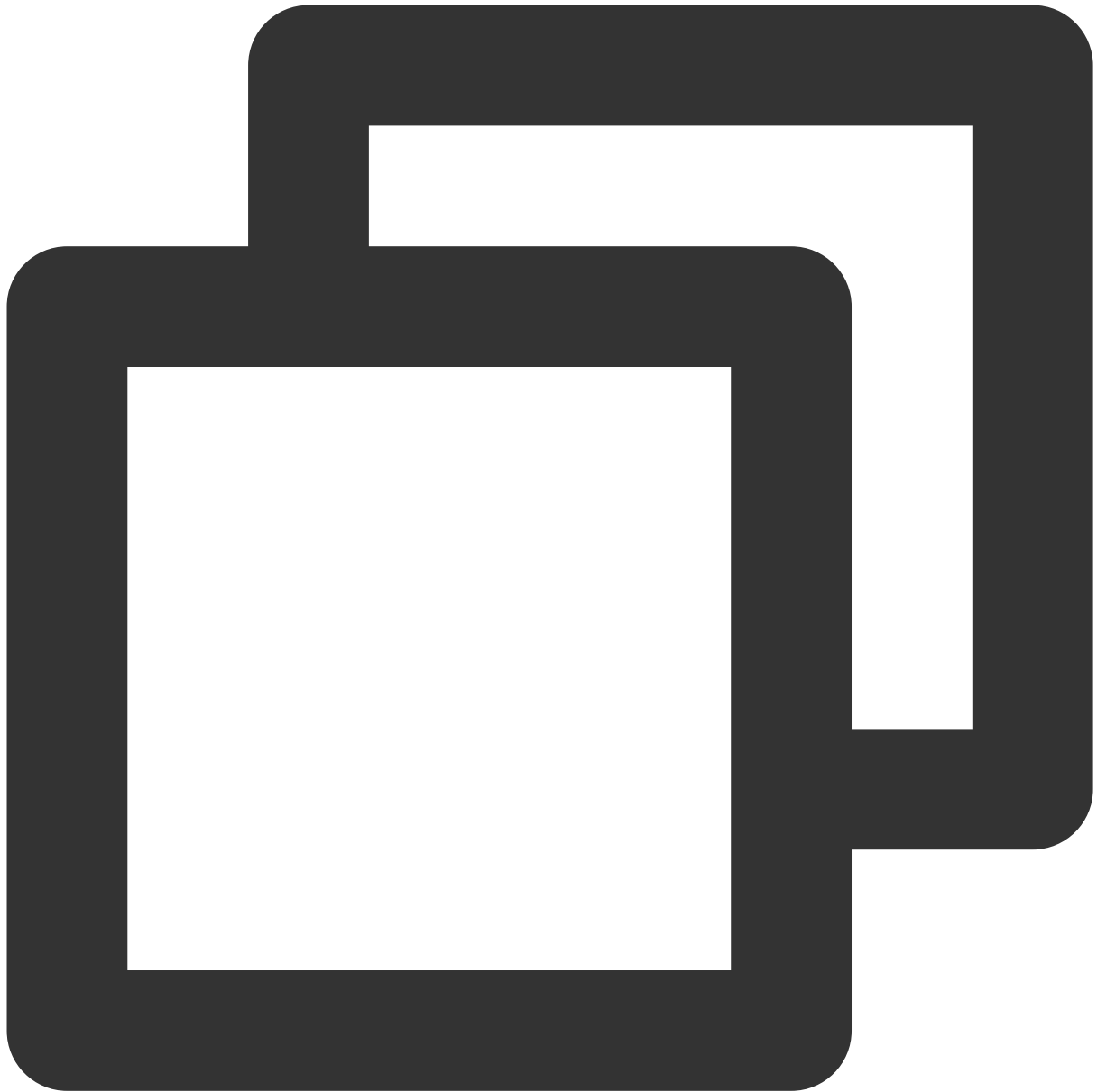


```
rpm --import https://www.rabbitmq.com/rabbitmq-release-signing-key.asc
```

3. 다음 명령어를 순서대로 실행하여 RabbitMQ Server를 설치합니다.

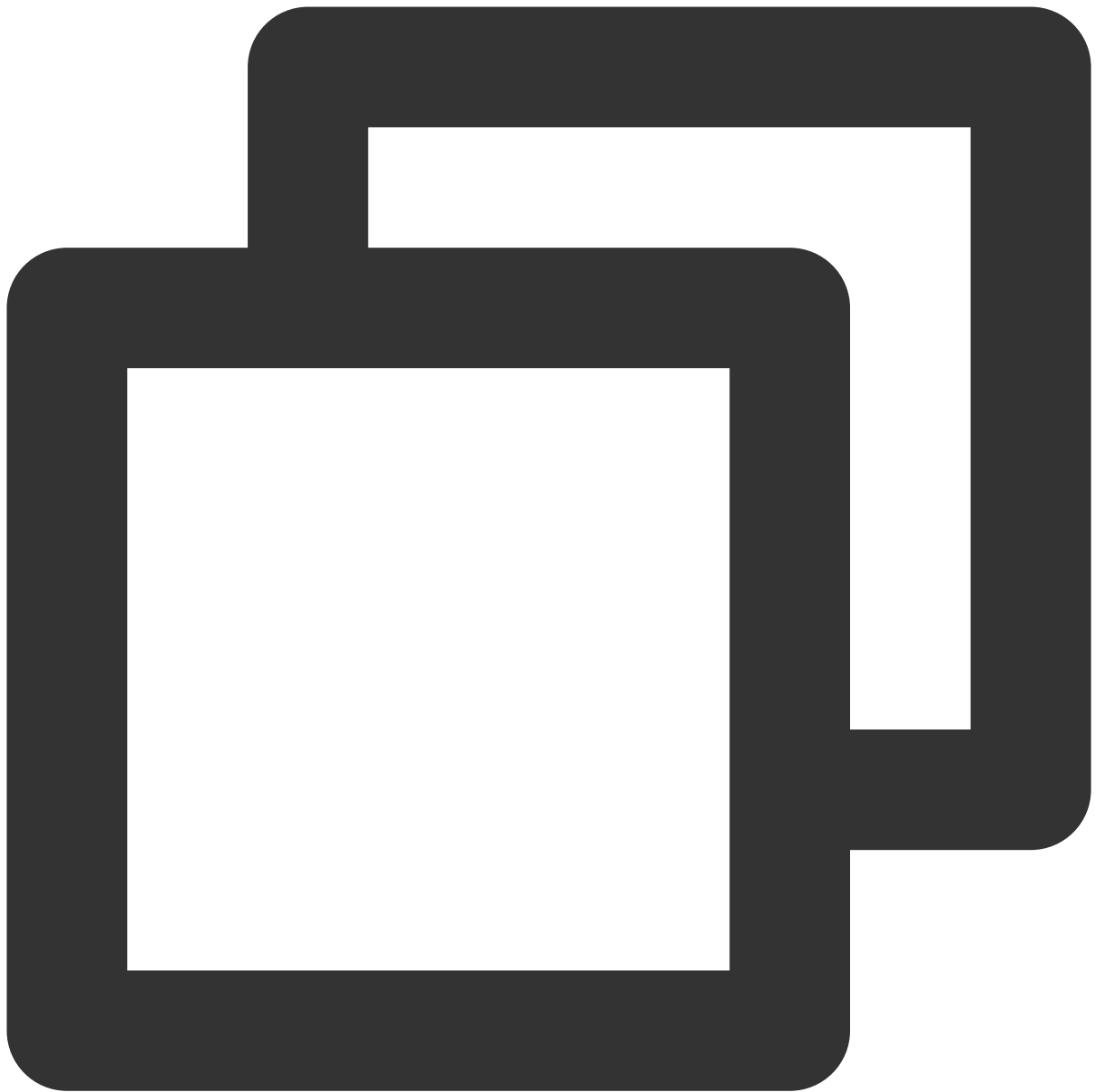


cd

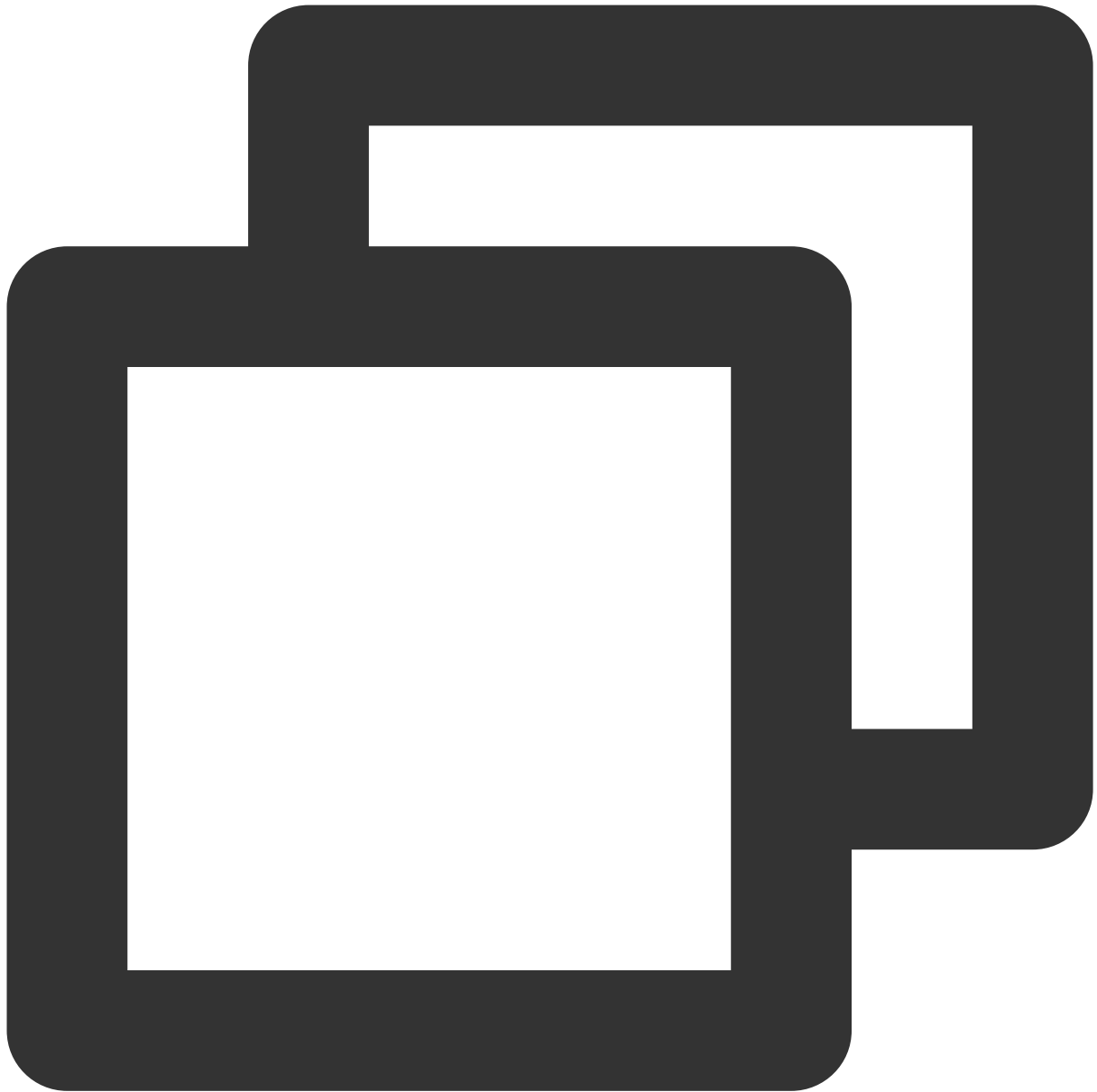


```
yum install rabbitmq-server-3.6.9-1.el7.noarch.rpm
```

4. 다음 명령어를 순서대로 실행하여 부팅 시 RabbitMQ 자동 실행으로 설정하고 RabbitMQ를 실행합니다.

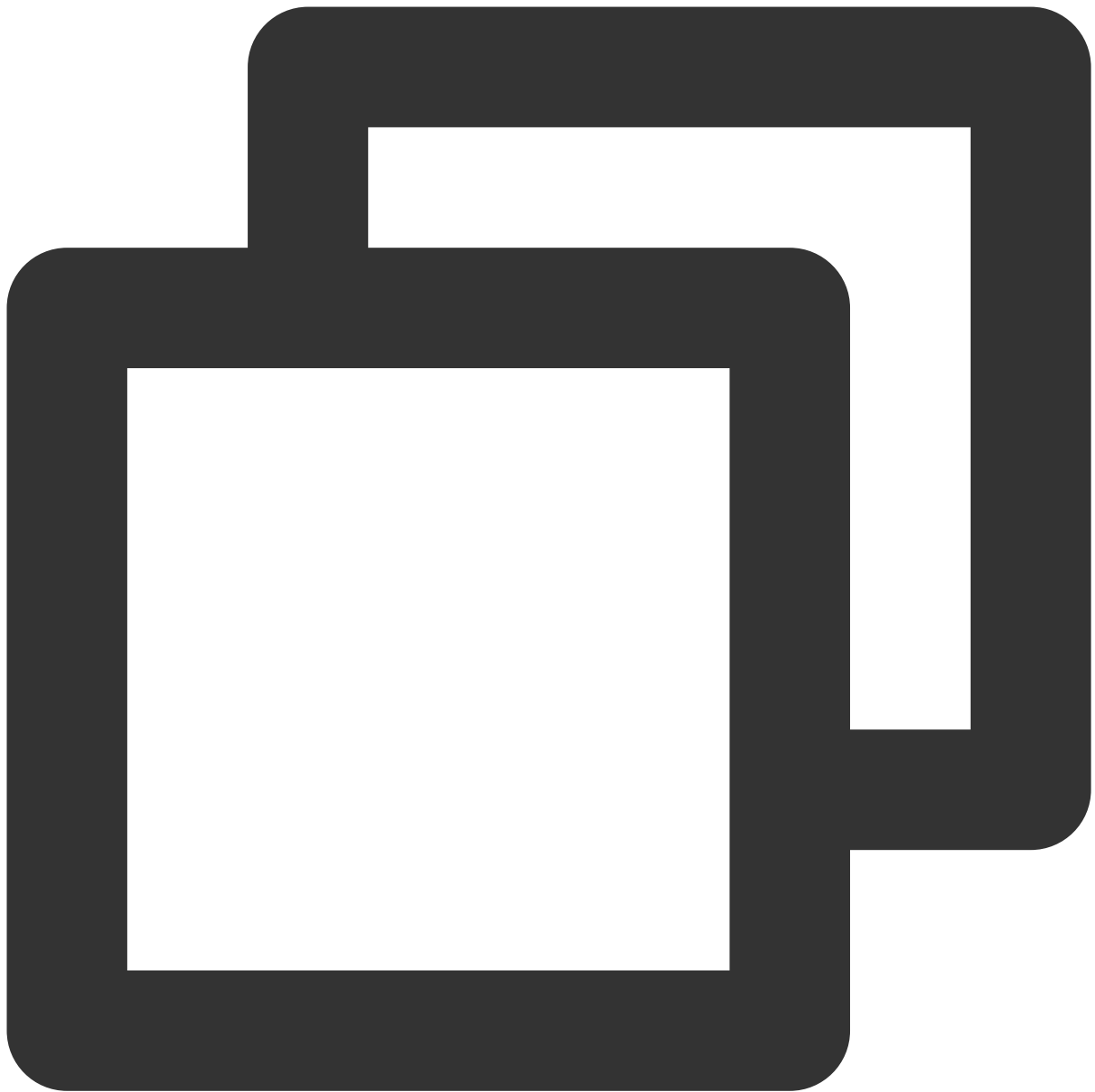


```
systemctl enable rabbitmq-server
```



```
systemctl start rabbitmq-server
```

5. 다음 명령어를 실행하여 RabbitMQ의 기본 guest 계정을 삭제합니다.

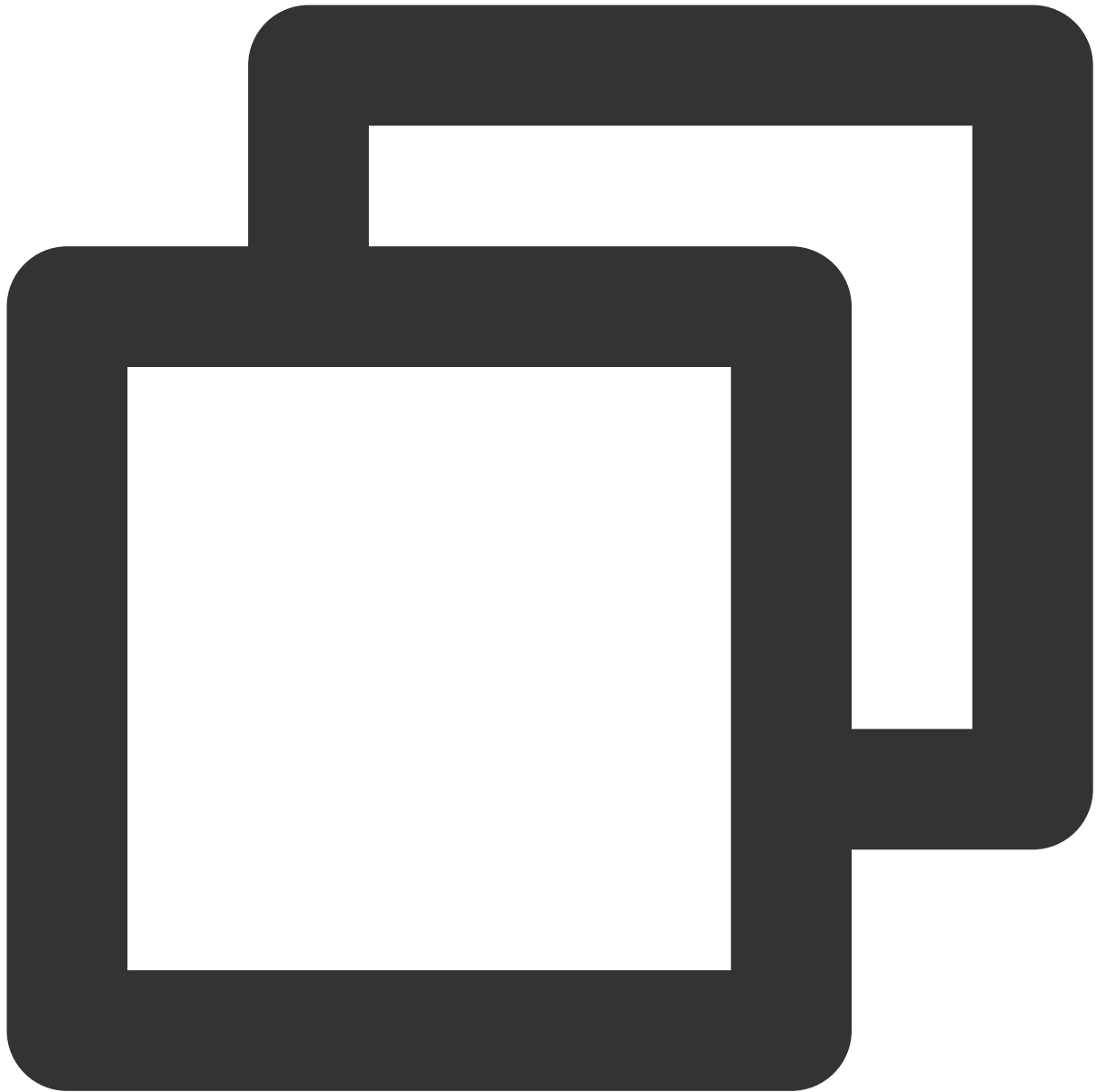


```
rabbitmqctl delete_user guest
```

6.

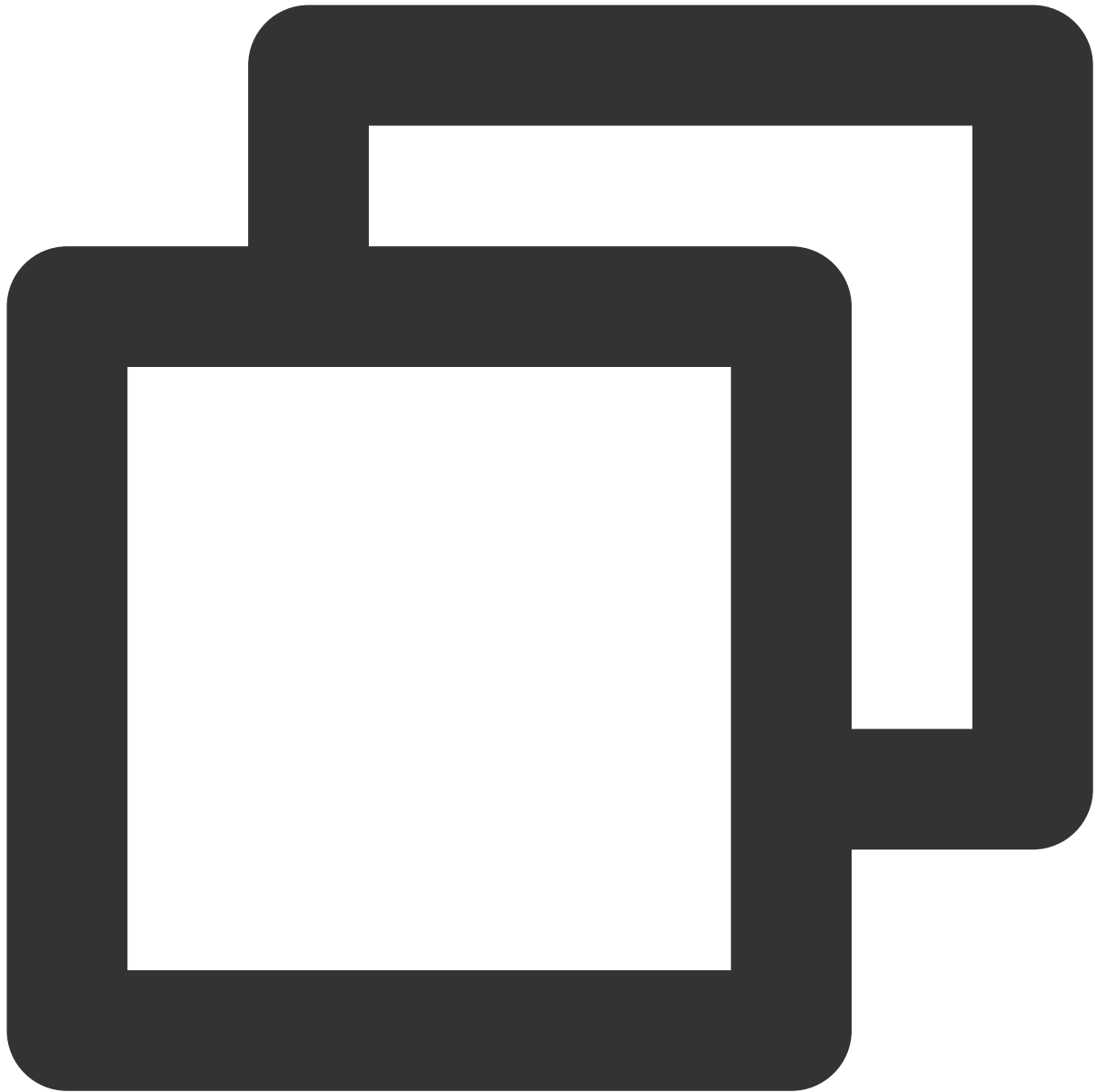
다음

명령어를 실행하여 신규 사용자를 생성합니다.



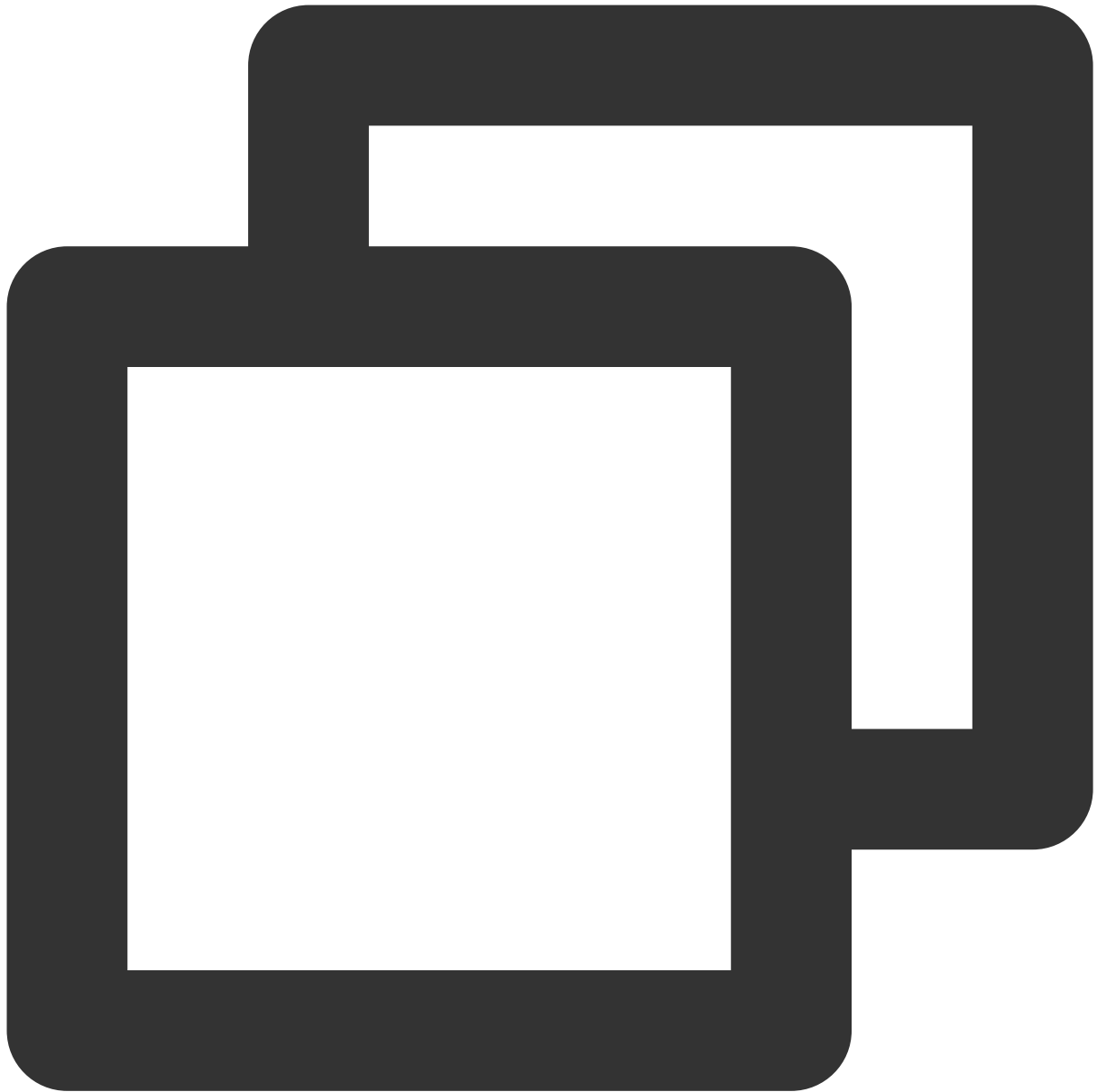
```
rabbitmqctl add_user 사용자 이름 비밀번호
```

7. 다음 명령어를 실행하여 신규 사용자를 관리자 계정으로 설정합니다.



```
rabbitmqctl set_user_tags 사용자 이름 administrator
```

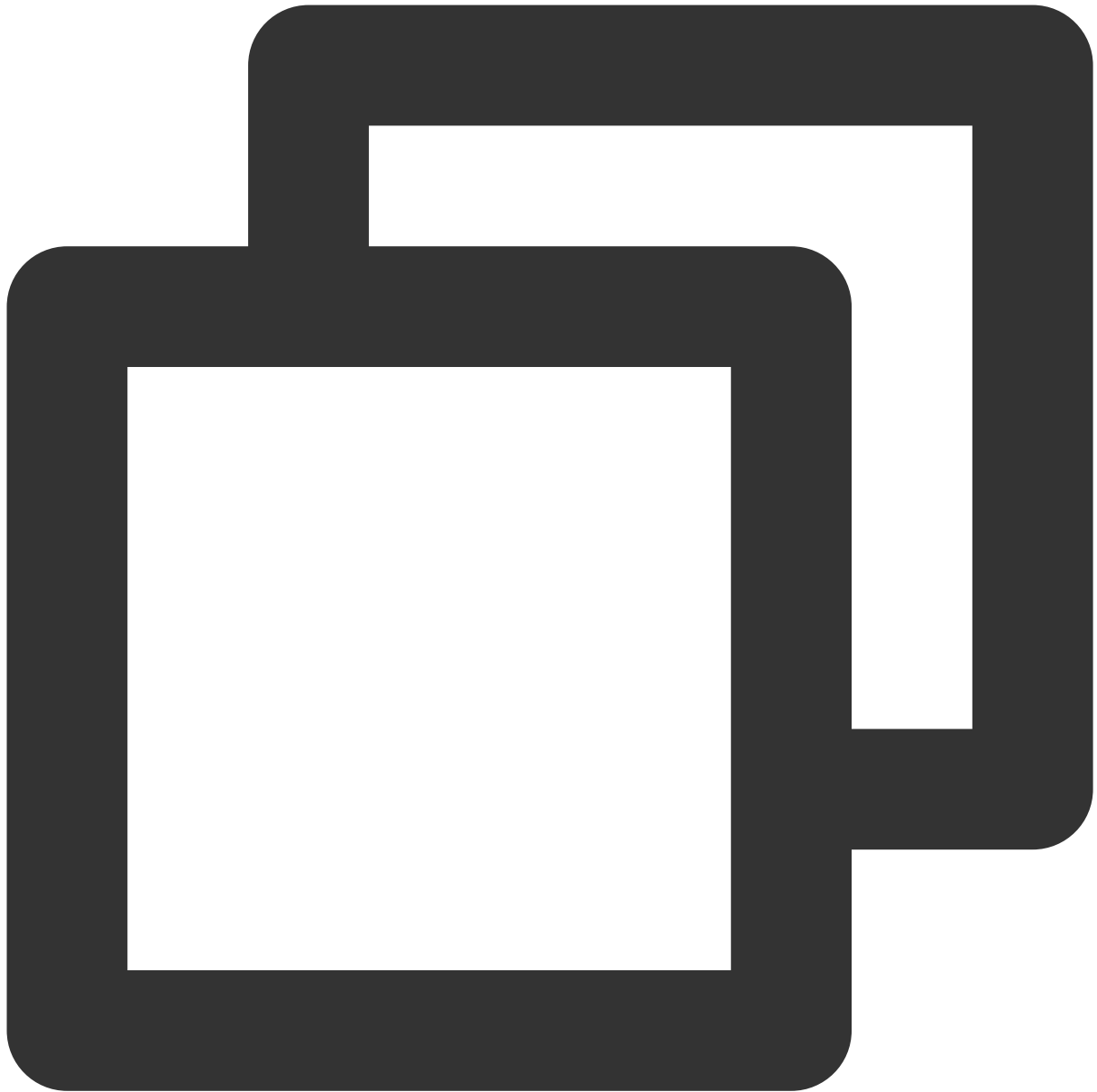
8. 다음 명령어를 실행하여 관리자 계정에 모든 권한을 부여합니다.



```
rabbitmqctl set_permissions -p / 사용자 이름 ".*" ".*" ".*"
```

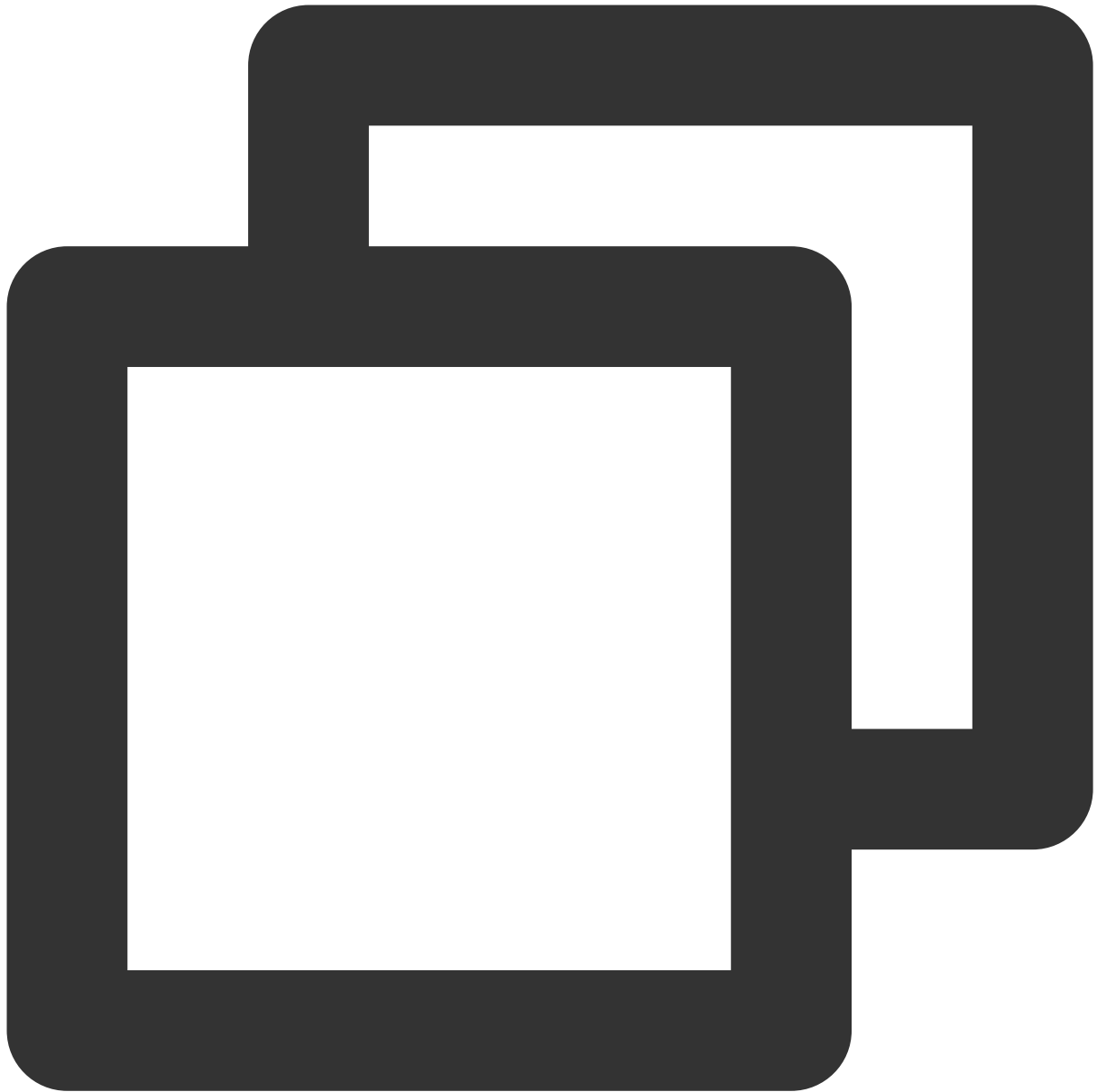
설치 확인

1. 다음 명령어를 실행하여 RabbitMQ의 Web 관리 인터페이스를 실행합니다.



```
rabbitmq-plugins enable rabbitmq_management
```

2. 브라우저를 사용하여 아래의 주소에 액세스합니다.



`http://인스턴스 공인 IP:15672`

인스턴스의 공인 IP 획득 방법은 [공인 IP 주소 획득](#)을 참고하십시오.

아래 이미지와 같은 인터페이스가 표시되면 RabbitMQ Server 설치에 성공했음을 의미합니다.



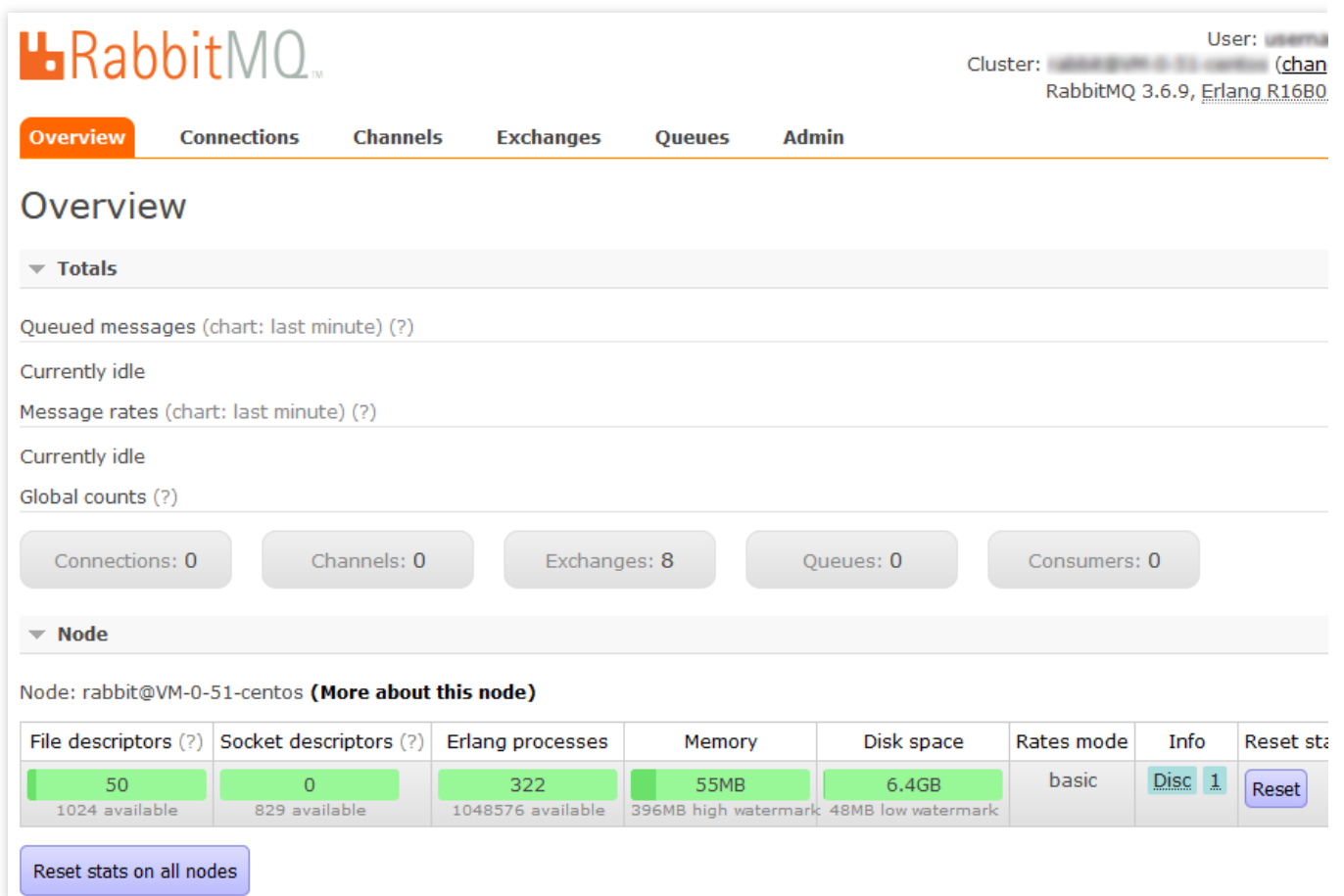
RabbitMQ™

Username:

Password:

Login

3. 아래 이미지와 같이 6단계에서 생성한 관리자 계정으로 로그인하면 RabbitMQ 관리 인터페이스로 이동할 수 있습니다.



RabbitMQ™

User: [username](#)

Cluster: [rabbit@VM-0-51-centos](#) (channel)

RabbitMQ 3.6.9, Erlang R16B0

Overview | Connections | Channels | Exchanges | Queues | Admin

Overview

▼ Totals

Queued messages (chart: last minute) (?)

Currently idle

Message rates (chart: last minute) (?)

Currently idle

Global counts (?)

Connections: 0 | Channels: 0 | Exchanges: 8 | Queues: 0 | Consumers: 0

▼ Node

Node: rabbit@VM-0-51-centos ([More about this node](#))

File descriptors (?)	Socket descriptors (?)	Erlang processes	Memory	Disk space	Rates mode	Info	Reset stats
50 1024 available	0 829 available	322 1048576 available	55MB 396MB high watermark	6.4GB 48MB low watermark	basic	Disc 1	Reset

[Reset stats on all nodes](#)

시각화 인터페이스 구축

Ubuntu 시각화 인터페이스 구축

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

VNC(Virtual Network Console)는 가상 네트워크 콘솔의 약자입니다. 유명한 AT&T 유럽 연구소에서 개발한 우수한 원격 제어 소프트웨어입니다. VNC는 UNIX 및 Linux 운영 체제를 기반으로 하는 오픈 소스 소프트웨어로, 강력한 원격 제어 기능, 높은 효율성 및 실용성을 갖추고 있으며, 그 성능은 Windows 및 MAC의 모든 원격 제어 소프트웨어와 견줄만합니다. 본문은 Ubuntu CVM에서 시각적 인터페이스를 구축하는 방법을 안내합니다.

전제 조건

Ubuntu CVM을 구입 완료해야 합니다.

작업 단계

인스턴스 보안 그룹 설정

VNC 서비스는 TCP 프로토콜을 사용하며 기본적으로 5901 포트가 사용됩니다. 인스턴스에 바인딩된 보안 그룹에서 5901 포트가 개방되어 있어야 합니다. 인바운드 규칙 TCP:5901을 생성하여 5901 포트를 개방합니다. 자세한 내용은 [보안 그룹 규칙 추가](#)를 참고하십시오.

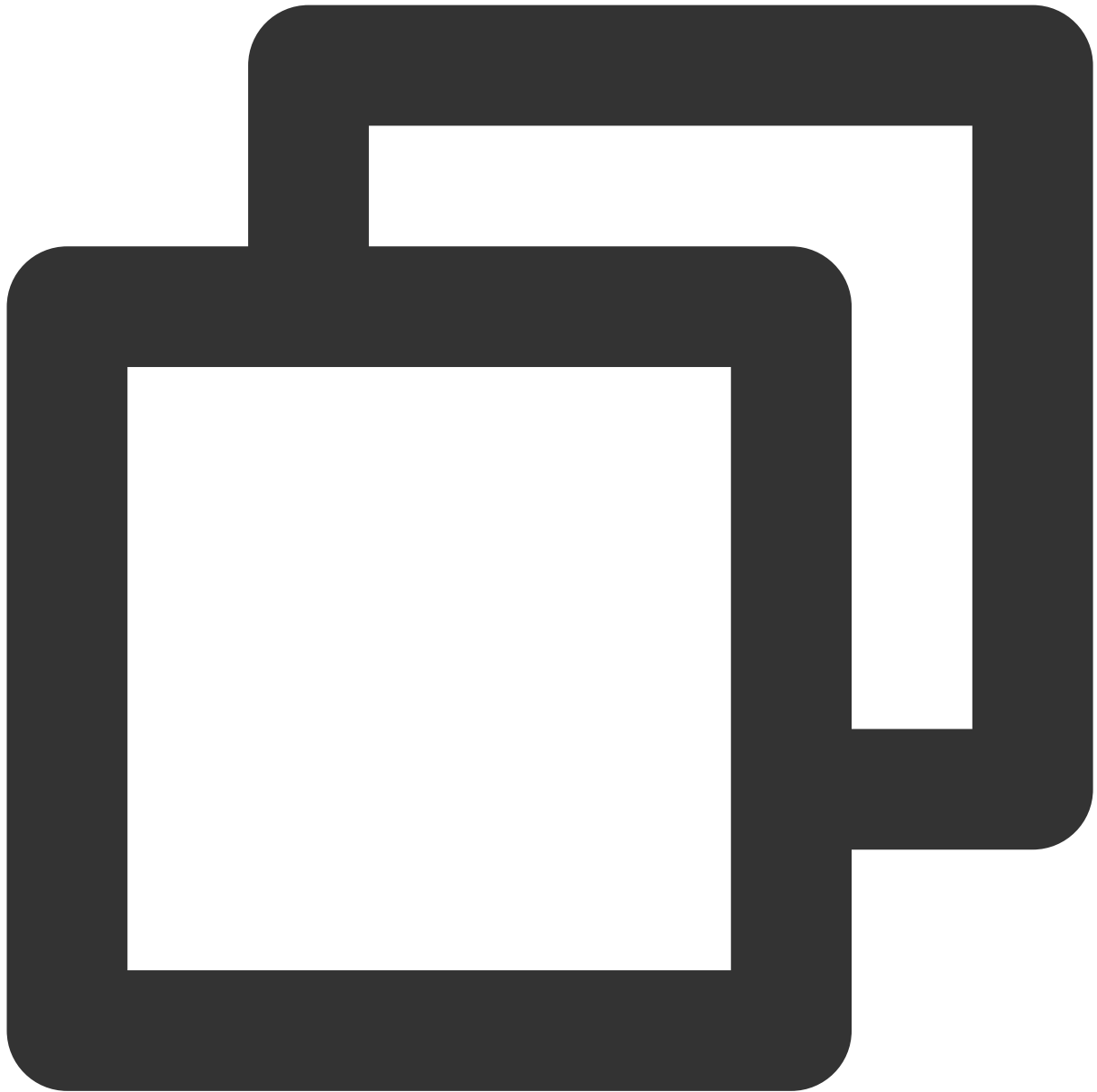
패키지 설치

Ubuntu 18.04

Ubuntu 20.04

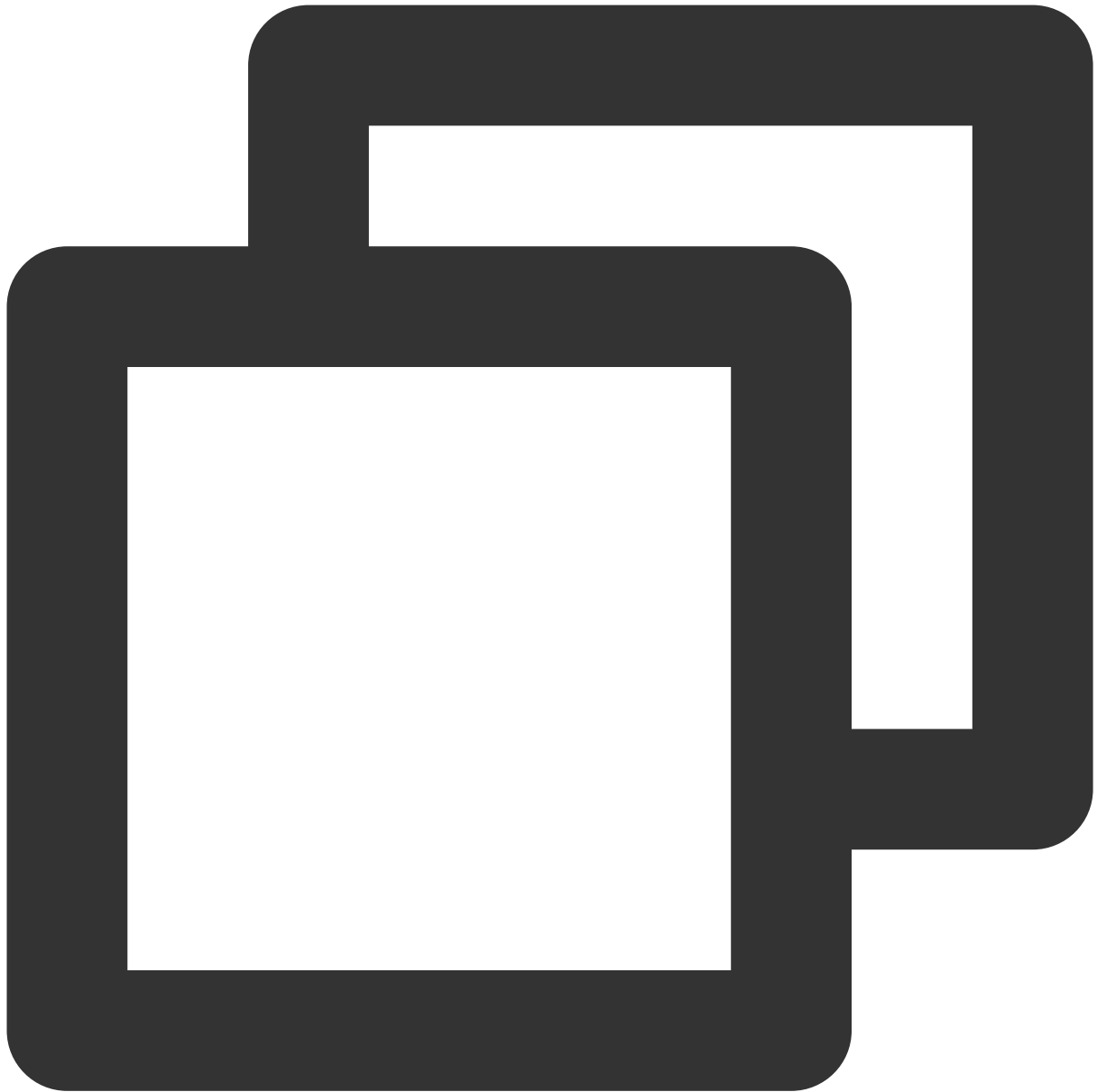
Ubuntu 22.04

1. 표준 방식으로 [Linux 인스턴스에 로그인\(권장\)](#)합니다.
2. 다음 명령을 실행하여 캐시를 삭제하고 소프트웨어 패키지 리스트를 업데이트합니다.



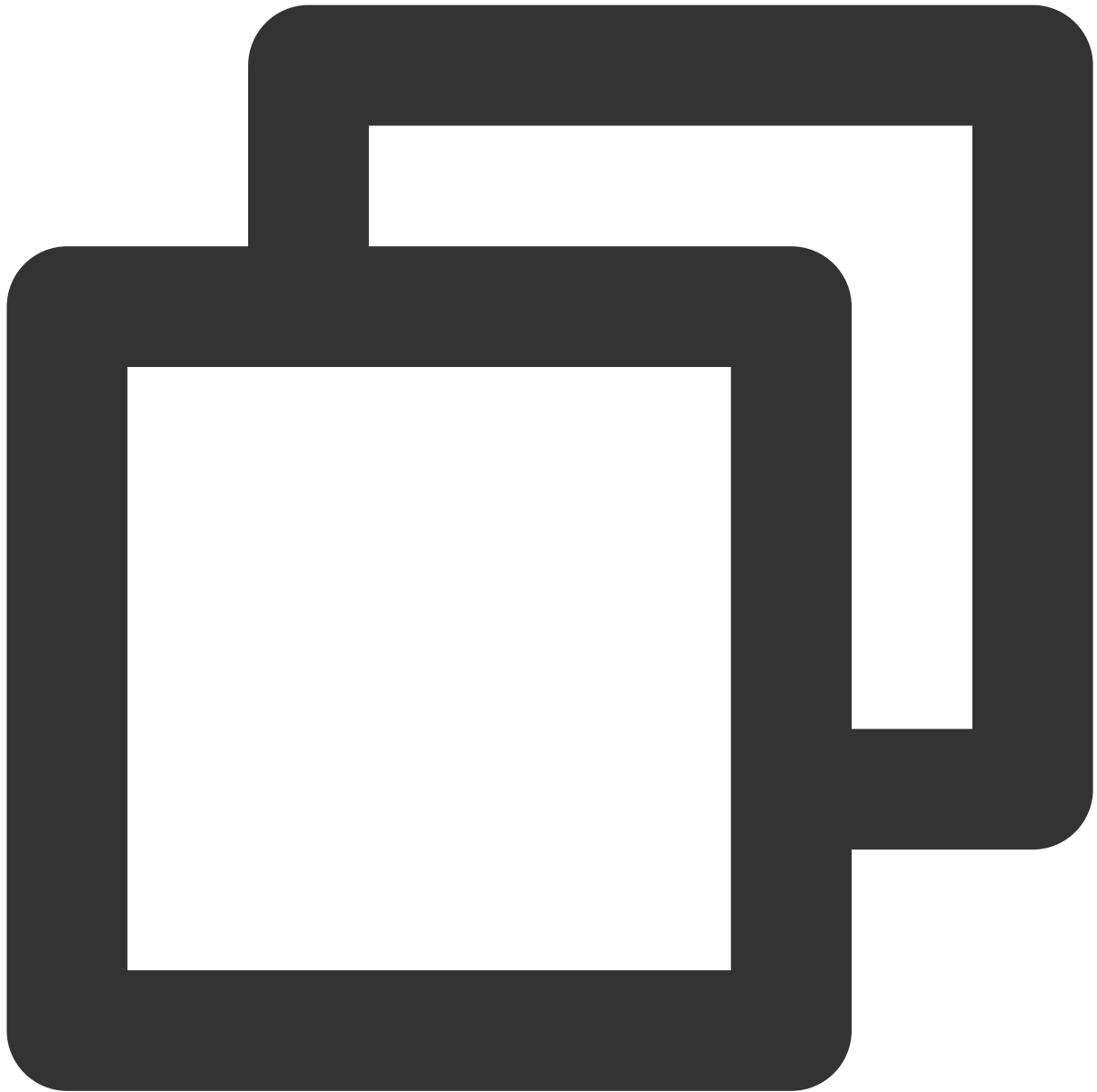
```
sudo apt clean all && sudo apt update
```

3. 다음 명령어를 실행하여 데스크톱 환경에 필요한 소프트웨어 패키지를 설치합니다. 시스템 패널, 창 관리자, 파일 브라우저 및 터미널과 같은 데스크톱 응용 프로그램이 포함됩니다.



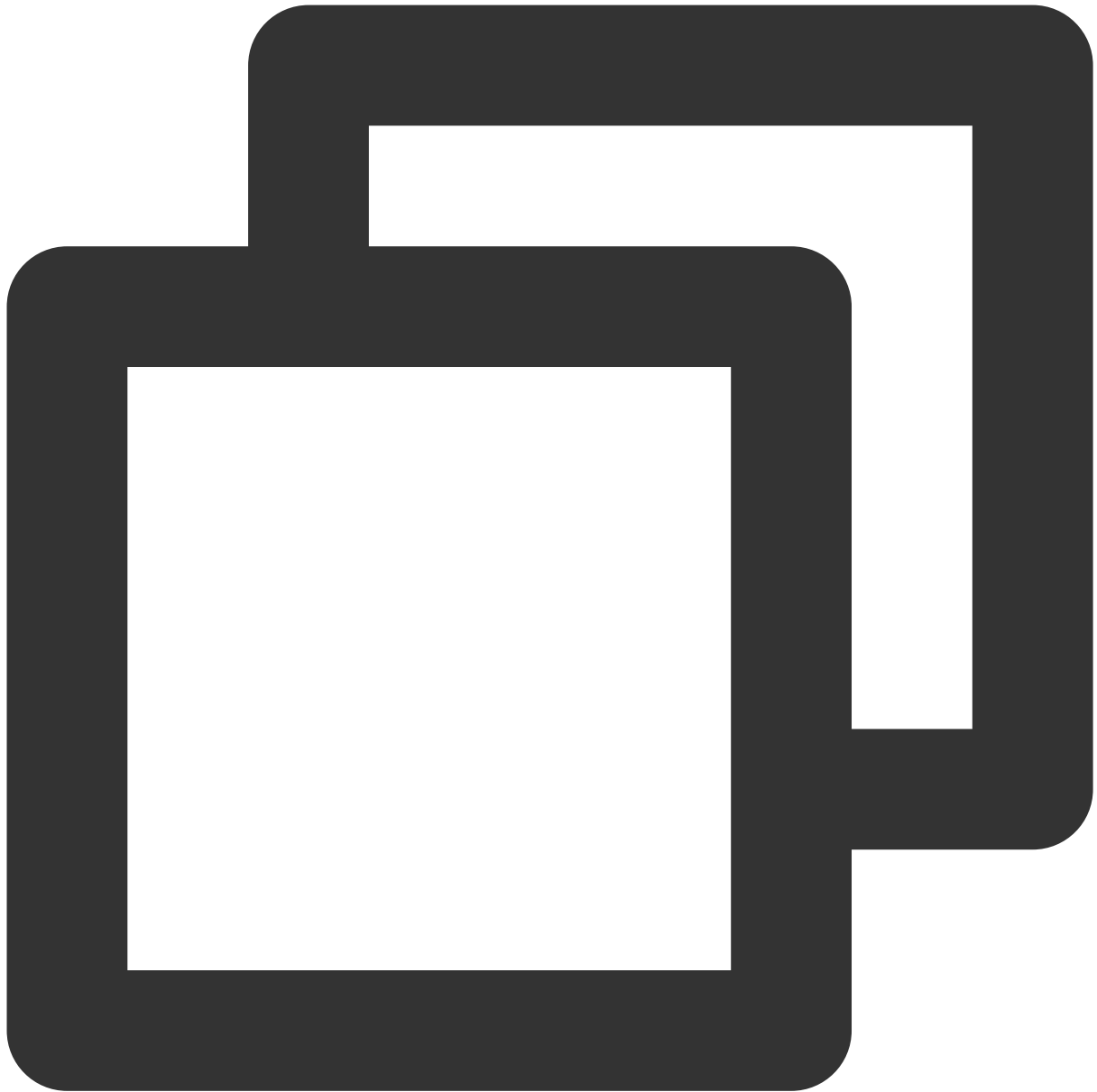
```
sudo apt install gnome-panel gnome-settings-daemon metacity nautilus gnome-terminal
```

4. 아래의 명령어를 실행하여 VNC를 설치합니다.



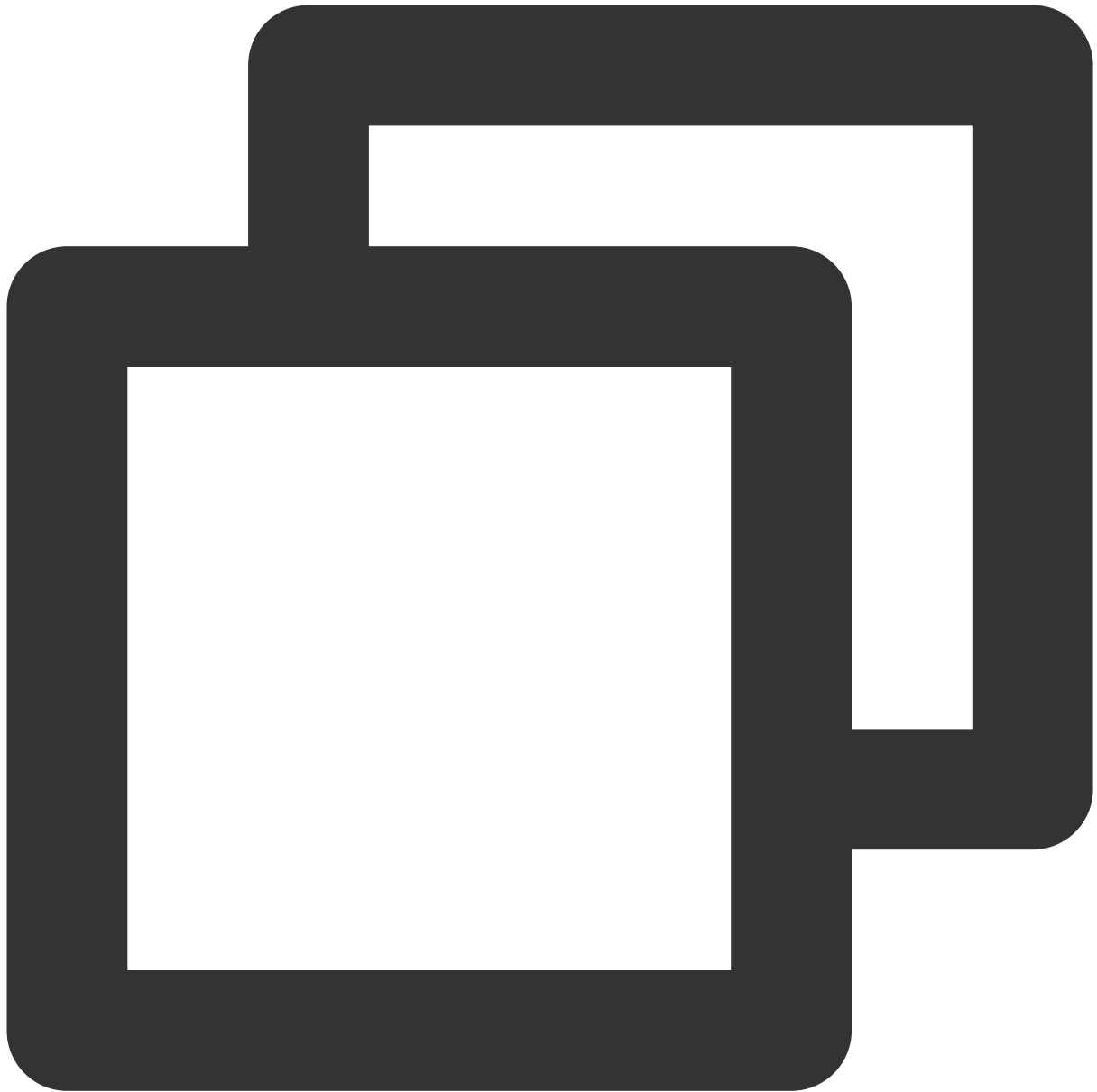
```
apt-get install vnc4server
```

1. 표준 방식으로 [Linux 인스턴스에 로그인\(권장\)](#)합니다.
2. 다음 명령을 실행하여 캐시를 삭제하고 소프트웨어 패키지 리스트를 업데이트합니다.



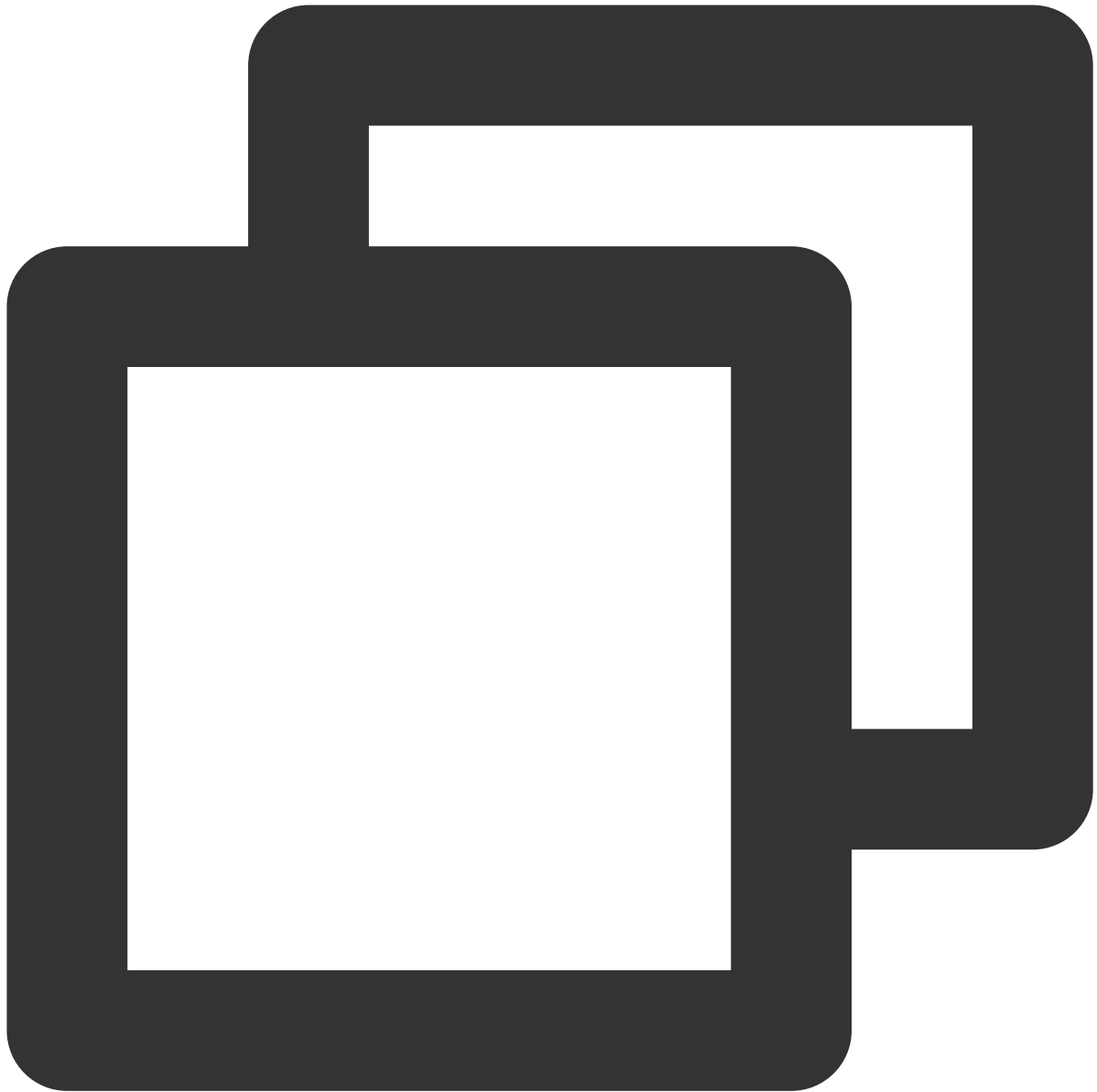
```
sudo apt clean all && sudo apt update
```

3. 다음 명령어를 실행하여 데스크톱 환경에 필요한 소프트웨어 패키지를 설치합니다. 시스템 패널, 창 관리자, 파일 브라우저 및 터미널과 같은 데스크톱 응용 프로그램이 포함됩니다.



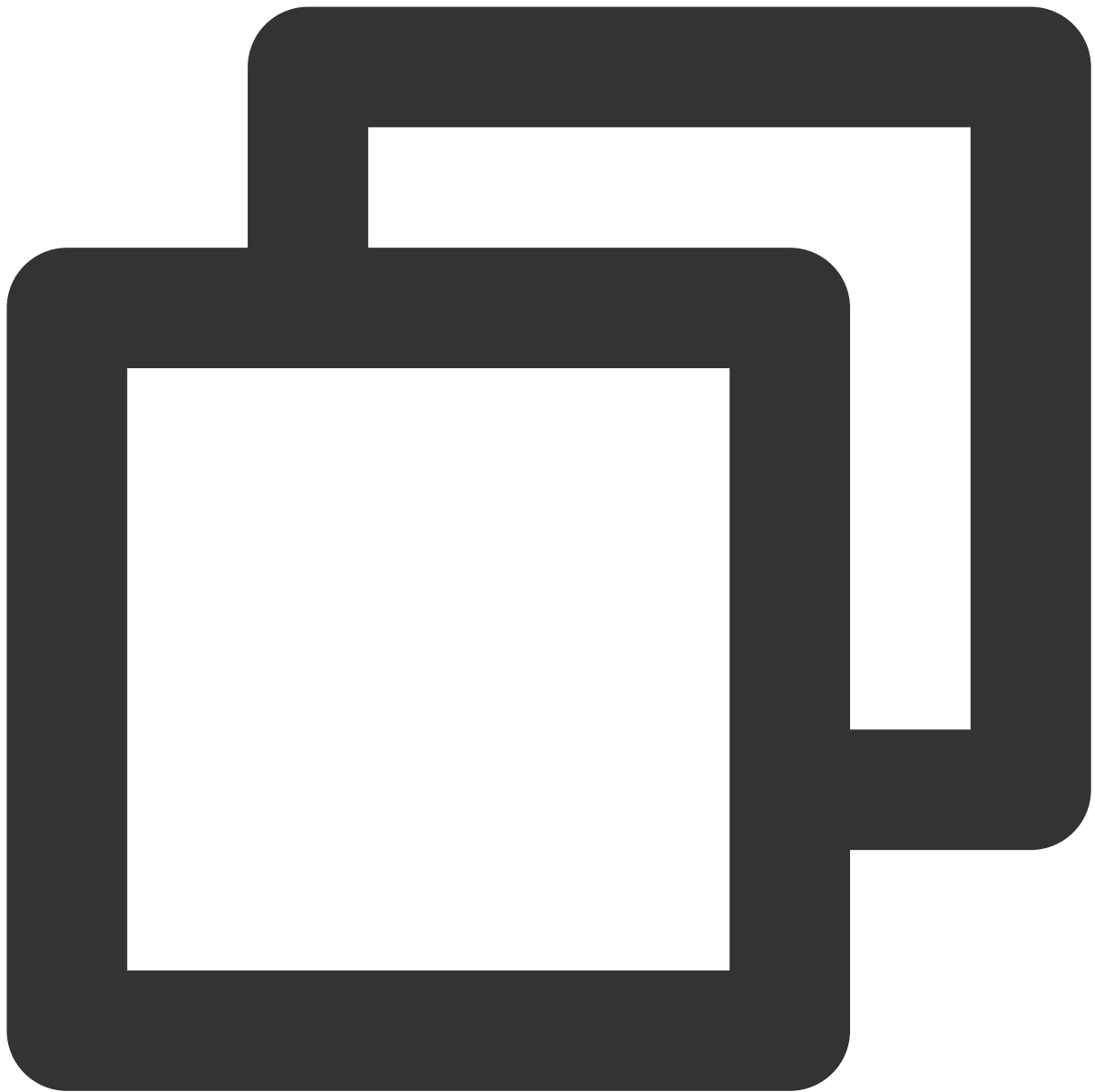
```
sudo apt install gnome-panel gnome-settings-daemon metacity nautilus gnome-terminal
```

4. 아래의 명령어를 실행하여 VNC를 설치합니다.



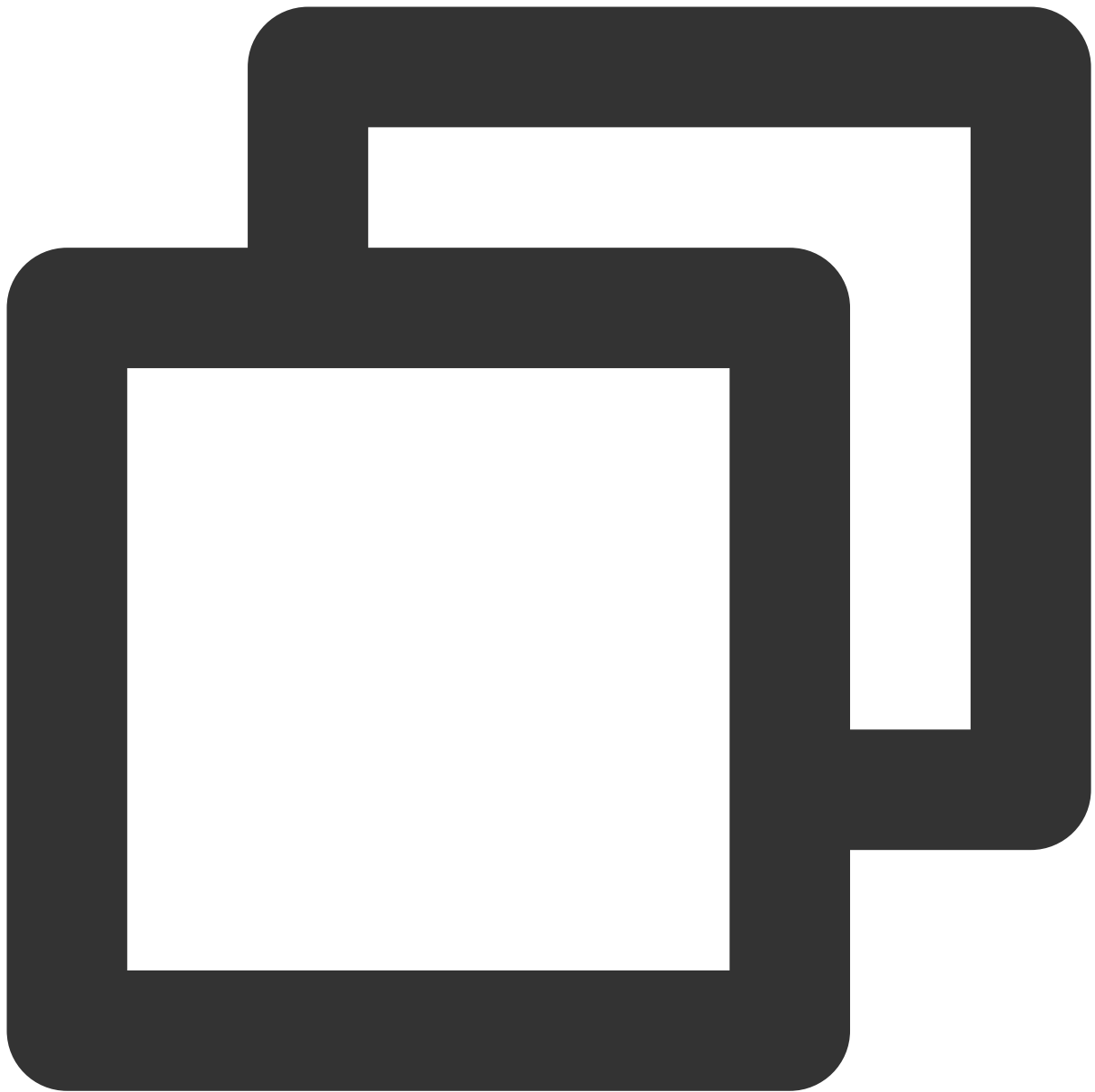
```
apt-get install tightvncserver
```

1. 표준 방식으로 [Linux 인스턴스에 로그인\(권장\)](#)합니다.
2. 캐시를 지우고 소프트웨어 패키지 목록을 업데이트합니다.



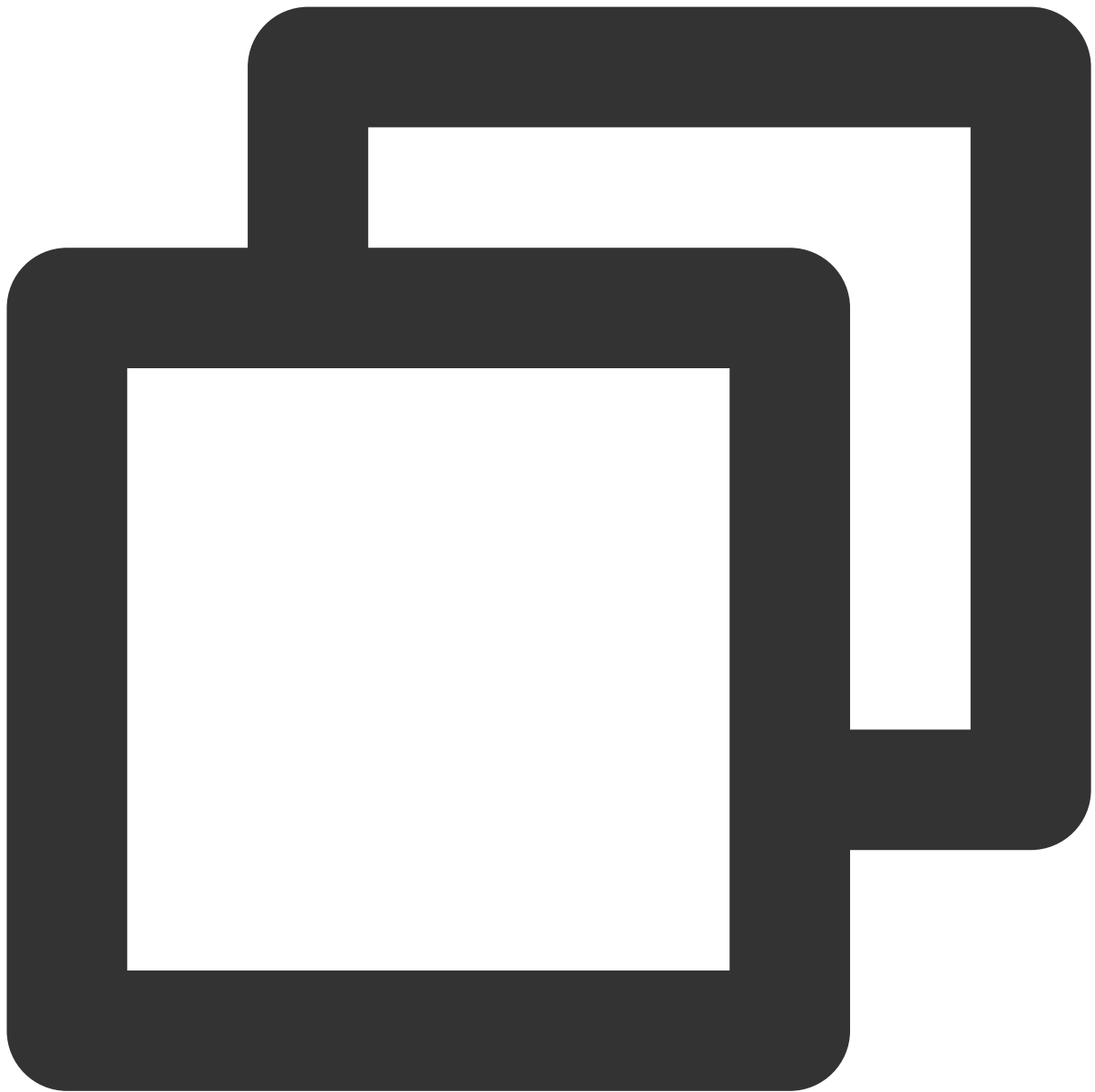
```
sudo apt clean all && sudo apt update
```

3. 데스크톱 환경을 설치합니다.



```
sudo apt install xfce4 xfce4-goodies
```

4. 아래의 명령어를 실행하여 VNC를 설치합니다.



```
sudo apt install tightvncserver
```

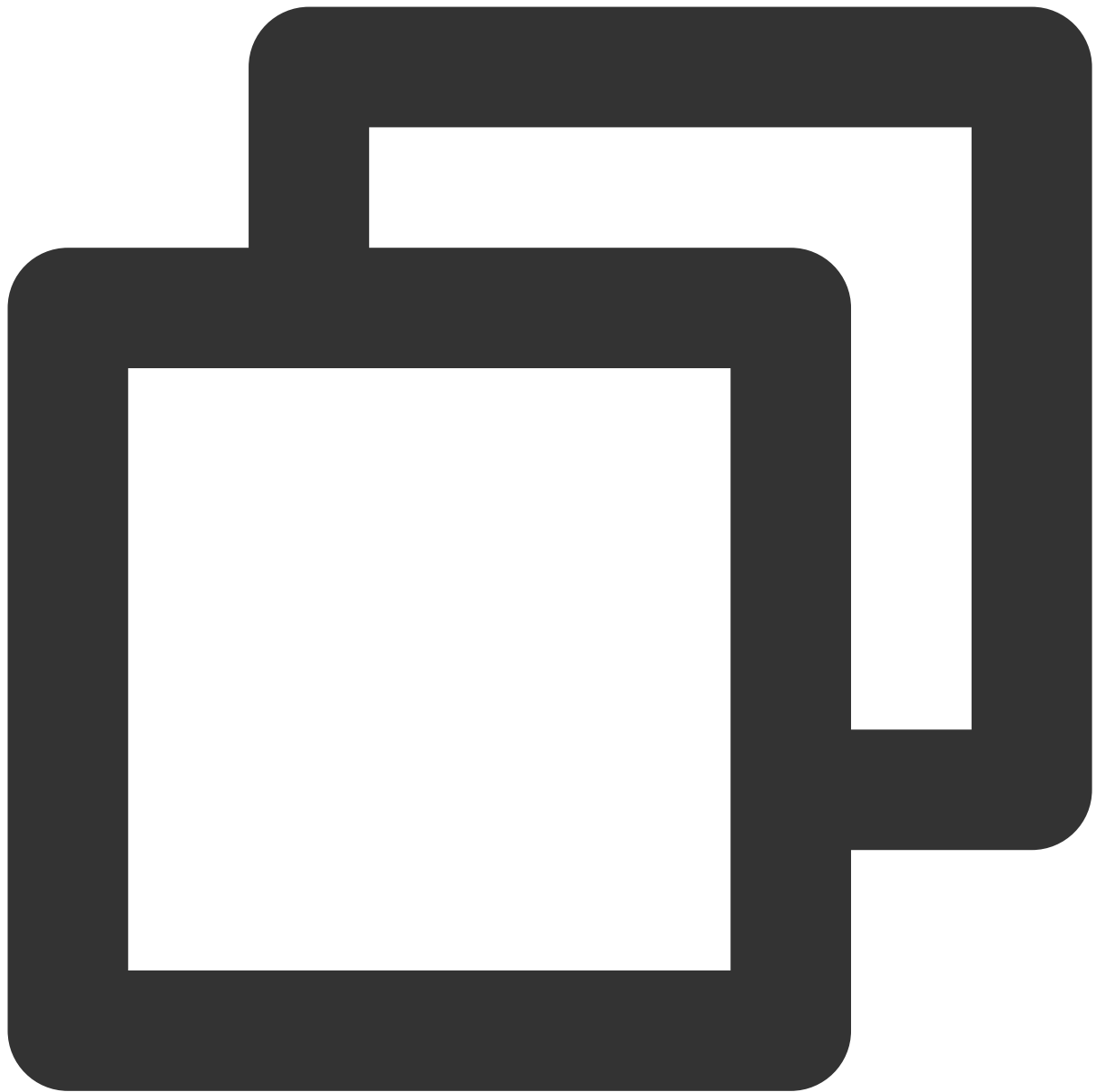
VNC 설정

Ubuntu 18.04

Ubuntu 20.04

Ubuntu 22.04

1. 다음 명령어를 실행하여 VNC 서비스를 시작하고 VNC의 비밀번호를 설정합니다.



```
vncserver
```

다음과 같은 결과가 반환되면 VNC가 성공적으로 실행되었음을 의미합니다.


```
root@VM-0-133-ubuntu:/home/ubuntu# vncserver

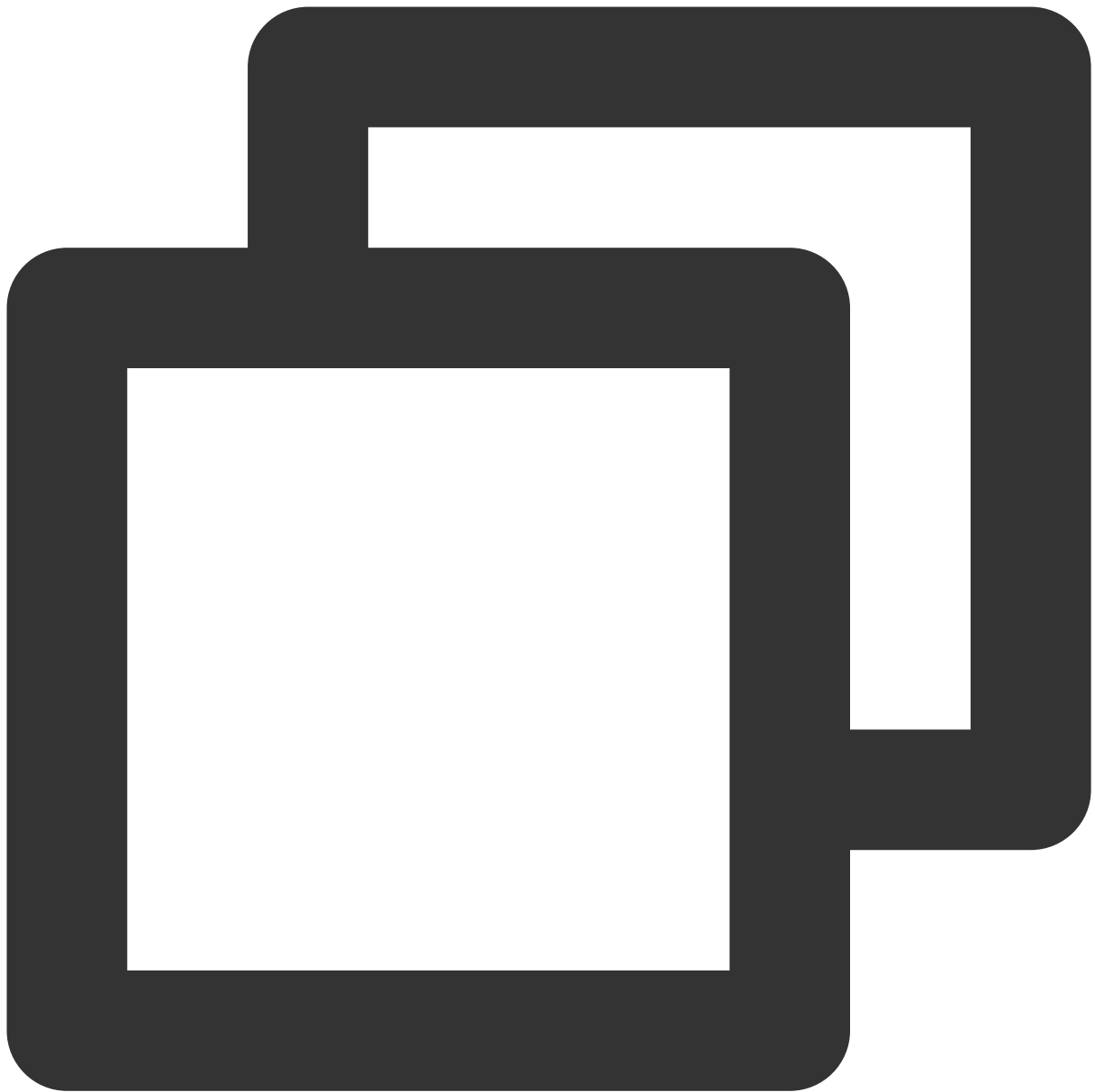
You will require a password to access your desktops.

Password:
Verify:
xauth:  file /root/.Xauthority does not exist

New 'VM-0-133-ubuntu:1 (root)' desktop is VM-0-133-ubuntu:1

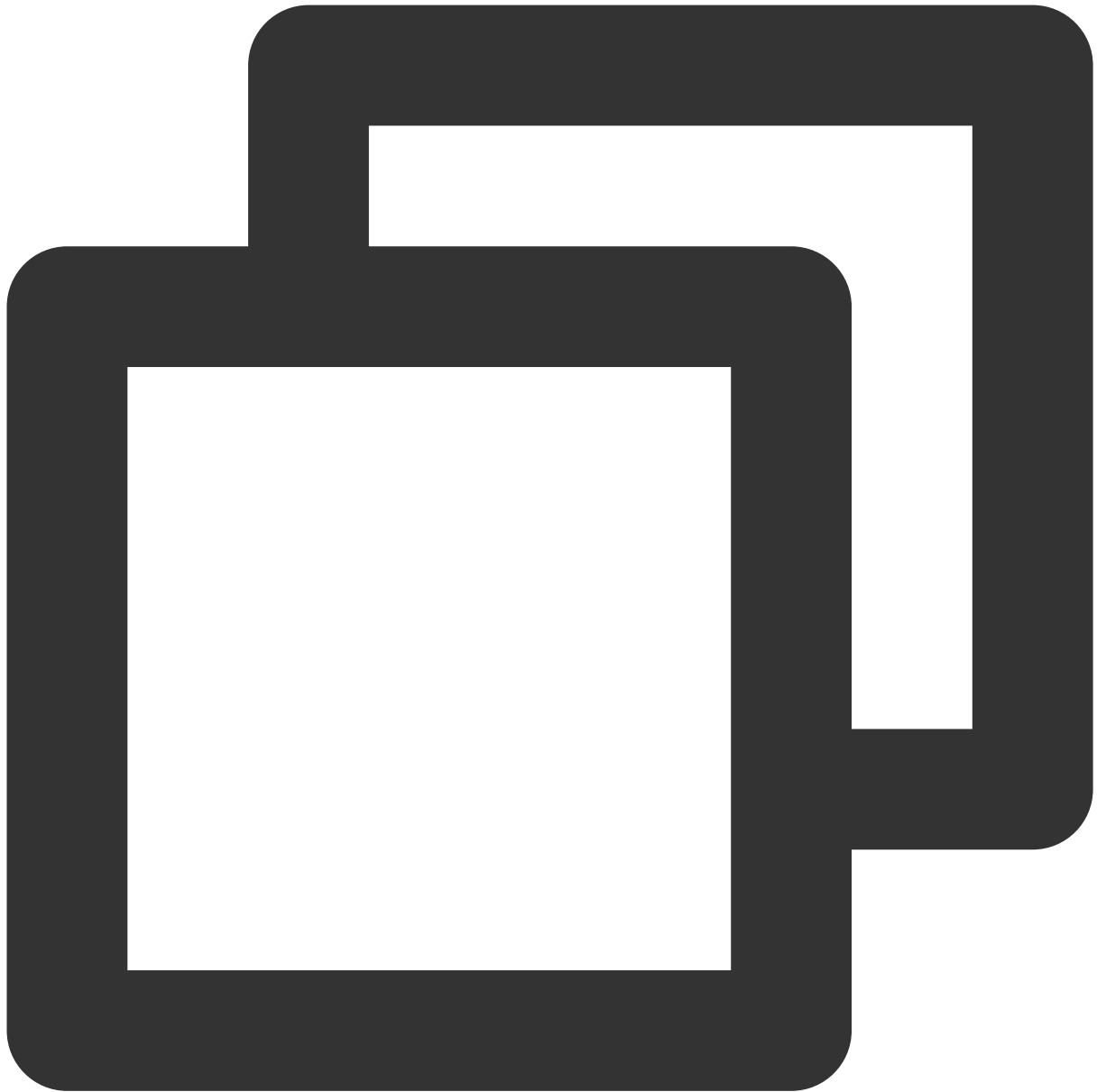
Creating default startup script /root/.vnc/xstartup
Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/VM-0-133-ubuntu:1.log
```

2. 다음 명령어를 실행하여 VNC 구성 파일을 엽니다.



```
vi ~/.vnc/xstartup
```

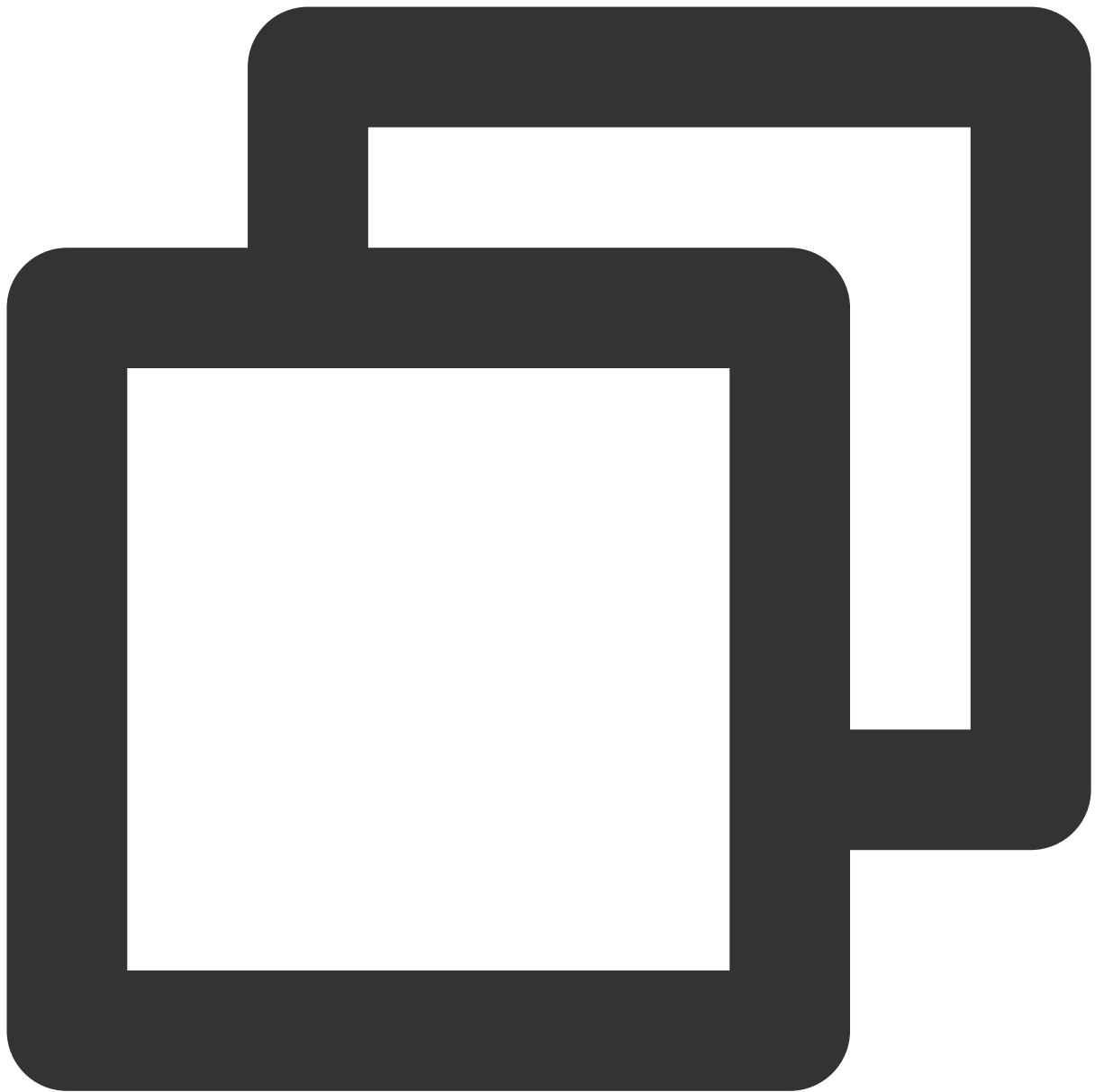
3. **i**를 눌러 편집 모드로 전환하고 구성 파일을 다음 콘텐츠와 같이 수정합니다.



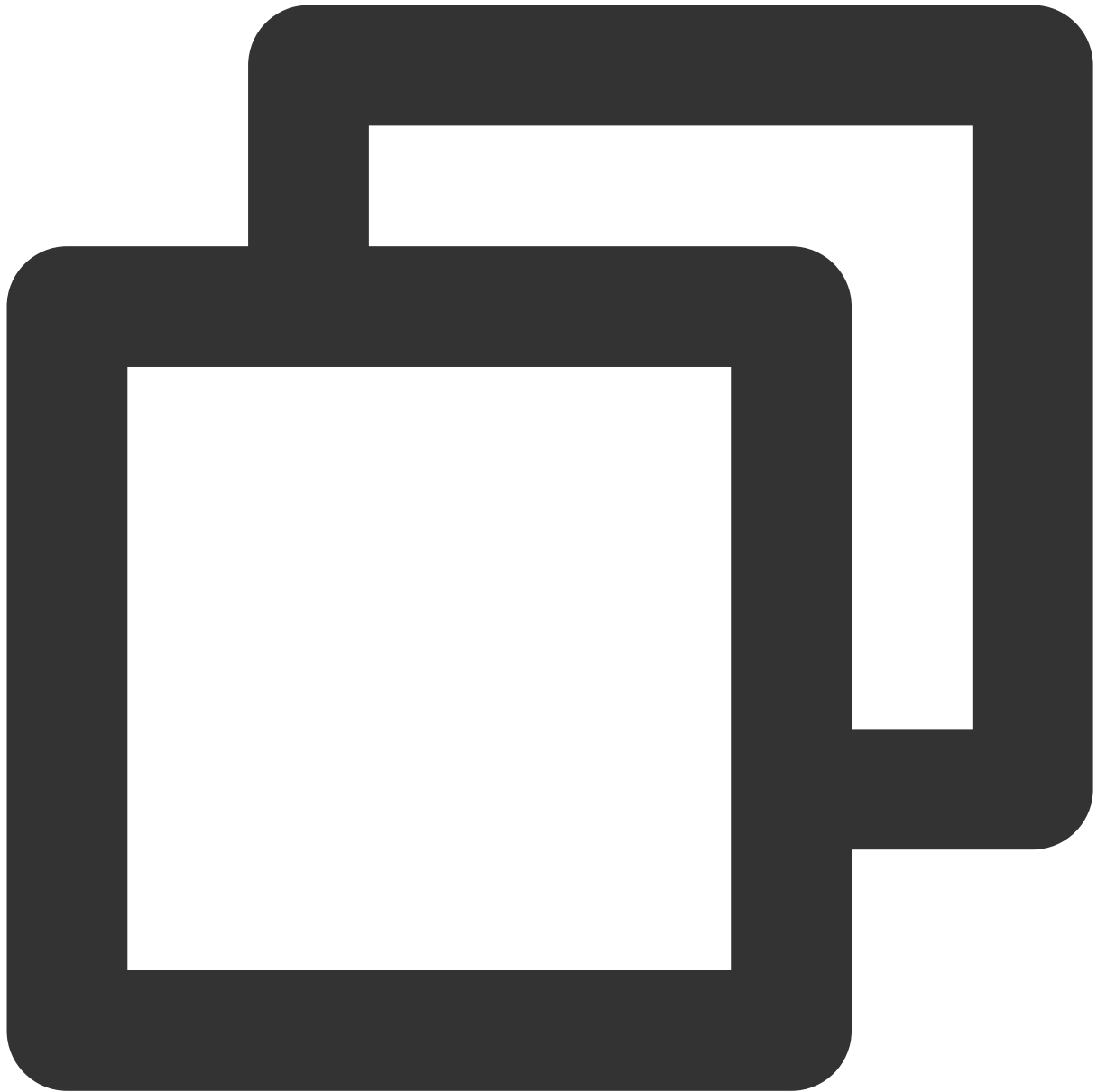
```
#!/bin/sh
export XKL_XMODMAP_DISABLE=1
export XDG_CURRENT_DESKTOP="GNOME-Flashback:GNOME"
export XDG_MENU_PREFIX="gnome-flashback-"
gnome-session --session=gnome-flashback-metacity --disable-acceleration-check &
```

4. **Esc**를 눌러 **:wq**를 입력하여 파일을 저장 및 반환합니다.

5. 다음 명령어를 실행하여 데스크톱 프로세스를 재시작합니다.



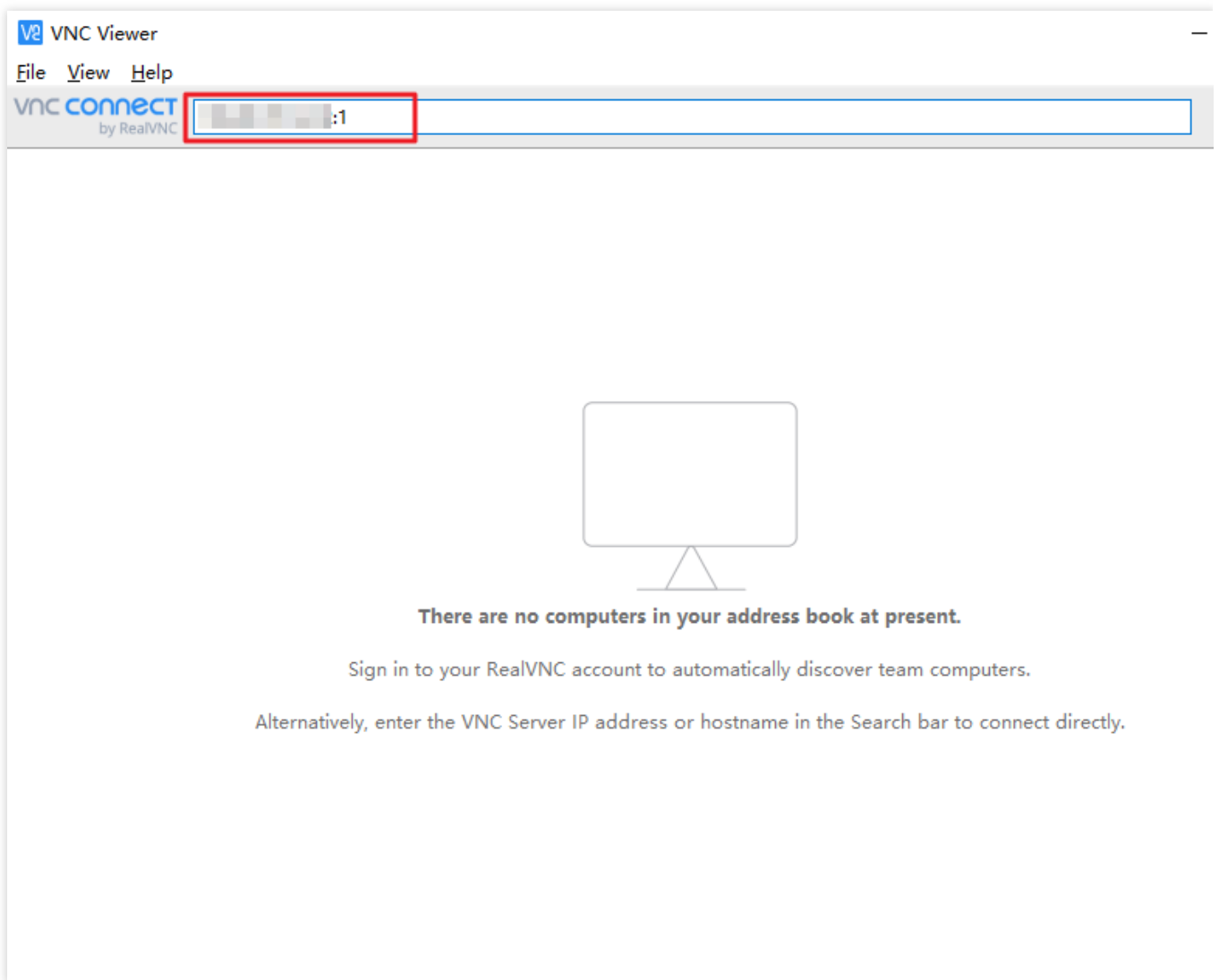
```
vncserver -kill :1 #기존 데스크톱 프로세스 종료 후 명령어 입력 (이 중 :1은 데스크톱 번호)
```



```
vncserver -geometry 1920x1080 :1 #새로운 세션 생성
```

6. [여기](#)를 클릭하여 VNC Viewer 공식 홈페이지로 이동한 후 로컬 컴퓨터의 운영 체제 유형에 따라 버전을 다운로드하고 설치합니다.

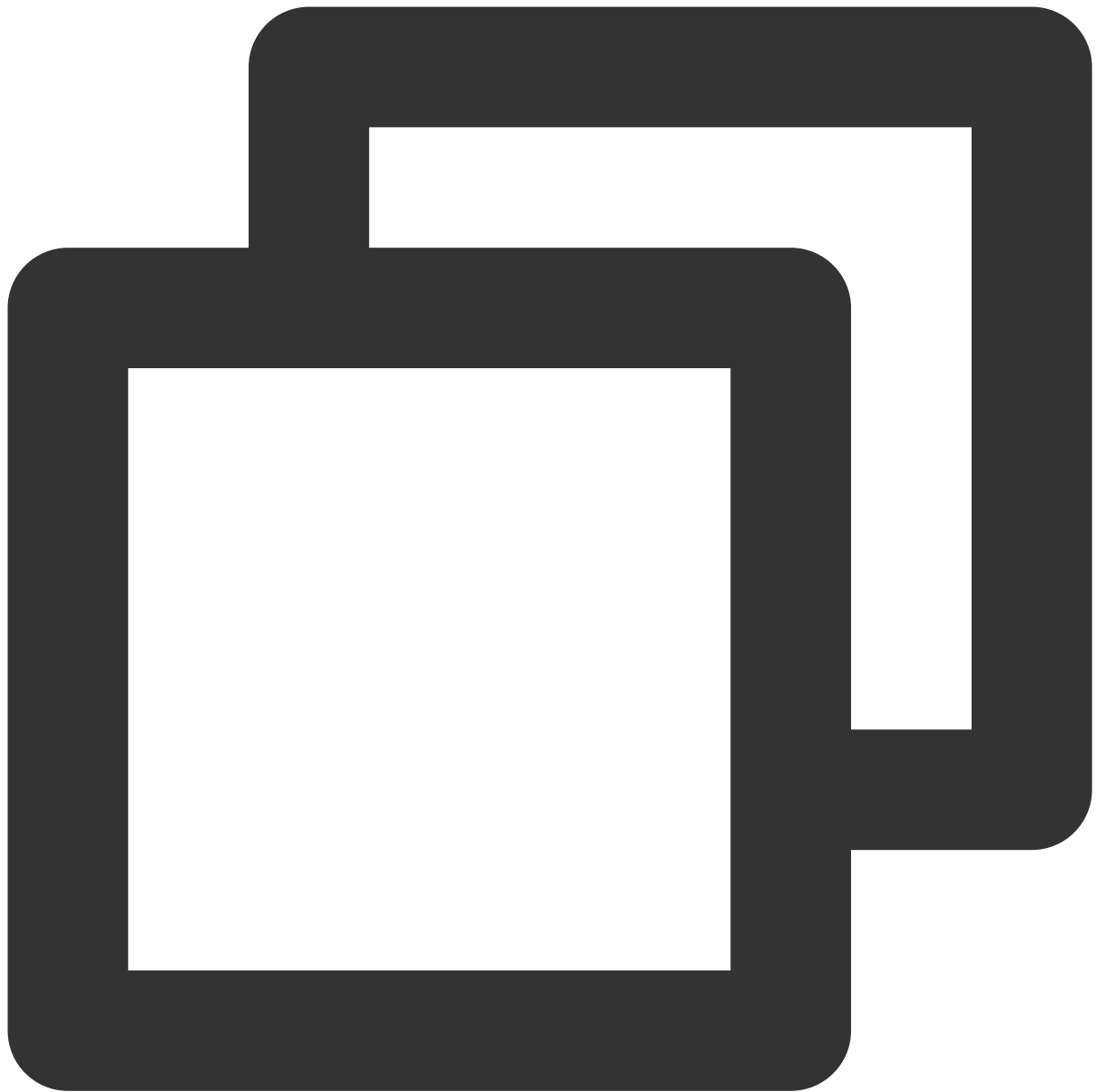
7. VNC Viewer 소프트웨어에서 CVM의 IP 주소 :1 을 입력하고 **Enter**를 누릅니다.



8. 팝업된 알림 창에서 **Continue**를 클릭합니다.

9. **2단계**에서 설정한 VNC 비밀번호를 입력하고 **OK**를 클릭하면 인스턴스에 로그인하여 그래픽 인터페이스를 사용할 수 있습니다.

1. 다음 명령어를 실행하여 VNC 서비스를 시작하고 VNC의 비밀번호를 설정합니다.



```
vncserver
```

다음과 같은 결과가 반환되면 VNC가 성공적으로 실행되었음을 의미합니다.

```
root@VM-0-133-ubuntu:/home/ubuntu# vncserver

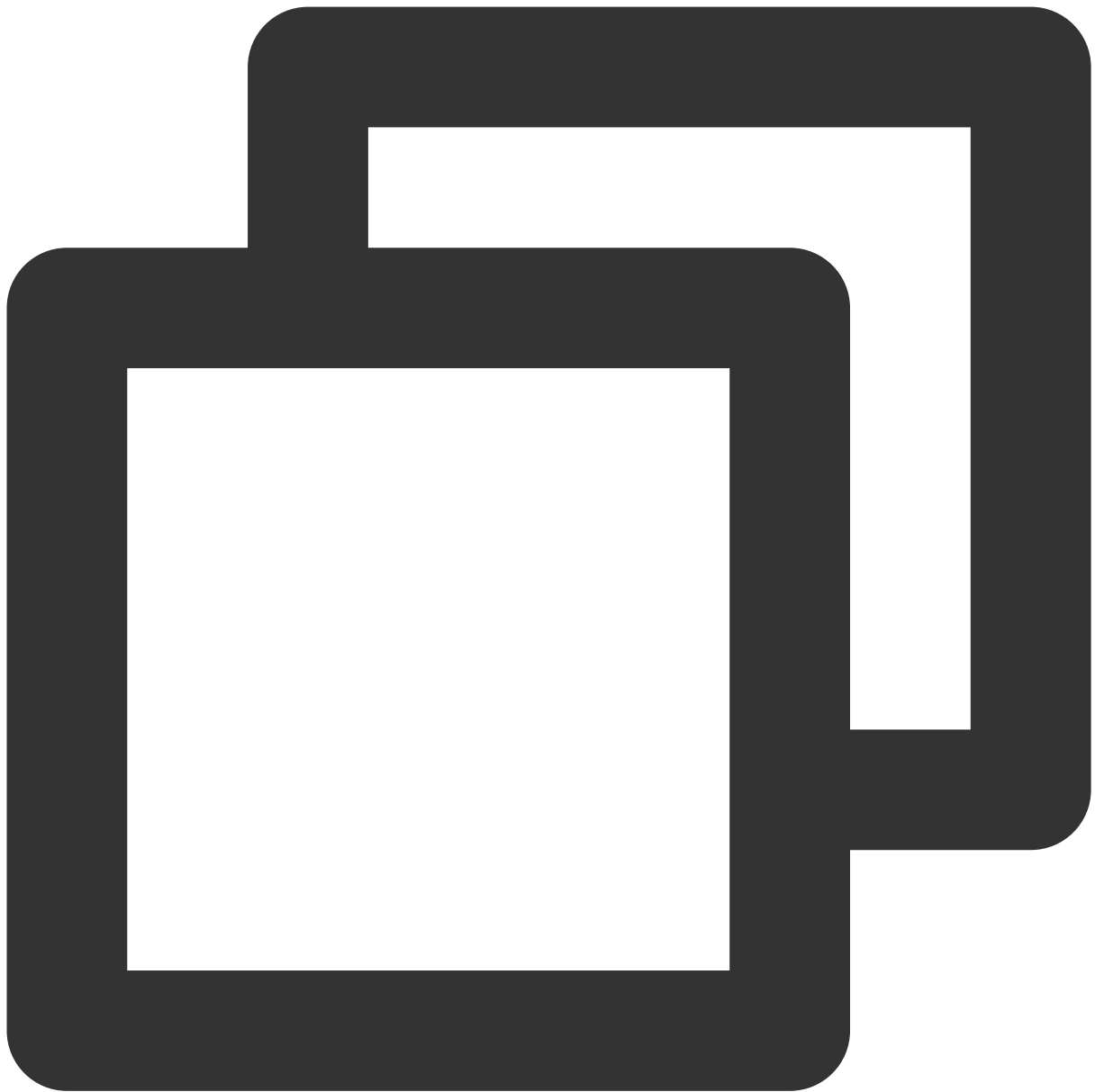
You will require a password to access your desktops.

Password:
Verify:
xauth:  file /root/.Xauthority does not exist

New 'VM-0-133-ubuntu:1 (root)' desktop is VM-0-133-ubuntu:1

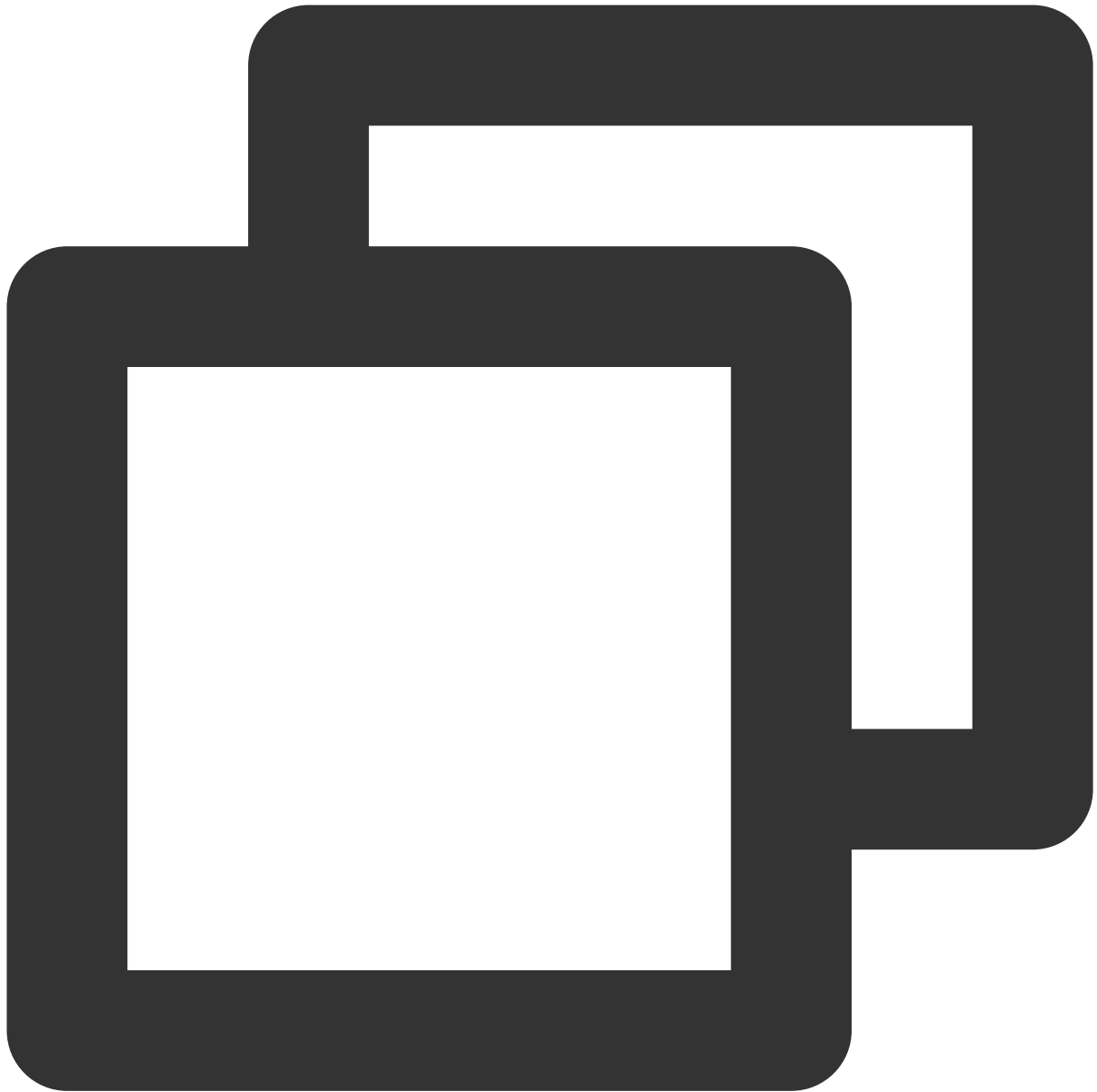
Creating default startup script /root/.vnc/xstartup
Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/VM-0-133-ubuntu:1.log
```

2. 다음 명령어를 실행하여 VNC 구성 파일을 엽니다.



```
vi ~/.vnc/xstartup
```

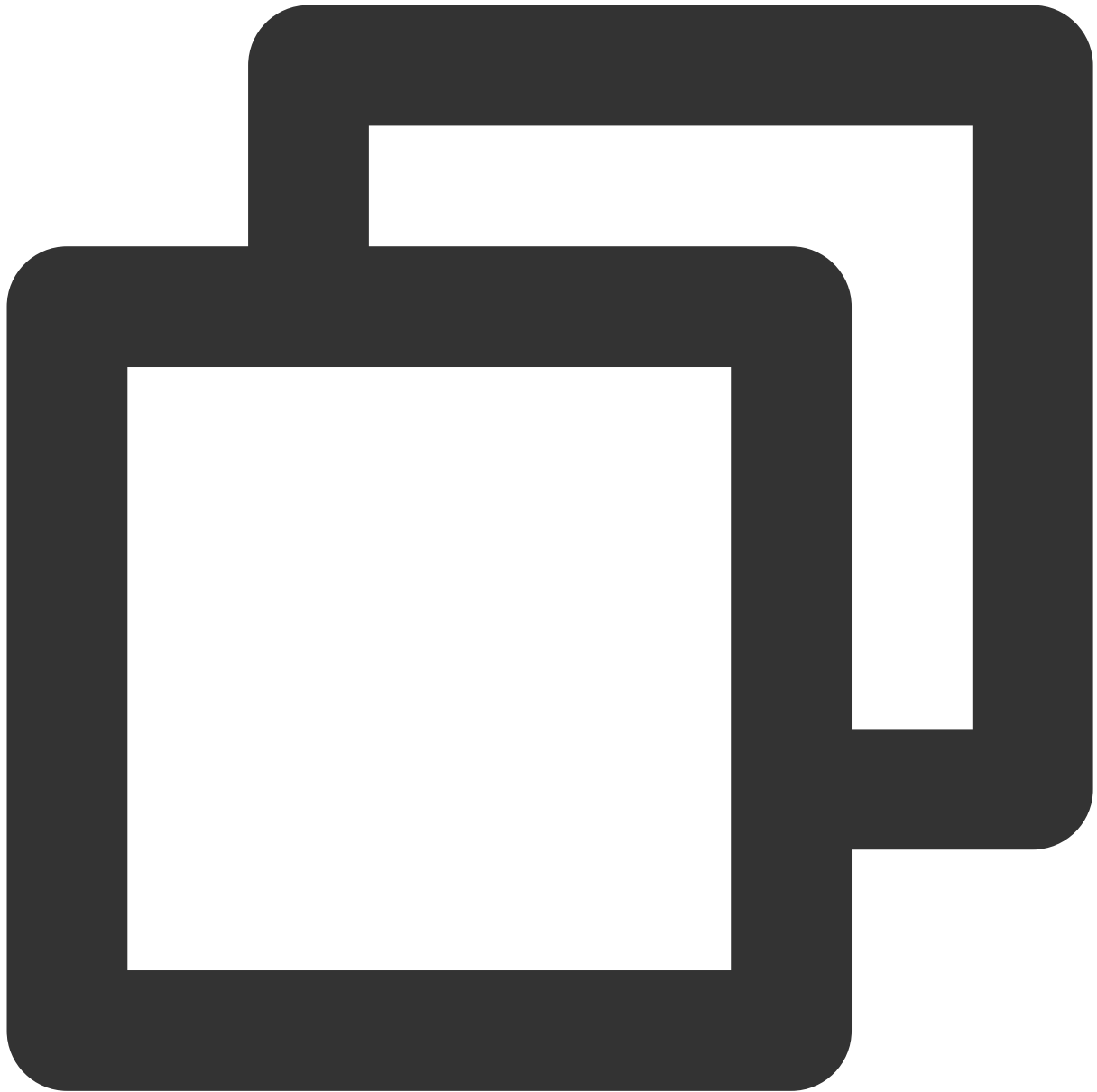
3. **i**를 눌러 편집 모드로 전환하고 구성 파일을 다음 콘텐츠와 같이 수정합니다.



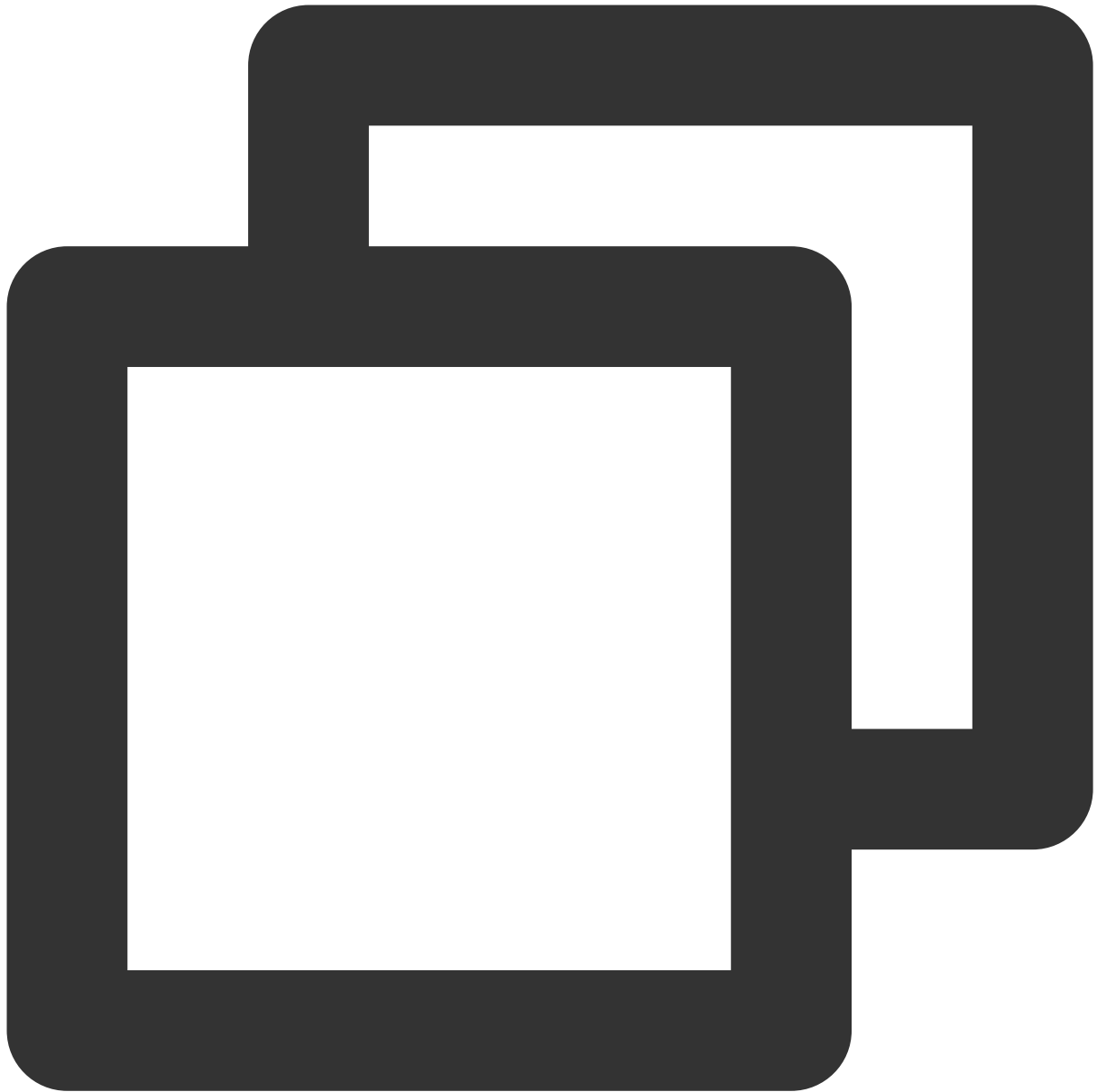
```
#!/bin/sh
export XKL_XMODMAP_DISABLE=1
export XDG_CURRENT_DESKTOP="GNOME-Flashback:GNOME"
export XDG_MENU_PREFIX="gnome-flashback-"
gnome-session --session=gnome-flashback-metacity --disable-acceleration-check &
```

4. **Esc**를 눌러 **:wq**를 입력하여 파일을 저장 및 반환합니다.

5. 다음 명령어를 실행하여 데스크톱 프로세스를 재시작합니다.



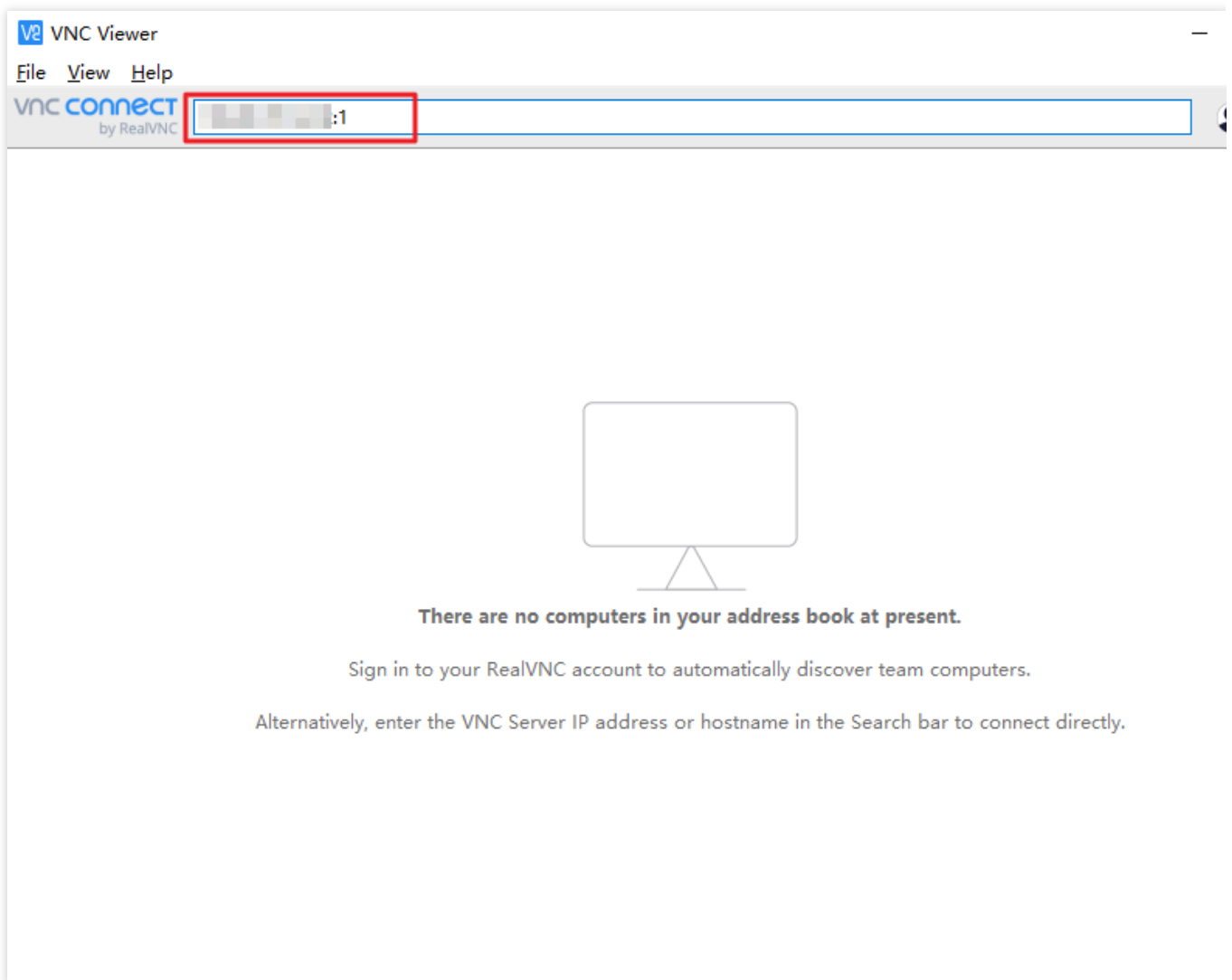
```
vncserver -kill :1 #기존 데스크톱 프로세스 종료 후 명령어 입력 (이 중 :1은 데스크톱 번호)
```



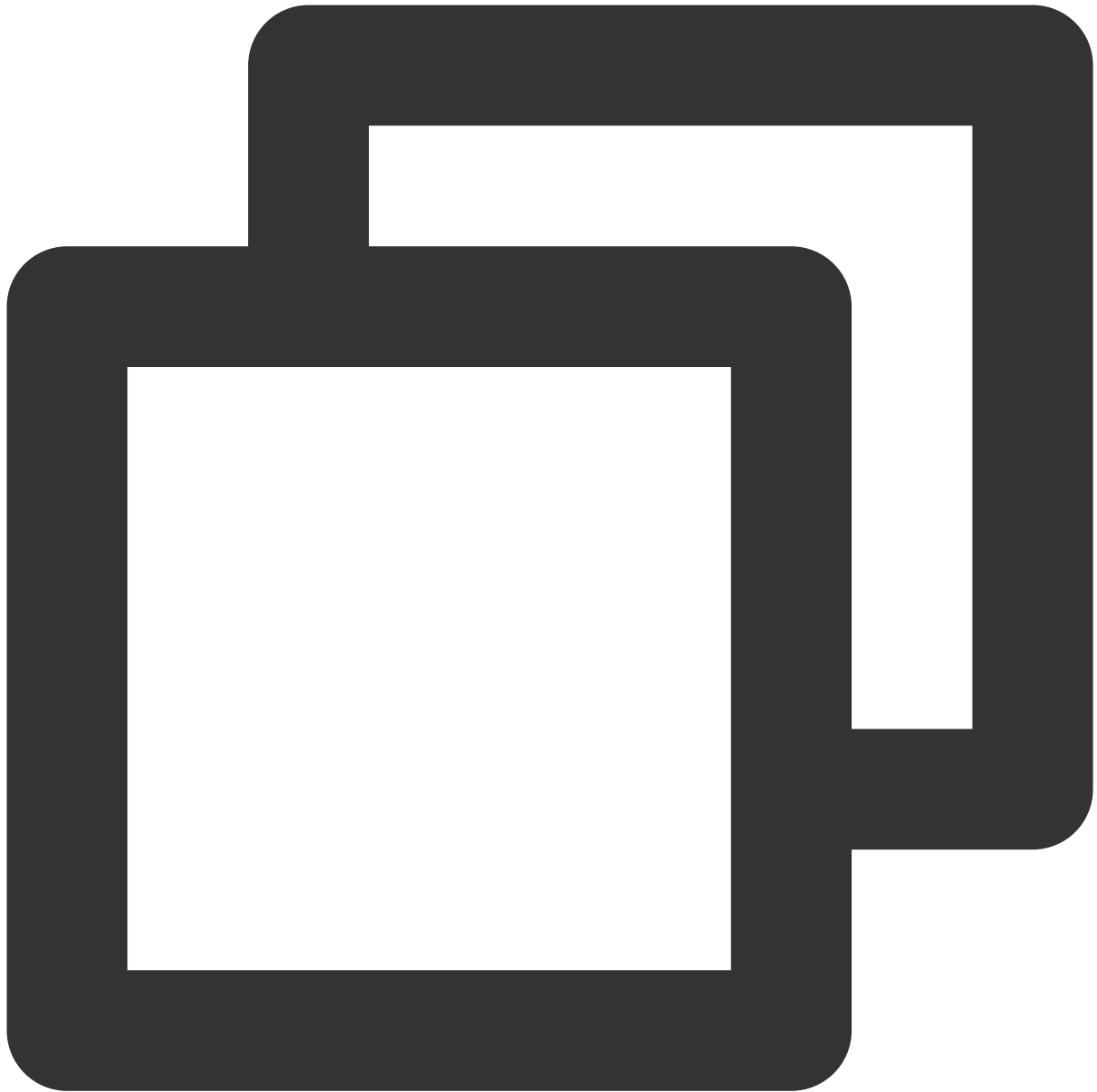
```
vncserver -geometry 1920x1080 :1 #새로운 세션 생성
```

6. [여기](#)를 클릭하여 VNC Viewer 공식 홈페이지로 이동한 후 로컬 컴퓨터의 운영 체제 유형에 따라 버전을 다운로드하고 설치합니다.

7. VNC Viewer 소프트웨어에서 CVM의 IP 주소 :1 을 입력하고 **Enter**를 누릅니다.



8. 팝업된 알림 창에서 **Continue**를 클릭합니다.
9. **2단계**에서 설정한 VNC 비밀번호를 입력하고 **OK**를 클릭하면 인스턴스에 로그인하여 그래픽 인터페이스를 사용할 수 있습니다.
1. 다음 명령어를 실행하여 VNC 서비스를 시작하고 VNC의 비밀번호를 설정합니다.



```
vncserver
```

다음과 같은 결과가 반환되면 VNC가 성공적으로 실행되었음을 의미합니다.

```

root@UM-0-133-ubuntu:/home/ubuntu# vncserver

You will require a password to access your desktops.

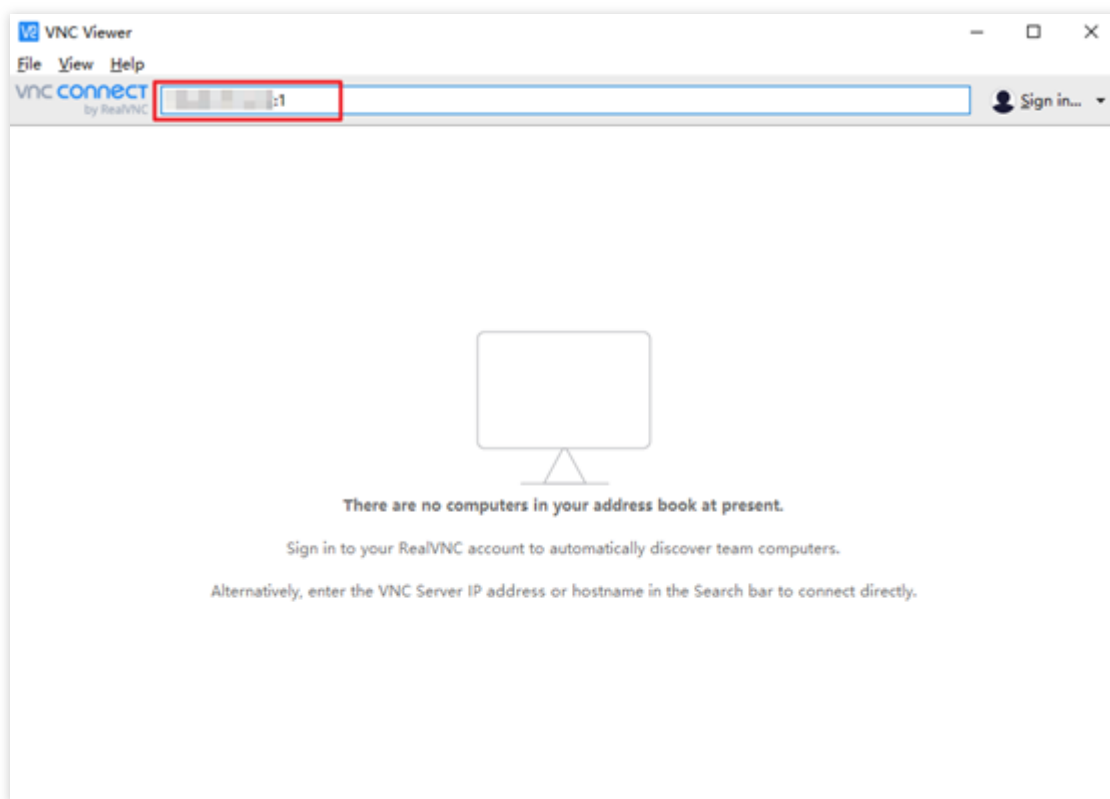
Password:
Verify:
xauth: file /root/.Xauthority does not exist

New 'UM-0-133-ubuntu:1 (root)' desktop is UM-0-133-ubuntu:1

Creating default startup script /root/.vnc/xstartup
Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/UM-0-133-ubuntu:1.log

```

2. **VNC Viewer** 공식 홈페이지로 이동한 후 로컬 컴퓨터의 운영 체제 유형에 따라 버전을 다운로드하고 설치합니다.
3. VNC Viewer 소프트웨어에서 CVM의 IP 주소 :1 을 입력하고 Enter를 누릅니다.



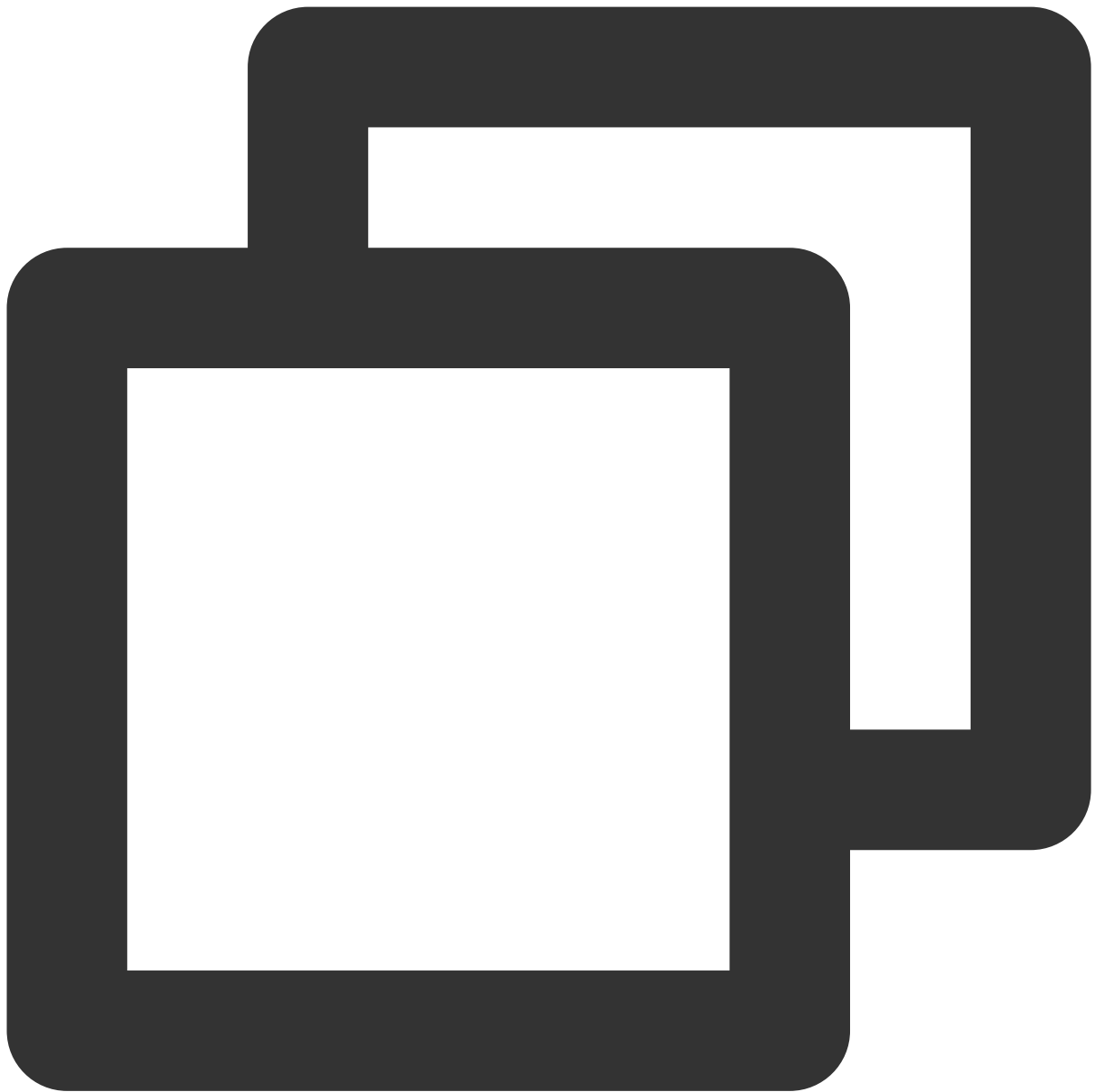
4. 팝업 창에서 **Continue**를 클릭합니다.
5. 이전 단계에서 vncserver 명령어로 생성한 비밀번호를 입력하고 OK를 클릭하면 인스턴스에 로그인하여 그래픽 인터페이스를 사용할 수 있습니다.

주의사항 :

비밀번호를 잊은 경우 인스턴스에서 `vncpasswd` 명령을 실행하여 vnc 로그인 비밀번호를 다시 변경해야 합니다.
부록:

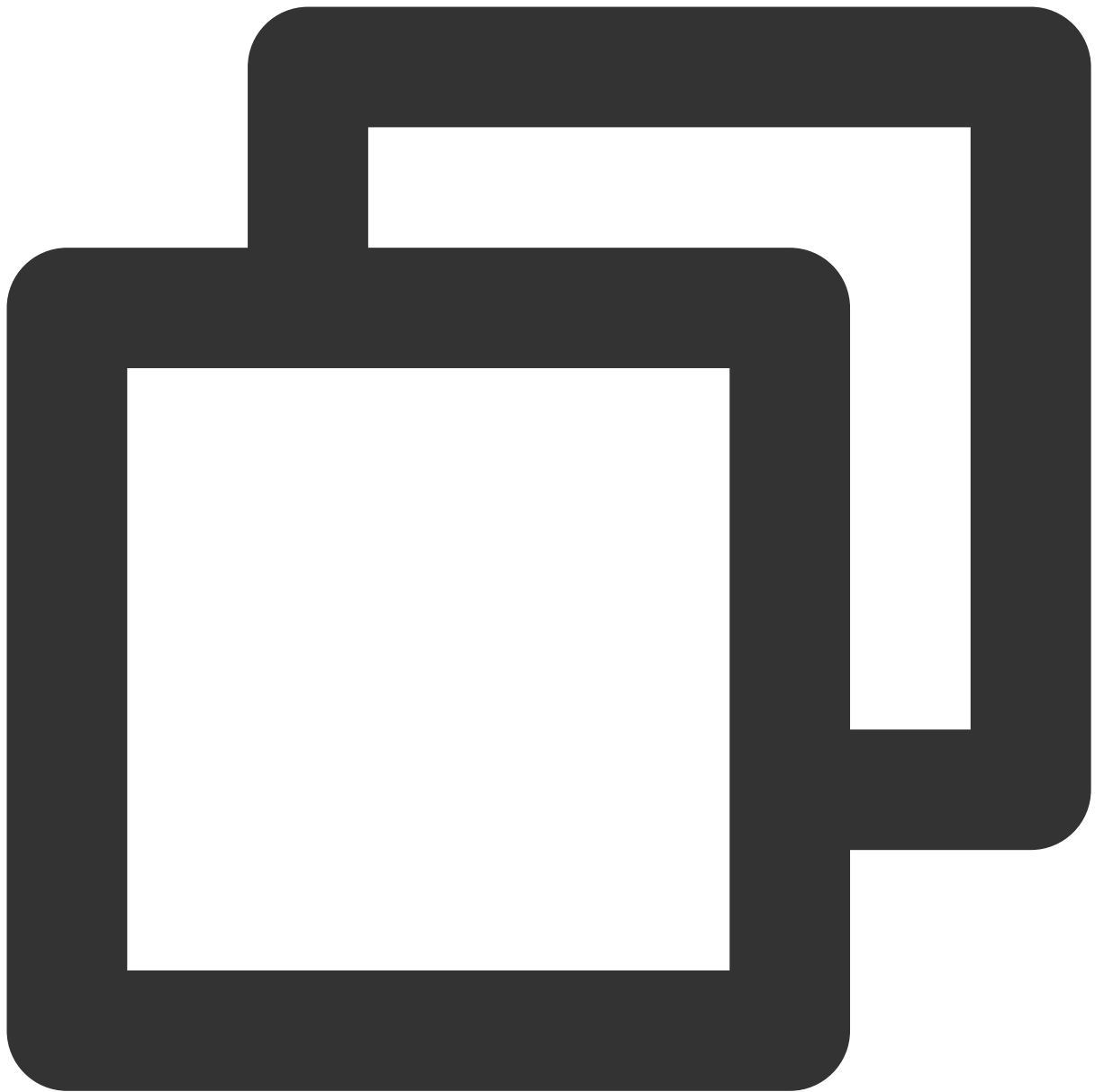
데스크톱 chrome 브라우저 설치:

인스턴스에서 명령을 실행하여 .deb 패키지 파일 다운로드



```
wget https://dl.google.com/linux/direct/google-chrome-stable_current_amd64.deb
```

.deb 파일 설치



```
sudo apt install ./google-chrome-stable_current_amd64.deb
```

CentOS 시각화 인터페이스 구축

최종 업데이트 날짜: : 2024-02-02 10:56:29

작업 시나리오

본문은 CentOS 8.2 및 CentOS 7.9 운영 체제의 Tencent Cloud Virtual Machine(CVM)을 예시로, CentOS 시각화 인터페이스를 구축하는 방법을 소개합니다.

관련 설명

성능 및 범용성을 고려하여 Tencent Cloud에서 제공하는 Linux 공용 이미지는 기본적으로 그래픽 모듈을 설치하지 않습니다.

설치 오류로 인해 인스턴스가 정상적으로 실행되지 않을 수 있으므로, [사용자 정의 이미지 생성](#), [스냅샷 생성](#)을 통해 데이터를 백업할 것을 권장합니다.

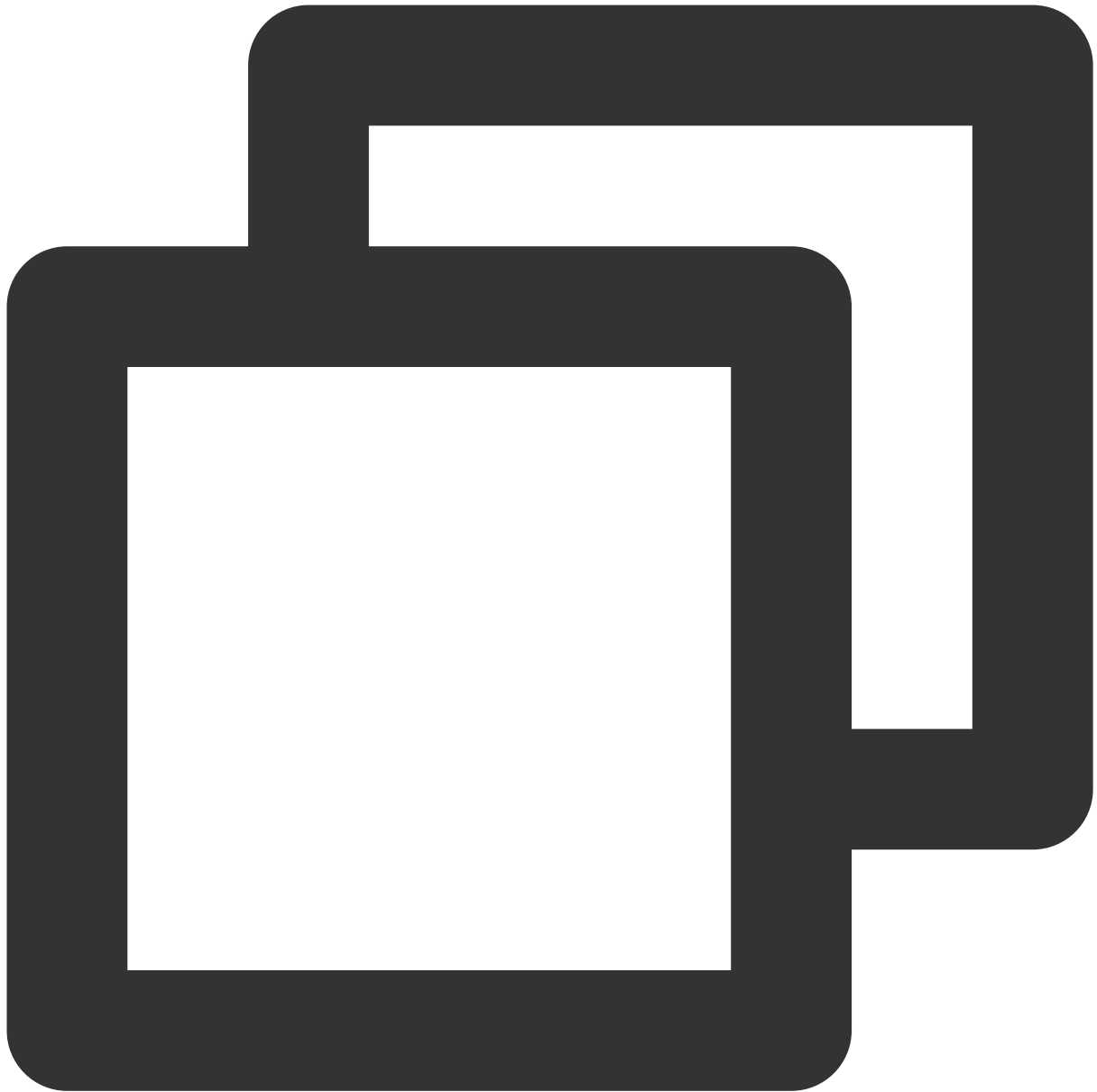
작업 순서

실제로 사용하는 CVM 운영 체제에 따라 다음 단계를 참고하십시오.

CentOS 8.2

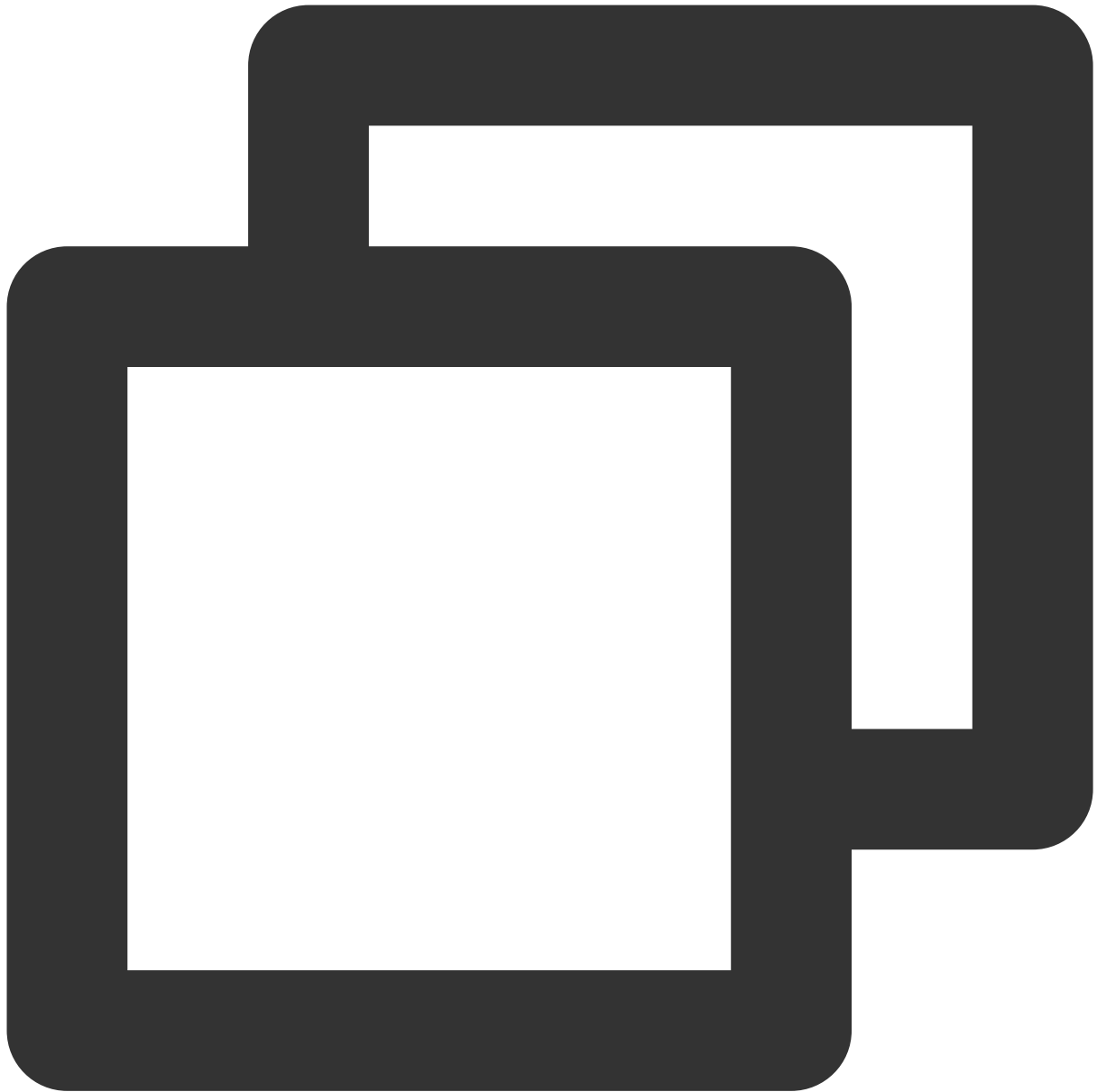
CentOS 7.9

1. 인스턴스에 로그인합니다. 자세한 내용은 [Linux 인스턴스에 로그인](#)을 참고하십시오.
2. 다음 명령을 실행하여 그래픽 인터페이스 모듈을 설치합니다.



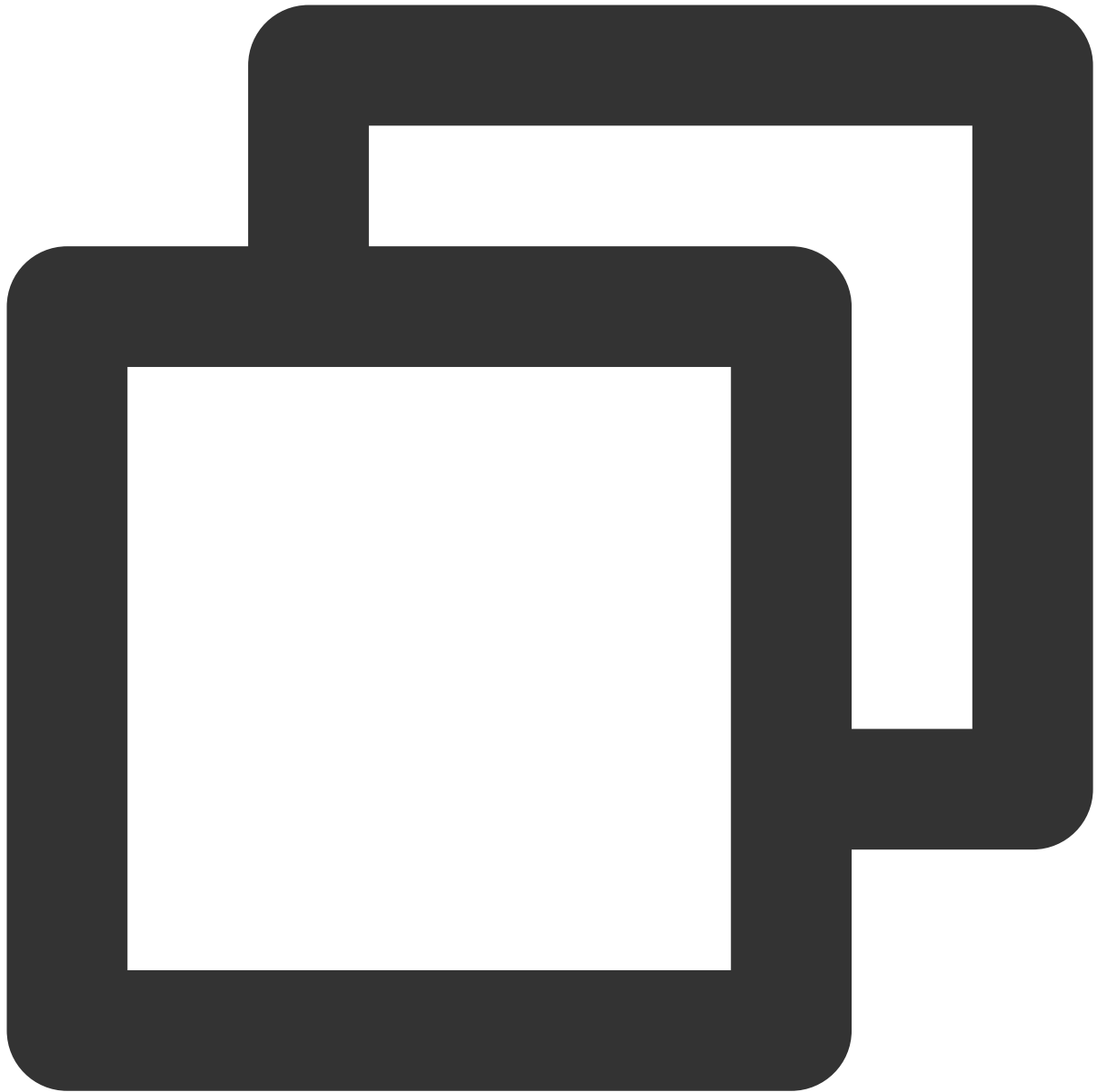
```
yum groupinstall "Server with GUI" -y
```

3. 다음 명령을 실행하여 그래픽 인터페이스 기본 실행을 설정합니다.



```
systemctl set-default graphical
```

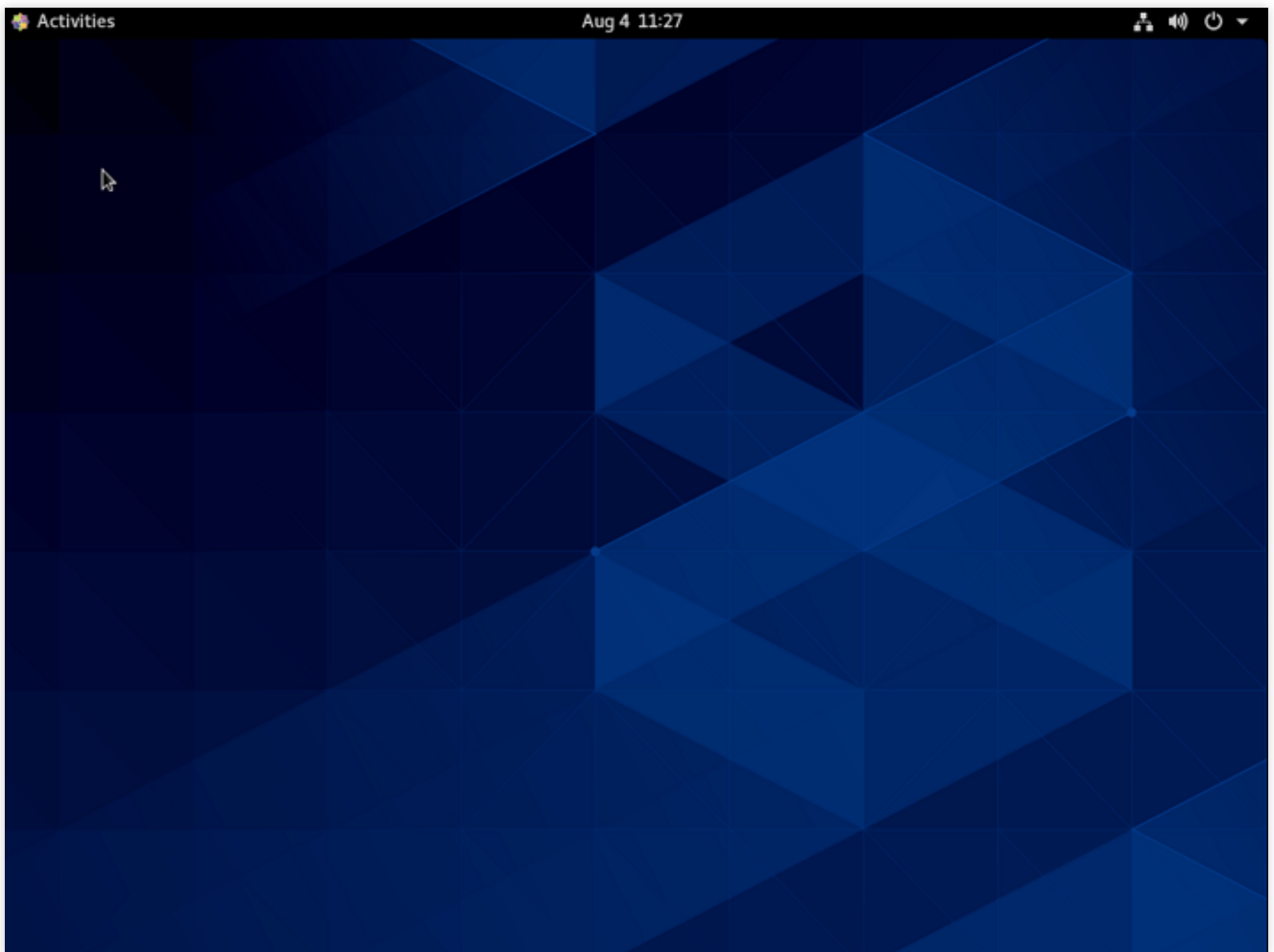
4. 아래의 명령을 실행하여 인스턴스를 재시작합니다.



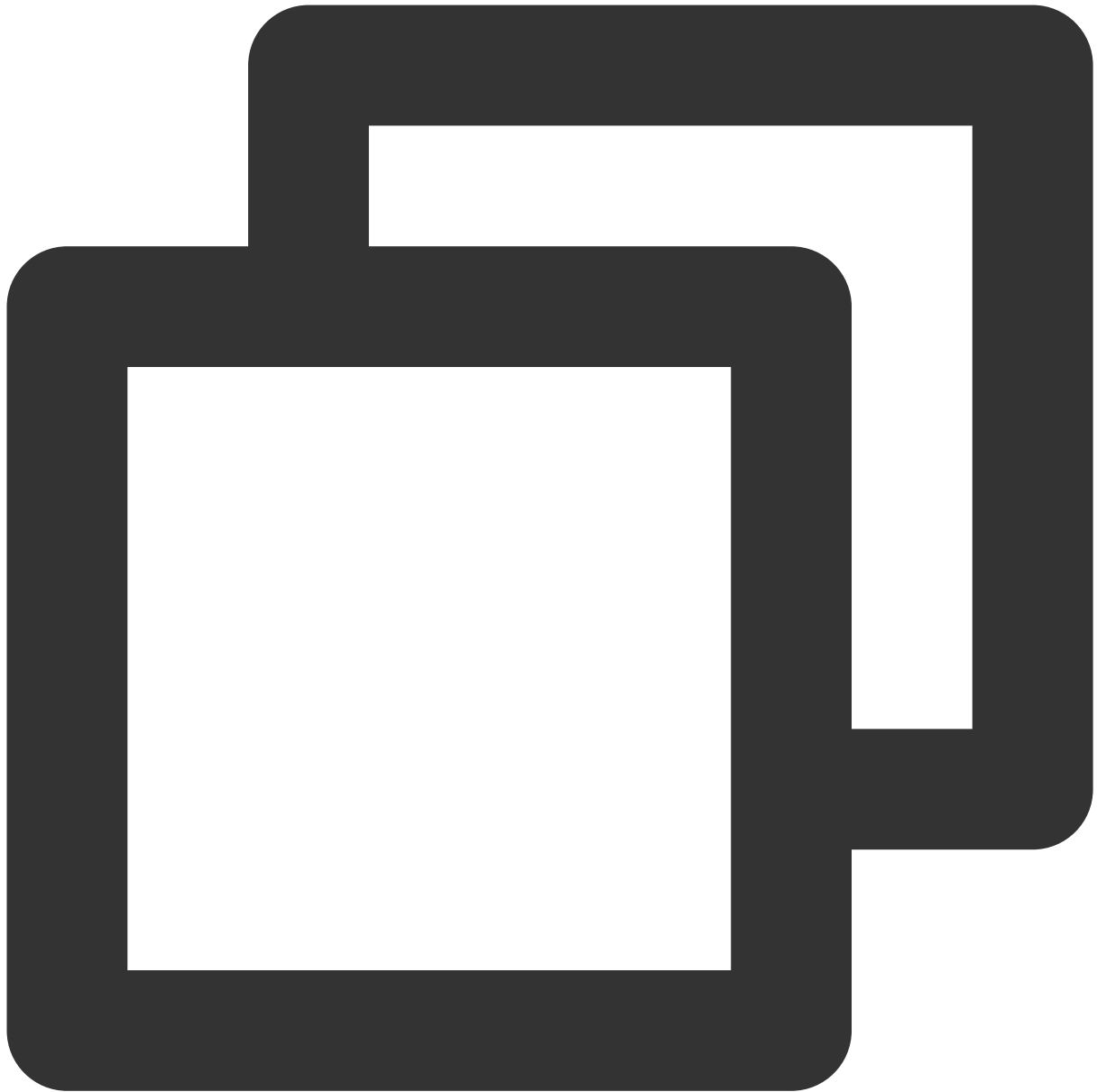
```
reboot
```

5. VNC 방식으로 인스턴스에 로그인합니다. 자세한 내용은 [VNC를 사용하여 Linux 인스턴스에 로그인](#)을 참고하십시오.

인스턴스에 로그인한 후 시각화 인터페이스가 나타나면 구축이 완료된 것입니다. 인터페이스 안내에 따라 구성을 진행하고, 바탕 화면으로 이동하여 필요에 따라 관련 작업을 수행할 수 있습니다. 아래 이미지를 참고하십시오.

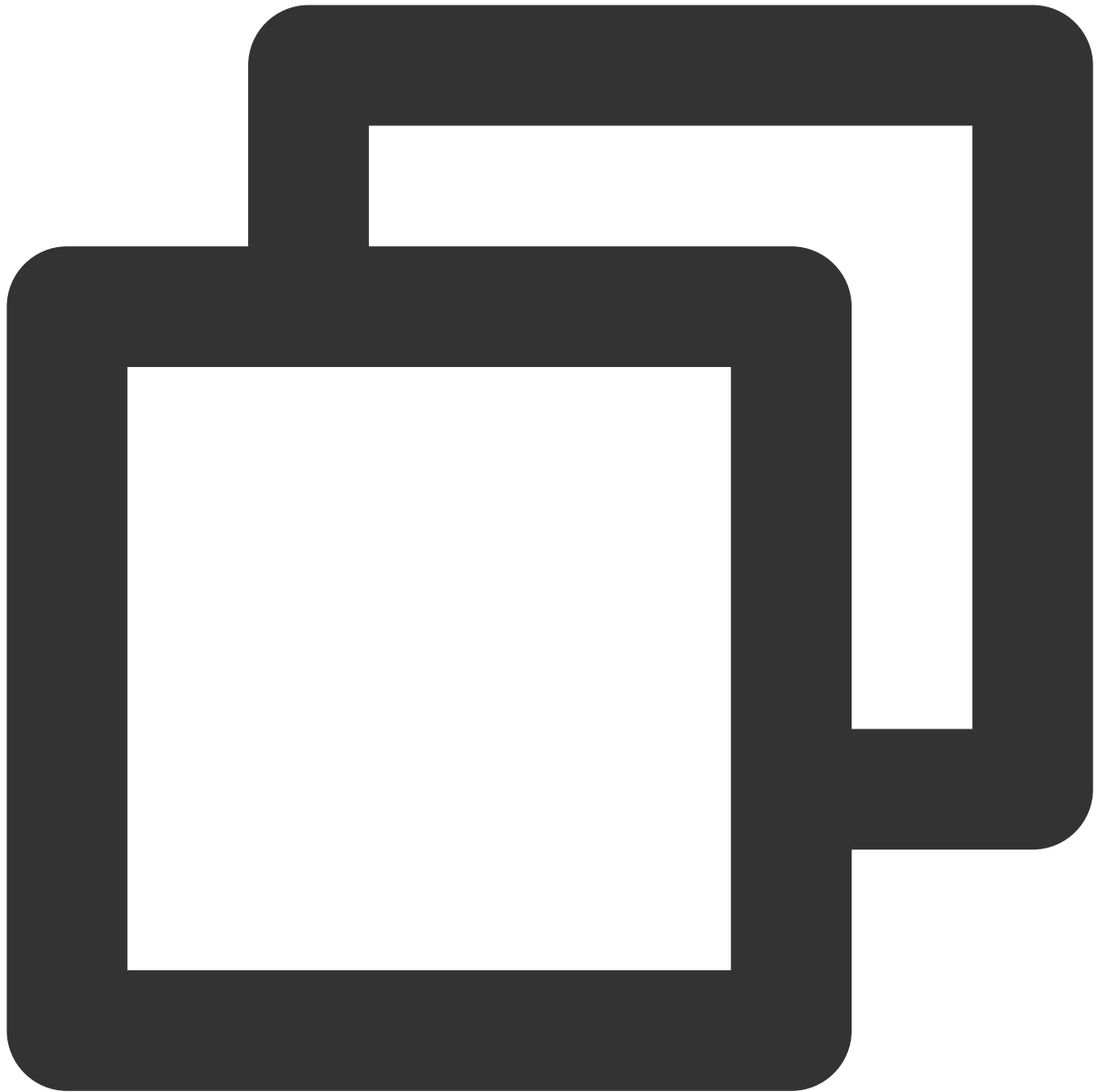


1. 인스턴스에 로그인합니다. 자세한 내용은 [Linux 인스턴스에 로그인](#)을 참고하십시오.
2. 다음 명령을 실행하여 그래픽 인터페이스 모듈을 설치합니다.



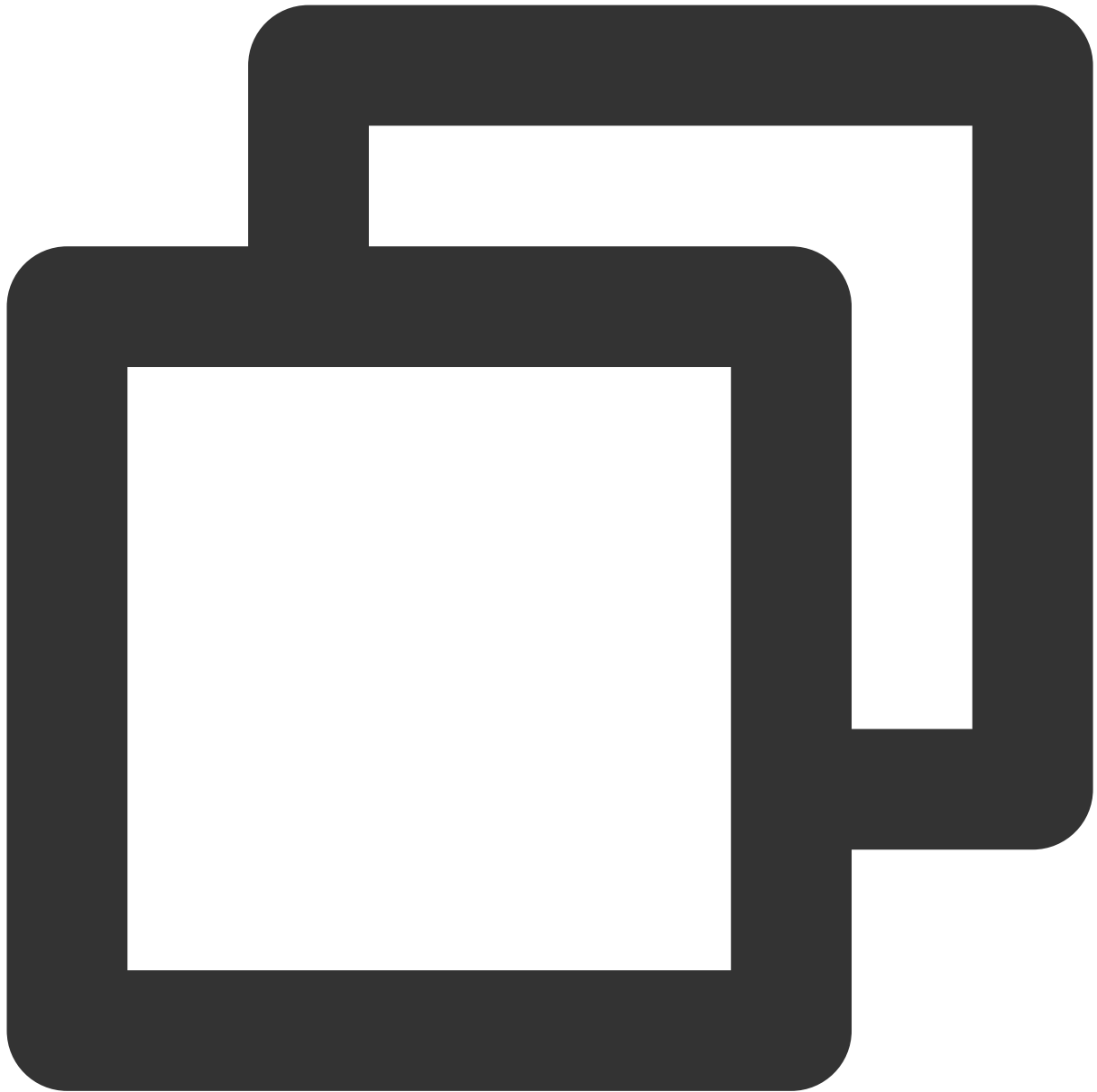
```
yum groupinstall "GNOME Desktop" "Graphical Administration Tools" -y
```

3. 다음 명령을 실행하여 그래픽 인터페이스 기본 실행을 설정합니다.



```
ln -sf /lib/systemd/system/runlevel5.target /etc/systemd/system/default.target
```

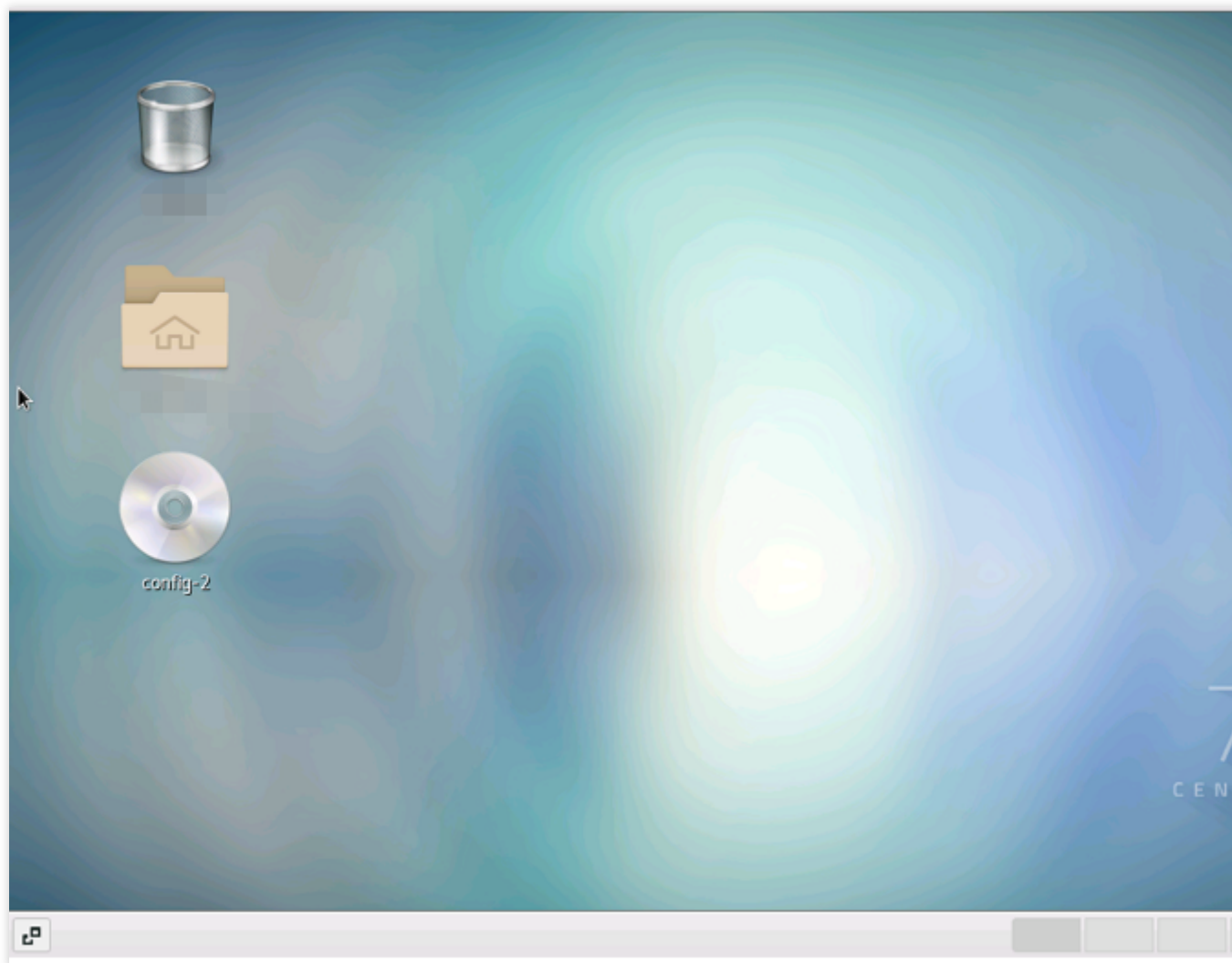
4. 아래의 명령을 실행하여 인스턴스를 재시작합니다.



```
reboot
```

5. VNC 방식으로 인스턴스에 로그인합니다. 자세한 내용은 [VNC를 사용하여 Linux 인스턴스에 로그인](#)을 참고하십시오.

인스턴스에 로그인한 후 시각화 인터페이스가 나타나면 구축이 완료된 것입니다. 인터페이스 안내에 따라 구성을 진행하고, 바탕 화면으로 이동하여 필요에 따라 관련 작업을 수행할 수 있습니다. 아래 이미지를 참고하십시오.



데이터 백업

최종 업데이트 날짜: : 2024-02-02 10:56:28

본 문서는 각종 CVM 관련 데이터 백업 및 보호 솔루션을 소개합니다. 중요한 비즈니스 데이터에 대해서는 적절한 백업 조치를 통한 데이터 보안을 강력히 권장합니다. 참고 문서는 다음과 같습니다.

[데이터 백업 및 복구 솔루션](#)

[시스템 디스크에서 이미지 생성을 통한 데이터 백업](#)

[데이터 디스크에서 스냅샷 생성을 통한 데이터 백업](#)

[중요한 데이터에 대한 정기적인 스냅샷 보호 설정](#)

[스냅샷에서 데이터 롤백](#)

데이터 백업에 문제가 발생한 경우 [데이터 백업 FAQ](#)를 참조하십시오.

CVM에 로컬 파일 업로드

로컬 파일을 CVM에 복사

최종 업데이트 날짜: : 2024-02-02 10:56:28

사용자는 일반적으로 로컬 파일을 저장하기 위해 CVM을 구입합니다. 본 문서는 파일을 CVM에 복사하는 방법을 설명합니다.

아래에서 로컬 컴퓨터의 운영 체제를 찾고 해당 지침을 참고하십시오.

로컬 OS	Linux CVM	Windows CVM
Windows	Windows 시스템에서 WinSCP를 사용하여 Linux CVM에 파일 업로드 Windows 시스템에서 FTP를 사용하여 CVM에 파일 업로드	Windows 시스템에서 MSTSC를 통해 Windows CVM에 파일 업로드
Linux	Linux 또는 MacOS 시스템에서 SCP를 사용하여 Linux CVM에 파일 업로드 Linux 시스템에서 FTP를 사용하여 CVM에 파일 업로드	Linux 시스템에서 RDP를 사용하여 Windows CVM에 파일 업로드
Mac OS		MacOS 시스템에서 MRD를 사용하여 Windows CVM에 파일 업로드

예를 들어 로컬 컴퓨터에서 Windows를 사용하고 Linux CVM이 있는 경우 WinSCP를 사용하여 로컬 컴퓨터에서 Linux CVM으로 파일을 업로드할 수 있습니다.

설명 :
 업로드해야 하는 파일이 36KB 미만이고 텍스트 파일인 경우 파일을 CVM으로 업로드하는 방식으로 콘솔을 통해 파일을 업로드하는 것이 좋습니다.

다음 단계 작업

중요한 데이터의 경우 백업 및 재해 복구를 위해 스냅샷을 만들 수 있습니다. 스냅샷 사용 사례 및 사용 방법에 대한 자세한 내용은 [Snapshot FAQs](#)를 참고하십시오.

문제가 있습니까?

[티켓 제출](#)하여 문의하거나 관련 문서를 사용하여 문제를 해결하십시오.
 다음은 사용자가 CVM을 사용할 때 발생하는 일반적인 문제입니다. 아래의 해당 문서를 참고하여 문제를 찾고 해결

하십시오.

CVM 로그인 비밀번호를 잊어버렸습니까?

[인스턴스 비밀번호 재설정](#)을 참고하십시오.

CVM에 로그인할 수 없습니까?

[Windows 인스턴스 로그인 불가](#) 또는 [Linux 인스턴스에 로그인할 수 없을 경우](#)를 참고하십시오.

Windows 시스템에서 MSTSC를 통해 Windows CVM에 파일 업로드

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

Windows CVM에 파일 업로드 시 일반적으로 MSTSC 원격 데스크톱 연결(Microsoft Terminal Services Client) 방식을 사용합니다. 본 문서에서는 로컬 Windows 컴퓨터에서 원격 데스크톱 연결을 통해 Windows CVM에 파일을 업로드하는 방법을 안내합니다.

전제 조건

Windows CVM이 공용 네트워크에 액세스할 수 있어야 합니다.

작업 단계

설명 :

다음의 작업 순서는 Windows 7 운영 체제를 사용하는 로컬 컴퓨터를 예로 들어 설명합니다. 운영 체제에 따라 세부 작업 순서에 약간의 차이가 있습니다.

공용 IP 획득

CVM 콘솔에 로그인한 후, 인스턴스 리스트 페이지에서 파일을 업로드할 CVM의 공용 IP를 다음 이미지와 같이 기록합니다.

Separate keywords with " ", and separate tags using the Enter key								
☐	ID/Name	Monitoring	Status	Availability Z	Instance Type	Instance Configuration	Primary IPv4	Primary IPv6
☐			Running	Guangzhou Zone 3			(Public) (Private)	-
☐			Running	Guangzhou Zone 3			(Public) (Private)	-

파일 업로드

1. 로컬 컴퓨터에서 단축 키 **Windows + R**을 사용해 '실행' 창을 엽니다.
2. 팝업된 '실행' 창에 **mstsc**를 입력한 후 **확인**을 클릭하여 '원격 데스크톱 연결' 창을 엽니다.
3. '원격 데스크톱 연결' 대화 상자에 CVM 공용 IP 주소를 입력한 후 **옵션**을 클릭합니다.
4. **일반** 탭에 CVM 공용 IP 주소 및 사용자 이름 Administrator를 입력합니다.
5. **로컬 리소스** 탭을 선택한 후 **세부 정보**를 클릭합니다.
6. 아래 이미지와 같이 '로컬 디바이스 및 리소스' 팝업 창에서 **드라이버**를 선택한 후 Windows CVM에 업로드할 파일이 있는 로컬 디스크를 선택한 다음 **확인**을 클릭합니다.
7. 로컬 설정을 마친 후, **연결**을 클릭하여 'Windows 보안' 팝업 창에 인스턴스의 로그인 비밀번호를 입력하여 Windows CVM에 원격 로그인합니다.
8. Windows CVM에서



을(를) 선택합니다. 열린 창에서 **내 PC**를 클릭하면 CVM에 마운트된 로컬 디스크를 확인할 수 있습니다.

9. 더블 클릭하여 마운트된 로컬 디스크를 열고, 복사할 로컬 파일을 Windows CVM의 기타 디스크에 복사해 넣으면 파일 업로드 작업이 완료됩니다.

예: 로컬 디스크(F)의 A 파일을 Windows CVM의 C: 드라이브에 복사합니다.

파일 다운로드

Windows CVM의 파일을 로컬 컴퓨터에 다운로드할 경우, 파일 업로드 작업을 참고할 수 있습니다. 다운로드할 파일을 Windows CVM에서 마운트된 로컬 디스크에 복사해 파일 다운로드 작업을 완료합니다.

MacOS 시스템에서 MRD를 사용하여 Windows CVM에 파일 업로드

최종 업데이트 날짜: : 2024-02-02 10:56:29

작업 시나리오

Microsoft Remote Desktop(이하 MRD)은 Microsoft가 Mac 디바이스용으로 출시한 원격 데스크톱 응용 프로그램입니다. 본 문서에서는 Mac 디바이스에서 MRD를 통해 Windows Server 2012 R2로 빠르게 파일을 업로드할 수 있는 운영 체제인 Cloud Virtual Machine(CVM)에 대해 소개합니다.

전제 조건

로컬 컴퓨터에 MRD가 다운로드 및 설치되어 있어야 합니다. 본 문서에서는 Microsoft Remote Desktop for Mac를 예로 들어 설명합니다. Microsoft는 2017년 Remote Desktop 클라이언트의 다운로드 링크 제공을 중단하였고, 자회사인 HockeyApp에서 Beta 버전을 배포하고 있습니다. [Microsoft Remote Desktop Beta](#)에서 Beta 버전을 다운로드 받으실 수 있습니다.

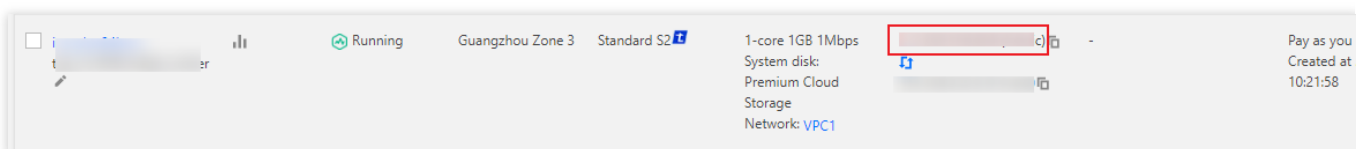
MRD는 Mac OS 10.10 이상의 버전을 지원하므로 지원하는 운영 체제를 사용해 주십시오.

Windows CVM을 구매해야 합니다.

작업 순서

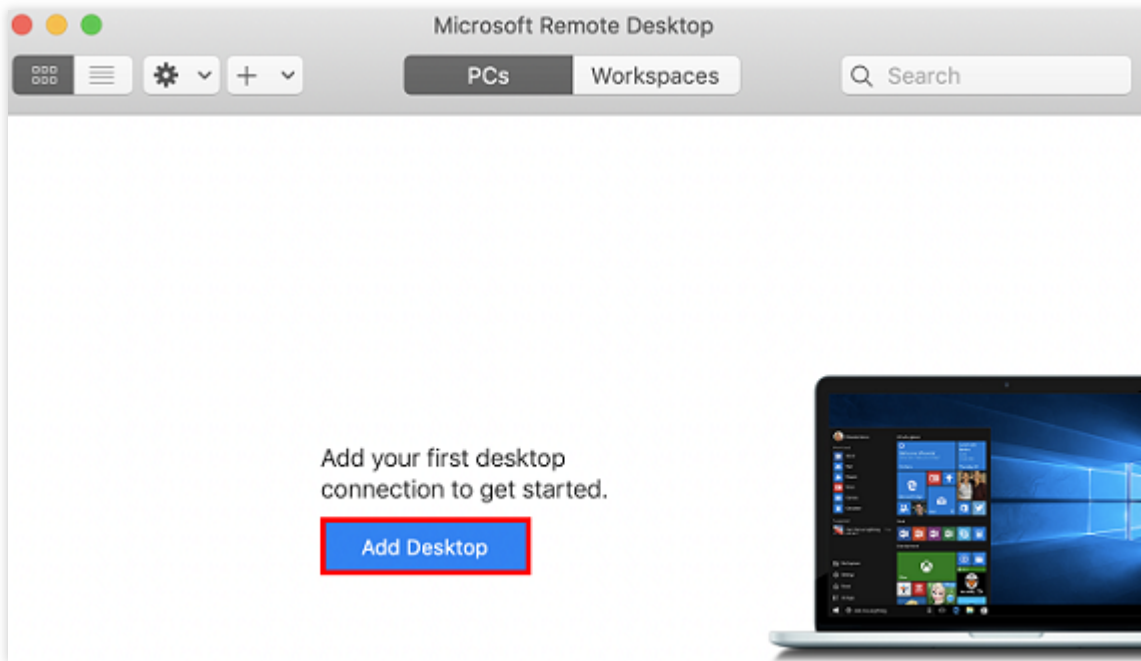
공용 IP 획득

[CVM 콘솔](#)에 로그인한 후, 인스턴스 리스트 페이지에서 파일을 업로드할 CVM의 공용 IP를 다음 이미지와 같이 기록합니다.

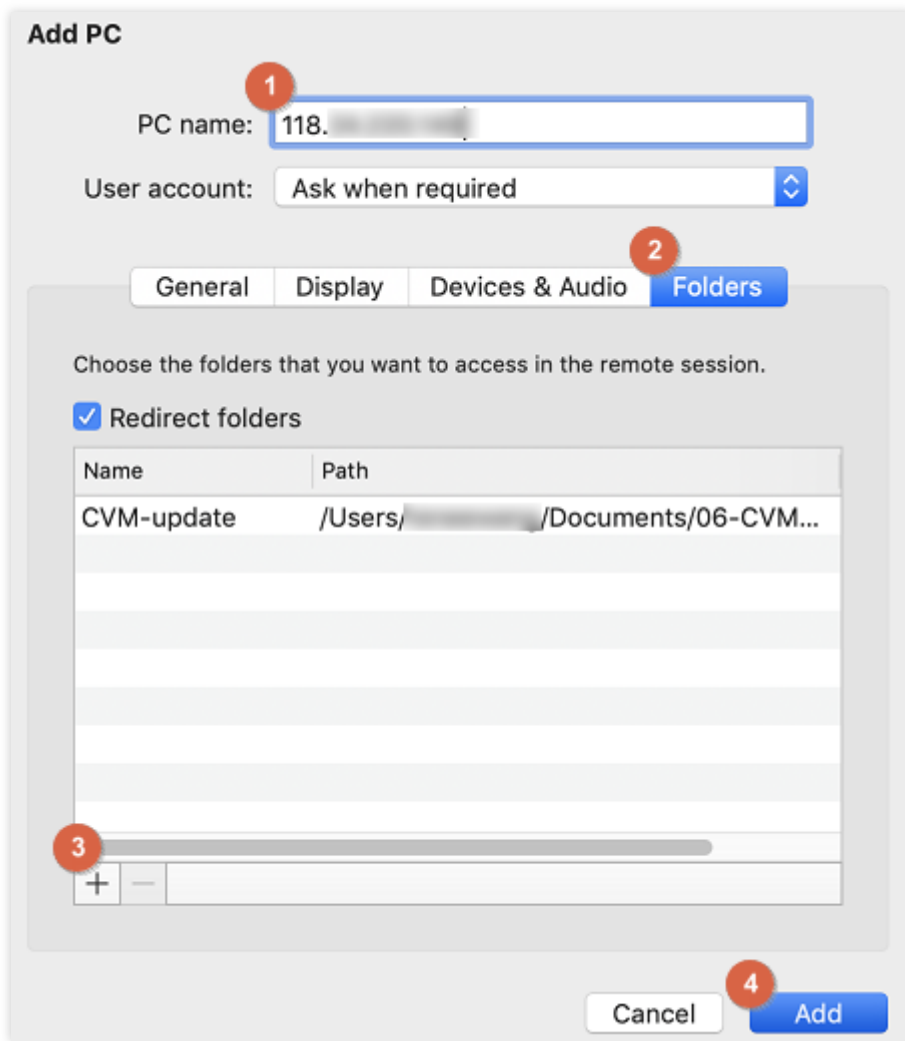


파일 업로드

1. 아래 이미지와 같이 MRD를 실행하고 [Add Desktop]을 클릭합니다.



2. 아래 이미지와 같이 'Add Desktop' 팝업창에서 아래의 순서대로 업로드할 폴더를 선택하고 링크를 생성합니다.



2.1 'PC name'에 획득한 CVM의 공용 IP를 입력합니다.

2.2 **Folders**를 클릭하여 선택한 폴더 리스트로 전환합니다.

2.3 왼쪽 하단의

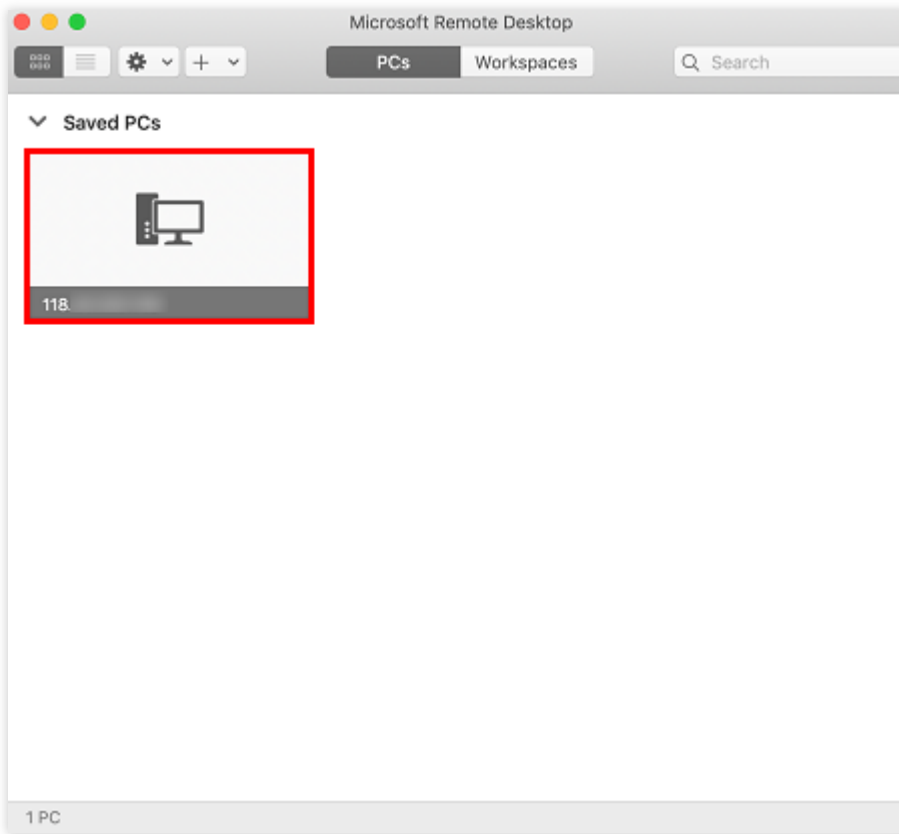


를 클릭하고 팝업창에서 업로드할 폴더를 선택합니다.

2.4 선택 완료 후, 업로드할 폴더 리스트를 조회할 수 있으며, [Add]를 클릭하여 생성을 확인합니다.

2.5 나머지 옵션은 기본 설정을 유지하고 링크 생성을 완료합니다.

생성된 링크는 다음과 같이 창에서 바로 확인할 수 있습니다.



3. 신규 생성한 링크를 더블 클릭하여 열고, 팝업창에서 뜨는 메시지에 따라 CVM 계정 및 비밀번호를 입력 후 **Continue**를 클릭합니다.

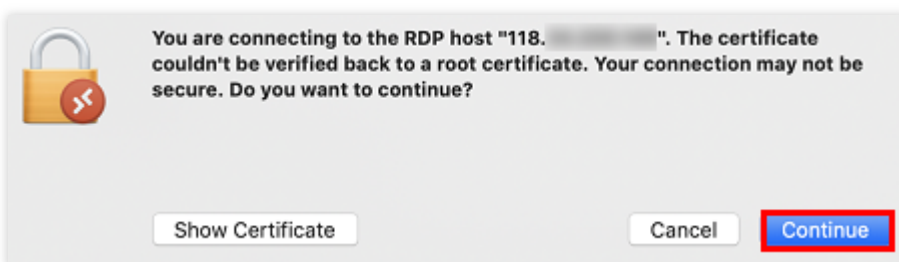
설명 :

CVM 계정은 Administrator 로 기본 설정되어 있습니다.

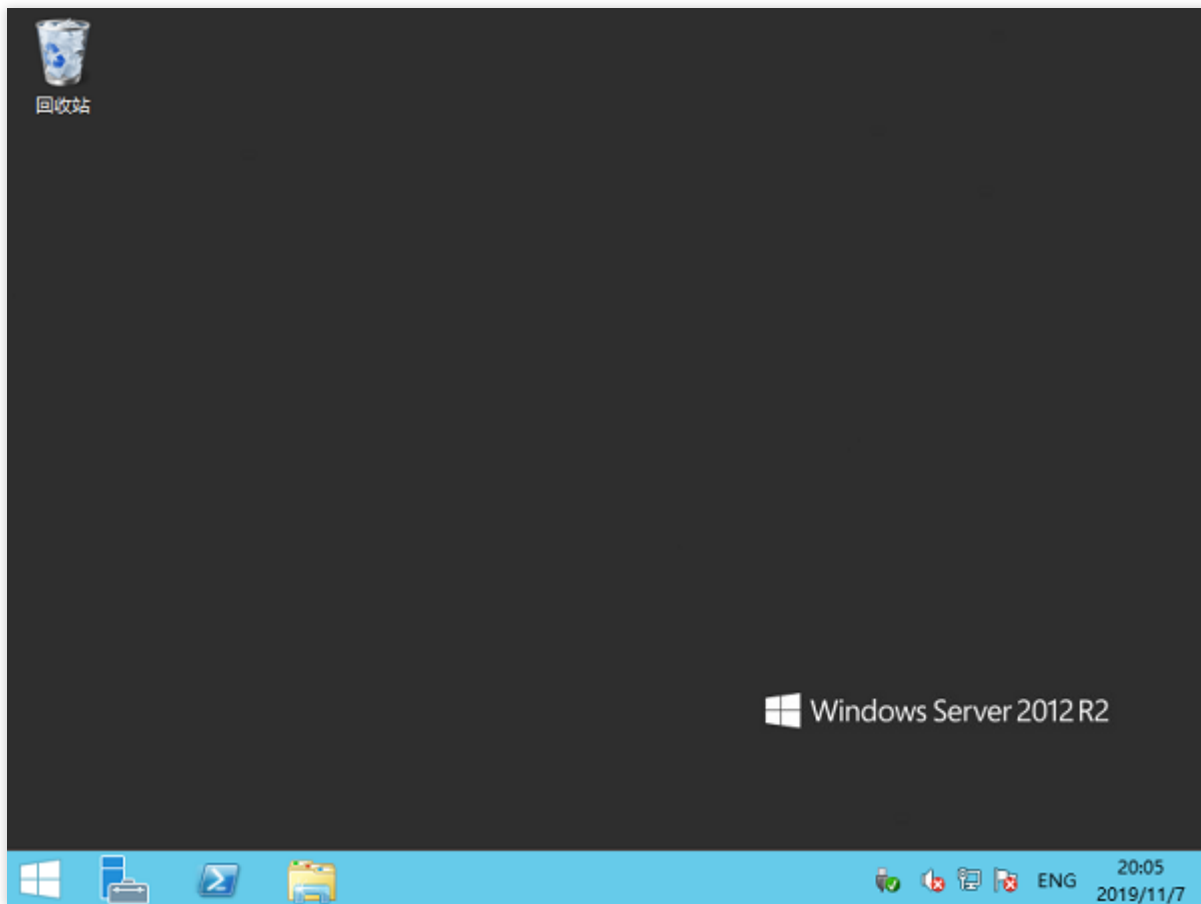
시스템 기본 비밀번호로 인스턴스에 로그인할 경우, 내부 메시지로 이동하여 획득하십시오.

비밀번호를 잊으신 경우, [인스턴스 비밀번호 재설정](#)을 참조하십시오.

4. 아래 이미지와 같이 팝업창에서 [Continue]를 클릭하여 연결합니다.



아래 이미지와 같이 연결 성공 후, Windows CVM 인터페이스가 열립니다.



5. 왼쪽 하단의



>[내 PC]를 클릭하면 공유 중인 폴더를 확인할 수 있습니다.

6. 더블 클릭으로 공유 폴더를 열고, 업로드하려는 로컬 파일을 Windows CVM의 다른 디스크에 복사해 넣으면 파일 업로드가 완료됩니다.

폴더 안의 A 파일을 Windows CVM의 C 드라이브로 복사하는 것을 예로 들 수 있습니다.

파일 다운로드

Windows CVM의 파일을 로컬 컴퓨터로 다운로드하려는 경우, 파일 업로드 작업을 참조하여 필요한 파일을 Windows CVM에서 공유 폴더로 복사해 파일을 다운로드할 수 있습니다.

Linux 시스템에서 RDP를 사용하여 Windows CVM에 파일 업로드

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

Rdesktop은 원격 데스크톱 프로토콜(RDP)의 오픈 소스 클라이언트로 Windows CVM을 연결하는 등의 작업에 사용됩니다. 본 문서는 로컬 Linux 기기에서 rdesktop을 사용하여 Windows Server 2012 R2 운영 체제의 Tencent Cloud Cloud Virtual Machine(CVM)에 빠르게 파일을 업로드하는 방법을 소개합니다.

설명 :

로컬 Linux 기기는 시각화 인터페이스를 구축하지 않으면 rdesktop을 사용할 수 없습니다.

본 문서의 Linux 운영 체제는 CentOS 7.6을 예로 들어 설명하고 있으며 버전 별로 운영 체제 단계가 상이할 수 있으니 실제 서비스 상황에 맞춰 문서를 참고하시기 바랍니다.

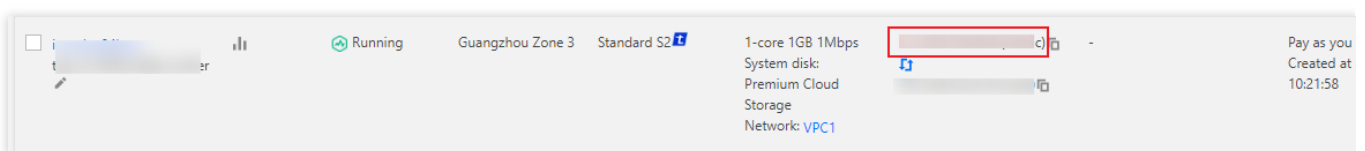
전제 조건

Windows CVM을 구매해야 합니다.

작업 순서

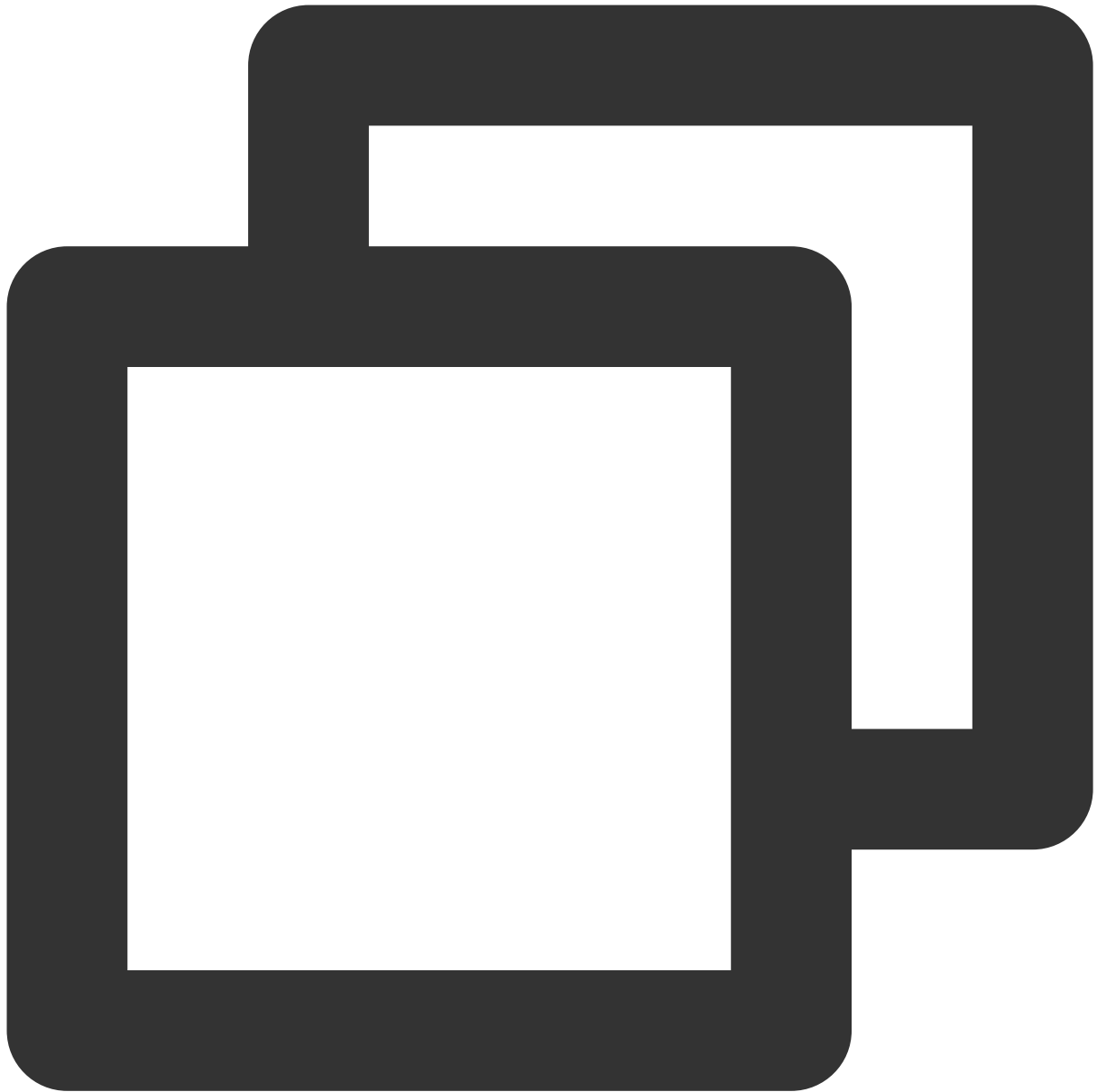
공용 IP 획득

[CVM 콘솔](#)에 로그인한 후, 인스턴스 리스트 페이지에서 파일을 업로드할 CVM의 공용 IP를 다음 이미지와 같이 기록합니다.



rdesktop 설치

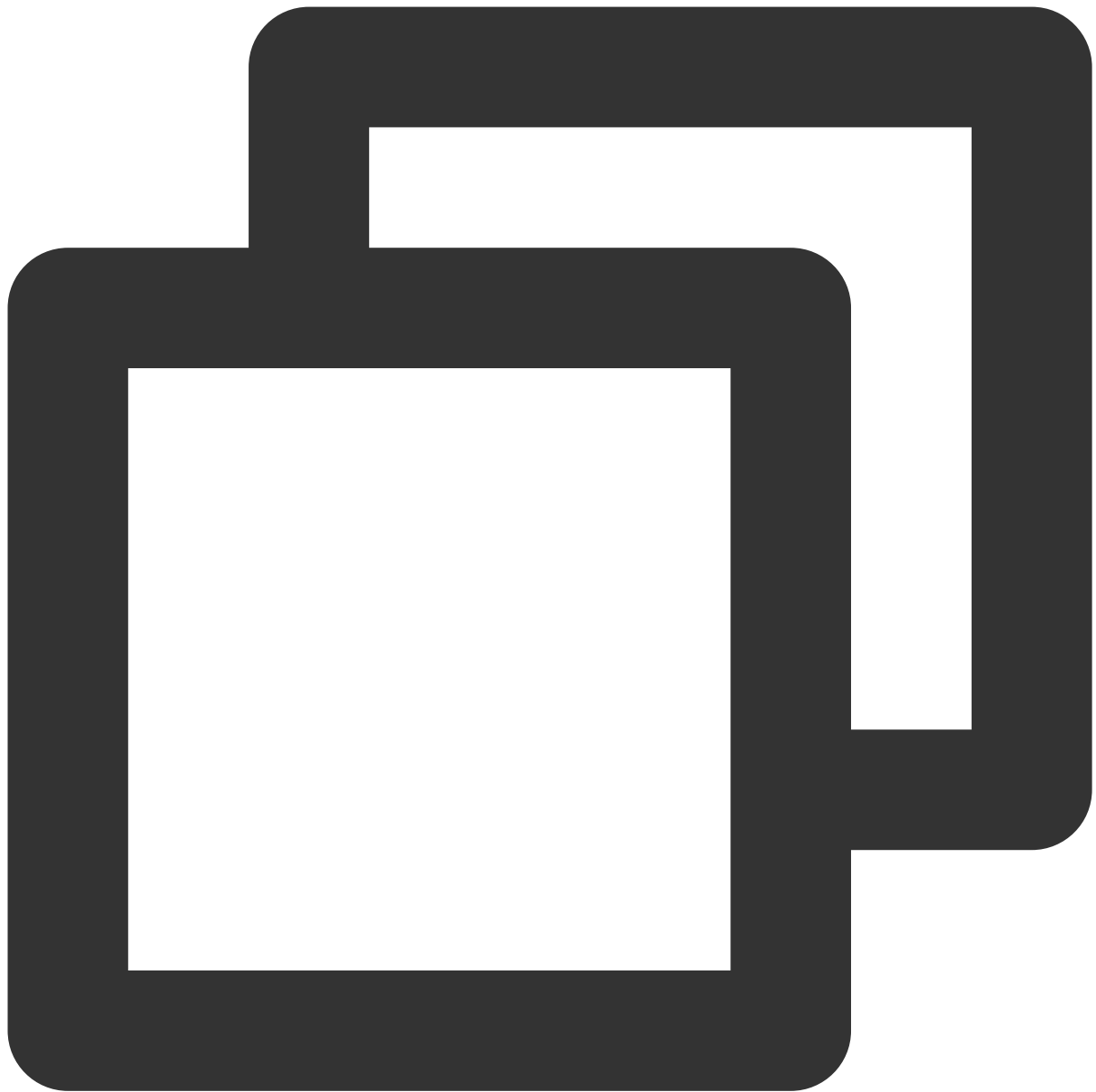
1. 단말기에서 다음 명령어를 실행하여 rdesktop 설치 패키지를 다운로드합니다. 이 단계에서는 rdesktop 1.8.3 버전을 예시로 사용합니다.



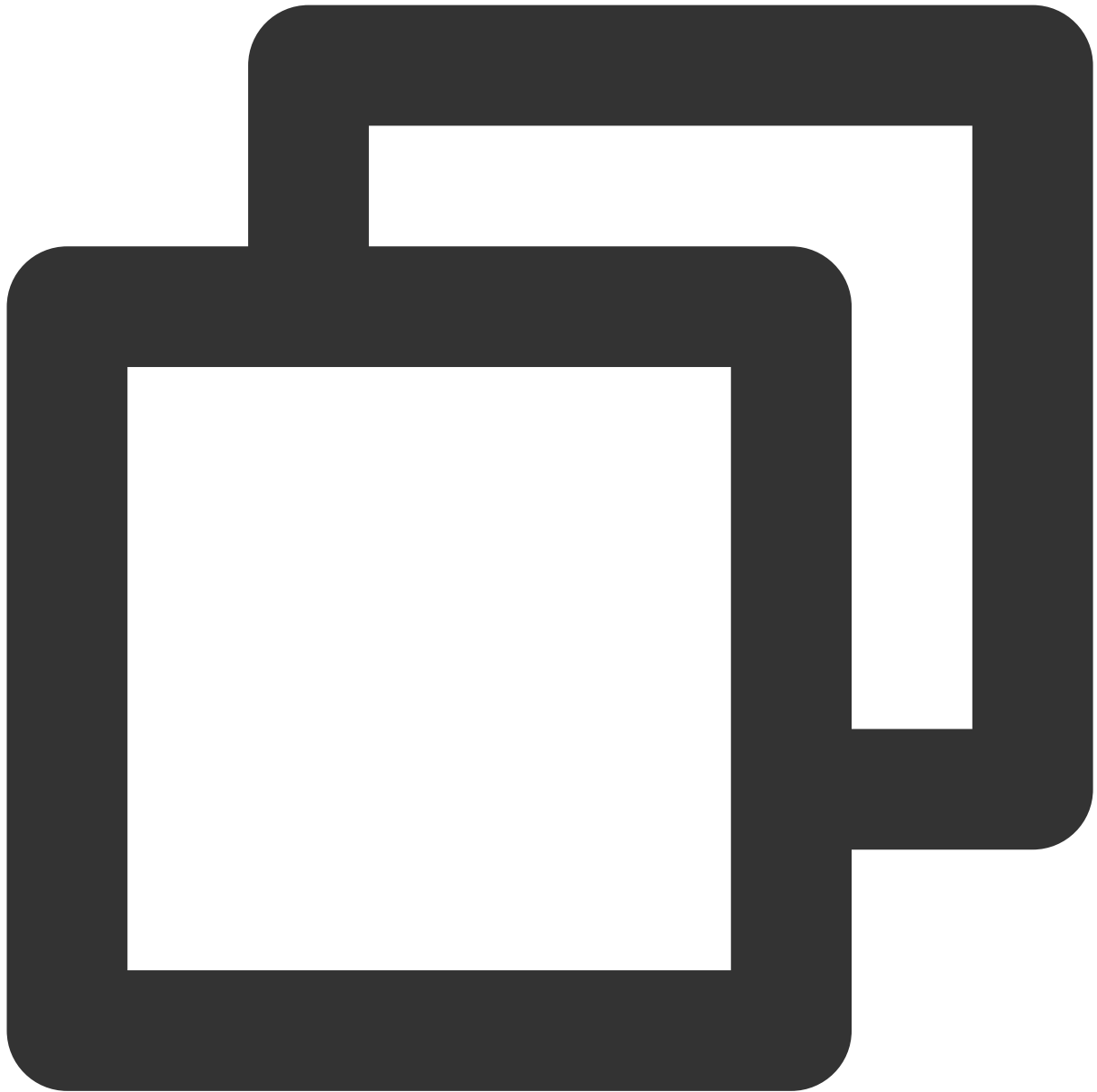
```
wget https://github.com/rdesktop/rdesktop/releases/download/v1.8.3/rdesktop-1.8.3.t
```

최신 설치 패키지가 필요한 경우 [GitHub rdesktop 페이지](#)에서 최신 설치 패키지를 검색하고 명령어 라인에서 최신 설치 경로로 바꿔줍니다.

2. 다음 명령어를 차례로 실행하고 설치 패키지를 압축 해제하여 설치 디렉터리로 들어갑니다.

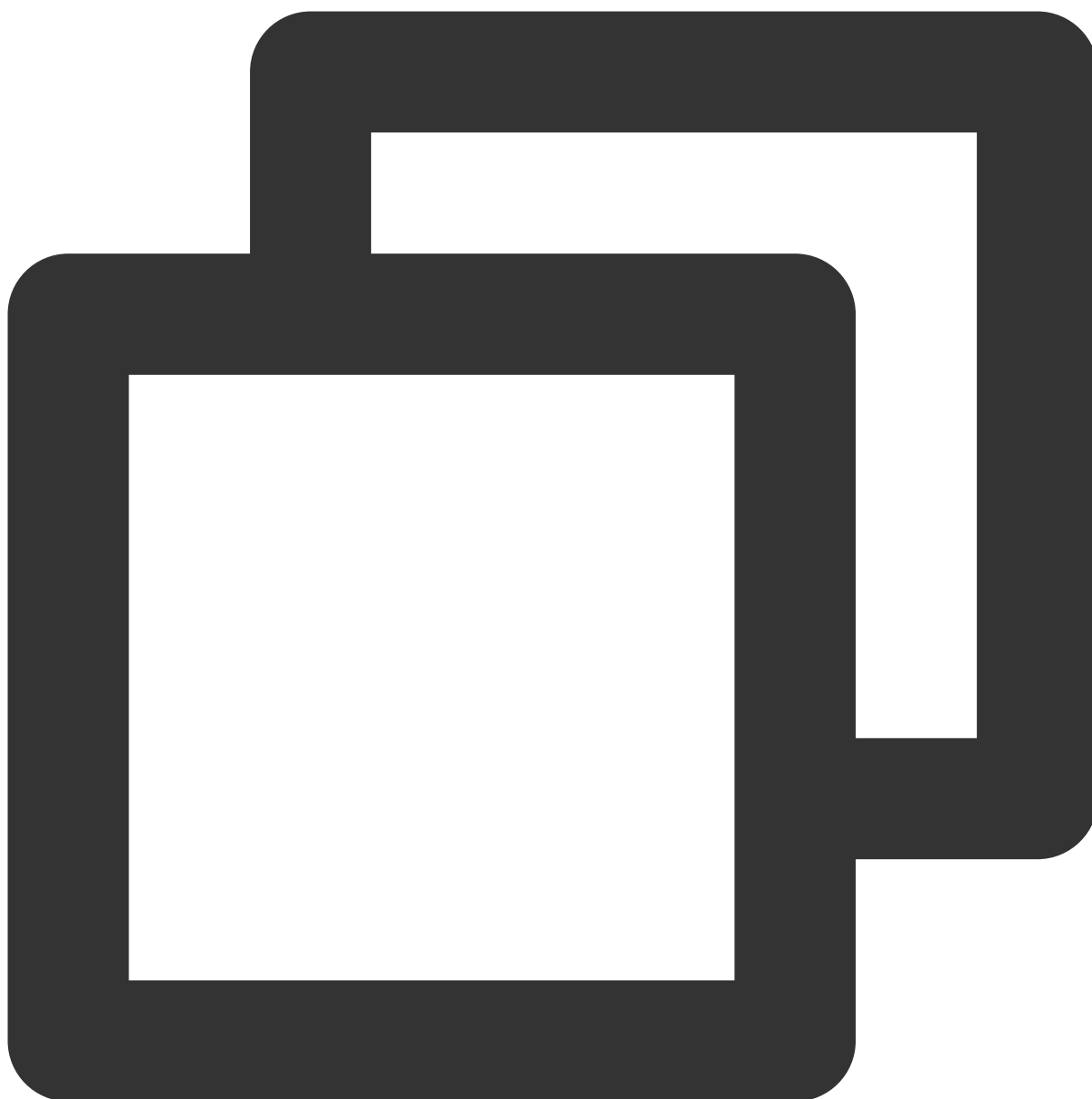


```
tar xvzf rdesktop-1.8.3.tar.gz
```

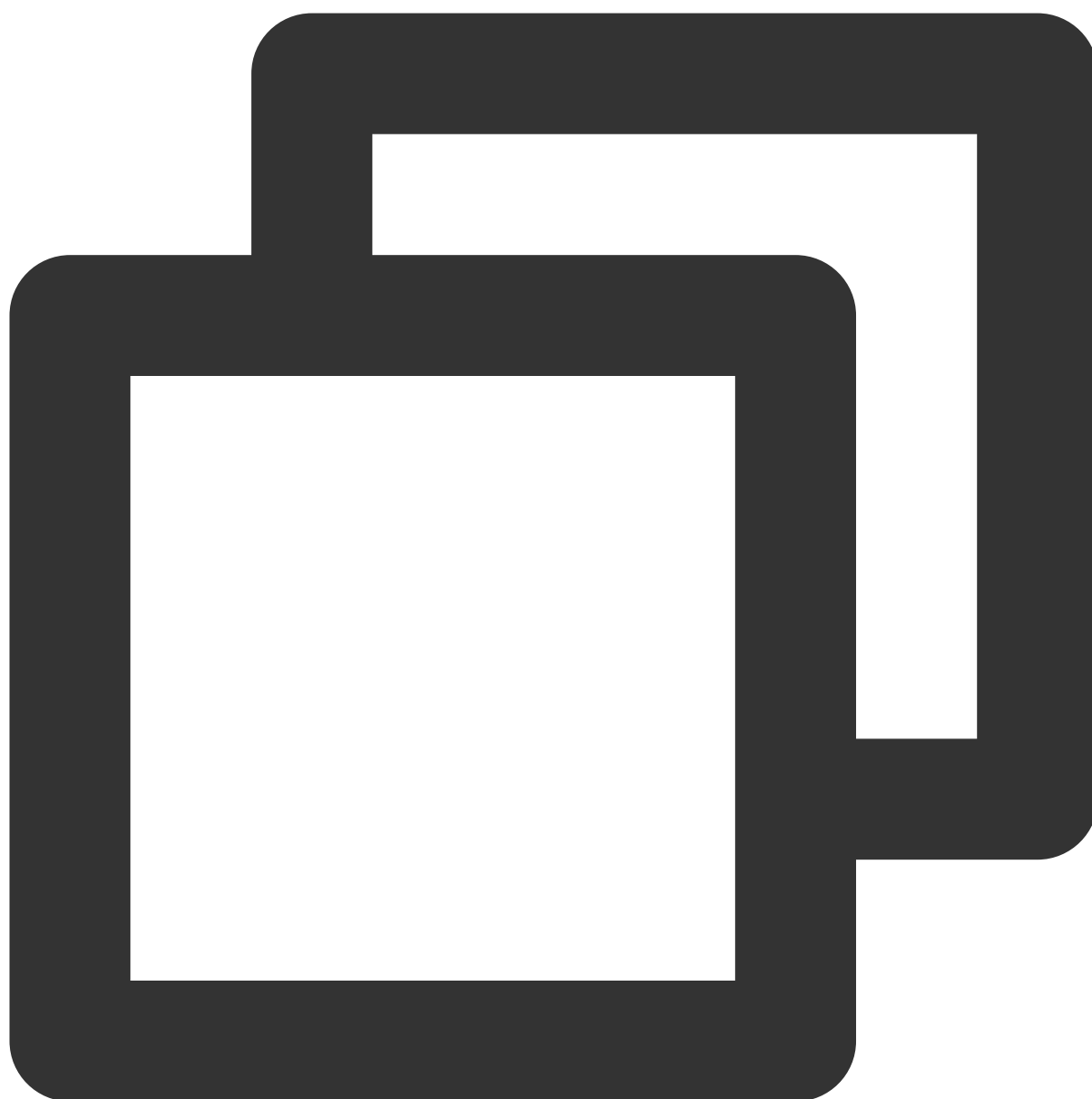


```
cd rdesktop-1.8.3
```

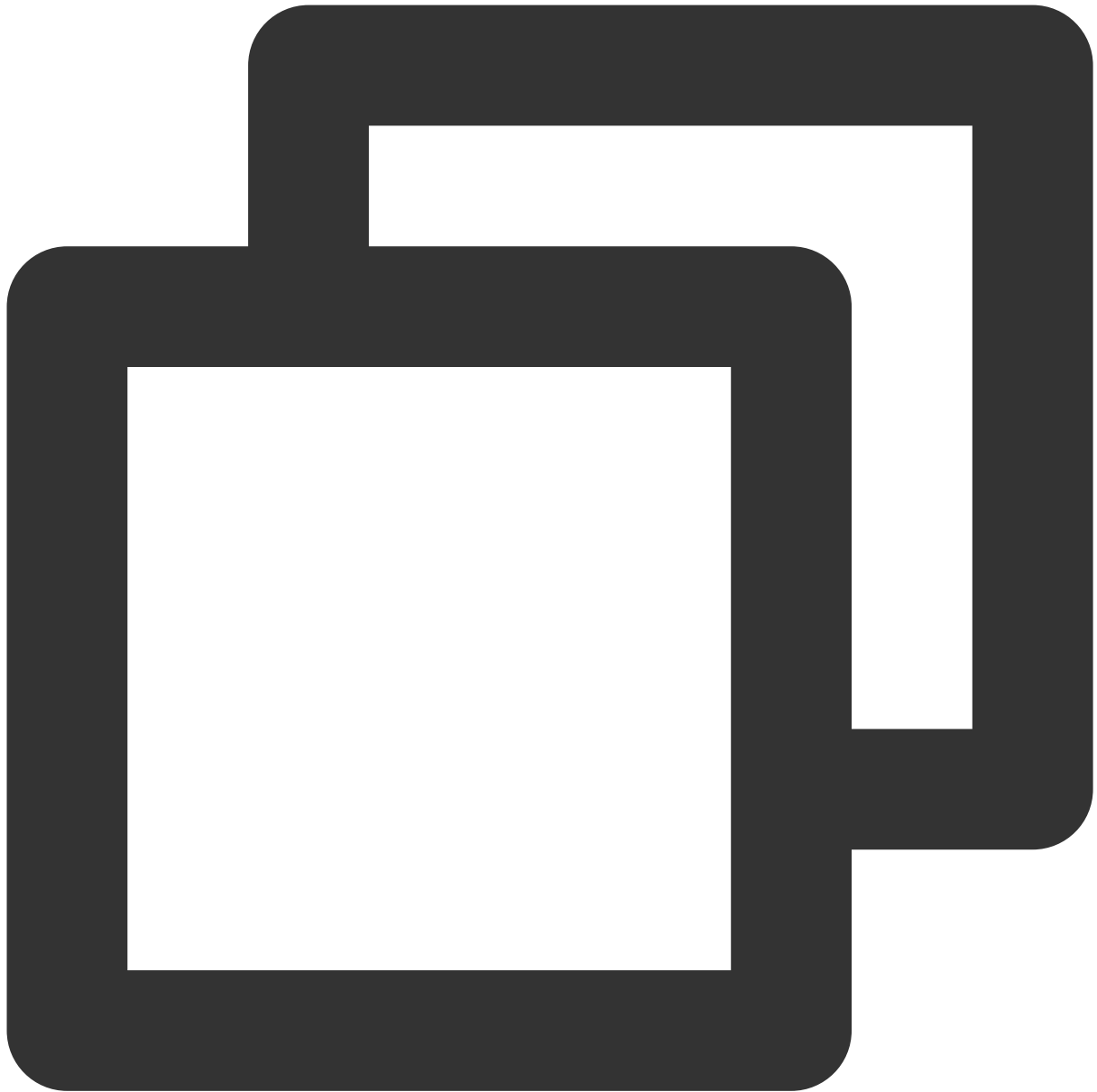
3. 다음 명령어를 차례로 실행하고 rdesktop을 컴파일 설치합니다.



```
./configure
```

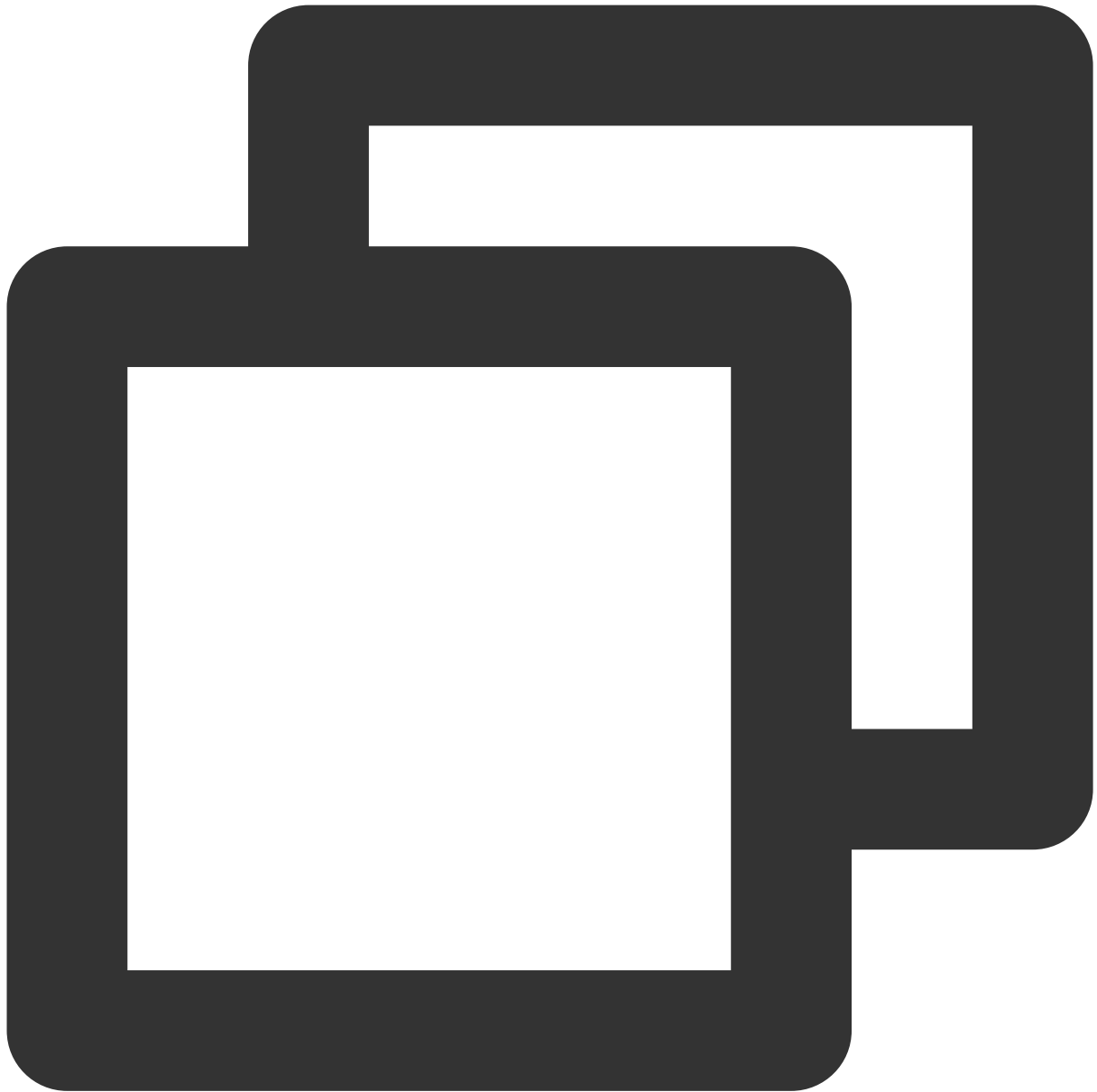


make



```
make install
```

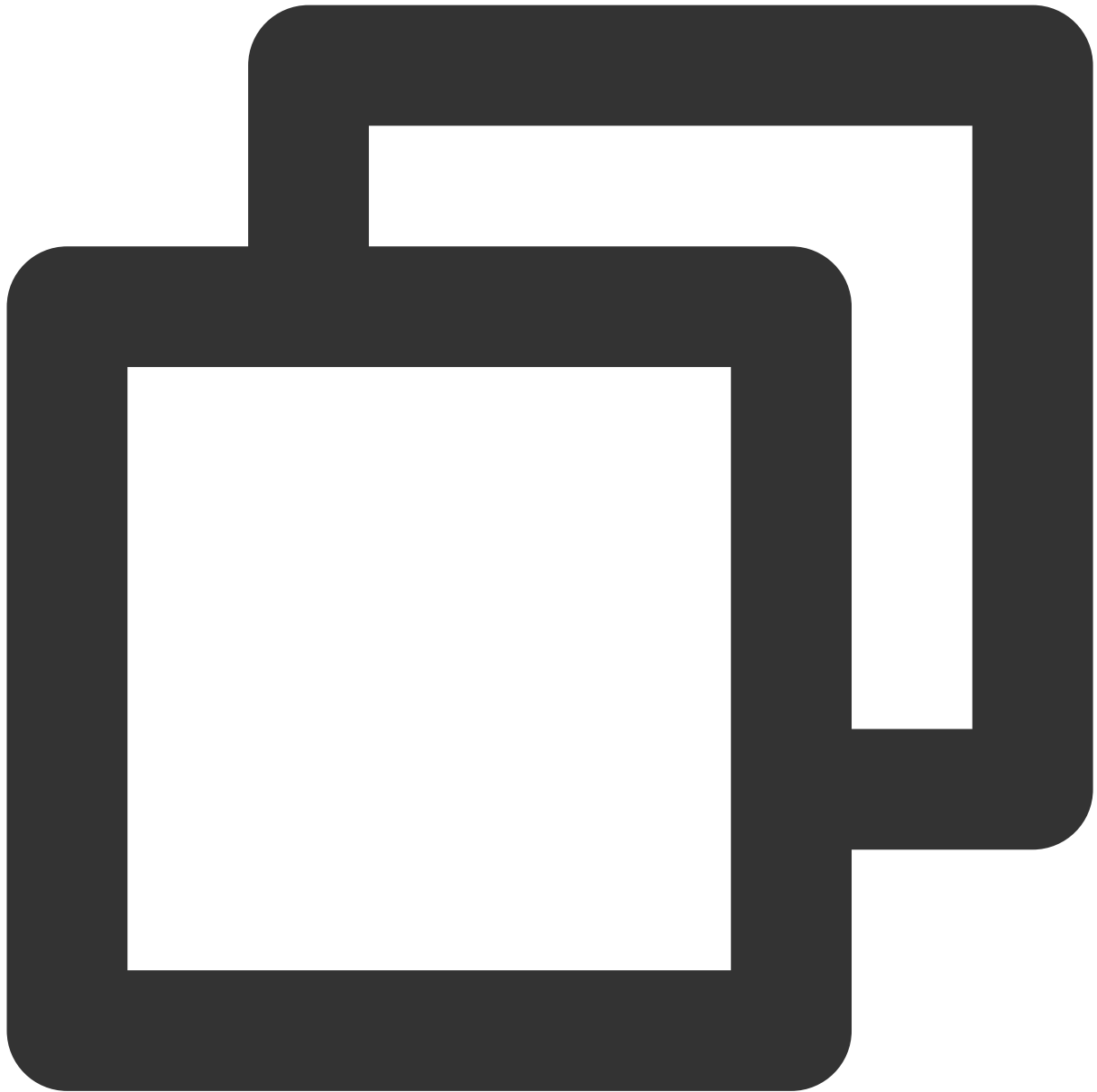
4. 설치가 완료되면 다음 명령어를 실행하여 정상적으로 설치되었는지 확인할 수 있습니다.



```
rdesktop
```

파일 업로드

1. 다음 명령어를 실행하고 CVM에 공유할 폴더를 지정합니다.



```
rdesktop CVM 공인 IP -u CVM 계정 -p CVM 로그인 비밀번호 -r disk: 지정된 공유 폴더 이름=로컬
```

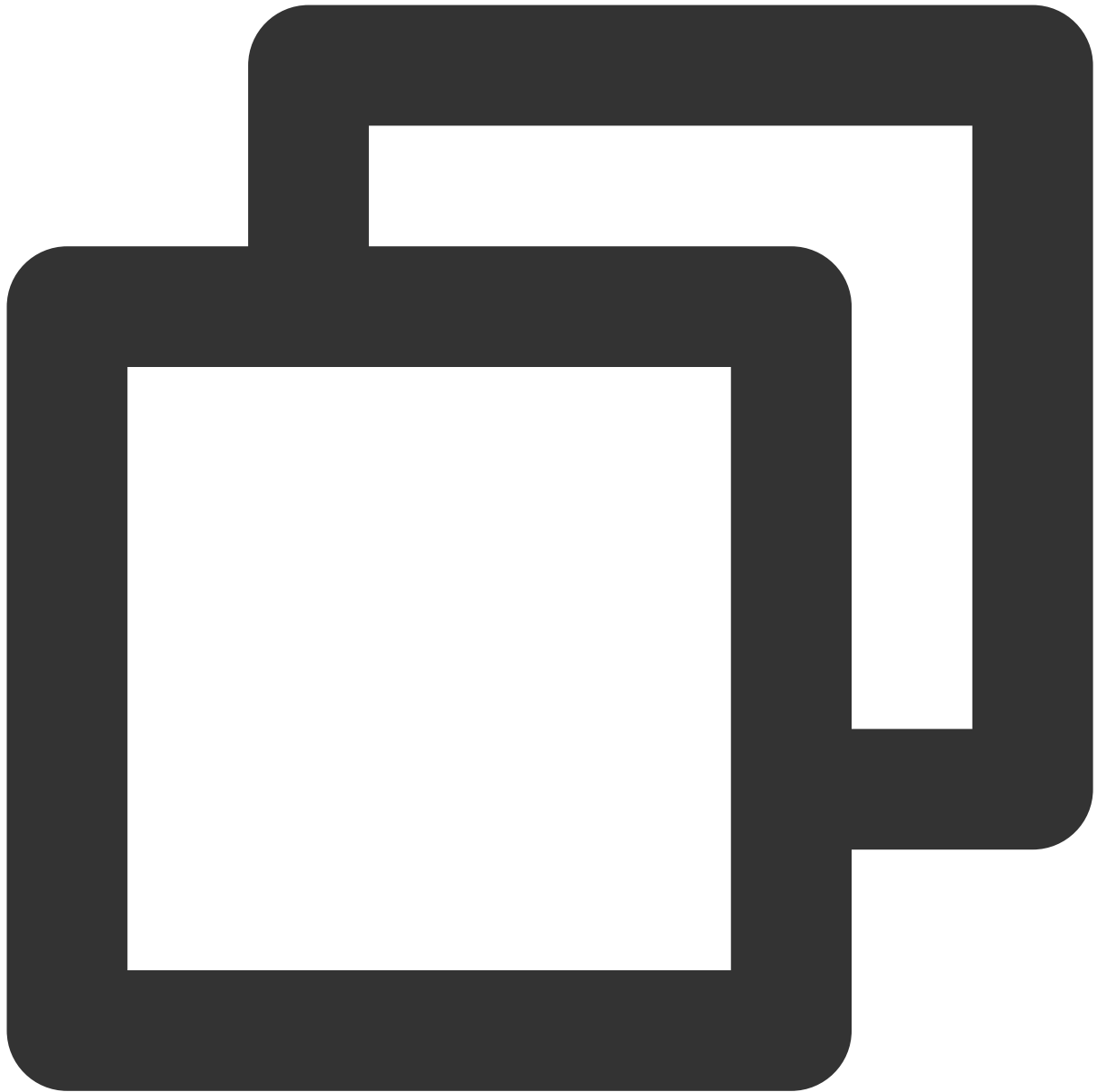
설명 :

CVM 계정은 Administrator 로 기본 설정되어 있습니다.

시스템 기본 설정 비밀번호로 인스턴스에 로그인할 경우, 내부 메시지로 이동하여 획득하십시오.

비밀번호를 잊으신 경우, 인스턴스 비밀번호 리셋을 참고하십시오.

예: 다음 명령어를 실행하여 로컬 컴퓨터의 /home 폴더를 지정된 CVM에 공유하고 공유 폴더 이름을 share 로 변경합니다.



```
rdesktop 118.xx.248.xxx -u Administrator -p 12345678 -r disk:share=/home
```

공유가 완료되면 Windows CVM 인터페이스를 실행합니다.

왼쪽 하단의



> [내 PC]를 클릭하면 CVM 시스템 인터페이스에서 공유 중인 폴더를 확인할 수 있습니다.

2. 더블 클릭으로 공유 폴더를 열고, 업로드하려는 로컬 파일을 Windows CVM의 다른 디스크에 복사해 넣으면 파일 업로드가 완료됩니다.

예: `share` 폴더 안의 A 파일을 Windows CVM의 C: 드라이브로 복사합니다.

파일 다운로드

Windows CVM의 파일을 로컬 컴퓨터로 다운로드하려는 경우, 파일 업로드 작업을 참고하여 필요한 파일을 Windows CVM에서 공유 폴더로 복사해 파일을 다운로드할 수 있습니다.

Windows 시스템에서 WinSCP를 사용하여 Linux CVM에 파일 업로드

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

WinSCP는 Windows 환경에서 SSH의 오픈 소스 그래픽을 사용하는 SFTP 클라이언트이며, 동시에 SCP 프로토콜을 지원합니다. 주요 기능은 로컬 컴퓨터와 원격 컴퓨터 사이에서 안전하게 파일을 복사하는 것입니다. FTP를 사용해 코드를 업로드하는 것과 비교해, WinSCP를 사용할 경우 서버 코드의 어떠한 구성도 없이 서버 계정 비밀번호를 사용해 서버에 직접 액세스할 수 있습니다.

전제 조건

로컬 컴퓨터에 WinSCP 클라이언트를 다운로드 후 설치되어 있어야 합니다(가져오기 경로: [공식 홈페이지](#)에서 최신 버전을 가져오기를 권장합니다).

작업 단계

WinSCP에 로그인

1. WinSCP를 열면, "WinSCP 로그인" 대화 상자가 나타납니다.
2. 로그인 파라미터를 설정하십시오.

프로토콜: SFTP 혹은 SCP를 입력합니다.

호스트 이름: 클라우드 서버의 공용 네트워크 IP. [클라우드 서버 콘솔](#)에 로그인하여 해당 클라우드 서버의 공용 네트워크 IP를 조회하십시오.

포트: 기본값은 22입니다.

사용자 이름: CVM에 로그인하는 사용자 이름입니다.

설명 :

기본 관리자 사용자 이름은 Linux 인스턴스의 경우 root이고 Ubuntu 시스템 인스턴스의 경우 ubuntu입니다. Ubuntu 운영 체제를 사용하는 경우 [Ubuntu 시스템에서 root 사용자로 인스턴스에 로그인하는 방법](#)을 참고하십시오. 설정 후 root로 로그인합니다.

비밀번호: 해당 사용자 이름의 비밀번호입니다.

시스템 기본 설정 비밀번호로 인스턴스에 로그인할 경우 [내부 메시지](#)에 접속하여 획득 바랍니다.

비밀번호를 잊으신 경우, [인스턴스 비밀번호 재설정](#)하시기 바랍니다.

3. **로그인**을 클릭하여 "WinSCP" 파일 전송 인터페이스로 이동합니다.

파일 업로드

1. **WinSCP** 파일 전송 인터페이스의 오른쪽 탭에서 파일이 서버에서 저장될 디렉터리를 선택하십시오. 예:

`/user` .

2. **WinSCP** 파일 전송 인터페이스의 왼쪽 탭에서 `F:\SSL 인증서\Nginx` 와 같은 로컬 컴퓨터 파일이 저장된 디렉터리를 선택한 뒤 전송할 파일을 선택하십시오.

3. **WinSCP** 파일 전송 인터페이스의 왼쪽 사이드바에서 **업로드**를 클릭합니다.

4. **업로드** 팝업창에서 업로드해야 할 파일과 원격 디렉터리를 확인한 뒤, **확인**을 클릭하여 로컬 컴퓨터의 파일을 클라우드 서버로 업로드합니다.

파일 다운로드

1. **WinSCP** 파일 전송 인터페이스의 왼쪽 탭에서 "F:\SSL 인증서\Nginx"와 같은 로컬 컴퓨터에 다운로드할 저장 디렉터리를 선택합니다.

2. **WinSCP** 파일 전송 인터페이스의 오른쪽 탭에서 `/user` 와 같이, 서버가 파일을 저장할 디렉터리를 선택하고 전송할 파일을 선택합니다.

3. **WinSCP** 파일 전송 인터페이스의 오른쪽 사이드바에서 **다운로드**를 클릭합니다.

4. **다운로드** 창에서 다운로드해야 하는 파일 및 원격 디렉터리를 확인한 뒤, **확인**을 클릭하여 클라우드 서버의 파일을 로컬 컴퓨터로 다운로드하십시오.

Linux 또는 MacOS 시스템에서 SCP를 사용하여 Linux CVM에 파일 업로드

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

본 문서에서는 CentOS 8.2 OS를 적용한 Tencent Cloud Cloud Virtual Machine(CVM)을 예로 들어 SCP를 통해 Linux CVM으로 파일을 업로드 또는 다운로드 하는 방법에 대해 소개합니다.

전제 조건

구매한 Linux CVM이 있어야 합니다.

작업 순서

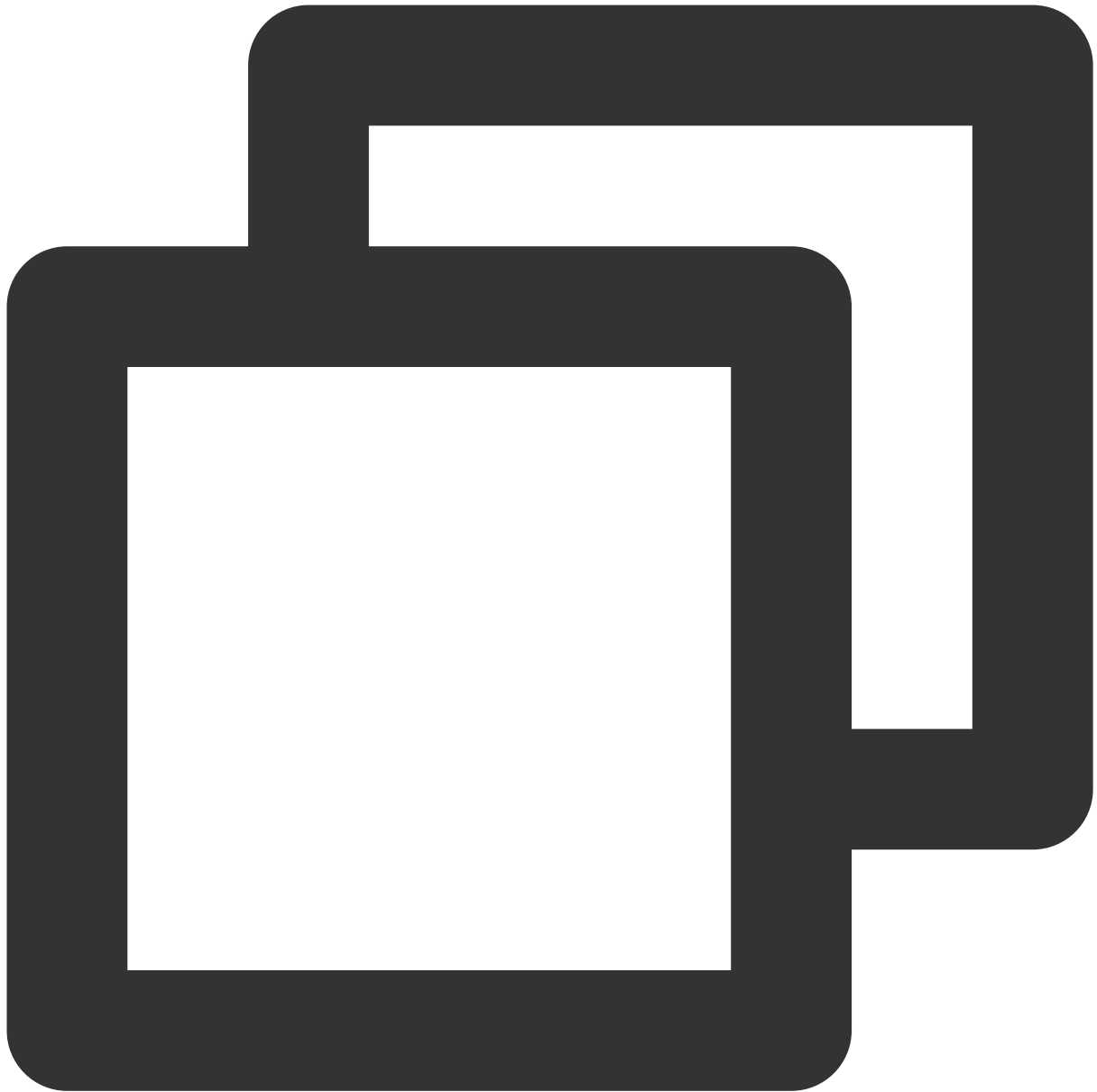
공용 IP 획득

[CVM 콘솔](#)에 로그인한 후, 인스턴스 리스트 페이지에서 파일을 업로드할 CVM의 공용 IP를 다음 이미지와 같이 기록합니다.

ID/Name	Monitoring	Status	Availability Zone	Instance Type	Instance Configuration	Primary IPv4	Primary IPv6	Instance Billing
 New		Running	Nanjing Zone 1	Standard S5	1-core 1GB 1Mbps System disk: Premium Cloud Storage Network: Default-VPC	 (Public) 	-	Pay as you go Created at 2024-02-02 10:23:04

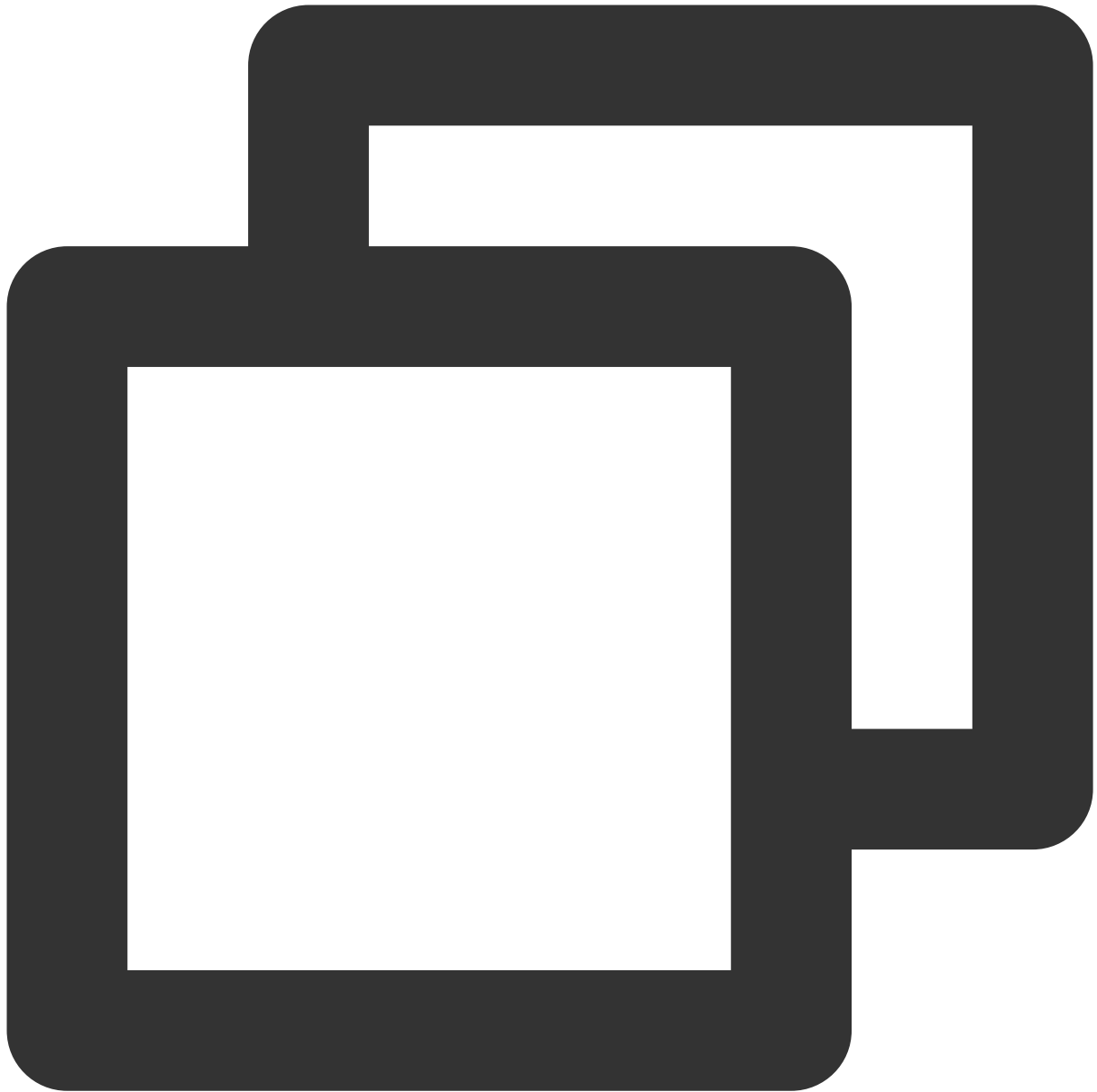
파일 업로드

1. 다음 명령어를 실행하여 Linux CVM에 파일을 업로드합니다.



scp 로컬 파일 주소 CVM 계정@CVM 공용 IP/도메인: CVM 파일 주소

예를 들어, 로컬 파일 `/home/lnmp0.4.tar.gz` 를 IP 주소가 '129.20.0.2'인 CVM 디렉터리에 업로드해야 할 경우, 다음과 같은 명령어를 실행합니다.



```
scp /home/Inmp0.4.tar.gz root@129.20.0.2:/home/Inmp0.4.tar.gz
```

설명 :

'-r' 매개변수를 추가하여 파일을 업로드할 수 있습니다. 더 많은 scp 명령 기능을 보려면 `man scp` 를 실행하여 더 많은 정보를 확인하십시오.

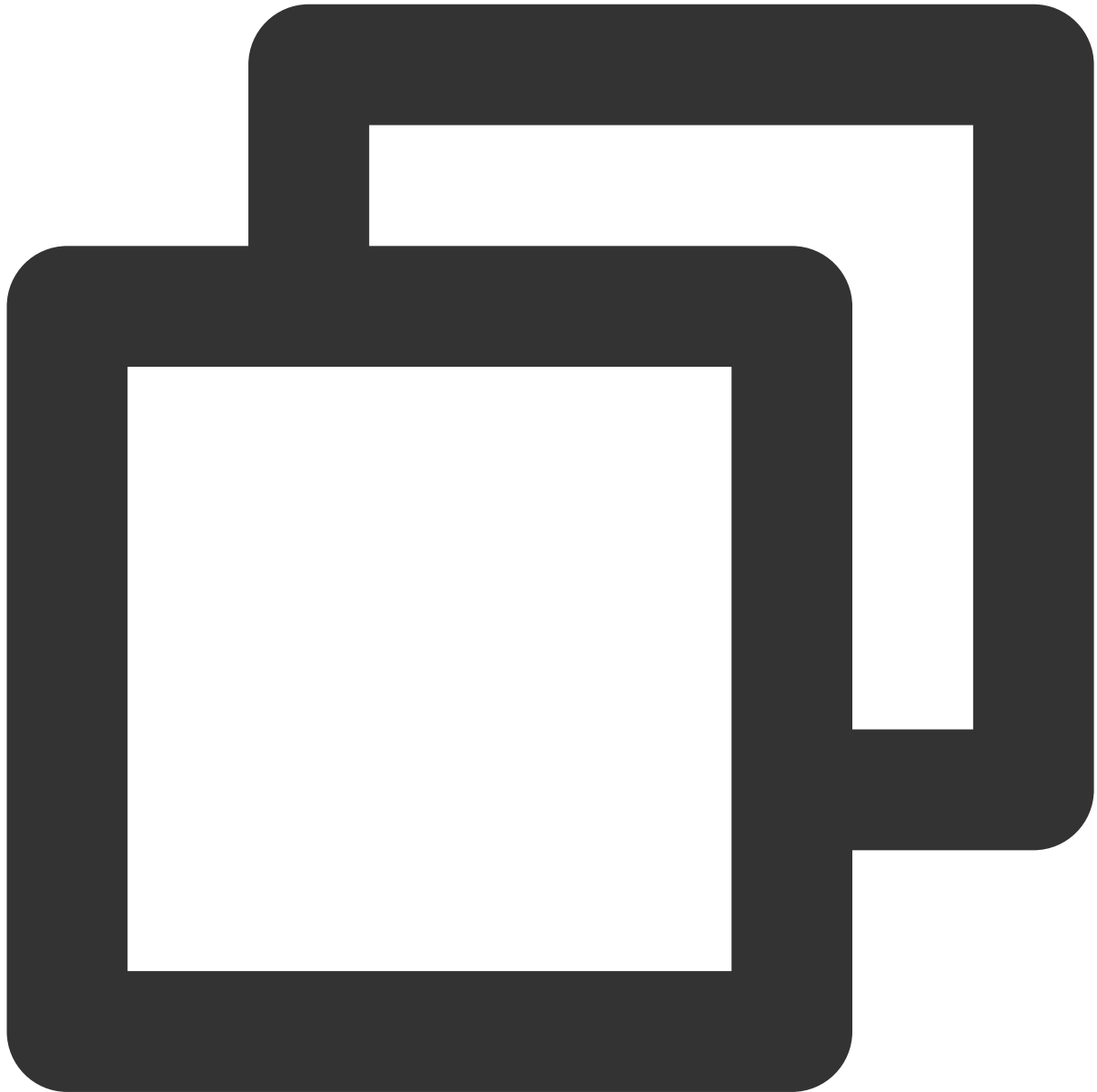
2. **yes**를 입력한 뒤 **Enter**를 눌러 업로드 여부를 확인하고 로그인 비밀번호를 입력하면 업로드가 완료됩니다.

시스템 기본 설정 비밀번호로 인스턴스에 로그인할 경우 [내부 메시지](#)에 접속하여 획득 바랍니다.

비밀번호를 잊으신 경우, [인스턴스 비밀번호 재설정](#)하시기 바랍니다.

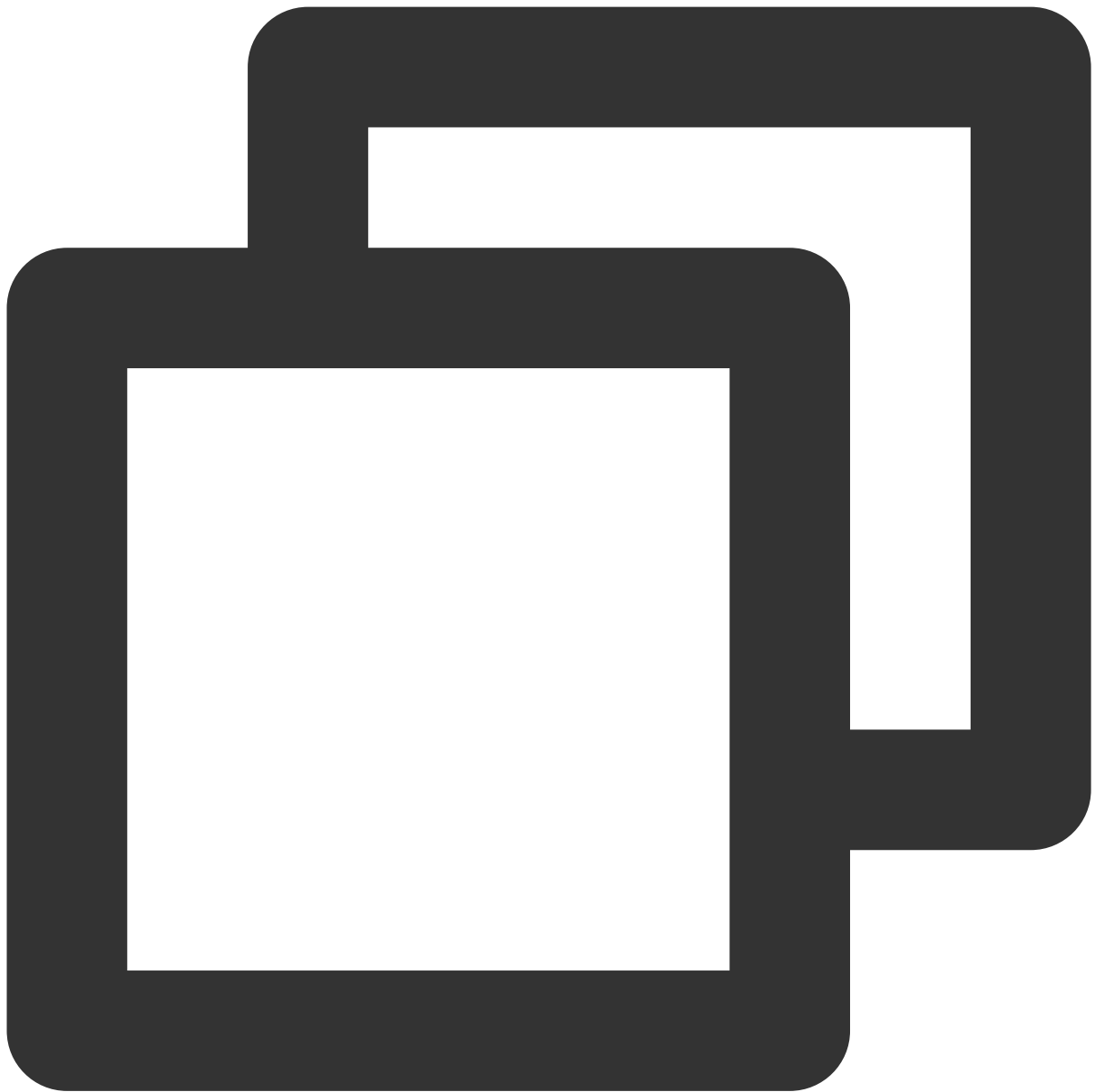
파일 다운로드

1. 다음 명령어를 실행하여 Linux CVM의 파일을 로컬에 다운로드합니다.



```
scp CVM 계정@CVM 인스턴스 공용 IP/도메인: CVM 파일 주소 로컬 파일 주소
```

예를 들어, IP 주소가 129.20.0.2 인 CVM 파일 /home/lamp0.4.tar.gz 을 해당 로컬 디렉터리로 다운로드 하는 경우, 다음과 같은 명령어를 실행합니다.



```
scp root@129.20.0.2:/home/Inmp0.4.tar.gz /home/Inmp0.4.tar.gz
```

Linux 시스템에서 FTP를 사용하여 CVM에 파일 업로드

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

본 문서는 Linux 시스템의 로컬 기기에서 FTP 서비스를 통해 로컬 파일을 CVM에 업로드하는 방법을 소개합니다.

전제 조건

CVM에 FTP 서비스가 구축되어 있어야 합니다.

CVM이 Linux 운영 체제일 경우, 자세한 작업 방식은 [Linux CVM에서 FTP 서비스 구축](#)을 참조 바랍니다.

CVM이 Windows 운영 체제일 경우, 자세한 작업 방식은 [Windows CVM에서 FTP 서비스 구축](#)을 참조 바랍니다.

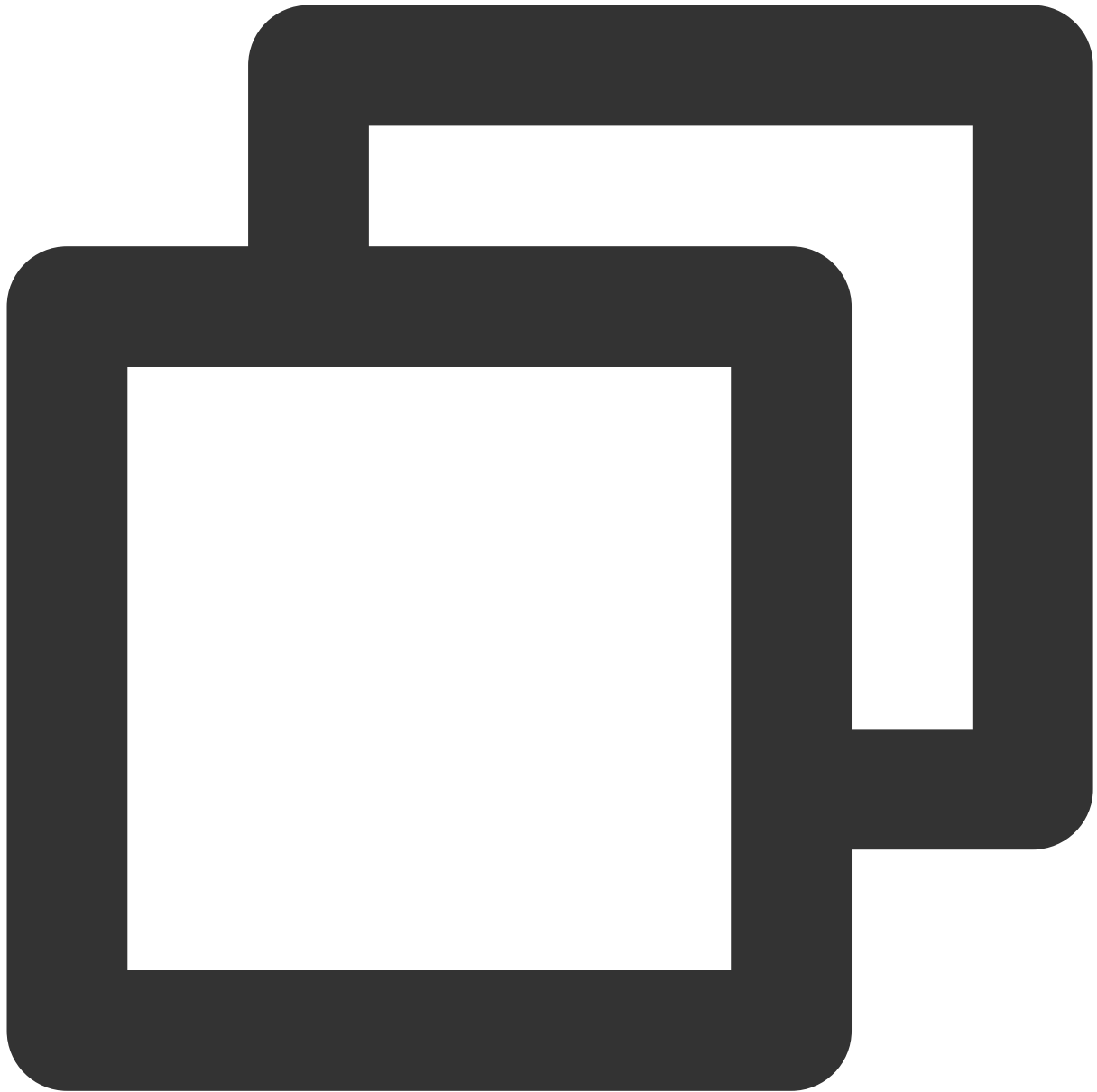
작업 순서

CVM 연결

1. 다음 명령어를 실행하여 ftp를 설치합니다.

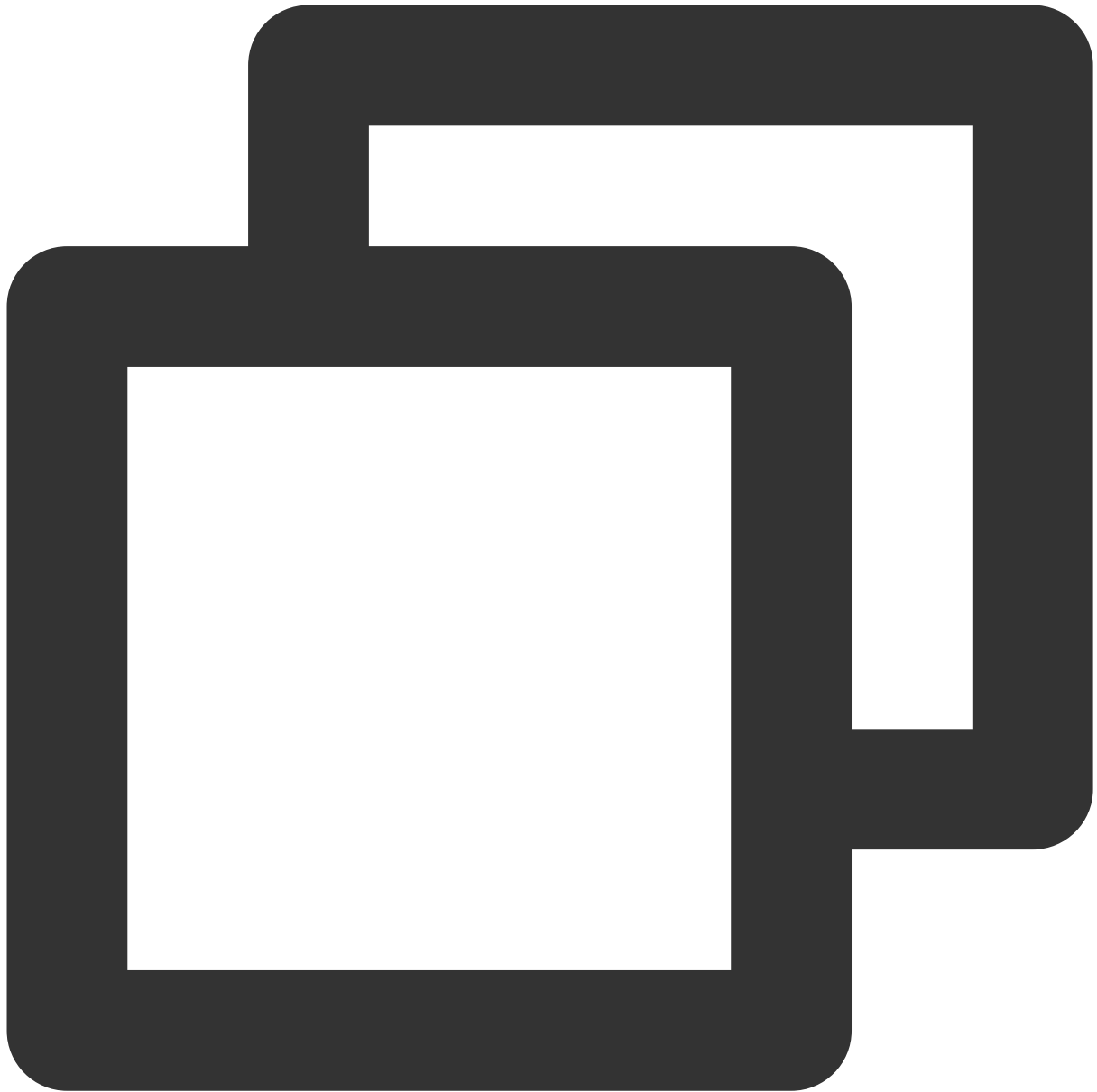
설명 :

Linux 시스템의 로컬 기기에 ftp가 설치되어 있다면, 이 단계를 건너뛰고 다음 단계를 진행하시기 바랍니다.



```
yum -y install ftp
```

2. 다음 명령어를 실행하여 로컬 컴퓨터에 CVM을 연결하고, 인터페이스 안내에 따라 FTP 서비스의 사용자 이름과 비밀번호를 입력합니다.



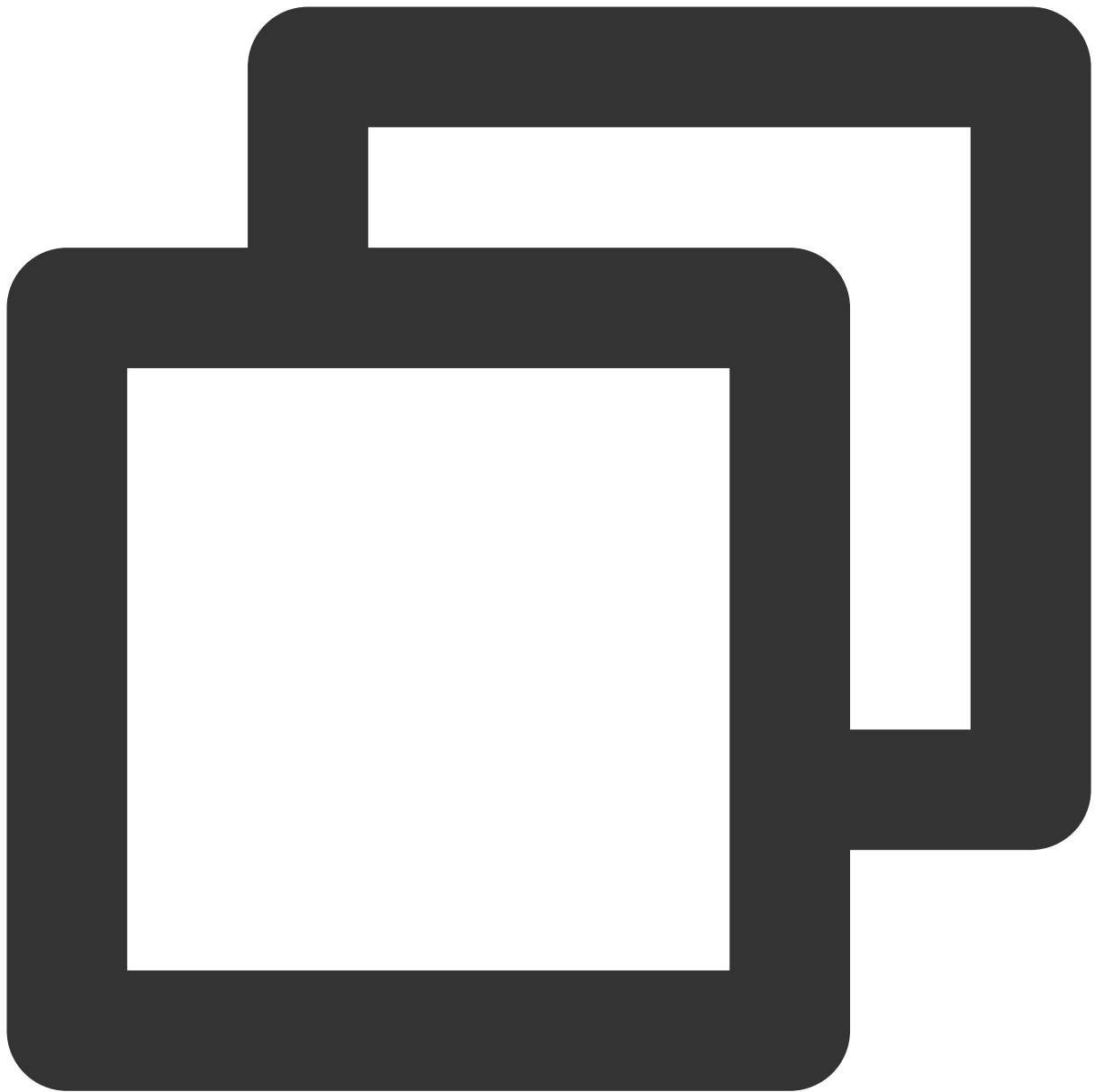
ftp CVM의 IP 주소

아래의 인터페이스로 이동하면 연결 성공입니다.

```
[root@VM_0_118_centos ~]# ftp 1[REDACTED].[REDACTED]
Connected to 1[REDACTED].[REDACTED] (1[REDACTED].[REDACTED]).
220 Microsoft FTP Service
Name ([REDACTED]:root): ftpuser
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> █
```

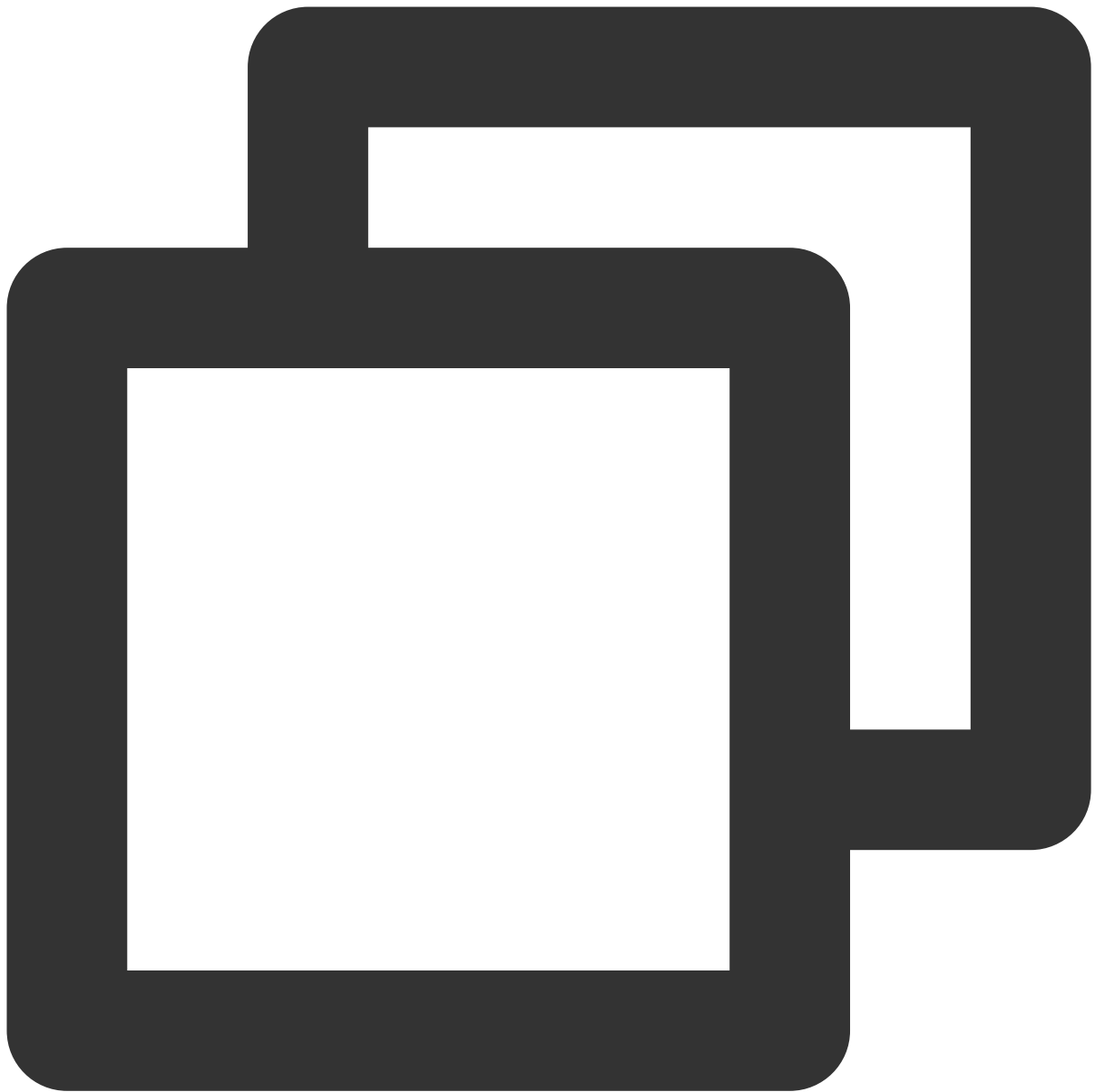
파일 업로드

다음 명령어를 실행하여 로컬 파일을 CVM에 업로드합니다.



```
put local-file [remote-file]
```

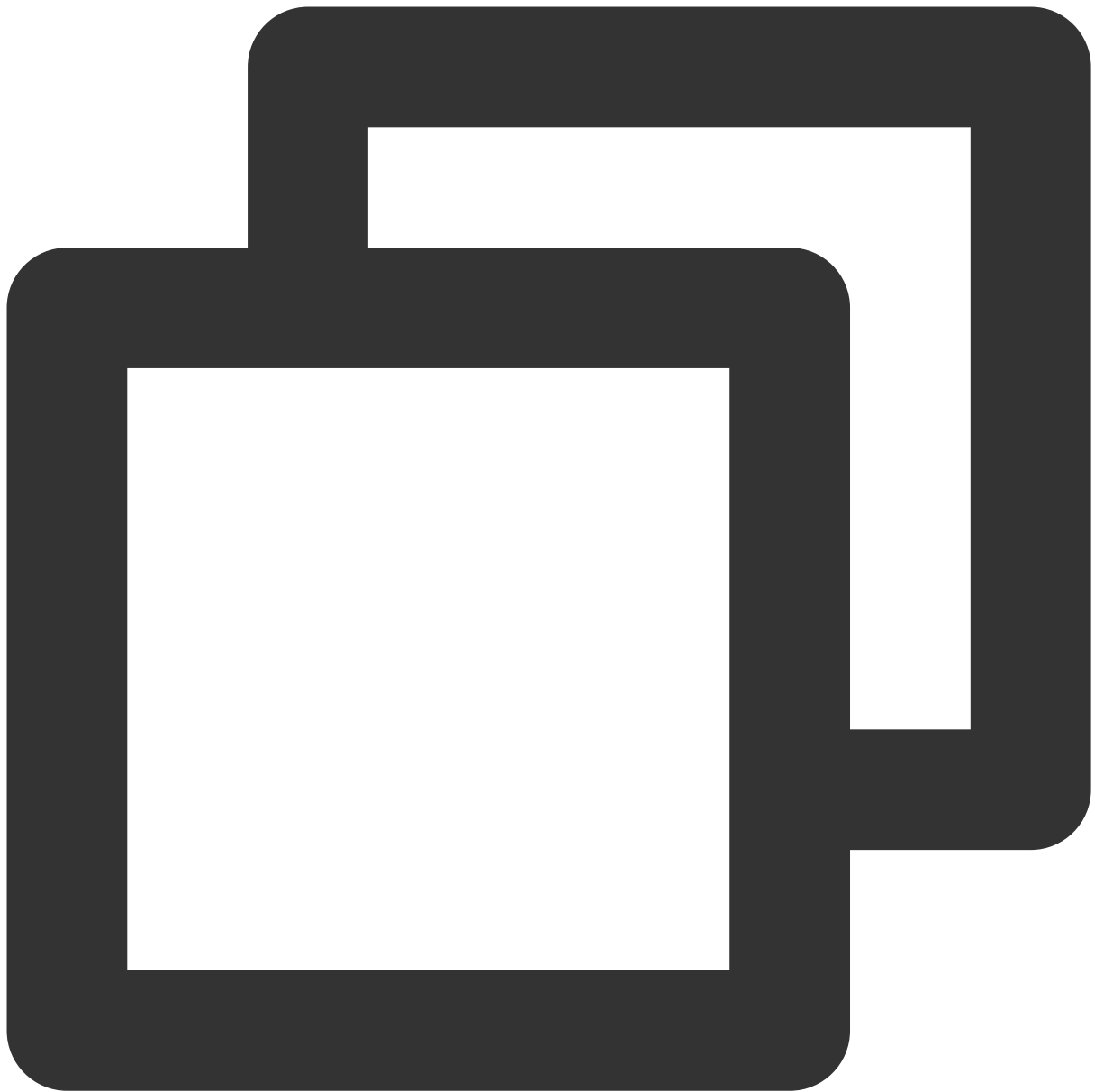
예시: 로컬 파일 `/home/1.txt` 를 CVM에 업로드.



```
put /home/1.txt 1.txt
```

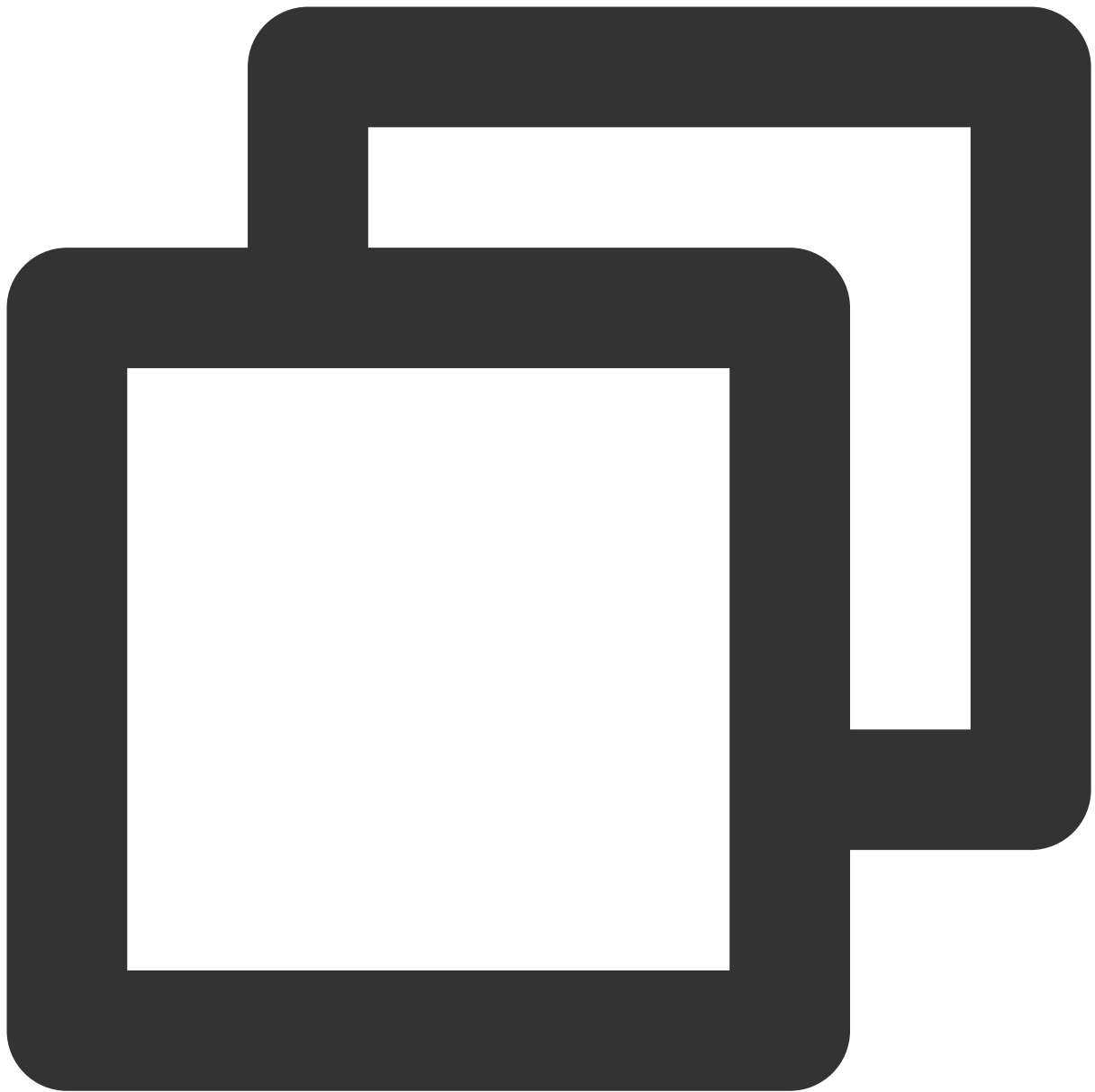
파일 다운로드

다음 명령어를 실행하여 CVM의 파일을 로컬에 다운로드합니다.



```
get [remote-file] [local-file]
```

예시: CVM의 `A.txt` 파일을 로컬 `/home` 디렉터리에 다운로드.



```
get A.txt /home/A.txt
```

Windows 시스템에서 FTP를 사용하여 CVM에 파일 업로드

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

본 문서는 Windows 시스템의 로컬 기기에서 FTP 서비스를 통해 로컬 파일을 CVM에 업로드하는 방법을 소개합니다.

전제 조건

CVM에 FTP 서비스가 구축되어 있어야 합니다.

CVM이 Linux 운영 체제일 경우, 자세한 작업 방식은 [Linux CVM에서 FTP 서비스 구축](#)을 참조 바랍니다.

CVM이 Windows 운영 체제일 경우, 자세한 작업 방식은 [Windows CVM에서 FTP 서비스 구축](#)을 참조 바랍니다.

작업 순서

CVM 연결

1. 로컬에 오픈 소스 소프트웨어인 FileZilla를 다운로드 및 설치합니다.

설명 :

FileZilla 3.5.3 버전을 사용해 FTP를 업로드할 경우, 업로드 실패 등의 문제가 발생할 수 있습니다. 공식 홈페이지에서 FileZilla 3.5.1 버전 혹은 3.5.2 버전을 다운로드받아 사용하시기를 권장합니다.

2. FileZilla를 엽니다.

3. FileZilla 창에서 호스트, 사용자 이름, 비밀번호 및 포트 등의 정보를 입력한 후, [빠른 연결]을 클릭합니다.

구성 정보 설명

호스트: CVM의 공인 IP입니다. [CVM 콘솔](#)의 인스턴스 관리 페이지에서 해당 CVM의 공인 IP를 조회할 수 있습니다.

사용자 이름: [FTP 서비스 구축](#)에서 설정한 FTP 사용자의 계정이며, 이미지의 "ftpuser1"는 예시입니다.

비밀번호: [FTP 서비스 구축](#)에서 설정한 FTP 사용자 계정의 비밀번호입니다.

포트: FTP 리스너 포트로서 기본값은 **21**입니다.

연결을 완료하면 CVM 원격 사이트 파일을 조회할 수 있습니다.

파일 업로드

왼쪽 하단의 "로컬 사이트" 창에서 업로드 대기 중인 로컬 파일을 마우스 우클릭 후 [업로드]를 선택하면 아래의 이미지와 같이 바로 Linux CVM에 파일을 업로드할 수 있습니다.

주의사항 :

CVM의 FTP 터널은 tar 압축 파일 업로드 후의 자동 압축 해제 및 tar 파일 삭제 기능을 지원하지 않습니다.
원격 사이트 경로는 파일을 Linux CVM에 업로드할 때 이용하는 기본 경로입니다.

파일 다운로드

오른쪽 하단의 “원격 사이트” 창에서 업로드 대기 중인 CVM 파일을 우클릭한 후 [업로드]를 선택하면 파일을 로컬에 다운로드할 수 있습니다.

기타 시나리오 관련 작업

최종 업데이트 날짜: : 2024-02-02 10:56:29

본 문서는 CVM 사용 시 자주 쓰는 기능에 대한 작업을 소개합니다. 다음 콘텐츠를 참조하여 필요에 따라 작업할 수 있습니다.

[Ubuntu 시각화 인터페이스 구축](#)

[로컬 파일을 CVM에 복사하는 방법](#)

[Linux CVM 데이터 복구](#)

[Windows CVM 디스크 용량 관리](#)

[오프라인 마이그레이션](#)

[CVM 리전 간 데이터 마이그레이션](#)

[CVM 계정 간 데이터 마이그레이션](#)

[Tencent Cloud에 AWS EC2 데이터 마이그레이션](#)

[Tencent Cloud에 Alibaba Cloud ECS 데이터 마이그레이션](#)

작업 중 문제가 발생한 경우 [응용 시나리오 관련 문제](#)를 참조하십시오.

CVM의 내부 네트워크를 통한 COS 액세스

최종 업데이트 날짜: : 2024-02-02 10:56:28

본문은 CVM이 COS에 액세스할 때 사용하는 액세스 방식과 사설망 액세스의 판단 방식을 소개하고, 연결성 테스트 예시를 제공합니다. 본문을 참고하여 CVM이 COS에 액세스하는 방법에 대해 자세히 알아볼 수 있습니다.

액세스 방식 설명

Tencent Cloud에 서비스를 배포하여 COS에 액세스하는 경우, 리전 내 액세스 방법에는 다음과 같은 차이점이 있습니다.

-동일 리전 내 액세스: 동일 리전 내에서의 액세스는 자동으로 사설망 주소로 연결되어, 사설망을 통해 서로 액세스할 수 있으므로 트래픽 비용이 발생하지 않습니다. 따라서 비용을 절약하기 위해 다른 Tencent Cloud 제품을 구매할 때 동일한 리전을 선택하는 것이 좋습니다.

리전 간 액세스: 사설망 액세스를 지원하지 않으며, 기본적으로 공중망 주소로 리졸브됩니다.

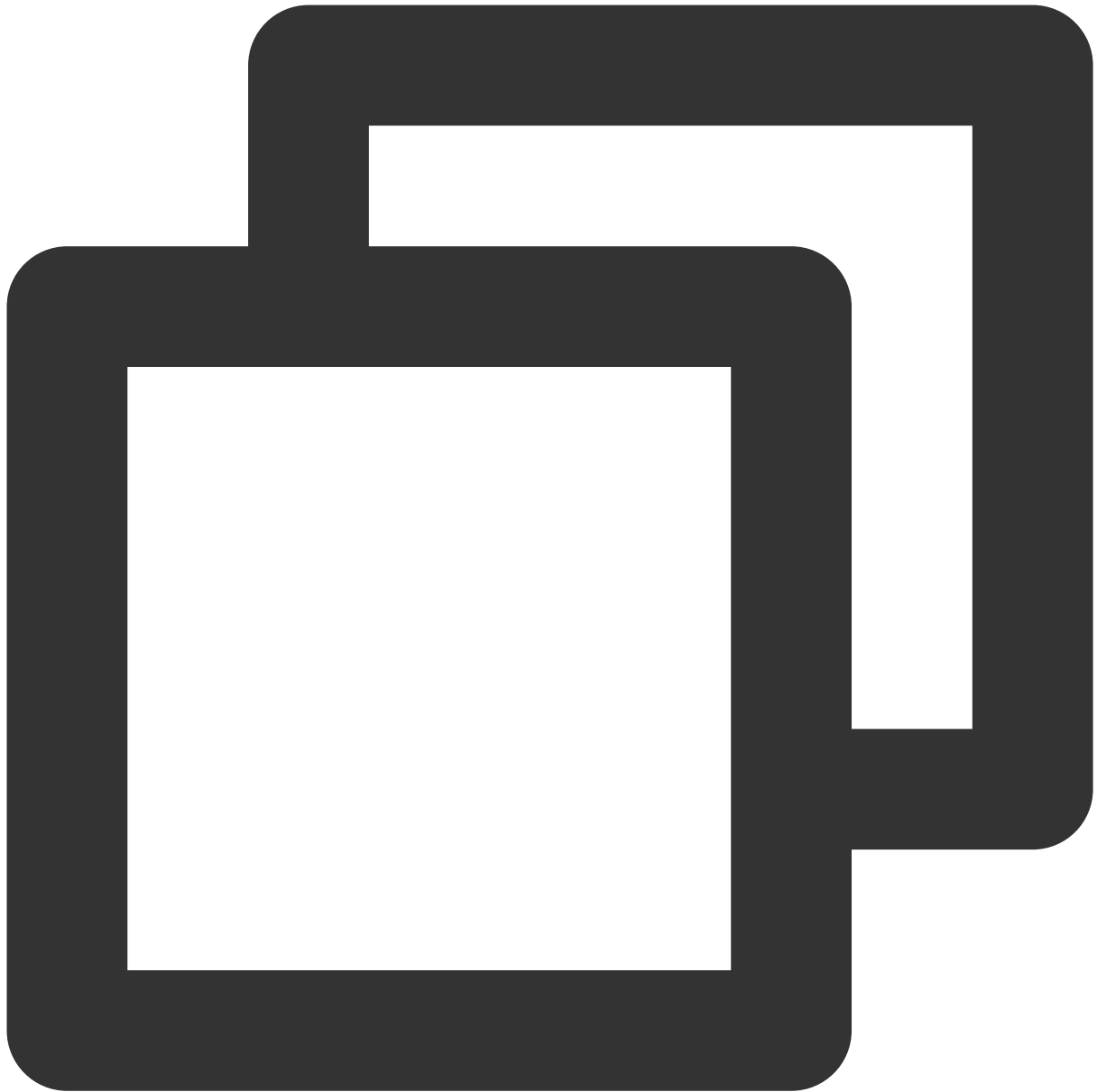
사설망 액세스 판단 방법

이 단계를 통하여 CVM이 사설망을 통해 COS에 액세스하는지 테스트할 수 있습니다.

CVM을 통한 COS 액세스의 경우, 사설망을 이용하여 COS에 액세스했는지 판단하려면, CVM에서 `nslookup` 명령어를 사용하여 COS 도메인을 리졸브할 수 있습니다. 사설 IP를 반환한다면 CVM과 COS 간 사설망으로 액세스한 것이고, 아니라면 공중망으로 액세스한 것입니다.

1. 버킷의 도메인 이름을 얻고 주소를 기록합니다. 자세한 내용은 [버킷 개요](#)를 참고하십시오.

2. 인스턴스에 로그인하고 `nslookup` 명령을 실행합니다. `examplebucket-1250000000.cos.ap-guangzhou.myqcloud.com` 이 대상 버킷 주소일 때, 다음 명령을 실행합니다.



```
nslookup examplebucket-1250000000.cos.ap-guangzhou.myqcloud.com
```

반환된 결과가 아래 이미지와 같다면, 여기서 `10.148.214.13` 및 `10.148.214.14` 이 두 IP는 사설망을 통해 COS에 액세스했음을 의미합니다.

설명 :

사설 IP 주소는 일반적으로 `10.*.*.*` , `100.*.*.*` 형식이며, VPC 네트워크는 일반적으로 `169.254.*.*` 등의 형식입니다. 해당 두 가지 형식의 IP는 사설망에 속합니다.

```
nslookup examplebucket-1250000000.cos.ap-guangzhou.myqcloud.com
Server: 10.138.224.65
Address: 10.138.224.65 #53
Name: examplebucket-1250000000.cos.ap-guangzhou.myqcloud.com
Address: 10.148.214.13
Name: examplebucket-1250000000.cos.ap-guangzhou.myqcloud.com
Address: 10.148.214.14
```

연결성 테스트

COS에 대한 공중망 액세스, 리전 내 CVM(기본 네트워크) 액세스, 리전 내 CVM(VPC 네트워크) 액세스의 예시를 제공합니다. 자세한 내용은 [연결성 테스트](#)를 참고하십시오.

관련 작업

[COS를 로컬 디스크로 Windows 서버에 마운트](#)

[COS에 WordPress 원격 첨부 파일 저장](#)

Linux 인스턴스 데이터 복구

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

본 문서에서는 운영 체제가 CentOS 8.0인 Tencent Cloud CVM(Cloud Virtual Machine)을 예로 들어 오픈 소스 툴 [Extundelete](#)을 사용하여 실수로 삭제된 데이터를 빠르게 복원하는 방법을 소개합니다.

Extundelete는 파일 시스템 유형이 `ext3` 및 `ext4`인 파일의 우발적 삭제 복구를 지원하지만 구체적인 복구 정도는 삭제 후 덮어쓰기 여부, 메타데이터 `journal` 보존 여부 등과 같은 요인과 관련이 있습니다. 복구할 데이터의 파일 시스템이 시스템 디스크에 있고 비즈니스 프로세스나 시스템 프로세스가 항상 파일에 쓰기 중인 경우 복구 가능성이 낮습니다.

설명 :

Tencent Cloud는 [스냅샷 생성](#), [사용자 정의 이미지 생성](#) 및 [객체 스토리지](#) 등의 데이터 스토리지 방식을 제공하오니, 정기적으로 데이터를 백업하여 데이터 보안성을 개선하시길 권장합니다.

준비 작업

데이터 복구 관련 작업을 수행하기 전에 다음 준비 작업을 완료하십시오.

[스냅샷 생성](#) 및 [사용자 정의 이미지 생성](#)을 참고하여 문제 발생 시 초기 상태로 복구할 수 있도록 데이터를 백업하시기 바랍니다.

관련 비즈니스 프로그램을 중지하고 파일 시스템에 데이터 쓰기를 계속합니다. 데이터 디스크를 복원해야 하는 경우 먼저 데이터 디스크에서 'umount' 작업을 수행할 수 있습니다.

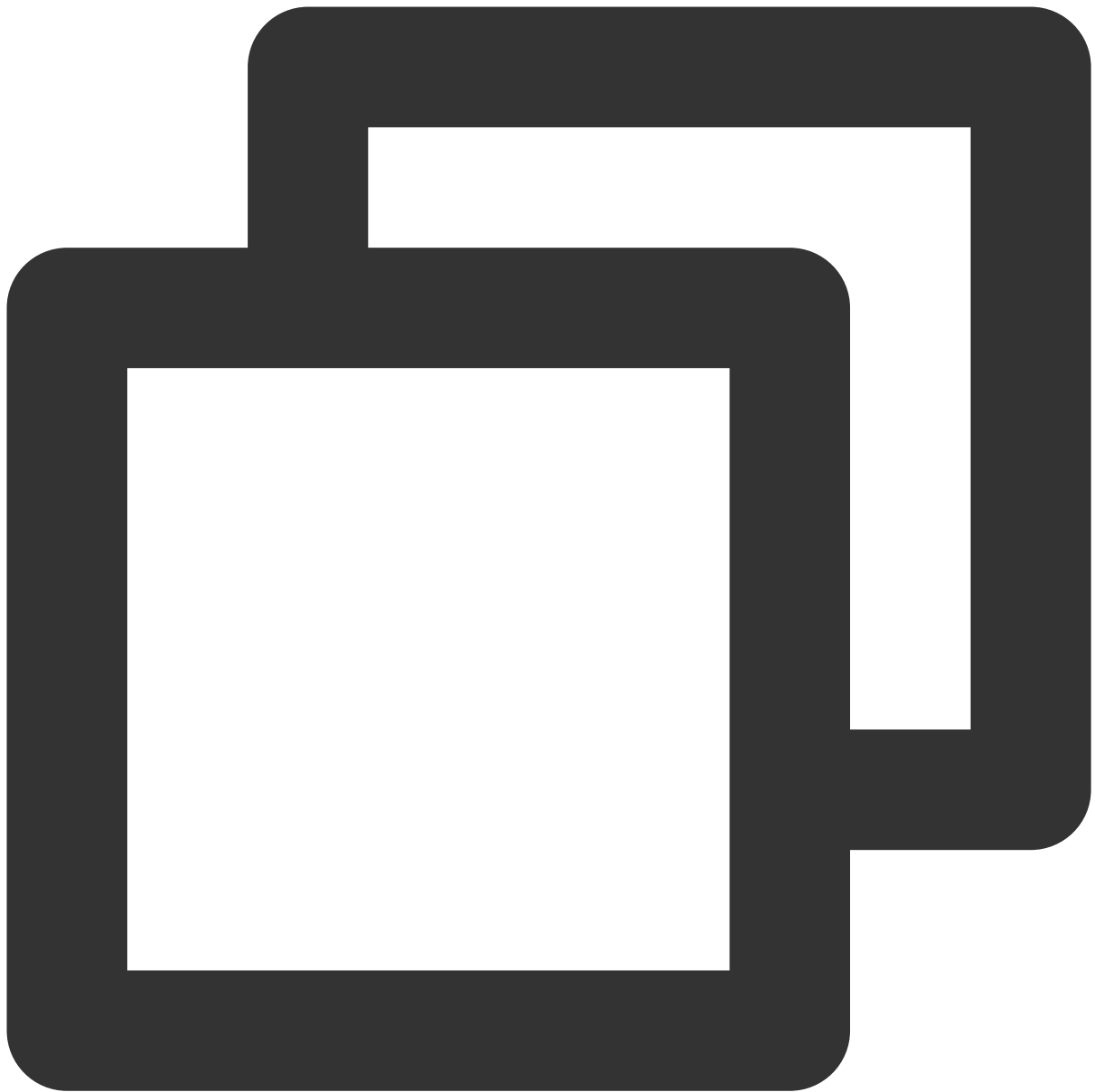
작업 단계

1. 다음 두 가지 방법으로 Extundelete를 설치합니다.

컴파일된 이진법 프로그램 다운로드(권장)

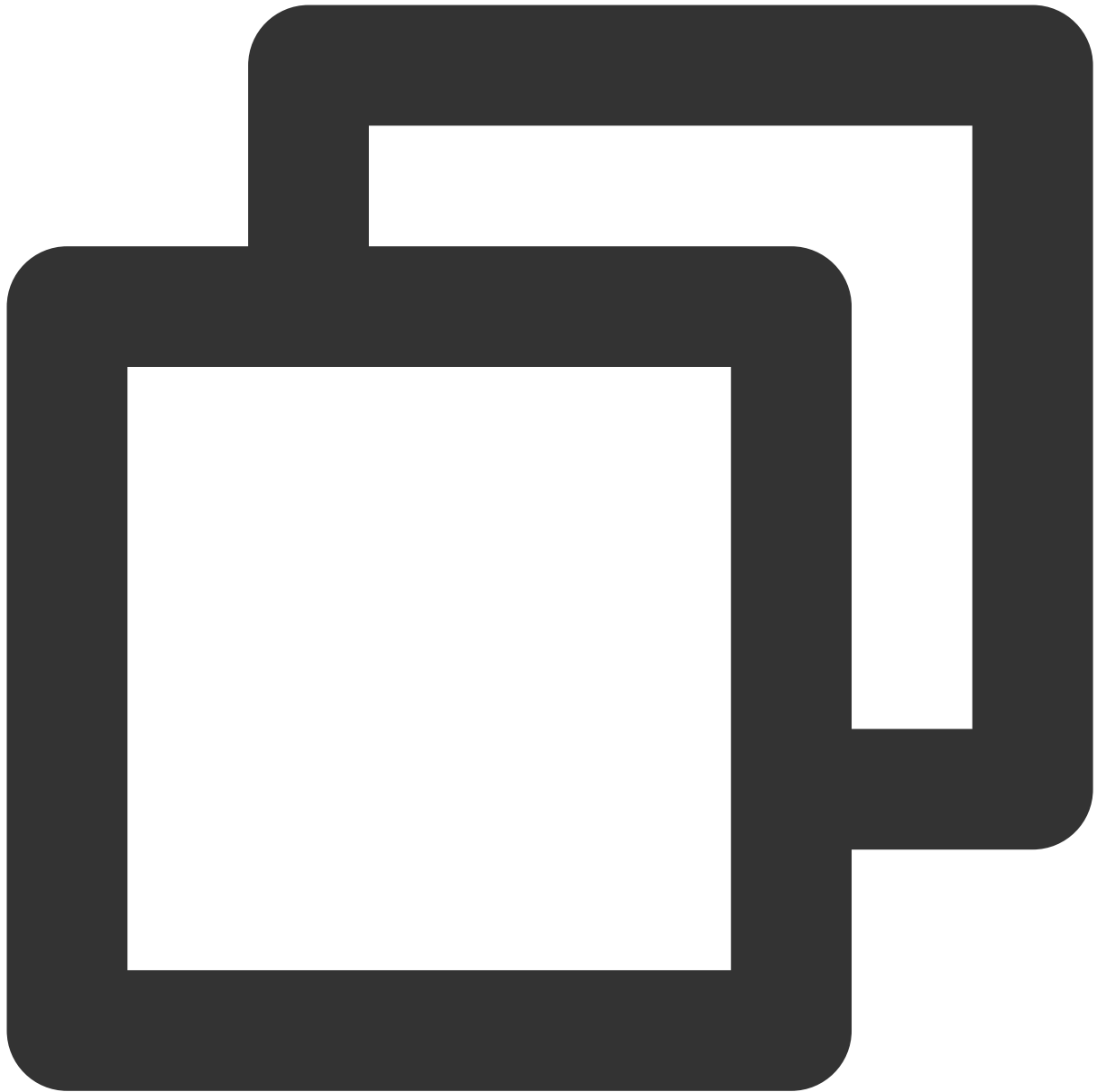
수동 컴파일 설치

1. 다음 명령을 실행하여 컴파일된 이진법 프로그램을 직접 다운로드합니다.



```
wget https://github.com/curu/extundelete/releases/download/v1.0/extundelete
```

2. 다음 명령어를 실행하여 파일 권한을 부여합니다.

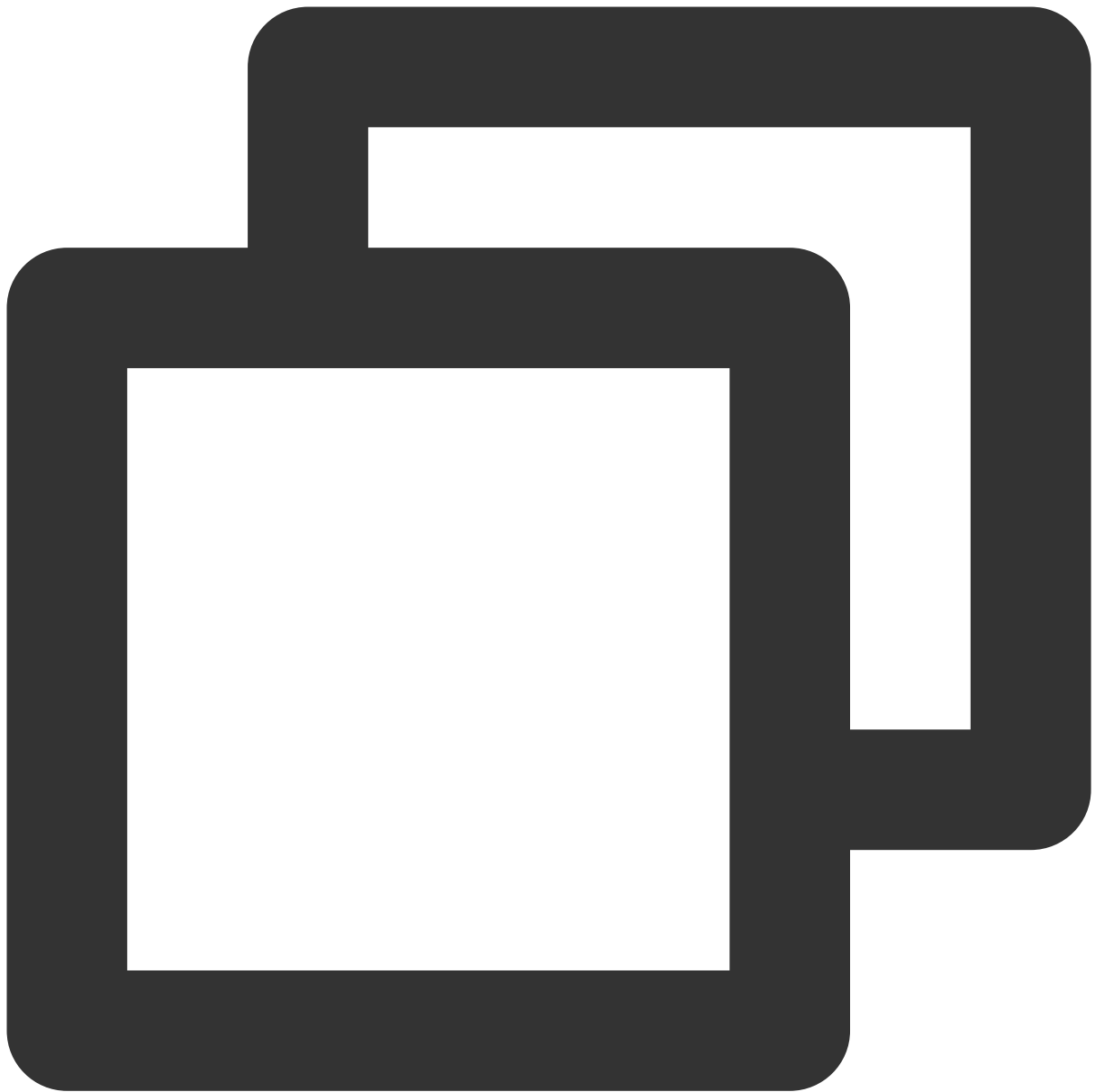


```
chmod a+x extundelete
```

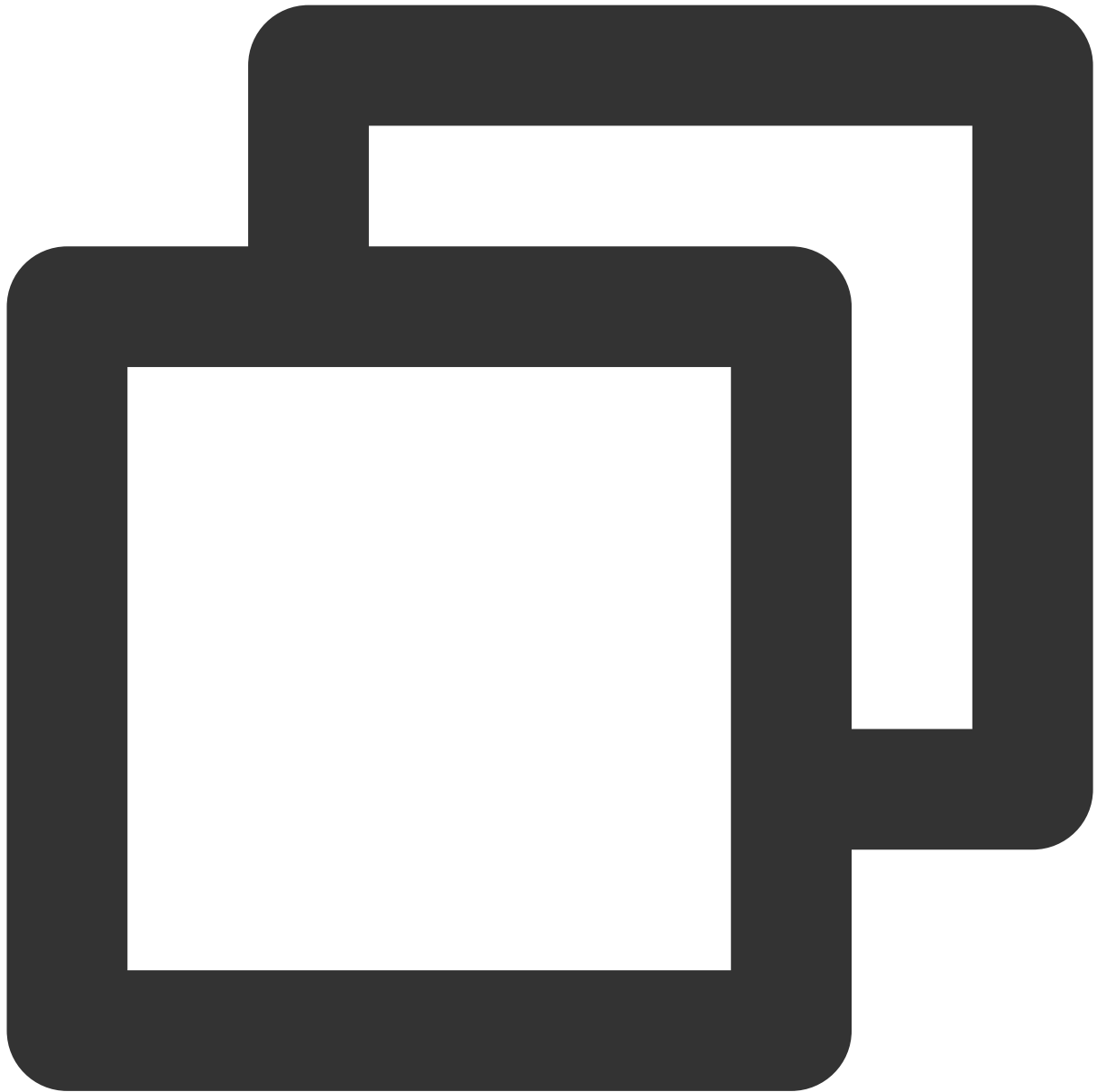
설명 :

이 단계는 CentOS 7 운영 체제를 예로 들며 시스템 환경에 따라 단계가 다르므로 실제 참고 문서에 따라 작업하십시오.

1. 다음 명령어를 순서대로 실행하여 Extundelete에 필요한 종속 및 라이브러리를 설치합니다.

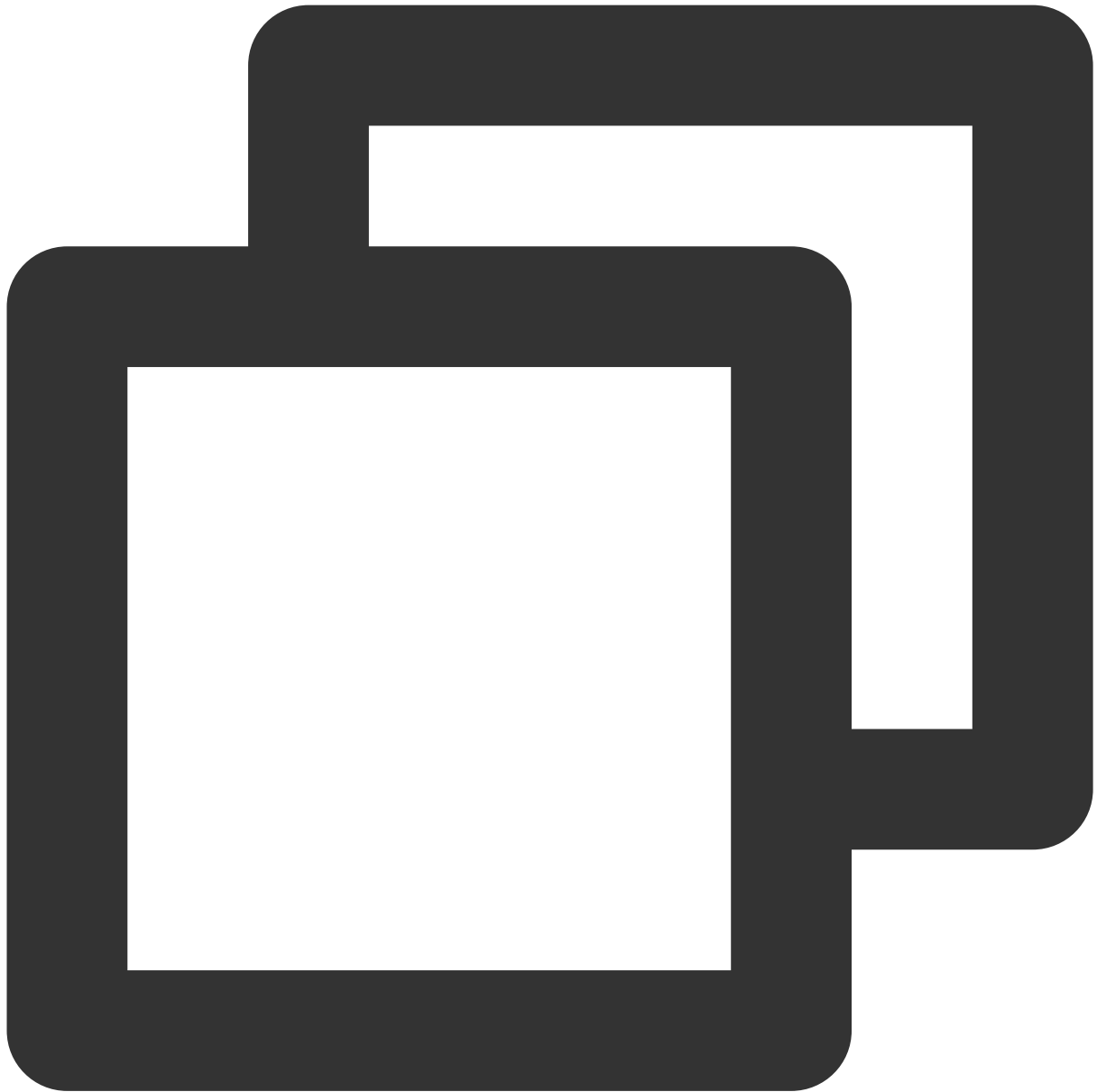


```
yum install libcom_err e2fsprogs-devel
```

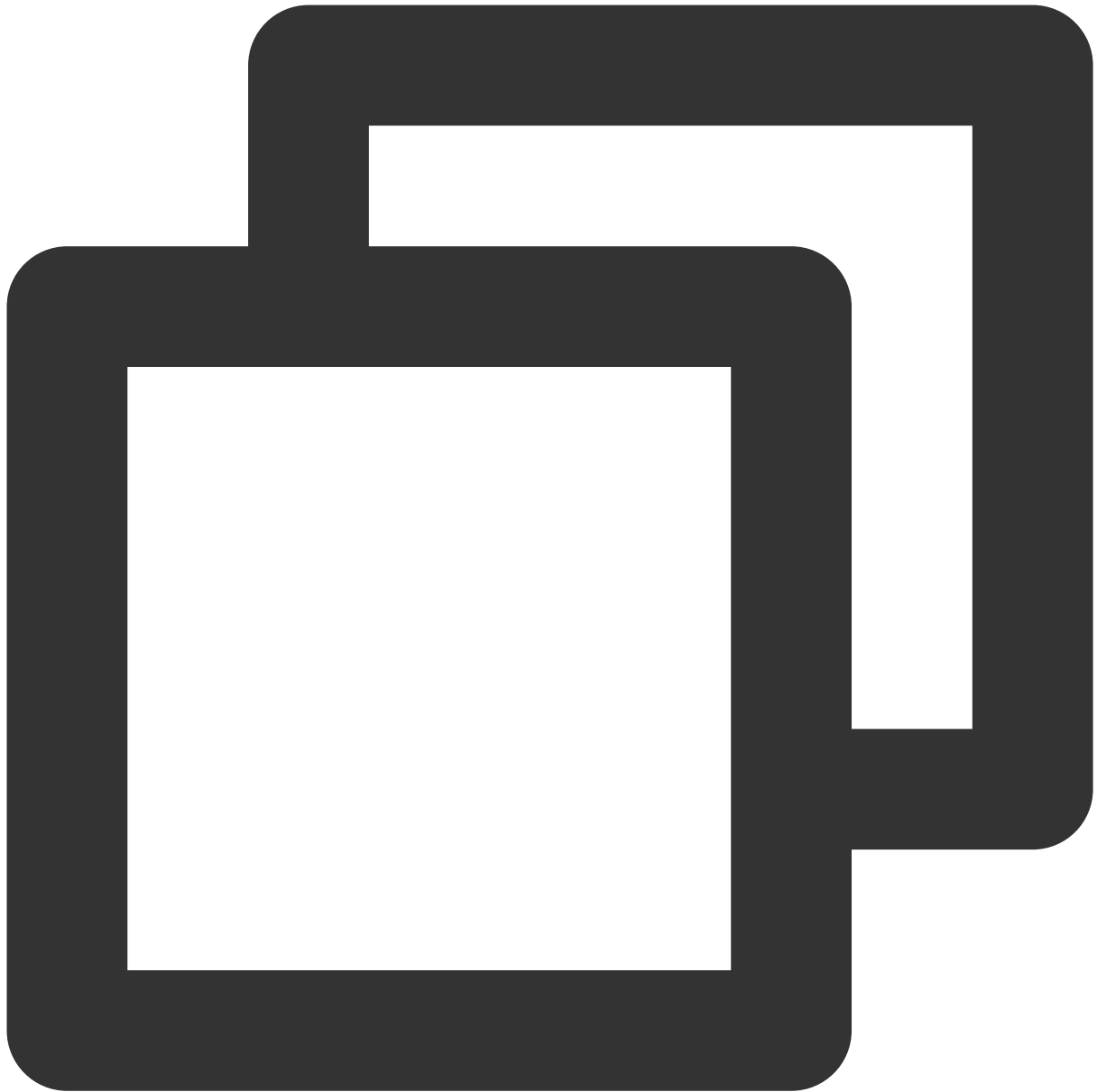
```
yum install gcc gcc-c++
```

2. 다음 명령어를 실행하여 Extundelete 소스 코드를 다운로드합니다.



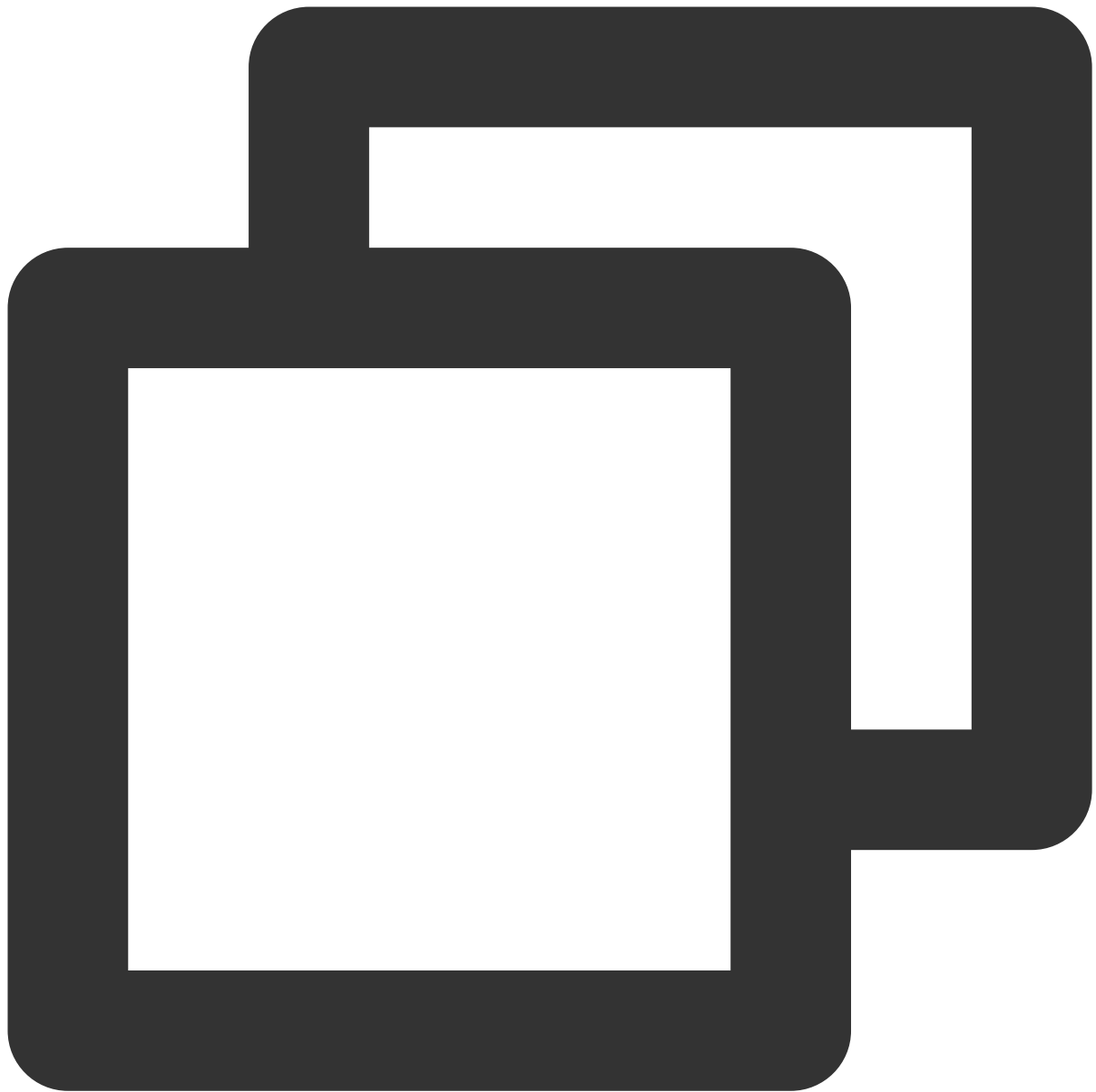
```
wget https://github.com/curu/extundelete/archive/refs/tags/v1.0.tar.gz
```

3. 다음 명령어를 실행하여 v1.0.tar.gz 파일을 압축 해제합니다.

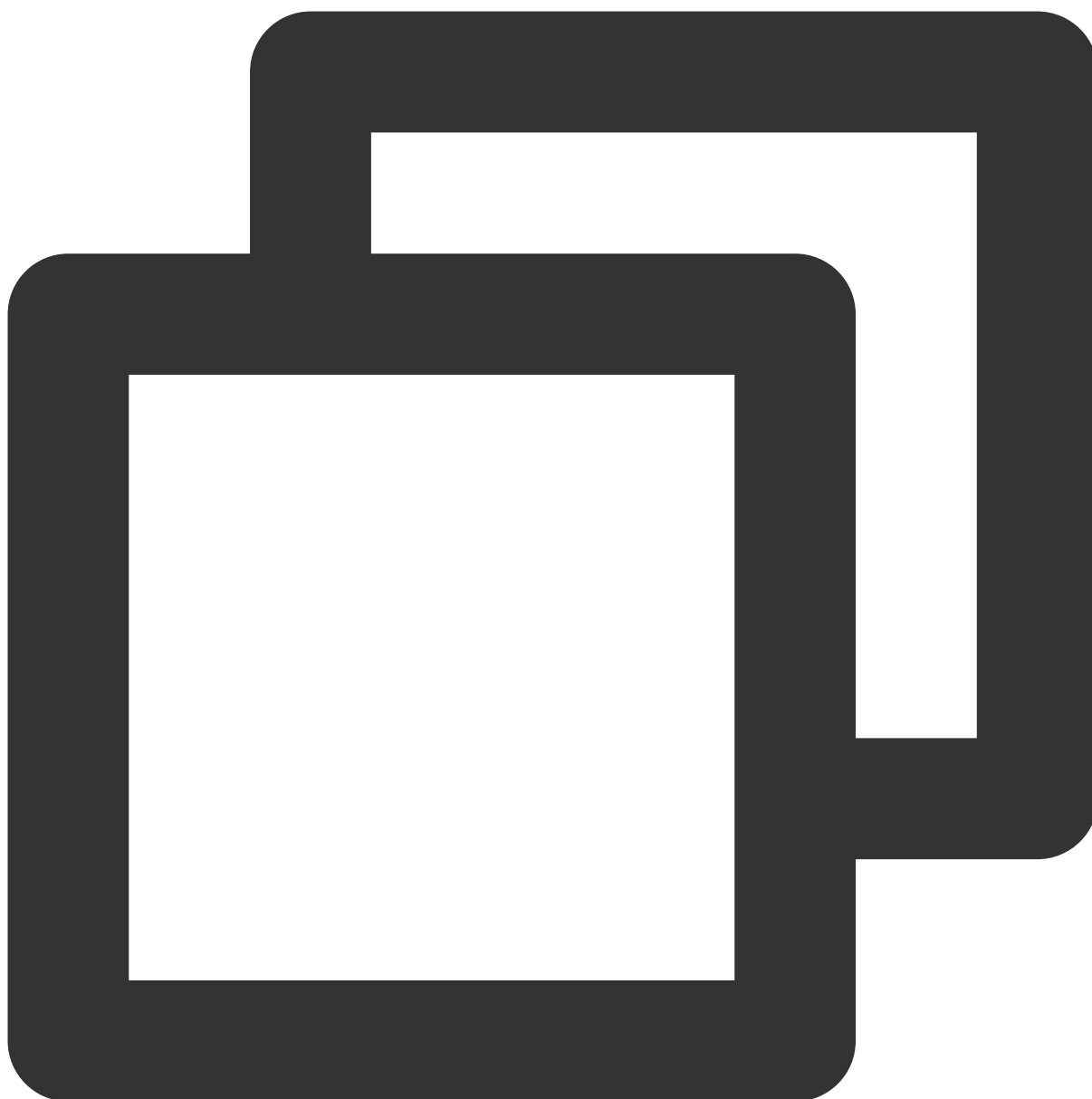


```
tar xf v1.0.tar.gz
```

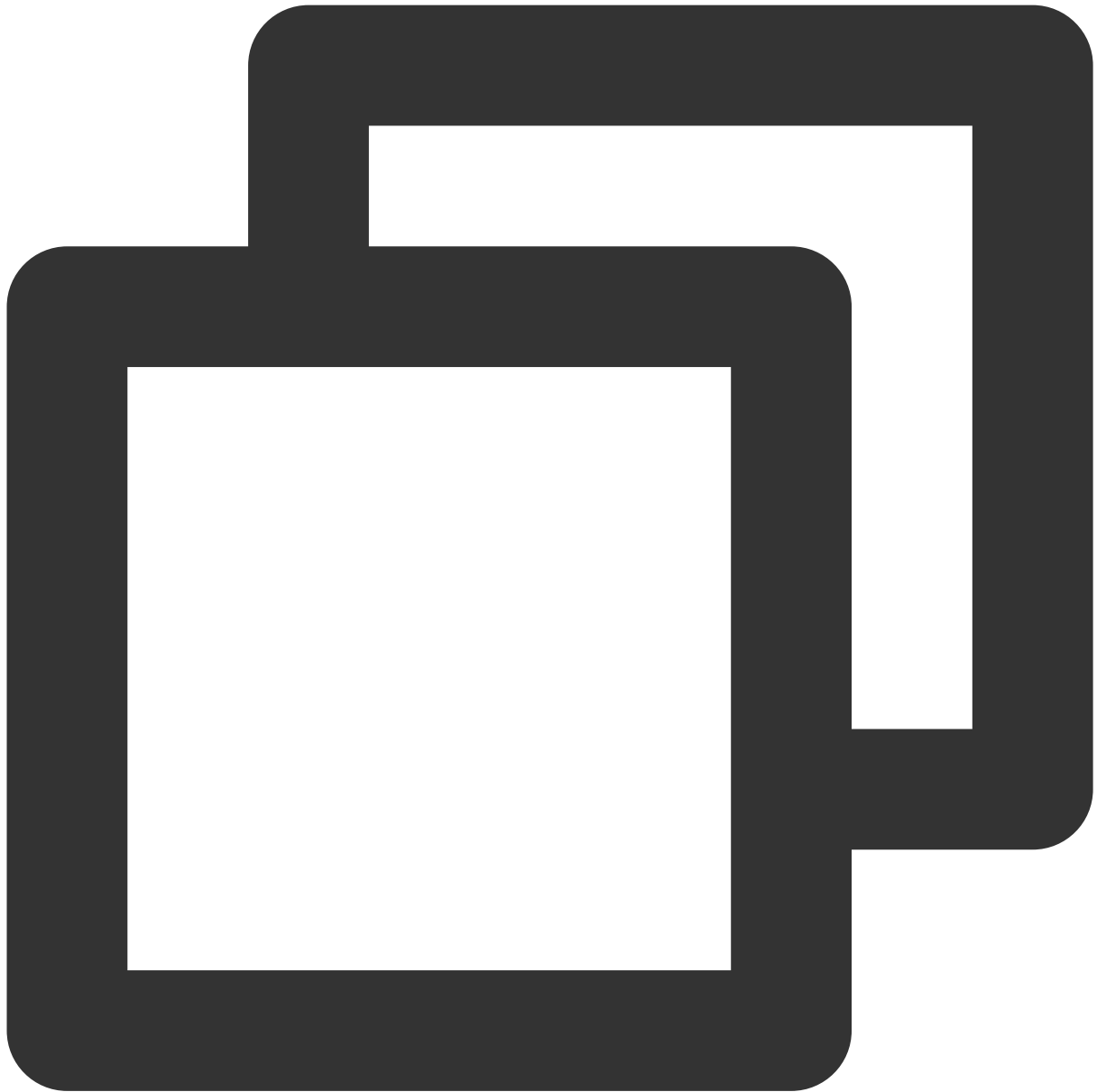
4. 다음 명령어를 순서대로 실행하여 컴파일 및 설치합니다.



```
cd extundelete-1.0
```

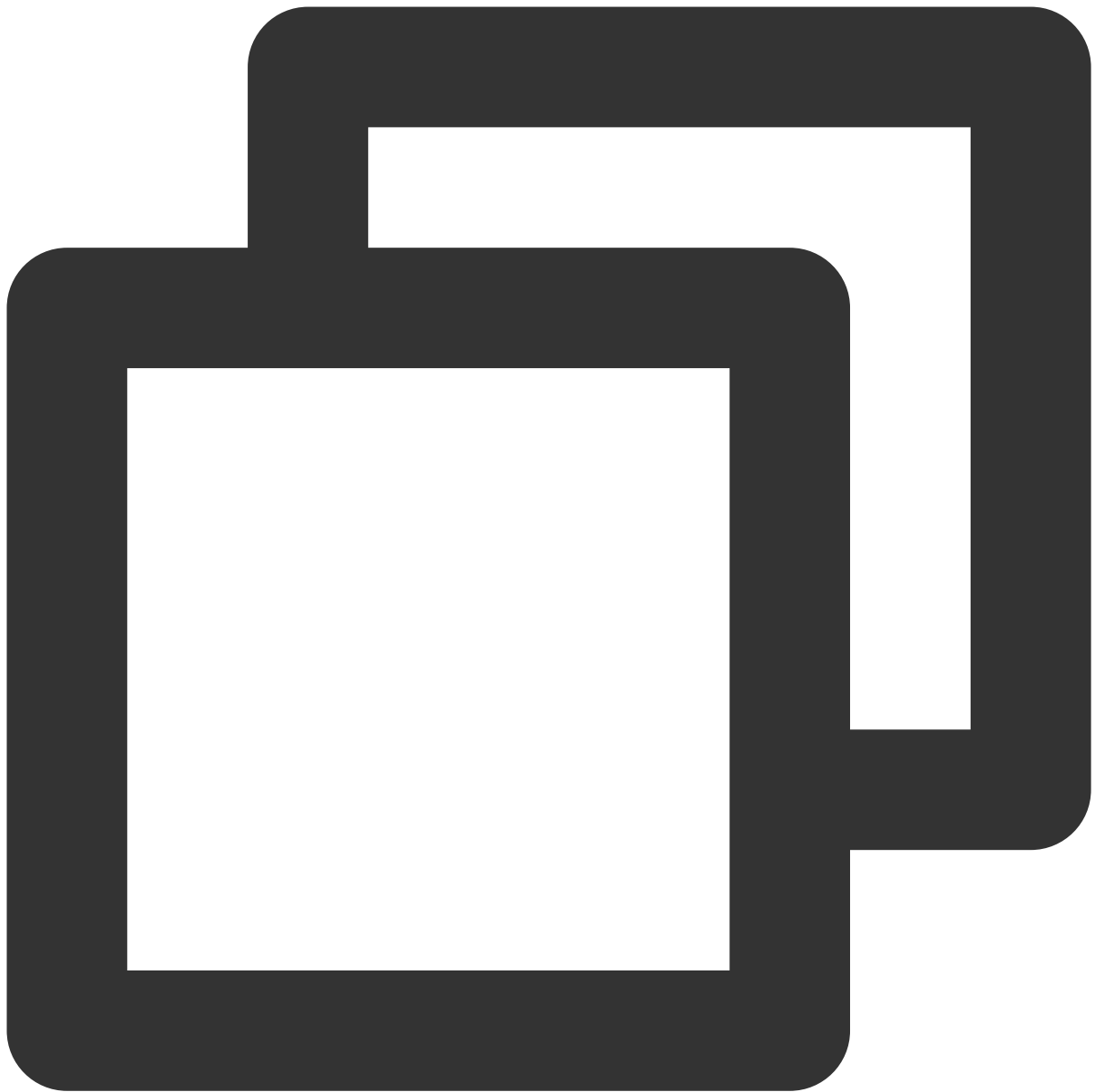


```
./configure
```



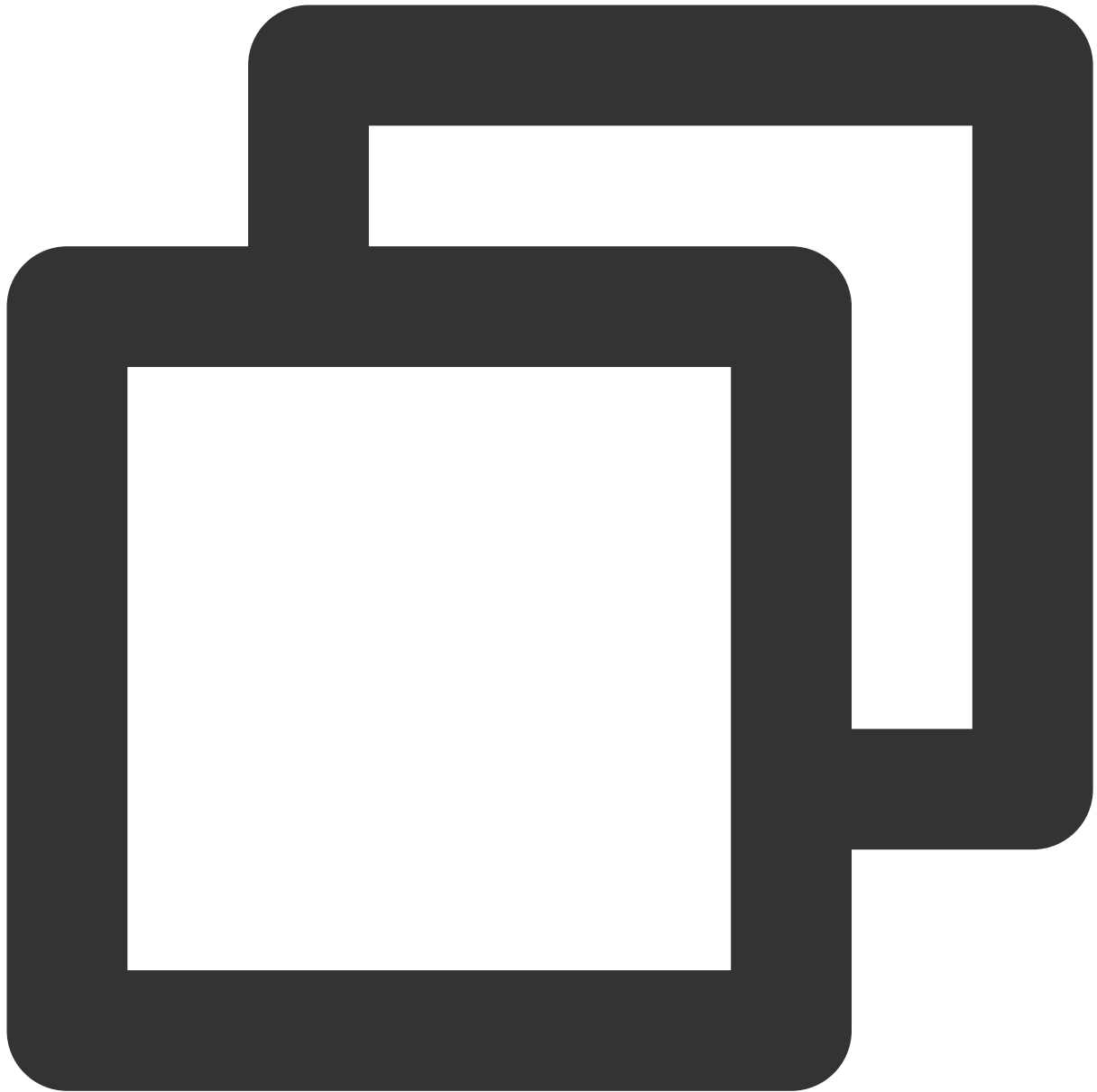
```
make
```

5. 다음 명령어를 실행하여 `src` 디렉터리로 이동하여 컴파일된 `Extundelete` 파일을 조회합니다.



```
cd ./src
```

2. 다음 명령어를 실행하여 데이터 복원을 시도합니다.



```
./extundelete --restore-all /dev/해당 디스크
```

복구된 파일은 같은 레벨 디렉터리의 'RECOVERED_FILES' 폴더에 있으므로 필요한 파일이 있는지 확인하십시오.

Windows 인스턴스 디스크 용량 관리

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

본 문서는 Windows Server 2012 R2 운영 체제의 Tencent Cloud CVM을 예로, Windows 인스턴스 디스크의 용량이 부족할 때의 용량 확보 작업 및 일상적인 디스크 점검 방법에 대해 소개합니다.

작업 순서

디스크 용량 확보

용량이 비교적 큰 파일 삭제 또는 불필요한 파일 삭제를 통해 디스크 용량이 부족한 문제를 해결할 수 있습니다. 파일을 정리해도 부족하다면 디스크 확장을 통해 용량을 확장할 수 있으며, 자세한 내용은 [확장 시나리오 소개](#)를 참조 바랍니다.

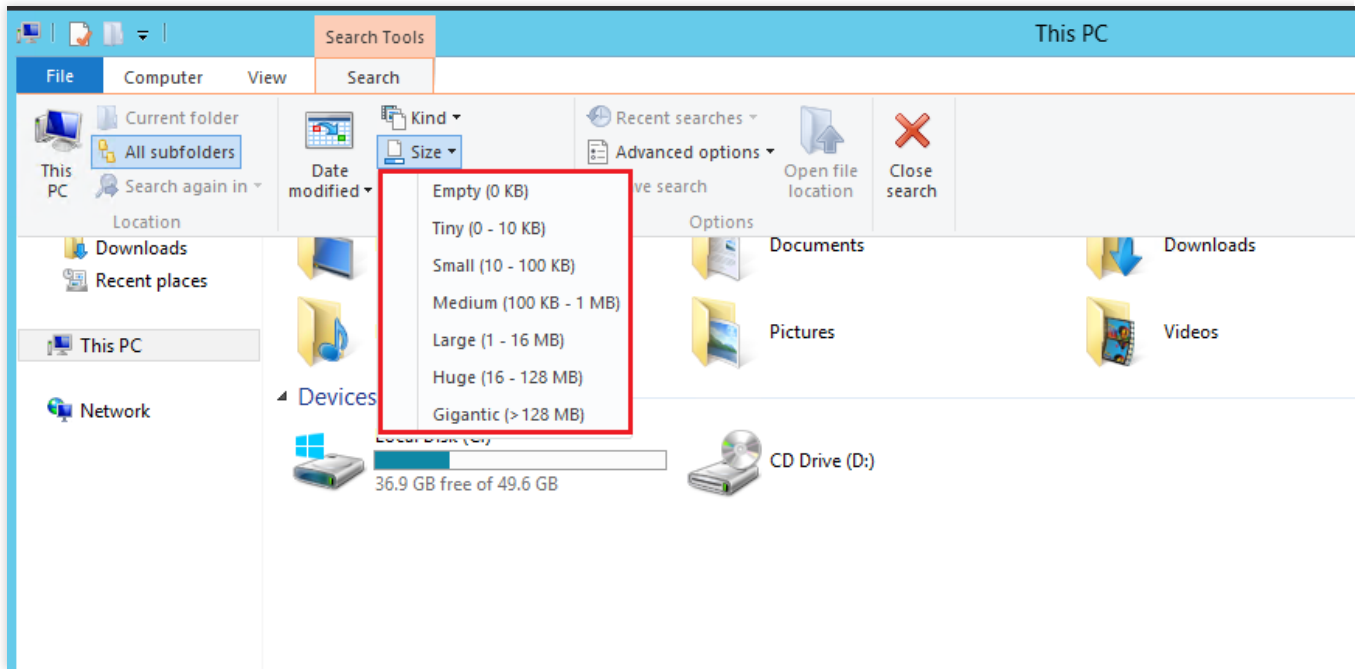
용량이 비교적 큰 파일 삭제

1. RDP 파일을 사용하여 Windows 인스턴스에 로그인(권장)하거나 실제 작업 스타일에 따라 원격 데스크톱 연결을 사용하여 Windows 인스턴스에 로그인할 수 있습니다.
2. 하단의 작업 표시줄에서



모양을 클릭하고 '내 PC' 창을 엽니다.

3. '내 PC'에서 정리할 디스크를 선택하고 **Crtl + F**를 눌러 검색 툴을 엽니다.
4. 아래 이미지와 같이 [검색]>[크기]를 선택하고, 시스템에 정의된 크기를 기준으로 필요에 따라 메뉴에서 선택해 파일을 필터링합니다.



설명 :

또는 '내 PC' 창 오른쪽 상단의 검색 창에서 파일 크기를 사용자 정의로 검색할 수 있습니다. 예시:

'크기: >500M'를 입력하면 해당 디스크에 있는 500M 이상의 파일을 검색합니다.

'크기: > 100M < 500M'를 입력하면 해당 디스크에 있는 100M 초과 500M 미만의 파일을 검색합니다.

불필요한 파일 삭제

1.

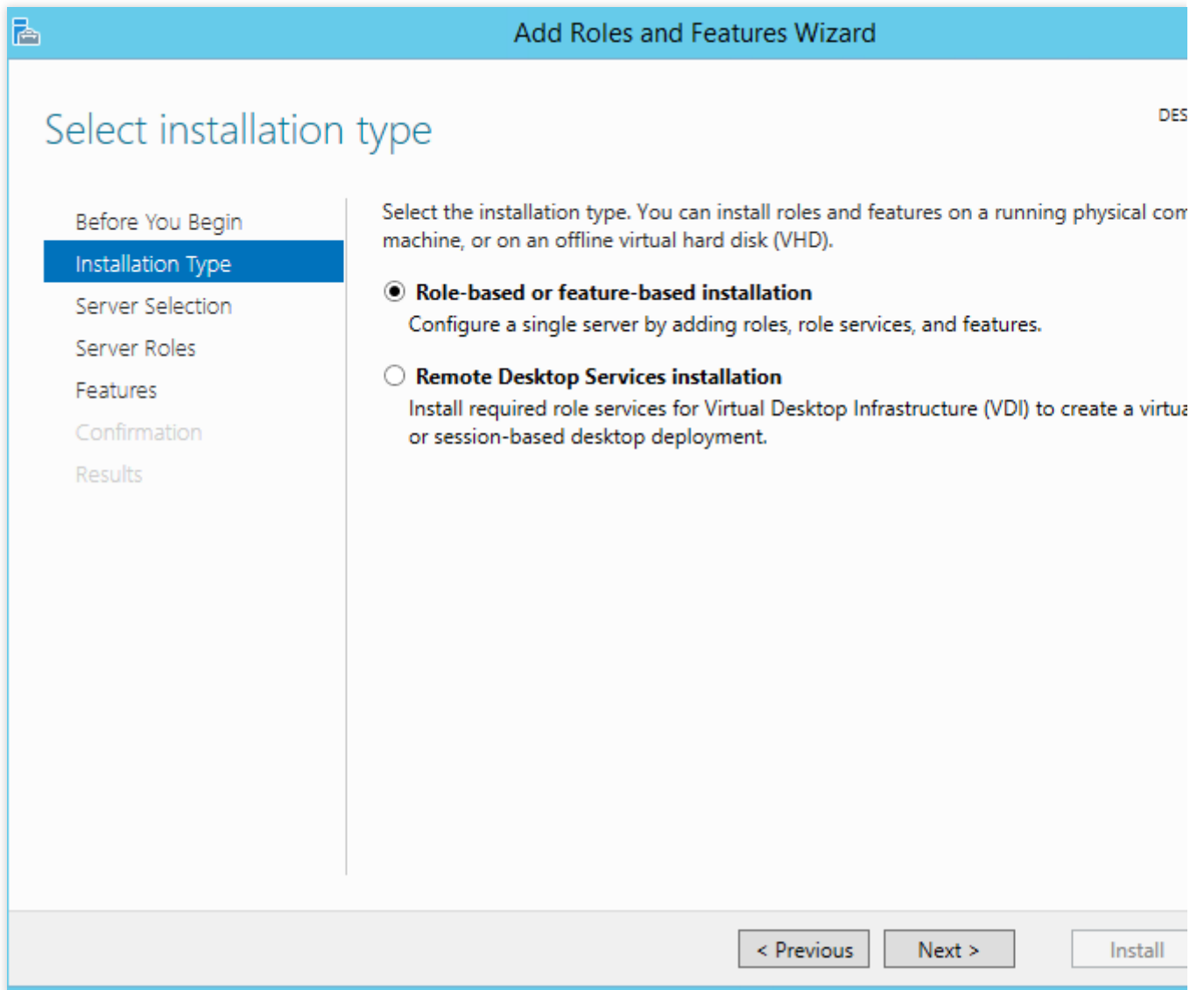


모양을 클릭하여 서버 관리자를 엽니다.

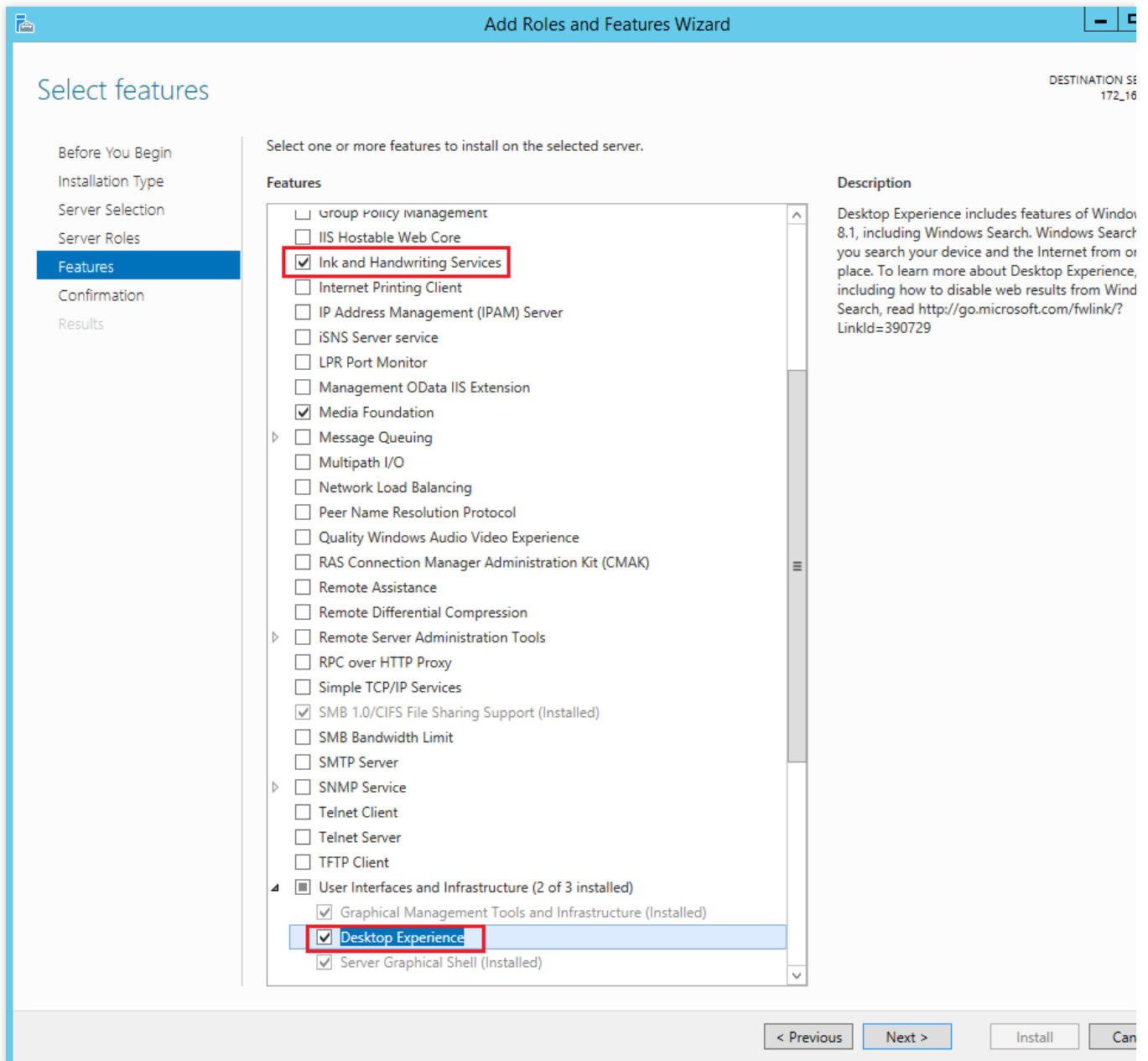
2. [역할 및 기능 추가]를 클릭하면 '역할 및 기능 추가 마법사' 창이 팝업됩니다.

3. '역할 및 기능 추가 마법사' 창에서 [다음]을 클릭합니다.

4. 아래 이미지와 같이 '설치 유형 선택' 인터페이스에서 [역할 기반 또는 기능 기반 설치]를 선택하고, [다음]을 3회 연속 클릭합니다.



5. 아래 이미지와 같이 '기능 선택' 인터페이스에서 '잉크 및 필기 서비스'와 '데스크톱 체험'을 선택하고 팝업된 대화 상자에서 [확인]을 클릭합니다.



6. [다음]을 선택하고 [설치]를 클릭합니다. 설치가 완료되면 인터페이스의 안내에 따라 서버를 재시작합니다.

7.

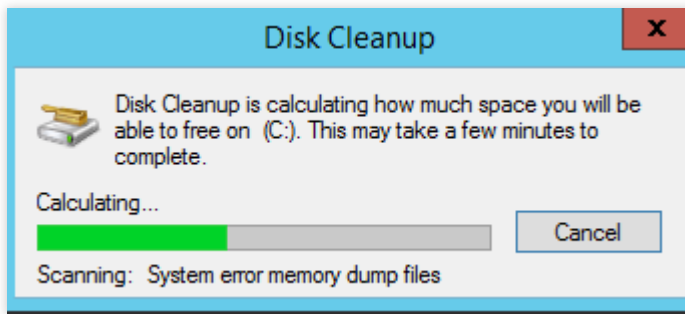


모양을 클릭하고 오른쪽 상단의



모양을 클릭합니다. 검색 창에 '디스크 정리'를 입력하여 검색합니다.

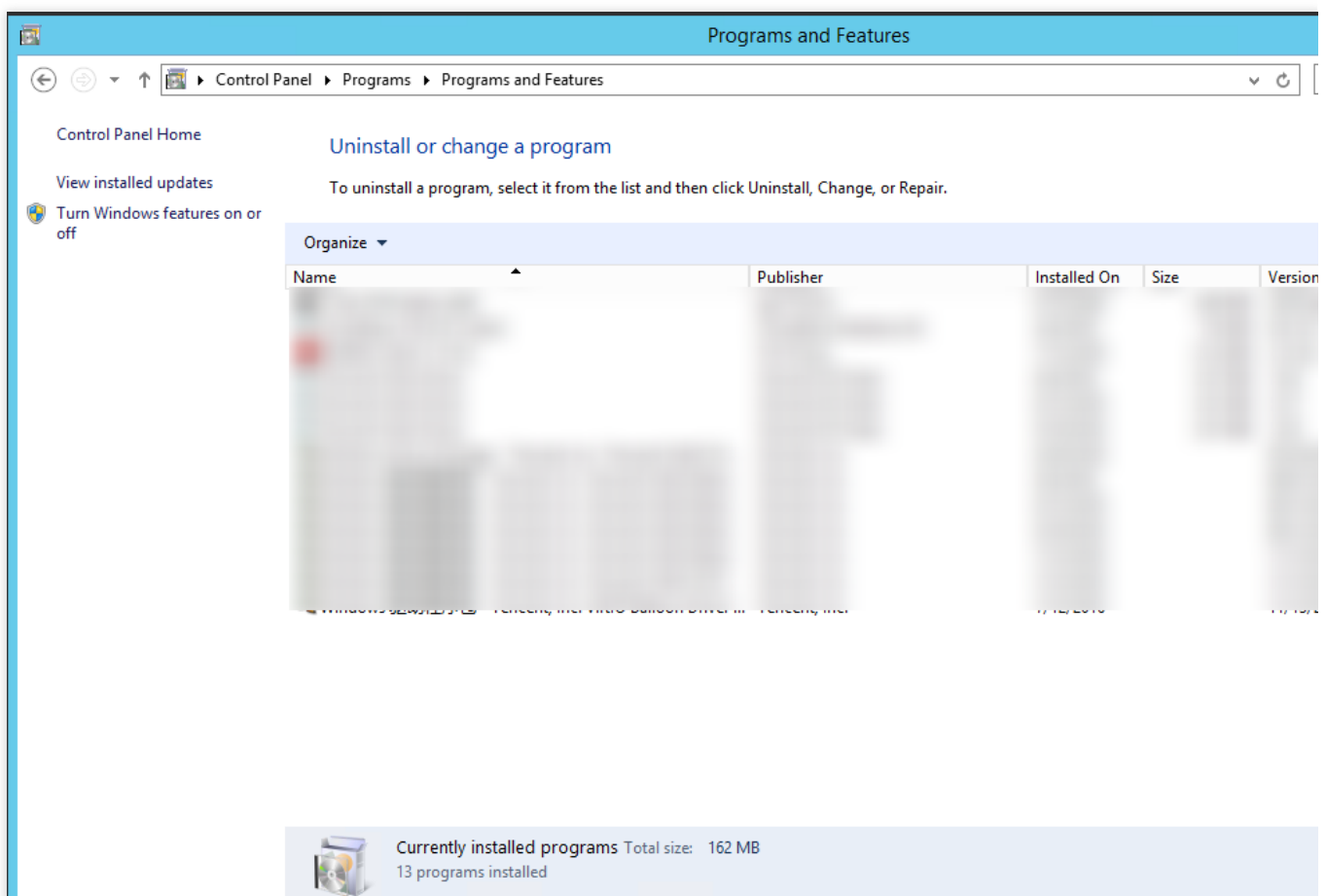
8. 아래 이미지와 같이, 팝업된 '디스크 정리' 창에서 해당하는 디스크를 선택한 뒤 정리를 시작합니다.



일상적인 디스크 점검

정기적인 응용 프로그램 정리

아래 이미지와 같이 '제어판'의 '프로그램 삭제'에서 사용하지 않는 응용 프로그램을 삭제할 수 있습니다.

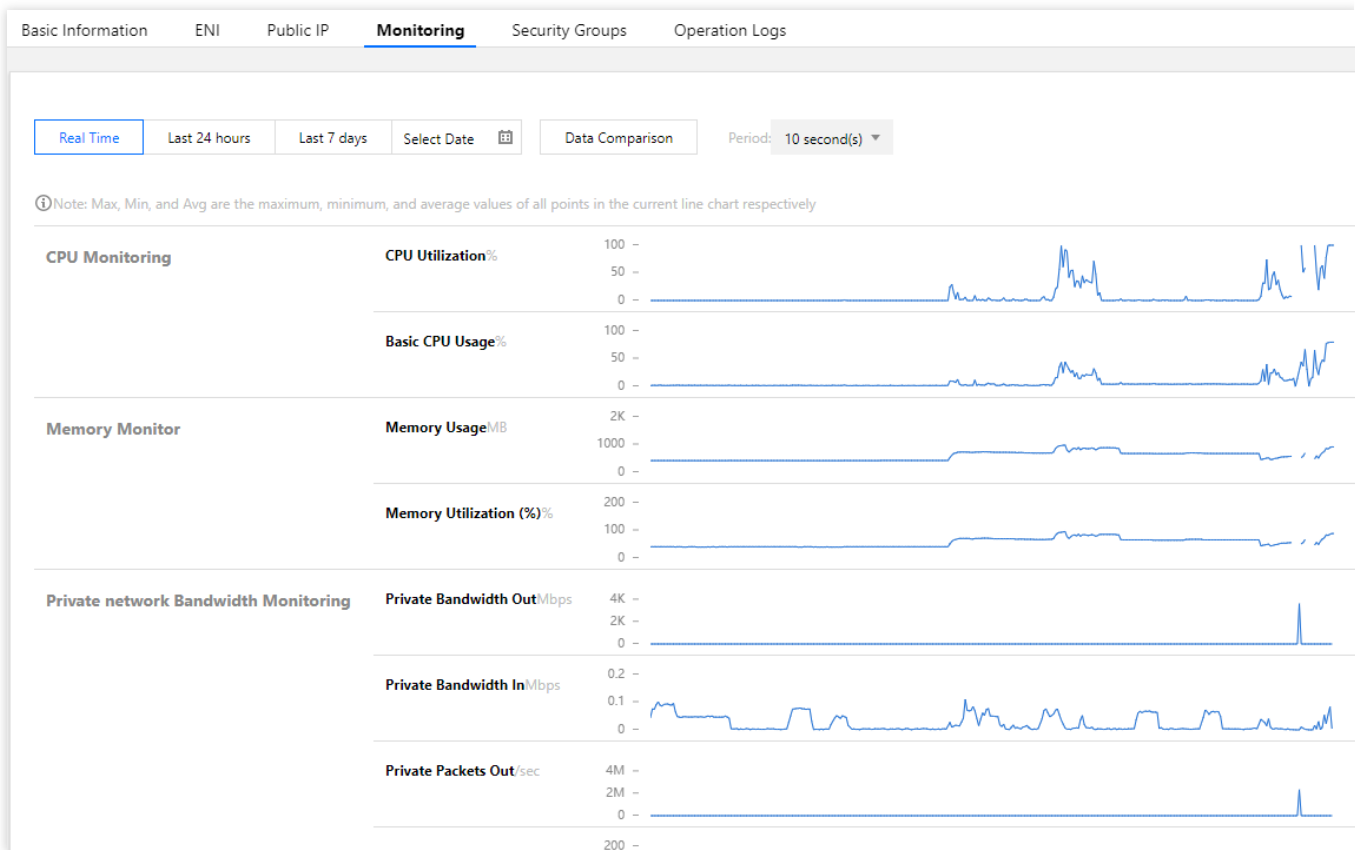


콘솔에서 디스크 사용 현황 조회

Tencent Cloud에서는 CVM 생성 시 클라우드 모니터링 서비스를 활성화하도록 기본 설정되어 있습니다. 따라서 콘솔에서 CVM 디스크 사용 현황을 조회할 수 있으며, 이에 대한 과정은 아래와 같습니다.

1. [CVM 콘솔](#)에 로그인하여 Instance List 페이지로 이동합니다.
2. 조회할 인스턴스 ID를 선택해 해당 인스턴스 상세 페이지로 이동합니다.

3. 아래 이미지와 같이 인스턴스 상세 페이지에서 [모니터링] 탭을 선택하면 해당 인스턴스의 디스크 사용 현황을 조회할 수 있습니다.



Linux 인스턴스에서 수동으로 커널 변경

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

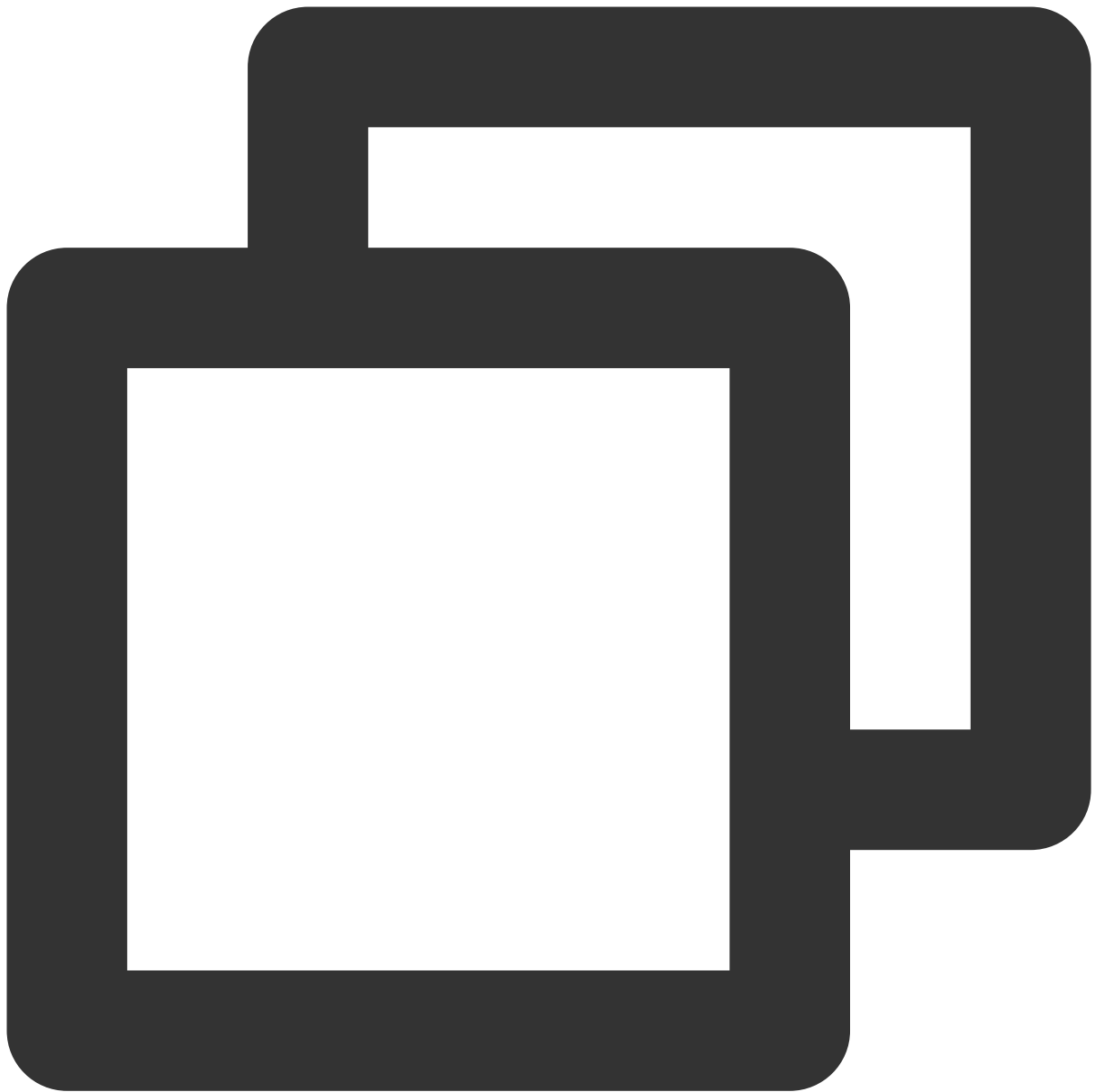
Bottleneck Bandwidth and Round-trip propagation time(BBR)은 Google이 2016년 개발한 TCP 혼잡 방지 알고리즘으로 Linux 서버의 처리량을 현저히 향상시키고 TCP 연결 딜레이를 줄일 수 있습니다. BBR을 활성화하려면 Linux 커널 4.10 이후 버전이 필요하므로, Linux 서버 커널이 4.10 이전 버전이면 이 글을 참고하여 작업을 진행할 수 있습니다.

본문에서는 CentOS 7.5 운영 체제의 CVM을 예로 들어 Linux 시스템에서 수동으로 커널을 교체하고 BBR을 활성화하는 방법을 안내합니다.

작업 순서

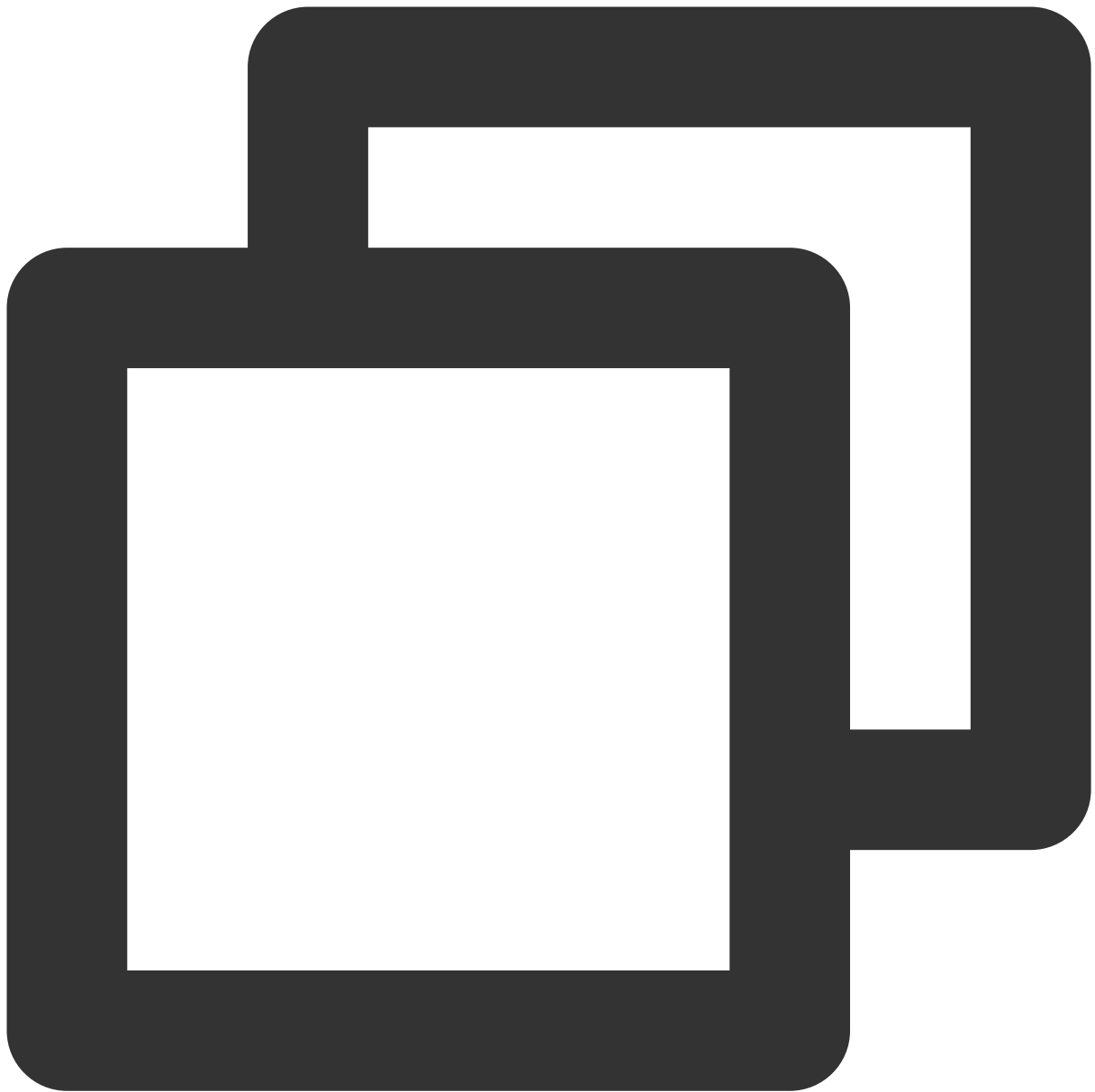
커널 패키지 업데이트

1. 다음 명령어를 실행하여 현재 Kernel 버전을 확인합니다.



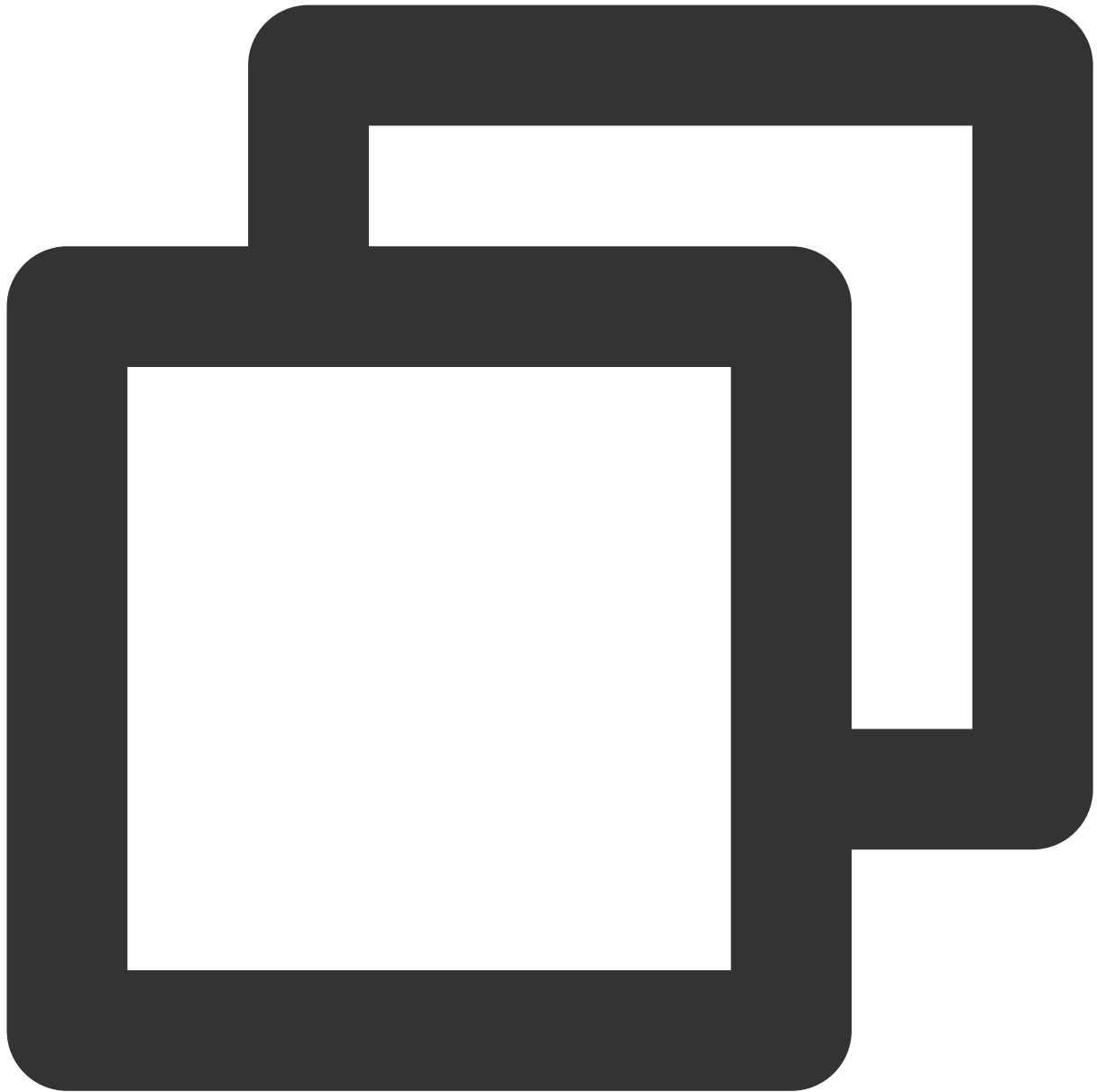
```
uname -r
```

2. 다음 명령어를 실행하여 소프트웨어 패키지를 업데이트합니다.



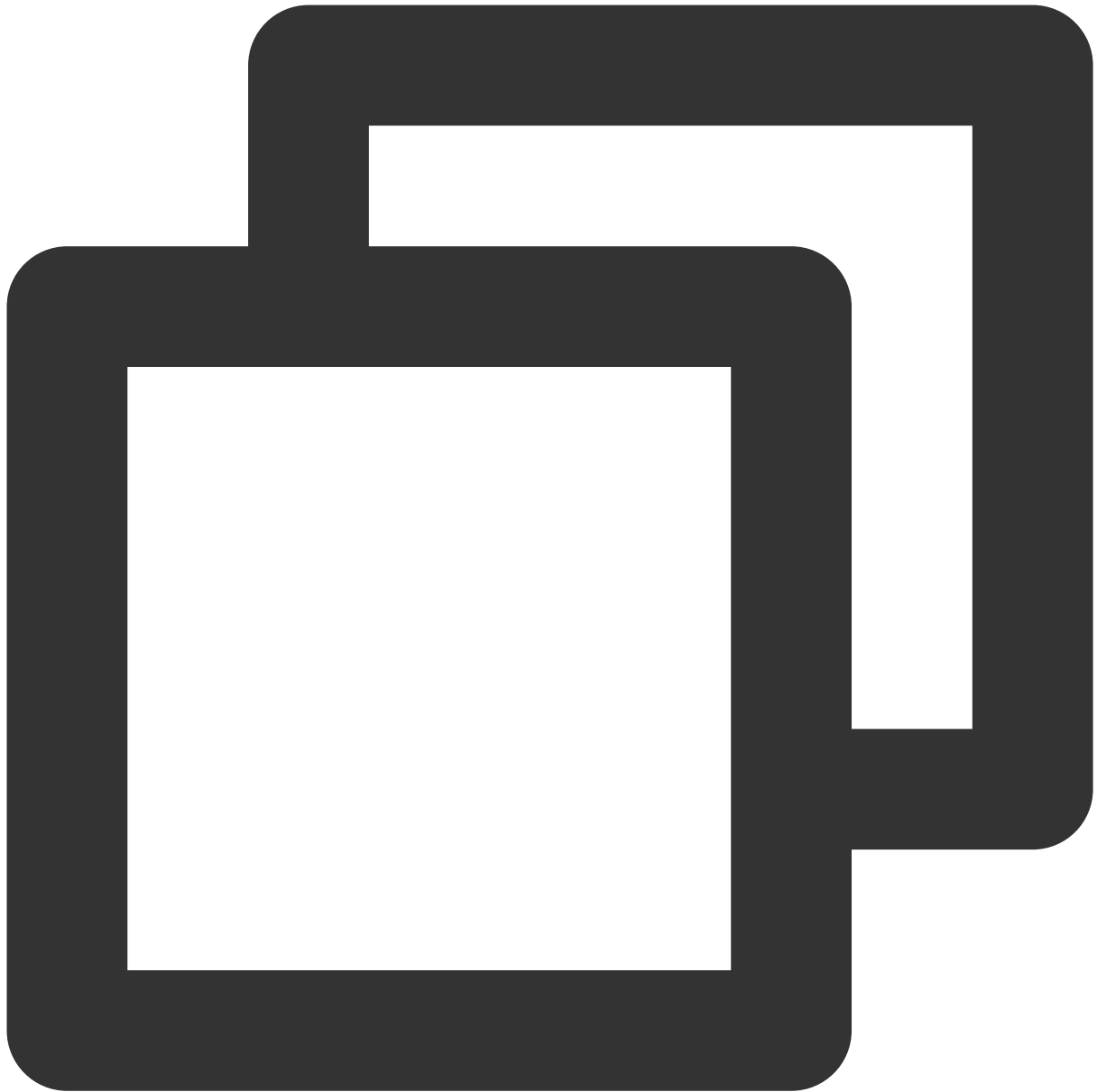
```
yum update -y
```

3. 다음 명령어를 실행하여 ELRepo 공개키를 가져옵니다.



```
rpm --import https://www.elrepo.org/RPM-GPG-KEY-elrepo.org
```

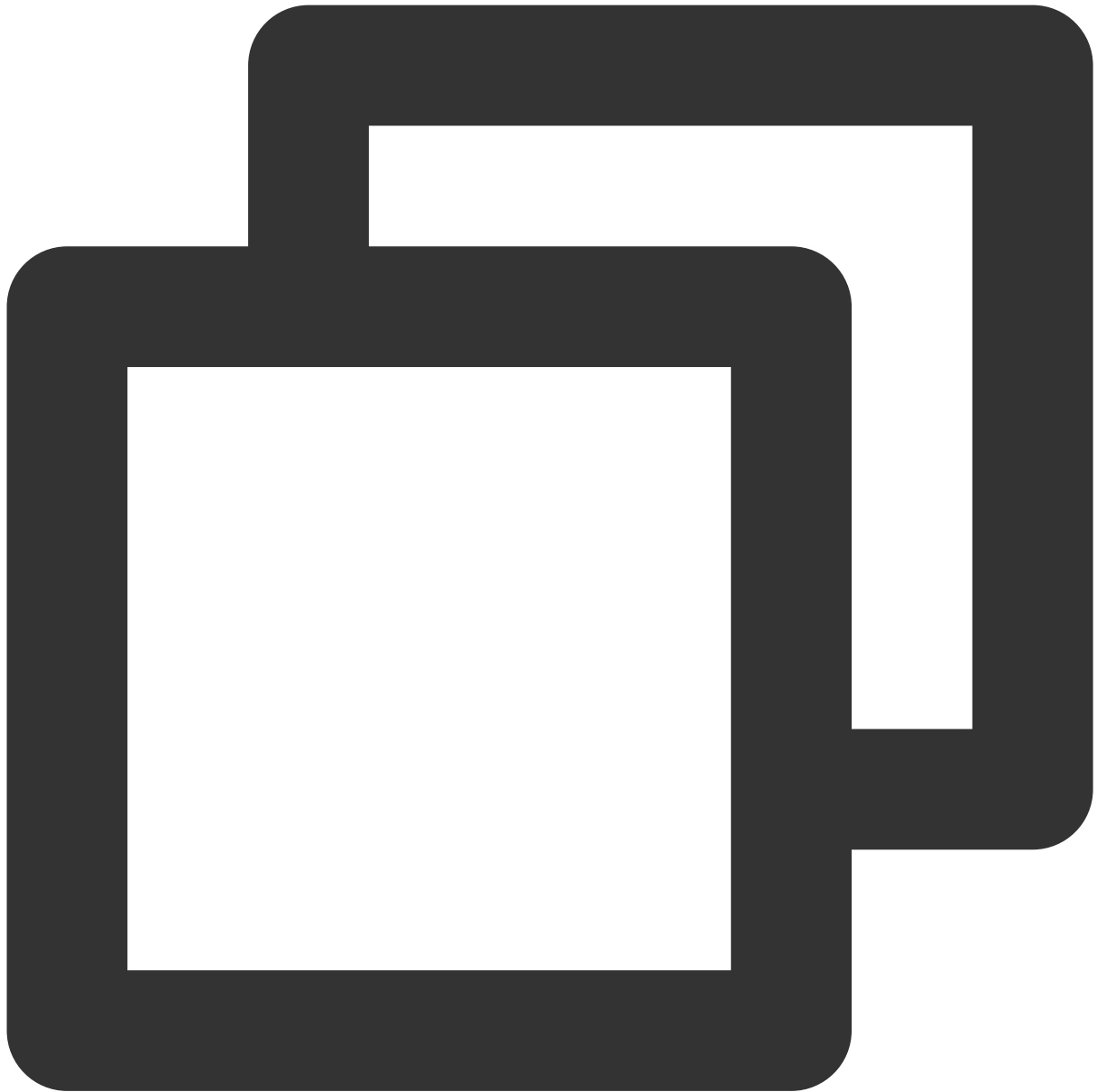
4. 다음 명령어를 실행하여 ELRepo의 yum 소스를 설치합니다.



```
yum install https://www.elrepo.org/elrepo-release-7.0-4.el7.elrepo.noarch.rpm
```

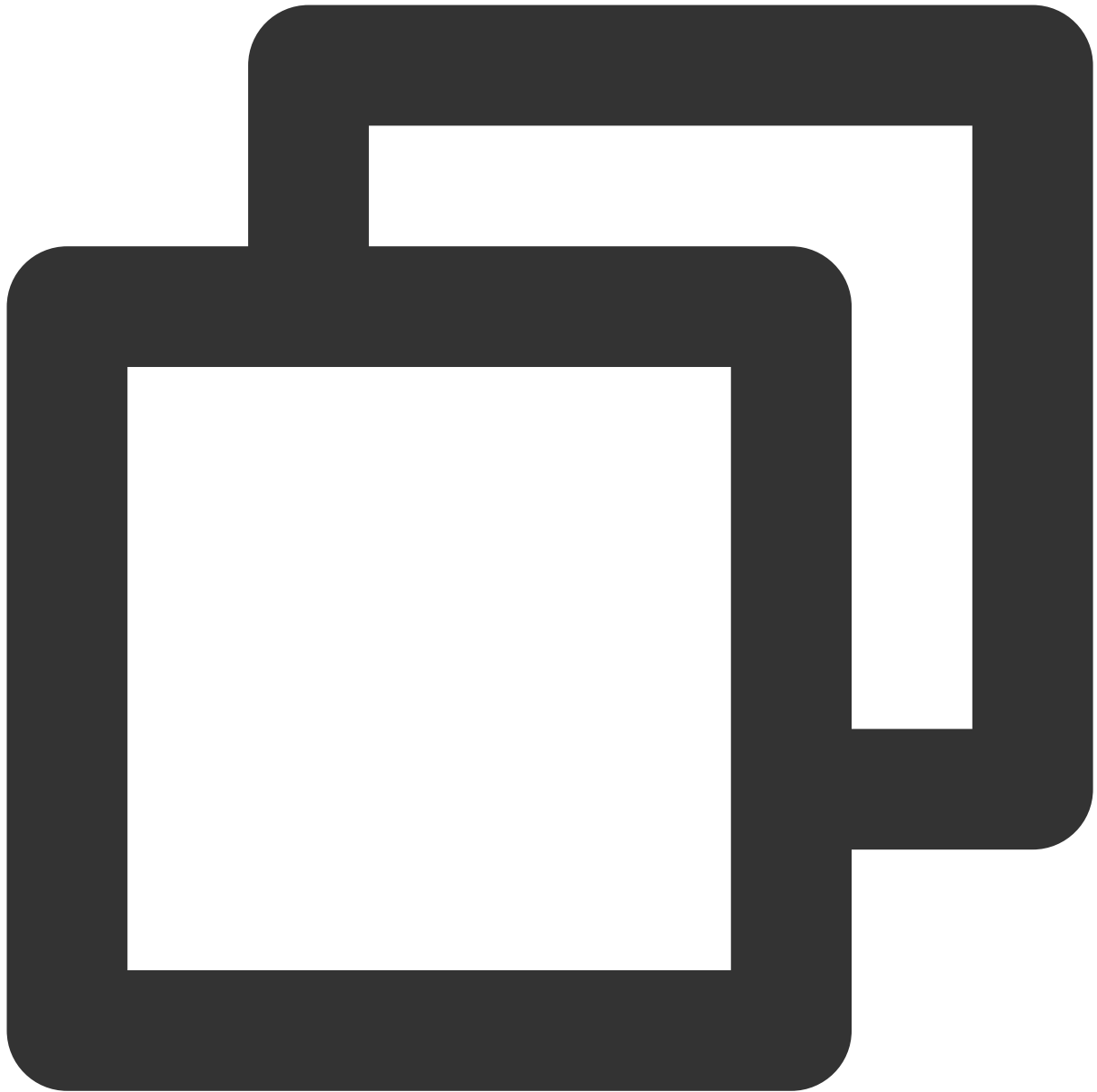
신규 커널 설치

1. 다음 명령어를 실행하여 ELRepo 리포지토리에서 현재 시스템이 지원하는 커널 패키지를 확인합니다.



```
yum --disablerepo="*" --enablerepo="elrepo-kernel" list available
```

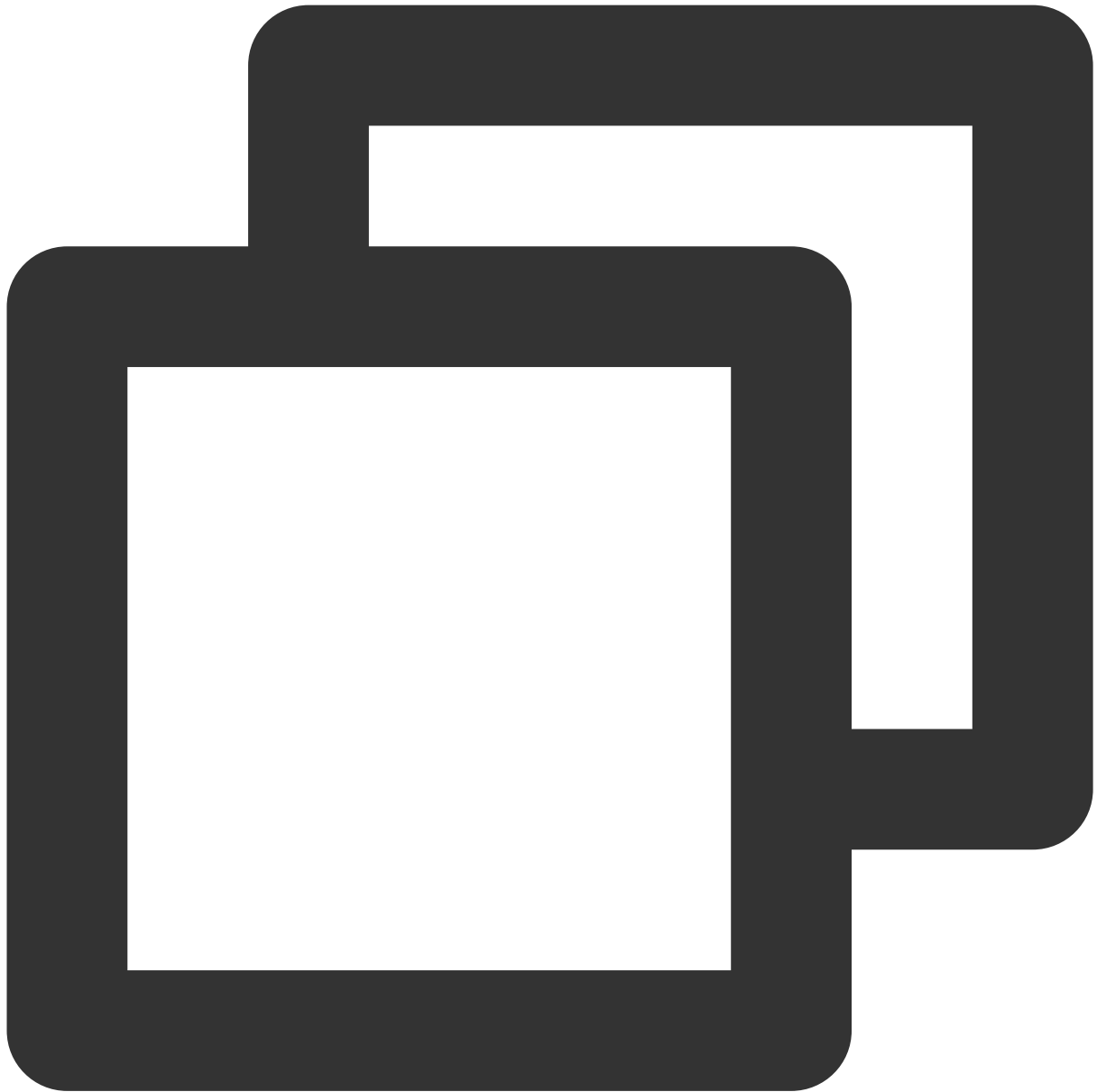
2. 다음 명령어를 실행하여 최신 메인 라인 안정 커널을 설치합니다.



```
yum --enablerepo=elrepo-kernel install kernel-ml
```

grub 설정 변경

1. 다음 명령어를 실행하여 `/etc/default/grub` 파일을 엽니다.



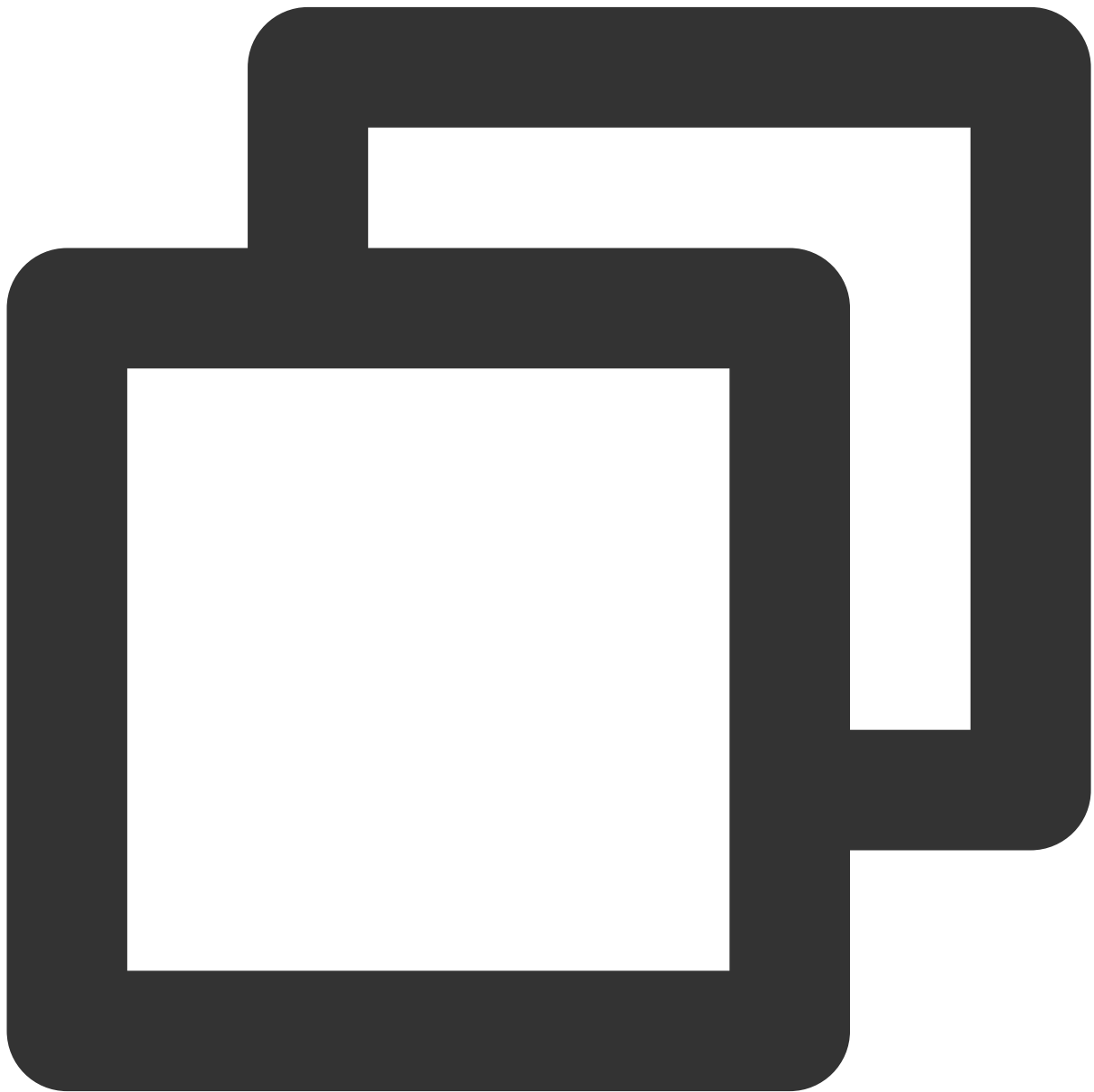
```
vim /etc/default/grub
```

2. **i**를 눌러 편집 모드로 전환하고 `GRUB_DEFAULT=saved` 를 `GRUB_DEFAULT=0` 으로 변경합니다.

```
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=0
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL="serial console"
GRUB_TERMINAL_OUTPUT="serial console"
GRUB_CMDLINE_LINUX="crashkernel=auto console=ttyS0 console=tty0 panic=5 net.ifnames=0 biosdevname=0"
GRUB_DISABLE_RECOVERY="true"
GRUB_SERIAL_COMMAND="serial --speed=9600 --unit=0 --word=8 --parity=no --stop=1"
```

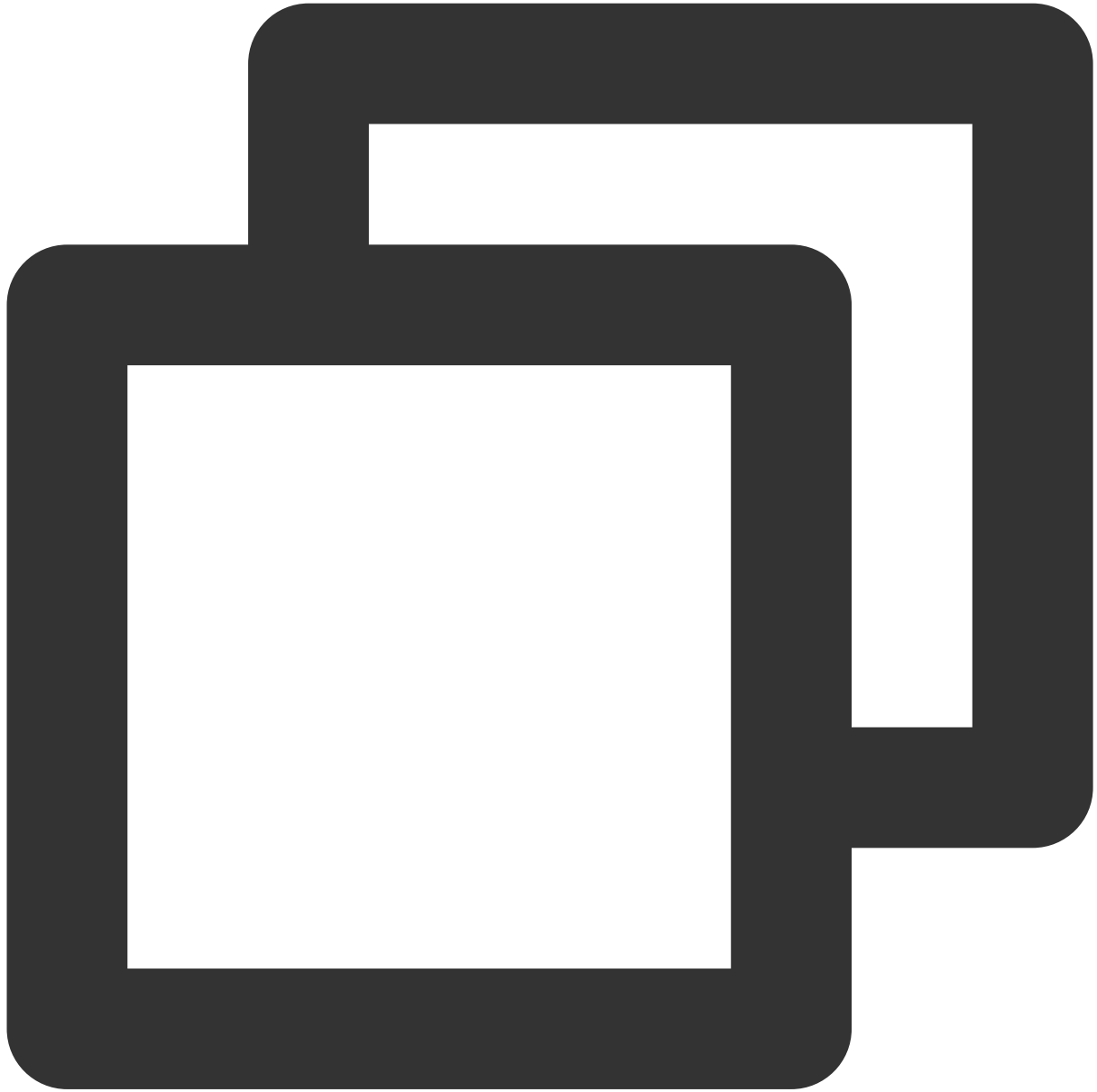
3. **Esc**를 누르고 **:wq**를 입력하여 파일을 저장하고 뒤로 돌아갑니다.

4. 다음 명령어를 실행하여 Kernel 구성을 다시 생성합니다.



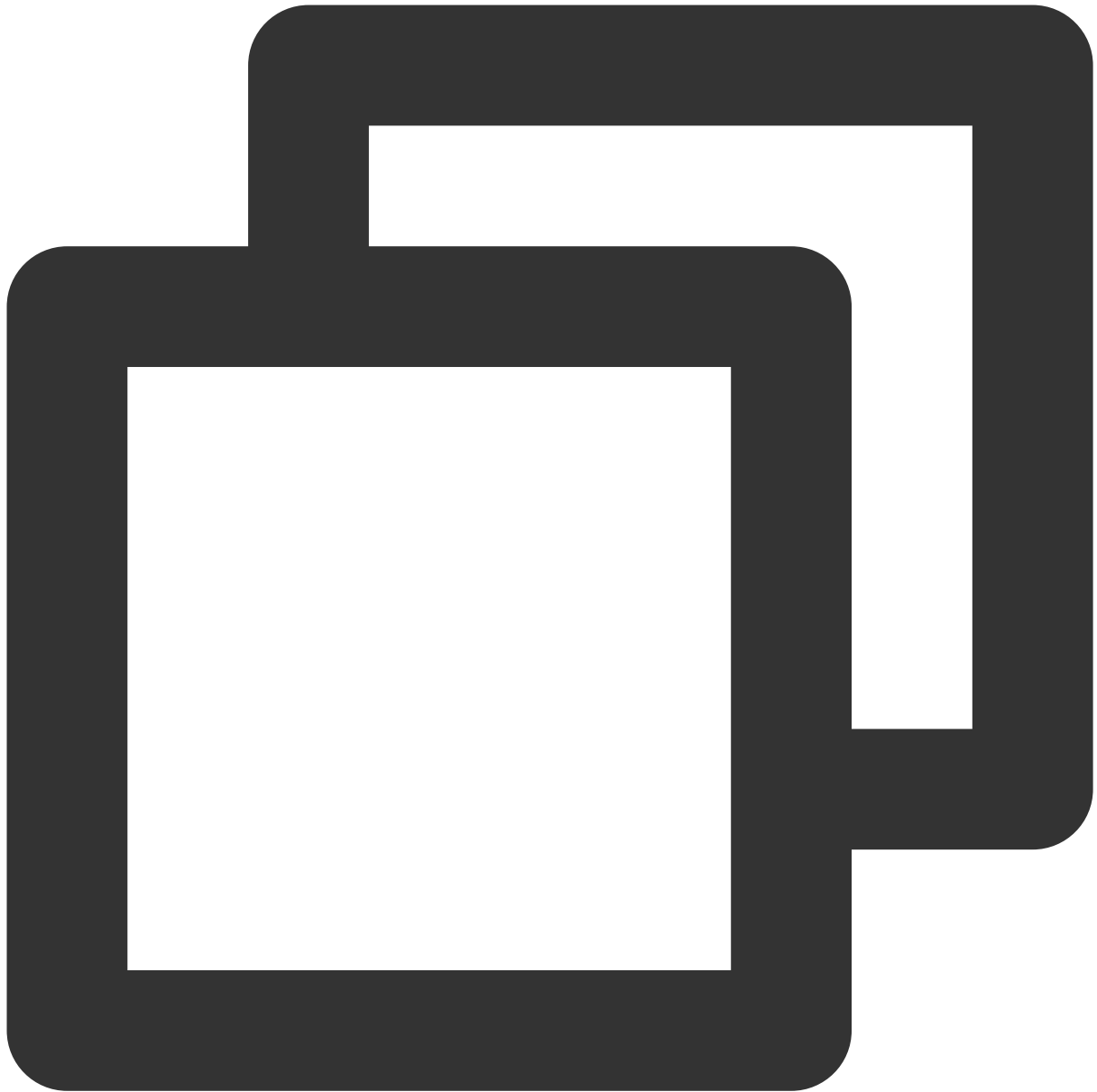
```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

5. 아래의 명령어를 실행하여 시스템을 재시작합니다.



```
reboot
```

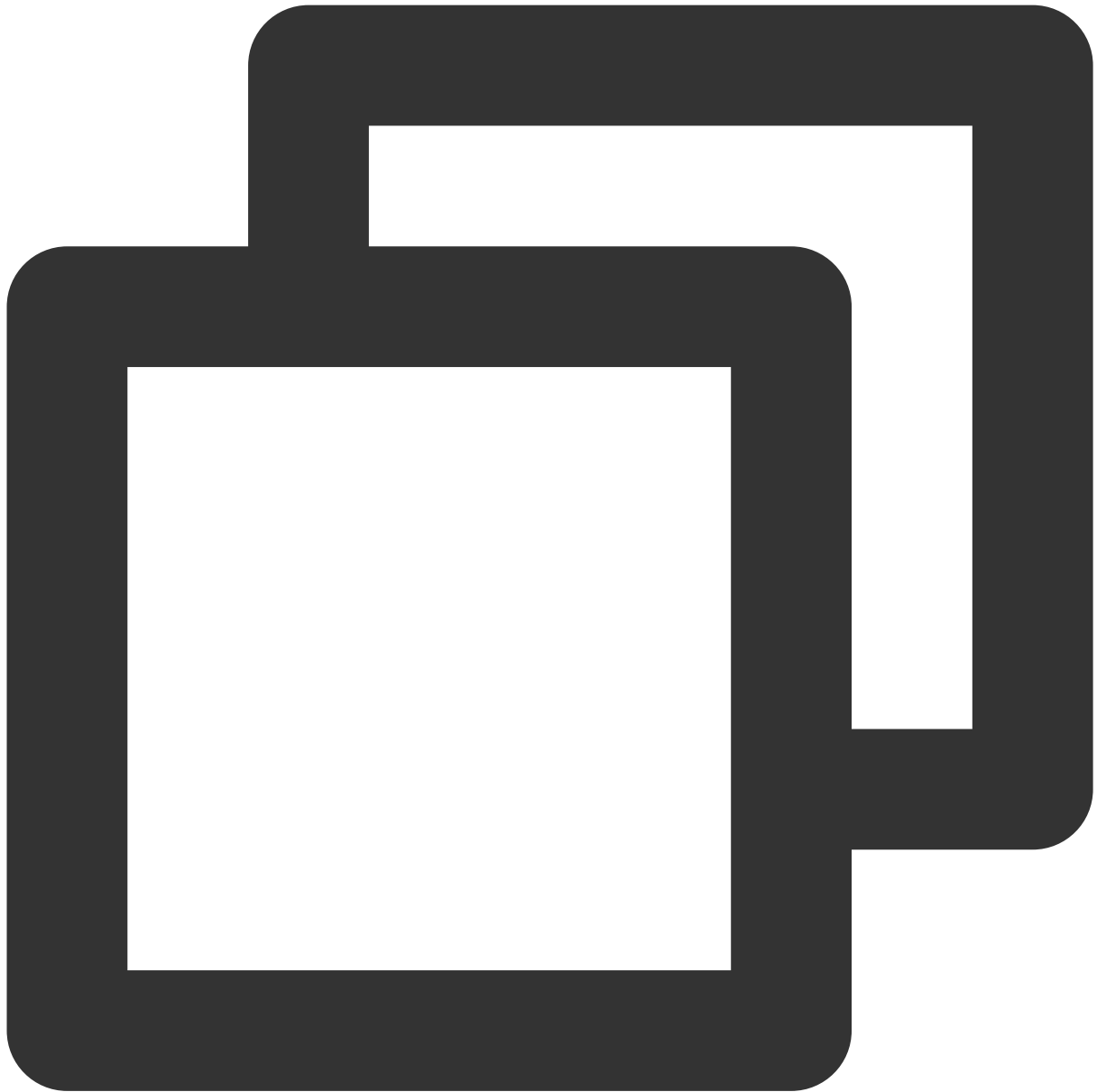
6. 다음 명령어를 실행하여 변경 성공 여부를 확인합니다.



```
uname -r
```

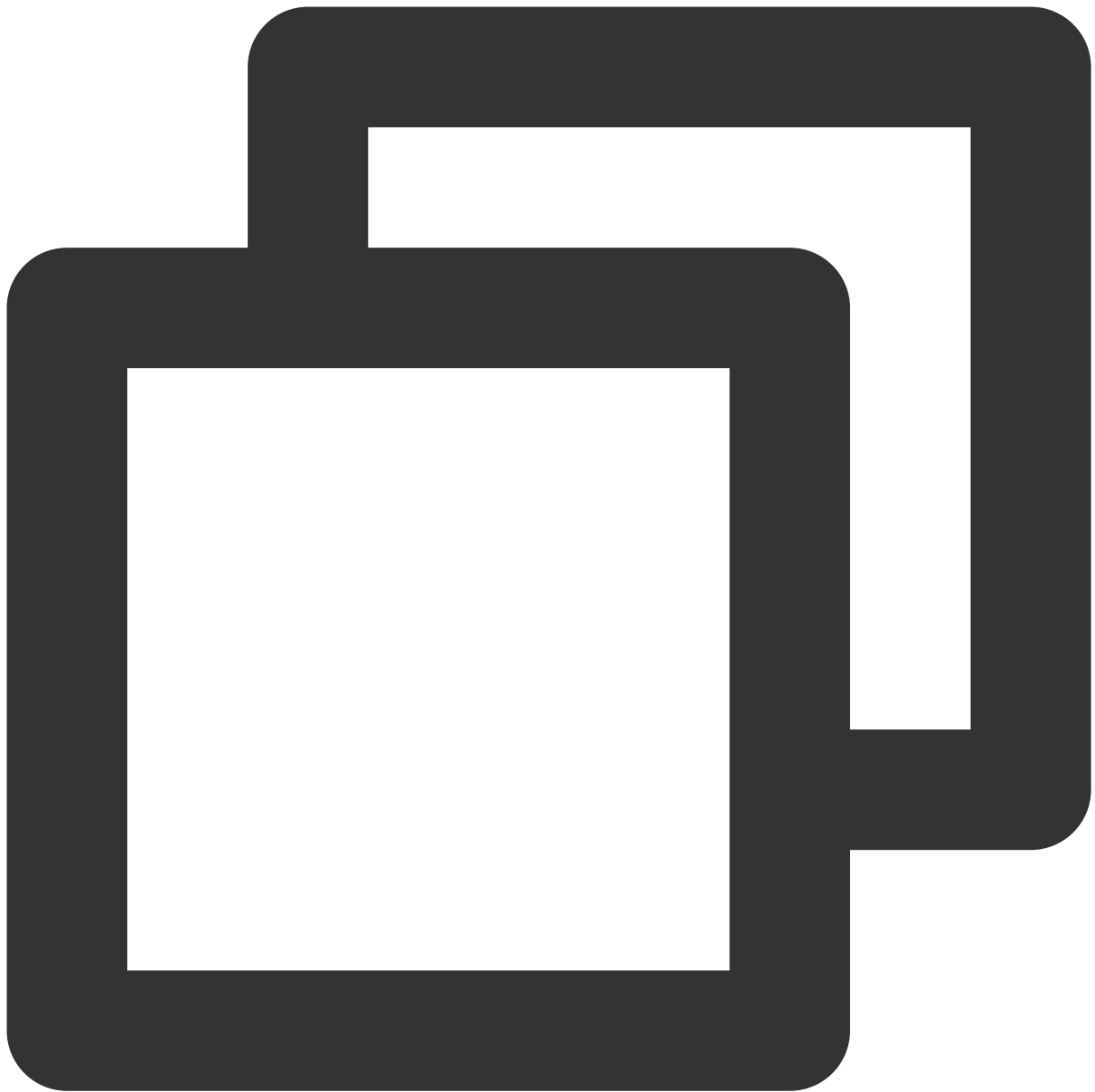
불필요한 커널 삭제

1. 다음 명령어를 실행하여 모든 Kernel을 조회합니다.



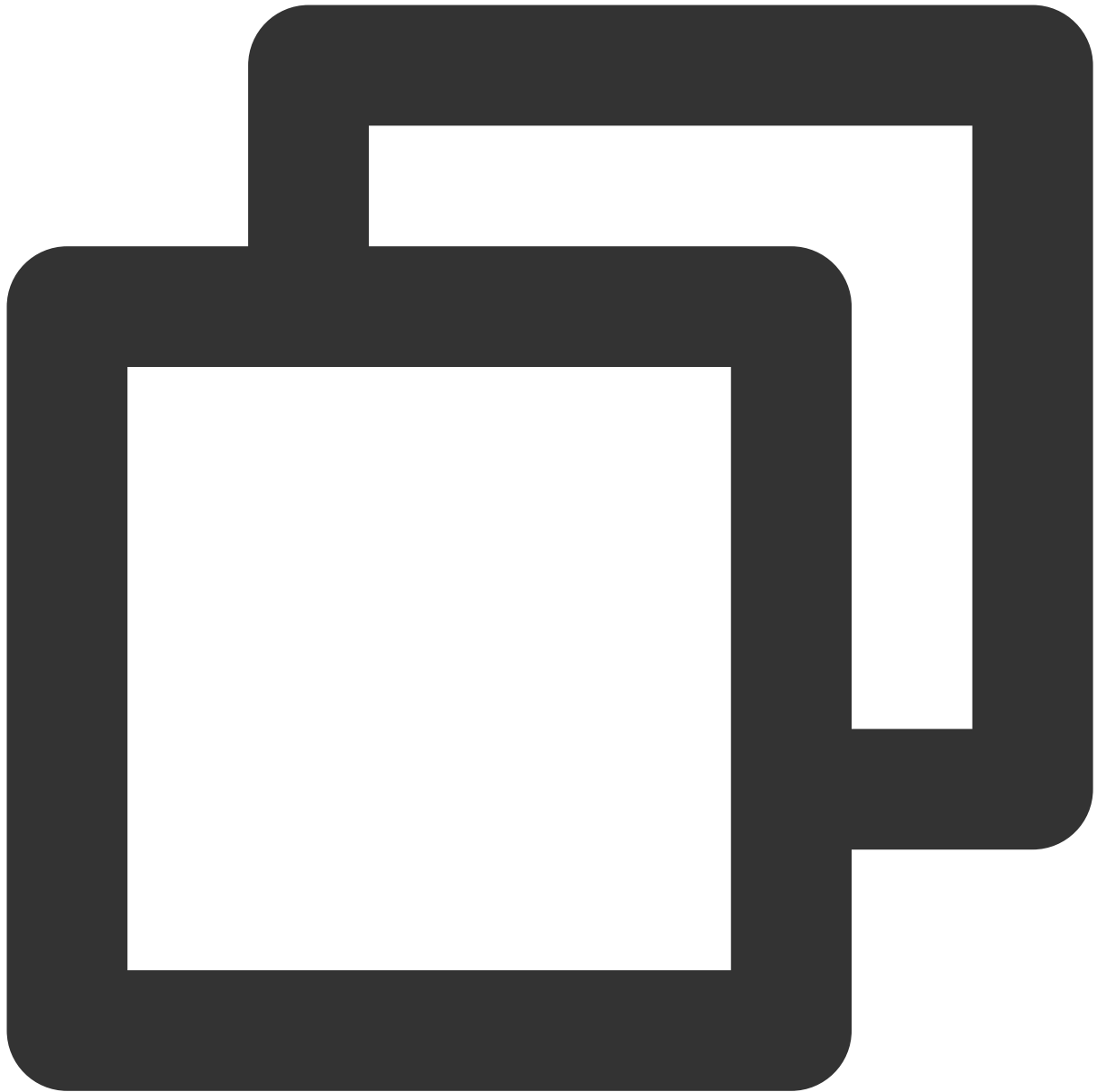
```
rpm -qa | grep kernel
```

2. 다음 명령어를 실행하여 이전 버전의 커널을 삭제합니다.



```
yum remove kernel-old_kernel_version
```

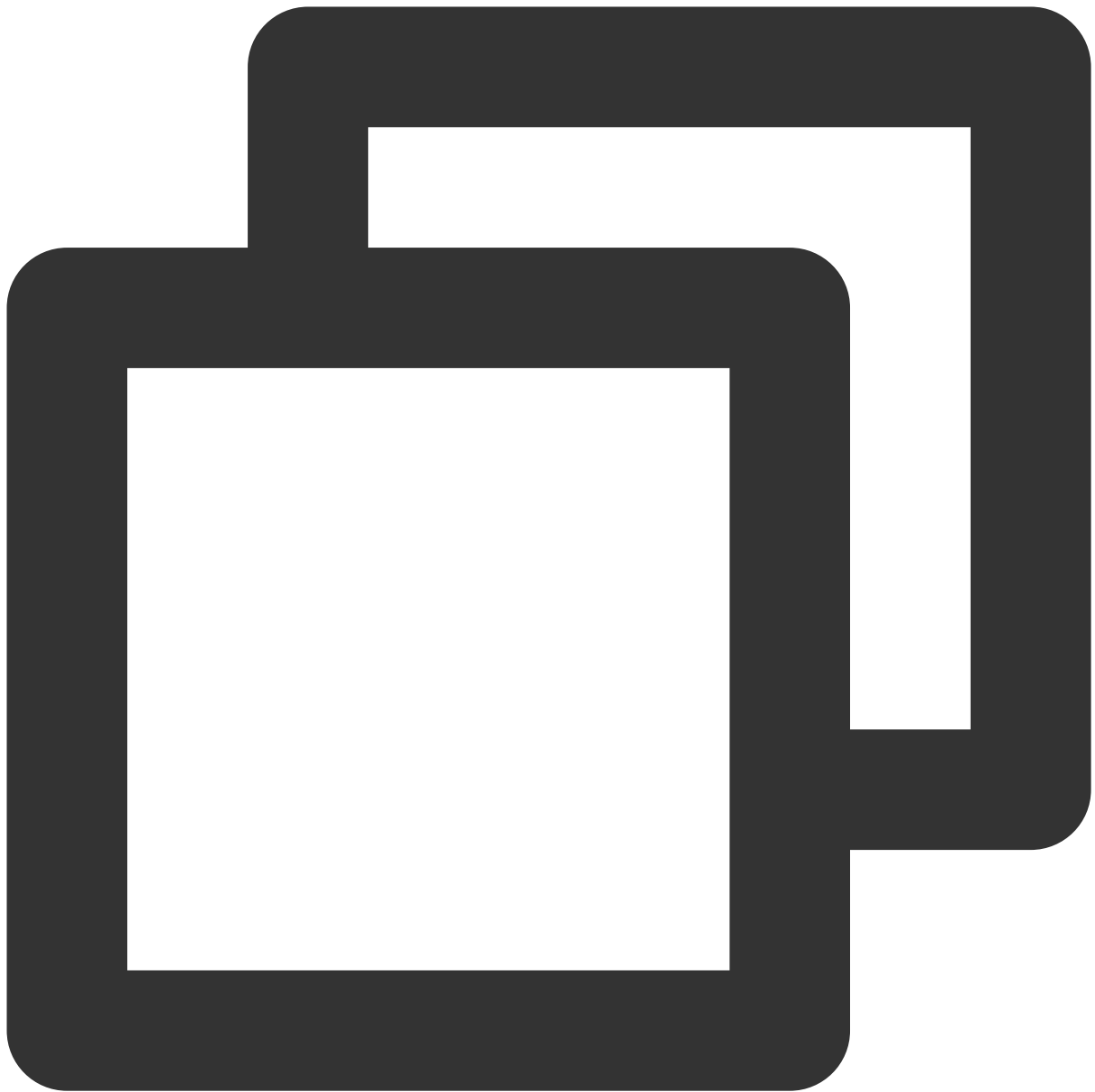
예시:



```
yum remove kernel-3.10.0-957.el7.x86_64
```

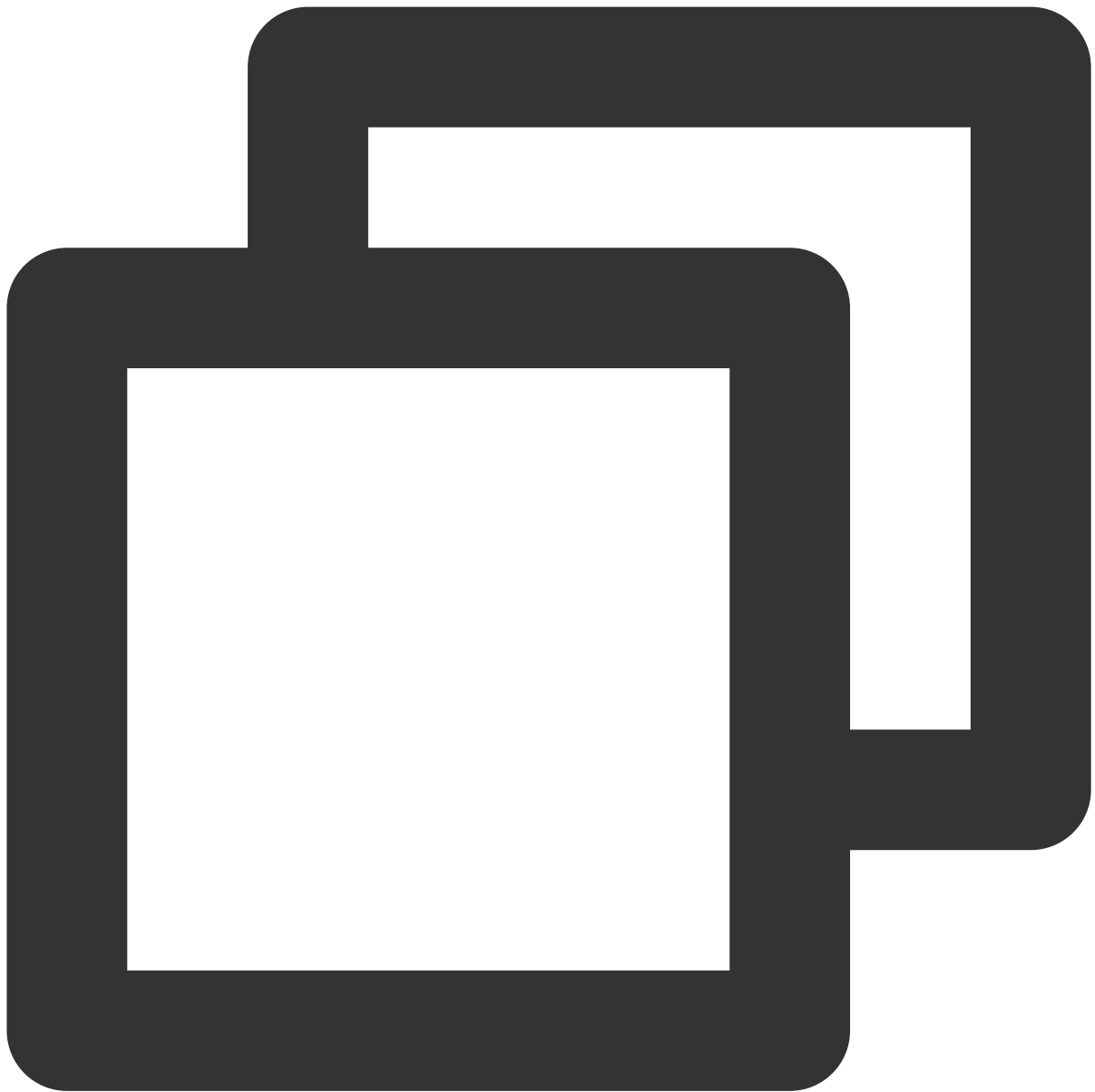
BBR 활성화

1. 다음 명령어를 실행하여 `/etc/sysctl.conf` 파일을 편집합니다.



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

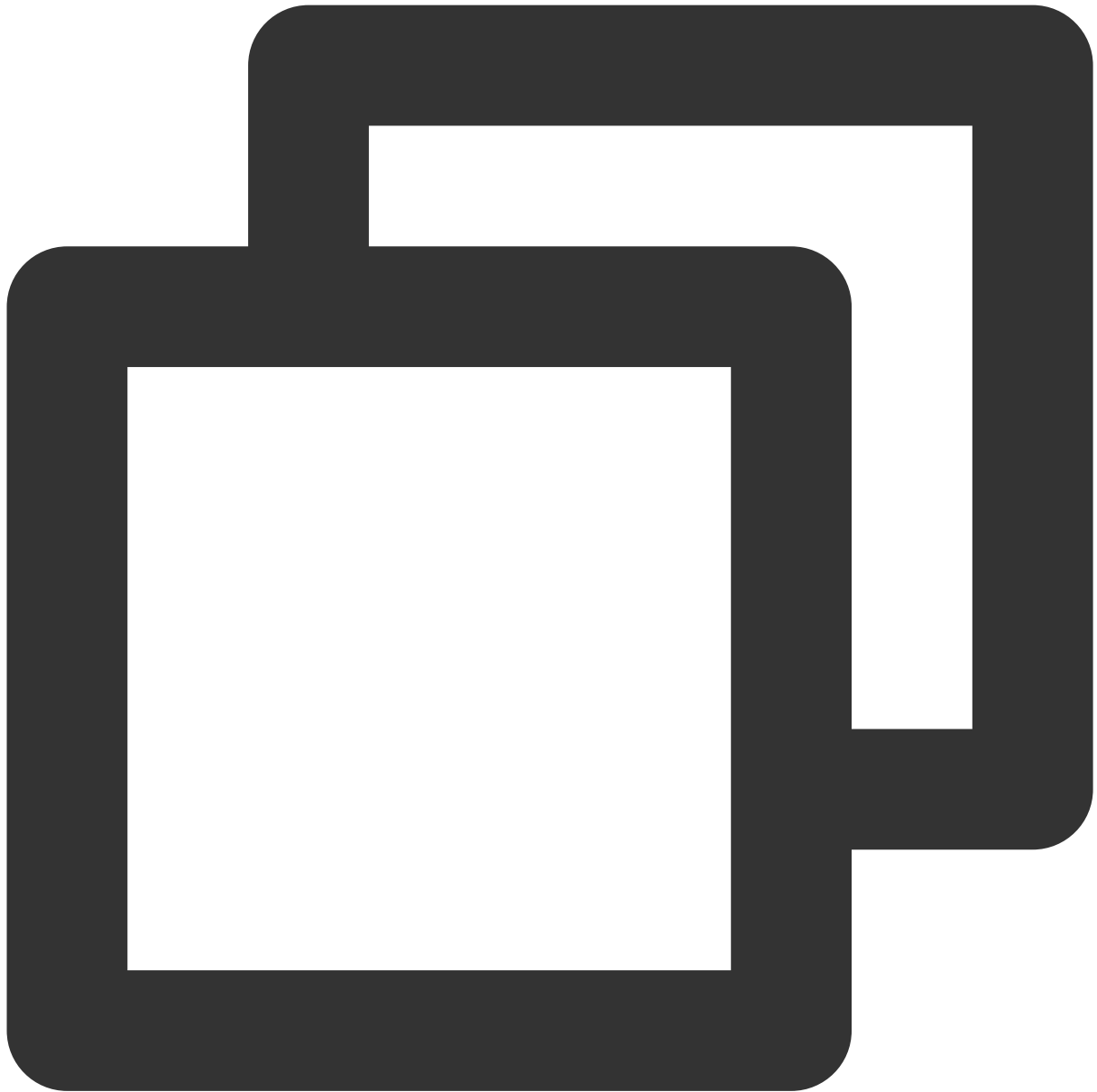
2. **i**를 눌러 편집 모드로 전환하고 다음을 추가합니다.



```
net.core.default_qdisc=fq
net.ipv4.tcp_congestion_control=bbr
```

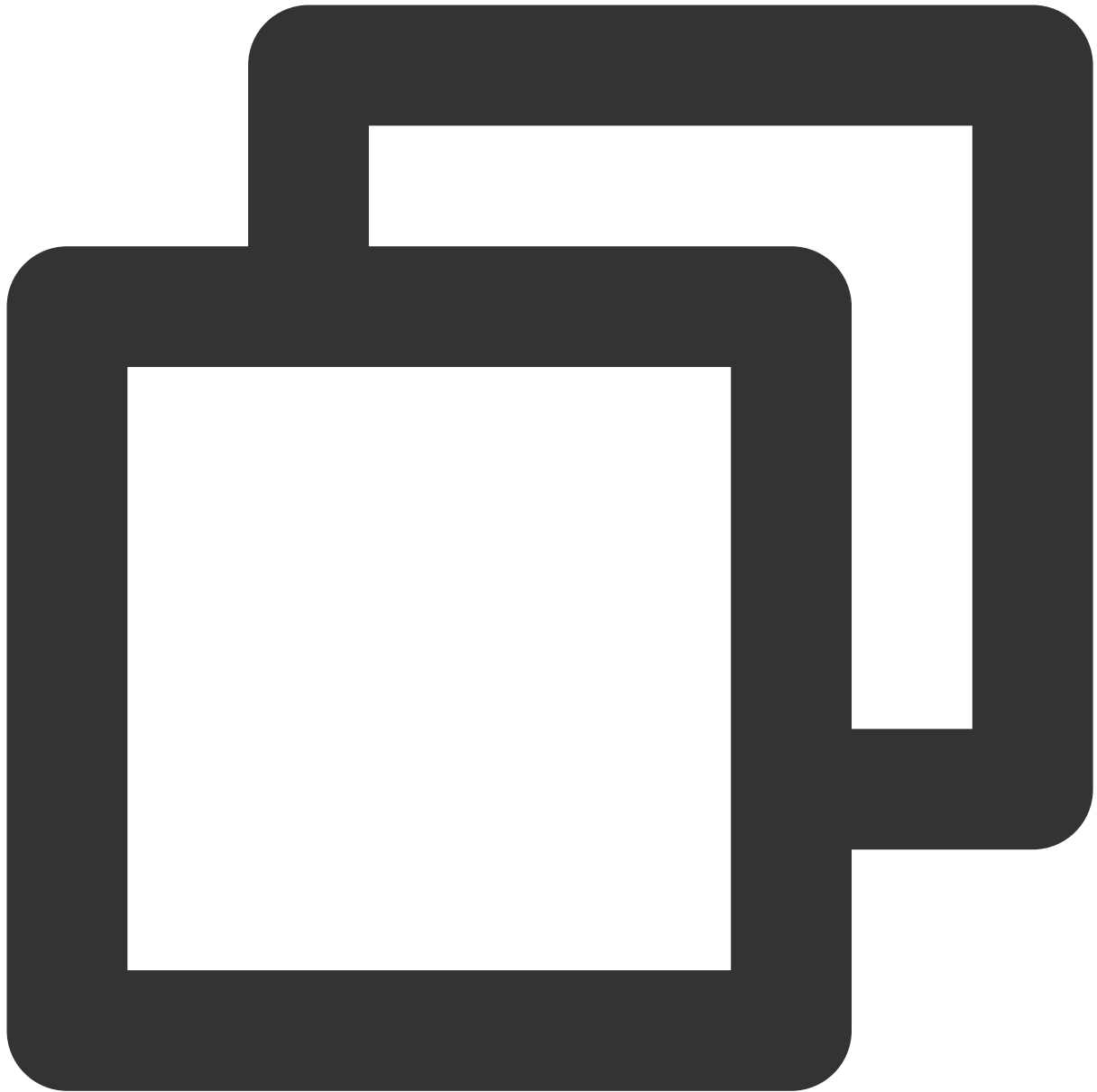
3. **Esc**를 누르고 **:wq**를 입력하여 파일을 저장하고 뒤로 돌아갑니다.

4. 다음 명령어를 실행하여 `/etc/sysctl.conf` 구성 파일에서 커널 매개변수 설정을 로딩합니다.

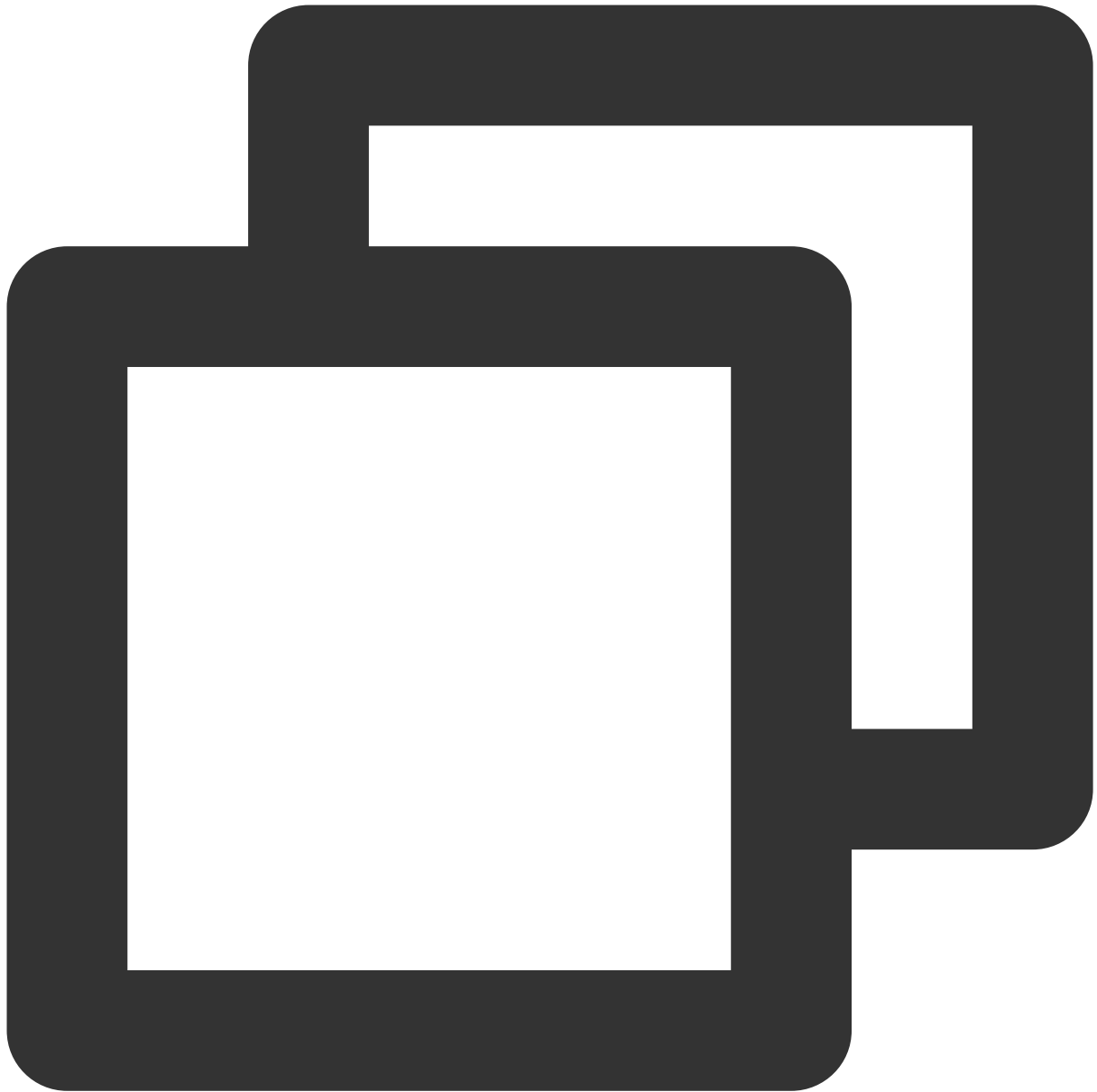


```
sysctl -p
```

5. 다음 명령어를 순서대로 실행하여 BBR이 성공적으로 활성화 되었는지 확인합니다.

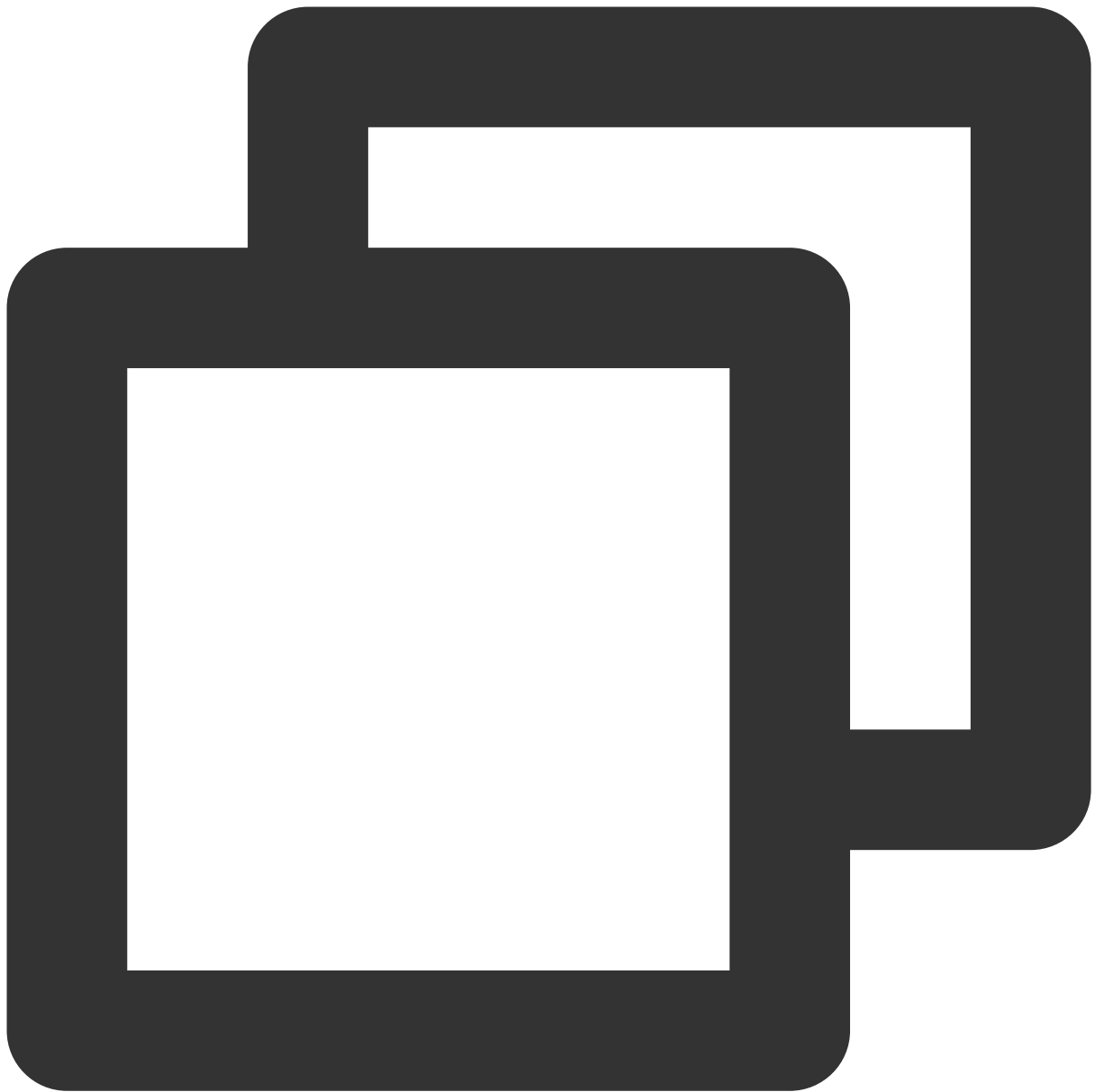


```
sysctl net.ipv4.tcp_congestion_control  
# 설정이 성공적으로 완료되면 다음이 표시됩니다.  
# net.ipv4.tcp_congestion_control = bbr
```

```
sysctl net.ipv4.tcp_available_congestion_control  
# 설정이 성공적으로 완료되면 다음이 표시됩니다.  
# net.ipv4.tcp_available_congestion_control = reno cubic bbr
```

6. 다음 명령어를 실행하여 커널 모듈이 로딩되었는지 확인합니다.



```
lsmod | grep bbr
```

다음 정보가 반환되면 성공적으로 활성화된 것입니다.

```
[root@VM_0_51_centos ~]# lsmod | grep bbr
tcp_bbr          20480  1
```

CVM에서 Windows 기반 AD 도메인 설정

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

AD(Active Directory)는 Microsoft 서비스의 핵심 컴포넌트입니다. AD는 사용자의 일괄 관리, 애플리케이션 배포 및 패치 업데이트와 같은 효율적인 관리를 실현할 수 있습니다. 많은 Microsoft 컴포넌트(예시: Exchange) 및 장애 조치 클러스터에도 AD 도메인 환경이 필요합니다. 본 문서에서는 Windows Server 2012 R2 데이터센터 버전 64비트 운영 체제를 예로 들어 AD 도메인을 구축하는 방법을 소개합니다.

전제 조건

2개의 Windows Cloud Server(CVM) 인스턴스가 도메인 컨트롤러(DC) 및 클라이언트(Client)로 생성되었습니다. 생성된 인스턴스는 다음 조건을 충족해야 합니다.

NTFS 파티션.

DNS 서비스 지원.

TCP/IP 프로토콜 지원.

인스턴스 네트워크 환경

네트워크 정보: 네트워크 유형은 VPC이며 스위치의 VPC IP 대역은 10.0.0.0/16입니다.

도메인 정보: 예시 도메인은 'example.com'입니다. DC로서의 CVM 인스턴스 IP 주소는 10.0.5.102이고 클라이언트로서의 CVM 인스턴스 IP 주소는 10.0.5.97입니다.

주의사항 :

AD 도메인 구축 후 CVM 인스턴스가 항상 동일한 IP 주소를 사용하는지 확인하십시오. 그렇지 않으면 IP 주소 변경으로 인해 액세스 예외가 발생합니다.

개념

AD(Active Directory)는 Microsoft 서비스의 핵심 구성 요소이며 관련 용어 및 개념은 다음과 같습니다.

DC: Domain Controllers, 도메인 컨트롤러.

DN: Distinguished Name, 고유 이름.

OU: Organizational Unit, 조직 단위.

CN: Canonical Name, 정식 이름.

SID: Security Identifier, 보안 식별자.

작업 단계

설명 :

기존 도메인 컨트롤러를 사용하여 사용자 정의 이미지를 만들어 새 도메인 컨트롤러를 배포하는 것은 권장되지 않습니다. 반드시 사용해야 하는 경우 사용자 정의 이미지를 생성하기 전에 새 인스턴스의 호스트 이름(hostname)과 인스턴스의 호스트 이름이 같아야 합니다. 그렇지 않으면 "서버의 보안 데이터베이스에 이 워크스테이션 신뢰 관계가 없습니다"라는 오류가 보고될 수 있습니다. 이 문제를 해결하기 위해 인스턴스 생성 후 동일한 호스트 이름으로 수정할 수도 있습니다.

AD 도메인 컨트롤러 배포

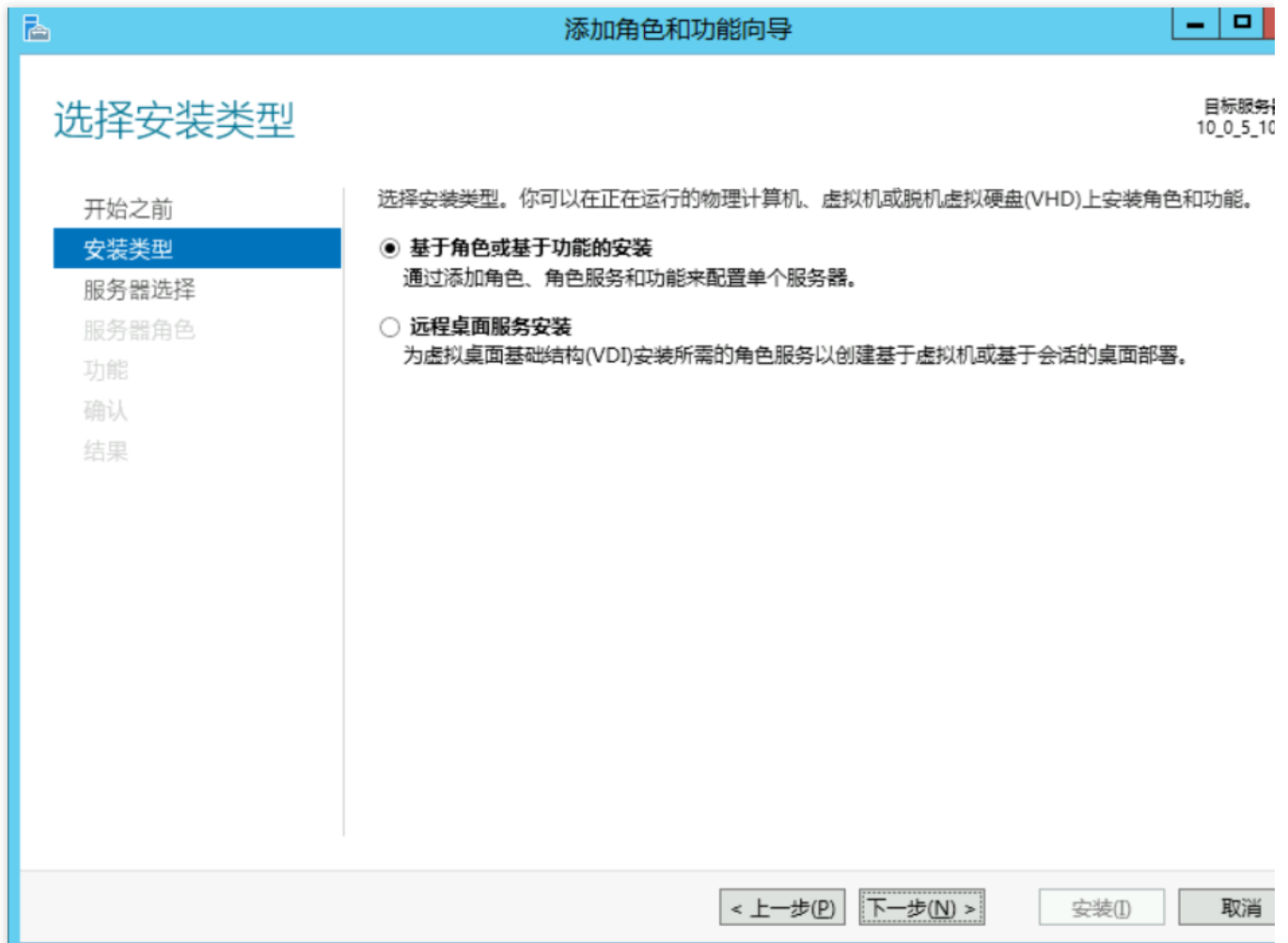
1. DC의 인스턴스로 로그인합니다. 자세한 내용은 [표준 방식으로 Windows 인스턴스에 로그인](#)을 참고하십시오.
2. 운영 체제 인터페이스에서



을(를) 클릭하고 서버 관리자를 엽니다.

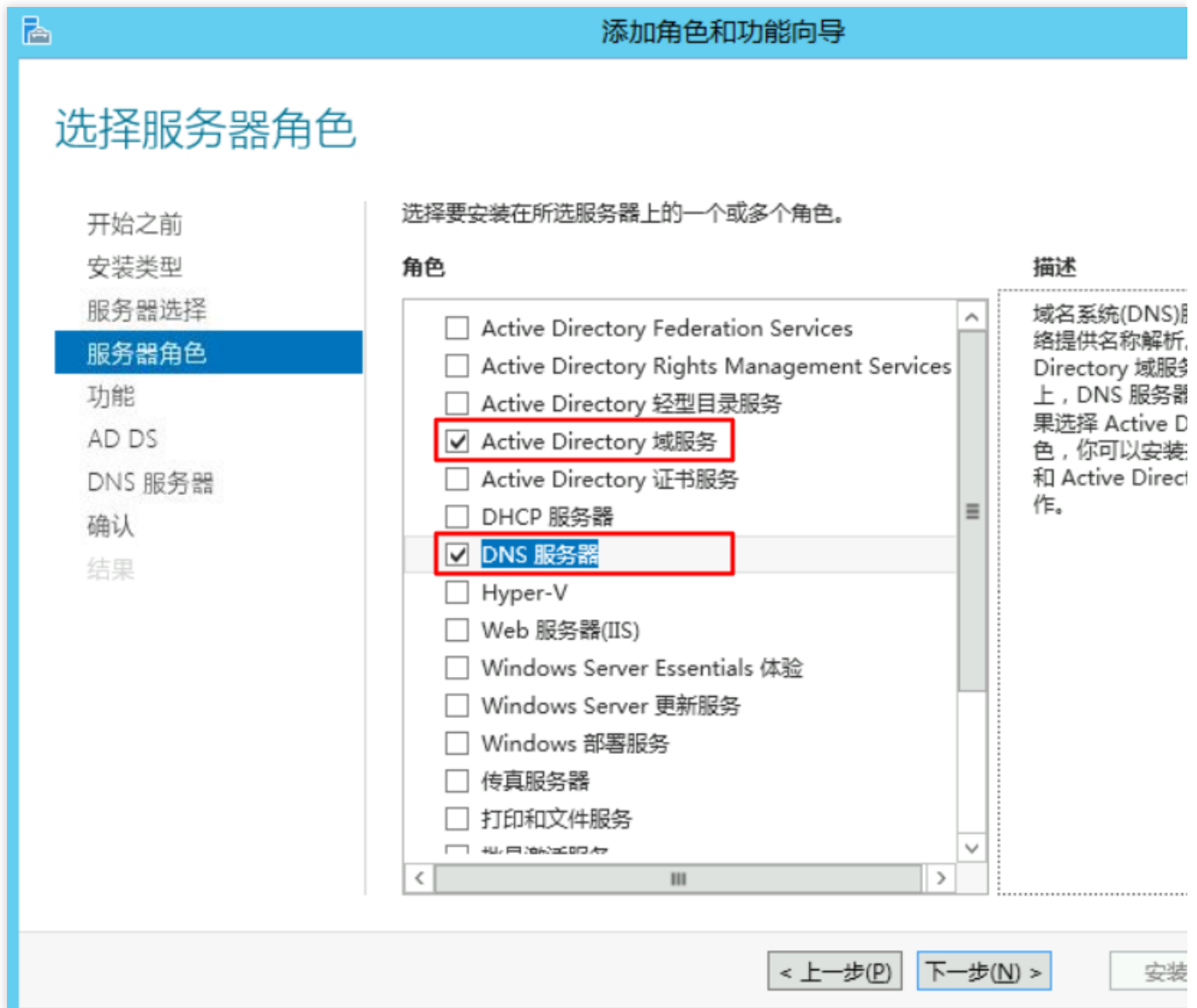
3. **역할 및 기능 추가**를 클릭하면 '역할 및 기능 추가 마법사' 창이 팝업됩니다.

4. 아래 이미지와 같이 '설치 유형 선택' 인터페이스에서 **역할 기반 또는 기능 기반 설치**를 선택하고, 다음 단계를 2회 연속 클릭합니다.



5. '인터페이스 역할 선택' 인터페이스에서 아래와 같이 'Active Directory 도메인 서비스'와 'DNS 서버'를 선택하고 팝업 창에서 **기능 추가** 및 **계속**을 클릭합니다.

이 단계에서는 동일한 인스턴스에 AD 도메인 서비스와 DNS 서비스를 배포하는 것을 예시로 사용합니다.



6. 기본 설정을 유지하고 **다음 단계**를 4회 연속 클릭합니다.

7. 정보 확인 페이지에서 **설치**를 클릭합니다.

설치가 완료되면 '역할 및 기능 추가' 대화 상자를 비활성화합니다.

8. 운영 체제 인터페이스에서



을(를) 클릭하고 서버 관리자를 엽니다.

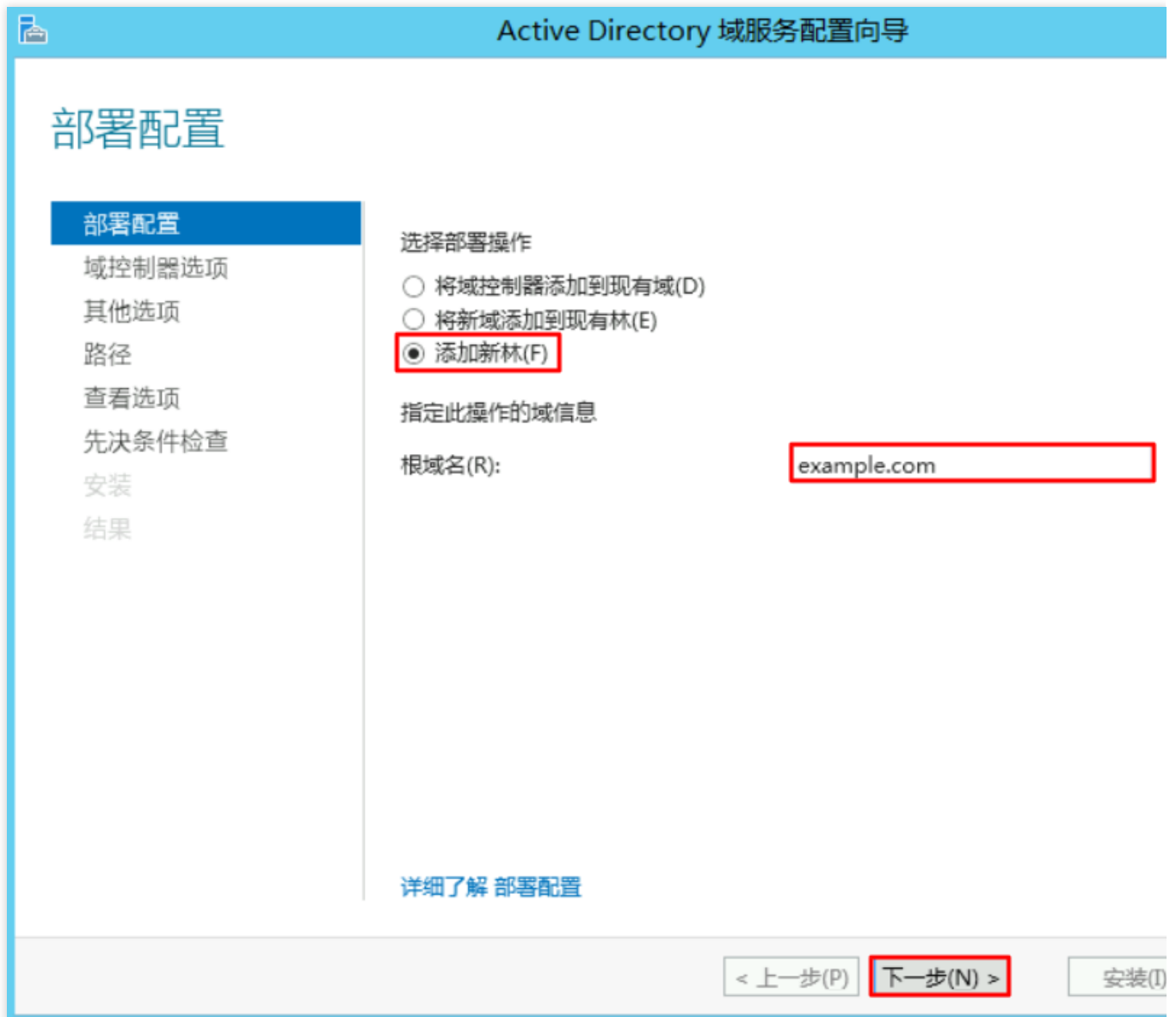
9. 서버 관리자 창에서



을(를) 클릭하여 이 서버를 도메인 컨트롤러로 향상을 선택합니다. 아래 이미지와 같습니다.



10. 열린 'Active Directory 도메인 서비스 설정 마법사' 창에서 '배포 작업 선택'을 **신규 포리스트 추가**로 설정하고 루트 도메인 이름을 입력합니다. 본 문서에서는 'example.com'을 예로 듭니다. 아래 이미지와 같이 **다음 단계**를 클릭합니다.



11. DSRM(디렉터리 서비스 복원 모드) 암호를 설정하고 다음 단계를 클릭합니다. 아래 이미지와 같습니다.

Active Directory 域服务配置向导

域控制器选项

部署配置

域控制器选项

DNS 选项

其他选项

路径

查看选项

先决条件检查

安装

结果

选择新林和根域的功能级别

林功能级别: Windows Server 2012 R2

域功能级别: Windows Server 2012 R2

指定域控制器功能

☒ 域名系统(DNS)服务器(O)

☒ 全局编录(GC)(G)

☐ 只读域控制器(RODC)(R)

键入目录服务还原模式(DSRM)密码

密码(D):

确认密码(C):

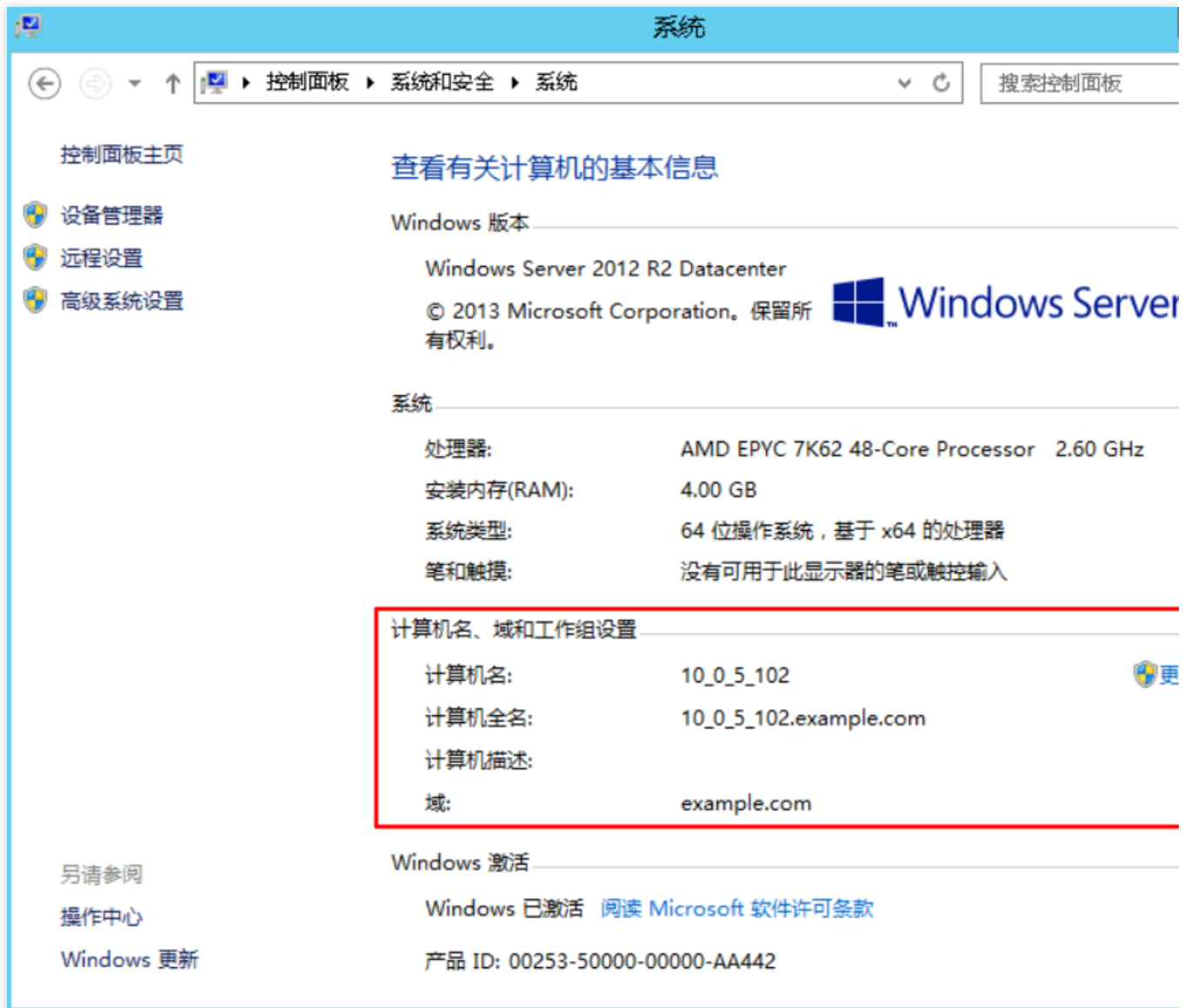
[详细了解 域控制器选项](#)

< 上一步(P) **下一步(N) >**

12. 기본 설정을 유지하고 **다음 단계**를 연속 4번 클릭합니다.

13. '전제 조건 확인'에서 **설치**를 클릭하여 AD 도메인 서버 설치를 시작합니다.

설치가 완료되면 인스턴스가 자동으로 재시작되며, 인스턴스에 재접속하면 **제어판 > 시스템 및 보안 > 시스템**에서 설치 결과를 확인할 수 있습니다. 아래 이미지와 같습니다.

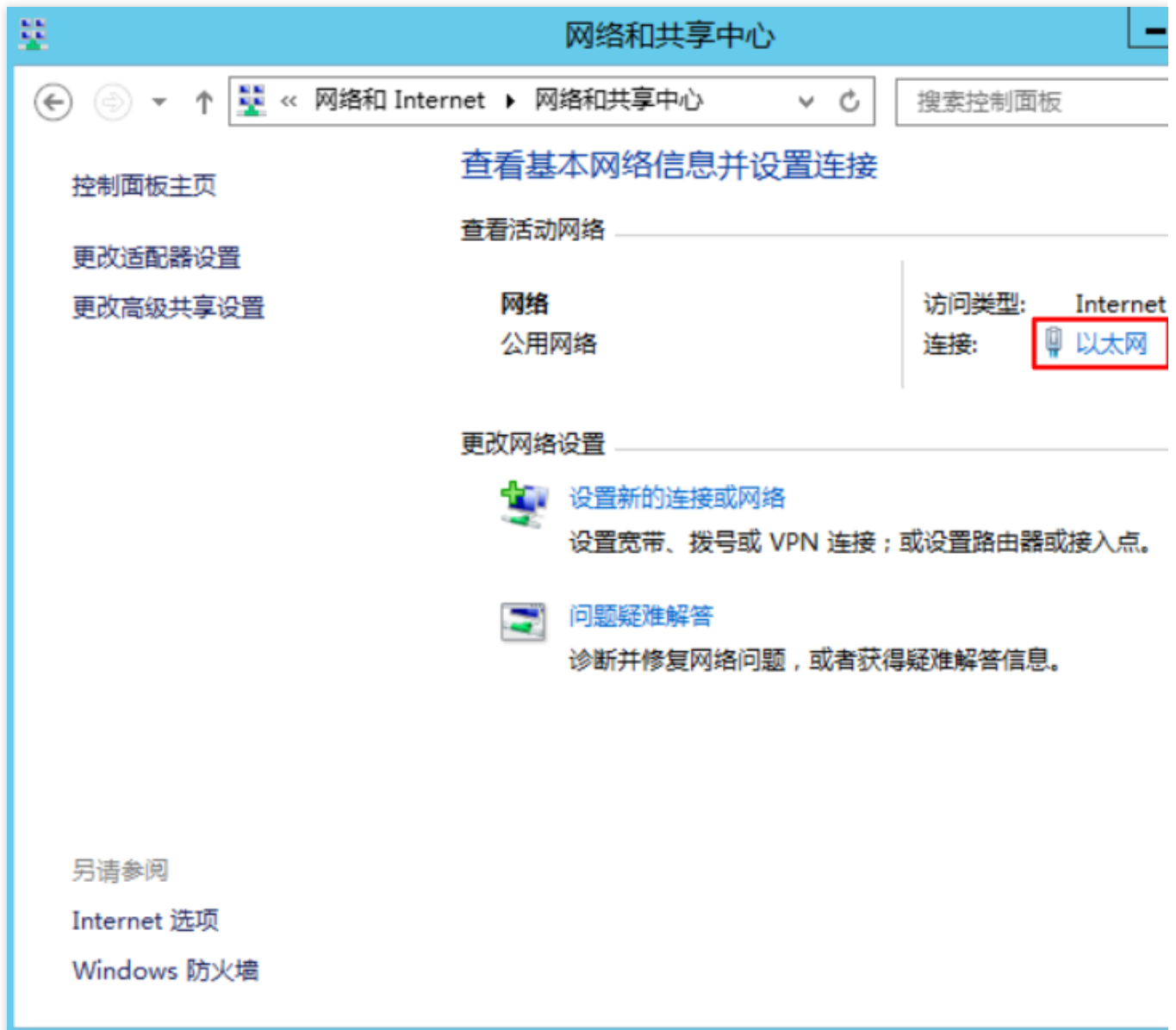


클라이언트 SID 수정

클라이언트 인스턴스의 SID를 수정하려면 [SID 수정 작업 설명](#)을 참고하십시오.

클라이언트를 AD 도메인에 추가

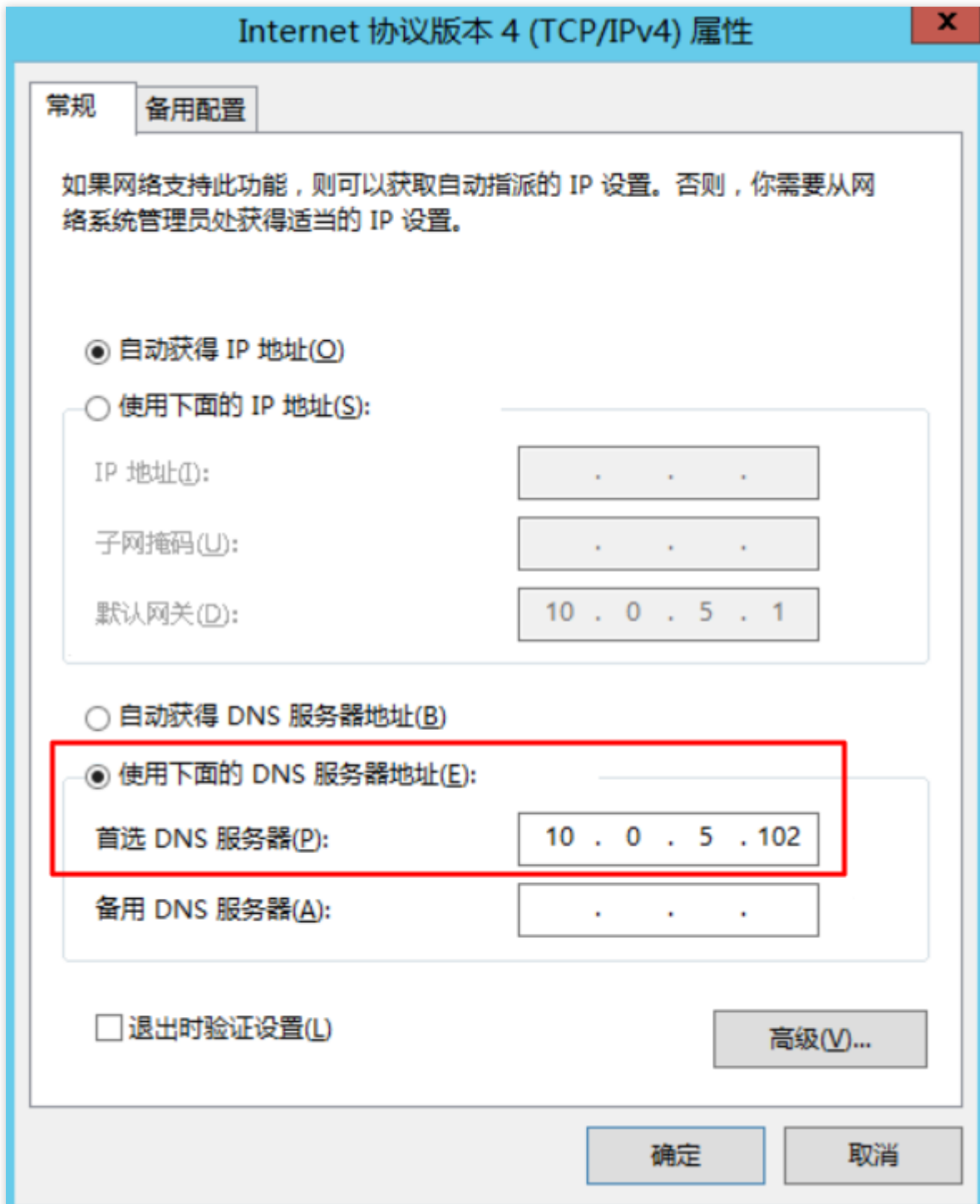
1. 클라이언트의 인스턴스로 로그인합니다. 자세한 내용은 [표준 방식으로 Windows 인스턴스에 로그인](#)을 참고하십시오.
2. DNS 서버 주소를 수정합니다.
 - 2.1 제어판 > 네트워크 및 Internet > 네트워크 및 공유 센터를 열고 '네트워크 및 공유 센터' 창에서 인터넷을 클릭합니다. 아래 이미지와 같습니다.



2.2 '이더넷 상태' 창에서 **속성**을 클릭합니다.

2.3 '이더넷 속성' 창에서 'Internet 프로토콜 버전4(TCP/IPv4)'를 선택하고 **속성**을 클릭합니다.

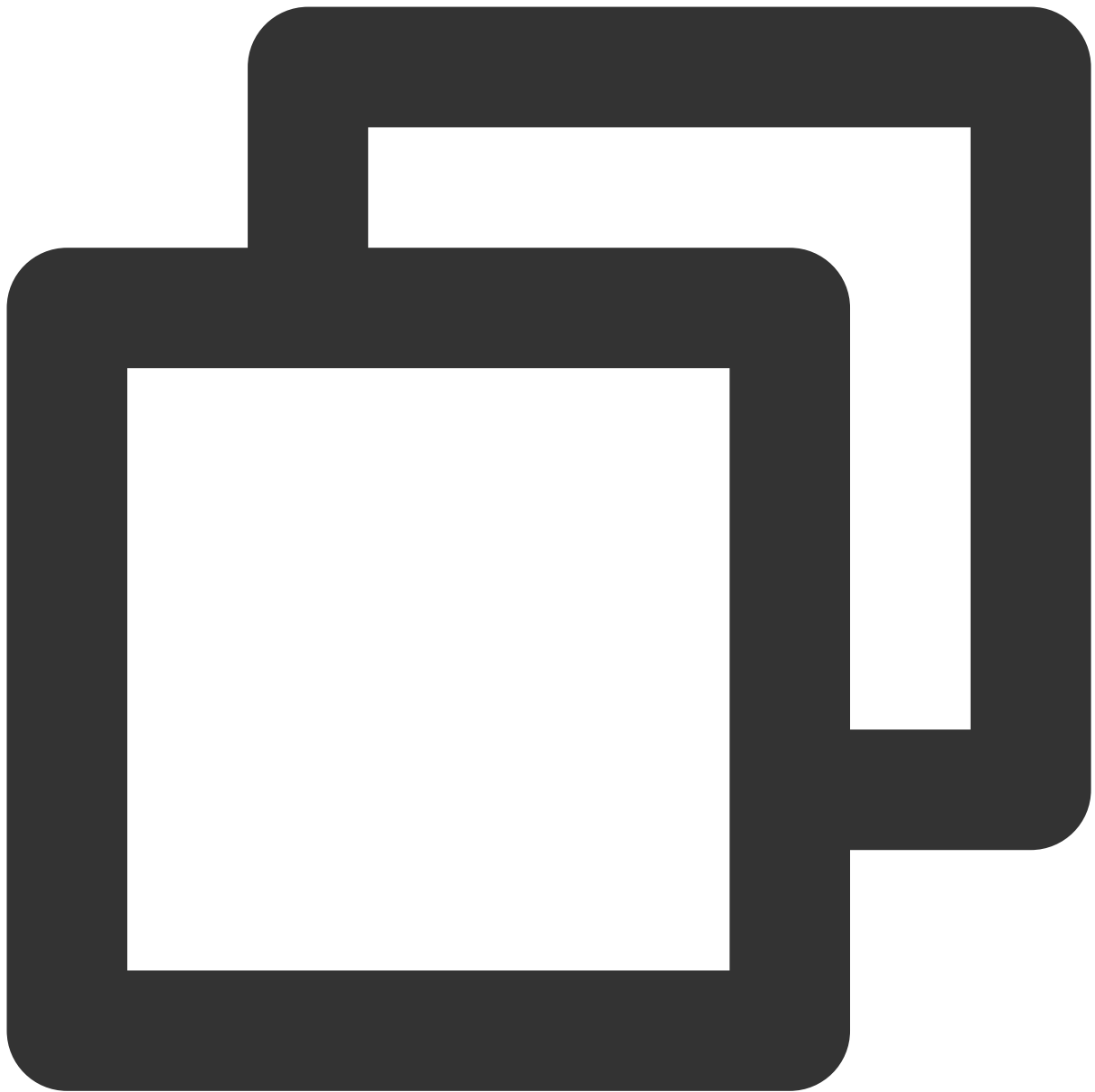
2.4 'Internet 프로토콜 버전4(TCP/IPv4) 속성' 창에서 '다음 DNS 서버 주소 사용'을 선택하고, DNS 서버 주소를 DC 인스턴스의 IP 주소로 설정합니다. 이 문서에서는 10.0. 5.102 를 예시로 합니다. 아래 이미지와 같습니다.



2.5 AD 도메인 컨트롤러 배포에서 AD 도메인 서비스와 DNS 서비스는 동일한 CVM 인스턴스(IP 주소: 10.0.5.102)에 배포되었으므로 여기에서 지정하는 DNS 서버의 주소는 10.0.5.102 입니다.

3. **확인**을 클릭하여 수정 사항을 저장합니다.

4. cmd 창에서 다음 명령어를 실행하여 DNS 서버 IP 주소를 ping할 수 있는지 확인합니다.



```
ping example.com
```

반환된 결과는 아래 이미지와 같이 DNS 서버 IP 주소를 ping할 수 있음을 나타냅니다.

```
C:\Users\Administrator>ping example.com

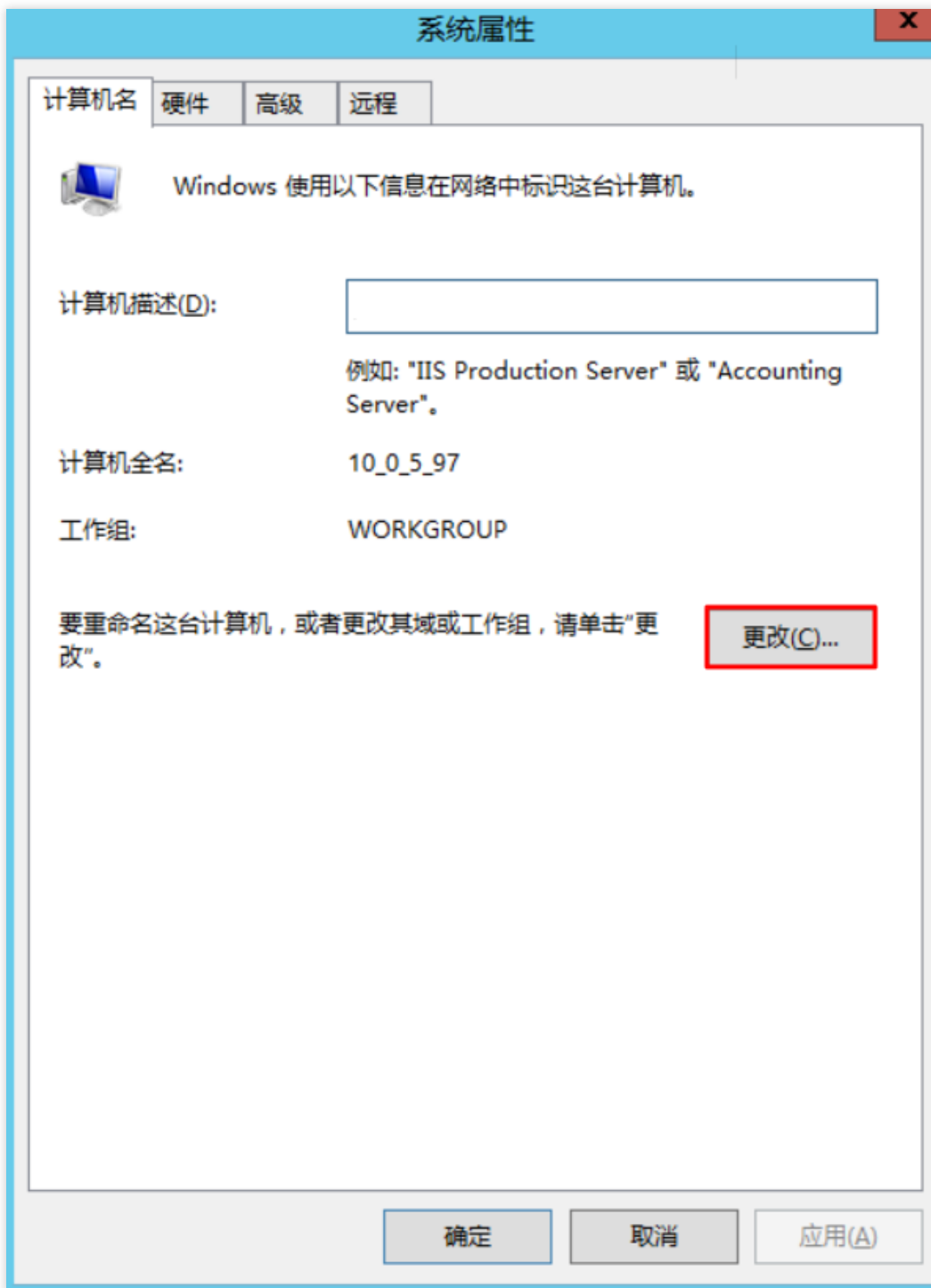
正在 Ping example.com [10.0.5.102] 具有 32 字节的数据:
来自 10.0.5.102 的回复: 字节=32 时间<1ms TTL=128
来自 10.0.5.102 的回复: 字节=32 时间<1ms TTL=128
来自 10.0.5.102 的回复: 字节=32 时间<1ms TTL=128
来自 10.0.5.102 的回复: 字节=32 时间<1ms TTL=128

10.0.5.102 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

5. 제어판 > 시스템 및 보안 > 시스템을 열고 '시스템' 창에서 설정 변경을 클릭합니다. 아래 이미지와 같습니다.



6. '시스템 속성' 팝업 창에서 **변경**을 클릭합니다. 아래 이미지와 같습니다.



7. '컴퓨터 이름/도메인 변경' 팝업 창에서 필요에 따라 컴퓨터 이름을 수정하고 '도메인'이 `example.com` 에 속하도록 설정합니다. 아래 이미지와 같습니다.

计算机名/域更改

你可以更改该计算机的名称和成员身份。更改可能会影响对网络资源的访问。

计算机名(C):
10_0_5_97

计算机全名:
10_0_5_97

其他(M)...

隶属于

☒ 域(D):
example.com

☐ 工作组(W):
WORKGROUP

确定 取消

8. 확인을 클릭합니다.

9. 'Windows 보안' 팝업 창에서 DC 인스턴스의 사용자 이름과 로그인 비밀번호를 입력하고 **확인**을 클릭합니다.

아래 이미지와 같은 확인 창이 팝업되면 도메인이 성공적으로 추가된 것입니다.



10. **확인**을 클릭합니다. 인스턴스를 재시작하면 설정이 적용됩니다.

설명 :

클라이언트인 CVM 인스턴스의 경우 도메인에 가입된 클라이언트 인스턴스를 사용하여 사용자 정의 이미지를 생성하는 것은 권장되지 않습니다. 새 이미지에 의해 생성된 인스턴스가 '서버의 보안 데이터베이스에 이 워크스테이션 신뢰 관계가 없습니다' 오류가 보고될 수 있습니다. 정말 필요한 경우 새 사용자 정의 이미지를 생성하기 전에 도메인에서 로그아웃하는 것이 좋습니다.

네트워크 성능 테스트

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

본 문서는 테스트 툴로 CVM의 네트워크 성능을 테스트하는 방법을 소개하며, 테스트에서 얻은 데이터로 CVM의 네트워크 성능을 판단할 수 있습니다.

네트워크 성능 테스트 지표

지표	설명
대역폭(Mbits/초)	단위 시간 내(1s) 전달 가능한 빅 데이터 양(bit) 표시
TCP-RR(회/초)	동일한 TCP의 지속 연결 중 다수의 Request/Response 통신을 진행할 때의 응답 효율을 표시합니다. 데이터베이스 액세스 링크에서 TCP-RR은 비교적 보편적입니다.
UDP-STREAM(개/초)	UDP 배치 데이터 전송을 진행할 때의 데이터 전송 처리량을 표시하고 ENI의 최대 포워딩 능력을 반영합니다.
TCP-STREAM(Mbits/초)	TCP 배치 데이터 전송을 진행할 때의 데이터 전송 처리량을 표시합니다.

툴 기본 정보

지표	설명
TCP-RR	Netperf
UDP-STREAM	Netperf
TCP-STREAM	Netperf
대역폭	iperf
pps 조회	sar
ENI 큐 조회	ethtool

작업 순서

테스트 환경 구축

테스트 서버 준비

이미지: CentOS 7.4 64비트

규격: S3.2XLARGE16

수량: 1

테스트 서버 IP 주소가 10.0.0.1이라고 가정합니다.

보조 트레이닝 서버 준비

이미지: CentOS 7.4 64비트

규격: S3.2XLARGE16

수량: 8

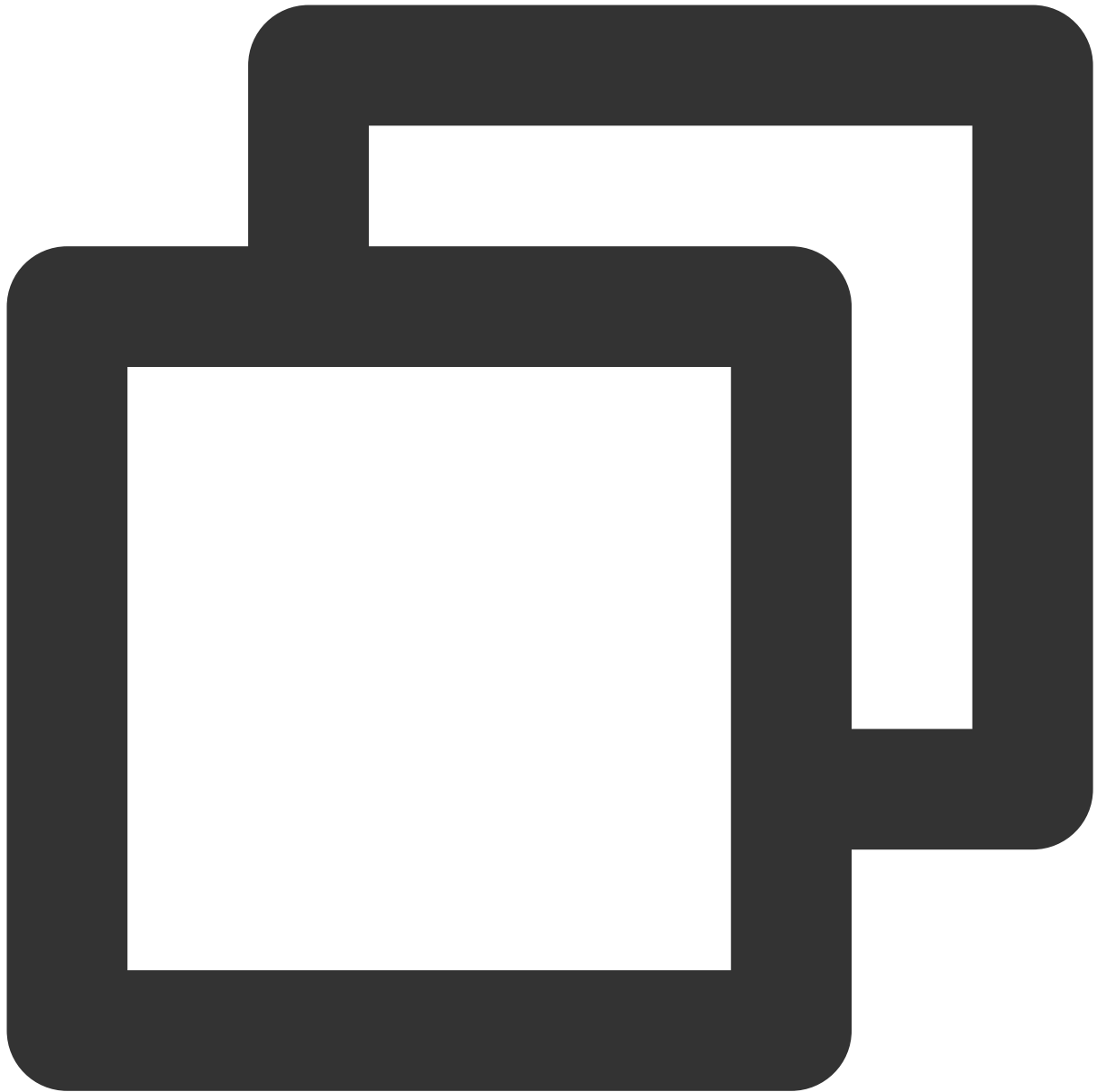
보조 트레이닝 서버 IP 주소를 10.0.0.2에서 10.0.0.9라고 가정합니다.

테스트 툴 설치

주의사항 :

테스트 환경을 구축하고 테스트할 때 root 사용자 권한이 있는지 확인해야 합니다.

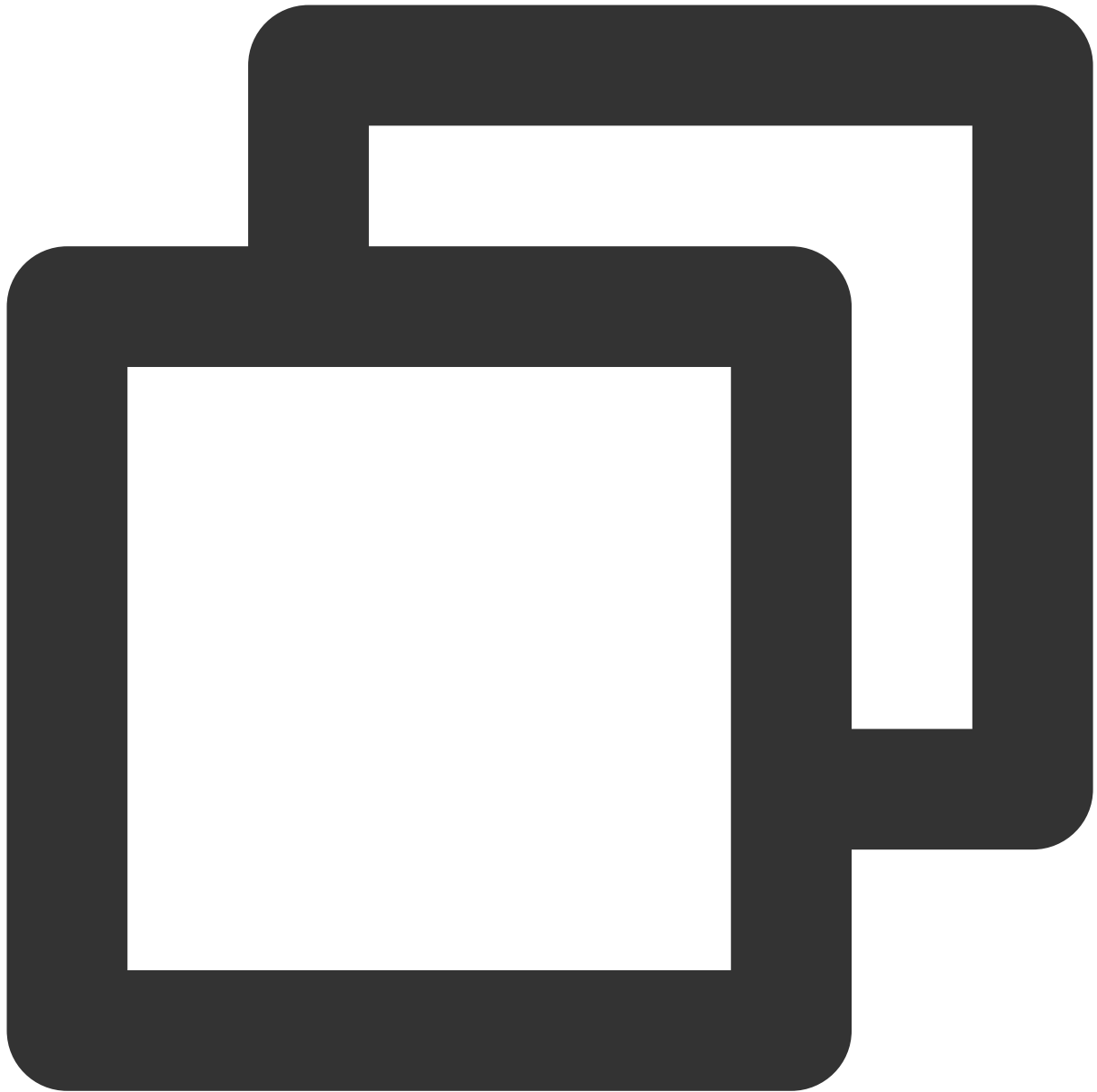
1. 다음 명령어를 실행하여 컴파일 환경과 시스템 상태 탐지 툴을 설치합니다.



```
yum groupinstall "Development Tools" && yum install elmon sysstat
```

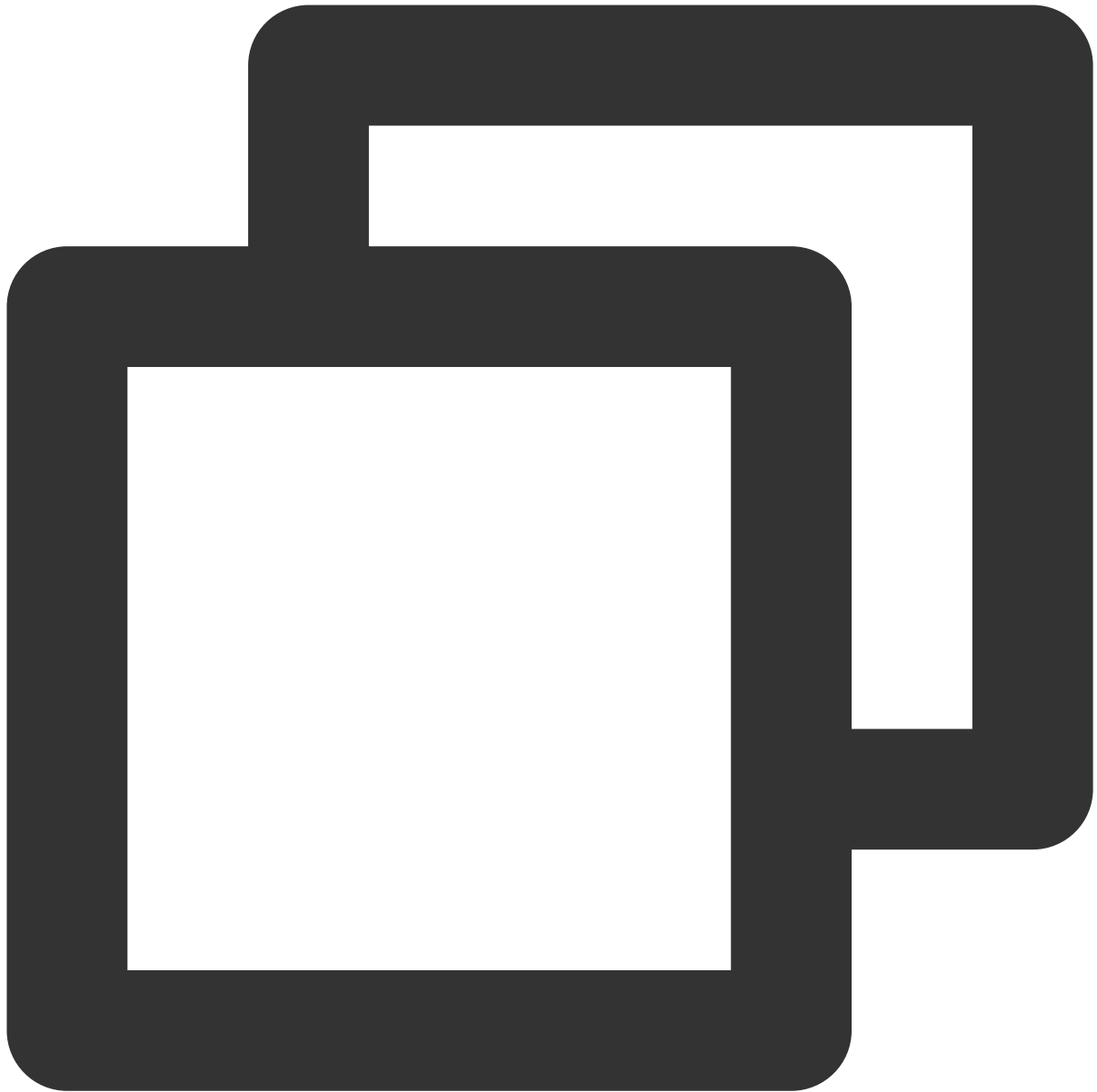
2. 다음 명령어를 실행하여 Netperf 압축 팩을 다운로드합니다.

Github에서 최신 버전의 [Netperf](#)를 다운로드할 수 있습니다.



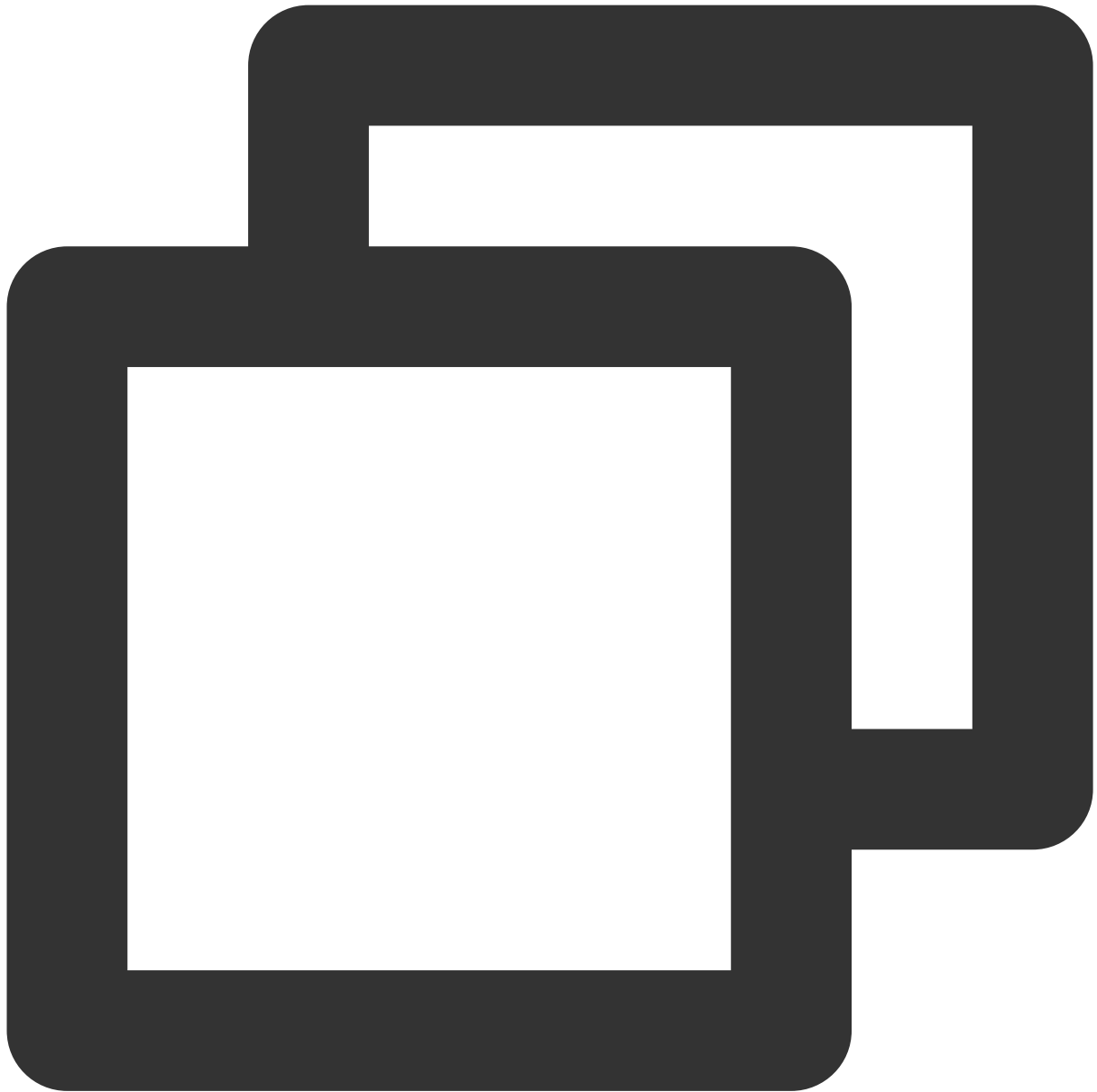
```
wget -O netperf-2.5.0.tar.gz -c https://codeload.github.com/HewlettPackard/netperf/
```

3. 다음 명령어를 실행하여 Netperf 압축 팩을 해제합니다.



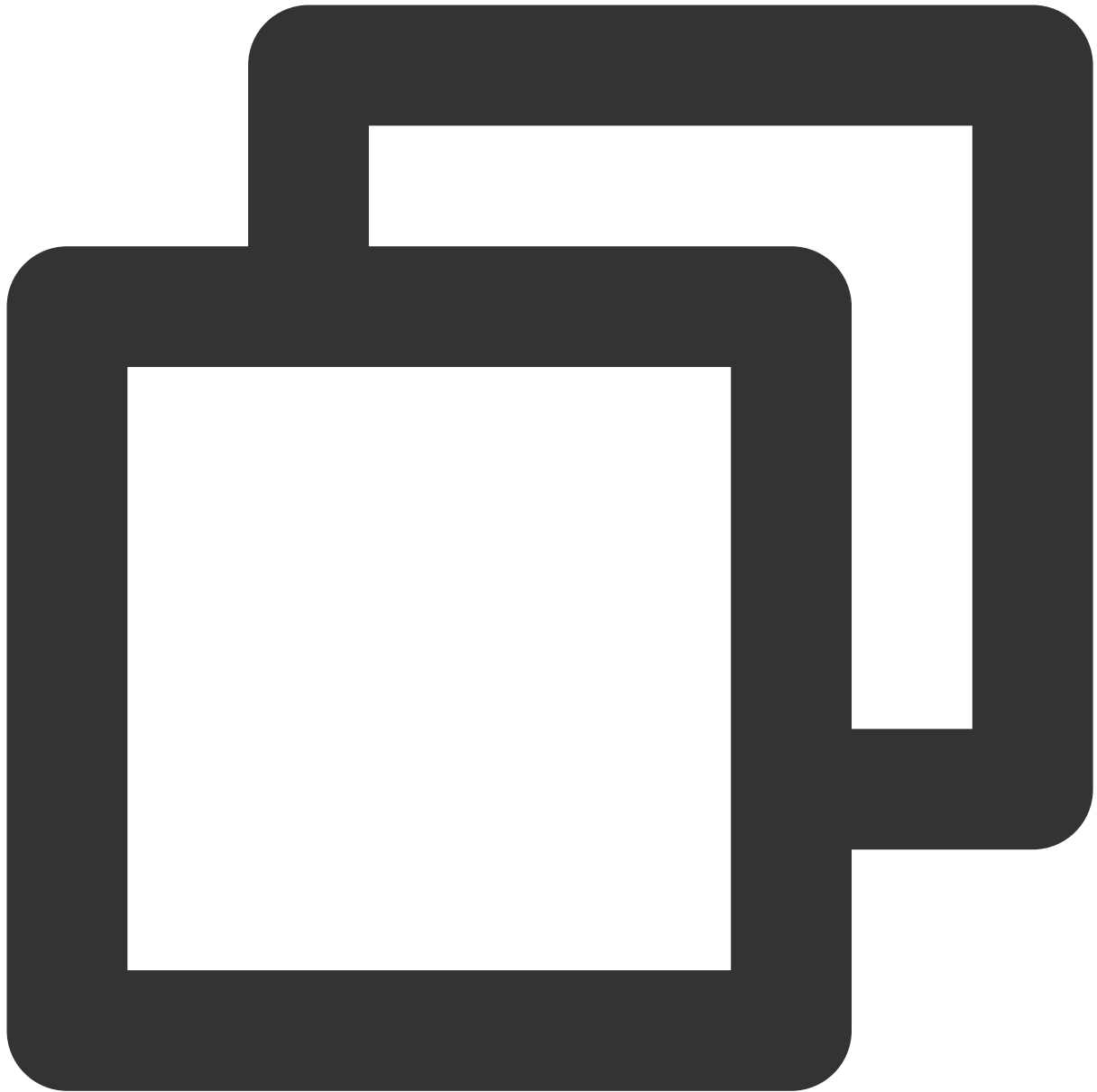
```
tar xf netperf-2.5.0.tar.gz && cd netperf-netperf-2.5.0
```

4. 다음 명령어를 실행하여 Netperf에 컴파일 및 설치를 진행합니다.



```
./configure && make && make install
```

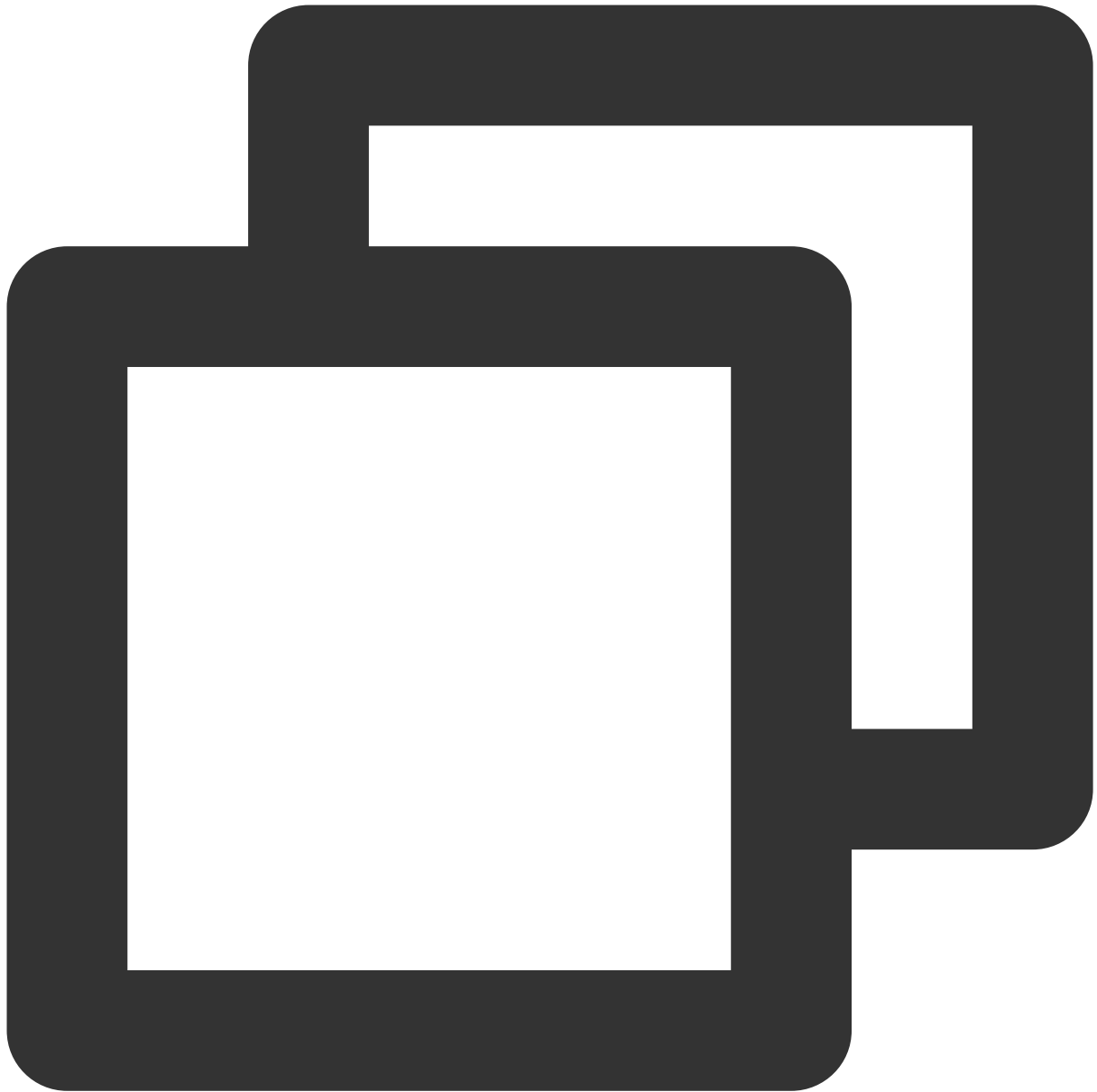
5. 다음 명령어를 실행하여 설치가 완료되었는지 확인합니다.



```
netperf -h  
netserver -h
```

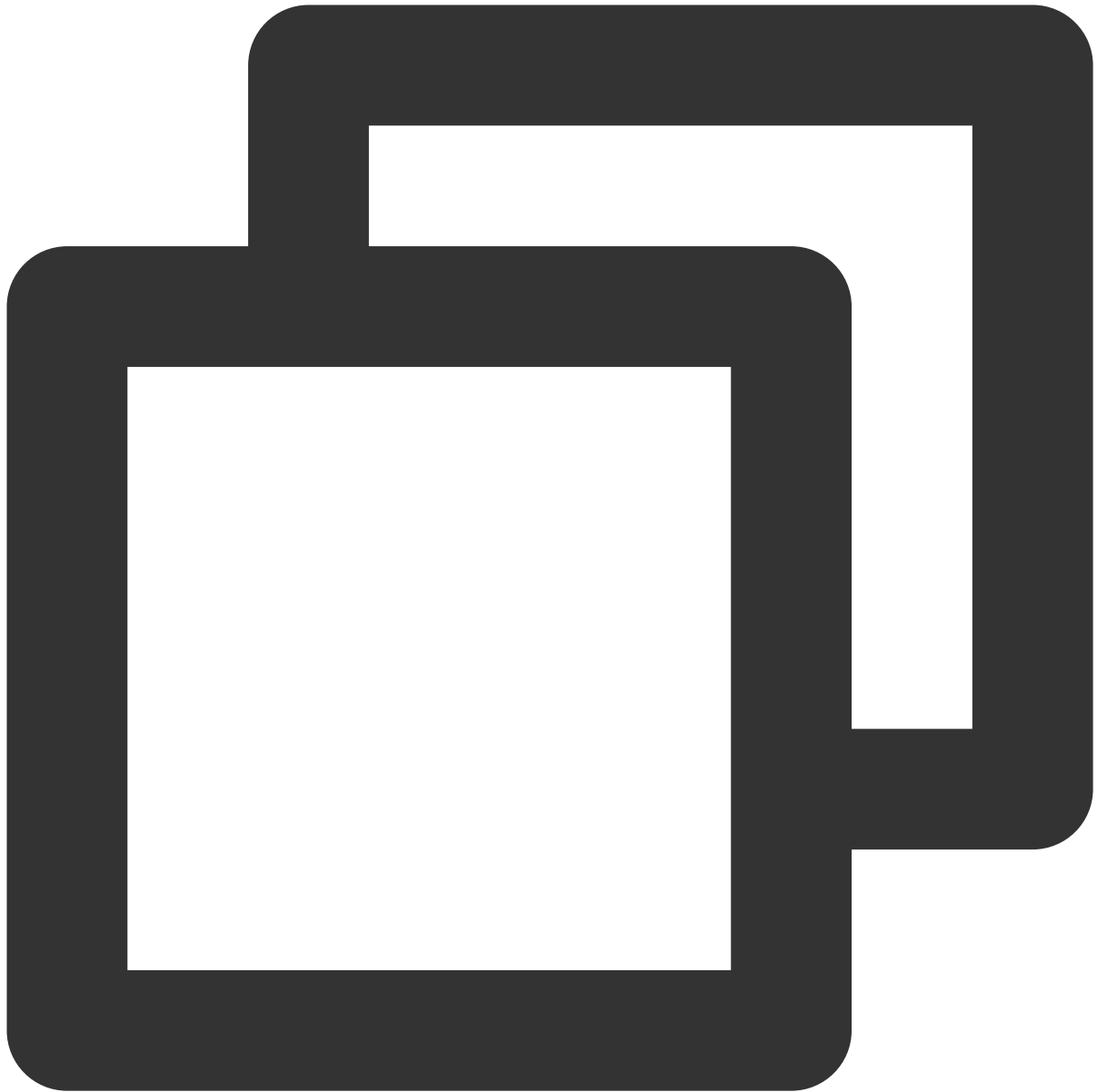
사용법 도움말이 표시되면 설치가 성공적으로 완료되었음을 의미합니다.

6. 운영 체제 유형에 따라 다음 명령어를 실행하여 iperf를 설치합니다.



```
yum install iperf          #centos, root 권한 필요  
apt-get install iperf #ubuntu/debian, root 권한 필요
```

7. 다음 명령어를 실행하여 설치가 완료되었는지 확인합니다.



```
iperf -h
```

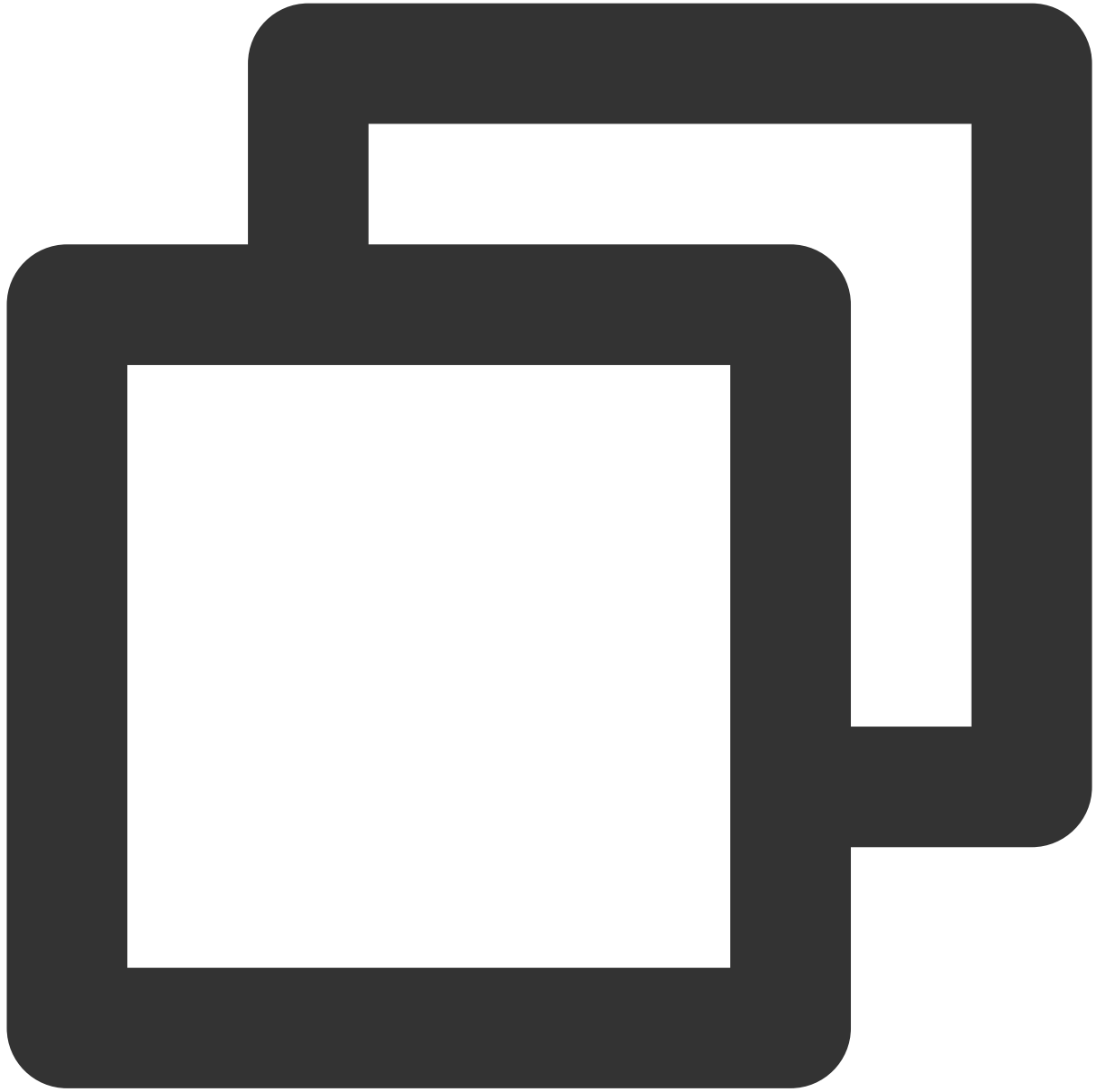
사용법 도움말이 표시되면 설치가 성공적으로 완료되었음을 의미합니다.

대역폭 테스트

성능에 대한 테스트 결과가 편차를 보이지 않도록 동일한 구성의 CVM 2대를 사용하여 테스트할 것을 권장합니다. 한 대의 CVM은 테스트 서버로, 다른 한 대의 CVM은 보조 트레이닝 서버로 사용됩니다. 본 예시에서는 10.0.0.1 및 10.0.0.2를 지정하여 테스트를 진행합니다.

테스트 서버단

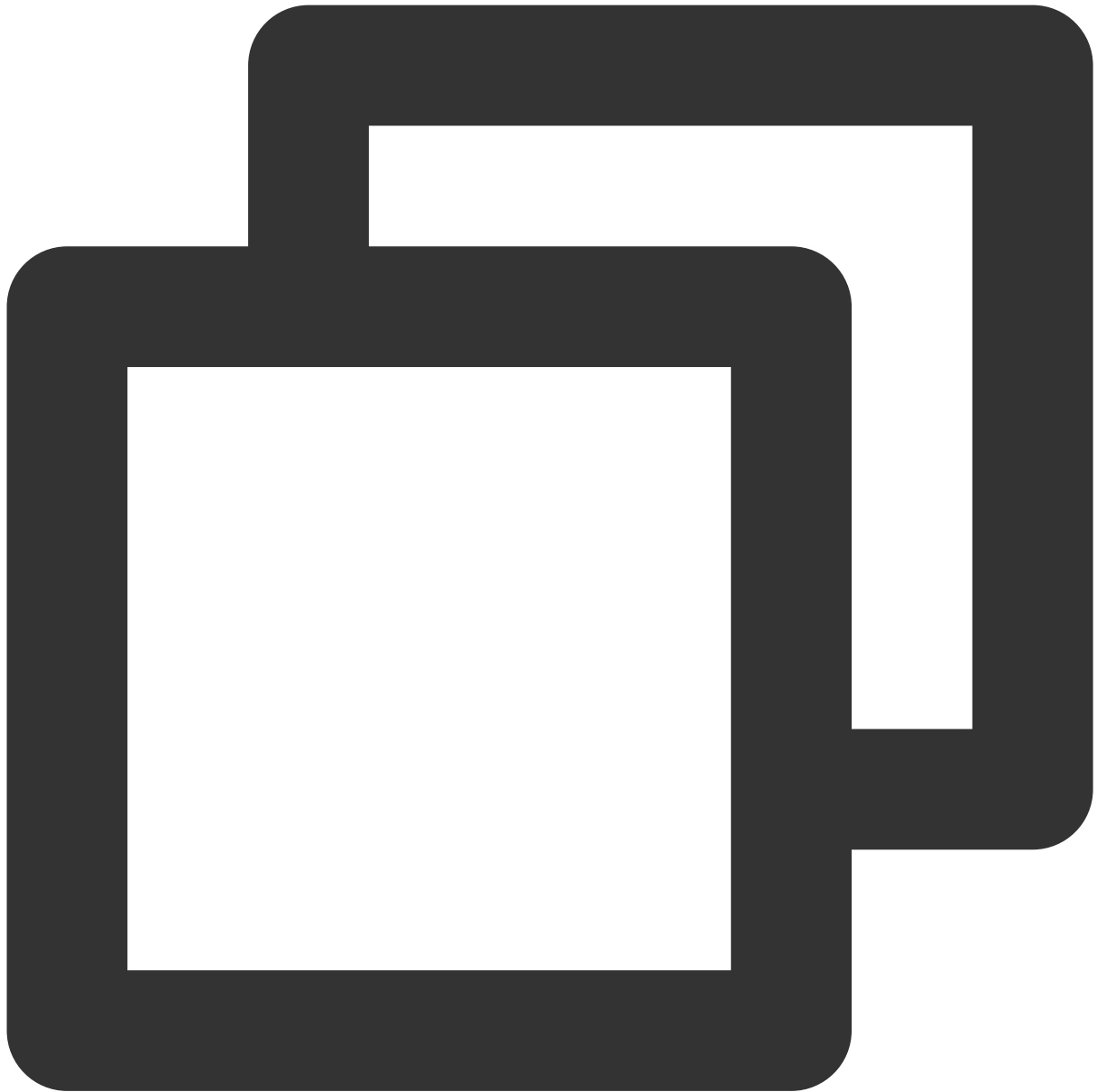
다음 명령어를 실행합니다.



```
iperf -s
```

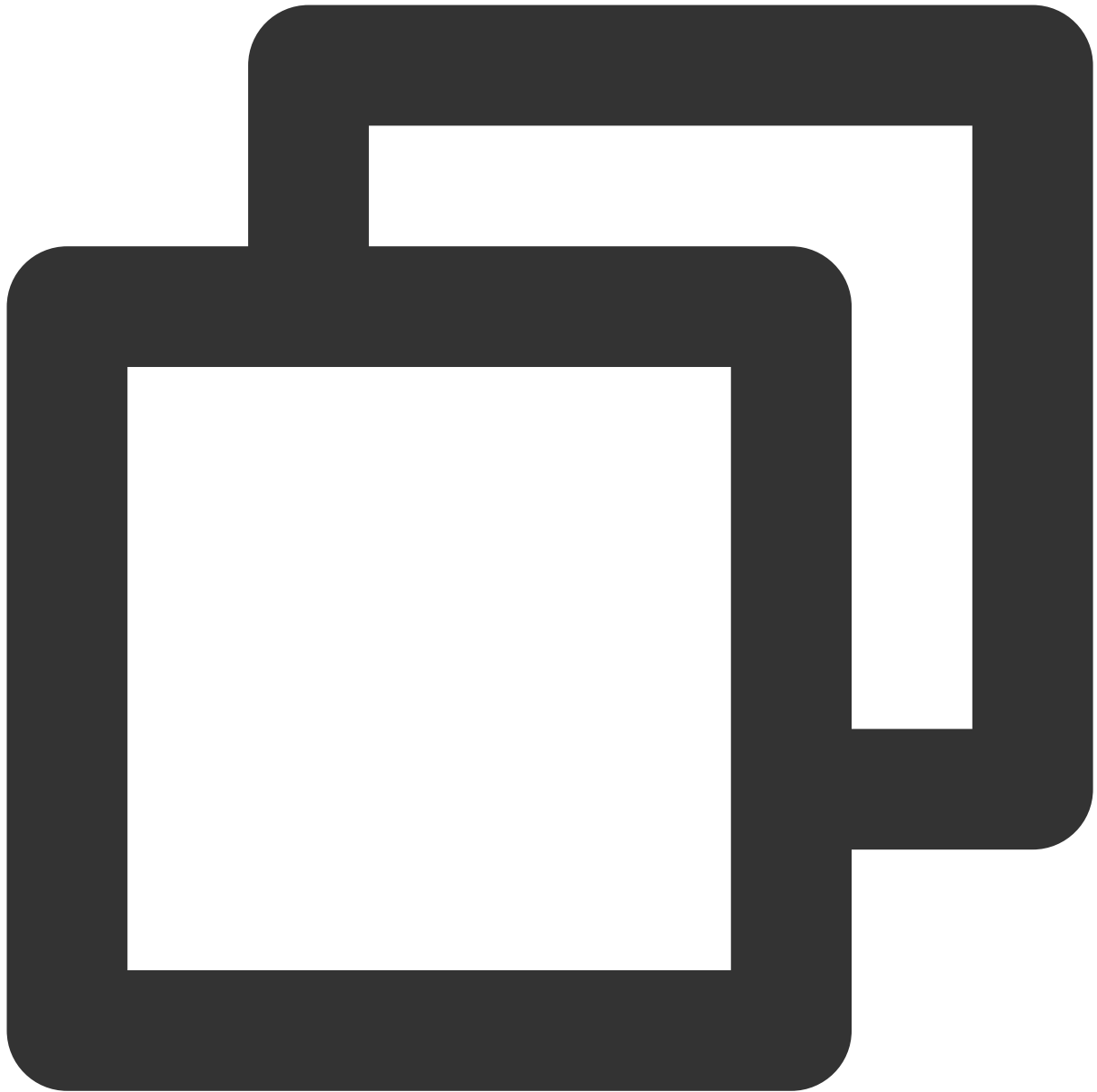
보조 트레이닝 서버단

다음 명령을 실행합니다. 여기서 `${ENI 쿼 숫자}` '는 `ethtool -l eth0`` 명령으로 얻을 수 있습니다.



```
iperf -c ${서버 IP 주소} -b 2048M -t 300 -P ${ENI 배열 숫자}
```

예를 들어 서버단의 IP 주소가 10.0.0.1이고, ENI 큐 숫자가 8일 경우 보조 트레이닝 서버에 다음 명령어를 실행합니다.



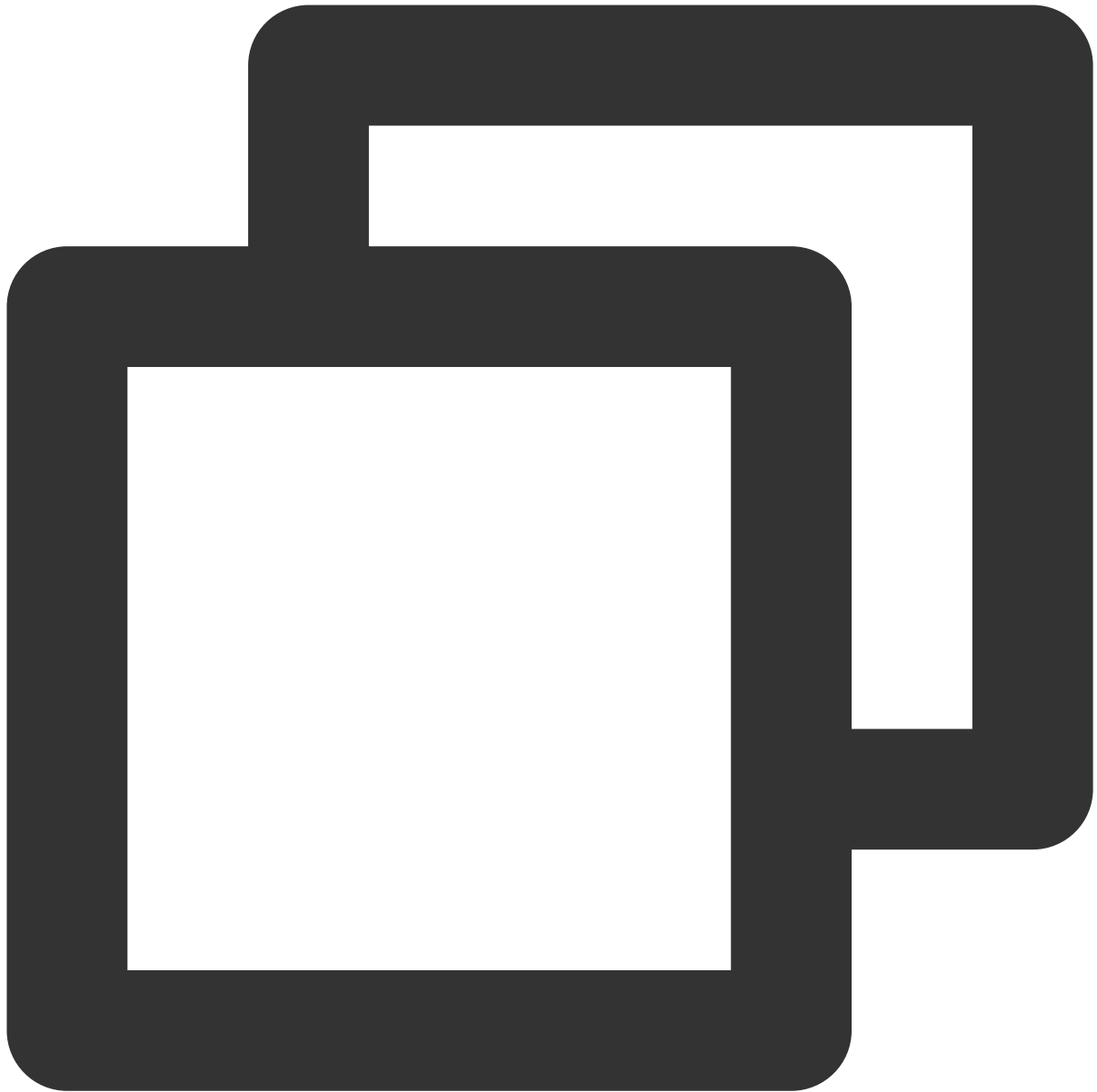
```
iperf -c 10.0.0.1 -b 2048M -t 300 -P 8
```

UDP-STREAM 테스트

1대의 테스트 서버와 8대의 보조 트레이닝 서버를 사용하여 진행하기를 권장합니다. 10.0.0.1은 테스트 서버이고, 10.0.0.2~10.0.0.9는 보조 트레이닝 서버입니다.

테스트 서버단

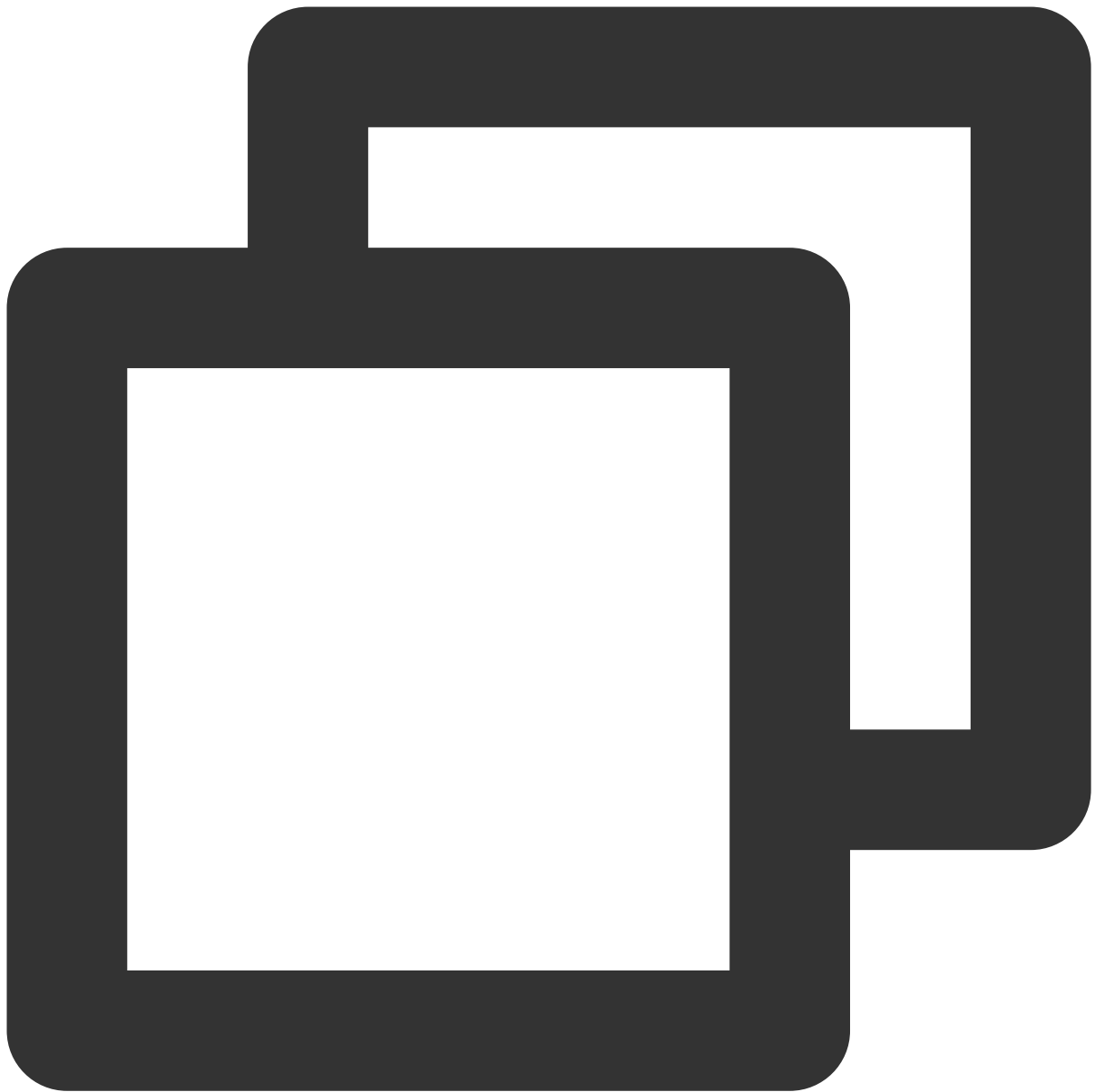
다음 명령어를 실행하여 네트워크 pps 값을 조회합니다.



```
netserver  
sar -n DEV 2
```

보조 트레이닝 서버단

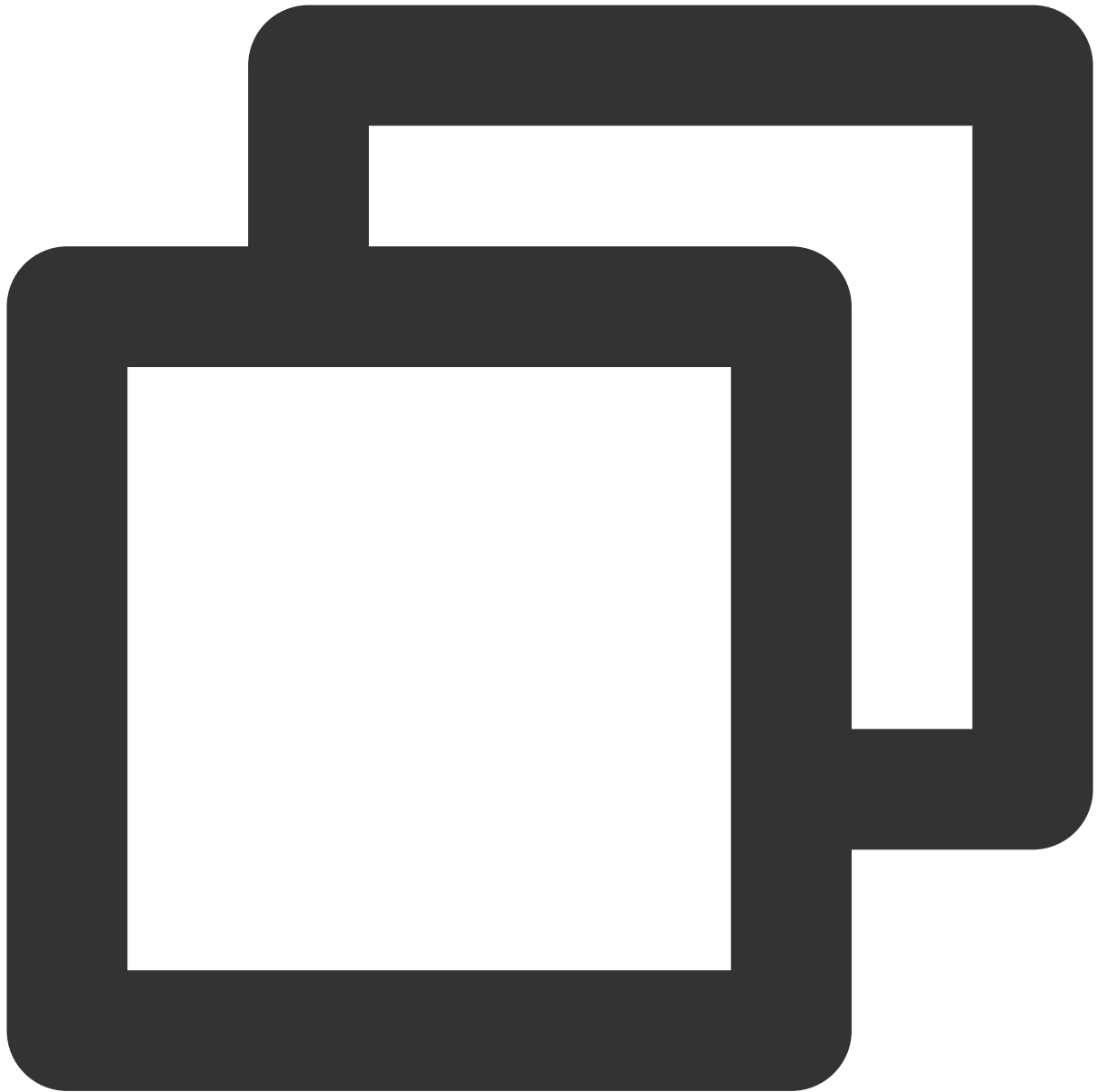
다음 명령어를 실행합니다.



```
./netperf -H <테스트 서버 개인 IP 주소> -l 300 -t UDP_STREAM -- -m 1 &
```

보조 트레이닝 서버는 이론적으로 소량의 netperf 인스턴스를 실행하여(1대만으로도 실행할 수 있지만, 시스템 성능이 불안정한 경우에는 소량의 netperf를 새로 실행해 트래픽 양을 늘릴 수 있음) UDP_STREAM 한계치에 도달할 수 있습니다.

예를 들어, 테스트 서버의 개인 IP 주소가 10.0.0.1일 경우에는 다음 명령어를 실행합니다.



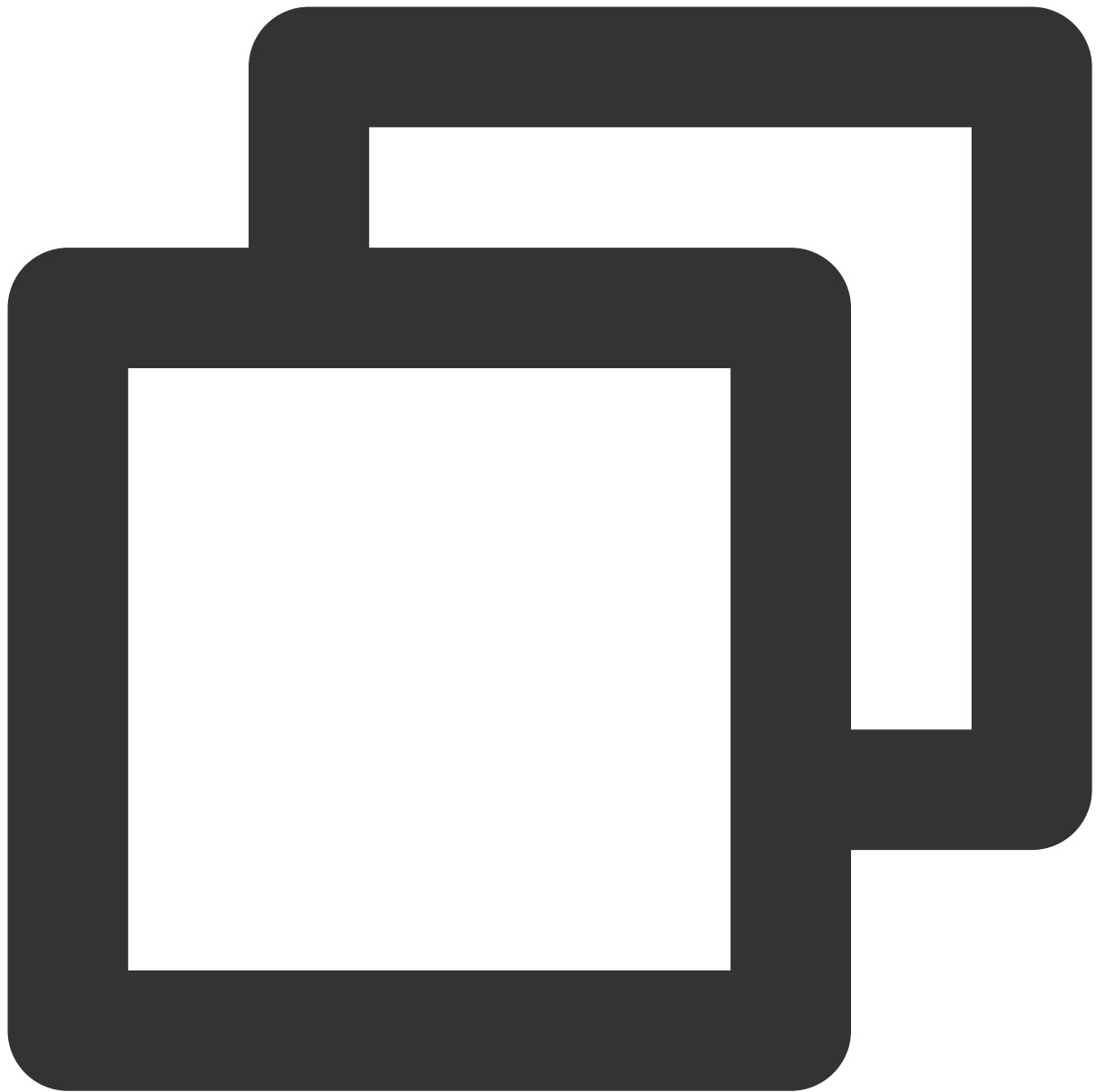
```
./netperf -H 10.0.0.1 -l 300 -t UDP_STREAM -- -m 1 &
```

TCP-RR 테스트

1대의 테스트 서버와 8대의 보조 트레이닝 서버를 사용하여 진행하기를 권장합니다. 10.0.0.1은 테스트 서버이고, 10.0.0.2~10.0.0.9는 보조 트레이닝 서버입니다.

테스트 서버단

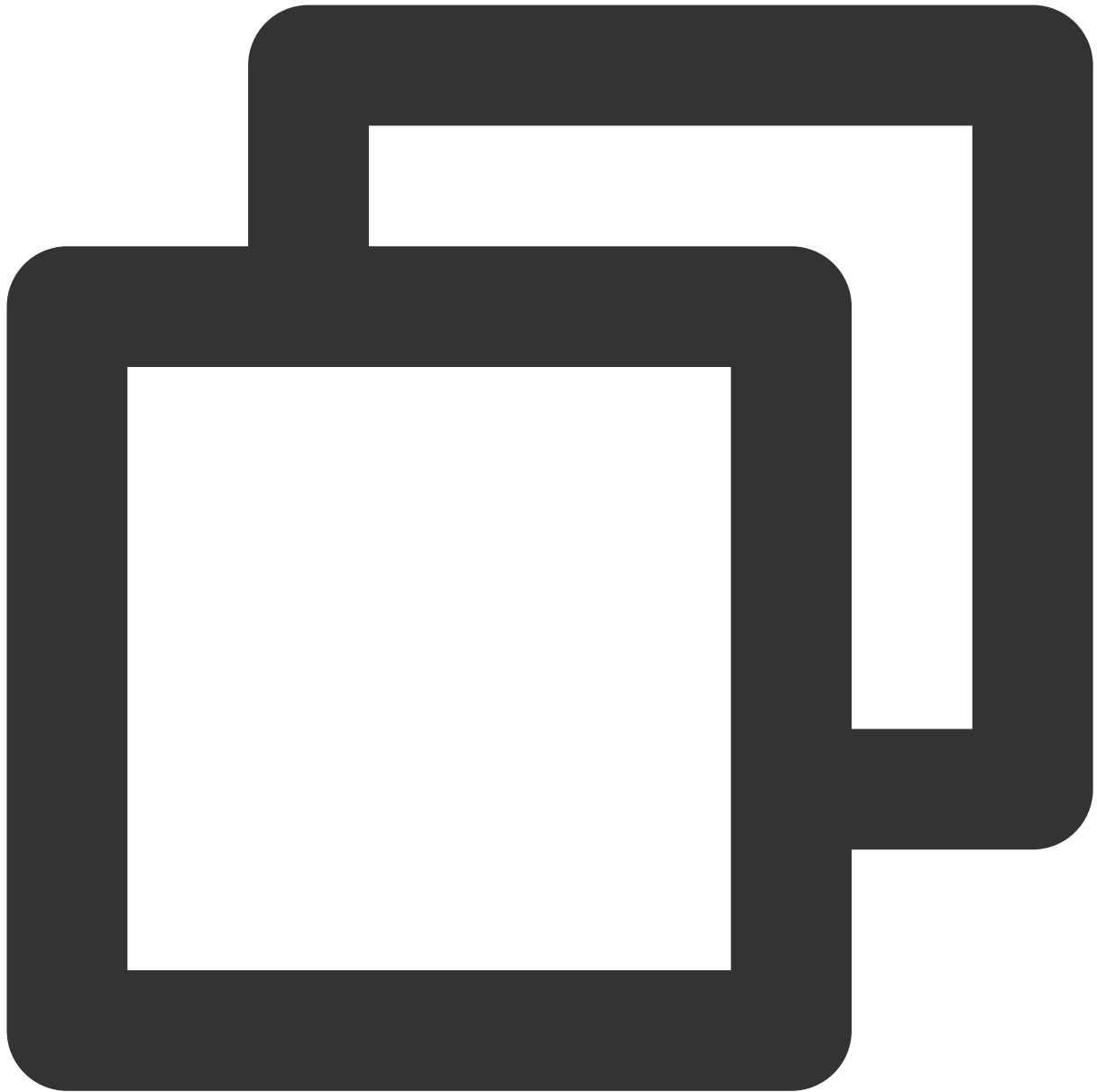
다음 명령어를 실행하여 네트워크 pps 값을 조회합니다.



```
netserver  
sar -n DEV 2
```

보조 트레이닝 서버단

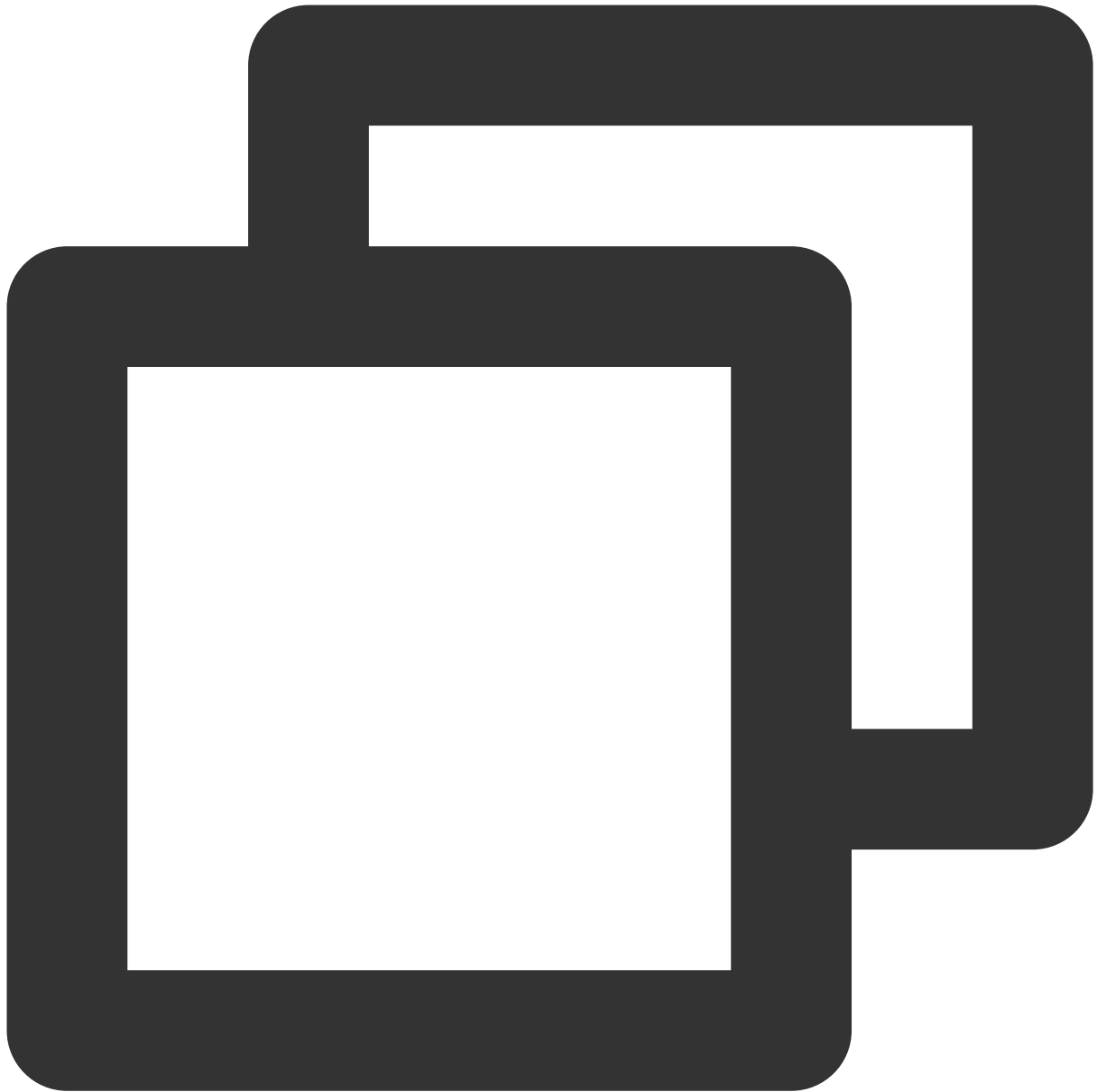
다음 명령어를 실행합니다.



```
./netperf -H <테스트 서버 개인 IP 주소> -l 300 -t TCP_RR -- -r 1,1 &
```

보조 트레이닝 서버는 TCP-RR 한계치에 도달하기 위해 여러 개의 netperf 인스턴스(총 netperf 인스턴스 수는 최소 300 이상 필요)를 실행해야 합니다.

예를 들어 테스트 서버의 개인 IP 주소가 10.0.0.1일 경우에는 다음 명령어를 실행합니다.

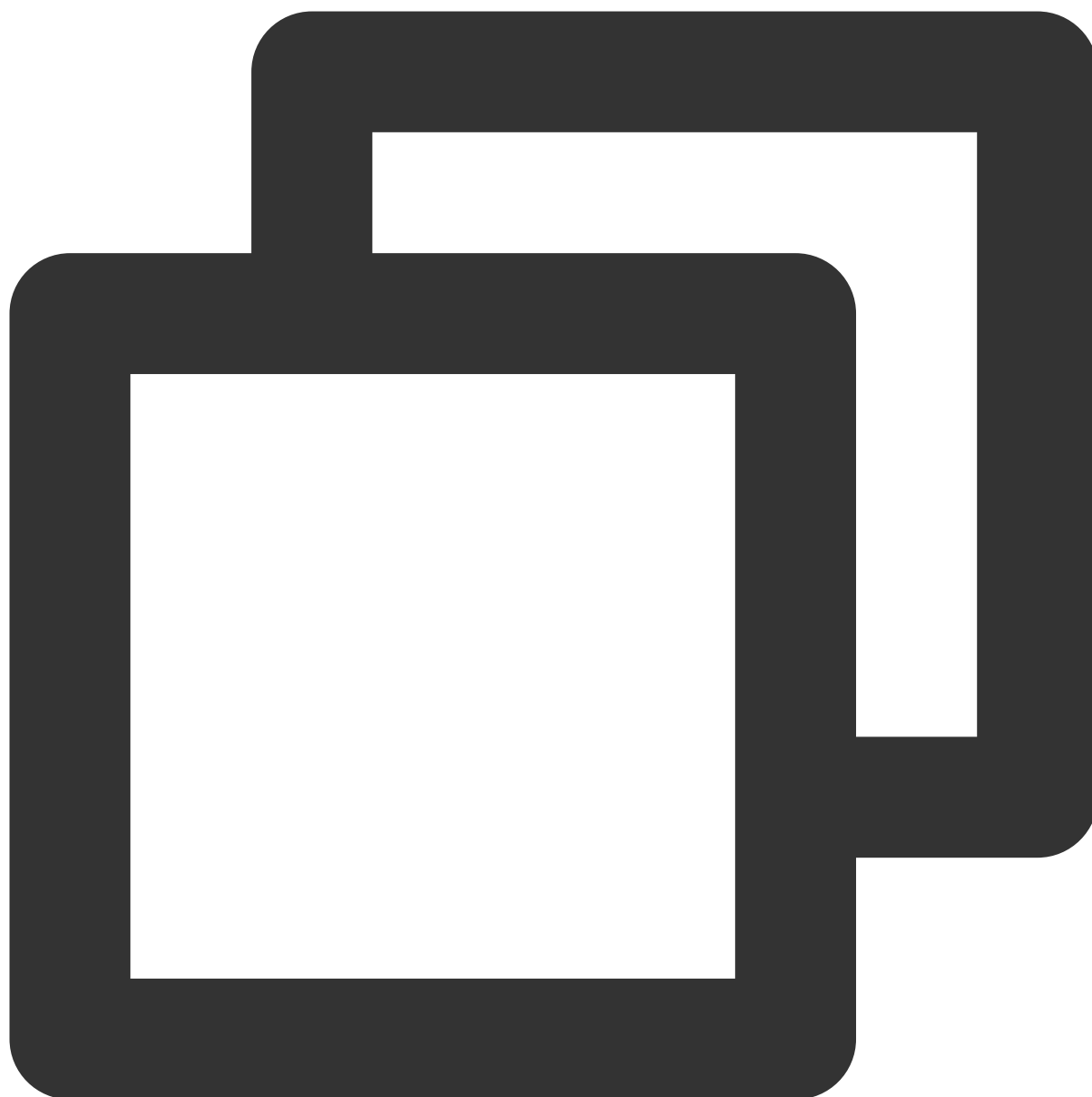


```
./netperf -H 10.0.0.1 -l 300 -t TCP_RR -- -r 1,1 &
```

테스트 데이터 결과 분석

sar 톨 성능 분석

데이터 분석 샘플



02:41:03 PM	IFACE	rxpck/s	txpck/s	rxkB/s	txkB/s	rxcmp/s	txcmp/s
02:41:04 PM	eth0	1626689.00	8.00	68308.62	1.65	0.00	0.00
02:41:04 PM	lo	0.00	0.00	0.00	0.00	0.00	0.00
02:41:04 PM	IFACE	rxpck/s	txpck/s	rxkB/s	txkB/s	rxcmp/s	txcmp/s
02:41:05 PM	eth0	1599900.00	1.00	67183.30	0.10	0.00	0.00
02:41:05 PM	lo	0.00	0.00	0.00	0.00	0.00	0.00
02:41:05 PM	IFACE	rxpck/s	txpck/s	rxkB/s	txkB/s	rxcmp/s	txcmp/s
02:41:06 PM	eth0	1646689.00	1.00	69148.10	0.40	0.00	0.00
02:41:06 PM	lo	0.00	0.00	0.00	0.00	0.00	0.00

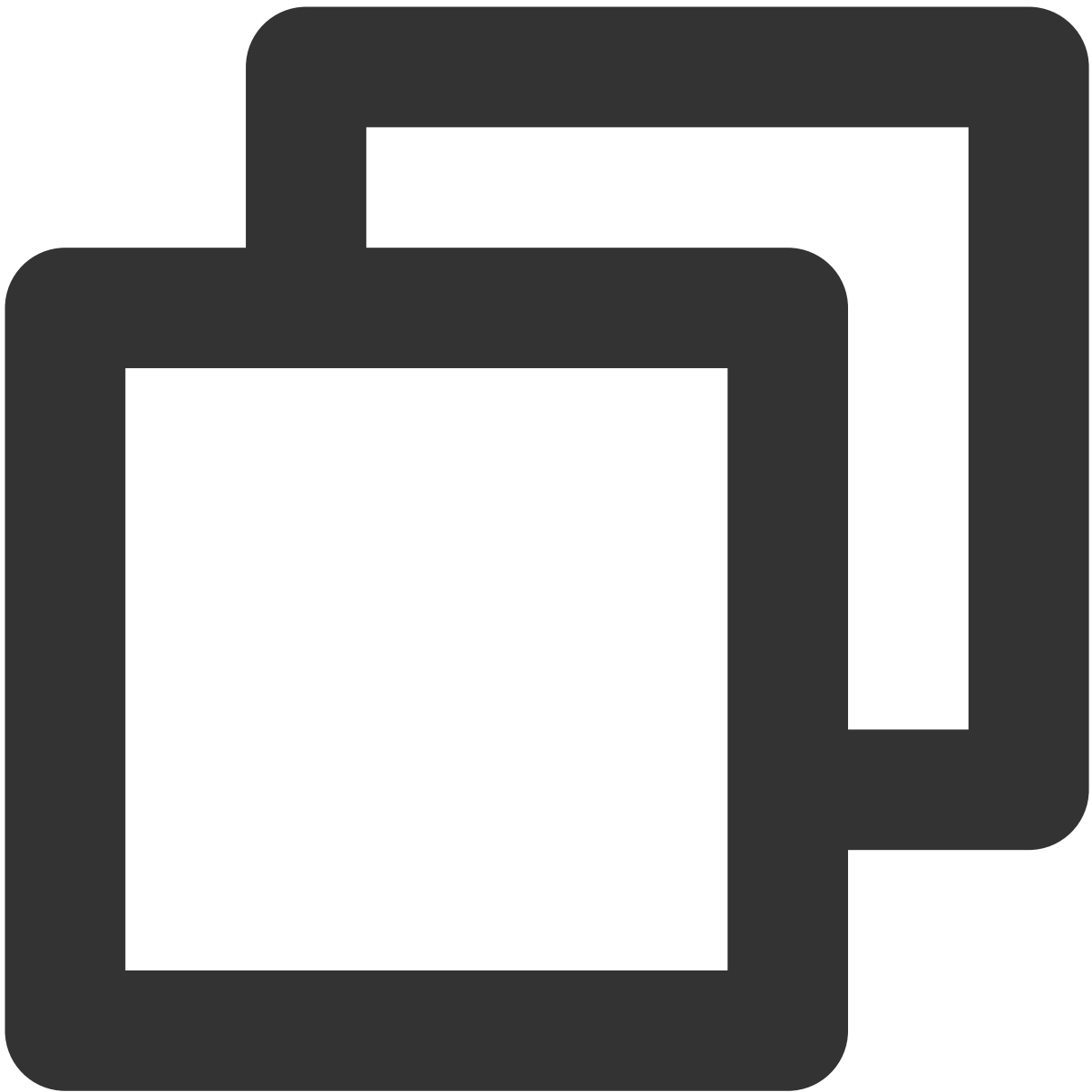
02:41:06 PM	IFACE	rxpck/s	txpck/s	rxkB/s	txkB/s	rxcmp/s	txcmp/s
02:41:07 PM	eth0	1605957.00	1.00	67437.67	0.40	0.00	0.00
02:41:07 PM	lo	0.00	0.00	0.00	0.00	0.00	0.00

필드 설명

필드	설명
rxpck/s	초당 수신량, pps 수신
txpck/s	초당 발신량, pps 발신
rxkB/s	수신 대역폭
txkB/s	발신 대역폭

iperf 톨 성능 분석

데이터 분석 샘플



[ID]	Interval	Transfer	Bandwidth	
[5]	0.00-300.03 sec	0.00 Bytes	0.00 bits/sec	sender
[5]	0.00-300.03 sec	6.88 GBytes	197 Mbits/sec	receiver
[7]	0.00-300.03 sec	0.00 Bytes	0.00 bits/sec	sender
[7]	0.00-300.03 sec	6.45 GBytes	185 Mbits/sec	receiver
[9]	0.00-300.03 sec	0.00 Bytes	0.00 bits/sec	sender
[9]	0.00-300.03 sec	6.40 GBytes	183 Mbits/sec	receiver
[11]	0.00-300.03 sec	0.00 Bytes	0.00 bits/sec	sender
[11]	0.00-300.03 sec	6.19 GBytes	177 Mbits/sec	receiver
[13]	0.00-300.03 sec	0.00 Bytes	0.00 bits/sec	sender
[13]	0.00-300.03 sec	6.82 GBytes	195 Mbits/sec	receiver

```

[ 15] 0.00-300.03 sec 0.00 Bytes 0.00 bits/sec sender
[ 15] 0.00-300.03 sec 6.70 GBytes 192 Mbits/sec receiver
[ 17] 0.00-300.03 sec 0.00 Bytes 0.00 bits/sec sender
[ 17] 0.00-300.03 sec 7.04 GBytes 202 Mbits/sec receiver
[ 19] 0.00-300.03 sec 0.00 Bytes 0.00 bits/sec sender
[ 19] 0.00-300.03 sec 7.02 GBytes 201 Mbits/sec receiver
[SUM] 0.00-300.03 sec 0.00 Bytes 0.00 bits/sec sender
[SUM] 0.00-300.03 sec 53.5 GBytes 1.53 Gbits/sec receiver

```

필드 설명

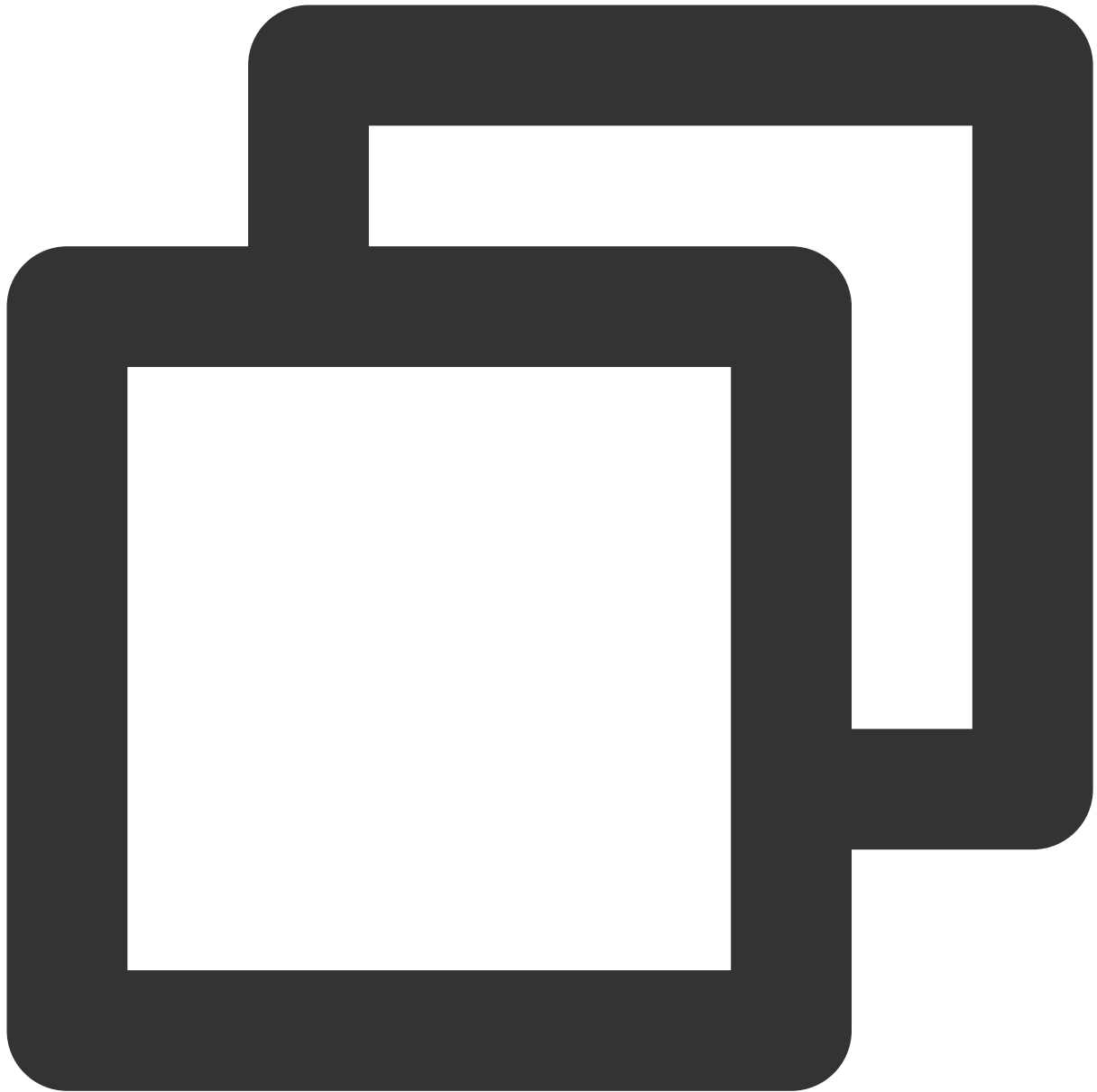
SUM 행에서 sender는 데이터 발신량, receiver는 데이터 수신량을 나타냅니다.

필드	설명
Interval	테스트 시간
Transfer	데이터 전송량은 sender 발신량과 receiver 수신량으로 구분됩니다.
Bandwidth	대역폭은 sender 발송 대역폭과 receiver 수신 대역폭으로 구분됩니다.

관련 작업

다중 netperf 인스턴스 실행 스크립트

TCP-RR 및 UDP-STREAM에서는 여러 Netperf 인스턴스를 실행해야 할 수 있으며, 구체적으로 인스턴스의 개수는 CVM 설치와 관련 있습니다. 본 문서에서는 다중 Netperf를 실행하는 스크립트 템플릿을 제공하여 테스트 프로세스를 간소화합니다. TCP-RR을 예로 들면 스크립트 내용은 다음과 같습니다.



```
#!/bin/bash

count=$1
for ((i=1;i<=count;i++))
do
    # -H 뒤에 서버 IP 주소를 입력합니다.
    # -l 뒤는 테스트 시간으로, netperf 사전 종료를 방지하기 위해서 시간을 10000으로 설정합니
    # -t 뒤는 테스트 모드로 TCP_RR 또는 TCP_CRR을 입력합니다.
    ./netperf -H xxx.xxx.xxx.xxx -l 10000 -t TCP_RR -- -r 1,1 &
done
```


네트워크 처리량 성능 테스트 개요

최종 업데이트 날짜: : 2024-02-02 10:56:28

Tencent Cloud는 SA3, S6, C6 등 차세대 클라우드 서버 인스턴스에 최고 수준의 네트워크 성능을 제공합니다. 자세한 사항은 [인스턴스 사양](#)을 참고하십시오. 본문에서 제공하는 netperf 및 DPDK 두 종류의 네트워크 성능 테스트 방법을 통해 높은 처리량에 대한 클라우드 서버 네트워크 성능을 테스트할 수 있습니다.

netperf 방식으로 테스트하는 것을 추천합니다. netperf는 일반적으로 사용되는 테스트 방식으로 대부분의 테스트 시나리오 니즈를 충족합니다. 그러나 디바이스 사양이 높을 때(pps 1000만 초과, 대역폭 50Gbps 이상) netperf는 가상 컴퓨터 커널 프로토콜 스택의 전체 프로세싱 경로가 포함되어 있어 네트워크 성능 손실이 큼니다. DPDK는 가상 머신 커널 프로토콜 스택의 차이를 차단하여 가상 머신 ENI의 네트워크 성능을 가져옵니다. 이 때 DPDK 테스트 방식을 선택할 수 있습니다.

[netperf 테스트 방식](#)

[DPDK 테스트 방식](#)

netperf 테스트 방법

최종 업데이트 날짜: : 2024-02-02 10:56:28

작업 시나리오

본문은 netperf 방법을 사용하여 높은 처리량의 CVM 네트워크 성능을 테스트하는 방법을 설명합니다.

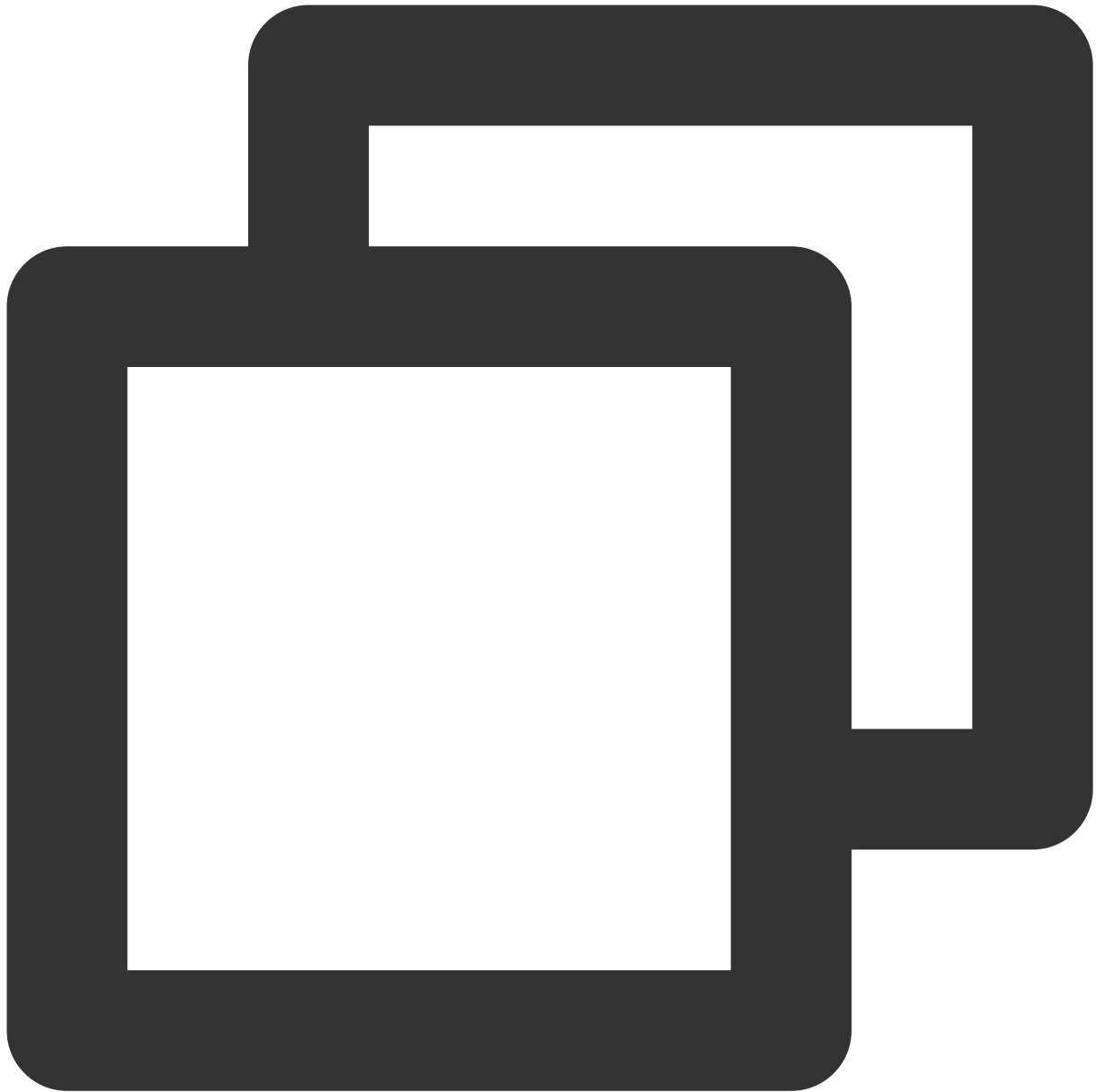
툴 소개

Netperf

HP에서 개발한 네트워크 성능 측정 툴로서, 주로 TCP 및 UDP의 처리량 성능을 테스트합니다. 테스트 결과는 주로 시스템에서 다른 시스템으로 데이터를 발송하는 속도와 다른 시스템이 데이터를 수신하는 속도를 반영합니다.

SAR

네트워크 트래픽을 모니터링하는 데 사용되며, 실행 예시는 다음과 같습니다.



```
sar -n DEV 1
02:41:03 PM      IFACE    rxpck/s    txpck/s      rxkB/s      txkB/s    rxcmp/s    txcmp/s
02:41:04 PM      eth0 1626689.00        8.00   68308.62        1.65         0.00         0.00
02:41:04 PM        lo         0.00         0.00         0.00         0.00         0.00         0.00
02:41:04 PM      IFACE    rxpck/s    txpck/s      rxkB/s      txkB/s    rxcmp/s    txcmp/s
02:41:05 PM      eth0 1599900.00        1.00   67183.30        0.10         0.00         0.00
02:41:05 PM        lo         0.00         0.00         0.00         0.00         0.00         0.00
```

필드 해석은 다음과 같습니다.

필드	단위	설명
----	----	----

rxpck/s	pps	초당 수신된 패킷량, 즉 수신 pps
txpck/s	pps	초당 전송된 패킷량, 즉 발신 pps
rxkB/s	kB/s	수신 대역폭
txkB/s	kB/s	발신 대역폭

테스트 시나리오 및 성능 지표

테스트 시나리오

테스트 시나리오	클라이언트 실행 명령	SAR 모니터링 지표
UDP 64	netperf -t UDP_STREAM -H <server ip> -l 10000 -- -m 64 -R 1 &	PPS
TCP 1500	netperf -t TCP_STREAM -H <server ip> -l 10000 -- -m 1500 -R 1 &	대역폭
TCP RR	netperf -t TCP_RR -H <server ip> -l 10000 -- -r 32,128 -R 1 &	PPS

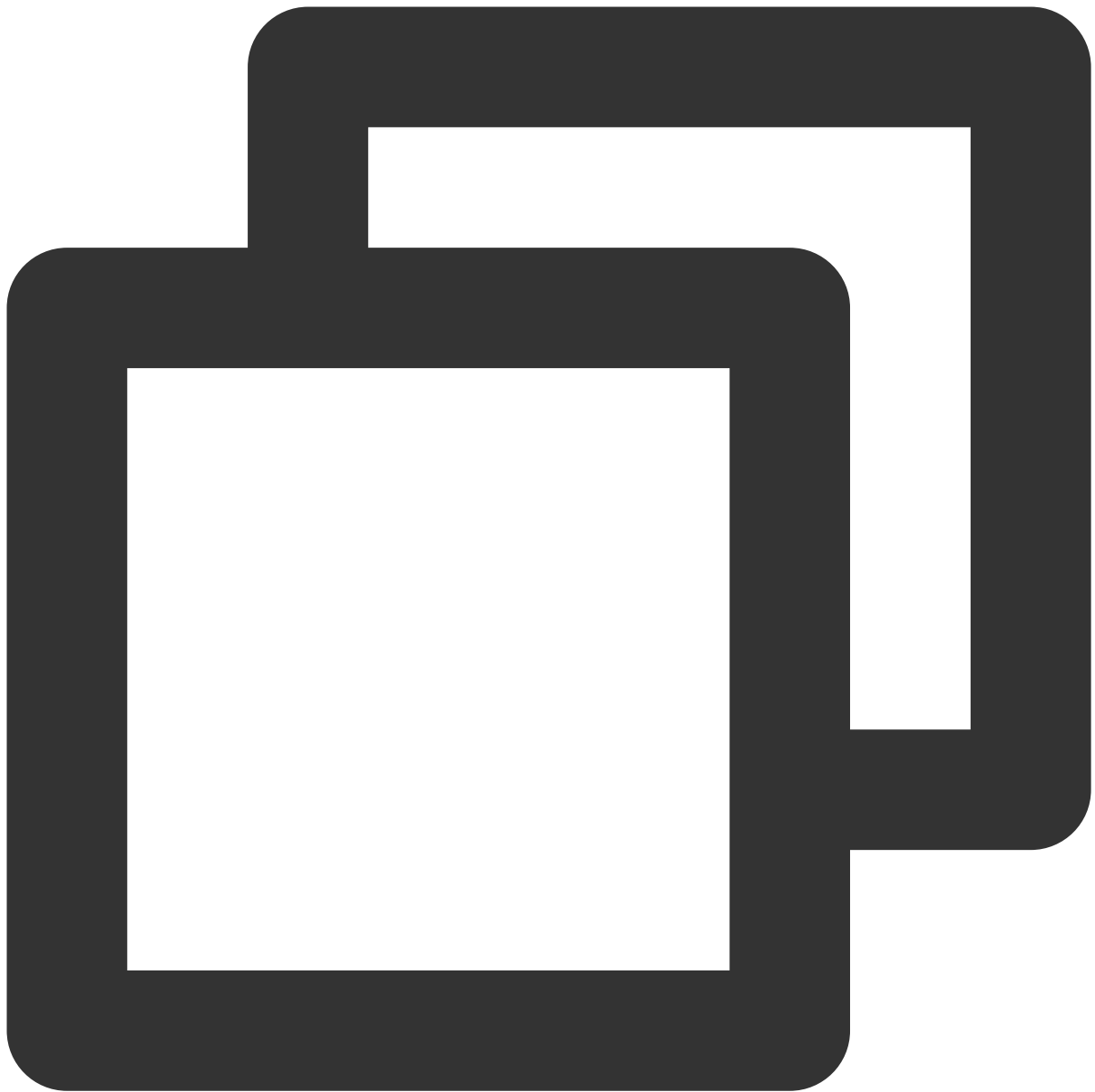
성능 지표

지표	설명
64바이트 UDP 수발신 PPS(패킷/초)	UDP를 통한 데이터 배치 발송 처리량을 나타내며, 이는 네트워크의 최대 전달 능력(패킷 손실이 발생할 수 있음)을 반영합니다.
1500바이트 TCP 수발신 대역폭 (Mbps/초)	TCP를 통한 데이터 배치 발송 처리량을 나타내며, 이는 네트워크의 최대 대역폭 성능(패킷 손실이 발생할 수 있음)을 반영합니다.
TCP-RR(회/초)	TCP 지속 연결 중에 Request/Response 작업을 반복하는 트랜잭션 처리량을 나타내며, 이는 패킷 손실 없는 TCP의 네트워크 전송 능력을 반영합니다.

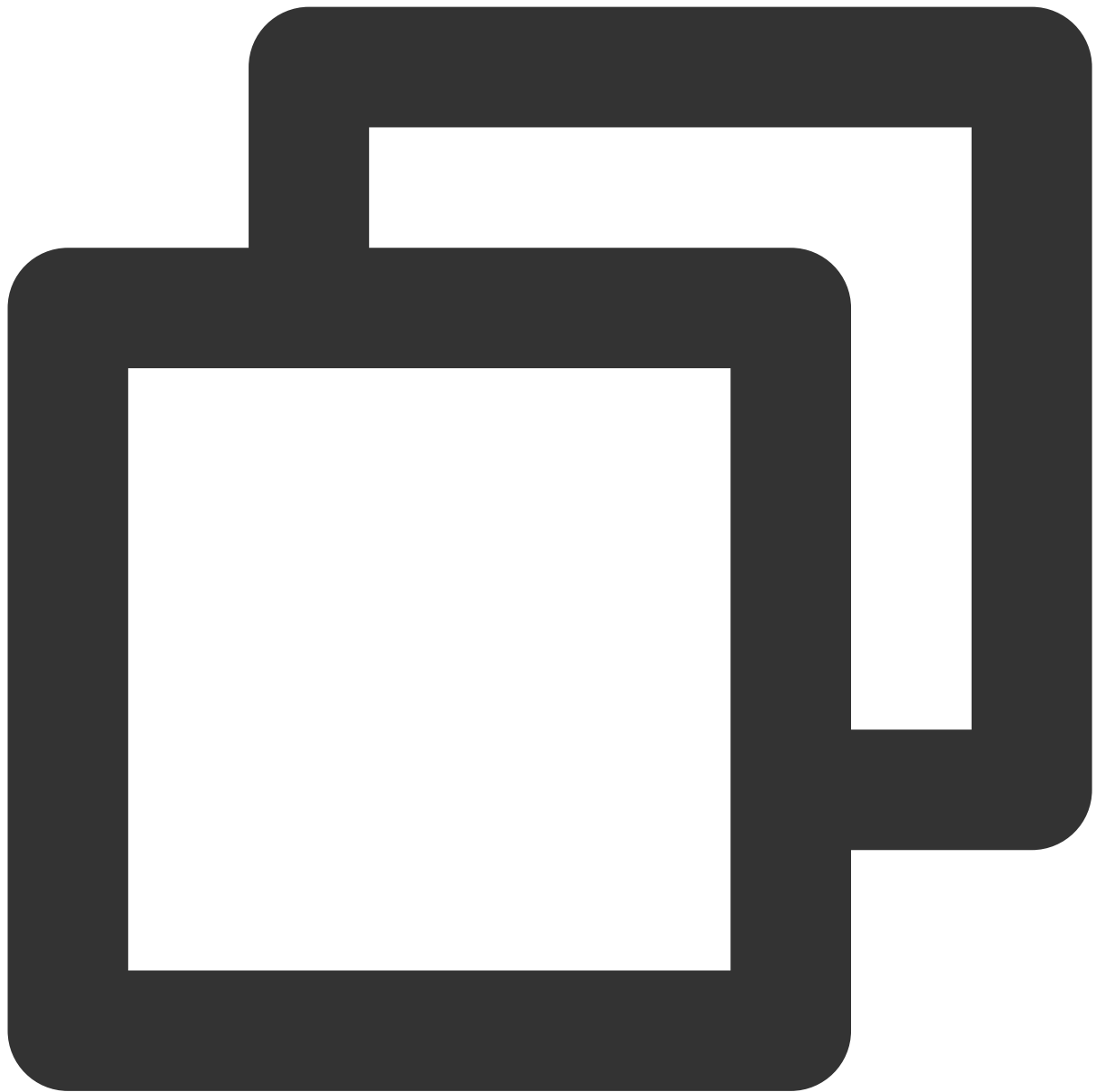
작업 순서

테스트 환경 준비

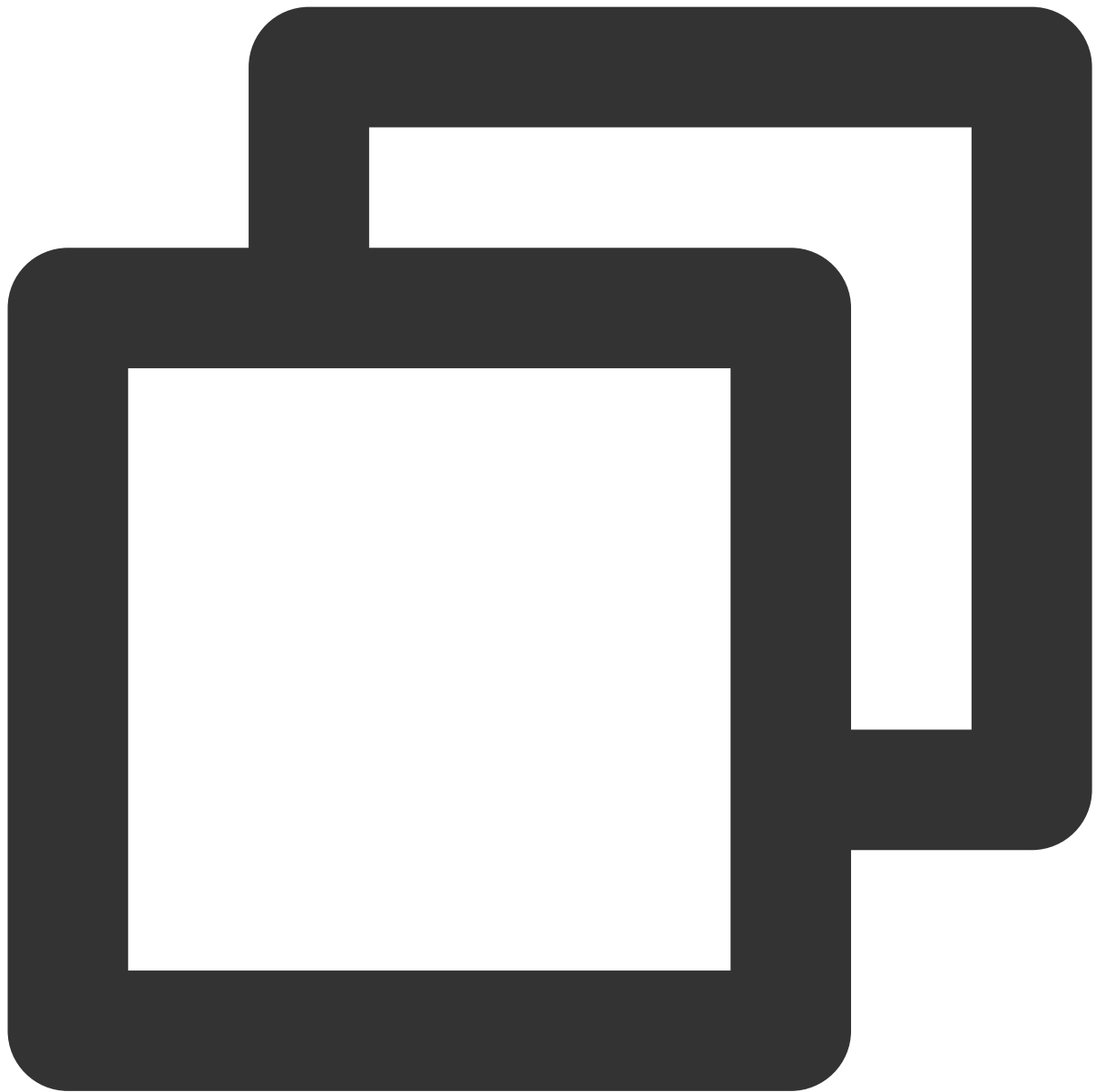
- 테스트 서버 3대를 준비합니다. [사용자 정의 Linux CVM 설정](#)을 참고하여 테스트 서버를 구매합니다. 본문의 테스트 서버는 CentOS 8.2 운영 체제를 사용합니다.
- 테스트 서버에 순서대로 로그인하고 다음 명령을 실행하여 netperf 툴을 다운로드합니다. CVM에 로그인하는 방법은 [Linux 인스턴스에 로그인](#)을 참고하십시오.



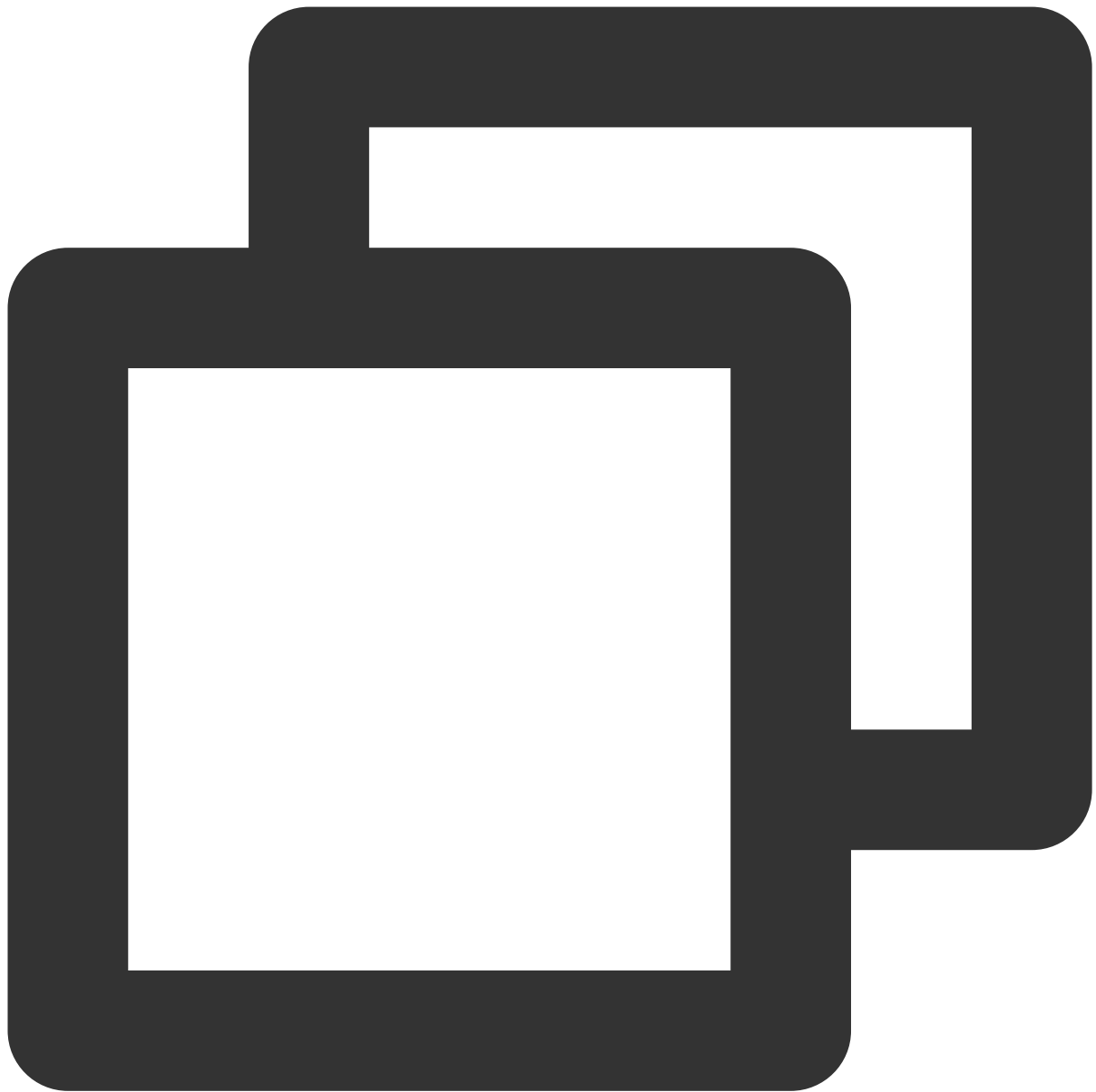
```
yum install -y sysstat wget tar automake make gcc
```



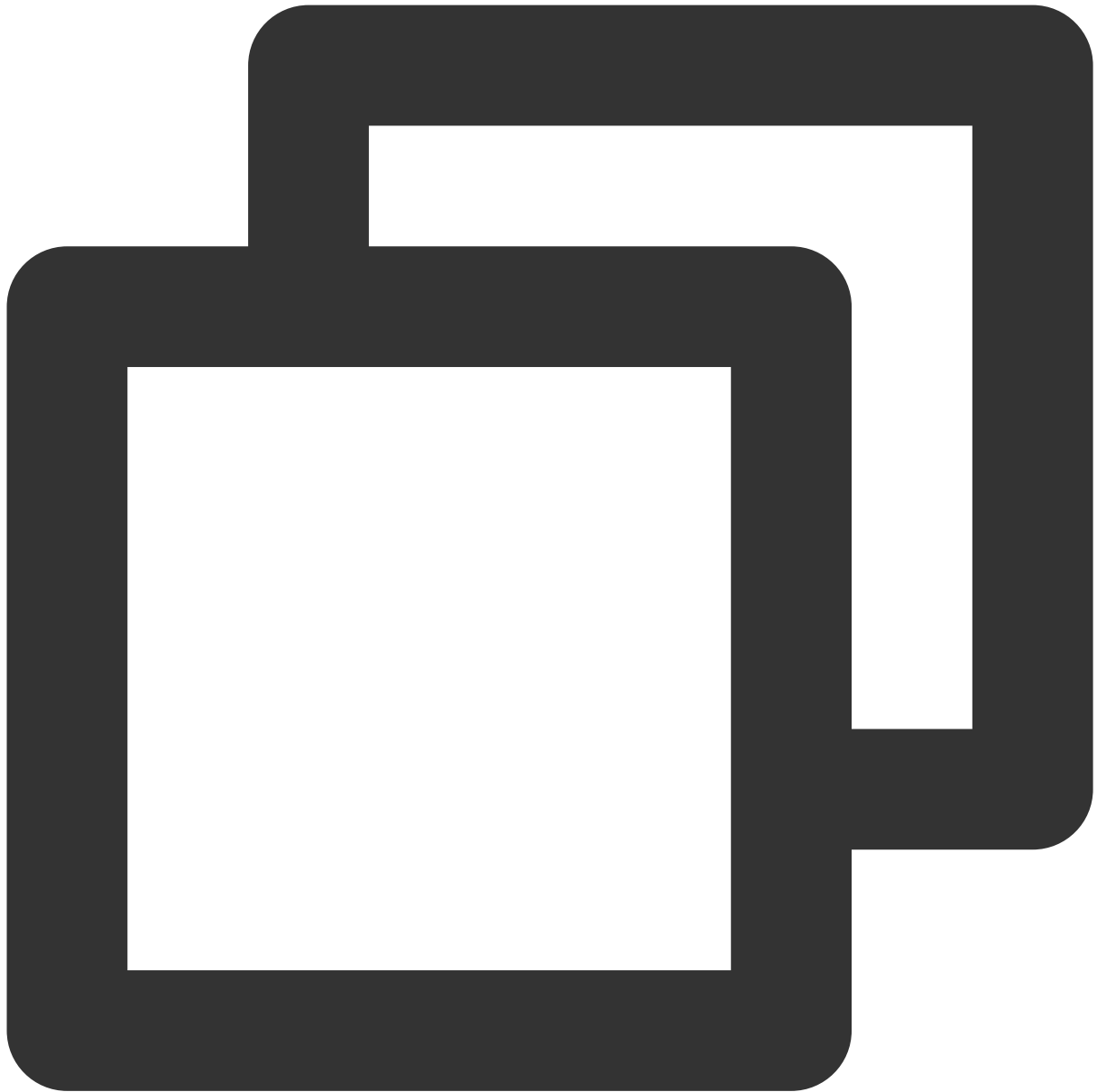
```
wget -O netperf-2.7.0.tar.gz -c https://codeload.github.com/HewlettPackard/netperf
```



```
tar xzf netperf-2.7.0.tar.gz
```

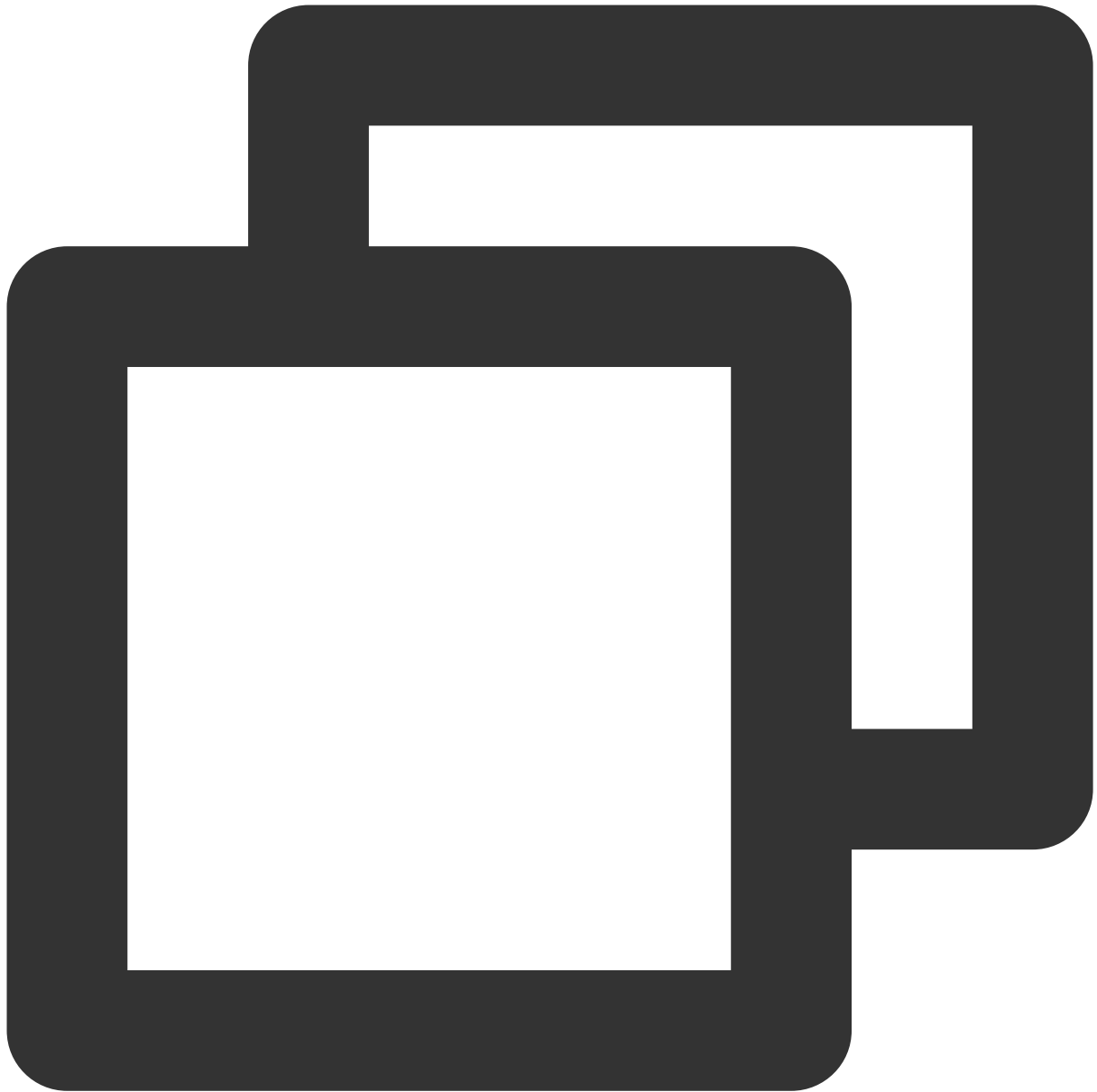
```
cd netperf-netperf-2.7.0
```



```
./autogen.sh && ./configure && make && make install
```

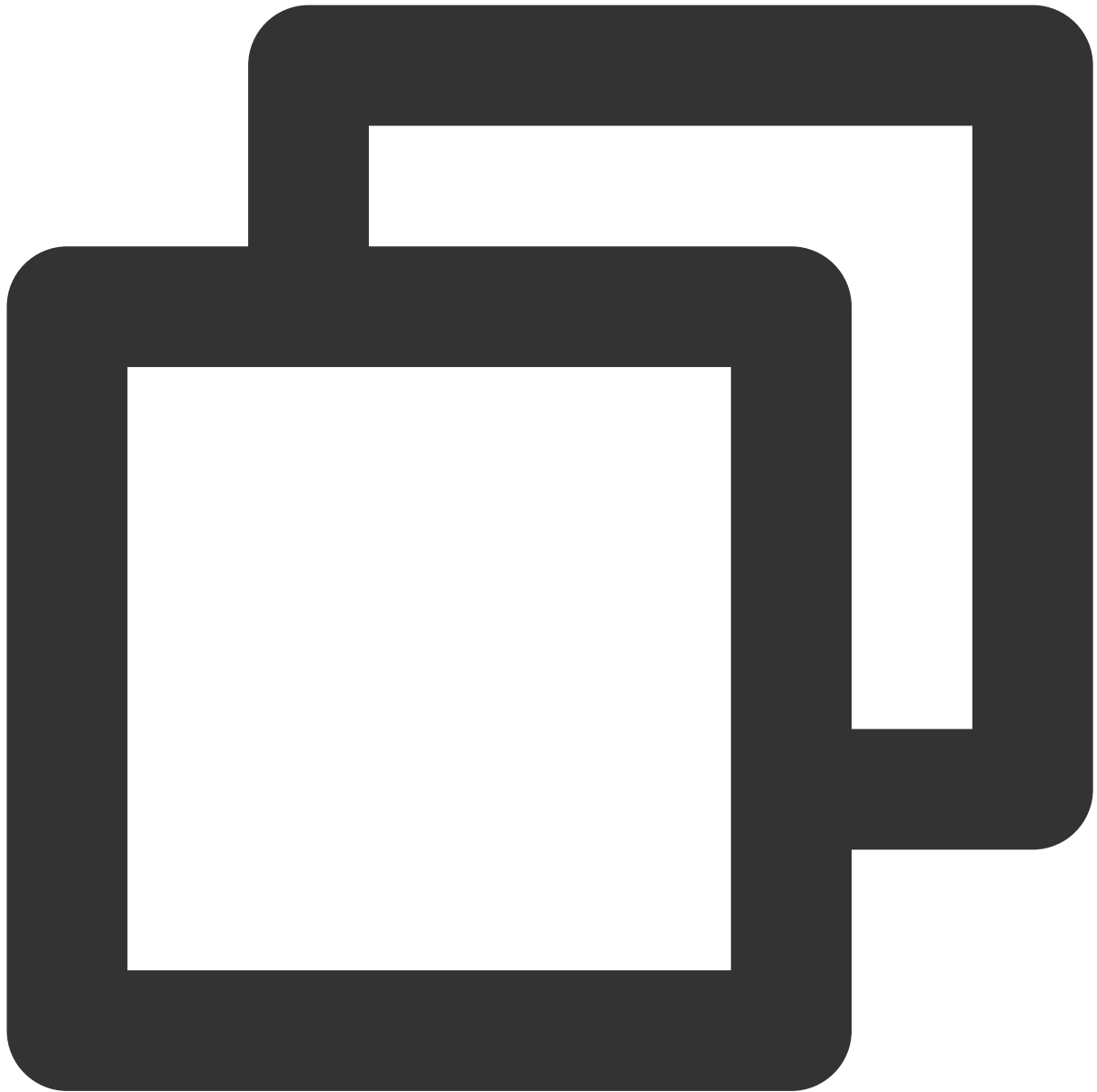
송신 패킷 성능 테스트

1. 디바이스에서 다음 명령을 실행하여, 나머지 `netperf` 및 `netserver` 프로세스를 중지합니다.



```
pskill netserver && pskill netperf
```

2. 디바이스 a를 클라이언트로, 디바이스 b와 c를 서버로 사용합니다. 서버에서 다음 명령을 실행하여 netserver를 실행합니다.



```
netserver
```

반환 결과가 아래 이미지와 같으면 아직 다른 netserver 프로세스가 있음을 의미합니다. [1단계](#)의 명령을 실행하여 프로세스를 중지합니다.

```
[root@VM-2-8-centos ~]# netserver
Unable to start netserver with 'IN(6)ADDR_ANY' port '12865' and family AF_
[root@VM-2-8-centos ~]#
```

반환 결과가 아래 이미지와 같으면 netserver가 성공적으로 실행되었음을 의미하므로 다음 단계를 진행합니다.

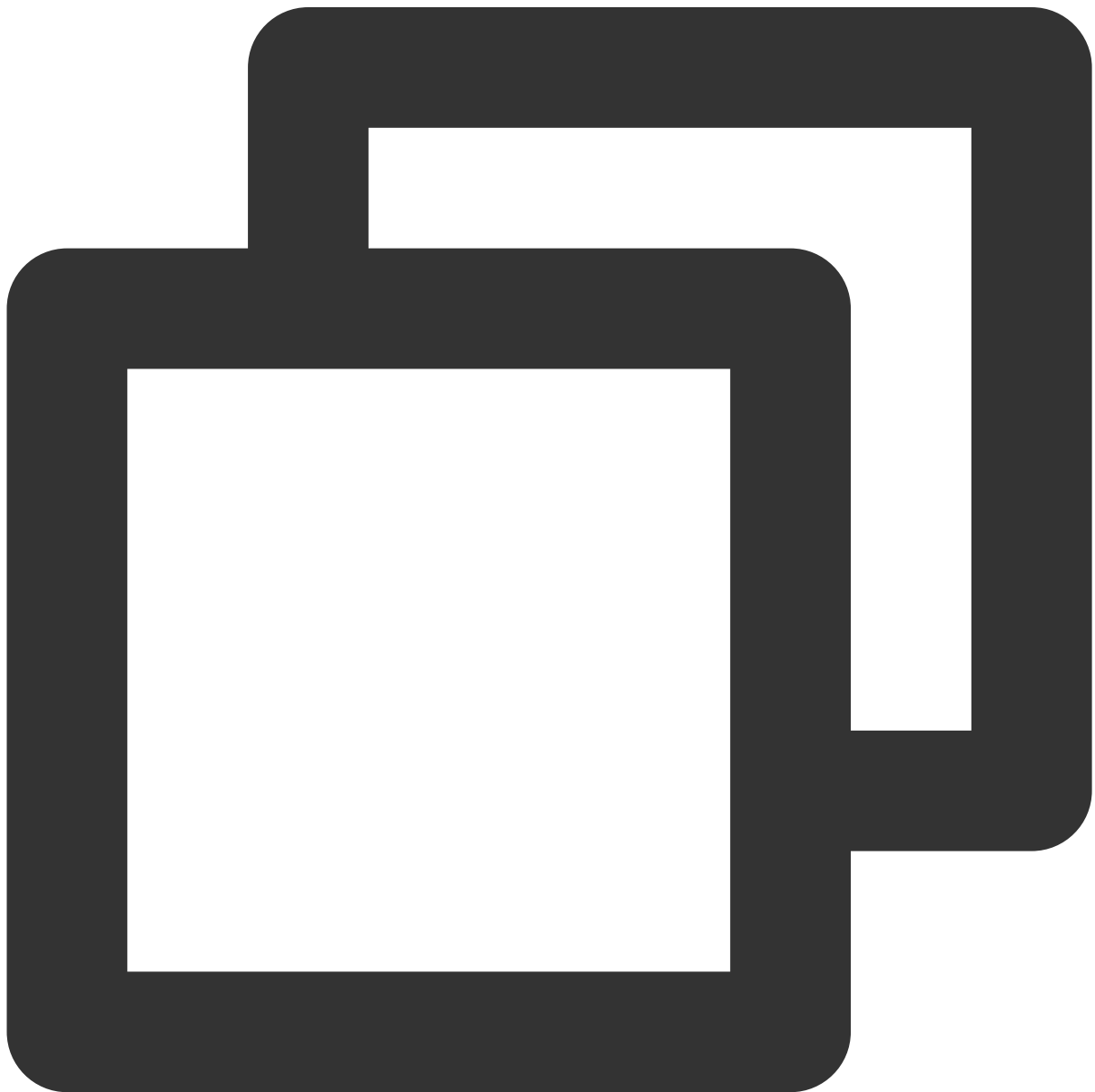
```
[root@VM-2-8-centos ~]# netserver
Starting netserver with host 'IN(6)ADDR_ANY' port '12865' and family AF_UNSPEC
[root@VM-2-8-centos ~]#
```

3. 클라이언트에서 [테스트 시나리오](#)에 제공된 명령을 실행하고, 클라이언트의 패킷 발송 성능이 더 이상 증가하지 않을 때까지 netperf 프로세스를 계속 늘리거나 줄입니다.

설명 :

명령을 반복 실행하고 server IP는 다른 서버 IP를 사용해야 합니다. 프로세스가 최대 성능에 도달하지 못하는 경우 [테스트 보조 스크립트](#)를 실행하여 프로세스를 일괄 실행할 수 있습니다.

4. 클라이언트에서 다음 명령을 실행하여 클라이언트의 패킷 전송 성능 변화를 모니터링하고 최대값을 얻습니다.

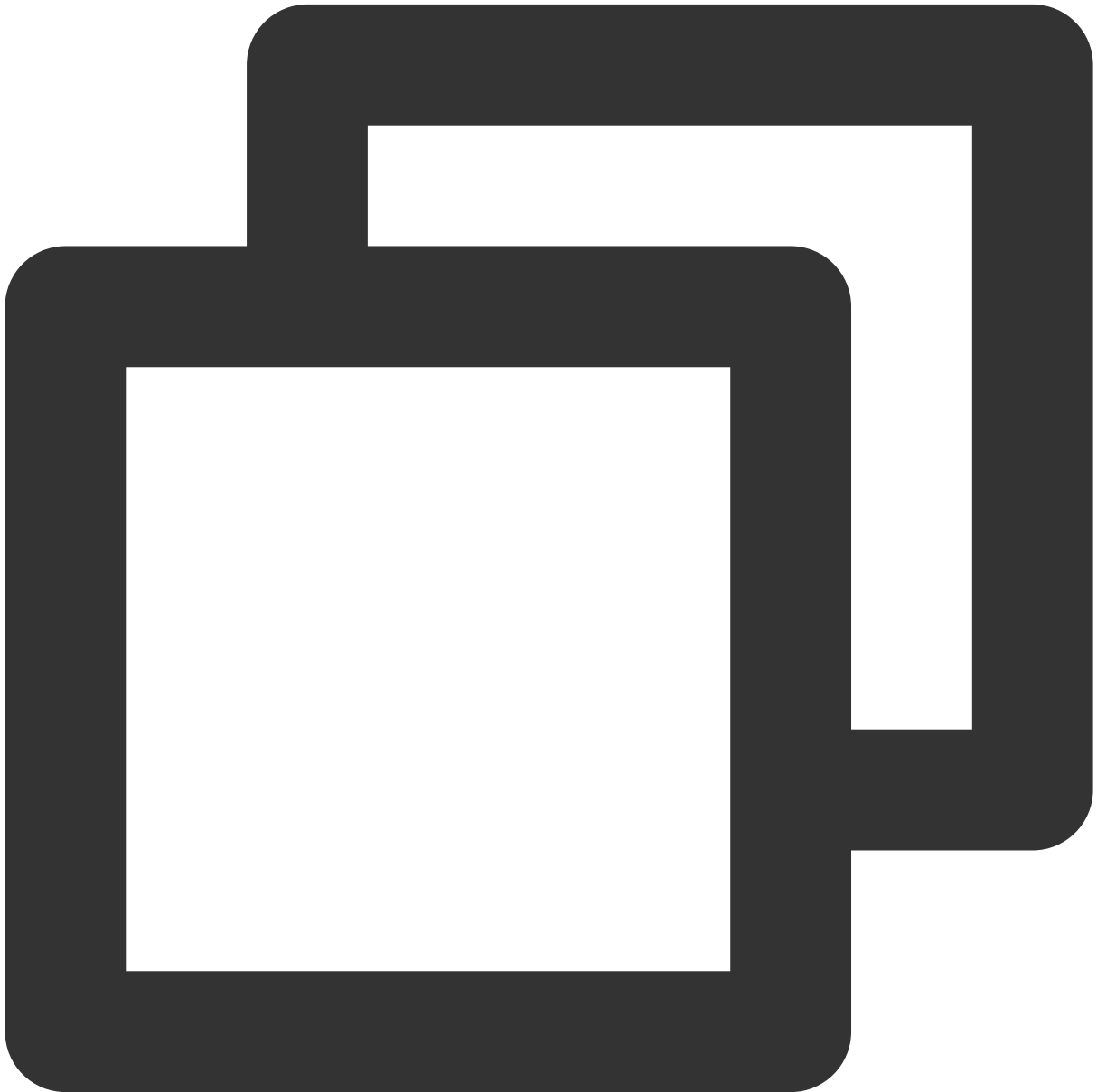


```
sar -n DEV 1
```

얻어진 결과에 따라 [성능 지표](#)를 참고하여 분석을 진행하고, 높은 처리량의 CVM 네트워크의 성능을 측정합니다.

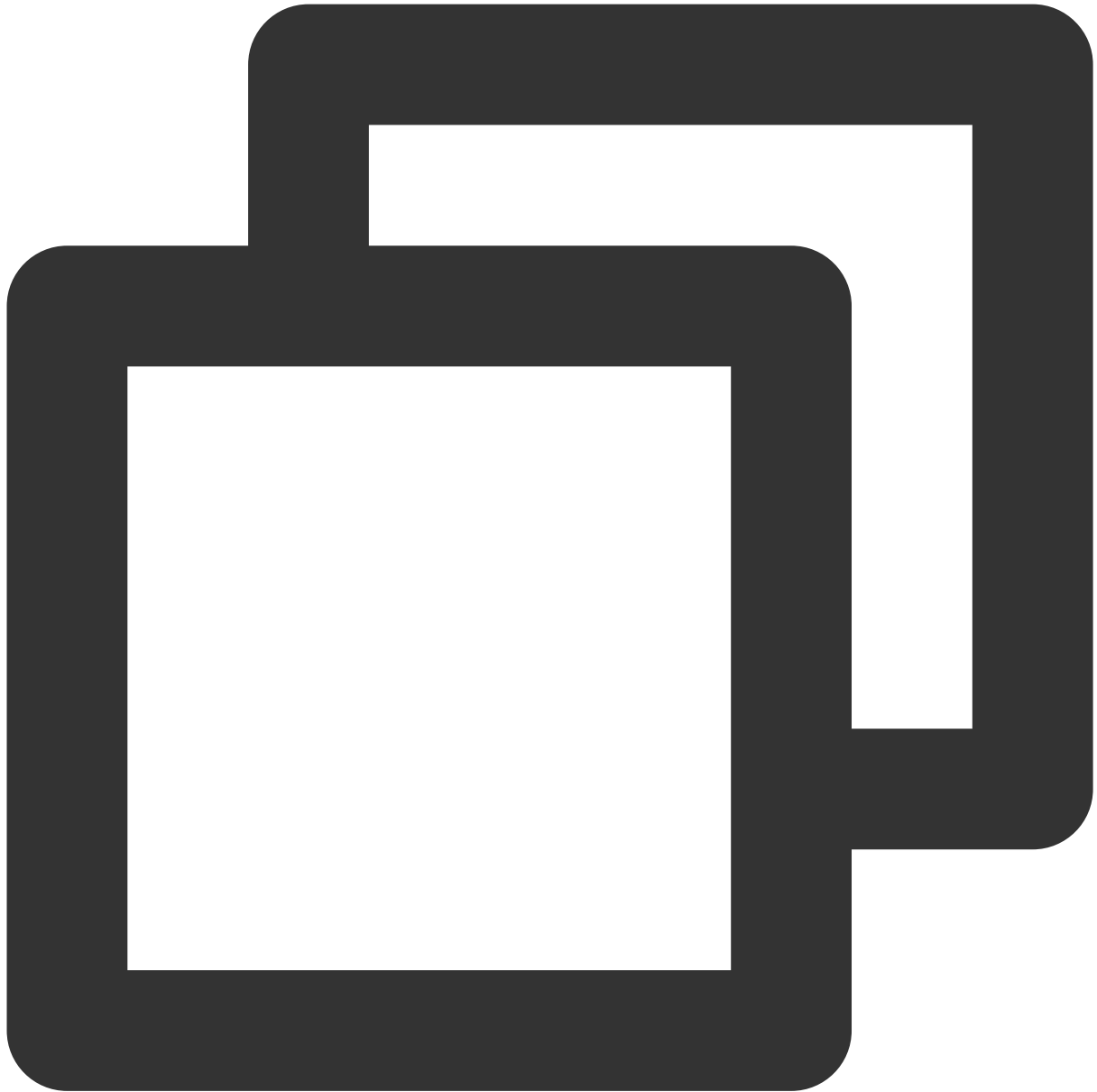
수신 패킷 테스트

1. 디바이스에서 다음 명령을 실행하여 나머지 netperf 및 netserver 프로세스를 중지합니다.



```
pkill netserver && pkill netperf
```

2. 디바이스 a를 서버로, 디바이스 b와 c를 클라이언트로 사용합니다. 서버에서 다음 명령을 실행하여 netserver를 실행합니다.



```
netserver
```

반환 결과가 아래 이미지와 같으면 아직 다른 netserver 프로세스가 있음을 의미합니다. 프로세스를 중지하려면 [1단계](#)의 명령을 실행하십시오.

```
[root@VM-2-8-centos ~]# netserver
Unable to start netserver with 'IN(6)ADDR_ANY' port '12865' and family AF_
[root@VM-2-8-centos ~]#
```

반환 결과가 아래 이미지와 같으면 netserver가 성공적으로 실행되었음을 의미하므로 다음 단계를 진행합니다.

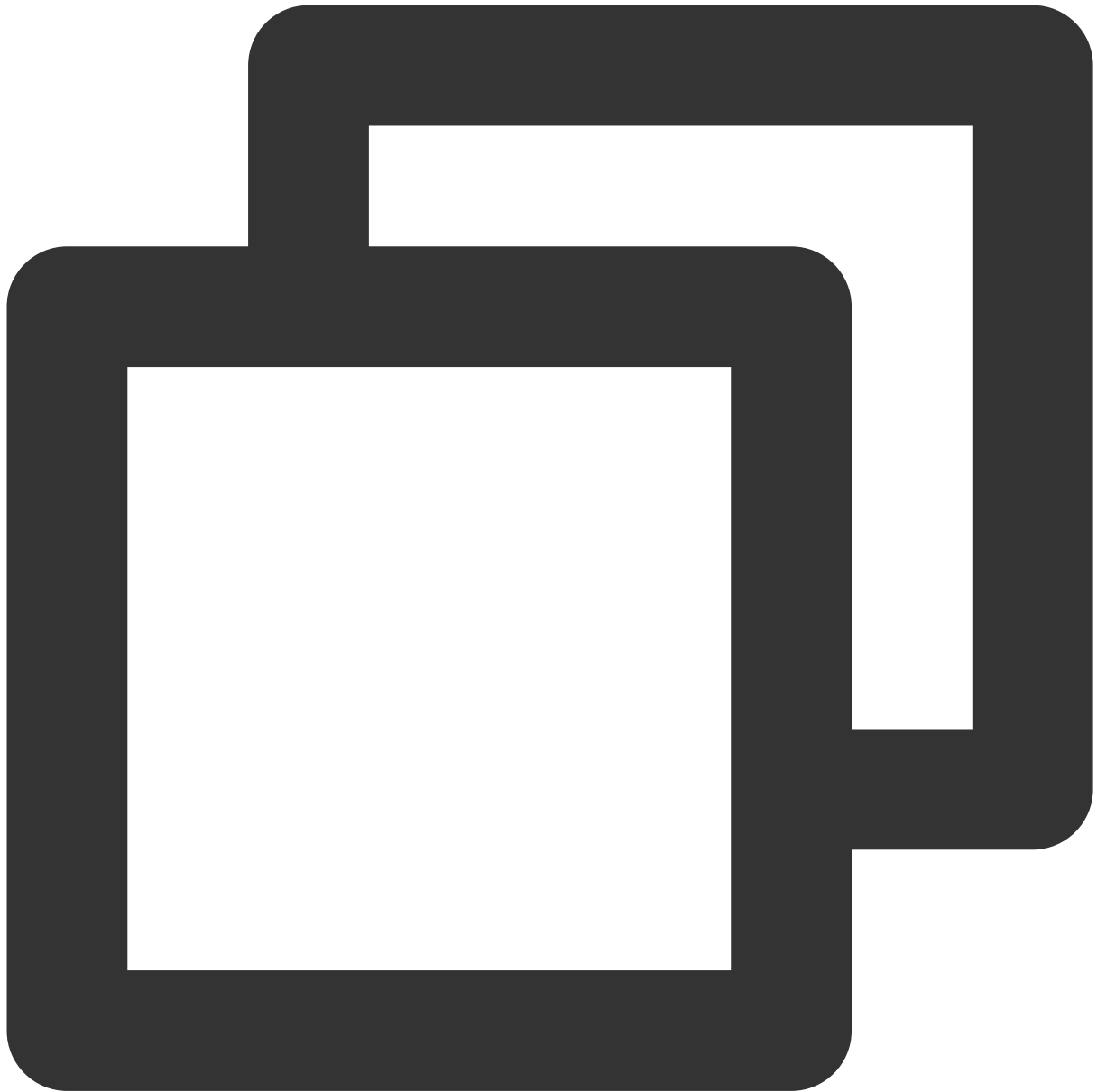
```
[root@VM-2-8-centos ~]# netserver
Starting netserver with host 'IN(6)ADDR_ANY' port '12865' and family AF_UN
[root@VM-2-8-centos ~]#
```

3. 클라이언트에서 [테스트 시나리오](#)에 제공된 명령을 실행하고, 클라이언트의 패킷 발송 성능이 더 이상 증가하지 않을 때까지 netperf 프로세스를 계속 늘리거나 줄입니다.

설명 :

명령을 반복 실행하고 각각의 클라이언트에서 netperf를 전송합니다. 프로세스가 최대 성능에 도달하지 못하는 경우 [테스트 보조 스크립트](#)를 실행하여 프로세스를 일괄 실행할 수 있습니다.

4. 클라이언트에서 다음 명령을 실행하여 클라이언트의 패킷 전송 성능 변화를 모니터링하고 최대값을 얻습니다.



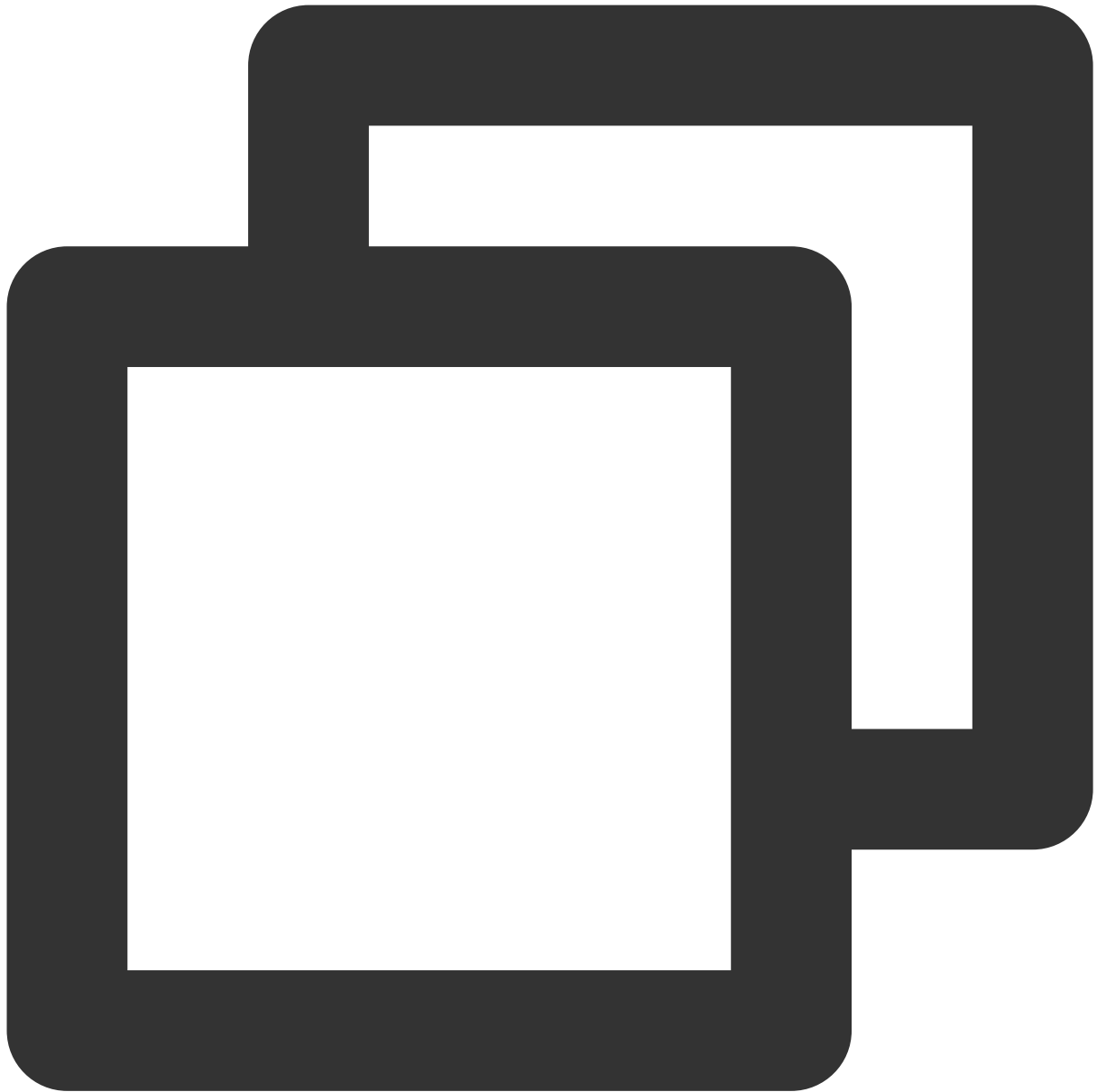
```
sar -n DEV 1
```

얻어진 결과에 따라 [성능 지표](#)를 참고하여 분석을 진행하고, 높은 처리량의 CVM 네트워크의 성능을 측정합니다.

부록

테스트 보조 스크립트

이 스크립트를 실행하면 여러 netperf 프로세스를 빠르게 전달할 수 있습니다.



```
#!/bin/bash
count=$1
for ((i=1;i<=count;i++))
do
    echo "Instance:$i-----"
    # 아래 명령은 테스트 시나리오 테이블의 명령으로 대체할 수 있습니다.
    # -H 뒤에 서버 IP 주소를 입력합니다.
    # -l 뒤는 테스트 시간으로, netperf 사전 종료를 방지하기 위해 시간을 10000으로 설정하십시오
    netperf -t UDP_STREAM -H <server ip> -l 10000 -- -m 64 -R 1 &
done
```


DPDK 테스트 방법

최종 업데이트 날짜: : 2024-02-02 10:56:28

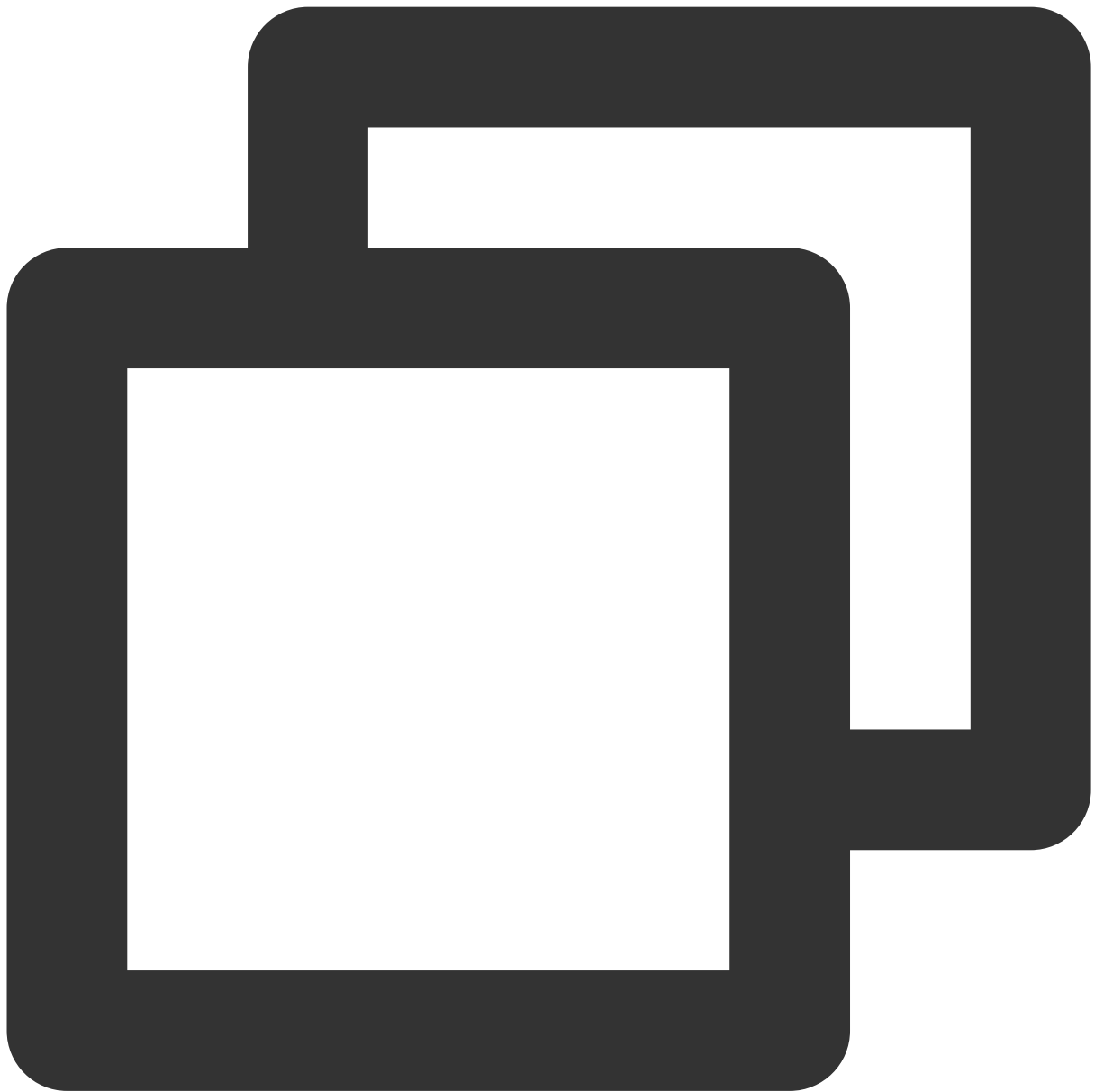
작업 시나리오

본문은 DPDK 방법을 사용하여 높은 처리량의 CVM 네트워크 성능을 테스트하는 방법을 설명합니다.

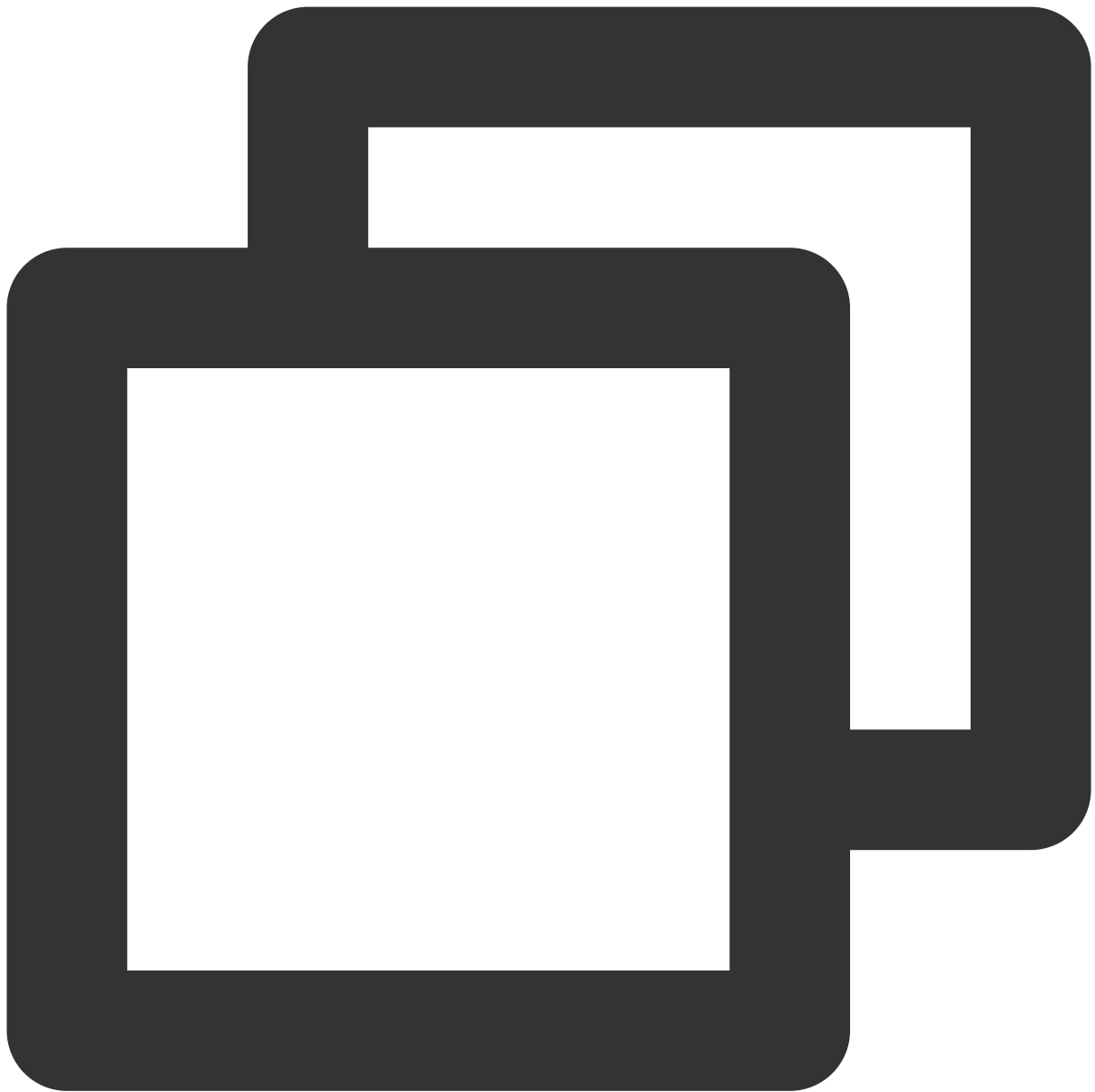
작업 단계

DPDK 컴파일 및 설치

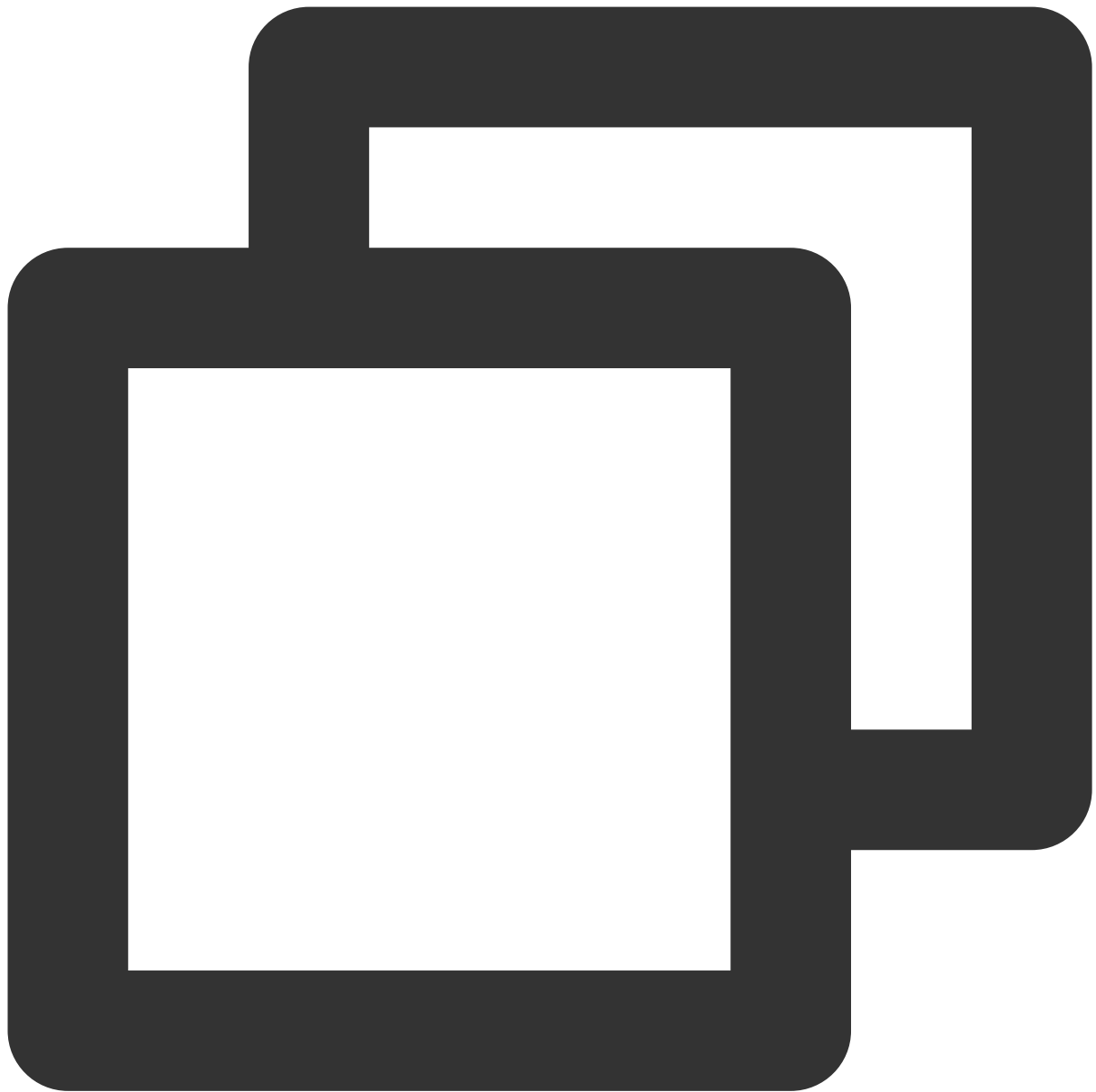
1. 테스트 서버 2대를 준비합니다. [Linux CVM 커스텀 설정](#)을 참고하여 테스트 서버를 구매하십시오. 본문의 테스트 서버는 CentOS 8.2 운영 체제를 사용합니다.
2. 테스트 서버에 하나씩 로그인하고 다음 명령을 실행하여 DPDK 도구를 다운로드합니다. CVM에 로그인하는 방법은 [Linux 인스턴스에 로그인](#)을 참고하십시오.



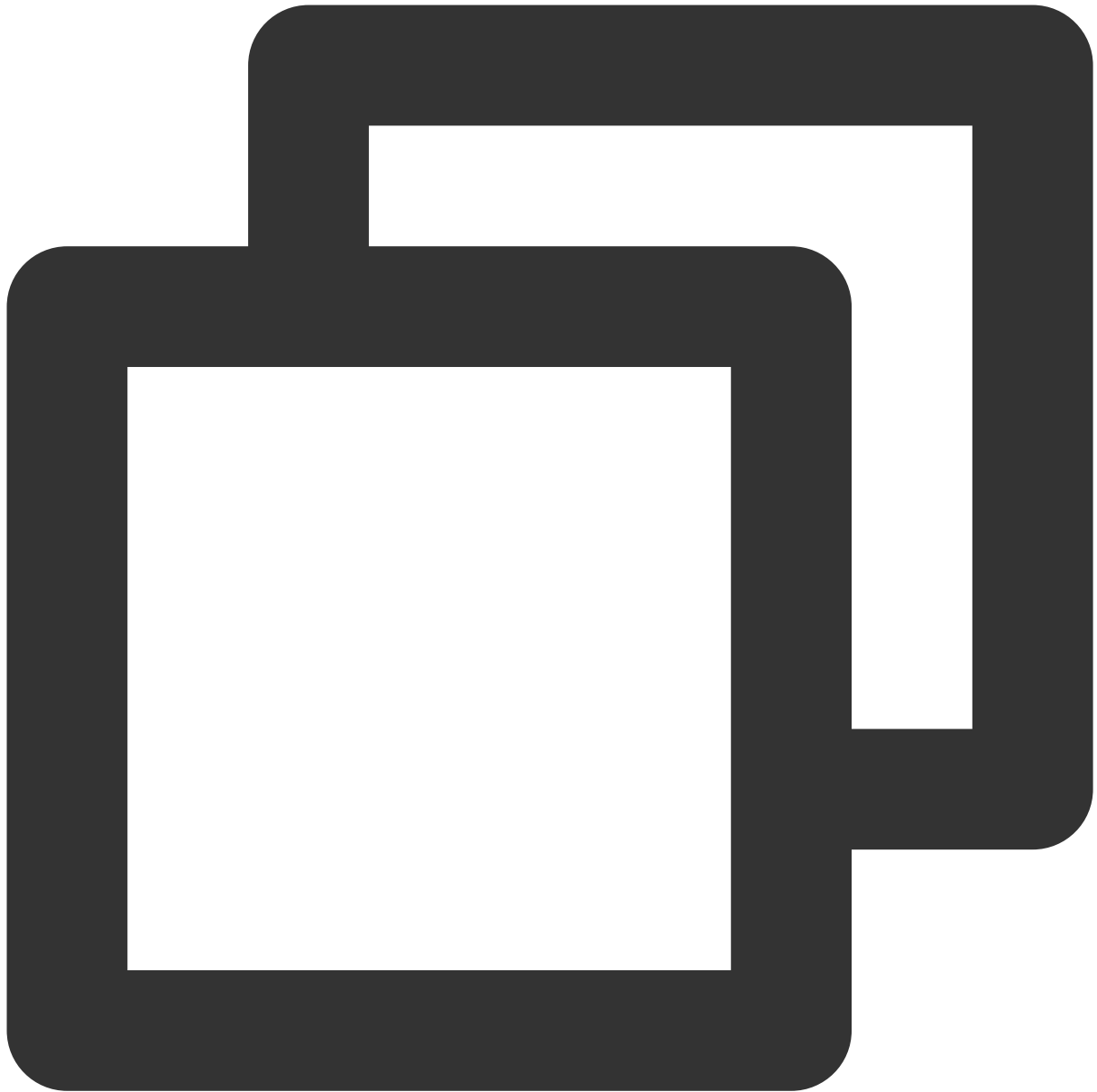
```
yum install -y sysstat wget tar automake make gcc
```



```
wget http://git.dpdk.org/dpdk/snapshot/dpdk-17.11.tar.gz
```

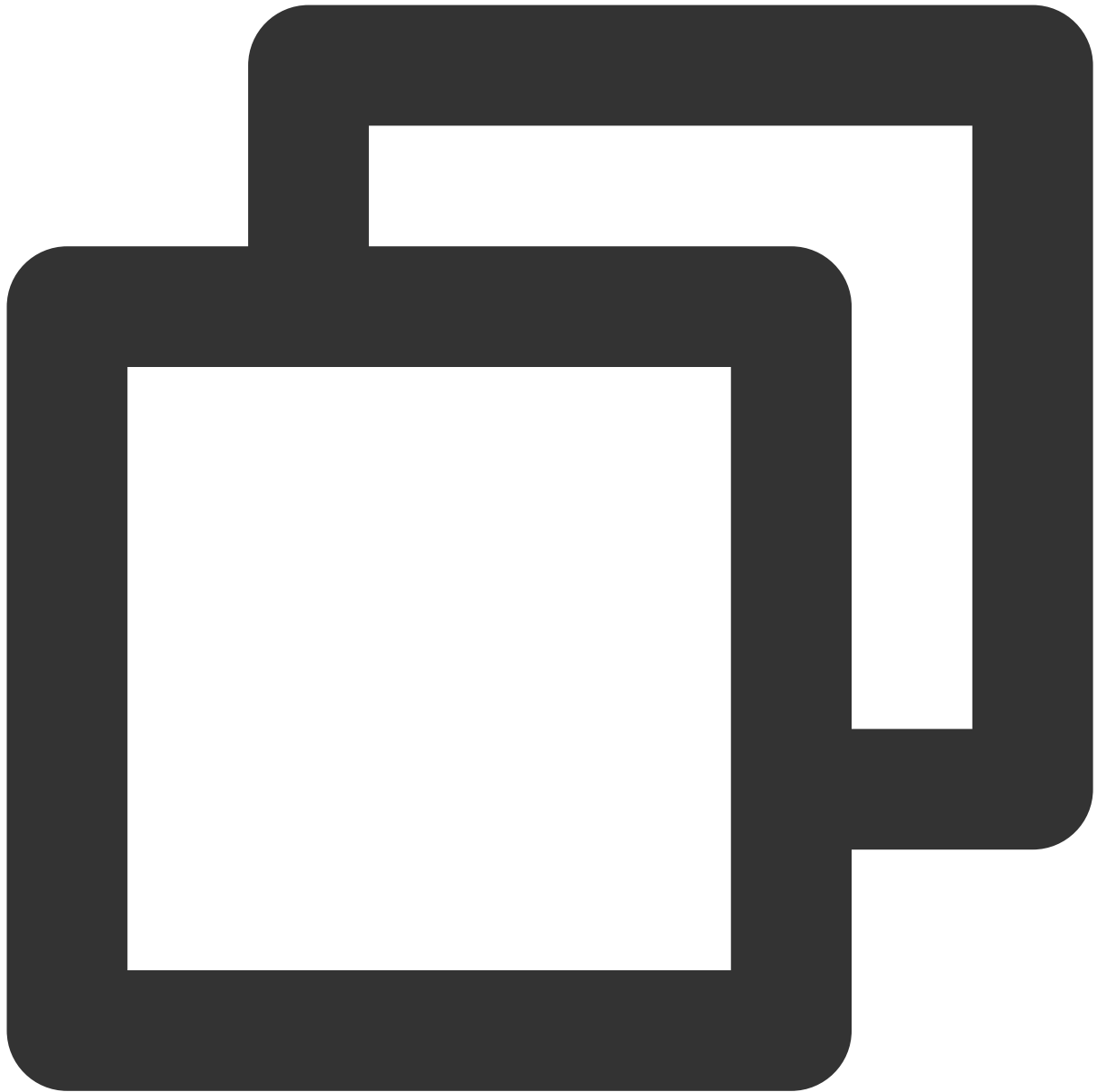


```
tar -xf dpdk-17.11.tar.gz
```



```
mv dpdk-17.11 dpdk
```

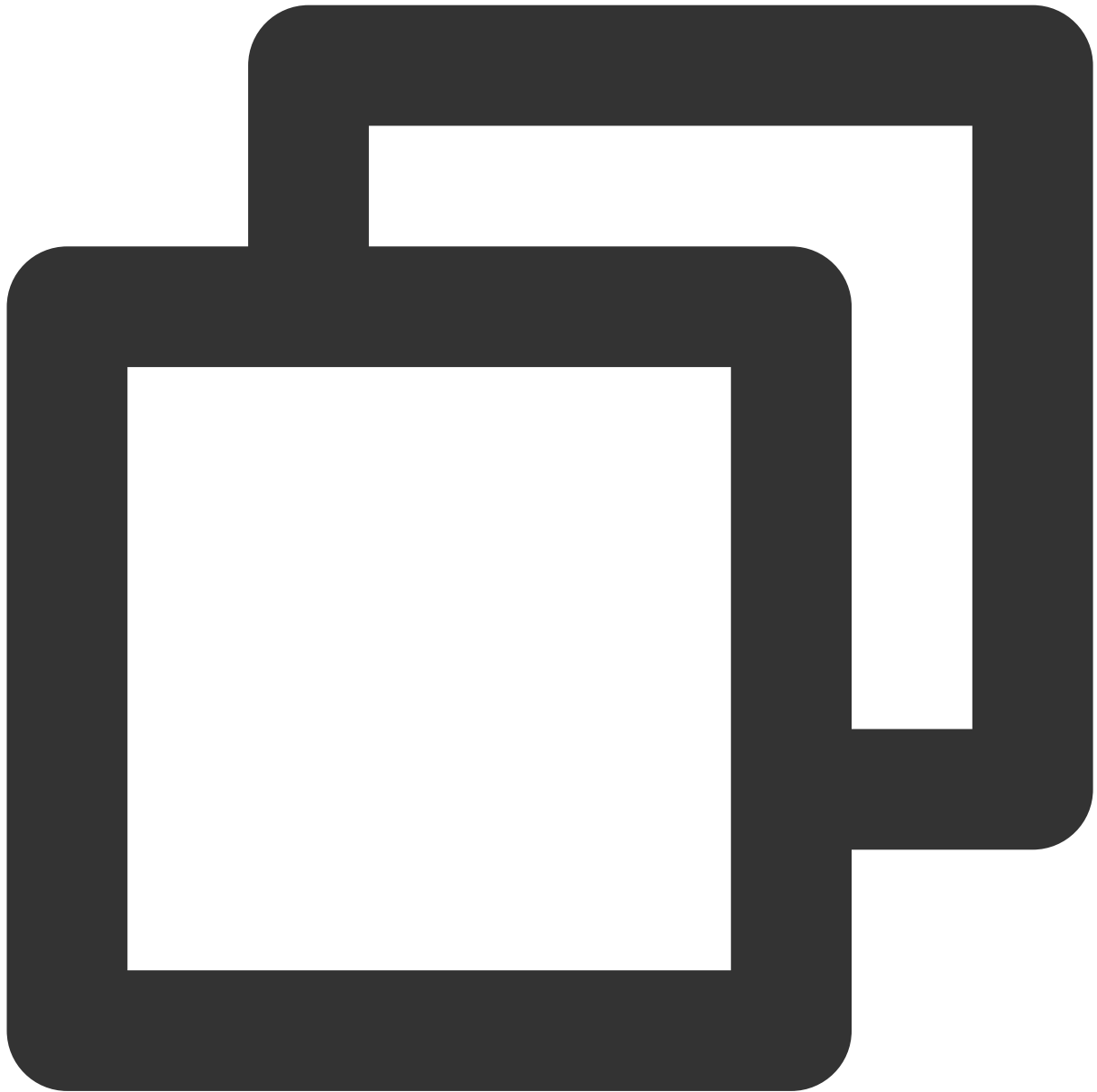
3. txonly 엔진을 수정하여 각 DPDK 송신 패킷의 CPU 상의 UDP 트래픽 포트가 여러 스트림을 생성하도록 합니다. 다음 명령어를 실행하여 `dpdk/app/test-pmd/txonly.c` 파일을 수정합니다.



```
vim dpdk/app/test-pmd/txonly.c
```

i를 눌러 편집 모드로 들어가 다음 내용을 수정합니다.

3.1.1 `#include "testpmd.h"` 를 찾아 새 행에 다음 내용을 입력합니다.



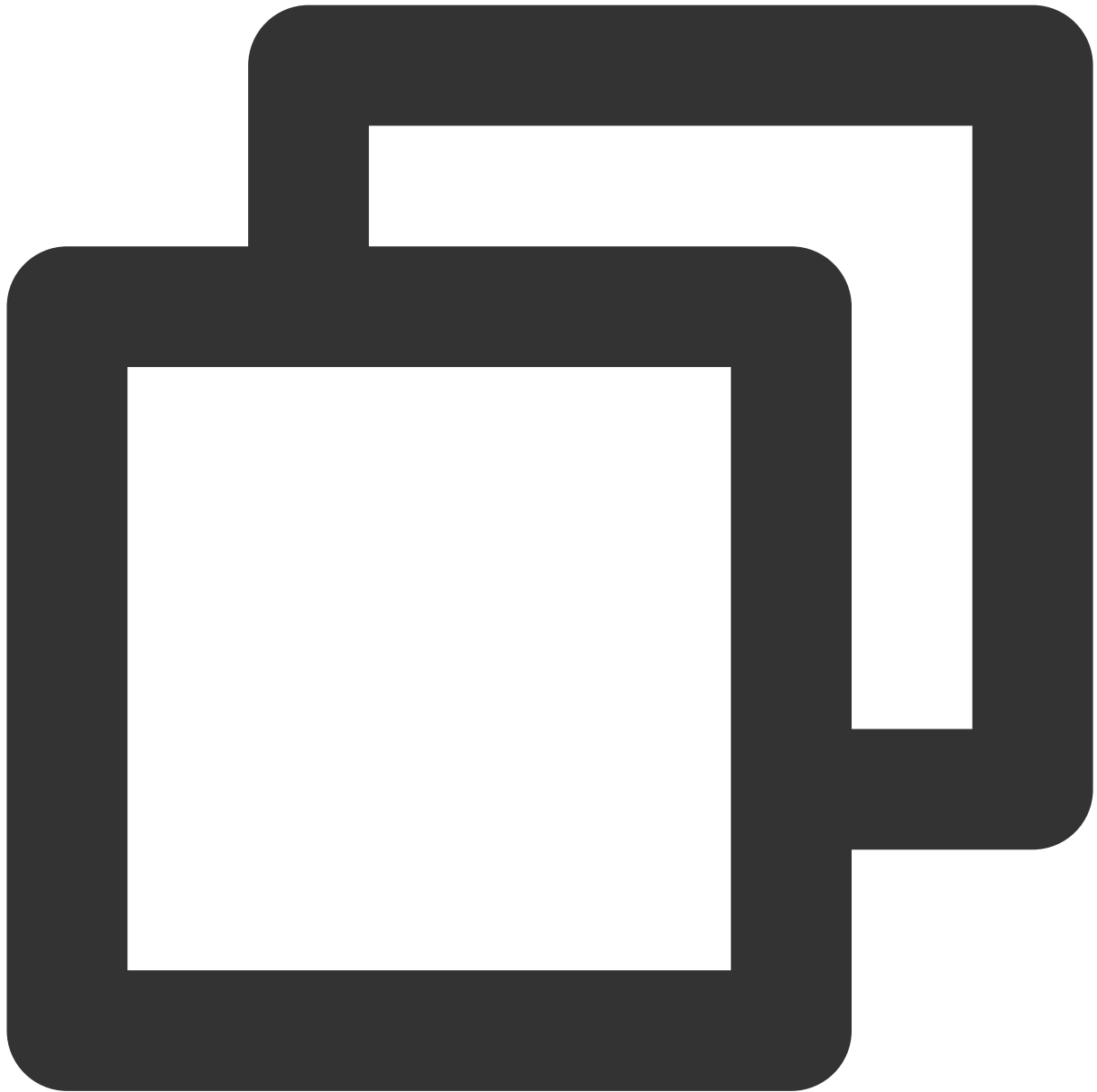
```
RTE_DEFINE_PER_LCORE(struct udp_hdr, lcore_udp_hdr);  
RTE_DEFINE_PER_LCORE(uint16_t, test_port);
```

다음과 같이 수정을 완료합니다.

```
#include "testpmd.h"
RTE_DEFINE_PER_LCORE(struct udp_hdr, lcore)
RTE_DEFINE_PER_LCORE(uint16_t, test_port)

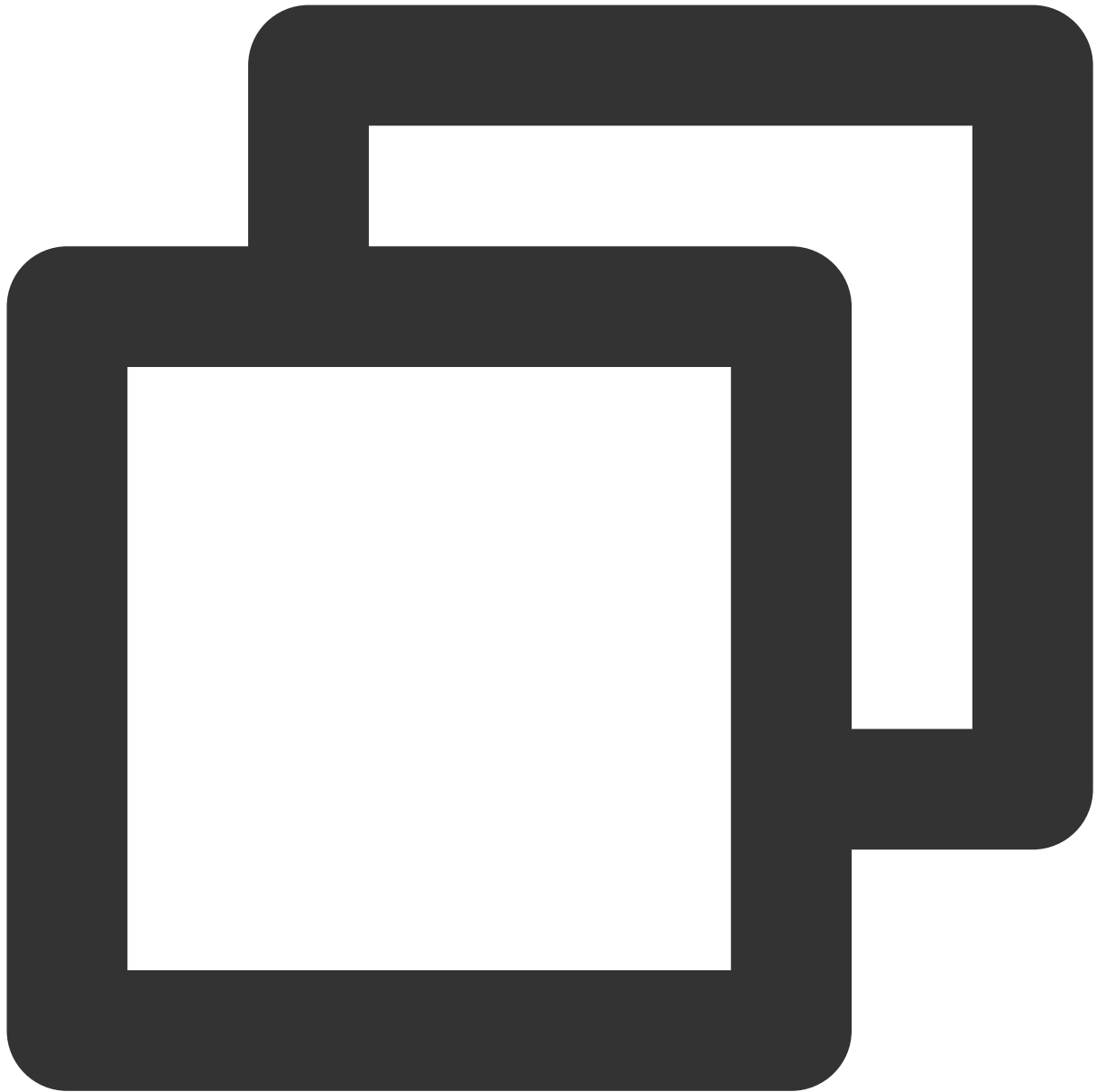
#define UDP_SRC_PORT 1024
#define UDP_DST_PORT 1024
```

3.1.2 `ol_flags |= PKT_TX_MACSEC;` 를 찾아 새 행에 다음 내용을 입력합니다.



```
/* dummy test udp port */  
memcpy(&RTE_PER_LCORE(lcore_udp_hdr), &pkt_udp_hdr, sizeof(pkt_udp_hdr));
```

3.1.3 그 다음 아래의 `for (nb_pkt = 0; nb_pkt < nb_pkt_per_burst; nb_pkt++) {` 을 찾아 새 행에 다음 내용을 입력합니다.



```
RTE_PER_LCORE(test_port)++;  
RTE_PER_LCORE(lcore_udp_hdr).src_port = rte_cpu_to_be_16(rte_lcore_id() * 199 + tes  
RTE_PER_LCORE(lcore_udp_hdr).dst_port = rte_cpu_to_be_16(rte_lcore_id() * 2000 + te
```

다음과 같이 수정을 완료합니다.

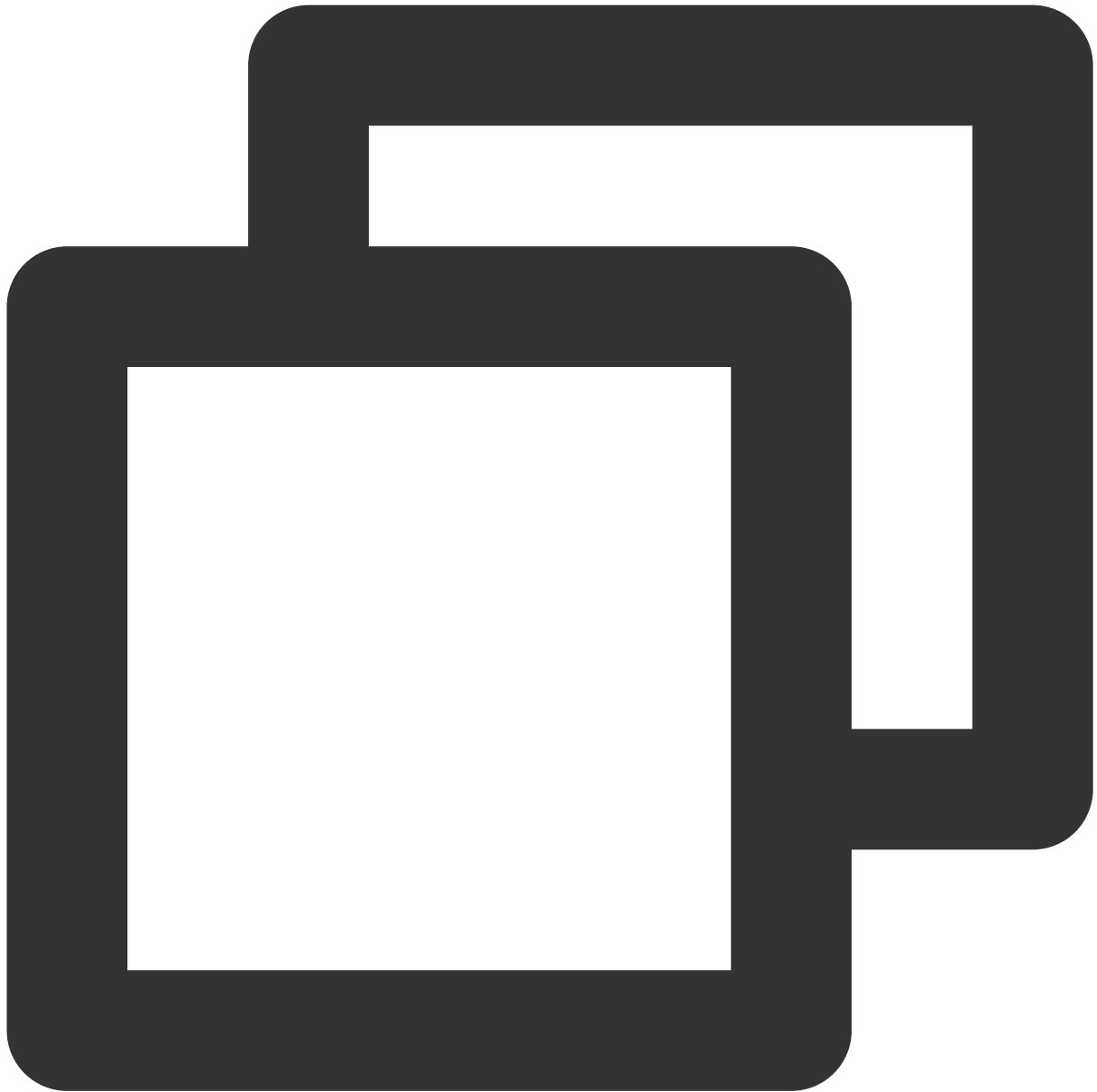
```
if (txp->tx_ol_flags & TESTPMD_TX_OFFLOAD_INSERT_QINQ)
    ol_flags |= PKT_TX_QINQ_PKT;
if (txp->tx_ol_flags & TESTPMD_TX_OFFLOAD_MACSEC)
    ol_flags |= PKT_TX_MACSEC;

/* dummy test udp port */
memcpy(&RTE_PER_LCORE(lcore_udp_hdr), &pkt_udp_hdr, sizeof(pkt_udp_hdr));

for (nb_pkt = 0; nb_pkt < nb_pkt per burst; nb_pkt++) {
    RTE_PER_LCORE(test_port)++;
    RTE_PER_LCORE(lcore_udp_hdr).src_port = rte_cpu_to_be_16(2222);
    RTE_PER_LCORE(lcore_udp_hdr).dst_port = rte_cpu_to_be_16(rte_lcore_id() * 2);

    pkt = rte_mbuf_raw_alloc(mbp);
    if (pkt == NULL) {
        nomore_mbuf:
        if (nb_pkt == 0)
            return;
        break;
    }
}
```

3.1.4 `copy_buf_to_pkt(&pkt_udp_hdr, sizeof(pkt_udp_hdr), pkt,` 를 찾아, 다음 내용으로 바꿉니다.



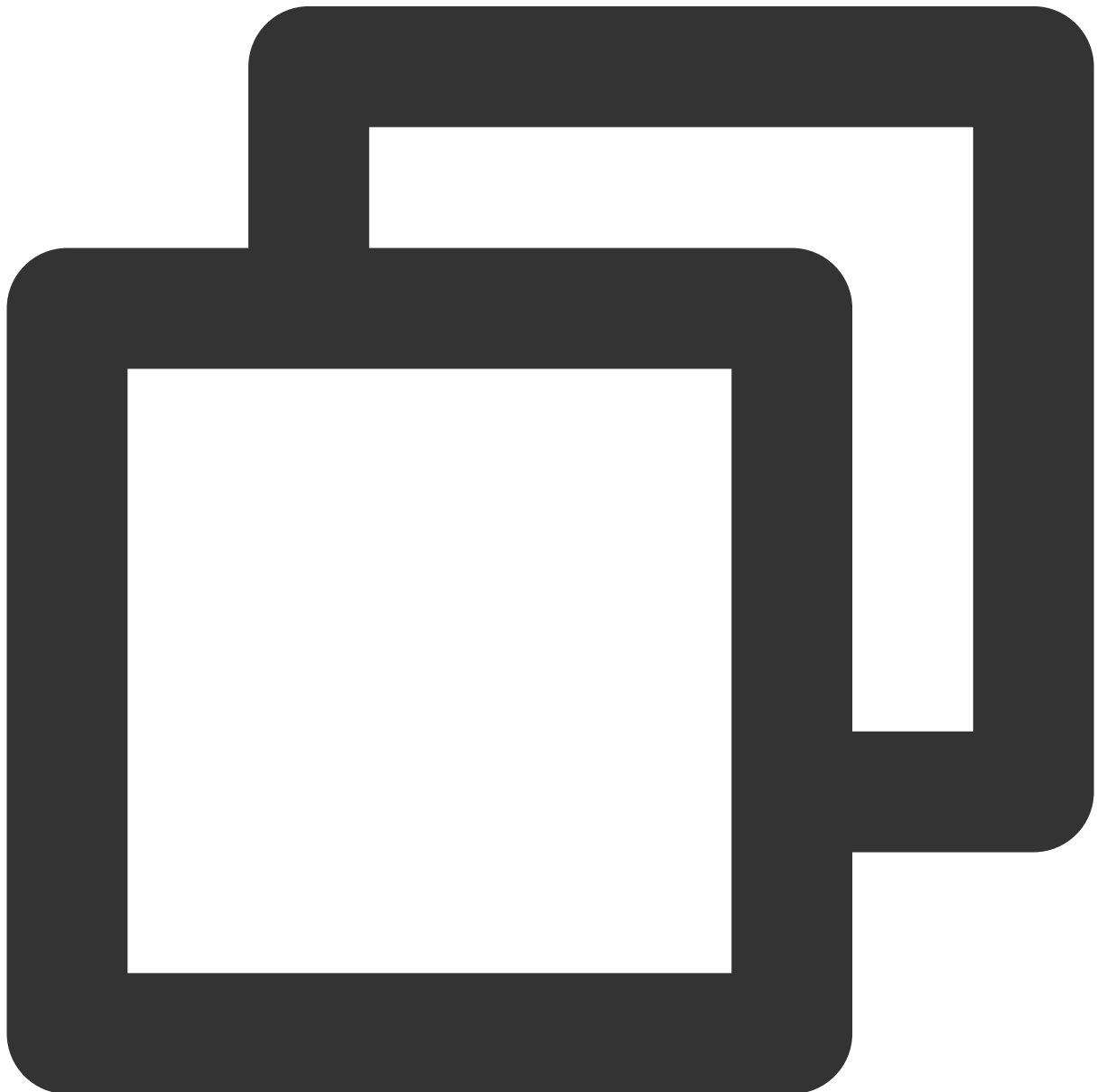
```
copy_buf_to_pkt (&RTE_PER_LCORE (lcore_udp_hdr), sizeof (RTE_PER_LCORE (lcore_udp_hdr))
```

다음과 같이 수정을 완료합니다.

```
copy_buf_to_pkt(&eth_hdr, sizeof(eth_hdr), pkt, 0);
copy_buf_to_pkt(&pkt_ip_hdr, sizeof(pkt_ip_hdr), pkt,
                sizeof(struct ether_hdr));
copy_buf_to_pkt(&RTE_PER_LCORE(lcore_udp_hdr), sizeof(RTE_PER_LCORE(lcore_
                sizeof(struct ether_hdr) +
                sizeof(struct ipv4_hdr));
```

Esc를 누르고 **:wq**를 입력하여 수정 사항을 저장하고 종료합니다.

다음 명령어를 실행하여 `dptk/config/common_base` 파일을 수정합니다.



```
vim dptk/config/common_base
```


i를 눌러 편집 모드로 들어가 `CONFIG_RTE_MAX_MEMSEG=256` 을 찾아 1024로 수정합니다. 수정 완료 후는 다음 이미지와 같습니다.

```
CONFIG_RTE_LIBRTE_EAL=y
CONFIG_RTE_MAX_LCORE=128
CONFIG_RTE_MAX_NUMA_NODES=8
CONFIG_RTE_MAX_MEMSEG=1024
CONFIG_RTE_MAX_MEMZONE=2560
CONFIG_RTE_MAX_TAILQ=32
```

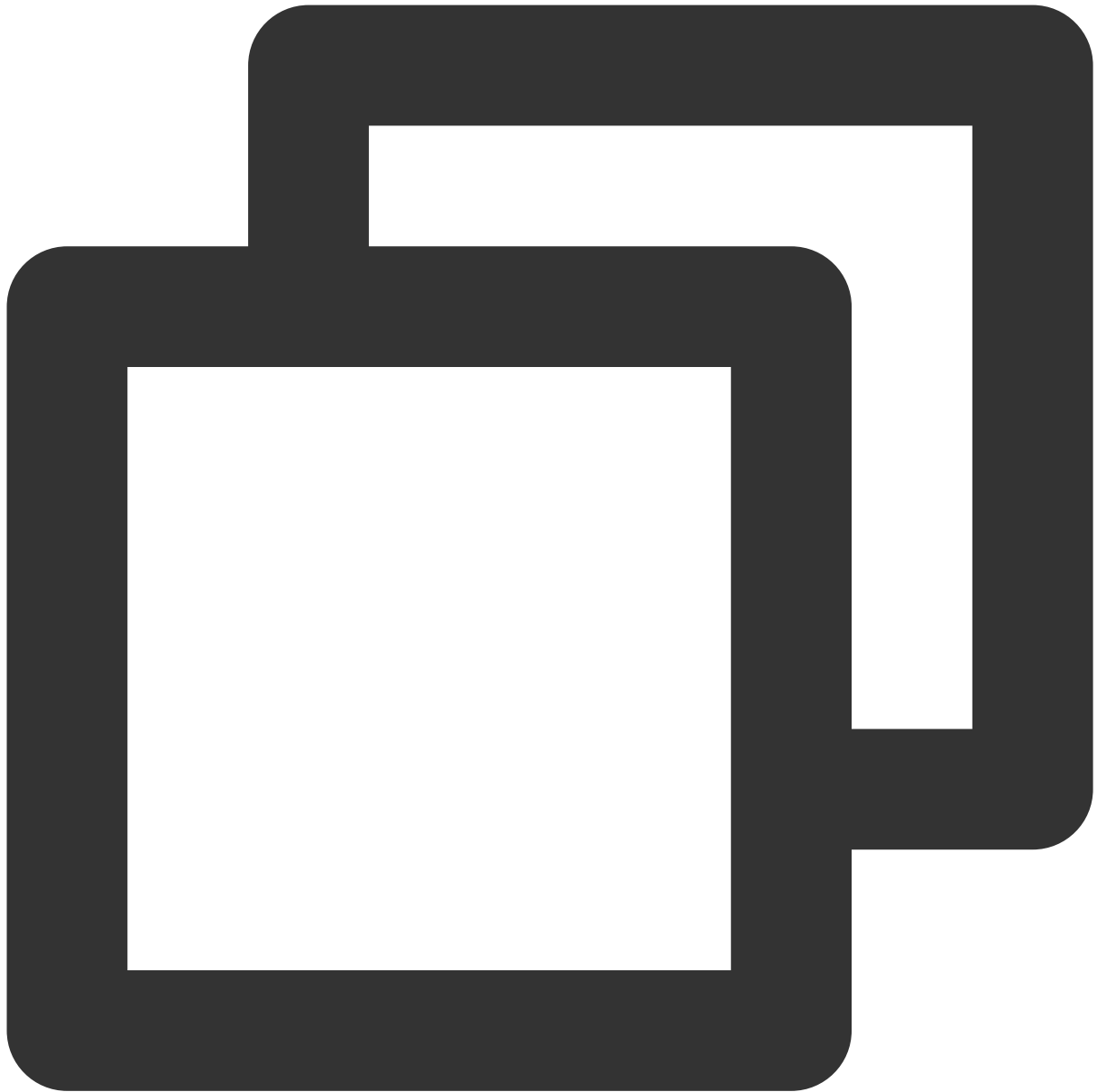
i를 눌러 편집 모드로 들어가 `CONFIG_RTE_MAX_LCORE=128` 을 찾습니다. 시스템의 CPU 코어 수가 128보다 크면 256으로 변경할 수 있습니다. 수정 완료 후는 다음 이미지와 같습니다.

```
CONFIG_RTE_LIBRTE_EAL=y
CONFIG_RTE_MAX_LCORE=256
CONFIG_RTE_MAX_NUMA_NODES=8
CONFIG_RTE_MAX_MEMSEG=256
CONFIG_RTE_MAX_MEMZONE=2560
CONFIG_RTE_MAX_TAILQ=32
```

Esc를 누르고 `:wq`를 입력하여 수정 사항을 저장하고 종료합니다.

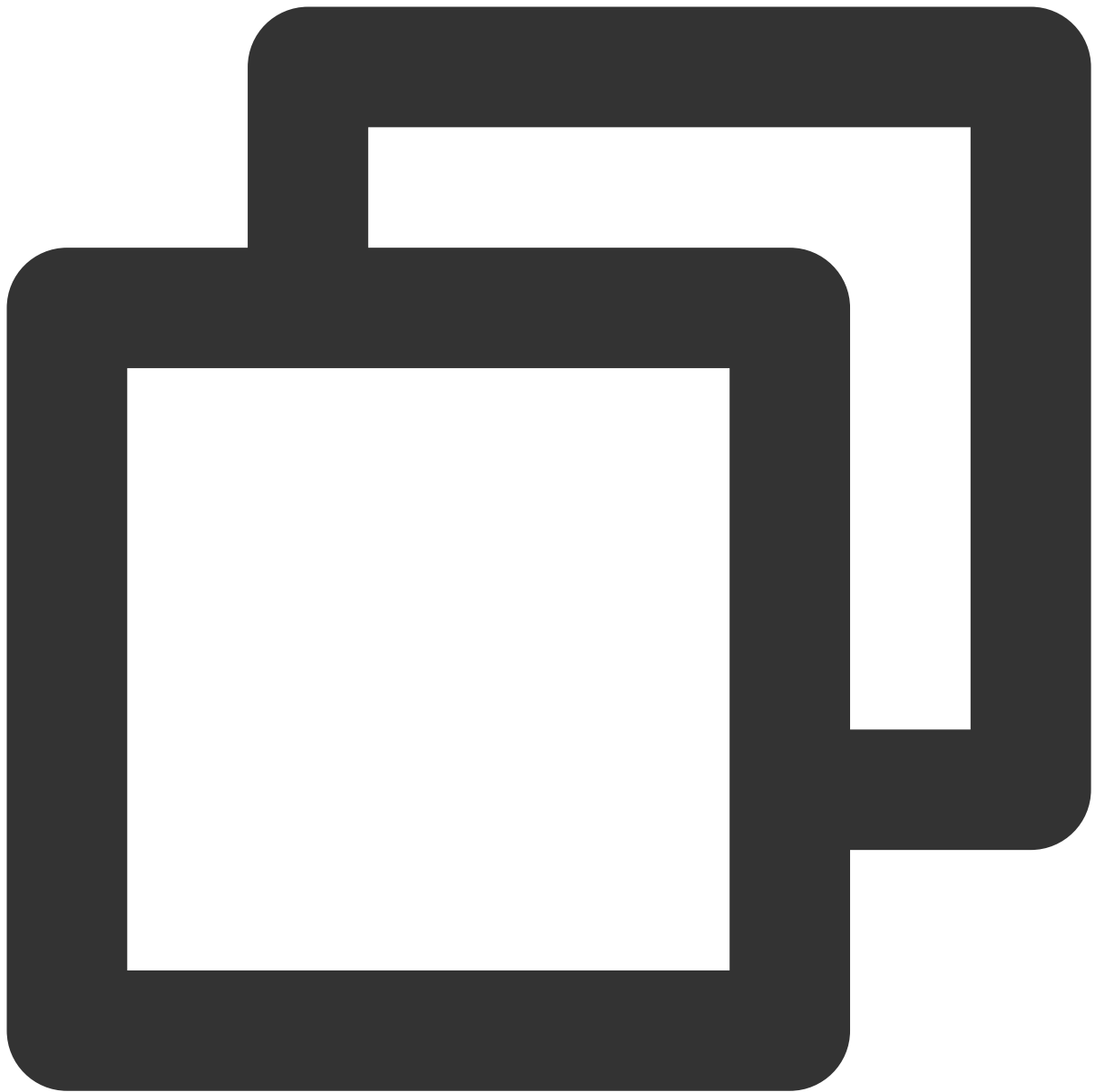
설명 :

수신측과 발신측 모두 상기 구성 파일을 수정해야 합니다. 다음 명령을 사용하여 수정된 파일을 피어로 전송하여 중복 수정을 방지할 수 있습니다.



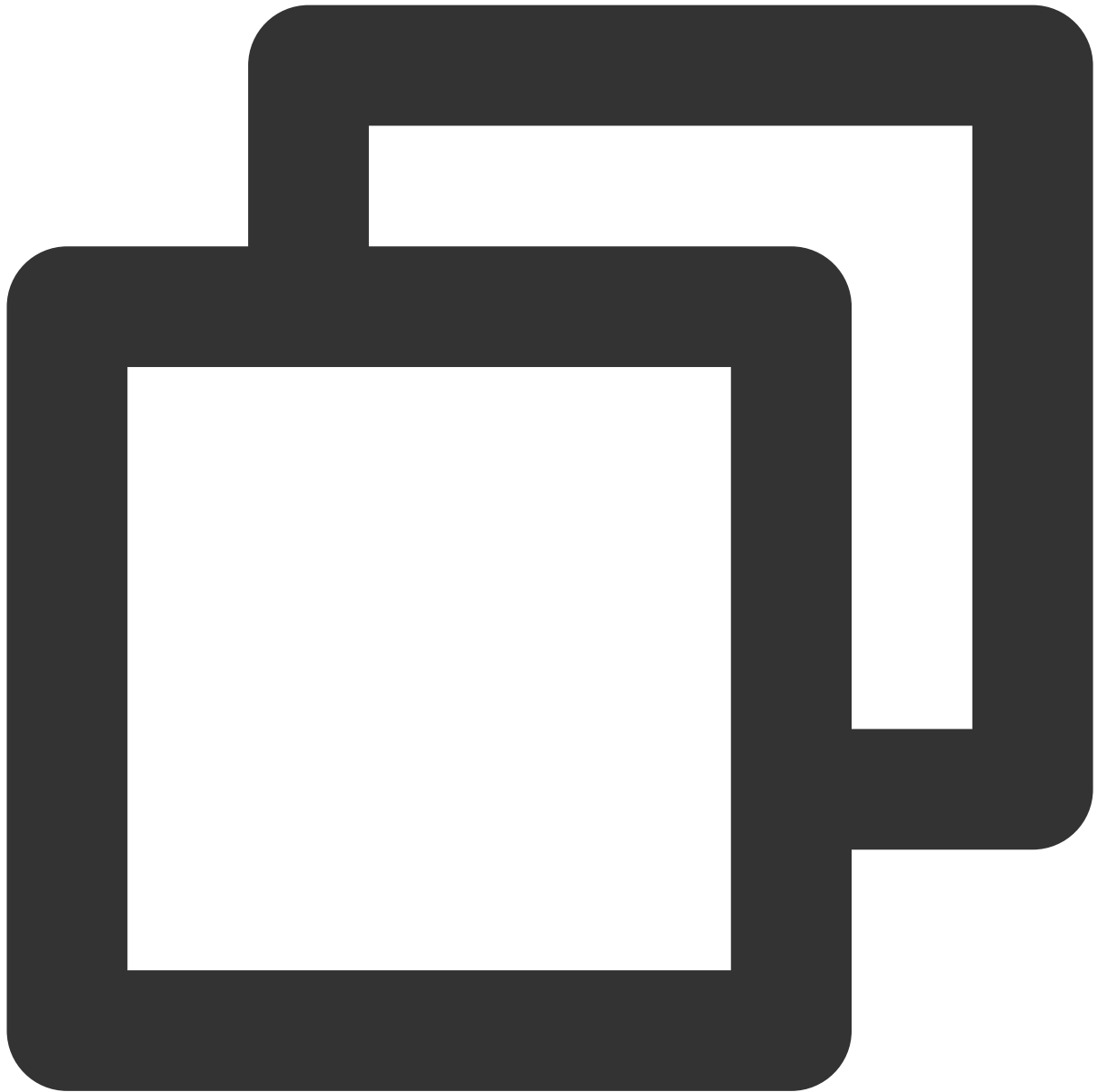
```
scp -P 22 /root/dpdk/app/test-pmd/txonly.c root@<IP주소>:/root/dpdk/app/test-pmd/  
scp -P 22 /root/dpdk/config/common_base root@<IP주소>:/root/dpdk/config
```

4. 다음 명령어를 실행하여 `dpdk/app/test-pmd/txonly.c` 의 IP 주소를 테스트 서버용 IP로 수정합니다.



```
vim dpdk/app/test-pmd/txonly.c
```

i를 눌러 편집 모드로 들어가 다음 내용을 찾습니다.



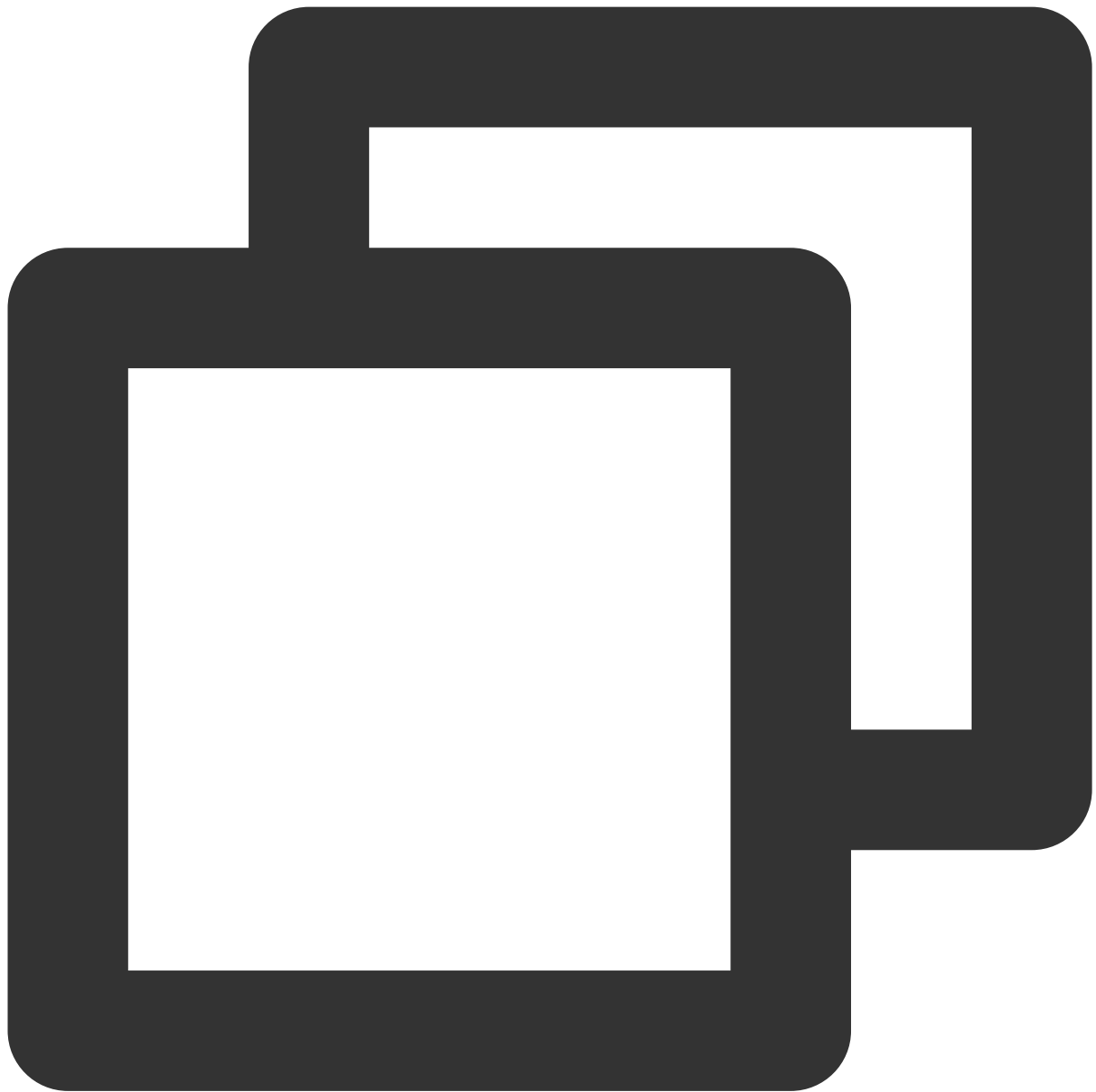
```
#define IP_SRC_ADDR (198U << 24) | (18 << 16) | (0 << 8) | 1;  
#define IP_DST_ADDR (198U << 24) | (18 << 16) | (0 << 8) | 2;
```

숫자 198, 18, 0, 1을 디바이스 IP로 바꿉니다. SRC_ADDR은 발신측 IP, DST_ADDR은 수신측 IP입니다.

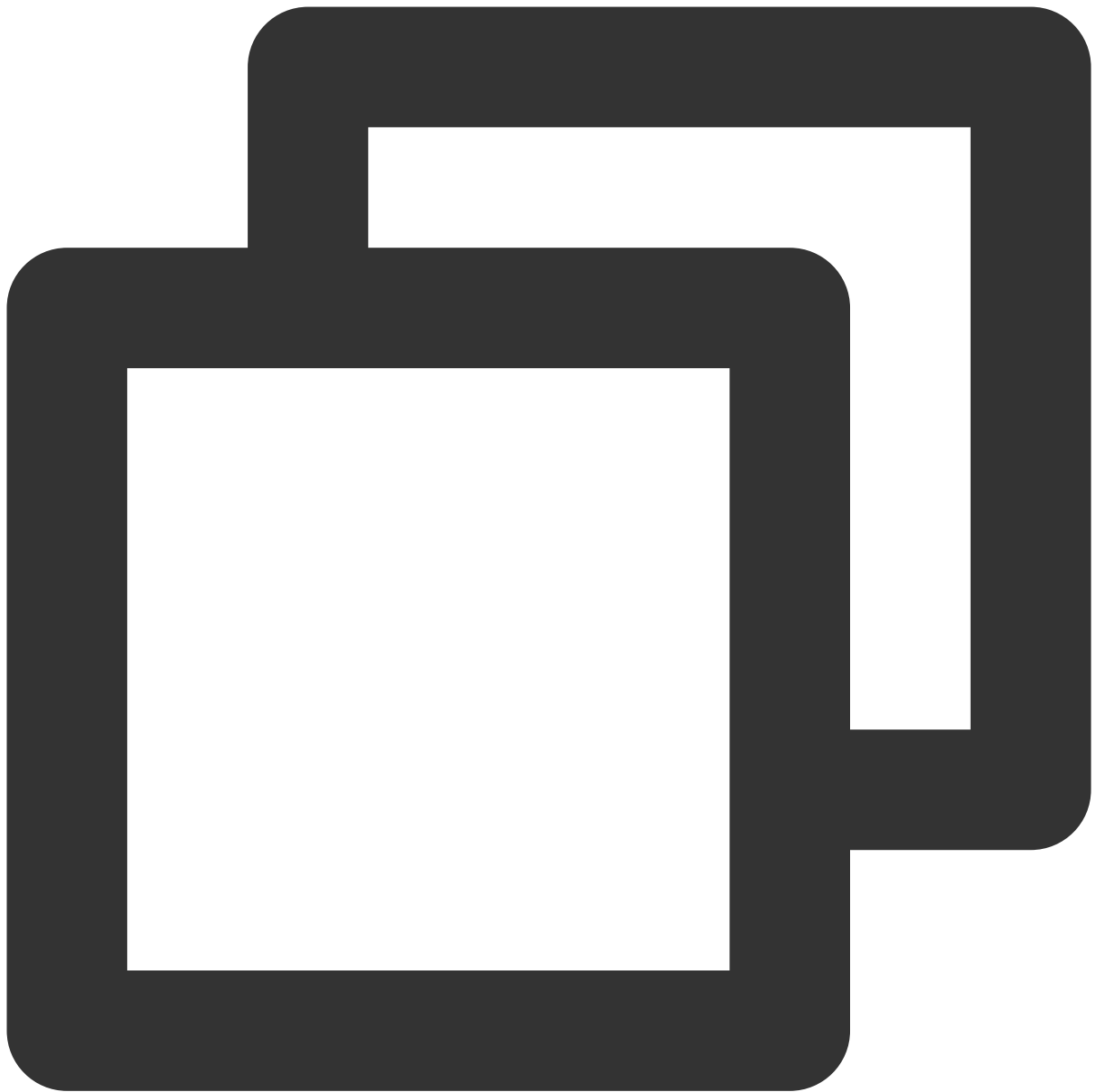
5. 디바이스 운영 체제에 따라 다음 명령을 실행하여 numa를 설치합니다.

CentOS

Ubuntu

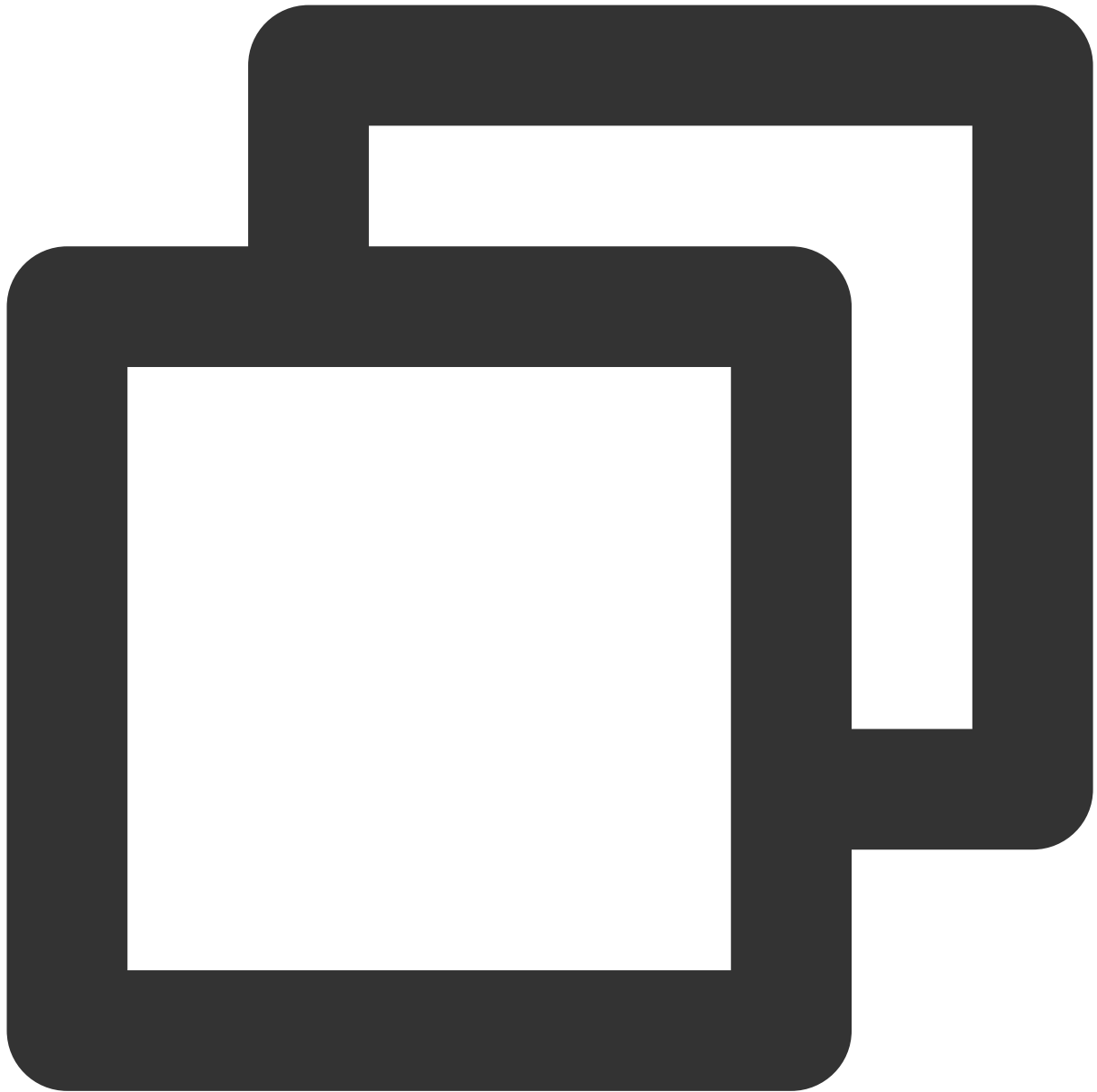


```
yum install numactl-devel
```



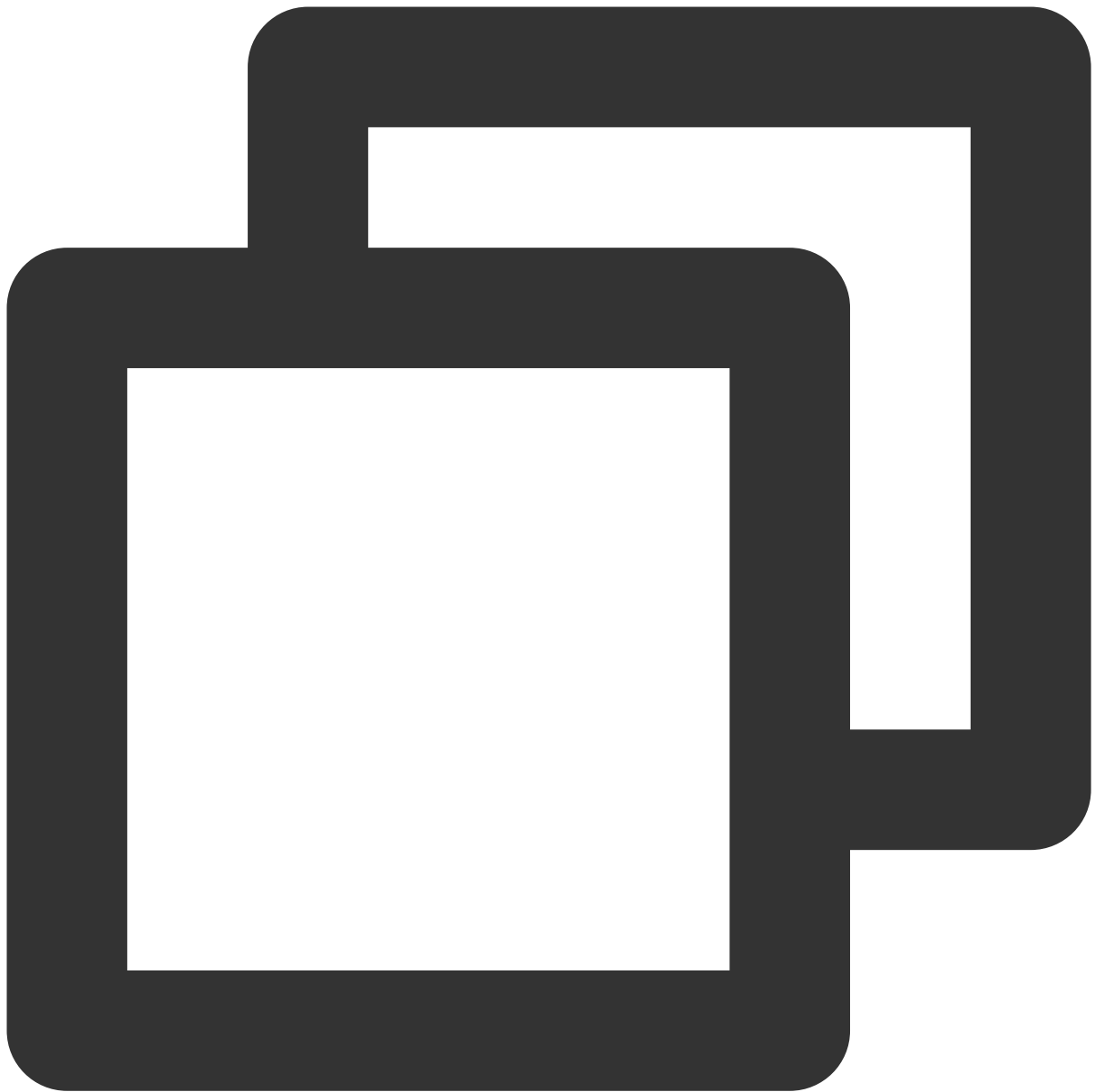
```
apt-get install libnuma-dev
```

6. `dpdk/` 디렉터리에서 다음 명령을 실행하고 KNI를 비활성화합니다.

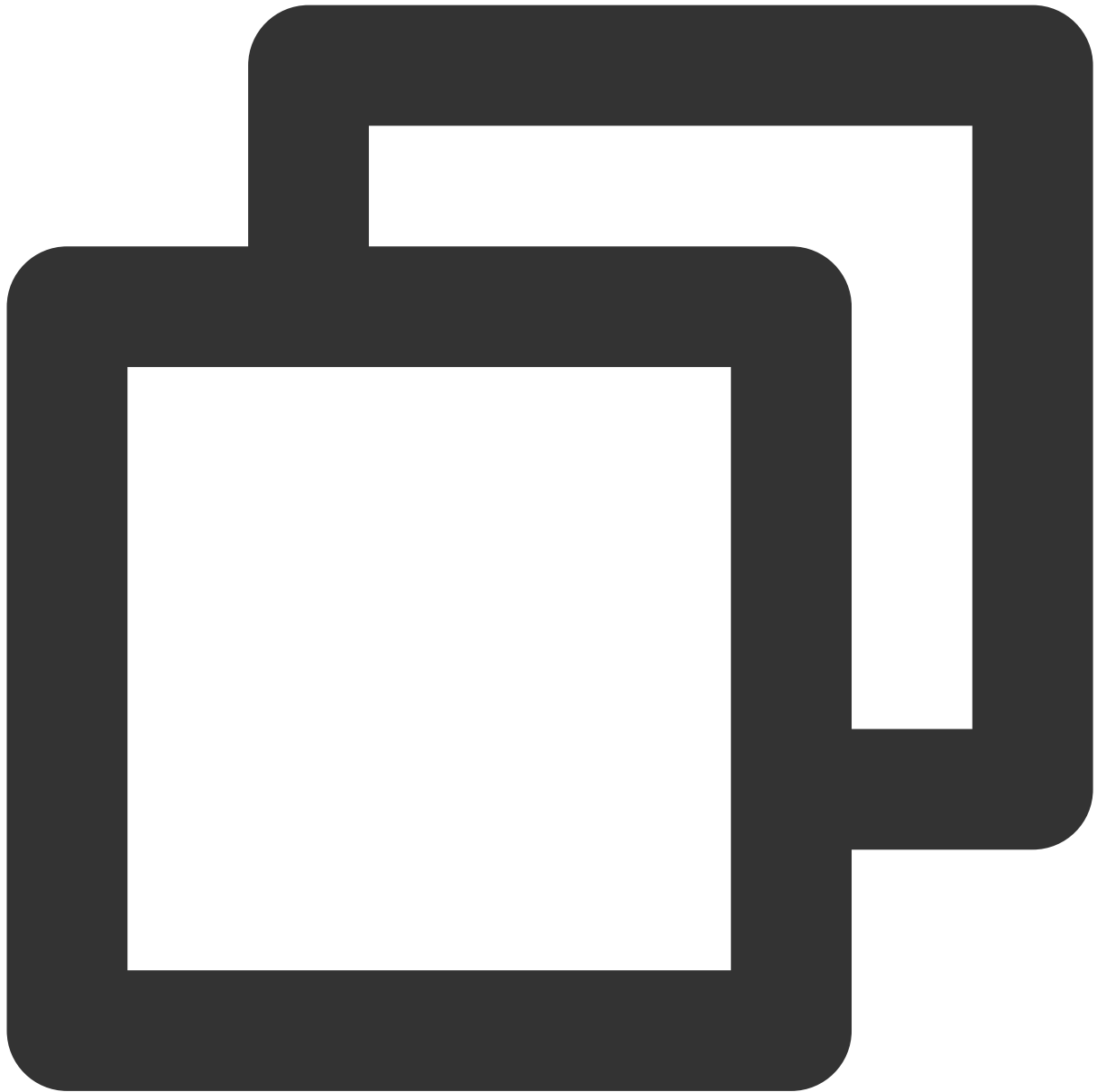


```
sed -i "s/\\(^CONFIG_.*KNI.*\\)=y/\\1=n/g" ./config/*
```

7. 운영 체제 커널 버전이 비교적 높은 경우(예: 5.3) 다음 명령을 실행하여 차이를 차단하십시오.

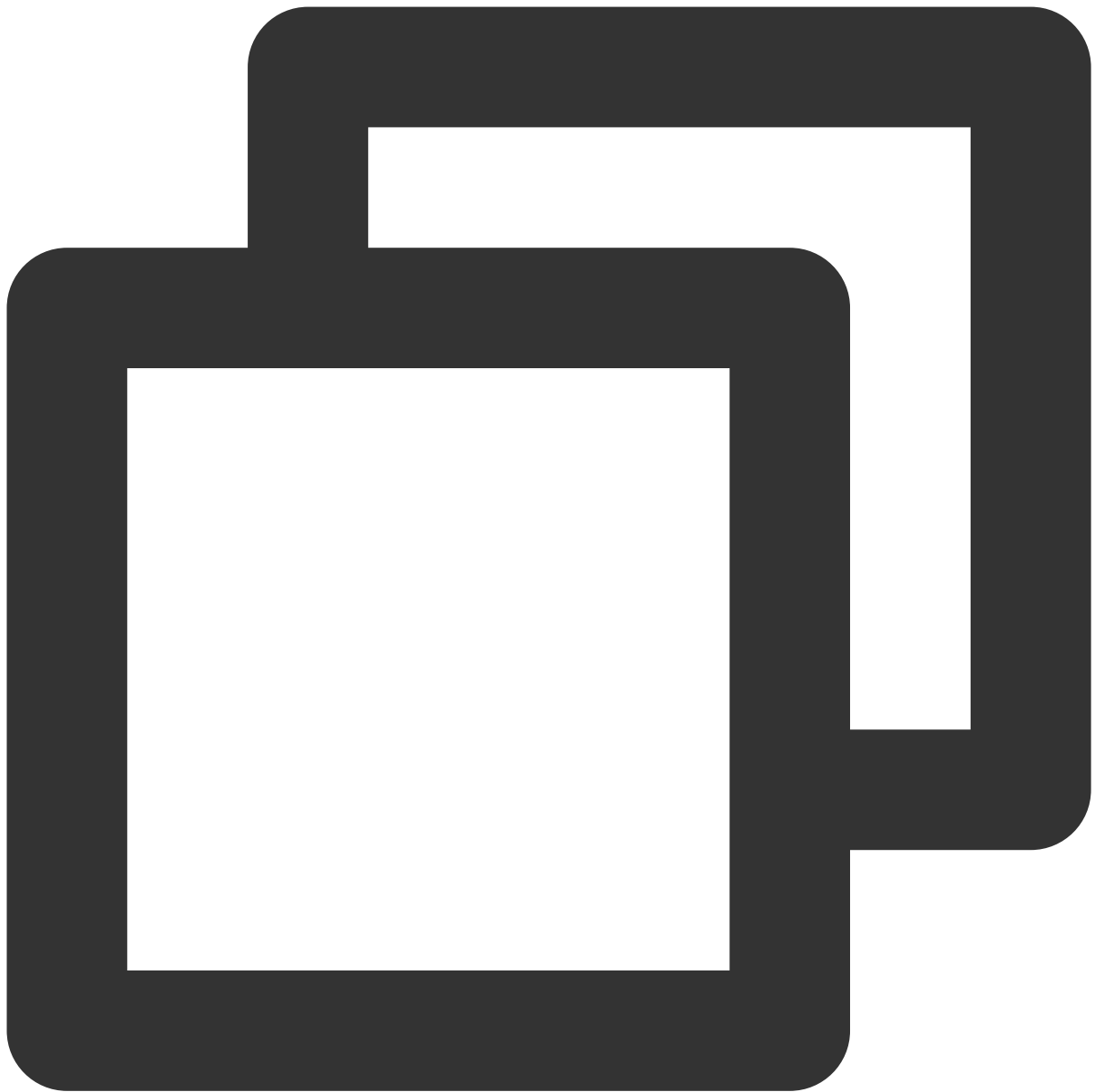


```
sed -i "s/\\(^WERROR_FLAGS += -Wundef -Wwrite-strings$\\)/\\1 -Wno-address-of-packed-member"
```

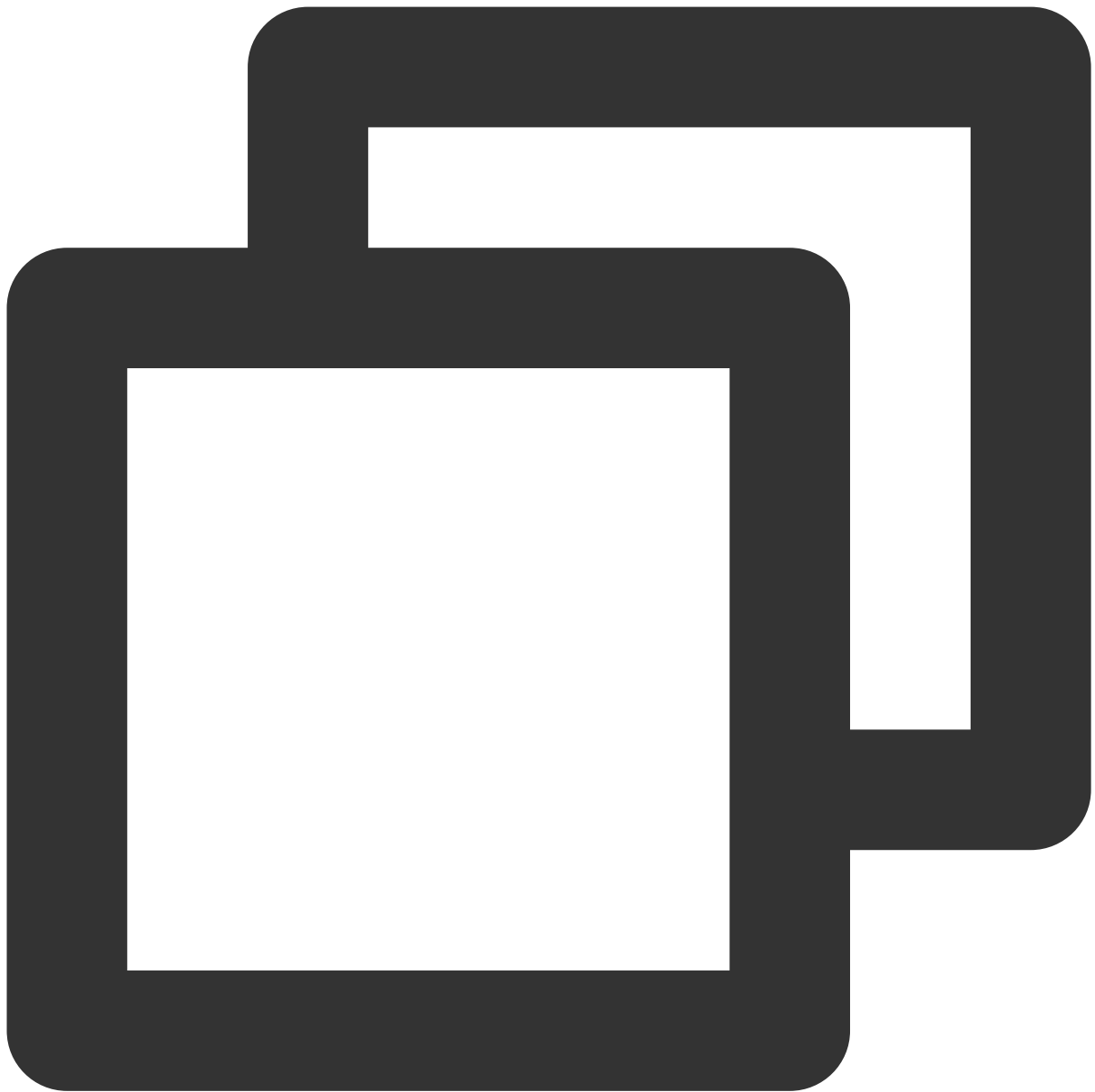



```
sed -i "s/fall back/falls through -/g" ./lib/librte_eal/linuxapp/igb_uio/igb_uio.c
```

8. 다음 명령을 실행하여 DPDK를 컴파일합니다.



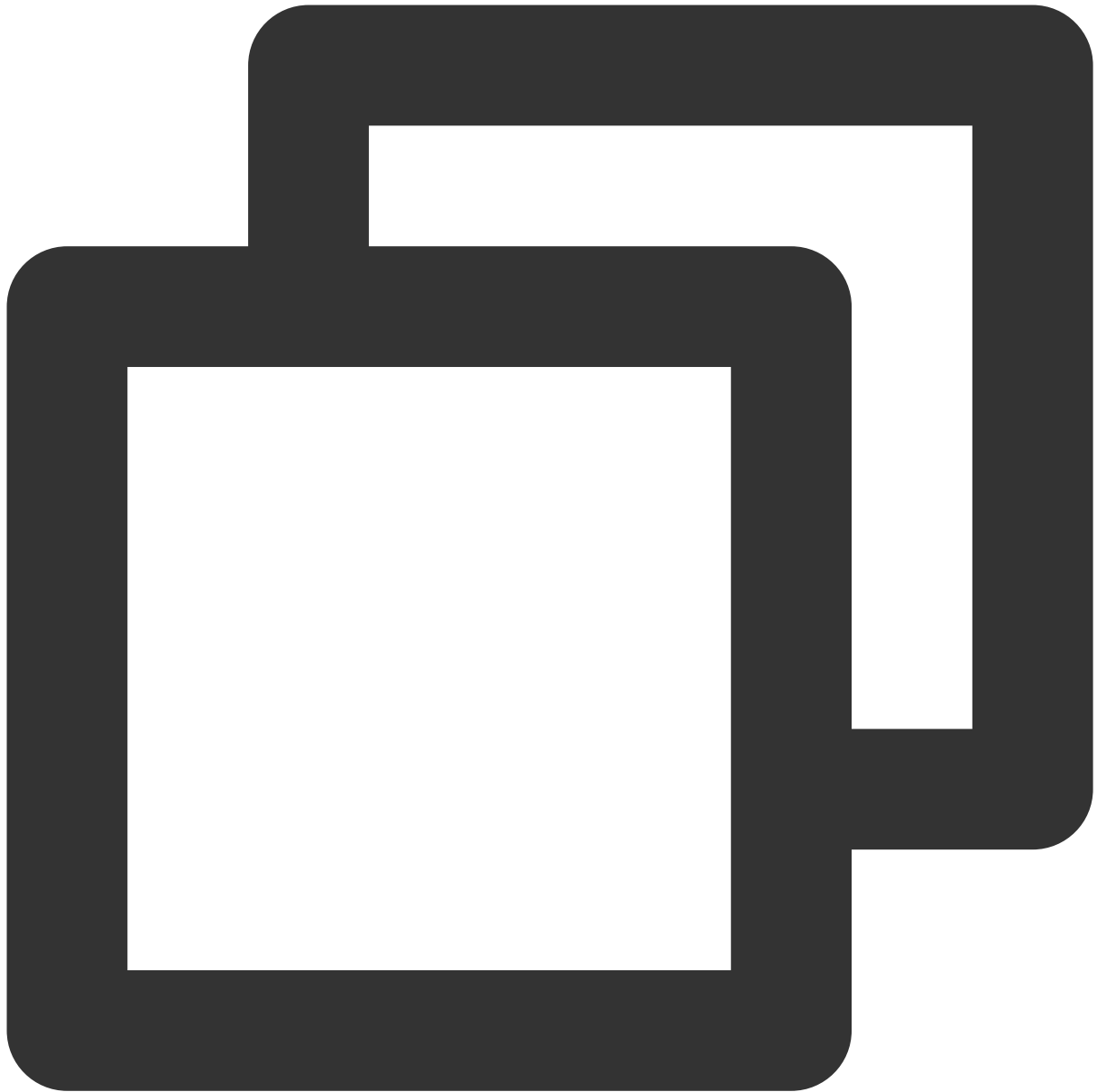
```
make defconfig
```



```
make -j
```

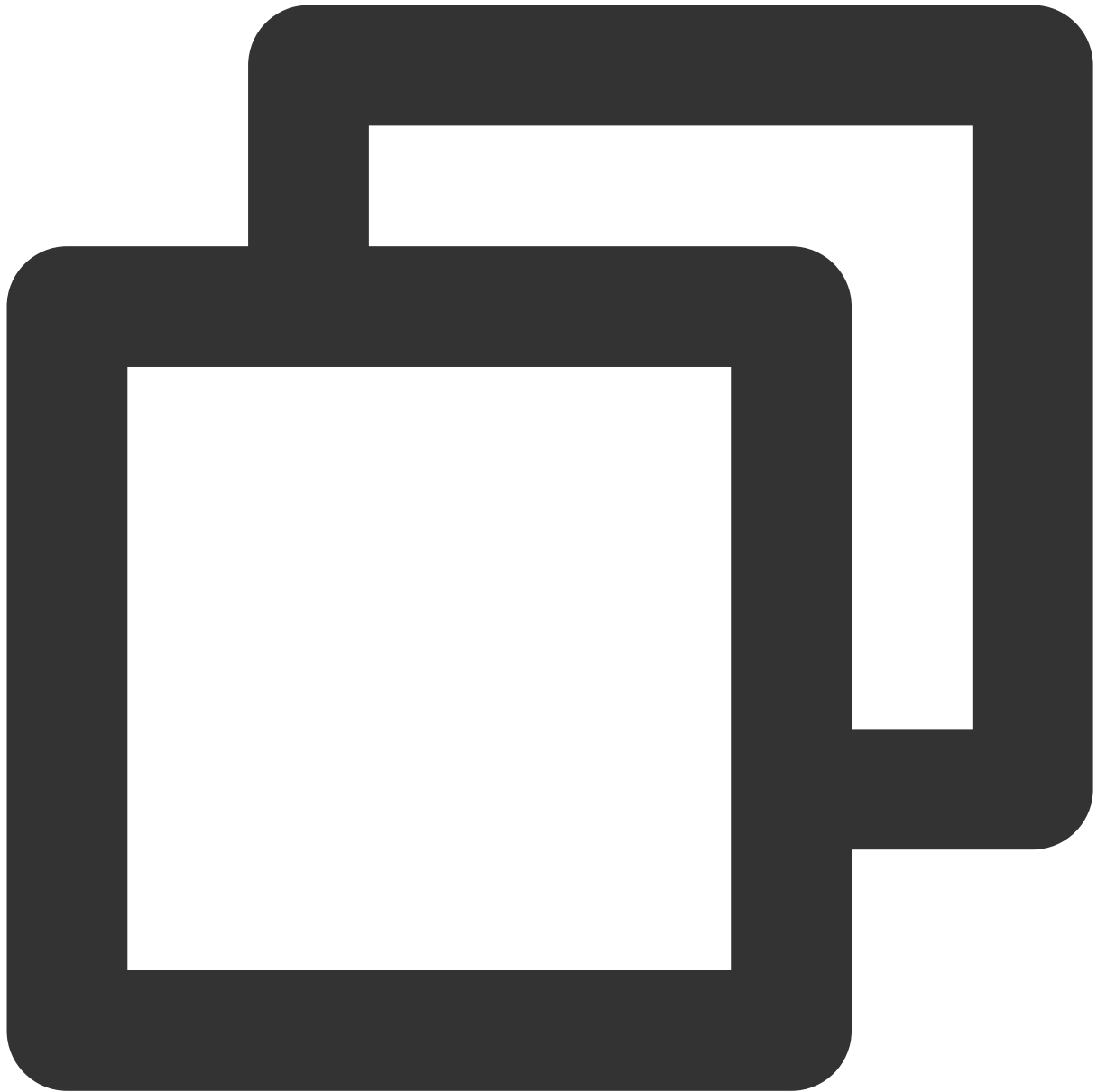
Hugepage 메모리 설정

다음 명령을 실행하여 Hugepage 메모리를 설정합니다.



```
echo 4096 > /sys/kernel/mm/hugepages/hugepages-2048kB/nr_hugepages
```

오류 메시지가 나타나면 **Hugepage** 메모리가 부족한 것입니다. 명령 구성을 조정할 수 있습니다. 예시:



```
echo 2048 > /sys/kernel/mm/hugepages/hugepages-2048kB/nr_hugepages
```

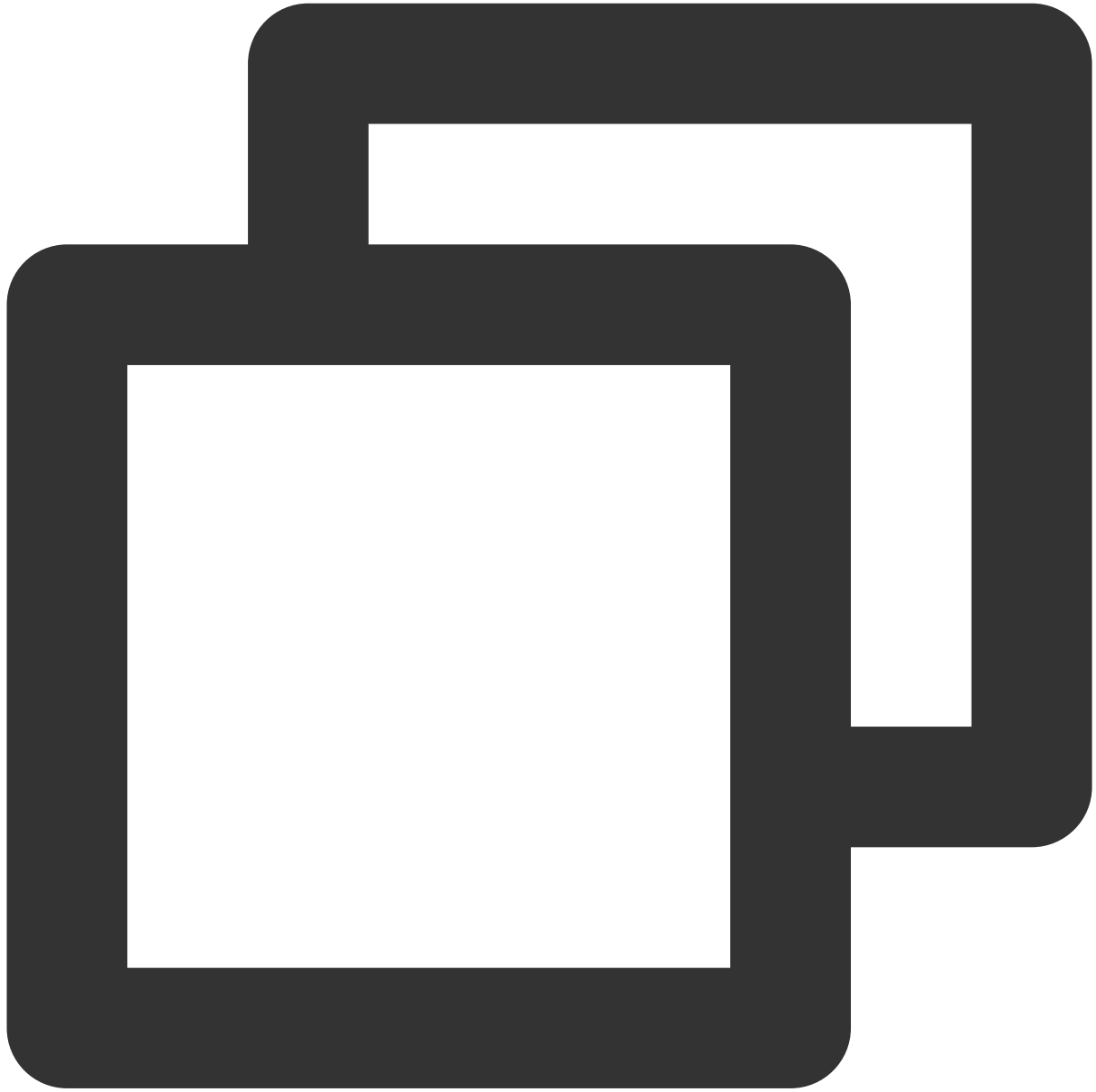
커널 모듈 설치 및 인터페이스 바인딩

설명 :

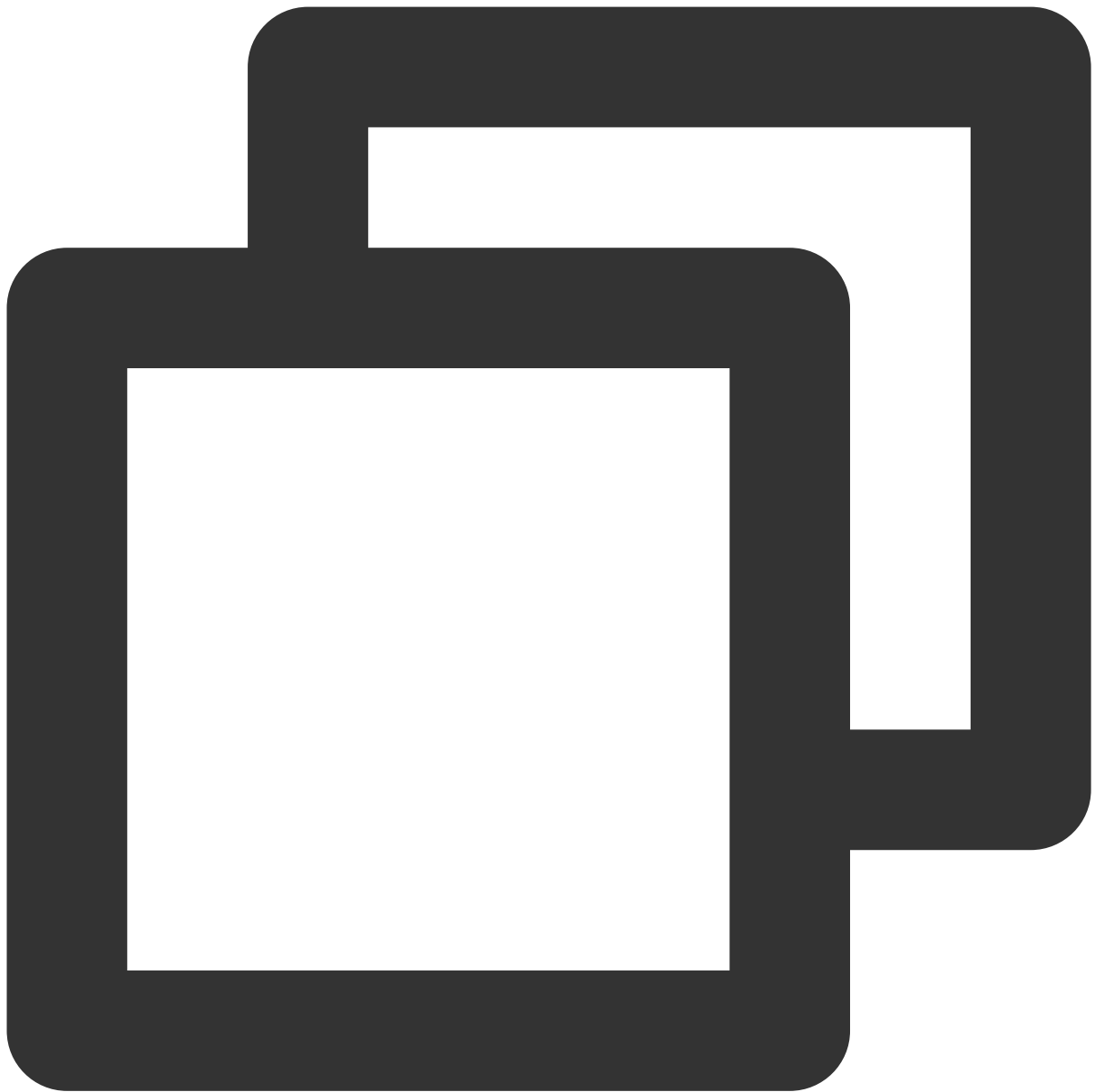
이 단계는 Python이 필요합니다. [Python 공식 웹사이트](#)에서 필요한 버전을 다운로드하여 설치하십시오. 본문은 Python 3.6.8을 예시로 설명합니다.

1. [VNC를 사용하여 Linux 인스턴스에 로그인](#)합니다. ENI 드라이버가 `igb_uio` 사용자 모드 드라이버에 바인딩된 후, 해당 ENI는 ssh 또는 IP를 통해 액세스할 수 없으며, VNC 또는 `console`을 통한 액세스만 지원됩니다.

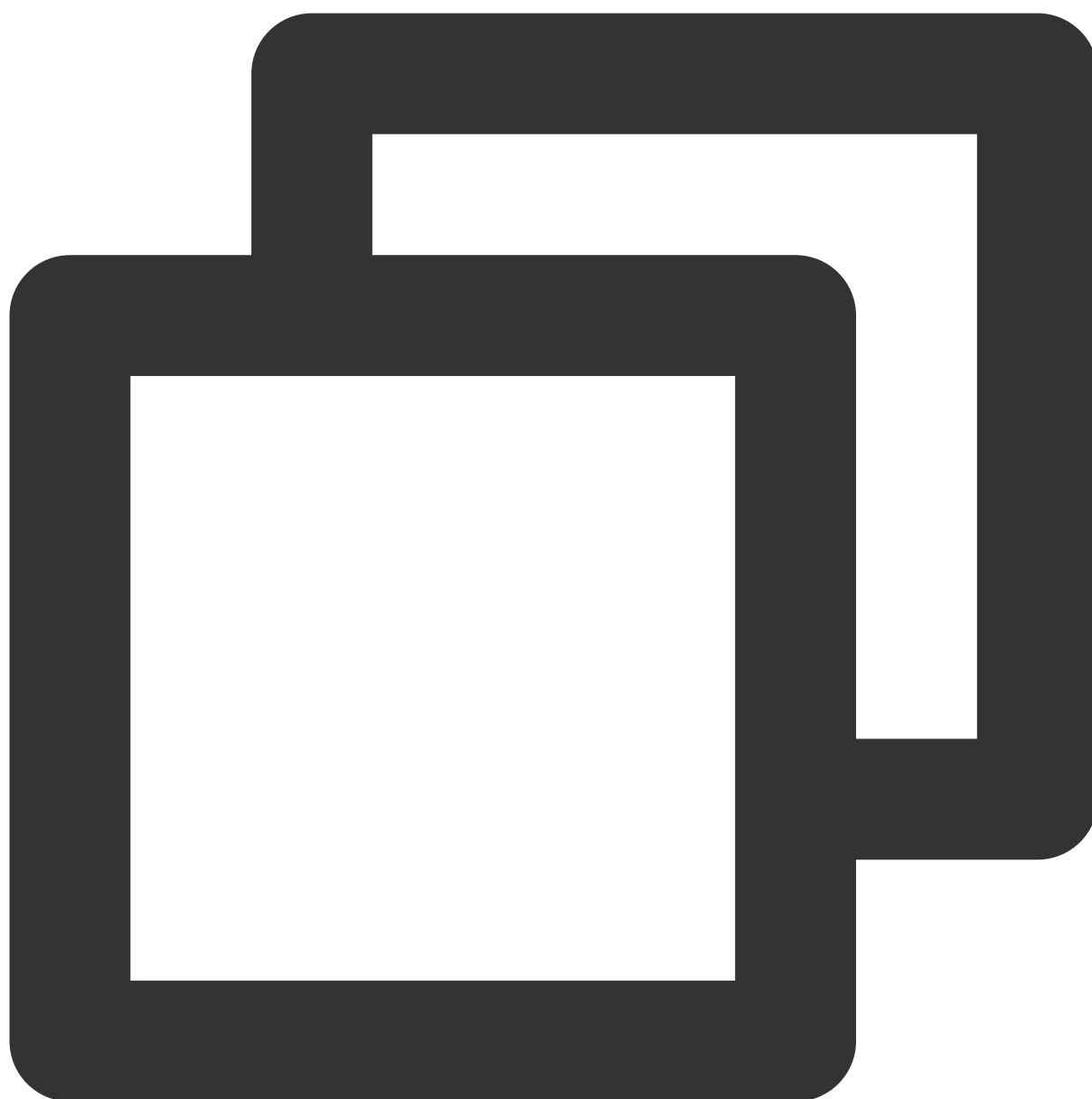
2. 다음 명령을 순서대로 실행하여 UIO 모듈을 설치하고 virito 인터페이스를 바인딩합니다.



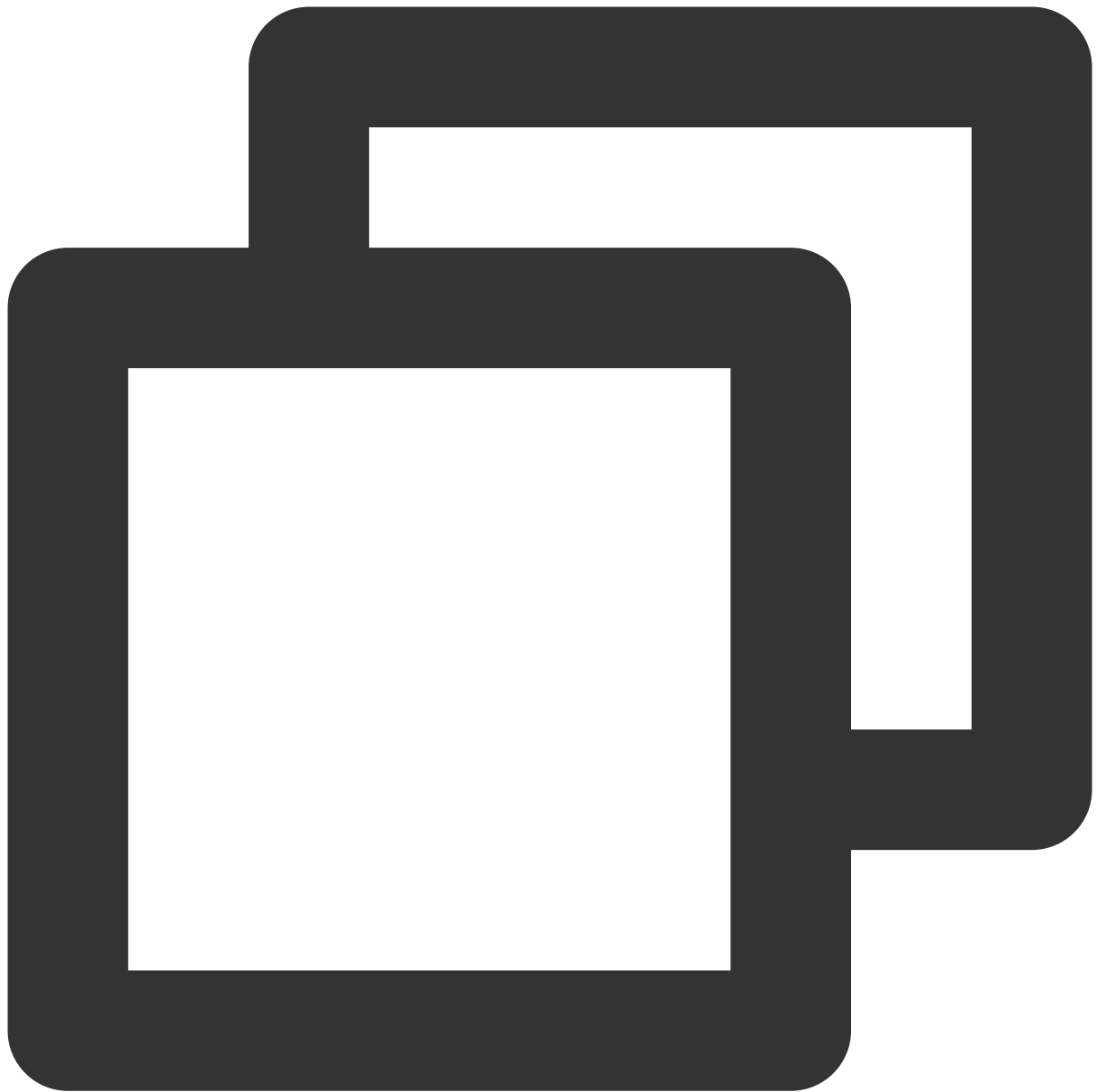
```
ifconfig eth0 0
```



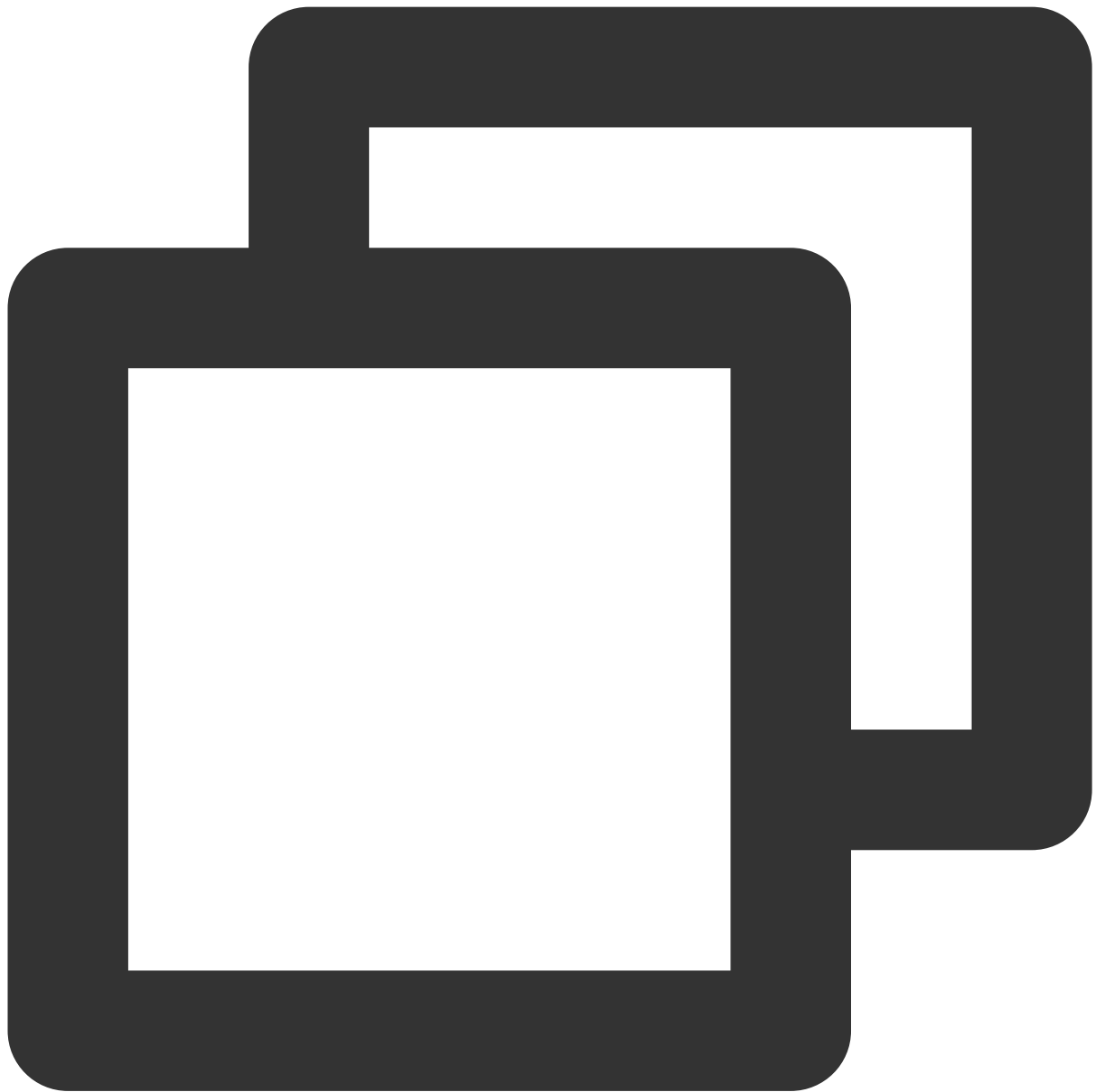
```
ifconfig eth0 down
```



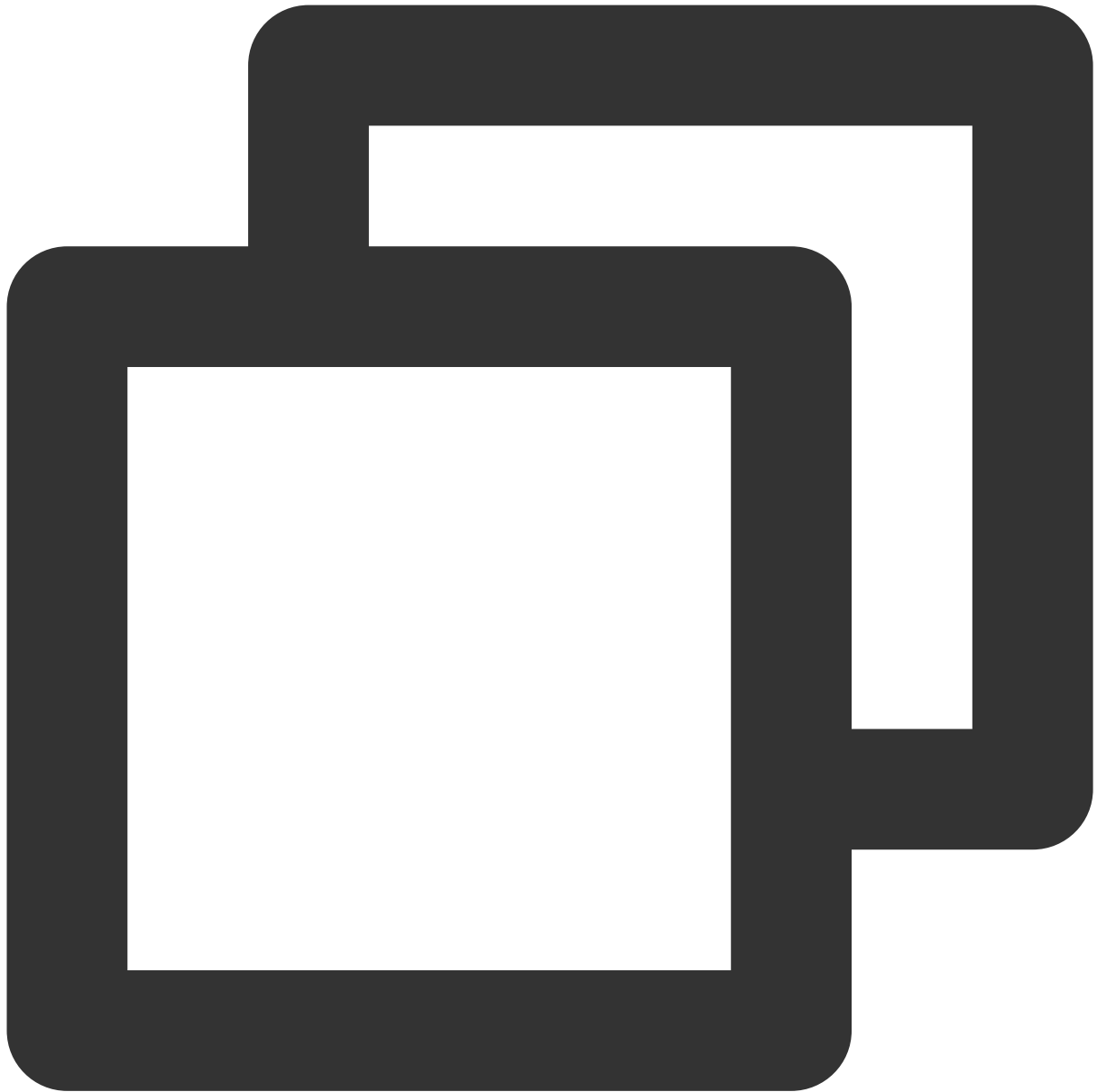
```
modprobe uio
```

```
insmod /root/dpdk/build/kmod/igb_uio.ko
```



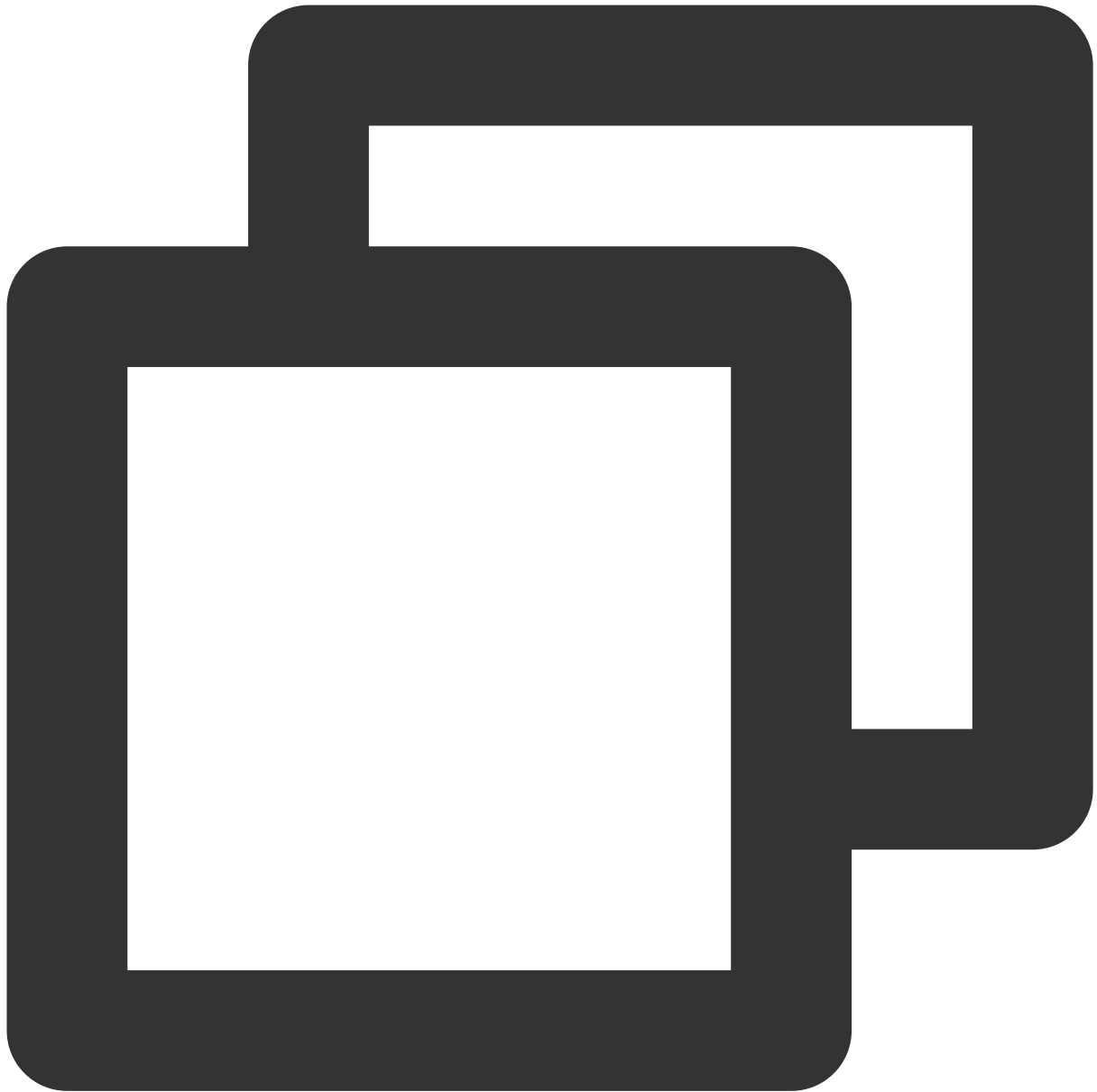
```
cd /root/dpdk/usertools/
```



```
python3 dpdk-devbind.py --bind=igb_uio 00:05.0
```

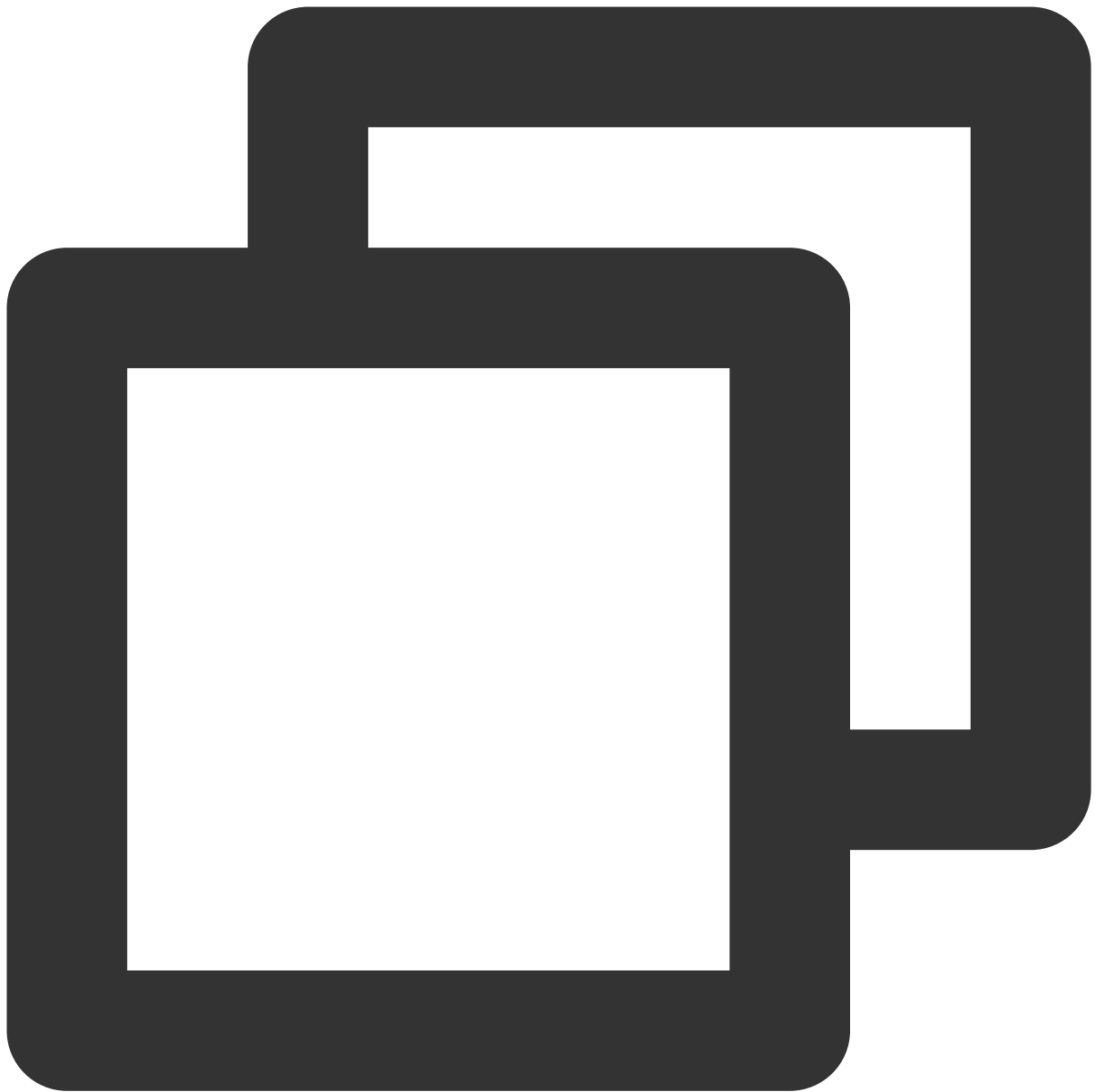
설명 :

명령어의 00.05.0은 예시 주소입니다. ENI의 실제 주소를 얻으려면 다음 명령을 실행하십시오.

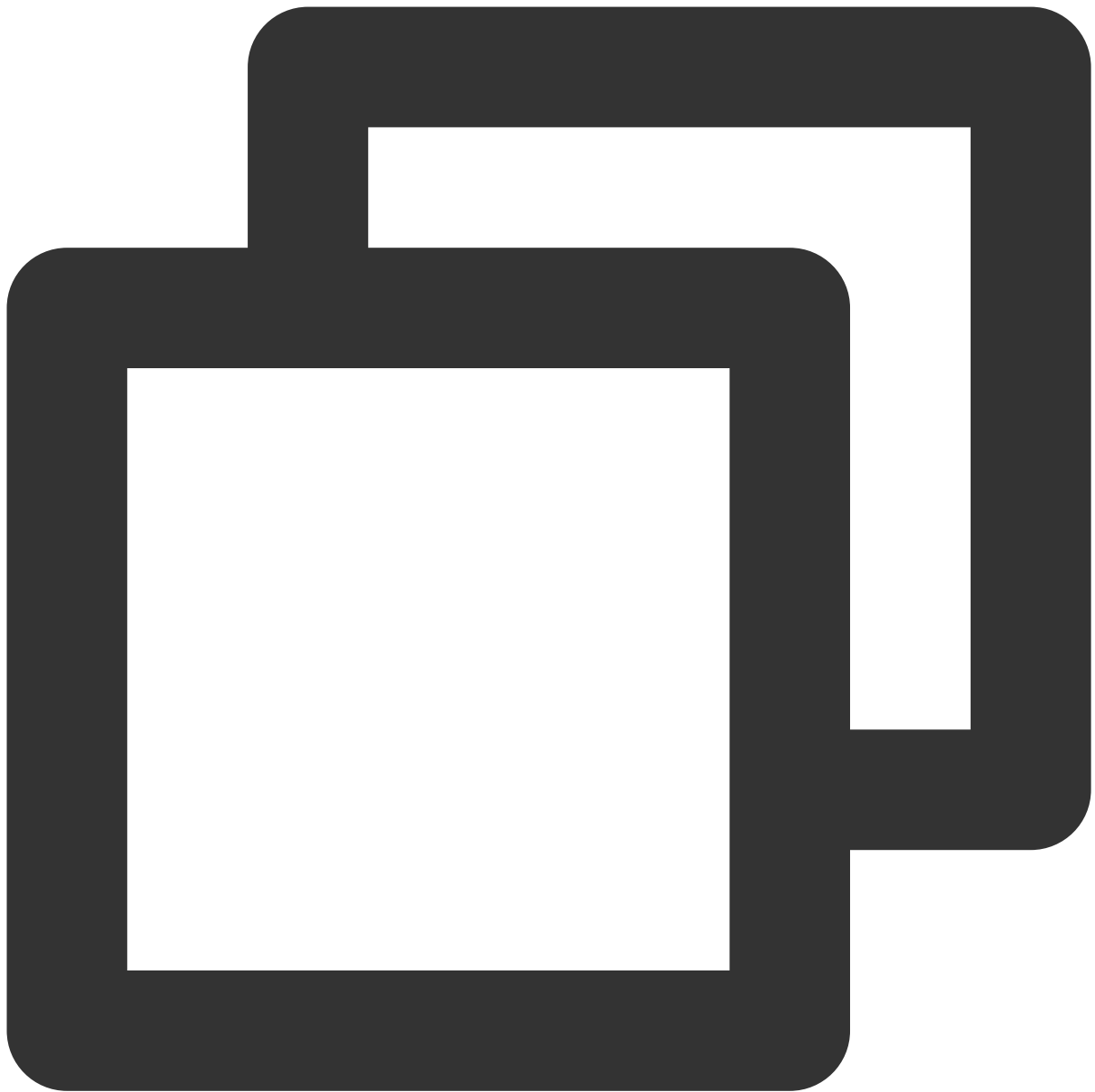


```
python3 dpdk-devbind.py -s
```

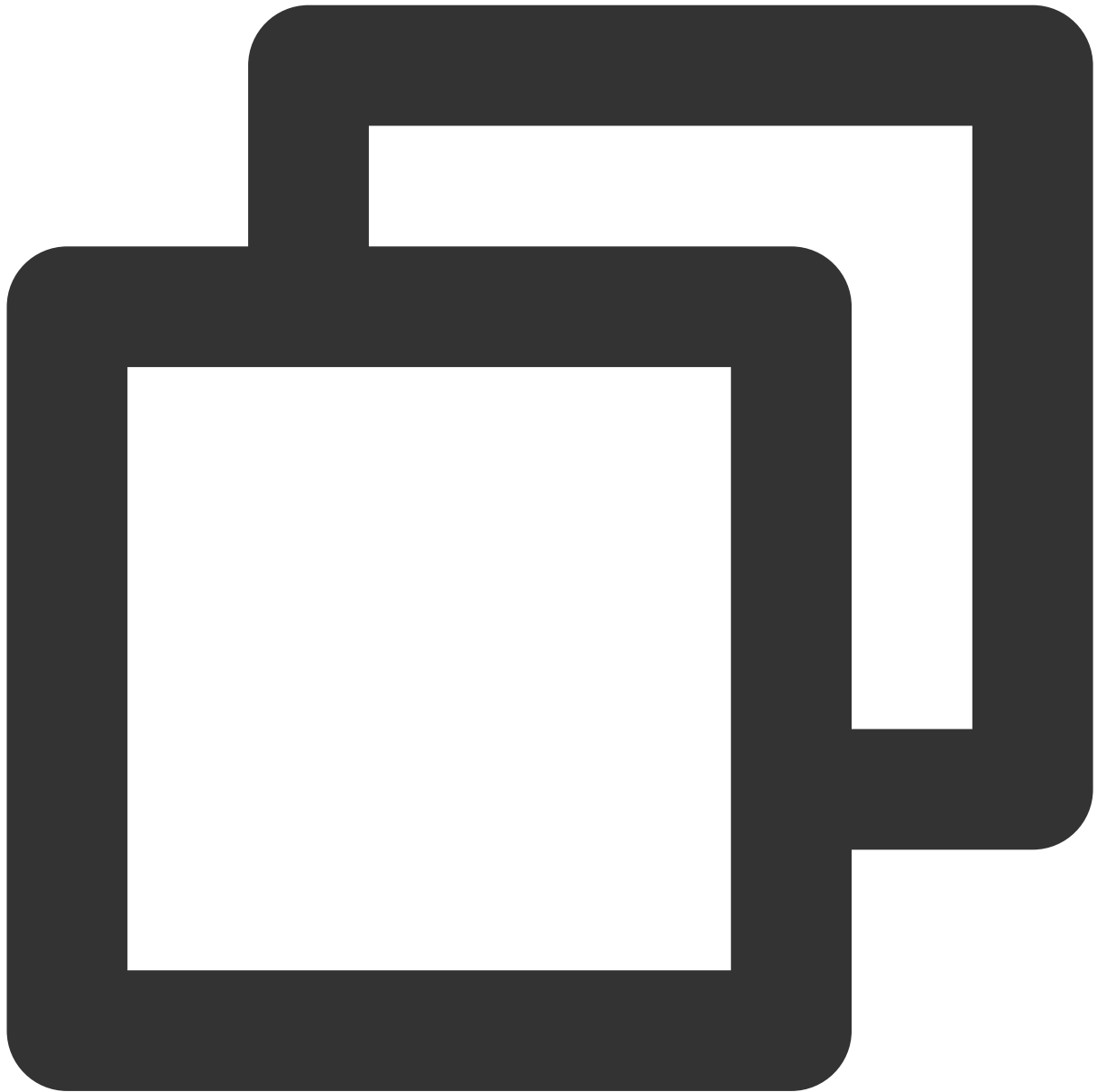
테스트 완료 후, 다음 명령을 실행하여 ENI 변경 사항을 복구할 수 있습니다.



```
cd /root/dpdk/usertools/
```



```
python3 dpdk-devbind.py --bind=virtio-pci 00:05.0
```



```
ifconfig eth0 up
```

대역폭 및 처리량 테스트

설명 :

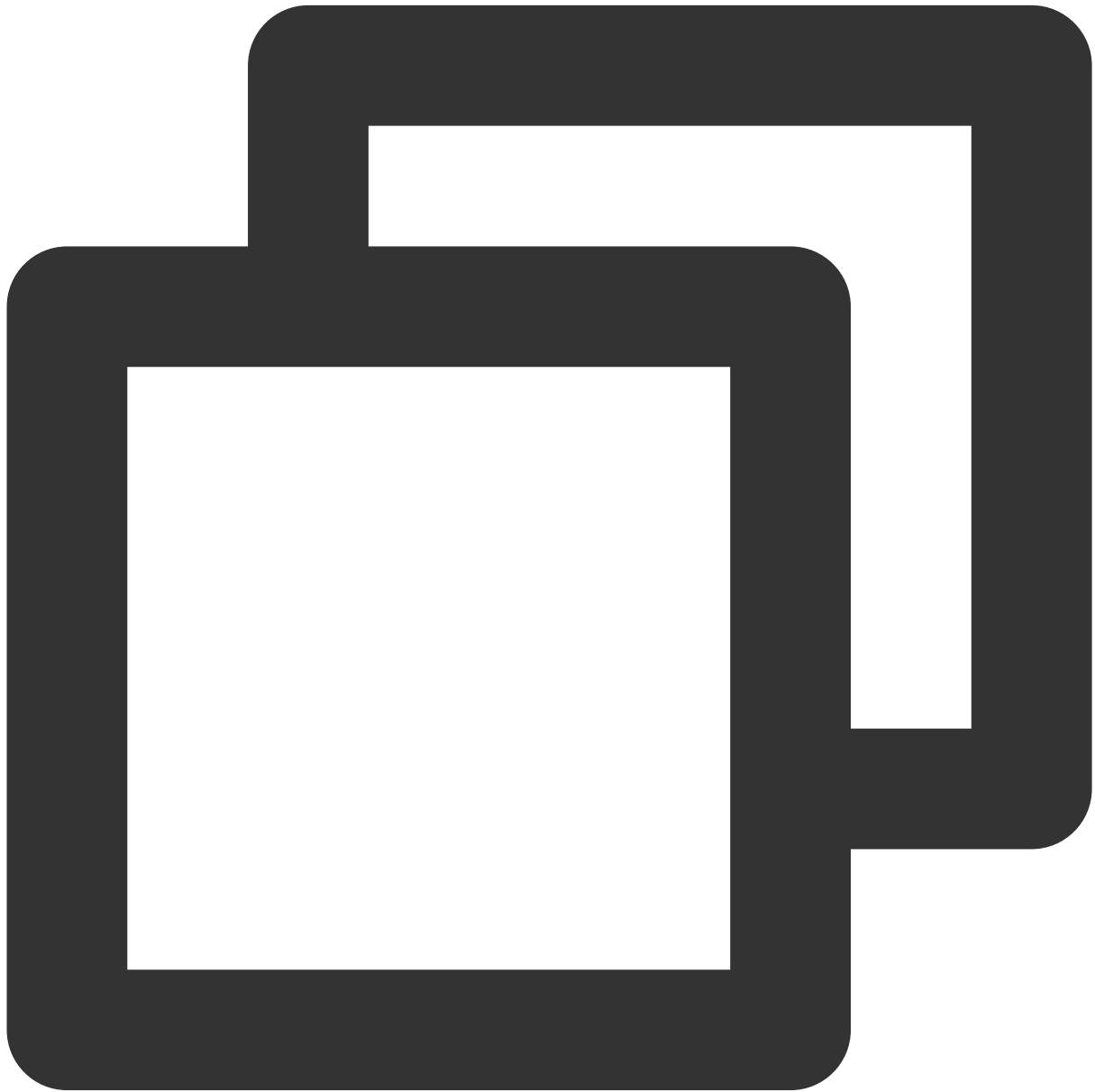
테스트 명령은 txpkts 매개변수를 사용하여 송신 패킷 크기를 제어합니다. 테스트 대역폭은 1430B를 사용하고, 테스트 pps는 64B를 사용합니다.

이 단계의 명령어 매개변수는 CentOS 8.2 운영 체제에 적합합니다. 다른 시스템 이미지 버전을 사용하는 경우 실제 상황에 따라 매개변수를 조정하고 다시 테스트해야 합니다. 예를 들어 CentOS 7.4의 커널 버전이 3.10이고 CentOS 8.2

의 커널 버전 4.18과 성능 차이가 존재하는 경우, 대역폭 테스트 명령에서 `nb-cores` 를 2로 수정할 수 있습니다. 명령 매개변수에 대한 자세한 내용은 [testpmd-command-line-options](#)를 참고하십시오.

1. 다음 명령을 실행합니다. 발신측은 TX only 모드를 사용하여 testpmd를 실행하고 수신측은 rxonly 모드를 활성화합니다.

발신측:

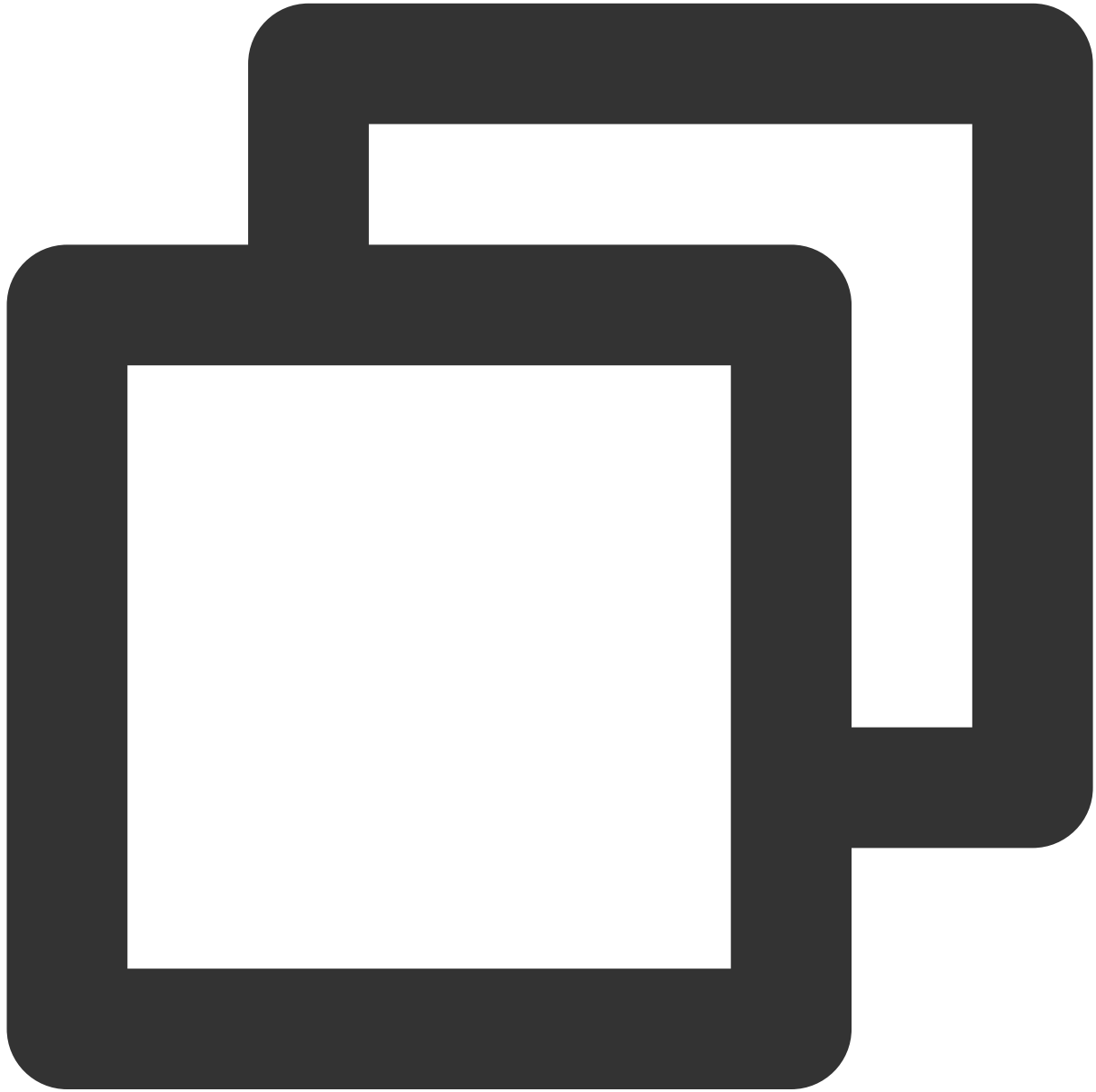


```
/root/dpdk/build/app/testpmd -- --txd=128 --rxd=128 --txq=512 --rxq=512 --nb-cores=
```

설명 :

이 중 `-l 8-191 -w 0000:00:05.0` 이 두 매개변수는 테스트 환경의 실제 값으로 대체해야 하며 그 다음은 동일하게 처리합니다.

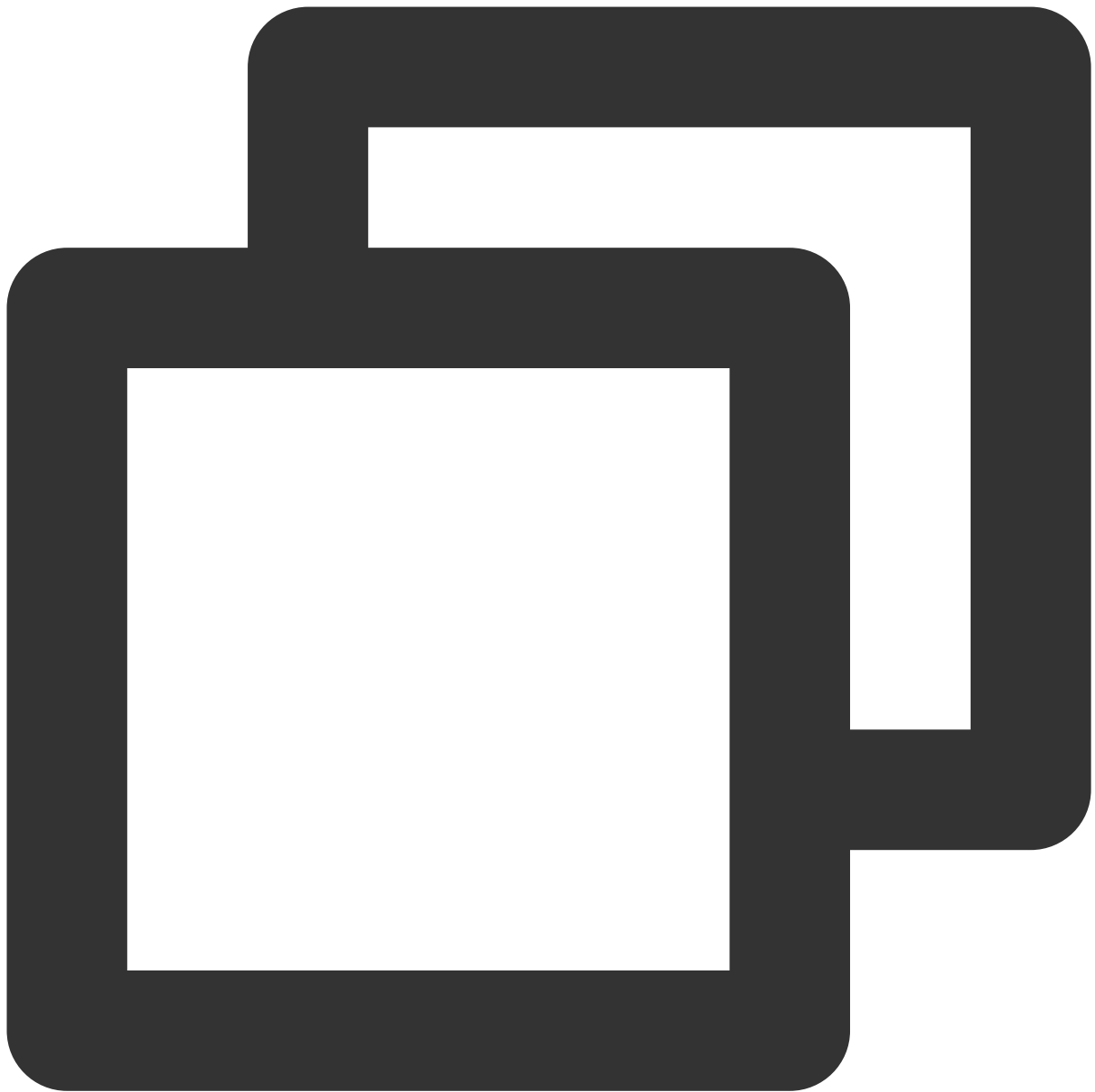
수신측:



```
/root/dpdk/build/app/testpmd -- --txd=128 --rx=128 --txq=512 --rxq=512 --nb-cores=
```

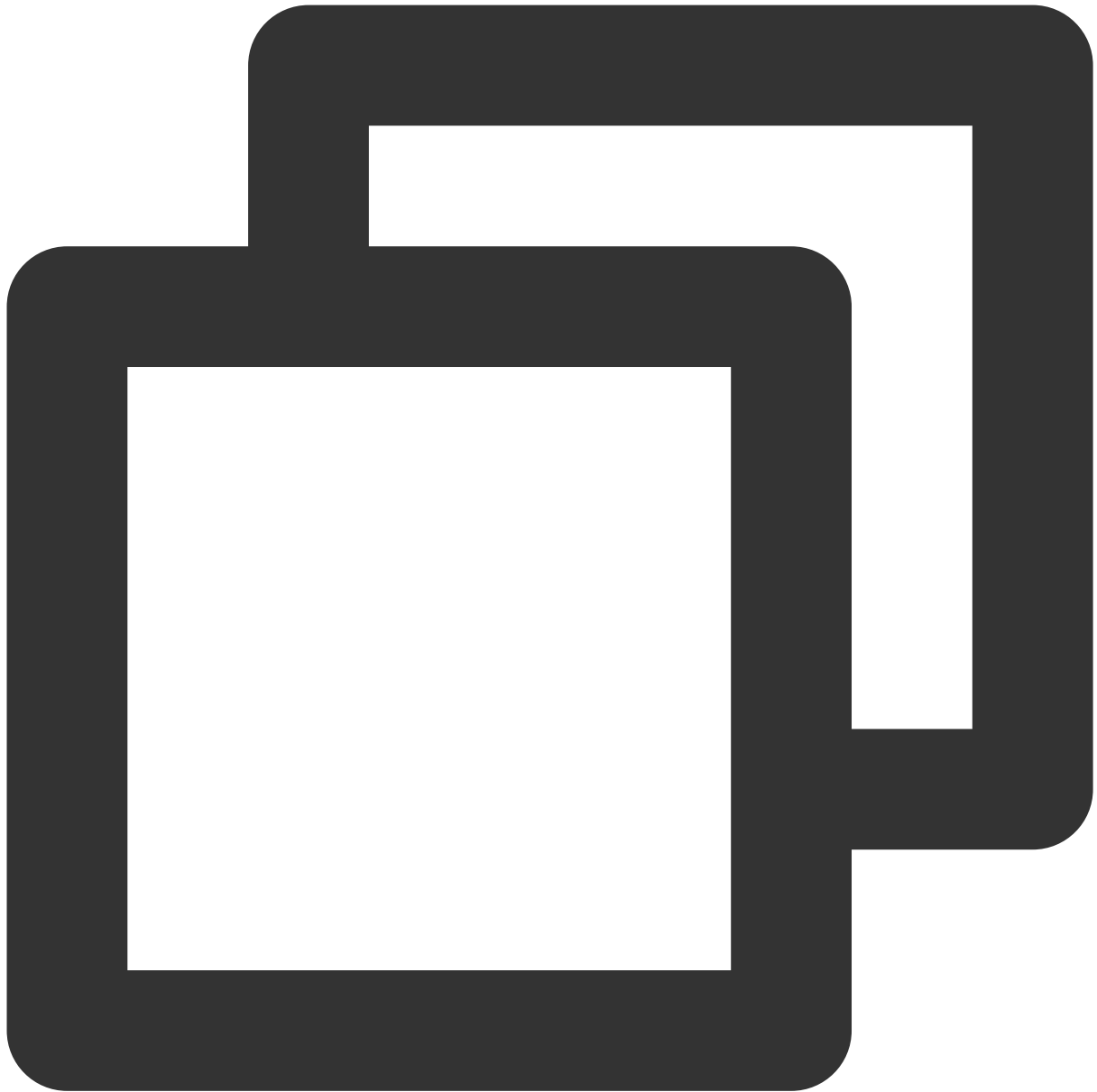
2. 다음 명령을 실행하여 pps(UDP 64B 패킷)를 테스트합니다.

발신측:



```
/root/dpdk/build/app/testpmd -- --txd=128 --rx=128 --txq=512 --rxq=512 --nb-cores=
```

수신측:



```
/root/dpdk/build/app/testpmd -- --txd=128 --rx=128 --txq=512 --rxq=512 --nb-cores=
```

아래 이미지와 같이 테스트 결과를 가져옵니다.

```

Port statistics =====
##### NIC statistics for port 0 #####
RX-packets: 0          RX-missed: 0          RX-bytes: 0
RX-errors: 0
RX-nombuf: 0
TX-packets: 69283890496 TX-errors: 0          TX-bytes: 99075963420720

Throughput (since last show)
Rx-pps: 0
Tx-pps: 31967172
#####

Port statistics =====
##### N
RX-packets: 11855403490 RX
RX-errors: 0
RX-nombuf: 0
TX-packets: 0          TX-

Throughput (since last sho
Rx-pps: 4692725
Tx-pps: 0
#####

```

네트워크 대역폭 계산

수신측 PPS와 테스트 패킷 길이에 따라 현재 네트워크의 수신 대역폭을 계산할 수 있으며, 공식은 다음과 같습니다.

$$\text{PPS} \times \text{packet length} \times 8\text{bit/B} \times 10^{-9} = \text{대역폭}$$

테스트에서 얻은 데이터와 결합하여, 현재 대역폭은 다음과 같이 계산할 수 있습니다.

$$4692725\text{pps} \times 1430\text{B} \times 8\text{bit/B} \times 10^{-9} \approx 53\text{Gbps}$$

설명 :

메시지 길이는 14B 이더넷 헤더, 4B CRC 및 20B IP 헤더를 포함하여 1430B입니다.

테스트 결과의 Rx-pps는 순시값입니다. 더 정확한 결과와 평균값을 얻기 위해 여러 번 테스트할 수 있습니다.

Linux 시스템에서 USB/IP를 사용하여 USB 장치 원격 공유

최종 업데이트 날짜: : 2024-02-02 11:01:47

작업 시나리오

USB/IP는 하나의 오픈 소스 프로젝트로, 커널이 포함되어 있어 Linux 환경에서 USB/IP를 사용하여 USB 장치를 원격으로 공유할 수 있습니다. 본 문서는 다음의 환경을 예로 들어, USB/IP를 사용한 USB 장치 원격 공유 방법을 소개합니다.

USB Client: CentOS 7.6 운영 체제의 CVM

USB Server: Debian 운영 체제의 로컬 컴퓨터

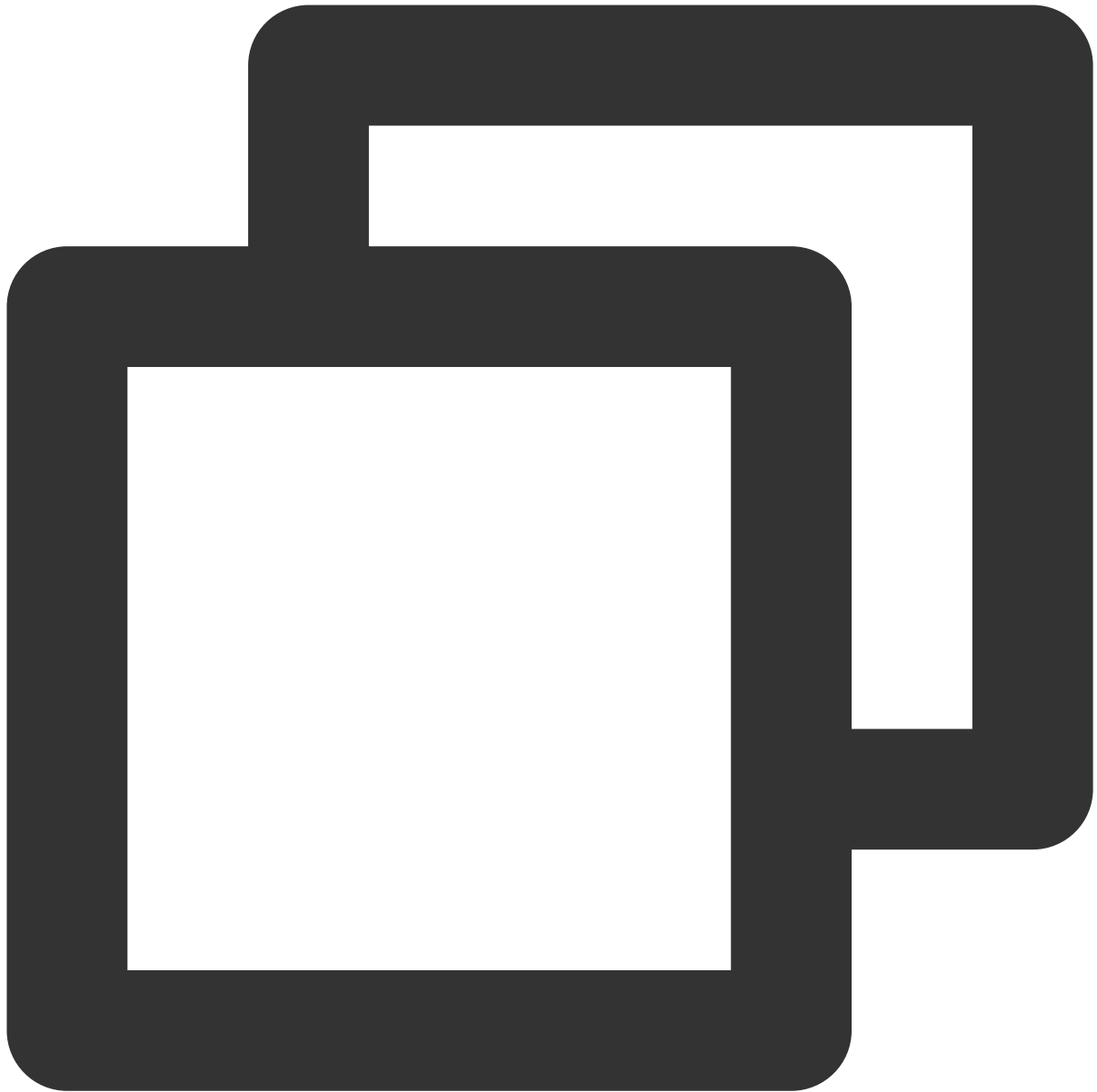
주의 사항

Linux 운영 체제의 릴리스 버전이 다르면 USB/IP 설치 방법과 커널 모듈 이름에 다소 차이가 있을 수 있습니다. 현재 사용하고 있는 Linux 시스템이 USB/IP 기능을 지원하는지 확인하시기 바랍니다.

작업 순서

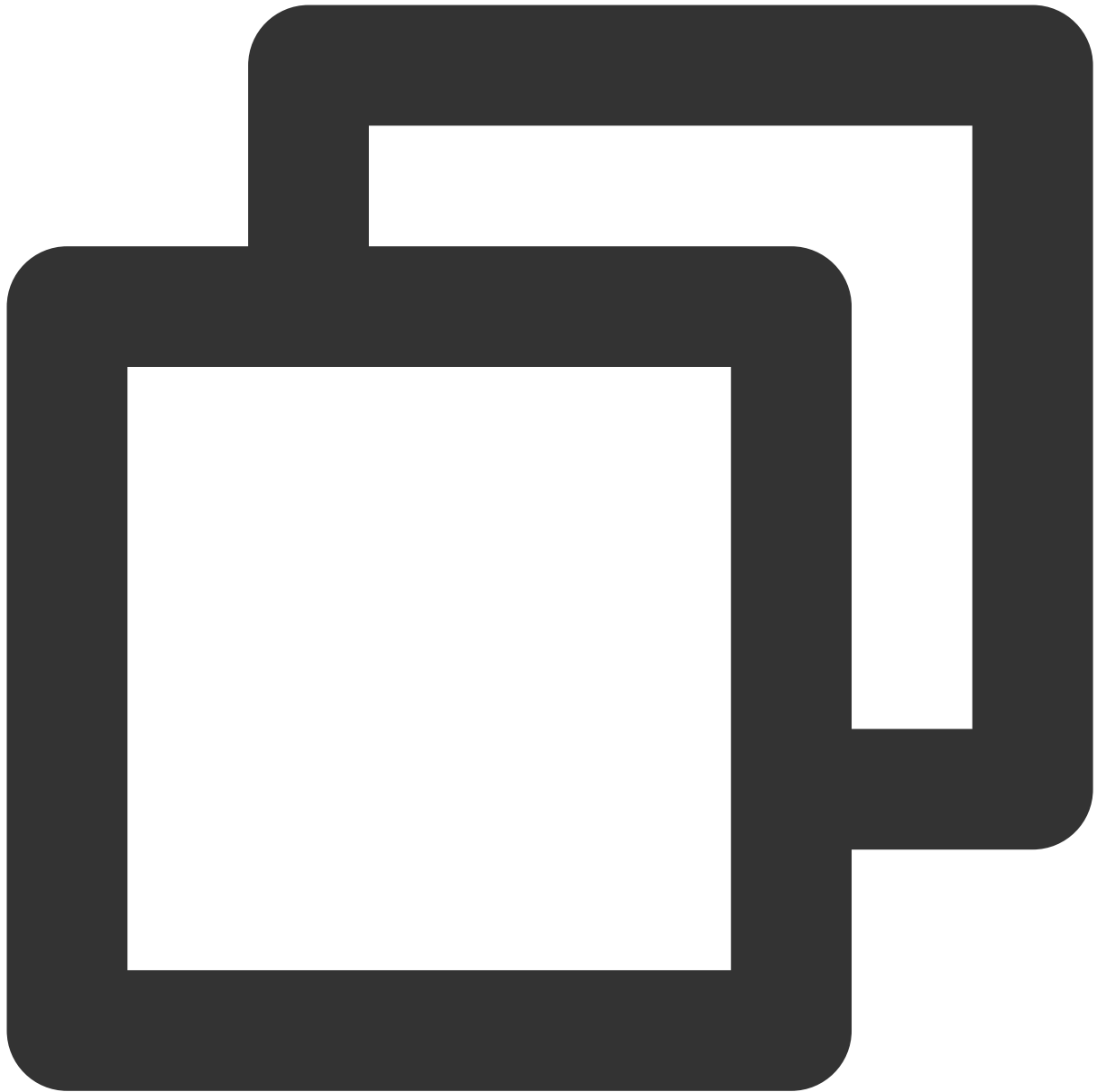
USB Server 설정

1. 로컬 컴퓨터에서 다음 명령어를 순서대로 실행하여 USB/IP를 설치하고 관련 커널 모듈을 다운로드합니다.



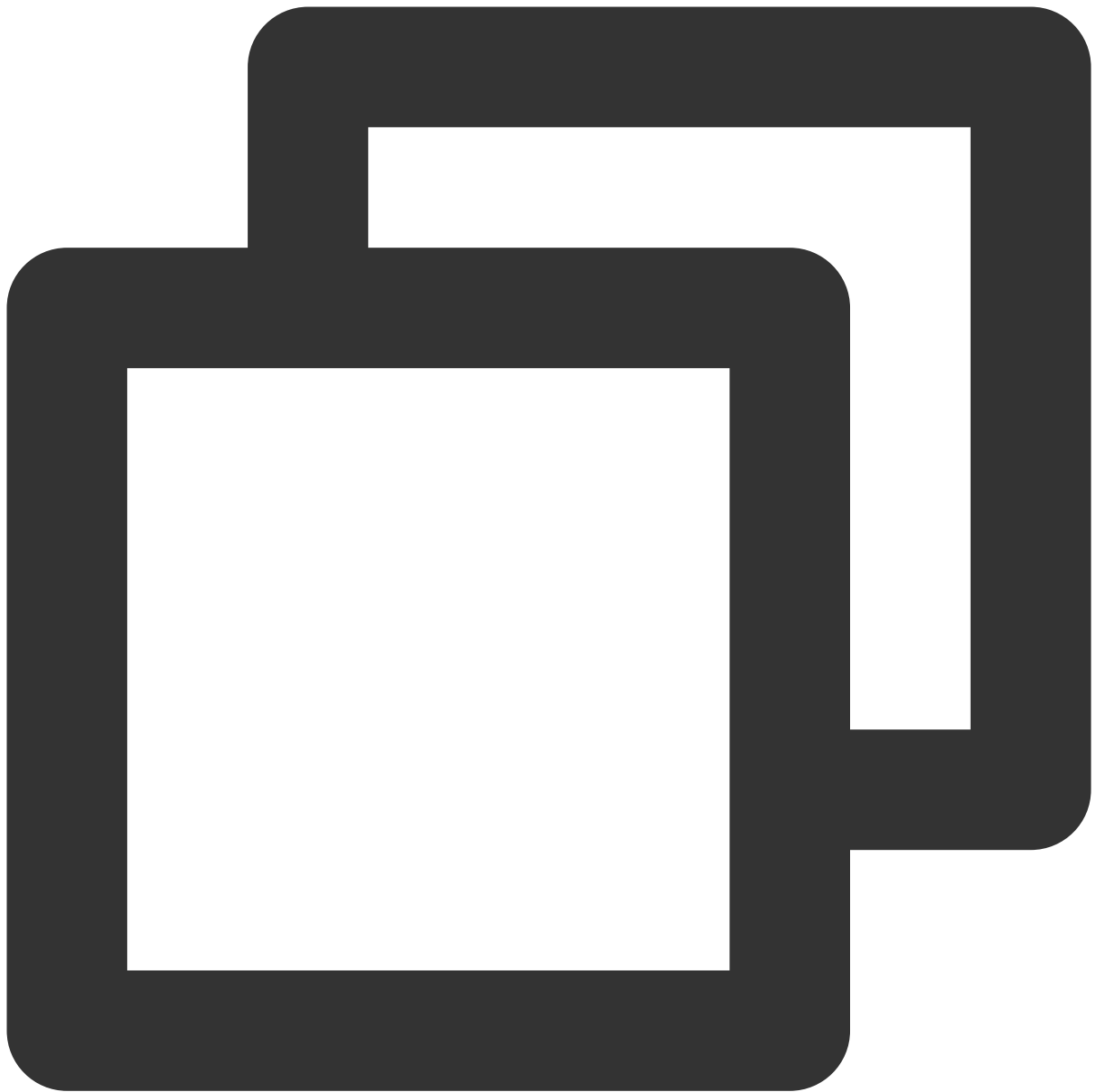
```
sudo apt-get install usbip  
sudo modprobe usbip-core  
sudo modprobe vhci-hcd  
sudo modprobe usbip_host
```

2. USB 장치를 삽입한 뒤 다음 명령어를 실행하여 사용 가능한 USB 장치를 조회합니다.



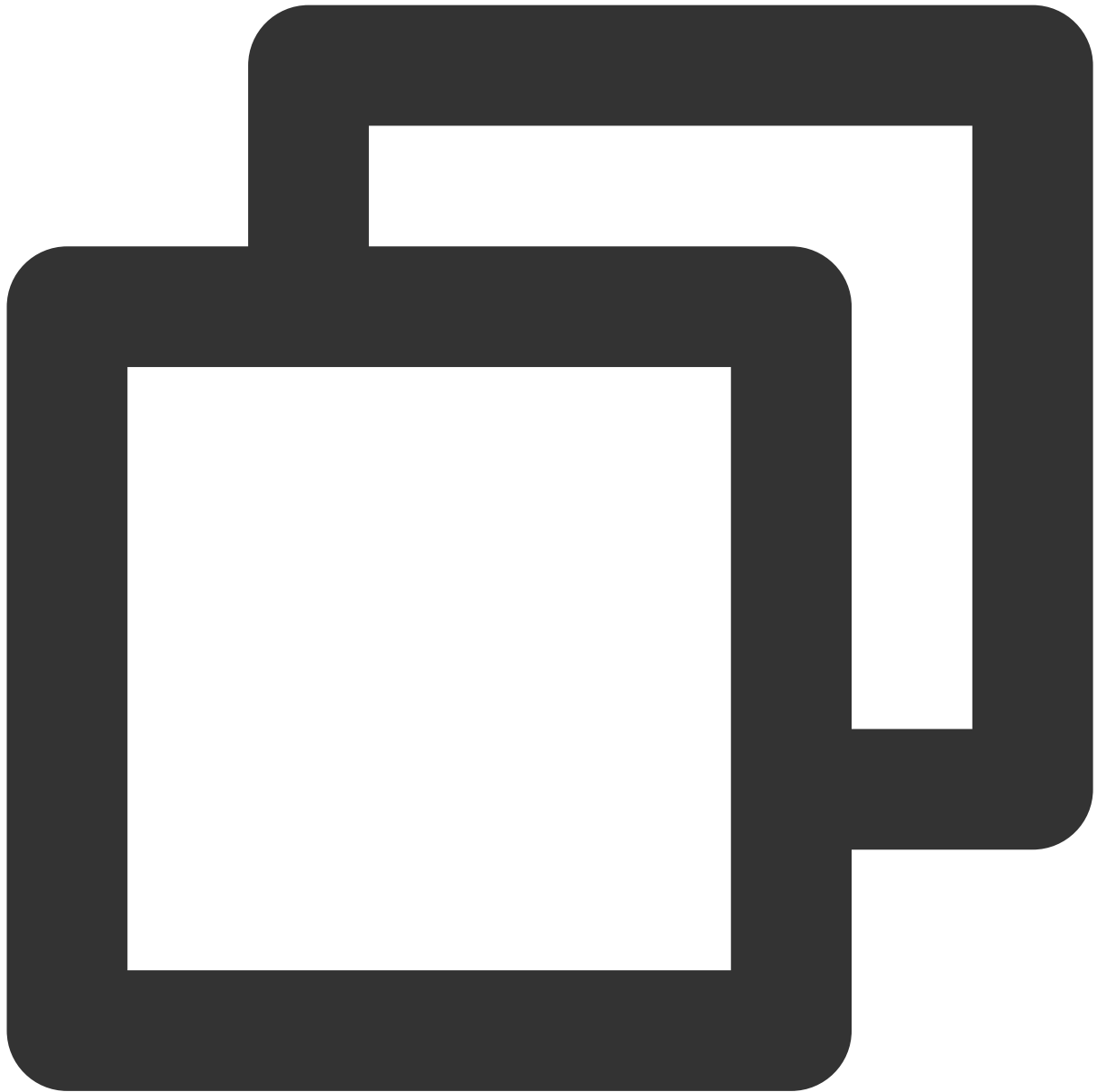
```
usbip list --local
```

예를 들어, 로컬 컴퓨터에 Feitian 이라는 U-Key 를 삽입하면, 다음과 같은 결과를 출력합니다.



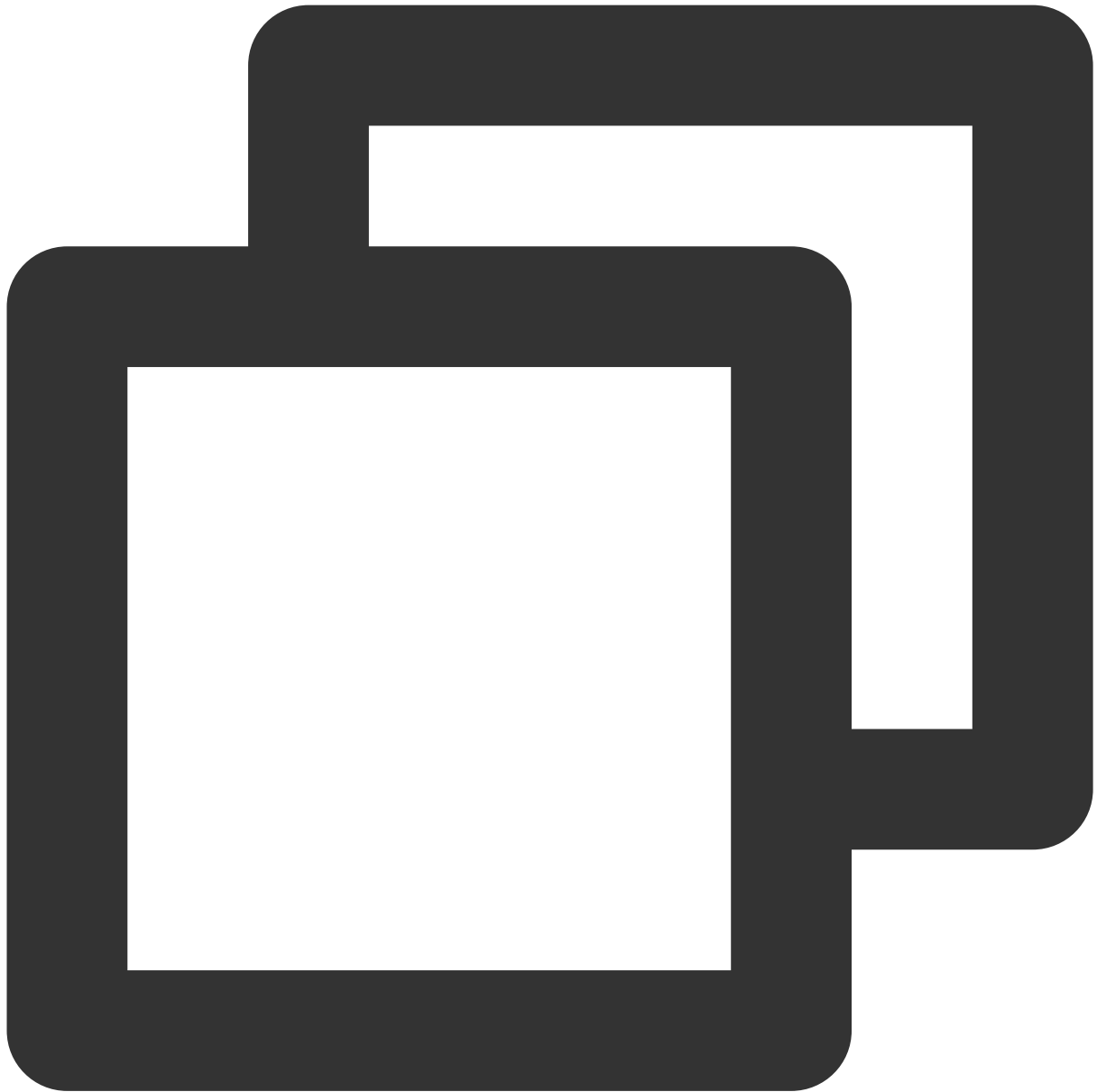
```
busid 1-1.3(096e:031b)  
Feitian Technologies, Inc.: unknown product(096e:031b)
```

3. busid 값을 기록하고 다음 명령어를 순서대로 실행하여 리스너 서비스를 실행합니다. USB/IP 포트 번호를 지정하여 USB 장치를 공유합니다.



```
sudo usbipd -D [--tcp-port PORT]
sudo usbip bind -b [busid]
```

예를 들어, 지정한 USB/IP의 포트 번호가 3240 포트이고(즉 USB/IP의 기본 포트), busid 값은 1-1.3 이라면, 다음의 명령어를 실행합니다.

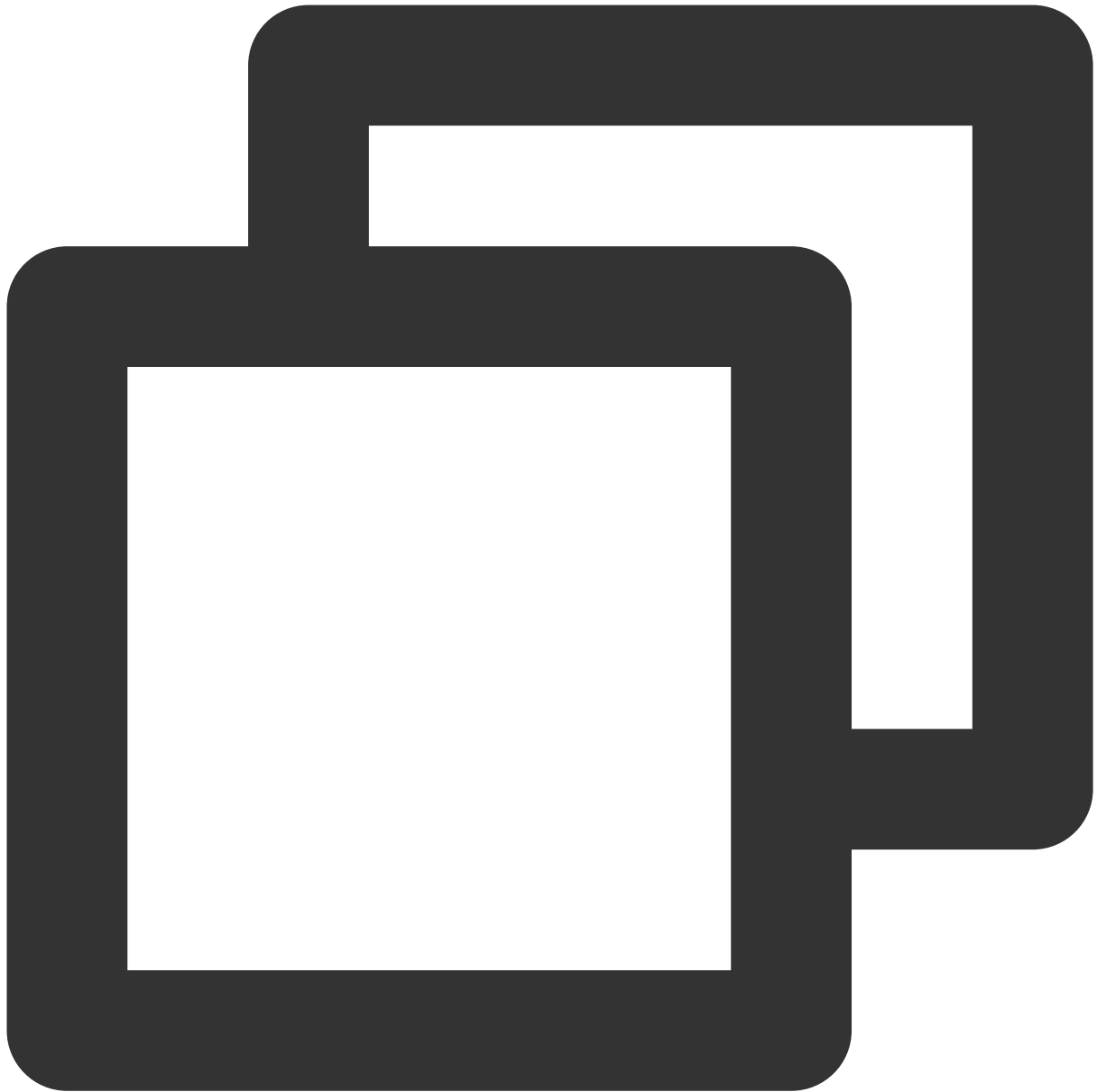


```
sudo usbipd -D
sudo usbip bind -b 1-1.3
```

4. (선택) 다음 명령어를 실행하여 SSH 터널을 생성하고, 포트 리스너를 사용합니다.

설명 :

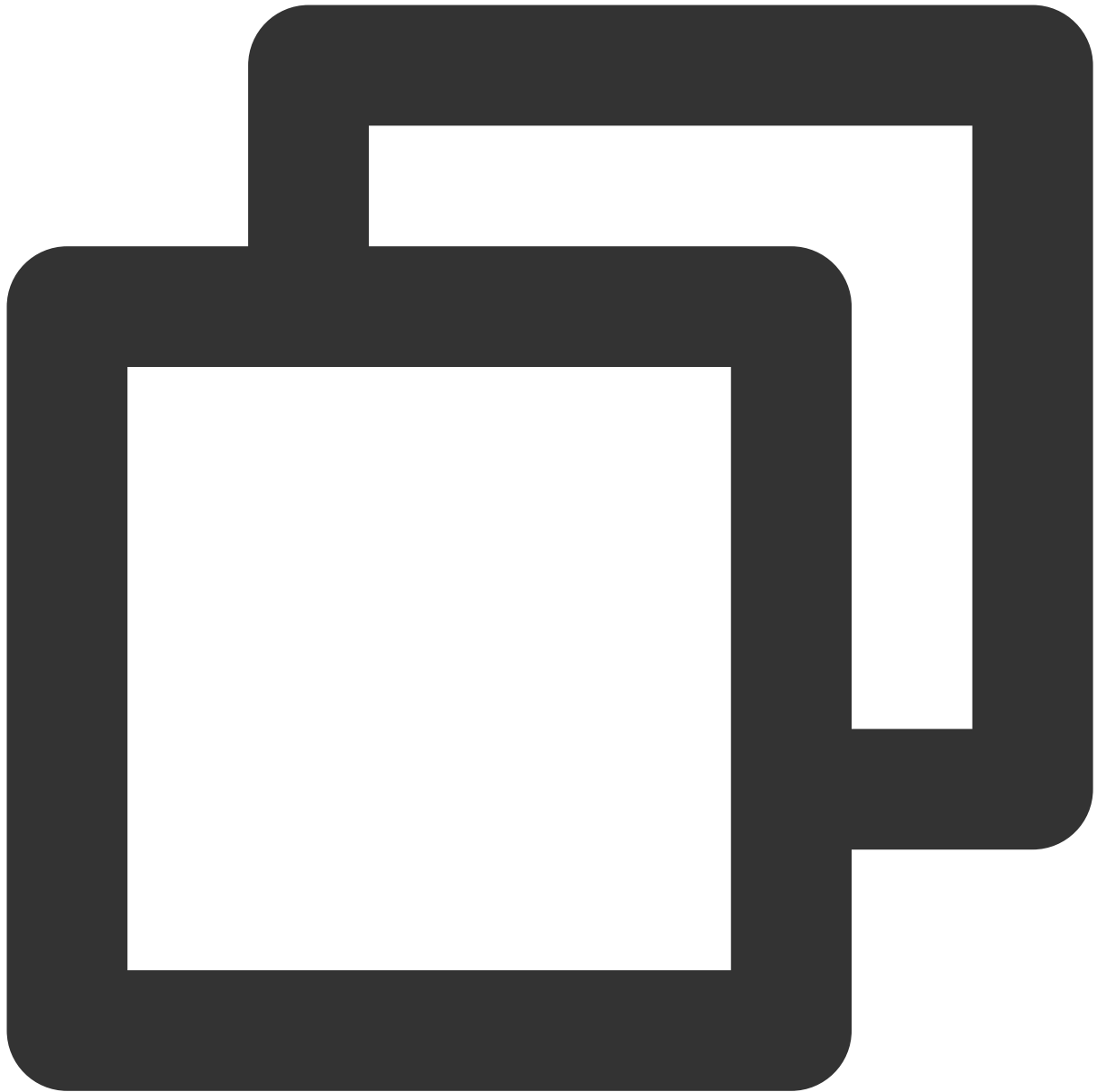
로컬 컴퓨터에 공인 IP가 없다면 이 작업을 실행하시고, 로컬 컴퓨터에 공인 IP가 있다면 이 작업을 건너뛰시기 바랍니다.



```
ssh -Nf -R USB/IP 지정 포트 번호: localhost: USB/IP 지정 포트 번호 root@your_host
```

`your_host` 는 CVM의 IP 주소를 나타냅니다.

예를 들어, USB/IP 포트 번호가 3240 포트이고 CVM의 IP 주소가 192.168.15.24 라면, 다음의 명령어를 실행합니다.



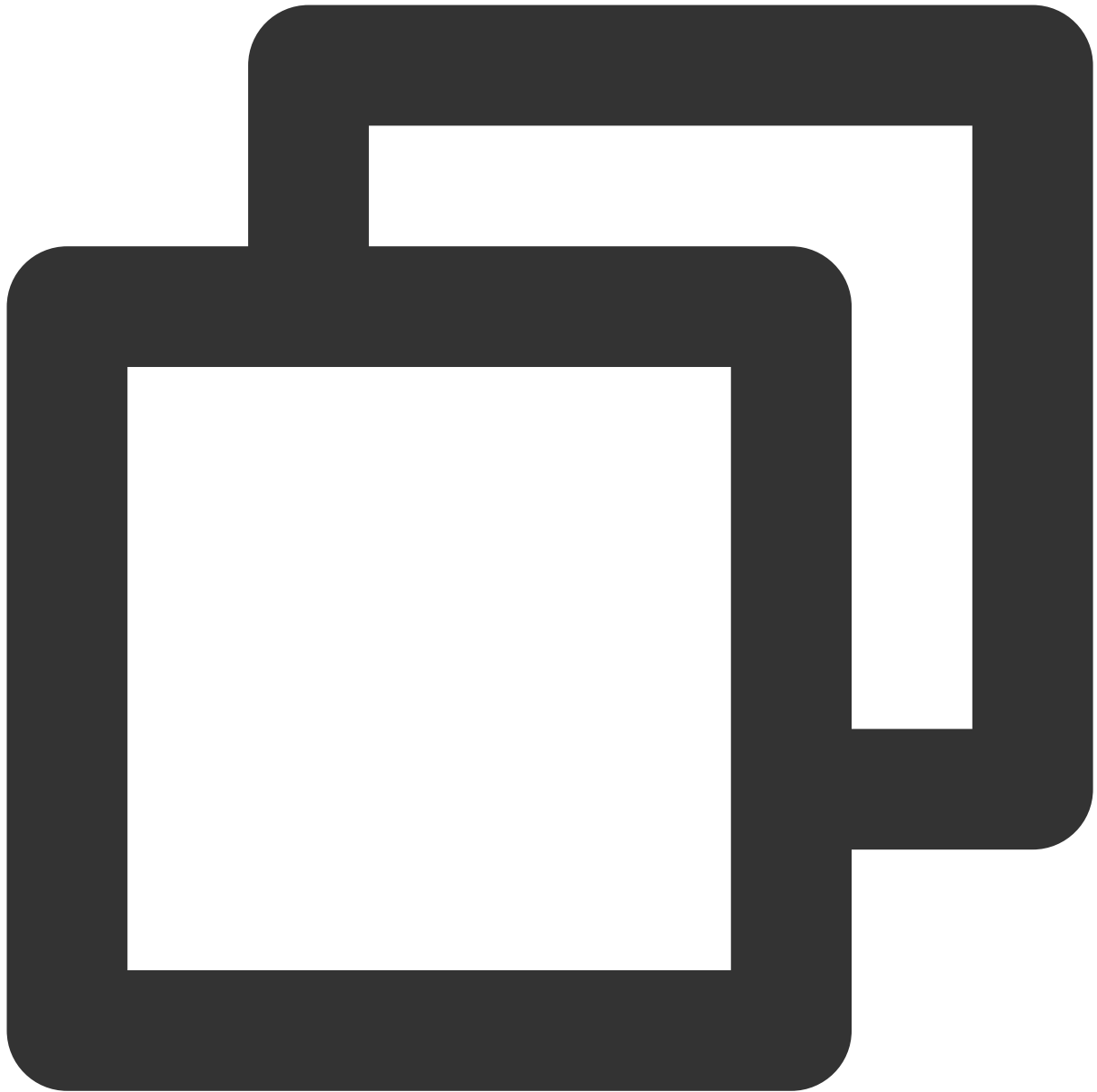
```
ssh -Nf -R 3240:localhost:3240 root@192.168.15.24
```

USB Client 설정

설명 :

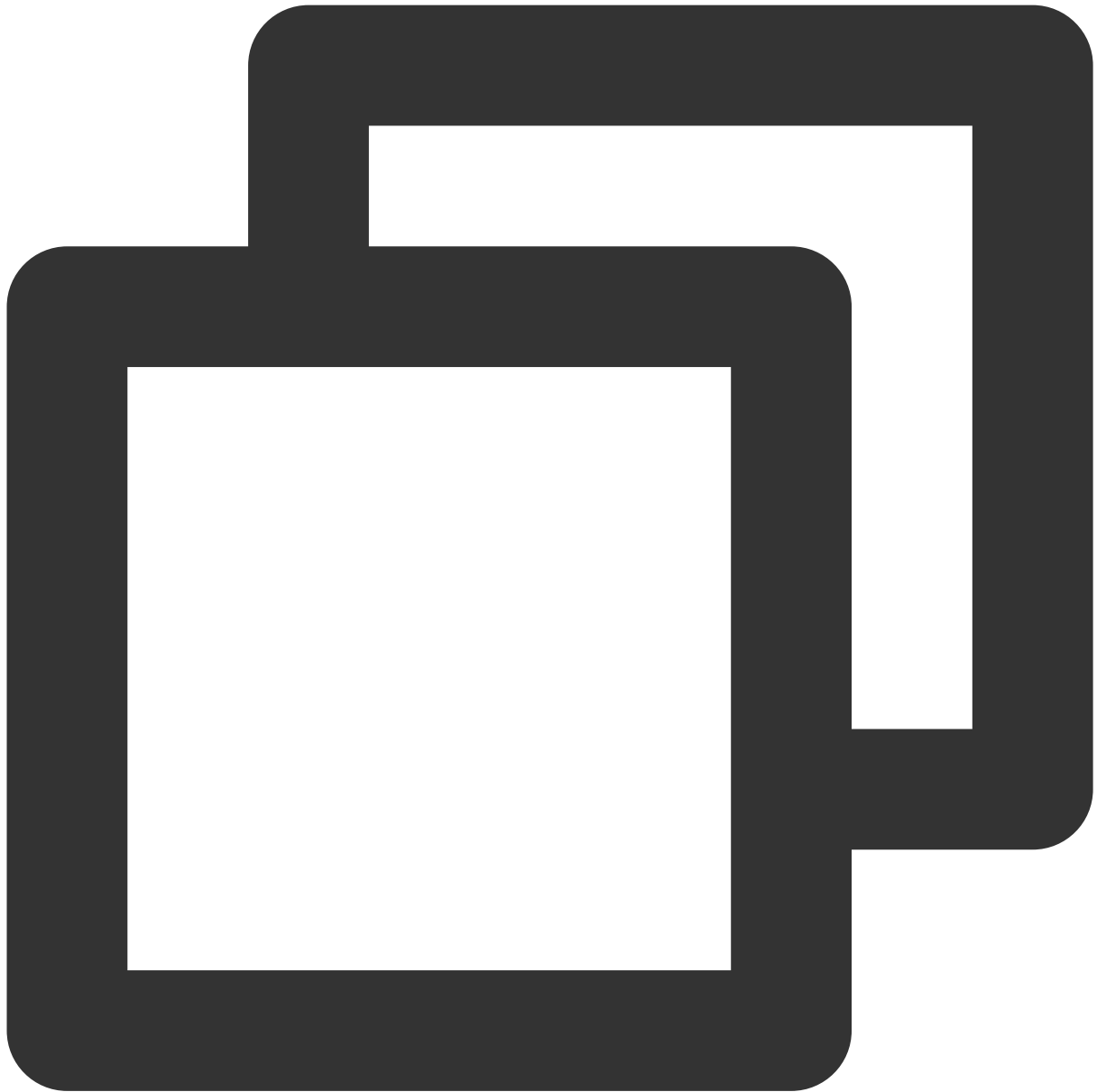
다음의 작업 순서는 로컬 컴퓨터에 공인 IP가 없는 상황을 예로 들어 설명합니다. 로컬 컴퓨터에 공인 IP가 있다면, 작업 순서 중의 127.0.0.1 를 본인의 로컬 컴퓨터의 공인 IP 주소로 수정하시기 바랍니다.

1. [표준 방식으로 Linux 인스턴스에 로그인\(권장\)](#)합니다.
2. 다음 명령어를 순서대로 실행하여, USB/IP 소스를 다운로드합니다.



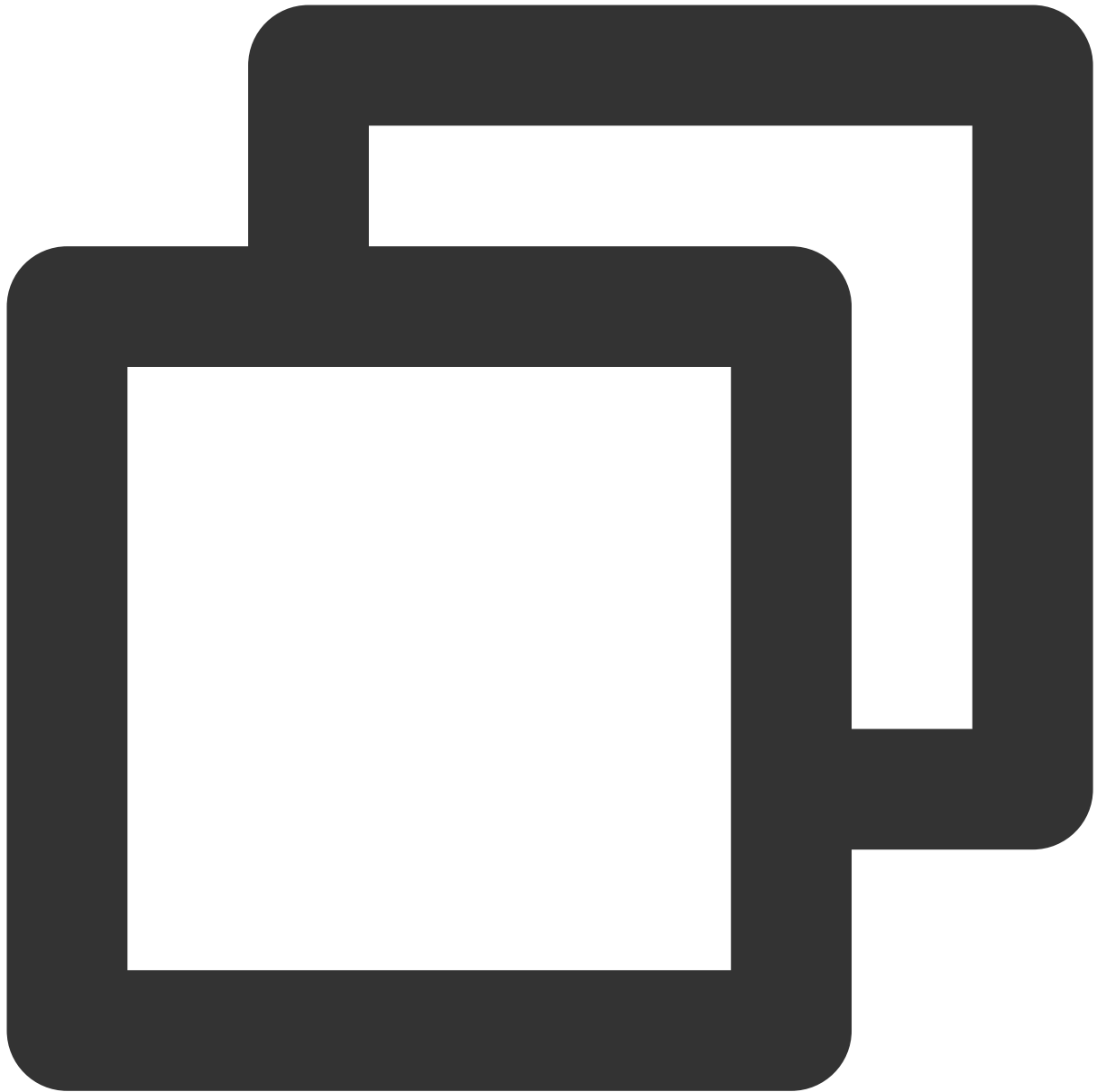
```
rpm --import https://www.elrepo.org/RPM-GPG-KEY-elrepo.org  
rpm -ivh http://www.elrepo.org/elrepo-release-7.0-3.el7.elrepo.noarch.rpm
```

3. 다음 명령어를 순서대로 실행하여 USB/IP를 설치합니다.



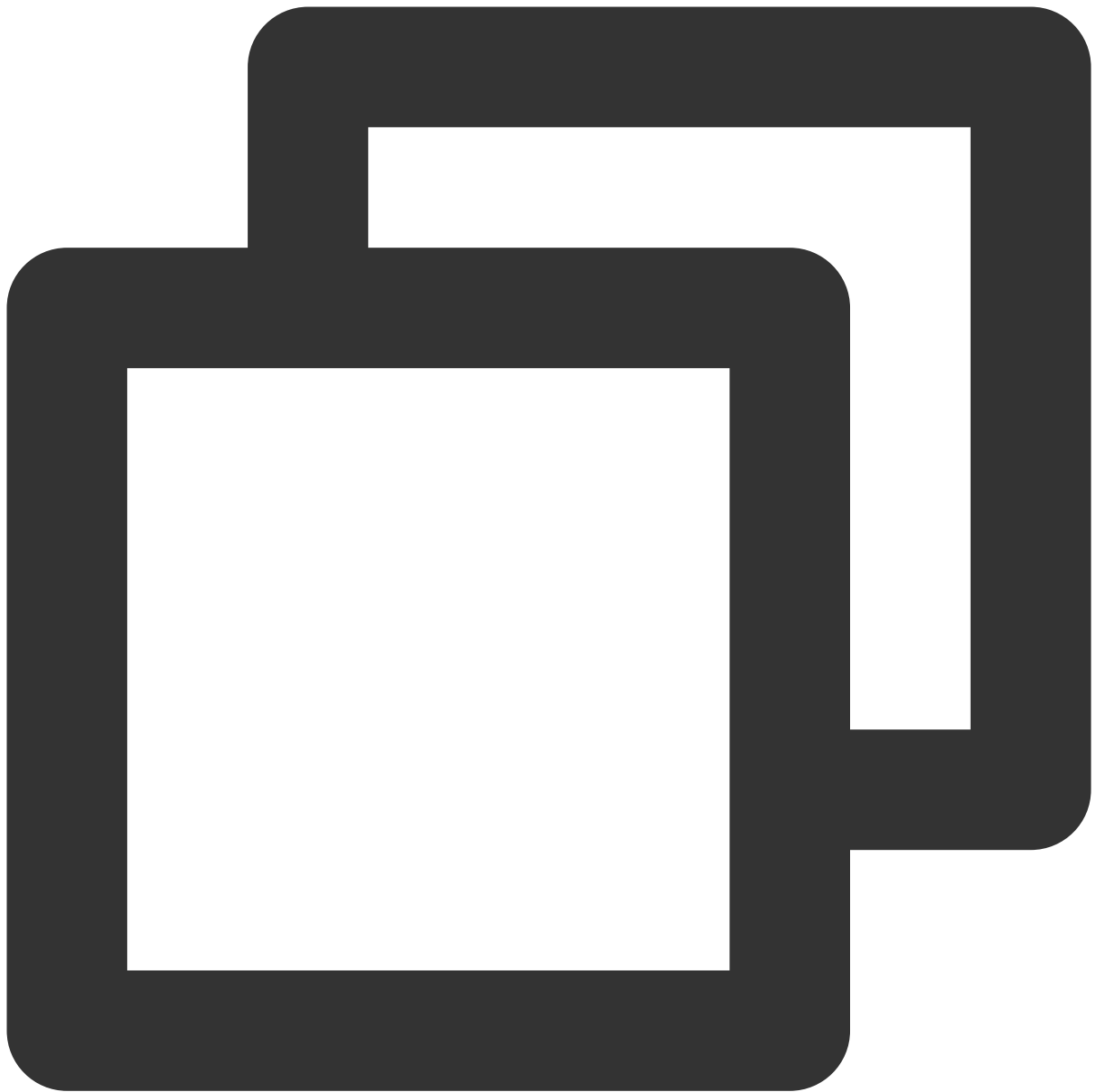
```
yum -y install kmod-usbip usbip-utils  
modprobe usbip-core  
modprobe vhci-hcd  
modprobe usbip-host
```

4. 다음 명령어를 실행하여 CVM에서 사용 가능한 USB 장치를 조회합니다.



```
usbip list --remote 127.0.0.1
```

예를 들어, Feitian 이라는 U-Key 정보를 찾으면, 다음과 같은 결과를 출력합니다.

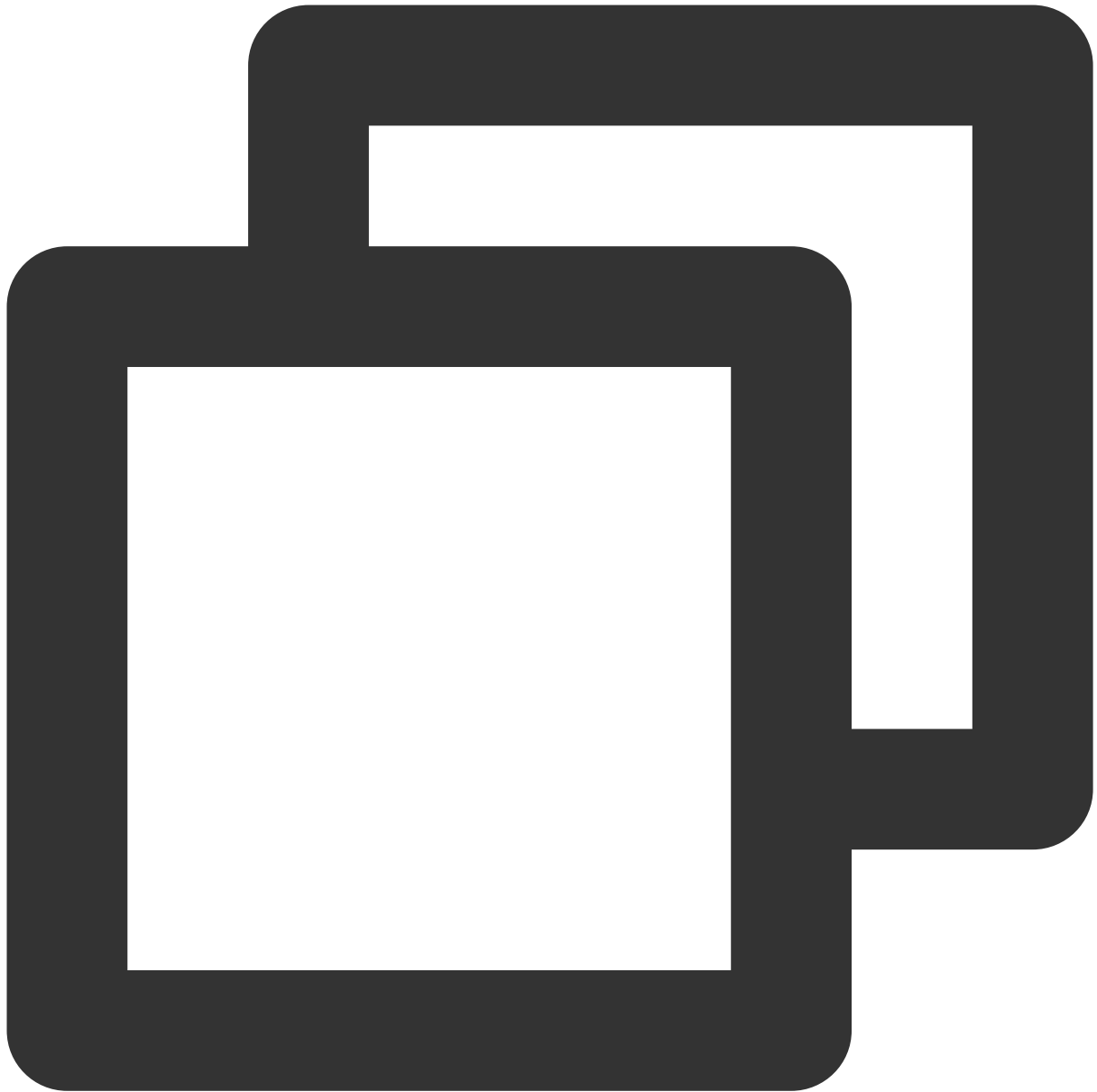


```
Exportable USB devices
```

```
=====
```

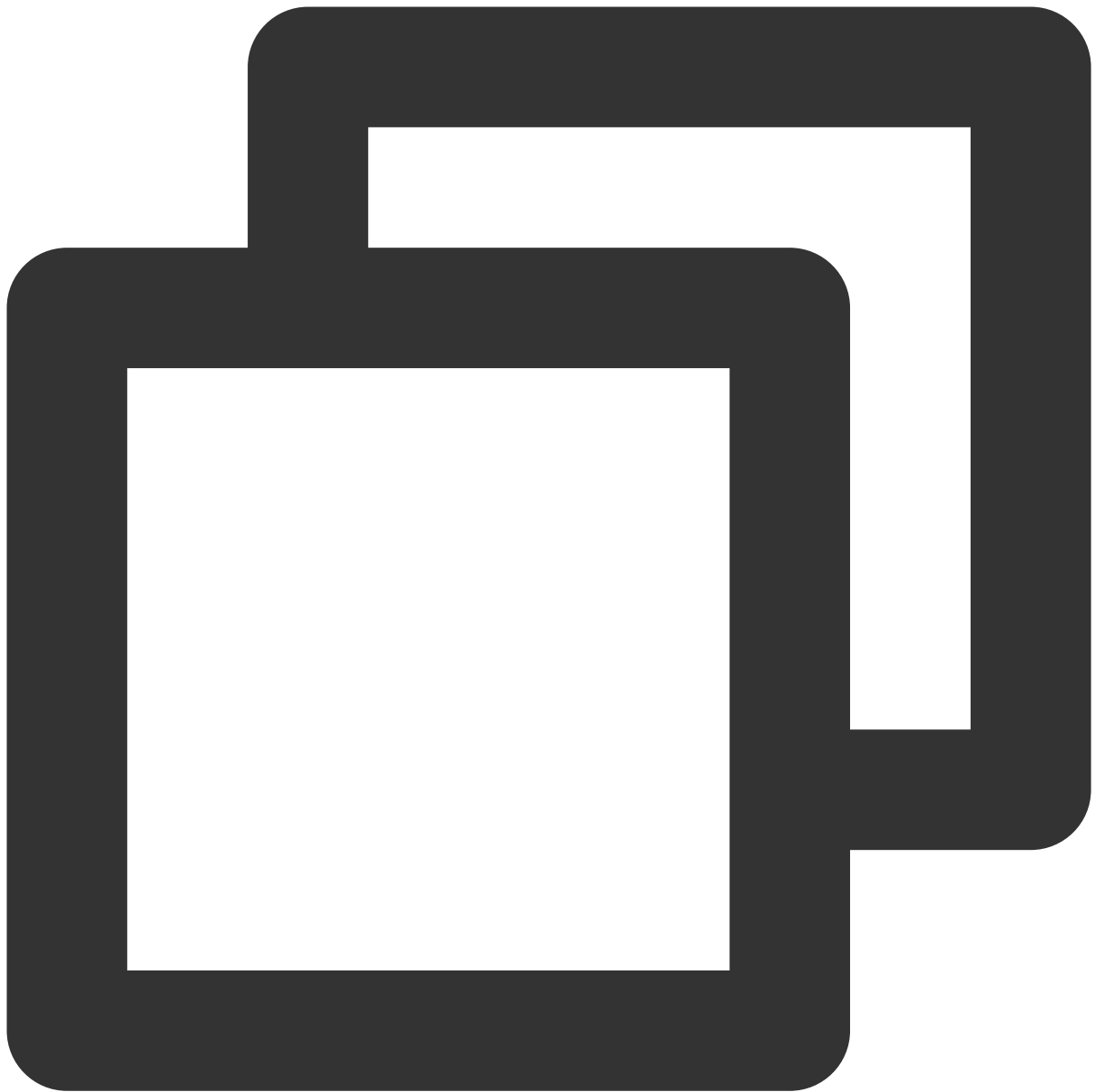
```
-127.0.0.1 1-1.3: Feitian Technologies, Inc.: unknown product (096e:031b):/sys/device
```

5. 다음 명령어를 실행하여 USB 장치를 서버에 바인딩합니다.



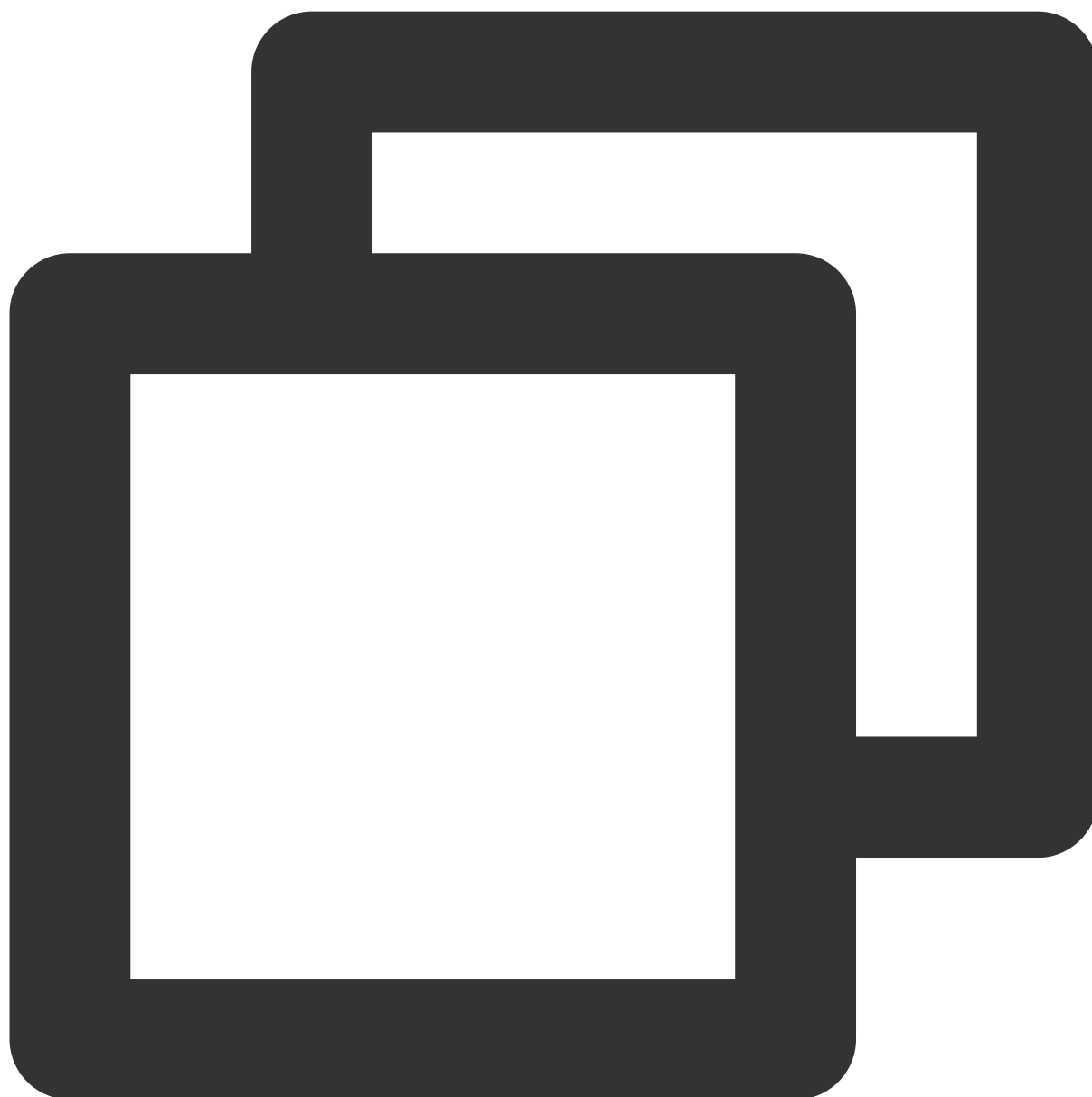
```
usbip attach --remote=127.0.0.1 --busid=1-1.3
```

6. 다음 명령어를 실행하여 현재 USB 장치 리스트를 조회합니다.



```
lsusb
```

다음과 같은 정보가 출력되면, 공유에 성공했음을 의미합니다.



```
Bus 002 Device 002:ID096e:031b Feitian Technologies, Inc.  
Bus 002 Device 001:ID1d6b:0002 Linux Foundation 2.0 root hub  
Bus 001 Device 001:ID1d6b:0001 Linux Foundation 1.1 root hub
```

Windows 시스템에서 RemoteFx를 사용하여 USB 장치 리디렉션

최종 업데이트 날짜: : 2024-02-02 11:01:47

작업 시나리오

RemoteFx는 Windows RDP 데스크톱 프로토콜의 업그레이드 버전으로, RDP 8.0 버전부터는 RemoteFx를 사용한 USB 리디렉션이 가능합니다. RDP의 데이터 채널을 통해 로컬 USB 장치를 원격 데스크톱으로 리디렉션하면, 클라우드 기기에서 USB 장치를 사용할 수 없는 문제를 해결할 수 있습니다.

본 문서는 다음과 같은 환경을 예로 들어, RDP의 RemoteFx USB Redirection 기능을 활성화하고 CVM에 리디렉션하는 방법을 소개합니다.

클라이언트: Windows 10 운영 체제

서버: Windows Server 2016 운영 체제

사용 제한

RDP 8.0 이상의 버전은 모두 RemoteFX USB Redirection 기능을 지원하며, Windows 8, Windows 10, Windows Server 2016 및 Windows Server 2019 도 모두 RemoteFX USB Redirection 기능을 지원합니다. 만약 로컬 컴퓨터의 운영 체제가 상기 버전이라면, RDP 8.0 Update 패치는 설치할 필요 없습니다. 만약 로컬 컴퓨터의 운영 체제가 Windows 7 이나 Windows Vista 라면, [Microsoft 공식 홈페이지](#)에서 RDP 8.0 Update 패치를 설치하시기 바랍니다.

작업 순서

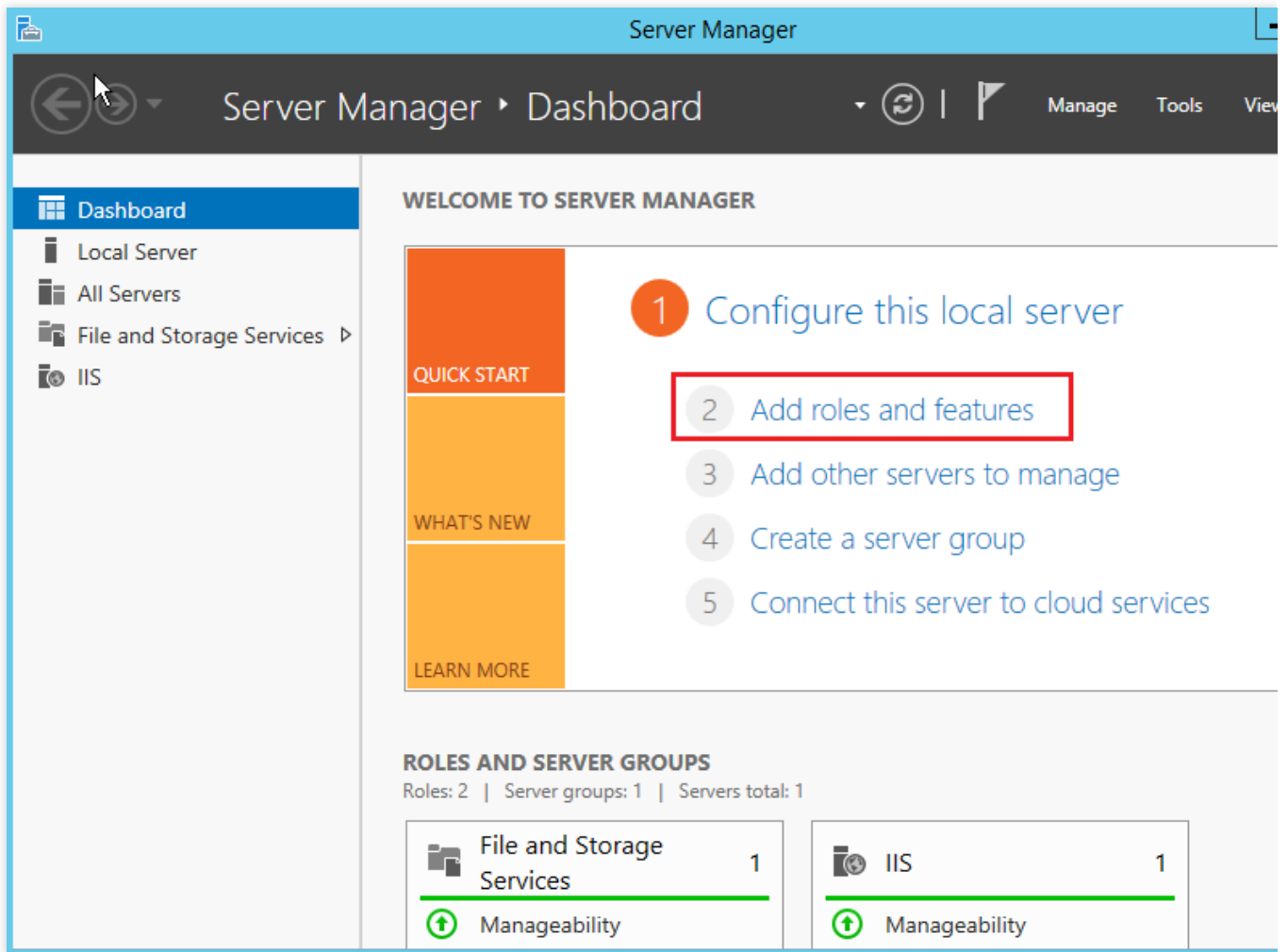
서버 설정

1. [RDP 파일을 사용하여 Windows 인스턴스에 로그인\(권장\)](#)합니다.
2. 운영 체제 인터페이스에서

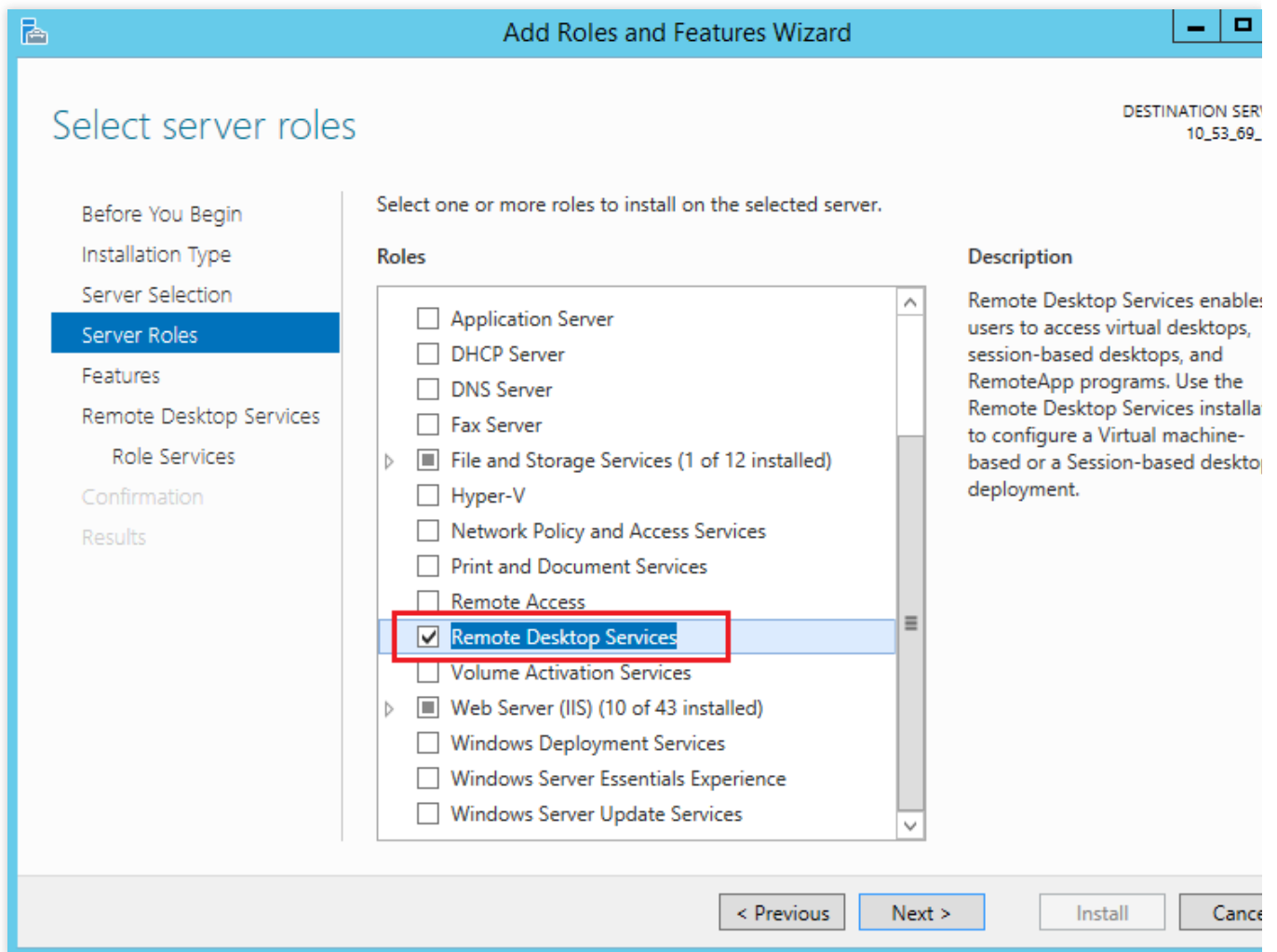


를 클릭한 뒤, [서버 관리자]를 선택해 서버 관리자 창을 엽니다.

3. 아래 이미지와 같이, '서버 관리자' 창에서 [역할 및 기능 추가]를 클릭합니다.

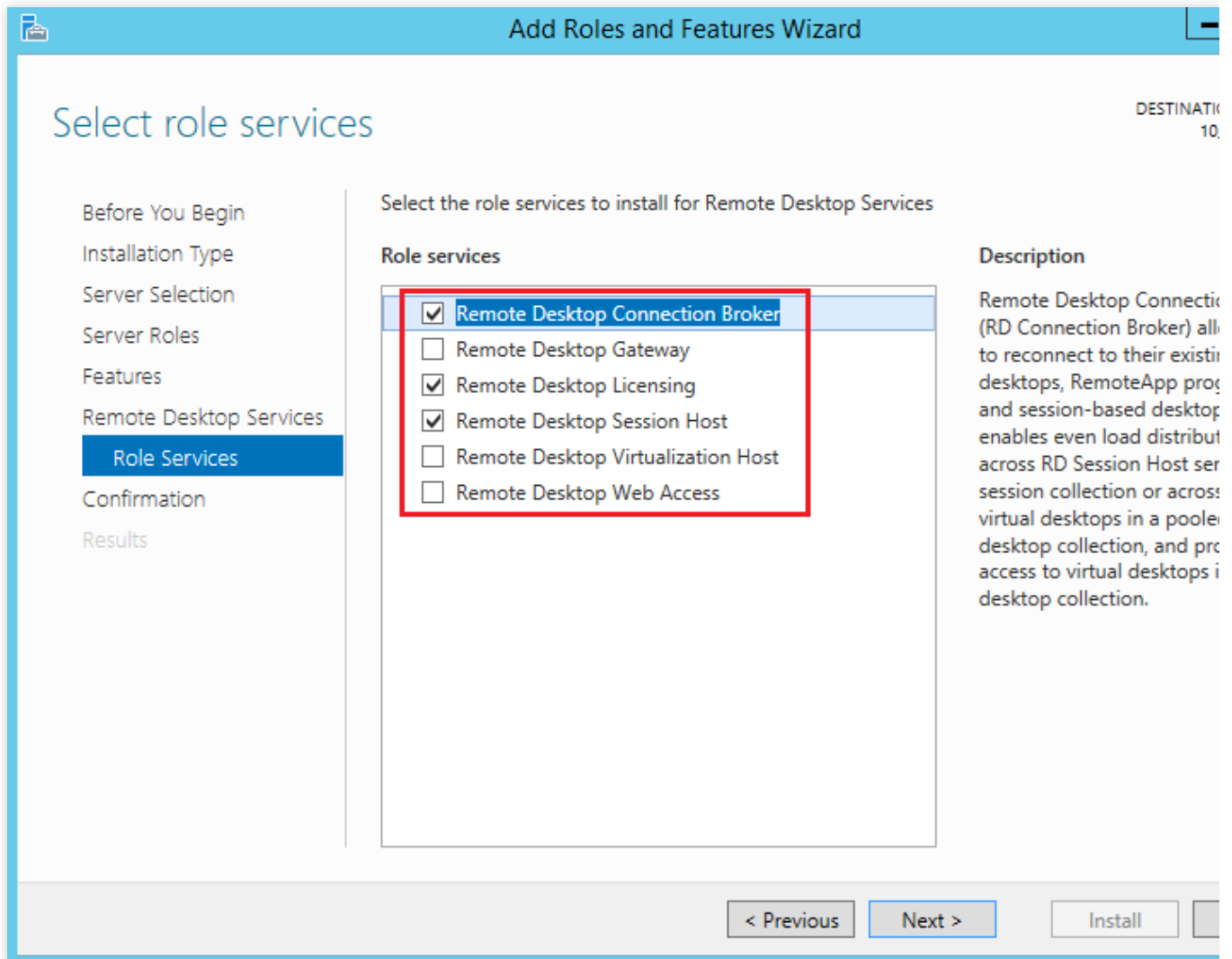


4. 팝업된 '역할 및 기능 추가 마법사' 창에서 [다음]을 클릭하여 '설치 유형 선택' 인터페이스로 이동합니다.
5. '설치 유형 선택' 인터페이스에서 [역할 기반 또는 기능 기반 설치]를 선택하고, [다음]을 클릭합니다.
6. '대상 서버 선택' 인터페이스에서 기본 설정을 유지한 채 [다음]을 클릭합니다.
7. 아래 이미지와 같이, '서버 역할 선택' 인터페이스에서 [원격 데스크톱 서비스]를 선택하고 [다음]을 클릭합니다.



8. 기본 설정을 유지한 채 [다음]을 2번 연속 클릭합니다.

9. 아래 이미지와 같이, '역할 서비스 선택' 인터페이스에서 [원격 데스크톱 세션 호스트], [원격 데스크톱 연결 브로커], [원격 데스크톱 라이선싱]을 선택한 뒤, 팝업 창에서 [기능 추가]를 클릭합니다.



10. [다음]을 클릭합니다.

11. [설치]를 클릭합니다.

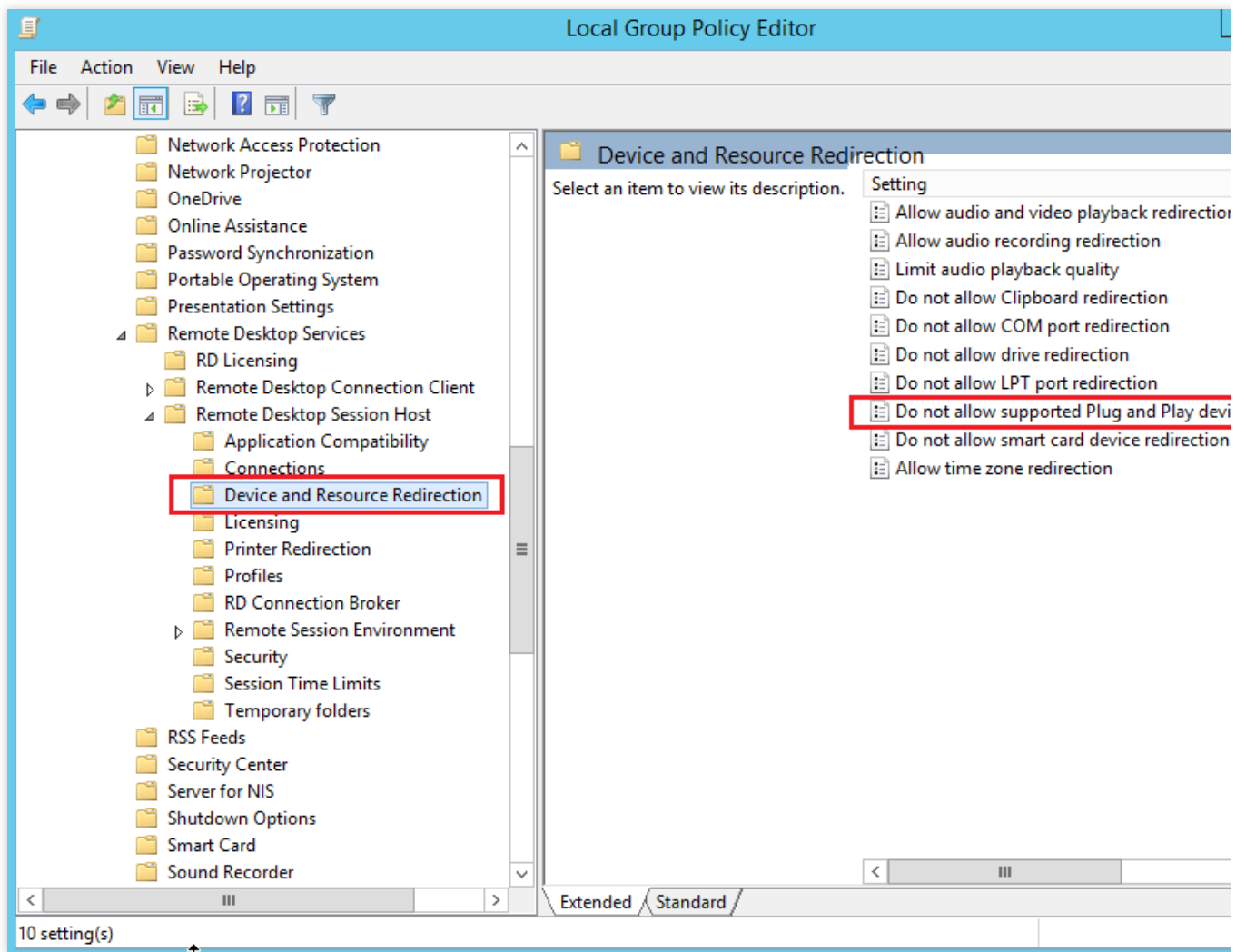
12. 설치가 완료되면 CVM을 재시작합니다.

13. 운영 체제 인터페이스에서

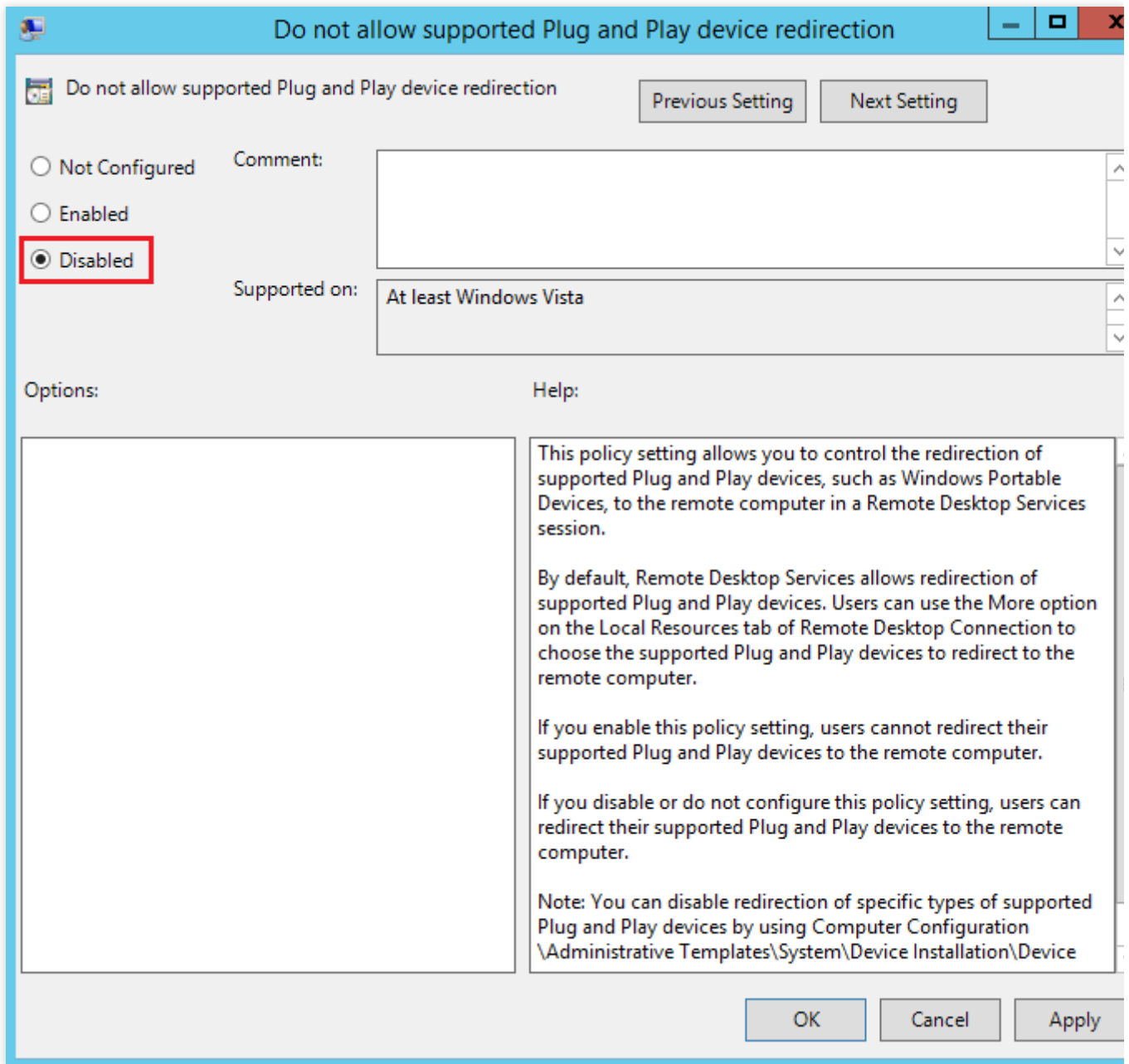


를 클릭하고, **gpedit.msc**를 입력한 뒤 **Enter**를 눌러 '로컬 그룹 정책 편집기'를 엽니다.

14. 아래 이미지와 같이 왼쪽 디렉터리 트리에서 [컴퓨터 구성]>[관리 템플릿]>[Windows 구성 요소]>[원격 데스크톱 서비스]>[원격 데스크톱 세션 호스트]>[장치 및 리소스 리디렉션]을 선택한 뒤, [지원되는 플러그 앤 플레이 장치 리디렉션 허용 안 함]을 더블 클릭하여 엽니다.



15. 아래 이미지와 같이, 팝업 창에서 [사용 안 함]을 선택한 뒤 [확인]을 클릭합니다.



16. CVM을 재시작합니다.

클라이언트 설정

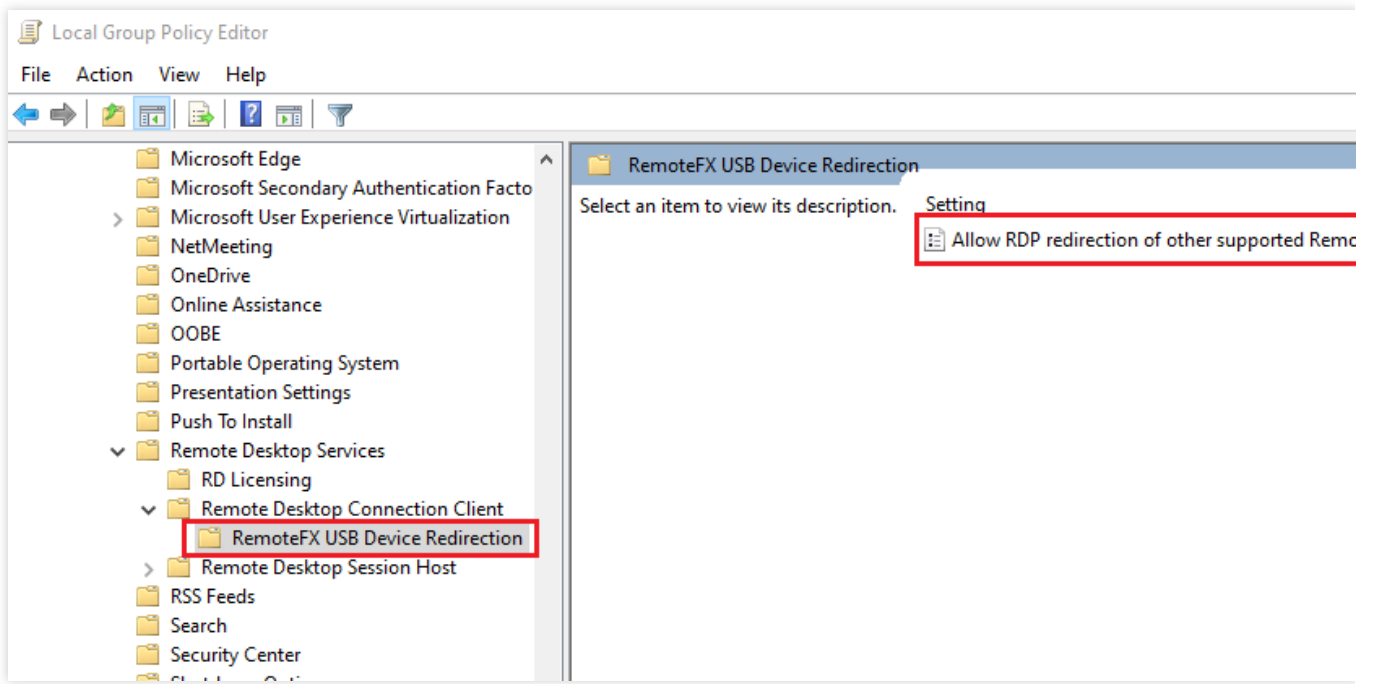
1. 로컬 컴퓨터에서



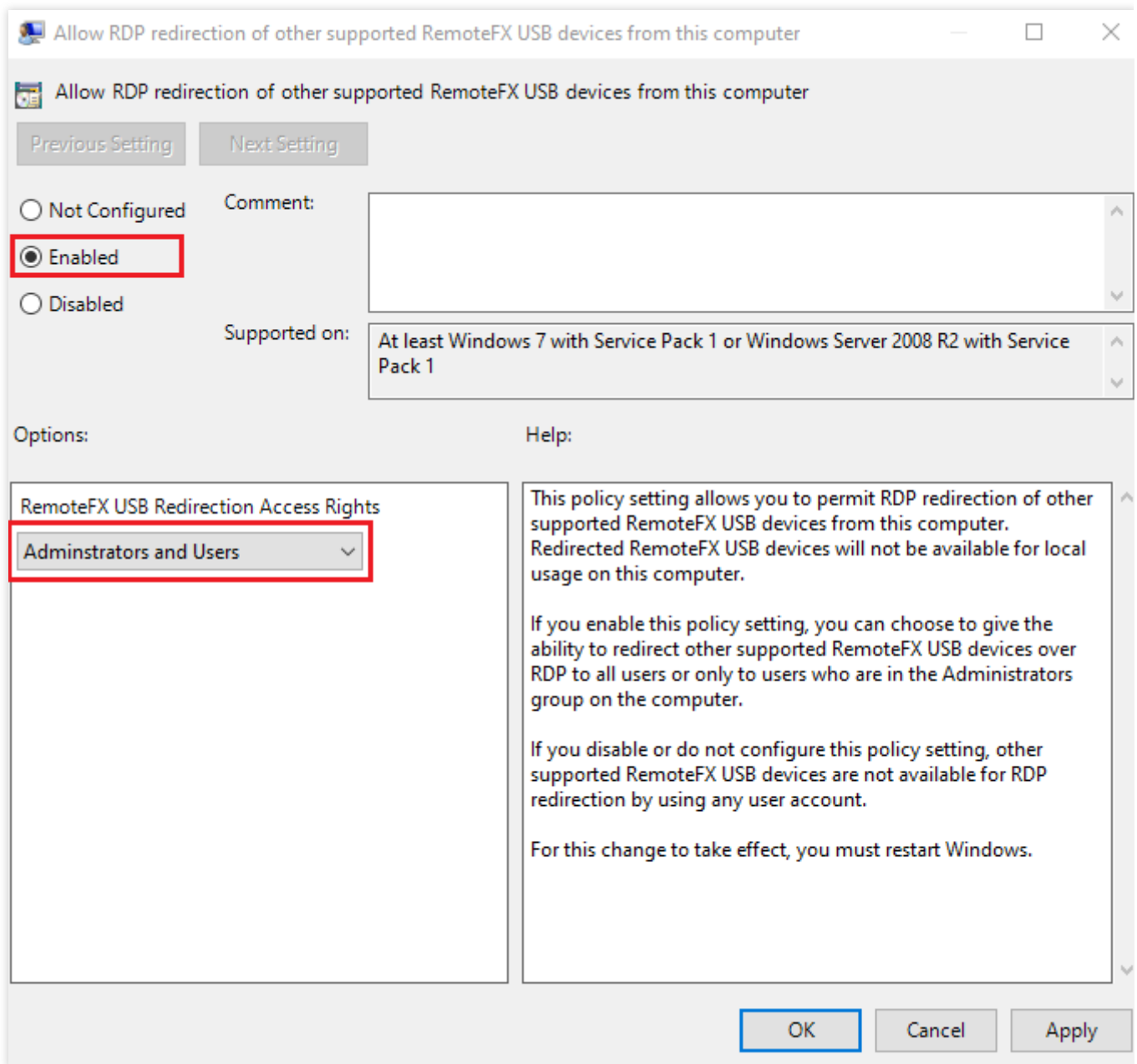
를 우클릭하고 [실행]을 선택하여 실행 대화 상자를 엽니다.

2. 실행 대화 상자에 **gpedit.msc**를 입력한 뒤 [확인]을 클릭하여 '로컬 그룹 정책 편집기'를 엽니다.

3. 아래 이미지와 같이 왼쪽 디렉터리 트리에서 [컴퓨터 구성]>[관리 템플릿]>[Windows 구성 요소]>[원격 데스크톱 서비스]>[원격 데스크톱 연결 클라이언트]>[RemoteFx USB 장치 리디렉션]을 선택한 뒤, [이 컴퓨터에서 지원되는 기타 RemoteFx USB 장치의 RDP 리디렉션 허용]을 더블 클릭하여 엽니다.



4. 아래 이미지와 같이, 팝업 창에서 [사용]을 선택한 뒤 RemoteFx USB 리디렉션 액세스 권한을 [관리자 및 사용자]로 설정합니다.



5. [확인]을 클릭합니다.

6. 로컬 컴퓨터를 재시작합니다.

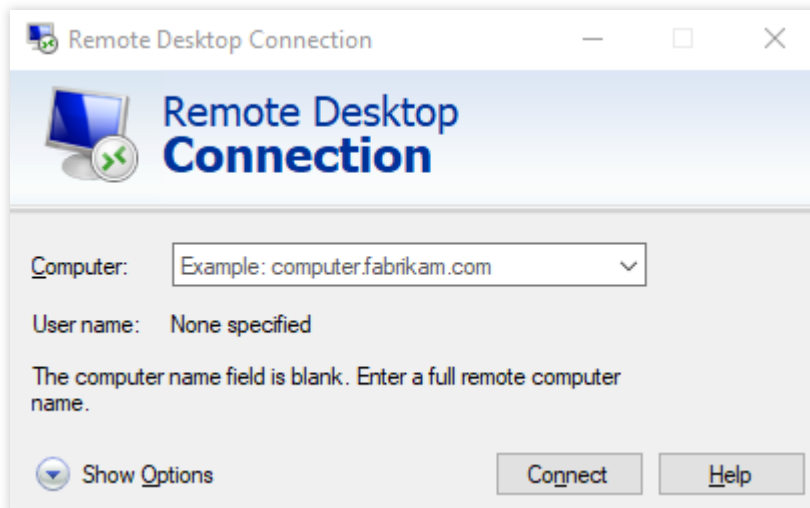
설정 효과 검증

1. 로컬 컴퓨터에 USB 장치를 삽입한 뒤,

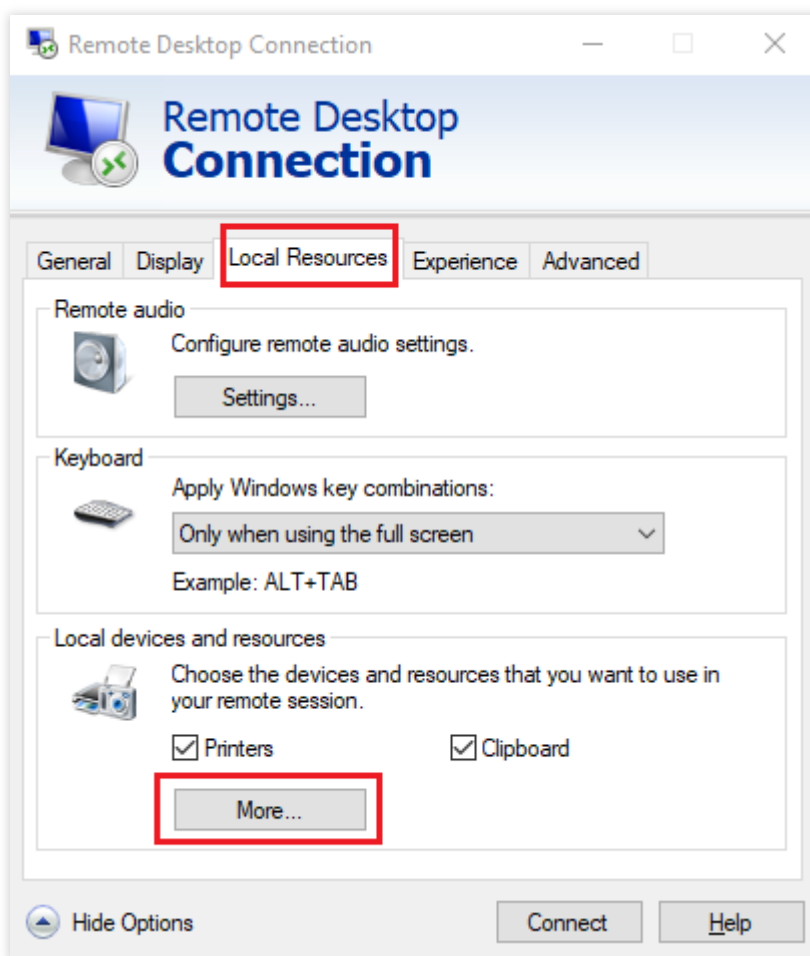


를 우클릭하고 [실행]을 선택하여 대화 상자를 엽니다.

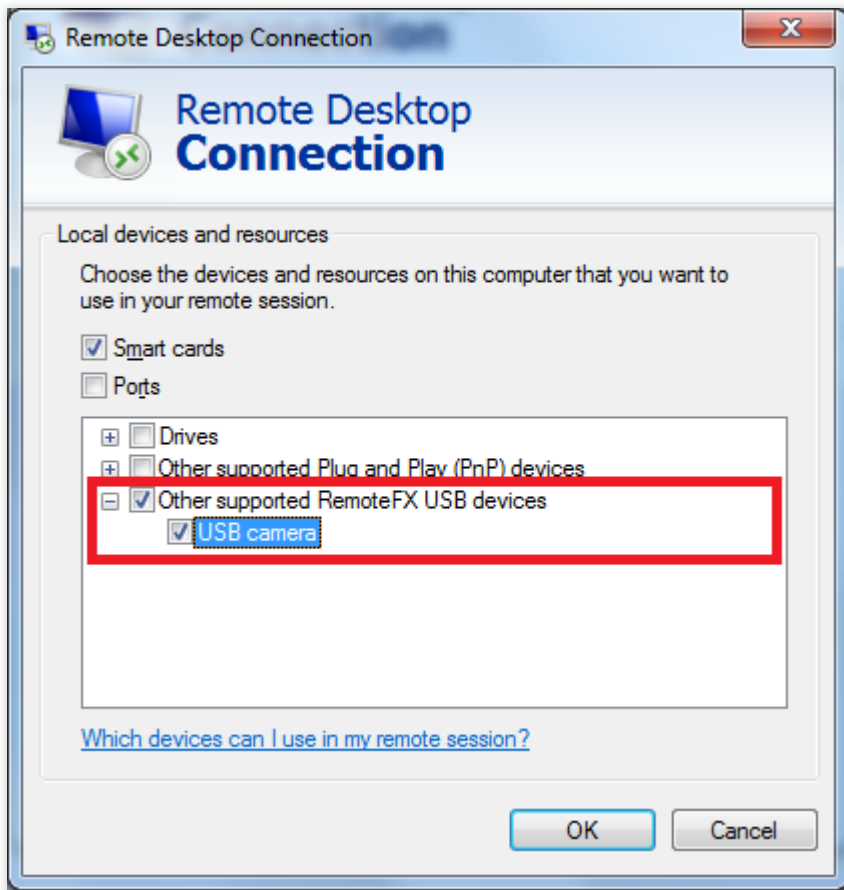
2. 아래 이미지와 같이, 실행 대화 상자에 **mstsc**를 입력한 뒤 **Enter**를 눌러 원격 데스크톱 연결 대화 상자를 엽니다.



3. [컴퓨터] 오른쪽 입력란에 Windows 서버의 공인 IP를 입력한 후 [옵션 표시]를 클릭합니다.
4. 아래 이미지와 같이, [로컬 리소스] 탭을 선택한 뒤 '로컬 장치 및 리소스' 메뉴의 [더 보기]를 클릭하면 로컬 장치 및 리소스 창이 팝업됩니다.

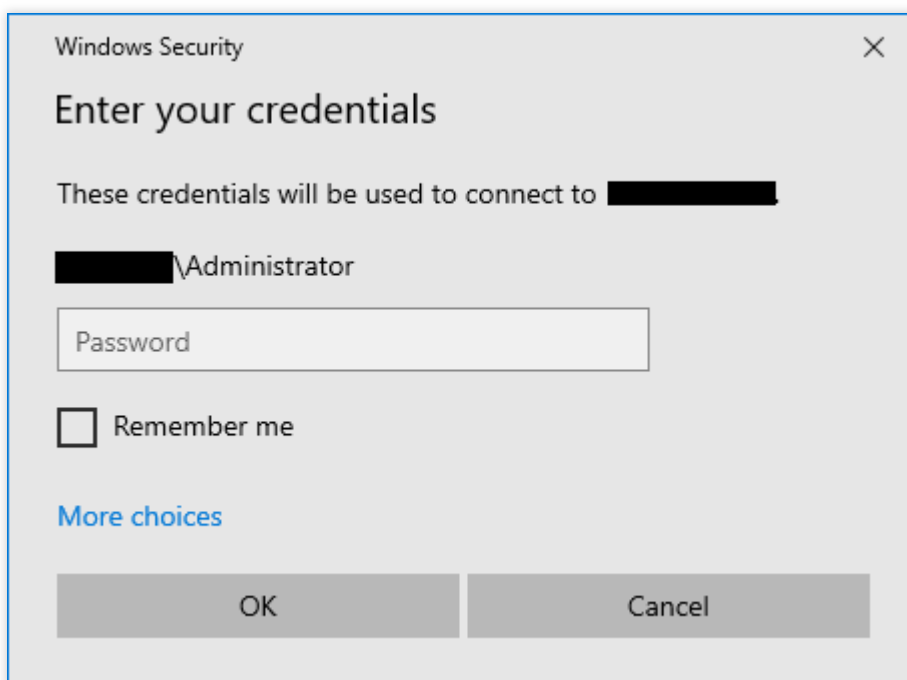


5. 팝업된 로컬 장치 및 리소스 창에서 [지원되는 다른 RemoteFx USB 장치]를 펼치고, 연결할 USB 장치를 선택한 다음 [확인]을 클릭합니다.



6. [연결]을 클릭합니다.

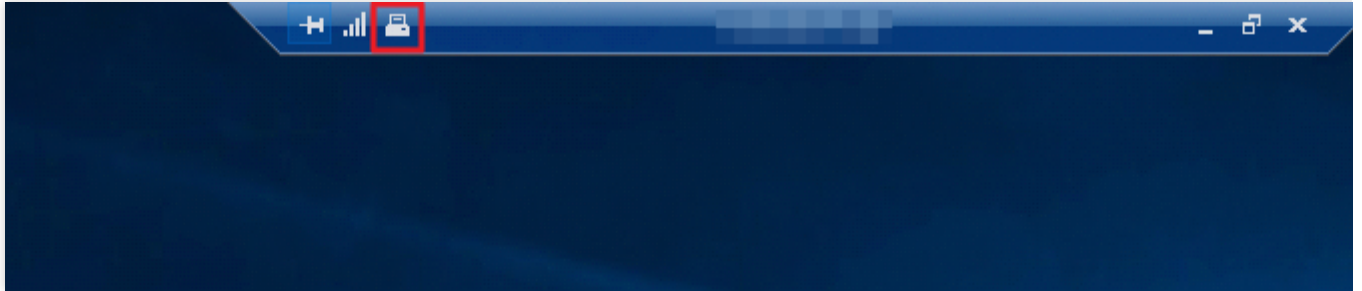
7. 아래 이미지와 같이, 팝업된 'Windows 보안' 창에서 인스턴스의 사용자 이름 및 암호를 입력합니다.



8. [확인]을 클릭하고 Windows 인스턴스에 로그인합니다.

Windows 인스턴스의 작업 인터페이스 상단에

가 나타난다면 설정 성공입니다.



관련 작업

Windows RDP 프로토콜은 자주 사용하는 USB 장치에 더 최적화된 연결 기능을 제공하므로, RemoteFx 기능을 활성화하지 않아도 디스크 드라이버, 카메라 등의 디바이스를 바로 매핑할 수 있습니다. 자주 사용하지 않는 USB 장치의 경우 RemoteFX USB Redirection 기능을 사용해야 하며, 아래의 내용을 참조하여 해당하는 리디렉션 방법을 선택하시기 바랍니다.

Device	Support Status	Redirection Method
All-in-One Printer	Supported	RemoteFX USB Redirection
Printer	Supported	Easy Print
Scanner	Supported	RemoteFX USB Redirection
Biometric	Supported while in session <i>Not supported during logon</i>	RemoteFX USB Redirection
PTP Camera	Supported	Plug and Play Device Redirection
MTP Media Player	Supported	Plug and Play Device Redirection
Webcam	Supported (LAN only)	RemoteFX USB Redirection
VoIP Telephone/Headset	Supported (LAN only)	RemoteFX USB Redirection
Audio (not a USB composite device)	Supported	Audio Redirection
CD or DVD Drive	Supported for read operations	Drive Redirection
Hard Drive or USB Flash Drive	Supported	Drive Redirection
Smart Card Reader	Supported	Smart Card Redirection
USB-to-Serial	Supported	RemoteFX USB Redirection
USB Network Adapter (also includes some personal digital assistants)	Blocked	N/A
USB Display	Blocked	N/A
USB Keyboard or Mouse	Supported	Input Redirection

AVX512를 통한 CVM에서의 AI 애플리케이션 가속

최종 업데이트 날짜: : 2024-02-02 11:01:47

작업 시나리오

Tencent Cloud의 6 시리즈 인스턴스 S6, M5, C4, IT5, D3에는 스마트 Intel® Xeon® 2 시리즈 확장 가능 프로세서 Cascade Lake가 탑재되었습니다. 더 많은 명령어 집합 및 특성을 제공하여 AI 애플리케이션 가속에 사용할 수 있습니다. 대량의 하드웨어 강화 기술이 통합되어 있으며, AVX-512(고급 벡터 확장)는 AI 추론 과정에 강력한 병렬 컴퓨팅 기능을 제공하여 보다 향상된 딥러닝 효과를 얻을 수 있습니다.

본 문서는 S5와 M5 인스턴스를 예시로 CVM에서 AVX512를 통해 AI 애플리케이션을 가속화하는 방법을 소개합니다.

권장 모델

CVM의 다양한 인스턴스 사양은 여러 가지 애플리케이션 개발에 사용할 수 있습니다. [표준형 S6](#), [표준형 S5](#) 및 [메모리형 M5](#)는 머신러닝 또는 딥러닝에 적합합니다. 이 인스턴스에는 Intel® Xeon® 2 시리즈 프로세서가 탑재되어 있으며, Intel® DL boost 학습 기능을 적용할 수 있습니다. 권장 사양은 다음과 같습니다.

플랫폼 유형	인스턴스 사양
딥러닝 학습 플랫폼	84vCPU의 표준형 S5 인스턴스 또는 48vCPU의 메모리형 M5 인스턴스
딥러닝 추론 플랫폼	8/16/24/32/48vCPU의 표준형 S5 인스턴스 또는 메모리형 M5 인스턴스
머신러닝 학습 또는 추론 플랫폼	48vCPU의 표준형 S5 인스턴스 또는 24vCPU의 메모리형 M5 인스턴스

장점

Intel® Xeon® 확장 가능 프로세서를 사용한 머신러닝 또는 딥러닝 워크로드 실행에는 다음과 같은 장점이 있습니다. 대규모 메모리형 워크로드, 의료 영상, GAN, 지진 분석, 유전자 시퀀서 등의 시나리오에서 사용하는 3D-CNN 토폴로지 처리에 적합합니다.

간단한 `numactl` 명령어를 사용해 효율적으로 코어를 제어할 수 있으며, 소량의 실시간 추론에도 사용할 수 있습니다.

강력한 생체 시스템 지원으로 대형 클러스터에서 분산형 학습을 직접 진행할 수 있어 별도의 대용량 스토리지와 고가의 캐시 메커니즘 없이 대규모 아키텍처 학습을 진행할 수 있습니다.

동일한 클러스터에서 다수의 워크로드(예: HPC, BigData, AI 등)를 지원하여 더 우수한 TCO를 획득할 수 있습니다.

SIMD 가속을 통해 다양한 실제 딥러닝 응용 프로그램의 컴퓨팅 요구사항을 충족합니다.

동일한 인프라를 직접 학습 및 추론에 사용할 수 있습니다.

작업 순서

인스턴스 생성

CVM 인스턴스 생성에 대한 자세한 내용은 [구매 페이지를 통한 인스턴스 생성](#)을 참고하십시오. 인스턴스 사양은 [권장 모델](#) 및 실제 비즈니스 시나리오에 따라 아래 이미지와 같이 선택하십시오.

Instance	All CPU	Total Mem						
	All Models	Standard	High IO	MEM-optimized	Compute	GPU-based		
	All types	Standard S5 Promo	Standard SA2	Standard S4	Standard Network-opti			
	Standard S2	Standard S1	High IO IT5 NEW	High IO IT3	High IO I3	MEM-optimized		

설명 :

자세한 인스턴스 사양 매개변수의 소개는 [인스턴스 스펙](#)을 참고하십시오.

로그인 인스턴스

CVM 인스턴스에 로그인합니다. 자세한 내용은 [표준 방식으로 Linux 인스턴스에 로그인\(권장\)](#)을 참고하십시오.

배포 예시

실제 비즈니스 시나리오에 따라 다음의 예시를 참고하여 AI 플랫폼을 배포하고, 머신러닝 또는 딥러닝 작업을 진행할 수 있습니다.

예시1: Intel®을 사용해 딥러닝 프레임워크 TensorFlow* 최적화

스마트 Intel® Xeon® 2 시리즈 확장 가능 프로세서 Cascade Lake에서 PyTorch와 IPEX는 자동으로 AVX-512 명령어 집합을 최적화하여 연산 능력을 최대로 높입니다.

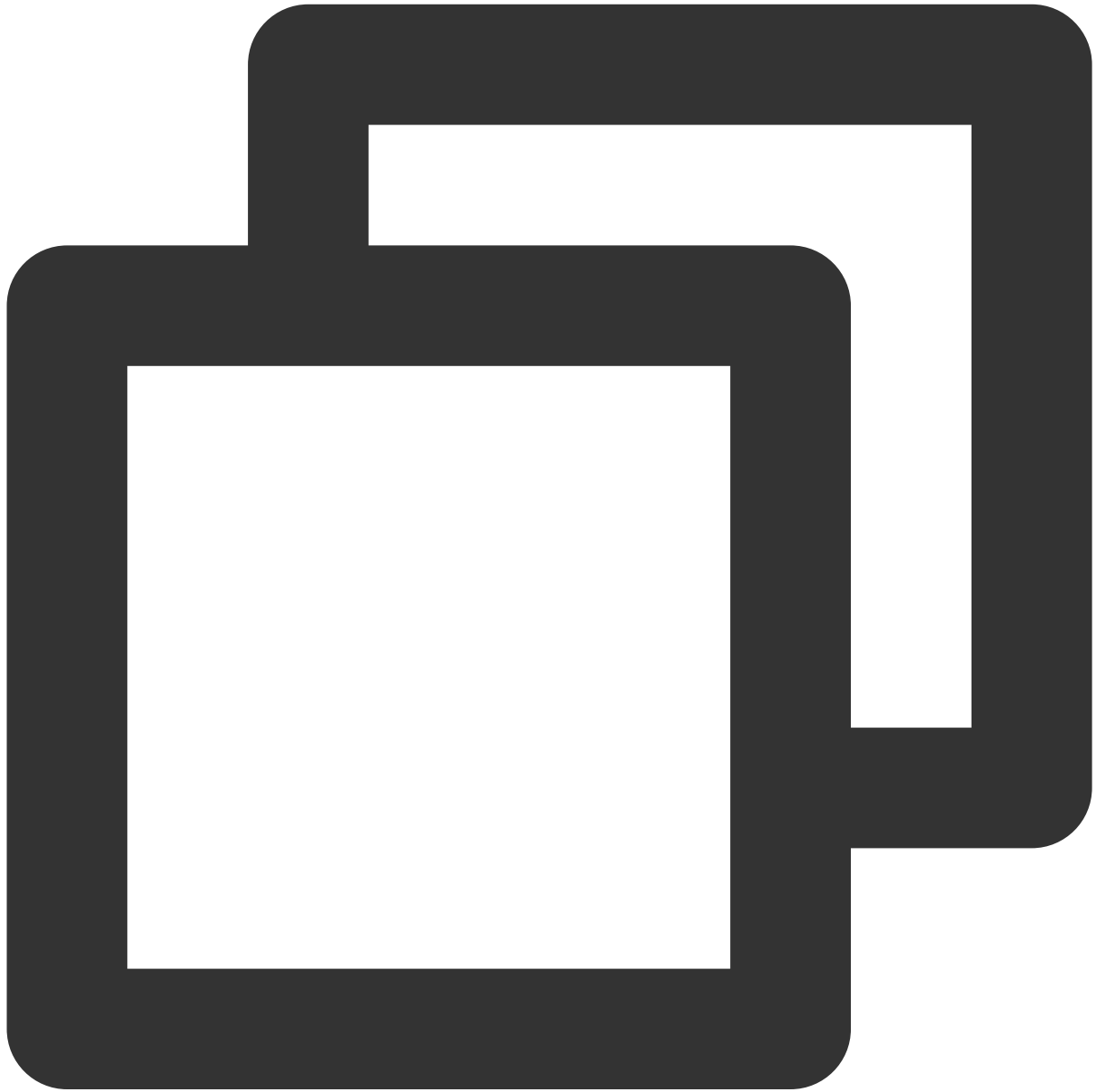
TensorFlow*는 대규모 머신러닝 및 딥러닝에 사용되는 인기 프레임워크 중 하나입니다. 해당 예시를 참고하여 인스턴스의 학습 능력과 추론 능력을 높일 수 있습니다. 프레임워크 배포에 대한 자세한 정보는 [Intel® Optimization for TensorFlow* Installation Guide](#)를 참고하십시오. 작업 순서는 다음과 같습니다.

TensorFlow* 프레임워크 배포

1. CVM에 Python을 설치합니다. 본 문서는 Python 3.7을 예시로 합니다.
2. 다음 명령어를 실행하여 Intel®에 최적화된 TensorFlow* 버전인 intel-tensorflow를 설치합니다.

설명 :

최신 기능 획득 및 최적화를 위해 **2.4.0 이상 버전** 사용을 권장합니다.



```
pip install intel-tensorflow
```

실행 시 매개변수 최적화 설정

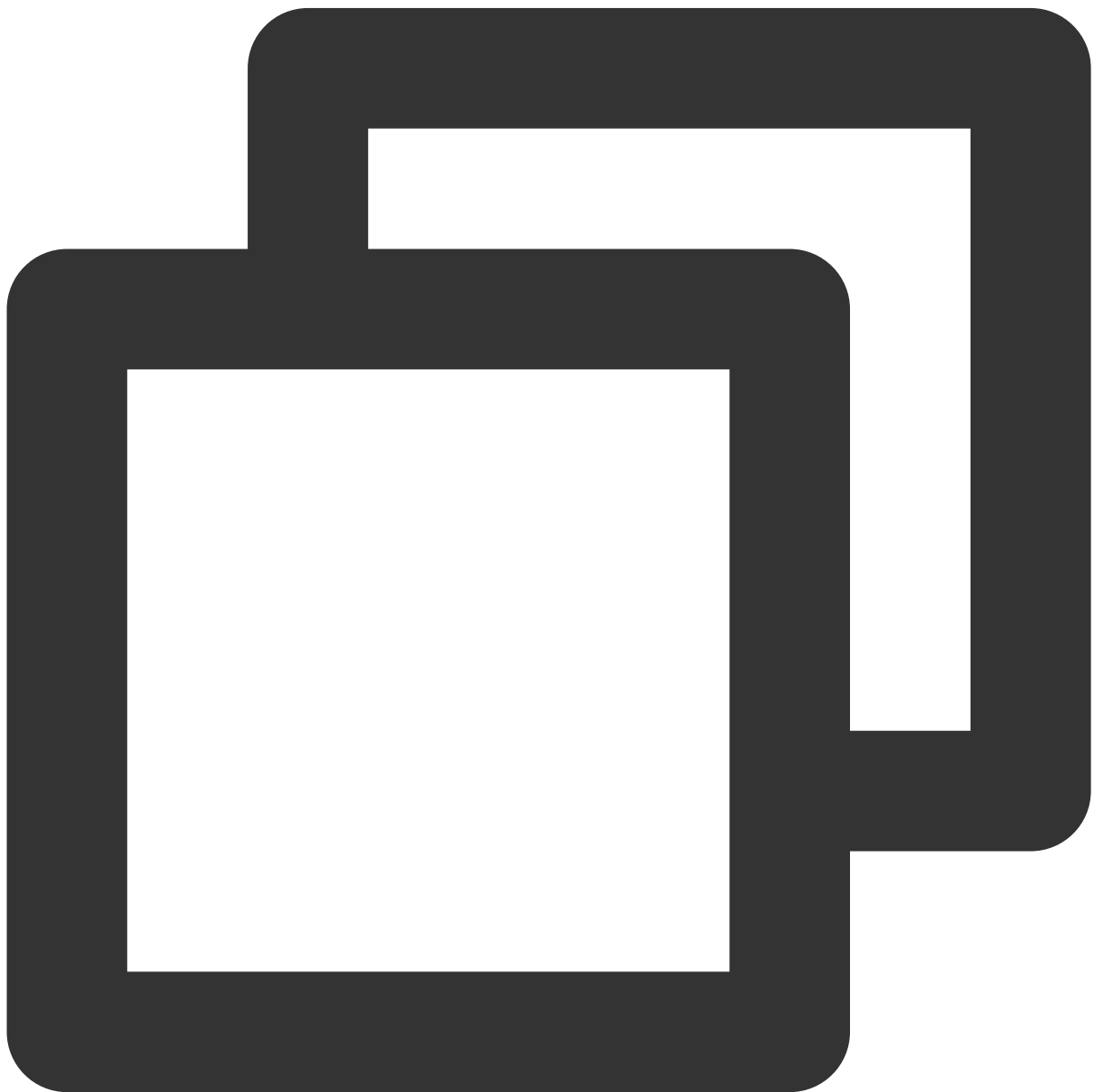
실행 시 매개변수 최적화 방식을 선택합니다. 일반적으로 다음 두 가지 실행 인터페이스를 사용하여 서로 다른 최적화 설정을 채택합니다. 실제 필요에 따라 선택할 수 있습니다. 매개변수 최적화 설정에 대한 자세한 설명은 [General Best Practices for Intel® Optimization for TensorFlow](#)를 참고하십시오.

Batch inference: BatchSize > 1로 설정하고, 초당 처리 가능한 입력 텐서의 총수를 측정합니다. 일반적으로 Batch Inference 방식은 동일한 CPU socket의 모든 물리 코어를 사용해 최적의 성능을 구현합니다.

On-line Inference(실시간 추론): BS = 1로 설정하고, 단일 입력 텐서(배치 1개의 크기는 1) 처리에 소요되는 시간을 측정합니다. 실시간 추론 방식은 여러 인스턴스의 동시 실행을 통해 최적의 처리량을 구현합니다.

작업 순서는 다음과 같습니다.

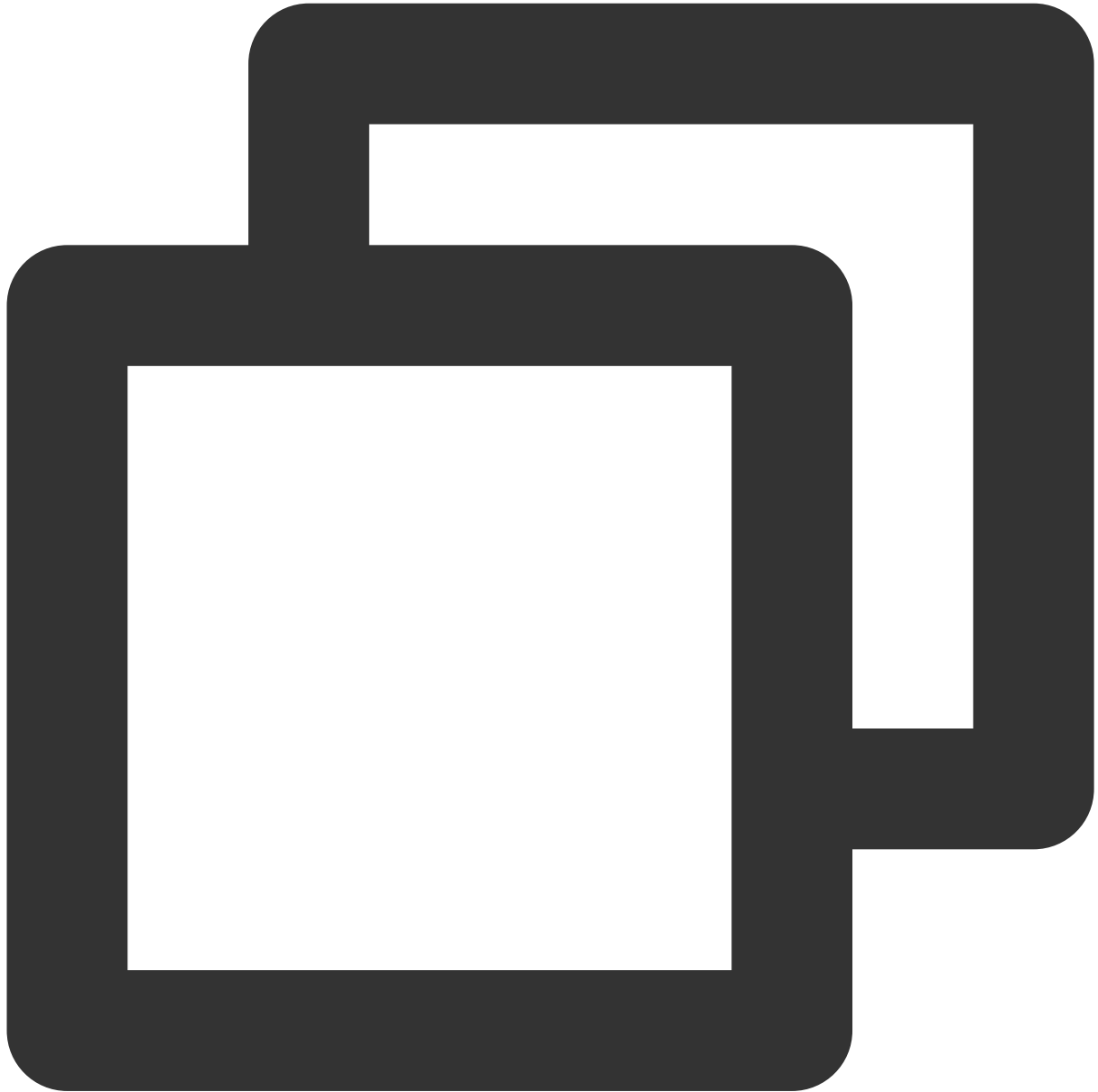
1. 다음 명령어를 실행하여 시스템의 물리 코어 개수를 확인합니다.



```
lscpu | grep "Core(s) per socket" | cut -d':' -f2 | xargs
```

2. 최적화 매개변수를 설정합니다. 다음 방식 중 한 가지를 선택할 수 있습니다.

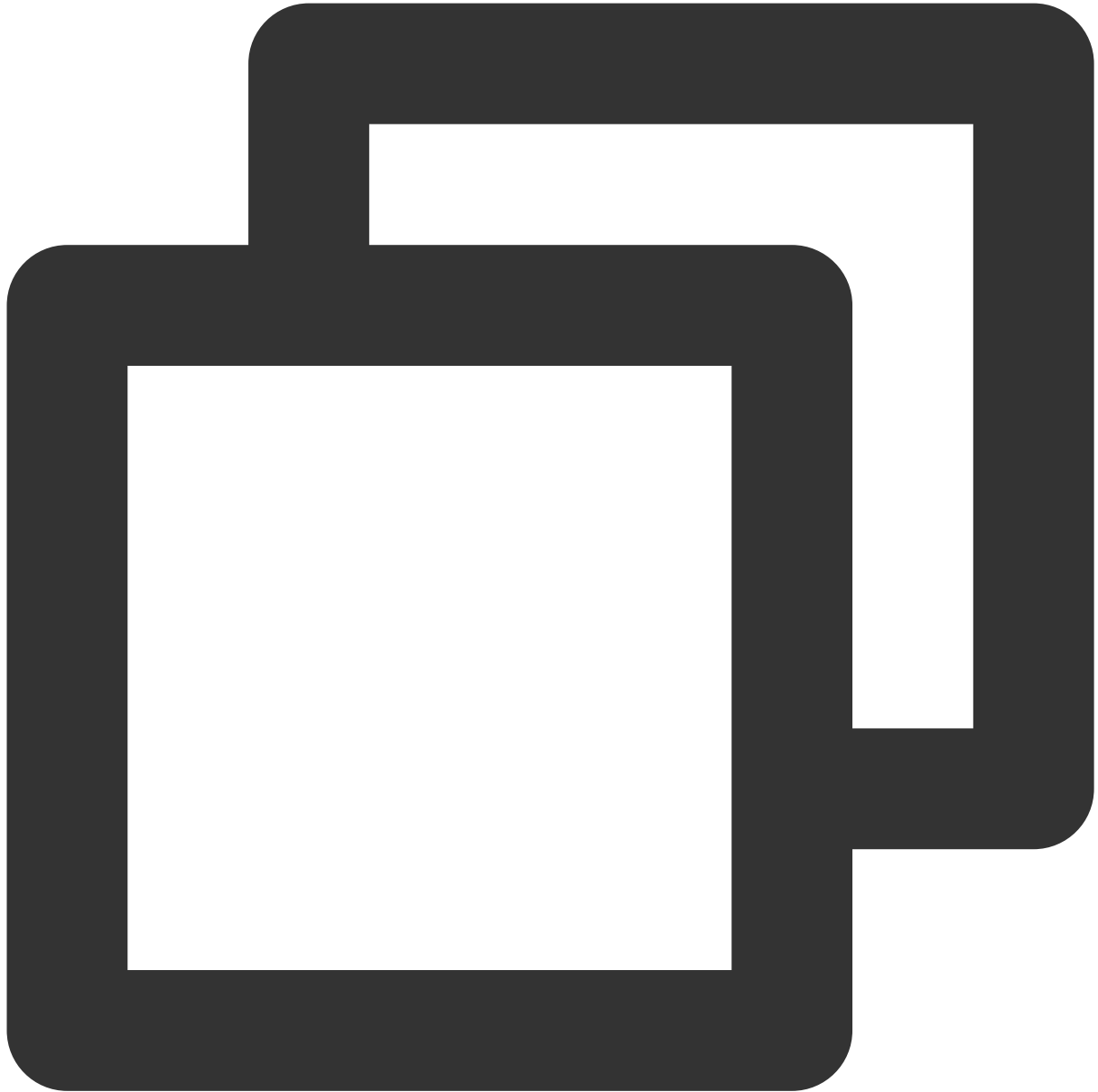
환경 실행 매개변수를 설정합니다. 환경 변수 파일에 다음 설정을 추가합니다.



```
export OMP_NUM_THREADS= # <physicalcores>
export KMP_AFFINITY="granularity=fine,verbose,compact,1,0"
export KMP_BLOCKTIME=1
export KMP_SETTINGS=1
export TF_NUM_INTRAOP_THREADS= # <physicalcores>
export TF_NUM_INTEROP_THREADS=1
```

```
export TF_ENABLE_MKL_NATIVE_FORMAT=0
```

코드에 환경 변수 설정을 추가합니다. 실행 중인 Python 코드에 다음의 환경 변수 설정을 추가합니다.



```
import os
os.environ["KMP_BLOCKTIME"] = "1"
os.environ["KMP_SETTINGS"] = "1"
os.environ["KMP_AFFINITY"] = "granularity=fine,verbose,compact,1,0"
if FLAGS.num_intra_threads > 0:
    os.environ["OMP_NUM_THREADS"] = # <physical cores>
os.environ["TF_ENABLE_MKL_NATIVE_FORMAT"] = "0"
config = tf.ConfigProto()
```

```
config.intra_op_parallelism_threads = # <physical cores>
config.inter_op_parallelism_threads = 1
tf.Session(config=config)
```

TensorFlow* 딥러닝 모델의 추론 실행

[Image Recognition with ResNet50, ResNet101 and InceptionV3](#)를 참고하여 기타 머신러닝/딥러닝 모델의 추론을 실행할 수 있습니다. 본 문서는 benchmark를 예시로 ResNet50의 inference benchmark를 실행하는 방법을 소개합니다. 자세한 내용은 [ResNet50 \(v1.5\)](#)을 참고하십시오.

TensorFlow* 딥러닝 모델의 학습 실행

본 문서는 ResNet50의 training benchmark를 실행하는 방법을 소개합니다. 자세한 내용은 [FP32 Training Instructions](#)를 참고하십시오.

TensorFlow 성능 안내

성능 데이터는 [Improving TensorFlow* Inference Performance on Intel® Xeon® Processors](#)를 참고하십시오. 실제 모드 및 물리 설정에 따라 성능 데이터에 차이가 있을 수 있습니다. 다음 성능 데이터는 참고용입니다.

딜레이 성능:

batch size가 1일 때 이미지 분류, 타깃 검증에 사용하는 일부 모델을 선별하여 테스트를 진행하면, AVX512 최적화 버전이 제공하는 추론 성능이 최적화하지 않은 버전보다 뚜렷하게 향상된 것을 확인할 수 있습니다. 예를 들어, 딜레이 성능을 최적화한 ResNet 50의 딜레이는 기존 대비 45% 낮아집니다.

처리량 성능:

batch size를 확대 설정해 처리량 성능을 테스트할 수 있습니다. 이미지 분류, 타깃 검증에 사용하는 일부 모델을 선별하여 테스트를 진행하면, 처리량 성능 데이터가 뚜렷하게 향상된 것을 확인할 수 있습니다. 최적화한 ResNet 50의 성능은 기존 대비 1.98배 향상됩니다.

예시2: 딥러닝 프레임워크 PyTorch* 배포

설치 순서

1. CVM에 Python3.6 이상의 버전을 설치합니다. 본 문서는 Python 3.7을 예시로 합니다.
2. [Intel® Extension for PyTorch 공식 홈페이지 github repo](#)의 설치 가이드에서 제공하는 정보에 따라 PyTorch 및 Intel® Extension for PyTorch(IPEX)를 컴파일 및 설치합니다.

실행 시 매개변수 최적화 설정

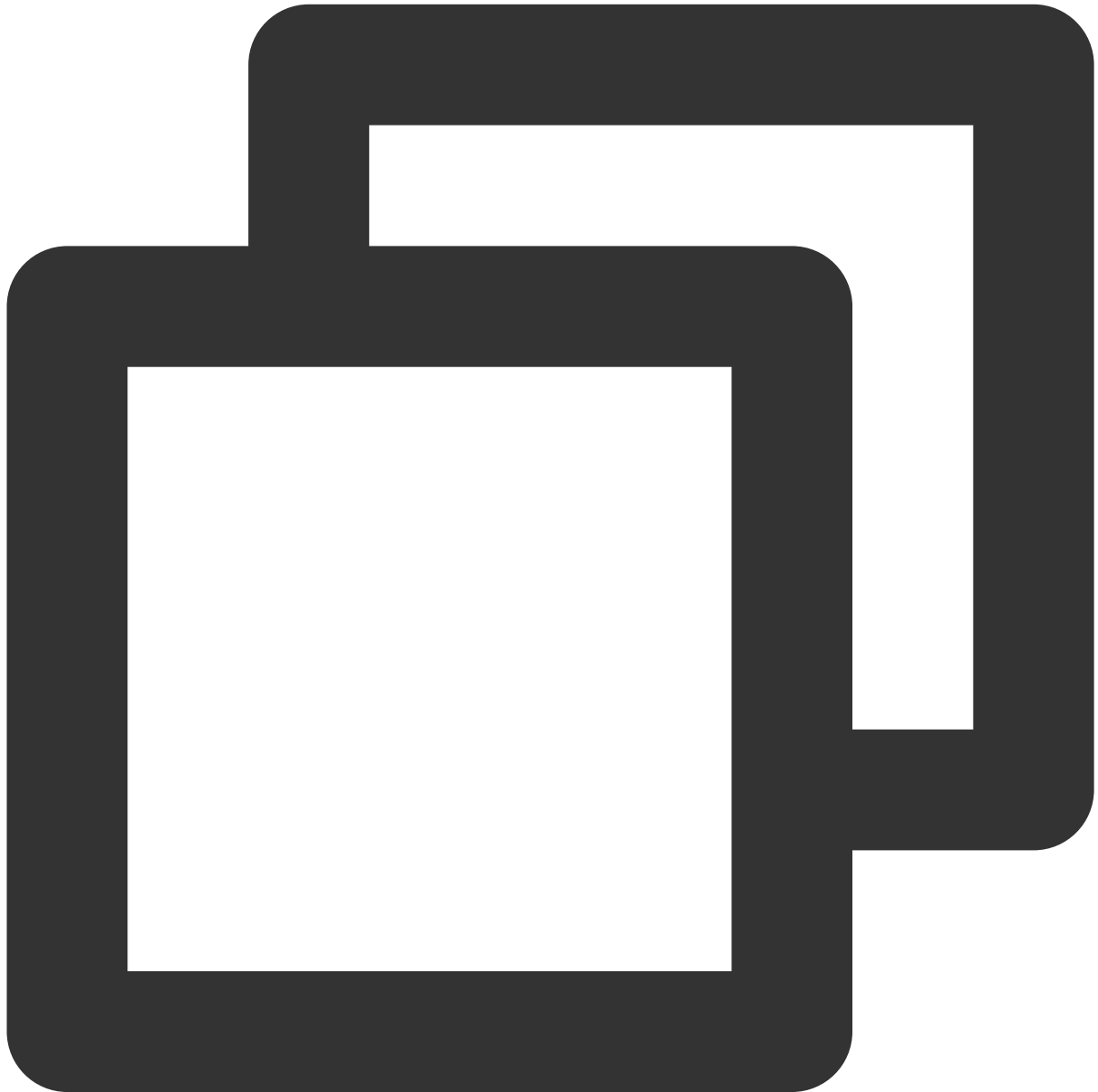
스마트 Intel® Xeon® 2 시리즈 확장 가능 프로세서 Cascade Lake에서 PyTorch와 IPEX는 자동으로 AVX-512 명령어 집합을 최적화하여 연산 능력을 최대로 높입니다.

이 단계에 따라 실행 시 매개변수 최적화 방식을 설정할 수 있습니다. 매개변수 최적화 설정에 대한 자세한 설명은 [Maximize Performance of Intel® Software Optimization for PyTorch* on CPU](#)를 참고하십시오.

Batch inference: BatchSize > 1로 설정하고, 초당 처리 가능한 입력 텐서의 총수를 측정합니다. 일반적으로 Batch Inference 방식은 동일한 CPU socket의 모든 물리 코어를 사용해 최적의 성능을 구현합니다.

On-line Inference(실시간 추론): BatchSize = 1로 설정하고, 단일 입력 텐서(배치 1개의 크기는 1) 처리에 소요되는 시간을 측정합니다. 실시간 추론 방식은 여러 인스턴스의 동시 실행을 통해 최적의 처리량을 구현합니다. 작업 순서는 다음과 같습니다.

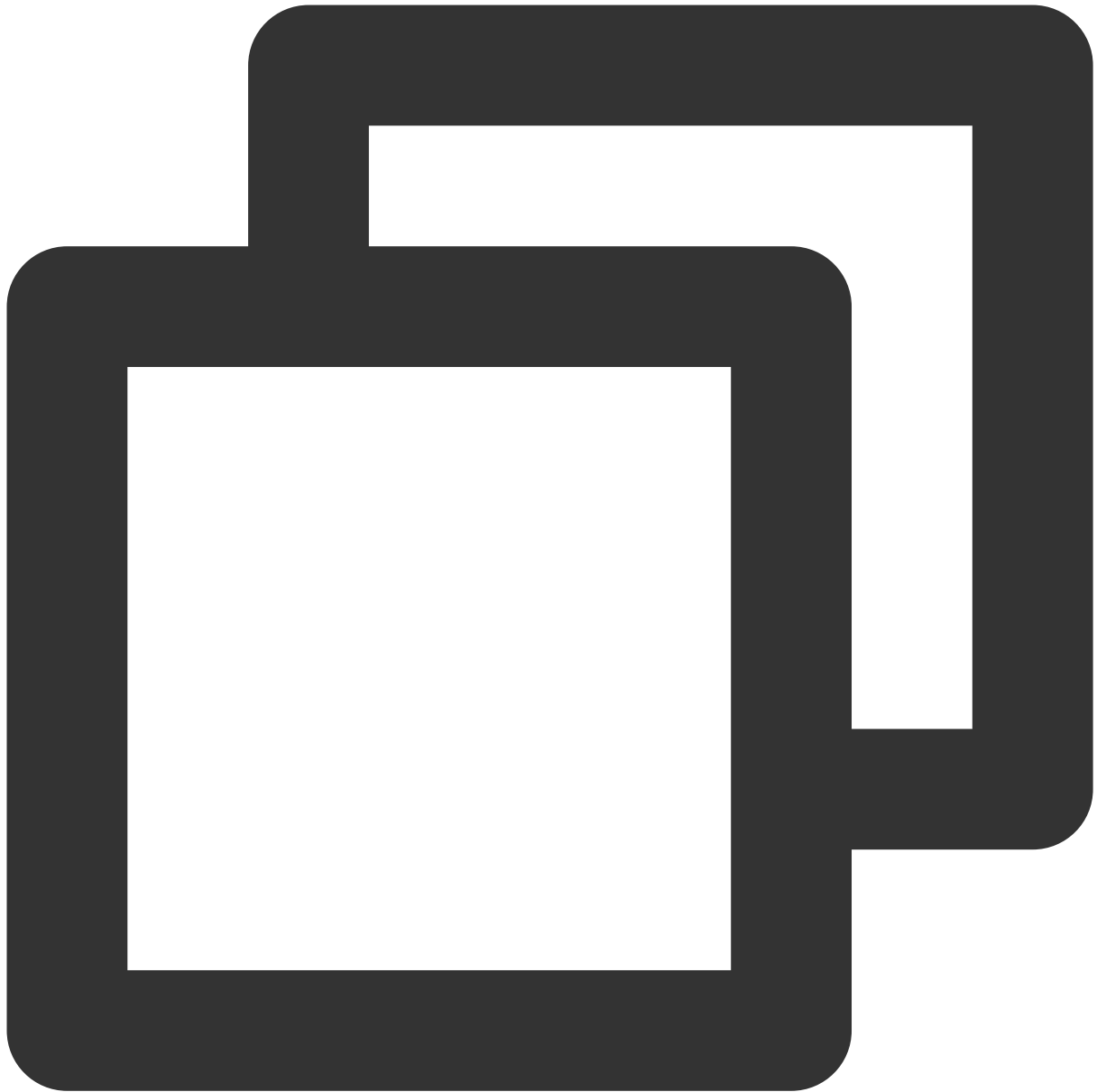
1. 다음 명령어를 실행하여 시스템의 물리 코어 개수를 확인합니다.



```
lscpu | grep "Core(s) per socket" | cut -d':' -f2 | xargs
```

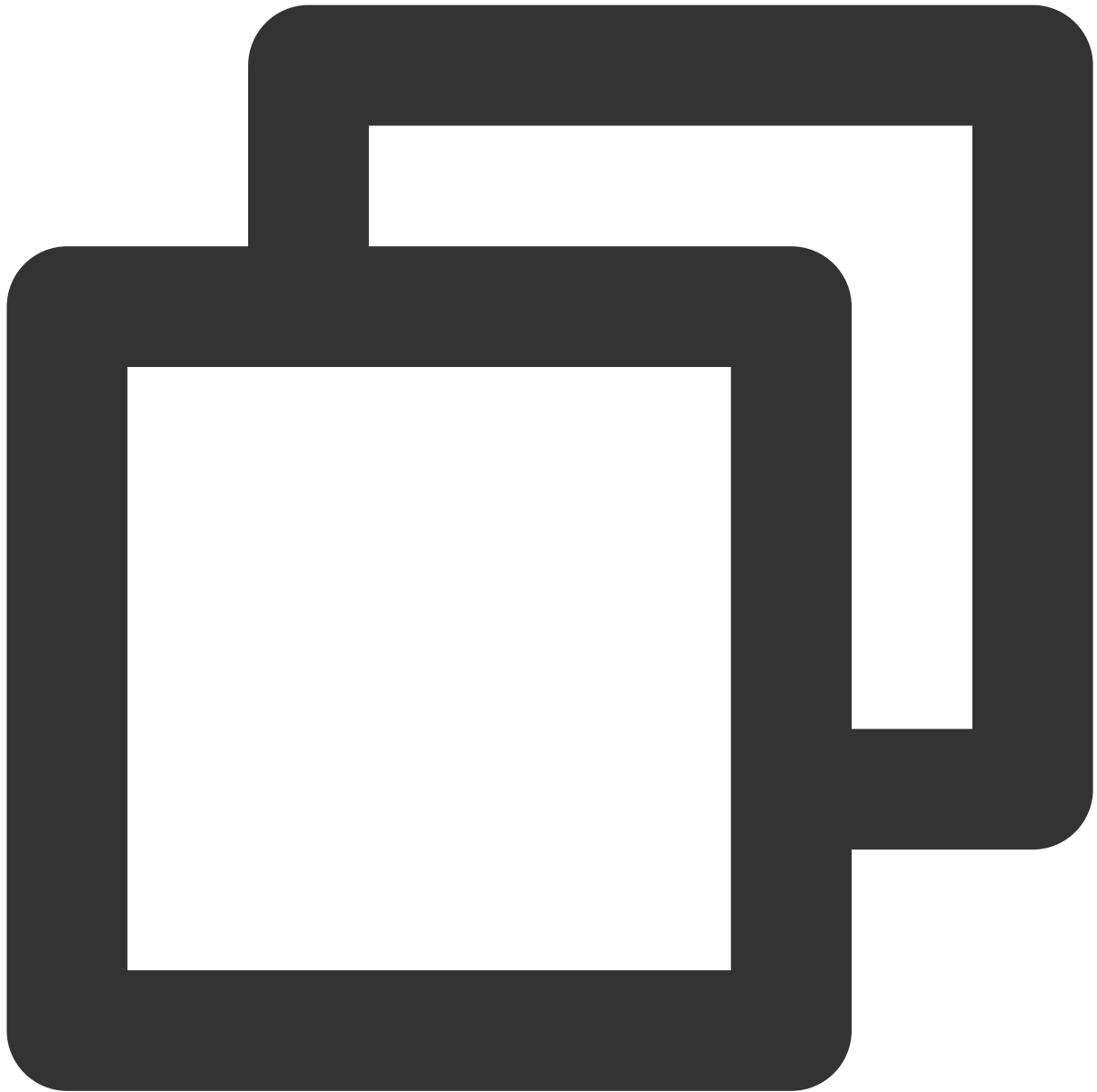
2. 최적화 매개변수를 설정합니다. 다음 방식 중 한 가지를 선택할 수 있습니다.

환경 실행 매개변수를 설정하고, GNU OpenMP* Libraries를 사용합니다. 환경 변수 파일에 다음 설정을 추가합니다.



```
export OMP_NUM_THREADS=physicalcores
export GOMP_CPU_AFFINITY="0-<physicalcores-1>"
export OMP_SCHEDULE=STATIC
export OMP_PROC_BIND=CLOSE
```

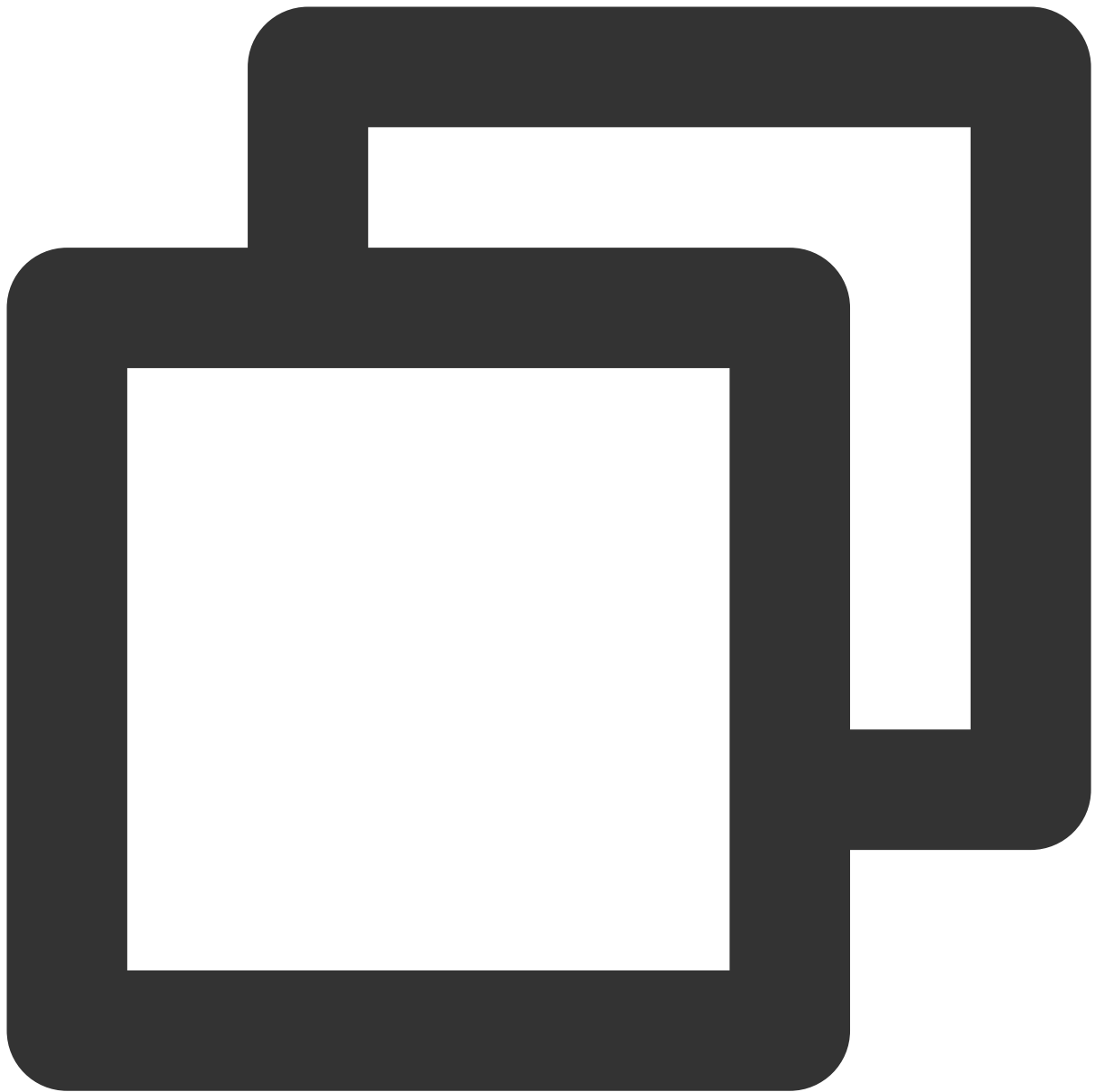
환경 실행 매개변수를 설정하고, Intel OpenMP* Libraries를 사용합니다. 환경 변수 파일에 다음 설정을 추가합니다.



```
export OMP_NUM_THREADS=physicalcores
export LD_PRELOAD=<path_to_libiomp5.so>
export KMP_AFFINITY="granularity=fine,verbose,compact,1,0"
export KMP_BLOCKTIME=1
export KMP_SETTINGS=1
```

PyTorch* 딥러닝 모델의 추론 및 학습 최적화 실행에 대한 권장사항

모델 추론 실행 시 Intel® Extension for PyTorch를 사용해 성능을 높일 수 있습니다. 예시 코드는 다음과 같습니다.



```
import intel_pytorch_extension
...
net = net.to('xpu')          # Move model to IPEX format
data = data.to('xpu')        # Move data to IPEX format
...
output = net(data)           # Perform inference with IPEX
output = output.to('cpu')    # Move output back to ATen format
```

추론 및 학습 성능은 `jemalloc`을 사용하여 최적화할 수 있습니다. `jemalloc`은 범용 `malloc(3)`으로 구현되며, 시스템에 메모리 할당자 제공을 위해 파편화 방지 및 확장 가능한 동시 지원을 강조합니다. `jemalloc`은 표준 할당자 기능을

뛰어넘는 여러 가지 자가 점검, 메모리 관리 및 조절 기능을 제공합니다. 자세한 내용은 [jemalloc](#) 및 [예시 코드](#)를 참고하십시오.

여러 socket의 분산형 학습에 대한 자세한 내용은 [PSSP-Transformer의 분산형 CPU 학습 스크립트](#)를 참고하십시오.

성능 결과

인텔의 Intel® Xeon® 2 시리즈 확장 가능 프로세서 Cascade Lake를 기반으로 한 2*CPU(28코어/CPU) 및 384G 메모리 시나리오에서 각 모델의 성능 테스트 데이터는 [성능 테스트 데이터](#)를 참고하십시오. 실제 모델 및 물리적 설정에 따라 성능 데이터에 차이가 있을 수 있으며, 본 문서에서 제공하는 테스트 데이터는 참고용입니다.

예시3: Intel® AI 저정밀 최적화 툴을 사용한 가속

Intel® 저정밀 최적화 툴은 오픈 소스 Python 라이브러리이며, 간단하고 편리하며 신경망 프레임워크 간의 저정밀 양자화 추론 인터페이스를 제공합니다. 해당 인터페이스를 간편하게 호출하여 모델 양자화로 생산성을 높이고, 3 시리즈 Intel® Xeon® DL Boost 확장 가능 프로세서 플랫폼에서 저정밀 모델의 추론 성능을 가속화합니다. 사용 방법에 대한 자세한 내용은 [Intel® 저정밀 양자화 툴 코드 리포지토리](#)를 참고하십시오.

지원하는 신경망 프레임워크 버전

Intel® 저정밀 최적화 툴 지원:

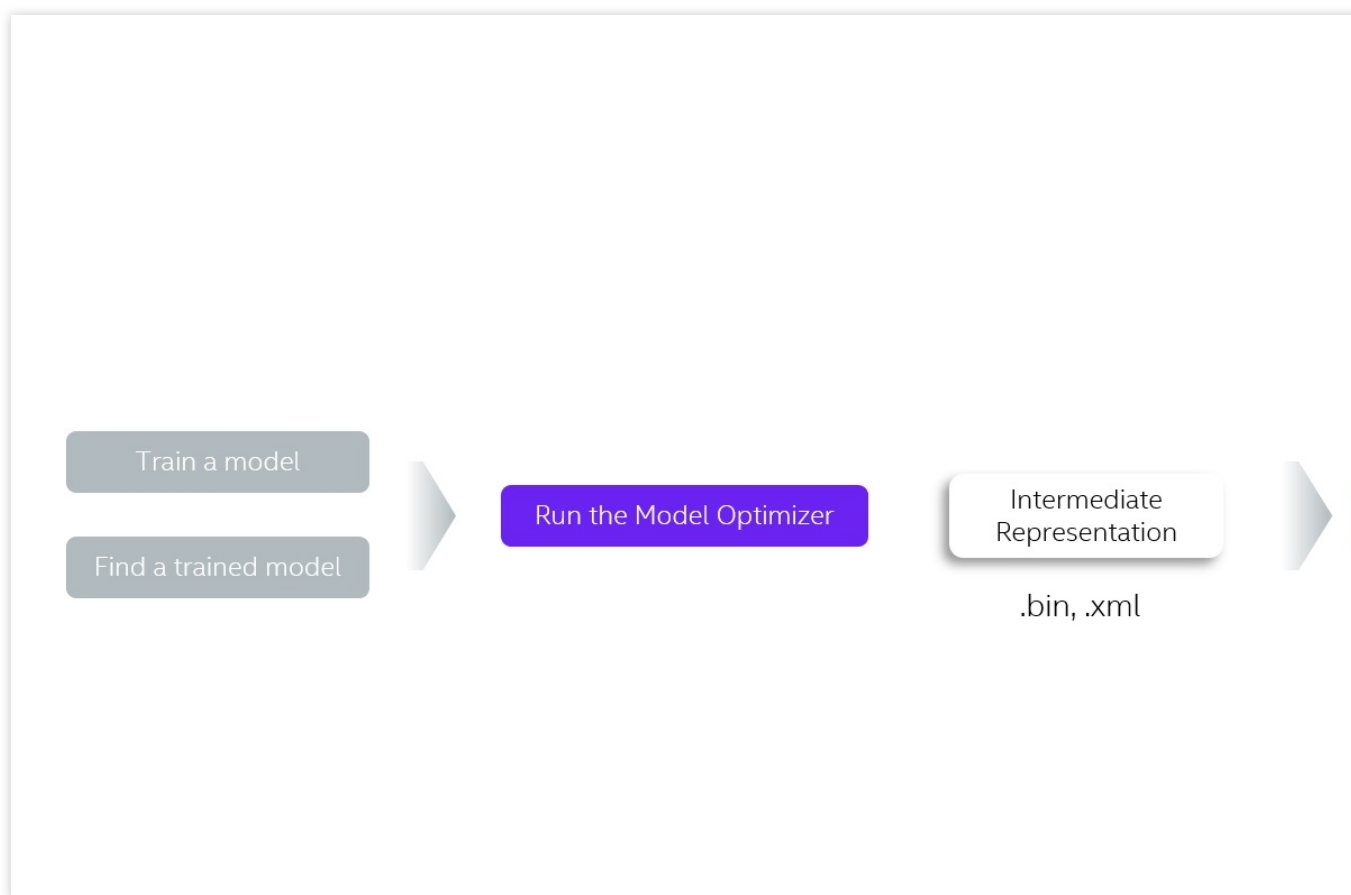
Intel®에 최적화된 TensorFlow* `v1.15.0` , `v1.15.0up1` , `v1.15.0up2` , `v2.0.0` , `v2.1.0` , `v2.2.0` , `v2.3.0` , `v2.4.0` .

Intel®에 최적화된 PyTorch `v1.5.0+cpu` , `v1.6.0+cpu`

Intel®에 최적화된 MXNet `v1.6.0` , `v1.7.0` 및 ONNX-Runtime `v1.6.0`

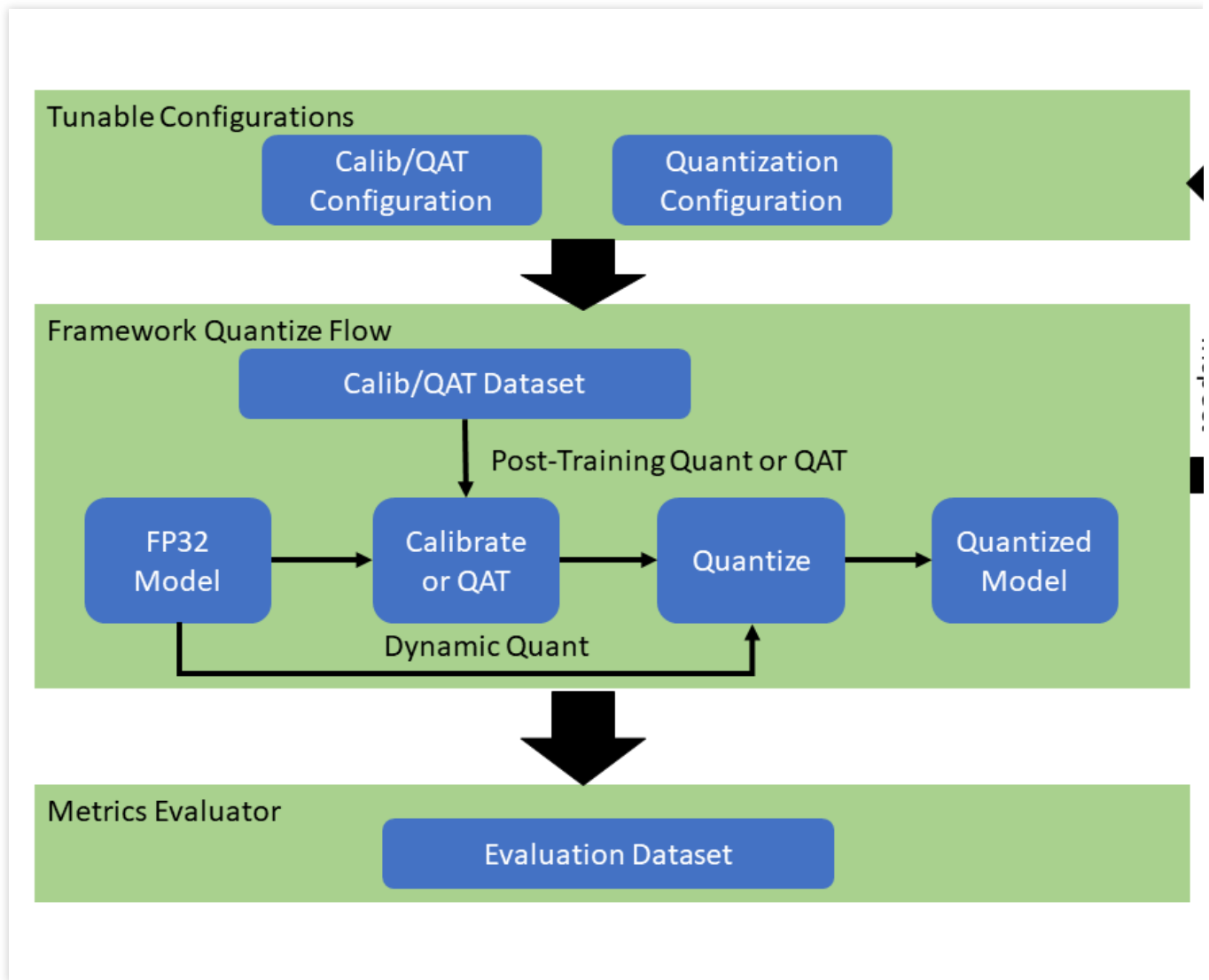
프레임워크 구현

Intel® 저정밀 최적화 툴을 사용한 프레임워크 구현 순서도는 다음과 같습니다.



워크플로

Intel® 저정밀 최적화 툴의 워크플로 순서도는 다음과 같습니다.



양자화 모델 성능 및 정밀도 예시

인텔의 Intel® Xeon® 2 시리즈 확장 가능 프로세서 Cascade Lake에서 일부 Intel® 저정밀 최적화 툴 양자화 모델의 성능 및 정밀도는 다음과 같습니다.

Framework	Version	Model	Accuracy			Performance speed up
			INT8 Tuning Accuracy	FP32 Accuracy Baseline	Acc Ratio [(INT8-FP32)/FP32]	Realtime Latency Ratio[FP32/INT8]
tensorflow	2.4.0	resnet50v1.5	76.92%	76.46%	0.60%	3.37x
tensorflow	2.4.0	resnet101	77.18%	76.45%	0.95%	2.53x
tensorflow	2.4.0	inception_v1	70.41%	69.74%	0.96%	1.89x

tensorflow	2.4.0	inception_v2	74.36%	73.97%	0.53%	1.95x
tensorflow	2.4.0	inception_v3	77.28%	76.75%	0.69%	2.37x
tensorflow	2.4.0	inception_v4	80.39%	80.27%	0.15%	2.60x
tensorflow	2.4.0	inception_resnet_v2	80.38%	80.40%	-0.02%	1.98x
tensorflow	2.4.0	mobilenetv1	73.29%	70.96%	3.28%	2.93x
tensorflow	2.4.0	ssd_resnet50_v1	37.98%	38.00%	-0.05%	2.99x
tensorflow	2.4.0	mask_rcnn_inception_v2	28.62%	28.73%	-0.38%	2.96x
tensorflow	2.4.0	vgg16	72.11%	70.89%	1.72%	3.76x
tensorflow	2.4.0	vgg19	72.36%	71.01%	1.90%	3.85x

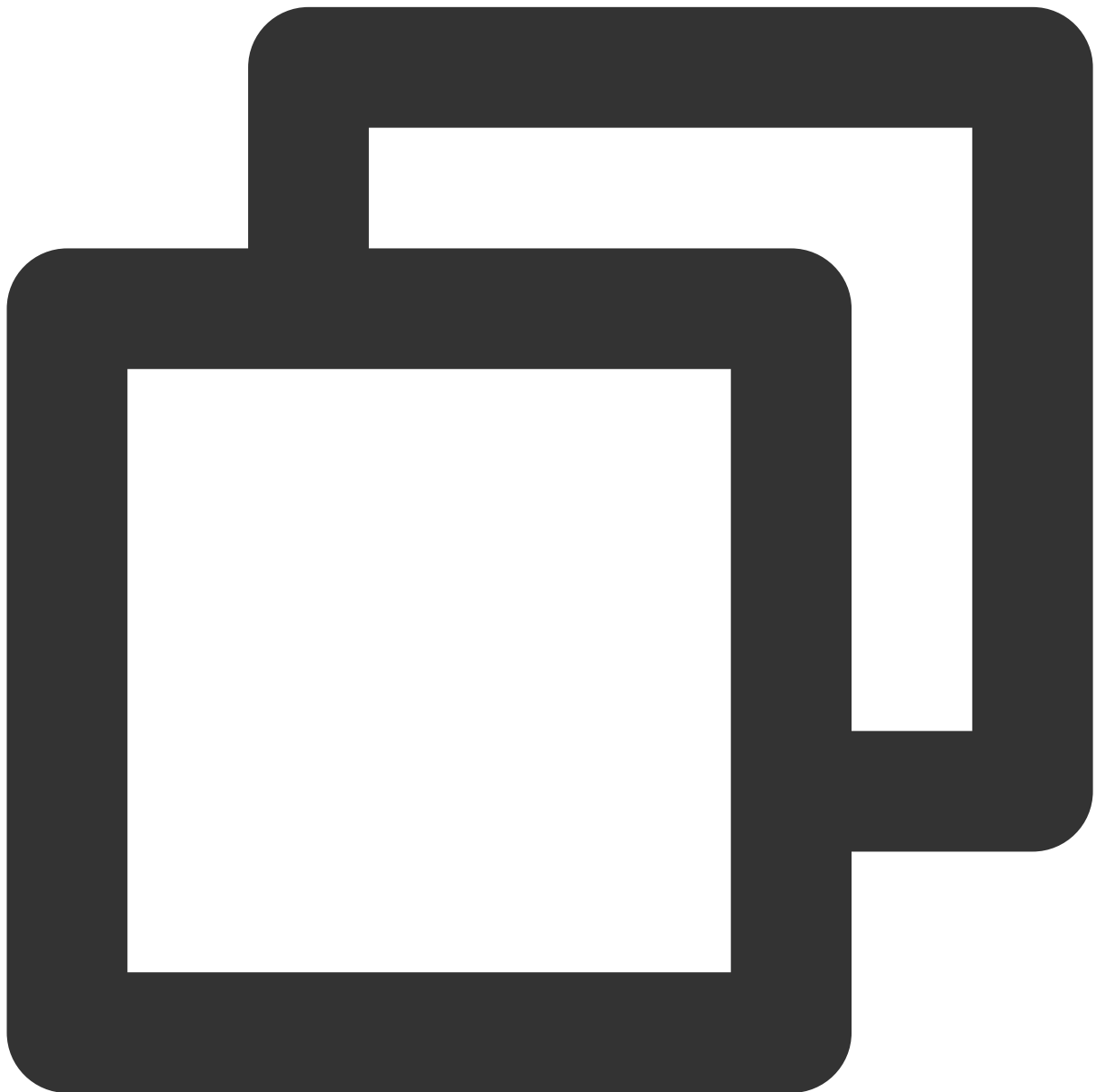
Framework	Version	Model	Accuracy			Performance speed up
			INT8 Tuning Accuracy	FP32 Accuracy Baseline	Acc Ratio [(INT8-FP32)/FP32]	Realtime Ratio[FP
pytorch	1.5.0+cpu	resnet50	75.96%	76.13%	-0.23%	2.46x
pytorch	1.5.0+cpu	resnext101_32x8d	79.12%	79.31%	-0.24%	2.63x
pytorch	1.6.0a0+24aac32	bert_base_mrpc	88.90%	88.73%	0.19%	2.10x
pytorch	1.6.0a0+24aac32	bert_base_cola	59.06%	58.84%	0.37%	2.23x
pytorch	1.6.0a0+24aac32	bert_base_sts-b	88.40%	89.27%	-0.97%	2.13x
pytorch	1.6.0a0+24aac32	bert_base_sst-2	91.51%	91.86%	-0.37%	2.32x
pytorch	1.6.0a0+24aac32	bert_base_rte	69.31%	69.68%	-0.52%	2.03x
pytorch	1.6.0a0+24aac32	bert_large_mrpc	87.45%	88.33%	-0.99%	2.65x
pytorch	1.6.0a0+24aac32	bert_large_squad	92.85	93.05	-0.21%	1.92x
pytorch	1.6.0a0+24aac32	bert_large_qnli	91.20%	91.82%	-0.68%	2.59x
pytorch	1.6.0a0+24aac32	bert_large_rte	71.84%	72.56%	-0.99%	1.34x
pytorch	1.6.0a0+24aac32	bert_large_cola	62.74%	62.57%	0.27%	2.67x

설명 :

표에서 PyTorch와 Tensorflow는 모두 Intel에 최적화된 프레임워크 기반입니다. 지원되는 양자화 모델의 전체 리스트는 [온라인 문서](#)를 참고하십시오.

Intel® 저정밀 최적화 툴 설치 및 사용 예시

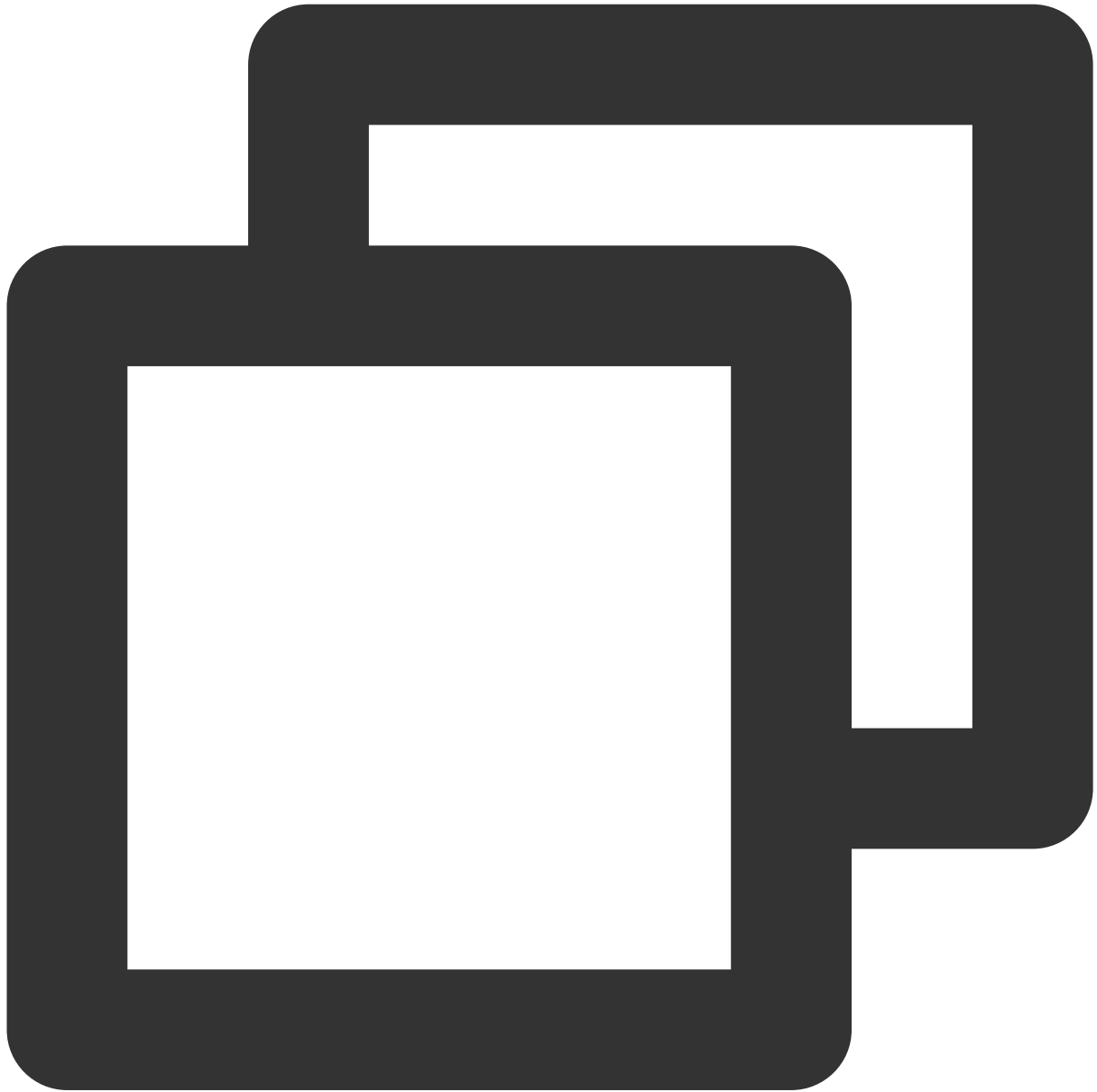
1. 순서에 따라 다음 명령어를 실행하고, anaconda를 사용해 lpot라는 이름의 python3.x 가상 환경을 구축합니다. 본 문서는 python 3.7을 예시로 합니다.



```
conda create -n lpot python=3.7
conda activate lpot
```

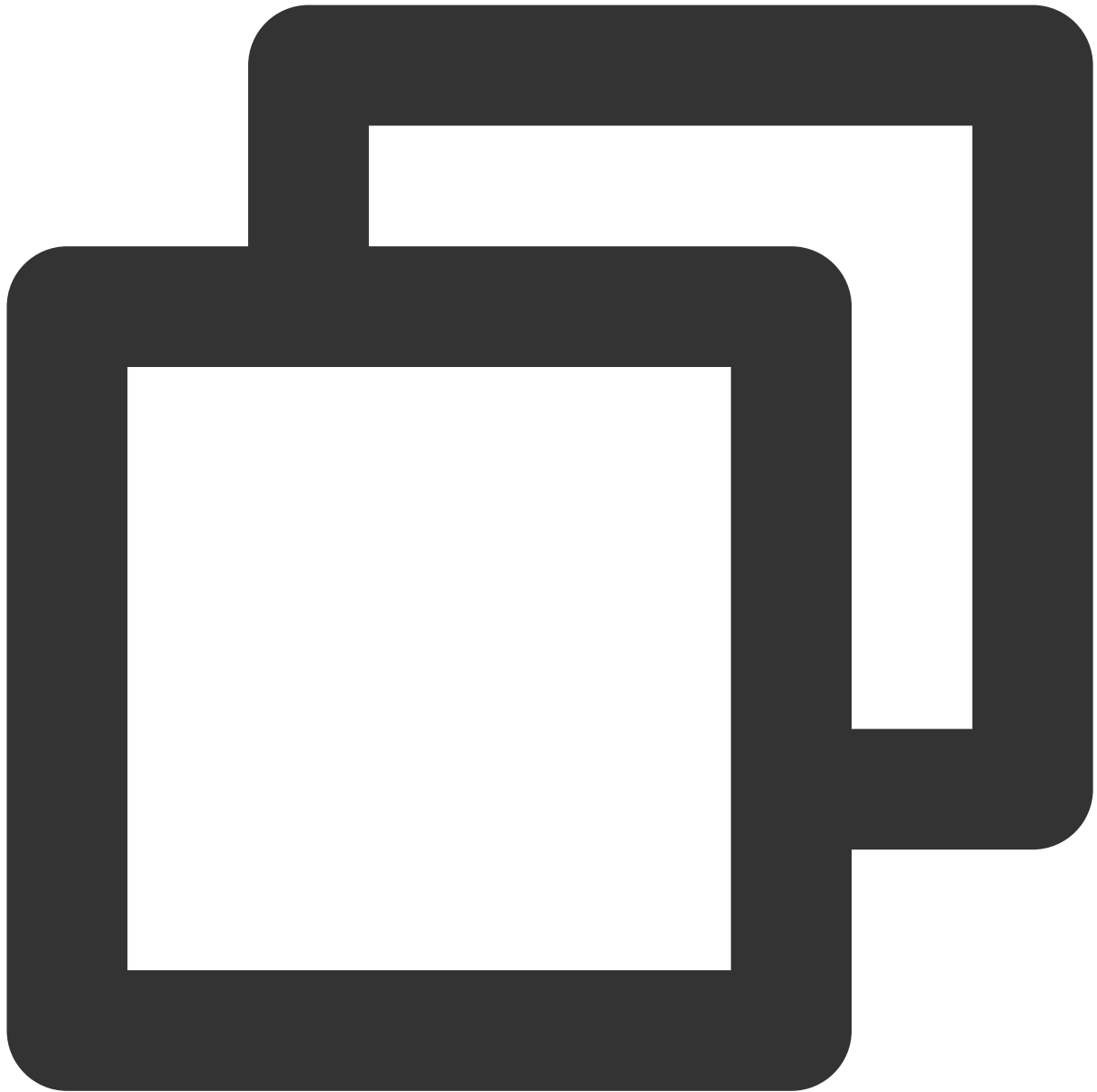
2. lpot를 설치합니다. 다음 두 가지 방식으로 설치할 수 있습니다.

다음 명령어를 실행하여 바이너리 파일에서 설치합니다.



```
pip install lpot
```

다음 명령어를 실행하여 소스 코드에서 설치합니다.

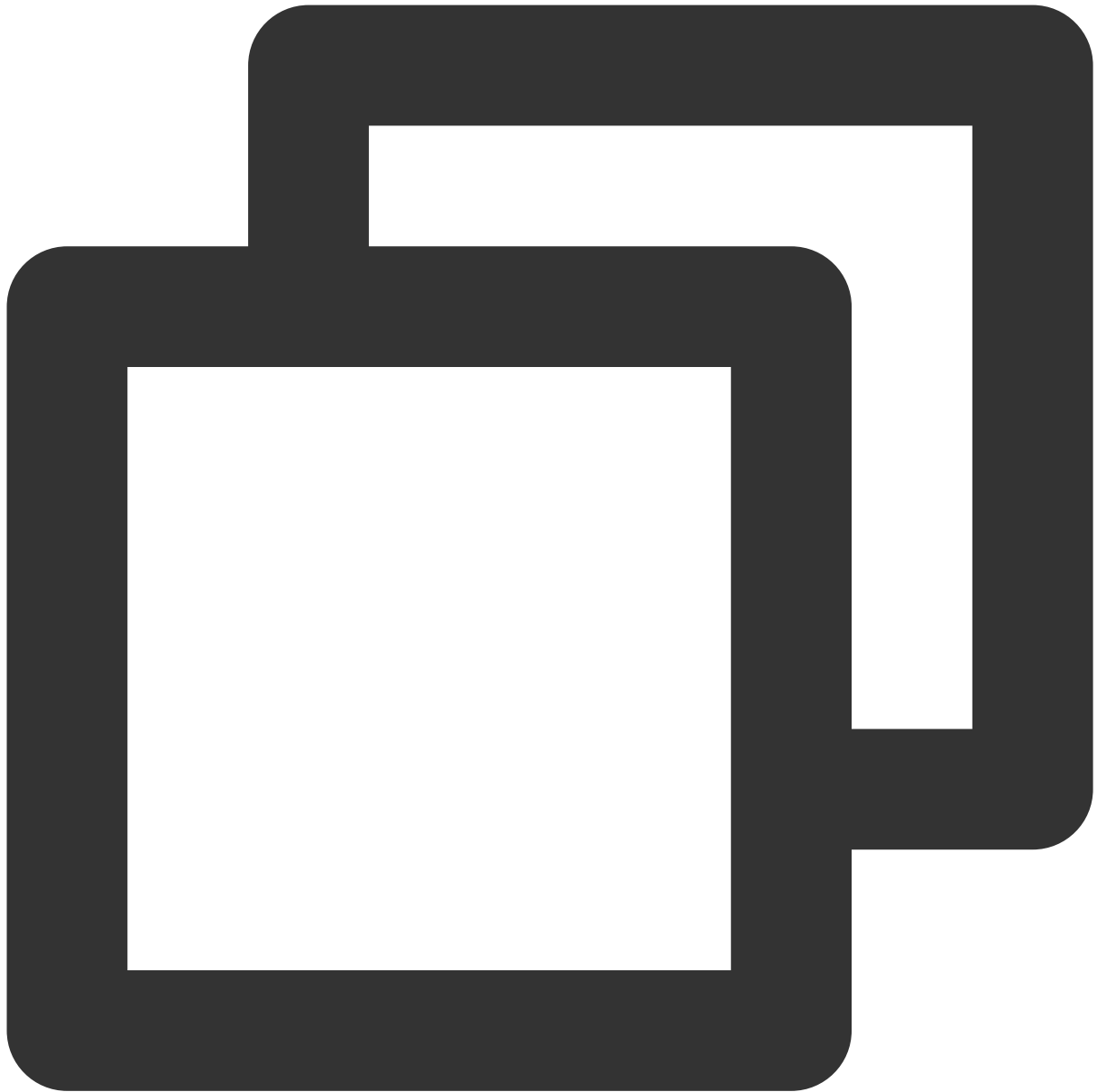


```
git clone https://github.com/intel/lpot.git
cd lpot
pip install -r requirements.txt
python setup.py install
```

3. TensorFlow ResNet50 v1.0를 양자화합니다. 본 문서는 ResNet50 v1.0을 예시로 해당 툴을 사용해 양자화하는 방법을 소개합니다.

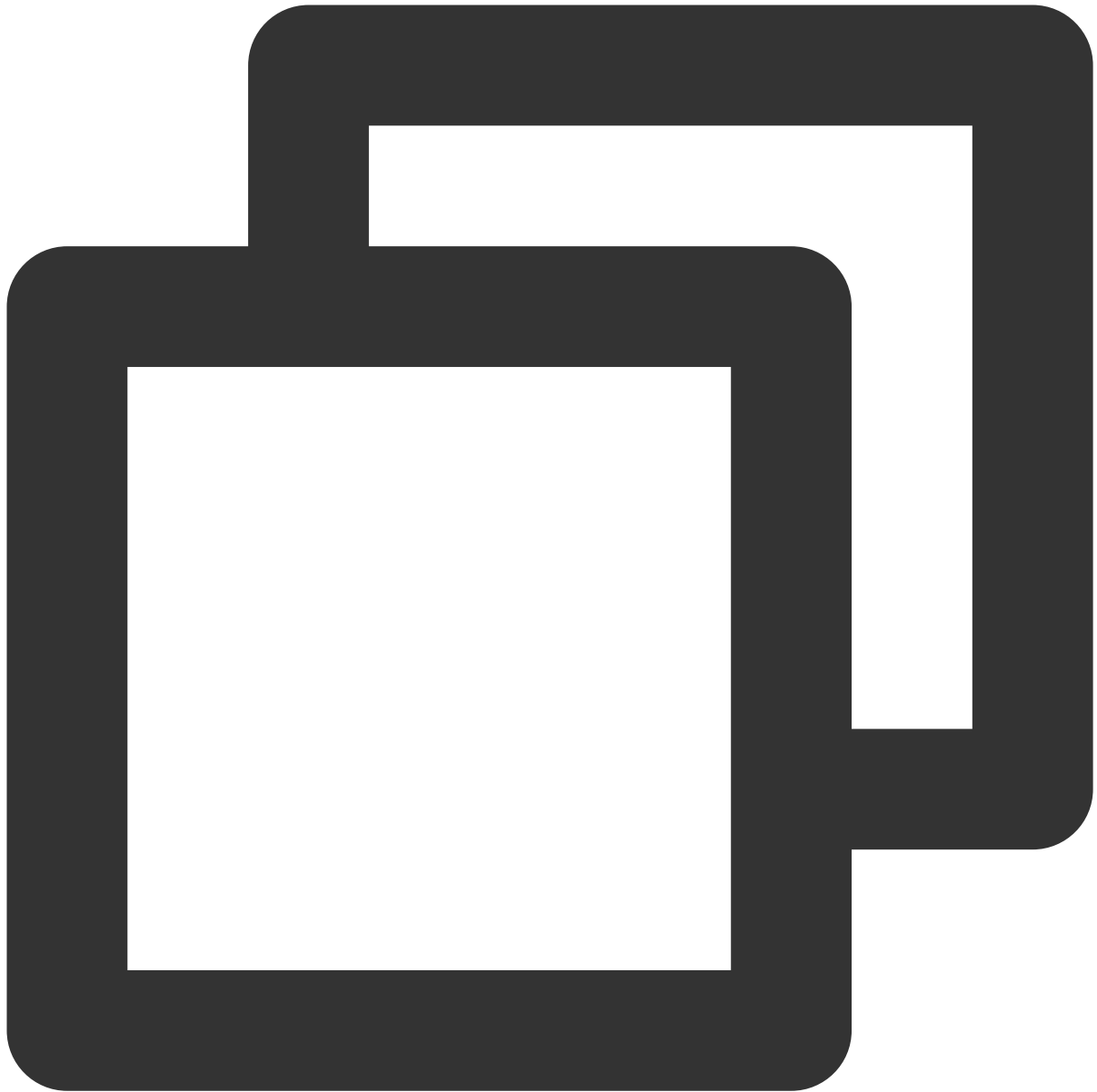
3.1 데이터 세트를 준비합니다.

다음 명령어를 실행하여 ImageNet validation 데이터 세트를 다운로드 및 압축 해제합니다.



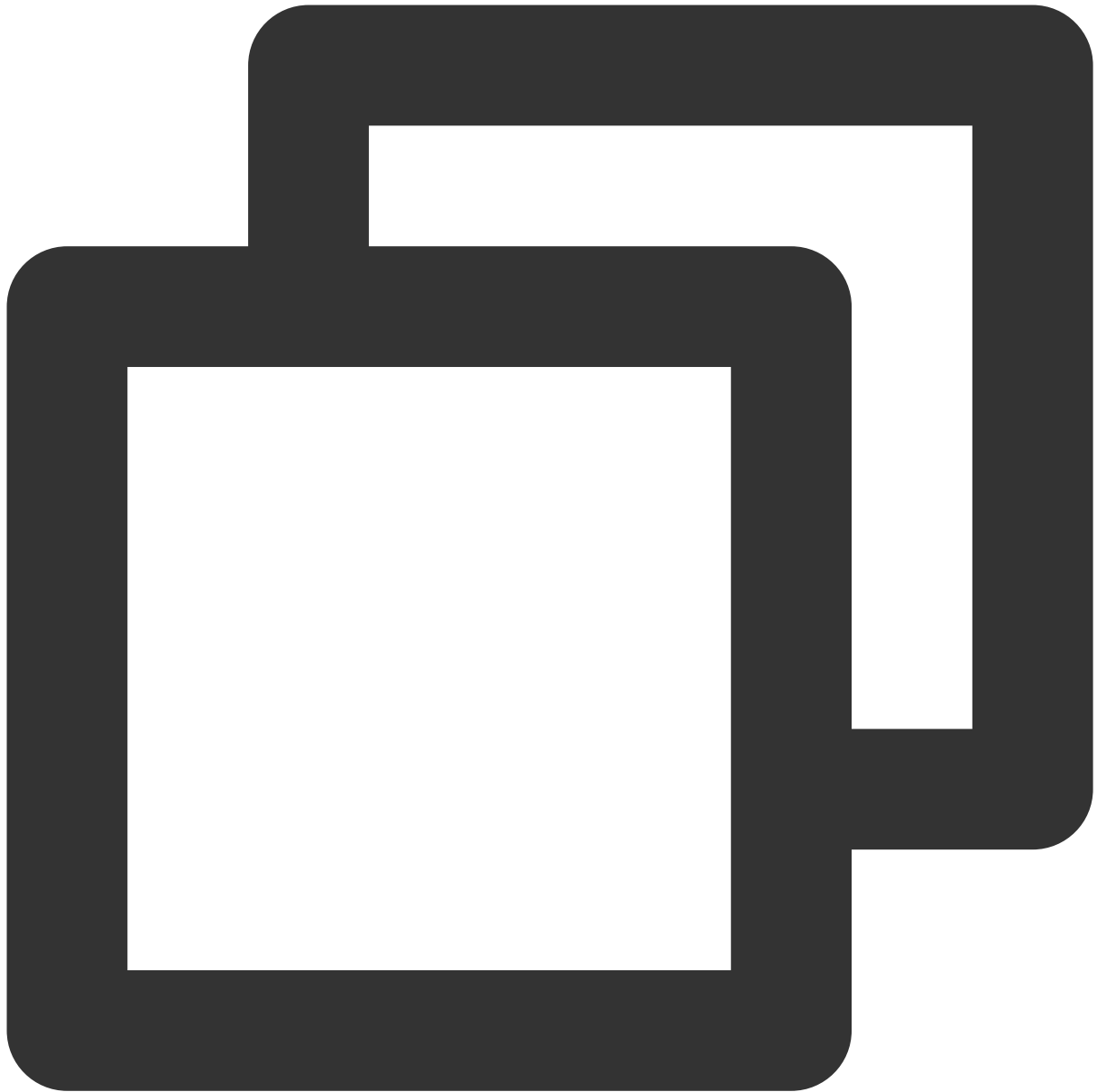
```
mkdir -p img_raw/val && cd img_raw
wget http://www.image-net.org/challenges/LSVRC/2012/dd31405981
ef5f776aa17412e1f0c112/ILSVRC2012_img_val.tar
tar -xvf ILSVRC2012_img_val.tar -C val
```

다음 명령어를 실행하여 image 파일을 label 분류에 따른 서브 디렉터리로 이동합니다.



```
cd val
wget -qO -https://raw.githubusercontent.com/soumith/
imagenetloader.torch/master/valprep.sh | bash
```

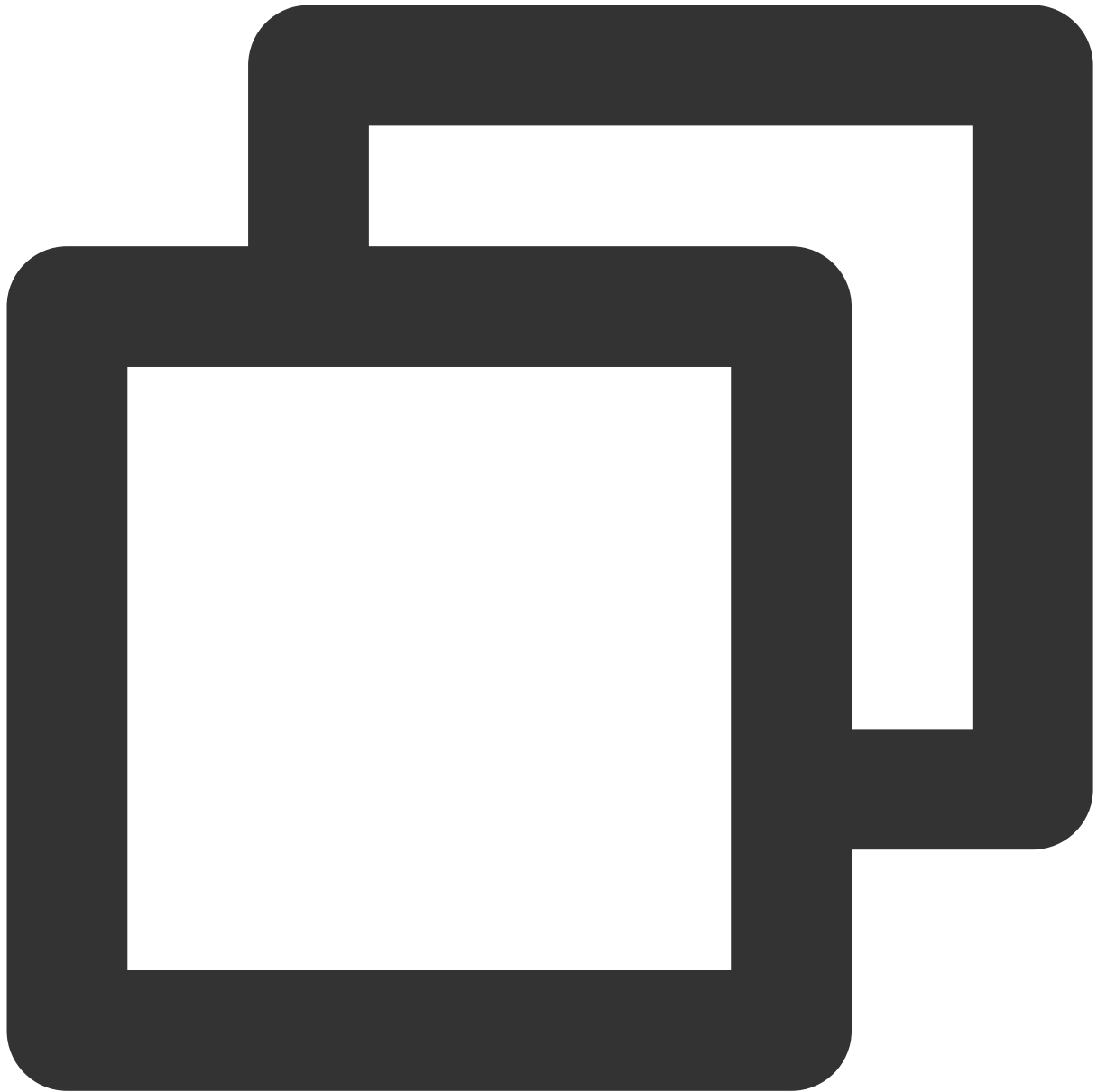
다음 명령어를 실행하여 스크립트 `prepare_dataset.sh` 를 사용해 원시 데이터를 TFrecord 포맷으로 변환합니다.



```
cd examples/tensorflow/image_recognition
bash prepare_dataset.sh --output_dir=./data --raw_dir=/PATH/TO/img_raw/val/
--subset=validation
```

데이터 세트 관련 자세한 내용은 [Prepare Dataset](#)를 참고하십시오.

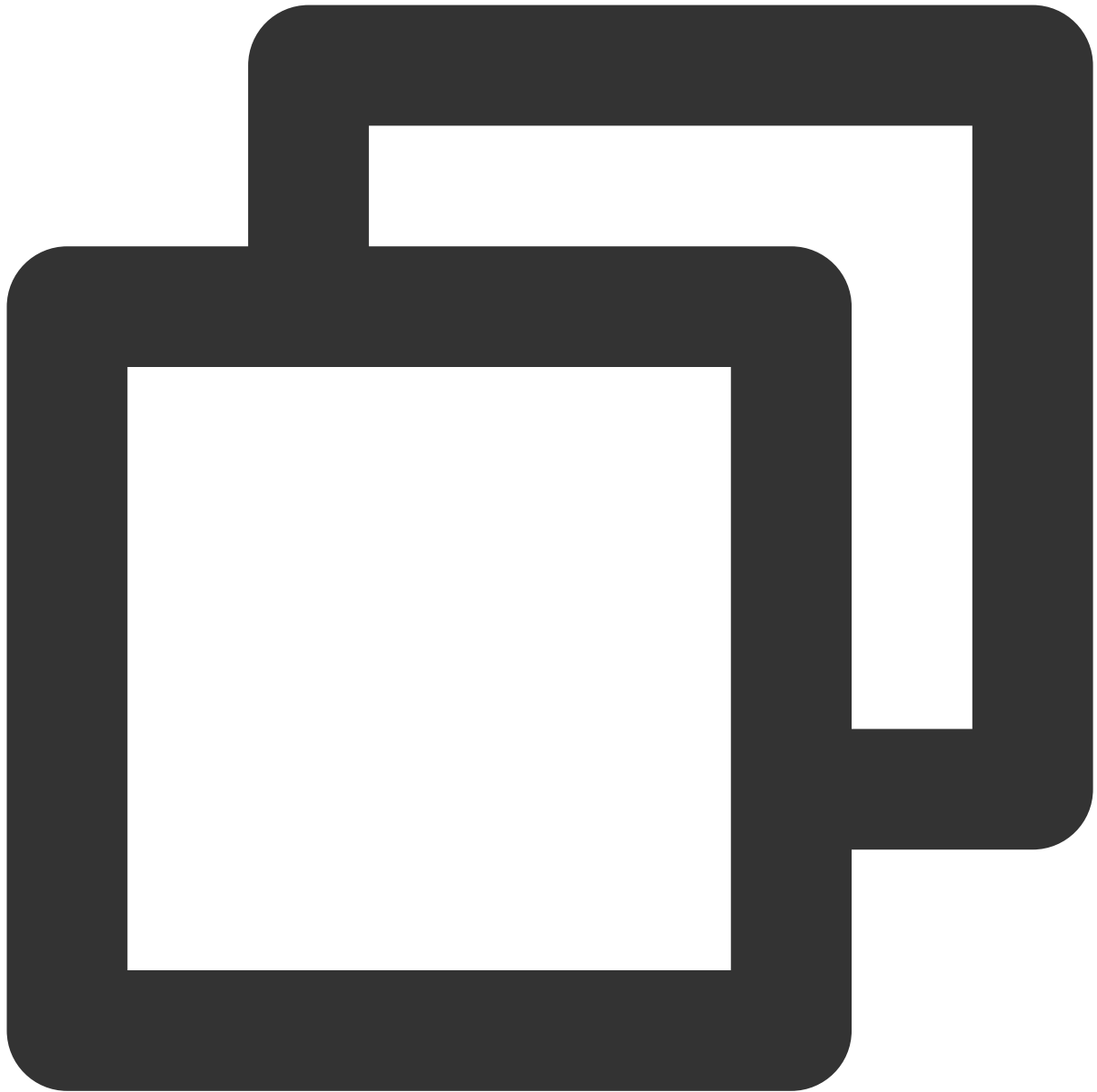
3.2 다음 명령어를 실행해 모델을 준비합니다.



```
wget https://storage.googleapis.com/intel-optimized-tensorflow/
models/v1_6/resnet50_fp32_pretrained_model.pb
```

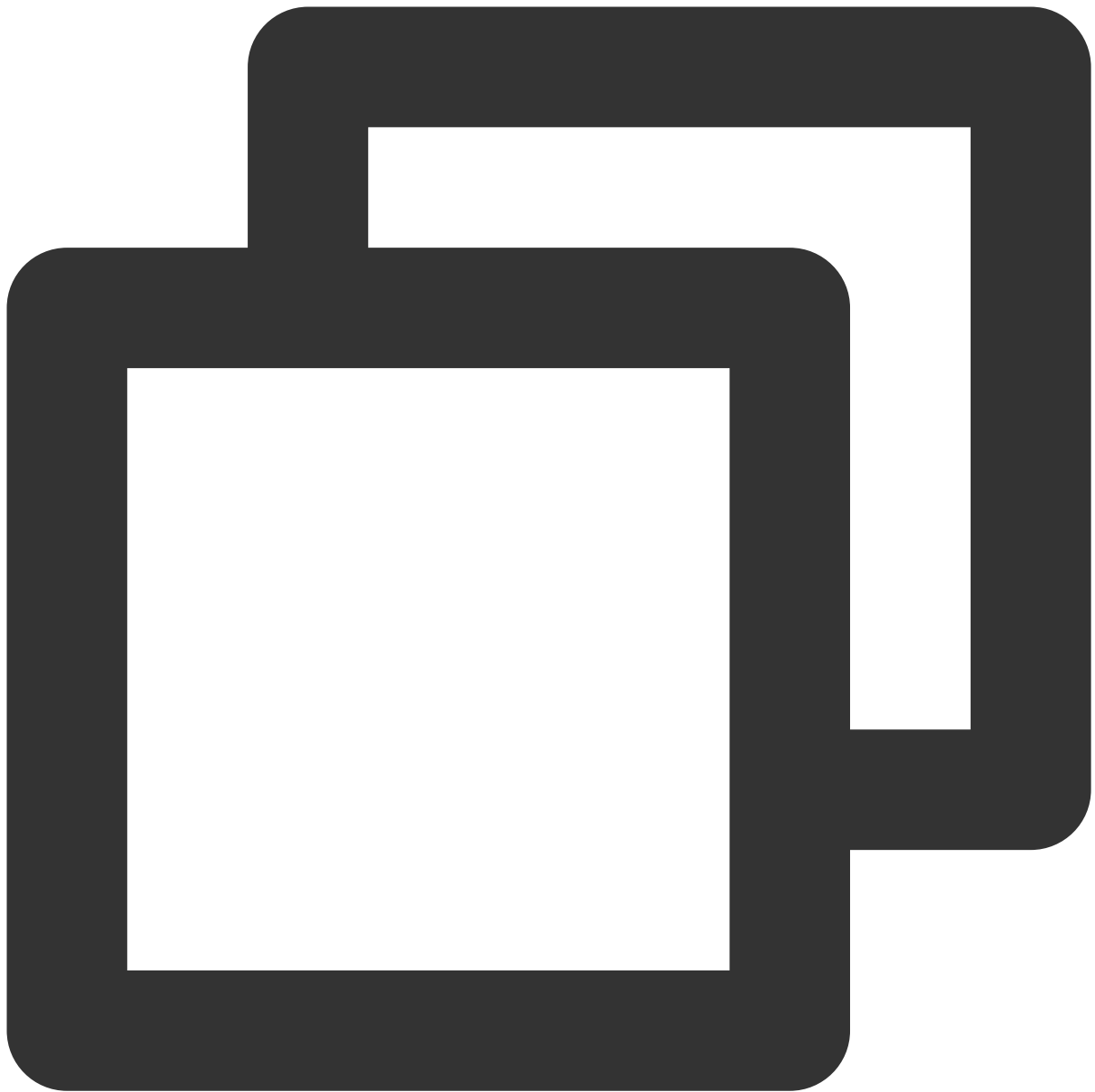
3.3 다음 명령어를 실행하여 Tuning을 실행합니다.

`examples/tensorflow/image_recognition/resnet50_v1.yaml` 파일을 수정해 `quantization\calibration`, `evaluation\accuracy`, `evaluation\performance` 세 부분의 데이터 세트 경로를 사용자의 실제 로컬 경로로 지정합니다. 이는 데이터 세트 준비 단계에서 생성한 TFrecord 데이터가 있는 위치입니다. 자세한 내용은 [ResNet50 V1.0](#)을 참고하십시오.



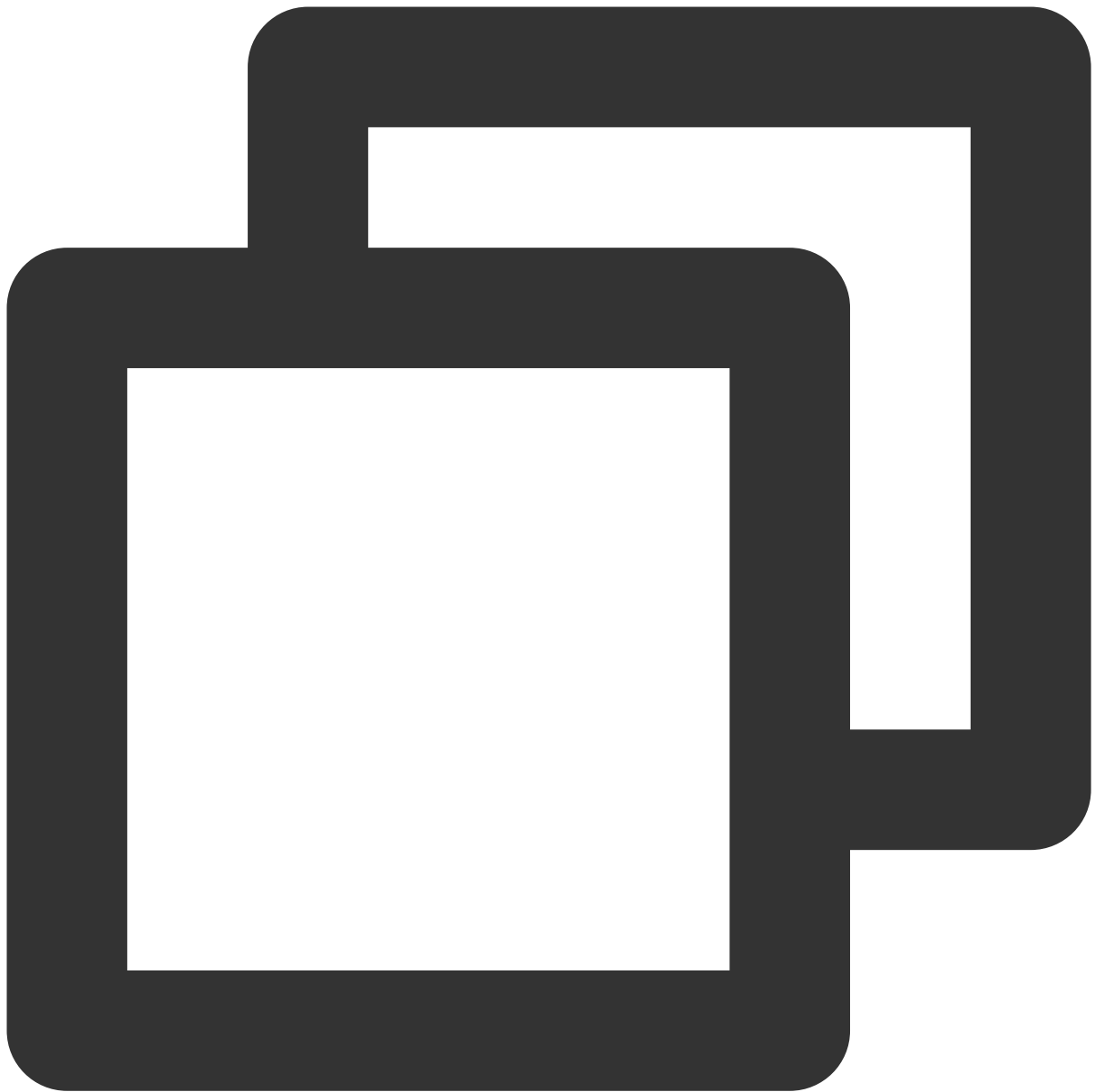
```
cd examples/tensorflow/image_recognition
bash run_tuning.sh --config=resnet50_v1.yaml \
--input_model=/PATH/TO/resnet50_fp32_pretrained_model.pb \
--output_model=./lpot_resnet50_v1.pb
```

3.4 다음 명령어를 실행하여 **Benchmark**를 실행합니다.



```
bash run_benchmark.sh --input_model=./lpot_resnet50_v1.pb  
--config=resnet50_v1.yaml
```

출력 결과는 다음과 같습니다. 성능 데이터는 참고용입니다.



```
accuracy mode benchmarkresult:  
Accuracy is 0.739  
Batch size = 32  
Latency: 1.341 ms  
Throughput: 745.631 images/sec  
performance mode benchmark result:  
Accuracy is 0.000  
Batch size = 32  
Latency: 1.300 ms  
Throughput: 769.302 images/sec
```


예시4: Intel® Distribution of OpenVINO™ Toolkit 를 사용해 추론 가속

Intel® Distribution of OpenVINO™ Toolkit는 컴퓨터의 시각화 및 기타 딥 러닝 애플리케이션 배포를 가속화할 수 있는 툴 패키지입니다. Intel 플랫폼의 다양한 가속기(CPU, GPU, FPGA, Movidius의 VPU 포함)를 통한 딥러닝 및 이중 하드웨어의 직접 실행을 지원합니다.

Intel® Distribution of OpenVINO™ Toolkit는 TensorFlow*, PyTorch* 등을 통해 학습된 모델을 최적화할 수 있습니다. 모델 옵티마이저, 추론 엔진, Open Model Zoo, 학습 후 최적화 툴(Post-training Optimization Tool) 등 배포 툴 패키지를 포함합니다.

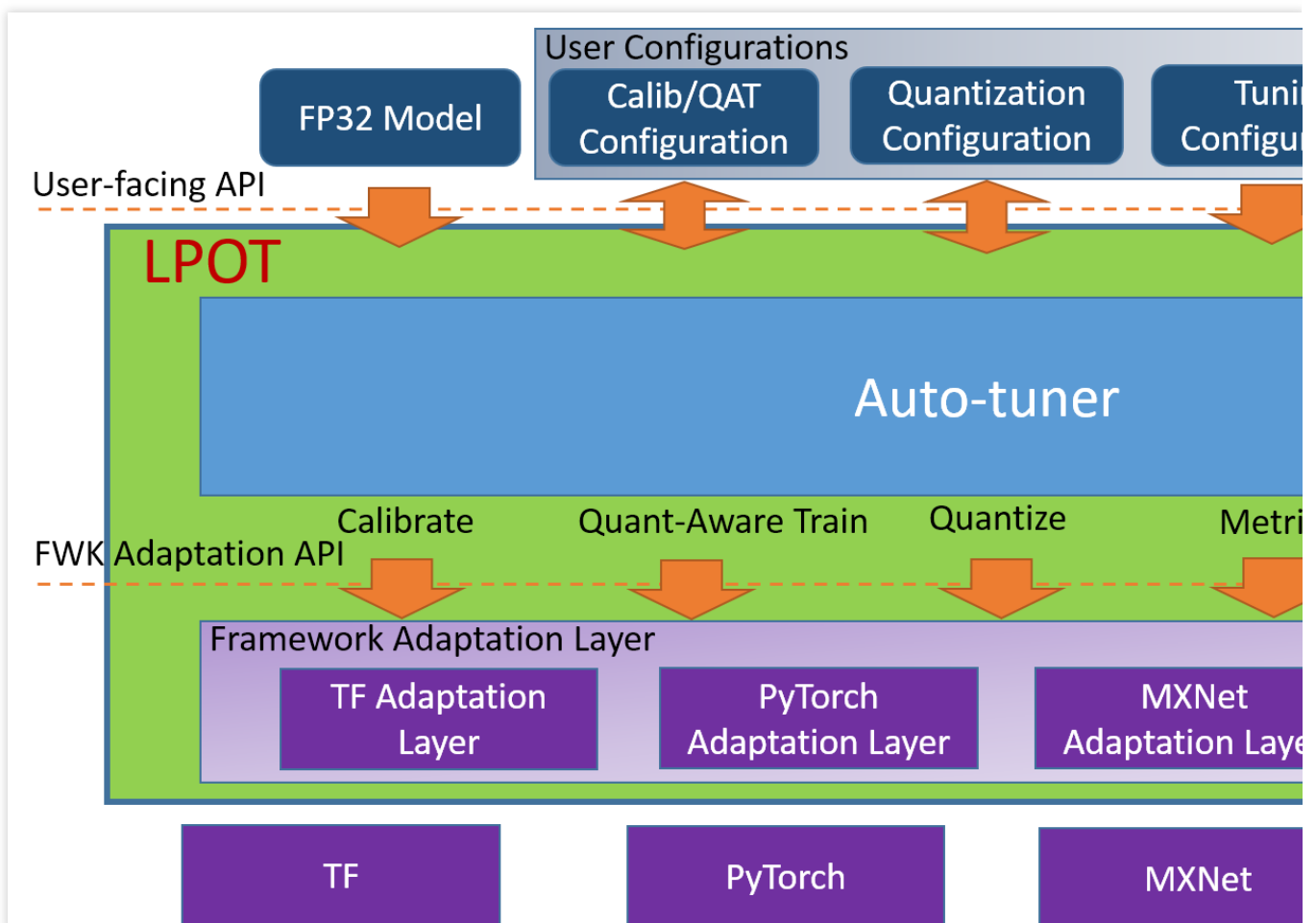
모델 옵티마이저(Model optimizer): Caffe*, TensorFlow*, PyTorch*, Mxnet* 등 다양한 프레임워크 학습 모델을 중간 표현(IR)으로 변환합니다.

추론 엔진(Inference Engine): 변환된 IR을 CPU, GPU, FPGA, VPU와 같은 하드웨어에서 실행하면 자동으로 하드웨어의 가속 패키지를 호출해 추론 성능을 가속화합니다.

[Intel® Distribution of OpenVINO™ Toolkit 공식 홈페이지](#) 또는 [온라인 문서](#)에서 자세한 정보를 확인할 수 있습니다.

워크플로

Intel® Distribution of OpenVINO™ Toolkit 툴 패키지 워크플로 순서도는 다음과 같습니다.



Intel® Distribution of OpenVINO™ Toolkit 추론 성능

The Intel® Distribution of OpenVINO™ 툴은 다양한 Intel 프로세서 및 가속 하드웨어에서 최적화 구현을 제공합니다. 이 툴은 Intel® Xeon® 확장 가능 프로세서 플랫폼에서 Intel® DL Boost 및 AVX-512 명령어 집합을 사용해 추론 네트워크 가속을 진행합니다.

Intel® Distribution of OpenVINO™ Toolkit를 사용한 딥러닝 개발 패키지(DLDT)

다음 자료를 참고하십시오.

[Intel® 딥러닝 배포 툴 패키지 소개](#)

[이미지 분류 C++ 예시\(비동기화 모드\)](#)

[객체 검증 C++ 예시\(SSD\)](#)

[자동 음성인식 C++ 예시](#)

[동작인식 Python* 예시](#)

[교차로 카메라 C++ 예시](#)

[포즈 예측 C++ 예시](#)

Intel® Distribution of OpenVINO™ Toolkit 기본 테스트

자세한 내용은 [Linux* 지향 Intel® OpenVINO™ 툴 패키지 배포 버전 설치](#)를 참고하십시오.

Tencent SGX 보안 컴퓨팅 환경 구축

최종 업데이트 날짜: : 2024-02-02 11:01:47

작업 시나리오

본문은 M6ce 인스턴스에서 Tencent SGX 보안 컴퓨팅 환경을 구축하는 방법을 소개하고, intel SGXSDK를 사용하여 SGX 기능을 인증하는 방법을 안내합니다.

전제 조건

M6ce 인스턴스를 생성 및 로그인 완료해야 합니다.

인스턴스 생성 방법은 [구매 페이지를 통한 인스턴스 생성](#)을 참고하십시오.

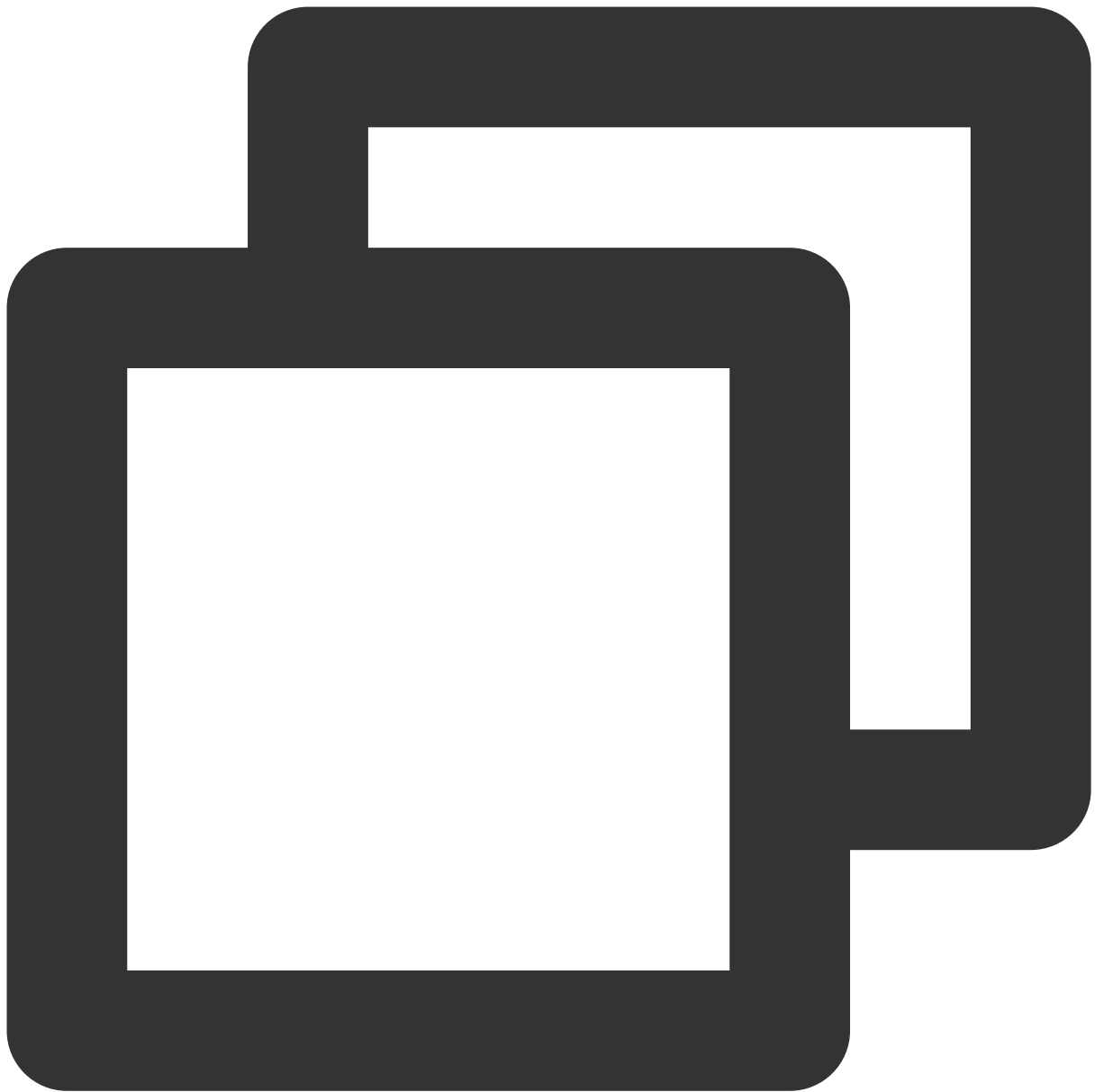
인스턴스에 로그인하는 방법은 [Linux 인스턴스에 로그인](#)을 참고하십시오.

설명 :

본문은 TencentOS Server 3.1(TK4) 운영 체제의 인스턴스를 예시로 사용합니다. 운영 체제 버전에 따라 과정이 다르므로 실제 상황에 맞게 작업하십시오.

작업 단계

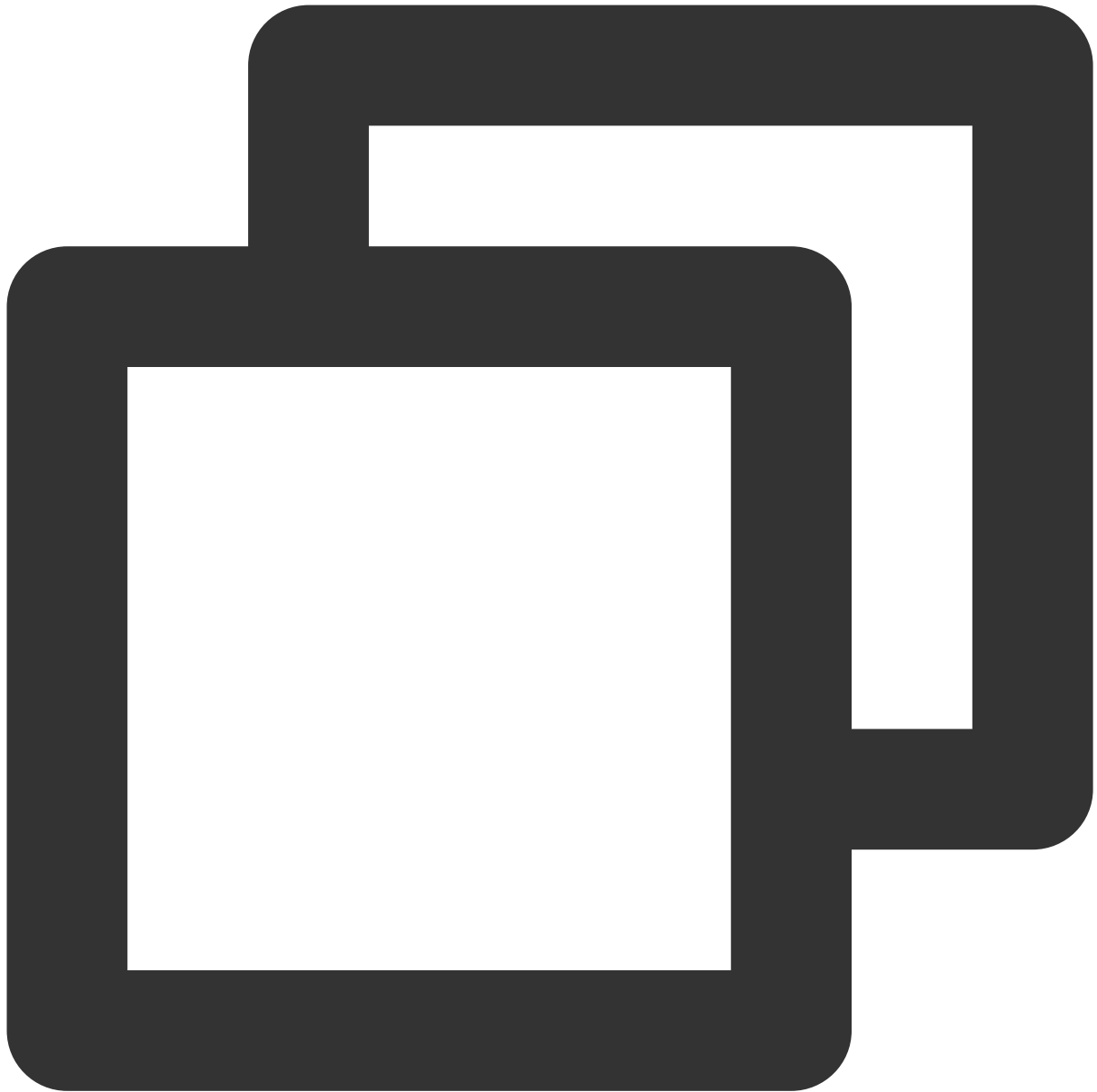
1. 다음 명령어를 실행하여 kernel 버전을 확인합니다.



```
uname -a
```

kernel 버전이 5.4.119-19.0008보다 낮은지 확인합니다.

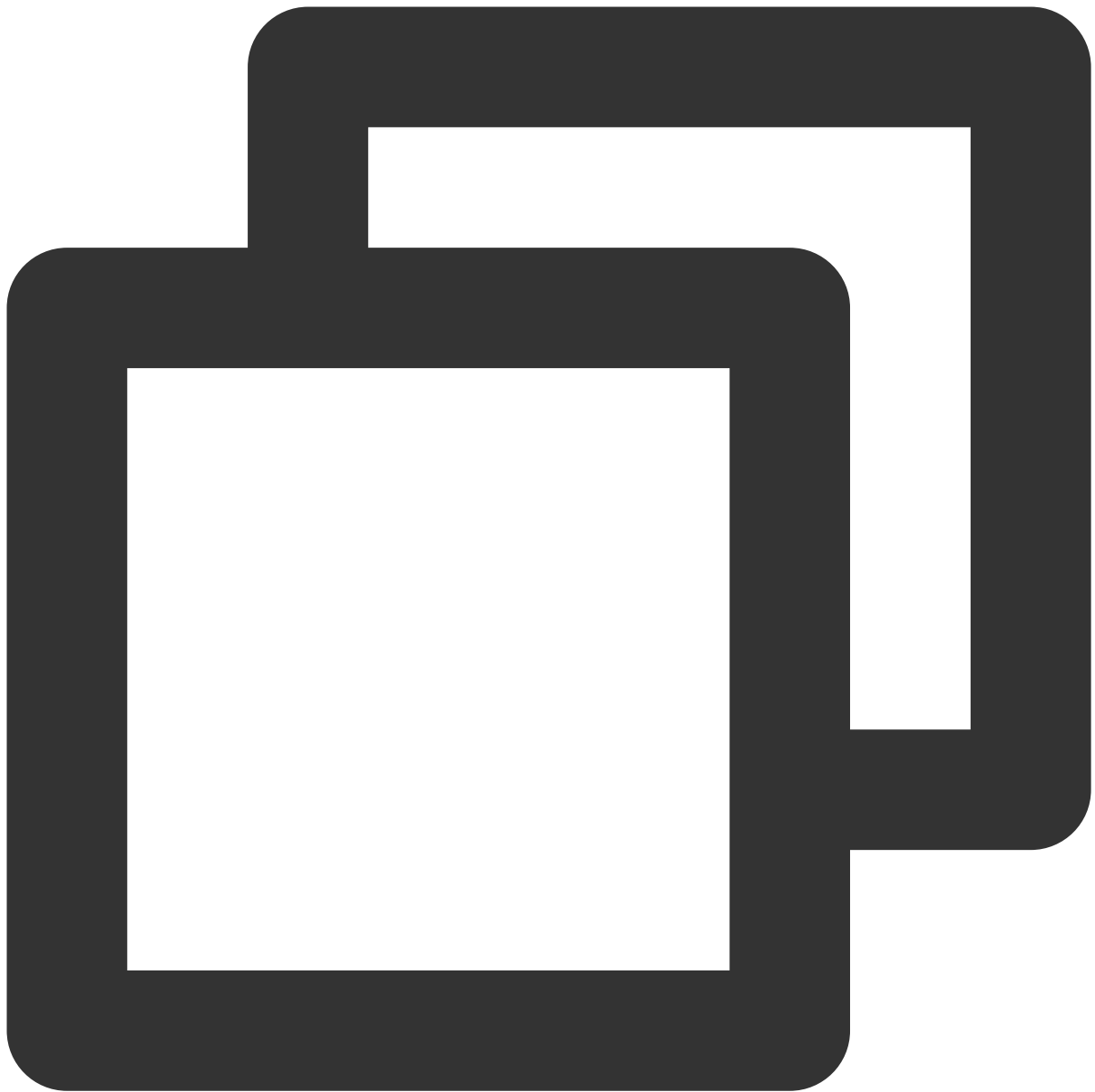
낮다면 다음 명령어를 실행하여 kernel을 업데이트합니다.



```
yum update kernel
```

낮지 않다면 다음 단계를 진행합니다.

2. 다음 명령어를 실행하여 SGX runtime에 필요한 소프트웨어 패키지를 설치합니다.

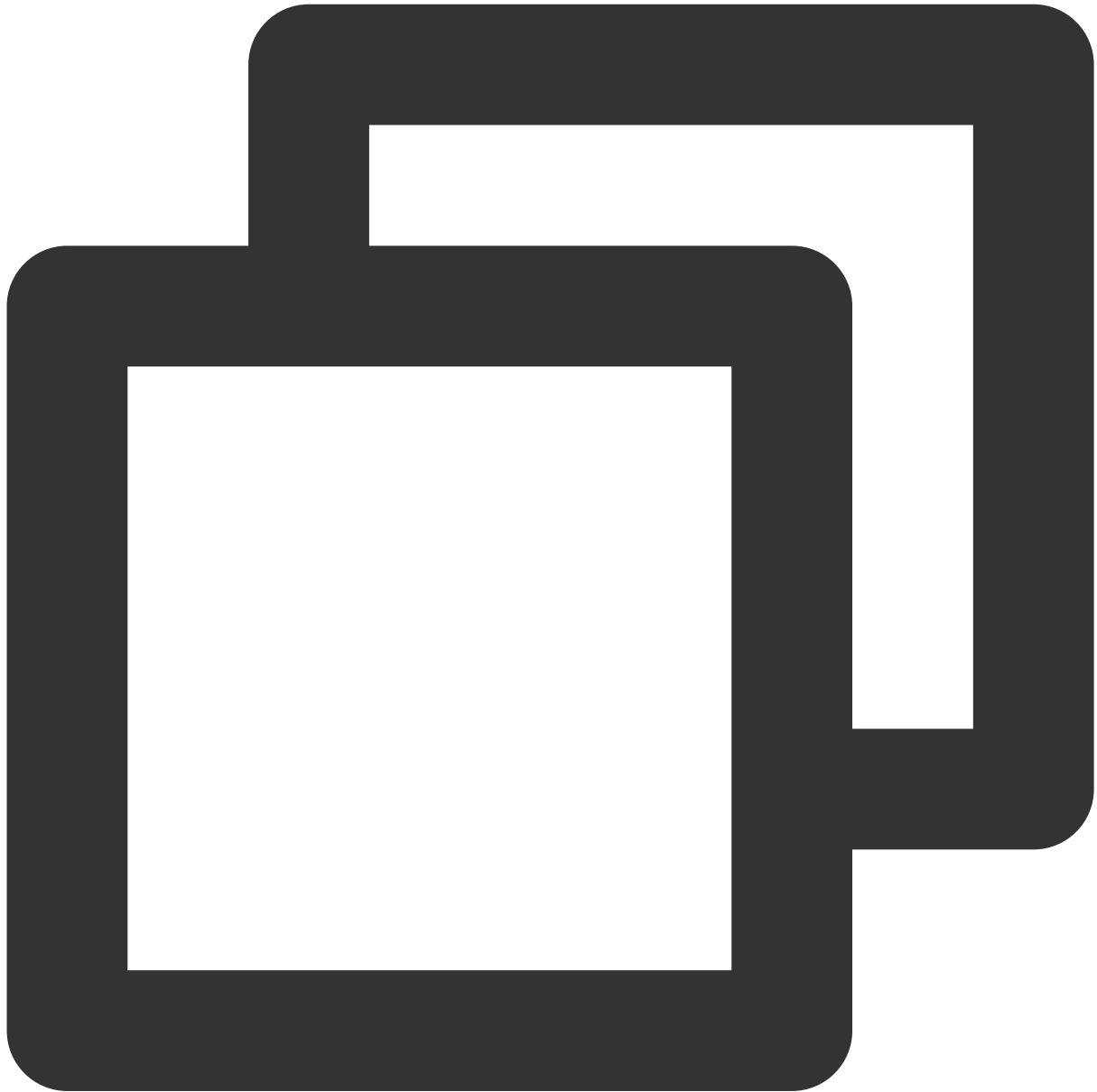


```
yum install \\  
  libsgx-aes-le libsgx-aes-pce libsgx-aes-qe3 libsgx-aes-qve \\  
  libsgx-aesm-ecdsa-plugin libsgx-aesm-launch-plugin libsgx-aesm-pce-plugin libsgx-a-  
  libsgx-dcap-default-qpl libsgx-dcap-default-qpl-devel libsgx-dcap-ql libsgx-dcap-q  
  libsgx-dcap-quote-verify libsgx-dcap-quote-verify-devel libsgx-enclave-common libs  
  libsgx-launch libsgx-launch-devel libsgx-pce-logic libsgx-qe3-logic libsgx-quote-e  
  libsgx-ra-network libsgx-ra-uefi libsgx-uae-service libsgx-urts sgx-ra-service \\  
  sgx-aesm-service
```

설명 :

SGX AESM 서비스의 기본 설치 디렉터리는 `/opt/intel/sgx-aesm-service` 입니다.

3. 다음 명령어를 실행하여 intel SGXSDK를 설치합니다.



```
yum install sgx-linux-x64-sdk
```

설명 :

Intel SGXSDK의 기본 설치 디렉터리는 `/opt/intel/sgxsdk` 입니다. [intel SGXSDK](#) 사용자 매뉴얼을 참고하여 SGX 프로그램을 개발할 수 있습니다.

4. SGX runtime 및 intel SGXSDK가 설치된 후 인스턴스를 재시작합니다. 자세한 내용은 [인스턴스 재시작](#)을 참고하십시오.

5. Tencent Cloud SGX 원격 증명 서비스를 설정합니다.

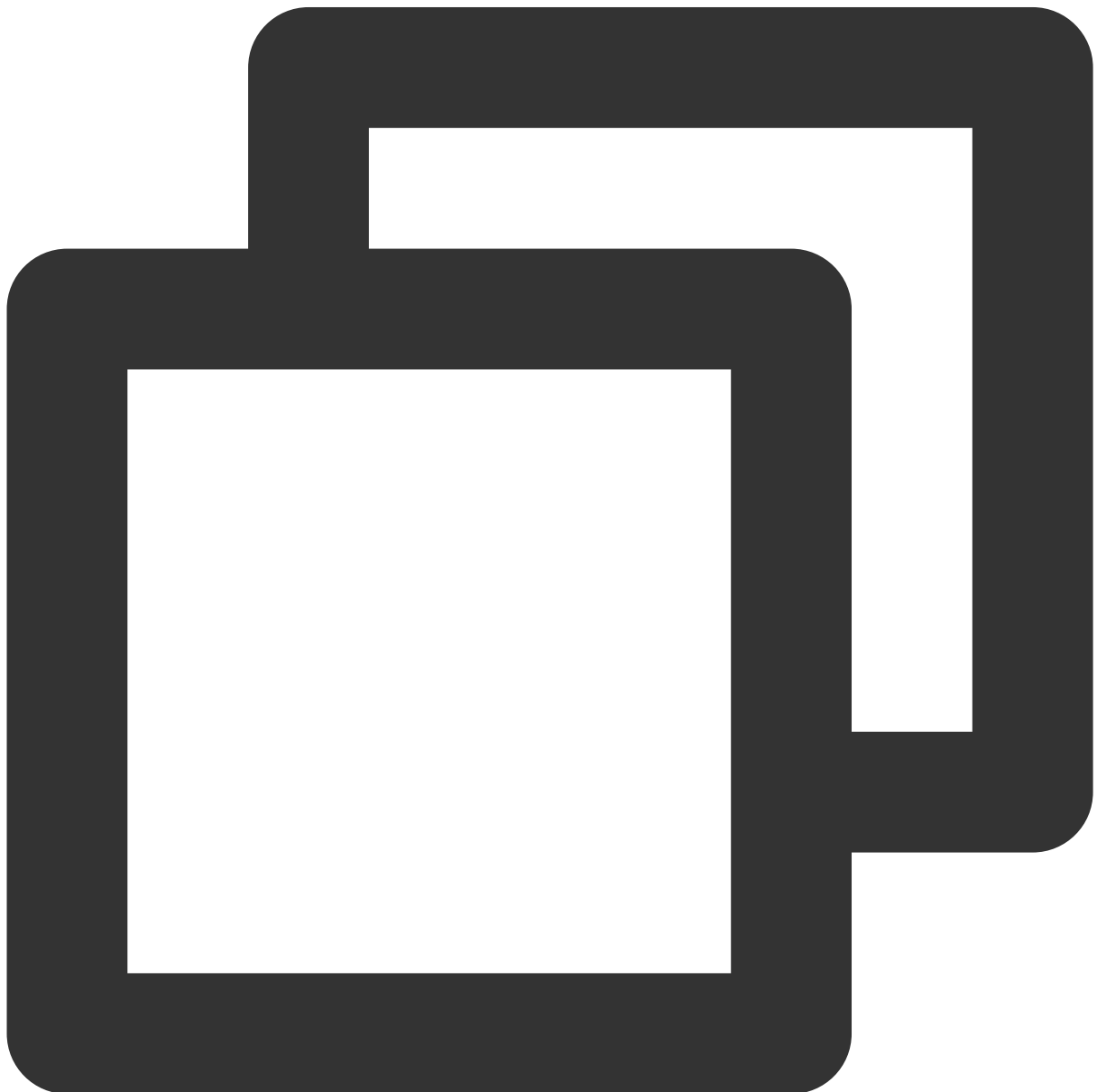
Tencent Cloud SGX 원격 증명 서비스는 리전별 배치가 적용됩니다. SGX CVM 인스턴스가 위치한 리전에서 Tencent Cloud SGX 원격 증명 서비스에 접속하여 최상의 경험을 얻을 수 있습니다. intel SGX SDK를 설치한 후 원격 증명 서비스의 기본 구성 파일 `/etc/sgx_default_qcnl.conf` 가 자동으로 생성됩니다. SGX CVM 인스턴스가 위치한 리전의 Tencent Cloud SGX 원격 증명 서비스에 맞게 파일을 수동으로 수정하려면 아래 단계를 따르십시오.

설명 :

현재 베이징, 상하이, 광저우 리전만 Tencent Cloud SGX 원격 증명 서비스를 지원합니다.

Intel Ice Lake는 Intel EPID 원격 증명 방식이 아닌 Intel SGX DCAP 기반 원격 증명 방식만 지원합니다.

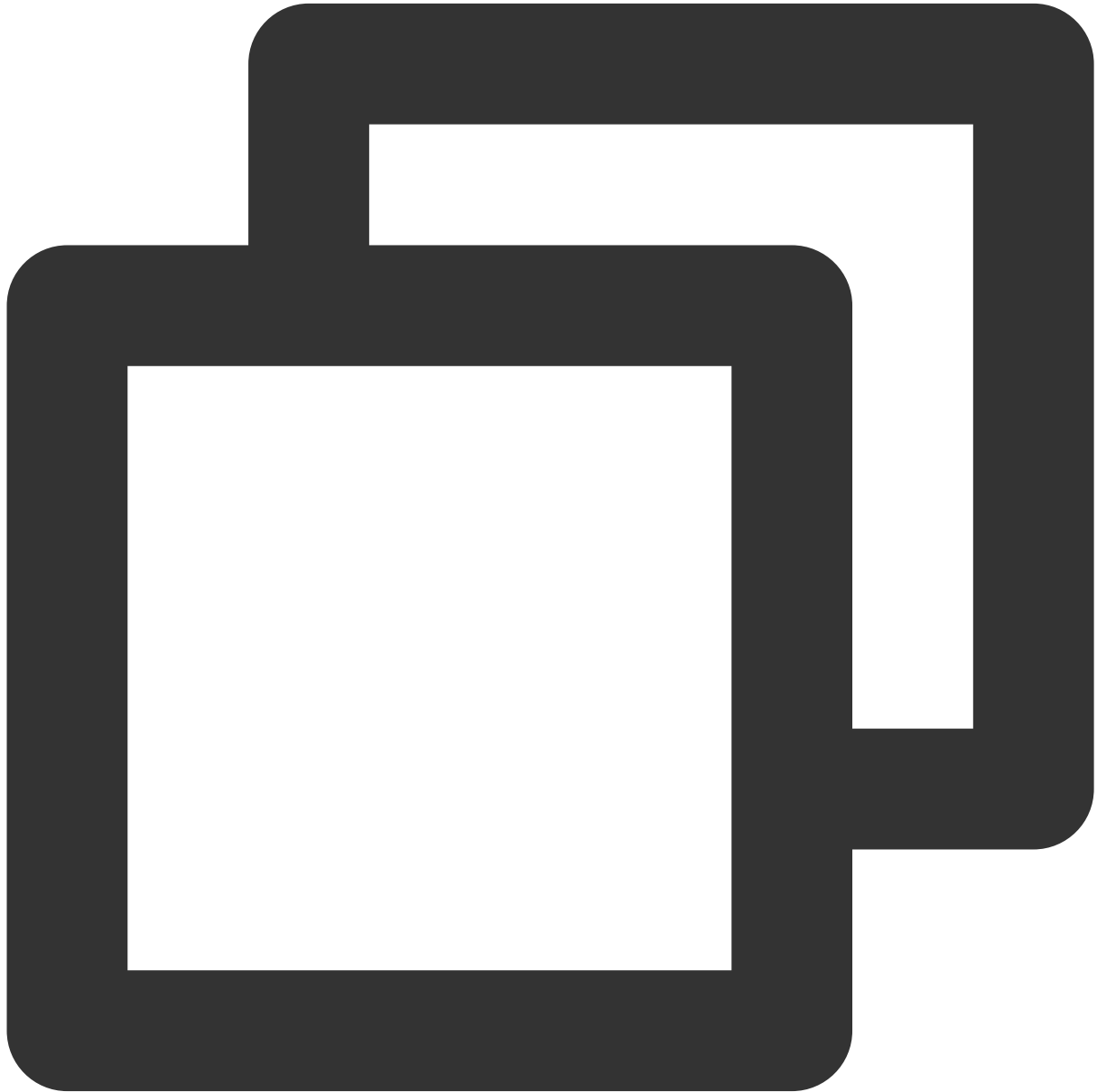
VIM 편집기를 사용하여 `/etc/sgx_default_qcnl.conf` 를 다음 내용으로 수정합니다.




```
# PCCS server address
PCCS_URL=https://sgx-dcap-server-tc.[Region-ID].tencent.cn/sgx/certification/v3/
# To accept insecure HTTPS cert, set this option to FALSE
USE_SECURE_CERT=TRUE
```

[Region-ID] 를 SGX CVM 인스턴스가 위치한 리전의 ID로 바꾸십시오. 예시: **
**

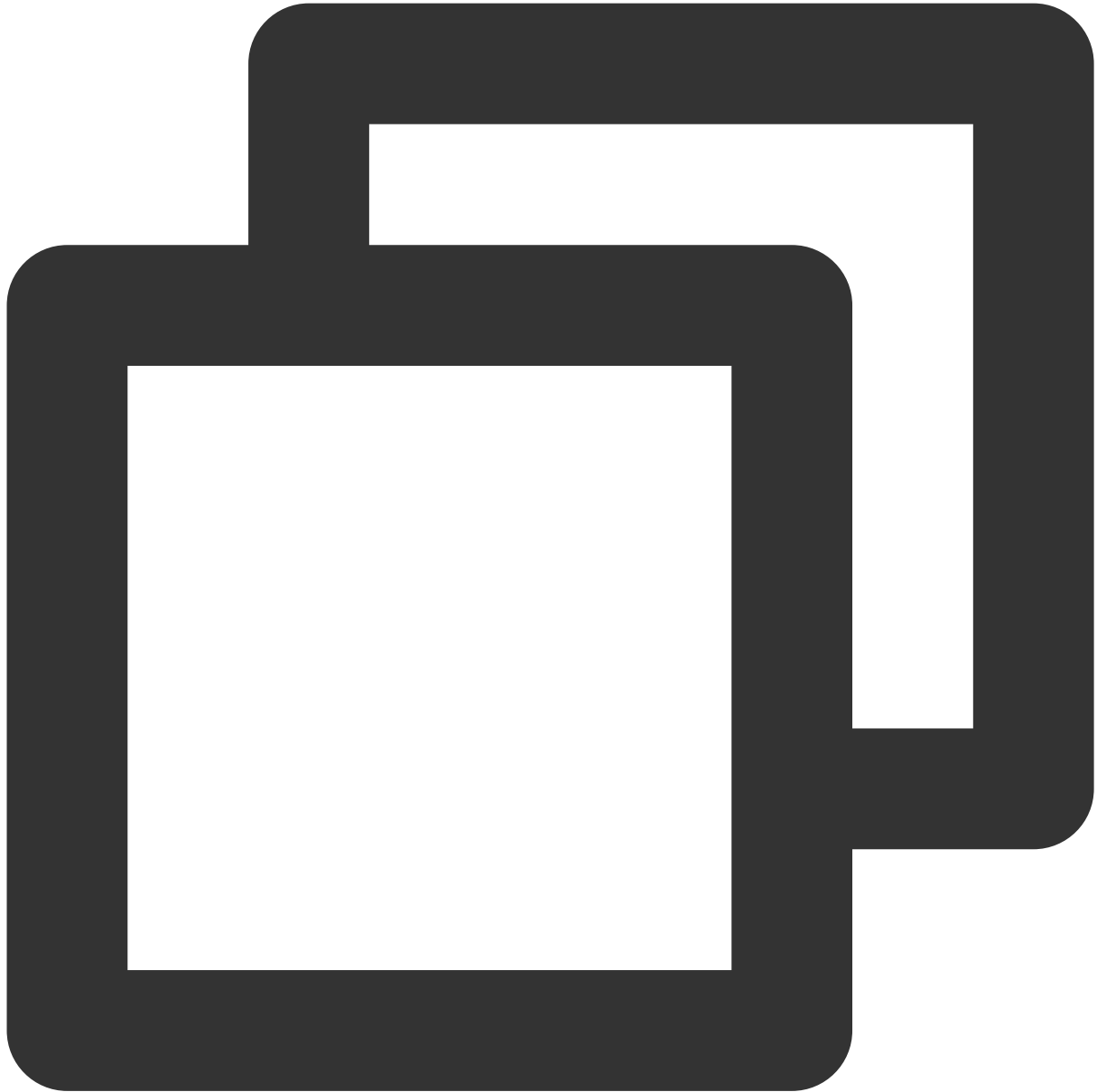
베이징 리전 수정 예시는 다음과 같습니다.



```
# PCCS server address
PCCS_URL=https://sgx-dcap-server-tc.bj.tencent.cn/sgx/certification/v3/
# To accept insecure HTTPS cert, set this option to FALSE
```

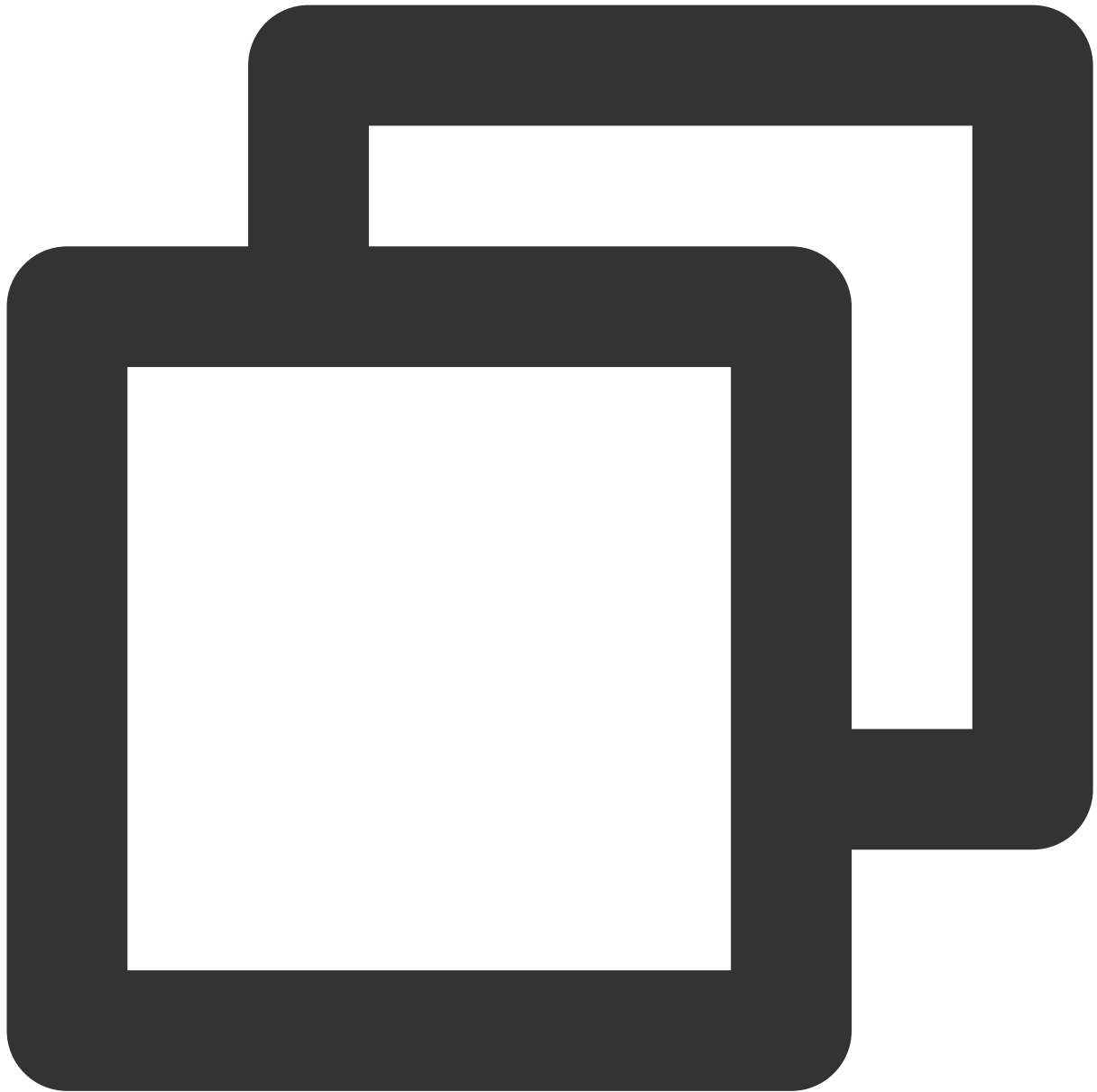
```
USE_SECURE_CERT=TRUE
```

상하이 리전 수정 예시는 다음과 같습니다.



```
# PCCS server address
PCCS_URL=https://sgx-dcap-server-tc.sh.tencent.cn/sgx/certification/v3/
# To accept insecure HTTPS cert, set this option to FALSE
USE_SECURE_CERT=TRUE
```

광저우 리전 수정 예시는 다음과 같습니다.



```
# PCCS server address
PCCS_URL=https://sgx-dcap-server-tc.gz.tencent.cn/sgx/certification/v3/
# To accept insecure HTTPS cert, set this option to FALSE
USE_SECURE_CERT=TRUE
```

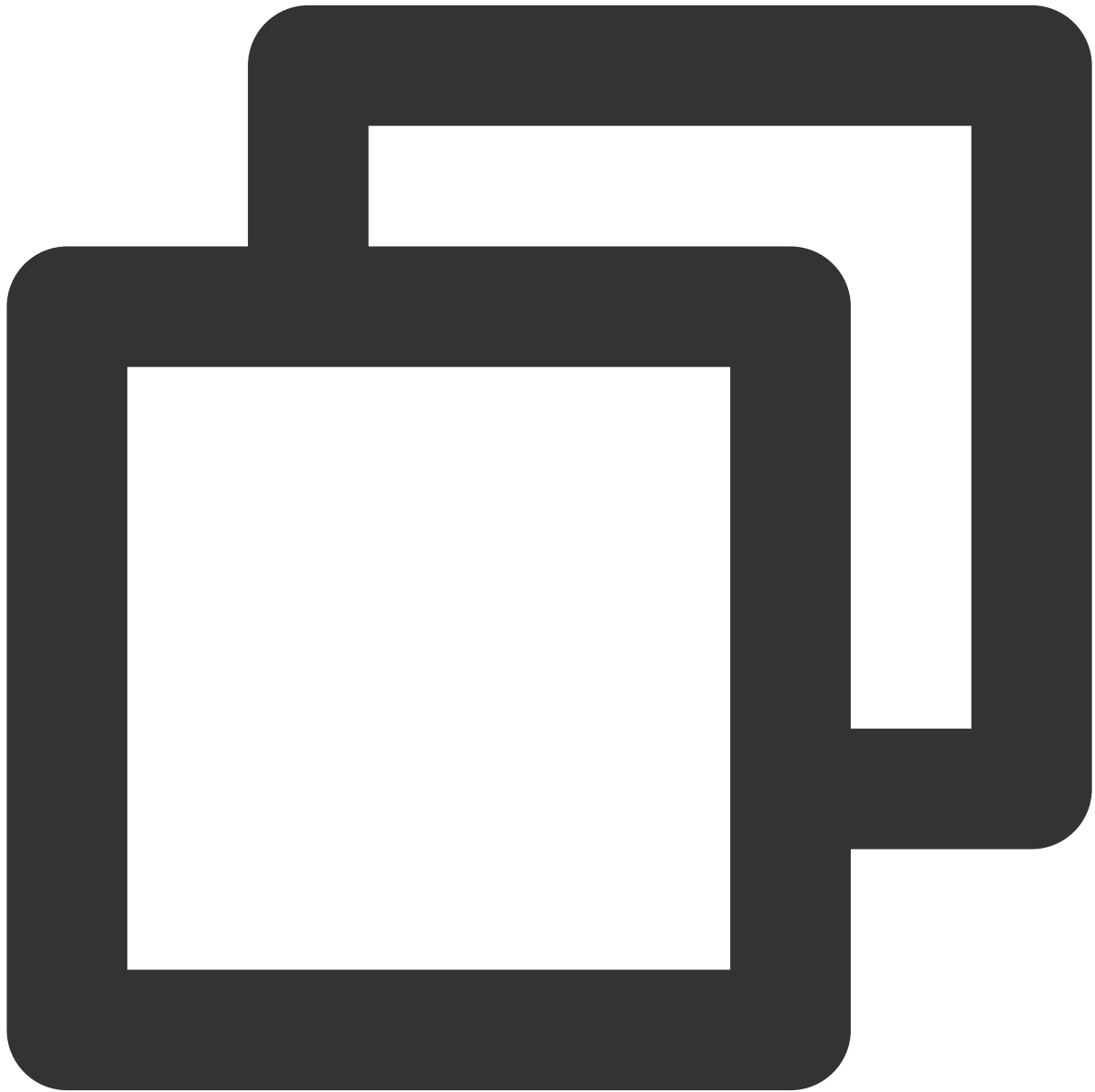
SGX 기능 인증 예시

예시1: Enclave 실행

Intel SGXSDK는 SGX 기능을 인증하기 위한 SGX 샘플 코드를 제공합니다. 기본 디렉터리는

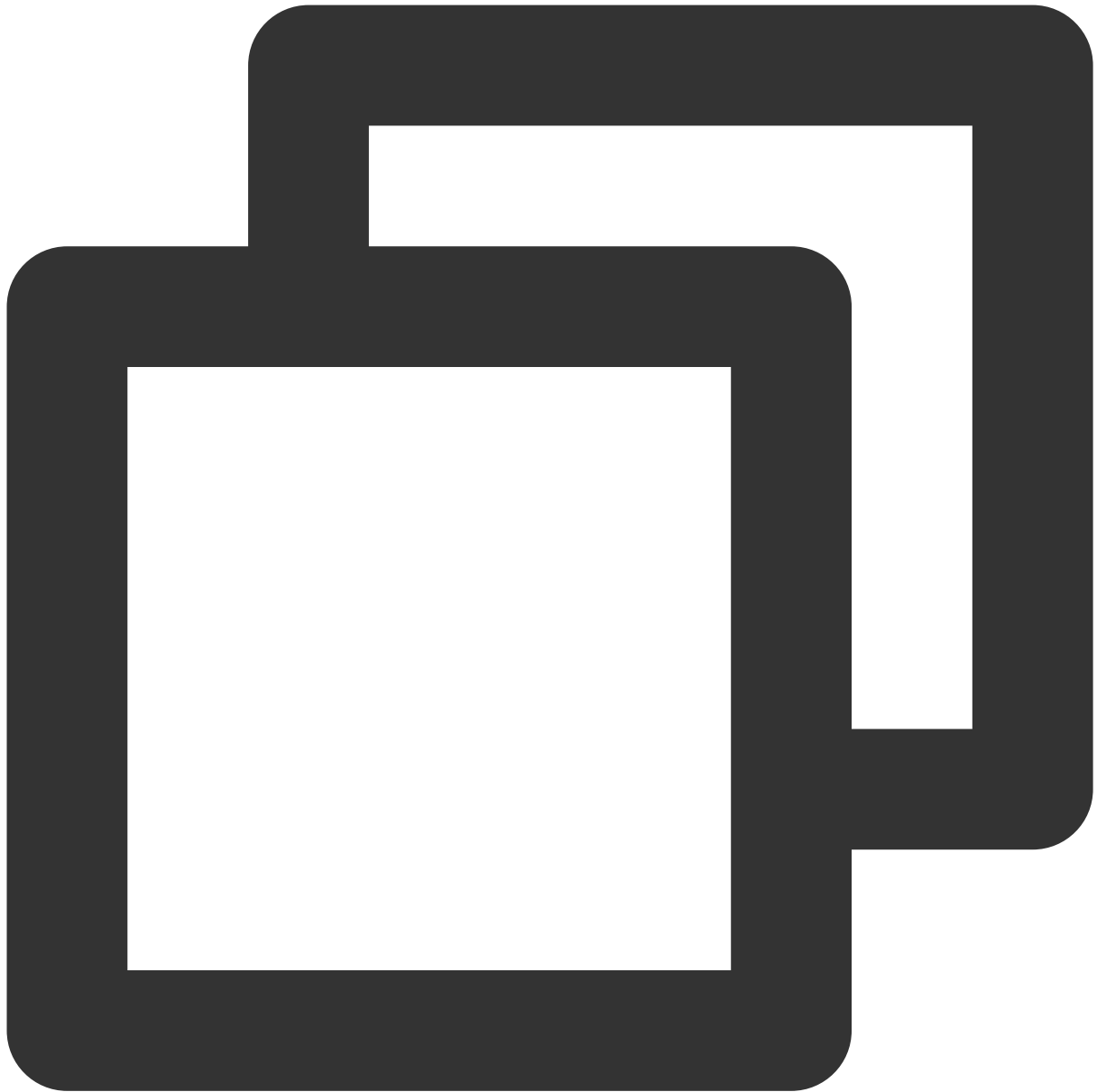
`/opt/intel/sgxsdk/SampleCode` 입니다. 이 예시에서 코드(SampleEnclave)의 효과는 설치된 SGXSDK의 정상 사용 여부와 SGX CVM 인스턴스의 보안 메모리 리소스 사용 가능 여부를 확인하기 위해 Enclave를 실행하는 것입니다.

1. 다음 명령어를 실행하여 intel SGXSDK와 관련된 환경 변수를 설정합니다.



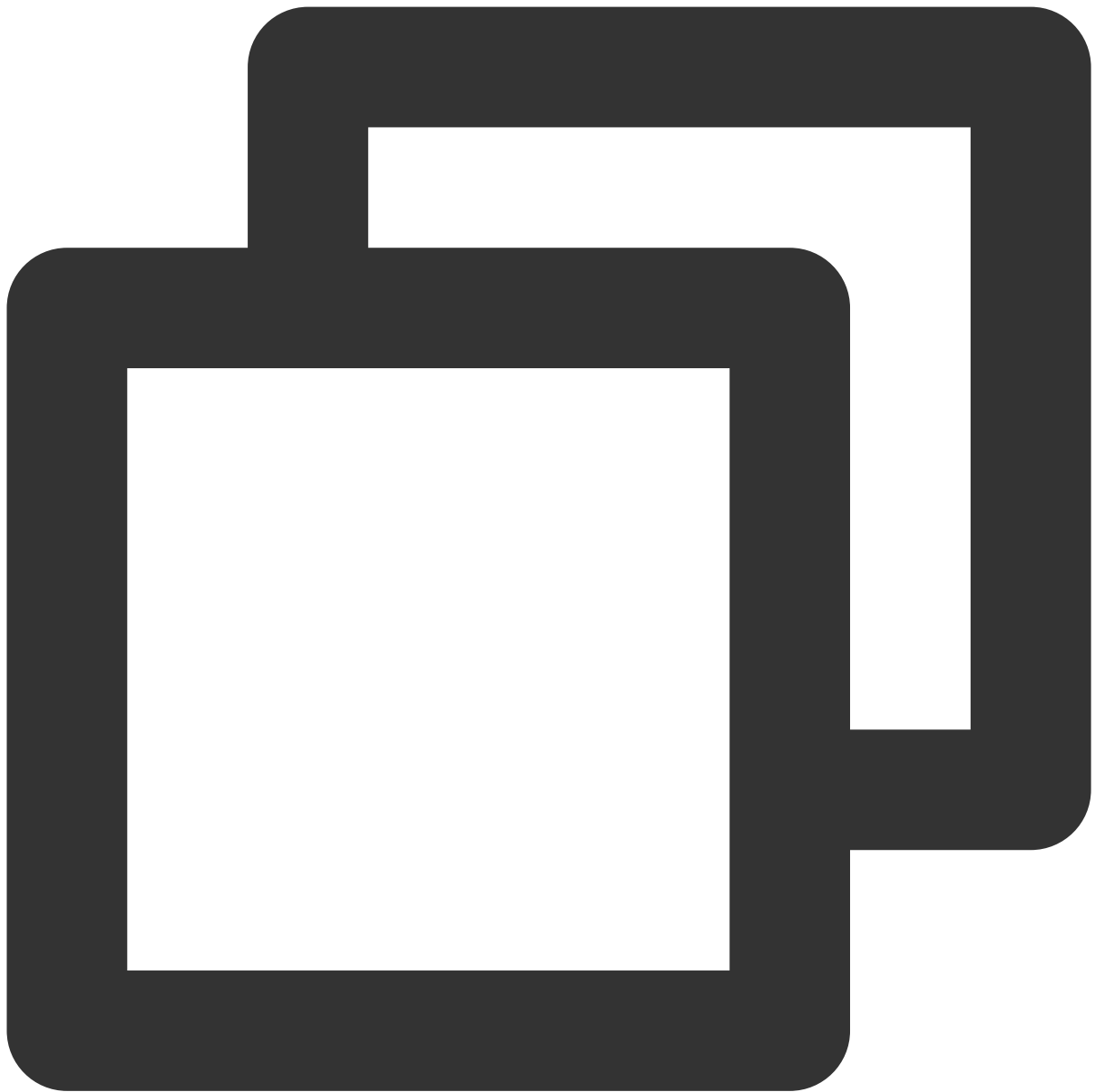
```
source /opt/intel/sgxsdk/environment
```

2. 다음 명령어를 실행하여 샘플 코드 SampleEnclave를 컴파일합니다.



```
cd /opt/intel/sgxsdk/SampleCode/SampleEnclave && make
```

3. 다음 명령어를 실행하여 컴파일된 실행 파일을 실행합니다.



```
./app
```

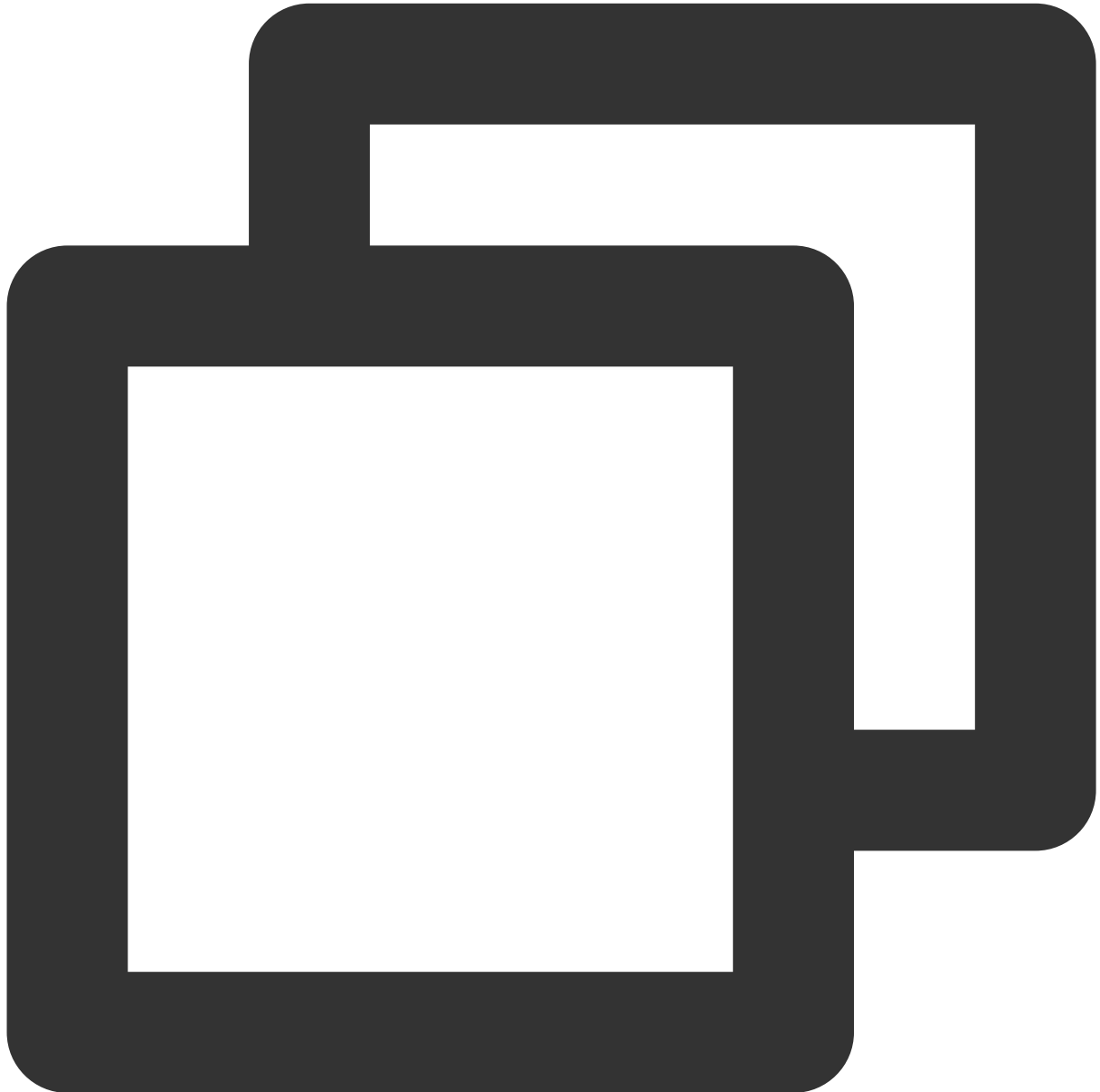
아래 이미지와 같은 결과가 반환되면 실행이 완료된 것입니다.

```
[root@VM-8-14-centos SampleEnclave]# ./app
Checksum(0x0x7ffcb9b49a30, 100) = 0xfffd4143
Info: executing thread synchronization, please wait...
Info: SampleEnclave successfully returned.
Enter a character before exit ...
```

예시2: SGX 원격 증명

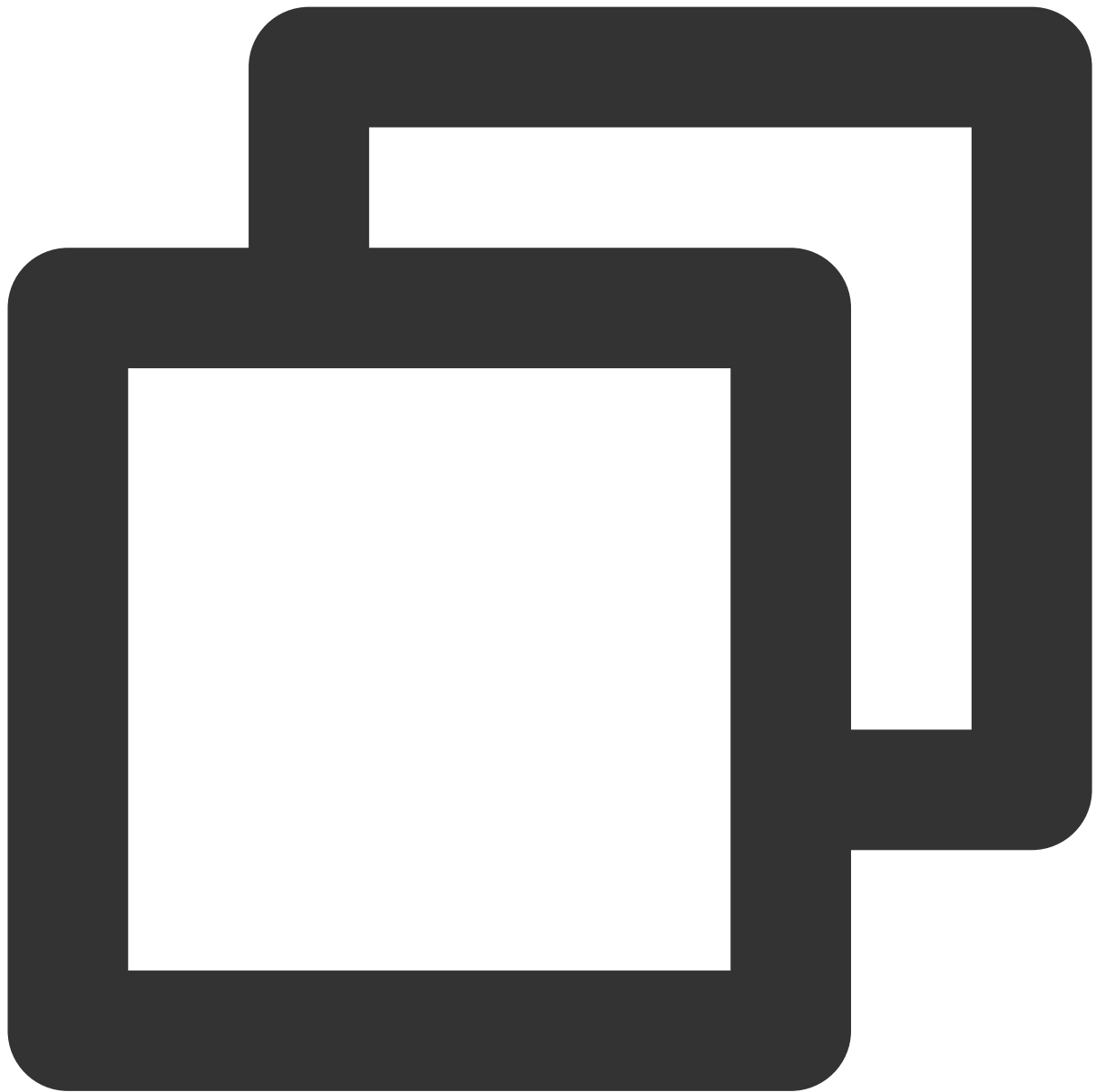
Intel sgx의 code tree는 SGX 원격 증명 기능(DCAP)을 인증하기 위한 샘플 코드를 제공합니다. 이 예시는 Quote 생성 및 인증을 위한 것으로, Quote 생성(QuoteGenerationSample) 및 Quote 인증(QuoteVerificationSample)을 포함합니다.

1. 다음 명령어를 실행하여 intel SGXSDK 관련 환경 변수를 설정합니다.

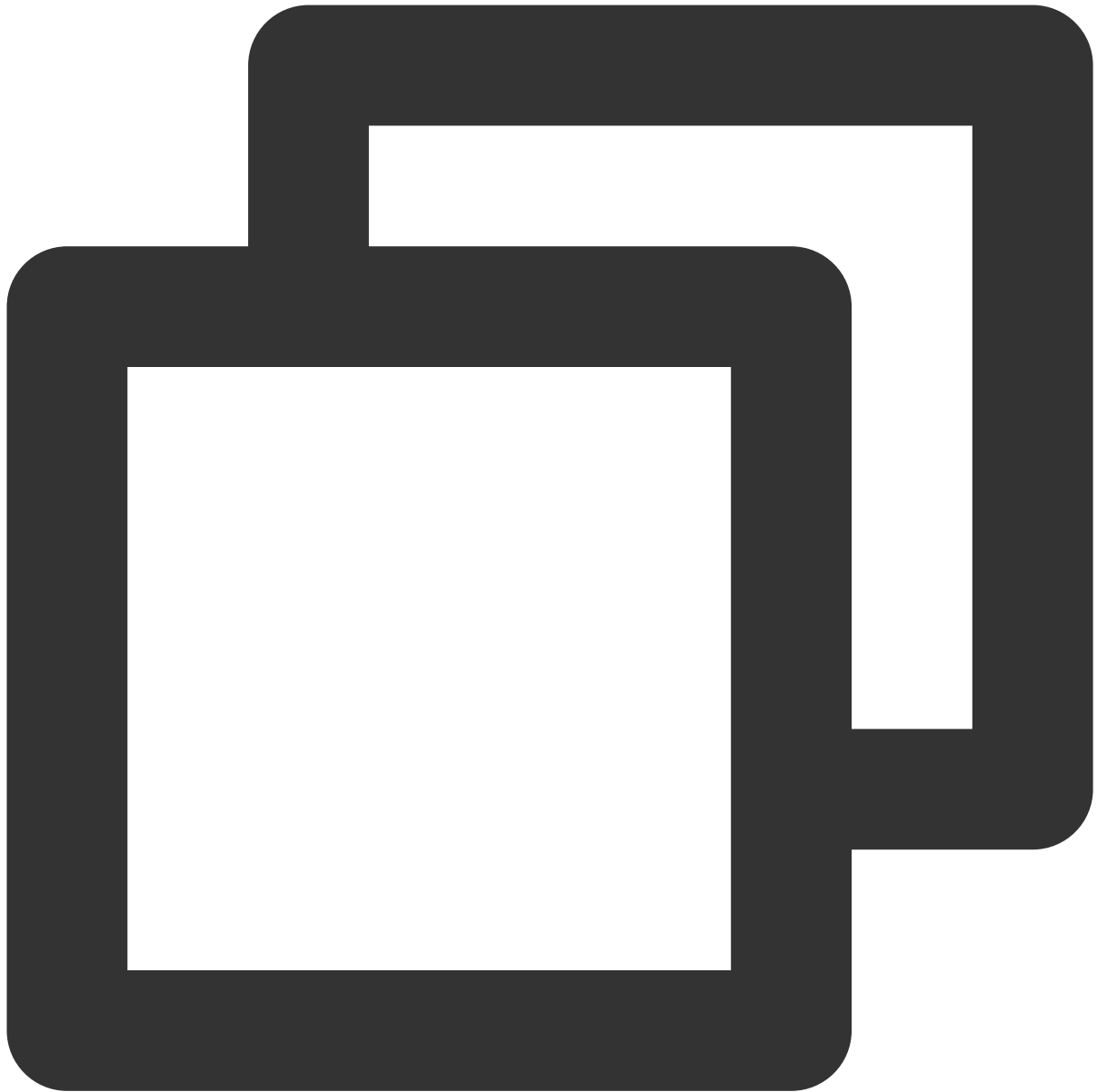


```
source /opt/intel/sgxsdk/environment
```

2. 다음 명령어를 순서대로 실행하여 git을 설치하고 intel sgx DCAP code tree를 다운로드합니다.



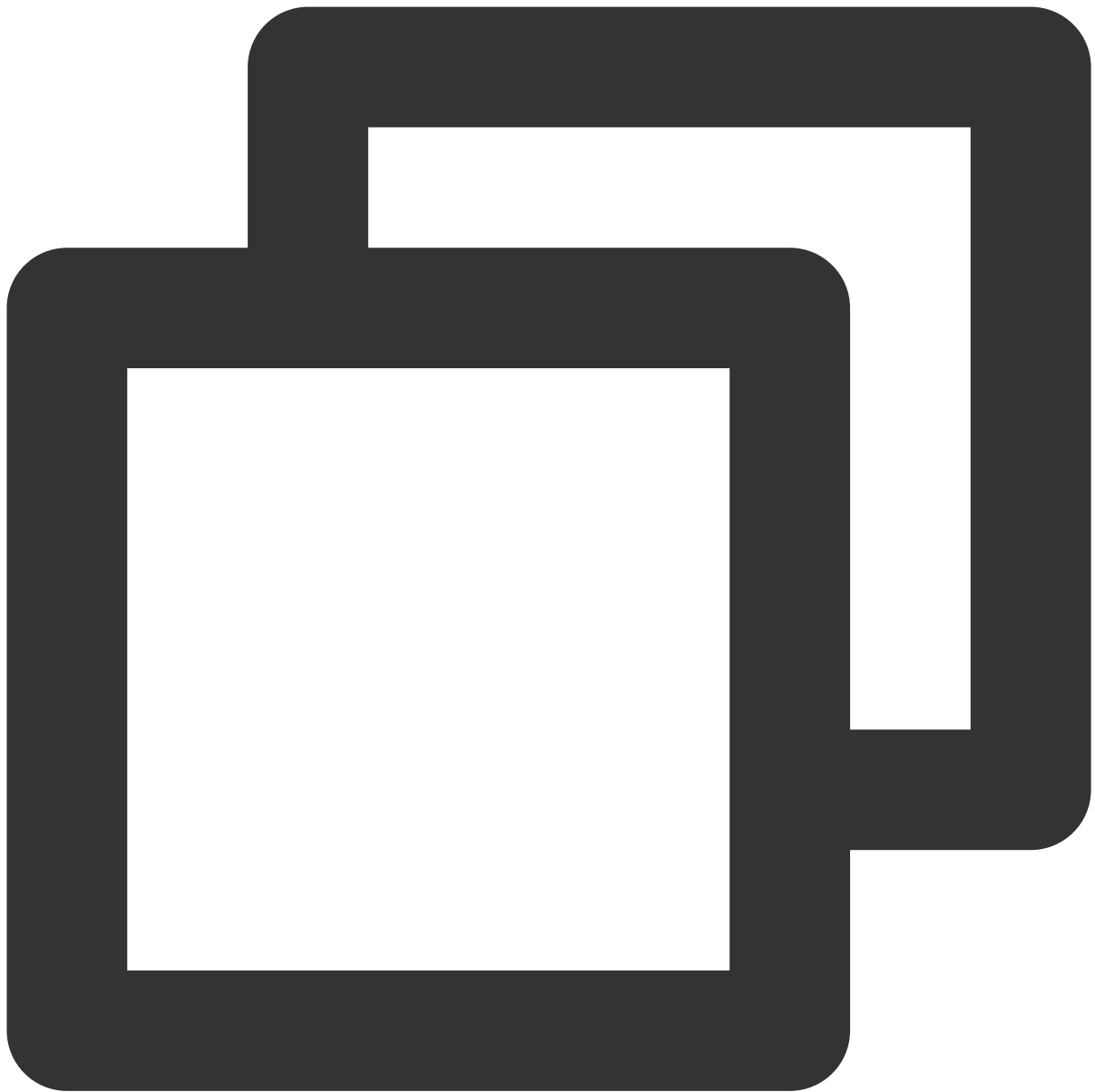
```
cd /root && yum install git
```

```
git clone https://github.com/intel/SGXDataCenterAttestationPrimitives.git
```

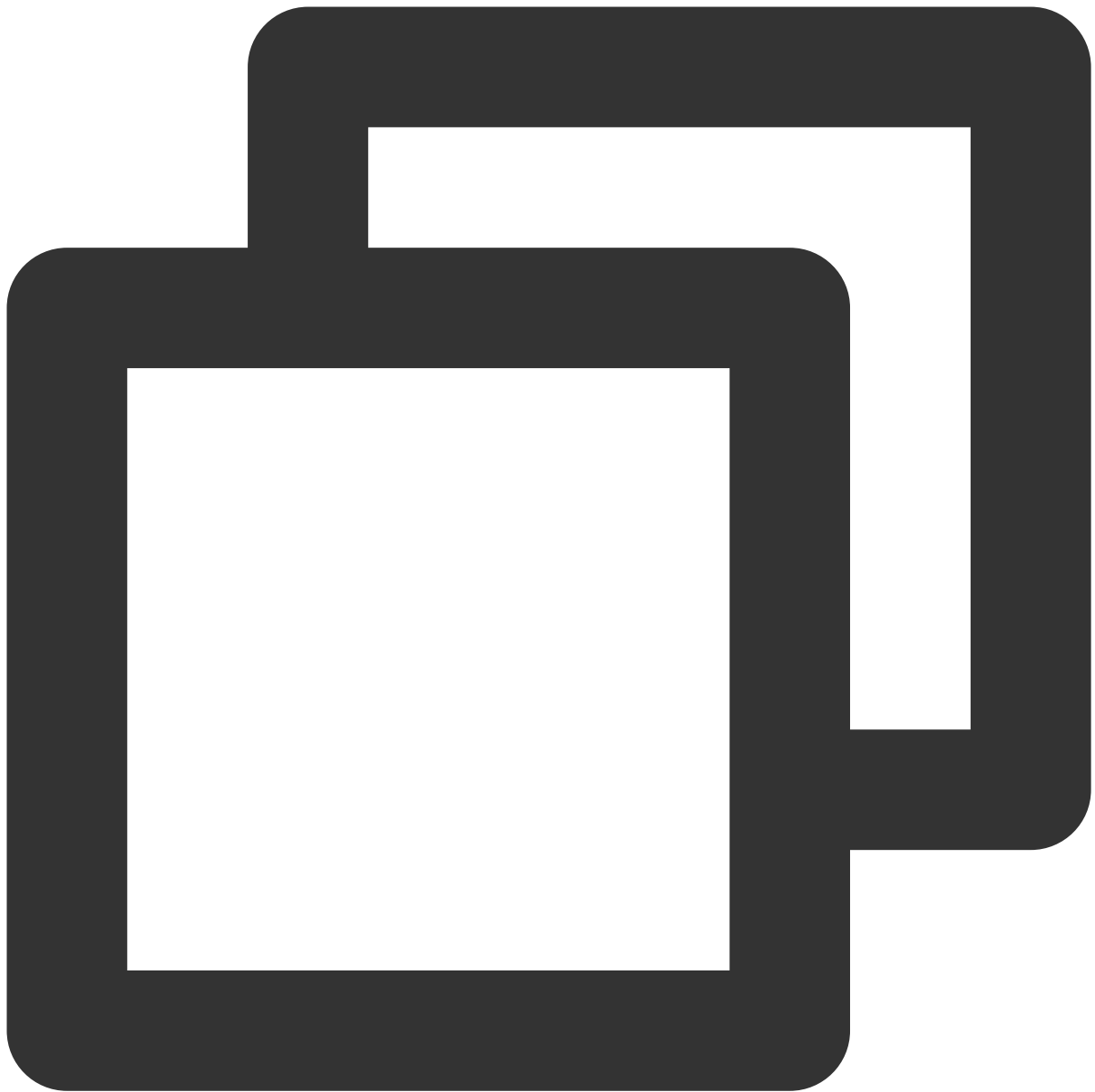
3. 다음 명령어를 순서대로 실행하여 Quote 생성의 QuoteGenerationSample 샘플 코드를 컴파일하고 실행합니다.

3.1 QuoteGenerationSample 디렉터리를 입력합니다.



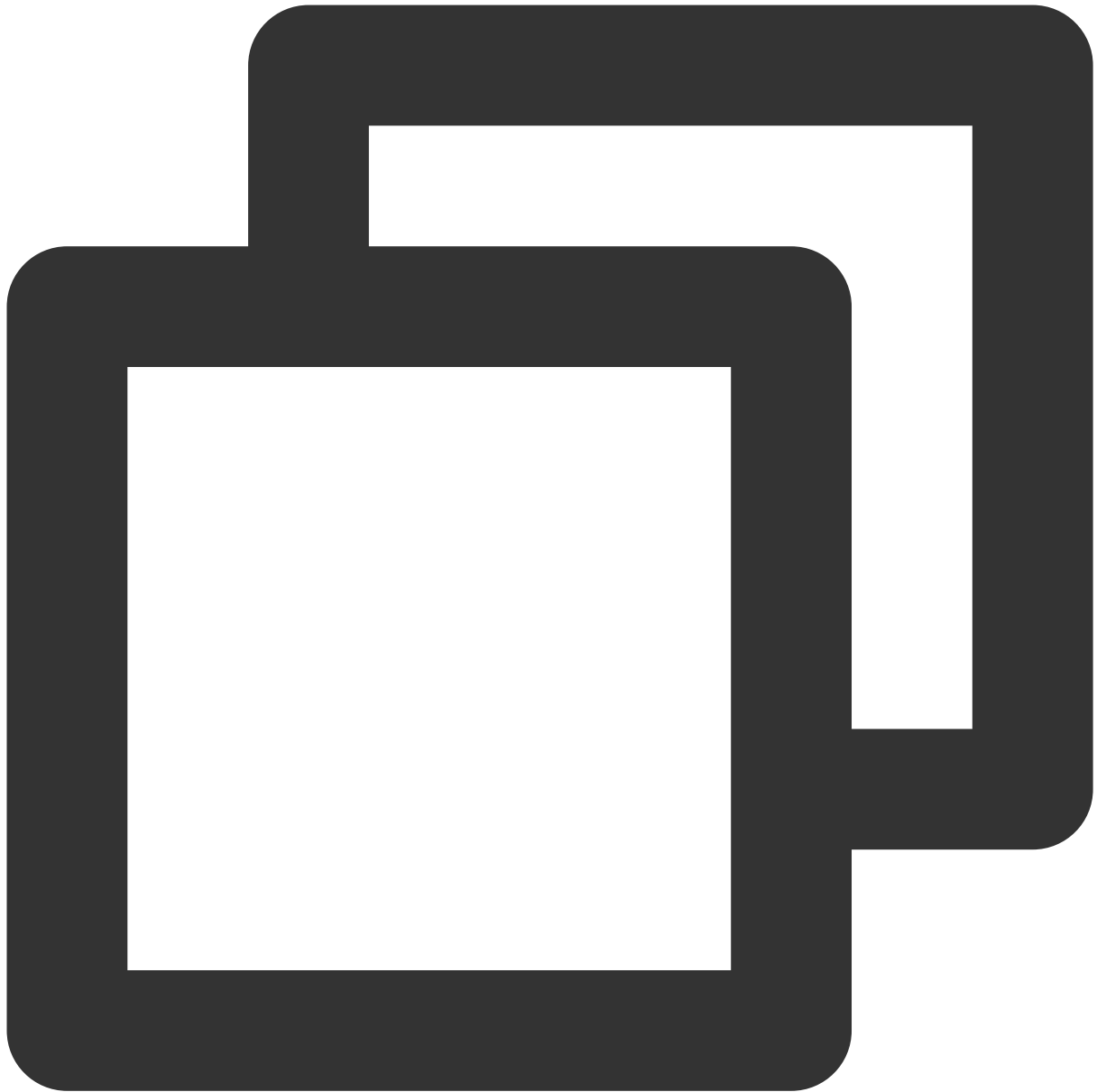
```
cd /root/SGXDataCenterAttestationPrimitives/SampleCode/QuoteGenerationSample
```

3.2 QuoteGenerationSample을 컴파일합니다.



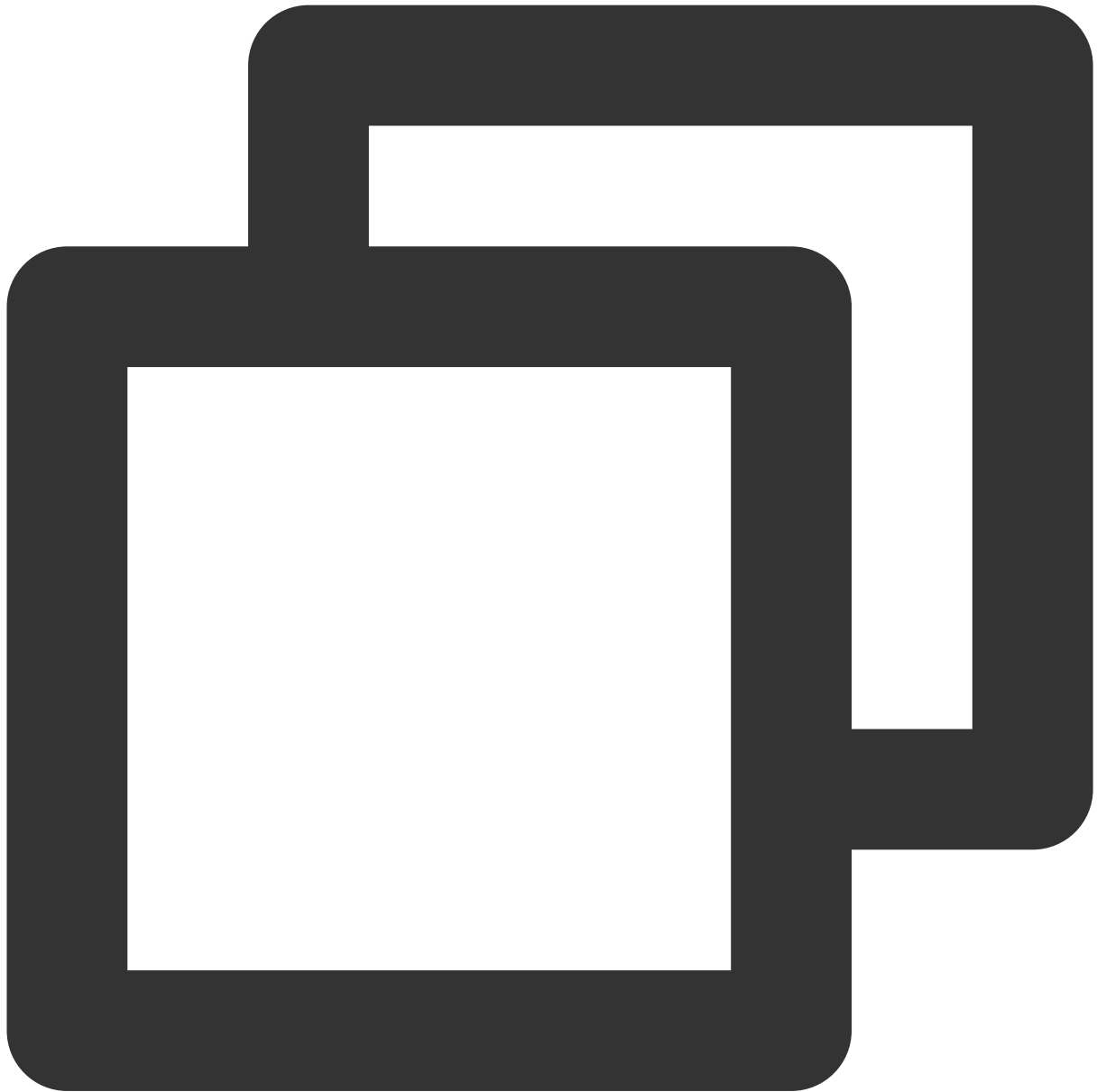
```
make
```

3.3 QuoteGenerationSample을 실행하고 Quote를 생성합니다.



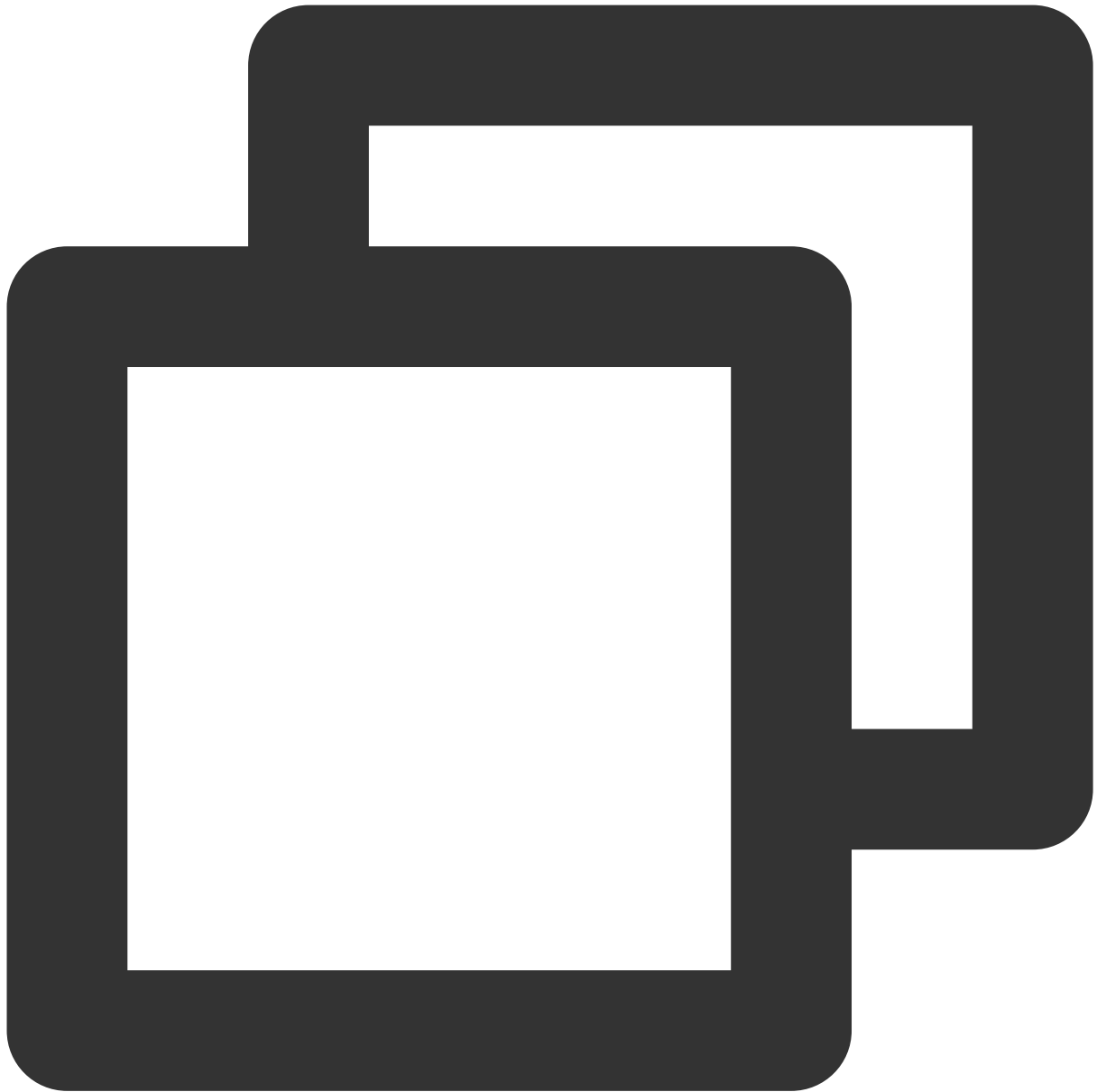
```
./app
```

4. 다음 명령어를 실행하여 Quote 인증의 QuoteVerificationSample 샘플 코드를 컴파일합니다.



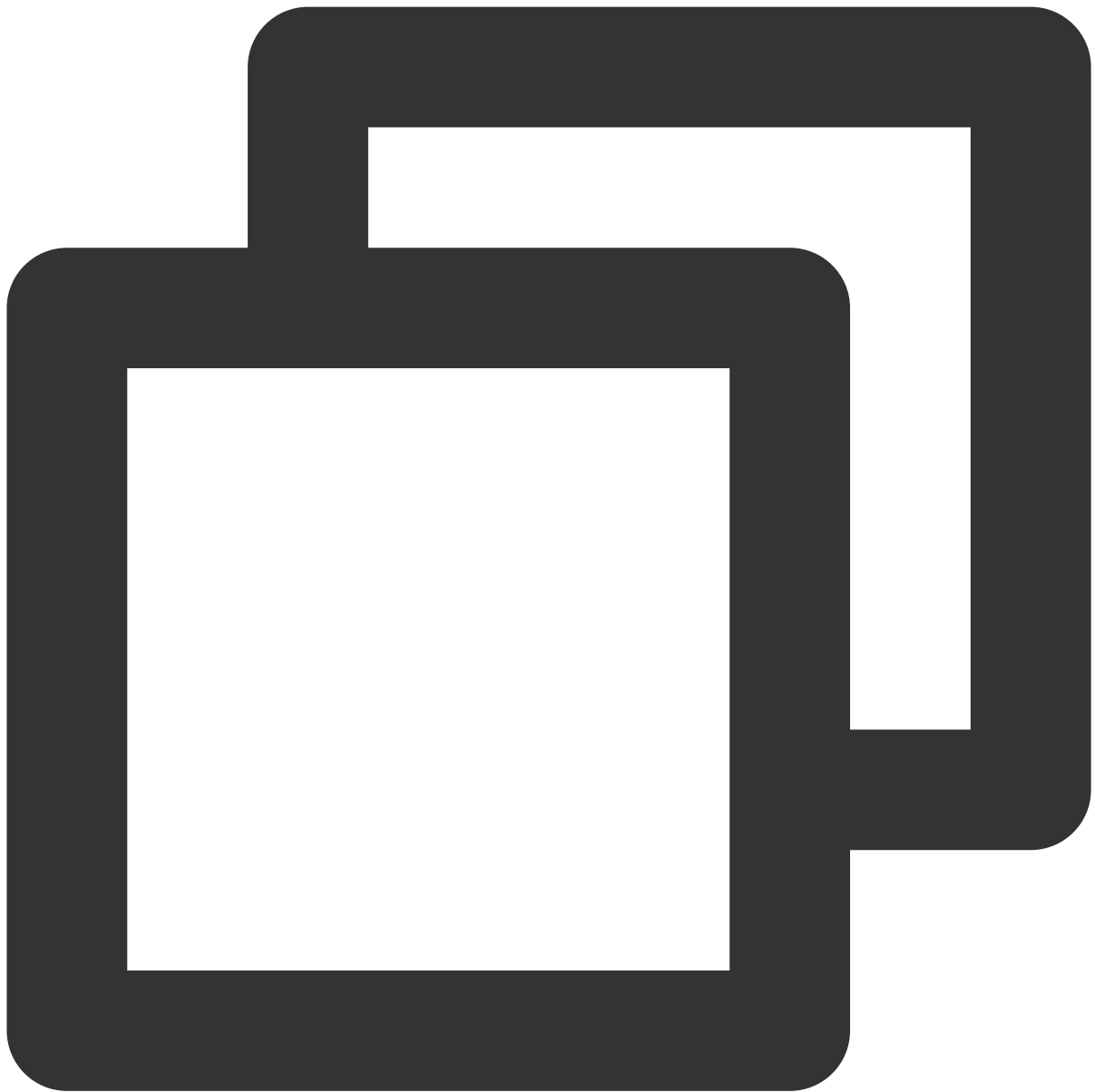
```
cd /root/SGXDataCenterAttestationPrimitives/SampleCode/QuoteVerificationSample && m
```

5. 다음 명령어를 실행하여 QuoteVerificationSample Enclave에 서명을 진행합니다.



```
sgx_sign sign -key Enclave/Enclave_private_sample.pem -enclave enclave.so -out encl
```

6. 다음 명령어를 통해 QuoteVerificationSample을 실행하여 Quote를 확인합니다.



```
./app
```

아래 이미지와 같은 결과가 반환되면 인증이 완료된 것입니다.

```
[root@VM-8-14-centos QuoteVerificationSample]# ./app
Info: ECDSA quote path: ../QuoteGenerationSample/quote.dat

Trusted quote verification:
Info: get target info successfully returned.
Info: sgx_qv_set_enclave_load_policy successfully returned.
Info: sgx_qv_get_quote_supplemental_data_size successfully returned.
Info: App: sgx_qv_verify_quote successfully returned.
Info: Ecall: Verify QvE report and identity successfully returned.
Info: App: Verification completed successfully.
Info: Supplemental data version: 3

=====

Untrusted quote verification:
Info: sgx_qv_get_quote_supplemental_data_size successfully returned.
Info: App: sgx_qv_verify_quote successfully returned.
Info: App: Verification completed successfully.
Info: Supplemental data version: 3
```


M6p 인스턴스 영구 메모리 설정

최종 업데이트 날짜: : 2024-02-02 11:01:47

작업 시나리오

본문은 M6p 인스턴스에서 영구 메모리를 설정하는 방법을 설명합니다.

인스턴스 설정

본문은 다음과 같이 설정된 CVM 인스턴스를 예시로 들고 있습니다. 적용 시 실제 조건을 기준으로 하십시오.

인스턴스 사양: 메모리형 M6p 인스턴스 M6p.LARGE16(4코어 16GB). 기타 사양 및 설정은 [메모리형 M6p](#)를 참고하십시오.

운영 체제: TencentOS Server 3.1(TK4).

설명 :

인스턴스에서 다음 운영 체제를 사용할 것을 권장합니다.

TencentOS Server 3.1

CentOS 7.6CentOS 7.6 이상 버전

Ubuntu 18.10 이상 버전

전제 조건

[M6p 인스턴스](#) 생성 및 로그인 완료되어있어야 합니다.

인스턴스 생성 방법은 [구매 페이지를 통한 인스턴스 생성](#)을 참고하십시오.

인스턴스 로그인 방법은 [Linux 인스턴스에 로그인](#)을 참고하십시오.

Intel® Optane™ DC BPS 하드웨어(PMEM) 모드 소개

Memory 모드

Memory 모드에서는 기존 DRAM이 가장 자주 액세스되는 데이터의 캐시 역할을 하는 반면, 영구 메모리는 백업 메모리로 사용되며, 캐시 관리 작업은 메모리 컨트롤러에서 자동으로 처리됩니다.

AD 모드

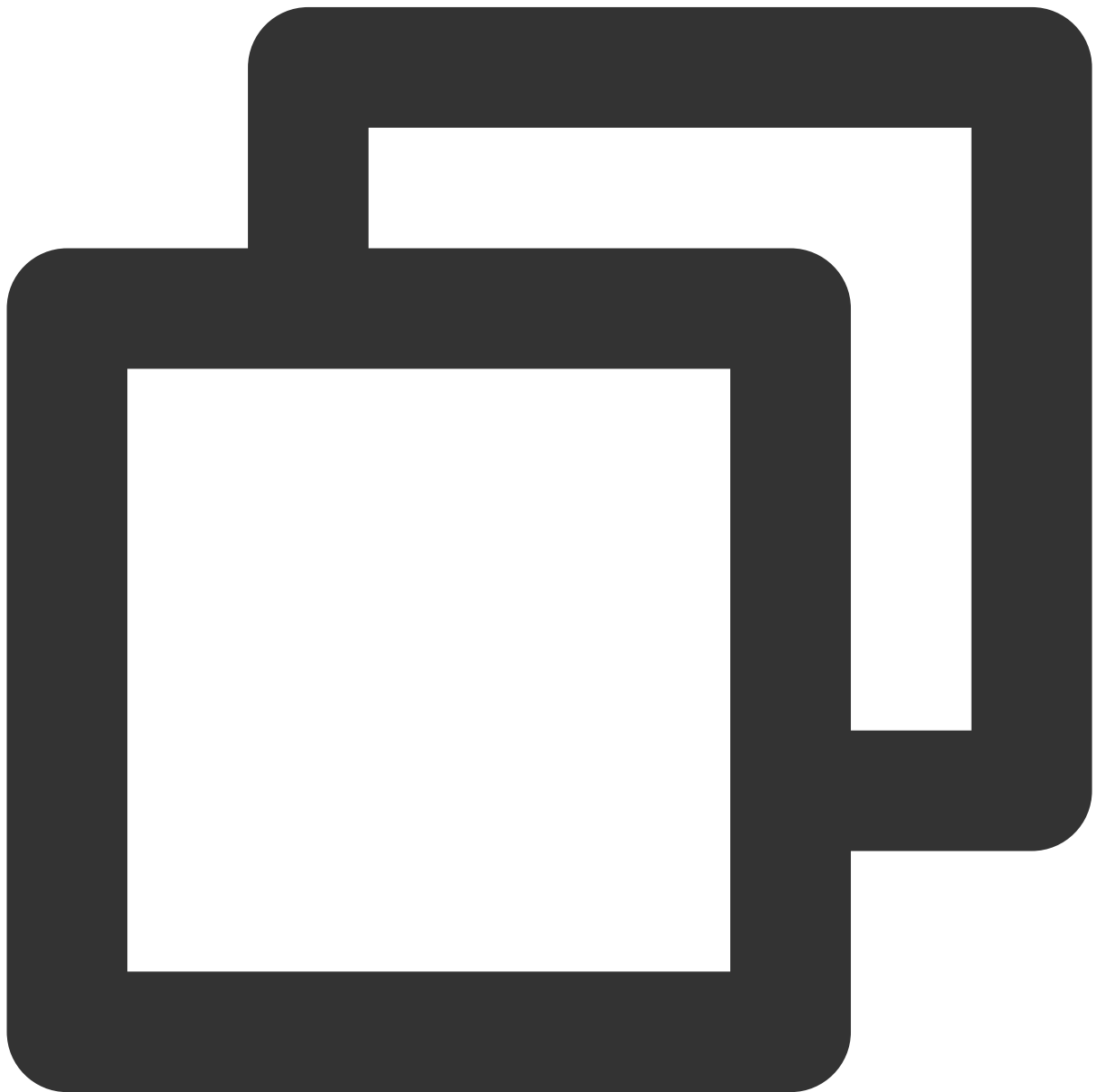
M6p 모델은 이 모드를 채택하고 있습니다. M6p 모델에서 플랫폼 측은 BPS 하드웨어를 AD 모드로 설정하고, CVM에 전송하여 사용하도록 합니다. AD 모드에서 애플리케이션은 PMEM 장치를 메모리 또는 로컬 SSD 디스크로 사용할

수 있습니다.

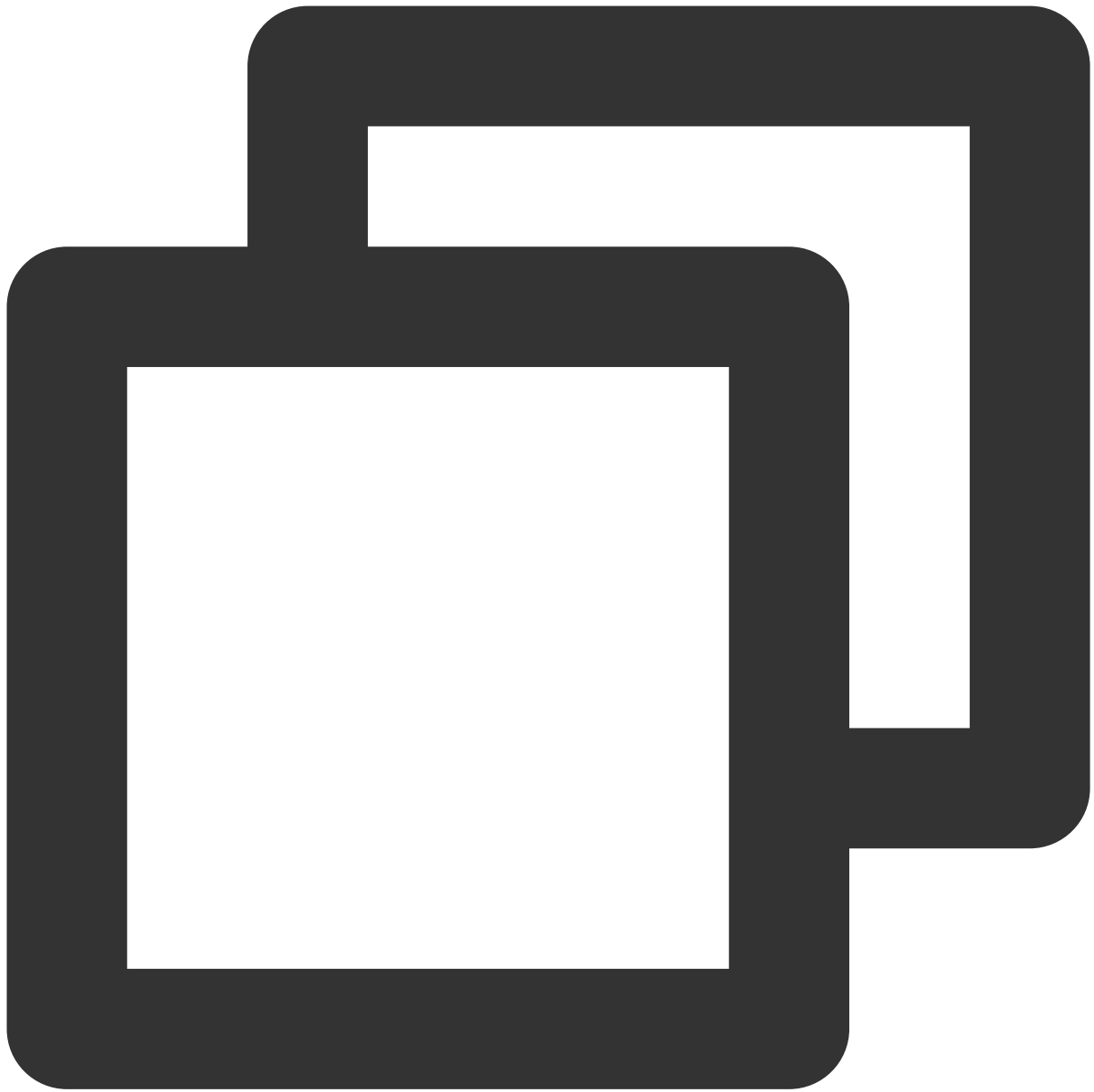
작업 단계

PMEM 초기화

인스턴스를 처음 사용하는 경우 다음 명령어를 순서대로 실행하여 PMEM 장치를 초기화합니다. 이미 PMEM 초기화한 경우 이 단계를 건너뛰십시오.



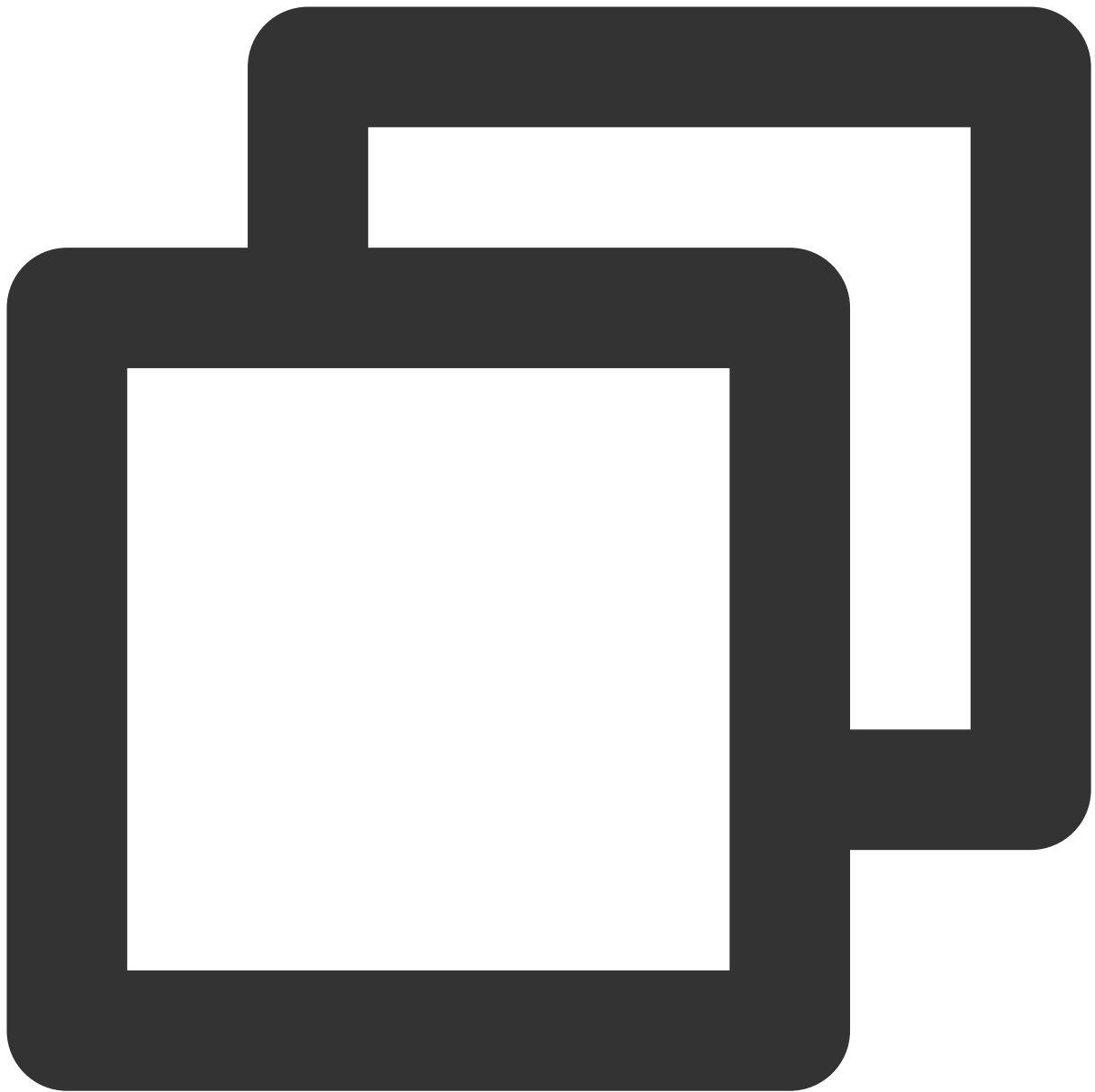
```
yum install -y ndctl
```



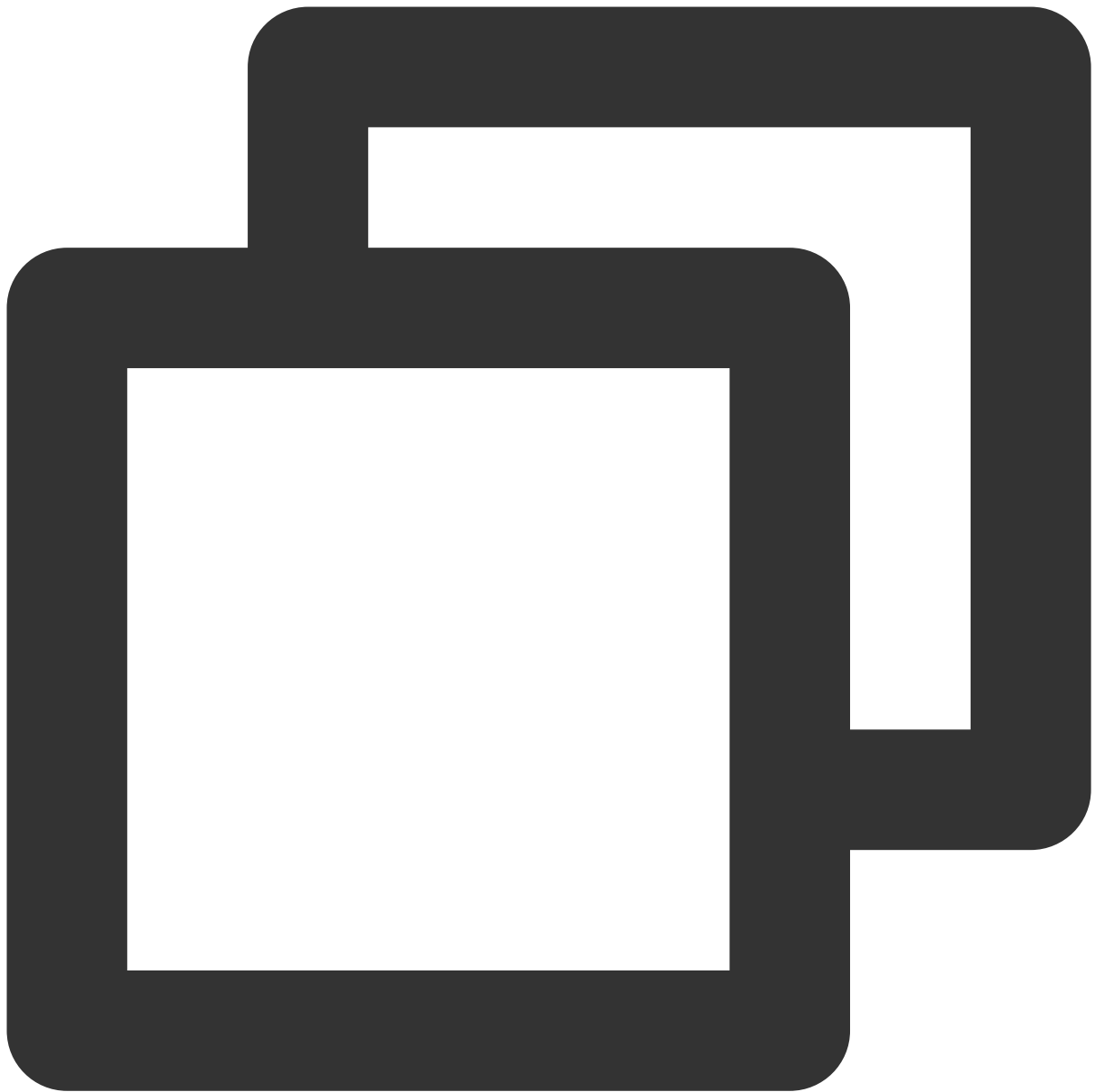
```
ndctl destroy-namespace all --force
```

설명 :

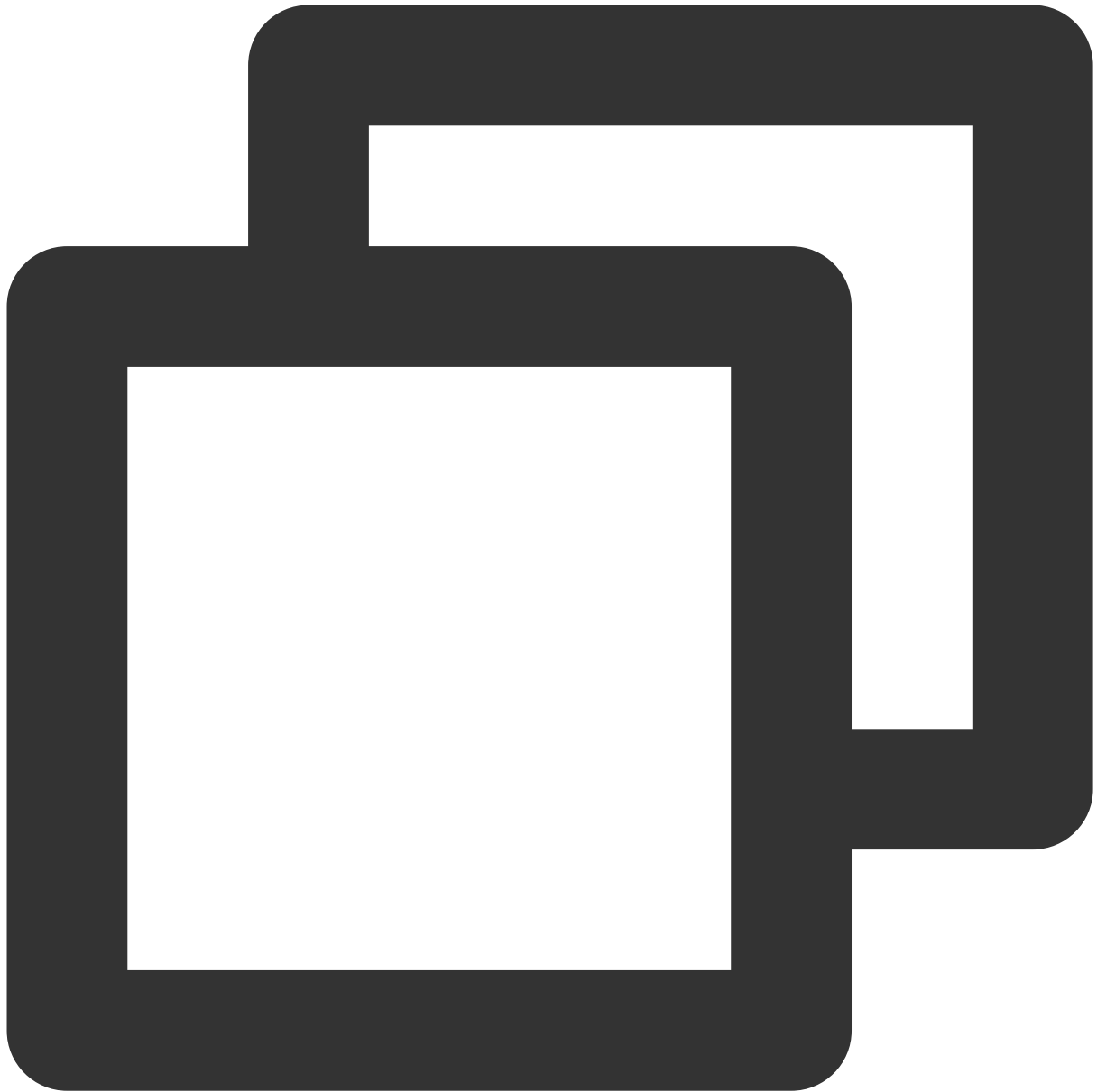
가장 큰 인스턴스에는 두 개의 region이 있습니다. 다음 명령어를 실행한 후 region0을 region1로 바꾸고 명령어를 다시 실행하십시오.



```
ndctl disable-region region0
```



```
ndctl init-labels all
```



```
ndctl enable-region region0
```

AD 모드에서 PMEM 설정

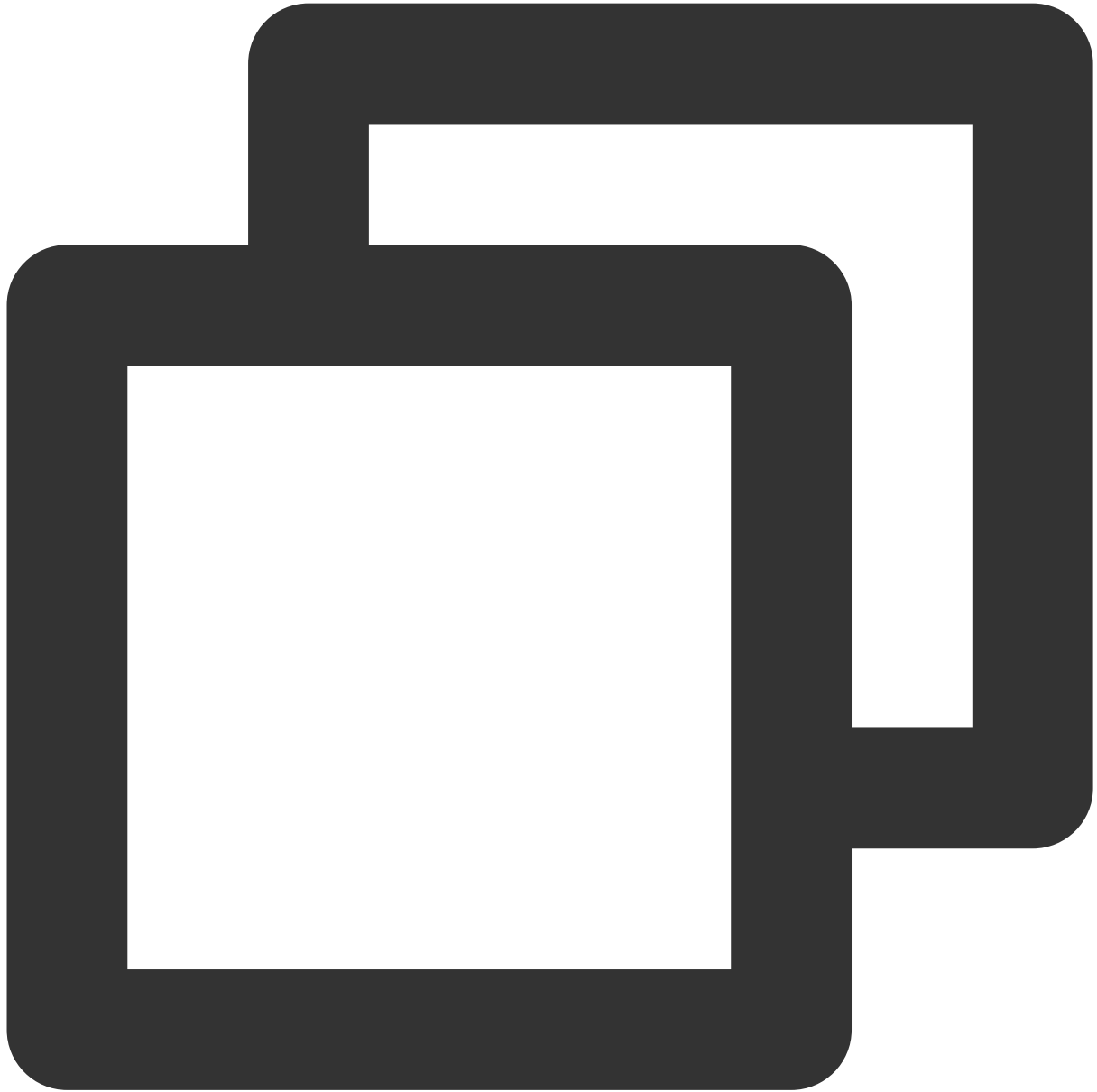
실제 필요에 따라 영구 메모리를 메모리 또는 로컬 SSD 디스크로 사용할 수 있습니다.

메모리로 사용

로컬 SSD 디스크로 사용

PMEM은 문자 장치로서 상위 애플리케이션 레이어(예시 **redis**)에 제공되어 영구 메모리 할당을 진행할 수 있습니다. **memkind**와 같은 **PMDK** 프레임워크를 통해 사용할 수 있습니다. 설정 방법은 다음과 같습니다.

1. 다음 명령어를 실행하여 문자 장치를 생성합니다.

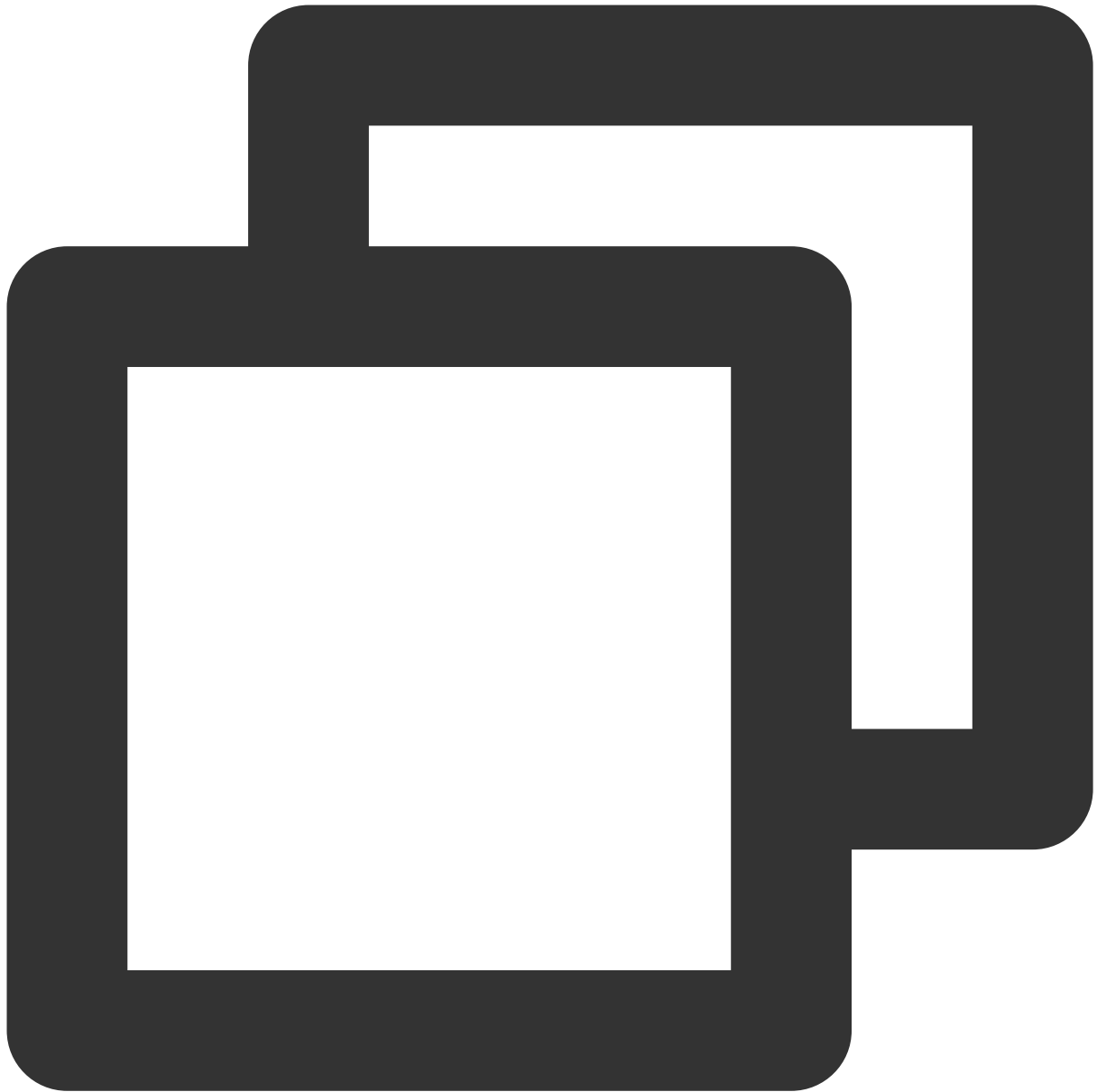


```
ndctl create-namespace -r region0 -m devdax
```

반환 결과가 아래 이미지와 같으면 'dax0.0' 문자 장치가 생성된 것입니다.

```
[root@VM-11-3-centos ~]# ndctl create-namespace -r region0 -m devdax
{
  "dev": "namespace0.0",
  "mode": "devdax",
  "map": "dev",
  "size": "61.04 GiB (65.54 GB)",
  "uuid": "71cceaeb-0ada-4fff-922b-2244f30f2e2f",
  "daxregion": {
    "id": 0,
    "size": "61.04 GiB (65.54 GB)",
    "align": 2097152,
    "devices": [
      {
        "chardev": "dax0.0",
        "size": "61.04 GiB (65.54 GB)",
        "target_node": 0,
        "mode": "devdax"
      }
    ]
  },
  "align": 2097152
}
```

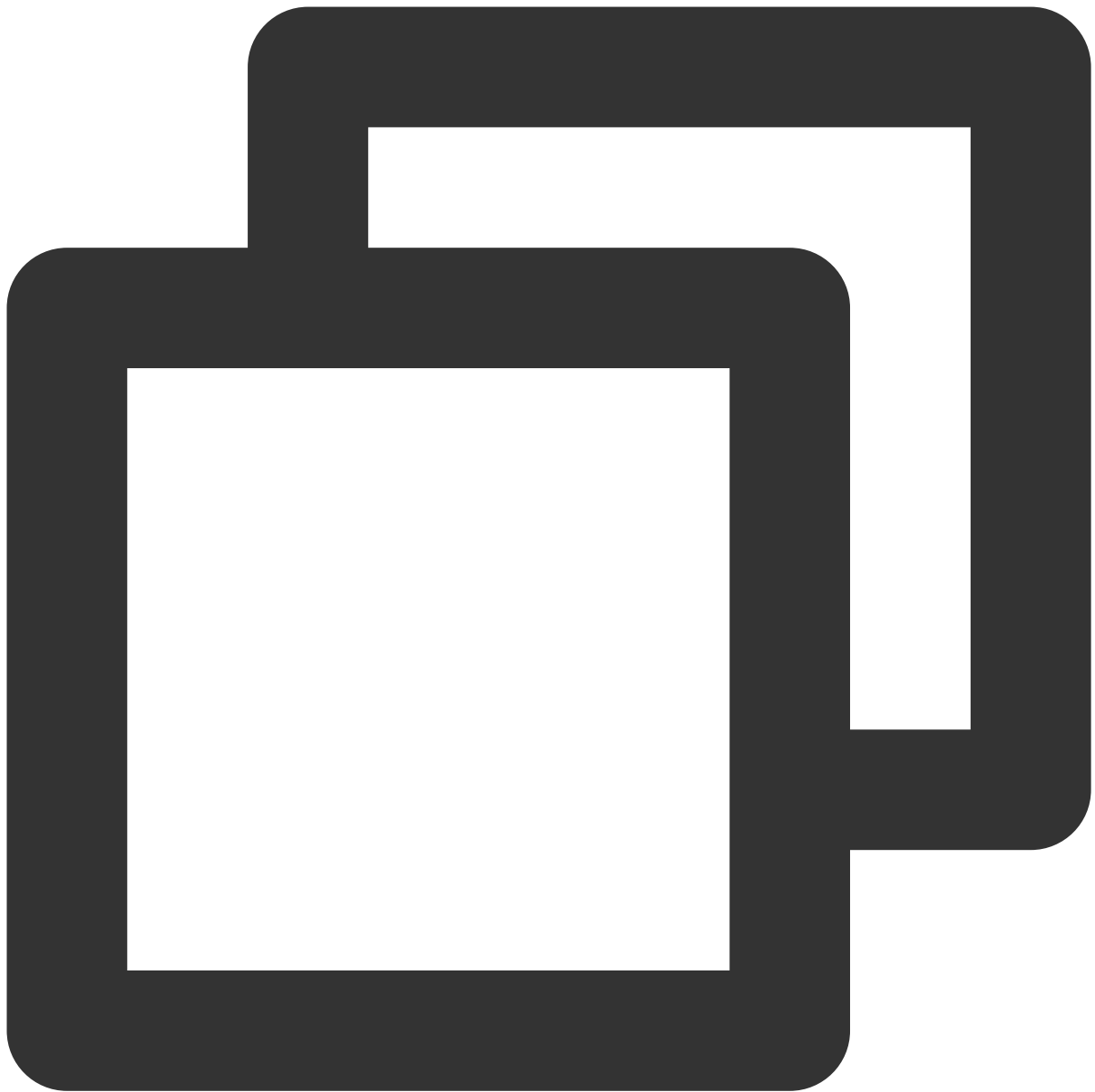
가장 큰 인스턴스에는 두 개의 region이 있으므로 가장 큰 인스턴스를 사용하는 경우 다음 명령어를 동시에 실행하십시오.



```
ndctl create-namespace -r region1 -m devdax -f
```

설정이 완료되면 `/dev` 디렉터리에 `dax0.0` 의 문자 장치가 생성되며, 이는 영구 메모리에 매핑될 수 있습니다.

2. 다음 명령어를 실행하여 영구 메모리 크기를 확인합니다.



```
ndctl list -R
```

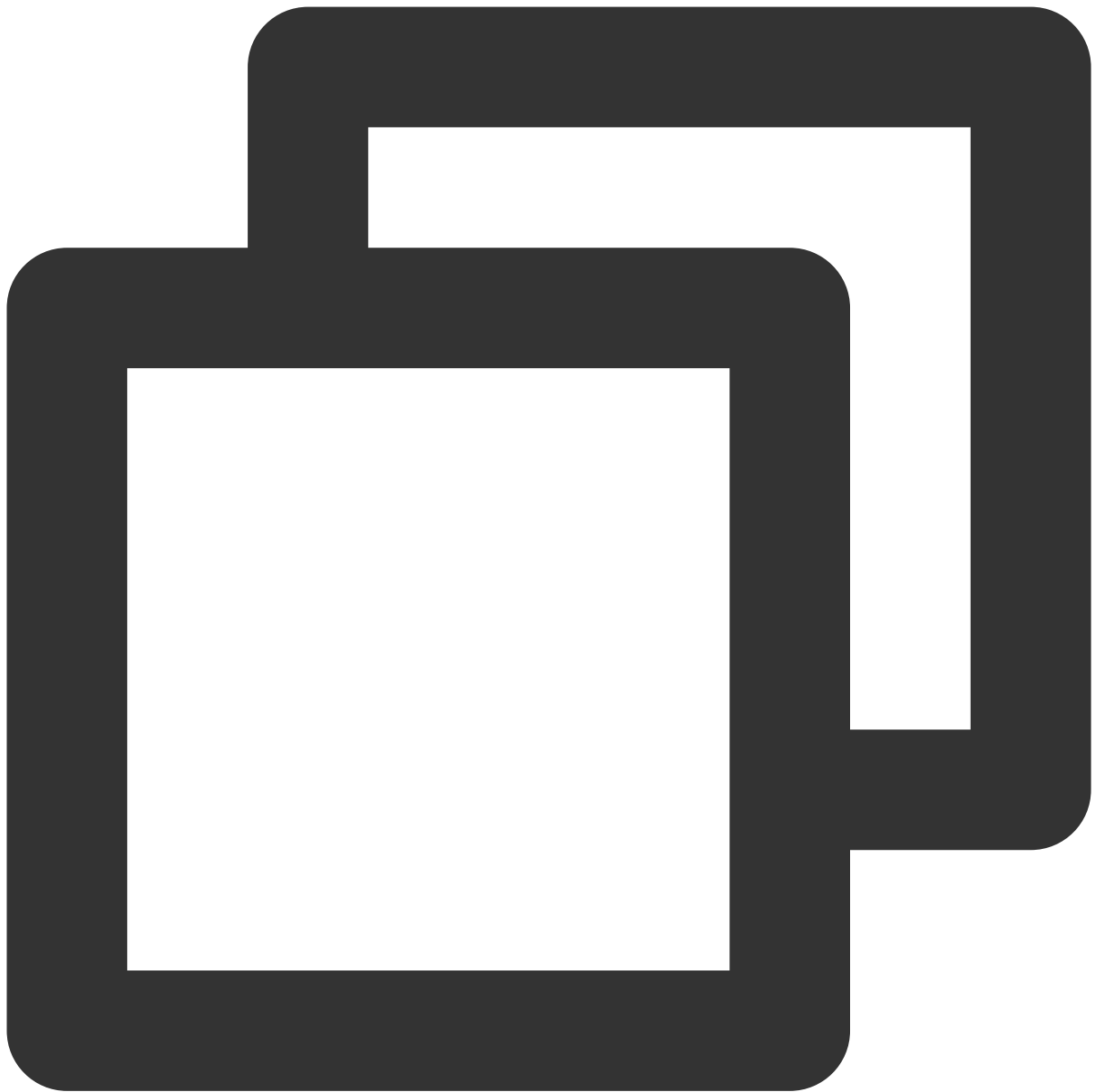
반환 결과는 다음 이미지와 같습니다.

```
[root@VM-11-3-centos ~]# ndctl list -R
[
  {
    "dev": "region0",
    "size": 66584576000,
    "available_size": 0,
    "max_available_extent": 0,
    "type": "pmem",
    "iset_id": 10248187106440278,
    "persistence_domain": "memory_controller"
  }
]
```

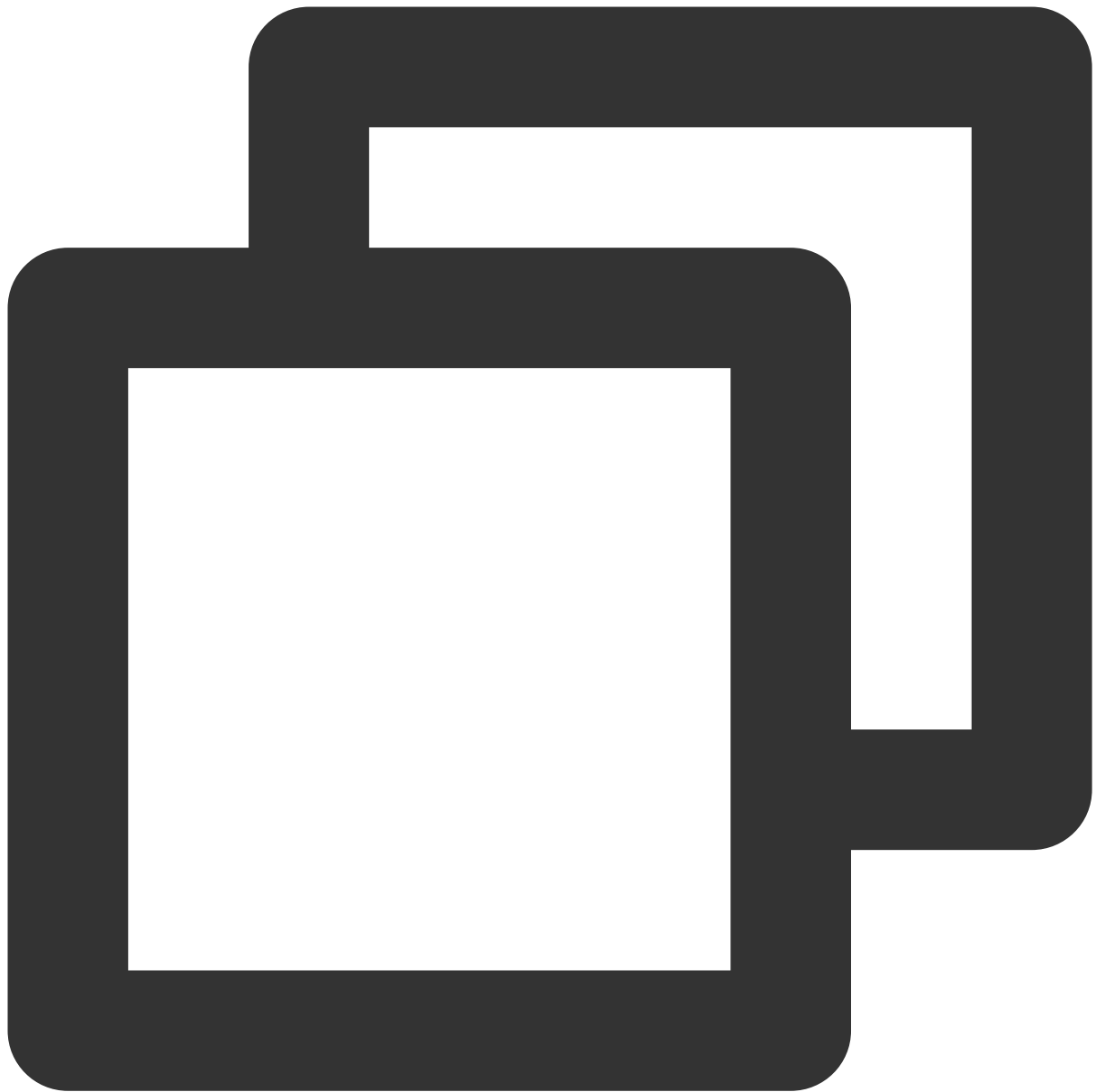
확장 기능(옵션)

이 단계를 통해 기능을 확장할 수 있습니다. 다음 명령어를 순서대로 실행하고 PMEM을 사용하여 CVM의 메모리를 확장합니다.

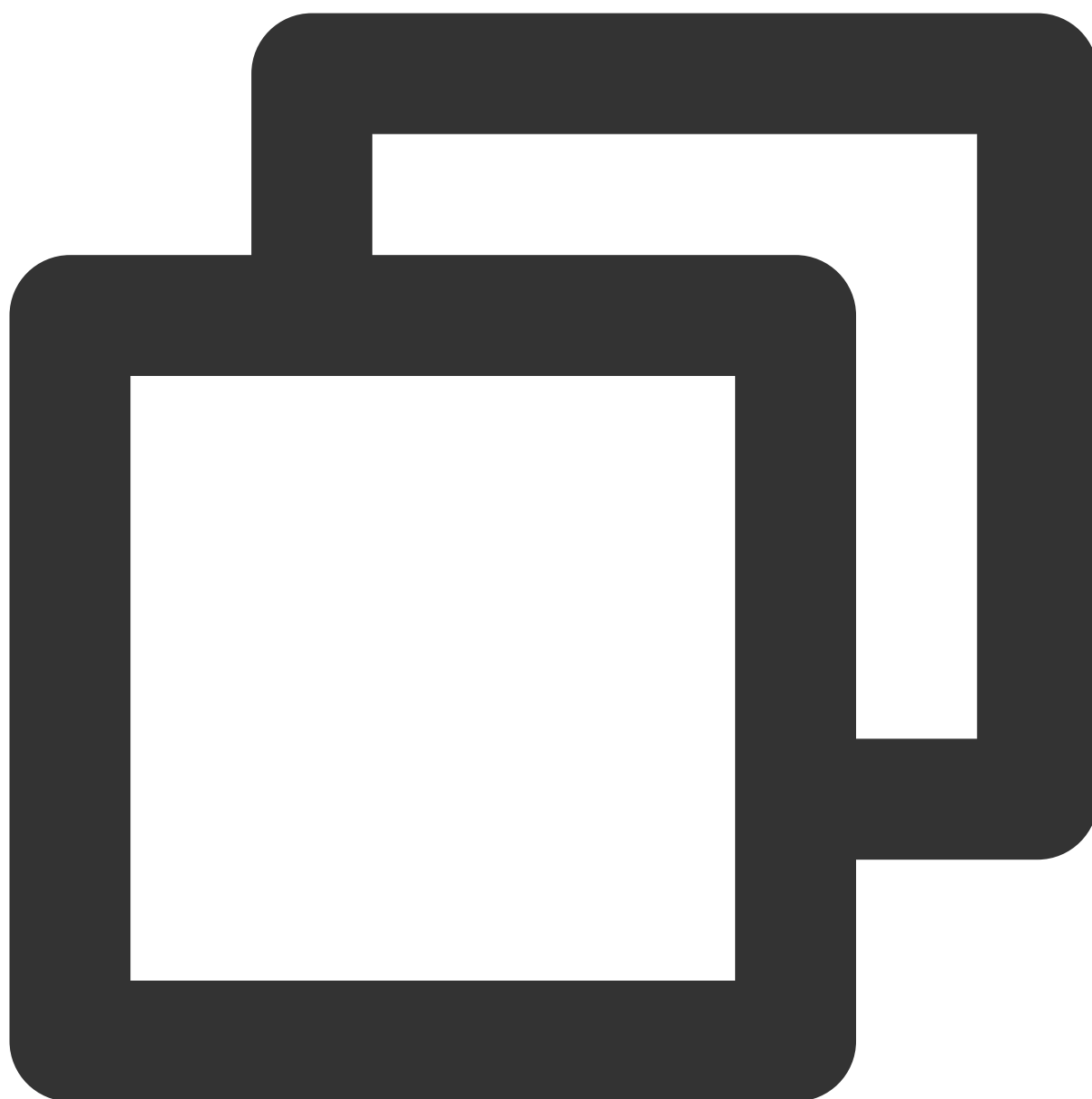
1. 상위 버전의 커널(5.1 이상 및 TencentOS Server 3.1 커널과 같은 KMEM DAX 드라이버 사용) 지원을 통해 devdax 모드의 PMEM을 kmemdax로 추가 설정할 수 있으며 PMEM을 사용하여 CVM의 메모리를 확장할 수 있습니다.



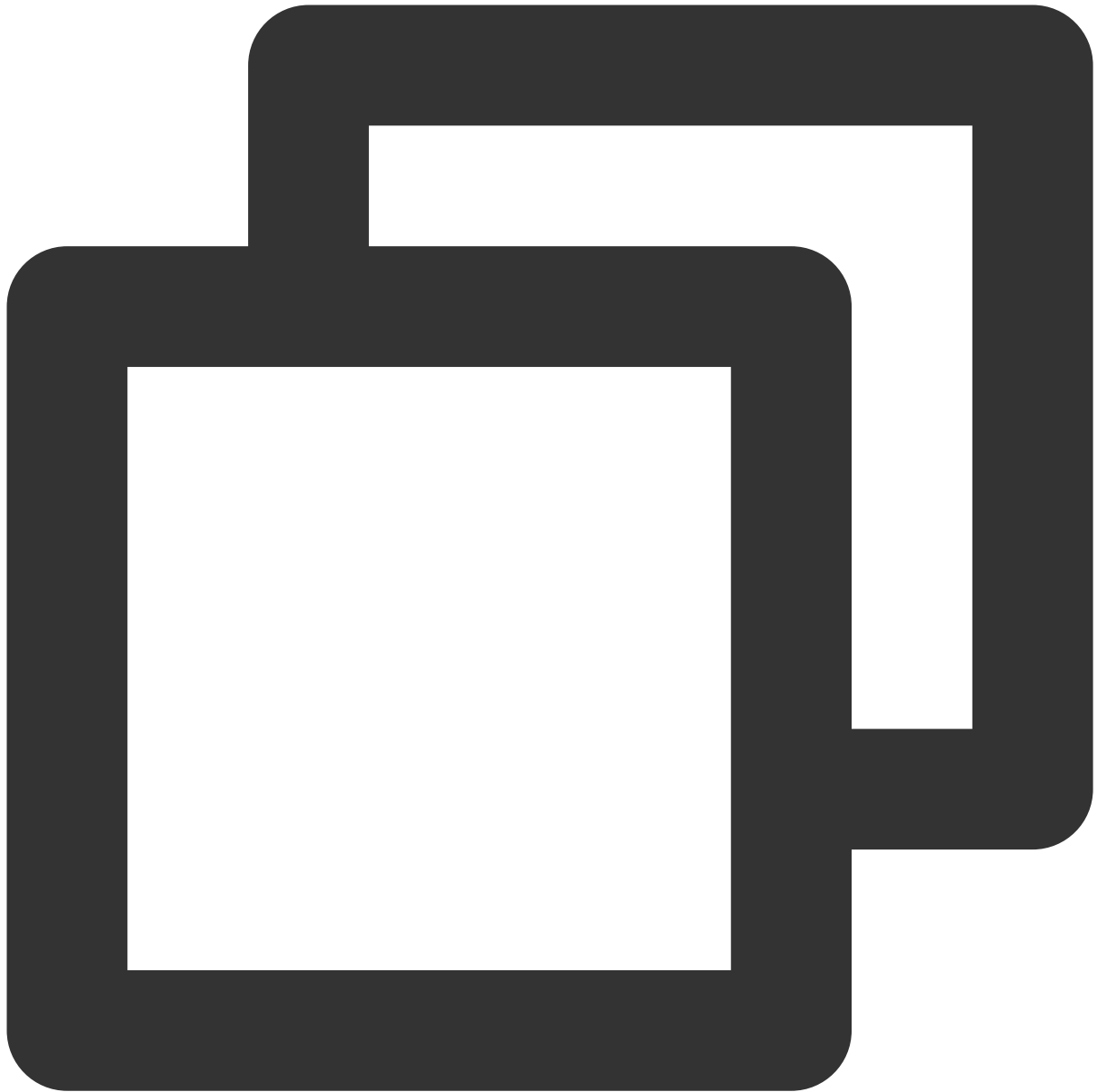
```
yum install -y daxctl
```



```
daxctl migrate-device-model
```



reboot

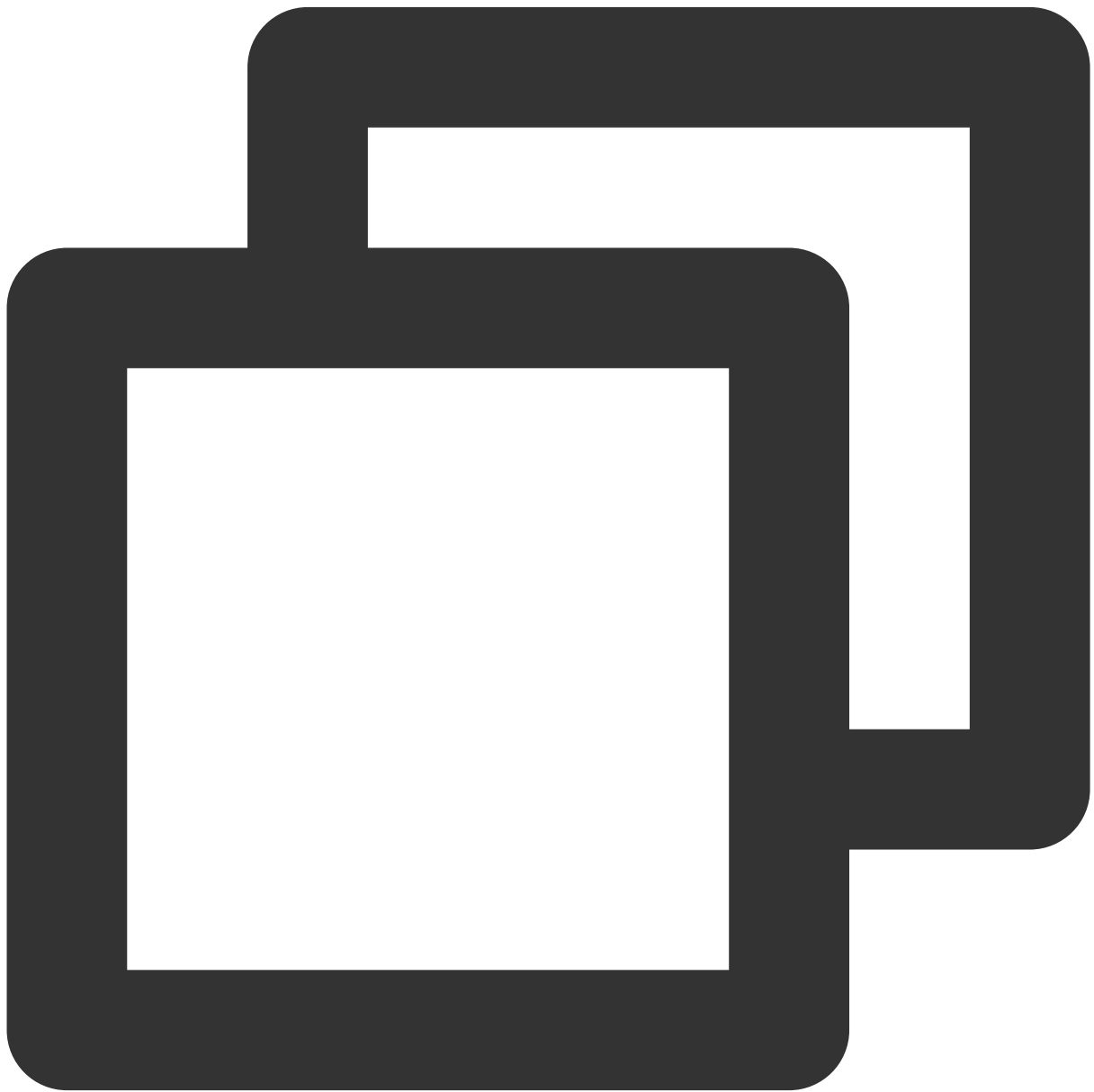


```
daxctl reconfigure-device --mode=system-ram --no-online dax0.0
```

반환 결과는 다음 이미지와 같습니다.

```
[root@VM-11-3-centos ~]# daxctl reconfigure-device --mode=system-ram --no-d
[
  {
    "chardev": "dax0.0",
    "size": 65542291456,
    "target_node": 0,
    "mode": "system-ram"
  }
]
```

2. 다음 명령어를 실행하여 시스템 메모리 확장을 확인합니다.



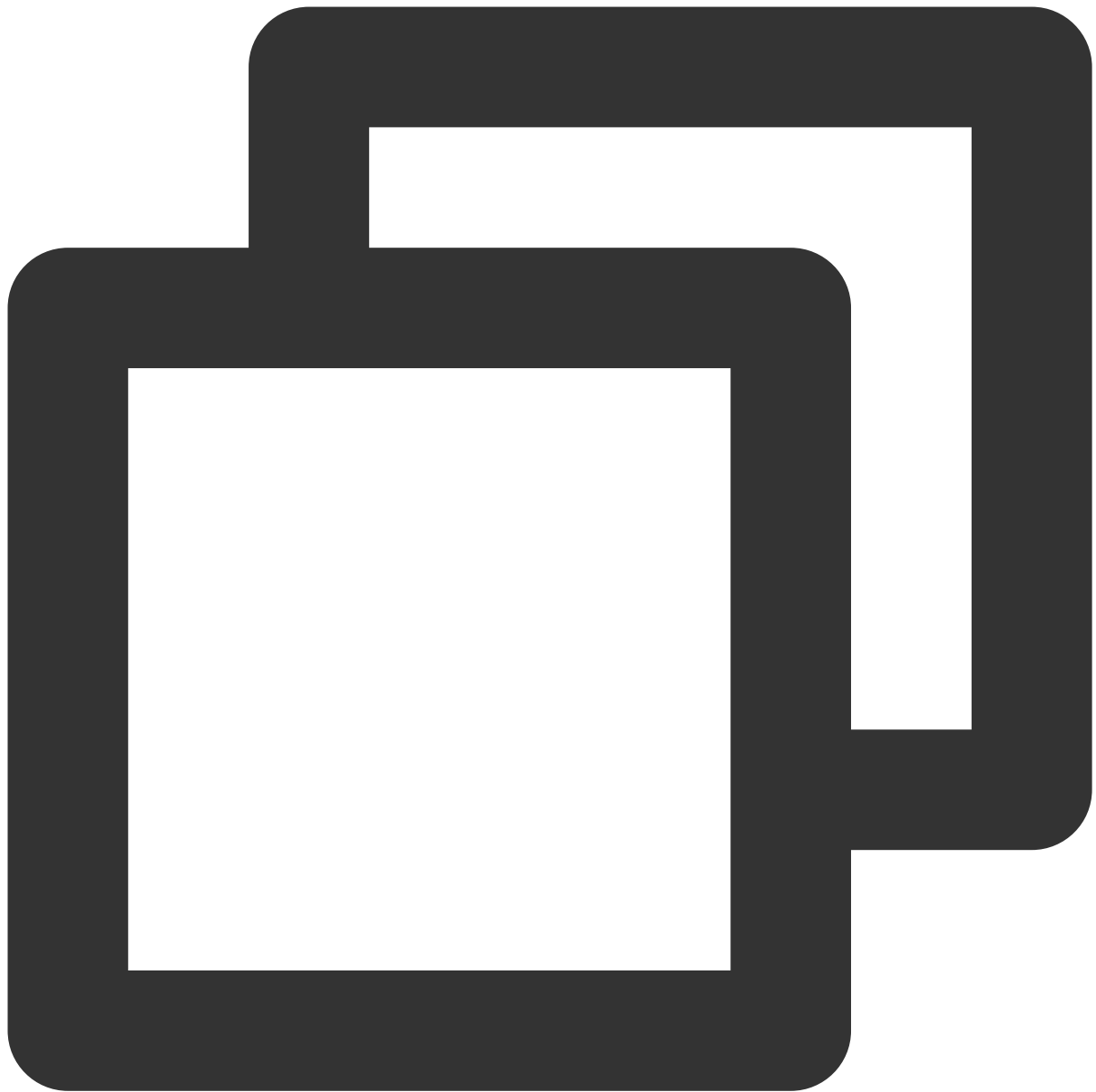

```
numactl -H
```

반환 결과는 다음 이미지와 같습니다.

```
[root@VM-11-3-centos ~]# numactl -H
available: 1 nodes (0)
node 0 cpus: 0 1 2 3
node 0 size: 77962 MB
node 0 free: 76586 MB
node distances:
node    0
 0:    10
```

AD 모드의 PMEM을 고속 블록 장치로 설정할 수도 있으며, 일반 블록 장치로 파일 시스템 생성, 베어 디스크 읽기/쓰기 등 작업을 할 수 있습니다. 설정 방법은 다음과 같습니다.

1. 다음 명령어를 실행하여 `/dev` 디렉터리에 `pmem0` 블록 장치를 생성합니다.

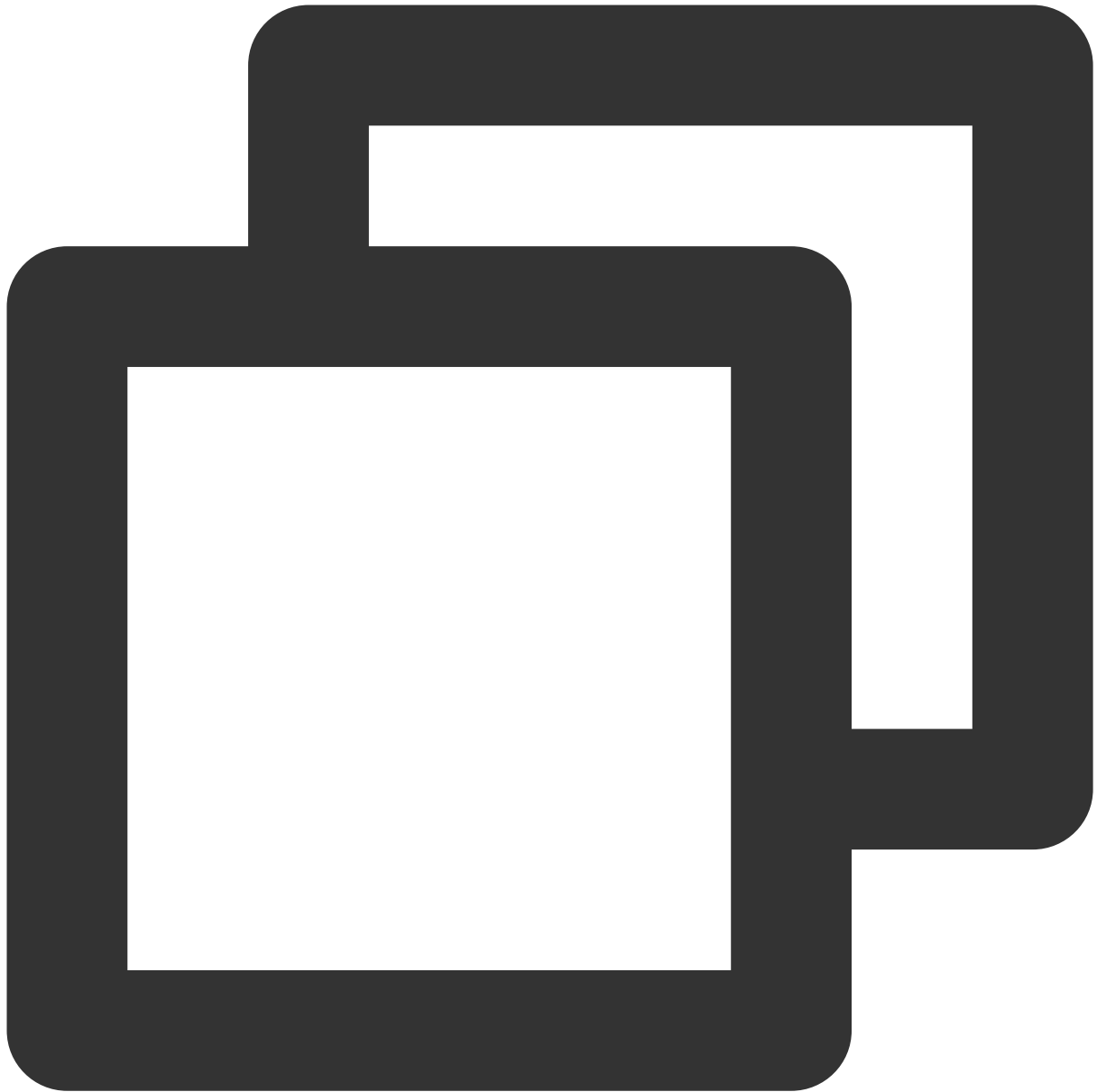


```
ndctl create-namespace -r region0 -m fsdax
```

반환 결과는 다음 이미지와 같습니다.

```
[root@VM-11-3-centos ~]# ndctl create-namespace -r region0 -m fsdax
{
  "dev": "namespace0.0",
  "mode": "fsdax",
  "map": "dev",
  "size": "61.04 GiB (65.54 GB)",
  "uuid": "2d7e4861-8052-47b2-9317-146b20890550",
  "sector_size": 512,
  "align": 2097152,
  "blockdev": "pmem0"
}
```

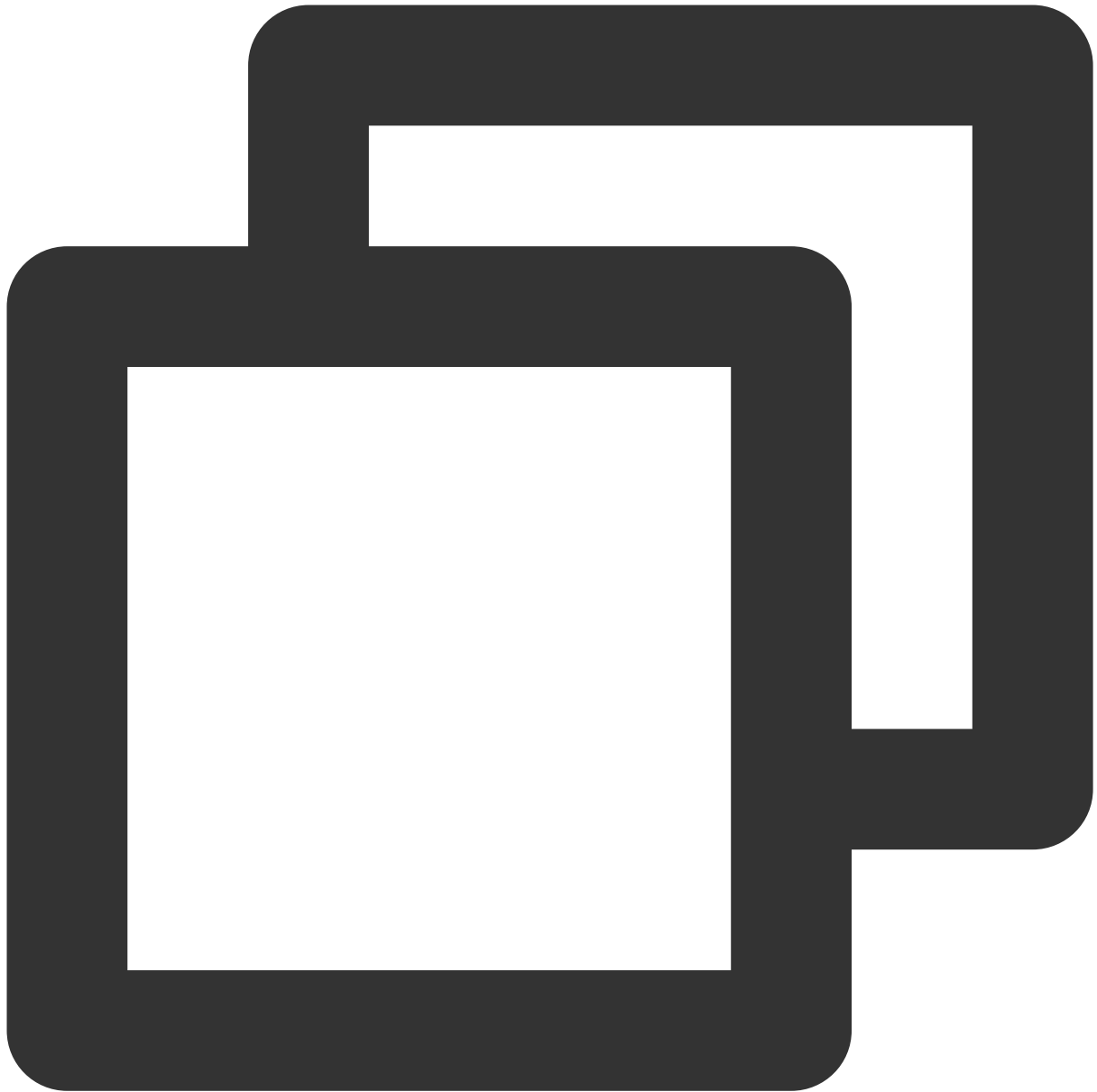
가장 큰 인스턴스에는 두 개의 region이 있으므로 가장 큰 인스턴스를 사용하는 경우 다음 명령어를 동시에 실행하십시오.



```
ndctl create-namespace -r region1 -m fsdax -f
```

2. 다음 명령어를 순서대로 실행하여 파일 시스템을 생성하거나 마운트하여 사용할 수 있습니다.

2.1 파일 시스템을 생성합니다.



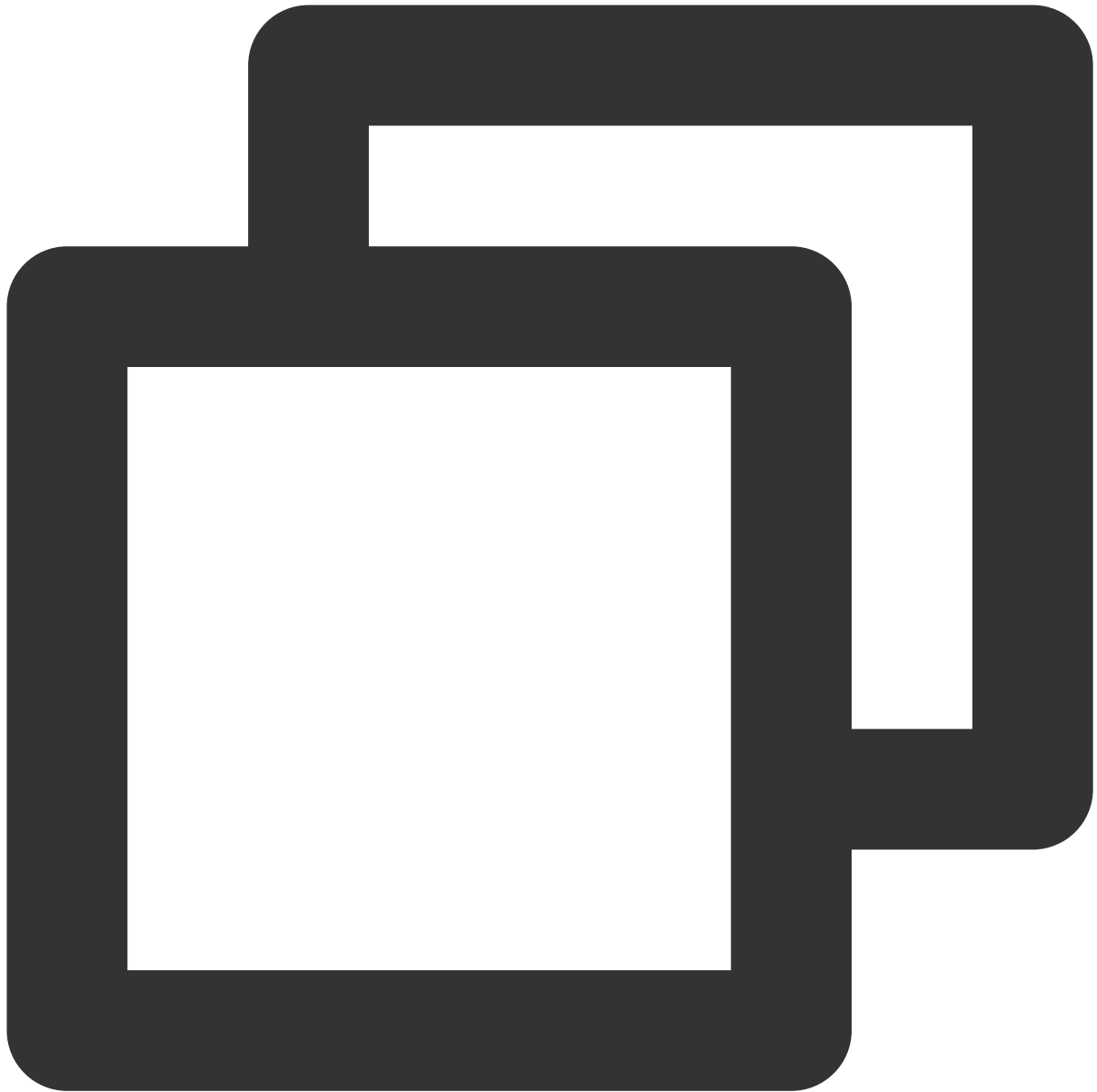
```
mkfs.ext4 /dev/pmem0
```

반환 결과가 아래 이미지와 같으면 파일 시스템이 성공적으로 생성된 것입니다.

```
[root@VM-11-3-centos ~]# mkfs.ext4 /dev/pmem0
mke2fs 1.45.6 (20-Mar-2020)
Creating filesystem with 16001536 4k blocks and 4005888 inodes
Filesystem UUID: ce9da959-85b7-462d-af32-dc0a42f0d729
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654
    4096000, 7962624, 11239424

Allocating group tables: done
Writing inode tables: done
Creating journal (65536 blocks): done
Writing superblocks and filesystem accounting information: done
```

2.2 /mnt/ 에 마운트합니다.



```
mount -o dax,noatime /dev/pmem0 /mnt/
```

참고 자료

[Intel® Optane™ DC Persistent Memory](#)

[Linux Provisioning for Intel® Optane™ Persistent Memory](#)