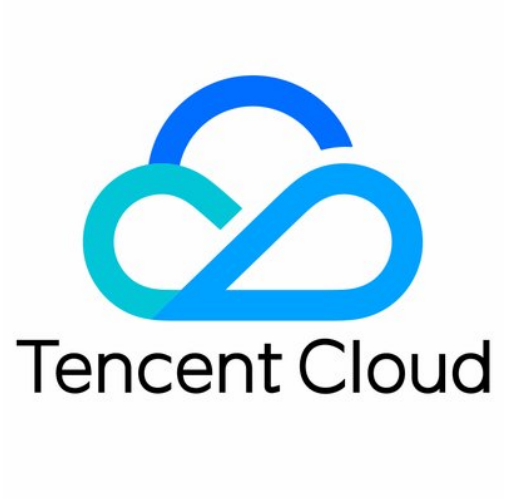
Cloud Virtual Machine

ベストプラクティス

製品ドキュメント



カタログ：

ベストプラクティス
CVMに対する最高実践

最終更新日：：2023-04-21 15:11:07

このドキュメントは、ユーザーが最大限に安全かつ確実にCVMを利用することに役立ちます。

セキュリティとネットワーク

アクセス制限：ファイアウォール（セキュリティグループ）を使用して、信頼できるアドレスがインスタンスへのアクセスを許可することによってアクセスを制限します。セキュリティグループで最も厳しい規則を設定します。例えばポートアクセス、IP アドレスアクセスを制限するなど。
セキュリティグレベル：異なるセキュリティグループ規則を作成して異なるセキュリティグレベルのインスタンスグループに適用し、重要な業務を実行しているインスタンスが外部に簡単にアクセスできないように確保します。
ネットワークロジック隔離：Virtual Private Cloud を利用してロジック領域の分割を行います。
アカウント権限管理：同じクラウドリソースグループに対して複数の異なるアカウント制御が必要な場合、ユーザーは ポリシーメカニズム を使用し、クラウドリソースへのアクセスを制御できます。
安全ログイン：できるだけ SSH キー でユーザーの Linux タイプのインスタンスにログインします。パスワードログイン を使用してのインスタンスは定期にパスワードを変更する必要があります。

ストレージ

ハードウェアストレージ：高い信頼性を求めるデータに対して、Tencent CloudのCloud Block Storageを利用してデータの永続性を保証し、できるだけ ローカルディスク を選択しないでください。詳細については、Cloud Block Storage製品ドキュメント をご参照ください。
データベース：頻繁にアクセスし、容量が不安定なデータベースに対して、Tencent Cloudクラウドデータベースを利用できます。

バックアップとリカバー

同一リージョンのインスタンスバックアップ：カスタマイズイメージおよび**Cloud Block Storageスナップショット**方式を利用してインスタンスと業務データをバックアップします。詳細については、Cloud Block Storageスナップショット と カスタマイズイメージの作成 をご参照ください。

クロスリージョンのインスタンスバックアップ：イメージレプリケーション を利用してクロスリージョンレプリケーションとインスタンスバックアップを行います。
インスタンス故障のブロック：Elastic IP によってドメイン名マッピングを行い、CVMが利用できない時に迅速にサービス IP を別のCVMインスタンスにリダイレクトすることを保証することにより、インスタンス故障をブロックします。

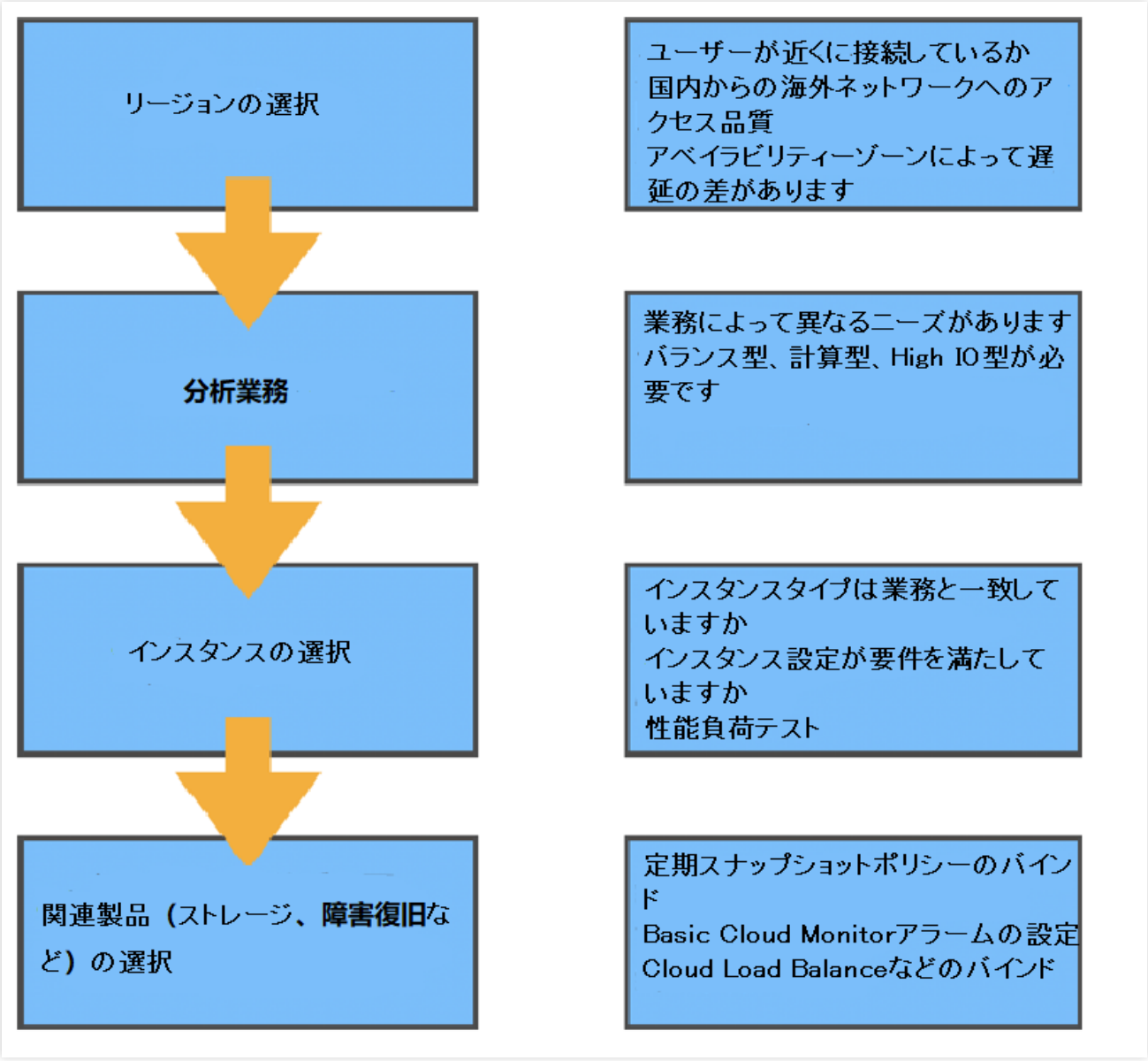
モニタリングとアラーム

モニタリングと応答イベント：定期的にモニタリングデータを確認して、かつ適切なアラームを設置します。詳細については、TCOP製品ドキュメント をご参照ください。
突発リクエストの処理：Auto Scaling を利用し、 ピークサービス中のCVMの安定性を保証でき、更に不健康のインスタンスを自動的に置き換えることもできます。

CVMタイプ選択のベストプラクティス

最終更新日：：2023-04-21 14:42:05

ここでは、CVMインスタンスの機能、一般的なビジネスシナリオ、注意事項およびベストプラクティスといった面から、インスタンスのタイプを選択する方法をご説明します。実際のビジネスシナリオと結び付けてCVMを選択、購入する方法を理解する上で役立ちます。インスタンスのタイプ選択の分析プロセスを次の図に示します：



リージョンとアベイラビリティーゾーン

リージョン

リージョン(Region)は、購入したクラウドコンピューティングリソースの地理的な場所を定め、お客様やお客様の顧客がリソースにアクセスするためのネットワーク条件をダイレクトに決定するものです。
中国本土以外のリージョンを購入する必要がある場合は、ネットワーク品質要因、関連するコンプライアンスポリシー要因およびいくつかのイメージ使用制限に特に注意してください（例えば、WindowsシステムとLinuxシステムを中国本土以外のリージョンで切り替えることはできません）。

アベイラビリティーゾーン

リージョンには1つ以上のアベイラビリティーゾーン(Zone)が含まれており、同じリージョン内の異なるアベイラビリティーゾーン間で販売されるCVMインスタンスのタイプは異なる場合があります。また、異なるアベイラビリティーゾーン間のリソースの相互アクセスには、ある程度のネットワーク遅延に差がある場合があります。
リージョンとアベイラビリティーゾーンの詳細情報については、リージョンとアベイラビリティーゾーン をご参照ください。

インスタンスタイプ

Tencent Cloudはさまざまなタイプのインスタンスを提供しており、各インスタンスタイプには複数のインスタンス仕様が含まれています。アーキテクチャに応じて、x86Compute、ARMCompute、ベアメタルCompute、異種Compute(GPU/FPGA)、Batch Computeなどに分けられます。特性・機能により、標準型、計算型、メモリ型、High IO型、ビッグデータ型などに分けられます。ここでは、インスタンスの特性・機能に応じて区分しており、詳細情報は次のとおりです：
標準型
標準型インスタンスの各性能パラメータはバランスが取れており、WebサイトやMiddlewareといったほとんどの通常業務に適しています。標準型インスタンスの主なシリーズは次のとおりです。
SおよびSAシリーズ：SシリーズはIntelコアであり、SAシリーズはAMDコアです。SAシリーズと比較して、同じ世代および構成のSシリーズは、より強力なシングルコアパフォーマンスを備えていますが、SAシリーズはよりコストパフォーマンスに優れています。
ストレージ最適化型S5seシリーズ：最新の仮想化テクノロジーSPDKに基づいて、ストレージプロトコルスタックのみを最適化し、CBSの機能を全面的に引き上げるので、大規模データベースやNoSQLデータベースなどのIOバウンド型サービスに適しています。
ネットワーク最適化型SN3neシリーズ：プライベートネットワークの最大送受信能力は600万ppsで、パフォーマンスは標準型S3インスタンスの約8倍です。プライベートネットワークの帯域幅は最大25Gbpsをサポートしており、プライベートネットワーク帯域幅は標準型S3に比べて2.5倍にもなります。これは、弾幕、ライブストリーミング、ゲームといった高ネットワークパケットの送受信シナリオに適しています。
計算型
計算型Cシリーズインスタンスは、最高のシングルコアコンピューティング性能を備えており、バッチ処理、ハイパフォーマンスコンピューティング、大規模ゲームサーバーなど、コンピューティング集約型アプリケーションに

適しています。例えば、高トラフィックのWebフロントエンドサーバー、MMO（マッシブリー・マルチプレイヤー・オンライン）ゲームサーバーおよびその他のコンピューティング集約型サービスなど。
メモリ型
メモリ型Mシリーズのインスタンスは大容量メモリという特徴を持ち、CPUとメモリの比率が1：8で、メモリ価格が最も安く、主に高性能データベース、分散メモリキャッシュなど、大容量メモリ操作や検索、コンピューティングを必要とするMySQL、Redisなどのアプリケーションに適しています。
High IO型
High IO型ITシリーズインスタンスデータディスクはローカルディスクストレージであり、最新のNVME SSDストレージを搭載し、高いランダムIOPS、高スループット、低アクセスレイテンシーといった特徴を備えており、低コストで非常に高いIOPSを提供します。ハードディスクの読み取り・書き込みや遅延に対して高い要件のある高性能データベースなど、例えば、高性能のリレーショナルデータベース、ElasticsearchといったIOバウンド型業務などのI/Oバウンド型アプリケーションに適しています。
説明：
ITシリーズインスタンスのデータディスクはローカルストレージであるため、データが失われるリスクがあります（ホストがダウンした場合など）。お客様のアプリケーションにデータ信頼性アーキテクチャがない場合は、CBSをデータディスクとして選択できるインスタンスの使用を強く推奨します。
ビッグデータ型
ビッグデータ型Dシリーズインスタンスはマスストレージリソースを搭載し、高スループットという特徴を備えており、Hadoop分散コンピューティング、大量のログ処理、分散ファイルシステム、大型データウェアハウスなど、スループット集約型アプリケーションに適しています。
説明：
ビッグデータモデルDシリーズインスタンスのデータディスクはローカルディスクであるため、データが失われるリスクがあります（ホストがダウンしている場合など）。アプリケーションにデータ信頼性アーキテクチャがない場合は、CBSをデータディスクとして選択できるインスタンスの使用を強く推奨します。
異種Compute
異種コンピューティングインスタンスはGPU、FPGAなどの異種ハードウェアを搭載し、リアルタイムの高速並列計算と浮動小数点演算機能を備え、ディープラーニング、科学計算、ビデオコーデック、グラフィックワークステーションなどの高性能アプリケーションに適しています。
NVIDIA GPUシリーズのインスタンスは、主流のT4/V100や最新世代のA100などを含めたNVIDIA Teslaシリーズの GPUを採用しており、優れた汎用コンピューティング機能を提供します。ディープラーニングのトレーニング/推論、計算科学などのアプリケーションシナリオでのベストな選択肢です。
Cloud Physical Machine2.0
Cloud Physical Machine2.0は、Tencent Cloudの最新仮想化テクノロジーに基づいて開発された究極のパフォーマンスを備えたECSベアメタルCVMです。Cloud Physical Machine2.0は、仮想マシンの柔軟性と物理マシンの高い安定性を兼ね備え、NetworkingやデータベースといったTencent Cloudの全製品とシームレスに統合します。Cloud Physical Machine2.0インスタンスマトリックスは、標準、High IO、ビッグデータおよび異種Computeのシナリオを網羅し、クラウド専用の高性能かつ安全に分離された物理サーバークラスターを分単位で構築できます。同時に、サードパーティの仮想化プラットフォームをサポートでき、高度にネストされた仮想化テクノロジーによっ

て、AnyStackのハイブリッドデプロイを実現し、先進的かつ効率的なハイブリッドクラウドソリューションを構築することができます。
高性能Computeクラスター
高性能Computeクラスターは、Cloud Physical Machine2.0をコンピューティングノードとして使用し、高速RDMA相互接続ネットワークサポートを提供するクラウド上のComputeクラスターです。自動車シミュレーション、流体力学、分子動力学といった大規模なコンピューティングシナリオを幅広くサポートできます。また、大規模な機械学習トレーニングなどのシナリオをサポートできる、高性能の異種リソースを提供します。
CVMのインスタンスタイプの関連情報の詳細については、インスタンス仕様 をご参照ください。

一般的なビジネスシナリオのタイプ選択に関する推奨事項

ビジネスシナリオ	一般的なソフトウェア	シナリオ紹介	推奨モデル
Webサービス	NginxApache	Webサービスには通常、個人のWebサイト、ブログおよび大規模なeコマースのWebサイトなどが含まれており、コンピューティング・ストレージ・メモリなどのリソースに対してはバランスが要求されるため、業務上のニーズを満たす標準型インスタンスをお勧めします。	標準型SおよびSAシリーズ
Middleware	Kafka MQ	メッセージキュー業務のコンピューティングやメモリリソースに対する要件は比較的バランスが要求されるので、標準型モデルにはストレージとしてCBSを搭載することをお勧めします。	標準型Sシリーズ計算型Cシリーズ
データベース	MySQL	データベースにはIO性能に対する非常に高い要件があるので、SSD CBSとローカルディスクを使用することをお勧めします（ローカルディスクモデルはデータが失われるリスクがあるため、データのバックアップに注意してください）。	High IO型シリーズメモリ型Mシリーズ
キャッシュ	RedisMemcache	キャッシュ型業務はメモリに対して高い要件がありますが、コンピューティングに対する要件は低めですので、メモリ比率の高いメモリ型インスタンスをお勧めします。	メモリ型Mシリーズ
ビッグデータ	HadoopES	ビッグデータ業務はマスストレージを必要とし、IOスループットに所定の要件があるため、専用のビッグデータ型Dシリーズをお勧めします（ローカルディスクモデルはデータが失われるリスクがあるため、データのバックアップに注意してください）。	ビッグデータ型Dシリーズ
高性能	StarCCMWRF-	高性能Computeの業務には、究極とも言える単一マシン	高性能

Compute	Chem	の計算機能が必要であるとともに、効率的なマルチマシン拡張も必要です。高速RDMAネットワークを搭載した高性能Computeクラスターまたは計算型インスタンスファミリーをお勧めします。	Computeクラスター計算型Cシリーズ
仮想化	KvmOpenStack	仮想化アプリケーションでは、クラウド上のサーバーが、パフォーマンスのオーバーヘッドを追加することなく、ネストされた仮想化の機能を備え、仮想化機能を従来の物理マシンと一貫性のある状態に保つ必要があります。Cloud Physical Machine2.0製品をお勧めします。	高性能Computeクラスター Cloud Physical Machine2.0
ビデオレンダリング	UnityUE4	ビデオレンダリングシナリオには、DirectXやOpenGLなどのグラフィック・画像処理APIのサポートが必要です。 GPUレンダリングタイプGN7vwをお勧めします。	GPUレンダリング型GN7vw
AI Compute	TensorFlowCUDA	AI Compute業務には並列処理機能が必要であり、GPUコンピューティング機能やグラフィックメモリに対する明確な要件があります。	GPU計算型高性能Computeクラスター

関連製品

一般的なクラウド製品のマッチングに関する推奨事項

実際のビジネスシナリオと結び付けて、他のTencent Cloud製品を組み合わせて使用することができます。ここでは、典型的なWebサイトのアーキテクチャを例として取り上げます。下図に示すように、クラウド製品と組み合わせることをお勧めします。

他のクラウド製品

実際のニーズに応じて、他のクラウド製品を選択、使用することもできます。例えば、基本的な業務のデプロイが完了したら、所定の障害復旧対策を講じて、システムアーキテクチャの堅牢性を確保するとともに、データセキュリティを確保することができます。次のTencent Cloud製品と組み合わせて、障害復旧を実現することができます。

スナップショット

スナップショットは、手軽で効率的なデータ保護サービスであり、非常に重要で効果的なデータ障害復旧対策でもあります。日常的なデータバックアップ、迅速なデータリカバリ、本番データの複数レプリカアプリケーション、迅速なデプロイ環境といったビジネスシナリオで使用することをお勧めします。スナップショットの作成には少額の料金がかかります。詳細については、スナップショットの料金概要 をご参照ください。

TCOP

クラウドリソースのTCOPアラームの設定は、業務の保証にとって同様に重要な役割を果たします。TCOPを使用して、クラウド製品のリソース使用率、アプリケーション性能やクラウド製品の実行状況を全面的に理解することができます。TCOPは、マルチインデックスモニタリング、カスタムアラーム、クロスリージョン/クロスプロジェクトインスタンスのグループ化、カスタムモニタリング、視覚化DashboardおよびPrometheusホスティングサービスといった機能もサポートします。クラウド製品に生じた緊急事態をタイムリーに制御かつ対処できるよう支援することによって、システムの安定性を高め、運用・保守の効率を向上させ、運用・保守のコストを削減します。

CLB

業務にシングルポイントのオペレーショナルリスクを発生させたくない場合は、CLBの設定を選択できます。CLBサービスは、仮想サービスアドレス(VIP)を設定することにより、同じリージョンにある複数のCVMリソースを高

性能で可用性の高いアプリケーションサービスプールに仮想化します。アプリケーションで指定された方法に従って、クライアントからのネットワークリクエストをCVMプールに配信します。
CLBサービスは、CVMプール内のCVMインスタンスのヘルスステータスをチェックし、異常な状態のインスタンスを自動的に隔離し、CVMのシングルポイントの問題を解消するとともに、アプリケーションの全体的なサービス機能を向上させます。

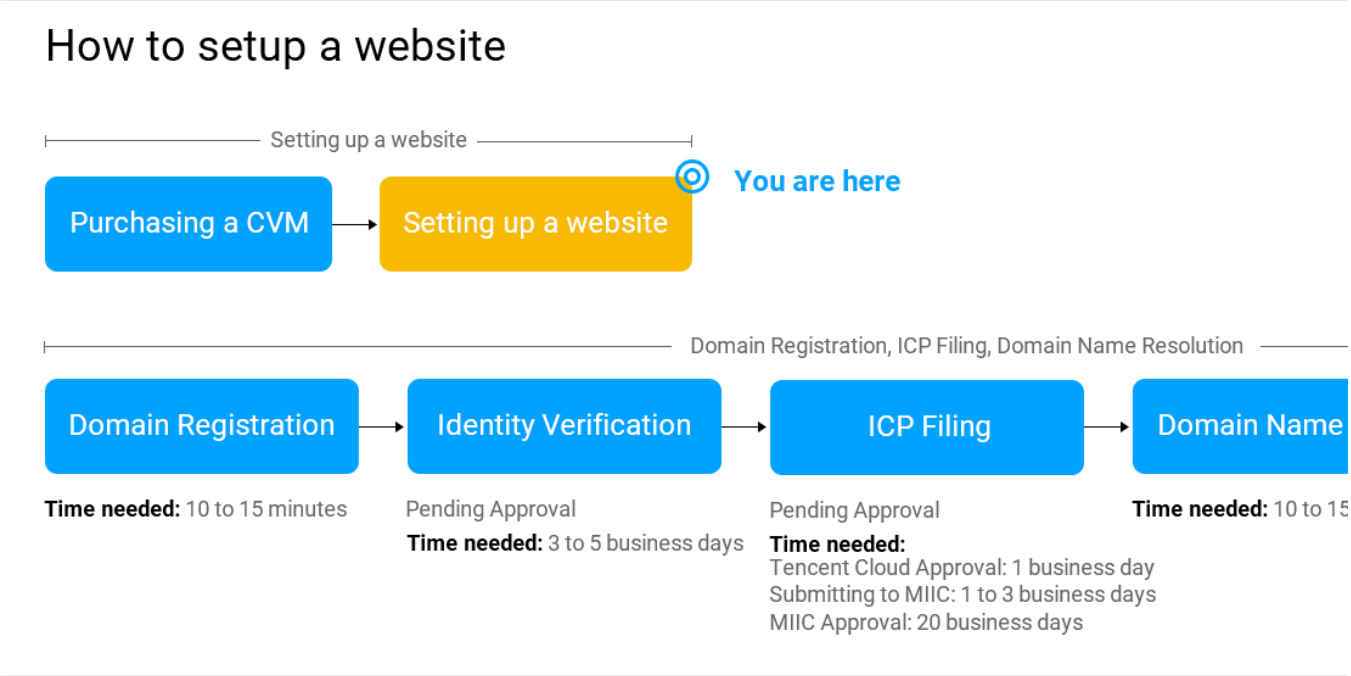
関連ドキュメント

リージョンとアベイラビリティーゾーン
-インスタンス仕様

ウェブサイトの構築方法

最終更新日：：2022-06-29 15:53:06

CVMの購入が完了したら、購入したサーバーにご自分のウェブサイトやフォーラムを構築することができます。
説明：
またLighthouseを使用すれば、「ワンクリックでのサイト構築」もでき、手動での設定が不要になります。作成時に必要なアプリケーションイメージを選択するだけで、個人のウェブサイトを構築することができます。詳細については、Lighthouseの購入方法 をご参照ください。



構築方法

Tencent Cloudは、主流のウェブサイトシステム向けに、さまざまなタイプのウェブサイト構築チュートリアルを提供しています。構築方法にはイメージデプロイと手動構築という2種類があり、それぞれ以下のような特徴を持っています。

比較項目	イメージのデプロイ	手動構築
構築	Tencent クラウドマーケットのシステムイメージから直接インストールしてデプロイすることを選	必要なソフトウェアを手動でインストールすると、カスタマイズが可能です。

方法	択します。	
特徴	付属のソフトウェアのバージョンは比較的固定されています。	付属バージョンもフレキシブルに選択することができます。
所要時間	比較的短い時間で、ワンクリックでデプロイできます。	比較的時間がかかり、手動で関連ソフトをインストールする必要があります。
難易度	比較的簡単です。	ソフトウェアパッケージのバージョンとインストール方法について、ある程度理解している必要があります。

サイトの構築

実際のニーズに応じて、さまざまなシステムで個人のウェブサイトを構築することができます。

ウェブサイトタイプ	構築方法	説明
WordPress	WordPress(Linux)の手動構築	WordPressは、PHP言語を使用して開発されたブログプラットフォームです。ユーザーは、PHPとMySQLデータベースをサポートするサーバーに、自分のウェブサイトを設置することができます。また、WordPressをコンテンツ管理システム(CMS)として使用することも可能です。
	WordPress(Linux)の手動構築	
Discuz!	Discuz!の手動構築	Discuz!は、PHP+MySQLアーキテクチャを使用して開発された汎用型のコミュニティフォーラムです。ユーザーは、サーバーへの簡単なインストールと設定により、パーフェクトなフォーラムサービスをデプロイすることができます。
LNMP環境	LNMP環境の手動構築（CentOS 7）	LNMP環境は、LinuxシステムでNginx+MySQL/MariaDB+PHPで構成されるウェブサイトサーバーアーキテクチャを表しています。
	LNMP環境の手動構築（CentOS 6）	
	LNMP環境の手動構築（openSUSE）	

LAMP環境	LAMPの手動構築	LAMP環境は、LinuxシステムでApache+MySQL/MariaDB+PHPで構成されるウェブサイトサーバーアーキテクチャを表しています。
WIPM環境	WIPMの手動構築	WIPM環境は、Windowsシステム上のIIS+PHP+MySQLで構成されるウェブサイトサーバーアーキテクチャを表しています。
Drupal	Drupalの手動構築	Drupalは、PHP言語で記述されたオープンソースのコンテンツ管理フレームワーク(CMF)であり、コンテンツ管理システム(CMS)とPHP開発フレームワーク(Framework)で構成されています。ユーザーは、個人またはグループでのウェブサイト開発のプラットフォームとしてDrupalを使用することができます。
Ghost	Ghostの手動構築	Ghostは、Node.jsをベースとして開発されたオープンソースのブログプラットフォームです。すばやいデプロイや簡素化されたオンライン公開プロセスといった機能的特徴により、ユーザーはGhostを使用すれば、個人のブログをすばやく作成することができます。
Microsoft SharePoint 2016	Microsoft SharePoint 2016の構築	Microsoft SharePointとは、Microsoft SharePoint Portal Serverの略称で、企業がインテリジェントなポータルサイトを開発できるようにするためのポータルサイトです。このサイトではチームやナレッジとシームレスにつながることができ、ユーザーは関連情報をビジネスプロセスで有効活用し、業務をより効率的に進められるようになります。

関連する操作

個人のウェブサイトは、インターネット上で外部からアクセスできるようになるまでに、ドメイン名の登録、ウェブサイトのICP登録、解決などの作業が必要です。CVMに個人のサイトをデプロイ済みで、インターネットに公開することを予定している場合は、使用可能なドメイン名を準備します。

環境構築
IISサービスをインストールする

最終更新日：：2023-05-09 16:40:04

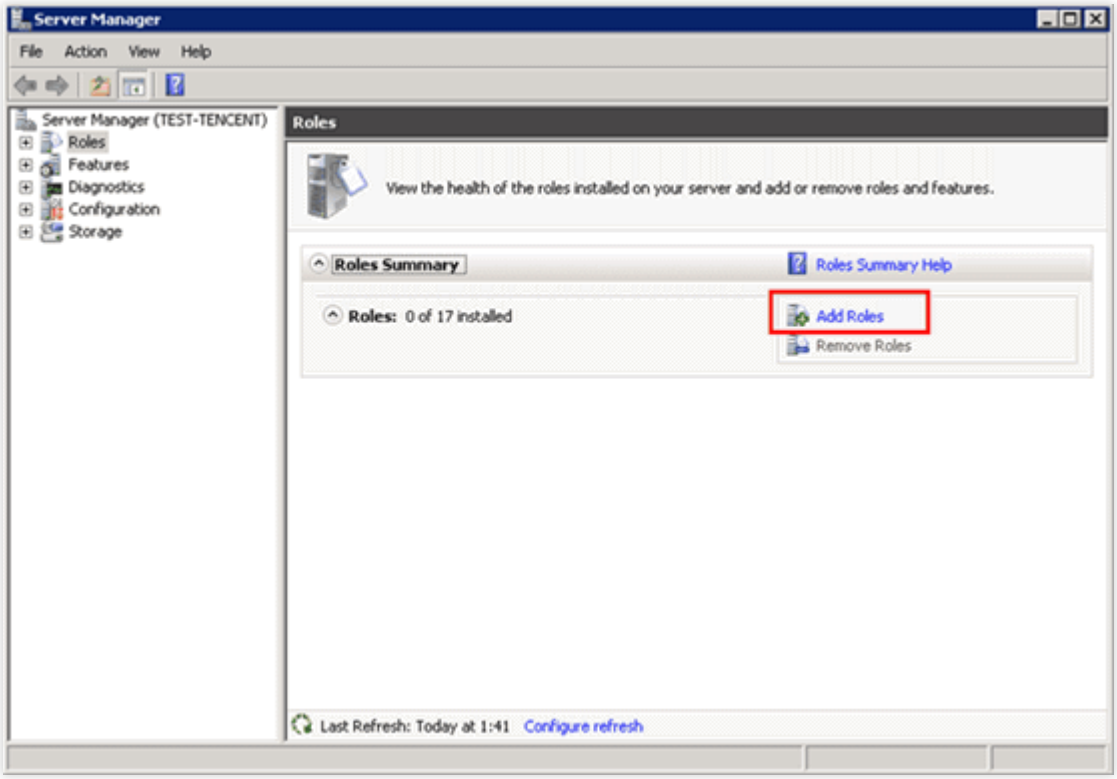
本ドキュメントはWindows 2012 R2 バージョンOSとWindows 2008 バージョンOSでのIISの追加とインストールするプロセスについて説明します。

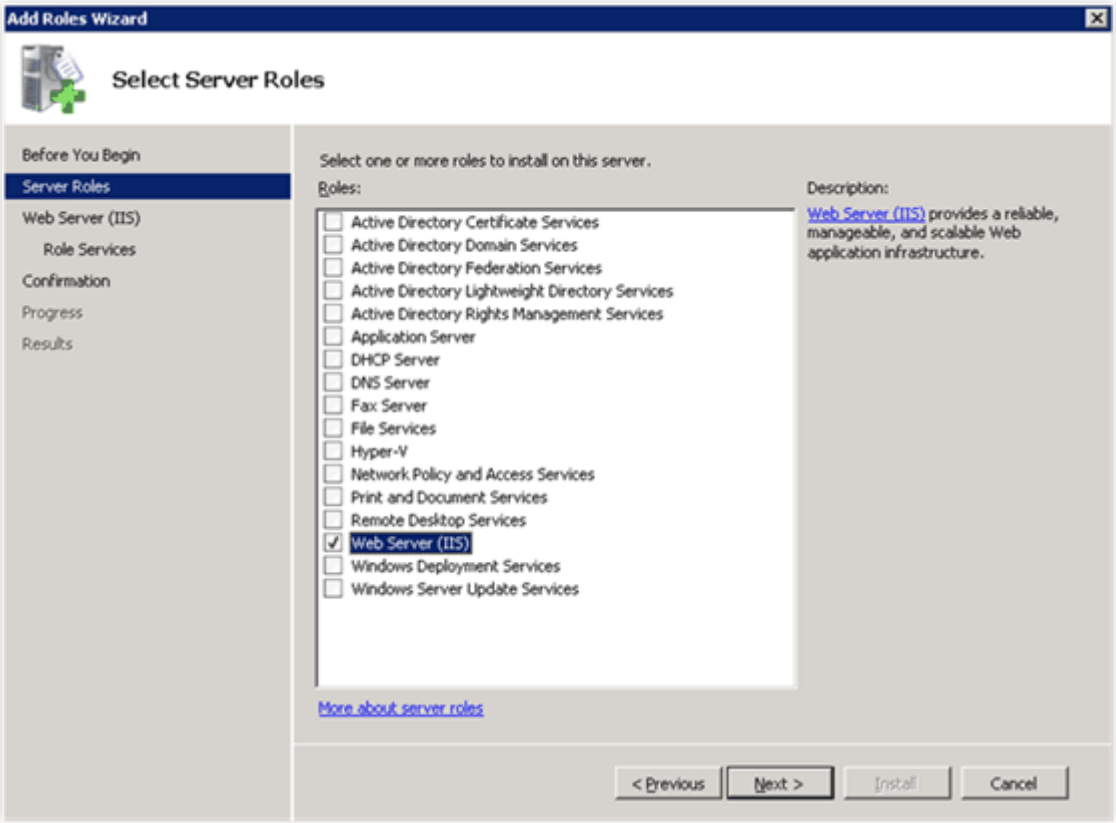
Windows 2012 R2 バージョン

1. Windows CVMにログインし、左下の**スタート(Start)をクリックして、サーバーマネージャー(Server Manager)**を選択して、サーバー管理画面を開きます。
2. **役割と機能の追加**を選択し、「役割と機能の追加ウィザード」の「開始する前に」画面で**次へ(N)>ボタンをクリックします。「インストールの種類」画面で、役割ベースまたは機能ベースのインストール**を選択して、**次へ(N)>**ボタンをクリックします。
3. ウィンドウの左側で「サーバーの役割」タブを選択し、**Web サーバー (IIS)をチェックして、ポップアップダイアログで機能の追加**ボタンをクリックして、**次へ(N)>**ボタンをクリックします。
4. 「機能」タブで「.Net3.5」をチェックして、**次へ(N)>**ボタンをクリックした後、「Webサーバーの役割(IIS)」タブを選択して、 **次へ(N)>**ボタンをクリックします。
5. 「役割サービス」タブで**CGI**オプションをチェックして、**次へ(N)>**ボタンをクリックします。
6. インストールを確認し、インストールが完了するまで待ちます。
7. インストールが完了したら、CVMのブラウザーで ``http://localhost/`` にアクセスして、インストールが成功したかどうかを確認します。 以下の画面が表示されたら、インストールが正常に完了したことを示しています。

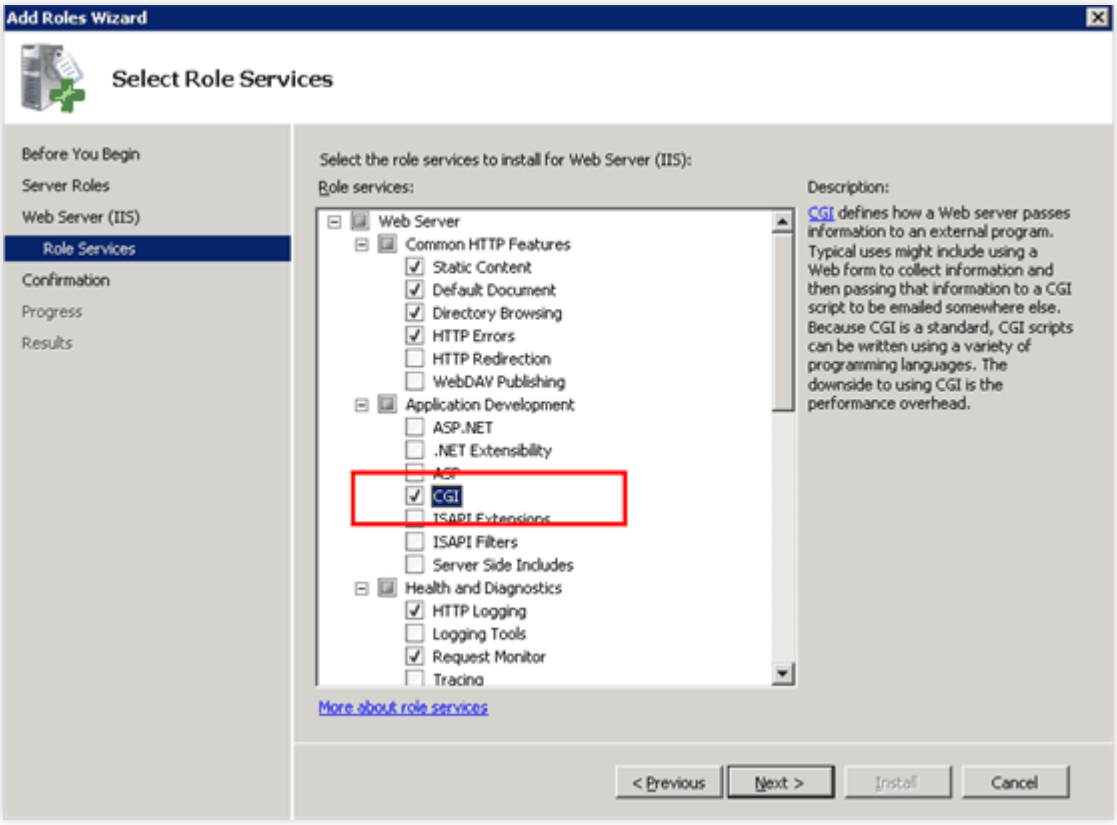
Windows 2008 バージョン

1. Windows CVMにログインし、左下にある**スタート(Start)メニュー中の管理ツール**中の**サーバーマネージャー**ボタンをクリックして、サーバー管理画面を開きます。
2. **役割と機能の追加(Add Roles)をクリックして、サーバーの役割を追加します。「Web Server(IIS)」オプションをチェックして、次へ(N)>**をクリックします。

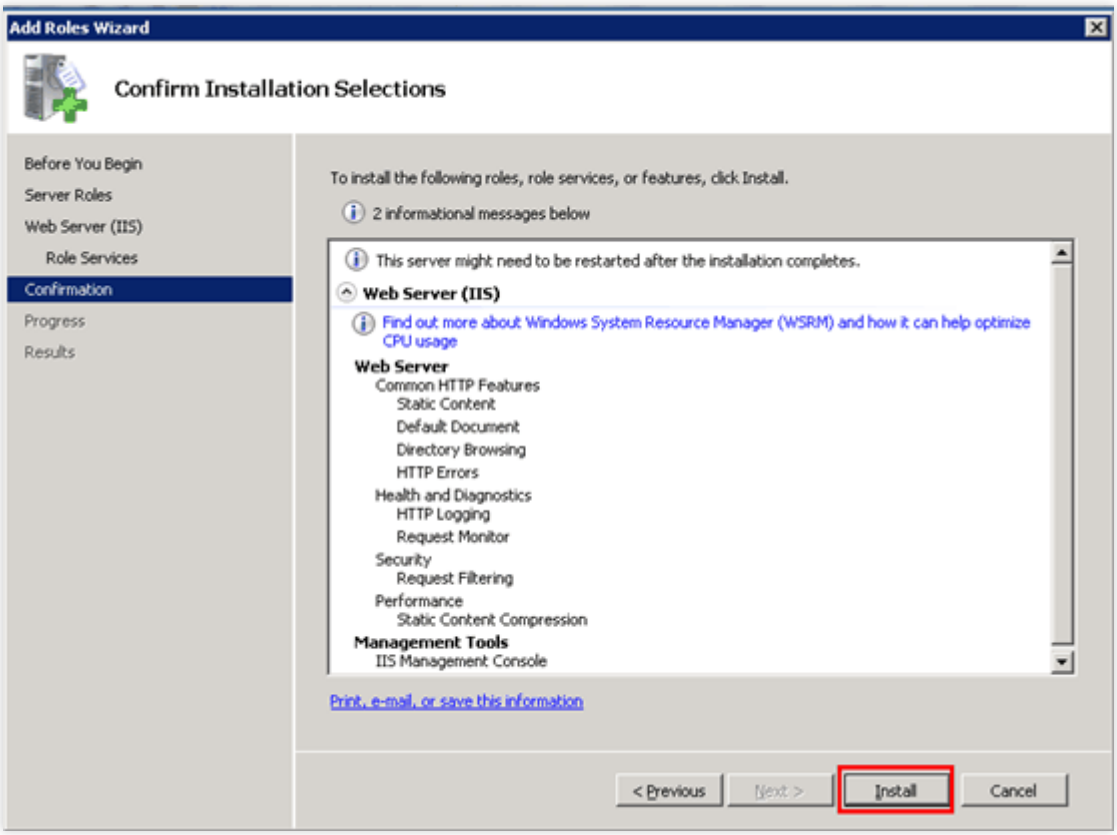




3. 「役割サービス(Role Services」)を選択する時に、「CGI」オプションをチェックします。



4. 設定が完了したら、**インストール(install)**をクリックして、インストールを続行します。



5. ブラウザーを介してWindows CVMのパブリックネットワークIPにアクセスして、IISサービスが正常に実行しているかどうかを確認します。下記のように表示されたら、IISのインストールと設定が成功したことを示しています。

ウェブサイトの構築
WordPress 個人用サイトを構築する
WordPress 個人用サイトを構築する

最終更新日：：2023-07-17 16:40:01

操作シナリオ

WordPressはPHP言語で開発されたブログプラットホームです。WordPressにより個人のブログプラットホームを構築することが可能です。本節はCentOS 7.6 OSのTencent Cloud CVMを例とし、手動でWordPressの個人サイトを構築することについて説明します。
WordPressの個人ブログを構築するには、Linux コマンド（例：CentOS環境におけるYUMによるソフトウェアをインストールする 等の常用コマンドに詳しい必要があります。また、インストールするソフトウェアの利用およびバージョン間の互換性を把握することも必要です。
ご注意：
手動による構築プロセスには長い時間がかかる場合があるため、Tencent Cloudは、クラウド市場のイメージ環境を介してWordPressの個人ブログをデプロイすることをお勧めします。

ソフトウェアのバージョン

本節で構築するWordPress個人サイトの構成バージョンとその説明は次のとおりです：
Linux：Linux OS、本ドキュメントはCentOS 7.6を例として説明します。
Nginx：Webサーバー、本節ではNginx 1.17.5を例に説明します。
MariaDB：データベース、本ドキュメントはMariaDB 10.4.8を例として説明します。
PHP：スクリプト言語、本ドキュメントはPHP 7.2.22を例とします。
WordPress：ブログプラットフォーム、本節ではWordPress 5.0.4を例に説明します。

操作手順

ステップ1：CVMにログインする

標準的な方法を使用してLinuxインスタンスにログインする（推奨）。実際の操作方法に応じて、他のログイン方法を選択することもできます：
リモートログインソフトウェアを使用してLinuxインスタンスにログインする
SSHキーを使用してLinuxインスタンスにログインする

ステップ2：手動でLNMP環境を構築する

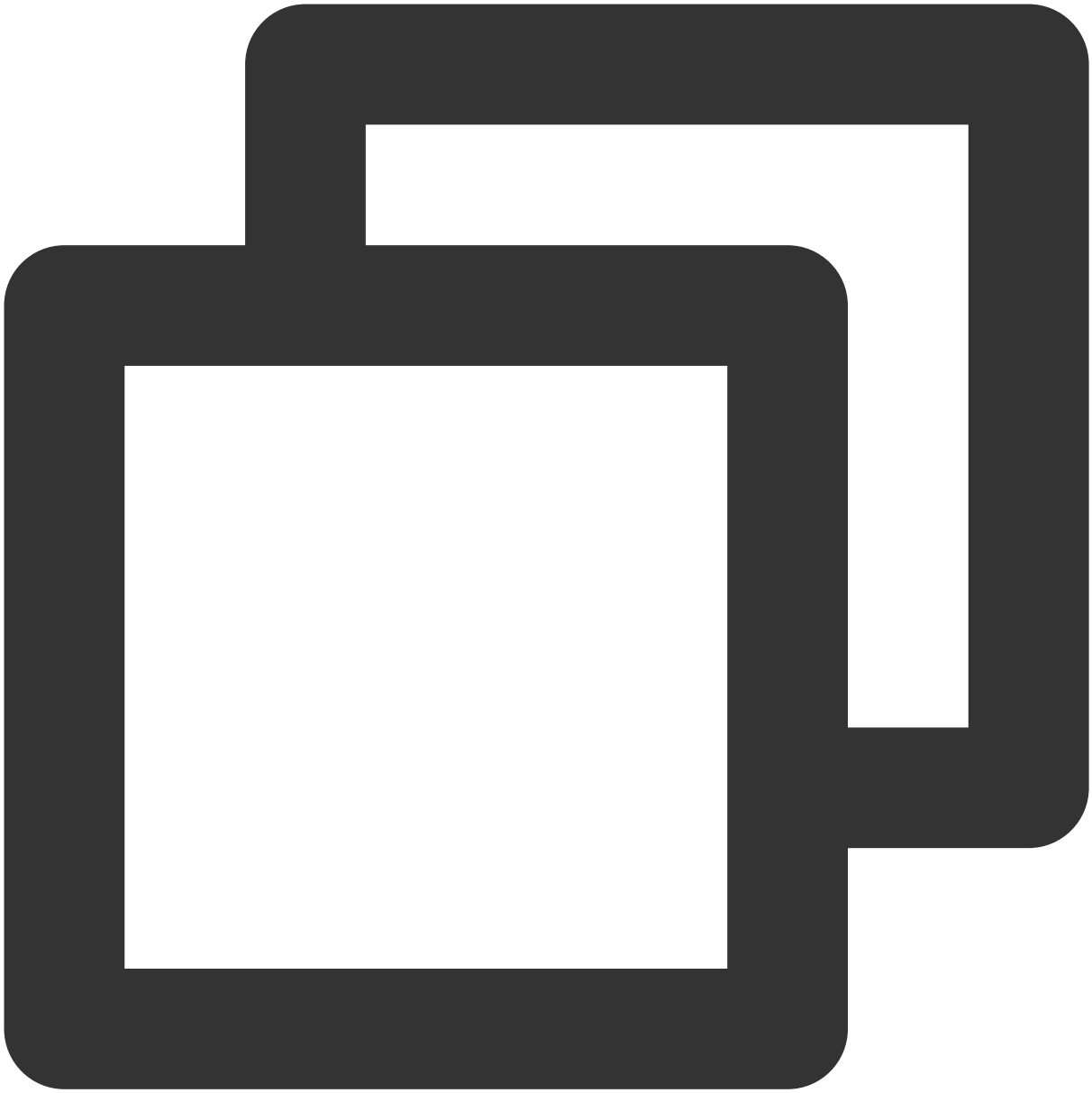
LNMP は Linux、Nginx、MariaDB およびPHPの略称であり、この組み合わせは最もよく使われているWebサーバー稼動環境の1つです。CVMインスタンスを作成しログインした後に、手動でLNMP環境を構築する を参考して、基本的な環境を構築できます。

ステップ3：データベースを構成する

ご注意：

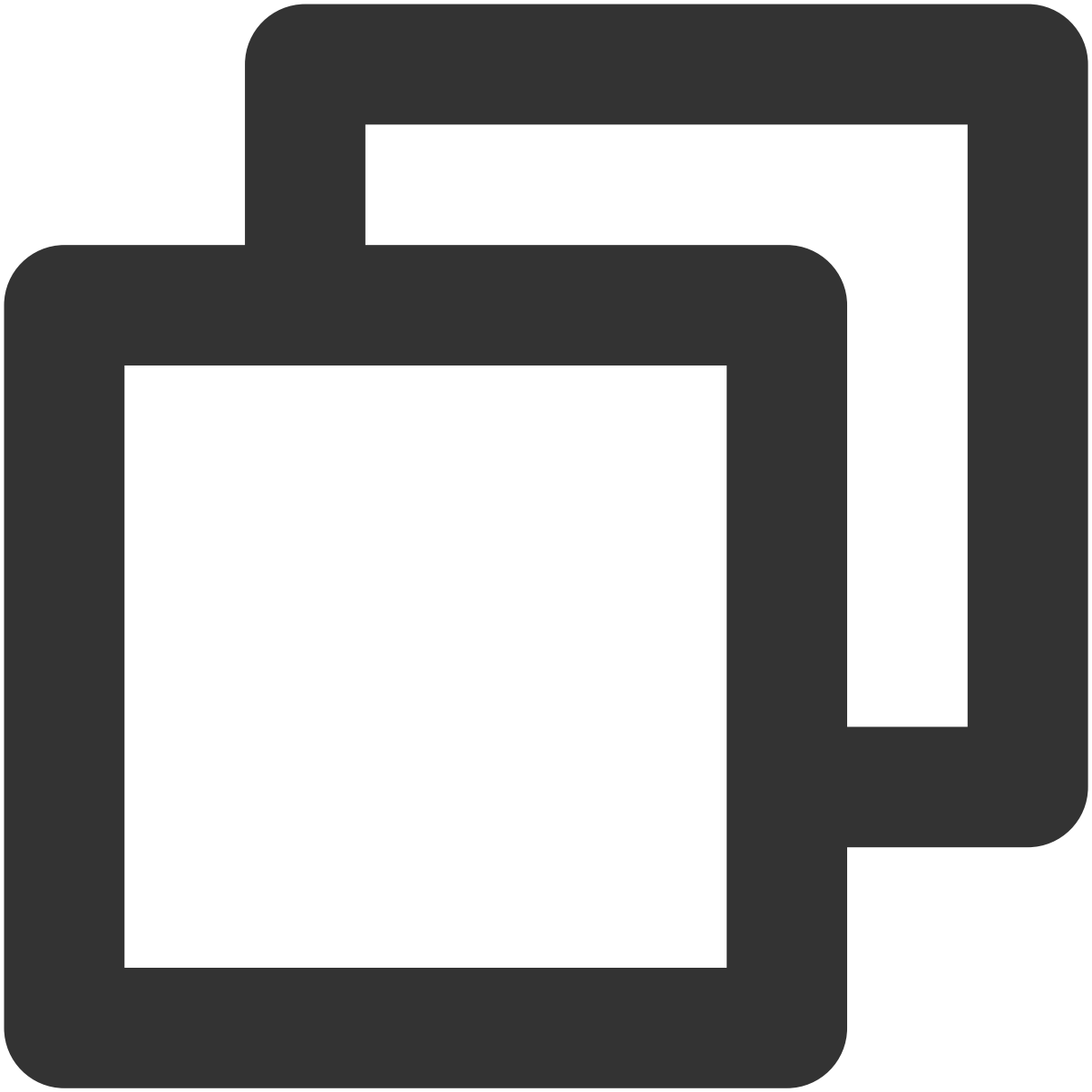
MariaDBのバージョンにより、ユーザー認証方法の設定は異なります。手順の詳細については、 MariaDBの公式サイトをご参照ください。

1. 以下のコマンドを実行し、MariaDBに入ります。



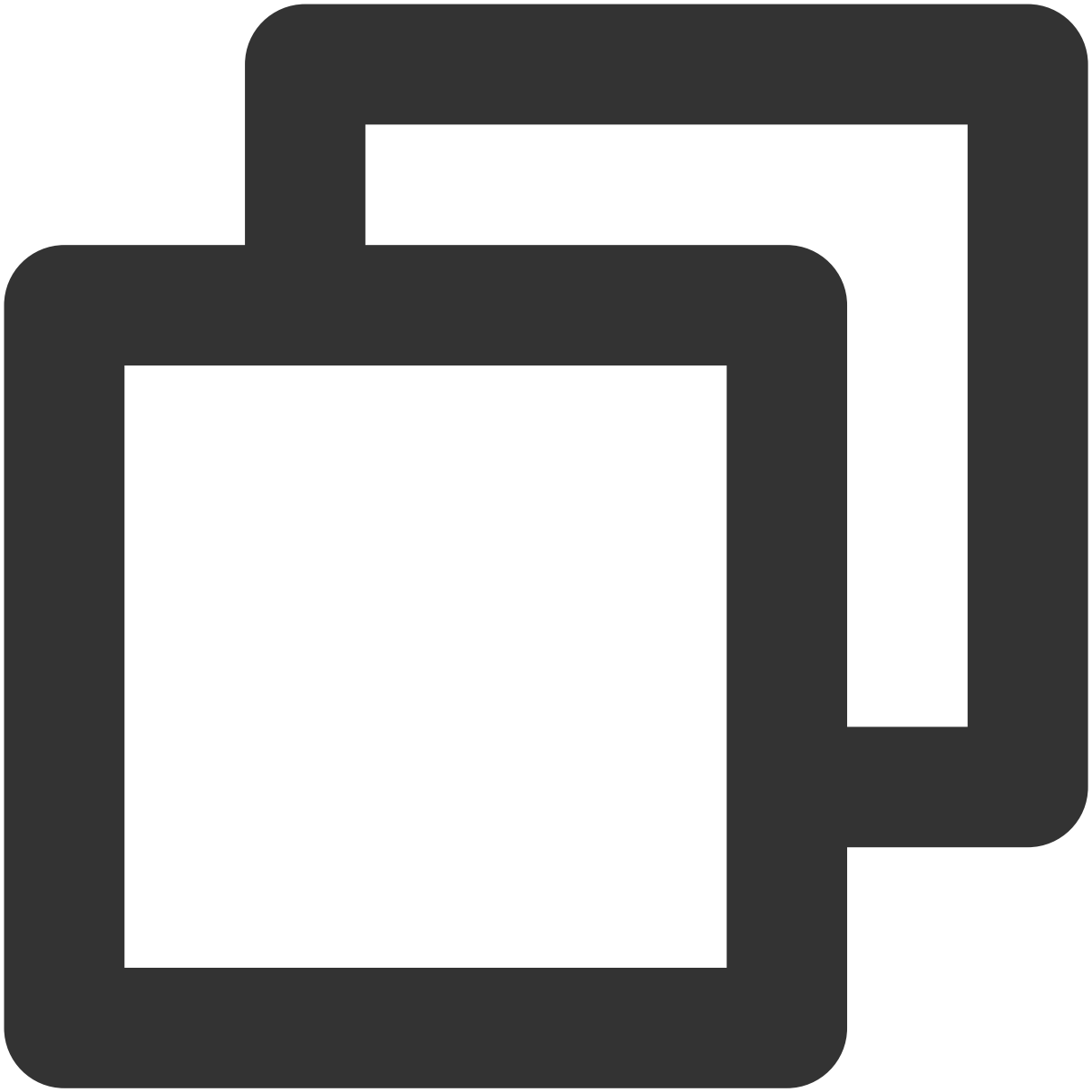
```
mysql
```

2. 以下のコマンドを実行し、MariaDBデータベース（「wordpress」を例に）を新規作成します。



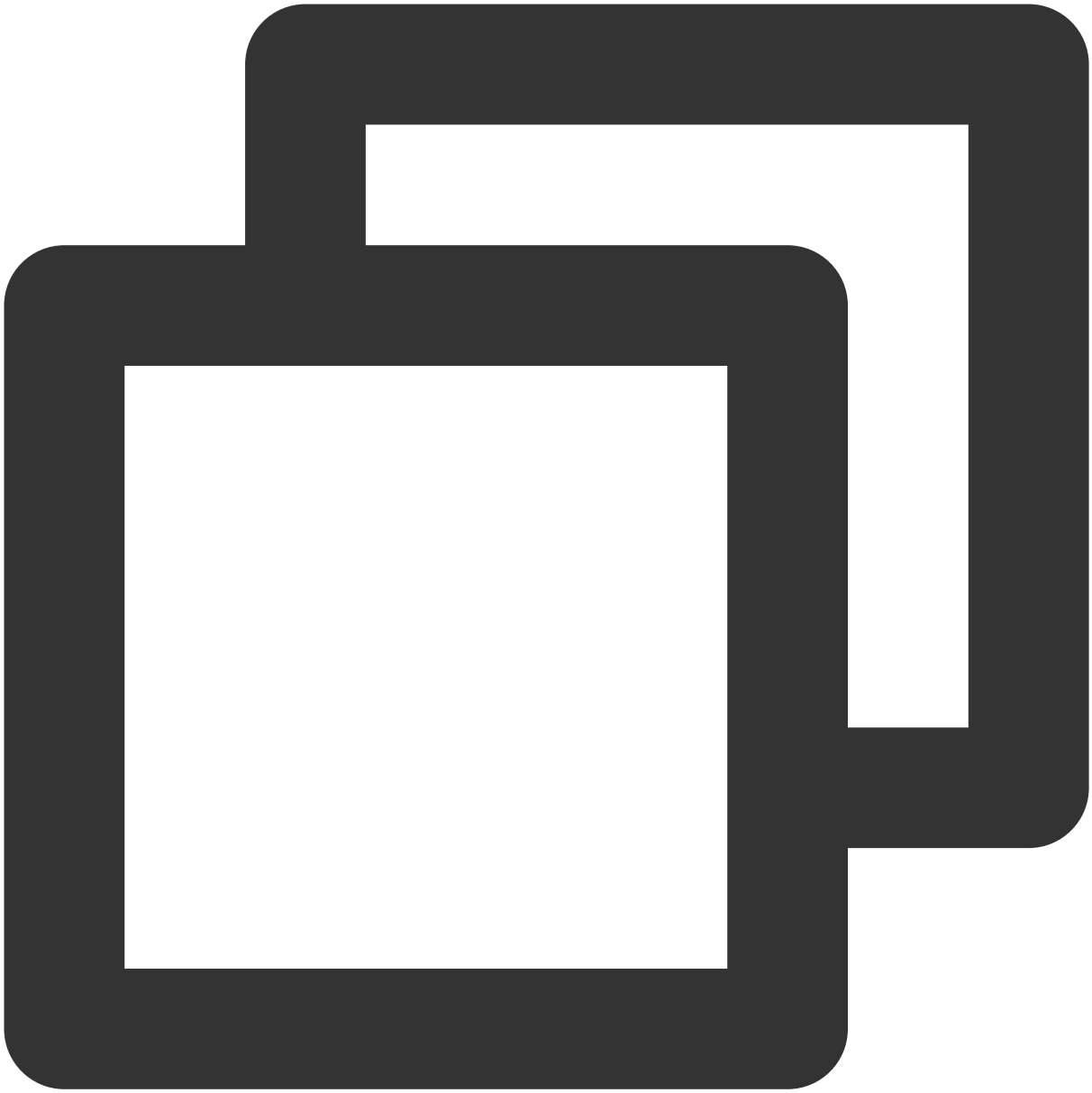
```
CREATE DATABASE wordpress;
```

3. 以下のコマンドを実行し、ユーザーを新規作成します。例えば「user」で、ログインパスワードは「123456」です。



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

4. 以下のコマンドを実行し、ユーザーに「wordpress」データベースのすべての権限を付与します。

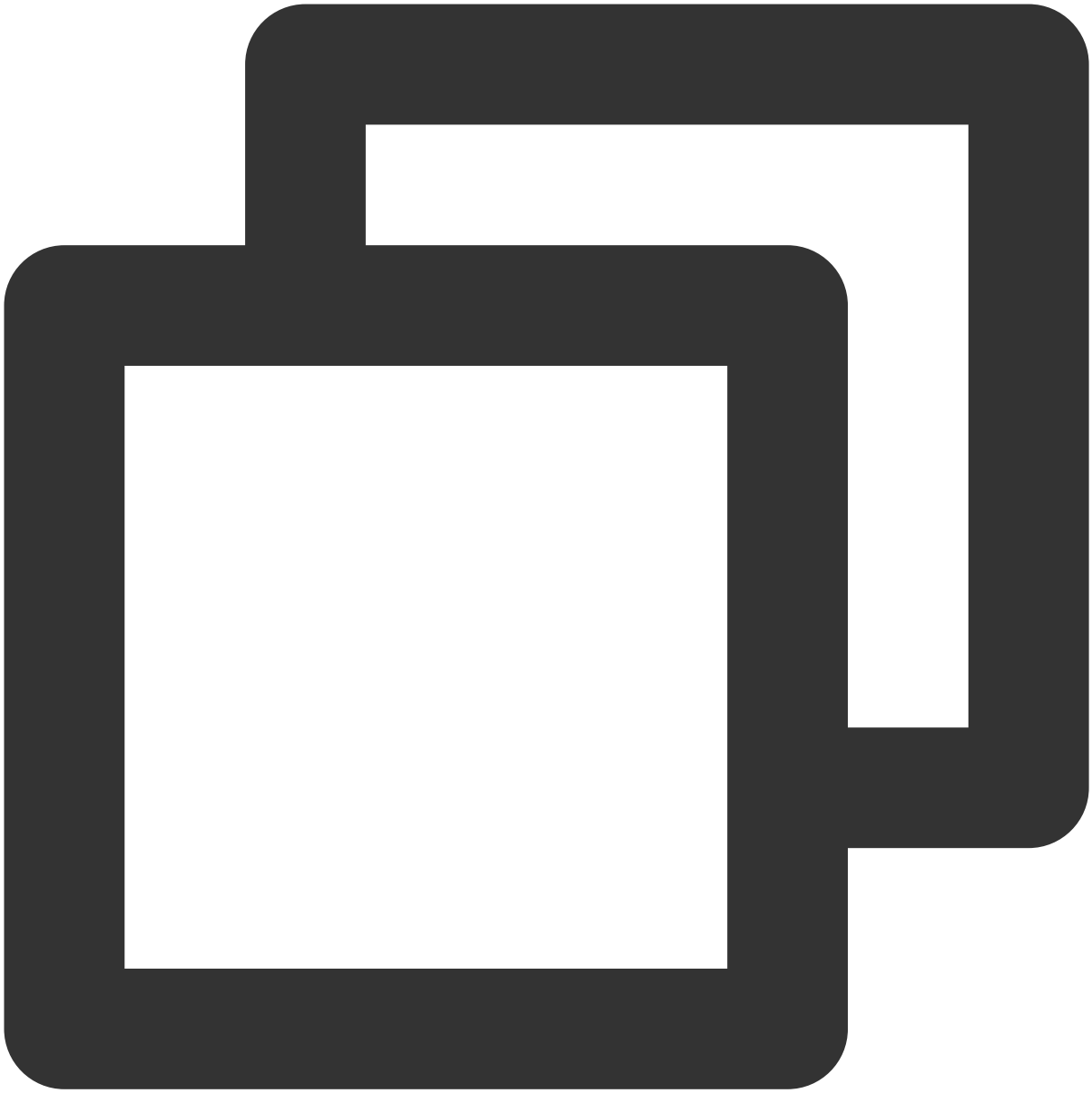


```
GRANT ALL PRIVILEGES ON wordpress.* TO 'user'@'localhost' IDENTIFIED BY '123456';
```

5. 以下のコマンドを実行し、rootアカウントのパスワードを設定します。

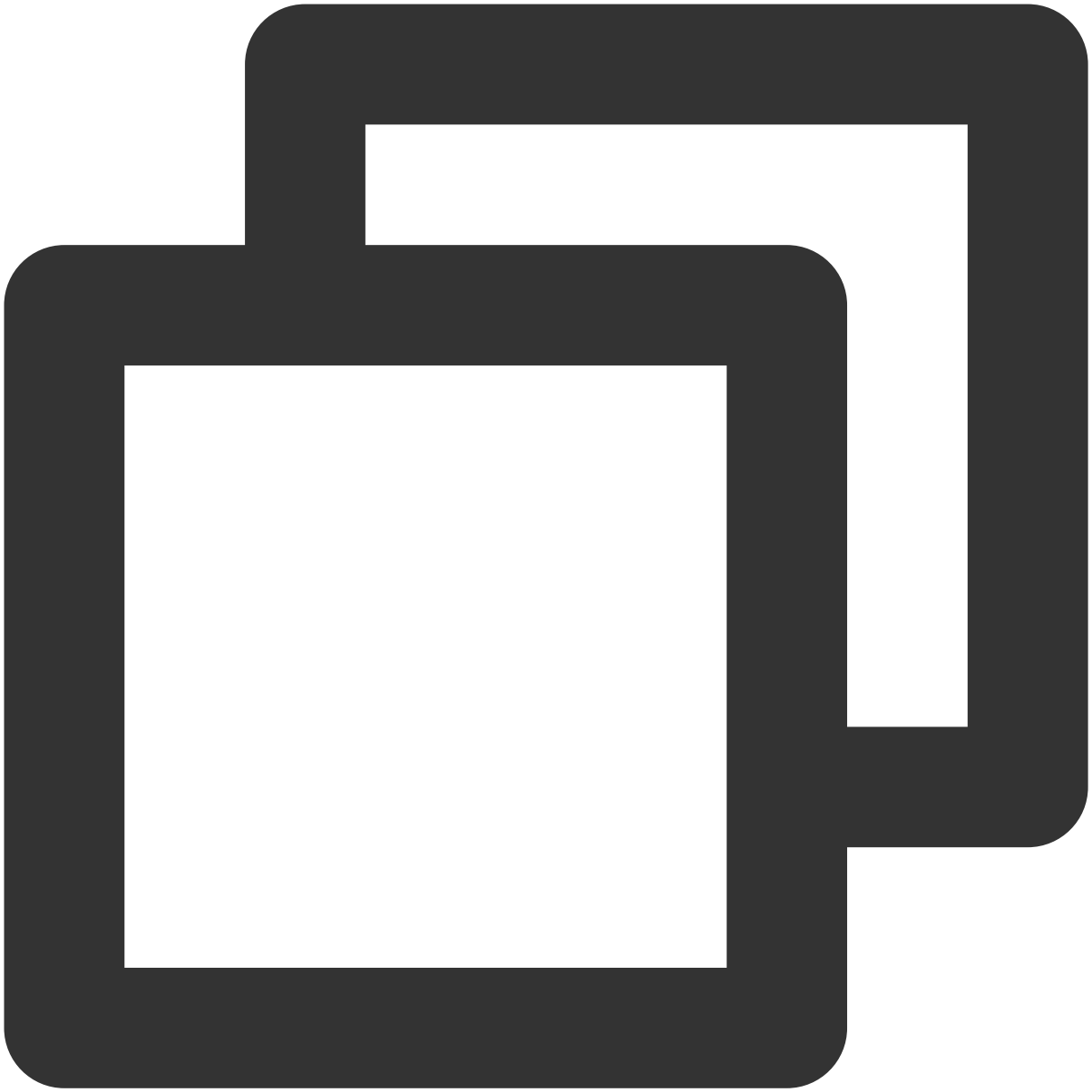
説明：

MariaDB 10.4はCentOSシステムにおいて rootアカウントパスワード不要のログイン機能を追加しました。下記のステップを実行し、自分のrootアカウントパスワードを設定し、保管してください。



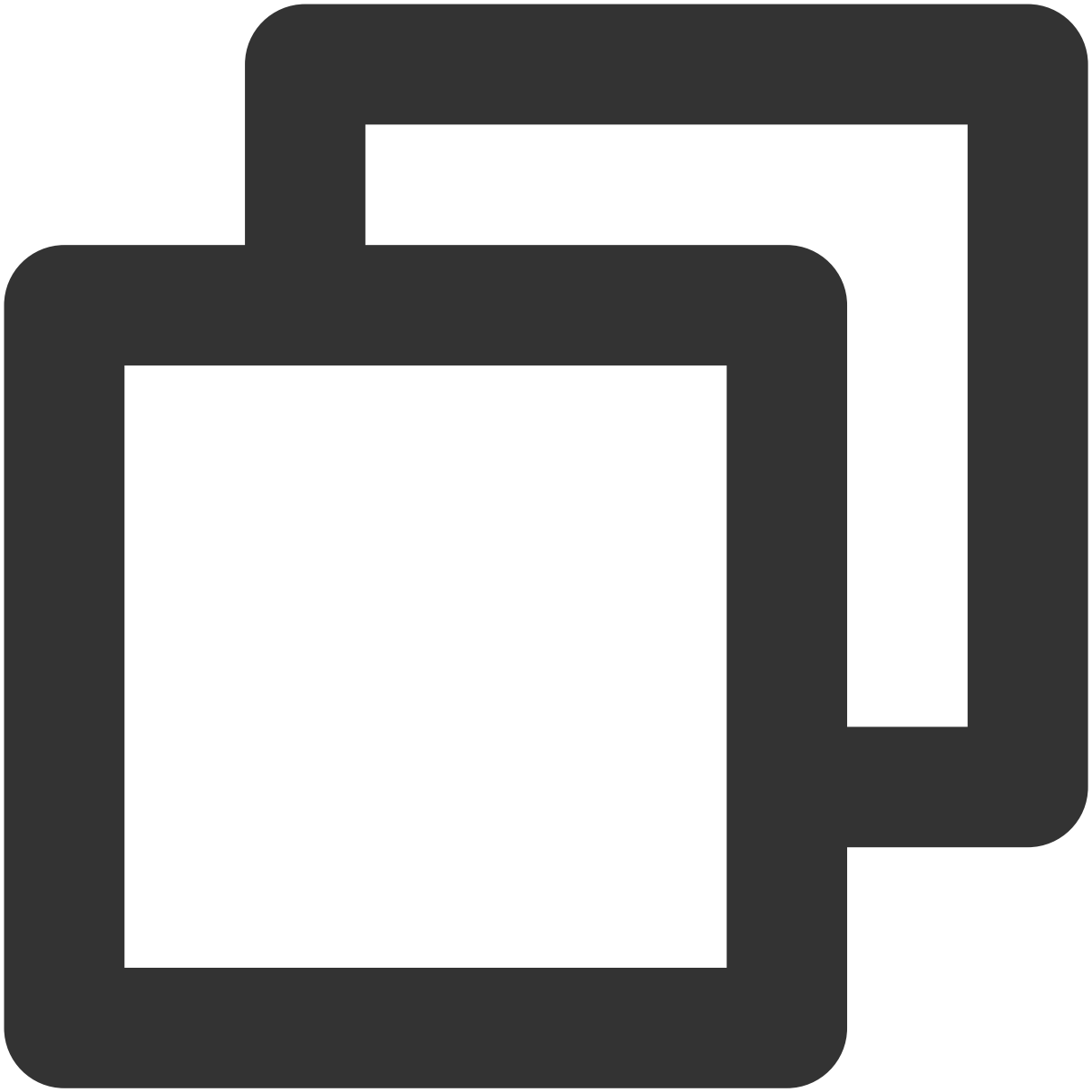
```
ALTER USER root@localhost IDENTIFIED VIA mysql_native_password USING PASSWORD('パス
```

6. 以下のコマンドを実行し、すべての構成を有効にします。



```
FLUSH PRIVILEGES;
```

7. 以下のコマンドを実行し、MariaDBを終了します。



```
\\q
```

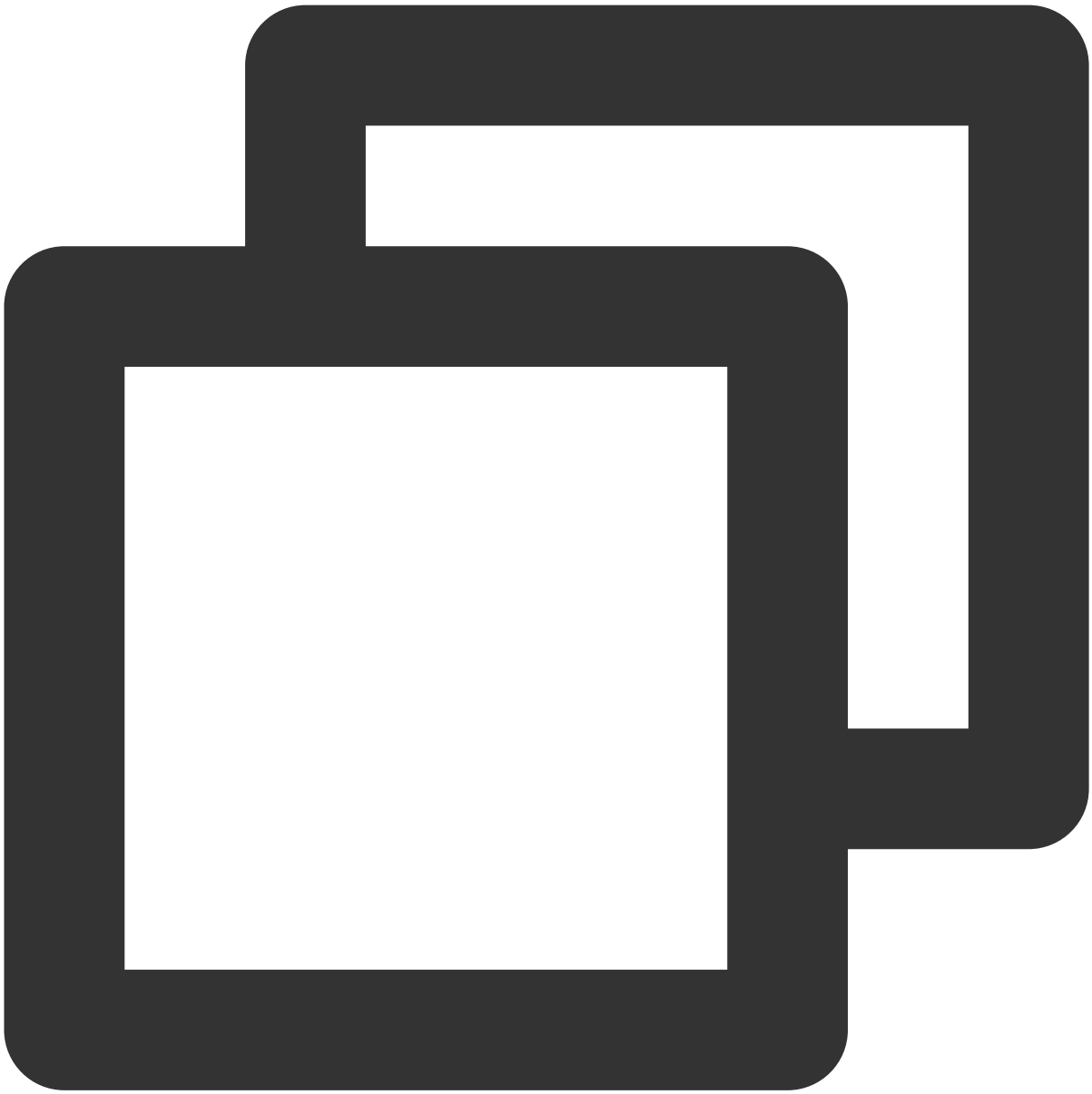
手順4：WordPressをインストールして設定する

WordPressのダウンロード

説明：

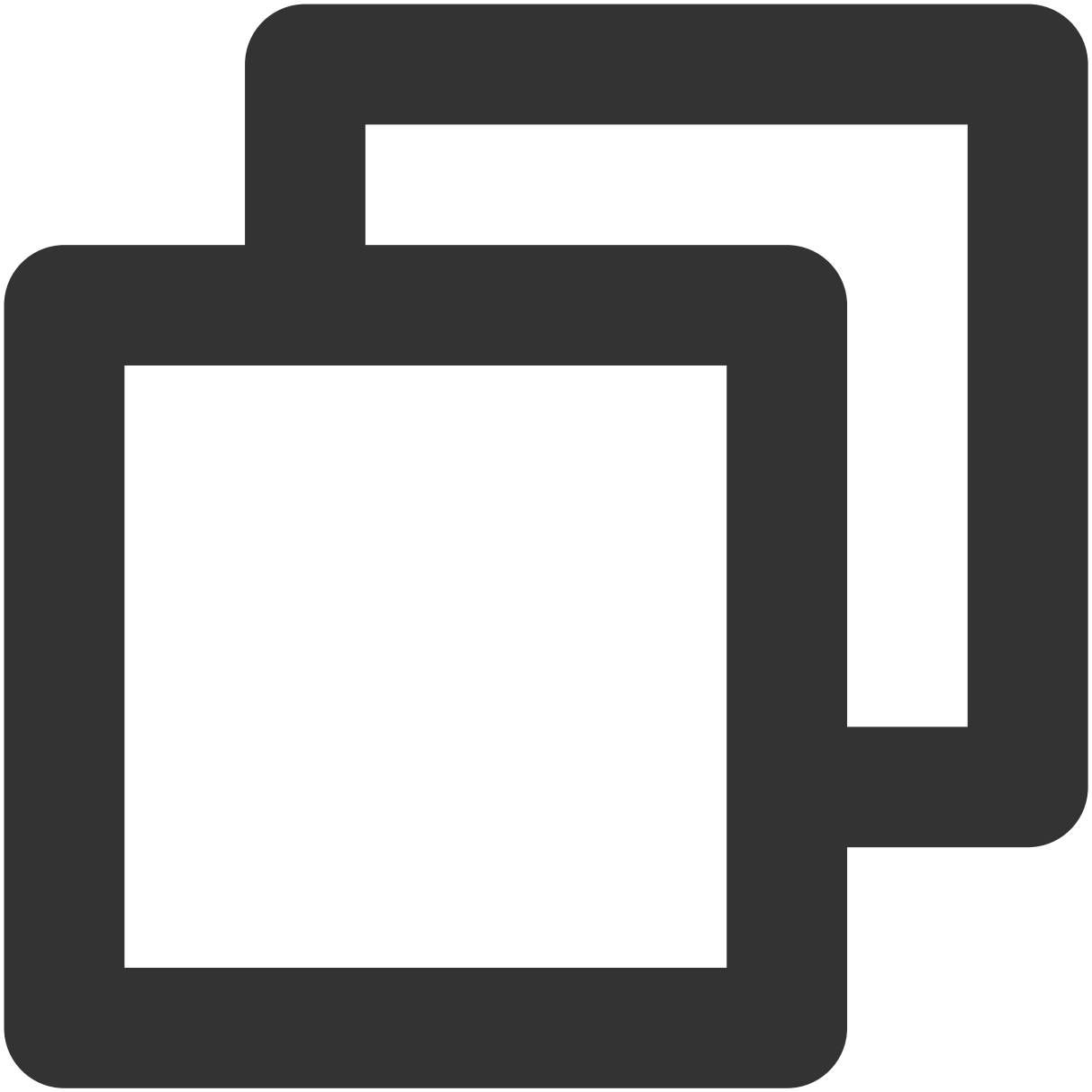
WordPressは、WordPressの公式ウェブサイトから最新のWordPress中国語版をダウンロードしてインストールできます。このドキュメントでは、WordPress中国語版を使用しています。

1. 以下のコマンドを実行し、ウェブサイトのルートディレクトリにあるPHP-Nginx設定をテストするための「index.php」ファイルを削除します。

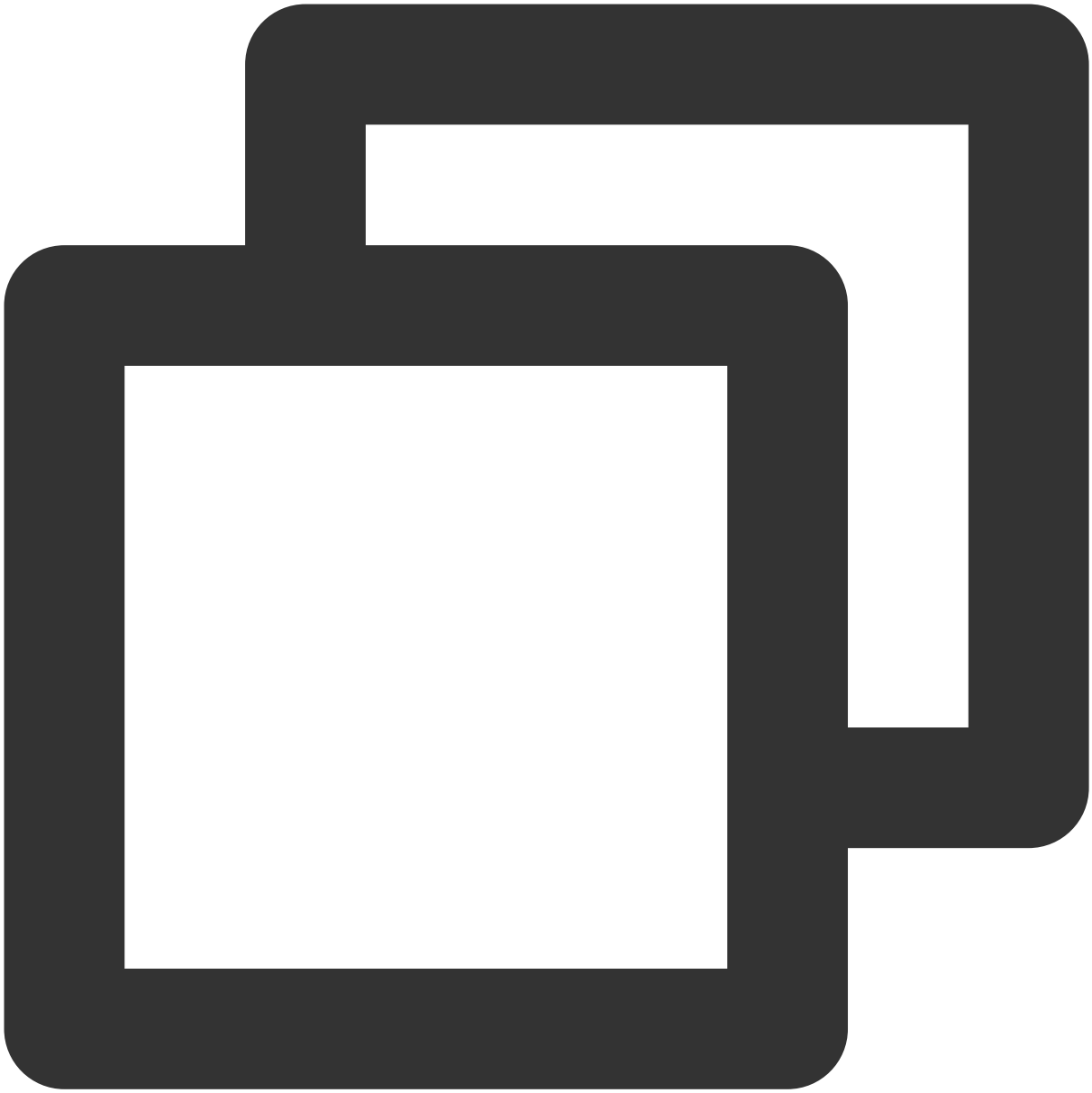


```
rm -rf /usr/share/nginx/html/index.php
```

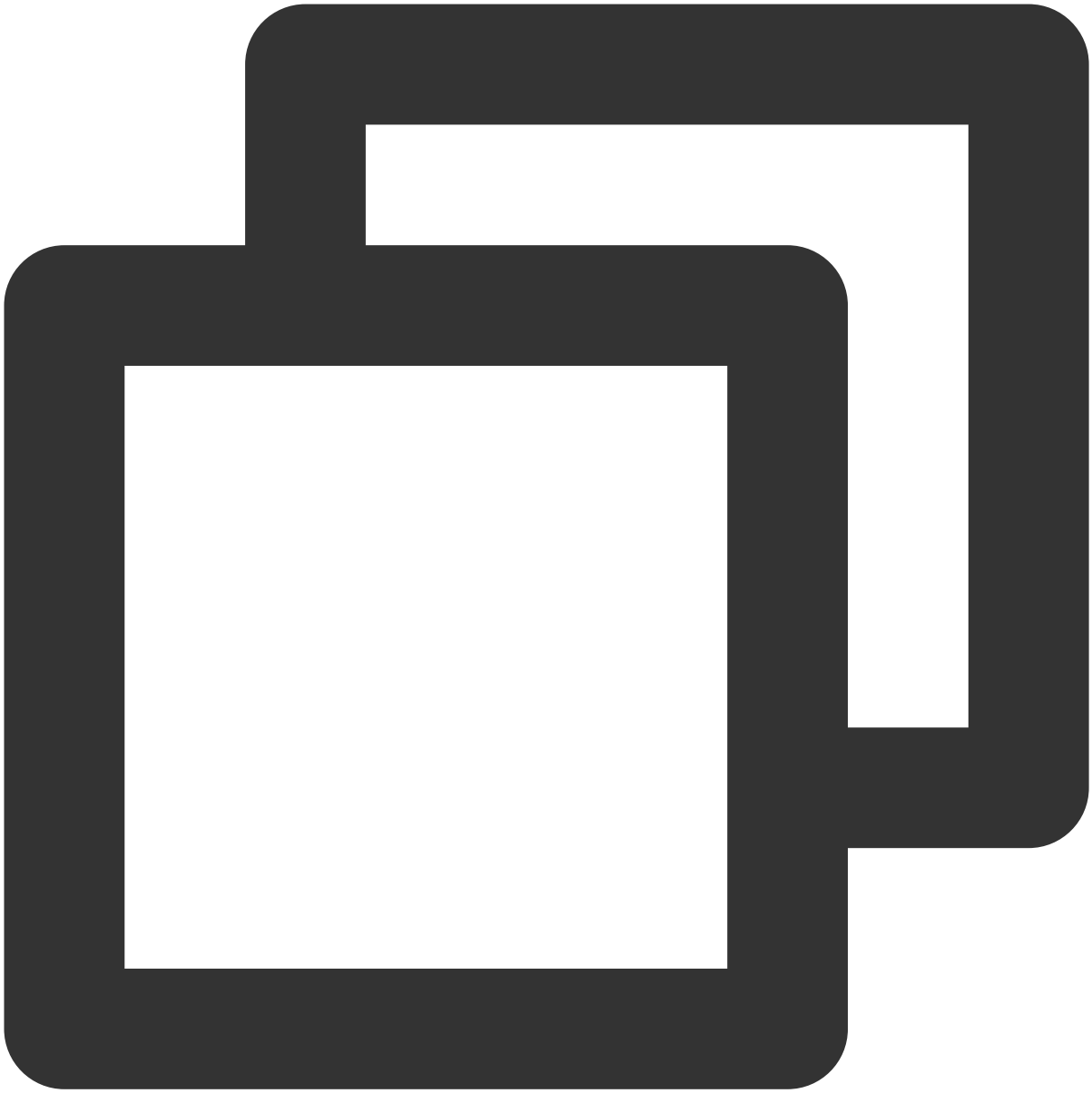
2. 以下のコマンドを順に実行し、「/usr/share/nginx/html/」ディレクトリに入り、WordPressをダウンロードしてから解凍します。



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



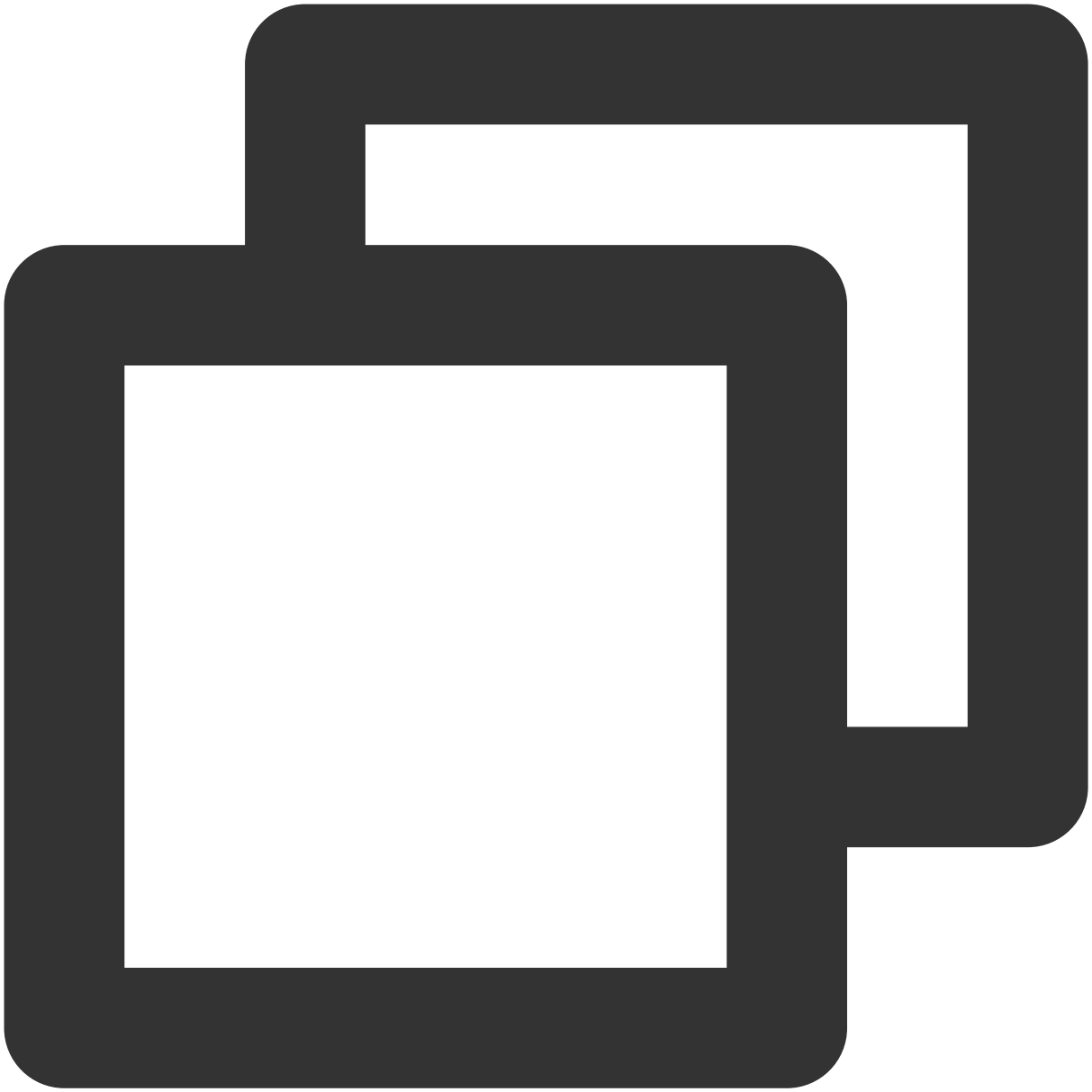
```
wget https://cn.wordpress.org/wordpress-5.0.4-zh_CN.tar.gz
```



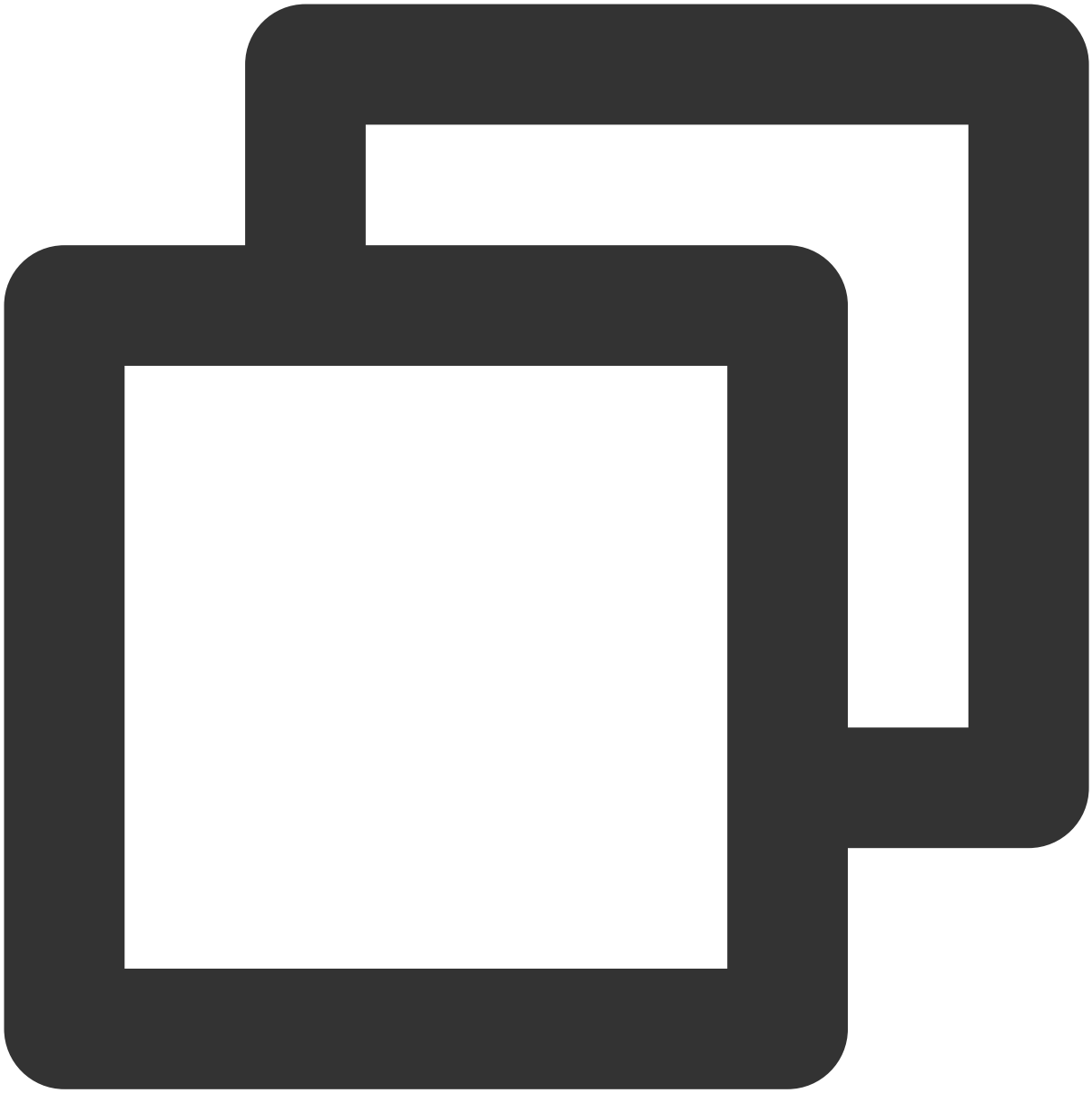
```
tar zxvf wordpress-5.0.4-zh_CN.tar.gz
```

WordPress設定ファイルの変更

1. 以下のコマンドを順に実行し、WordPressのインストールディレクトリに入り、「wp-config-sample.php」ファイルを「wp-config.php」ファイルにコピーし、元のサンプル設定ファイルをバックアップとします。

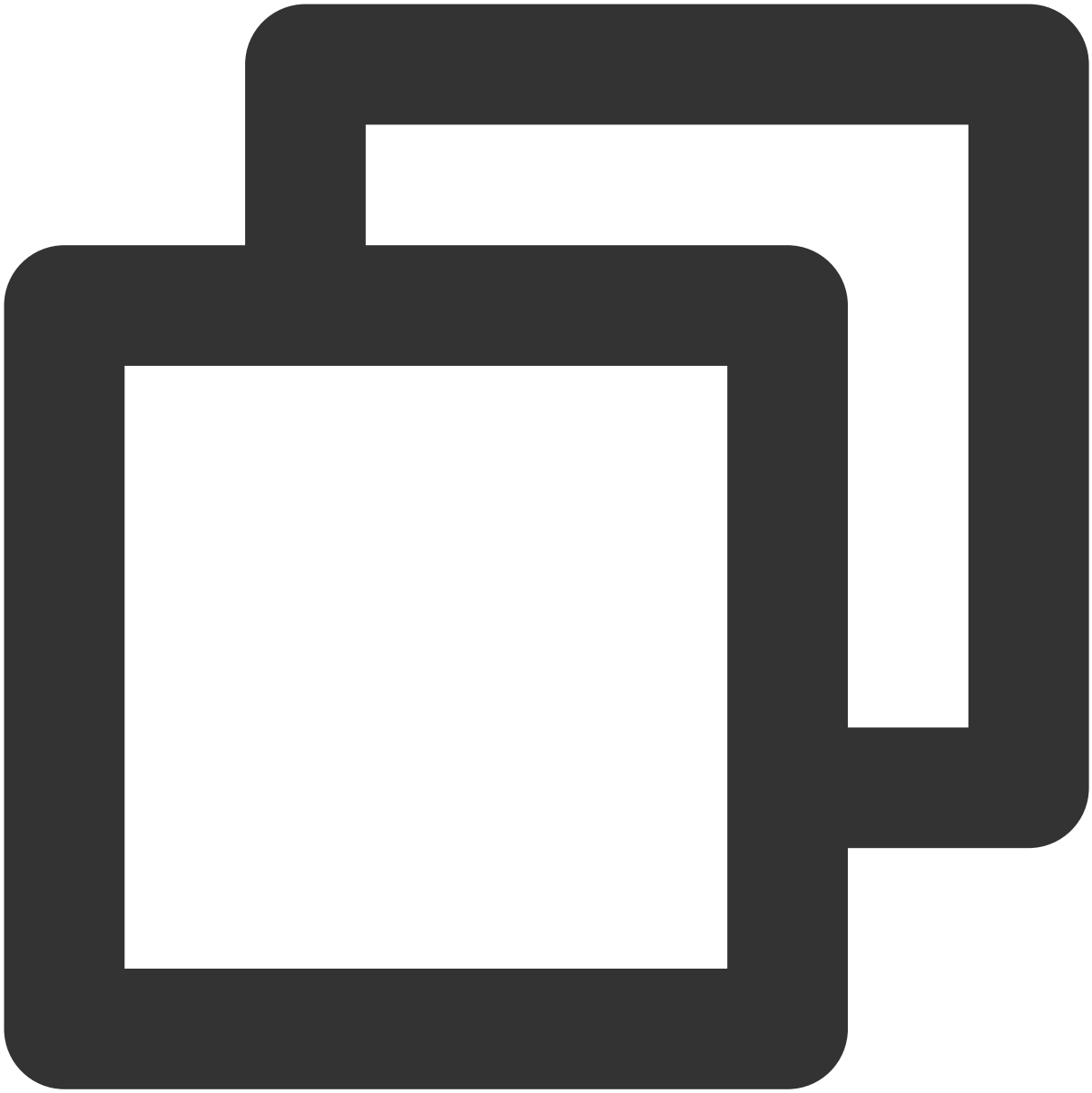


```
cd /usr/share/nginx/html/wordpress
```



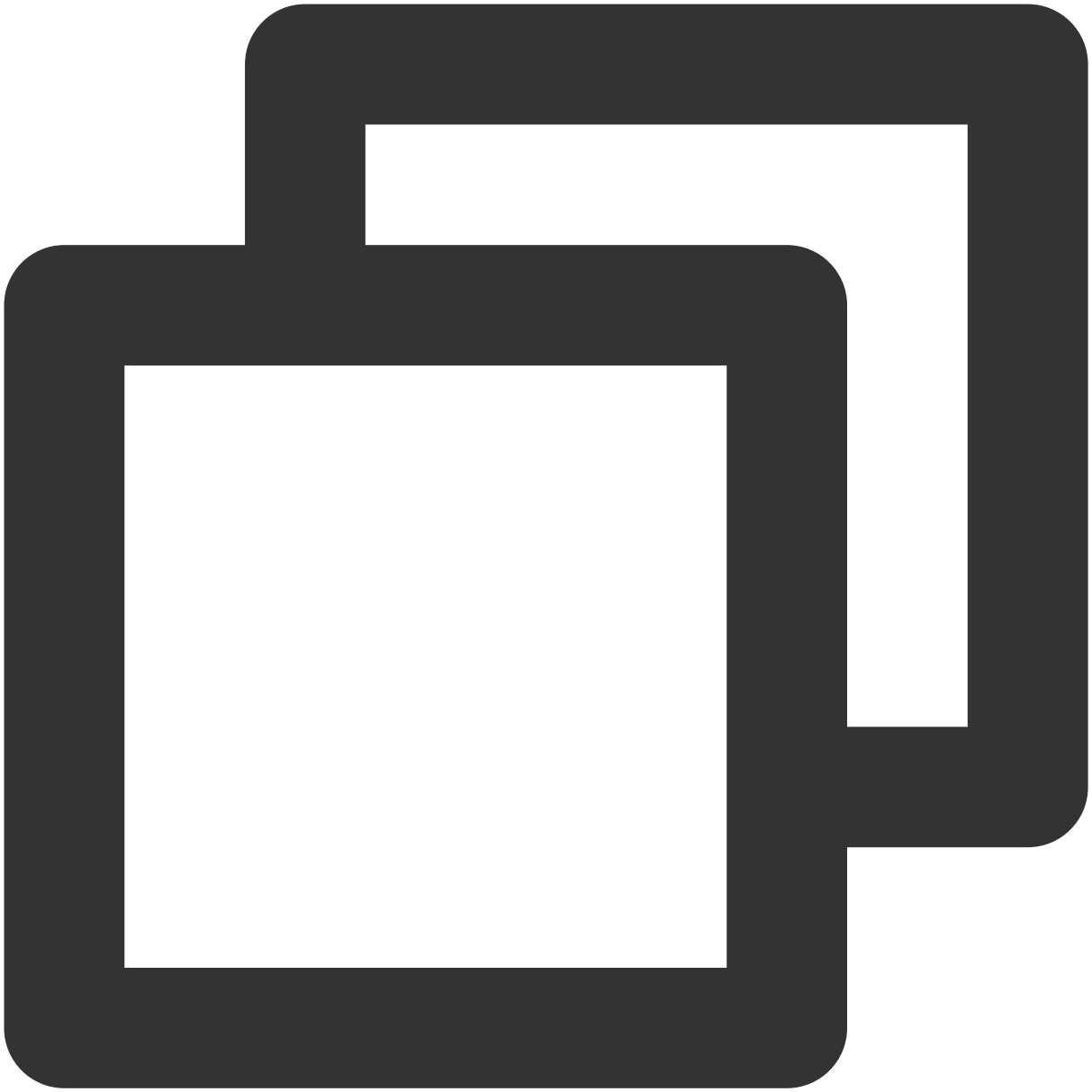
```
cp wp-config-sample.php wp-config.php
```

2. 以下のコマンドを実行し、新規作成された設定ファイルを開いて編集します。



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

3. **i**を押して、編集モードに入り、ファイルのMySQLの部分を見つけ、関連設定情報を WordPressデータベースの設定 の内容に変更ます。

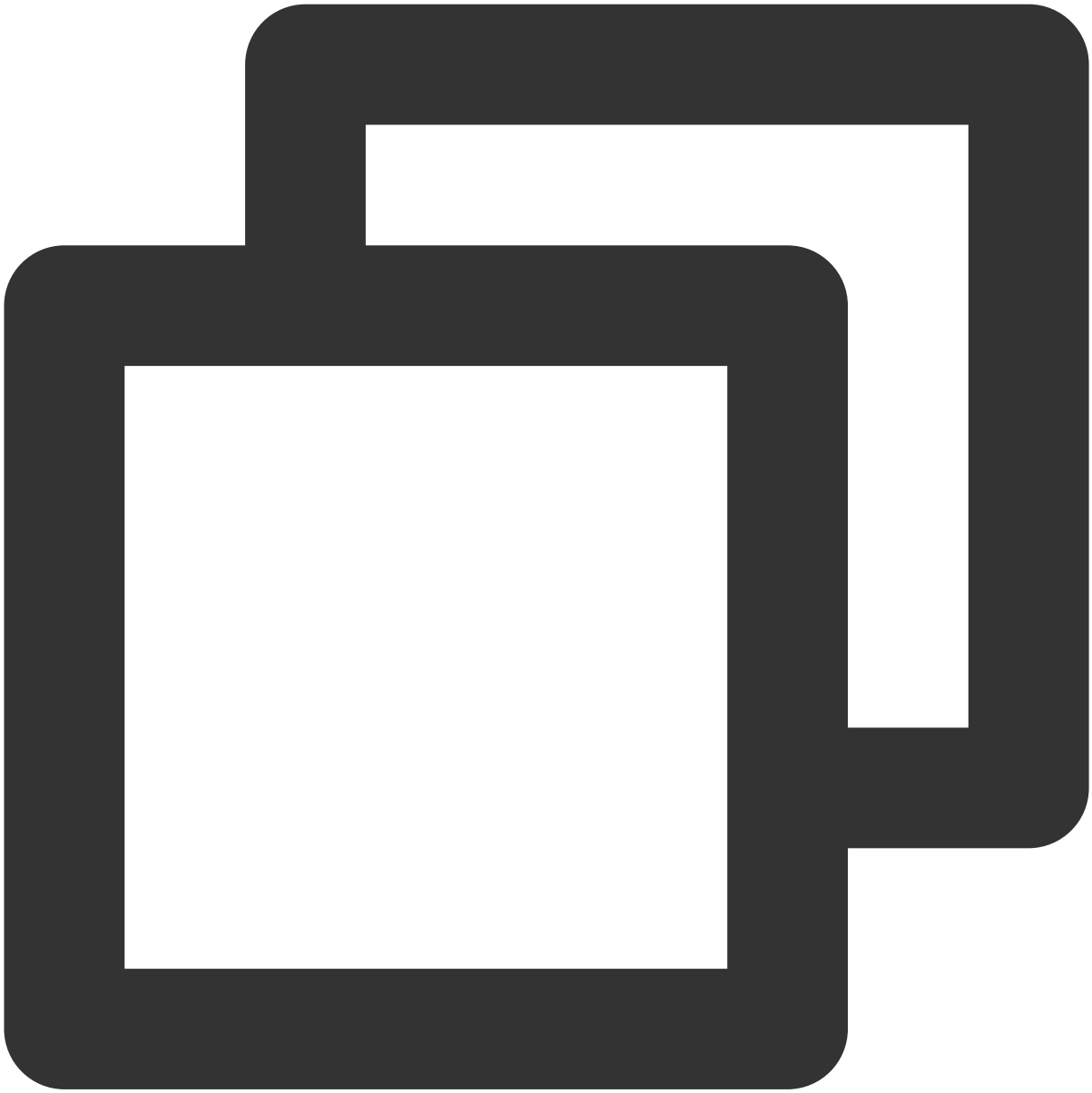


```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');
/** MySQL database username */
define('DB_USER', 'user');
/** MySQL database password */
define('DB_PASSWORD', '123456');
/** MySQL hostname */
define('DB_HOST',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

4. 変更した後に、**Esc**を押して、**:wq**を入力し、ファイルを保存して戻ります。

ステップ5： WordPress インストールの確認

1. ブラウザーのアドレス欄に「http://ドメイン名またはCVMインスタンスのパブリックIP/wordpressフォルダー」を入力します。例えば、



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

WordPressインストールページに入り、WordPressを設定します。

2. WordPressインストールウィザードの指示に従って、下記のインストール情報を入力し、**WordPressをインストールする**をクリックし、インストールを完了します。

必要な情	説明

報	
サイトのタイトル	WordPressウェブサイト名。
ユーザー名	WordPress 管理者の名前。セキュリティのために、 adminと異なる名前を設定することをお勧めします。デフォルトユーザー名であるadmin と比べては、当該名前は一層クラックしにくいようにする必要があります。
パスワード	デフォルトの強いパスワードまたはカスタマイズパスワードを使用できます。既存のパスワードを重複に使用せず、パスワードを安全の場所に保管してください。
メール	通知を受信するためのメールアドレスです。

これからWordPressブログにログインし、ブログ投稿を行うことが可能になります。

関連する操作

自分のWordPressブログサイト用に別のドメイン名を設定できます。ユーザーは複雑なIPアドレスを使用せずに、覚えやすいドメイン名でWebサイトにアクセスできます。 一部のユーザーは学習目的でのみWebサイトを構築するため、IPアドレスを使用して直接インストールしては一時的に使用できますが、このような操作はお勧めできません。

よくあるご質問

CVMの使用中に問題が発生した場合は、下記のドキュメントを参照しながら実際状況に合わせ分析した上で問題を解決することが可能です。
CVMのログインに関する問題は、パスワードとキー、ログインとリモート接続 ドキュメントをご参照ください。
CVMのネットワークに関する問題は、 IPアドレス、ポートとセキュリティグループ ドキュメントをご参照ください。
CVMのハードディスクに関する問題は、システムディスクとデータディスクドキュメントをご参照ください。

WordPress個人サイト（Windows）の手動による構築

最終更新日：：2022-05-06 16:57:27

概要

WordPressはPHP言語で開発されたブログプラットホームです。WordPressにより個人のブログプラットホームを構築することが可能です。このドキュメントでは、Windows Server 2012 OSのTencent Cloud CVMを例として取り上げ、手動でWordPressの個人サイトを構築することについて説明します。

ご注意：

手動による構築プロセスには長い時間がかかる場合があるため、Tencent Cloudは、クラウド市場のイメージ環境を介してWordPressの個人ブログをデプロイすることをお勧めします。

ソフトウェアバージョン

WordPressの個人サイトは、PHP 5.6.20以降のバージョンおよびMySQL 5.0以降のバージョンで構築できます。セキュリティを強化するために、WordPressの個人サイトを構築するとき、PHP 7.3以降のバージョンおよびMySQL 5.6以降のバージョンを選択してインストールすることをお勧めします。

このドキュメントでは、構築するWordPressの個人サイトの構成バージョンおよびその説明は次のとおりです：

Windows：Windows OSです。このドキュメントでは、64ビットの中国語版のWindows Server 2012 R2 Data Center Editionを例として説明します。

IIS：Webサーバーです。このドキュメントでは、IIS 8.5を例として説明します。

MySQL：データベースです。このドキュメントでは、MySQL 8.0.19を例として説明します。

PHP：スクリプト言語です。このドキュメントでは、PHP 7.1.30を例として説明します。

WordPress：ブログプラットフォームです。このドキュメントでは、WordPress 5.9を例として説明します。

操作手順

ステップ1：CVMにログインする

RDPファイルを使用したWindowsインスタンスへのログイン（推奨）。

また、実際の操作習慣に応じて、リモートデスクトップとの接続によるWindowsインスタンスへのログイン。

手順2：WIPM環境を構築する

WIPM環境の手動構築 を参照して、以下のとおり操作します：

1. IISサービスをインストールします。

2. PHP 5.6.20以降のバージョンの環境をデプロイします。

3. MySQL 5.6以降のバージョンのデータベースをインストールします。

手順3：WordPressをインストールして設定する

説明：

WordPressは、WordPressの公式ウェブサイトから最新のWordPress中国語版をダウンロードしてインストールできます。このドキュメントでは、WordPress中国語版を使用しています。

1. WordPressをダウンロードして、WordPressインストールパッケージをCVMに解凍します。

例えば、WordPressインストールパッケージを `C:\\wordpress` ディレクトリに解凍します。

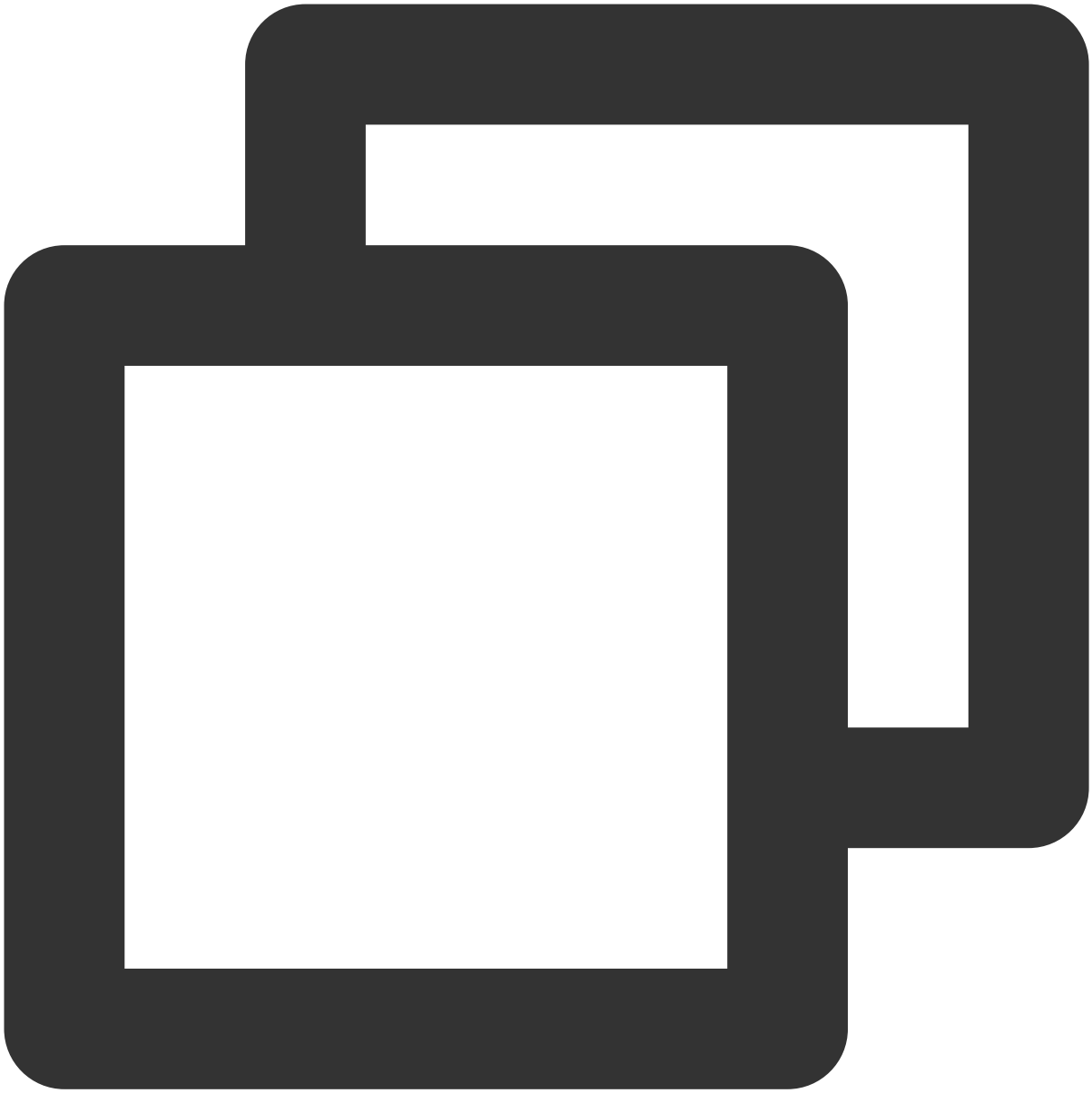
2.

>

> **MySQL 5.6 Command Line Client**をクリックして、MySQLTencent Cloud Command Line Interfaceクライアントを開きます。

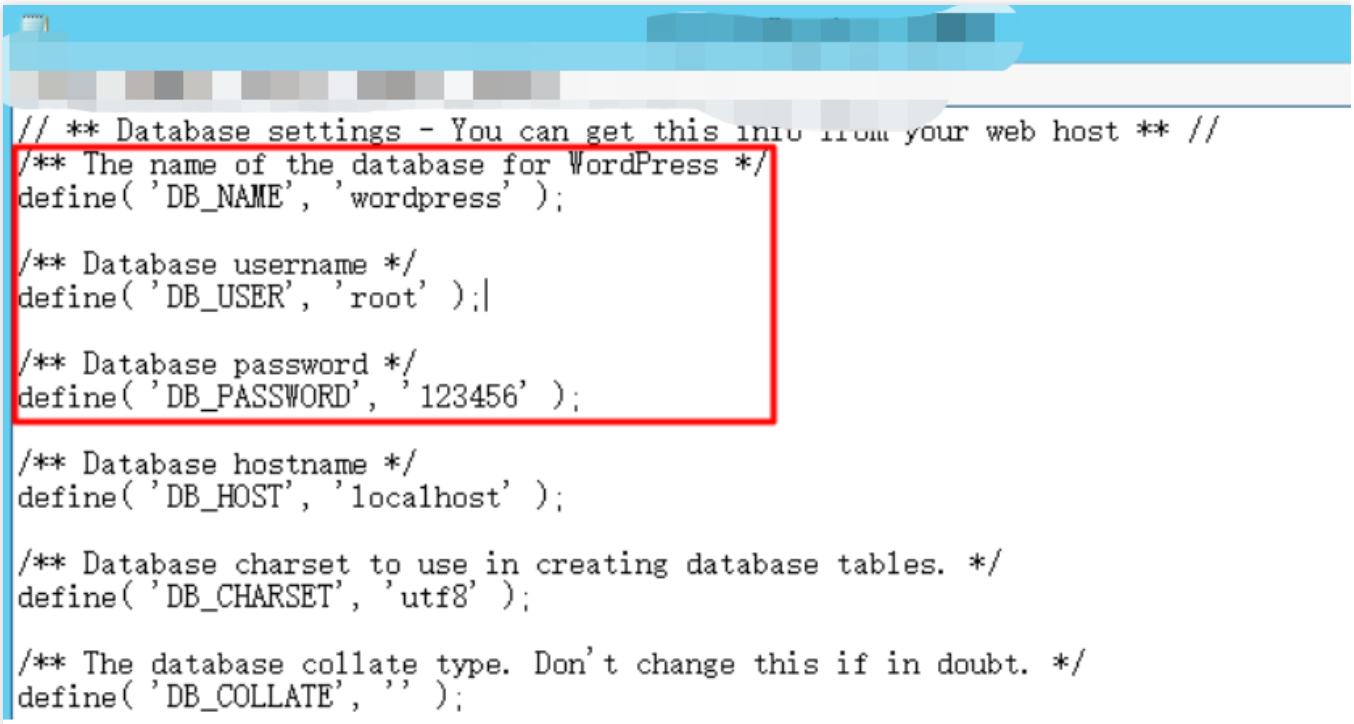
3. MySQL Tencent Cloud Command Line Interfaceクライアントでは、次のコマンドを実行して、WordPressデータベースを作成します。

例えば、「wordpress」データベースを作成します。



```
create database wordpress;
```

4. WordPressの解凍したインストールパスで、 `wp-config-sample.php` ファイルを見つけてコピーし、ファイルの名前を `wp-config.php` に変更します。
5. テキストエディタで `wp-config.php` ファイルを開き、関連する設定情報を 手順3：MySQLデータベースをインストールする の内容に変更します。下図の通りです：



6. `wp-config.php` ファイルを保存します。
7.  をクリックして、サーバーマネージャーを開きます。
8. サービスマネージャーの左側ナビゲーションバーで**IIS**を選択し、右側のIIS管理ウィンドウで**サーバー**列のサーバー名を右クリックして、**Internet Information Sevices (IIS)マネージャー**を選択します。
9. 開かれた「Internet Information Sevices (IIS)マネージャー」ウィンドウで、左側のナビゲーションバーにあるサーバー名を展開して、**ウェブサイト**をクリックして、「ウェブサイト」管理ページに進みます。
10. **ウェブサイト**の下のポート80にバインディングされているウェブサイトを削除します。
ウェブサイトのバインディングポートを別の占有されていないポート番号に変更することもできます。例えば、8080ポートに変更します。
11. 右側の**操作**列で、**ウェブサイトの追加**をクリックします。
12. ポップアップ表示されたウィンドウで、下記情報を記入して、**OK**をクリックします。
ウェブサイト名：wordpressなど、ユーザーによってカスタマイズされます。
アプリケーションプール：**DefaultAppPool**として選択します。
物理パス： `C:\\wordpress` など、WordPressが解凍された後のパスを選択します。
13. PHPの解凍したインストールパスで、 `php.ini` ファイルを開き、次の内容を変更します。
13.1 PHPバージョンに応じて、対応する構成パラメータを変更します：
PHPバージョン5.Xの場合、 `extension=php_mysql.dll` を見つけて、前の `;` を削除します。
PHPバージョン7.Xの場合、 `extension=php_mysqli.dll` または `extension=mysqli` を見つけて、前の `;` を削除します。

13.2 `extension_dir = "ext"` を見つけて、前の `;` を削除します。
14. `php.ini` ファイルを保存します。

ステップ4：WordPressの設定を確認する

1. ブラウザを使用して `http://localhost/wp-admin/install.php` にアクセスし、WordPressインストールページに進み、WordPressを設定します。
2. WordPressインストールウィザードの指示に従って、下記のインストール情報を入力し、**WordPressをインストールする**をクリックし、インストールを完了します。

必要な情報	説明
サイトタイトル	WordPressウェブサイト名です。
ユーザー名	WordPress管理者の名前です。セキュリティのために、adminと異なる名前を設定することをお勧めします。デフォルトユーザー名であるadminと比べて、この名前はクラックしにくいです。
パスワード	強力なデフォルトパスワードまたはカスタマイズパスワードを使用できます。既存のパスワードを再利用しないでください。また、パスワードを安全な場所に保管してください。
Eメール	通知を受け取るために使用されるEメールアドレスです。

これからWordPressブログにログインし、ブログ投稿を行うことが可能になります。

よくあるご質問

CVMの使用中に問題が発生した場合は、下記のドキュメントを参照しながら実際状況に合わせ分析した上で問題を解決することが可能です：
CVMのログインに関する問題については、パスワードとキー、ログインとリモート接続 をご参照ください。
CVMのネットワークに関する問題については、IPアドレス、ポートとセキュリティグループ をご参照ください。
CVMのハードディスクに関する問題については、システムディスクとデータディスク をご参照ください。

Discuz!フォーラムを構築する
Discuz!フォーラムを手動で構築する

最終更新日：：2022-05-10 11:38:10

概要

Discuz!は、成熟度が最も高く、世界最大のフォーラムWebサイトのソフトウェアシステムの1つであり、200万人を超えるWebサイトユーザーによって使用されています。 Discuz! を通じてフォーラムを構築できます。本ドキュメントでは、Tencent Cloud CVMインスタンスで Discuz! フォーラムと必要な LAMP（Linux + Apache + MariaDB + PHP）環境を構築する方法について説明します。
手動でDiscuz! フォーラムを構築するには、Linux コマンド（例：CentOS環境でのYUMを使用してソフトウェアのインストール）等の常用コマンドに精通している必要があります。また、インストールされているソフトウェアの使い方及びバージョン間の互換性について十分に理解している必要があります。

ソフトウェアのバージョン

この記事で作成したDiscuz!フォーラムソフトウェアのバージョンと説明は次の通り：
Linux：Linux OS、本ドキュメントはCentOS 7.6を例として説明します。
Apache：Webサーバー、この記事では、 Apache 2.4.15 を例として説明します。
MariaDB：データベース、この記事では、 MariaDB 5.5.60を例として説明します。
PHP：スクリプト言語、この記事では、PHP 5.4.16を例として説明します。
Discuz!：フォーラムウェブサイトソフトウェア、この記事では、Discuz! X3.4を例として説明します。

操作手順

ステップ1：CVMにログインする

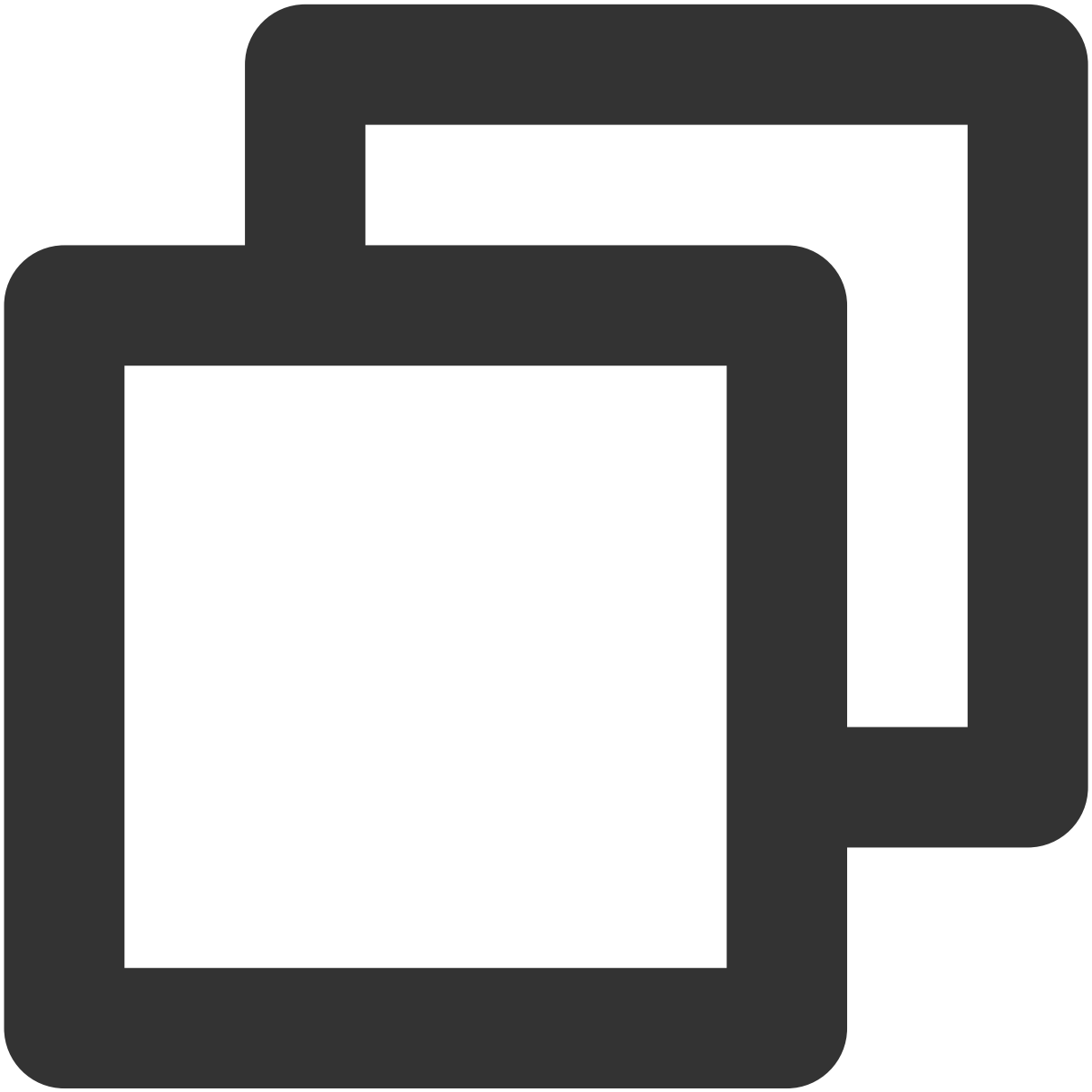
標準的な方法を使用してLinuxインスタンスにログインする（推奨）。実際の操作方法に応じて、他のログイン方法を選択することもできます：
リモートログインソフトウェアを使用してLinuxインスタンスにログインする
SSHキーを使用してLinuxインスタンスにログインする

手順2：LAMP環境を構築する

CentOSシステムの場合、Tencent CloudはCentOS公式のソフトウェアと同期するソフトウェアインストールソースを提供します。同梱されているソフトウェアは現在最も安定したバージョンであり、Yumを介して直接インストールできます。

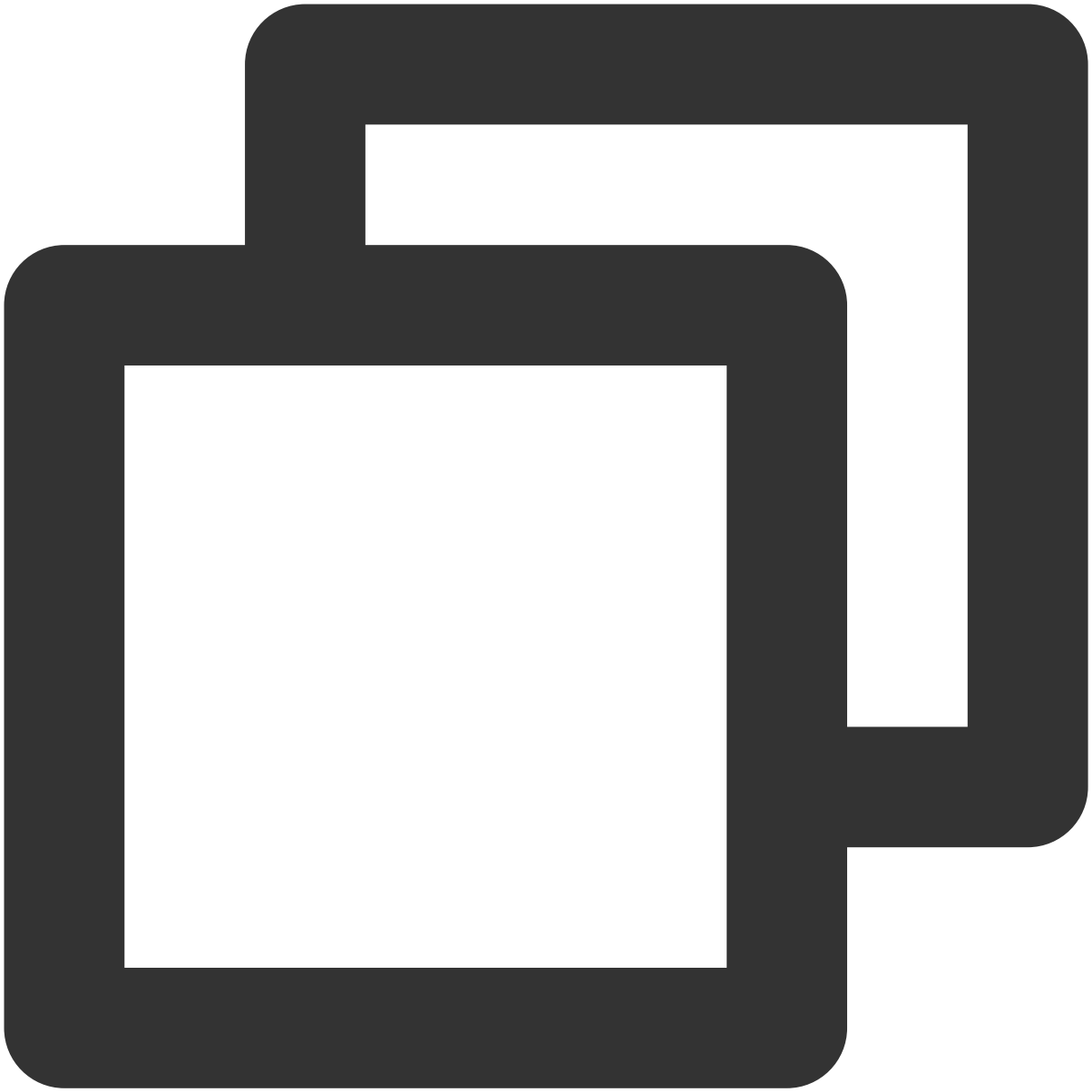
必要ソフトウェアをインストールして設定する

1. 次のコマンドを実行して、必要なソフトウェア（Apache、MariaDB、PHP、Git）をインストールします：

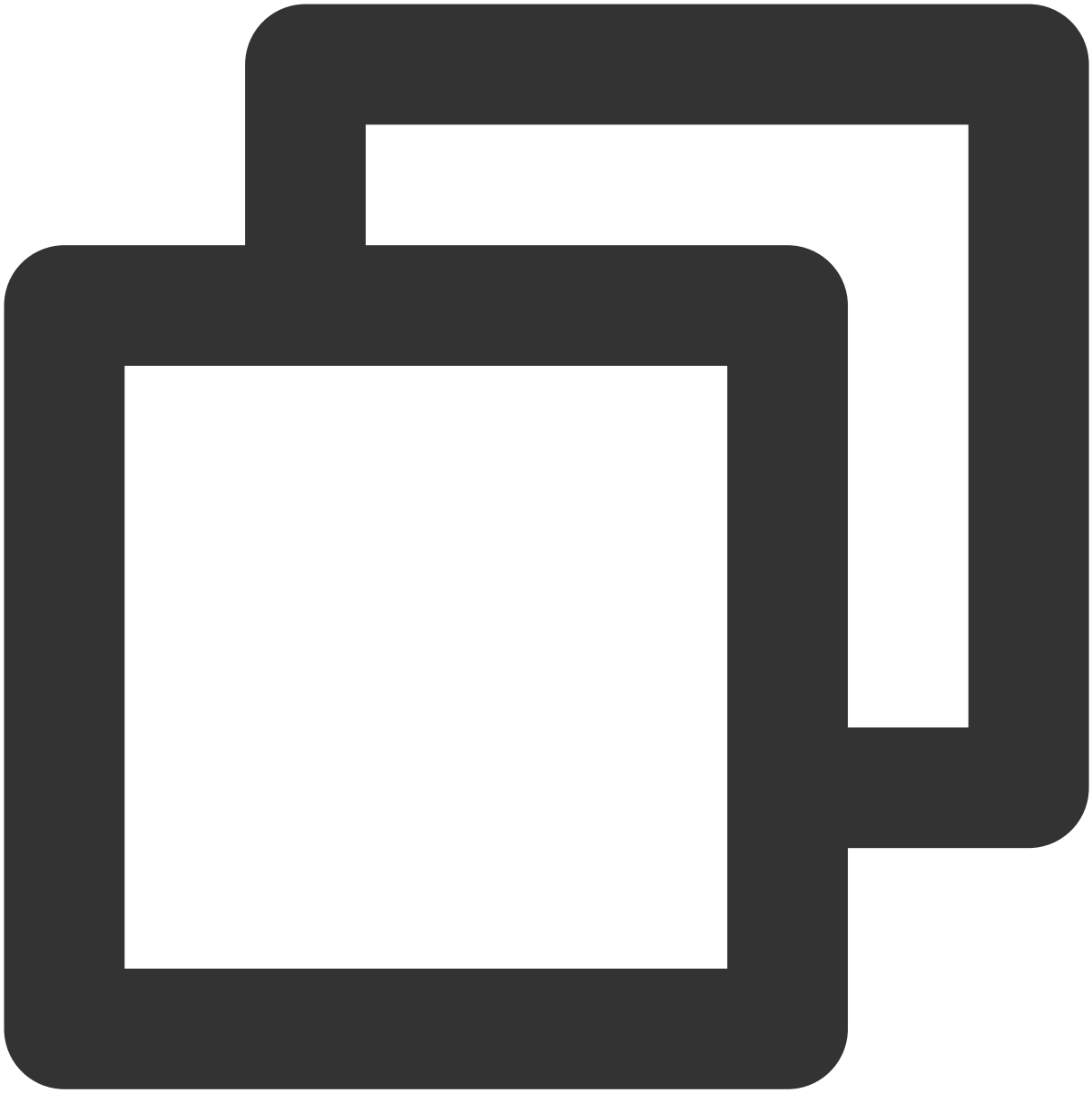


```
yum install httpd php php-fpm php-mysql mariadb mariadb-server git -y
```

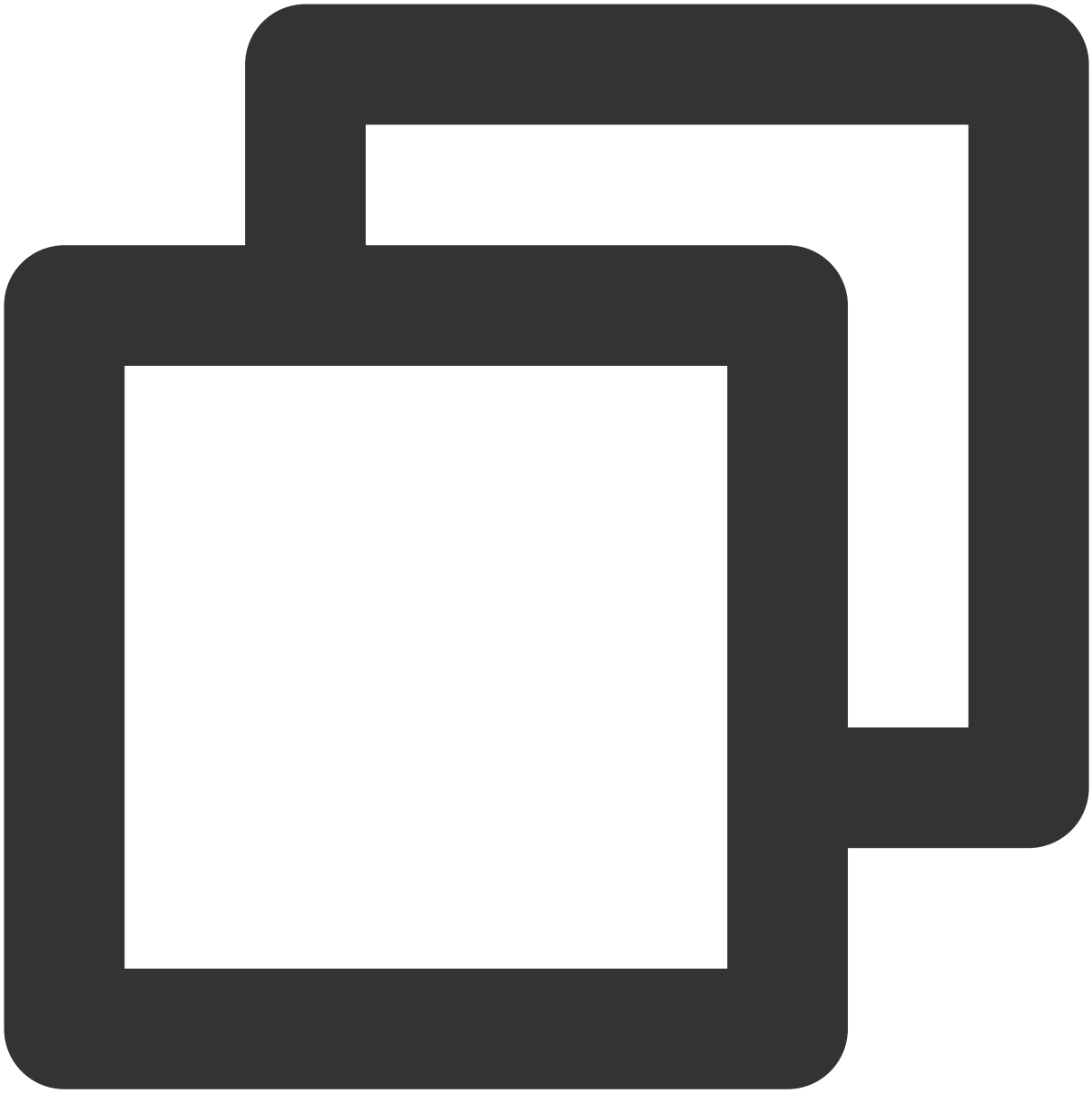
2. 下記のコマンドを順に実行して、サービスを起動します。



```
systemctl start httpd
```



```
systemctl start mariadb
```

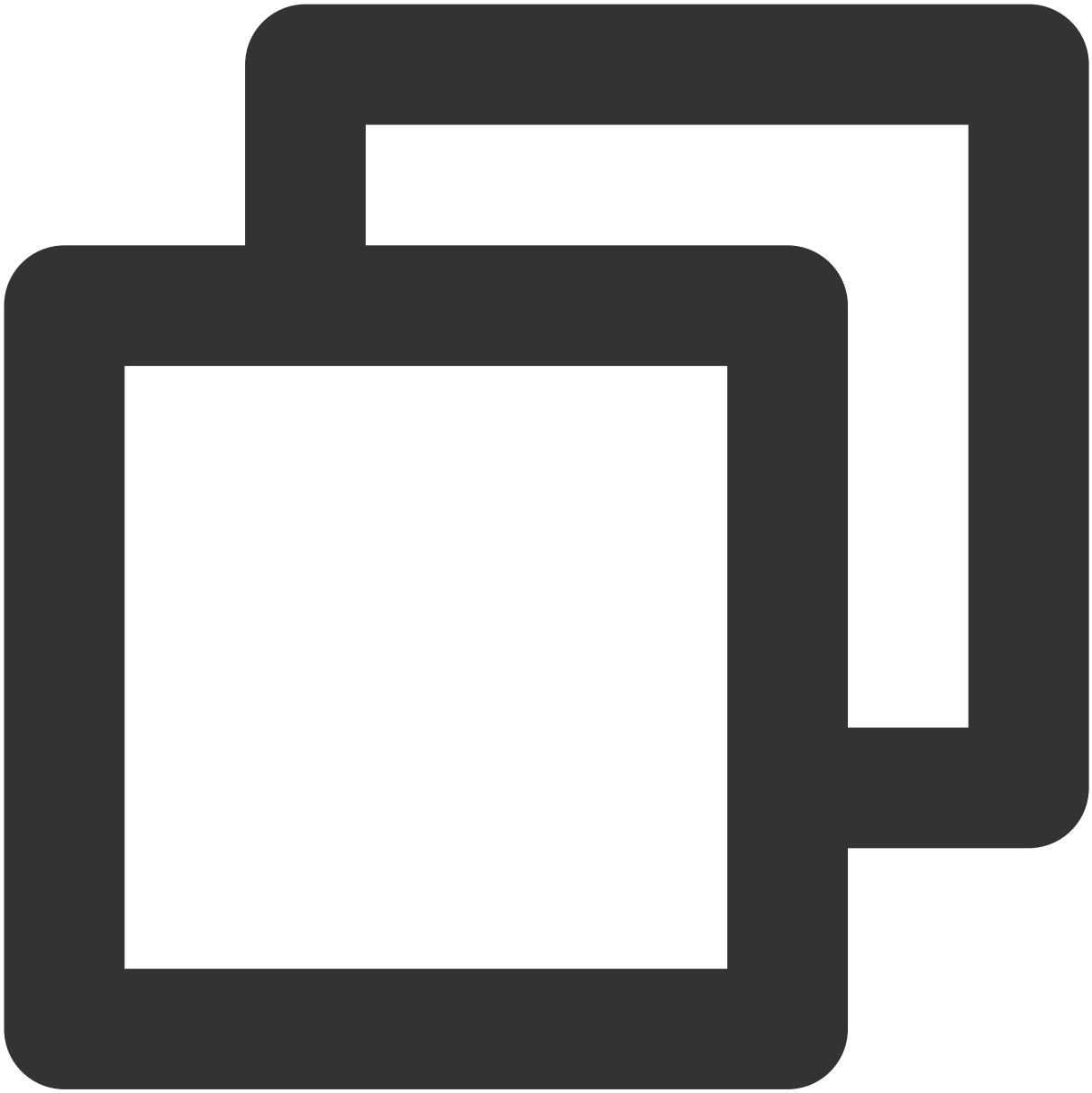


```
systemctl start php-fpm
```

3.
次のコマンドを実行して、rootアカウントのパスワードと基本構成を設定し、rootユーザーがデータベースにアクセスできるようにします。

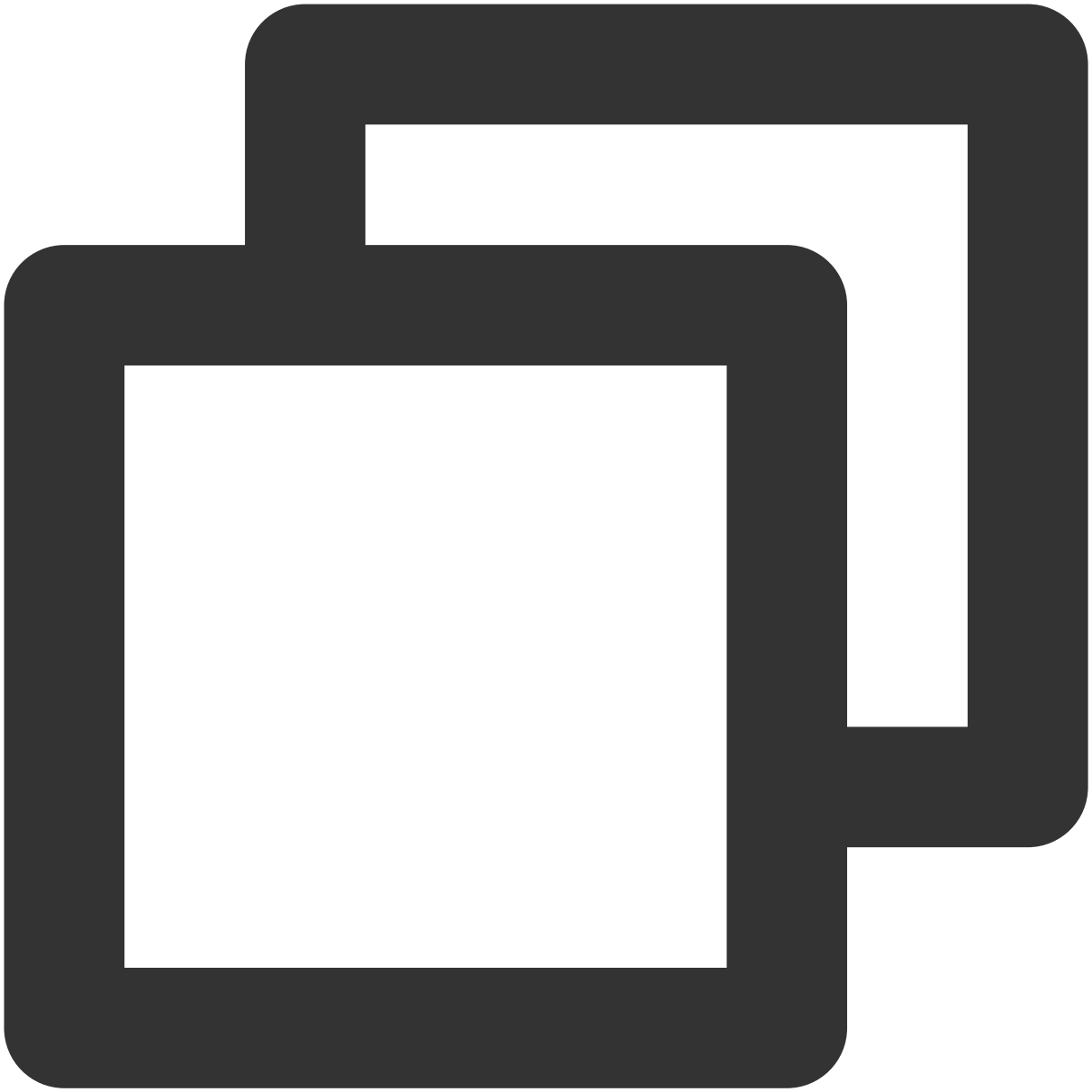
ご注意：
MariaDBに初めてログインする前に、次のコマンドを実行してユーザーパスワードの入力と基本設定を行います。

rootパスワードの入力を求めるプロンプトが初めて表示されたら、 **Enter**を押して rootパスワード設定手順に直接進みます。rootパスワードは設定の際、デフォルトでは画面に表示されません。画面上の指示に従ってその他の基本構成を順に完了してください。



```
mysql_secure_installation
```

4. 次のコマンドを実行し、MariaDBにログインして、手順3 で設定したパスワードを入力し、**Enter**キーを押します。

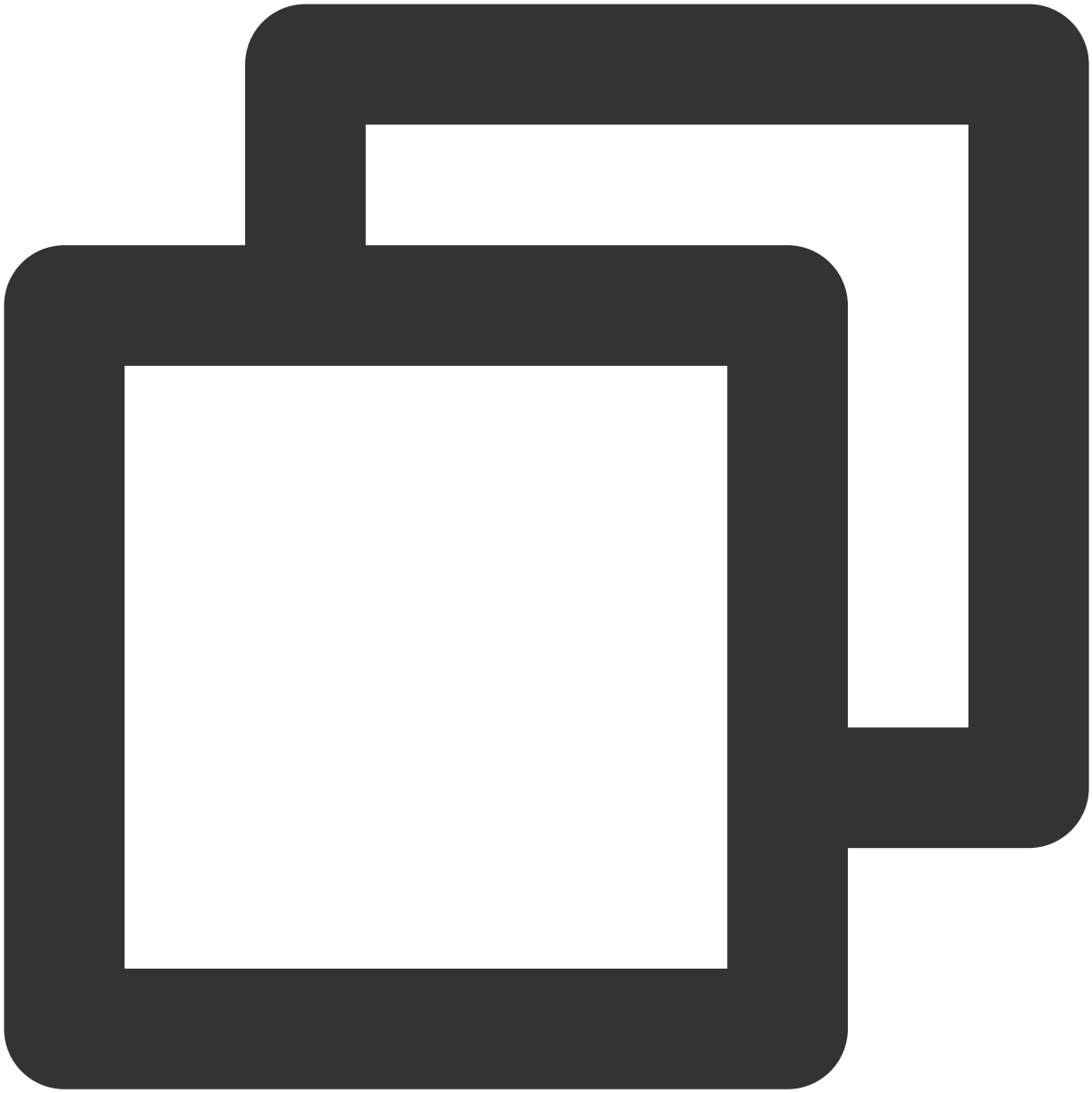


```
mysql -u root -p
```

設定したパスワードを入力してMariaDBにログインできる場合、設定は正しいことを示します。 次の図に示すように：

```
[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 stateme

MariaDB [(none)]>
```

5. 次のコマンドを実行し、 MariaDBデータベースを終了します。

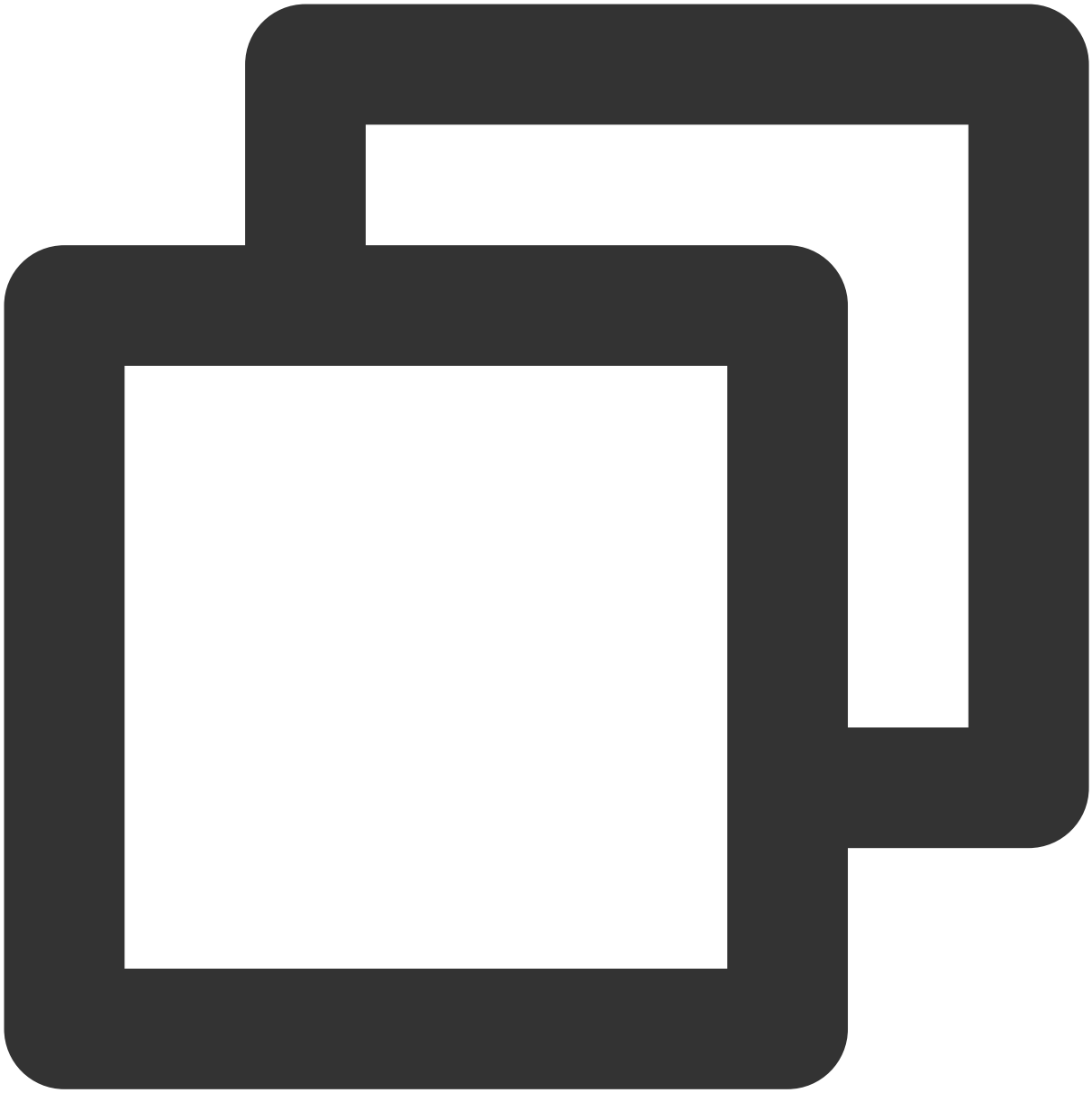


```
\\q
```

環境設定の検証

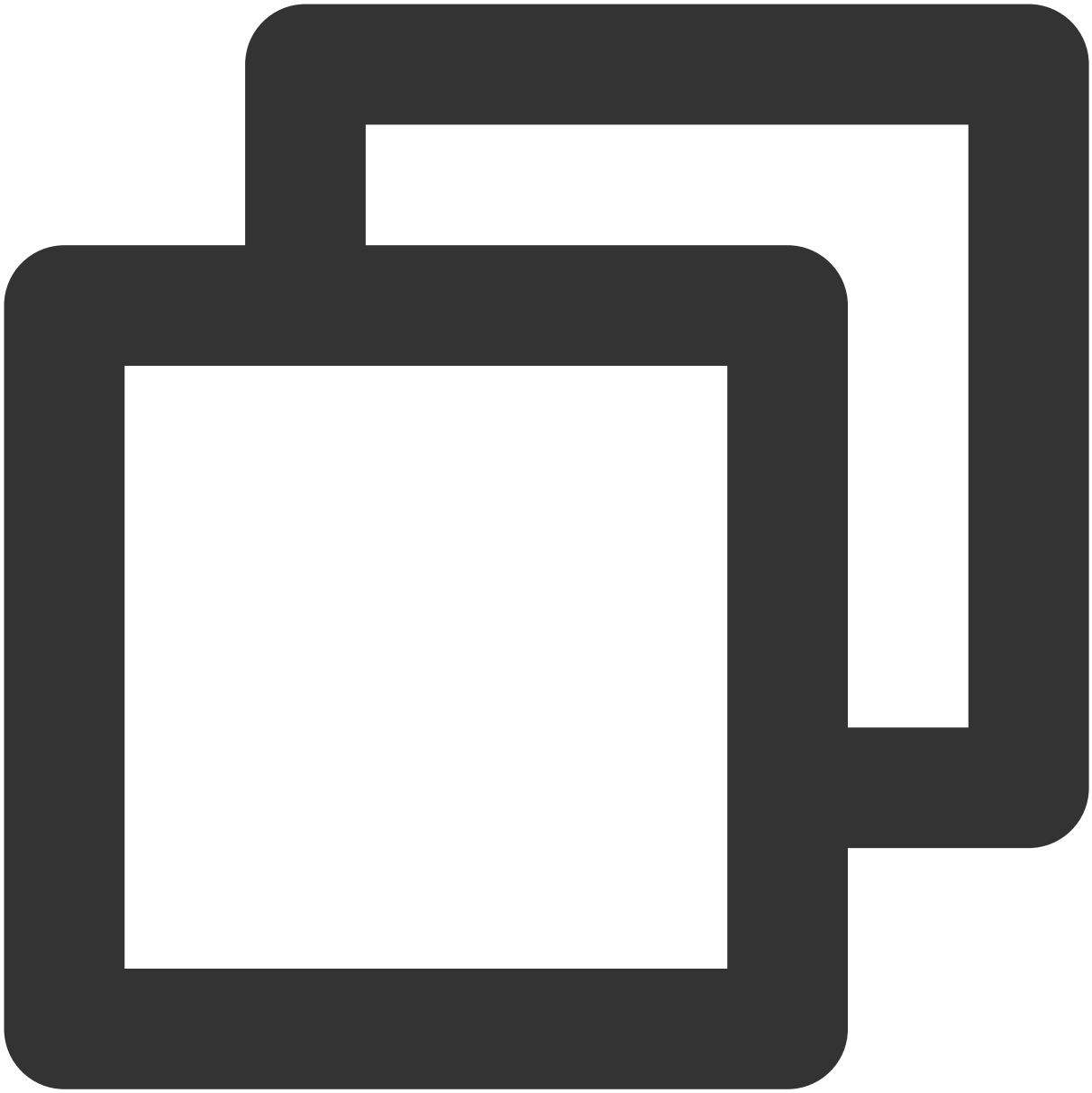
環境が正常に構築されていることを確認するには、次の操作を実行して検証できます：

1. 次のコマンドを実行して、Apacheのデフォルトのルートディレクトリ `/var/www/html` にテストファイル `test.php` を作成します。



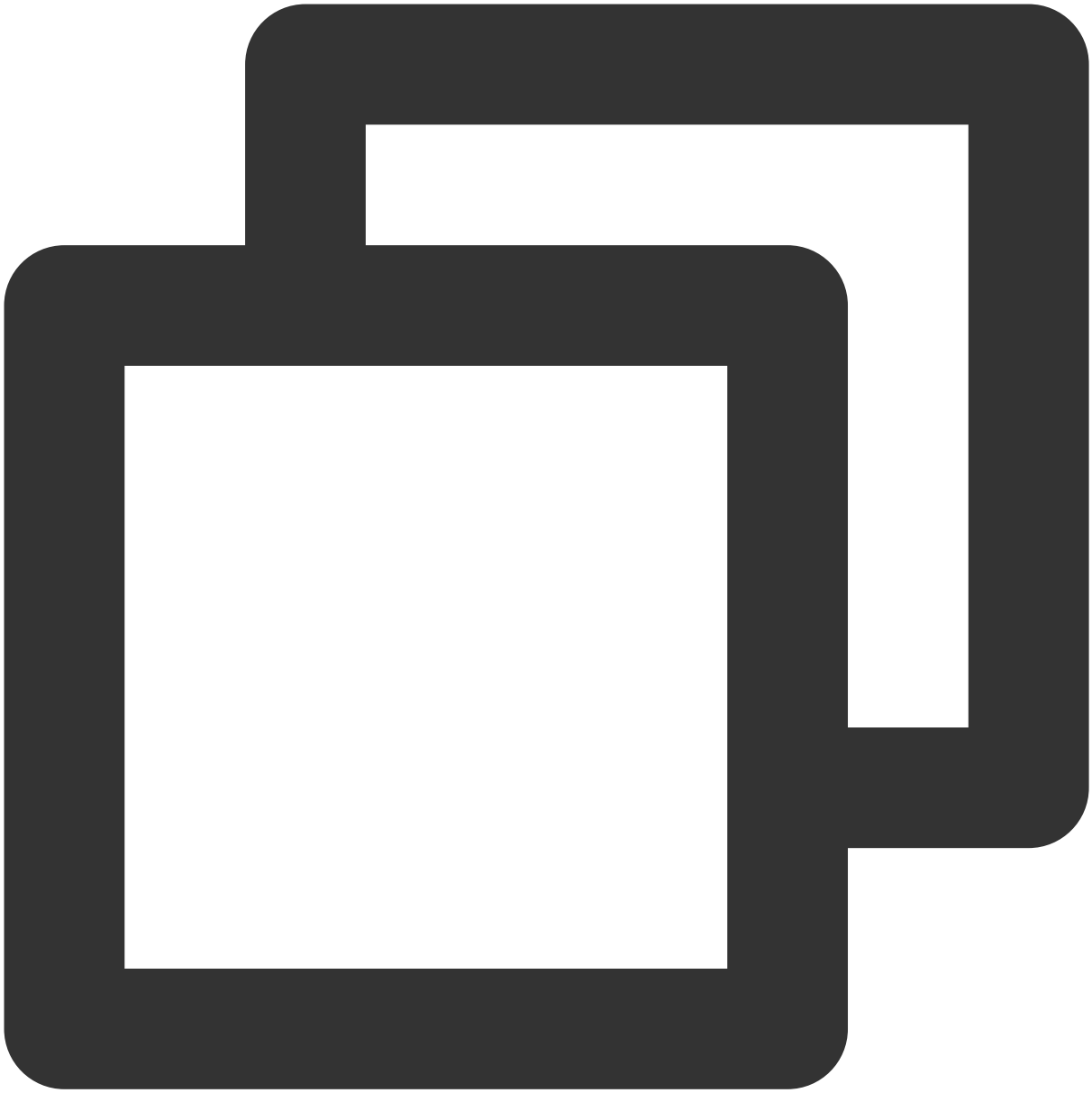
```
vim /var/www/html/test.php
```

2. **i**キーを押して編集モードに切り替え、次のように書き込みます。



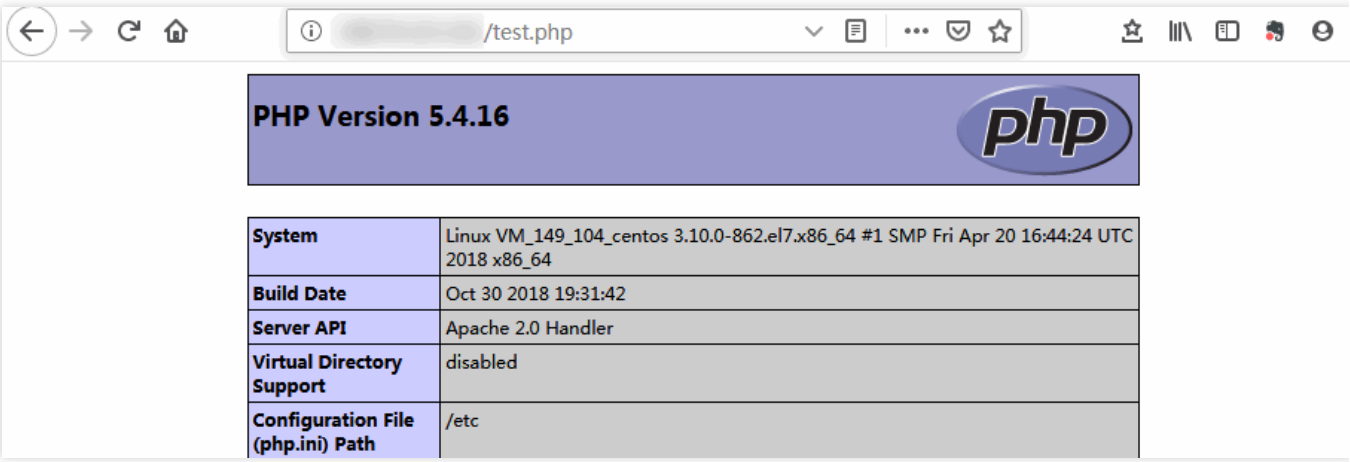
```
<?php
echo "<title>Test Page</title>";
phpinfo()
?>
```

3. **Esc**を押し、**:wq**を入力して、ファイルを保存して戻ります。
4. ブラウザで、 `test.php` ファイルにアクセスして、環境設定が成功したかどうかを確認します。



```
http://CVMのパブリックIP/test.php
```

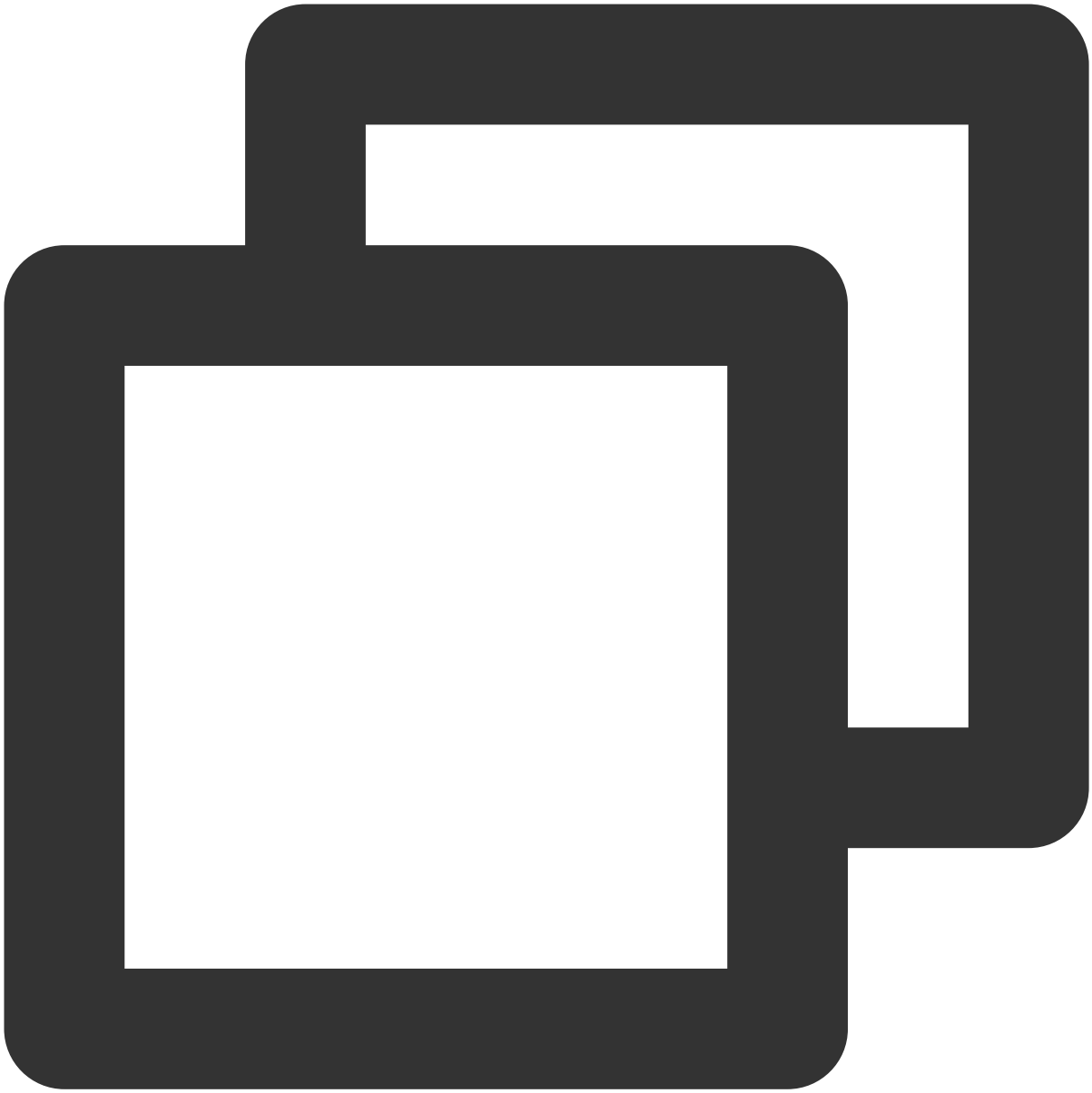
次の画面が表示されたら、LAMP環境が正常に設定されていることを示しています。



手順3：Discuz!のインストールと設定

Discuz!をダウンロードする

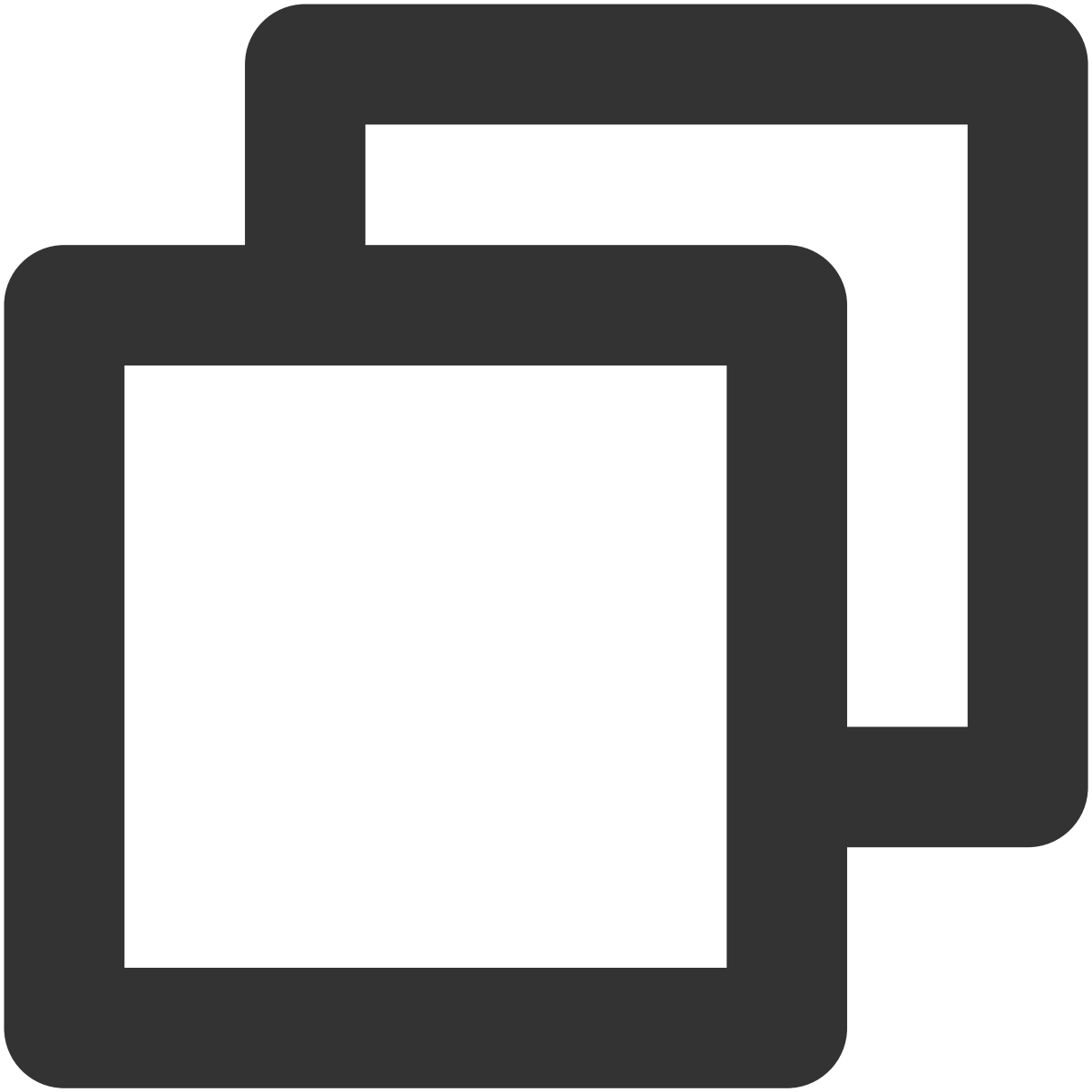
次のコマンドを実行して、インストールパッケージをダウンロードします。



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

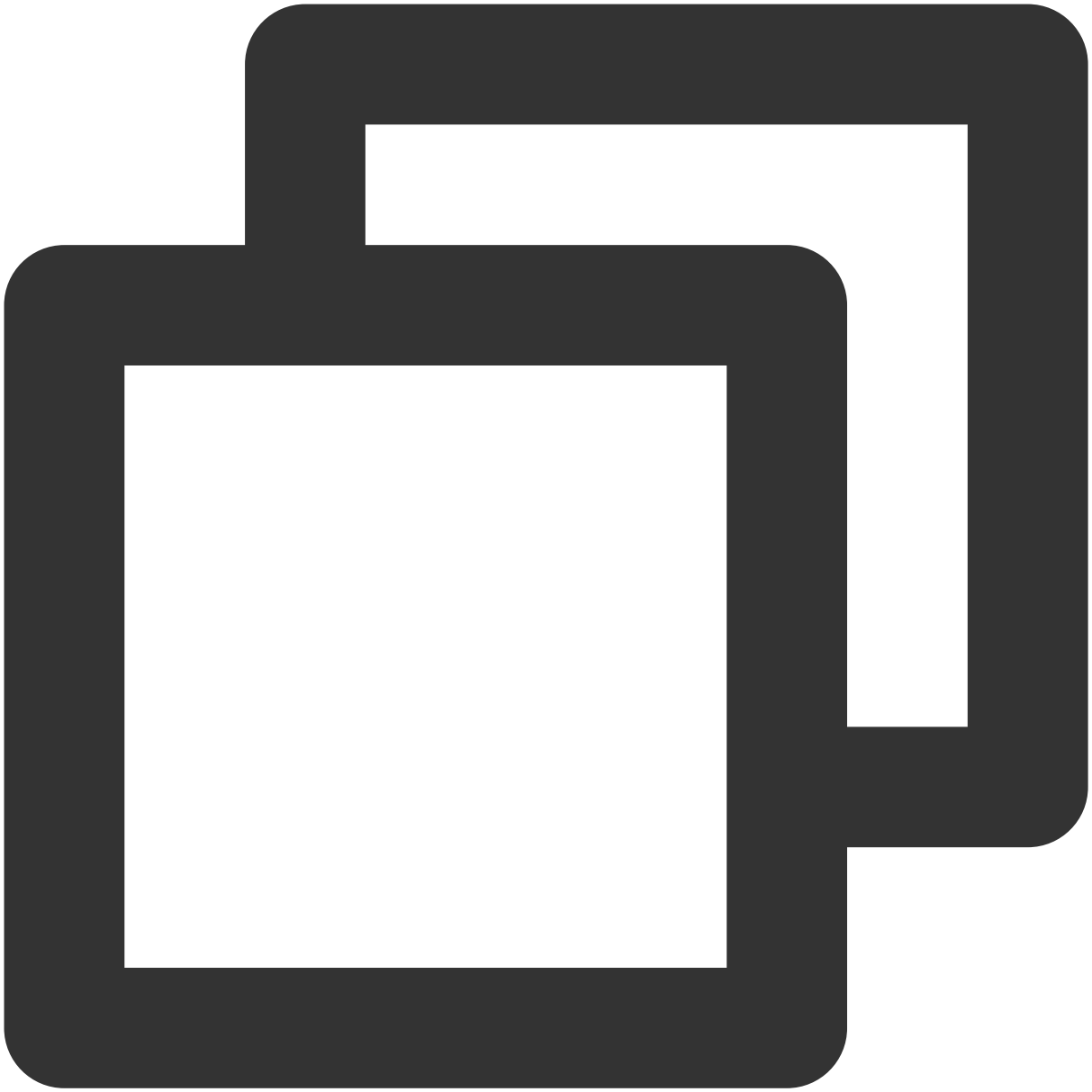
インストールの準備作業

1. 次のコマンドを実行して、ダウンロードしたインストールディレクトリに入ります。



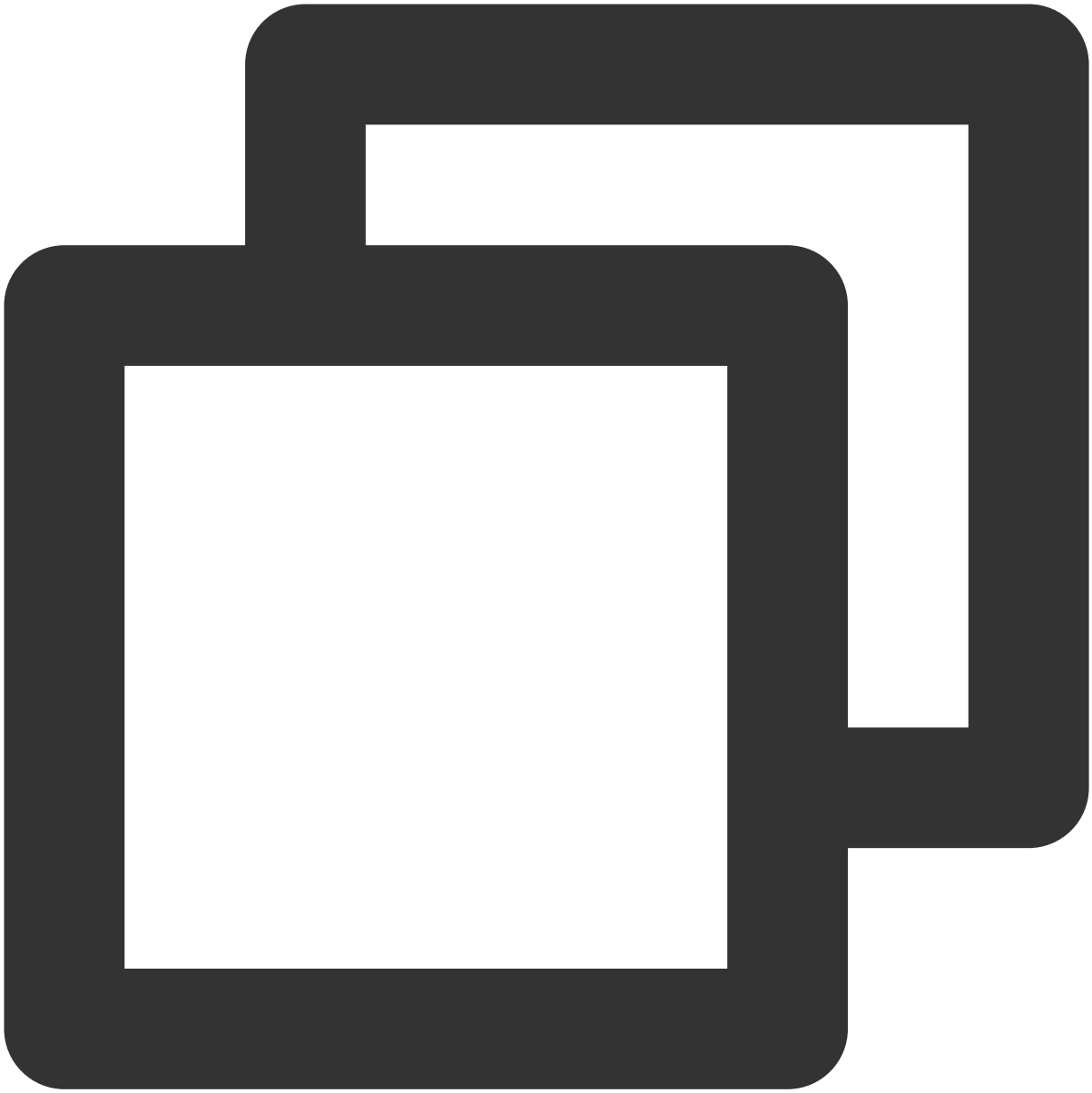
```
cd DiscuzX
```

2. 次のコマンドを実行して、「upload」フォルダ内のすべてのファイルを `/var/www/html/` にコピーします。



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

3. 次のコマンドを実行して、他のユーザーに書き込み権限を割り当てます。



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

Discuz!をインストールする

1. Webブラウザのアドレスバーに、Discuz!サイトのIPアドレス（CVMインスタンスのパブリックIPアドレス）、または関連操作 で取得した利用可能なドメイン名を入力すると、Discuz!インストールインターフェースが表示されます。

説明：

本ドキュメントでは、インストール手順のみ示しています。低いバージョンであるというセキュリティアラートが表示された場合、より高いバージョンのイメージを使用することを推奨します。
2. **同意する**をクリックして、インストール環境の確認ページに進みます。
3. 現在のステータスが正常であることを確認して、 **次のステップ**をクリックし、実行環境の設定ページに進みます。
4. クリーンインストールを選択して、**次のステップ**をクリックし、データベースの作成ページに進みます。
5. 画面上の指示に従って、情報を記入し、Discuz!のデータベースを作成します。
ご注意：
必要なソフトウェアのインストール で設定したrootアカウントとパスワードを利用してデータベースに接続し、システムメールボックス、管理者アカウント、パスワード、およびEmailを設定してください。
管理者ユーザーとパスワードを覚えておいてください。
6. **次のステップ**をクリックしてインストールを開始します。
7. インストールが完了したら、**フォーラムのインストールが完了しました。ここをクリックしてアクセスしてください**をクリックすれば、フォーラムにアクセスできます。

関連操作

自分のDiscuz!フォーラム個別のドメイン名を設定できます。ユーザーは複雑なIPアドレスを使用せずに、覚えやすいドメイン名でWebサイトにアクセスできます。一部のユーザーは学習目的でのみのフォーラムの構築に、IPを使って直接インストールして臨時に使用する場合がありますが、このような操作はお勧めしません。

よくあるご質問

CVMの使用中に問題が発生した場合は、下記のドキュメントを参照しながら実際状況に合わせ分析した上で問題を解決することが可能です。
CVMのログインに関する問題は、パスワードとキー、ログインとリモート接続 ドキュメントをご参照ください。
CVMのネットワークに関する問題は、 IPアドレス、ポートとセキュリティグループドキュメントをご参照ください。
CVMのハードディスクに関する事項については、システムディスクとデータディスクをご参照ください。

Ghostブログの手動構築

最終更新日：：2021-11-01 15:45:25

操作シナリオ

GhostはNode.js言語を使用して作成するオープンソースブログプラットフォームです。 Ghostを使用すると、すぐにブログを立ち上げることができ、 オンラインパブリッシングのプロセスを簡略化できます。このドキュメントでは、Tencent CloudのCloud Virtual Machine（CVM）上で、Ghost個人ウェブサイトを手動で構築する方法についてご紹介します。
Ghostウェブサイトを構築するには、Lunux OSおよびコマンドに精通している必要があります。例えば、Ubuntu環境下でのApt-getによるソフトウェアインストール 等の常用コマンドです。

ソフトウェアバージョンの例

ここでGhostブログの作成に使用するOSおよびソフトウェアのバージョンと説明は次のとおりです。
OS：ここではUbuntu 20.04を例として説明します。
Nginx：Webサーバー。ここではNginx 1.18.0を例として説明します。
MySQL：データベース。ここではMySQL 8.0.25を例として説明します。
Node.js：実行環境。ここではNode.js 14.17.0バージョンを例として説明します。
Ghost：オープンソースブログプラットフォーム。ここではGhost 4.6.4バージョンを例として説明します。

前提条件

Linux CVMを購入済みであること。CVMを購入していない場合は、Linux CVMのカスタマイズ設定 をご参照ください。
Ghostブログ設定の過程では、ICP登録が完了し、かつ使用するCVMへの解決が完了しているドメイン名を使用する必要があります。

操作手順

ステップ1：Linuxインスタンスにログインする

標準方式を使用してLinuxインスタンスにログイン（推奨）します。実際の操作方法に応じて、他のログイン方法を選択することもできます。

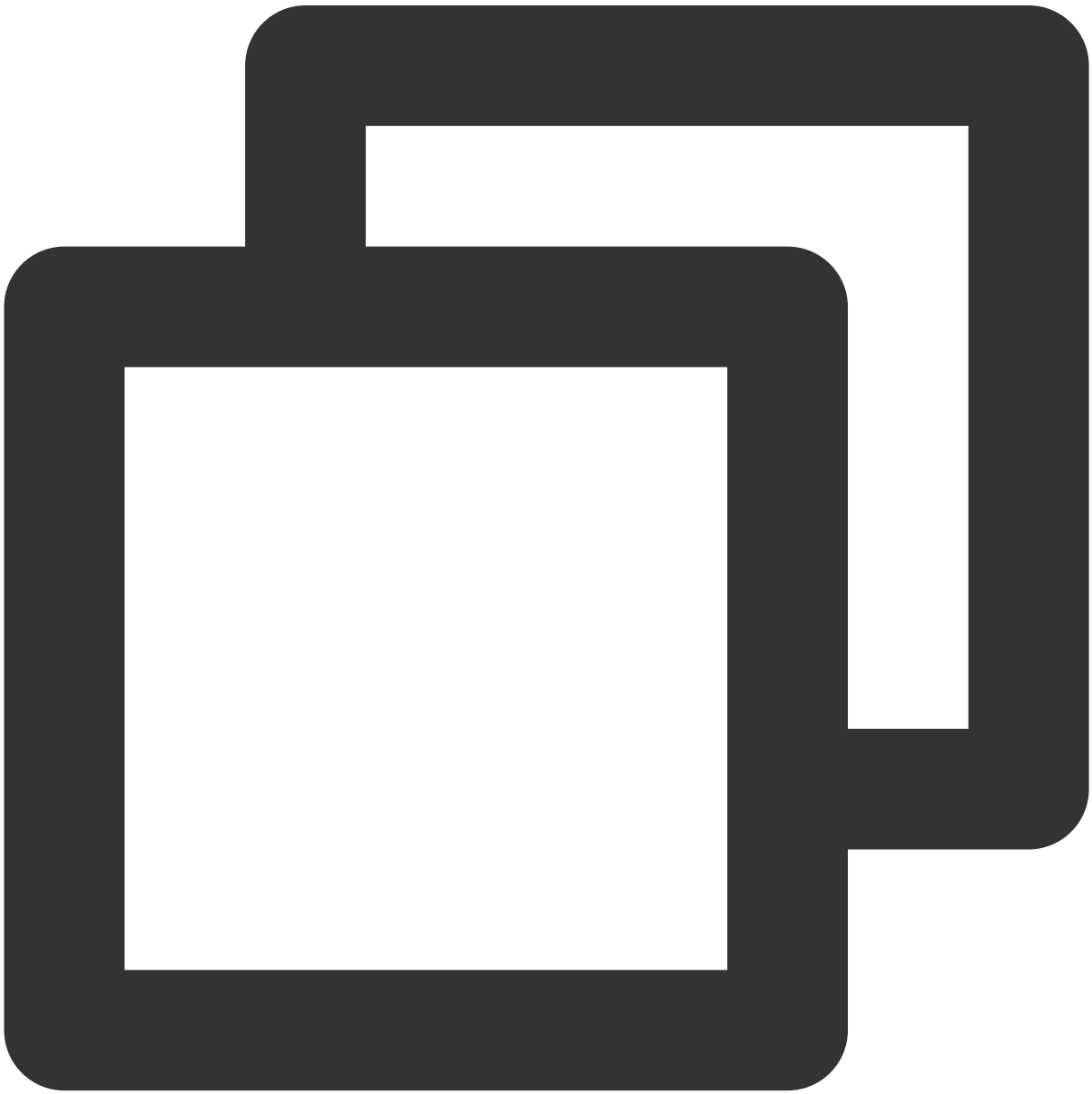
リモートログインソフトウェアを使用してLinuxインスタンスにログインする
SSHを使用してLinuxインスタンスにログイン

手順2：新規ユーザーの作成

1. Ubuntu OSのCVMにログインした後、Ubuntuシステムでrootユーザーを使用してログイン を参照して、rootユーザーに切り替えてください。
2. 以下のコマンドを実行し、新規ユーザーを作成します。ここでは `user` を例とします。

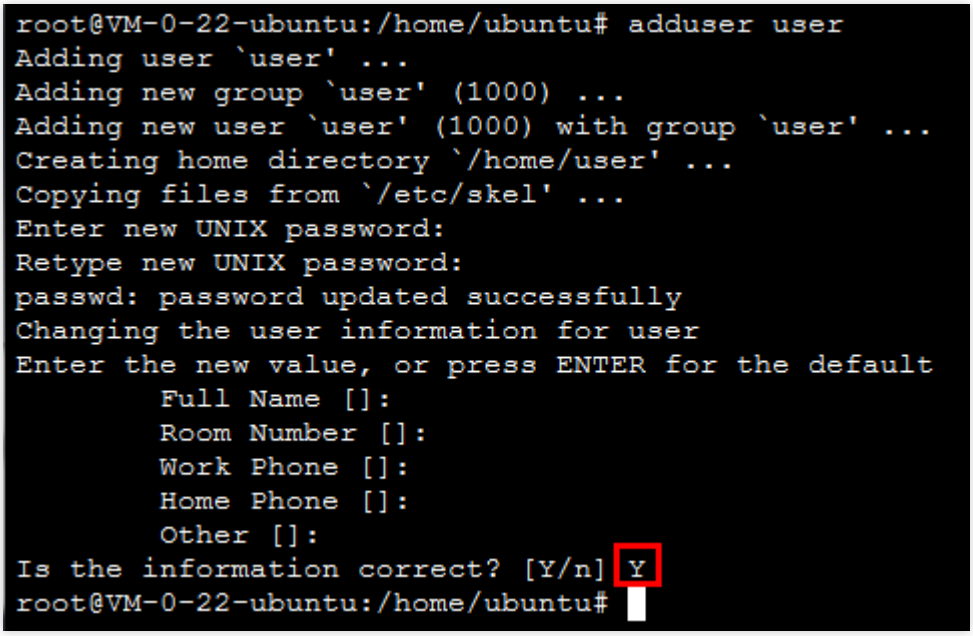
ご注意：

Ghost-CLIとの競合が発生する場合がありますので、 `ghost` をユーザー名に使用しないでください。

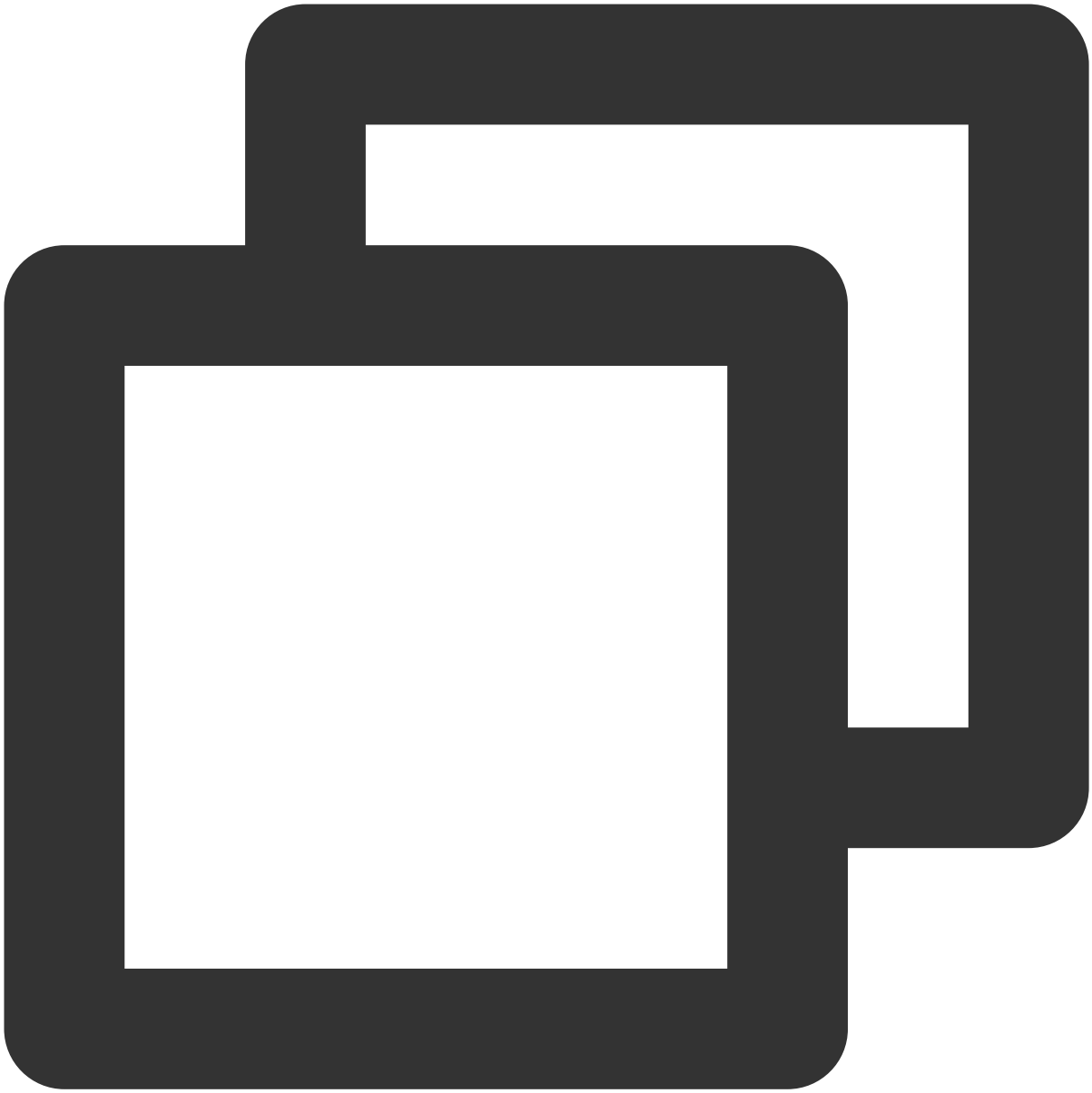


```
adduser user
```

3. 表示に従ってユーザーパスワードを入力し、確認してください。パスワードはデフォルトでは表示されません。入力し終わったら**Enter** を押し、次の手順に進んでください。
4. 実際の状況に応じてユーザー関連情報を入力します。デフォルトでは入力しなくても結構です。**Enter** を押して次の手順に進んでください。
5. **Y**を入力して情報を確認し、**Enter**を押すと設定が完了します。下図に示します。

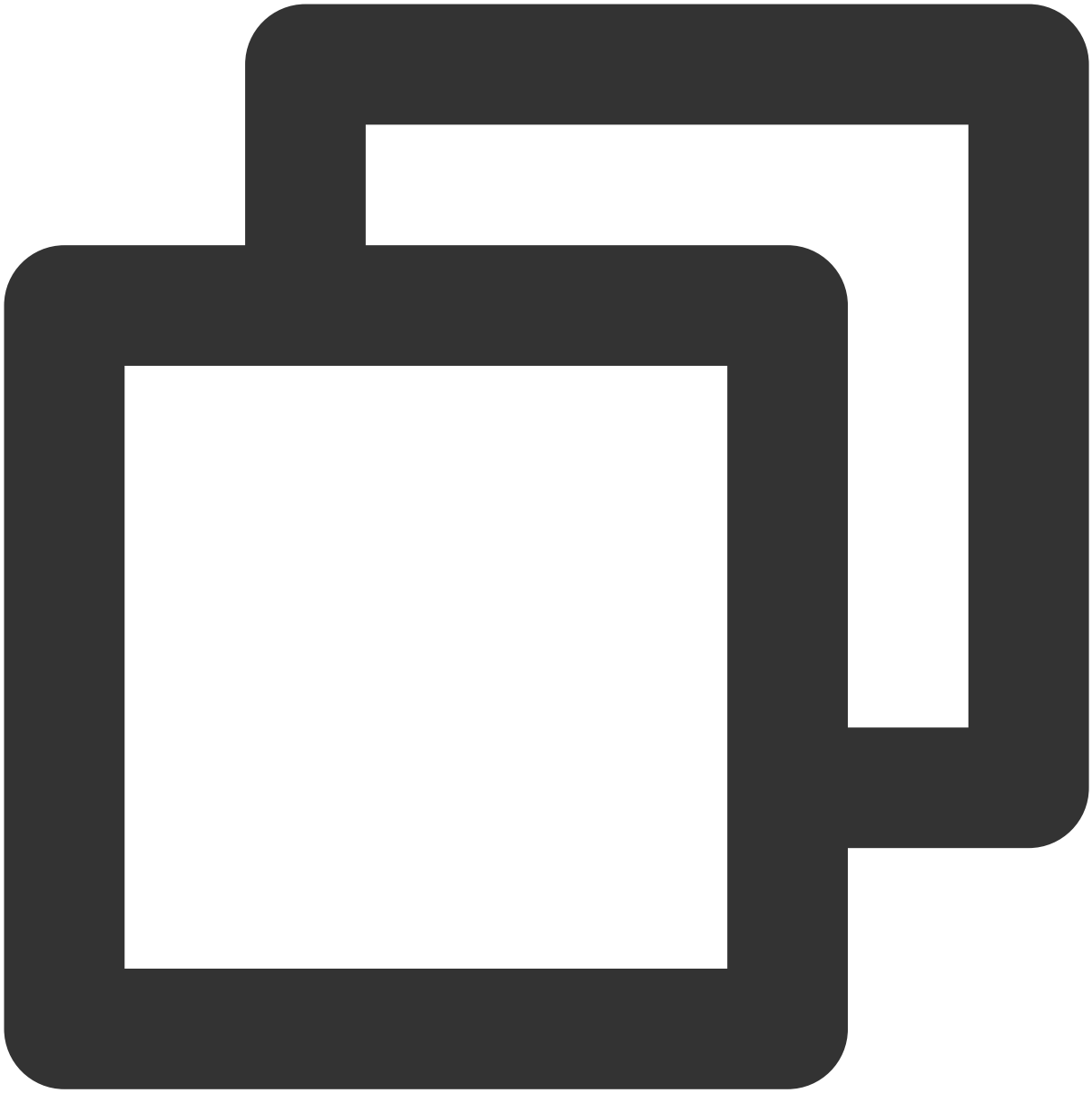


6. 以下のコマンドを実行し、ユーザー権限を追加します。



```
usermod -aG sudo user
```

7. 以下のコマンドを実行し、 `user` によるログインに切り替えます。



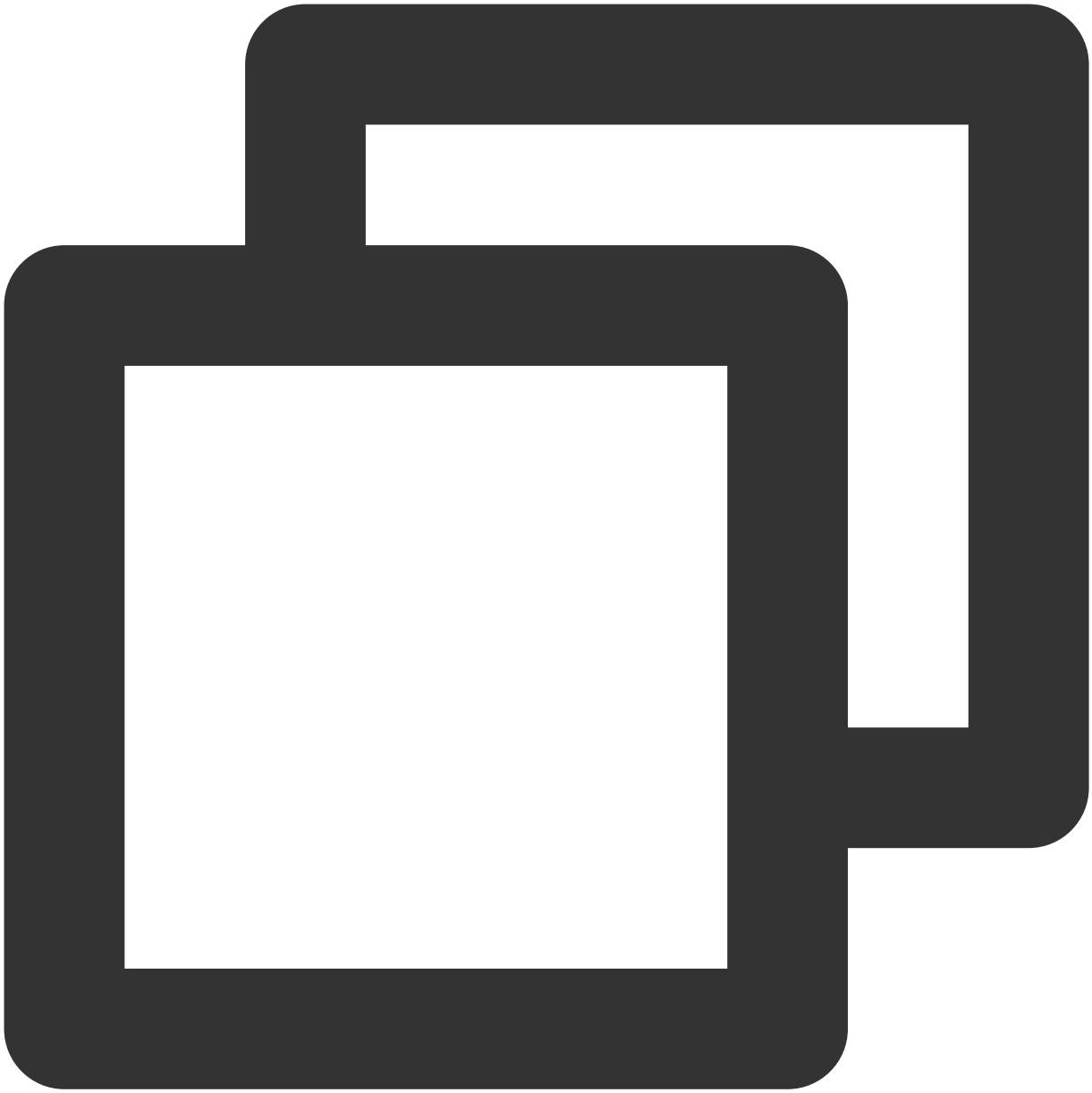
```
su - user
```

手順3：インストールパッケージの更新

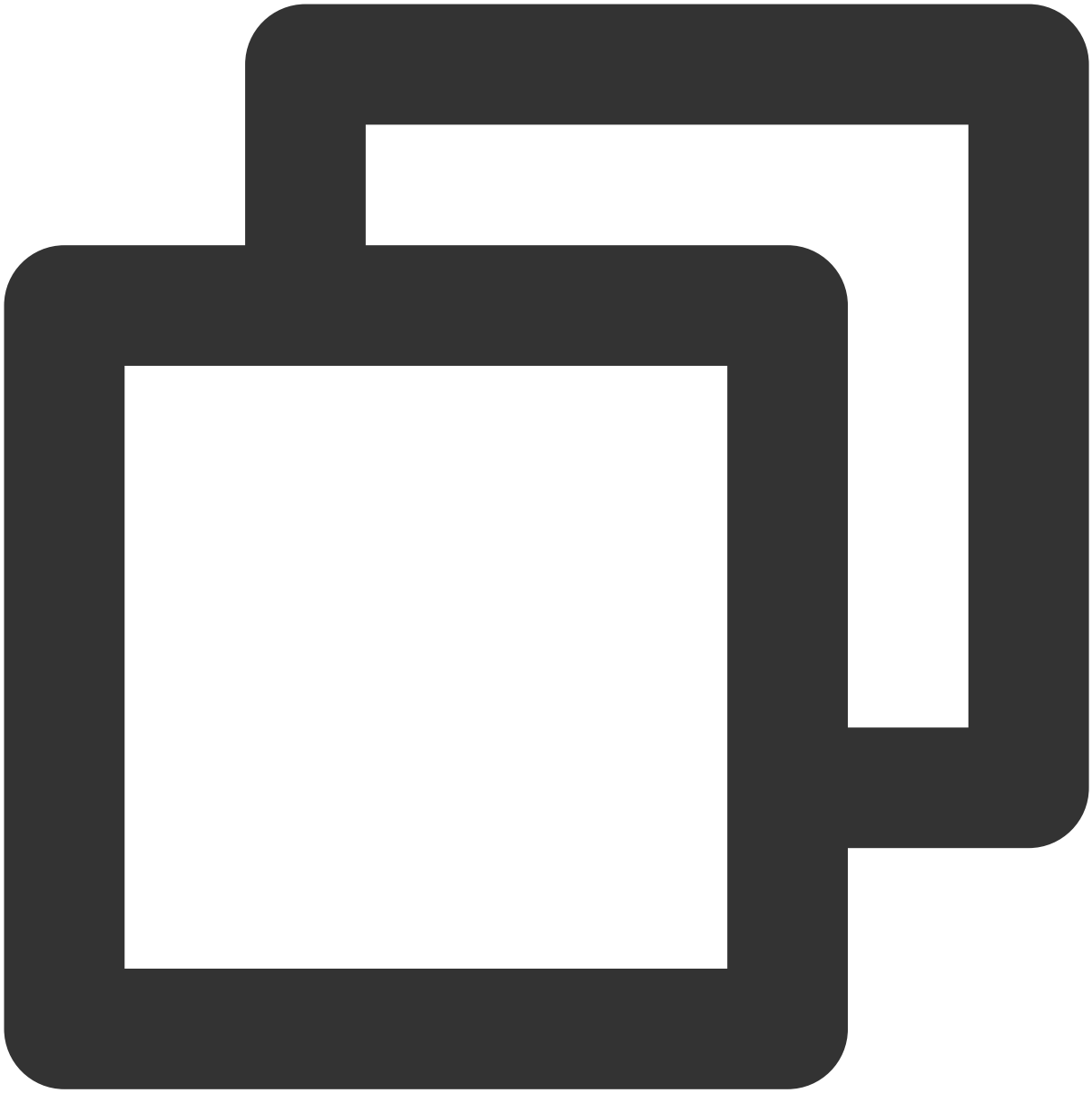
以下のコマンドを順に実行して、インストールパッケージを更新します。

説明：

画面上の表示に従って、 `user` のパスワードを入力し、**Enter** を押して更新を開始してください。



```
sudo apt-get update
```

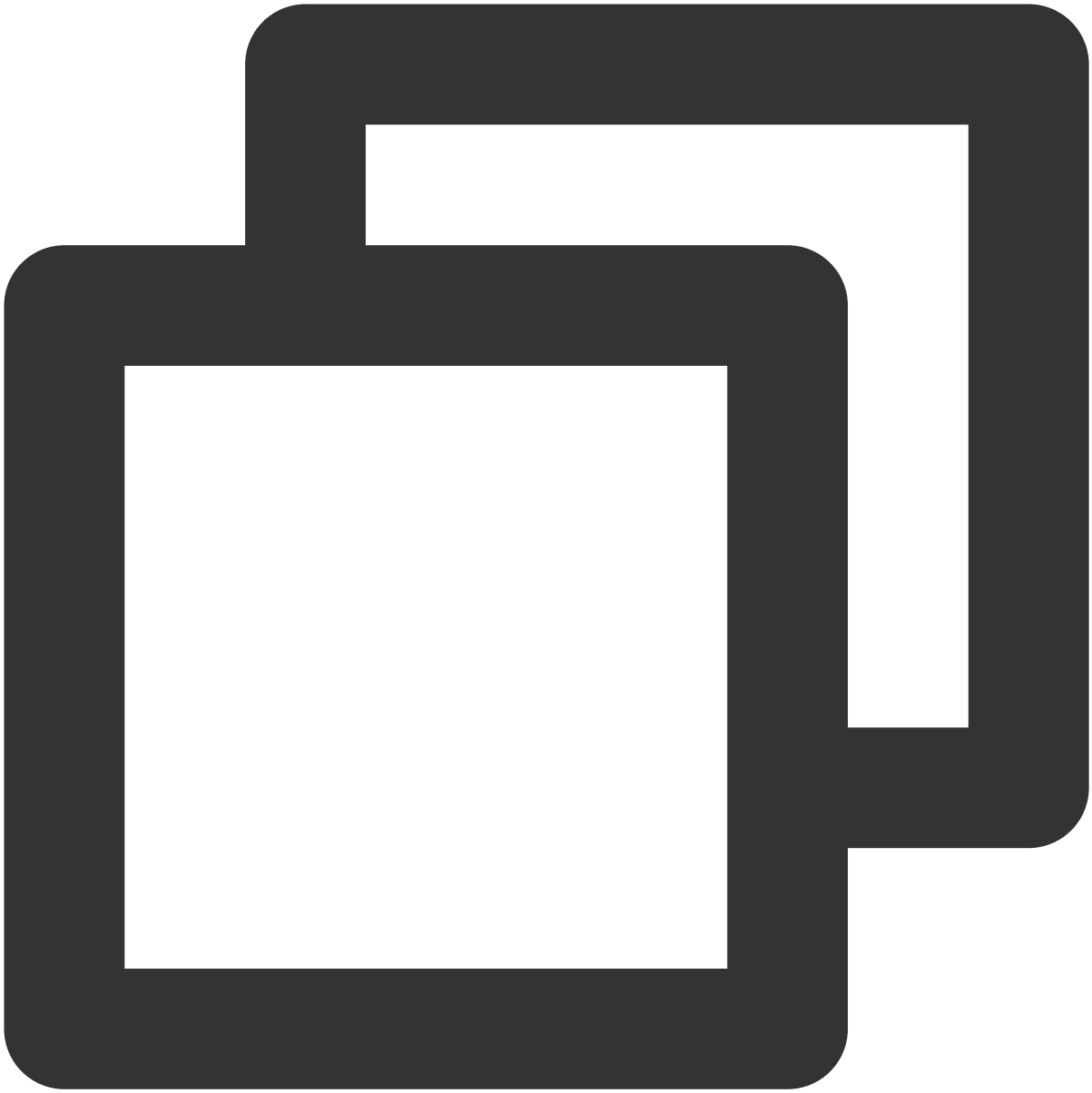


```
sudo apt-get upgrade -y
```

手順4：環境の構築

Nginxのインストールと設定

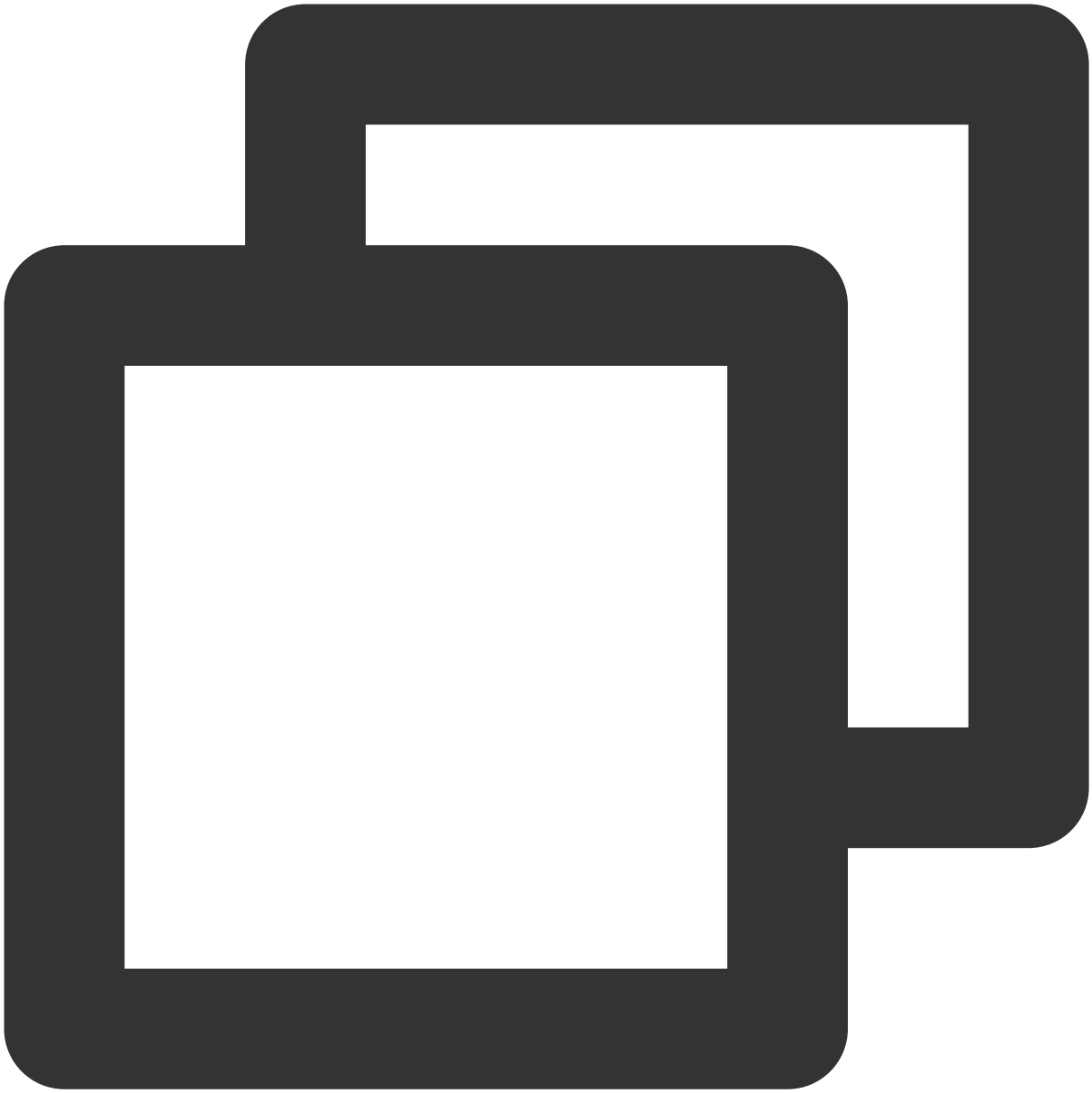
以下のコマンドを実行し、Nginxをインストールします。



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

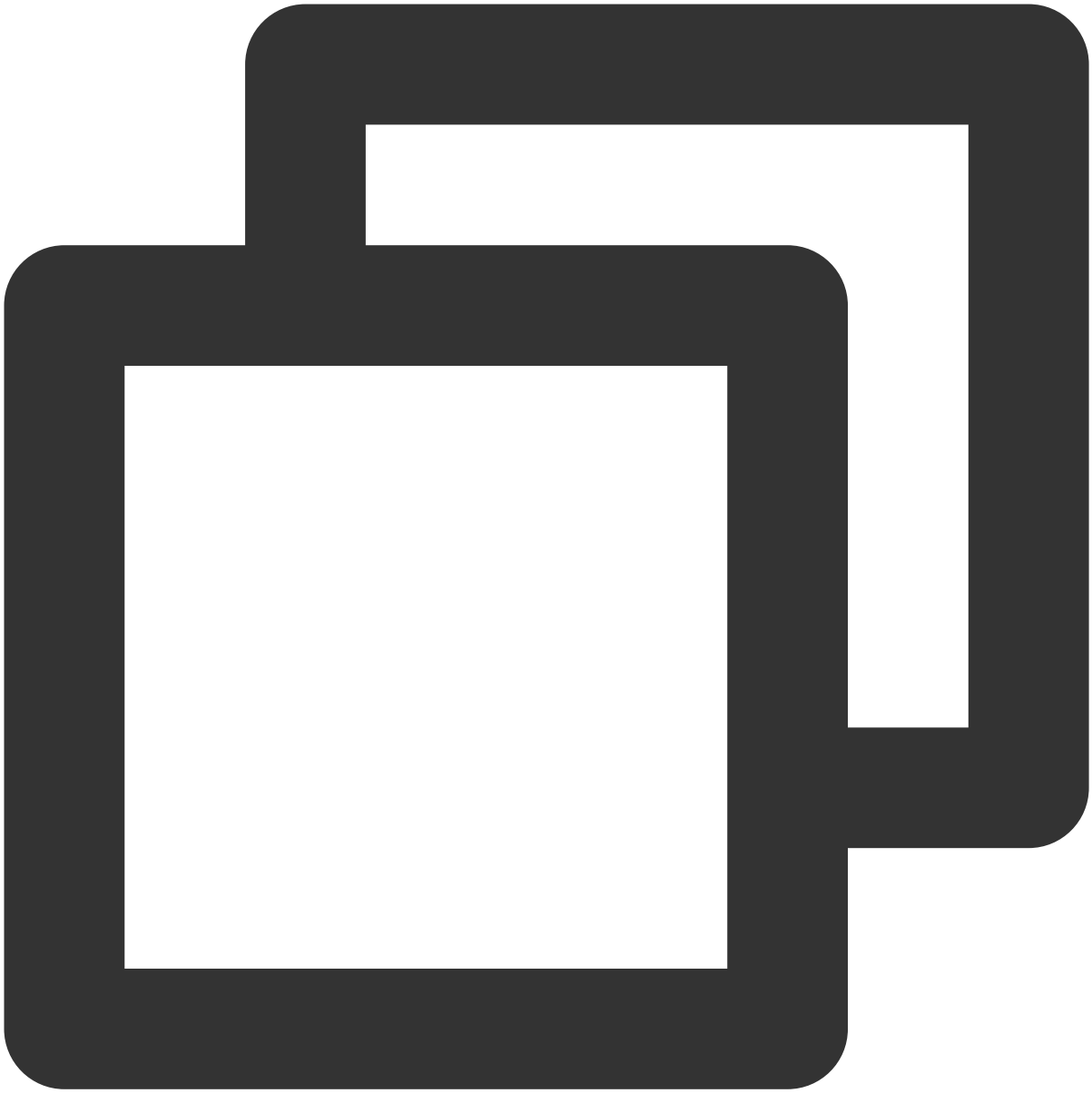
MySQLのインストールと設定

1. 以下のコマンドを実行し、MySQLをインストールします。



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

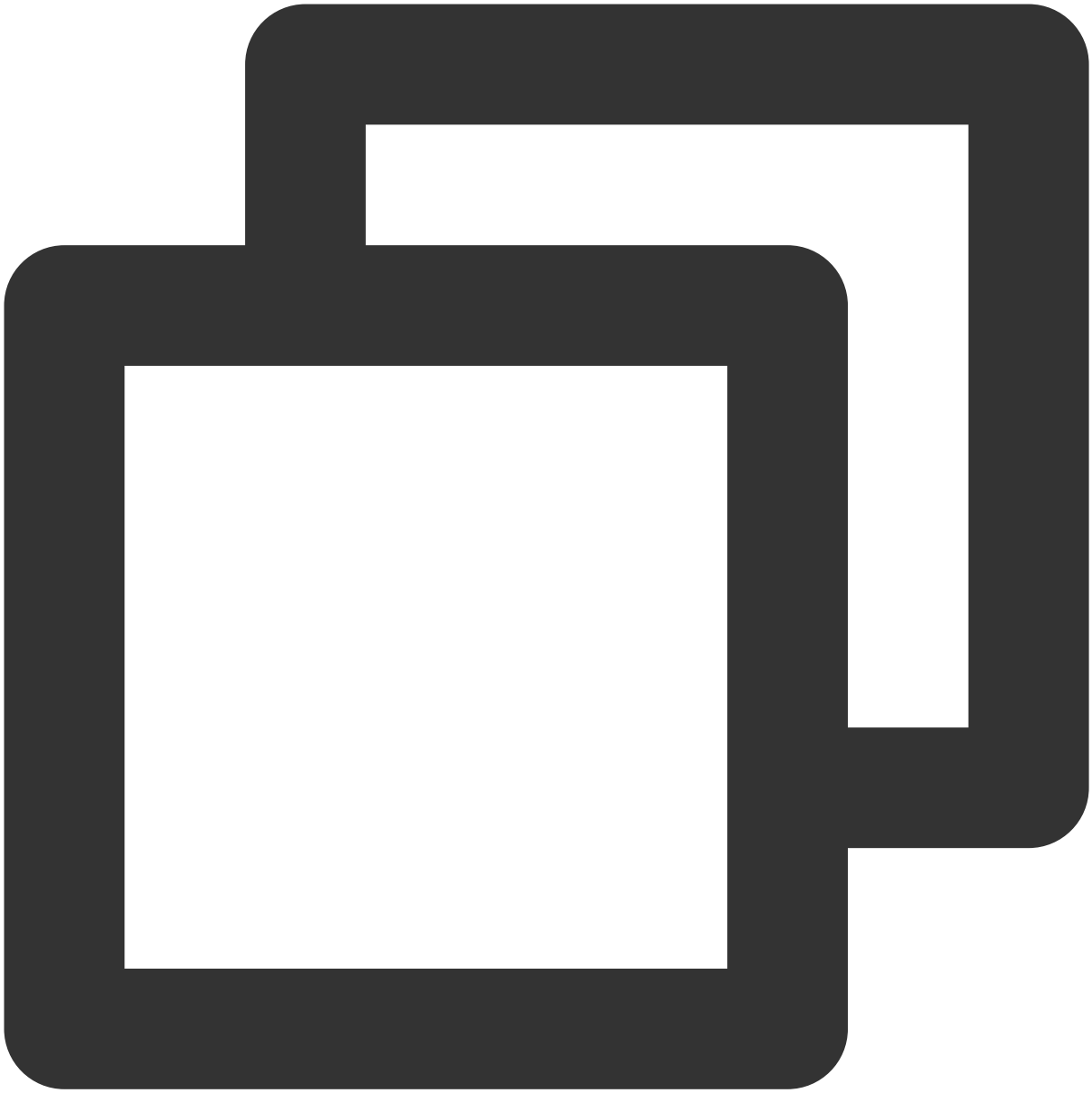
2. 以下のコマンドを実行し、MySQLに接続します。



```
sudo mysql
```

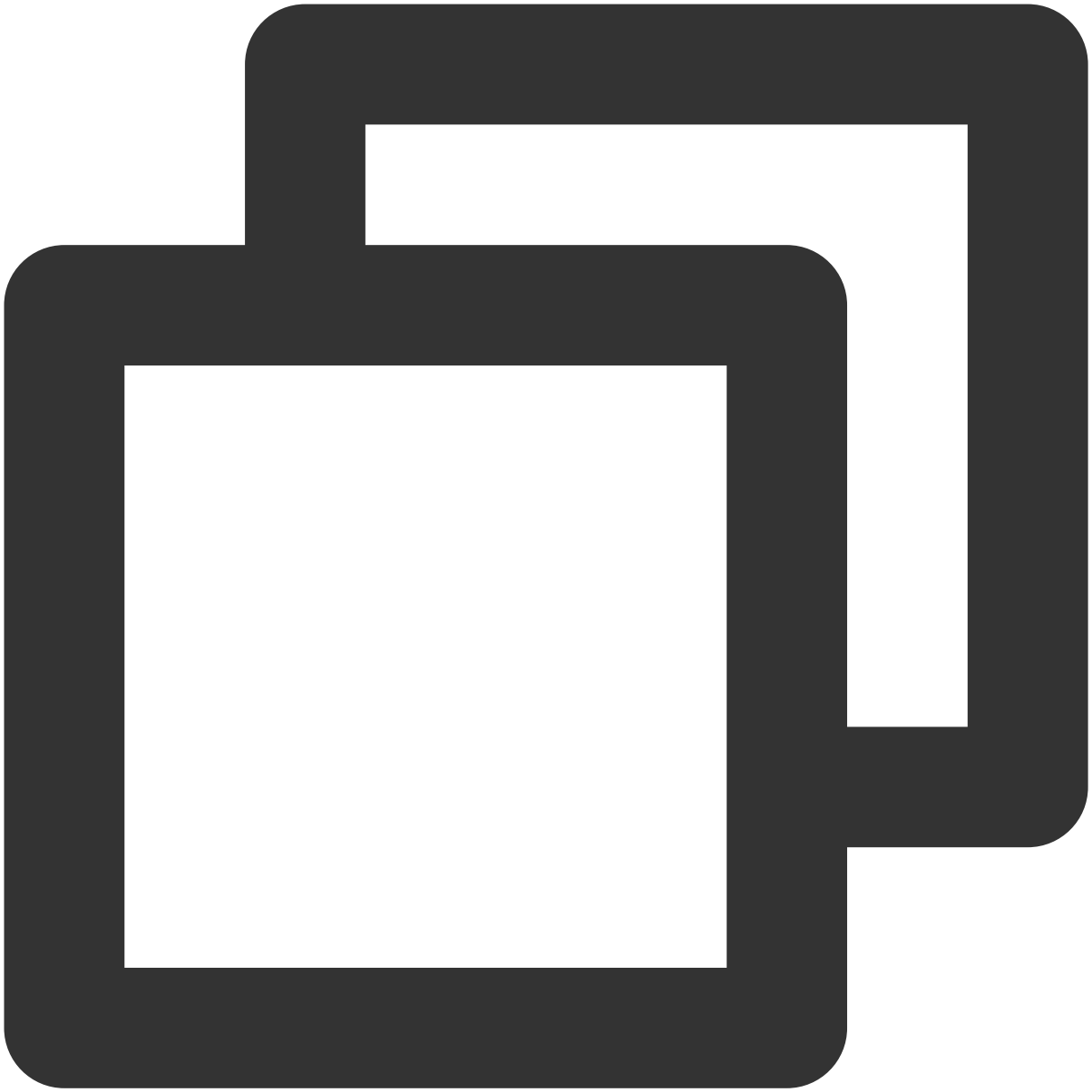
3.

以下のコマンドを実行し、Ghostで使用するデータベースを作成します。ここでは `ghost_data` を例とします。



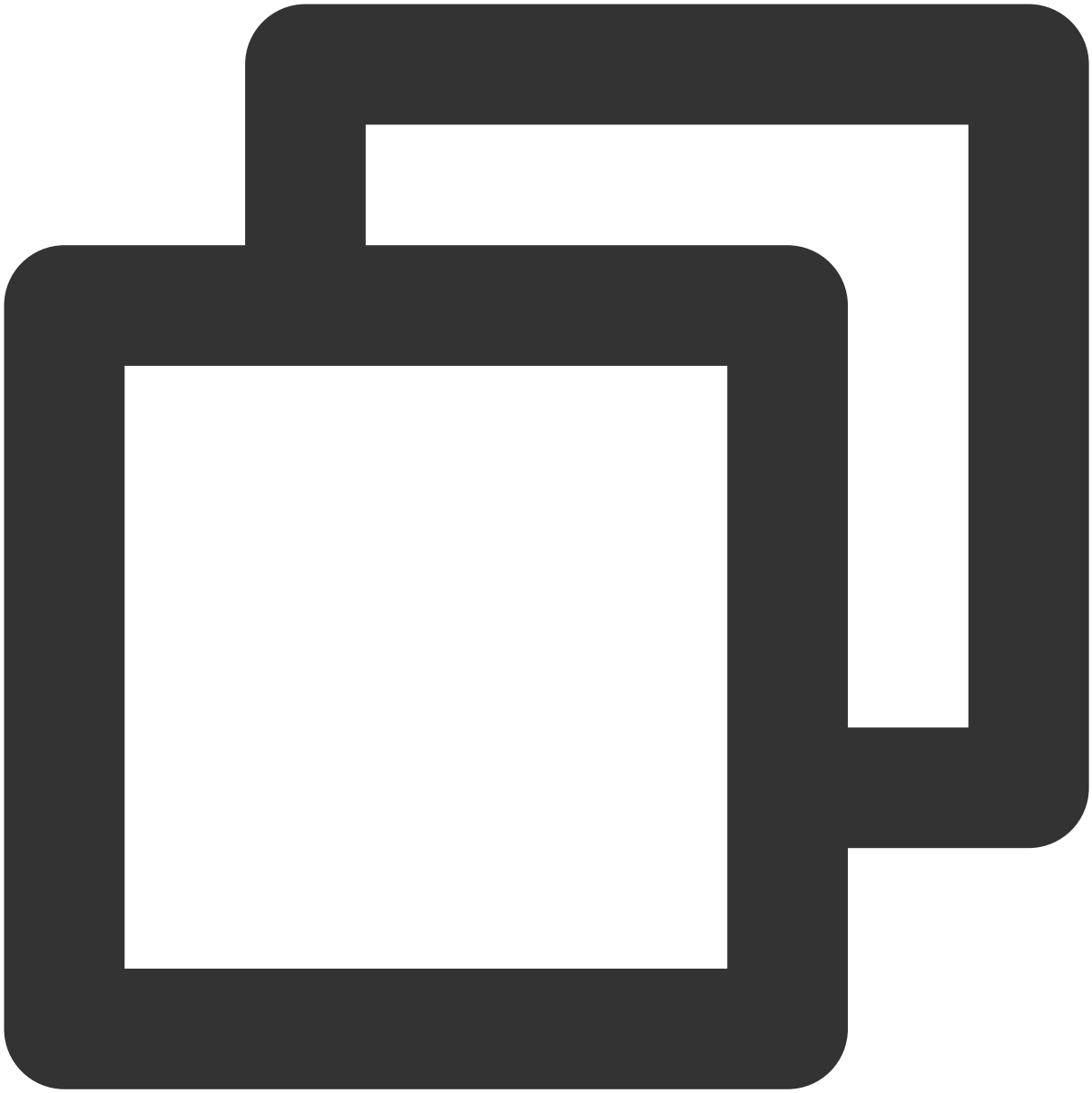
```
CREATE DATABASE ghost_data;
```

4.
以下のコマンドを実行し、rootアカウントのパスワードを設定します。



```
ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'rootアカウン
```

5. 以下のコマンドを実行し、MySQLを終了します。



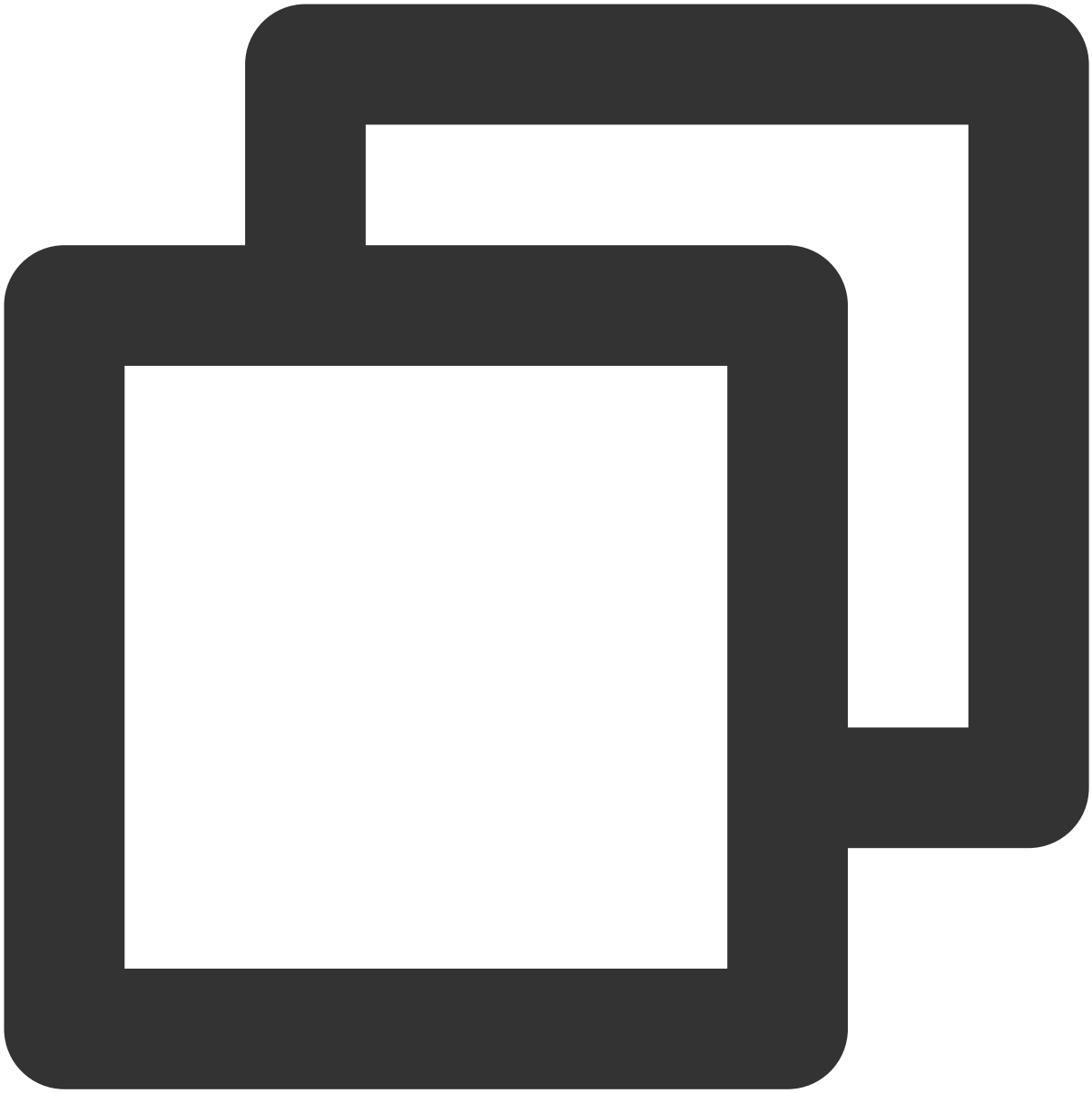
```
\\q
```

Node.jsのインストールと設定

1. 以下のコマンドを実行し、 Node.jsのサポートするインストールバージョンを追加します。

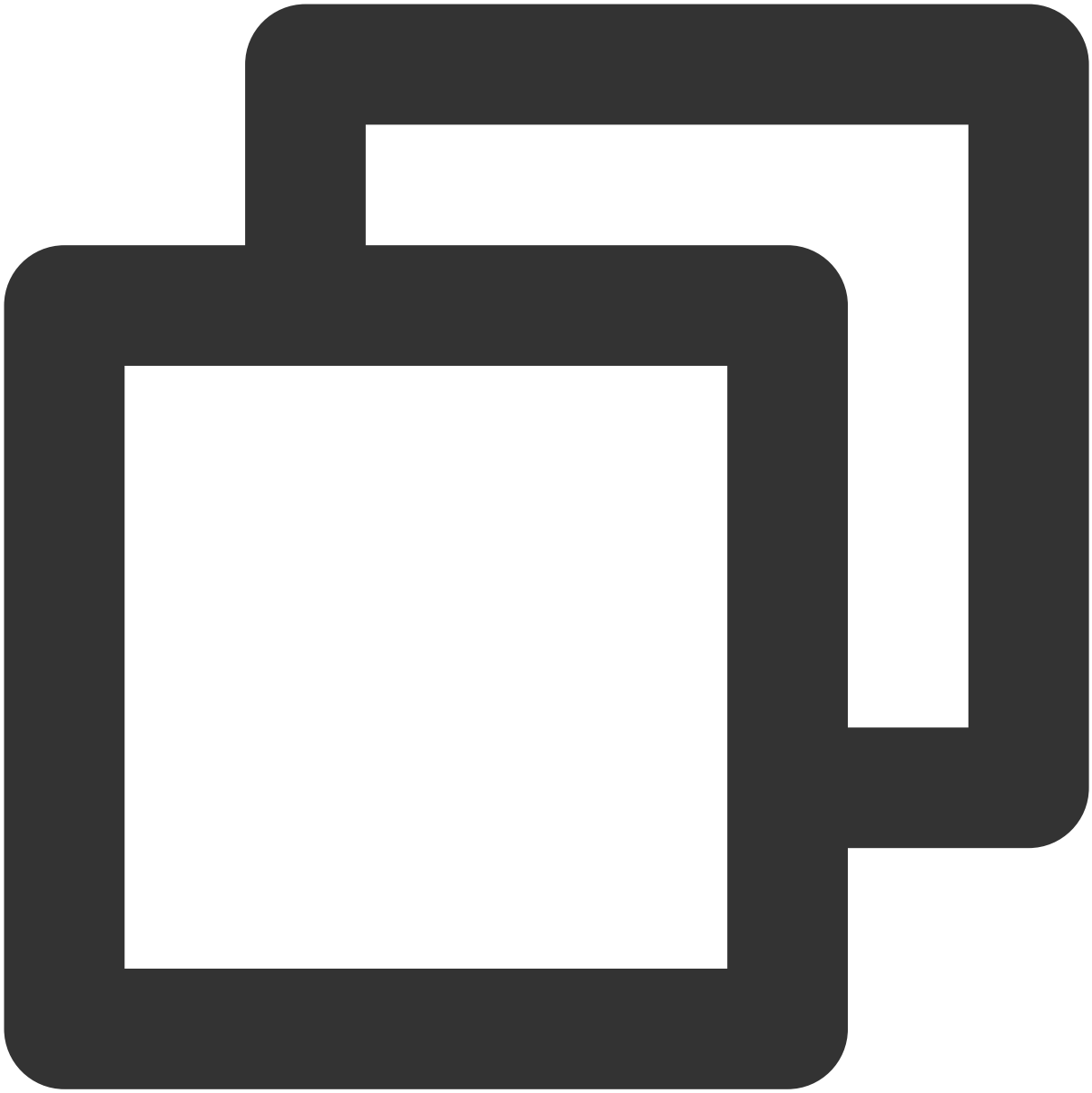
説明：

Ghostのバージョンによって、必要なNode.jsのバージョンが異なります。upported Node versions および以下のコマンドを参照し、対応するコマンドを実行してください。



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

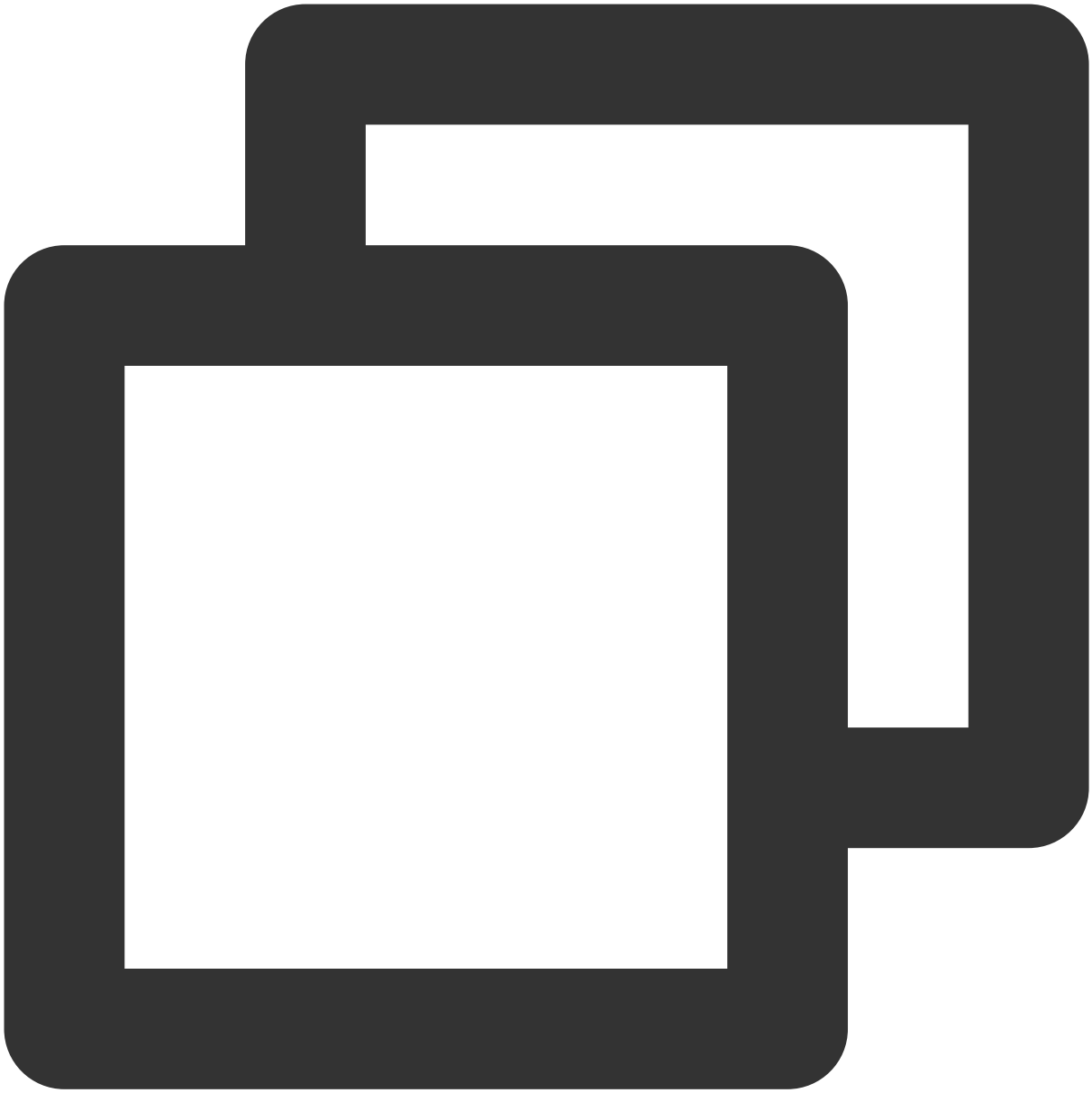
2. 以下のコマンドを実行し、Node.jsをインストールします。



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

Ghost-CLIのインストール

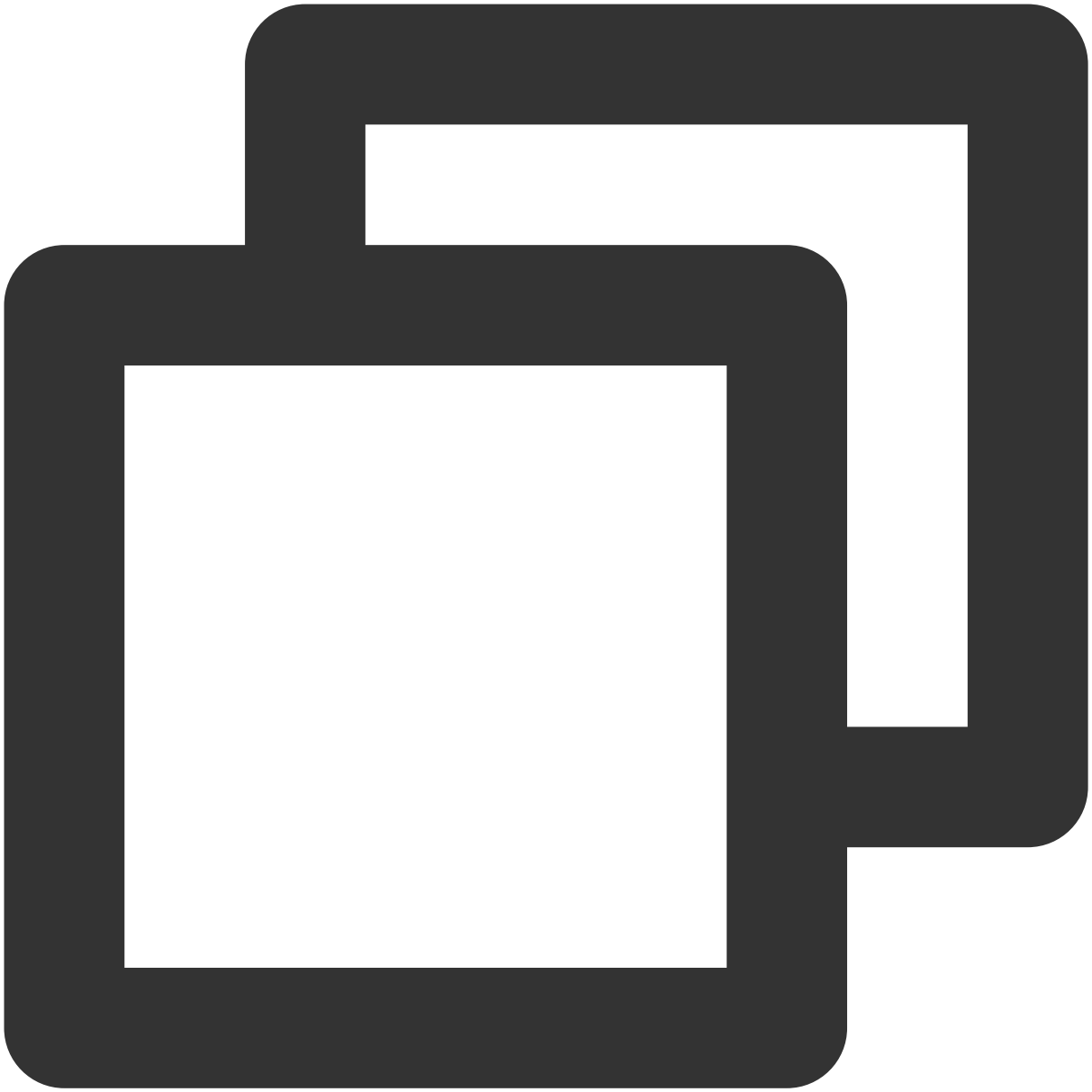
以下のコマンドを実行し、Ghostコマンドラインツールをインストールすると、Ghostのクイック設定を行うことができます。



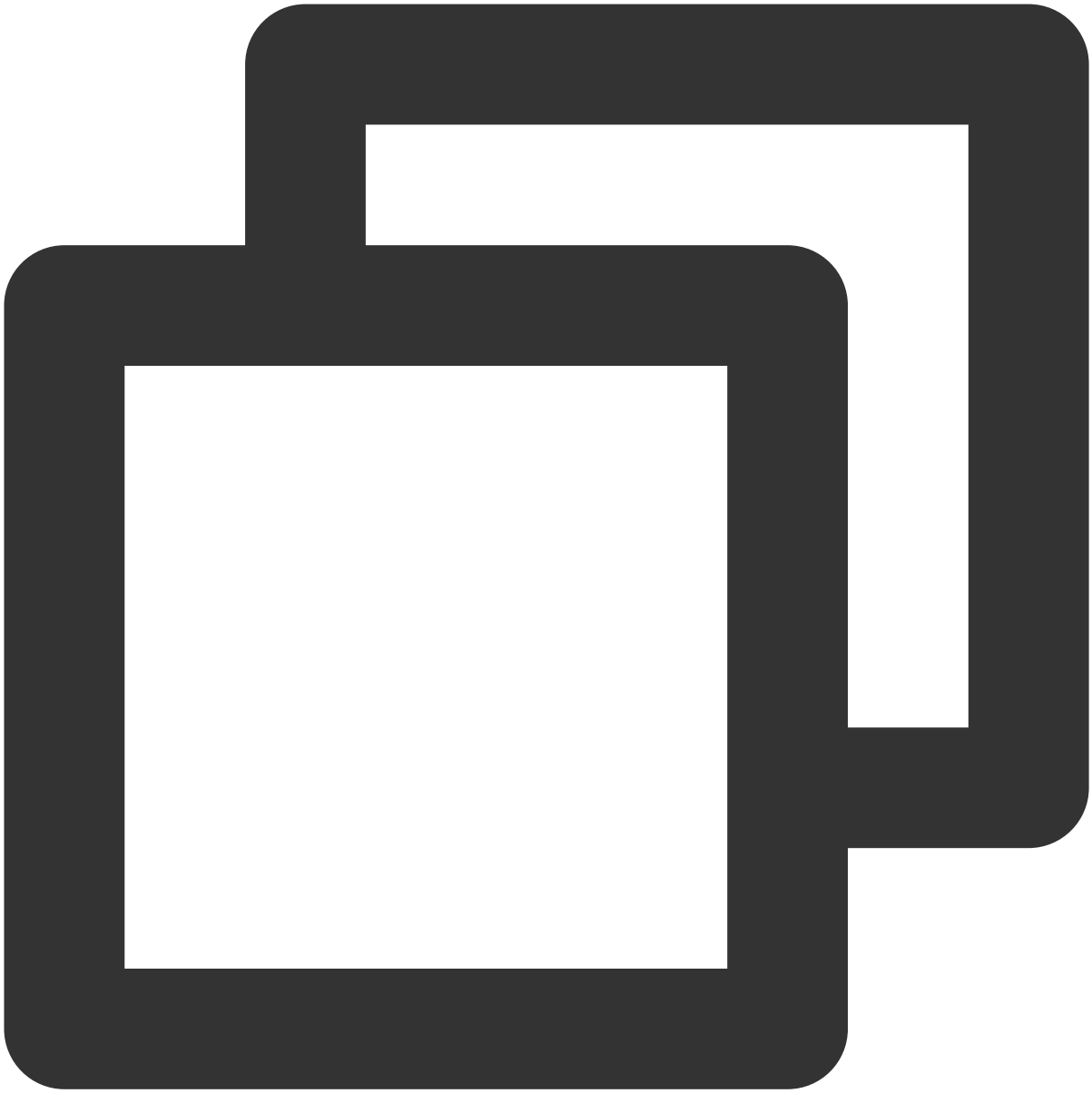
```
sudo npm install ghost-cli@latest -g
```

手順5：Ghostのインストールと設定

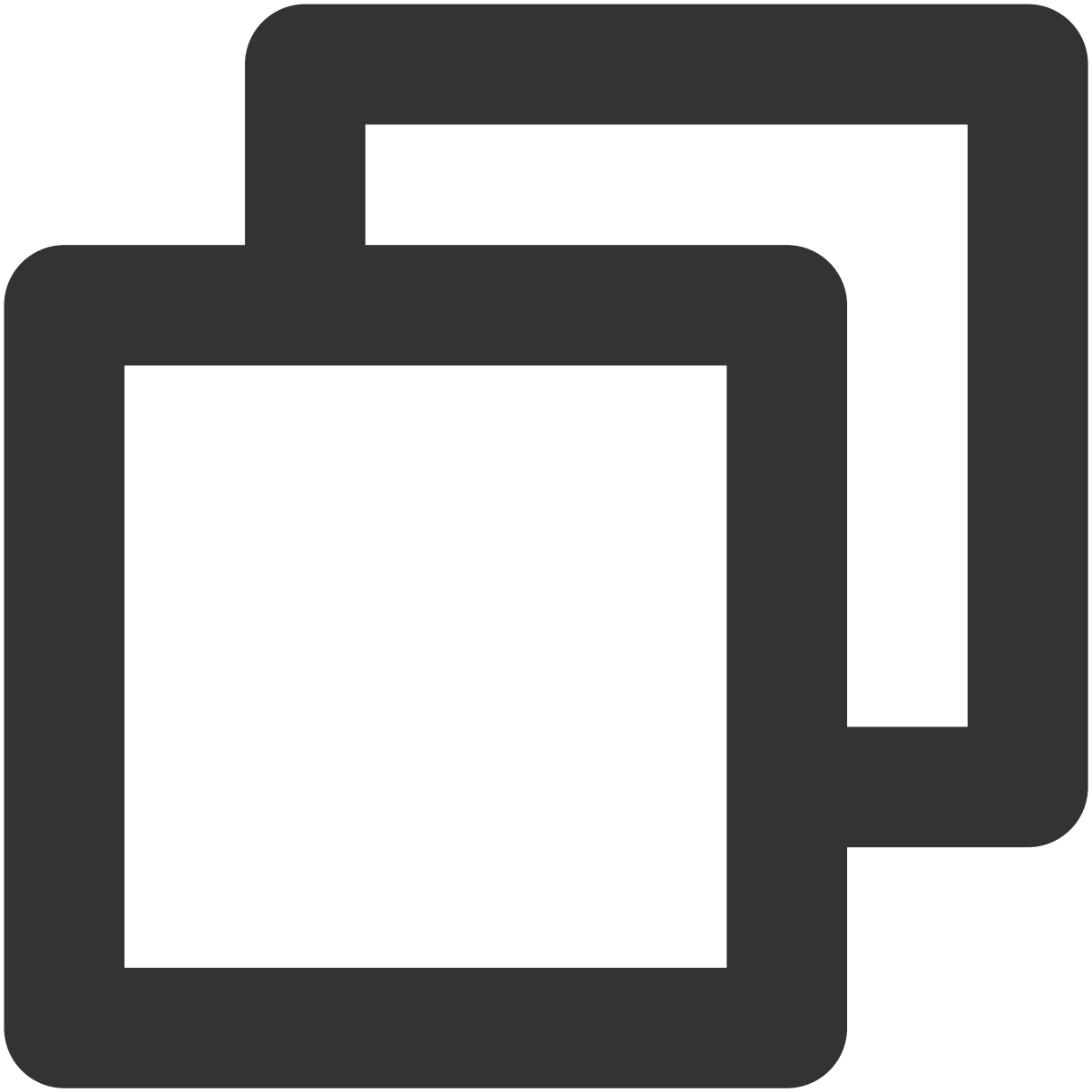
1. 次のコマンドを順に実行し、設定してGhostインストールディレクトリに進みます。



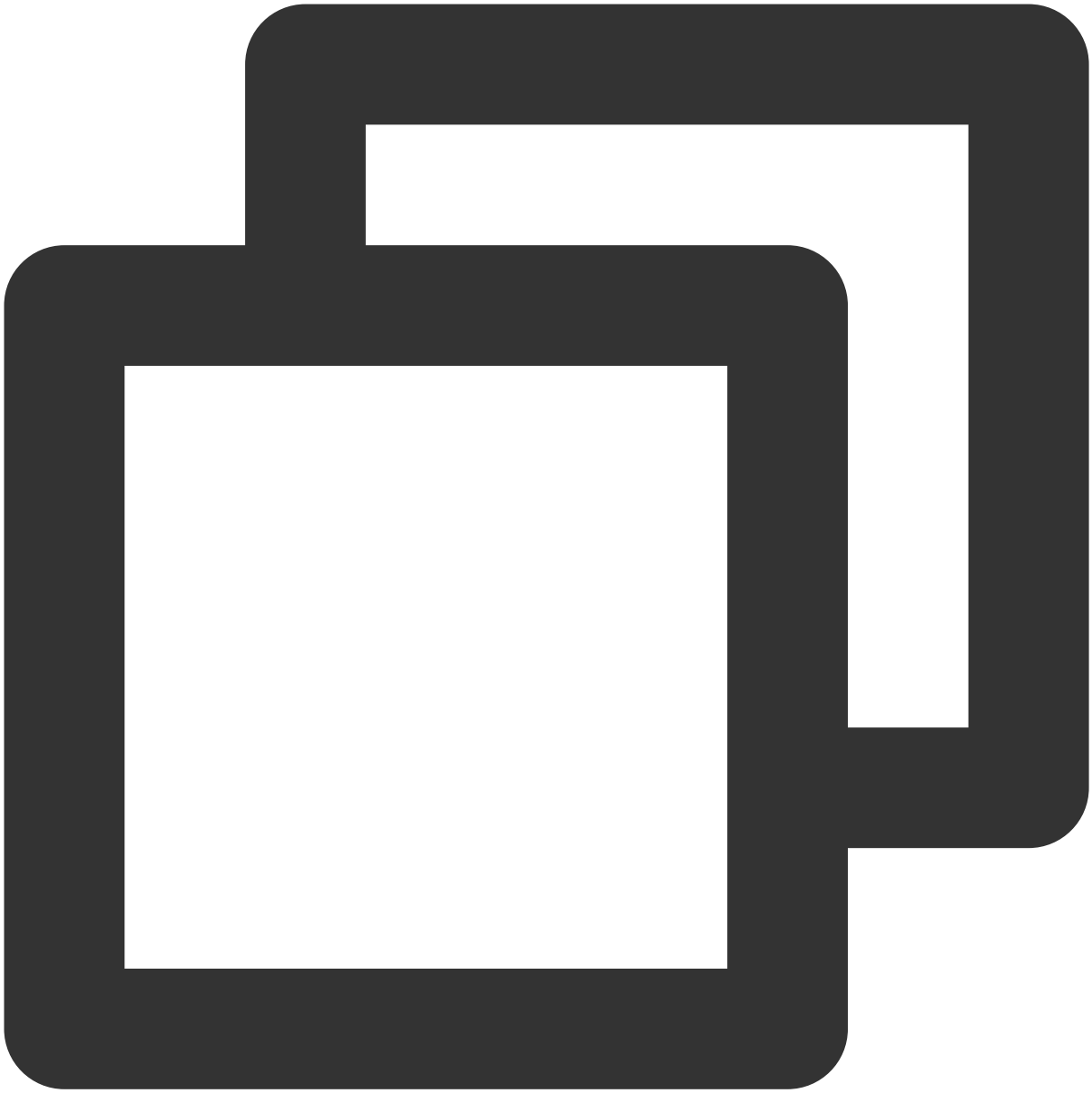
```
sudo mkdir -p /var/www/ghost
```



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

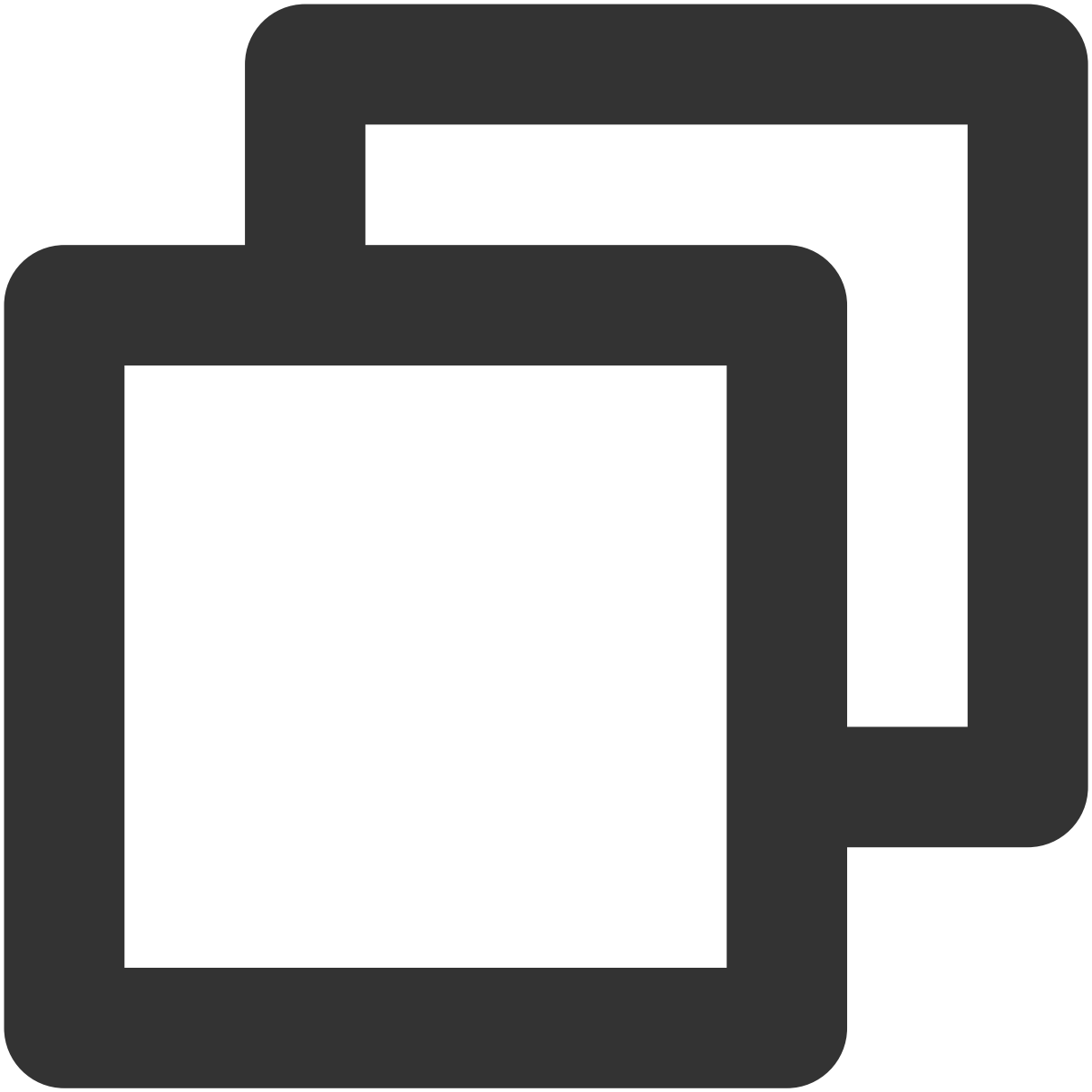


```
sudo chmod 775 /var/www/ghost
```



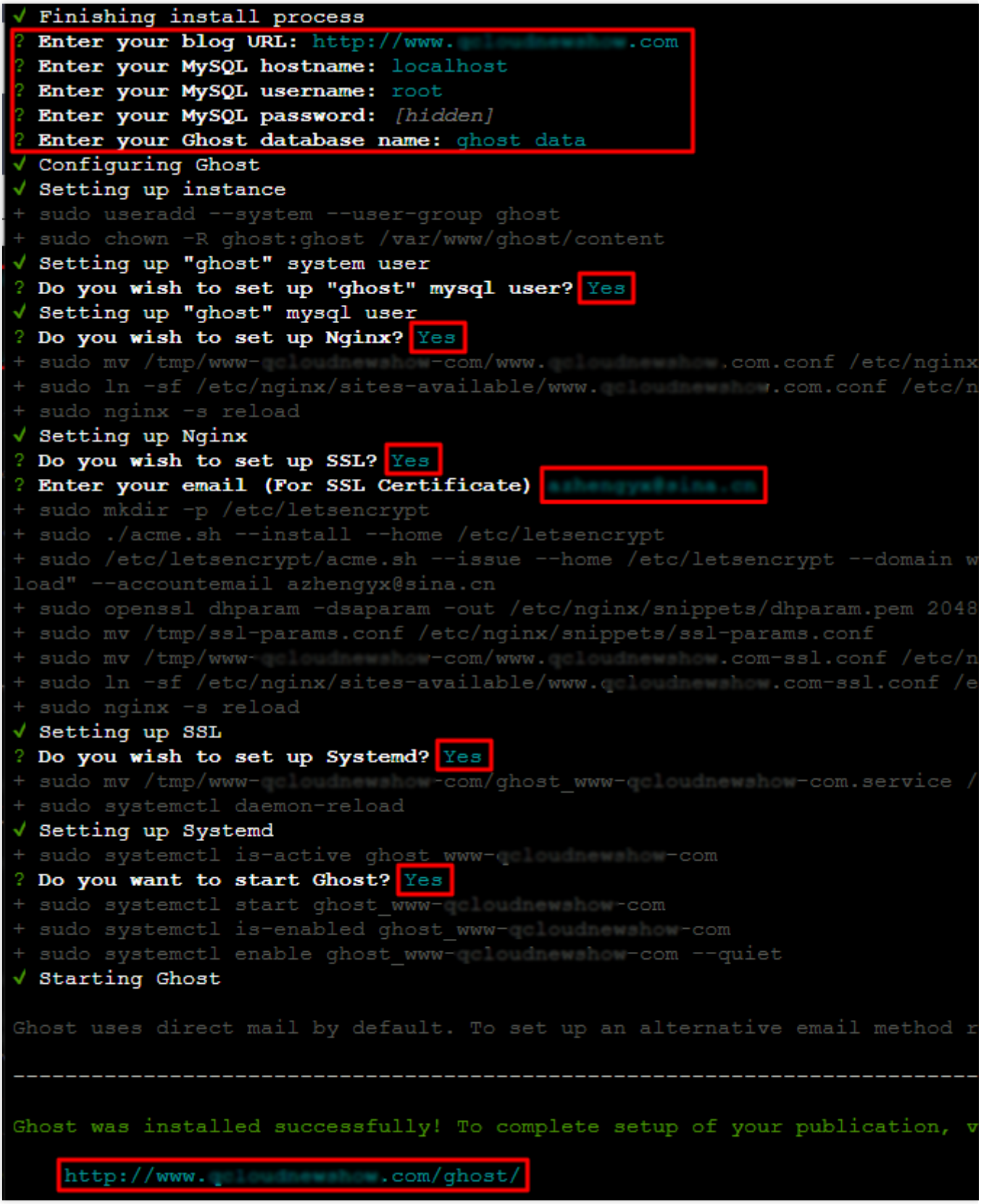
```
cd /var/www/ghost
```

2. 以下のコマンドを実行し、インストールプログラムを実行します。



```
ghost install
```

3. インストールの過程で関連の設定を行う必要があります。画面および以下の表示を参照して設定を完了してください。下図に示します。



主要な設定は次のとおりです。

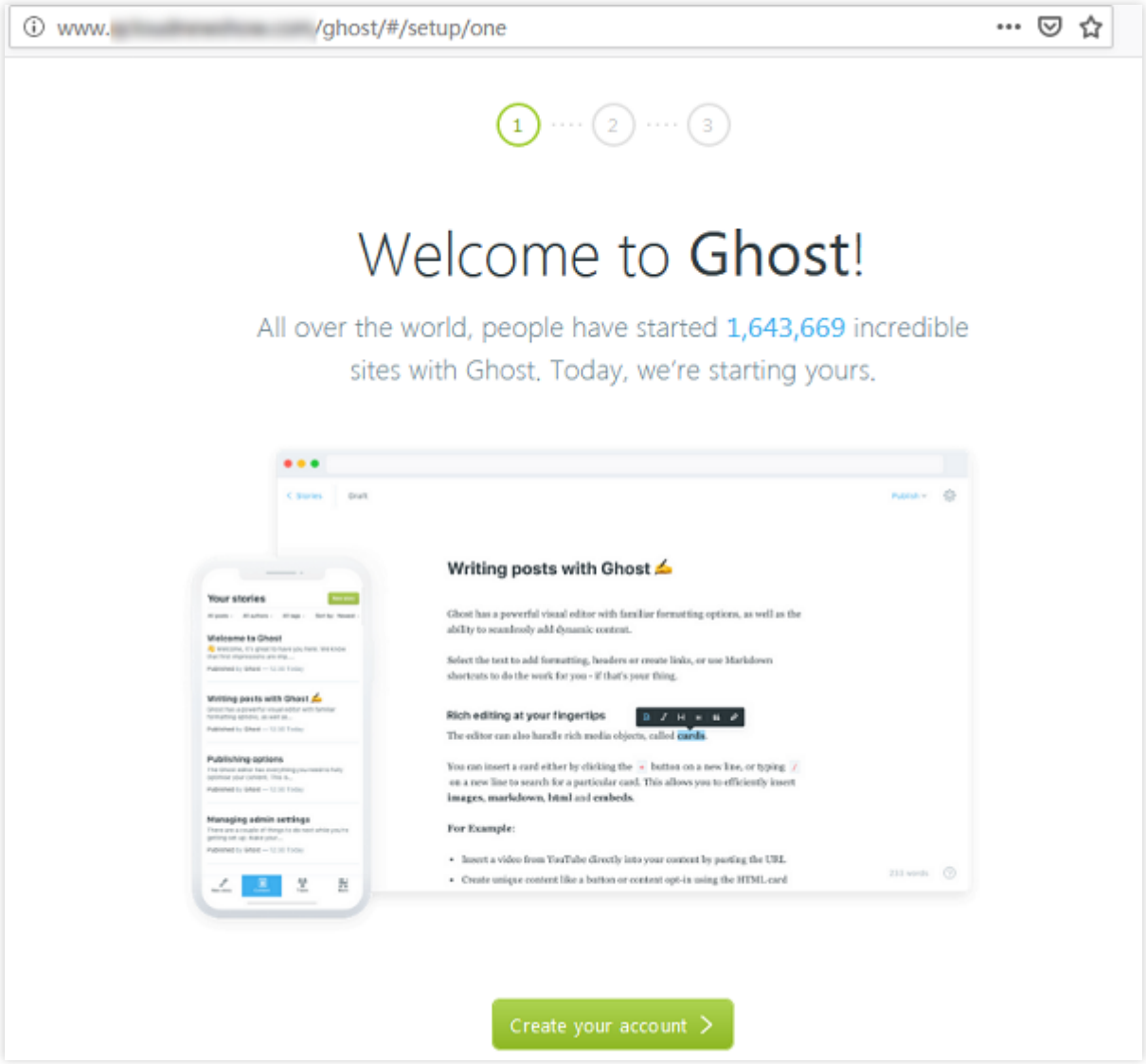
1. **Enter your blog URL**：解決済みのドメイン名を入力します。`http://(ドメイン名)` を入力してください。

2. **Enter your MySQL hostname**：データベース接続アドレスを入力します。 `localhost` を入力し、**Enter**を押してください。
3. **Enter your MySQL username**：データベースのユーザー名を入力します。 `root` を入力し、**Enter**を押してください。
4. **Enter your MySQL password**：データベースのパスワードを入力します。 rootアカウントのパスワード設定 で設定済みのパスワードを入力し、**Enter**を押してください。
5. **Enter your database name**：Ghostで使用するデータベースを入力します。 データベースの作成 で作成済みの `ghost_data` を入力し、**Enter**を押してください。
6. **Do you wish to set up SSL?：HTTPSアクセスを有効にしたい場合はY**を入力し、**Enter**を押してください。
その他の設定は実際の状況に応じて、画面の表示に従って完了してください。設定完了後、画面の下にGhostの管理者アクセス用アドレスが出力されます。
7. ローカルブラウザを使用して、Ghostの管理者アクセス用アドレスにアクセスし、個人ブログの設定を開始します。下図に示します。

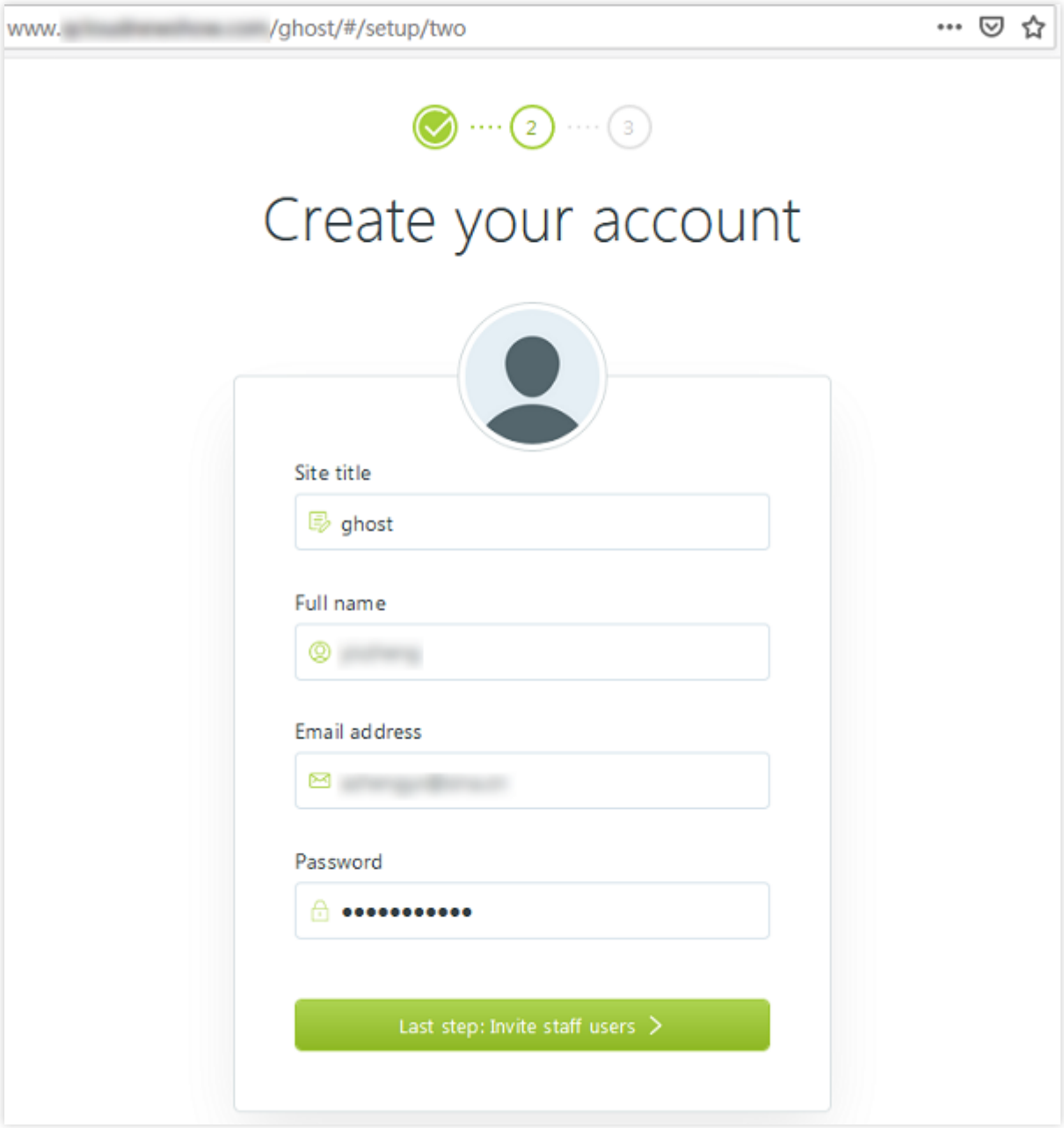
説明：

HTTPSアクセスを有効にしている場合は、 `https://` を使用してアクセスまたはブログ設定などの操作を行ってください。

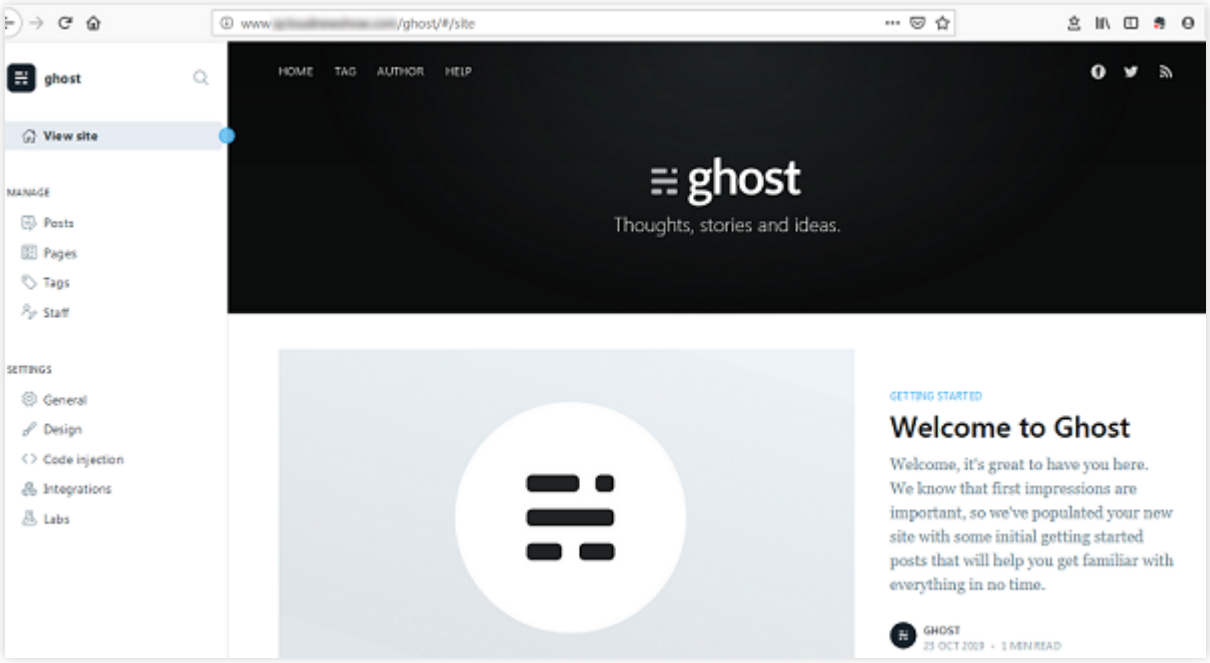
【Create your account】をクリックし、管理者アカウントの作成を開始します。



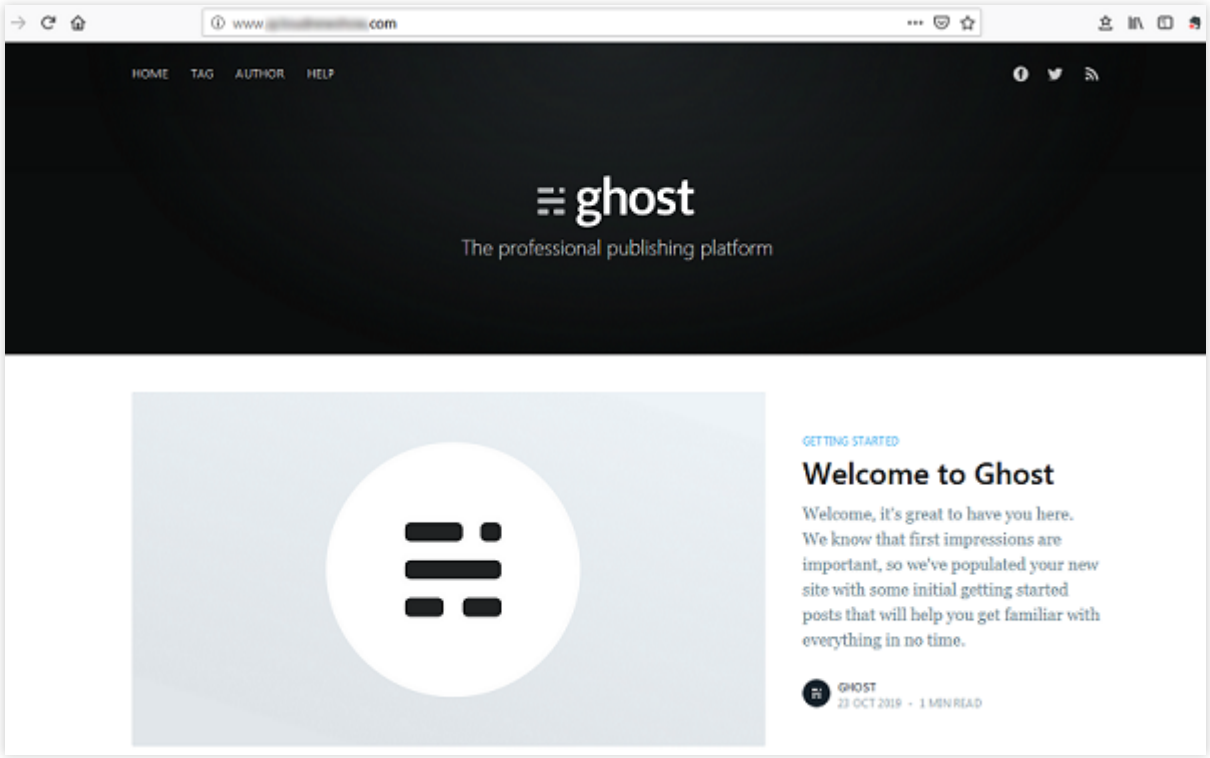
8. 関連情報を入力し、【Last step】をクリックします。下図に示します。



9. 他の人を招待して一緒にブログを作成することもでき、この手順をスキップすることもできます。
10. 管理インターフェースに入ると、ブログの管理を開始できます。下図に示します。



設定完了後、ローカルブラウザを使用して、設定済みのドメイン名 `www.xxxxxxxx.xx` にアクセスすると、個人ブログのトップページを見ることができます。下図に示します。



よくあるご質問

CVMの使用中に問題が発生した場合は、下記のドキュメントを参照して、実際の状況に応じて問題を分析して解決できます。
CVMのログインに関する問題は、パスワードとキー、ログインとリモート接続 ドキュメントをご参照ください。
CVMのネットワークに関する問題は、 IPアドレス、ポートとセキュリティグループ ドキュメントをご参照ください。
CVMのハードディスクに関する問題は、システムディスクとデータディスクドキュメントをご参照ください。

アプリケーションの構築
FTPサービスの構築
Linux CVMでFTPサービスを構築

最終更新日：：2022-05-07 15:18:55

概要

Vsftpd（very secure FTP daemon）は、多数のLinuxディストリビューションのデフォルトのFTPサーバーです。本節では、CentOS 7.6 64ビットOSのTencent Cloud Server（CVM）を例に、vsftpdを使用してLinux CVMのFTPサービスを構築します。

ソフトウェアのバージョン

本文では、作成したFTPサービスのコンポーネントバージョンは次のとおりです：
Linux OS ：本節では、公開イメージCentOS 7.6を例に説明します。
Vsftpd：本節では、vsftpd 3.0.2を例に説明します。

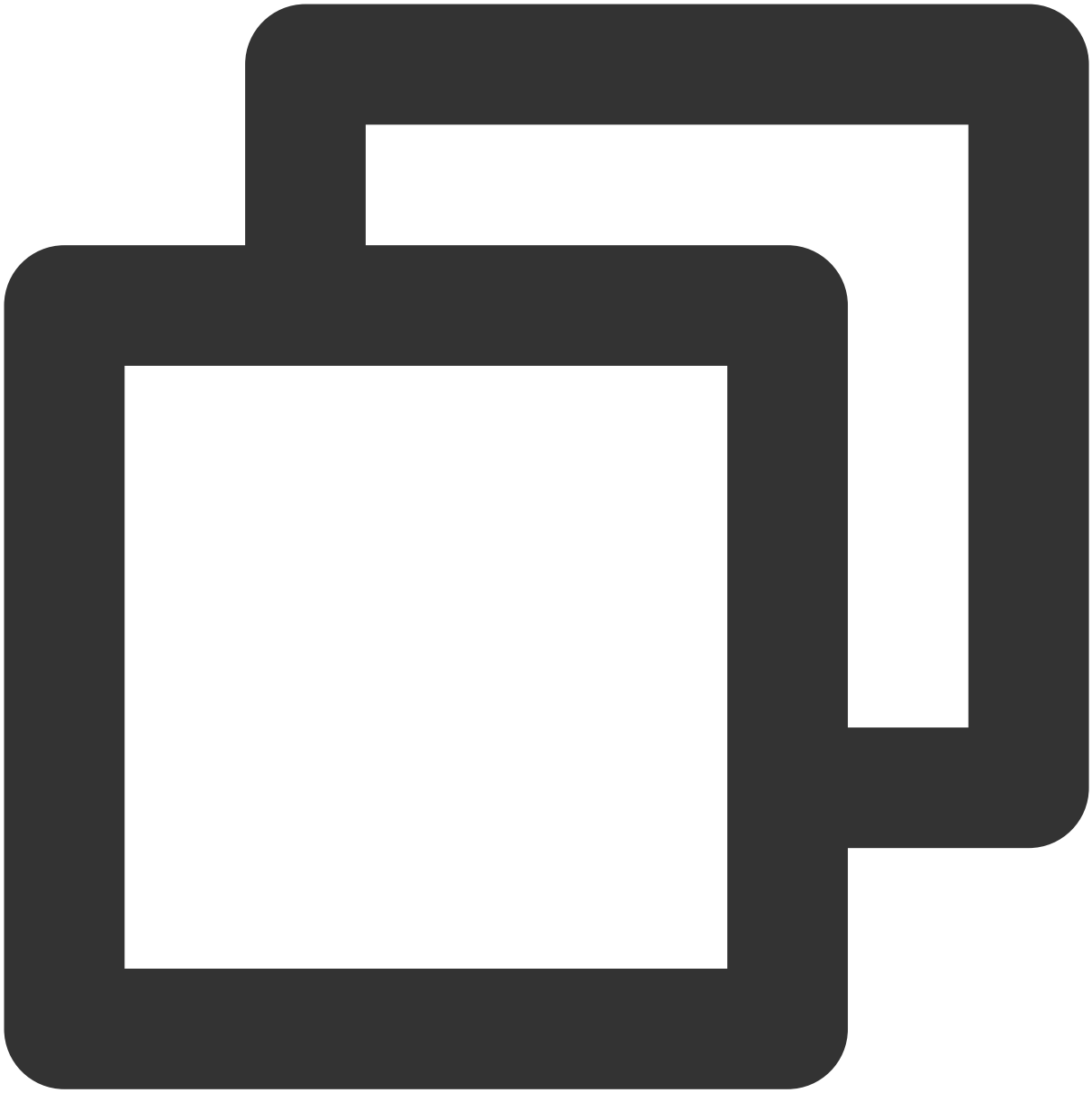
操作手順

ステップ1：CVMにログインする

標準的な方法を使用してLinuxインスタンスにログインする（推奨）。実際の操作方法に応じて、他のログイン方法を選択することもできます：
リモートログインソフトウェアを使用してLinuxインスタンスにログインする
SSHキーを使用してLinuxインスタンスにログインする

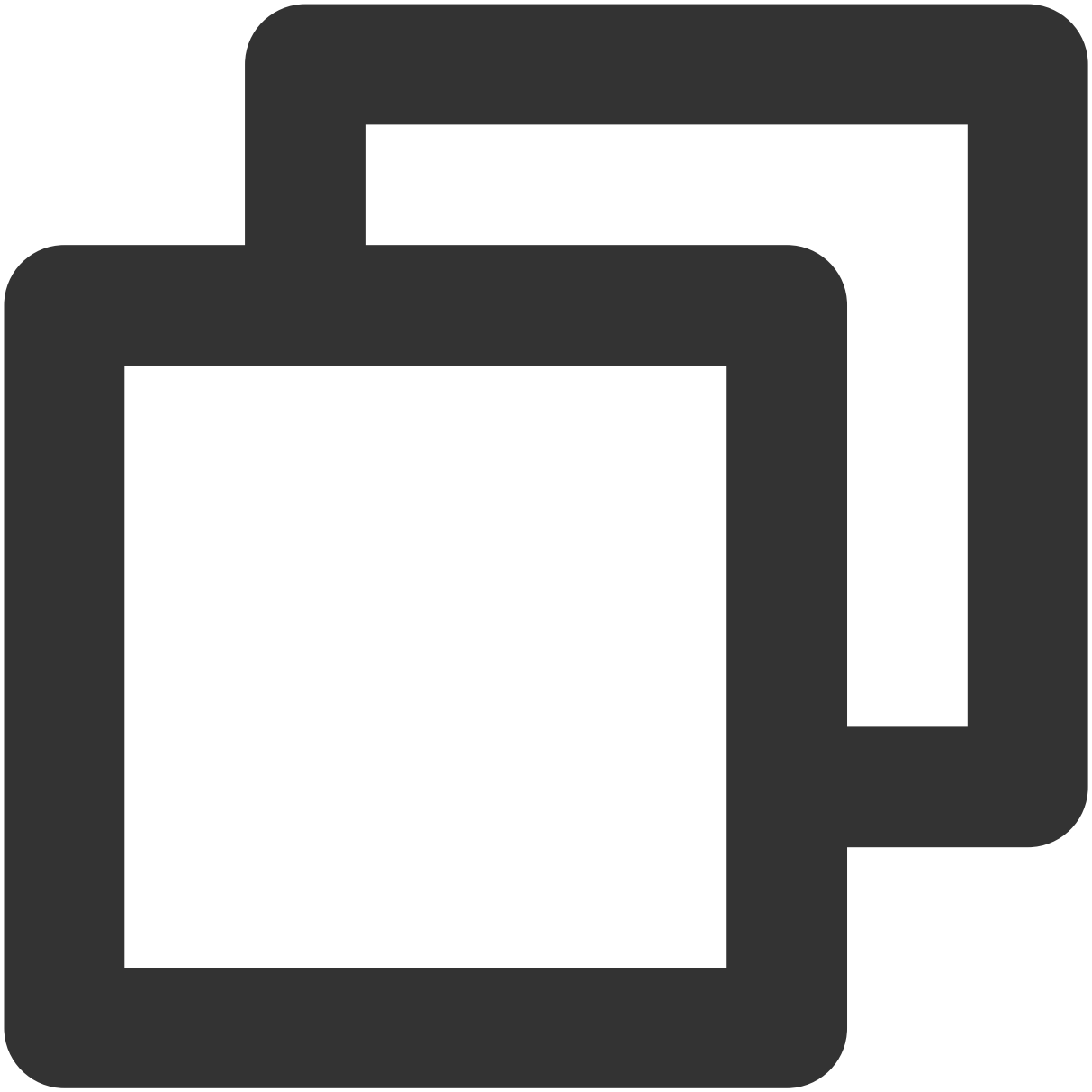
手順2：vsftpdのインストール

1. 次のコマンドを実行し、vsftpdをインストールします。



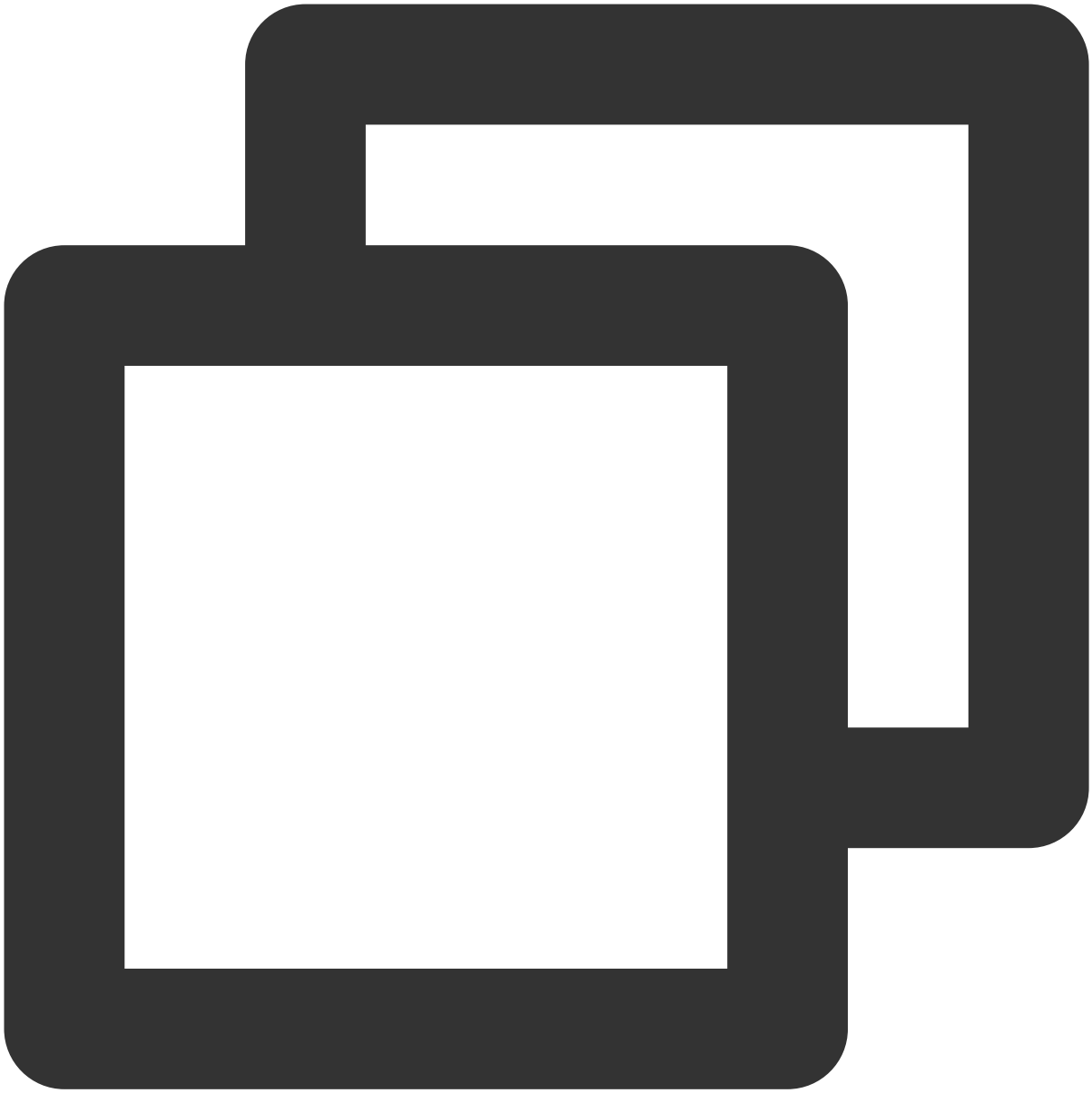
```
yum install -y vsftpd
```

2. 次のコマンドを実行し、vsftpdをスタートアップ時に自動起動に設定します。



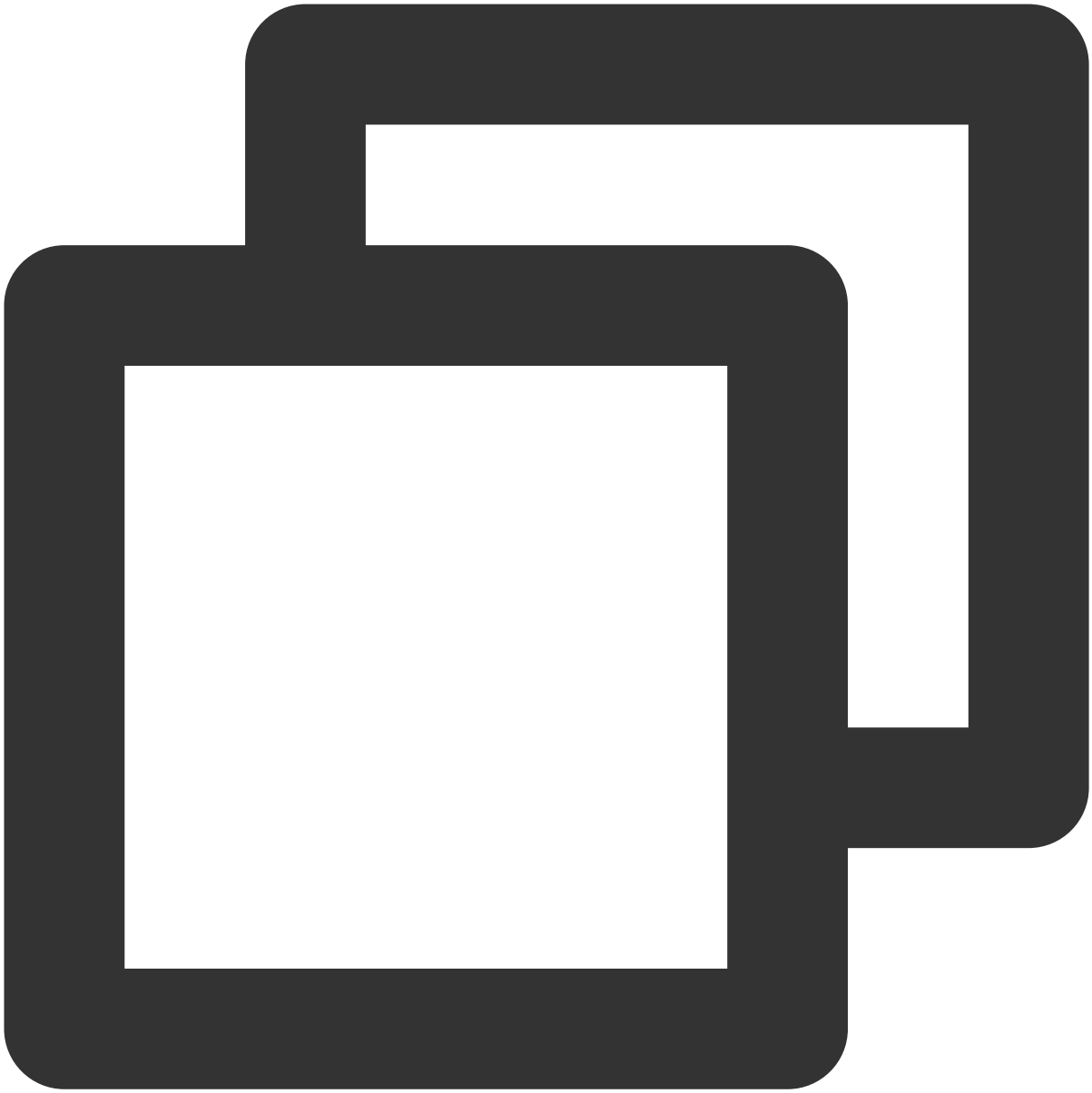
```
systemctl enable vsftpd
```

3. 次のコマンドを実行し、FTPサービスを起動します。



```
systemctl start vsftpd
```

4. 次のコマンドを実行し、サービスが起動されているかどうかを確認します。



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

次の結果が表示され、FTPサービスが正常に開始されたことを示します。

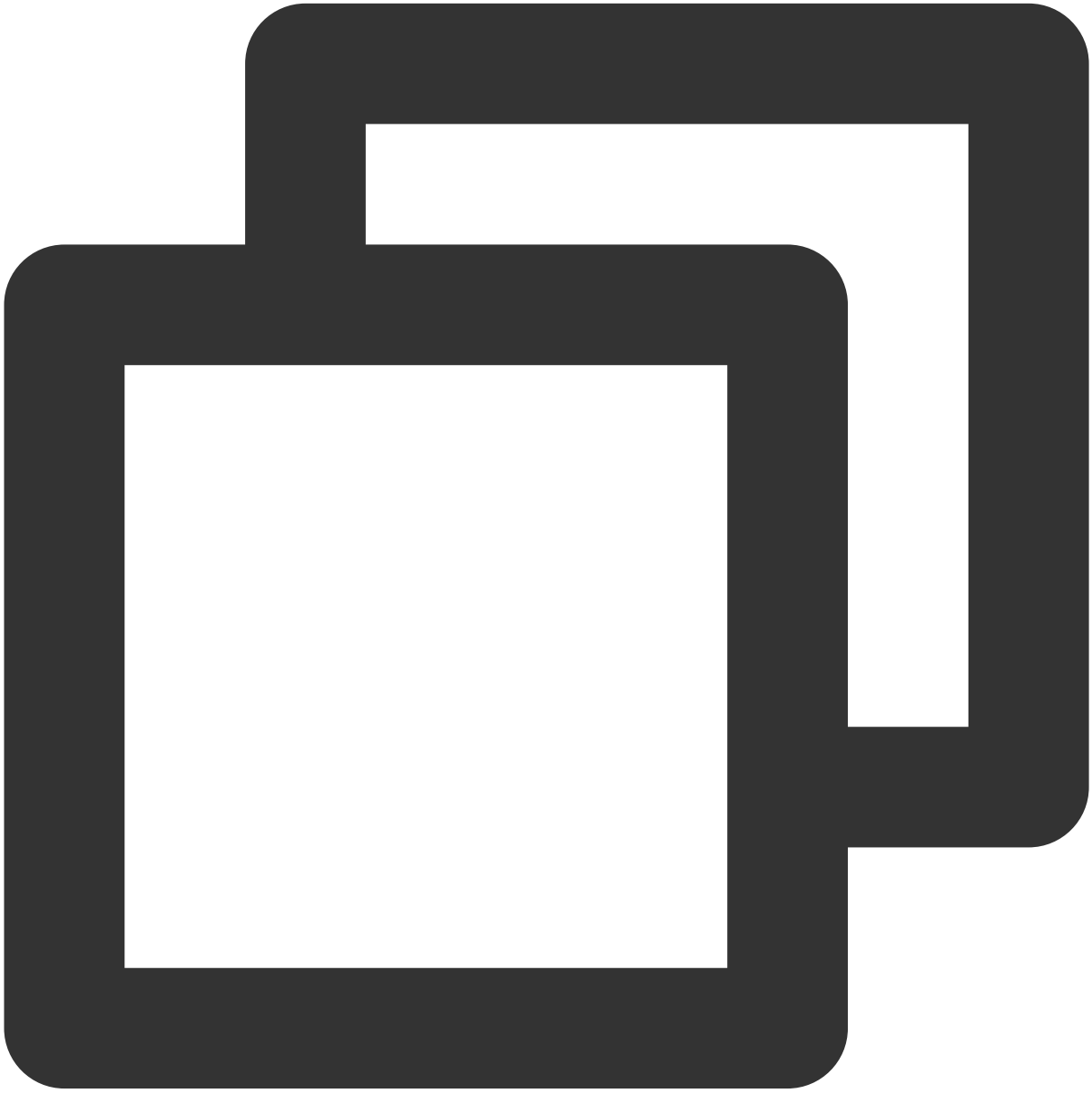
```
[root@VM_0_117_centos ~]# systemctl start vsftpd
[root@VM_0_117_centos ~]# netstat -antup | grep ftp
tcp6       0      0 :::21                   :::*                    LISTEN
```

このとき、vsftpdはデフォルトで匿名アクセスモードを有効化しており、ユーザー名およびパスワードを必要とす

ることなくFTPサーバーにログインできます。この方法でFTPサーバーにログインするユーザーには、ファイルを変更またはアップロードする権限がありません。

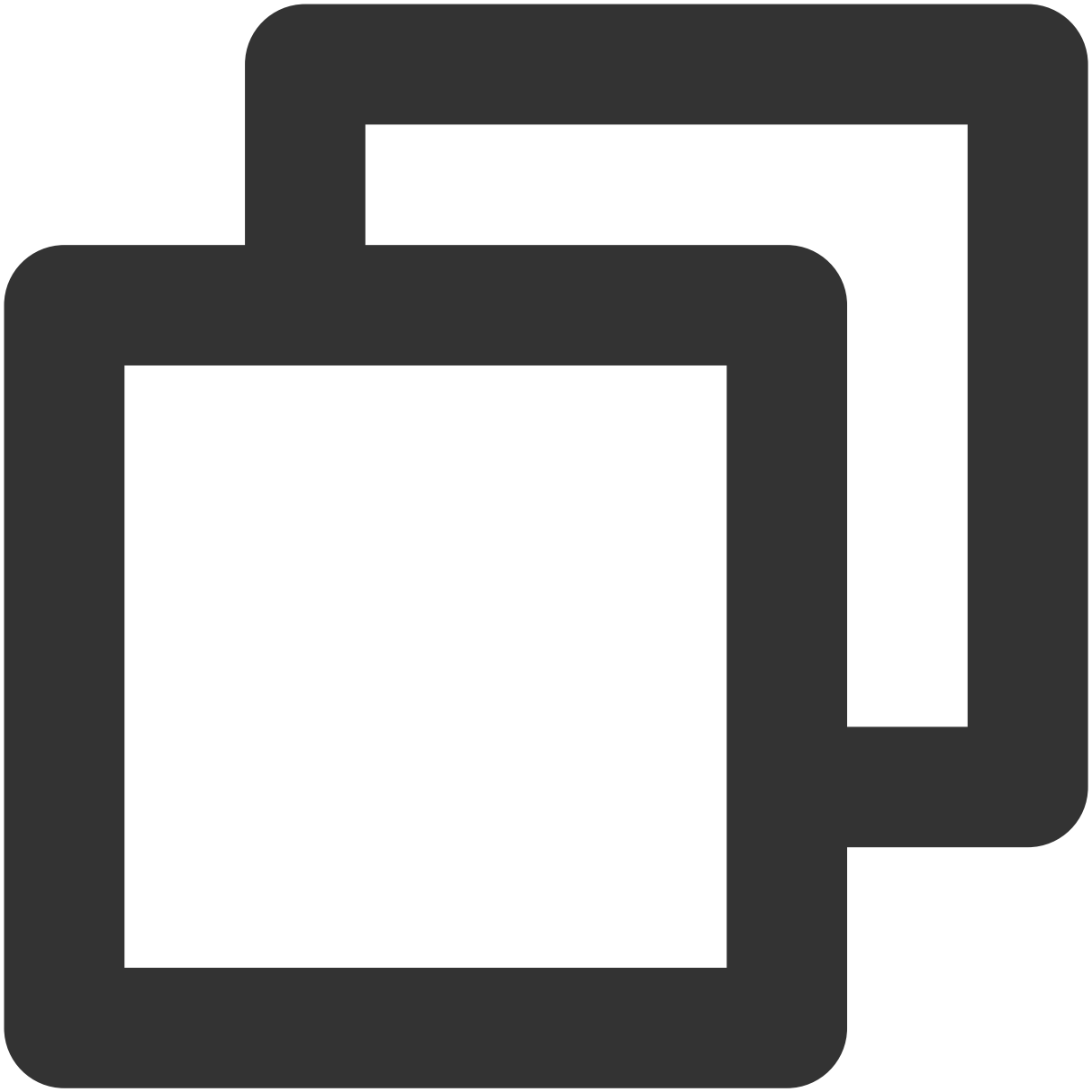
手順3：vsftpdの設定

1. 次のコマンドを実行して、FTPサービス用のLinuxユーザーを作成します。本節では、ftpuserを例に説明します。



```
useradd ftpuser
```

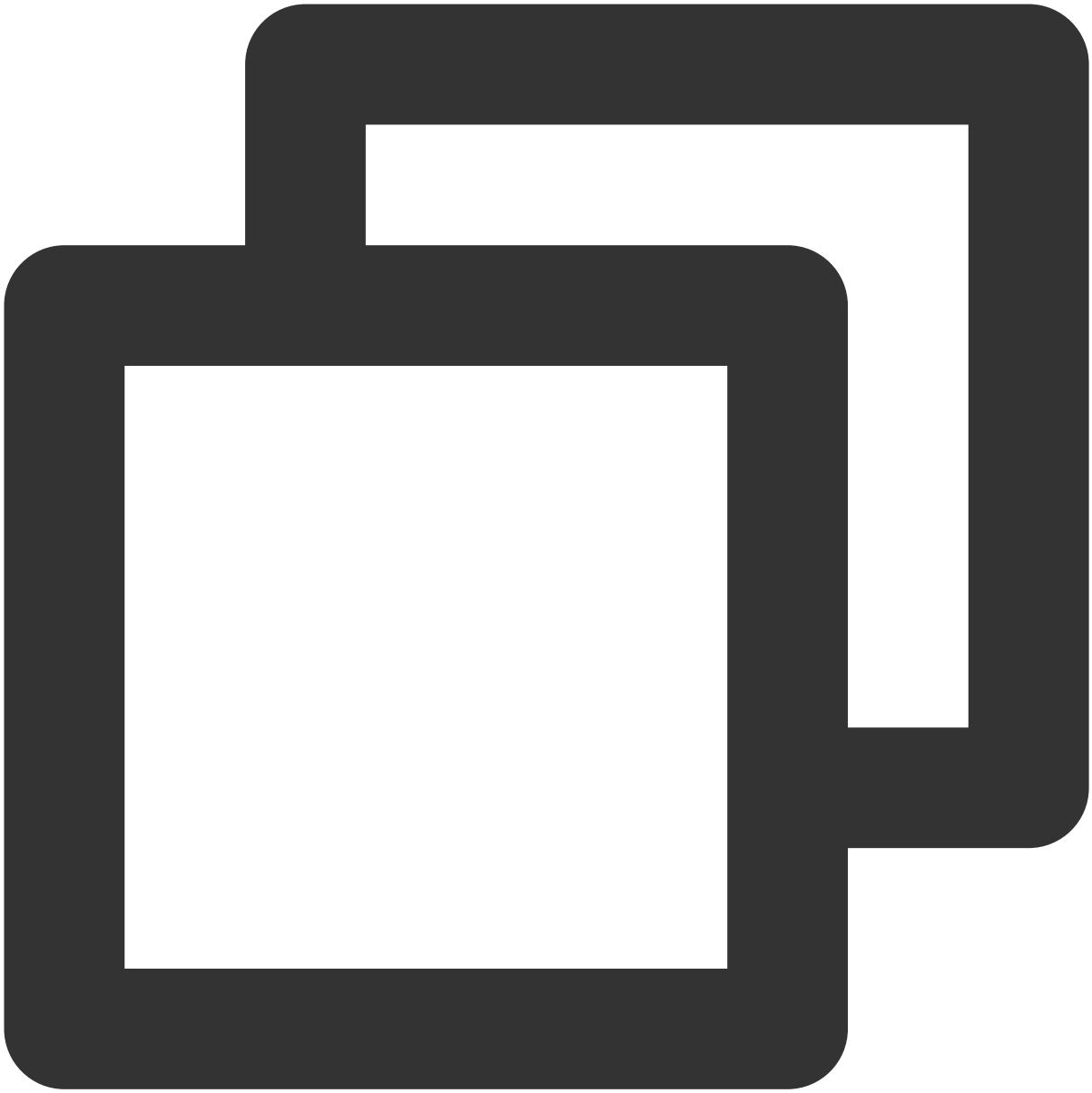
2. 次のコマンドを実行して、ftpuserユーザーのパスワードを設定します。



```
passwd ftpuser
```

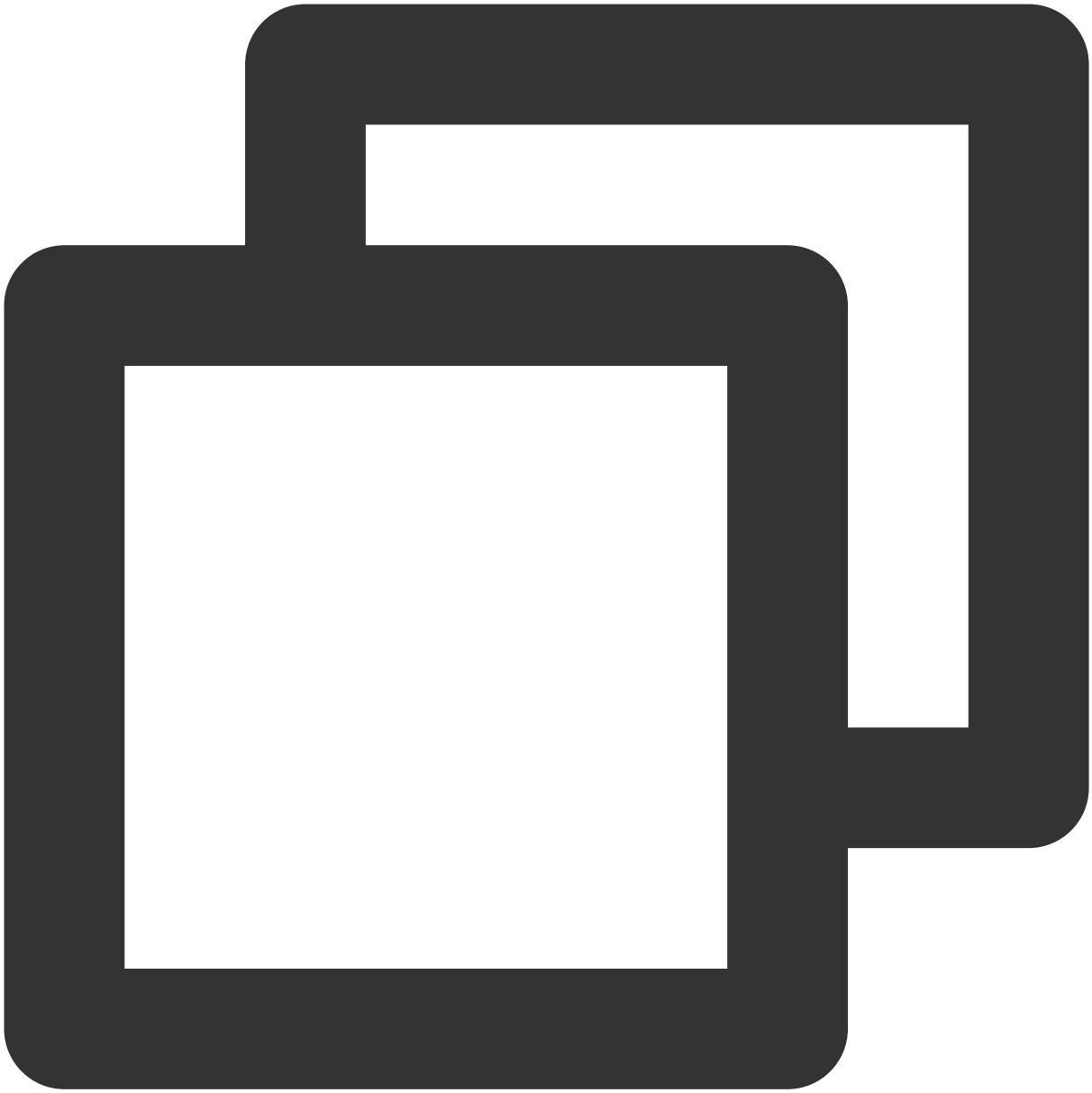
パスワードを入力したら、** Enter **キーを押して確認します。デフォルトではパスワードは表示されません。本節では「tf7295TFY」を例にしています。

3. 次のコマンドを実行して、FTPサービスが使用するファイルディレクトリを作成します。本節では、「/var/ftp/test」を例にしています。



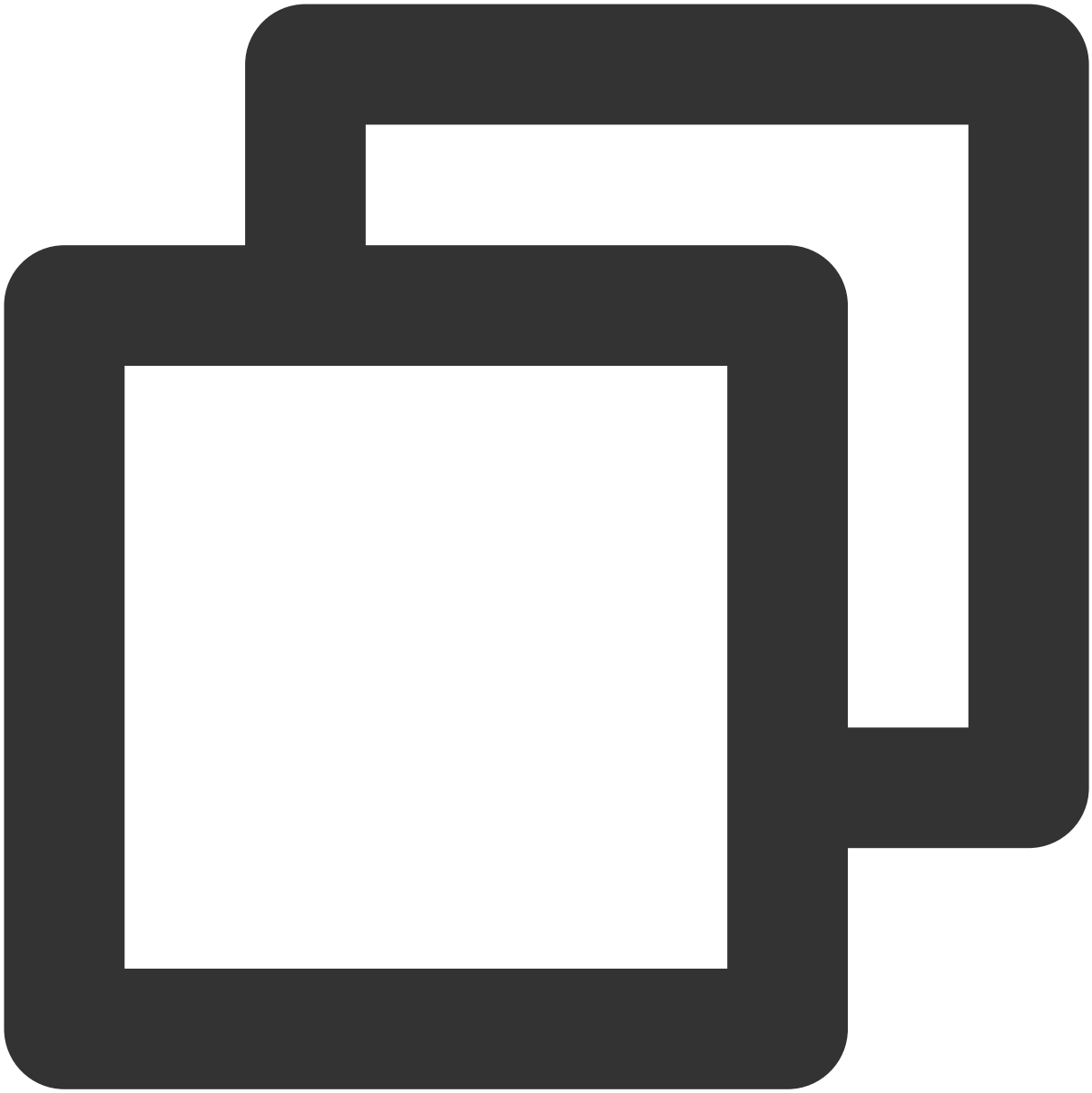
```
mkdir /var/ftp/test
```

4. 次のコマンドを実行して、ディレクトリの権限を変更します。



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

5. 次のコマンドを実行し、「vsftpd.conf」ファイルを開きます。



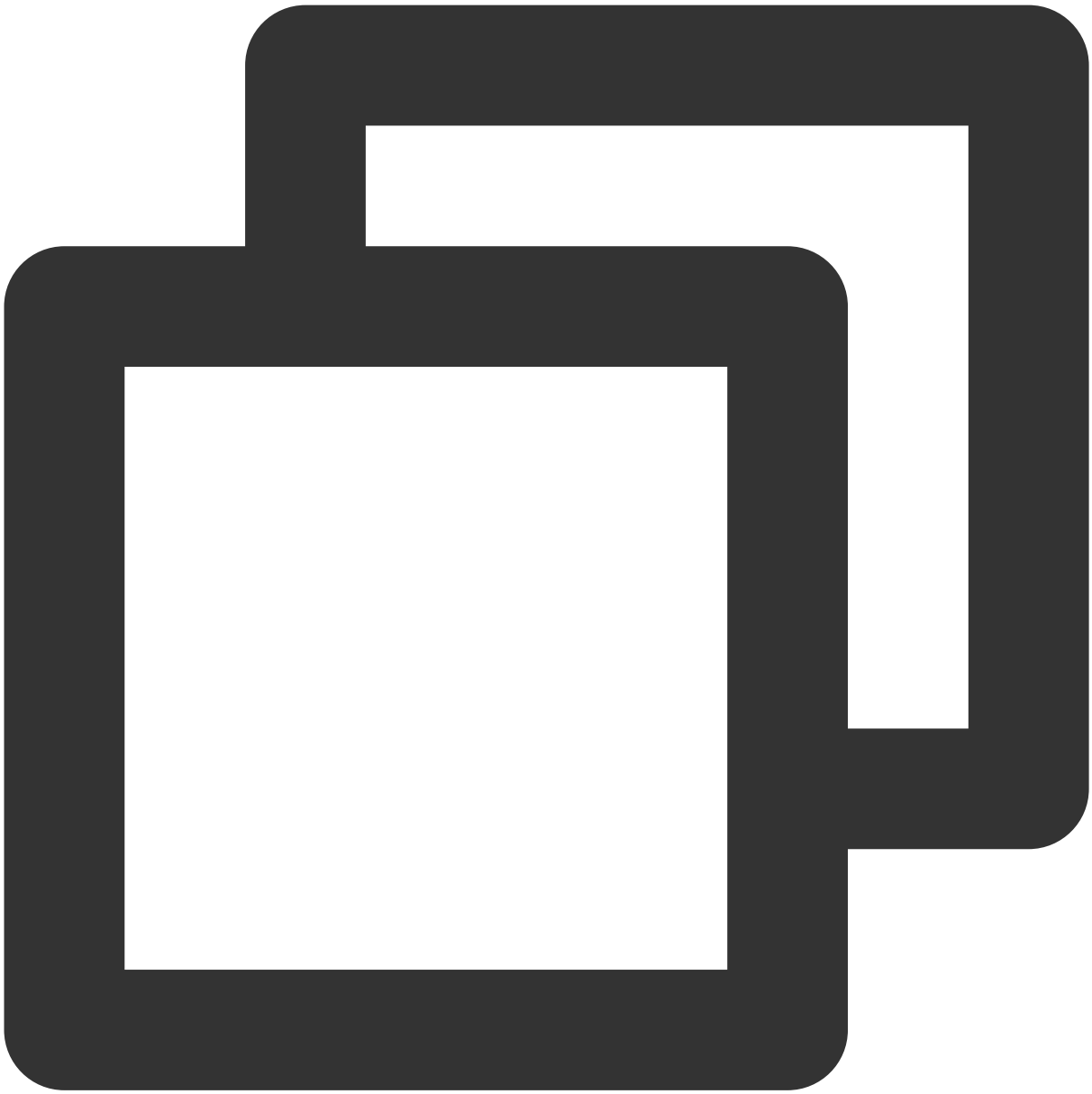
```
vim /etc/vsftpd/vsftpd.conf
```

6. **i**を押して編集モードに切り替え、必要に応じてFTPモードを選択し、設定ファイル `vsftpd.conf` ：を変更します

ご注意：

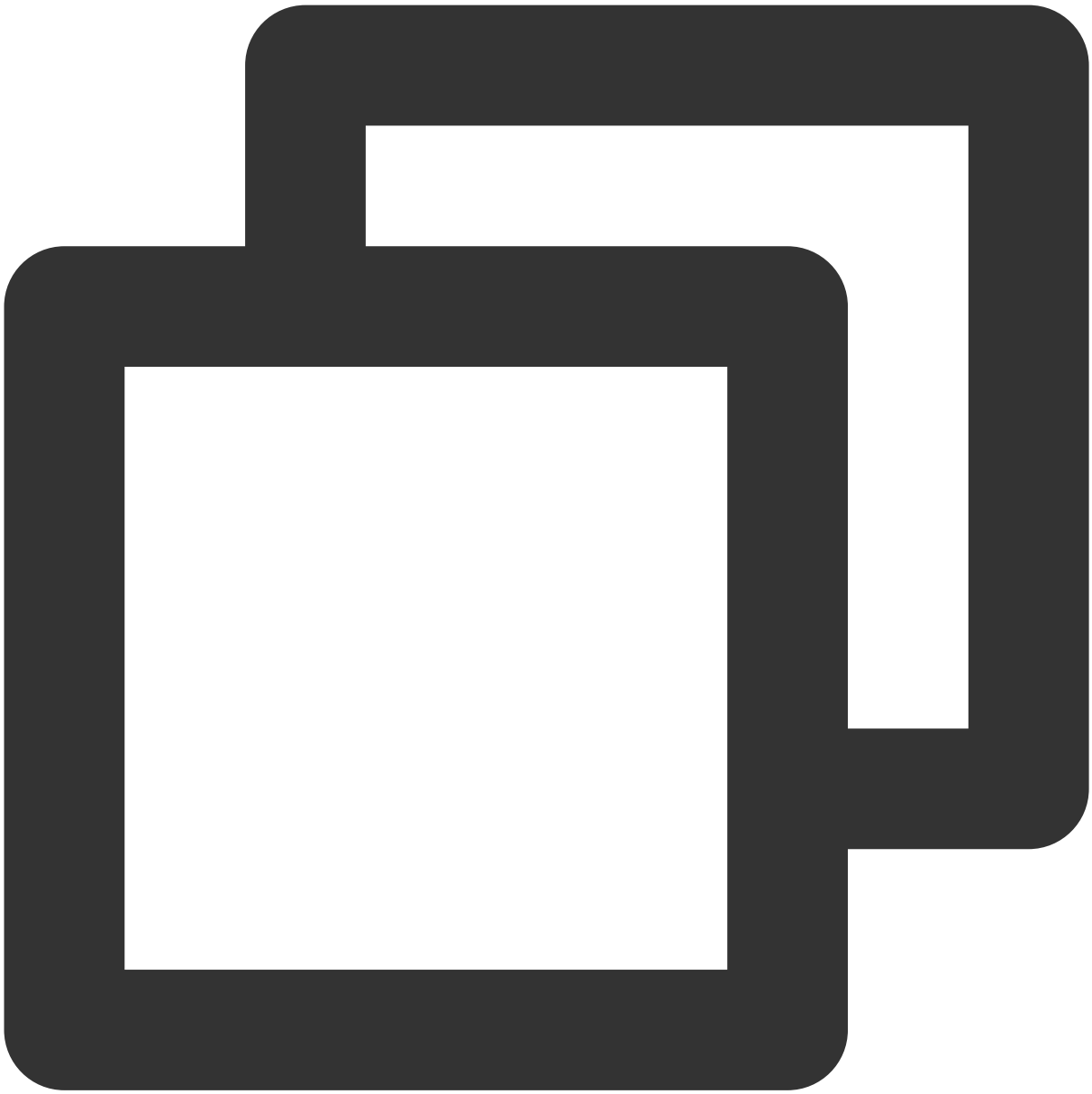
FTPは、アクティブモードとパッシブモードでクライアント端末に接続してデータを転送できます。ほとんどのクライアント端末のファイアウォール設定および実際のIPアドレスを取得できないため、**パッシブモード**を選択してFTPサービスを構築することをお勧めします。次の変更では、パッシブモードの設定を例として説明します。アクティブモードを選択したい場合は、FTPアクティブモードの設定に進んでください。

6.1 以下の構成パラメータを変更し、匿名ユーザーとローカルユーザーのログイン権限を設定して、指定された例外ユーザーリストファイルのパスを設定し、IPv4 socketsのリスニングを有効にします。



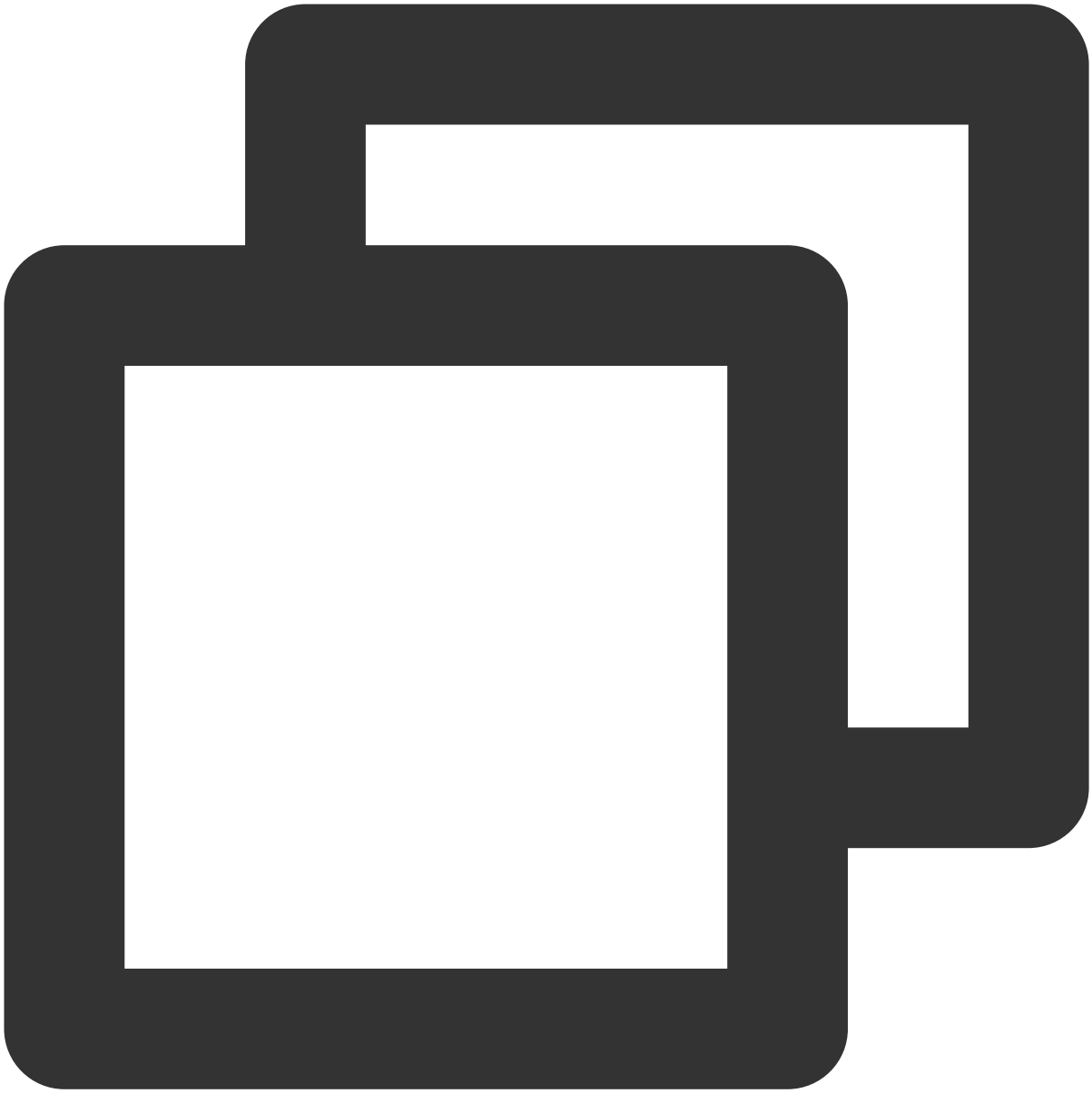
```
anonymous_enable=NO
local_enable=YES
write_enable=YES
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
listen=YES
```

6.2 行の先頭に `#` を付けて、 `listen_ipv6=YES` 構成パラメータに注釈を付け、IPv6 socketsのリスニングを無効にします。



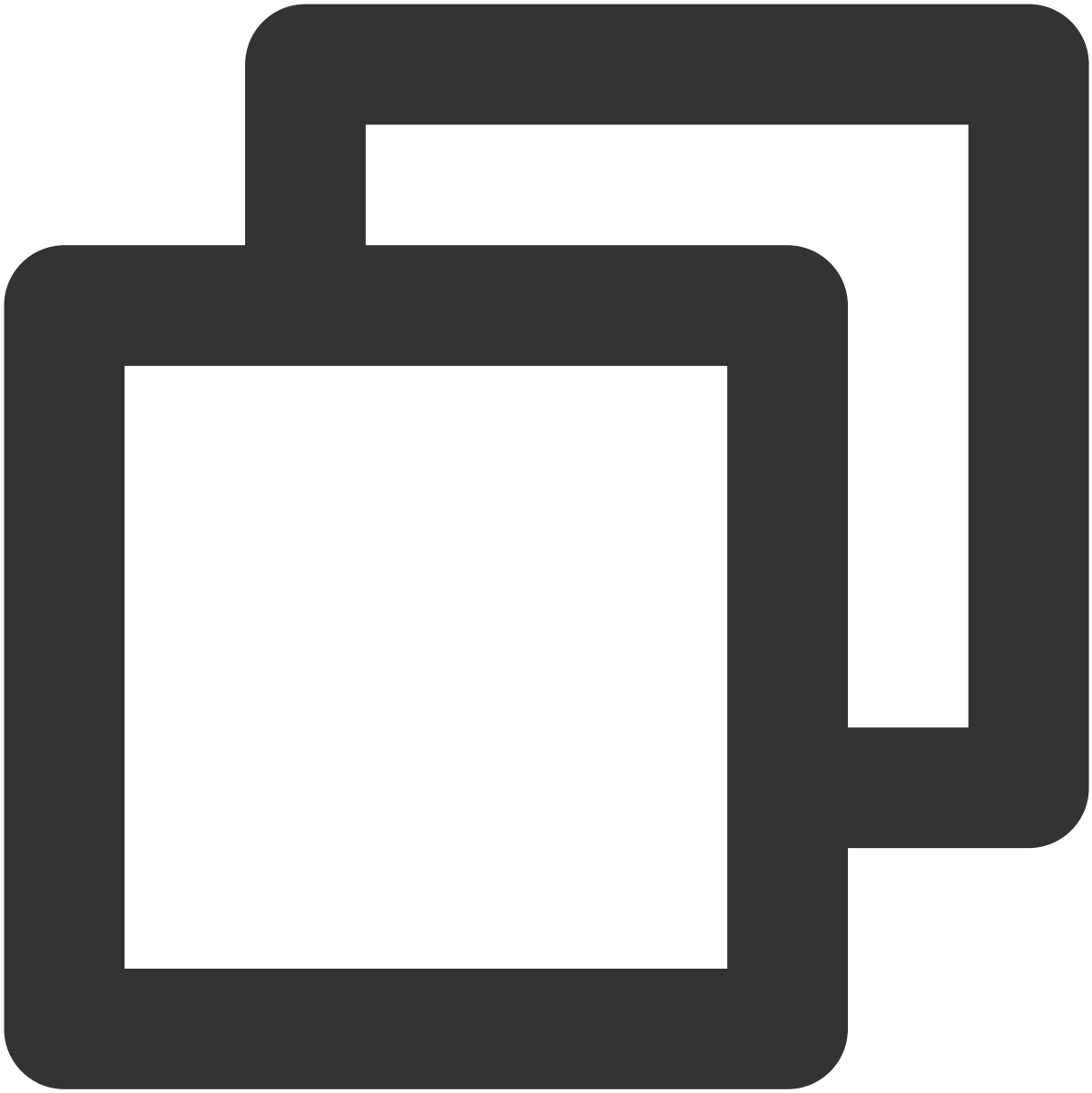
```
#listen_ipv6=YES
```

6.3 以下の構成パラメータを追加し、パッシブモードを有効にし、ローカルユーザーがログインした後のディレクトリ、およびCVMがデータ転送を確立するために使用できるポート範囲の値を設定します。



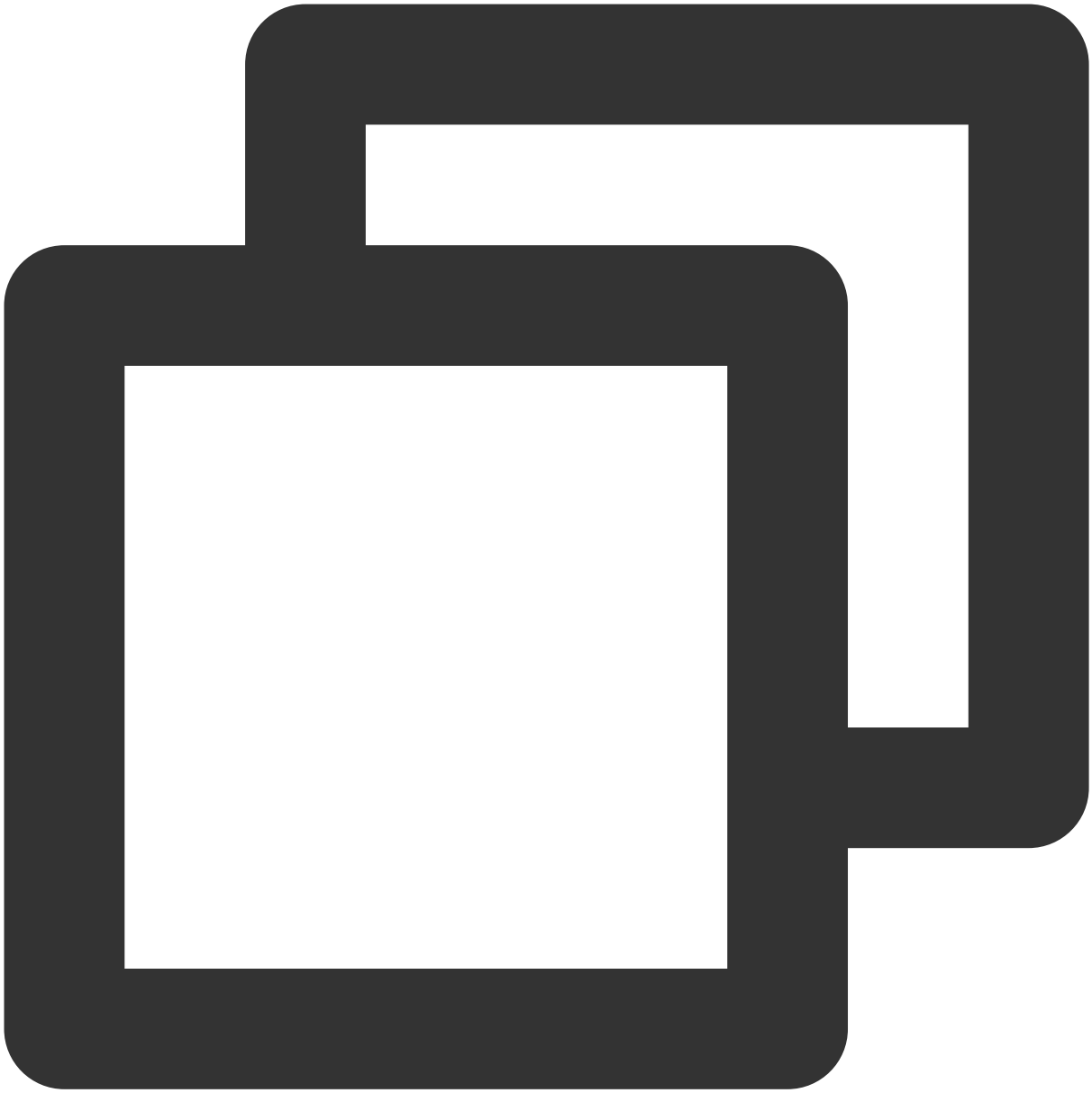
```
local_root=/var/ftp/test
allow_writeable_chroot=YES
pasv_enable=YES
pasv_address=xxx.xx.xxx.xx #ご利用のLinux CVMパブリックIPに変更してください
pasv_min_port=40000
pasv_max_port=45000
```

7. **Esc**を押して、**:wq**と入力し、保存して終了します。
8. 次のコマンドを実行して、 `chroot_list` ファイルを作成して編集します。



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

9. **i**を押して編集モードに入り、ユーザー名を入力します。1つのユーザー名が1行に収まり、設定が完了すると、**Esc**を押し、**:wqを入力して保存して終了します。
設定するユーザーの権限はルートディレクトリに限定されていません。例外ユーザーを設定する必要がない場合は、この手順をスキップでき、:wq**を入力してファイルを終了します。
10. 次のコマンドを実行し、sshサービスを再起動します。



```
systemctl restart vsftpd
```

手順4：セキュリティグループの設定

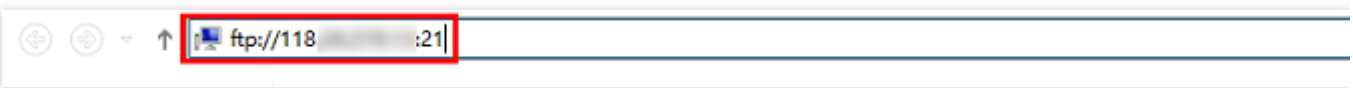
FTPサービスを構築した後、実際に使用するFTPモードに従って、Linux CVMに**インバウンドルール**をインターネットにオープンする必要があります。詳細については、セキュリティグループルールの追加 をご参照ください。
ほとんどのクライアント端末はLANにあり、IPアドレスが変換されたものです。FTPのアクティブモードを選択し

た場合は、クライアントマシンが真のIPアドレスを取得したことを確認してください。取得していない場合、クライアントがFTPサーバーにログインできない場合があります。
アクティブモードの場合：ポート21を開きます。
パッシブモードの場合：ポート21と、および 設定ファイルの変更 で設定されている `pasv_min_port` から `pasv_max_port` までのすべてのポートを開きます。（本節では、ポート40000～45000を開きます）。

手順5：FTPサービスの検証

FTPクライアントソフトウェア、ブラウザ、またはファイルエクスプローラなどのツールを使用してFTPサービスを検証できます。本節では、クライアントのファイルエクスプローラを例に説明します。
1. クライアントのInternet Explorerを開き、**ツール>インターネットオプション>詳細設定**を選択し、選択したFTPモードに応じて変更します：
アクティブモードの場合：「パッシブFTPを使用する」のチェックを外します。
パッシブモードの場合：「パッシブFTPを使用する」のチェックを入れます。
2. 次の図に示すように、クライアントでWindowsエクスプローラーを開き、アドレスボックスに次のアドレスを入力して、Enterキーを押します：

```
ftp://云服务器公网IP:21
```



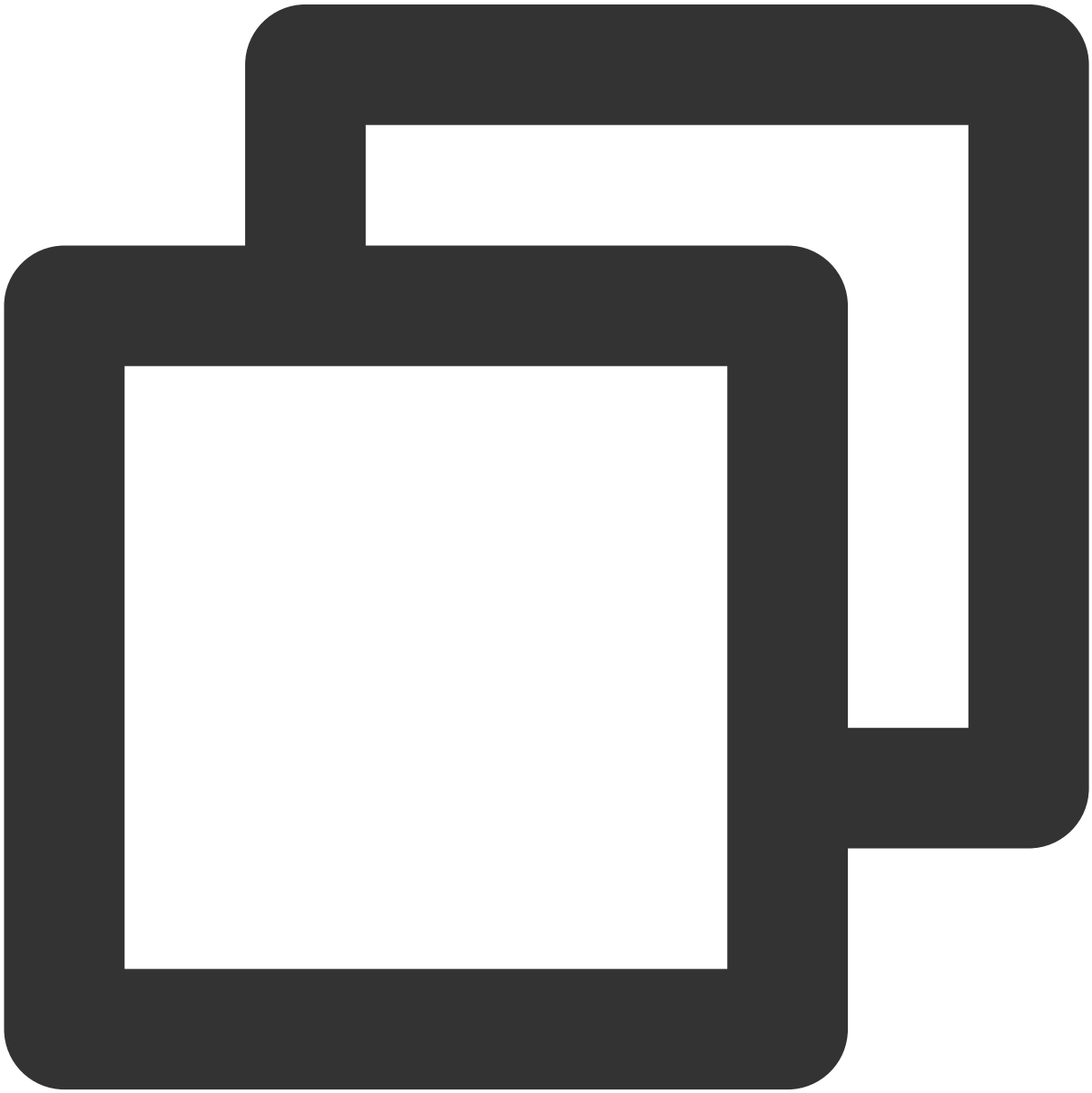
3. ポップアップされた「ログインID」画面に vsftpdを設定する で設定されたユーザー名とパスワードを入力します。

本節で使用するユーザー名が「ftpuser」、パスワードが「tf7295TFY」です。
4. ログインが成功したら、ファイルをアップロード及びダウンロードできます。

付録

FTPのアクティブモードの設定

アクティブモードで変更が必要な設定は次のとおりであり、それ以外の設定項目はデフォルトのままにします：



```
anonymous_enable=NO        #匿名ユーザーのログインを禁止する
```

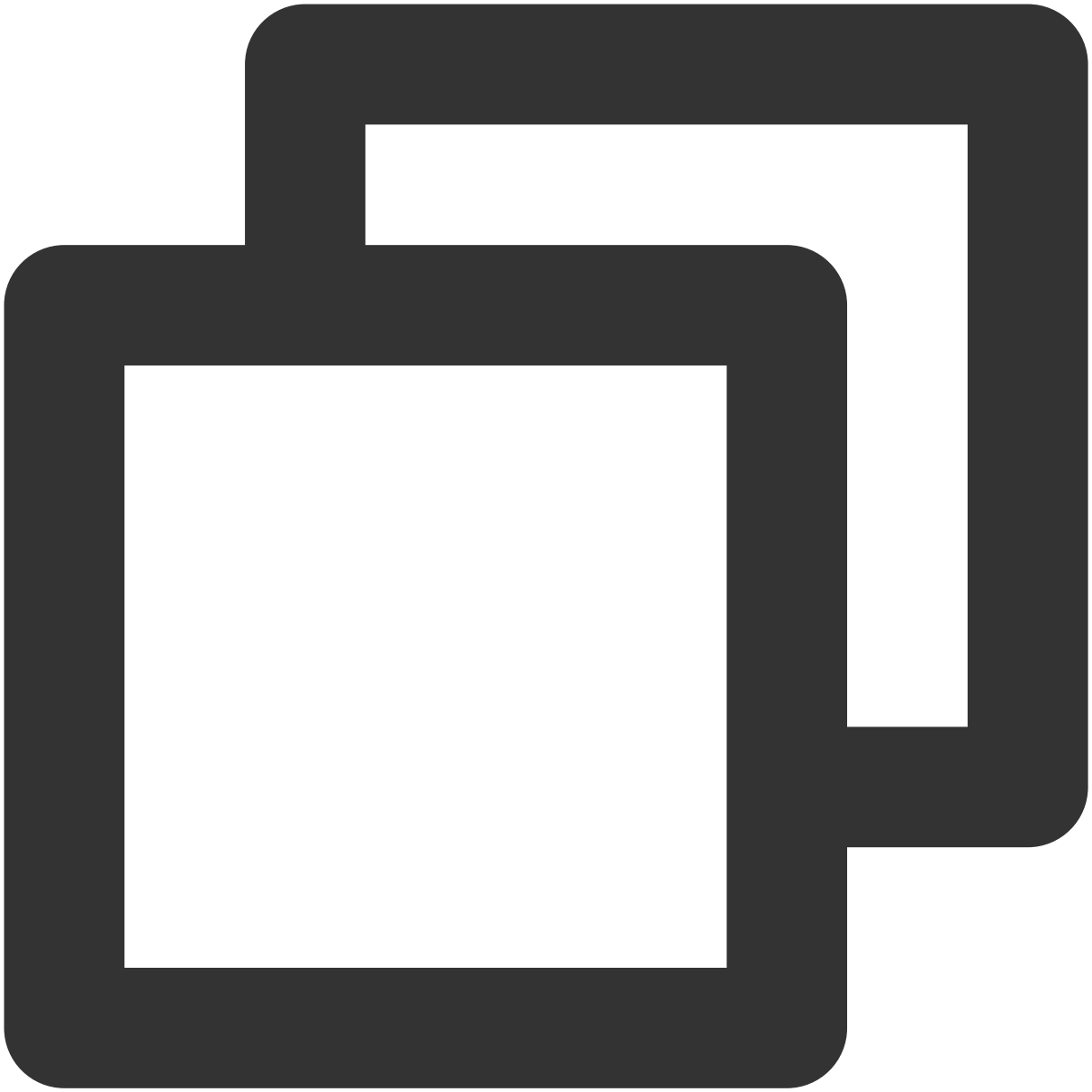
```
local_enable=YES          #ローカルユーザーのログインを許可する
chroot_local_user=YES     #すべてのユーザーがルートディレクトリのみにアクセスするように制限する
chroot_list_enable=YES    #例外ユーザーリストを有効にする
chroot_list_file=/etc/vsftpd/chroot_list  #ユーザーリストファイルを指定します。このリストの
listen=YES                #IPv4 socketsをリスニングする
#行の先頭に#を付けて、次のパラメータをコメントアウトします
#listen_ipv6=YES          #IPv6 socketsのリスニングをオフにする
#次のパラメータを追加する
allow_writeable_chroot=YES
local_root=/var/ftp/test #ローカルユーザーがログインした後の常駐するディレクトリを設定する
```

Esc を押して**:wq**を入力し、保存して終了します。手順8 に進み、vsftpdの設定を完了します。

FTPクライアントからのファイルアップロード処理がエラー

問題の説明

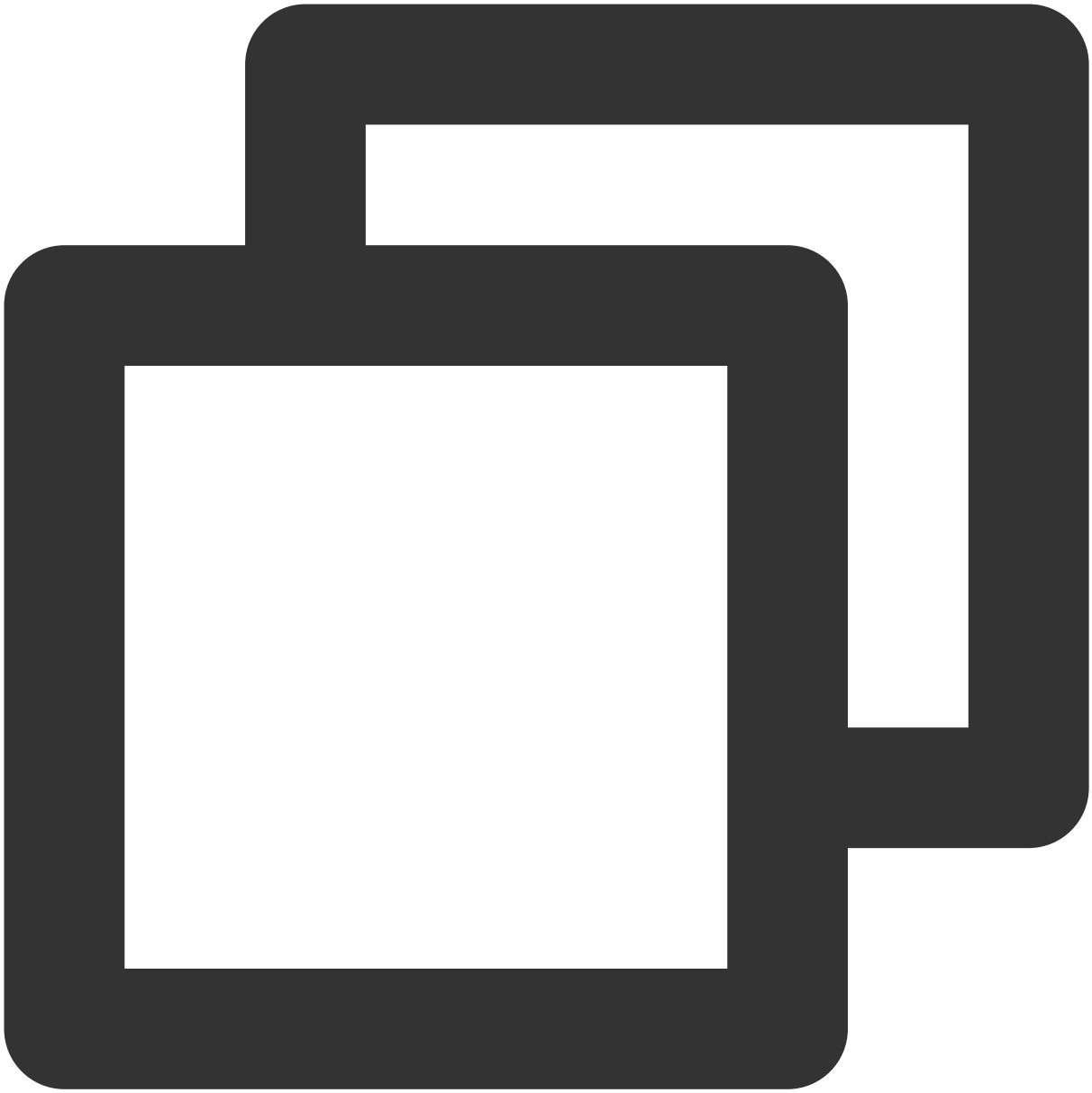
Linuxシステム環境では、vsftp経由でファイルをアップロードする時に、下記のようなエラー情報が表示されます。



```
553 Could not create file
```

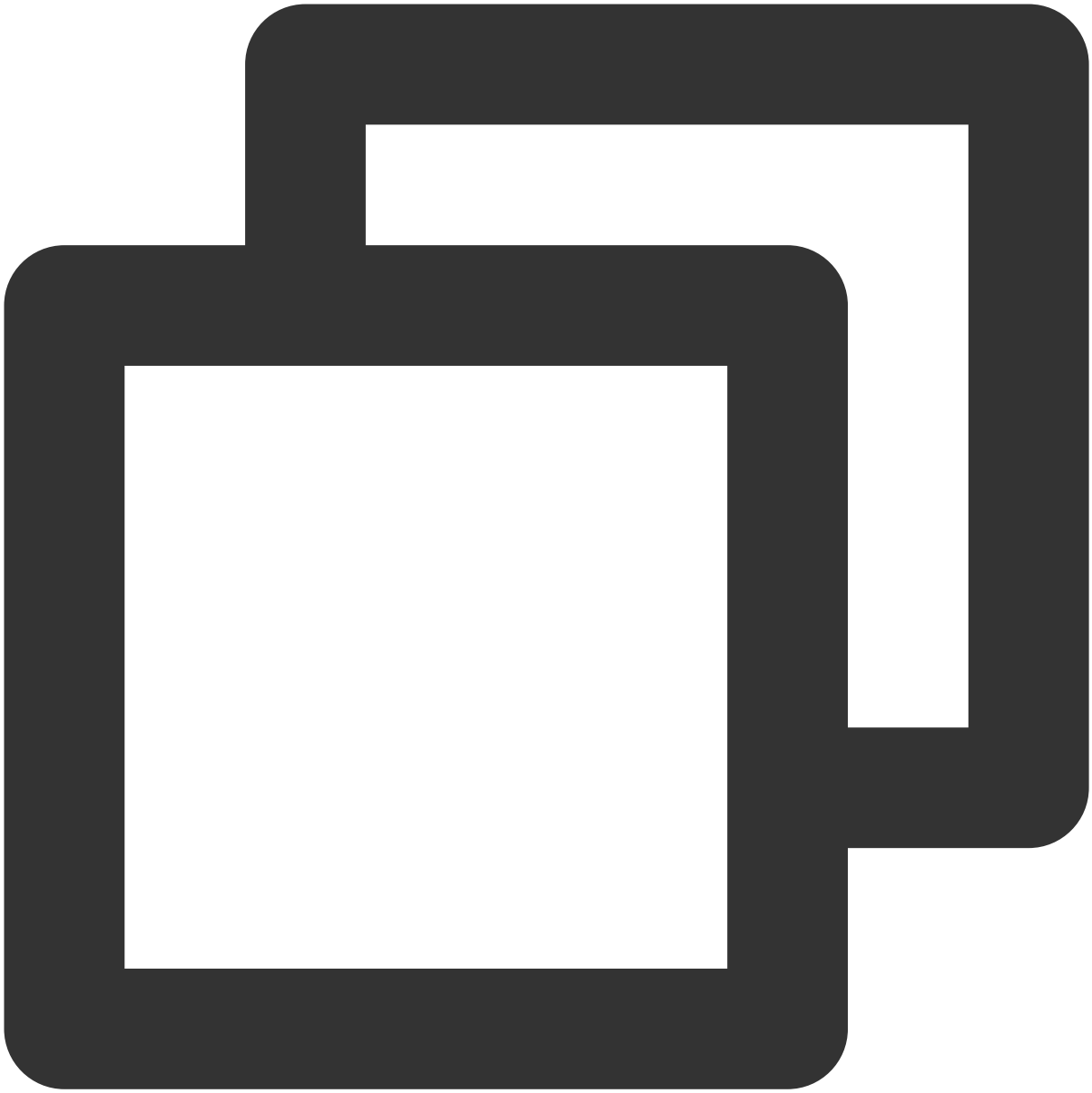
ソリューション

1. 次のコマンドを実行し、サーバーのディスク領域の使用率を確認します。



```
df -h
```

ディスクに十分な空き容量がない場合、ファイルをアップロードできないため、ディスク上の大容量のファイルを削除することをお勧めします。
ディスク容量が十分な場合は、次のステップを実行してください。
2. 次のコマンドを実行し、FTP ディレクトリへの書き込み権限があるかどうかを確認します。

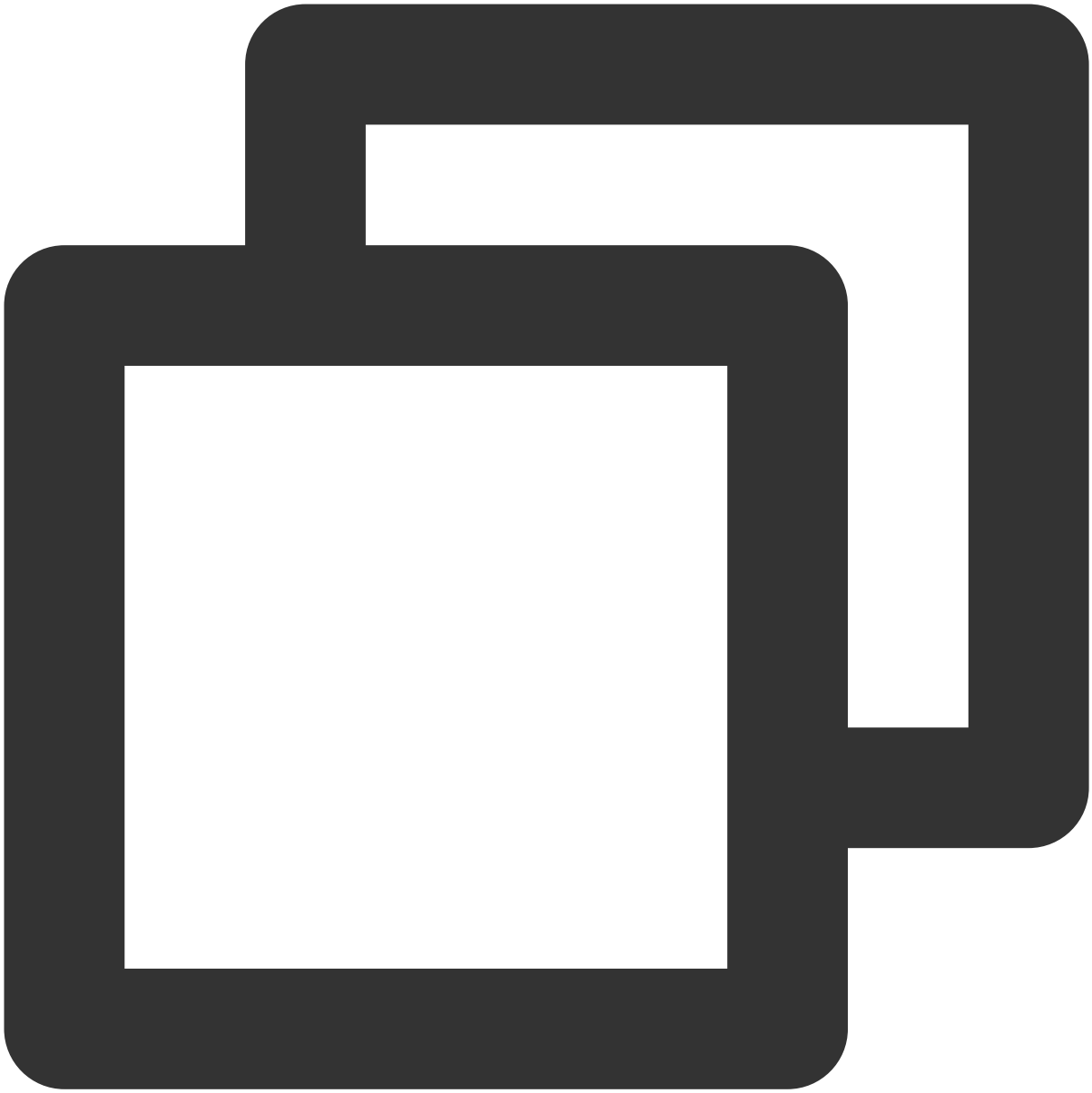


```
ls -l /home/test
# /home/testはFTP ディレクトリです。実際のFTPディレクトリに変更してください。
```

戻された結果に「w」がない場合は、当該ユーザーに書き込み権限がないことを示し、次のステップを実行してください。

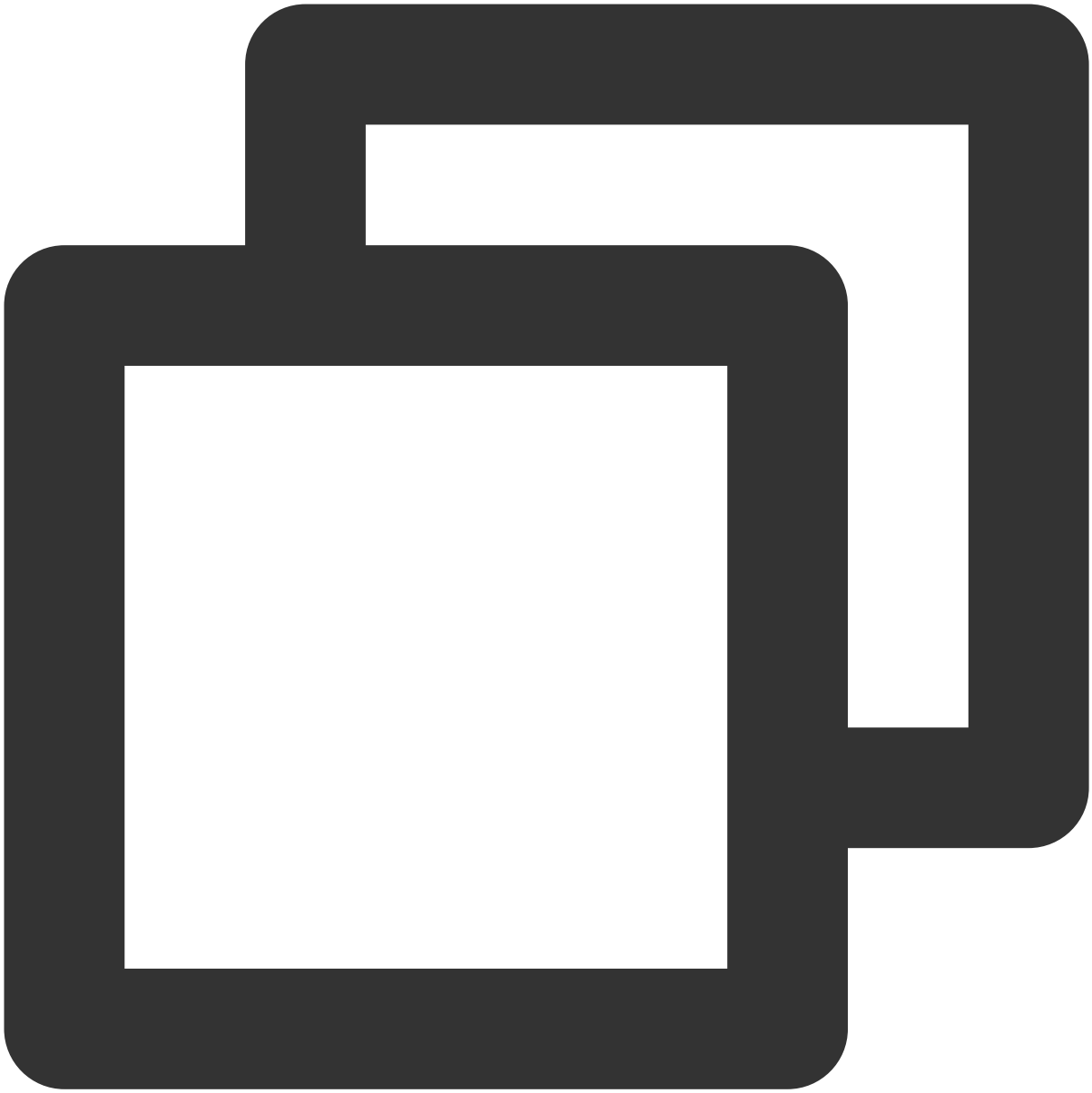
返された結果の中に `w` があれば、チケットを提出 してフィードバックしてください。

3. 次のコマンドを実行し、FTPディレクトリへの書き込み権限を付与します。



```
chmod +w /home/test
# /home/testはFTP ディレクトリです。実際のFTPディレクトリに変更してください。
```

4. 次のコマンドを実行し、書き込み権限が正常に設定されたかどうかを再度確認します。



```
ls -l /home/test
# /home/testはFTP ディレクトリです。実際のFTPディレクトリに変更してください。
```

Windows CVMでFTPサービスを構築する

最終更新日：：2022-05-07 15:41:38

概要

このドキュメントでは、IISを使用してWindows CVMインスタンスにFTPサイトを構築する方法について説明します。

ソフトウェアバージョン

このドキュメントでは、構築したFTPサービスのソフトウェアバージョンは次のとおりです。
Windows OS、このドキュメントでは Windows Server 2012 を例として説明します。
IIS：Web サーバー、このドキュメントでは IIS 8.5 を例として説明します。

操作手順

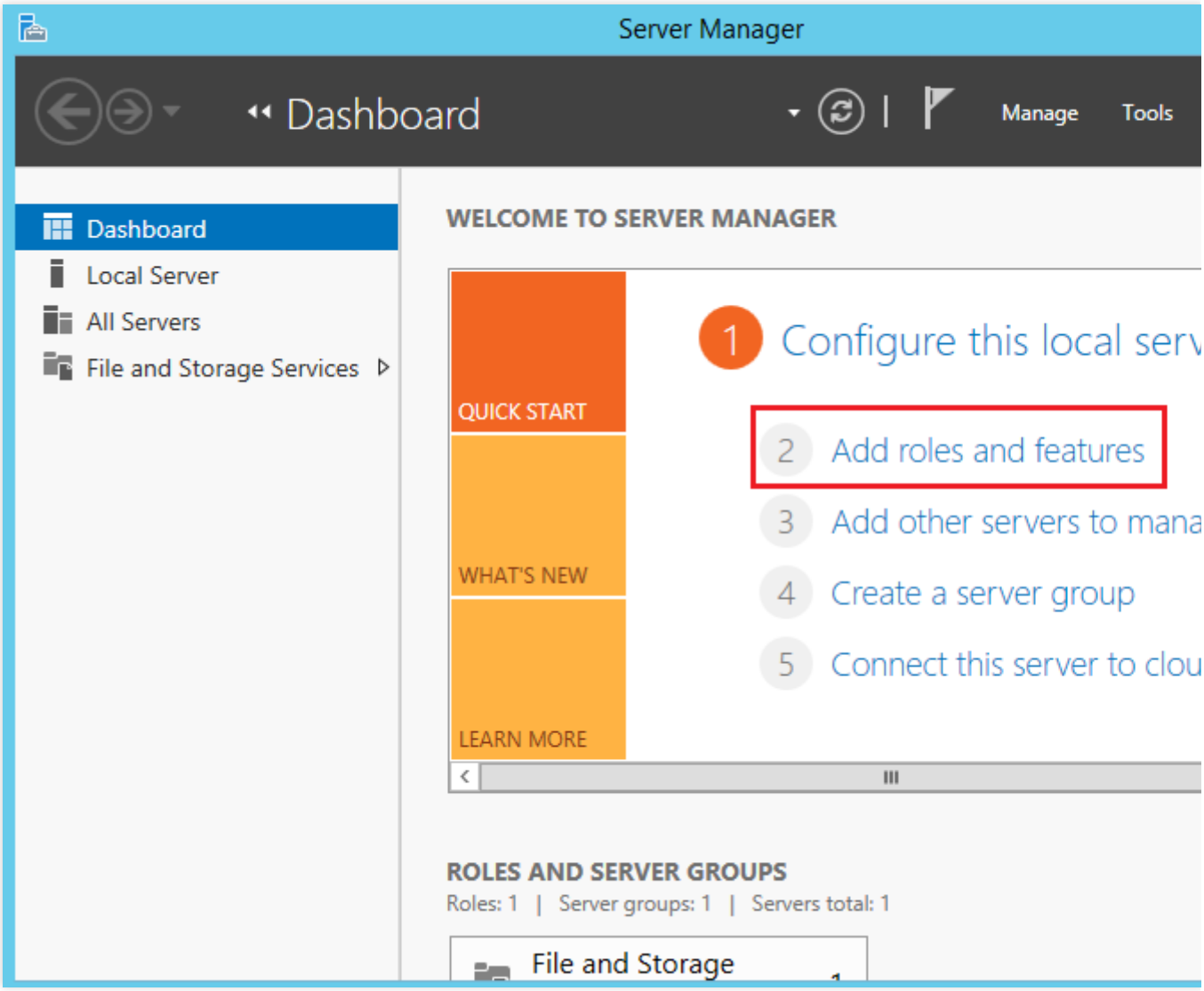
手順１：CVMにログインする

RDP ファイルを使用してWindows インスタンスにログインする（推奨）。
リモートデスクトップを使用してWindows インスタンスにログインする。

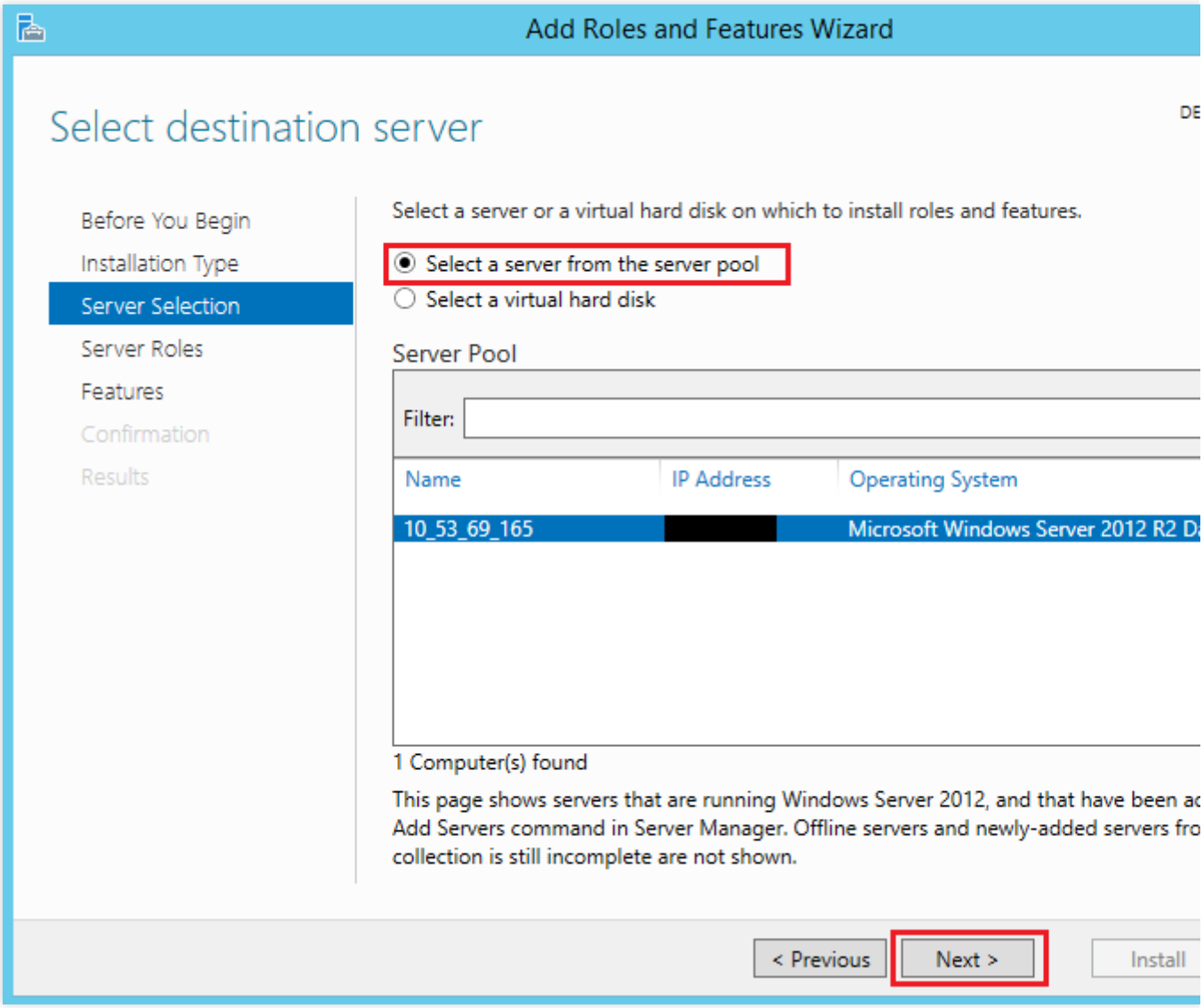
手順2：IIS にFTPサービスをインストールする

1. OSインターフェースで、

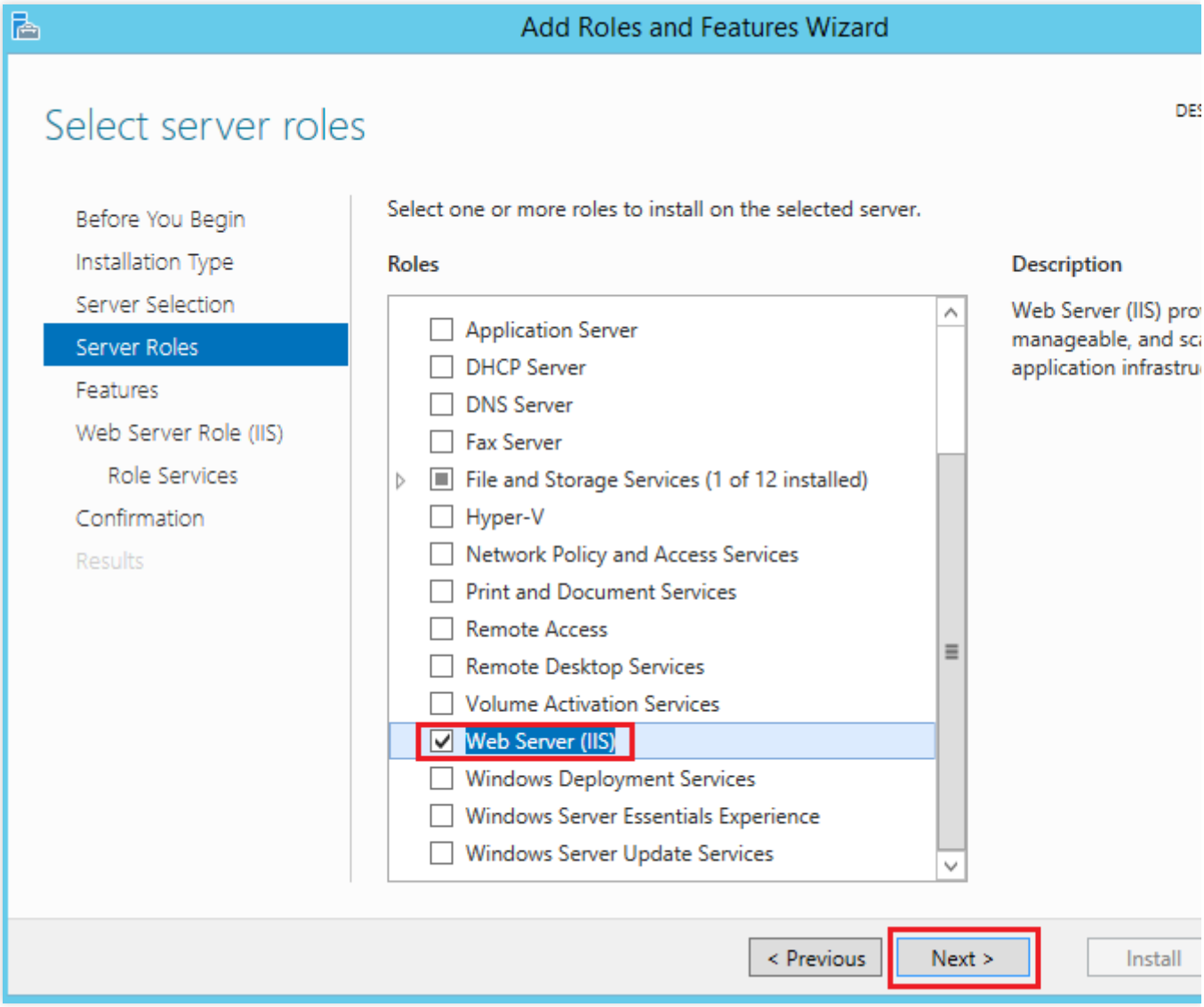
をクリックして、サーバーマネージャーを開きます。
2. 「サーバーマネージャー」画面で、次の図に示すように、**役割と機能の追加**をクリックします。



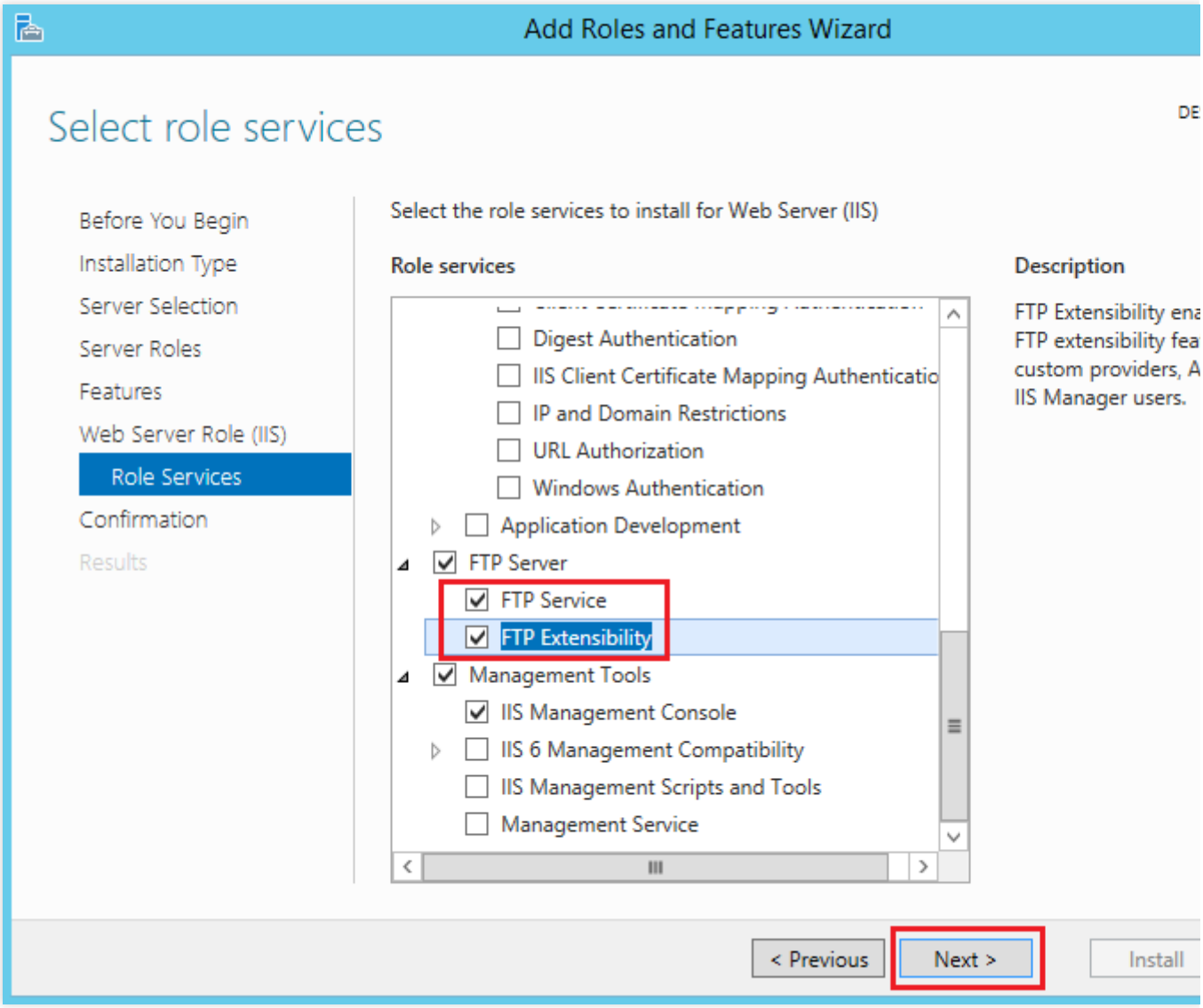
3. 「役割と機能の追加ウィザード」で、**次へ**をクリックして、「インストールの種類の選択」画面に入ります。
4. 「インストールの種類の選択」画面で、**役割ベースまたは機能ベースのインストール**を選択して、**次へ**をクリックします。
5. 「対象サーバーの選択」画面で、デフォルト設定を保持して、**次へ**をクリックします。次の図に示すように：



6. 「サーバーの役割の選択」画面で、**Web サーバー(IIS)**をチェックし、ポップアップウィンドウで**機能の追加**をクリックします。次の図に示すように：



7. **次へ**を連続して3回押す、「役割サービスの選択」画面に入ります。
8. 「役割サービスの選択」画面で、**FTP サービス**と**FTP拡張**をチェックし、**次へ**をクリックします。次の図に示すように：



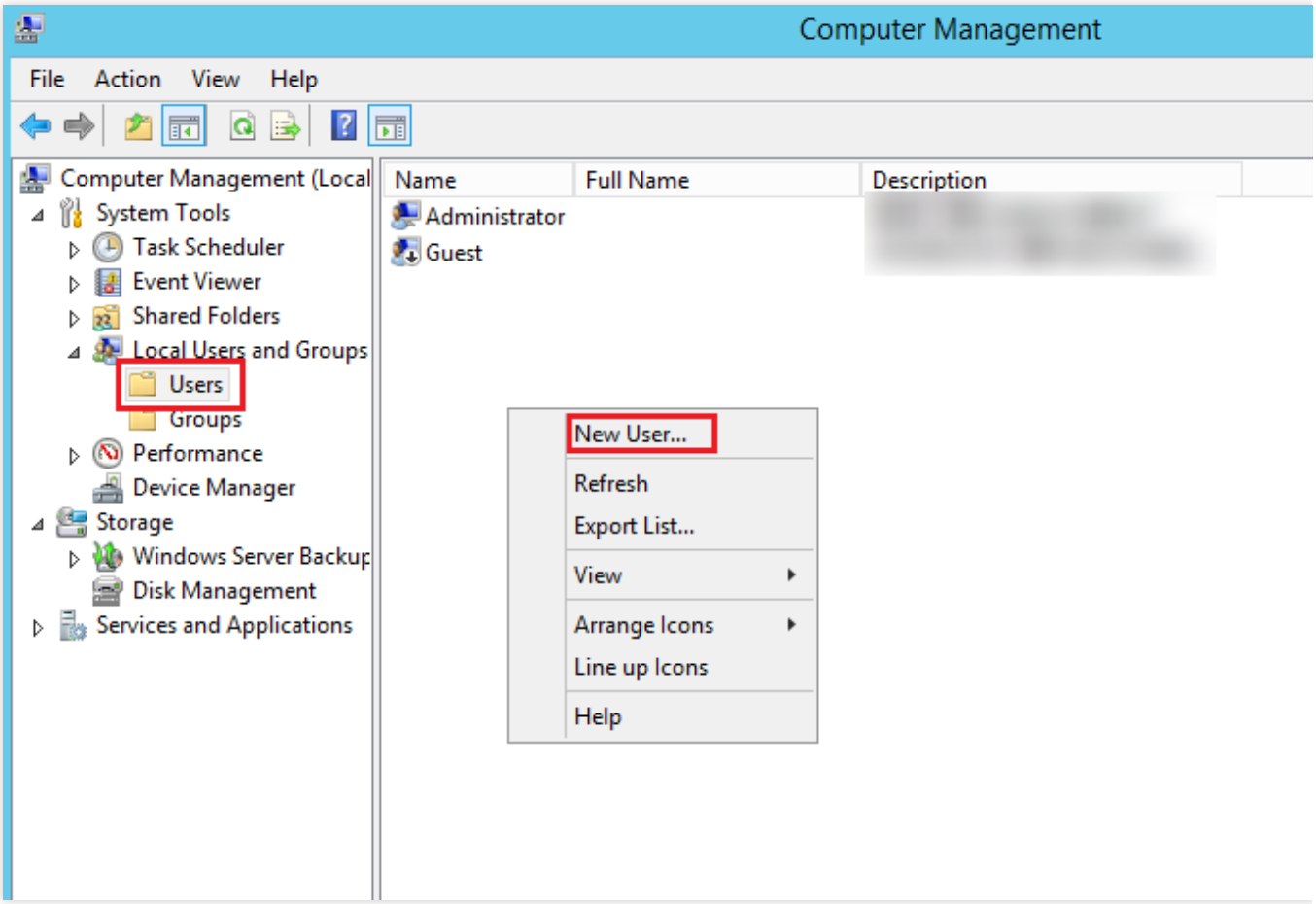
9. **インストール**をクリックして、 FTP サービスのインストールを開始します。
10. インストールが完了したら、**閉じる**をクリックします。

手順3： FTP ユーザー名とパスワードを作成する

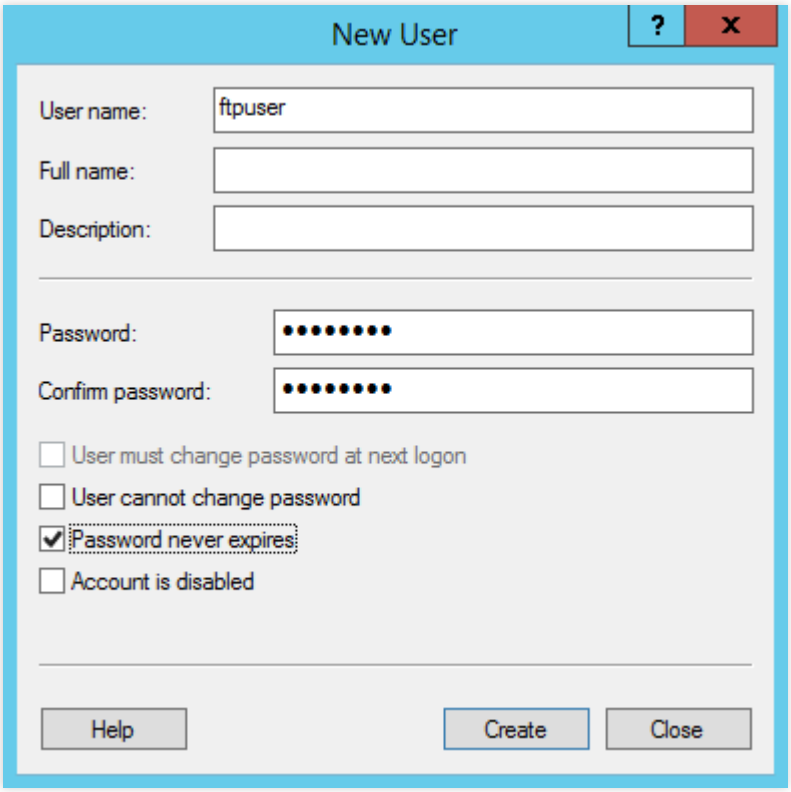
説明：

以下の手順に従ってFTPユーザー名とパスワードを設定してください。匿名ユーザーとしてFTP サービスにアクセスする必要がある場合は、この手順をスキップできます。

1. 「サーバーマネージャー」ウィンドウで、右上隅のナビゲーションバーにある**管理ツール > コンピューターの管理**を選択して、コンピューター管理ウィンドウを開きます。
2. 「コンピューターの管理」画面で、**システムツール > ローカルユーザーとグループ > ユーザー** を選択します。
3. **ユーザー**画面の右側で、空白スペースを右クリックして、**新しいユーザー**を選択します。次の図に示すように：



4. 「新しいユーザー」画面で、以下のプロンプトに従ってユーザー名とパスワードを設定し、**作成**をクリックします。次の図に示すように：



主なパラメータは次の通り：
ユーザー名：カスタム。このドキュメントでは、 `ftpuser` を例として説明します。
パスワードと確認パスワード：カスタム。パスワードには大文字と小文字、数字を全て含める必要があります。このドキュメントでは、 `tf7295TFY` を例として説明します。
ユーザは次回ログオン時にパスワードの変更が必要のチェックを外し、**パスワードを無制限にする**にチェックを入れます。
実際のニーズに応じてチェックしてください。このドキュメントでは**パスワードを無制限にする**ことを例として説明します。
5. **閉じる**をクリックし、「新しいユーザー」ウィンドウを閉じた後に、リストに作成された `ftpuser` ユーザーを確認できます。

手順4：共有フォルダーのアクセス権限を設定する

説明：
ここでは `C:\\test` ファイルを例として、FTPサイトの共有フォルダを設定します。このフォルダには共有する必要のあるファイル `test.txt` が含まれています。この例を参照して、新しいフォルダ `C:\\test` とファイル `test.txt` を作成することができます。また実際のニーズに応じて、他のフォルダをFTPサイトの共有フォルダとして設定することもできます。
1. OSインターフェースで、

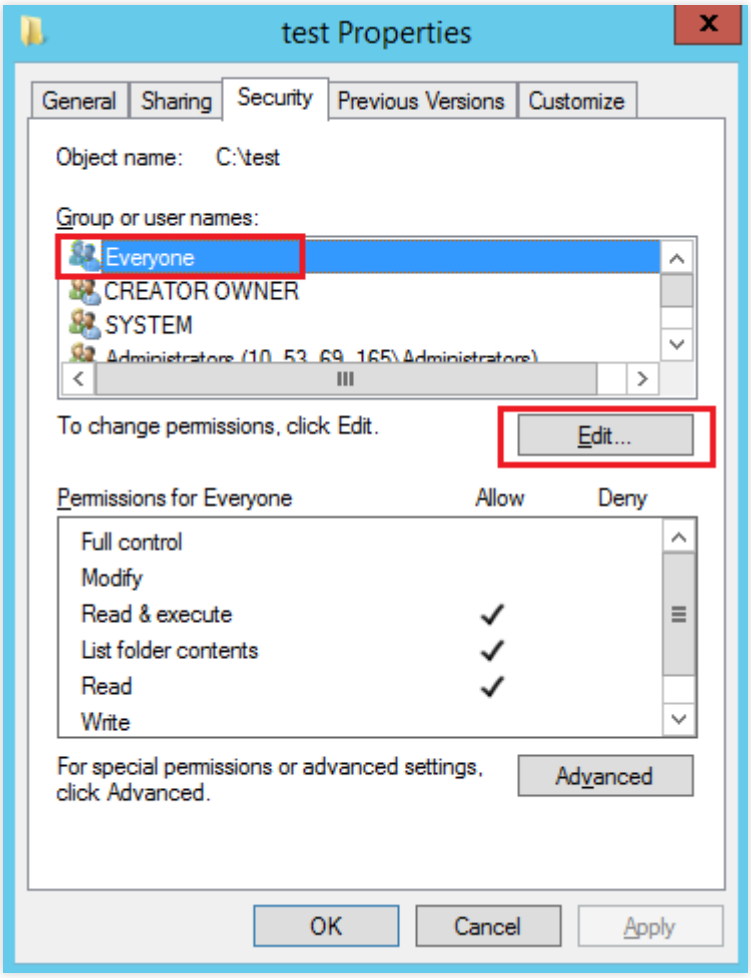

をクリックして、「PC」を開きます。

2. Cドライブで、 `test` フォルダーを選択して右クリックし、**プロパティ**を選択します。

3. 「test プロパティ」ウィンドウで、**セキュリティ**タグを選択します。

4. `Everyone` ユーザーを選択し、**編集**をクリックします。次の図に示すように：

「グループまたはユーザー名」に `Everyone` が含まれていない場合は、Everyone Userの追加 を参考してユーザーを追加してください。

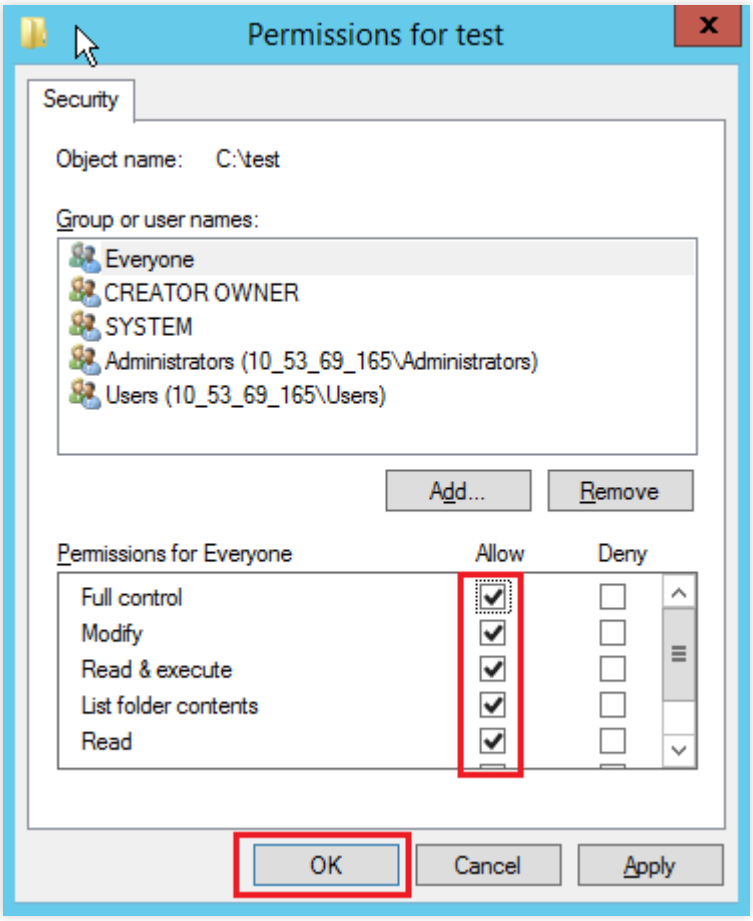


5.

「test の権限」画面で、

必要に応じて `Everyone` ユーザーの権限を設定し、【OK】をクリックします。次の図に示すように：

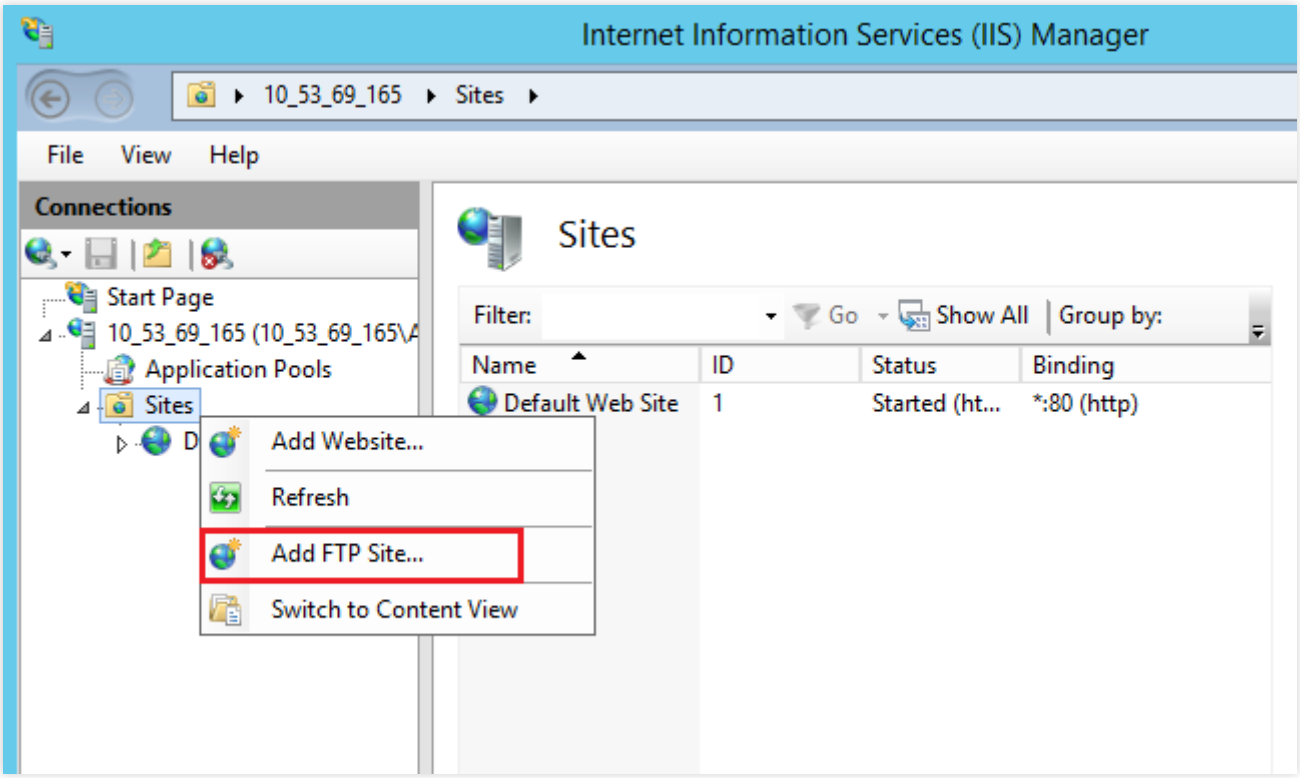
このドキュメントでは、 `Everyone` ユーザーにすべての権限を付与することを例として説明します。



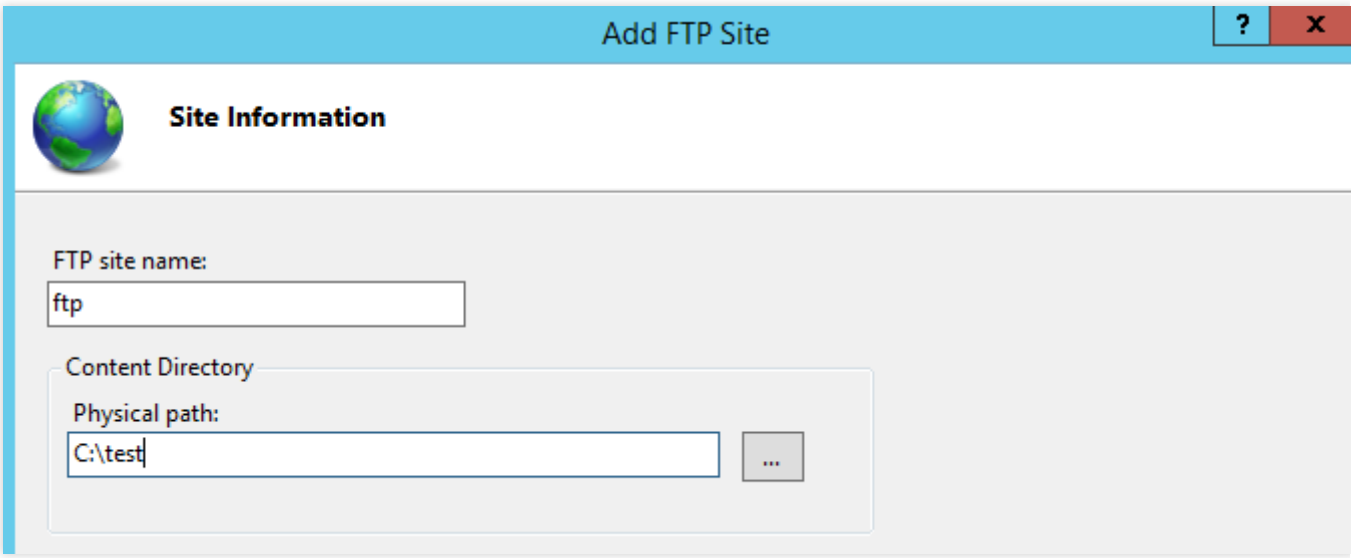
6. 「test プロパティ」ウィンドウで、【OK】をクリックして設定を完了します。

手順5： FTPサイトを追加する

1. 「サーバーマネージャー」ウィンドウで、右上隅のナビゲーションバーにある**管理ツール > インターネット インフォメーション サービス (IIS) マネージャ**を選択します。
2. 表示される「インターネット インフォメーション サービス (IIS) マネージャ」ウィンドウで、左側ナビゲーションバーのサーバー名を展開し、**ウェブサイト**を右クリックして、**FTP サイトの追加**を選択します。次の図に示すように：



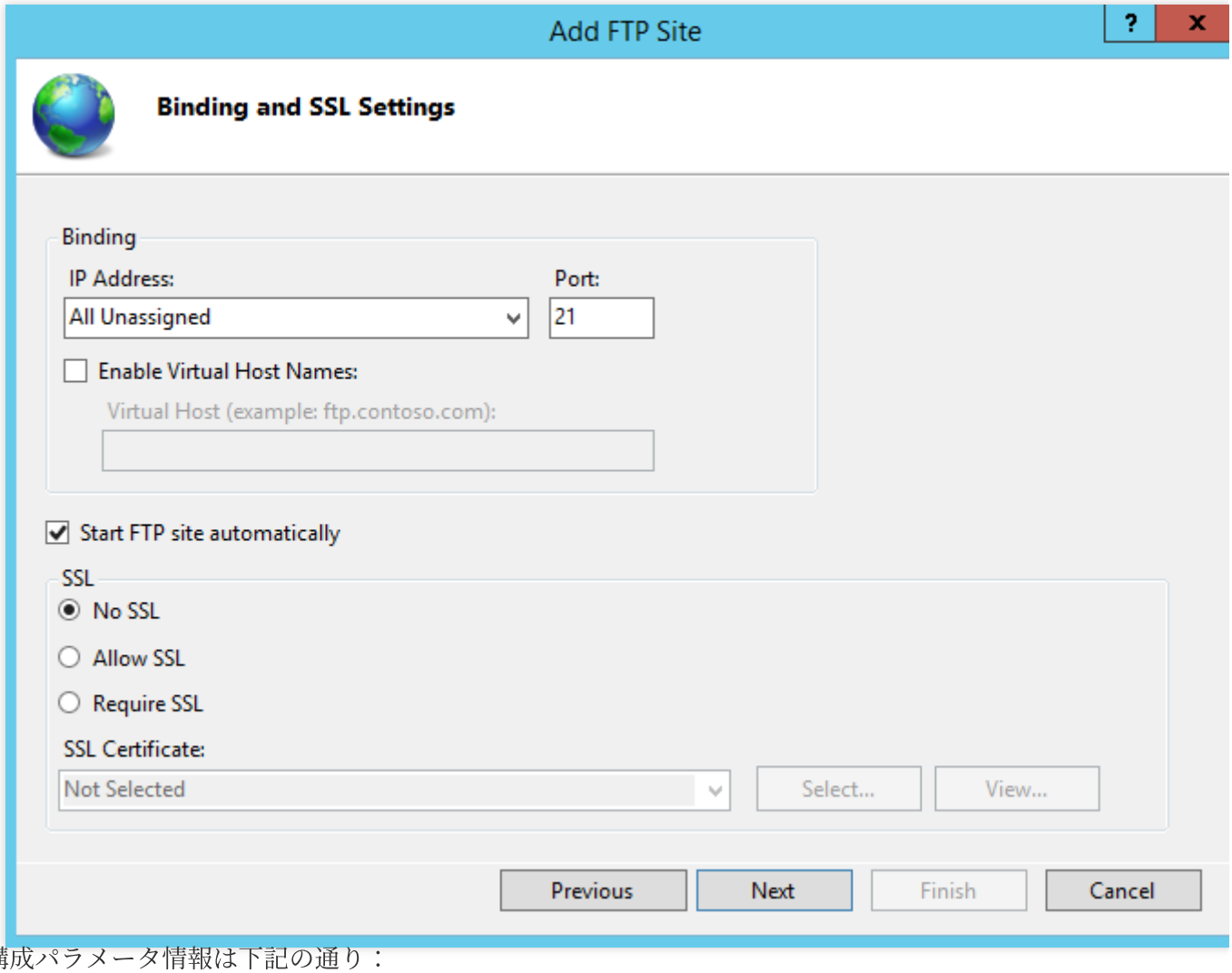
3. 「サイト情報」画面で、以下の情報を参考して設定し、**次へ**をクリックします。次の図に示すように：



FTP サイト名：FTP サイト名を記入し、このドキュメントでは `ftp` を例としています。

物理パス：権限が設定された共有フォルダーのパスを選択し、このドキュメントでは、`C:\\test` を例としています。

4. 「バインドと SSL の設定」画面で、以下の情報を参考して設定し、**次へ**をクリックします。次の図に示すように：



主な構成パラメータ情報は下記の通り：

バインド：IP アドレスのデフォルト選択は**すべて未割り当て**で、デフォルトのポート番号は21（FTP のデフォルトのポート番号）であり、カスタムポート番号を設定できます。

SSL：必要に応じて選択してください、このドキュメントでは**SSL 無し**を例としています。

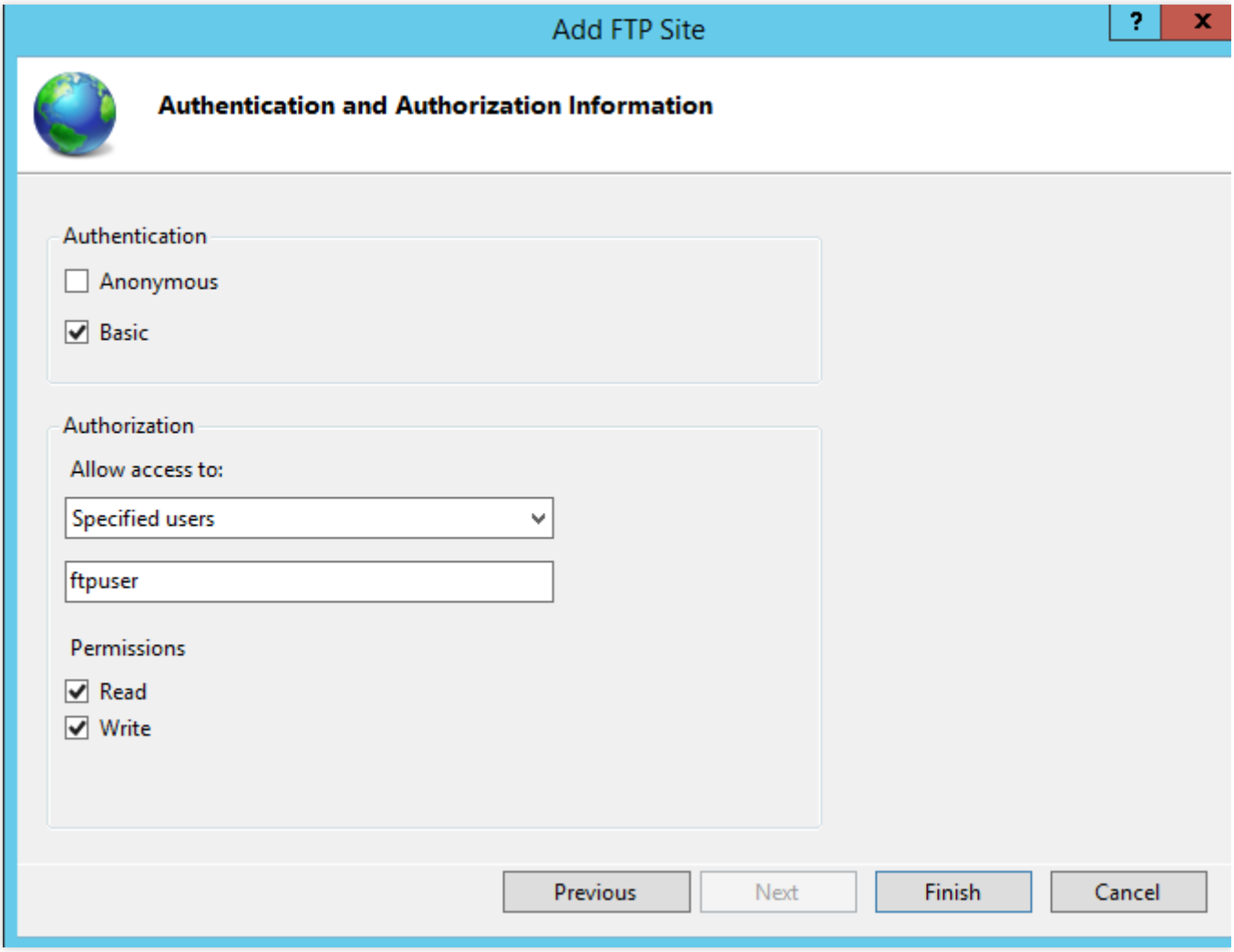
SSL 無し：SSL暗号化は必要ありません。

SSL の許可：FTPサーバーによるクライアントとの非SSLおよびSSL接続のサポートを許可します。

SSL が必要： FTPサーバーとクライアント間の通信にはSSL暗号化が必要です。

許可あるいは**必要**を選択した場合、「SSL証明書」で既存のSSL証明書を選択するか、サーバー証明書の作成 を参考してSSL証明書を作成することもできます。

5. 「認証および承認の情報」画面で、以下の情報を参考して設定し、**次へ**をクリックします。次の図に示すように：



認証：認証方法を選択します。このドキュメントでは、**基本**を例として説明します。
匿名：匿名またはFTPユーザー名を提供するユーザーがコンテンツにアクセスできるようにします。
基本：ユーザーは、コンテンツにアクセスするために有効なユーザー名とパスワードを提供する必要があります。基本モードでは、暗号化されていないパスワードをネットワーク経由で送信するため、クライアントと FTP サーバー間の接続が安全であることが分っている場合（たとえば、Secure Sockets Layer を使用する場合）にのみ、この認証方法を使用します。
認可：「アクセス許可」ドロップダウンリストから方式を選択して、このドキュメントでは、指定されたユーザー `ftpuser` を例として説明します。
- **すべてのユーザー**： 匿名ユーザーまたは識別されたユーザーに関係なく、すべてのユーザーがコンテンツにアクセスできます。
- **匿名ユーザー**：匿名ユーザーはコンテンツにアクセスできます。
- **指定されたロール或はユーザーグループ**：特定のロール或はユーザーグループのメンバーのみがコンテンツにアクセスできます。このオプションを選択する場合は、ロールまたはユーザーグループを指定する必要があります。
- **指定されたユーザー**：指定されたユーザーのみがコンテンツにアクセスできます。このオプションを選択する場合は、ユーザー名を指定する必要があります。

権限：必要に応じて権限を設定してください。本文では**読み取り**と**書き込み**権限の設定を例として説明します。

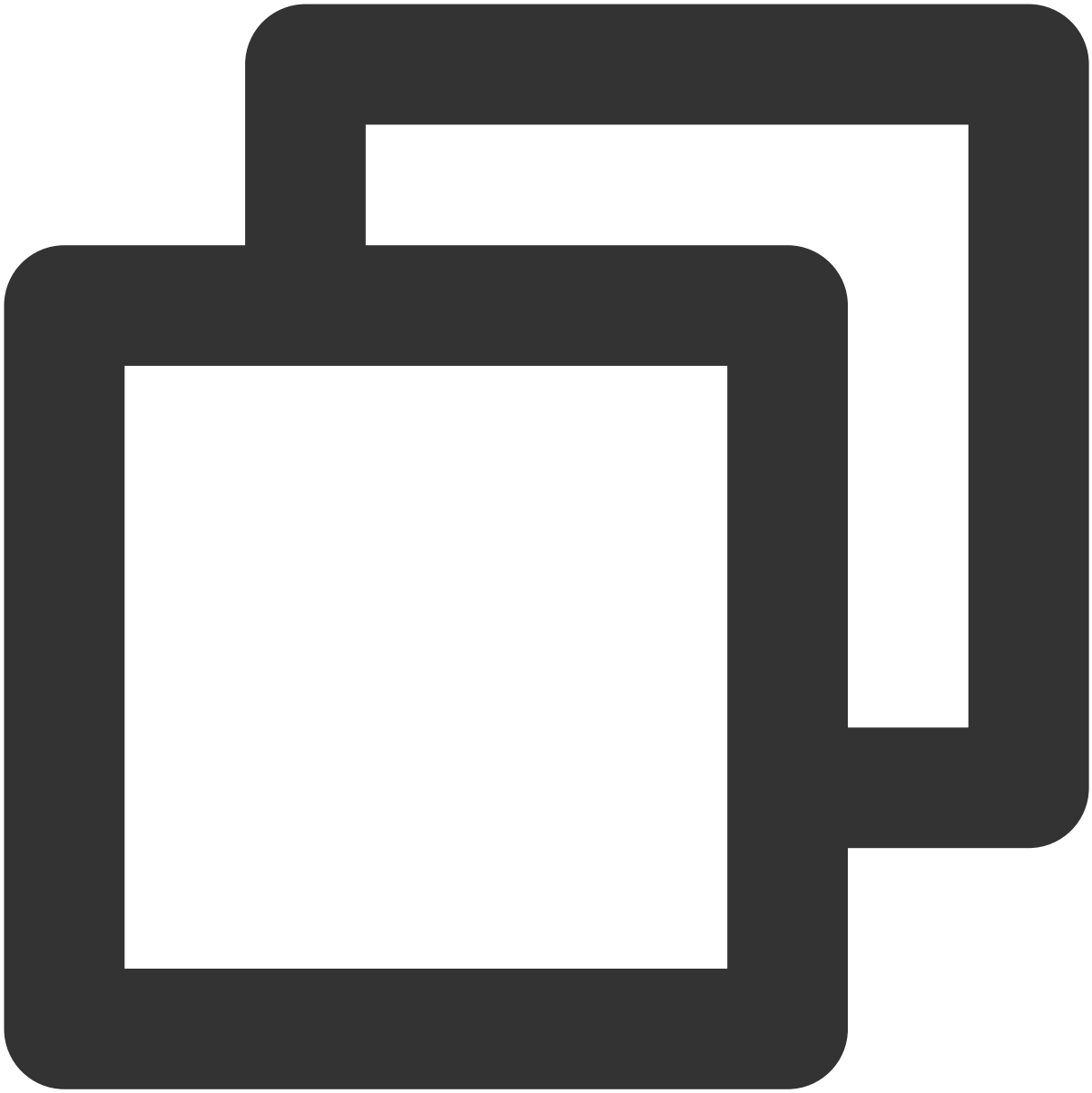
読み取り：許可されたユーザーがディレクトリからコンテンツを読み取ることができます。
書き込み：許可されたユーザーがディレクトリに書き込むことができます。
6. **完了**をクリックして、 FTP サイトを作成できます。

手順6：セキュリティグループとファイアウォールを設定する

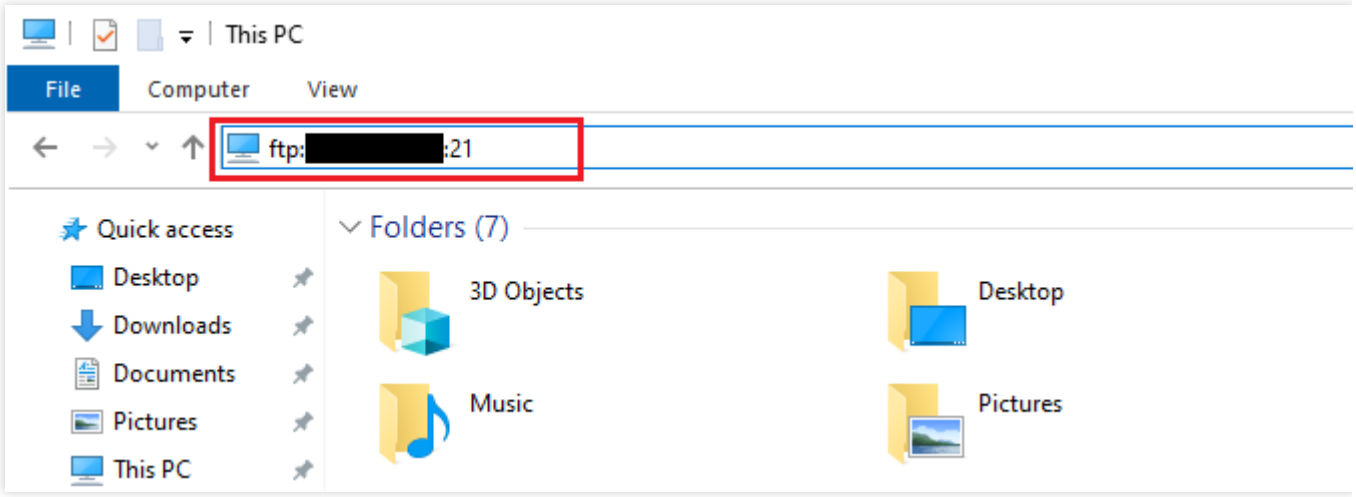
1. FTPサイトの構築が完了したら、FTPアクセスモードに対応して、FTPサイトを追加するときに、ポートをバインドするためのインバウンドルールを許可してください。
アクティブモード：ポート20と21を開きます。
パッシブモード：ポート21および 1024 ~ 65535（たとえば、ポート5000~6000）の間のポートを開きます。
対応するインバウンドルールを追加する方法については、セキュリティグループルールの追加 をご参照ください。
2. （オプション）Microsoft公式ドキュメント を参考して FTP サイトのファイアウォールサポートを設定することにより、 FTP サーバーはファイアウォールからのパッシブ接続を受け入れることができるようにします。

手順7：FTP サイトをテストする

FTP クライアントソフトウェア、ブラウザー或はファイルエクスプローラーなどのツールを利用してFTP サービスをテストできます。本文ではクライアント側のファイルエクスプローラーを例として説明します。
1. 実際の使用状況に応じて、 IE ブラウザを設定してください：
FTPサイトファイアウォールが構成されています（アクティブモード）：
クライアントの IEブラウザを開き、**ツール** > **インターネットオプション** > **詳細設定**を選択し、**パッシブ FTP(ファイアウォールおよびDSLモデム互換用)を使用する**のチェックを外して、【OK】ボタンをクリックします。
FTPサイトファイアウォールが構成されていません（パッシブモード）：
1.1.1 **FTP サーバー**の IE ブラウザを開き、**ツール** > **インターネットオプション** > **詳細設定** を選択し、**パッシブ FTP(ファイアウォールおよびDSLモデム互換用)を使用する**のチェックを外して、【OK】ボタンをクリックします。
1.1.2 **クライアント**の IEブラウザを開き、**ツール** > **インターネットオプション** > **詳細設定**を選択し、**パッシブ FTP(ファイアウォールおよびDSLモデム互換用)を使用する**のチェックを外して、【OK】ボタンをクリックします。
2. 次の図に示すように、クライアントでWindowsエクスプローラーを開き、アドレスボックスに次のアドレスを入力して、Enterキーを押します。



```
ftp://CVMパブリックIP:21
```

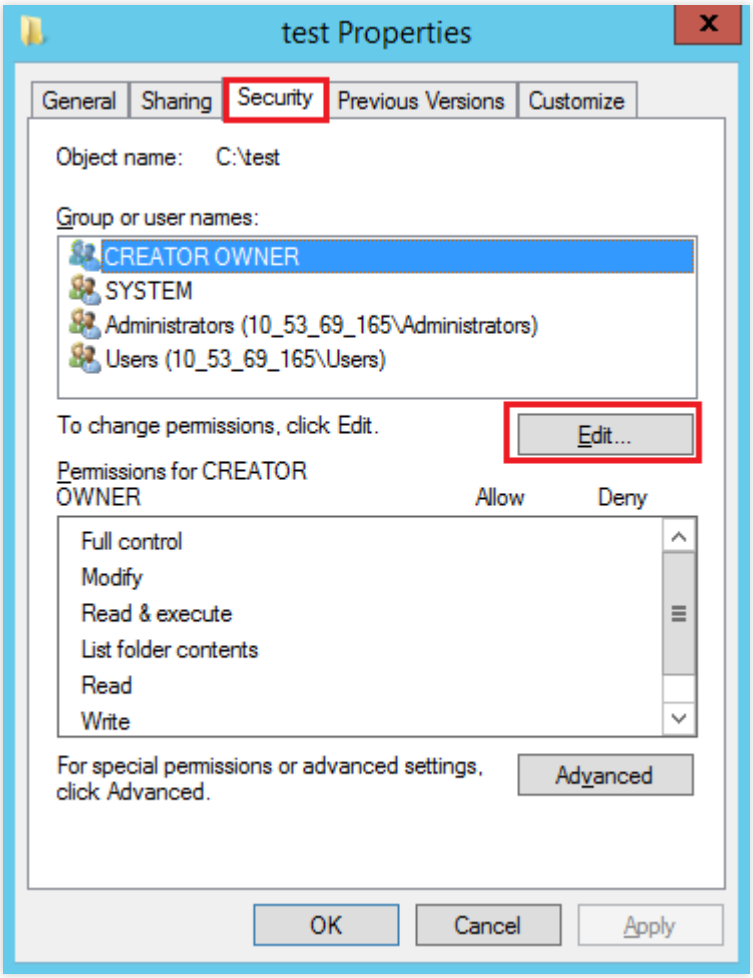


3. ポップアップされた「ログイン」ウィンドウで、 FTP ユーザー名とパスワードの作成 で設定されたユーザー名とパスワードを入力します。
このドキュメントで使用されるユーザー名は `ftpuser` で、パスワードは `tf7295TFY` です。
4. ログインが成功したら、ファイルをアップロード及びダウンロードできます。

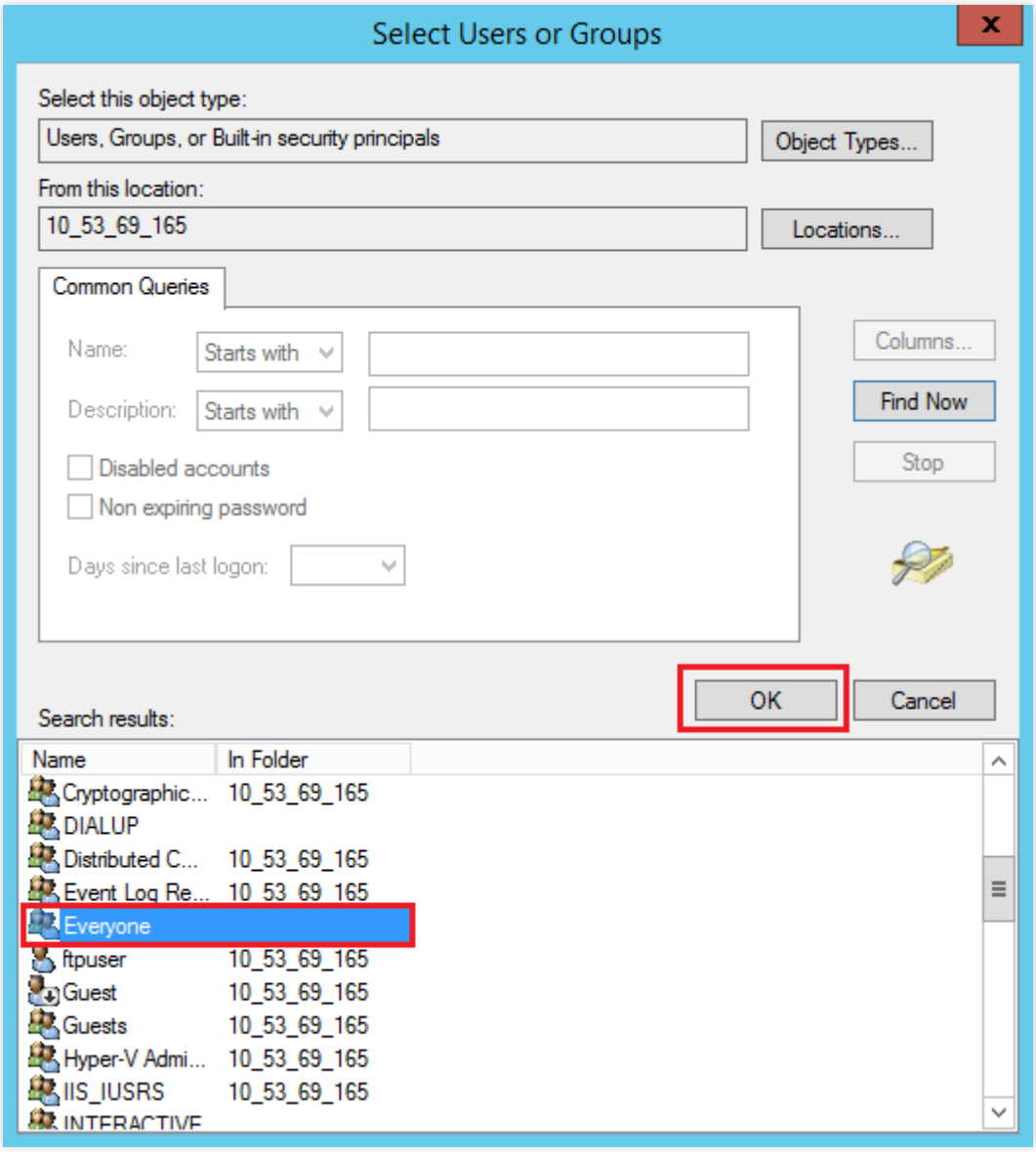
付録

Everyone ユーザーを追加する

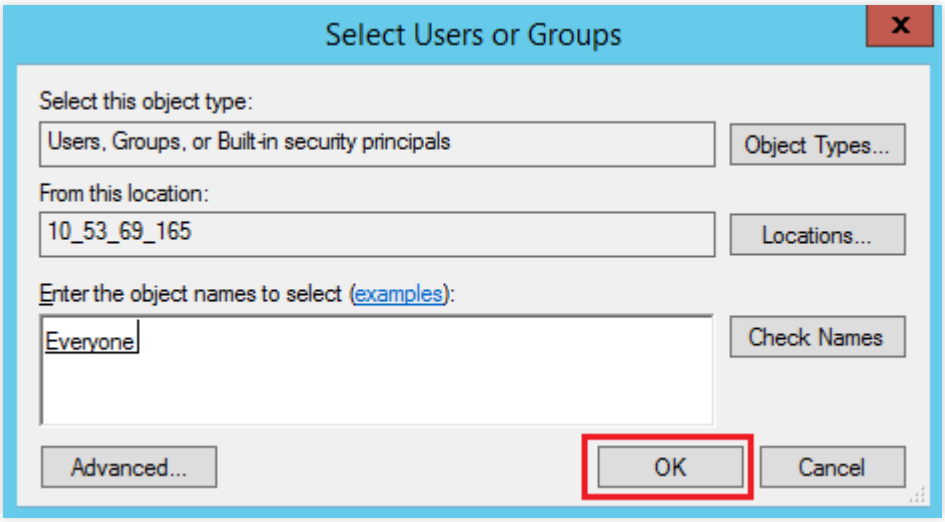
1. 「test プロパティ」ウィンドウで、**セキュリティ**タグを選択し、**編集**をクリックします。次の図に示すように：



2. 「権限テスト」画面で、**追加**をクリックします。
3. 「ユーザーまたはグループの選択」画面で、**詳細設定**をクリックします。
4. 表示される「ユーザーまたはグループの選択」画面で、**今すぐ検索**をクリックします。
5. 検索結果に `Everyone` を選択し、【OK】をクリックします。次の図に示すように：



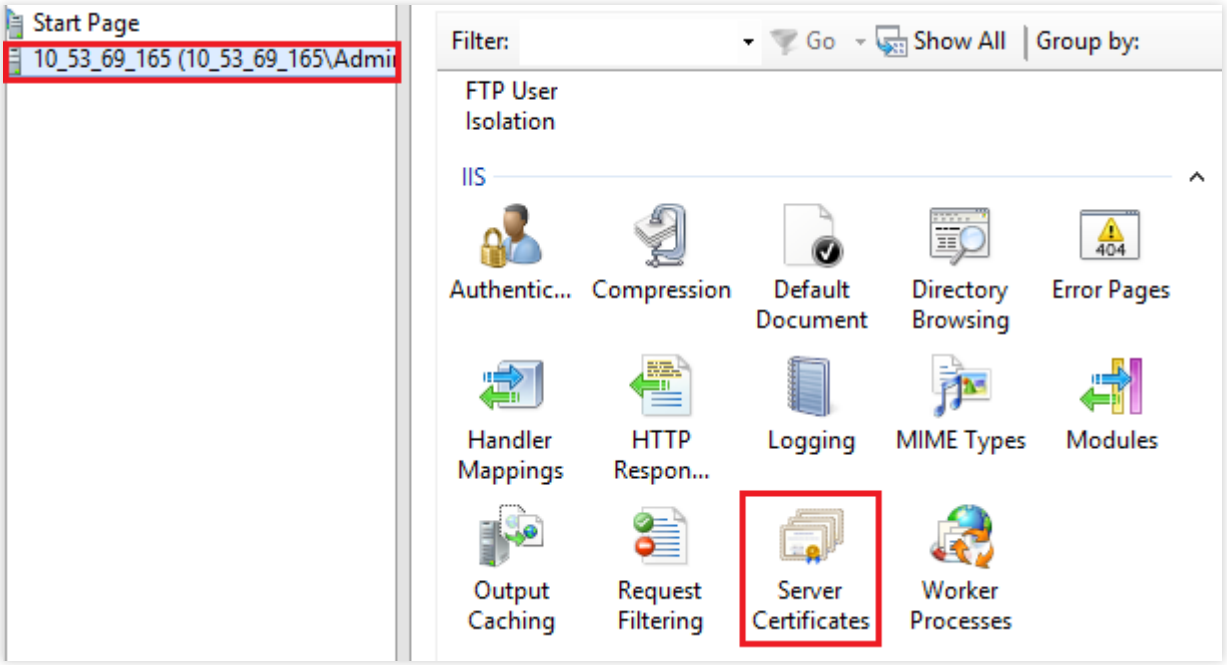
6. 「ユーザーまたはグループの選択」画面で、【OK】をクリックしてEveryoneユーザー追加できます。次の図に示すように：



手順5 に進み、 `Everyone` ユーザーの権限を設定します。

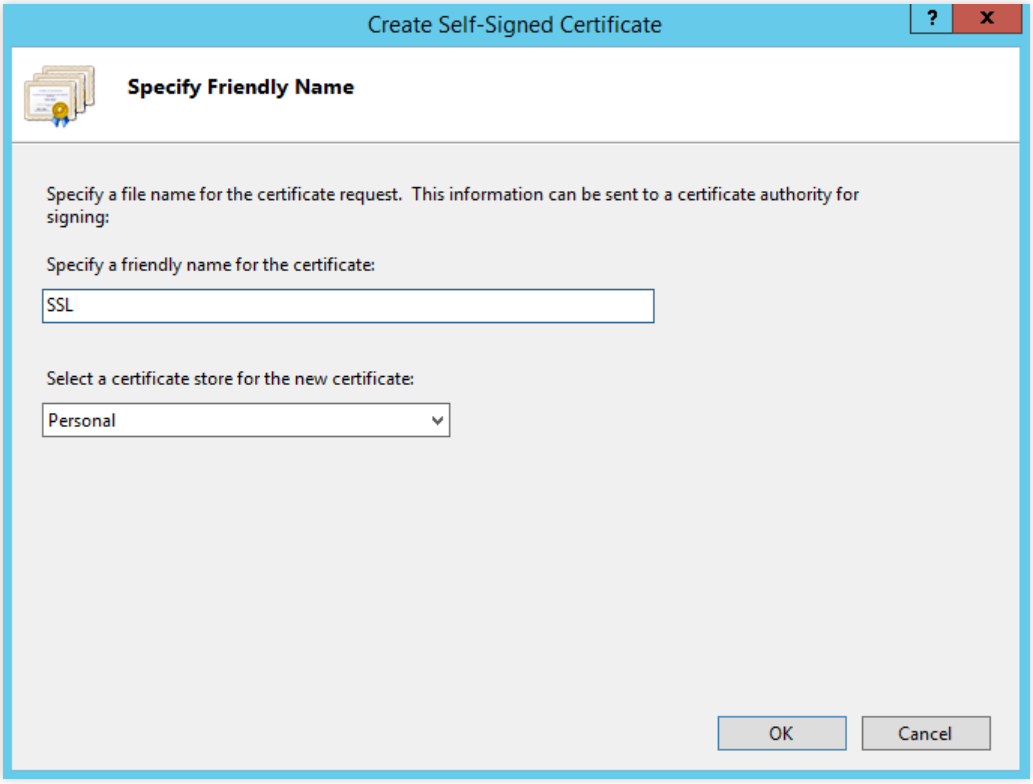
サーバー証明書の作成

1. 「サーバーマネージャー」ウィンドウで、右上隅のナビゲーションバーにある**管理ツール > インターネット インフォメーションサービス(IIS) マネージャ**を選択します。
2. 表示される「インターネット インフォメーションサービス (IIS) マネージャ」ウィンドウで、左側のナビゲーションバーでサーバーを選択し、右側の画面にある**サーバー証明書**をダブルクリックします。次の図に示すように：



3. 画面右側の**自己署名証明書の作成**を選択します。
4. 表示される「自己署名証明書の作成」ウィンドウで、証明書名とストレージタイプを設定します。次の図に示すように：

このドキュメントでは個人用ストレージタイプのSSL証明書の作成を例として説明します。



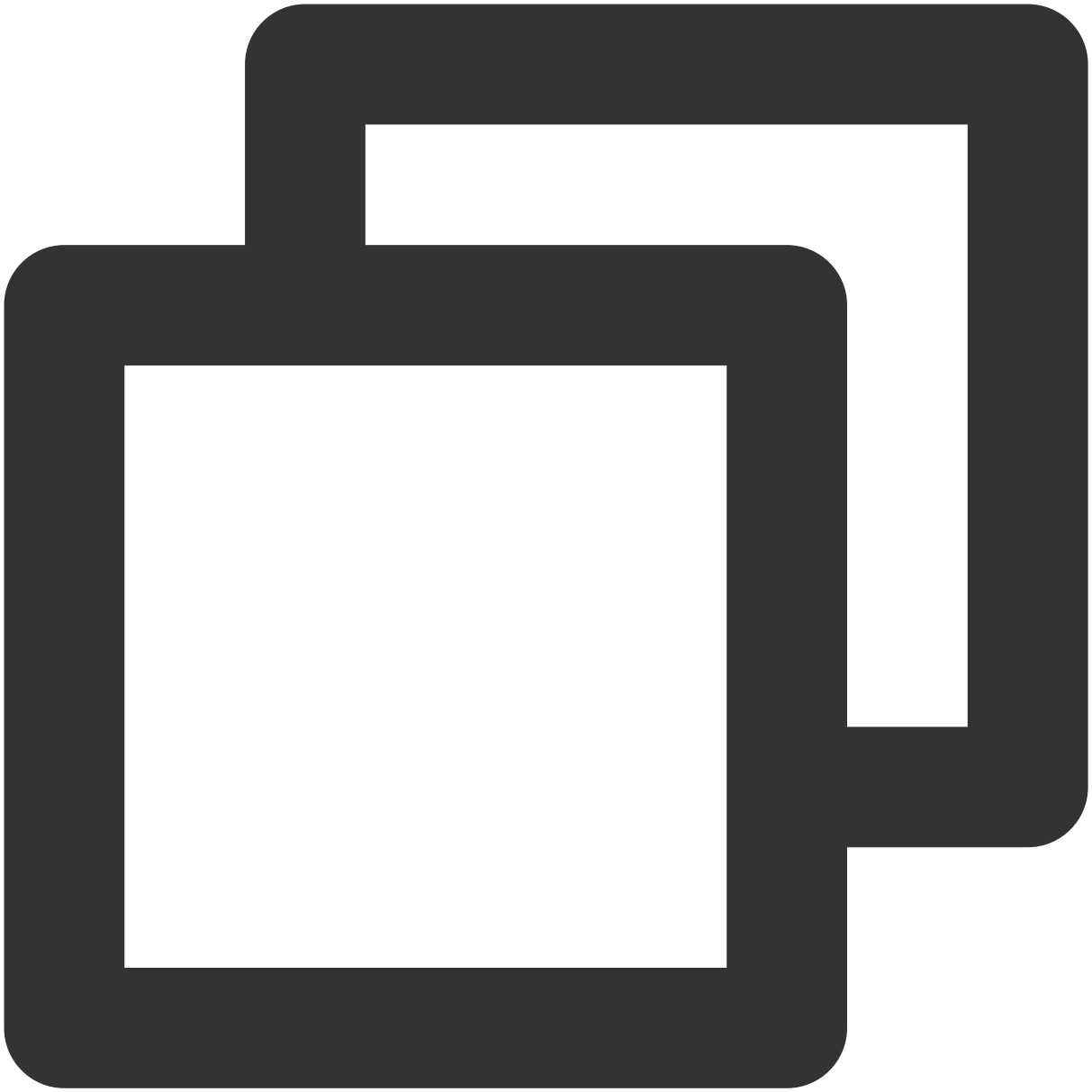
5. 【OK】をクリックして、サーバー証明書を作成します。

NTP サービス
NTPサービスの概要

最終更新日：：2022-05-07 16:03:47

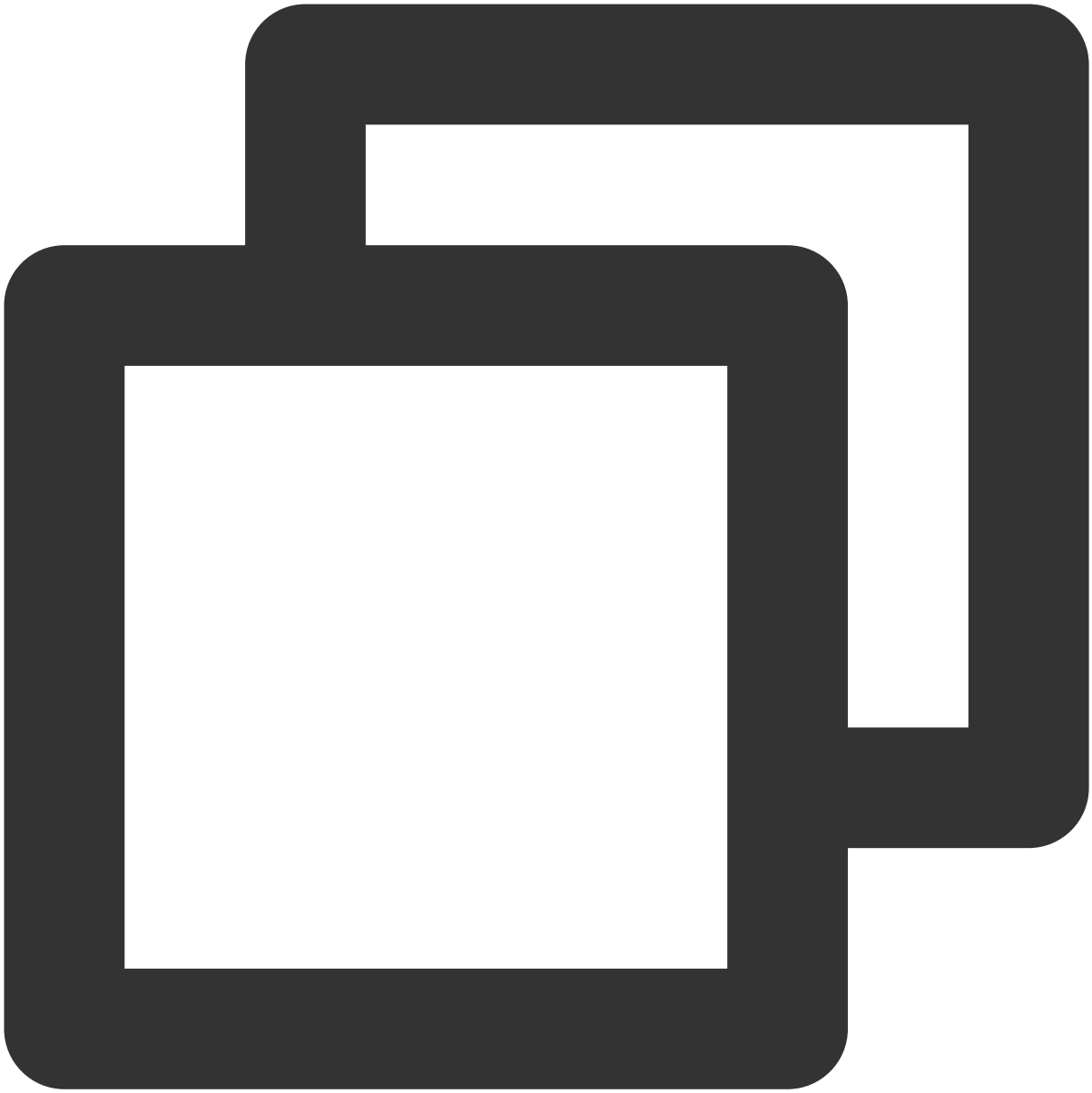
ネットワークタイムプロトコル（Network Time Protocol，NTP）は、ネットワーク内の各コンピューターの時刻を同期するために使用されるプロトコルです。その目的は、コンピューターの時計を協定世界時UTCに同期させることです。
Tencent Cloudは、プライベートネットワークデバイス用のプライベートネットワークNTPサーバーを提供します。Tencent Cloud以外のデバイスの場合、Tencent Cloudが提供するパブリックネットワークNTPサーバーを使用できます。

プライベートネットワーク NTP サーバー



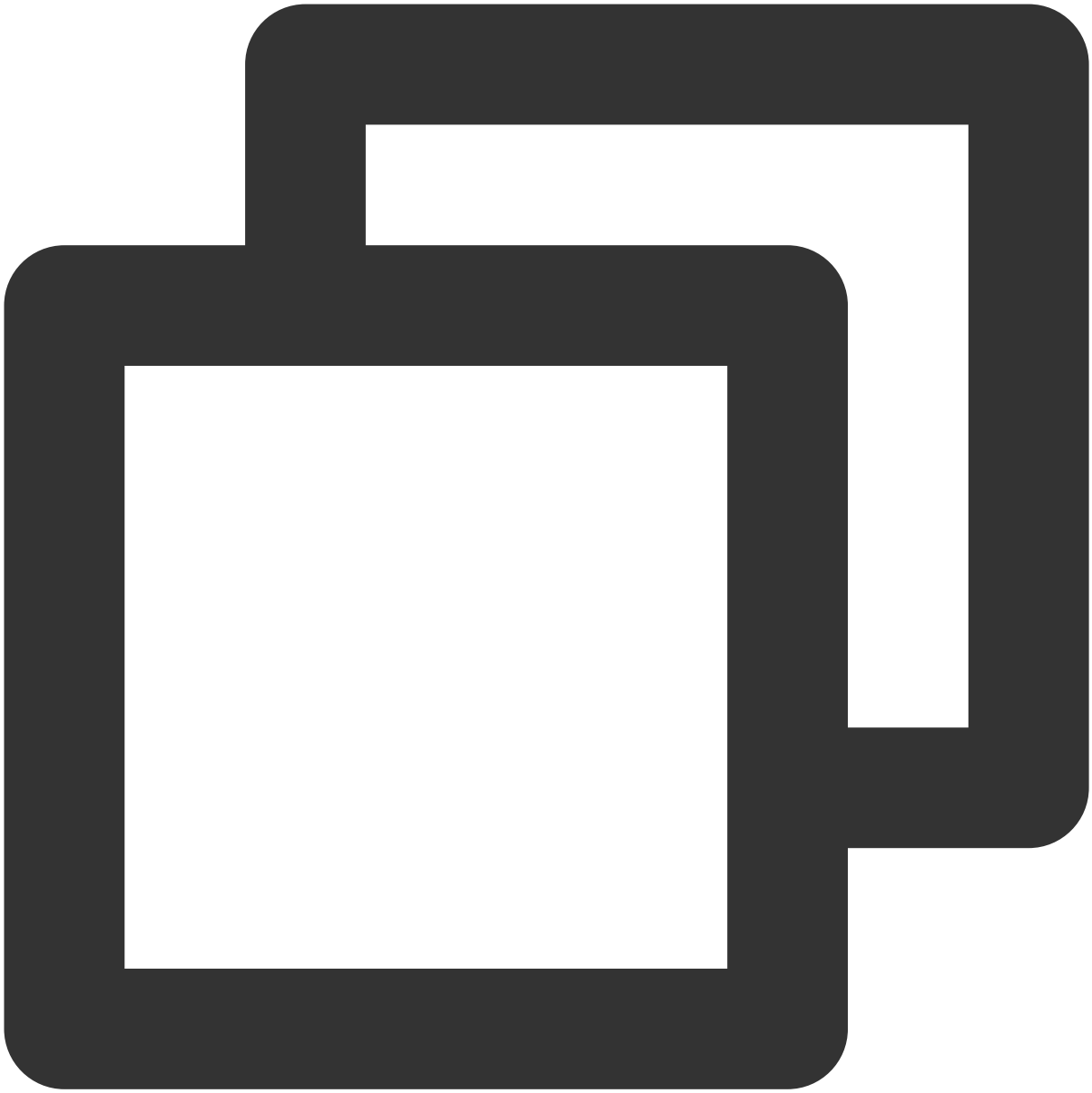
```
time1.tencentyun.com
time2.tencentyun.com
time3.tencentyun.com
time4.tencentyun.com
time5.tencentyun.com
```

パブリックネットワークNTPサーバー



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

以下は、古いパブリックネットワークNTPサーバーアドレスです。古いアドレスは引き続き使用できますが、新しいパブリックネットワークNTPサーバーアドレスを構成して使用することをお勧めします。



```
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システムのNTPクロックソースサーバーの設定方法の詳細については、LinuxインスタンスのNTPサービスの設定 をご参照ください。

WindowsシステムのNTPクロックソースサーバーの設定方法の詳細については、WindowsインスタンスのNTPサービスの設定をご参照ください。

LinuxインスタンスでNTPサービスを設定する

最終更新日：：2022-03-07 11:41:48

操作シナオリ

Network Time Protocol daemon (NTPD) は Linux OSのデーモンプロセスであり、ローカルシステムとクロックソースサーバ間の時間差を修正するために使用され、NTP プロトコルを完全に実現します。NTPDとNTPDateの違いは、NTPDateは強制的に即時更新するために使用でき、NTPDは体系的な方法として使用できます。このドキュメントでは、CentOS 7.5 OSのCVMを例として使用して、NTPDをインストールおよび設定する方法について説明します。

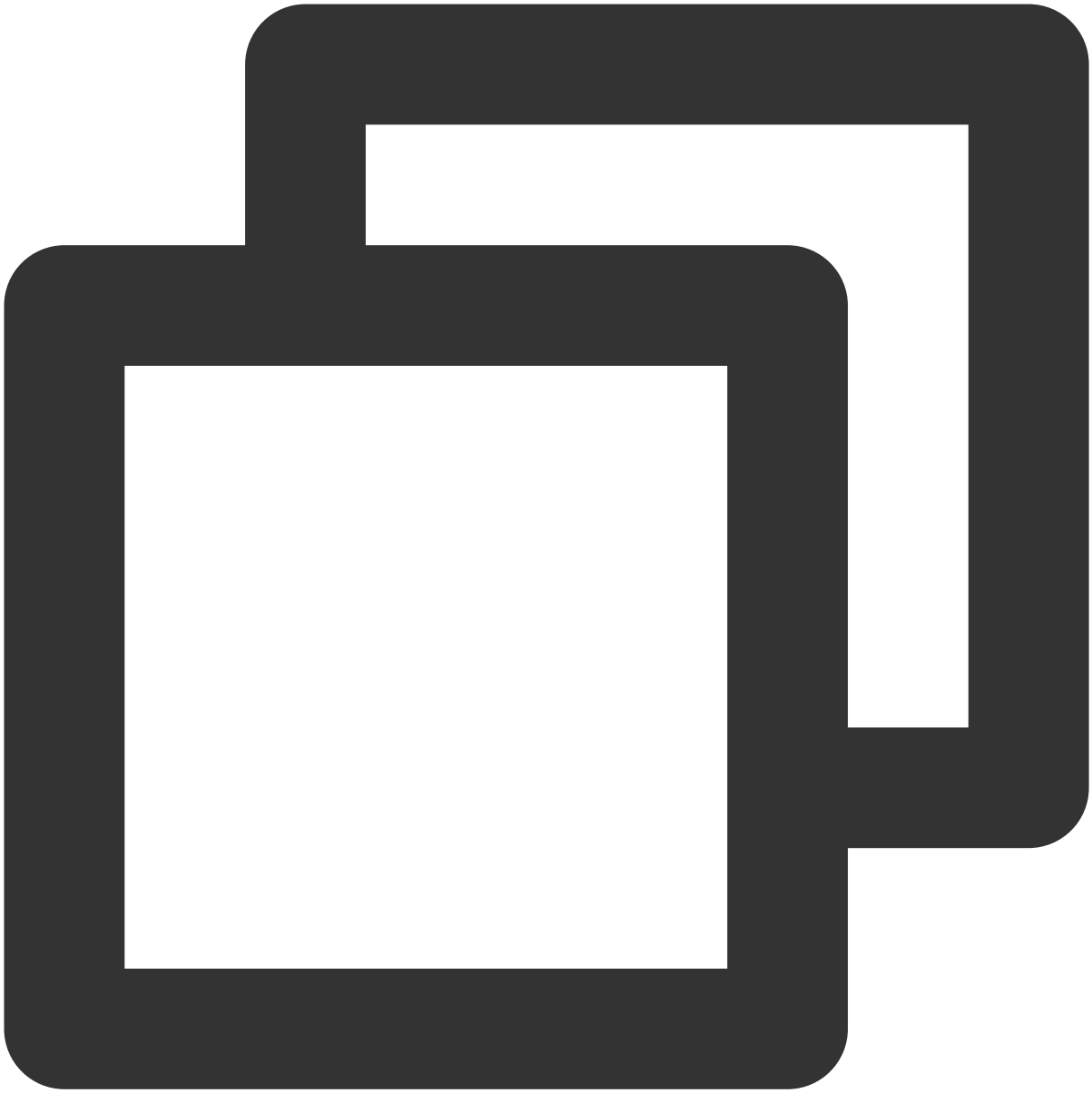
注意事項

一部のOSでは、デフォルトのNTPサービスとしてchronyを使用しています。NTPDが実行中であり、起動時に自動的に起動するように設定されていることを確認してください。
`systemctl is-active ntpd.service` コマンドを使用して、NTPDが実行されているかどうかを確認します。
`systemctl is-enabled ntpd.service` コマンドを使用して、NTPDが起動時に自動的に起動するように設定されているかどうかを確認します。
NTPサービスの通信ポートはUDP 123です。NTPサービスを設定する前に、UDP 123ポートをインターネットに開放することを確認してください。
このポートが開放されていない場合、セキュリティグループルールの追加 を参照して、ポートをインターネットに開放してください。

操作手順

NTPDサービスのインストール

次のコマンドを実行して、NTPDがインストールされているかどうかを確認します。

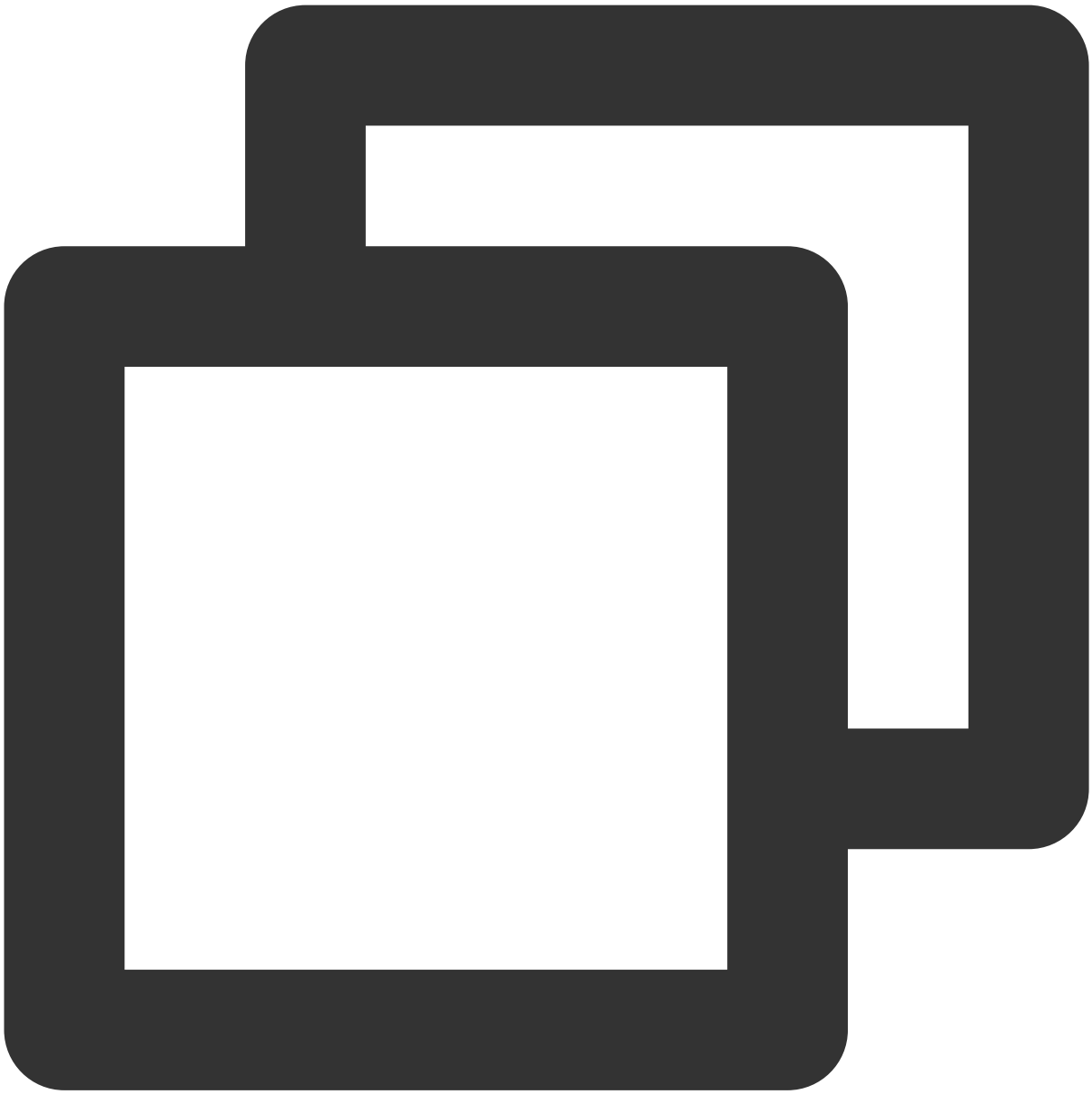


```
rpm -qa | grep ntp
```

次の結果が返される場合、NTPDがインストールされていることを意味します。

```
[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
```

NTPDがインストールされていない場合は、 `yum install ntp` コマンドを実行してNTPDをインストールしてください。

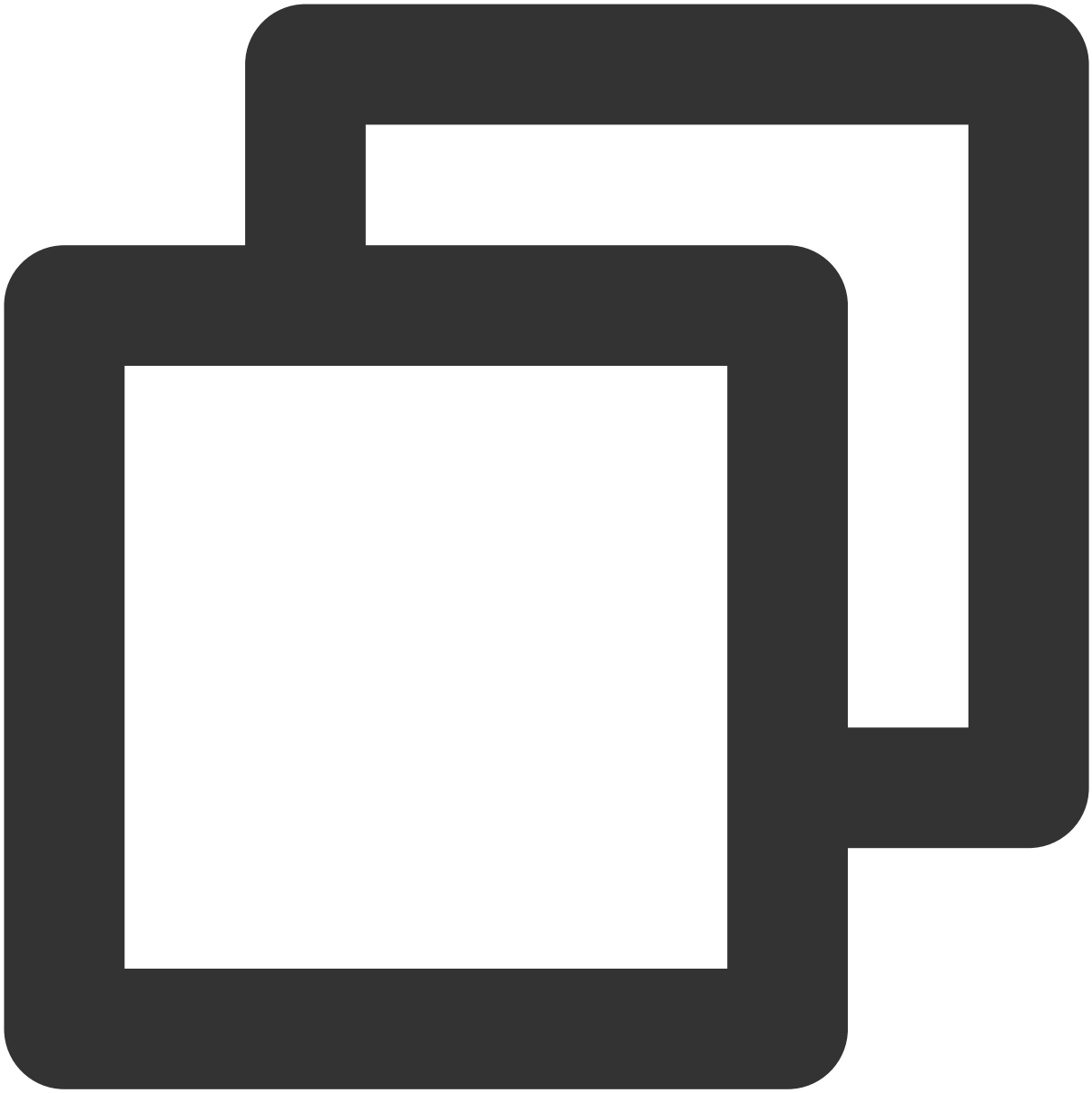


```
yum -y install ntp
```

NTPDはデフォルトでクライアントモードを使用します。

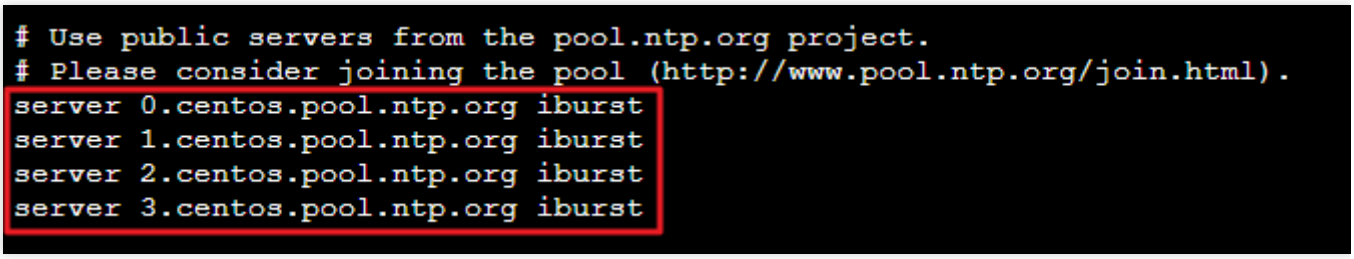
NTPの設定

1. 次のコマンドを実行して、NTPサービスの構成ファイルを開きます。



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

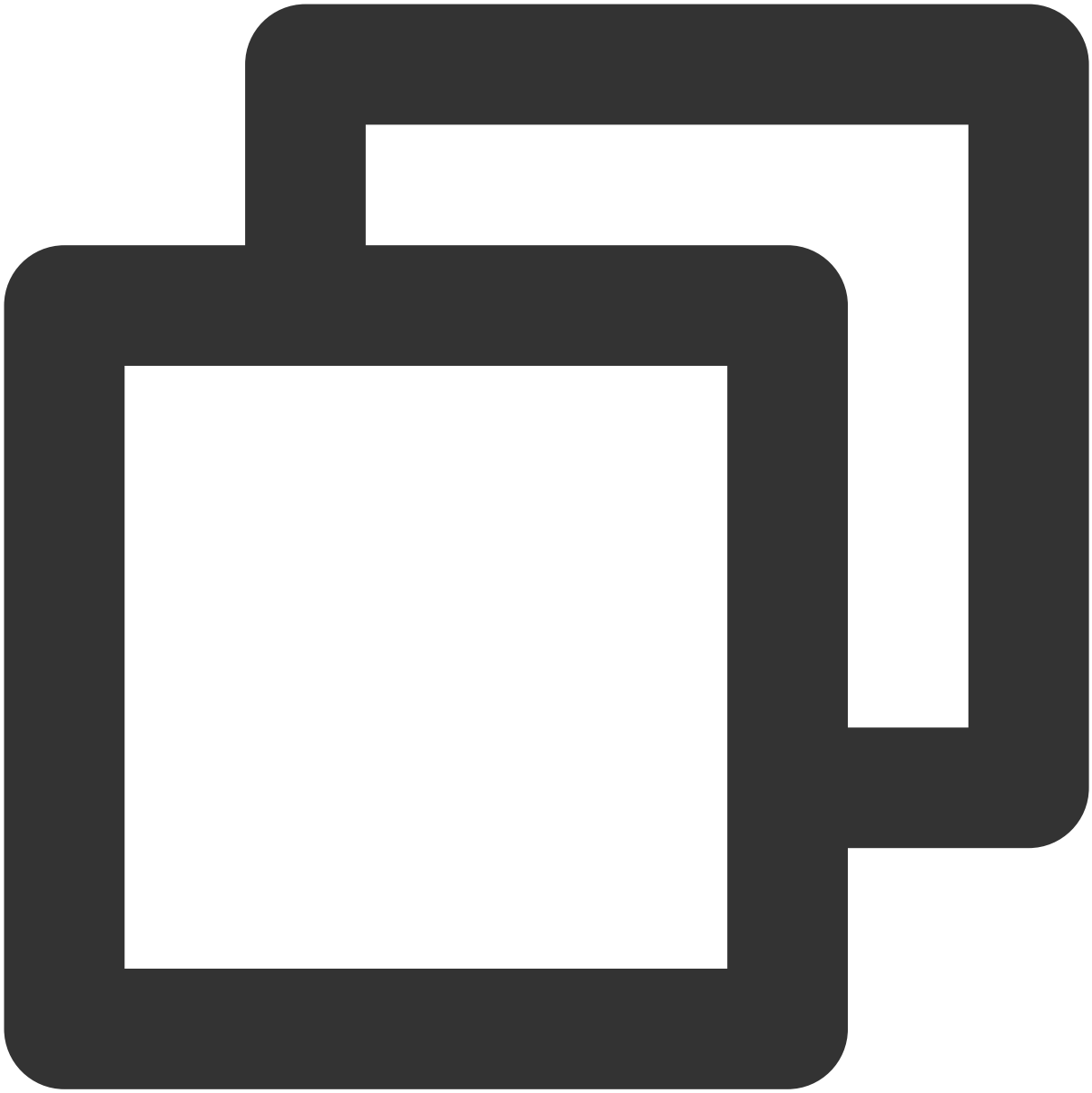
2. **i**キーを押して編集モードに切り替え、サーバーの関連設定を見つけます。以下に示すように、サーバーを、設定するターゲットNTPクロックソースサーバ（`time1.tencentyun.com` など）に変更し、不要なNTPクロックソースサーバを削除します。



3. 「**Esc**」キーを押し、**:wq**を入力し、ファイルを保存して閉じます。

NTPDの起動

次のコマンドを実行して、NTPDサービスを再起動します。

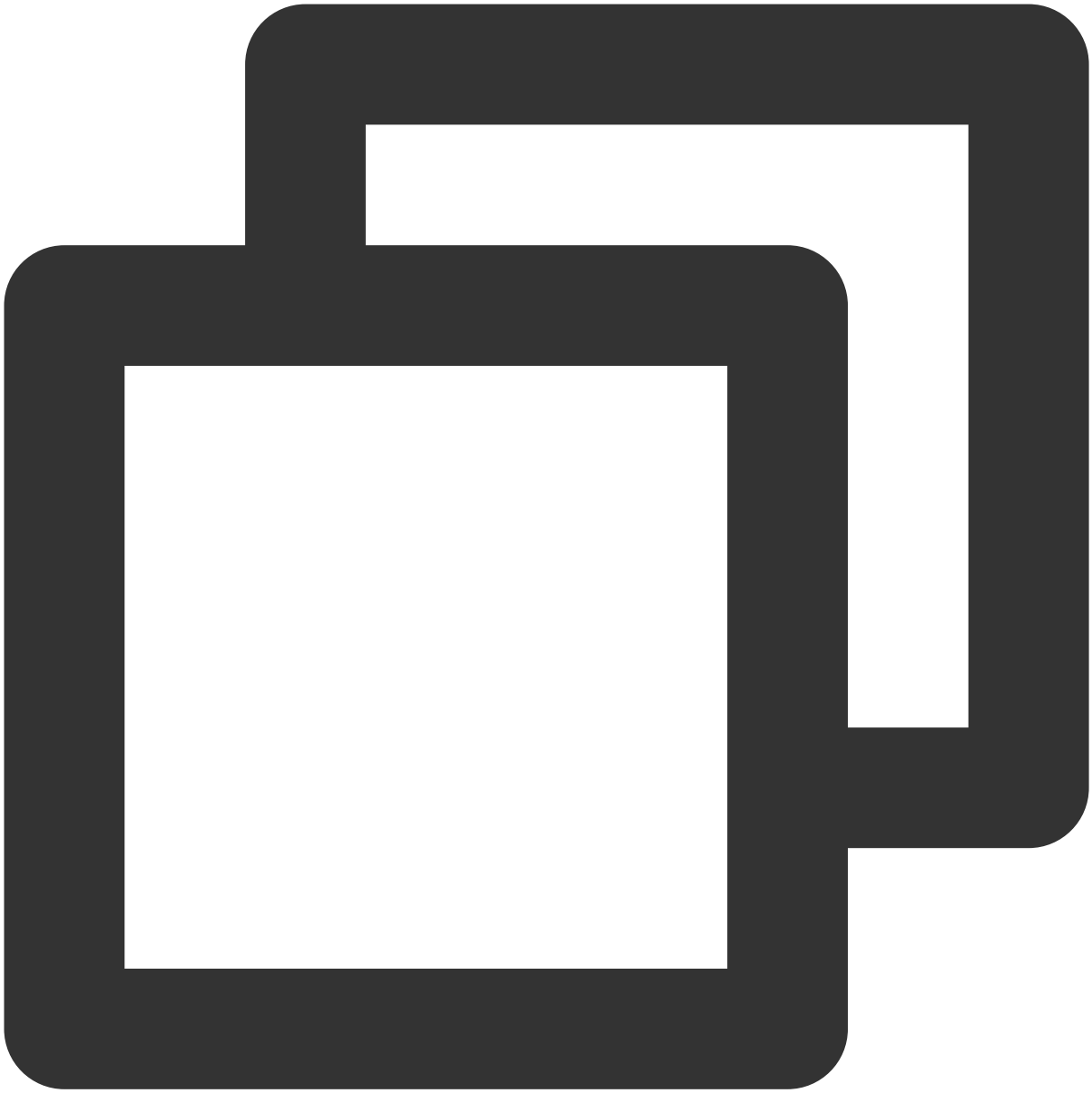


```
systemctl restart ntpd.service
```

NTPDステータスの確認

次のコマンドを実行して、必要に応じてNTPDのステータスを確認します。

次のコマンドを実行して、NTPがサービスポートUDP 123で正常にリッスンされているかどうかを確認します。

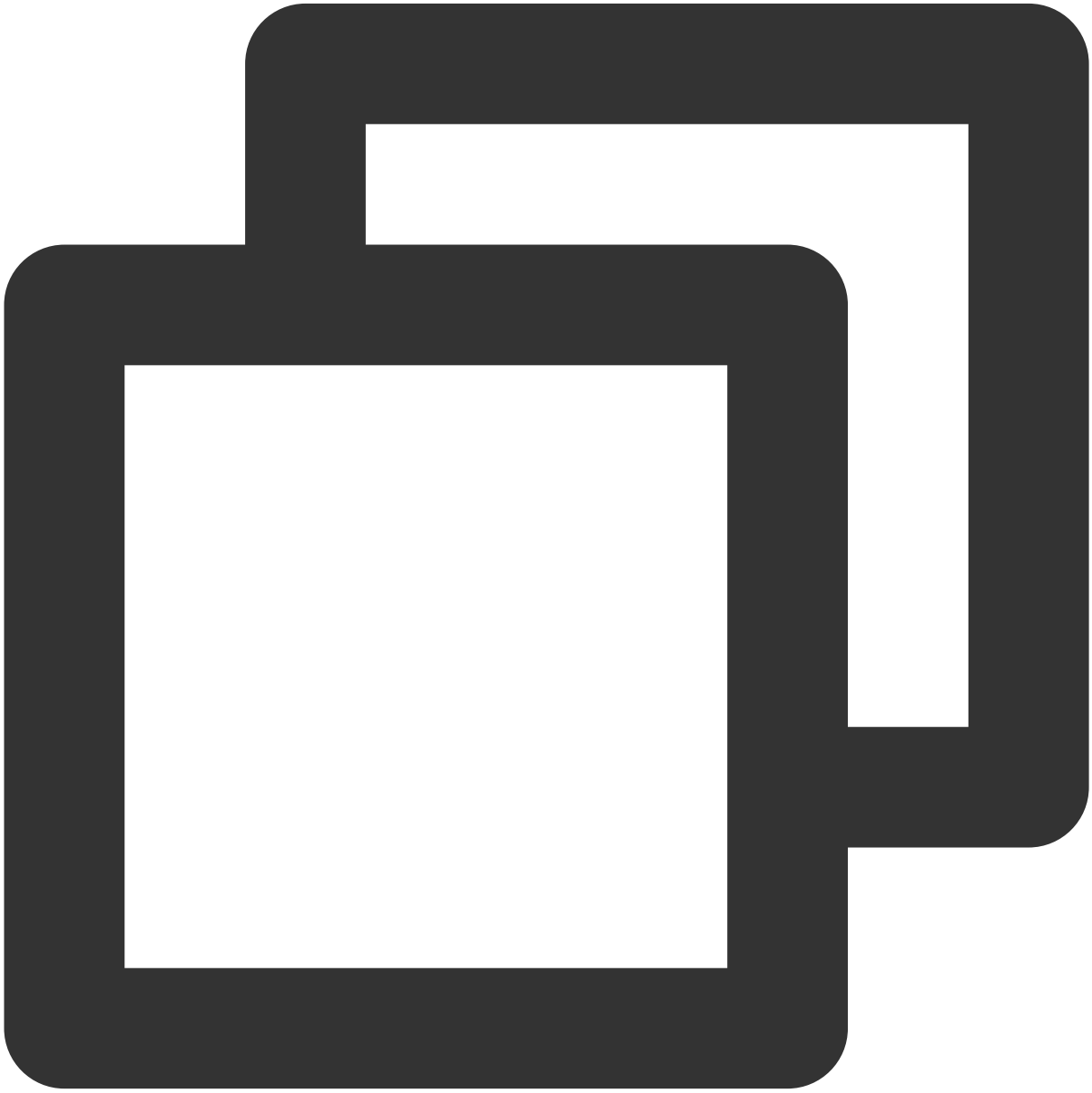


```
netstat -nupl
```

以下のような結果が返されると、正常にリッスンされていることを意味します。

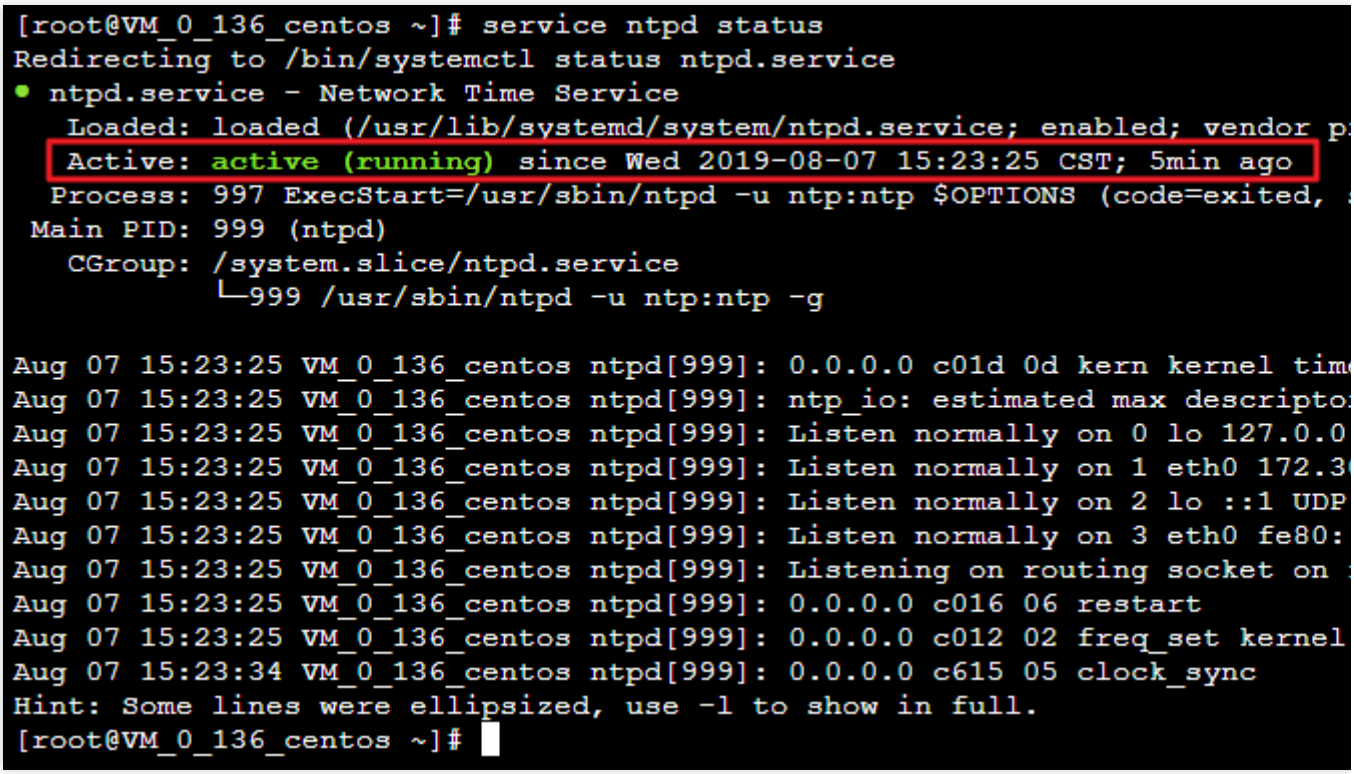
```
[root@VM_0_136_centos ~]# netstat -nupl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 172.30.0.136:123        0.0.0.0:*
udp        0      0 127.0.0.1:123           0.0.0.0:*
udp6       0      0 fe80::5054:ff:fec2::123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

次のコマンドを実行して、NTPDステータスが正常かどうかを確認します。

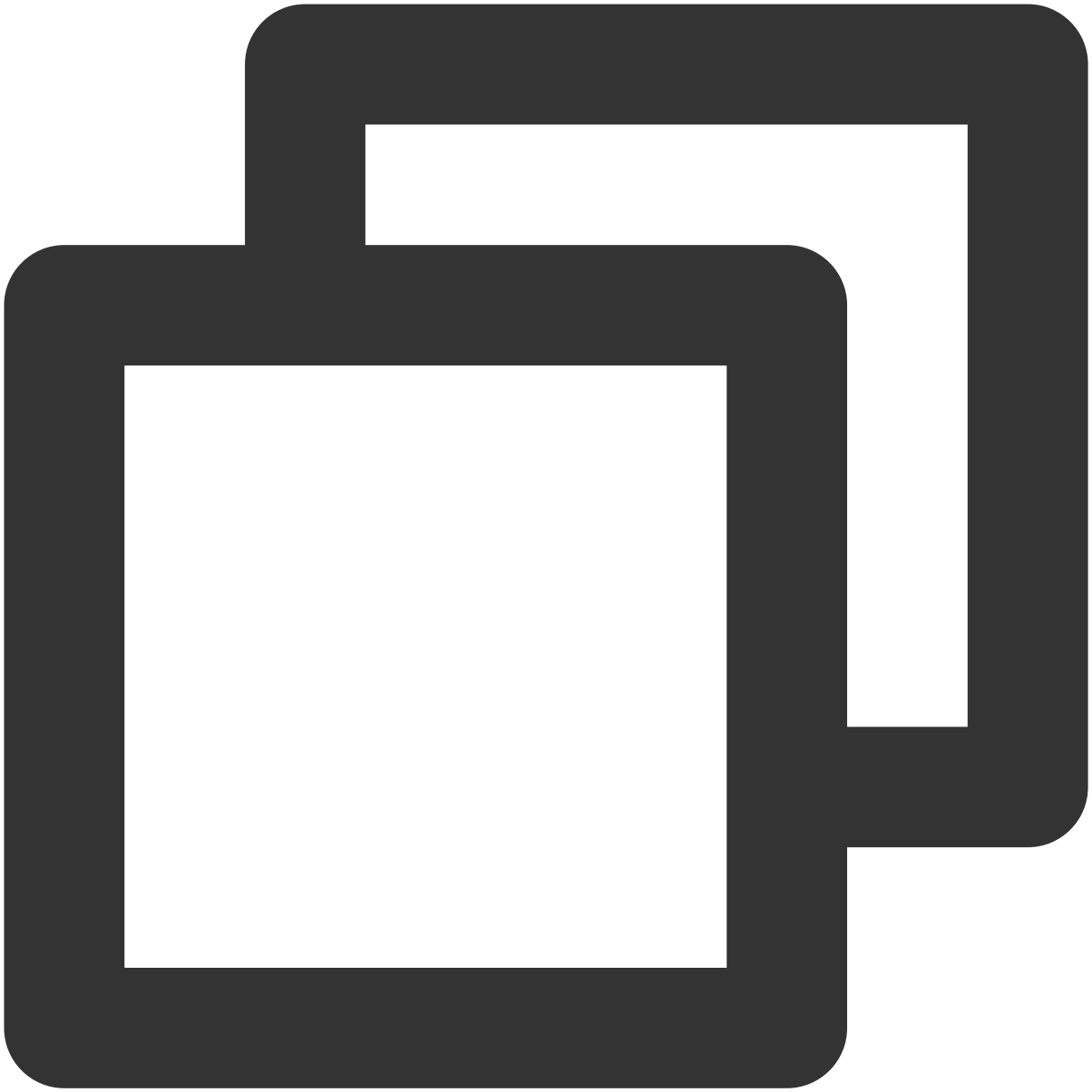


```
service ntpd status
```

以下のような結果が返されると、NTPDステータスが正常であることを意味します。

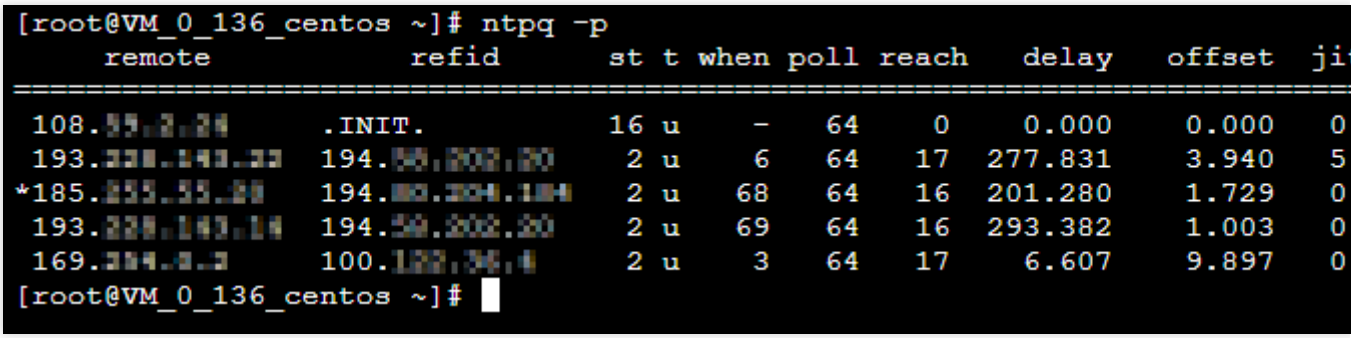


次のコマンドを実行して、より詳細なNTPサービス情報を取得します。



```
ntpq -p
```

以下のような結果が返されます：



remote：このリクエストに応答するNTPサーバの名前。

refid：NTP サーバが使用する上位NTPサーバです。

st：リモートサーバーの階層。サーバーのストラタムは、1から16まで、高から低に設定できます。負荷やネットワークの輻輳を軽減するため、原則としてストラタム1サーバーへの直接接続は避けることが推奨されています。

when：最後に成功したリクエストから経過した秒数。

poll：ローカルサーバーとリモートサーバー間の同期間隔（秒単位）。NTPを最初に実行すると、pollの値が小さく、サーバと同期頻度が高いため、できるだけ早く正しい時間範囲に調整することをお勧めします。調整後、pollの値は徐々に増加し、同期頻度は減少します。

reach：サーバーに接続できるかどうかをテストするために使用される8進数。接続が成功するたびに、reachの値が増加します。

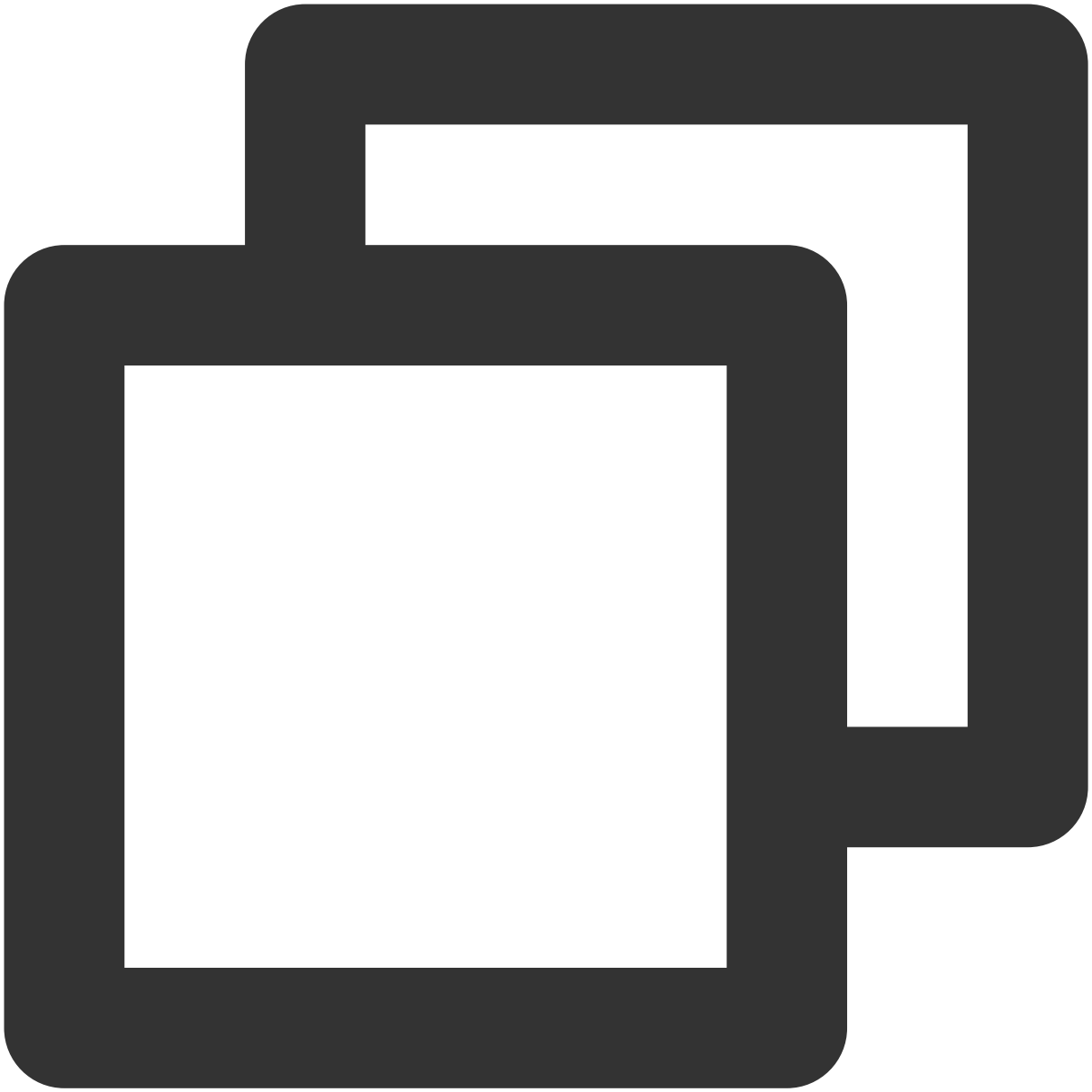
delay：ローカルマシンからNTPサーバーに同期要求を送信する往復時間。

offset：NTPを介してホストとタイムソース間のミリ秒（ms）単位の時間差。オフセットが0に近いほど、ホストとNTPサーバーの時間が近くなります。

jitter：統計に使用される値。特定の連続したコネクション数の場合のオフセットの分布を集計します。つまり、絶対値が小さいほど、ホスト時間は正確になります。

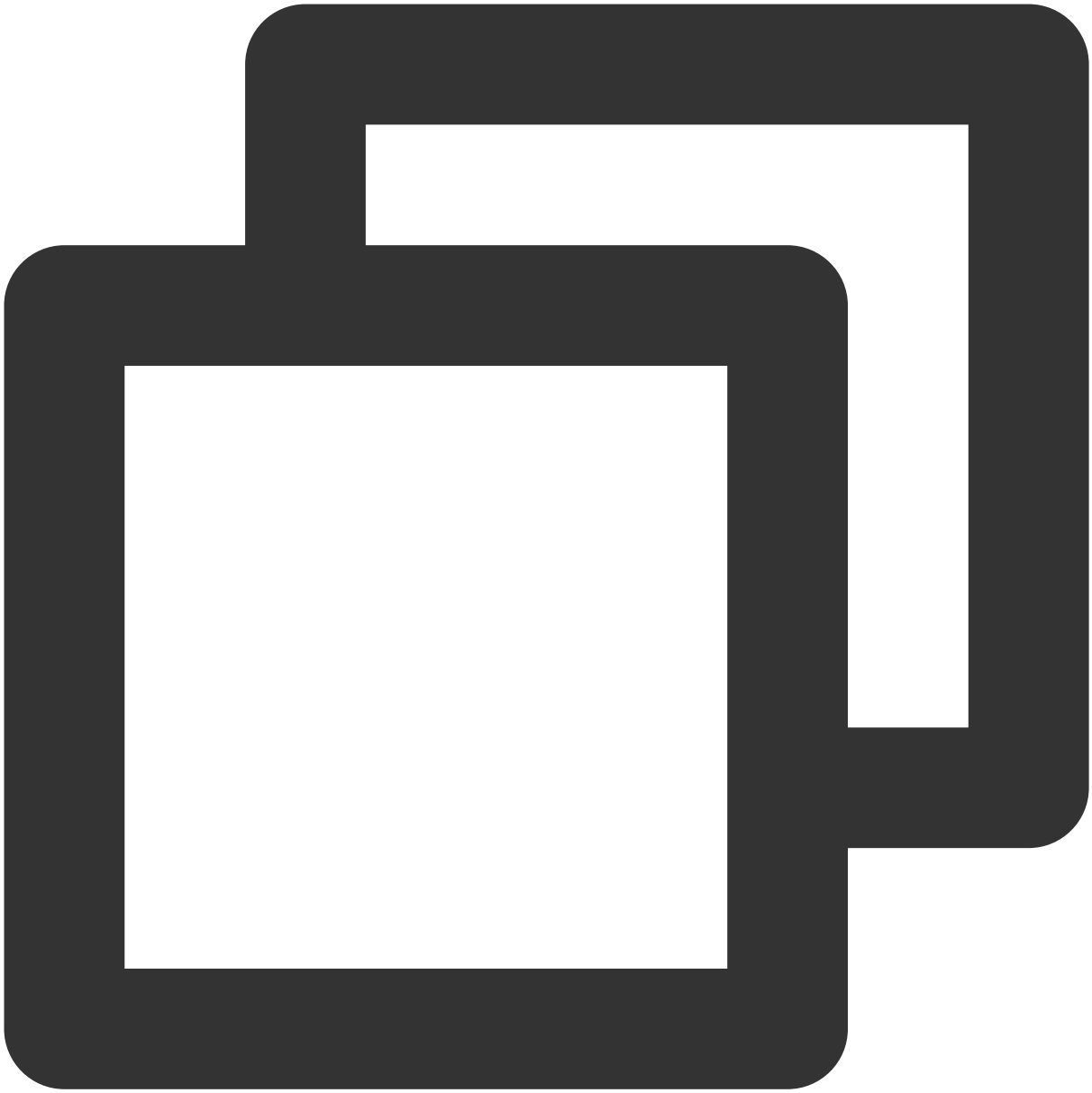
NTPD を自動起動に設定する

1. 次のコマンドを実行して、NTPDが起動時に自動的に起動するように設定します。



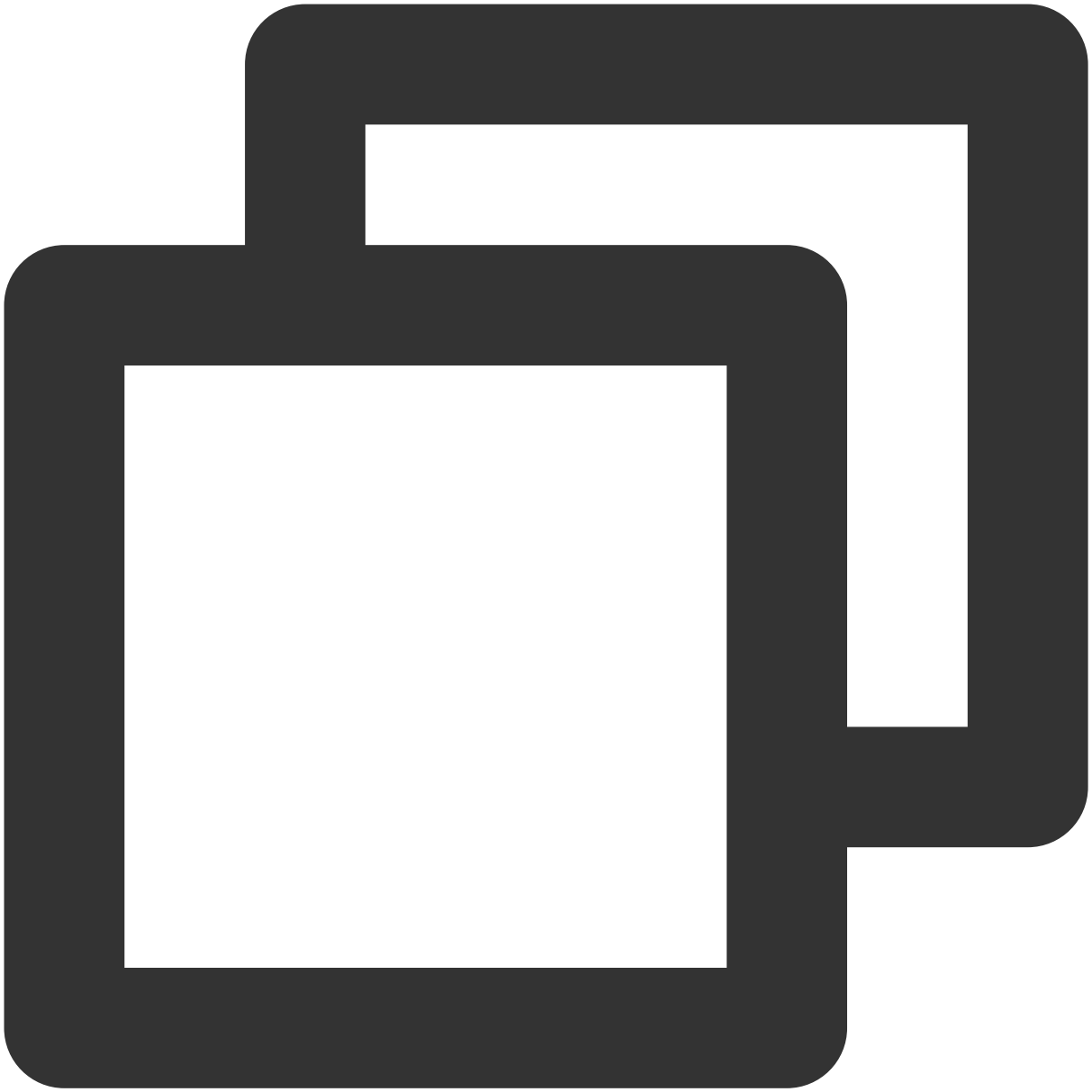
```
systemctl enable ntpd.service
```

2. 次のコマンドを実行して、chronyが起動時に自動的に起動するように設定されているかどうかを確認します。



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

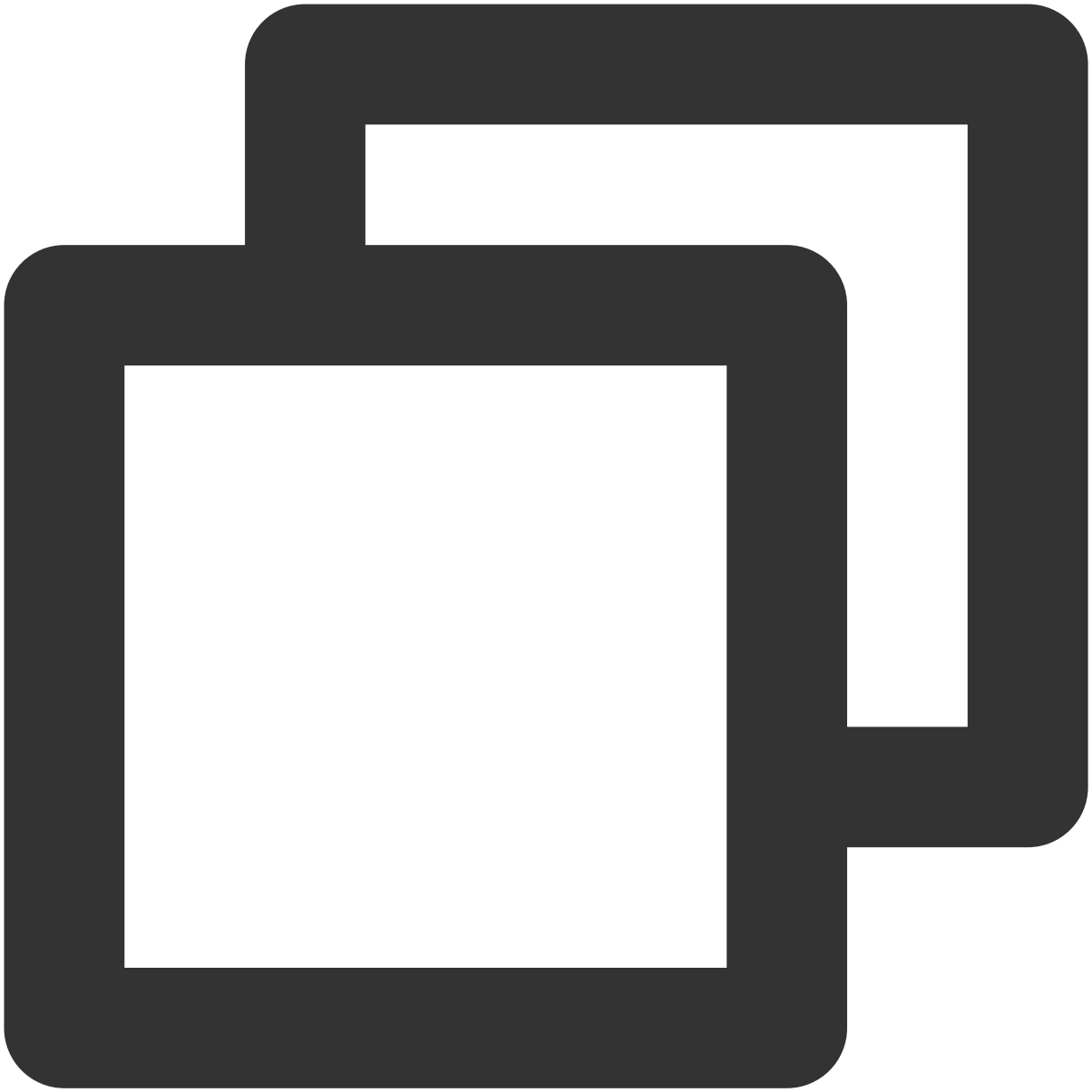
chronyが起動時に自動的に起動するように設定されている場合は、次のコマンドを実行して、自動起動リストからchronyを削除します。
chronyがNTPDと競合しているため、 NTPD の起動に失敗する可能性があります。



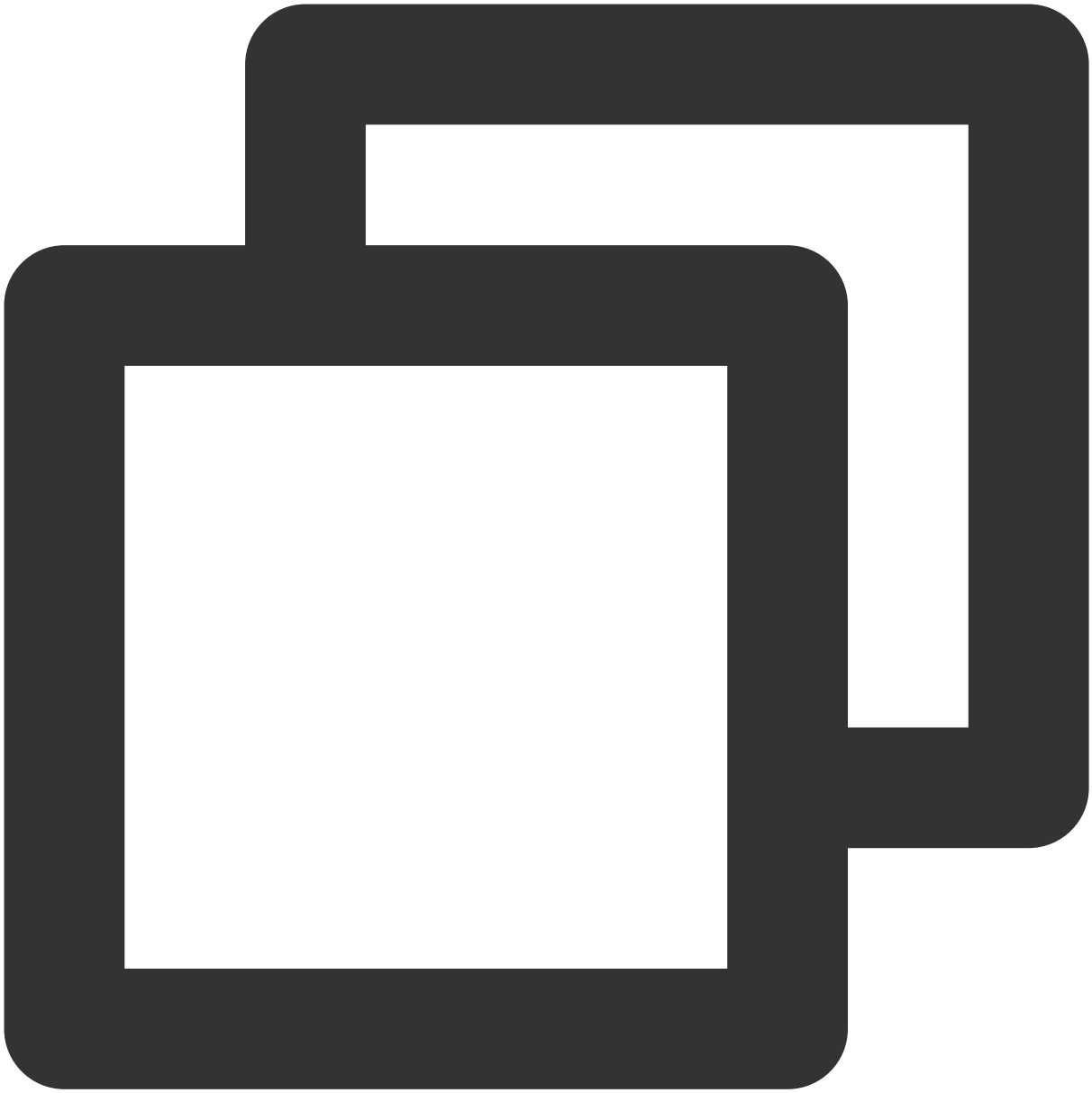
```
systemctl disable chronyd.service
```

NTPDセキュリティ強化

/etc/ntp.conf設定ファイルのセキュリティを強化するには、次のコマンドを順番に実行します。



```
interface ignore wildcard
```



```
interface listen eth0
```

Linuxインスタンス：NTPDateからNTPDへの変換

最終更新日：：2022-05-07 15:42:08

操作シナオリ

Linux インスタンスには、NTPサービスを同期させるためNTPDateとNTPDの2つの方法が用意されています。NTPDateは強制的に即時更新するために使用でき、NTPDは体系的な方法として使用できます。 NTPDateサービスは、新しいインスタンスに使用できますが、ntpd はビジネスを実行しているインスタンスに対して使用することを推奨します。このドキュメントでは、CentOS 7.5 OSを使用して、CVMでNTPDateからNTPDに変換する方法について説明します。

前提条件

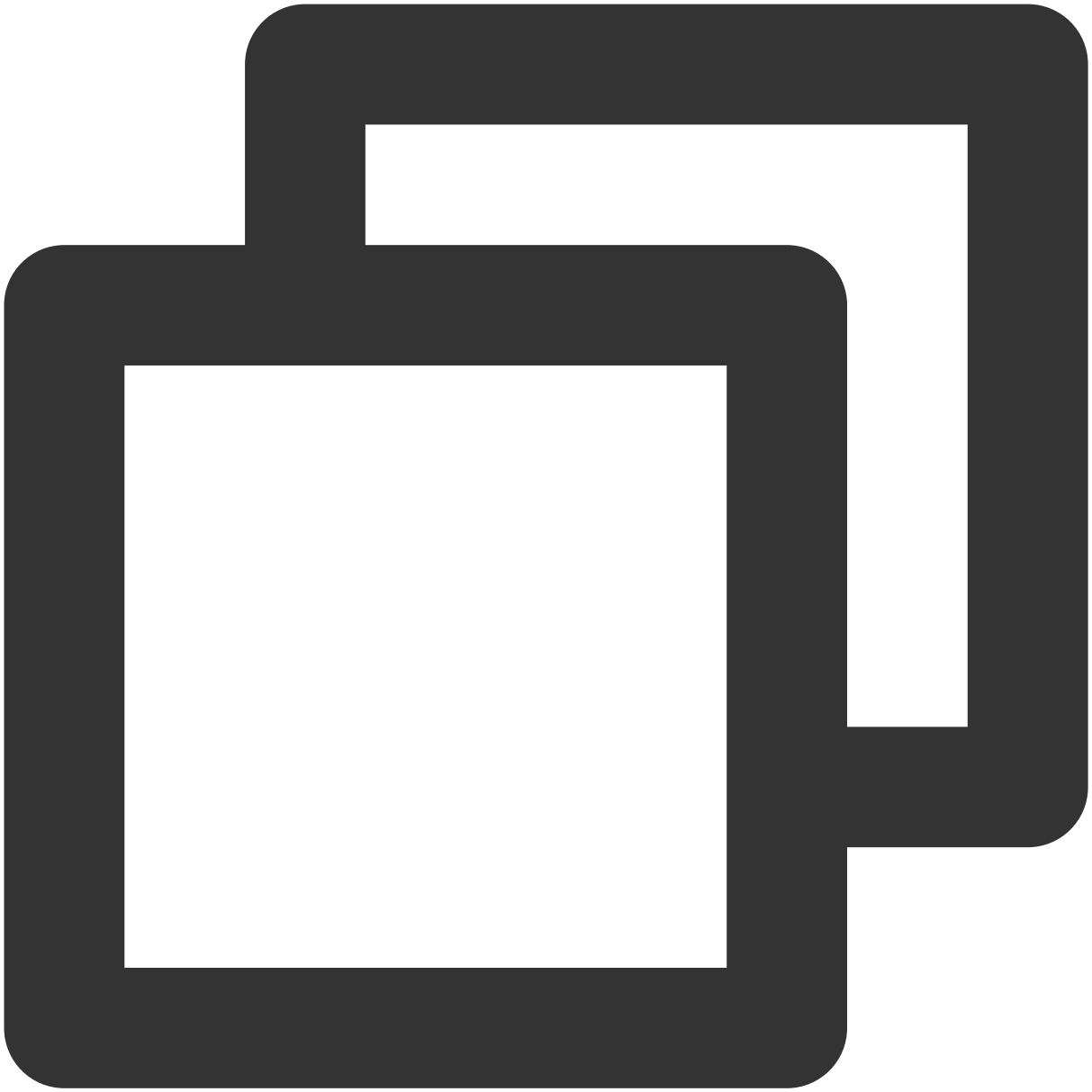
NTPサービスの通信ポートは、UDP 123です。NTPサービスに変換する前に、UDP ポート123 をインターネットに開放することを確認してください。
このポートが開放されていない場合、セキュリティグループルールの追加 をご参照ください。

操作手順

NTPDateをNTPDに手動で変換する

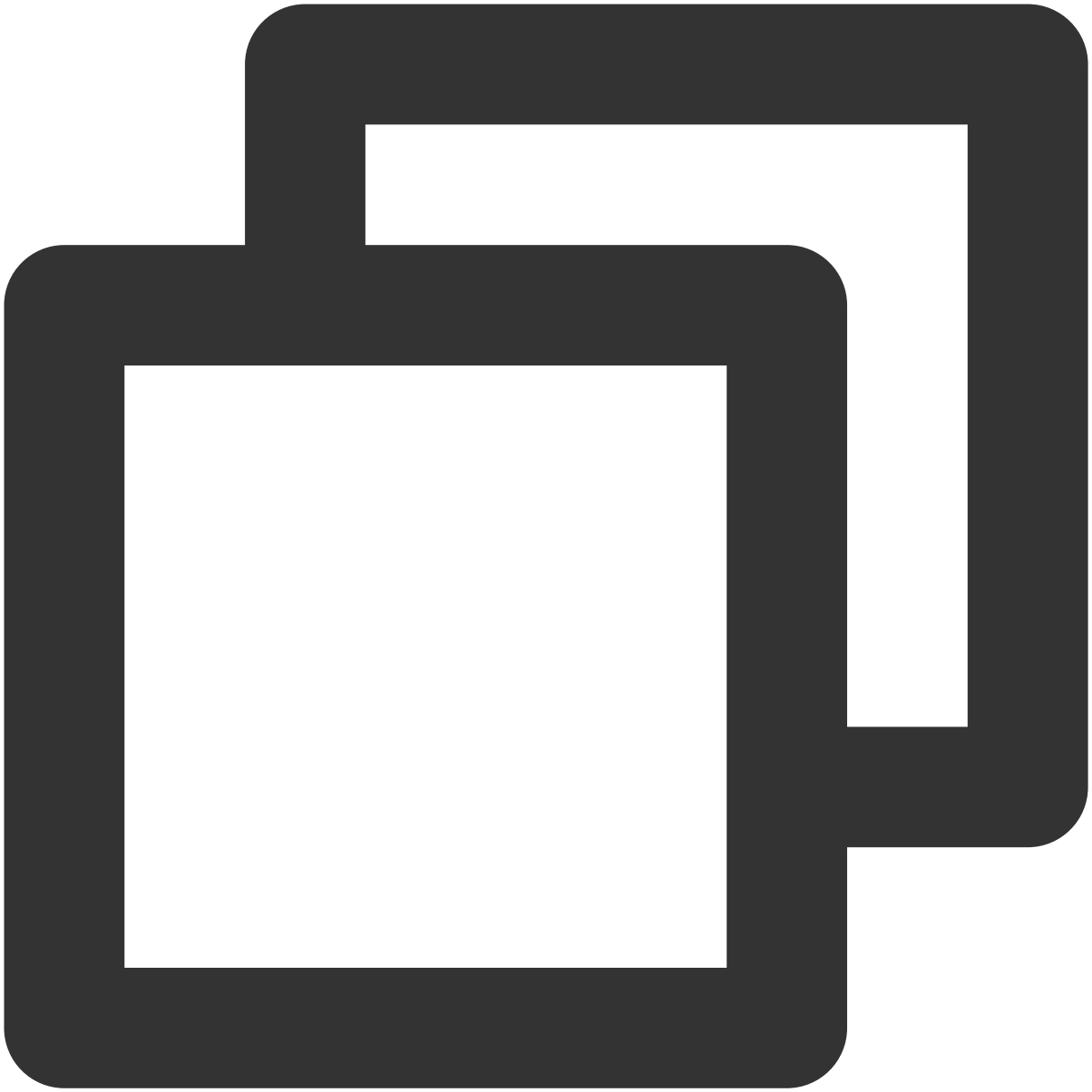
NTPDateのシャットダウン

1. 次のコマンドを実行して、crontab設定をエクスポートし、NTPDateをフィルタリングします。



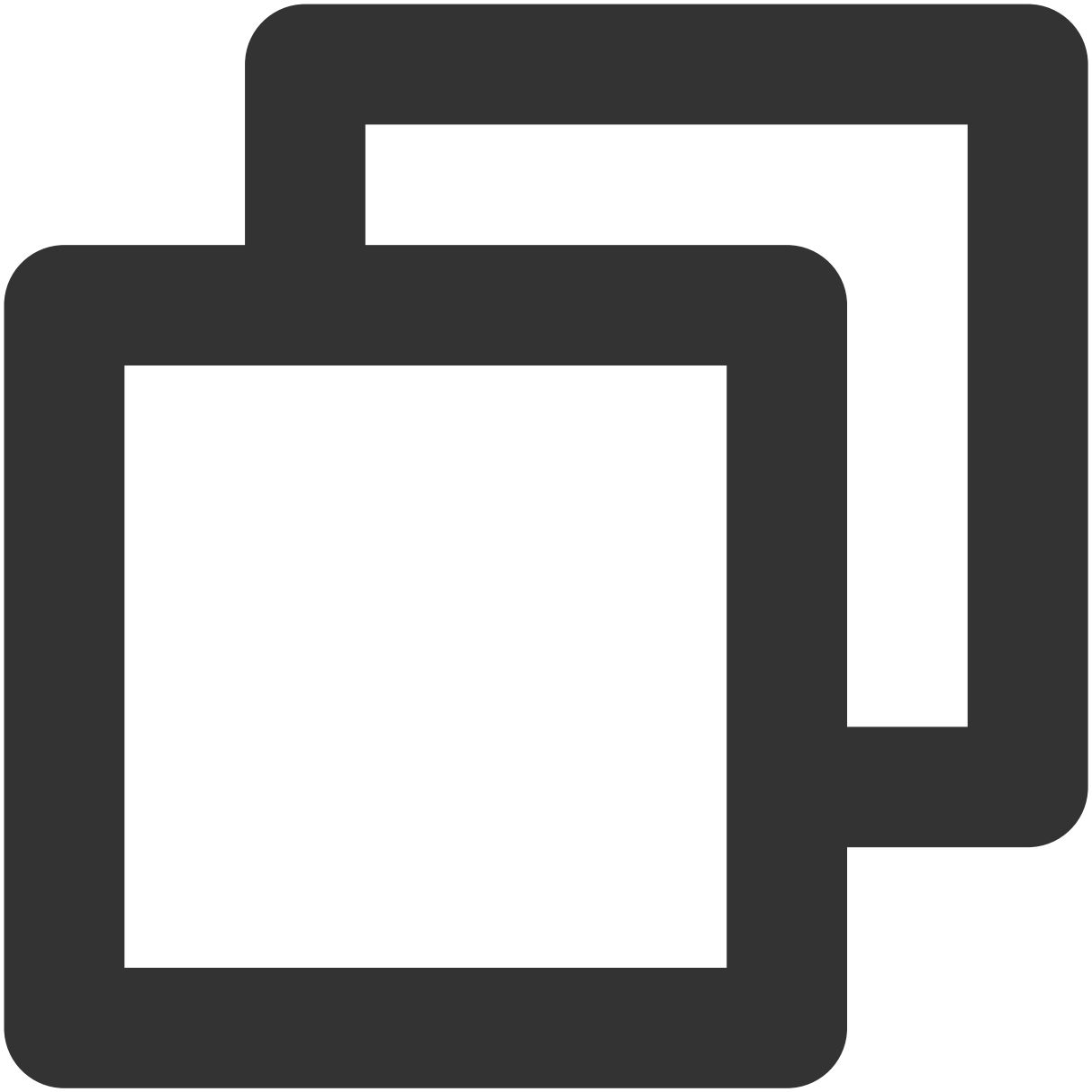
```
crontab -l |grep -v ntpupdate > /tmp/cronfile
```

2. 次のコマンドを実行して、NTPDate設定を更新します。



```
crontab /tmp/cronfile
```

3. 次のコマンドを実行して、`rc.localファイルを変更します。

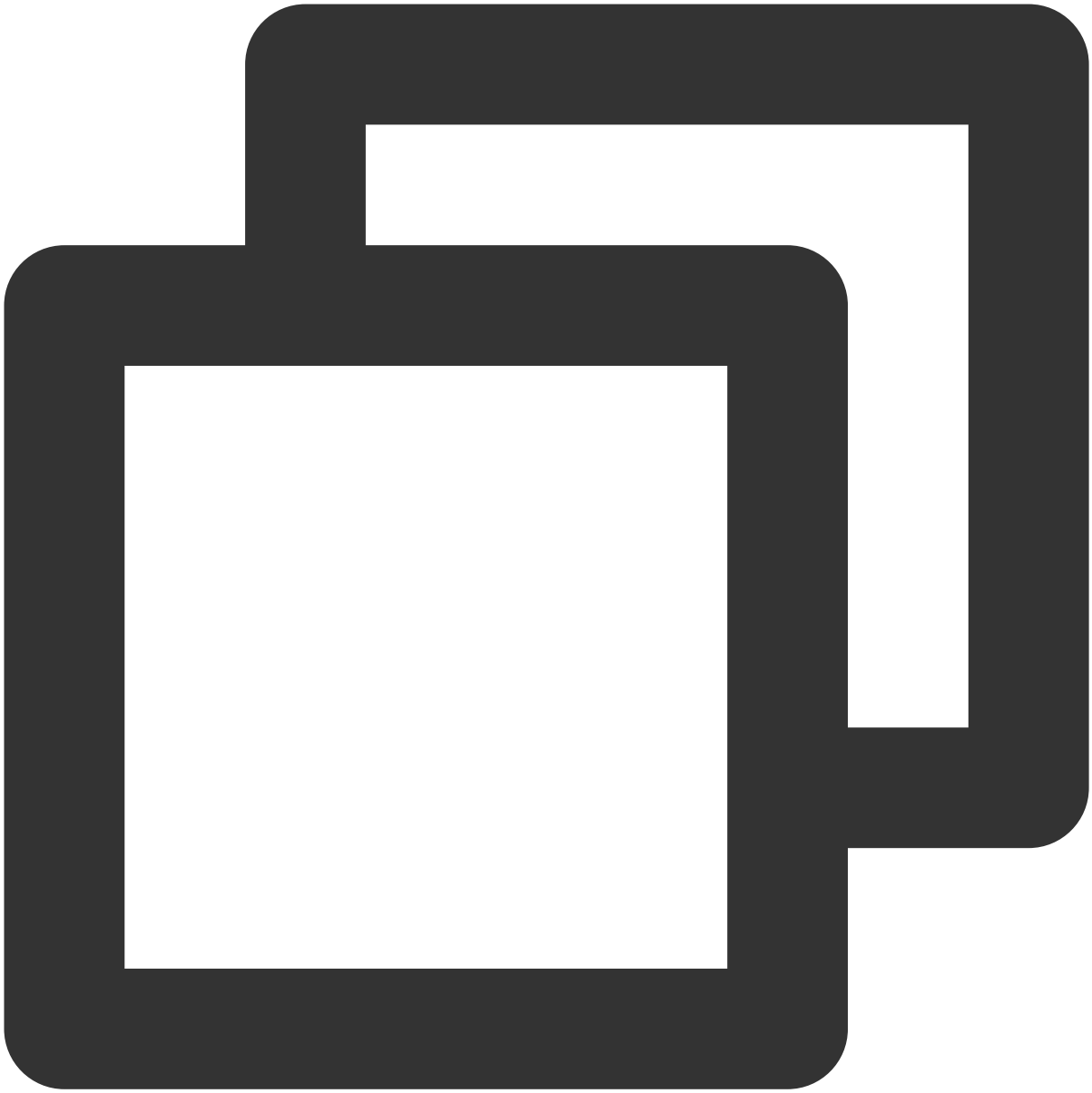


```
vim rc.local
```

4. 「**i**」を押して編集モードに切り替え、ntpupdateの設定行を削除します。
5. 「**Esc**」キーを押して、**:wq**を入力し、ファイルを保存してから戻ります。

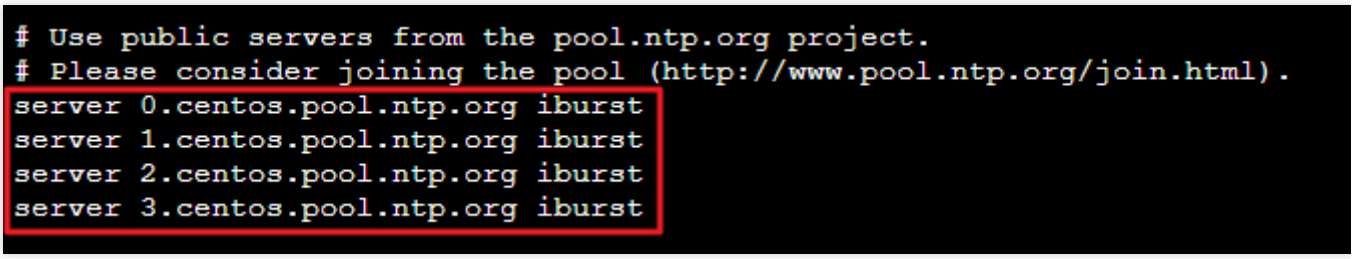
NTPDの設定

1. 次のコマンドを実行して、NTPサービスの設定ファイルを開きます。



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

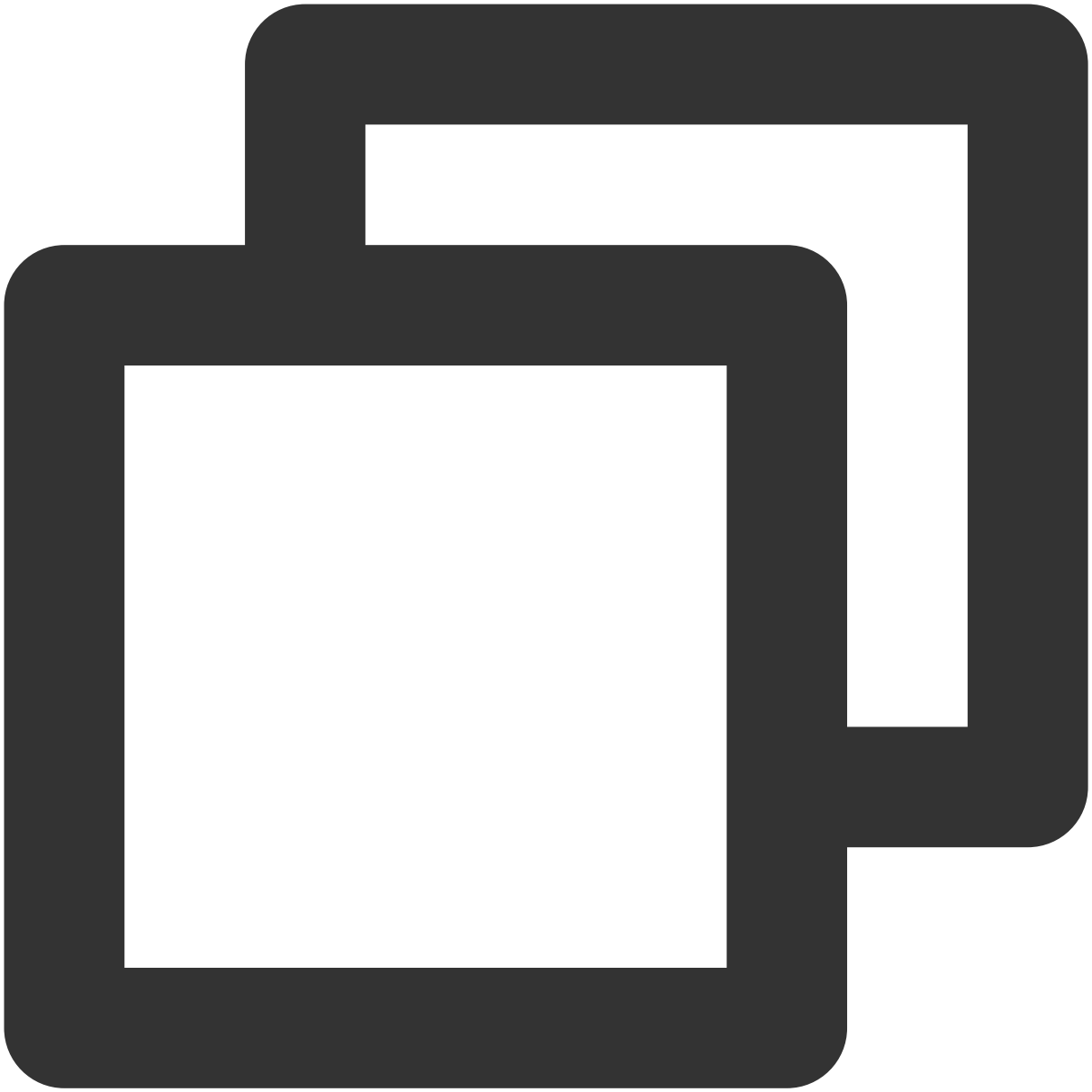
2. **i**キーを押して編集モードに切り替え、サーバーの関連設定を見つけ、サーバーを、設定するターゲットNTPクロックソースサーバ（`time1.tencentyun.com` など）に変更し、一時的に不要なNTPクロックソースサーバを削除します。以下の通りです。



3. 「**Esc**」キーを押し、**:wq**を入力し、ファイルを保存してから戻ります。

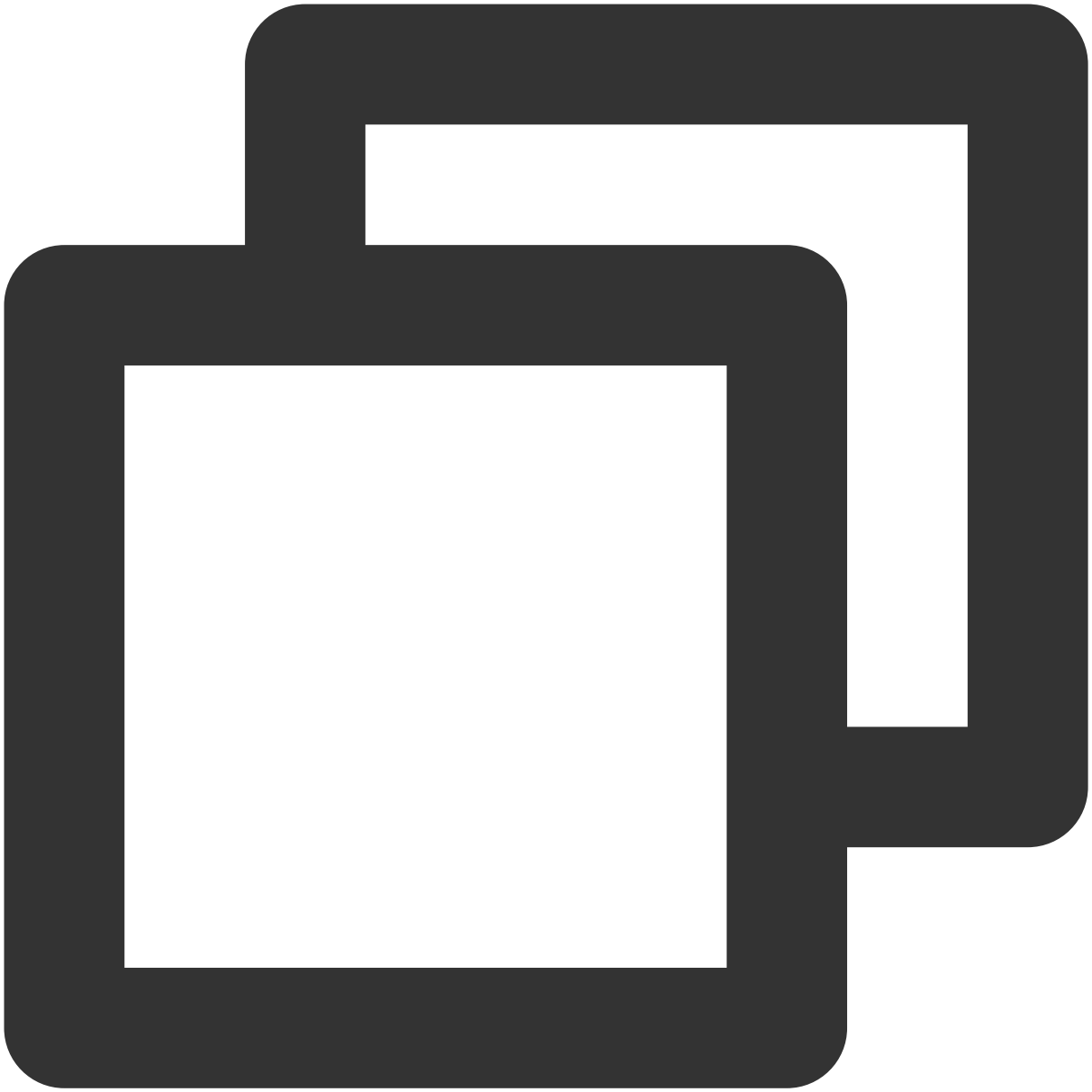
NTPDateをNTPDへ自動変換

1. `ntpd_enable.sh` スクリプトをダウンロードします。



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

2. 次のコマンドを実行し、 `ntpd_enable.sh` スクリプトを使用してNTPDateをNTPDに変換します。



```
sh ntpd_enable.sh
```

WindowsインスタンスでNTPサービスを設定する

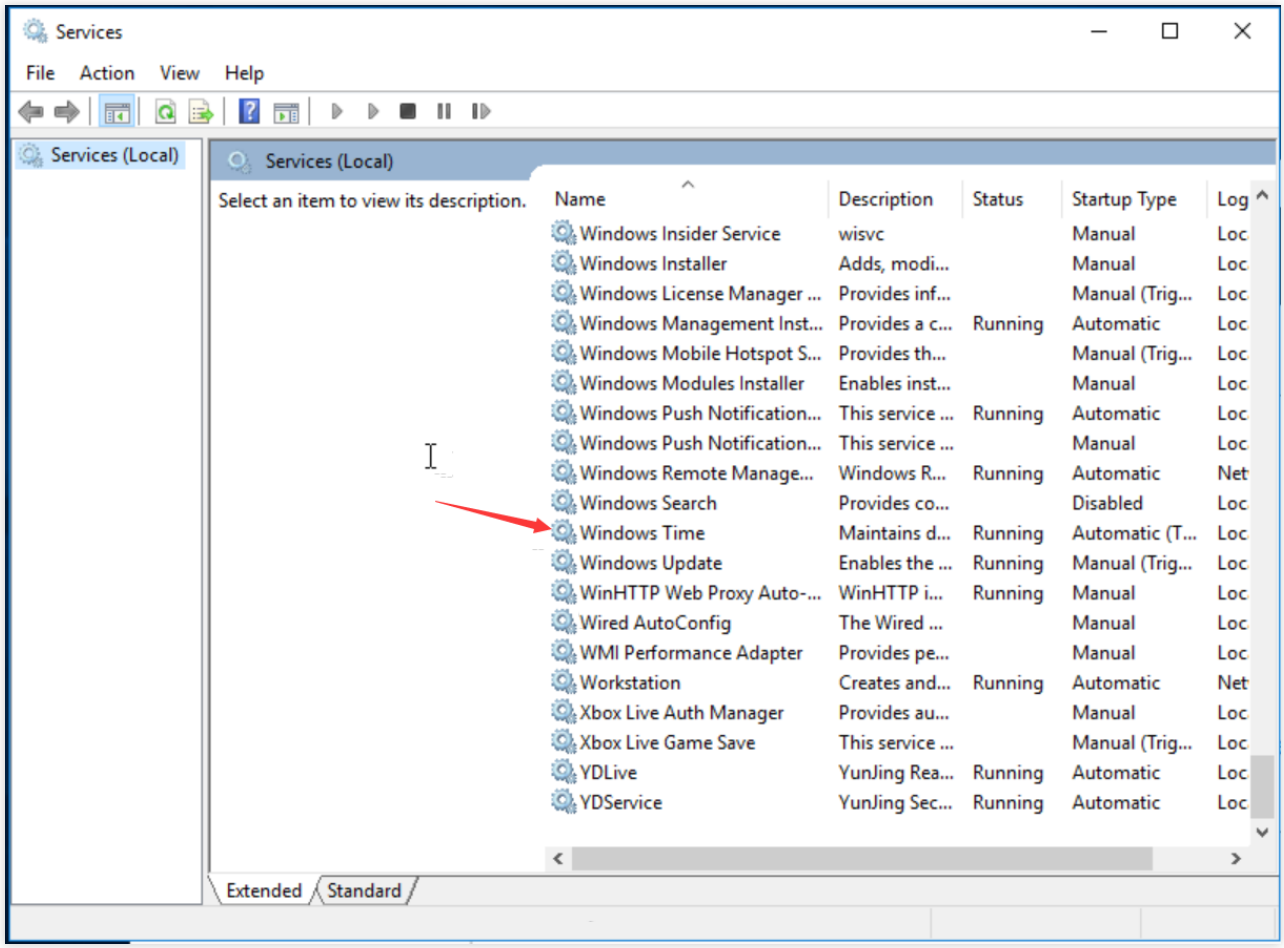
最終更新日：：2021-08-03 10:20:28

ユースケース

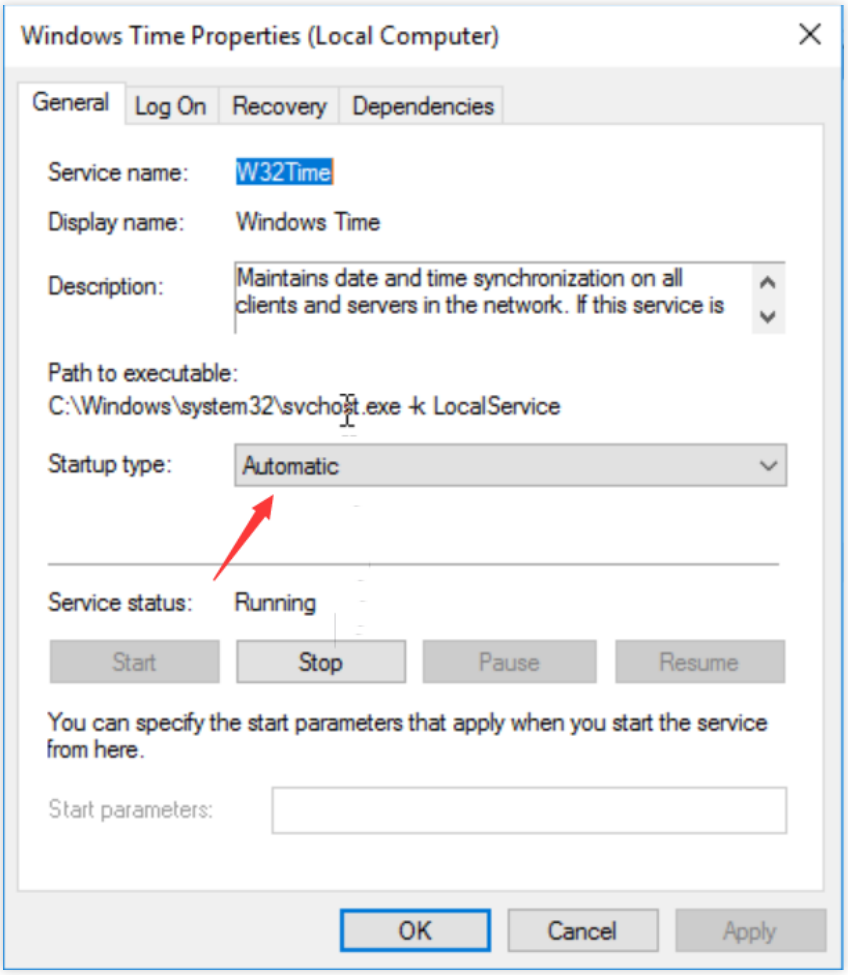
このドキュメントでは、Windows ServerでNTPサービスを有効にし、クロックソースサーバーのアドレスを変更する方法について説明します。
Windowsタイムサービス（Windows Time service、 W32Time）は、ローカルシステムとクロックソースサーバー間の時刻を同期するために使用されます。 ネットワークタイムプロトコル（NTP）を使用して、ネットワーク全体でコンピューターのクロックを同期します。 以下では、Windows Server 2016を例として、クライアントとコマンドラインを使用してNTPサービスを有効にし、クロックソースサーバーアドレスを変更する方法について説明します。

操作手順

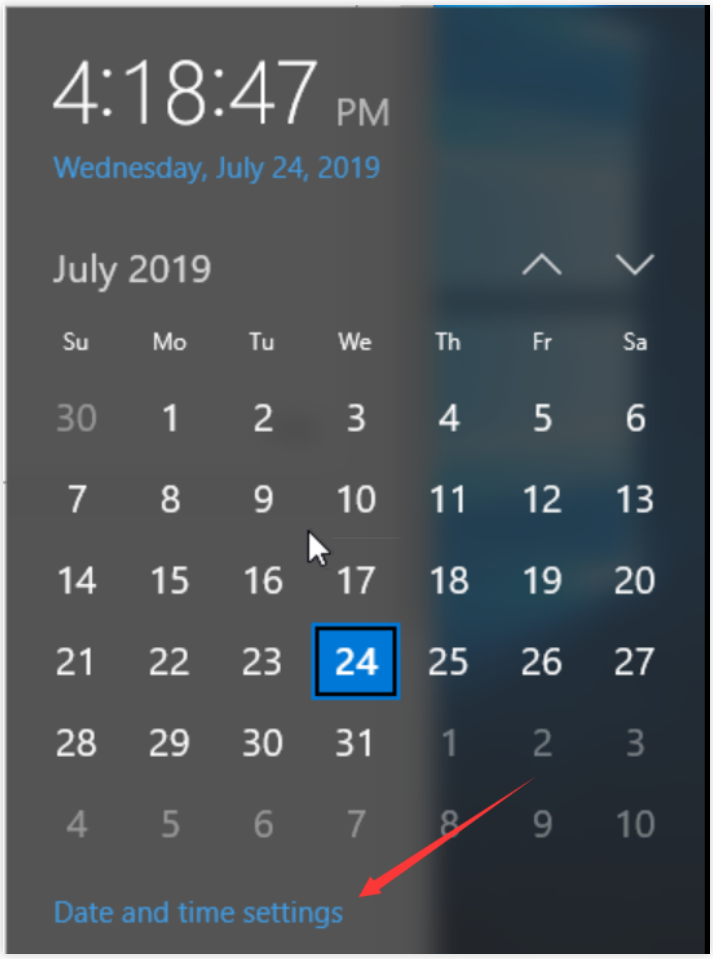
1. Windowsインスタンスへのリモートログイン。
2. 「管理 > サービス > Windows Time」をクリックします。



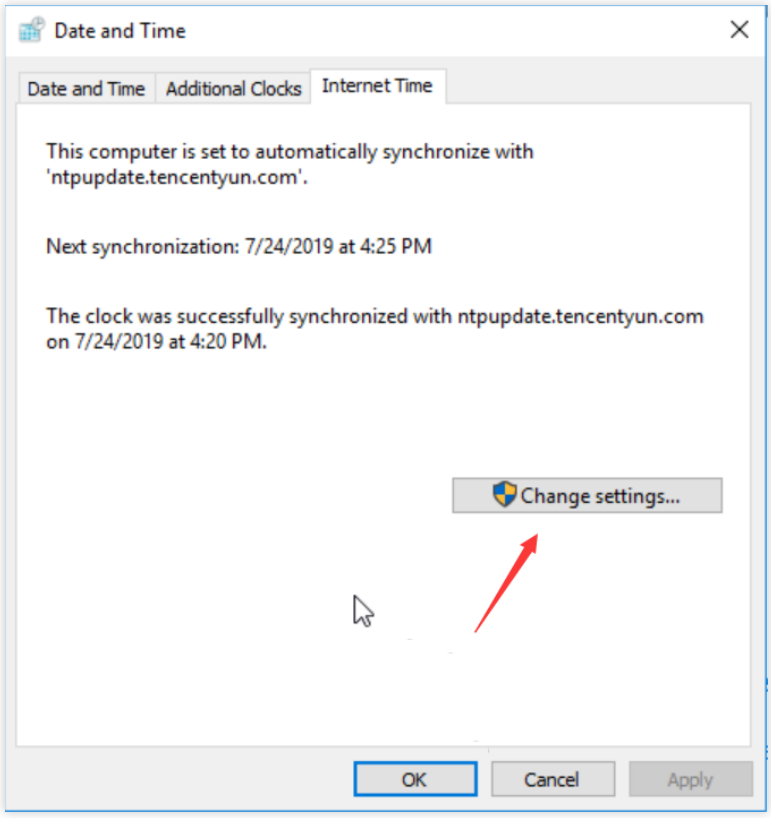
3. 起動の種類は「自動」に設定されています。サービスが起動されていない場合は、「起動」をクリックします。



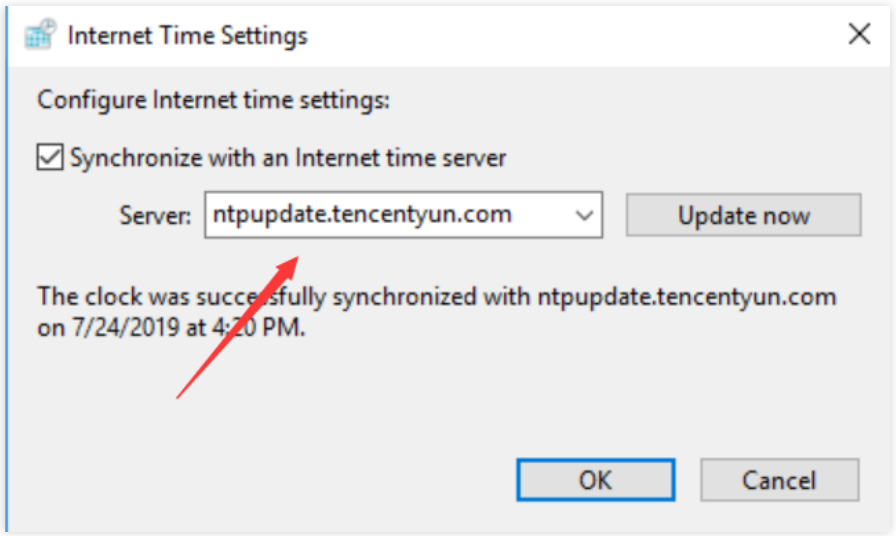
4. タスクバーの通知領域で、時刻をクリックし、「日付けと時刻」をクリックします。



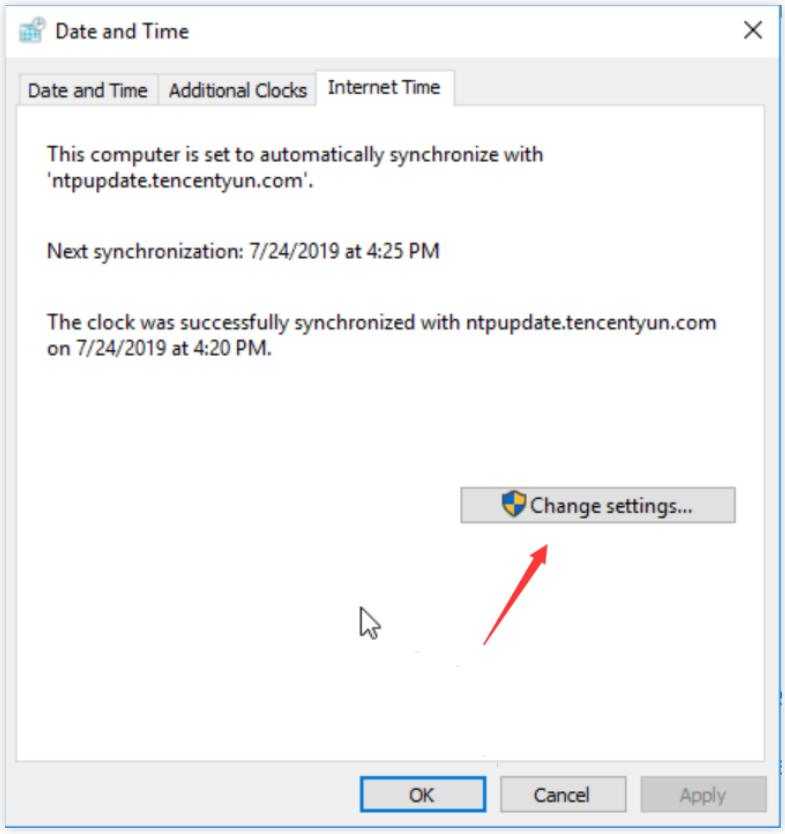
5. 「インターネット時刻」タグに切り替えて、設定の変更をクリックします。



6. Internet 時刻の設定ウィンドウで、ターゲットクロックソースサーバーのドメイン名またはIPアドレスを入力し、「OK」をクリックします。



7. 設定が完了したら、「日付と時刻」を再度開くと、クロックソースサーバーが変更されていることがわかります。



PostgreSQL マスターアーキテクチャとスレーブアーキテクチャの構築

最終更新日：：2023-02-16 11:41:05

概要

PostgreSQLは、拡張性と標準への準拠に焦点を重点に置いたオープンソースオブジェクトのリレーショナルデータベース管理システムです。PostgreSQLは、エンタープライズの複雑なSQL処理用のOLTPオンライントランザクション処理シナリオであり、NoSQLデータタイプ（JSON/XML/hstore）をサポートし、GIS（Geographic Information SystemまたはGeo－Information system）地理情報処理をサポートし、信頼性とデータ整合性の点で高い評判を得ています。インターネットのWebサイト、ロケーションアプリケーションシステム、複雑なデータオブジェクト処理などのアプリケーションシナリオに適しています。
このドキュメントでは、CentOS 7のCVMインスタンスでのPostgreSQLの構築方法について説明します。

ソフトウェアのバージョン

このドキュメントで作成されたPostgreSQLの構成およびバージョンの使用方法は次のとおりです：
Linux：Linux OSです。このドキュメントではCentOS 7.6を例として説明します。
PostgreSQL：リレーショナルデータベース管理システムです。このドキュメントでは、PostgreSQL 12を例として説明します。

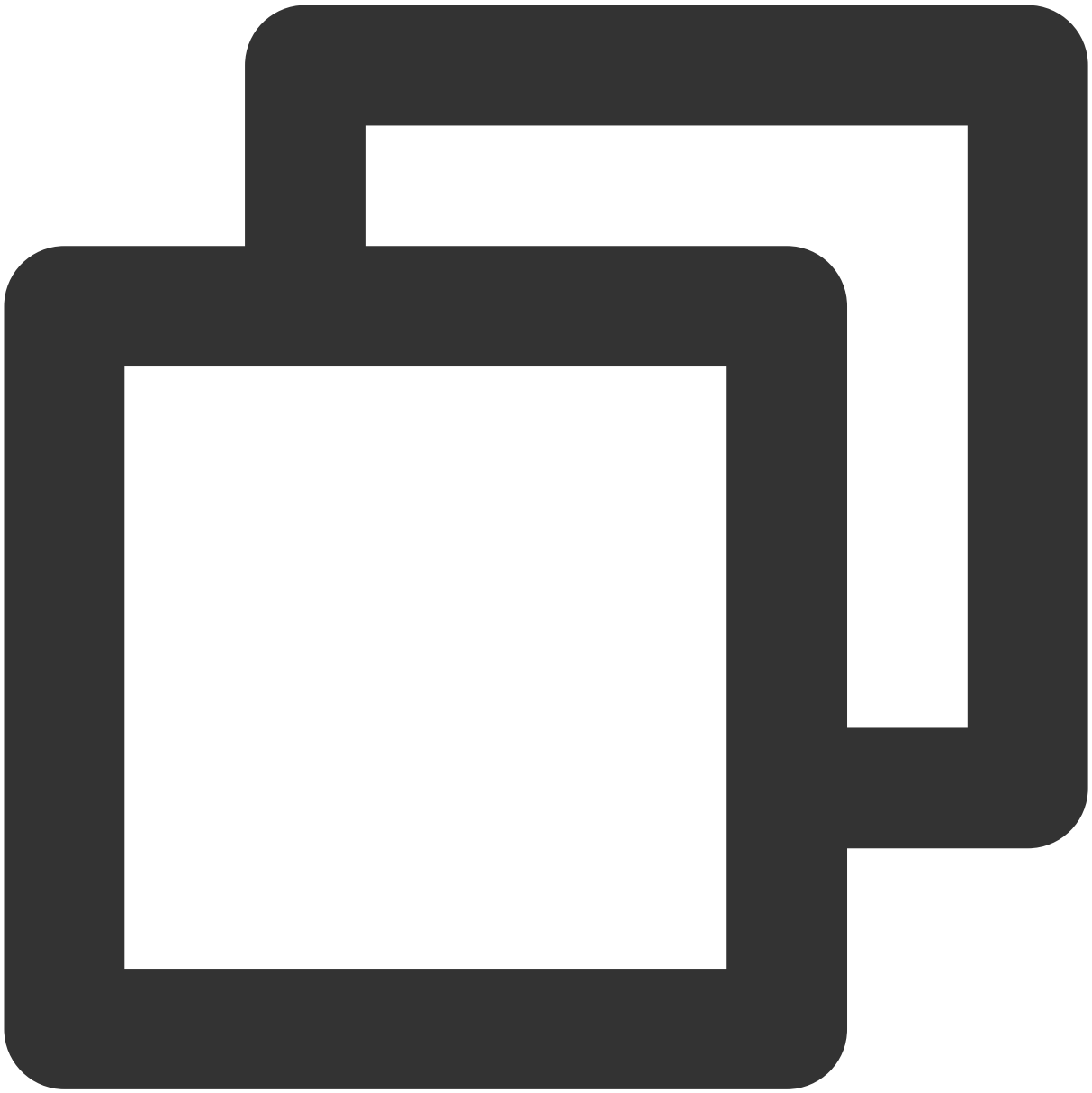
前提条件

2つのCVMインスタンスが作成されています（1つのCVMインスタンスがマスターノードとして機能し、もう1つのCVMインスタンスがスレーブノードとして機能します）。
具体的な手順については、購入ページでのインスタンスの作成 をご参照ください。
新しく作成された2つのCVMインスタンスは、セキュリティグループルールが構成されています。ポート5432がオープンされています。
具体的な手順については、セキュリティグループルールの追加 をご参照ください。

操作手順

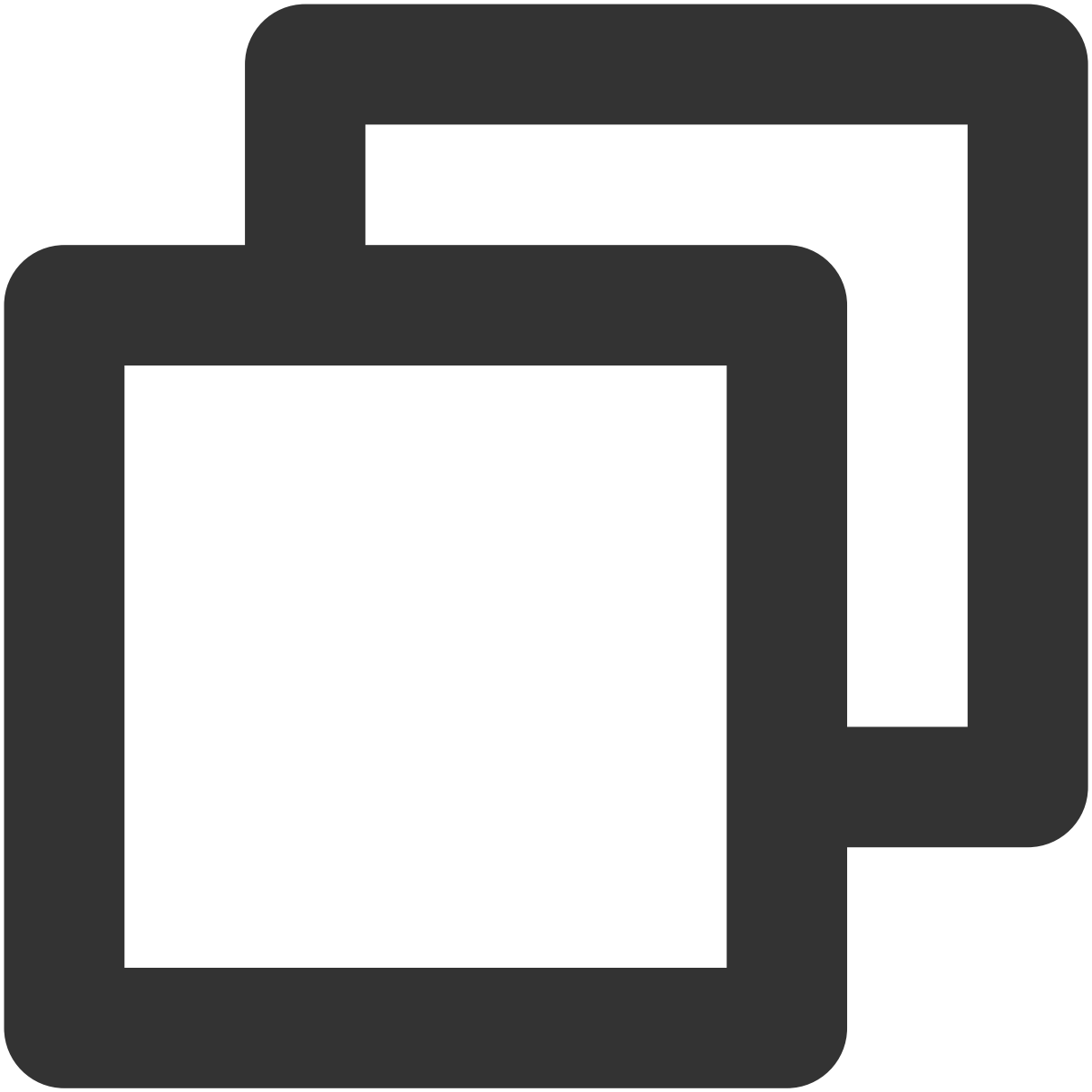
マスターノードの設定

1. マスターノードインスタンスにログインします。
2. 次のコマンドを実行して、すべてのパッケージ、システムバージョン、カーネルをアップグレードします。

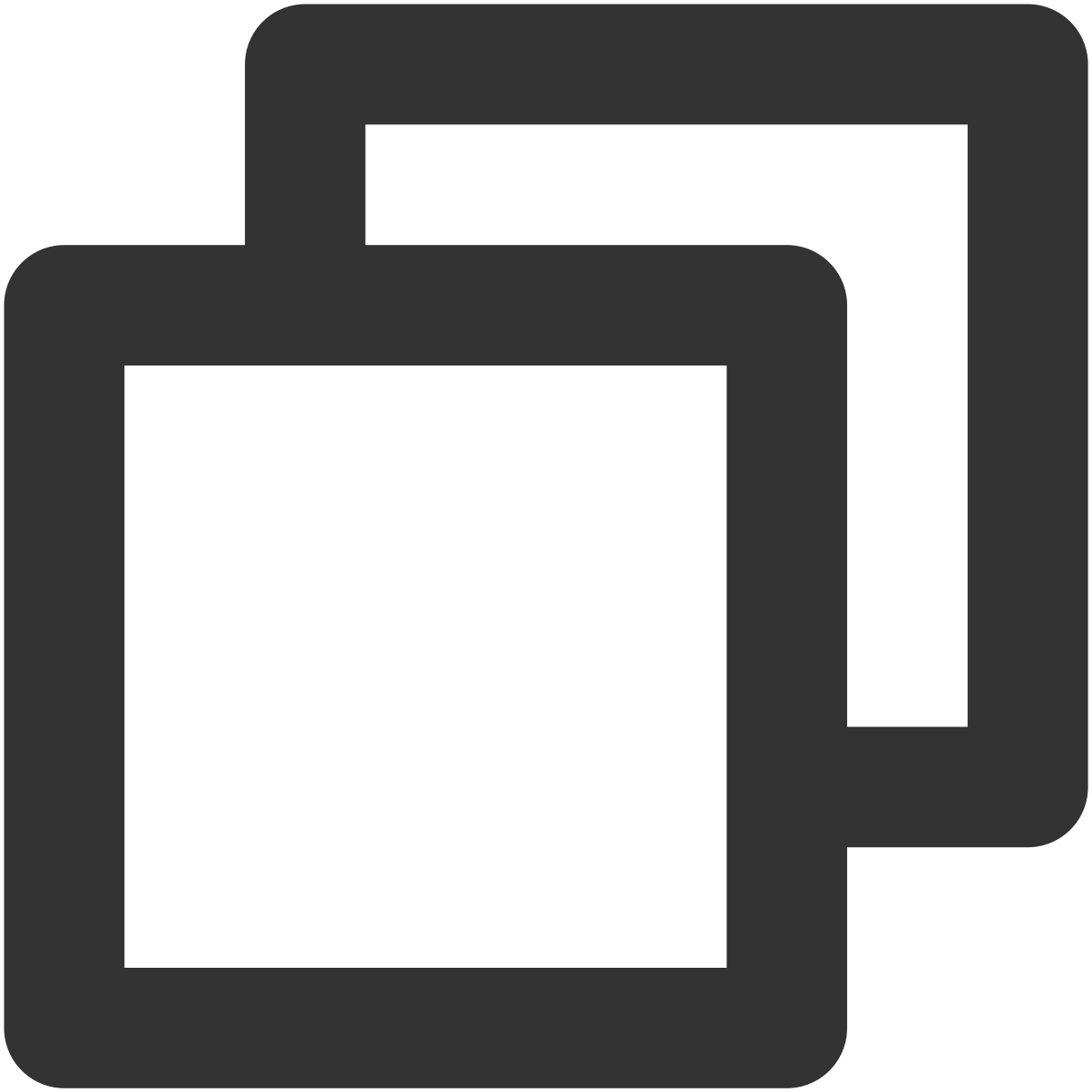


```
yum update -y
```

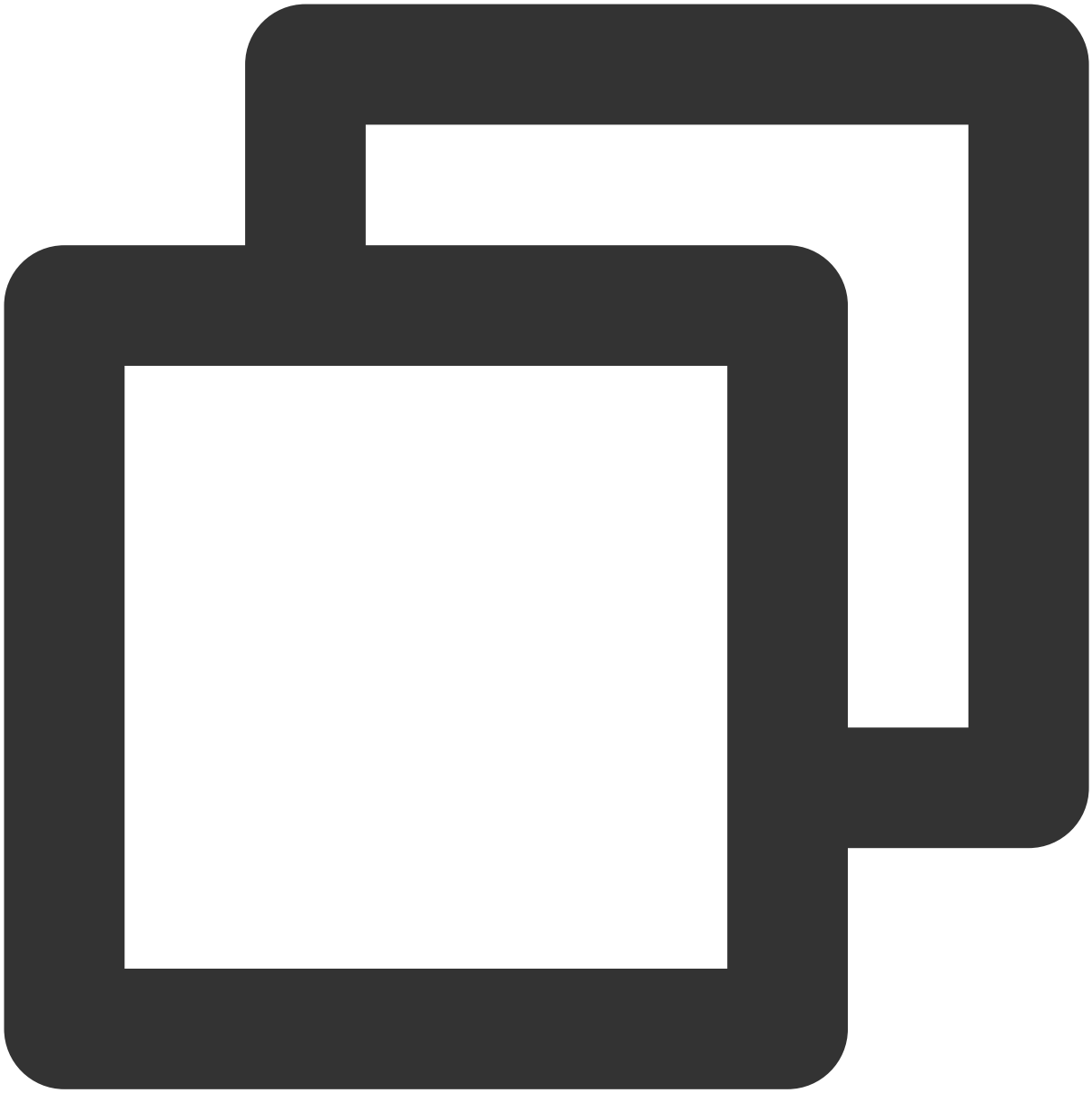
3. 次のコマンドを順番に実行して、PostgreSQLをインストールします。
このドキュメントでは、PostgreSQL 12バージョンを例として説明しますが、必要に応じてその他のバージョンを選択することもできます。



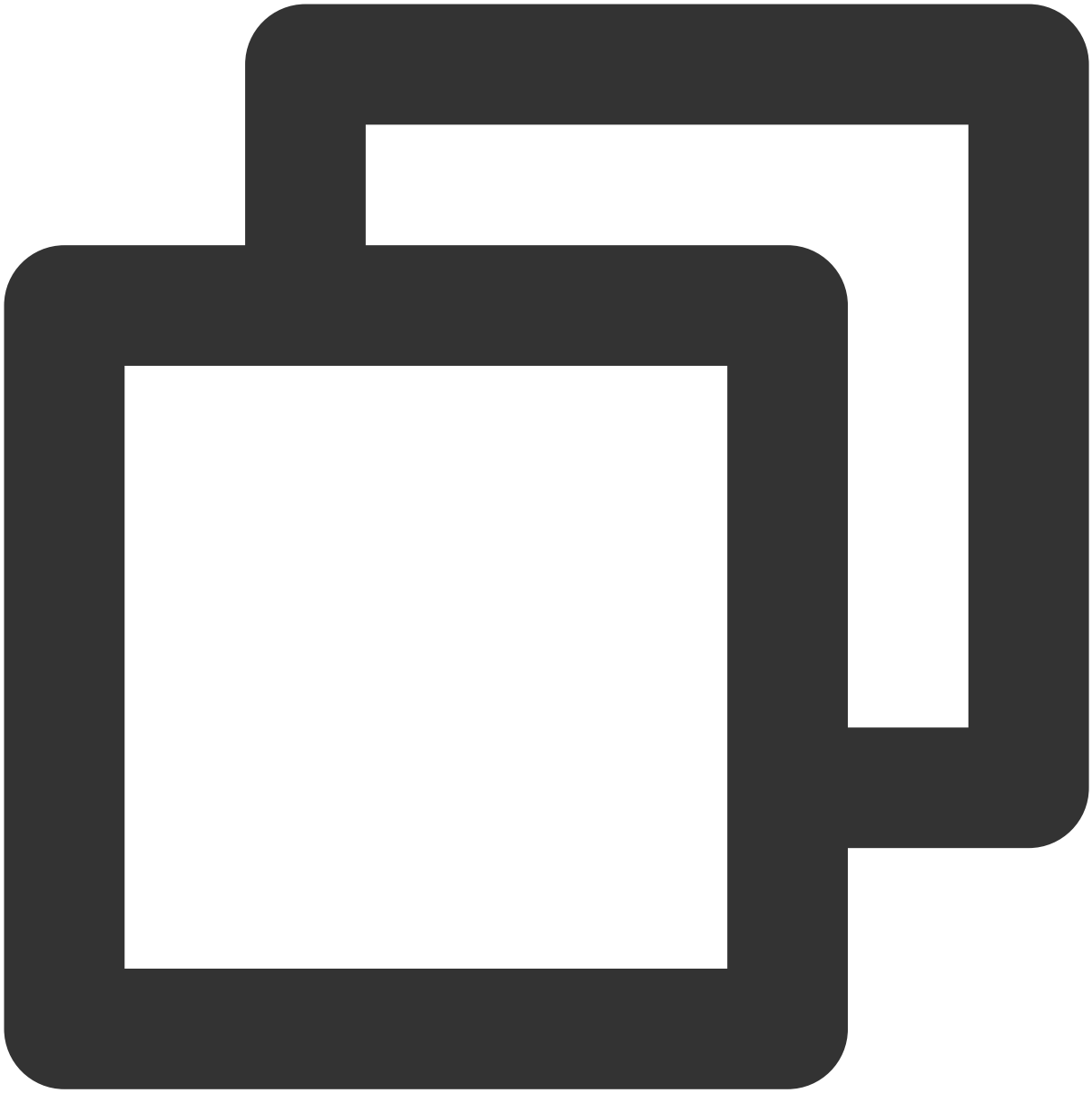
```
wget --no-check-certificate https://download.postgresql.org/pub/repos/yum/reporpms/
```



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

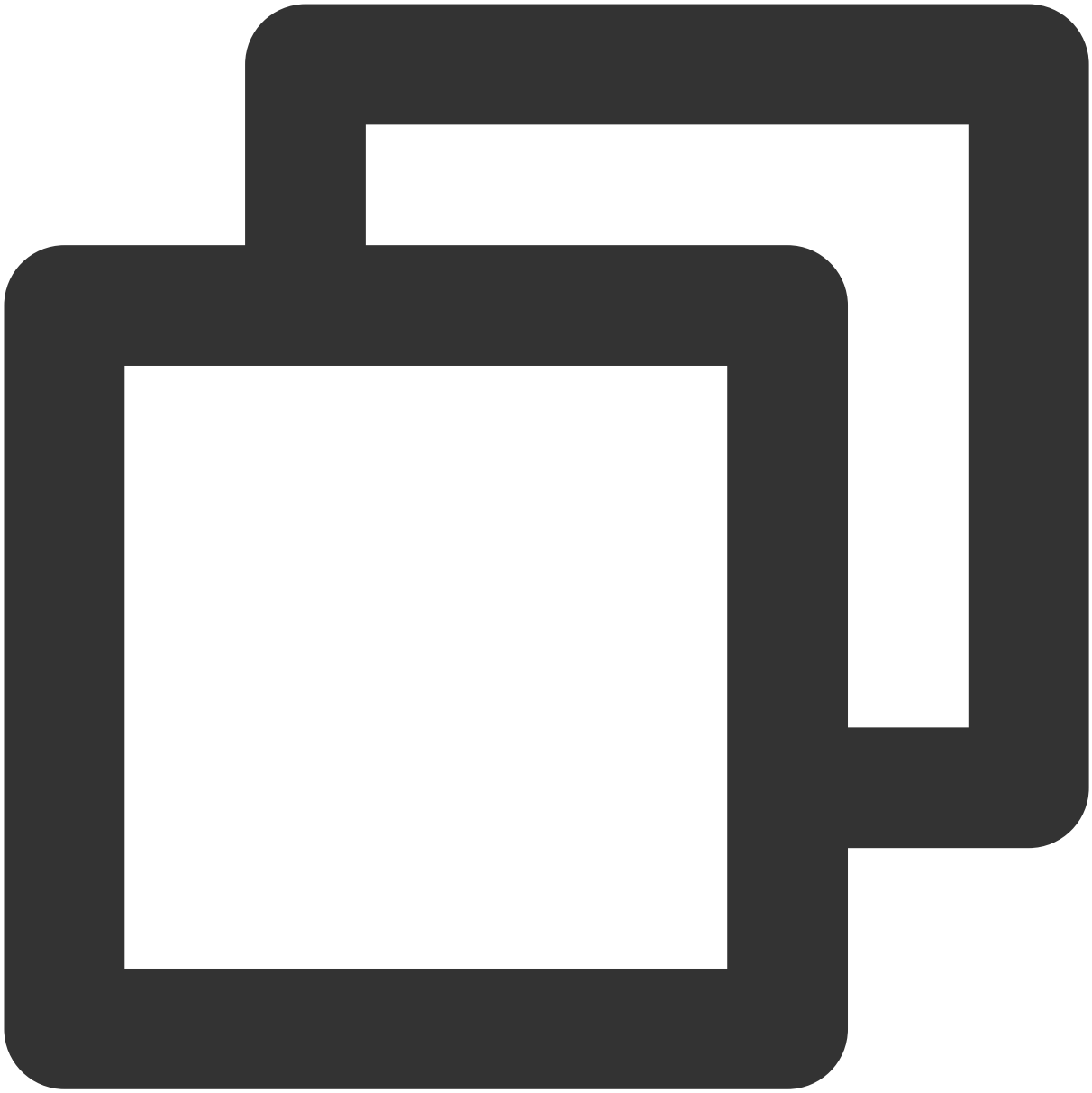


```
yum install postgresql12-server postgresql12-contrib -y
```



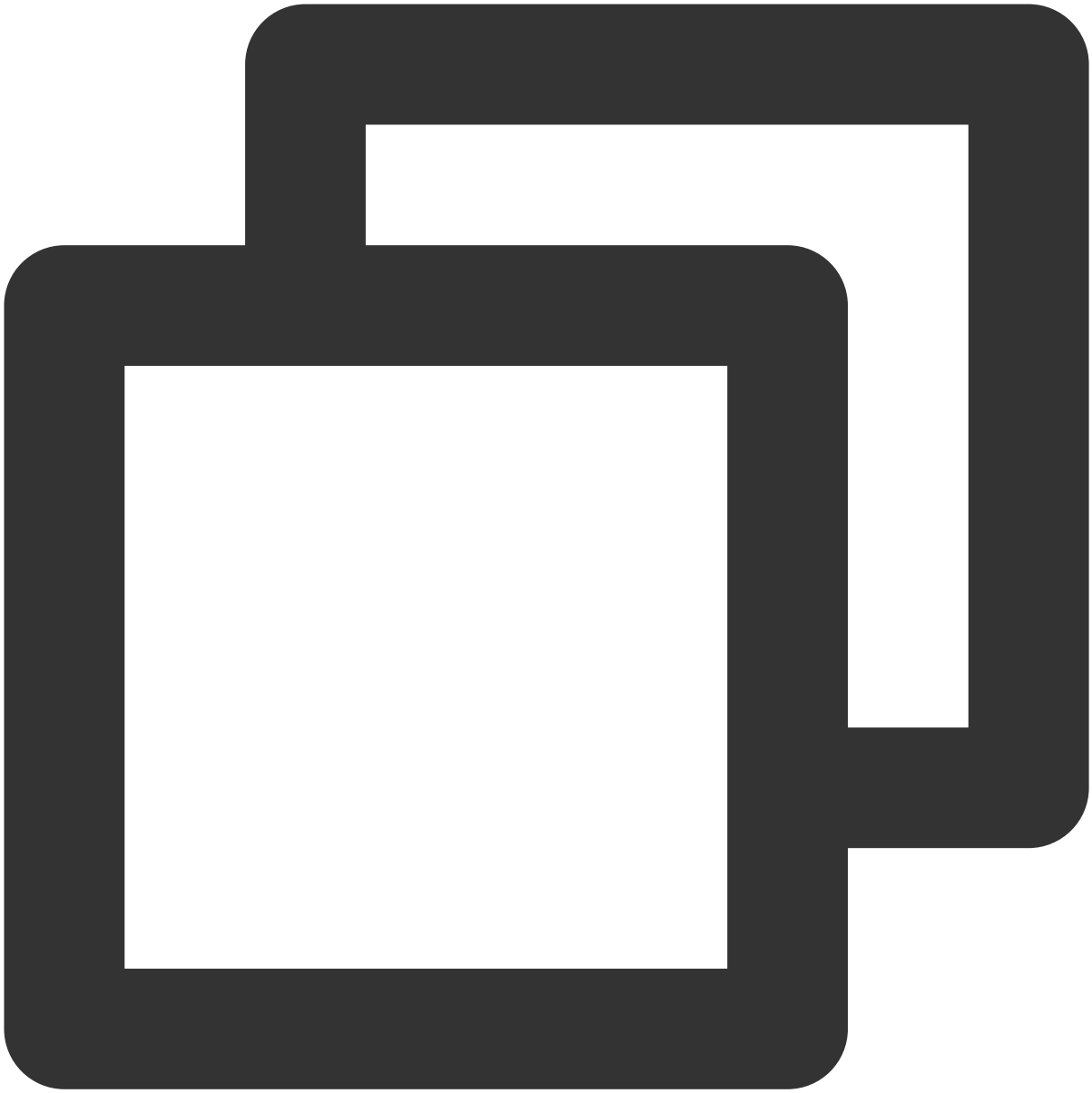
```
/usr/pgsql-12/bin/postgresql12-setup initdb
```

4. 次のコマンドを実行して、サービスを起動します。



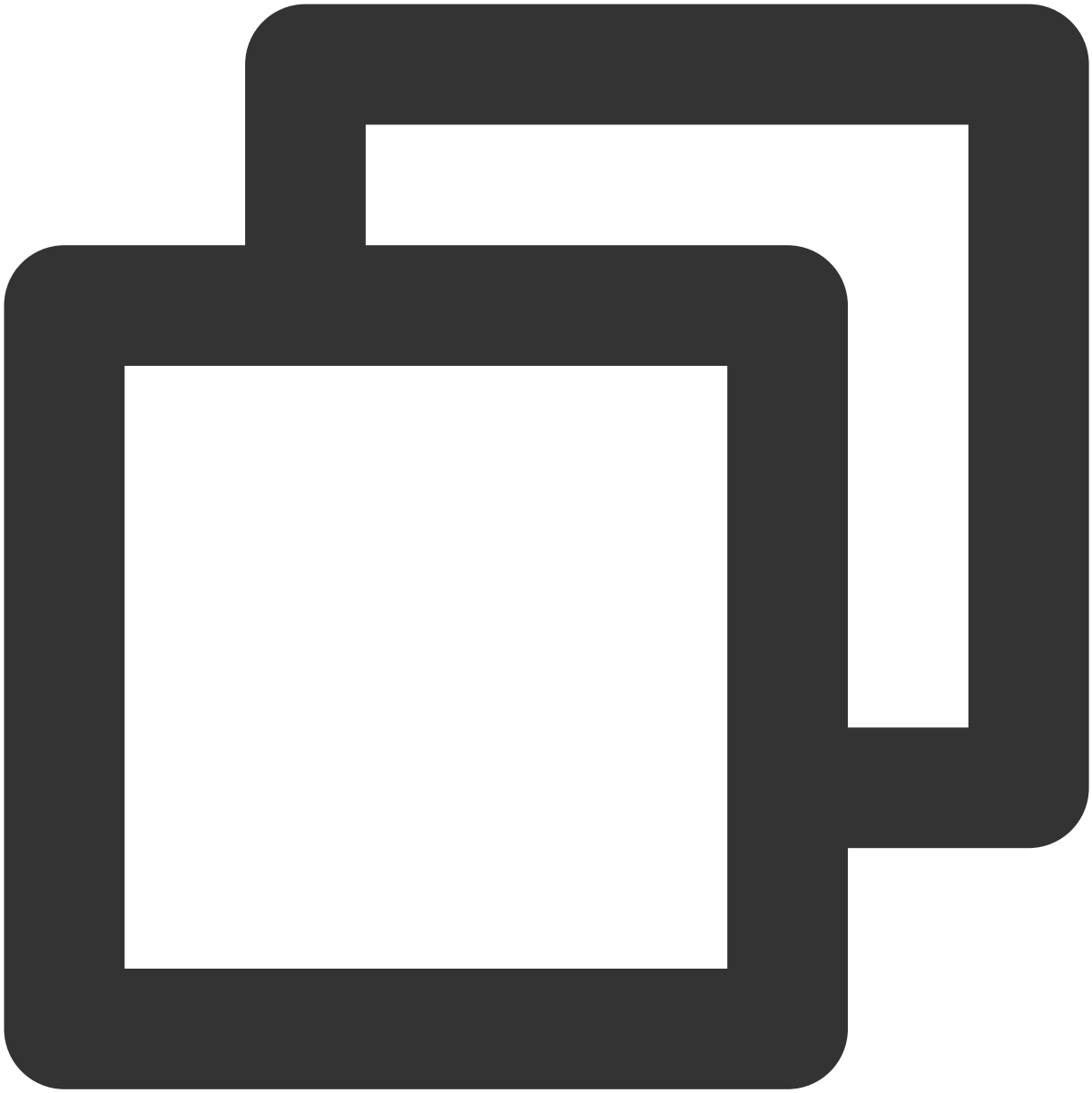
```
systemctl start postgresql-12.service
```

5. 次のコマンドを実行して、起動時に自動的にサービスを開始するように設定します。



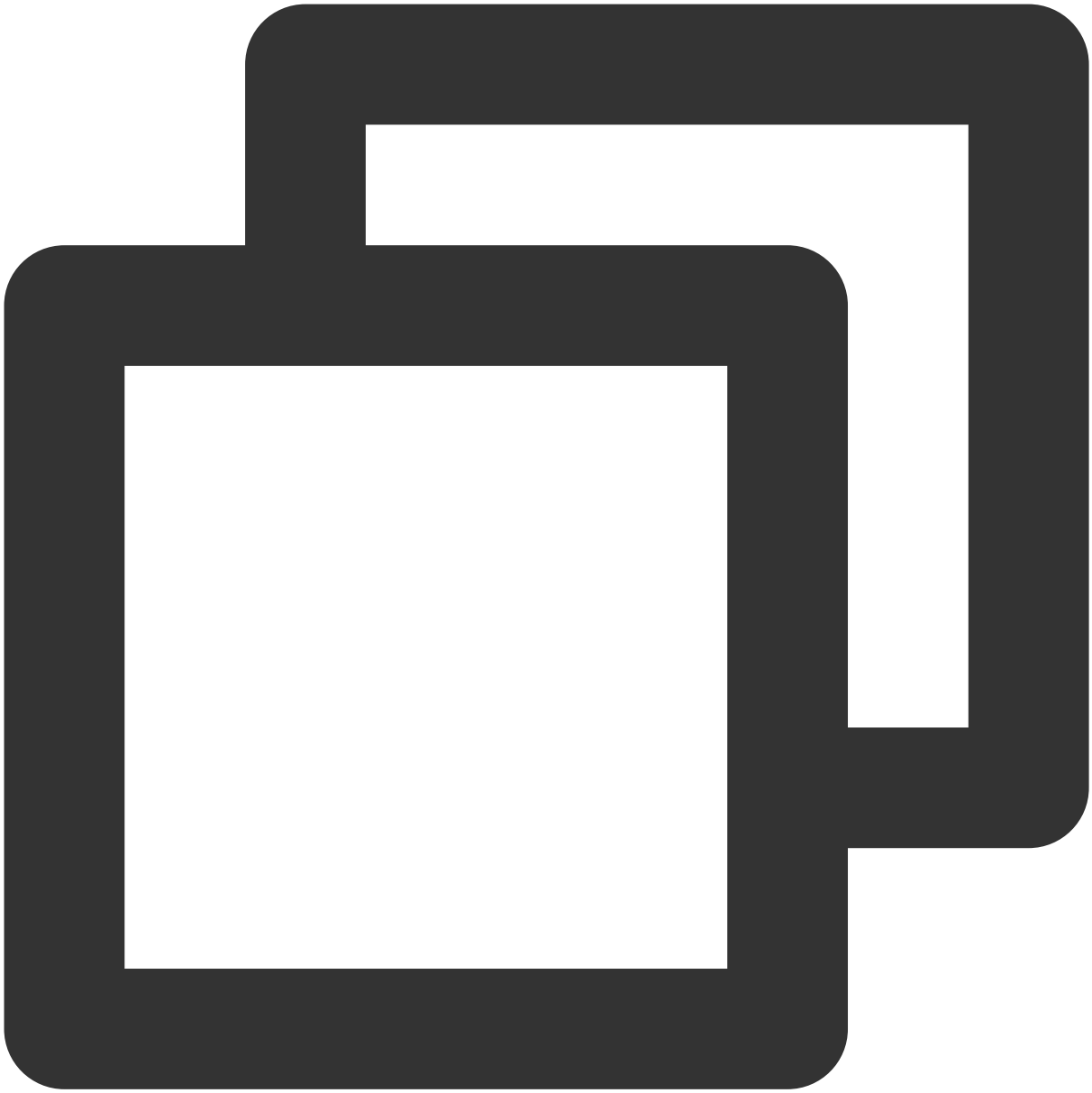
```
systemctl enable postgresql-121.service
```

6. 次のコマンドを実行して、postgresユーザーにログインします。



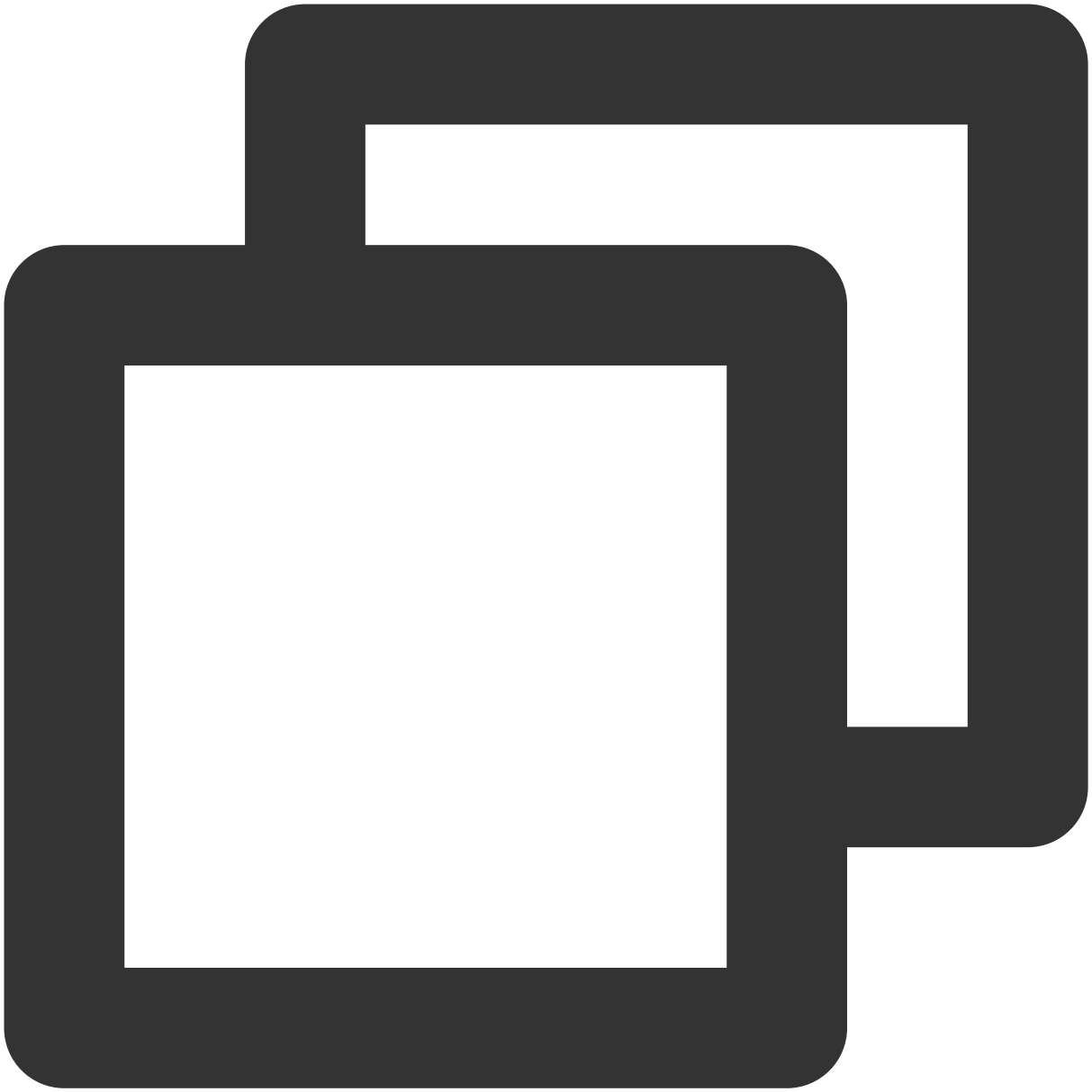
```
su - postgres
```

7. 次のコマンドを実行して、PostgreSQLインタラクティブ端末に入ります。



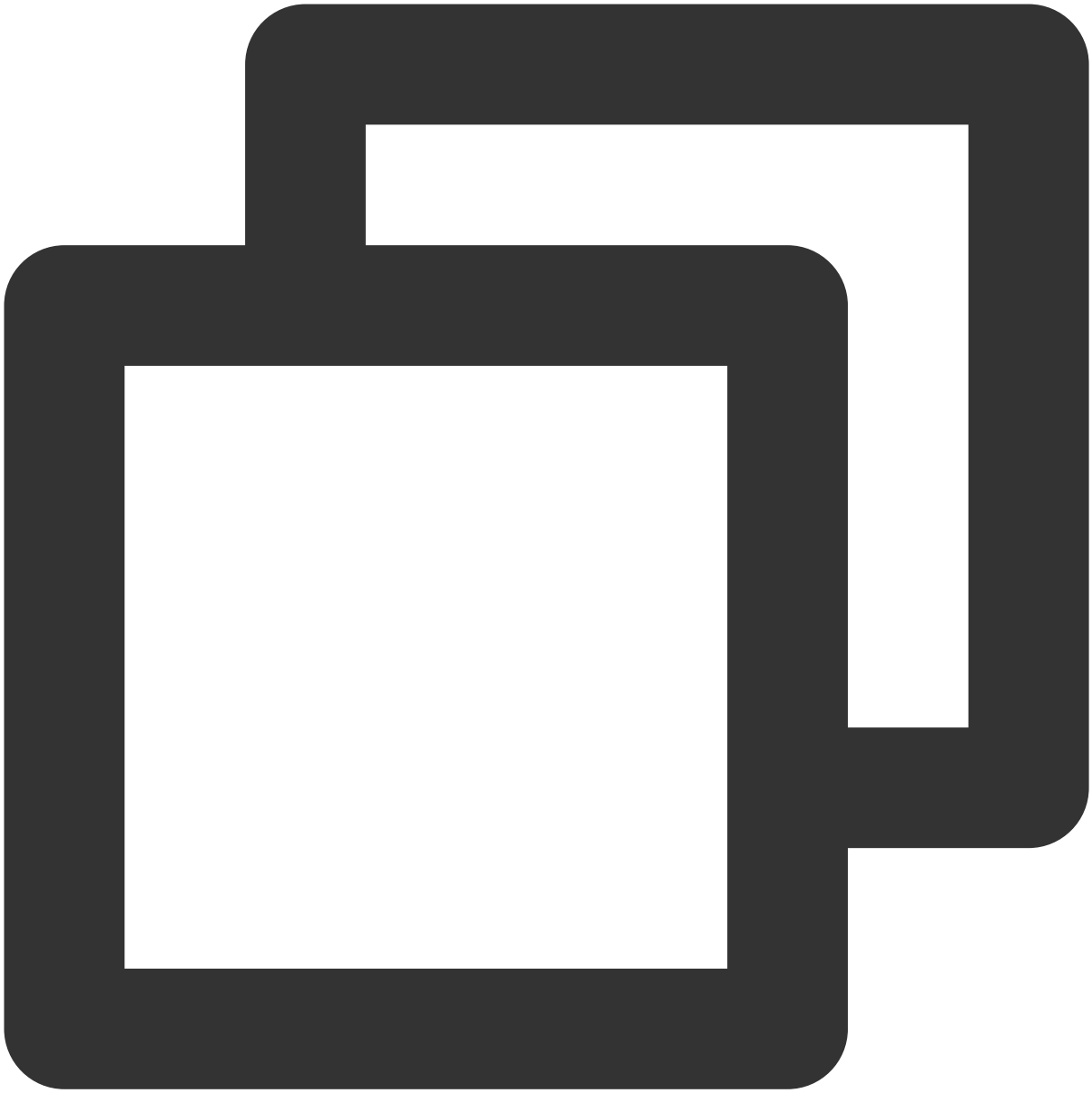
```
psql
```

8. 次のコマンドを実行して、ユーザーpostgresのパスワードを設定して、セキュリティを強化します。



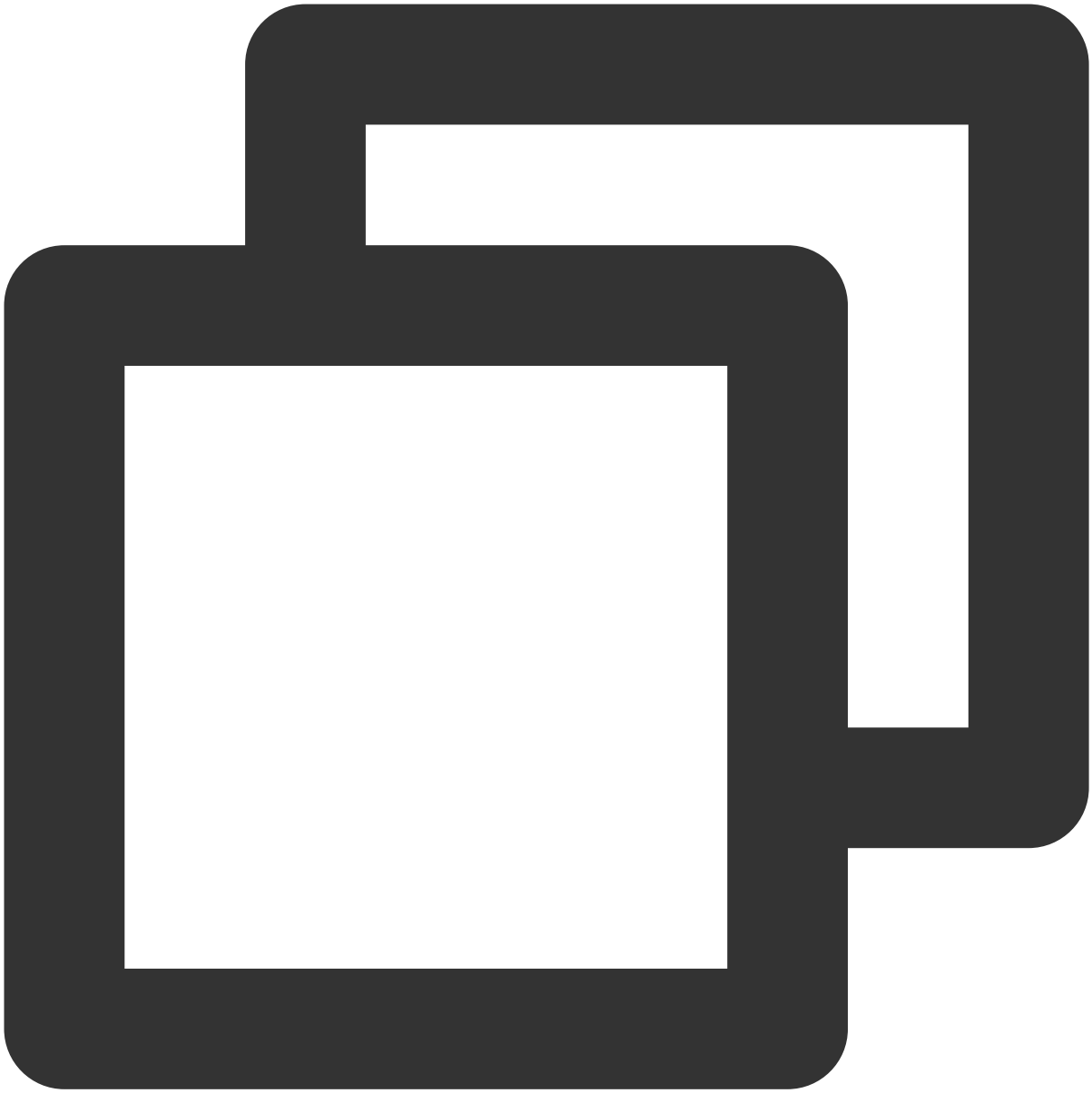
```
ALTER USER postgres WITH PASSWORD '自定义密码';
```

9. 次のコマンドを実行して、データベースのアカウントを作成し、パスワード、ログイン権限、バックアップ権限を設定します。



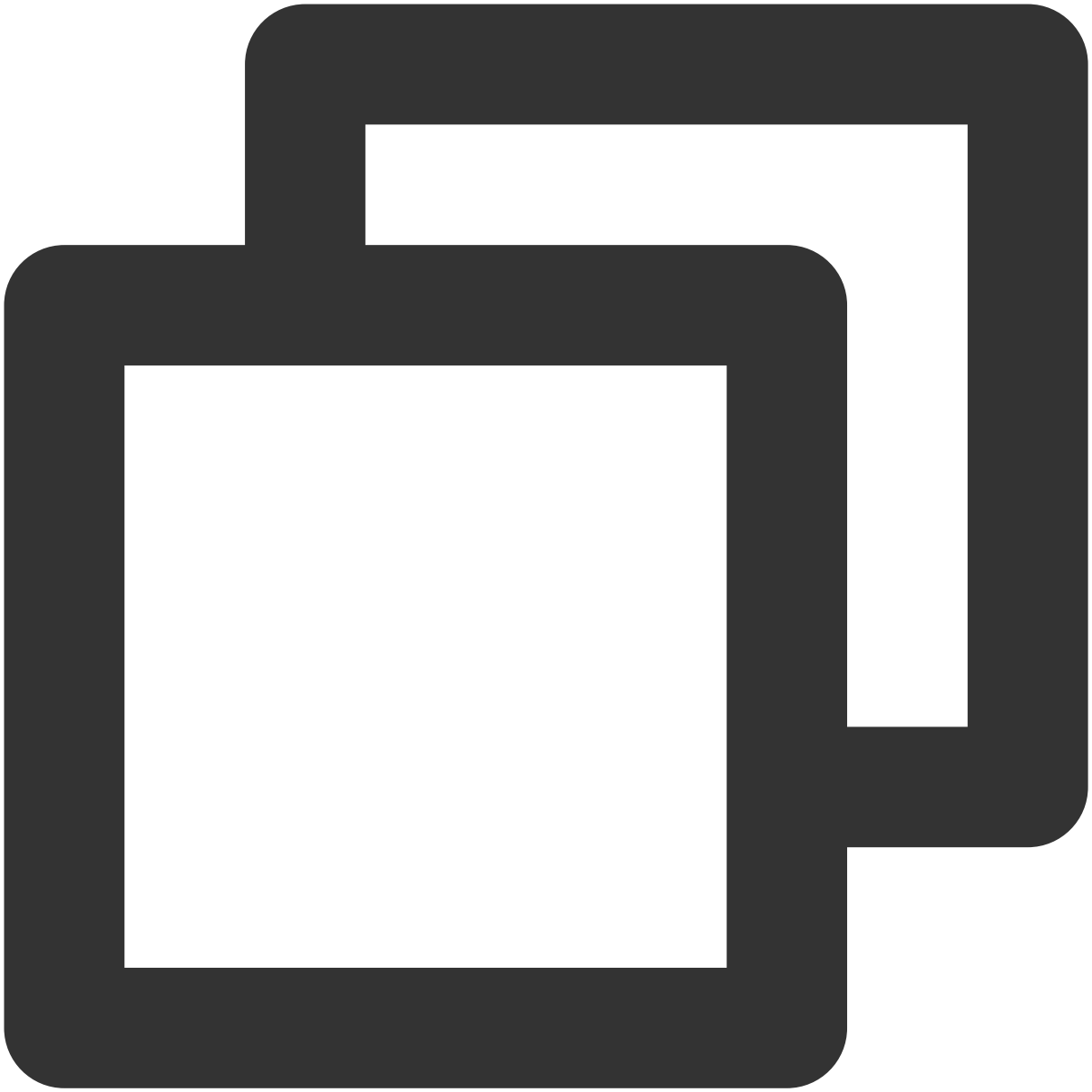
```
create role アカウント名 login replication encrypted password 'カスタマイズパスワード';
```

このドキュメントでは、次のコマンドを実行して、データベースアカウント `replica` およびパスワード `123456` の作成を例として説明します。



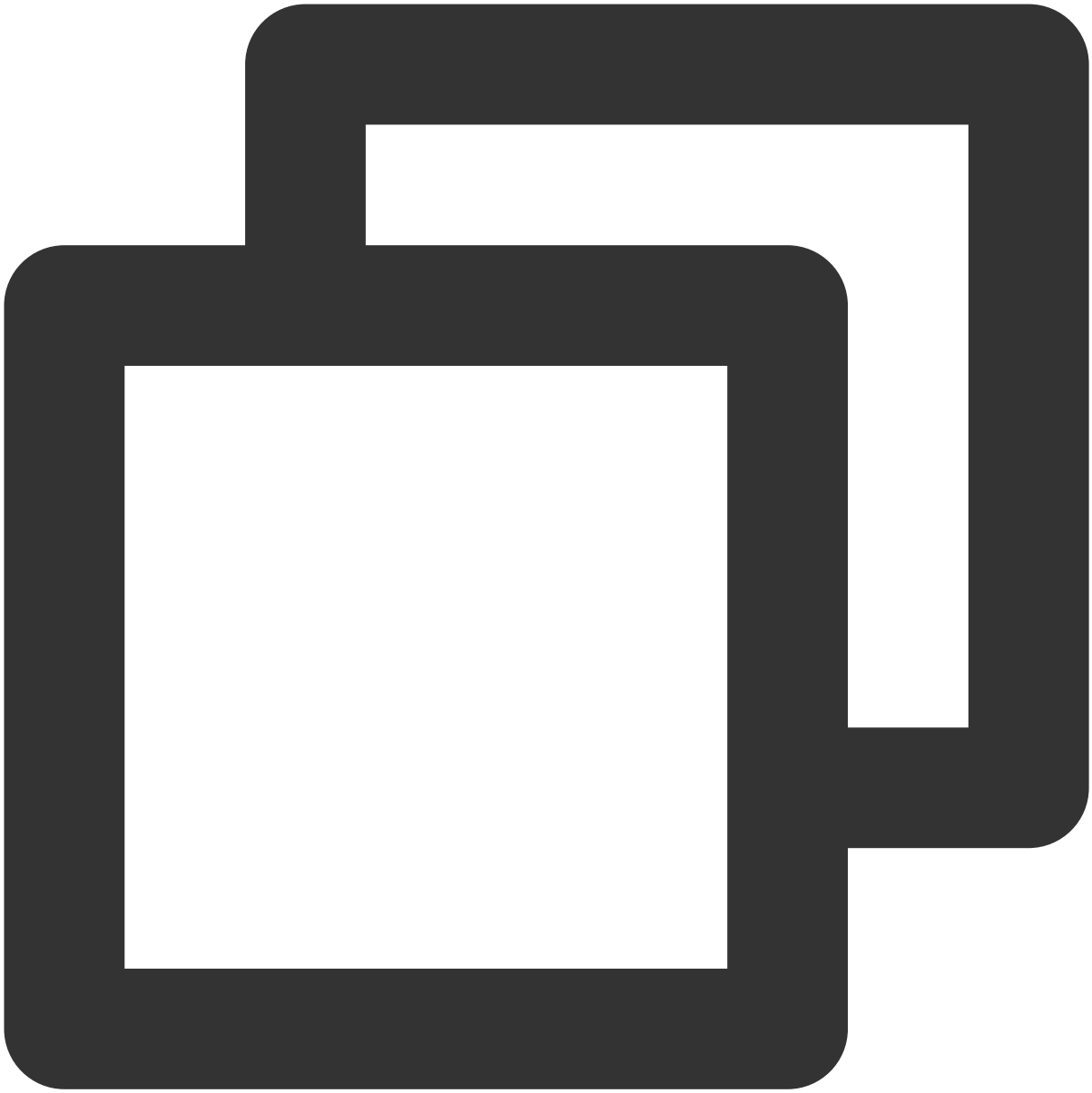
```
create role replica login replication encrypted password '123456';
```

10. 次のコマンドを実行して、アカウントが正常に作成されたかどうかを確認します。



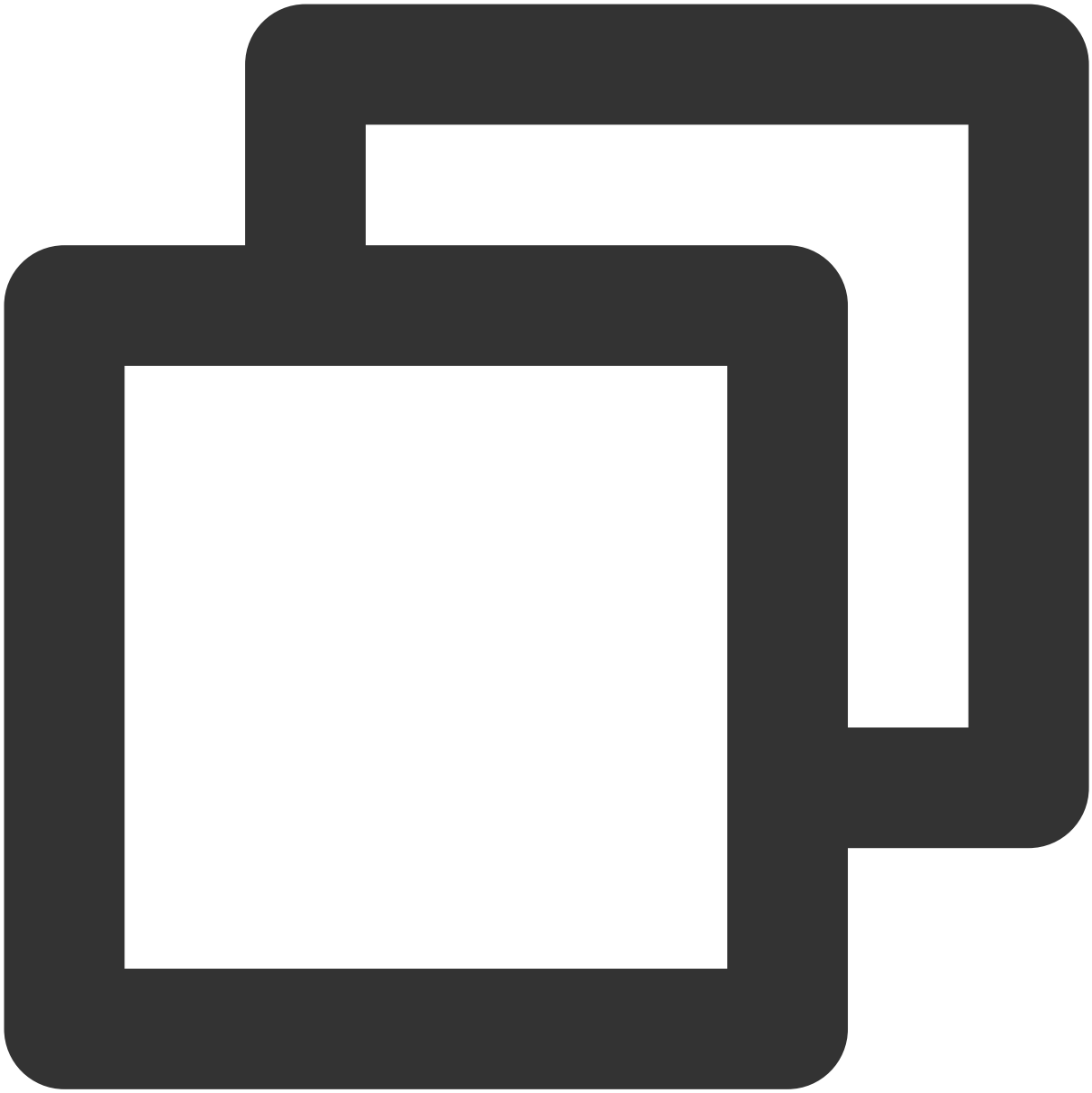
```
SELECT usename from pg_user;
```

次の結果が返された場合、正常に作成されたことを示します。



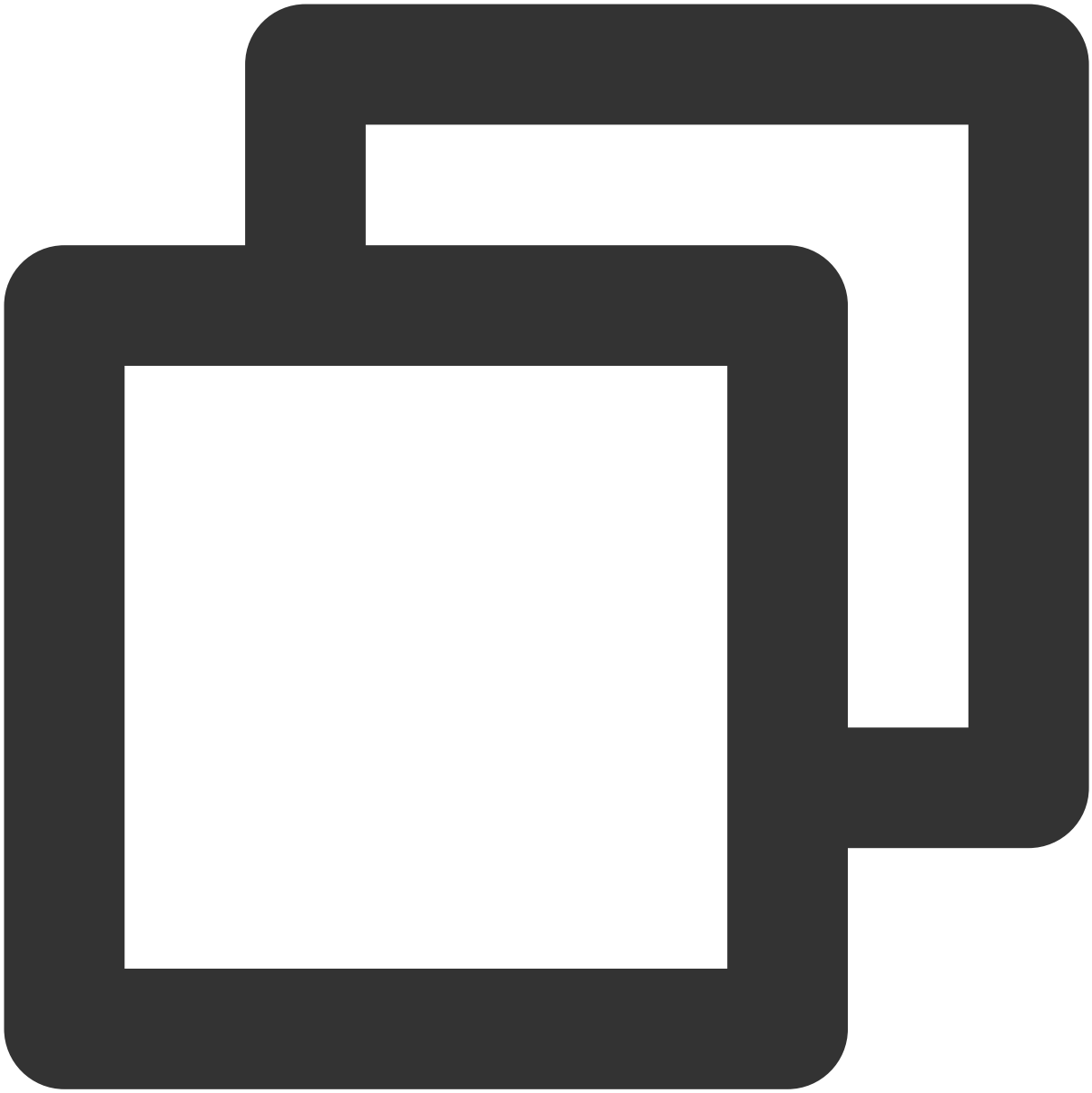
```
usename
----------
postgres
replica
(2 rows)
```

11. 次のコマンドを実行して、権限が正常に作成されたかどうかを確認します。



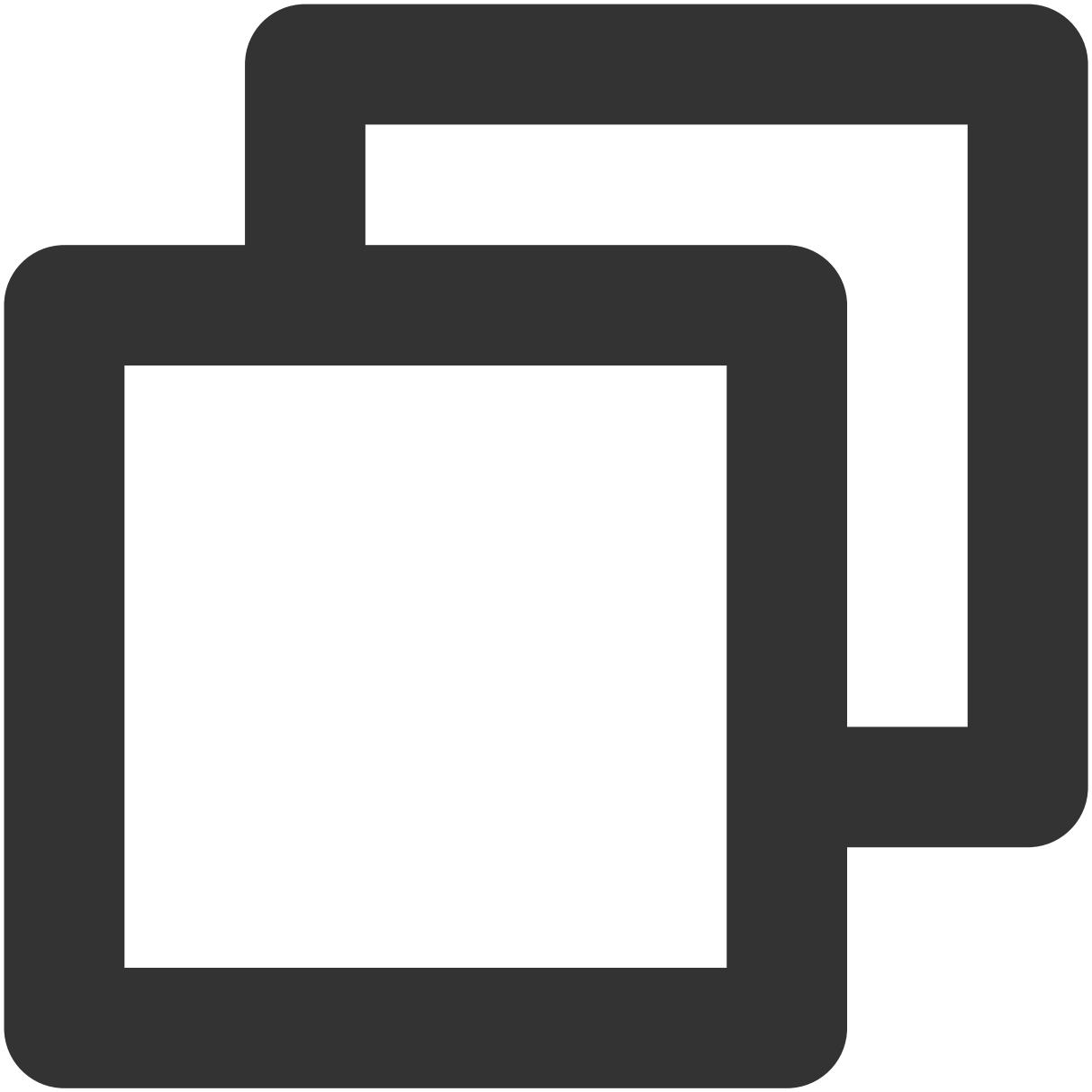
```
SELECT rolname from pg_roles;
```

次の結果が返された場合、正常に作成されたことを示します。



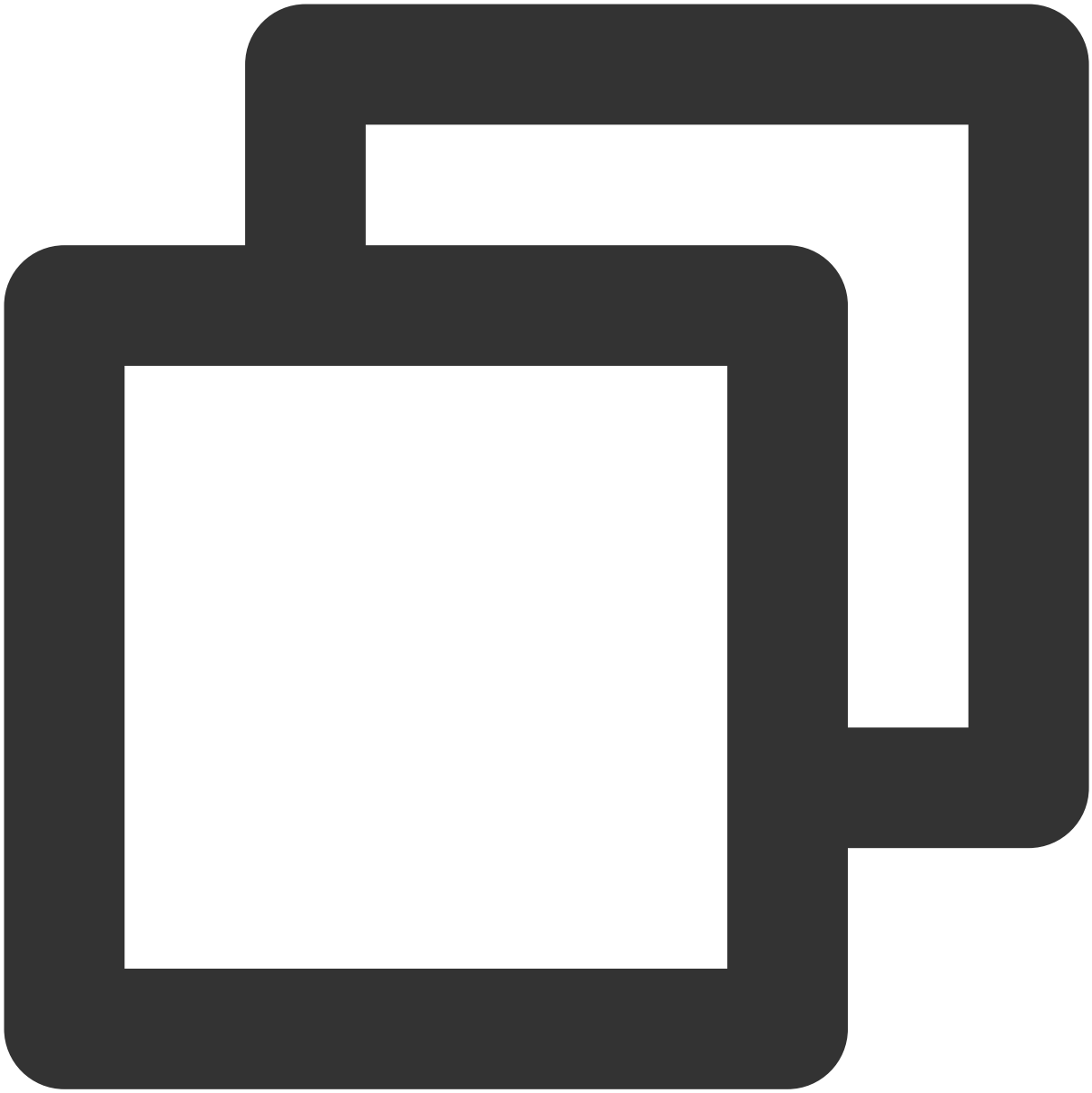
```
rolname
-------------------
pg_signal_backend
postgres
replica
(3 rows)
```

12. 「\\q」を入力し、Enterを押して、SQL端末を終了します。
13. 「exit」を入力し、Enterを押して、PostgreSQLを終了します。
14. 次のコマンドを実行して、pg_hba.conf設定ファイルを開き、replicaユーザーホワイトリストを設定します。



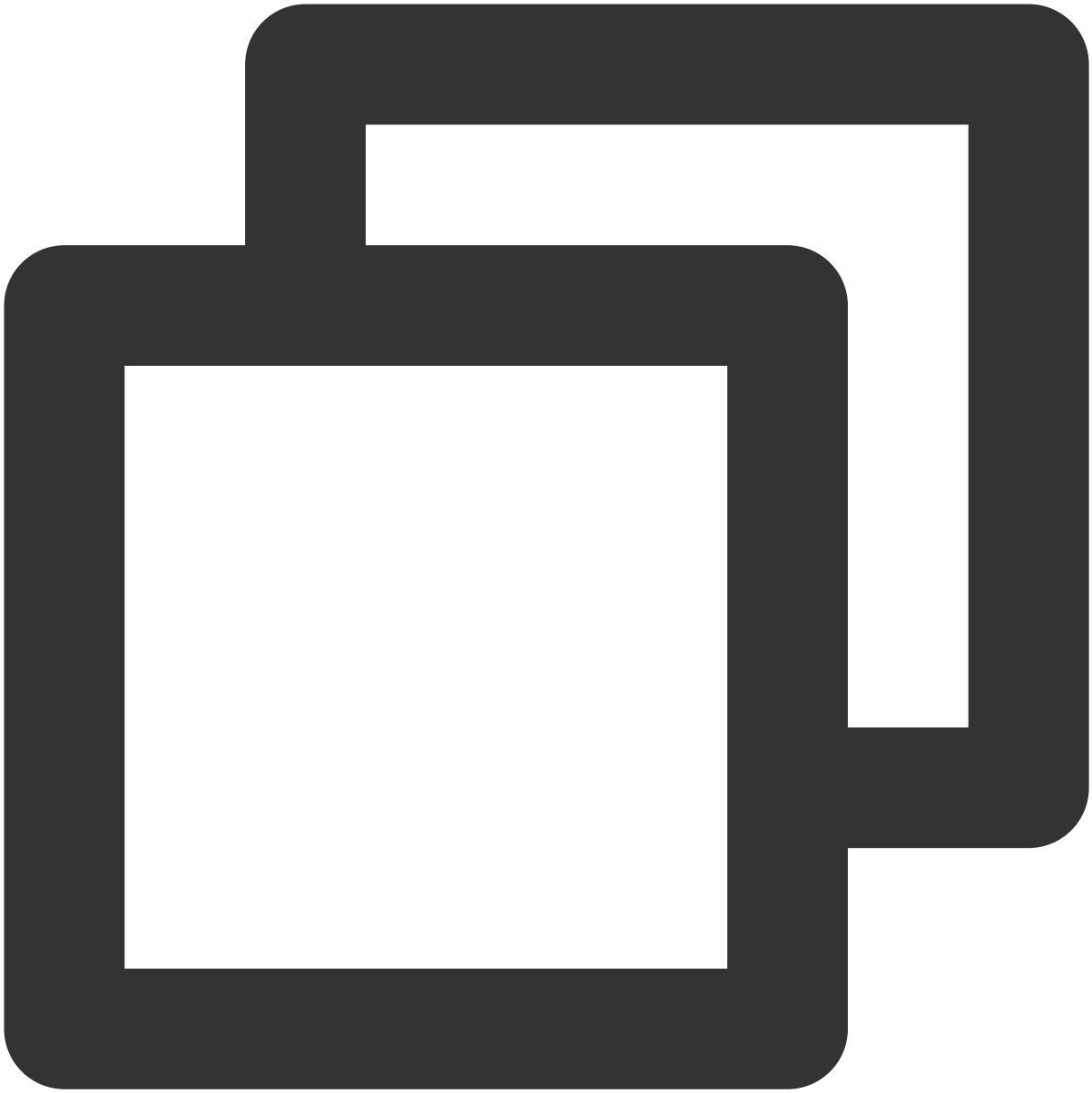
```
vim /var/lib/pgsql/12/data/pg_hba.conf
```

15. iを押して編集モードに切り替え、IPv4 local connectionsセクションに次の2行を追加します：



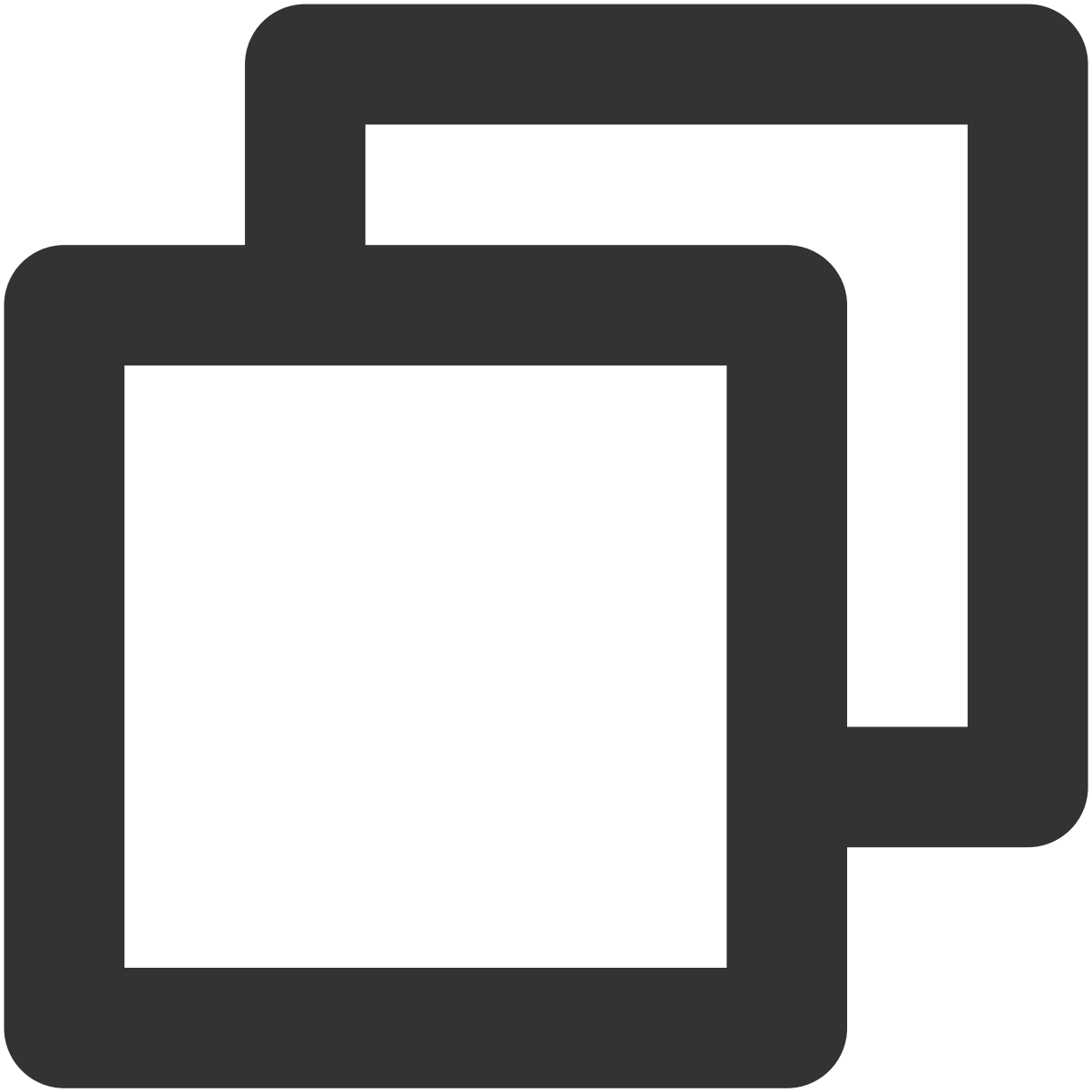
```
host    all             all             <スレーブノードのVPC IPv4セグメント>          m
host    replication     replica         <スレーブノードのVPC IPv4セグメント>          m
```

例えば、データベースアカウントがreplicaで、スレーブノードのVPC IPv4セクションがxx.xx.xx.xx/16である場合、IPv4 local connectionsセクションに次の内容を追加します。



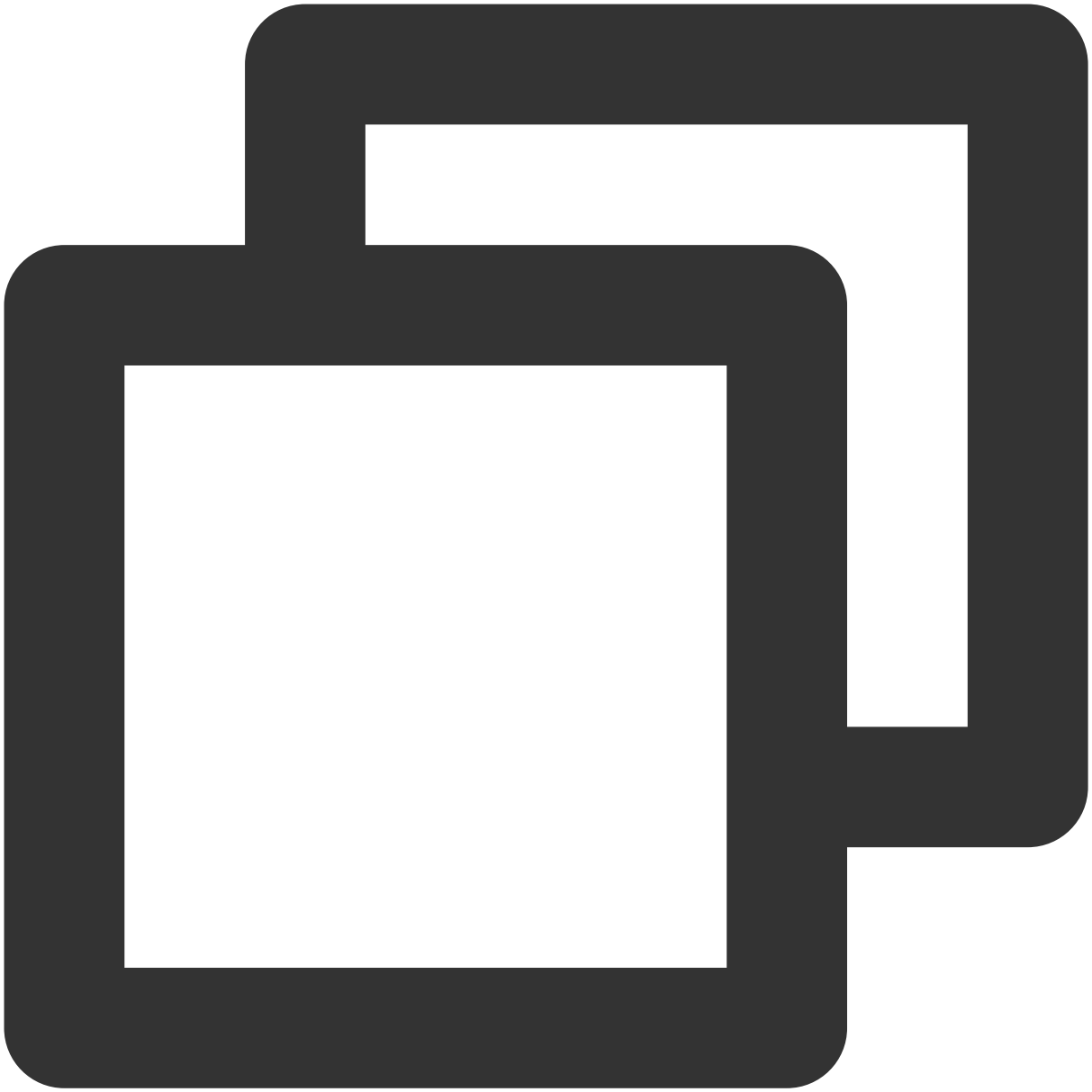
```
host    all             all             xx.xx.xx.xx/16          md5
host    replication     replica         xx.xx.xx.xx/16          md5
```

16. Escを押し、:wqを入力して、ファイルを保存して戻ります。
17. 次のコマンドを実行して、postgresql.confファイルを開きます。



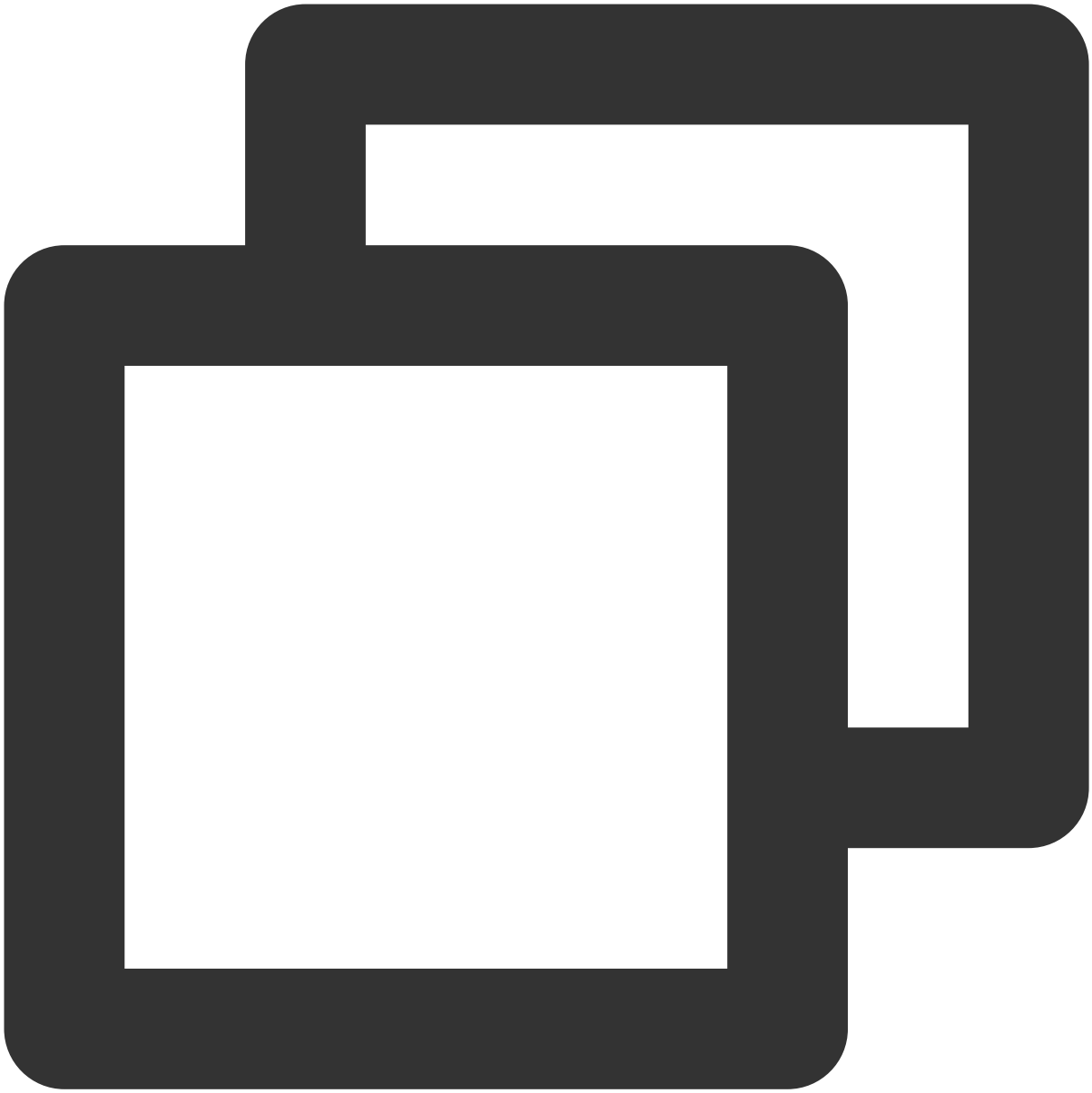
```
vim /var/lib/pgsql/12/data/postgresql.conf
```

18. iを押して編集モードに入り、次のパラメータをそれぞれ見つけて、パラメータを次のように変更します：



```
listen_addresses = '*'    #モニタリングされているプライベートネットワークIPアドレス
max_connections = 100     #接続の最大数です。スレーブデータベースのmax_connectionsはマスター
wal_level = hot_standby   #ホットバックアップモードを有効にする
synchronous_commit = on   #同期レプリケーションを有効にする
max_wal_senders = 32      #同期プロセスの最大数
wal_sender_timeout = 60s #ストリーミングレプリケーションホストがデータを送信するためのタイムア
```

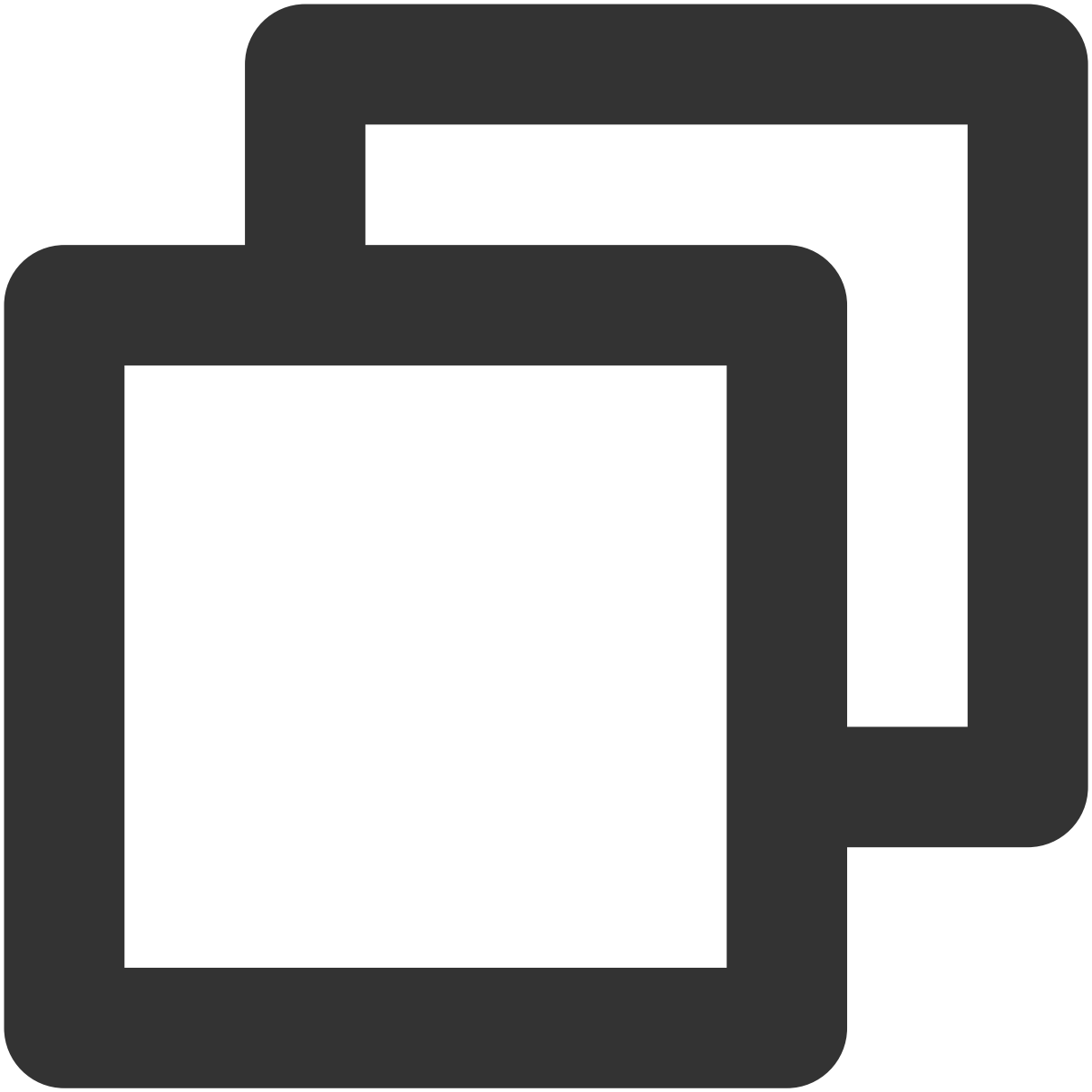
19. Escを押し、:wqを入力して、ファイルを保存して戻ります。
20. 次のコマンドを実行して、サービスを再起動します。



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

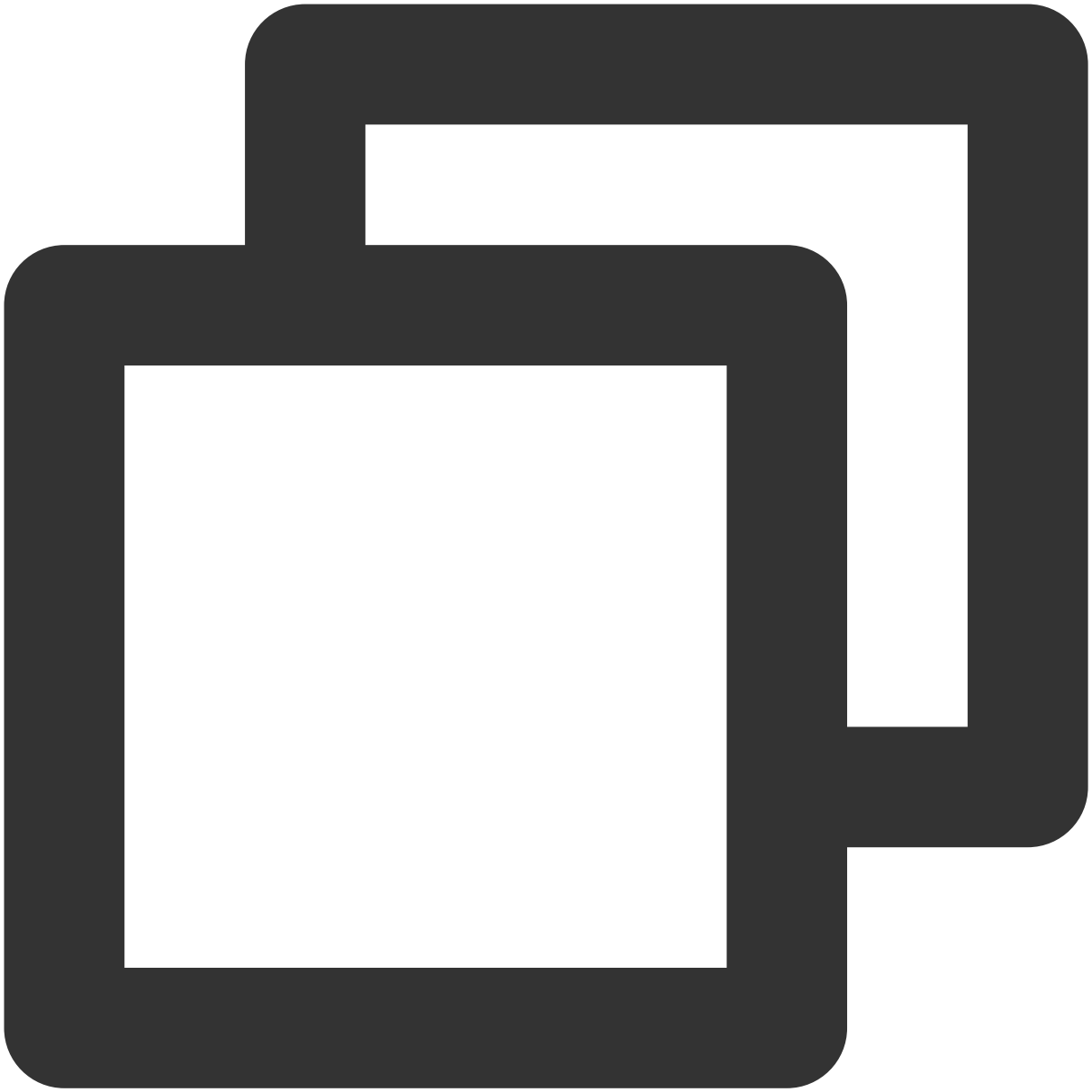
スレーブノードの設定

1. スレーブノードインスタンスにログインします。
2. 次のコマンドを実行して、すべてのパッケージ、システムバージョン、カーネルをアップグレードします。

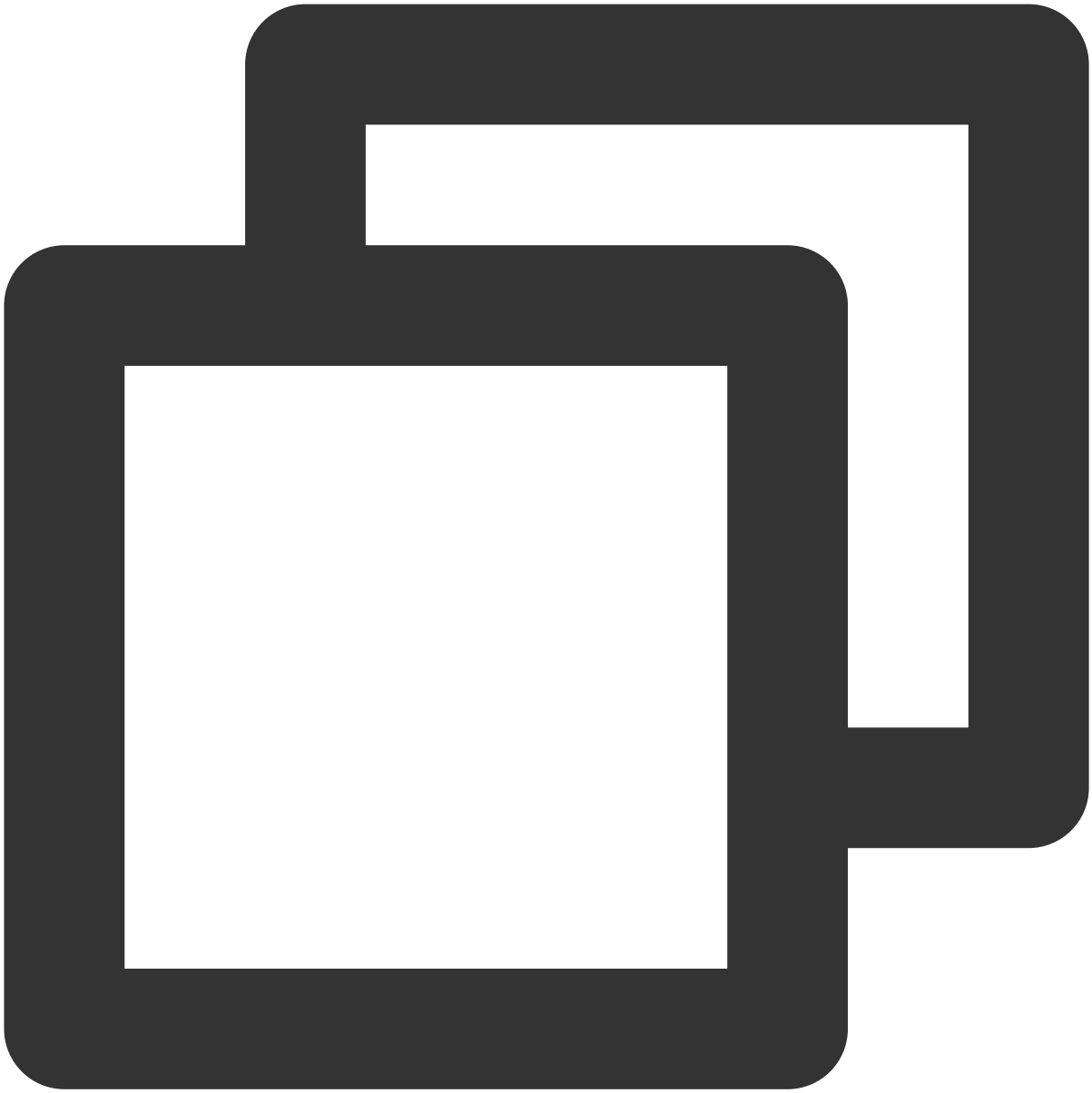


```
yum update -y
```

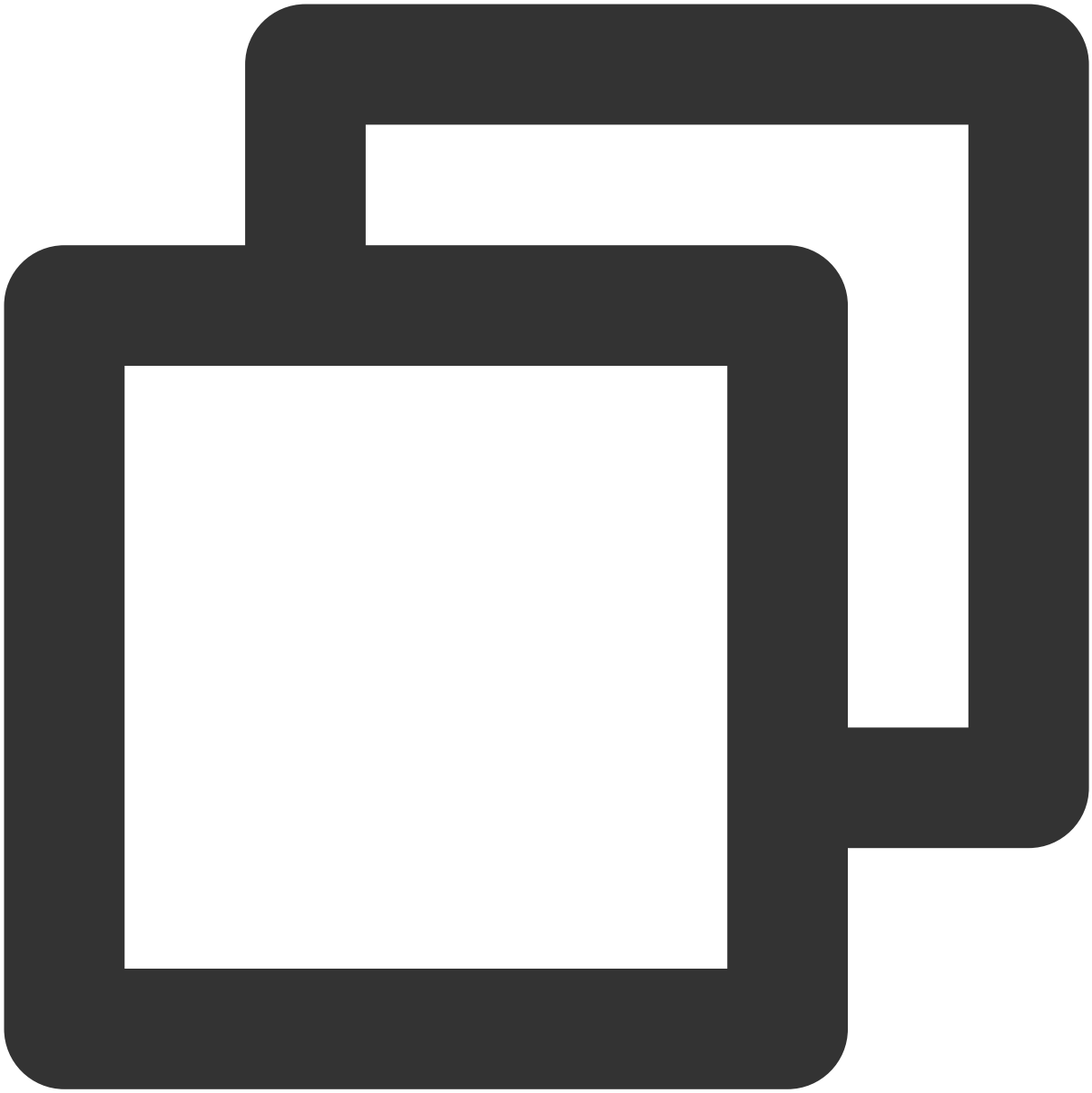
3. 次のコマンドを順番に実行して、PostgreSQLをインストールします。



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

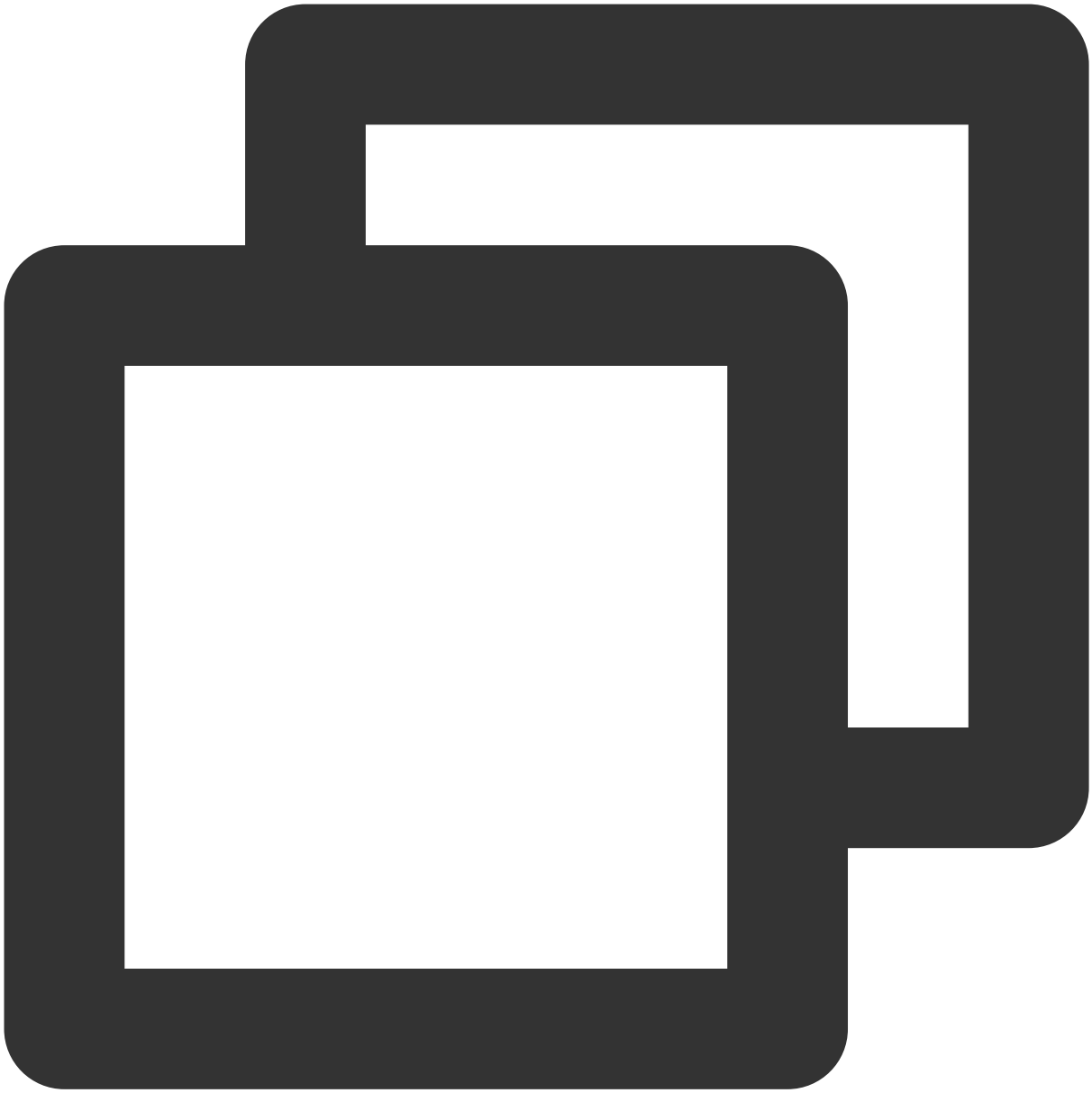


```
rpm -ivh pgdg-redhat-repo-latest.noarch.rpm
```



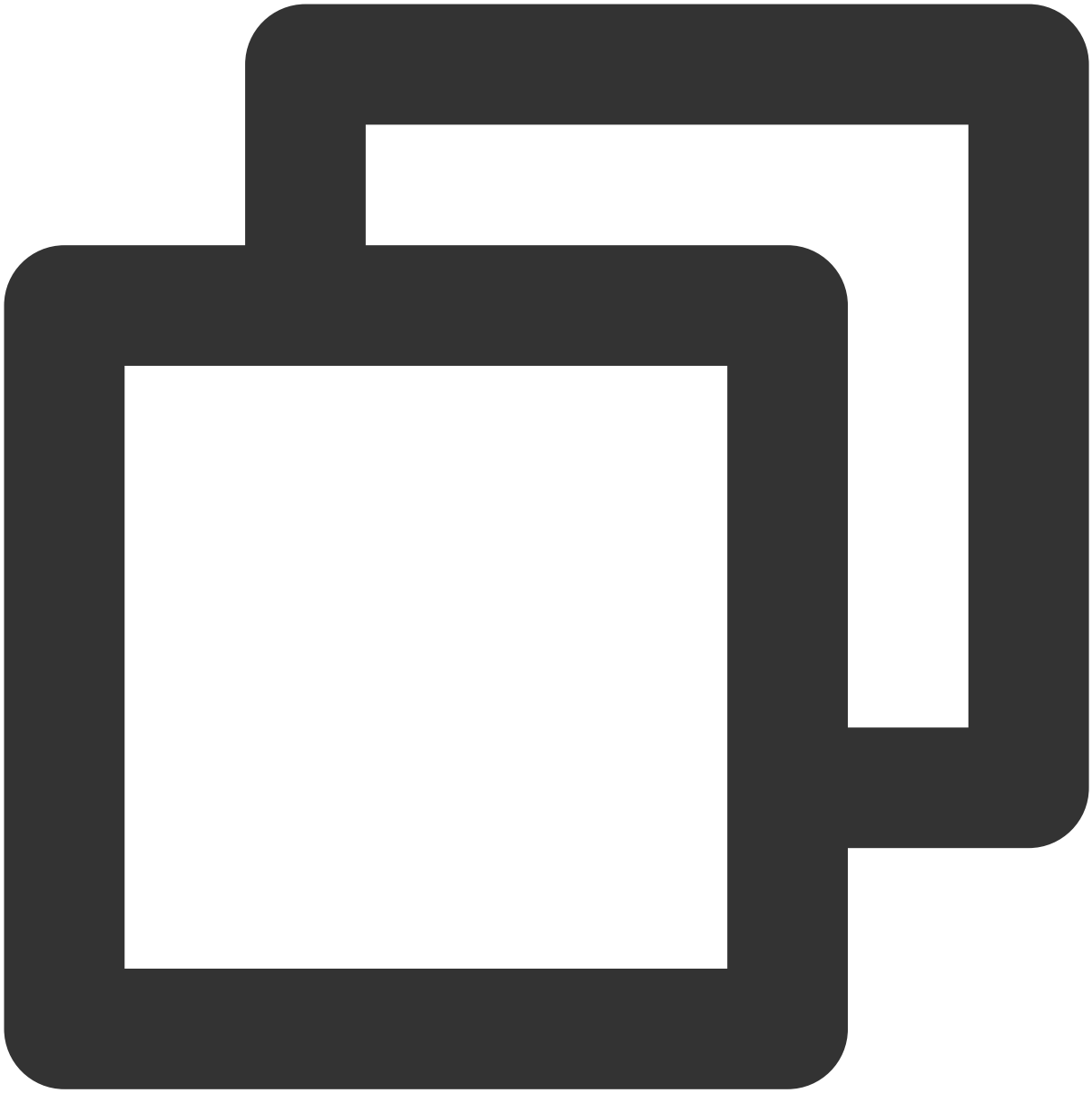
```
yum install postgresql12-server postgresql12-contrib -y
```

4. 次のコマンドを実行して、pg_basebackupベースバックアップツールを使用して、バックアップディレクトリを生成します。



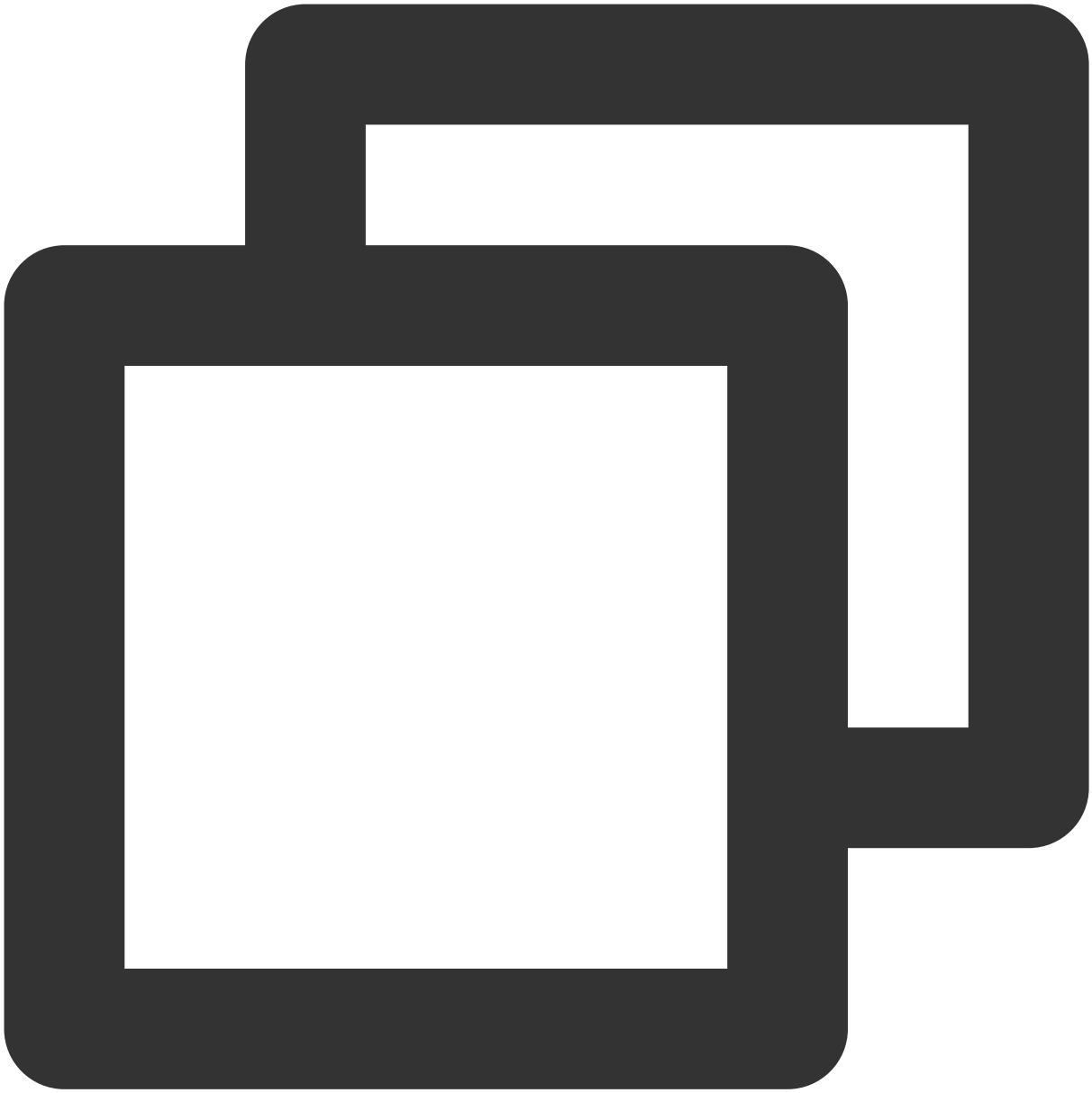
```
pg_basebackup -D /var/lib/pgsql/12/data -h <マスターノードのパブリックネットワークIP> -p 5
```

メッセージに従って、データベースアカウントに対応するパスワードを入力し、**Enter**を押します。次の結果が返された場合、正常にバックアップされたことを示します。



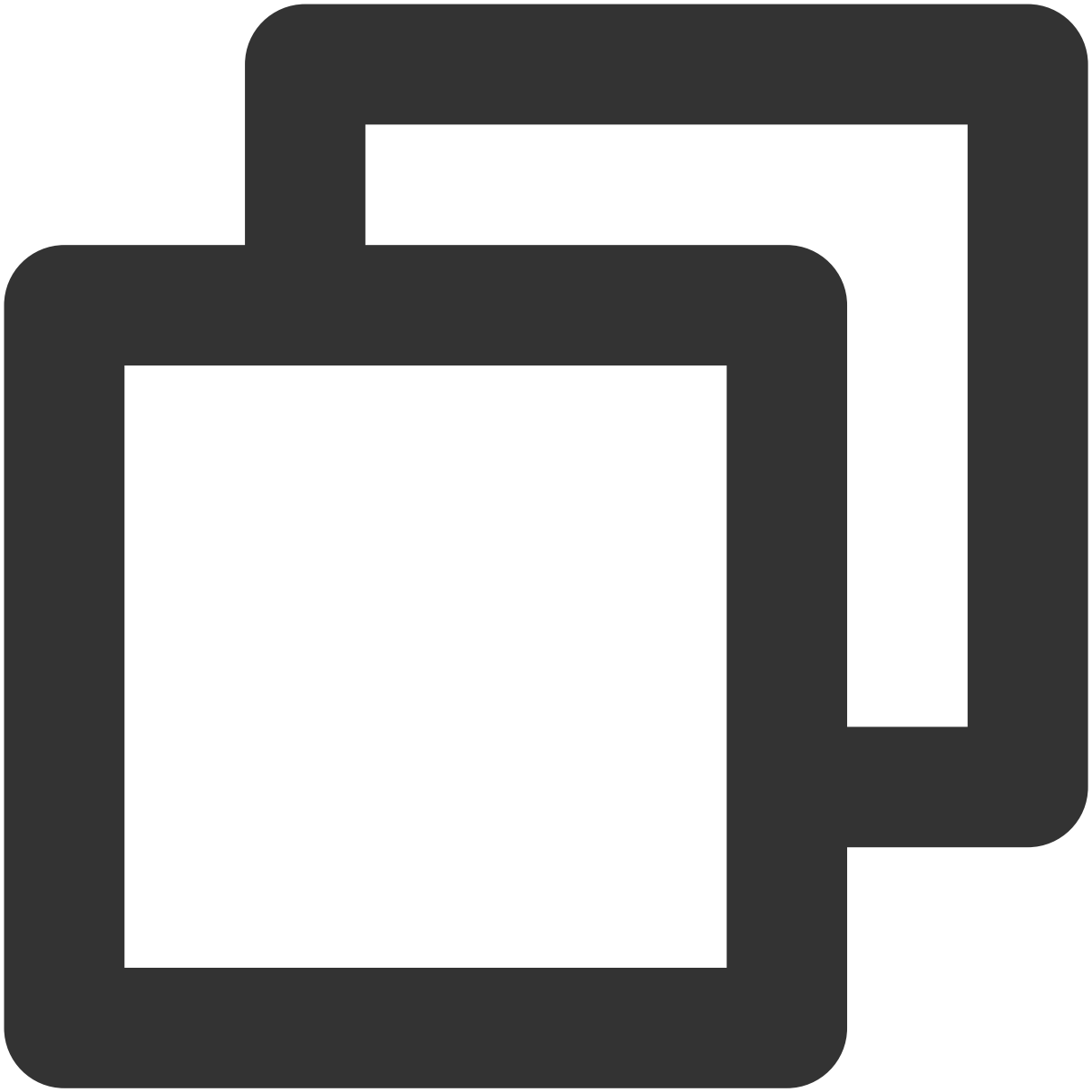
```
Password:
24526/24526 kB (100%), 1/1 tablespace
```

5. 次のコマンドを実行して、master設定の関連ファイルをコピーします。



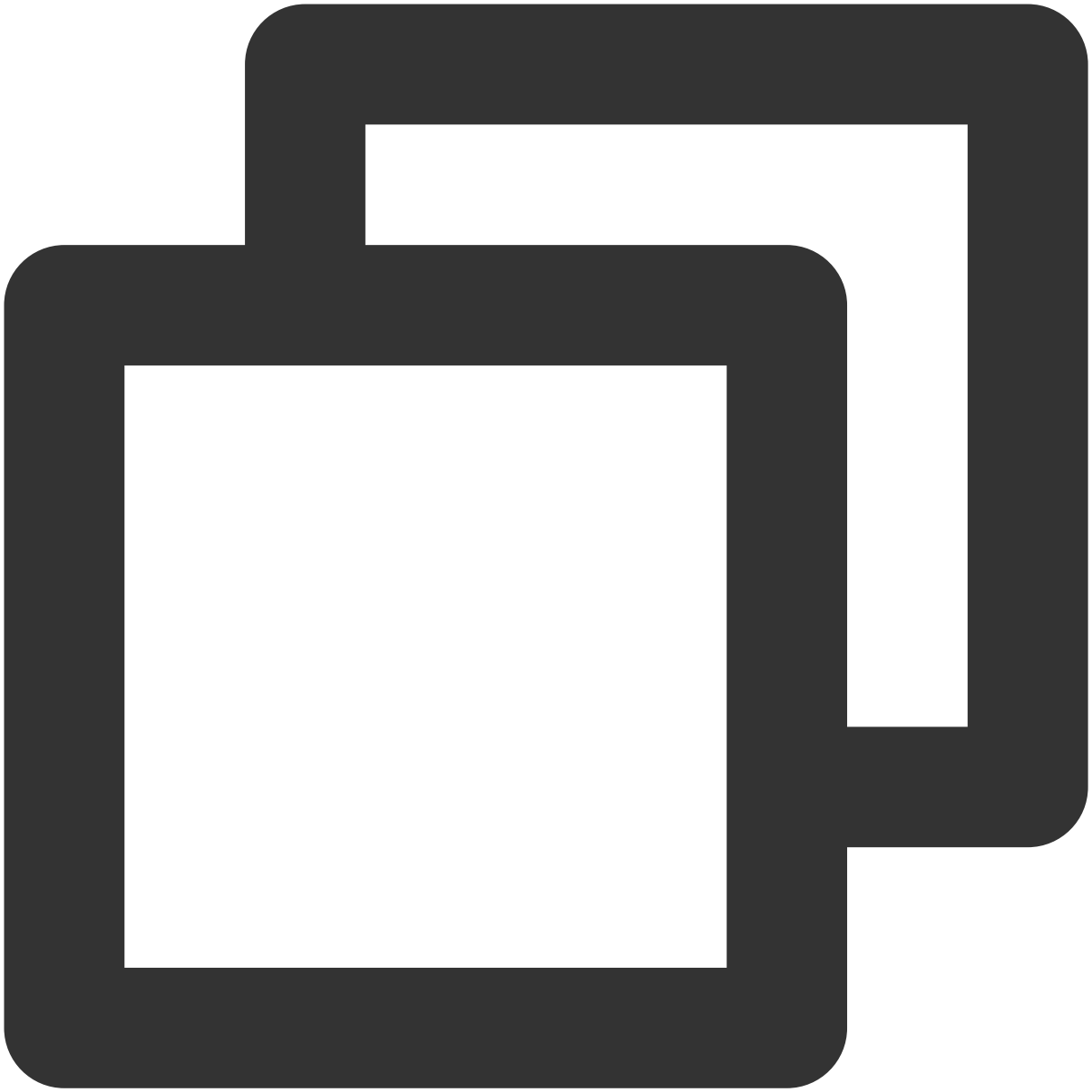
```
cp /usr/pgsql-12/share/recovery.conf.sample /var/lib/pgsql/12/data/recovery.conf
```

6. 次のコマンドを実行して、 `recovery.conf` ファイルを開きます。



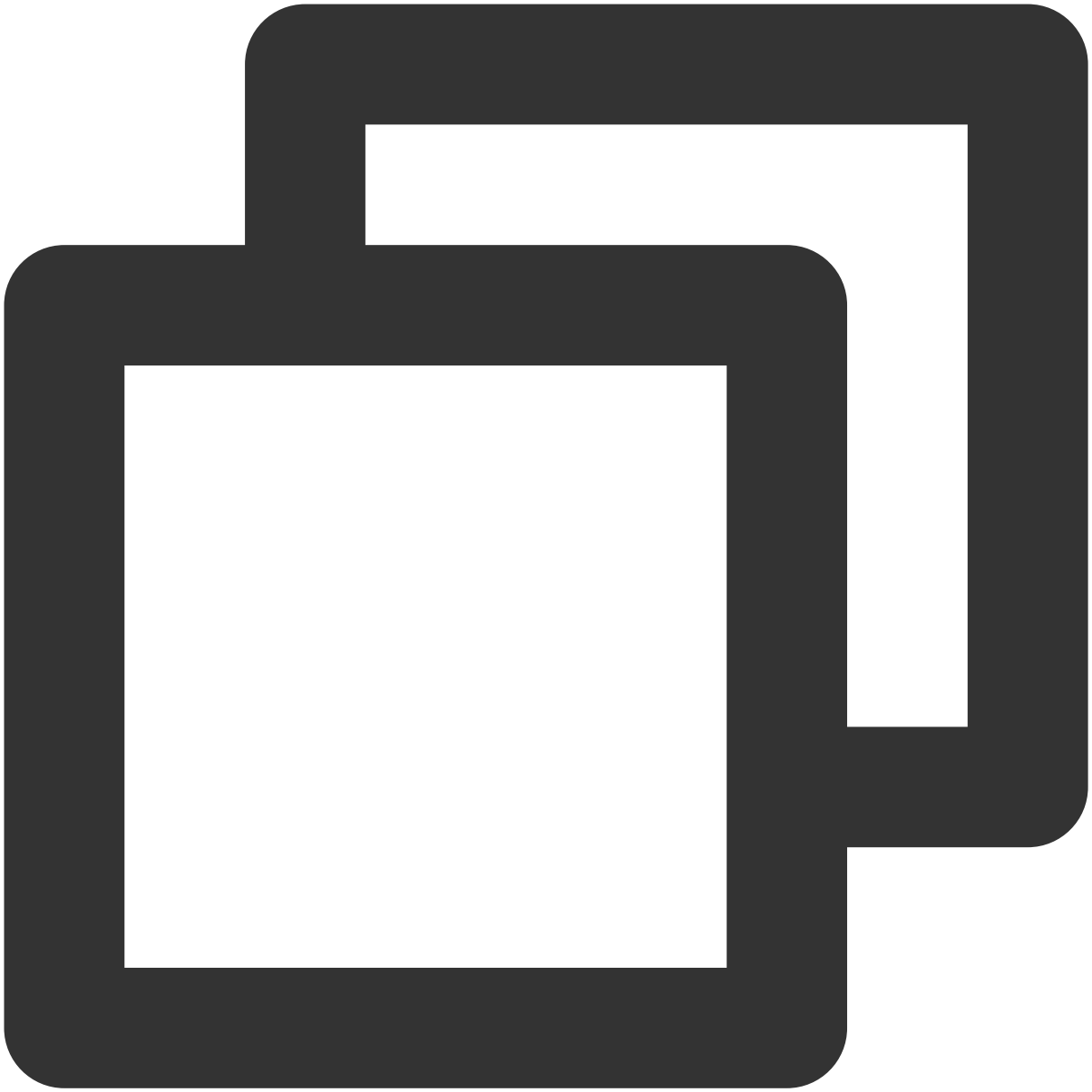
```
vim /var/lib/pgsql/12/data/recovery.conf
```

7. iを押して編集モードに切り替え、次のパラメータをそれぞれ見つけて、パラメータを次のように変更します：



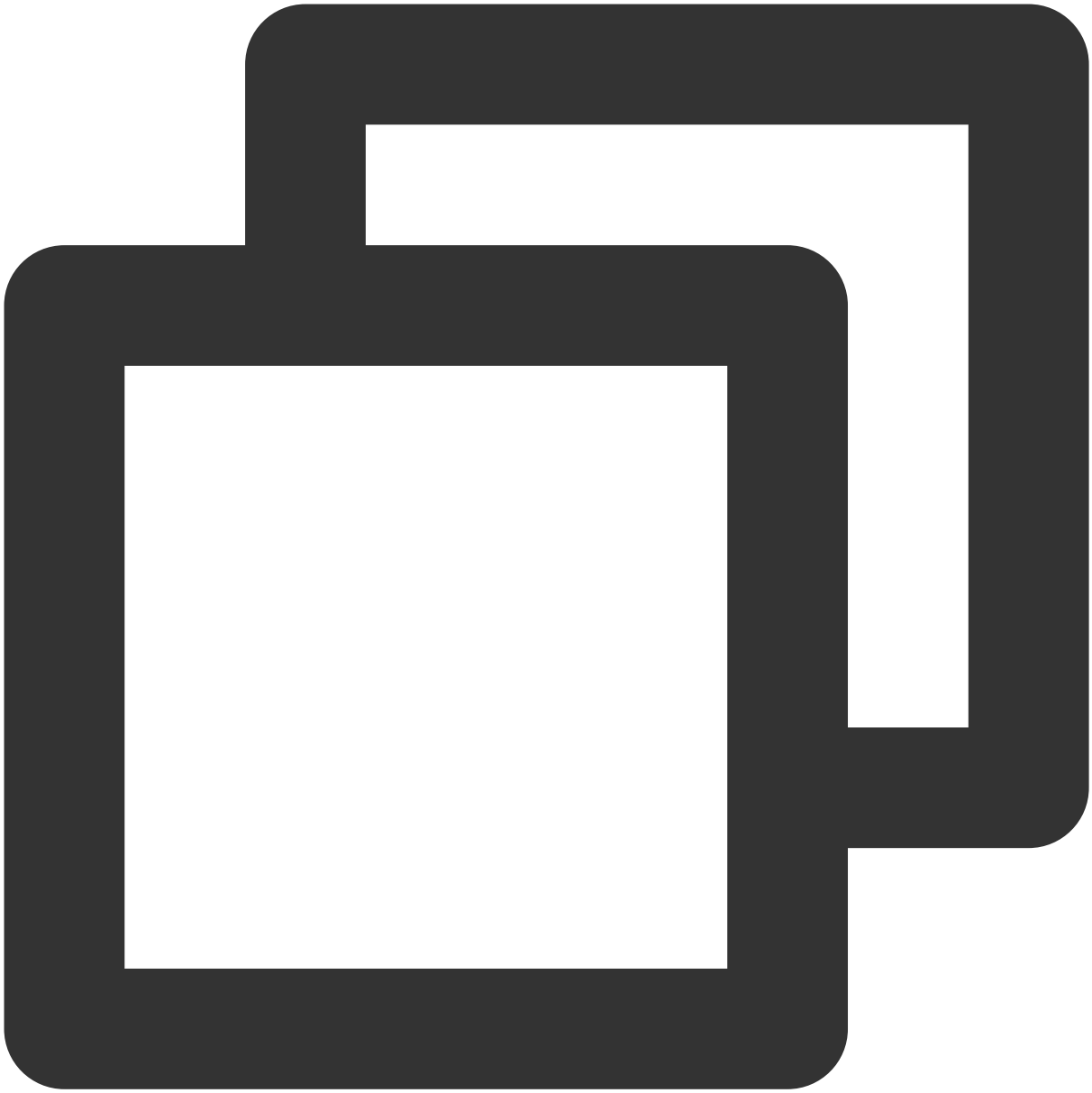
```
standby_mode = on      #このノードをスレーブデータベースとして宣言する
primary_conninfo = 'host=<マスターノードのパブリックネットワークIP> port=5432 user=データベ
recovery_target_timeline = 'latest' #ストリーミングレプリケーションは最新のデータに同期する
```

8. Escを押し、:wqを入力して、ファイルを保存して戻ります。
9. 次のコマンドを実行して、**postgresql.conf**ファイルを開きます。



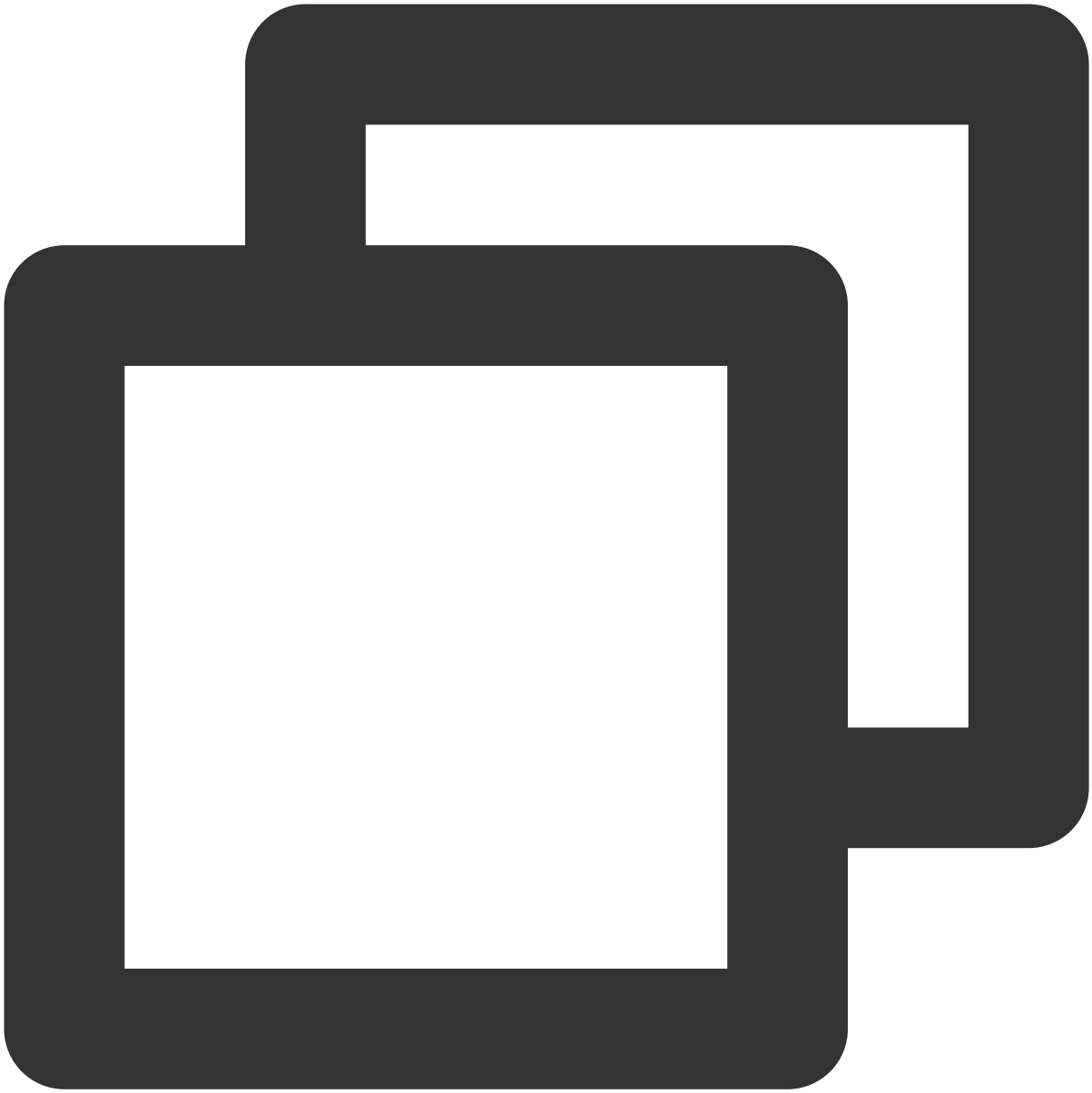
```
vim /var/lib/pgsql/12/data/postgresql.conf
```

10. iを押して編集モードに切り替え、次のパラメータをそれぞれ見つけて、パラメータを次のように変更します：



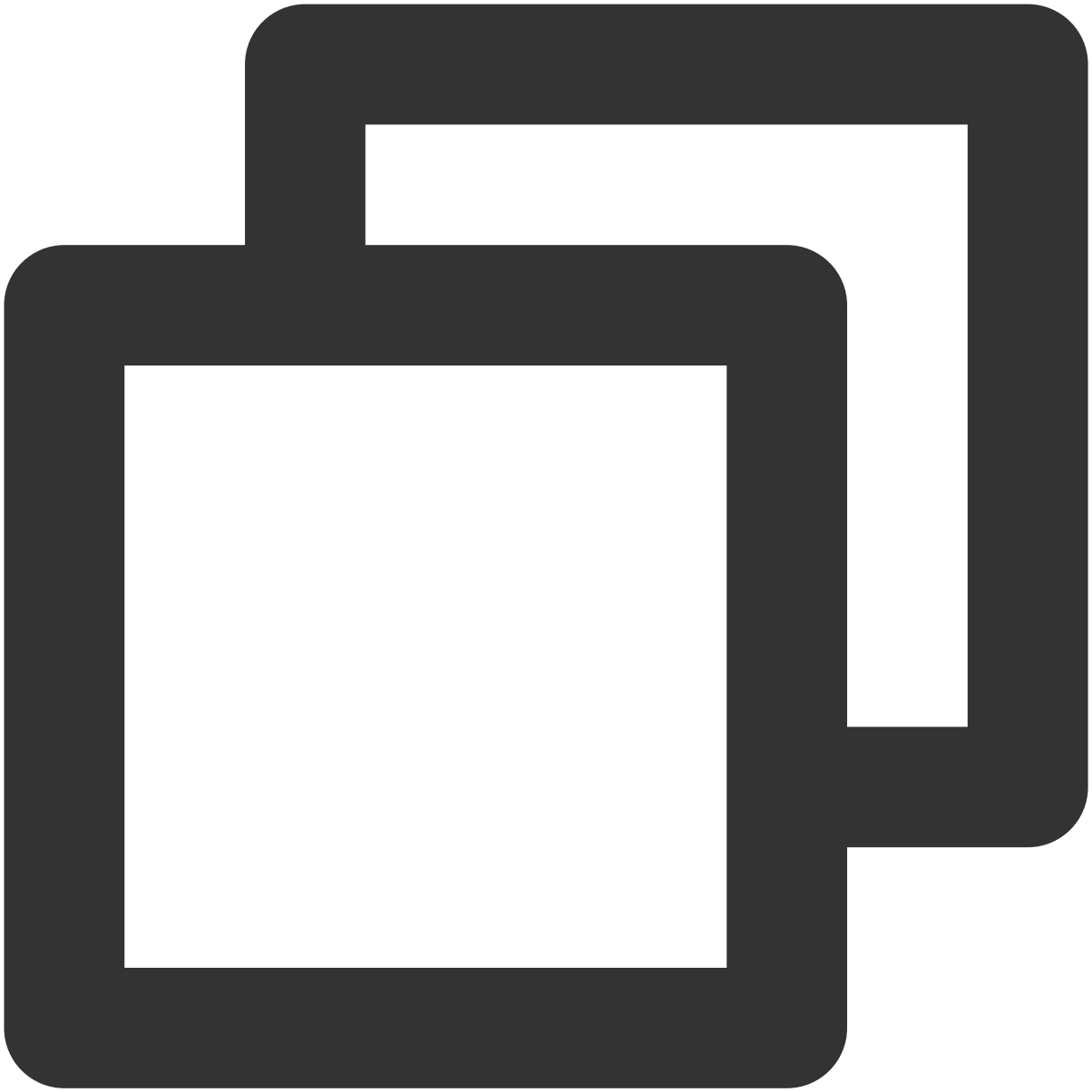
```
max_connections = 1000              #接続の最大数です。スレーブデータベースのmax_connection
hot_standby = on                    # ホットバックアップを有効にする
max_standby_streaming_delay = 30s   # ストリーミングバックアップの最大遅延
wal_receiver_status_interval = 1s   # スレーブノードがそのステータスをマスターノードに報告する
hot_standby_feedback = on           # データのレプリケーションにエラーがある場合、マスターに報
```

11. Escを押し、**:wq**を入力して、ファイルを保存して戻ります。
12. 次のコマンドを実行して、データディレクトリのグループと所有者を変更します。



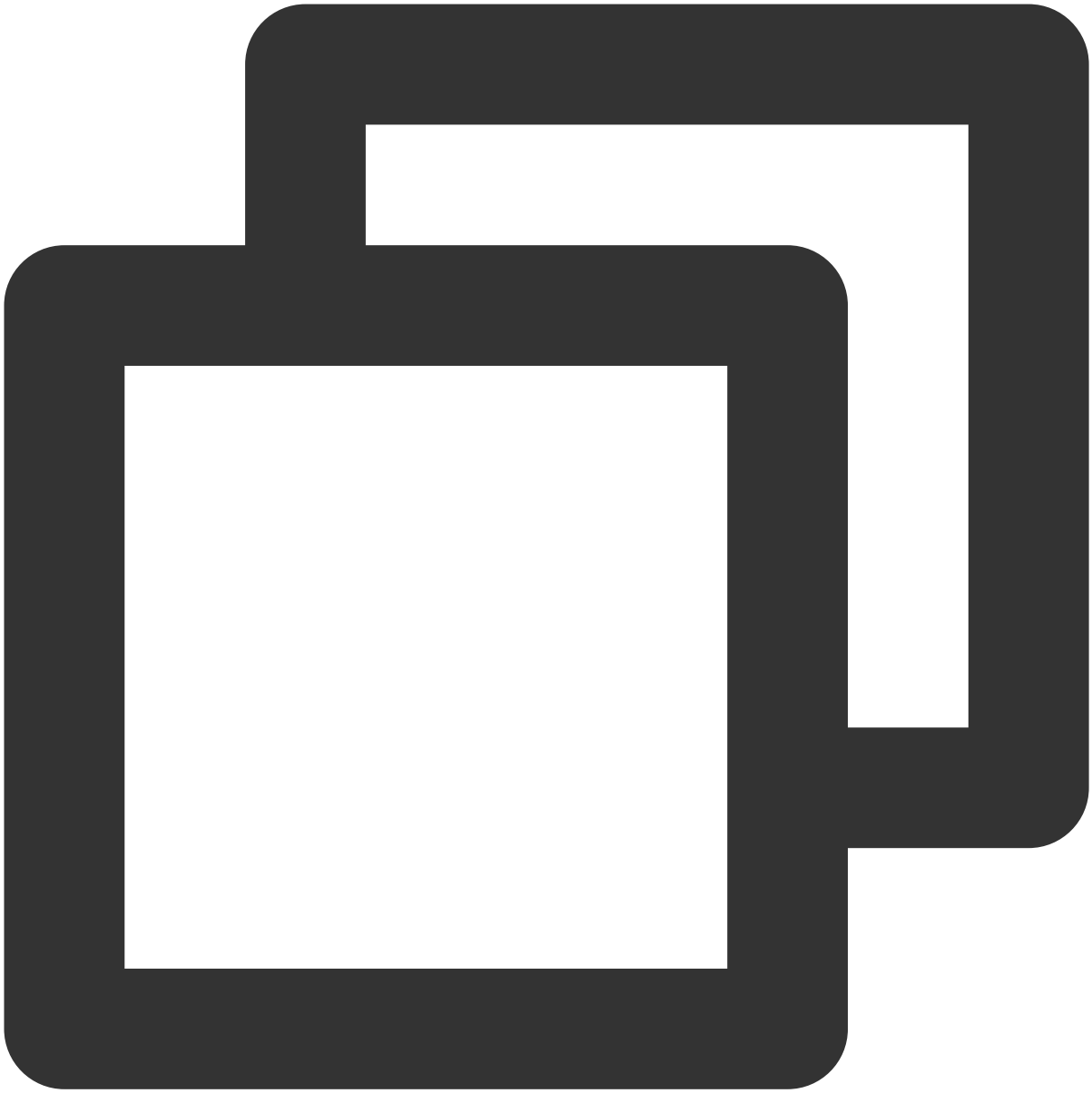
```
chown -R postgres.postgres /var/lib/pgsql/12/data
```

13. 次のコマンドを実行して、サービスを起動します。



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

14. 次のコマンドを実行して、起動時に自動的にサービスを開始するように設定します。

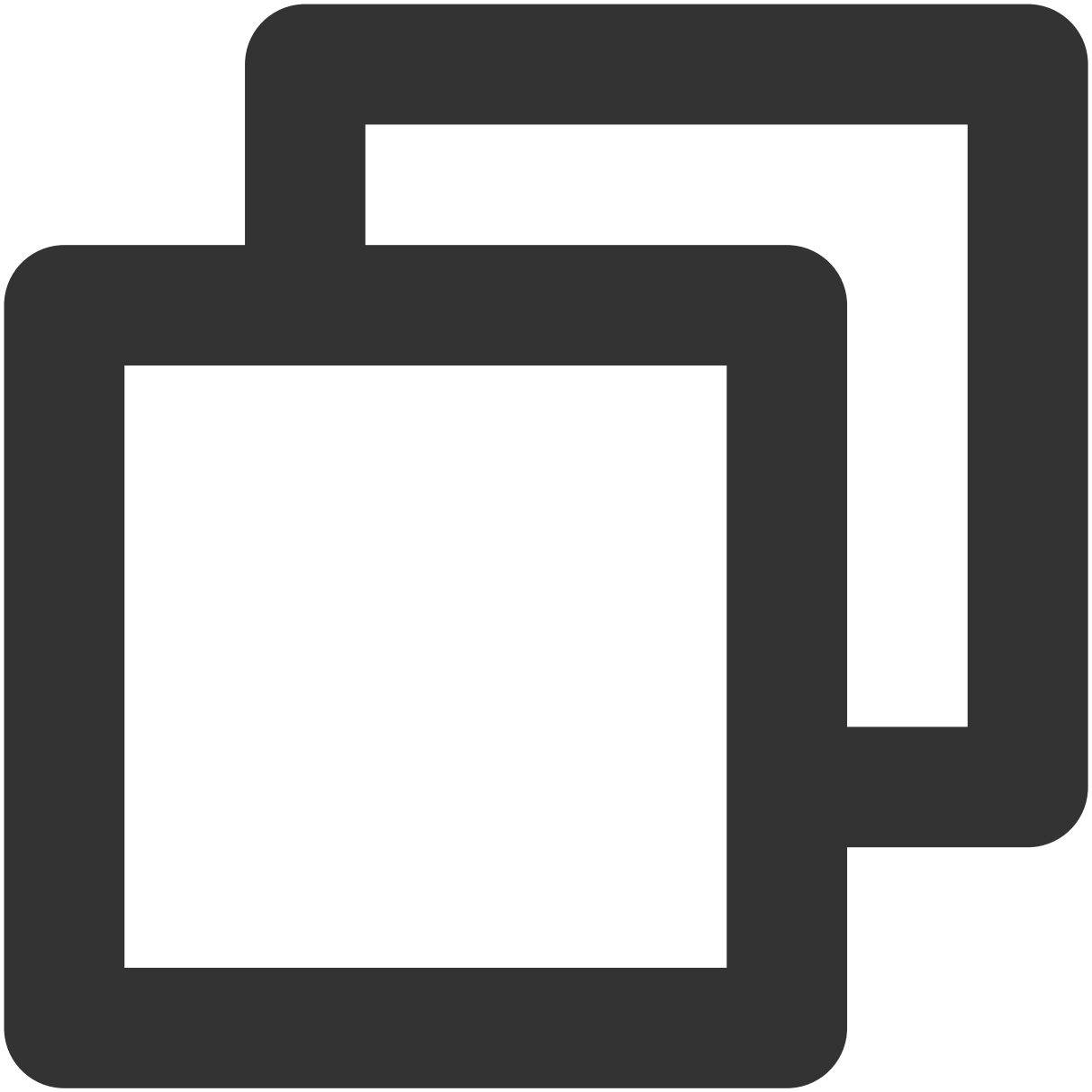


```
systemctl enable postgresql-12.service
```

デプロイの検証

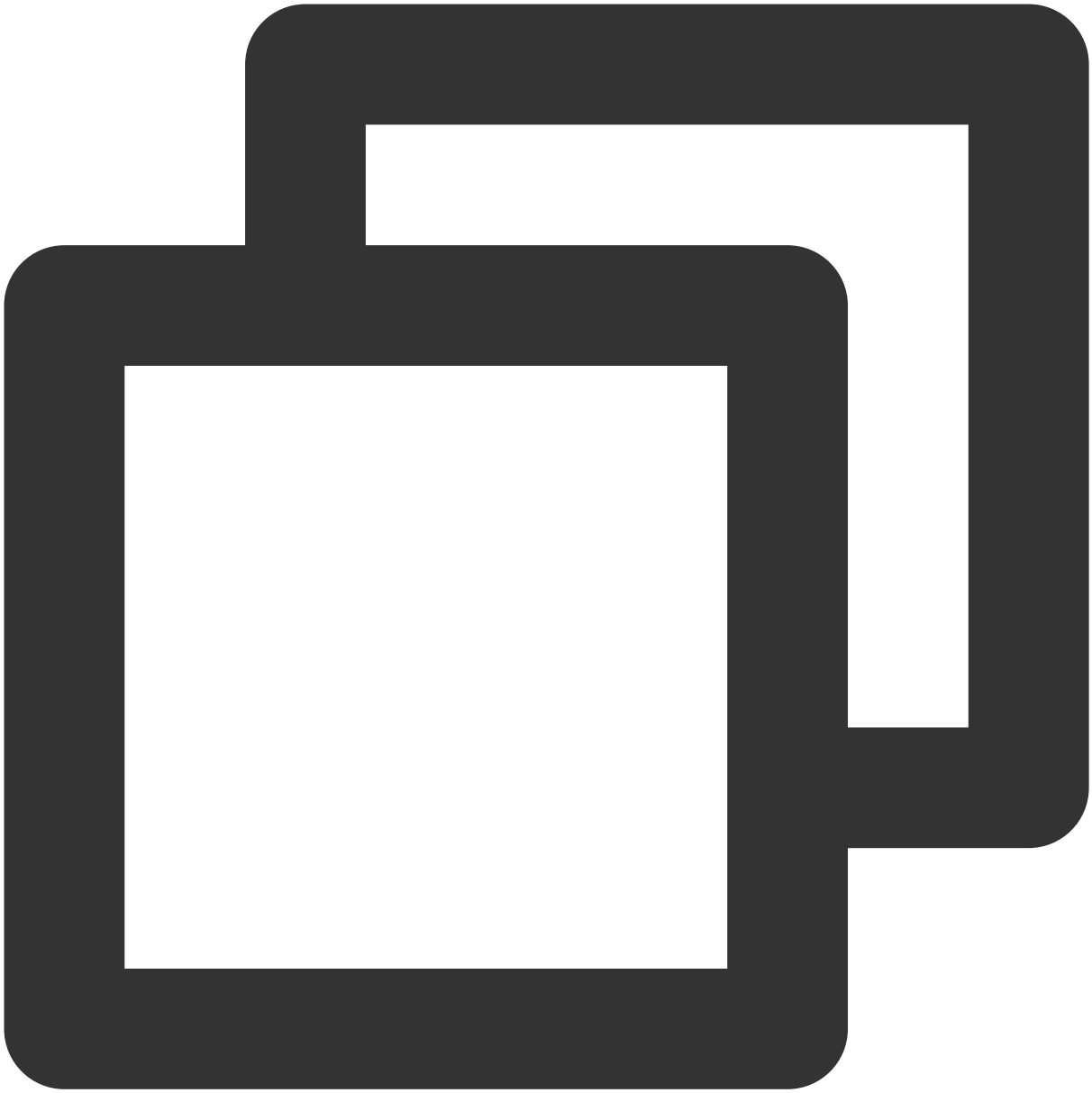
次の手順を実行して、正常にデプロイされたかどうかを確認できます：

1. 次のコマンドを実行して、ノードからディレクトリをバックアップします。



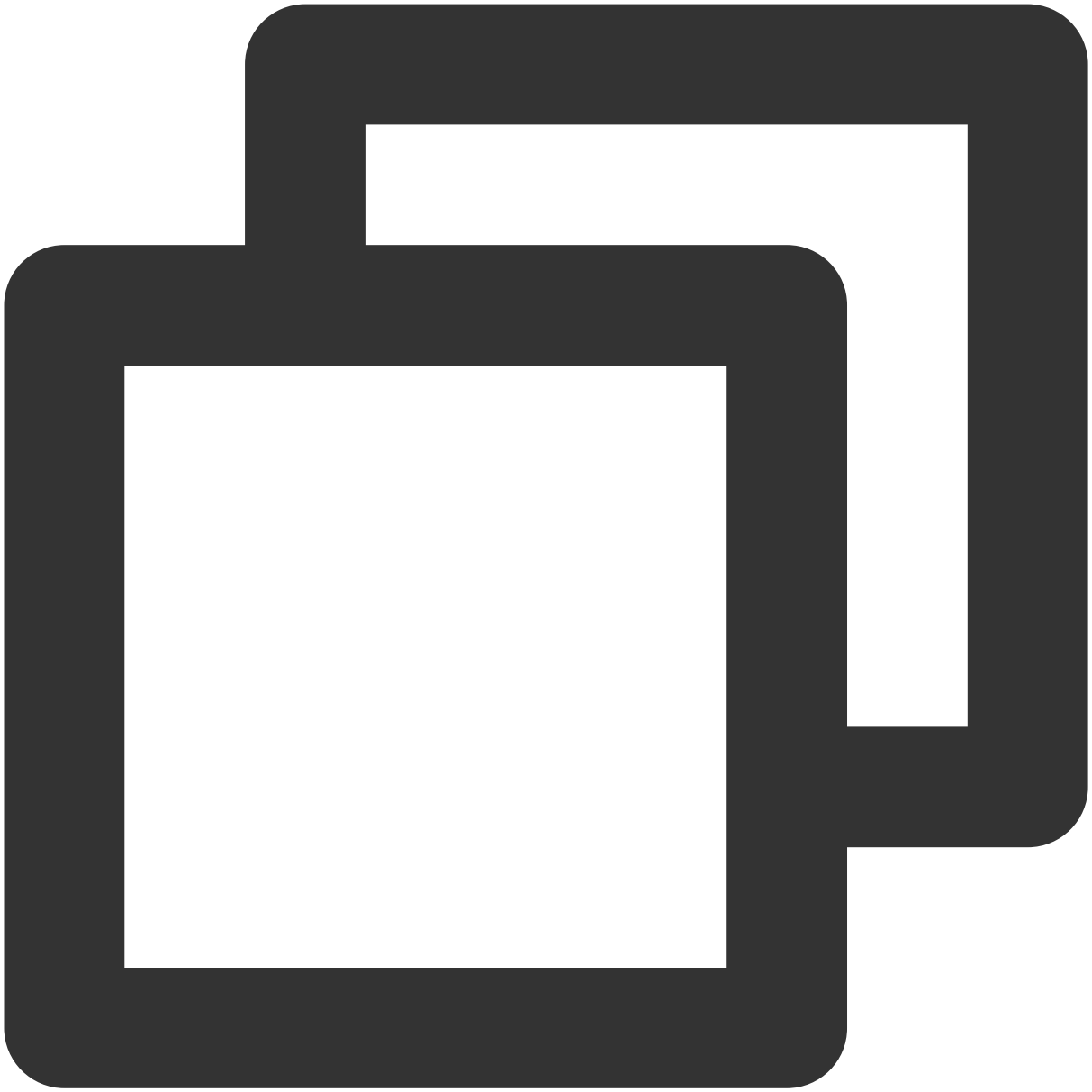
```
pg_basebackup -D /var/lib/pgsql/12/data -h <マスターノードのパブリックネットワークIP> -p 5
```

データベースのパスワードを入力し、Enterを押して、次の結果が返された場合は、正常にバックアップされたことを示します。



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

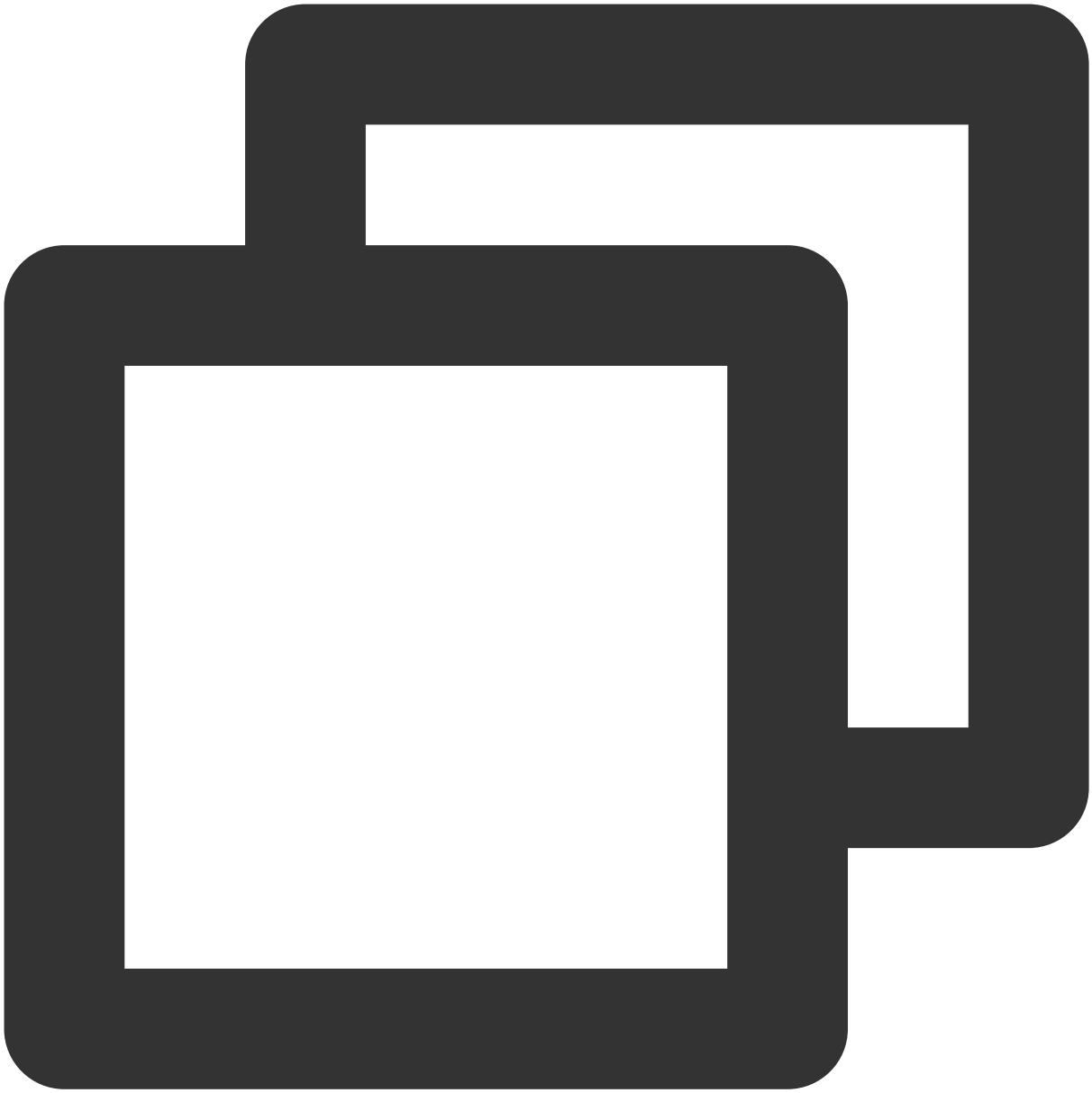
2. マスターノードで、次のコマンドを実行して、senderプロセスを表示します。



```
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 replica 114.117.197.14
00CA0
root     19724  0.0  0.0 112812   972 pts/0    S+   13:00   0:00 grep --color=auto sender
```

3. スレーブノードで、次のコマンドを実行して、receiverプロセスを表示します。

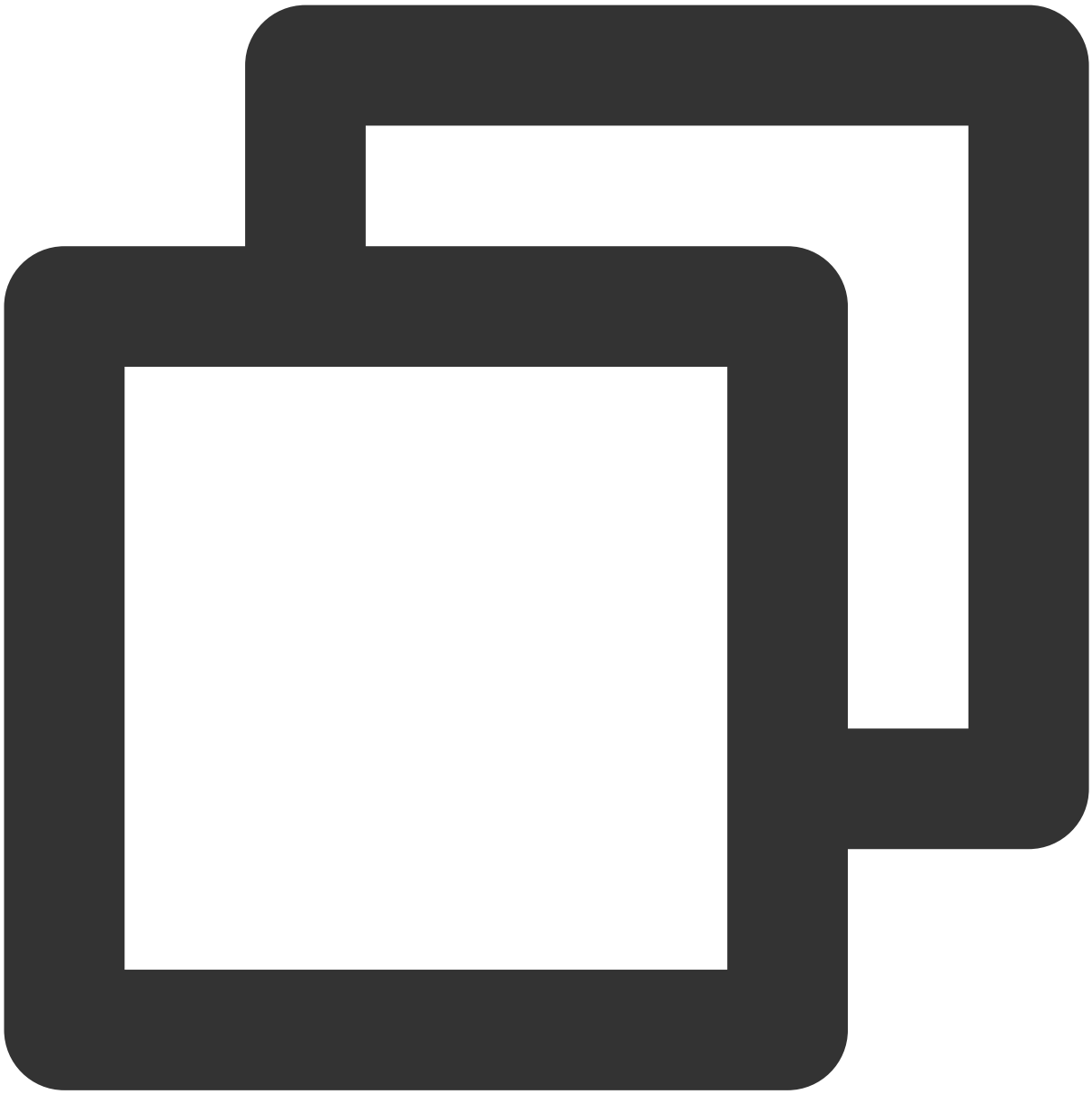


```
ps aux |grep receiver
```

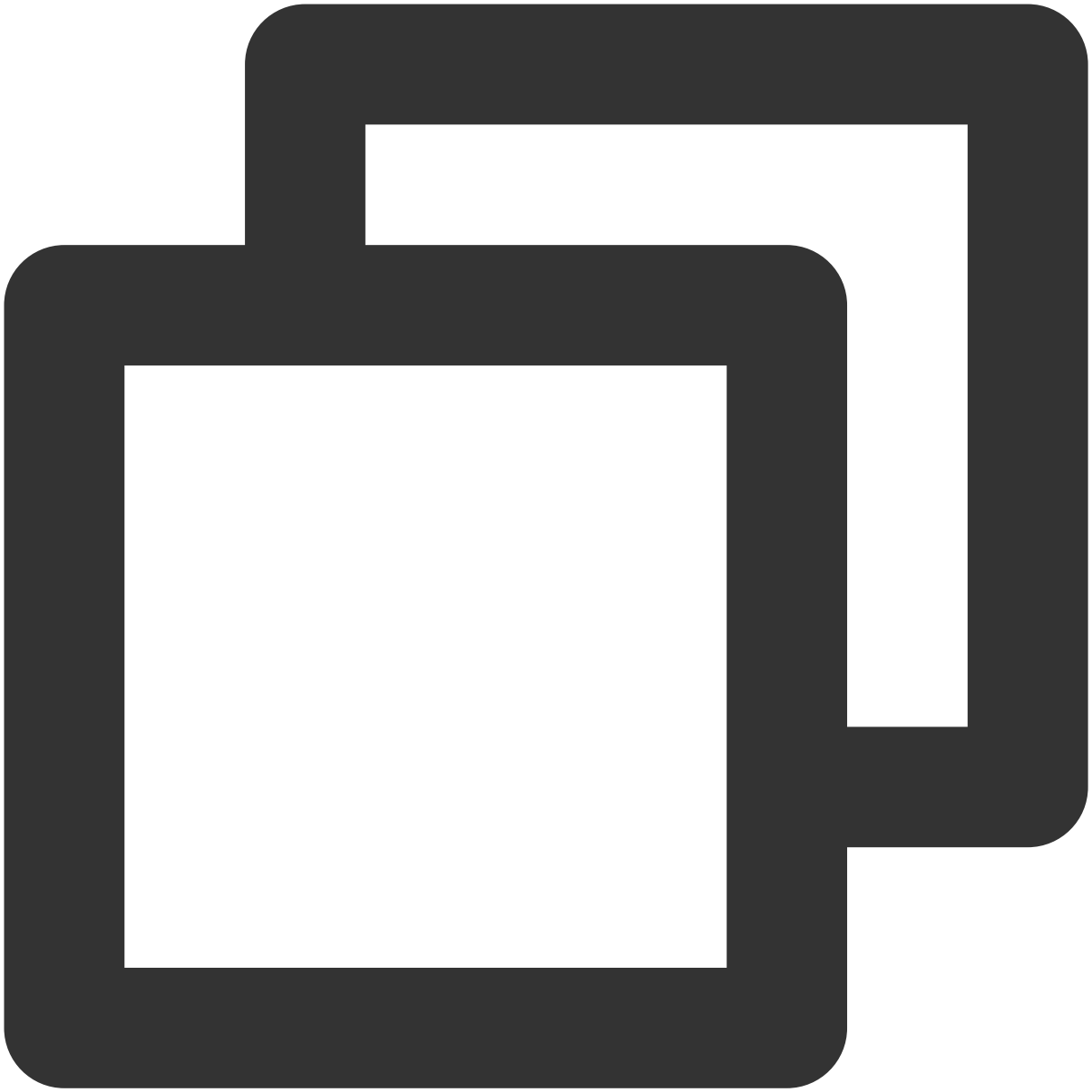
次の結果が返された場合は、receiverプロセスを正常に表示できることを示します。

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

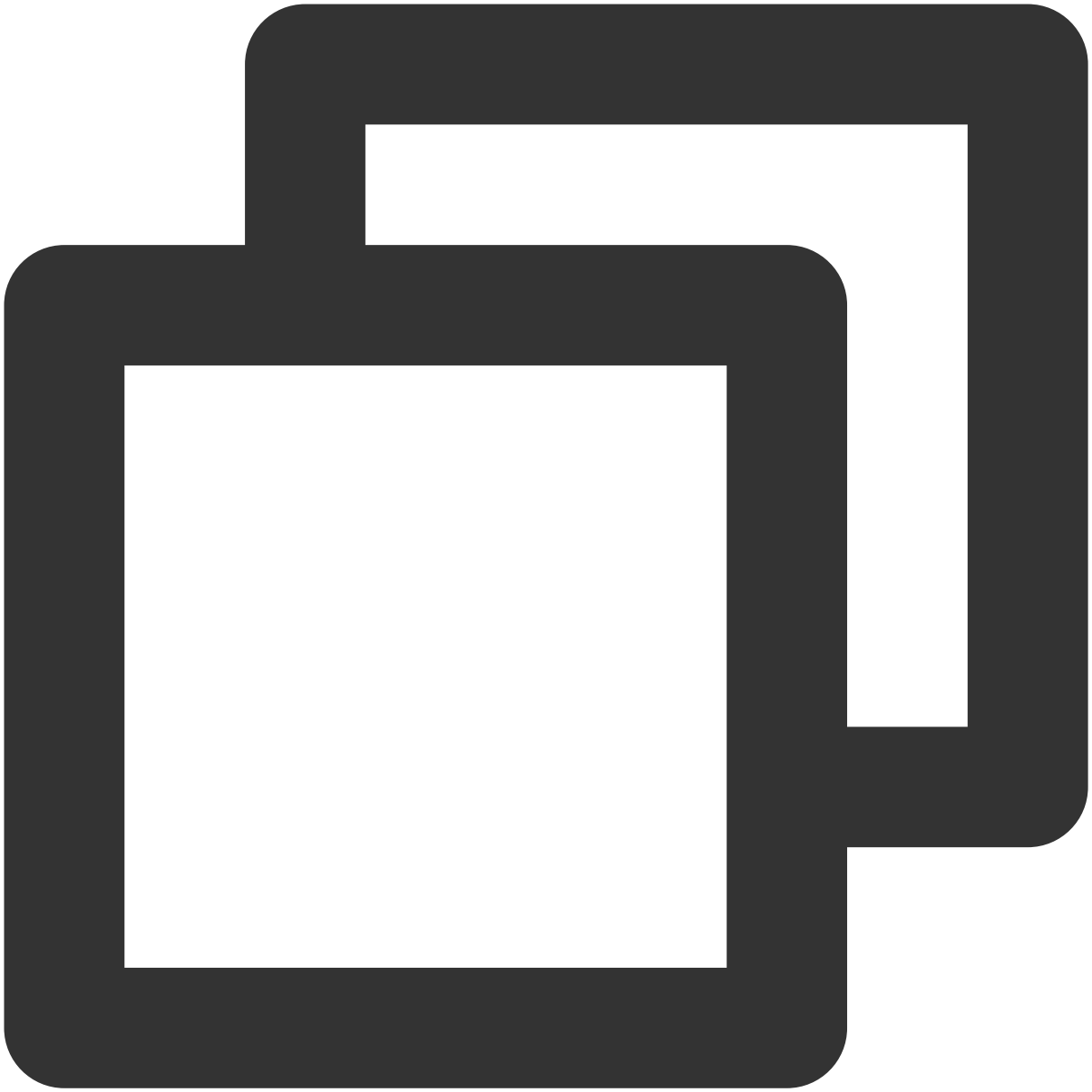
4. マスターノードでは、次のコマンドを順番に実行して、PostgreSQLインタラクティブ端末に入り、マスターデータベースでスレーブデータベースのステータスを表示します。



```
su - postgres
```



```
psql
```



```
select * from pg_stat_replication;
```

次の結果が返された場合は、スレーブデータベースのステータスを正常に表示できることを示します。

```
postgres=# select * from pg_stat_replication;
 pid   | usesysid | usename | application_name |    client_addr    | client_hostname | client_port |         back
mi
n |   state    | sent_location | write_location | flush_location | replay_location | sync_priority | sync_state
------+----------+---------+------------------+----------------+-----------------+-------------+------------
--
--+-----------+---------------+----------------+----------------+-----------------+-------------+-----------
 3875 |    16384 | replica | walreceiver      | 114.117.197.144 |                 |       44724 | 2022-01-27 1
76
2 | streaming | 0/3000AE0     | 0/3000AE0      | 0/3000AE0      | 0/3000AE0       |           0 | async
(1 row)
```

Microsoft SharePoint 2016の構築

最終更新日：：2022-06-29 15:44:12

ユースケース

このドキュメントでは、CVMインスタンス上でMicrosoft SharePoint 2016を構築する方法についてご説明します。

ソフトウェアバージョンの例

ここで例に挙げる手順において使用するCVMインスタンスのハードウェア仕様は次のとおりです。
vCPU：4コア
メモリ： 8GB
ここで例に挙げる手順では、次のソフトウェアバージョンを使用しています。
OS：Windows Server 2012 R2 データセンターバージョン64ビット英語版
データベース：SQL Server 2014

前提条件

Windows CVMを購入済みであること。CVMを購入していない場合は、Windows CVMのクイック設定 をご参照ください。

操作手順

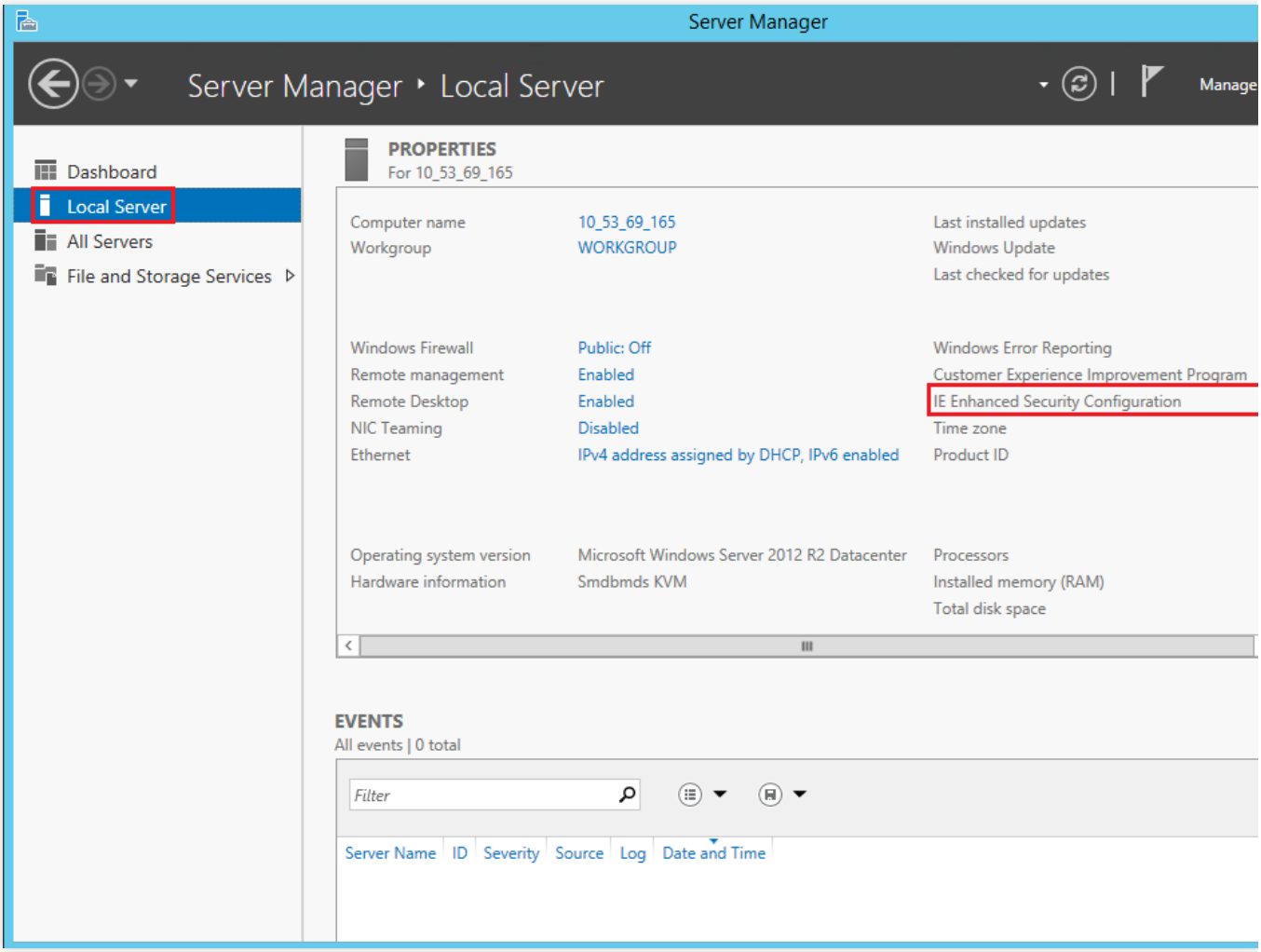
ステップ1：Windowsインスタンスへのログイン

RDPファイルを使用してWindowsインスタンスにログイン（推奨）します。実際の操作習慣に合わせて、リモートデスクトップを利用してWindowsインスタンスにログイン することもできます。

ステップ2：AD、DHCP、DNS、IISサービスの追加

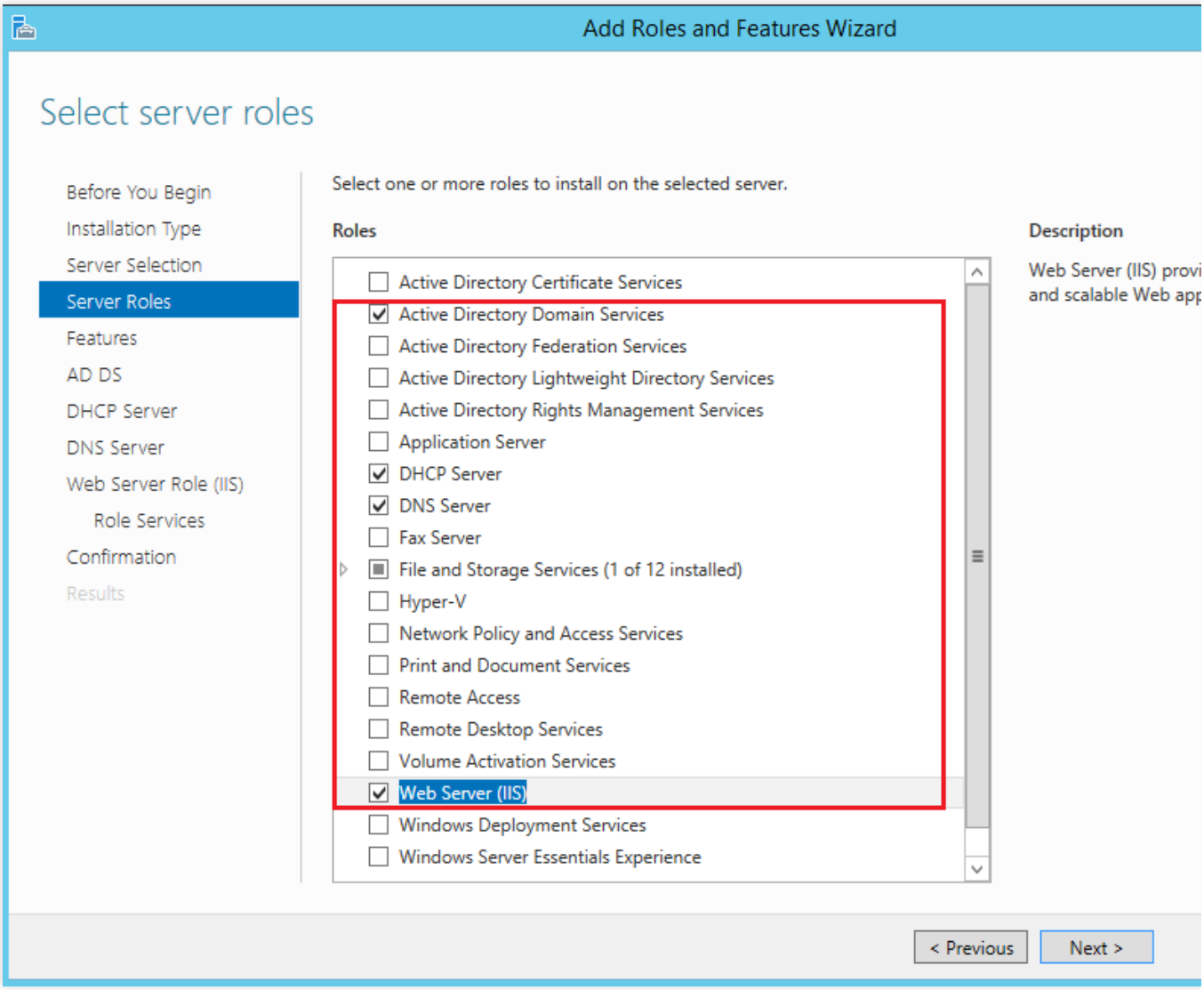
1. OSの画面で、

をクリックして、サーバーマネージャーを開きます。
2. 下図のように、左側ナビゲーションバーで**ローカルサーバー**を選択し、**Internet Explorer拡張セキュリティ構成**を見つけます。

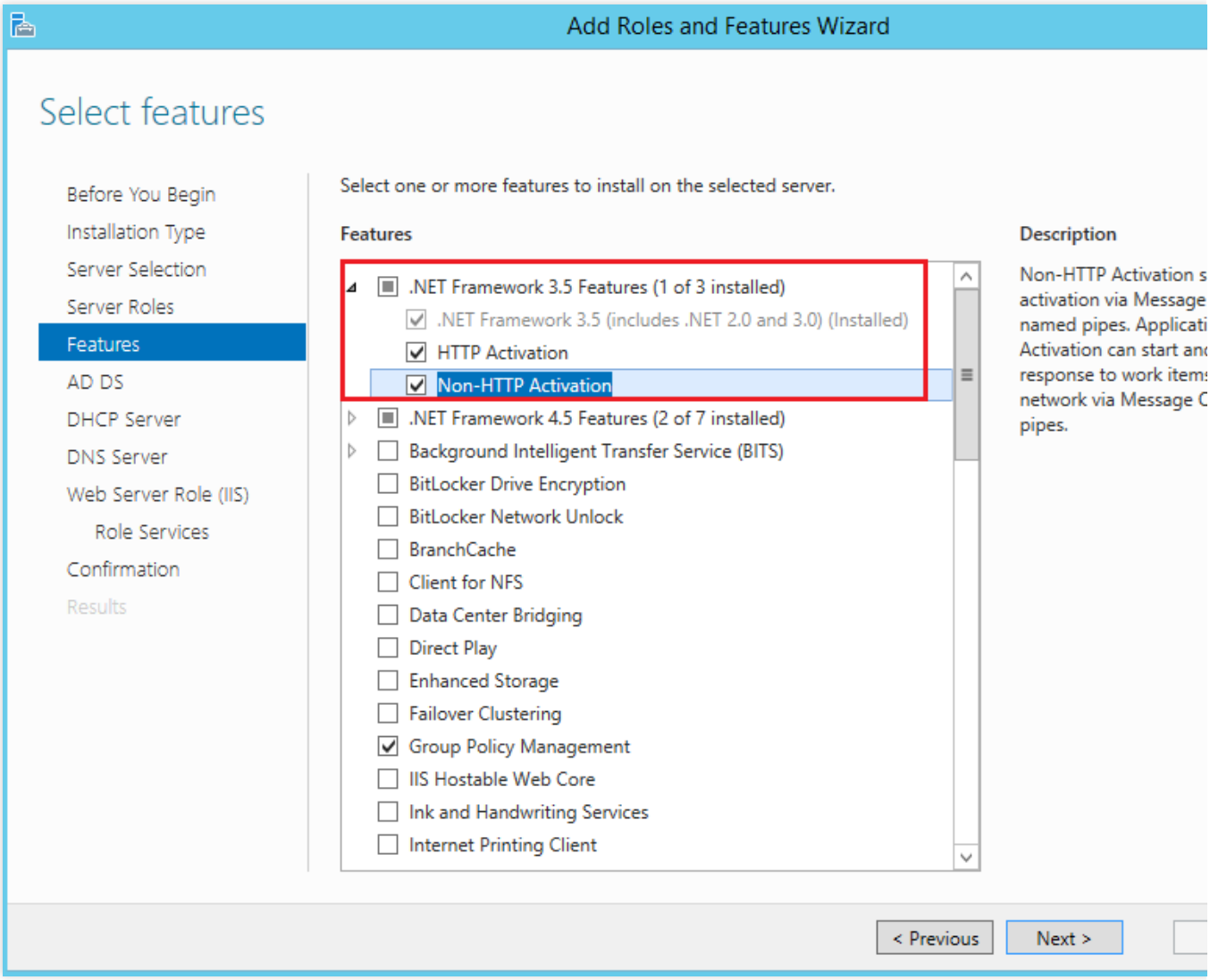


3. 下図のように、**Internet Explorer拡張セキュリティ構成**をオフにします。

4. 左側ナビゲーションバーで**ダッシュボード**を選択し、**ロールと機能の追加**をクリックして、「ロールと機能の追加ウィザード」ウィンドウを開きます。
5. 「ロールと機能の追加ウィザード」ウィンドウで、デフォルトの設定を維持したまま、**次へ**を3回続けてクリックします。
6. 下図のように、「サーバーロールの選択」画面で、**Active Directoryドメインサービス**、**DHCPサーバー**、**DNSサーバー**、**Webサーバー(IIS)にチェックを入れ、ポップアップしたウィンドウで機能の追加**をクリックします。



7. **次へ**をクリックします。
8. 下図のように、「機能の選択」画面で、「.NET Framework 3.5機能」にチェックを入れ、ポップアップしたウィンドウで**機能の追加**をクリックします。



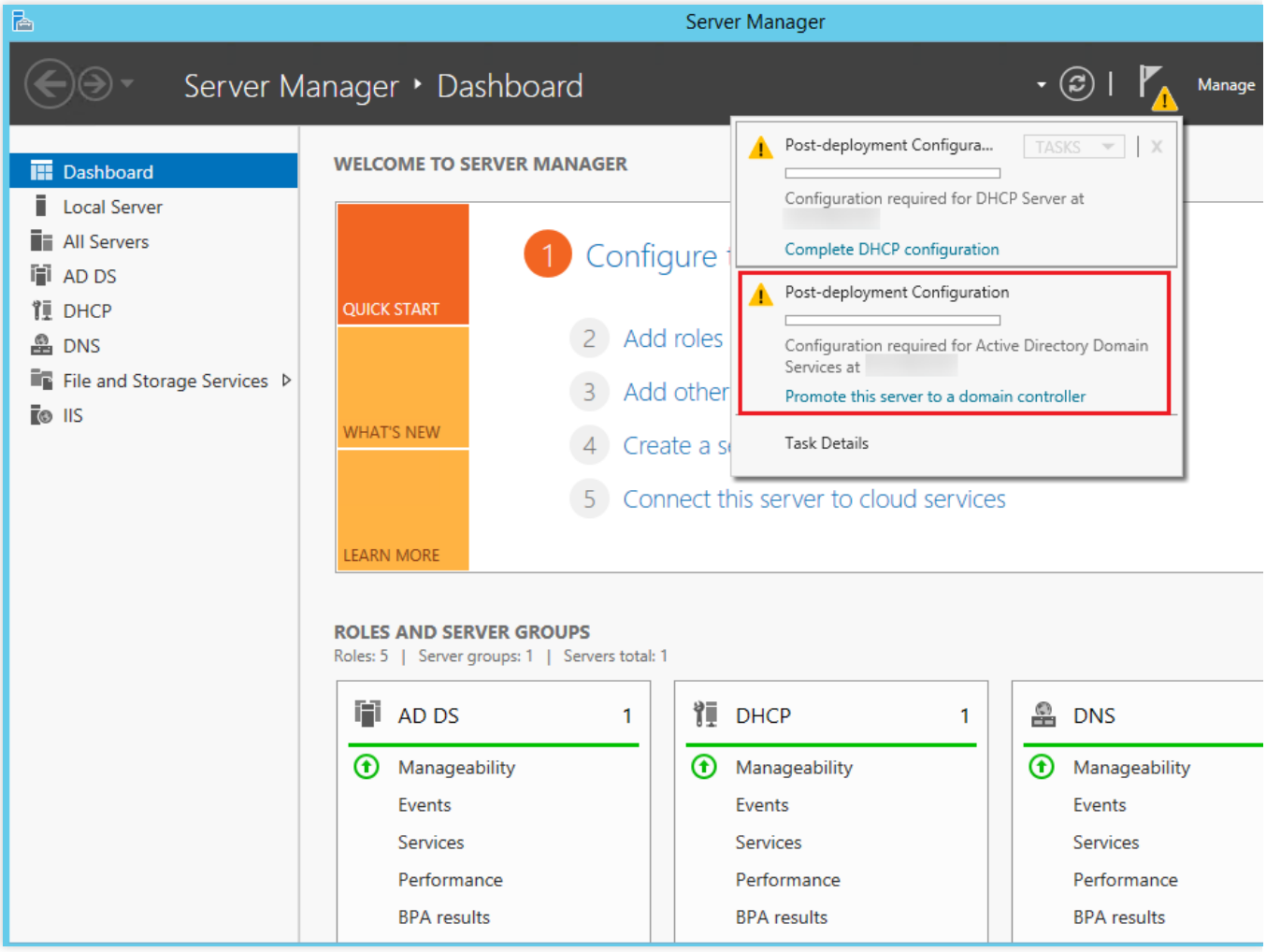
9. デフォルトの設定を維持したまま、**次へ**を6回続けてクリックします。
10. インストール情報を確認し、**インストール**をクリックします。
11. インストールの完了後にCVMを再起動します。

ステップ3： ADサービスの設定

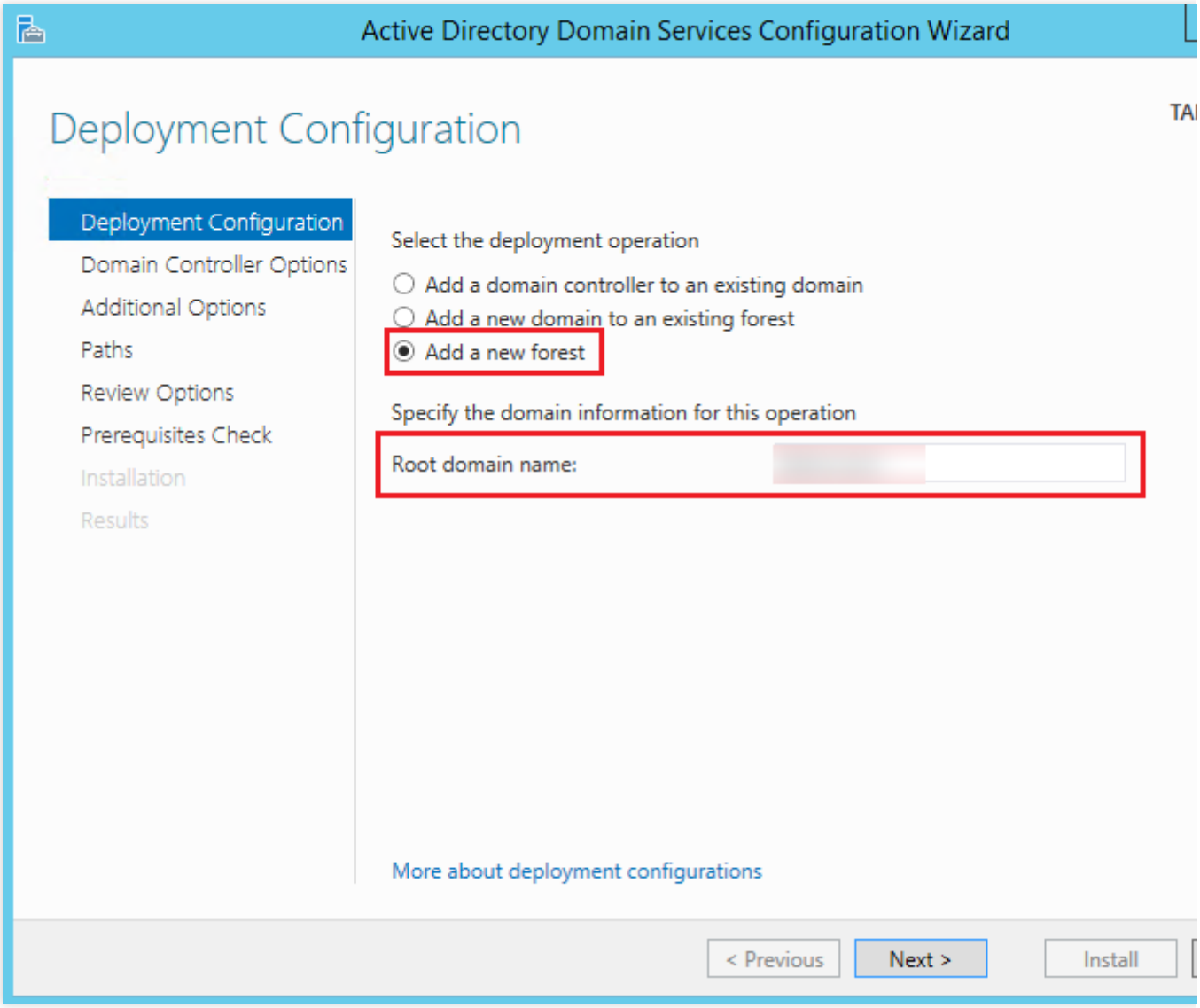
1. OSの画面で、

をクリックして、サーバーマネージャーを開きます。
2. 下図のように、サーバーマネージャーのウィンドウで、

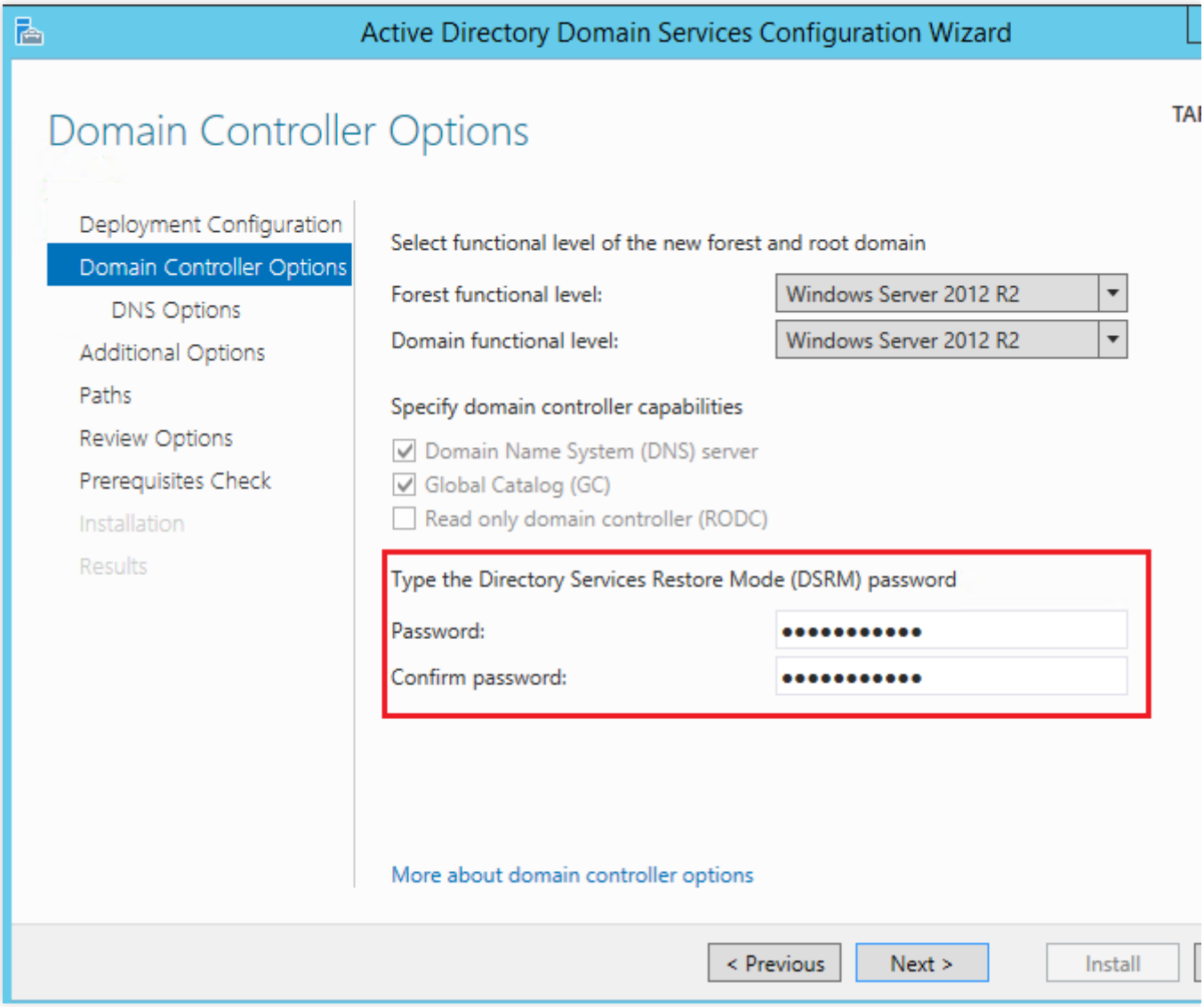
をクリックして、**このサーバーをドメインコントローラに変更する**を選択します。



3. 下図のように、表示された「Active Directoryドメインサービスの設定ウィザード」画面で、「デプロイ操作の選択」を**フォレストの新規追加**に設定し、ルートドメイン名を入力し、**次へ**をクリックします。



4. 下図のように、ディレクトリサービス復元モデル（DSRM）のパスワードを設定して、**次へ**をクリックします。



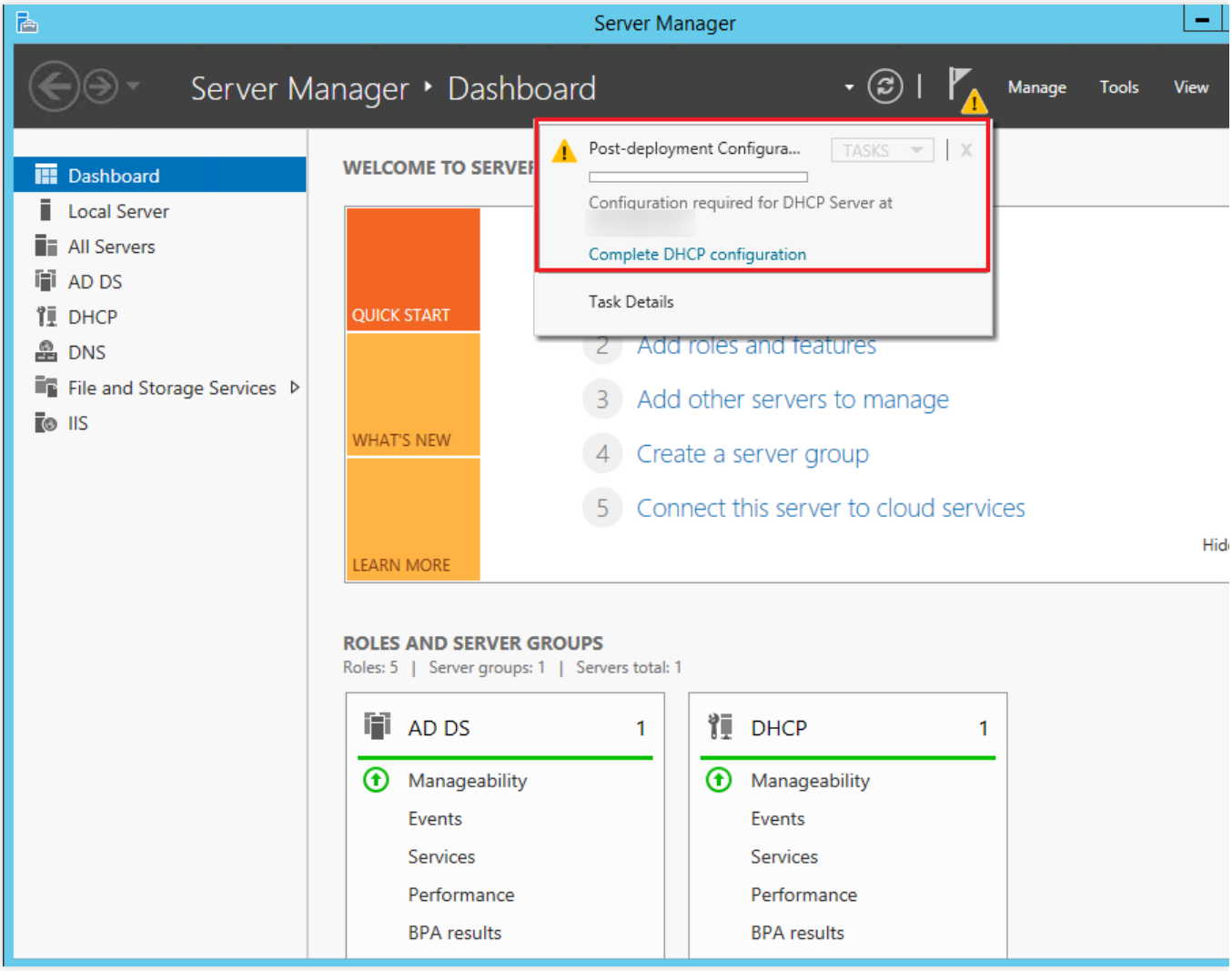
5. デフォルトの設定を維持したまま、**次へ**を4回続けてクリックします。
6. **インストール**をクリックします。

ステップ4： DHCPサービスの設定

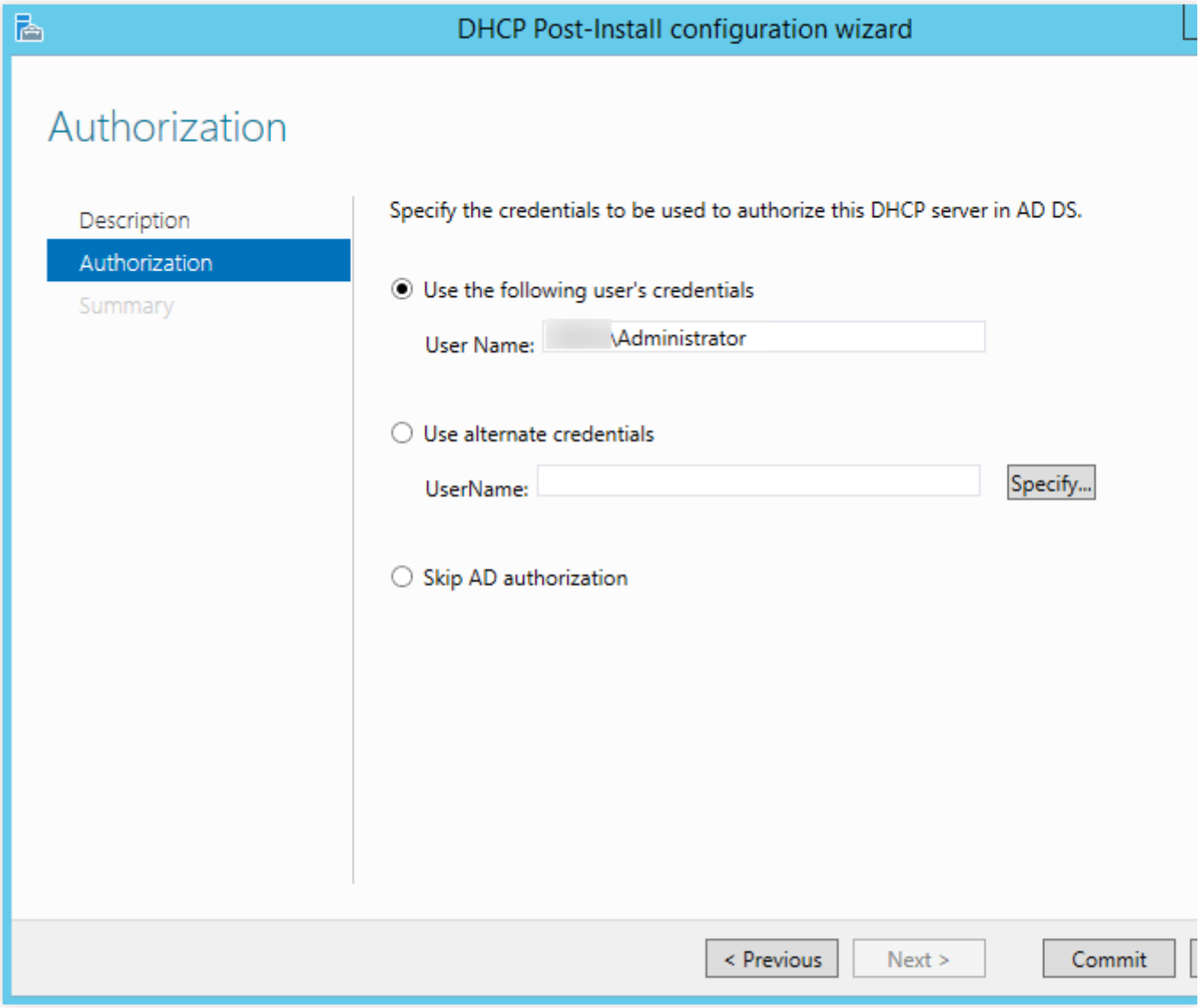
1. OSの画面で、

をクリックして、サーバーマネージャーを開きます。
2. 下図のように、サーバーマネージャーのウィンドウで、

をクリックして、**DHCPの設定を完了する**を選択します。



3. 表示された「DHCPインストール後設定ウィザード」ウィンドウで、**次へ**をクリックします。
4. 下図のように、デフォルトの設定を維持し、**送信**をクリックすると、インストール設定が完了します。



5. **閉じる**をクリックし、ウィザードウィンドウを閉じます。

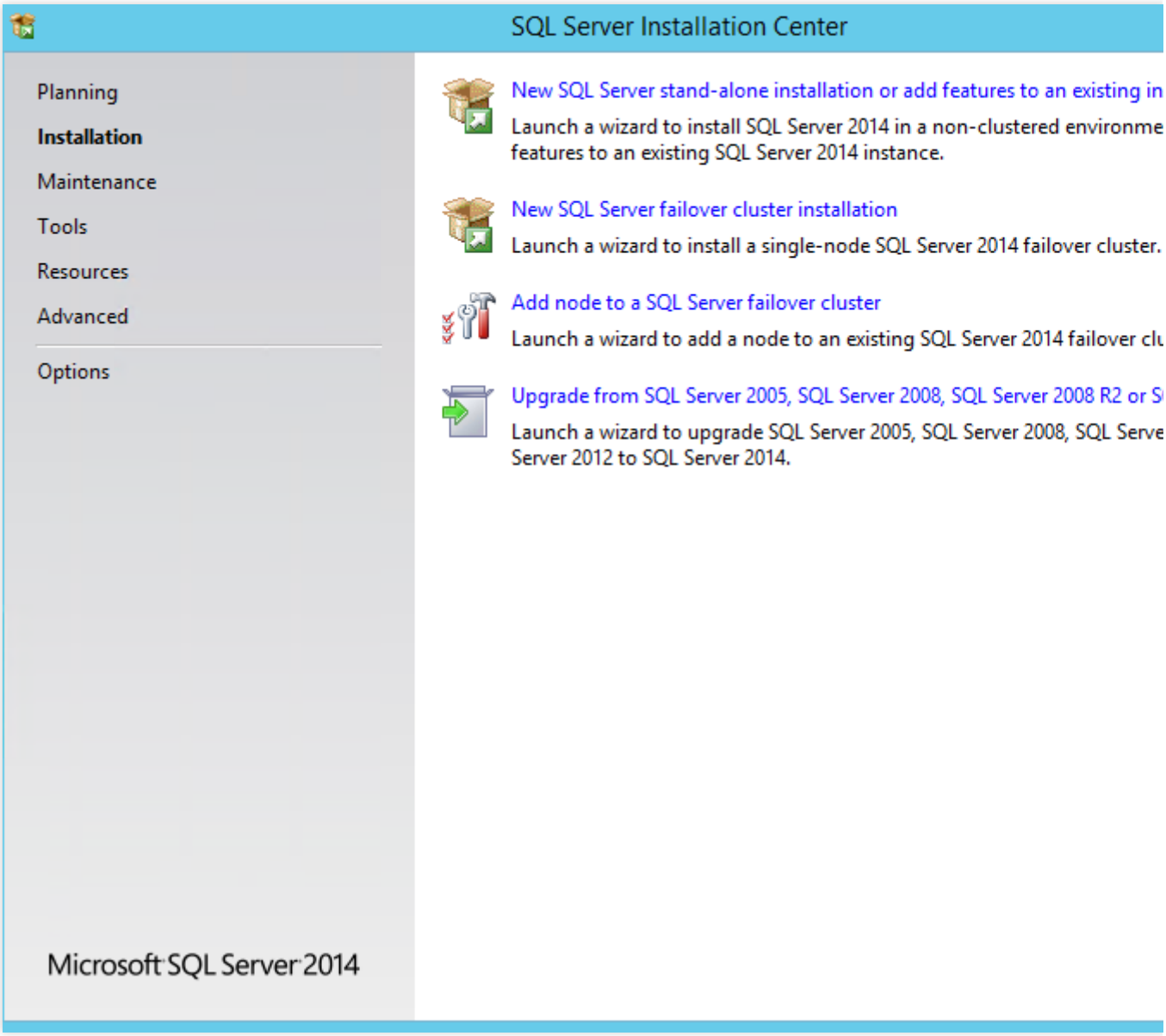
ステップ5：データベースSQL Server 2014のインストール

1. CVMでブラウザを開き、SQL Server 2014公式サイトにアクセスし、SQL Server 2014インストールパッケージをダウンロードします。

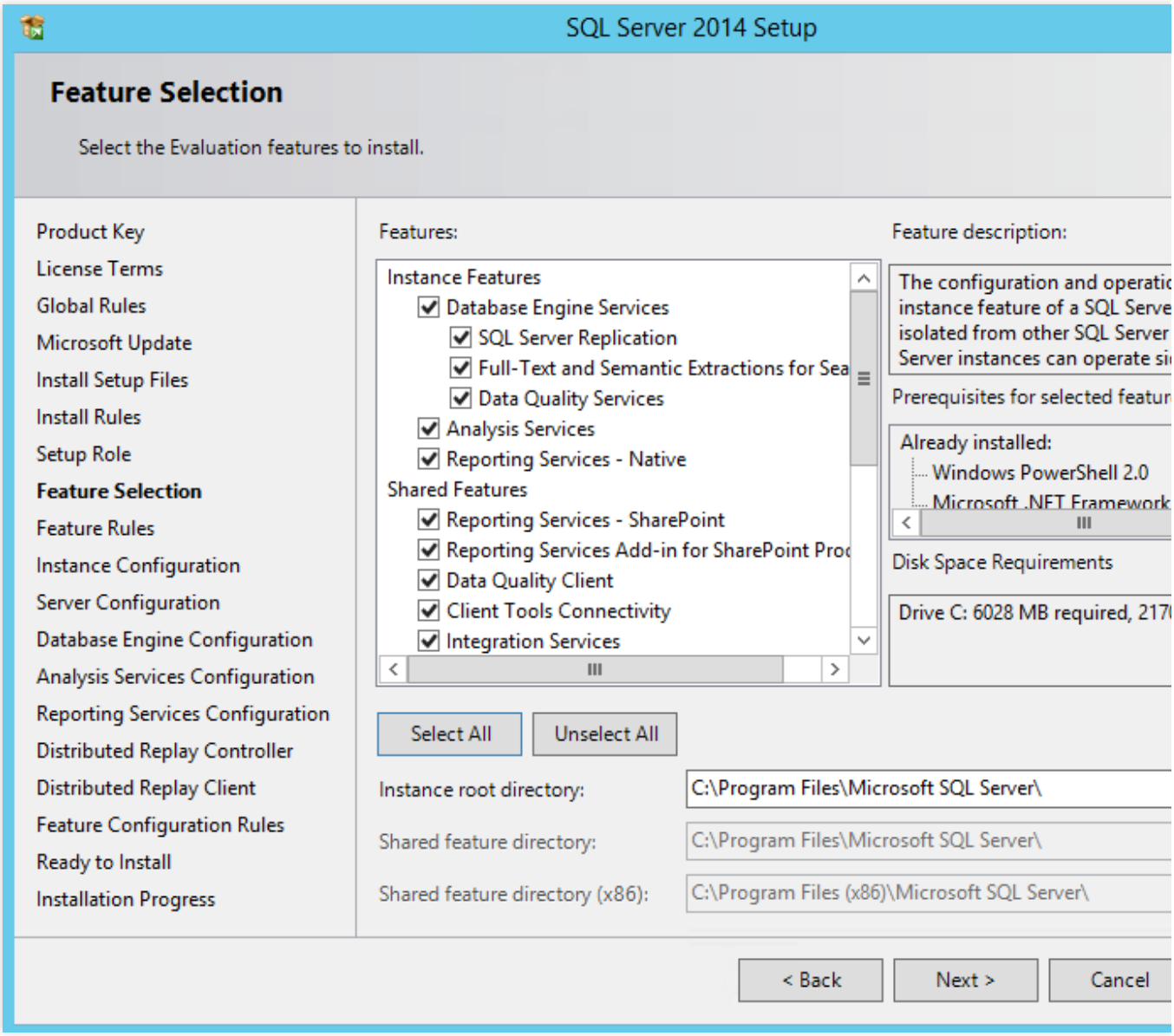
説明：

サードパーティのウェブサイトまたはその他の合法的な手段によってSQL Server 2014インストールパッケージを入手することもできます。

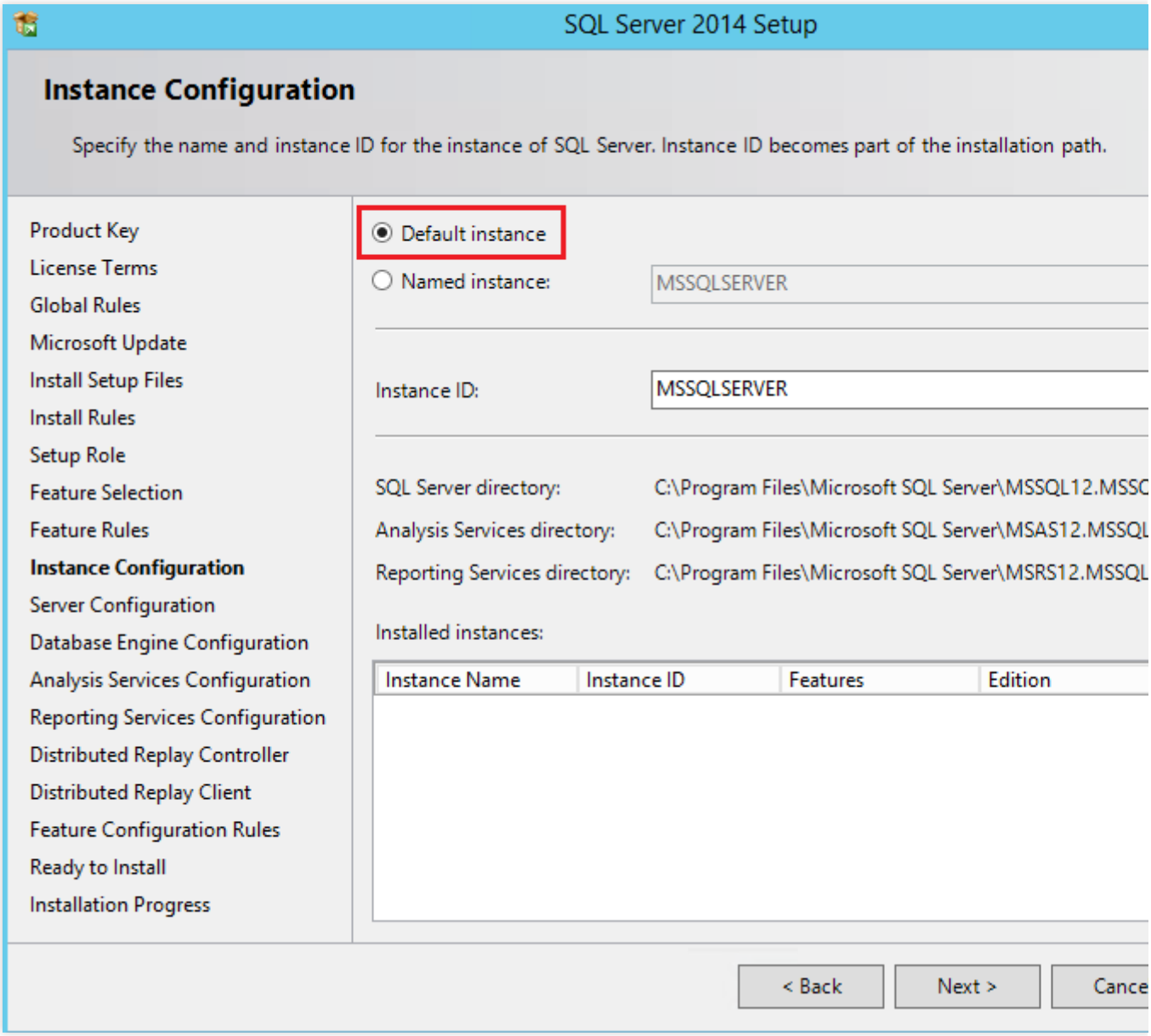
2. 「Setup.exe」ファイルをダブルクリックしてSQL Serverインストールウィザードを開き、下図のように、インストールオプションタブ画面で**新SQL Serverの単体インストールまたは既存のインストールに機能を追加する**をクリックします。



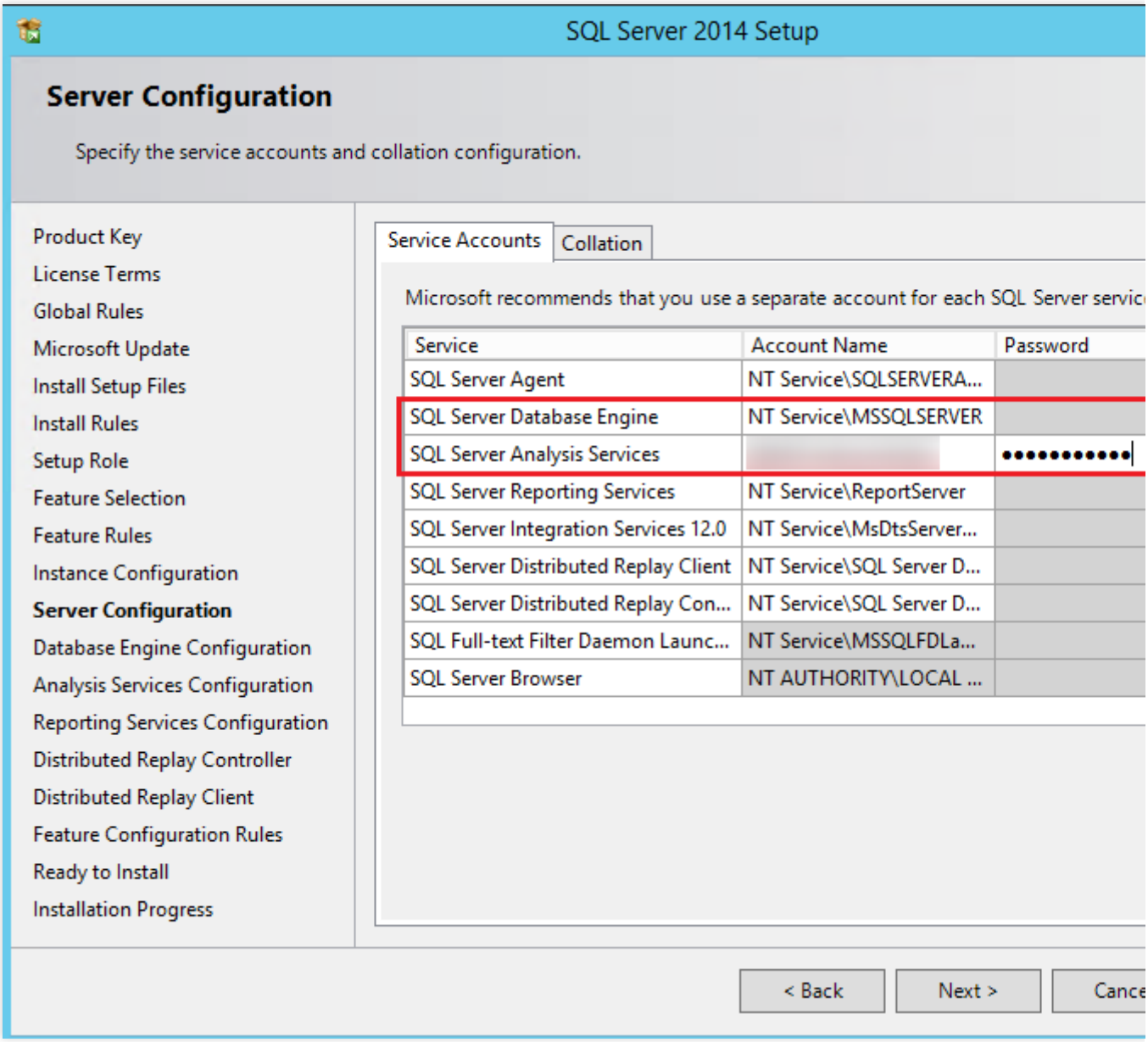
3. 製品キーを入力し、**次へ**をクリックします。
4. 「ライセンス条項に同意する」にチェックを入れ、**次へ**をクリックします。
5. デフォルトの設定を維持したまま、**次へ**をクリックします。
6. インストールチェックの完了後、**次へ**をクリックします。
7. デフォルトの設定を維持したまま、**次へ**をクリックします。
8. 下図のように、「機能の選択」画面で**すべて選択**をクリックし、すべての機能を選択して**次へ**をクリックします。



9. 下図のように、「インスタンスの設定」画面で**デフォルトのインスタンス**を選択し、**次へ**をクリックします。



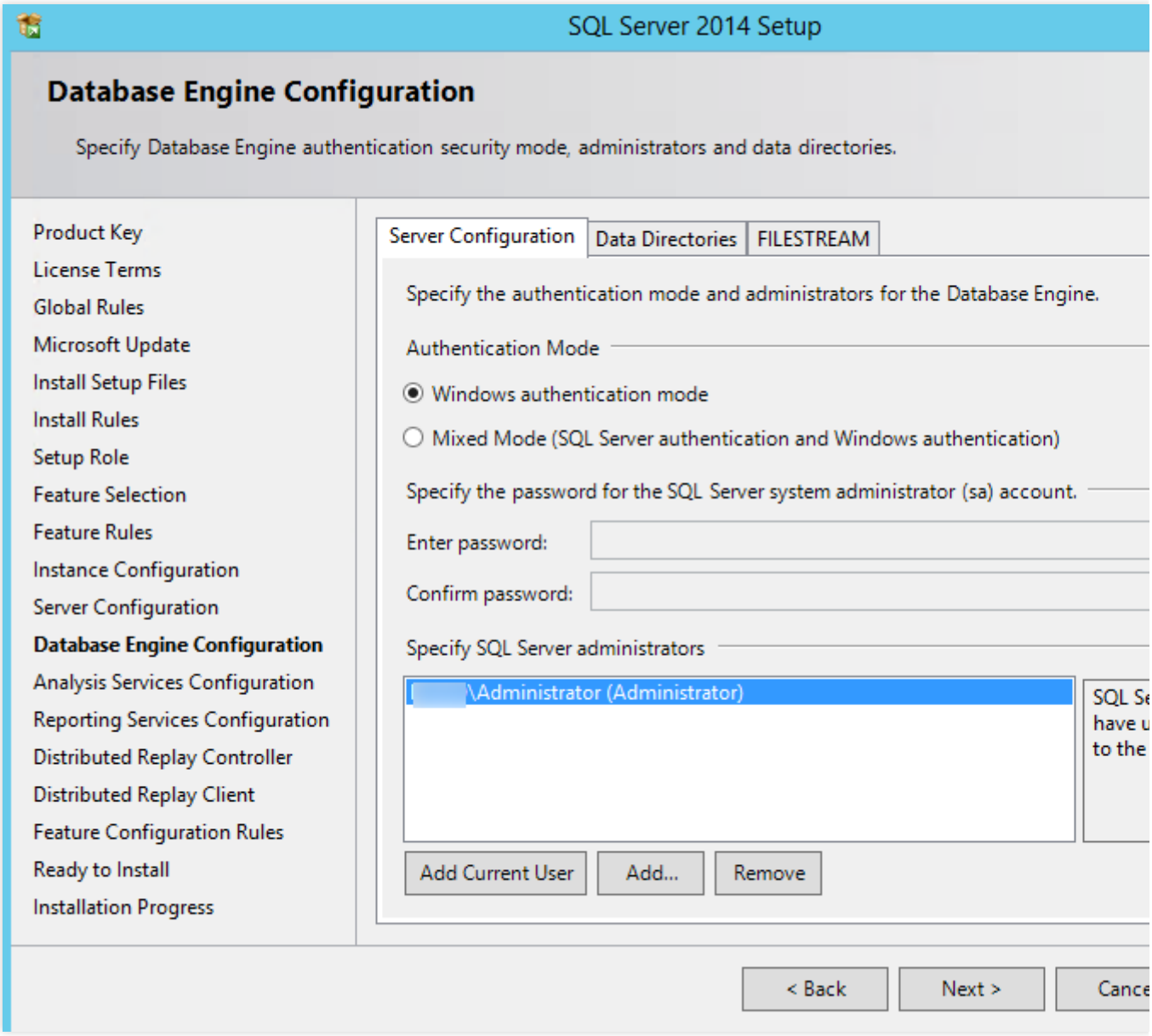
10. 下図のように、「サーバーの設定」画面で、SQL ServerデータベースエンジンサービスおよびSQL Server Analysis Servicesのアカウントとパスワードを設定し、**次へ**をクリックします。



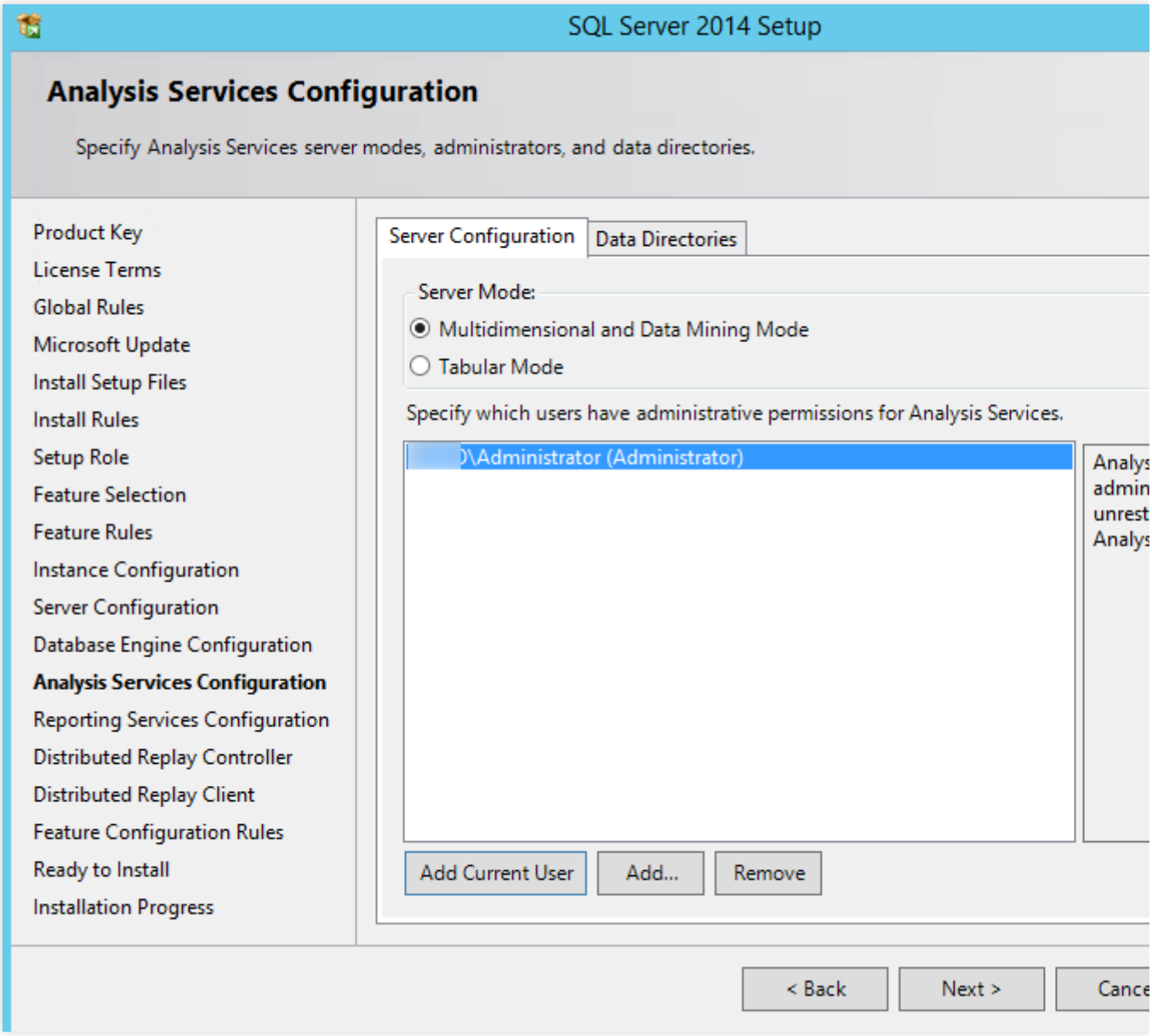
「SQL Serverデータベースエンジン」のアカウント名を「NT AUTHORITY\\NETWORK SERVICE」に設定します。

「SQL Server Analysis Services」のアカウント名とパスワードに、ステップ2：AD、DHCP、DNS、IISサービスの追加 中 14 - 15で設定したドメインアカウントとパスワードを設定します。

11. 下図のように、「データベースエンジン」画面で、**現在のユーザーを追加する**をクリックし、現在のアカウントをSQL Serverの管理者アカウントとし、**次へ**をクリックします。



12. 下図のように、「Analysis Servicesの設定」画面で、**現在のユーザーを追加する**をクリックし、現在のアカウントにAnalysis Servicesの管理者権限を追加し、**次へ**をクリックします。

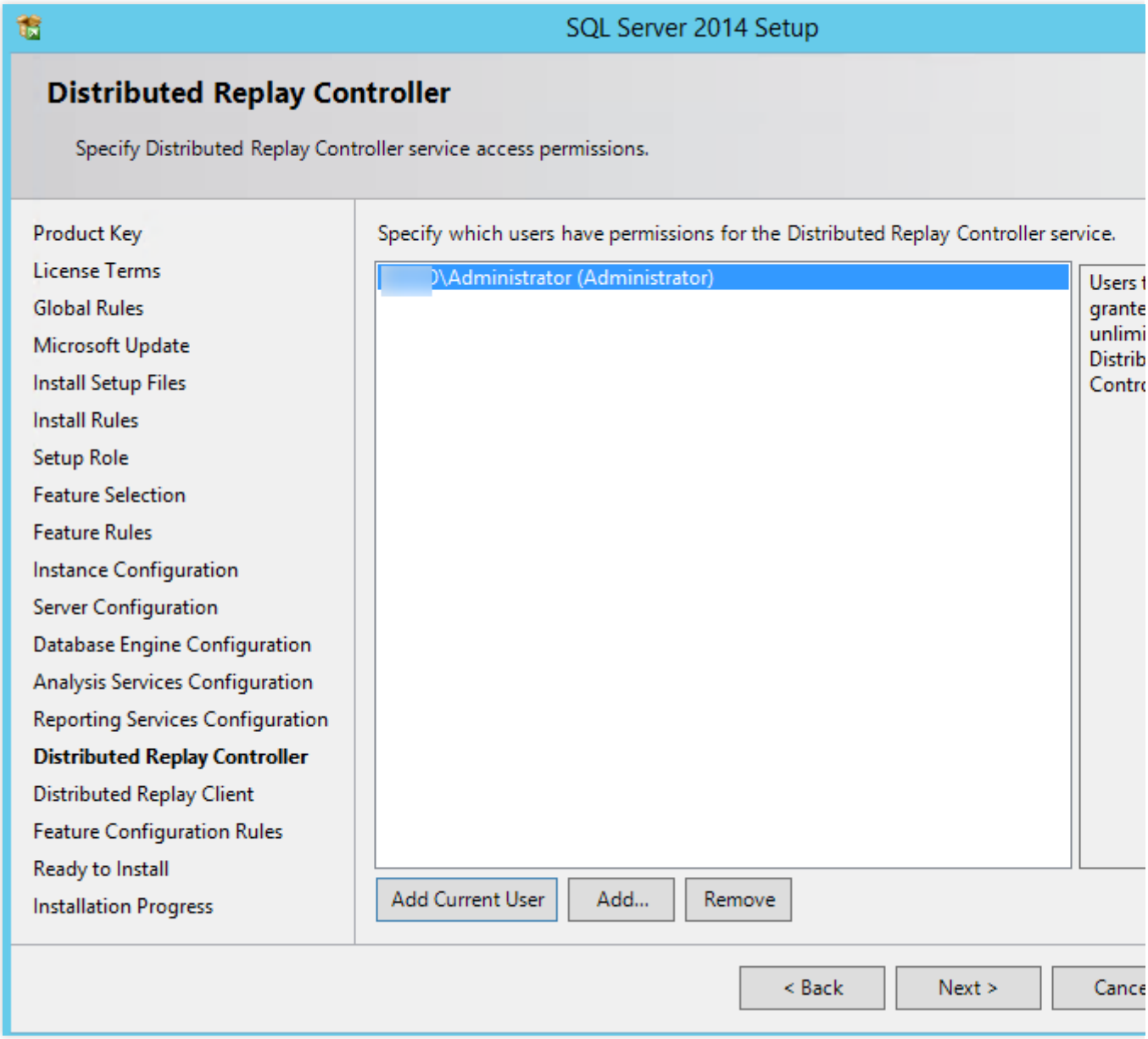


13. デフォルトの設定を維持したまま、**次へ**をクリックします。

14.

下図のように

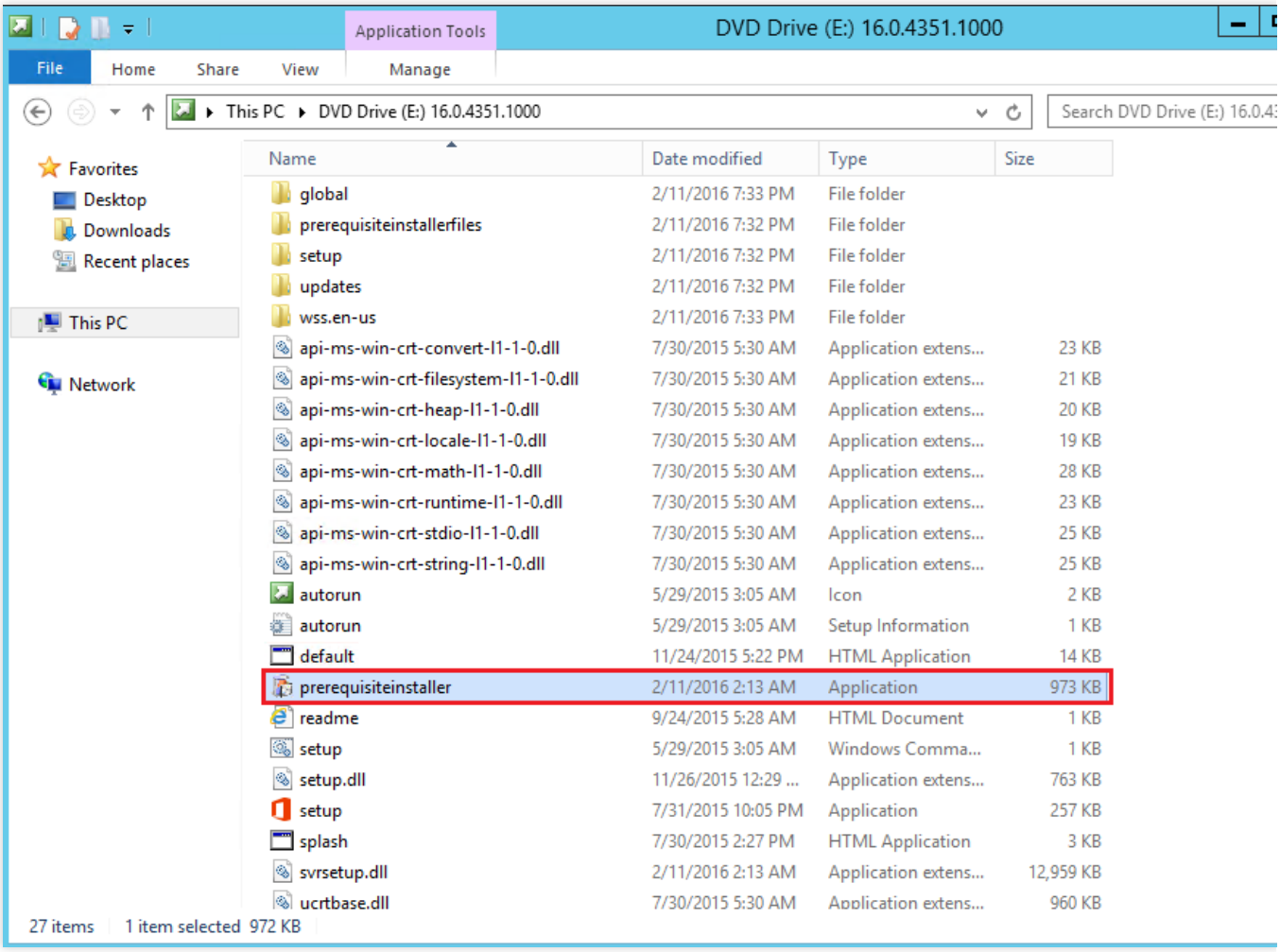
、「Distributed Replayコントローラ」画面で、**現在のユーザーを追加する**をクリックし、現在のアカウントにDistributed Replayコントローラの権限を追加し、**次へ**をクリックします。



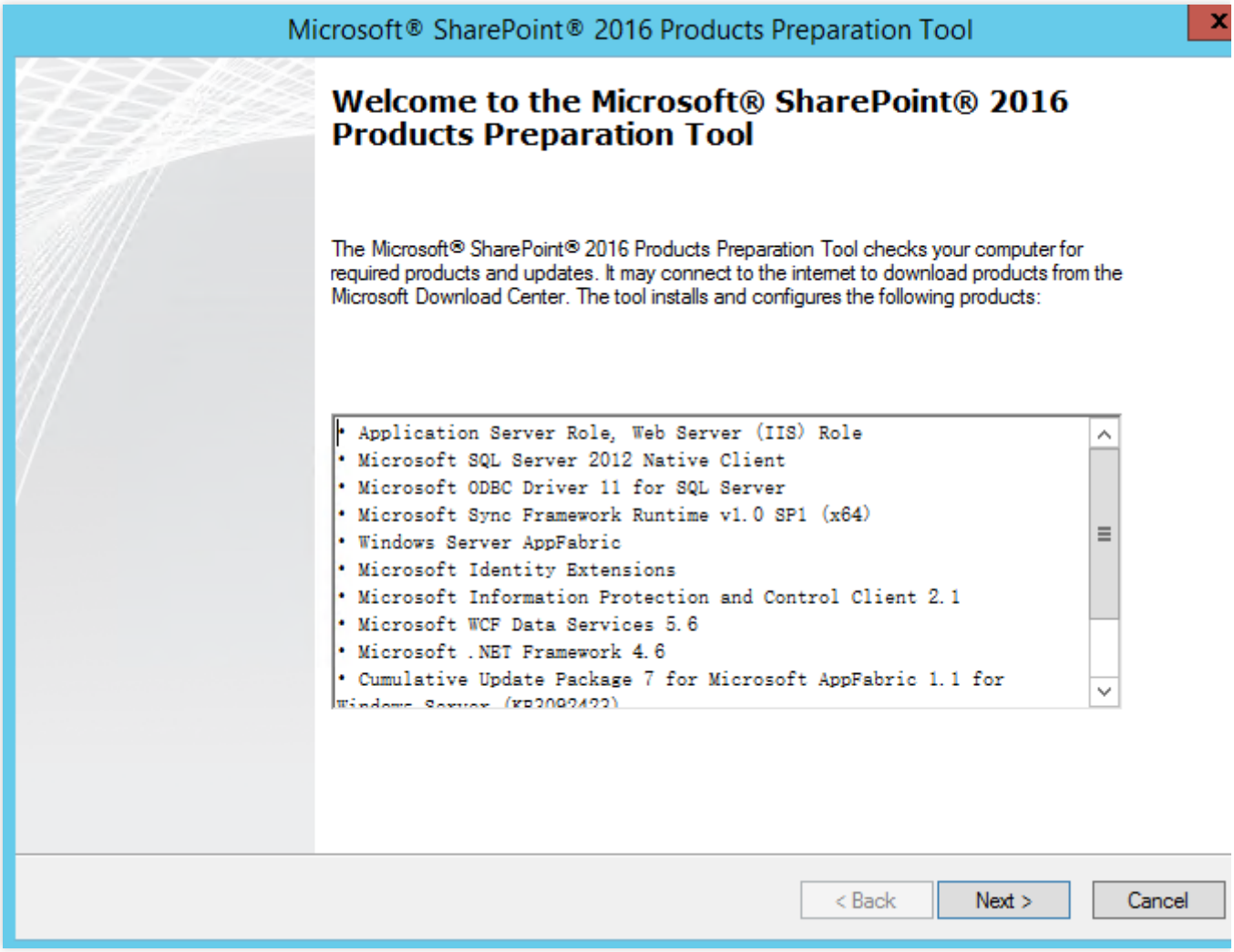
15.
デフォルト
の設定を維持したまま、インストールが完了するまで**次へ**をクリックします。

ステップ6：SharePoint 2016のインストール

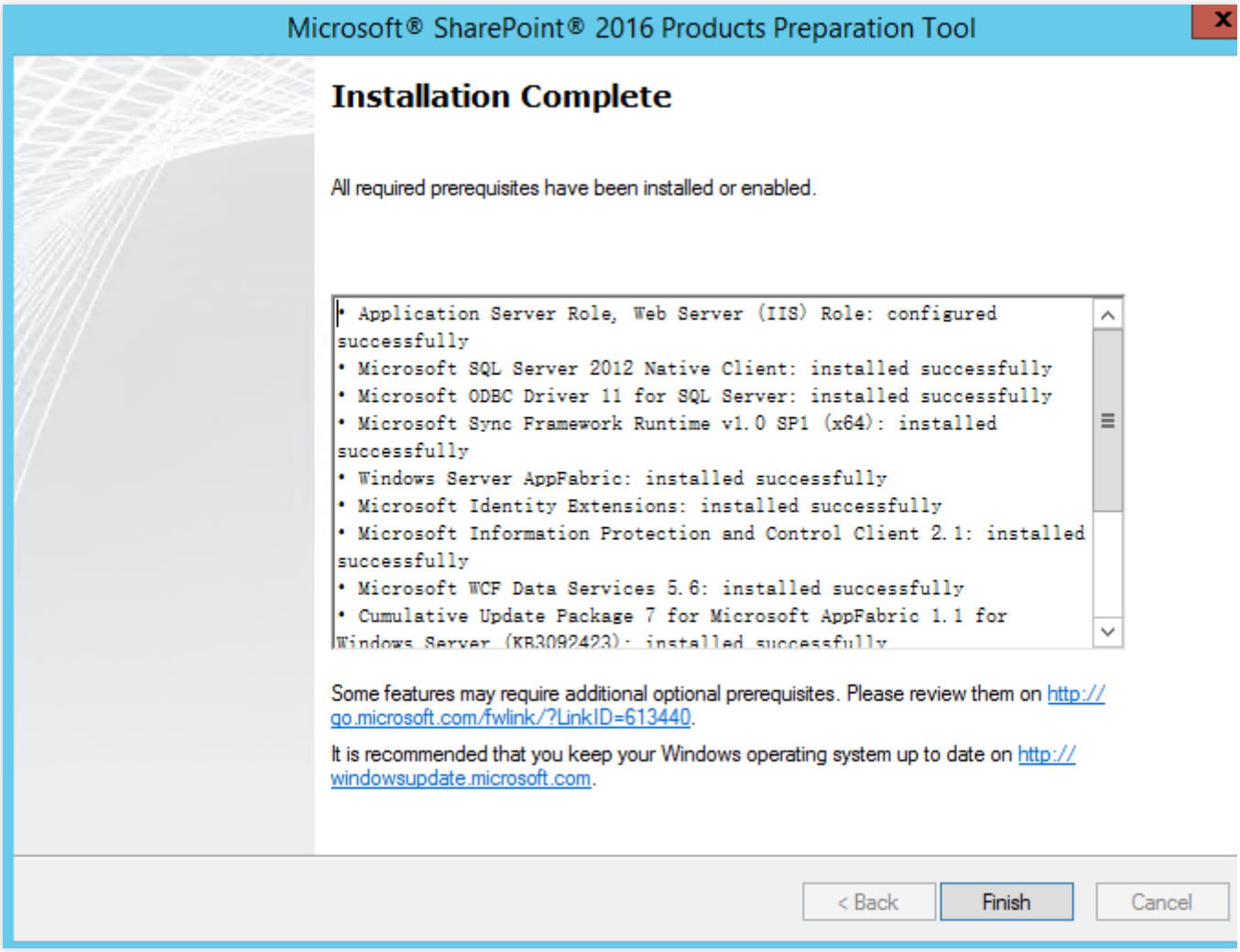
1. CVMでブラウザを開き、Microsoft SharePoint 2016公式サイトにアクセスし、Microsoft SharePoint 2016インストールパッケージをダウンロードします。
2. 下図のように、Microsoft SharePoint 2016イメージファイルを開き、準備ツールの実行可能ファイル `prerequisiteinstaller.exe` をダブルクリックし、Microsoft SharePoint 2016準備ツールをインストールします。



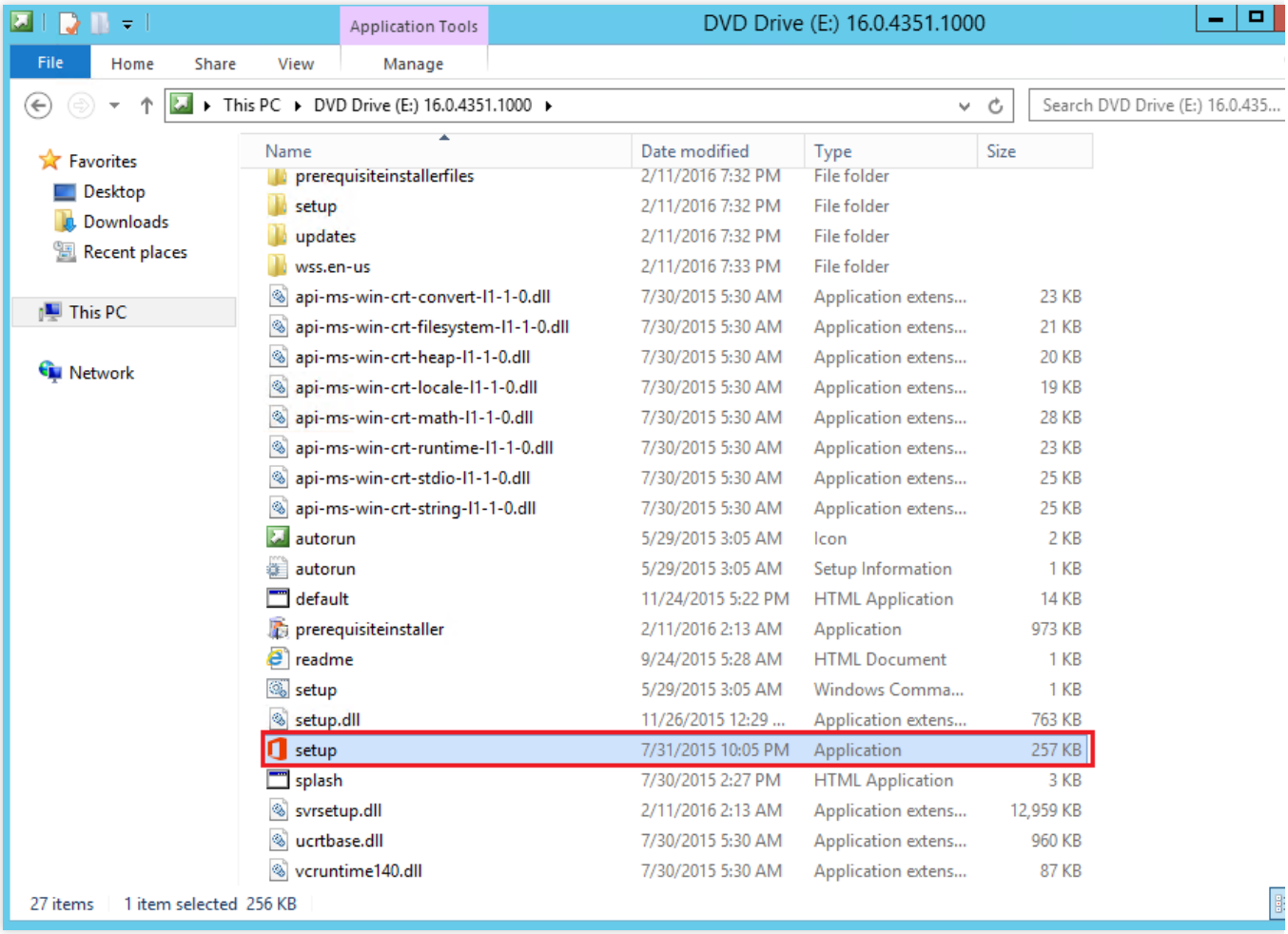
3. 下図のように、表示されたMicrosoft SharePoint 2016製品準備ツールのウィザードウィンドウで、**次へ**をクリックします。



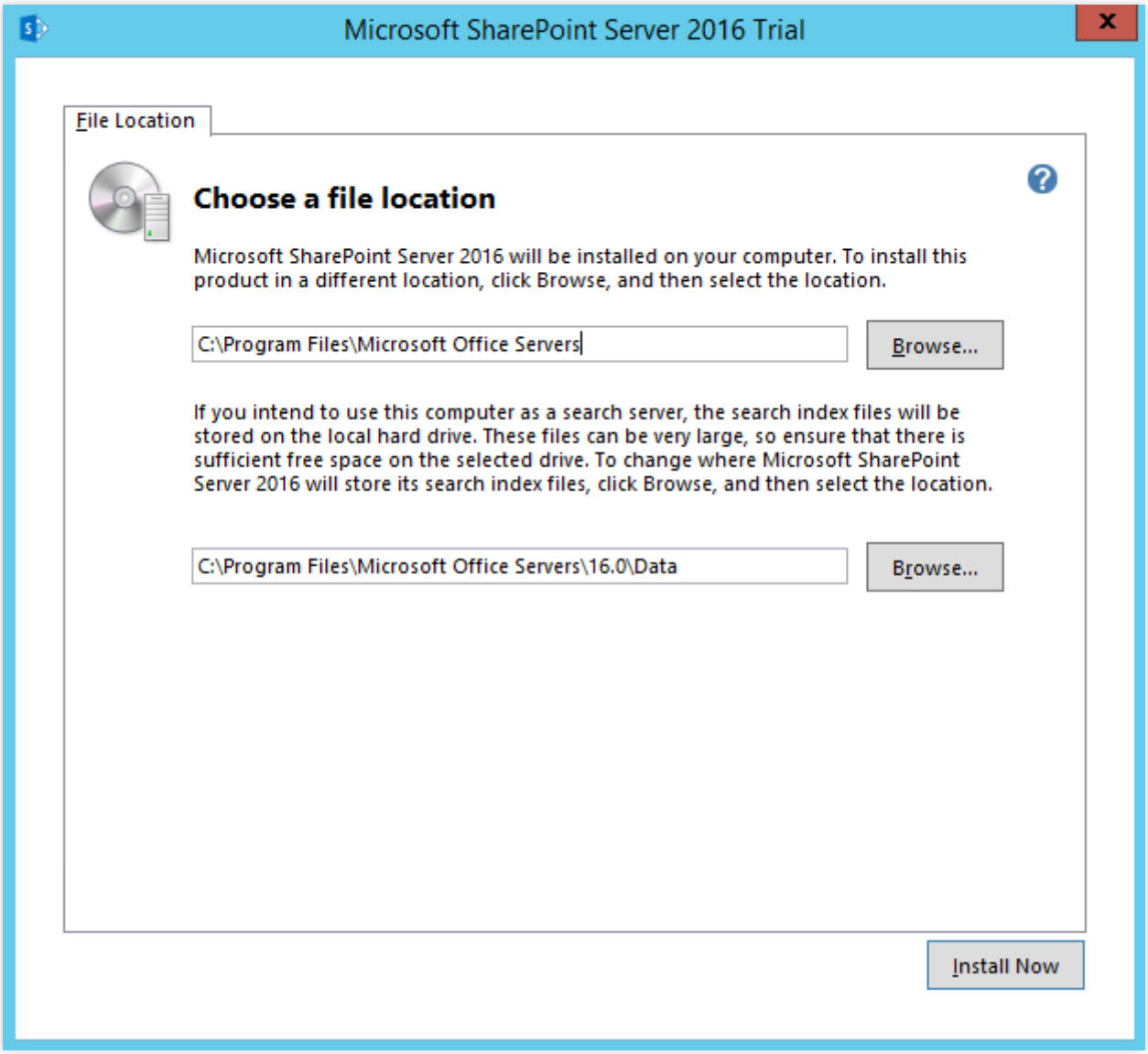
4. 「ライセンス規約の条項に同意する」にチェックを入れ、**次へ**をクリックします。
5. 下図のように、必須コンポーネントのインストールが完了してから、**完了**をクリックし、CVMを再起動します。



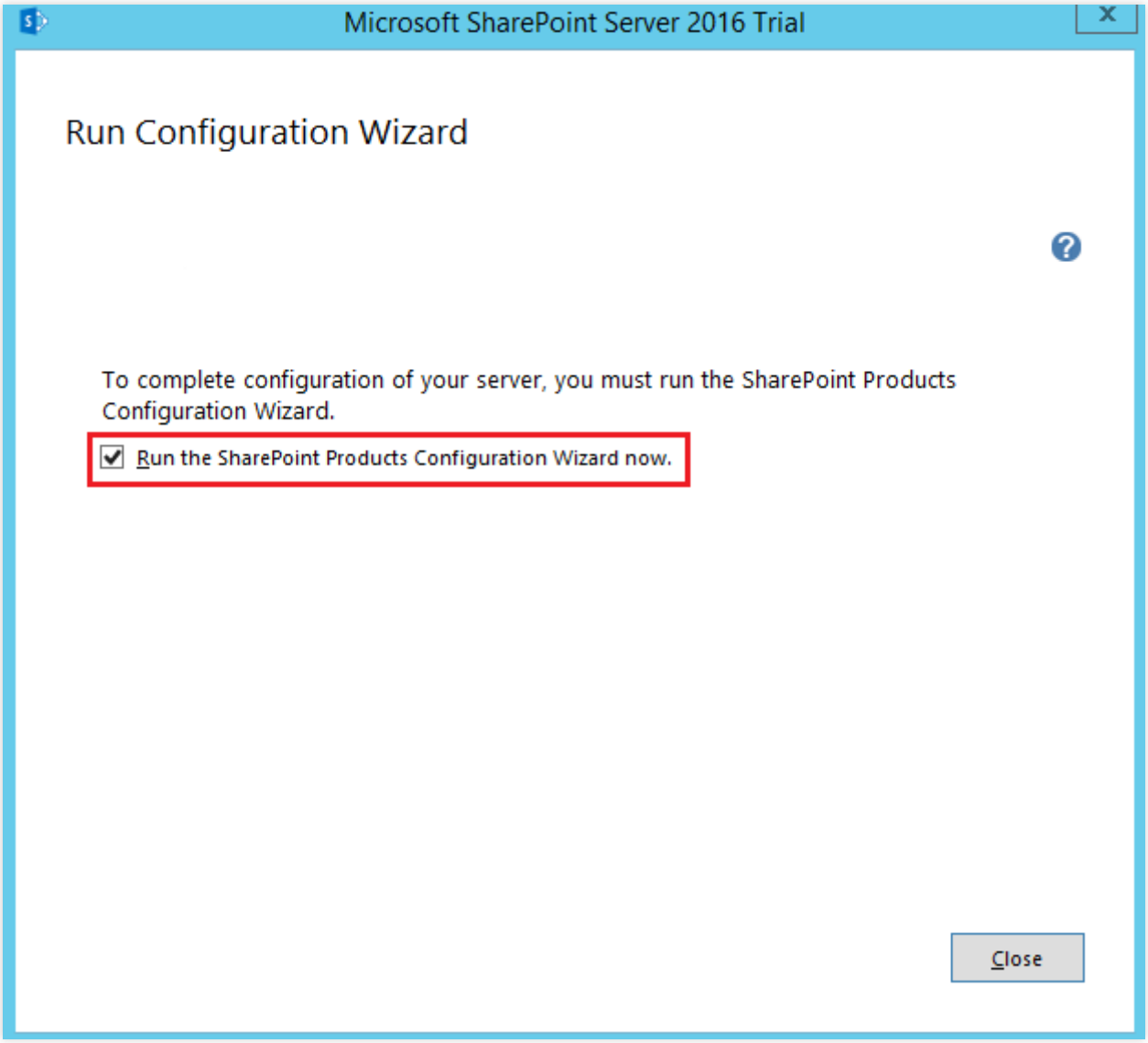
6. 下図のように、Microsoft SharePoint 2016イメージファイルを開き、インストールファイル `setup.exe` をダブルクリックし、Microsoft SharePoint 2016のインストールを開始します。



7. 製品キーを入力し、**続ける**をクリックします。
8. 「この規約の条項に同意する」にチェックを入れ、**続ける**をクリックします。
9. 下図のように、インストールディレクトリを選択し（この例ではデフォルト設定を維持していますが、実際の状況に応じて対応するインストールディレクトリを選択できます）、**今すぐインストール**をクリックします。

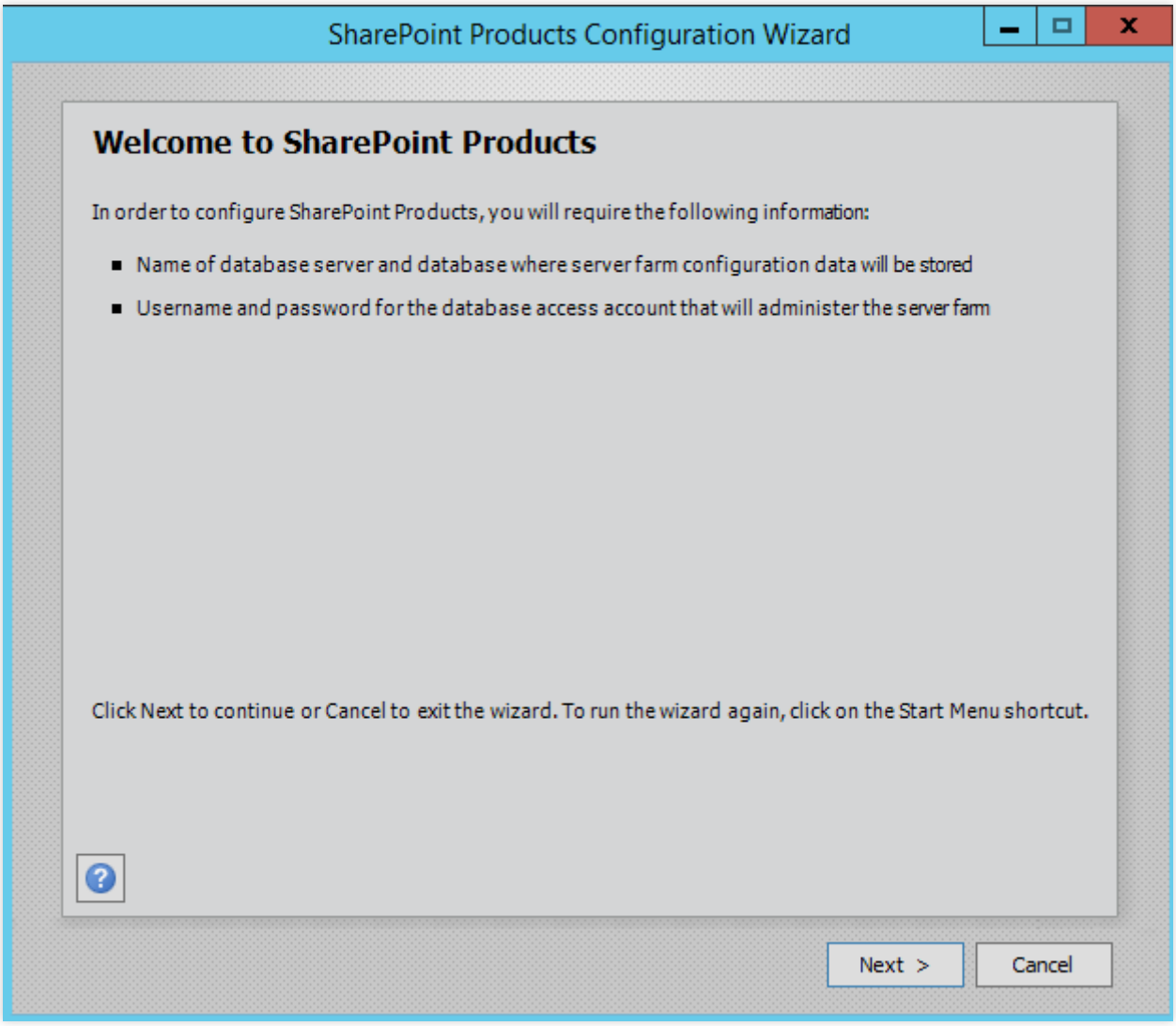


10. インストールの完了後、下図のように、「SharePoint製品設定ウィザードを今すぐ実行する」にチェックを入れ、**閉じる**をクリックします。



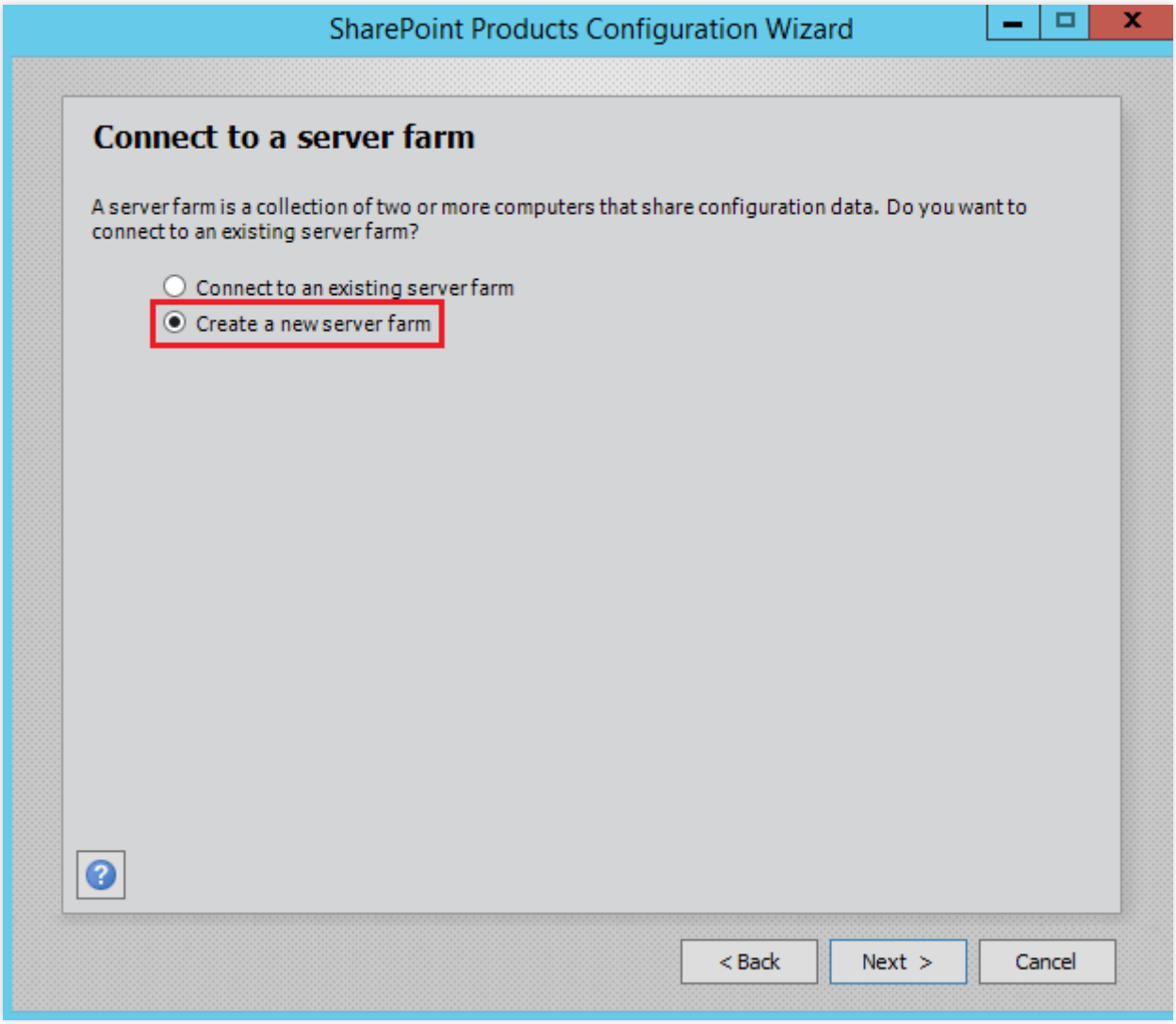
ステップ7：SharePoint 2016の設定

1. 下図のように、実行したSharePoint製品設定ウィザードで、**次へ**をクリックします。



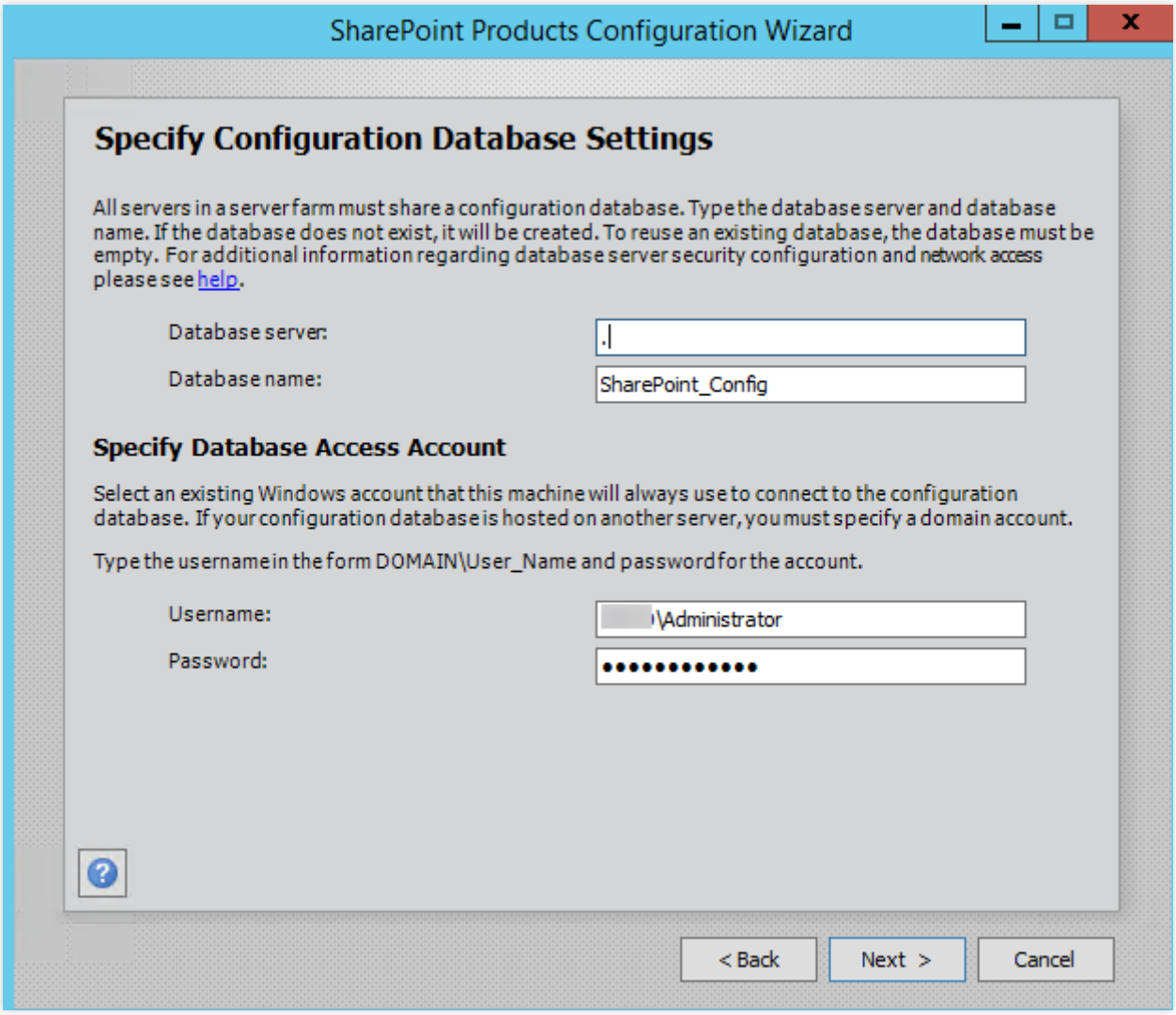
2. ポップアップしたプロンプトウィンドウで、**はい**をクリックし、設定途中でのサービスの再起動を許可します。

3. 下図のように、**サーバーファームを新規作成する**を選択し、**次へ**をクリックします。

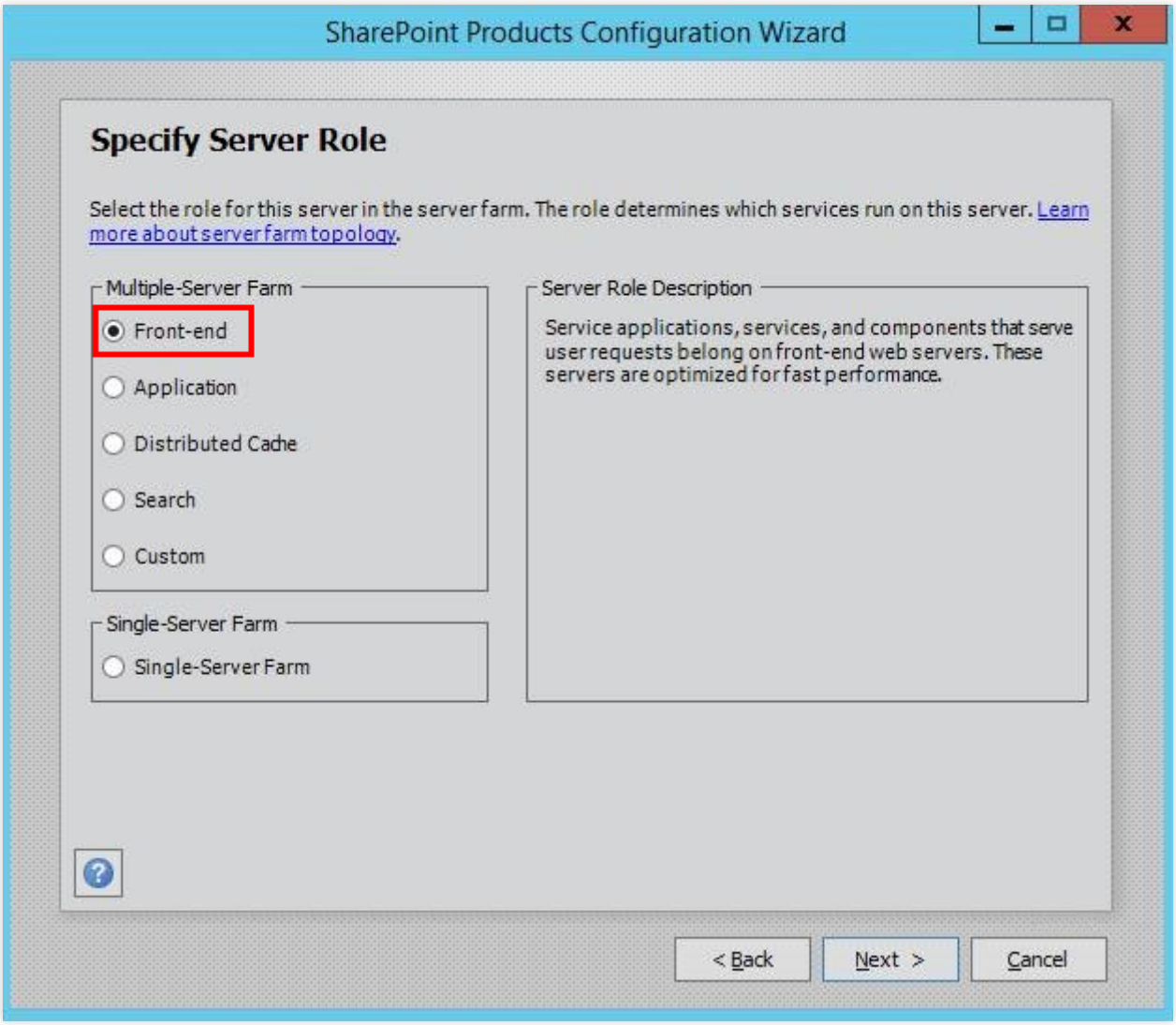


4. 下図のように、データベース設定とデータベースにアクセスするアカウントの情報を指定し、**次へ**をクリックします。

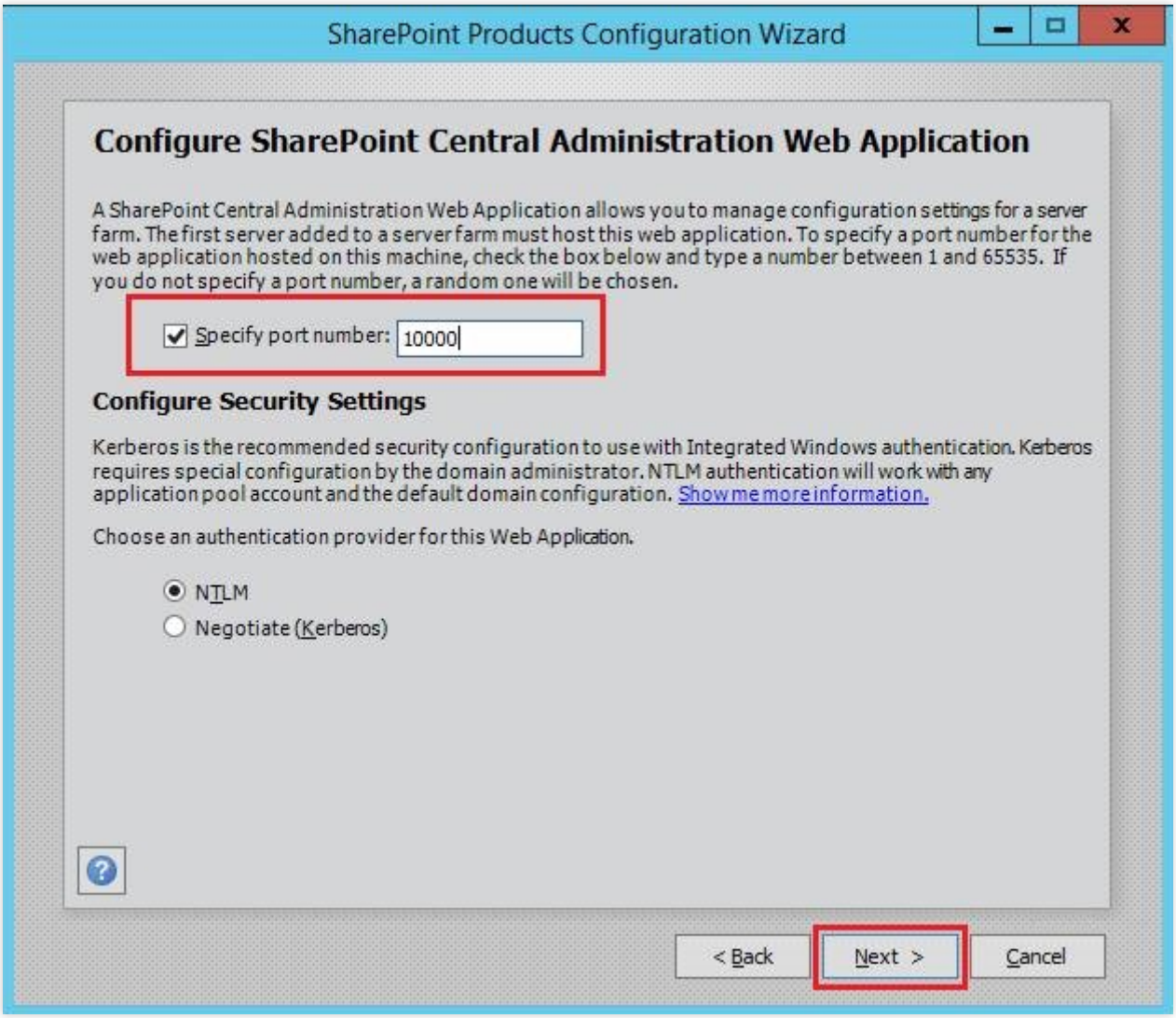
Sharepointのデータベースはローカルマシンにあるため、ローカルマシンのデータベースとアカウントを入力します。



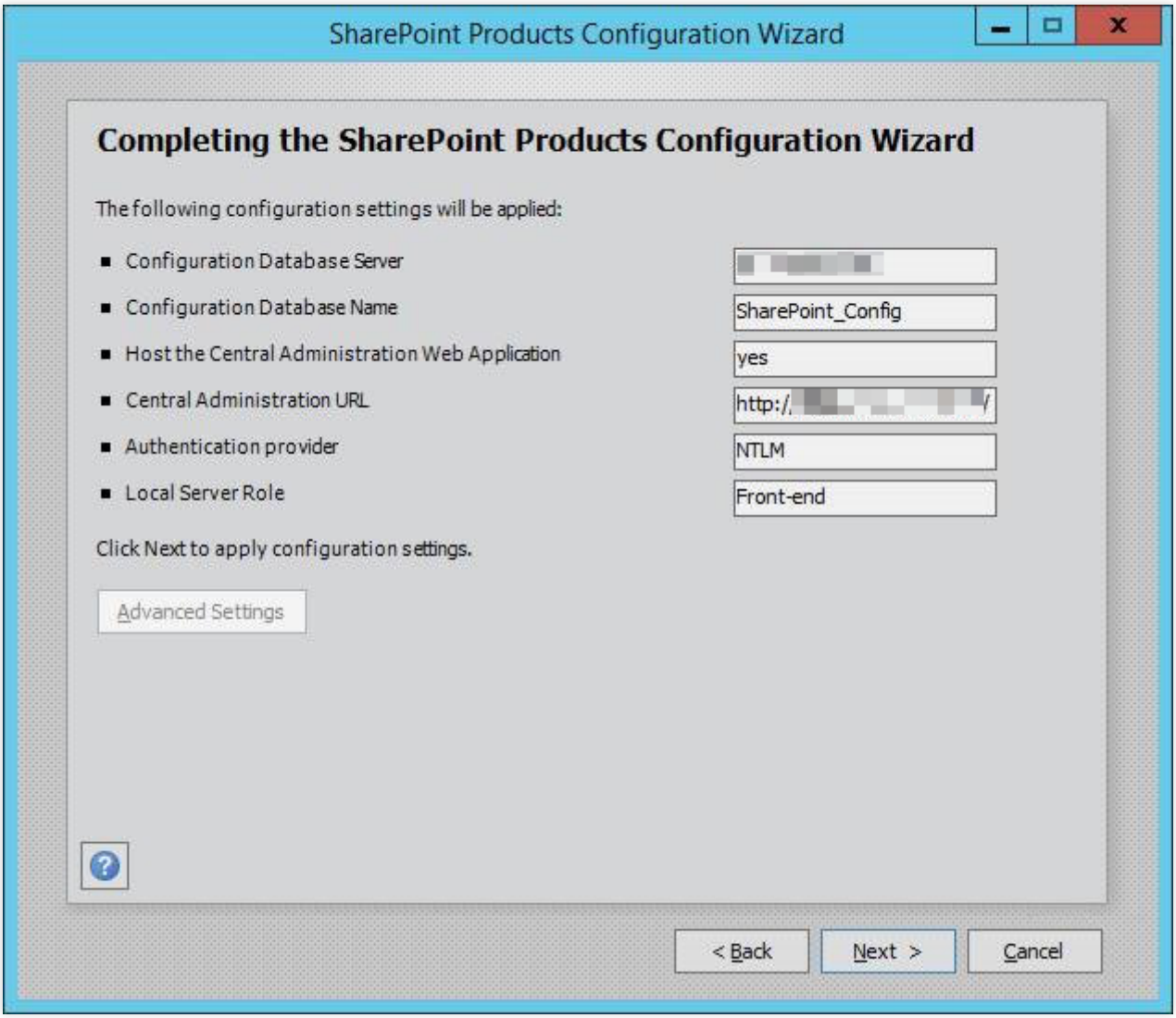
5. 指定するサーバーファームのパスワードを設定し、**次へ**をクリックします。
6. 下図のように、「マルチサーバーファーム」を**フロントエンド**に設定し、**次へ**をクリックします。



7. 下図のように、Sharepoint管理センターのポート番号を設定し（この例ではポート番号を10000としていますが、ポート番号は実際の状況に応じて設定することができます）、**次へ**をクリックします。



8. 下図のように、SharePointの設定を確認し、**次へ**をクリックします。



9. SharePointの設定完了後、**完了**をクリックします。

BT Windowsパネルのインストール

最終更新日：：2022-05-07 15:20:31

概要

BTパネルは、LinuxおよびWindowsシステムをサポートする使いやすく、一生無料で使える強力でインタラクティブなサーバー管理ソフトウェアです。BTパネルでは、LAMP、LNMP、Webサイト、データベース、FTP、SSLをワンクリックで設定でき、Web側からサーバーを簡単に管理できます。
このドキュメントでは、WindowsオペレーティングシステムのCVMで、Tencent Cloud Market Mirrorを介してBTパネルを速やかにインストールする方法について説明します。

操作手順

CVMの作成時のBTパネルインストール

ご注意：
購入したCVMにBTパネルをインストールする場合は、システムの再インストール をして、イメージ市場で対応するイメージを選択し、環境の導入を完了できます。海外の一部の地域のCVMでは、イメージ市場におけるシステムの再インストールがサポートされていません。別の地域のCVMを使用することをお勧めします。インストールの詳細については BTパネルの公式サイト をご参照ください。
1. CVMコンソール にログインし、インスタンス管理ページの**新規作成**をクリックします。
2. ページの指示に従ってモデルを選択し、「イメージ」で**イメージ市場>イメージ市場から選択する**をクリックします。下図の通りです：
ご注意：
海外の一部の地域のCVMでは、イメージ市場におけるCVMの新規作成がサポートされていません。選択した地域に**イメージ市場**がない場合、他のイメージ市場をサポートする地域を選択してください。
2 GB以上のメモリと40 GB以上のシステムディスクを備えたインスタンス構成をお勧めします。
3. 「イメージ市場」ウィンドウのの検索ボックスで、**運用保守ツール**を選択し、「BT」と入力して

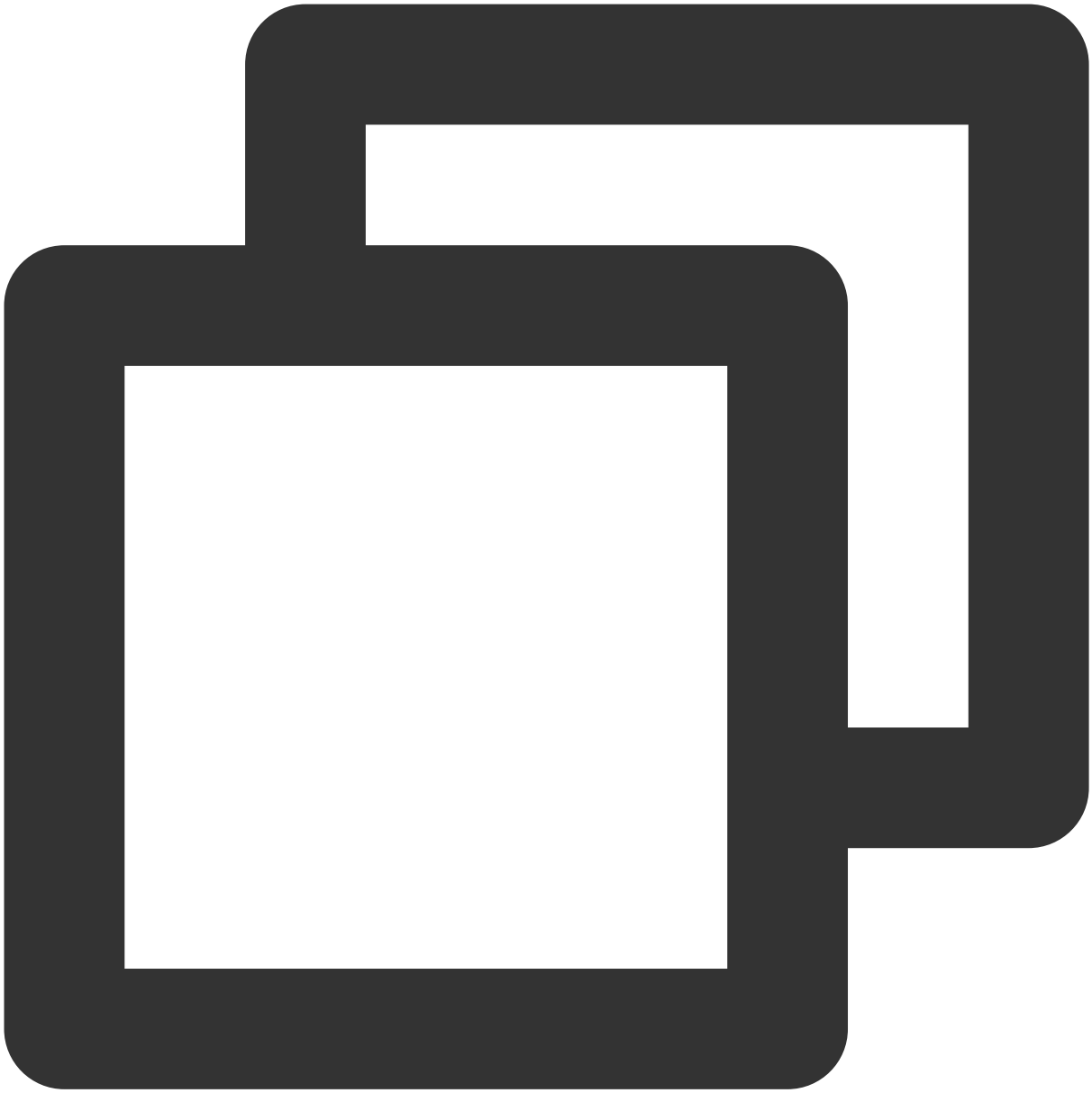
をクリックします。
4. 希望のイメージを選択します。このドキュメントでは、**BT Windowsパネル公式版（WAMP/WNMP/Tomcat/Node.js）**を例とします。**無料利用**をクリックします。
5. インスタンスに関連付けられるセキュリティグループにはポート8888をオープンするためのインバウンドルールを追加してください。詳細については、セキュリティグループルールの追加 をご参照ください。

ストレージメディア、帯域幅などの他の設定は実際のニーズに合わせて選択して、最後に購入を選択しBTパネルの作成を完了します。

パネルログイン情報の取得

1. CVMにログインします。詳細については、標準方式を使用してWindowsインスタンスにログイン をご参照ください。
2. オペレーティングシステムの画面で、左下の

を右クリックし、ポップアップメニューから**実行**をクリックします。
3. cmdウィンドウで次のコマンドを実行すると、ログイン情報を取得します。

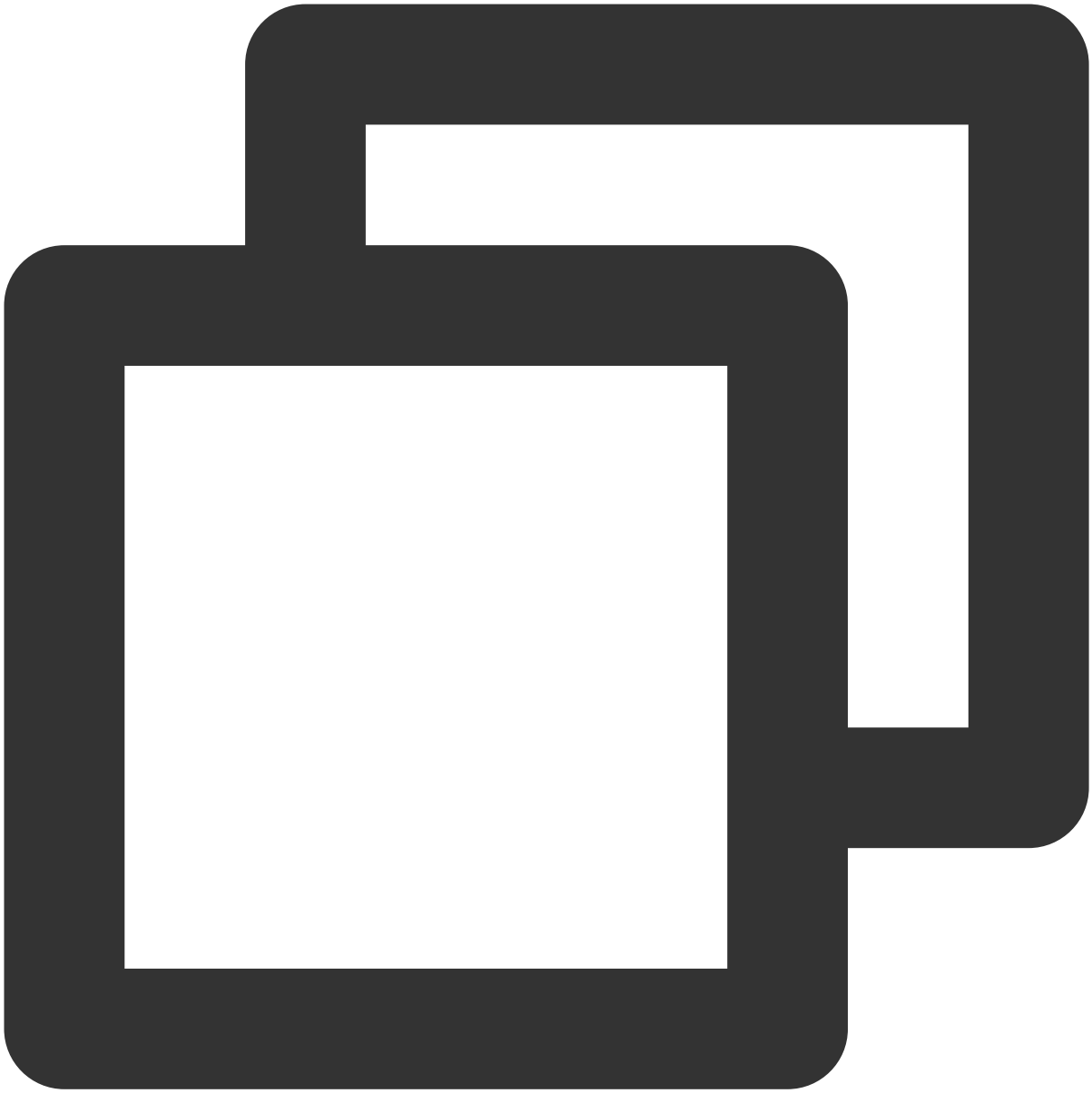


```
bt default
```

結果が返された後。 BT パネルのアドレスとログイン情報を記録します。

BTパネルのログイン

1. ローカルコンピュータでブラウザを開き、取得したBTパネルのアドレスにアクセスします。



```
http://云服务器公网 IP:8888/xxxx
```

2. レコードの「username」と「password」を入力し、**ログイン**をクリックします。
3. [利用規約に同意します]のチェックを入れ、**パネルへ進む**をクリックします。
4. 実際のビジネスニーズに応じて、インストールするコンポーネントと導入Webサイトをパネルから選択します。

Dockerの構築

最終更新日：：2024-03-05 16:43:39

概要

ここでは、Tencent Cloud CVMでDockerを構築、使用する方法についてご説明します。Linux OSを熟知し、Tencent Cloud CVMを使い始めたばかりの開発者を対象にしています。Dockerの詳細については、Docker公式ドキュメント をご参照ください。

説明：

Windows OSのCVMでDockerを構築、使用する必要がある場合は、WindowsへのDockerデスクトップのインストール をご参照ください。

デモ用オペレーティングシステム

このドキュメントでは、CVMインスタンスのオペレーティングシステムの例としてCentOS 8.2およびをを使用します。

TencentOS Serverオペレーティングシステムを使用している場合は、実際の対応バージョンを使用してください：

TencentOS Server 2.4：イメージにはDockerが組み込まれたため、インストールする必要はありません。Dockerの使用 を参照してそのまま使用してください。

TencentOS Server 3.1(TK4)：ドキュメントの手順を参照して構築してください。

前提条件

Linux CVMを購入済みであること。

説明：

Dockerの構築には64ビットシステムを使用し、カーネルバージョンが3.10以上である必要があります。

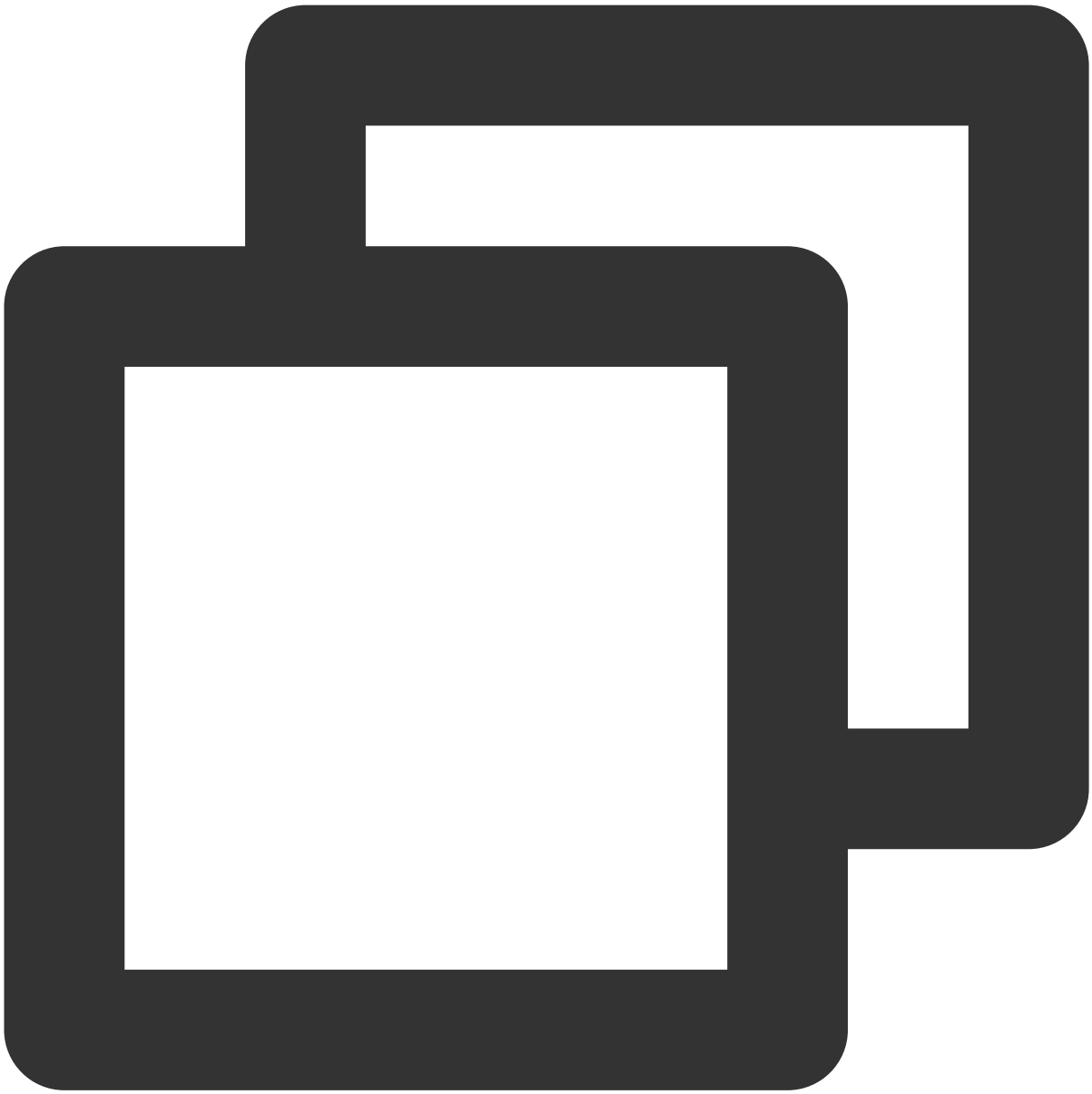
操作手順

Dockerのインストール

実際に使用しているOSのバージョンに応じて、次の手順で操作します：

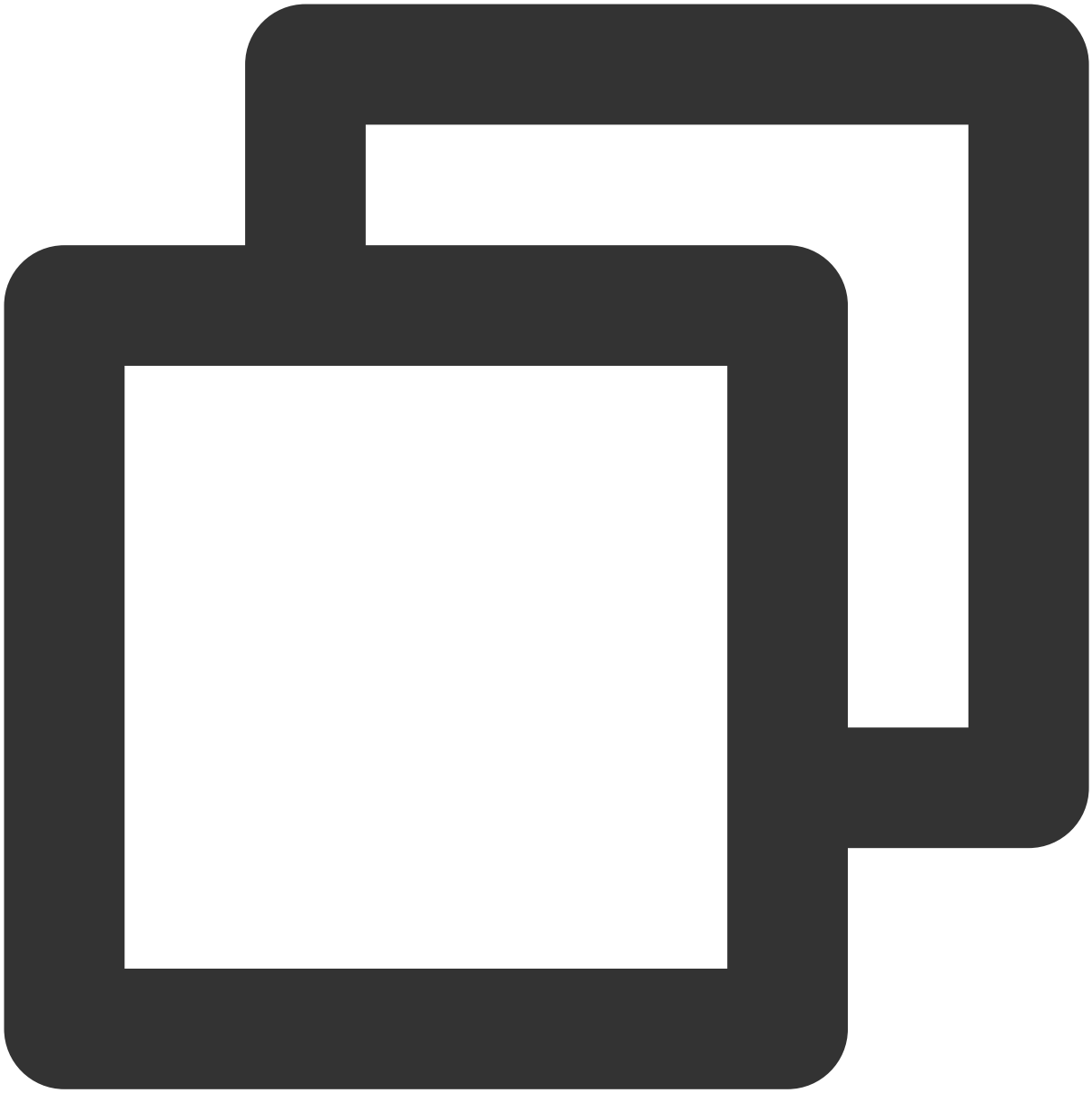
CentOS 8.2

1. 標準方式を使用してLinuxインスタンスにログイン（推奨）します。
2. 次のコマンドを実行して、Dockerリポジトリを追加します。



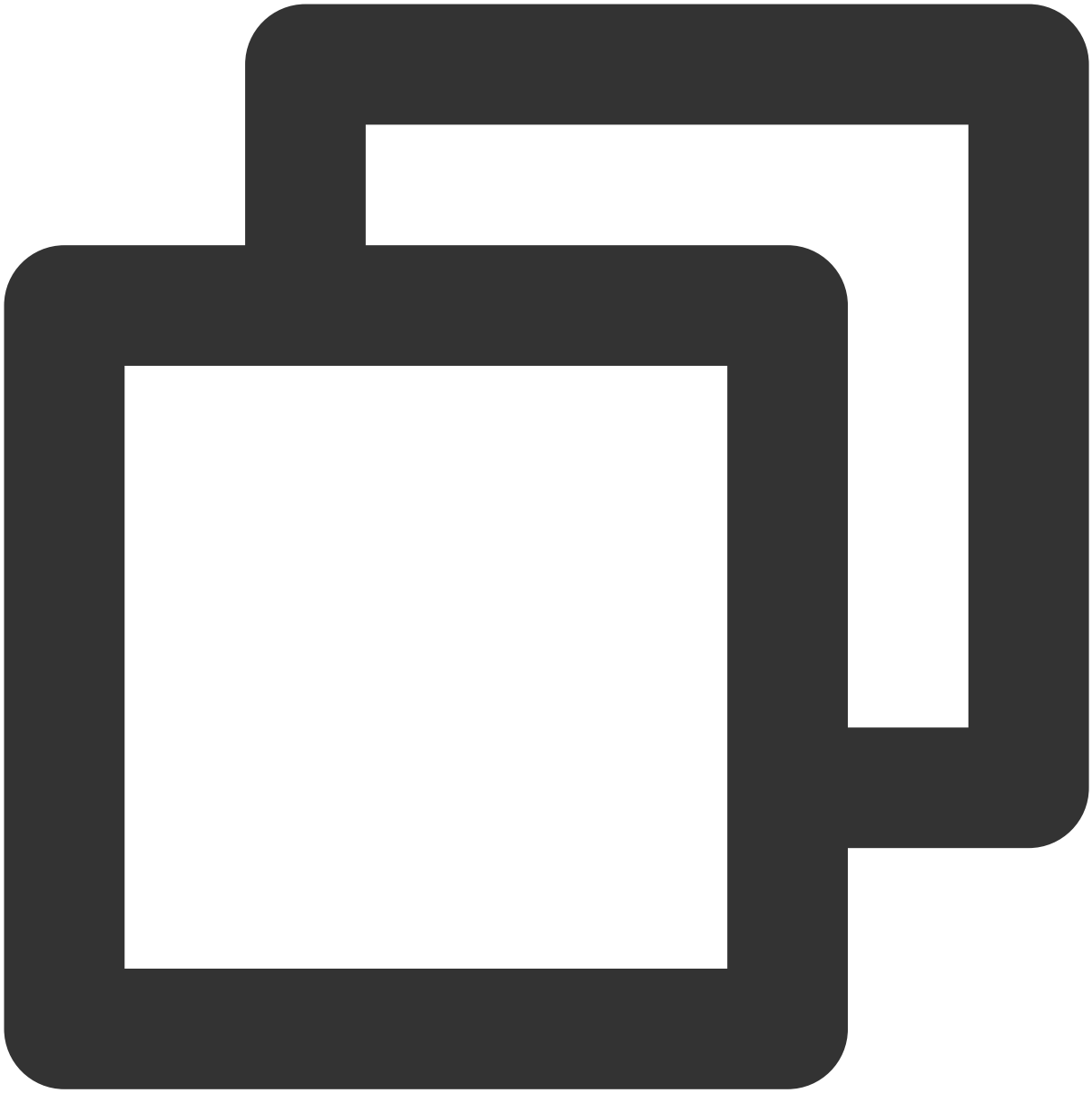
```
dnf config-manager --add-repo=http://mirrors.tencent.com/docker-ce/linux/centos/doc
```

3. 次のコマンドを実行して、追加されたDockerリポジトリを確認します。



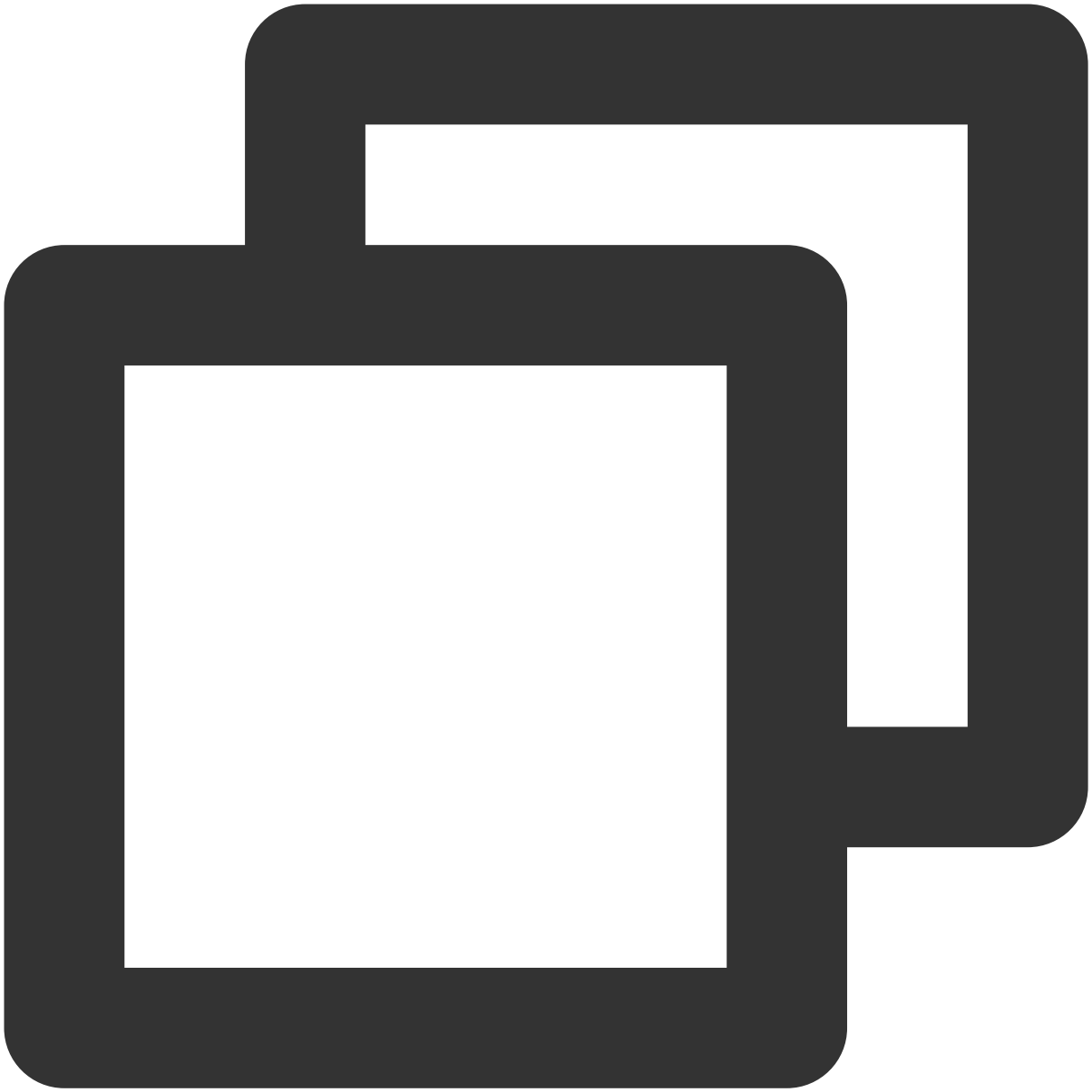
```
dnf list docker-ce
```

4. 次のコマンドを実行して、Dockerをインストールします。



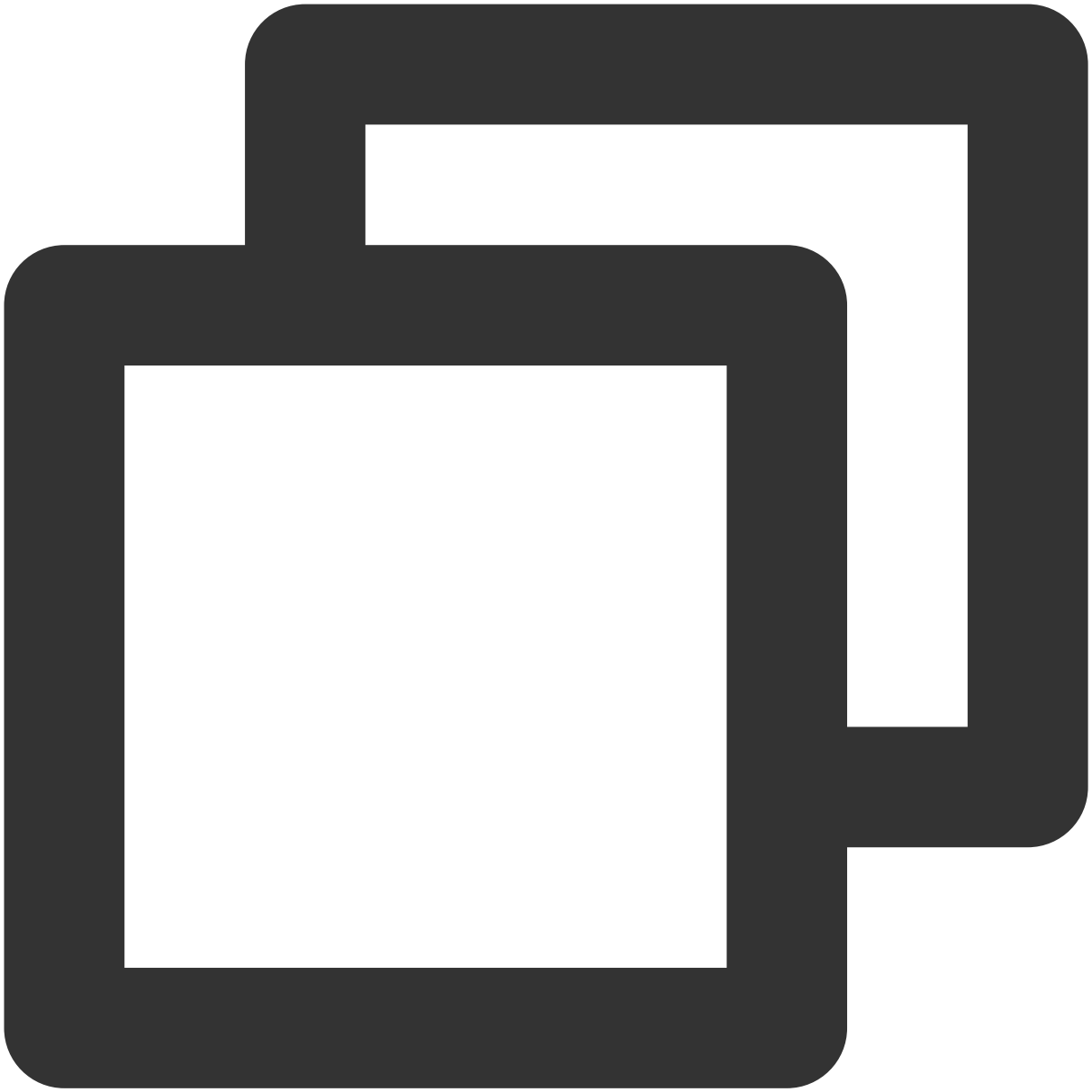
```
dnf install -y docker-ce --nobest
```

5. 次のコマンドを実行して、Dockerを実行します。



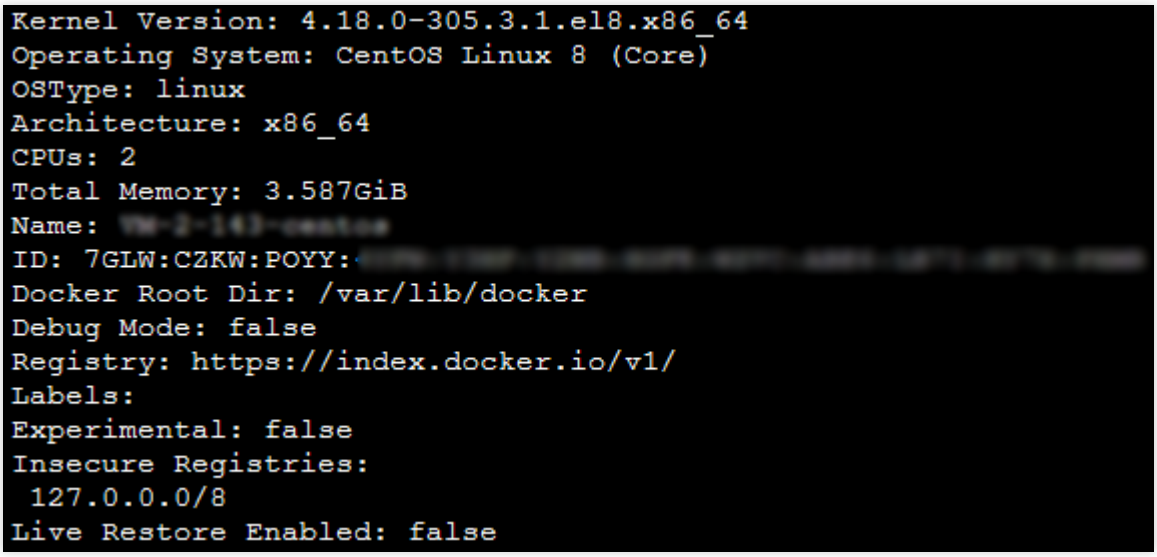
```
systemctl start docker
```

6. 次のコマンドを実行して、インストール結果をチェックします。



```
docker info
```

次のような情報が返されれば、インストールが完了しています。

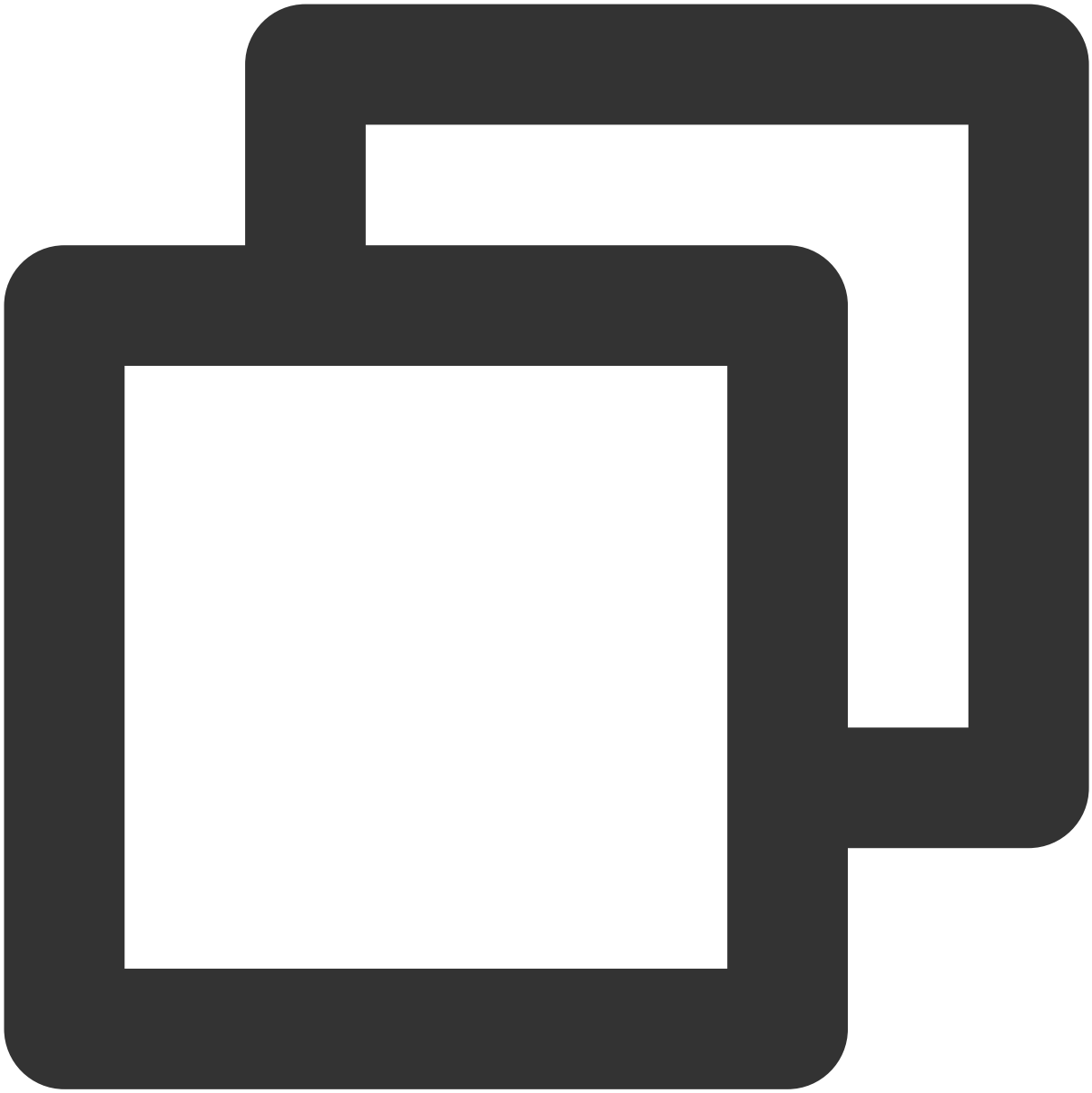


Dockerの使用

Dockerを使用するための基本的なコマンドは次のとおりです：

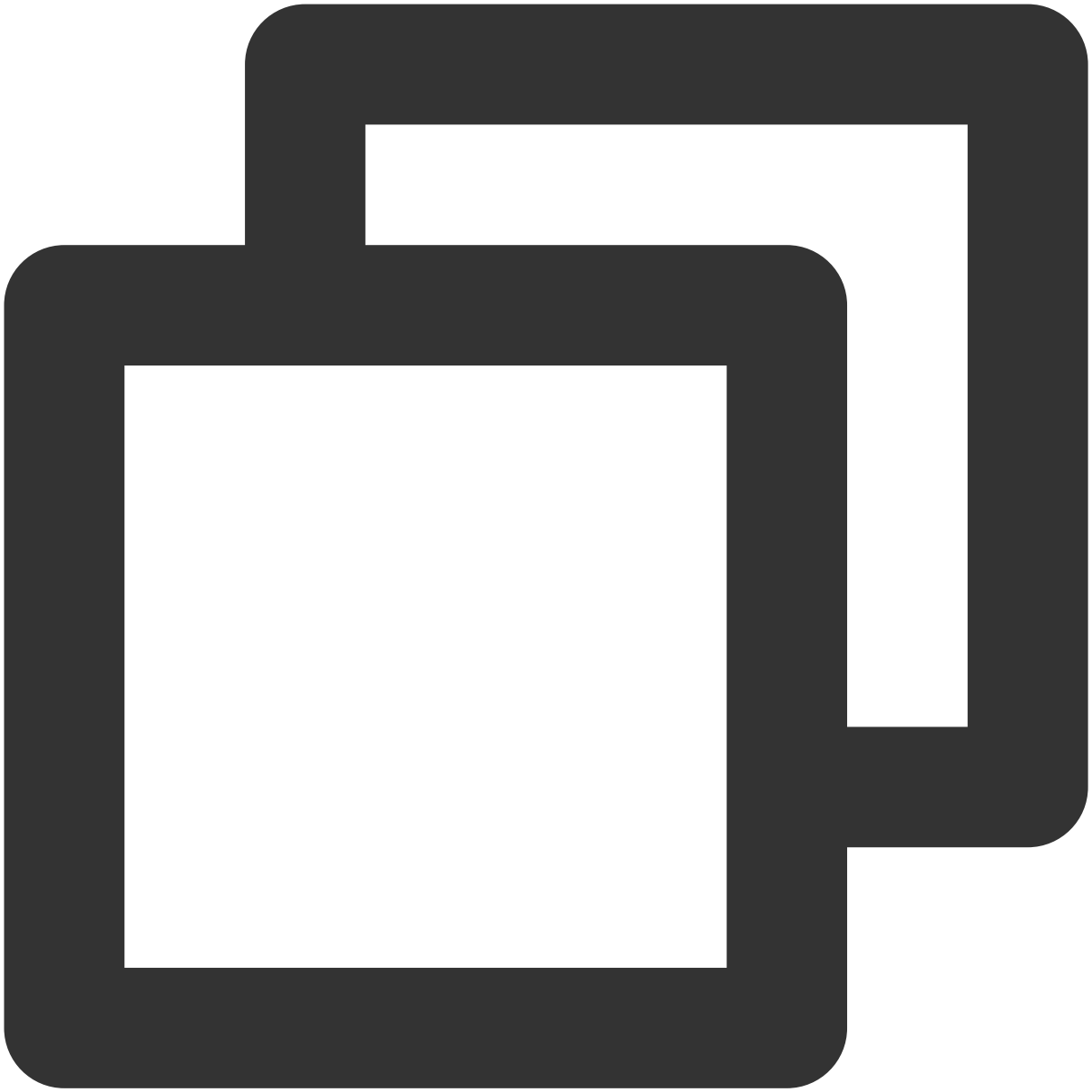
Dockerデーモンを管理します。

Dockerデーモンを実行します：



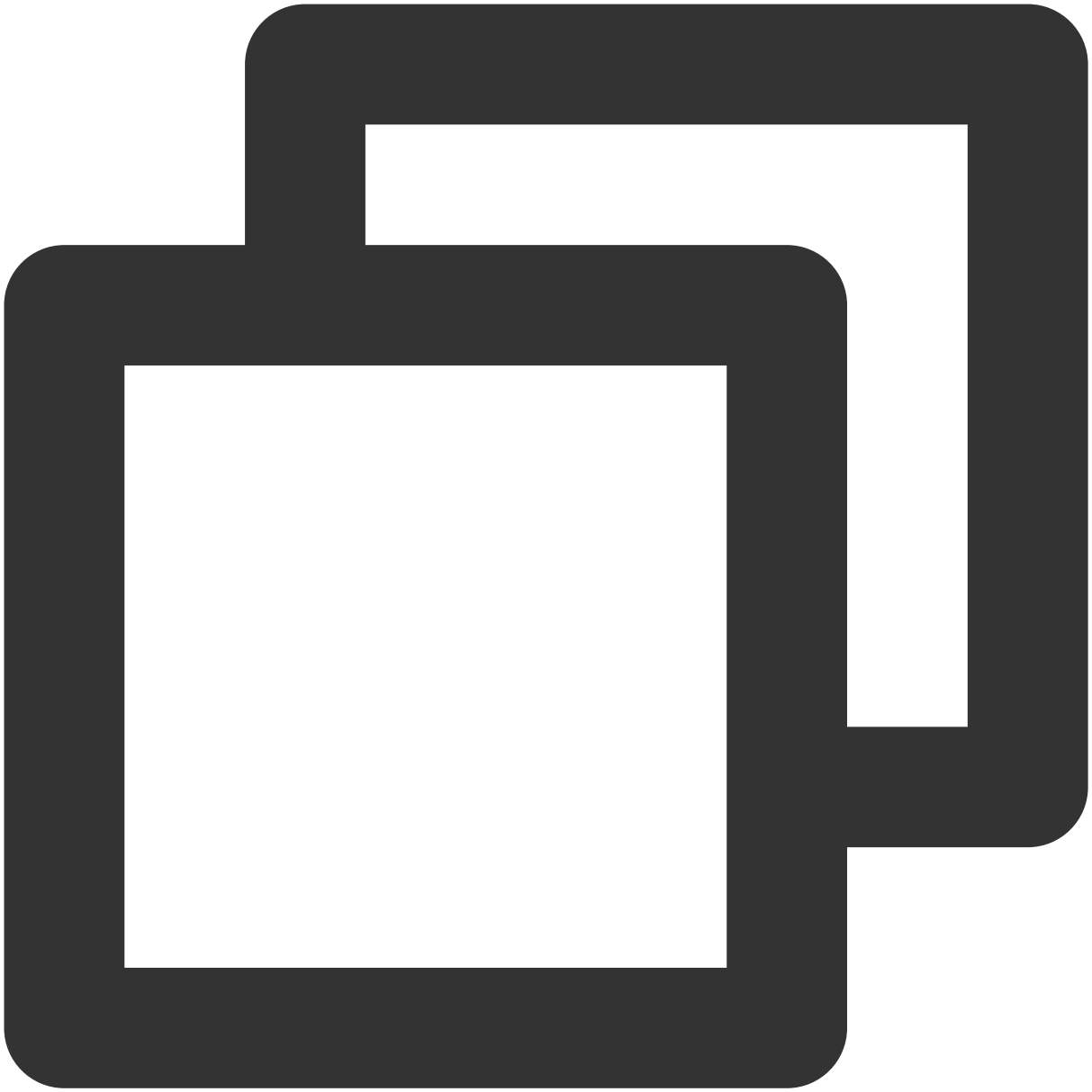
```
systemctl start docker
```

Dockerデーモンを停止します：



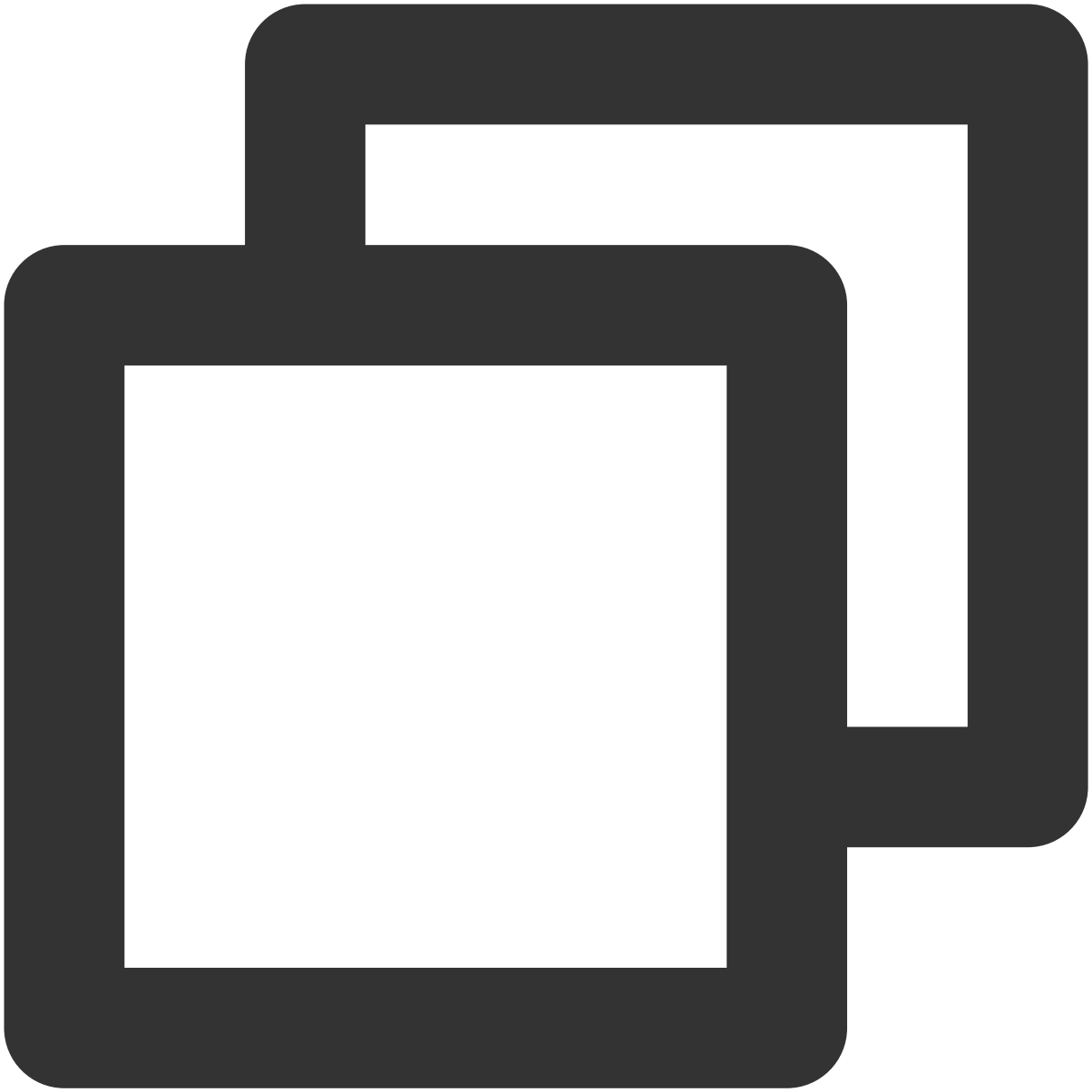
```
systemctl stop docker
```

Dockerデーモンを再起動します：



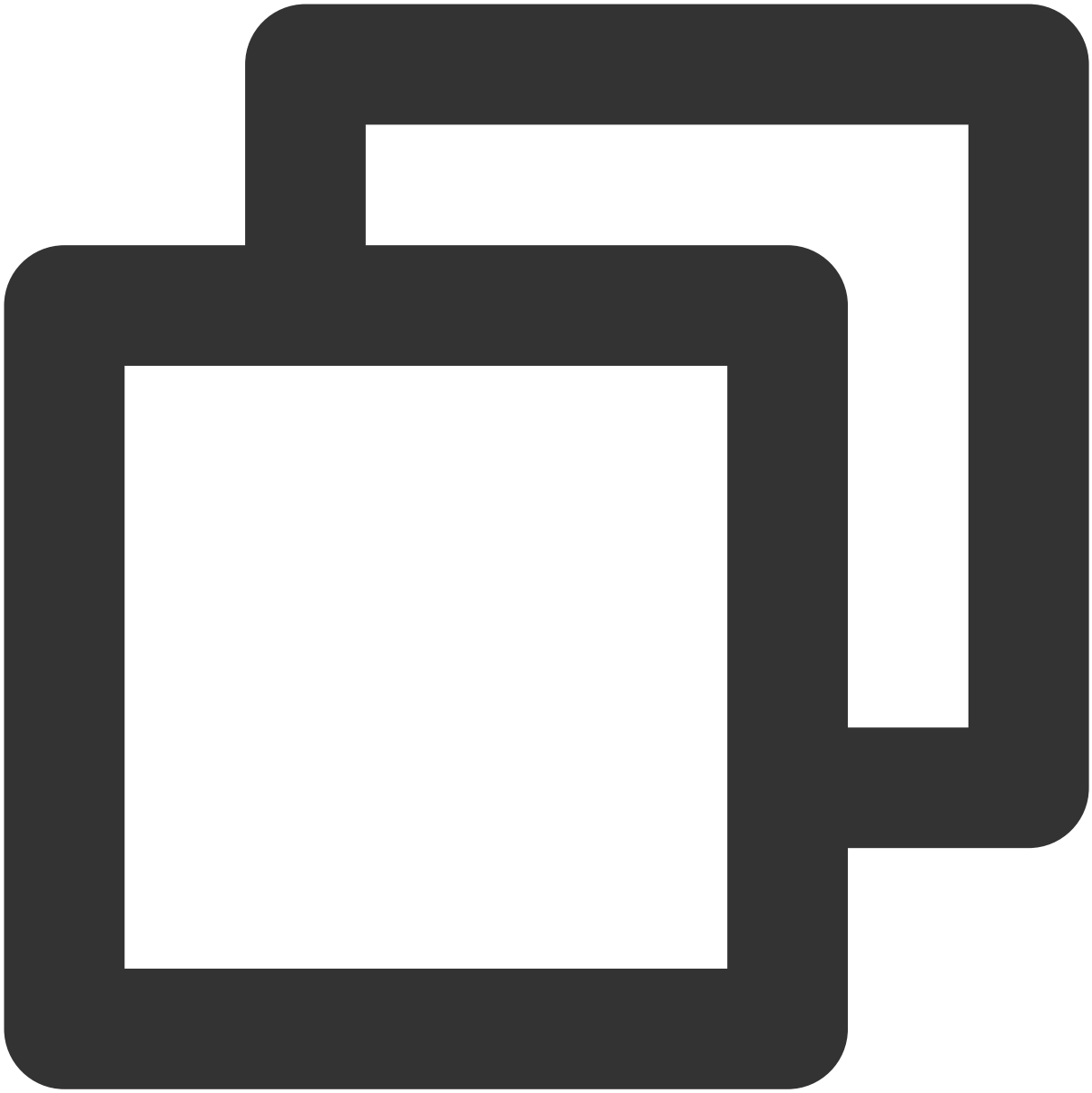
```
systemctl restart docker
```

イメージを管理します。ここではDocker HubのNginxイメージを例として取り上げます。



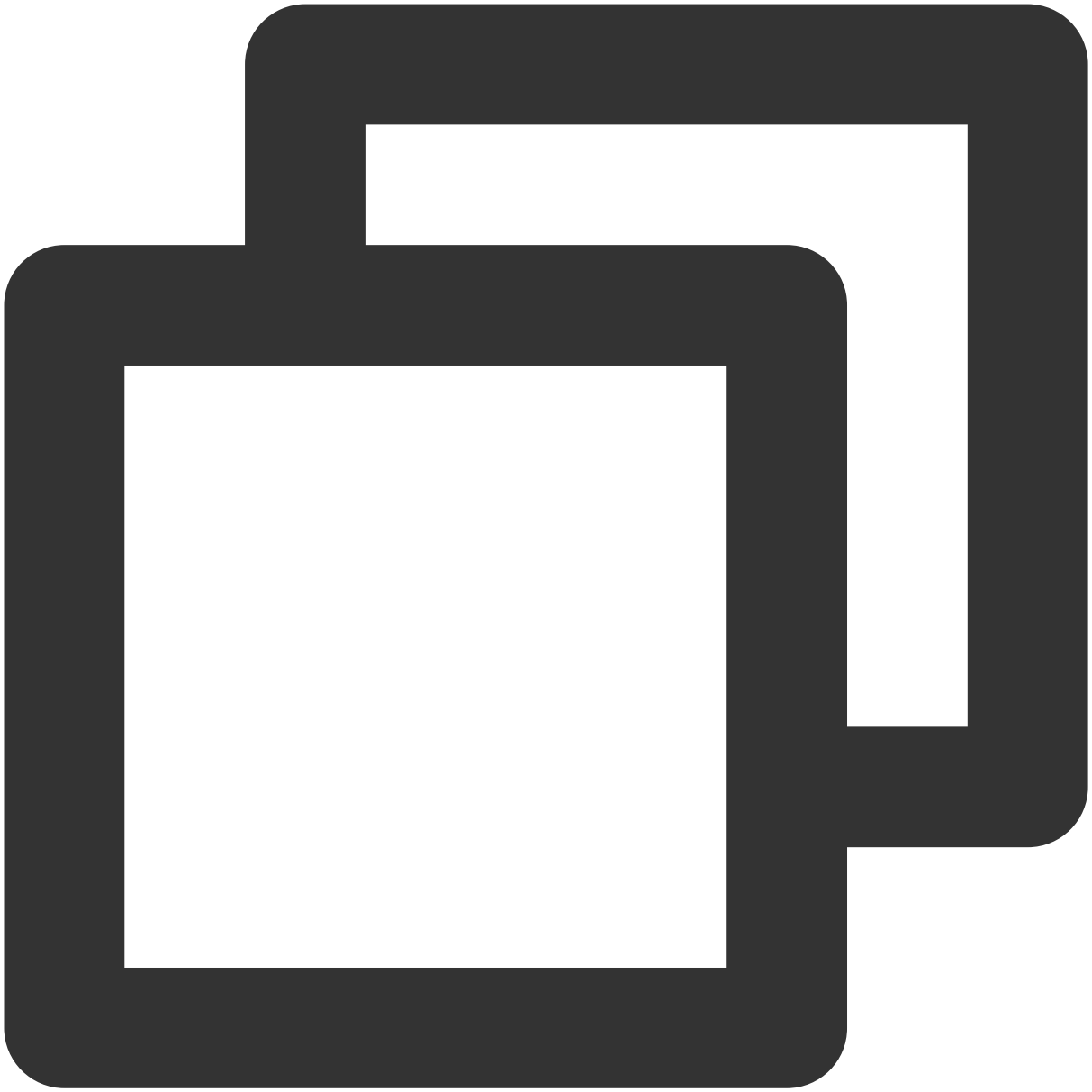
```
docker pull nginx
```

タグの変更：イメージタグを変更して、違いを記憶させることができます。



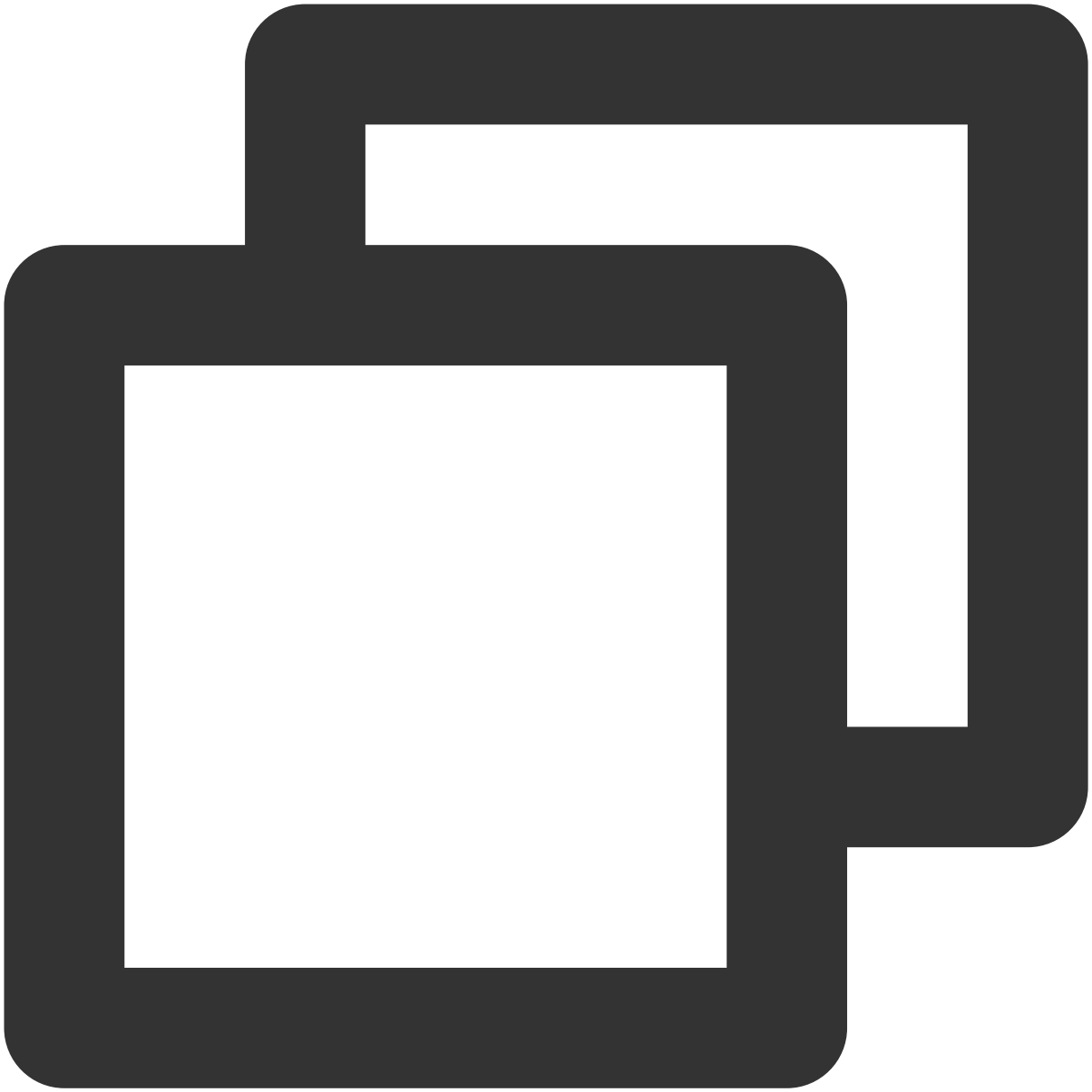
```
docker tag docker.io/nginx:latest tencentyun/nginx:v1
```

既存イメージを確認します：



```
docker images
```

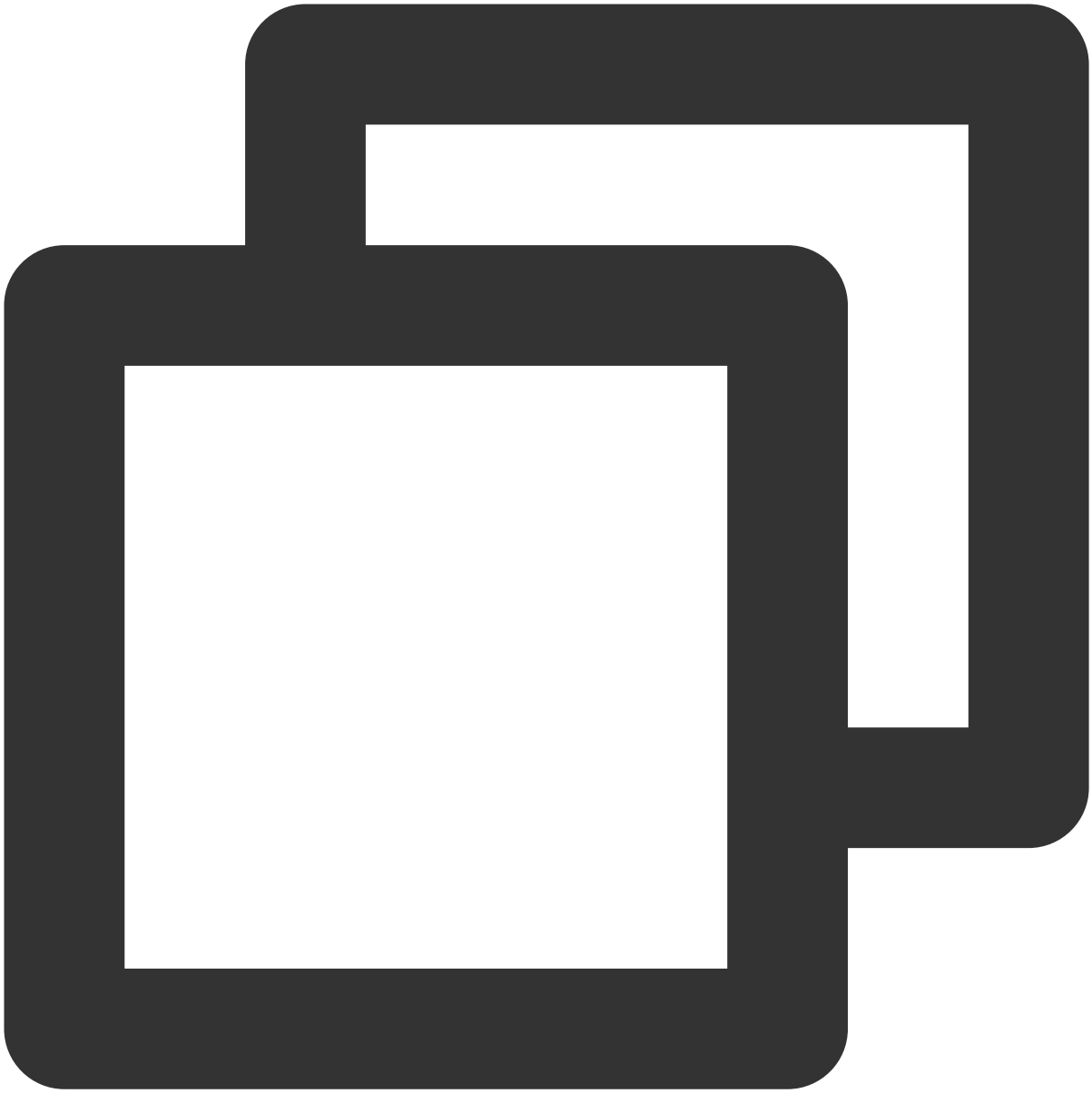
イメージを強制的に削除します：



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

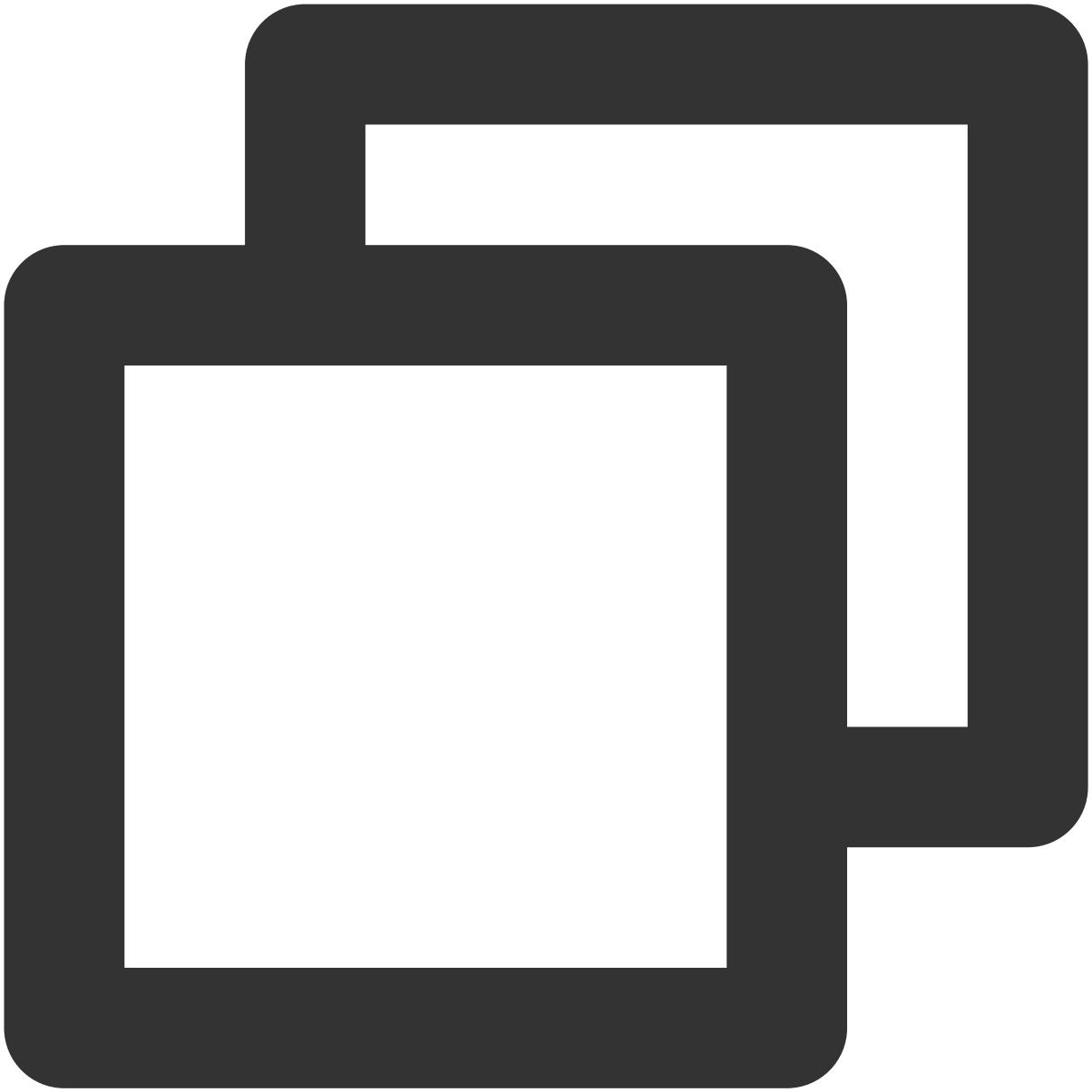
コンテナを管理します。

コンテナにログインします：



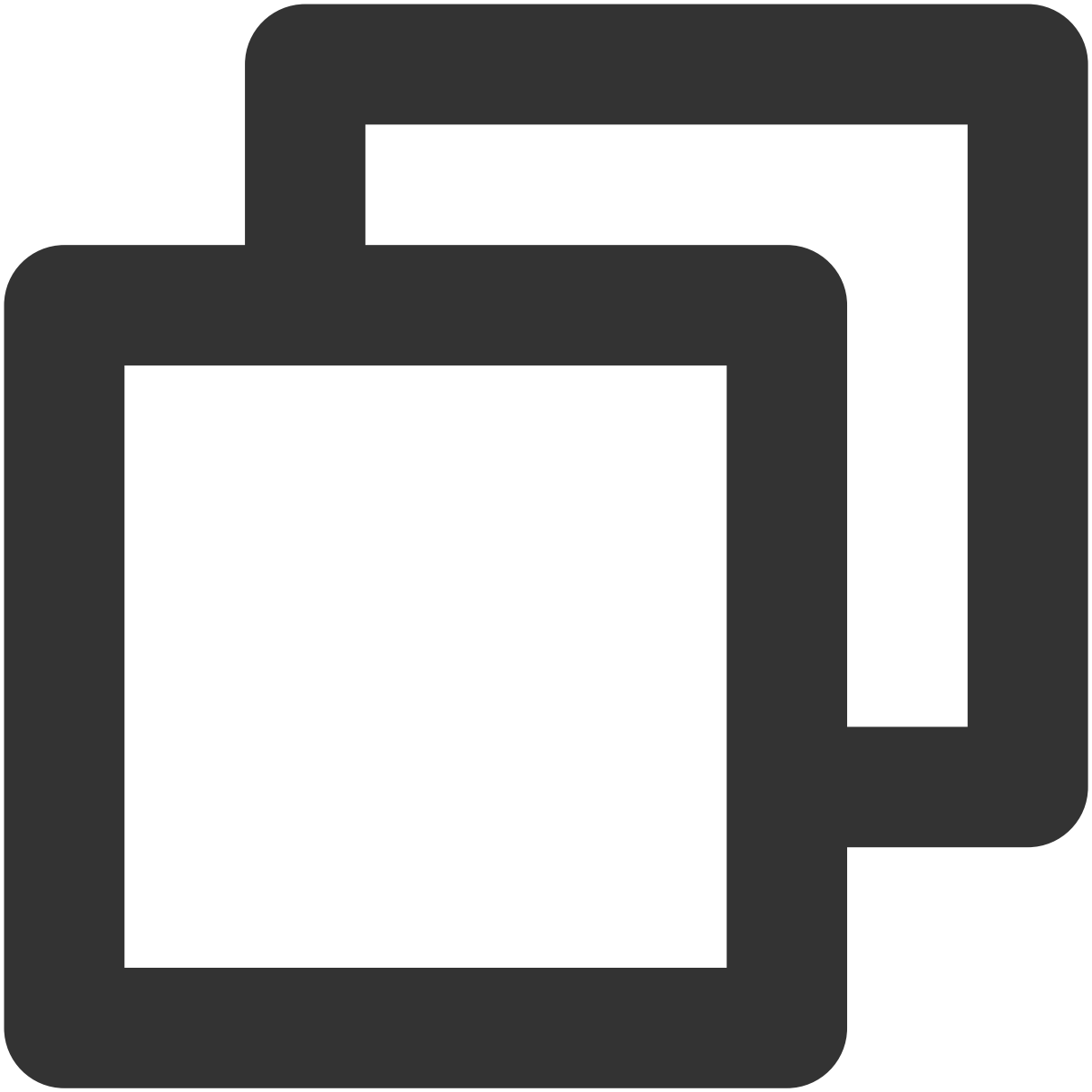
```
docker run -it ImageId /bin/bash
```

そのうち、 `ImageId` は `docker images` コマンドを実行することで取得できます。
コンテナからのログアウト： `exit` コマンドを実行し、現在のコンテナからログアウトします。
バックグラウンドで実行されているコンテナにログインします：



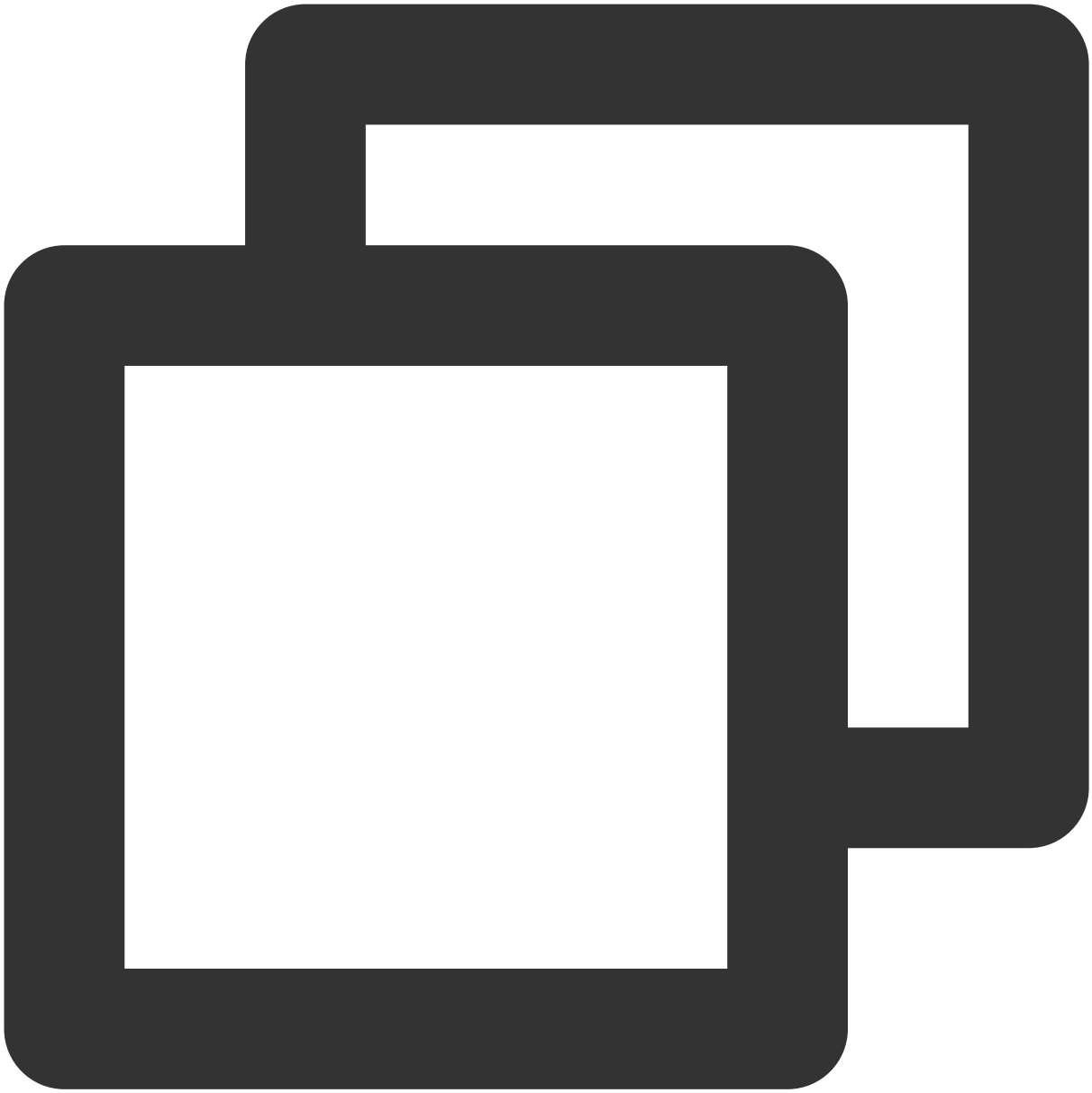
```
docker exec -itコンテナID /bin/bash
```

コンテナをイメージ化します：



```
docker commit <コンテナIDまたはコンテナ名> [<リポジトリ名>[:<タグ>]]
```

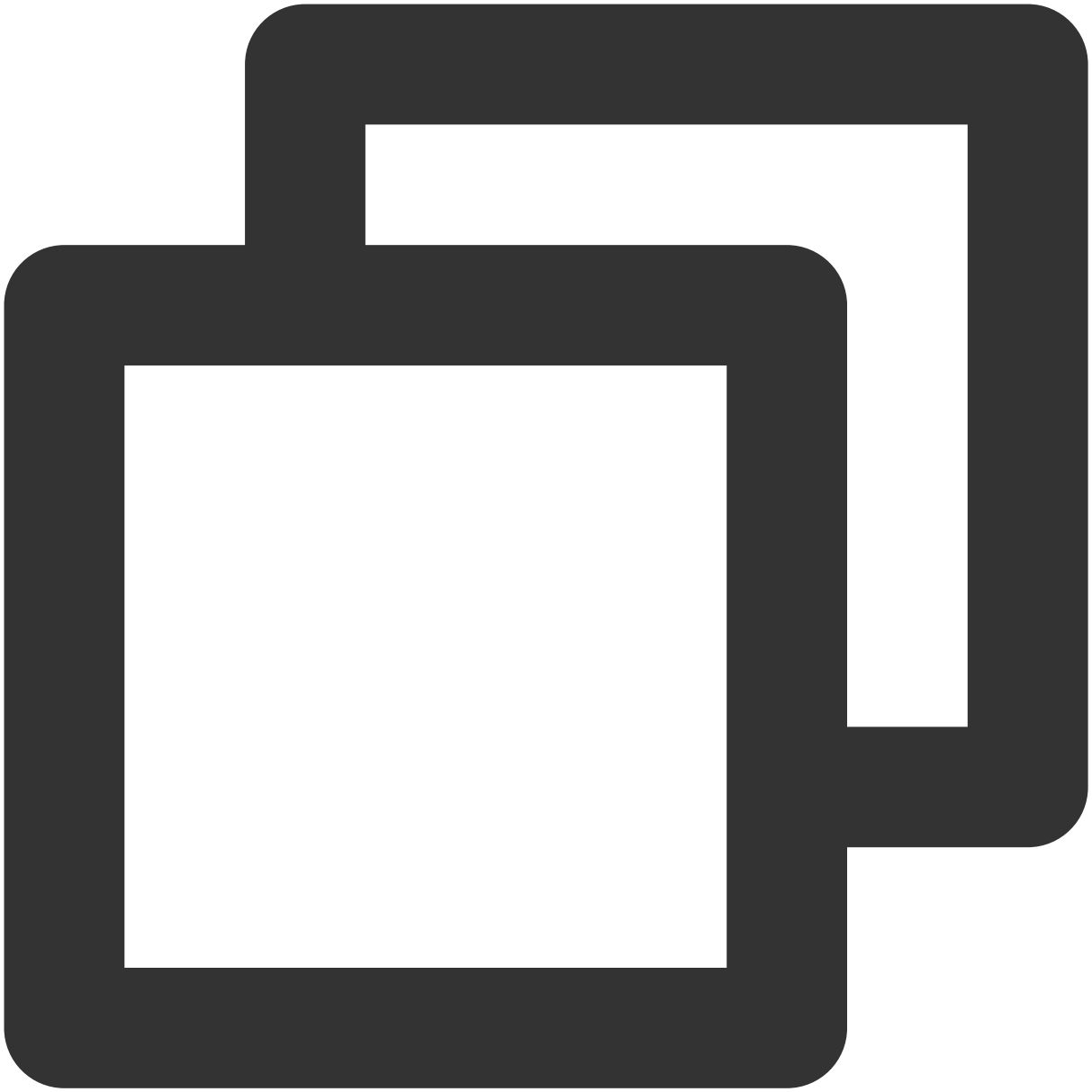
例：



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

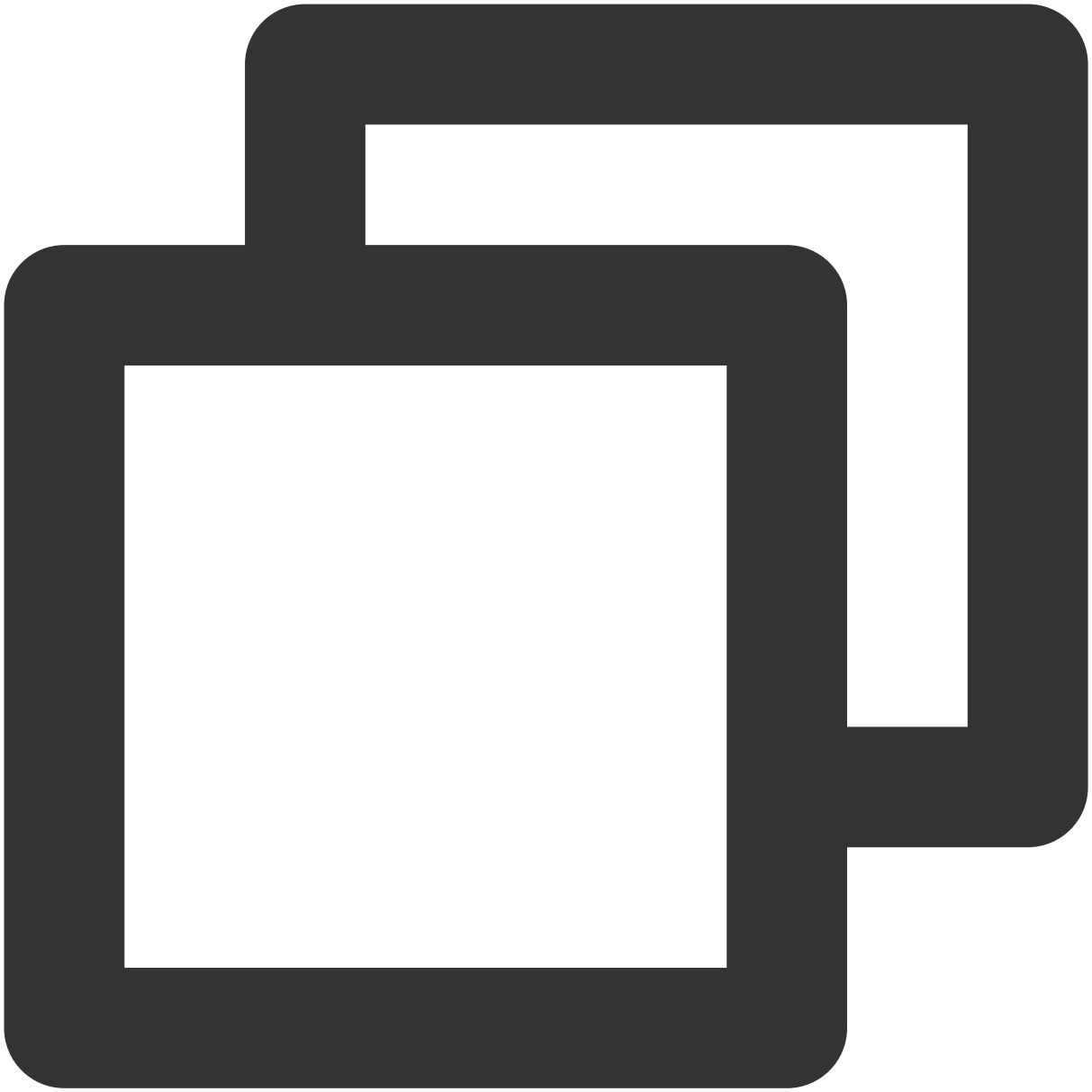
イメージの作成

1. 次のコマンドを実行して、Dockerfileファイルを開きます。



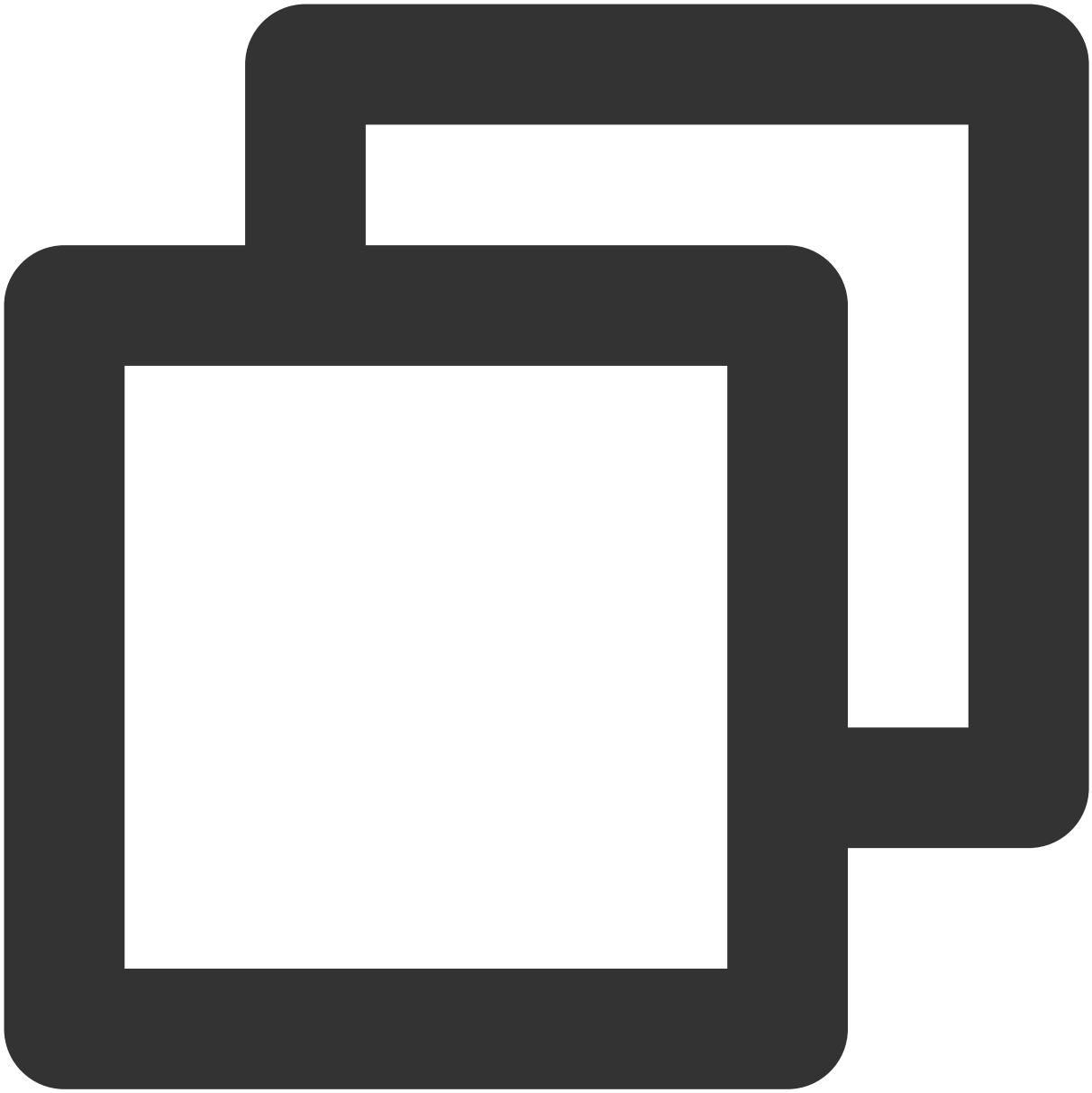
```
vim Dockerfile
```

2. **i**を押して編集モードに切り替え、次の内容を追加します。



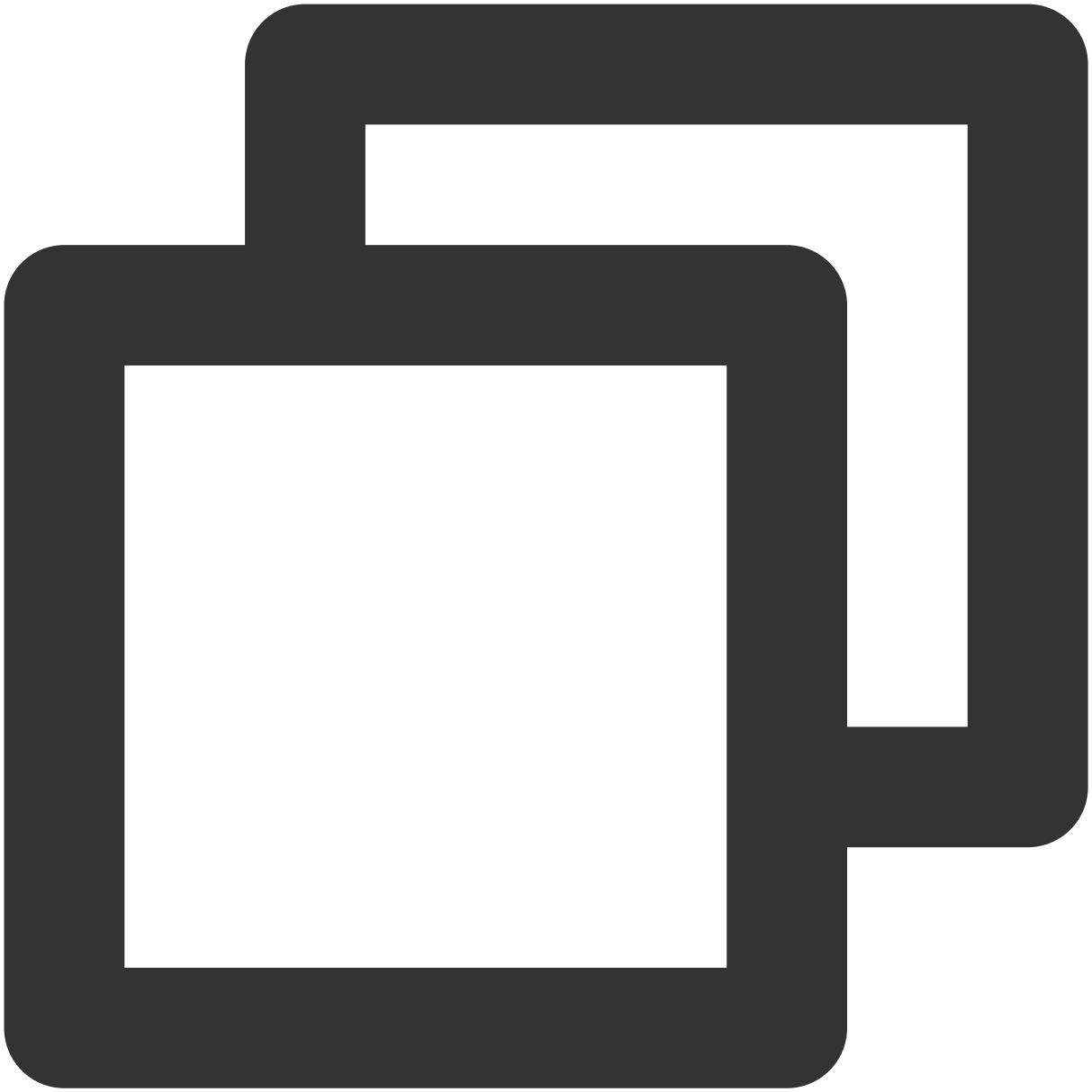
```
FROM tencentyun/nginx:v2  #ベースイメージのソースを宣言します。
MAINTAINER DTSTACK #イメージの所有者を宣言します。
RUN mkdir /dtstact # RUNの後ろには、コンテナを実行する前に実行する必要のあるコマンドが続きます。
ENTRYPOINT ping https://cloud.tencent.com/ #ブートコマンドです。ここでの最後のコマンドは、
```

3. **Esc**を押し、**:wq**を入力して、ファイルを保存して戻ります。
4. 次のコマンドを実行して、イメージを作成します。



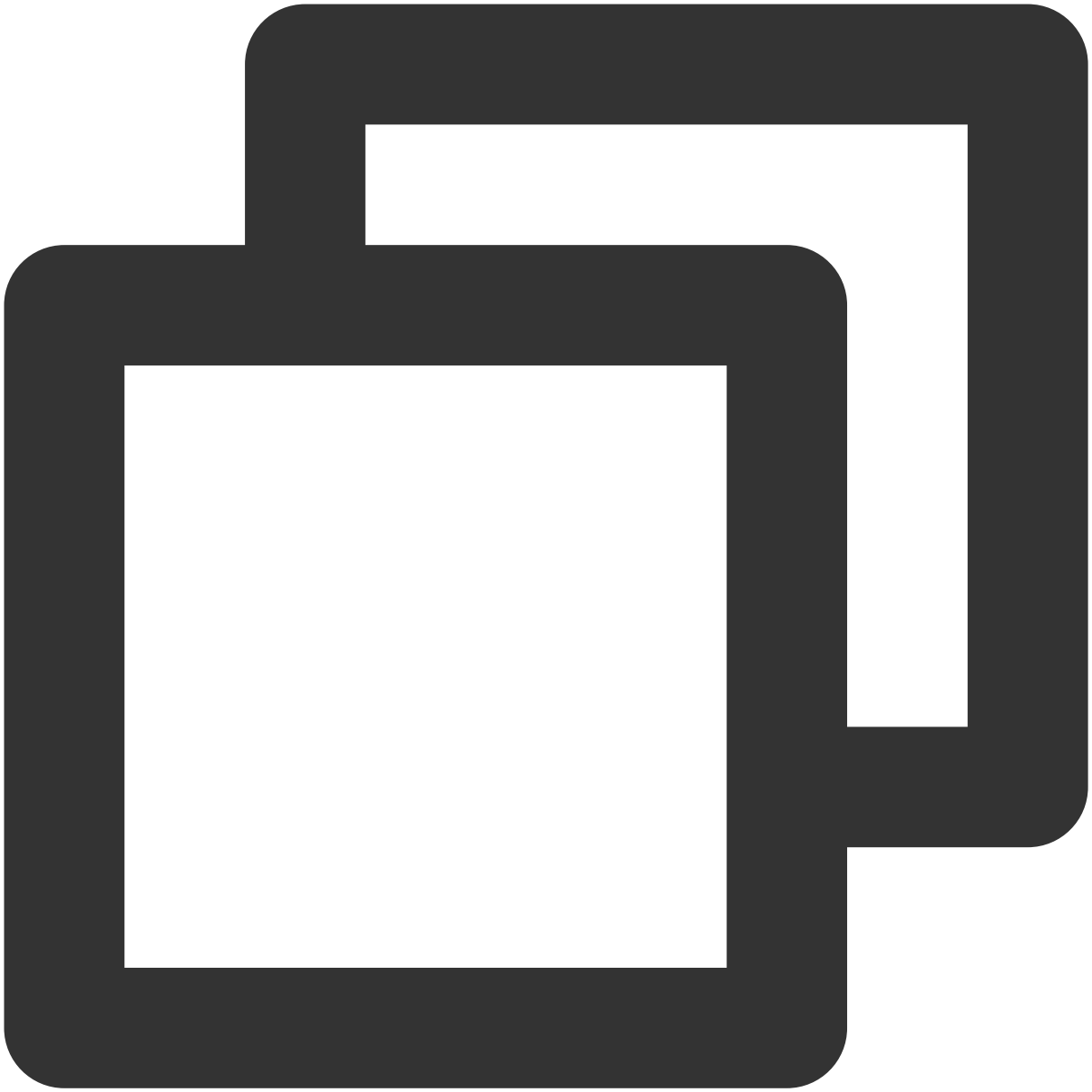
```
docker build -t nginxos:v1 .  #.は、Dockerfileファイルのパスなので、無視することはできませ
```

5. 次のコマンドを実行して、イメージの作成が成功したかどうかを確認します。



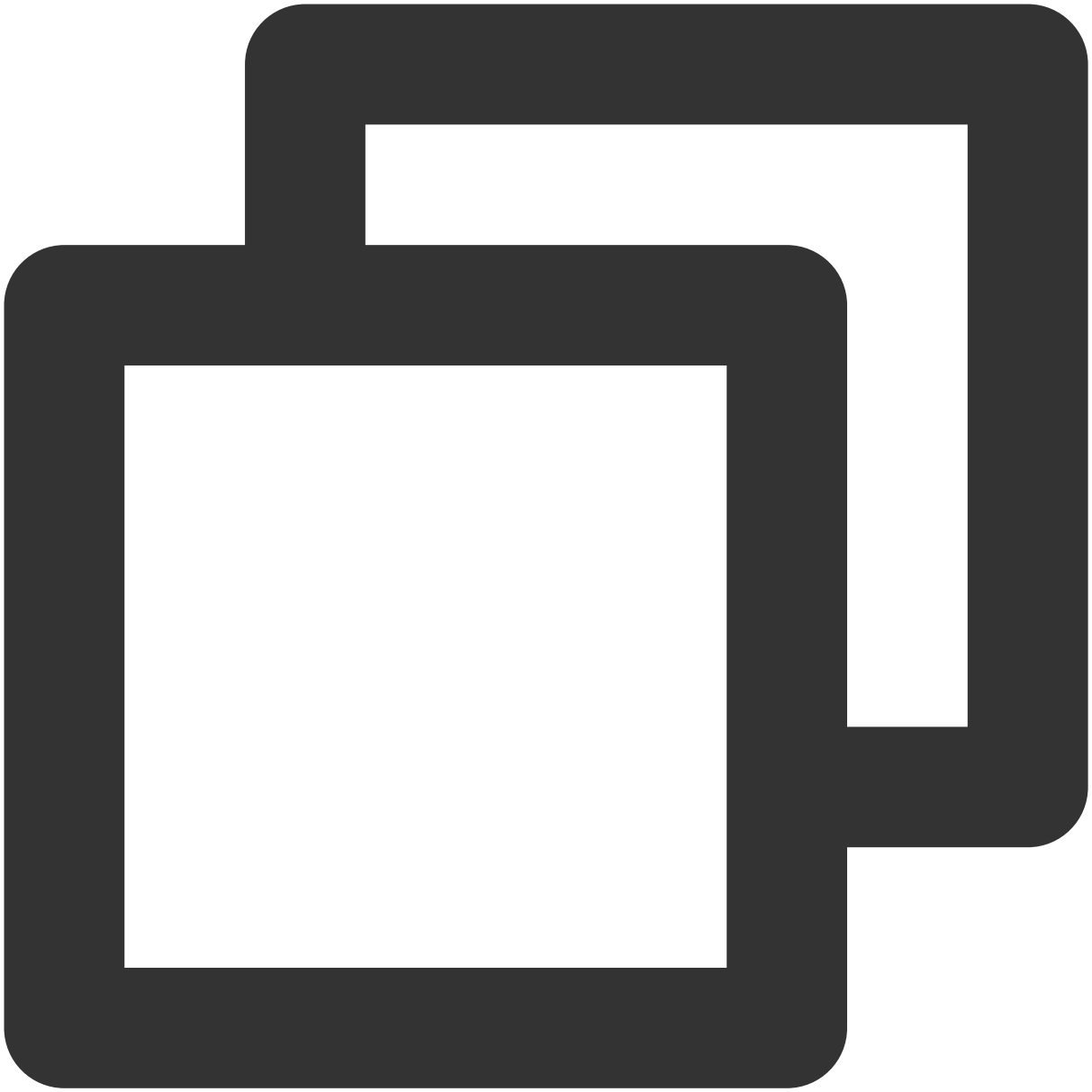
```
docker images
```

6. 次のコマンドを順に実行して、コンテナの実行とコンテナの表示を行います。



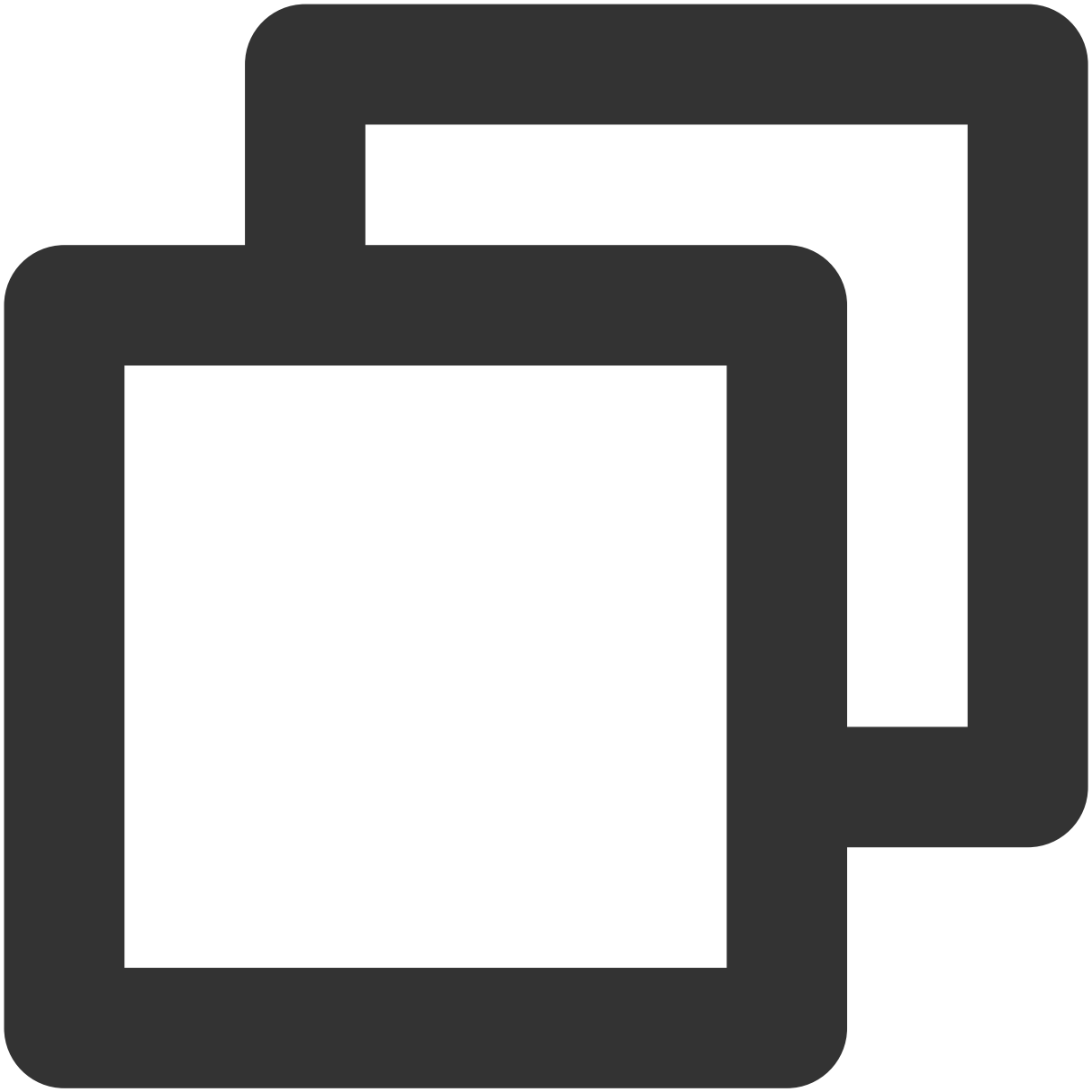
```
docker run -d nginxos:v1          #コンテナをバックグラウンドで実行します。
docker ps                         #現在実行中のコンテナを確認します。
docker ps -a                      #実行されていないコンテナを含むすべてのコンテナを確認します。
docker logs CONTAINER ID/IMAGE    #先ほど実行したコンテナが表示されない場合は、コンテナIDまた
```

7. 次のコマンドを順に実行して、イメージを作成します。



```
docker commit fb2844b6**** nginxweb:v2 #commitパラメータの後に、コンテナID、作成する新しい
docker images                          #ローカル（ダウンロード済みおよびローカルで作成された）イメ
```

8. 次のコマンドを順に実行して、リモートリポジトリにイメージをプッシュします。
デフォルトでDockerHubにプッシュします。まずDockerにログインして、タグをイメージにバインドし、イメージに`Dockerユーザー名/イメージ名:タグの形式で名前を付け、最後にプッシュを完了する必要があります。



```
docker login #実行後、イメージリポジトリのユーザー名とパスワードを入力します
docker tag [イメージ名]:[タグ] [ユーザー名]:[タグ]
docker push [ユーザー名]:[タグ]
```

プッシュが完了したら、ブラウザを使用してDocker Hubの公式ウェブサイトにログインし、確認することができます。

GitLabの構築

最終更新日：：2022-04-11 18:43:06

概要

GitLabは、Rubyで書かれているオープンソースのバージョン管理システムであり、Gitをコード管理ツールとしてセルフホスティングのGitプロジェクトリポジトリを実現し、Webインターフェースを介してパブリックおよびプライベートプロジェクトにアクセスすることができます。このドキュメントでは、Tencent Cloud CVMでGitLabをインストールおよび使用する方法について説明します。

ソフトウェア

このドキュメントに使用するCVMインスタンスは次のように構成する必要があります。
vCPU：2コア
メモリ：4GB
Linux OS ：本節では、CentOS 7.7を例として説明します。

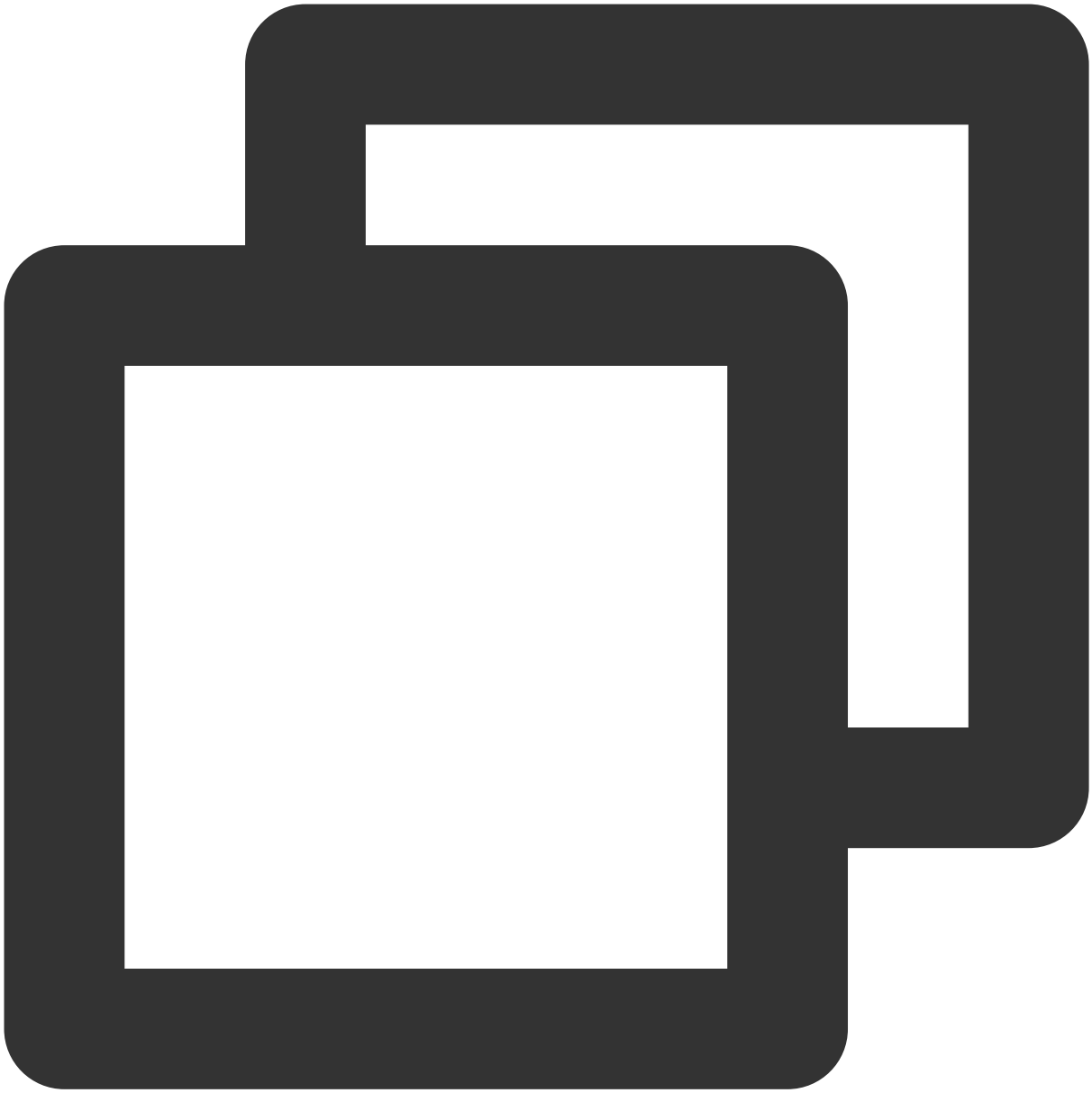
前提条件

GitLabをインストールするにはLinux CVMが必要です。Linux CVMをまだ購入していない場合は、Linux CVM設定のカスタマイズ をご参照ください。
Linuxインスタンスのセキュリティグループルールはすでに設定されています。ポート80を開きます。詳細については、セキュリティグループルールの追加 をご参照ください。

操作手順

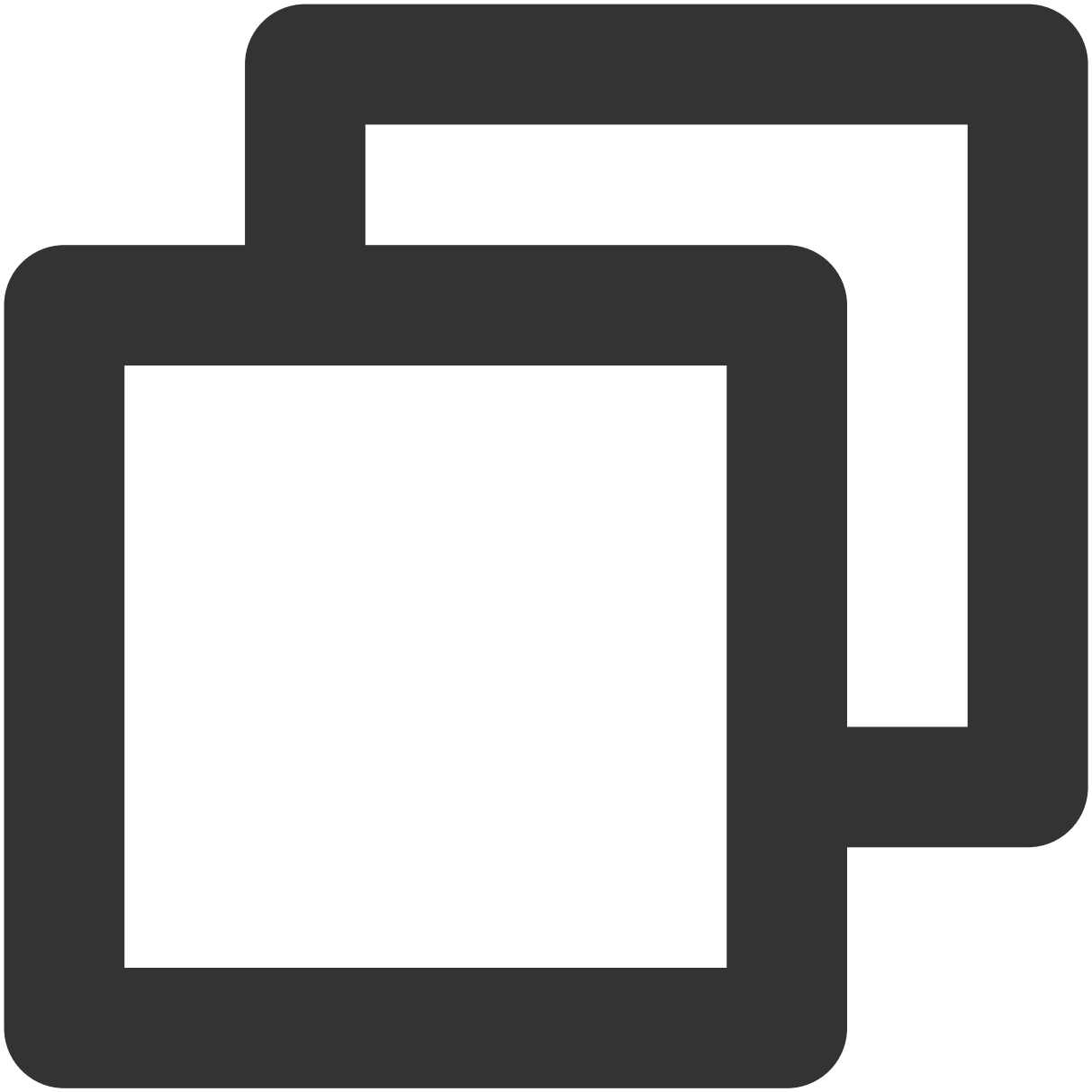
GitLabのインストール

1. 標準方法を使用してLinuxインスタンスにログインします（推奨）。実際の操作方法に応じて、他のログイン方法を選択することもできます。
リモートログインソフトウェアを使用してLinuxインスタンスにログインします
SSHキーを使用してLinuxインスタンスにログインします
2. 以下のコマンドを実行して、依存関係をインストールします。

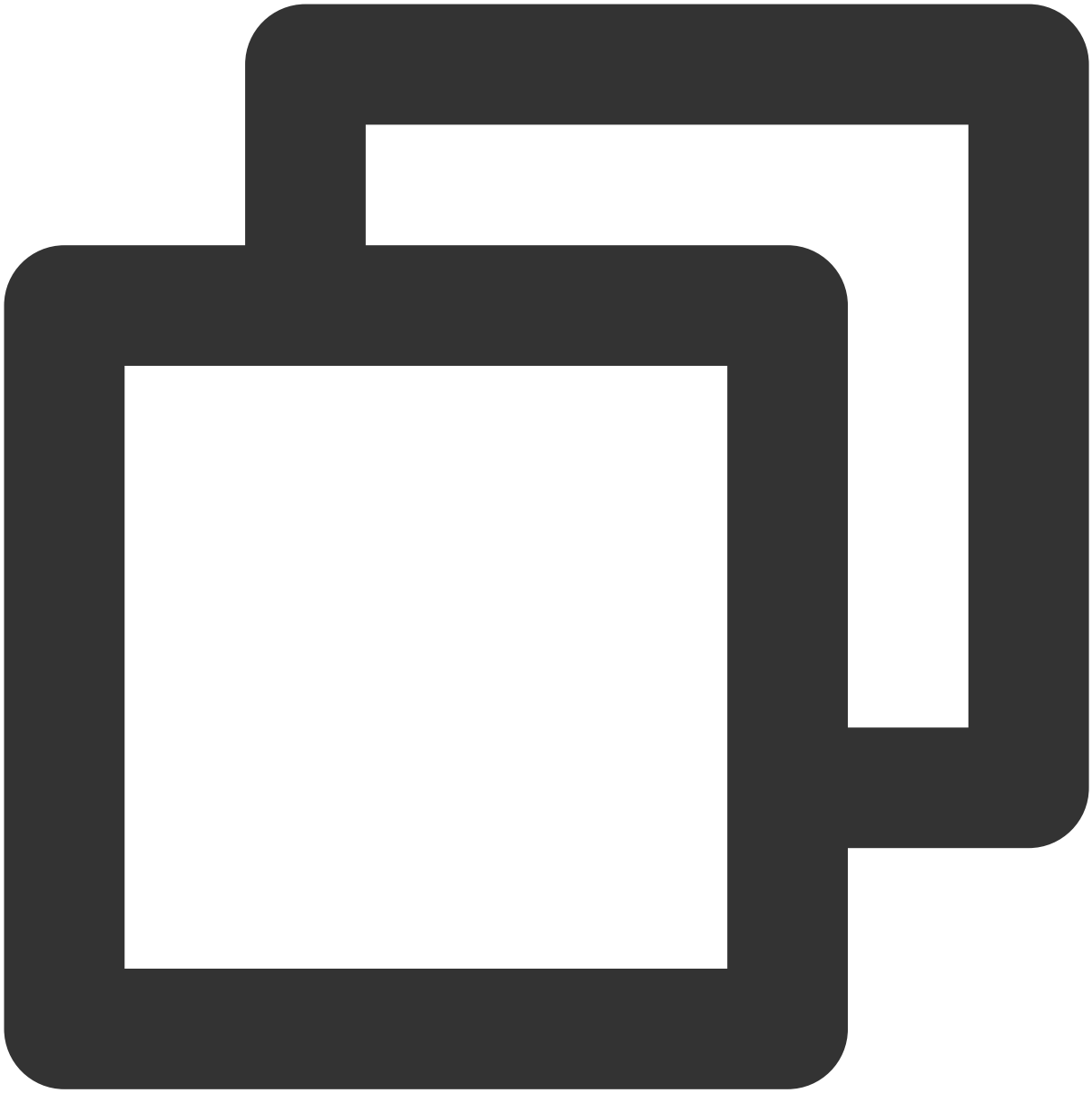


```
yum install -y curl policycoreutils-python openssh-server
```

3. 次のコマンドを順番に実行して、SSHサービスの自動起動を有効にし、SSHサービスを開始します。

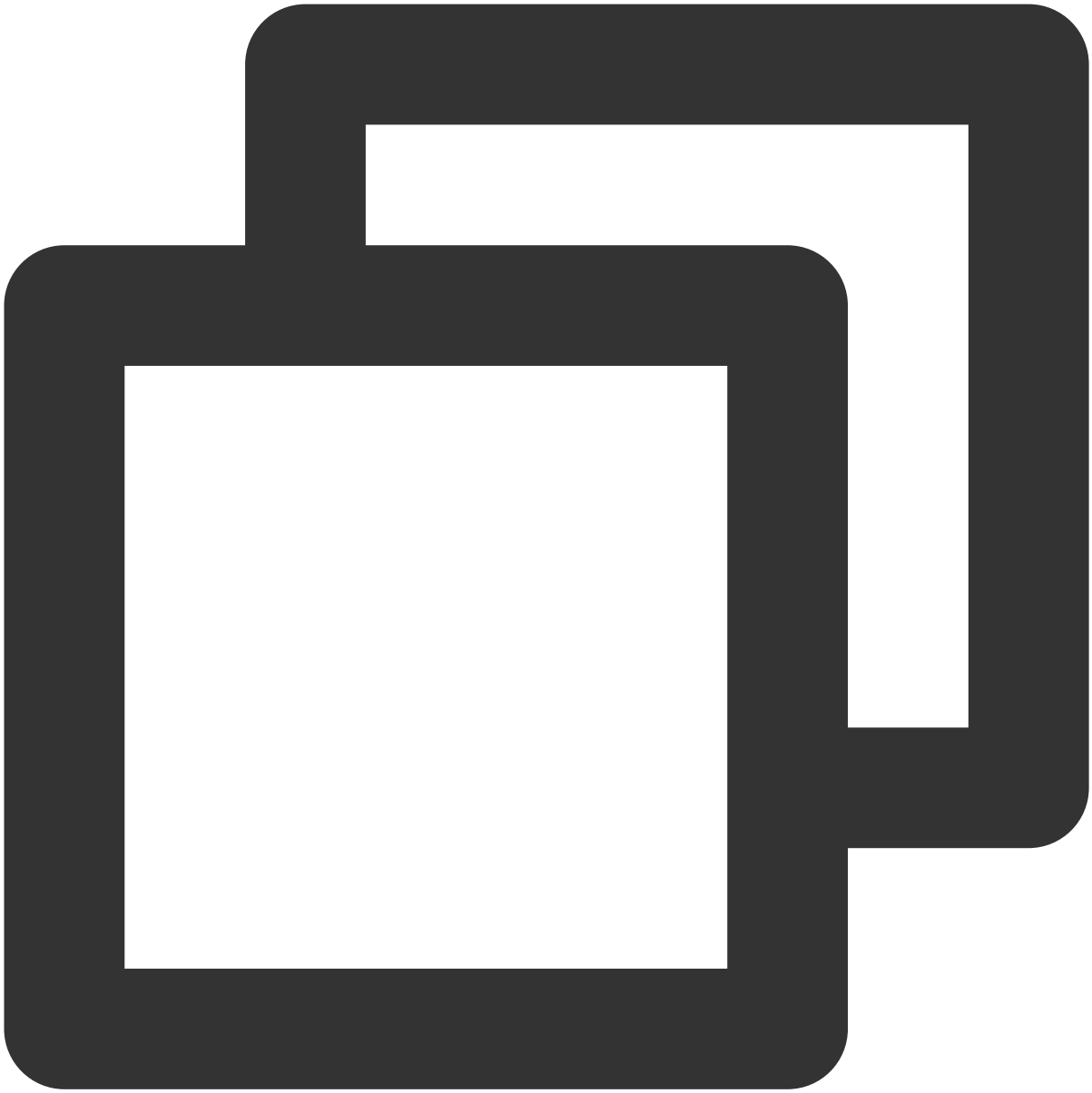


```
systemctl enable sshd
```



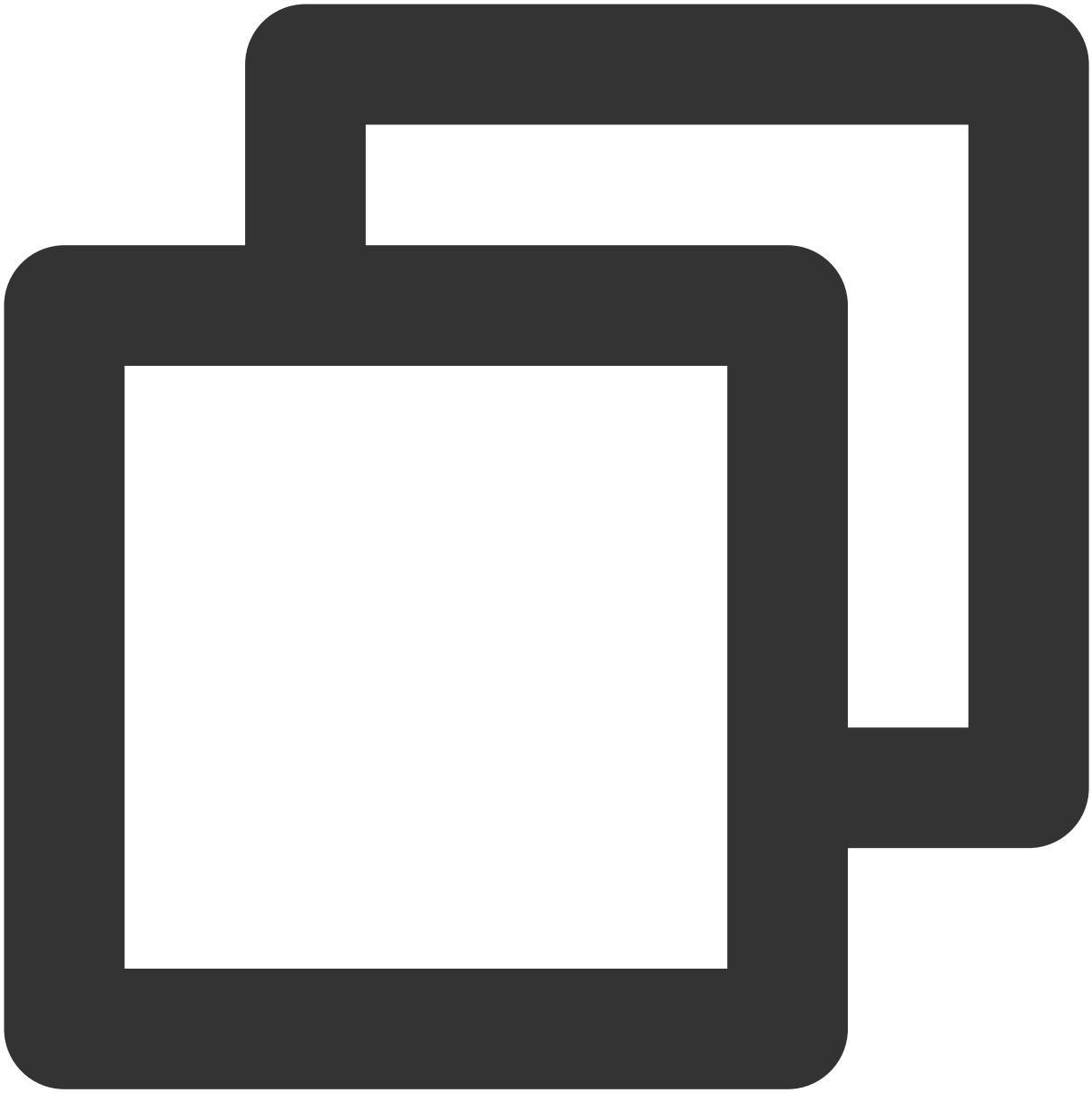
```
systemctl start sshd
```

4. 次のコマンドを実行して、Postfixをインストールします。



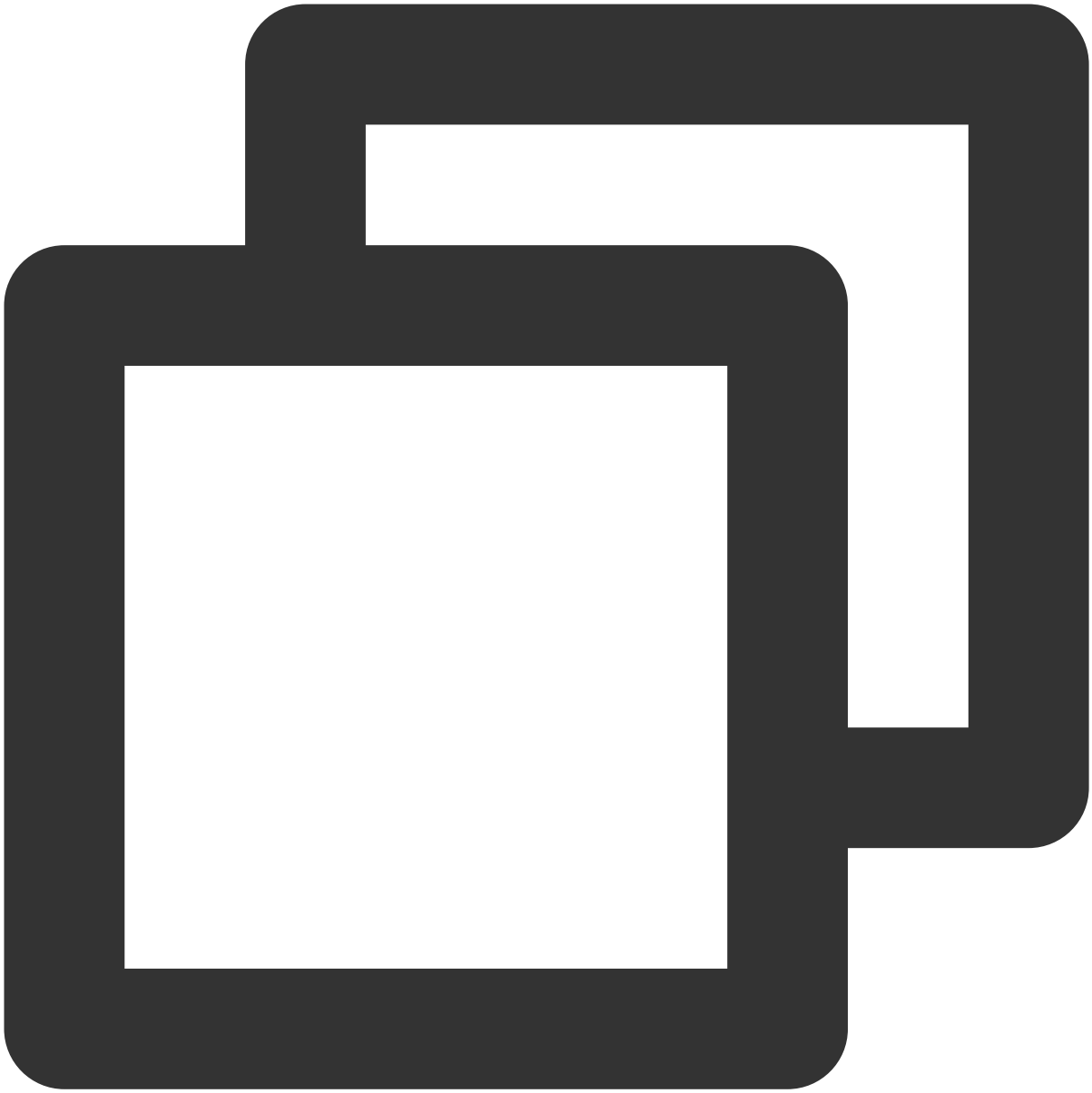
```
yum install -y postfix
```

5. 次のコマンドを実行して、Postfixサービスの自動起動を設定します。



```
systemctl enable postfix
```

6. 次のコマンドを実行して、Postfixの構成ファイルmain.cfを開きます。

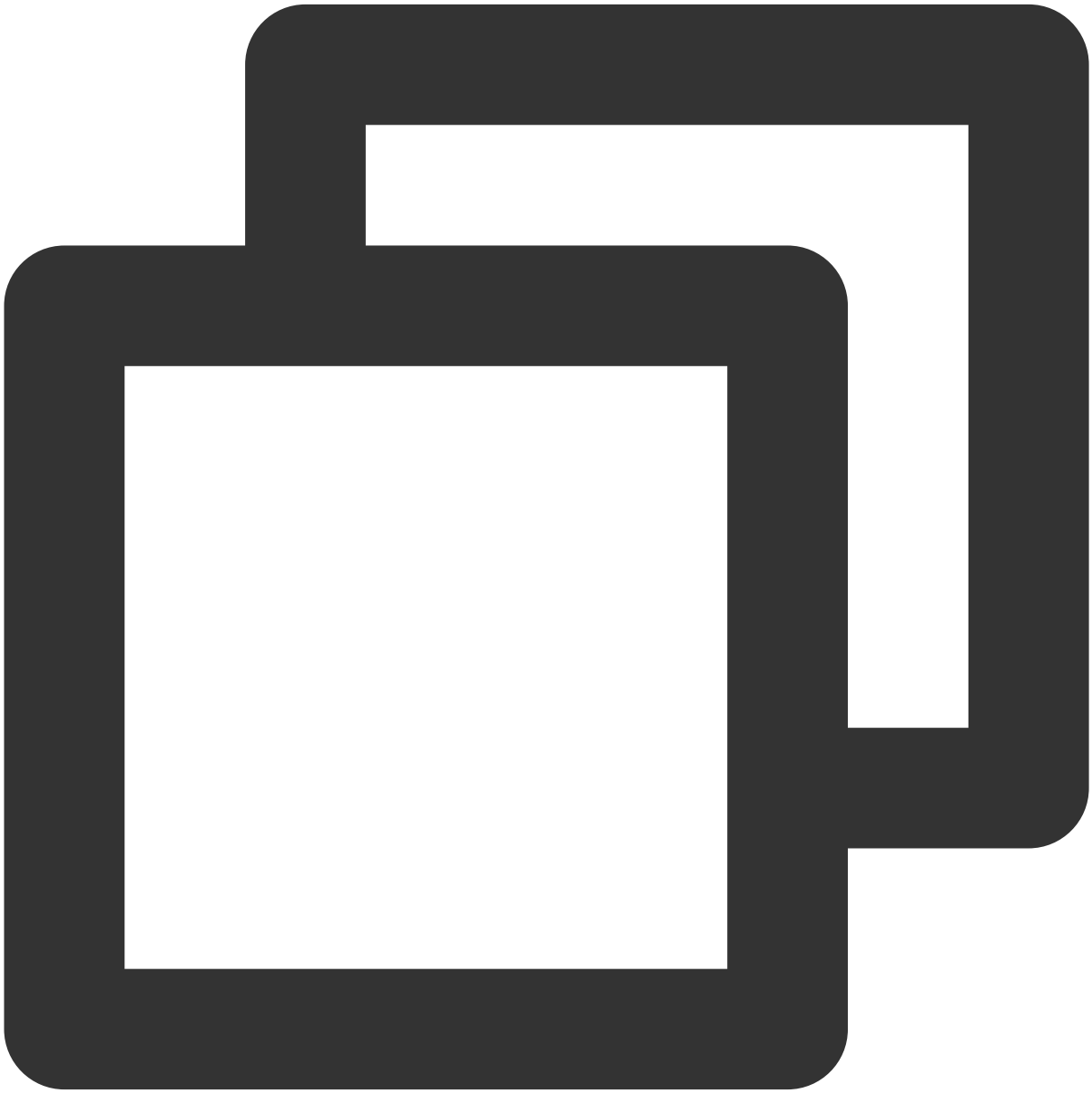


```
vim /etc/postfix/main.cf
```

7. **i**を押して編集モードに入り、`inet_interfaces = all` 前の `#` を削除し、`inet_interfaces = localhost` の前に `#` を追加します。変更した後は以下の通りです。

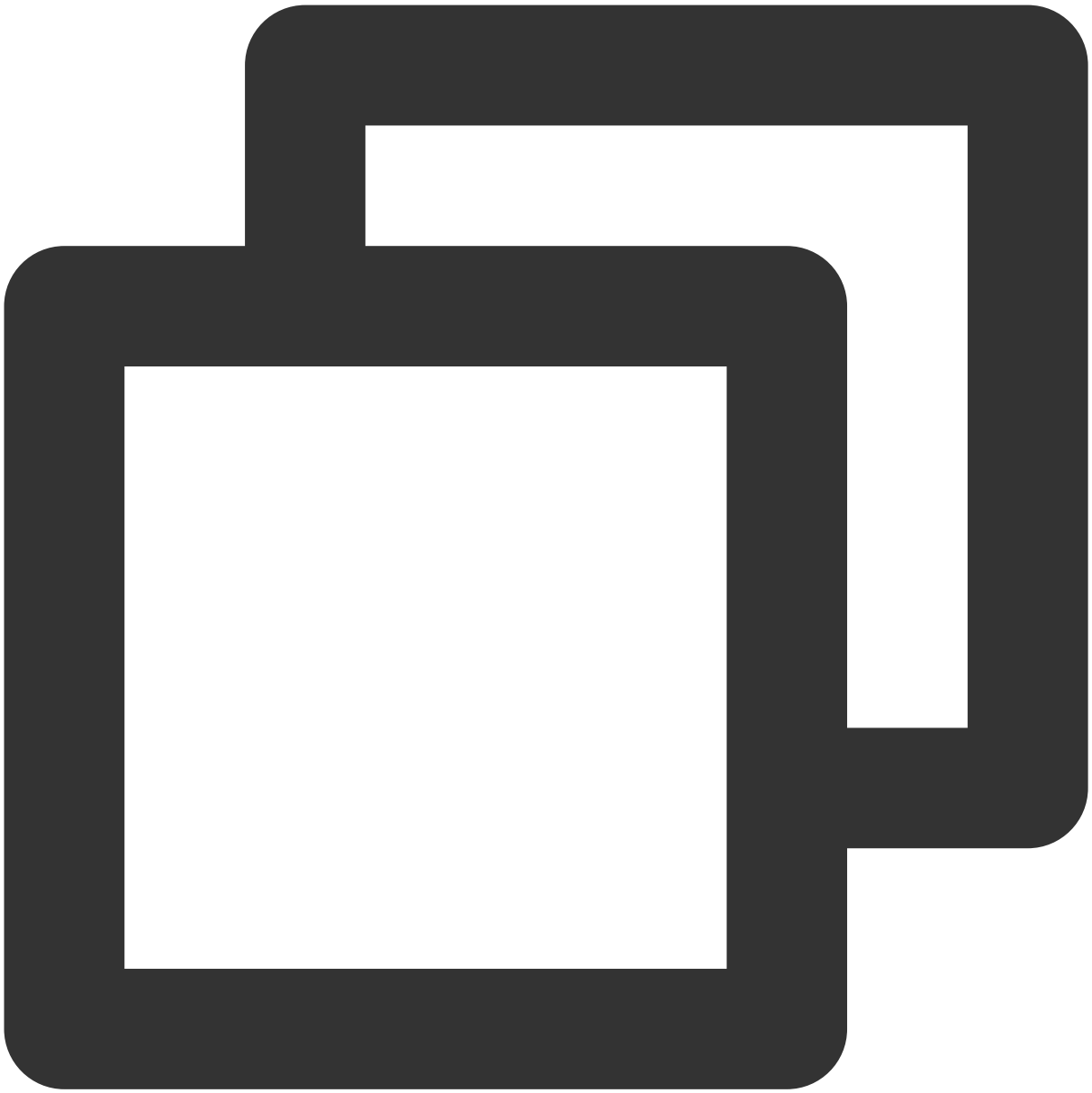
```
inet_interfaces = all
#inet_interfaces = $myhostname
#inet_interfaces = $myhostname, localhost
#inet_interfaces = localhost
```

8. **Esc**キーを押して、**:wq**を入力し、変更を保存してからファイルを終了します。
9. 次のコマンドを実行して、Postfixを起動します。



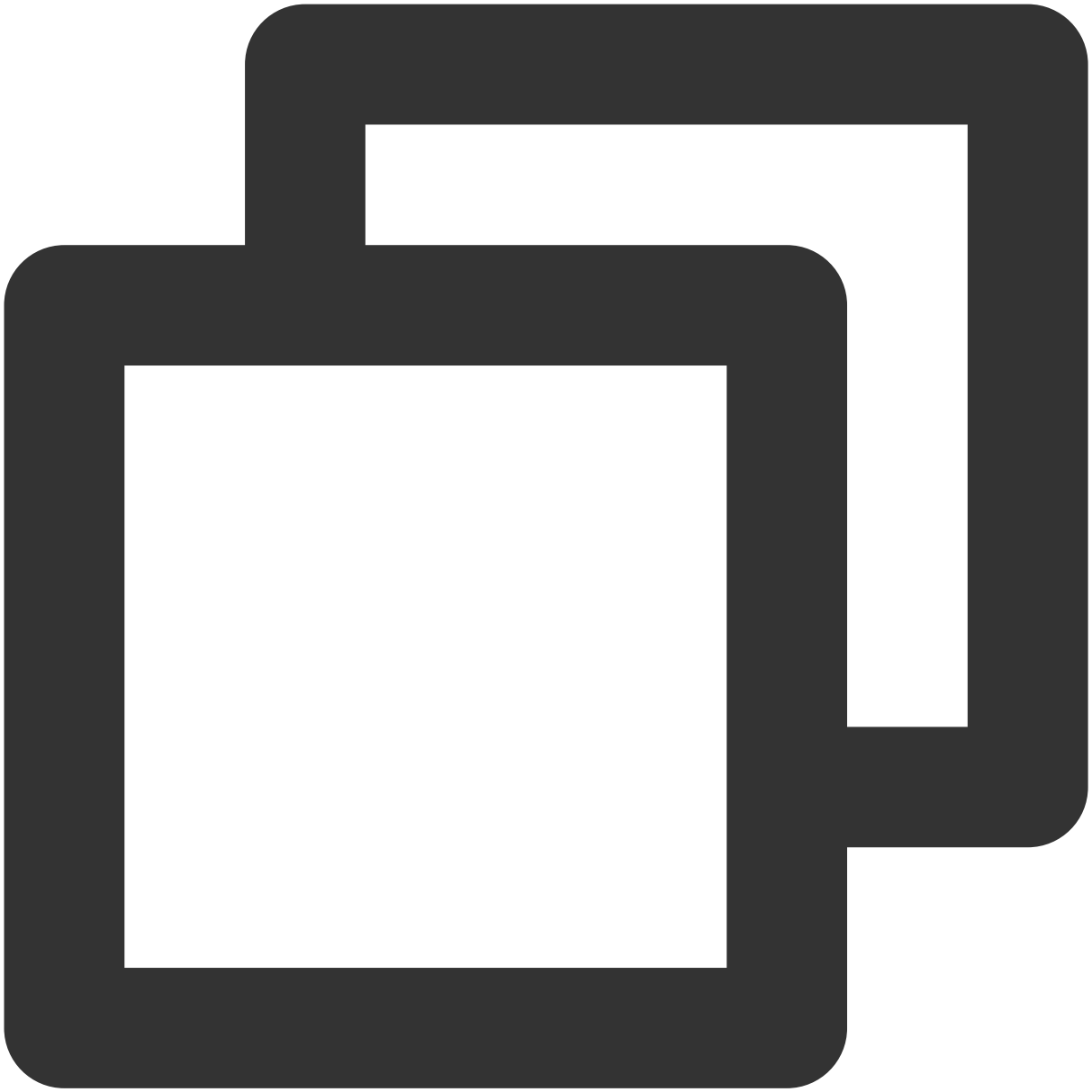
```
systemctl start postfix
```

10. 次のコマンドを実行して、GitLabのソフトウェアリポジトリをインストールします。



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

11. 次のコマンドを実行して、GitLabをインストールします。



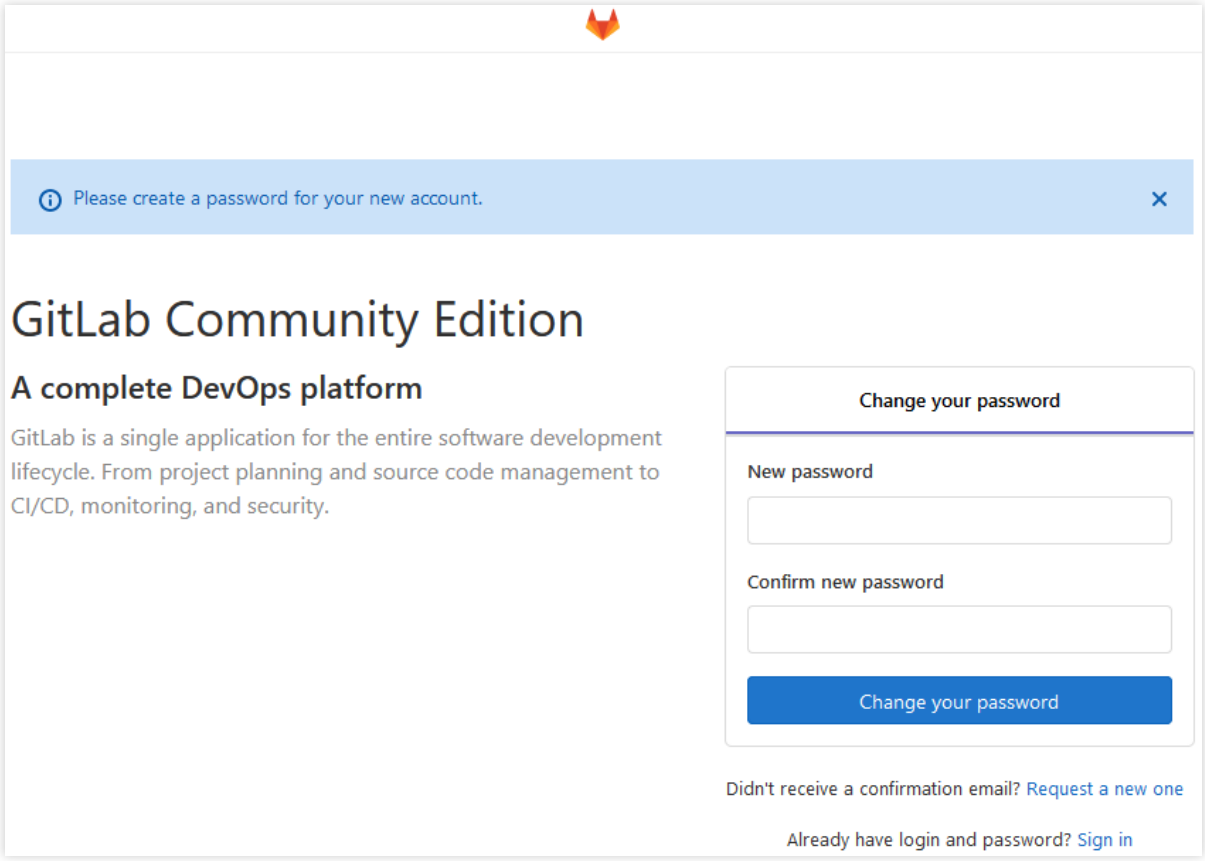
```
sudo EXTERNAL_URL="インスタンスのパブリックIPアドレス" yum install -y gitlab-ce
```

インスタンスのパブリックIPを取得する方法の詳細については、パブリックIPアドレスの取得をご参照ください。

12.ローカルブラウザで、取得したパブリックIPアドレスにアクセスします。以下のようなページが表示されると、GitLabのインストールに成功したことを意味します。

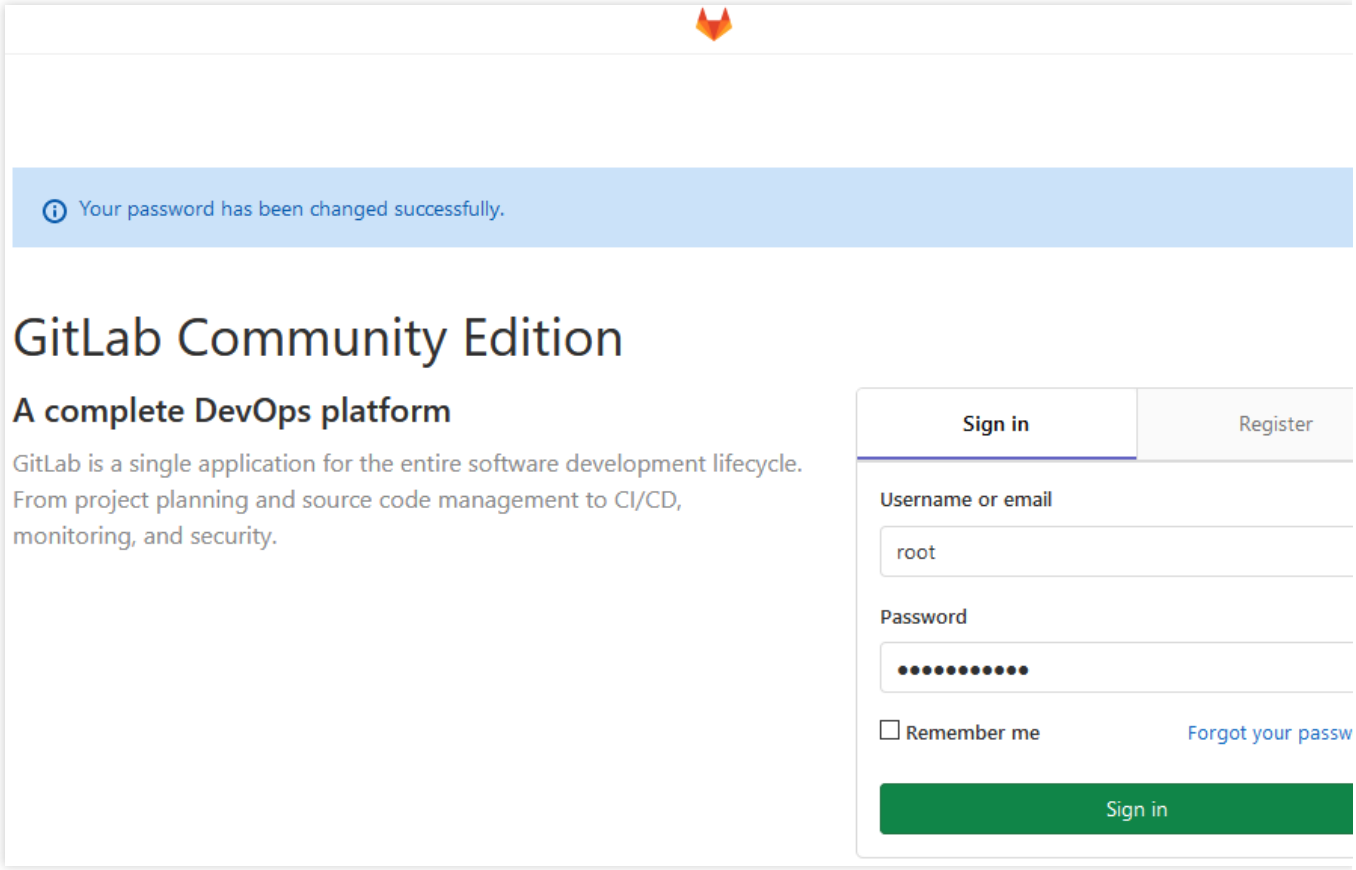
説明：

このページでGitLabアカウントのパスワードを設定してください。

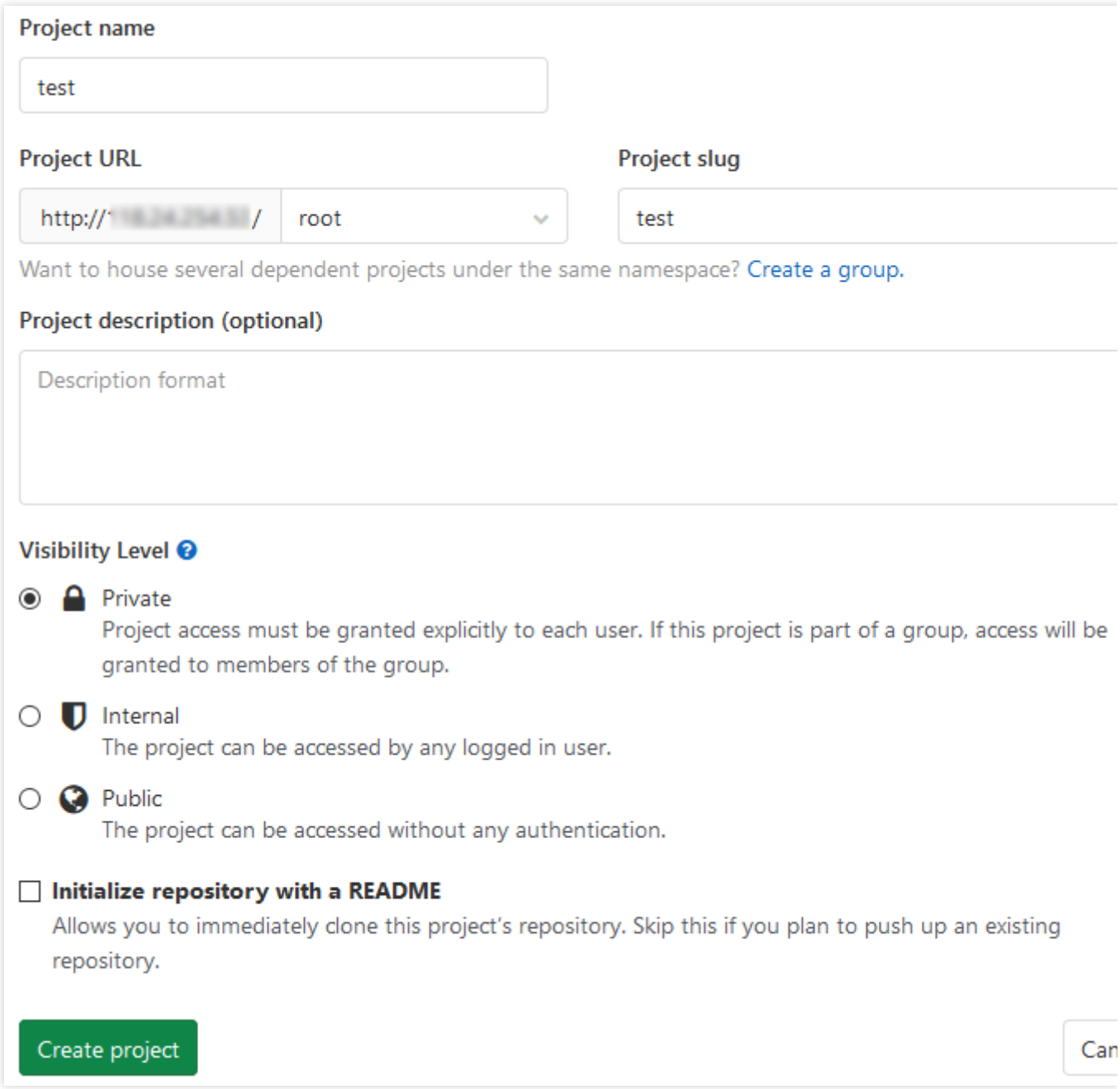


プロジェクトの新規作成

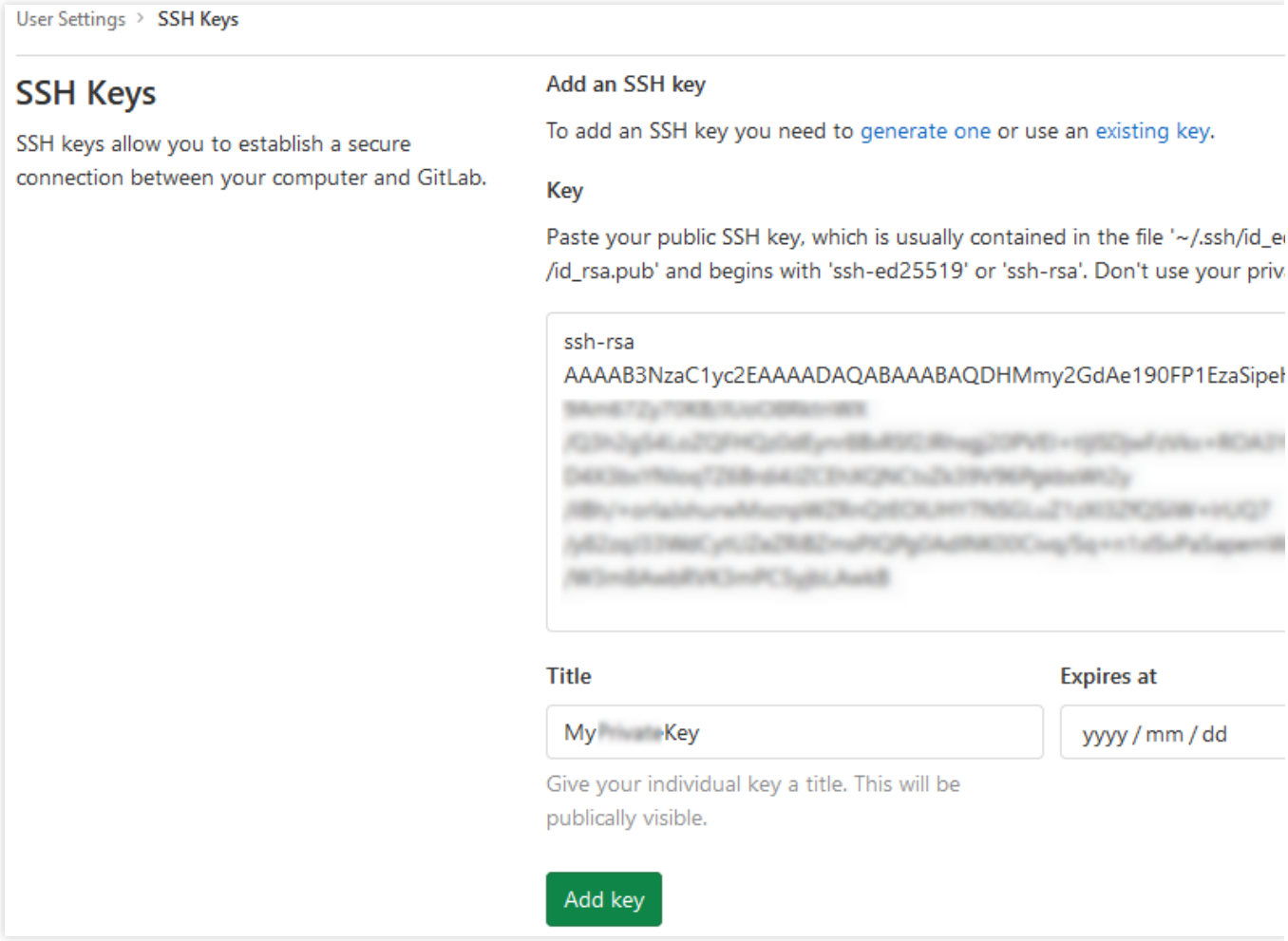
1. ローカルブラウザで、CVMのパブリックIPアドレスにアクセスして、GitLabのログイン画面に入ります。 `root` アカウントおよび設定したログインパスワードを使用してログインします。以下の通りです。



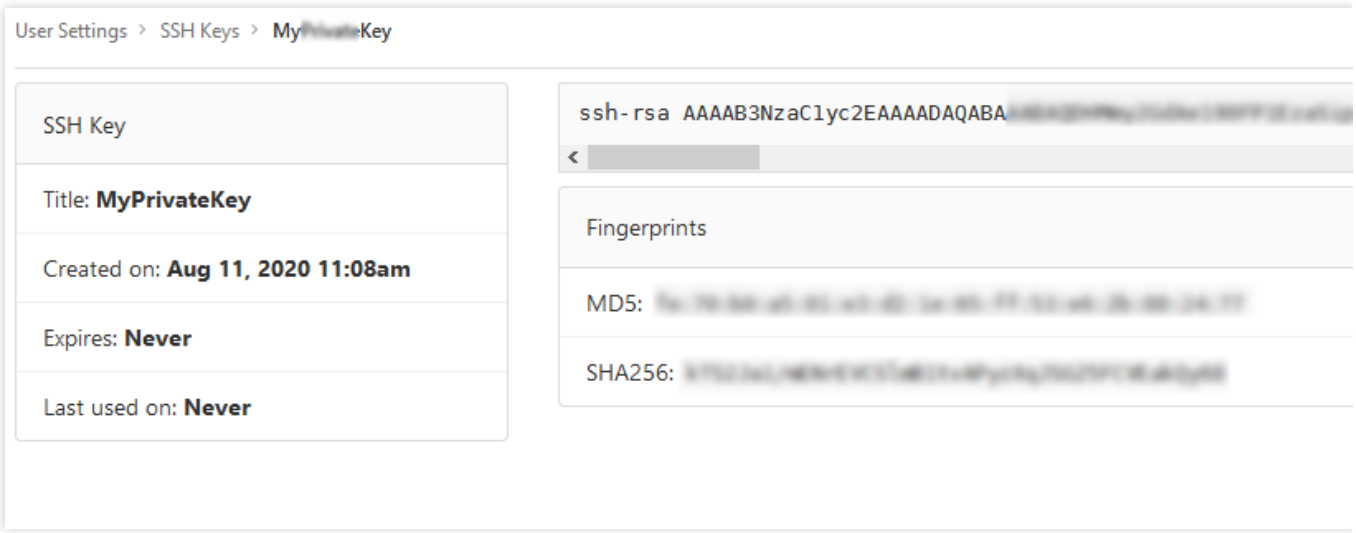
2. 画面の案内に従ってプライベートプロジェクトを新規作成します。本節では、 `test` を例として説明します。以下の通りです。



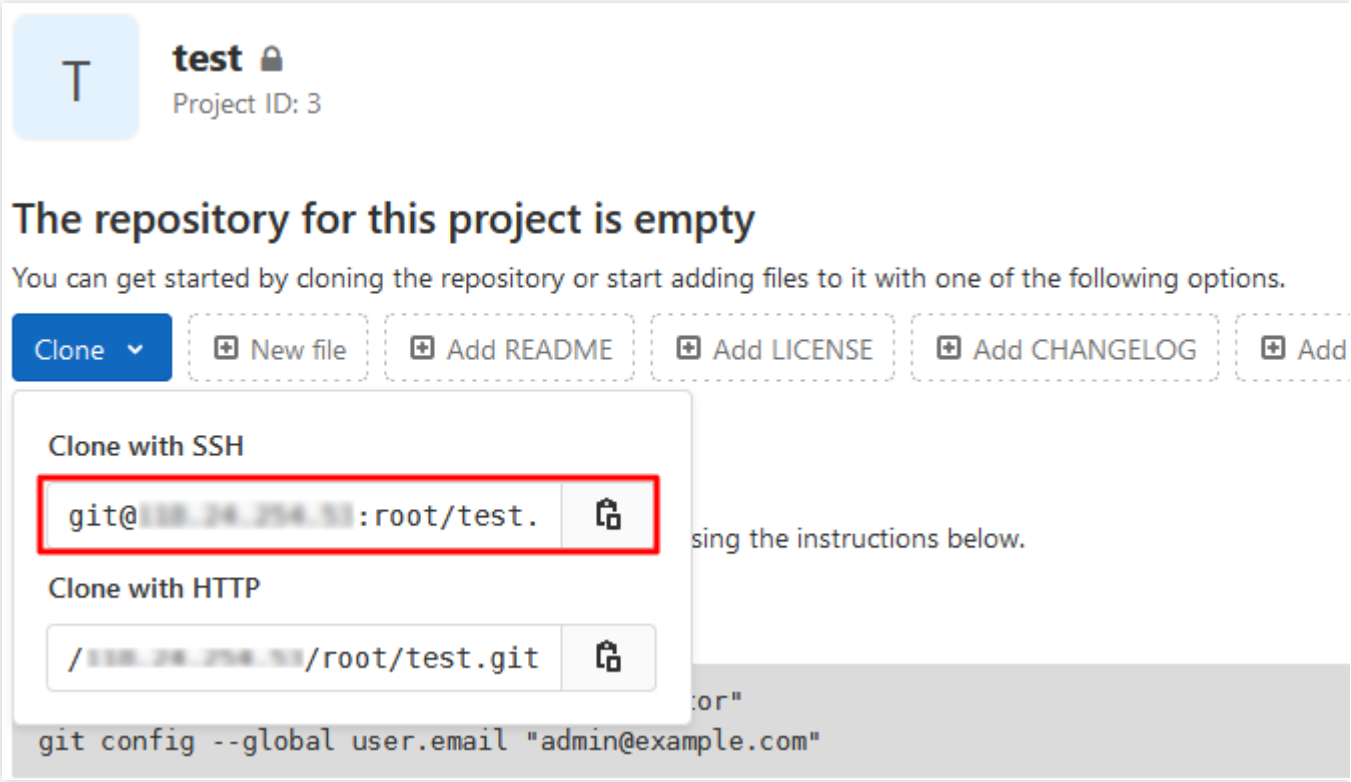
3. プロジェクト作成に成功した後、ページの上部にある【Add SSH Key】をクリックします。
4. 「SSH Keys」ページに入り、次の手順でSSH Keyを追加します：
4.1 キーの取得 ステップで、PCのキー情報を取得し、「Key」に貼り付けます。
4.2 「Title」でこのキーの名前をカスタマイズします。
4.3 【Add key】をクリックするとキーを追加できます。以下の通りです。



次のように表示されるとキーの追加に成功したことを意味します。

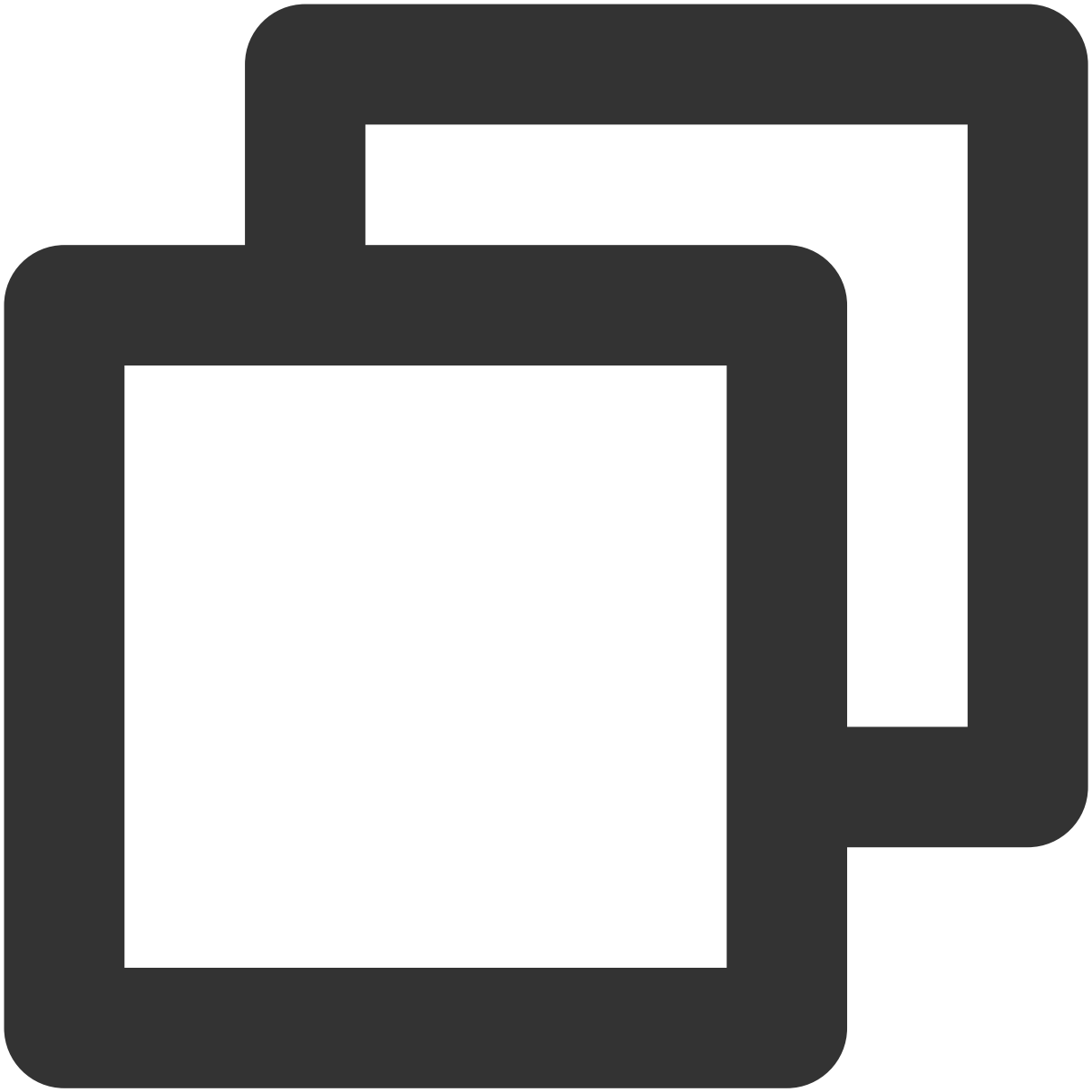


5.
プロジェクトのホームページに戻り
、【clone】をクリックするとプロジェクトアドレスを記録します。以下の通りです。



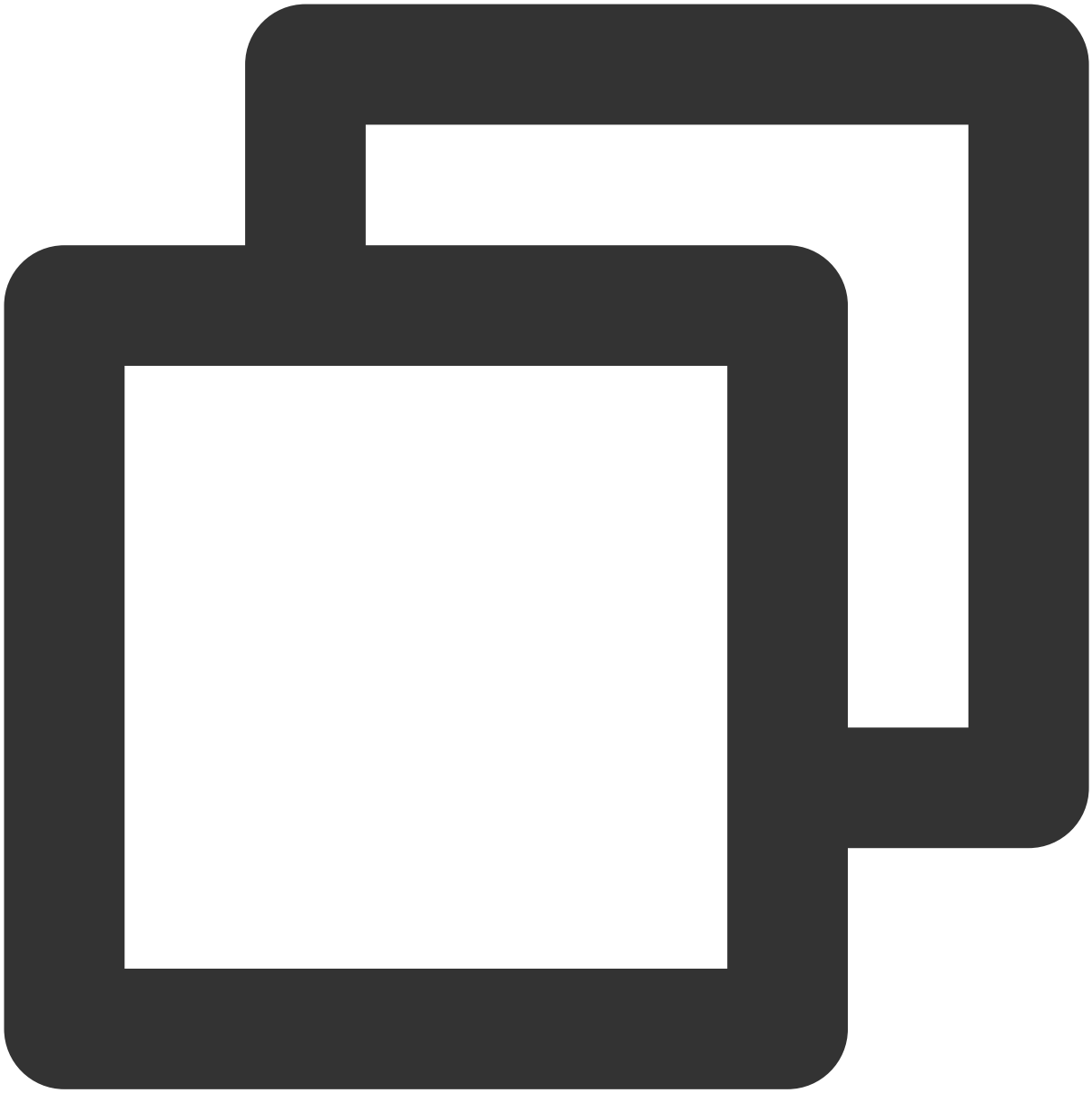
プロジェクトの複製

1. 管理対象のPCで次のコマンドを実行して、Gitリポジトリを使用する担当者の氏名を設定します。



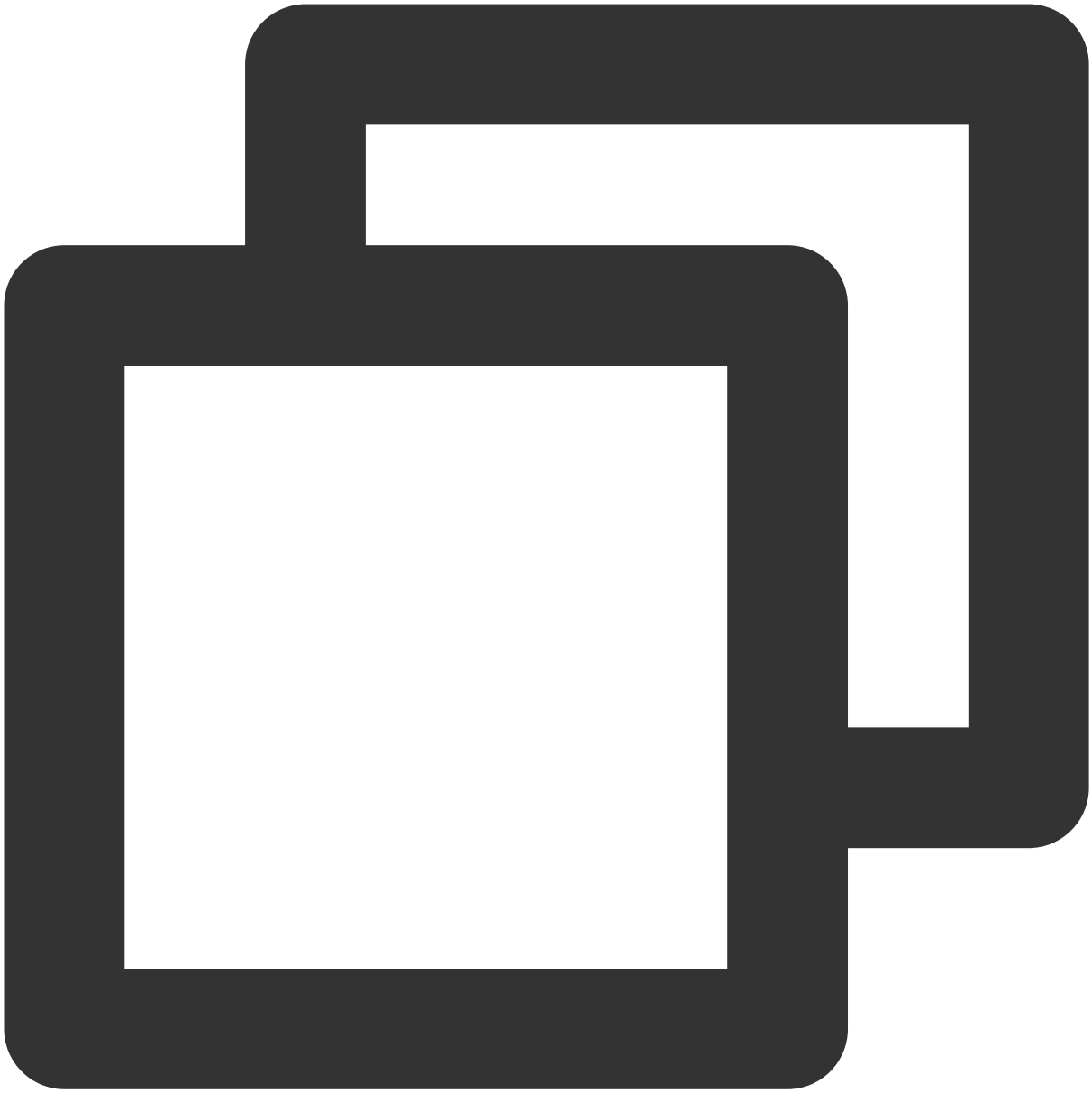
```
git config --global user.name "username"
```

2. 次のコマンドを実行して、Gitリポジトリを使用する担当者のメールボックスを設定します。



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

3. 次のコマンドを実行して、プロジェクトを複製します。ここで、「プロジェクトアドレス」をステップ5で取得したプロジェクトアドレスに置き換えてください。

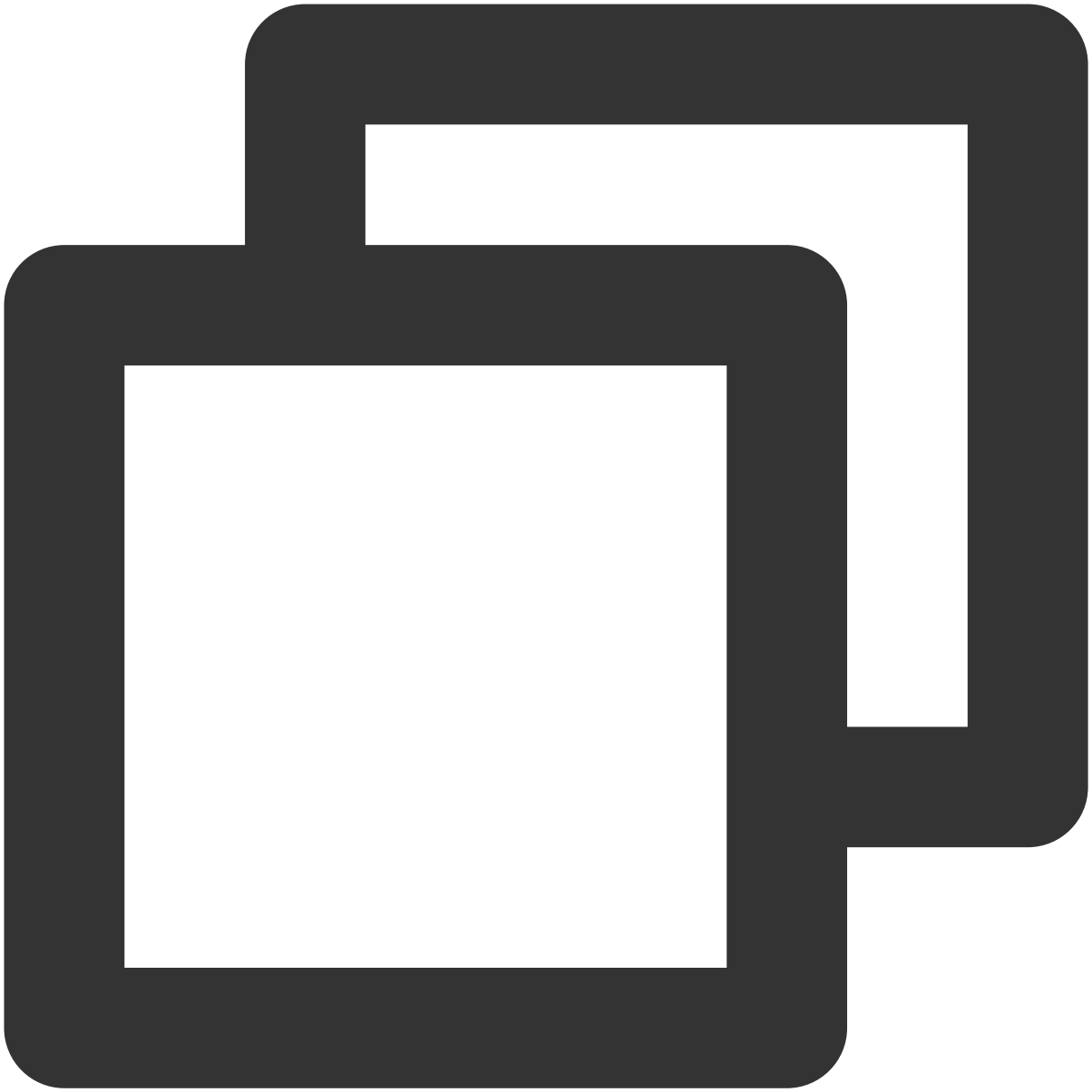


```
git clone 「プロジェクトアドレス」
```

プロジェクトの複製が成功すると、ローカルに同名ディレクトリを生成し、その中にプロジェクトのすべてのファイルが格納されます。

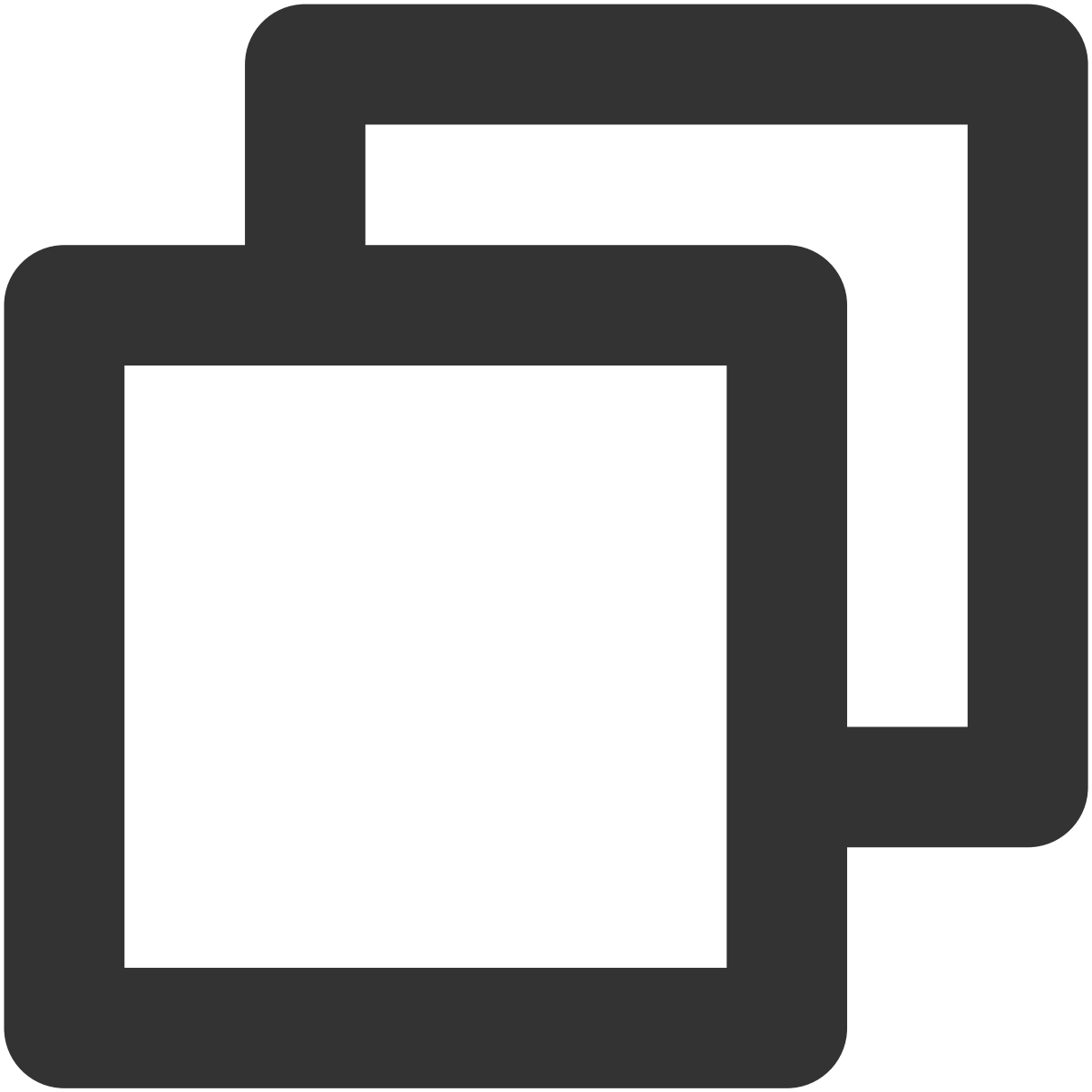
ファイルのアップロード

1. 次のコマンドを実行して、プロジェクトディレクトリに入ります。



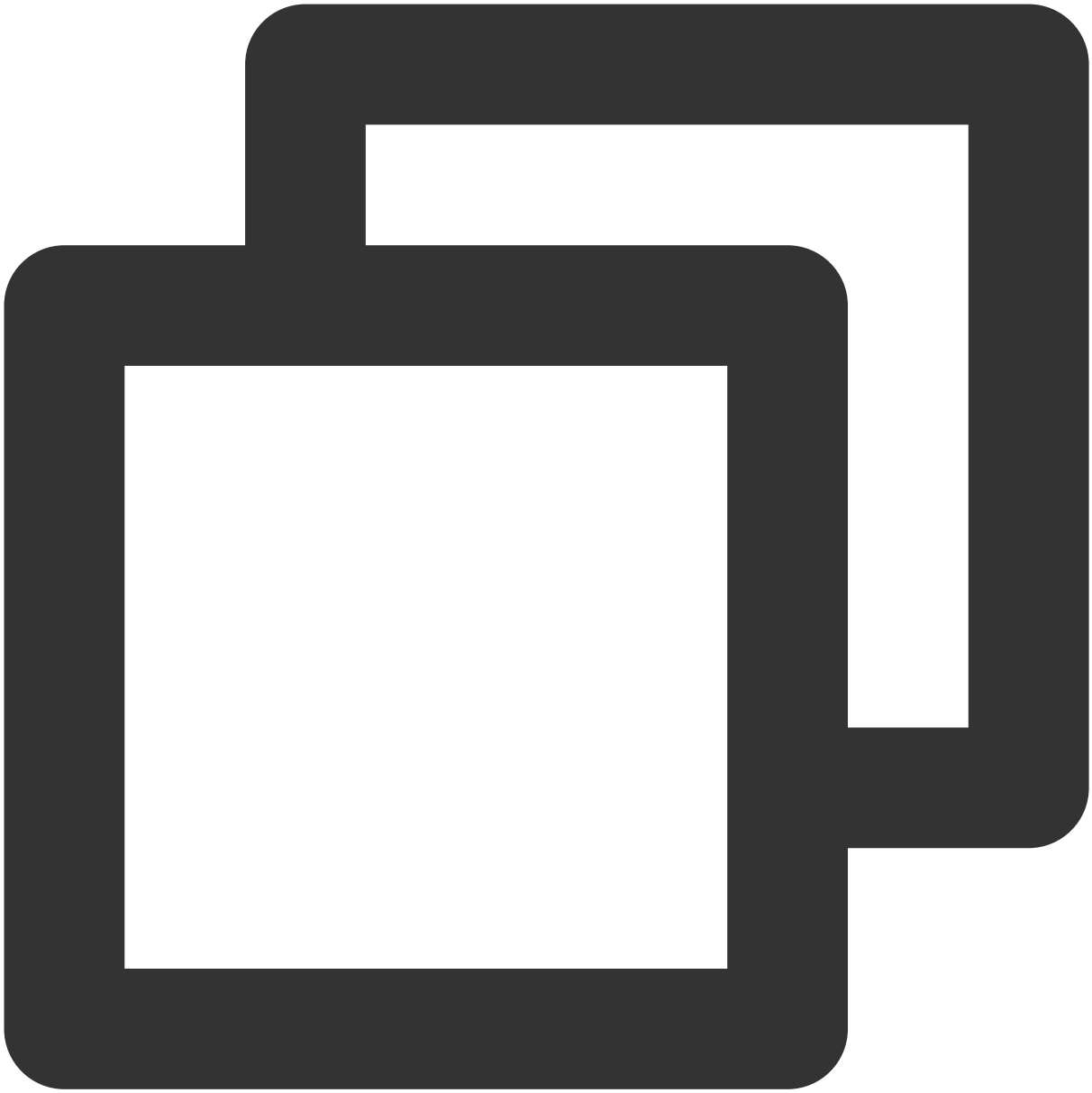
```
cd test/
```

2. 次のコマンドを実行して、GitLabにアップロードするターゲットファイルを作成します。本節では、test.shを例として説明します。



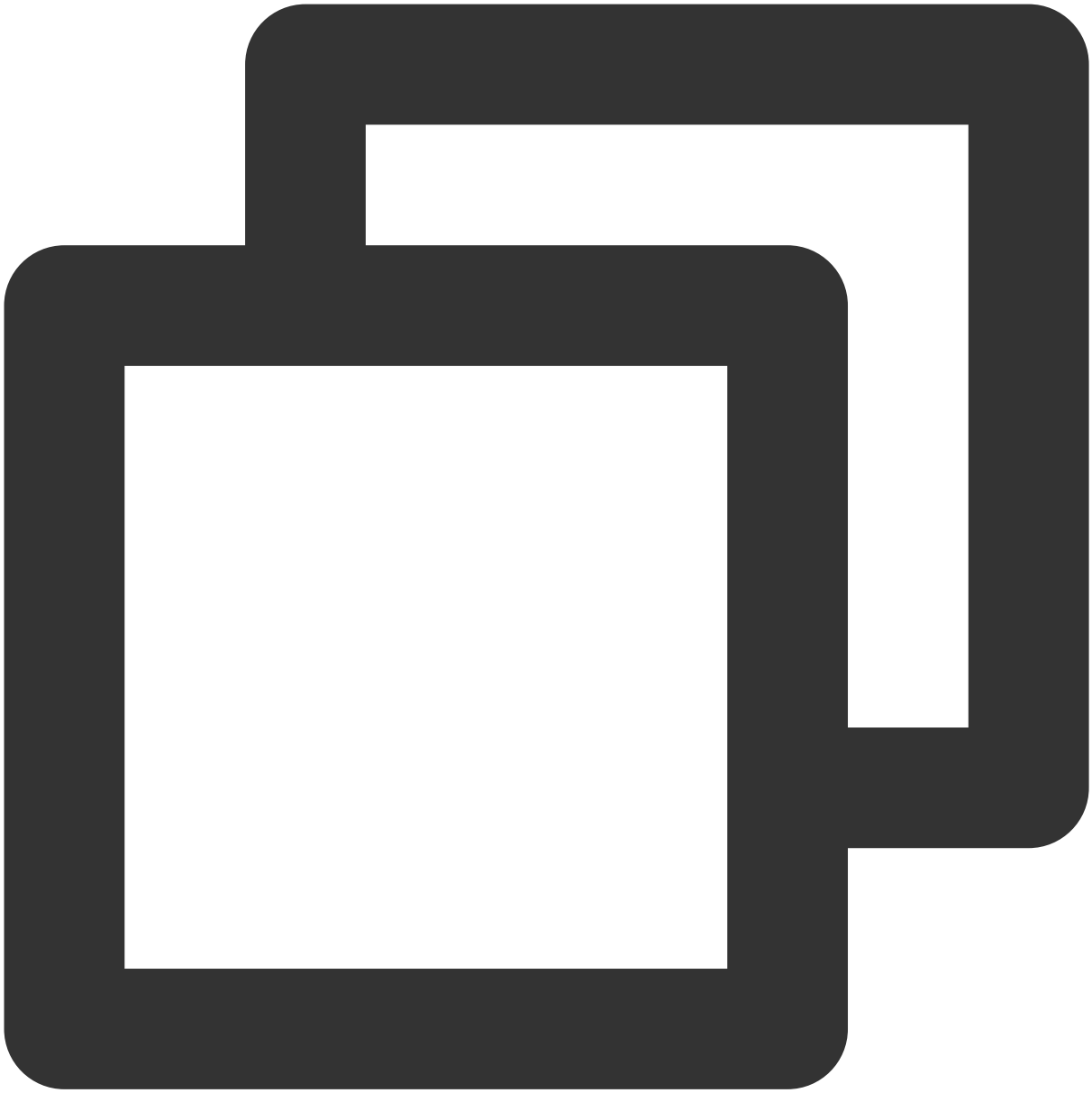
```
echo "test" > test.sh
```

3. 次のコマンドを実行して、test.shファイルをインデックスに追加します。



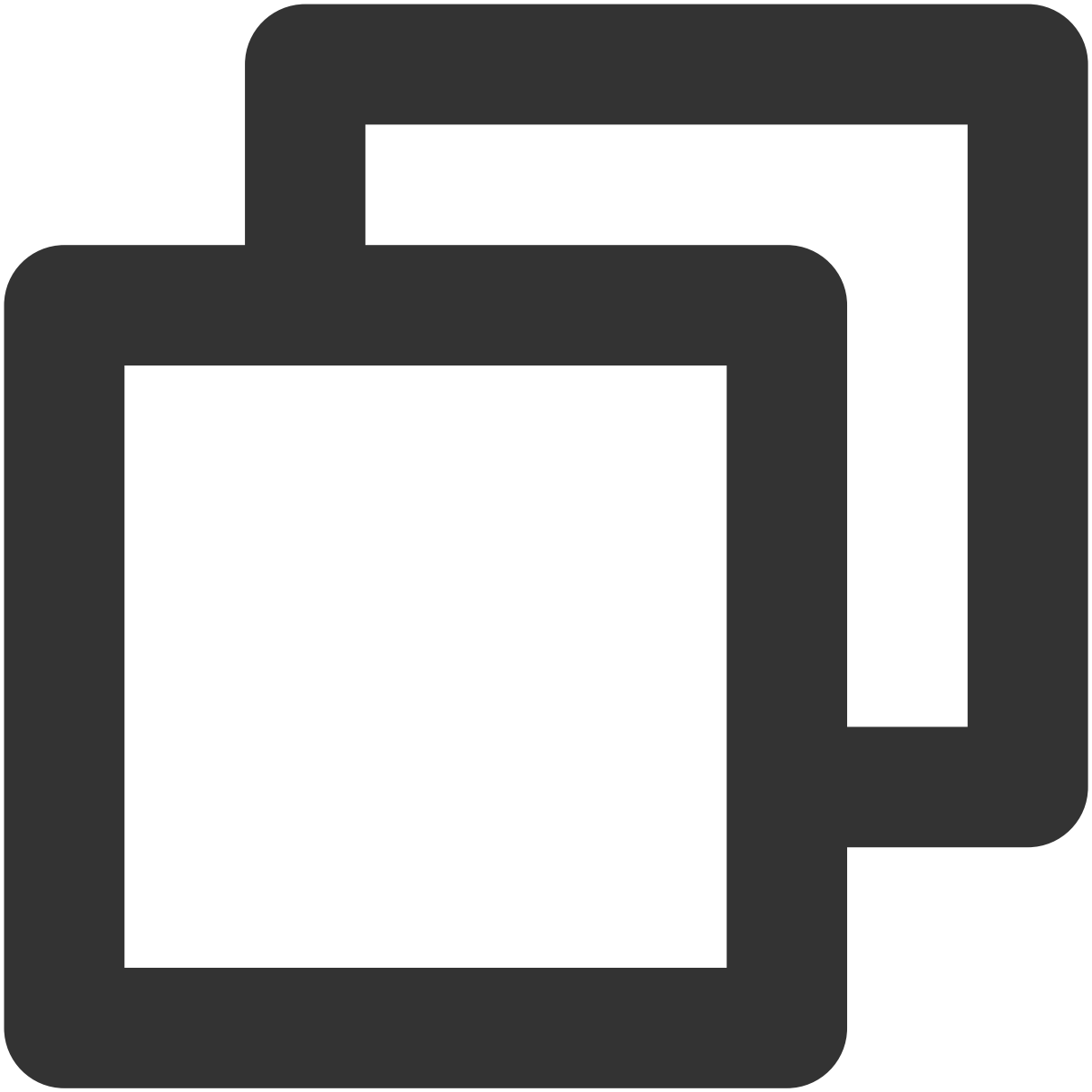
```
git add test.sh
```

4. 次のコマンドを実行して、test.shをローカルリポジトリに提出します。



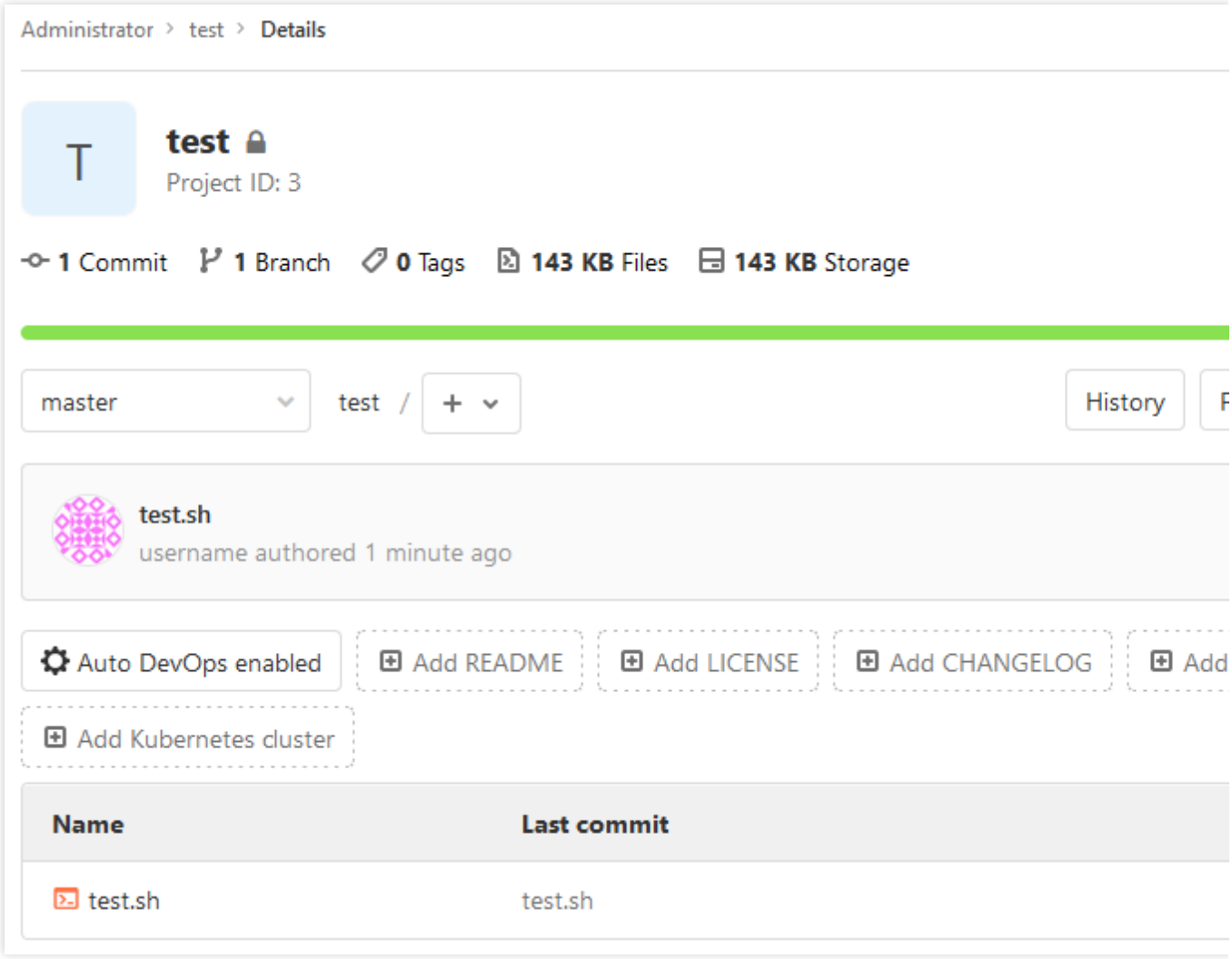
```
git commit -m "test.sh"
```

5. 次のコマンドを実行して、test.shをGitLabサーバーに同期します。



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

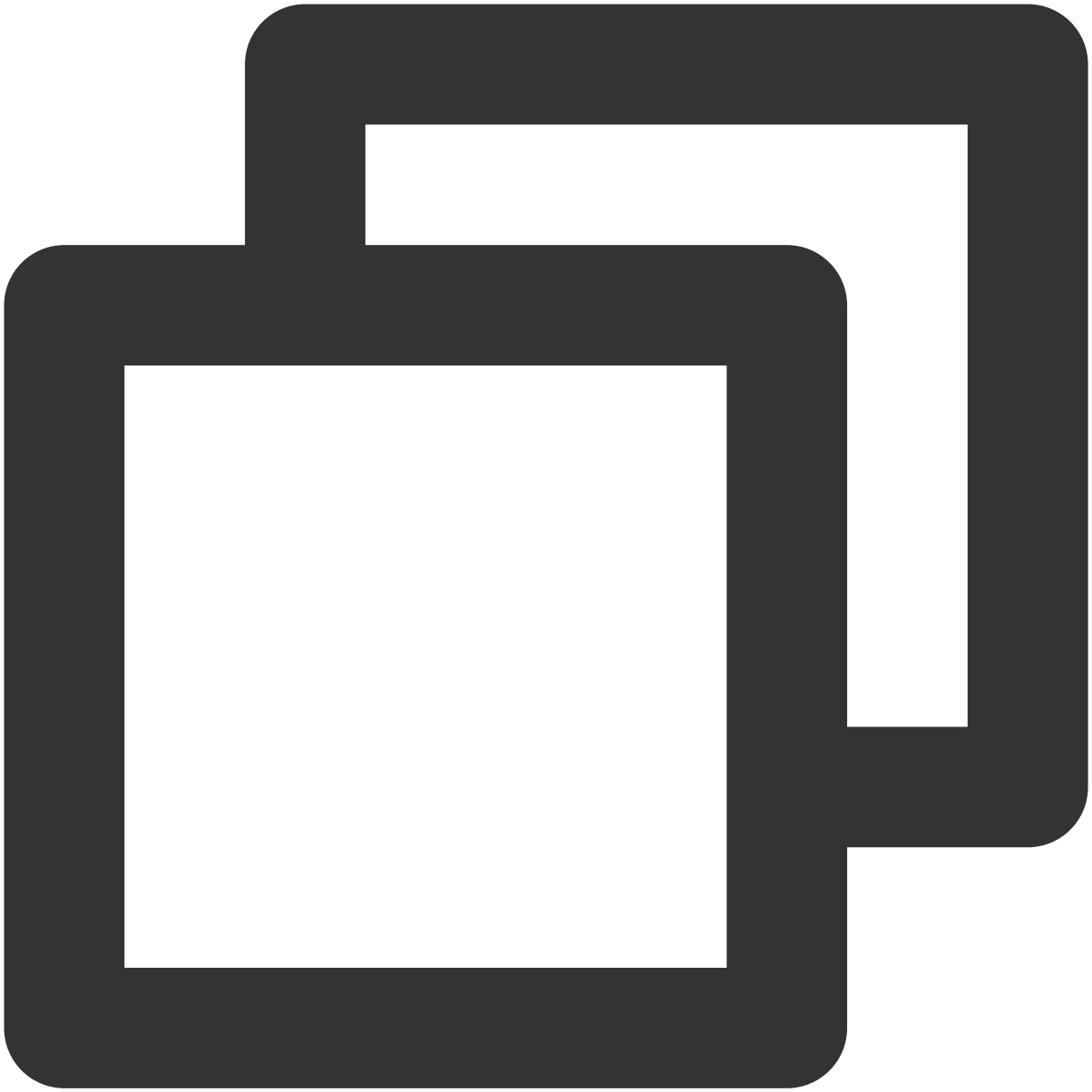
testプロジェクト画面に戻ると、ファイルのアップロードに成功したことを確認できます。以下の通りです。



関連操作

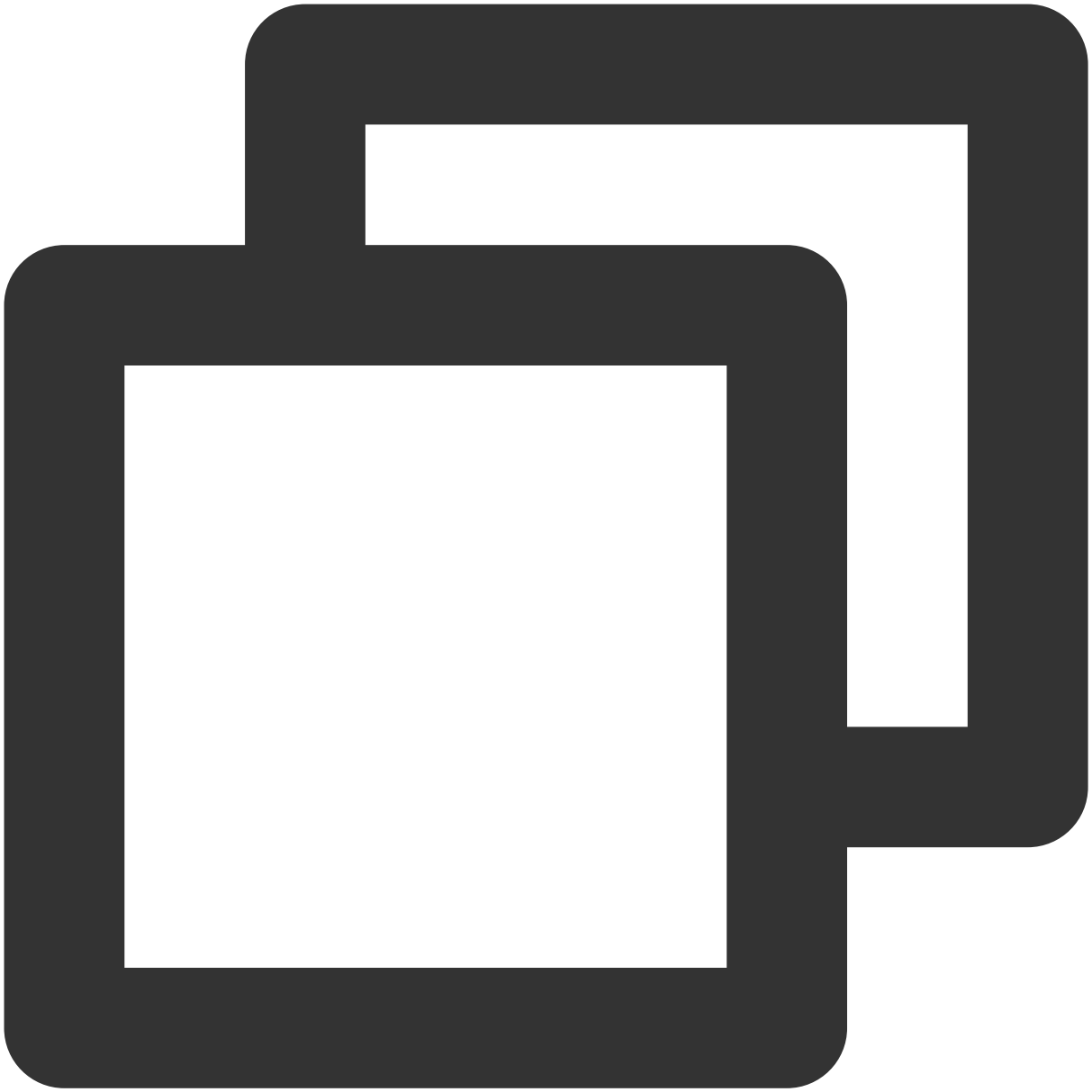
キーの取得

1. プロジェクト管理に組み入れる必要があるPCで、次のコマンドを実行して、Gitをインストールします。



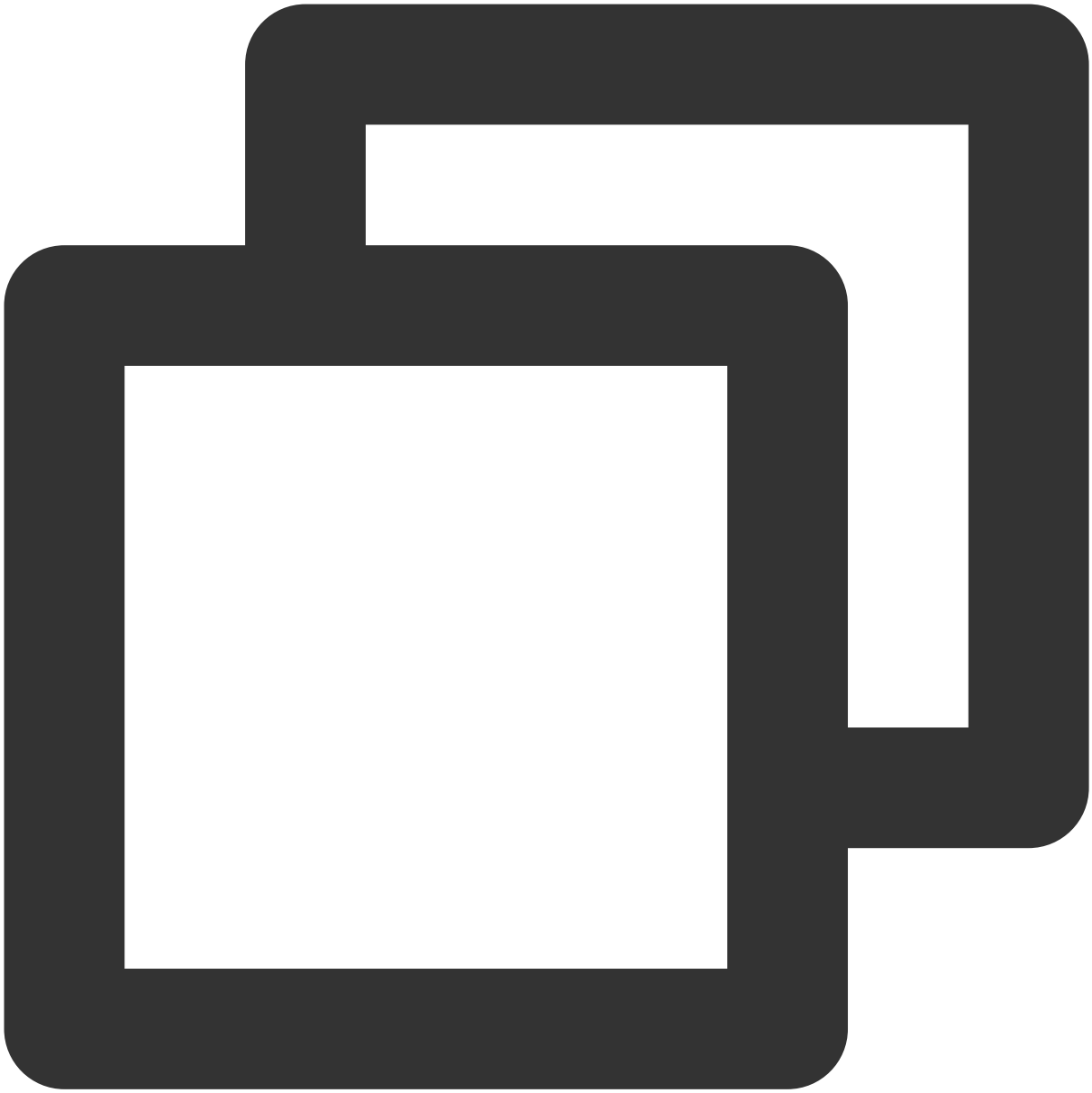
```
yum install -y git
```

2. 次のコマンドを実行して、キーファイル.ssh/id_rsaを生成します。キーファイルの生成プロセス中に、**Enter**キーを押してデフォルト設定を保持します。



```
ssh-keygen
```

3. 次のコマンドを実行して、キー情報を表示および記録します。



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

RabbitMQクラスタの構築

最終更新日：：2022-03-16 16:54:45

操作シナリオ

RabbitMQは、高度なメッセージキュープロトコル（Advanced Message Queuing Protocol、AMQP）を実現したオープンソースのメッセージブローカーです。サーバー側はErlang言語を用いて作成され、Python、Ruby、.NET、Java、JMS、C、PHP、ActionScript、XMPP、STOMP、AJAXなど多様なクライアントをサポートしています。ユーザビリティ、拡張性および高可用性などのメリットがあり、本節を参考にして、RabbitMQをTencent Cloud CVMで配置することができます。

ソフトウェア

本節の説明例に使用するソフトウェアバージョンおよびその構成は次の通りです。
Linux：Linux OS。このドキュメントでは、CentOS 7.7を例として説明します。
RabbitMQ Server：オープンソースのメッセージブローカーです。本節では、RabbitMQ Server 3.6.9を例として説明します。
Erlang：プログラミング言語です。本節では、Erlang 19.3を例として説明します。

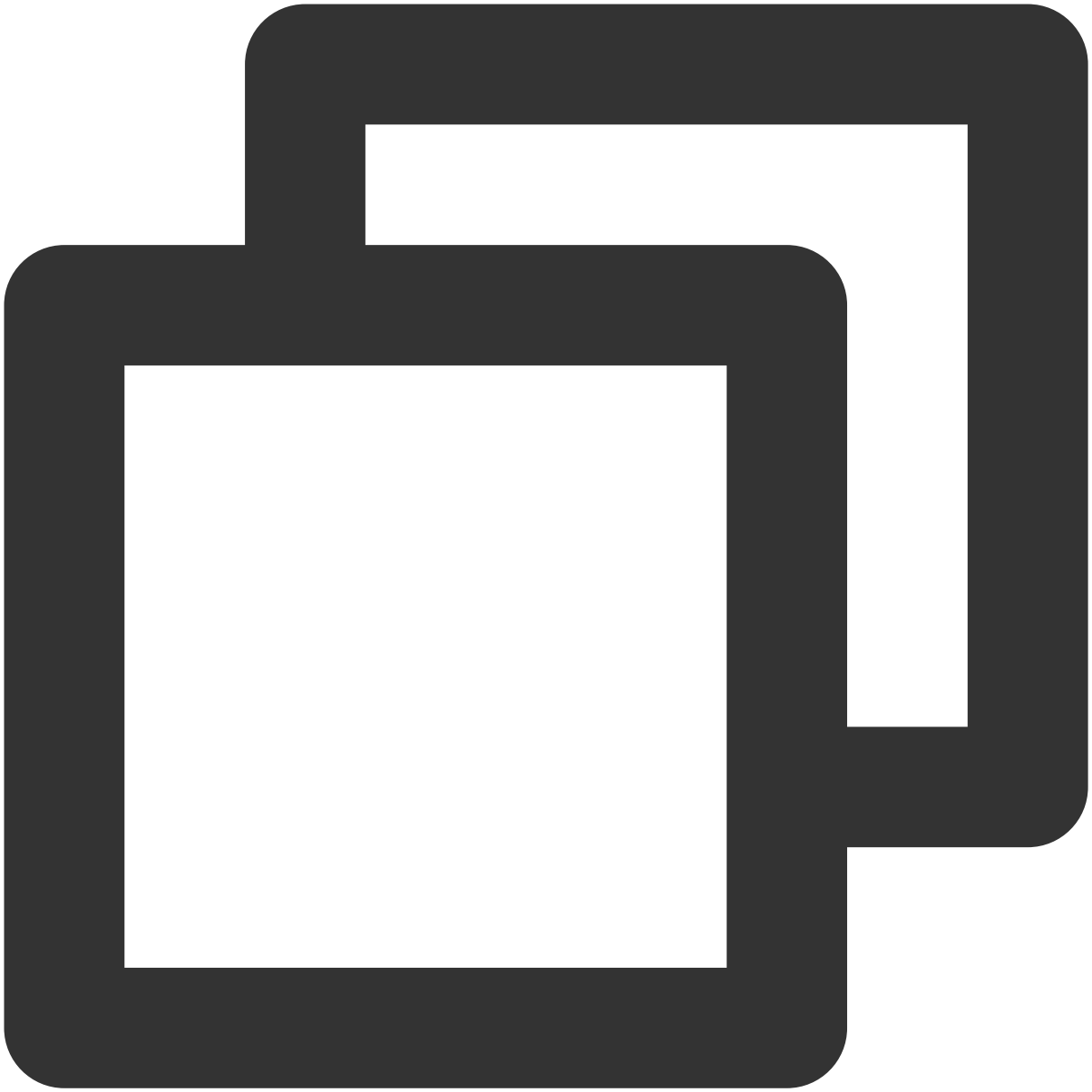
前提条件

Linux CVMを購入済みであること。
Linuxインスタンスのセキュリティグループルールはすでに設定されています。ポート80、5672、15672を開きます。詳細については、セキュリティグループルールの追加 をご参照ください。

操作手順

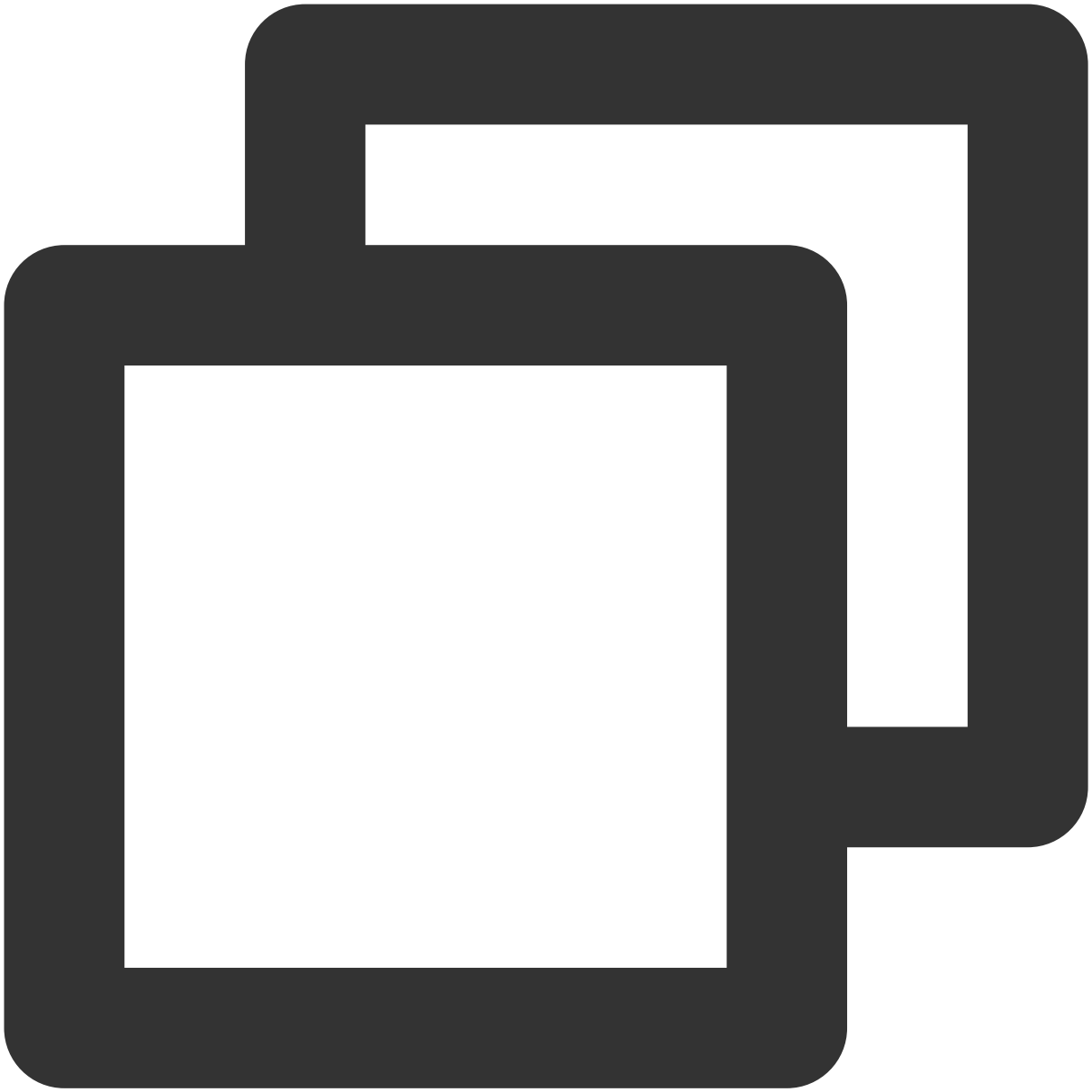
Erlangのインストール

1. 標準方法を使用してLinuxインスタンスにログインします（推奨）。実際の操作方法に応じて、他のログイン方法を選択することもできます。
リモートログインソフトウェアを使用してLinuxインスタンスにログインする
SSHキーを使用してLinuxインスタンスにログインする
2. 以下のコマンドを実行して、依存関係をインストールします。



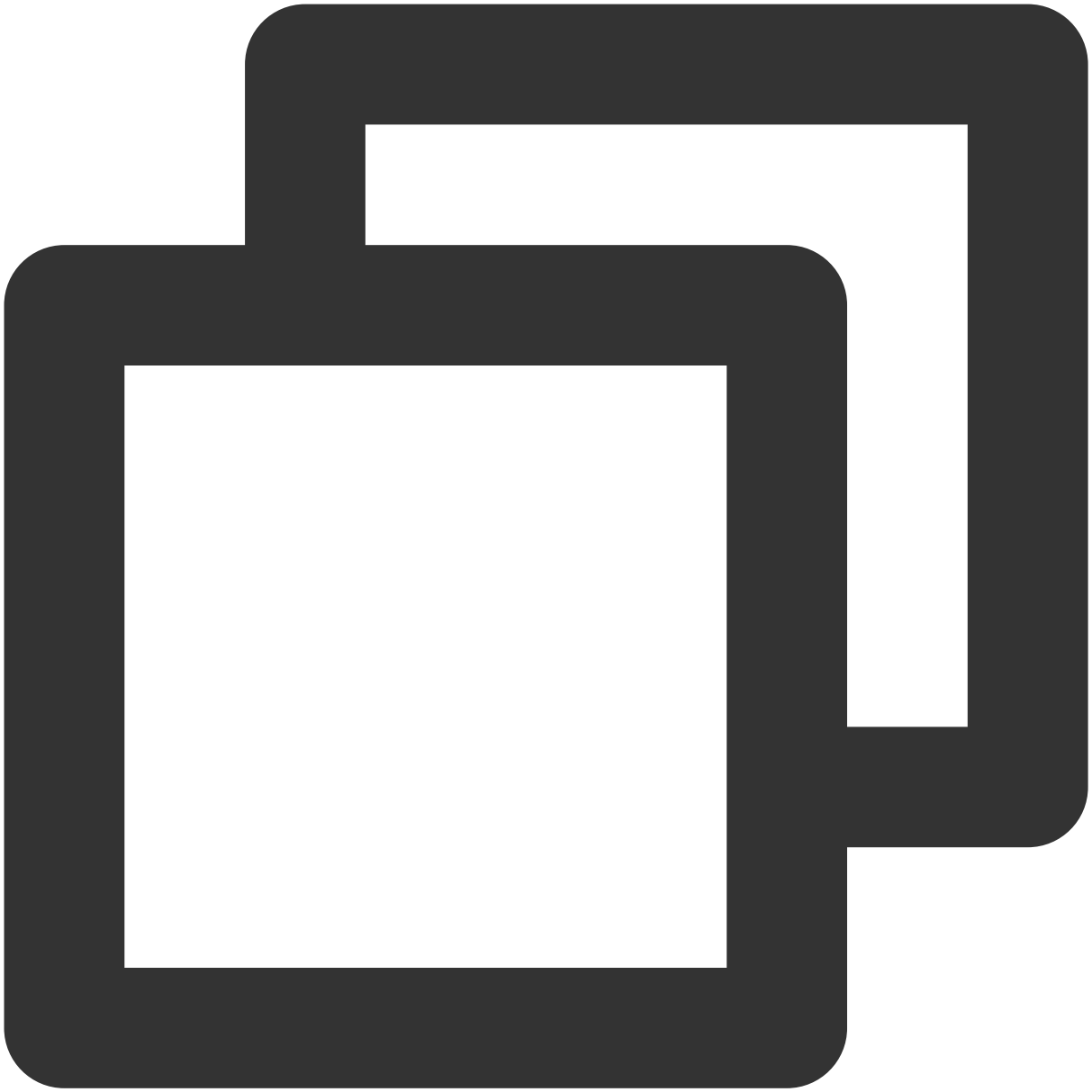
```
yum -y install make gcc gcc-c++ m4 ncurses-devel openssl-devel unixODBC-devel
```

3. 次のコマンドを実行して、Erlangインストールパッケージをダウンロードします。



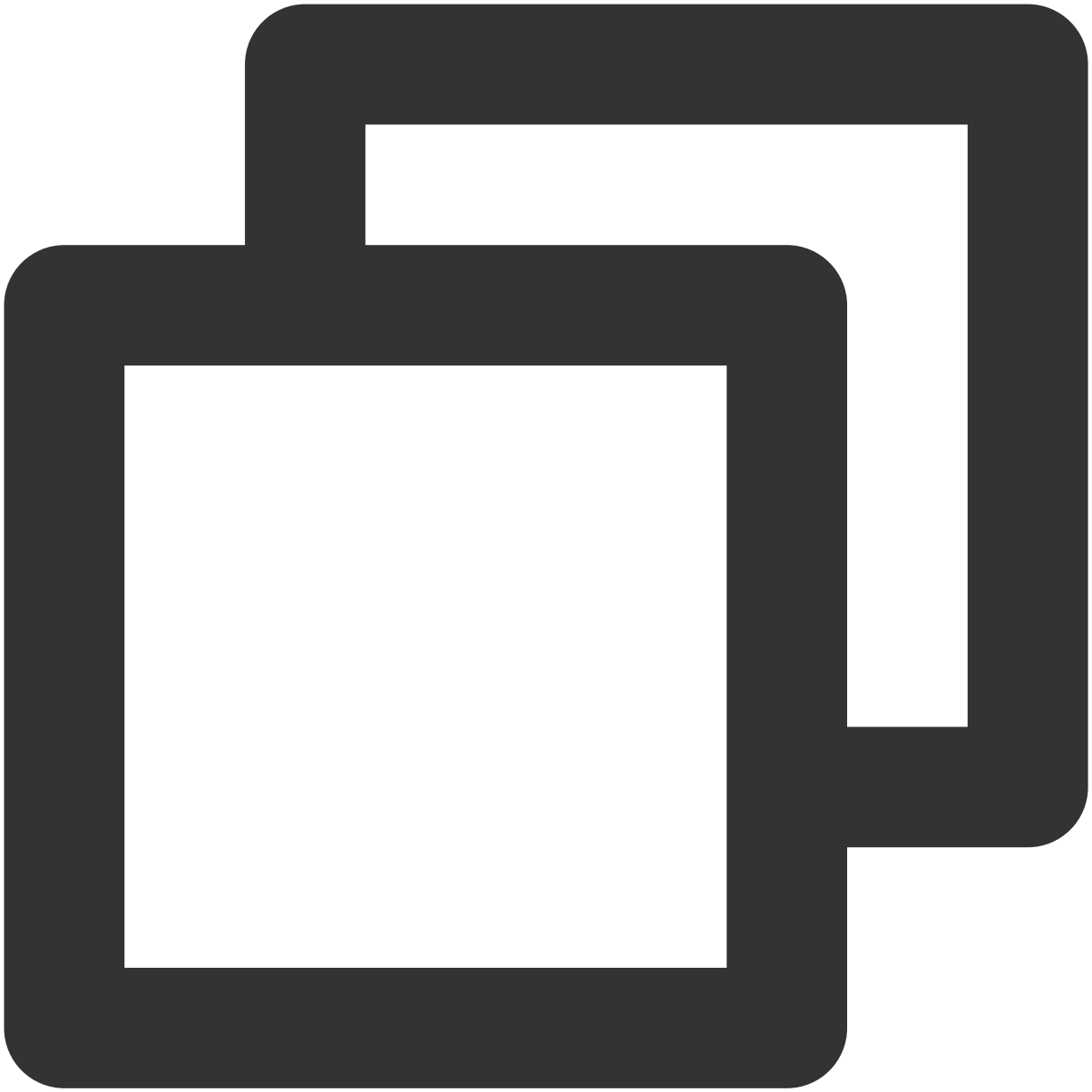
```
wget http://erlang.org/download/otp_src_19.3.tar.gz
```

4. 次のコマンドを実行して、Erlangインストールパッケージを解凍します。



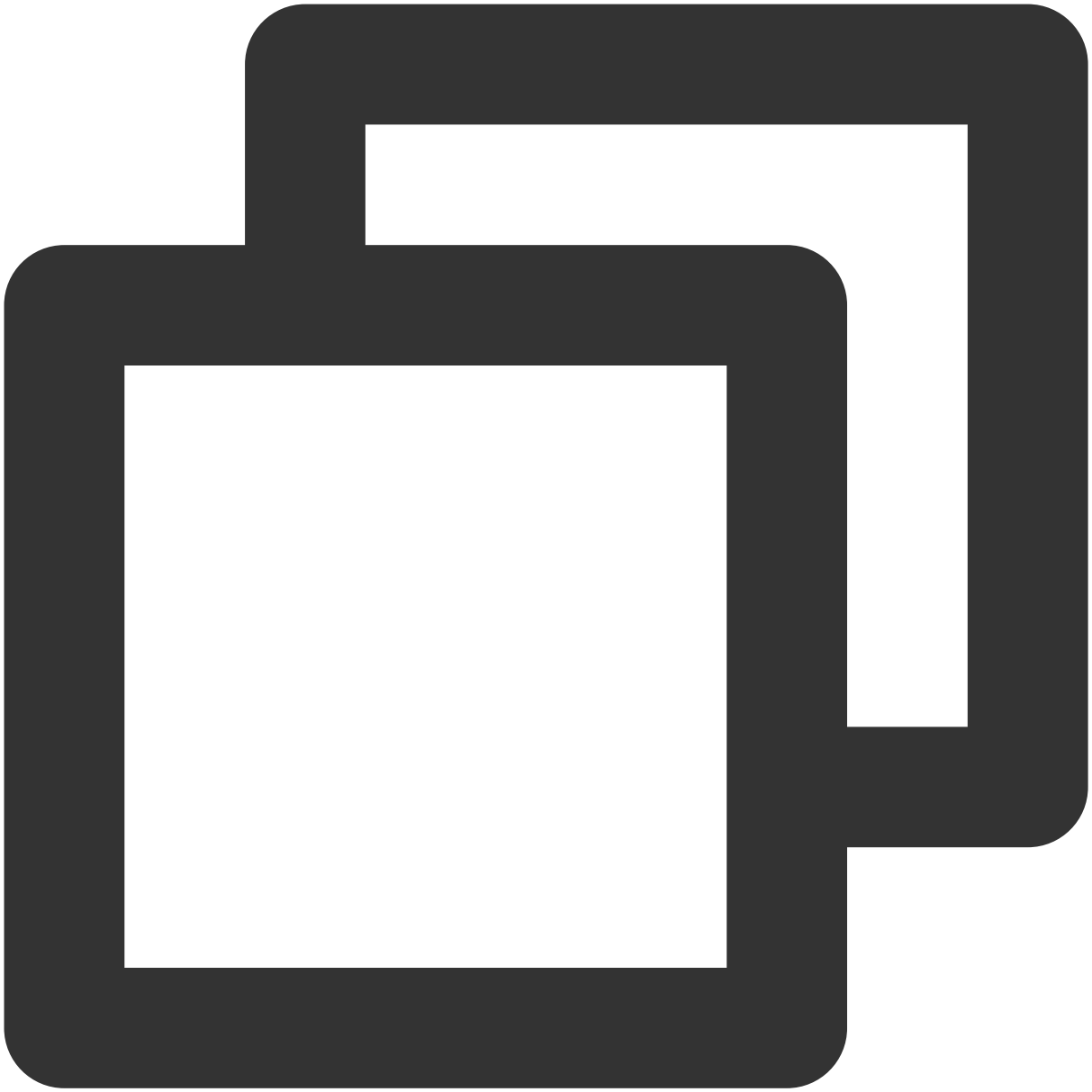
```
tar xzf otp_src_19.3.tar.gz
```

5. 次のコマンドを実行して、Erlangフォルダを作成します。

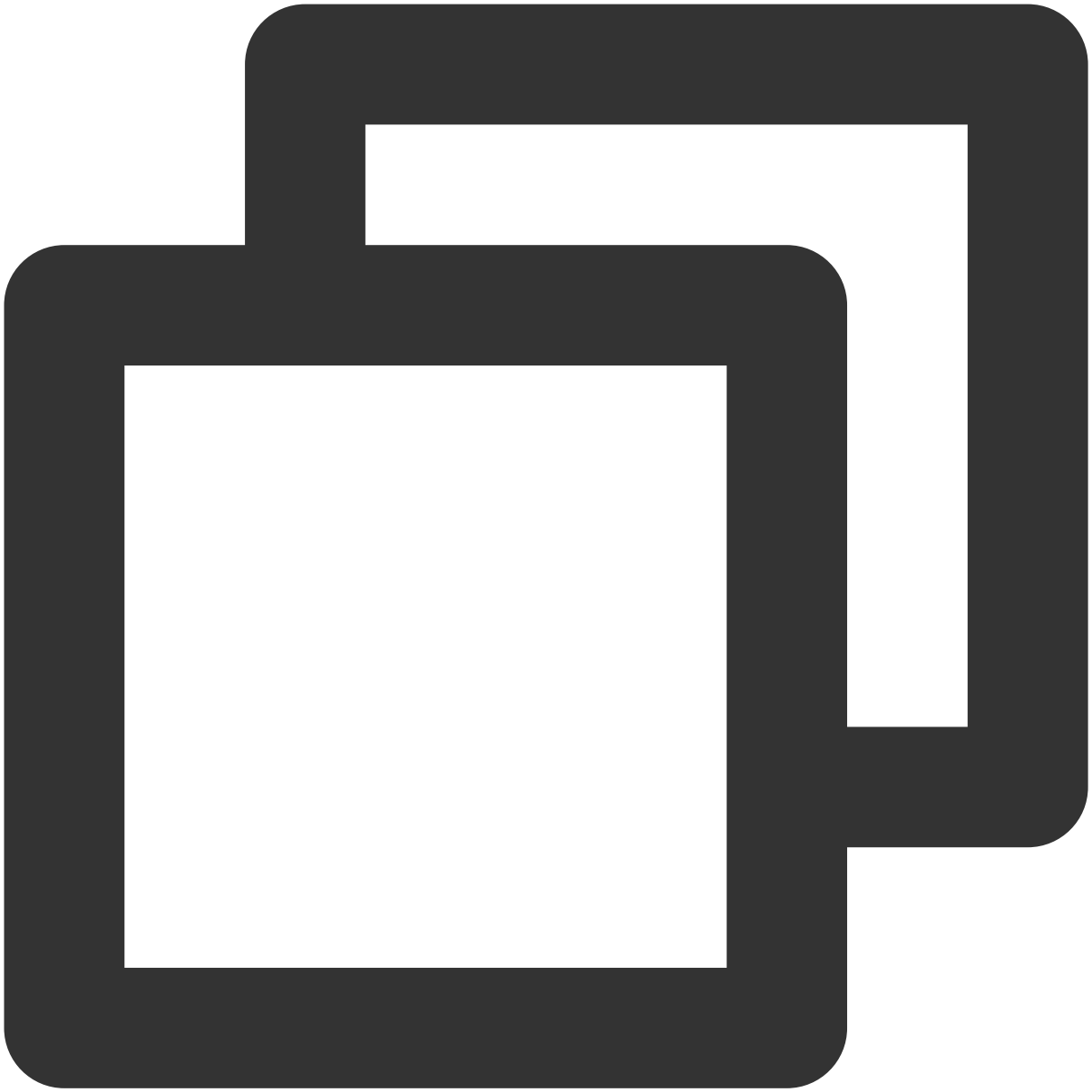


```
mkdir /usr/local/erlang
```

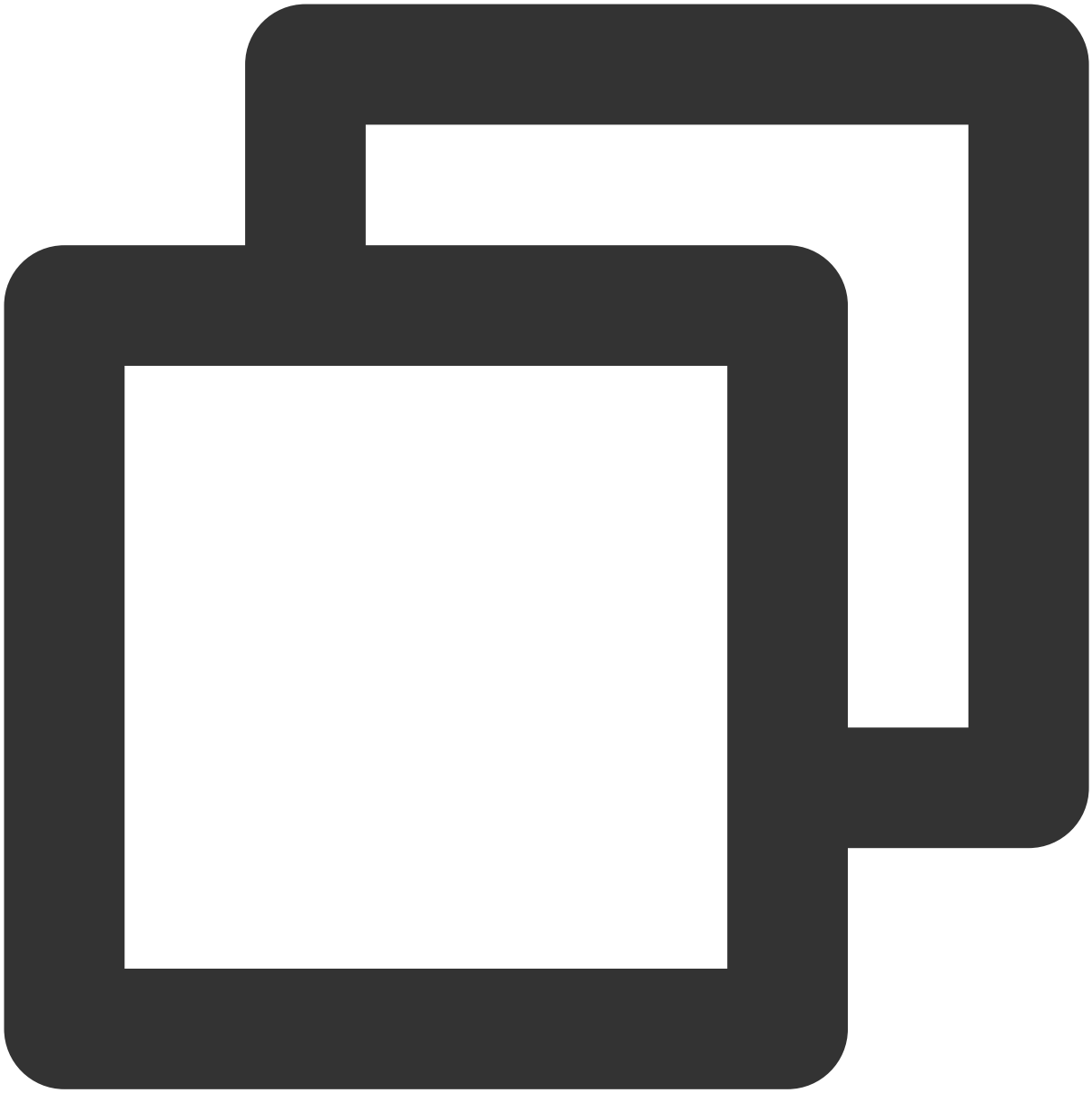
6. 次のコマンドを順次実行して、Erlangをコンパイルしてインストールします。



```
cd otp_src_19.3
```

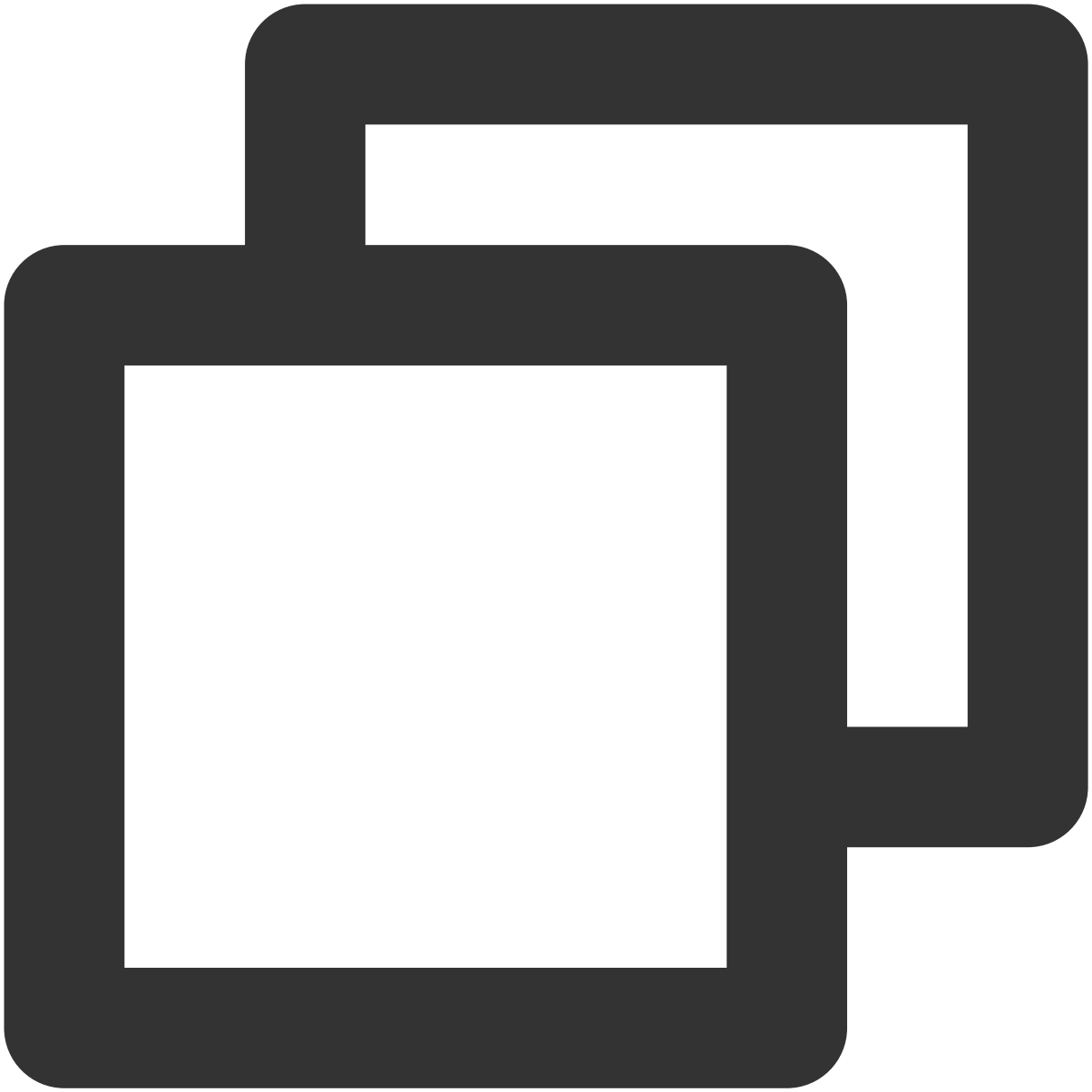


```
./configure --prefix=/usr/local/erlang --without-javac
```



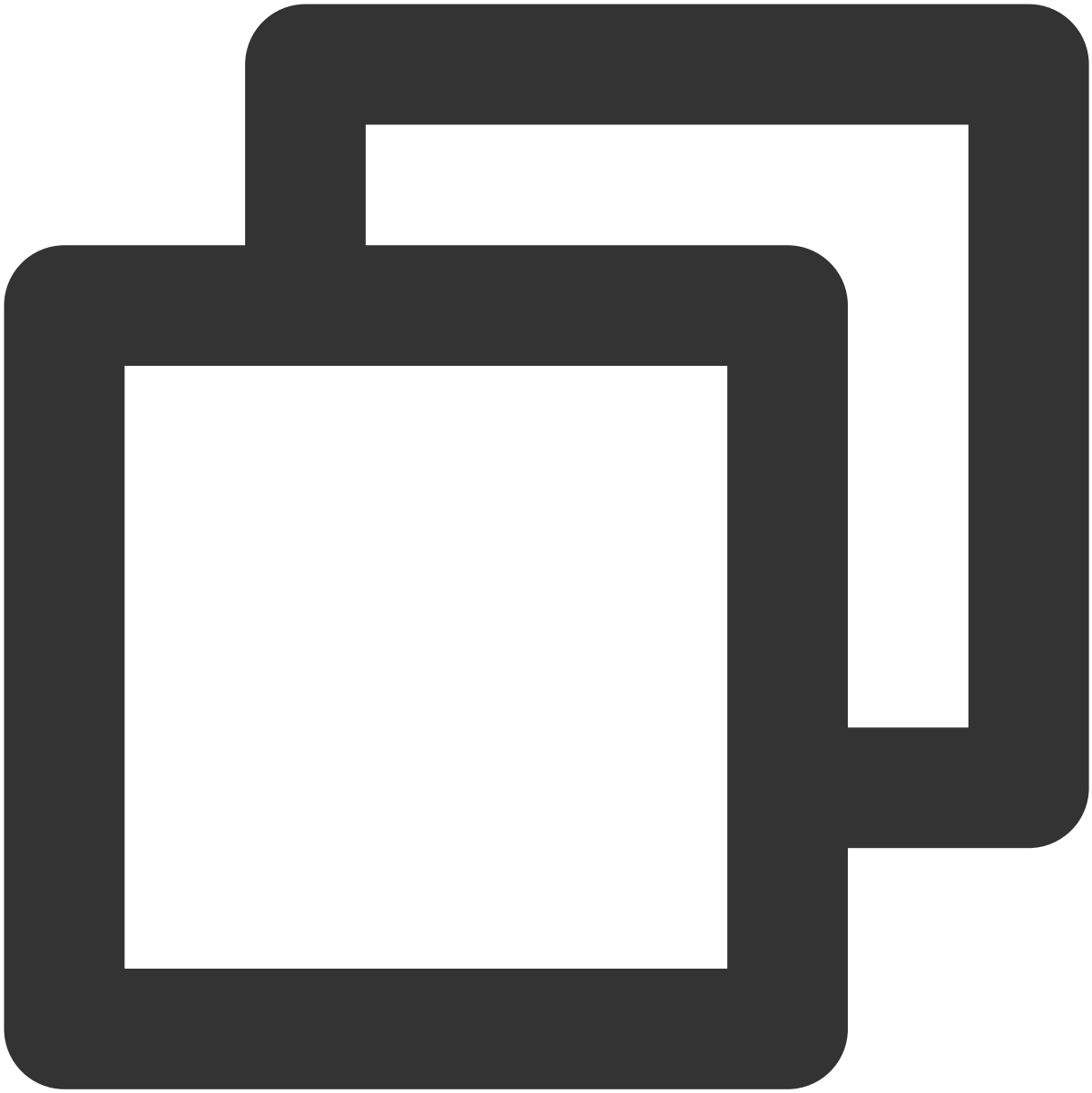
```
make && make install
```

7. 次のコマンドを実行して、profile構成ファイルを開きます。



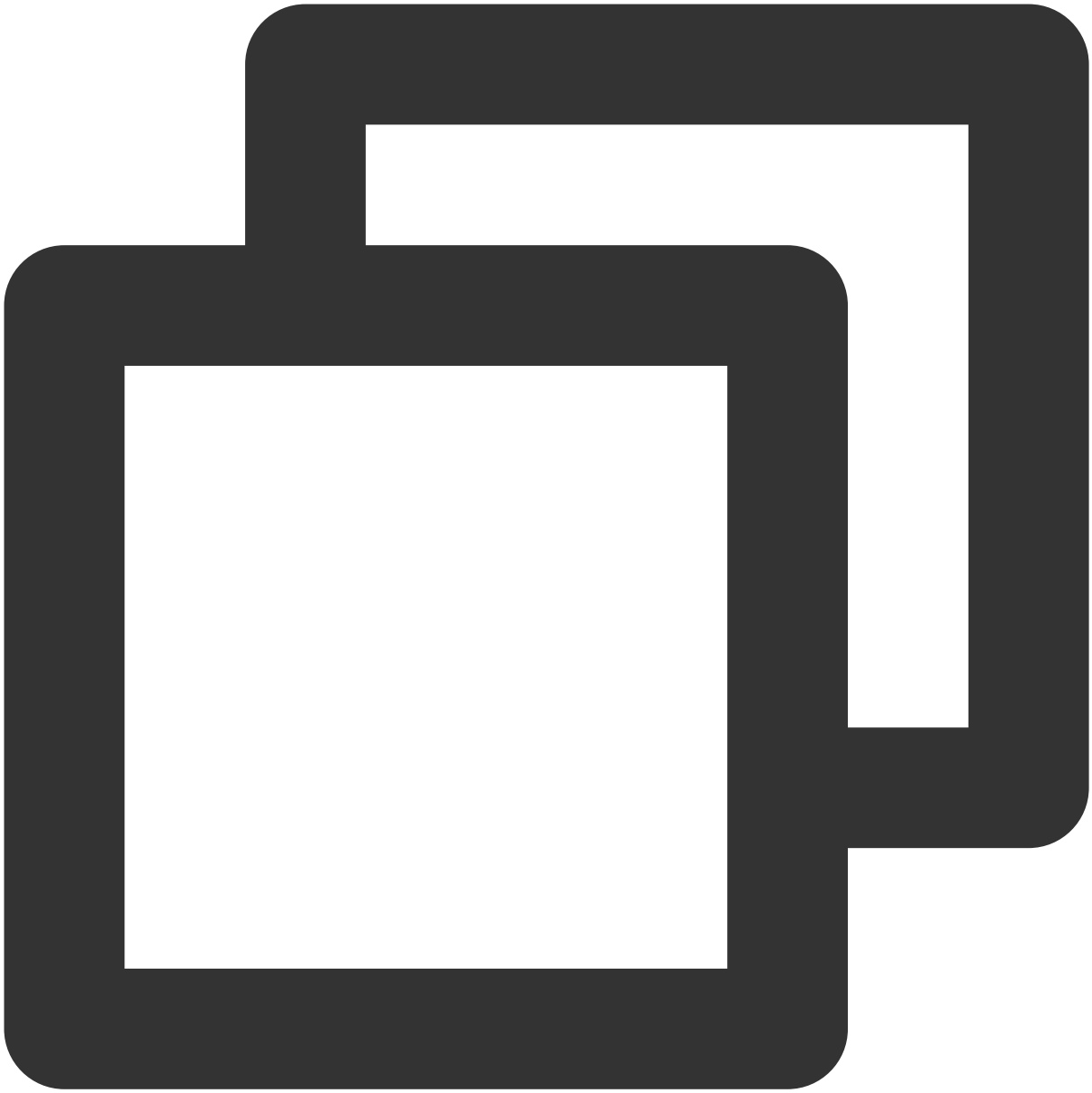
```
vi /etc/profile
```

8. **i**を押して編集モードに入り、ファイルの最後に次のように入力します。



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

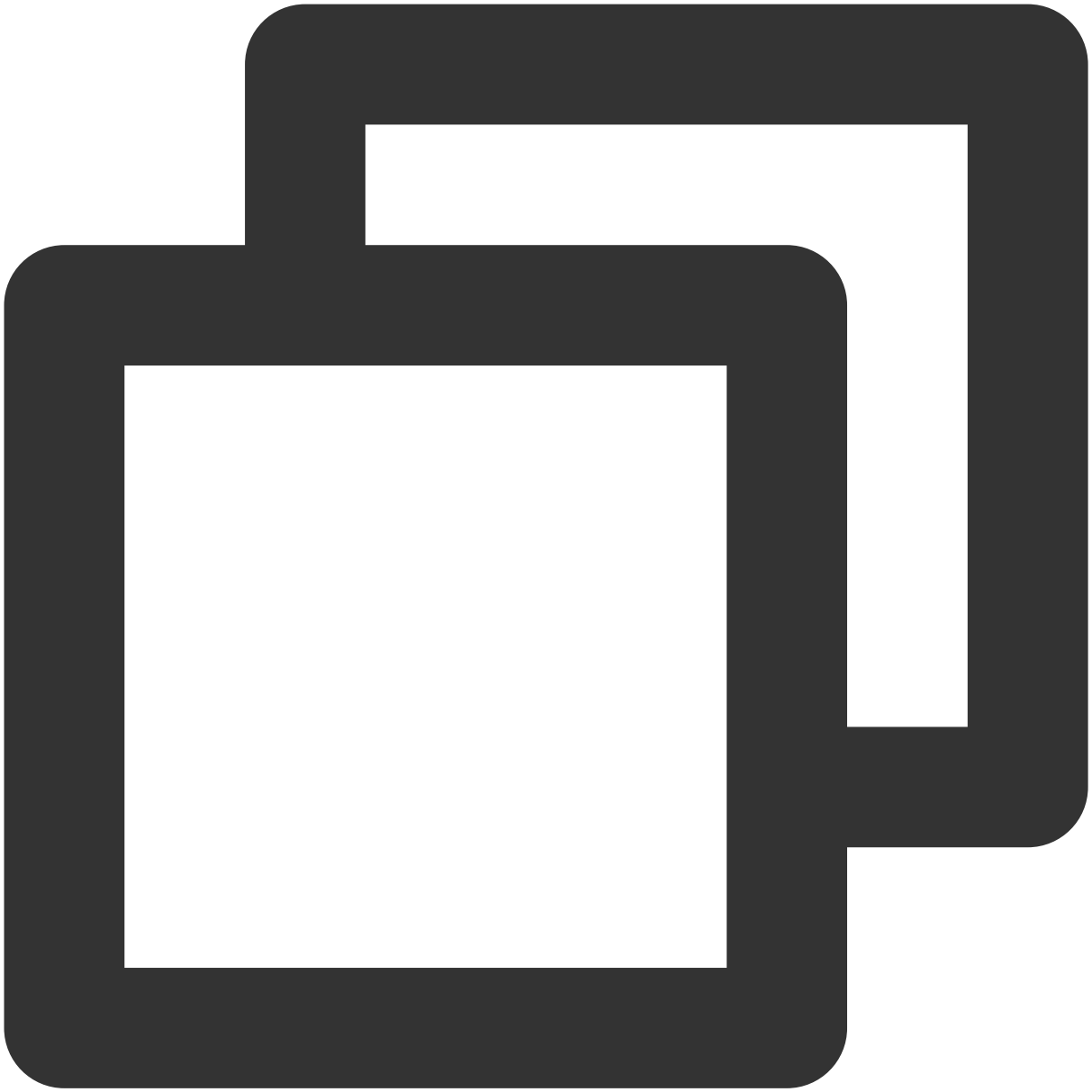
9. **Esc**キーを押し、**:wq**を入力し、ファイルを保存してから終了します。
10. 次のコマンドを実行して、直ちに環境変数を有効にします。



```
source /etc/profile
```

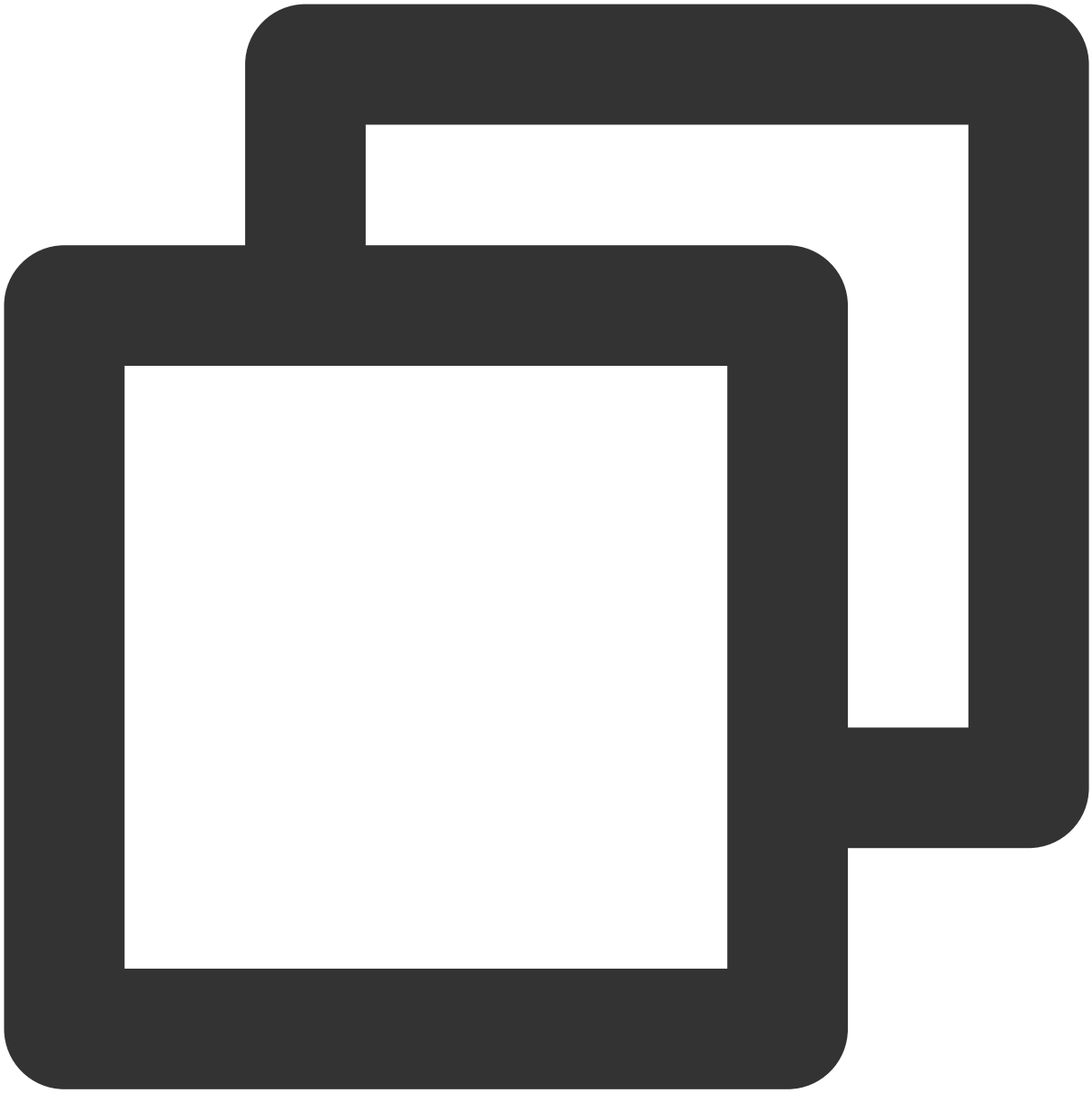
RabbitMQ Serverのインストール

1. 次のコマンドを実行して、RabbitMQ Serverインストールパッケージをダウンロードします。



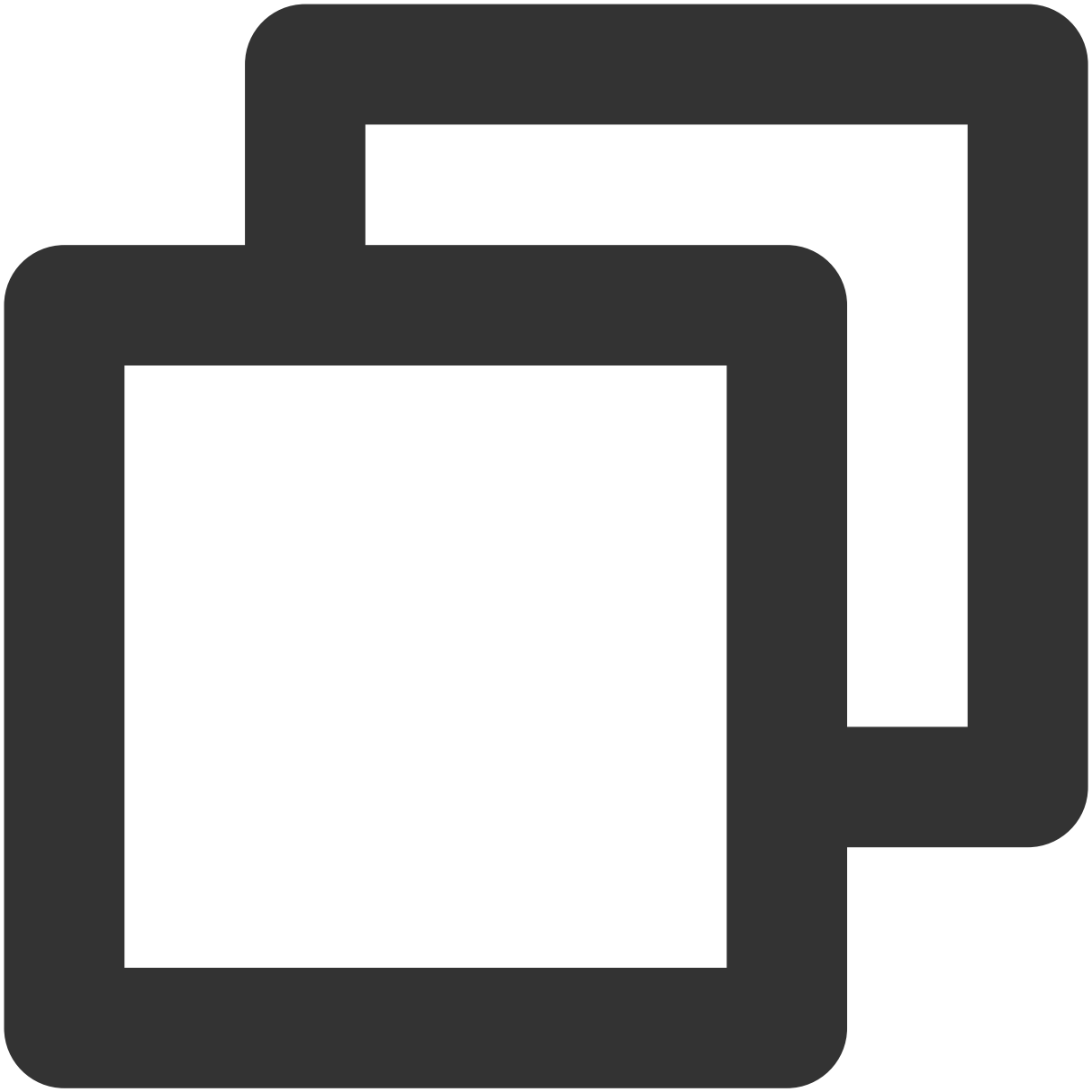
```
wget https://github.com/rabbitmq/rabbitmq-server/releases/download/rabbitmq_v3_6_9/
```

ここでは、RabbitMQバージョン3.6.9を例として取り上げ、また、RabbitMQの公式ウェブサイトから提供されているダウンロードアドレスを使用します。ダウンロードリンクが機能していない場合、またはRabbitMQの別のバージョンが必要な場合は、rabbitmq-serverにアクセスしてインストール情報を取得してください。
2. 次のコマンドを実行して、署名キーをインポートします。

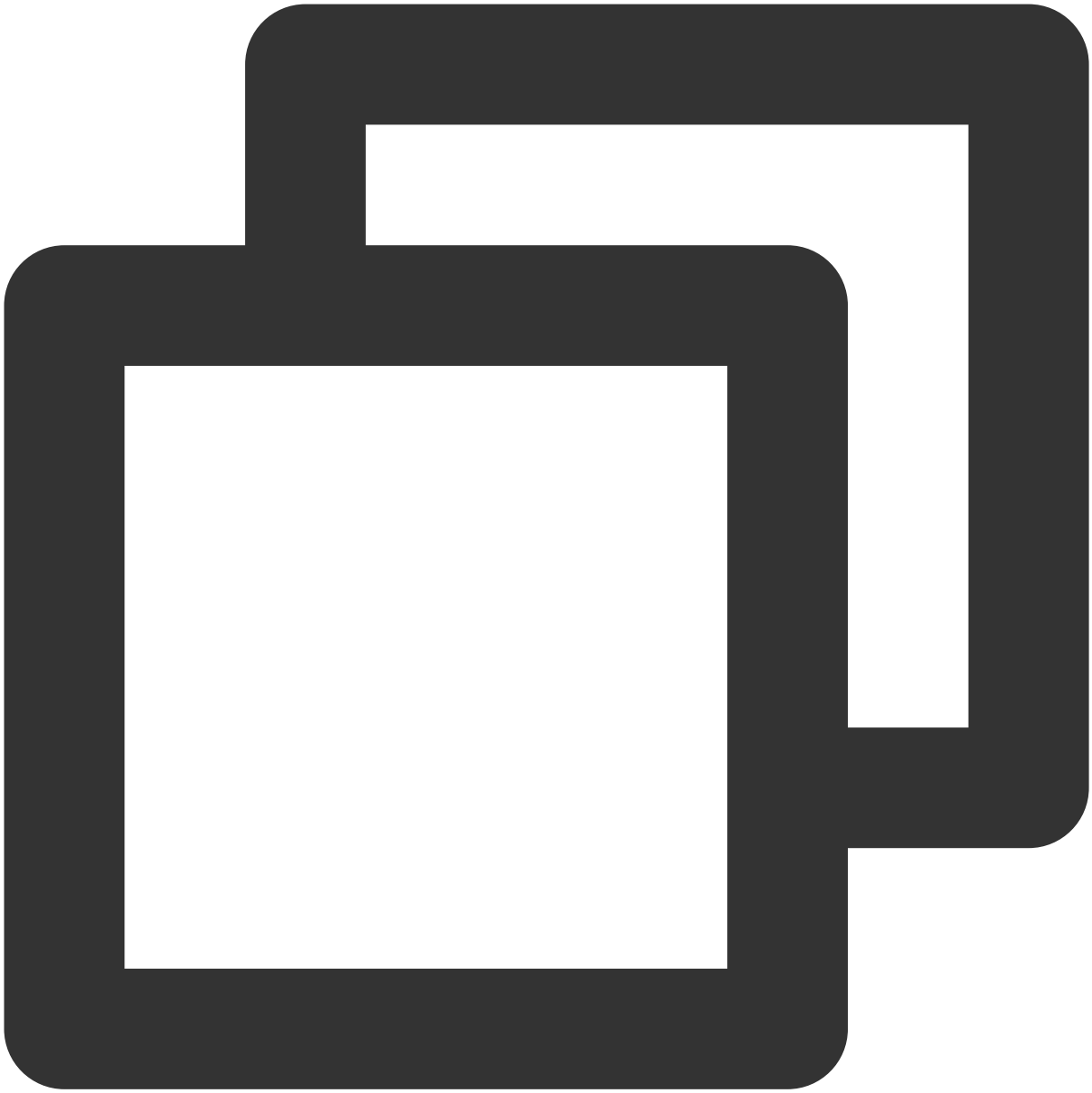


```
rpm --import https://www.rabbitmq.com/rabbitmq-release-signing-key.asc
```

3. 次のコマンドを順次実行して、RabbitMQ Serverをインストールします。

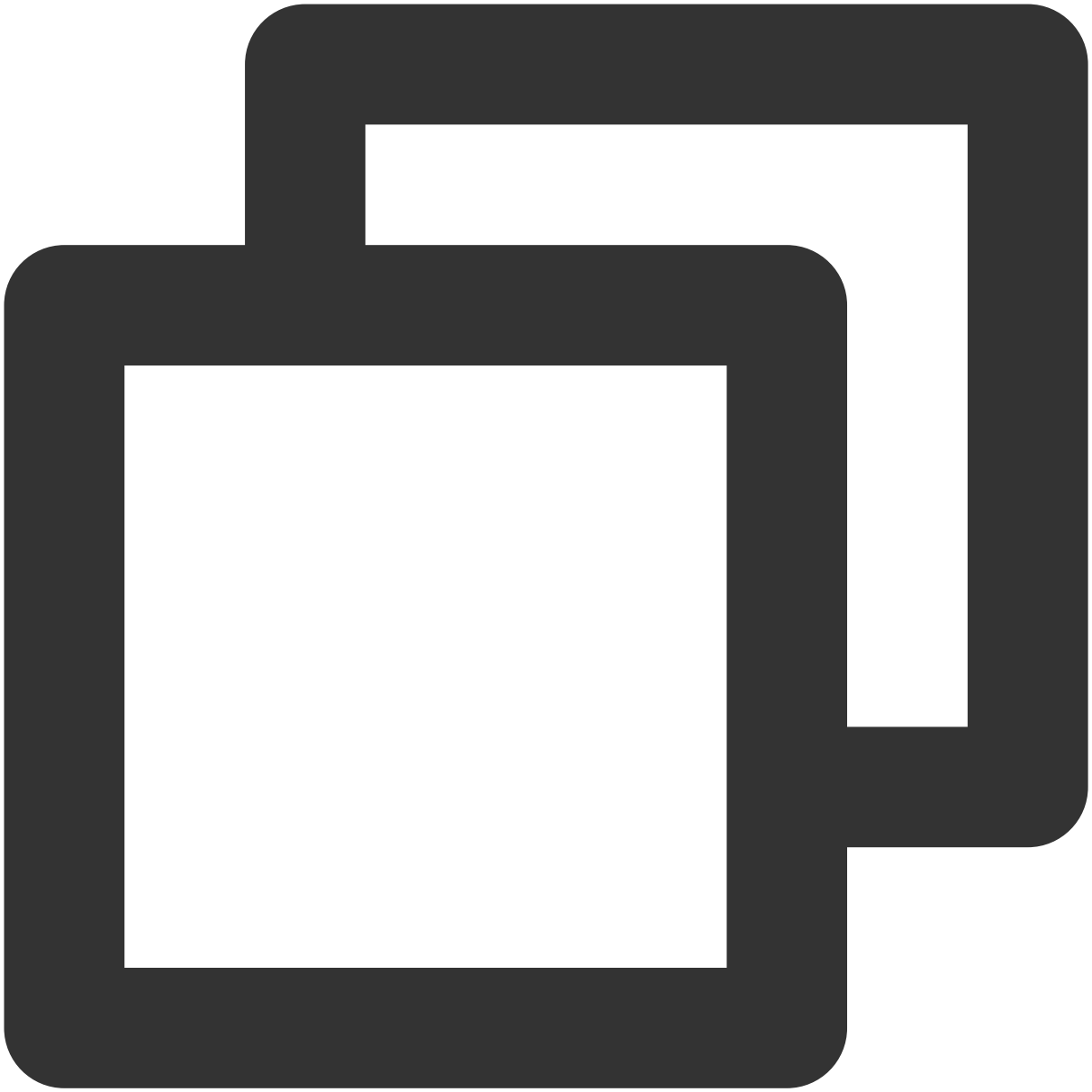


```
cd
```

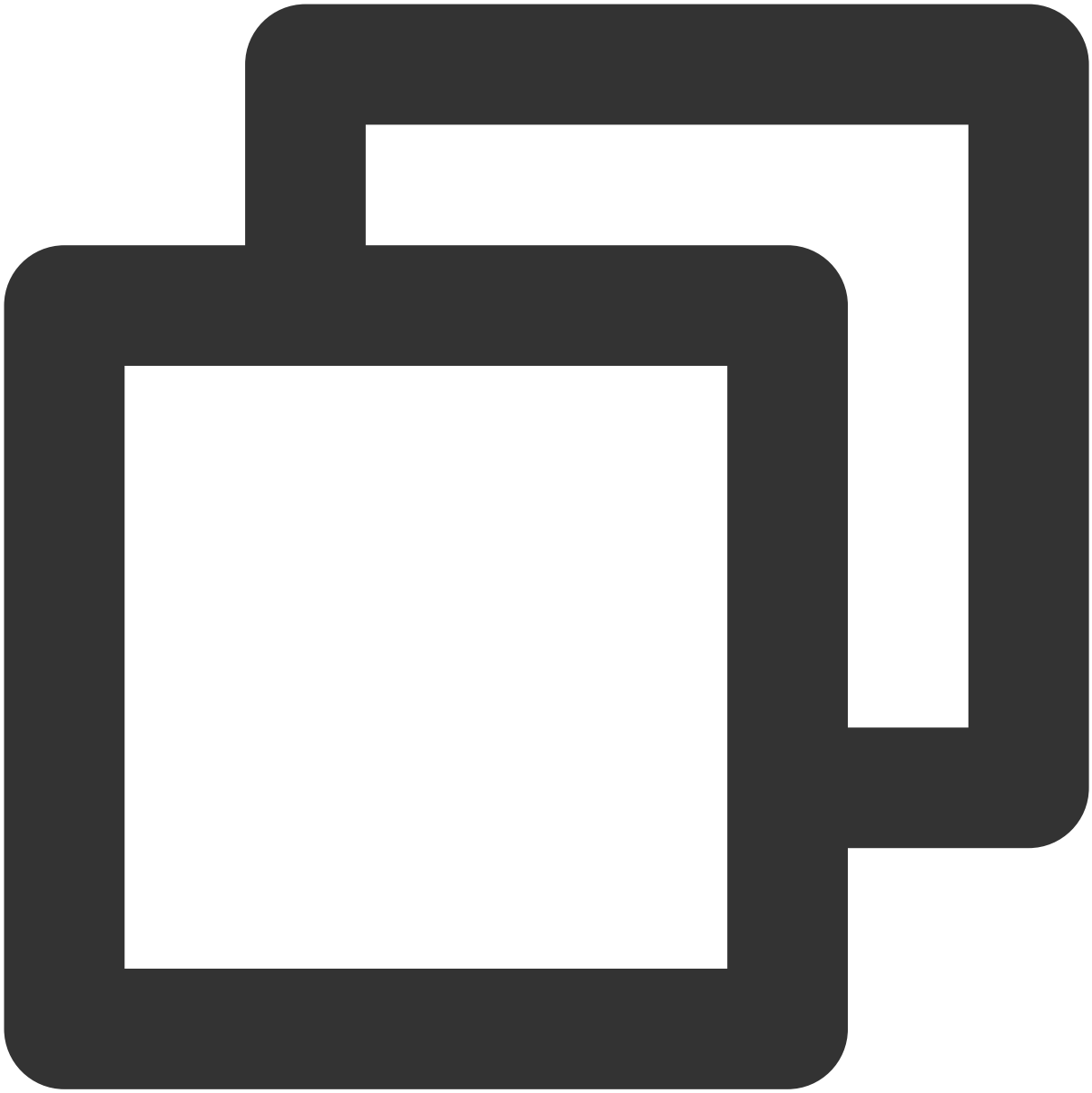


```
yum install rabbitmq-server-3.6.9-1.el7.noarch.rpm
```

4. 次のコマンドを順次実行して、RabbitMQの自動起動を設定してRabbitMQを起動します。

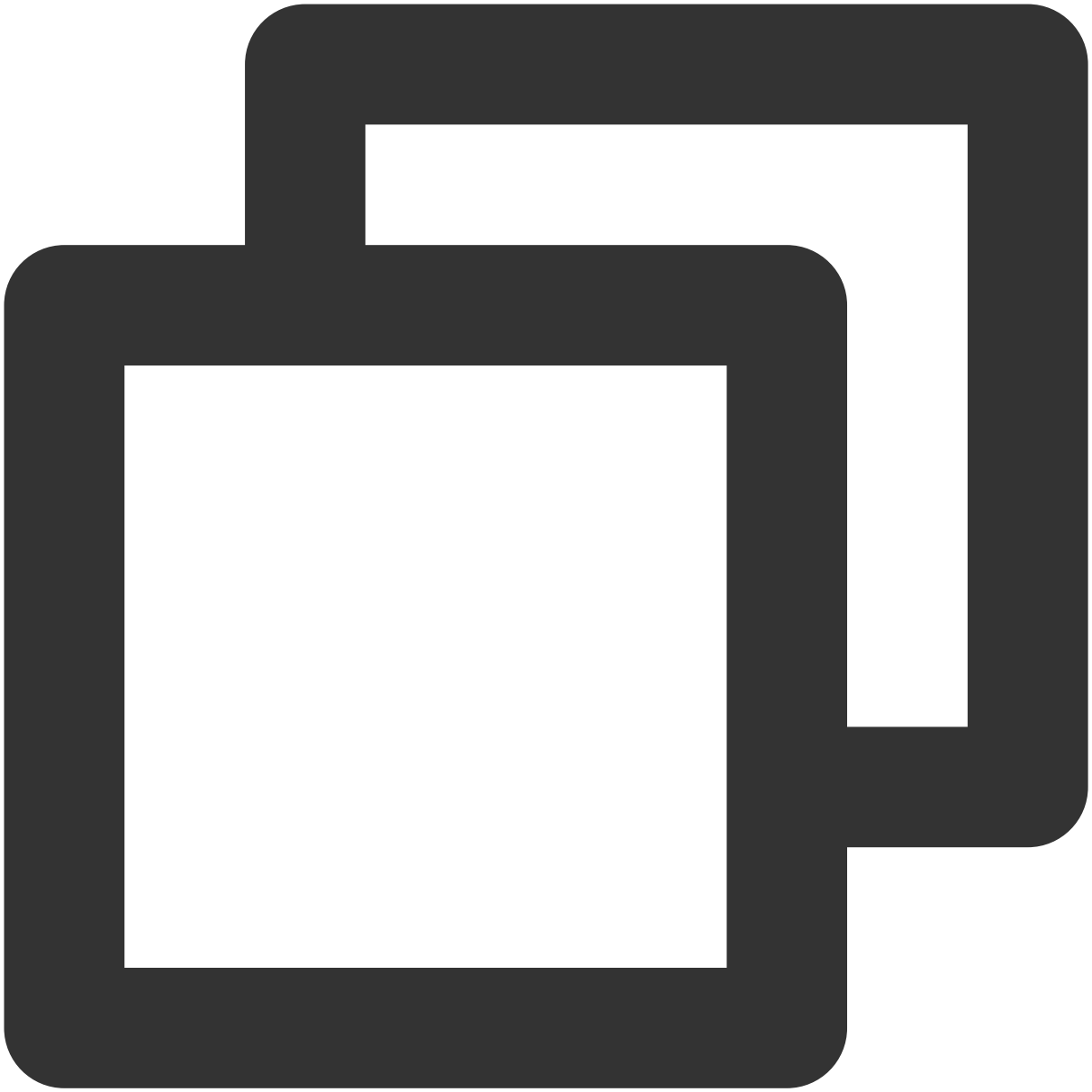


```
systemctl enable rabbitmq-server
```



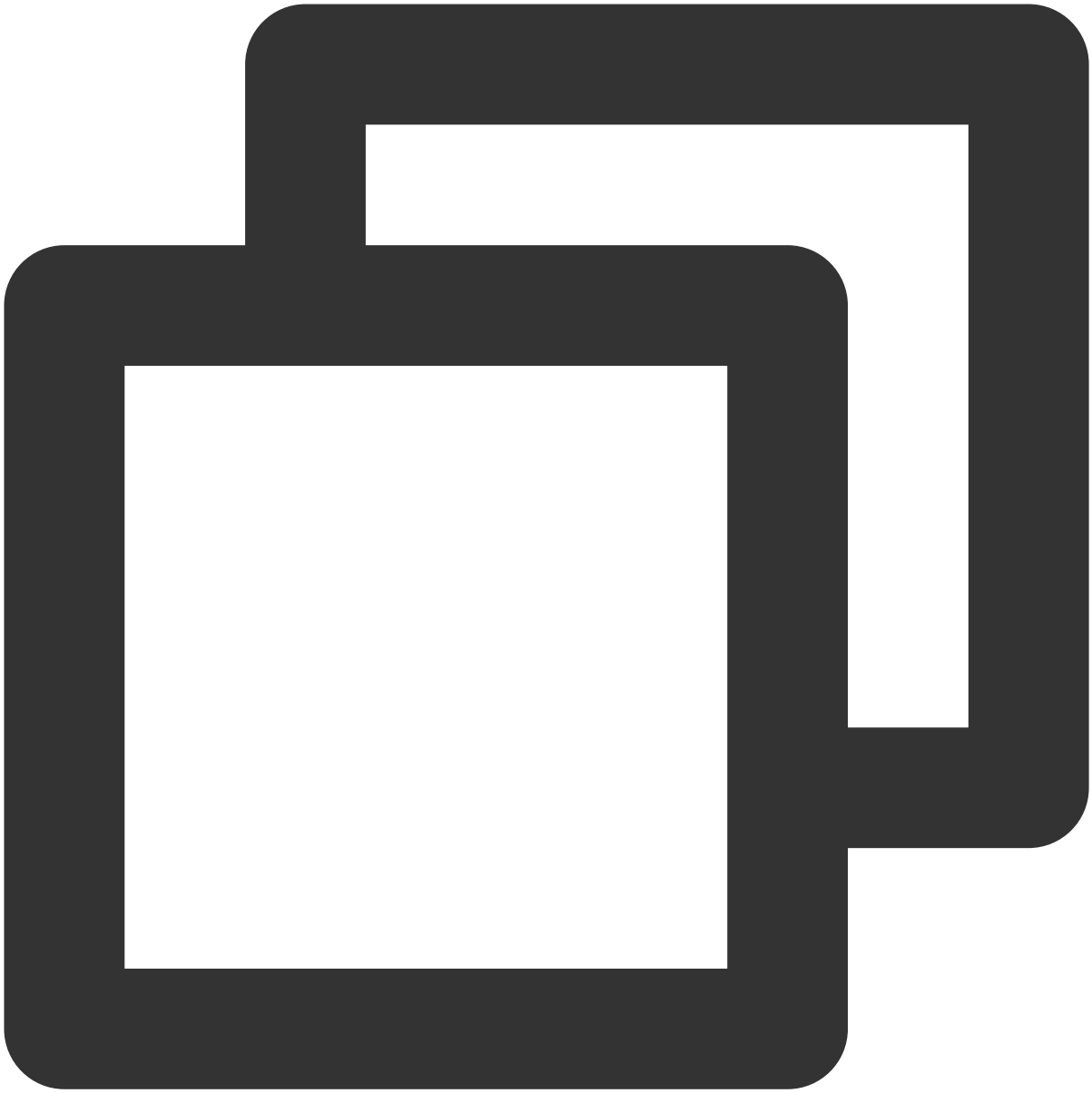
```
systemctl start rabbitmq-server
```

5. 次のコマンドを実行して、RabbitMQのデフォルトのguestアカウントを削除します。



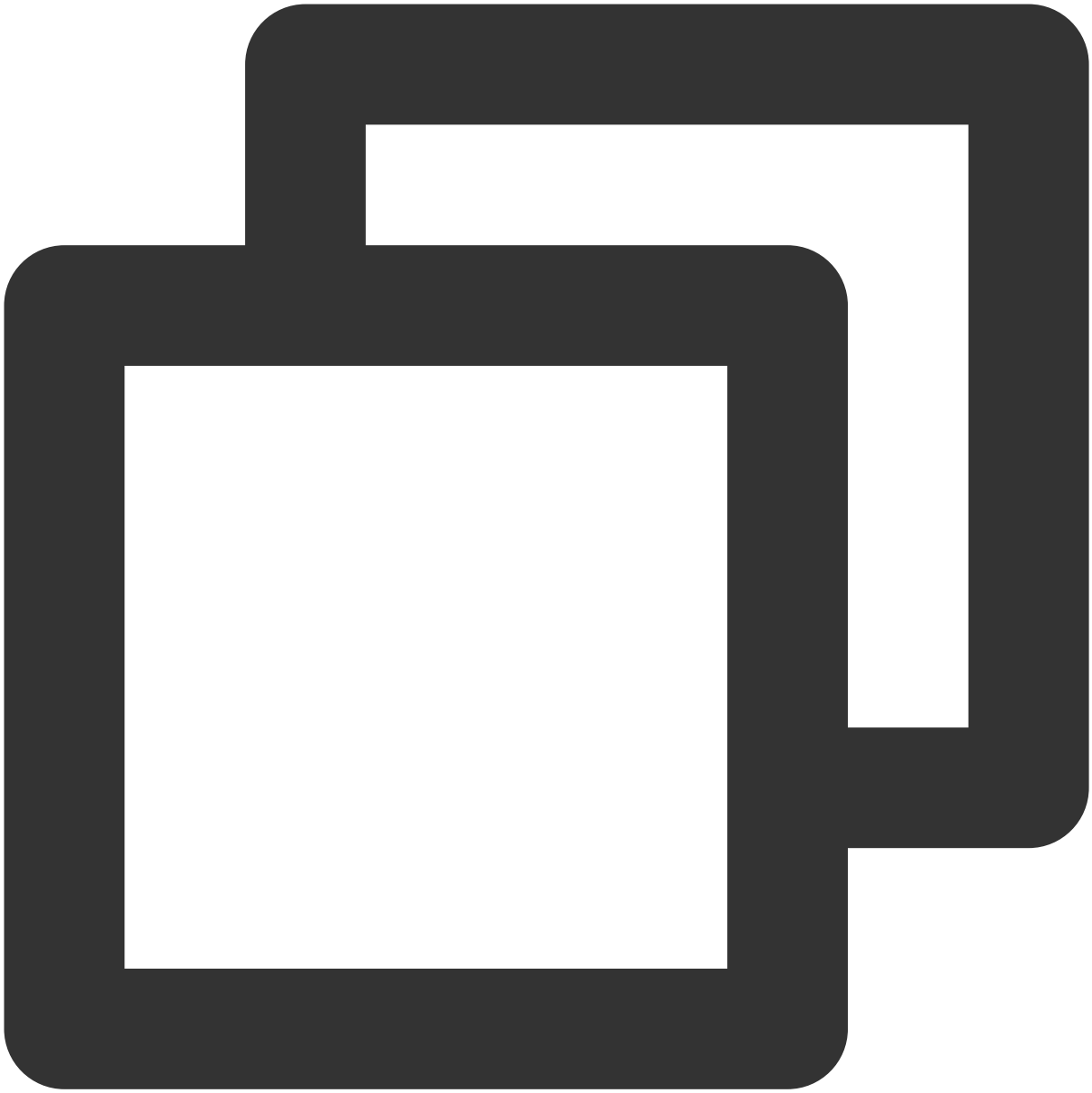
```
rabbitmqctl delete_user guest
```

6.
次のコマンドを実行して、新しいユーザーを作成します。



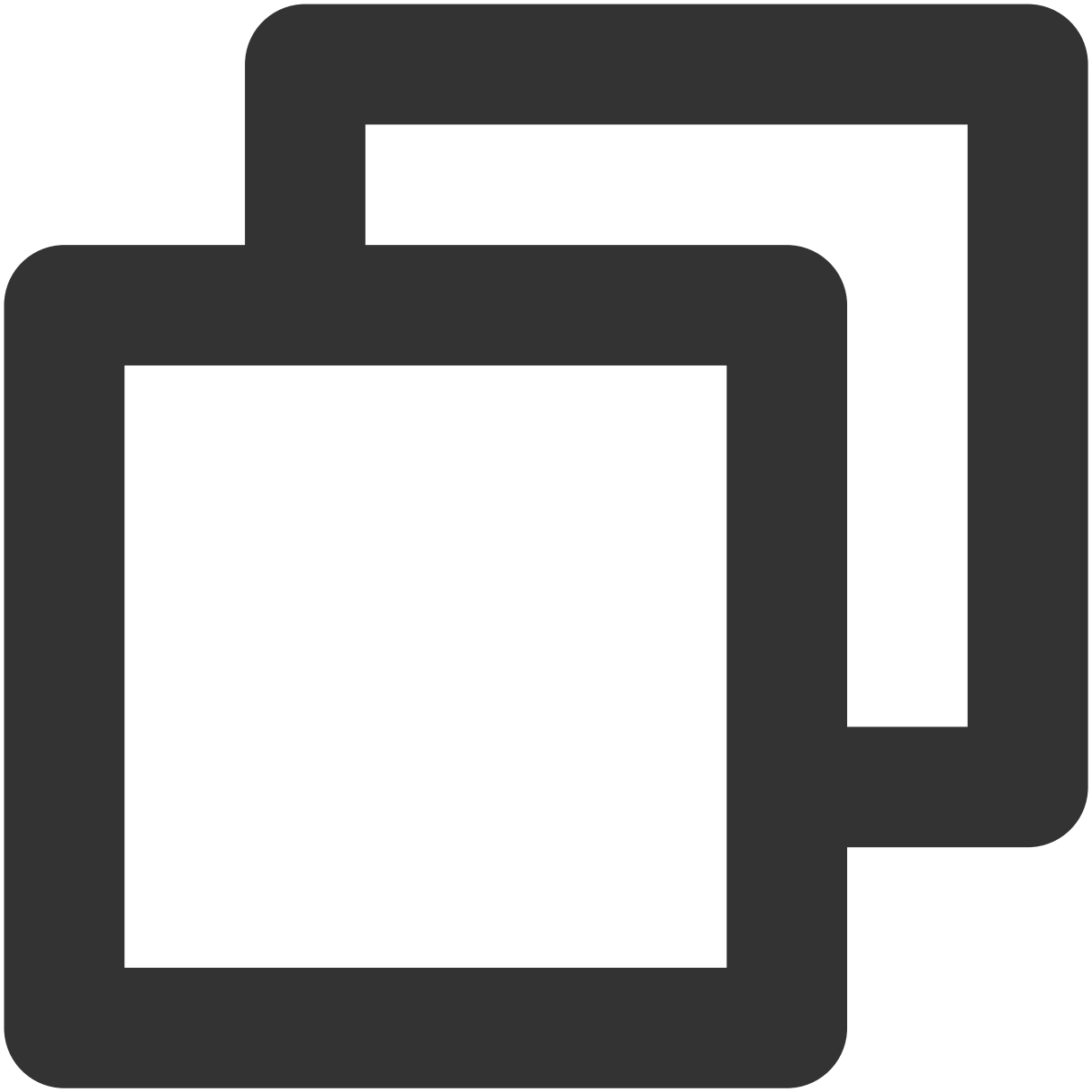
```
rabbitmqctl add_user ユーザー名 パスワード
```

7. 次のコマンドを実行して、新しいアカウントを管理者アカウントとして設定します。



```
rabbitmqctl set_user_tags ユーザー名 administrator
```

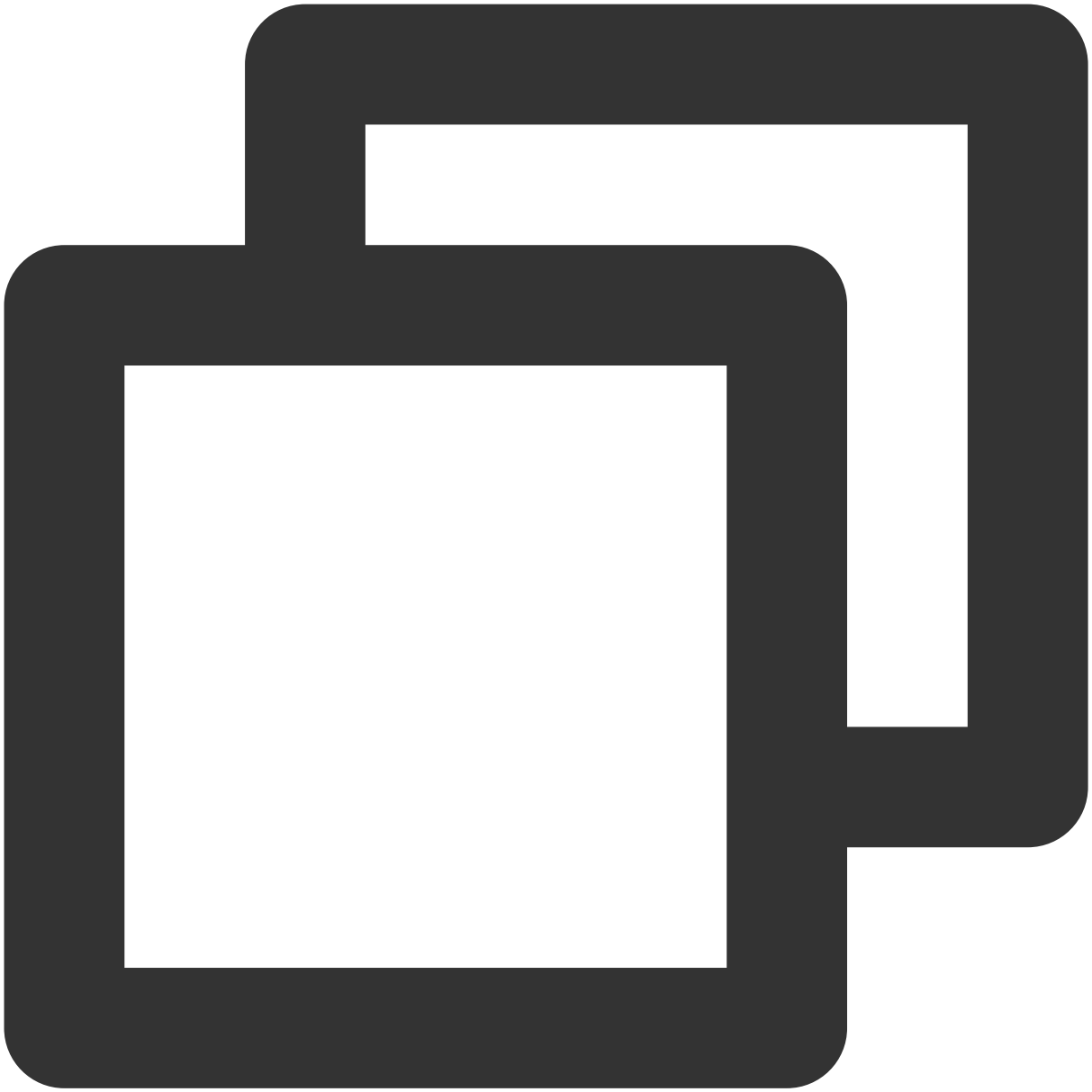
8. 次のコマンドを実行して、管理者アカウントにすべての権限を付与します。



```
rabbitmqctl set_permissions -p / ユーザー名 ".*" ".*" ".*"
```

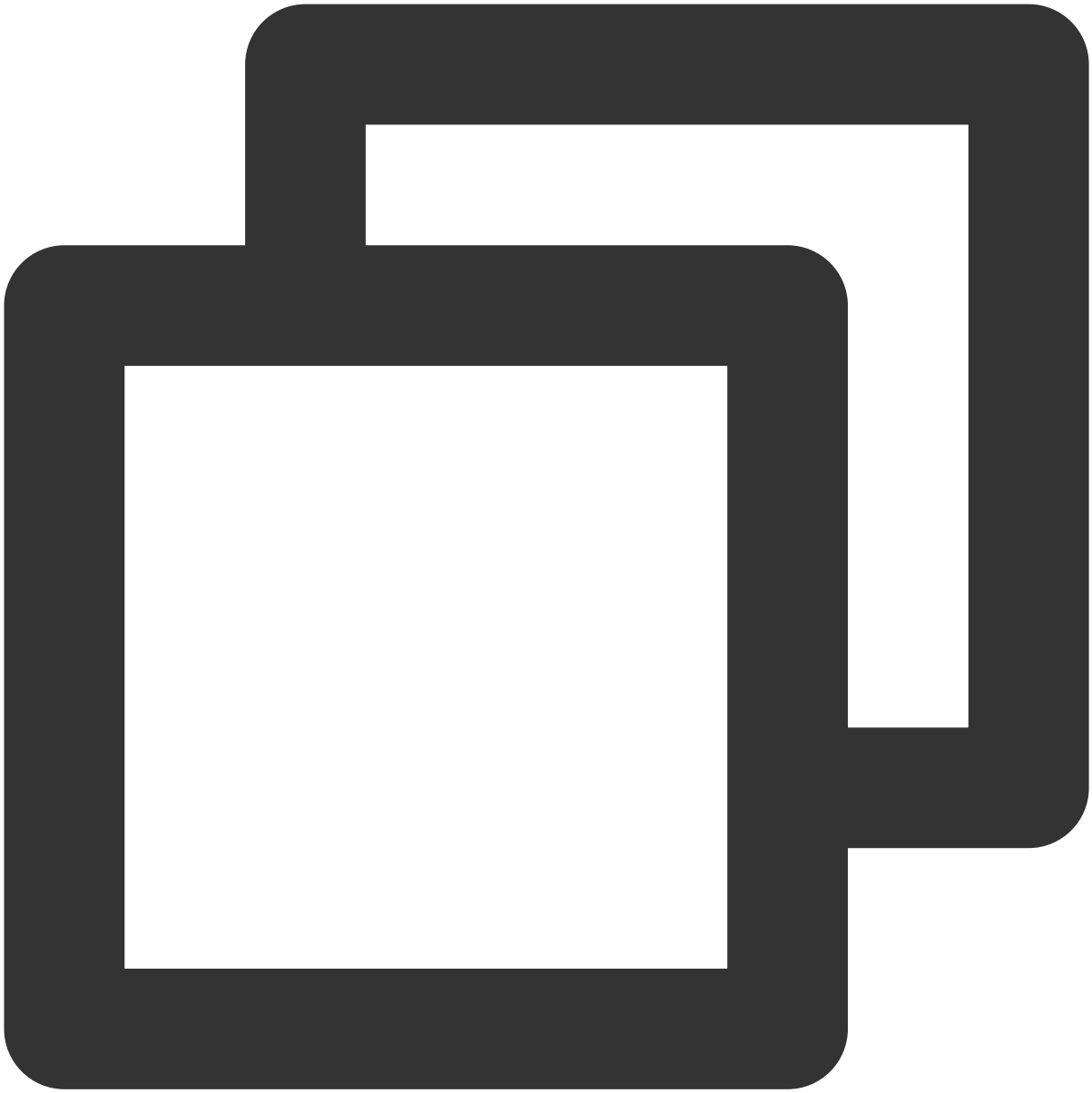
インストールの検証

1. 次のコマンドを実行して、RabbitMQのWeb管理画面を開きます。



```
rabbitmq-plugins enable rabbitmq_management
```

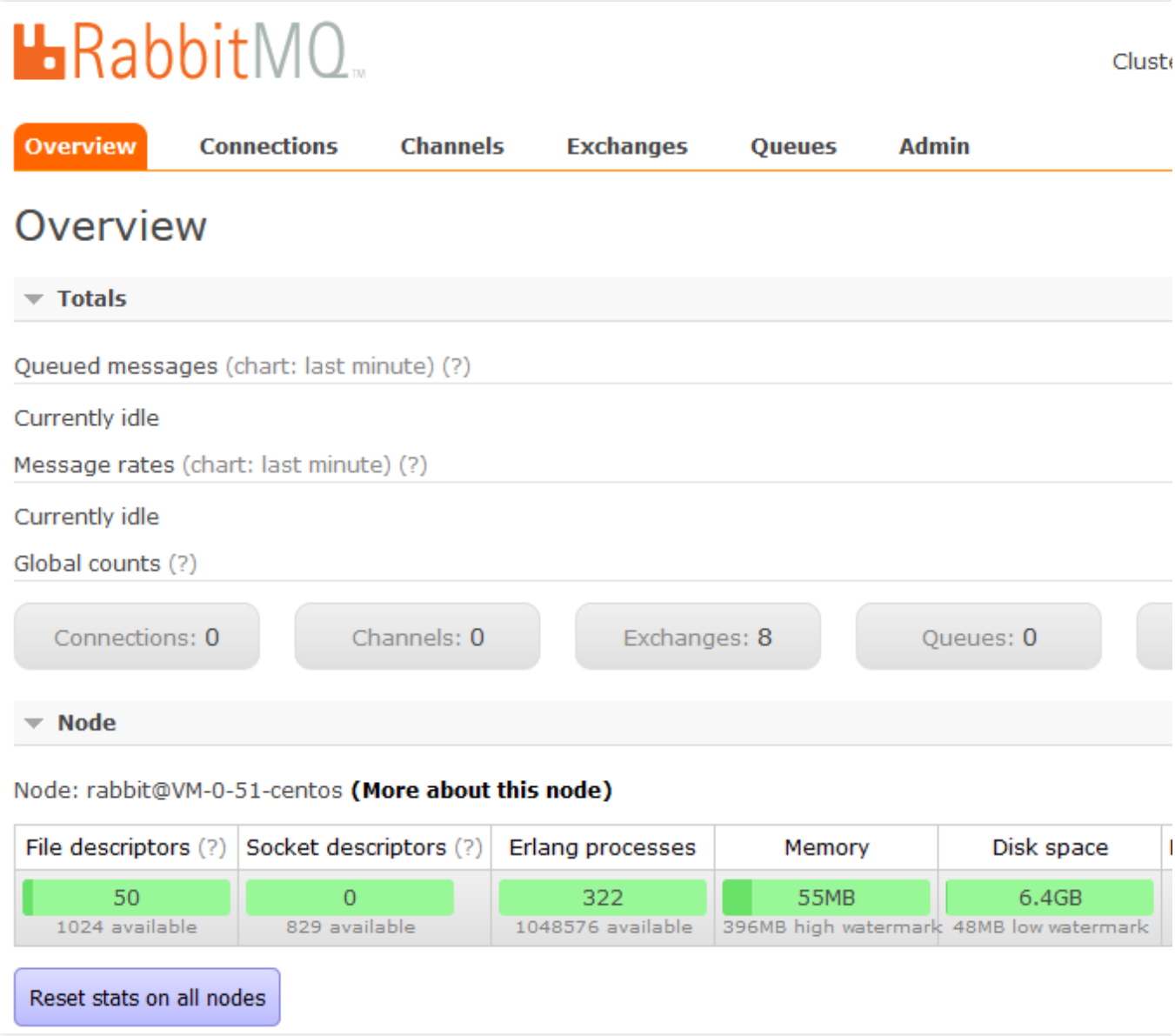
2. ブラウザーを開いて、以下のアドレスにアクセスします。



```
http://インスタンスのパブリックIPアドレス:15672
```

インスタンスのパブリックIPアドレスを取得する方法の詳細については、パブリックIPアドレスの取得 をご参照ください。
次のように表示画面が表示されると、RabbitMQ Serverのインストールに成功したことを意味します。

3. ステップ6 で作成した管理者ユーザーを使用してログインし、RabbitMQ管理インターフェースに入ります。下図のとおりです。



ビジュアルインターフェイスを作成 Ubuntuビジュアルインターフェースの構築

最終更新日：：2023-06-30 15:28:14

概要

仮想ネットワークコンソール (VNC) はAT&T ケンブリッジ研究所によって開発されたリモートコントロールソフトウェアです。UNIX および Linux OSをベースとしたオープンソースソフトウェアであるVNC は、リモートコントロール機能が高く、効率的かつ実用的で、その機能はWindowsおよびMACのどのリモートコントロールソフトウェアより優れています。このドキュメントでは、Ubuntu OSを搭載した CVMインスタンスでビジュアルインターフェースを構築する方法を説明します。

前提条件

Ubuntu OSを搭載した Linux インスタンスを購入しました。

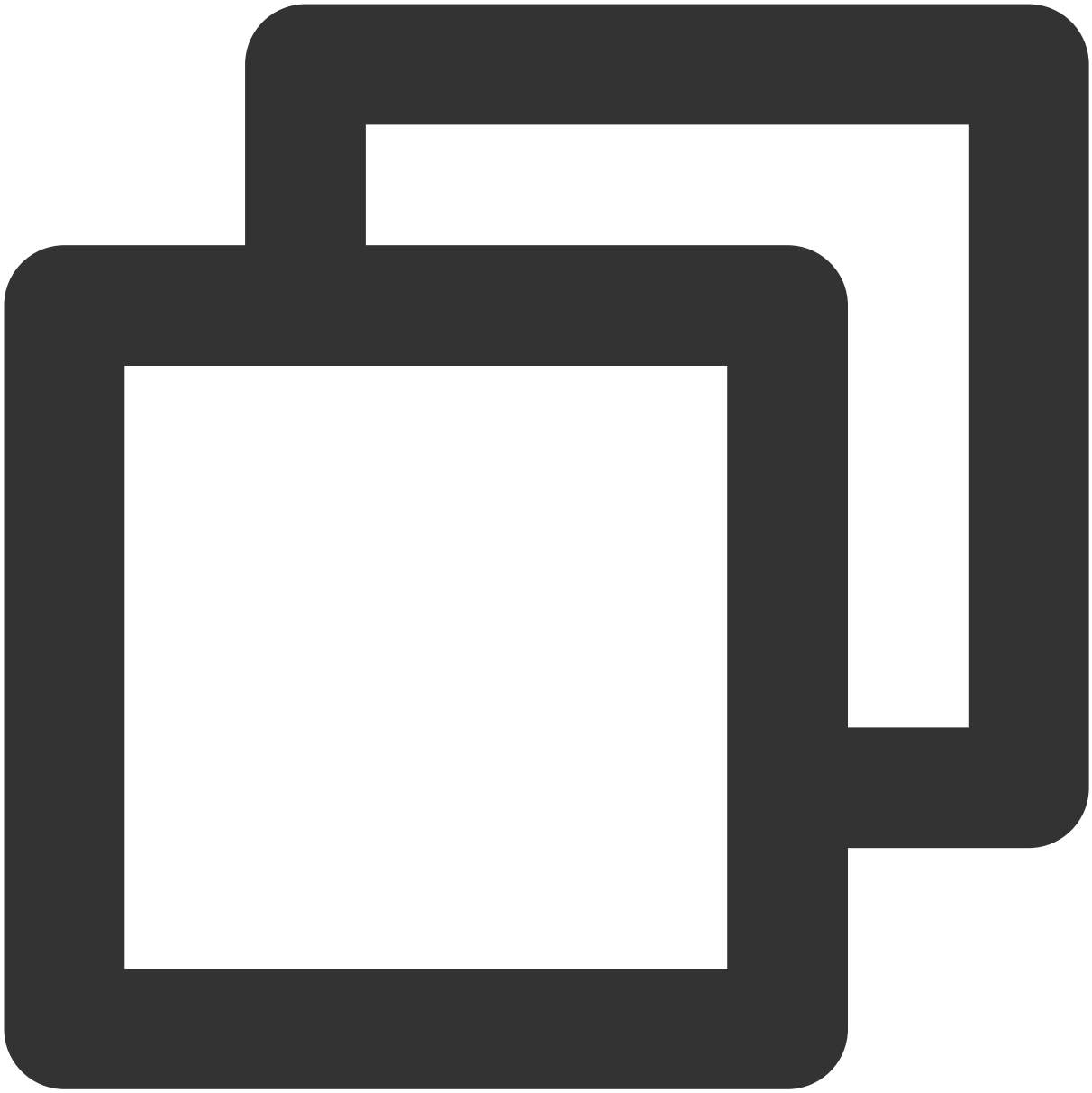
操作手順

インスタンスセキュリティグループの設定

VNCサービスは、デフォルトで TCPプロトコルとポート5901 を使用します。インスタンスに関連付けられているセキュリティグループでポート5901を開く必要があり、即ち、「インバウンドルール」にプロトコルポートTCP:5901を開くためのルールを追加する必要があります。具体的な操作については、セキュリティグループルールの追加 をご参照ください。

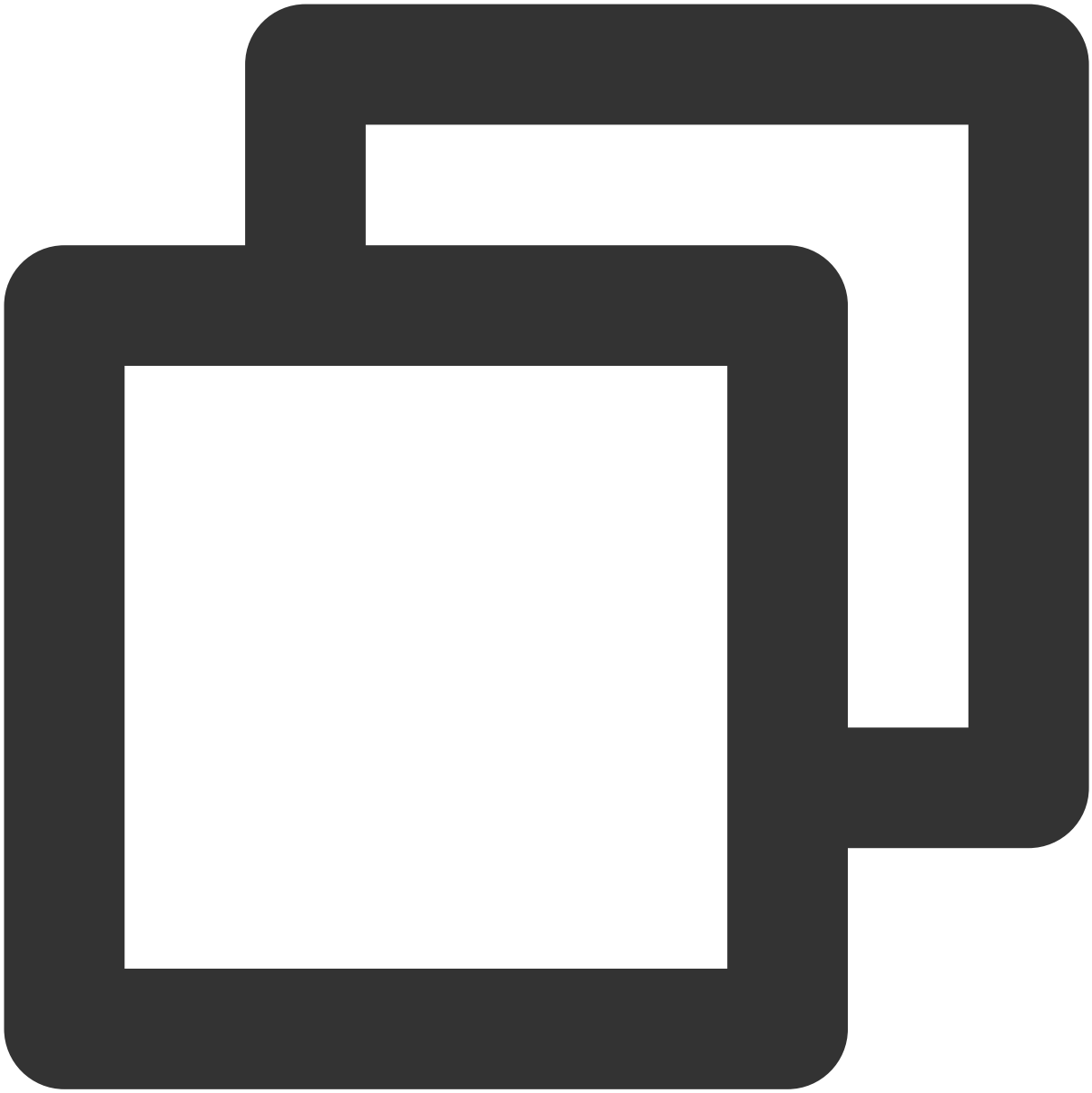
ソフトウェアパッケージのインストール

Ubuntu 18.04
Ubuntu 20.04
Ubuntu 22.04
1. 標準ログイン方式を使用してLinuxインスタンスにログインする（推奨）。
2. 次のコマンドを実行してキャッシュをクリアし、ソフトウェアパッケージリストを更新します。



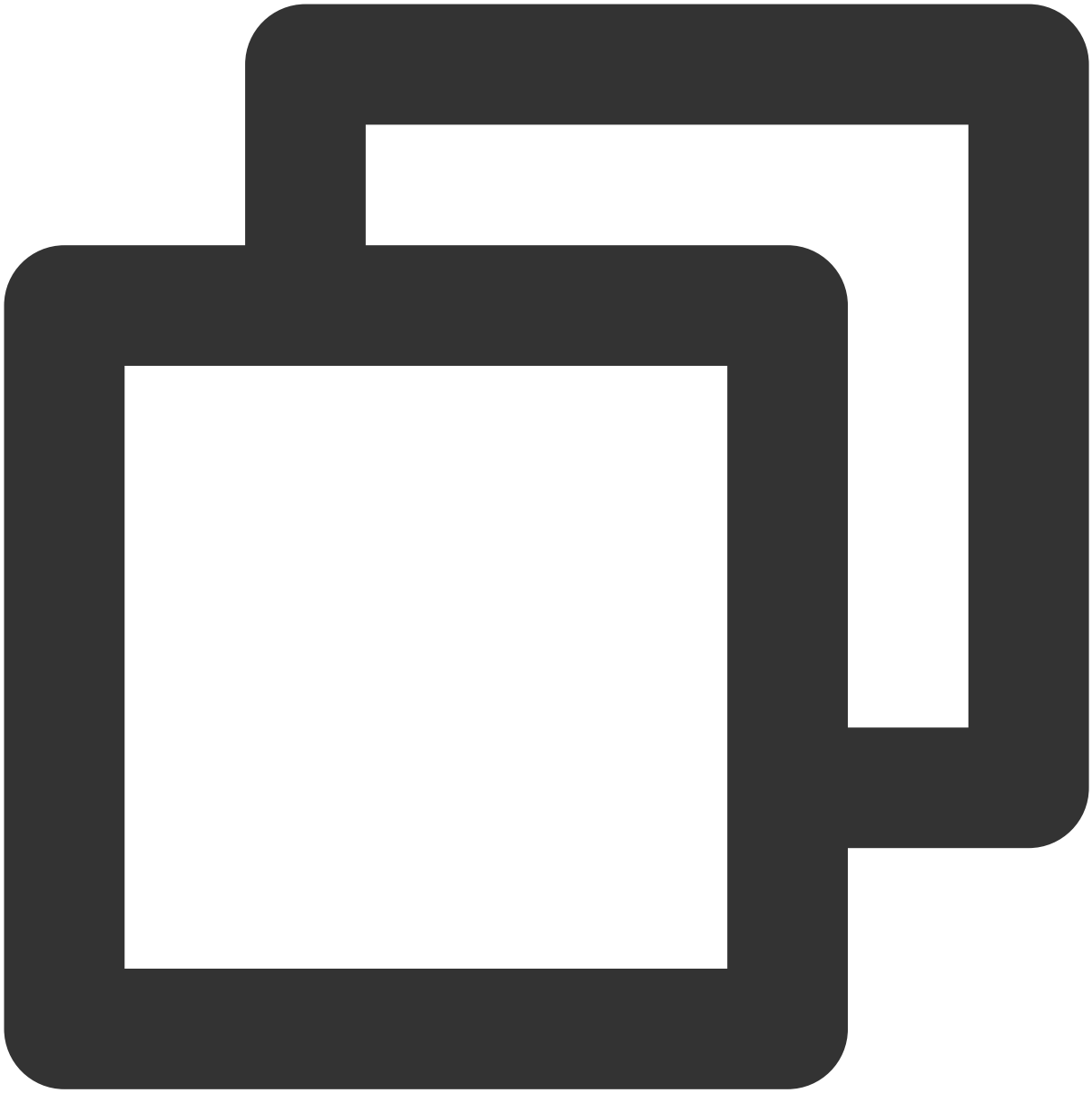
```
sudo apt clean all && sudo apt update
```

3. 次のコマンドを実行して、デスクトップ環境に必要なソフトウェアパッケージをインストールします。これにはシステムパネル、ウィンドウマネージャー、ファイルブラウザ、端末などのデスクトップアプリケーションプログラムが含まれます。



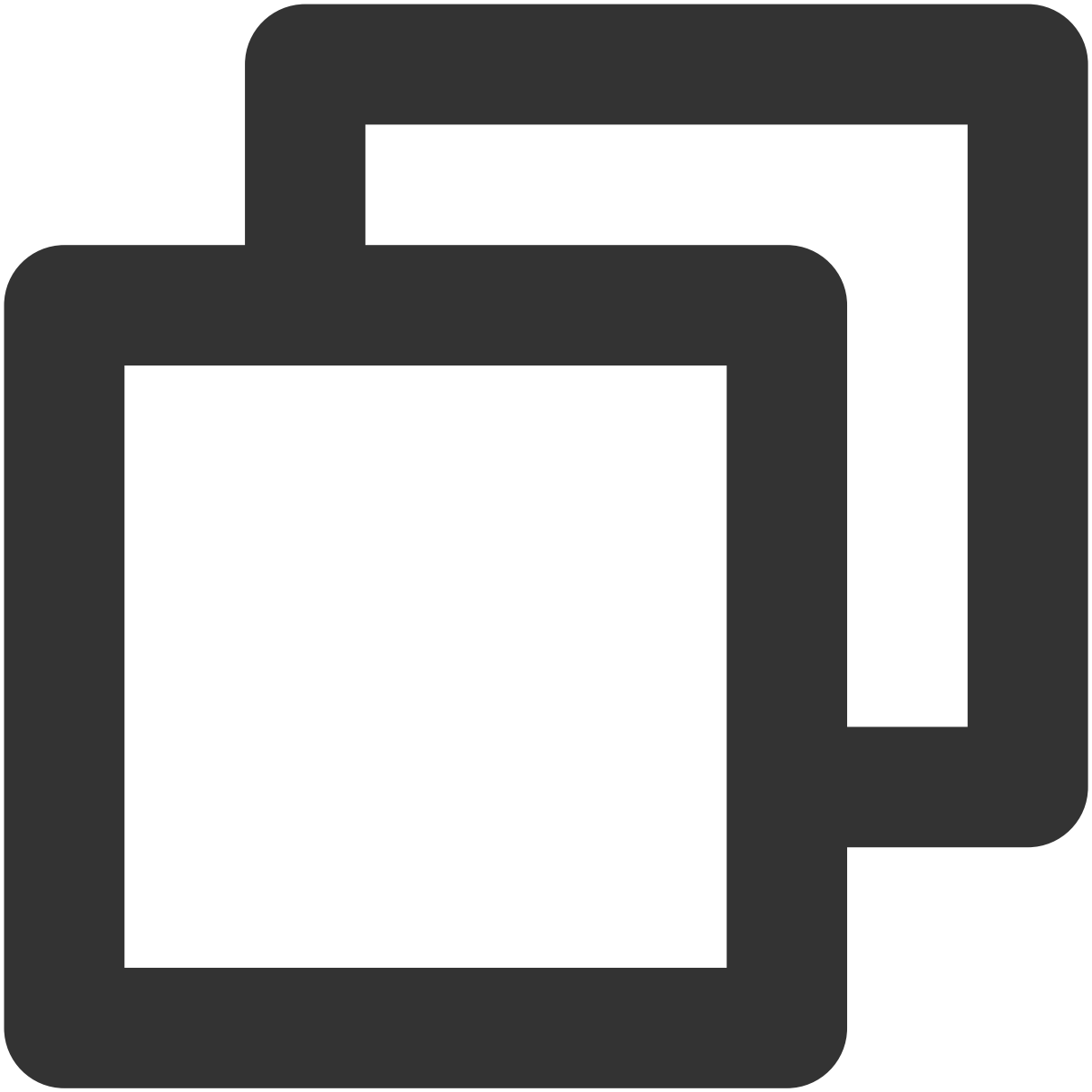
```
sudo apt install gnome-panel gnome-settings-daemon metacity nautilus gnome-terminal
```

4. 次のコマンドを実行して VNC をインストールします。



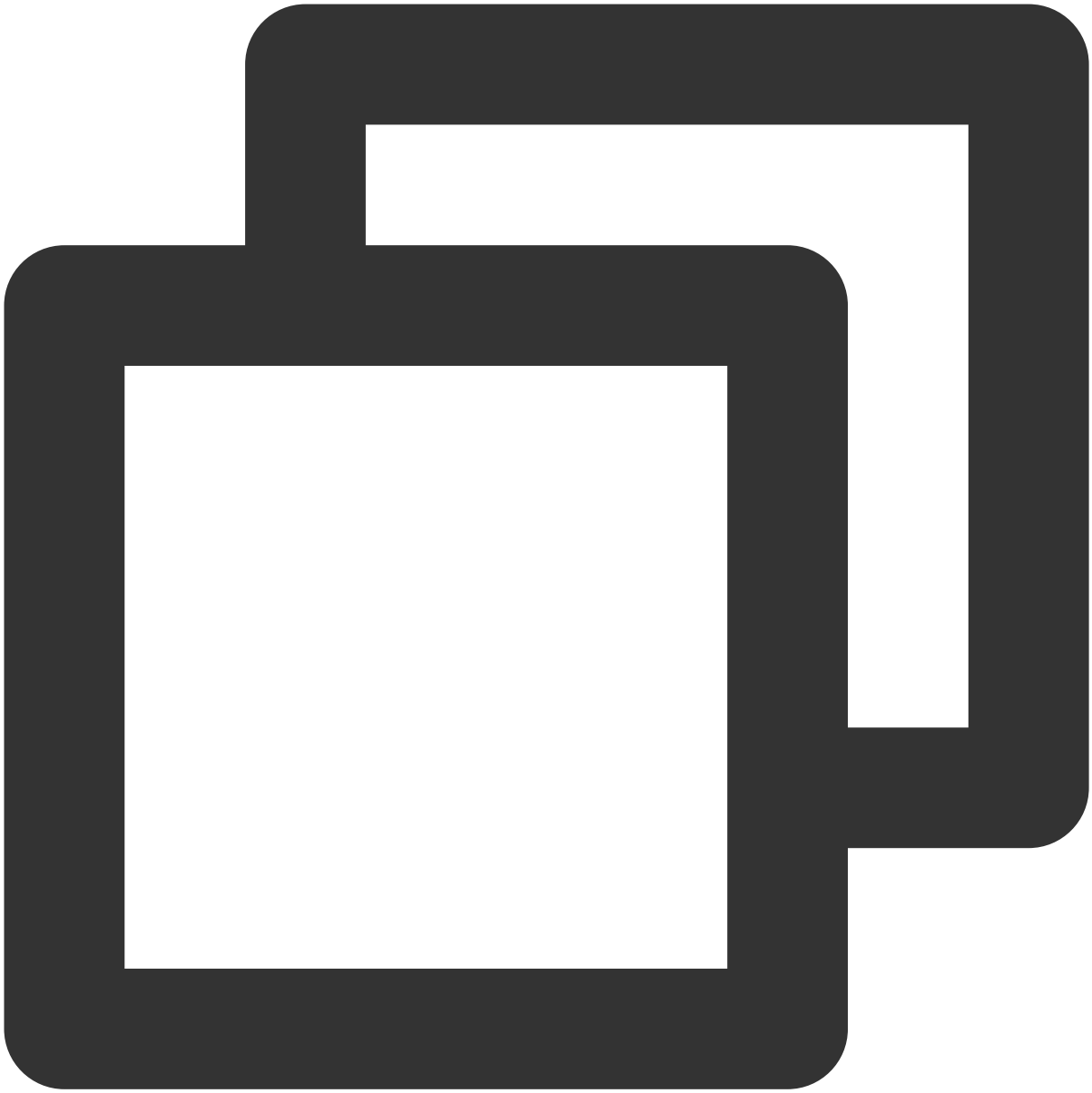
```
apt-get install vnc4server
```

1. 標準ログイン方式を使用してLinuxインスタンスにログインする（推奨）。
2. 次のコマンドを実行してキャッシュをクリアし、ソフトウェアパッケージリストを更新します。



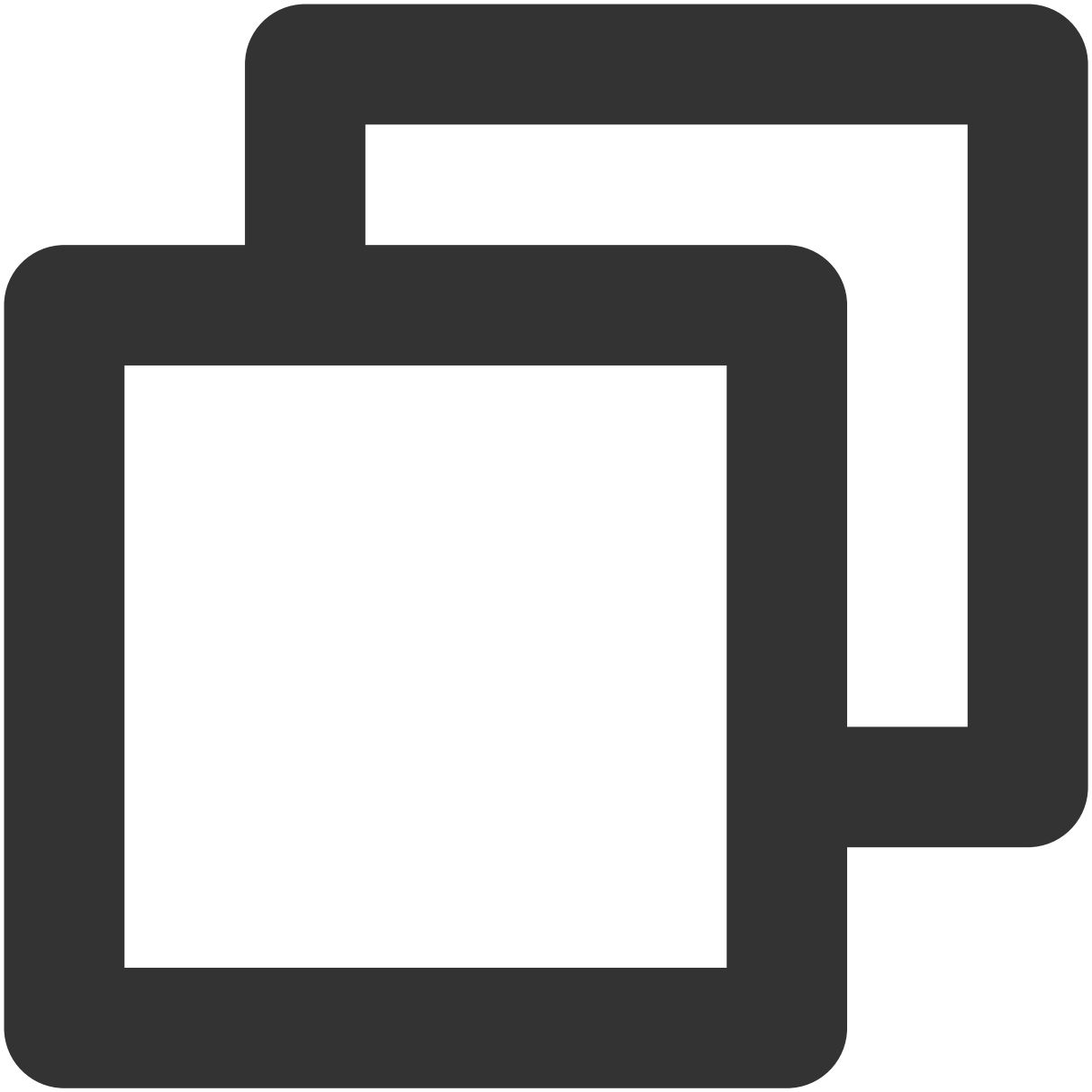
```
sudo apt clean all && sudo apt update
```

3. 次のコマンドを実行して、デスクトップ環境に必要なソフトウェアパッケージをインストールします。これにはシステムパネル、ウィンドウマネージャー、ファイルブラウザ、端末などのデスクトップアプリケーションプログラムが含まれます。



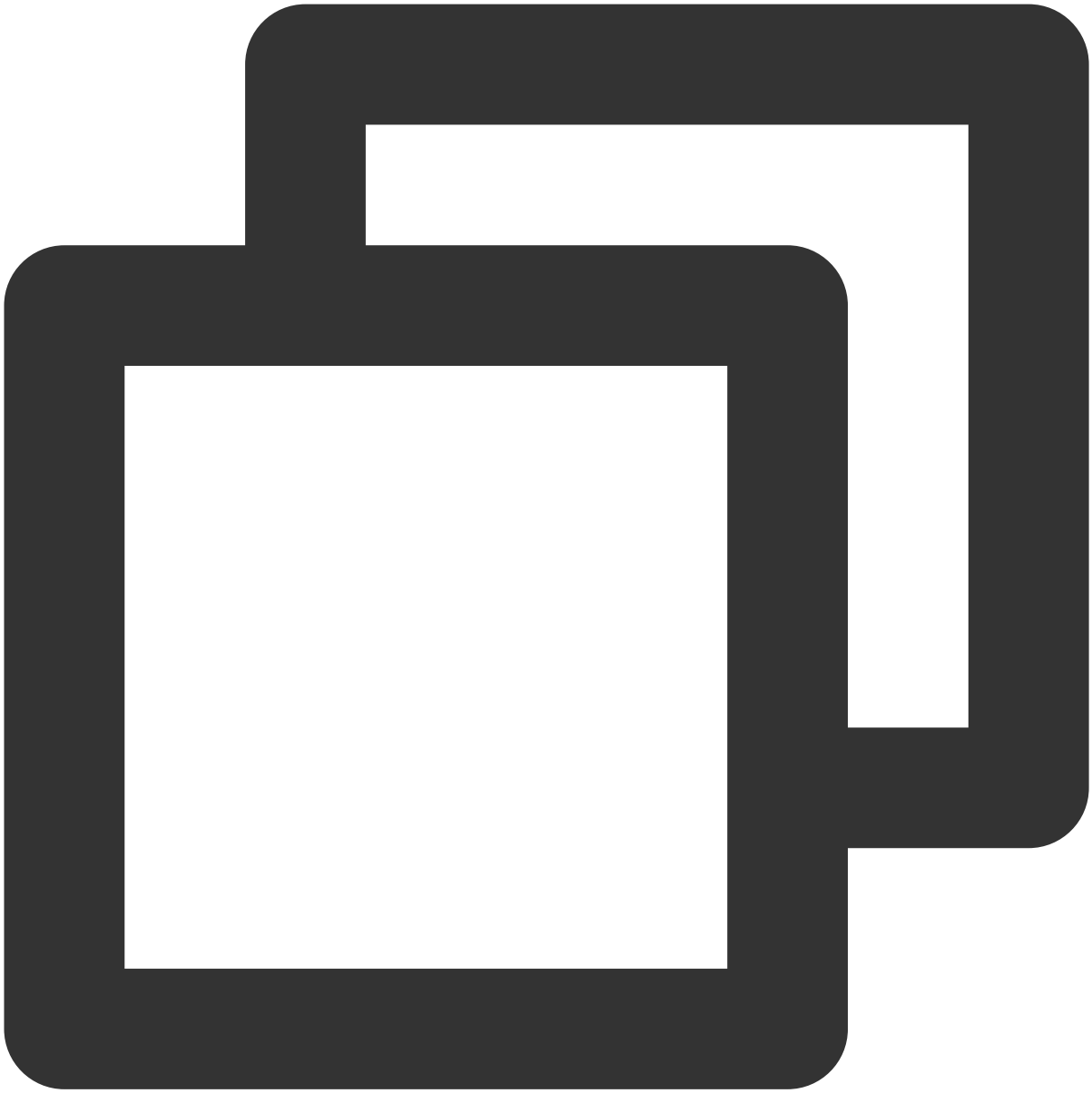
```
sudo apt install gnome-panel gnome-settings-daemon metacity nautilus gnome-terminal
```

4. 次のコマンドを実行して VNC をインストールします。



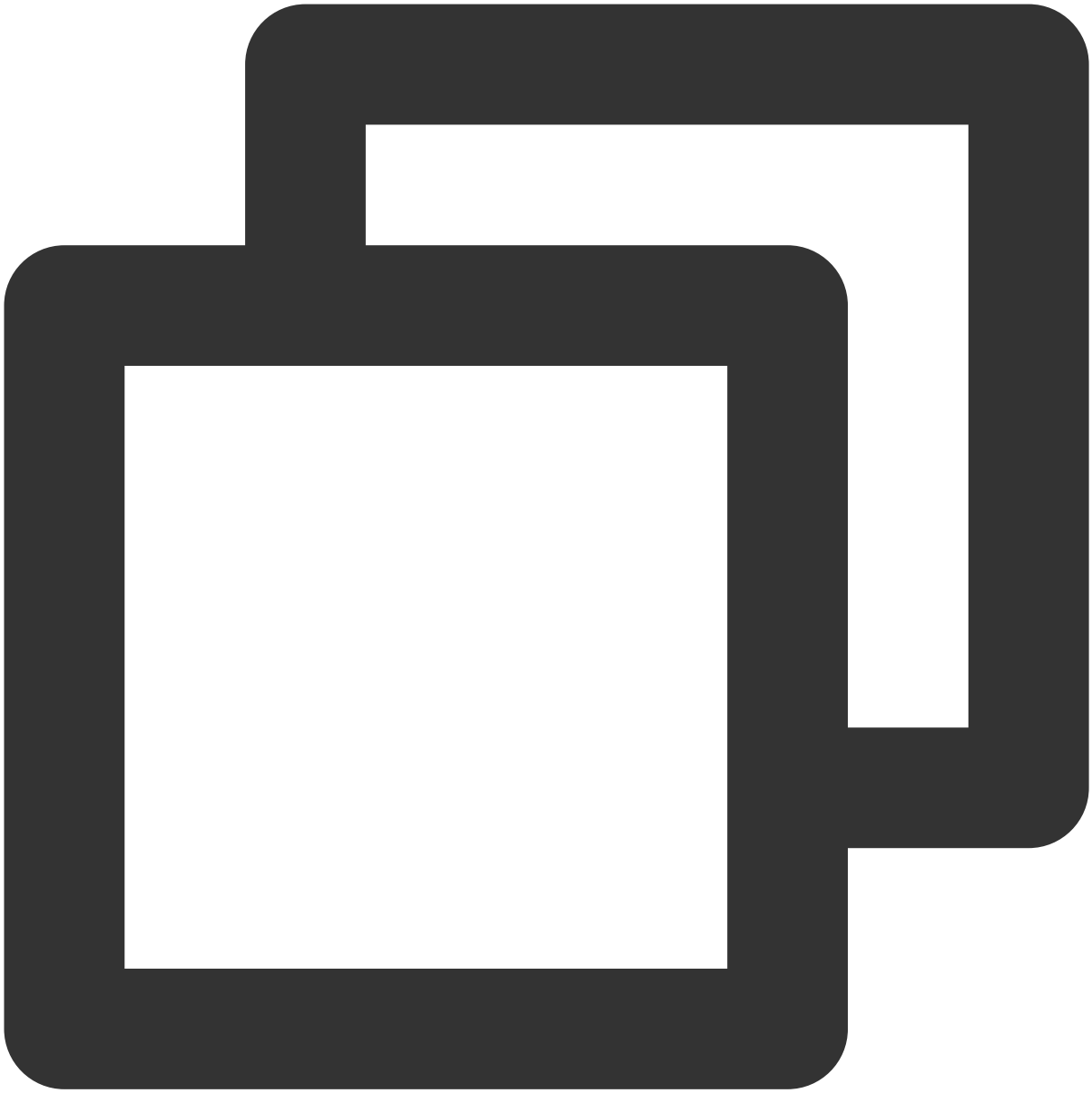
```
apt-get install tightvncserver
```

1. 標準ログイン方式を使用してLinuxインスタンスにログインする（推奨）。
2. キャッシュをクリアし、ソフトウェアパッケージリストを更新します。



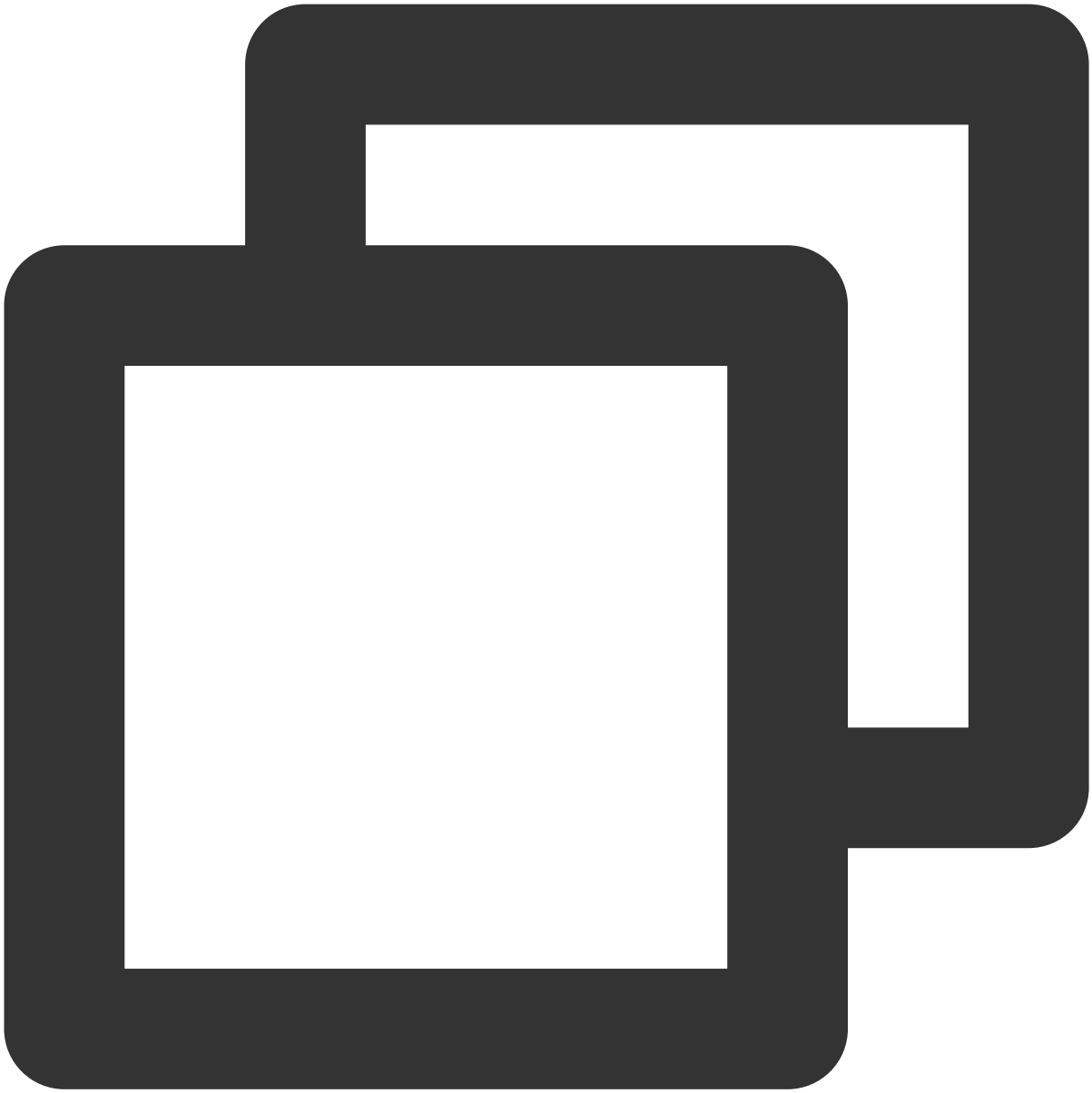
```
sudo apt clean all && sudo apt update
```

3. デスクトップ環境をインストールします。



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

4. 次のコマンドを実行して VNC をインストールします。



```
sudo apt install tightvncserver
```

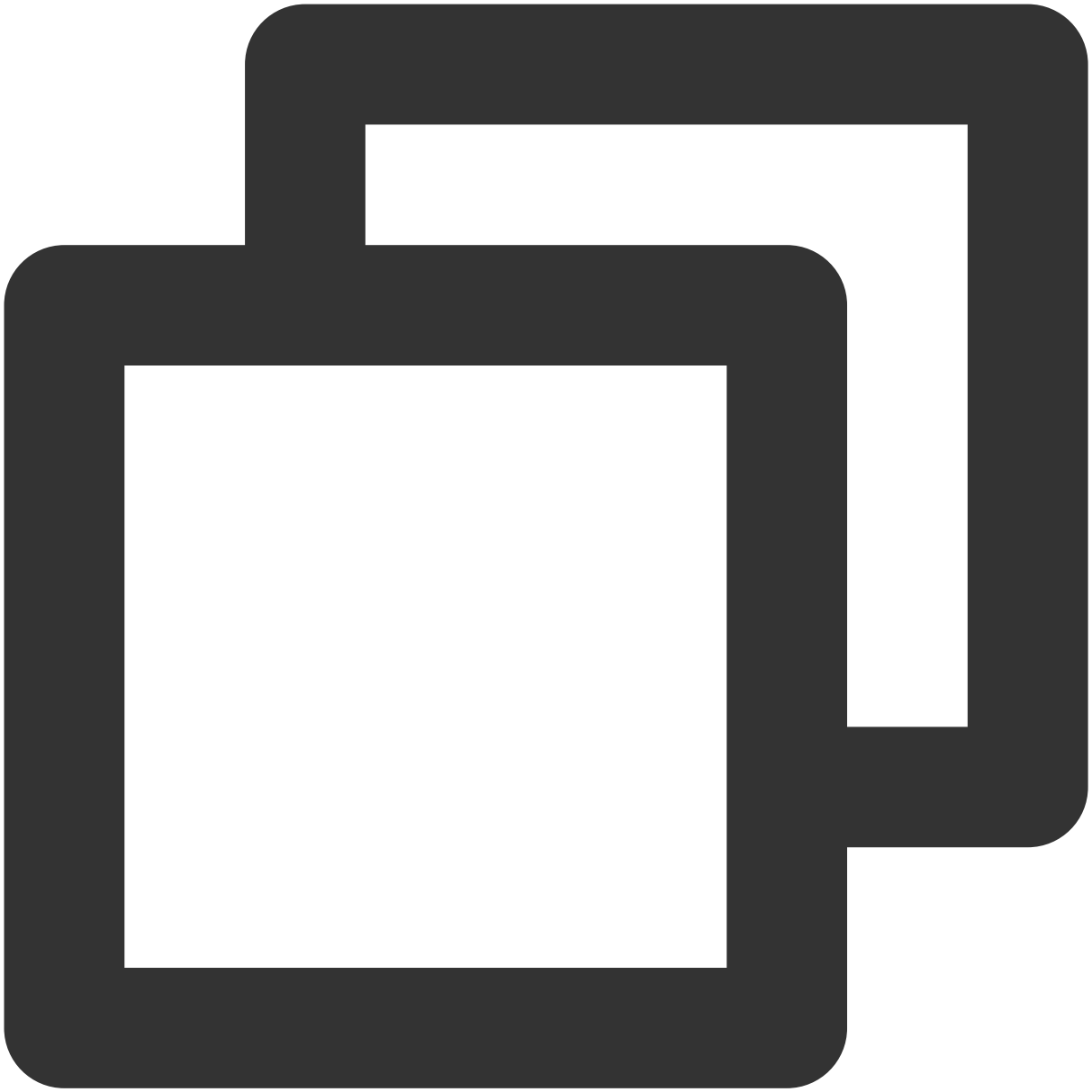
VNCの構成

Ubuntu 18.04

Ubuntu 20.04

Ubuntu 22.04

1. 次のコマンドを実行してVNCサービスを起動し、パスワードを設定します。

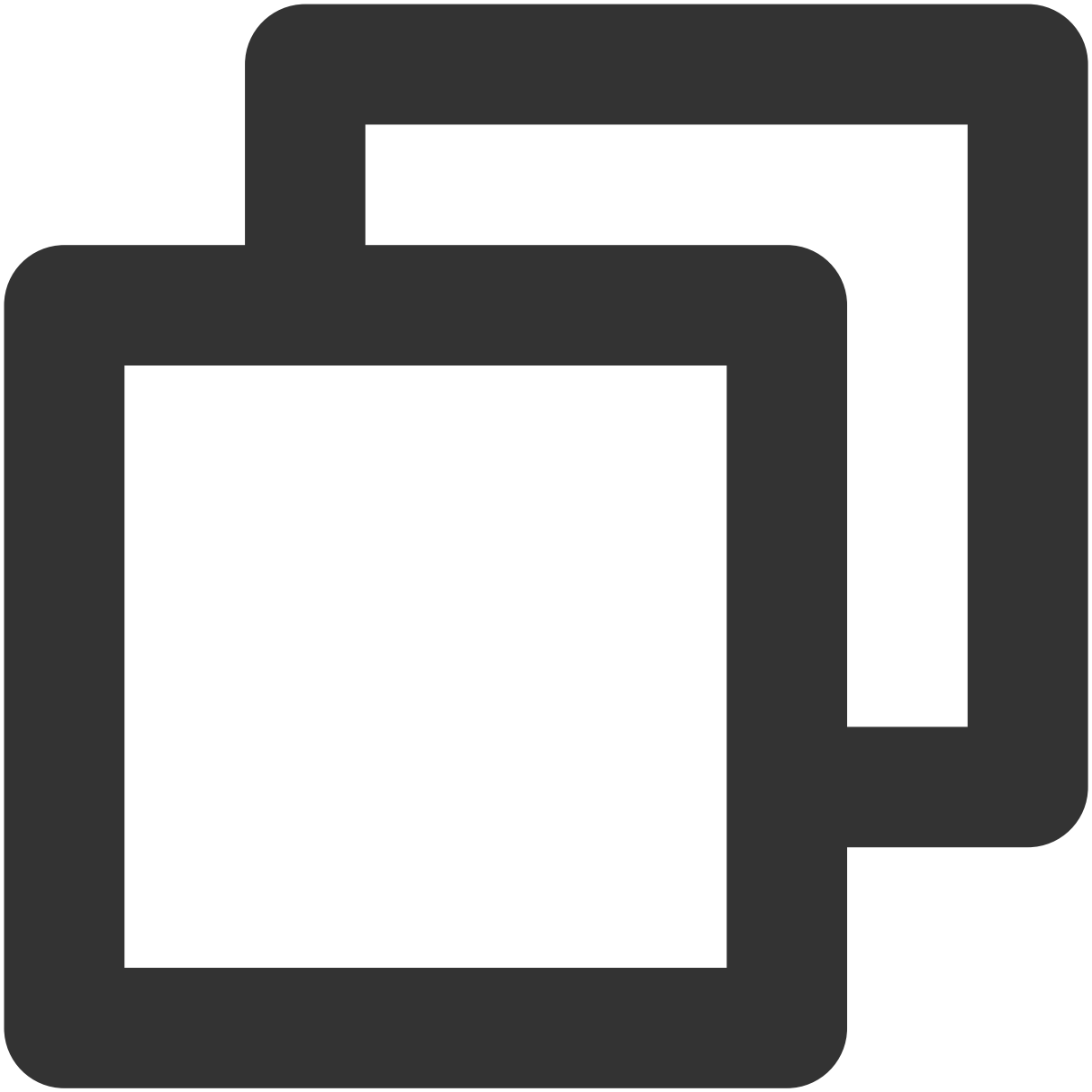


```
vncserver
```

次のような結果が返された場合は、VNCが正常に起動されたことを示します。

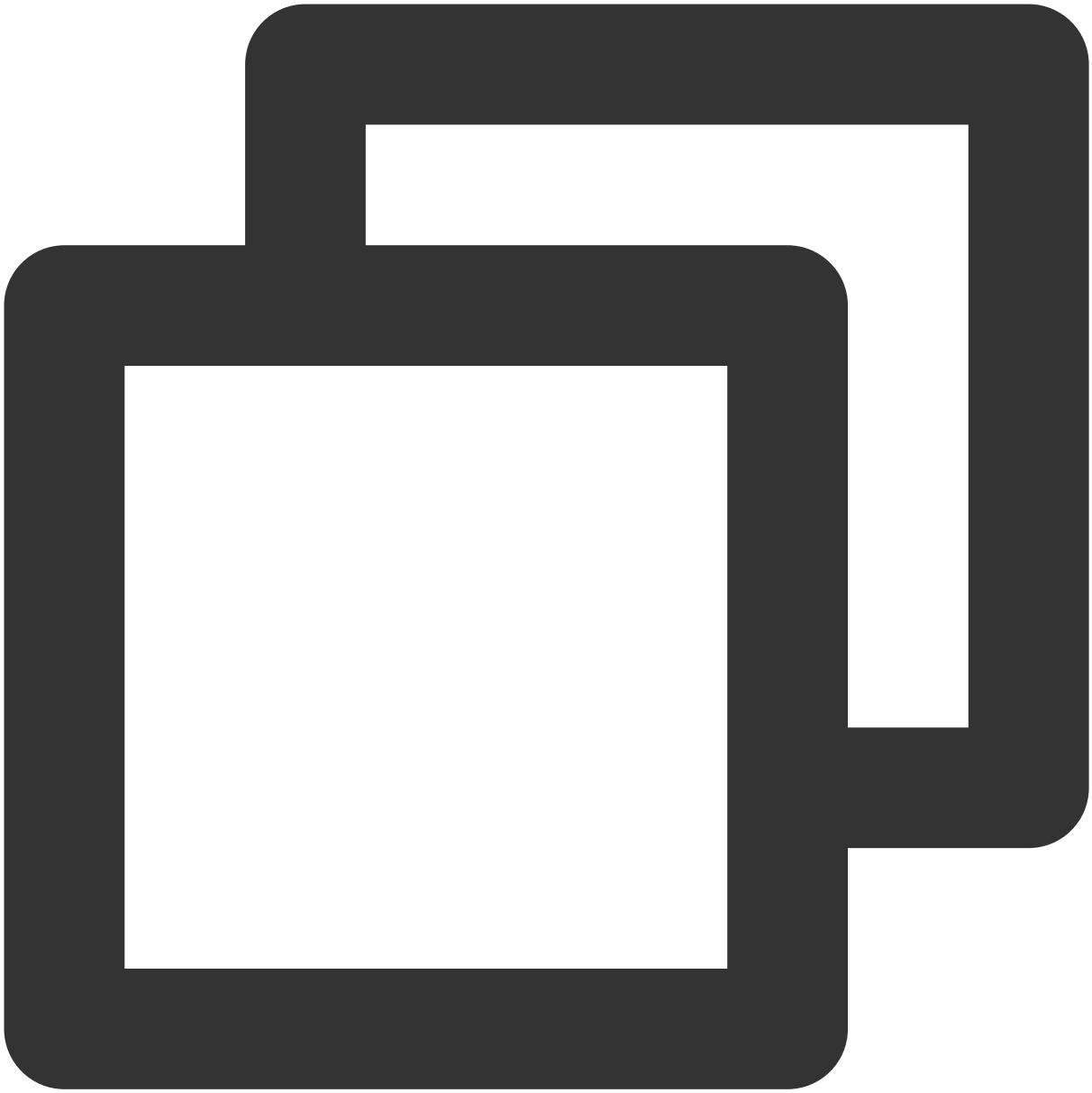
```
root@VM-0-133-ubuntu:/home/ubuntu# vncserver

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. 次のコマンドを実行して、VNC 構成ファイルを開きます。



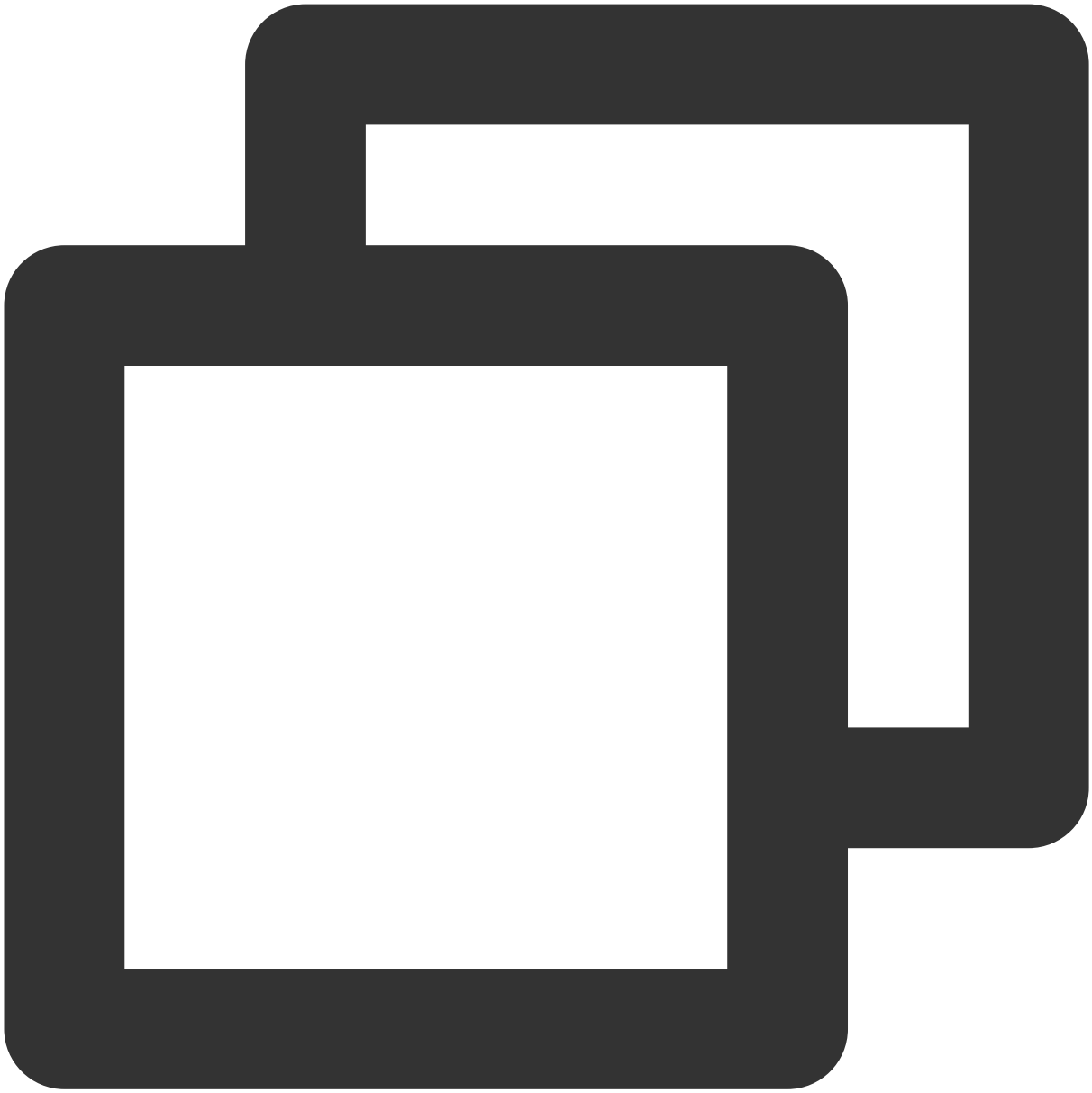
```
vi ~/.vnc/xstartup
```

3. **i** を押して編集モードに切り替え、構成ファイルを以下の内容に変更します。

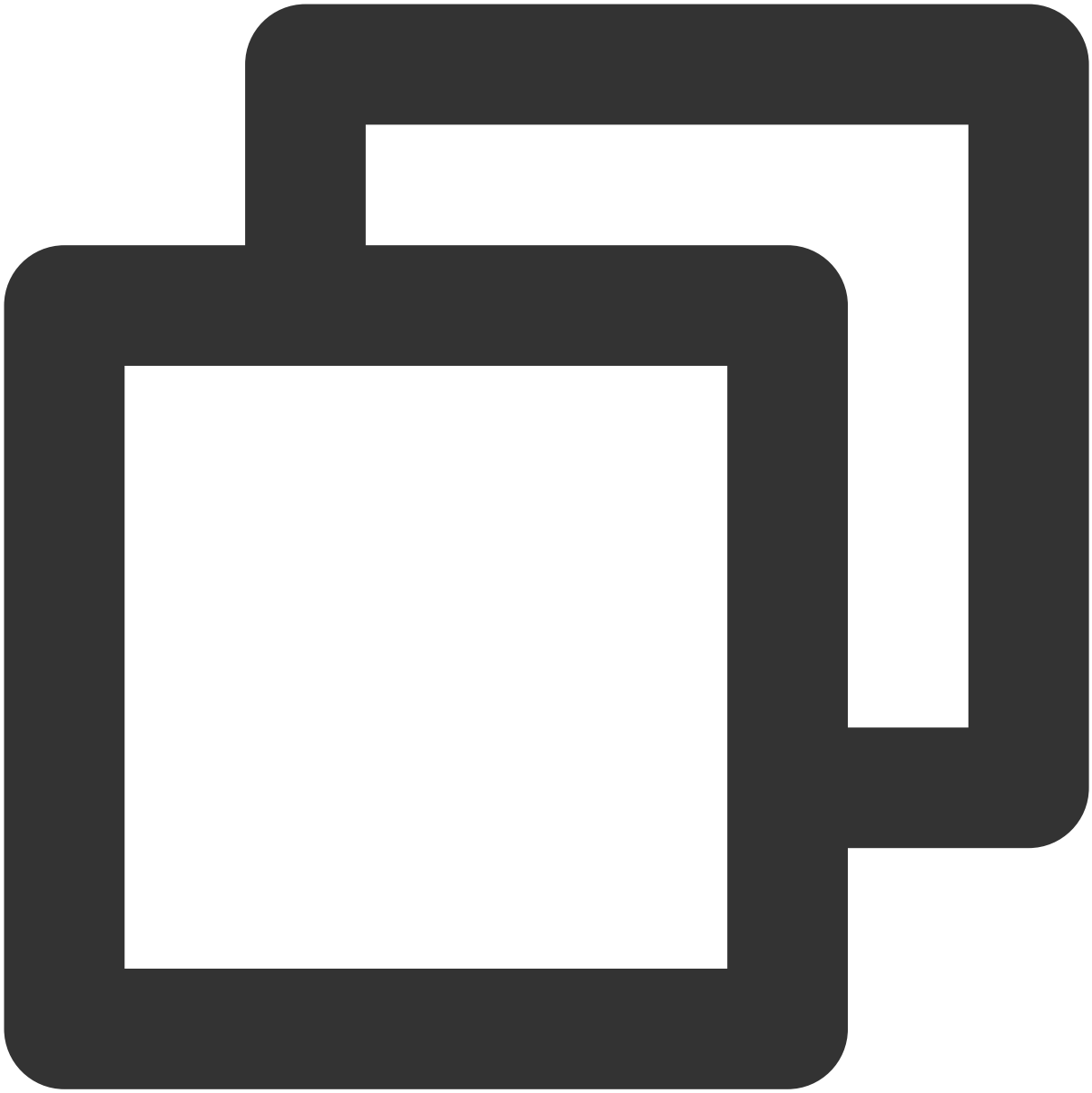


```
#!/bin/sh
export XKL_XMODMAP_DISABLE=1
export XDG_CURRENT_DESKTOP="GNOME-Flashback:GNOME"
export XDG_MENU_PREFIX="gnome-flashback-"
gnome-session --session=gnome-flashback-metacity --disable-acceleration-check &
```

4. **Esc**を押し、**:wq**を入力して、ファイルを保存して戻ります。
5. 次のコマンドを実行して、デスクトッププロセスを再起動します。

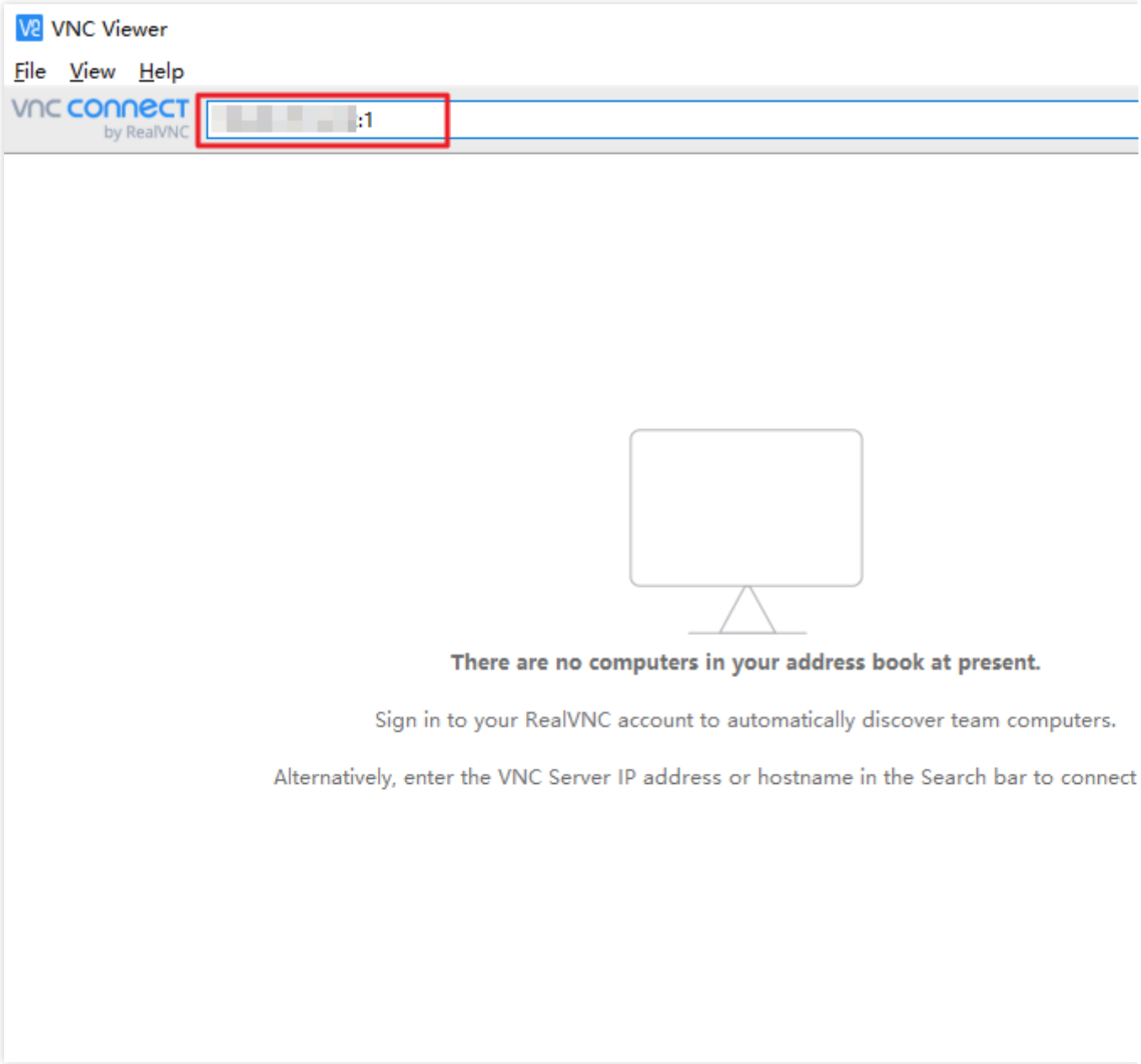


```
vncserver -kill :1 #元のデスクトッププロセスを終了し、コマンドを入力します（ここで:1はデスクト
```

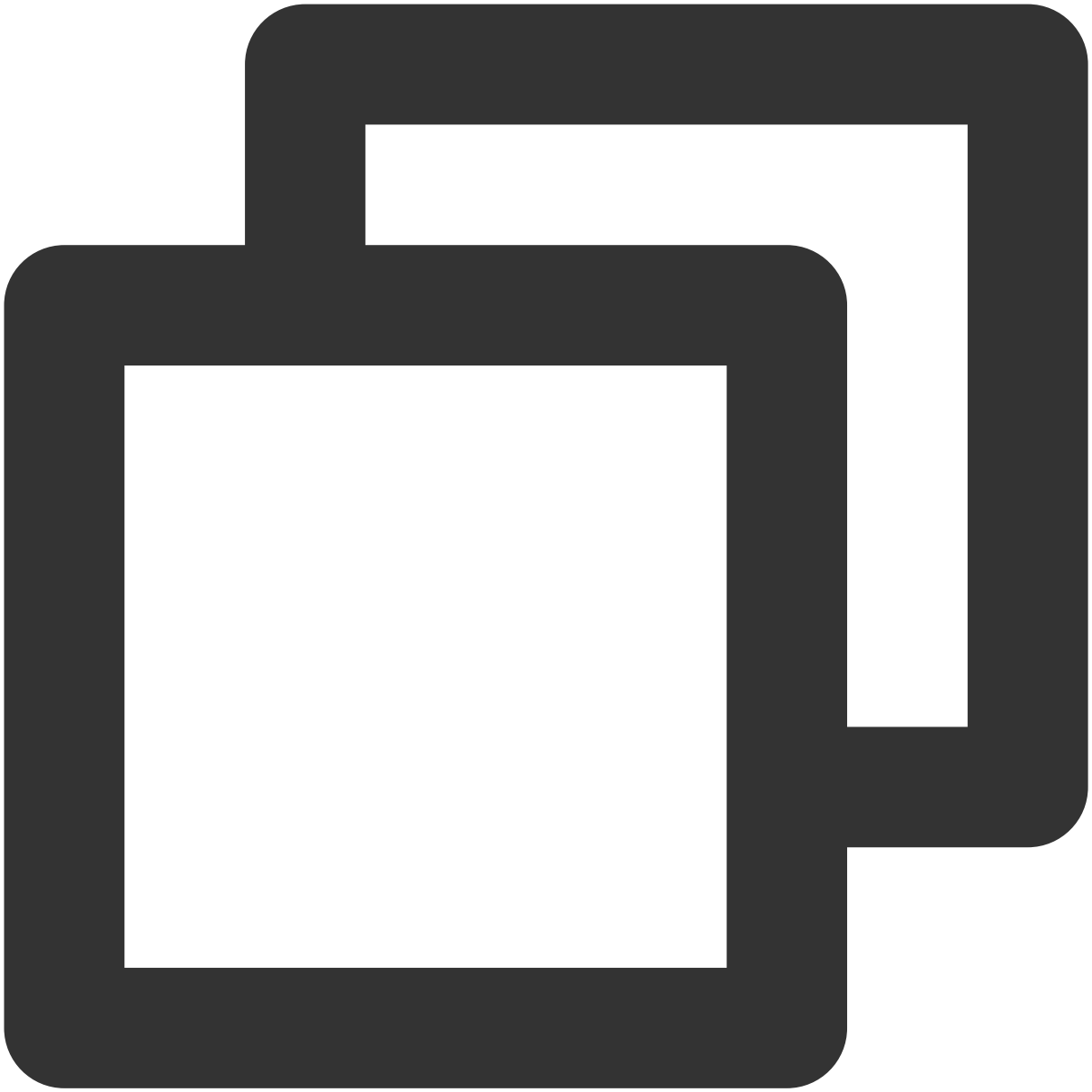


```
vncserver -geometry 1920x1080 :1 #新しいセッションを生成します
```

6. ここをクリックして VNC Viewer公式サイトに進み、ローカルコンピューターのオペレーティングシステムタイプに合わせて、対応するバージョンをダウンロードおよびインストールします。
7. VNC Viewerソフトウェア内で、 `CVMのIPアドレス:1` を入力し、 **Enter **を押します。



8. ポップアップしたダイアログボックスで **Continue **をクリックします。
9. 手順2 で設定したVNCのパスワードを入力し、**OK**をクリックすれば、インスタンスにログインしてグラフィック化インターフェースを使用することができます。
1. 次のコマンドを実行してVNCサービスを起動し、パスワードを設定します。

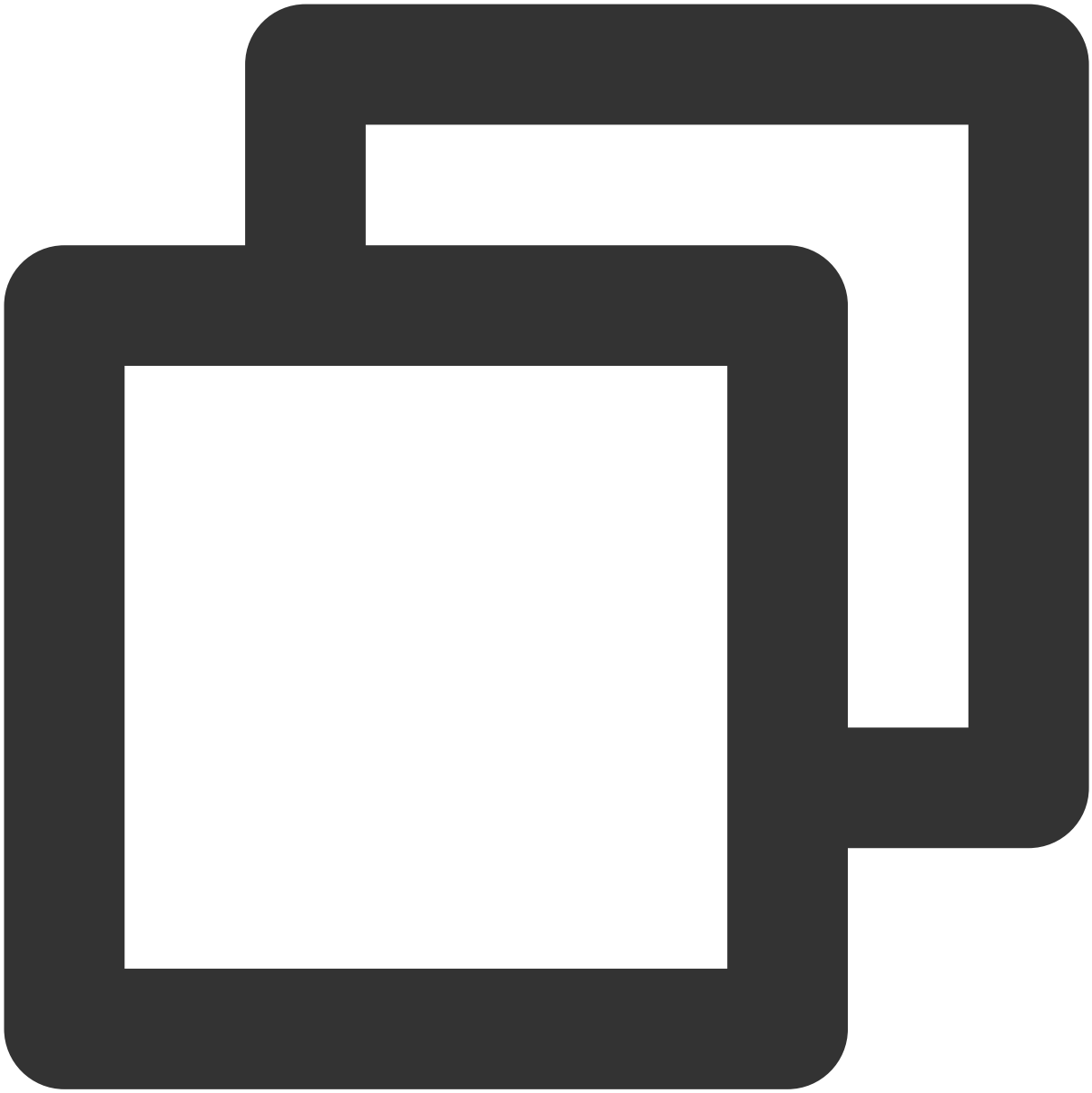


```
vncserver
```

次のような結果が返された場合は、VNCが正常に起動されたことを示します。

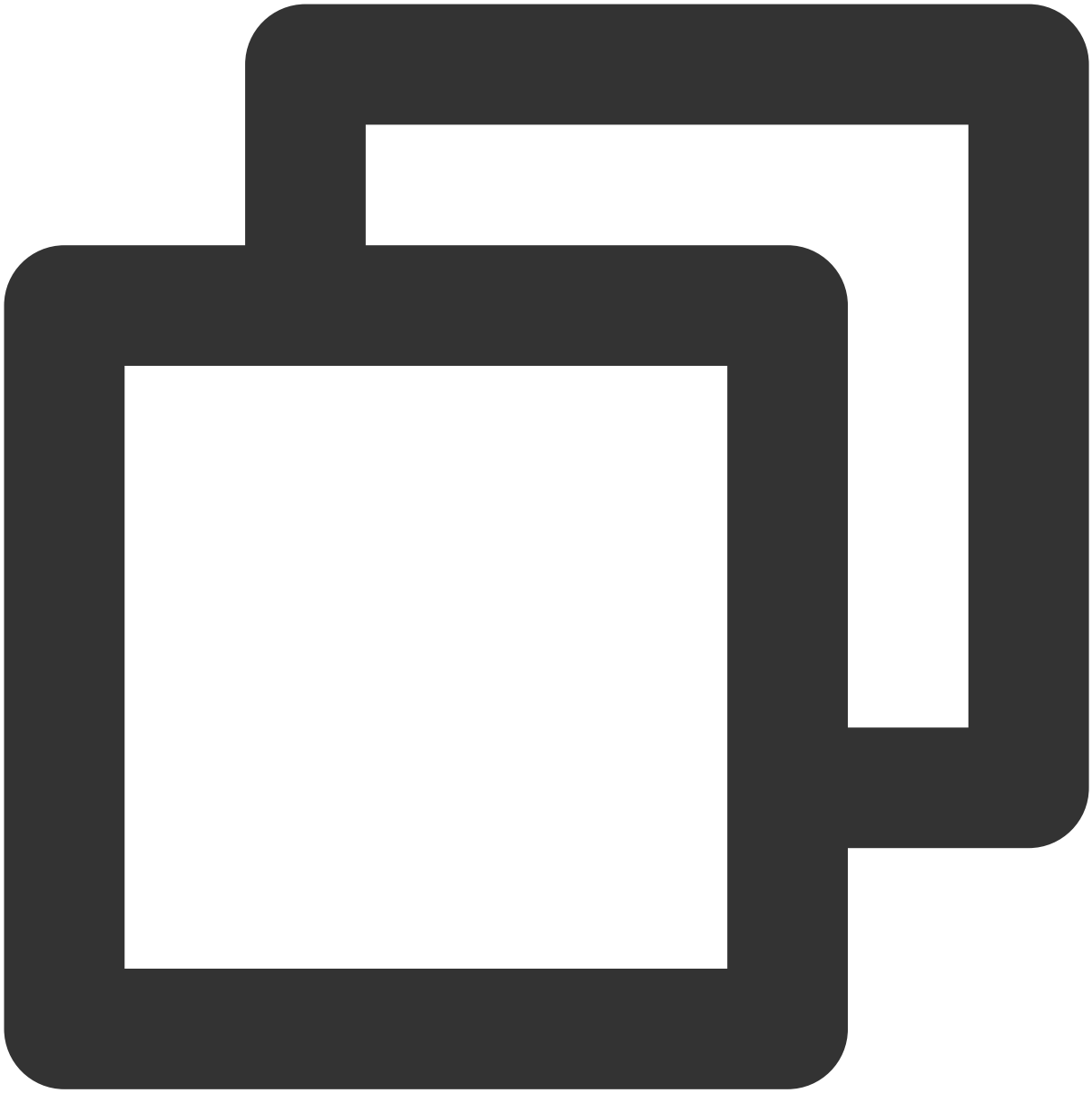
```
root@VM-0-133-ubuntu:/home/ubuntu# vncserver

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. 次のコマンドを実行して、VNC 構成ファイルを開きます。



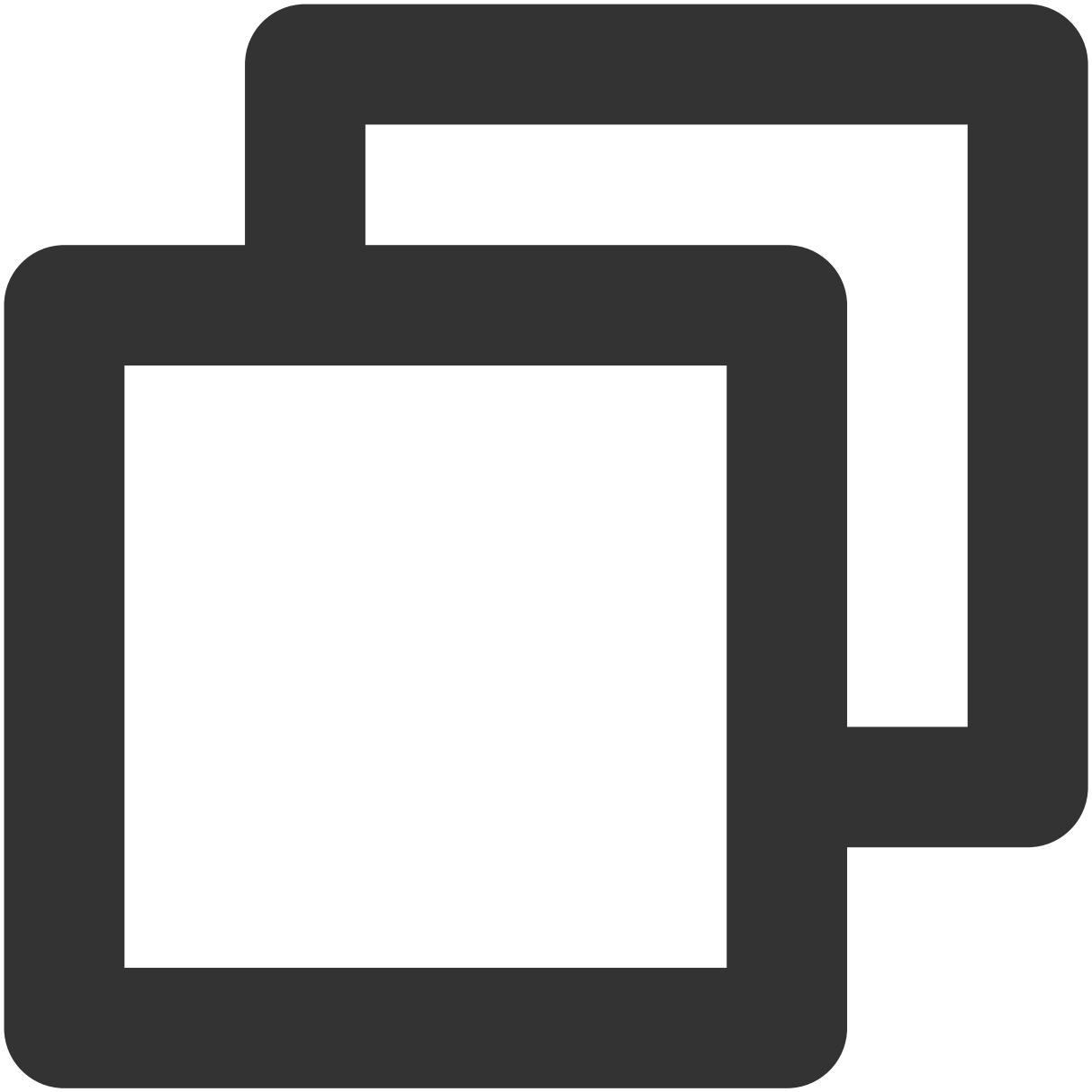
```
vi ~/.vnc/xstartup
```

3. **i** を押して編集モードに切り替え、構成ファイルを以下の内容に変更します。

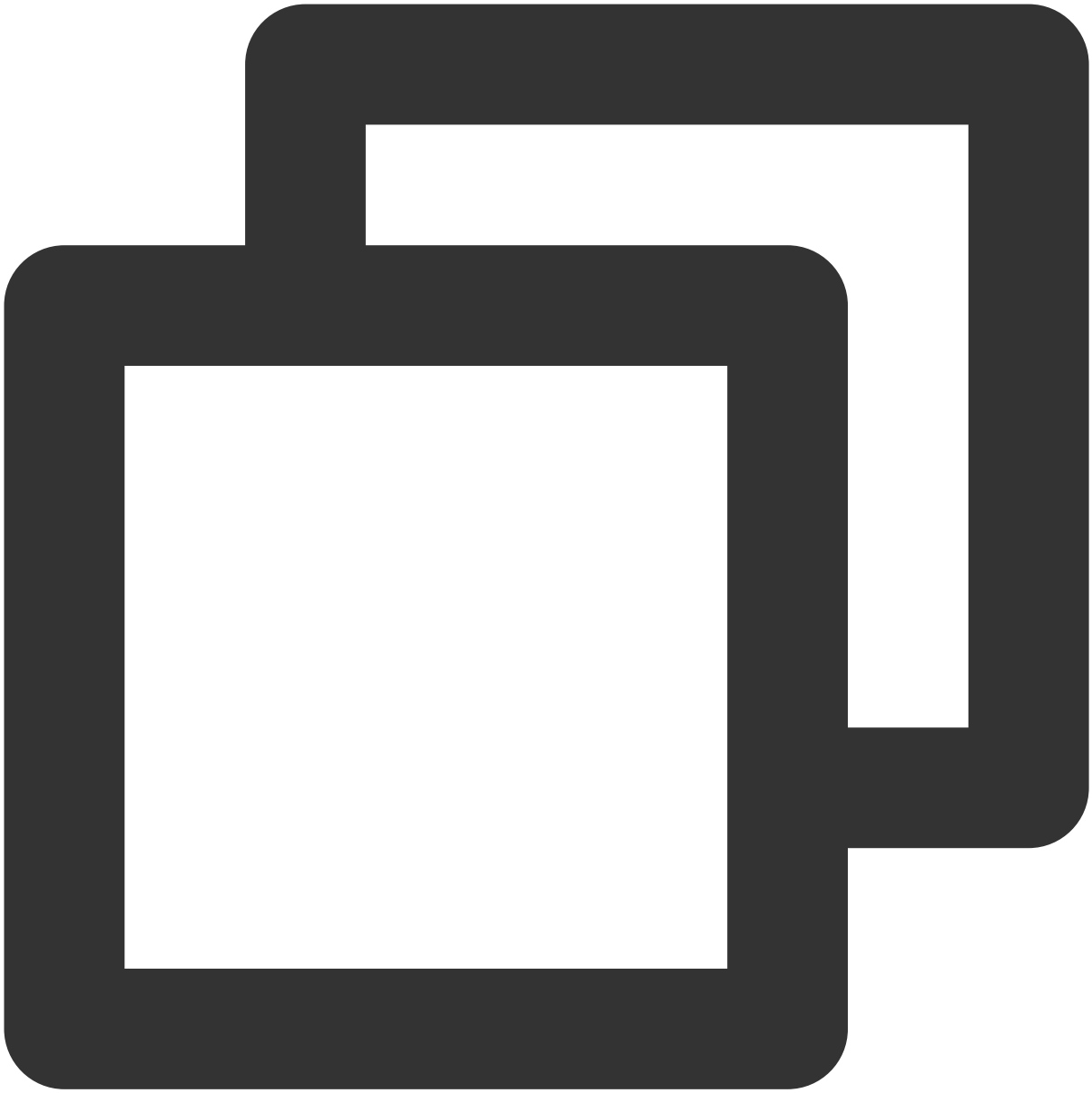


```
#!/bin/sh
export XKL_XMODMAP_DISABLE=1
export XDG_CURRENT_DESKTOP="GNOME-Flashback:GNOME"
export XDG_MENU_PREFIX="gnome-flashback-"
gnome-session --session=gnome-flashback-metacity --disable-acceleration-check &
```

4. **Esc**を押し、**:wq**を入力して、ファイルを保存して戻ります。
5. 次のコマンドを実行して、デスクトッププロセスを再起動します。

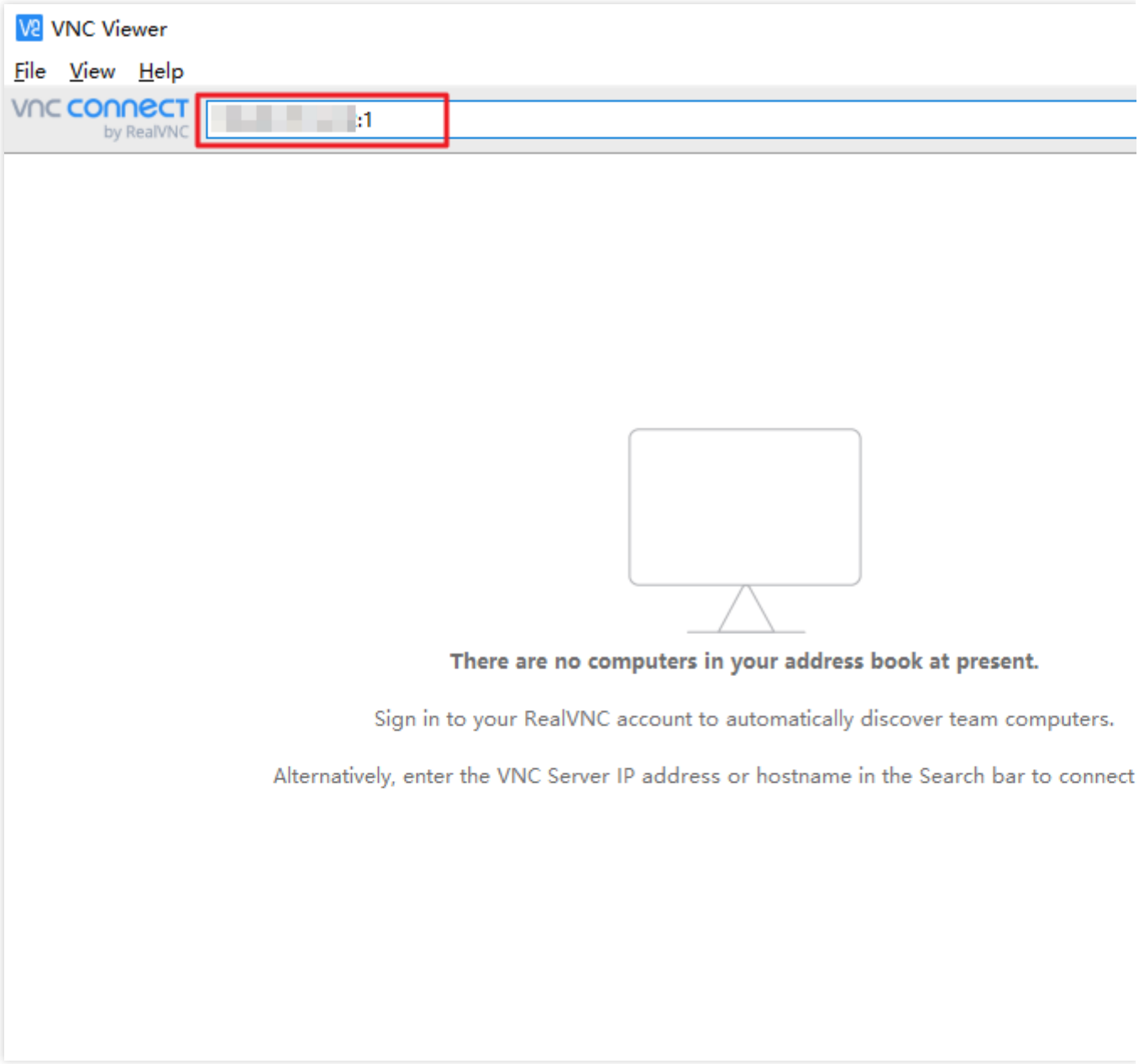


```
vncserver -kill :1 #元のデスクトッププロセスを終了し、コマンドを入力します（ここで:1はデスクト
```



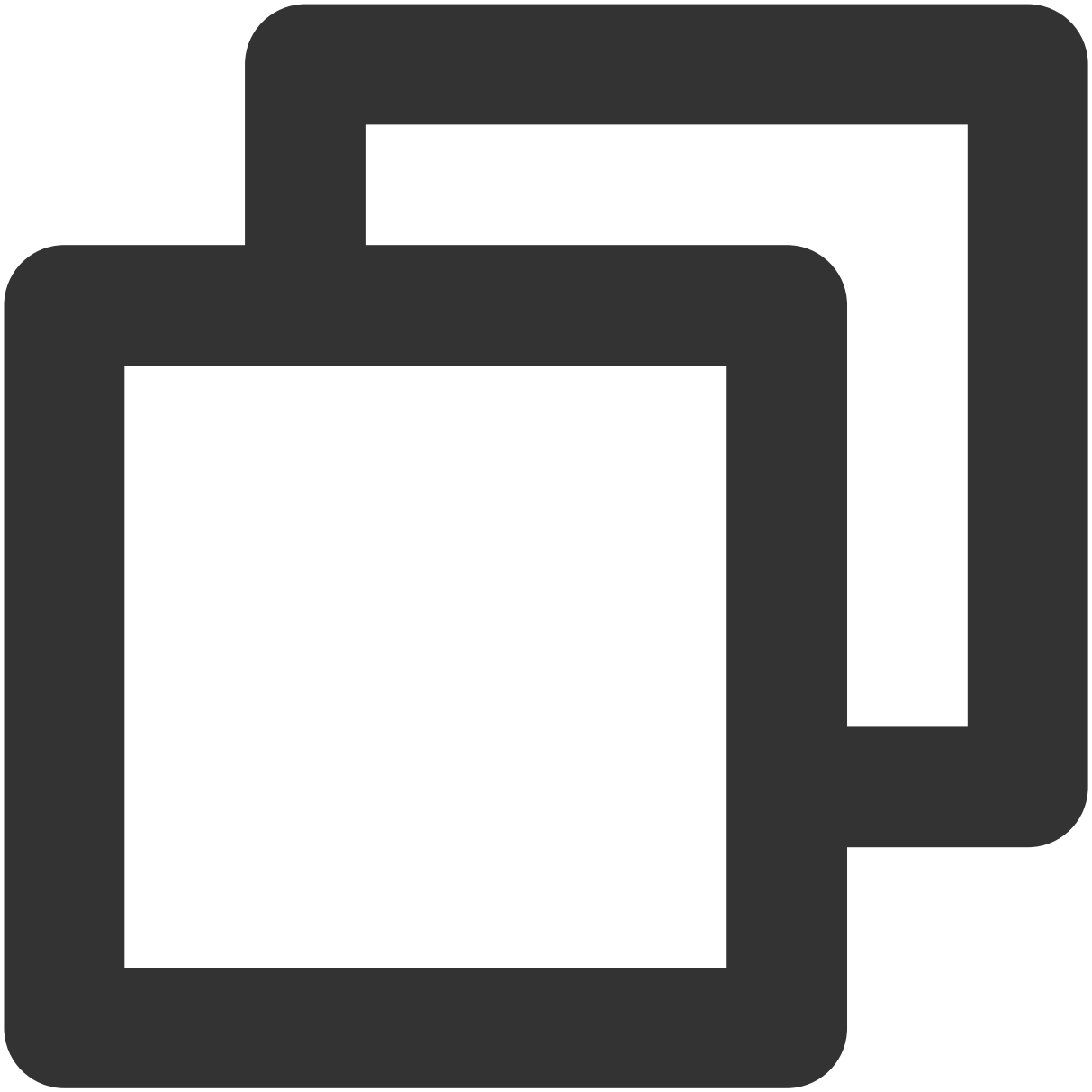
```
vncserver -geometry 1920x1080 :1 #新しいセッションを生成します
```

6. ここをクリックして VNC Viewer公式サイトに進み、ローカルコンピューターのオペレーティングシステムタイプに合わせて、対応するバージョンをダウンロードおよびインストールします。
7. VNC Viewerソフトウェア内で、 `CVMのIPアドレス:1` を入力し、 **Enter **を押します。



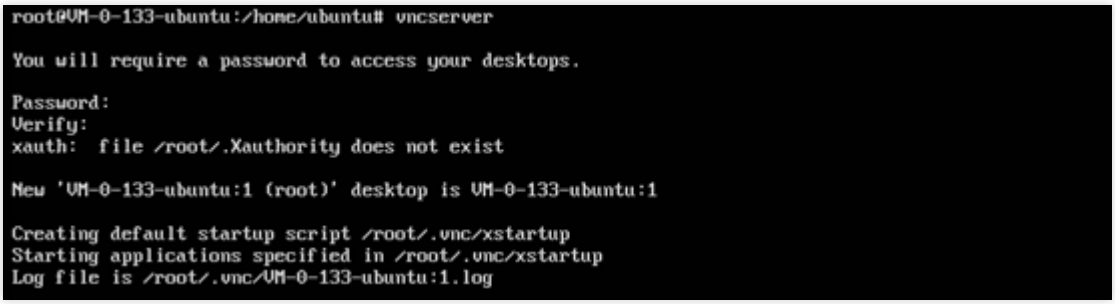
8. ポップアップしたダイアログボックスで **Continue **をクリックします。
9. 手順2 で設定したVNCのパスワードを入力し、**OK**をクリックすれば、インスタンスにログインしてグラフィック化インターフェースを使用することができます。

1. 次のコマンドを実行してVNCサービスを起動し、パスワードを設定します。



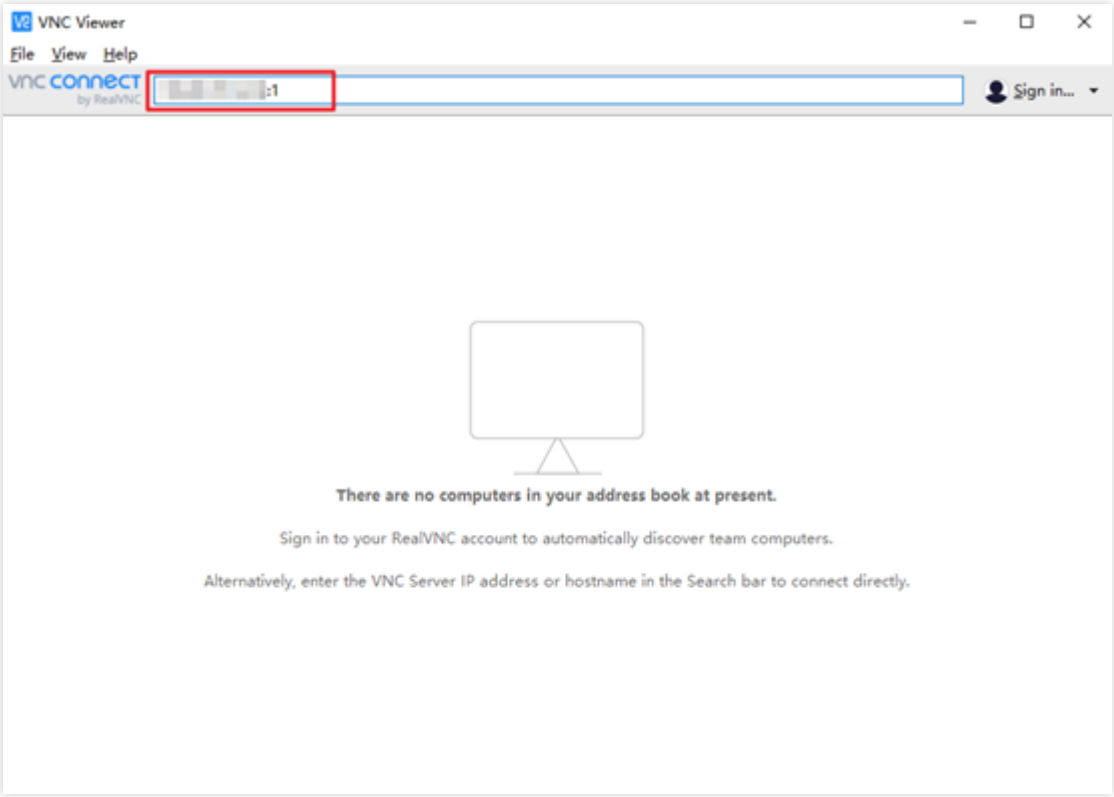
```
vncserver
```

次のような結果が返された場合は、VNCが正常に起動されたことを示します。



2. VNC Viewer 公式サイトに進み、ローカルコンピューターのオペレーティングシステムタイプに合わせて、対応するバージョンをダウンロードおよびインストールします。

3. VNC Viewerソフトウェア内で、 `CVMのIPアドレス:1` を入力し、**Enter**を押します。



4. ポップアップしたダイアログボックスで **Continue **をクリックします。

5. 前の手順で作成したパスワードを入力し、**OK** をクリックします。

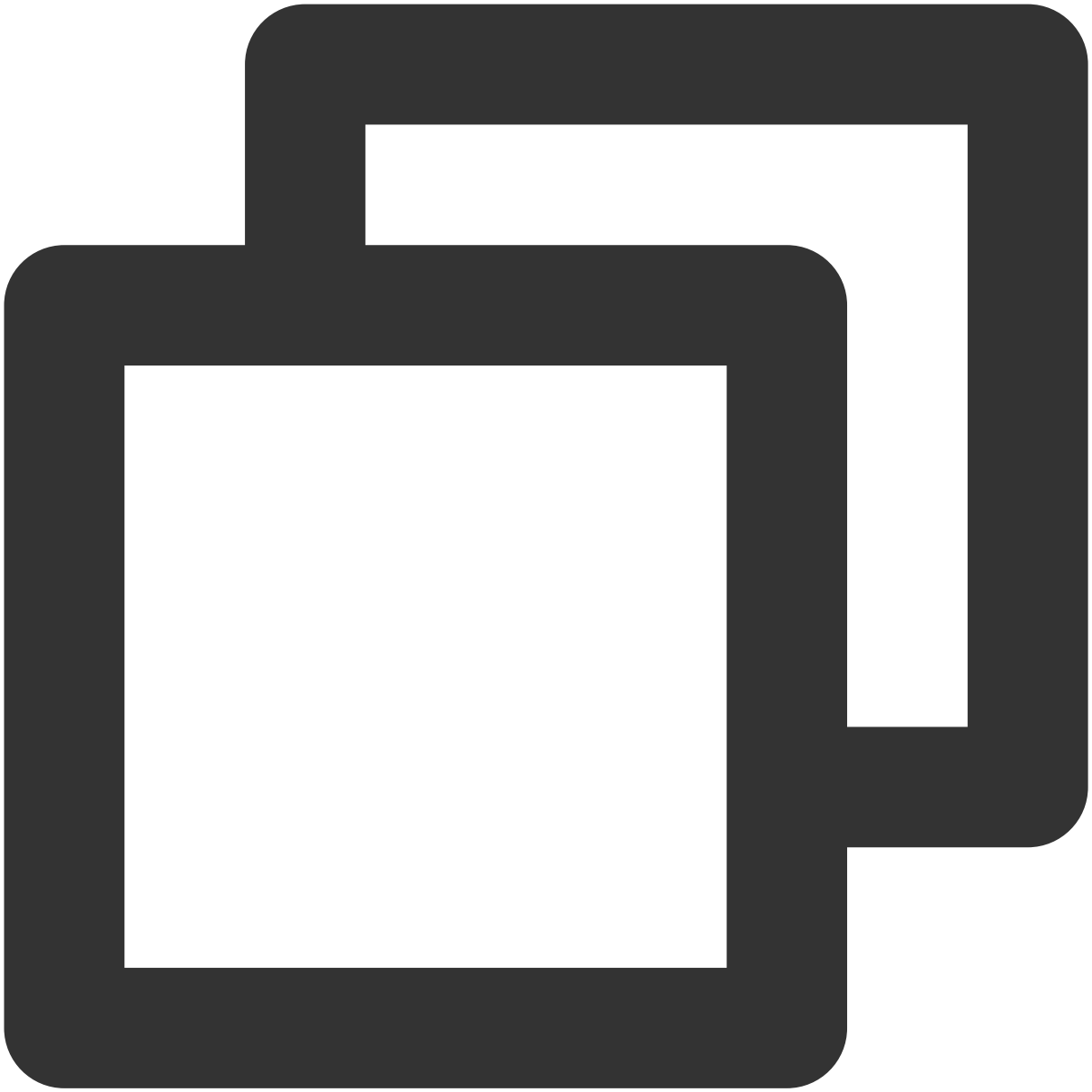
ご注意：

パスワードを忘れた場合は、インスタンスにログインし、 `vncpasswd` コマンドを実行して VNCログインパスワードをリセットします。

付録：

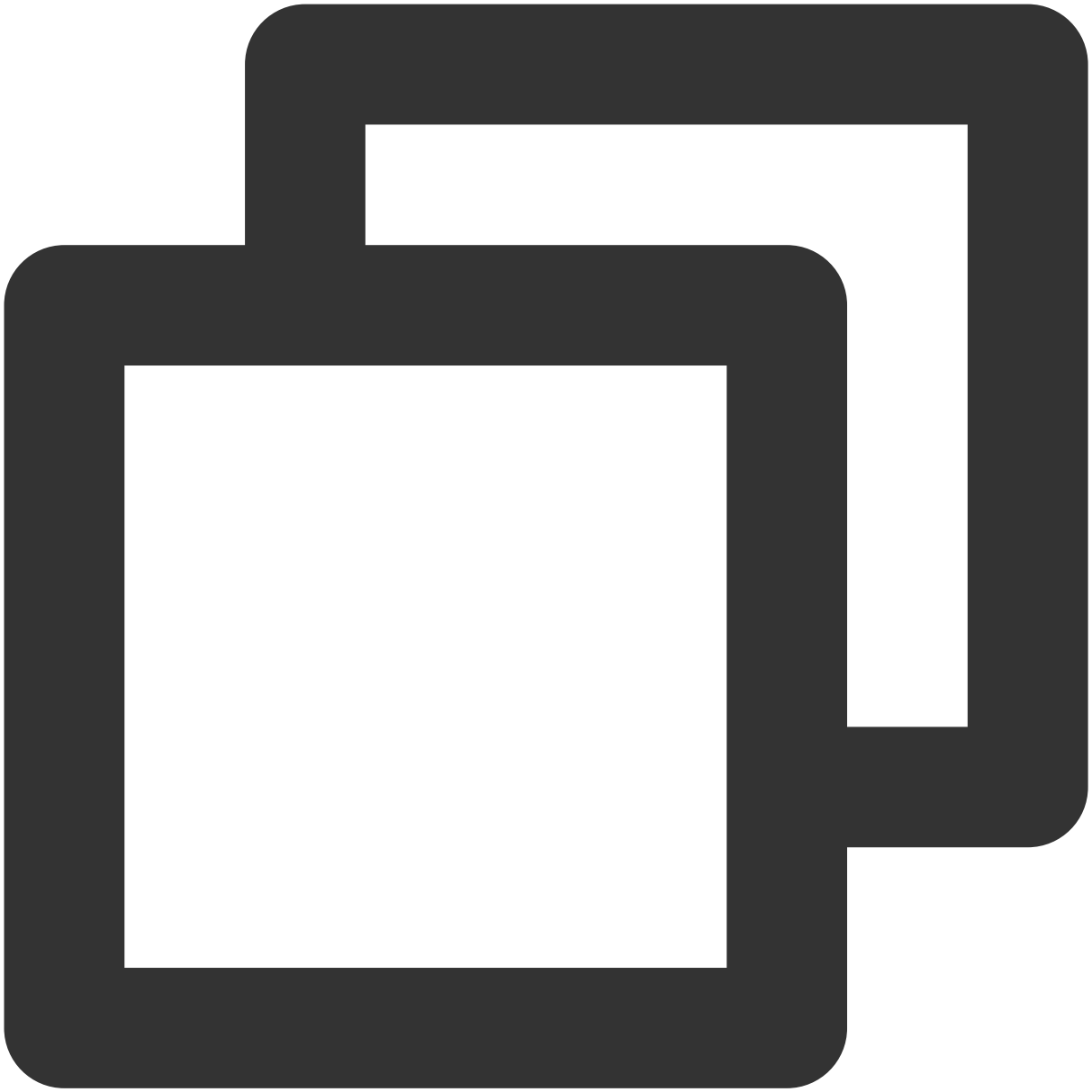
Chrome をインストールする：

インスタンスにログインし、次のコマンドを実行して **.deb** パッケージ ファイルをダウンロードします。



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

.deb ファイルをインストールする



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

CentOS視覚化インターフェースの構築

最終更新日：：2022-07-12 10:50:32

操作シナリオ

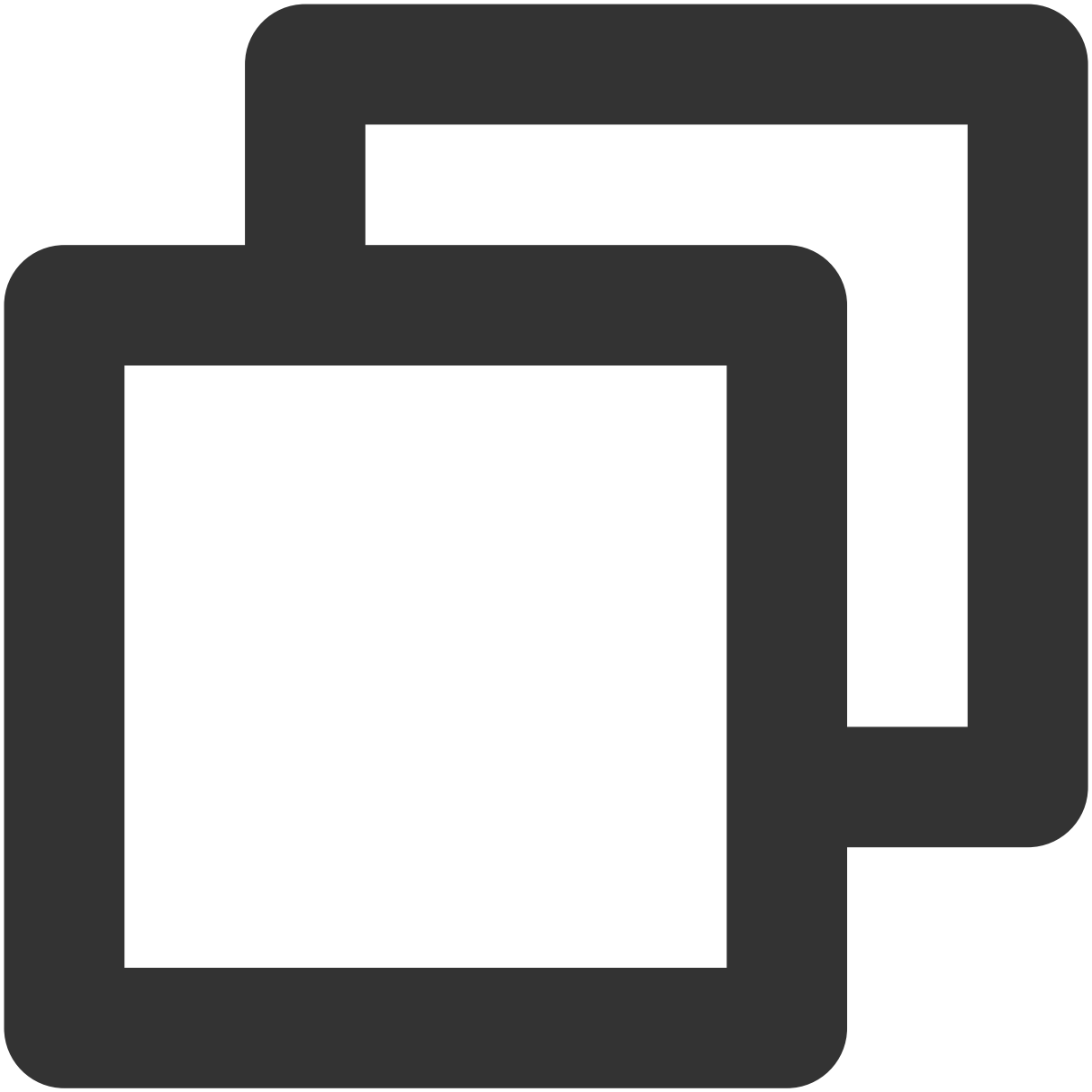
ここでは、OSがCentOS 8.2およびCentOS 7.9のTencent Cloud CVMを例にとり、CentOS視覚化インターフェースの構築方法についてご紹介します。

説明事項

性能と汎用性の観点から、Tencent Cloudの提供するLinuxパブリックイメージには、デフォルトではグラフィックコンポーネントをインストールしていません。
インストールが不適切な場合はインスタンスが正常に起動しなくなるおそれがあります。カスタムイメージの作成 または スナップショットの作成 によってデータバックアップを作成することをお勧めします。

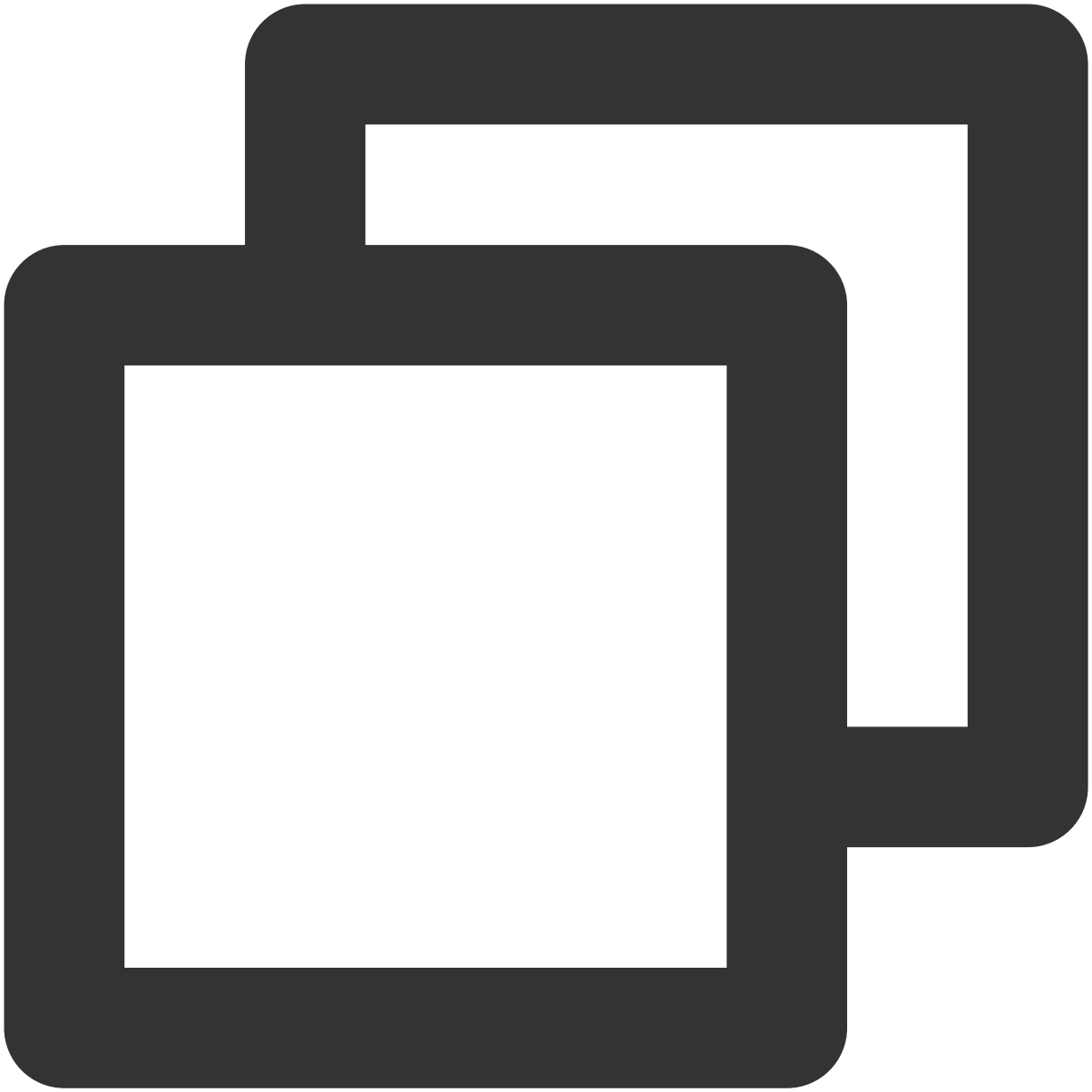
操作手順

実際に使用するCVMのOSに応じて、次の手順を参照して操作を行ってください。
CentOS 8.2
CentOS 7.9
1. インスタンスにログインします。詳細については、標準ログイン方式を使用してLinuxインスタンスにログイン（推奨）をご参照ください。
2. 以下のコマンドを実行し、グラフィックインターフェースコンポーネントをインストールします。



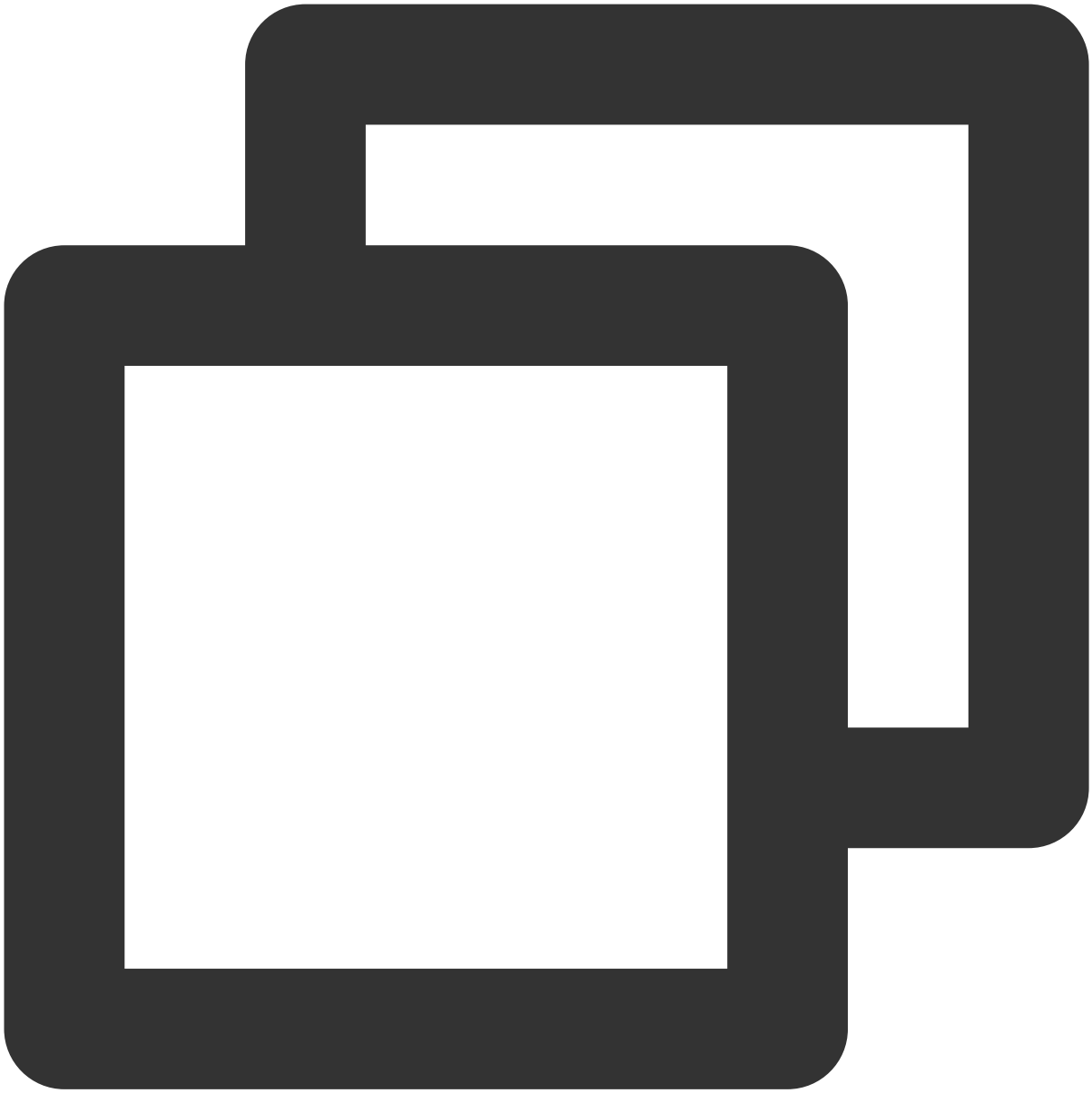
```
yum groupinstall "Server with GUI" -y
```

3. 以下のコマンドを実行し、デフォルトのグラフィックインターフェースを設定します。



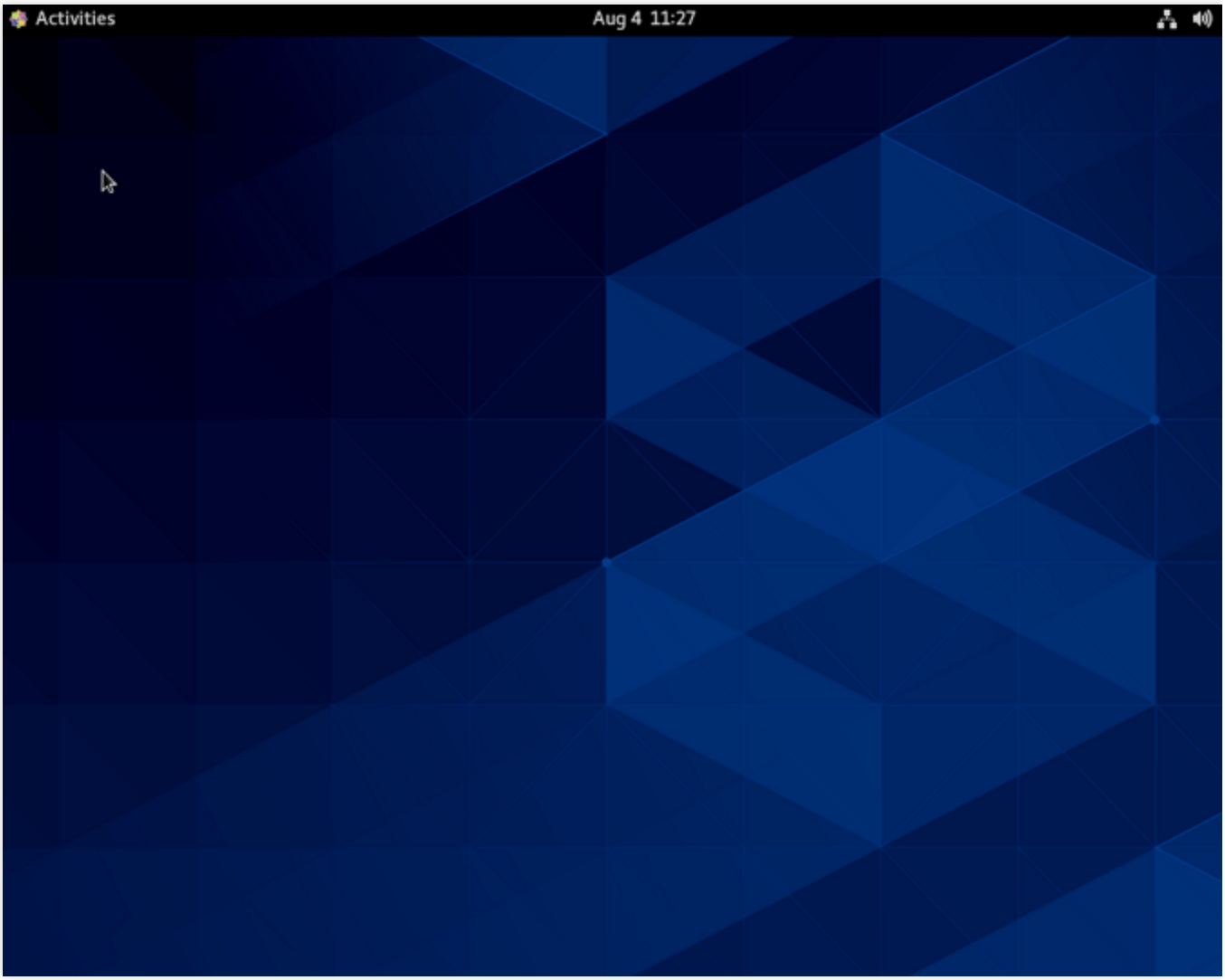
```
systemctl set-default graphical
```

4. 以下のコマンドを実行して、インスタンスを再起動します。

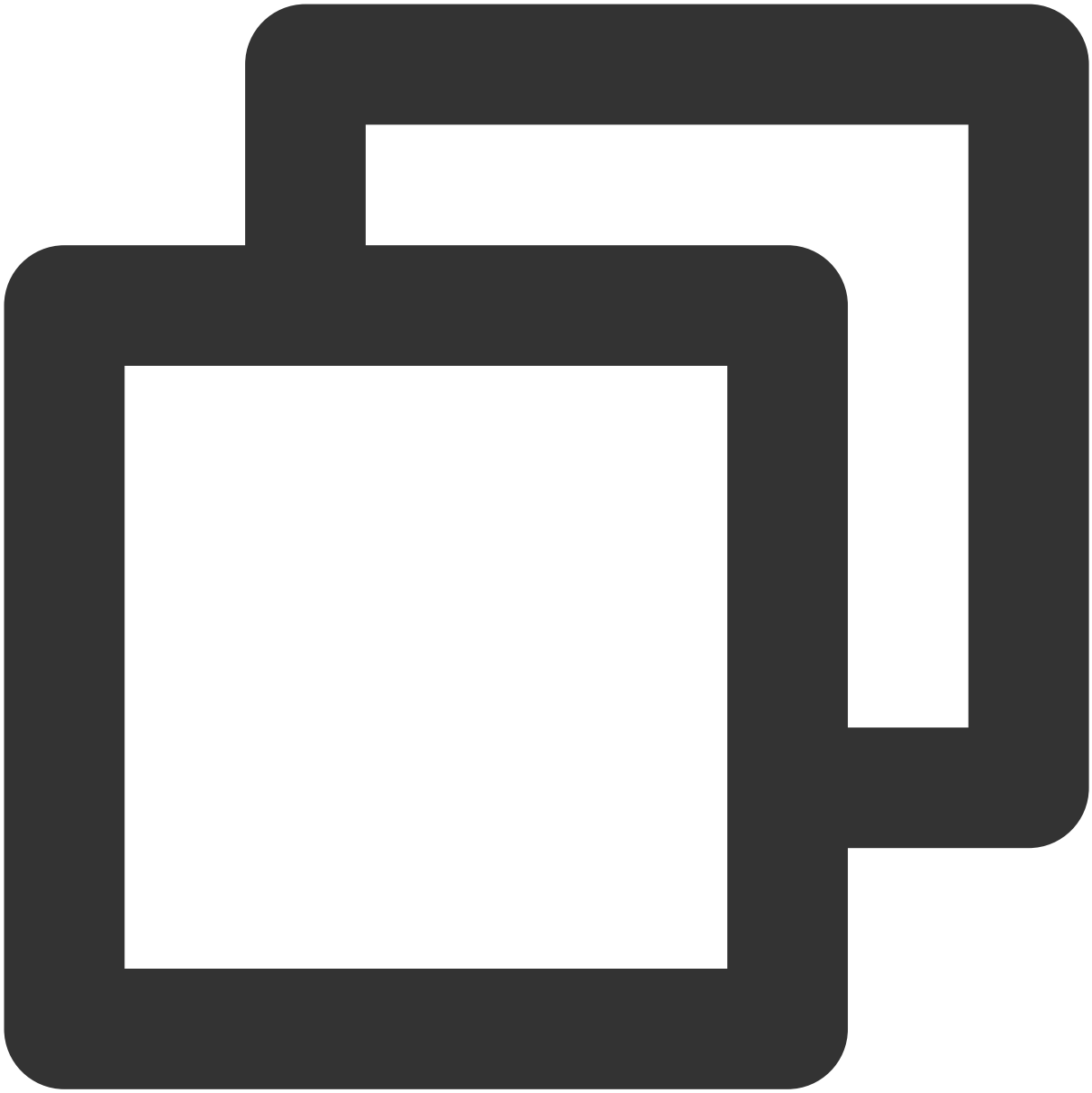


```
reboot
```

5. VNC方式でインスタンスにログインします。詳細については VNCを使用してLinuxインスタンスにログイン をご参照ください。
インスタンスにログイン後、視覚化インターフェースが確認できれば構築は成功です。インターフェースの表示に従って設定を行い、デスクトップに入った後、必要に応じて関連の操作を行うことができます。下図に示します。

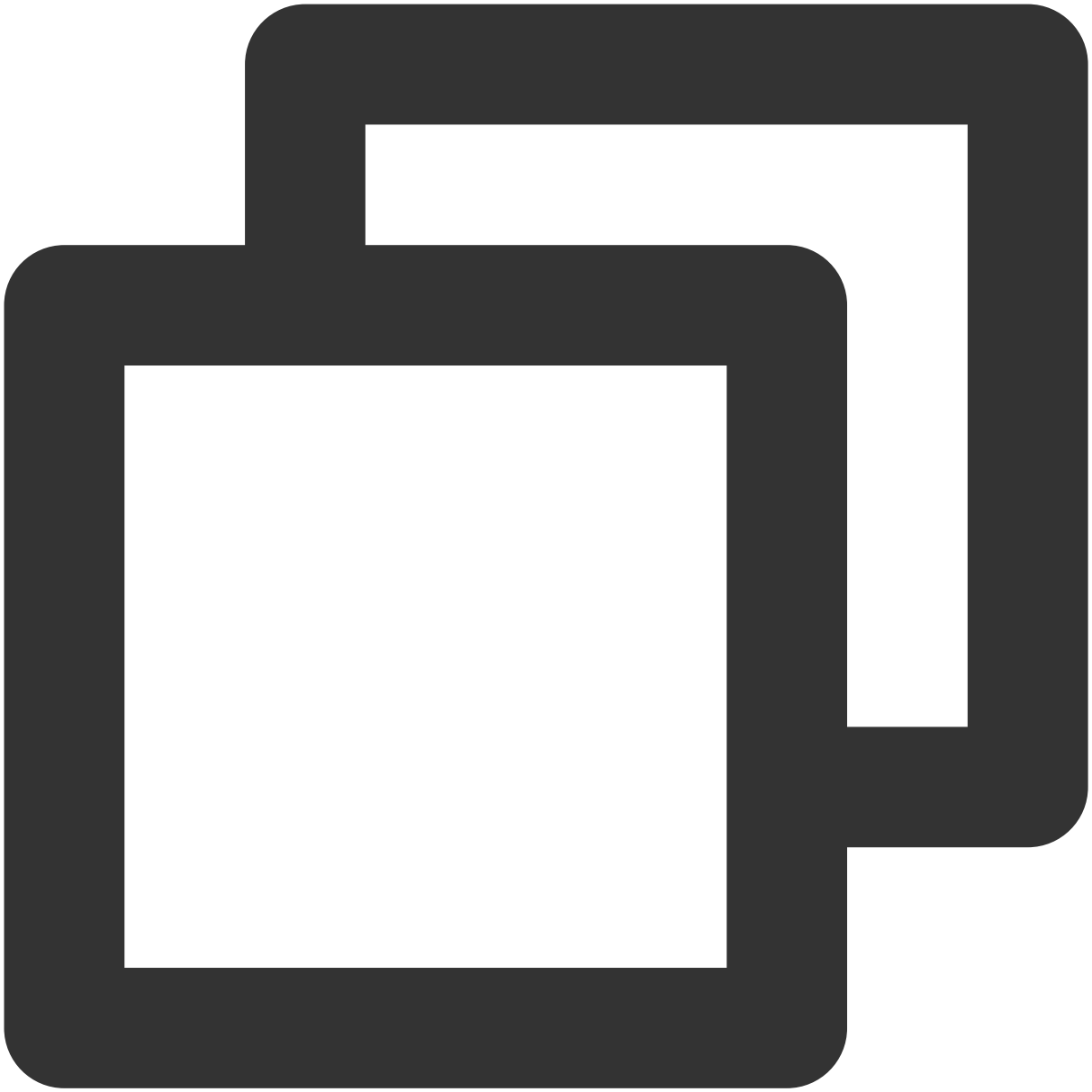


1. インスタンスにログインします。詳細については、標準ログイン方式を使用してLinuxインスタンスにログイン（推奨）をご参照ください。
2. 以下のコマンドを実行し、グラフィックインターフェースコンポーネントをインストールします。



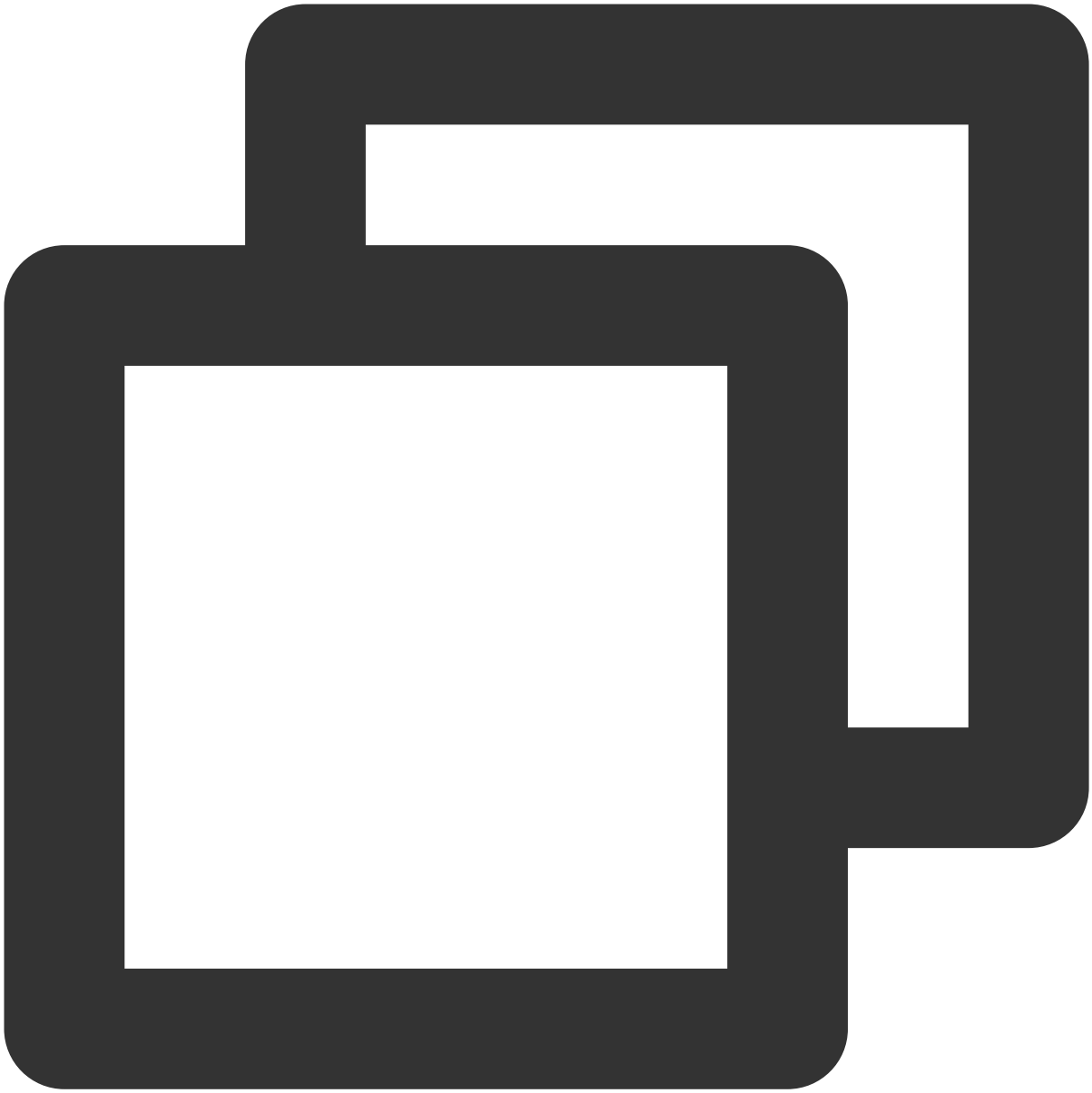
```
yum groupinstall "GNOME Desktop" "Graphical Administration Tools" -y
```

3. 以下のコマンドを実行し、デフォルトのグラフィックインターフェースを設定します。



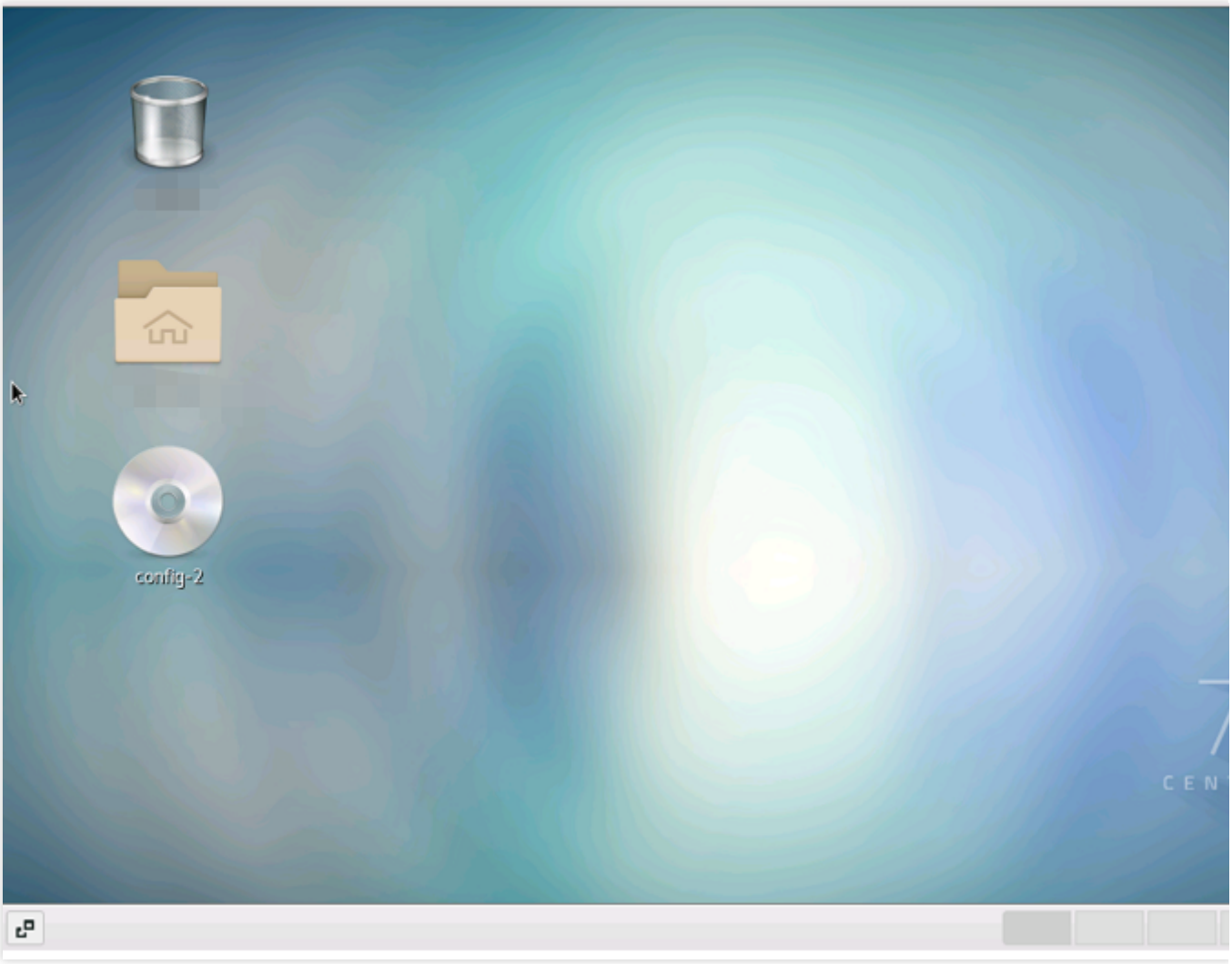
```
ln -sf /lib/systemd/system/runlevel5.target /etc/systemd/system/default.target
```

4. 以下のコマンドを実行して、インスタンスを再起動します。



```
reboot
```

5. VNC方式でインスタンスにログインします。詳細については VNCを使用してLinuxインスタンスにログイン をご参照ください。
インスタンスにログイン後、視覚化インターフェースが確認できれば構築は成功です。インターフェースの表示に従って設定を行い、デスクトップに入った後、必要に応じて関連の操作を行うことができます。下図に示します。



データバックアップ

最終更新日：：2024-01-05 11:05:53

このドキュメントでは、CVMデータのバックアップおよび保護ソリューションを紹介します。データのセキュリティを保護するために、大切なデータは定期的にバックアップを取ることをお勧めします。詳細については、次のドキュメントをご参照ください：

バックアップと復元
カスタムイメージの作成
スナップショットの作成
スケジュールされたスナップショット
スナップショットからデータをロールバック

データのバックアップ時に問題が発生した場合は、データのバックアップに関するFAQ ドキュメントを参照して問題のトラブルシューティングを行ってください。

ローカルファイルをCVMにアップロードします
ローカルファイルをCVMにコピーする方法

最終更新日：：2022-07-07 16:19:39

ローカルのファイルをCVMに保存することは、CVMを購入するユーザーの一般的な用途の一つです。このドキュメントでは、ローカルのファイルをCVM上にコピーする方法についてご説明します。
ローカルのOSのタイプおよび購入したサーバーのタイプに応じて、次の方法を参照して操作を行うことができます。

本地操作系统类型	云服务器操作系统（Linux）	云服务器操作系统（Windows）
Windows	通过 WinSCP 方式上传文件到云服务器 通过 FTP 方式上传文件到云服务器	Windows OSからMSTSCを利用して、Windows CVMにファイルをアップロードする
Linux	SCP方式でファイルをCVMにアップロードする FTP方式でファイルをCVMにアップロードする	RDS方式でファイルをCVMにアップロードする
Mac OS		MRDによってファイルをCVMにアップロードする

ローカルコンピュータのOSがWindowsであり、購入したCVMのOSがLinuxの場合は、WinSCP方式でファイルをCVMにアップロードすることができます。
説明：
アップロードしたいファイルが36KB未満で、なおかつテキストファイルの場合はファイルをCVMにアップロードする方式をお勧めします。コンソール上での簡単な操作でファイルをアップロードできます。

次の操作

重要な業務データがある場合、または個人ファイルのバックアップが必要な場合は、ファイルのCVMへのアップロードが完了した後、重要ファイルのスナップショットを手動または自動で作成することもできます。スナップショットを適用可能なシーンおよび使用方法についてお知りになりたい場合は、スナップショットに関するご質問 をご参照ください。

問題が発生した場合

ご不便をおかけして申し訳ございません。チケットを提出 してお問い合わせください。もしくは先に関連ドキュメントをご参照の上、問題の特定および対処を行っていただくこともできます。
以下は、CVMをご使用中のユーザーからのよくあるご質問です。先にドキュメントをご参照の上、問題の特定および対処を行っていただくことをお勧めします。
CVMのログインパスワードを忘れました。
インスタンスのパスワードをリセット をご参照ください。
CVMにログインできません。
Windowsインスタンスにログインできない または Linuxインスタンスにログインできない をご参照ください。

WindowsシステムはMSTSCを介して Windows CVMにファイルをアップロードします

最終更新日：：2022-03-24 15:19:52

概要

Windows CVMにファイルをアップロードする方法は通常MSTSCリモートデスクトップ接続（Microsoft Terminal Services Client）を使用することです。このドキュメントでは、ローカルWindowsコンピューターのリモートデスクトップ接続を使用して、Windows CVMにファイルをアップロードする方法について説明します。

前提条件

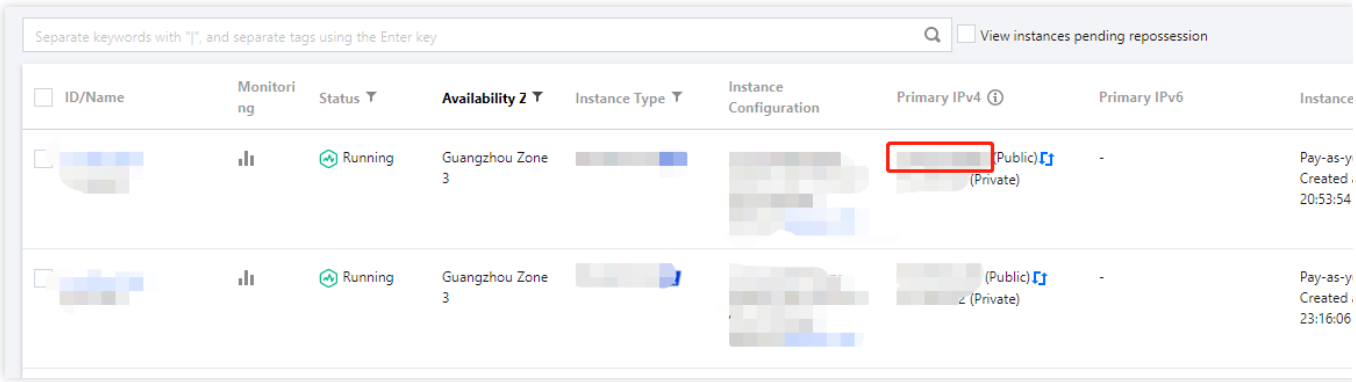
Windows CVM がパブリックネットワークにアクセスできることを確認してください。

操作手順

説明：
以下の操作手順は、Windows7のOSのローカルコンピュータを例としています。詳細な操作手順は、OSによって若干異なります。

パブリックIPの取得

CVMコンソール にログインし、ファイルをアップロードするCVMのパブリックIPを、インスタンスリストページに記述します。下図に示すとおりです。



ファイルのアップロード

1. ローカルコンピュータで、ショートカットキー**Windows + R**を使用して**実行**ウィンドウを開きます。
2. ポップアップした「実行」ウィンドウで**mstsc**と入力し、**OK**をクリックして「リモートデスクトップ接続」ダイアログボックスを開きます。
3. 「リモートデスクトップ接続」ダイアログボックスで、CVMパブリックIPアドレスを入力し、**オプション**をクリックします。
4. **通常**タブで、CVMのパブリックネットワークのIPアドレスとユーザー名Administratorを入力します。
5. **ローカルリソース**タブを選択し、**詳細情報**をクリックします。
6. 下図のように、ポップアップした「ローカルデバイスとリソース」ウィンドウで、**ドライブ**モジュールを選択し、Windows CVMにアップロードしたいファイルが存在するローカルディスクにチェックを入れ、**OK**をクリックします。
7. ローカル設定完了後、**接続**をクリックし、ポップアップした「Windowsセキュリティ」ウィンドウで、インスタンスのログインパスワードを入力し、Windows CVMにリモートログインします。
8. Windows CVMで、

を選択し、開いたウィンドウで**このコンピュータ**をクリックすると、CVMにマウントされているローカルディスクを確認することができます。
9. ダブルクリックしてマウントされたローカルハードディスクを開き、Windows CVMの他のハードディスクにコピーする必要があるローカルファイルをレプリケートすると、ファイルのアップロード操作は完了です。
例えば、ローカルハードディスク(F)のAファイルをWindows CVMのCドライブにレプリケートします。

ファイルのダウンロード

Windows CVMからローカルコンピュータにファイルをダウンロードする必要がある場合は、ファイルのアップロード操作を参照して、必要なファイルをWindows CVMからマウントされたローカルハードディスクにレプリケートすると、ファイルのダウンロード操作は完了です。

MRDを介してMacOSからWindows CVMにファイルをアップロード

最終更新日：：2021-12-27 11:18:37

シナリオ

Microsoft Remote Desktop (以下MRDと呼ぶ）は、MicrosoftがMac向けに提供しているリモートデスクトップ接続アプリです。このドキュメントでは、MacOSでMRDを使用して、Windows Server 2012 R2システムがインストールされているTencent Cloud CVMにファイルをアップロードする方法について説明します。

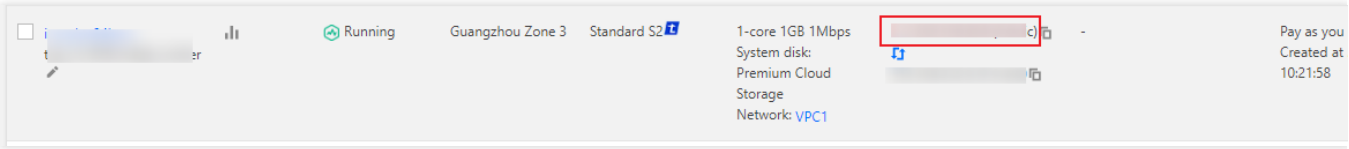
前提条件

MRDをダウンロードしてローカルコンピューターにインストールしました。このドキュメントでは、Microsoft Remote Desktop for Macを例として説明します。Microsoft社は、2017年にRemote Desktopクライアントへのダウンロードリンクの提供を停止し、ベータ版のリリースは、その子会社であるHockeyAppによって提供されます。ベータ版をダウンロードするには、Microsoft Remote Desktop Beta にアクセスしてください。
MRDはMacOS10.10以降のバージョンをサポートします。サポートされているOSを使用してください。
Windows CVMを購入しました。

操作手順

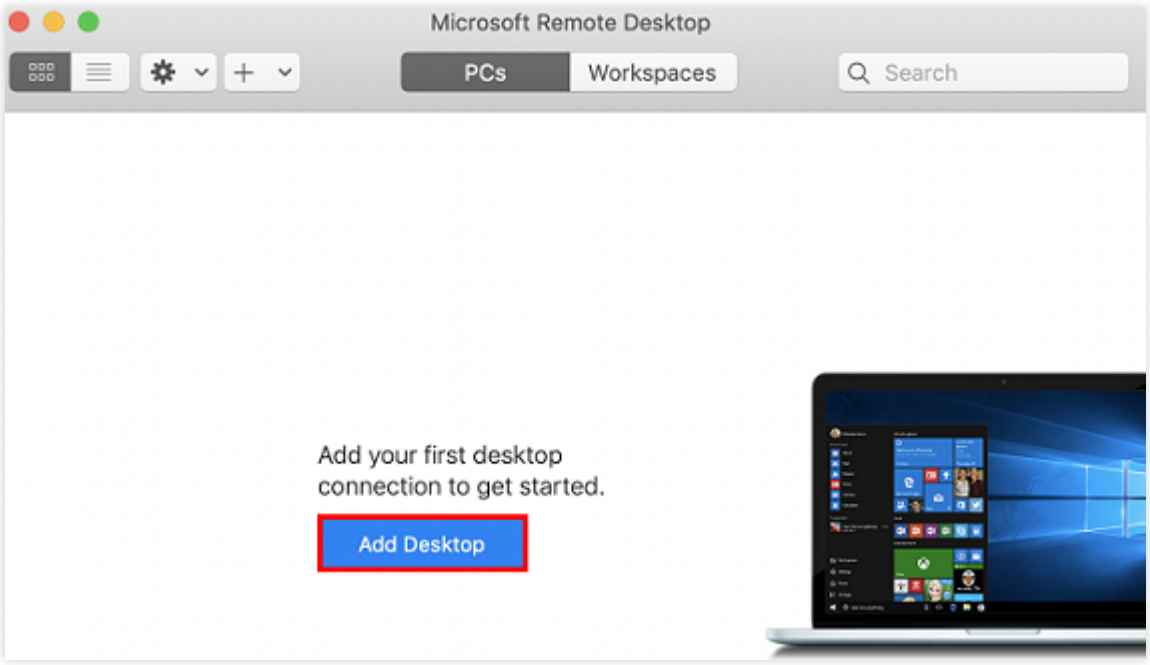
パブリックIPを取得する

CVMコンソール にログインし、インスタンスリストページに移動して、ファイルをアップロードするCVMのパブリックIPを記録します。次の図に示すように：

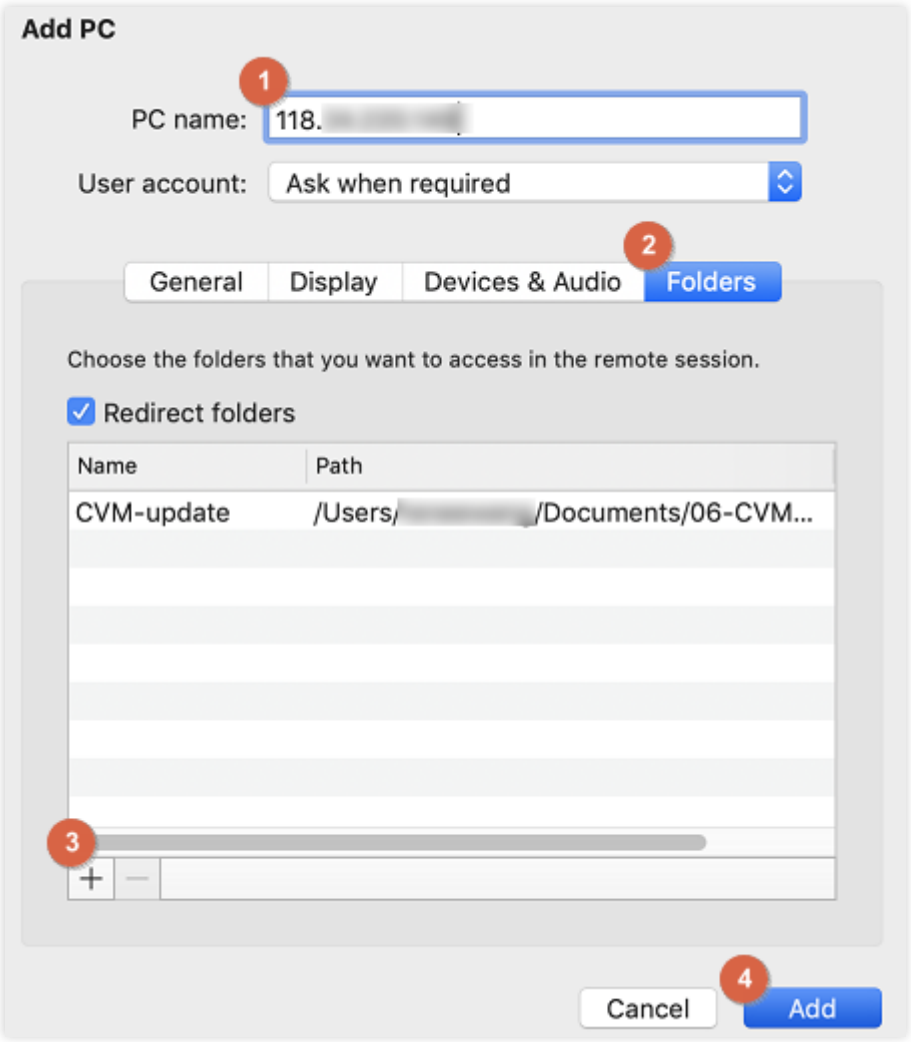


ファイルをアップロードする

1. MRDを起動し、**Add Desktop**をクリックします。次の図に示すように：



2. 表示されるダイアログボックスで、以下の手順に従って、アップロードするフォルダを選択し、Windows CVM との接続を確立します。次の図に示すように：



2.1 「PC name」に CVMのパブリックIPアドレスを入力します。

2.2 **Folders**をクリックして、フォルダリストに切り替えます。

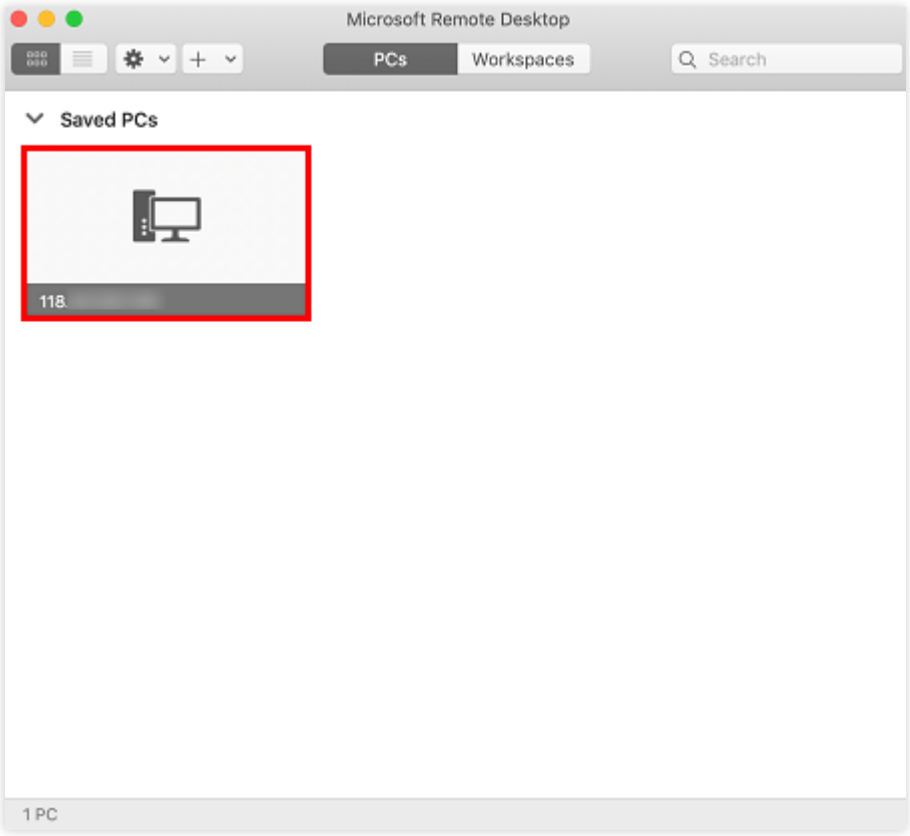
2.3 左下隅の

をクリックして、表示されるダイアログボックスでアップロードするフォルダを選択します。

2.4 選択が完了したら、アップロードするフォルダのリストを確認して、**Add**をクリックします。

2.5 他のオプションはデフォルト設定のままにして、接続を作成します。

ウィンドウで作成された接続を確認できます。次の図に示すように：



3. 新しく作成した接続をダブルクリックして開き、表示されるダイアログボックスでプロンプトに従って、CVMのアカウントとパスワードを入力し、**Continue**をクリックしてください。

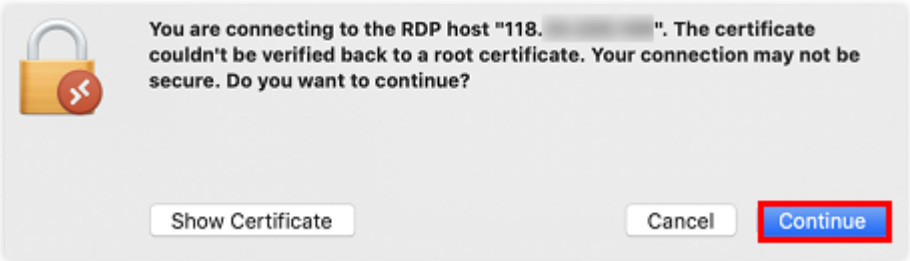
説明：

Windows CVMのデフォルトアカウントは `Administrator` です。

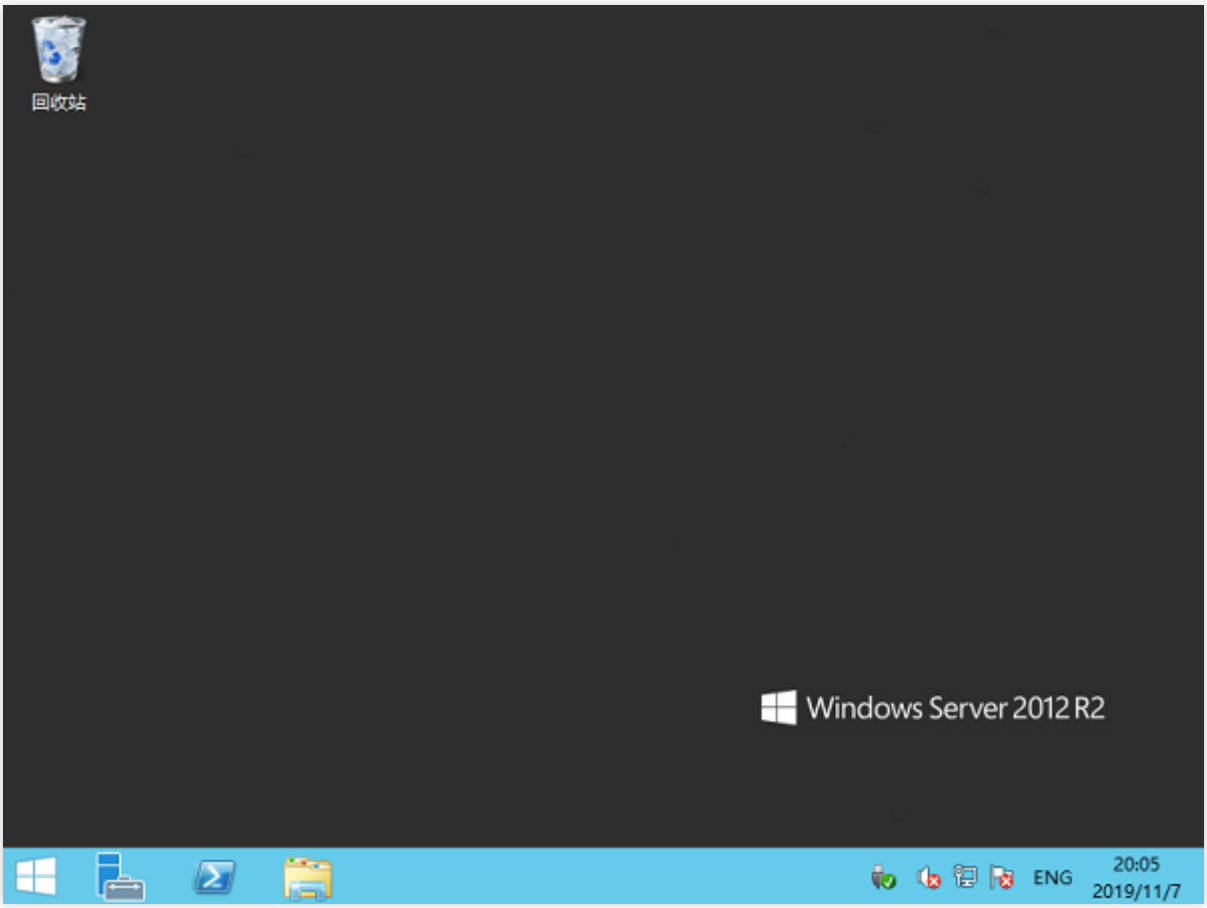
システムのデフォルトパスワードを使用してインスタンスにログインする場合は、サイト内メール にアクセスしてパスワードを取得してください。

パスワードを忘れた場合、インスタンスパスワードのリセット を行ってください。

4. 表示されるダイアログボックスで**Continue**をクリックして、接続を確立します。次の図に示すように：



接続が成功すると、次のページが表示されます。



5. 左下隅の

＞をクリックし、**My Computer**を選択して、共有フォルダが表示されます。

6. 共有フォルダをダブルクリックして開き、アップロードする必要があるローカルファイルをWindows CVMの別のドライブにコピーします。

例えば、フォルダ内のAファイルをWindows CVMのCドライブにコピーします。

ファイルをダウンロードする

Windows CVMからローカルコンピューターにファイルをダウンロードする必要がある場合は、必要なファイルをWindows CVMから共有フォルダにコピーして、ファイルのダウンロード操作を完了することができます。

LinuxシステムはRDPを介してWindows CVMにファイルをアップロードします

最終更新日：：2021-10-27 17:20:01

操作シナリオ

Rdesktopは、リモートデスクトッププロトコル(RDP)のオープンソースクライアントであり、Windows CVMへの接続などの操作に用いられます。ここでは、ローカルLinuxマシンからファイルを、rdesktopを介してWindows Server 2012 R2 OSのTencent CloudCloud Virtual Machine(CVM)にすばやくアップロードする方法についてご説明します。

説明：

ローカルLinuxマシンはビジュアルインターフェースを構築する必要があり、構築しないとrdesktopが使えません。

ここではLinuxマシンのOSに、CentOS 7.6を使用した場合を例として取り上げます。OSのバージョンによって手順が異なる場合がありますので、実際の業務状況に応じてドキュメントを参照して操作を行ってください。

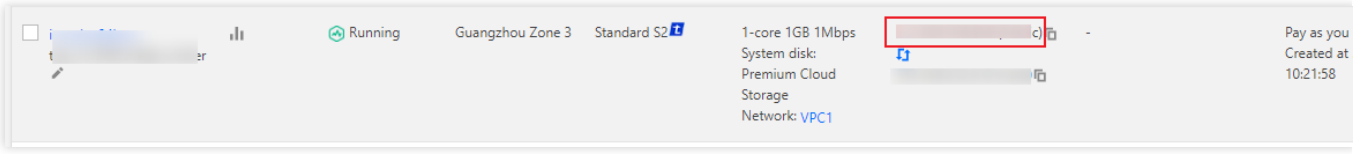
前提条件

Windows CVMを購入済みであること。

操作手順

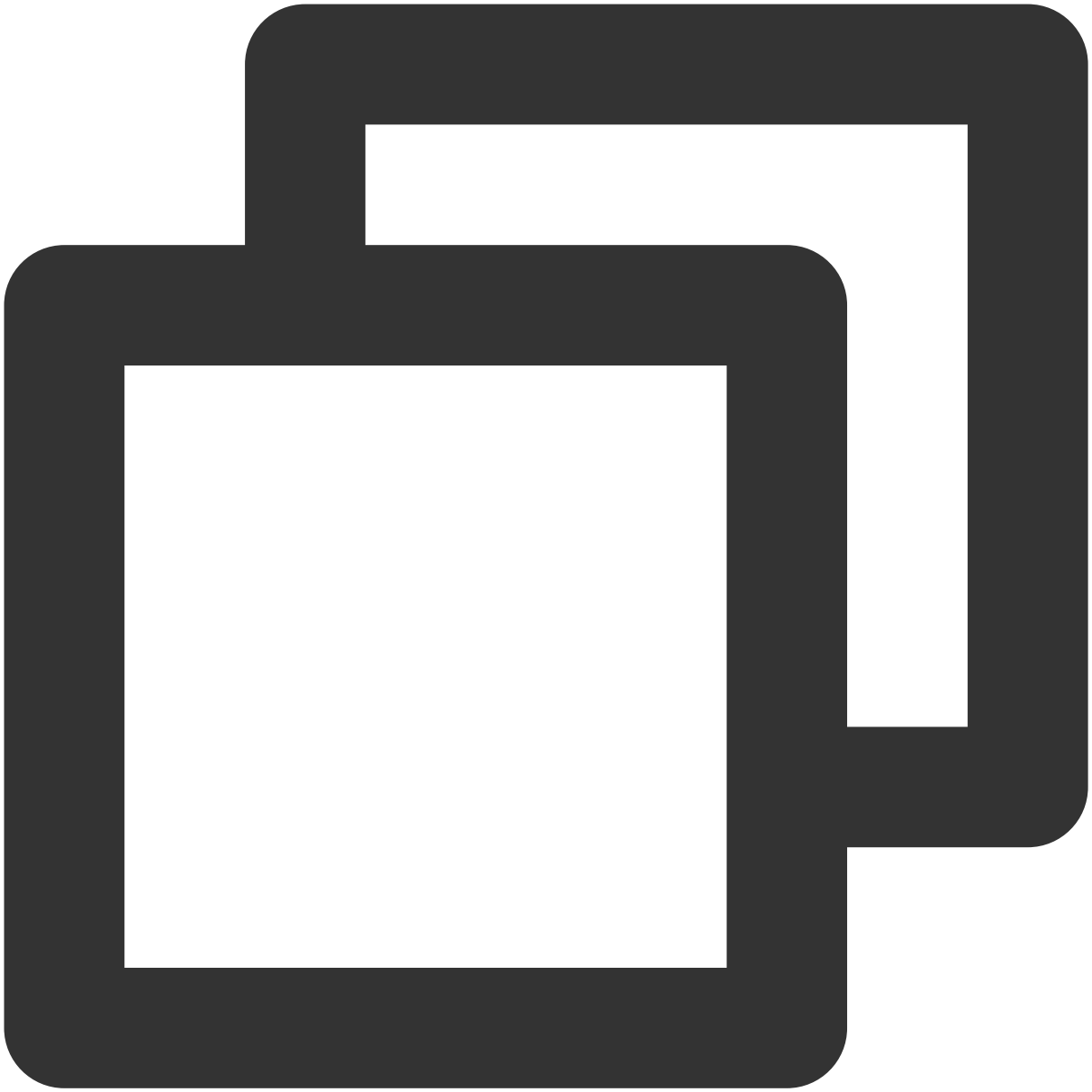
パブリックIPの取得

CVMコンソール にログインし、ファイルをアップロードするCVMのパブリックIPを、インスタンスリストページに記述します。下図に示すとおりです。



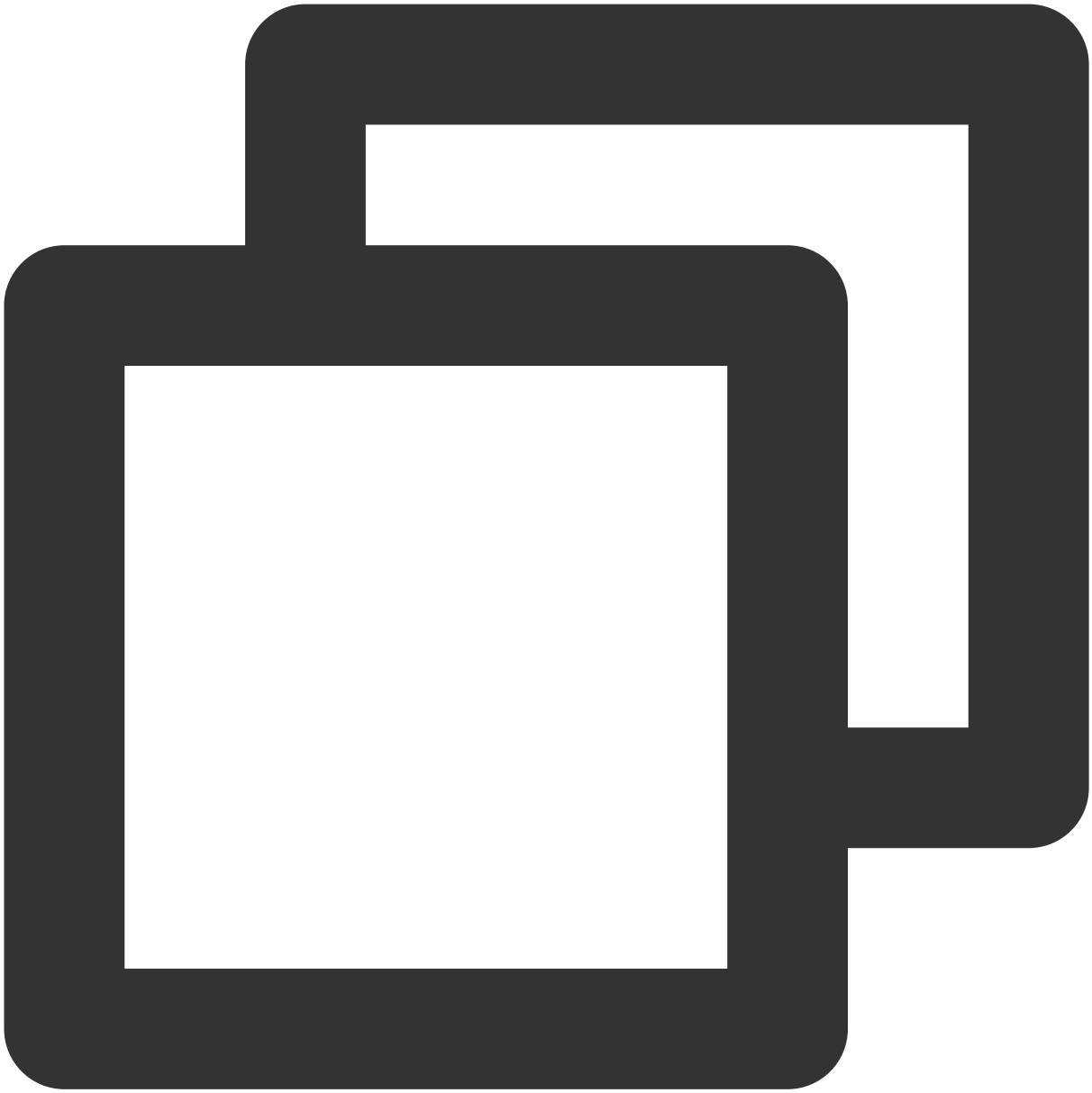
rdesktopのインストール

1. 端末で以下のコマンドを実行し、rdesktopのインストールパッケージをダウンロードします。この手順はrdesktop 1.8.3バージョンを例とします。

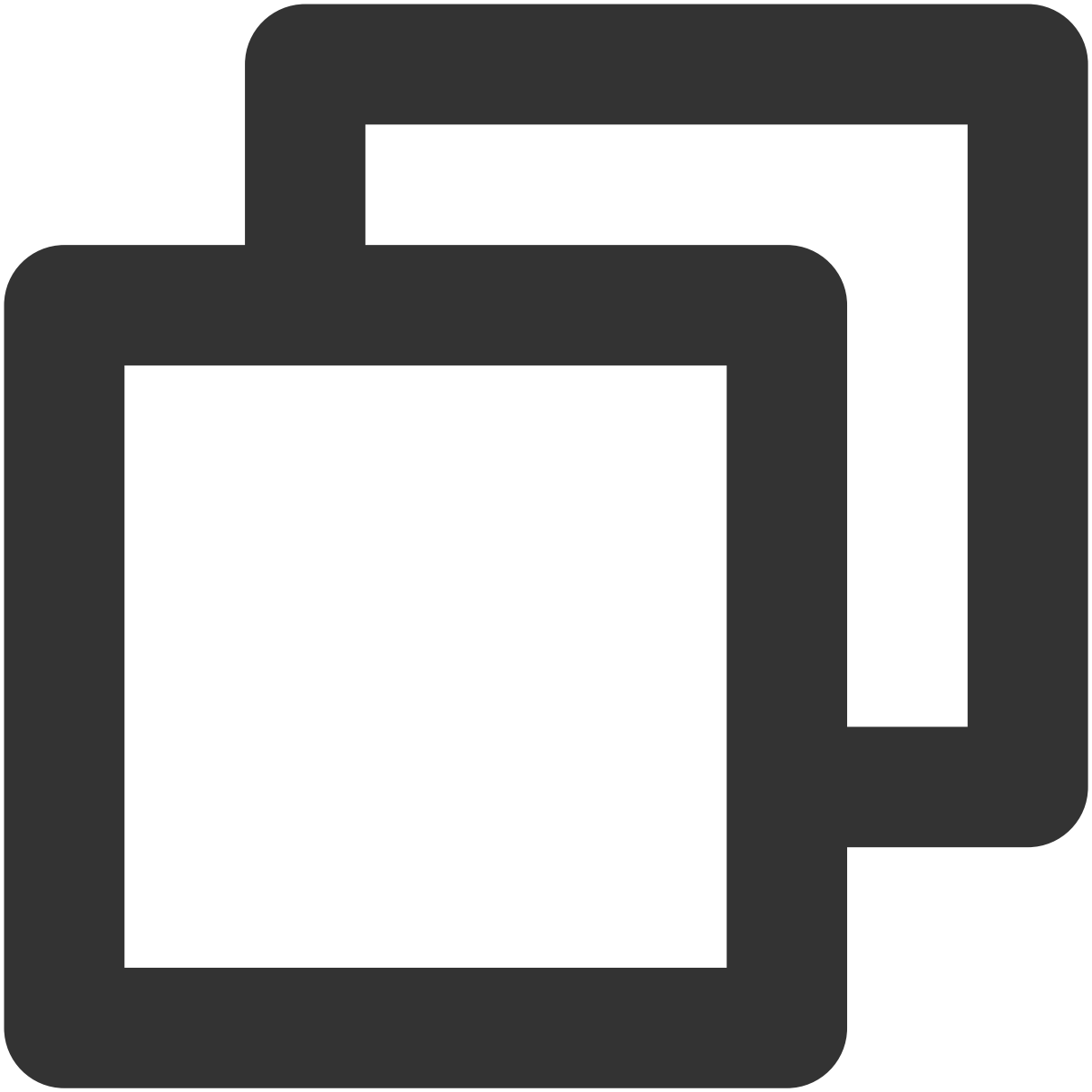


```
wget https://github.com/rdesktop/rdesktop/releases/download/v1.8.3/rdesktop-1.8.3.t
```

最新のインストールパッケージが必要な場合は、GitHub rdesktopページ にアクセスし、最新のインストールパッケージを検索して、コマンドラインで最新のインストールパスに置き換えることができます。
2. 次のコマンドを順番に実行して、インストールパッケージを解凍し、インストールディレクトリに入ります。

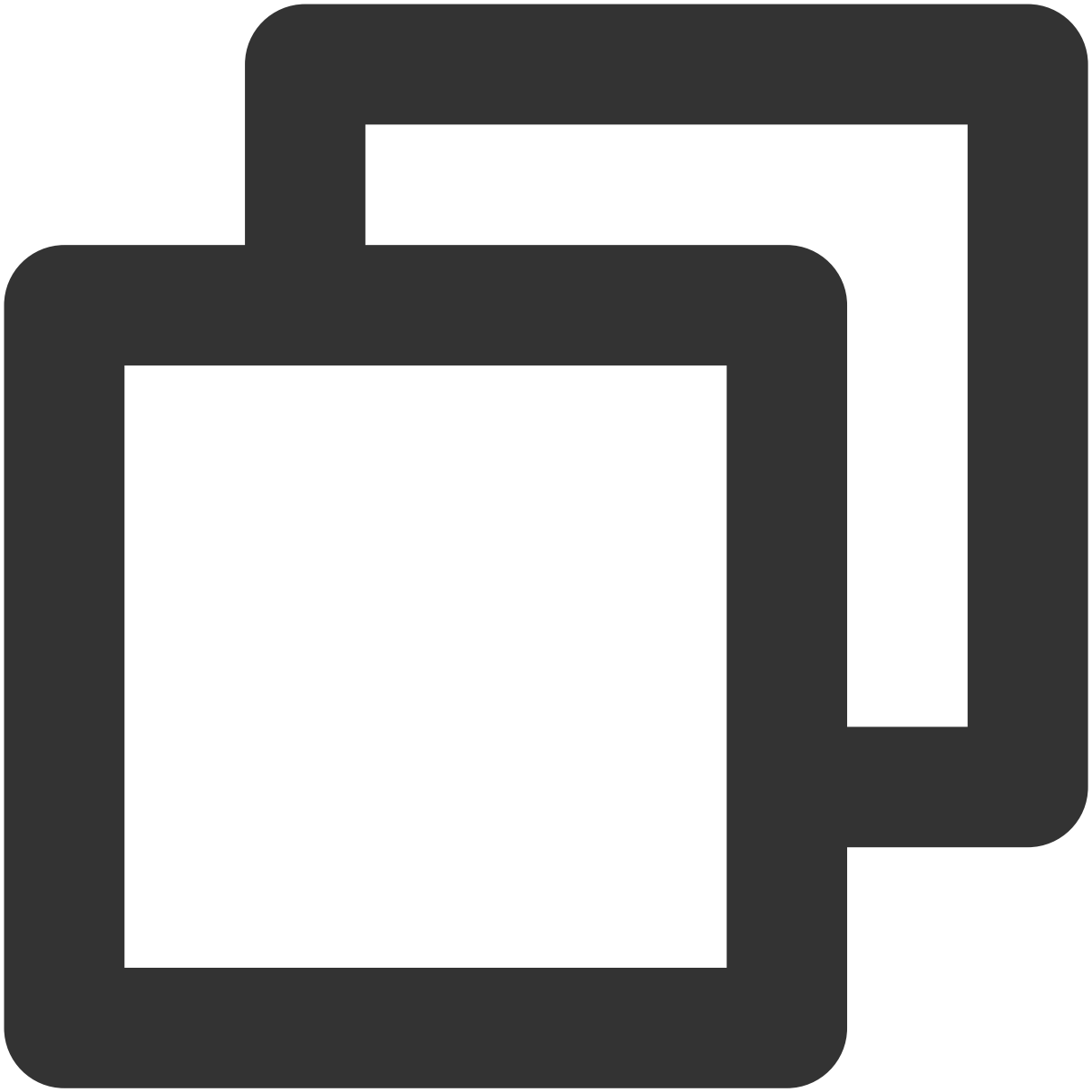


```
tar xvzf rdesktop-1.8.3.tar.gz
```

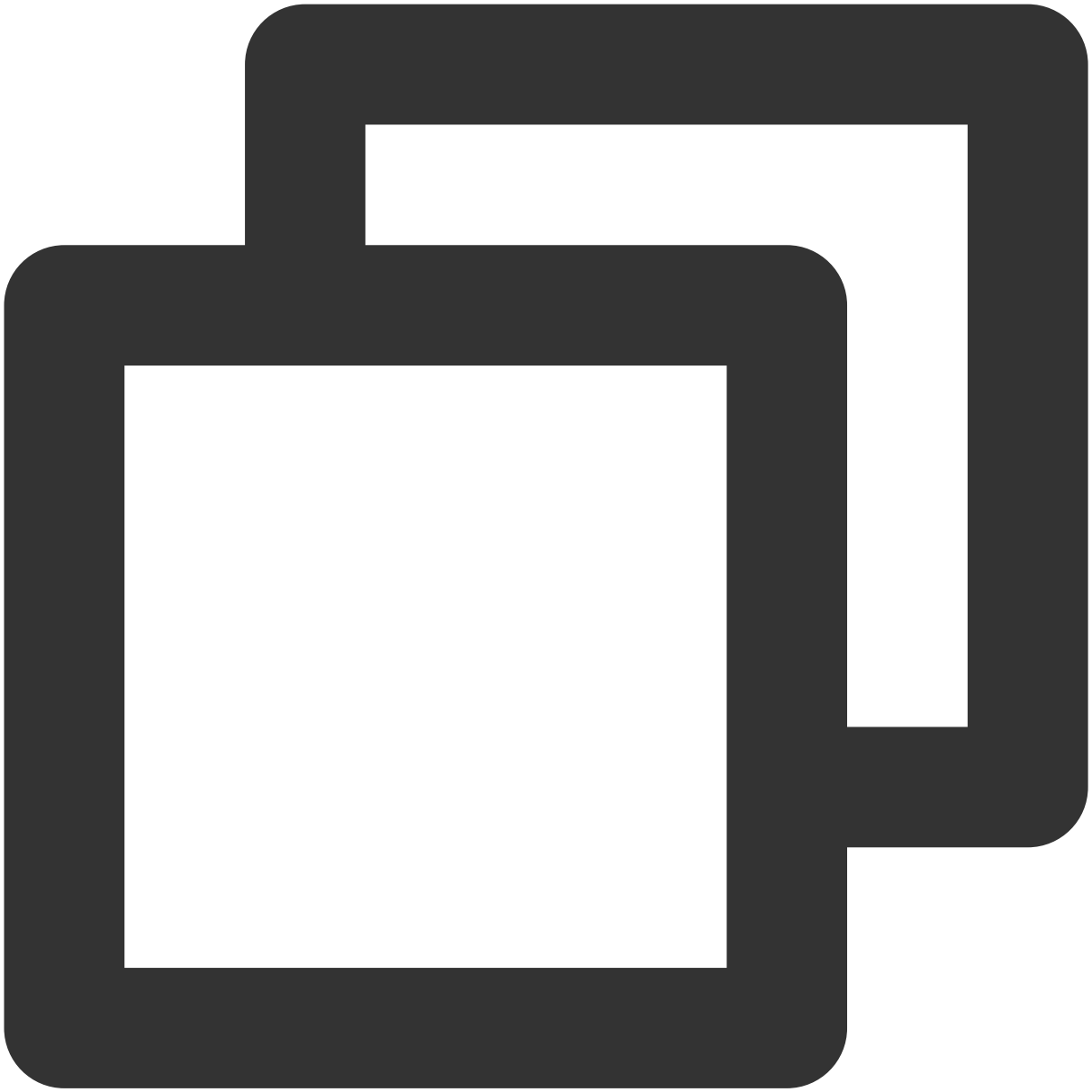


```
cd rdesktop-1.8.3
```

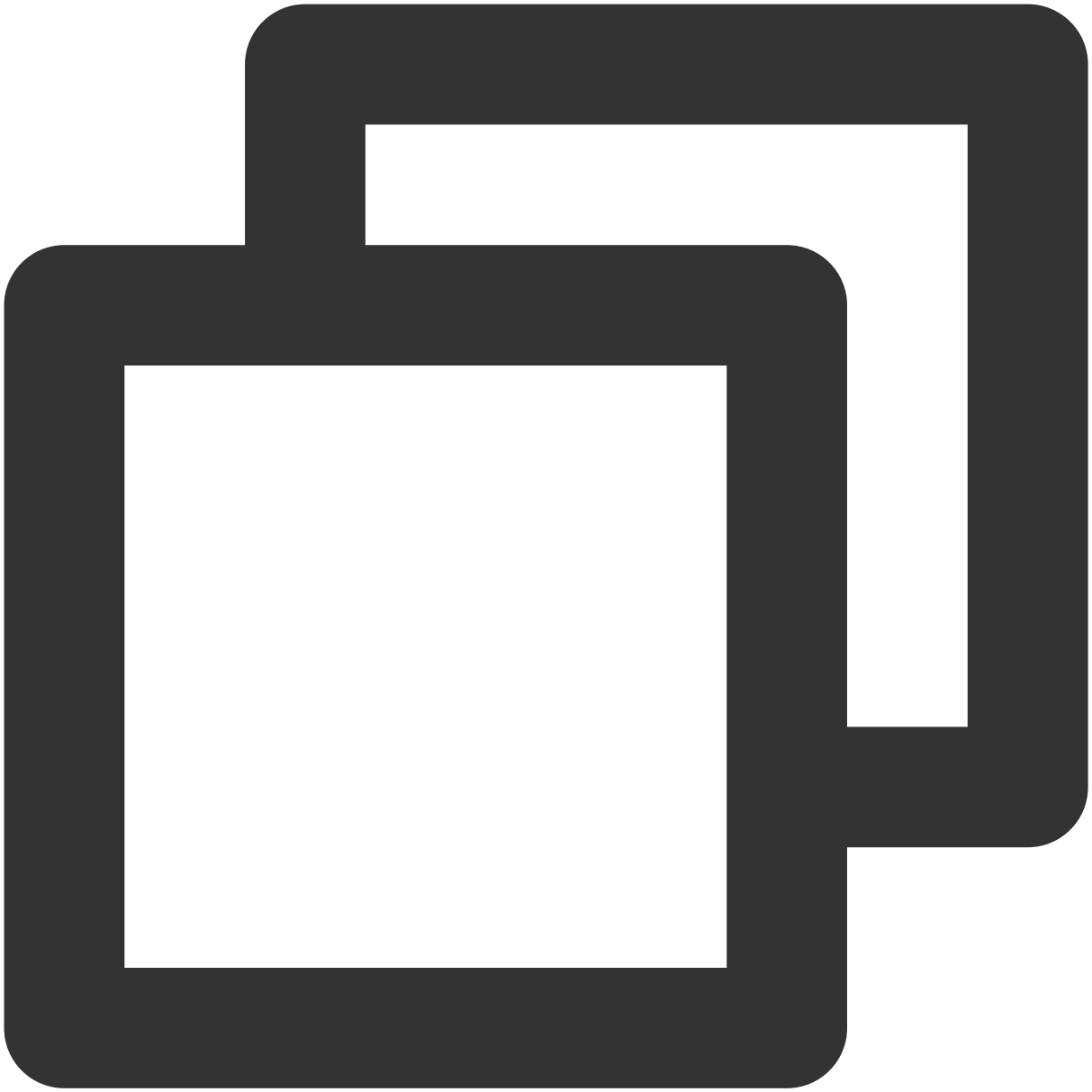
3. 次のコマンドを順番に実行して、rdesktopをコンパイルしてインストールします。



```
./configure
```

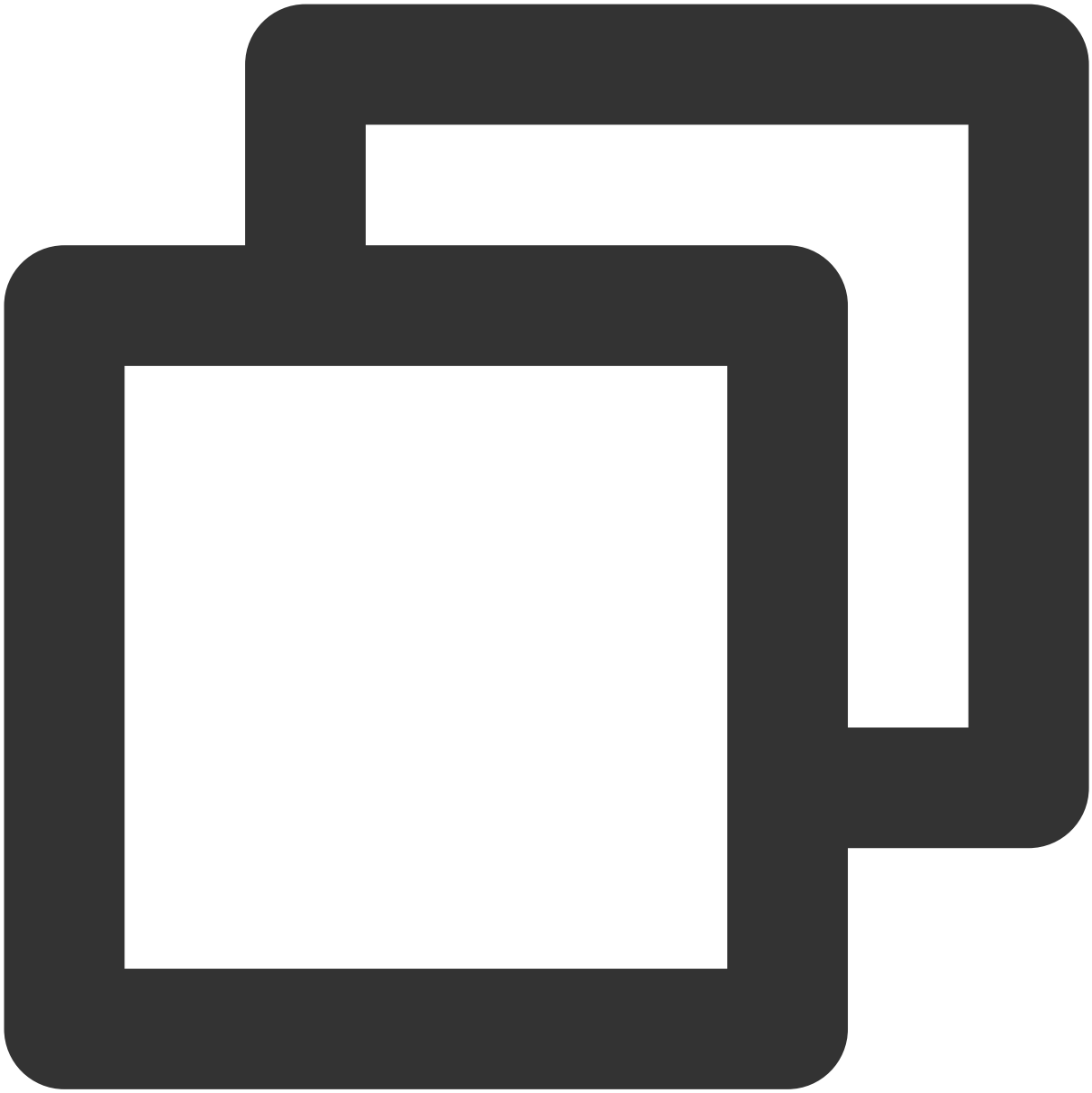


```
make
```



```
make install
```

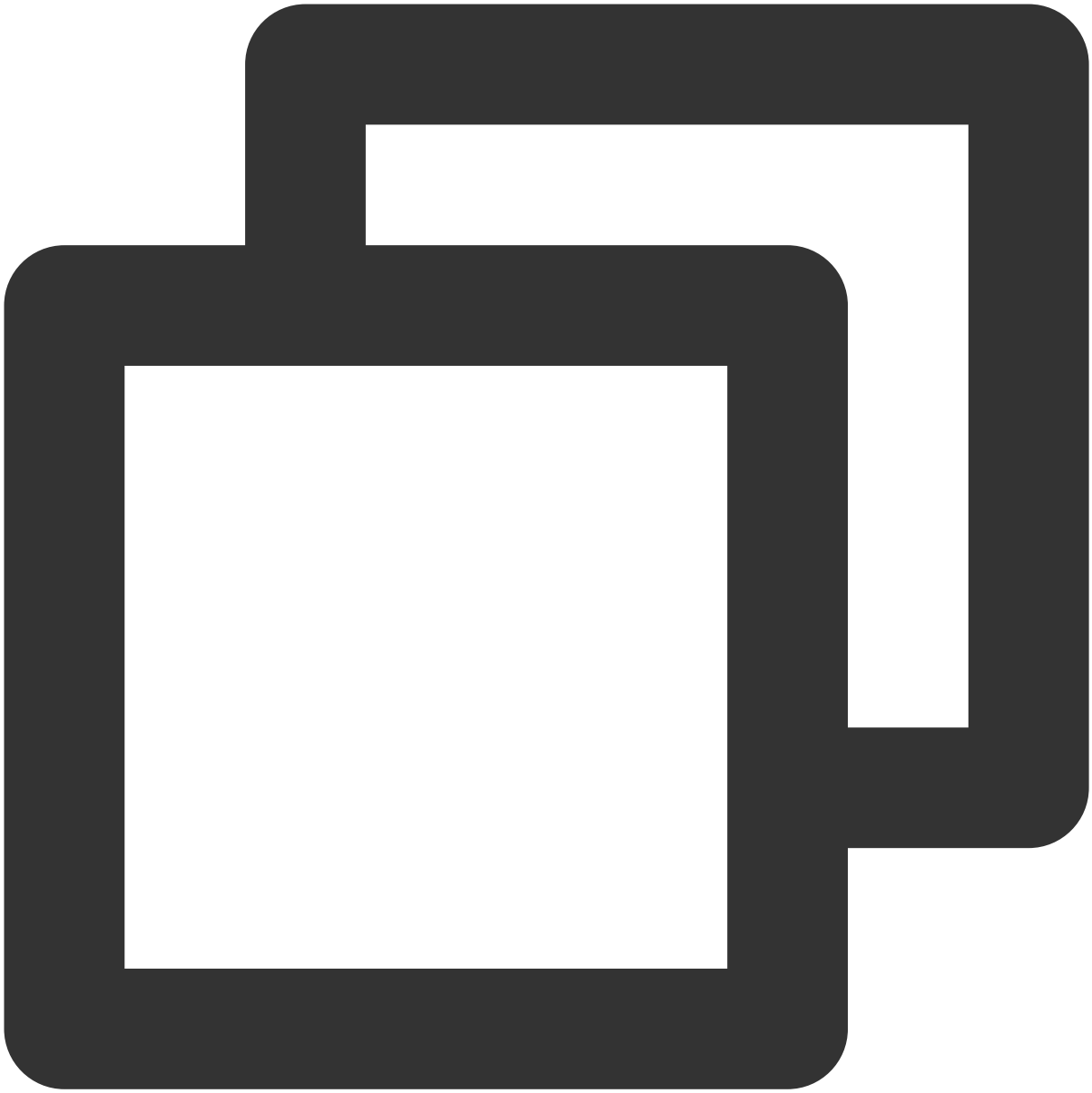
4. インストールが完了したら、次のコマンドを実行して、インストールが成功したかどうか確認します。



```
rdesktop
```

ファイルのアップロード

1. 次のコマンドを実行して、CVMと共有するフォルダを指定します。



```
rdesktopCVMパブリックIP  -u CVMアカウント -pCVMログインパスワード -r disk:指定された共有フォ
```

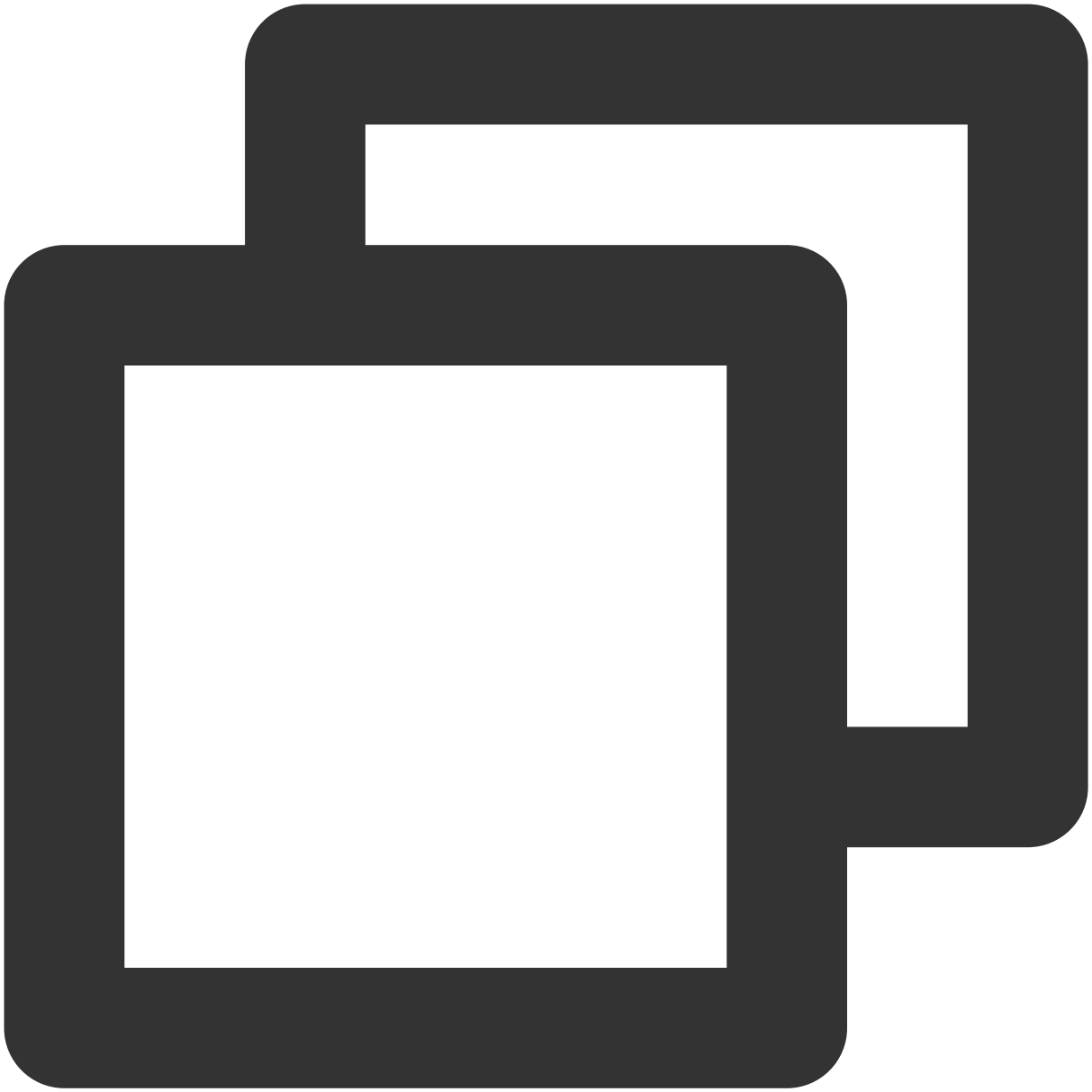
説明：

CVMのアカウントはデフォルトで `Administrator` となります。

システムのデフォルトパスワードを使用してインスタンスにログインする場合は、サイト内メッセージ に進んで取得してください。

パスワードを忘れた場合は、インスタンスのパスワードをリセット してください。

例えば、次のコマンドを実行して、ローカルコンピュータの `/home` フォルダを指定したCVMと共有し、共有フォルダ名を `share` に変更します。



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

共有が成功すると、Windows CVMのインターフェースが開きます。
左下隅にある

> **このコンピュータ**を選択し、CVMシステムインターフェースで共有フォルダを表示することができます。
2. ダブルクリックして共有フォルダを開き、Windows CVMの他のハードディスクにアップロードする必要がある
ローカルファイルをレプリケートすると、ファイルのアップロード操作は完了です。

例えば、 `share` フォルダ内のAファイルをWindows CVMのCドライブにレプリケートします。

ファイルのダウンロード

Windows CVMからローカルコンピュータにファイルをダウンロードする必要がある場合は、ファイルのアップロード操作を参照して、必要なファイルをWindows CVMから共有フォルダにレプリケートすると、ファイルのダウンロード操作は完了です。

WinSCPを介してWindowsからLinux CVMにファイルをアップロード

最終更新日：：2022-03-21 17:38:47

概要

WinSCPは、Windows環境でSSHを利用するオープンソースグラフィカルSFTPクライアントであり、SCPプロトコルもサポートします。WinSCPの主な機能は、ローカルとリモートコンピューター間でファイルを安全にコピーすることです。 FTPを使用してコードをアップロードすることと比較して、WinSCPはサーバー側で設定を行うことなく、サーバーのアカウントとパスワードを使用してサーバーに直接アクセスできます。

前提条件

ローカルコンピューターでWinSCPクライアントをダウンロードしてインストールしました。（ダウンロードURL：公式ウェブサイト 获取最新版本）から最新バージョンを取得することをお勧めします）。

操作手順

WinSCP にログインする

1. WinSCPを開くと、「WinSCPログイン」ダイアログボックスが表示されます。
2. ログインパラメータを設定する：

プロトコル：オプションSFTPまたはSCPのうちどちらでも構いません。
ホスト名：CVMのパブリックIPです。CVMコンソール にログインすると、対応するCVMのパブリックIPが確認できます。
ポート：デフォルトは22です。
ユーザー名：CVMにログインするためのユーザー名です。
説明：
Linuxインスタンスのデフォルトの管理者ユーザー名はroot、Ubuntuシステムのインスタンスはubuntuです。Ubuntu OSをお使いの場合は、Ubuntuシステムでrootユーザーを使用してインスタンスにログインする方法 を参照して構成した後、rootを使用してログインしてください。
パスワード：ユーザー名に対応するパスワードです。
システムのデフォルトパスワードを使用してインスタンスにログインする場合は、サイト内メール にアクセスしてパスワードを取得してください。

パスワードを忘れた場合は、インスタンスのパスワードをリセット してください。
3. **ログイン**をクリックして、「WinSCP」ファイル転送インターフェースに入ります。

ファイルのアップロード

1. 「WinSCP」ファイル転送インターフェースの右側のペインで、 `/user` など、ファイルをサーバーに保存するディレクトリを選択します。
2. 「WinSCP」ファイル転送インターフェースの左側のペインで、 `F:\\SSL証明書\\Nginx` など、ファイルをローカルコンピュータに保存するディレクトリを選択し、転送するファイルを選びます。
3. 「WinSCP」ファイル転送インターフェースの左側のメニューバーで、**アップロード**をクリックします。
4. 表示された「アップロード」ダイアログボックスで、アップロードするファイルとリモートディレクトリを確認し、**OK**をクリックすると、ローカルコンピュータからCVMにファイルがアップロードされます。

ファイルのダウンロード

1. 「WinSCP」ファイル転送インターフェースの左側のペインで、 `F:\\SSL証明書\\Nginx` など、ローカルコンピュータにダウンロードするストレージディレクトリを選択します。
2. 「WinSCP」ファイル転送インターフェースの右側のペインで、 `/user` など、ファイルをサーバーに保存するディレクトリを選択し、転送するファイルを選びます。
3. 「WinSCP」ファイル転送インターフェースの右側のメニューバーで、**ダウンロード**をクリックします。
4. 表示された「ダウンロード」ダイアログボックスで、ダウンロードするファイルとリモートディレクトリを確認し、**OK**をクリックすると、CVMからローカルコンピュータにファイルをダウンロードすることができます。

LinuxまたはMacOSマシンでSCPを介して ファイルをLinux CVMにアップロード

最終更新日：：2022-07-08 18:53:29

概要

このドキュメントではCentOS 8.2オペレーティングシステムにおけるTencent CloudのCloud Virtual Machine（CVM）を例として、SCPを使用してLinux CVMにファイルをアップロードまたはダウンロードします。

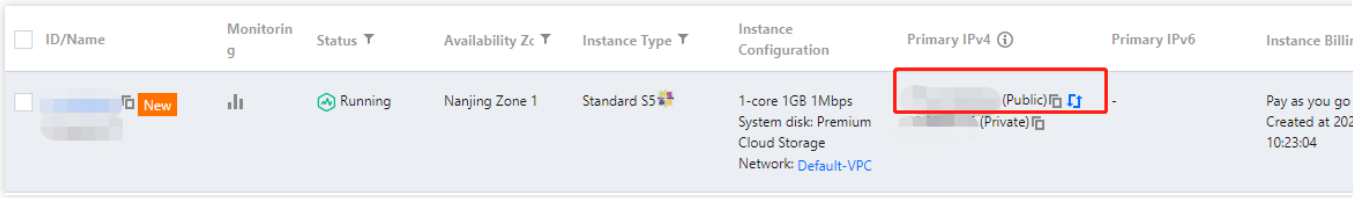
前提条件

Linux CVMを購入済みであること。

操作手順

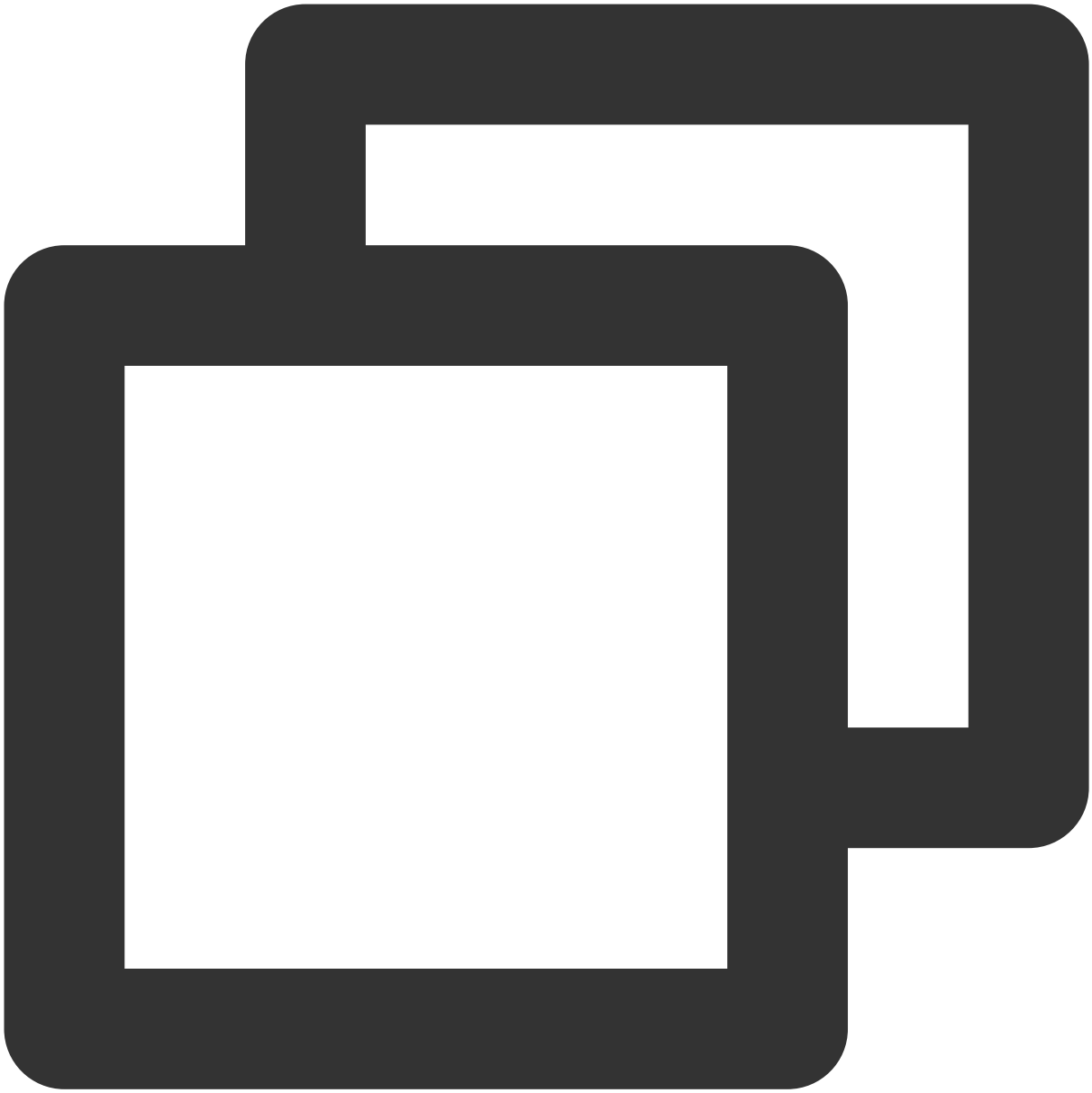
パブリックIPの取得

CVMコンソール にログインし、ファイルをアップロードするCVMのパブリックIPを、インスタンスリストページに記述します。下図に示すとおりです。



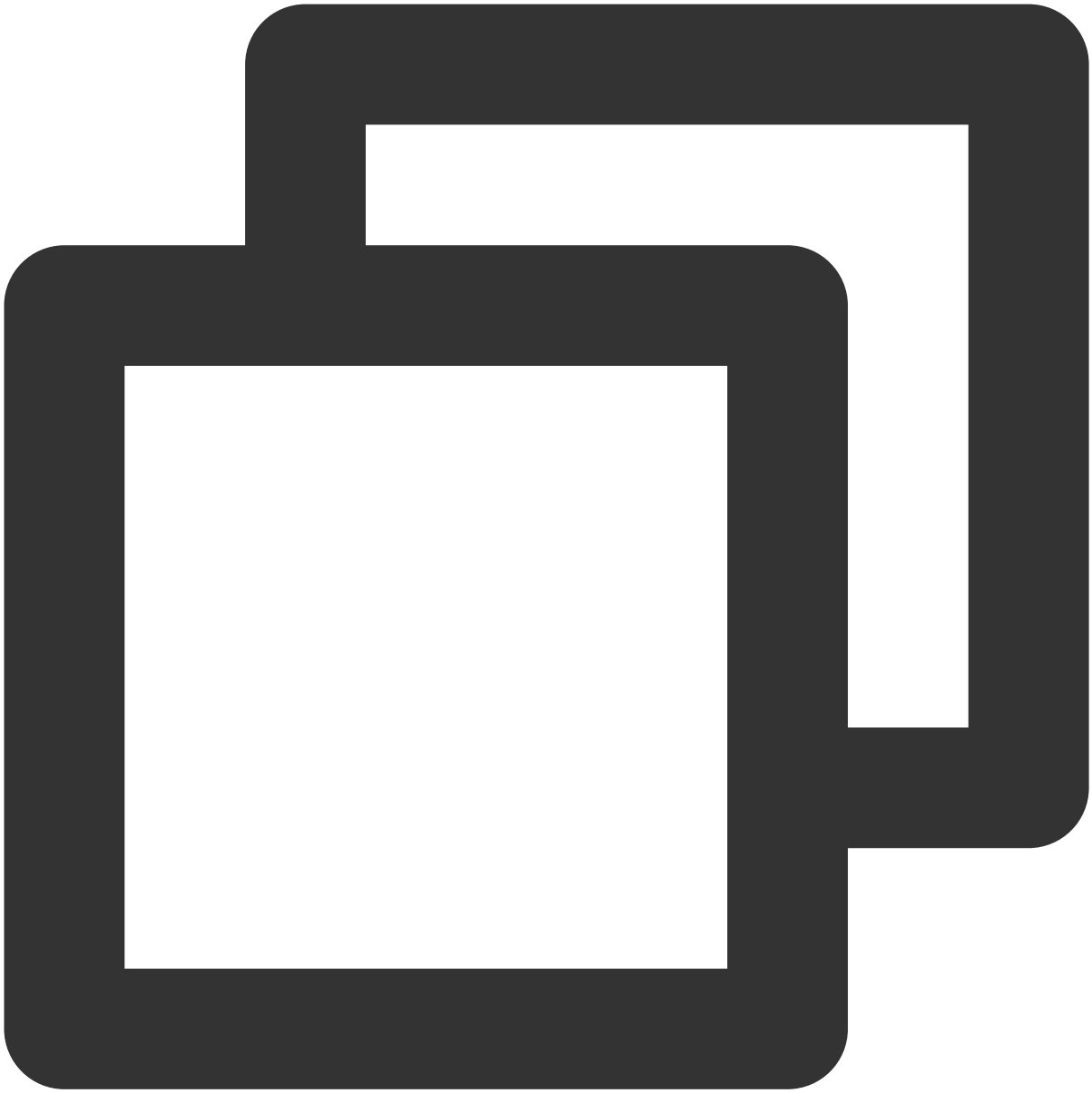
ファイルのアップロード

1. 次のコマンドを実行して、Linux CVMにファイルをアップロードします。



```
scpローカルファイルアドレス CVMアカウント@CVMインスタンスのパブリックIP/ドメイン名:CVMファイルア
```

例えば、ローカルファイル `/home/lnmp0.4.tar.gz` をIPアドレスが `129.20.0.2` のCVMの対応ディレクトリにアップロードする必要がある場合、実行するコマンドは以下のようになります。



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

説明：

`-r` パラメータを追加することでフォルダをアップロードすることができます。より多くのscpコマンドの機能をお知りになりたい場合は、 `man scp` を実行して情報を取得することができます。

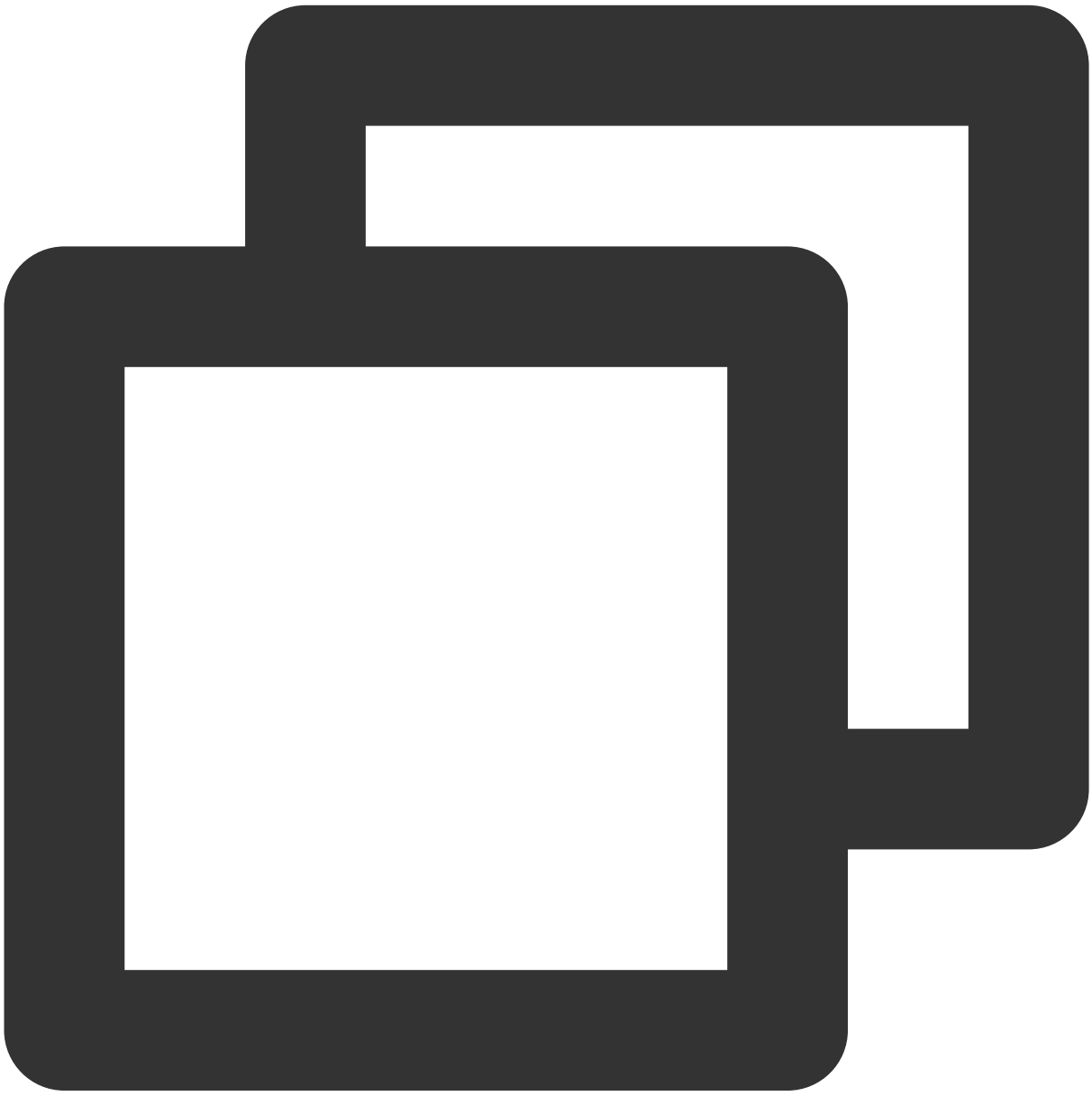
2. **yes**を入力してから**Enter**を押してアップロードを確認し、ログインパスワードを入力すると、アップロードが完了します。

システムのデフォルトパスワードを使用してインスタンスにログインする場合は、サイト内メール にアクセスしてパスワードを取得してください。

パスワードを忘れた場合は、インスタンスのパスワードをリセット してください。

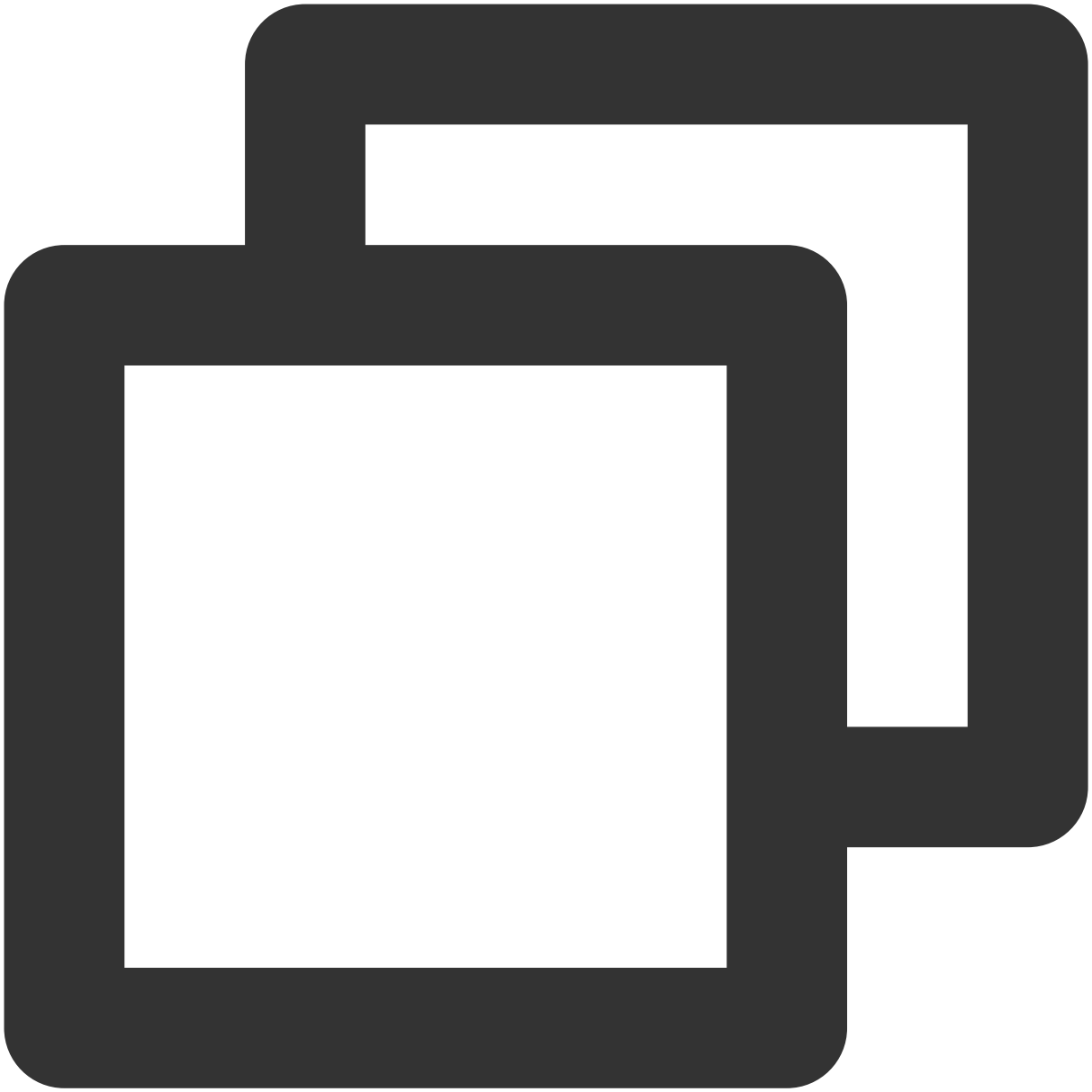
ファイルのダウンロード

次のコマンドを実行して、Linux CVM上のファイルをローカルにダウンロードします。



```
scp CVMアカウント@CVMインスタンスのパブリックIP/ドメイン名:CVMファイルアドレス ローカルファイル
```

例えば、IPアドレスが `129.20.0.2` であるCVMのファイル `/home/lnmp0.4.tar.gz` をローカルの対応ディレクトリにダウンロードする必要がある場合、実行するコマンドは以下のようになります。



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

LinuxシステムはFTP経由でファイルをCVMにアップロード

最終更新日：：2020-07-23 17:27:10

操作シナリオ

このドキュメントでは、LinuxシステムのローカルPC上でFTPサービスを使用して、ファイルをローカルからCVMにアップロードする方法について説明します。

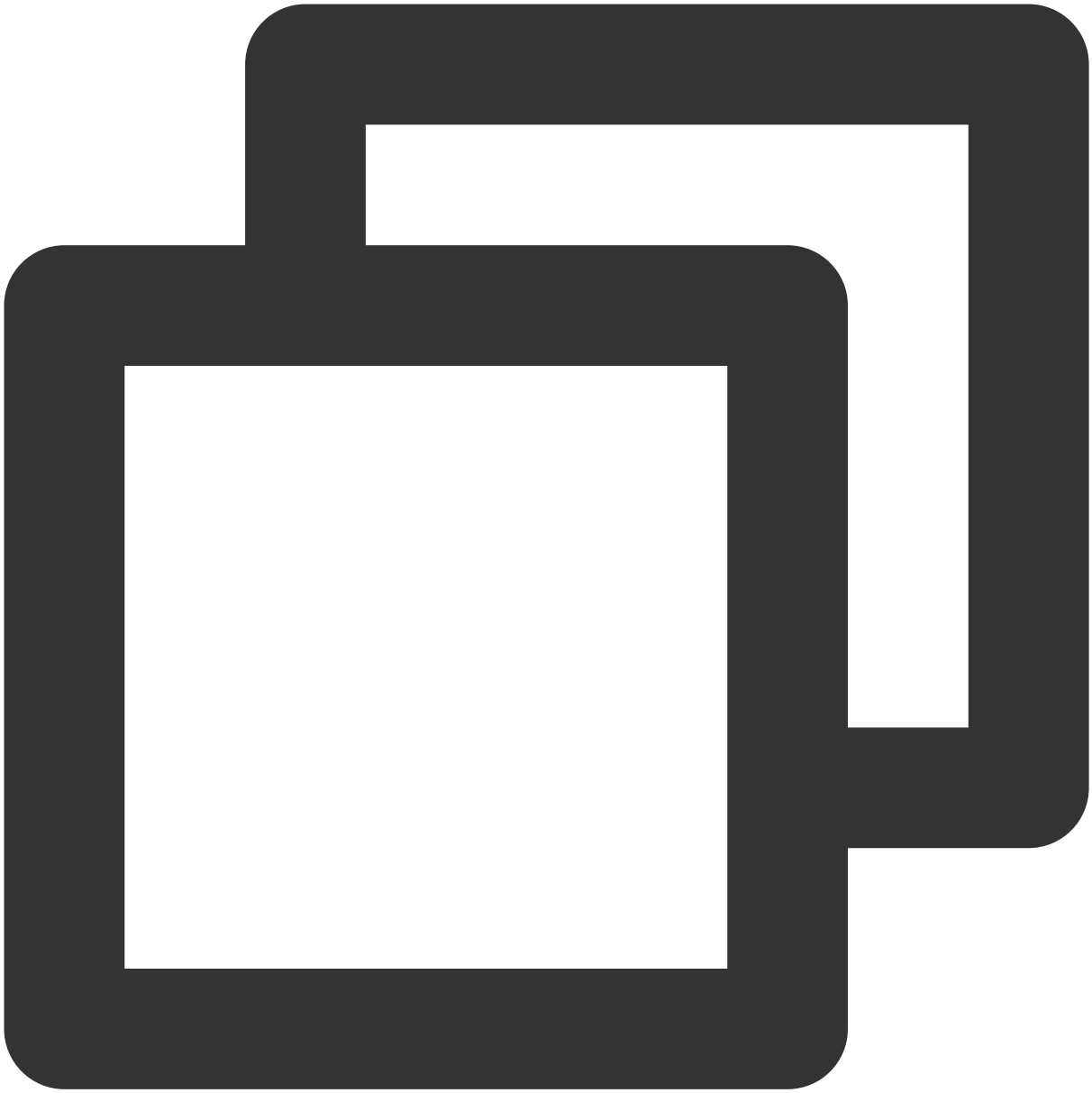
前提条件

Cloud Virtual Machine(CVM)にFTPサービスを構築済み。
FTPを使用してファイルをLinux CVMにアップロードするには、Linux CVMでFTPサービスの構築 をご参照ください。
FTPを使用してファイルをWindows CVMにアップロードするには、Windows CVMでFTPサービスの構築 をご参照ください。

操作手順

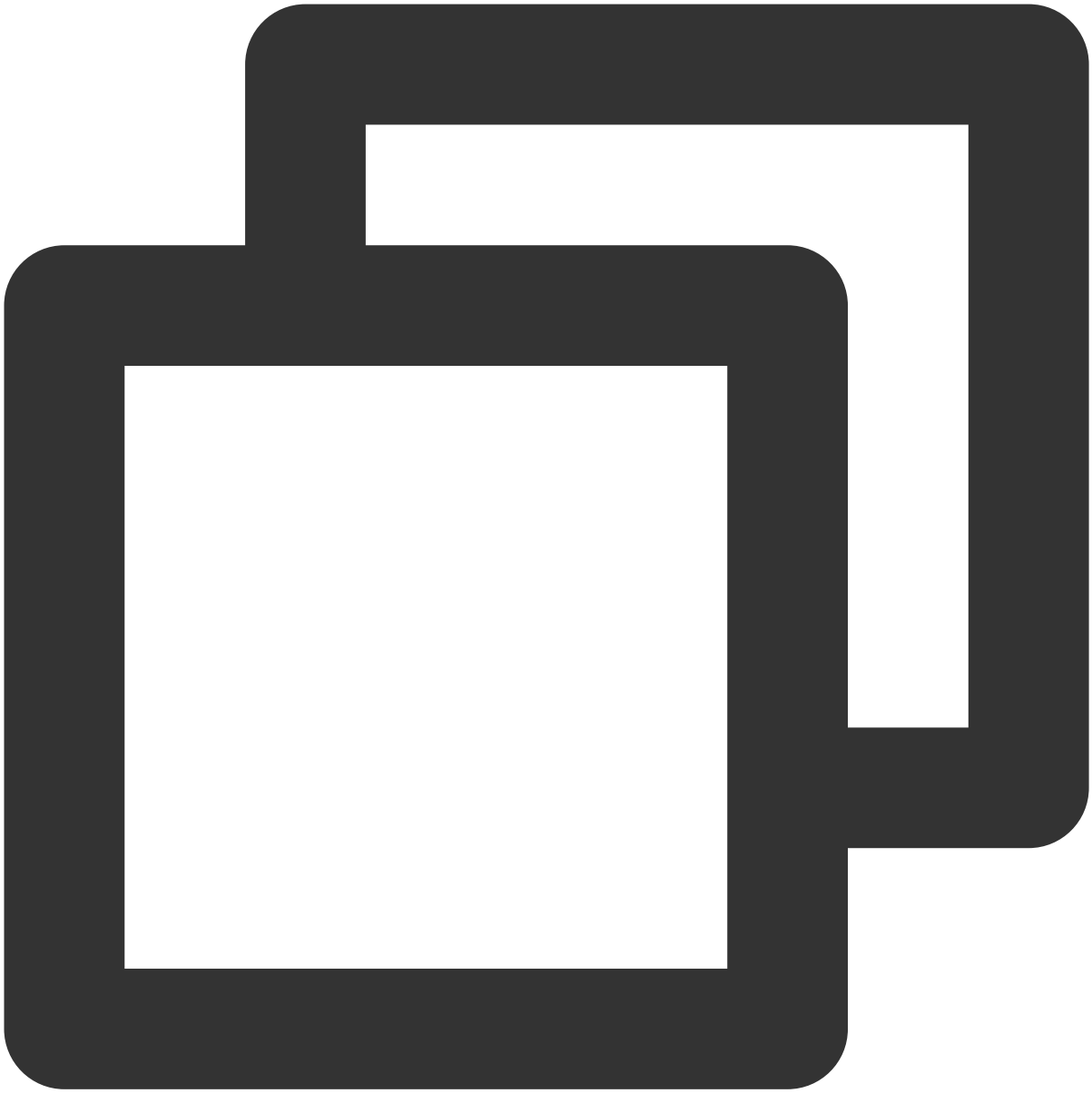
CVMへの接続

1. 次のコマンドを実行し、FTPサービスをインストールします。
説明：
LinuxシステムのローカルPCにFTPサービスがインストールされている場合は、このステップをスキップして次に進んでください。



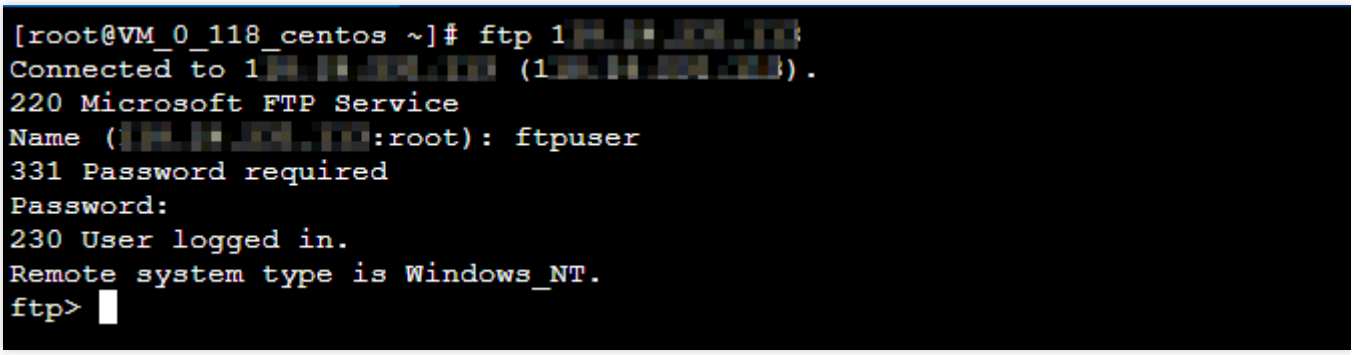
```
yum -y install ftp
```

2. 次のコマンドを実行し、ローカルPCでCVMに接続します。画面の指示に従って、FTPサービスのアカウントとパスワードを入力します。



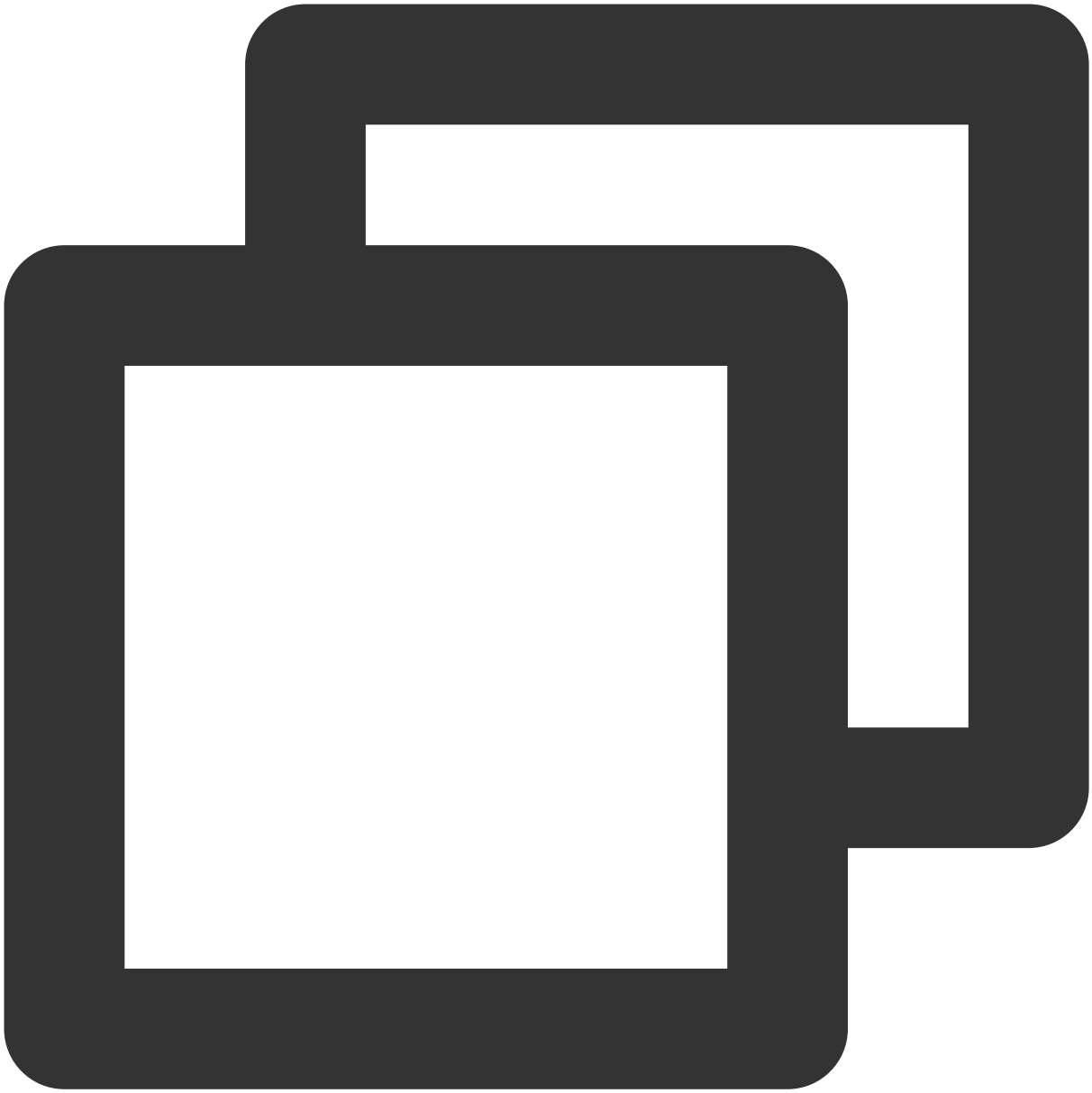
```
ftp CVMのIPアドレス
```

次の画面に進むと、接続は正常に確立されています。



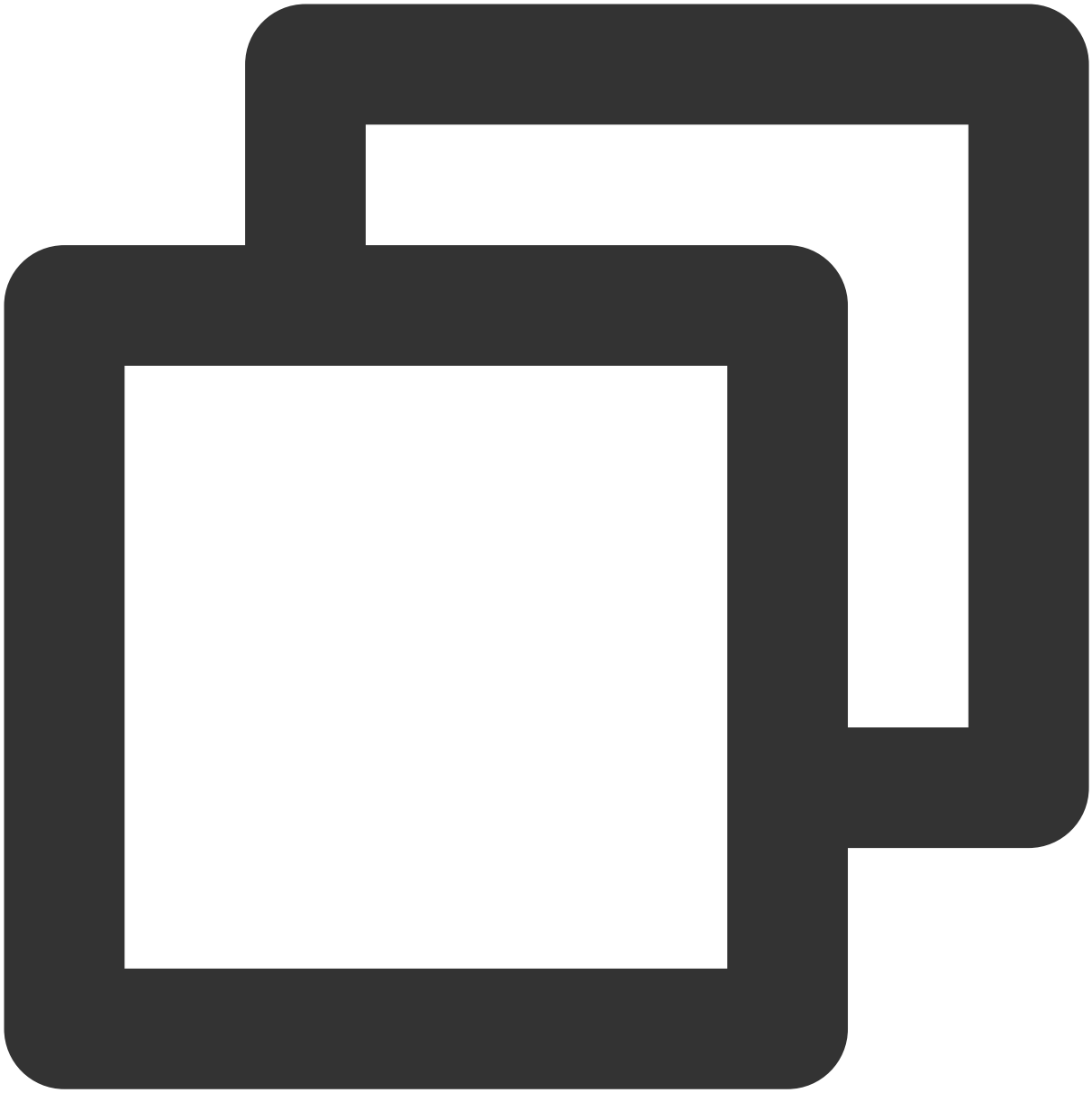
ファイルのアップロード

次のコマンドを実行して、ローカルファイルをCVMにアップロードします。



```
put local-file [remote-file]
```

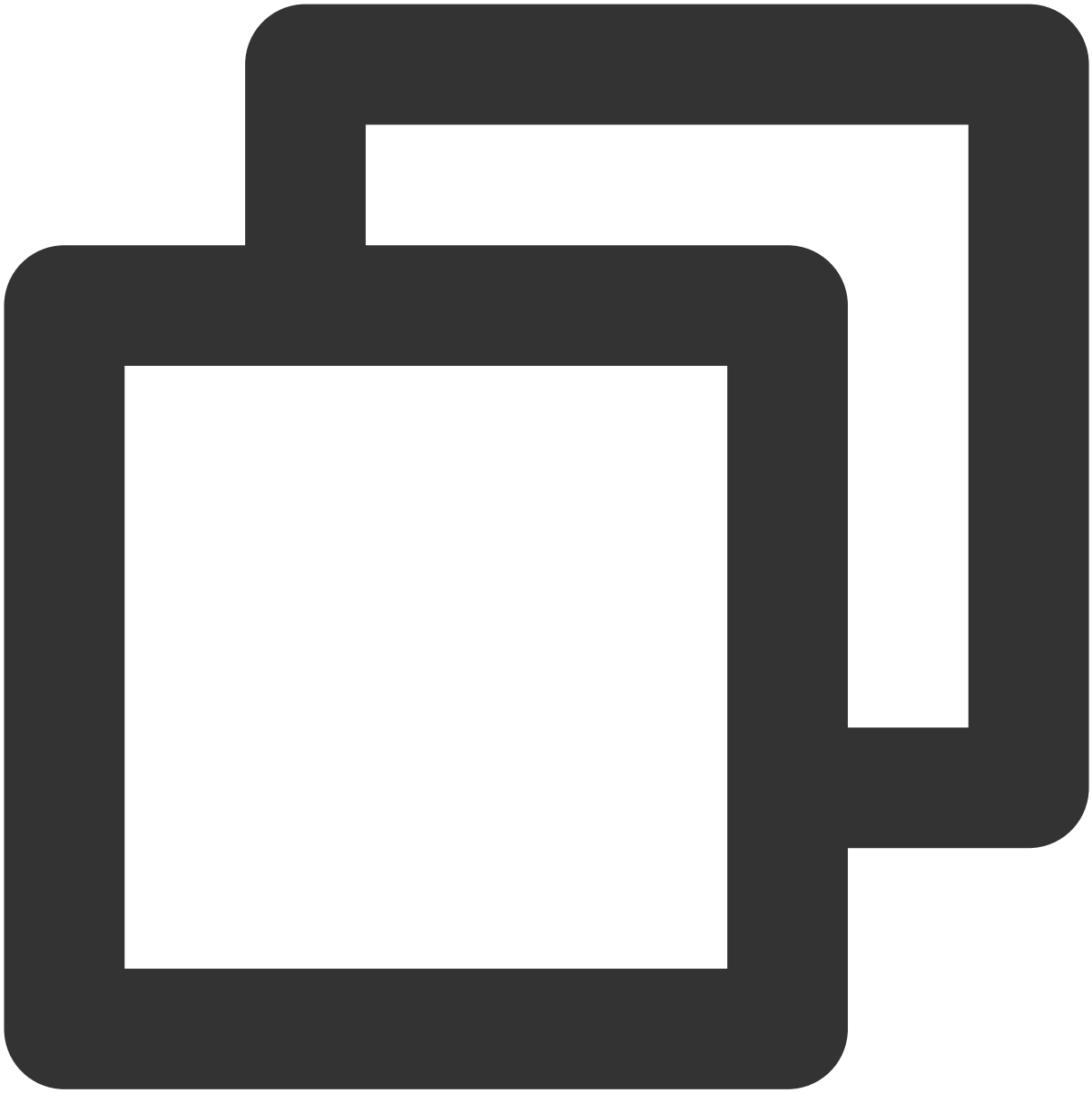
たとえば、ローカルファイル `/home/1.txt` をCVMにアップロードします。



```
put /home/1.txt 1.txt
```

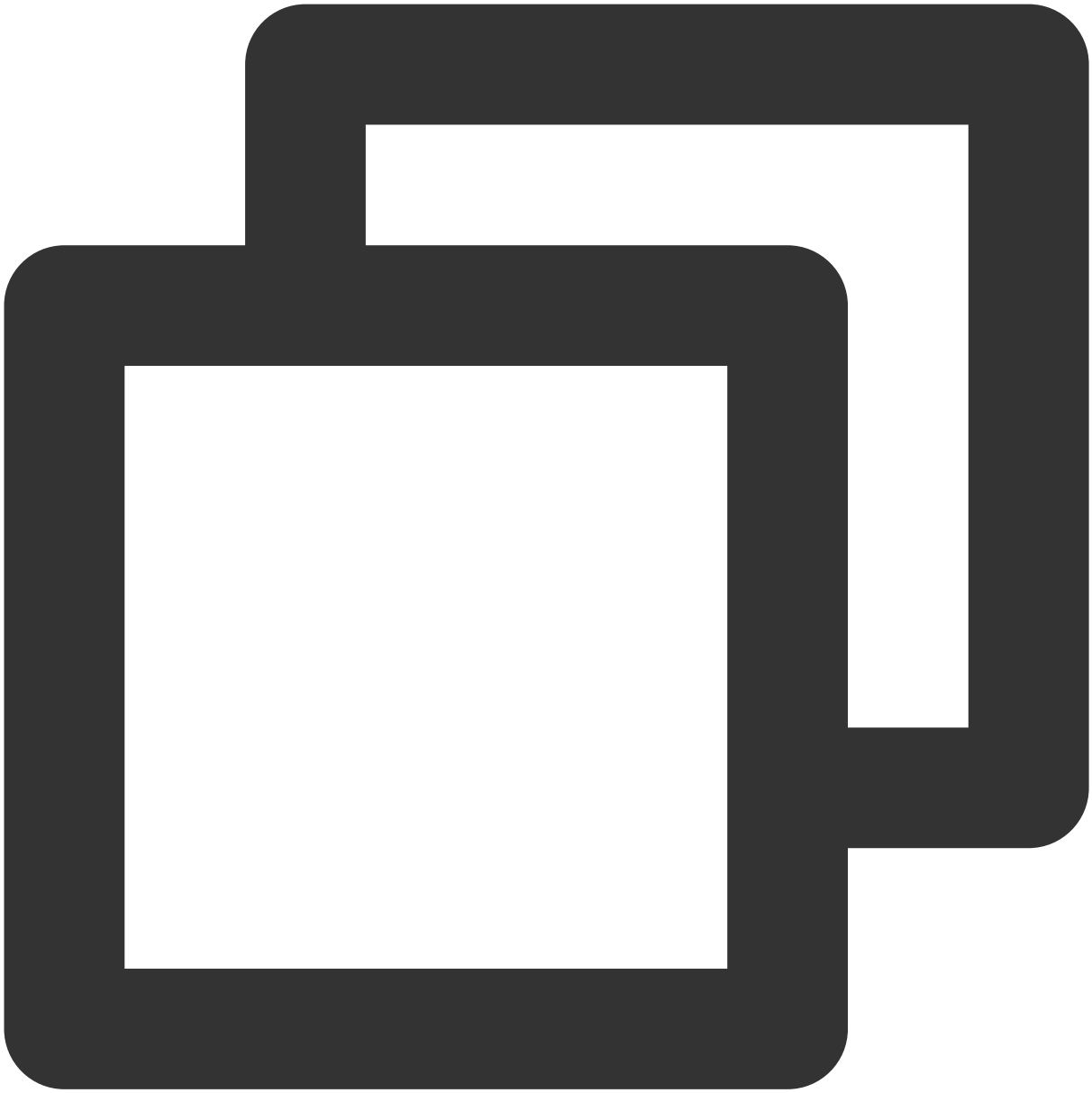
ファイルのダウンロード

次のコマンドを実行して、CVM上のファイルをローカルディレクトリにダウンロードします。



```
get [remote-file] [local-file]
```

たとえば、CVM上の `A.txt` ファイルをローカルの `/ home` ディレクトリにダウンロードします。



```
get A.txt /home/A.txt
```

Windows OSからFTPを利用して、CVMにファイルをアップロードする

最終更新日：：2022-07-27 11:43:01

操作シナリオ

このドキュメントでは、Windowsシステムのローカルコンピューターで FTPサービスを使用して、ファイルをローカルからCVMにアップロードする方法について説明します。

前提条件

Cloud Virtual Machine(CVM)にFTPサービスを構築済み。
FTPを使用してファイルをLinux CVMにアップロードするには、Linux CVMでFTPサービスの構築 をご参照ください。
FTPを使用してファイルをWindows CVMにアップロードするには、Windows CVMでFTPサービスの構築 をご参照ください。

操作手順

CVMへの接続

1. オープンソースソフトウェアFileZillaをローカルでダウンロードしてインストールします。
説明：
バージョン3.5.3のFileZillaを使用してFTP経由でファイルをアップロードすると、アップロードが失敗する場合があります。公式WebサイトからFileZillaのバージョン3.5.1または3.5.2をダウンロードして使用することをお勧めします。
2. FileZillaを開きます。
3. FileZillaウィンドウで、ホスト、ユーザー名、パスワード、ポートなどの情報を入力して、**クイック接続**をクリックします。
設定情報の説明：
ホスト：CVMのパブリックIPです。 CVMコンソール のインスタンス管理画面で、CVMのパブリックIPを確認できます。
ユーザー名：FTPサービスの構築 で設定されたFTPユーザーのアカウントです。 図では、「ftpuser1」を例に説明します。

パスワード：FTPサービスの構築で設定されたFTPユーザーアカウントに対応するパスワードです。
ポート：FTPリスニングポートです。デフォルトは**21**です。
接続が成功したら、リモートCVMサイトでファイルを表示できます。

ファイルのアップロード

左下の「ローカルサイト」ウィンドウで、アップロードするローカルファイルを右クリックし、**アップロード**を選択すると、Linux CVMにファイルを以下の図に示すようにアップロードします。

ご注意：

CVM FTPパスは、アップロードされた圧縮tarファイルの自動解凍または削除をサポートしていません。
リモートサイトパスは、Linux CVMにファイルをアップロードするためのデフォルトパスです。

ファイルのダウンロード

右下の「リモートサイト」ウィンドウで、ダウンロードするCVMファイルを右クリックし、**ダウンロード**を選択すると、ファイルをローカルディレクトリにダウンロードします。

その他のCVM操作

最終更新日：：2021-08-12 11:00:57

このドキュメントでは、一般的なCVM操作をご紹介します。必要に応じて、次のコンテンツを参照して操作できます。

Ubuntuビジュアルインターフェースを構築する
ローカルファイルをCVMにコピーする方法
Linux CVMでのデータ回復
Windows CVMでのディスク領域の管理
オフライン移行
アベイラビリティーゾーン間でTencent Cloud CVMデータを移行
アカウント間でTencent Cloud CVMデータを移行
AWS EC2からTencent Cloud CVMへのデータ移行
Alibaba Cloud ECSからTencent Cloud CVMへのデータ移行

操作中に問題が発生した場合は、ユースケースに関するFAQ ドキュメントを参照して問題のトラブルシューティングを行ってください。

CVMのプライベートネットワークによるCOSへのアクセス

最終更新日：：2023-06-30 15:28:14

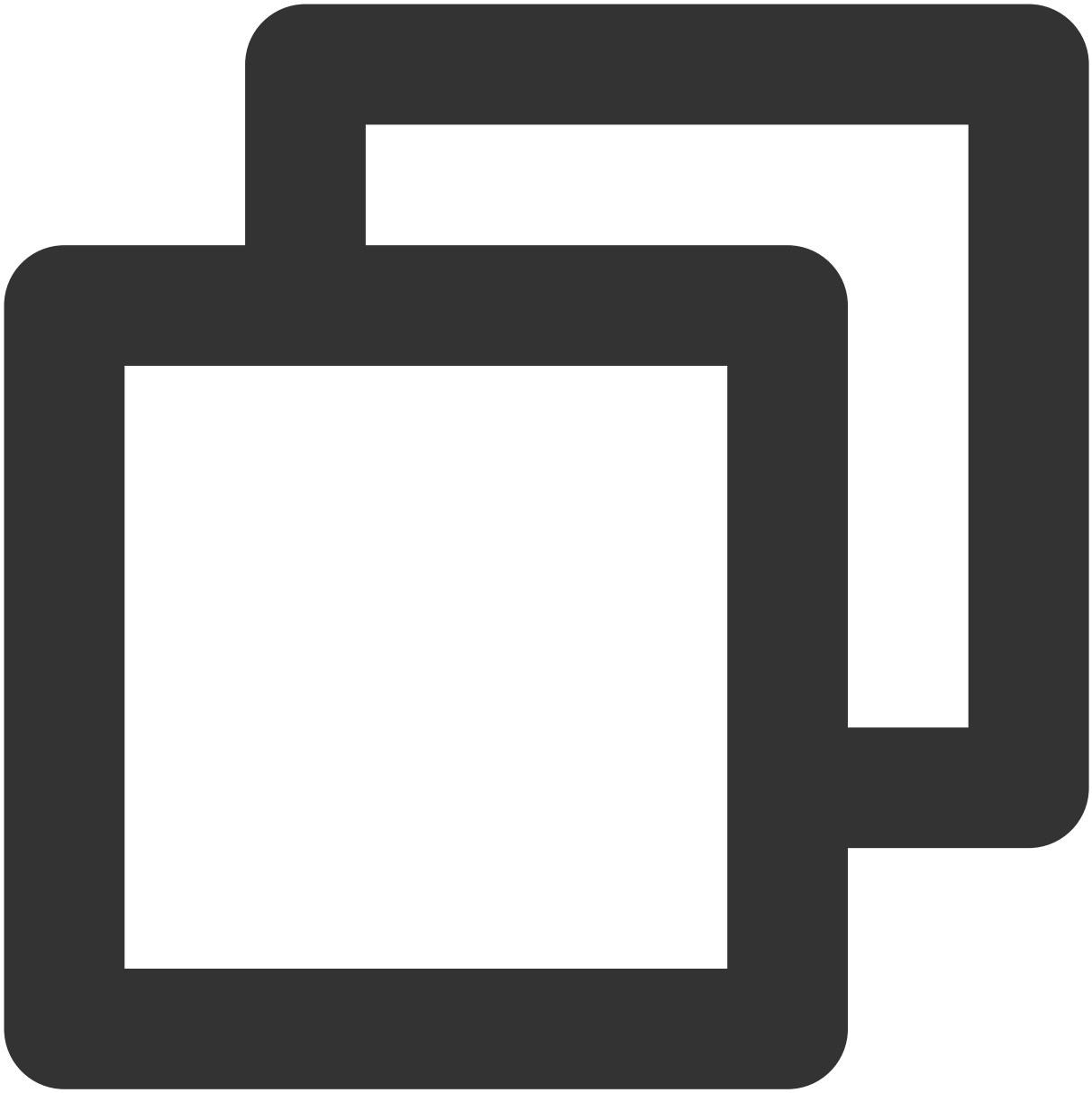
ここではCloud Virtual Machine（CVM）がCloud Object Storage（COS）にアクセスする際に使用するアクセス方法および、プライベートネットワークアクセスの判定方法についてご紹介し、接続性テストのサンプルもご提供します。こちらを参照することで、CVMのCOSへのアクセスに関する情報についてさらに理解を深めることができます。

アクセス方法

Tencent Cloud内でCOSへのアクセス用のサービスを展開している場合、リージョンごとのアクセス方法には次のような違いがあります。
同一リージョン内のアクセス：同一リージョンの範囲内でのアクセスに対しては自動的にプライベートネットワークアドレスに転送されます。つまり、プライベートネットワーク接続は自動的に使用され、それによるプライベートネットワークトラフィックには料金が発生しません。このため、コストを節約するために、別のTencent Cloud 製品を購入する場合は同じリージョンを選択することをお勧めします。
クロスリージョンアクセス：現在、クロスリージョンリクエストはプライベートネットワークアクセスをサポートしておらず、デフォルトではパブリックネットワークアドレスに解決されます。

プライベートネットワークアクセスの判定方法

この手順によって、CVMがプライベートネットワーク経由でCOSにアクセスするかどうかをテストすることができます。
CVM上で `nslookup` コマンドを使用してCOSドメイン名を解決します。プライベートネットワークIPが返された場合は、CVM がプライベートネットワーク経由でCOS にアクセスすることを示します。そうでない場合はパブリックネットワーク経由でのアクセスです。
1. バケットの概要 の説明に従ってバケットのアクセスドメインを取得して記録します。
2. インスタンスにログインし、nslookupコマンドを実行します。 `examplebucket-1250000000.cos.ap-guangzhou.myqcloud.com` が宛先バケットのアドレスであると仮定して、次のコマンドを実行します。



```
nslookup examplebucket-1250000000.cos.ap-guangzhou.myqcloud.com
```

コマンド出力の `10.148.214.13` および `10.148.214.14` の IP は、COS へのアクセスがプライベートネットワーク経由であることを示しています。

説明：

プライベートIPアドレスの一般的な形式は `10.*.*.*` 、 `100.*.*.*` であり、VPC IP アドレスは一般的に `169.254.*.*` などです。これらの形式のIPはすべてプライベートネットワークに該当します。

```
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
```

接続性のテスト

パブリックネットワークからのCOSアクセス、同一リージョンのCVM（クラシックネットワーク）からのCOSアクセス、同一リージョンのCVM（VPCネットワーク）からのCOSアクセスのサンプルをご提供します。詳細については、 接続性のテスト をご参照ください。

関連する操作

COSをローカルドライブとしてWindowsサーバーにマウントする
WordPressリモート添付ファイルのCOS への保存

Linux CVMでのデータリカバリ

最終更新日：：2022-05-06 16:57:28

概要

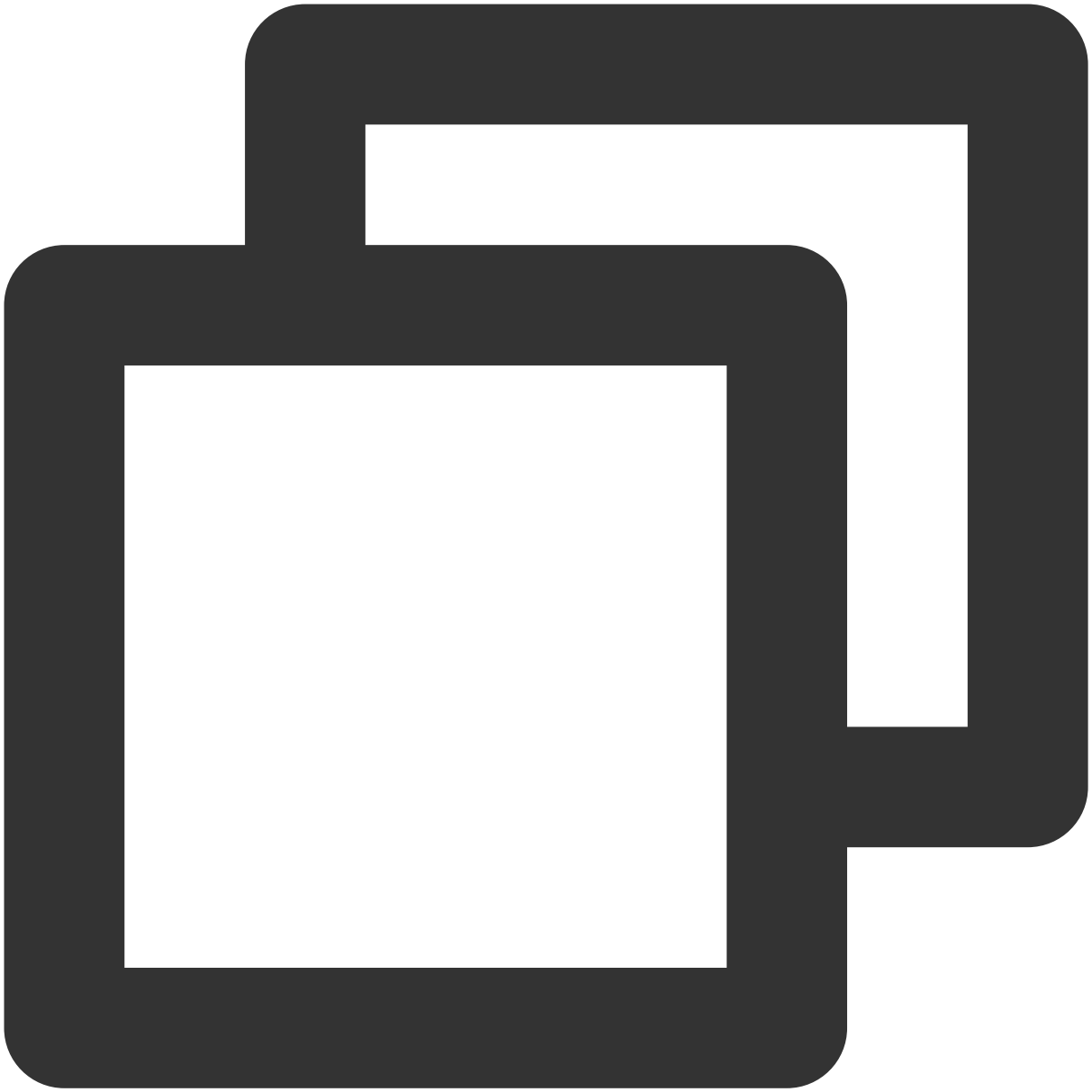
このドキュメントでは、CentOS 8.0を搭載したTencent Cloud CVMを例として取り上げ、オープンソースツール Extundelete を使用して誤って削除されたデータをすばやくリカバーする方法について説明します。
Extundeleteは、誤って削除されたファイルシステムタイプext3およびext4のファイルのリカバーをサポートしますが、具体的なリカバーの度合いは、削除後に書き込みによって上書きされるかどうか、メタデータがjournalに保存されるかどうかなどの要因に関連します。データのリカバーを必要とするファイルシステムがシステムディスクにあり、常にサービスプロセスまたはシステムプロセスがファイルを書き込んでいる場合、リカバーの可能性は低くなります。
説明：
Tencent Cloudは、スナップショットの作成、カスタマイズイメージの作成 および Cloud Object Storage などのデータストレージ方法を提供しています。データセキュリティを向上させるために、定期的にデータバックアップを行うことをお勧めします。

準備作業

データリカバーに関連する操作を実行する前に、次の準備を完了してください：
問題が発生するときに初期状態にリカバーできるために、スナップショットの作成 および カスタマイズイメージの作成 を参照してデータをバックアップしてください。
関連するサービスプログラムを停止し、ファイルシステムへのデータの書き込みを続行します。データディスクをリカバーする必要がある場合、最初にデータディスクで `umount` 操作を実行できます。

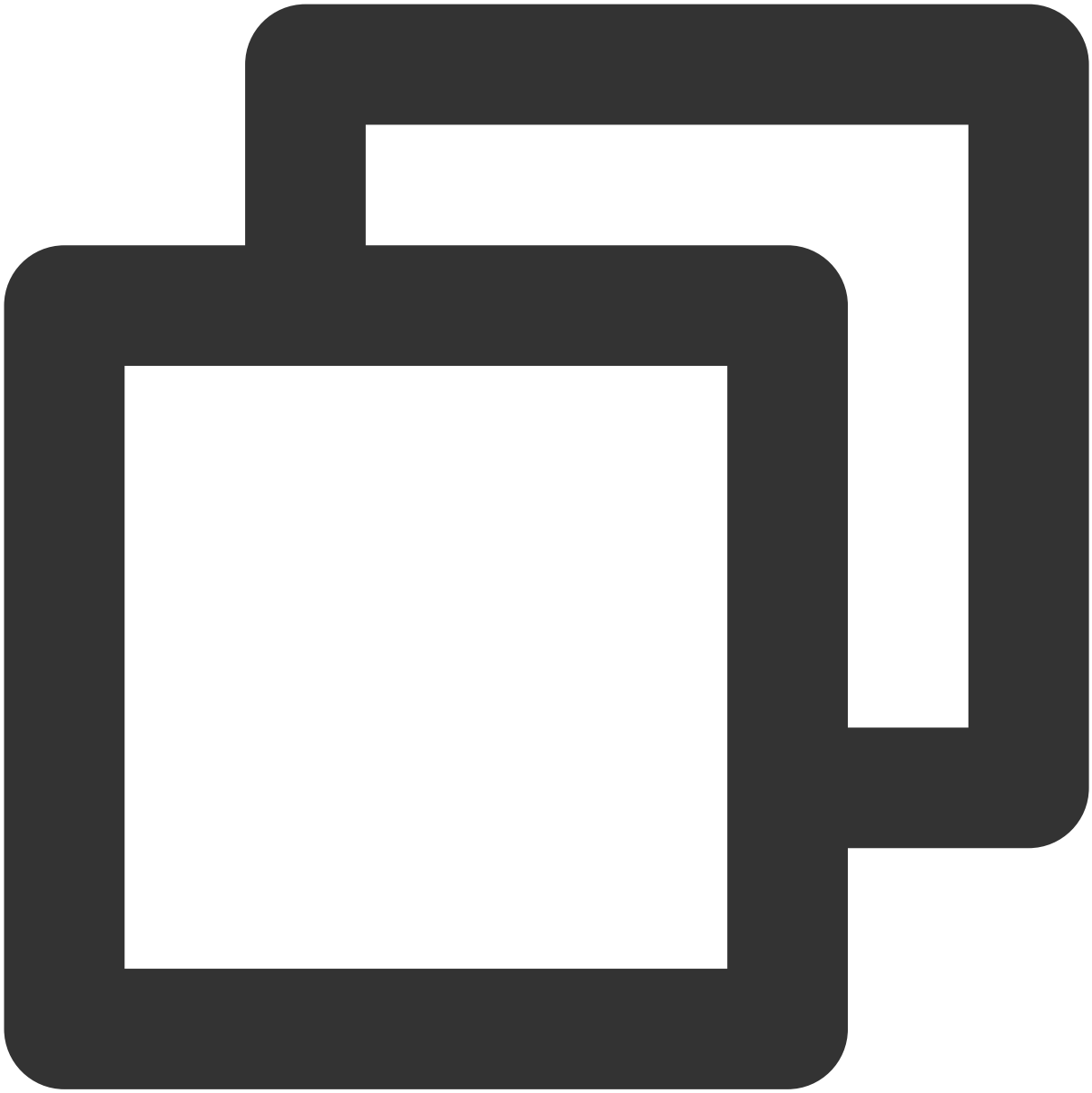
操作手順

1. 次の2つの方法を使用して、Extundeleteをインストールします：
コンパイルされたバイナリプログラムをダウンロードします（推奨）
手動によるコンパイルとインストール
1. 次のコマンドを実行して、コンパイルされたバイナリプログラムを直接ダウンロードできます。



```
wget https://github.com/curu/extundelete/releases/download/v1.0/extundelete
```

2. 次のコマンドを実行して、ファイルの権限を付与します。

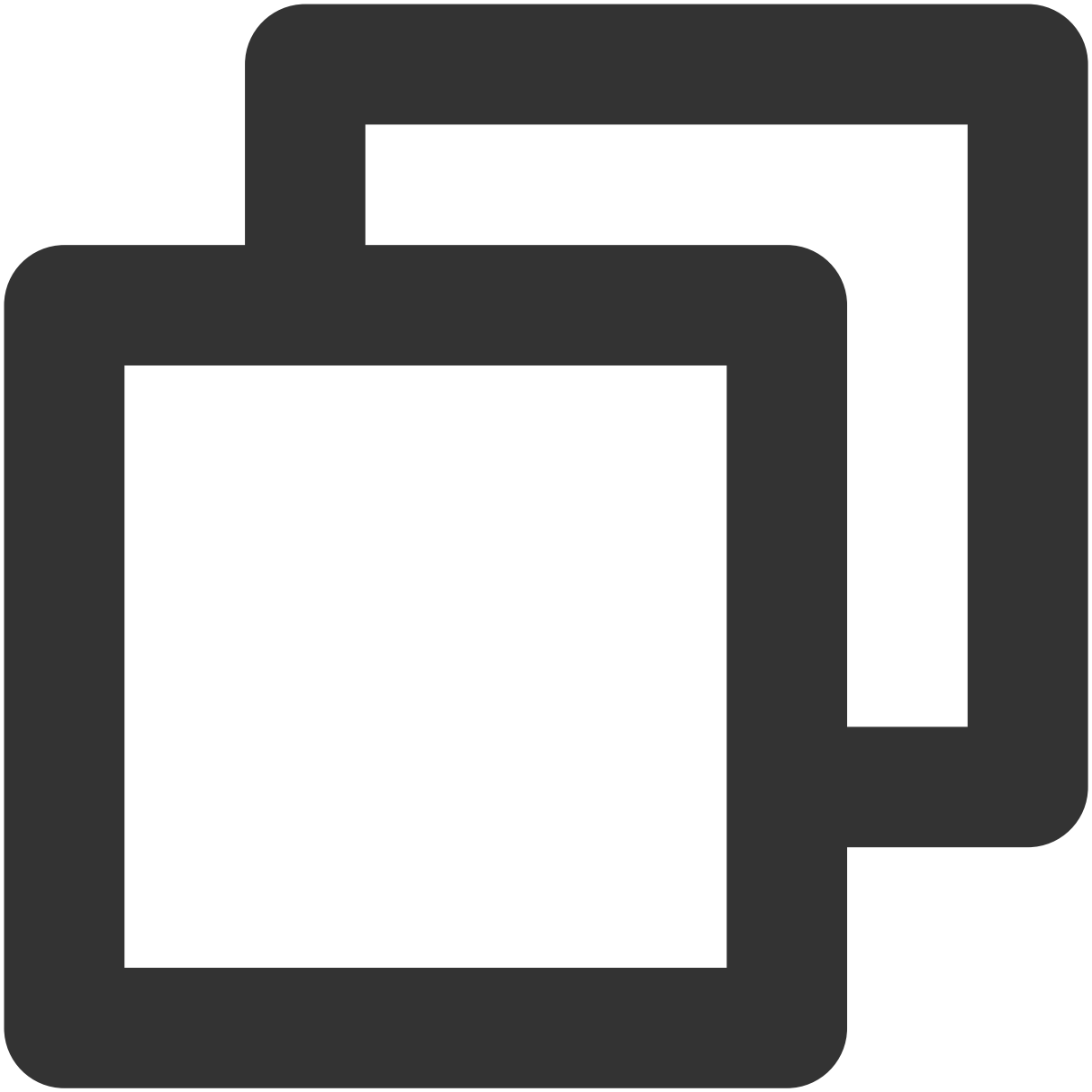


```
chmod a+x extundelete
```

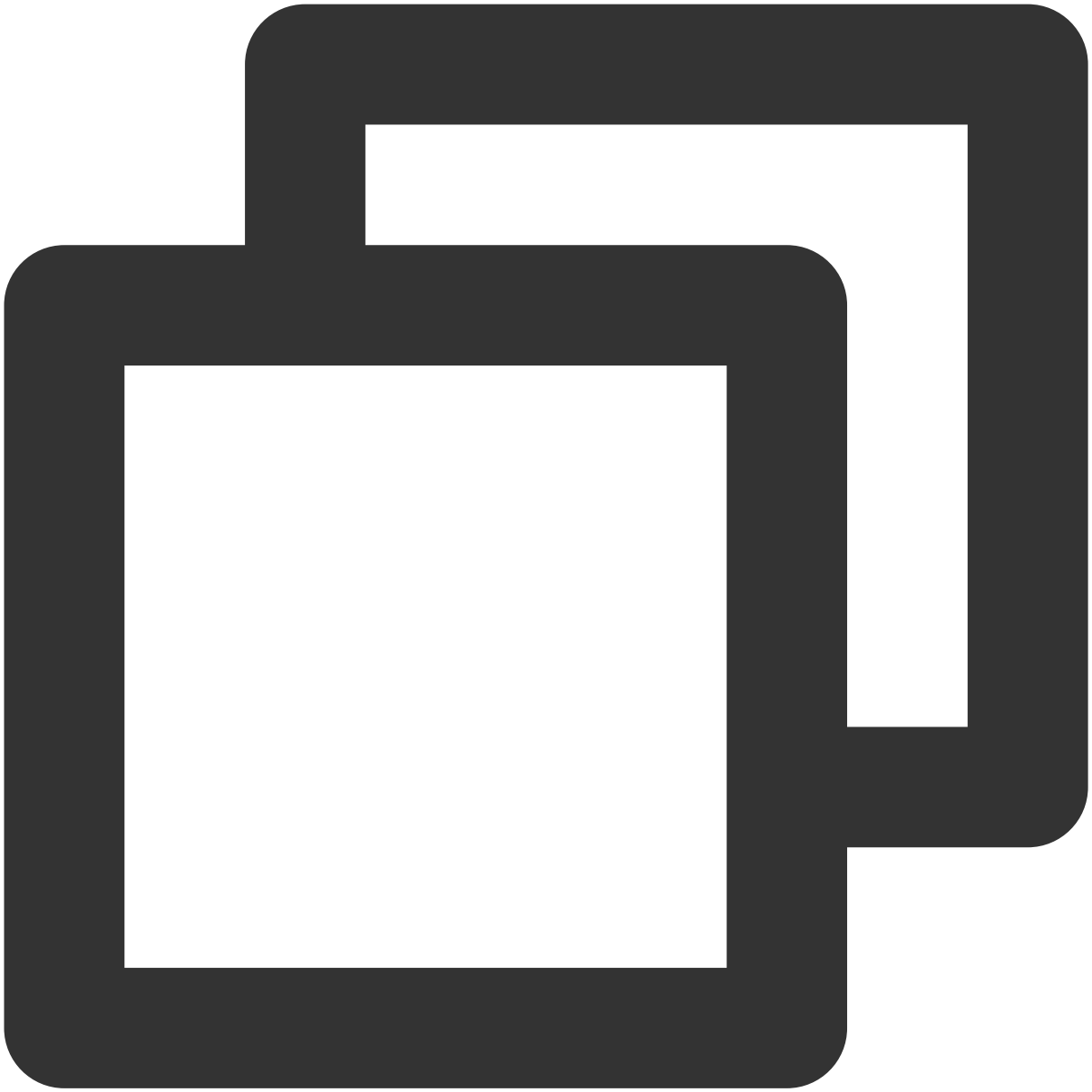
説明：

この手順では、CentOS 7 OSを例として取り上げます。手順はシステム環境によって異なります。実際のリファレンスドキュメントに従って操作してください。

1. 次のコマンドを実行して、Extundeleteに必要な依存関係とライブラリをインストールします。

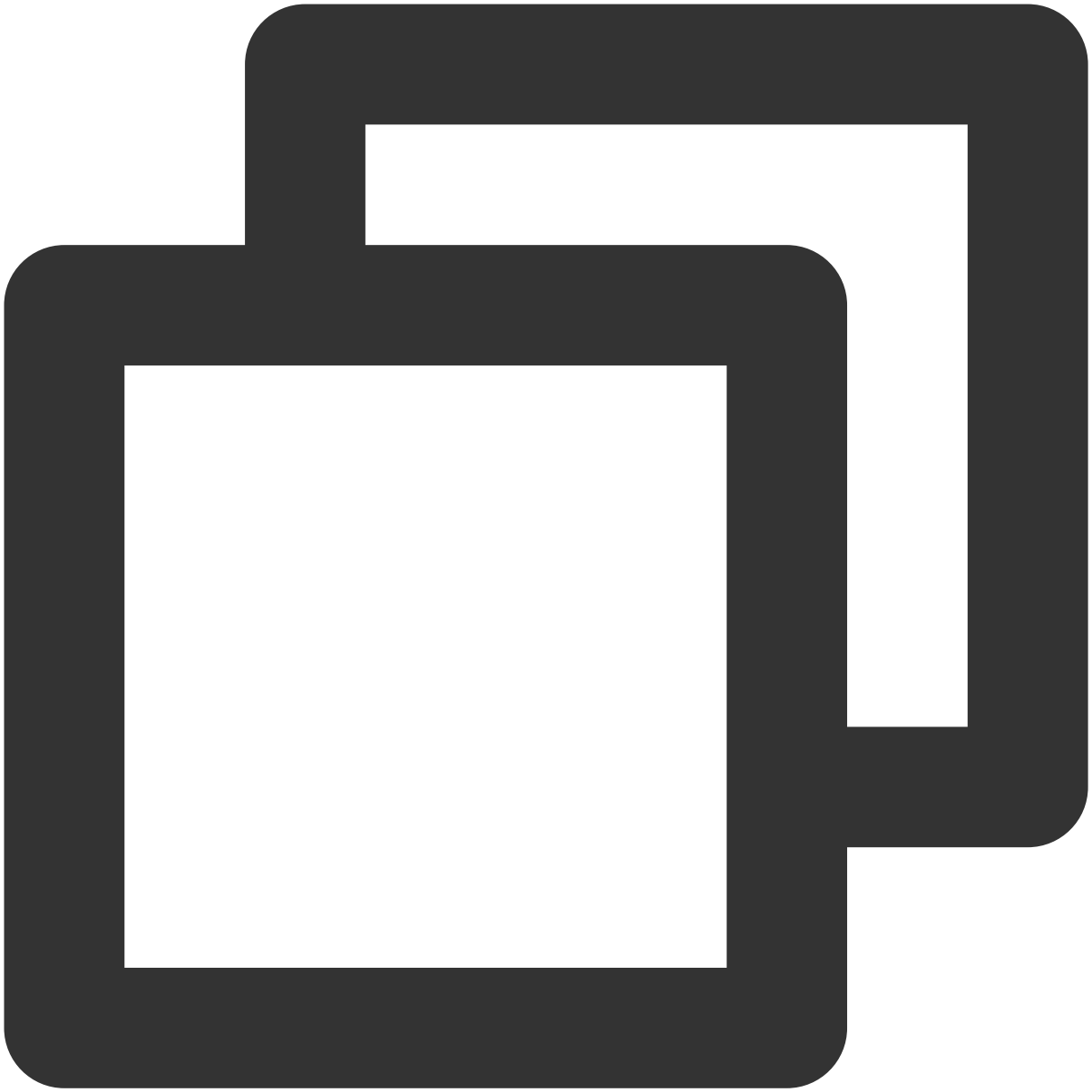


```
yum install libcom_err e2fsprogs-devel
```



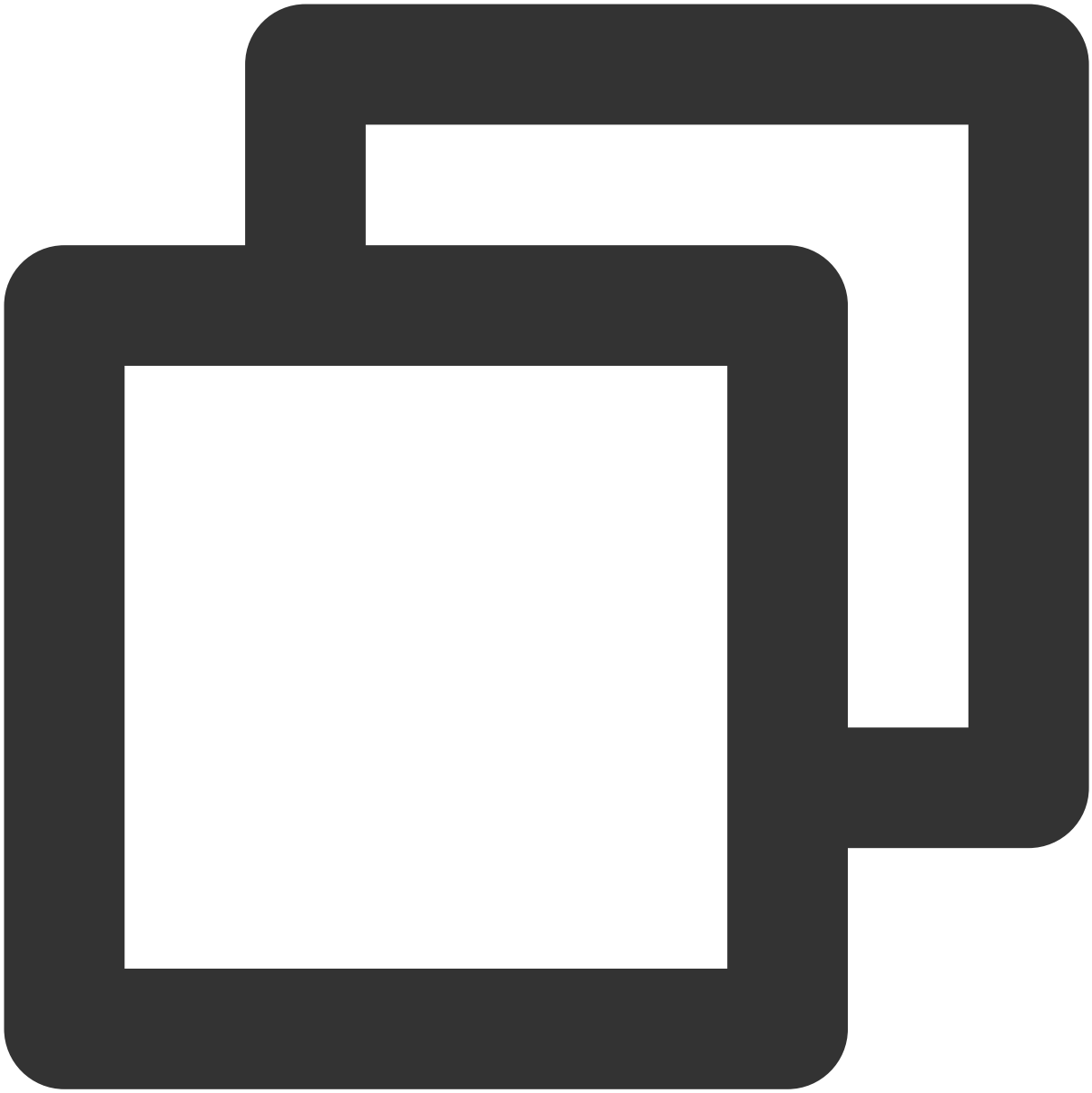
```
yum install gcc gcc-c++
```

2. 次のコマンドを実行して、Extundeleteソースコードをダウンロードします。



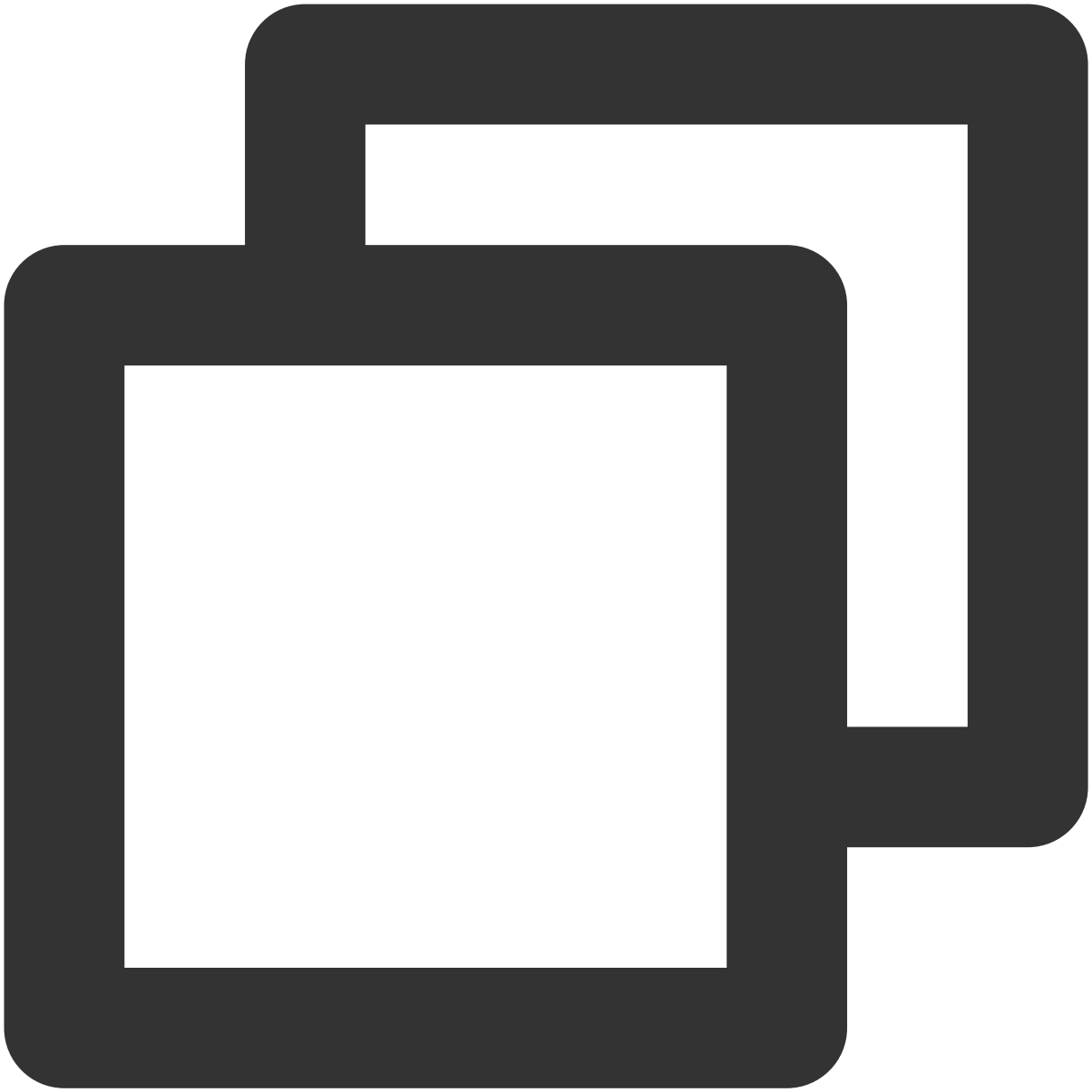
```
wget https://github.com/curu/extundelete/archive/refs/tags/v1.0.tar.gz
```

3. 次のコマンドを実行して、v1.0.tar.gzファイルを解凍します。

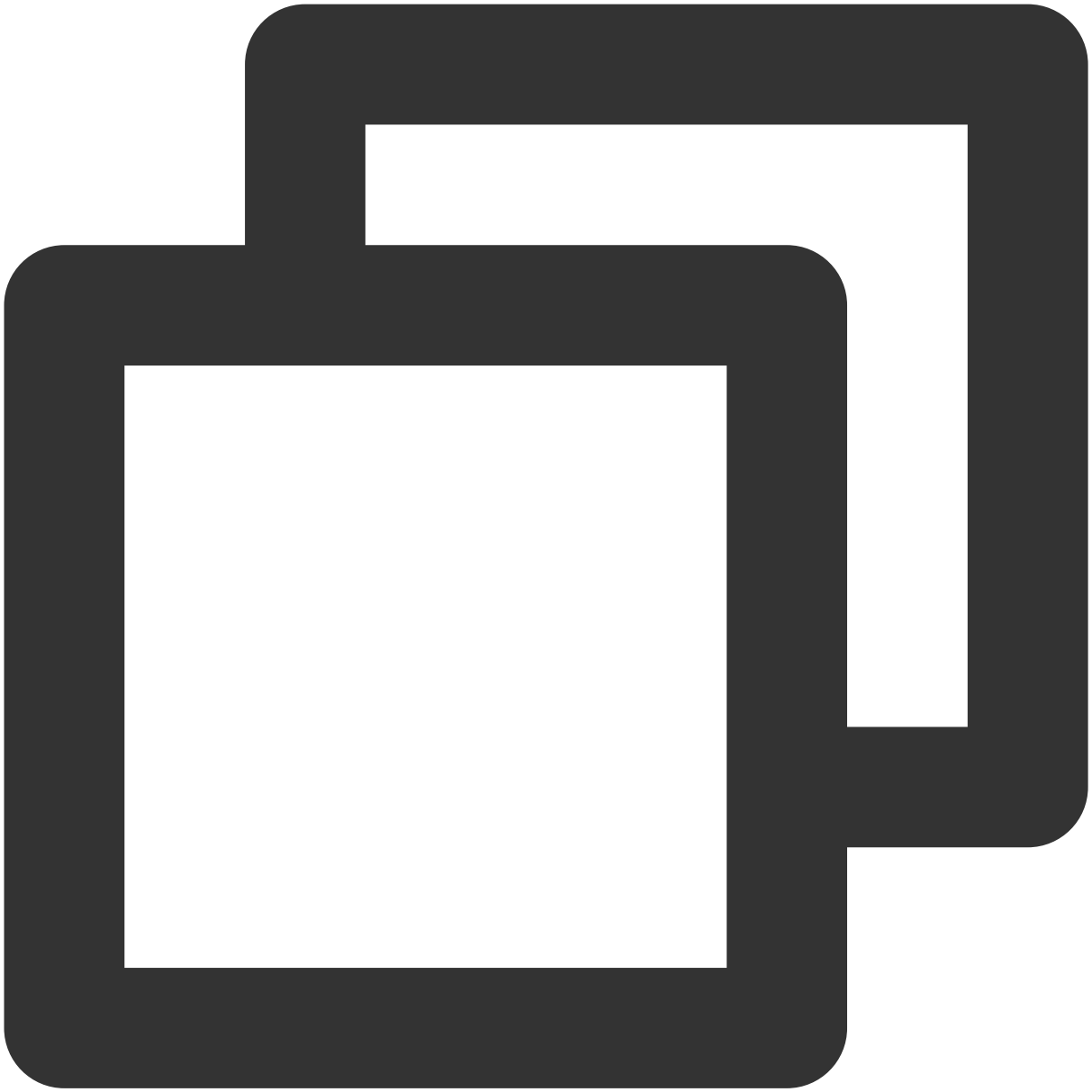


```
tar  xf v1.0.tar.gz
```

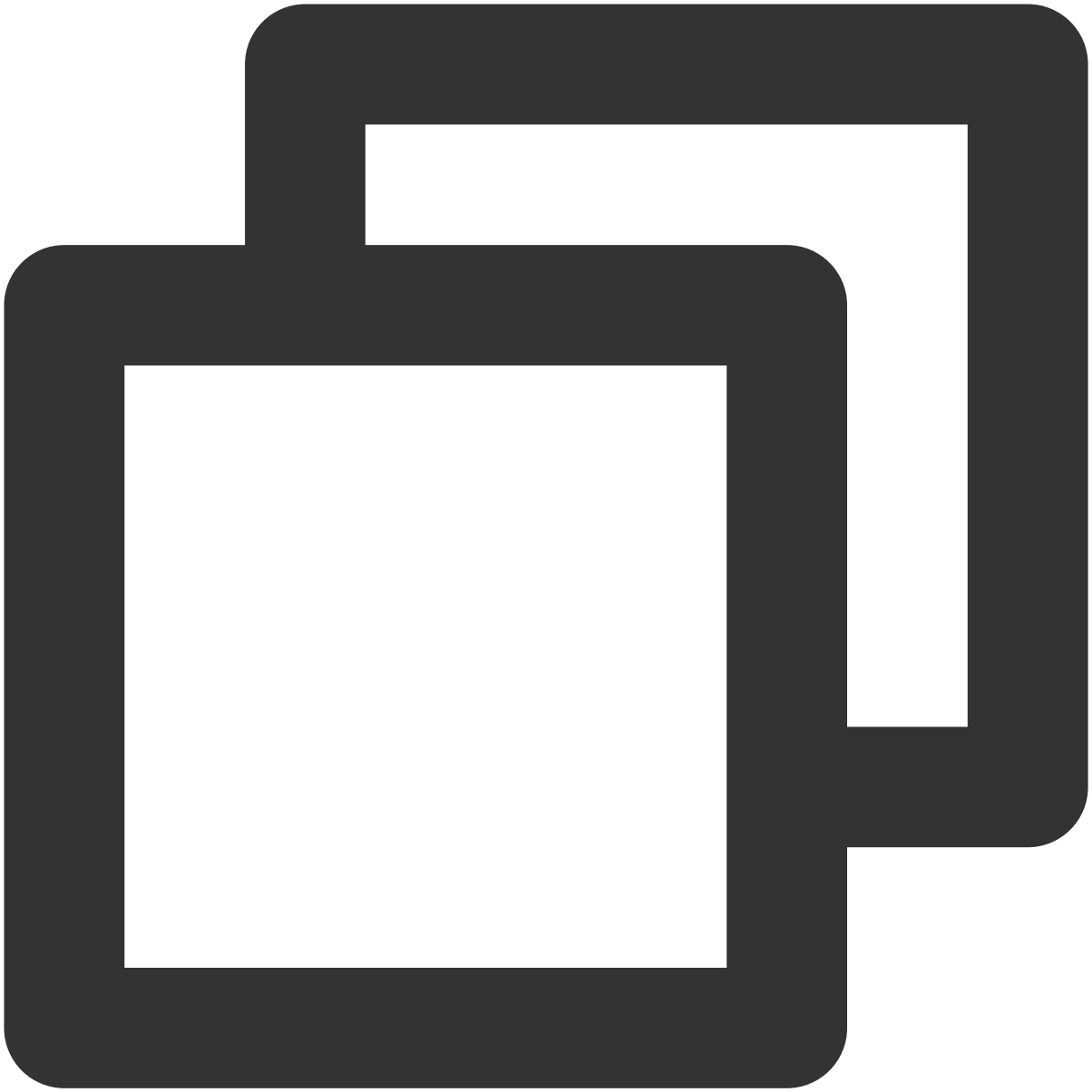
4. 次のコマンドを実行して、コンパイルしてインストールします。



```
cd extundelete-1.0
```

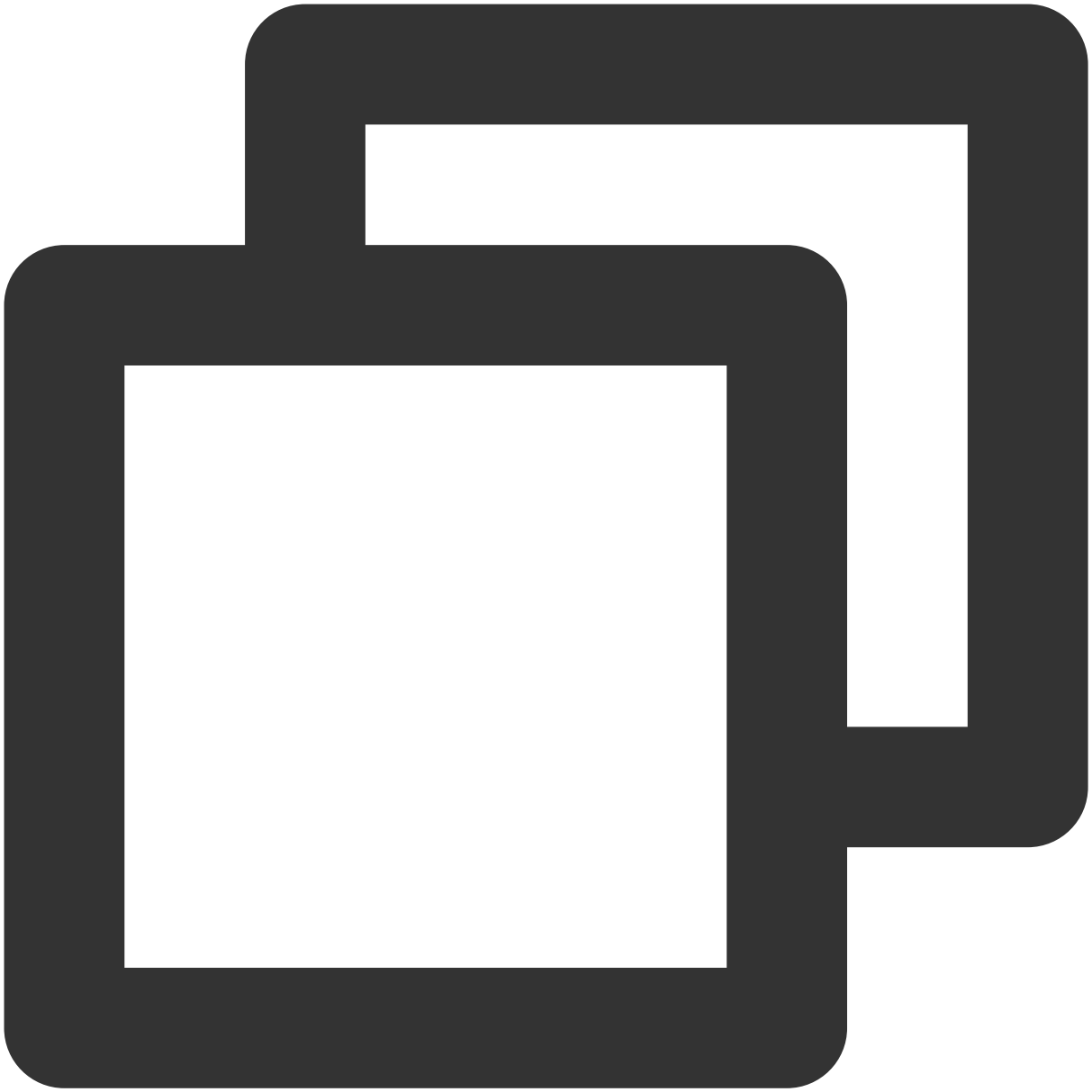


```
./configure
```



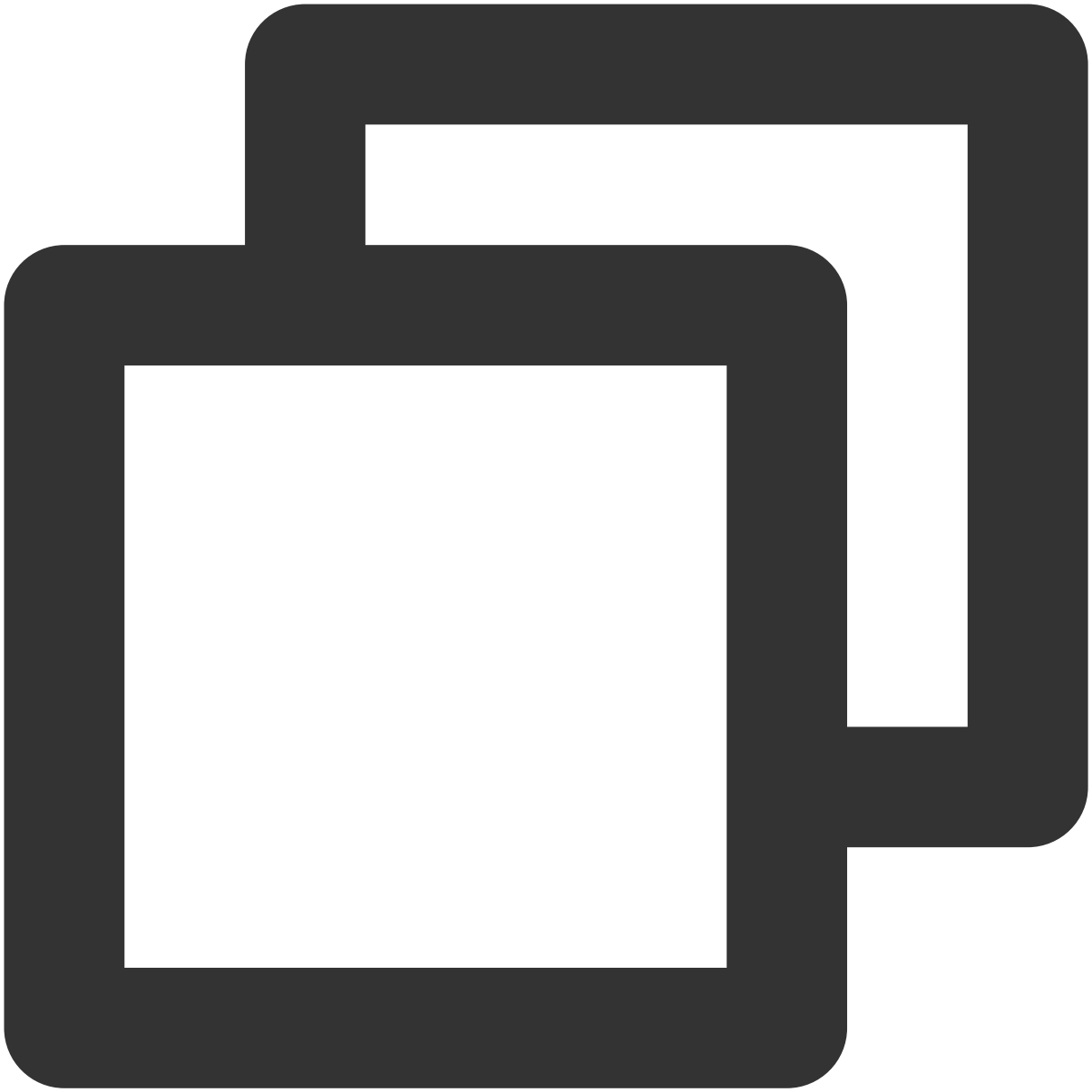
```
make
```

5. 次のコマンドを実行して、srcディレクトリに入り、コンパイルされたExtundeleteファイルを表示できます。



```
cd ./src
```

2. 次のコマンドを実行して、データのリカバーを試みます。



```
./extundelete  --restore-all  /dev/対応するディスク
```

リカバーされたファイルは同じレベルのディレクトリの `RECOVERED_FILES` フォルダにあります。必要なファイルがあるかどうかを確認してください。

Windows CVMでのディスク容量の管理

最終更新日：：2020-09-10 14:59:25

操作シナリオ

このドキュメントでは、Windows Server 2012 R2のTencent Cloud CVMを例に、Windowsインスタンスのディスク容量が不足している場合に容量を解放する方法と、ディスクの日常的な保守を行う方法について説明します。

操作手順

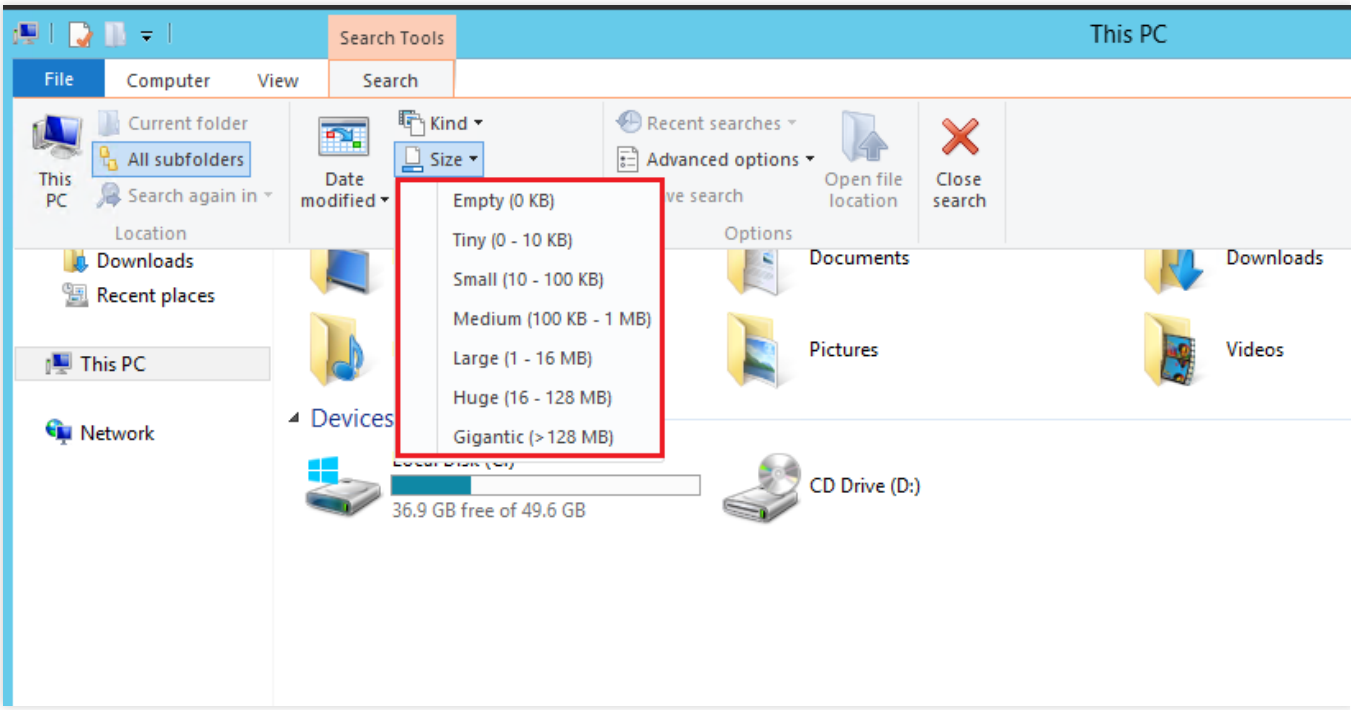
ディスクの空き容量を増やす

ディスク容量不足の問題は、大容量ファイルの削除 または 不要ファイルの削除 によって解決できます。ファイルをクリーンアップしても実際のニーズを満たすことができない場合は、ディスクの容量拡張を選択してディスク容量を拡張します。詳細については、容量拡張ケースの概要 をご参照ください。

大容量ファイルの削除

1. RDPファイルを使用してWindowsインスタンスにログイン（推奨）します。また、実際の操作方法により、リモートデスクトップ接続を使用してWindowsインスタンスにログイン することもできます。
2. 下部ツールバーの

を選択して、「このコンピュータ」ウィンドウを開きます。
3. 「このコンピュータ」で、クリーンアップするディスクを選択し、**Crtl+F**を押して検索ツールを開きます。
4. **検索 > サイズ**を選択し、システムで設定されたサイズに基づいてメニューから必要に応じてファイルをフィルタリングします。以下の通りです。



説明：

「このコンピュータ」の右上隅にある検索ボックスで、ファイルのサイズをカスタマイズして検索することもできます。例：

「サイズ：>500M」と入力すると、ディスクの500Mを超えたファイルが検索されます。

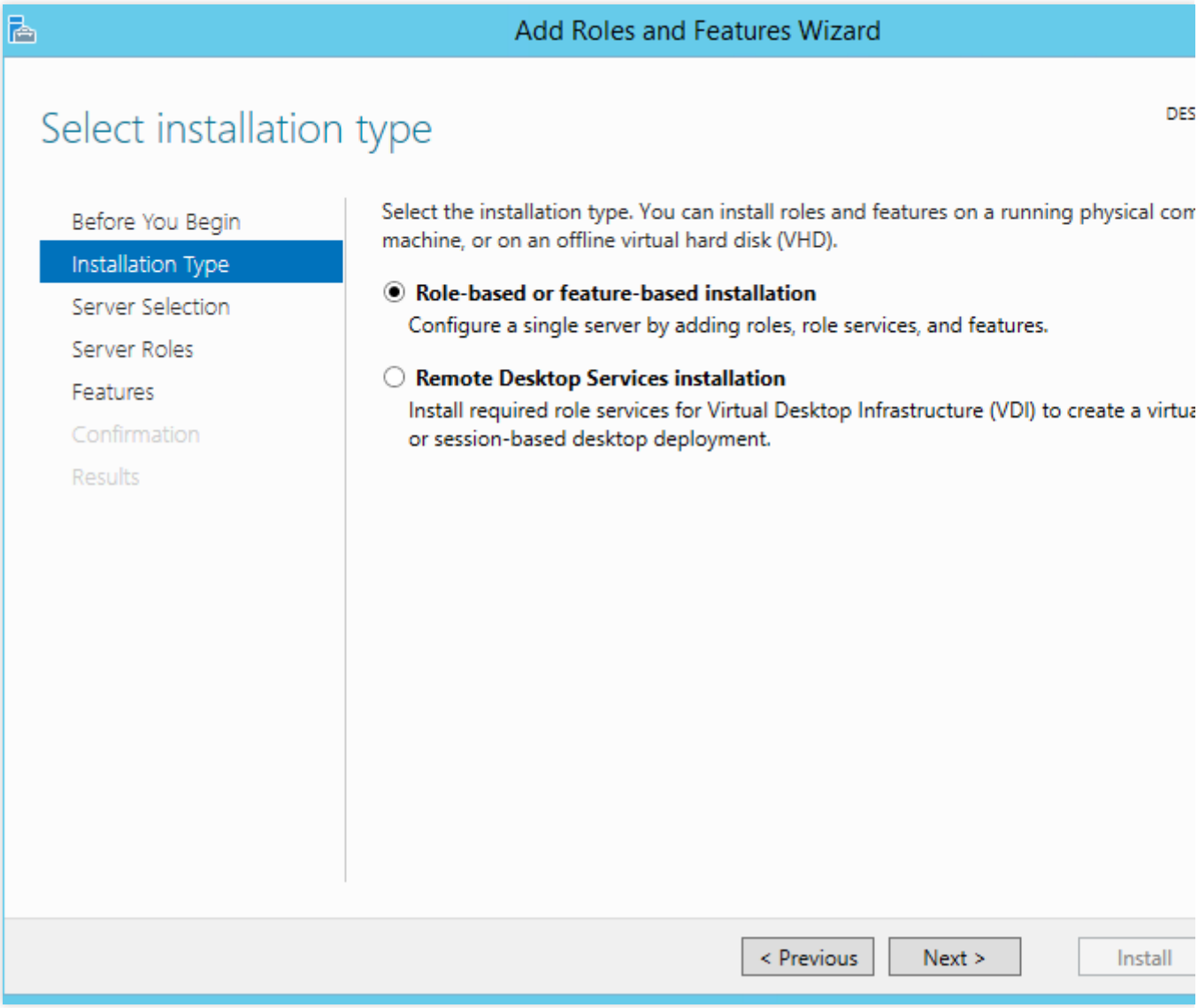
「サイズ：>100M<500M」と入力すると、ディスクの100Mを超えて且つ500M未満のファイルが検索されます。

不要ファイルの削除

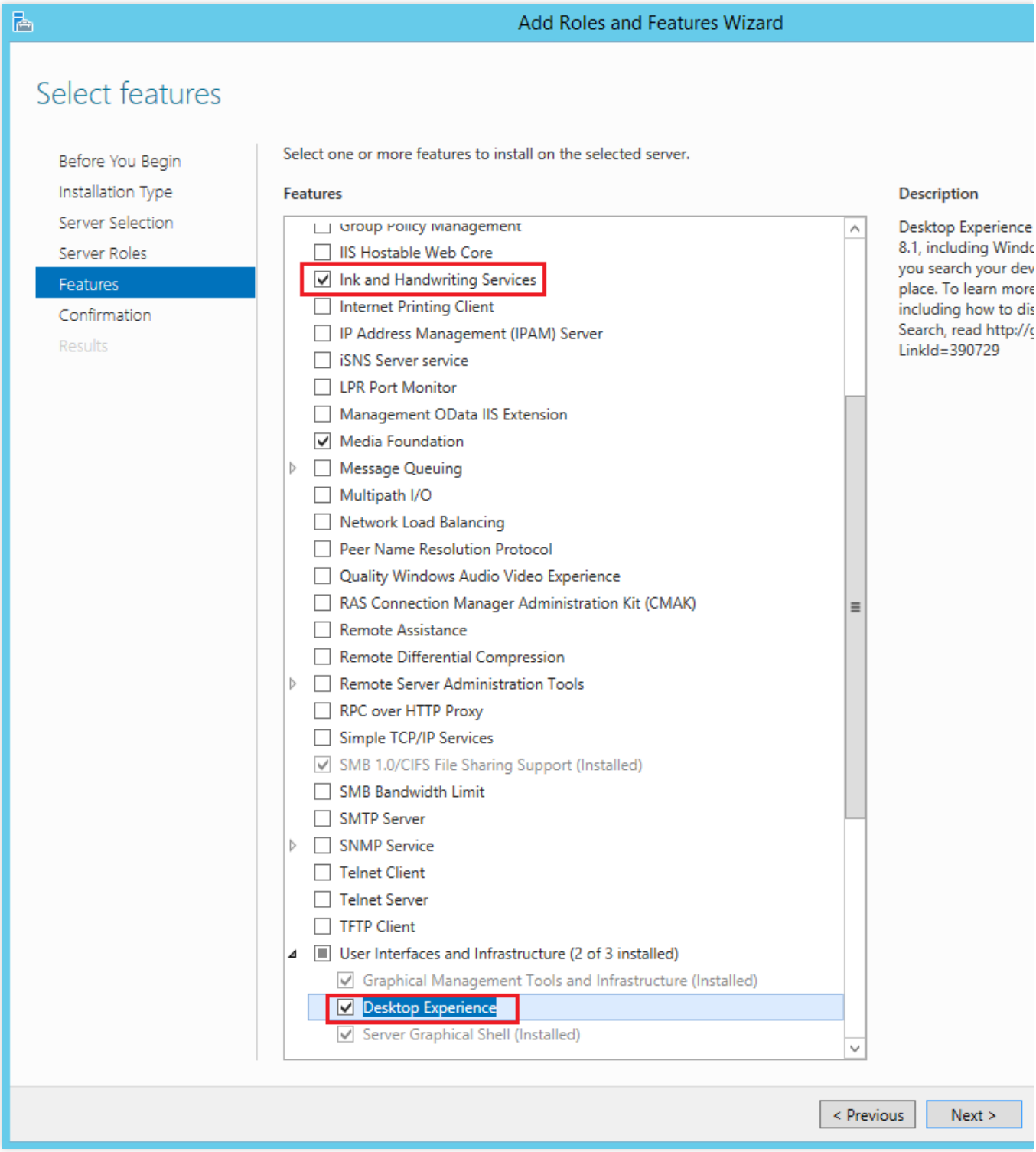
1.

を選択して、「サーバーマネージャ」を開きます。

2. **【役割と機能の追加】**をクリックして、「役割と機能の追加ウィザード」画面が表示されます。
3. 「役割と機能の追加ウィザード」ウィンドウで、**次へ**をクリックします。
4. 「インストールタイプを選択」画面で、**役割ベースまたは機能ベースのインストール**を選択して、3回続けて【次へ】をクリックしてください。以下の通りです。



5. 「機能の選択」画面で「インクと手書きサービス」と「デスクトップエクスペリエンス」をチェックし、表示されたプロンプトボックスで【OK】をクリックします。以下の通りです。

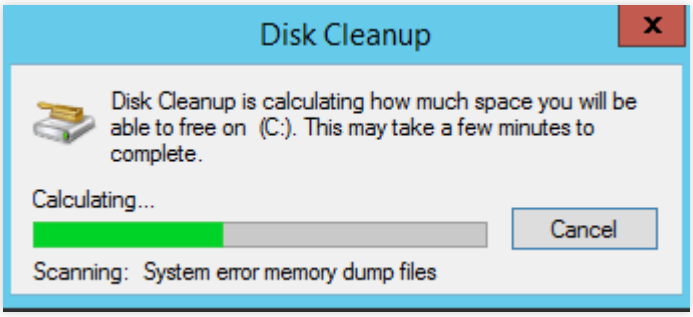


6. **次へ**を選択し、**インストール**をクリックします。インストールが完了したら、画面の通知メッセージを参照してサーバーを再起動します。

7.


を選択し、右上隅の

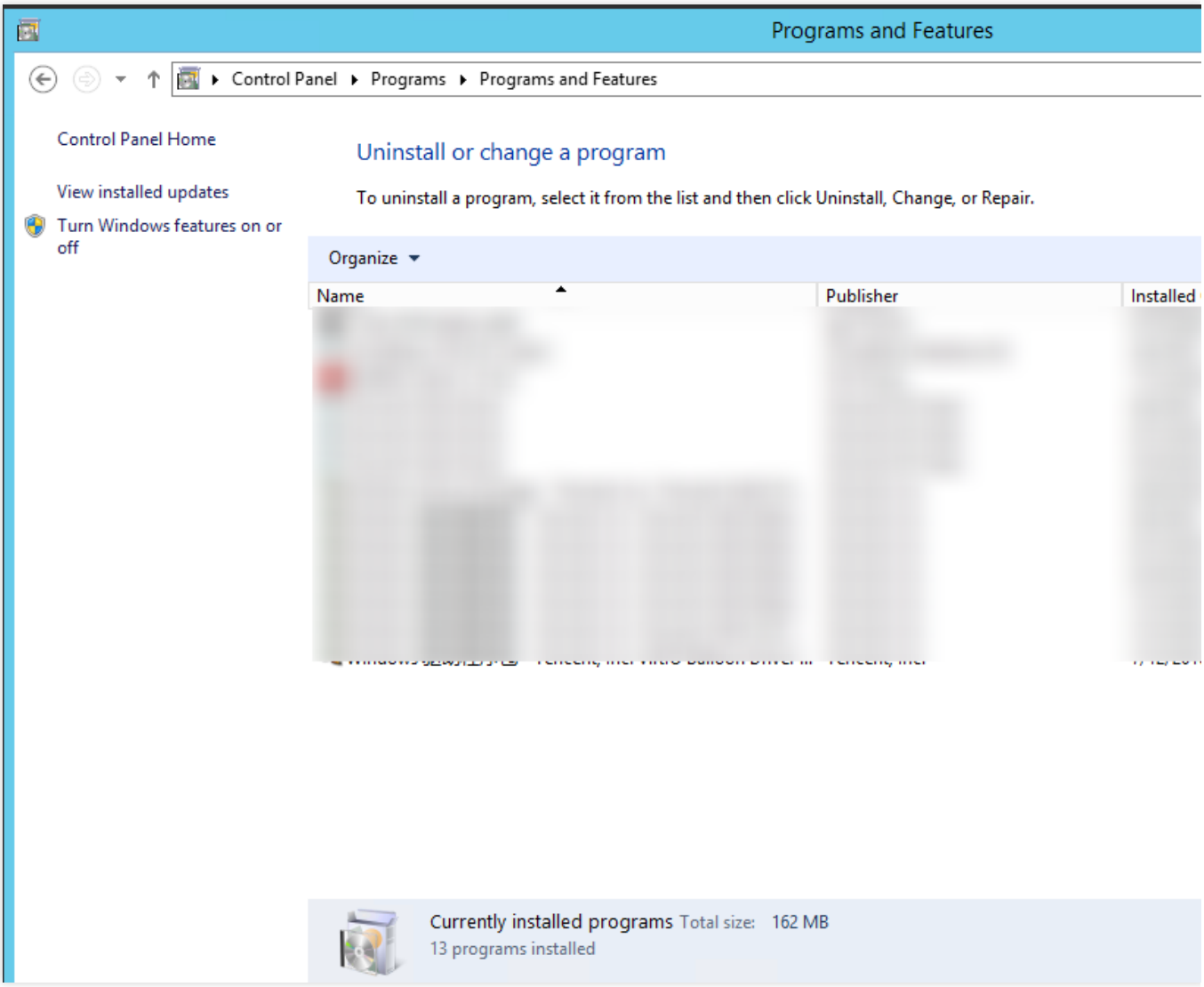

をクリックします。検索ボックスに**ディスク管理**を入力して検索します。
8. 表示された「ディスククリーンアップ」ウィンドウで、対応するディスクを選択してクリーンアップを開始します。以下の通りです。



ディスクの日常的な保守

定期的にプログラムを削除する

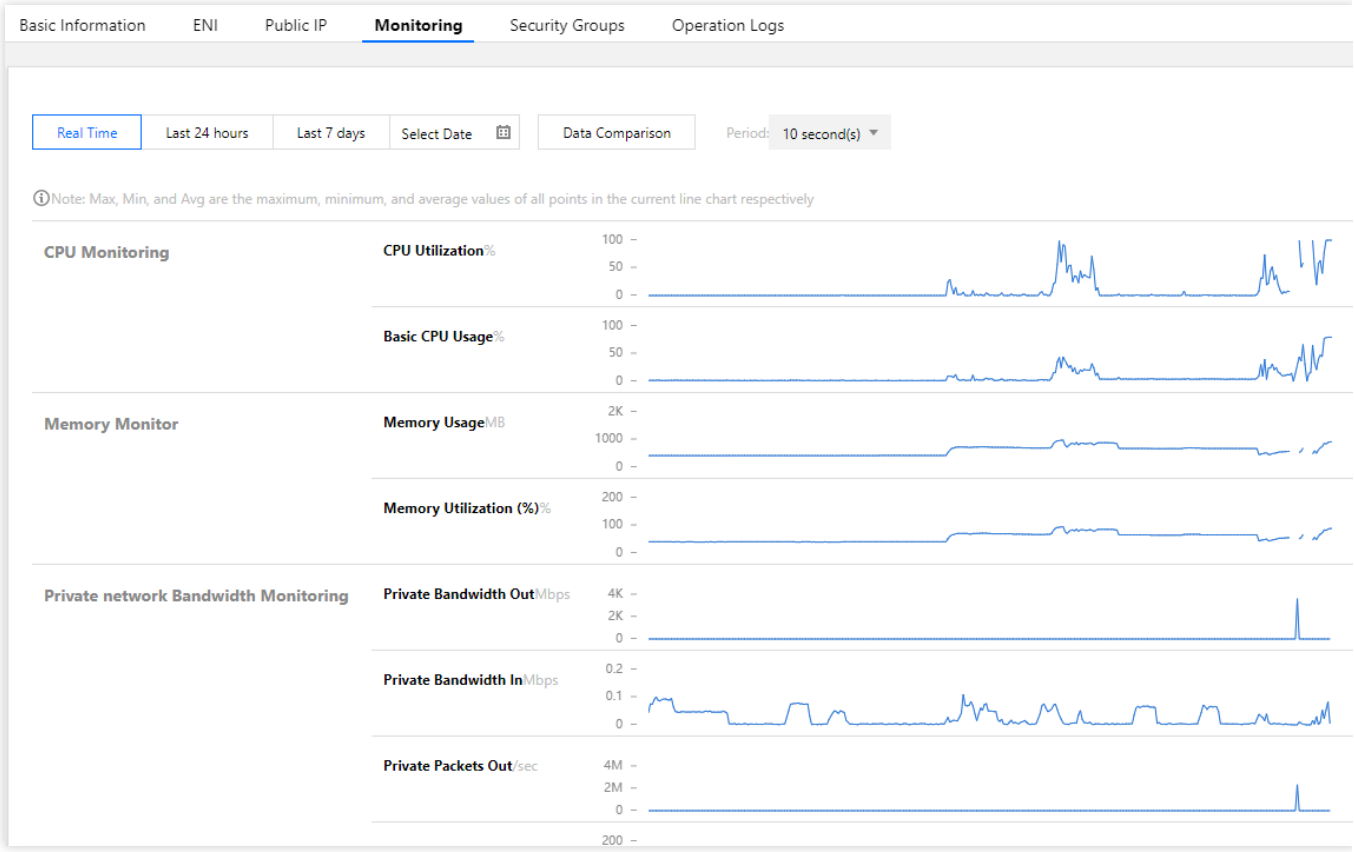
「コントロールパネル」の「プログラムのアンインストールまたは変更」を選択して、使用しなくなったプログラムを定期的にクリーンアップできます。以下の通りです。



コンソールでディスク使用状況を表示する

Cloud Monitor機能は、CVMインスタンスが作成されると自動的に有効になります。次の手順を実行して、コンソールからCVMのディスク使用状況を表示することができます。

1. CVMコンソール にログインし、「インスタンス」ページに進みます。
2. ターゲットインスタンスのID /名前を選択して、インスタンスの詳細ページに入ります。
3. インスタンスの詳細ページで、**監視**タブを選択すると、そのインスタンスのディスク使用状況が表示されます。以下の通りです。



Linuxインスタンスのカーネルを手動で変更する

最終更新日：：2021-10-27 18:04:06

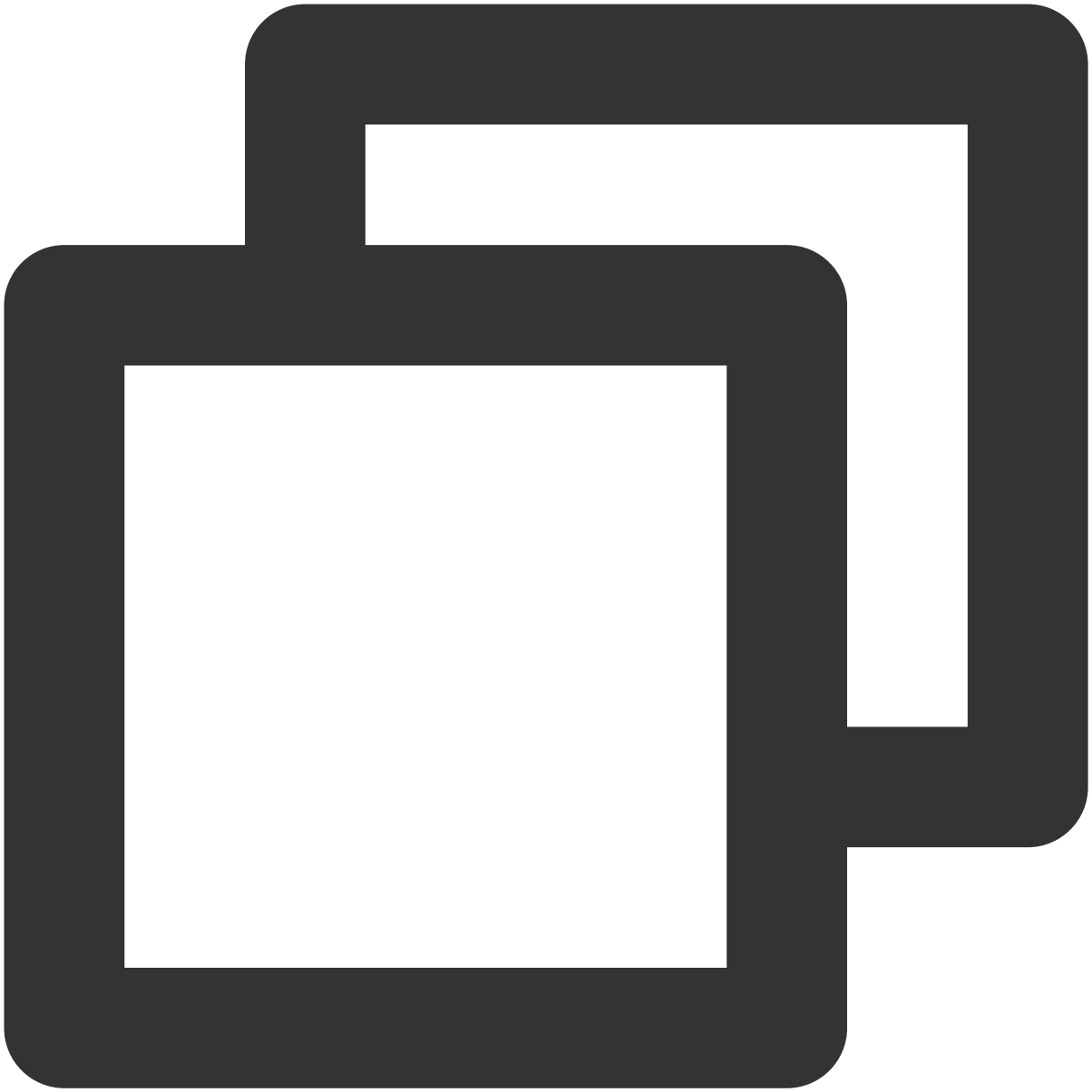
概要

Bottleneck Bandwidth and Round-trip propagation time（BBR）は、Googleが2016年に開発したTCP輻輳制御アルゴリズムであり、Linuxサーバーのスループットを大きく引き上げ、TCP接続のディレイを低減させることができます。BBRの有効化には、4.10以上のバージョンのLinuxカーネルが必要となりますが、Linuxサーバーのカーネルが4.10より低い場合は、本文を参照して操作することが可能です。
ここでは、CentOS 7.5 OSのCVMを例に、Linuxシステムでカーネルを手動で変更し、BBRを有効化する方法をご説明します。

操作手順

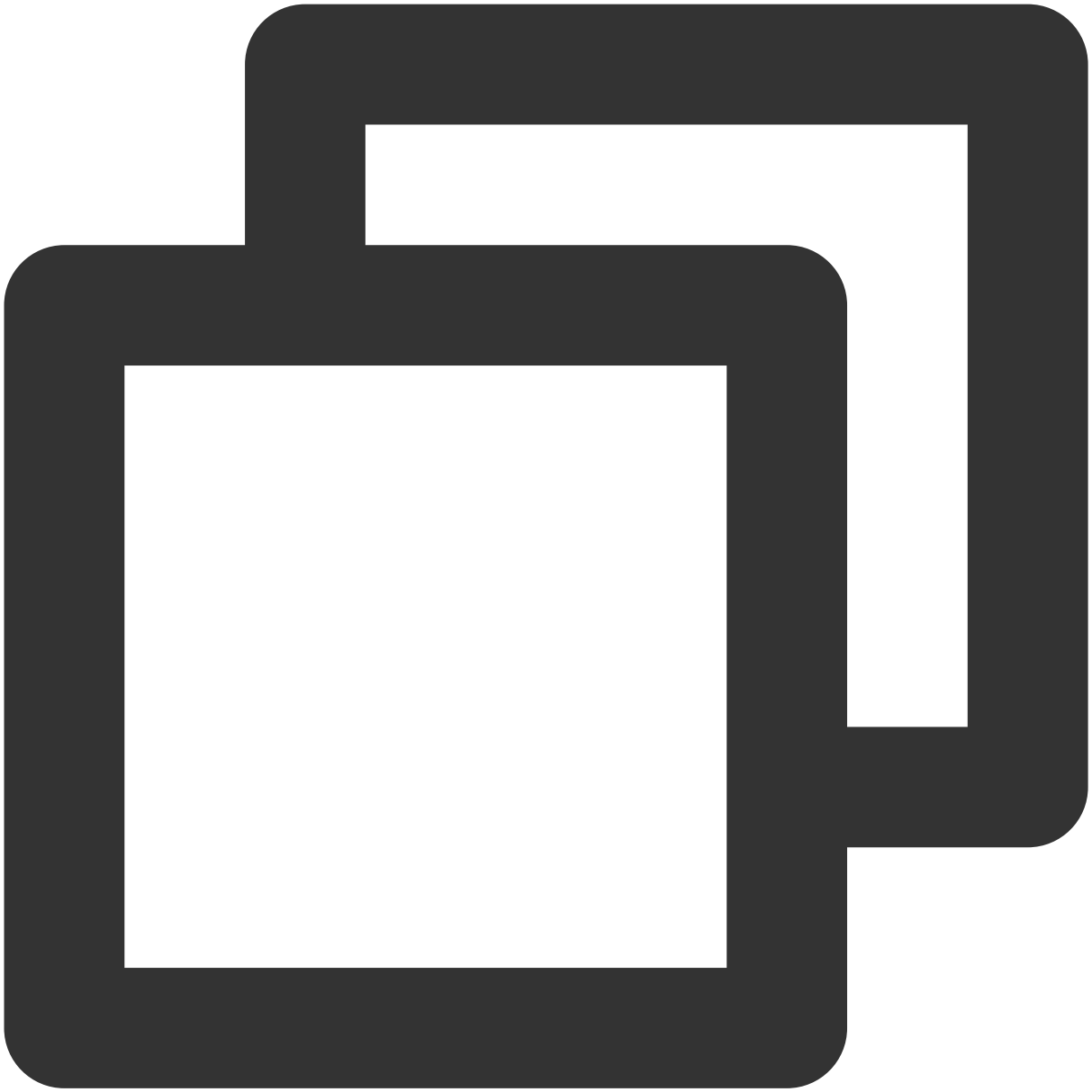
カーネルパッケージの更新

1. 次のコマンドを実行し、現在のKernelバージョンを表示します。



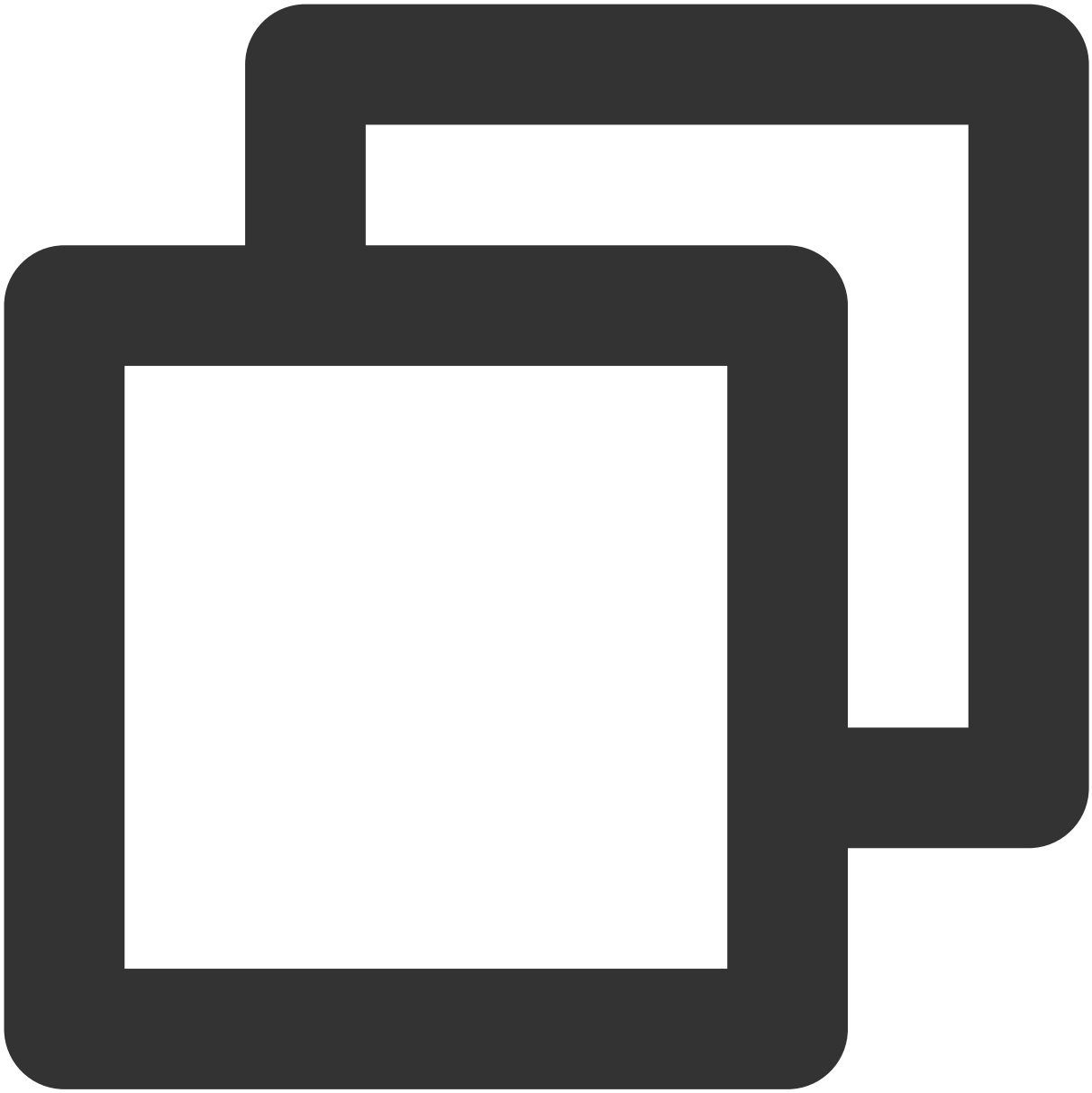
```
uname -r
```

2. 次のコマンドを実行し、ソフトウェアパッケージを更新します。



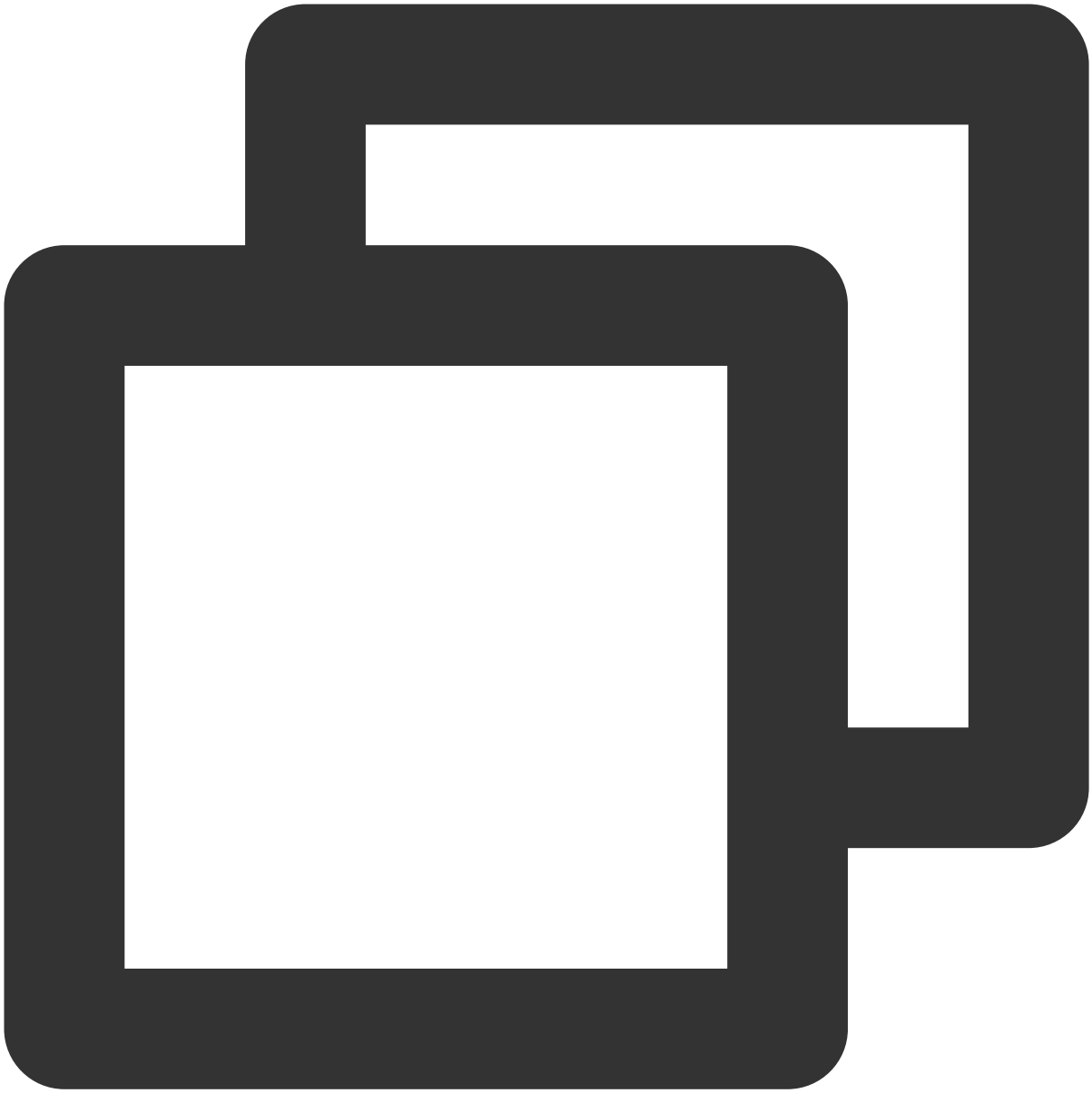
```
yum update -y
```

3. 次のコマンドを実行し、ELRepoの公開鍵をインポートします。



```
rpm --import https://www.elrepo.org/RPM-GPG-KEY-elrepo.org
```

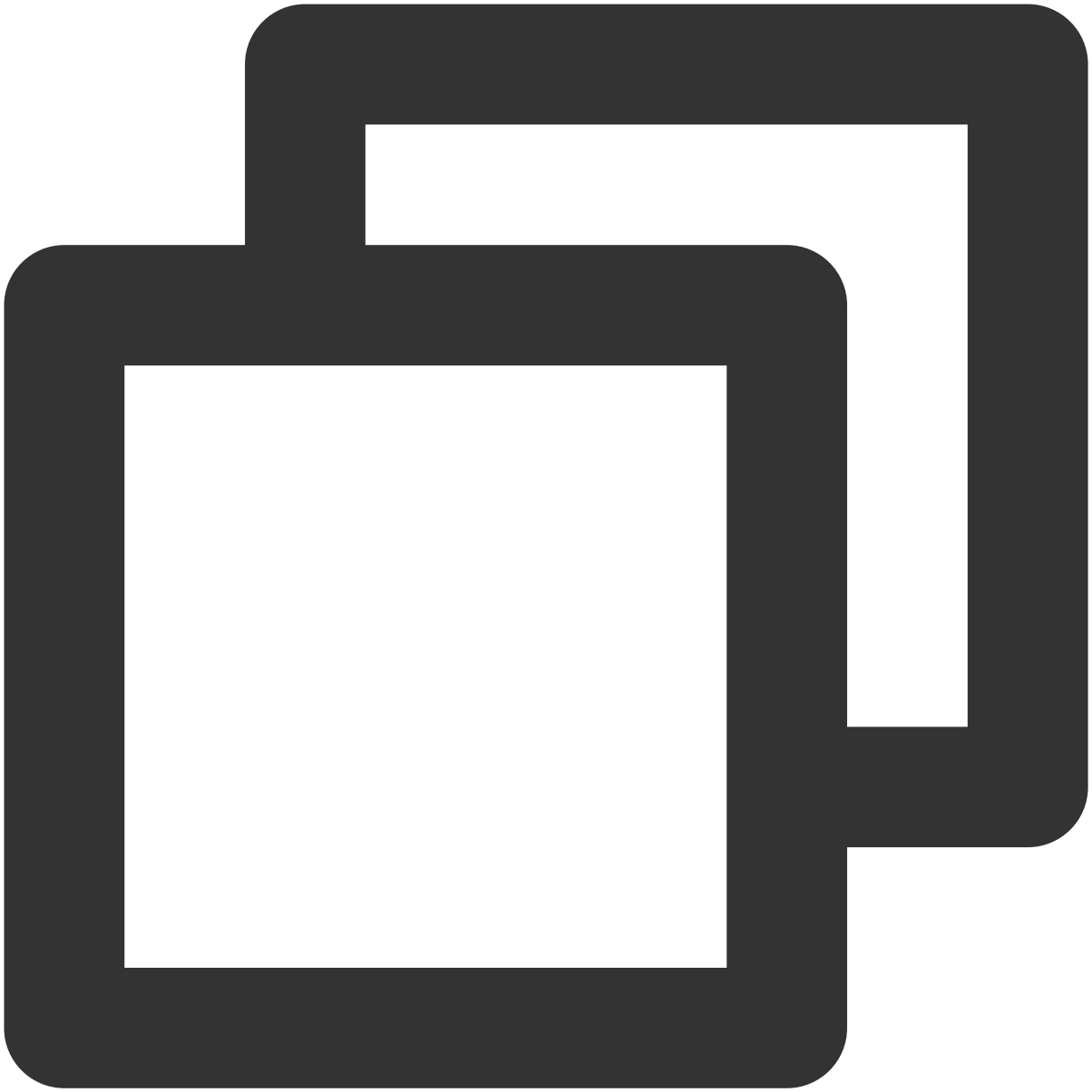
4. 次のコマンドを実行し、ELRepoのyumリポジトリをインストールします。



```
yum install https://www.elrepo.org/elrepo-release-7.0-4.el7.elrepo.noarch.rpm
```

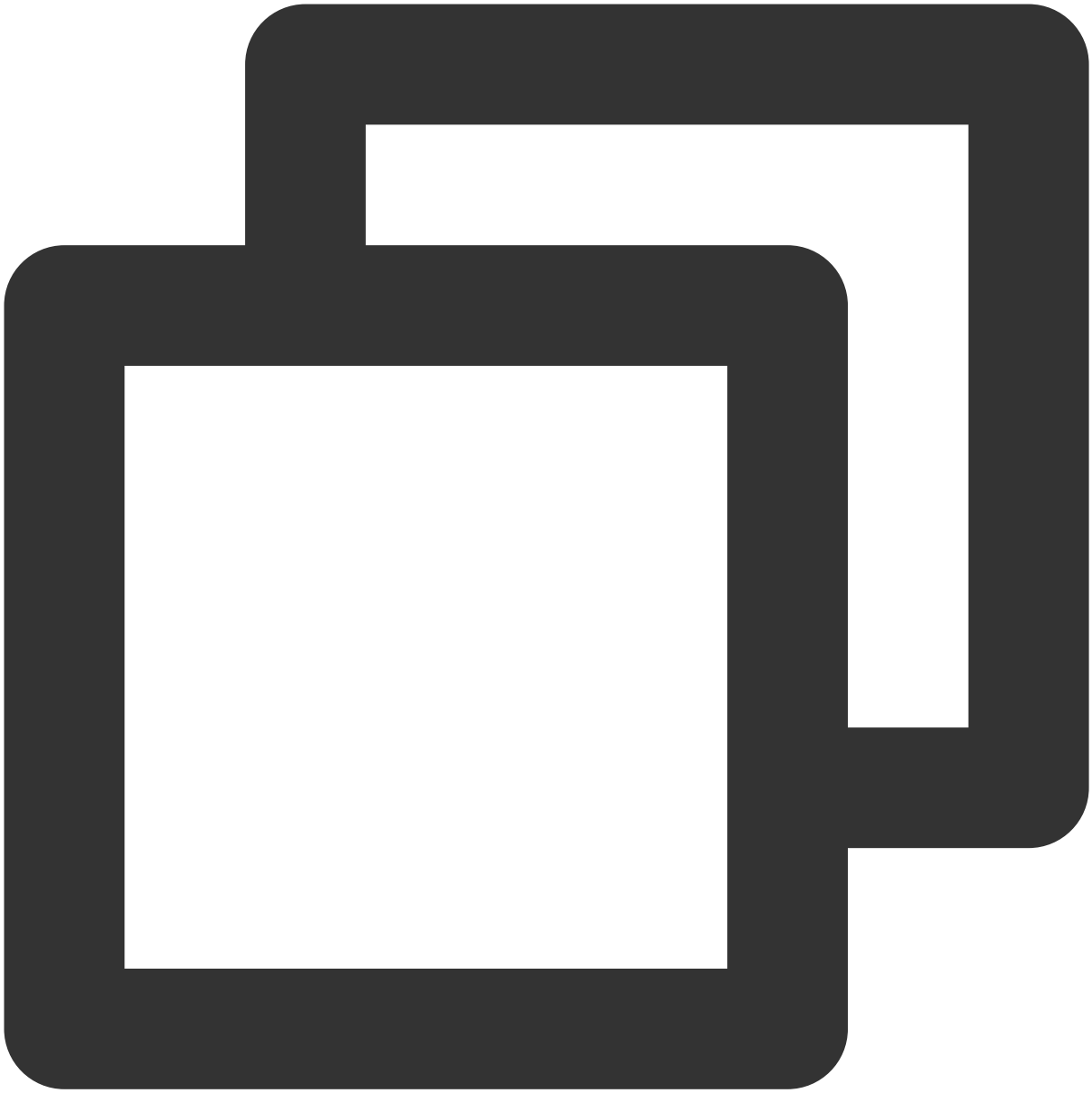
新しいカーネルのインストール

1. 次のコマンドを実行し、ELRepoリポジトリで現在システムがサポートしているカーネルパッケージを表示します。



```
yum --disablerepo="*" --enablerepo="elrepo-kernel" list available
```

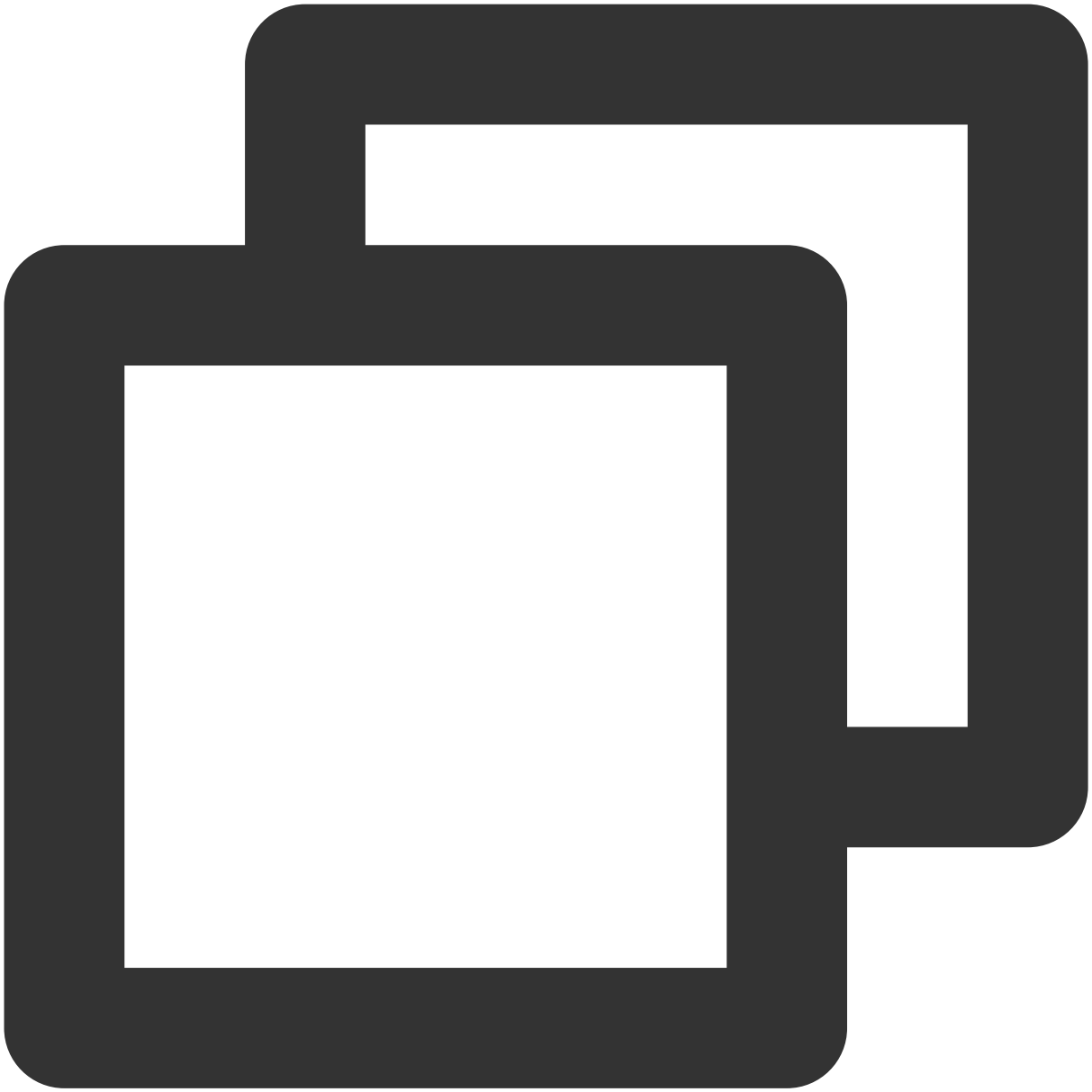
2. 次のコマンドを実行し、最新のメインライン・安定版のカーネルをインストールします。



```
yum --enablerepo=elrepo-kernel install kernel-ml
```

grub設定の変更

1. 以下のコマンドを実行して、 `/etc/default/grub` ファイルを開きます。

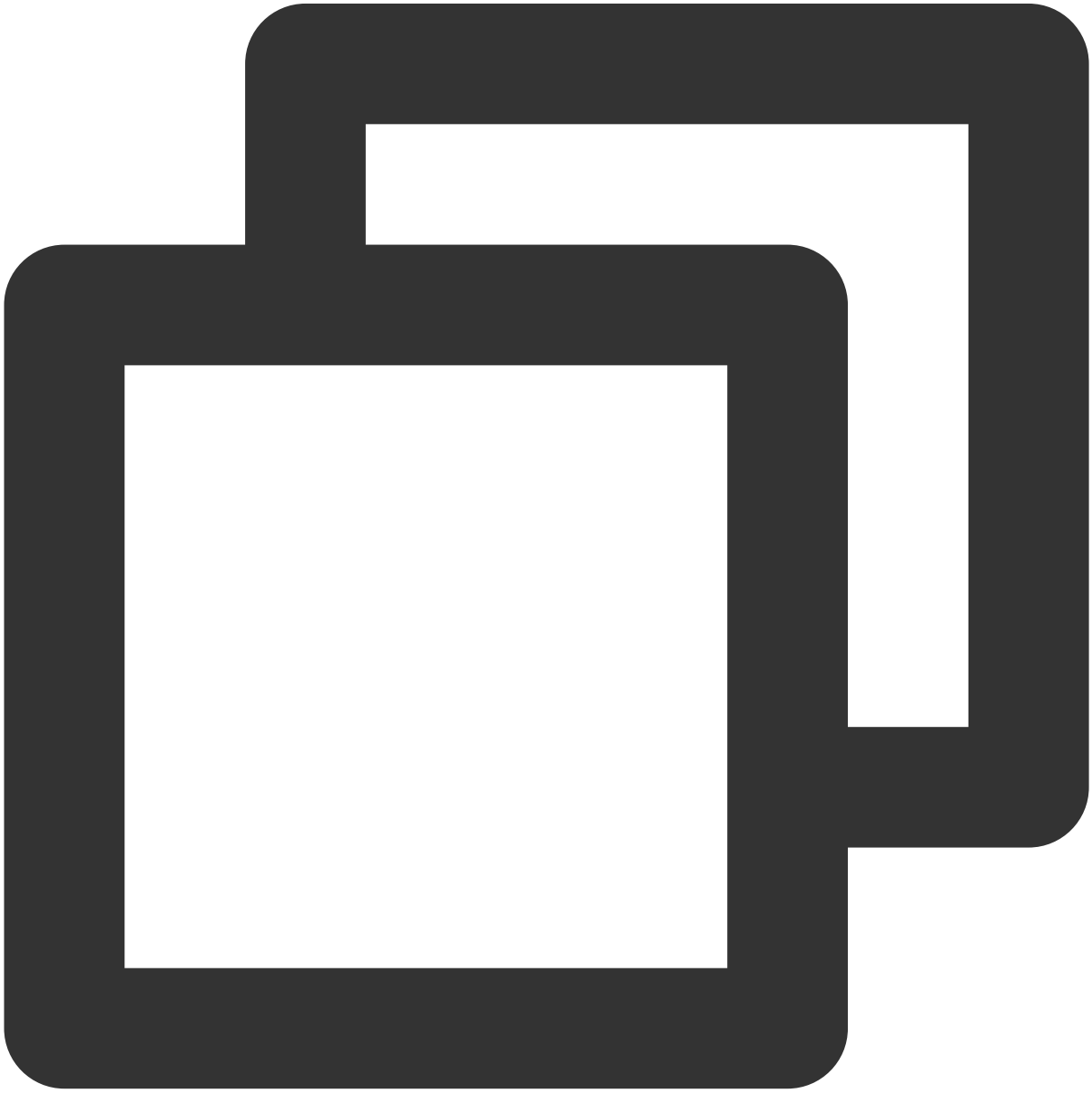


```
vim /etc/default/grub
```

2. **i**を押して編集モードに切り替え、`GRUB_DEFAULT=saved` を `GRUB_DEFAULT=0` に変更します。

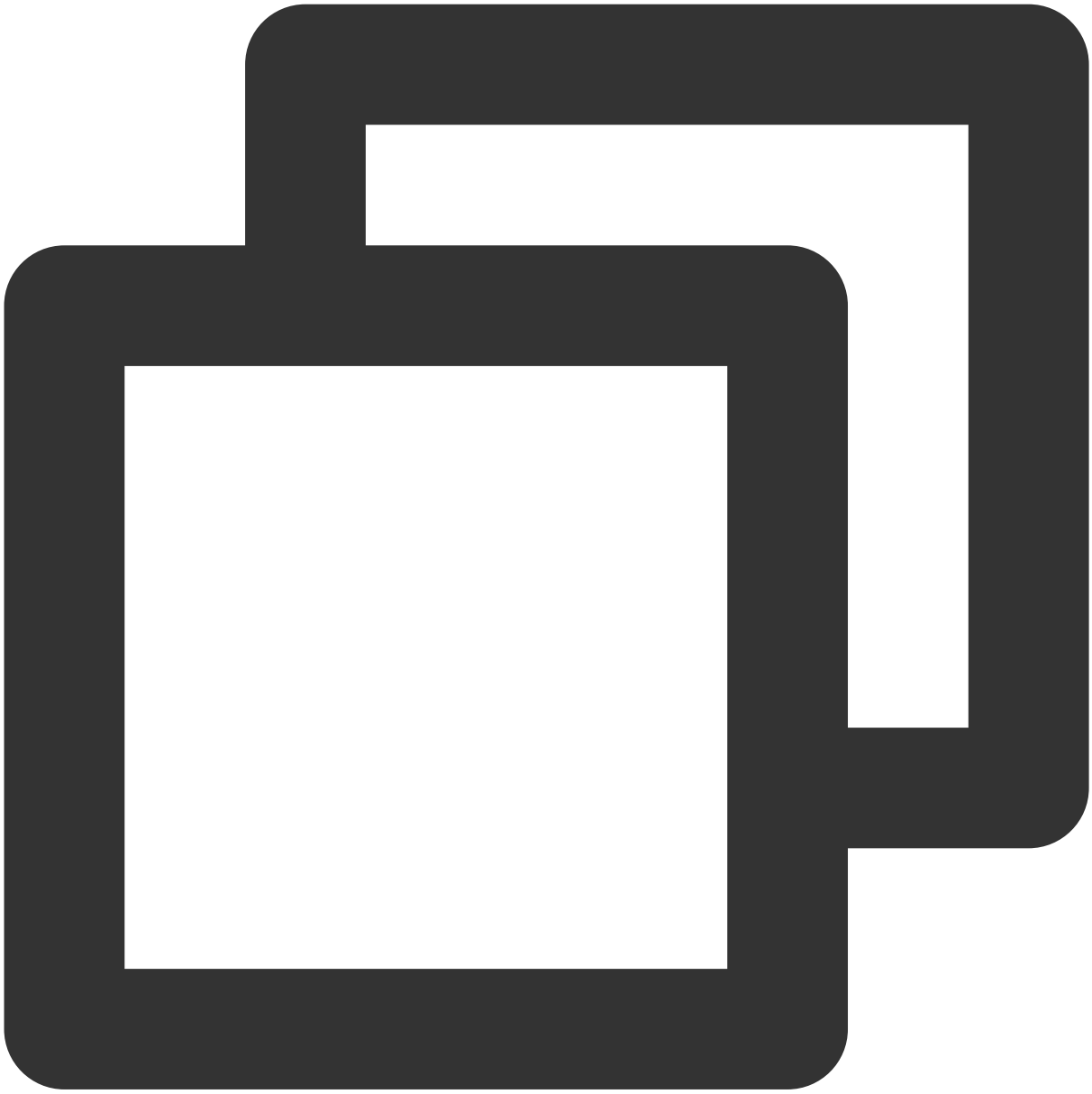
```
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=0
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL="serial console"
GRUB_TERMINAL_OUTPUT="serial console"
GRUB_CMDLINE_LINUX="crashkernel=auto console=ttyS0 console=tty0 panic=5 net.ifnames=0 biosdevname=0
GRUB_DISABLE_RECOVERY="true"
GRUB_SERIAL_COMMAND="serial --speed=9600 --unit=0 --word=8 --parity=no --stop=1"
```

3. **Esc**を押し、**:wq**を入力して、ファイルを保存して戻ります。
4. 次のコマンドを実行して、Kernel設定をあらためて生成します。



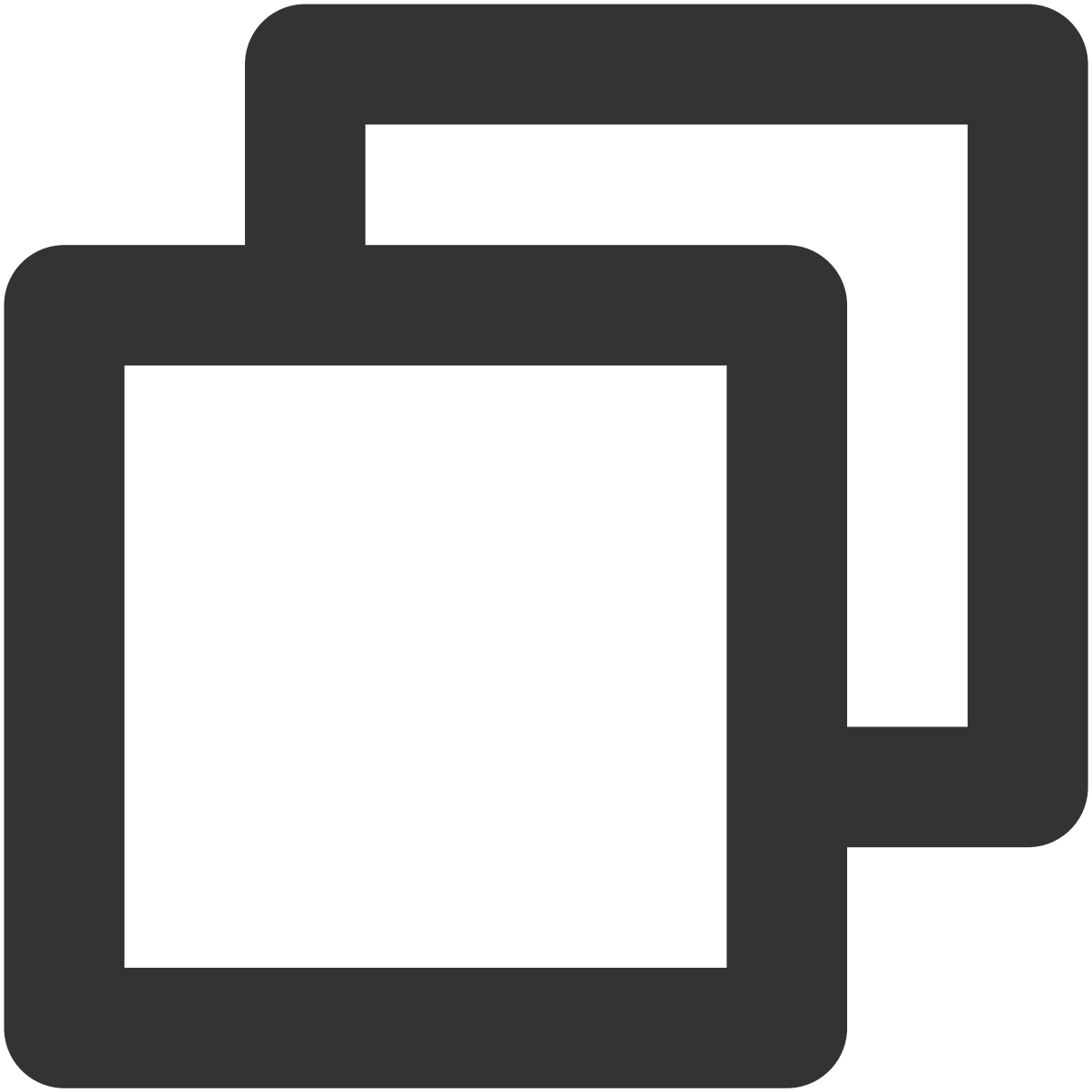
```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

5. 次のコマンドを実行して、マシンを再起動します。



```
reboot
```

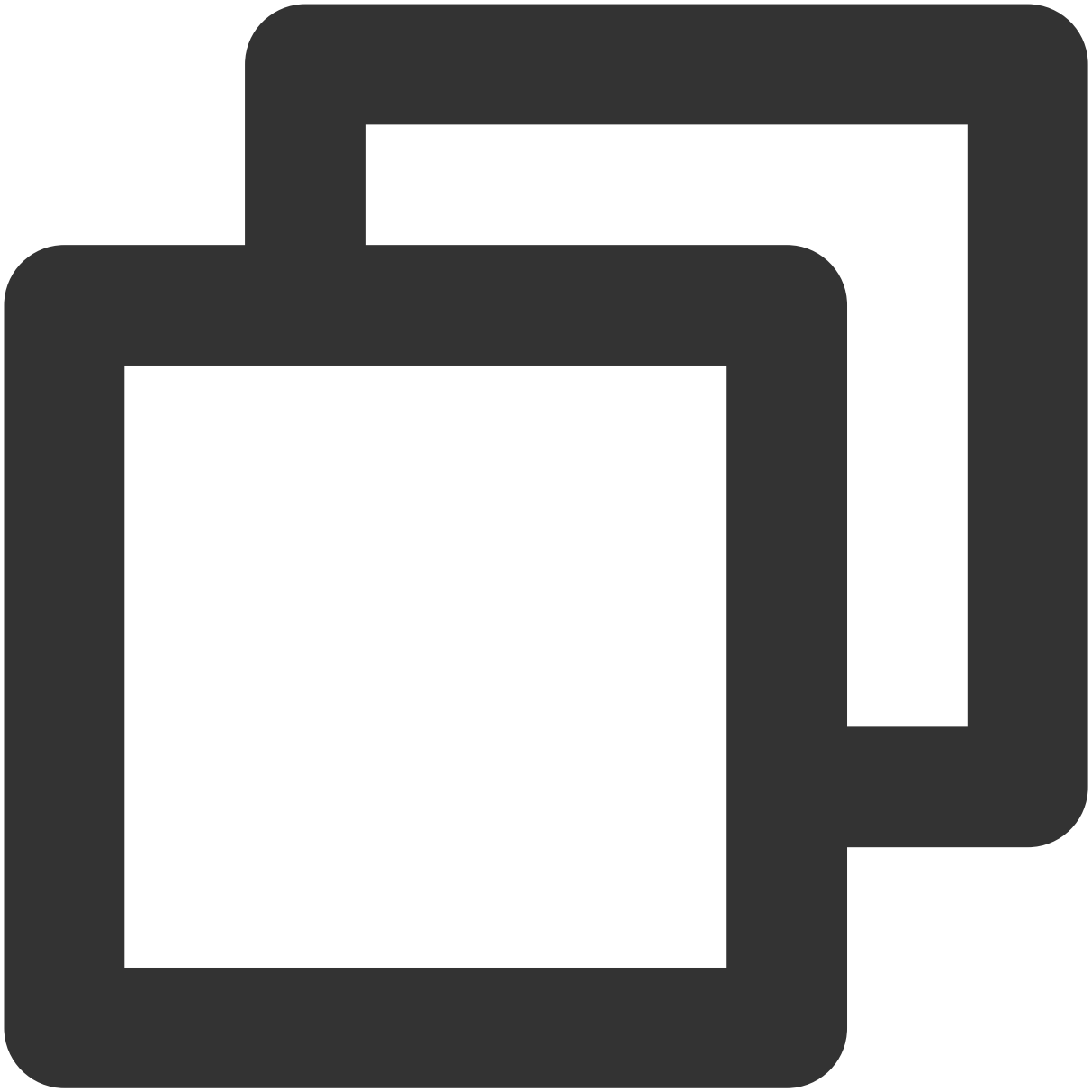
6. 次のコマンドを実行して、変更が成功したかどうかをチェックします。



```
uname -r
```

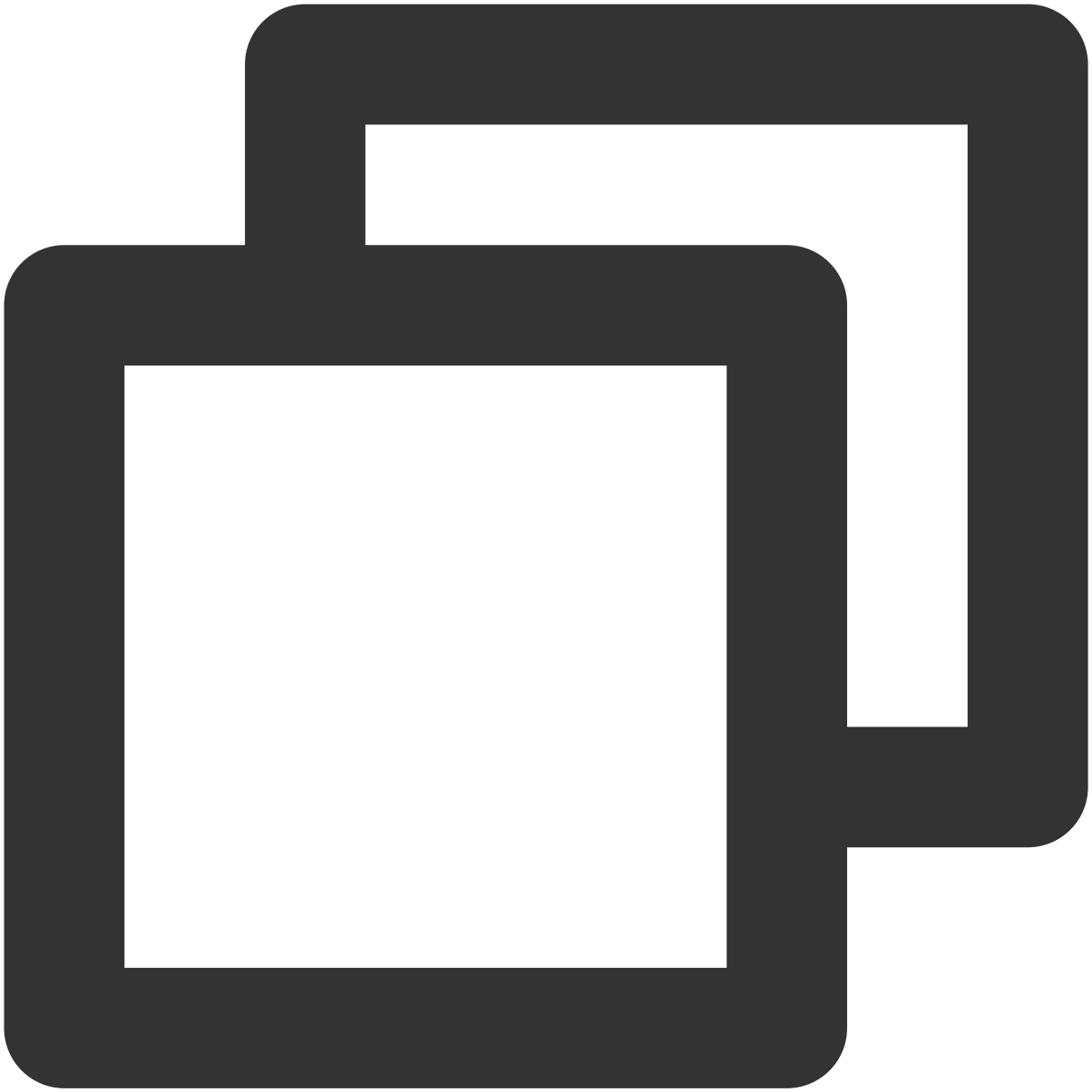
余分なカーネルの削除

1. 次のコマンドを実行して、すべてのKernelを表示します。



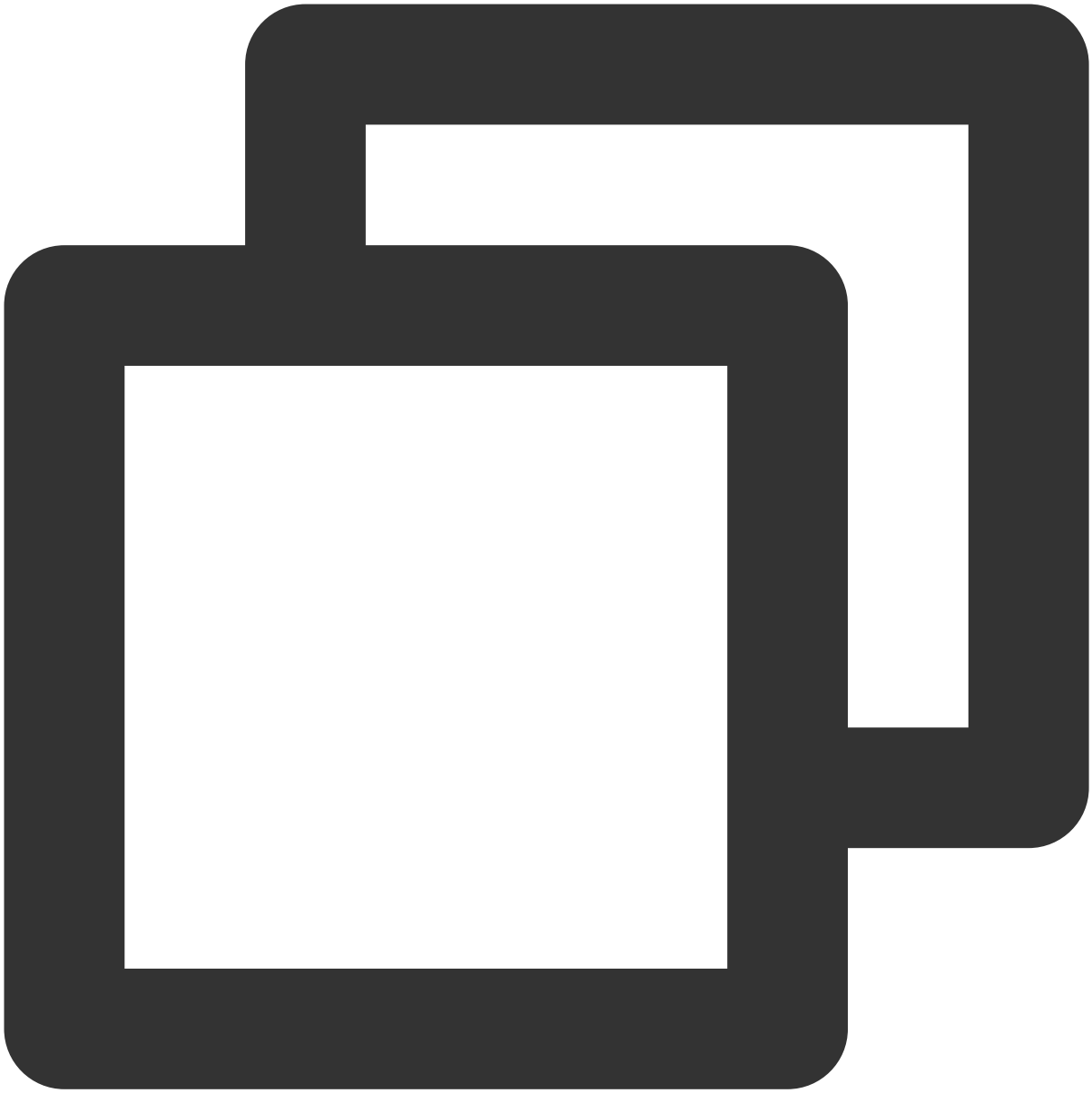
```
rpm -qa | grep kernel
```

2. 次のコマンドを実行して、旧バージョンのカーネルを削除します。



```
yum remove kernel-old_kernel_version
```

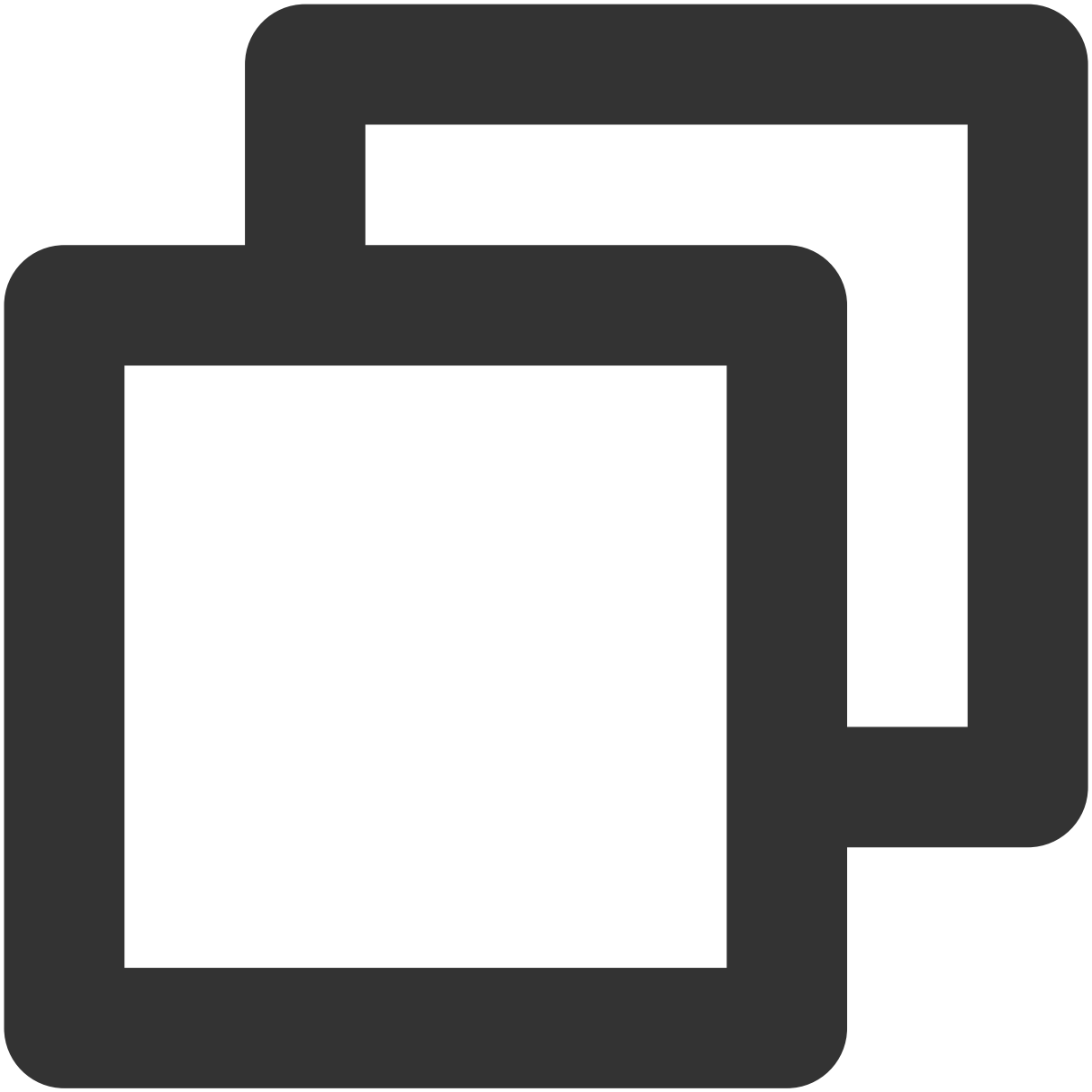
例：



```
yum remove kernel-3.10.0-957.el7.x86_64
```

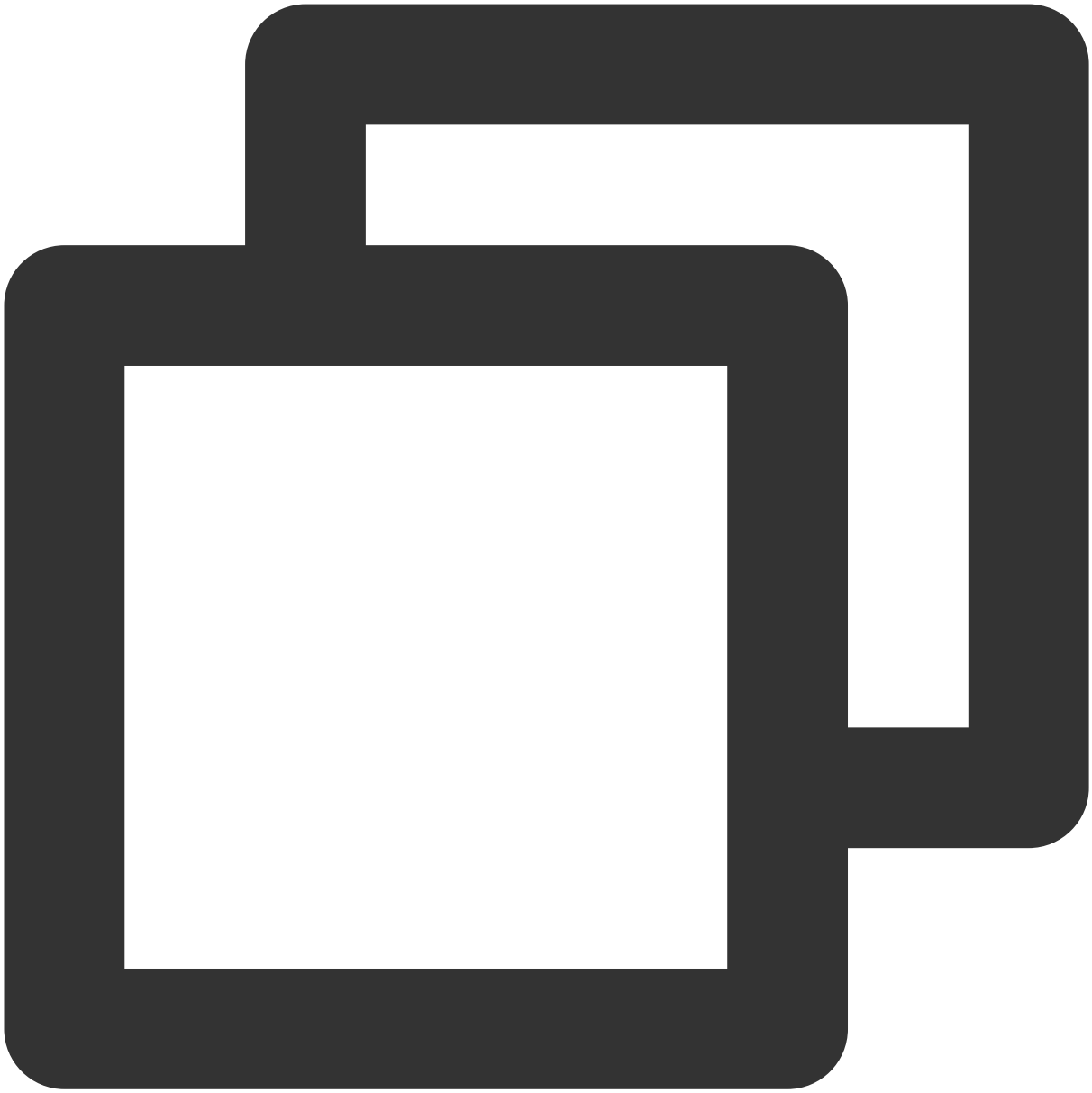
BBRの有効化

1. 次のコマンドを実行して、 `/etc/sysctl.conf` ファイルを編集します。



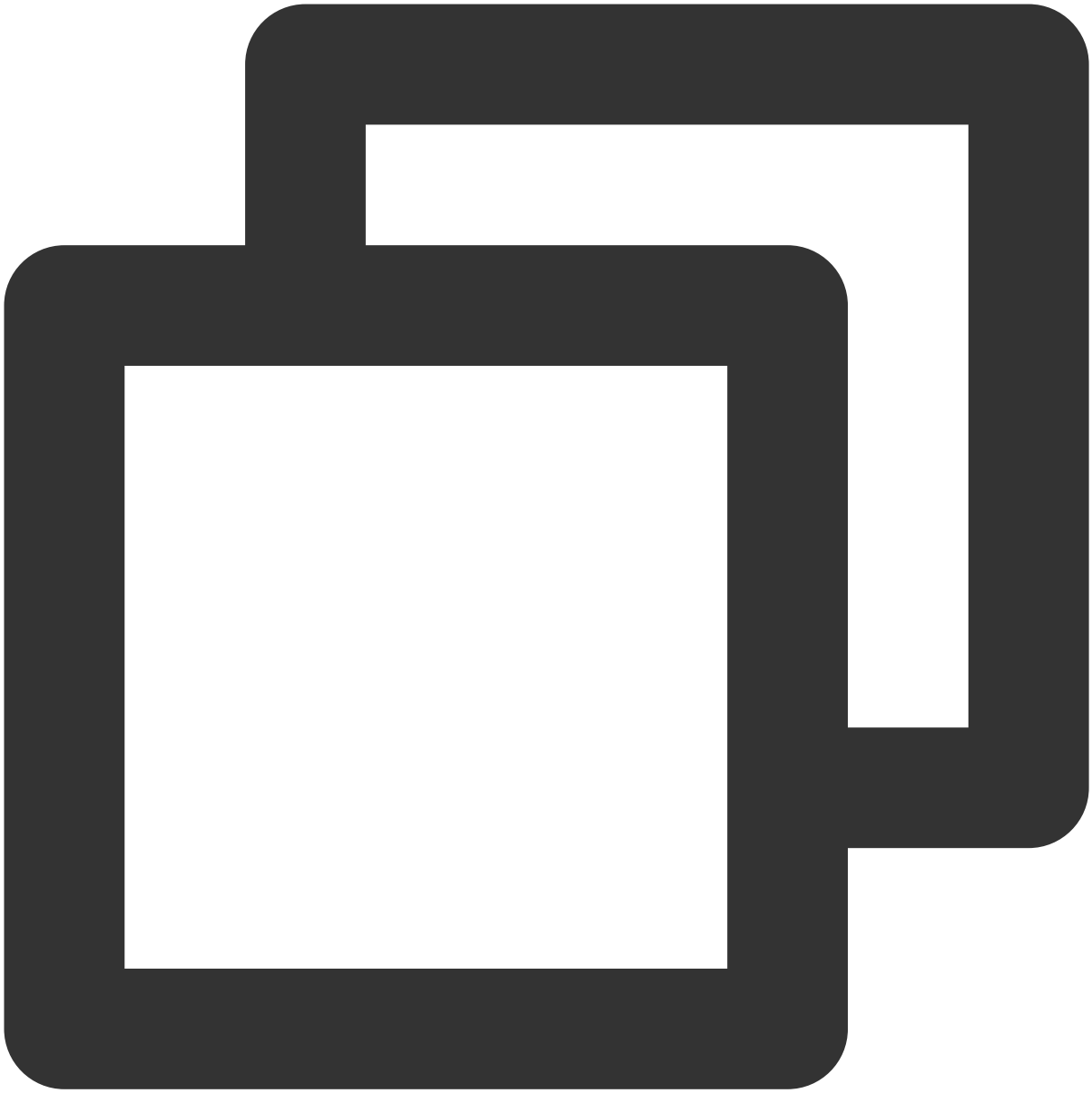
```
vim /etc/sysctl.conf
```

2. **i**を押して編集モードに切り替え、次の内容を追加します。



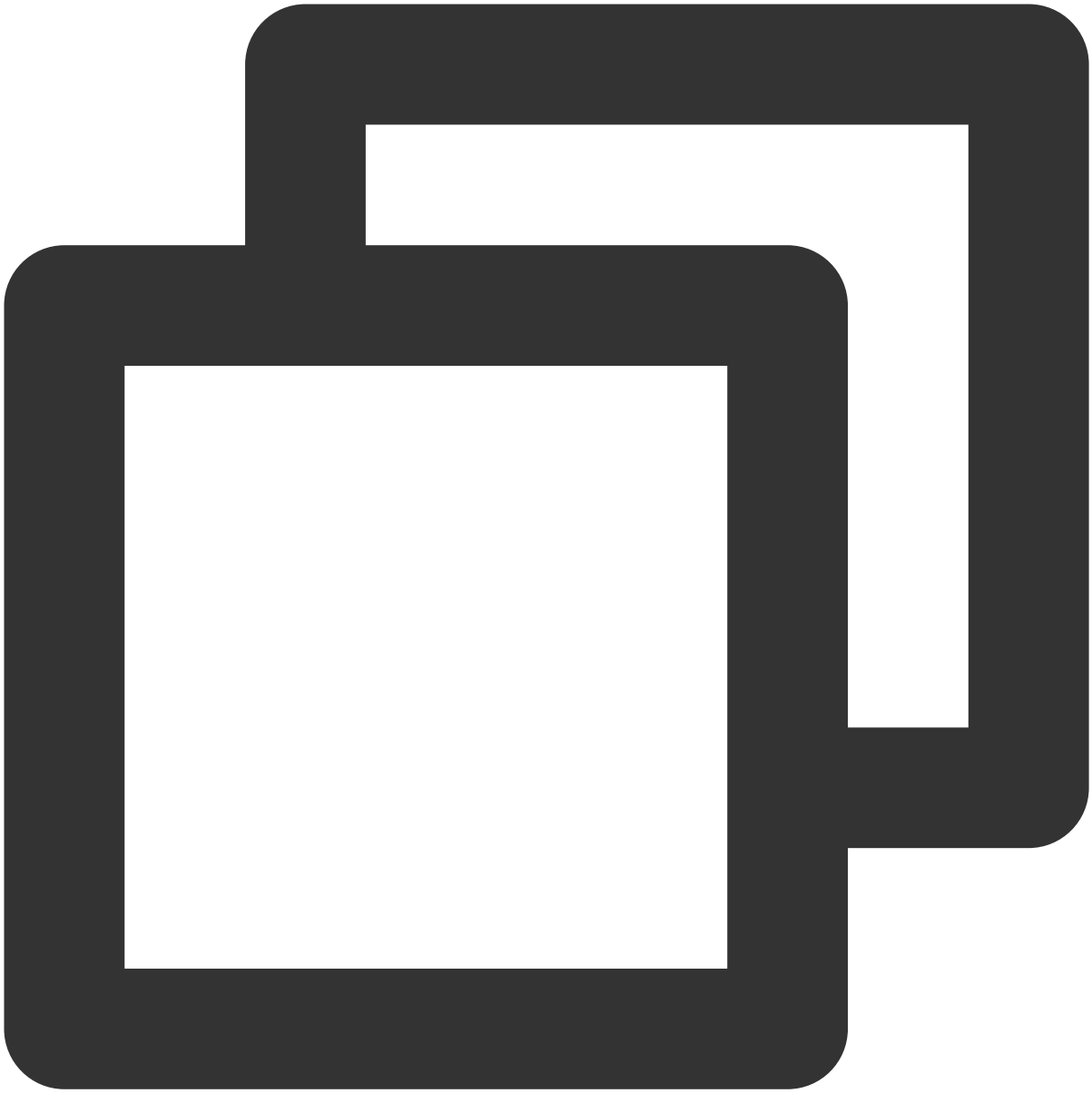
```
net.core.default_qdisc=fq
net.ipv4.tcp_congestion_control=bbr
```

3. **Esc**を押し、**:wq**を入力して、ファイルを保存して戻ります。
4. 次のコマンドを実行して、`/etc/sysctl.conf` 設定ファイルからカーネルパラメータ設定をロードします。

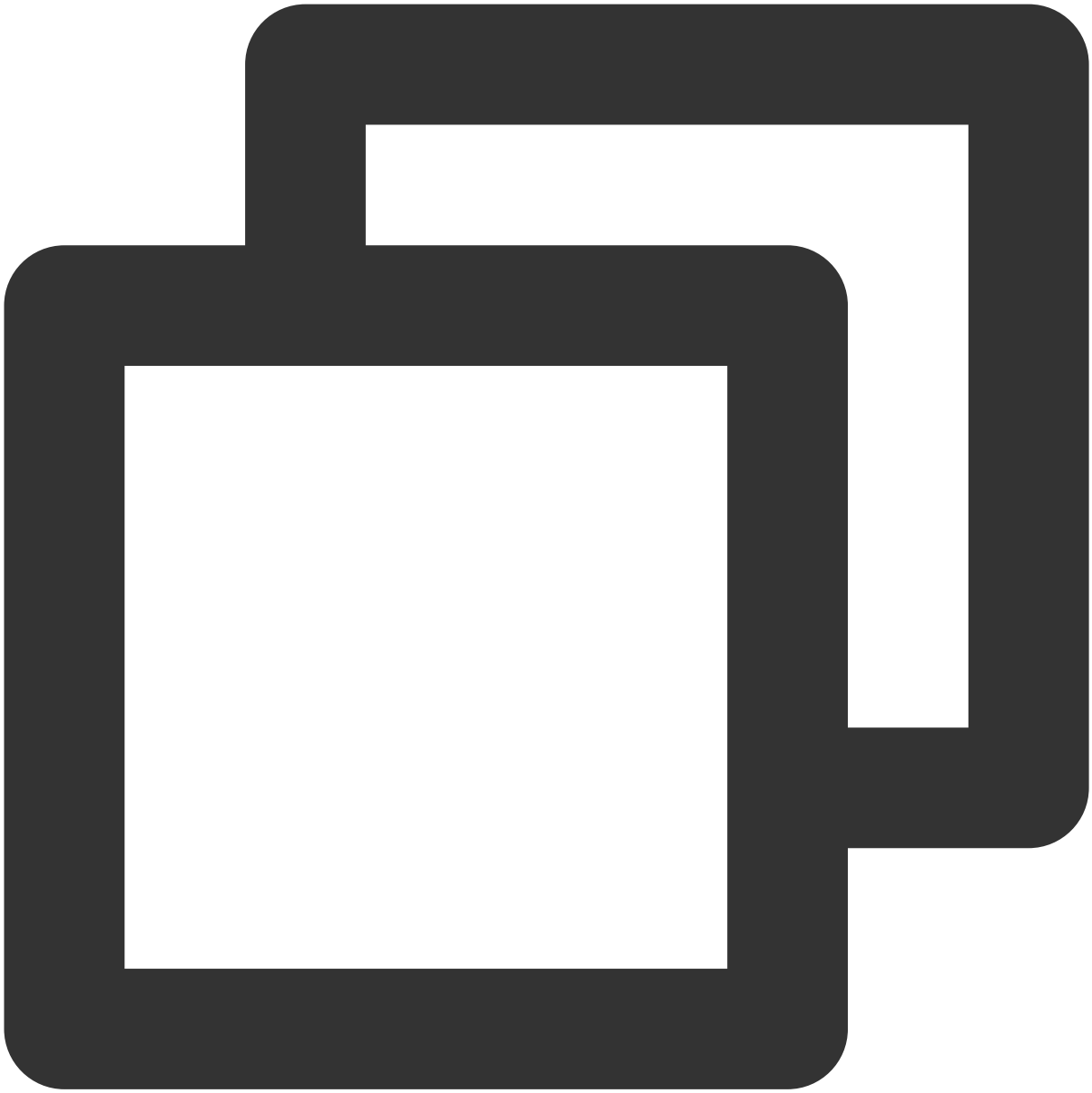


```
sysctl -p
```

5. 次のコマンドを順次実行して、BBRの有効化が成功したかどうか検証します。

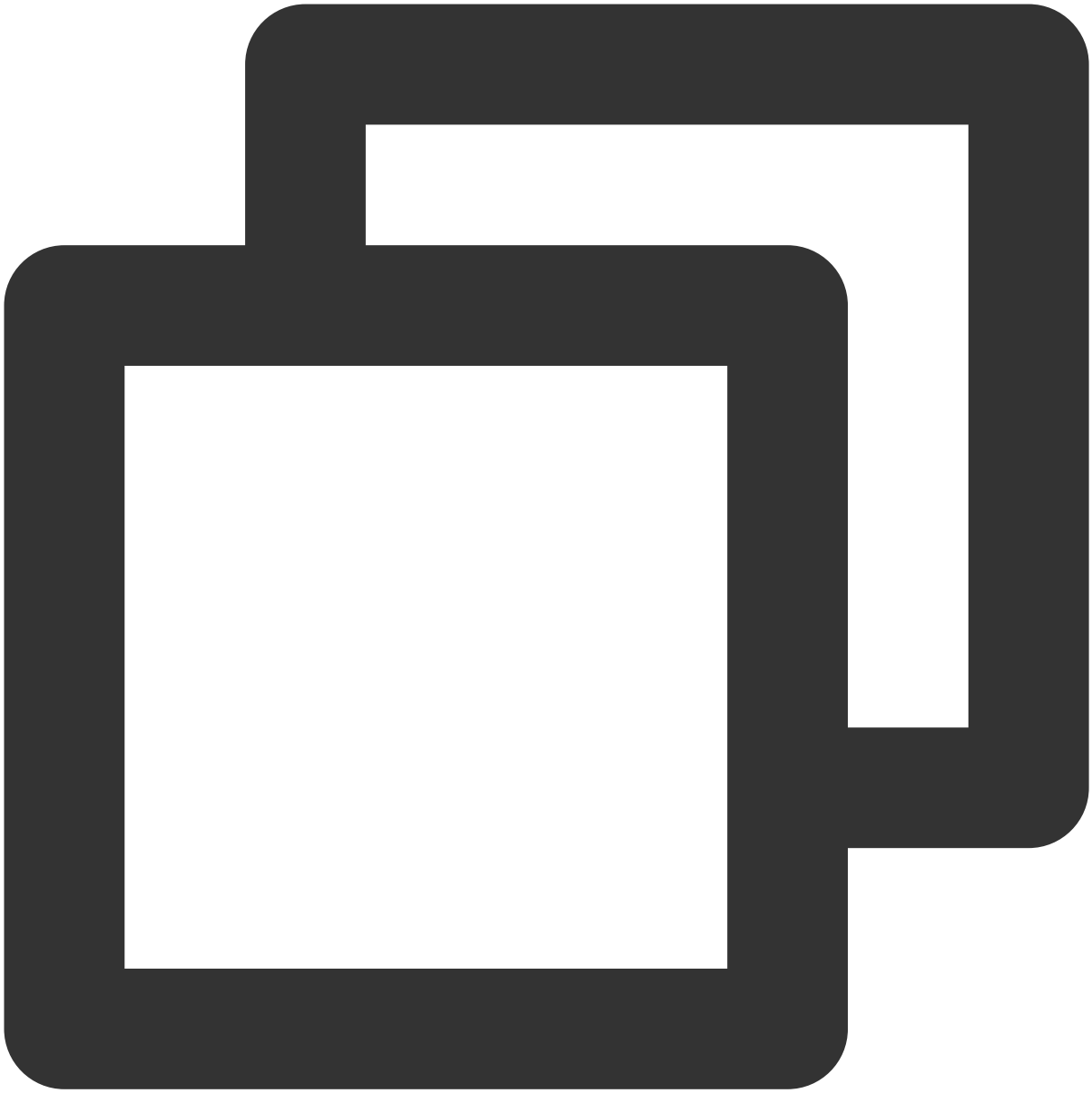


```
sysctl net.ipv4.tcp_congestion_control
# 次の内容が表示されればOKです。
# net.ipv4.tcp_congestion_control = bbr
```



```
sysctl net.ipv4.tcp_available_congestion_control
# 次の内容が表示されればOKです。
# net.ipv4.tcp_available_congestion_control = reno cubic bbr
```

6. 次のコマンドを実行して、カーネルモジュールがロードされたかどうか確認します。



```
lsmod | grep bbr
```

次の情報が返ってきた場合、有効化が成功したことを意味します。

```
[root@VM_0_51_centos ~]# lsmod | grep bbr
tcp_bbr                20480  1
```

Cloud Virtual MachineによるWindowsシステムのADドメインの構築

最終更新日：：2022-05-06 15:46:33

概要

アクティブディレクトリAD（Active Directory）はMicrosoftサービスの主要なコンポーネントです。ADではユーザーの一括管理、アプリケーションのデプロイメント、 パッチの更新等の、効果的な管理を実現することができます。Microsoftの多くのコンポーネント（Exchange等）およびフェイルオーバークラスターにもADドメイン環境が必要です。この文書ではWindows Server 2012 R2 Datacenterエディション64ビットオペレーティングシステムを例にして、ADドメインの構築方法をご紹介します。

前提条件

2つのWindows Cloud Virtual Machine (CVM)インスタンスを作成し、ドメインコントローラ（DC）およびクライアント（Client）に割り当て済みであること。
作成したインスタンスが以下の条件を満たしていること：
NTFSパーティションにパーティション化されている。
インスタンスがDNSサービスをサポートしている。
インスタンスがTCP/IPプロトコルをサポートしている。

インスタンスネットワーク環境

グループネットワーク情報：ネットワークタイプはVirtual Private Cloud (VPC)を採用し、スイッチハブのプライベートネットワークセグメントは10.0.0.0/16です。
ドメイン名情報：例示のインスタンスのドメイン名は `example.com` です。DCのCVMインスタンスのIPアドレスは10.0.5.102で、クライアントのCVMインスタンスのIPアドレスは10.0.5.97です。
ご注意：
ADドメインの構築後、CVMインスタンスが常に同じIPアドレスを使用していることを確認してください。IPアドレスが変更されるとアクセスに異常が発生する可能性があります。

関連概念

アクティブディレクトリAD（Active Directory）はMicrosoftサービスの主要なコンポーネントです。関連用語の概念は以下のとおりです：

DC：Domain Controllers。ドメインコントローラです。

DN：Distinguished Name。識別名です。

OU：Organizational Unit。組織単位です。

CN：Canonical Name。正式名称です。

SID：Security Identifier。セキュリティ識別子です。

操作手順

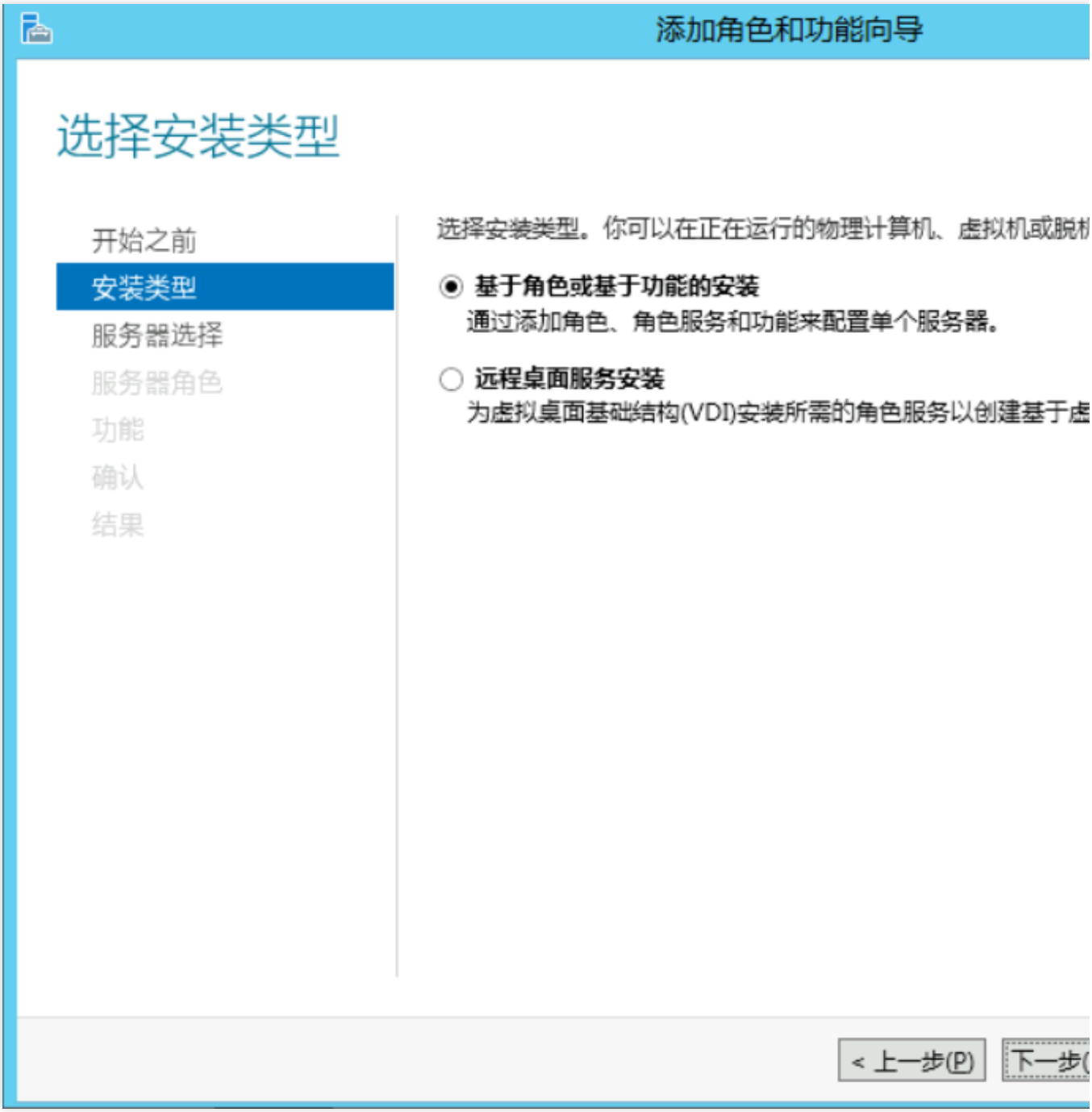
説明：

既存のドメインコントローラを使用してカスタムイメージを作成し、新しいデプロイコントローラをデプロイメントすることは推奨されません。どうしても使用する必要がある場合は、新規作成したインスタンスのホスト名(hostname）とカスタムイメージ作成前のインスタンスのホスト名が一致していることを確認してください。一致していないと「サーバー上のセキュリティデータベースにこのワークステーションの信頼関係が存在しません」というエラーメッセージが表示されます。インスタンスを作成してから同じホスト名に変更すると、この問題が解決されます。

ADドメインコントローラのデプロイ

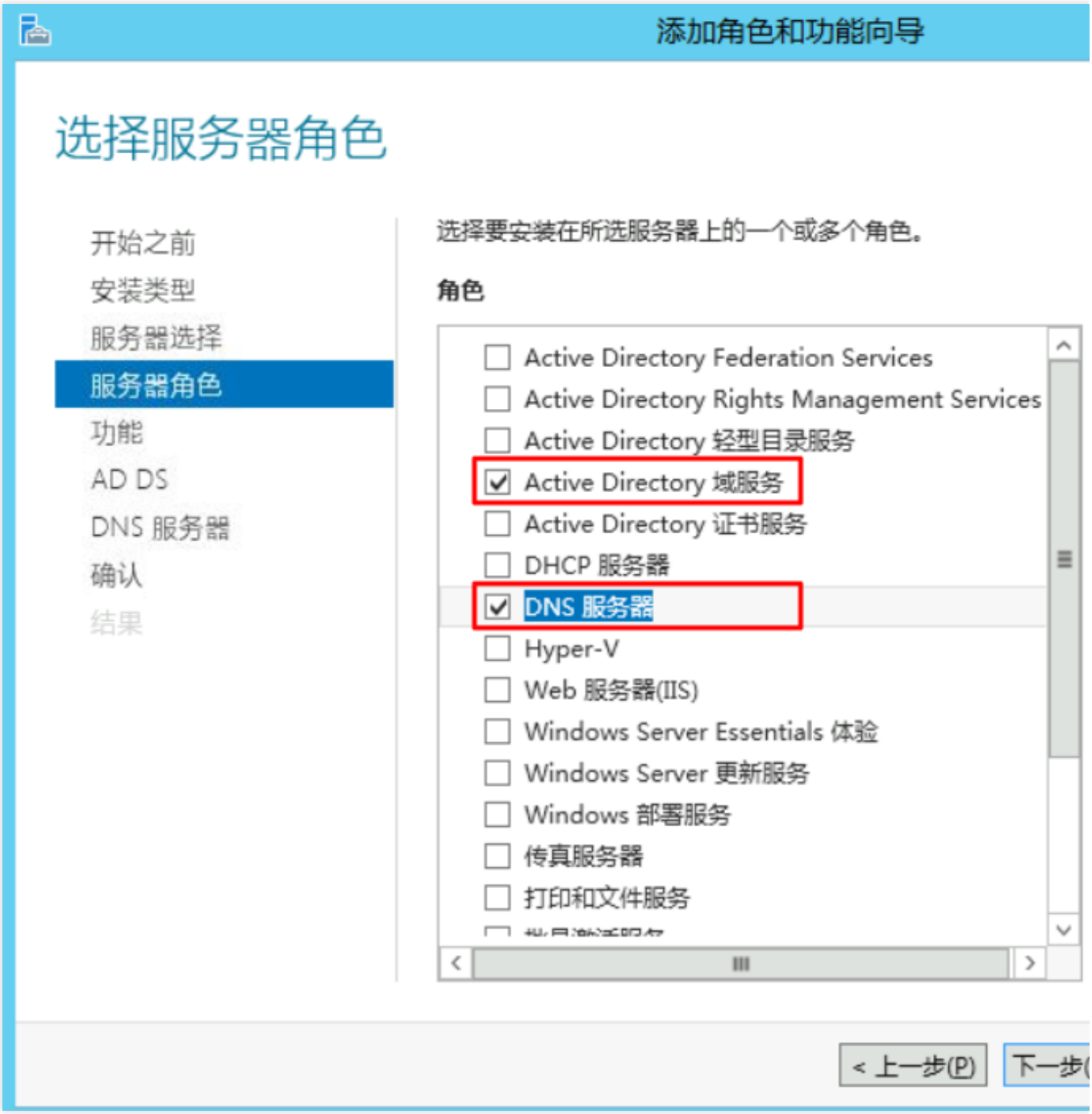
1. DCにするインスタンスにログインします。詳細については、標準方式を使用してWindowsインスタンスにログイン をご参照ください。
2. オペレーティングシステムのインターフェースで、

をクリックして、サーバーマネージャーを開きます。
3. **ロールと機能の追加**をクリックすると、「ロールと機能の追加ウィザード」ウィンドウがポップアップします。
4. 「インストールタイプの選択」インターフェースで、**ロールまたは機能に基づくインストール**を選択して、[次のステップ]を連続して2回クリックします。下図のとおりです。



5. 「サーバーロールの選択」インターフェースで、下図に示す「Active Directoryドメインサービス」および「DNSサーバー」にチェックを入れて、ポップアップ画面で**機能の追加**および**続ける**をクリックします。

この手順では、ADドメインサービスおよびDNSサービスデプロイが同じインスタンス上にある場合を例にしています。



6. デフォルトの設定を維持したまま、**次へ**を4回続けてクリックします。
7. 情報の確認ページで、**インストール**をクリックします。

インストールの完了後、「ロールおよび機能の追加」ダイアログボックスを閉じます。

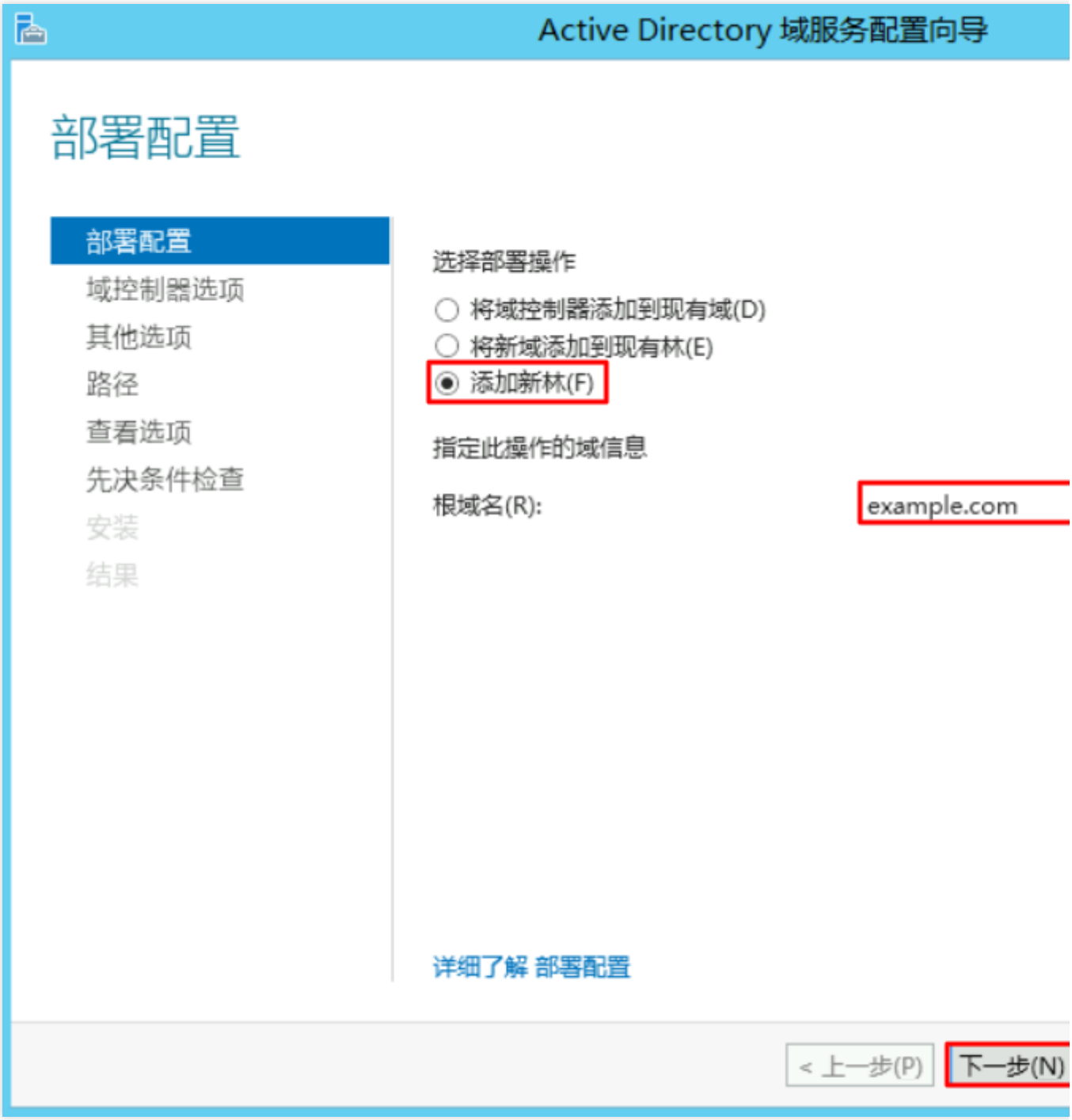
8. オペレーティングシステムのインターフェースで、

をクリックして、サーバーマネージャーを開きます。

9. サーバーマネージャーのウィンドウで、

をクリックして、**このサーバーをドメインコントローラに変更する**を選択します。下図のとおりです。

10. 開いた「Active Directoryドメインサービスの設定ウィザード」画面で、「デプロイ操作の選択」設定を**フォレストの新規追加**にして、ルートドメイン名を入力し(この文書では「example.com」)、**次へ**をクリックします。下図のとおりです。



11. ディレクトリサービス復元モデル（DSRM）のパスワードを設定して、**次へ**をクリックします。下図のとおりです。

12. デフォルトの設定を維持したまま、**次へ**を4回続けてクリックします。
13. 「前提条件の検査中」で、**インストール**をクリックしてADドメインサーバーのインストールを開始します。インストールが完了すると自動的にインスタンスが再起動し、インスタンスに再接続すると、**コントロールパネル > システムとセキュリティ > システム**にインストール結果が表示されます。下図のとおりです。

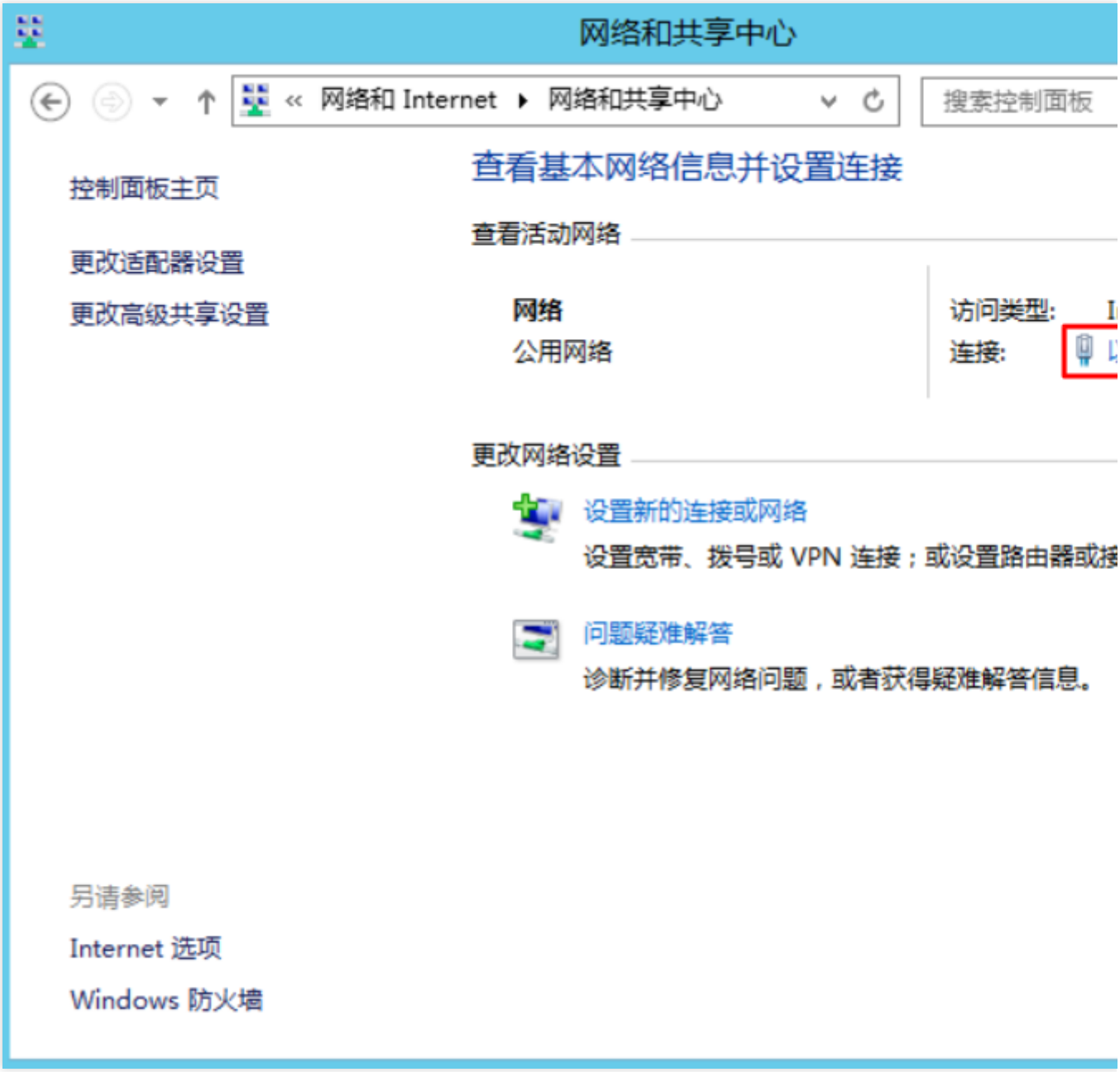
クライアントSIDの変更

SIDの変更操作の説明 をご参考の上、クライアントインスタンスにするSIDを変更してください。

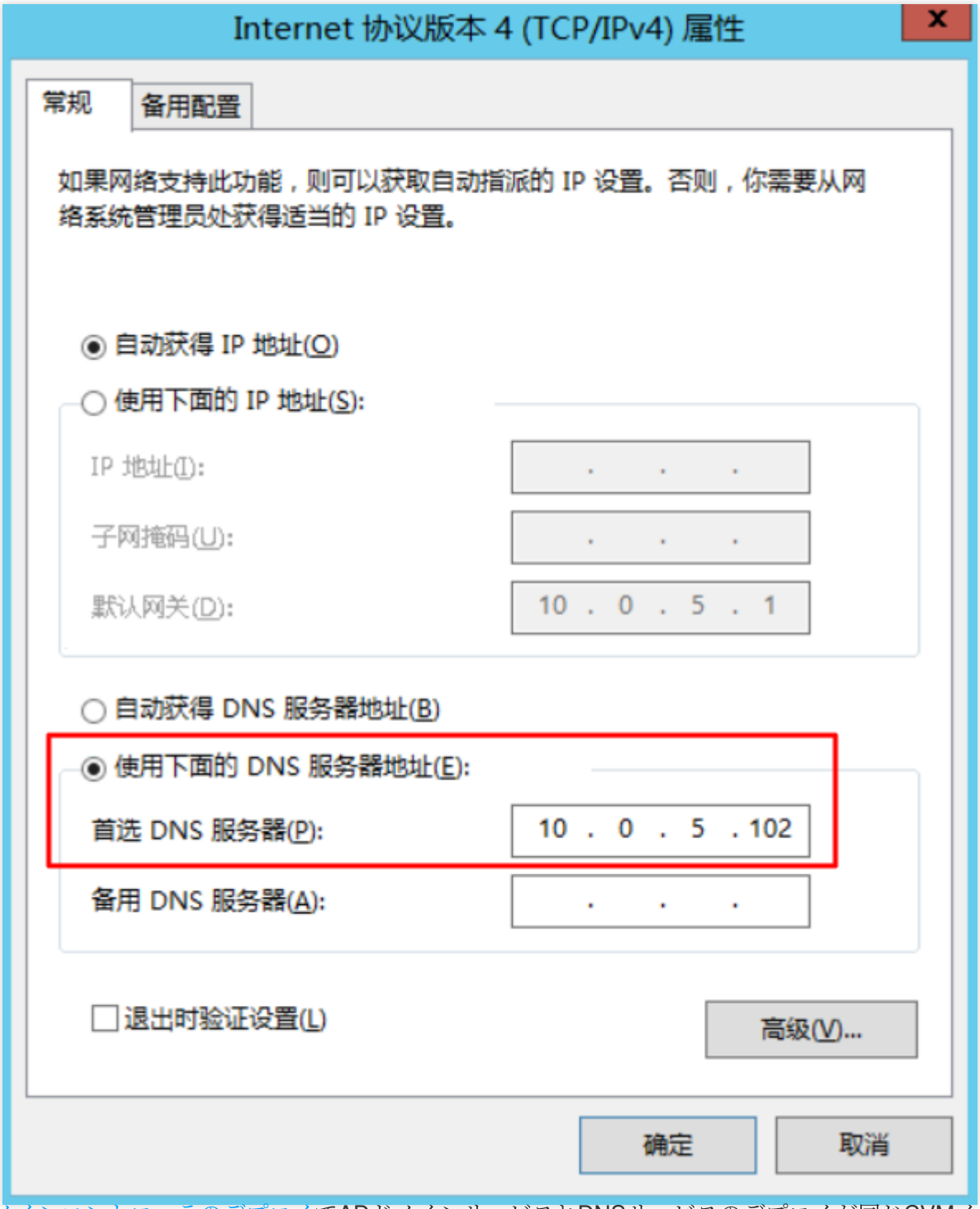
クライアントのADドメインへの追加

1. クライアントにするインスタンスにログインします。詳細については、標準方式を使用してWindowsインスタンスにログイン をご参照ください。

2. DNSサーバーアドレスを変更します。
3. **コントロールパネル** > **ネットワークとインターネット** > **ネットワークと共有センター**の順に開いて、「ネットワークと共有センター」画面で**イーサネット**をクリックします。下図のとおりです。



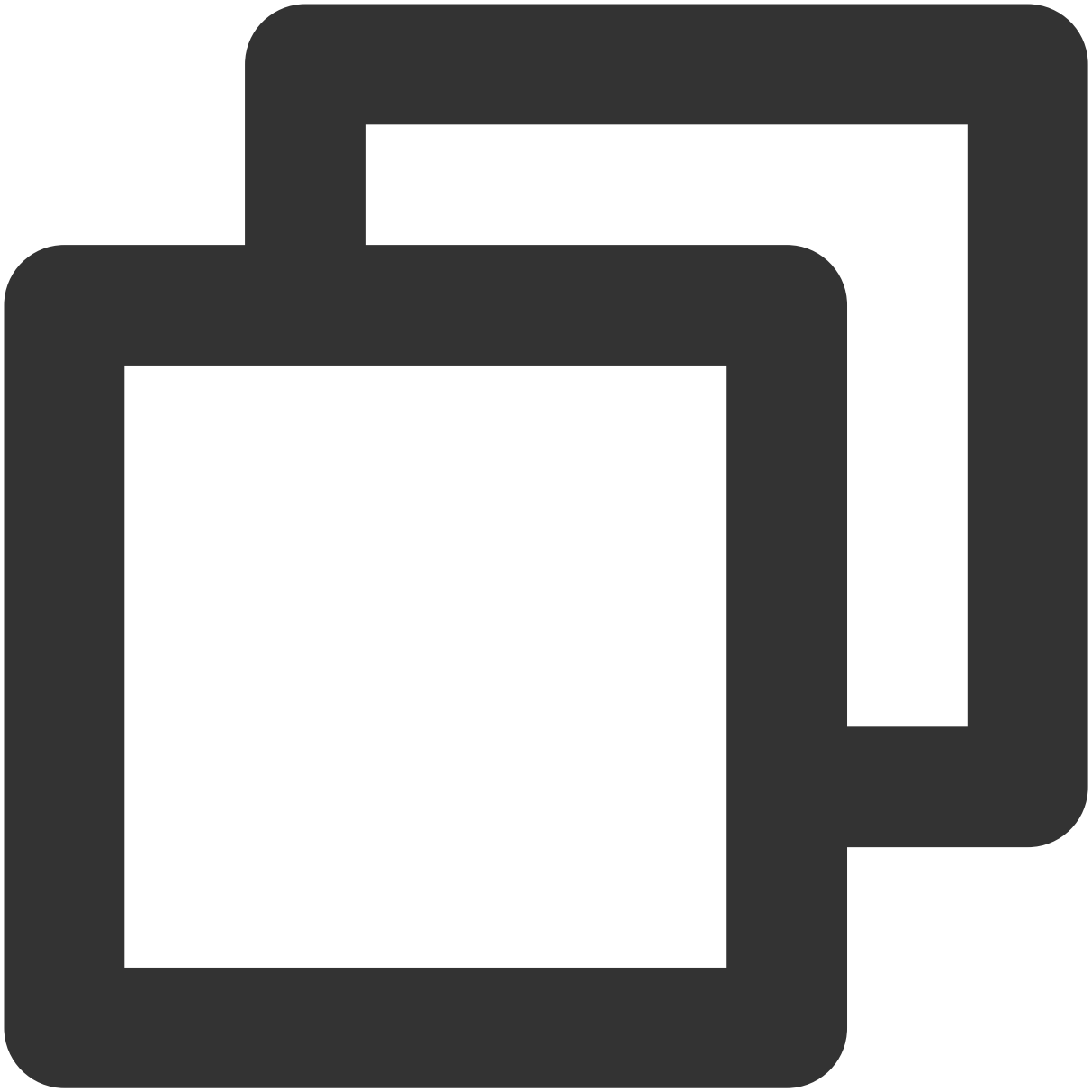
4. 「イーサネットのステータス」画面で、**属性**をクリックします。
5. 「イーサネットの属性」画面で「Internetプロトコルバージョン4（TCP/IPv4）」を選択して、**属性**をクリックします。
6. 「Internetプロトコルバージョン4（TCP/IPv4）の属性」画面で、「以下のDNSサーバーアドレスを使用する」を選択して、最初に選択したDNSサーバーアドレスの設定をDCインスタンスのIPアドレスにします(ここでは `10.0.5.102`)。下図のとおりです。



ADドメインコントローラのデプロイでADドメインサービスとDNSサービスのデプロイが同じCVMインスタンス上（IPアドレスは10.0.5.102）に設定済みなので、ここではDNSサーバーのアドレスを10.0.5.102に指定します。

7. **OK**をクリックして、変更を保存します。

8. cmdウィンドウで、以下のコマンドを実行して、PingがDNSサーバーのIPアドレスを通過できるかを確認します。

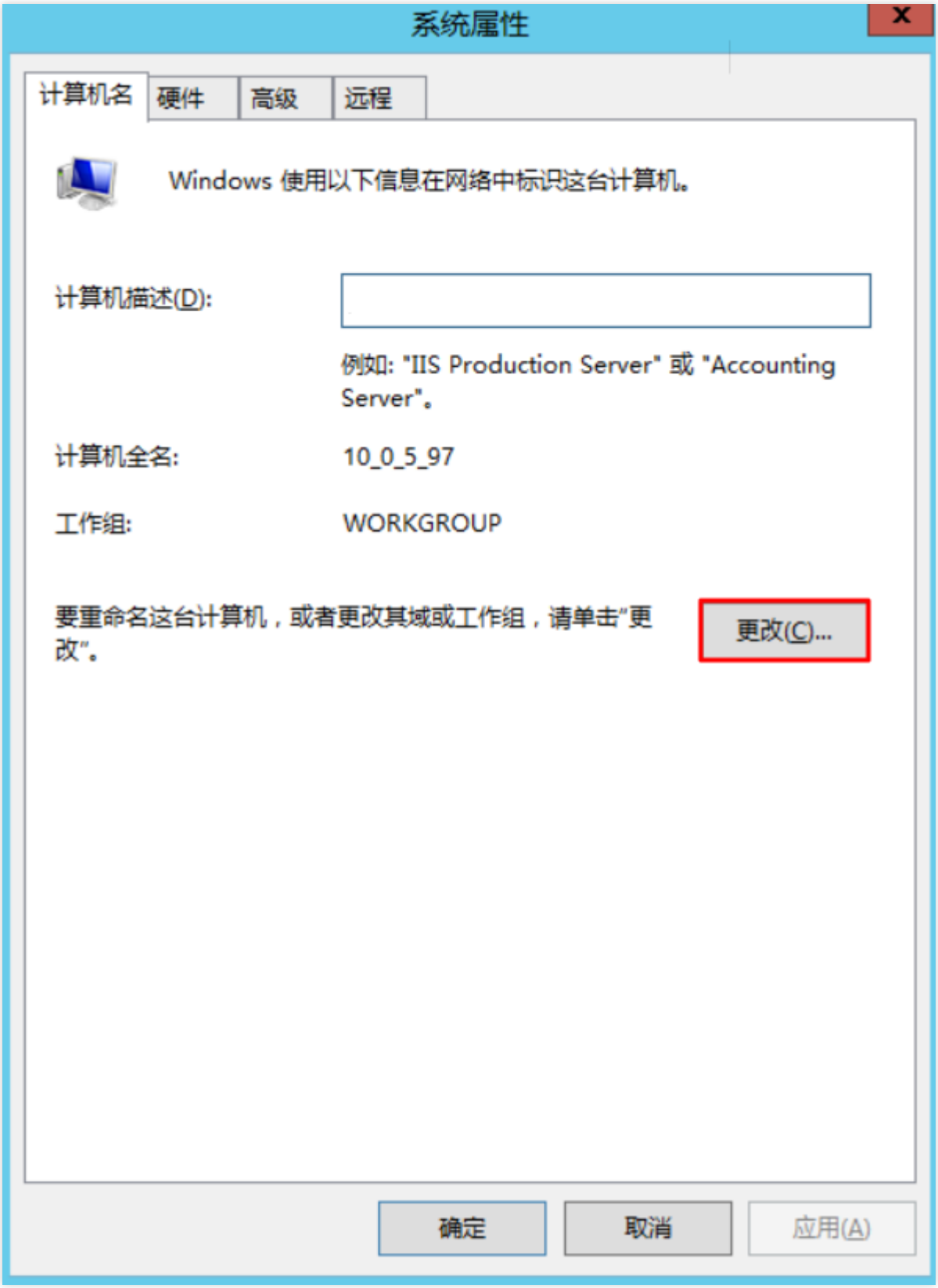


```
ping example.com
```

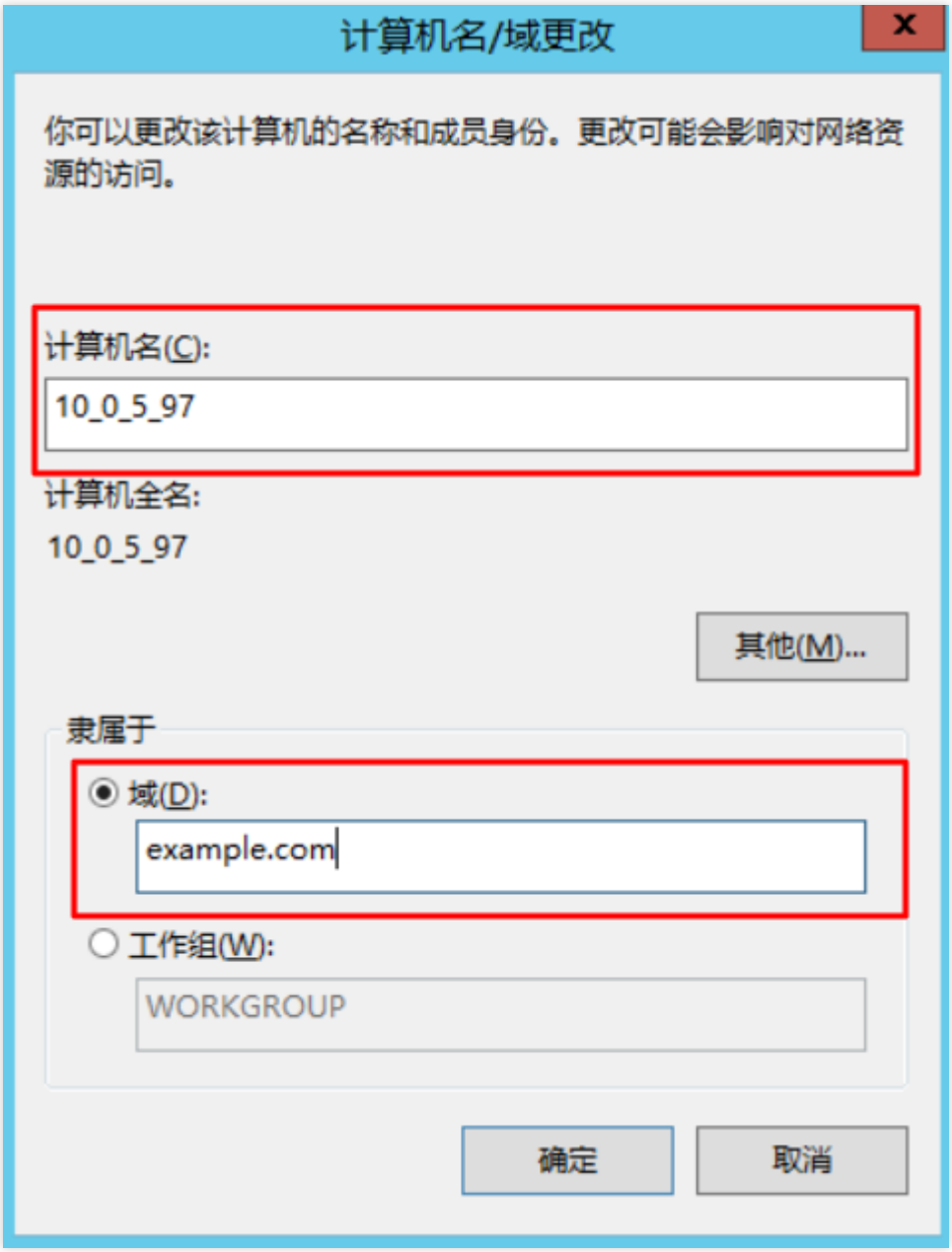
返された結果は下図のようになり、PingがDNSサーバーのIPアドレスを通過できることを示しています。

9. **コントロールパネル** > **システムとセキュリティ** > **システム**の順に開いて、「システム」画面で**設定の変更**をクリックします。下図のとおりです。

10. 表示された「システムの属性」ウィンドウで、**変更**をクリックします。下図のとおりです。



11. 表示された「コンピュータ名/ドメインの変更」ウィンドウで、変更する必要があるコンピュータ名を押して、属する「ドメイン」を「example.com」に設定します。下図のとおりです。



12. **OK**をクリックします。
13. 表示される「Windowsセキュリティ」ウィンドウで、DCインスタンスのユーザー名を入力してパスワードを登録し、**OK**をクリックします。

下図のような確認画面が表示され、ドメインのログインが成功したことを示します。

14. **OK**をクリックして、インスタンスを再起動して設定を有効にします。

説明：

クライアントにするCVMインスタンスでは、ドメインにログイン済みのクライアントインスタンスを使用してカスタムイメージを作成しないようお勧めします。加入済みのものを使用すると、新規作成したイメージのインスタンスのせいで「サーバー上のセキュリティデータベースにこのワークステーションの信頼関係が存在しません」というエラーメッセージが表示されます。どうしても使用する必要がある場合は、新しいカスタムイメージを作成する前にドメインをログアウトすることをお勧めします。

ネットワーク性能のテスト

最終更新日：：2021-10-27 17:20:01

概要

このドキュメントでは、ツールを使用してCVMネットワークパフォーマンスをテストする方法について説明します。テストで取得したデータに基づいてCVMネットワークパフォーマンスを判断することができます。

ネットワークパフォーマンスのテストメトリクス

メトリック	説明
帯域幅（Mbits/秒）	単位時間（1秒）あたりに転送できる最大データ量（ビット）を表します。
TCP-RR（回/秒）	同じTCP接続において複数回のRequest/Response通信を行う時の応答効率を表します。データベースへのアクセスリンクにおいて、TCP-RRはよく利用される方式です。
UDP-STREAM（パケット/秒）	UDPがデータのバッチ転送を行う時のスループットを表し、ENIの最大転送能力を反映することができます。
TCP-STREAM（Mbits/秒）	TCPがデータのバッチ転送を行う時のスループットを表します。

ツールの基本情報

メトリック	説明
TCP-RR	Netperf
UDP-STREAM	Netperf
TCP-STREAM	Netperf
帯域幅	iperf
ppsの確認	sar

ENIキューの確認	ethtool

操作手順

テスト環境の構築

テストサーバーの準備

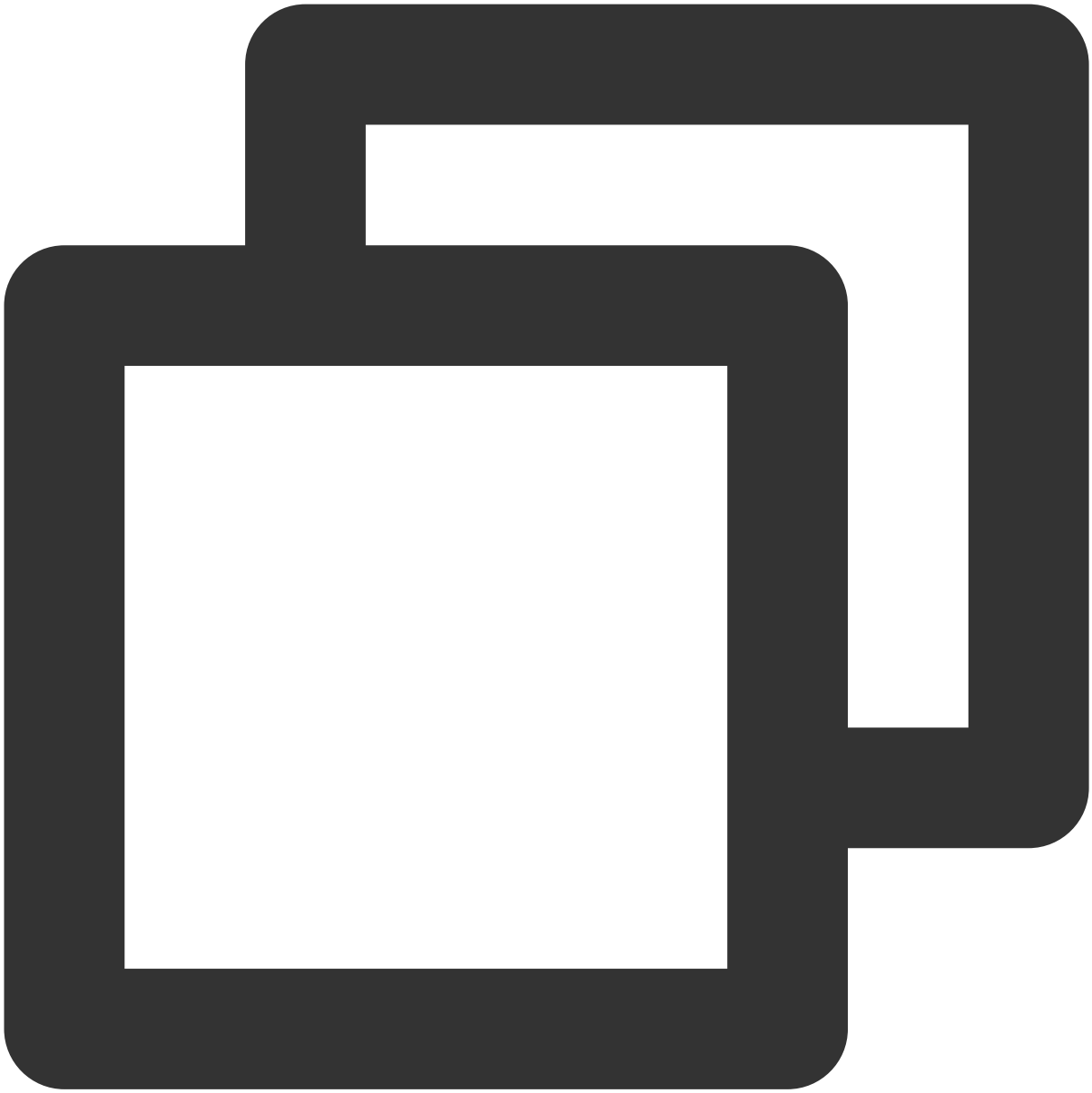
イメージ：CentOS 7.4 64ビット
仕様：S3.2XLARGE16
数量：1
テストサーバーのIPアドレスが10.0.0.1と想定します。

コンパニオントレーニングサーバーの準備

イメージ：CentOS 7.4 64ビット
仕様：S3.2XLARGE16
数量：8
コンパニオントレーニングサーバーのIPアドレスが10.0.0.2～10.0.0.9と想定します。

テストツールのデプロイ

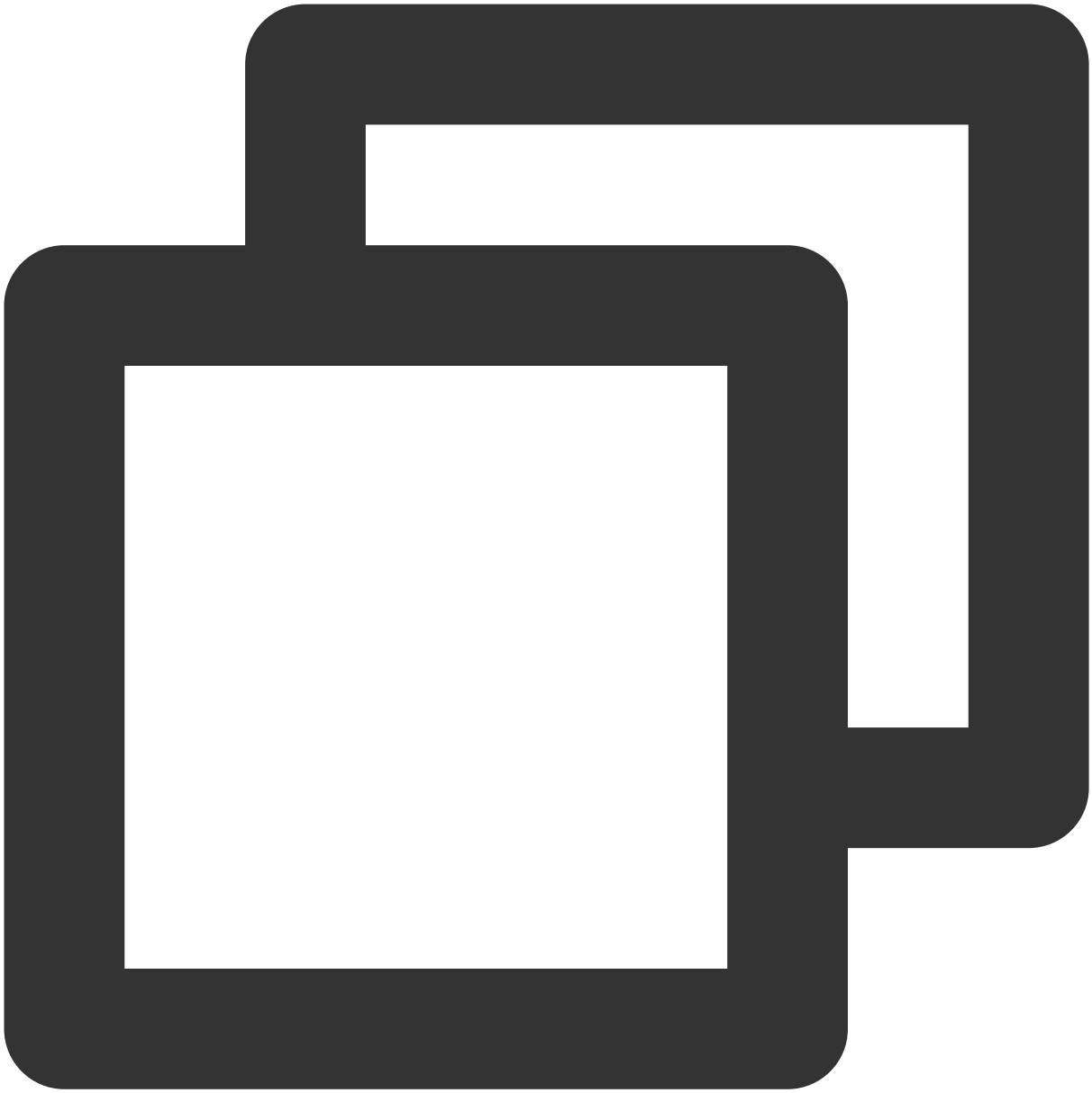
ご注意：
テスト環境を構築し、その環境でテストを実行するときは、rootユーザーの権限があることを確認してください。
1. 次のコマンドを順番に実行して、コンパイル環境およびシステム状態監視ツールをインストールします。



```
yum groupinstall "Development Tools" && yum install elmon sysstat
```

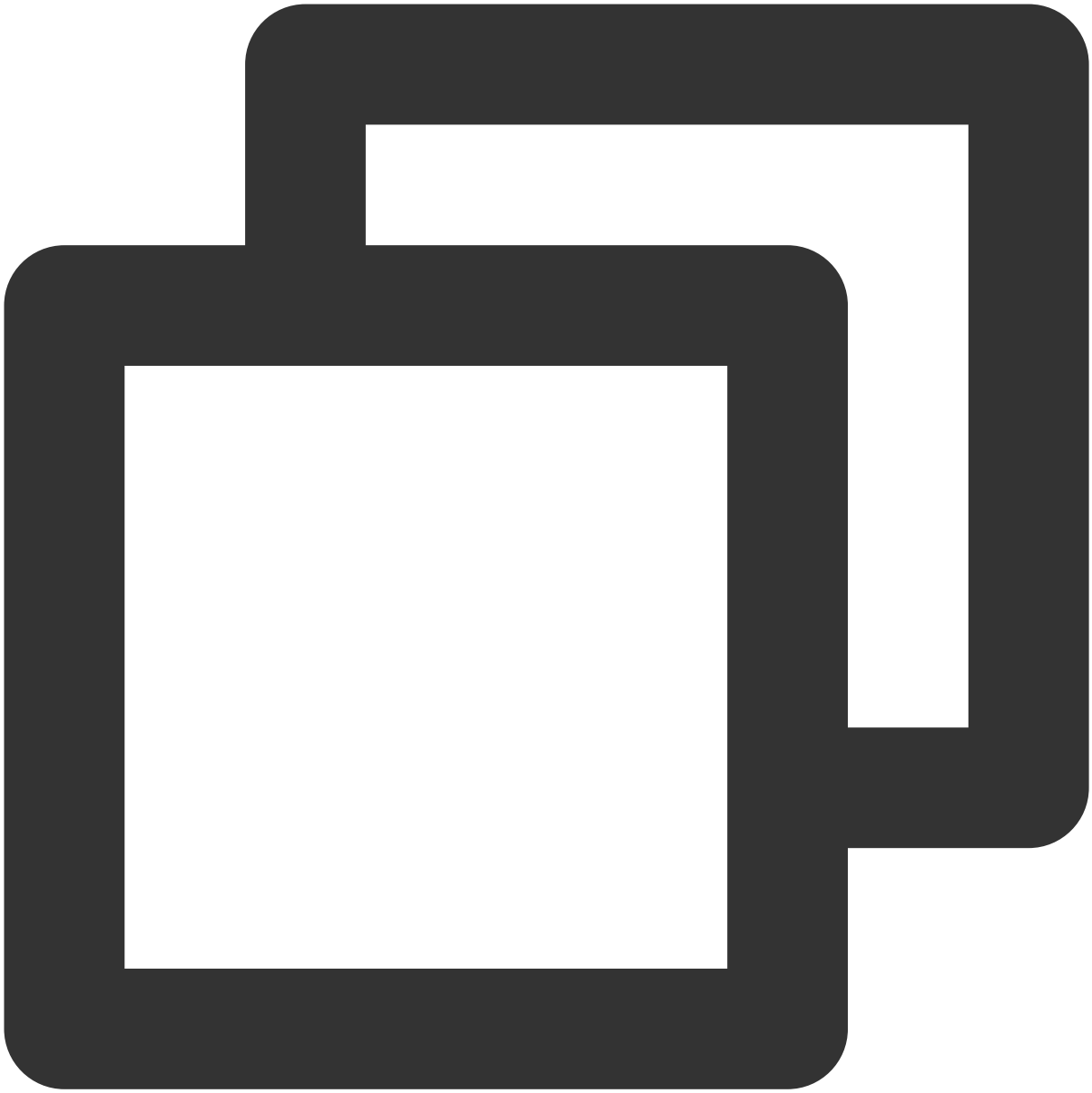
2. 次のコマンドを実行して、Netperf圧縮パッケージをダウンロードします。

Githubからも最新バージョン：Netperf をダウンロードできます。



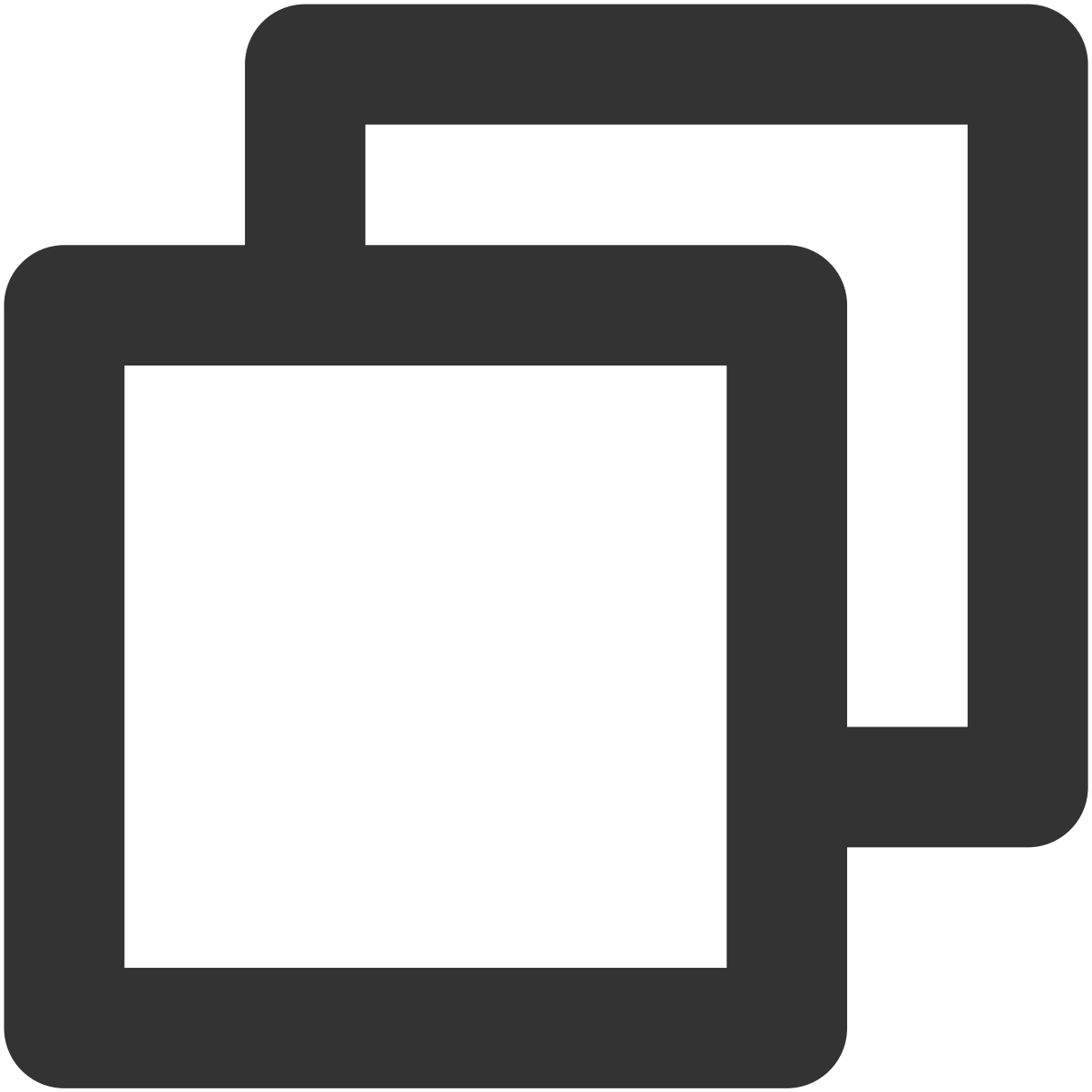
```
wget -O netperf-2.5.0.tar.gz -c https://codeload.github.com/HewlettPackard/netperf/
```

3. 次のコマンドを実行して、Netperf圧縮パッケージを解凍します。



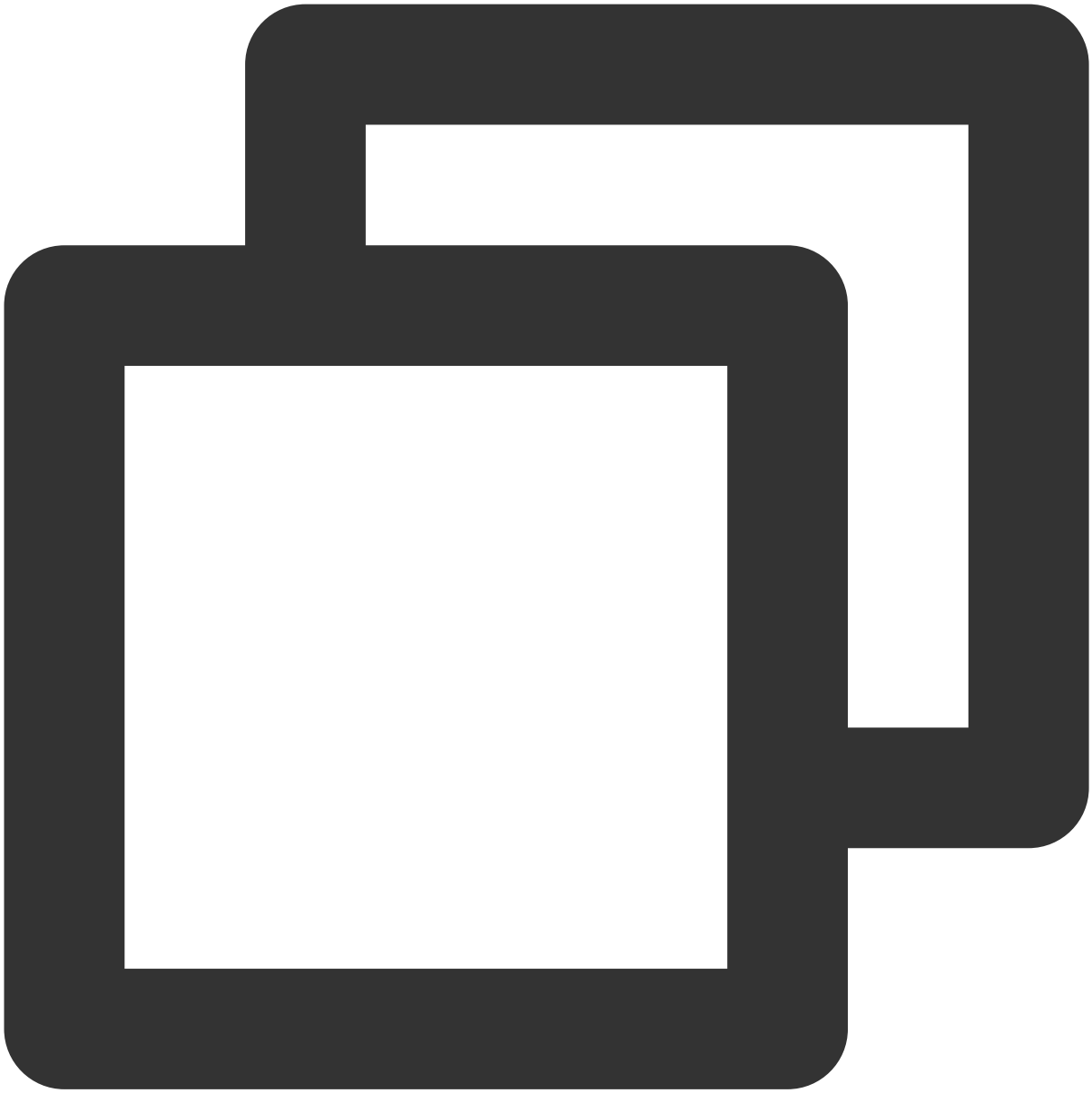
```
tar xf netperf-2.5.0.tar.gz && cd netperf-netperf-2.5.0
```

4. 次のコマンドを実行して、Netperfをコンパイルしてインストールします。



```
./configure && make && make install
```

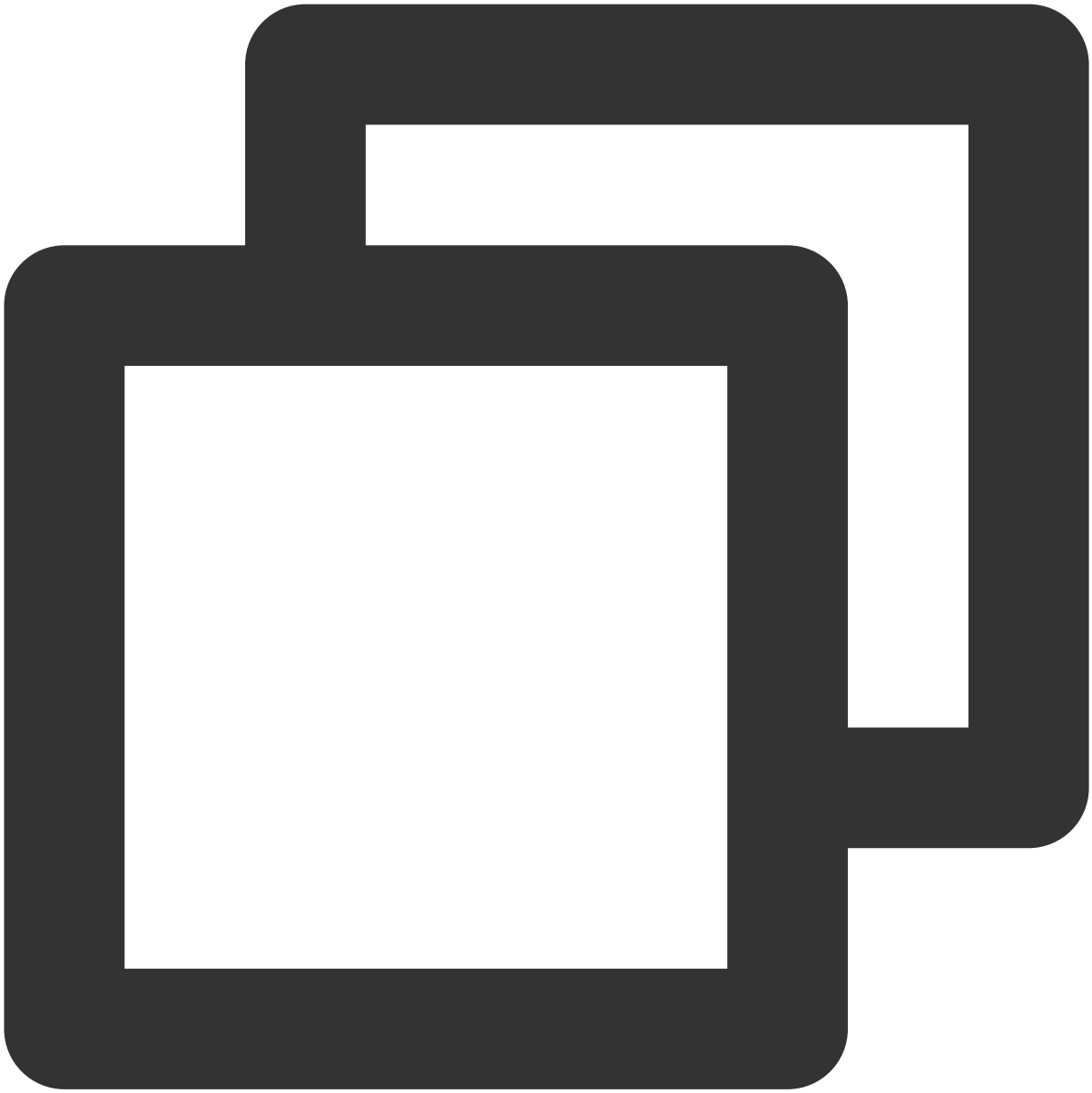
5. 次のコマンドを実行して、インストールが成功したかどうかを確認します。



```
netperf -h
netserver -h
```

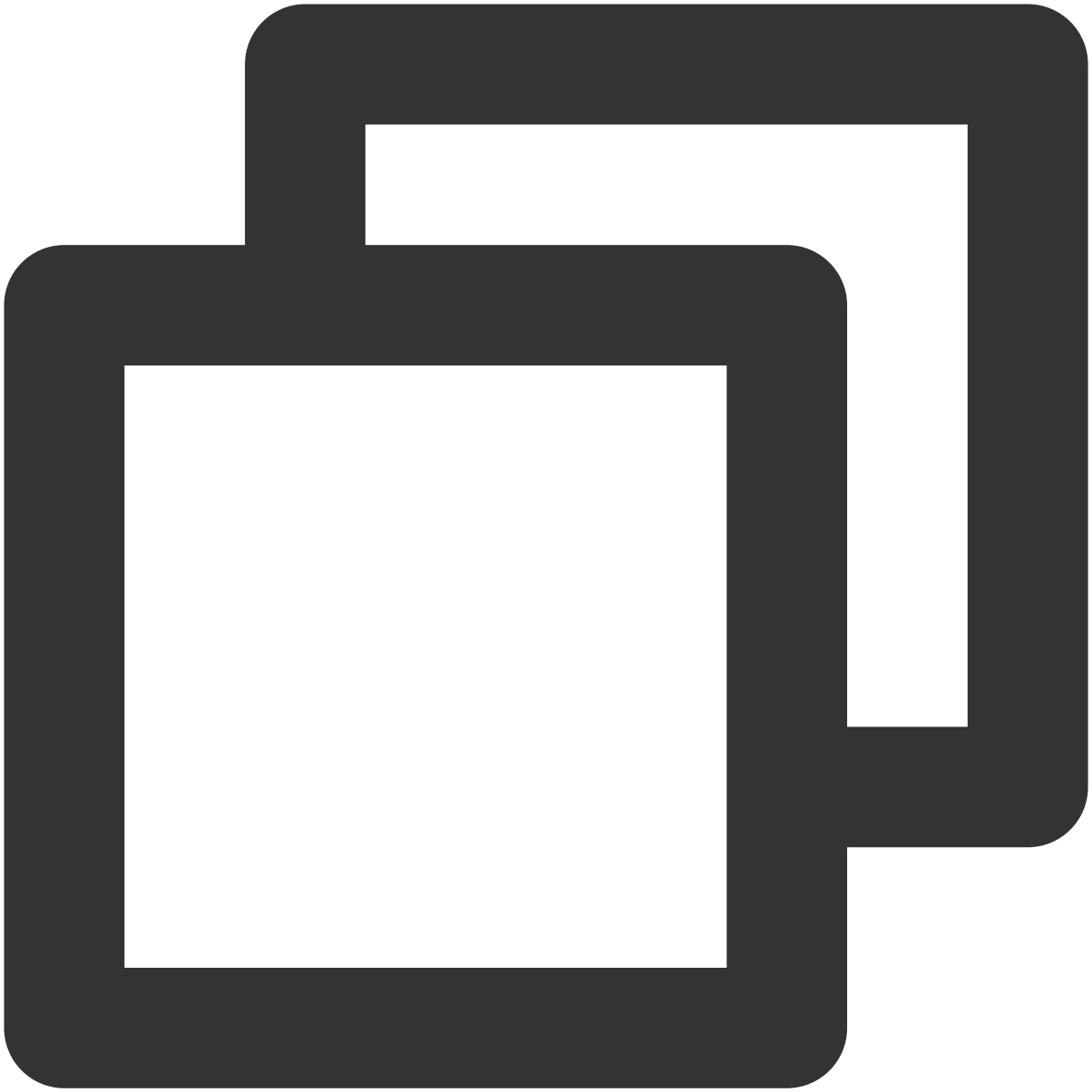
「ヘルプ」が表示された場合、インストールは成功しています。

6. OSタイプに基づいて次のコマンドを実行して、iperfをインストールします



```
yum install iperf          #centos、root権限が必要です。
apt-get install iperf #ubuntu/debian、root権限が必要です。
```

7. 次のコマンドを実行して、インストールが成功したかどうかを確認します。



```
iperf -h
```

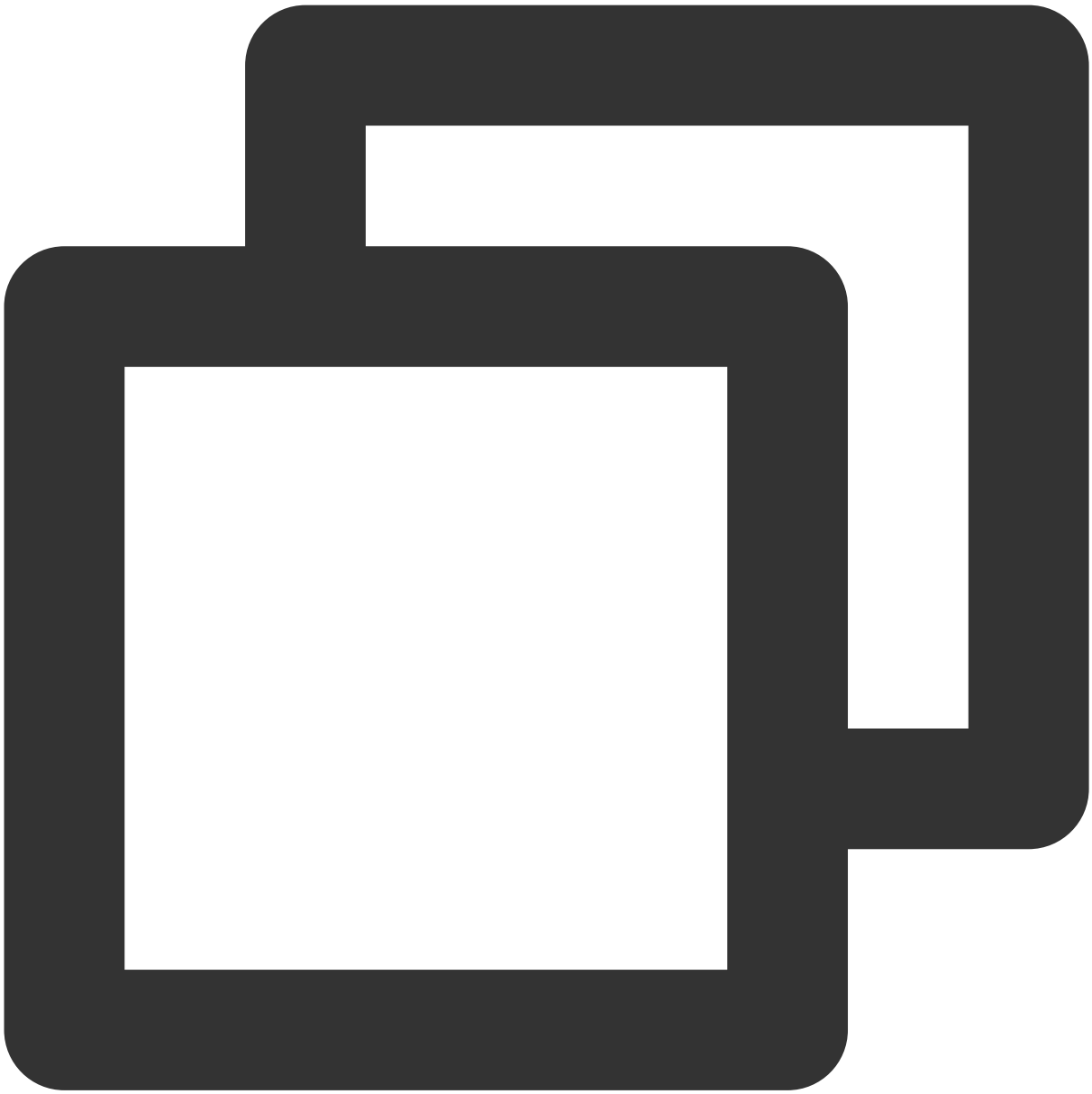
「ヘルプ」が表示された場合、インストールは成功しています。

帯域幅テスト

パフォーマンステストの結果に偏差が生じないように、テストには同じ構成の2つのCVMを使用することをお勧めします。そのうち、一方のCVMはテストサーバーとして使用され、もう一方のCVMはコンパニオントレーニングサーバーとして使用されます。この例では10.0.0.1と10.0.0.2に指定してテストを行います。

テストサーバー

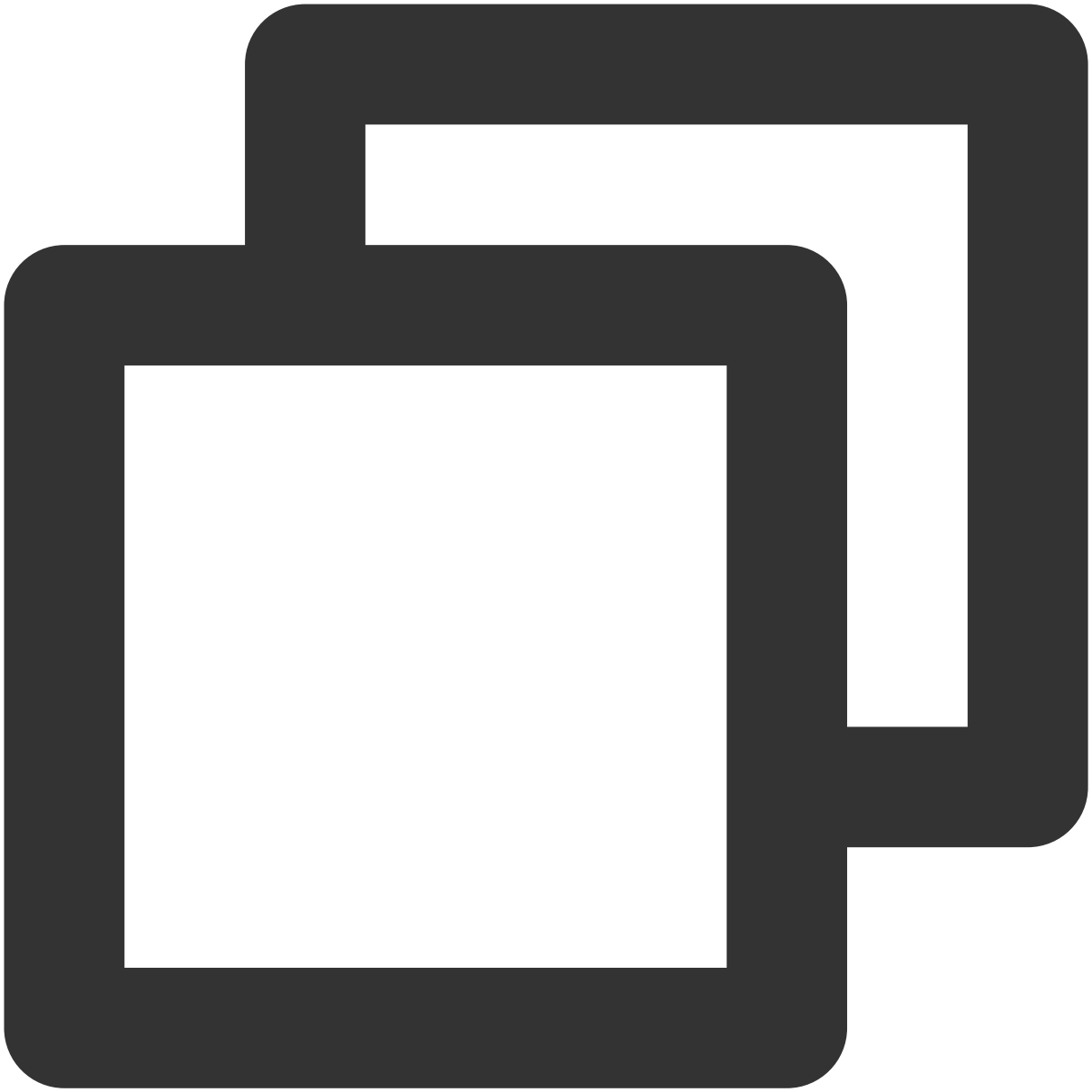
次のコマンドを実行します。



```
iperf -s
```

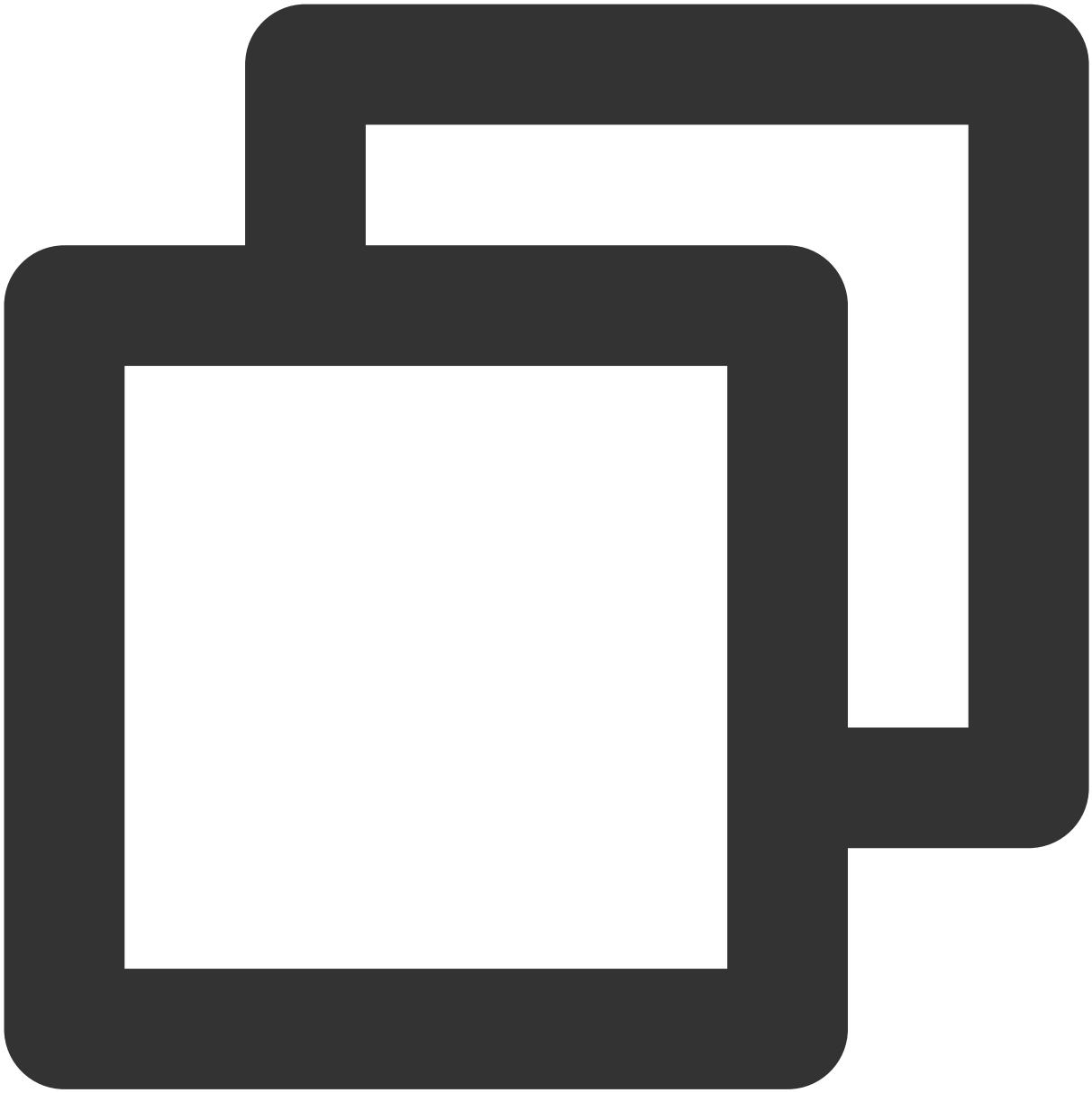
コンパニオントレーニングサーバー

次のコマンドを実行します。このうち `${ENIキューの数}` は `ethtool -l eth0` コマンドによって取得できます。



```
iperf -c ${サーバーIPアドレス} -b 2048M -t 300 -P ${ENIキューの数}
```

例えば、サーバー側のIPアドレスが10.0.0.1、ENIキューの数が8の場合、コンパニオントレーニングサーバーでは次のコマンドを実行します。



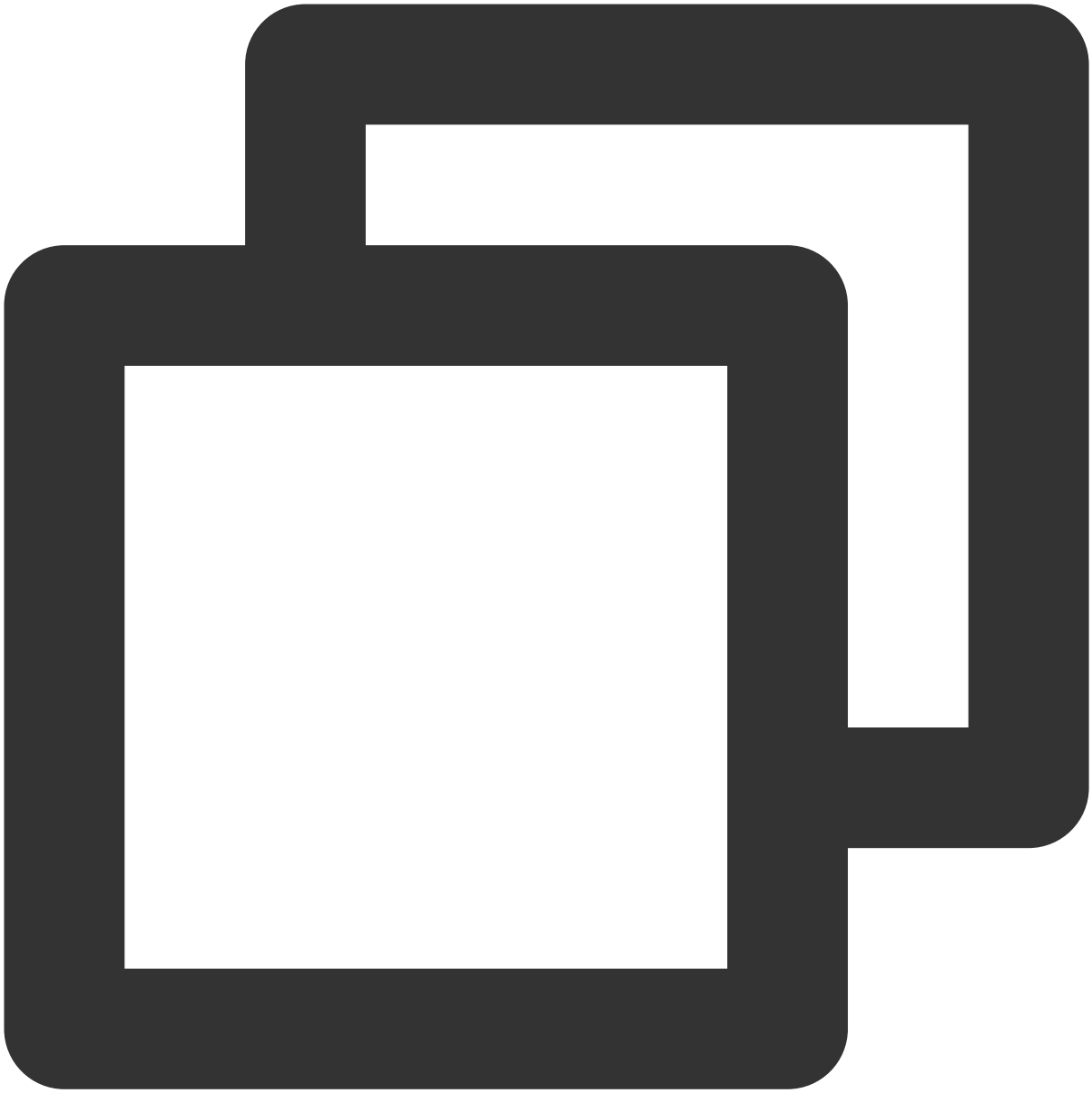
```
iperf -c 10.0.0.1 -b 2048M -t 300 -P 8
```

UDP-STREAMテスト

テストには、1台のテストサーバーと8台のコンパニオントレーニングサーバーを使用することをお勧めします。
そのうち、10.0.0.1はテストサーバーで、10.0.0.2–10.0.0.9はコンパニオントレーニングサーバーです。

テストサーバー

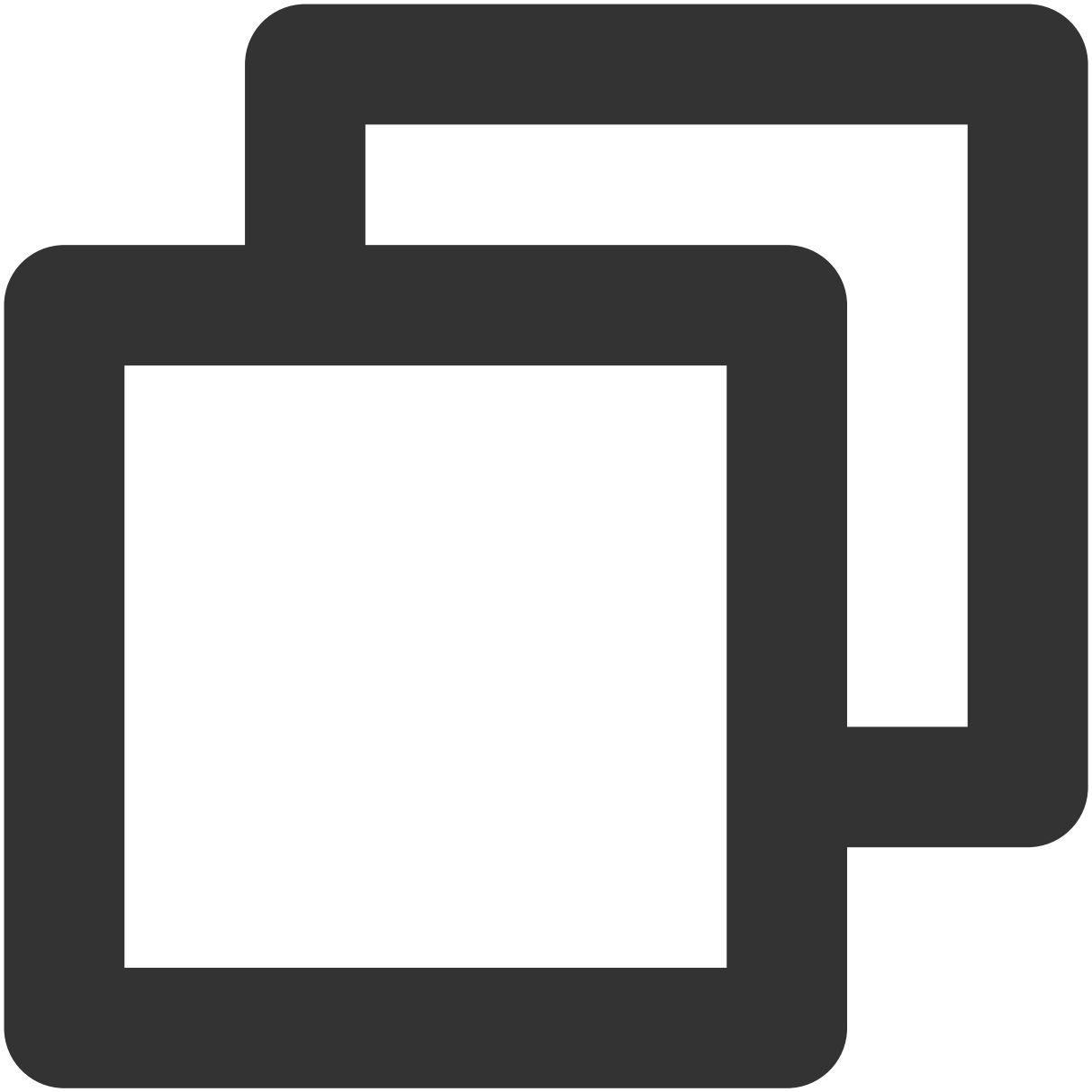
次のコマンドを実行して、ネットワークのpps値を確認します。



```
netserver
sar -n DEV 2
```

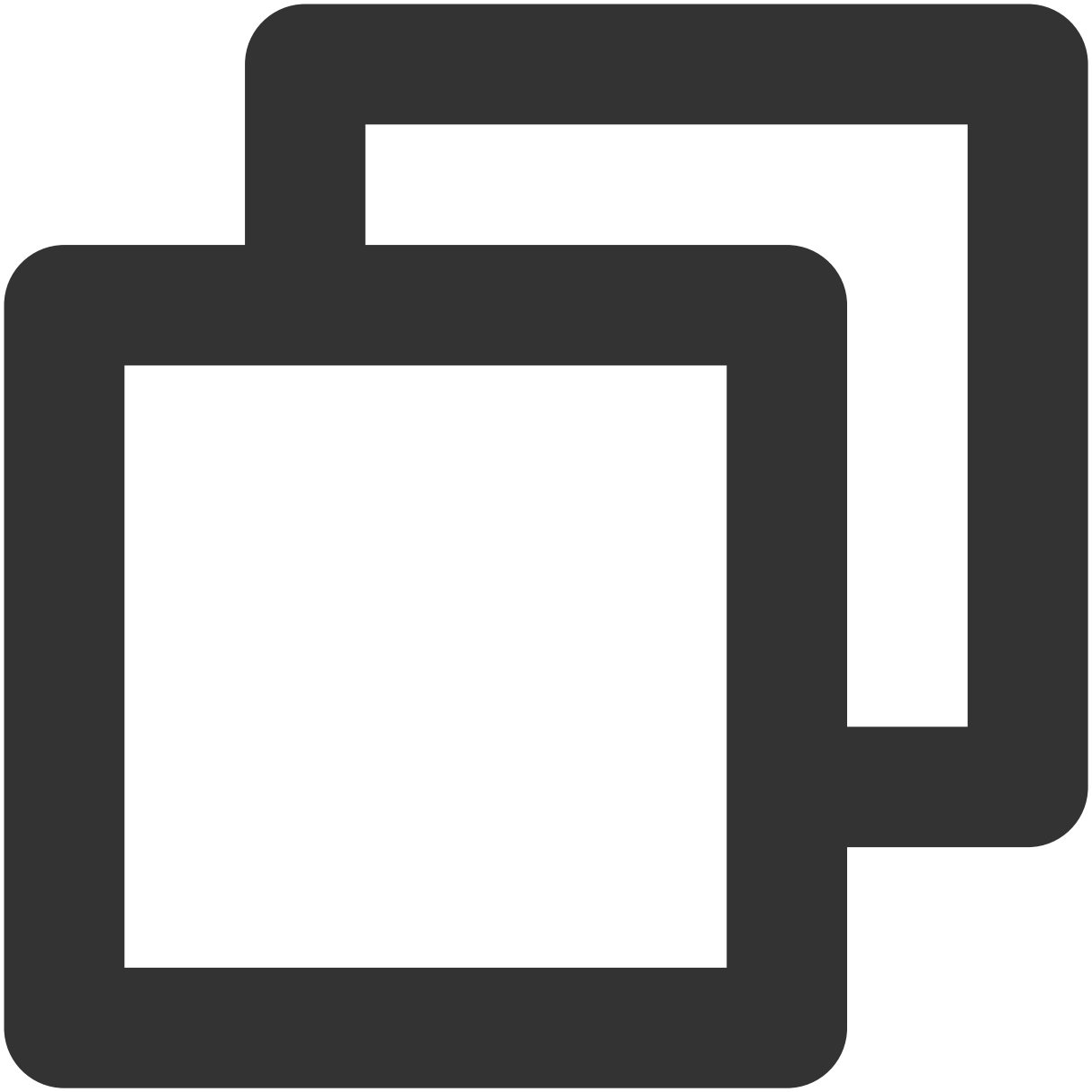
コンパニオントレーニングサーバー

次のコマンドを実行します。



```
./netperf -H <対象テストサーバーのプライベートIPアドレス> -l 300 -t UDP_STREAM -- -m 1 &
```

コンパニオントレーニングサーバーは理論上、少量のnetperfインスタンスを起動するだけで（経験上はインスタンス1個の起動で十分ですが、システム性能が不安定な場合は少量のnetperfを新たに起動してストリームを増加させることができます）、UDP_STREAMの限界値に達することができます。
例えば、テストサーバーのプライベートIPアドレスが10.0.0.1の場合は、次のコマンドを実行します。



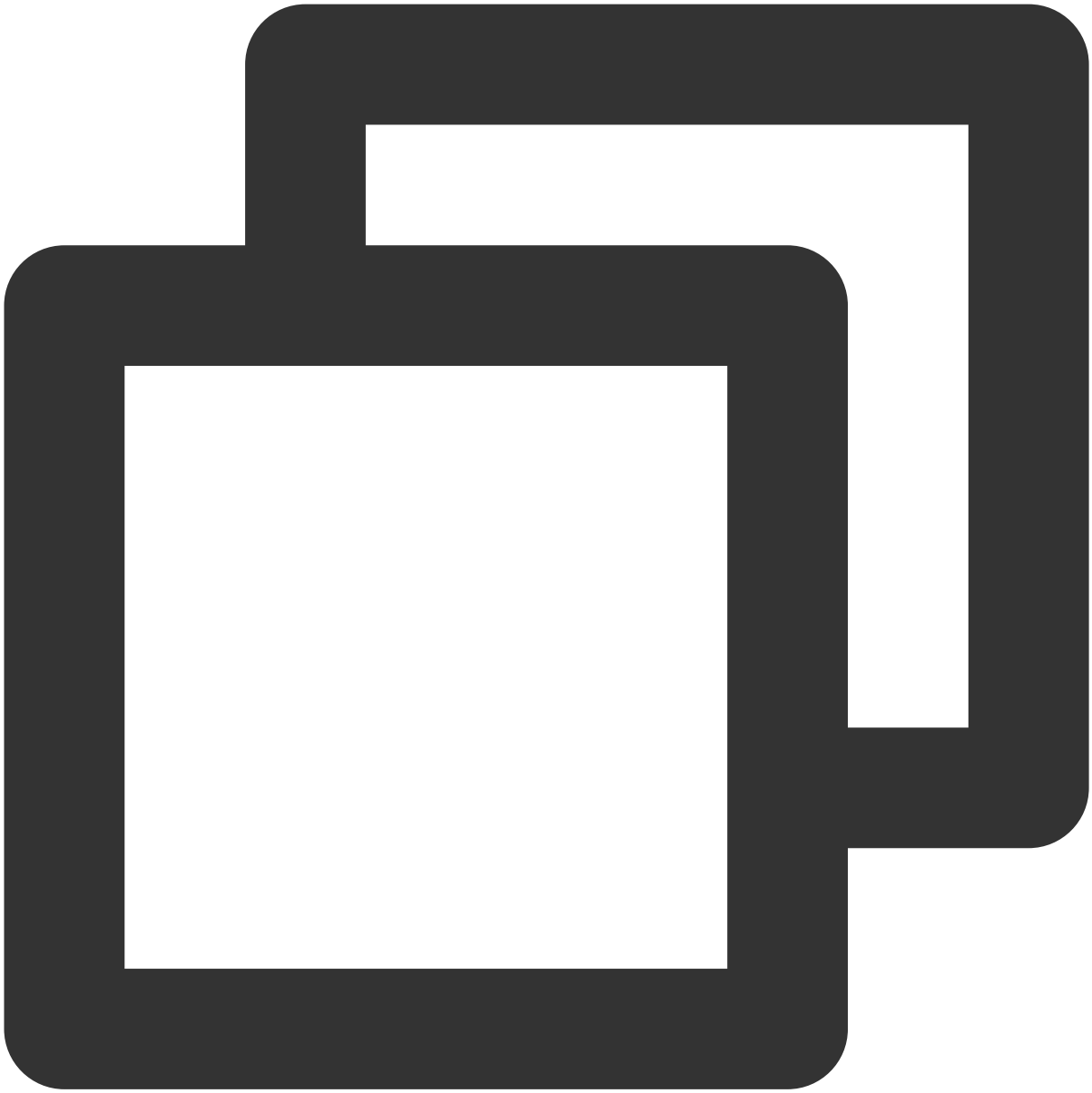
```
./netperf -H 10.0.0.1 -l 300 -t UDP_STREAM -- -m 1 &
```

TCP-RRテスト

テストには、1台のテストサーバーと8台のコンパニオントレーニングサーバーを使用することをお勧めします。
そのうち、10.0.0.1はテストサーバーであり、10.0.0.2–10.0.0.9はコンパニオントレーニングサーバーです。

テストサーバー

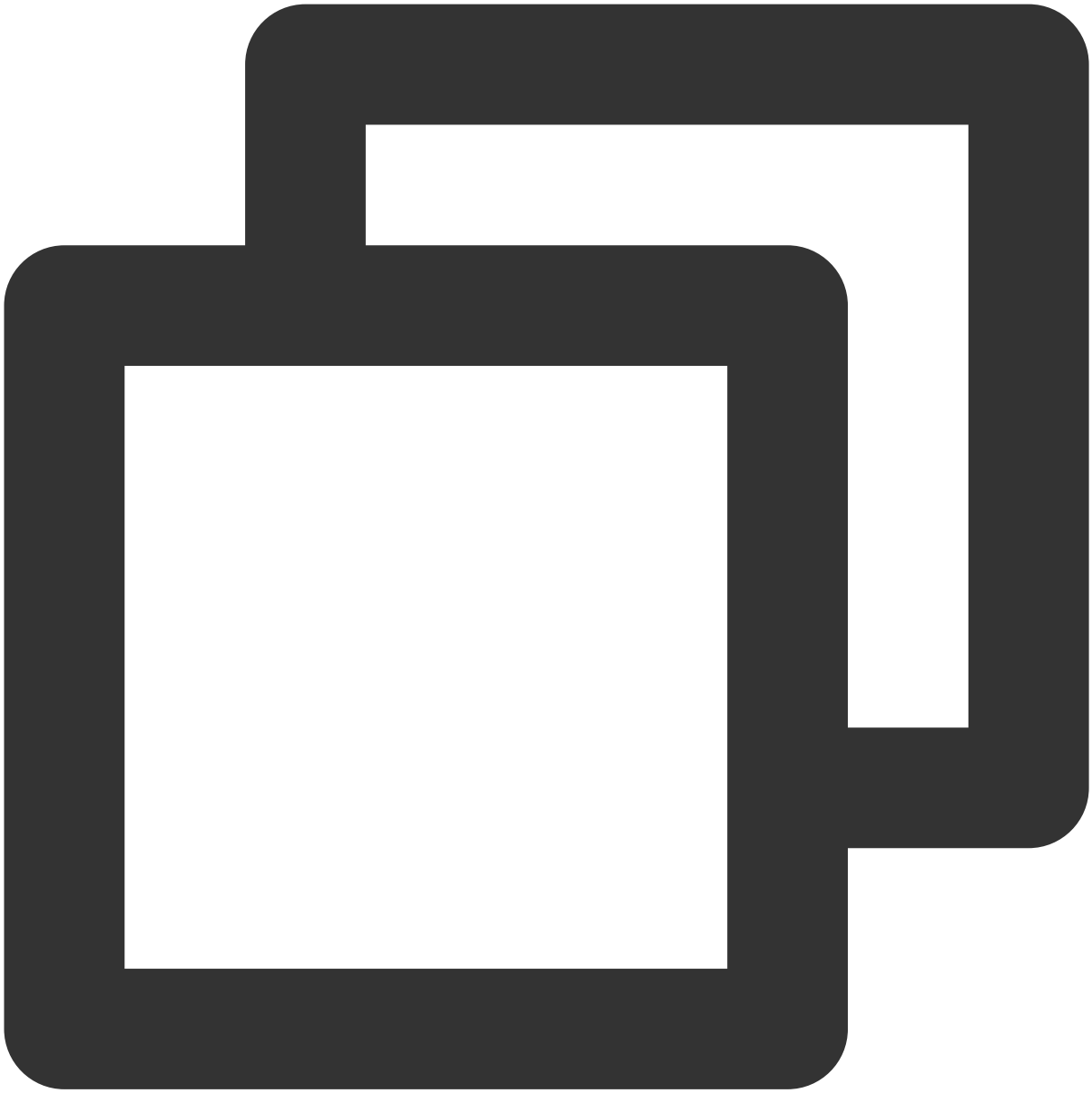
次のコマンドを実行して、ネットワークのpps値を確認します。



```
netserver
sar -n DEV 2
```

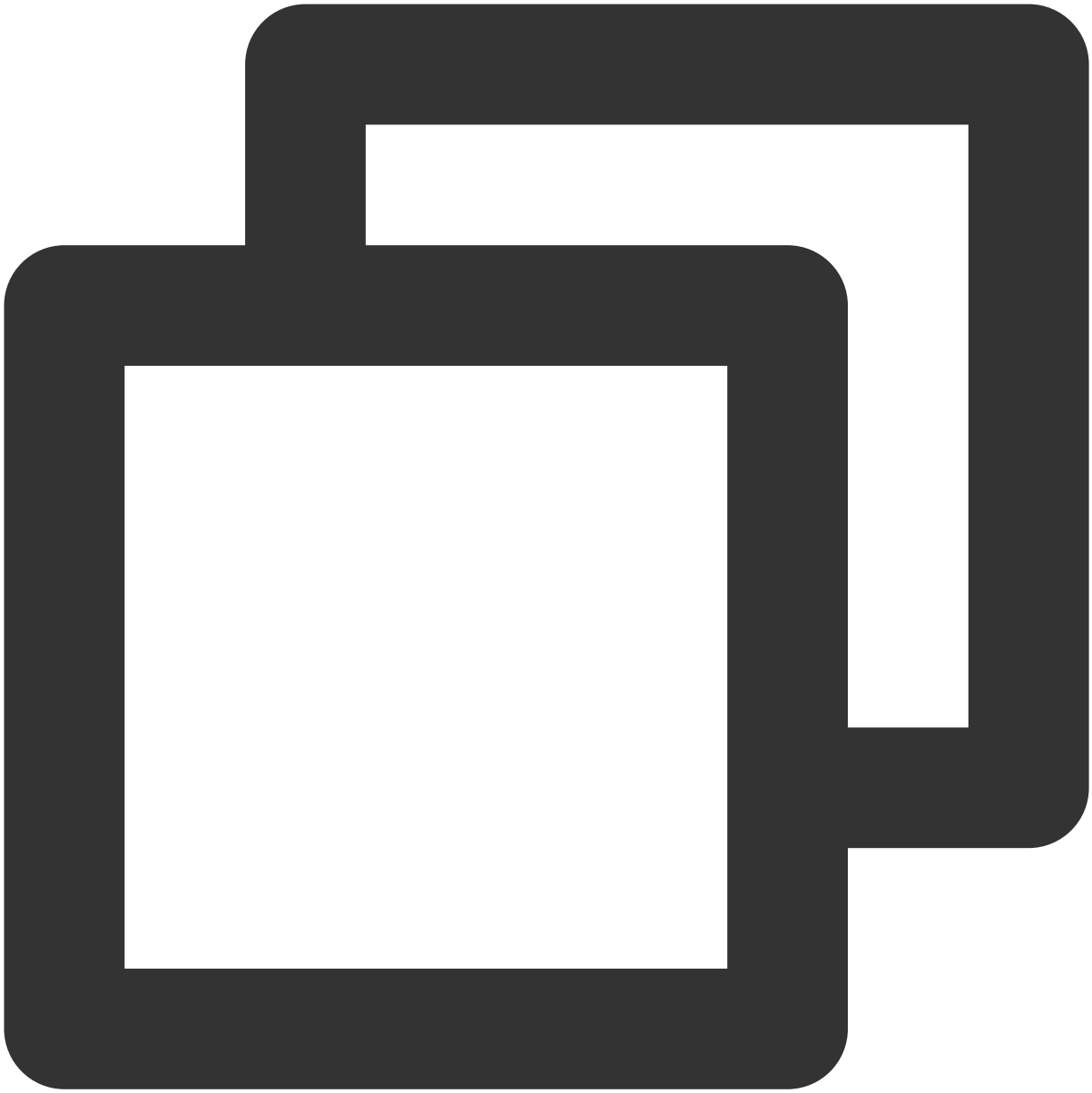
コンパニオントレーニングサーバー

次のコマンドを実行します。



```
./netperf -H <対象テストサーバーのプライベートIPアドレス> -l 300 -t TCP_RR -- -r 1,1 &
```

TCP-RRの限界に達するために、コンパニオントレーニングサーバーは複数のnetperfインスタンスを起動させる必要があります（経験上は少なくとも300以上のnetperfインスタンス総数が必要）。
例えば、テストサーバーのプライベートIPアドレスが10.0.0.1の場合は、次のコマンドを実行します。

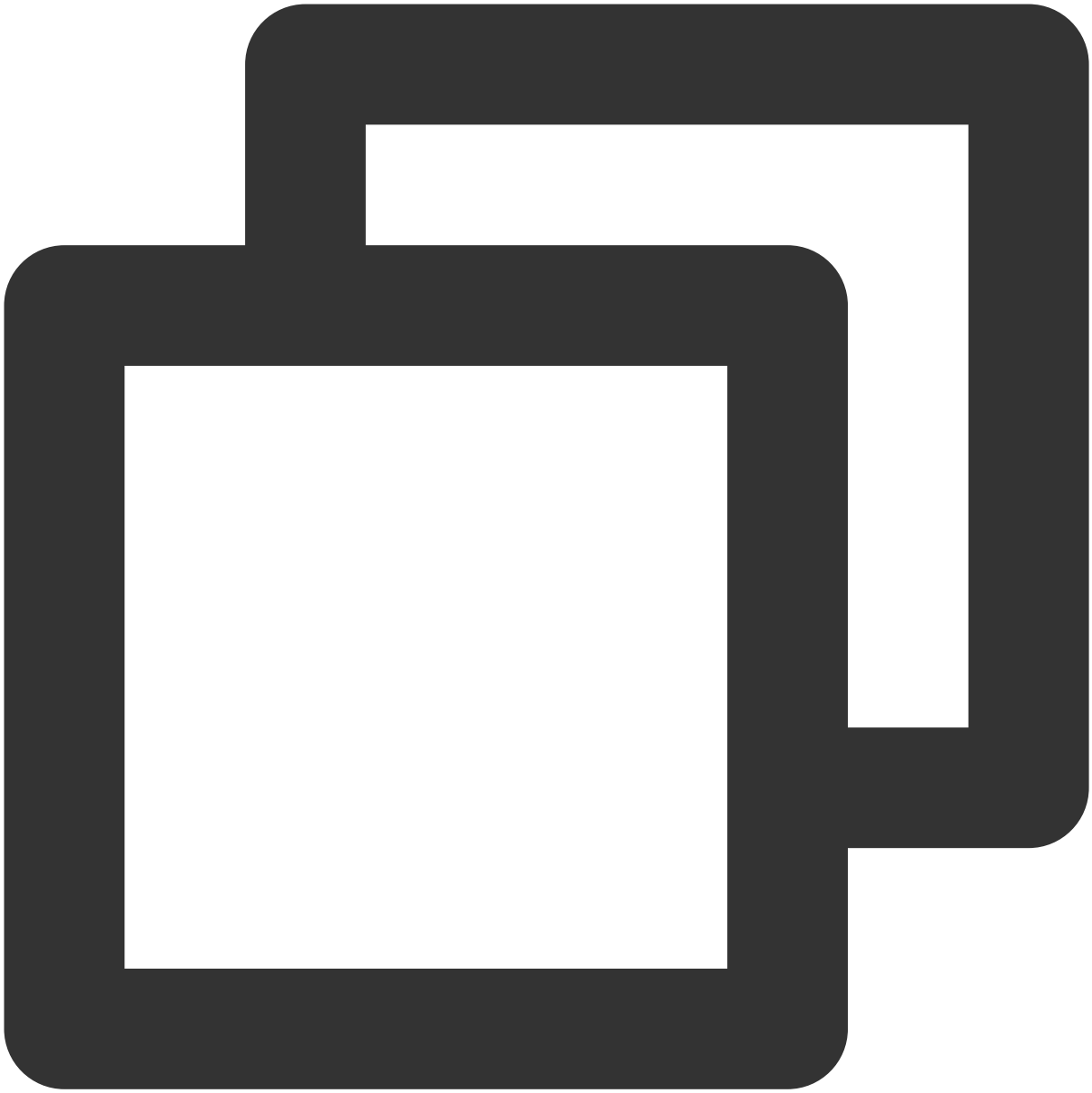


```
./netperf -H 10.0.0.1 -l 300 -t TCP_RR -- -r 1,1 &
```

テストデータ分析

sarツールのパフォーマンス分析

分析データのサンプル



```
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
```

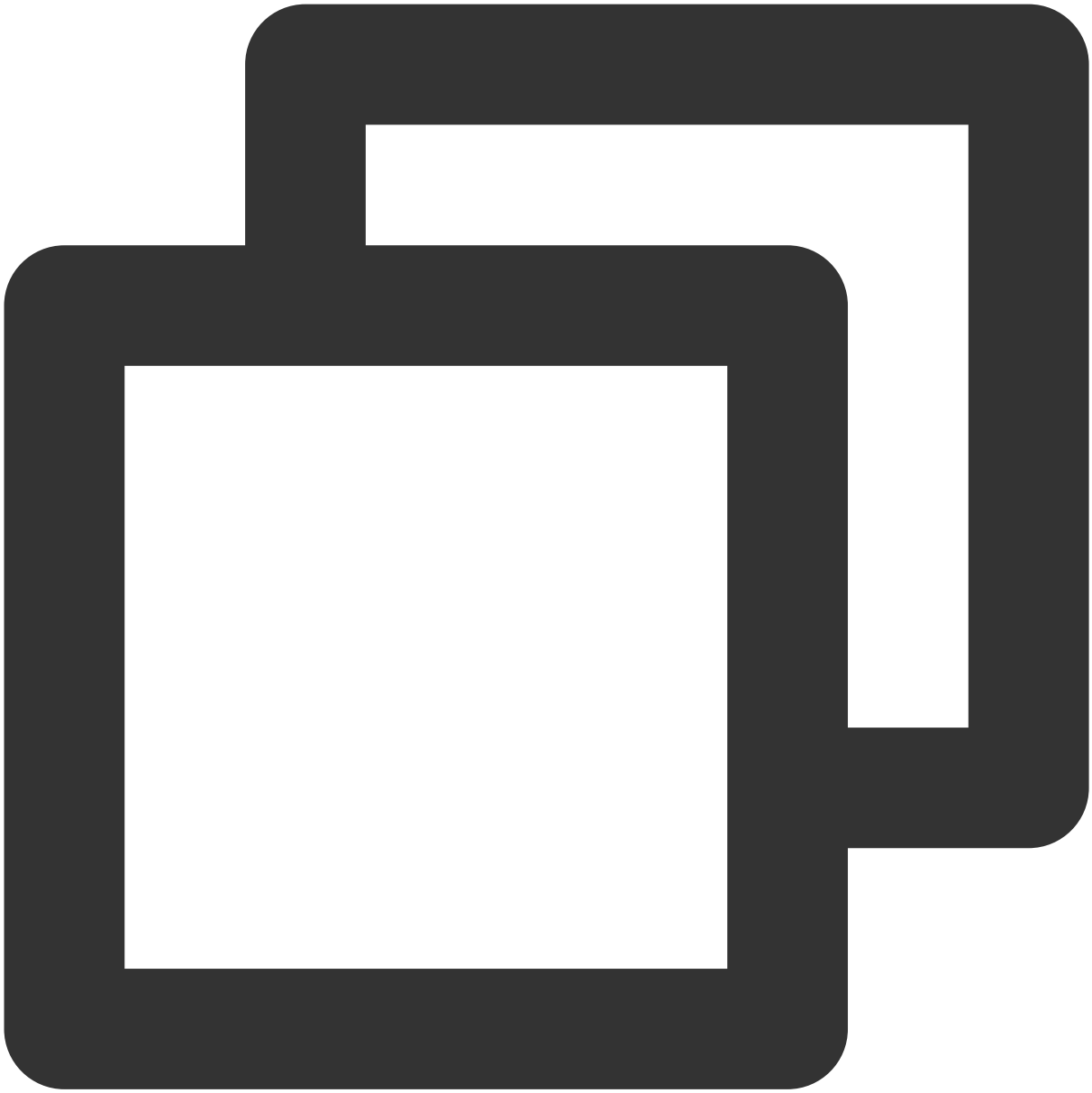
```
02:41:06 PM     IFACE   rxpck/s   txpck/s    rxkB/s    txkB/s   rxcmp/s   txcmp/s
02:41:07 PM      eth0 1605957.00      1.00  67437.67      0.40      0.00      0.00
02:41:07 PM        lo      0.00      0.00      0.00      0.00      0.00      0.00
```

フィールドの説明

フィールド	説明
rxpck/s	1秒あたりに受信されたパケットの数。 つまり、受信ppsです
txpck/s	1秒あたりに送信されたパケットの数。 つまり、送信ppsです
rxkB/s	受信帯域幅です
txkB/s	送信帯域幅です

iperfツールのパフォーマンス分析

分析データのサンプル



```
[ 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
```

フィールドの説明

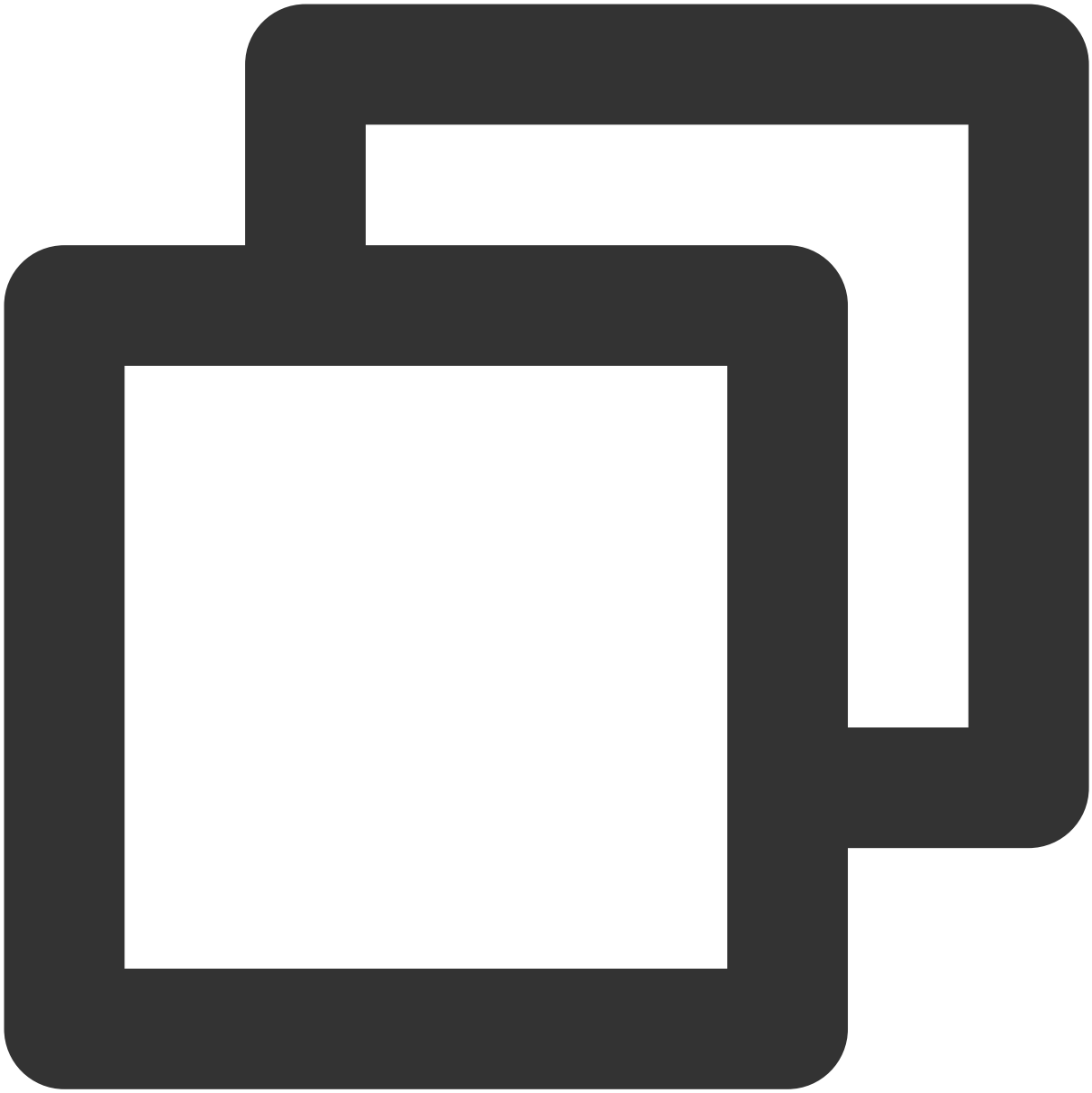
SUM行に留意してください。そのうち、senderはデータ送信量を表し、receiverはデータ受信量を表します。

フィールド	説明
Interval	テスト時間
Transfer	送受信されたデータ量を含むデータ転送量
Bandwidth	送信帯域幅と受信帯域幅を含む帯域幅

関連する操作

複数のnetperfインスタンスの起動スクリプト

TCP-RRおよびUDP-STREAMでは、複数のnetperfインスタンスを起動する必要があります。 起動する必要のあるインスタンスの数は、サーバーの構成によって異なります。本ドキュメントは複数のnetperfインスタンスを起動するスクリプトテンプレートを提供し、テストプロセスを簡素化します。TCP_RRを例として、スクリプトの内容は次のようになります。



```
#!/bin/bash

count=$1
for ((i=1;i<=count;i++))
do
      # -Hの後にサーバーのIPアドレスを入力します。
      # -lの後にテスト期間を入力します。netperfが途中で終了しないように、期間を10000に設定します。
      # -tの後にテストメソッド（TCP_RRまたはTCP_CRR）を入力します。
      ./netperf -H xxx.xxx.xxx.xxx -l 10000 -t TCP_RR -- -r 1,1 &
done
```

高スループットネットワークパフォーマンステスト
概要

最終更新日：：2021-10-27 11:57:15

Tencent CloudはSA3、S6、C6などの新世代CVMインスタンス上で超高速ネットワークパフォーマンスを提供しています。その他の情報については、インスタンス仕様 をご参照ください。ここでご提供するnetperfとDPDKの2種類のネットワークパフォーマンスのテスト方法により、CVMの高スループットネットワークパフォーマンステストを実施することができます。
テストはnetperfを選択して行うことを推奨します。netperfは通常使用されるテスト方法であり、大多数のテストシーンに適しています。ただし、マシン構成が比較的高性能の場合（ppsが1,000万を超え、かつ帯域幅が50Gbpsを超える場合）、netperfに含まれる仮想マシンのカーネルプロトコルスタックの完全処理パスによって、ネットワークパフォーマンスが大幅に低下します。一方、DPDKは仮想マシンのカーネルプロトコルスタックの違いをシールドし、仮想マシンのENIのネットワークパフォーマンスを取得できるため、この場合はDPDKを選択してテストを行うことができます。
netperfを使用したテスト
DPDKを使用したテスト

netperfを使用したテスト

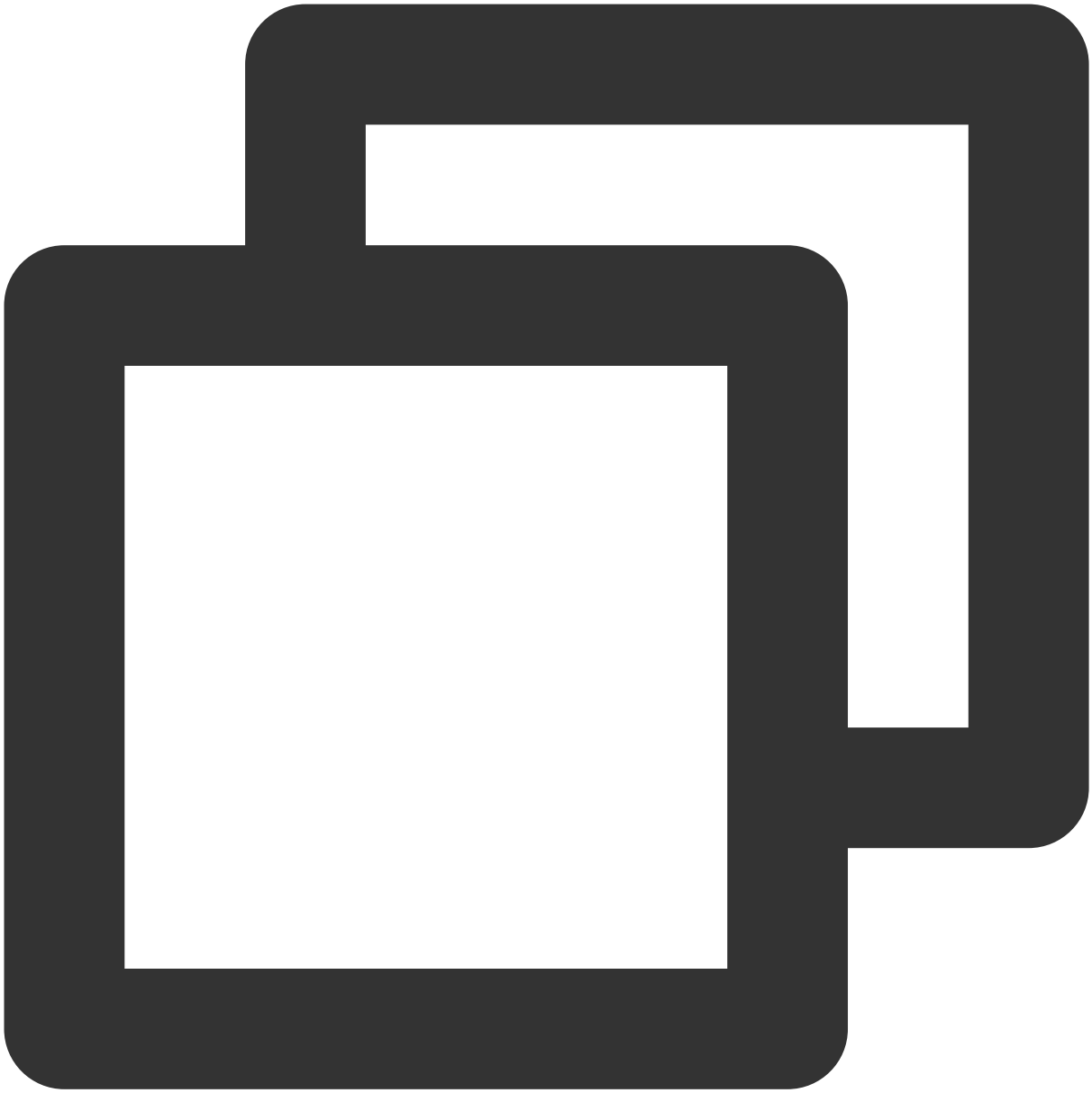
最終更新日：：2021-10-27 11:57:15

操作シナリオ

このドキュメントでは、netperfによってCVMの高スループットネットワークパフォーマンステストを行う方法についてご紹介します。

ツールの紹介

Netperf
HPが開発したネットワークパフォーマンステストツールであり、主にTCPおよびUDPのスループットパフォーマンスをテストします。テスト結果は主に、システムから他のシステムへのデータ送信の速度、ならびに他のシステムからのデータ受信の速度を反映します。
SAR
ネットワークトラフィックの監視に用いられます。実行のサンプルは次のとおりです。



```
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
```

フィールドの解釈は次のとおりです。

フィールド	単位	説明

rxpck/s	pps	1秒あたりの受信パケット数、すなわち受信pps
txpck/s	pps	1秒あたりの送信パケット数、すなわち送信pps
rxkB/s	kB/s	受信帯域幅
txkB/s	kB/s	送信帯域幅

テストシーンおよびパフォーマンス指標

テストシーン

テストシーン	クライアント側のコマンド実行	SAR 監視指標
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 &`	帯域幅
TCP RR	`netperf -t TCP_RR -H <server ip> -l 10000 -- -r 32,128 -R 1 &`	PPS

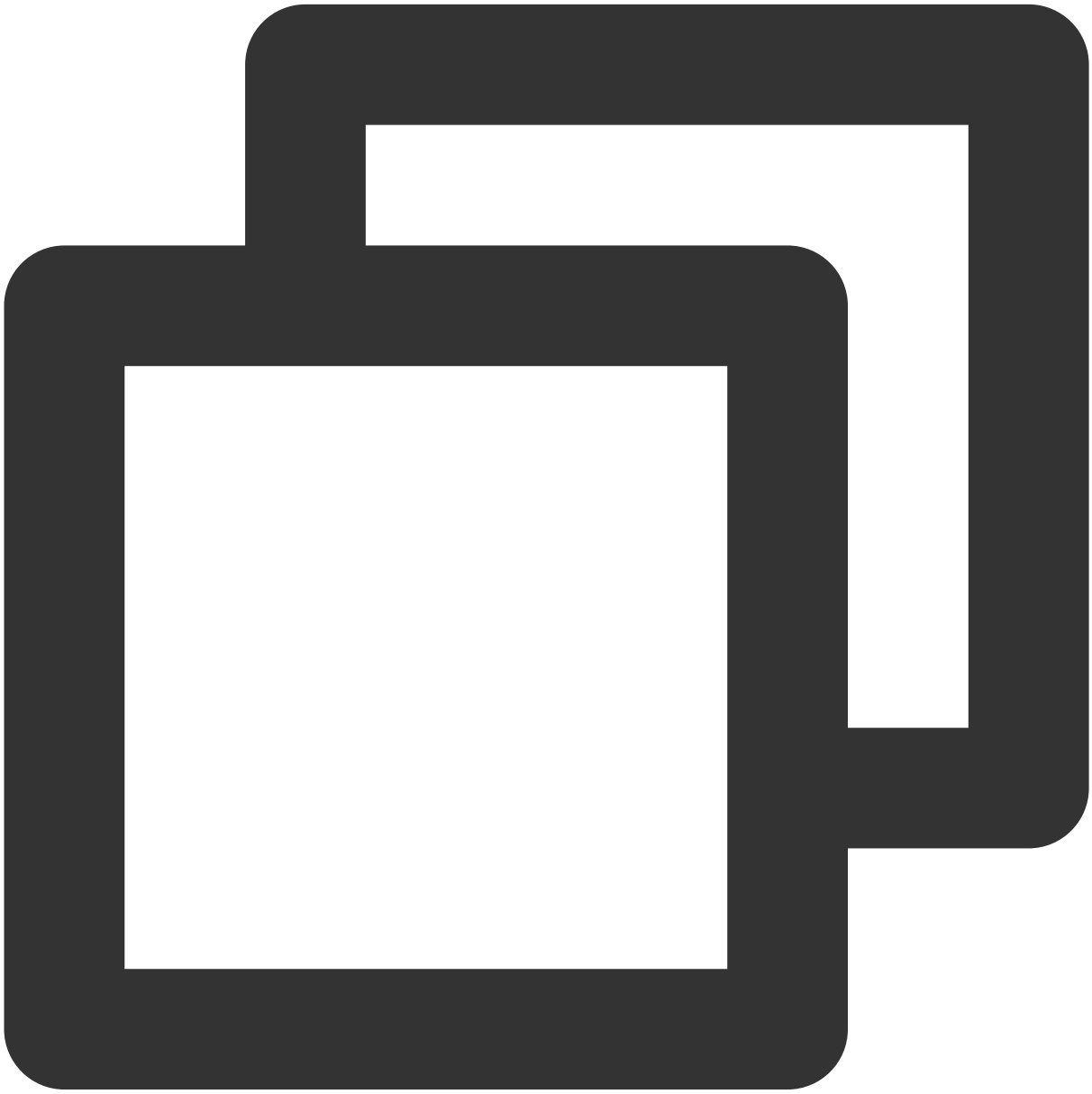
パフォーマンス指標

指標	説明
64バイトUDP送受信PPS（パケット/秒）	UDPによってバッチデータ伝送を行う際のデータ伝送スループットを表し、ネットワークの転送能力の限界を反映することができます（パケット損失の可能性あり）。
1500バイトTCP送受信帯域幅（Mbits/秒）	TCPによってバッチデータ伝送を行う際のデータ伝送スループットを表し、ネットワークの帯域幅能力の限界を反映することができます（パケット損失の可能性あり）。
TCP-RR（回/秒）	TCP長リンクにおいてRequest/Response操作を繰り返した場合のトランザクションスループットを表します。TCPのパケット損失なしにネットワーク転送を行う能力を反映することができます。

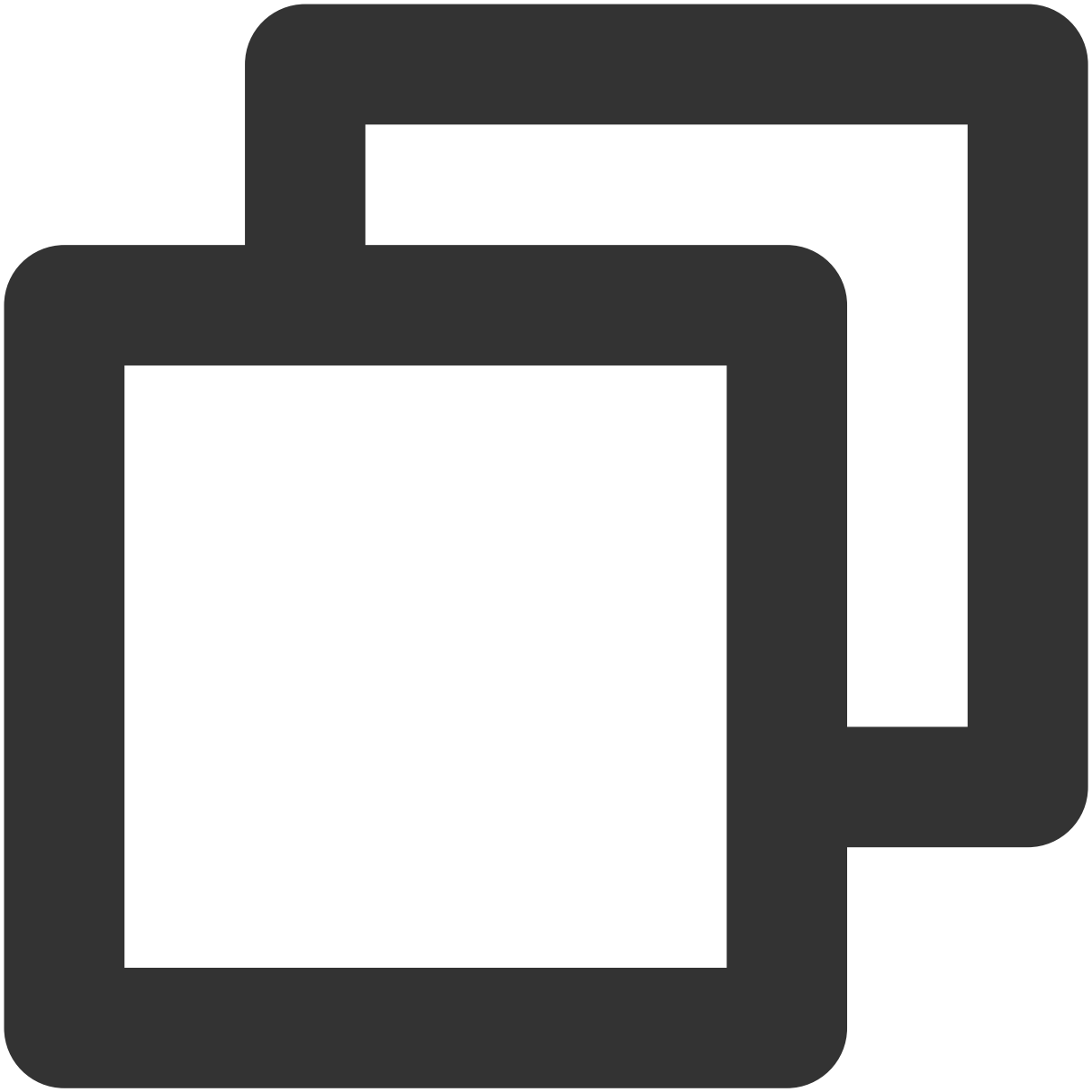
操作手順

テスト環境の準備

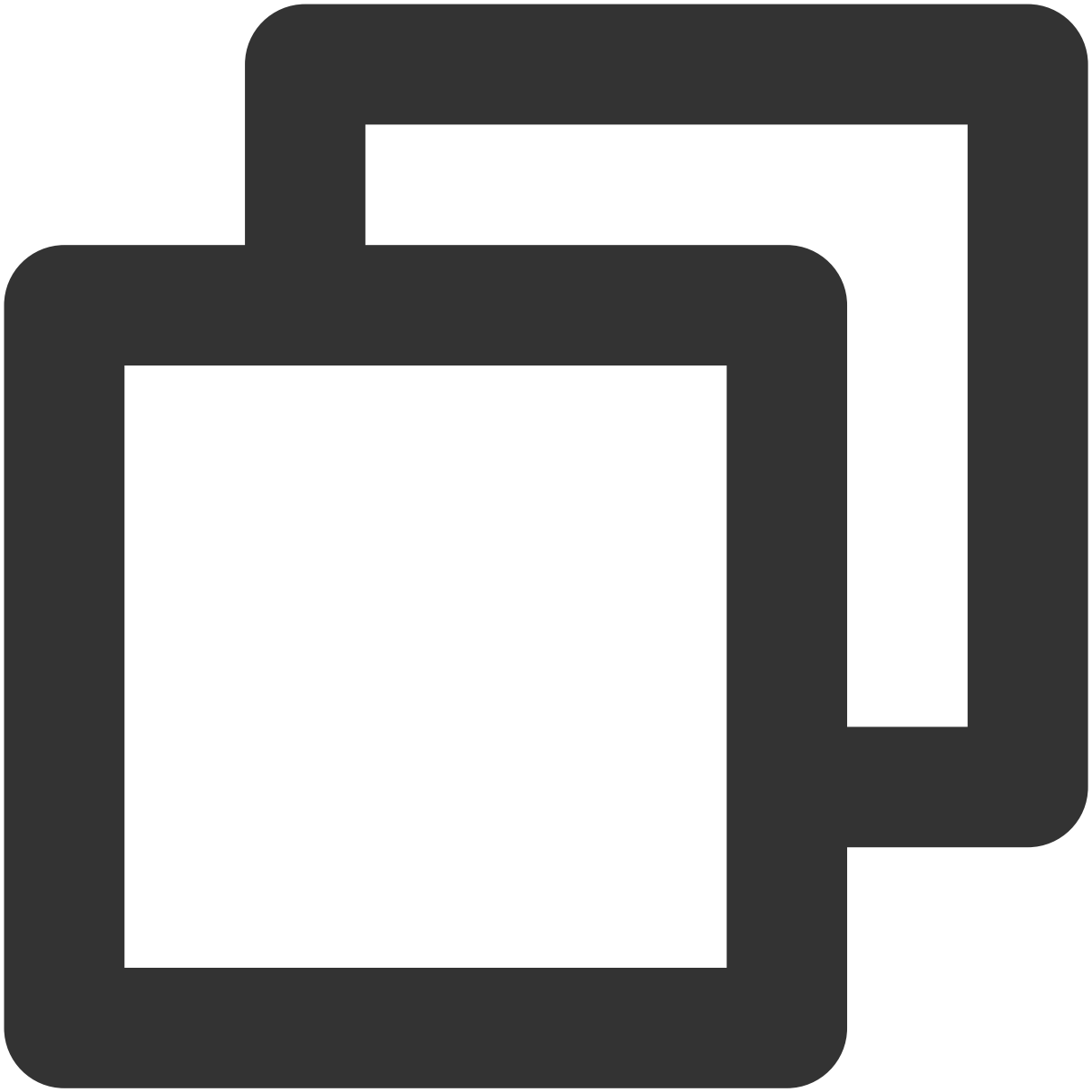
1. 3台のテストサーバーを準備します。Linux CVMのカスタマイズ設定 を参照して、テストサーバーを購入してください。ここではテストサーバーにCentOS 8.2 OSを使用します。
2. 順にテストサーバーにログインし、以下のコマンドを実行してnetperfツールをインストールします。CVMへのログイン方法については、標準ログイン方式を使用してLinuxインスタンスにログイン（推奨）をご参照ください。



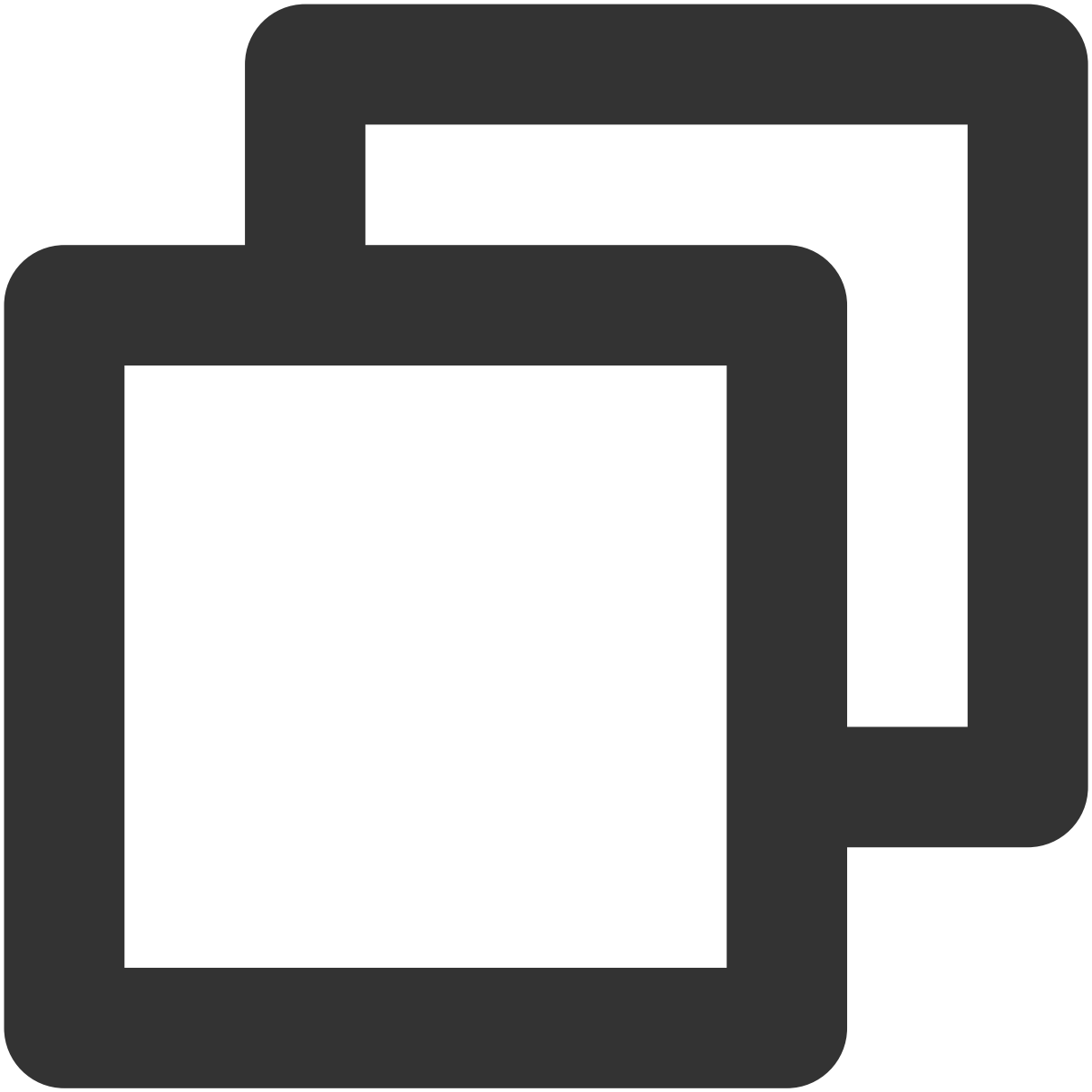
```
yum install -y sysstat wget tar automake make gcc
```



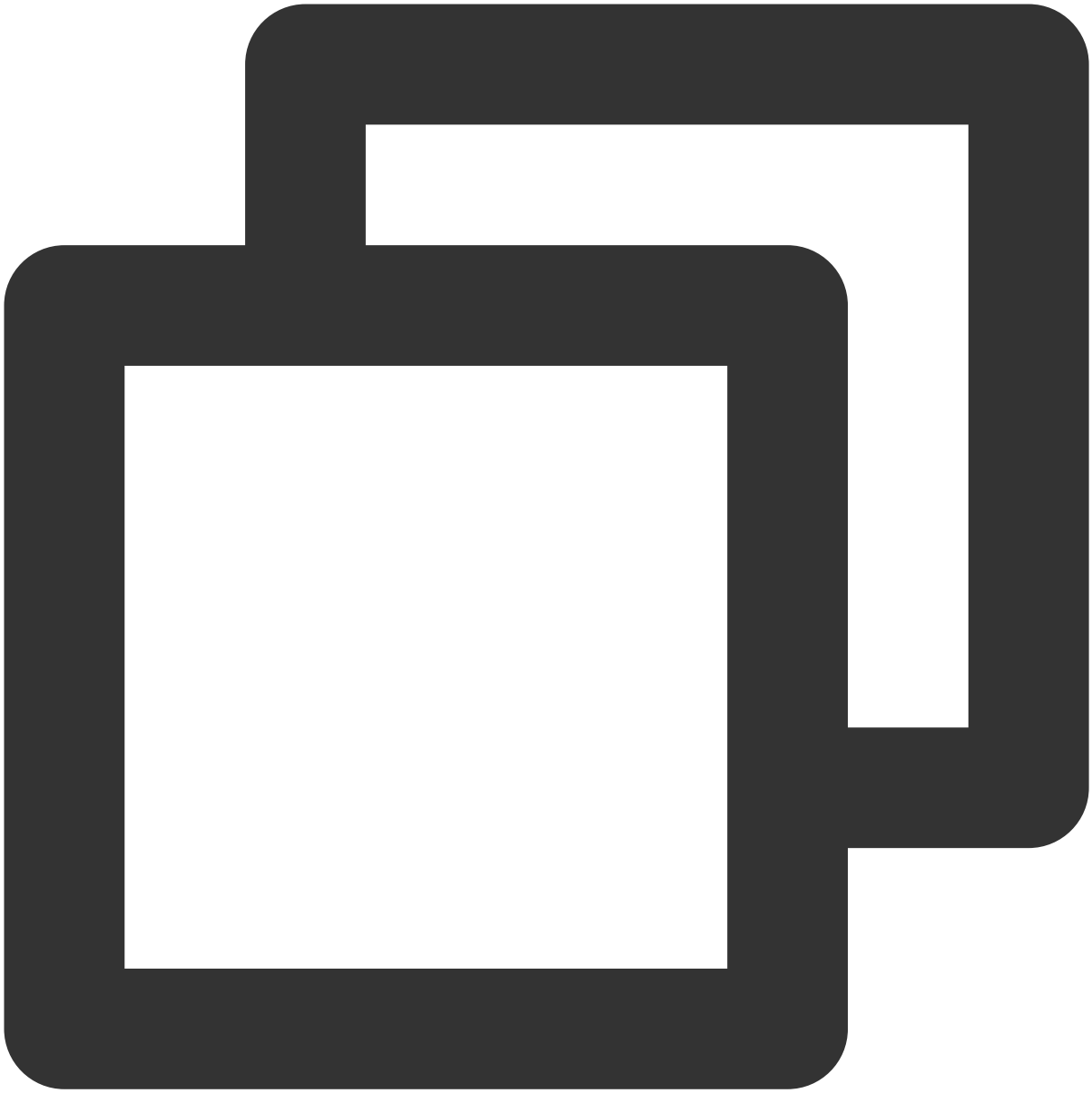
```
wget -O netperf-2.7.0.tar.gz -c  https://codeload.github.com/HewlettPackard/netperf
```



```
tar zxf netperf-2.7.0.tar.gz
```



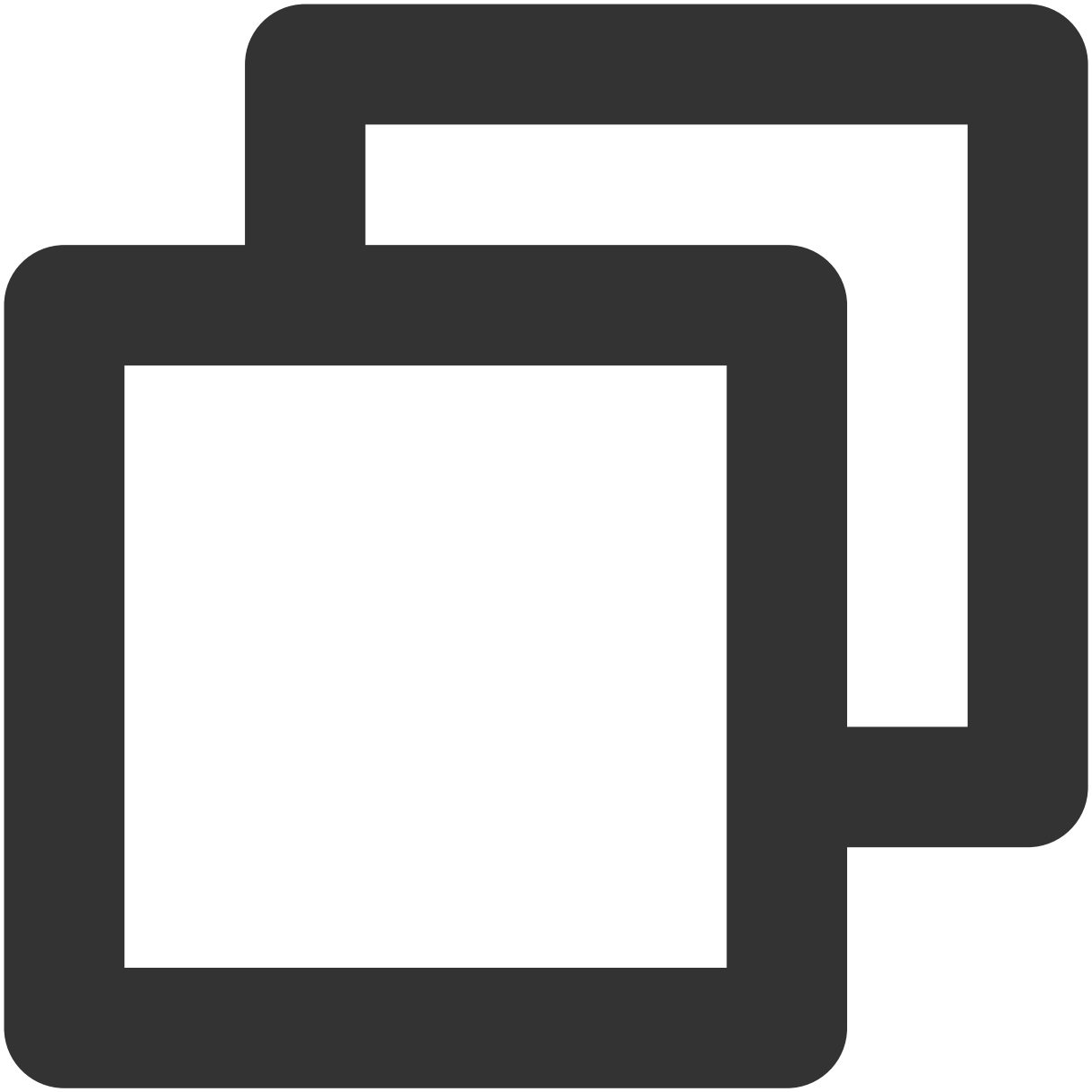
```
cd netperf-netperf-2.7.0
```



```
./autogen.sh && ./configure && make && make install
```

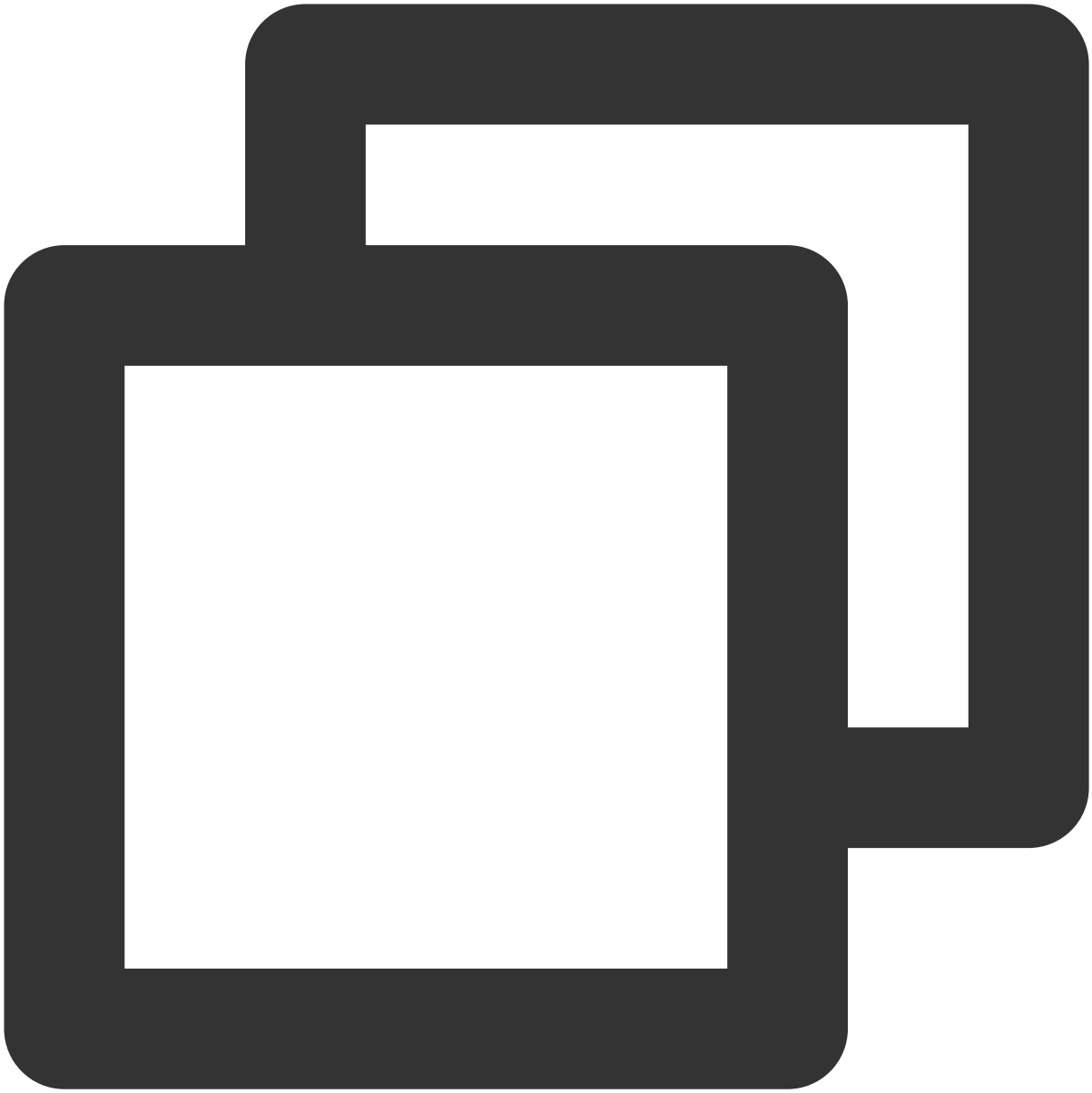
パケット送信パフォーマンスのテスト

1. サーバー上でそれぞれ以下のコマンドを実行し、netperfおよびnetserverの残りのプロセスを停止します。



```
pkill netserver && pkill netperf
```

2. このうちサーバーaをクライアント側、 サーバーbとサーバーcをサーバー側とします。サーバー側で以下のコマンドを実行し、netserverを実行します。

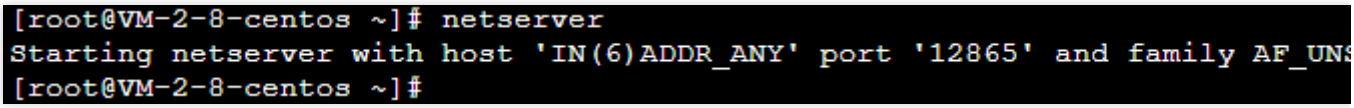


```
netserver
```

返された結果が下図のとおりであれば、他のnetserverプロセスがまだ存在することを表します。手順1 中のコマンドを実行し、該当のプロセスを停止してください。

```
[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 ~]#
```

返された結果が下図のとおりであれば、netserverの実行に成功したことを表します。続けて次の操作を行ってください。

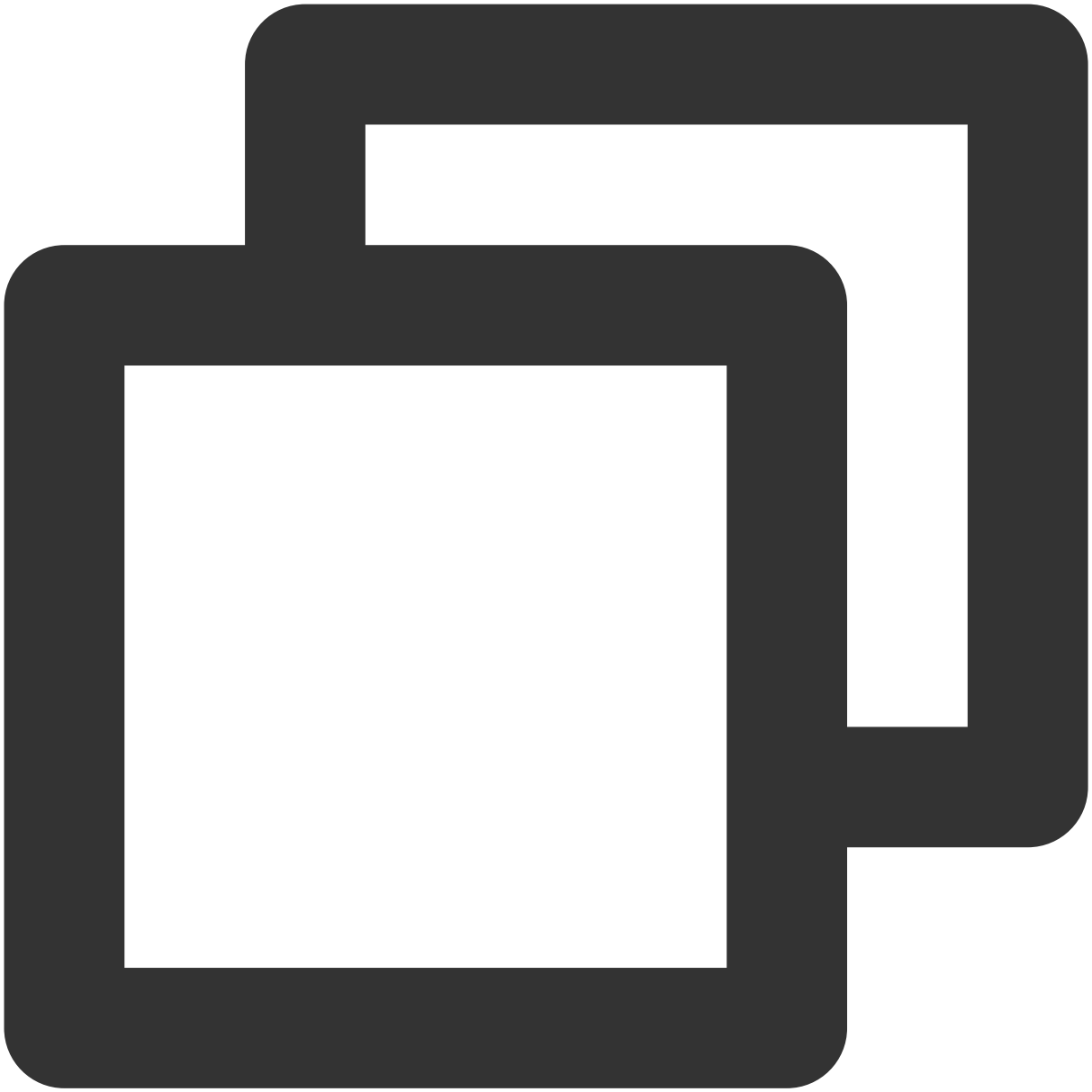


3. テストシーン で提供されたコマンドをクライアント側で実行し、クライアント側のパケット送信パフォーマンスがそれ以上向上しなくなるまでnetperfプロセスを増減し続けます。

説明：

コマンド実行を繰り返す必要があり、かつserver ipには異なるサーバーIPを使用する必要があります。1つのプロセスが最大パフォーマンスに達しない場合は、テスト支援スクリプト を実行し、プロセスを一括して開始することができます。

4. クライアント側で以下のコマンドを実行し、クライアント側のパケット送信パフォーマンスの変化を観察し、最大値をとります。

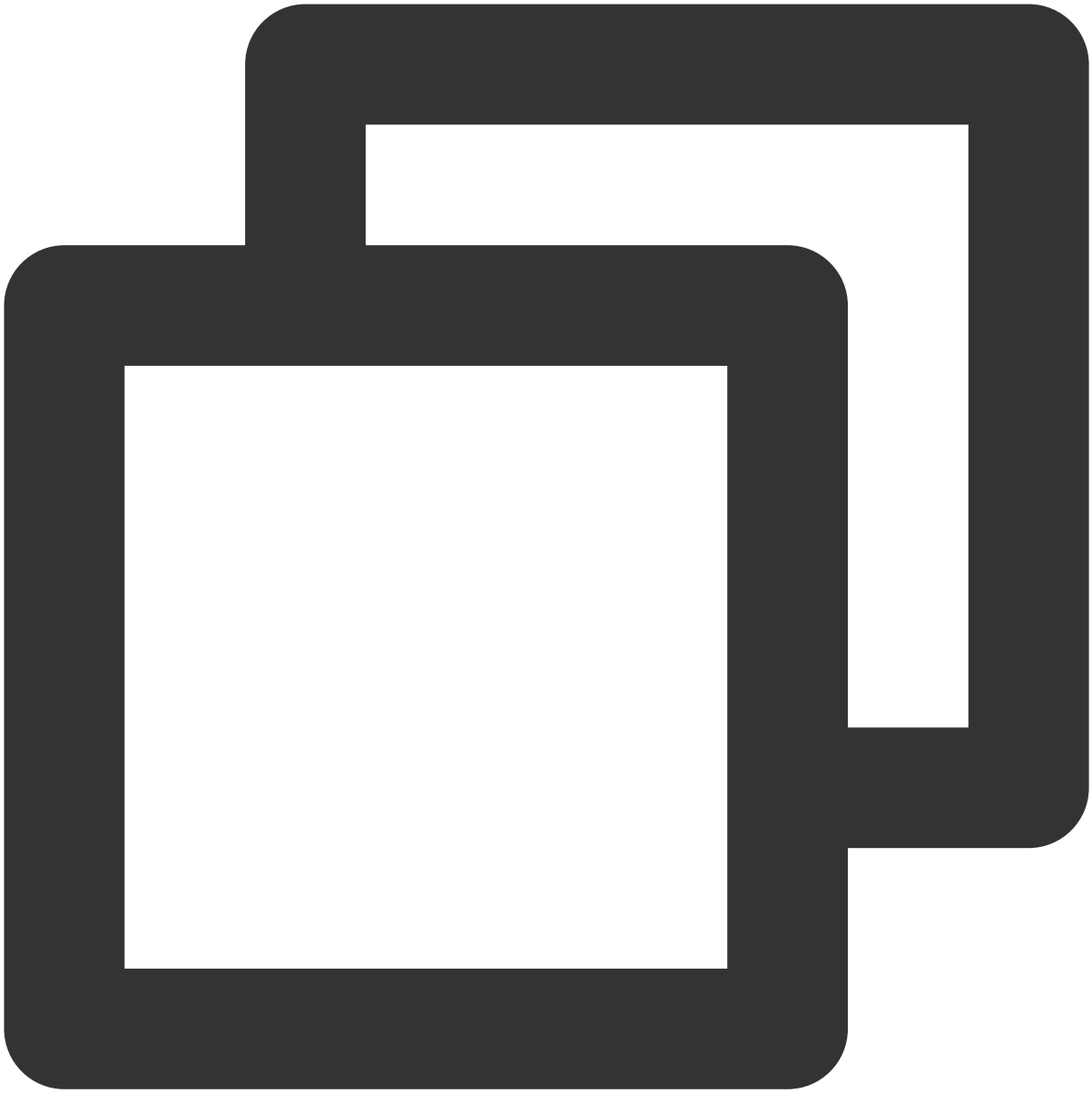


```
sar -n DEV 1
```

得られた結果に基づき、パフォーマンス指標 を参照して分析を行うことで、CVMの高スループットネットワークパフォーマンスを測定することができます。

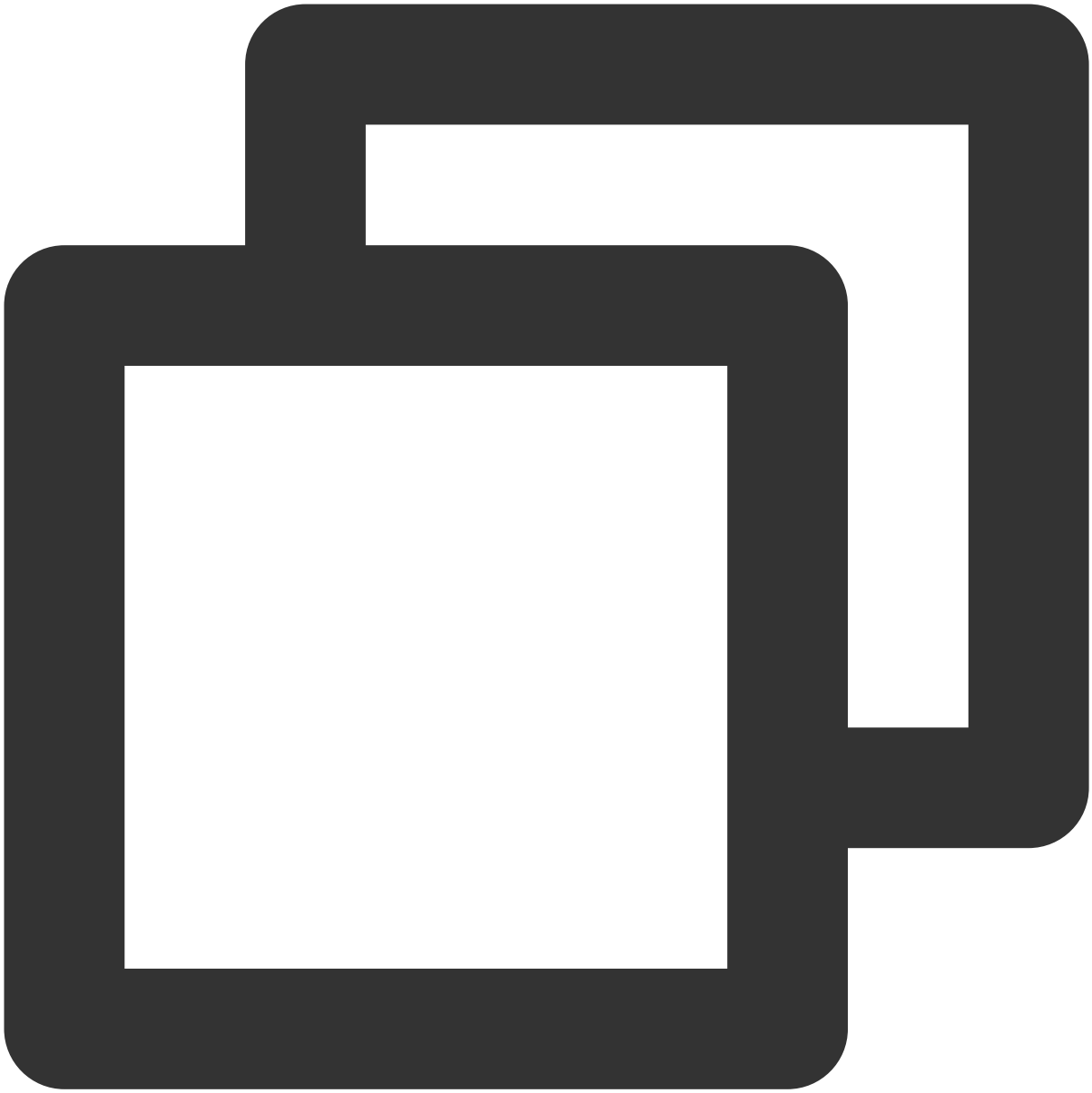
パケット受信パフォーマンスのテスト

1. サーバー上でそれぞれ以下のコマンドを実行し、netperfおよびnetserverの残りのプロセスを停止します。



```
pkill netserver && pkill netperf
```

2. このうちサーバーaをサーバー側、 サーバーbとサーバーcをクライアント側とします。サーバー側で以下のコマンドを実行し、netserverを実行します。

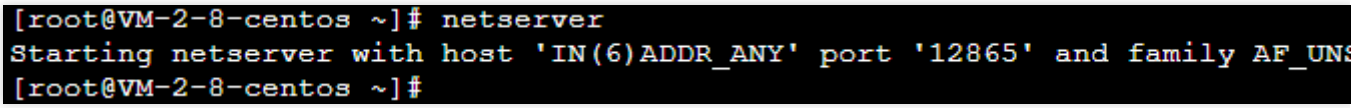


```
netserver
```

返された結果が下図のとおりであれば、他のnetserverプロセスがまだ存在することを表します。手順1中のコマンドを実行し、該当のプロセスを停止してください。

```
[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 ~]#
```

返された結果が下図のとおりであれば、netserverの実行に成功したことを表します。続けて次の操作を行ってください。

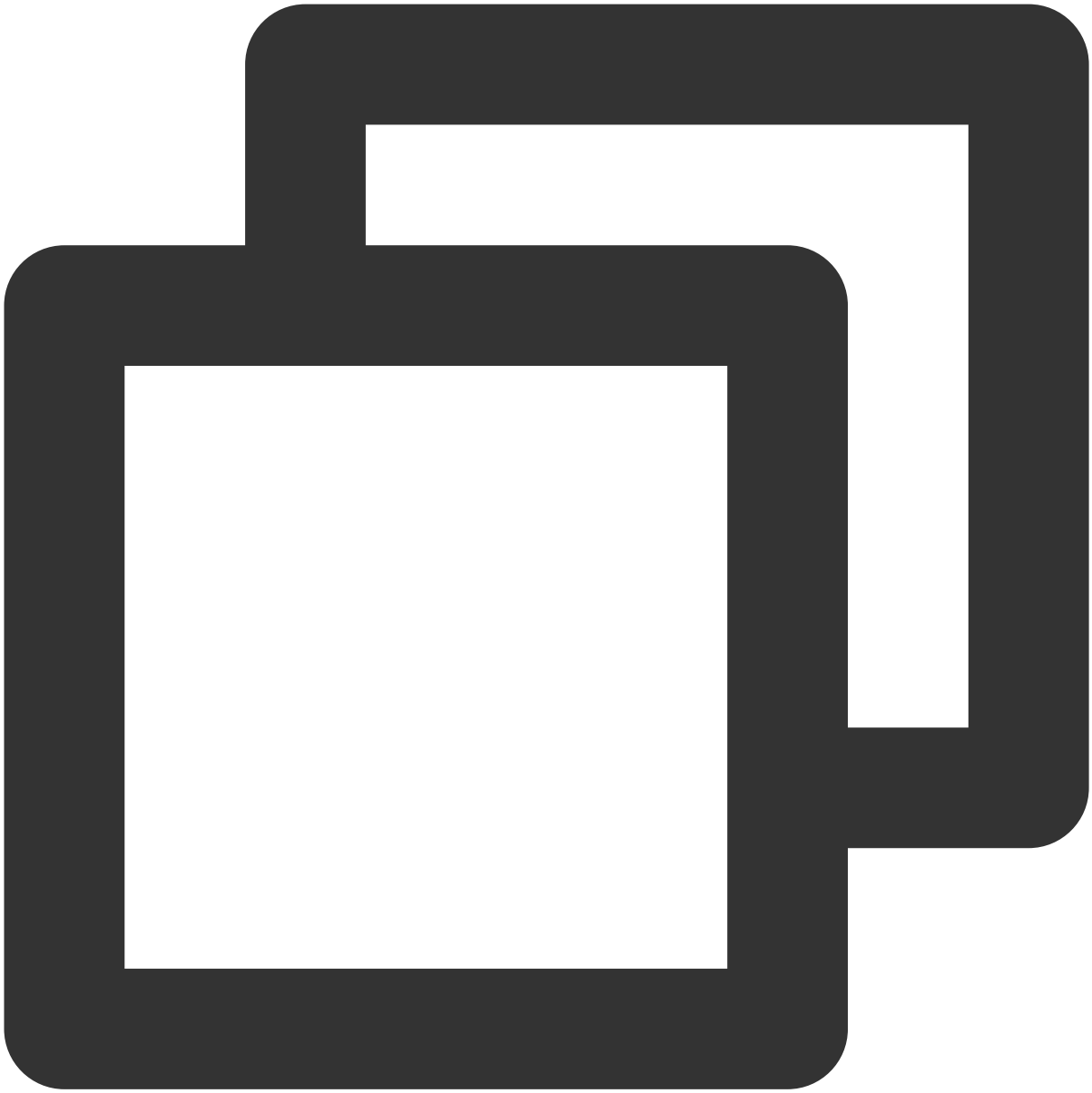


3. テストシーン で提供されたコマンドをクライアント側で実行し、クライアント側のパケット送信パフォーマンスがそれ以上向上しなくなるまでnetperfプロセスを増減し続けます。

説明：

コマンド実行を繰り返す必要があり、クライアント側はそれぞれnetperfを開始します。1つのプロセスが最大パフォーマンスに達しない場合は、テスト支援スクリプト を実行し、プロセスを一括して開始することができます。

4. サーバー側で以下のコマンドを実行し、サーバー側のパケット受信パフォーマンスの変化を観察し、最大値をとります。



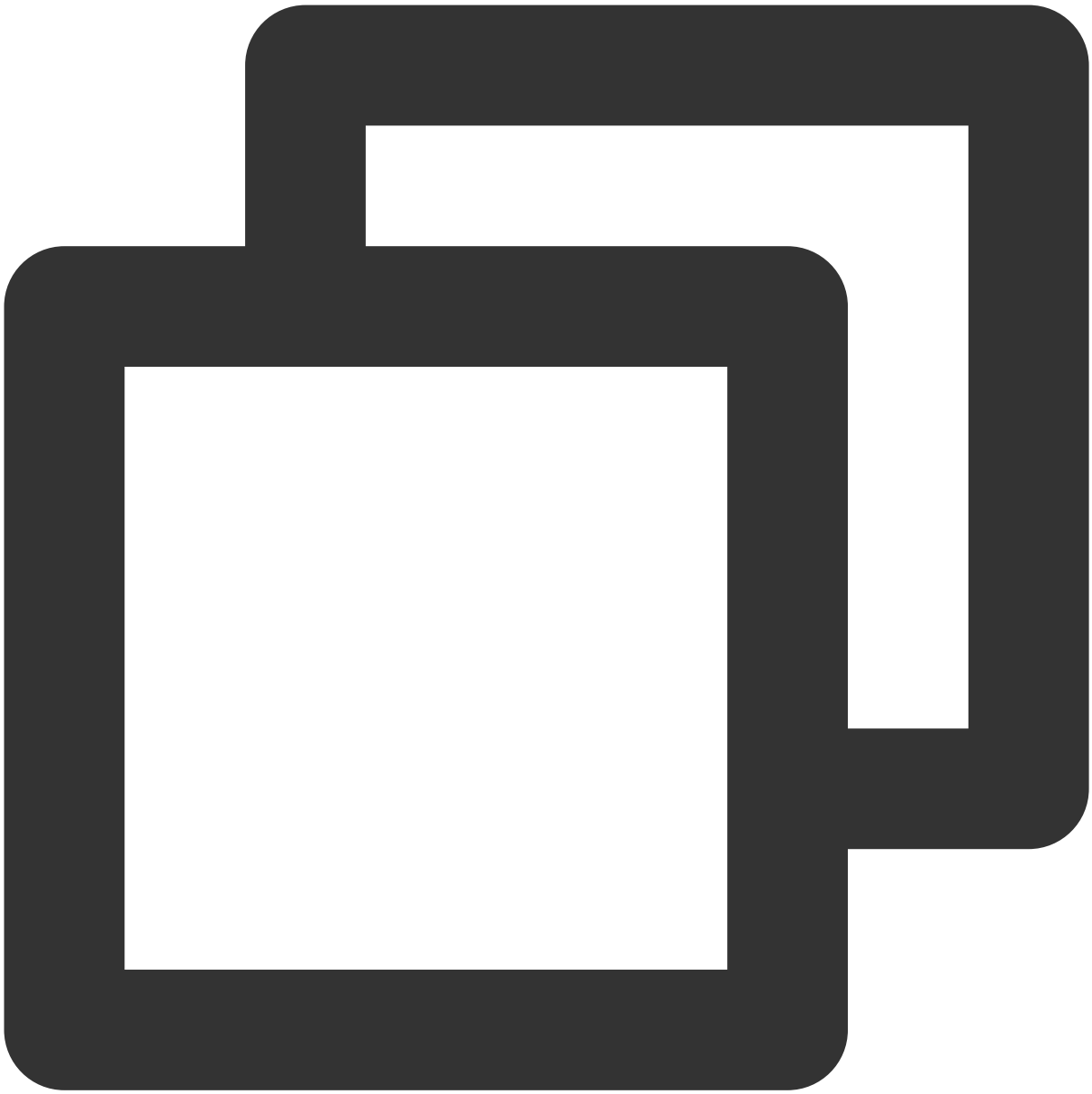
```
sar -n DEV 1
```

得られた結果に基づき、パフォーマンス指標 を参照して分析を行うことで、CVMの高スループットネットワークパフォーマンスを測定することができます。

付録

テスト支援スクリプト

このスクリプトを実行すると、複数のnetperfプロセスを迅速に開始することができます。



```
#!/bin/bash
count=$1
for ((i=1;i<=count;i++))
do
    echo "Instance:$i-------"
    # 下記のコマンドはテストシーンの表内のコマンドに置き換え可能です
    # -Hの後にサーバーのIPアドレスを入力します。
    # -lの後にテスト期間を入力します。netperfが途中で終了しないように、期間を10000に設定します。
    netperf -t UDP_STREAM -H <server ip> -l 10000 -- -m 64 -R 1 &
```

```
done
```

DPDKを使用したテスト

最終更新日：：2023-06-30 15:28:14

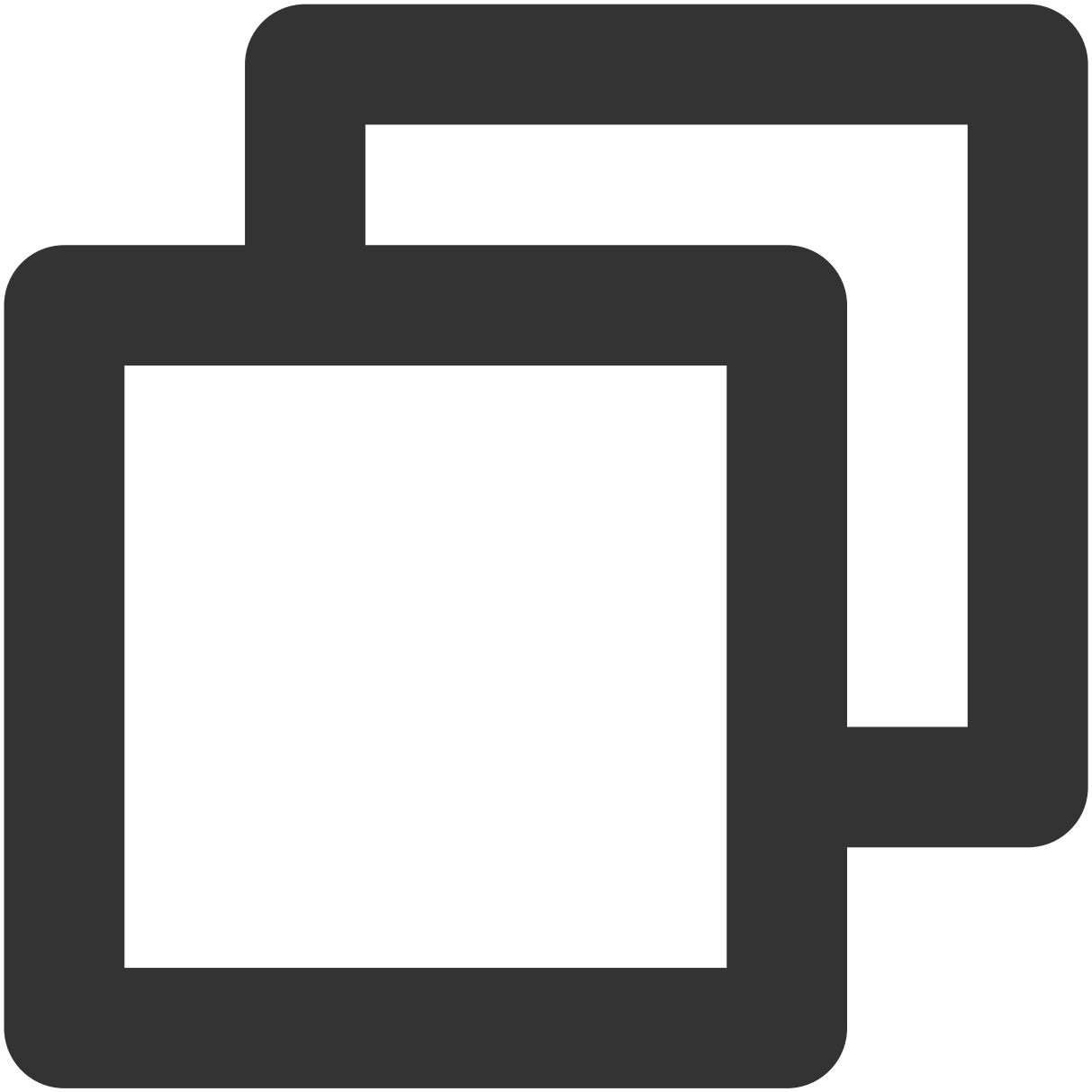
概要

このドキュメントでは、DPDK を使用してCVM インスタンスの高スループットネットワークパフォーマンスをテストする方法について説明します。

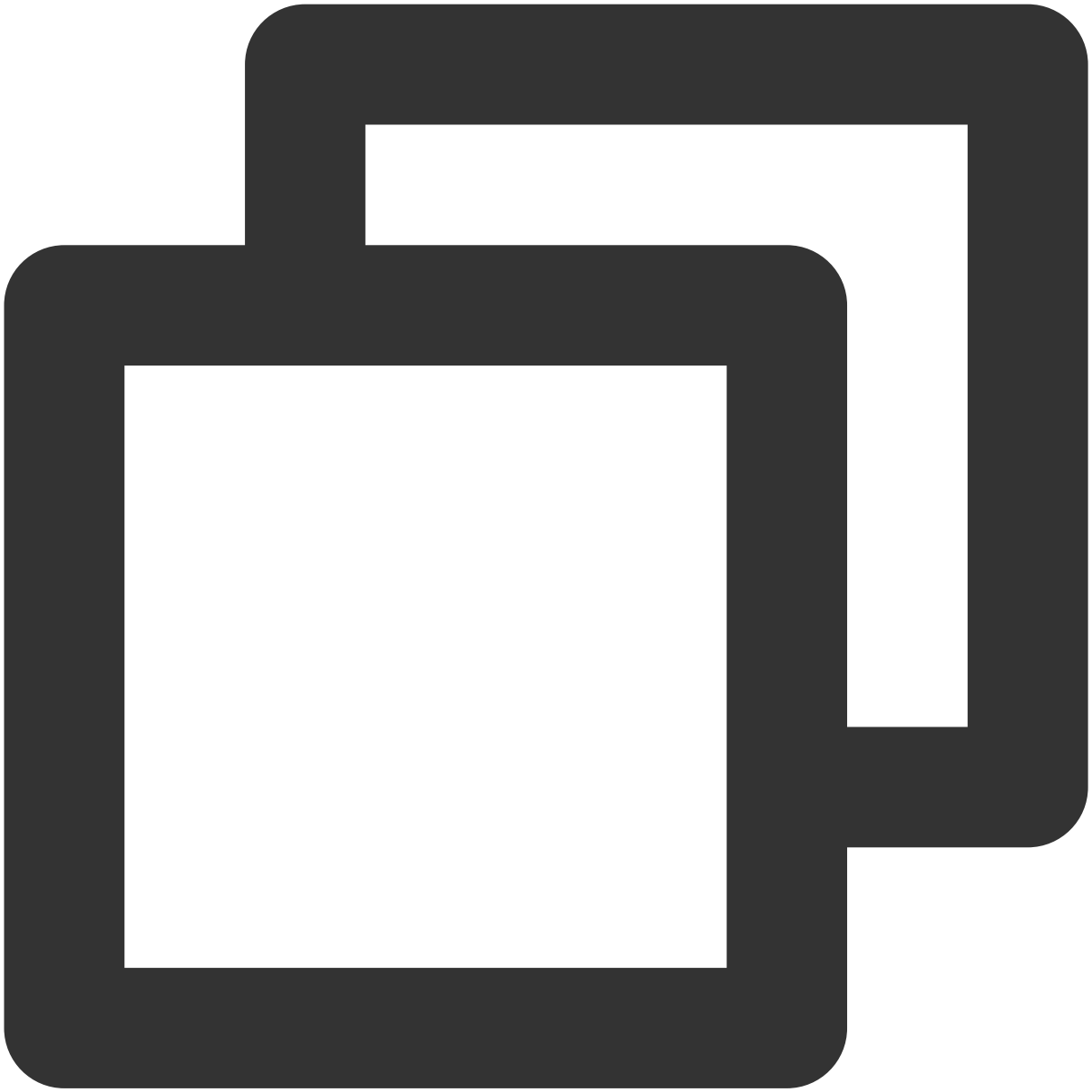
操作手順

DPDKのコンパイルとインストール

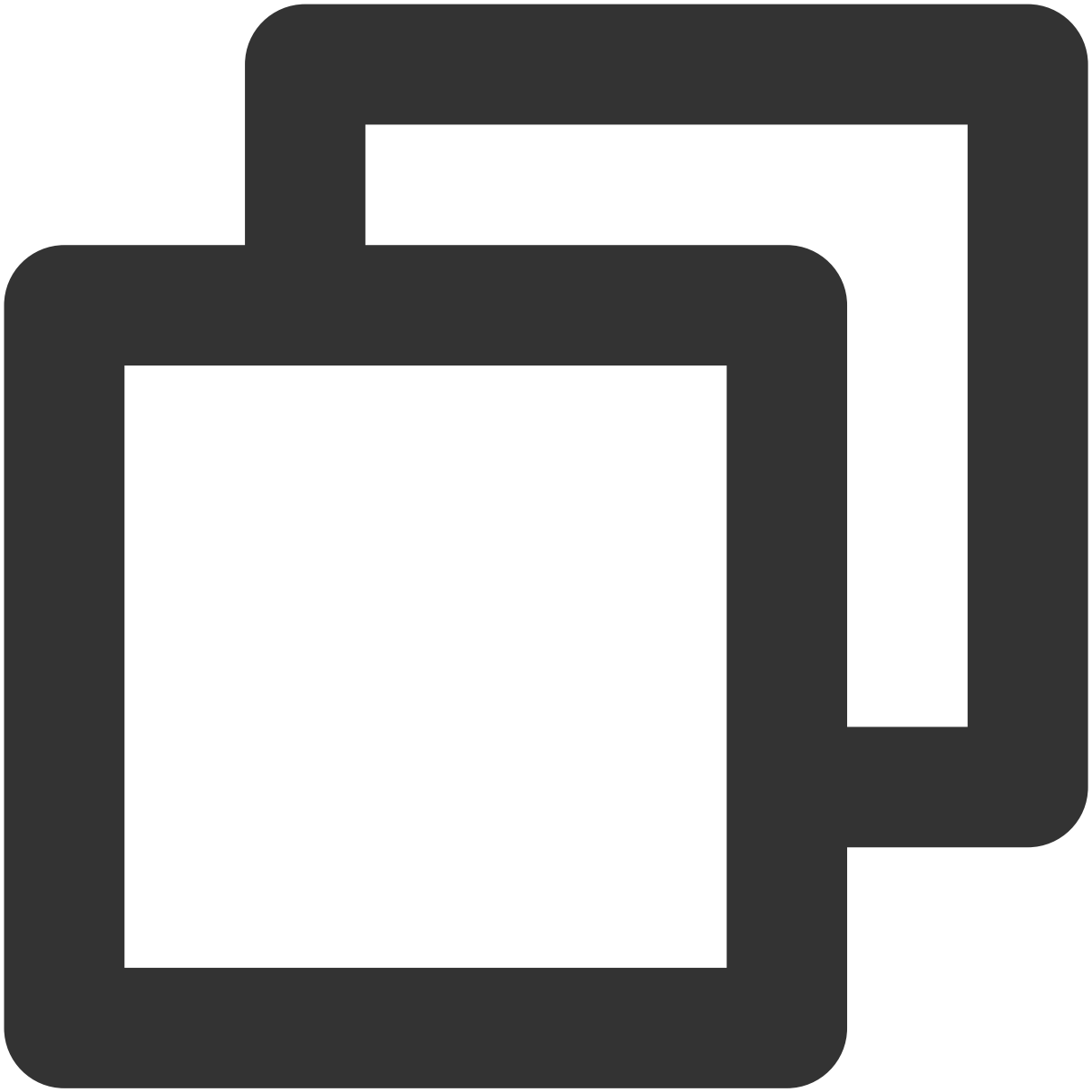
1. 2つのテストサーバーが必要です。サーバーは Linux CVM 構成のカスタマイズ の指示に従って購入できます。ここではテストサーバーにCentOS 8.2 OSを使用します。
2. 順にテストサーバーにログインし、以下のコマンドを実行してDPDKツールをダウンロードします。CVMへのログイン方法については、 標準ログイン方式を使用してLinuxインスタンスにログイン（推奨）をご参照ください。。



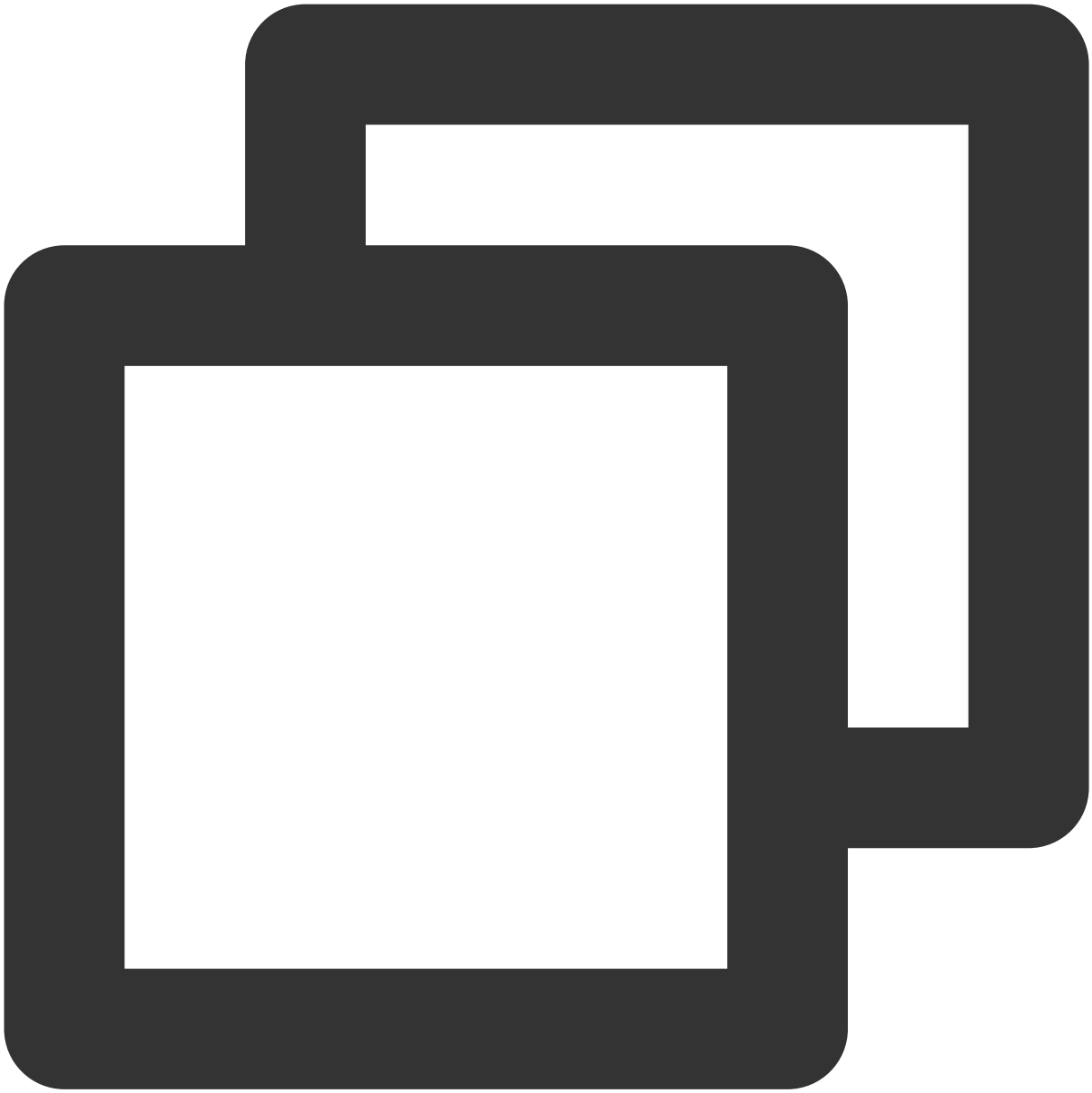
```
yum install -y sysstat wget tar automake make gcc
```



```
wget http://git.dpdk.org/dpdk/snapshot/dpdk-17.11.tar.gz
```

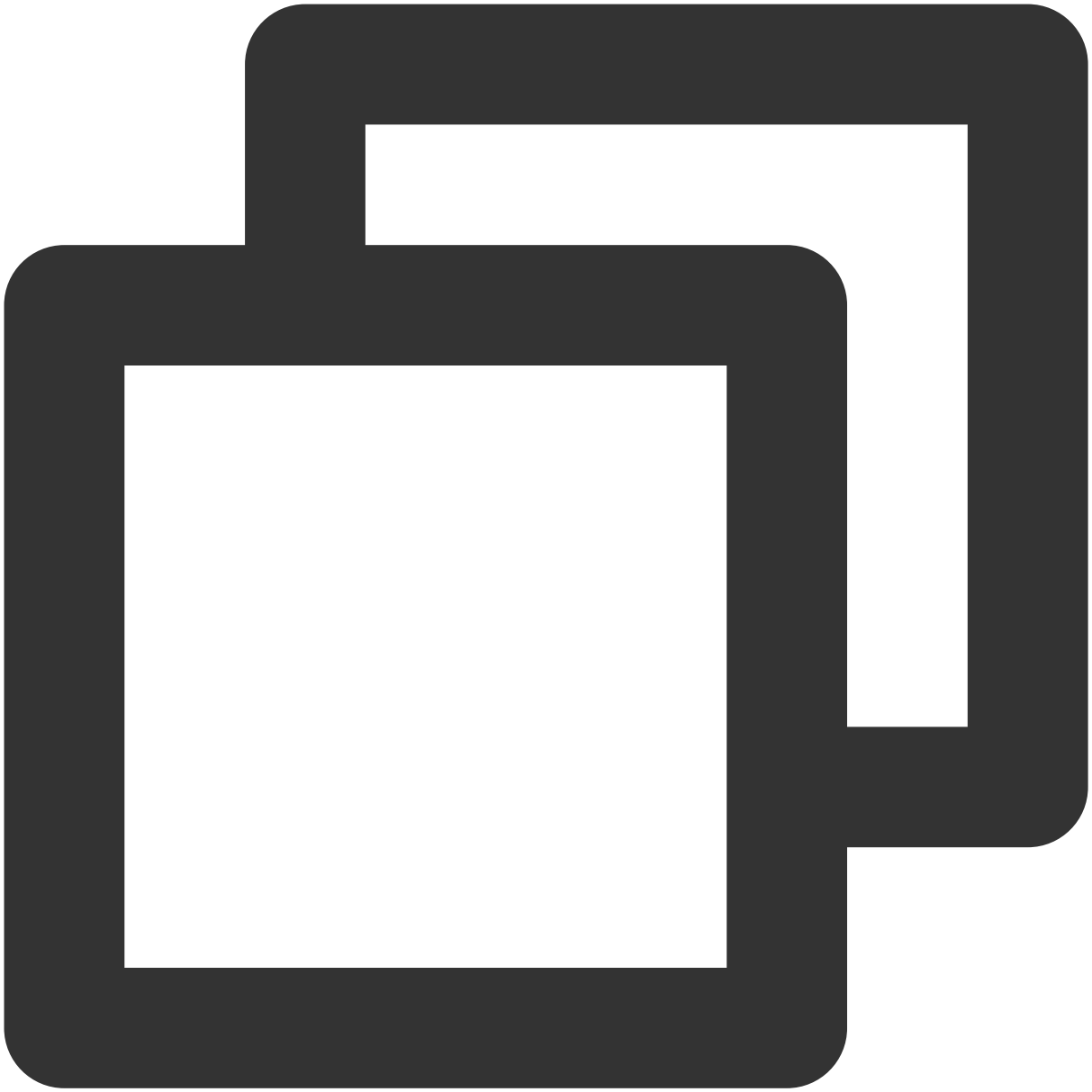


```
tar -xf dpdk-17.11.tar.gz
```



```
mv dpdk-17.11 dpdk
```

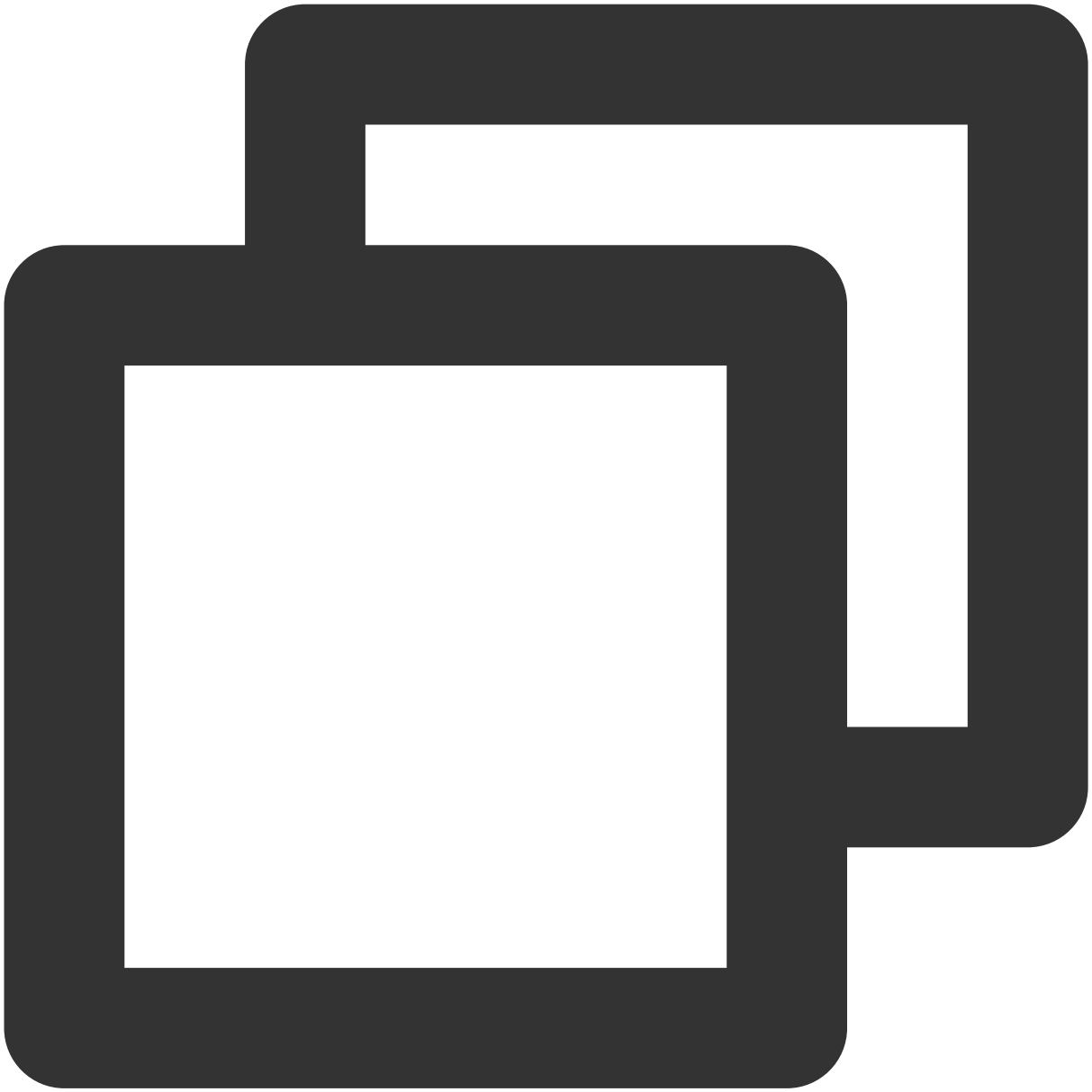
3. txonlyエンジンを変更し、各DPDKのパケット送信CPUのUDPトラフィック用ポートを、複数のストリームを発生させるよう変更します。
以下のコマンドを実行し、 `dpdk/app/test-pmd/txonly.c` ファイルを変更します。



```
vim dpdk/app/test-pmd/txonly.c
```

i を押して編集モードに入り、以下の内容を変更します。

3.1.1 `#include "testpmd.h"を見つけます。 次の内容を次の行に追加します。

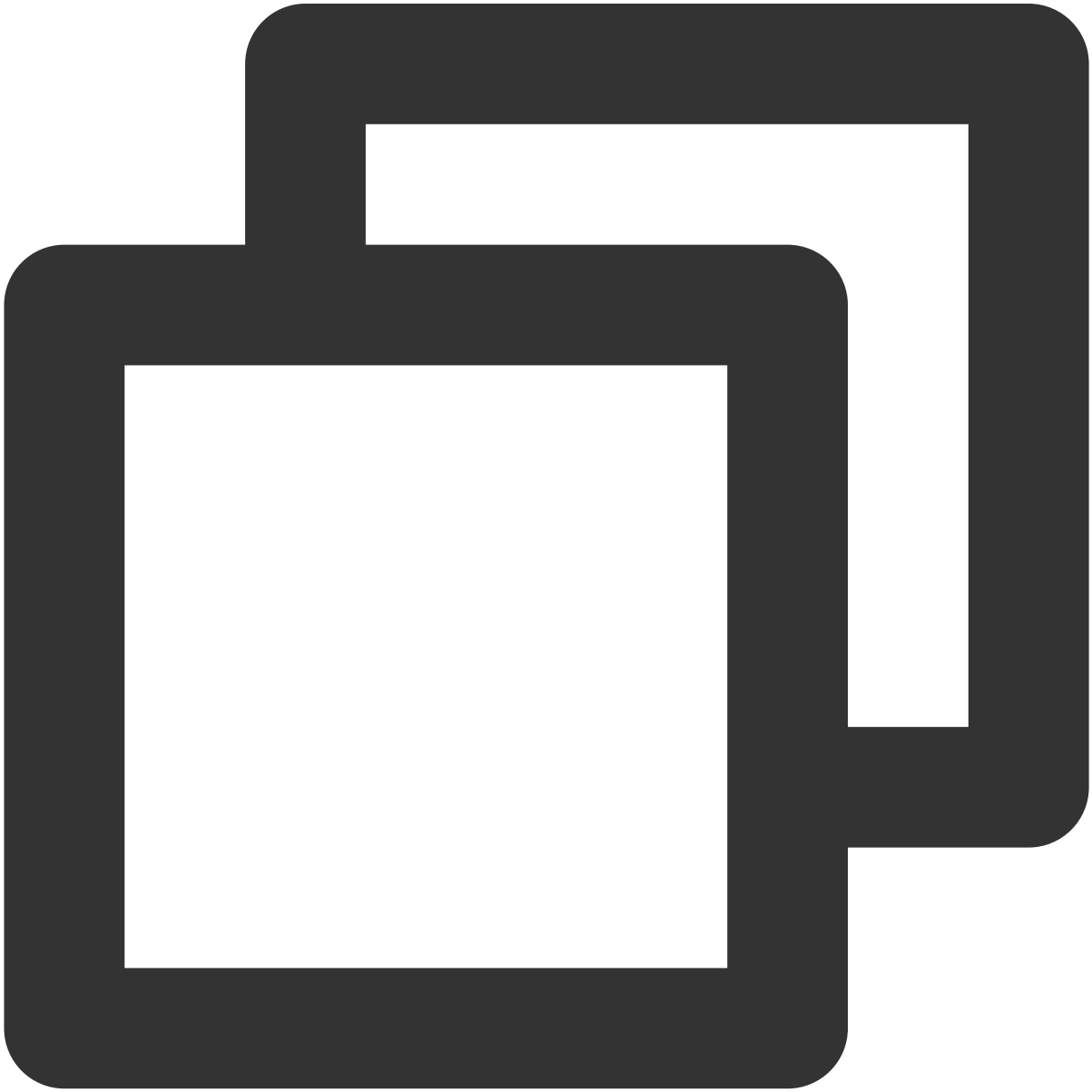


```
RTE_DEFINE_PER_LCORE(struct udp_hdr, lcore_udp_hdr);
RTE_DEFINE_PER_LCORE(uint16_t, test_port);
```

結果は次のようになります：

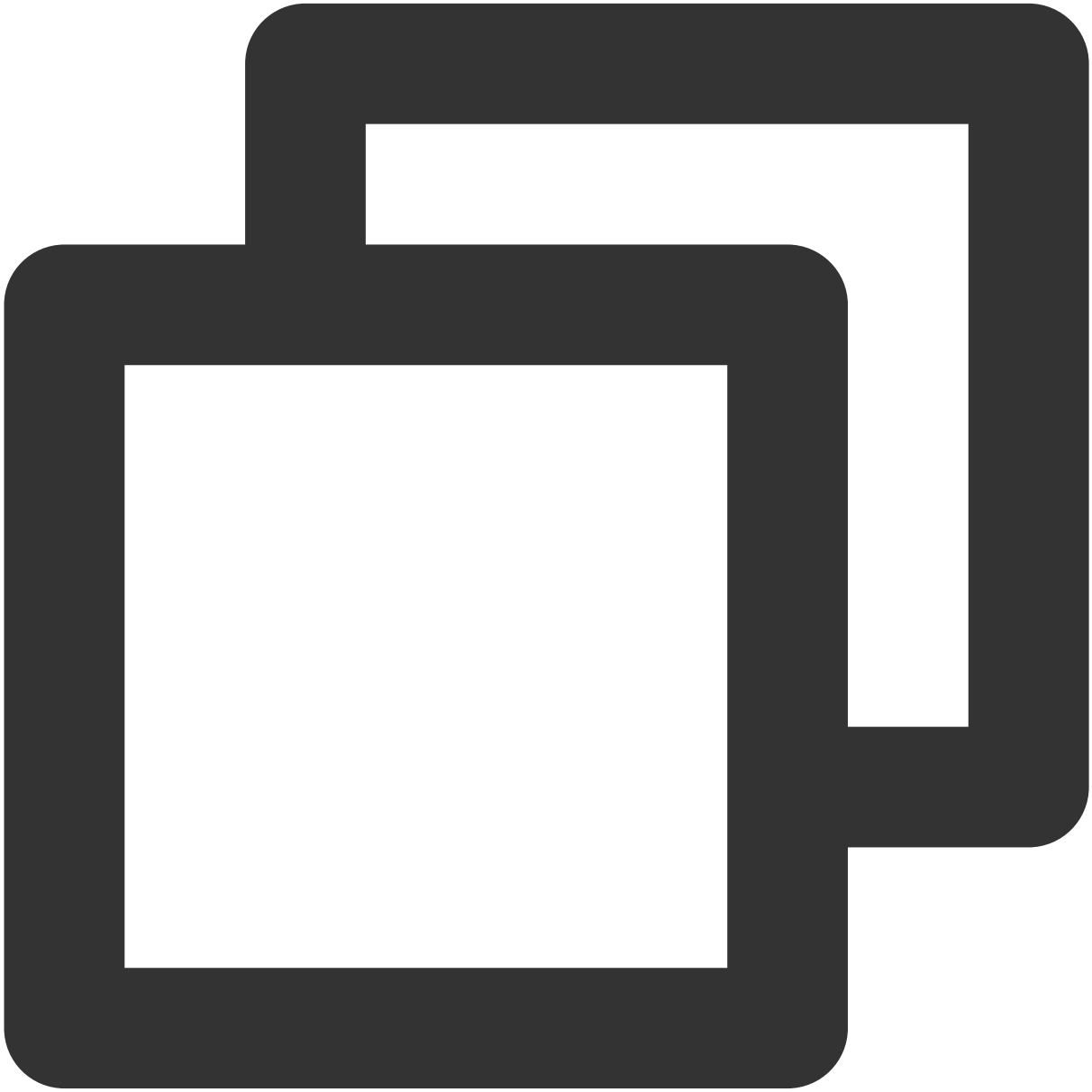
```
#include "testpmd.h"
RTE_DEFINE_PER_LCORE(struct udp_hdr, lcore_udp_hdr);
RTE_DEFINE_PER_LCORE(uint16_t, test_port);

#define UDP_SRC_PORT 1024
#define UDP_DST_PORT 1024
```

3.1.2 `ol_flags |= PKT_TX_MACSEC;` を見つけます。 次の内容を次の行に追加します。



```
/* dummy test udp port */
memcpy(&RTE_PER_LCORE(lcore_udp_hdr), &pkt_udp_hdr, sizeof(pkt_udp_hdr));
```

3.1.3 `for (nb_pkt = 0; nb_pkt < nb_pkt_per_burst; nb_pkt++) {` を見つけ、これを以下の内容に置き換えます。

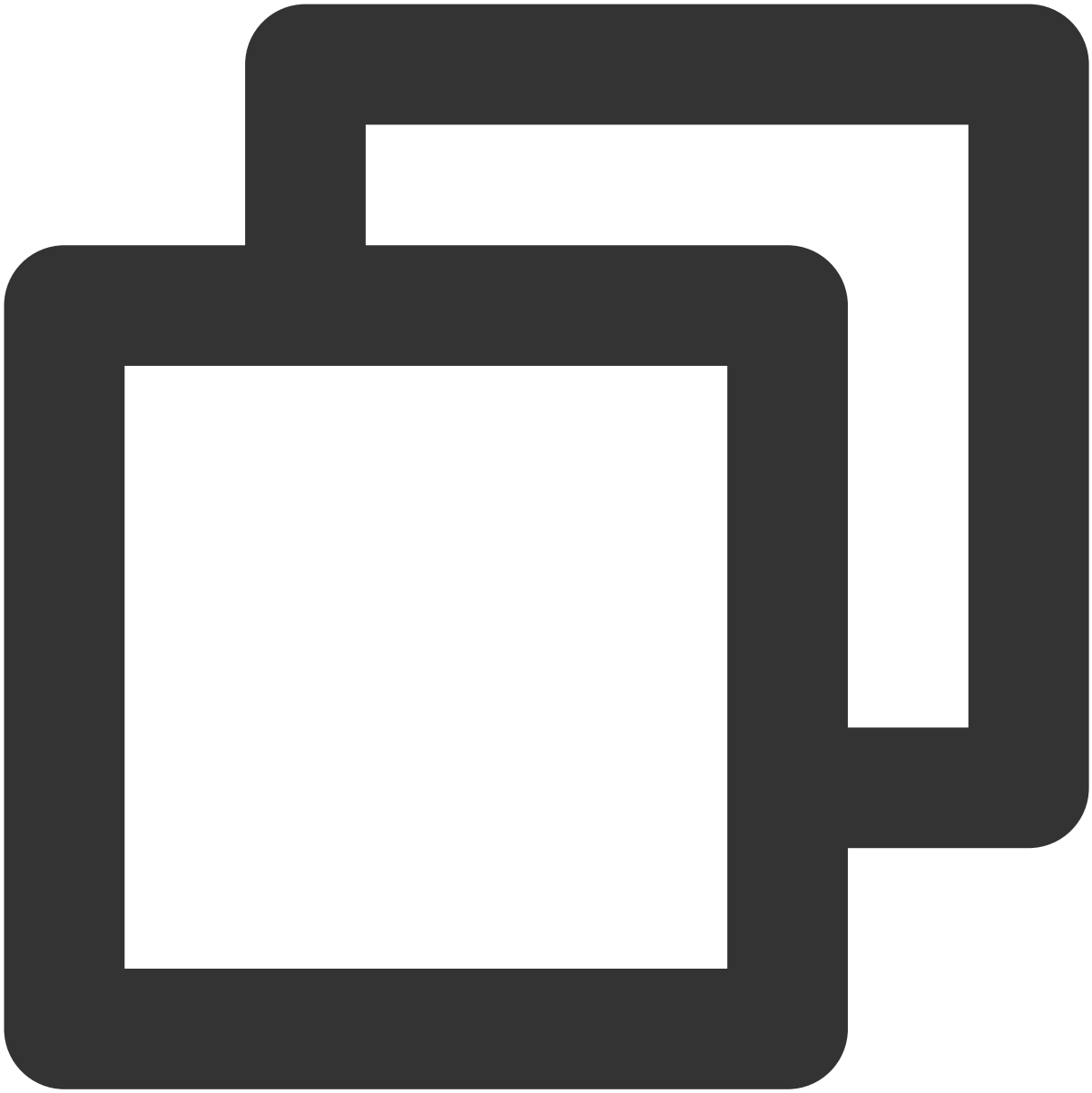


```
RTE_PER_LCORE(test_port)++;
RTE_PER_LCORE(lcore_udp_hdr).src_port = rte_cpu_to_be_16(2222);
RTE_PER_LCORE(lcore_udp_hdr).dst_port = rte_cpu_to_be_16(rte_lcore_id() * 2000 + RT
```

結果は次のようになります：

```
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() * 2000 + RTE_PER_LCO

        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,` を見つけ、これを以下の内容に置き換えます。



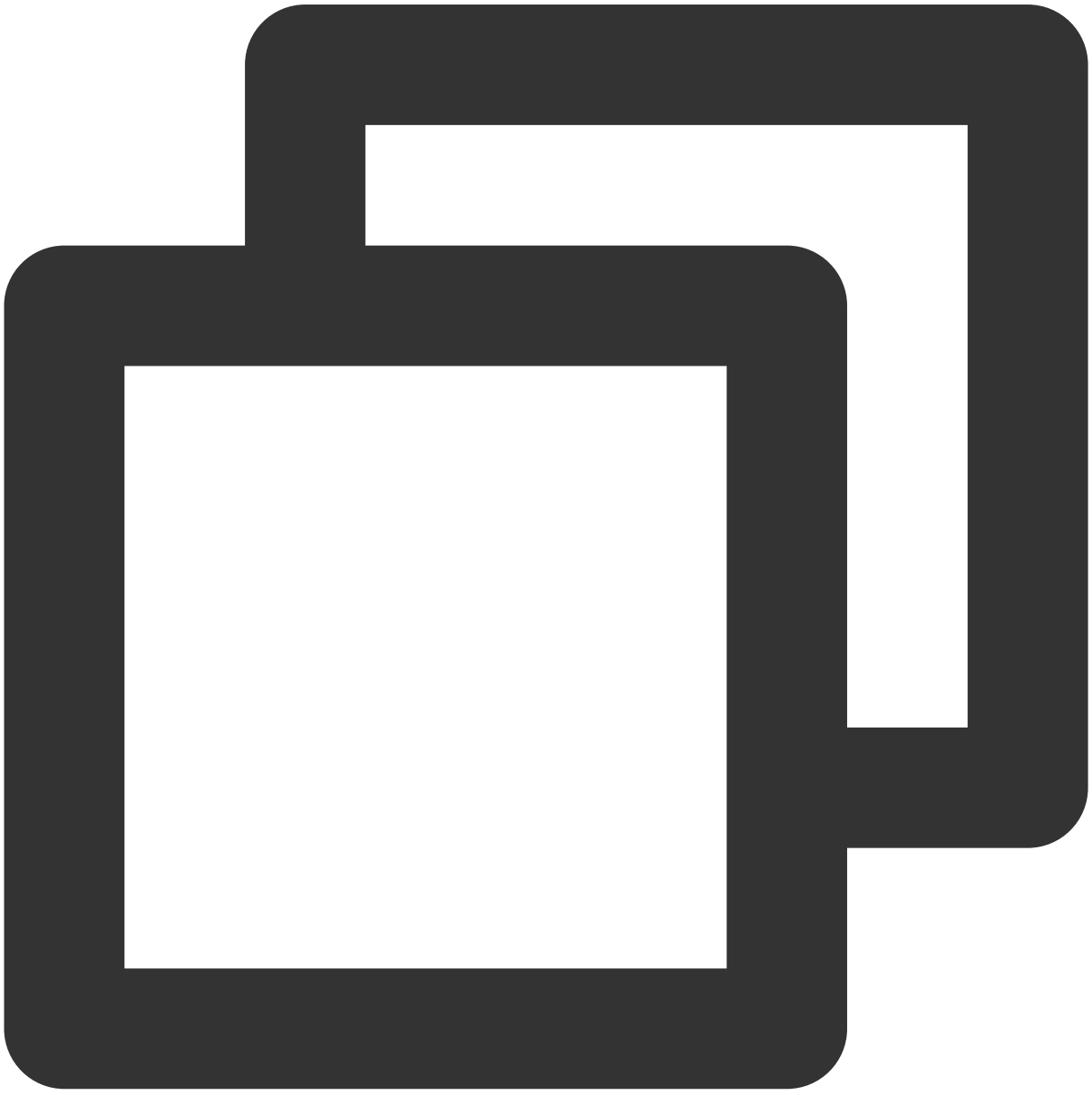
```
copy_buf_to_pkt(&RTE_PER_LCORE(lcore_udp_hdr), sizeof(RTE_PER_LCORE(lcore_udp_hdr))
```

結果は次のようになります：

```
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));
```

Esc を押し、**:wq** を入力して変更を保存し、終了します。

以下のコマンドを実行し、 `dpdk/config/common_base` ファイルを変更します。



```
vim dpdk/config/common_base
```

i を押して編集モードに入り、 `CONFIG_RTE_MAX_MEMSEG=256` を見つけて、これを1024に変更します。変更が完了すると、以下のようになります。

```
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
```

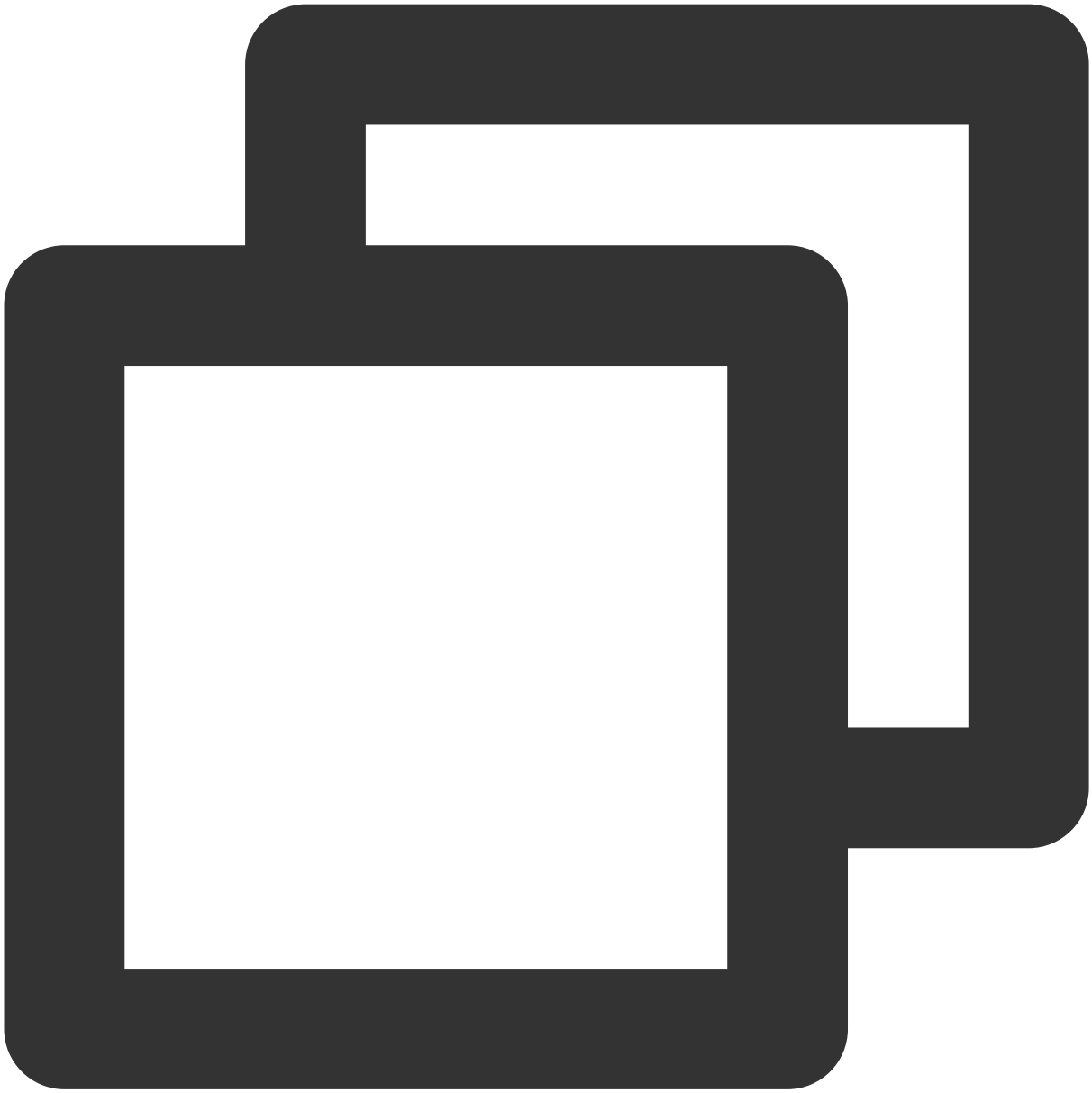
i を押して編集モードに入り、 CONFIG_RTE_MAX_LCORE=128`を見つけて、システムのCPU コアの数が128より大きい場合は、256に変更できます。変更が完了すると、以下のようになります。

```
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
```

Esc を押し、**:wq** を入力して変更を保存し、終了します。

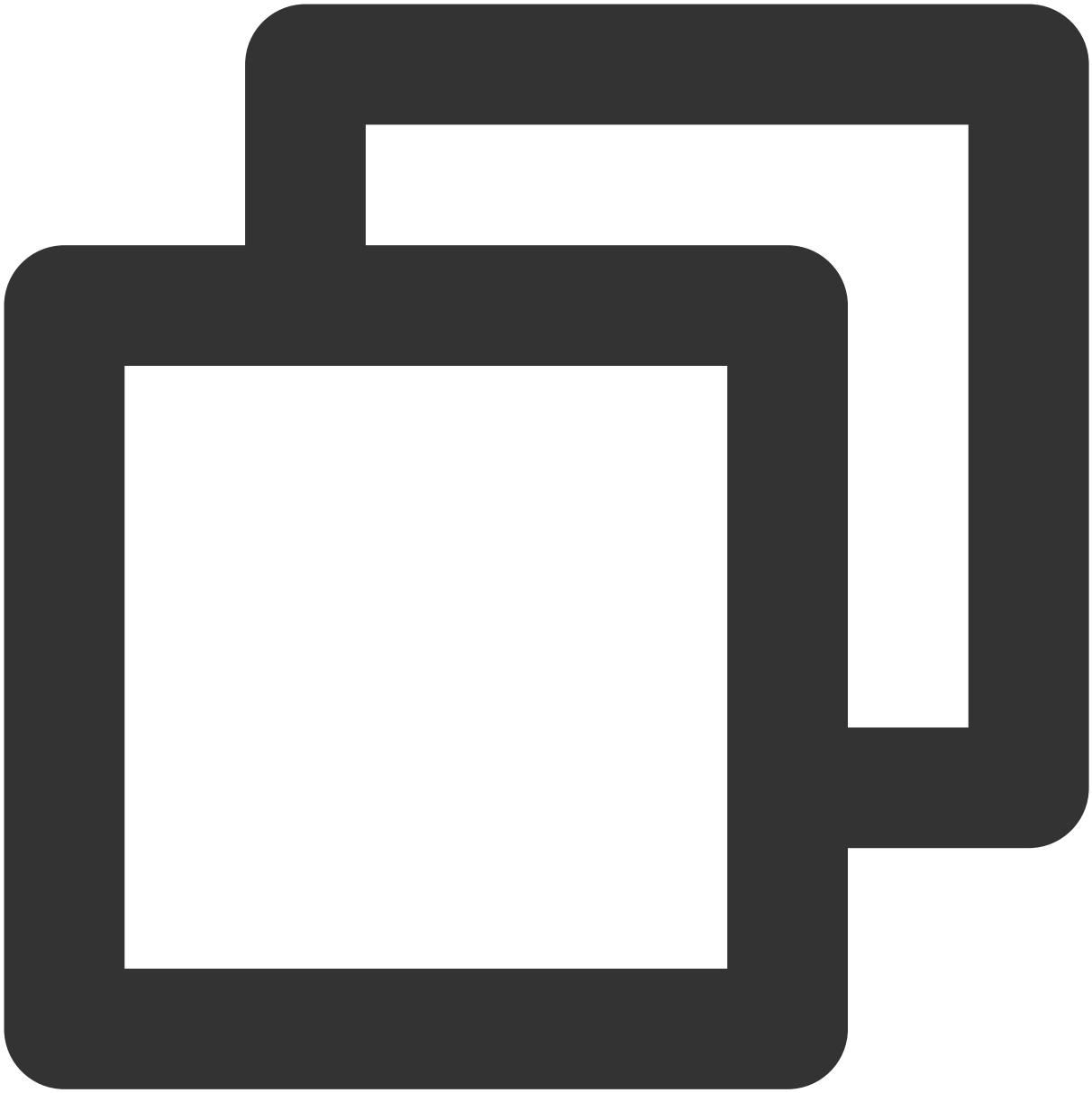
説明：

受信側および送信側テストサーバーの両方で上記の構成ファイルを変更する必要があります。以下のコマンドを使用すると、変更されたファイルを相手側に送信し、変更の重複を避けることができます。



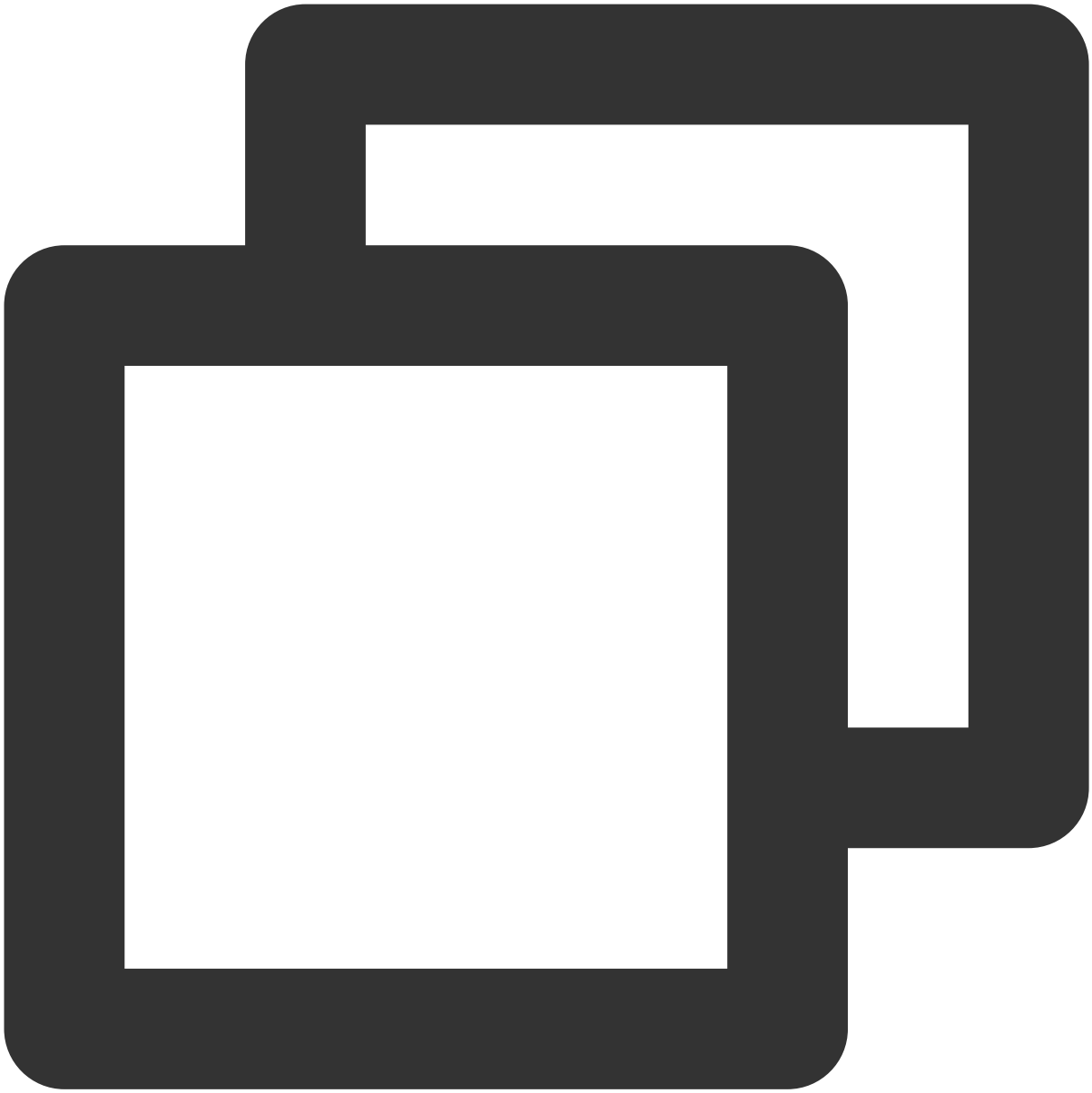
```
scp -P 22 /root/dpdk/app/test-pmd/txonly.c root@<IPアドレス>:/root/dpdk/app/test-pmd/
scp -P 22 /root/dpdk/config/common_base root@<IPアドレス>:/root/dpdk/config
```

4. 以下のコマンドを実行し、 `dpdk/app/test-pmd/txonly.c` のIPアドレスを、テストサーバーのIPに変更します。



```
vim dpdk/app/test-pmd/txonly.c
```

i を押して編集モードに入り、以下の内容を見つけます。



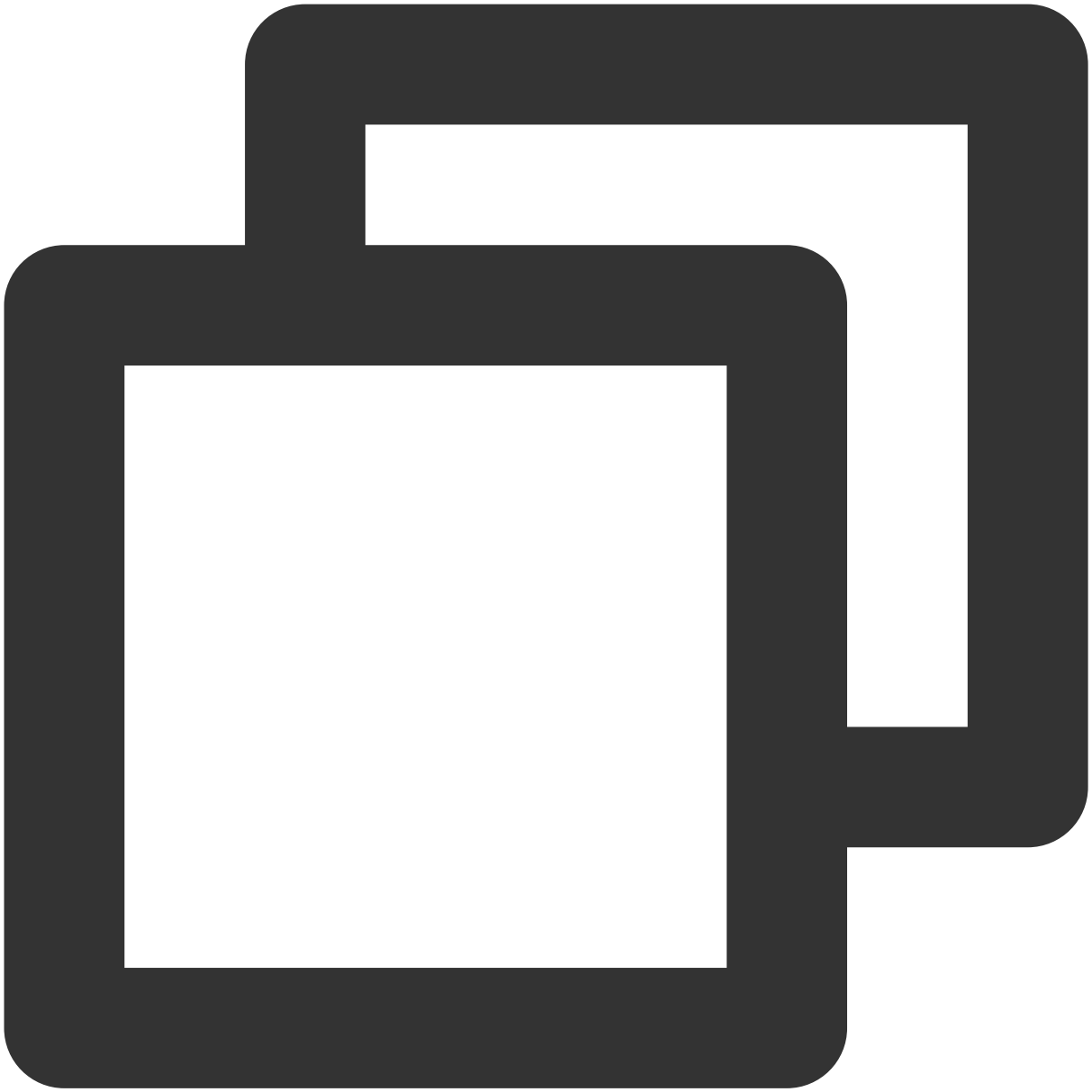
```
#define IP_SRC_ADDR (198U << 24) | (18 << 16) | (0 << 8) | 1;
#define IP_DST_ADDR (198U << 24) | (18 << 16) | (0 << 8) | 2;
```

数字の198、18、0、1をサーバーのIPに置き換えます。SRC_ADDRは送信側の IP、DST_ADDRは受信側のIPとします。

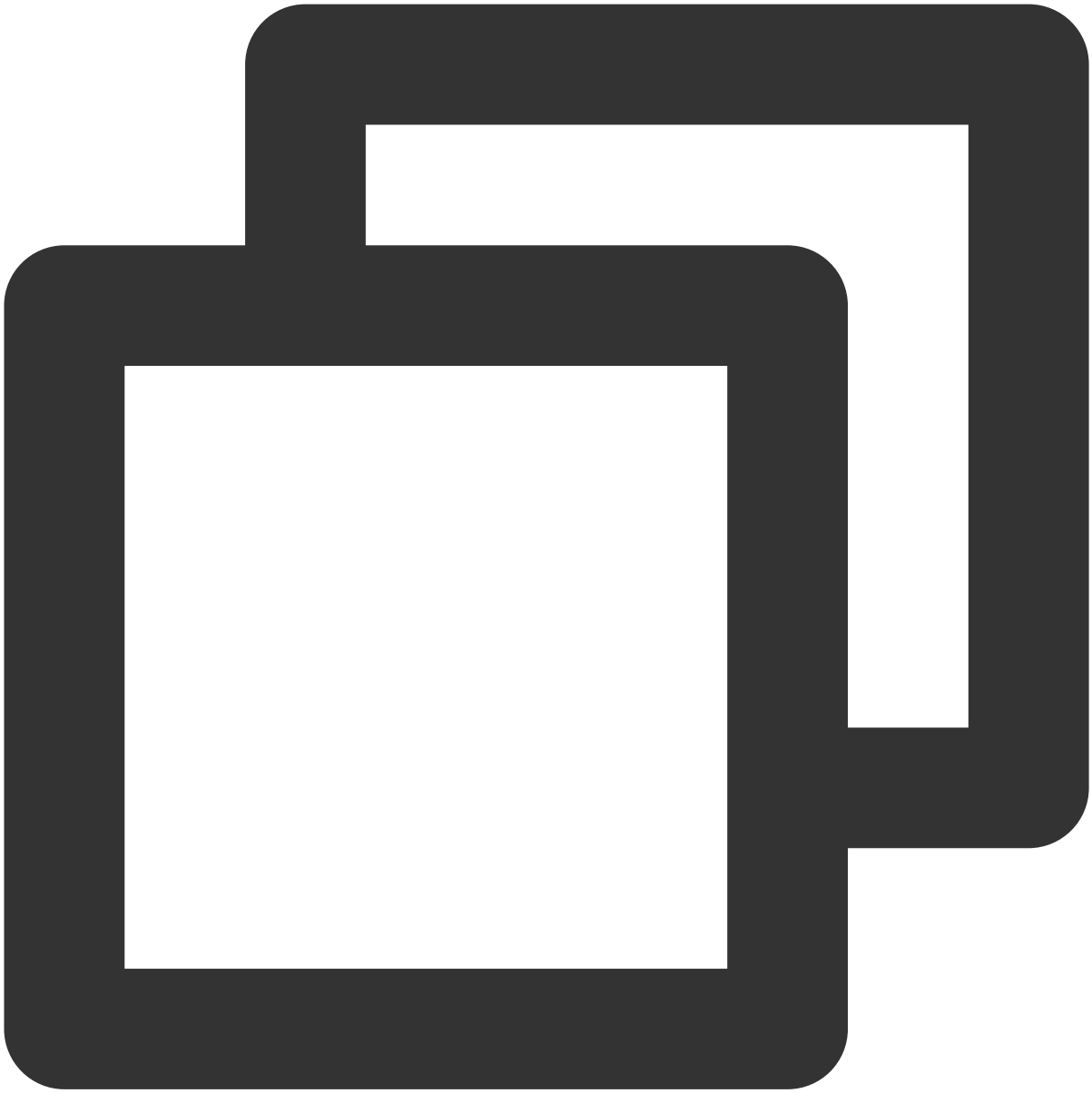
5. サーバーのOSに応じて以下のコマンドを実行し、numaライブラリをインストールします。

CentOS

Ubuntu

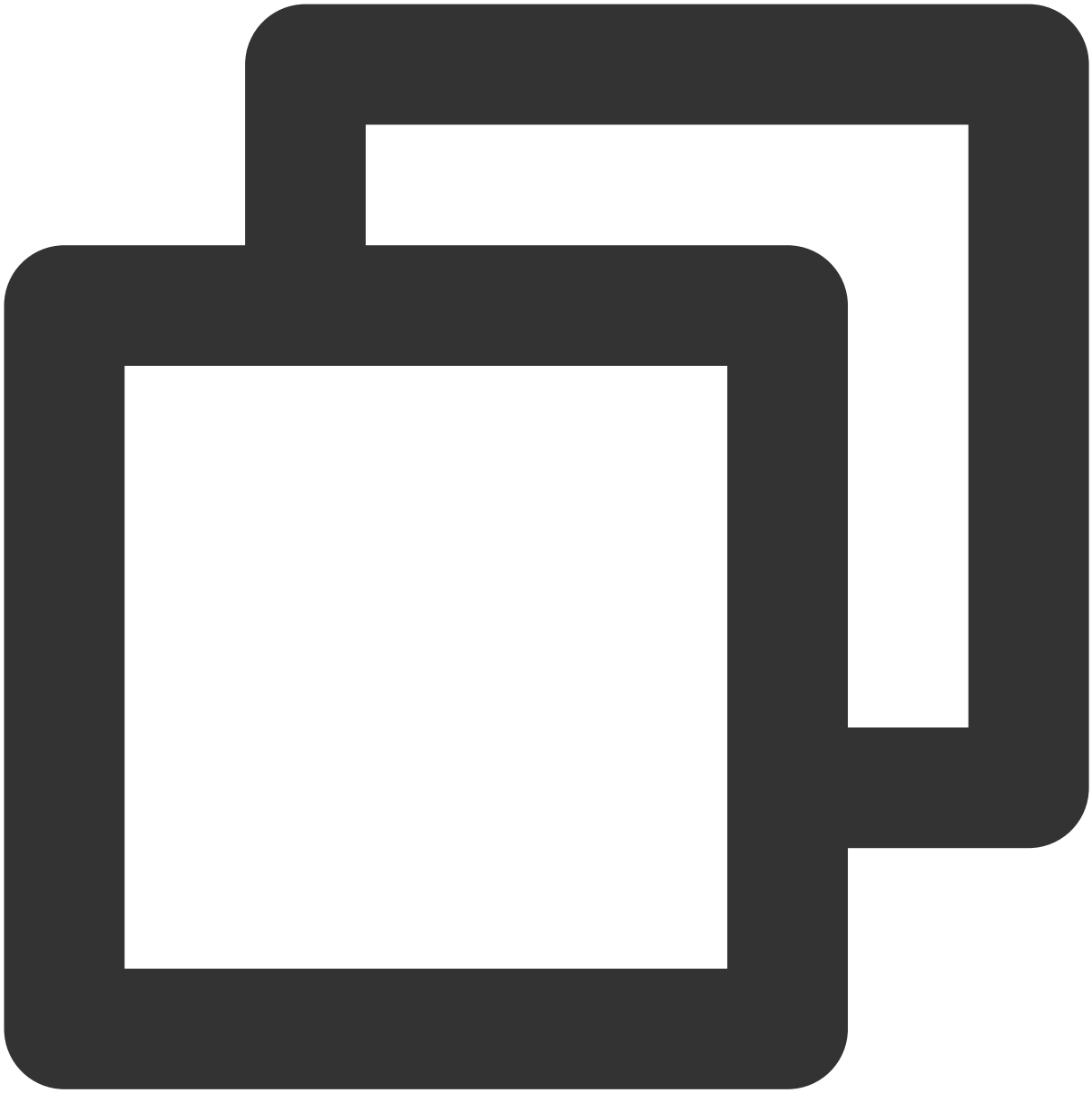


```
yum install numactl-devel
```



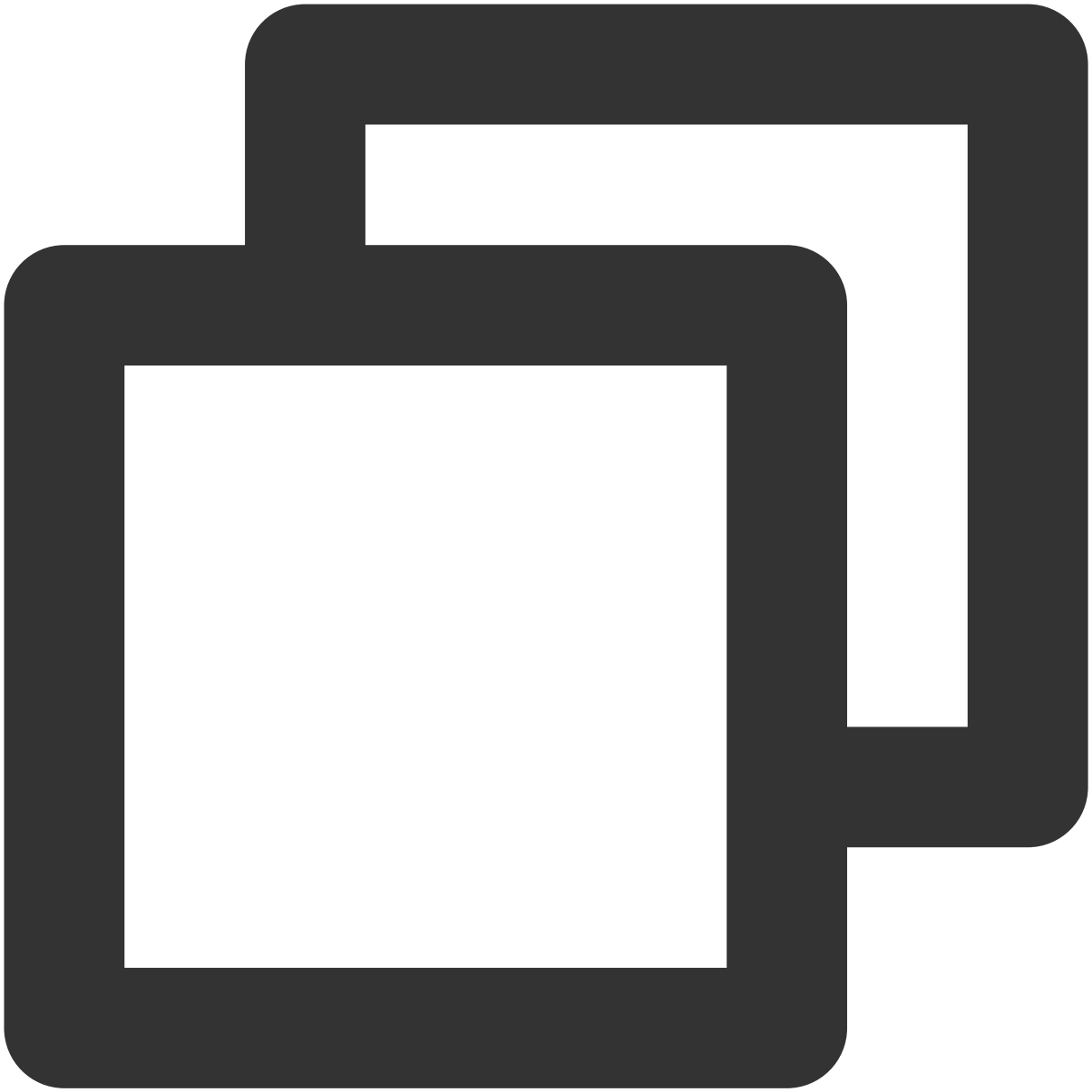
```
apt-get install libnuma-dev
```

6. `dpdk/` ディレクトリで以下のコマンドを実行し、KNIを無効化します。

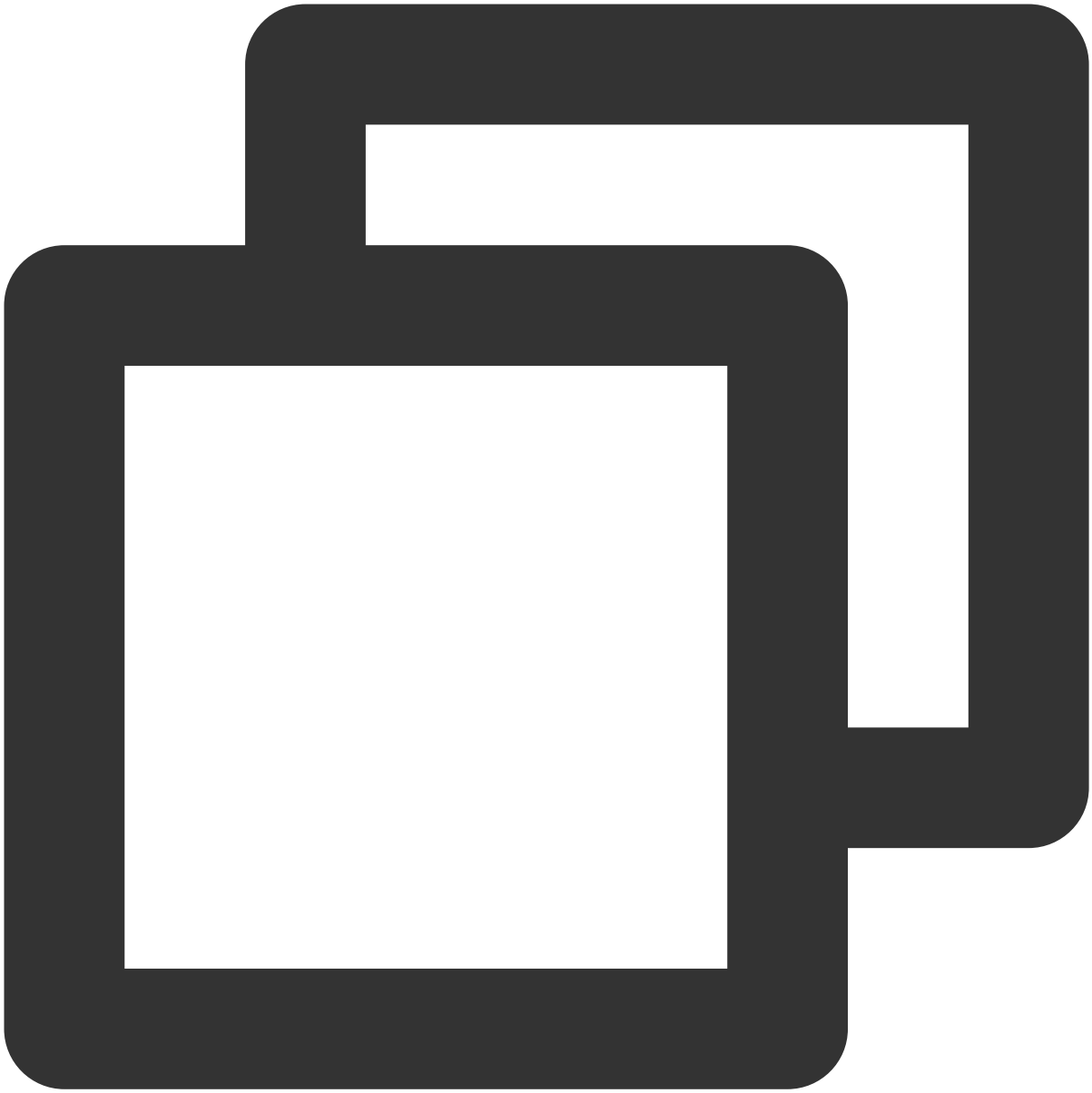


```
sed -i  "s/\\(^CONFIG_.*KNI.*\\)=y/\\1=n/g" ./config/*
```

7. OS が新しいカーネルバージョン (5.3 など) を使用している場合は、次のコマンドを実行して差異をシールドしてください。

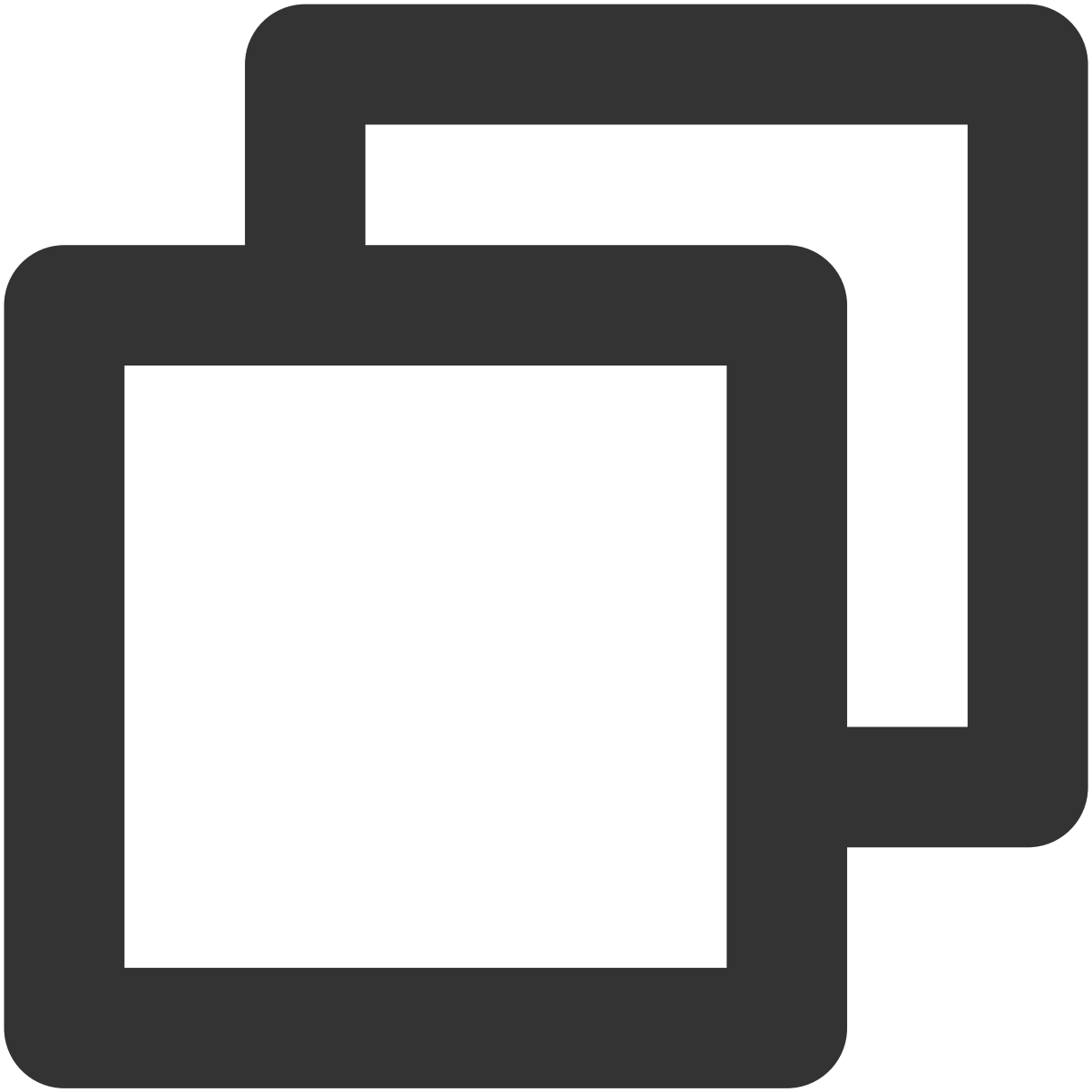


```
sed -i "s/\\(^WERROR_FLAGS += -Wundef -Wwrite-strings$\\)/\\1 -Wno-address-of-packe
```

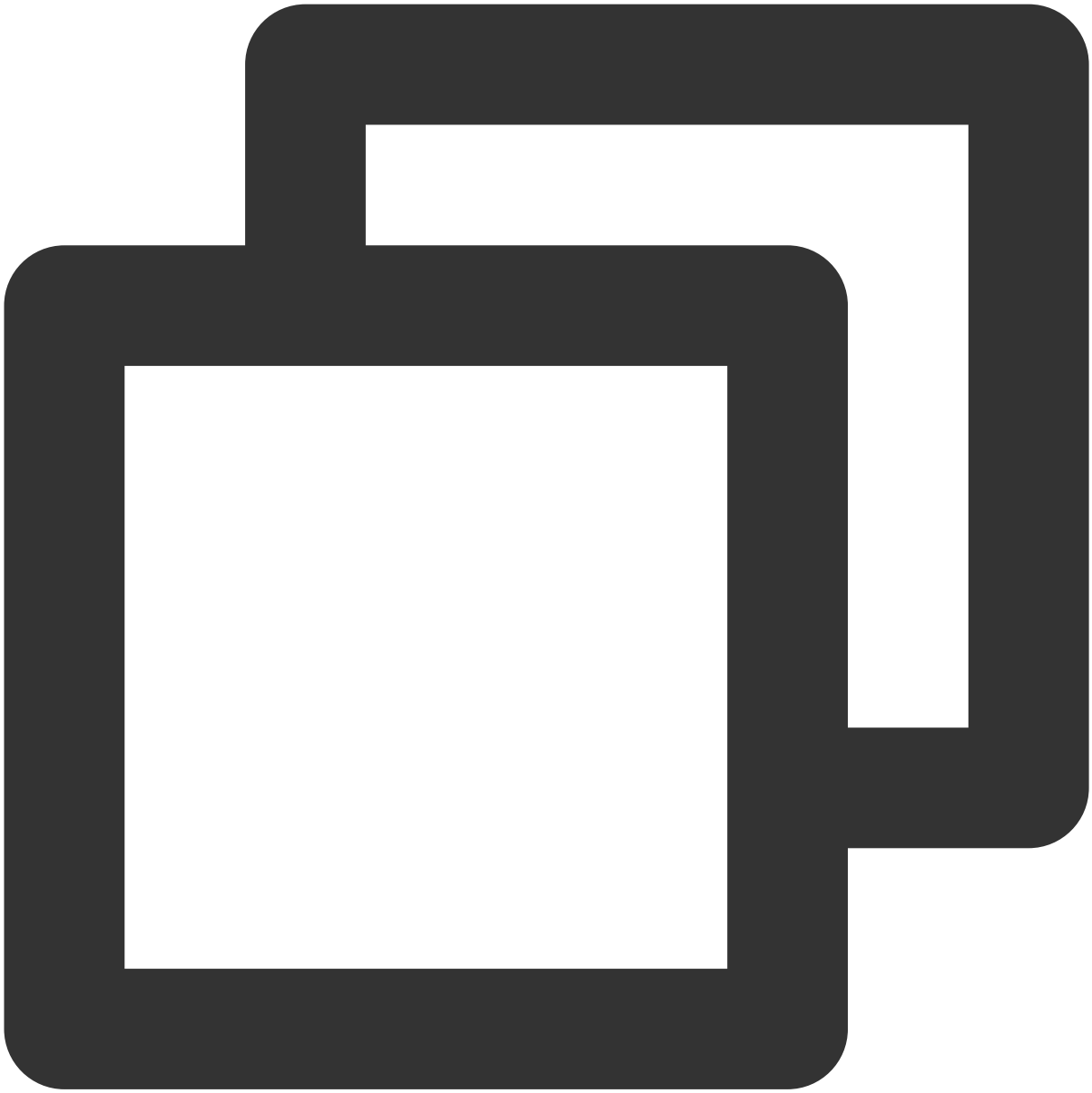


```
sed -i "s/fall back/falls through -/g" ./lib/librte_eal/linuxapp/igb_uio/igb_uio.c
```

8. 以下のコマンドを実行し、DPDKをコンパイルします。



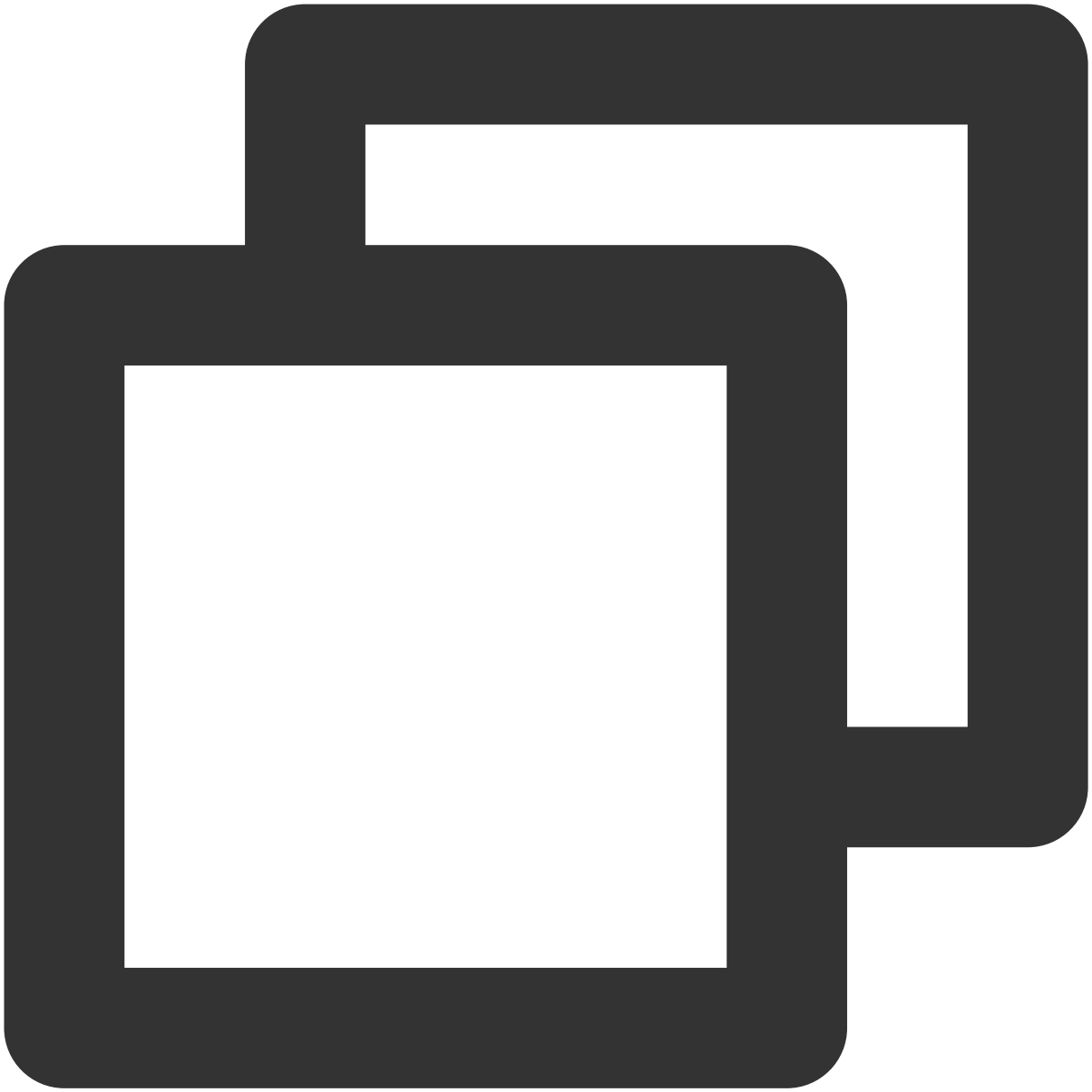
```
make defconfig
```



```
make -j
```

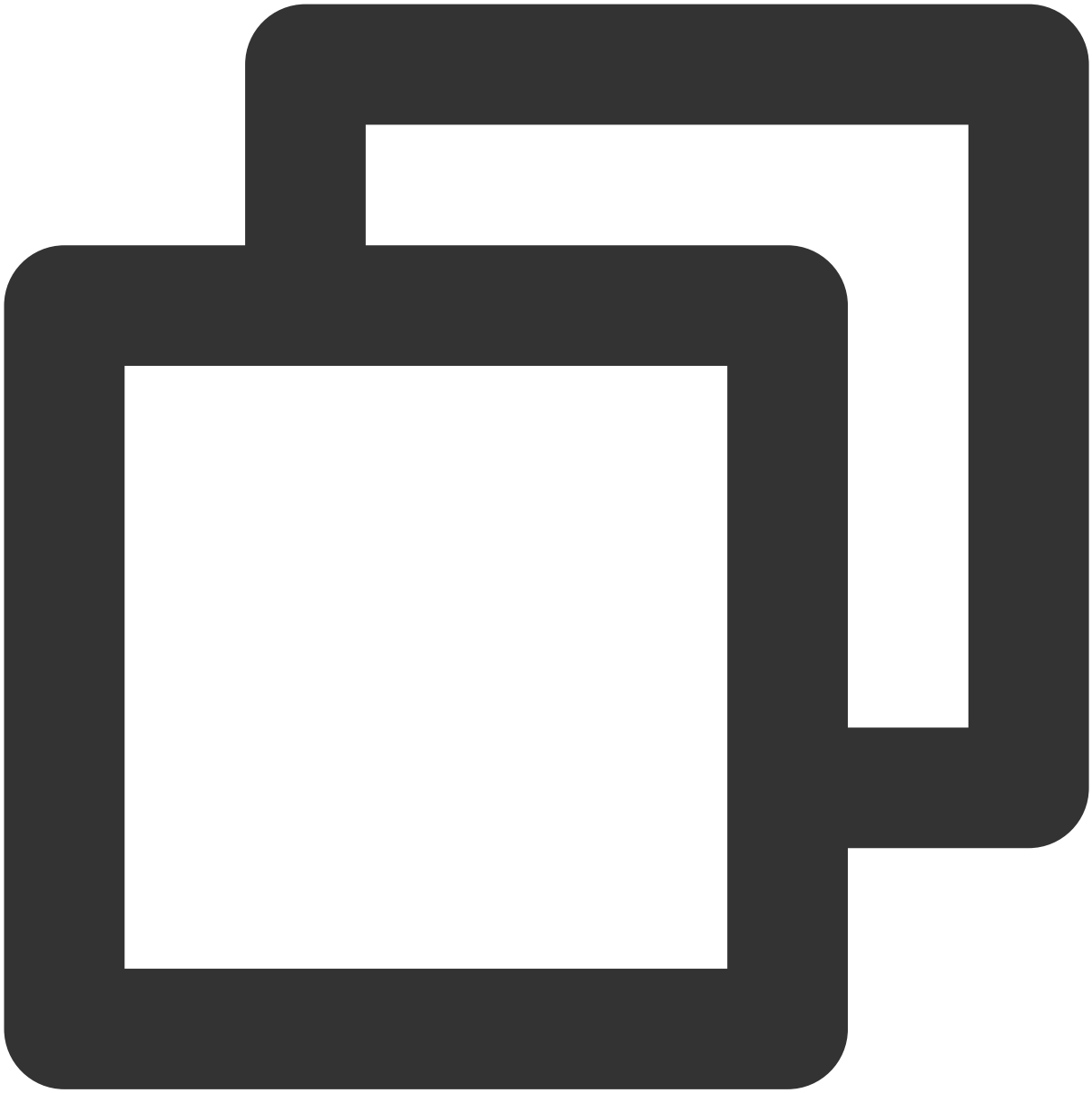
ラージページメモリの構成

以下のコマンドを実行し、ラージページメモリを構成します。



```
echo 4096 > /sys/kernel/mm/hugepages/hugepages-2048kB/nr_hugepages
```

エラー情報が表示された場合は、ラージページメモリが不足していることを表します。次の例のように、コマンド構成の調整が可能です。



```
echo 2048 > /sys/kernel/mm/hugepages/hugepages-2048kB/nr_hugepages
```

カーネルモジュールのロードおよびインターフェースのバインド

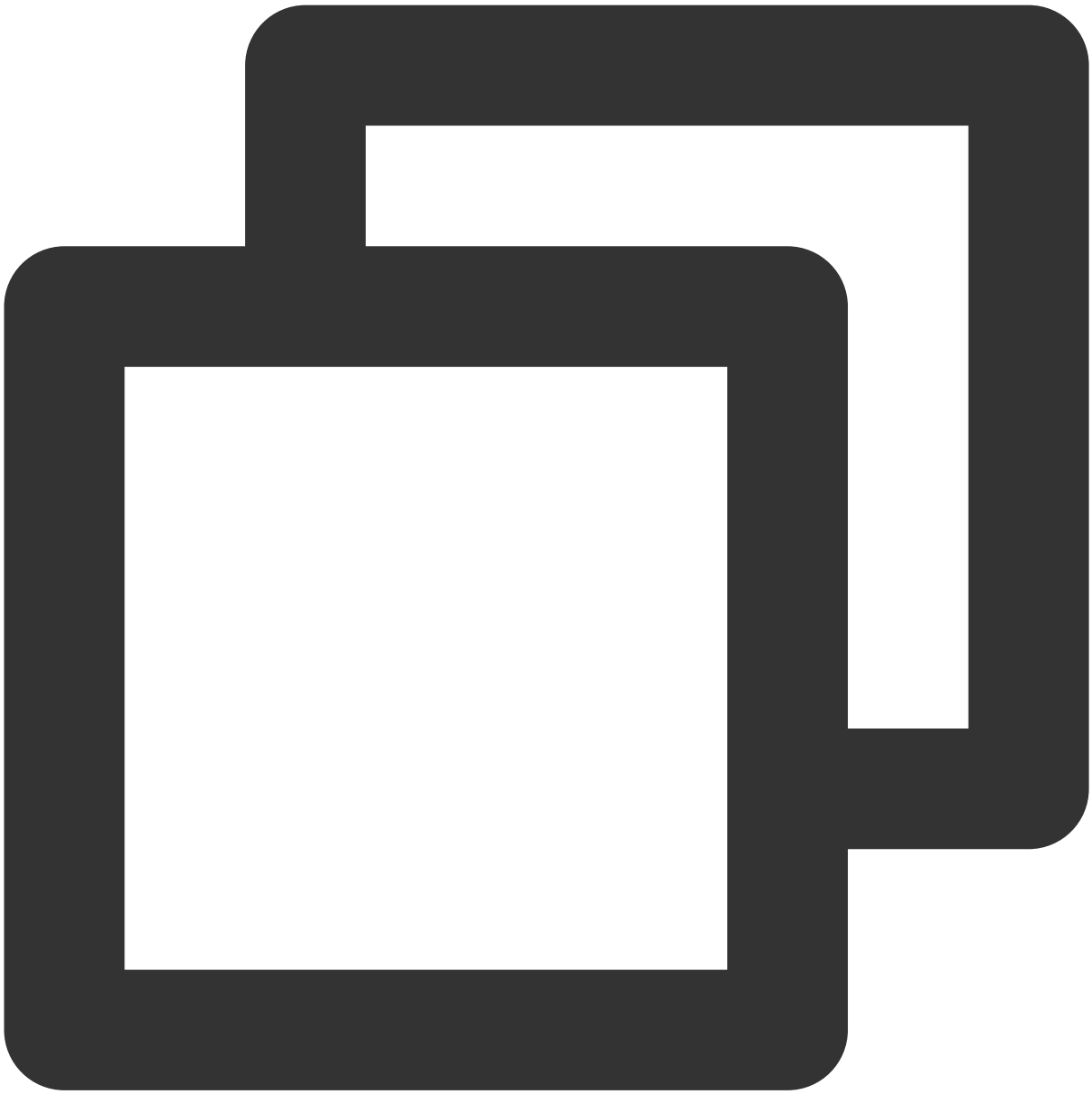
説明：

この手順ではPythonを使用する必要があります。 Python公式サイト にアクセスして、適切なバージョンをダウンロードしてインストールします。ここではPython 3.6.8を例とします。

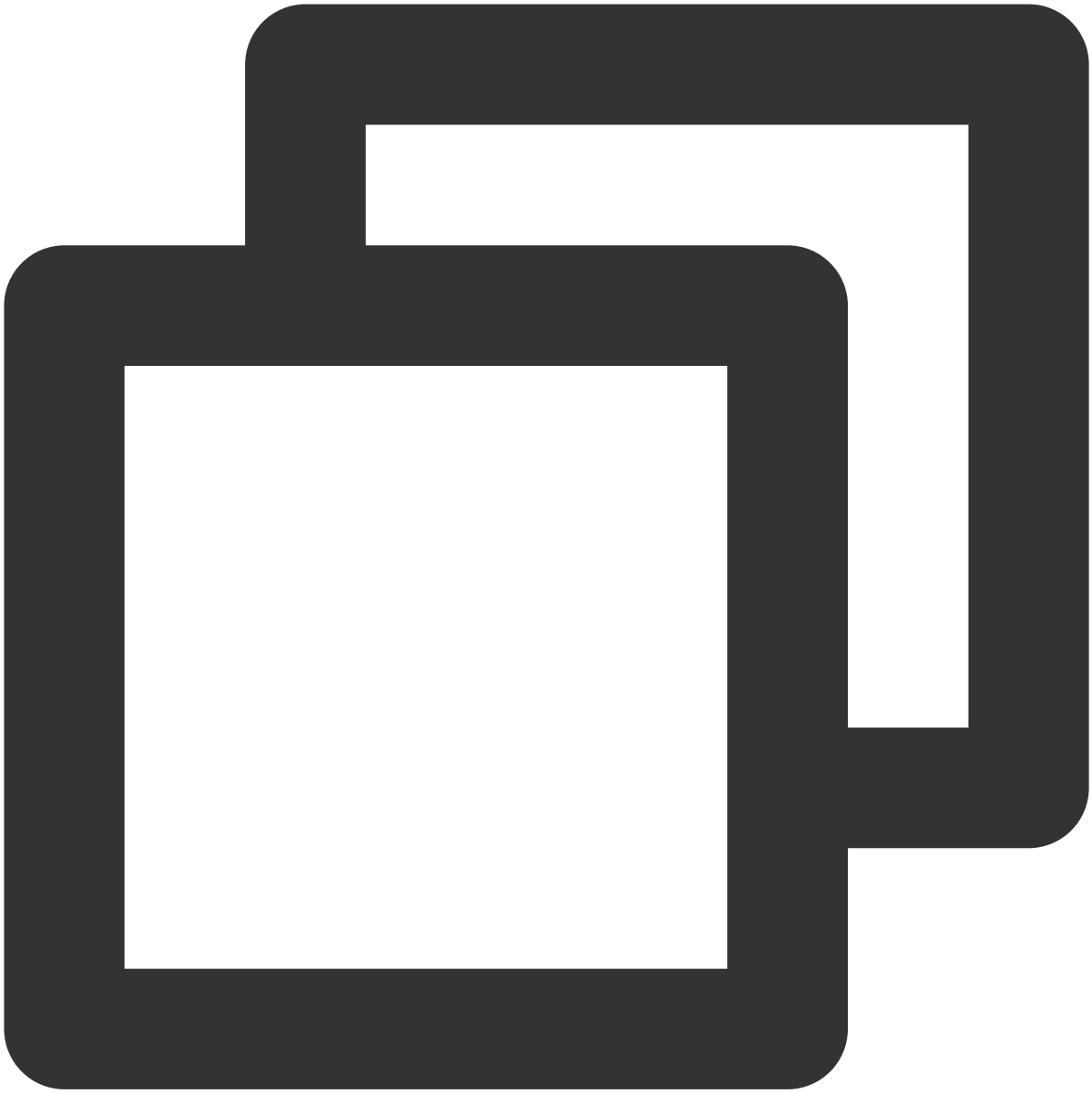
1. VNCを使用してLinuxインスタンスにログイン します。ENIドライバーが igb_uio ユーザー モードドライバーにバインドされた後は、SSH キーまたは IP アドレスではなく、VNC またはコンソール経由でのみ ENI にアクセス

できます。

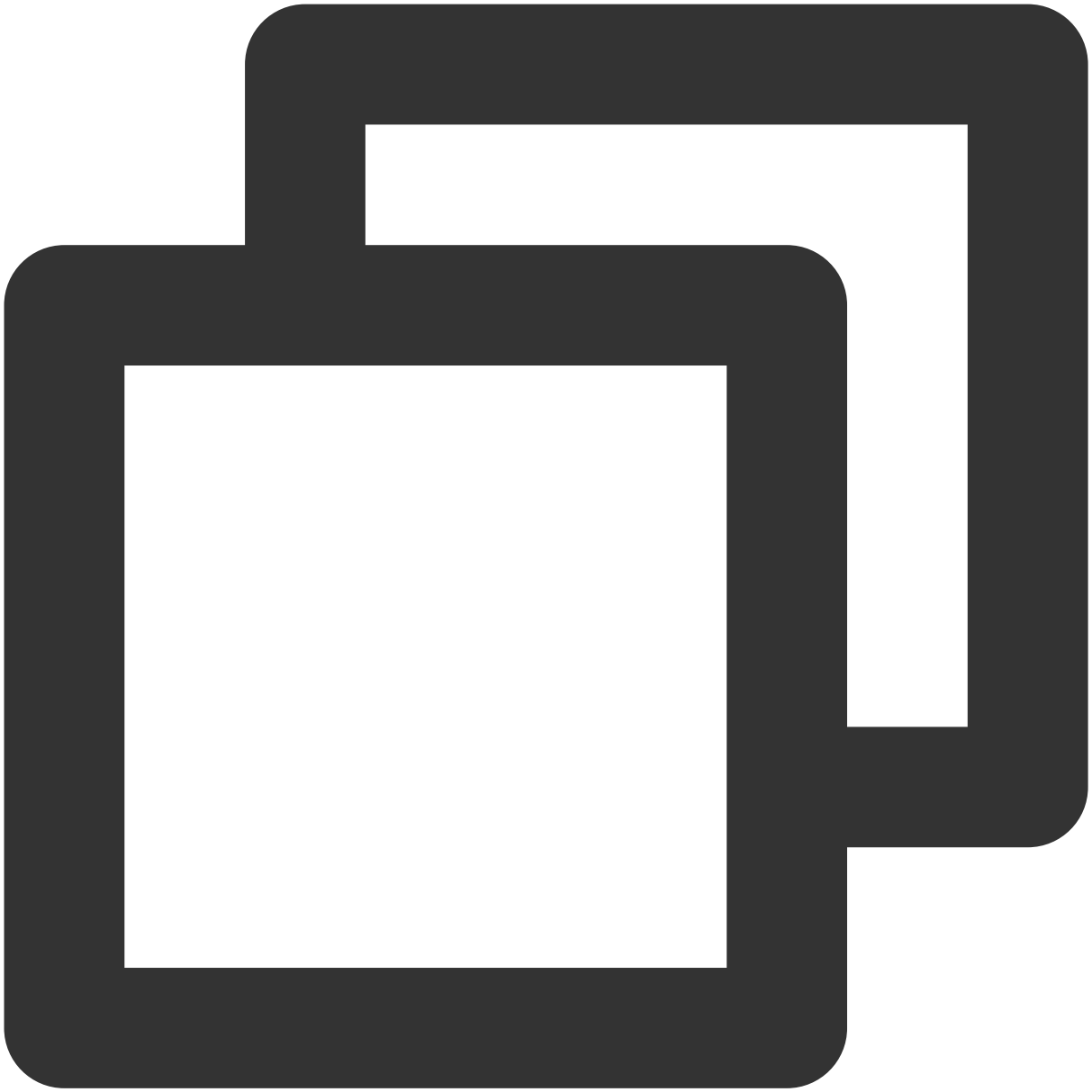
2. 次のコマンドを順に実行し、UIOモジュールをロードし、virtioインターフェイスをバインドします。



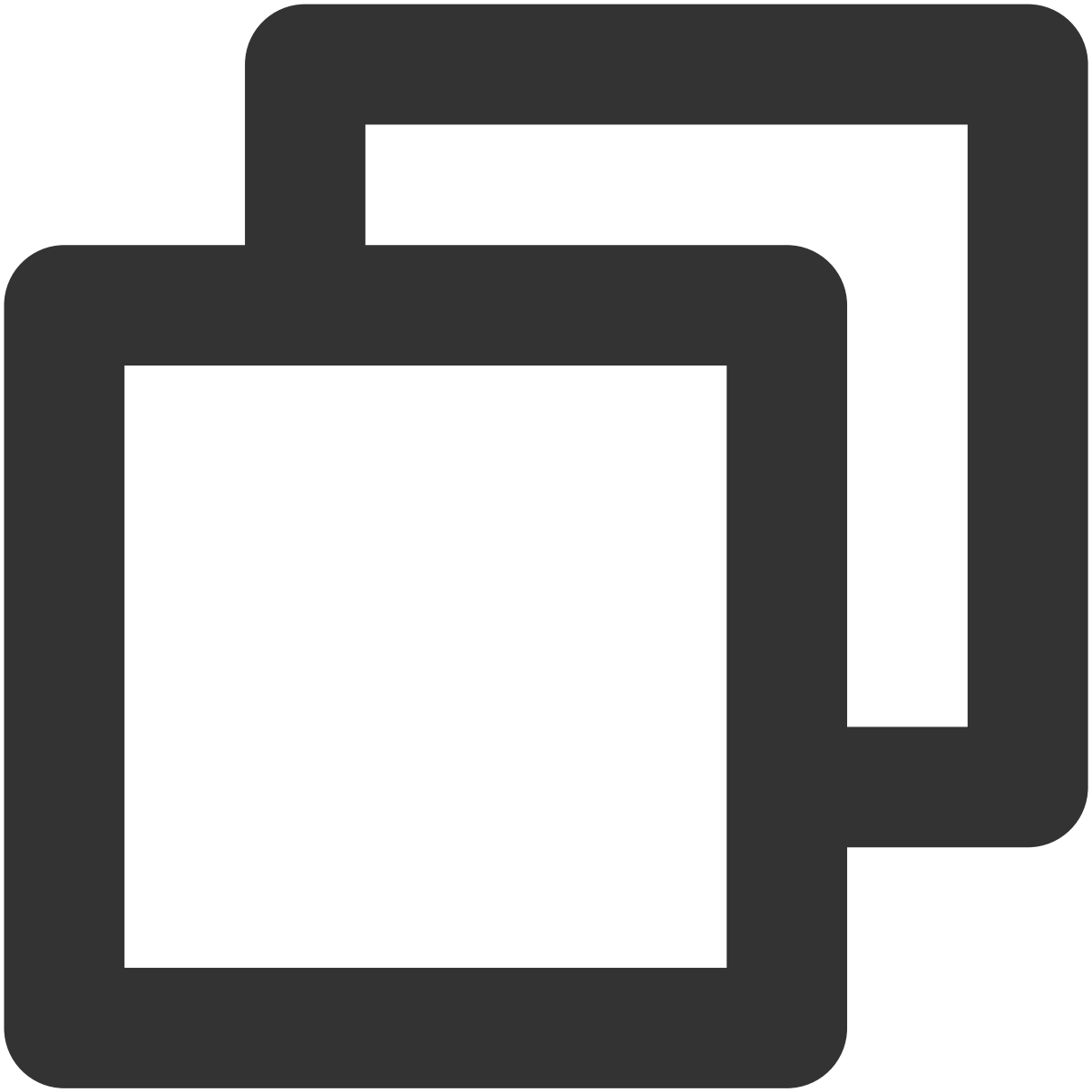
```
ifconfig eth0 0
```



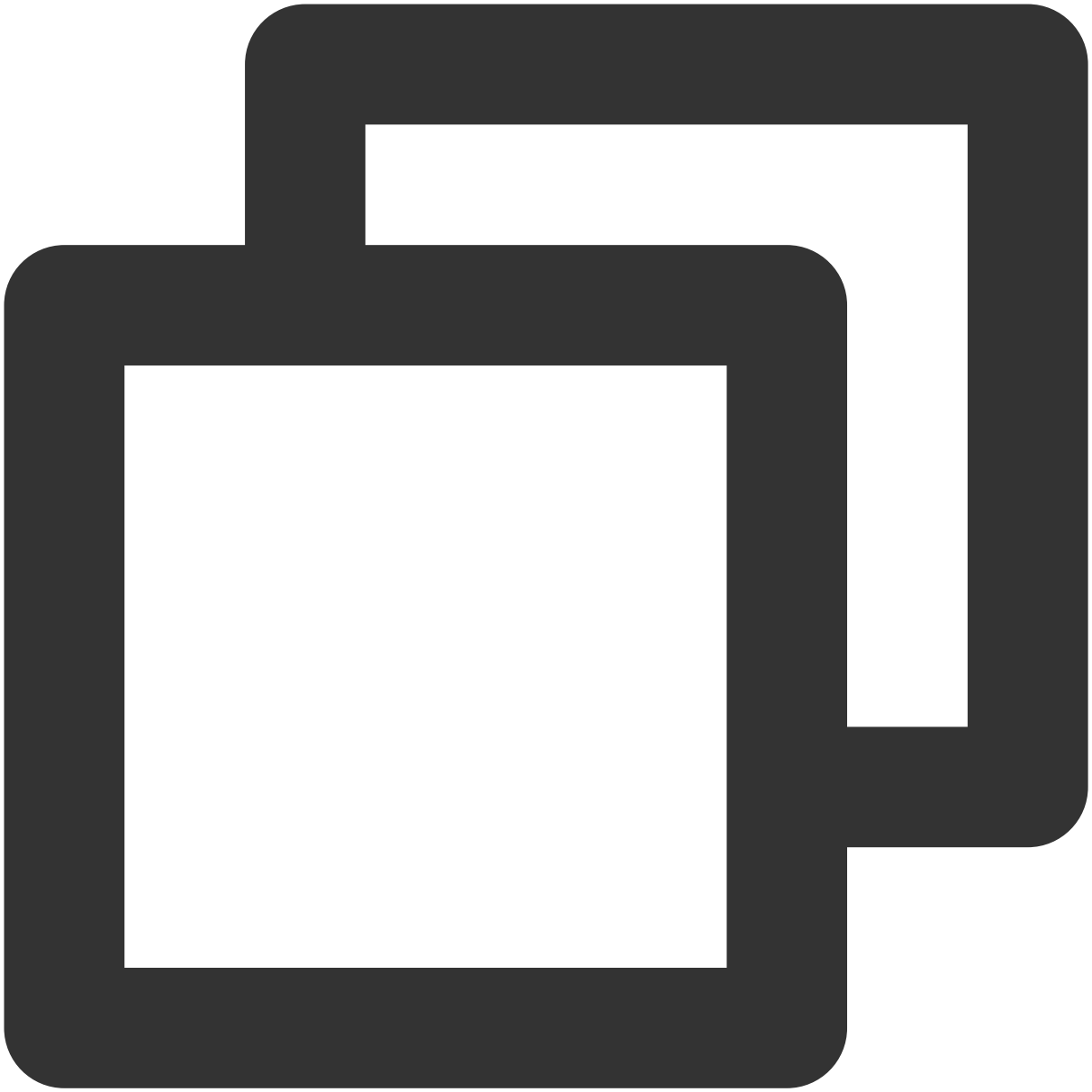
```
ifconfig eth0 down
```



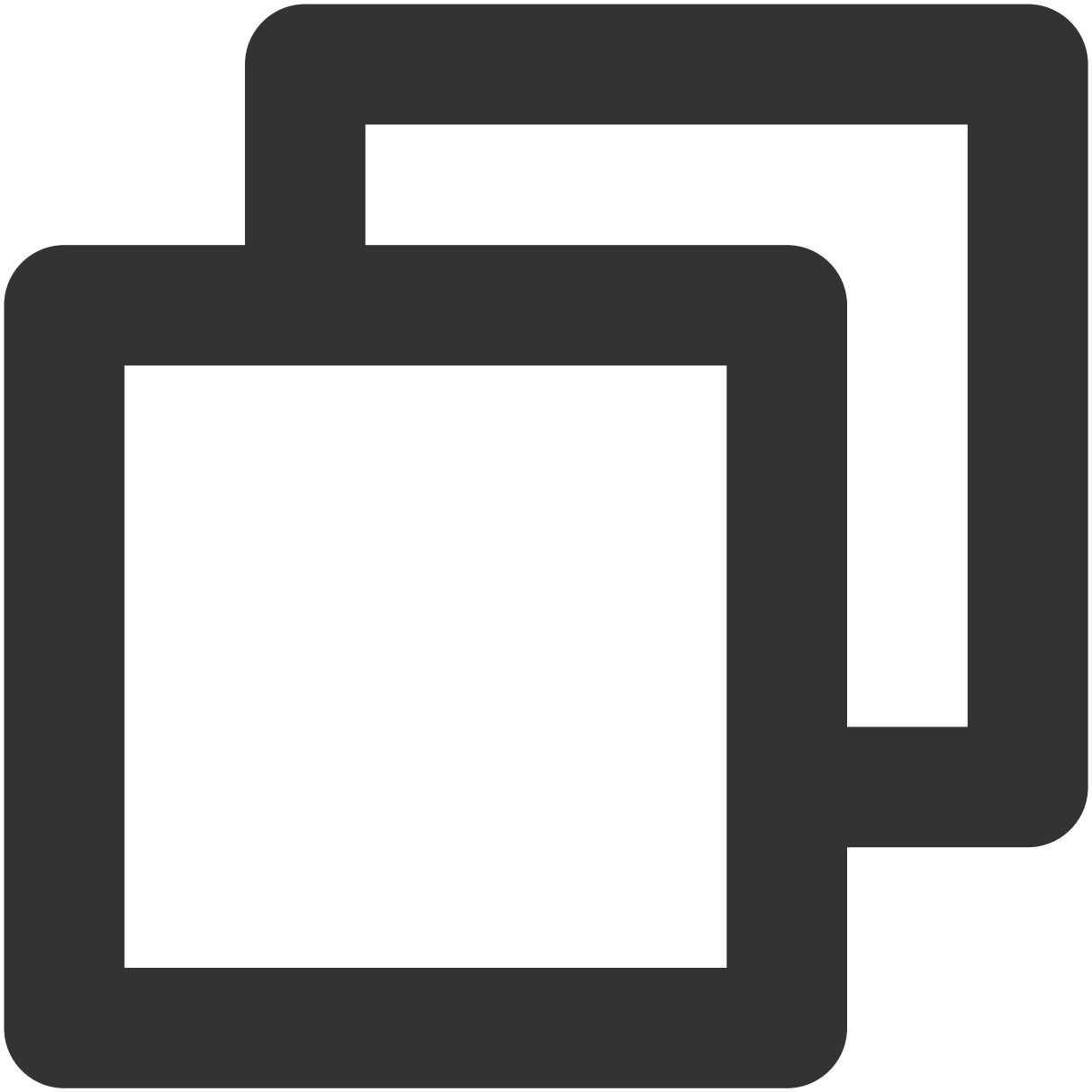
```
modprobe uio
```



```
insmod /root/dpdk/build/kmod/igb_uio.ko
```



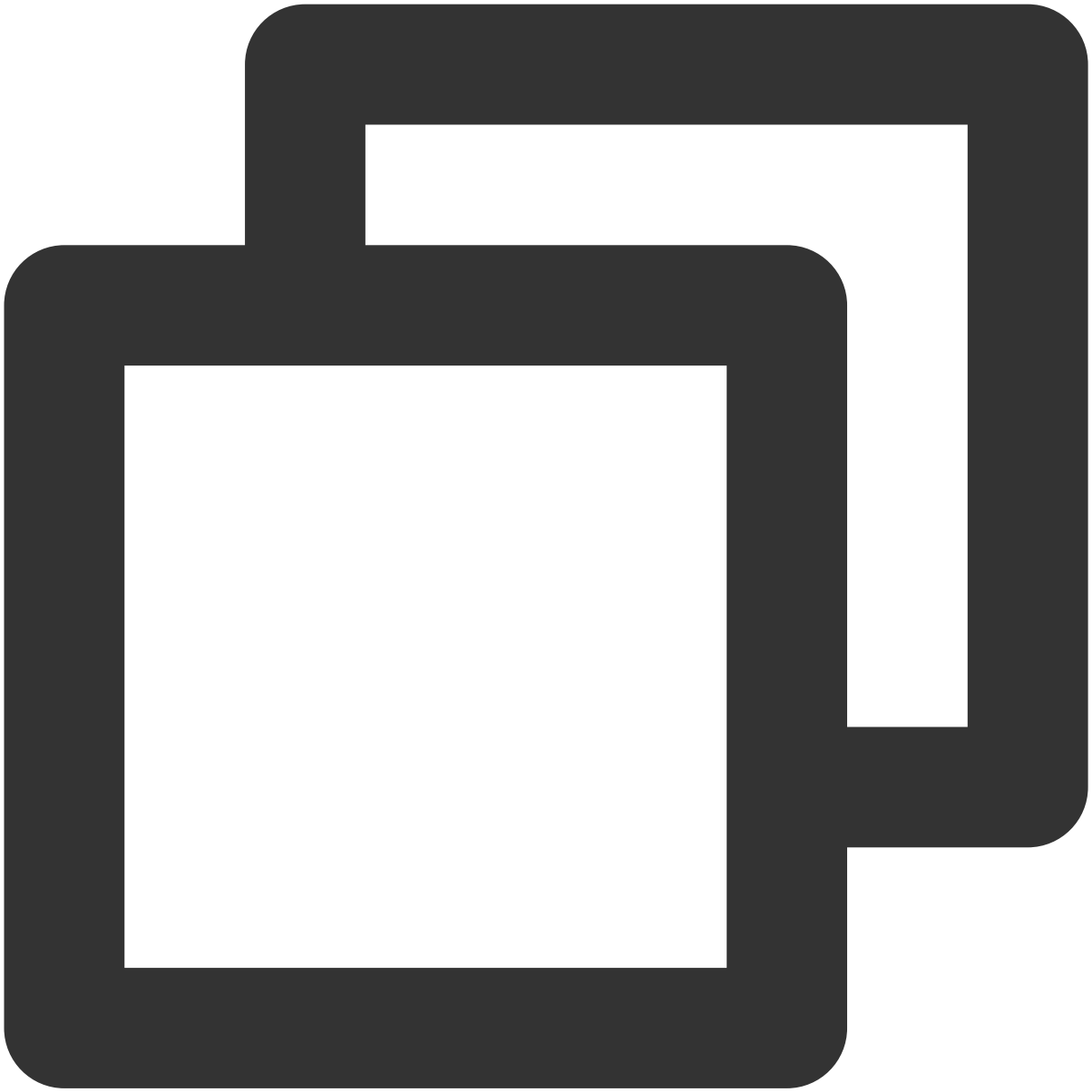
```
cd /root/dpdk/usertools/
```



```
python3 dpdk-devbind.py --bind=igb_uio 00:05.0
```

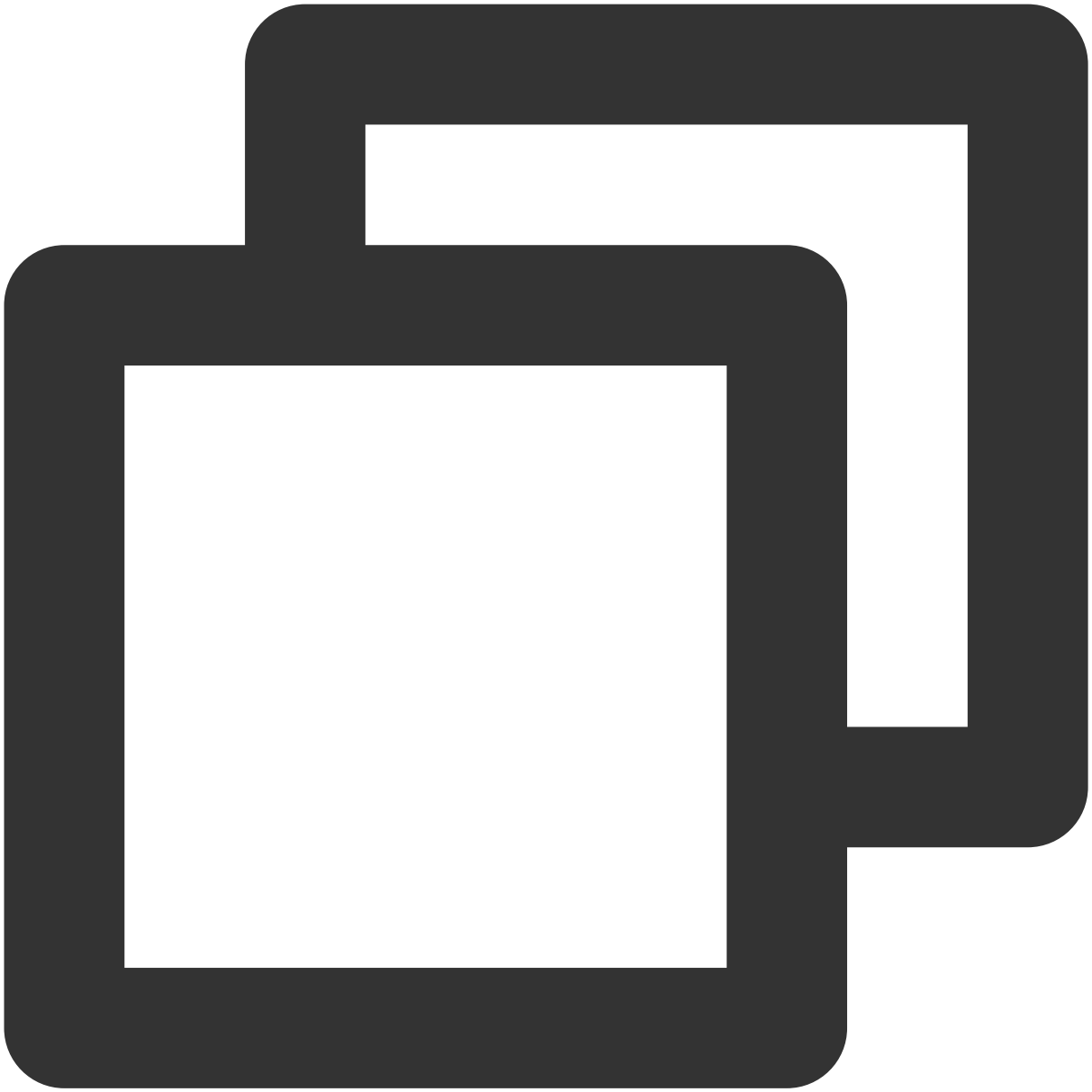
説明：

コマンドの中の00.05.0はサンプルアドレスです。以下のコマンドを実行し、ENIの実際のアドレスを取得してください。

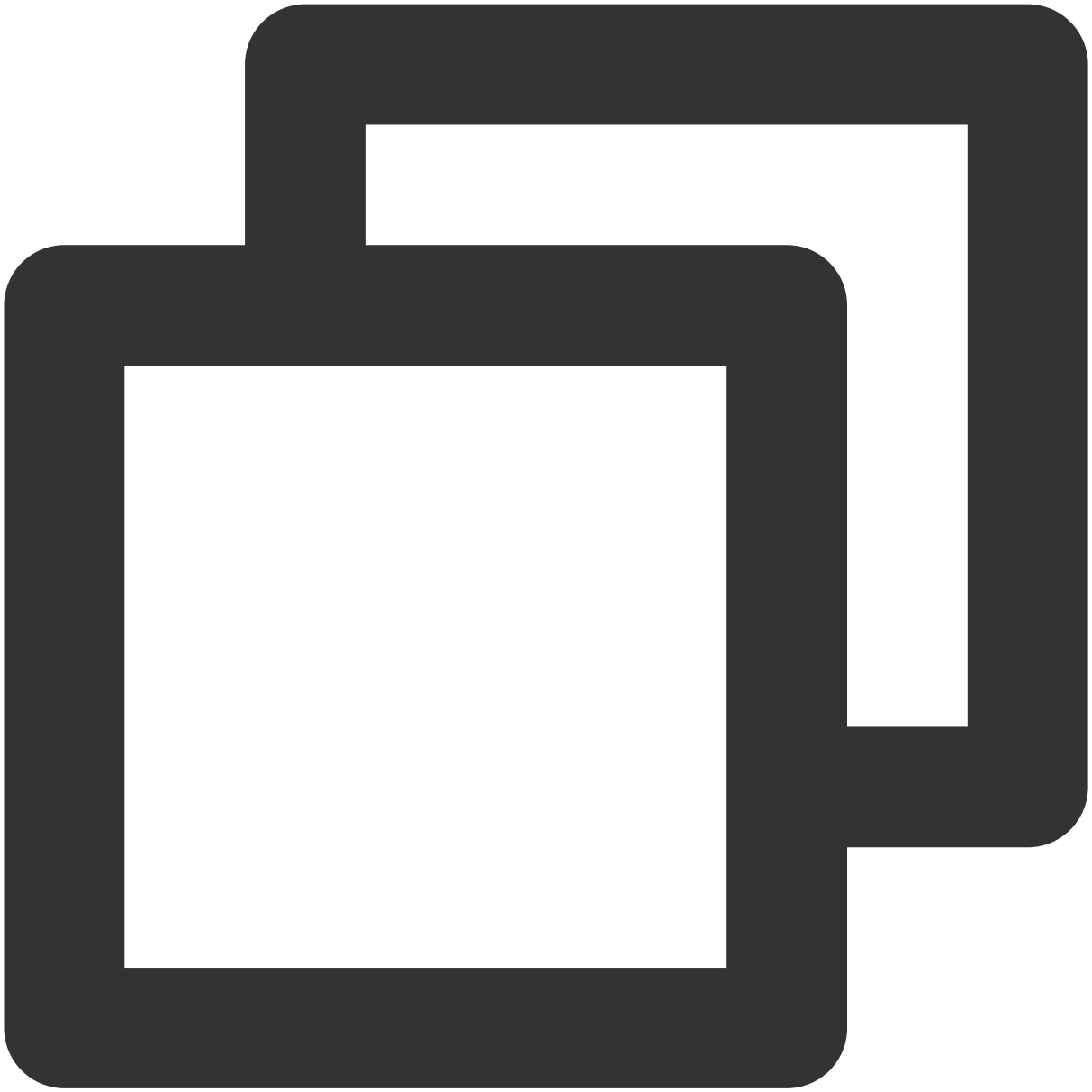


```
python3 dpdk-devbind.py -s
```

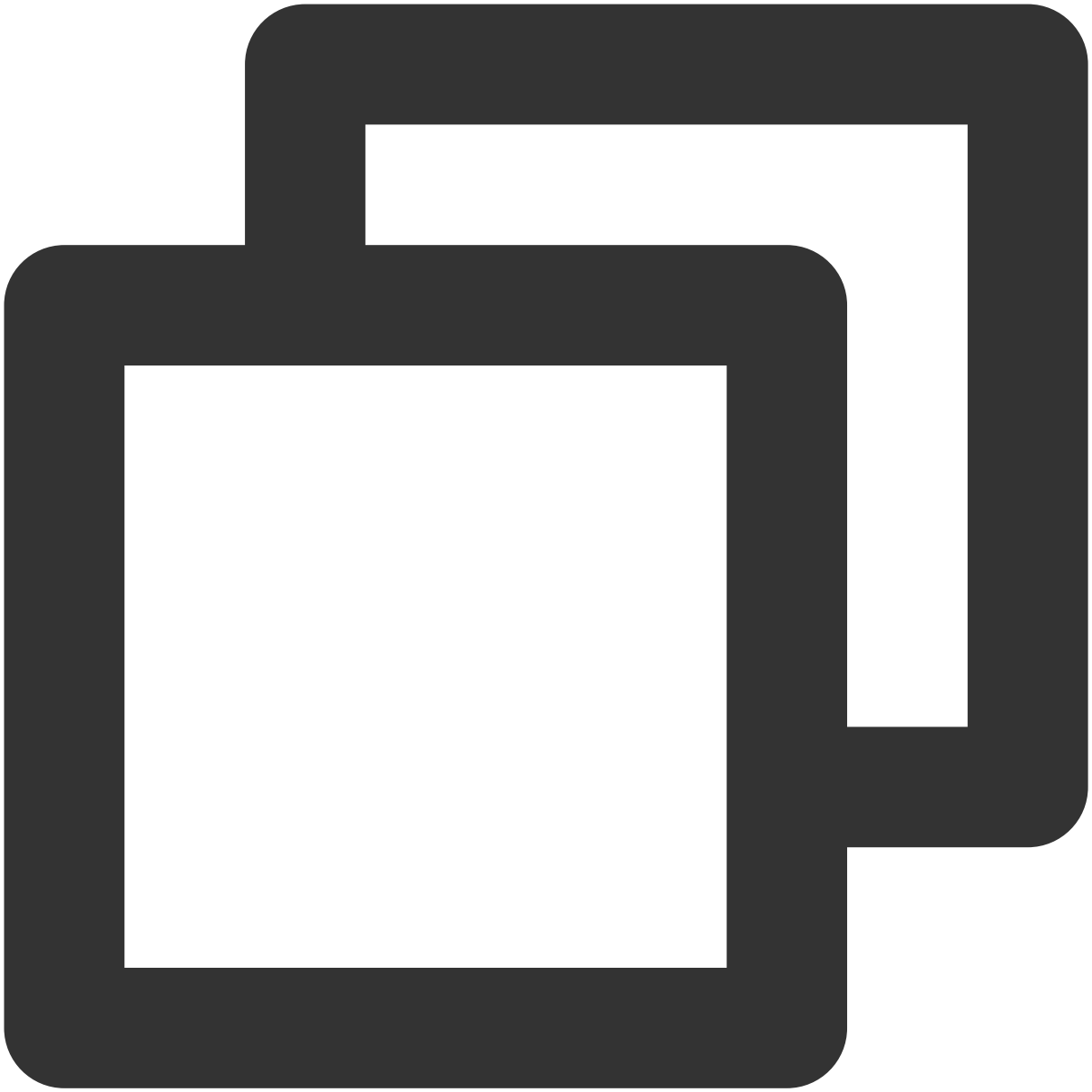
テストが完了したら、次のコマンドを実行してENIを復元します。



```
cd /root/dpdk/usertools/
```



```
python3 dpdk-devbind.py --bind=virtio-pci 00:05.0
```



```
ifconfig eth0 up
```

帯域幅とスループットのテスト

説明：

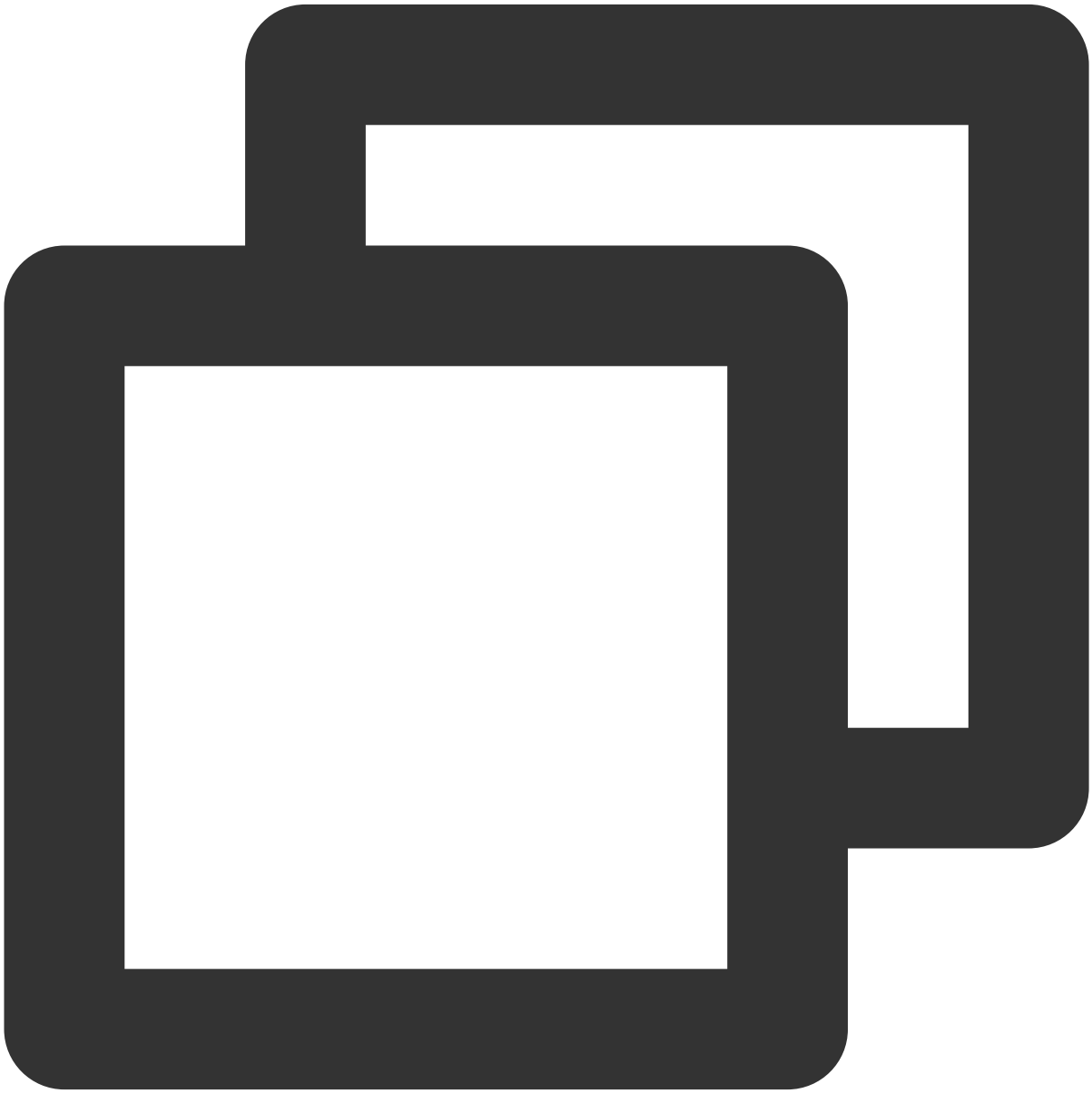
テストコマンドはtxpktsパラメータを使用してパケットのサイズを制御します。テスト帯域幅は1430B、テストppsは64Bをそれぞれ使用します。

この手順で提供されるコマンドパラメータは CentOS 8.2に適用されます。その他のシステムイメージバージョンを使用する場合は、実際のシーンに応じてパラメータを調整した後、再度テストを行う必要があります。例えば、

CentOS 7.4のカーネルバージョンが3.10の場合、CentOS 8.2 のカーネルバージョン4.18との間に性能差が存在するため、帯域幅テストコマンドの中の `nb-cores` を2に変更することができます。コマンドのパラメータに関するその他の情報については、 testpmd-command-line-options をご参照ください。

1. 次のコマンドを実行して、送信側で testpmdをtxonlyモードで起動し、受信側でrxonlyモードを有効にします。

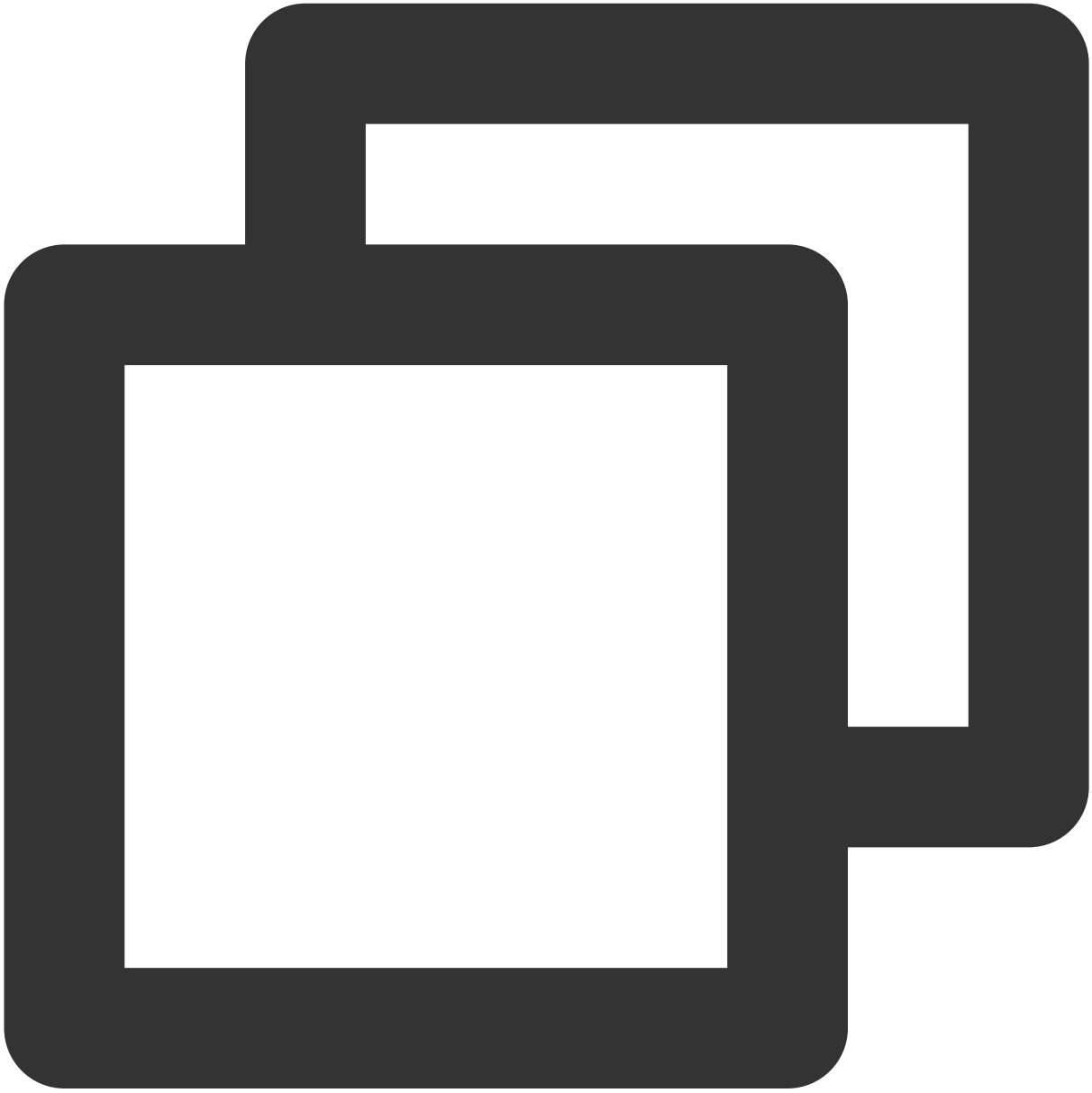
送信側：



```
/root/dpdk/build/app/testpmd  -l 8-191 -w 0000:00:05.0 -- --burst=128 --nb-cores=32
```

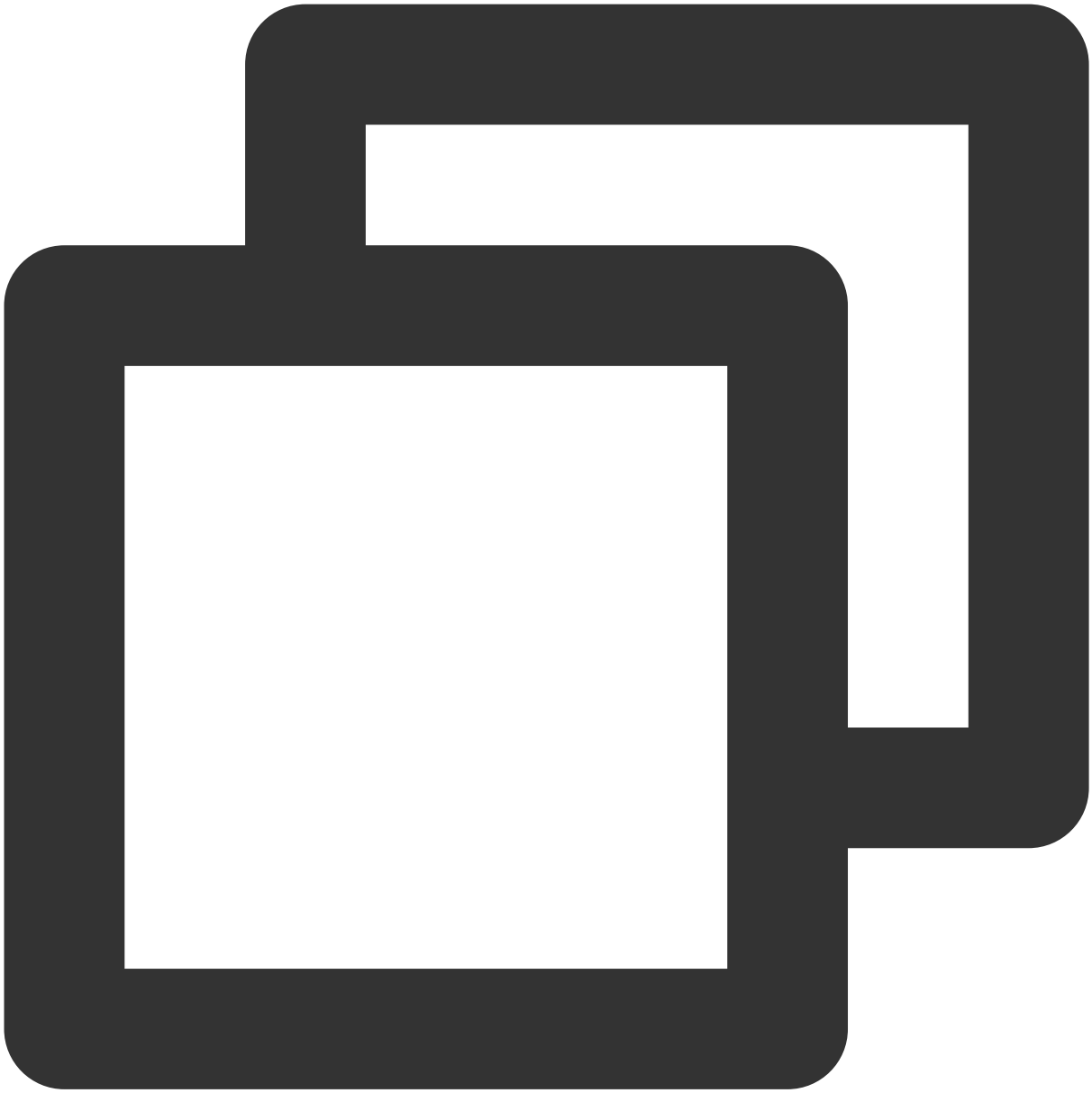
説明：

このうち `-l 8-191 -w 0000:00:05.0` これら 2 つのパラメータはテスト環境の実際の値に置き換える必要があります。
受信側：



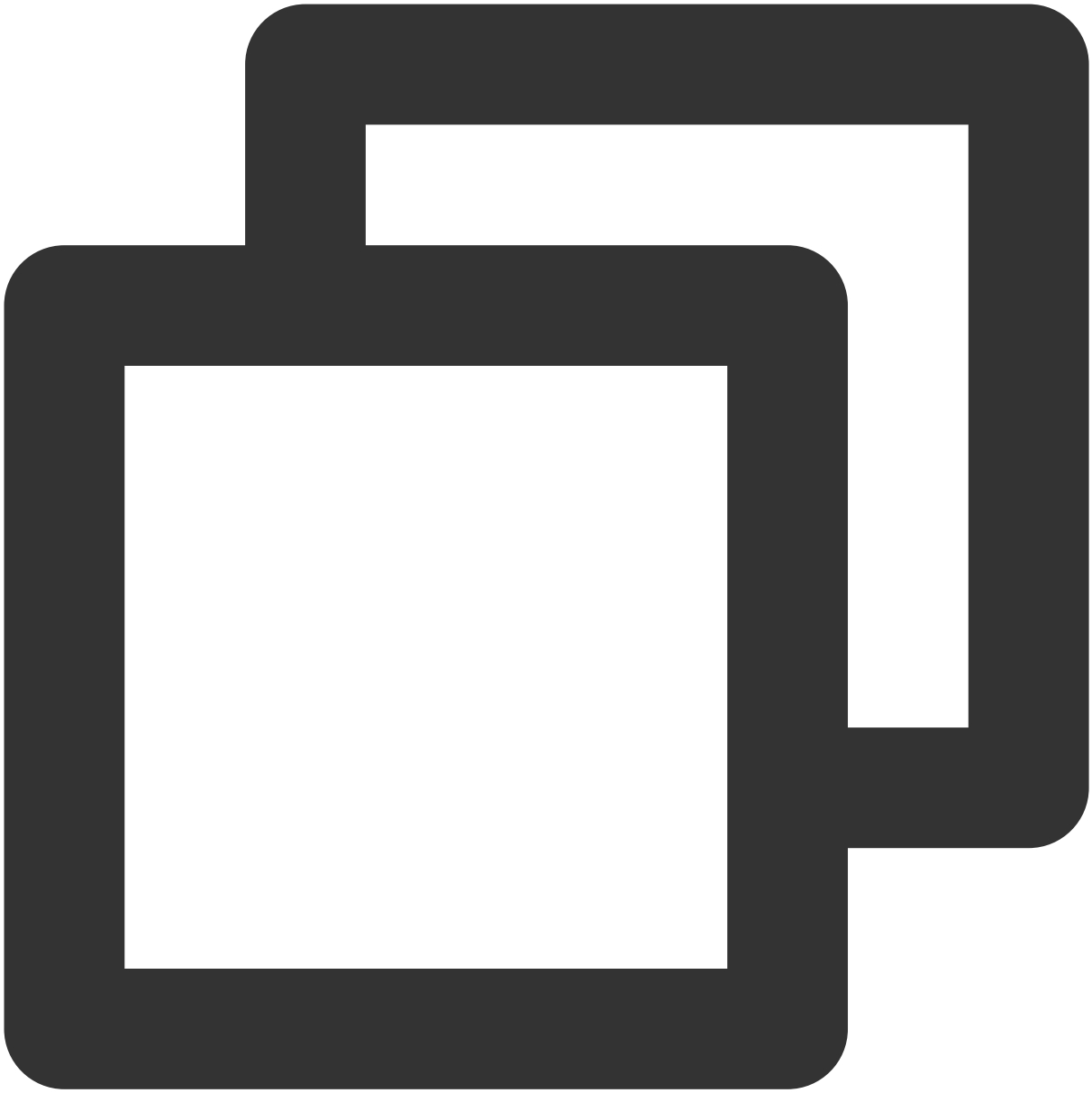
```
/root/dpdk/build/app/testpmd -l 8-191 -w 0000:00:05.0 -- --burst=128 --nb-cores=32
```

2. 次のコマンドを実行し、ppsをテストします(UDP 64B パケット)。
送信側：



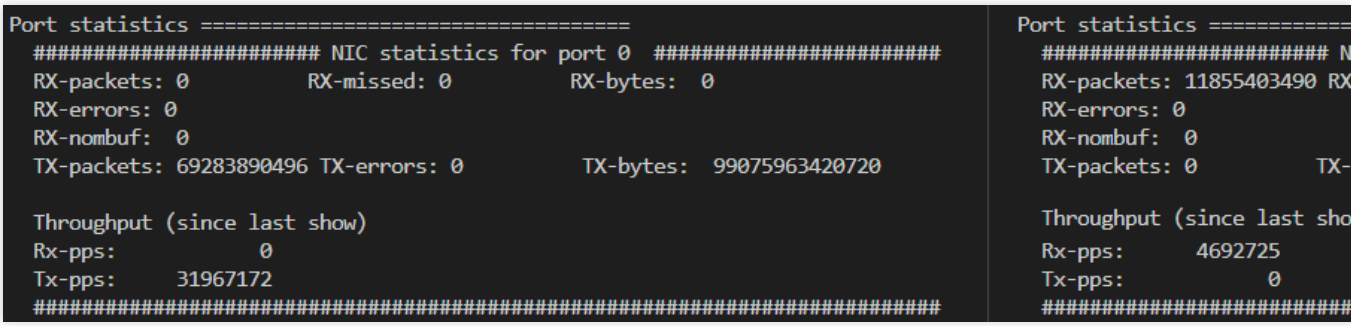
```
/root/dpdk/build/app/testpmd -l 8-191 -w 0000:00:05.0 -- --burst=128 --nb-cores=32
```

受信側：



```
/root/dpdk/build/app/testpmd -l 8-191 -w 0000:00:05.0 -- --burst=128 --nb-cores=32
```

テスト結果は以下のとおりです：



ネットワーク帯域幅の計算

受信側のPPSとテストパケットの長さに基づいて、現在のネットワークの受信帯域幅を計算することができます。公式は次のとおりです。

PPS × packet length × 8bit/B × 10^{-9} = 帯域幅

テストで得られたデータと合わせて、得られた現在の帯域幅は次のとおりです。

4692725pps × 1430B × 8bit/B × 10^{-9} ≈ 53Gbps

説明：

パケット長は1430Bで、14Bイーサネットヘッダー、8B CRC、20B IPヘッダーが含まれます。

テスト結果のRx-ppsは瞬間統計値であり、複数回のテストによって平均値を求めることで、より正確な結果を得ることができます。

LinuxでUSB/IPを使用してUSBデバイスを共有する

最終更新日：：2021-03-26 15:39:38

シナリオ

USB/IP カーネルに統合されたオープンソースのプロジェクトで、Linux環境ではUSB/IPを介してUSBデバイスをリモートで共有できます。このドキュメントでは、次の環境バージョンを例に、USB/IPを使用してUSBデバイスをリモートで共有する方法をデモします。
USB Client：CentOS 7.6 OSのCVM
USB Server：Debian OSのローカルコンピュータ

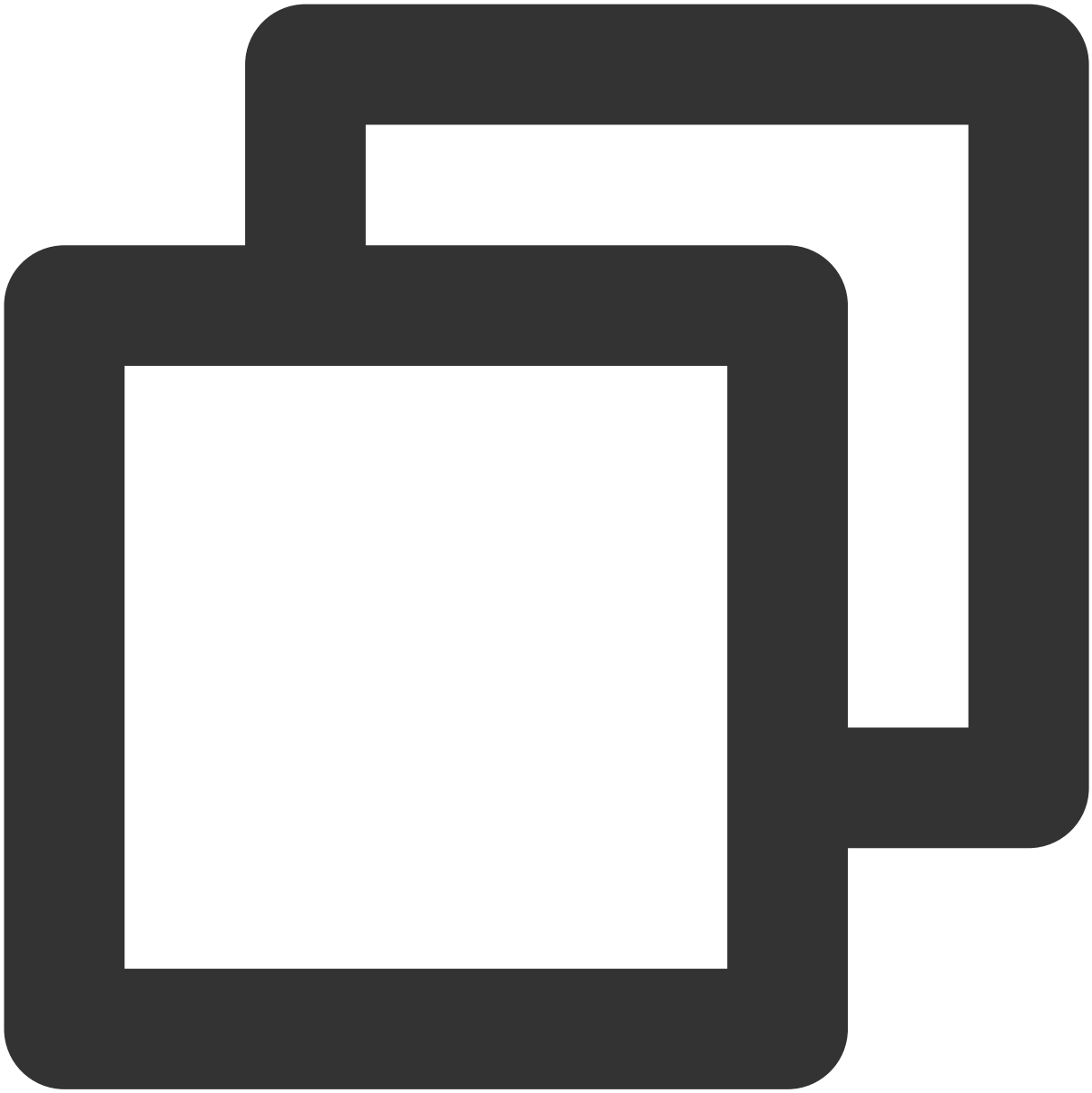
注意事項

USB/IPのインストール方法とカーネルモジュール名は、Linux OSのディストリビューションによって異なります。現在のLinux OSがUSB/IP機能をサポートしているかどうかを確認してください。

操作手順

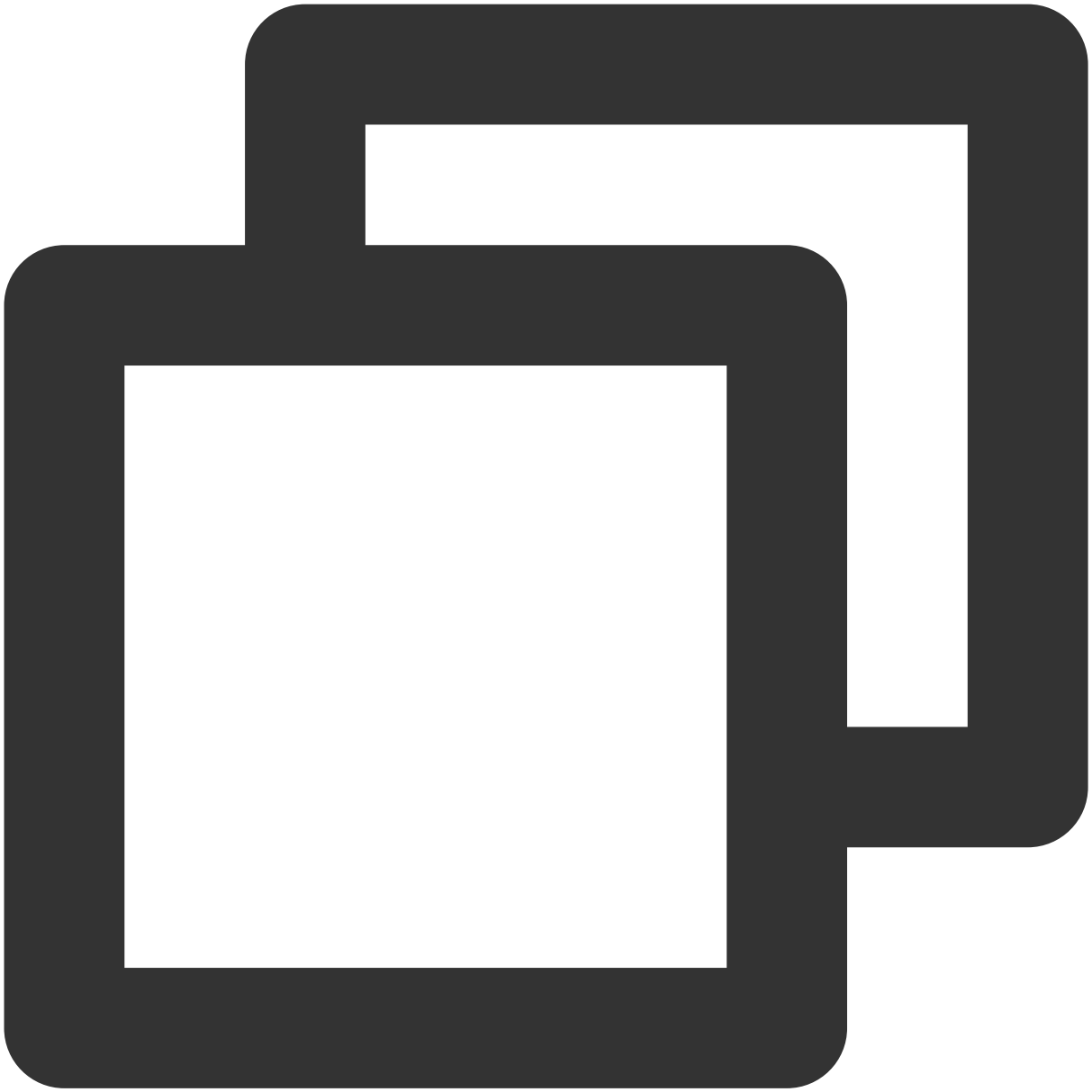
USB Serverを設定する

1. ローカルPCで次のコマンドを順に実行して、USB/IPをインストールし、関連するカーネルモジュールをロードします。



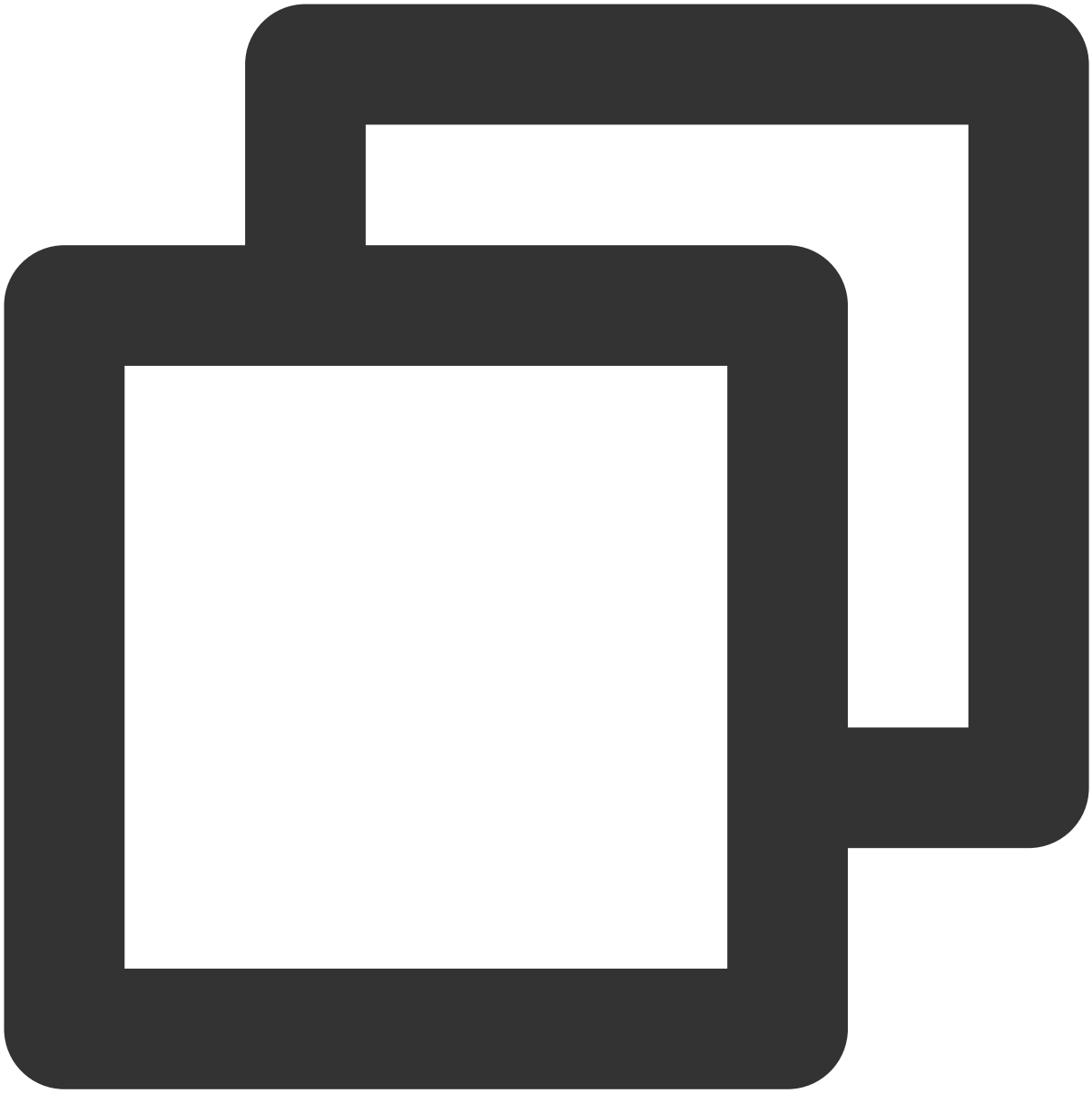
```
sudo apt-get install usbip
sudo modprobe usbip-core
sudo modprobe vhci-hcd
sudo modprobe usbip_host
```

2. USBデバイスを挿入し、次のコマンドを実行して、利用可能なUSBデバイスを確認します。



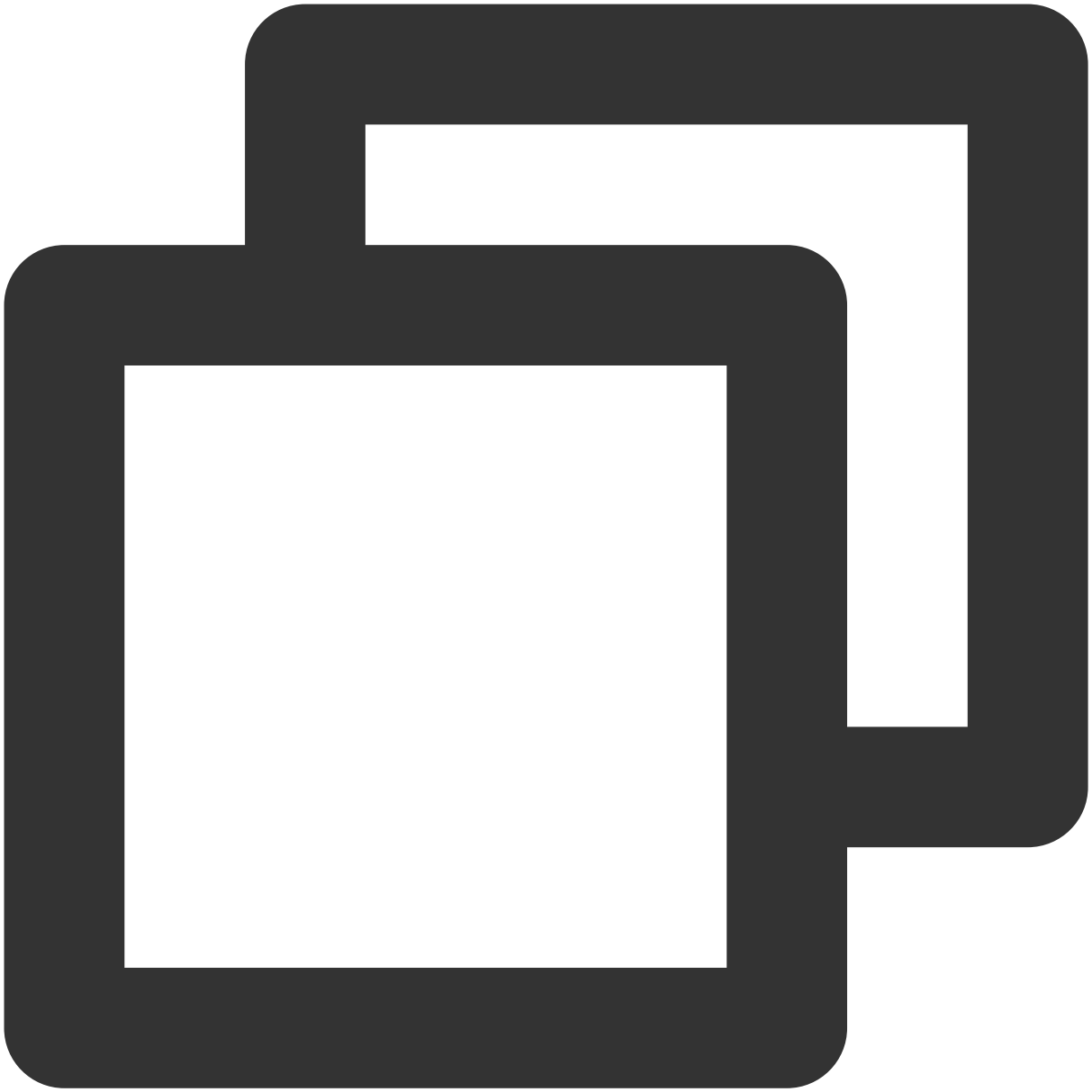
```
usbip list --local
```

たとえば、Feitian USBキーがローカルPCに挿入されると、次の結果が返されます。



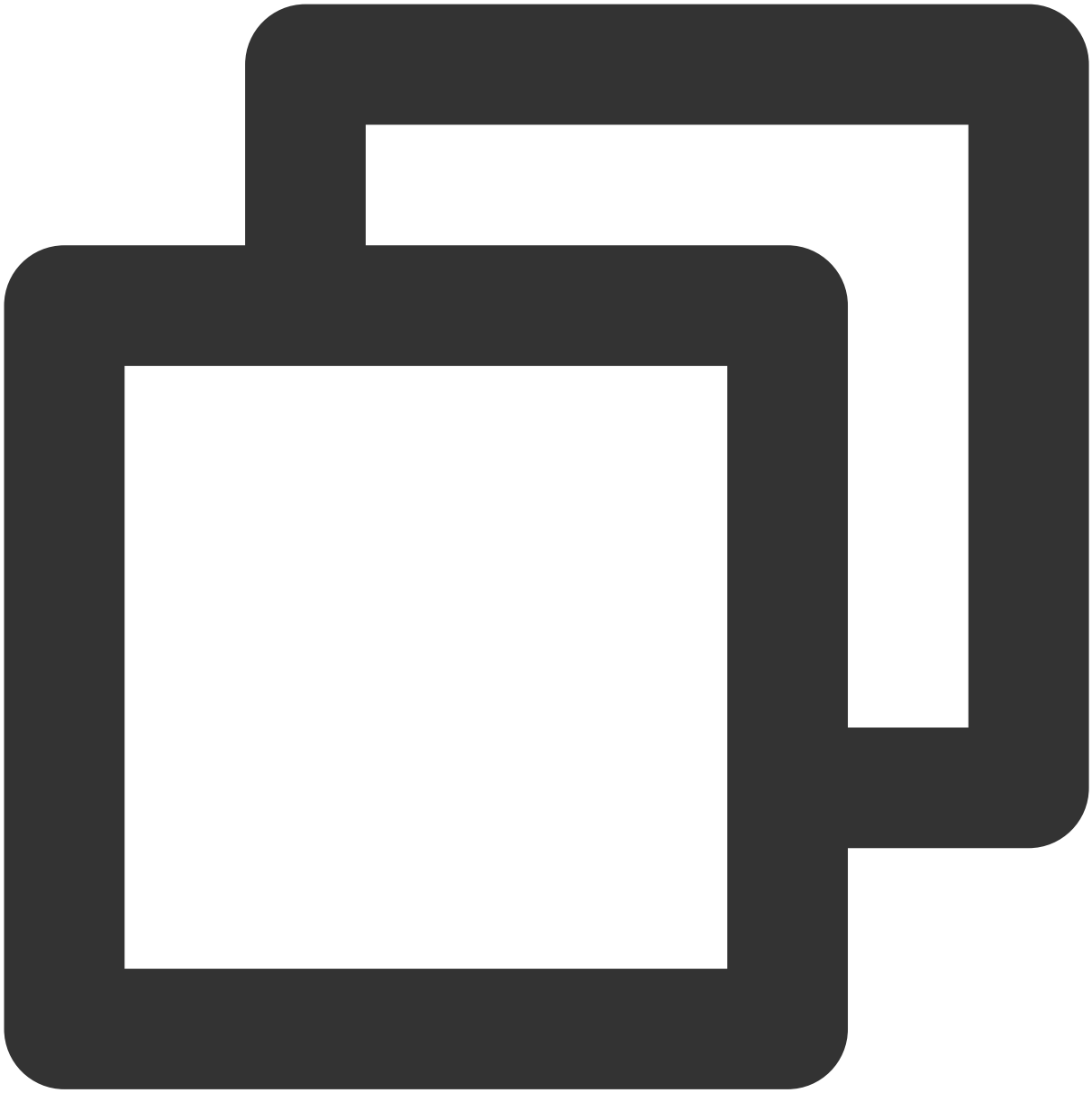
```
busid 1-1.3(096e:031b)
Feitian Technologies, Inc.: unknown product(096e:031b)
```

3. busid値を記録し、以下のコマンドを順に実行して、リスニングサービスを有効にし、USB/IPポート番号を指定して、USBデバイスを共有します。



```
sudo usbipd -D [--tcp-port PORT]
sudo usbip bind -b [busid]
```

たとえば、指定されたUSB/IPポート番号が3240（つまり、USB/IPのデフォルトポート）で、busidが `1-1.3` の場合、次のコマンドを実行します。

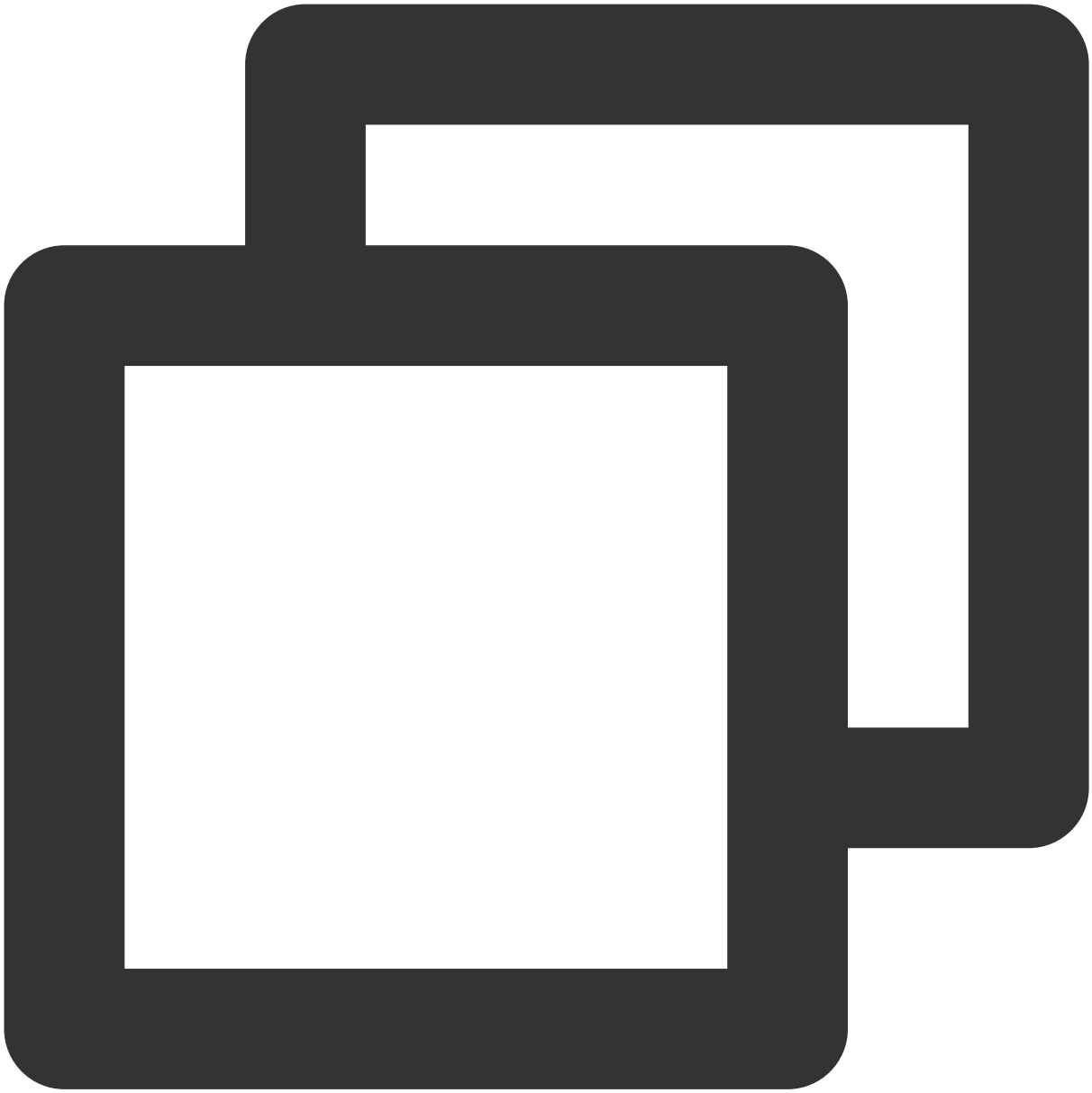


```
sudo usbipd -D
sudo usbip bind -b 1-1.3
```

4.（オプション）次のコマンドを実行してSSHトンネルを作成し、ポートでリスニングします。

説明：

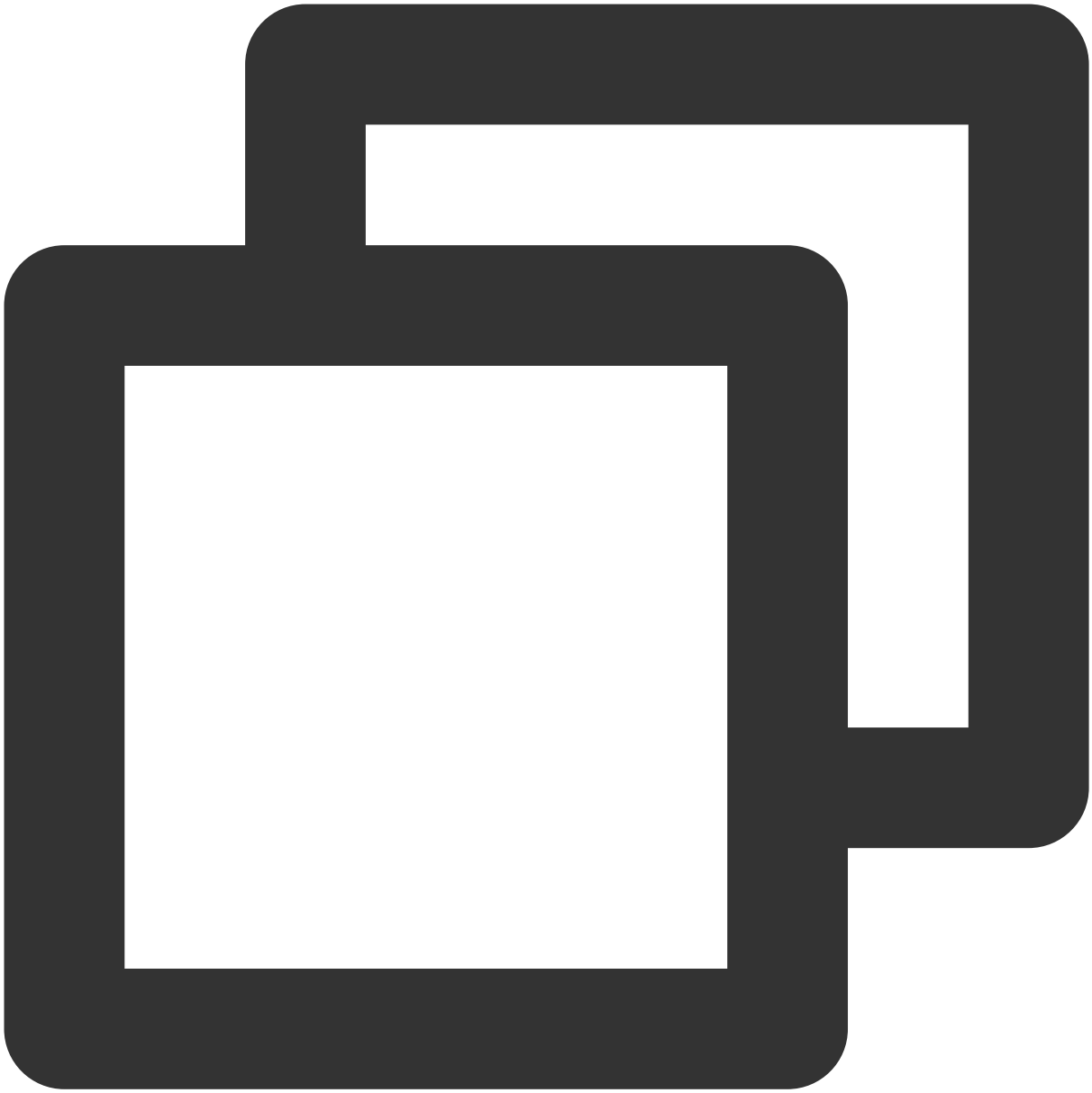
パブリックIPのないローカルPCは、この手順を実行してください。ローカルPCにパブリックIPがある場合は、この手順をスキップしてください。



```
ssh -Nf -R <Specified USB/IP port>:localhost:<Specified USB/IP port> root@your_host
```

`your_host` はCVMのIPアドレスを示します。

たとえば、USB/IPのポート番号が3240で、CVMのIPアドレスが192.168.15.24の場合、次のコマンドを実行します。



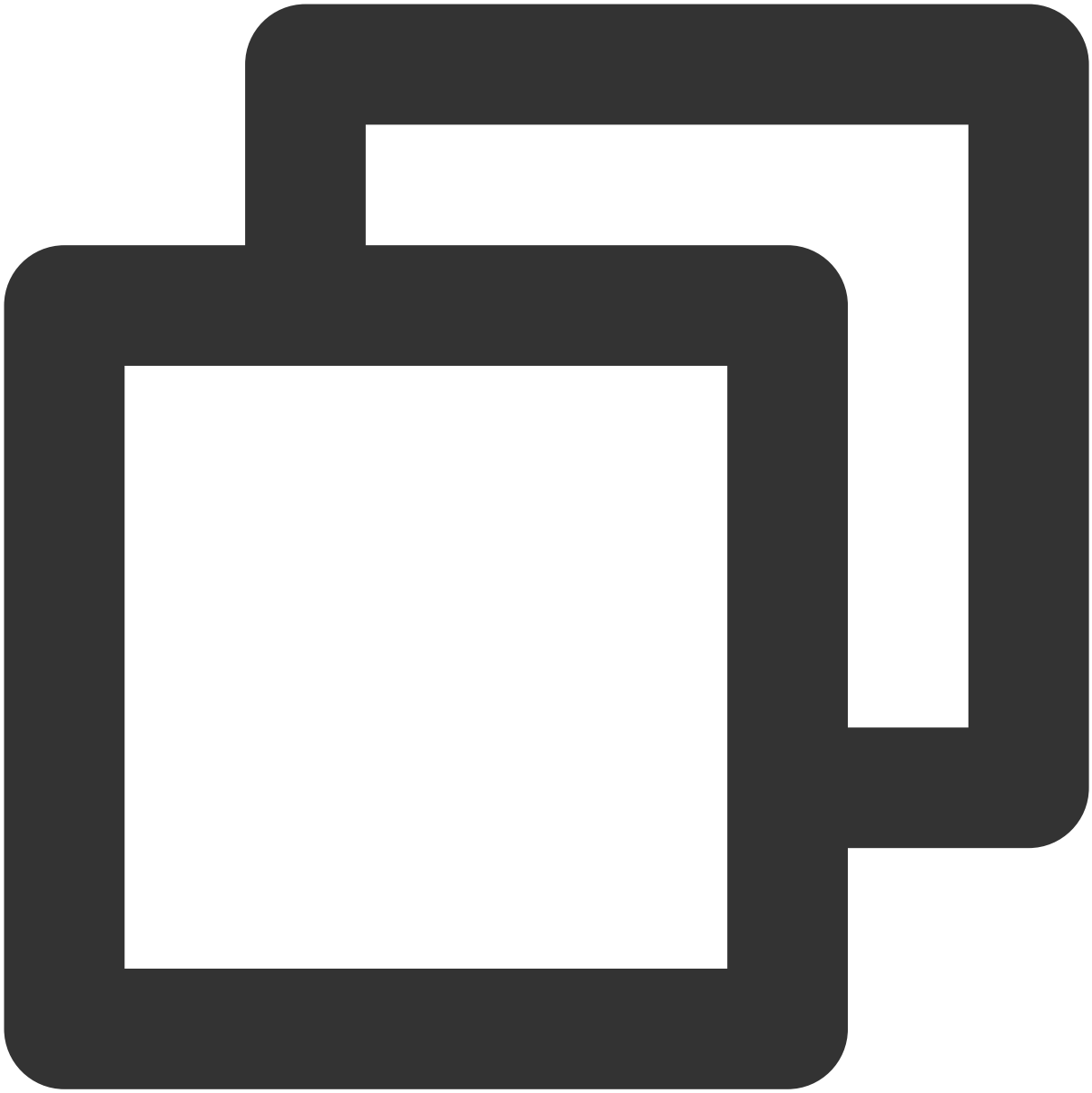
```
ssh -Nf -R 3240:localhost:3240 root@192.168.15.24
```

USBクライアントを設定する

説明：

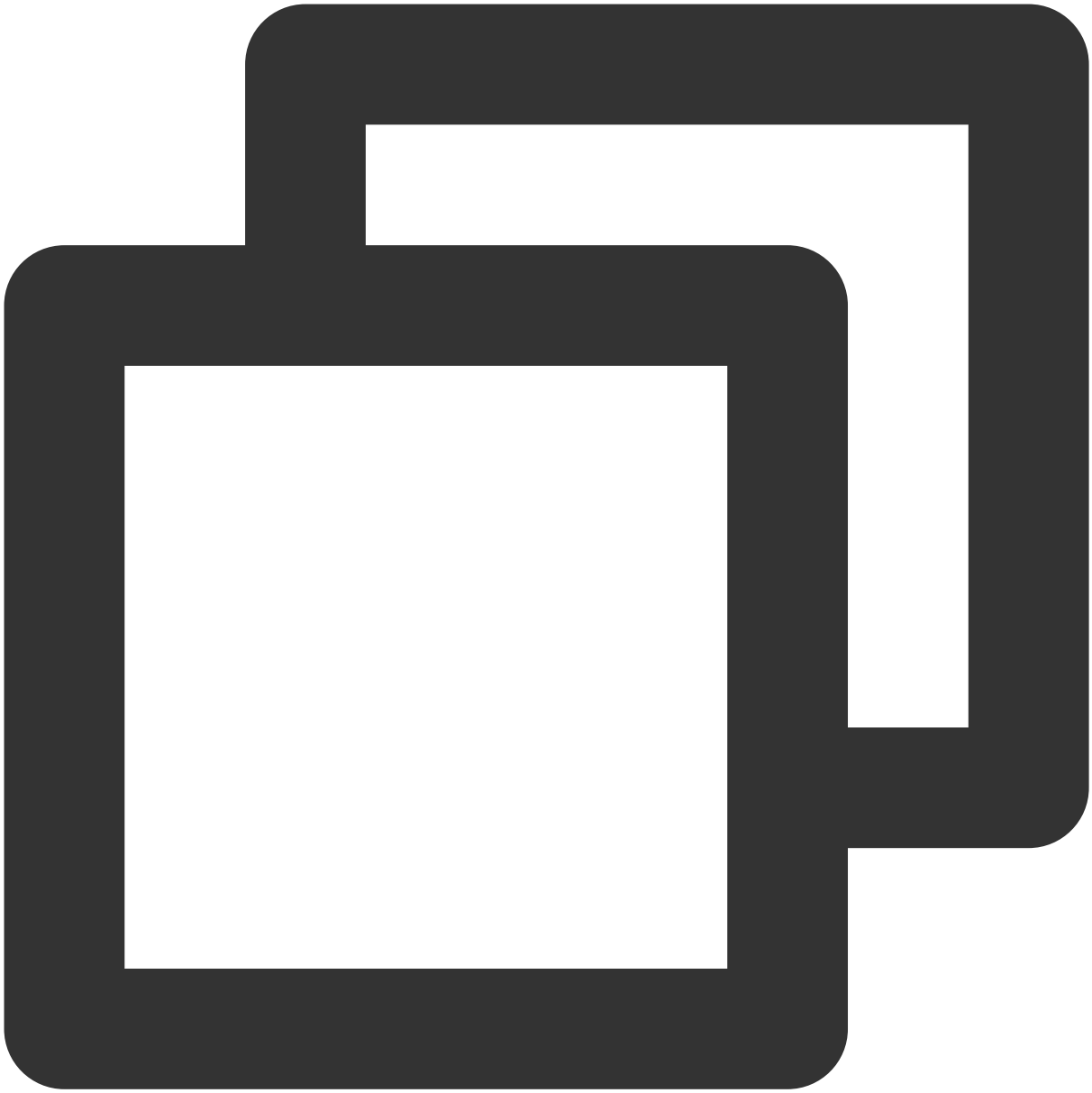
以下の手順では、パブリックIPアドレスのないローカルPCを例に説明します。ローカルPCにパブリックIPアドレスがある場合は、次の手順の `127.0.0.1` をローカルPCのパブリックIPアドレスに置き換えます。

1. 標準のログイン方法を使用してLinuxインスタンスにログインする（推奨）。
2. 次のコマンドを順に実行して、USB/IPソースをダウンロードします。



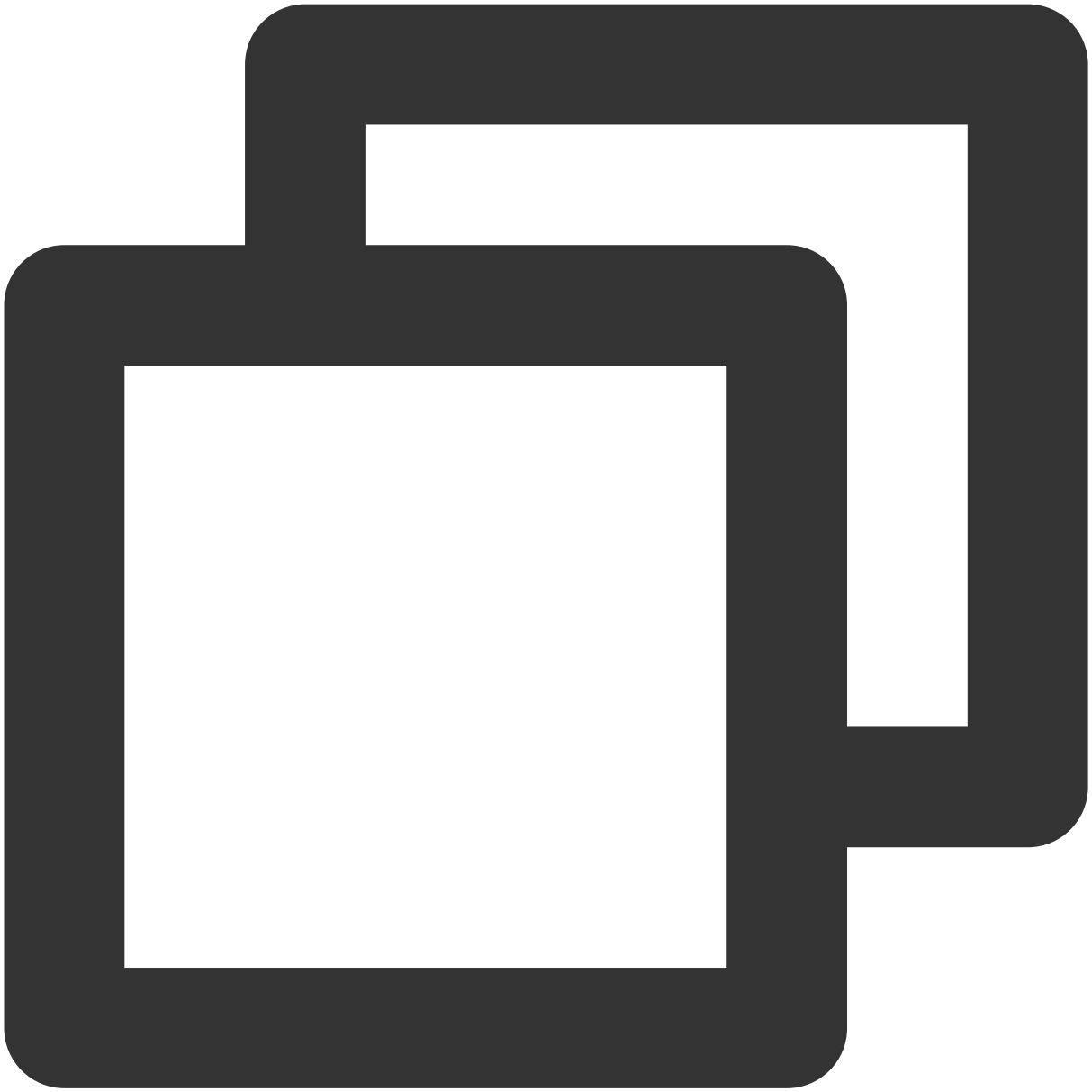
```
rpm --import https://www.elrepo.org/RPM-GPG-KEY-elrepo.org
rpm -ivh http://www.elrepo.org/elrepo-release-7.0-3.el7.elrepo.noarch.rpm
```

3. 次のコマンドを順に実行して、USB/IPをインストールします。



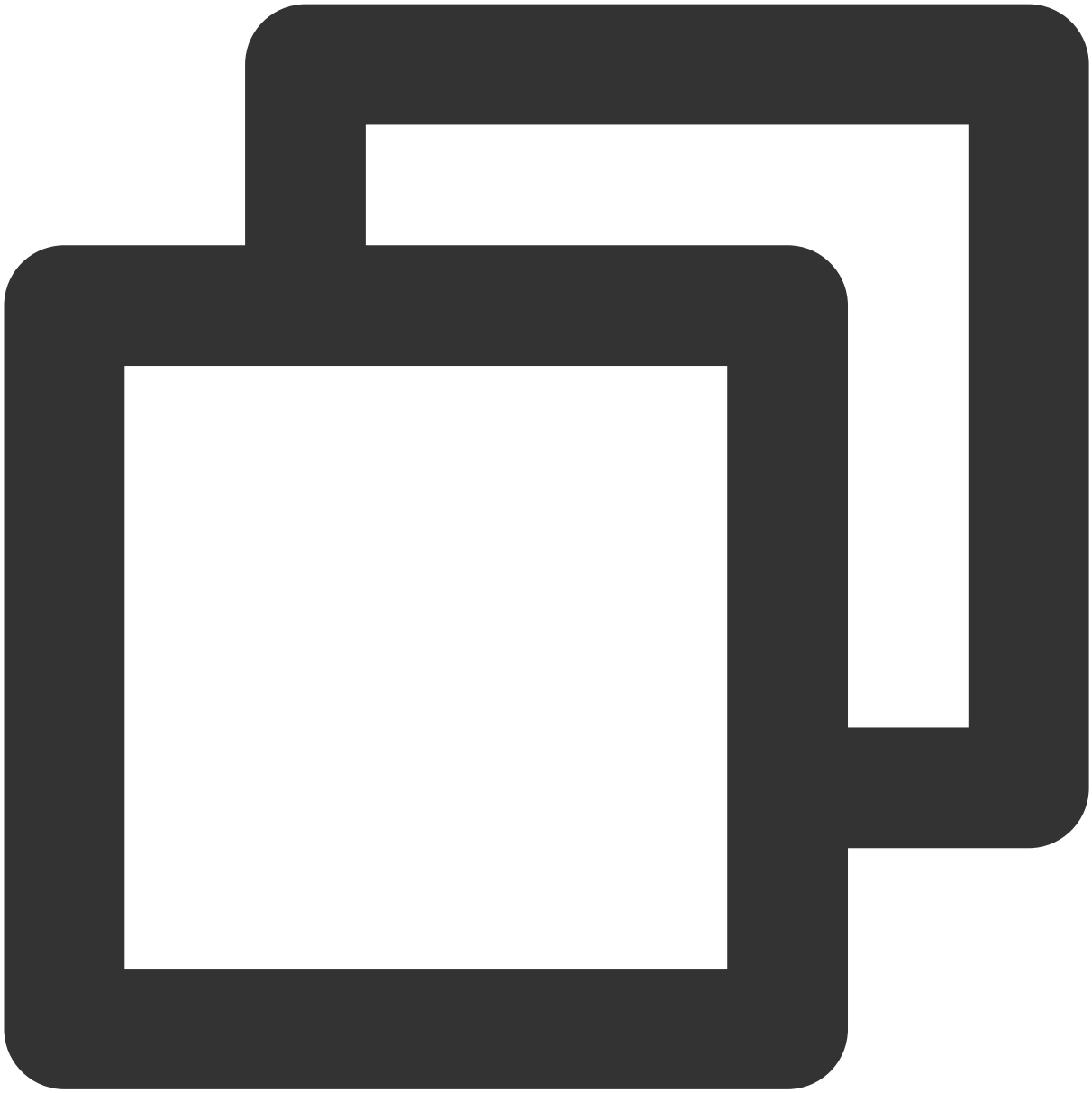
```
yum -y install kmod-usbip usbip-utils
modprobe usbip-core
modprobe vhci-hcd
modprobe usbip-host
```

4. 次のコマンドを実行して、CVMの利用可能なUSBデバイスを確認します。



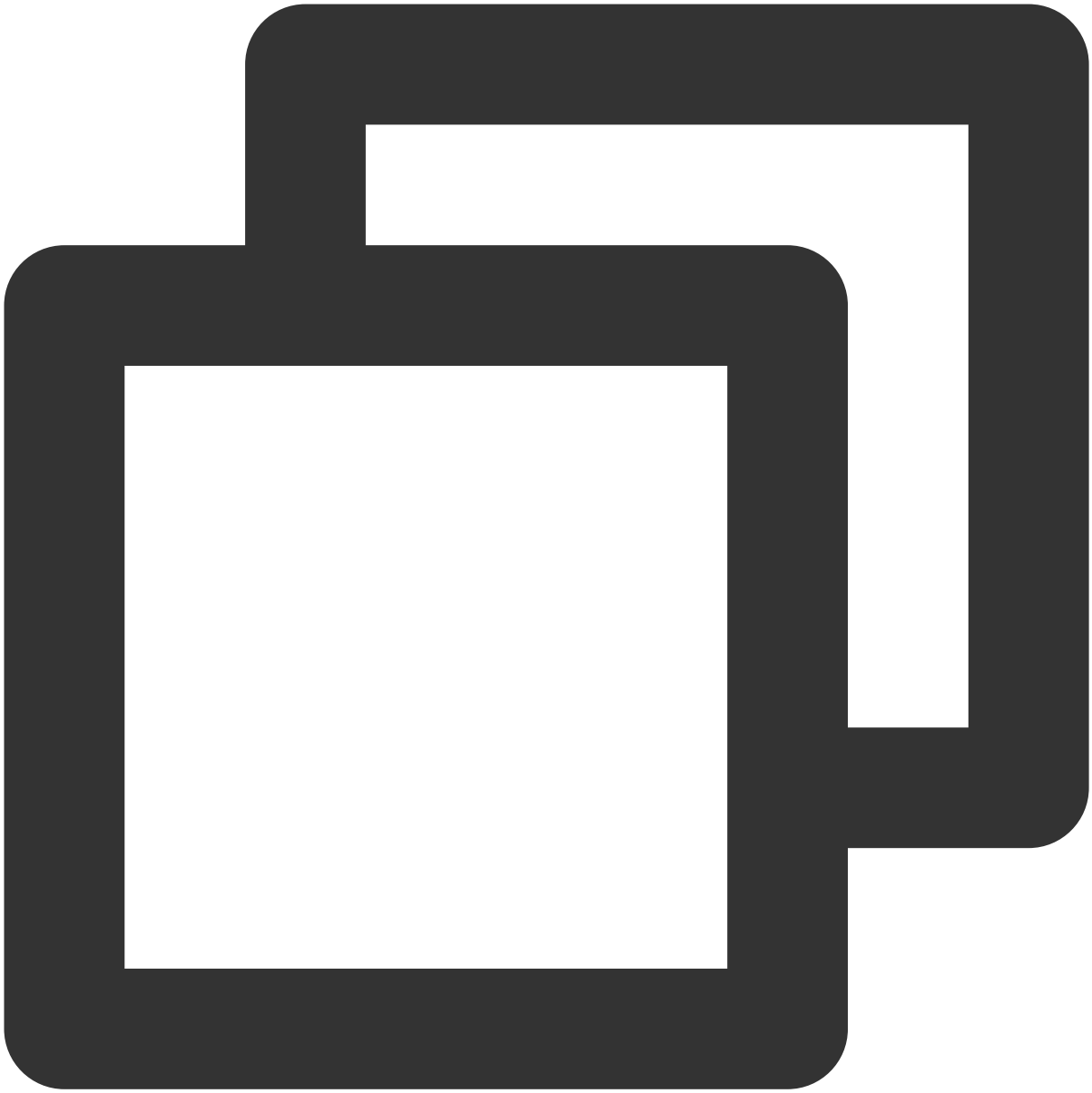
```
usbip list --remote 127.0.0.1
```

たとえば、Feitian USBキーの情報を見つけて、次の結果が返されます。



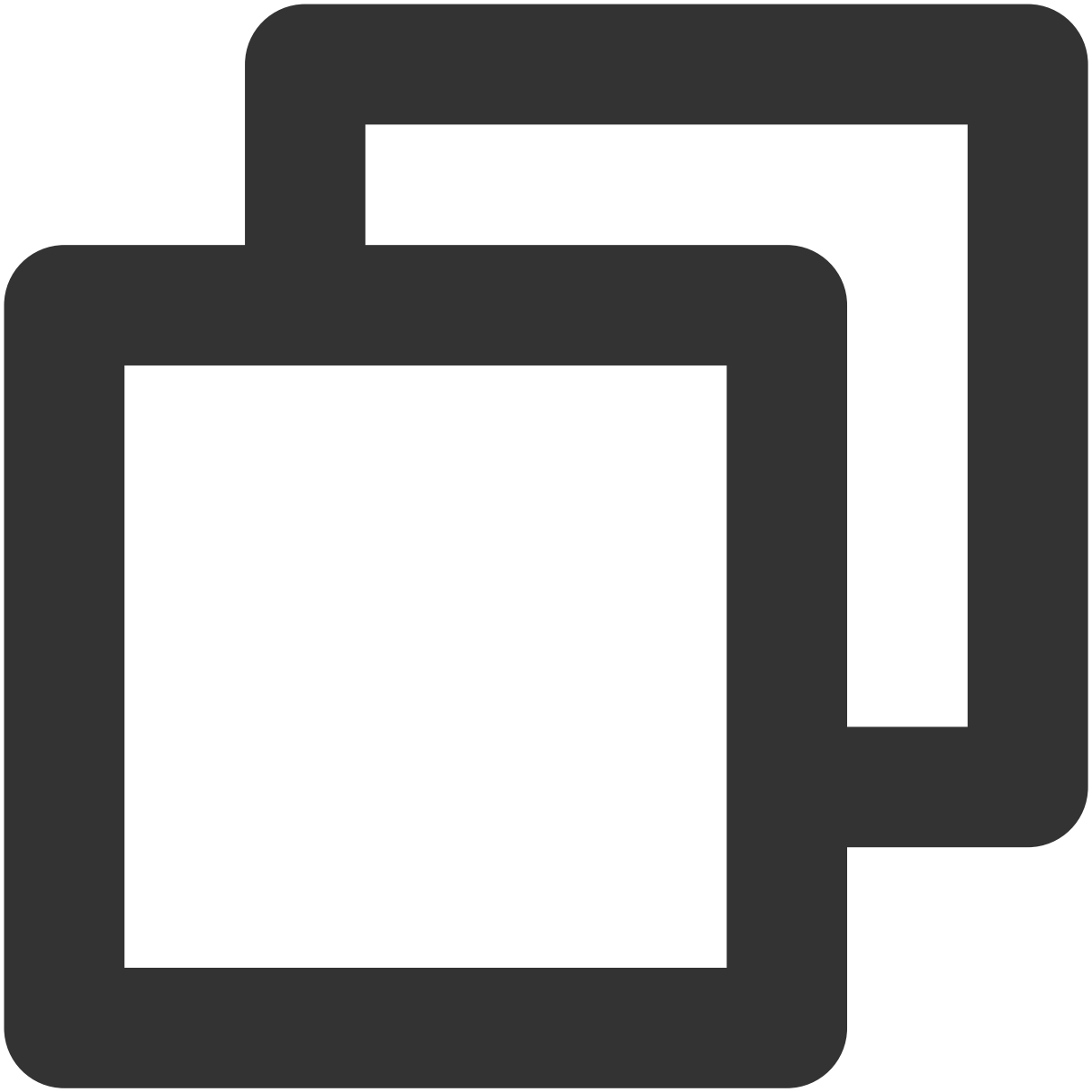
```
Exportable USB devices
======================
-127.0.0.1 1-1.3: Feitian Technologies, Inc.: unknown product(096e:031b):/sys/devi
```

5. 次のコマンドを実行して、USBデバイスをCVMにバインドします。



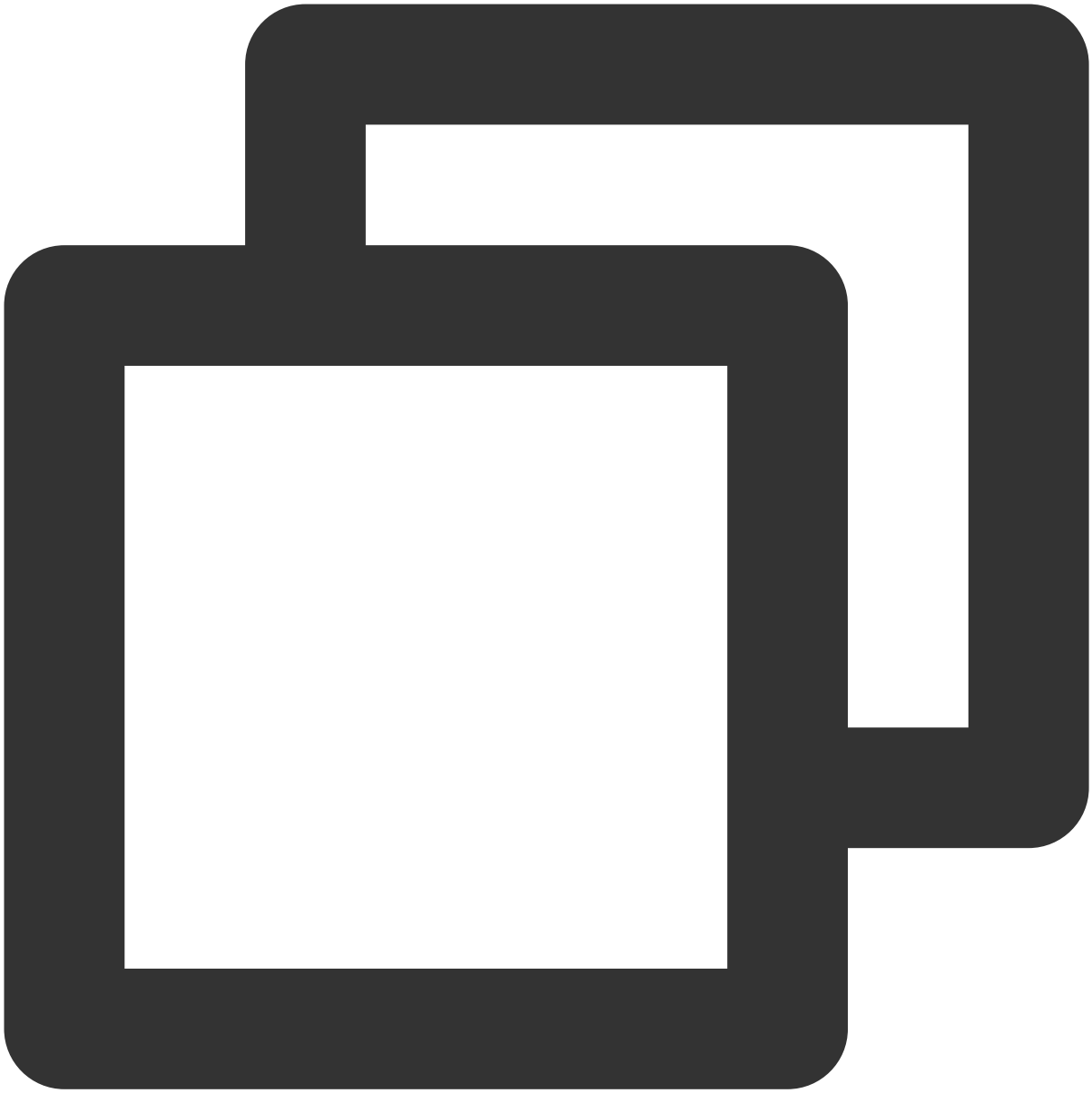
```
usbip attach --remote=127.0.0.1 --busid=1-1.3
```

6. 次のコマンドを実行して、現在のUSBデバイスリストをクエリーします。



```
lsusb
```

下記のような情報が返された場合は、共有が成功したことを示しています。



```
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インスタンス：CPUまたはメモリの使用率が高いため、CVMにログインできない

最終更新日：：2022-05-26 12:01:52

ユースケース

RemoteFxは、Windows デスクトッププロトコル（RDP）のアップグレード版です。RDP8.0以降は、RemoteFxを使用して、RDPデータチャネルを介してローカルUSBデバイスをリモートデスクトップにリダイレクトして、CVMがUSBデバイスを使用できない問題を解決できます。
このドキュメントでは、次の環境バージョンを例として、RDPのRemoteFx USBリダイレクト機能を有効にしてUSBデバイスをCVMにリダイレクトする方法を説明します。
クライアント：Windows 10 OS
サーバー：Windows Server 2016 OS

使用制限

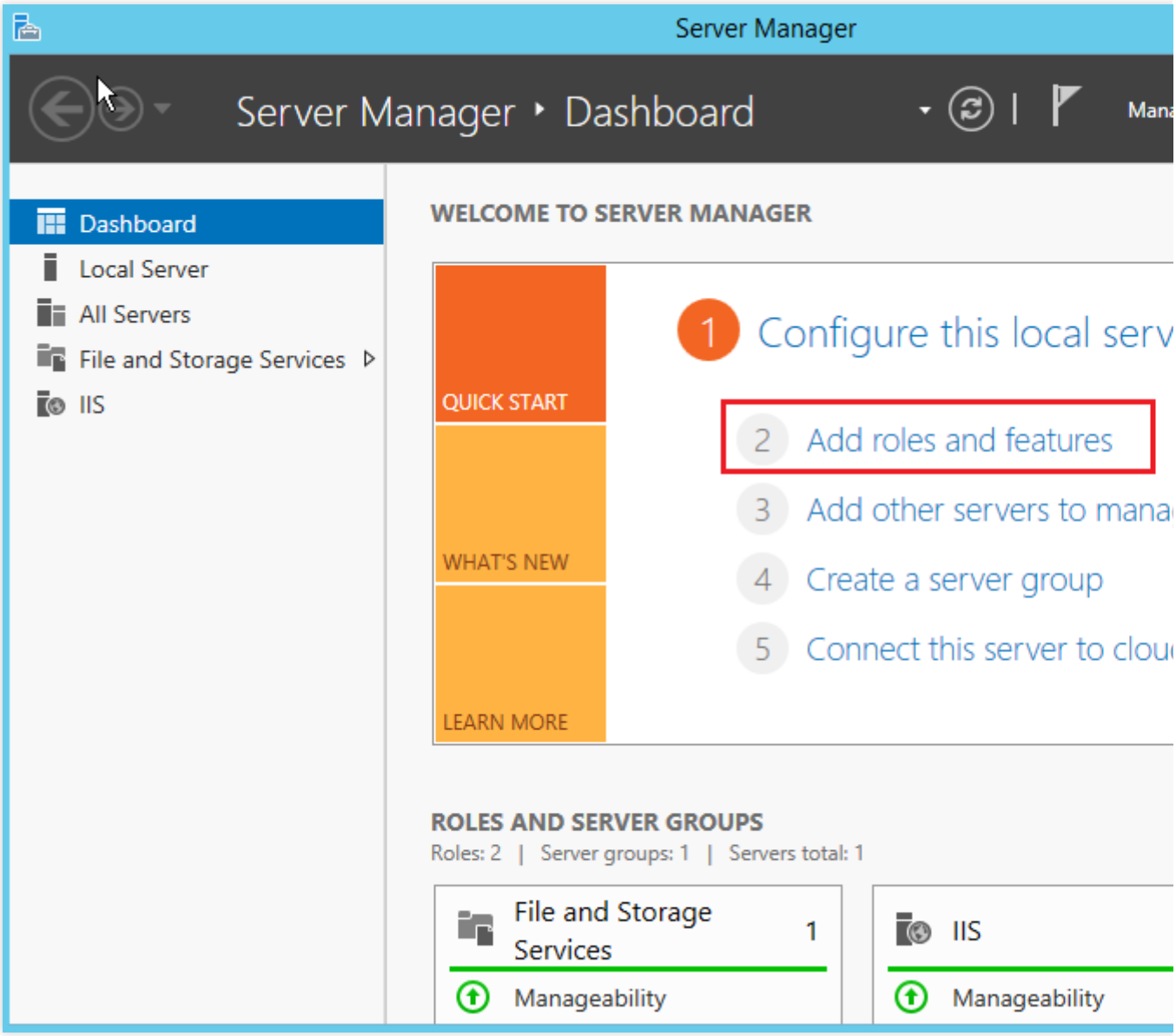
RDP 8.0以降のバージョンは、RemoteFX USB Redirection機能をサポートしているため、Windows 8、Windows 10、Windows Server 2016、およびWindows Server 2019がこの機能をサポートしています。ローカルPCのOSバージョンが上記のバージョンのいずれかである場合、RDP 8.0 Updateパッチをインストールする必要はありません。ローカルPCのOSバージョンがWindows 7またはWindows Vistaの場合は、マイクロソフトの公式Webサイト にアクセスして、RDP 8.0更新パッチを入手してインストールしてください。

操作手順

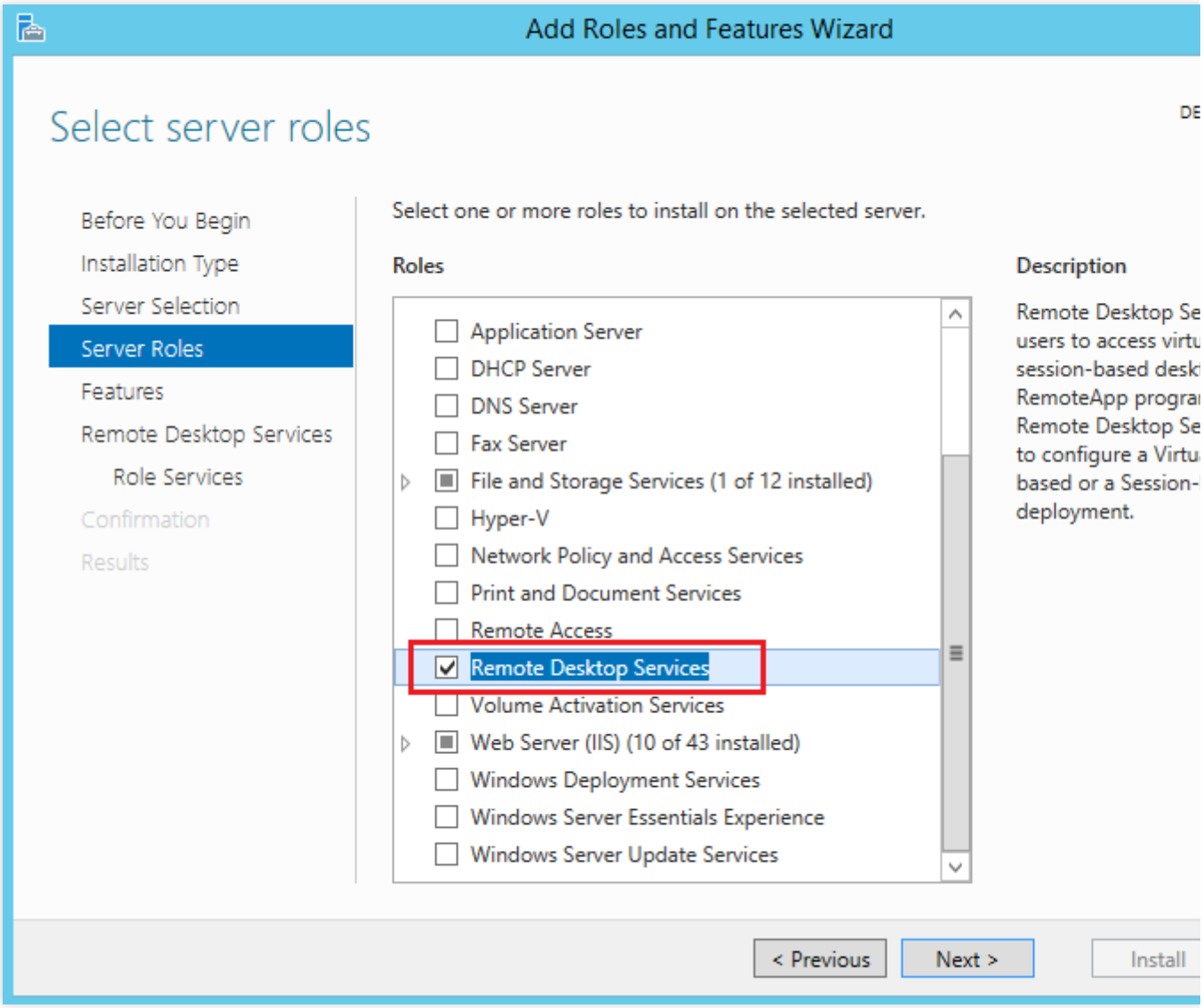
サーバーを設定する

1. RDPファイルを利用してWindowsインスタンスにログインする（推奨）。
2. OSの画面で、

をクリックして、**サーバーマネージャー**を選択して、サーバーマネージャーを開きます。
3. 「サーバーマネージャー」画面で、次の図に示すように、**役割と機能の追加**をクリックします。

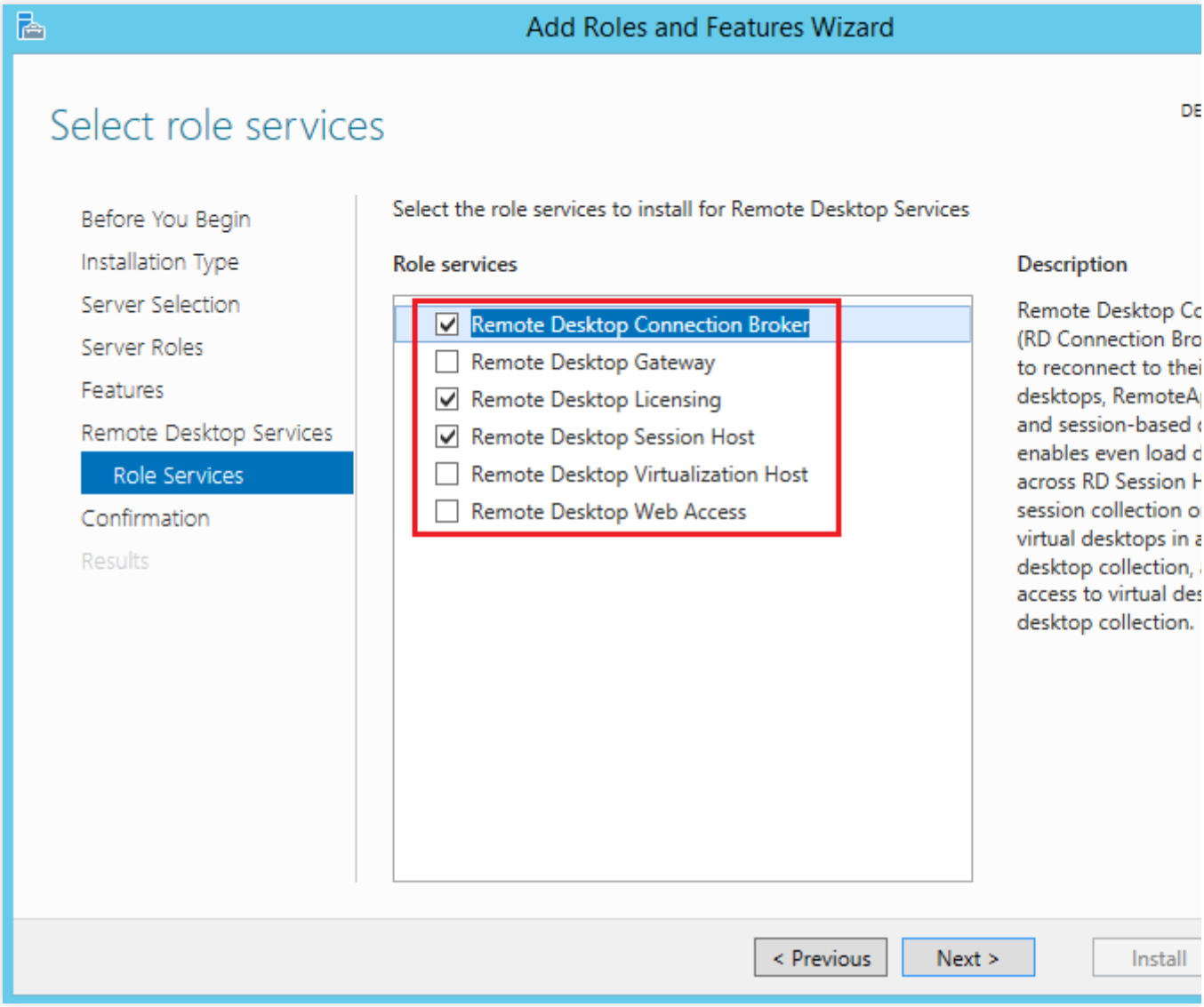


4. ポップアップされた「役割と機能の追加ウィザード」画面で、**次へ**をクリックして、「インストールの種類を選択」画面に入ります。
5. 「インストールの種類を選択」画面で、**役割ベースまたは機能ベースのインストール**を選択して、**次へ**をクリックします。
6. 「対象サーバーの選択」画面で、デフォルト設定のままにして、**次へ**をクリックします。
7. 「サーバーのロールを選択」画面で、次の図に示すように、**リモートデスクトップサービス**を選択し、**次へ**をクリックします。



8. デフォルト設定のままにして、**次へ**を2回クリックします。

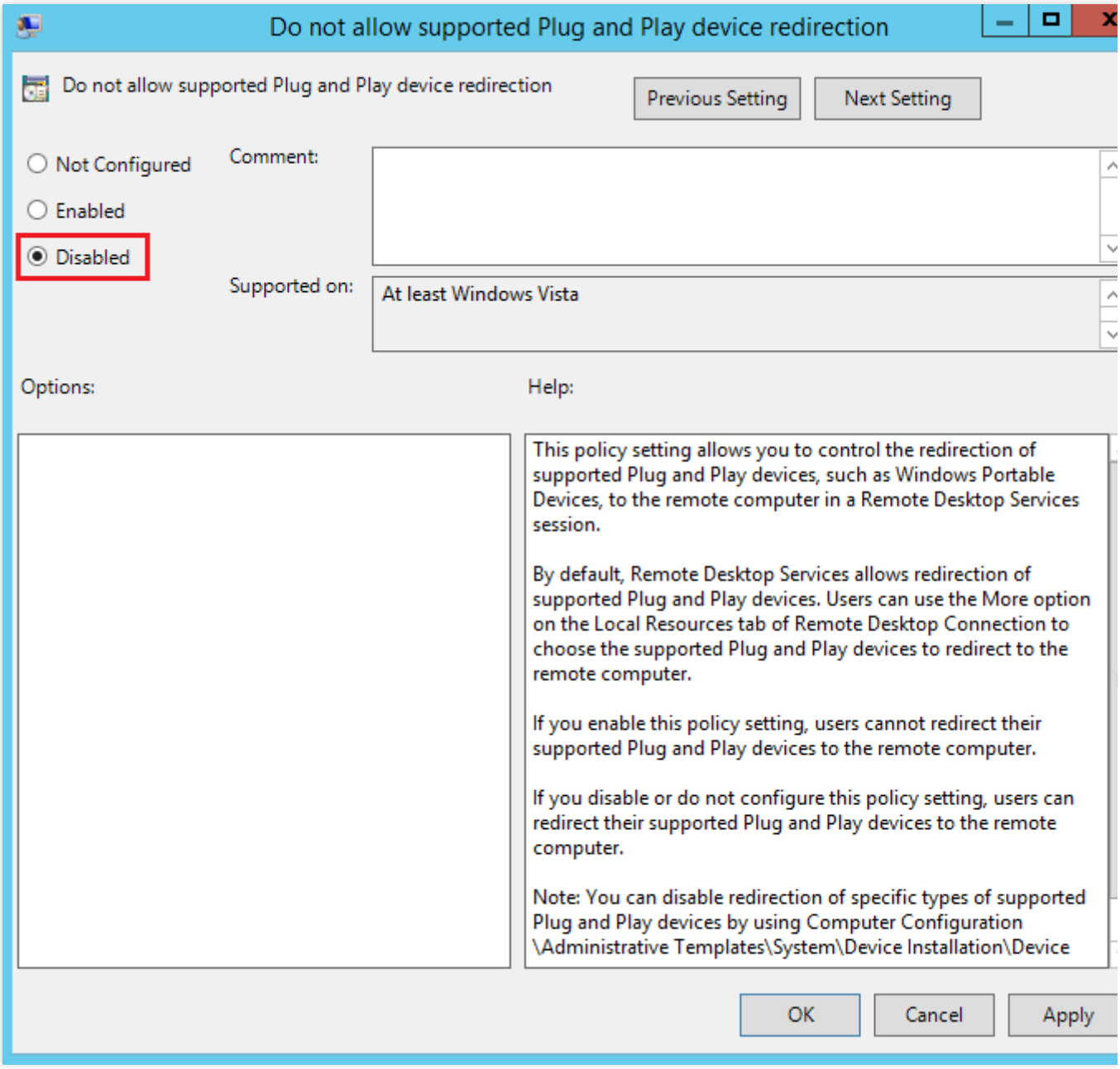
9. 「役割サービスの選択」画面で、次の図に示すように、**リモートデスクトップセッションホスト**、**リモートデスクトップ接続ブローカー**、および**リモートデスクトップライセンス**にチェックをいれて、ポップアップされた画面で**機能の追加**をクリックします。



10. **次へ**をクリックします。
11. **インストール**をクリックします。
12. インストールが完了すると、CVMを再起動します。
13. OS画面で、

をクリックし、**gpedit.msc**を入力して、**Enter**キーを押して、「ローカルグループポリシーエディター」を開きます。

14. 左側のナビゲーションツリーで、次の図に示すように、**コンピューターの設定>管理用テンプレート>Windowsコンポーネント>リモートデスクトップサービス> リモートデスクトップセッションホスト>デバイスとリソースのリダイレクト**を選択し、**サポートされているプラグ アンド プレイ デバイスのリダイレクトを許可しない**をダブルクリックして開きます。



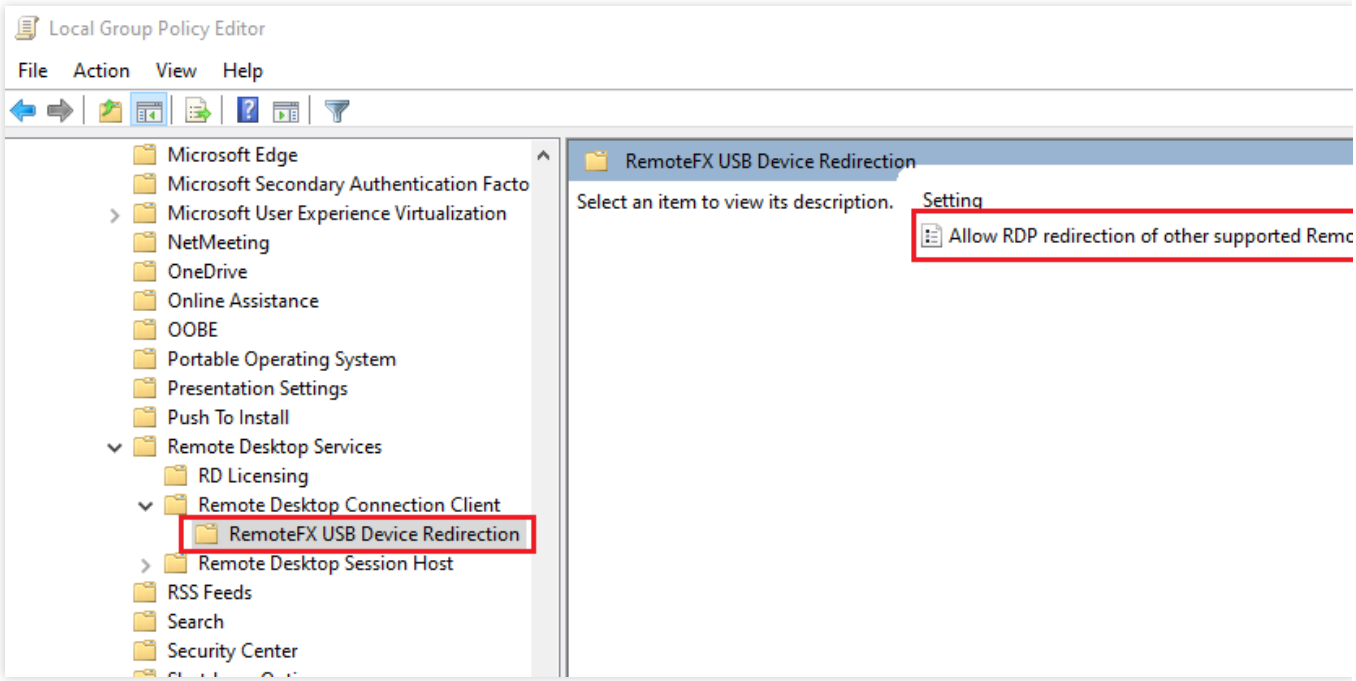
15. ポップアップされた画面で、次の図に示すように、**無効**を選択し、**OK**をクリックします。
16. CVMを再起動します。

クライアントを設定する

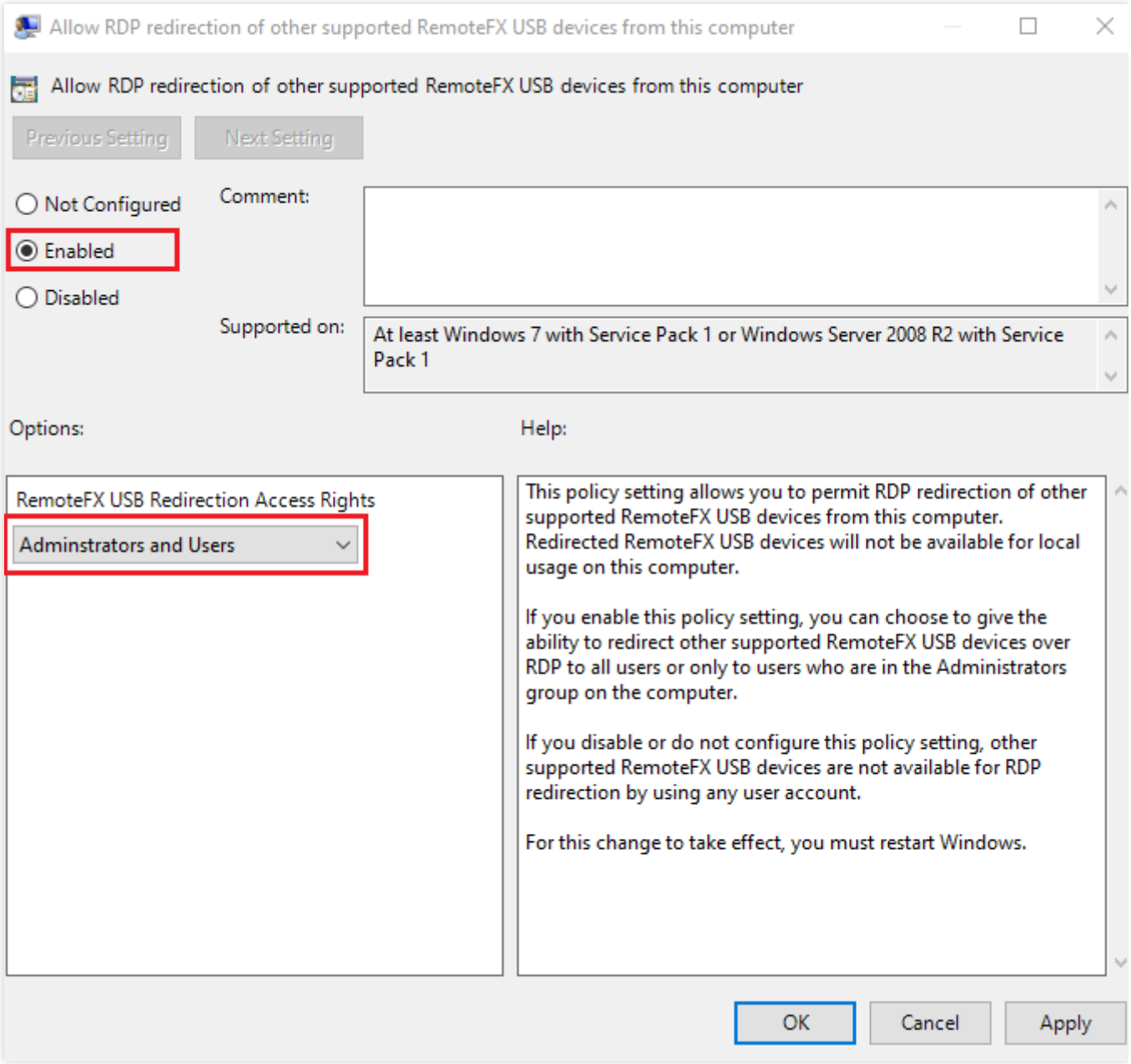
1. ローカルコンピュータで、

を右クリックし、**実行**を選択し、実行ダイアログボックスを開きます。
2. 実行ダイアログボックスで**gpedit.msc**と入力し、**OK**をクリックして「ローカルグループポリシーエディター」を開きます。

3. 左側のナビゲーションツリーで、次の図に示すように、**コンピューターの設定** > **管理用テンプレート** > **Windowsコンポーネント** > **リモートデスクトップサービス** > **リモートデスクトップセッションホスト** > **RemoteFx USBデバイスリダイレクト**を選択します。**サポートされている他の RemoteFX USB デバイスの、このコンピューターからの RDP リダイレクトを許可する**をダブルクリックして開きます。



4. ポップアップされた画面で、次の図に示すように、**有効**を選択し、RemoteFx USBリダイレクトのアクセス権限を**管理者とユーザー**に設定します。

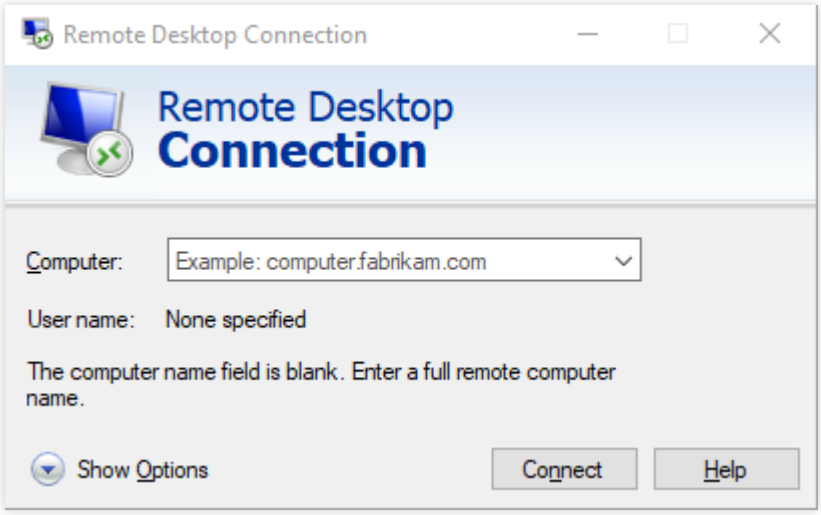


5. **OK**をクリックします。
6. ローカルPCを再起動します。

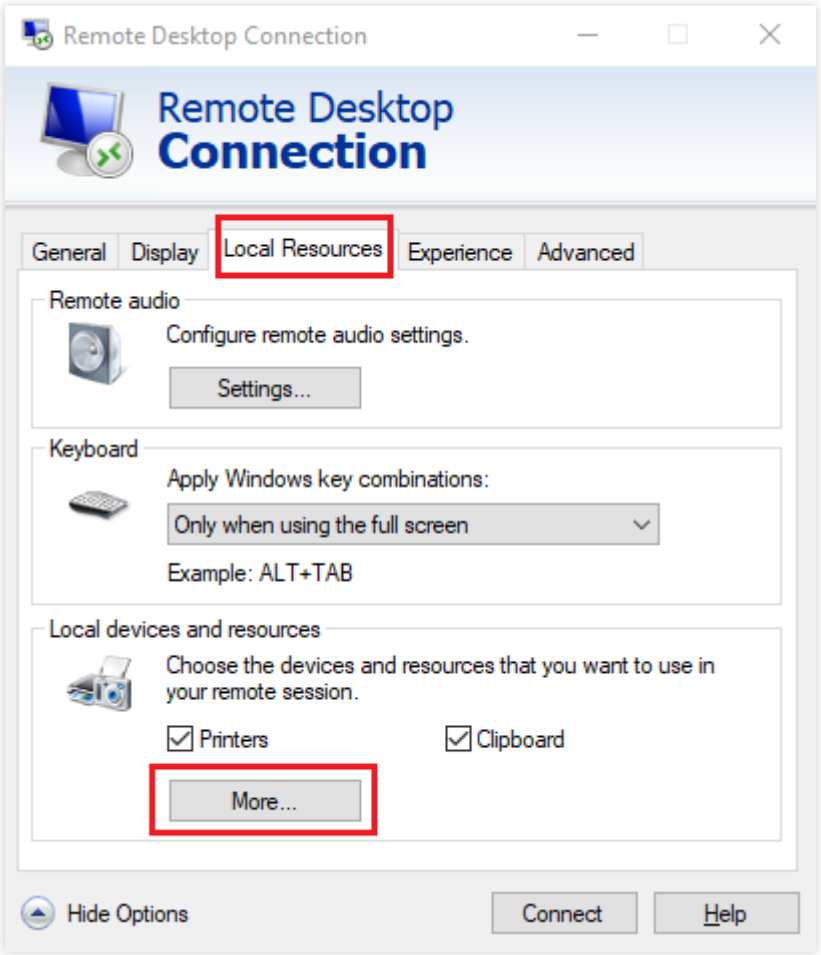
設定結果を確認する

1. ローカルPCで、USBデバイスを挿入し、

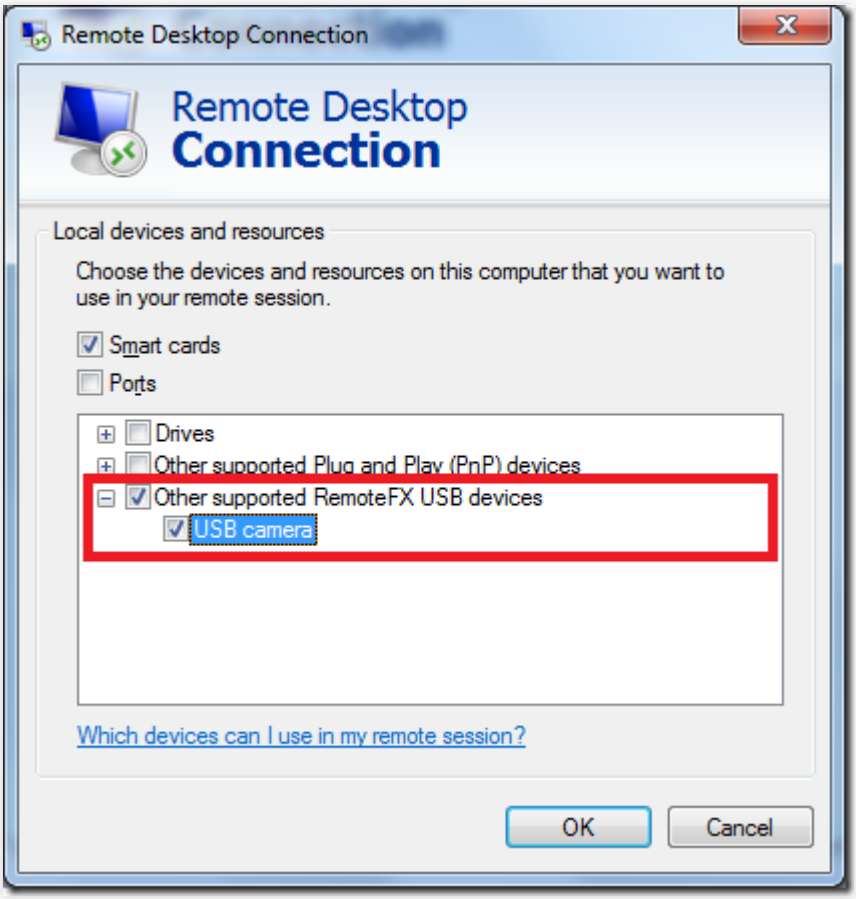
を右クリックして、**実行**を選択して、実行ダイアログボックスを開きます。
2. 実行ダイアログで、次の図に示すように、**mstsc**と入力し、**Enter**キーを押して、リモートデスクトップ接続ダイアログボックスを開きます。



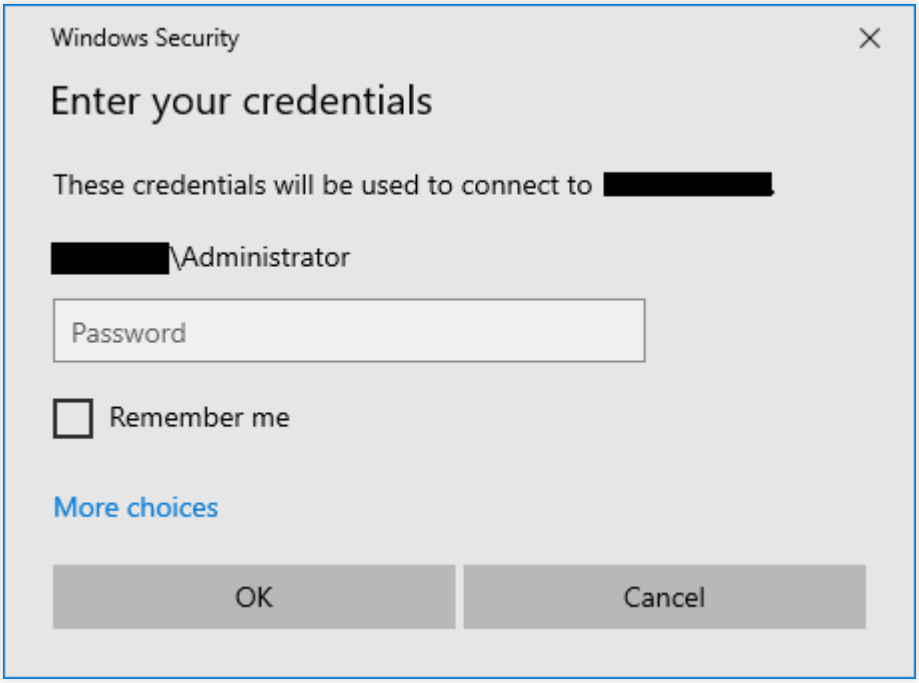
3. **コンピュータ**の後に、Windowsサーバーのパブリックipアドレスを入力し、**オプション**をクリックします。
4. **ローカルリソース**タブを選択し、「ローカルデバイスとリソース」列の**詳細**をクリックして、次の図に示すように、ローカルデバイスとリソースの画面が表示されます。



5. ポップアップされたローカルデバイスとリソースの画面で、**その他のサポートされているRemoteFX USBデバイス**を展開し、挿入されたUSBデバイスを選択して、**OK**をクリックします。

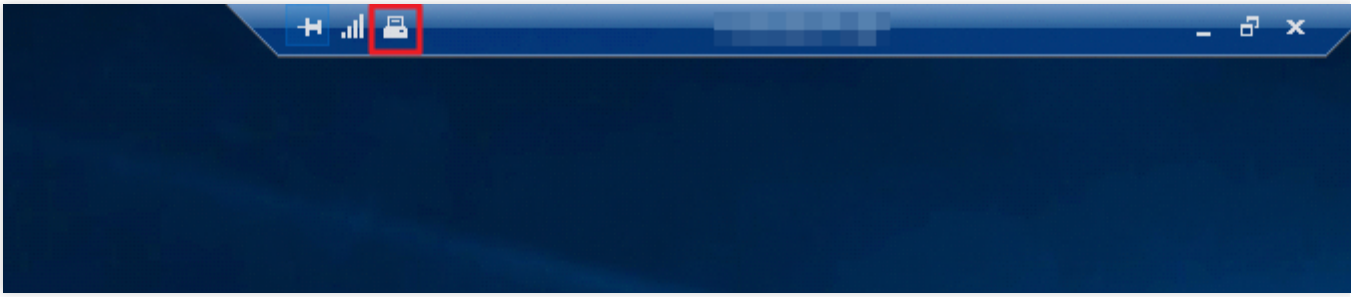


6. **接続**をクリックします。
7. ポップアップされた「Windowsセキュリティ」画面で、次の図に示すように、インスタンスの管理者アカウントとパスワードを入力します。



8. **OK**をクリックして、Windowsインスタンスにログインします。
Windows インスタンスの操作画面の上部に

が表示されると、設定が成功したことを示します。



関連操作

Windows RDPプロトコルは、一般的に使用されるUSBデバイスに対してより最適化された接続パフォーマンスを提供できます。つまり、RemoteFx機能を有効にすることなく、ドライブやカメラなどのデバイスを直接マッピングできます。よく使われていないUSBデバイスは、RemoteFX USBリダイレクト機能によってのみ実現できます。よく使われていないUSBデバイスは、以下を参照して、対応するリダイレクト方法を選択できます。

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 *Not supported during logon*	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

CVMでAVX512を介して人工知能アプリケーションをアクセラレーションします

最終更新日：：2023-05-09 14:17:55

操作シナリオ

Tencent Cloudの第6世代S6および第5世代インスタンスS5、M5、C4、IT5、D3は、第2世代インテリジェントIntel®Xeon®スケーラブルプロセッサCascadeLakeを全面的に採用しています。より多くの命令セットや機能を提供して、人工知能のアプリケーションのアクセラレーションに使用するとともに、多数のハードウェア拡張技術を統合することができます。中でも、AVX-512（アドバンスト・ベクトル・エクステンション）は、AI推論プロセスに強力な並列コンピューティング機能を提供し、ユーザーのディープラーニングの効果をより高めることができます。
ここではS5、M5インスタンスを例として、CVMでAVX512を介して人工知能アプリケーションをアクセラレーションする方法を説明します。

モデル選択時の推奨事項

CVMのさまざまなインスタンス仕様は、さまざまなアプリケーション開発に用いることができます。中でも標準型 S6、標準型S5 および メモリ型M5 は、 機械学習やディープラーニングに適しています。これらのインスタンスには、Intel® DL boost学習機能に適応する第2世代Intel®Xeon®プロセッサが搭載されています。推奨される構成は下表のとおりです。

プラットフォームタイプ	インスタンス仕様
ディープラーニングトレーニングプラットフォーム	84vCPUの標準型S5インスタンスまたは48vCPUのメモリ型M5インスタンス。
ディープラーニング推論プラットフォーム	8/16/24/32/48vCPUの標準型S5インスタンスまたはメモリ型M5インスタンス。
機械学習トレーニングまたは推論プラットフォーム	48vCPUの標準型S5インスタンスまたは24vCPUのメモリ型M5インスタンス。

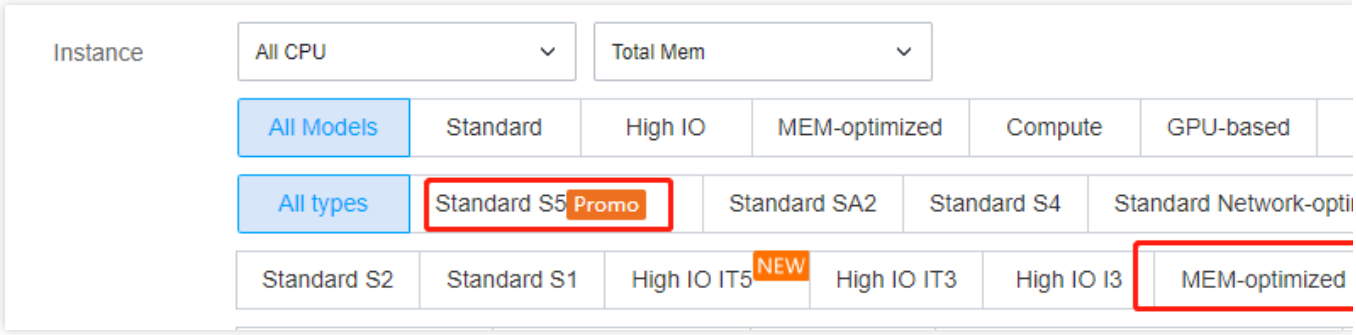
有する利点

Intel® Xeon®スケーラブルプロセッサを使用して機械学習またはディープラーニングのワークロードを実行する場合、以下の利点があります。
大容量メモリ型ワークロード、医用画像、GAN、地震解析、遺伝子シーケンシングなどのシナリオで使用される3D-CNNトポロジーの処理に適しています。
シンプルな `numactl` コマンドを使用した柔軟なコア制御をサポートしており、小さなバッチのリアルタイム推論にも適しています。
強力なエコシステムをサポートしており、大型クラスターで分散型トレーニングを直接実行できるため、大容量ストレージの追加や高価なキャッシュメカニズムを必要とする大規模なアーキテクチャトレーニングを回避することができます。
同じクラスター内で複数のワークロード（HPC、BigData、AIなど）をサポートしており、より優れたTCOを取得できます。
SIMDによってアクセラレーションし、ディープラーニングのアプリケーションプログラムに関する多くの実質的なコンピューティング要件を満たします。
同じインフラストラクチャをトレーニングと推論に直接使用できます。

操作手順

インスタンスを作成

CVMインスタンスを作成します。詳細については、購入画面でインスタンスを作成 をご参照ください。そのうち、インスタンス仕様は、モデル選択時の推奨事項 と実際の業務シナリオに従って選択する必要があります。下図のとおりです。



説明：
インスタンス仕様のパラメータについては、インスタンス仕様 をご参照ください。

インスタンスへのログイン

CVMインスタンスにログインします。詳細については、標準方式を使用してLinuxインスタンス（推奨）にログイン をご参照ください。

デプロイ例

実際の業務シナリオに基づき、次の例を参照して人工知能プラットフォームをデプロイし、機械学習またはディープラーニングタスクを実行することができます。

例1： Intel®を使用して、ディープラーニングフレームワークを最適化します TensorFlow*

第2世代Intel®Xeon®スケーラブルプロセッサCascade LakeのPyTorchおよびIPEXでは、演算性能を最大限にアップさせるため、AVX-512命令セットの最適化が自動的に有効になります。

TensorFlow*は、大規模な機械学習とディープラーニングに用いる、人気のフレームワークの1つです。この例を参照して、インスタンスのトレーニングと推論性能を向上させることができます。フレームワークのデプロイに関する情報については、Intel® Optimization for TensorFlow* Installation Guide をご参照ください。操作手順は次のとおりです。

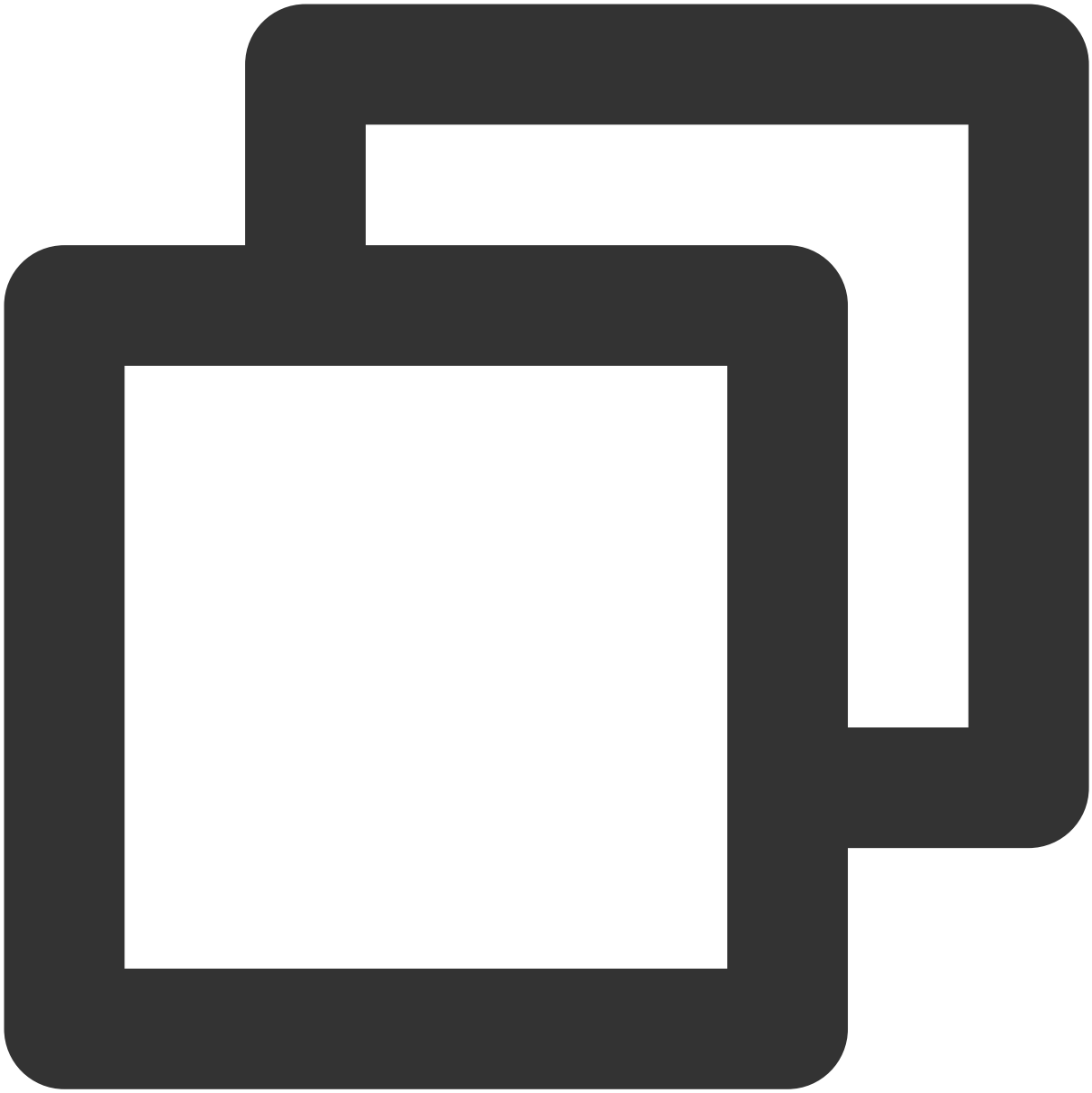
TensorFlow*フレームワークのデプロイ

1. CVMにPythonをインストールします。ここでは、Python3.7を例とします。

2. 以下のコマンドを実行して、Intel®に最適化されたTensorFlow*バージョンのintel-tensorflowをインストールします。

説明：

最新の機能と最適化を利用するため、**2.4.0およびそれ以降のバージョン**を使用することをお勧めします。



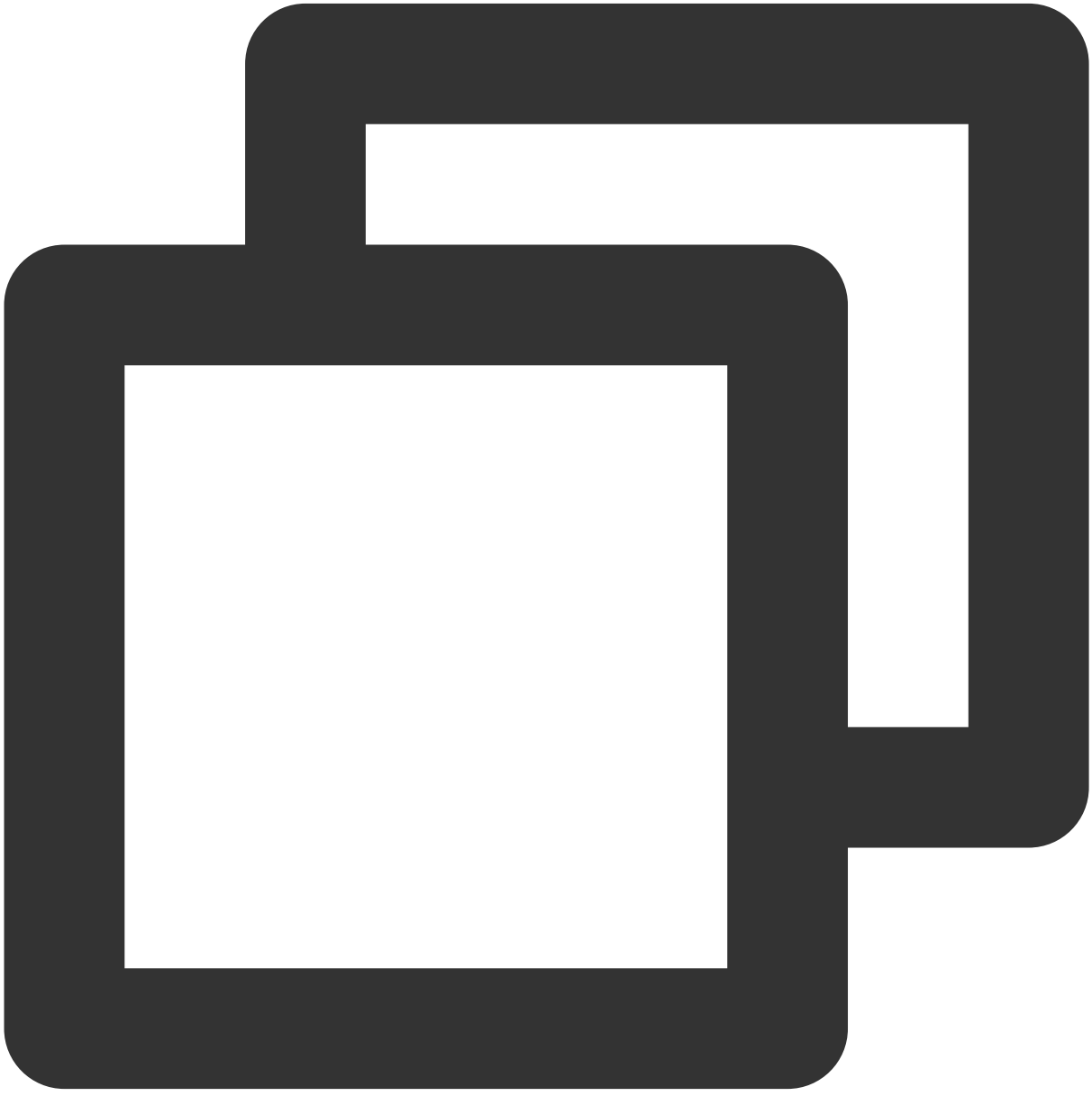
```
pip install intel-tensorflow
```

ランタイム最適化パラメータを設定

ランタイムパラメータの最適化方法を選択します。 通常、以下の2つの実行インターフェースを使用して、異なる最適化設定を採用します。実際のニーズに応じて選択できます。パラメータ最適化の設定に関する説明については、General Best Practices for Intel® Optimization for TensorFlow をご参照ください。

Batch inference：BatchSize >1に設定し、1秒あたりに処理できる入力テンソルの総数を測定します。通常の状況では、Batch Inference方式は、同じCPU socketですべての物理コアを使用することによって最高のパフォーマン

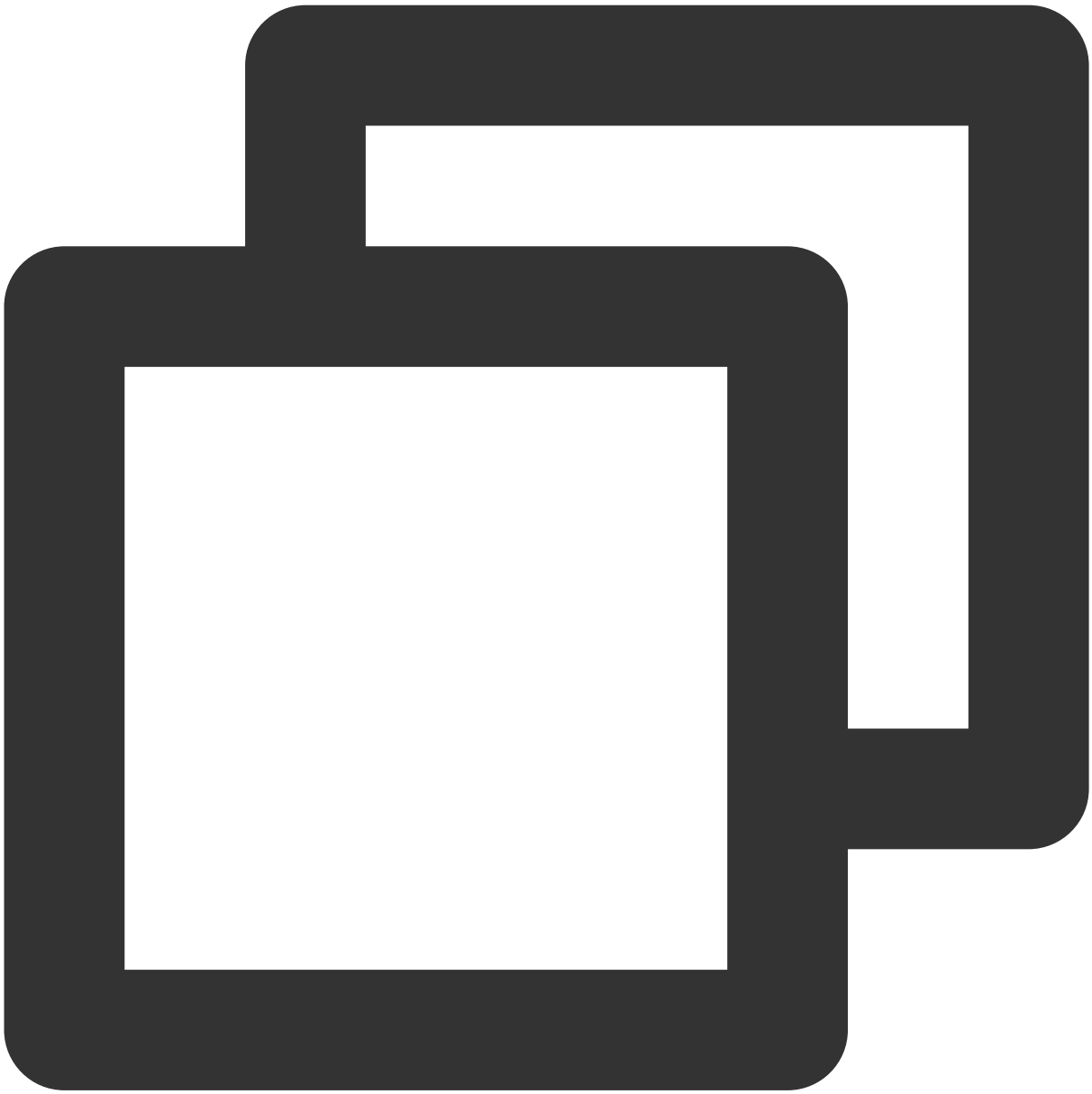
スを実現できます。
On-line Inference（リアルタイム推論とも呼びます）：BS = 1に設定し、単一の入力テンソルの処理（バッチサイズは1）に必要な時間を測定します。リアルタイム推論スキームでは、マルチインスタンスを同時実行して、最高のスループットを得ることができます。
操作手順は次のとおりです。
1. 以下のコマンドを実行して、システム内の物理コアの数を取得します。



```
lscpu | grep "Core(s) per socket" | cut -d':' -f2 | xargs
```

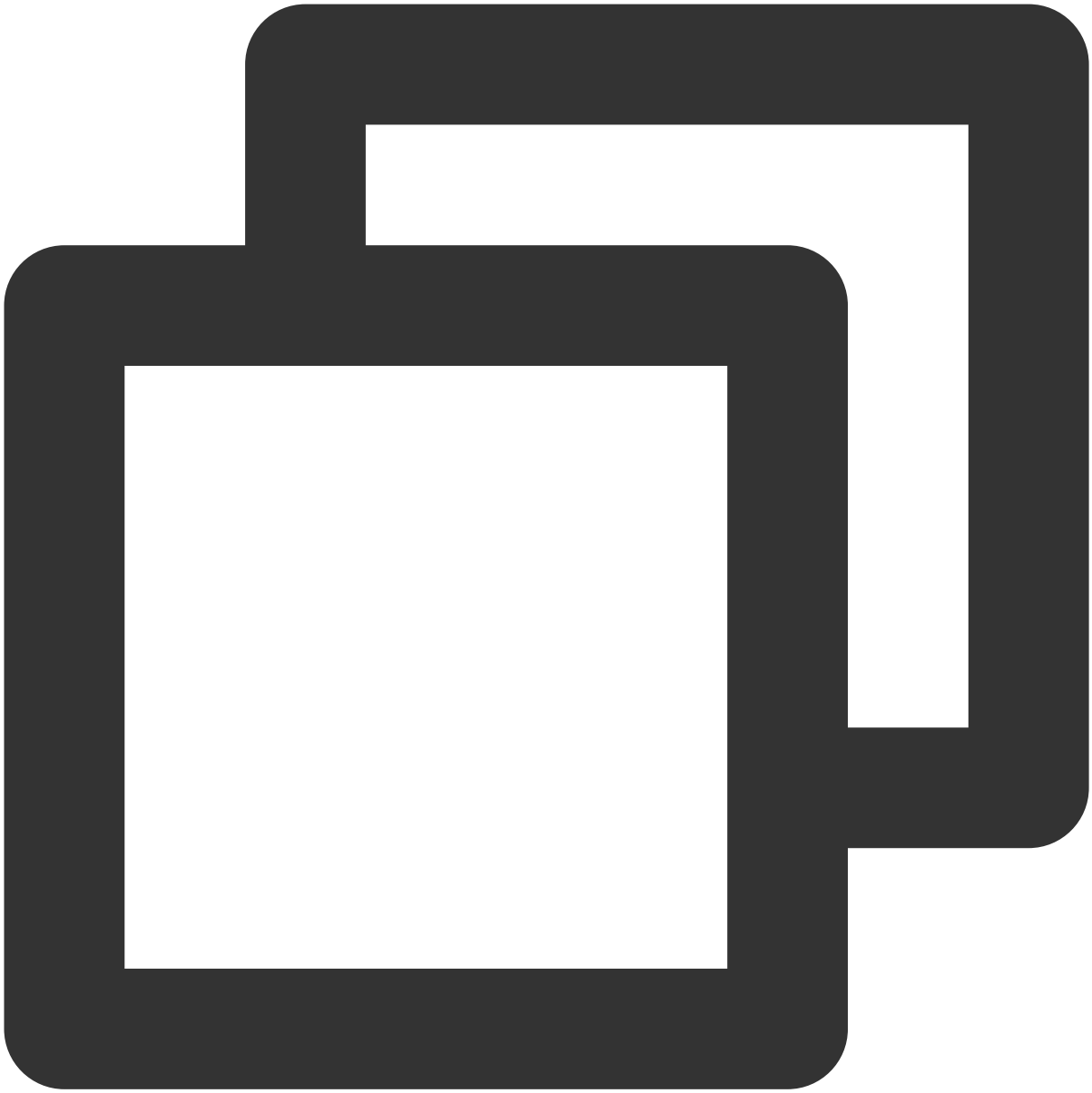
2. 最適化パラメータを設定します。以下のいずれかの方法を選択できます。

環境の実行パラメータを設定します。環境変数ファイルに、以下の構成を追加します。



```
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
```

コードに環境変数設定を追加します。実行中のPythonコードに、以下の環境変数設定を追加します：



```
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*ディープラーニングモデルの推論を実行する

Image Recognition with ResNet50, ResNet101 and InceptionV3 を参照して、他の機械学習/ディープラーニングモデルの推論を実行してください。ここでは、benchmarkを例として、ResNet50のinference benchmarkを実行する方法を説明します。詳細については、ResNet50 (v1.5) をご参照ください。

TensorFlow*ディープラーニングモデルのトレーニングを実行する

ここでは、ResNet50のtraining benchmarkを実行する方法を説明します。詳細については、FP32 Training Instructions をご参照ください。

TensorFlowの性能デモンストレーション

パフォーマンスデータについては、Improving TensorFlow* Inference Performance on Intel® Xeon® Processors をご参照ください。実際のモードと物理構成によって、パフォーマンスデータはある程度異なります。以下のパフォーマンスデータはあくまでも参考です。

レイテンシー性能：

テストを通じて、batch sizeが1の場合に画像分類とターゲット検出に適したモデルをいくつか選択すると、AVX512最適化バージョンでは、最適化されていないバージョンと比べて推論性能が明らかに向上していることがわかります。例えば、レイテンシーに関しては、最適化されたResNet 50のレイテンシーは元の45%まで低減します。

スループット性能：

batch sizeを大きくしてスループット性能をテストし、画像分類やターゲット検出に適したモデルをいくつか選択してテストします。スループット性能データも明らかに向上していることがわかります。最適化後、ResNet 50のパフォーマンスは元の1.98倍までアップします。

例2：ディープラーニングフレームワークをデプロイする PyTorch*

デプロイ手順

1. CVMにPython3.6以降のバージョンをインストールします。ここでは、Python3.7を例とします。
2. Intel® Extension for PyTorc 公式github repo に移動し、インストールガイドに記載されている情報に従って、PyTorchおよびntel® Extension for PyTorch (IPEX)のコンパイルとインストールを行います。

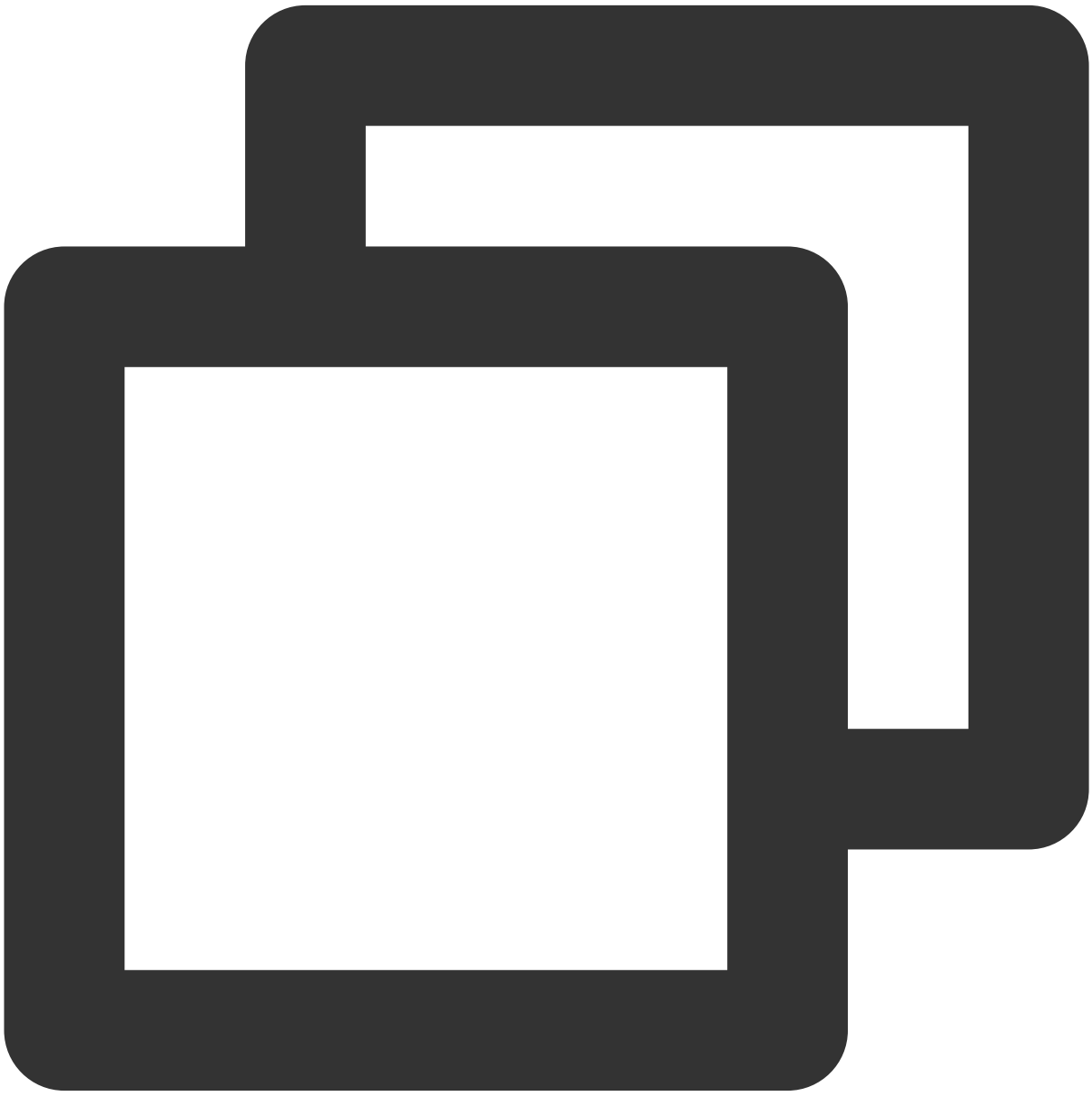
ランタイム最適化パラメータを設定

第2世代Intel®Xeon®スケーラブルプロセッサCascade LakeのPyTorchおよびIPEXでは、演算性能を最大限にアップさせるため、AVX-512命令セットの最適化が自動的に有効になります。

この手順に従って、ランタイムパラメータの最適化方法を設定できます。パラメータ最適化の設定手順の詳細については、Maximize Performance of Intel® Software Optimization for PyTorch* on CPU をご参照ください。

Batch inference：BatchSize >1に設定し、1秒あたりに処理できる入力テンソルの総数を測定します。通常の状況では、Batch Inference方式は、同じCPU socketですべての物理コアを使用することによって最高のパフォーマンスを実現できます。

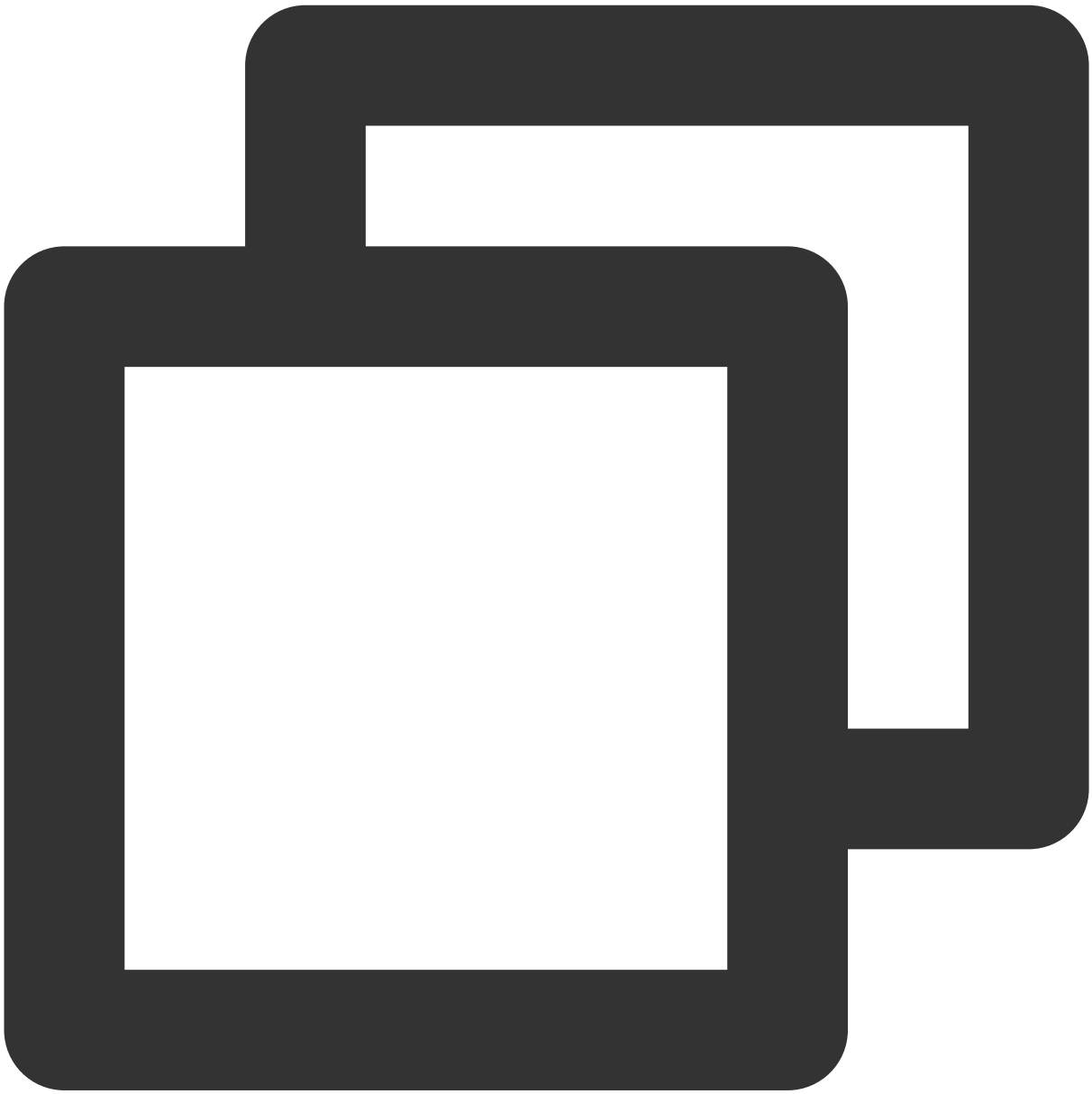
On-line Inference（リアルタイム推論とも呼びます）：BatchSize = 1に設定し、単一の入力テンソルの処理（バッチサイズは1）に必要な時間を測定します。リアルタイム推論スキームでは、マルチインスタンスを同時実行して、最高のスループットを得ることができます。
操作手順は次のとおりです。
1. 以下のコマンドを実行して、システム内の物理コアの数を取得します。



```
lscpu | grep "Core(s) per socket" | cut -d':' -f2 | xargs
```

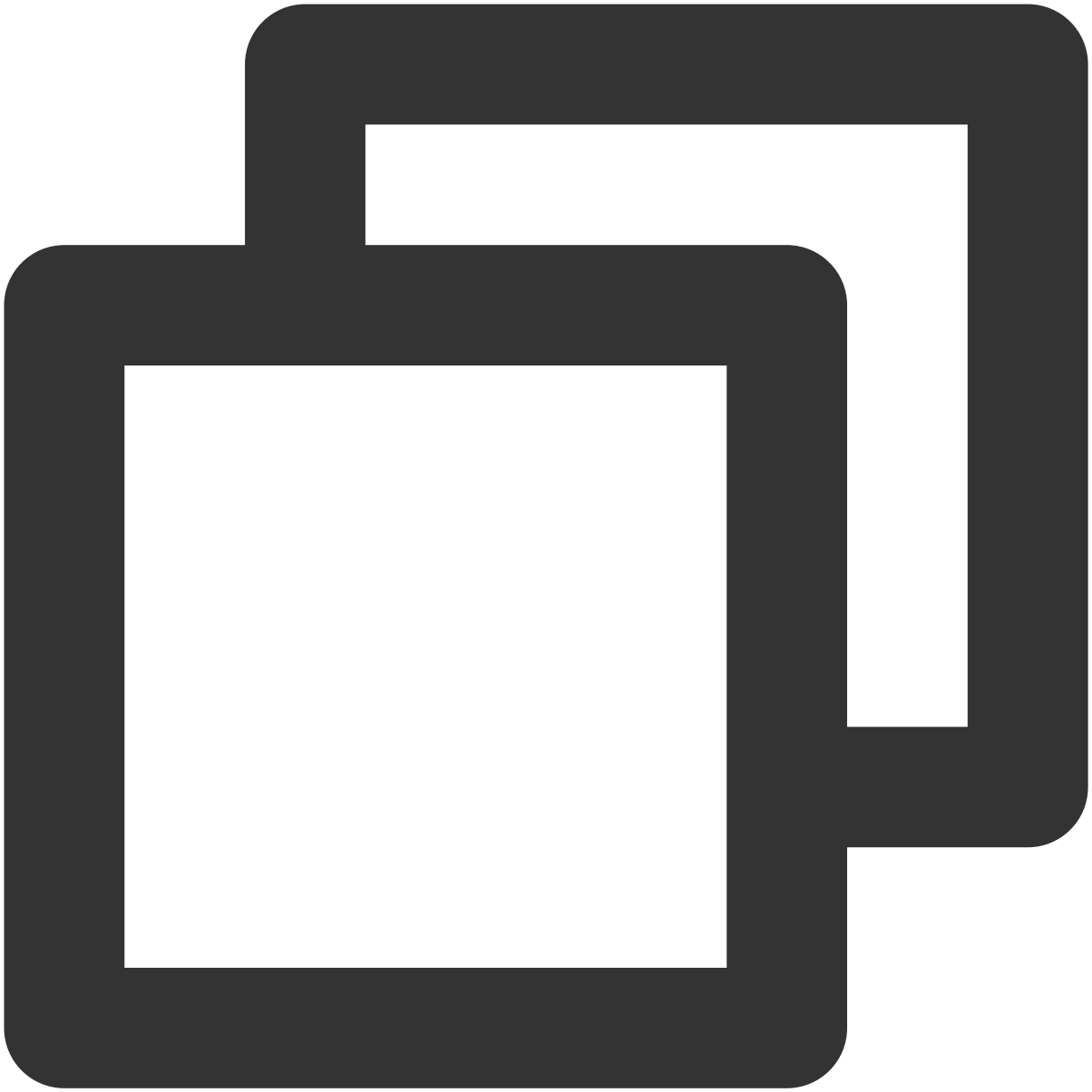
2. 最適化パラメータを設定します。以下のいずれかの方法を選択できます。

環境の実行パラメータを設定し、GNU OpenMP* Librariesを使用します。環境変数ファイルに、以下の構成を追加します。



```
export OMP_NUM_THREADS=physicalcores
export GOMP_CPU_AFFINITY="0-<physicalcores-1>"
export OMP_SCHEDULE=STATIC
export OMP_PROC_BIND=CLOSE
```

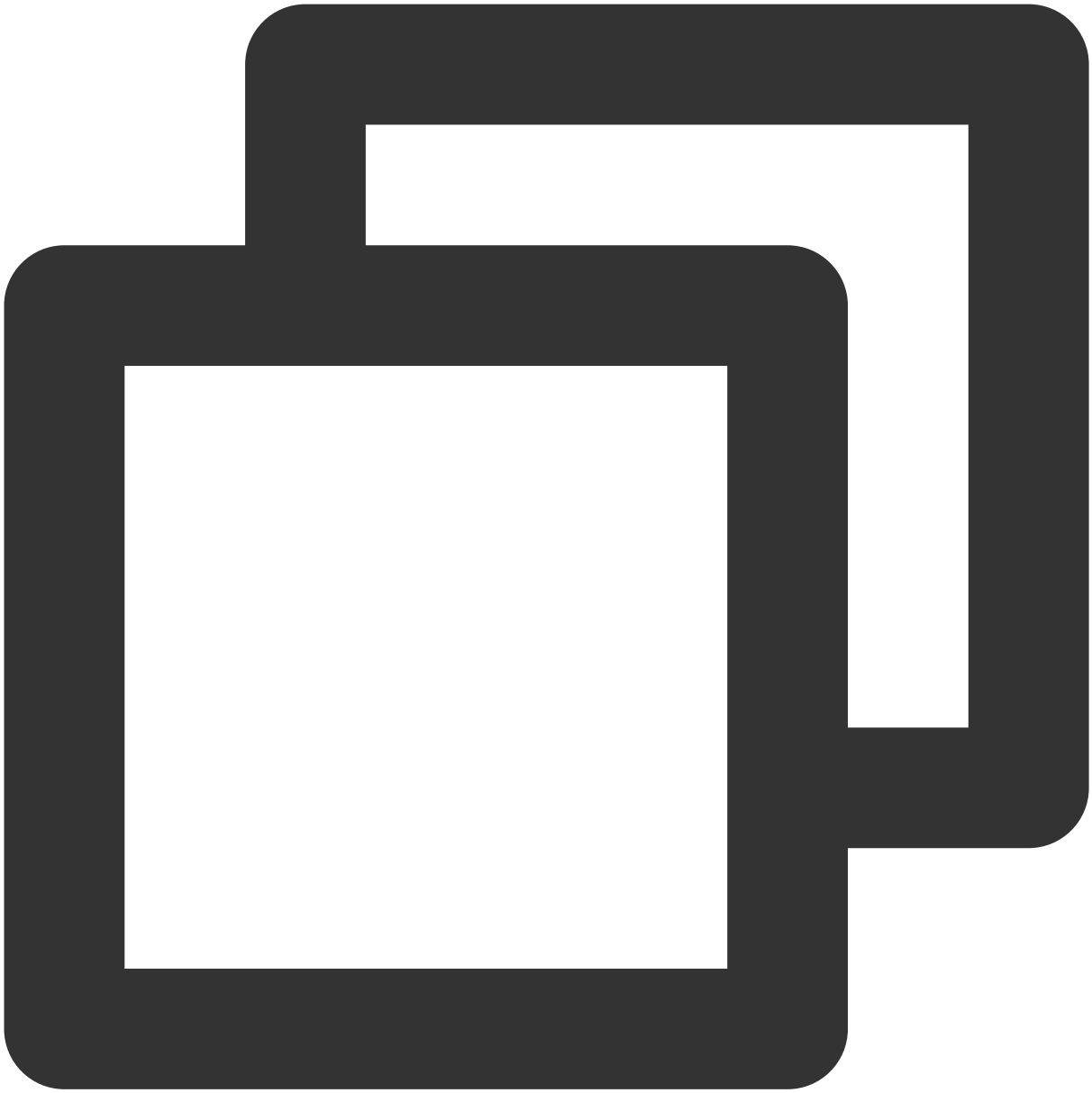
環境の実行パラメータを設定し、Inte OpenMP* Librariesを使用します。環境変数ファイルに、以下の構成を追加します。



```
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*ディープラーニングモデルの推論の実行とトレーニングの最適化の提案

モデル推論を実行する場合、Intel® Extension for PyTorchを使用してパフォーマンスを向上させることができます。サンプルコードは次のとおりです。



```
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
```

推論とトレーニングでは、jemallocを使用してパフォーマンスを最適化できます。jemallocとは、断片化の回避やスケール可能な並行処理に対応していることを強調する、 `malloc(3)` の汎用実装であり、システムにメモリア

ロケータを提供することを目的としています。jemallocは、標準のアロケータ機能を超える多くのイントロスペクション、メモリ管理、および変更機能を提供しています。 詳細については、jemalloc および サンプルコード をご参照ください。
複数のsocketを使用した分散型トレーニングの詳細については、PSSP-Transformerの分散型CPUトレーニングスクリプト をご参照ください。

パフォーマンス結果

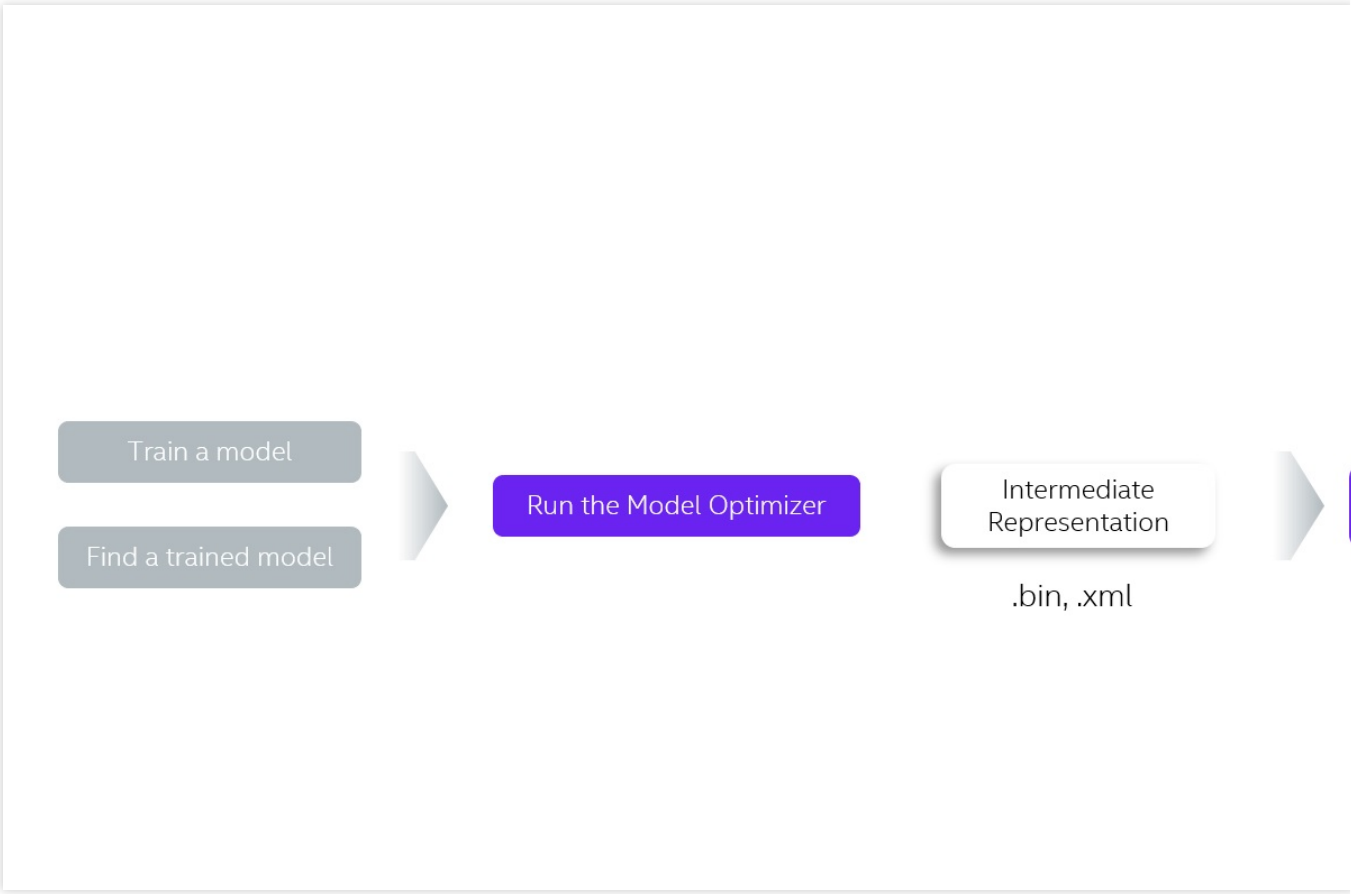
Intelの第2世代Intel®Xeon®スケーラブルプロセッサCascade Lakeをベースとする、2*CPU（28コア/CPU）および384Gメモリシナリオにおける、さまざまなモデルテストのパフォーマンスデータについては、パフォーマンステストデータ をご参照ください。実際のモデルや物理構成が異なるため、パフォーマンスデータにも差異が生じます。ここに記載されているテストデータは、あくまでも参考です。
例3： Intel®AI の低精度最適化ツールを使用してアクセラレーションする
Intel® 低精度最適化ツールは、オープンソースのPythonライブラリです。これは、シンプルで使いやすい、ニューラルネットワークフレームワーク間の低精度定量的推論インターフェースを提供することを目的としています。ユーザーは、インターフェースを呼び出すだけでモデルを定量化し、生産性を向上させることによって、第3世代Intel® Xeon® DL Boostスケーラブルプロセッサプラットフォームでの推論性能をアクセラレーションすることができます。使用法の詳細については、Intel® 低精度定量化ツールコードライブラリをご参照ください。

サポートされているニューラルネットワークフレームワークバージョン

Intel®低精度最適化ツールは以下をサポートしています。
Intel® 最適化したTensorFlow* `v1.15.0` 、 `v1.15.0up1` 、 `v1.15.0up2` 、 `v2.0.0` 、 `v2.1.0` 、 `v2.2.0` 、 `v2.3.0` および `v2.4.0` 。
Intel® 最適化したPyTorch `v1.5.0+cpu` および `v1.6.0+cpu` 。
Intel® 最適化したMXNet `v1.6.0` 、 `v1.7.0` およびONNX-Runtime `v1.6.0` 。

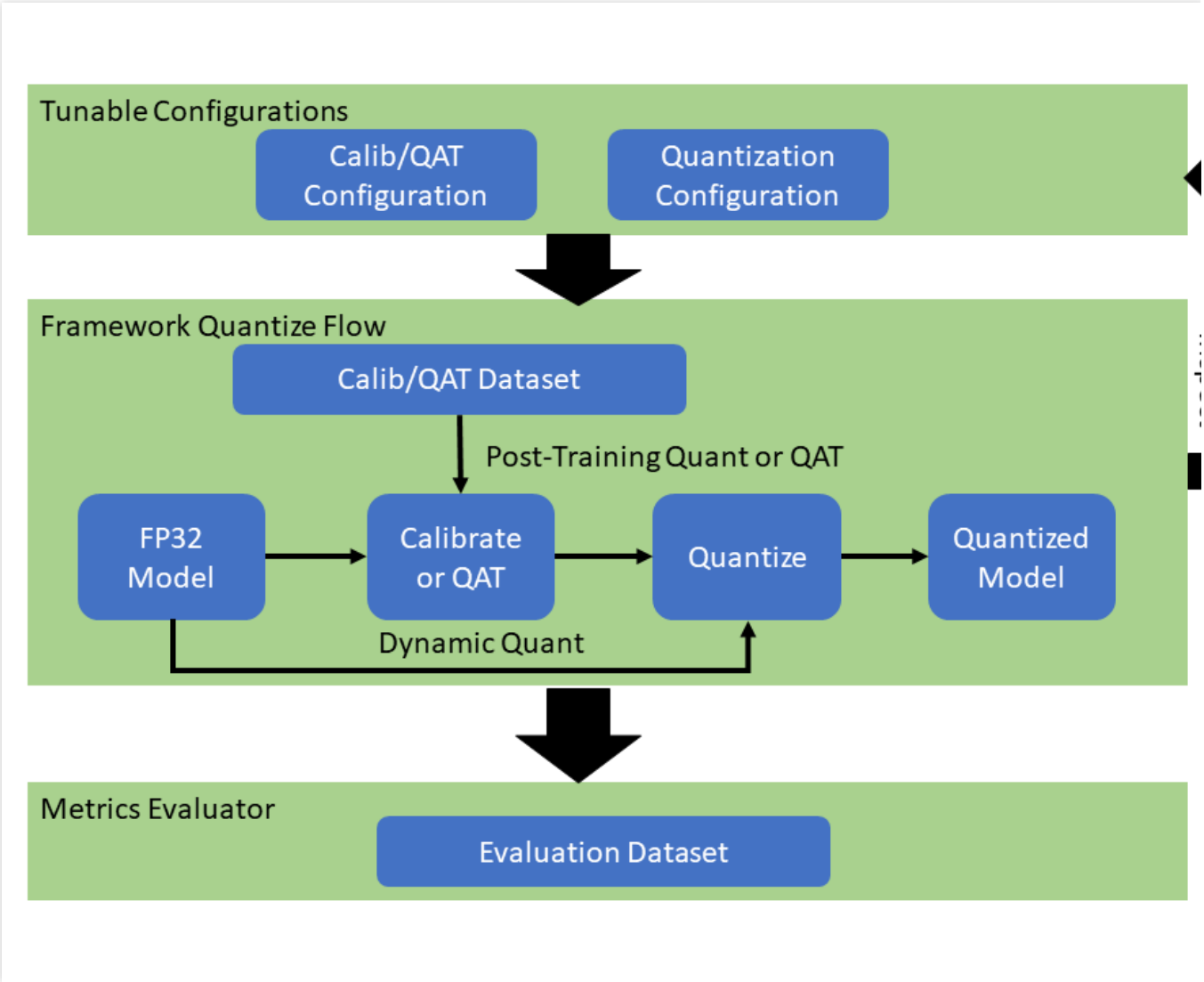
実装フレームワーク

Intel® 低精度最適化ツールの実装フレームワーク略図は次のとおりです。



ワークフロー

Intel® 低精度最適化ツールのワークフローチャートは次のとおりです。



定量的モデルのパフォーマンスと精度の例

Intel® 低精度最適化ツールによって定量化されたモデルの第2世代Intel®Xeon®スケーラブルプロセッサCascade Lakeにおいて得られるパフォーマンスと精度の一部は次のとおりです。

Framework	Version	Model	Accuracy			Performance speed up
			INT8 Tuning Accuracy	FP32 Accuracy Baseline	Acc Ratio [(INT8-FP32)/FP32]	Realtime La Ratio[FP32/
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

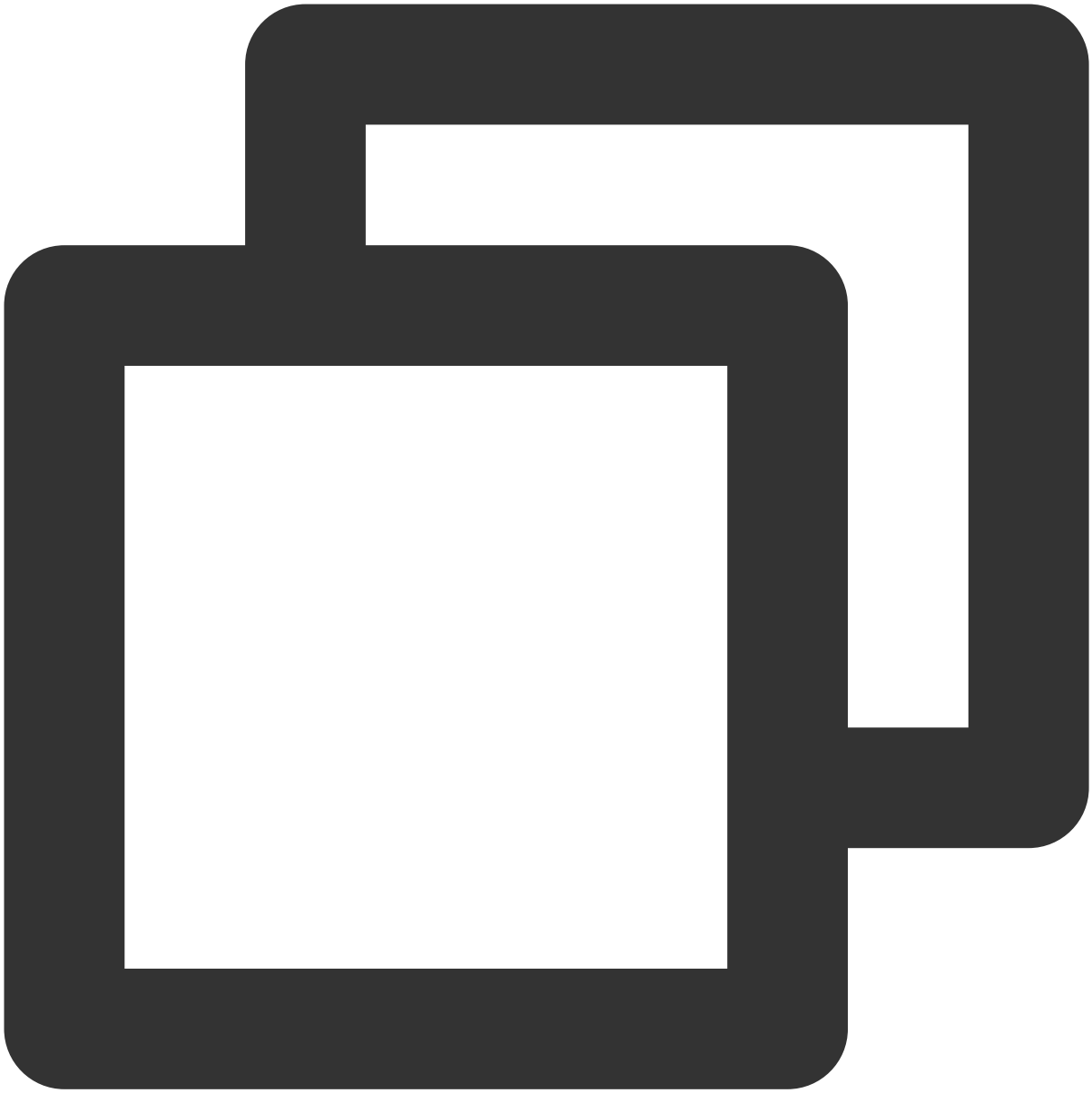
Framework	Version	Model	Accuracy			Performa speed up
			INT8 Tuning Accuracy	FP32 Accuracy Baseline	Acc Ratio [(INT8-FP32)/FP32]	Realtime Ratio[FP
pytorch	1.5.0+cpu	resnet50	75.96%	76.13%	-0.23%	2.46x
pytorch	1.5.0+cpu	resnext101_32x8d	79.12%	79.31%	-0.24%	2.63x
pytorch	1.6.0a0+24aac32	bert_base_mrpc	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

説明：
表のPyTorchとTensorflowはどちらも、Intelをベースとして最適化されたフレームワークです。完全にサポートされている定量的モデルのリストについては、オンラインドキュメント をご参照ください。

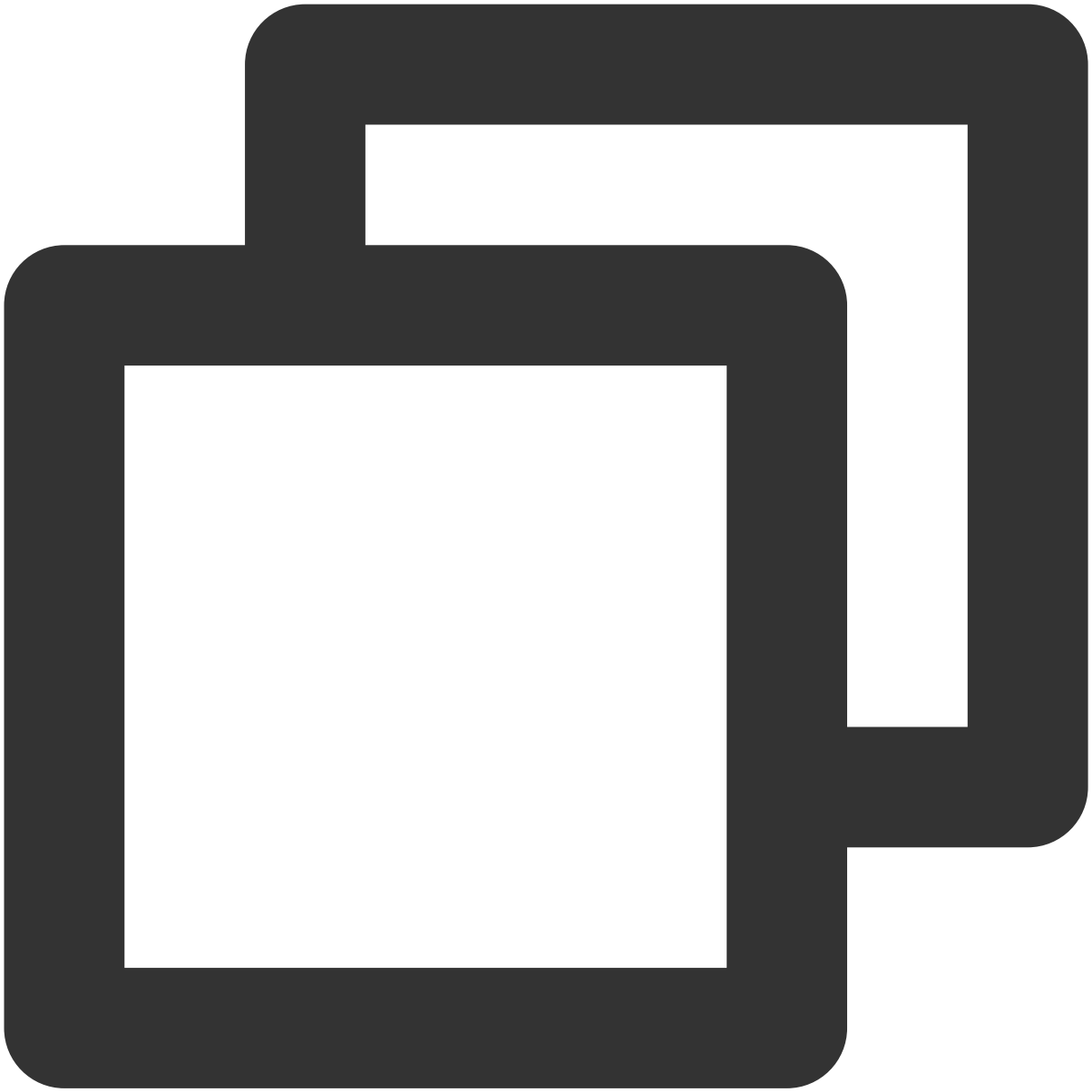
Intel®低精度最適化ツールのインストールと使用例

1. 以下のコマンドを順番に実行し、anacondaを使用してlpotという名前のpython3.x仮想環境を構築します。ここでは、python 3.7を例とします。



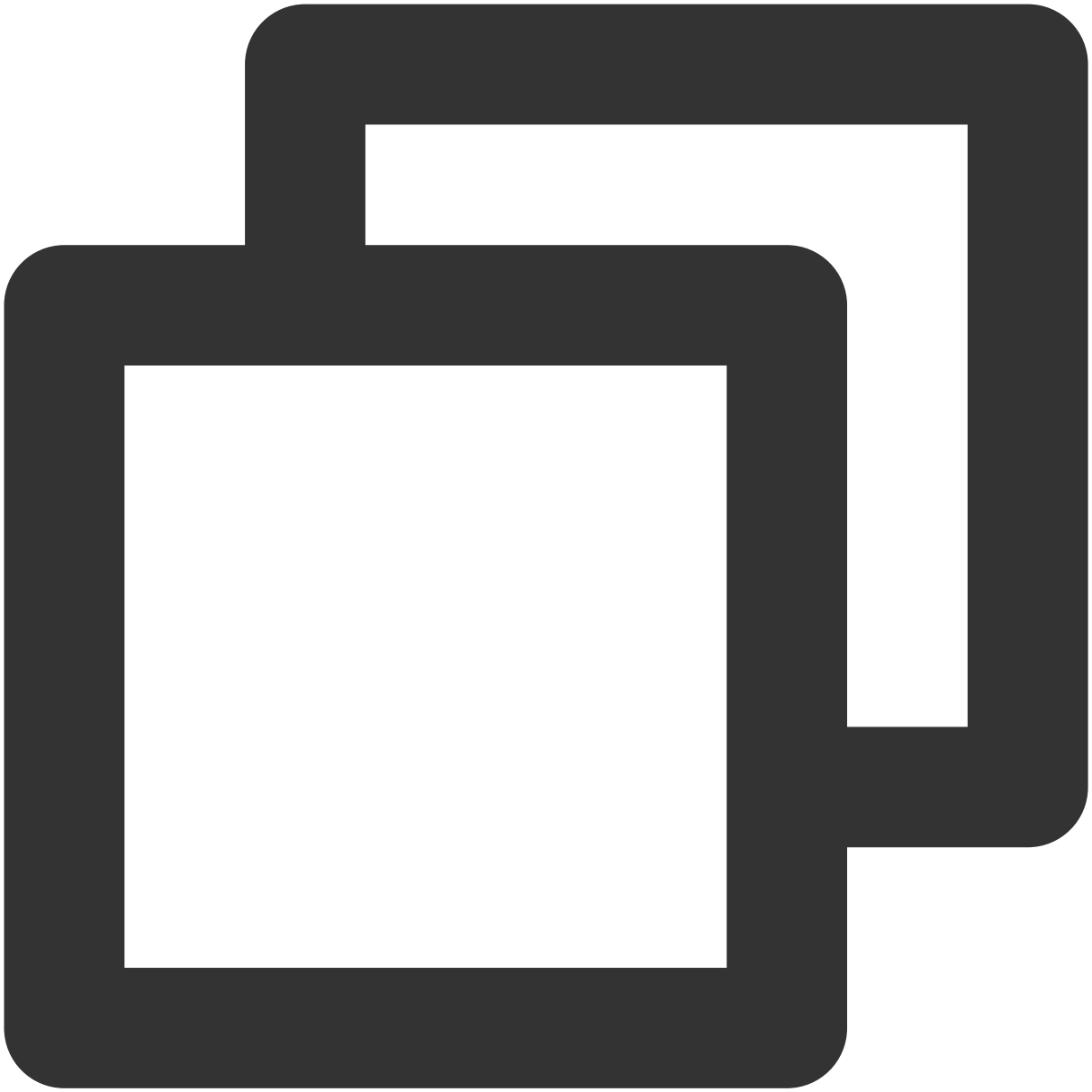
```
conda create -n lpot python=3.7
conda activate lpot
```

2. lpotをインストールするには、以下の2つの方法があります。
以下のコマンドを実行して、バイナリーファイルからインストールします。



```
pip install lpot
```

以下のコマンドを実行して、ソースからインストールします。

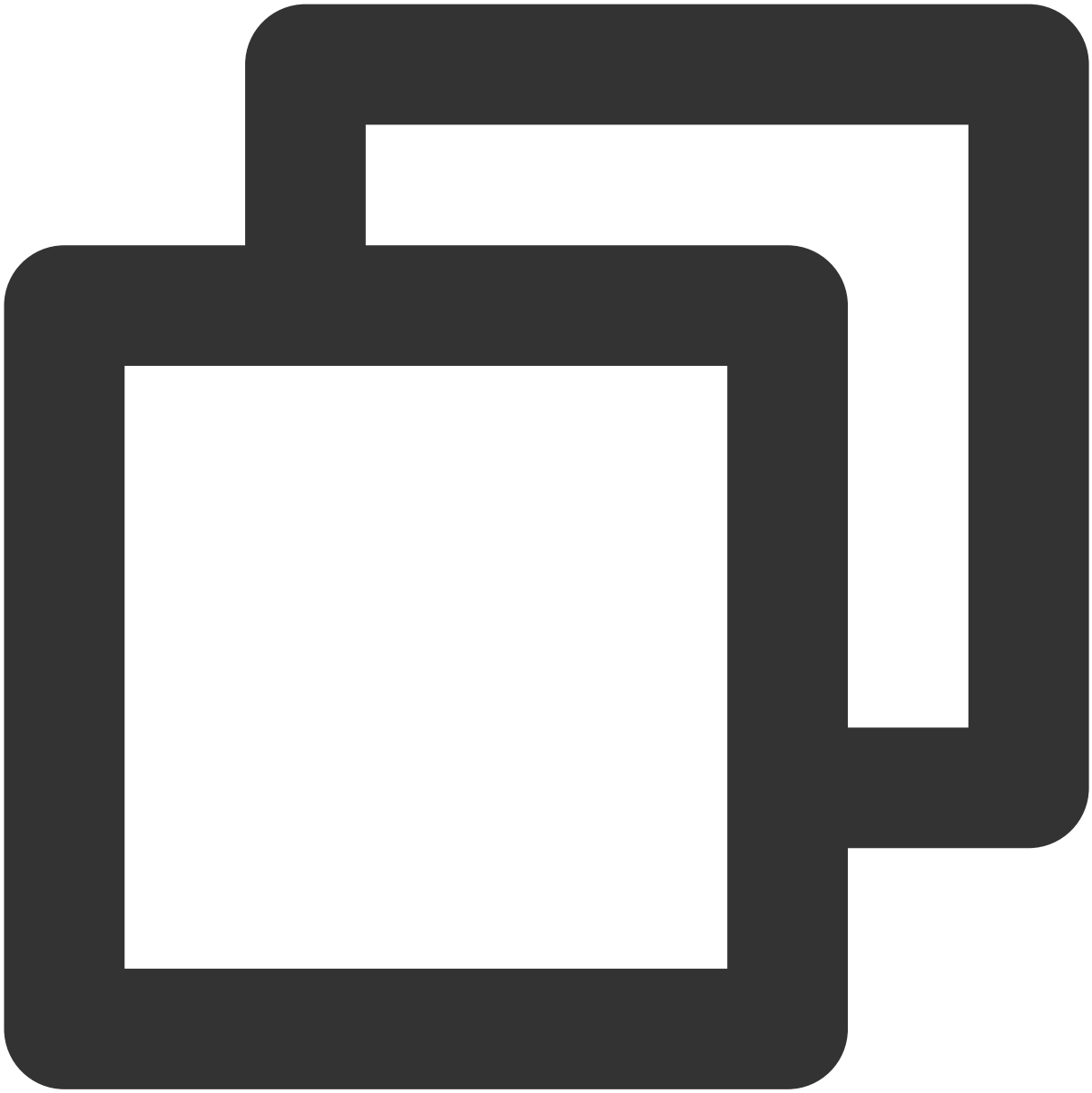


```
git clone https://github.com/intel/lpot.git
cd lpot
pip install -r requirements.txt
python setup.py install
```

3. TensorFlow ResNet50 v1.0を定量化します。ここでは、ResNet50 v1.0を例として、このツールを使用して定量化する方法を説明します。

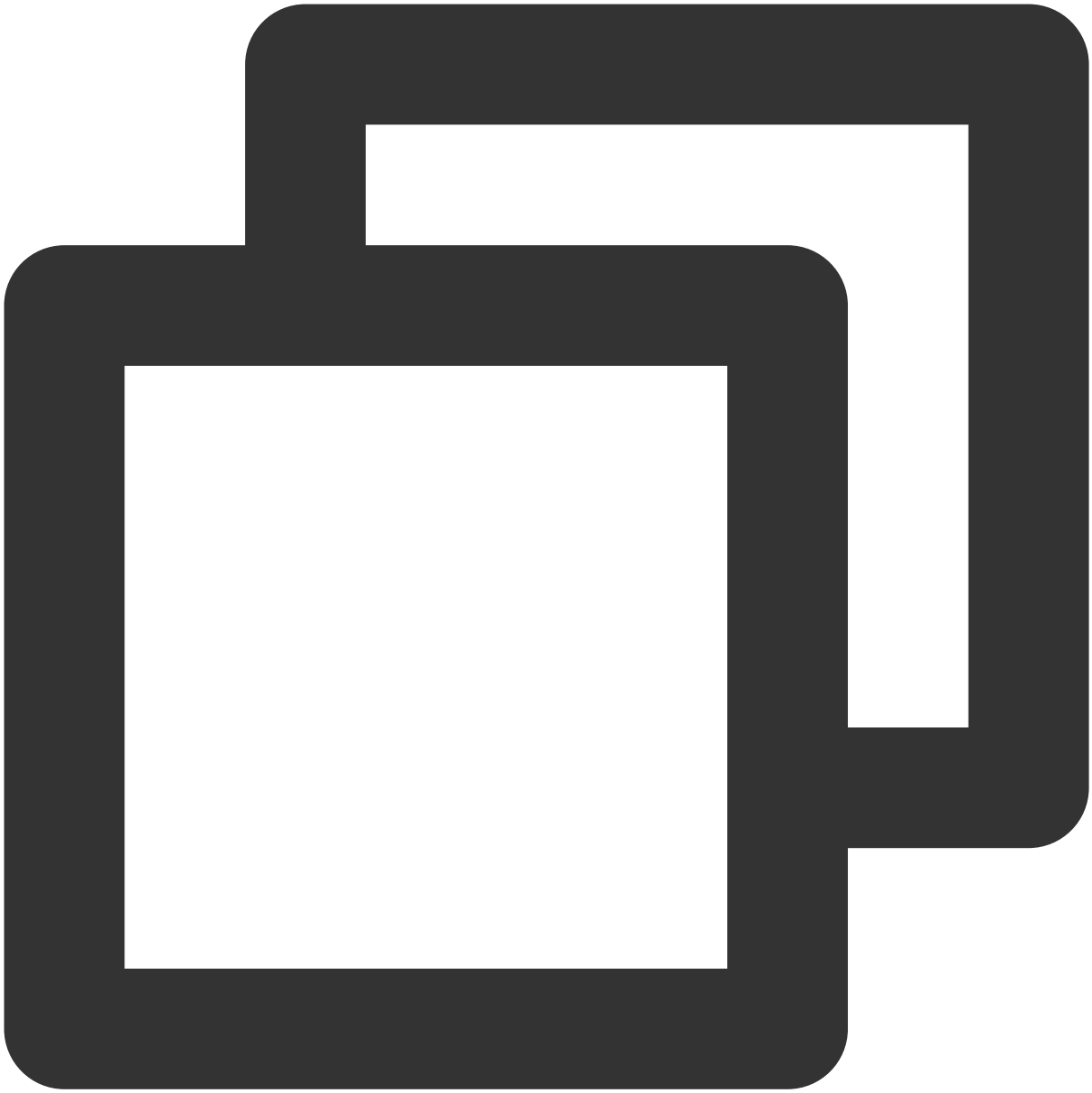
3.1 データセットの準備をします。

以下のコマンドを実行して、ImageNet validationデータセットをダウンロードして解凍します。



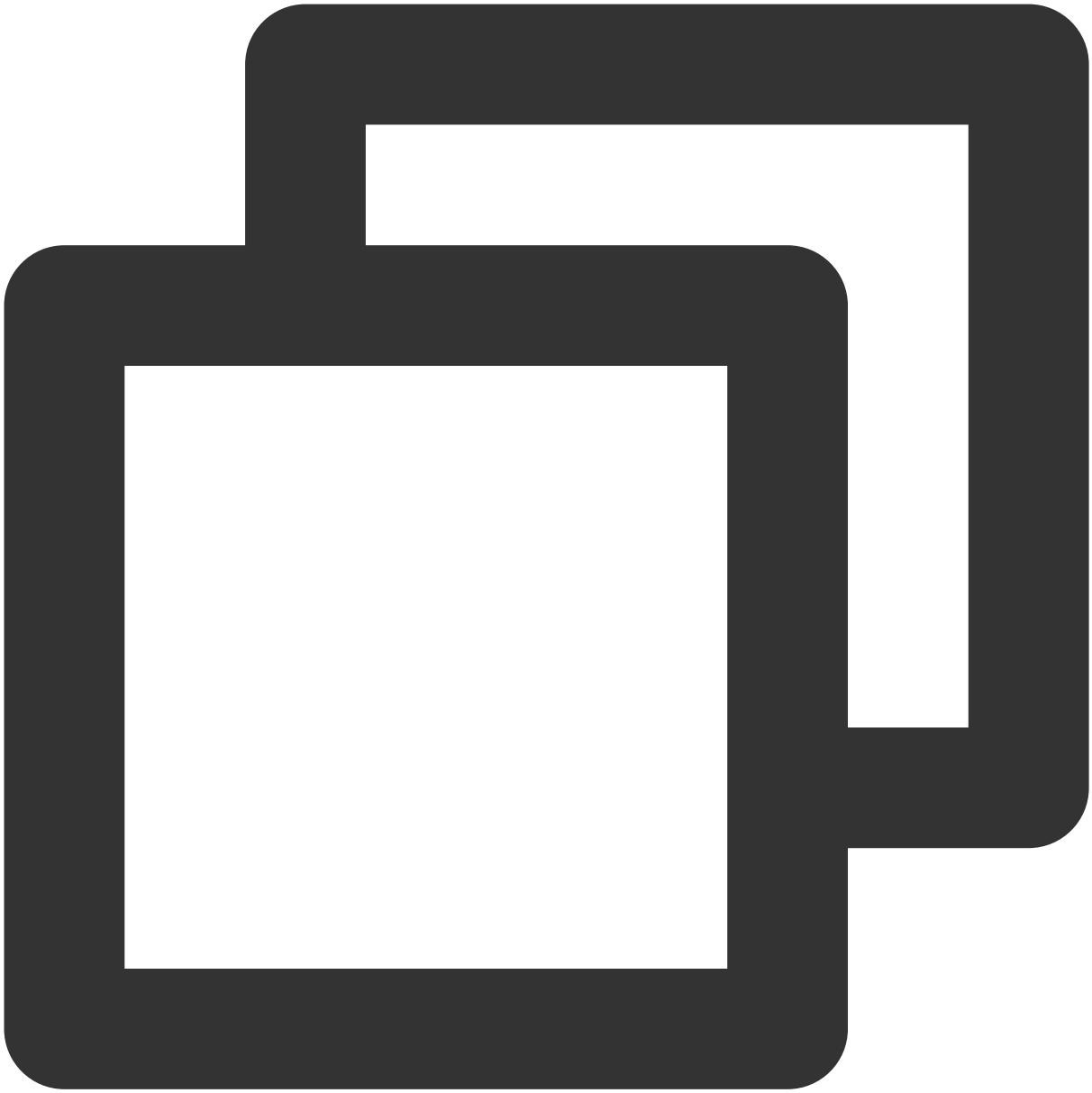
```
mkdir -p img_raw/val && cd img_raw
wget http://www.image-net.org/challenges/LSVRC/2012/dd31405981
ef5f776aa17412e1f0c112/ILSVRC2012_img_val.tar
tar -xvf ILSVRC2012_img_val.tar -C val
```

以下のコマンドを実行して、imageファイルをlabelで分類されたサブディレクトリに移動します。



```
cd val
wget -qO -https://raw.githubusercontent.com/soumith/
imagenetloader.torch/master/valprep.sh | bash
```

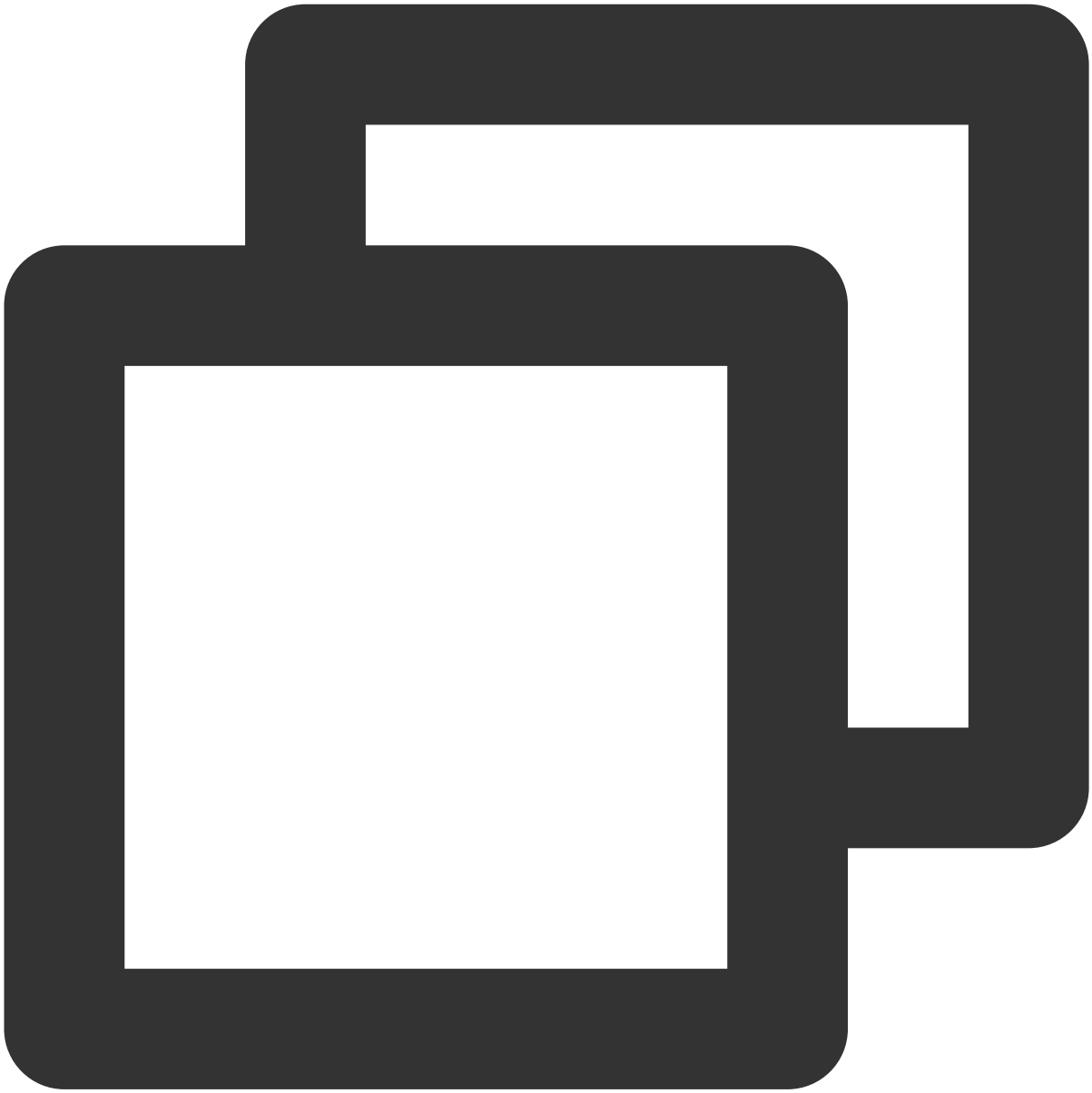
以下のコマンドを実行して、スクリプト prepare_dataset.shを使用して、元のデータをTFrecord形式に変換します。



```
cd examples/tensorflow/image_recognition
bash prepare_dataset.sh --output_dir=./data --raw_dir=/PATH/TO/img_raw/val/
--subset=validation
```

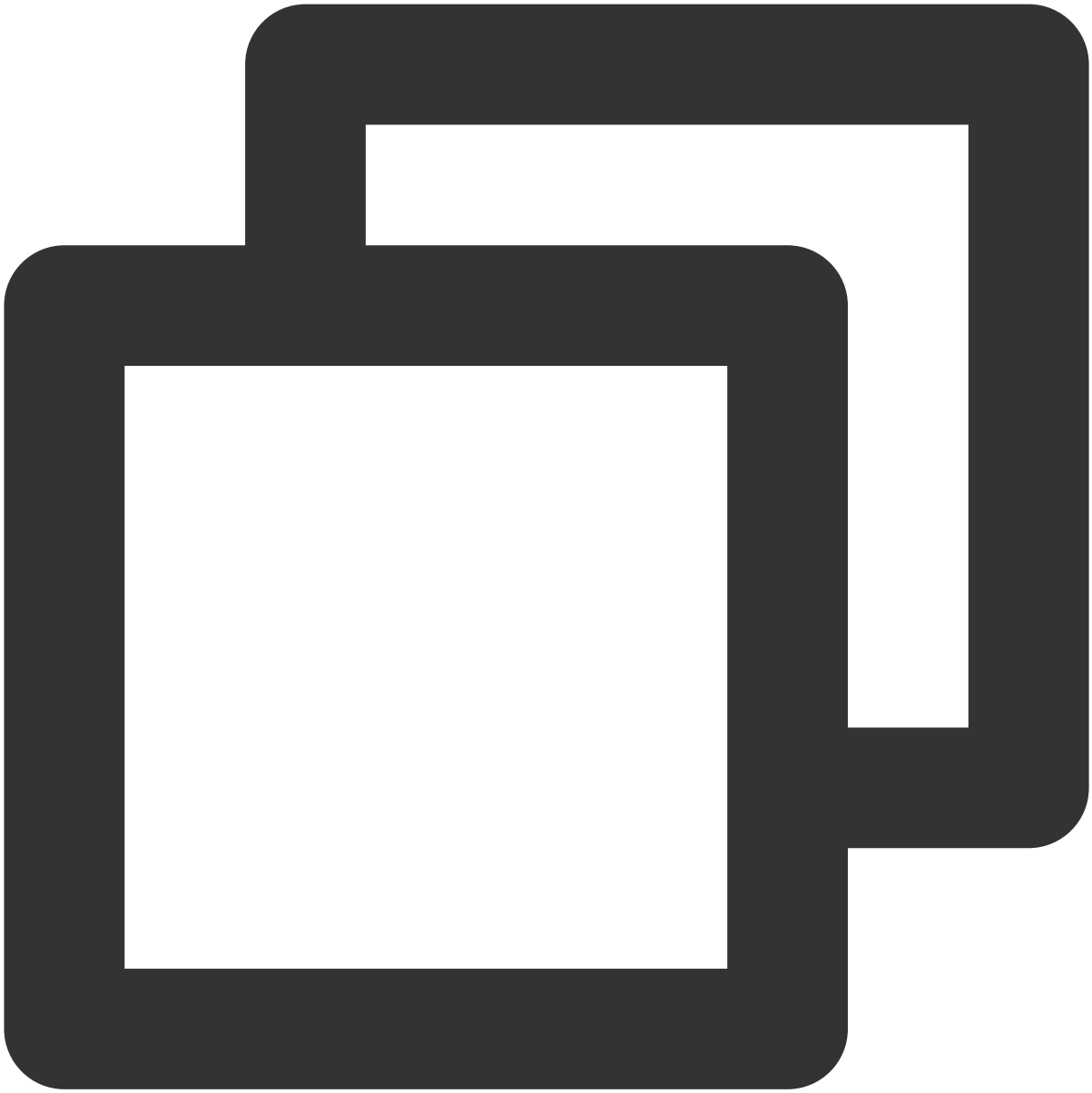
データセットの詳細情報については、Prepare Dataset をご参照ください。

3.2 以下のコマンドを実行して、モデルを準備します。



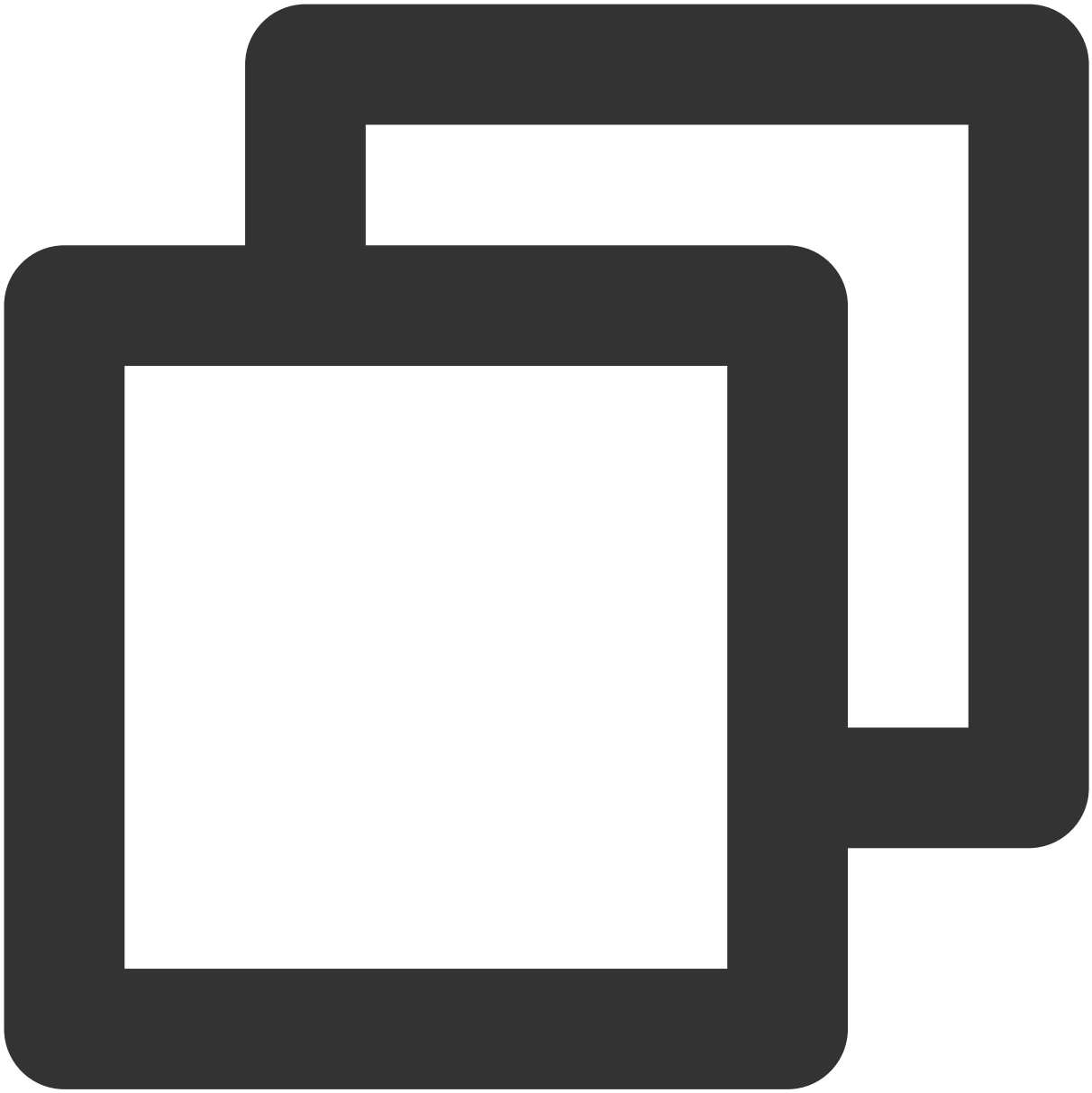
```
wget https://storage.googleapis.com/intel-optimized-tensorflow/
 models/v1_6/resnet50_fp32_pretrained_model.pb
```

3.3 以下のコマンドを実行して、Tuningを実行します。
ファイル `examples/tensorflow/image_recognition/resnet50_v1.yaml` を変更して、 `quantization\\calibration` 、 `evaluation\\accuracy` 、 `evaluation\\performance` という3つの部分のデータセットパスがユーザーのローカルの実際のパス、つまりデータセットの準備段階で生成されたTFrecordデータが所在する場所を指すようにします。詳細については、ResNet50 V1.0をご参照ください。



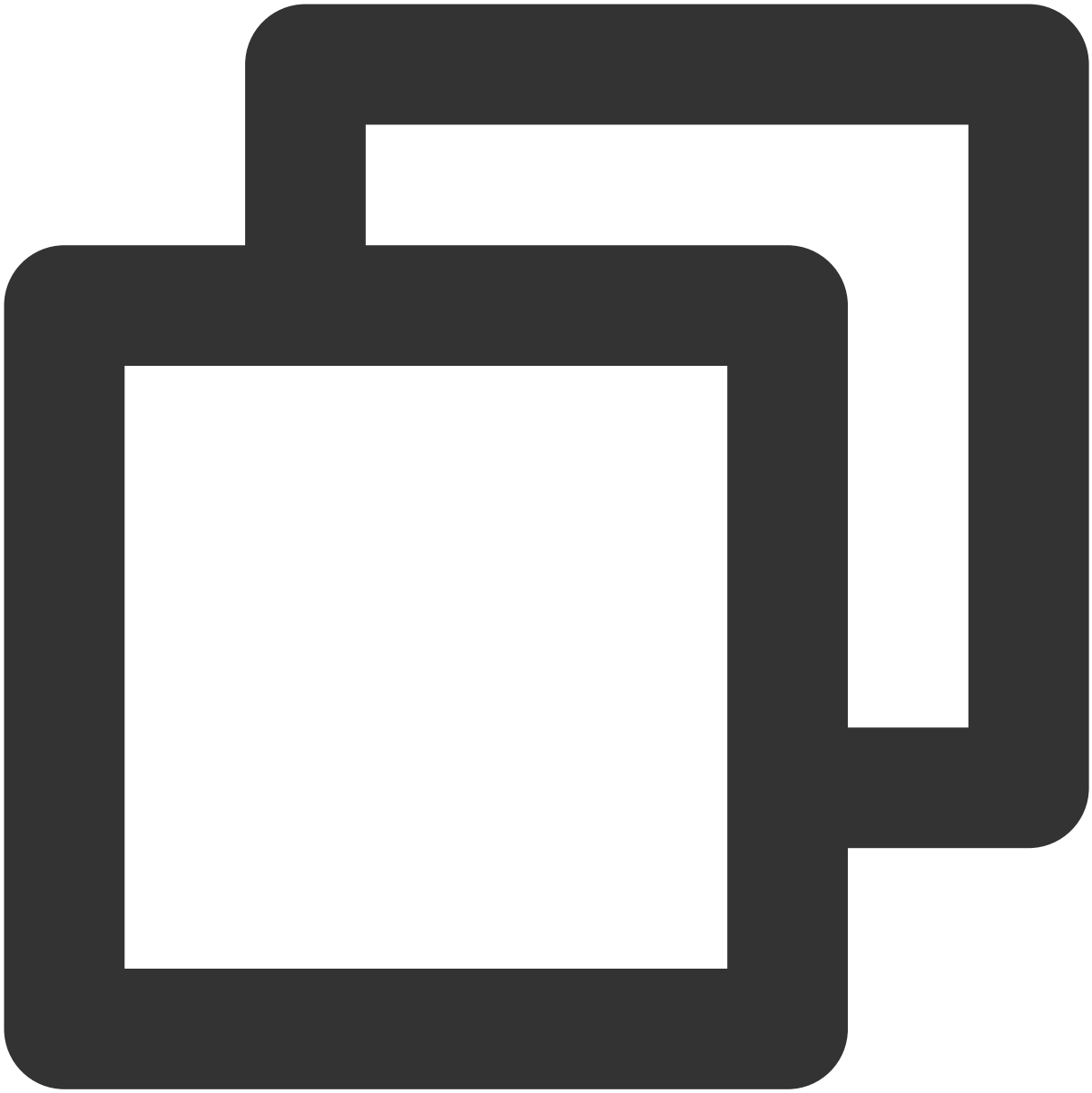
```
cd examples/tensorflow/image_recognition
bash run_tuning.sh --config=resnet50_v1.yaml \\
--input_model=/PATH/TO/resnet50_fp32_pretrained_model.pb \\
--output_model=./lpot_resnet50_v1.pb
```

3.4 以下のコマンドを実行して、Benchmarkを実行します。



```
bash run_benchmark.sh --input_model=./lpot_resnet50_v1.pb
--config=resnet50_v1.yaml
```

出力結果は次のとおりです。パフォーマンスデータはあくまでも参考です：



```
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
```

例4： Intel® Distribution of OpenVINO™ Toolkit を使用して推論のアクセラレーションを行う

Intel® Distribution of OpenVINO™ Toolkitとは、コンピュータビジョンやその他のディープラーニングアプリケーションのデプロイを高速化できるツールキットであり、Intelプラットフォームのさまざまなアクセラレーター（CPU、GPU、FPGAおよびMovidiusのVPUを含む）をサポートしてディープラーニングを行うとともに、異種ハードウェアを直接サポートすることができます。

Intel® Distribution of OpenVINO™ Toolkitは、TensorFlow*、PyTorch*などを介してトレーニングされたモデルを最適化できます。これには、モデルオプティマイザー、推論エンジン、Open Model Zoo、トレーニング後の最適化ツール（Post-training Optimization Tool）など、一連のデプロイツールが含まれます。

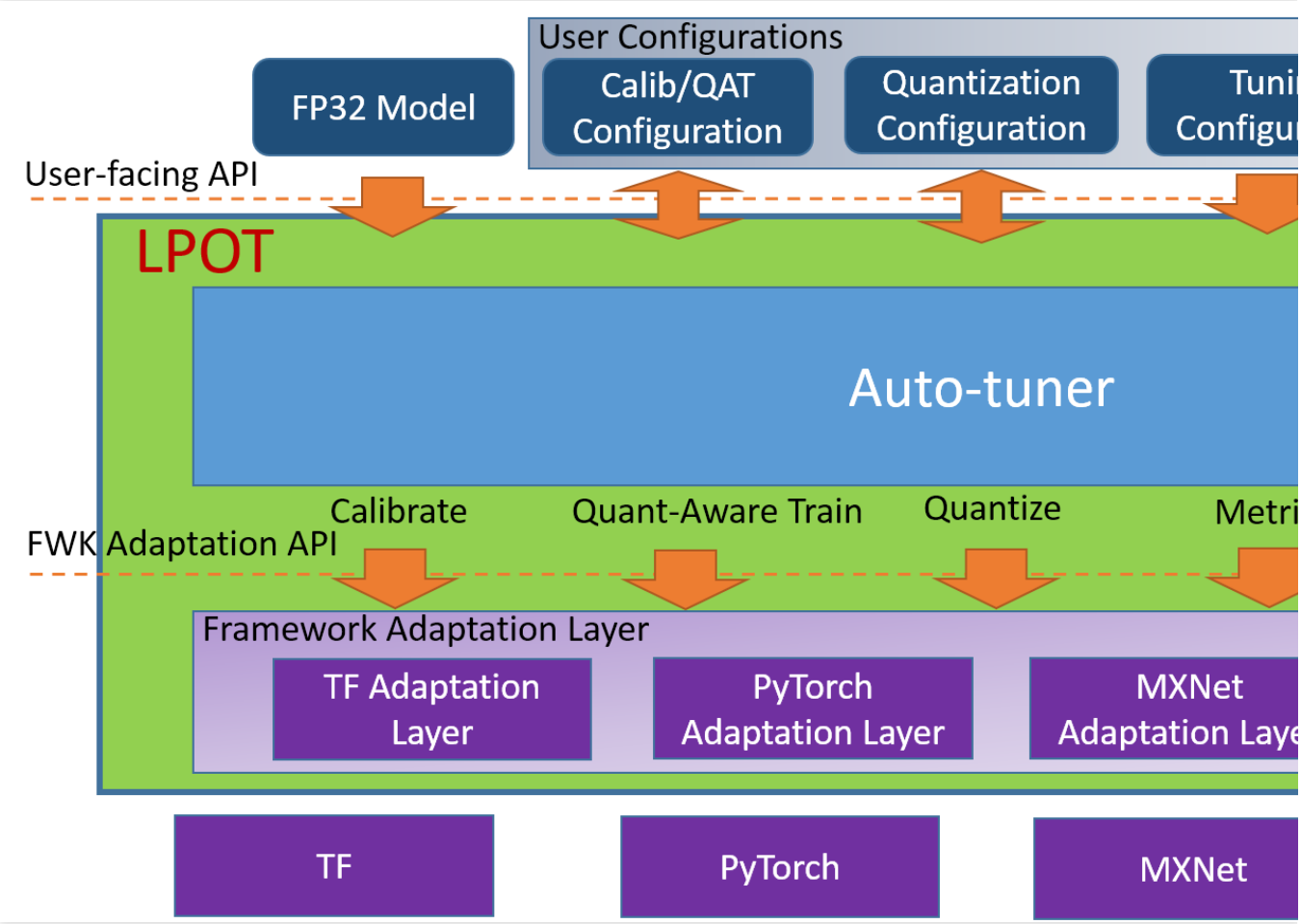
モデルオプティマイザー（Model optimizer）：Caffe*、TensorFlow* 、PyTorch*およびMxnet*など、さまざまなフレームワークによってトレーニングされたモデルを中間表現(IR)に変換します。

推論エンジン（Inference Engine）：変換されたIRをCPU、GPU、FPGAおよびVPUなどのハードウェアに配置して実行し、ハードウェアアクセラレーションキットを自動的に呼び出して推論性能のアクセラレーションを行います。

Intel® Distribution of OpenVINO™ Toolkit公式ウェブサイトに移動するか、またはオンラインドキュメントをご覧いただけば、詳細情報が確認できます。

ワークフロー

Intel® Distribution of OpenVINO™ Toolkitツールキットのワークフローチャートは次のとおりです。



Intel® Distribution of OpenVINO™ Toolkitの推論性能

The Intel® Distribution of OpenVINO™ツールは、さまざまなIntelプロセッサと高速ハードウェアで最適化を実装します。Intel®Xeon®スケーラブルプロセッサプラットフォームでは、Intel® DLBoostおよびAVX-512命令セットを使用して推論ネットワークをアクセラレーションします。

Intel® Distribution of OpenVINO™ Toolkitディープラーニング開発キット（DLDT）の使用

以下の資料をご参照ください

Intel®ディープラーニングデプロイツールキットの概要

画像分類C++の例（非同期モード）

オブジェクト検出C++の例（SSD）

自動音声認識C++の例

動作認識Python*デモンストレーション

クロスロードカメラC++デモンストレーション

姿勢推定C++デモンストレーション

Intel® Distribution of OpenVINO™ Toolkitのベンチマークテスト

詳細については、Linux*用Intel® OpenVINO™ツールキットディストリビューション版のインストールをご参照ください。

Tencent SGXコンフィデンシャル・コンピューティング環境の構築

最終更新日：：2022-12-01 14:21:34

概要

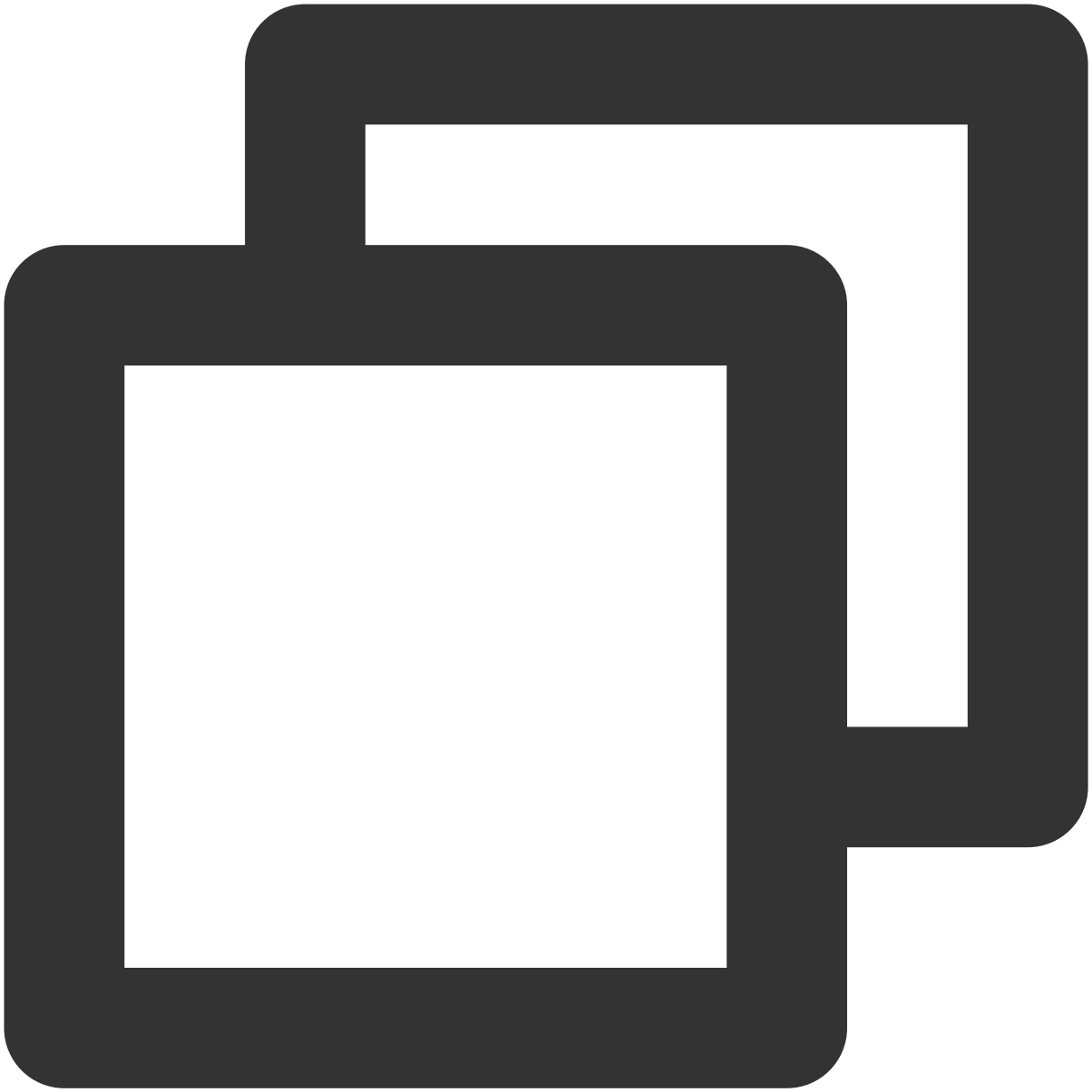
ここでは、M6ceインスタンスでTencent SGXコンフィデンシャル・コンピューティング環境を構築する方法と、Intel SGXSDKを使用してSGX機能を検証する方法をデモンストレーションします。

前提条件

M6ceインスタンス が作成され、ログインしていること。
-インスタンスの作成方法については、購入画面でインスタンスを作成 をご参照ください。
-インスタンスのログイン方法については、標準ログイン方式を使用してLinuxインスタンスにログイン（推奨）をご参照ください。
説明：
ここでの手順は、OSがTencentOS Server 3.1(TK4)のインスタンスを使用した例であり、OSのバージョンが異なると手順も異なる場合がありますので、実際の状況に応じて操作してください。

操作手順

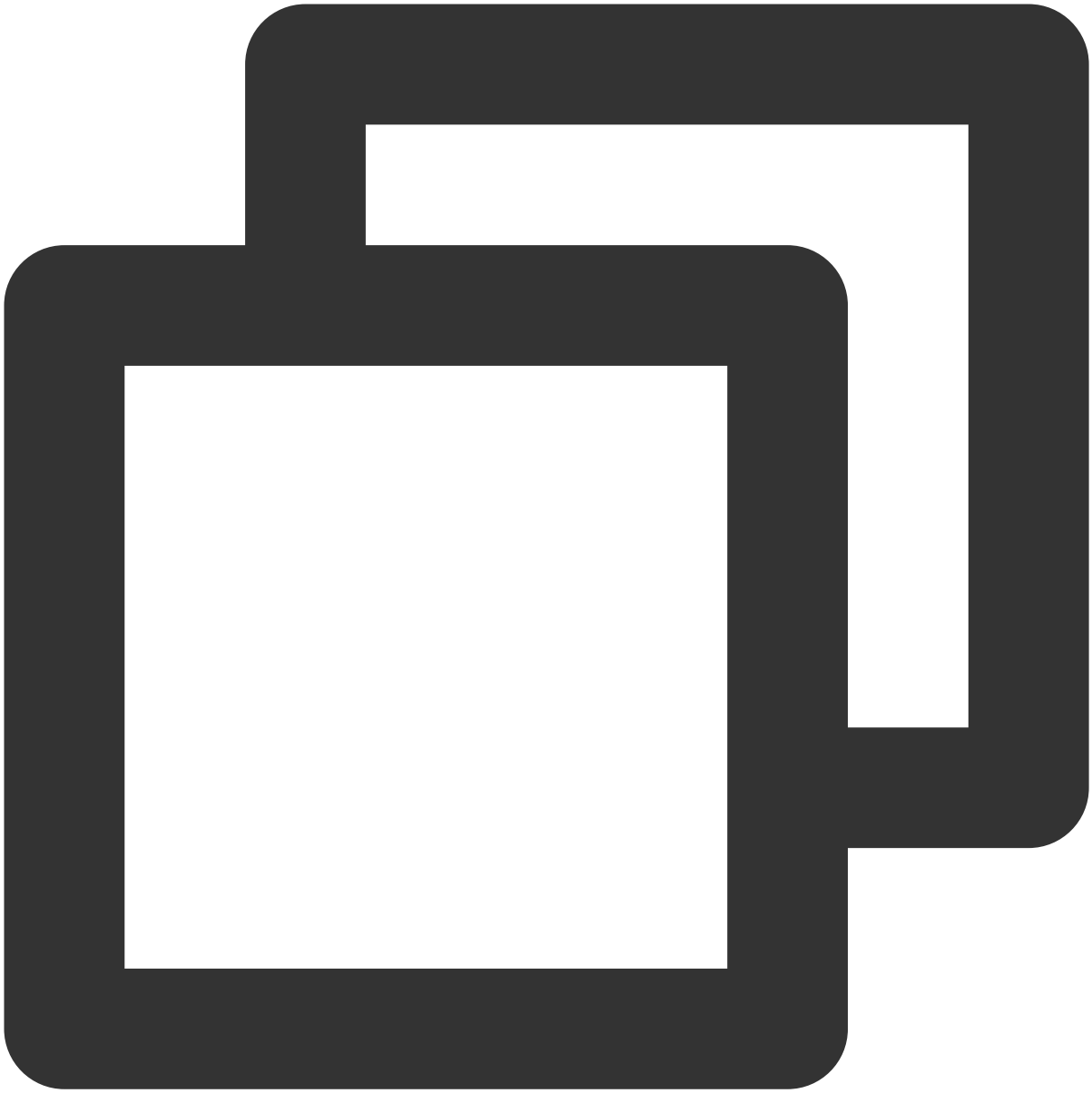
1. 次のコマンドを実行して、kernelバージョンをチェックします。



```
uname -a
```

kernelが5.4.119-19.0008より低いバージョンかどうかを確認します。

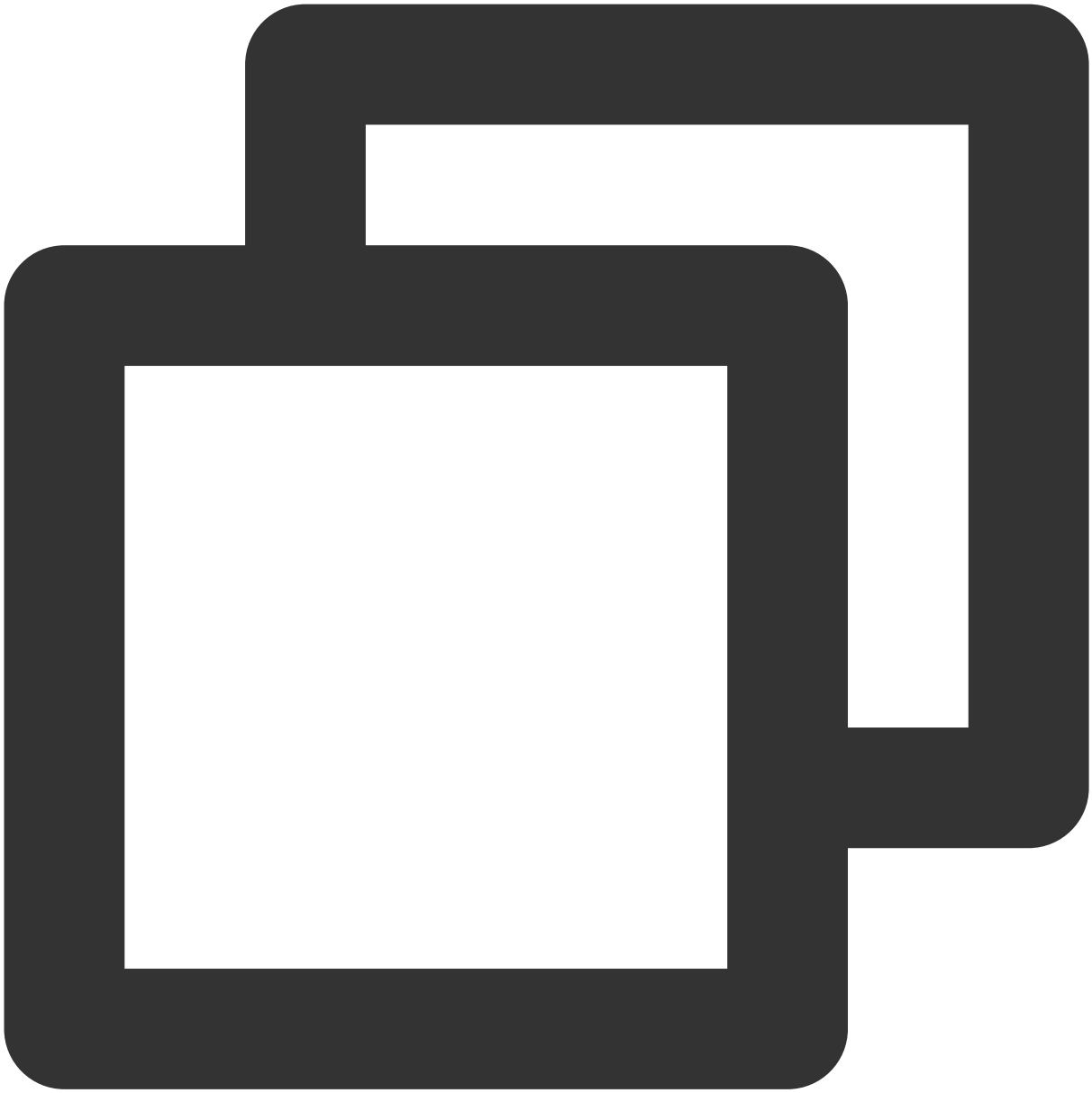
「はい」の場合は、次のコマンドを実行して、kernelを更新してください。



```
yum update kernel
```

「いいえ」の場合は、次の手順に進んでください。

2. 次のコマンドを実行して、SGX runtimeに必要なパッケージをインストールします。

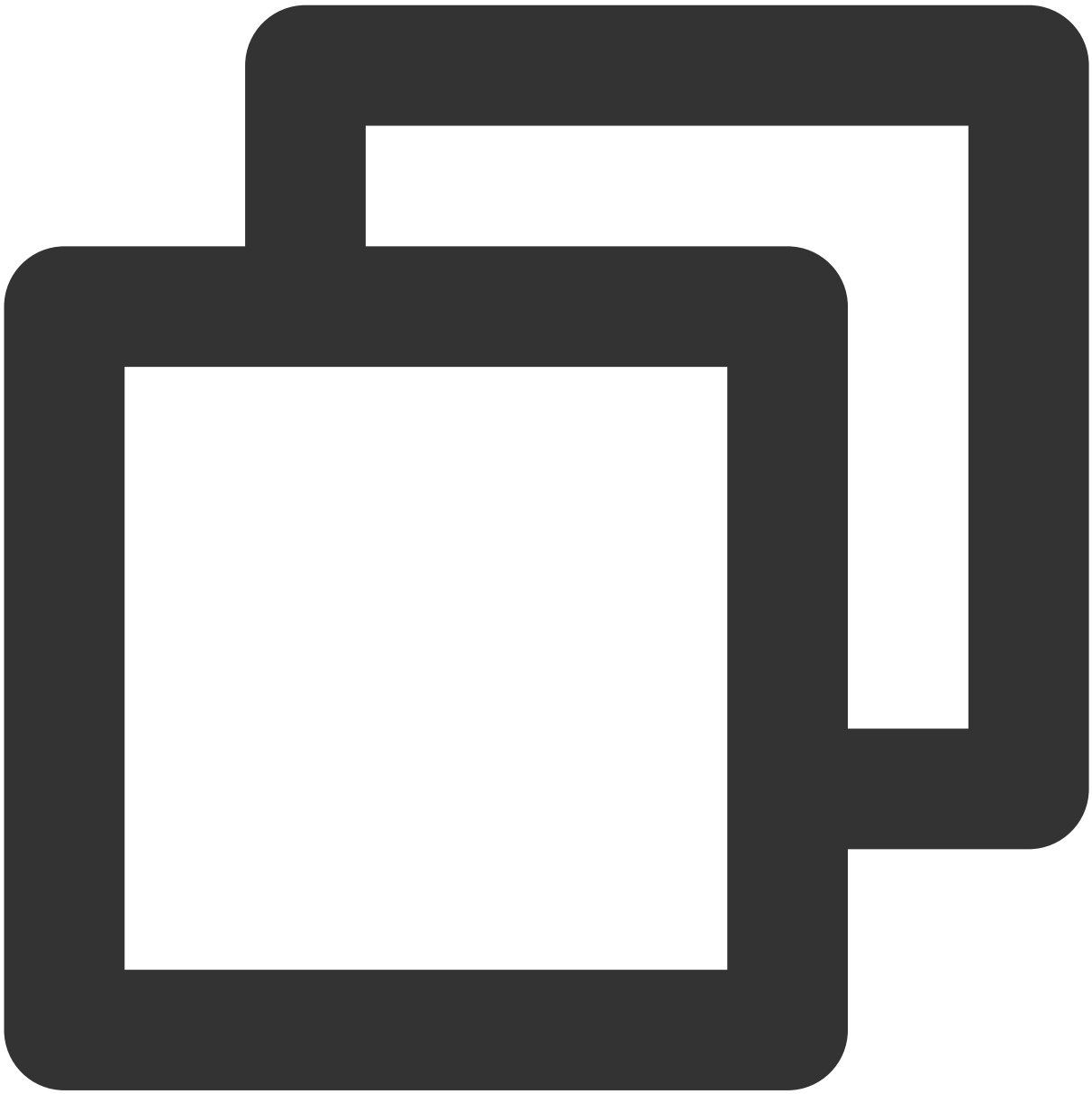


```
yum install \\
 libsgx-ae-le libsgx-ae-pce libsgx-ae-qe3 libsgx-ae-qve \\
 libsgx-aesm-ecdsa-plugin libsgx-aesm-launch-plugin libsgx-aesm-pce-plugin libsgx-a
 libsgx-dcap-default-qpl libsgx-dcap-default-qpl-devel libsgx-dcap-ql libsgx-dcap-q
 libsgx-dcap-quote-verify libsgx-dcap-quote-verify-devel 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
```

説明：

SGX AESMサービスのデフォルトのインストールディレクトリは、`/opt/intel/sgx-aesm-service` です。

3. 次のコマンドを実行して、Intel SGXSDKをインストールします。



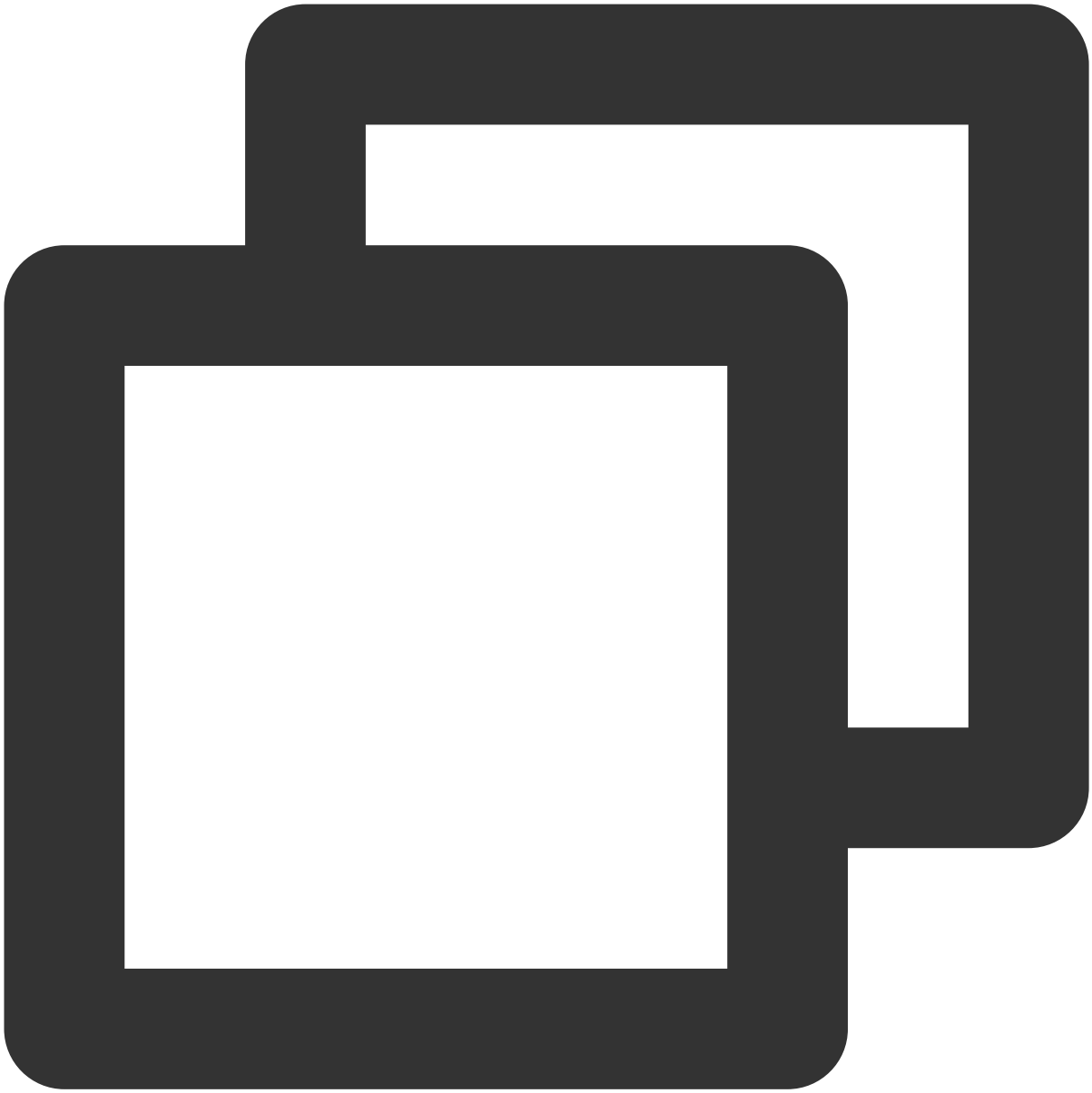
```
yum install sgx-linux-x64-sdk
```

説明：

Intel SGXSDKのデフォルトのインストールディレクトリは、/ `opt/intel/sgxsdk` です。Intel SGXSDK ユーザーマニュアルを参照して、SGXプログラムを開発することができます。

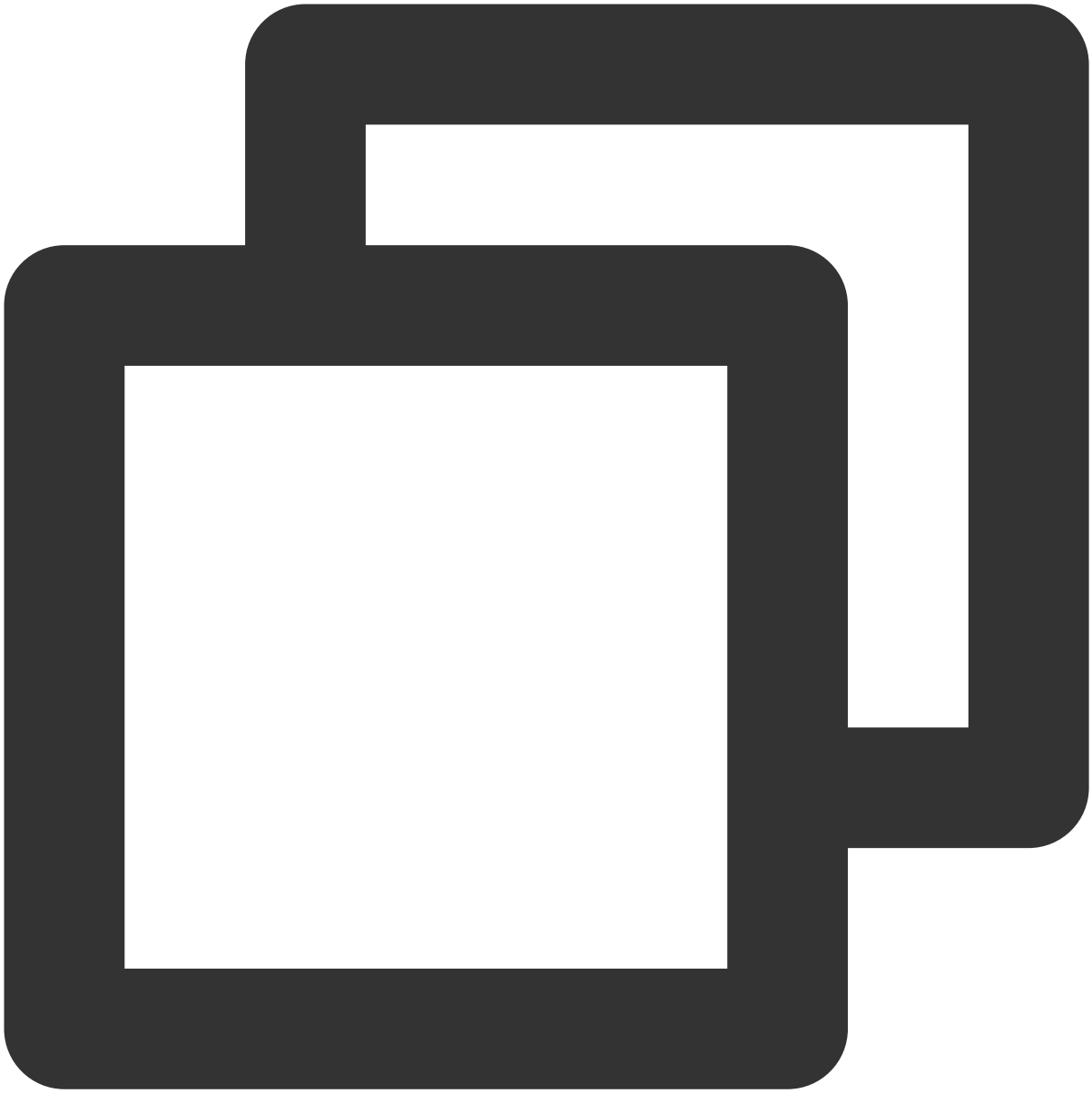
4. SGX runtimeとIntel SGXSDKのインストールが完了したら、インスタンスを再起動してください。詳細については、インスタンスの再起動 をご参照ください。

5. Tencent Cloud SGXリモートアテステーションサービスを構成します。
Tencent Cloud SGXリモートアテステーションサービスは、リージョン化デプロイを採用しています。SGX CVMインスタンスが配置されているリージョンでTencent Cloud SGXリモートアテステーションサービスにアクセスすれば、最高のカスタマーエクスペリエンスを体験できます。Intel SGXSDKをインストールすると、リモートアテステーションサービスのデフォルト構成ファイル `/etc/sgx_default_qcnl.conf` が自動的に生成されます。SGX CVMインスタンスが配置されているリージョンのTencent Cloud SGXリモートアテステーションサービスに適応するように、以下の手順に従ってこのファイルを手動で変更してください。
説明：
現在、北京、上海および広州リージョンのみで、Tencent Cloud SGXリモートアテステーションサービスがサポートされています。
Intel Ice Lakeは、Intel SGX DCAPベースのリモートアテステーション方式のみをサポートし、Intel EPIDリモートアテステーション方式はサポートしていません。
VIMエディタを使用して、 `/etc/sgx_default_qcnl.conf` を以下のように変更します。



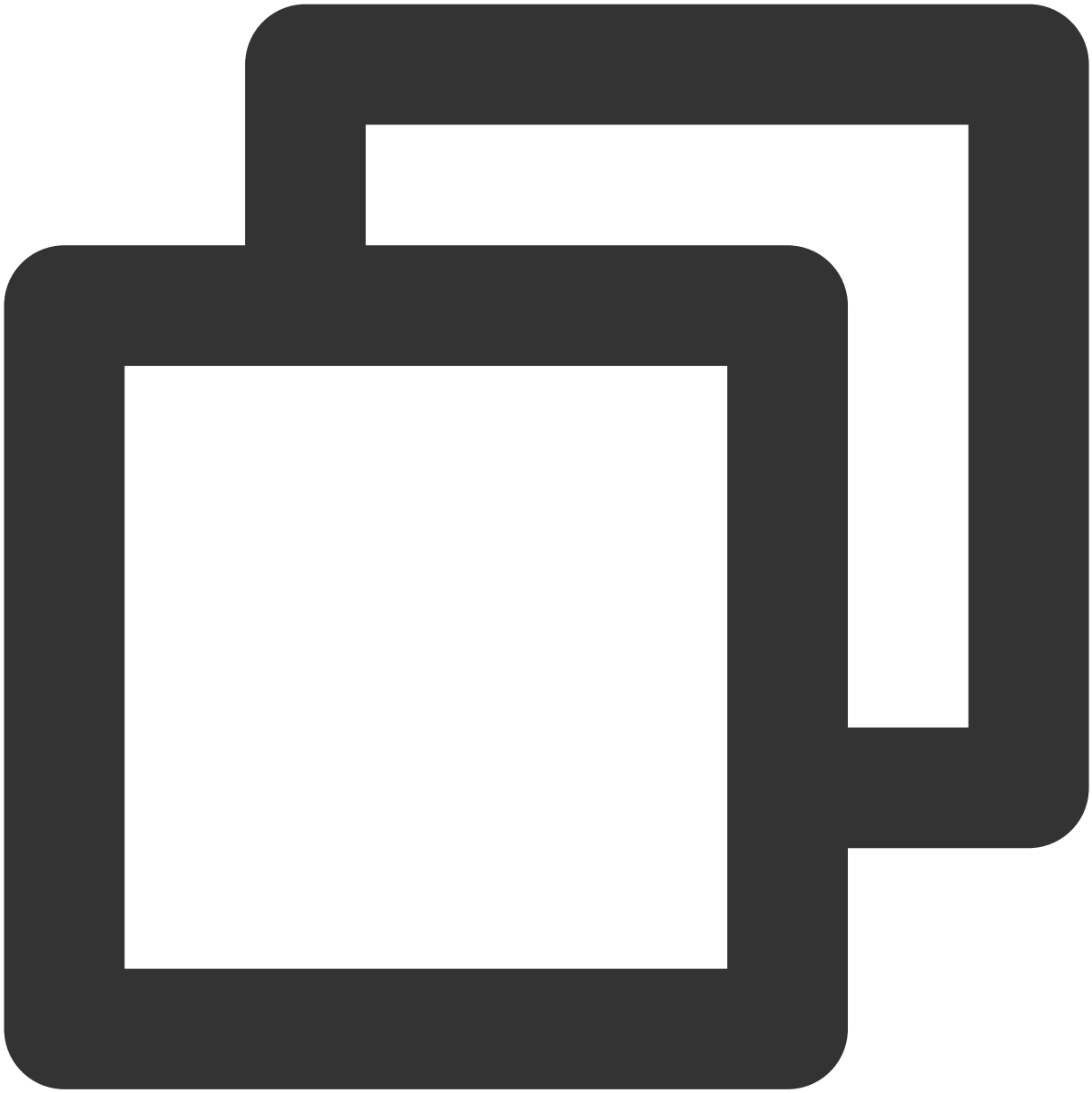
```
# PCCS server address
PCCS_URL=https://sgx-dcap-server-tc.[Region-ID].tencent.cn/sgx/certification/v3/
# To accept insecure HTTPS cert, set this option to FALSE
USE_SECURE_CERT=TRUE
```

`[Region-ID]` をSGX CVMインスタンスが配置されているリージョンのIDに置き換えてください。 例：
北京リージョンの変更例は次のとおりです。



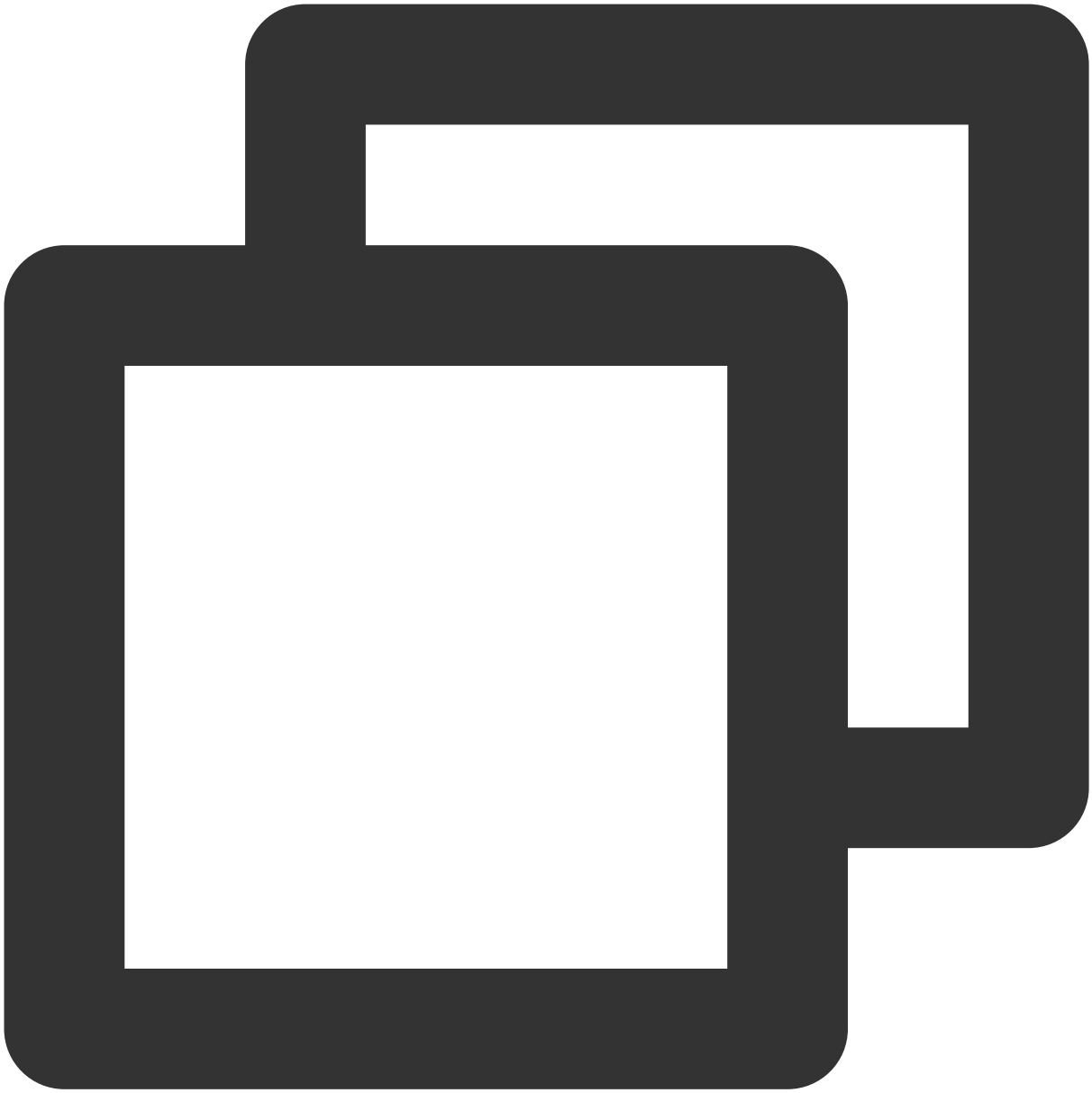
```
# PCCS server address
PCCS_URL=https://sgx-dcap-server-tc.bj.tencent.cn/sgx/certification/v3/
# To accept insecure HTTPS cert, set this option to FALSE
USE_SECURE_CERT=TRUE
```

上海リージョンの変更例は次のとおりです。



```
# 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
```

広州リージョンの変更例は次のとおりです。



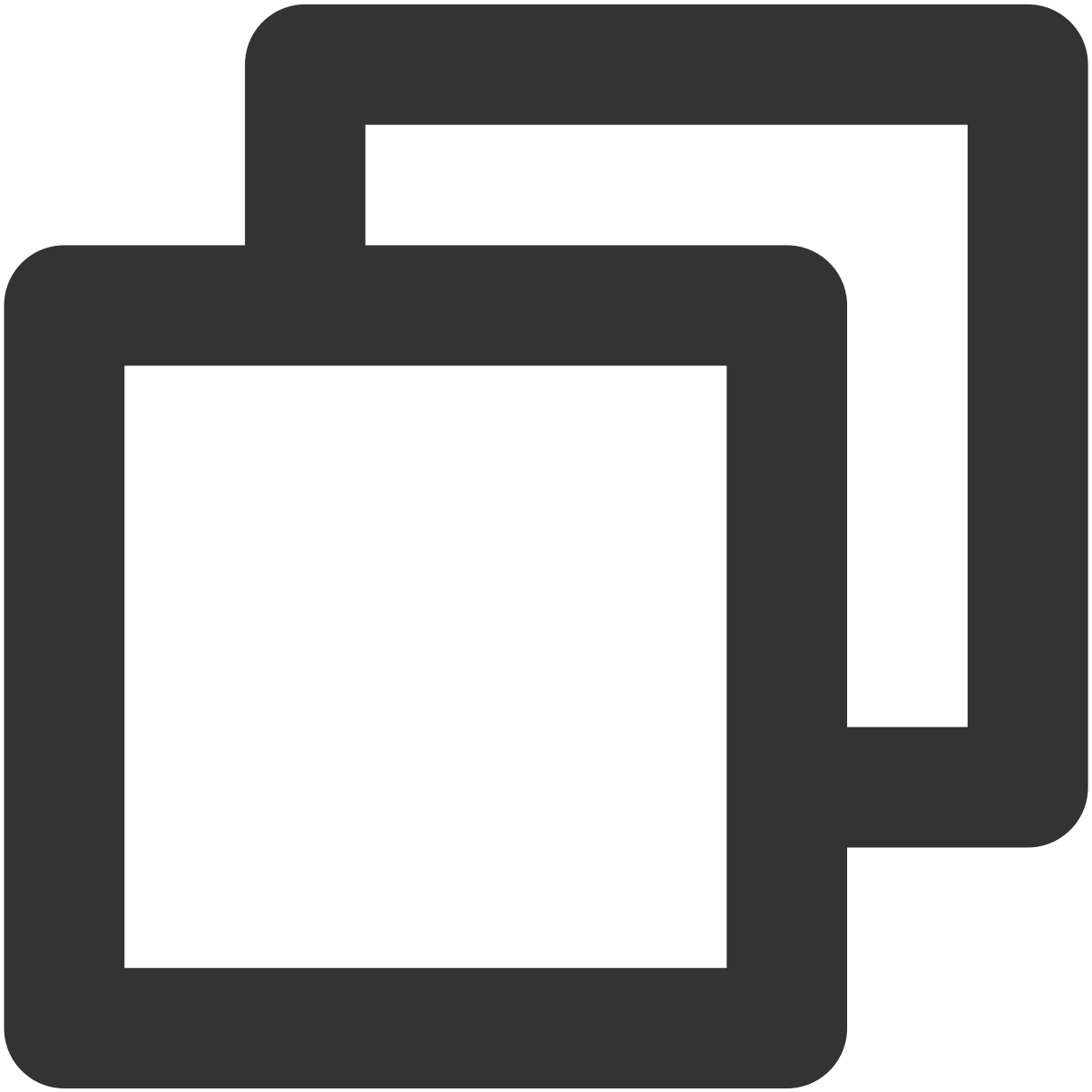
```
# PCCS server address
PCCS_URL=https://sgx-dcap-server-tc.gz.tencent.cn/sgx/certification/v3/
# To accept insecure HTTPS cert, set this option to FALSE
USE_SECURE_CERT=TRUE
```

SGX機能の検証例

例1：Enclaveの起動

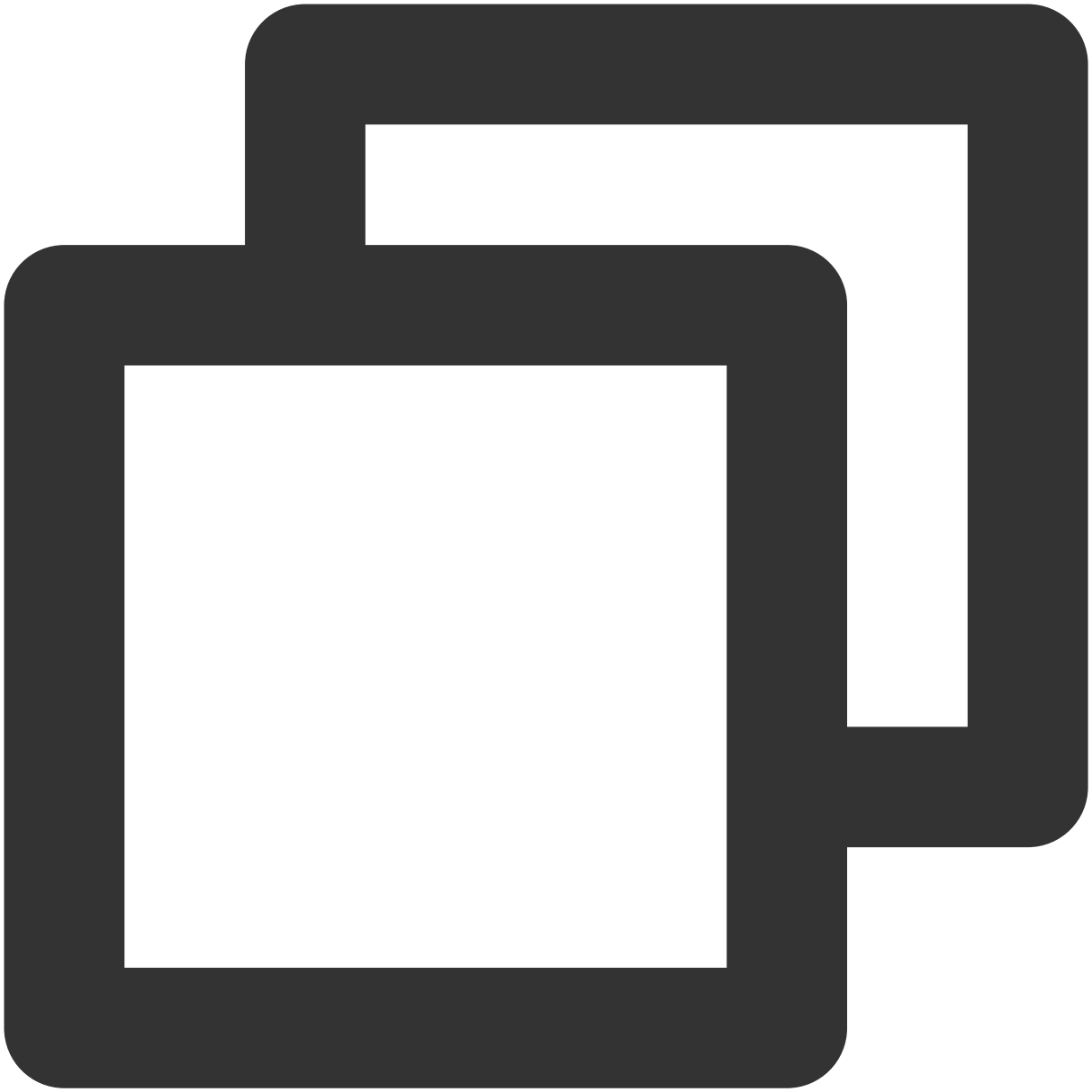
Intel SGXSDKは、SGX機能を検証するためのSGXサンプルコードを提供します。デフォルトのディレクトリは、`/opt/intel/sgxsdk/SampleCode`です。この例のコード(SampleEnclave)の効果は、Enclaveを起動して、インストールされたSGXSDKが正常に使用されているか、また、SGX CVMインスタンスの機密メモリリソースが使用可能かどうかを検証することです。

1. 次のコマンドを実行して、Intel SGXSDKに関連する環境変数を設定します。



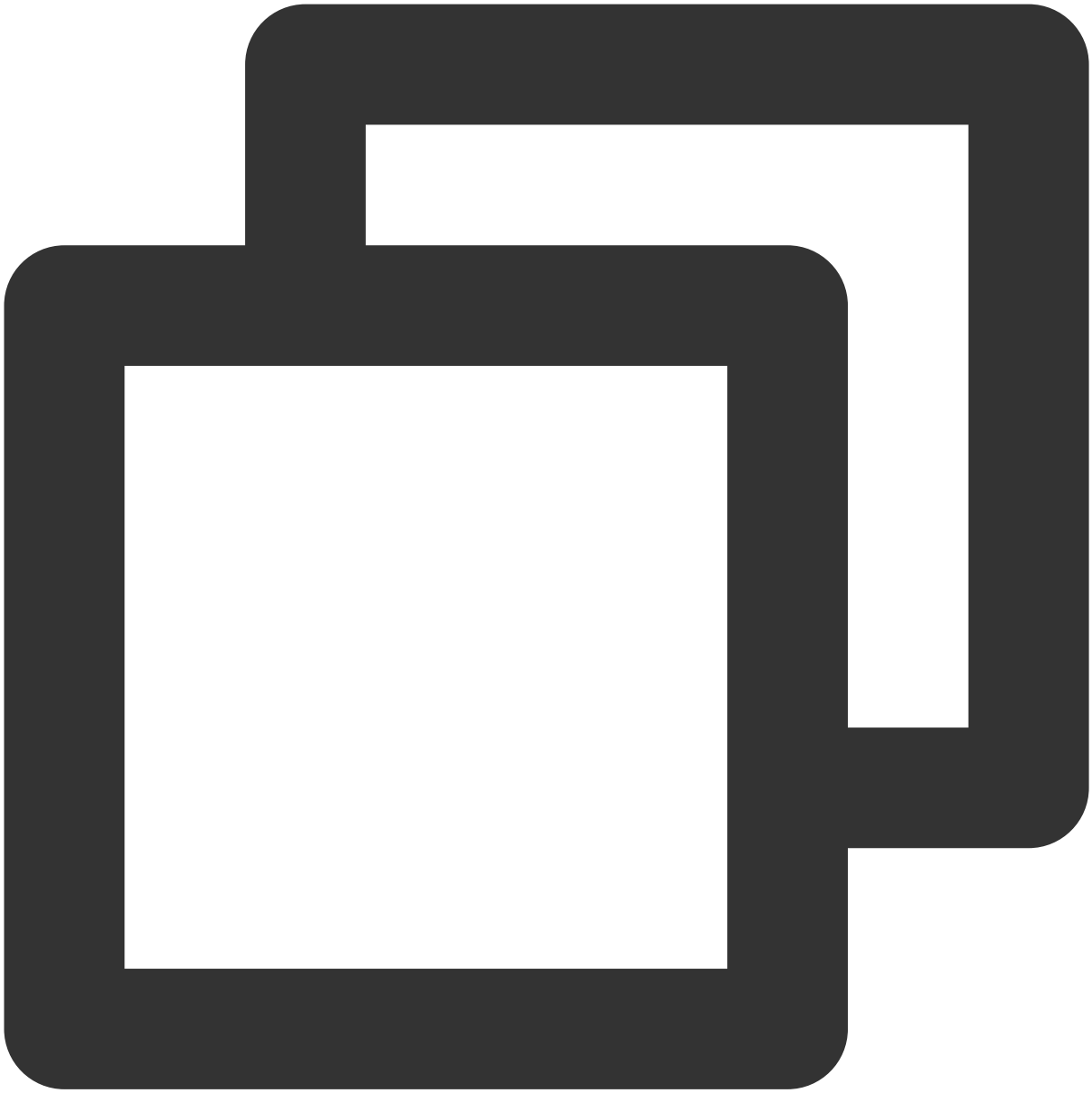
```
source /opt/intel/sgxsdk/environment
```

2. 次のコマンドを実行して、サンプルコードSampleEnclaveをコンパイルします。



```
cd /opt/intel/sgxsdk/SampleCode/SampleEnclave && make
```

3. 次のコマンドを実行して、コンパイルされた実行可能ファイルを実行します。



```
./app
```

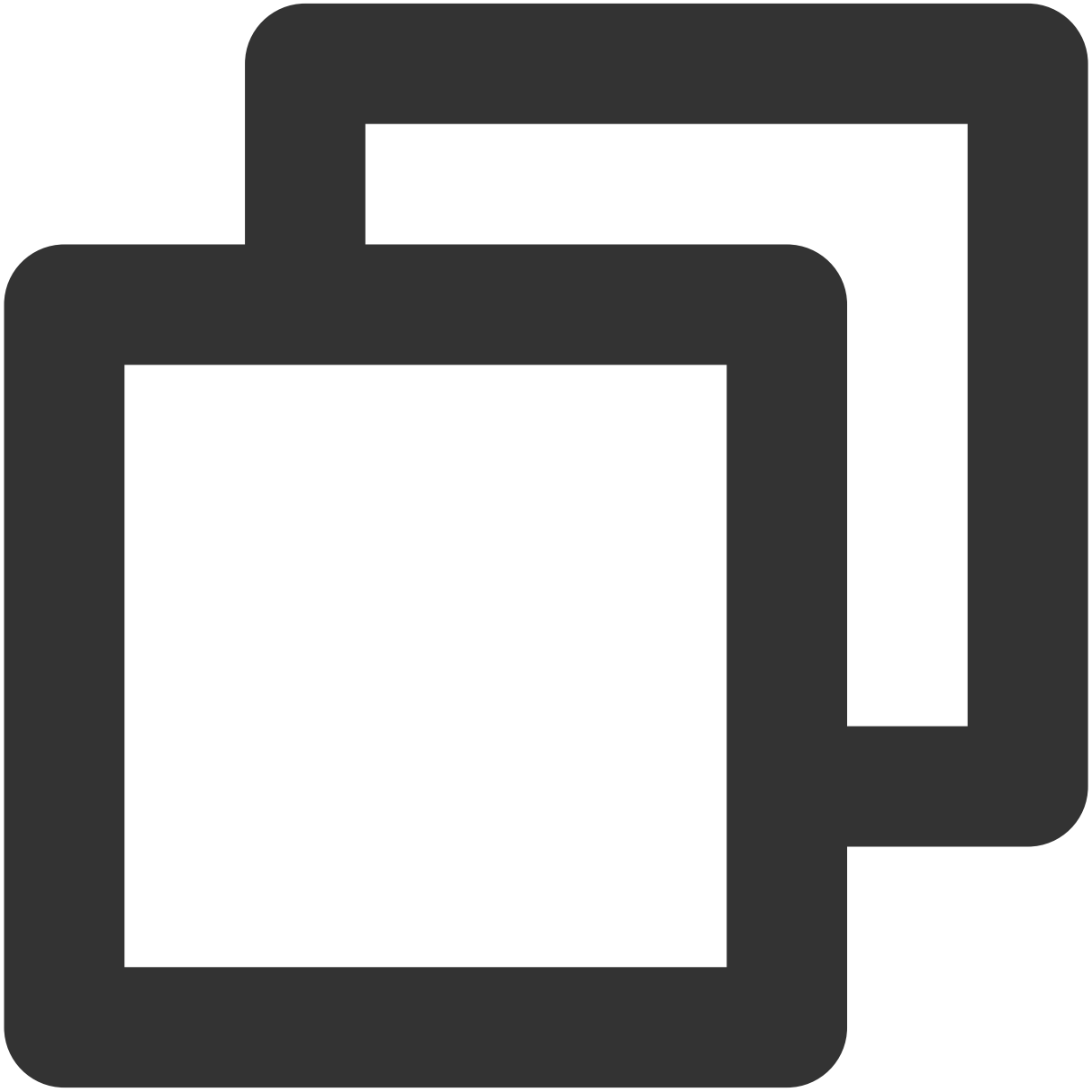
以下のような結果が返されれば、起動に成功しています。

```
[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 ...
```

例2：SGXリモートアテステーション

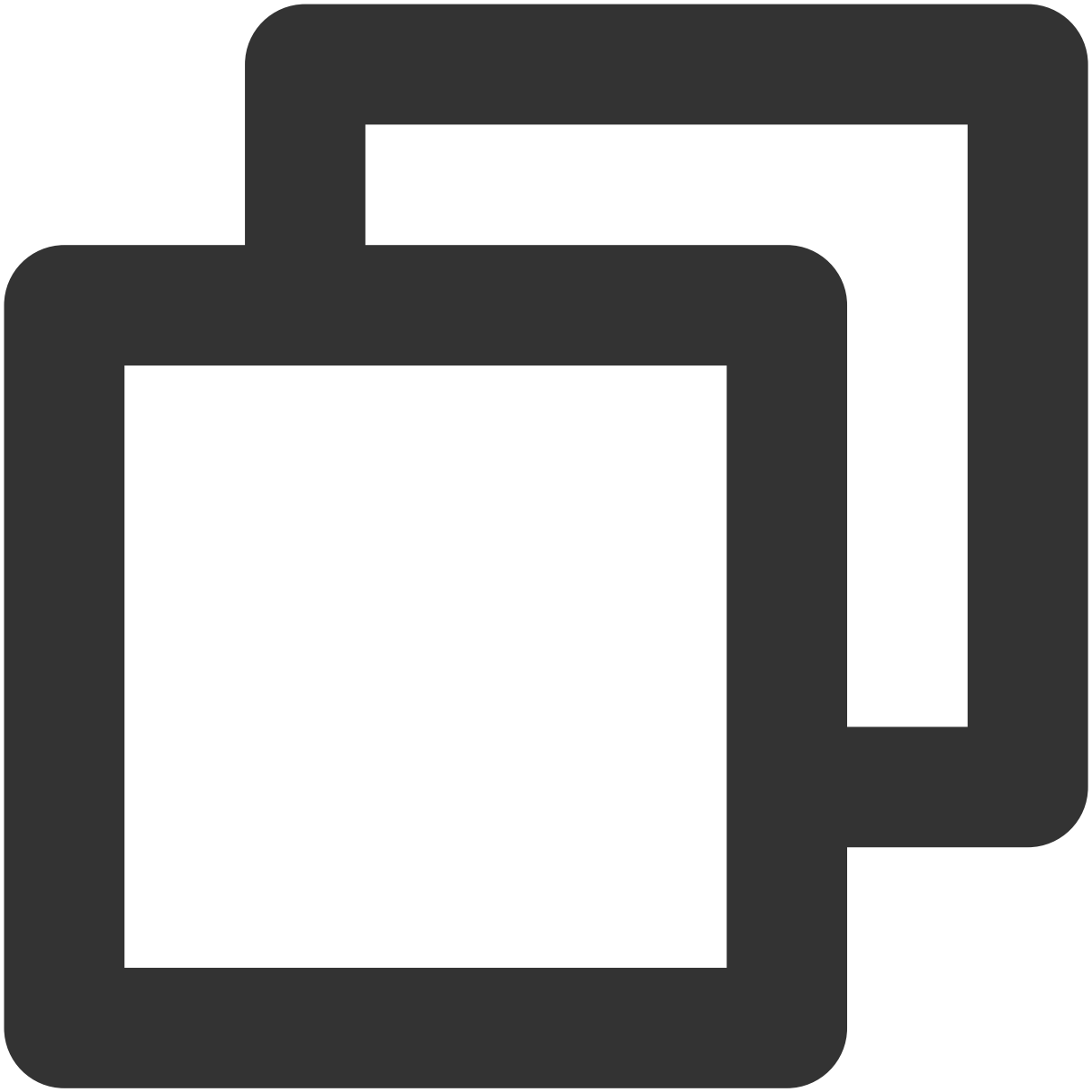
Intel SGXのcode treeは、SGXリモートアテステーション機能(DCAP)を検証するためのサンプルコードを提供します。この例は、Quoteを発行および検証するためのもので、Quote Generator(QuoteGenerationSample)とQuote Verifier(QuoteVerificationSample)が含まれます。

1. 次のコマンドを実行して、Intel SGXSDKに関連する環境変数を設定します。

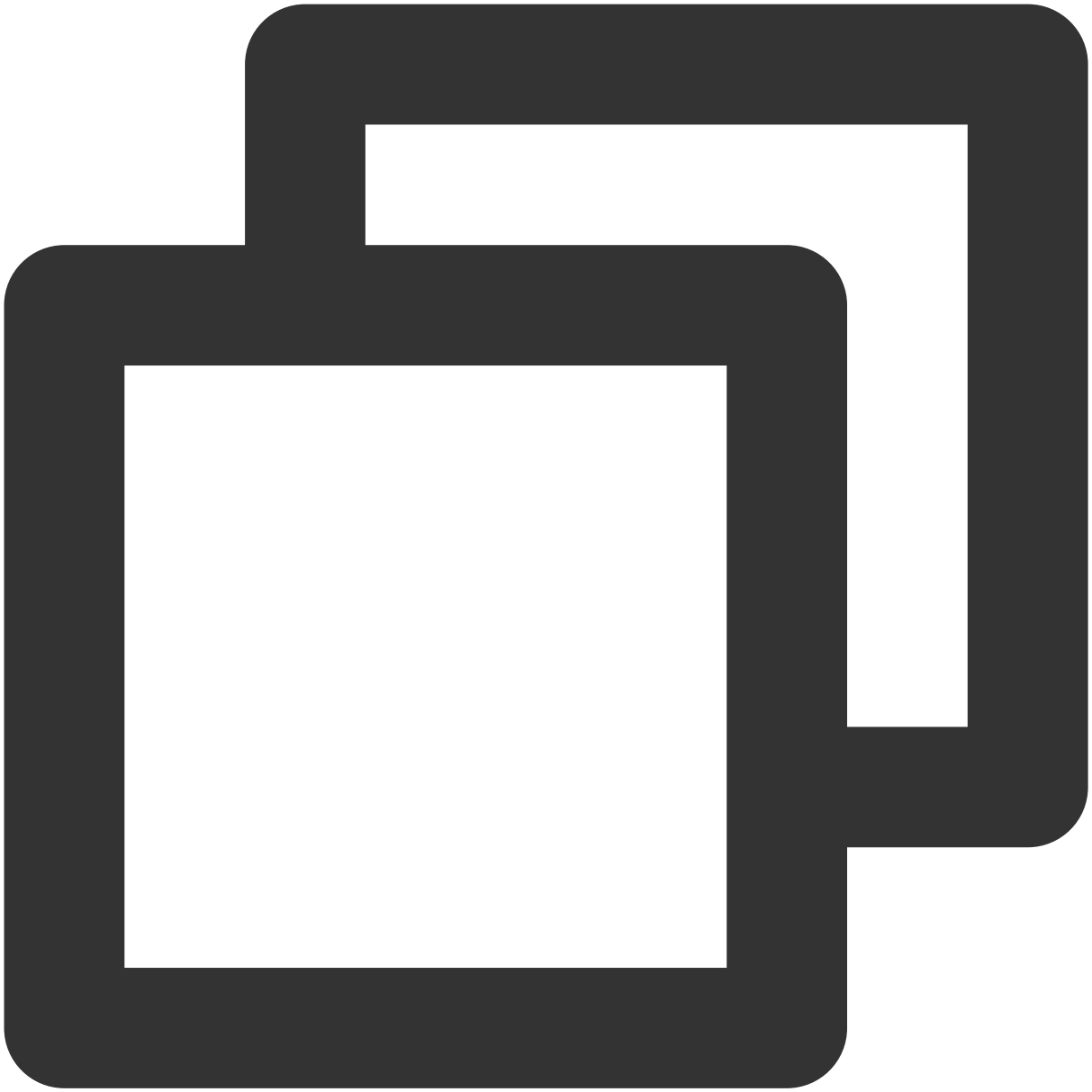


```
source /opt/intel/sgxsdk/environment
```

2. 次のコマンドを順に実行してgitをインストールし、Intel SGX DCAP code treeをダウンロードします。



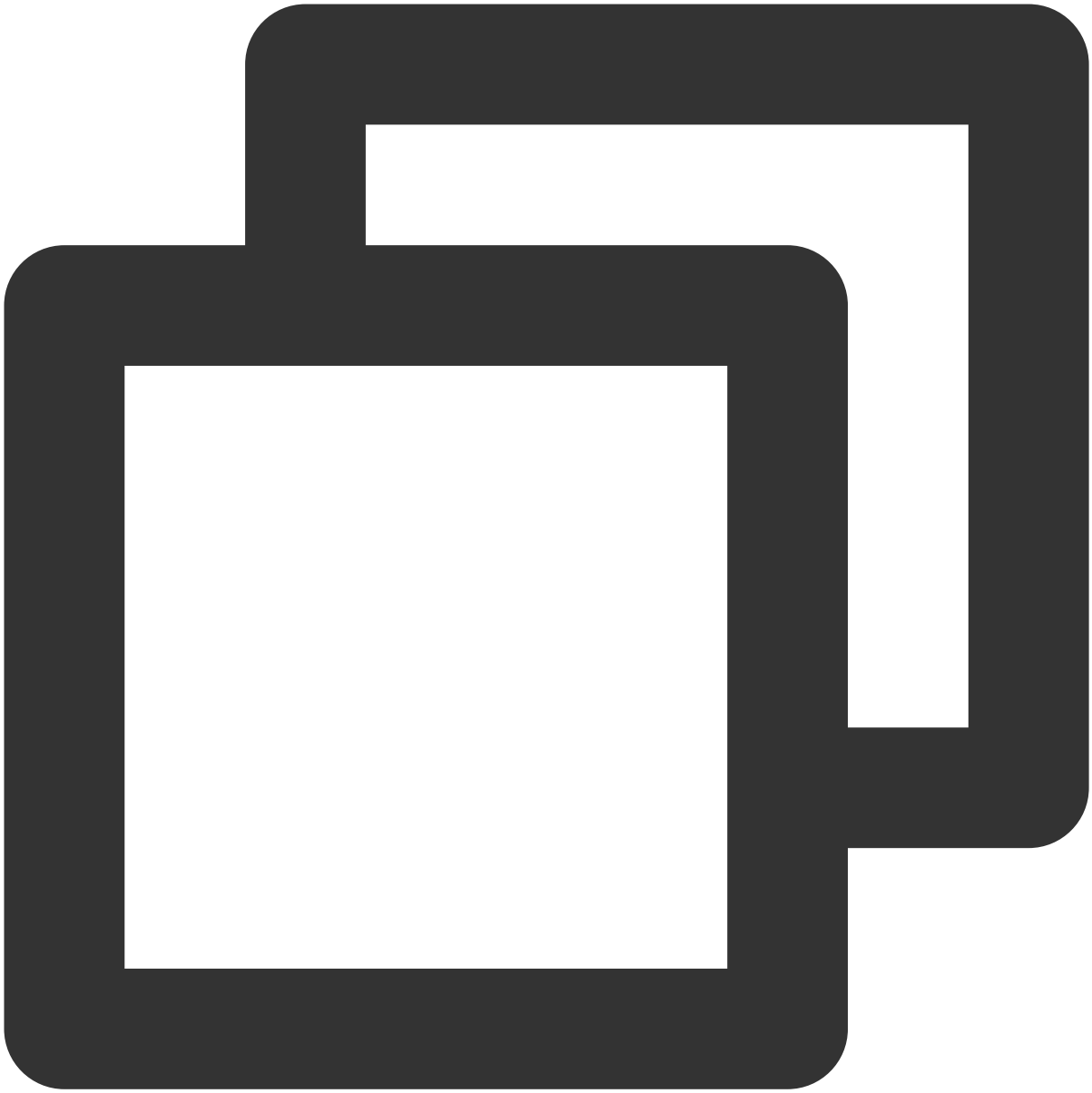
```
cd /root && yum install git
```



```
git clone https://github.com/intel/SGXDataCenterAttestationPrimitives.git
```

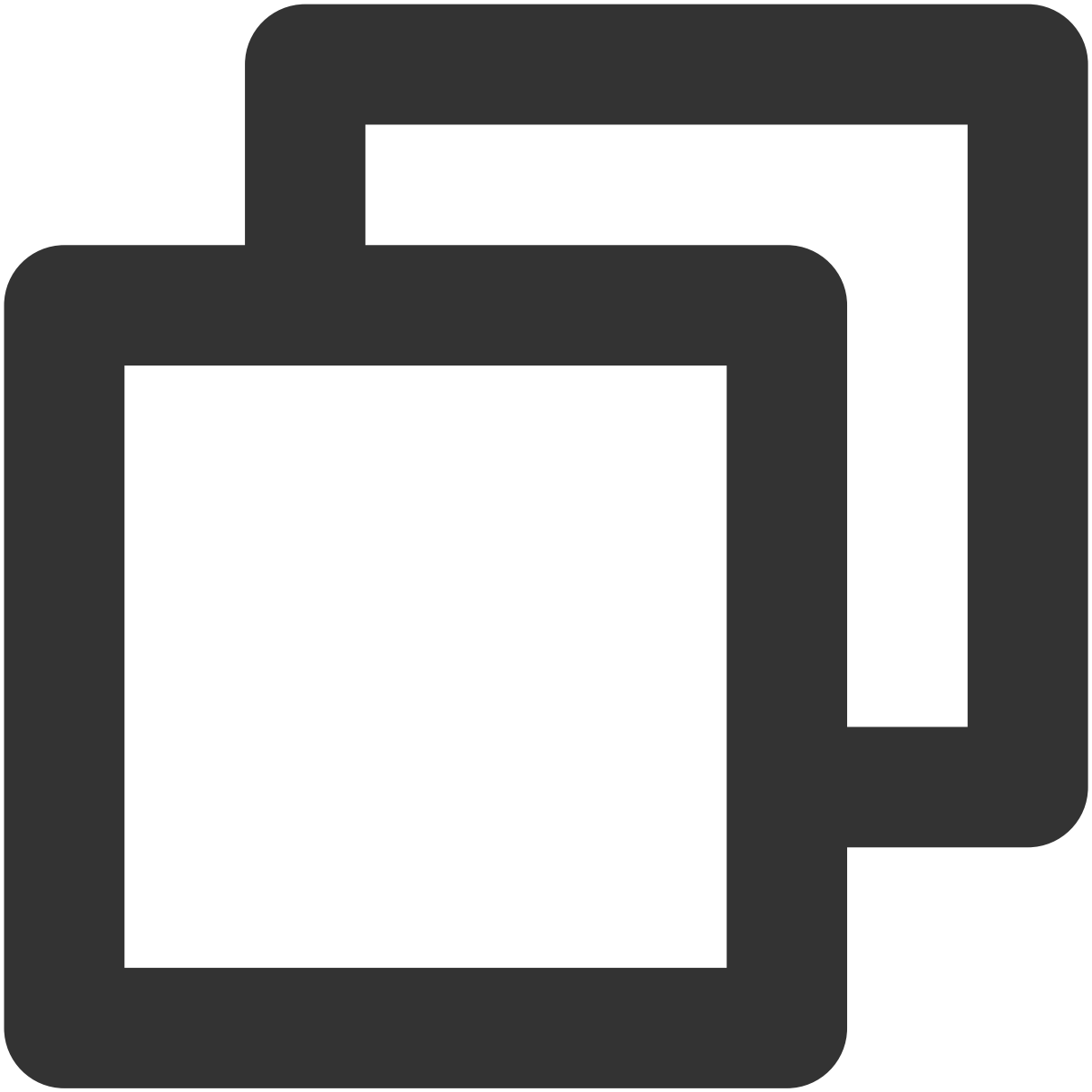
3. 次のコマンドを順に実行して、Quote GeneratorのサンプルコードQuoteGenerationSampleをコンパイルして実行します。

3.1 QuoteGenerationSampleディレクトリに入ります。



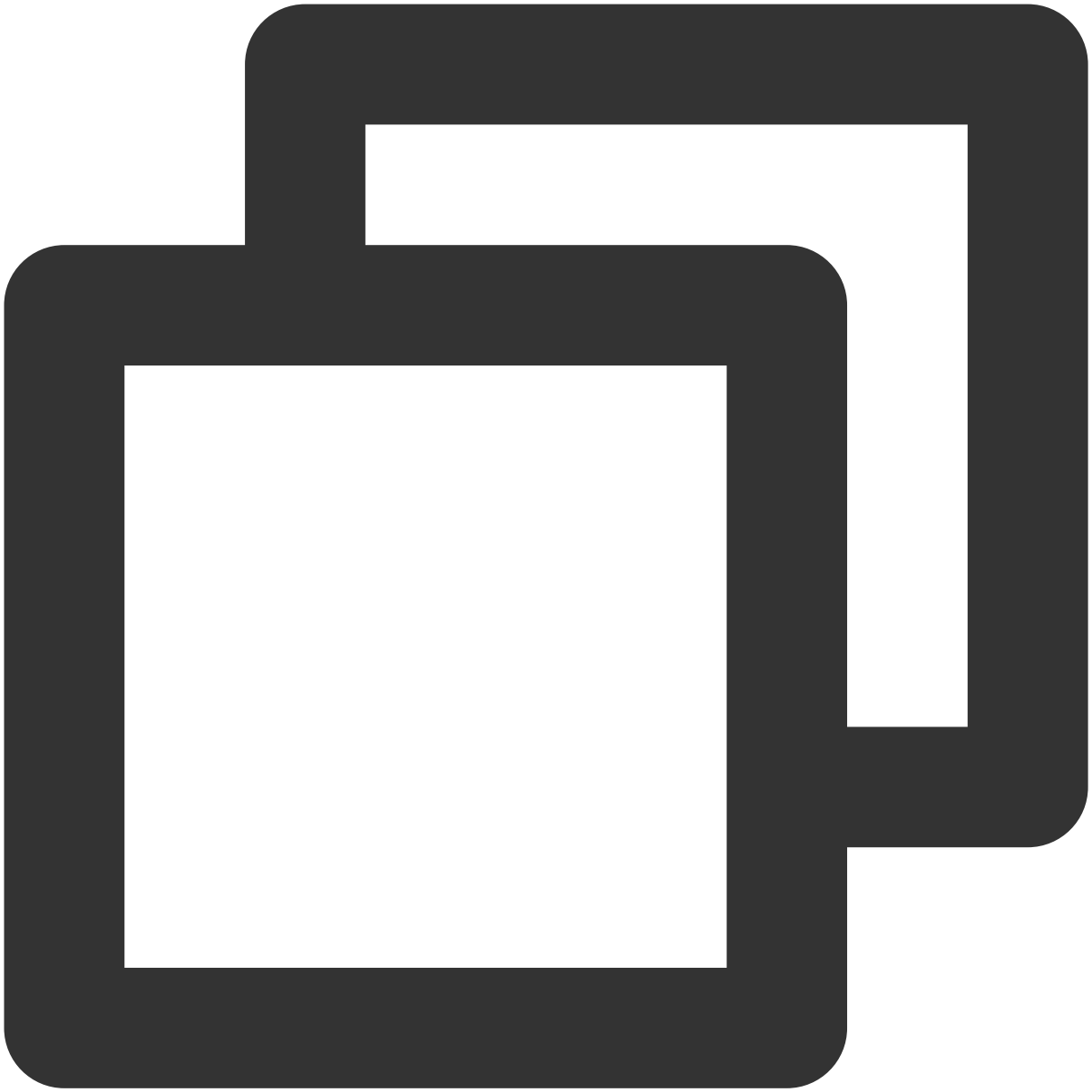
```
cd /root/SGXDataCenterAttestationPrimitives/SampleCode/QuoteGenerationSample
```

3.2 QuoteGenerationSampleをコンパイルします。



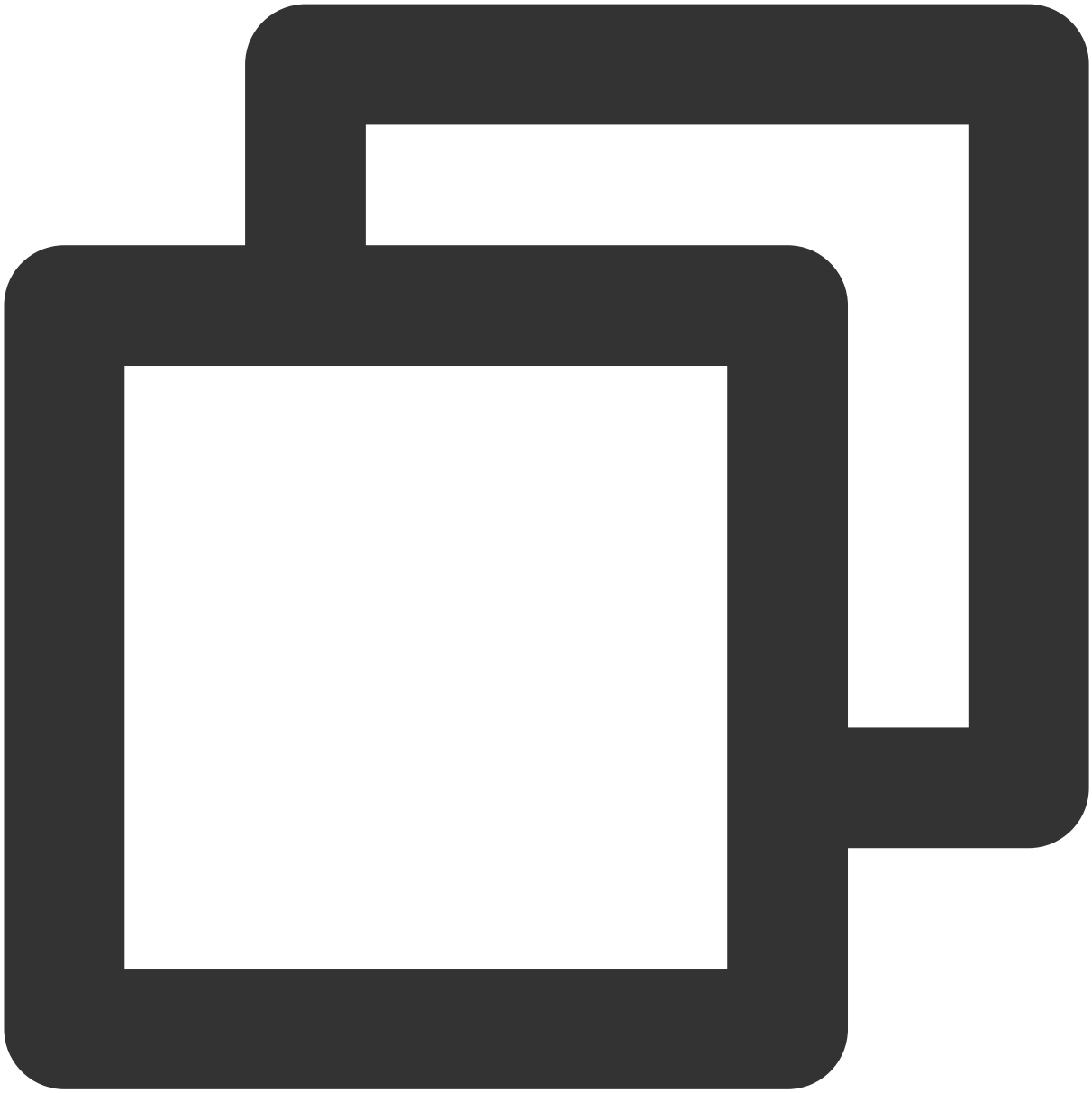
```
make
```

3.3 QuoteGenerationSampleを実行し、Quoteを発行します。



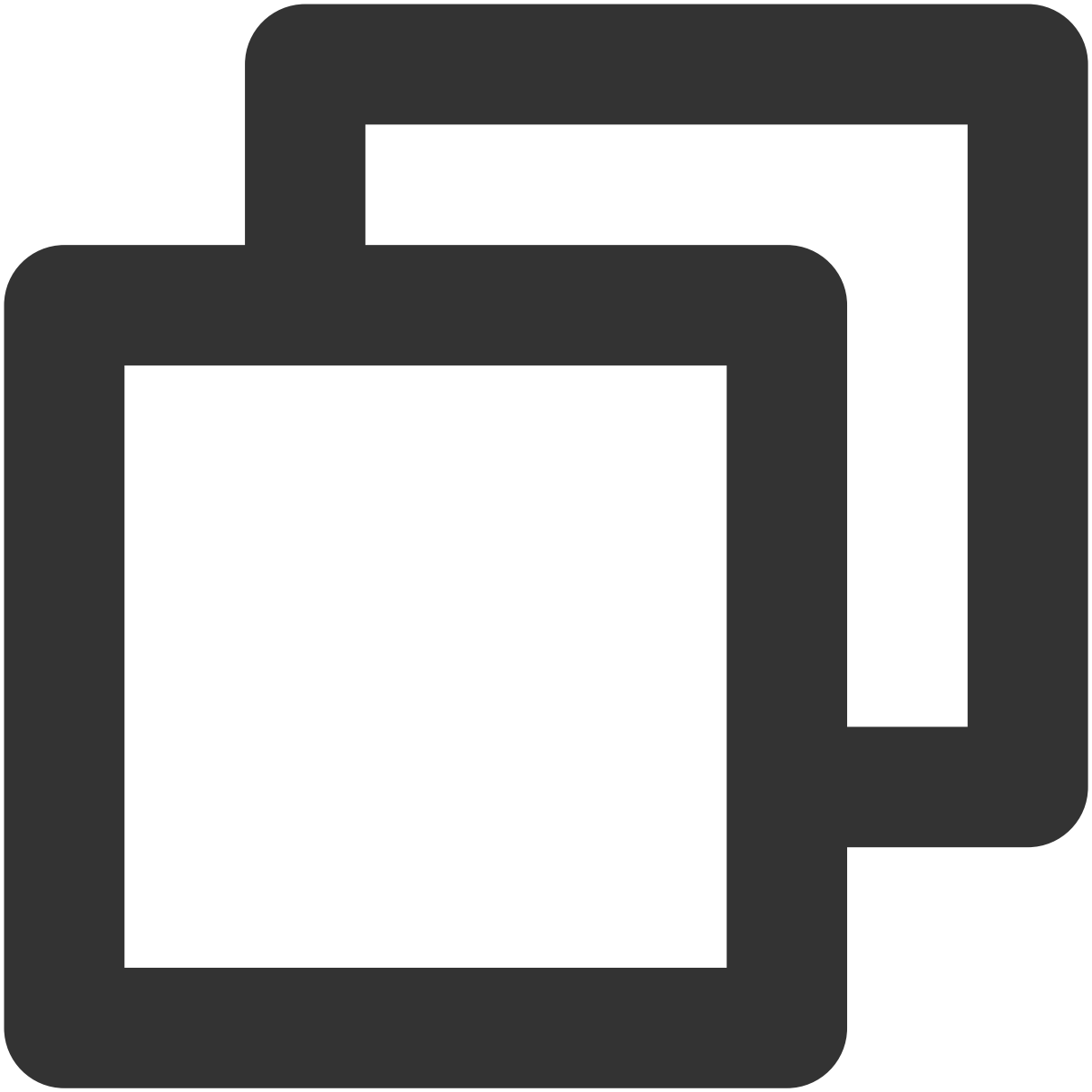
```
./app
```

4. 次のコマンドを実行して、QuoteVerifierのサンプルコードQuoteVerificationSampleをコンパイルします。



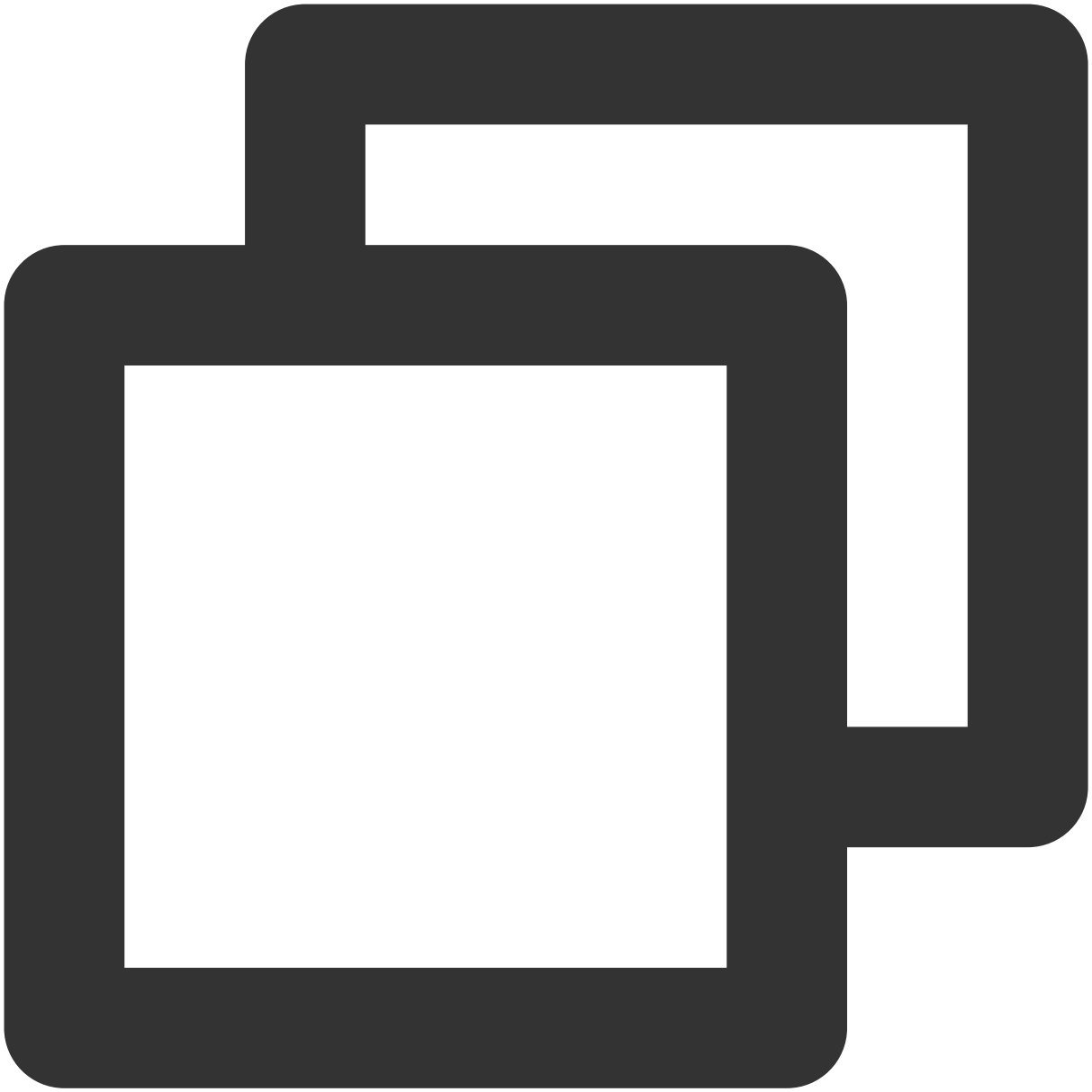
```
cd /root/SGXDataCenterAttestationPrimitives/SampleCode/QuoteVerificationSample && m
```

5. 次のコマンドを実行して、QuoteVerificationSample Enclaveに署名します。



```
sgx_sign sign -key Enclave/Enclave_private_sample.pem -enclave enclave.so -out encl
```

6. 次のコマンドを実行して、QuoteVerificationSampleを実行し、Quoteを検証します。



```
./app
```

以下のような結果が返されれば、検証に成功しています。

```
[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インスタンスによる永続メモリの構成

最終更新日：：2022-03-16 17:10:24

概要

ここでは、M6pインスタンスで永続メモリを構成する方法についてご説明します。
##インスタンス構成
ここでは、次の構成のCVMインスタンスを使用します。取得に関する情報については、実際の状況によります。
インスタンス仕様：メモリ型M6pインスタンスM6p.LARGE16（4 コア 16GB）。その他の仕様については、メモリ型 M6p をご参照ください。
オペレーティングシステム： TencentOS Server 3.1(TK4)。
説明：
インスタンスには、次のオペレーティングシステムを使用することをお勧めします。
TencentOS Server 3.1
CentOS 7.6およびそれ以降のバージョン
Ubuntu 18.10およびそれ以降のバージョン

前提条件

M6pインスタンス が作成され、ログインしていること。
-インスタンスの作成方法については、購入画面でインスタンスを作成 をご参照ください。
-インスタンスのログイン方法については、標準ログイン方式を使用してLinuxインスタンスにログイン（推奨）をご参照ください。

Intel® Optane™ DC BPSハードウェア(PMEM)モードのご紹介

Memoryモード

Memoryモードでは、通常のDRAMがアクセス頻度の高いデータのキャッシュとして機能し、永続メモリはバックアップメモリとして使用され、高速なキャッシュの管理操作はメモリコントローラが自動的に処理します。

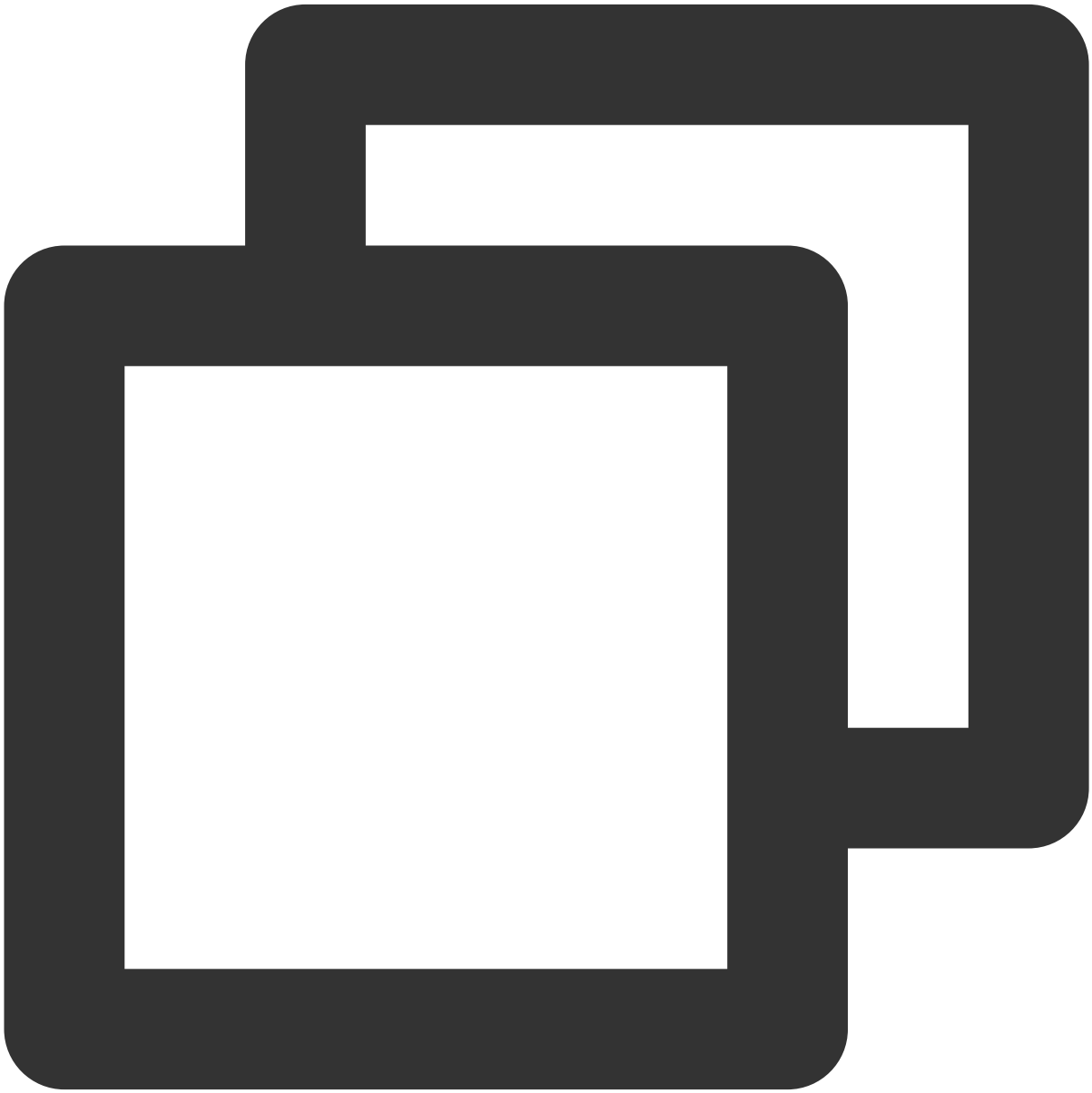
ADモード

M6pモデルはこのモードを採用しています。M6pモデルでは、プラットフォーム側でBPSハードウェアをADモードで構成し、CVMにパススルーして使用します。ADモードでは、アプリケーションはPMEMデバイスをメモリとして使用したり、ローカルのSSDディスクとして使用したりすることができます。

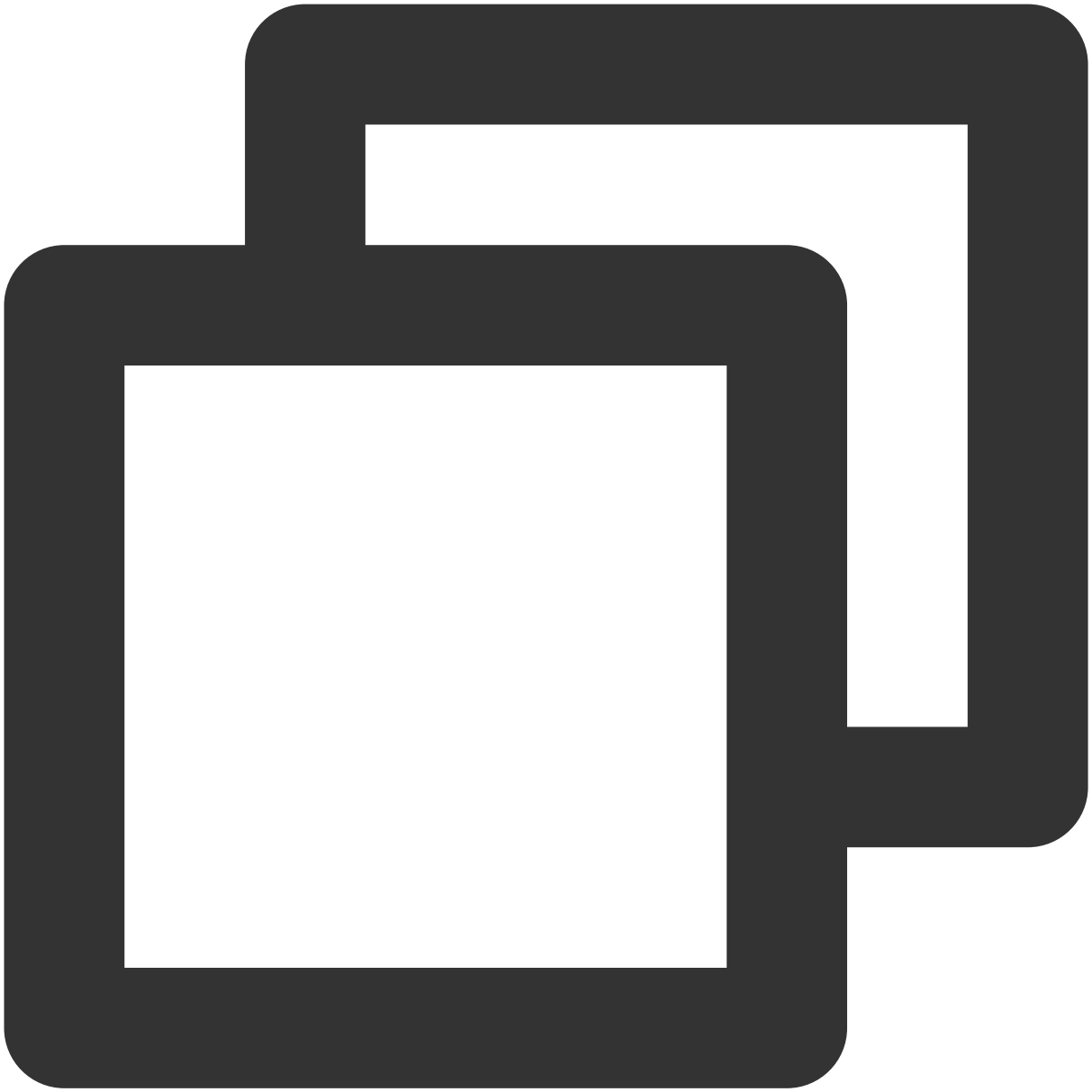
操作手順

PMEM初期化

インスタンスを初めて使用する場合は、次のコマンドを順に実行して、PMEMデバイスを初期化します。すでにPMEMの初期化を実行している場合は、この手順をスキップしてください。



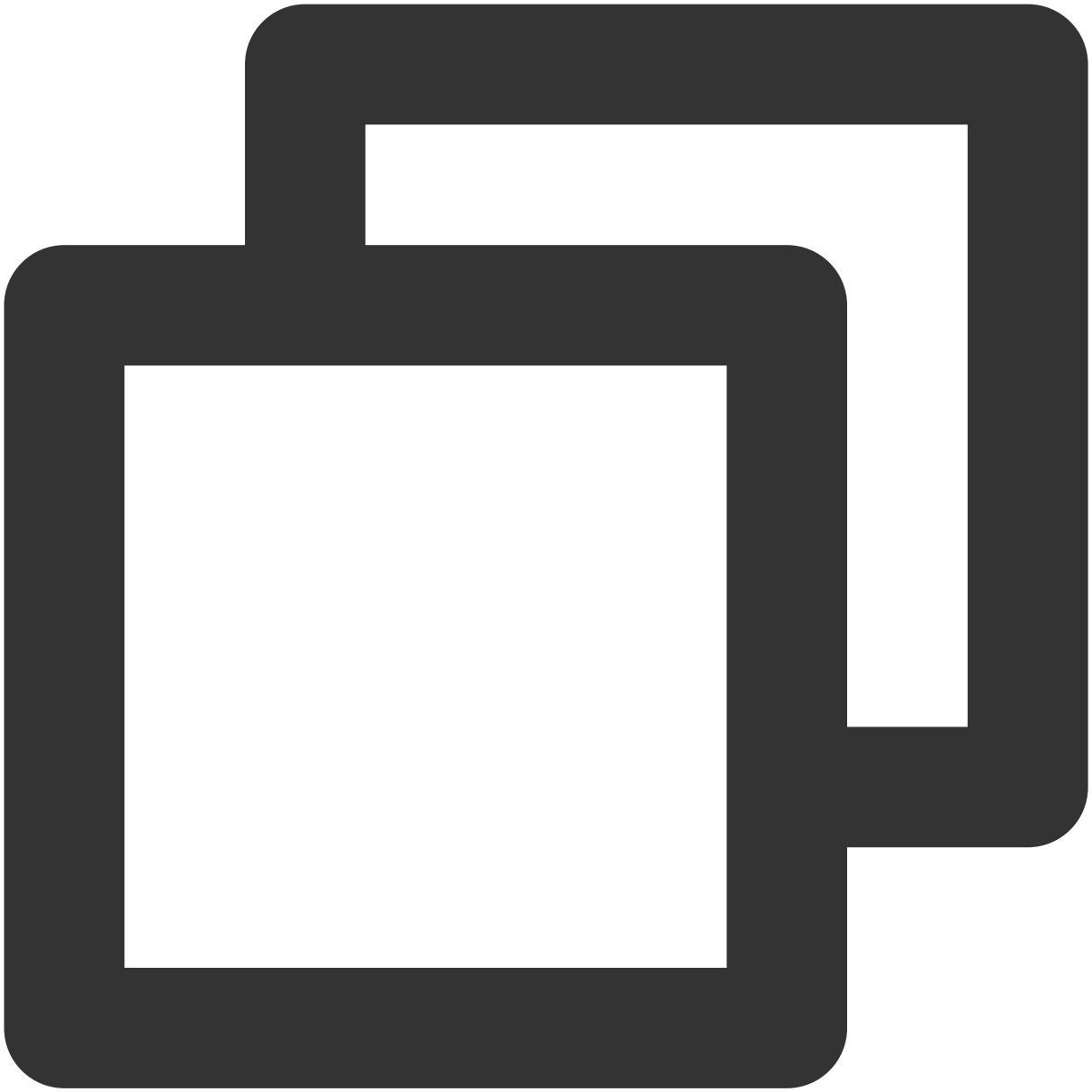
```
yum install -y ndctl
```



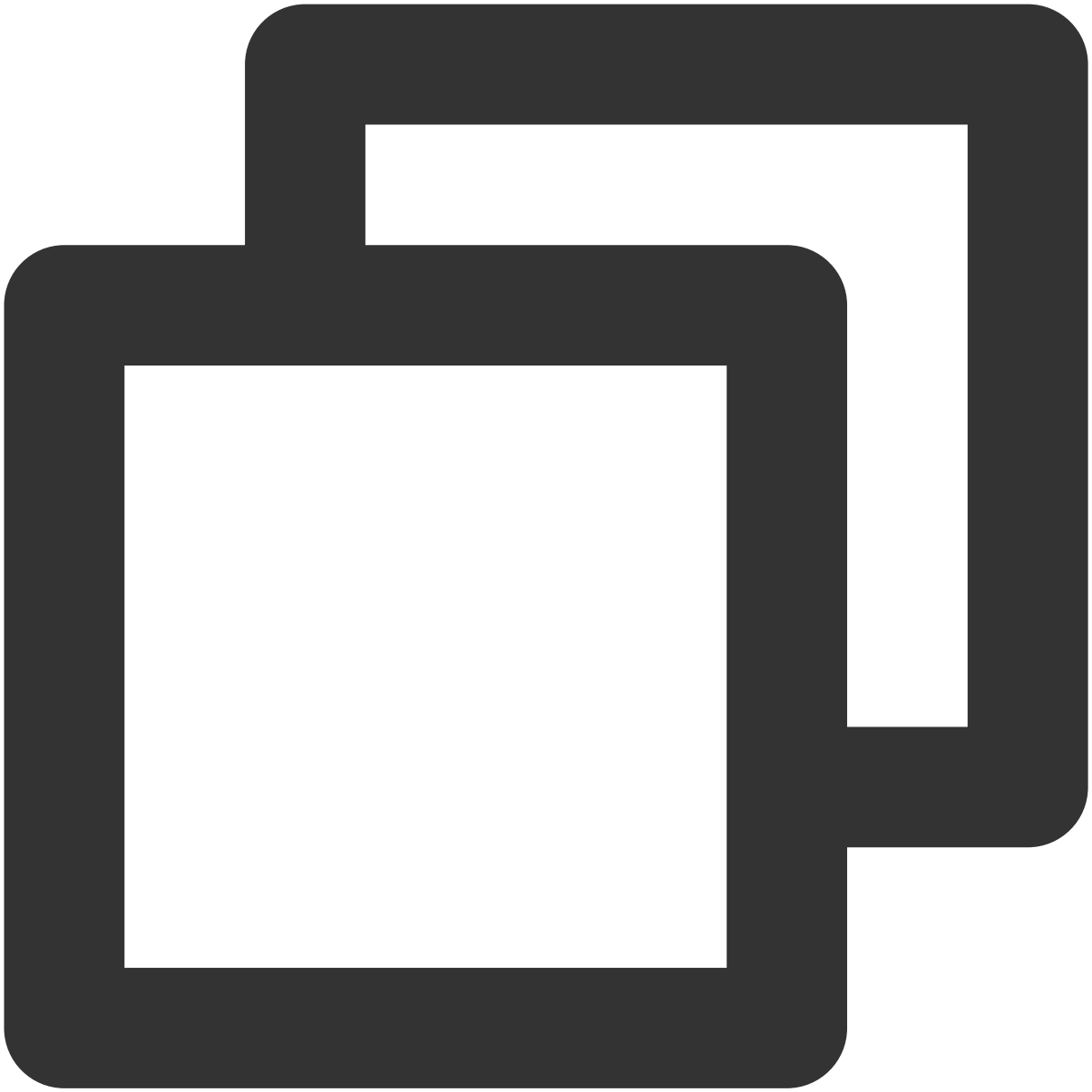
```
ndctl destroy-namespace all --force
```

説明：

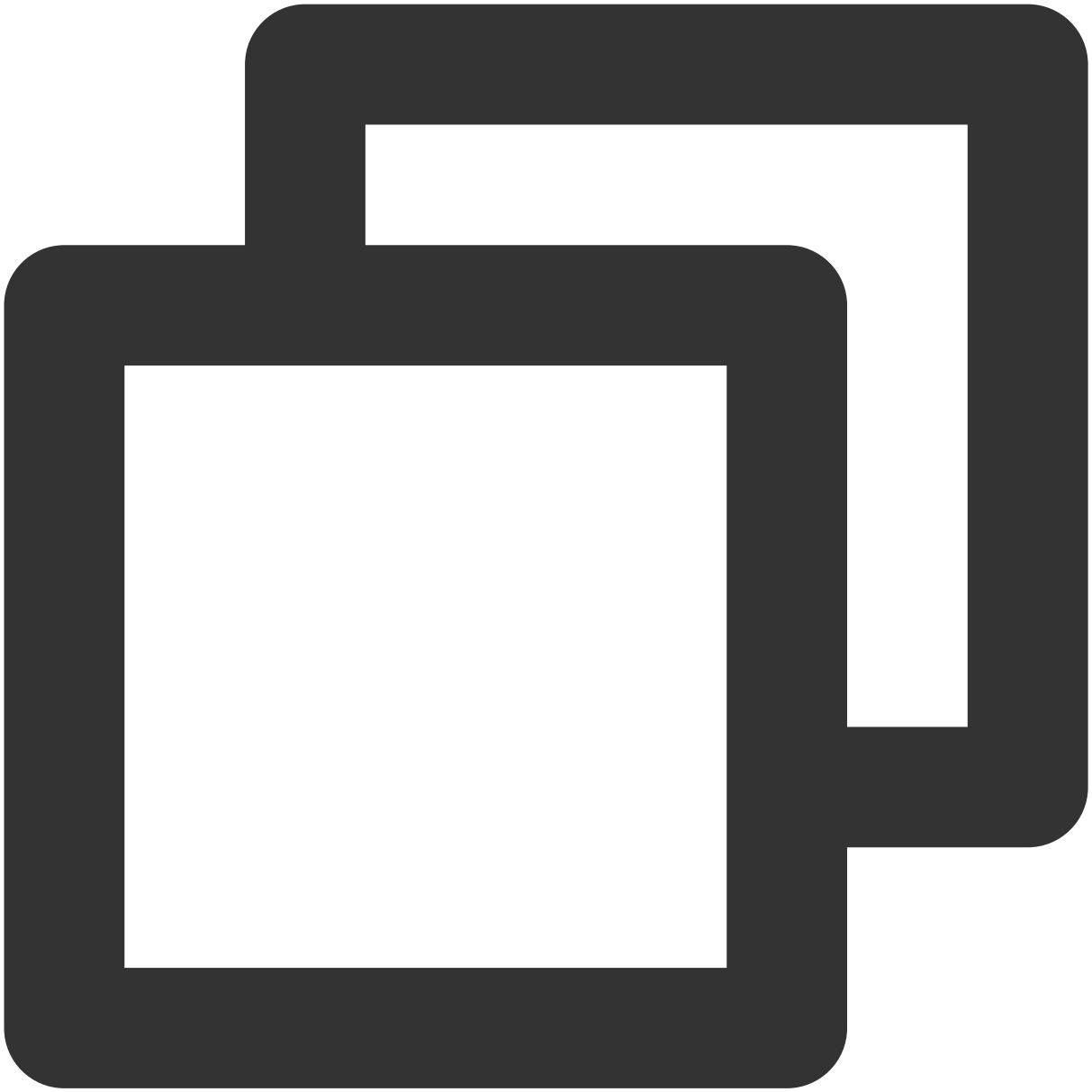
最大仕様のインスタンスには2つのregionがあります。次のコマンドを実行した後、region0をregion1に置き換えて、コマンドを再実行してください。



```
ndctl disable-region region0
```



```
ndctl init-labels all
```



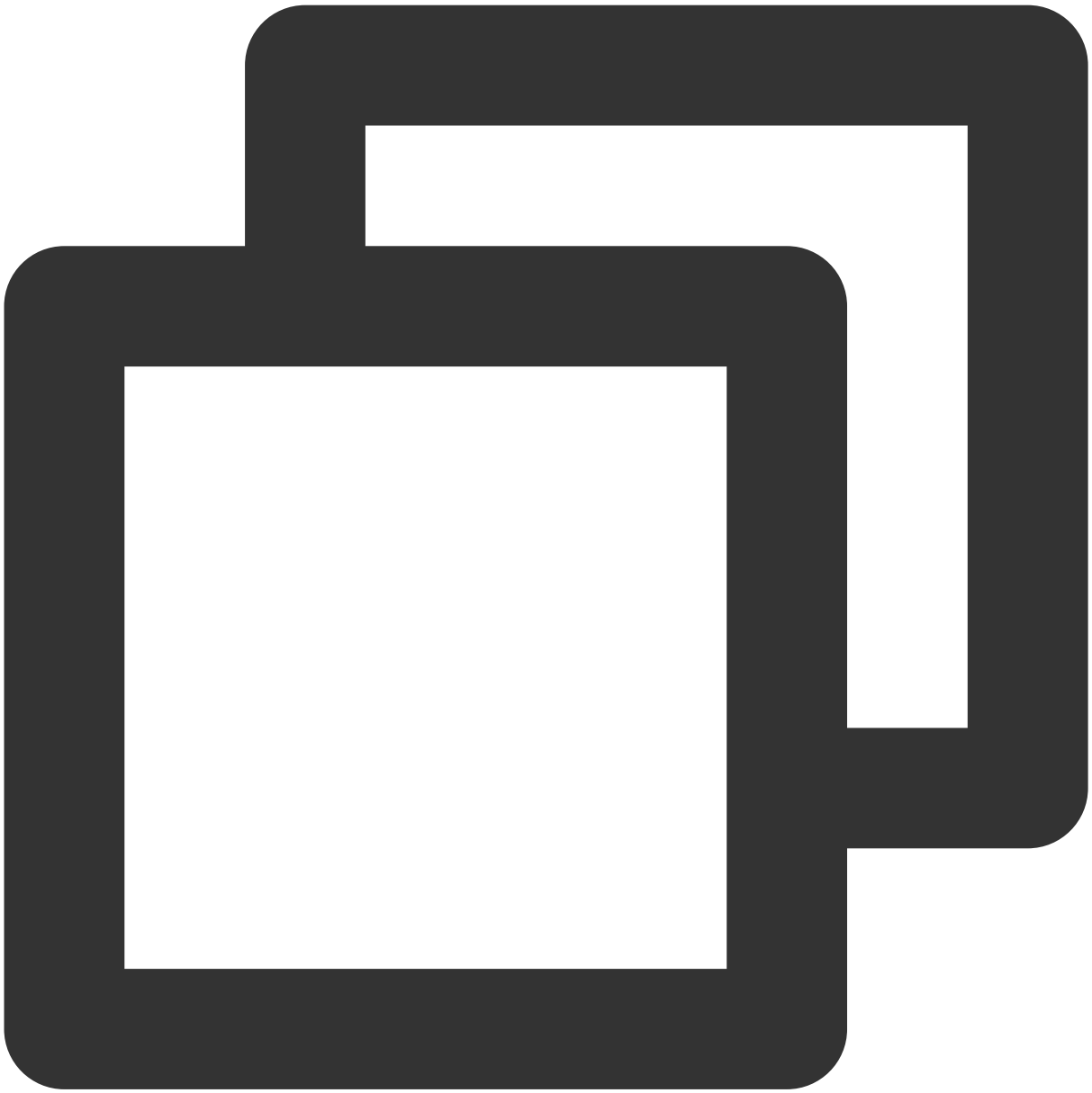
```
ndctl enable-region region0
```

ADモードでのPMEMの構成

実際のニーズに応じて、永続メモリをメモリまたはローカルSSDディスクとして使用できます。
メモリとして使用
ローカルSSDディスクとして使用
PMEMは、上位レイヤのアプリケーション（redisなど）に永続メモリを割り当てるためのキャラクタデバイスとして使用できます。memkindなどのPMDKフレームワークの機能によって使用できます。構成方法は以下のとおり

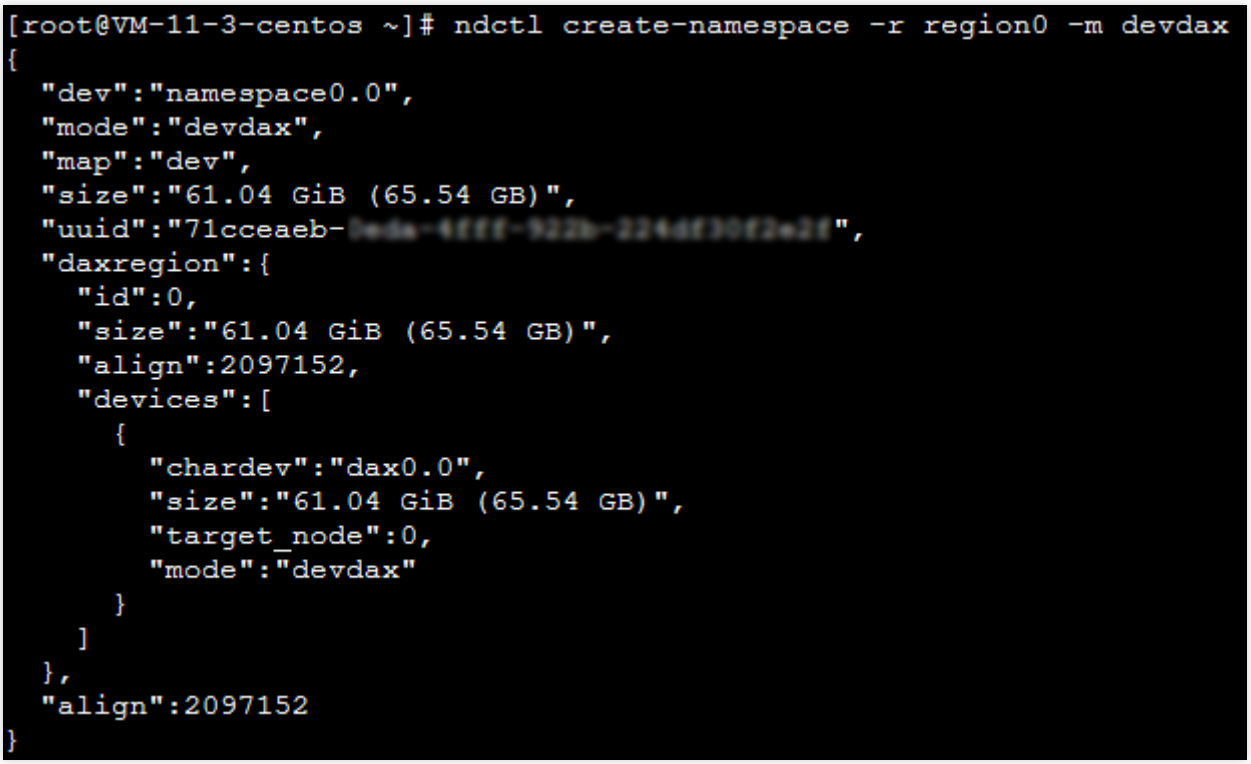
です。

1. 次のコマンドを実行して、キャラクタデバイスを生成します。

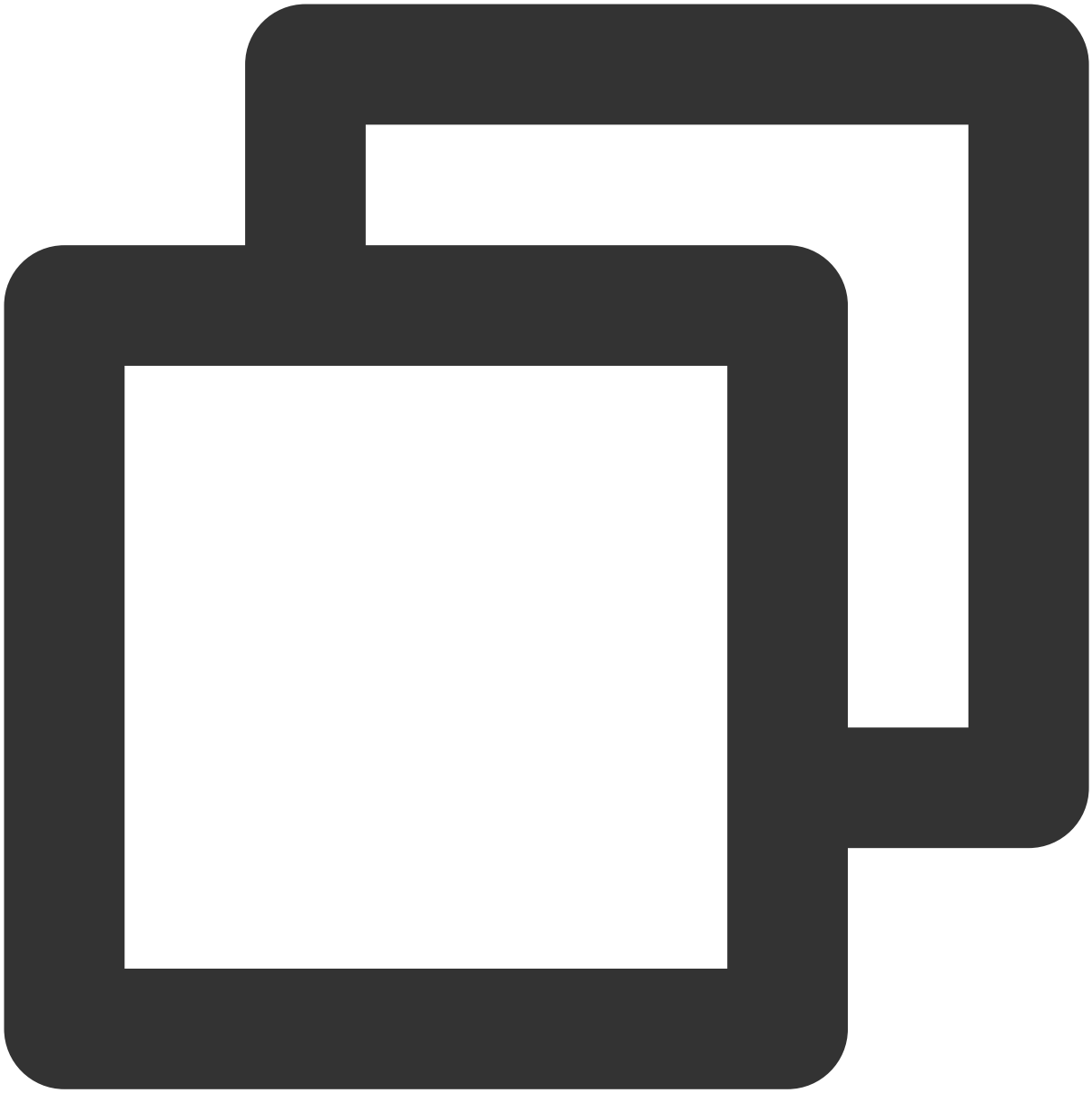


```
ndctl create-namespace -r region0 -m devdax
```

返された結果を下図に示します。これは、 `dax0.0` キャラクタデバイスが生成されたことを示しています。



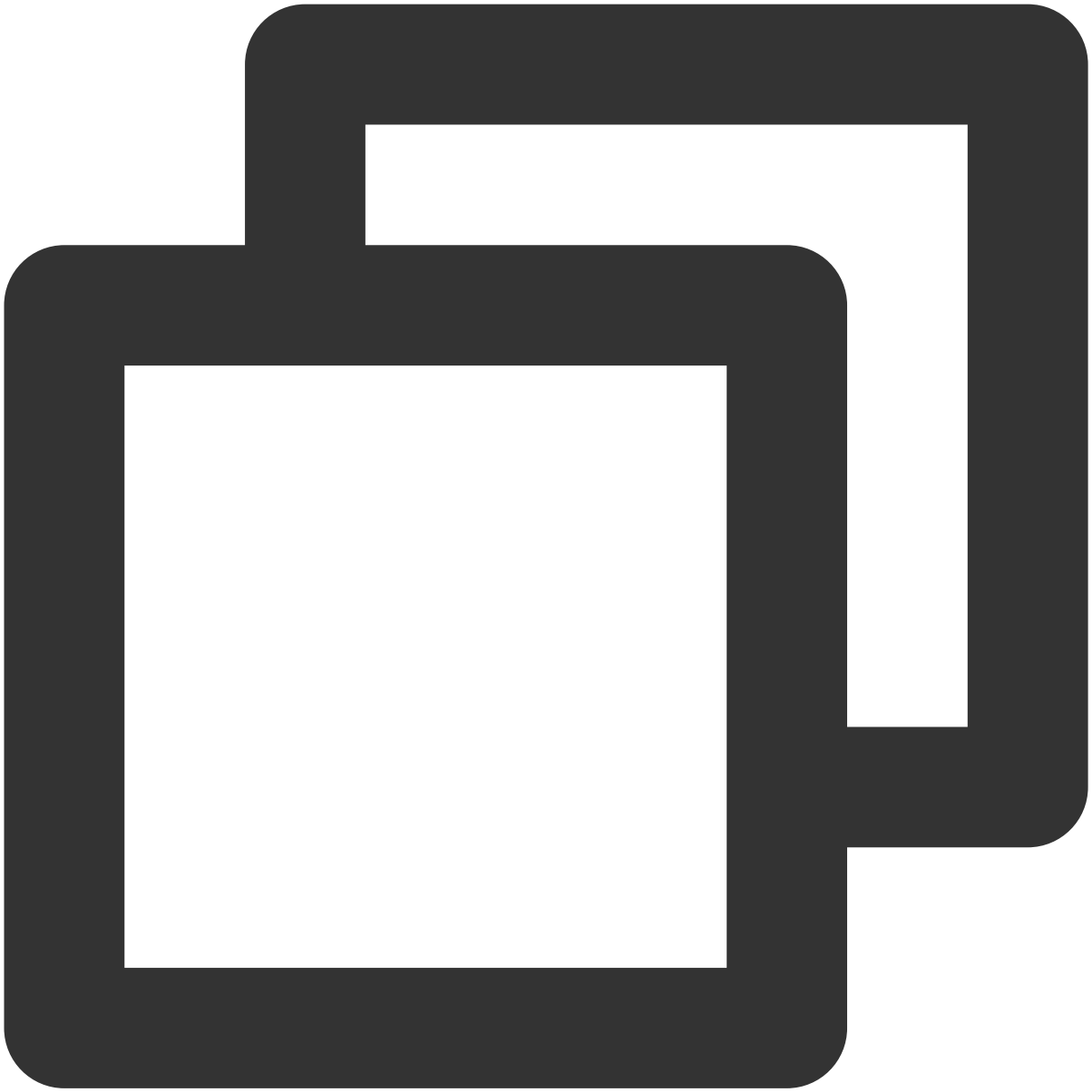
最大仕様のインスタンスには2つのregionがあります。最大仕様のインスタンスを使用する場合は、次のコマンドを同時に実行してください。



```
ndctl create-namespace -r region1 -m devdax -f
```

構成が完了すると、 `/dev` ディレクトリに `dax0.0` キャラクタデバイスが生成され、永続メモリにマッピングできます。

2. 次のコマンドを実行して、永続メモリサイズを確認します。



```
ndctl list -R
```

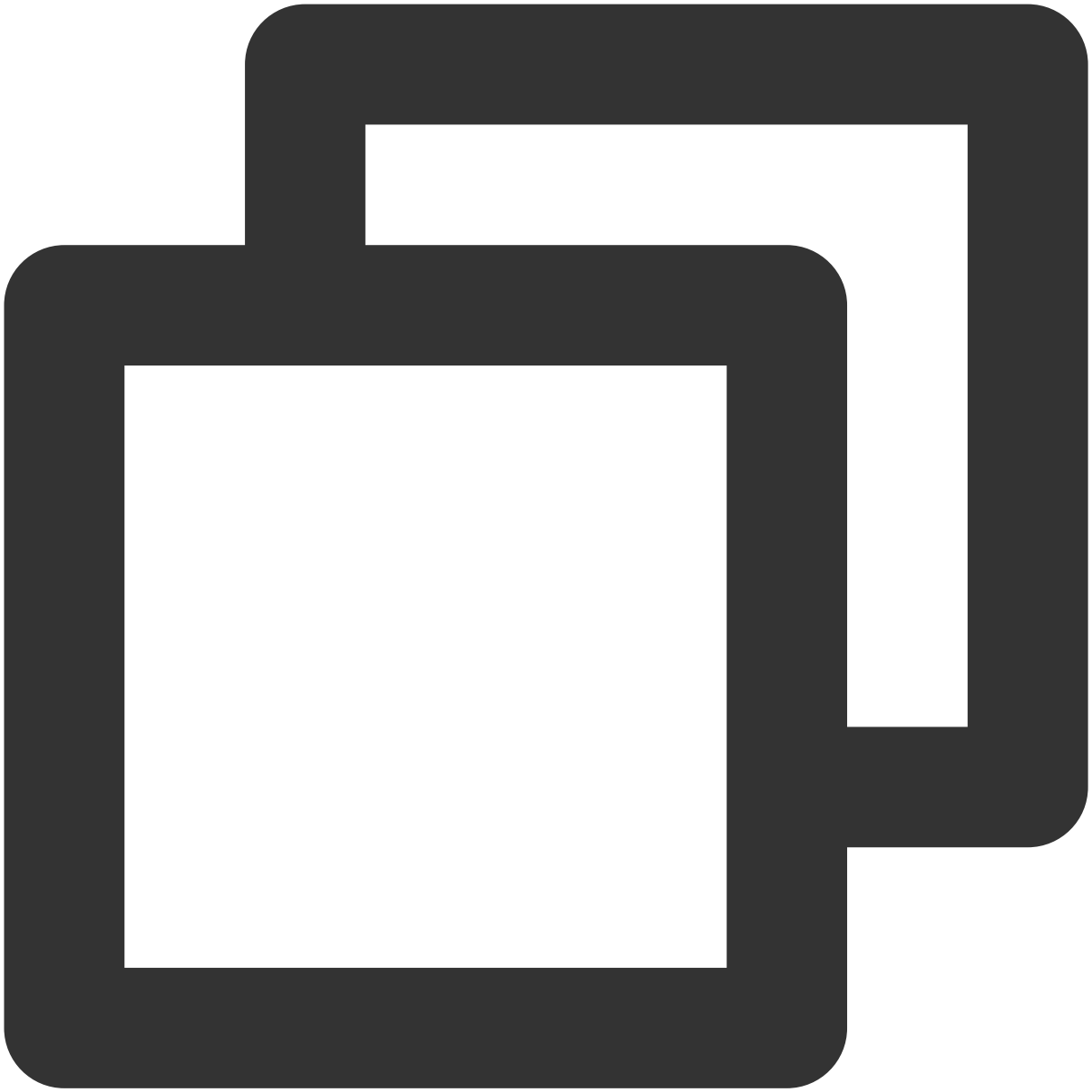
実行結果は下図に示すように：

```
[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"
  }
]
```

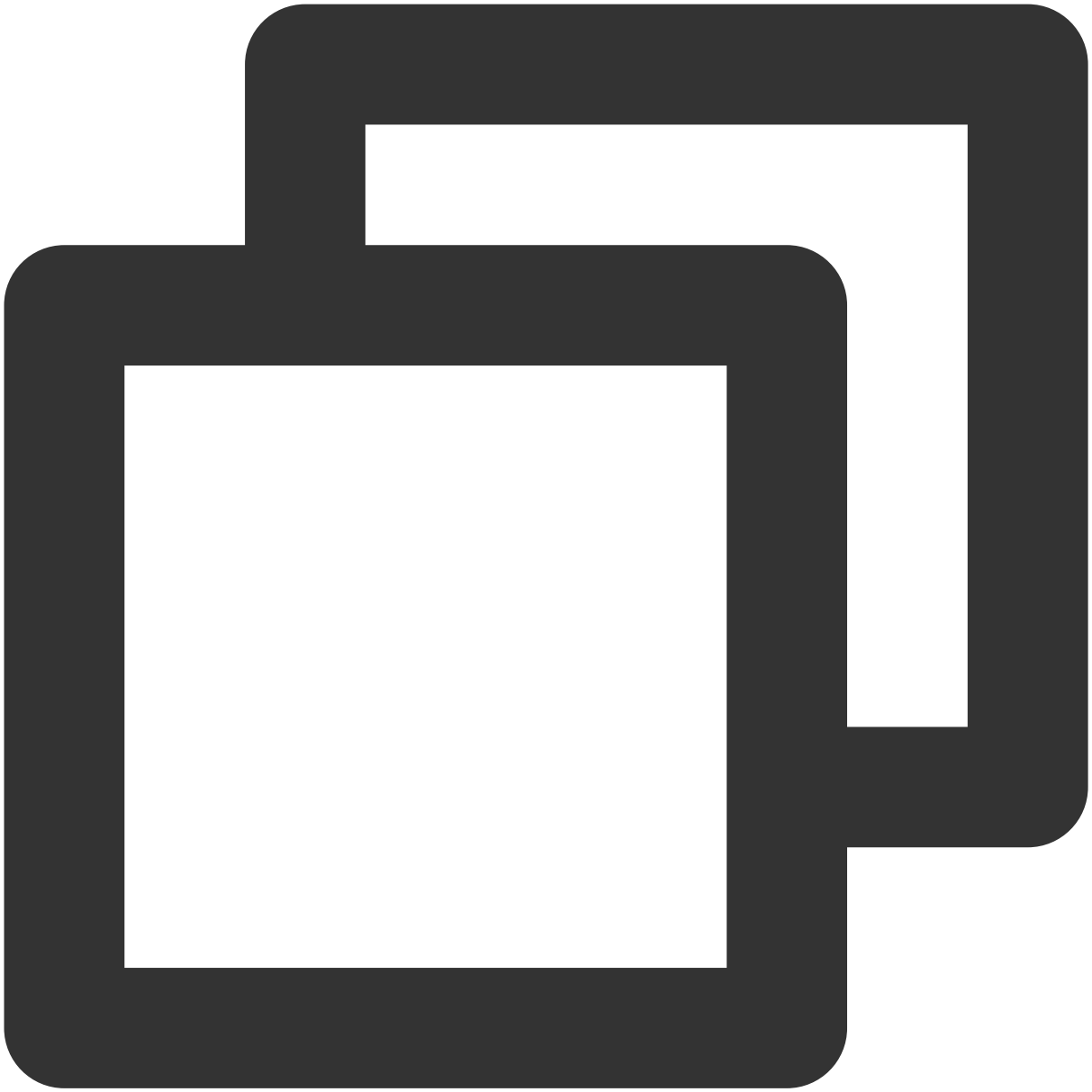
拡張機能（オプション）

この手順で機能を拡張し、次のコマンドを順に実行することで、PMEMを使用してCVMのメモリを拡張することができます。

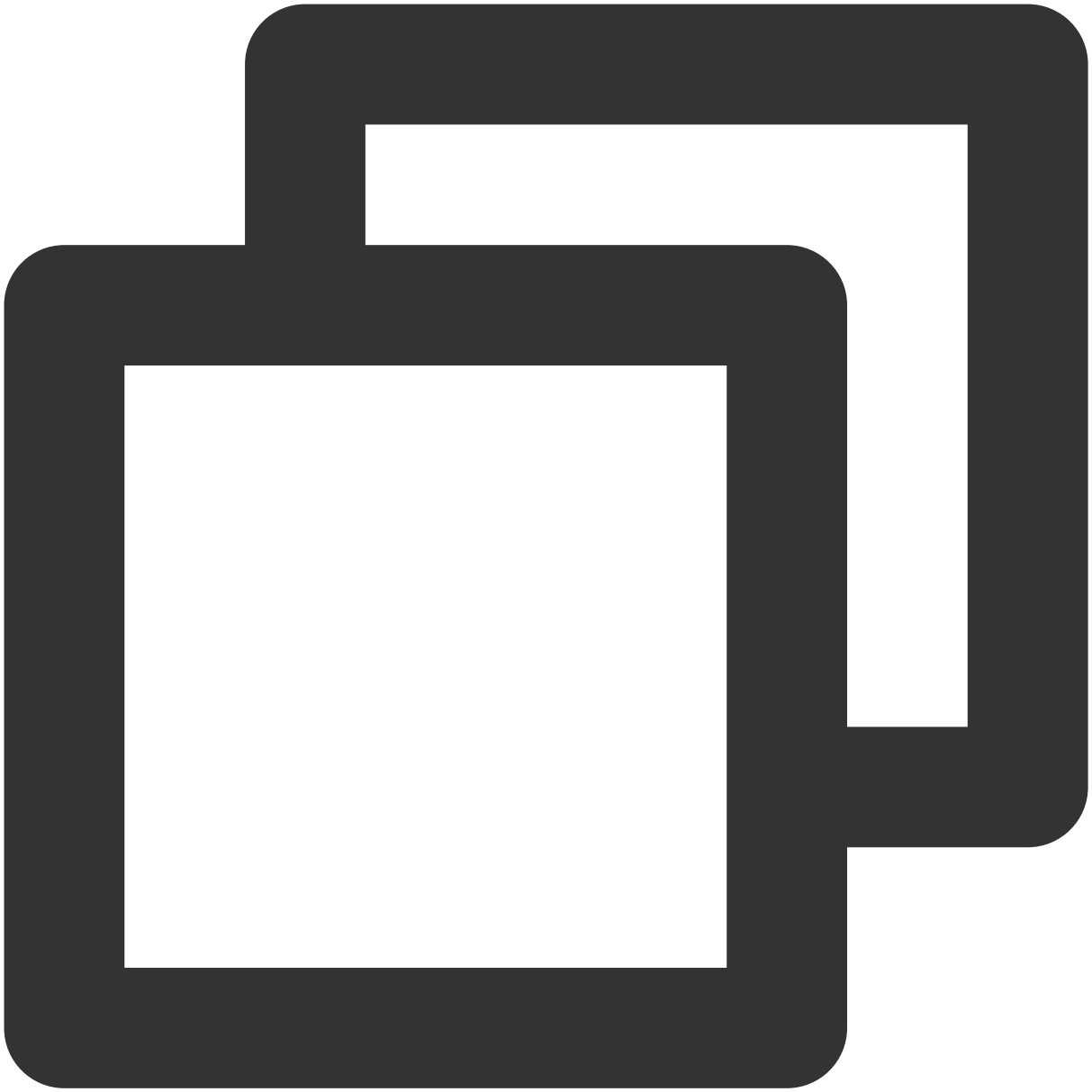
1. 上位バージョンのカーネル（5.1以上かつKMEM DAXドライバーを使用、例：TencentOS Server 3.1のカーネル）のサポートにより、devdaxモードのPMEMをさらにkmemdaxに構成すると、PMEMを使用して、CVMのメモリを拡張することができます。



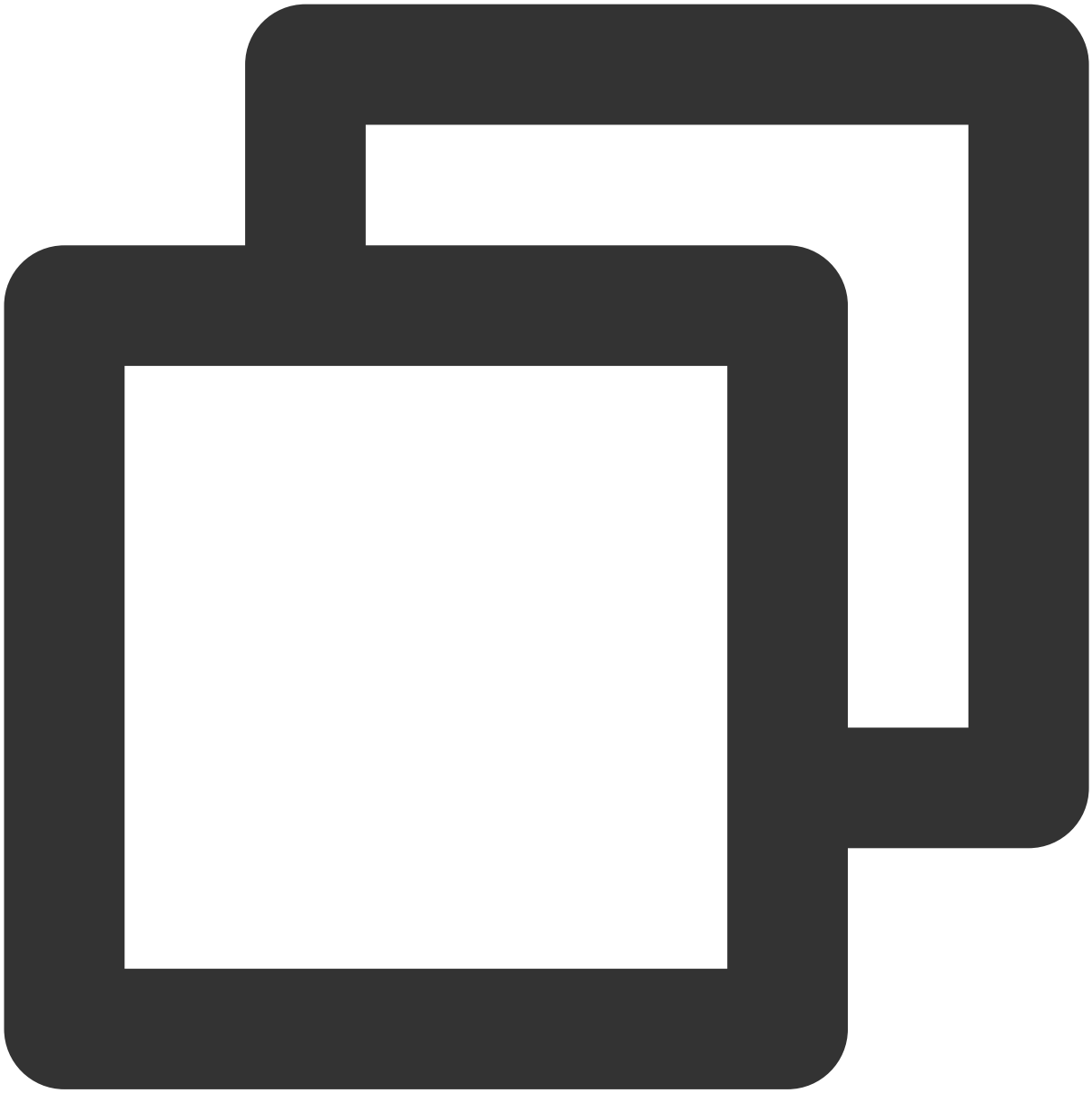
```
yum install -y daxctl
```



```
daxctl migrate-device-model
```



```
reboot
```

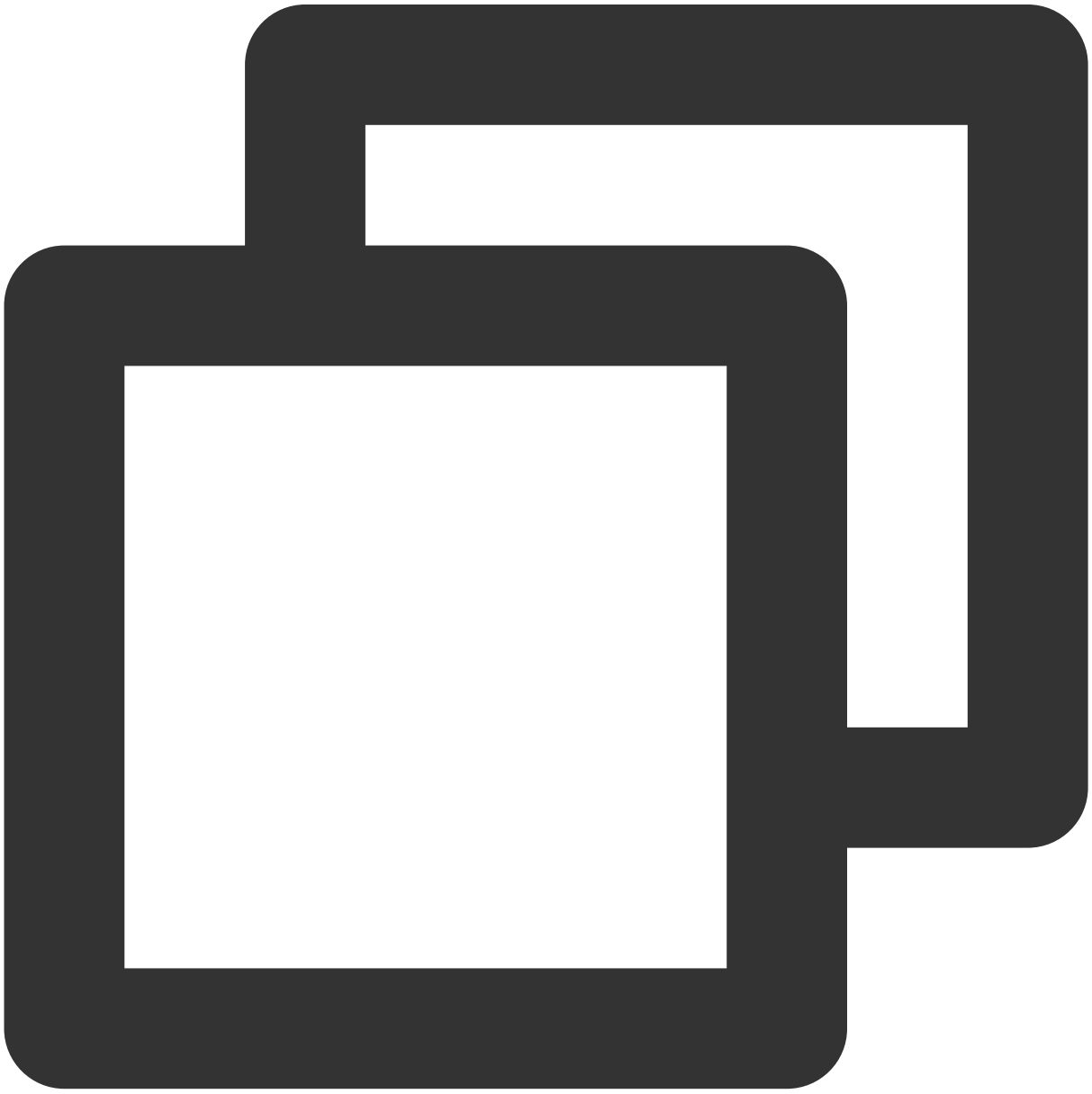


```
daxctl reconfigure-device --mode=system-ram --no-online dax0.0
```

実行結果は下図に示すように：

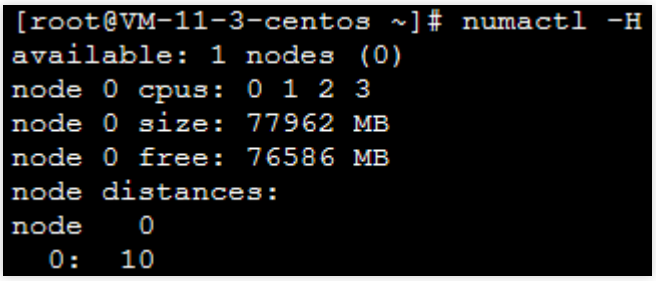
```
[root@VM-11-3-centos ~]# daxctl reconfigure-device --mode=system-ram --no-c
[
  {
    "chardev":"dax0.0",
    "size":65542291456,
    "target_node":0,
    "mode":"system-ram"
  }
]
```

2. 次のコマンドを実行して、システムメモリの拡張状況を確認します。



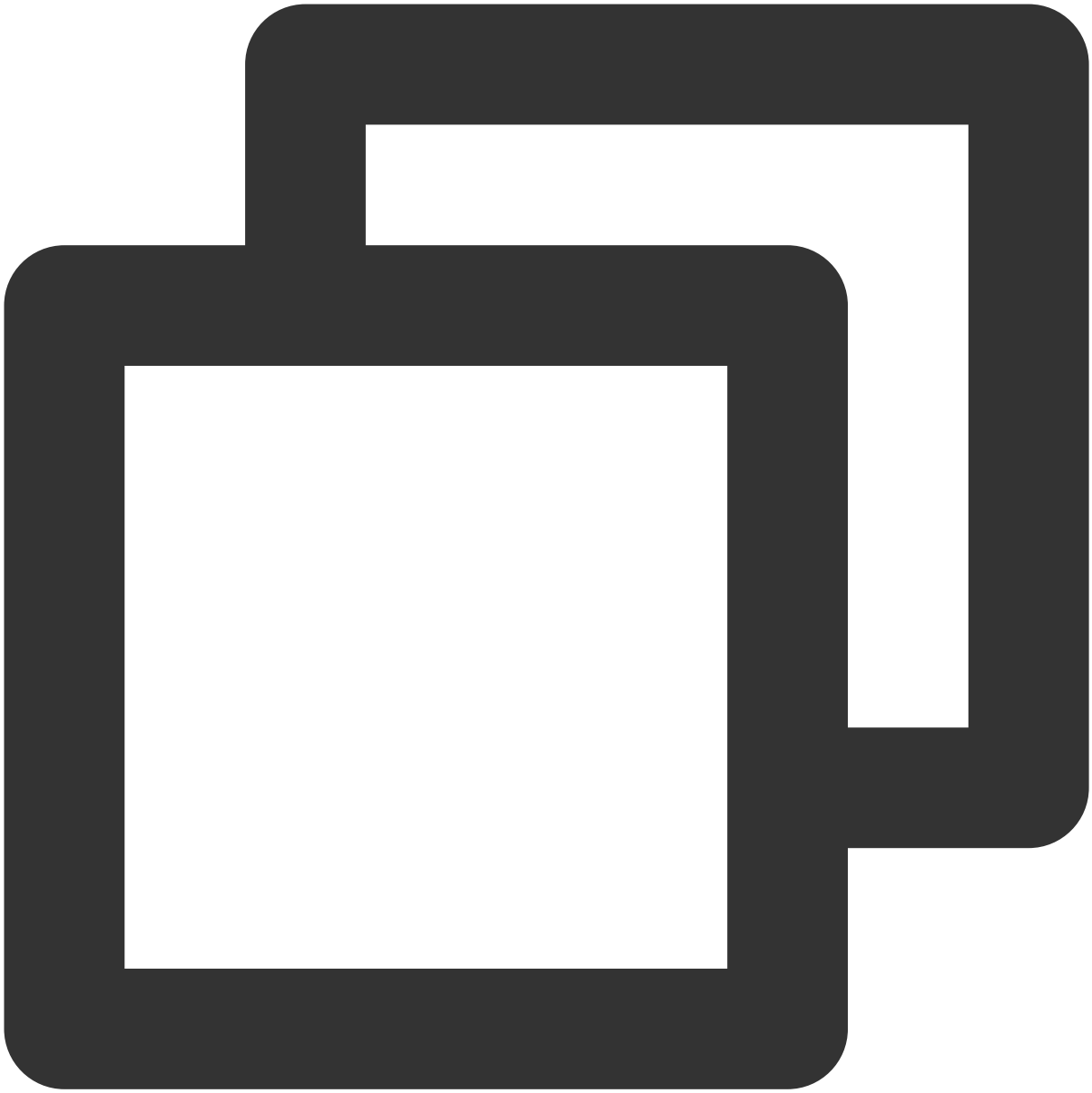
```
numactl -H
```

実行結果は下図に示すように：



ADモードのPMEMは、高速ブロックデバイスとして構成することもでき、ファイルシステムの作成やベアディスクの読み取り・書き込み操作など、一般的なブロックデバイスとして使用できます。構成方法は以下のとおりです。

1. 次のコマンドを実行して、 `/dev` ディレクトリにpmem0ブロックデバイスを生成します。

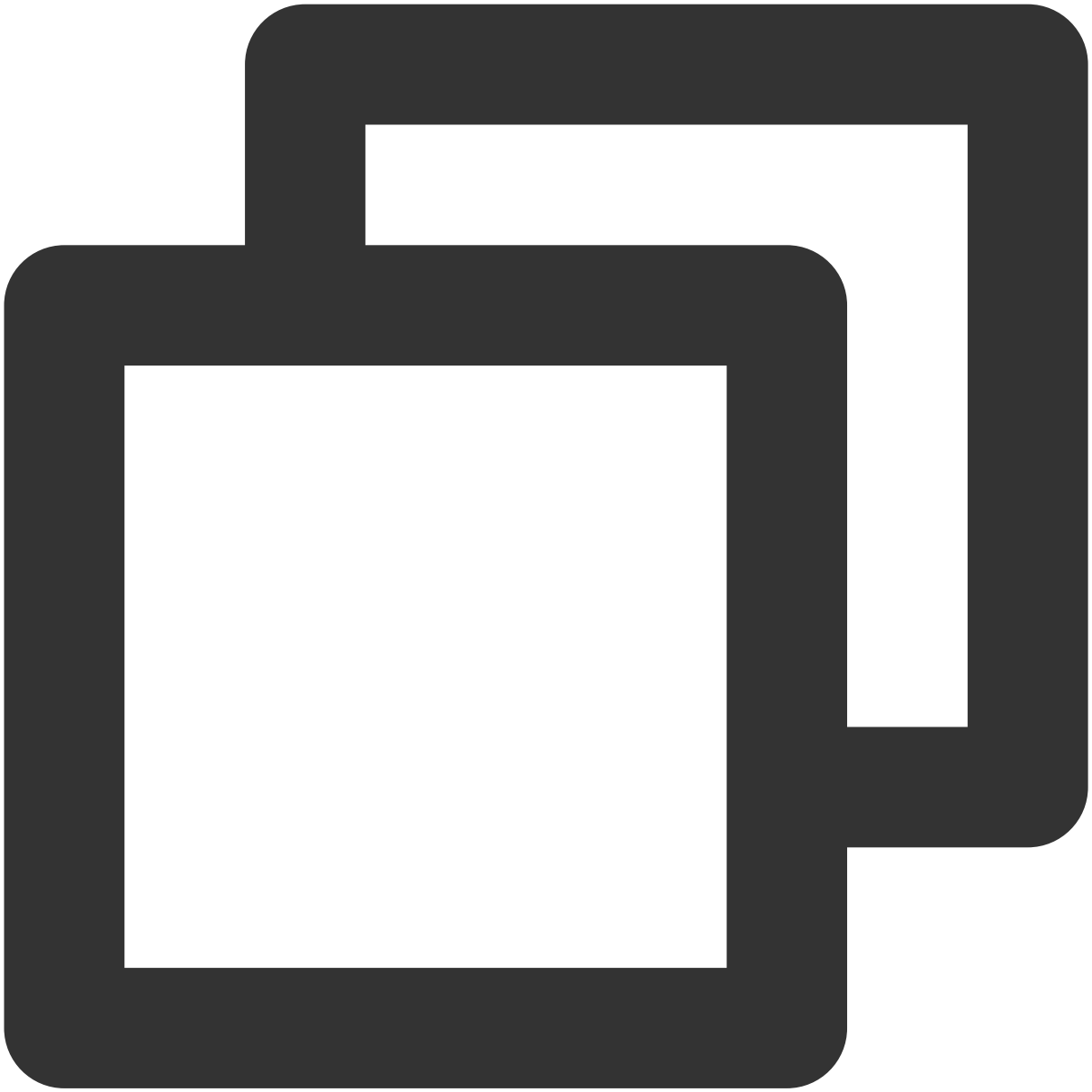


```
ndctl create-namespace -r region0 -m fsdax
```

実行結果は下図に示すように：

```
[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-[illegible]",
  "sector_size":512,
  "align":2097152,
  "blockdev":"pmem0"
}
```

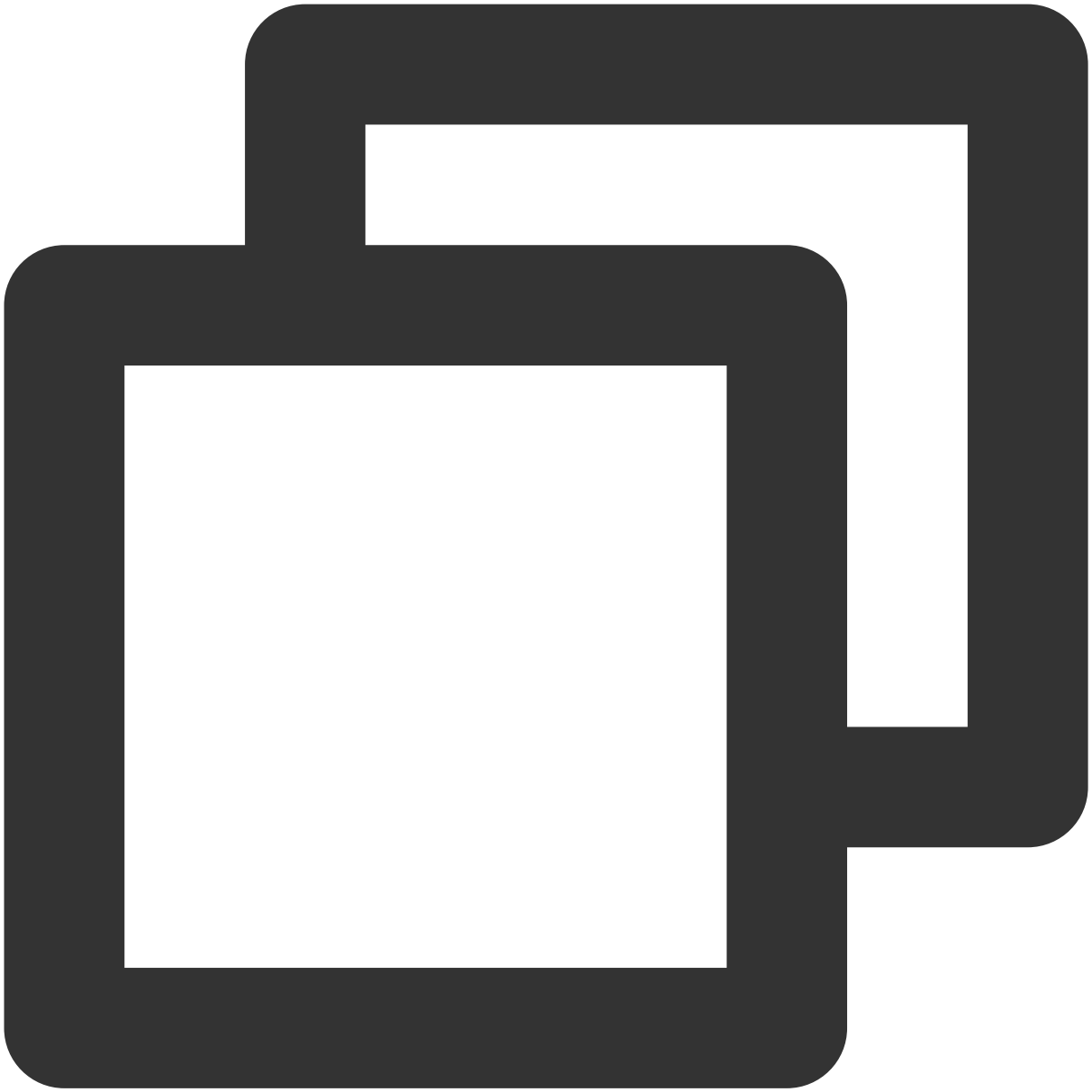
最大仕様のインスタンスには2つのregionがあります。最大仕様のインスタンスを使用する場合は、次のコマンドを同時に実行してください。



```
ndctl create-namespace -r region1 -m fsdax -f
```

2. 次のコマンドを順に実行して、ファイルシステムを作成するか、マウントして使用します。

2.1 ファイルシステムを作成します。

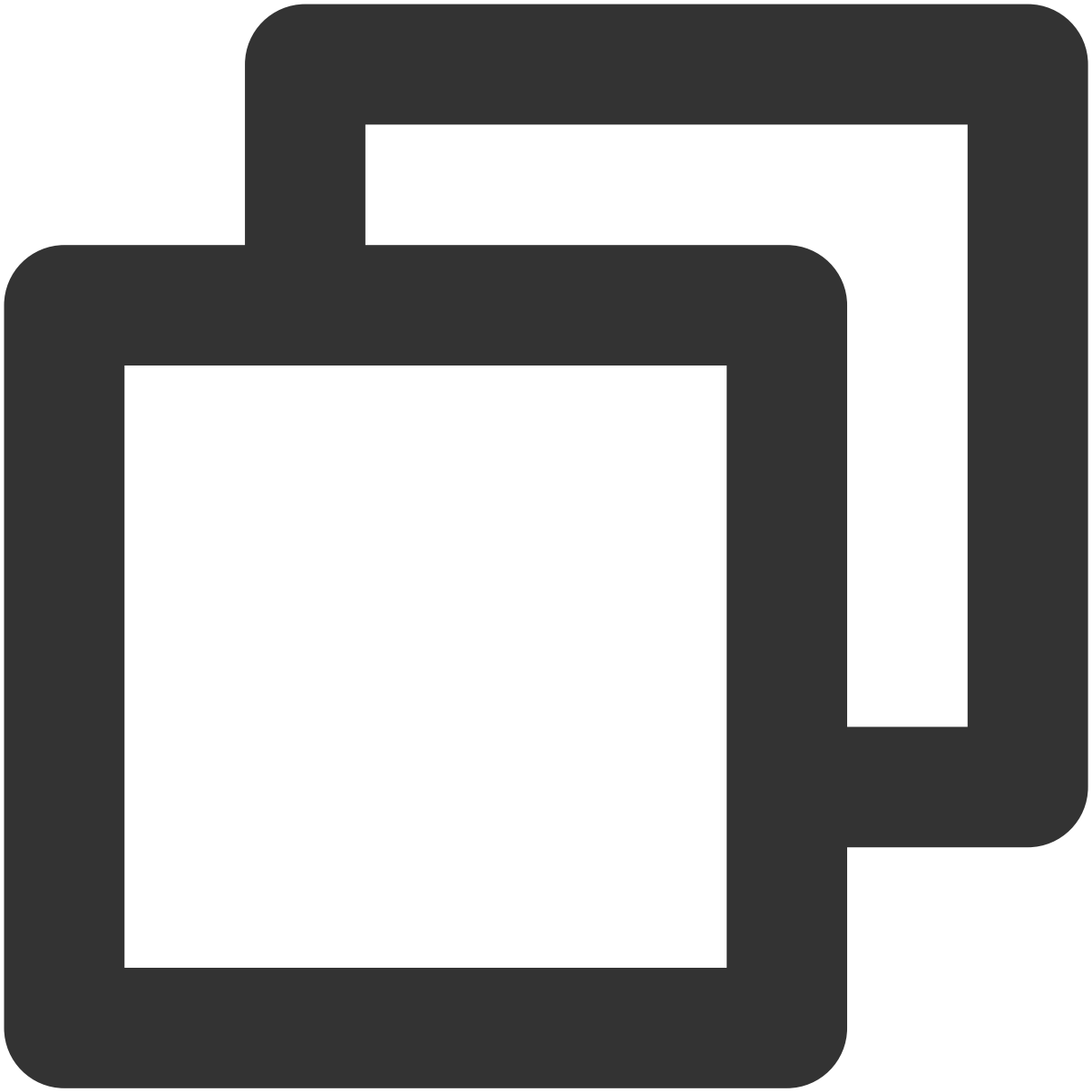


```
mkfs.ext4 /dev/pmem0
```

返された結果を下図に示します。これは、ファイルシステムの作成が成功したことを示しています。

```
[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-[illegible]
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 265
        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/` にマウントします。



```
mount -o dax,noatime /dev/pmem0 /mnt/
```

参考資料

Intel® Optane™ DC Persistent Memory

Linux Provisioning for Intel® Optane™ Persistent Memory

Python 経由でクラウド API を呼び出してカスタムイメージを一括共有

最終更新日：：2023-06-25 18:00:02

操作步骤

このドキュメントでは、Python SDKを使用してAPIを呼び出し、サブユーザーを通じてCVMのカスタムイメージを一括でまとめて共有する方法について説明します。同様のニーズがある場合、またはSDKの使用方法を知りたい場合は、このドキュメントをご覧ください。

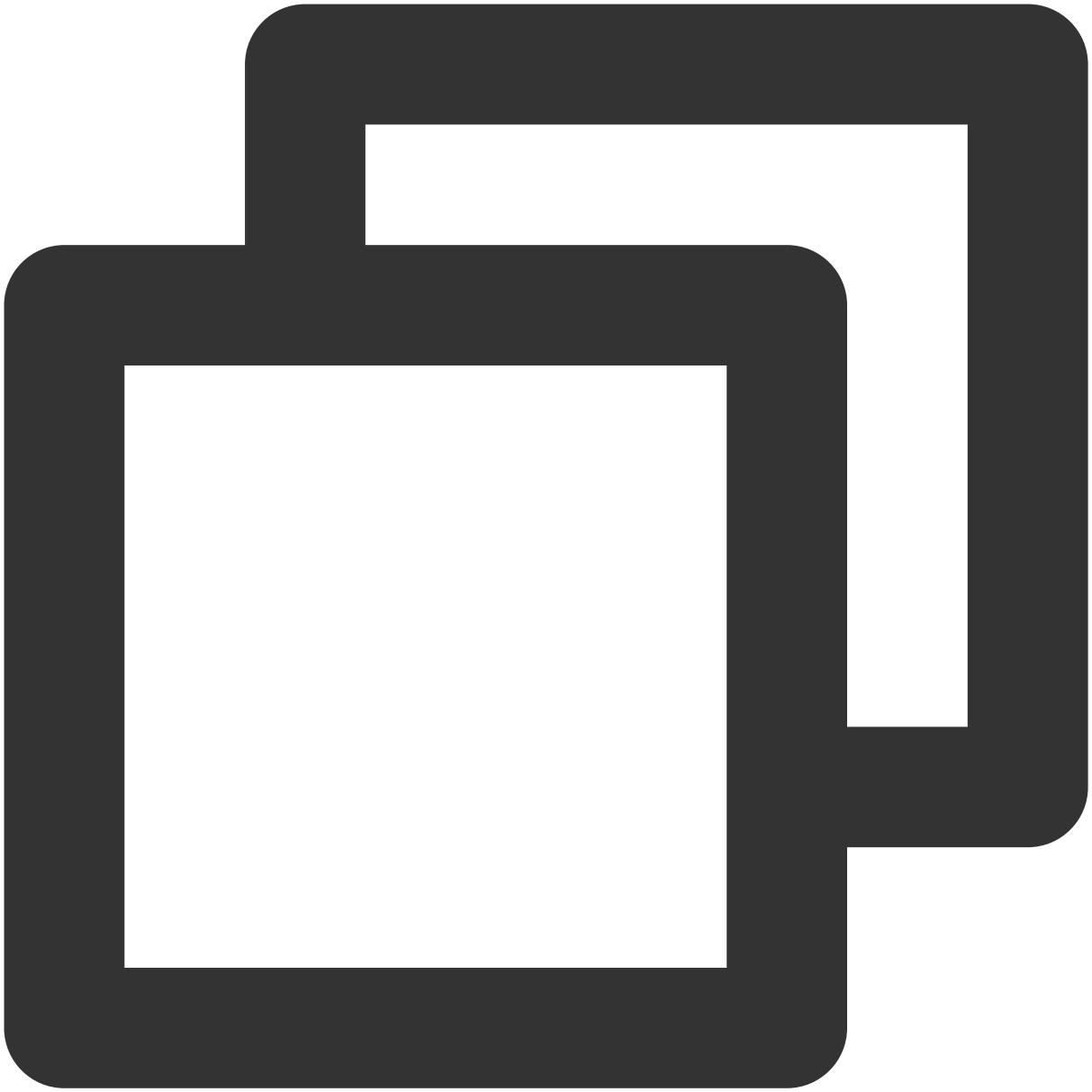
前提条件

サブユーザーを作成しました。そのサブユーザーは CVM およびクラウド APIに対するすべての権限を持ちます。
サブユーザーの作成方法については、 サブユーザーの作成 をご参照ください。
サブユーザーに権限を付与する方法については、サブユーザー権限の設定 をご参照ください。このドキュメントでは、サブユーザーに `QcloudCVMFullAccess` と `QcloudAPIFullAccess` のプリセットポリシーを付与します。
サブユーザーの SecretId と SecretKey を作成します。操作手順については、アクセスキー をご参照ください。作成したSecretId と SecretKeyを適切に保存する必要があります。
共有するカスタムイメージがあります。カスタムイメージを作成する必要がある場合は、 カスタムイメージの作成 をご参照ください。

操作手順

Pythonのインストール

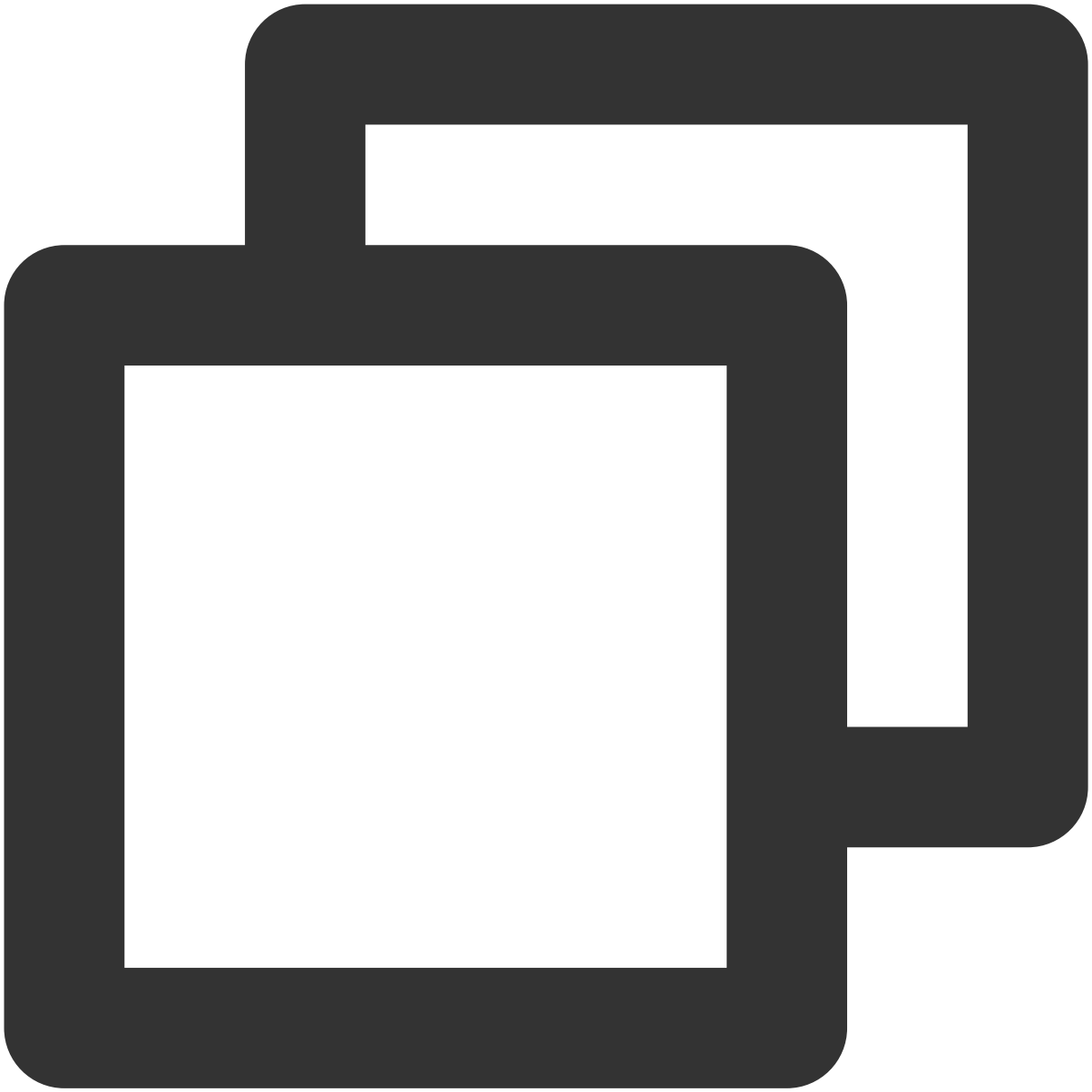
1. 次のコマンドを実行して、Python 3.6 以降が現在のCVMインスタンスにインストールされているかどうかを確認します。インストールされている場合は、このステップをスキップしてください。



```
python --version
```

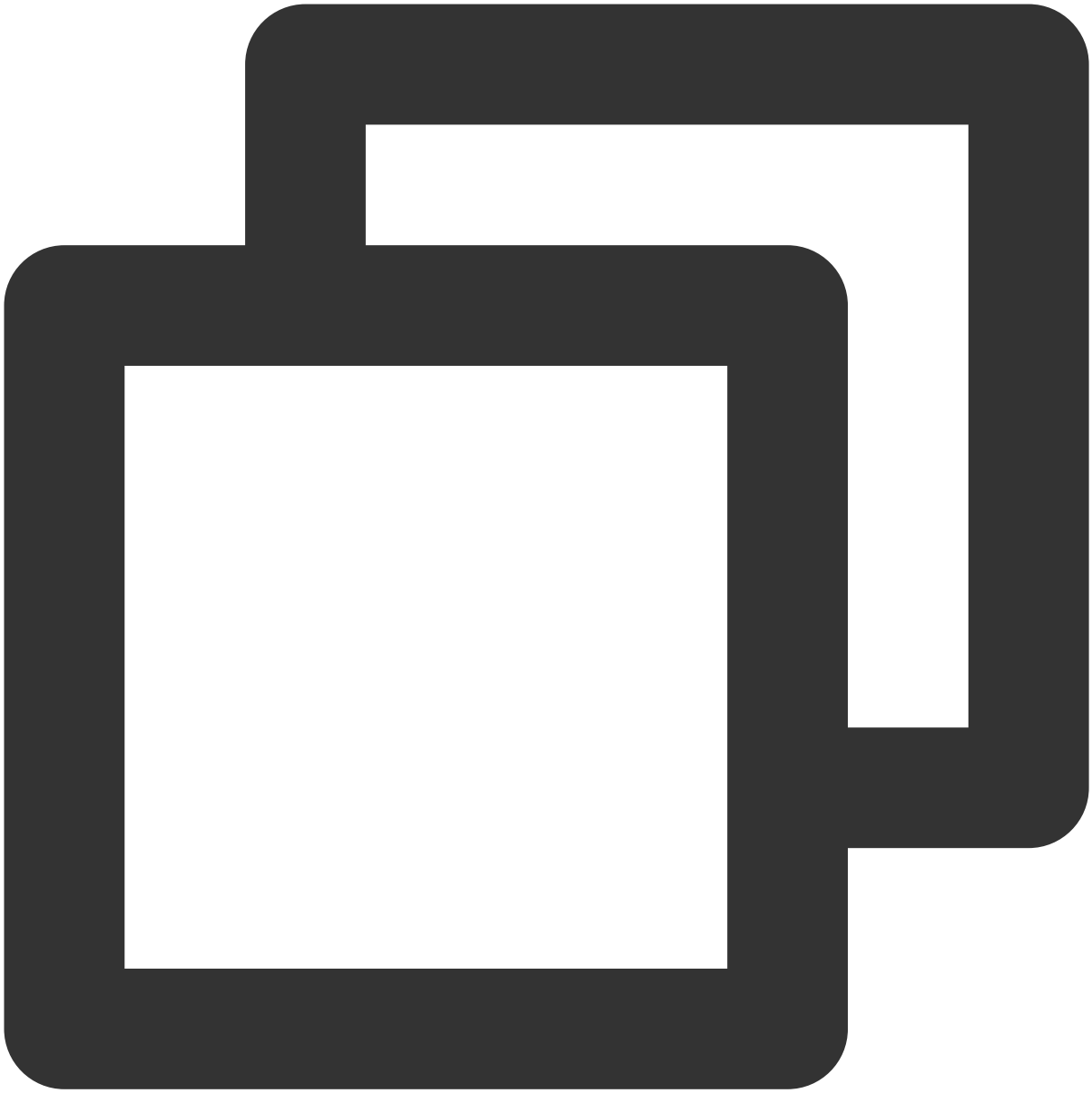
2. CVMインスタンスに Python がインストールされていない場合。

CentOS 上の CVM インスタンスの場合は、次のコマンドを実行して Python をインストールします。



```
yum install python3
```

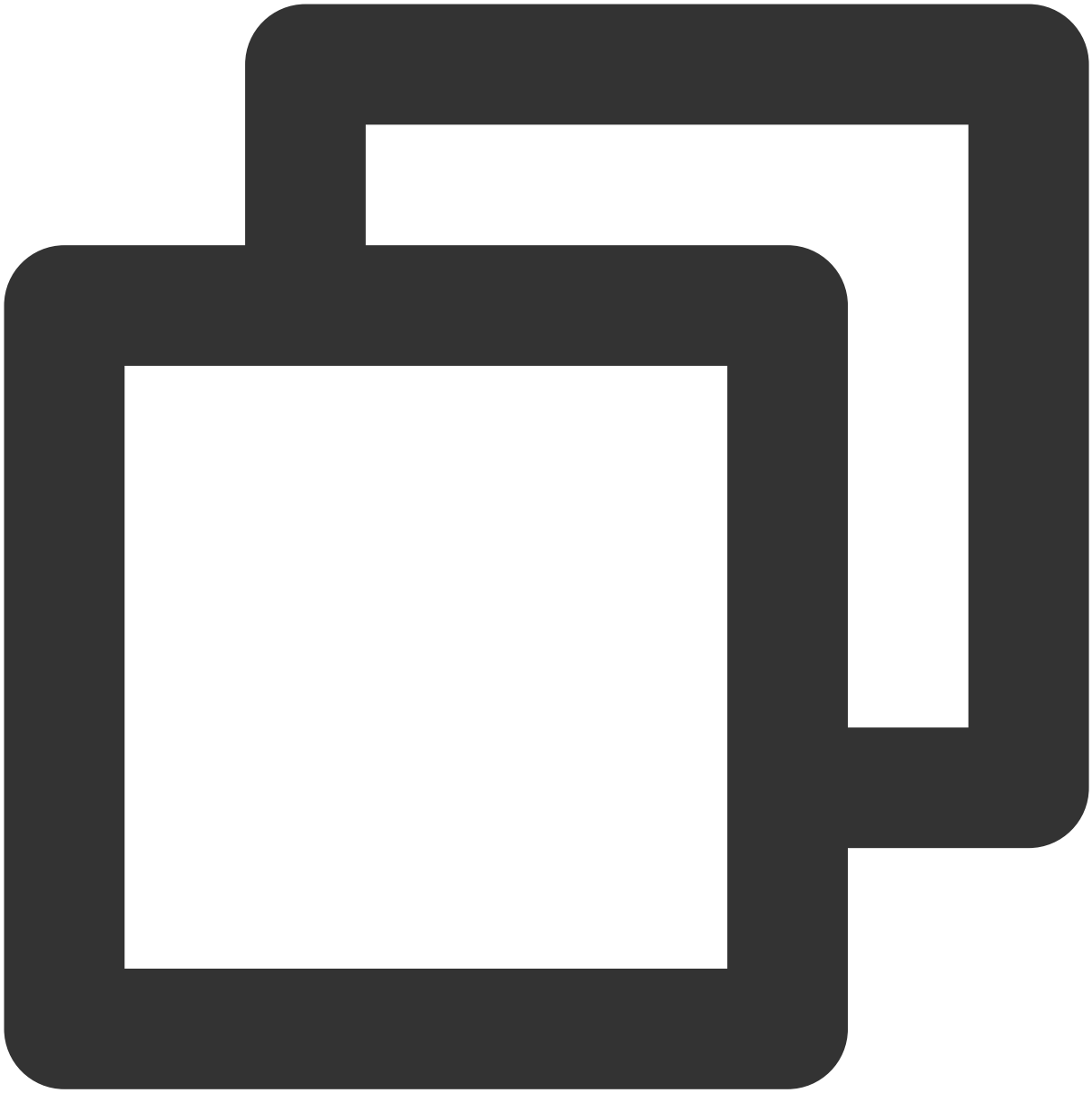
Ubuntu または Debian上のCVM インスタンスの場合は、次のコマンドを実行して Python をインストールします。



```
sudo apt install python3
```

他のOS上の CVM インスタンスの場合は、 Python 公式ウェブサイト にアクセスし、Python 3.6 以降をダウンロードし、インストールパッケージを Linux サーバーにアップロードし、パッケージを解凍してPython をインストールします。

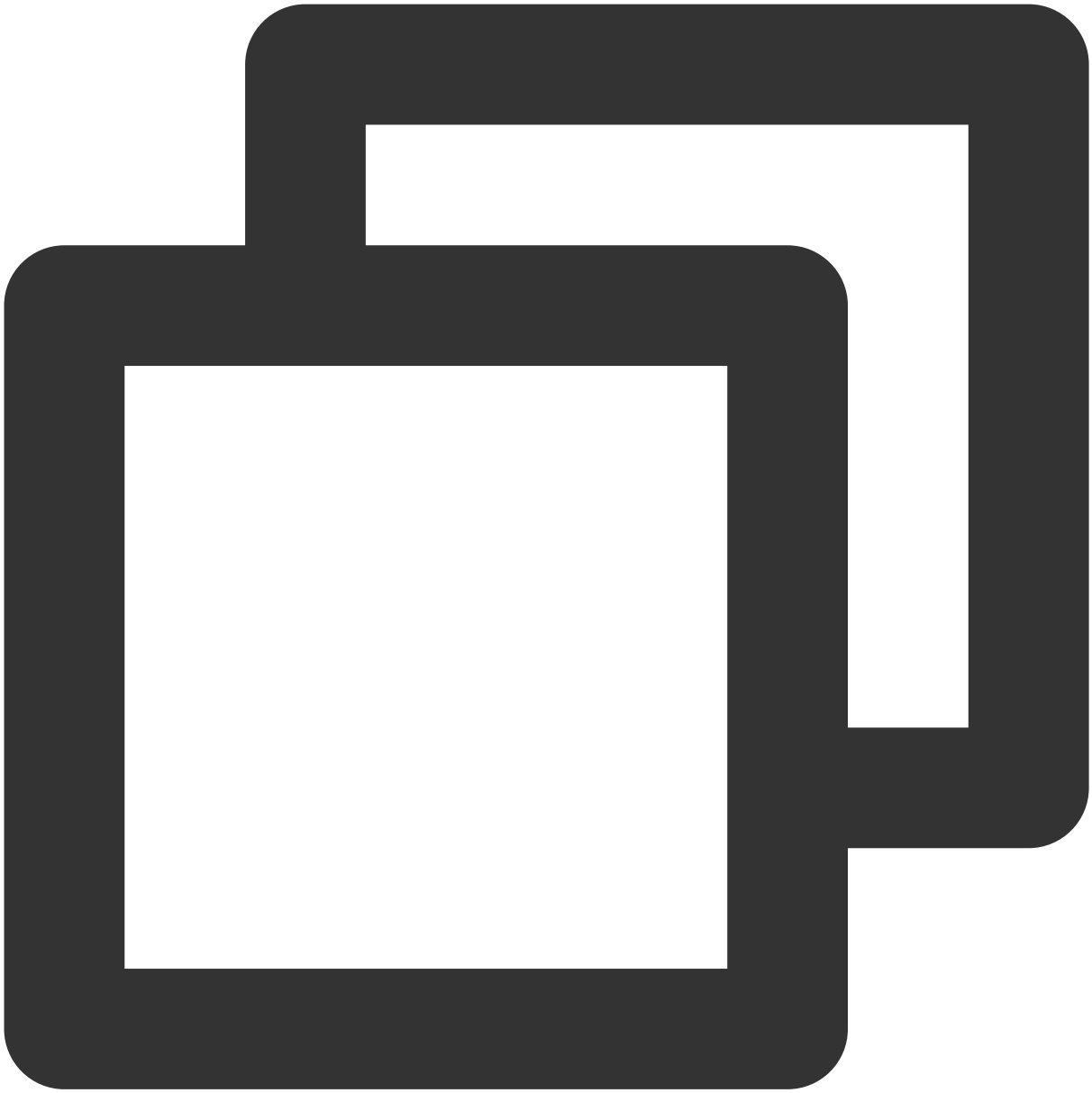
3. インストールが完了したら、次のコマンドを実行して Python のバージョンを確認します。



```
python --version
```

コード作成

1. ターゲットマシン上に `test.py` ファイルを作成し、次のコードを入力します。



```
import json
from tencentcloud.common import credential
from tencentcloud.common.profile.client_profile import ClientProfile
from tencentcloud.common.profile.http_profile import HttpProfile
from tencentcloud.common.exception.tencent_cloud_sdk_exception import TencentCloudS
from tencentcloud.cvm.v20170312 import cvm_client, models
# デフォルトでは、環境変数 TENCENTCLOUD_SECRET_ID および TENCENTCLOUD_SECRET_KEY を読み取
# 認証情報の管理方法の詳細については、https://github.com/TencentCloud/tencentcloud-sdk-py
cred = credential.EnvironmentVariableCredential().get_credential()
httpProfile = HttpProfile()
httpProfile.endpoint = "cvm.tencentcloudapi.com"
```

```
clientProfile = ClientProfile()
clientProfile.httpProfile = httpProfile
# この例では南京が使用されています。 実際の状況に応じてリージョンを変更します。 たとえば、上海の場合
aria = 'ap-nanjing'
client = cvm_client.CvmClient(cred,aria, clientProfile)
def img_share(img_id,img_name,accountids):
 try:
     req1 = models.ModifyImageSharePermissionRequest()
     params1 = {
         "ImageId": img_id,
         "AccountIds": accountids,
         "Permission": "SHARE"
     }
     req1.from_json_string(json.dumps(params1))

     resp1 = client.ModifyImageSharePermission(req1)
     response1 = json.loads(resp1.to_json_string())
     print(img_name,'共有成功！',response1)
 except TencentCloudSDKException as err:
     print(img_name,'共有失敗!',err)
try:
 req = models.DescribeImagesRequest()
 params = {
     "Filters": [
         {
             "Name": "image-type",
             "Values": ["PRIVATE_IMAGE"]
         }
     ],
     "Limit": 100
 }
 req.from_json_string(json.dumps(params))
 resp = client.DescribeImages(req)
 response = json.loads(resp.to_json_string())
 img_num = response["TotalCount"]
 print('イメージリストを取得中....')
 share_config = input('1.すべてのイメージを共有します\\n\\n2.. 共有するイメージを決定します\
 accountids = input('イメージを共有するユーザーの UIN を入力し、複数のUINをカンマで区切ってく
 for i in range(img_num):
     basic = response['ImageSet'][i]
     img_id = basic['ImageId']
     img_name = basic['ImageName']
     if share_config == '1':
         img_share(img_id,img_name,accountids)
     elif share_config == '2':
         print('イメージID：',img_id,'イメージ名：',img_name)
         share_choice = input('このイメージを共有するかどうか y/n:') or 'y'
```

```
            if share_choice == 'y':
                img_share(img_id,img_name,accountids)
            elif share_choice == 'n':
                continue
            else:
                print('正しいオプションを入力してください！！')
        else:
            print('正しいオプションを入力してください！！')
    except TencentCloudSDKException as err:
     print(err)
```

SecretId と SecretKey： 前提条件 で作成したサブユーザーのSecretIdとSecretKey に置き換えてください。
aria：共有するカスタムイメージが存在する実際のリージョンに置き換えてください。詳細については、共通パラメータ をご覧ください。
2. ターゲットマシンで次のコマンドを実行してコードを実行します。
画面上の指示に従って1または2を入力(すべてのイメージを同時に共有するか、イメージを 1 つずつ選択して共有するかを選択)、ピアアカウントIDを入力します。ピアアカウント所有者に アカウント情報 ページに移動してアカウントIDを取得するように通知できます。
イメージが正常に共有されると、対応する数の RequestID が返されます。

関連する API ドキュメント

このドキュメントで使用されるAPIは DescribeImages と ModifyImageSharePermissionです。