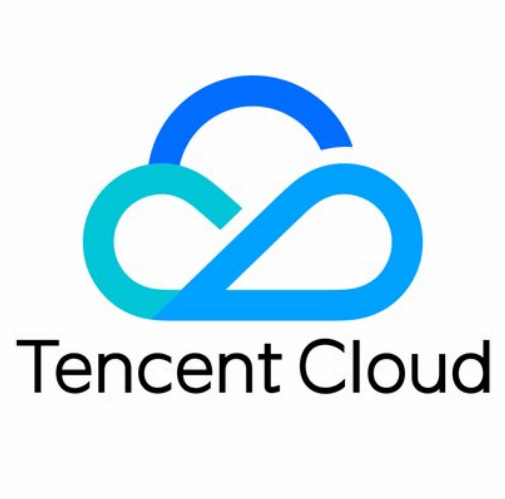
Cloud Virtual Machine

トラブルシューティング

製品ドキュメント



カタログ：

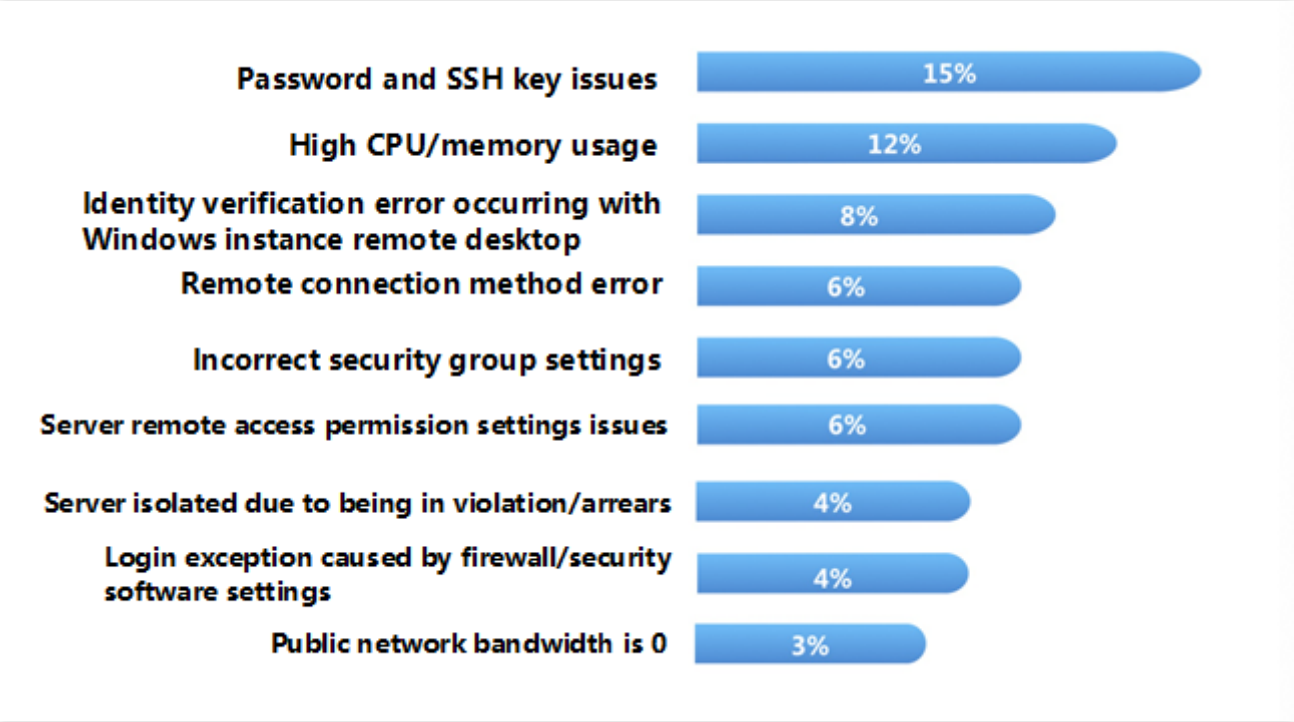
トラブルシューティング
インスタンス関連障害
CVMインスタンスにログインできない原因や対処法

最終更新日：：2023-05-16 09:54:55

このドキュメントでは、Cloud Virtual Machine（CVM）インスタンスの購入後にログインできない原因を特定し、問題を解決するのに役立ちます。

考えられる原因

次の図は、CVMインスタンスにログインできない主な原因とその発生確率を示しています。インスタンスにログインできない場合は、インテリジェント診断ツールを使用して、以下の手順に従ってトラブルシューティングを実行することをお勧めします。



トラブルシューティング

インスタンスタイプを確認する

最初に、購入したインスタンスがWindows システムインスタンスか Linuxシステムインスタンスかを判断する必要があります。インスタンスにログインできない原因は、インスタンスタイプによって異なります。購入したインスタンスタイプに応じて、次のドキュメントを参照して問題を特定して解決します。

Windows インスタンスにログインできない

Linuxインスタンスにログインできない

診断ツールを使用して原因を特定する

Tencent Cloudは、セルフ診断ツールとセキュリティグループ(ポート)検証ツール を提供し、ログインできない原因を特定するのに役立ちます。70%以上のログイン問題は、このツールでチェックして特定できます。

セルフ診断ツール

このツールを使用すると、帯域幅の使用率が高すぎる、パブリックネットワーク帯域幅が0、サーバの負荷が高い、不適切なセキュリティグループルール、DDoS攻撃のブロック、セキュリティ分離やアカウントの滞納など、さまざまな問題を診断できます。

セキュリティグループ（ポート）検証ツール

このツールは、セキュリティグループとポートに関連する故障を診断できます。セキュリティグループ設定に問題がある場合は、このツールの「すべてのポートを開く」機能を通じて、セキュリティグループの一般的に使用されるすべてのポートを開くことができます。
このツールを使用して問題の原因を特定した場合、対応する問題のガイドラインに従って問題を解決することをお勧めします。

インスタンスの再起動

診断ツールで該当の故障を特定して処理した後、あるいは診断ツールを使用してログインできない原因を特定できない場合、インスタンスを再起動してリモートで再接続し、接続が成功するかどうかを確認できます。
インスタンスを再起動する方法については、インスタンスの再起動 をご参照ください。

ログイン失敗のその他の一般的な原因

上記の手順を実行しても問題の原因が特定できない場合、またはCVMへのログイン時に次のエラーメッセージが表示される場合は、次の解決策をご参照ください。

Windows インスタンス

Windows インスタンス：リモートデスクトップサービスを使ったログオンを拒否

Windows インスタンス：Mac用のリモートデスクトップクライアントを使用したインスタンスへのログインに失敗

Windowsインスタンス：認証エラーが発生した

Windows インスタンス：リモートデスクトップはリモートコンピューターに接続できません

Linuxインスタンス

Linux インスタンス: CPU とメモリの使用率が高いためログインできません

後続操作

上記の手順を実行してもリモートデスクトップ接続ができない場合は、関連するログと自己診断結果を保存してから、チケットを送信してください。

Windowsインスタンス関連
Windows のインスタンスにログインできない

最終更新日：：2023-04-21 15:01:49

このドキュメントでは主にWindowsインスタンスに接続できない場合のトラブルシューティング方法と、Windowsインスタンスに接続できない主な原因について解説し、問題のトラブルシューティング、特定および解決について説明します。

考えられる原因

Windowsインスタンスにログインできない主な原因：
パスワードの問題によりログインできない
帯域幅利用率が高すぎる
サーバー負荷が高い
リモートポート設定の異常
セキュリティグループルールが不適切
ファイアウォールまたはセキュリティソフトによるログインの異常
リモートデスクトップ接続における認証エラー

自己診断ツールの使用

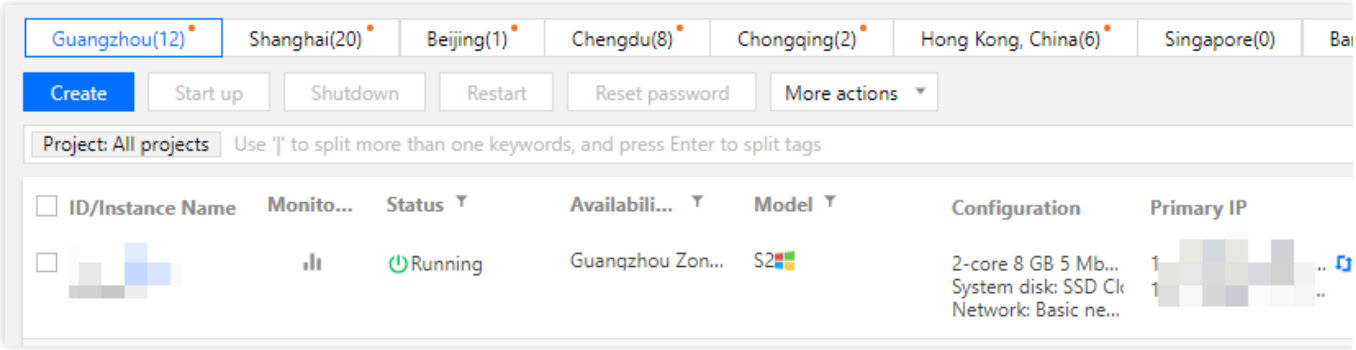
Tencent Cloudは、Windowsインスタンスに接続できない原因が、帯域幅、ファイアウォールおよびセキュリティグループの設定などの一般的な問題かどうかを判断するのに役立つ自己診断ツールを提供しています。 障害の70%はツールで特定でき、検出された問題をもとにログインできない原因となっている可能性のある障害を特定できます。
1. セルフチェック をクリックし 、自己診断ツールを開きます。
2. ツールインターフェースのプロンプトに基づき、診断したいCVMを選択し、**検出開始**をクリックします。
トラブルシューティングツールによって確認できない問題については、CVMに VNC方式でログイン し、段階ごとにトラブルシューティングを実施することをお勧めします。

障害処理

VNC 方式を介したログイン

RDPまたはリモートログインソフトウェアを使用してWindowsインスタンスにログインできない場合は、Tencent Cloud VNC方式でログインし、障害の原因特定に役立てることができます。

1. Tencent Cloudコンソール にログインします。
2. 下図のように、インスタンスの管理画面で、ログインしたいインスタンスを選択し、**ログイン**をクリックします。

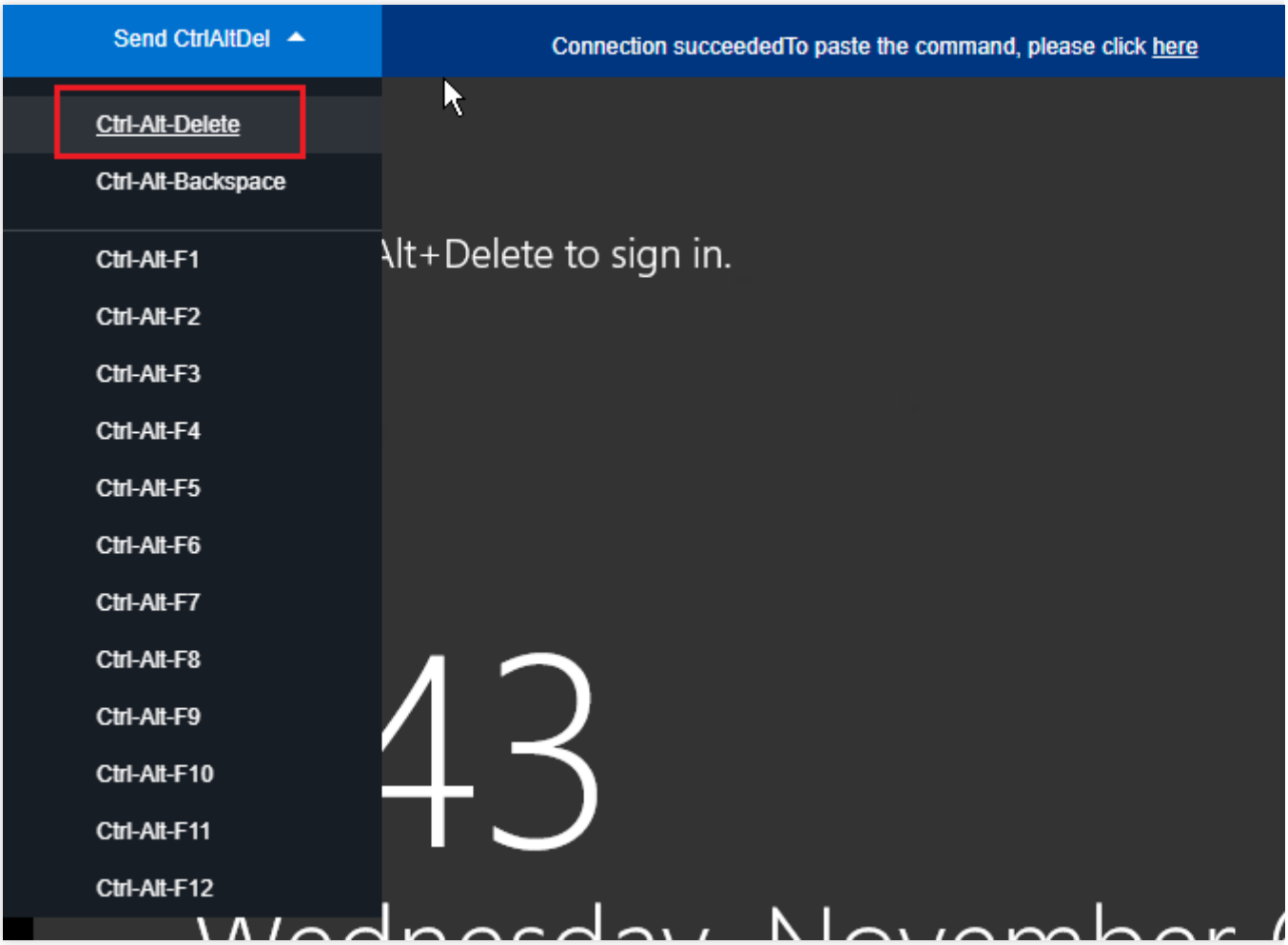


3. ポップアップした「標準ログイン | Windowsインスタンス」ウィンドウで、**VNCログイン**を選択します。

説明：

ログイン中に、パスワードを忘れた場合は、コンソールでこのインスタンスのパスワードをリセットできます。具体的な操作については、インスタンスのパスワードをリセット ドキュメントをご参照ください。

4. 下図のように、ポップアップしたログインウィンドウで、左上の「リモートコマンドの送信」を選択し、 Ctrl-Alt-Deleteをクリックしてシステムログイン画面に進みます。



パスワードの問題によりログインできない

障害事象：パスワードの入力ミス、パスワードを忘れた、パスワードのリセットに失敗したなどの理由で正常にログインできない。
処理手順：Tencent Cloudコンソール でインスタンスのパスワードをリセットし、インスタンスを再起動してください。詳細については、インスタンスのパスワードをリセット ドキュメントをご参照ください。

帯域幅利用率が高すぎる

障害事象：自己診断ツールによって、帯域幅利用率が高すぎることが問題だと表示された。
処理手順：
1. VNCログイン によってインスタンスにログインします。
2. 帯域幅の利用率が高いためログインできない ドキュメントを参照し、インスタンスの帯域幅使用状況および障害の処理について確認します。

サーバー負荷が高い

障害事象：セルフチェックツールまたはTCOPによって、サーバーのCPU負荷が高いためにシステムがリモート接続できなくなっている、またはアクセスが非常に遅くなっていると表示された。

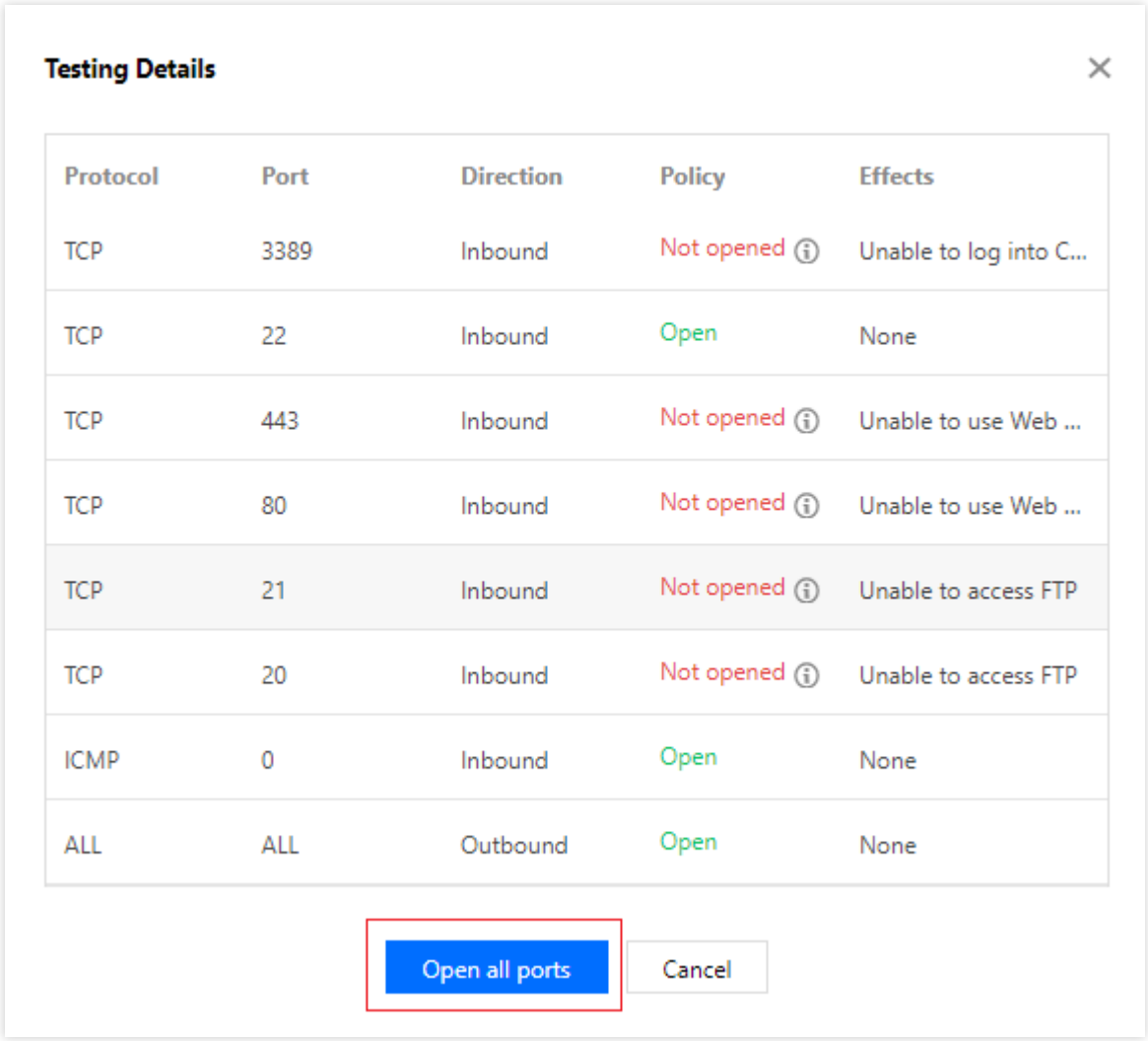
考えられる原因：ウイルスやトロイの木馬、サードパーティ製のウイルス対策ソフト、アプリケーションプログラムの異常、ドライバーの異常、またはソフトウェアのバックエンドでの自動更新によってCPU占有率が高くなり、CVMにログインできない、またはアクセスが遅いといった問題が発生している。
処理手順：
1. VNCログイン によってインスタンスにログインします。
2. Windowsインスタンス：CPUとメモリ占用率が高いため、ログインできない ドキュメントを参照し、「タスクマネージャー」で負荷の高いプロセスを特定します。

リモートポート設定の異常

障害事象：リモート接続ができない、リモートアクセスポートがデフォルトのポートではない、変更されている、またはポート3389が開かない。
問題特定の考え方：pingをインスタンスのパブリックIPに通すことができるかどうか。telnetコマンドによってポートが開いているかどうかをテストする。
処理手順：具体的な操作については、ポート問題が原因でリモートログインできない ドキュメントをご参照ください。

セキュリティグループルールが不適切

障害事象：セルフチェックツールでのチェックの結果、セキュリティグループルールが不適切なためにログインできないことがわかった。
処理手順：セキュリティグループ（ポート）検証ツール によってチェックを行います。
ご注意：
Windowsインスタンスへのリモートログインにはポート3389の開放が必要です。



-セキュリティグループルールのカスタム設定を行いたい場合は、セキュリティグループルールの追加 をご参照の上、セキュリティグループルールを再設定してください。

ファイアウォールまたはセキュリティソフトによるログインの異常

障害事象：CVMファイアウォールの設定またはセキュリティソフトによるログインの異常。

問題特定の考え方：VNCログイン方法でWindowsインスタンスにログインし、サーバー内でファイアウォールが有効になっているか、360、Safedogなどのセキュリティソフトをインストールしているかどうかをチェックする。

ご注意：

この操作はCVMファイアウォールの無効化を伴います。ご自身にこの操作を実行する権限があるかどうかをご確認ください。

処理手順：ファイアウォールまたはインストールされているセキュリティソフトを無効化してからリモート接続をリトライし、リモートログインに成功するかどうかを確認します。以下の操作は Windows Server 2016インスタンスのファイアウォールの無効化を例に説明します。

1. VNCログイン によってインスタンスにログインします。

2. OSの画面で、

をクリックし、**コントロールパネル**を選択し、コントロールパネルウィンドウを開きます。
3. **Windowsファイアウォール**をクリックし、「Windowsファイアウォール」画面に進みます。
4. 左側の**Windowsファイアウォールの有効化または無効化**をクリックし、「設定のカスタマイズ」画面に進みます。
5. 「プライベートネットワークの設定」と「パブリックネットワークの設定」を「Windowsファイアウォールを無効にする」に設定し、**OK**をクリックします。
6. インスタンスを再起動してリモート接続をリトライし、リモートログインに成功するかどうかを確認します。

リモートデスクトップ接続における認証エラー

障害事象：リモートデスクトップを使用したWindowsインスタンスへの接続とログイン時に、「認証エラーが発生しました。関数に提供されたトークンは無効です」または「認証エラーが発生しました。要求された関数はサポートされていません」というエラーが発生する。
問題の原因：Microsoftは2018年3月にセキュリティ更新をリリースしました。この更新はCredential Security Support Providerプロトコル（CredSSP）に基づいてID認証の過程でリクエストを検証する方法によって、CredSSPに存在する、リモートでコードが実行される脆弱性を修正するものです。この更新はクライアントとサーバーの両方にインストールする必要があり、そうしなければ「問題の説明」のような状況が発生する可能性があります。
処理手順：セキュリティ更新をインストールする方法で対処することを推奨します。具体的には、Windowsインスタンス：認証エラーが発生した ドキュメントをご参照ください。

その他の対処方法

上述のトラブルシューティングを行っても、Windowsインスタンスに接続できない場合は、セルフチェック結果を保存し、チケットを提出してフィードバックしてください。

Windowsインスタンス：認証エラーが発生した

最終更新日：：2023-05-16 10:56:42

問題の説明

リモートデスクトップ接続クライアントを使用してWindowsインスタンスにログインする場合は、次のエラーが発生します。
「認証エラーが発生しました。この関数に提供されたトークンは無効です」。
「認証エラーが発生しました。要求された関数はサポートされていません」。

問題の分析

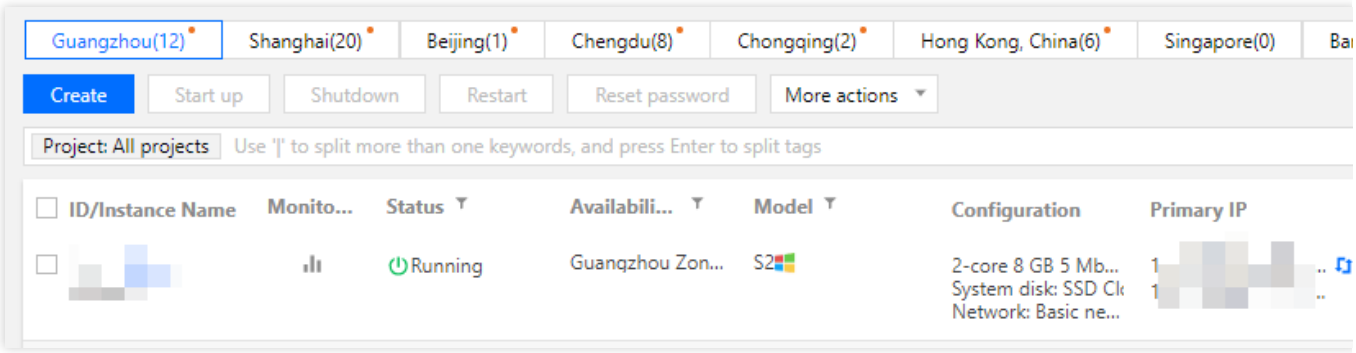
Microsoftは2018年3月にセキュリティ更新プログラムを公開しました。このセキュリティ更新プログラムは、認証プロセス中にCredSSPプロトコルが要求を検証する方法を修正することにより、CredSSPのリモートでコードが実行される脆弱性を解決します。 クライアントとサーバーの両方にセキュリティ更新プログラムをインストールする必要があります。そうしないと、そうしなければ「問題の説明」のような状況が発生する可能性があります。
インスタンスにリモートでログインできない場合、主に次の3つの原因が考えられます。
原因 1:セキュリティ更新プログラムはサーバーにインストールされていますが、クライアントにはインストールされておらず、「強制的に更新されたクライアント」ポリシーが構成されています。
原因 2：セキュリティ更新プログラムはクライアントにインストールされていますが、サーバーにはインストールされておらず、「強制的に更新されたクライアント」ポリシーが構成されています。
原因 3：セキュリティ更新プログラムはクライアントにインストールされていますが、サーバーにはインストールされておらず、「緩和」ポリシーが構成されています。

対処方法

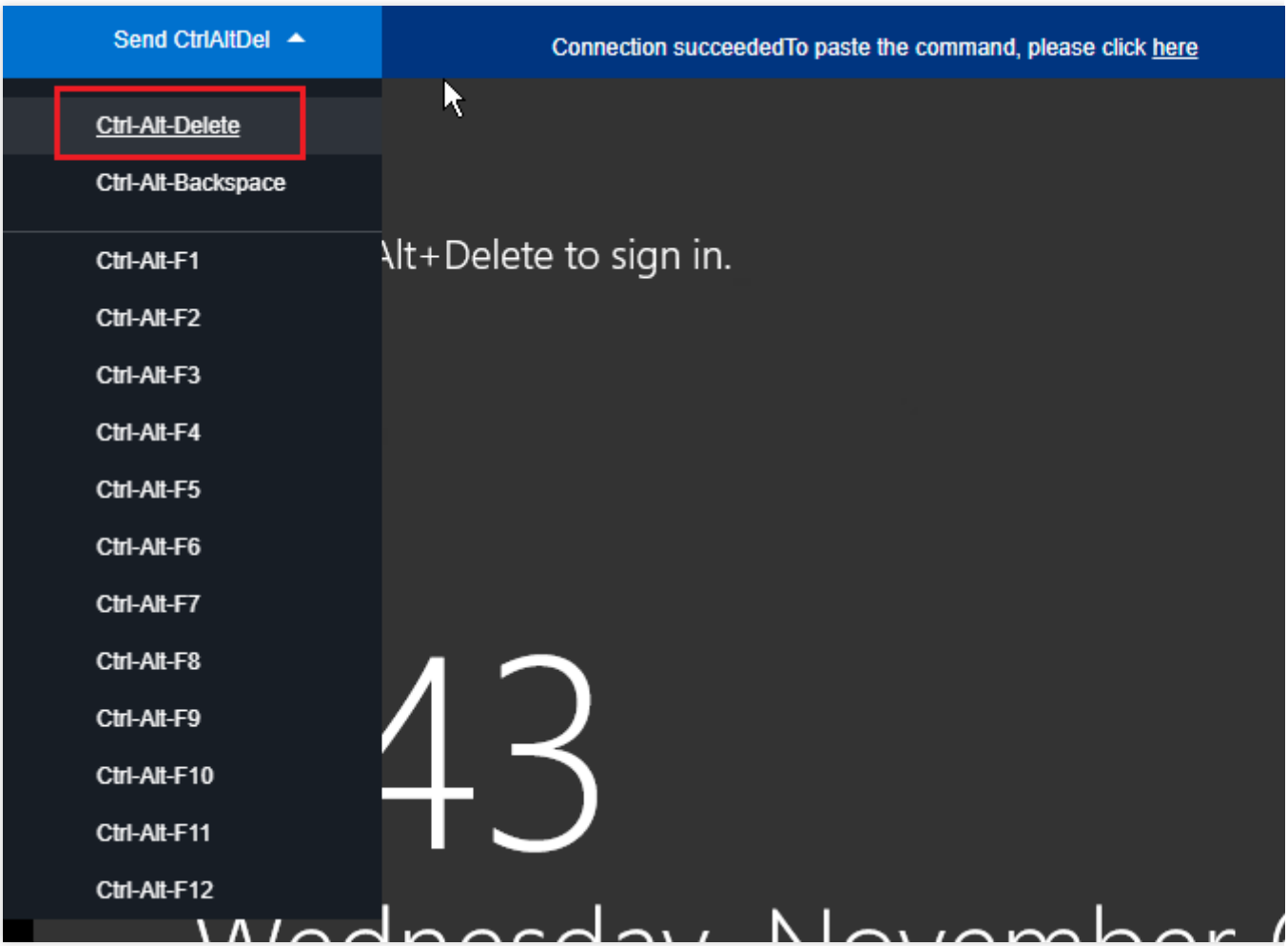
説明：
ローカルクライアントのみをアップグレードする場合は、解決策 1：セキュリティ更新プログラムのインストール（推奨）を直接実行してください。

VNC経由でCVMにログインする

1. CVMコンソール にログインします。
2. 下図のように、インスタンスの管理画面で目的のCVMインスタンスを見つけ、**ログイン**をクリックします。



3. ポップアップした「標準ログイン | Windowsインスタンス」ウィンドウで、**VNCログイン**を選択します。
4. 下図のように、ポップアップしたログインウィンドウの中で、左上の「リモートコマンドの送信」を選択し、**Ctrl-Alt-Delete**をクリックしてシステムログイン画面に進みます。



5. ログインパスワードを入力し、**Enter**を押せば、Windows CVMにログインできます。

解決策 1：セキュリティ更新プログラムのインストール（推奨）

パッチが適用されていないクライアントまたはサーバーにセキュリティ更新プログラムをインストールします。各システムに対応する更新の状況については、CVE-2018-0886 | CredSSPのリモートでコードが実行される脆弱性

をご参照ください。このソリューションではWindows Server 2016を例とします。
その他のOSの場合は、以下の操作を参照して**Windows Update**に進んでください。
Windows Server 2012：

> コントロールパネル > システムとセキュリティ > Windows Update
Windows Server 2008：**スタート > コントロールパネル > システムとセキュリティ > Windows Update**
Windows10：

> 設定 > 更新とセキュリティ
Windows 7：

> コントロールパネル > システムとセキュリティ > Windows Update
1. OSの画面で、

をクリックし、表示されたメニューから**設定**をクリックします。
2. 「設定」が表示されます。**更新とセキュリティ**をクリックします。
3. 「更新とセキュリティ」画面が表示されます。画面の左側から**Windows Update**をクリックし、右側に表示された**更新プログラムのチェック**をクリックします。
4. 画面の表示に従って、**インストールの開始**をクリックします。
5. インストールの完了後にインスタンスを再起動すると、更新が完了します。

解決策 2. ポリシーの設定変更

セキュリティ更新プログラムがインストールされているCVMインスタンスで、**暗号化オラクルの修復**ポリシーを「脆弱」に設定します。このソリューションでは、Windows Server 2016を例とします。操作手順は次のとおりです。

ご注意：

Windows 10 HomeのOSで、グループポリシーエディタがない場合は、レジストリを変更することで実装できます。操作手順については、解決策 3：レジストリの変更 をご参照ください。
1. OS画面で、

をクリックし、**gpedit.msc**と入力し、**Enter**を押して、「ローカルグループポリシーエディタ」を開きます。
説明：
ショートカットキー「**Win+R**」を使用して実行画面を開くこともできます。

2. 左側ナビゲーションツリーで、**コンピューターの構成 > 管理用テンプレート>システム > 資格情報の委任**を選択し、暗号化オラクルの修復をダブルクリックします。
3. 「暗号化オラクルの修復」画面が表示されます。**有効**を選択し、**保護レベル**を**脆弱**に設定します。
4. **OK**をクリックして設定を完了します。

解決策 3：レジストリの変更

1. OS画面で、

をクリックし、**regedit**と入力し、**Enter**を押して、レジストリエディタを開きます。
説明：
ショートカットキー「**Win+R**」を使用して実行画面を開くこともできます。
2. 左側ナビゲーションツリーで、順に**コンピュータ > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Windows > CurrentVersion > Policies > System > CredSSP > Parameters** ディレクトリを開きます。
説明：
ディレクトリパスが存在しない場合は、手動で作成してください。
3. **Parameters**を右クリックし、**新規作成 > DWORD(32ビット)値**を選択し、ファイル名を「AllowEncryptionOracle」とします。
4. 新規作成した「AllowEncryptionOracle」ファイルをダブルクリックし、「数値データ」を「2」に設定し、**OK**をクリックします。
5. インスタンスを再起動します。

関連ドキュメント

CVE-2018-0886 | CredSSPのリモートでコードが実行される脆弱性
CVE-2018-0886のCredSSPの更新プログラム

CVMパスワードリセット失敗、またはパスワードが無効

最終更新日：：2023-06-12 17:07:05

このドキュメントでは、Windows Server 2012のOSを例として、Windows CVMインスタンスのパスワードリセットが失敗または有効にならなかった場合のトラブルシューティング方法および対処方法を説明します。

現象の説明

CVMのパスワードをリセットした後、「システムがビジー状態のため、インスタンスはインスタンスパスワードのリセットに失敗しました(7617d94c)」と表示されます。
CVMのパスワードをリセットした後、新しいパスワードは有効にならず、ログインパスワードは古いパスワードのままです。

考えられる原因

CVMパスワードリセットが失敗または有効にならなかったことについて考えられる理由は次のとおりです。
CVMの `cloudbase-init` コンポーネントが破損している、変更されている、禁止されている、または起動していないことによります。
CVMに360 Safeguardまたは火絨などのサードパーティ製セキュリティソフトウェアをインストールしており、サードパーティ製セキュリティソフトウェアがパスワードリセットコンポーネント `cloudbase-init` をブロックしたことにより、インスタンスのパスワードリセットが無効になった可能性があります。

障害の特定および処理

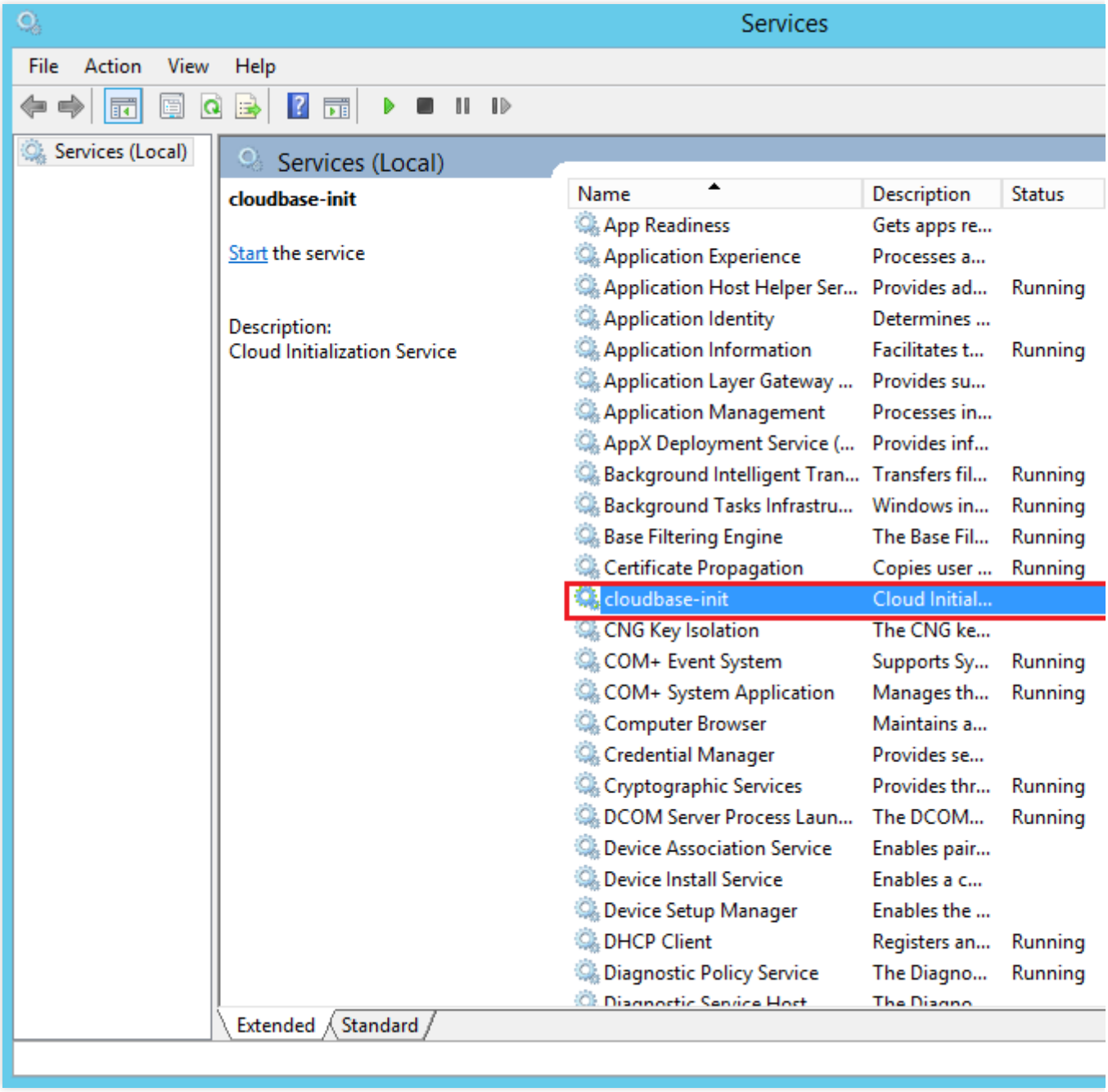
パスワードリセットの失敗の考えられる原因に従って、次の2つの確認方法が提供されています。

cloudbase-initサービスの確認

1. 標準方式を使用してWindowsインスタンスにログイン（推奨）を参照し、目的のWindowsインスタンスにログインします。
2. OS画面で、

を右クリックして**実行**を選択し、**実行**画面で**services.msc**と入力し、**Enter**を押して「サービス」ウィンドウを開きます。

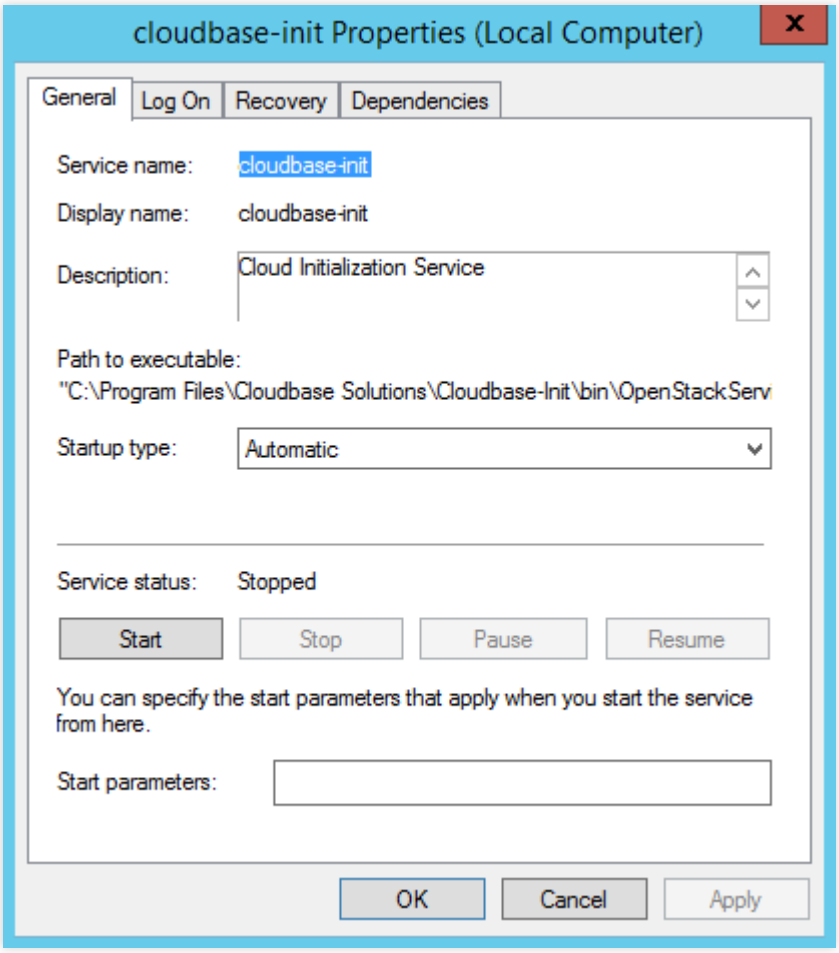
3. `cloudbase-init` サービスが存在するかどうかを確認します。次の図に示します。



「はい」の場合は、次の手順に進んでください。

「いいえ」の場合は、 `cloudbase-init` サービスを再インストールしてください。具体的な操作については Windows OSのCloudbase-Initインストール をご参照ください。

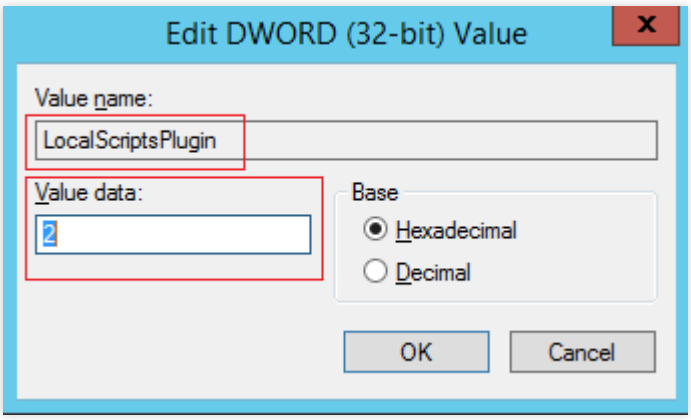
4. ダブルクリックして `cloudbase-init` のプロパティを開きます。次の図に示します。



5. **通常**タブで、 `cloudbase-init` の起動タイプが**自動**に設定されているかどうかを確認します。
「はい」の場合は、次の手順に進んでください。
「いいえ」の場合は、 `cloudbase-init` の起動タイプを**自動**に設定してください。
6. **ログイン**タブに切り替え、 `cloudbase-init` のログインIDで**ローカルシステムアカウント**が選択されているかどうかを確認します。
「はい」の場合は、次の手順に進んでください。
「いいえ」の場合は、 `cloudbase-init` のログインIDを**ローカルシステムアカウント**に設定してください。
7. **通常**タブに切り替え、サービスステータスの**起動**をクリックし、 `cloudbase-init` を手動で起動し、エラーが表示されるかどうかを観察します。
「はい」の場合は、CVMにインストールされているセキュリティソフトウェアを確認する を行ってください。
「いいえ」の場合は、次の手順に進んでください。
8. OS画面で、

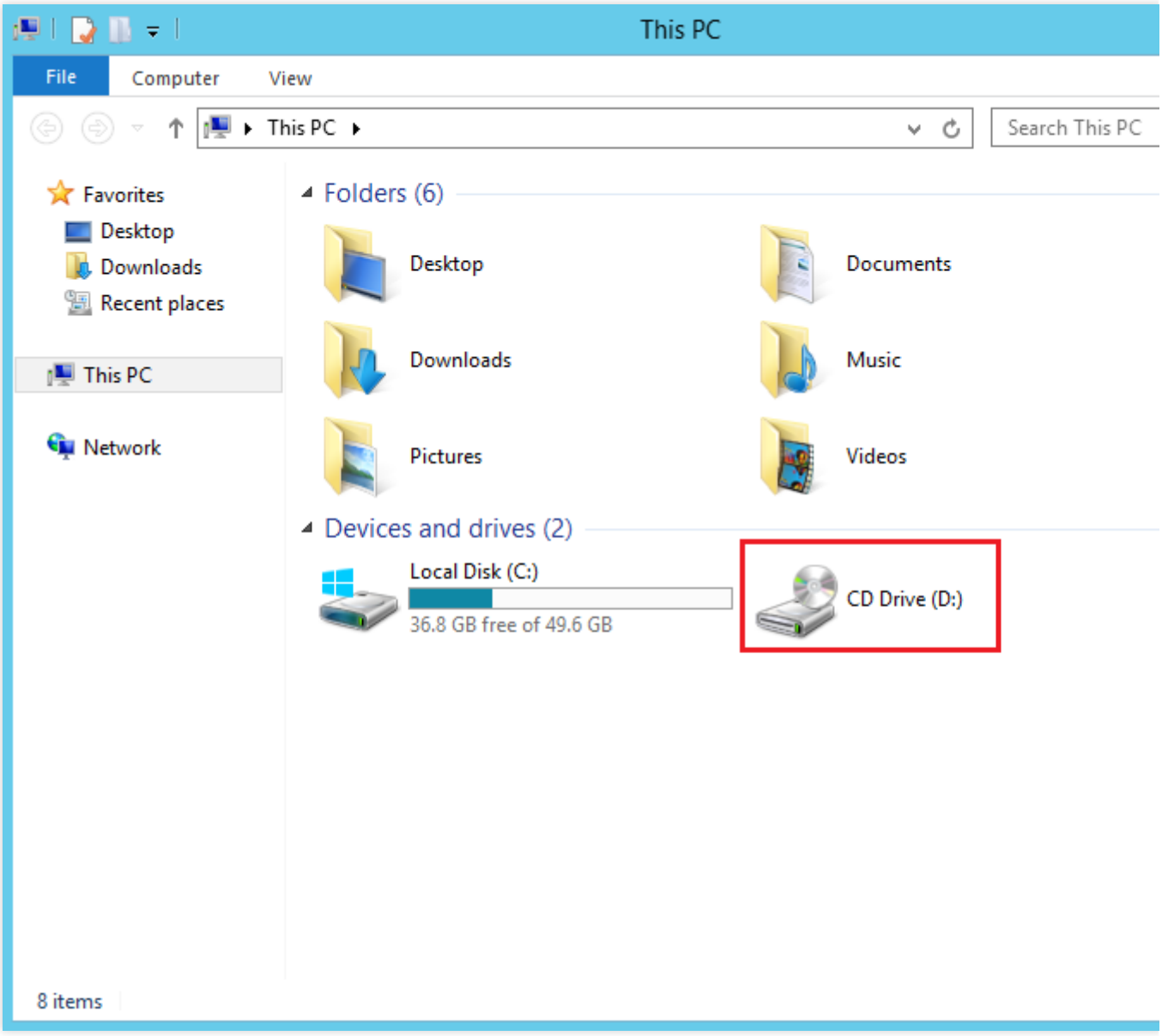
を右クリックして**実行**を選択し、**実行**画面で**regedit**と入力し、**Enter**を押して「レジストリエディタ」ウィンドウを開きます。

9. 左側のレジストリナビゲーションに、順に**HKEY_LOCAL_MACHINE>SOFTWARE>Cloudbase Solutions>Cloudbase-Init**ディレクトリが表示されます。
10. **ins-xxx**下のすべての「LocalScriptsPlugin」レジストリを探し、LocalScriptsPluginの数値データが2かどうかを確認します。



「はい」の場合は、次の手順に進んでください。
「いいえ」の場合は、LocalScriptsPluginの数値データを2に設定してください。
11. OS画面で、

をクリックし、**このコンピュータ**を選択し、デバイスとドライバーの中にCD-ドライバーがロードされているかどうかを確認します。次の図に示します。



そうである場合、CVMにインストールされているセキュリティソフトウェアを確認する。
そうでない場合、デバイスマネージャでCD-ROMドライブを起動します。

CVMにインストールされているセキュリティソフトウェアを確認する

インストールされているセキュリティソフトウェアでフルスキャンを選択し、CVMに脆弱性がないか、および `cloudbase-init` のコアコンポーネントがブロックされていないかを確認します。
CVMの脆弱性が検出された場合は、修復してください。
コアコンポーネントのブロックが検出された場合は、ブロックを取り消してください。
`cloudbase-init` コンポーネントの確認および設定の手順は次のとおりです。
1. 標準方式を使用してWindowsインスタンスにログイン（推奨）を参照し、目的のWindowsインスタンスにログインします。

2. 実際にインストールされているサードパーティ製セキュリティソフトウェアに応じて、`cloudbase-init` コンポーネントをリカバリし、設定します。

Windows インスタンス：リモートデスクトップサービスを使ったログオンを拒否

最終更新日：：2022-05-26 16:09:18

故障について

故障1
：Windowsがリモートデスクトップを使用してWindowsインスタンスに接続する際に、「このユーザーアカウントはリモートログインを許可されていないため、接続は拒否されました。」 というメッセージが出て来ます。

故障2
：Windowsがリモートデスクトップを使用してWindowsインスタンスに接続する際に、「リモートログインするには、リモートデスクトップサービスを使用したログインを許可する権限が付与されている必要があります。デフォルトでは、リモートデスクトップのユーザグループのメンバーのみこの権限があります。所属するグループにこの権限がない、あるいはリモートデスクトップのユーザグループから権限が削除されている場合は、手動でこの権限を付与する必要があります。」というメッセージが出て来ます。

考えられる原因

このアカウントはリモートデスクトップ接続を介してWindowsインスタンスにログインすることが許可されていません。

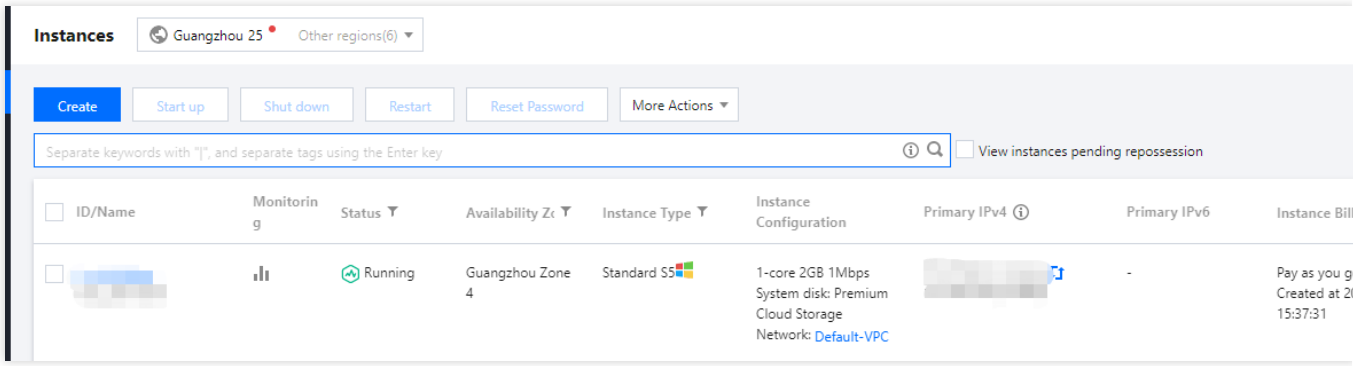
ソリューション

リモートデスクトップからWindowsインスタンスに接続するときに、故障1 が発生した場合は、リモートデスクトップサービス接続を介したログインを許可するには、Windowsインスタンスで設定されているリストにユーザーアカウントを追加する必要があります。詳細については、リモートログインを許可する権限の設定 をご参照ください。
リモートデスクトップからWindowsインスタンスに接続するときに、故障2 が発生した場合は、リモートデスクトップサービスを介したログインするために、Windowsインスタンスによって拒否されたアカウントのリストからユーザーアカウントを削除する必要があります。詳細については、リモートログインを拒否する権限の変更 をご参照ください。

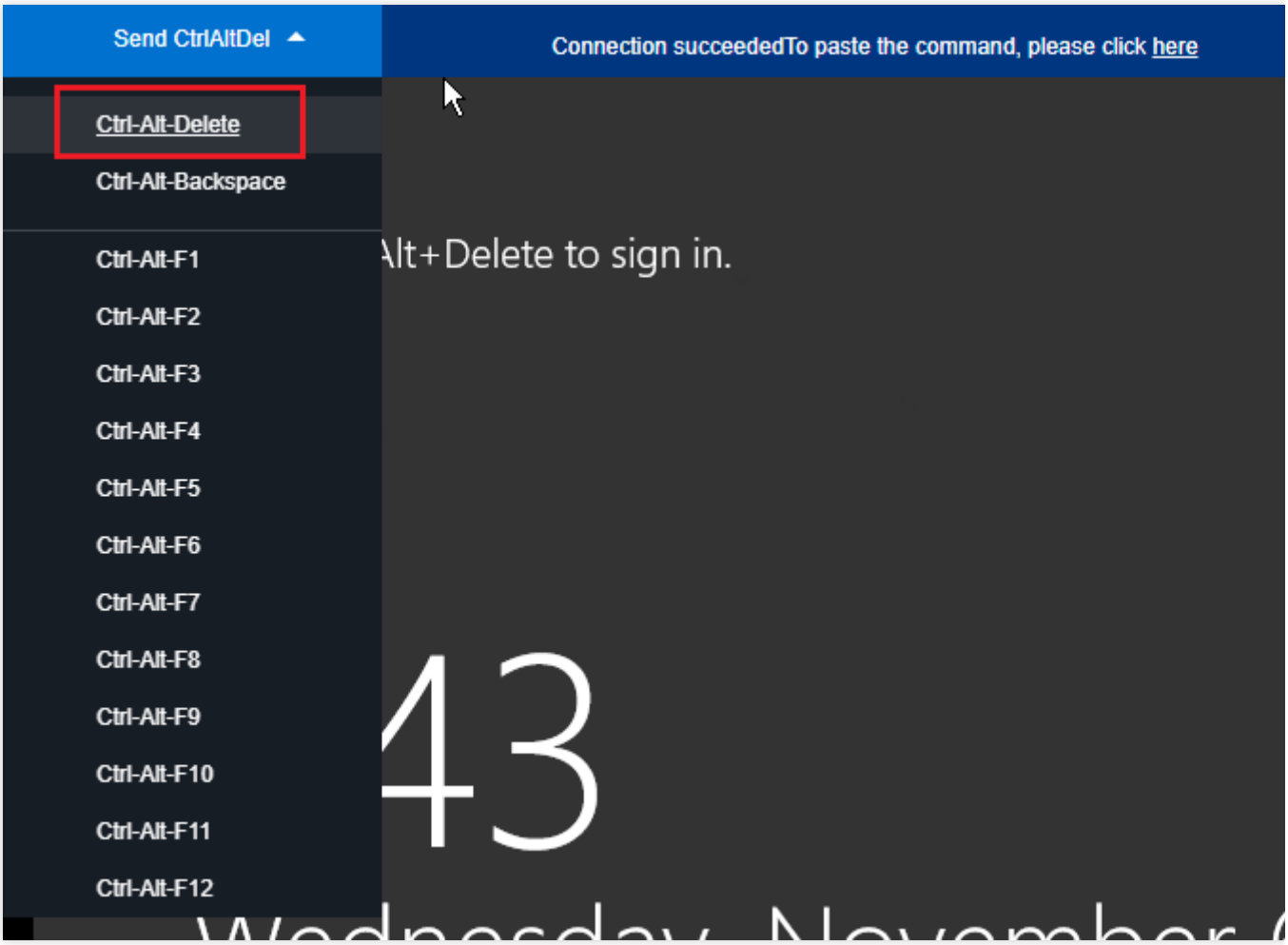
処理手順

VNCを利用してCVMにログインする

1. CVMコンソール にログインします。
2. インスタンスの管理ページで、下図に示すように、対象のCVMインスタンスを見つけて、**ログイン**をクリックします。



3. ポップアップウインドウ「Windowsインスタンスにログインする」に、**その他の方式(VNC）**を選択し、**今すぐログイン**をクリックして、CVMにログインします。
4. ポップアップしたログイン画面で、左上隅の「リモートコマンドの送信」を選択し、**Ctrl-Alt-Delete**をクリックすると、システムログインインターフェースに入ります。



リモートログインを許可する権限の設定

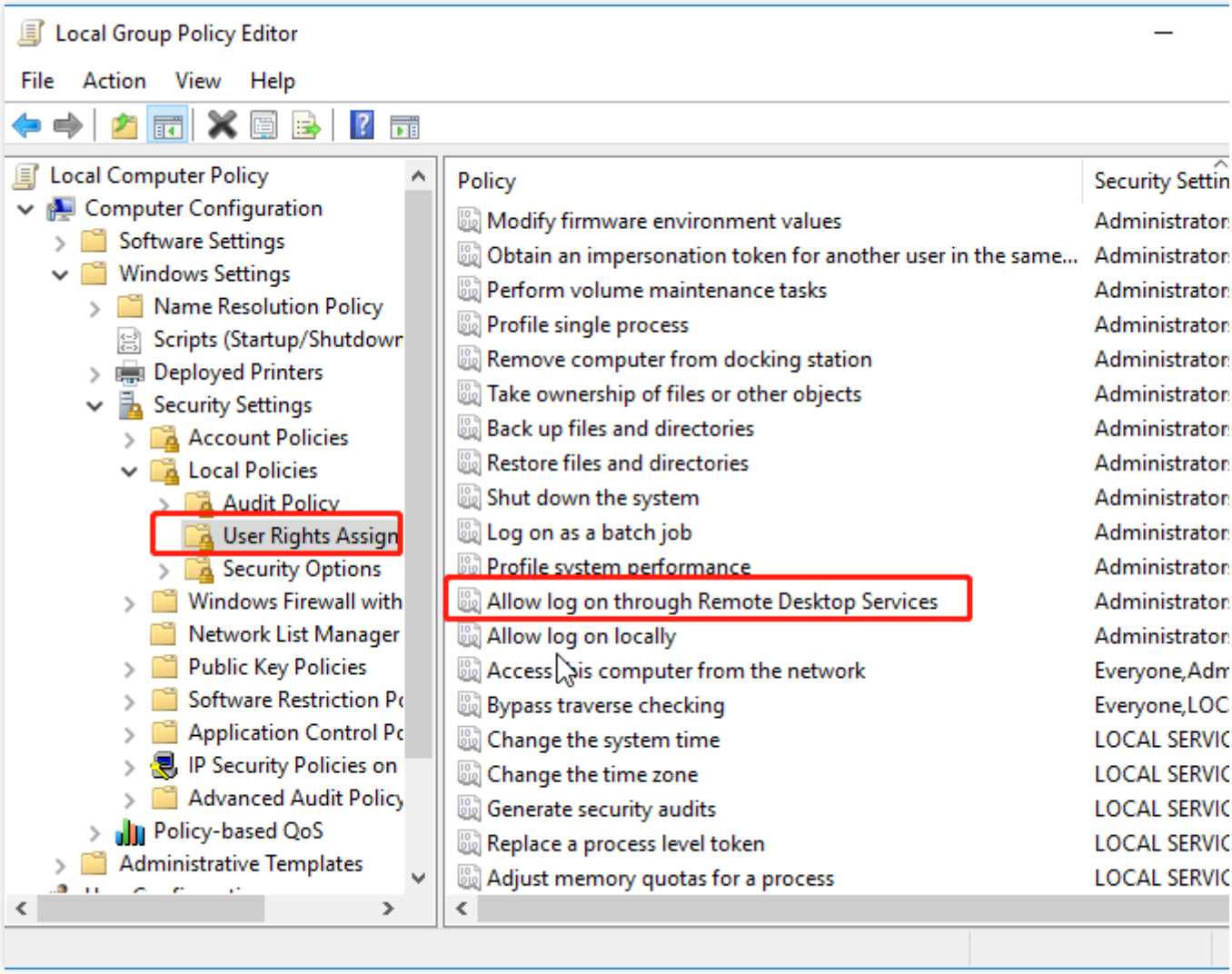
説明：

以下の操作は Windows Server 2016 を例として説明します。

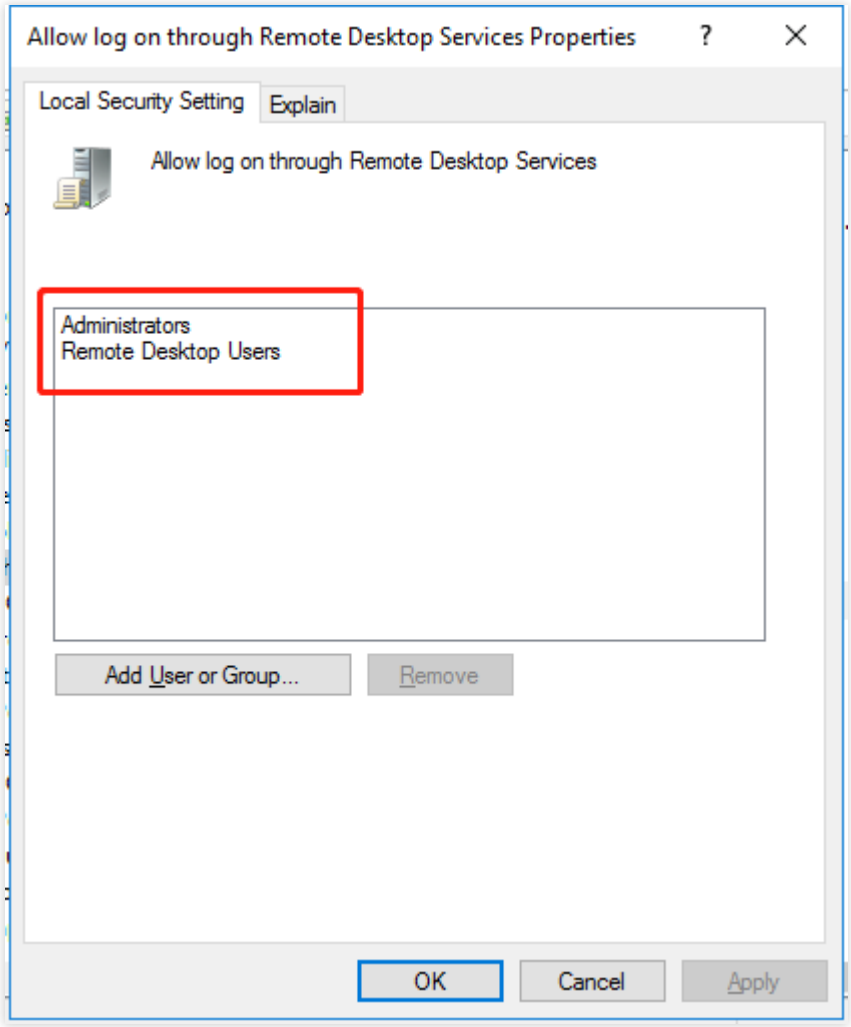
1. OSインターフェースで、

をクリックして、**gpedit.msc**を入力し、**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。

2. 左側のナビゲーションツリーで、**コンピューターの構成** > **Windowsの設定** > **セキュリティの設定** > **ローカルポリシー** > **ユーザー権利の割り当て**の順で選択し、**リモートデスクトップサービスを使ったログオンを許可する**をダブルクリックして開きます。



3. 開いた「リモートデスクトップサービスを使ったログオンを許可のプロパティ」のウィンドウで、リモートログインに使用するユーザーアカウントが、[リモートデスクトップサービスを介したログオンを許可する]のユーザーリストにあるかどうかを確認します。



このアカウントがリストにない場合は、手順4 に進んでください。
このアカウントがリストにある場合は、チケットを送信 してフィードバックしてください。
4.
ユーザーまたはグループの追加をクリックして、「ユーザーまたはグループの選択」のウィンドウを開きます。

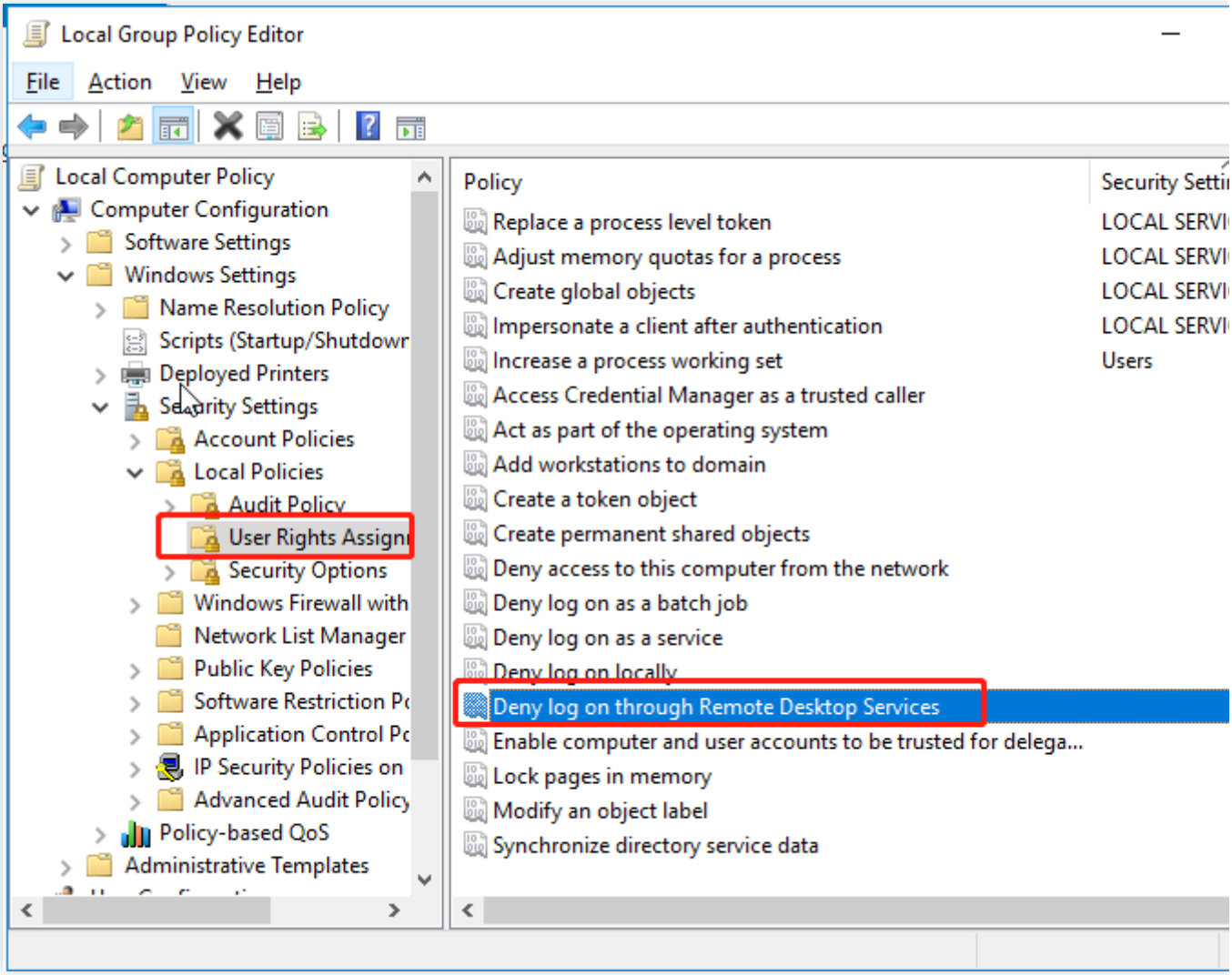
5. リモートログインに使用するアカウントを入力し、**OK**をクリックします。
6. **OK**をクリックして、ローカルグループポリシーエディターを閉じます。
7. インスタンスを再起動し、このアカウントを使用してWindowsインスタンスへのリモートデスクトップ接続を再度試してください。

リモートログインを拒否する権限の変更

説明：
以下の操作は Windows Server 2016 を例として説明します。
1. OSインターフェースで、

をクリックして、**gpedit.msc**を入力し、**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。

2. 左側のナビゲーションツリーで、**コンピューターの構成 > Windowsの設定 > セキュリティの設定 > ローカルポリシー > ユーザー権利の割り当て**の順で選択し、**リモートデスクトップサービスを使ったログオンを拒否**をダブルクリックして開きます。



3. 開いた「リモートデスクトップサービスを使ったログオンを拒否のプロパティ」ウィンドウで、リモートログインに使用するユーザーアカウントが「リモートデスクトップサービス使ったログオンを拒否」のユーザーリストにあるかどうかを確認します。

ユーザーがリストにある場合は、リストからユーザーアカウントを削除し、インスタンスを再起動します。

ユーザーがリストにない場合は、 チケットを送信 してフィードバックしてください。

Windowsインスタンス：ネットワークレベルの認証が必要

最終更新日：：2023-05-16 11:12:07

このドキュメントでは、リモートデスクトップを使用してWindowsインスタンスに接続する時に、「リモートコンピュータには、お使いのコンピュータでサポートされていないネットワークレベルの認証が必要です。サポートが必要な場合は、システム管理者かテクニカルサポートに問い合わせてください。」のエラーが表示されて接続できなかった時の対処法について詳しく紹介します。

故障

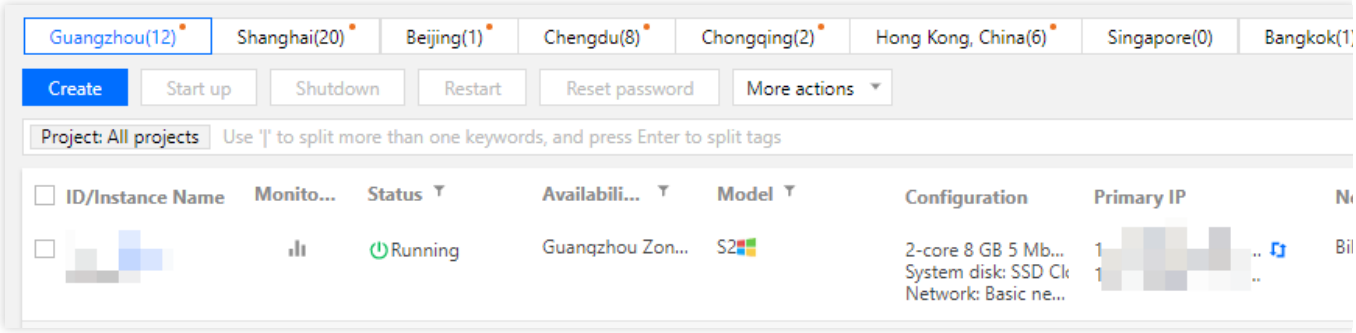
「リモートコンピュータには、お使いのコンピュータでサポートされていないネットワークレベルの認証が必要です。サポートが必要な場合は、システム管理者かテクニカルサポートに問い合わせてください。」とエラーメッセージが表示されリモートデスクトップ接続ができない。

トラブルシューティング

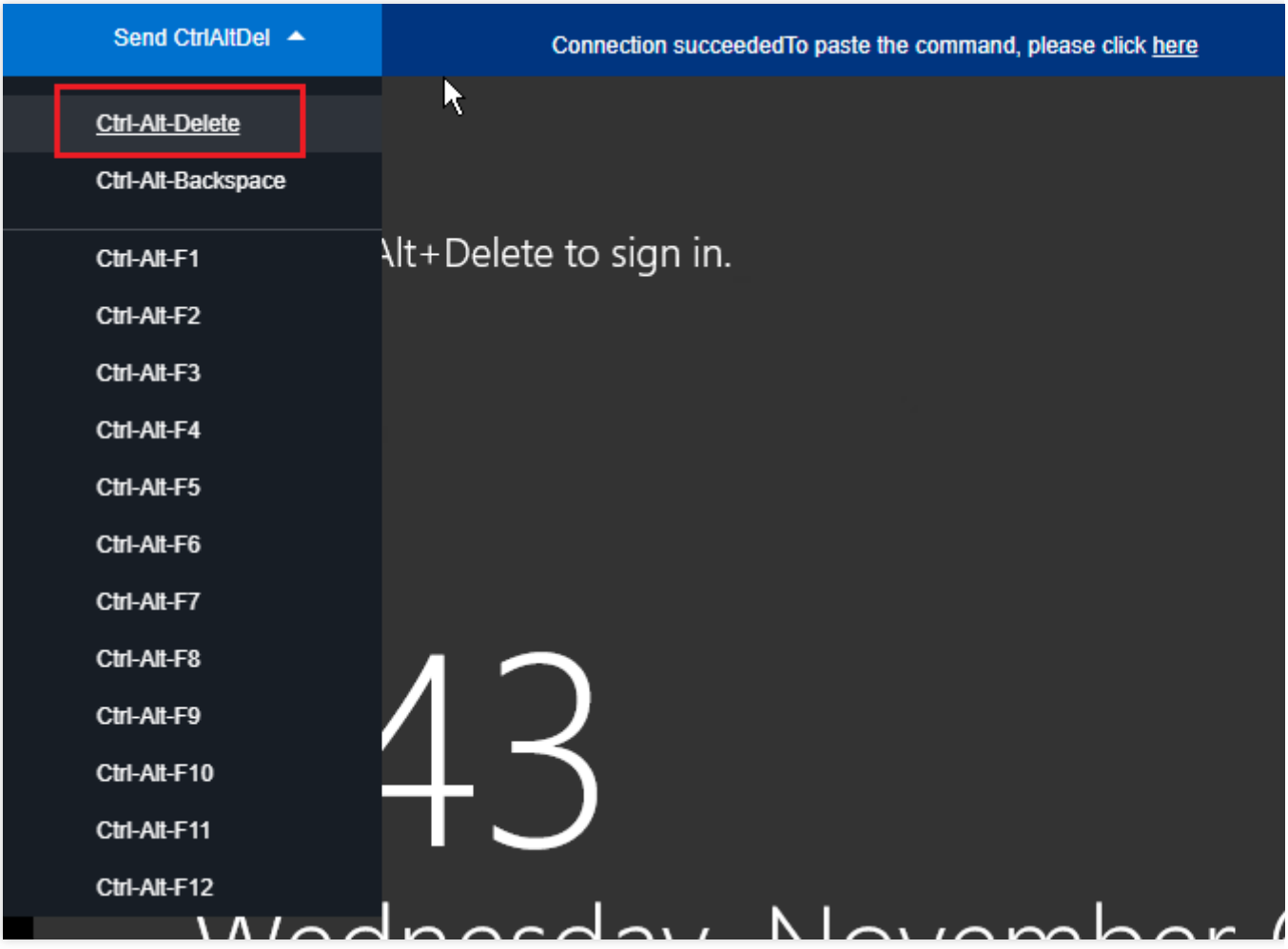
説明：
以下の操作は Windows Server 2016 を例として説明します。

VNC経由でCVMにログインする

1. CVMコンソール にログインします。
2. インスタンスの管理ページで、対象のCVMインスタンスを見つけて、**ログイン**をクリックします。下図に示すように：



3. ポップアップされた「Windowsインスタンスにログインする」ウィンドウで、**その他の方式(VNC）**を選択し、**今すぐログイン**をクリックして、CVMにログインします。
4. 表示されるログインウィンドウで、左上隅にある「リモートコマンドの送信」を選択し、Ctrl-Alt-Deleteをクリックして、システムログインインターフェースに入ります。次の図に示すように：

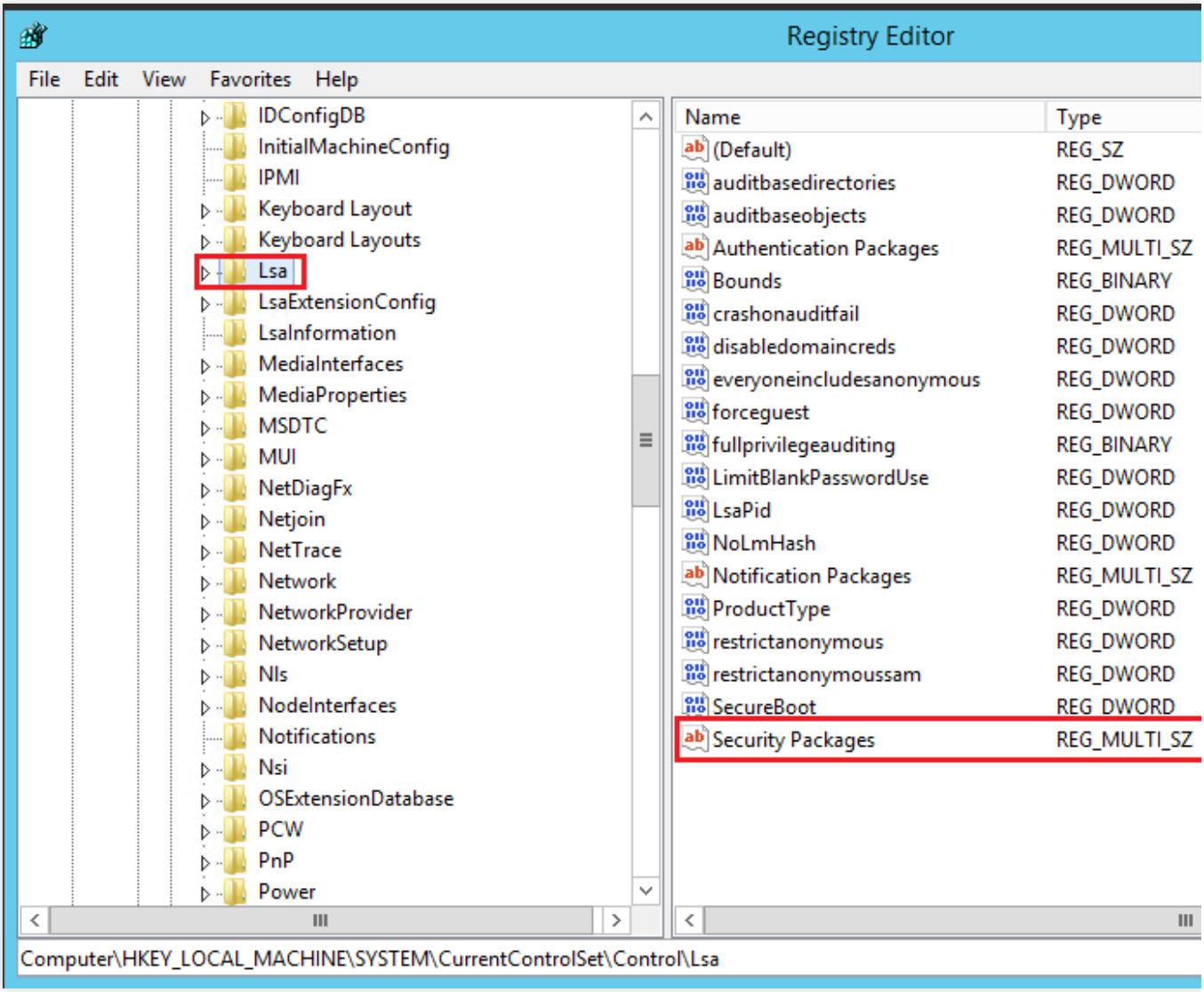


レジストリを変更する

1. OSインターフェースで、

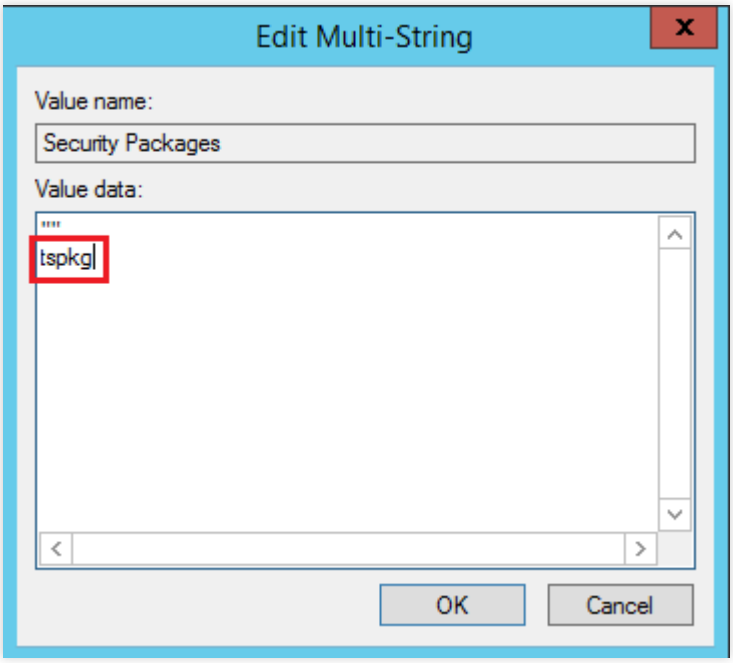
をクリックして、 **regedit**と入力し、**Enter**キーを押してレジストリエディターを開きます。

2. 左側のナビゲーションツリーで、**コンピューター** > **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Control** > **Lsa**ディレクトリを開き、右側のウィンドウで**Security Packages**を見つけます。以下に示すように：

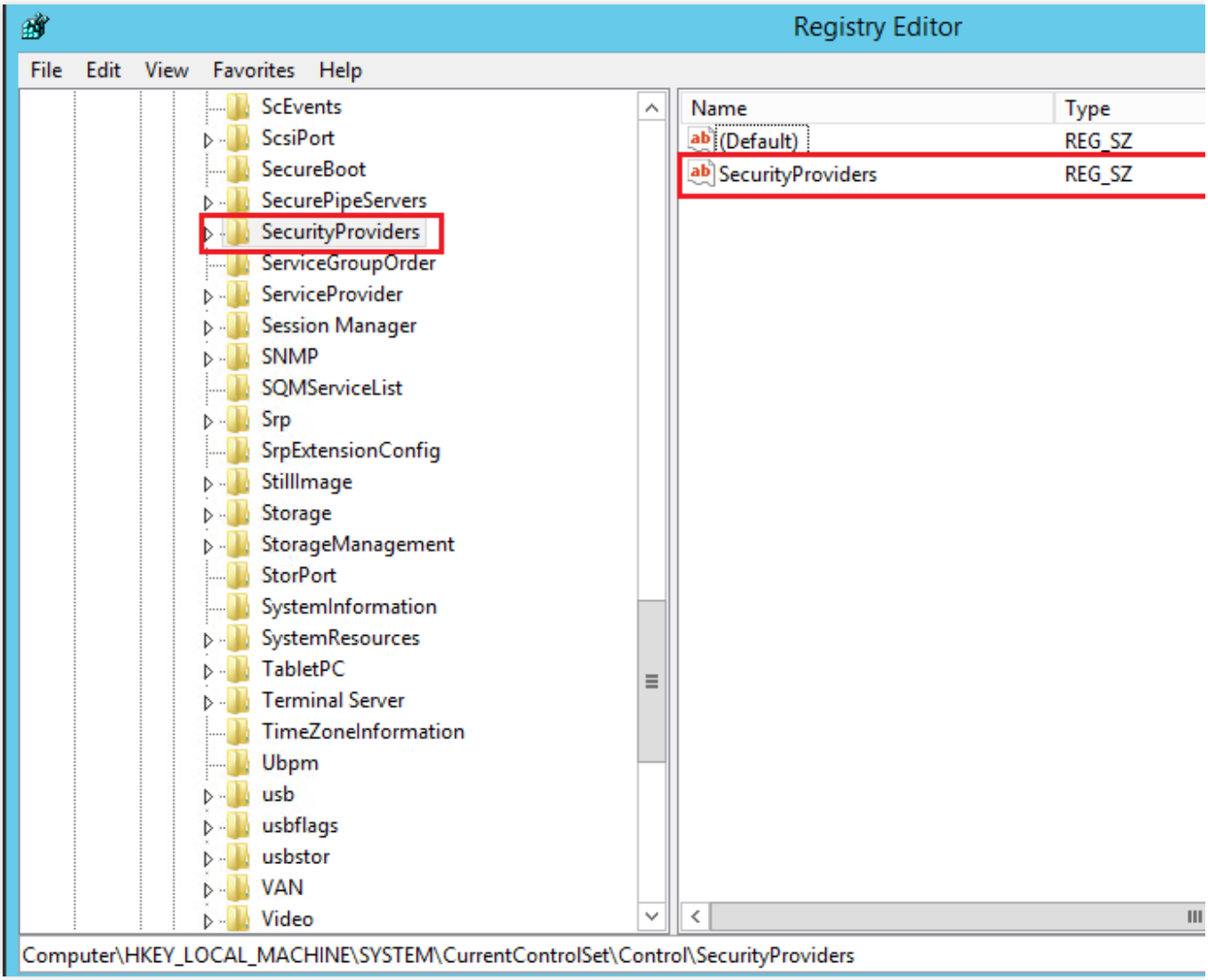


3. **Security Packages**をダブルクリックして、**複数行文字列の編集**ダイアログボックスを開きます。

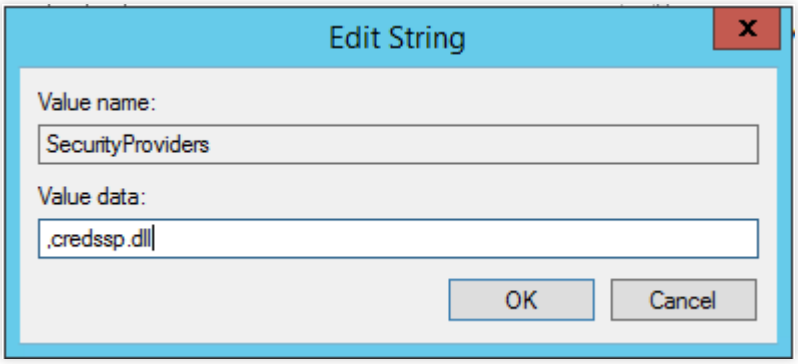
4. 「複数行文字列の編集」ダイアログボックスで、**tspkg**文字を追加し、**OK**をクリックします。以下に示すように：



5. 左側のナビゲーションツリーで、**コンピューター** > **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Control** > **SecurityProviders**ディレクトリを展開し、右側のウィンドウで**SecurityProviders**を見つけます。次の図に示すように：



6. **SecurityProviders**をダブルクリックして、複数行文字列の編集ダイアログボックスを開きます。
7. 「複数行文字列の編集」ダイアログボックスの**値のデータ**の最後に `, credssp.dll` を追加し、**OK**をクリックします。次の図に示すように：



8. レジストリエディターを閉じて、インスタンスを再起動してリモートログインできます。

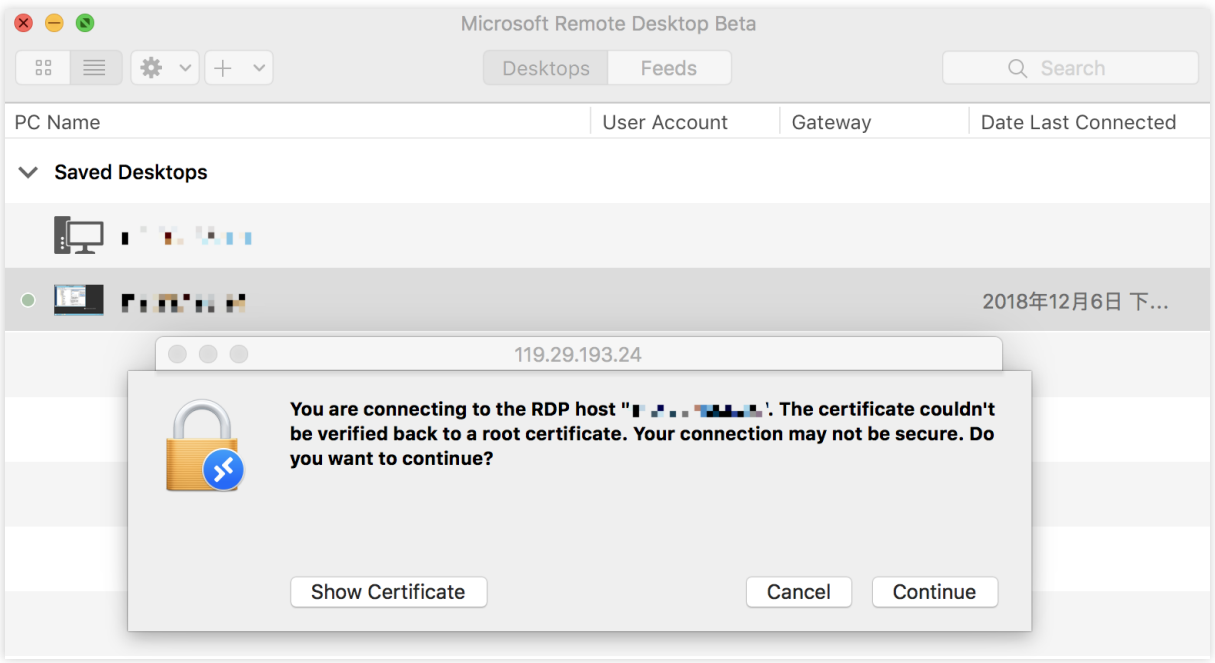
Windowsインスタンス：Macリモートログイン異常

最終更新日：：2022-05-26 16:56:10

このドキュメントでは、Mac が Microsoft Remote Desktop経由でWindows CVMにログインする時に発生する可能性のある一般的な故障現象及び対処方法について説明します。

故障について

Mac が Microsoft Remote Desktop 経由でWindows CVMにログインする時に、「The certificate couldn't be verified back to a root certificate.」というプロンプトが表示されます。



Mac でリモートデスクトップ接続（Remote Desktop Connection）を使用すると、「接続先のコンピューターのIDを確認できません」というプロンプトが表示されます。

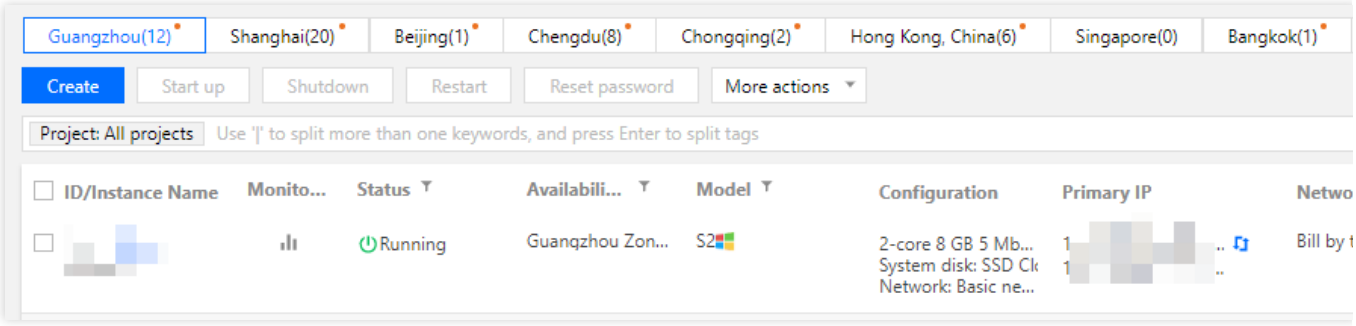
トラブルシューティング

説明：

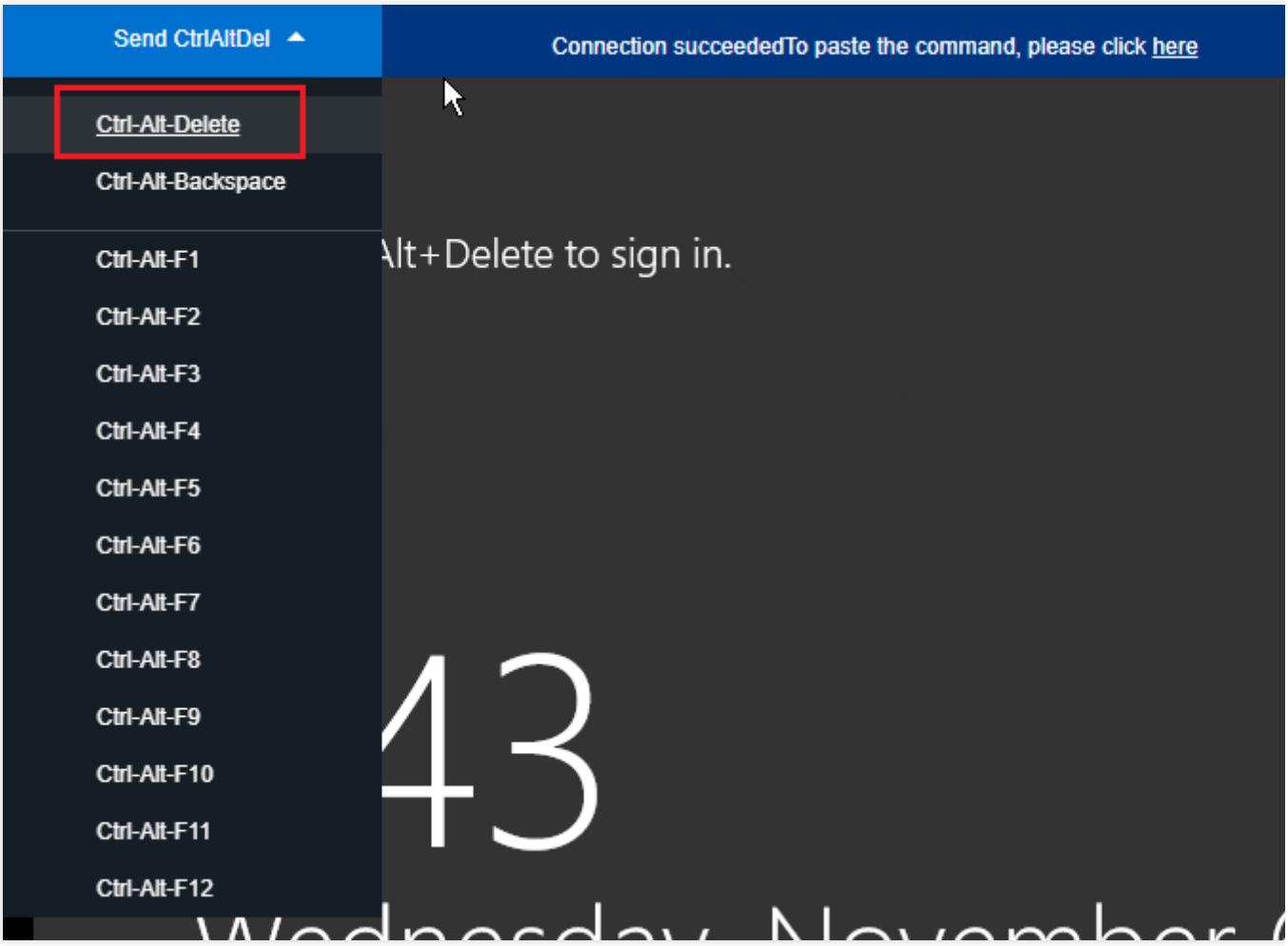
下記操作は Windows Server 2016 を例として説明します。

VNC を使用してCVMにログインする

1. CVMコンソール にログインします。
2. インスタンス管理ページで、対象CVMインスタンスを見つけて、**ログイン**をクリックします。次の図に示すように：



3. ポップアップした「Windowsインスタンスにログインする」ウィンドウで、**その他の方式(VNC）**を選択し、**今すぐログイン**をクリックして、CVMにログインします。
4. ポップアップウィンドウで、左上隅にある「リモートコマンドの送信」を選択し、**Ctrl-Alt-Delete** をクリックして、システムログインインターフェースに入ります。次の図に示すように：



インスタンスのローカルグループポリシーの変更

1. OSインターフェースで、

をクリックして、 **gpedit.msc**を入力し、**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。

説明：

「Win+R」ショートカットを使用して実行インターフェースを開くこともできます。

2. 左側のナビゲーションツリーで、**コンピューターの構成 > 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 > セキュリティ**を選択し、**リモート (RDP) 接続に特定のセキュリティ レイヤーの使用を必要とする**をダブルクリックします。

3. 開いた 「リモート (RDP) 接続に特定のセキュリティ レイヤーの使用を必要とする」ウインドウで、**有効**を選択し、かつ**セキュリティレイヤー**を**RDP**に設定します。

4. **OK**をクリックし、設定を完了します。

5. インスタンスを再起動して、接続が成功したかどうかを再試行します。接続が失敗した場合に、 チケットを送信 してフィードバックしてください。

Windowsインスタンス：CPUまたはメモリの使用率が高いためログインできない

最終更新日：：2021-08-12 16:33:59

このドキュメントでは、CPUまたはメモリの使用率が高いため、Windows CVMにログインできない問題のトラブルシューティングと対処方法について説明します。

説明：

以下の操作手順はWindows server 2012 R2を例に説明します。OSのバージョンによって操作手順の詳細が若干異なります。

考えられる原因

CPUまたはメモリの使用率が高すぎると、サービスのレスポンスが遅くなるや、CVMにログインできないなどの問題が発生します。ハードウェア、システムプロセス、サービスプロセス、トロイの木馬などに起因する可能性があります。クラウドモニター を利用して、CPUまたはメモリ使用率のアラームしきい値を作成し、しきい値を超えると、リアルタイムにユーザーに通知することができます。

トラブルシューティング

1. CPUまたはメモリの使用率が高くなるプロセスを特定します。
2. CPUまたはメモリの使用率が高くなるプロセスを分析します。

異常なプロセスである場合は、ウイルスまたはトロイの木馬が原因である可能性があります。この場合、プロセスを終了するか、セキュリティソフトを使用してシステムをスキャンします。

サービスプロセスの場合は、アクセスボリュームの変更が原因でCPUまたはメモリの使用率が高くなっていること、および最適化できるかどうかを確認します。

Tencent Cloudコンポーネントプロセスの場合、チケットを送信 してください。

ツール

タスクマネージャー：これは、Microsoft Windows OSでアプリケーションとプロセスを管理するためのツールです。実行中のプロセスの名前、CPU負荷、メモリ使用量、I/Oの詳細、ログインしているユーザー、Windowsサービスなど、コンピューターのパフォーマンスと実行中のソフトウェアに関する情報を提供します。

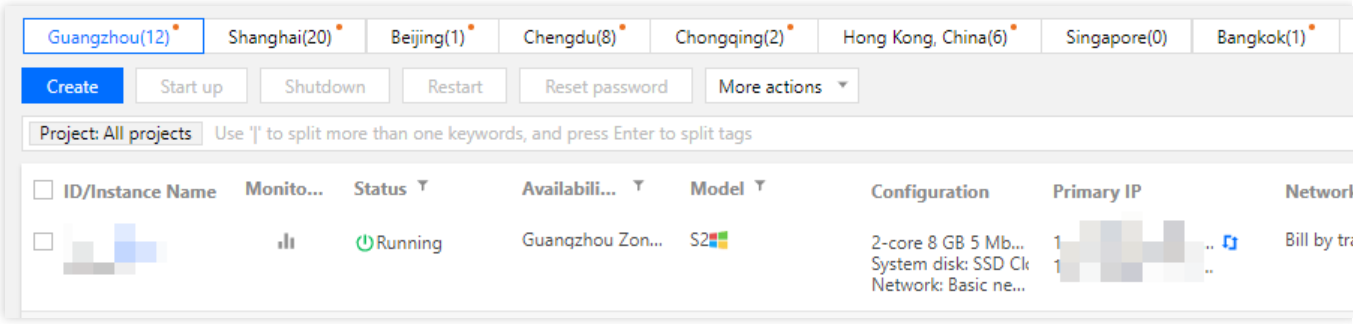
プロセス：システムで実行中のプロセスの一覧です。

パフォーマンス：システムのパフォーマンスに関する全体の統計です。例とえば、全体的なCPU使用量とメモリ使用率。
ユーザー：システムでセッションを持つすべてのユーザーです。
詳細：PID、ステータス、CPU使用率、メモリ使用量などの情報を含む、実行中のプロセスの詳細情報を提供します。
サービス：システムのすべてのサービス（実行されていないービスも含む）です。

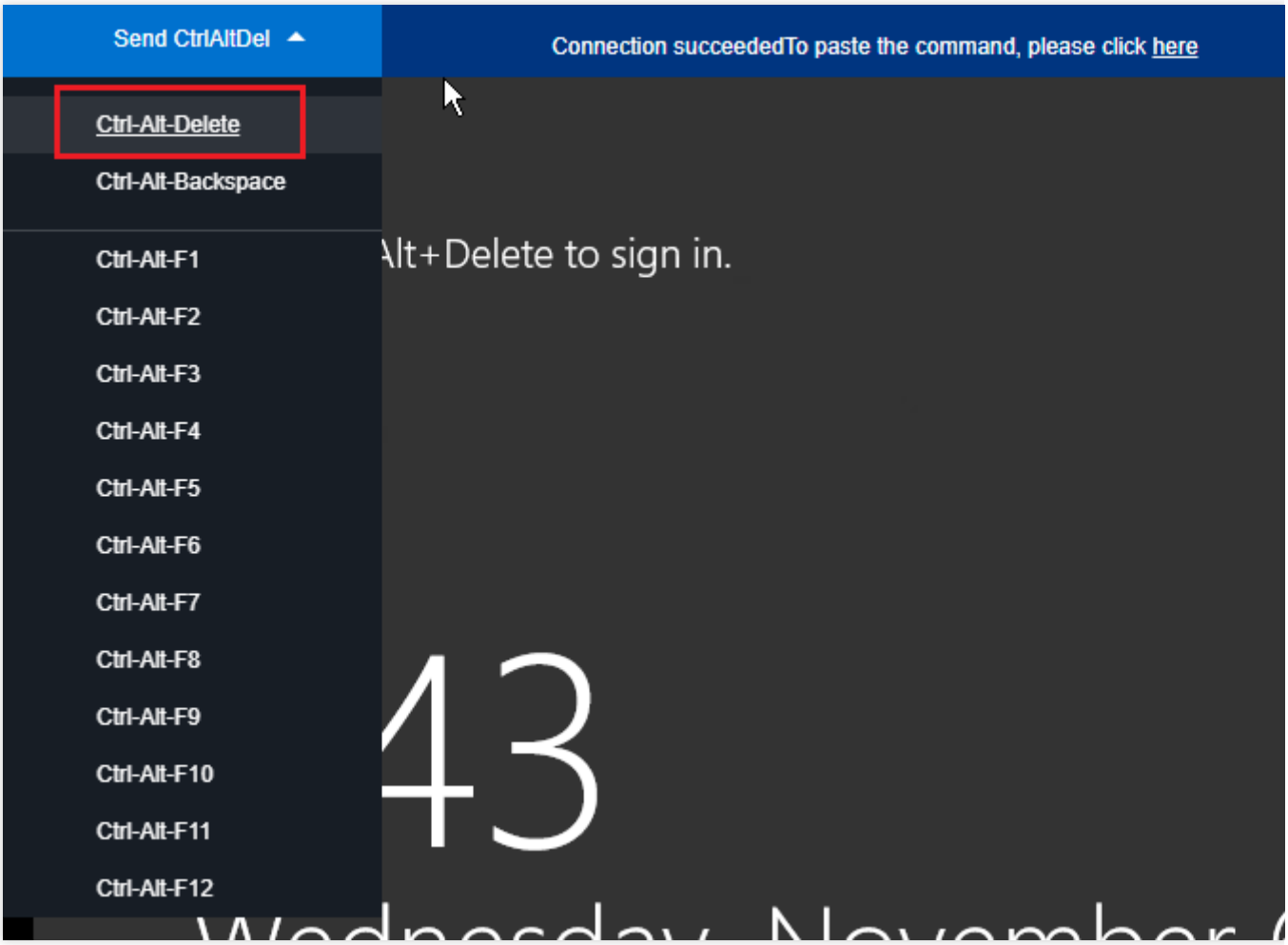
ソリューション

VNCを使用してCVMインスタンスにログインする

説明：
CPUまたはメモリの使用率が高いためにCVMインスタンスにログインできない場合は、VNCを使用してWindowsインスタンスにログインする ことをお勧めします。
1. CVMコンソール にログインします。
2. インスタンスの管理ページで、下図に示すように、対象のCVMインスタンスを見つけて、**ログイン**をクリックします。

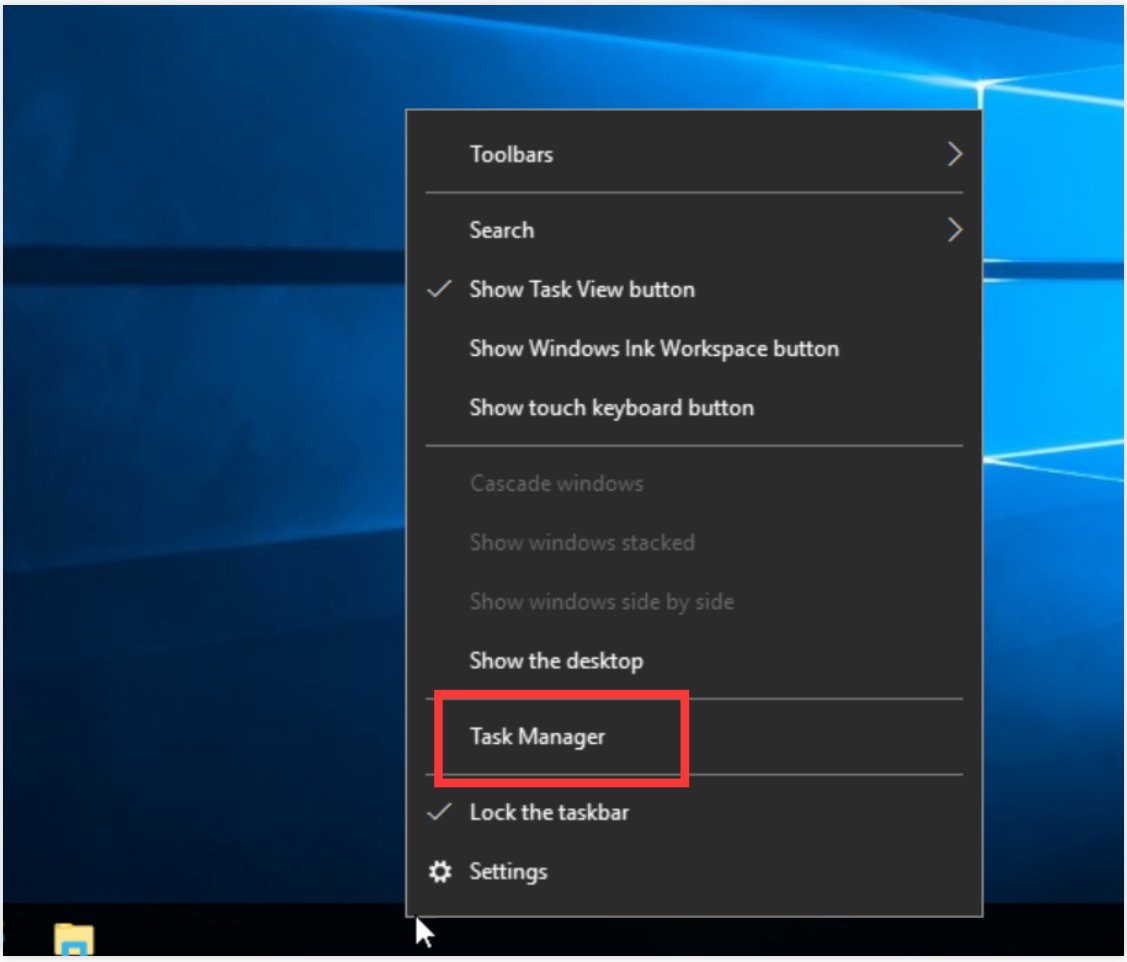


3. ポップアップされた 「Windowsインスタンスにログインする」画面で、**その他の方式(VNC）**を選択し、**すぐにログインする**をクリックして、CVMにログインします。
4. ポップアップされたログインウィンドウで、下図に示すように、左上の「Send CtrlAltDe」を選択し、**Ctrl-Alt-Delete** をクリックすると、システムログイン画面に入ります。



プロセスのリソース使用状況を確認する

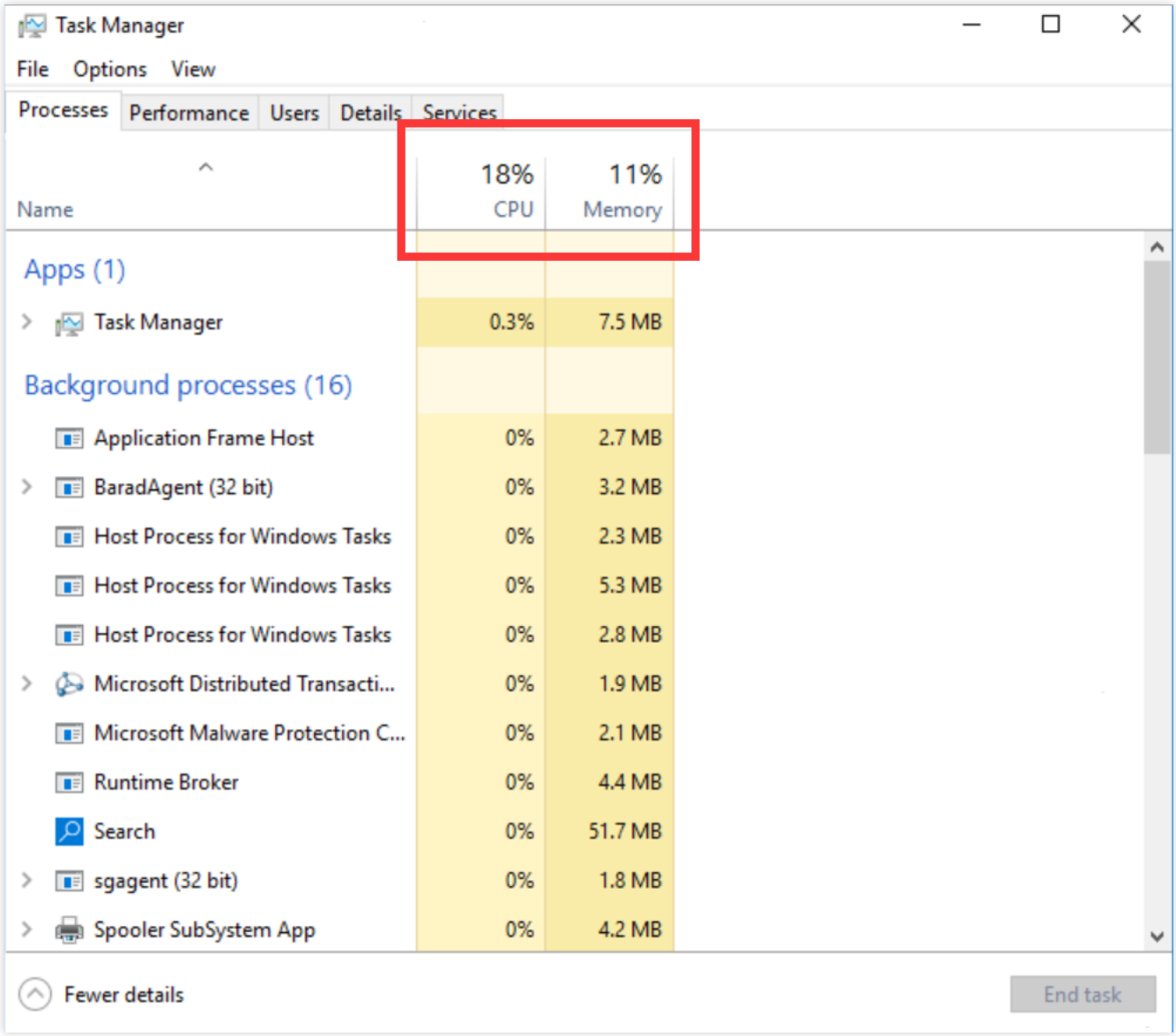
1. CVMで、下図に示すように、「タスクバー」を右クリックして、**タスクマネージャー**を選択します。



2. 開かれた「タスクマネージャー」で、下図に示すように、リソース使用状況を確認できます。

説明：

CPUまたはメモリをクリックして、プロセスを昇順/降順で並べ替えます。



プロセスを分析する

タスクマネージャーでプロセスを分析して原因を特定し、適切な対策を講じます。

CPUやメモリリソースを大量に消費しているプロセスはシステムプロセスの場合

システムプロセスがCPUまたはメモリリソースを大量に消費していることが判明した場合は、以下の内容をご確認ください。

1. プロセス名を確認する。

一部の悪意のあるプログラムは、svch0st.exe、explore.exe、iexplorer.exeなどのシステムプロセスに類似した名前を使用することがあります。

2. プロセスの実行可能ファイルのパスを確認します。

ステムプロセスの実行可能ファイルは通常 `C:\\Windows\\System32` ディレクトリにあり、有効な署名と説

明があります。タスクマネージャで表示するプロセスを右クリックし、**ファイルの場所を開く**を選択して、特定の実行可能ファイルの場所（ `svchost.exe` など）を表示できます。
実行可能ファイルが `C:\\Windows\\System32` ディレクトリに配置されていない場合、CVMインスタンスがウイルスに感染している可能性があります。この場合、手動またはセキュリティソフトを使用してウイルスを検出し、駆除してください。
実行可能ファイルが `C:\\Windows\\System32` ディレクトリにある場合は、システムを再起動するか、安全だが不要なシステムプロセスを終了します。
通常のシステムプロセスは次のとおりです。
System Idle Process：システムアイドルプロセス。CPUがアイドル状態である時間の割合を表示します。
system：メモリ管理プロセスを示します。
explorer：デスクトップとファイル管理プロセスを示します。
iexplore：Microsoft Internet Explorerのプロセスを示します。
csrss：Microsoftクライアント/サーバー上のランタイムサブシステムを示します。
svchost：DLLを実行するためのシステムプロセスを示します。
Taskmgr：タスクマネージャーを示します。
lsass：ローカルセキュリティ権限サービスを示します。

CPUまたはメモリリソースを大量に消費しているプロセスは異常なプロセスの場合

xmr64.exe（マイニングウイルス）などの見慣れない名前のプロセスがCPUまたはメモリリソースを大量に消費している場合は、CVMインスタンスがウイルスやトロイの木馬に感染している可能性があります。この場合、検索エンジンを使用して、トロイの木馬ウイルスプロセスかどうかを検索・確認することをお勧めします。
プロセスがウイルスまたはトロイの木馬の場合は、セキュリティソフトを使用してスキャン・駆除して、必要に応じて、データをバックアップし、OSを再インストールしてください。
プロセスがウイルスやトロイの木馬でない場合は、システムを再起動するか、安全だが不要なプロセスを終了してください。

CPUまたはメモリリソースを大量に消費しているプロセスはサービスプロセスの場合

CPU使用率が高いプロセスは、お客様のサービスプロセスである場合、例えば：IIS、HTTPD、PHPとJava など、さらに分析することをお勧めします。
たとえば、現在のサービス負荷が大きいかどうかを判断します。
ビジネス負荷が大きい場合は、サーバー構成をアップグレード することをお勧めします。サーバー構成をアップグレードしない場合は、サービスプログラムを最適化する可能性を検討して、最適化してください。
ビジネス負荷が少ない場合は、サービスエラーログをさらに分析する必要があります。たとえば、不適切なパラメータ設定によりリソースが無駄になっていないかどうかを確認します。

CPUまたはメモリリソースを大量に消費しているプロセスはTencent Cloudコンポーネントプロセスの場合

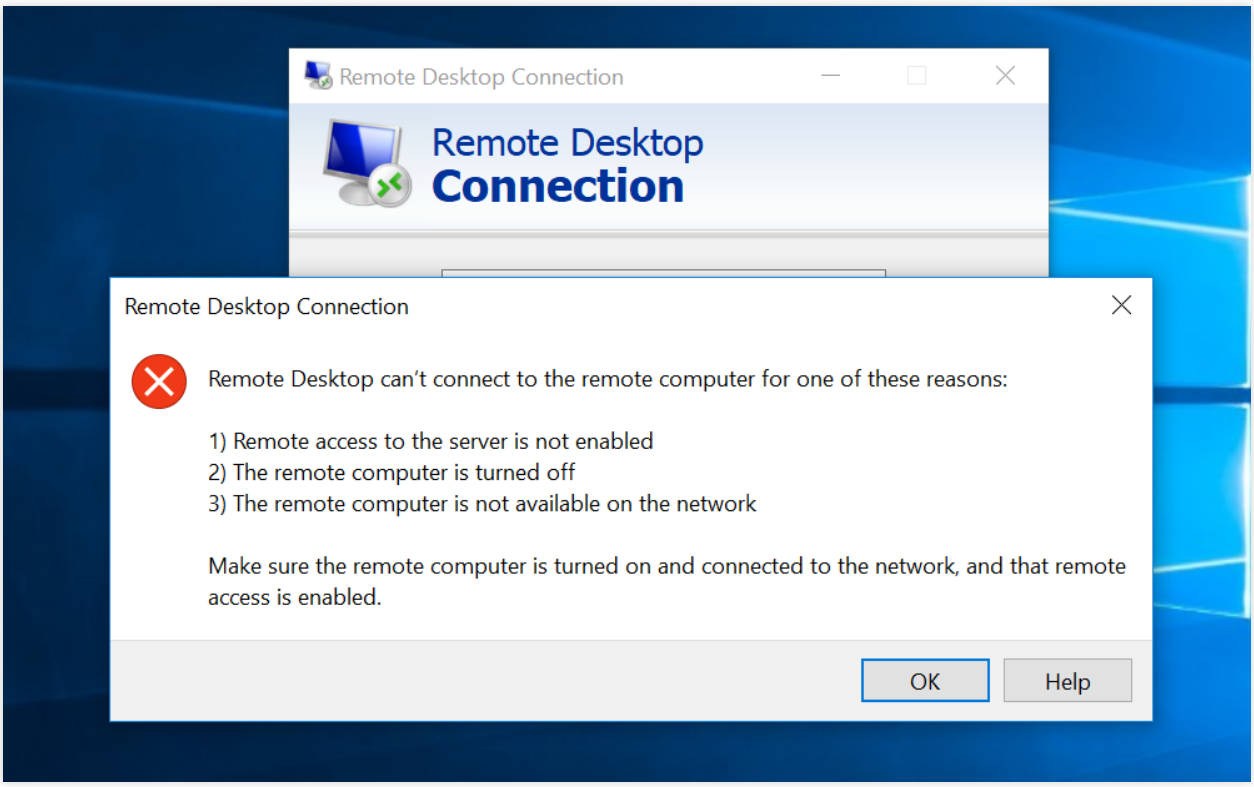
チケットを送信 して特定・対処方法について、お問い合わせください。

Windowsインスタンス：リモートデスクトップでリモートパソコンに接続できない

最終更新日：：2022-06-29 15:46:38

現象の説明

WindowsインスタンスへのWindowsリモート接続の適用時に、下図のような表示があらわれます。



リモートデスクトップが以下のいずれかの原因でリモートコンピュータに接続できなくなっています。

1）サーバーのリモートアクセスを有効にしていない

2）リモートコンピュータがシャットダウンされている

3）ネットワーク上でリモートコンピュータが利用できなくなっている

リモートコンピュータを起動していること、ネットワークに接続していてリモートアクセスを有効にしていることを確認します。

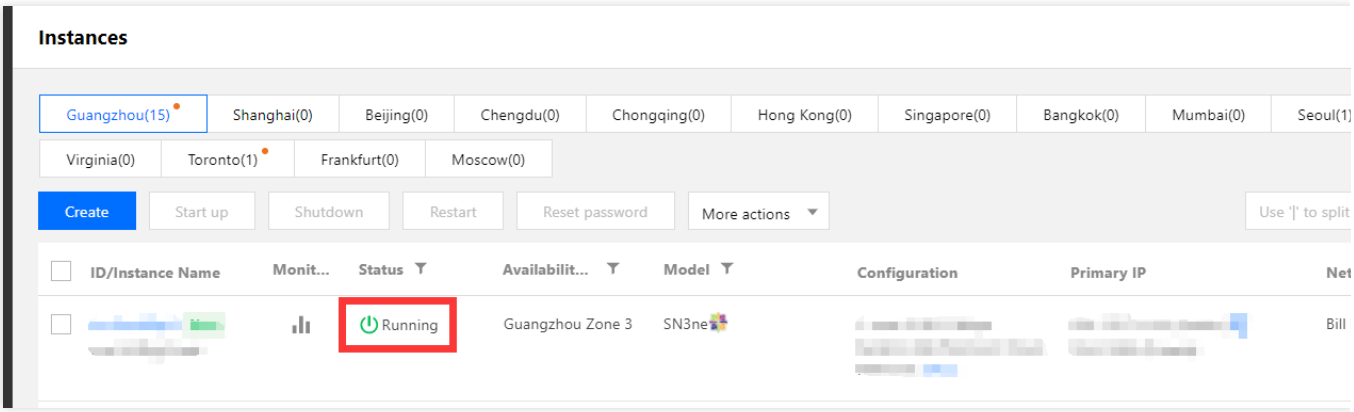
考えられる原因

上記が表示された原因には次のものがあります（これらに限定されません。実際の状況に応じて分析を行ってください）。
インスタンスが正常な実行状態にない
パブリックIPがない、またはパブリックネットワーク帯域幅が0
インスタンスをバインドしたセキュリティグループがリモートログインポートを開放していない（デフォルトでは3389）
リモートデスクトップサービスを起動していない
リモートデスクトップの設定に問題がある
Windowsファイアウォールの設定に問題がある

トラブルシューティングの手順

インスタンスが実行状態かどうかをチェックする

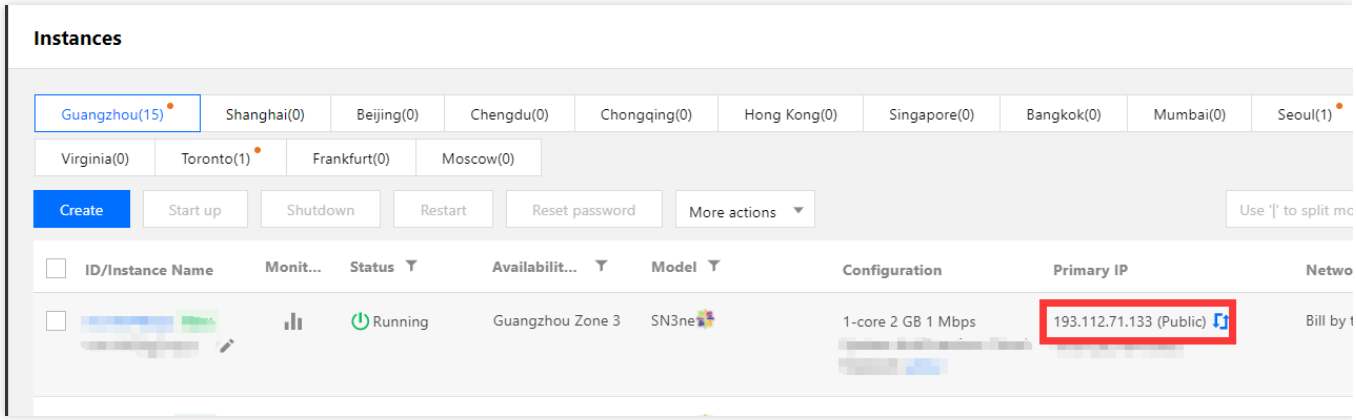
1. CVMコンソール にログインします。
2. 下図のように、インスタンスの管理画面で、インスタンスが「実行中」かどうかを確認します。



「はい」の場合は、サーバーがパブリックIPを設定しているかどうかをチェック してください。
「いいえ」の場合は、そのWindowsインスタンスを起動してください。

サーバーがパブリックIPを設定しているかどうかをチェックする

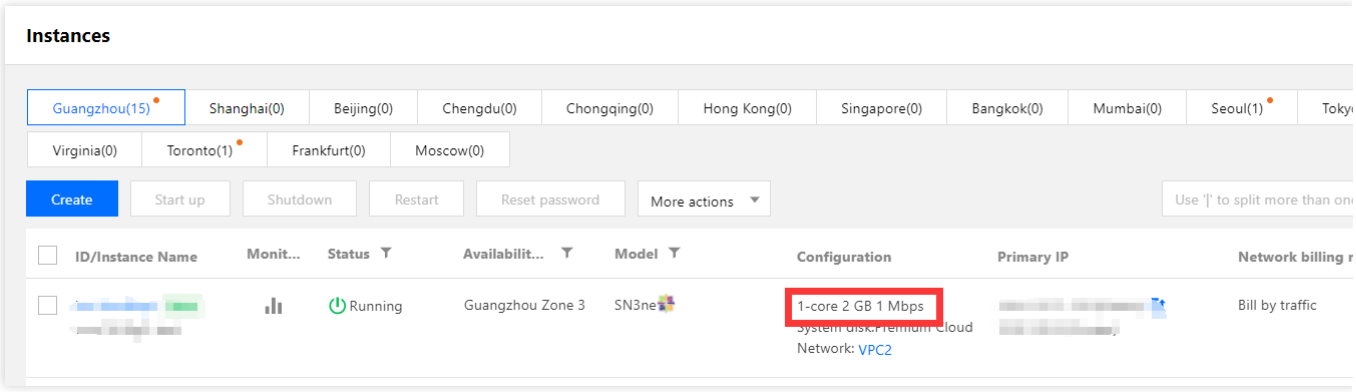
下図のように、サーバーがパブリックIPを設定しているかどうかをCVMコンソールでチェックします。



「はい」の場合は、パブリックネットワーク帯域幅を購入しているかどうかをチェック してください。
「いいえ」の場合は、Elastic IPを申請してバインド してください。

パブリックネットワーク帯域幅を購入しているかどうかをチェックする

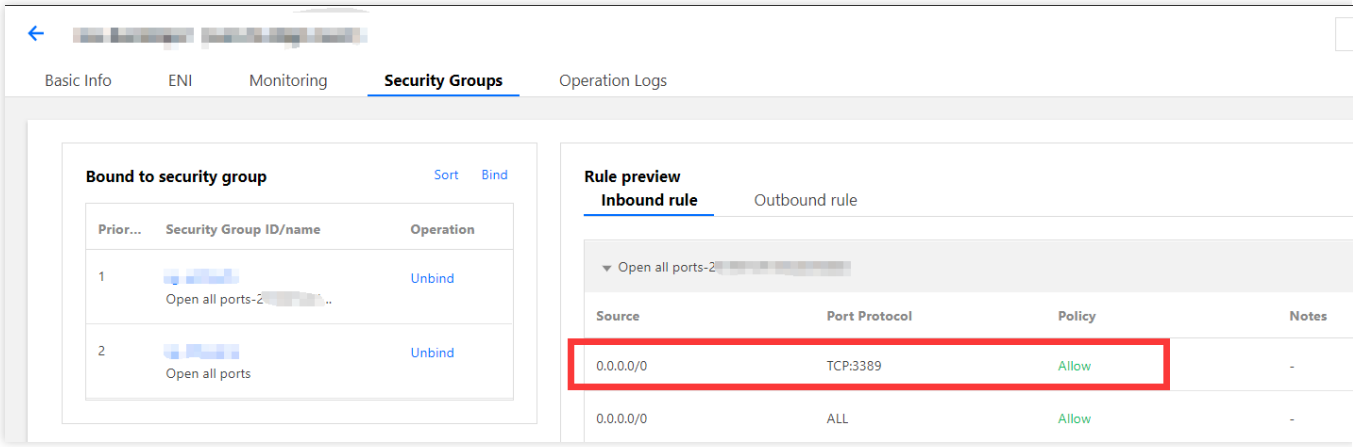
パブリックネットワーク帯域幅が0Mbかどうかをチェックします（最少1Mbps）。
「はい」の場合は、ネットワークの調整 を参照し、帯域幅を5Mbps以上に調整することをお勧めします。



「いいえ」の場合は、インスタンスのリモートログインポート（3389）が開放されているかどうかをチェック してください。

インスタンスのリモートログインポート（3389）が開放されているかどうかをチェックする

1. CVMコンソールのインスタンス管理ページで、ログインしたいインスタンスID/インスタンス名をクリックし、そのインスタンスの詳細ページに進みます。
2. 下図のように、**セキュリティグループ**タブで、インスタンスのセキュリティグループがリモートログインポート（デフォルトリモートデスクトップポート：3389）を開放しているかどうかをチェックします。



「はい」の場合は、リモートデスクトップサービスをチェック してください。
「いいえ」の場合は、対応するセキュリティグループルールを編集し、開放してください。操作方法については、セキュリティグループルールの追加 をご参照ください。

リモートデスクトップサービスをチェックする

1. VNCを使用してインスタンスにログイン し、Windowsインスタンスのリモートデスクトップサービスが有効になっているかどうかをチェックします。

説明：

以下の操作はWindows Server 2016 OSのインスタンスを例に説明します。

2.

を右クリックし、表示されたメニューから**システム**を選択します。

3. 表示された「システム」ウィンドウで、**高度なシステム設定**を選択します。

4. 表示された「システムのプロパティ」ウィンドウで、**リモート**タブを選択し、「このコンピュータへのリモート接続を許可する」にチェックが入っているかを確認します。

「はい」の場合は、ステップ5 を実行してください。
「いいえ」の場合は、チェックを入れて**OK**をクリックしてください。

5.

を右クリックし、表示されたメニューから**コンピュータの管理**を選択します。

6. 表示された「コンピュータの管理」ウィンドウの左側メニューバーで、**サービスとアプリケーション > サービス**を選択します。

7. 右側のサービスリストで、**Remote Desktop Services**を起動しているかどうかをチェックします。

「はい」の場合は、ステップ8 を実行してください。
「いいえ」の場合はサービスを起動してください。

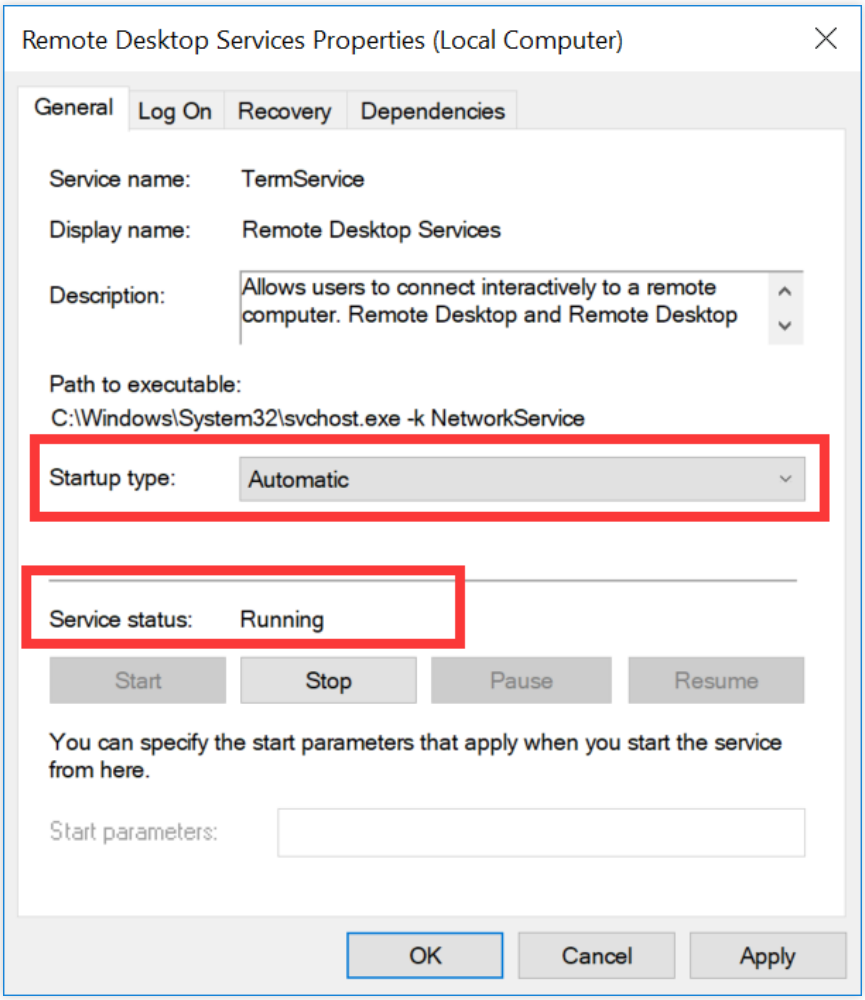
8.


を右クリックし、表示されたメニューから**実行**を選択します。
9. ポップアップした「実行」ウィンドウで**msconfig**と入力し、**OK**をクリックします。
10. 表示された「システム設定」ウィンドウで、**正常に起動**にチェックが入っているかを確認します。
「はい」の場合は、Windowsインスタンスのシステム設定をチェック してください。
「いいえ」の場合は、チェックを入れて**OK**をクリックしてください。

Windowsインスタンスのシステム設定をチェックする

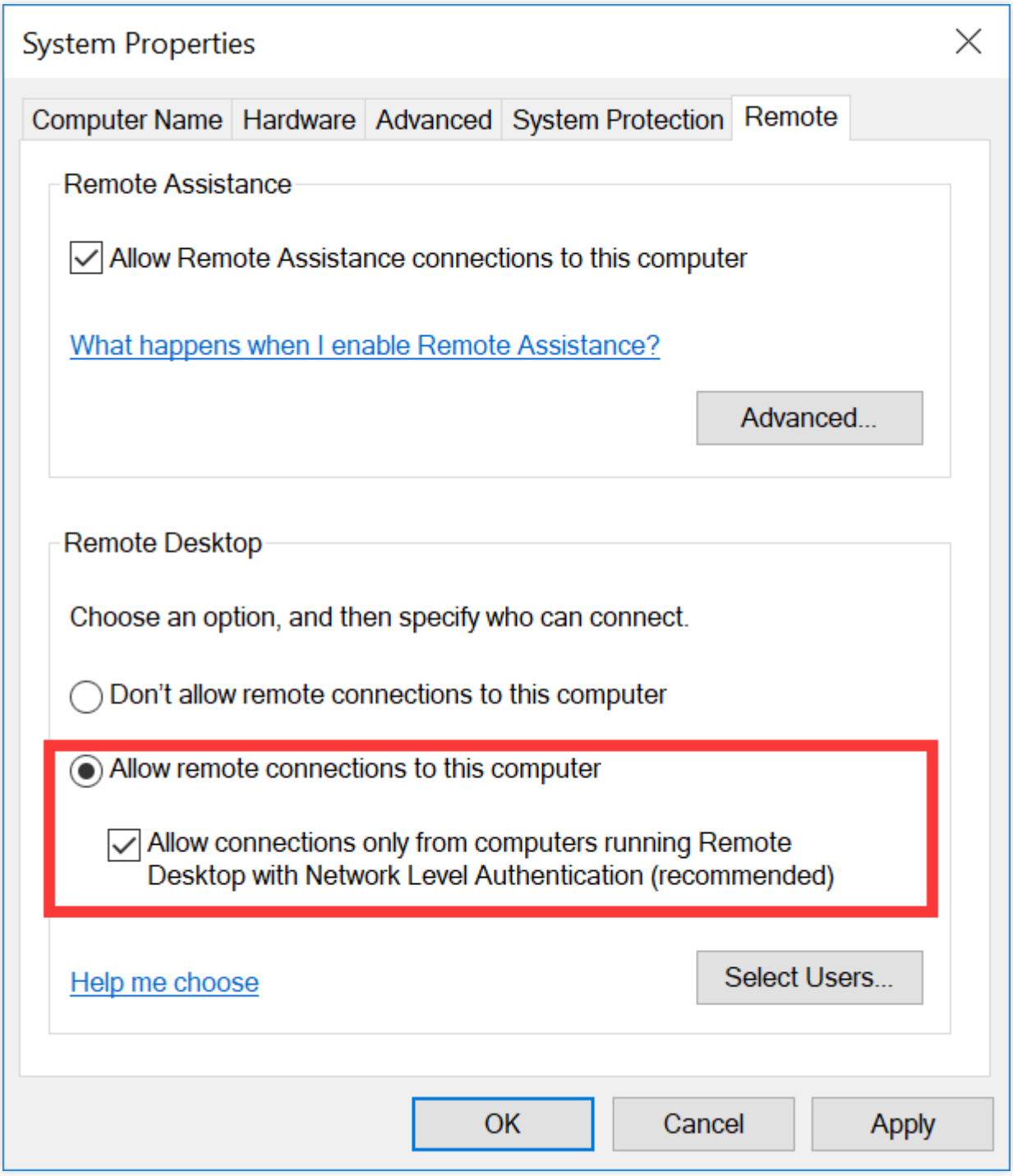
1. VNCを使用してインスタンスにログイン し、Windowsインスタンスのシステム設定のトラブルシューティングを行います。
説明：
次の操作はWindows Server 2012 OSのインスタンスを例に説明します。
2.


を右クリックし、表示されたメニューから*実行*を選択します。
3. ポップアップした「実行」に**services.msc**と入力し、**Enter**を押して「サービス」ウィンドウを開きます。
4. 下図のように、「Remote Desktop Services」のプロパティをダブルクリックし、リモートデスクトップサービスを起動しているかどうかをチェックします。



「はい」の場合は、ステップ5 を実行してください。
「いいえ」の場合は、「起動のタイプ」を「自動」に設定し、「サービスステータス」を「実行中」に設定します（**起動**をクリックするとサービスが起動します）。
5.

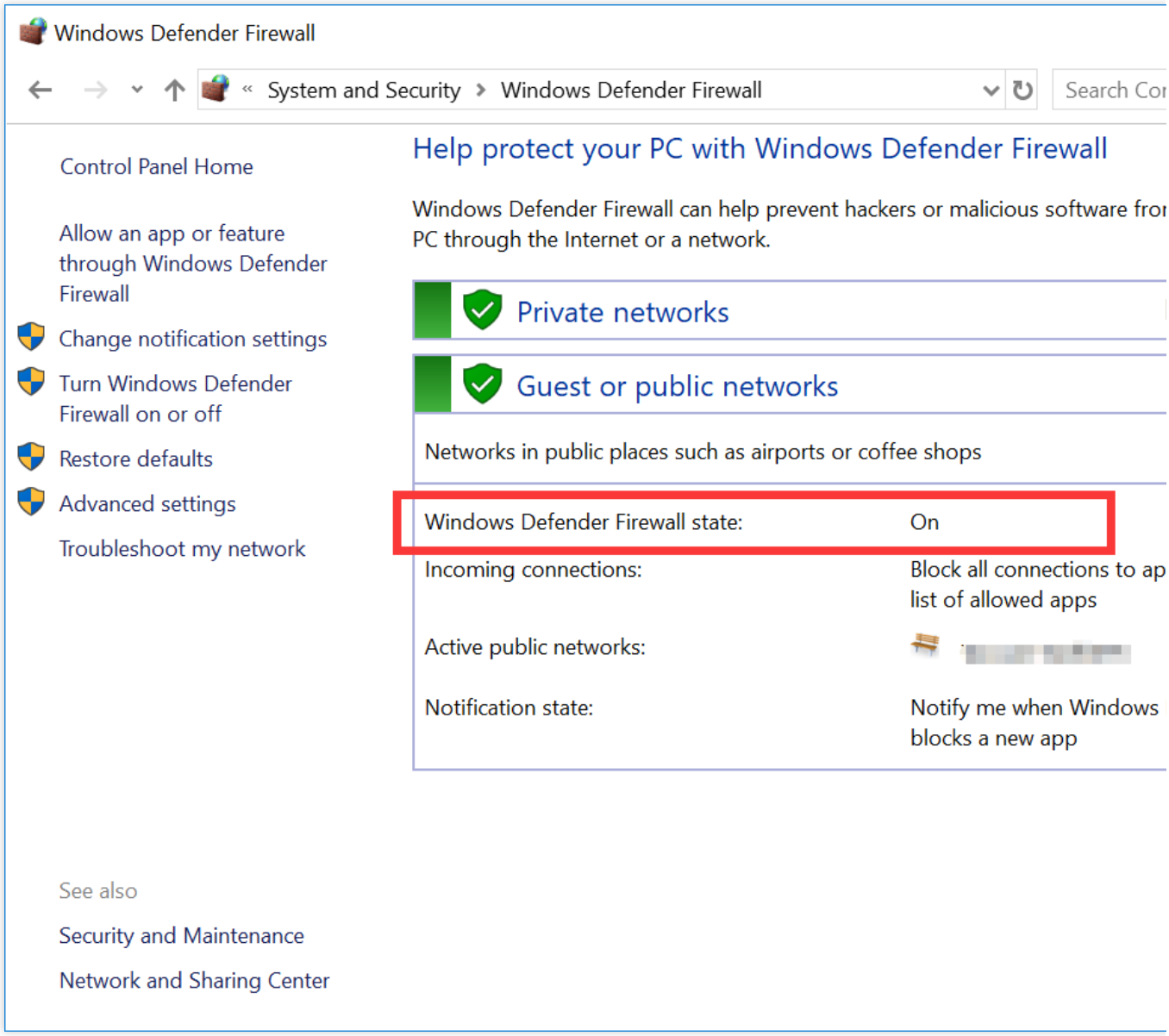
を右クリックし、表示されたメニューから*実行*を選択します。
6. ポップアップした「実行」ウィンドウに**sysdm.cpl**と入力し、**Enter**を押して、「システムのプロパティ」ウィンドウを開きます。
7. 下図のように、「リモート」タブで、リモートデスクトップの設定が「このコンピュータへのリモート接続を許可する(L)」となっているかどうかをチェックします。



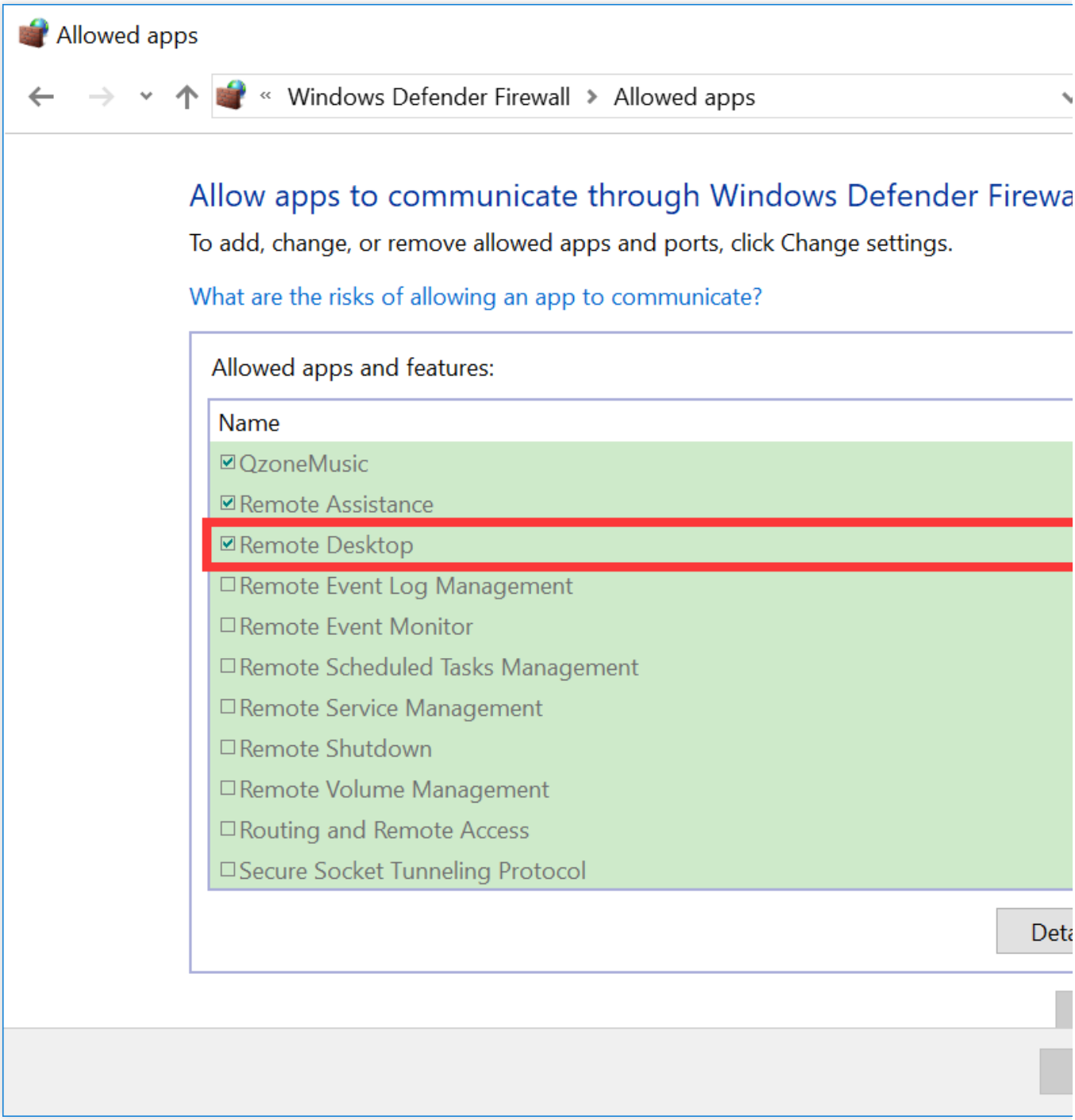
「はい」の場合は、ステップ8 を実行してください。
「いいえ」の場合は、リモートデスクトップを「このコンピュータへのリモート接続を許可する(L)」に設定してください。
8.

をクリックし、**コントロールパネル**を選択し、コントロールパネルを開きます。

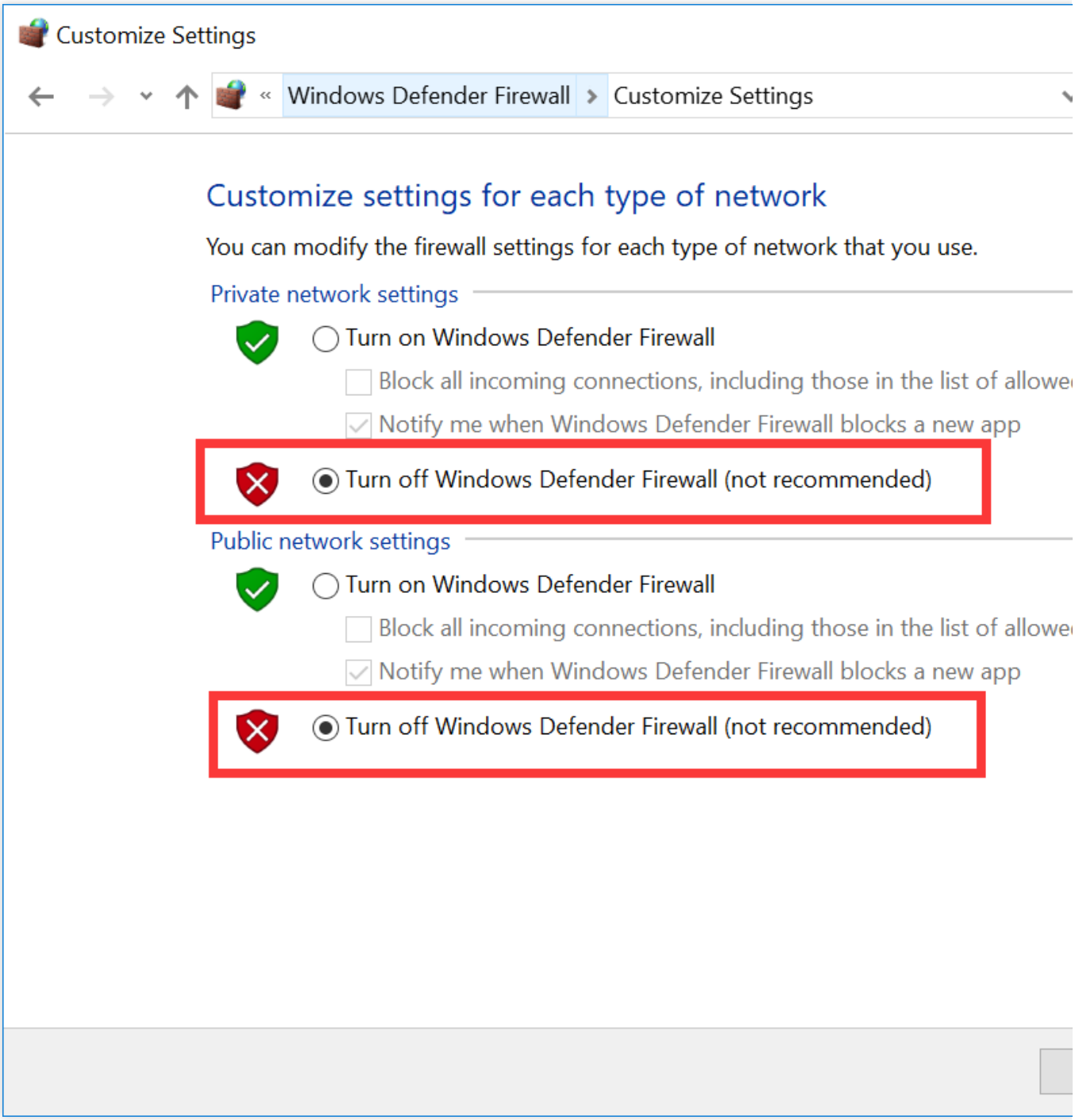
9. 「コントロールパネル」で、**システムとセキュリティ > Windowsファイアウォール**を選択し、「Windowsファイアウォール」を開きます。
10. 下図のように、「Windowsファイアウォール」でWindowsファイアウォールの状態をチェックします。



「有効」な状態であれば、ステップ11 を実行してください。
「無効」な状態であれば、オンラインサポート を通してフィードバックします。
11. 「Windowsファイアウォール」で**Windowsファイアウォールによるアプリケーションの許可**をクリックし、「許可されたアプリケーション」ウィンドウを開きます。
12. 下図のように、「許可されたアプリケーション」ウィンドウで、「許可されたアプリケーションおよび機能(A)」の「リモートデスクトップ」にチェックが入っているかどうかを確認します。



「はい」の場合は、ステップ13 を実行してください。
「いいえ」の場合は、「リモートデスクトップ」にチェックを入れ、「リモートデスクトップ」を有効にしてください。
13. 「Windowsファイアウォール」で**Windowsファイアウォールの有効化または無効化**をクリックし、「設定のカスタマイズ」ウィンドウを開きます。
14. 下図のように、「設定のカスタマイズ」ウィンドウで、「プライベートネットワークの設定」と「パブリックネットワークの設定」を「Windowsファイアウォールを無効にする（非推奨）」に設定します。



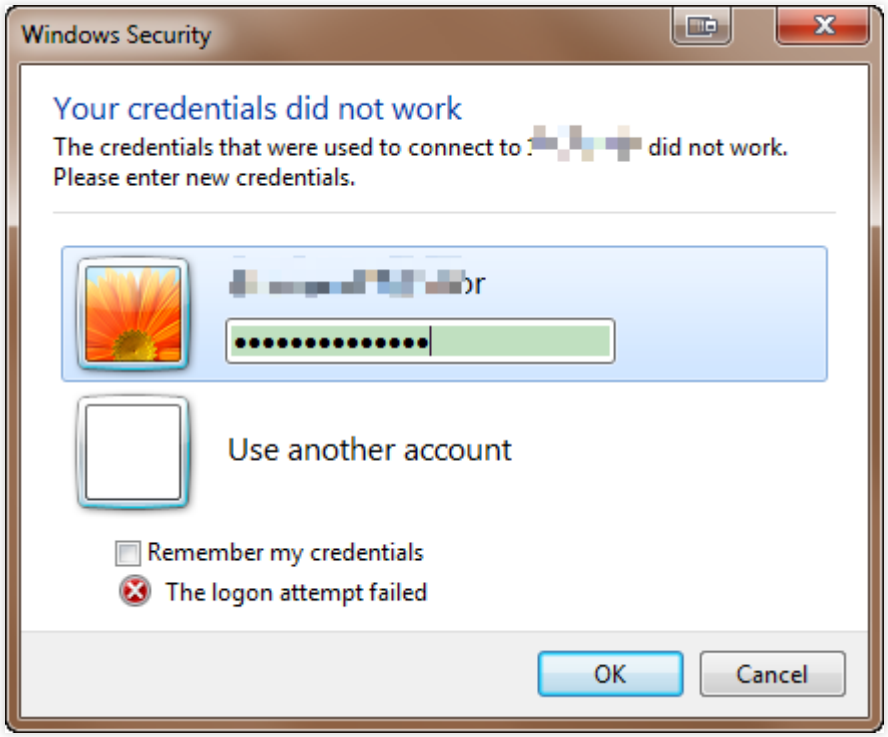
上記の操作を実行しても、リモートデスクトップによってWindowsインスタンスに接続できない場合は、オンラインサポート に連絡してフィードバックしてください。

Windowsインスタンス：お使いの資格情報は機能しませんでした

最終更新日：：2022-05-26 15:41:32

問題の説明

Windows OSのローカルコンピュータがRDPプロトコル（MSTSCなど）により、リモートデスクトップ接続を使用してWindows CVMにログインすると、次のエラーが表示されます。
お使いの資格情報は機能しませんでした。XXX.XXX.XXX.XXX への接続に使用された資格情報は機能しませんでした。新しい資格情報を入力してください。



処理手順

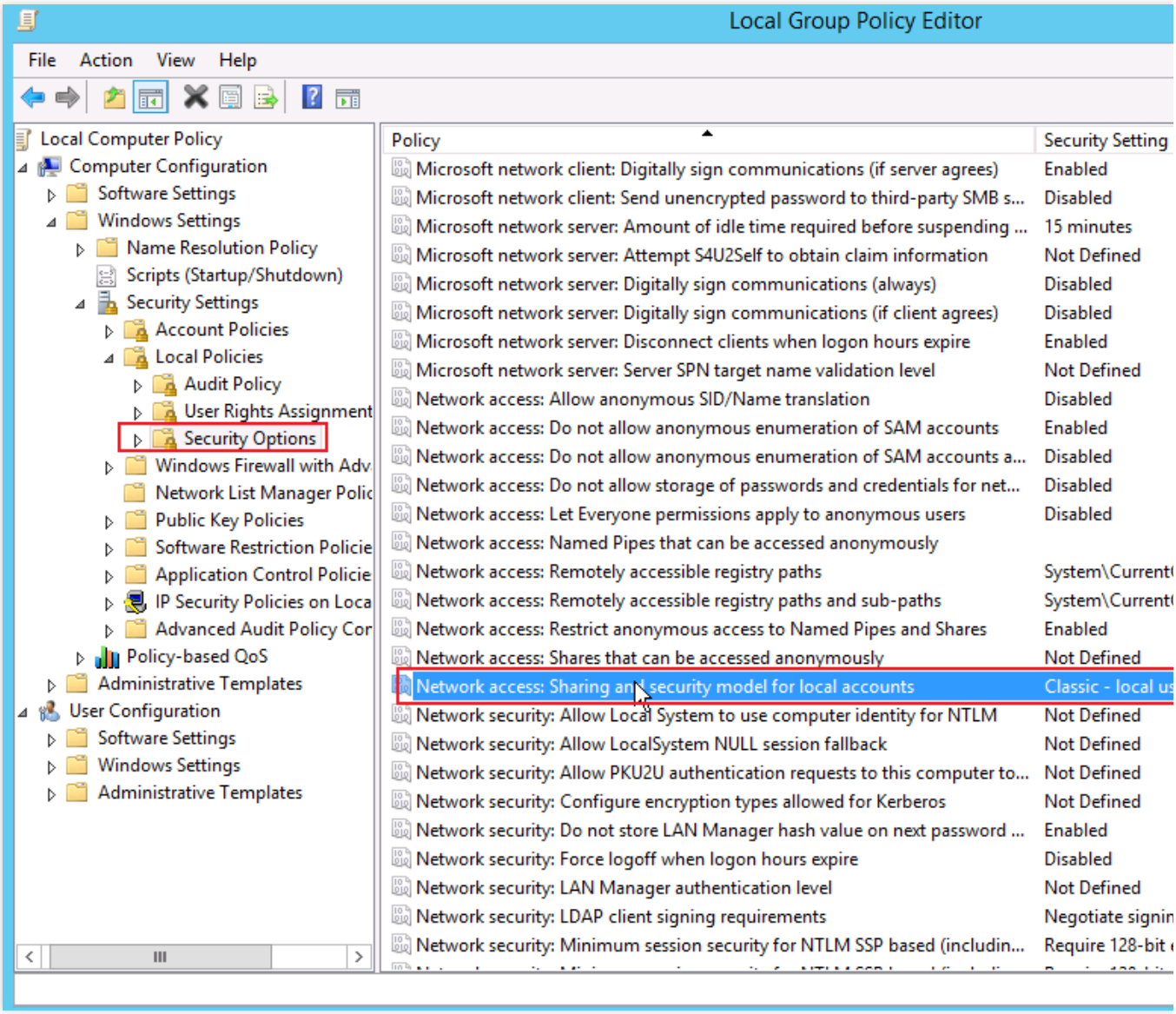
説明：
Windows Server 2012 OSを例にしていますが、OSのバージョンが異なるため、操作手順の詳細はわずかに異なります。
以下の手順に従ってトラブルシューティングを行い、各手順が実行した後、Windows CVMに再接続して問題が解決されたか確認します。問題が解決されていない場合は、次の手順に進みます。

ステップ1：ネットワークアクセスポリシーを変更する

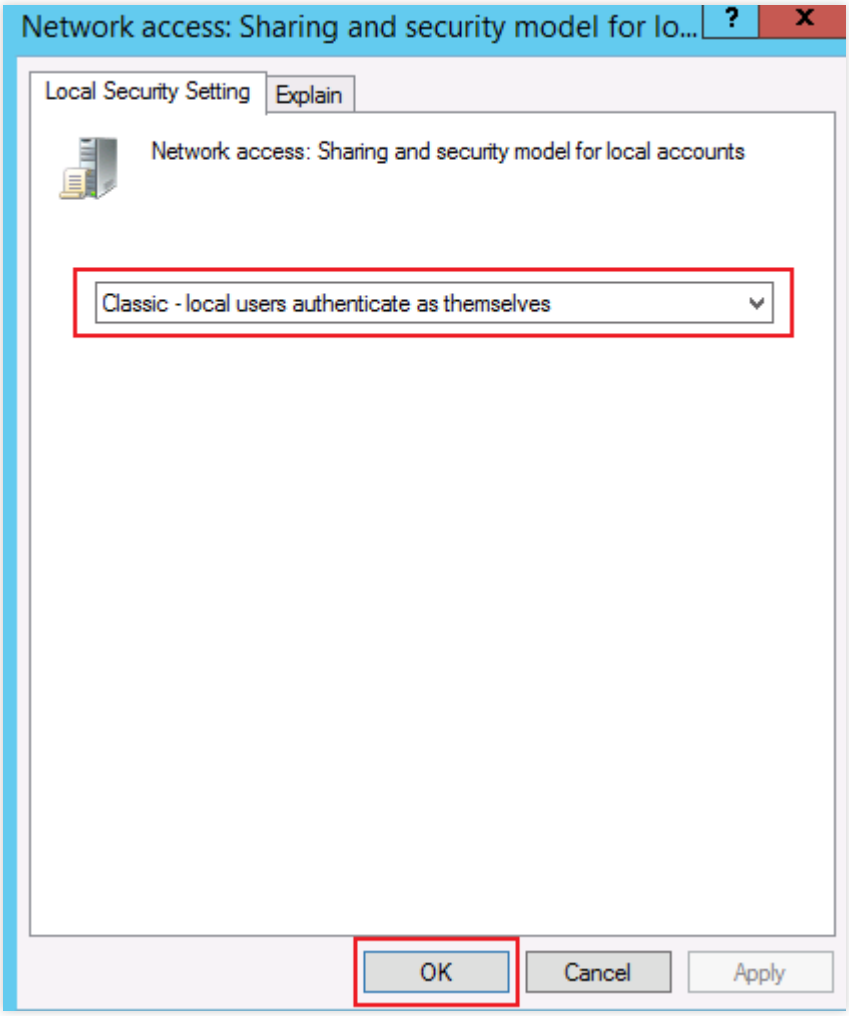
1. VNCを使用してWindowsインスタンスにログインします。
2. OS画面で、

をクリックして、「Windows PowerShell」ウインドウを開きます。

3. 「Windows PowerShell」ウィンドウで、**gpedit.msc**を入力し、**Enter**キーを押すと、「ローカルグループポリシーエディター」を起動します。
4. 左側のナビゲーションで、**コンピュータの構成 > ポリシー>Windows の設定 > セキュリティの設定 > ローカルポリシー > セキュリティ オプション**ディレクトリを順次展開します。
5. **セキュリティオプション**の**ネットワークアクセス：ローカルアカウントの共有とセキュリティモデル**を探して開きます。以下の通りです。



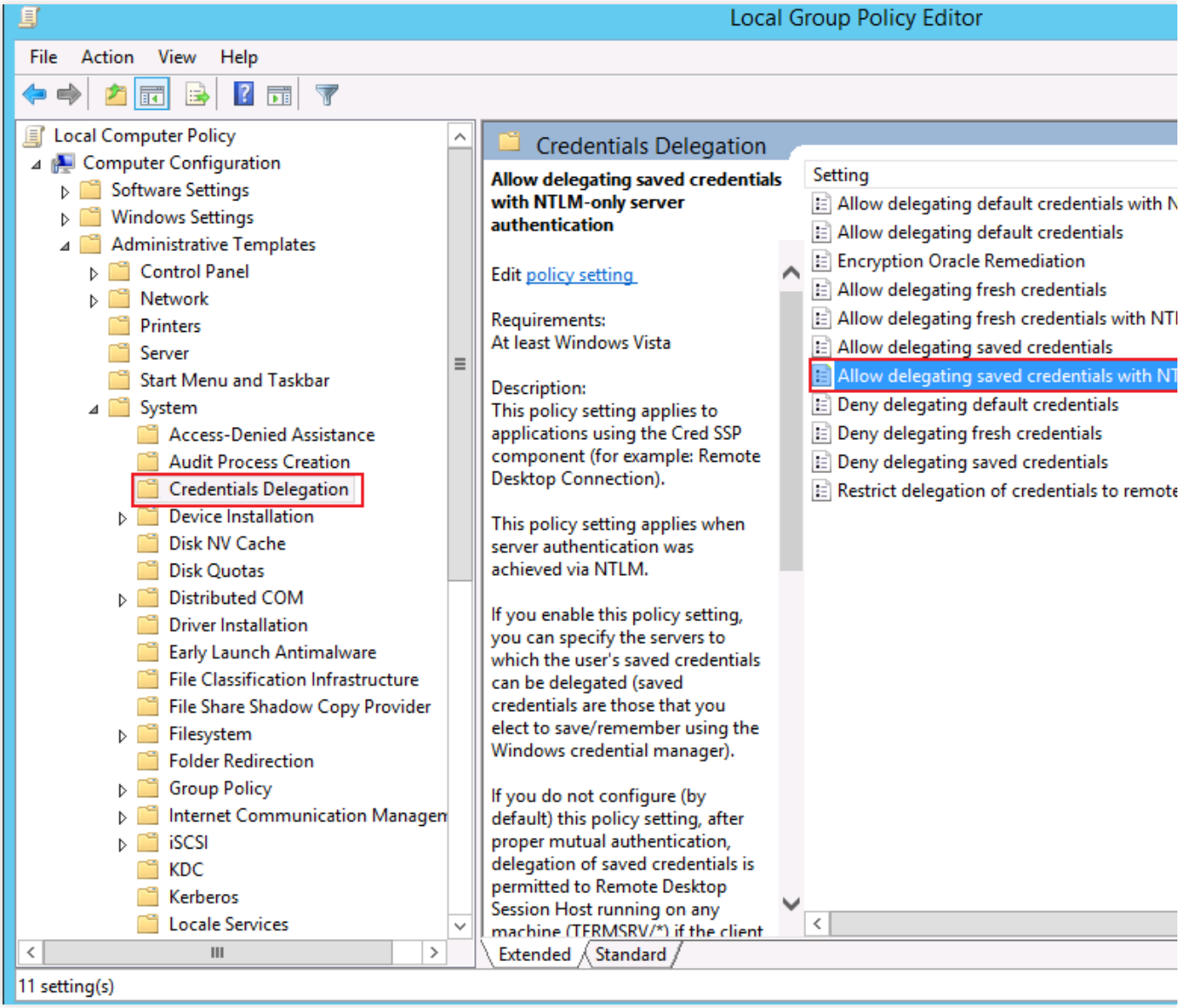
6. **クラシック – ローカルユーザーがローカルユーザーとして認証する**を選択し、**OK**をクリックします。以下の通りです。



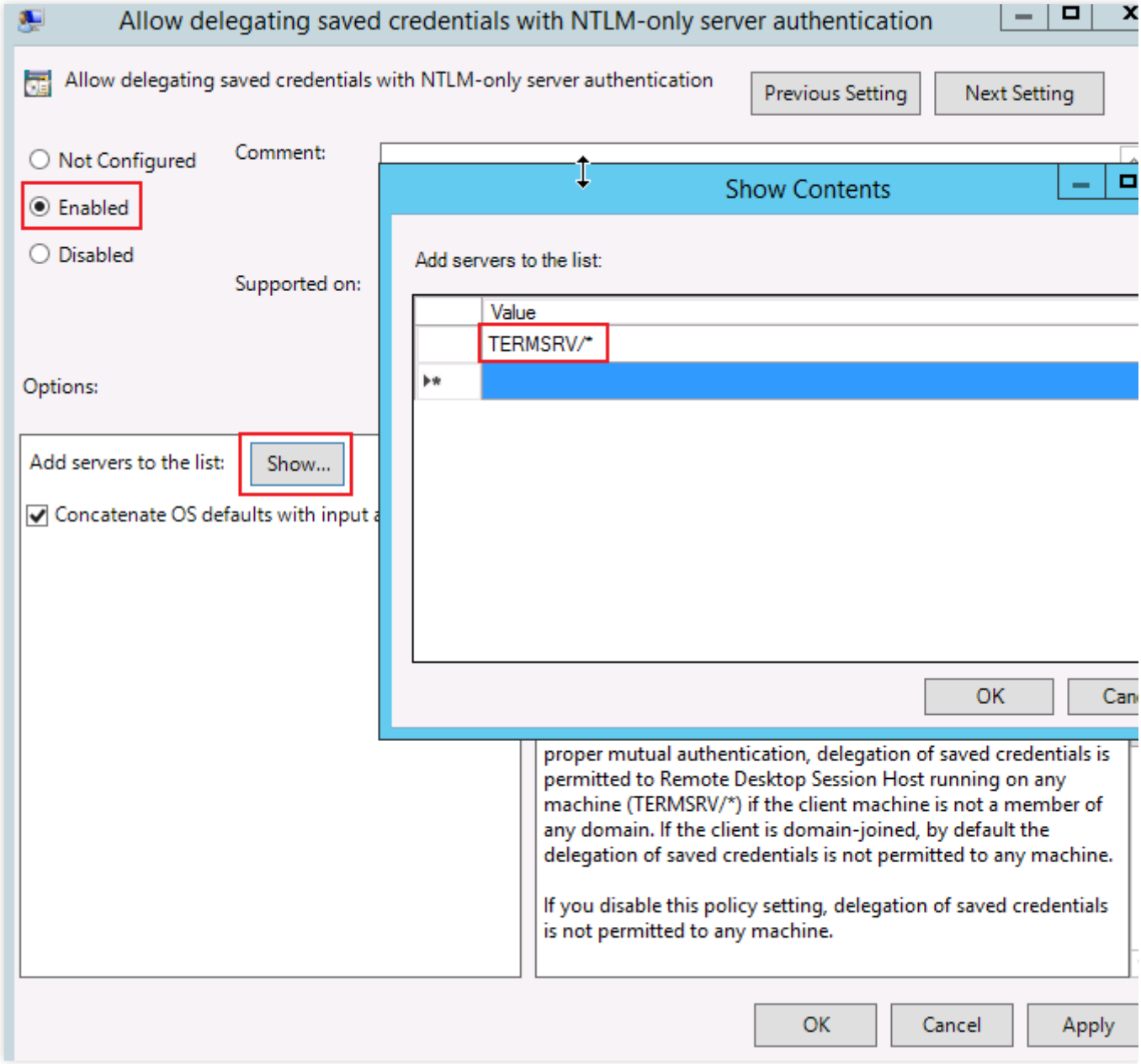
7. Windows CVMに再接続し、接続に成功したか確認します。
はい、タスクは終了しました。
いいえ、ステップ2（資格情報の委任を変更する）を実行してください。

ステップ2：資格情報の委任を変更する

1. 「ローカルグループポリシーエディター」の左側のナビゲーションバーで、**コンピューターの構成 > ポリシー > 管理用テンプレート > システム > 資格情報の委任**ディレクトリを順次展開します。
2. **資格情報の委任 のNTLMのみのサーバー認証で保存された資格情報の委任を許可する**を見つけて有効にします。以下の通りです。



3. 設定を有効にし、「表示」をクリックします。Windows 資格情報を使用して接続したいサーバーのIPアドレスやホスト名を指定します。ホスト名を指定する前に、「TERMSRV/」をつける必要があります。すべてのサーバーへの接続を許可したい場合は、「＊」を使用します。

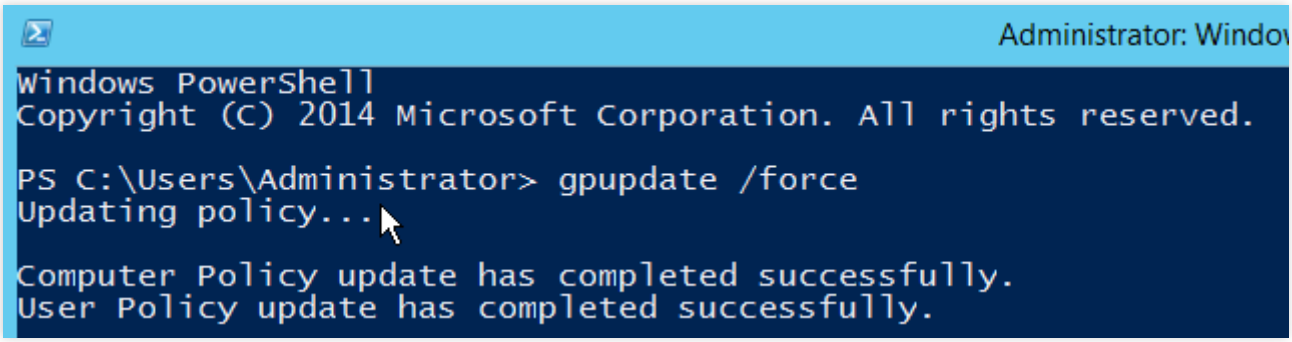


4. **OK**をクリックします。

5. OS画面で、

をクリックして、「Windows PowerShell」ウインドウを開きます。

6. 「Windows PowerShell」ウィンドウで、**gpupdate/force**を入力し、**Enter**キーを押してグループポリシーを更新します。以下の通りです。



7. Windows CVMに再接続し、接続に成功したか確認します。

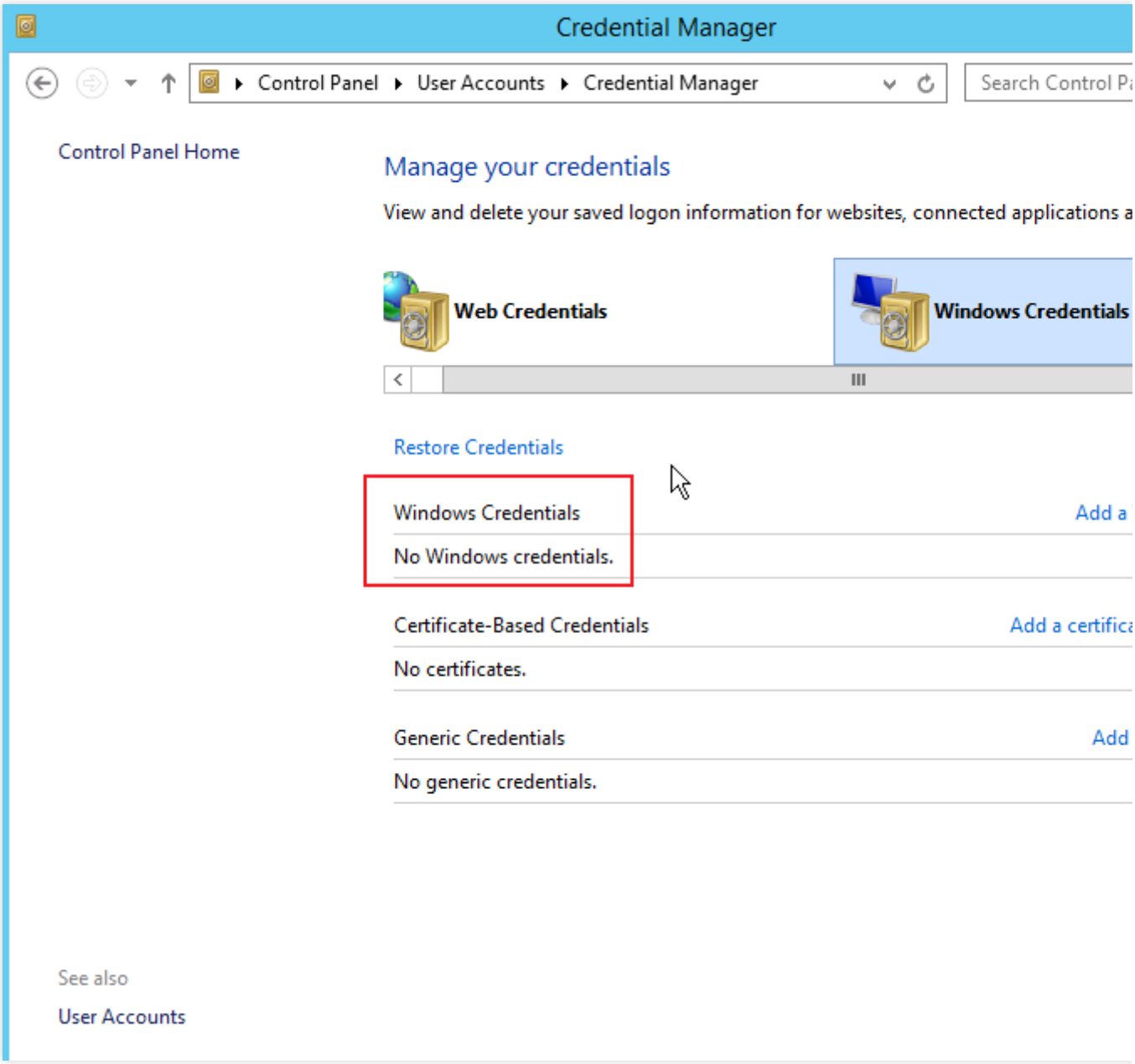
はい、タスクは終了しました。

いいえ、ステップ3（ローカル資格情報の設定）を実行してください。

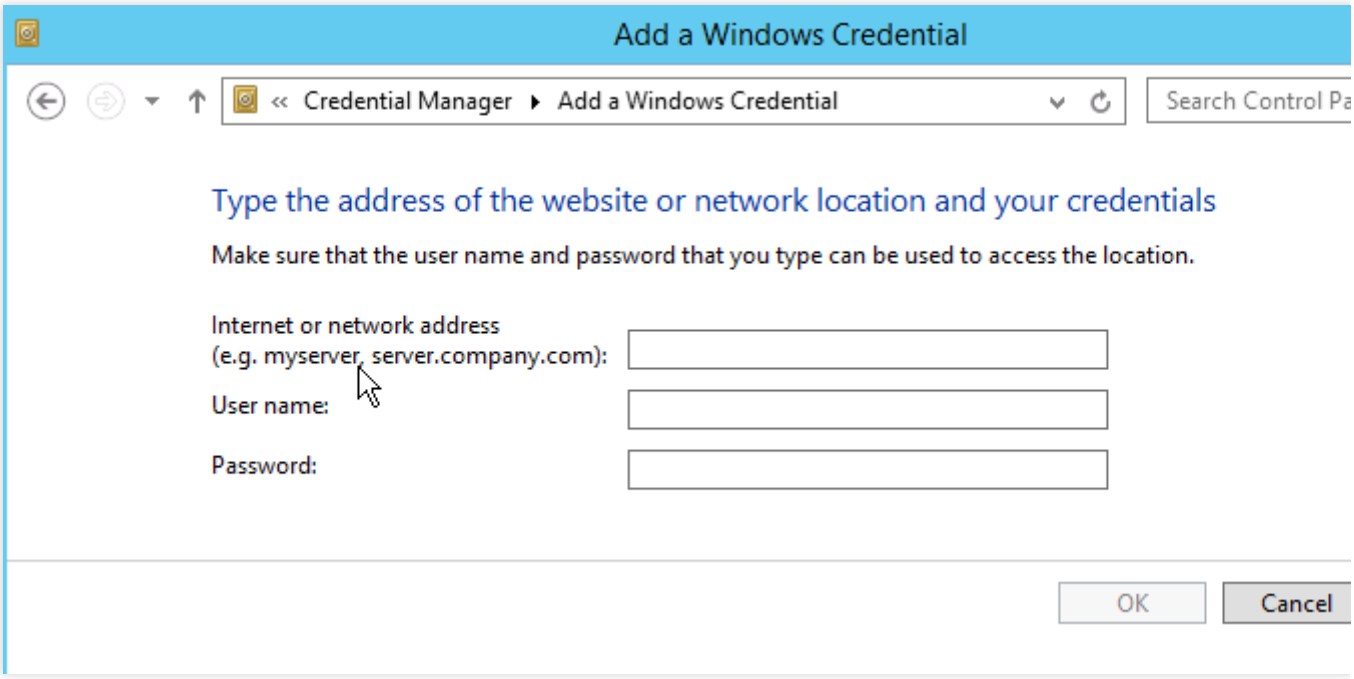
ステップ3：ローカル資格情報の設定

1. OS画面で、

＞**コントロールパネル**＞**ユーザーアカウント**をクリックし、**資格情報マネージャー**の**Windows 資格情報の管理**を選択すると、Windows資格情報画面に進みます。以下の通りです。



2. Windowsの資格情報の下に、現在ログインしているCVMの資格情報があるかどうかを確認します。
ない場合は、次のステップに進み、Windows資格情報を追加します。
ある場合は、ステップ4（CVMのパスワード保護共有の無効設定）を実行してください。
3. **Windows資格情報の追加**をクリックして、Windows資格情報追加画面に進みます。以下の通りです。



4. 現在ログインしているCVMのIPアドレス、ユーザー名とパスワードを入力し、**OK**をクリックします。

説明：

CVMのIPアドレスは、CVMインスタンスのパブリックIPアドレスを指します。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。

Windowsインスタンスのデフォルトのユーザー名は `Administrator` であり、パスワードはインスタンスの作成時に設定されます。ログインパスワードを忘れた場合は、 インスタンスパスワードのリセット をご参照ください。

5. Windows CVMに再接続し、接続に成功したか確認します。

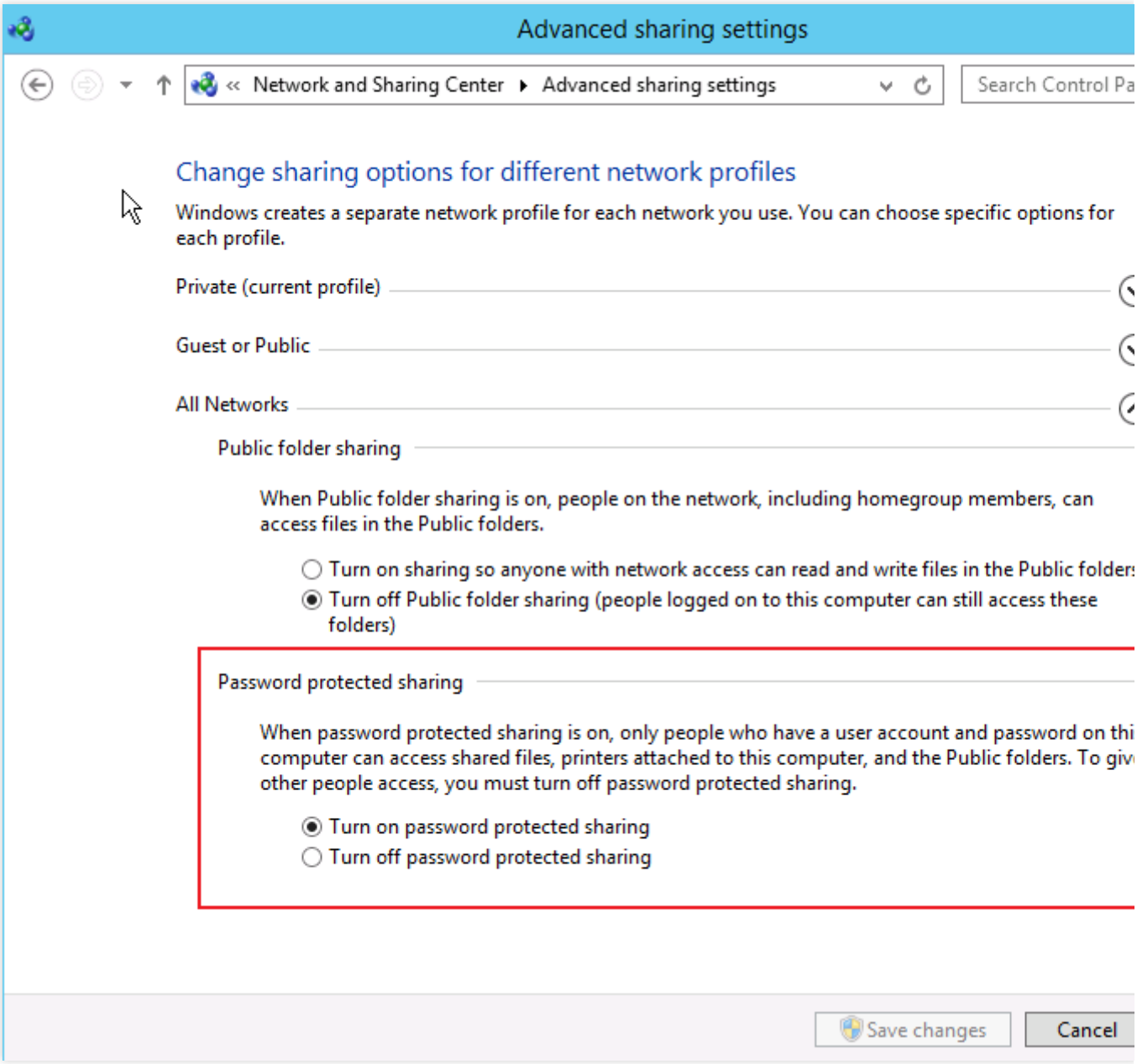
はい、タスクは終了しました。

いいえ、ステップ4（CVMのパスワード保護共有の無効設定）を実行してください。

ステップ4：CVMのパスワード保護共有の無効設定

1. OS画面で、

＞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＞共有の詳細設定の変更をクリックして、共有設定画面に進みます。以下の通りです。



2. **すべてのネットワーク**タブを展開し、**パスワード保護共有**の下で**パスワード保護共有を無効にする**を選択し、**変更の保存**をクリックします。

3. Windows CVMに再接続し、接続に成功したか確認します。

はい、タスクは終了しました。

いいえ、チケットを送信 して問題を報告してください。

Windows インスタンス：ポート問題が原因でリモートログインできない

最終更新日：：2023-06-08 16:54:00

このドキュメントでは、Cloud Virtual Machineがポートの問題によりリモートログインできない場合のトラブルシューティングと解決案について説明します。

説明：

以下の操作は、Windows Server 2012システムを使用したCVMを例にします。

検証ツール

Tencent Cloudが提供するツールを使用して、ログインできない問題はポートとセキュリティグループの設定に関連しているかどうかを判断することができます：

セルフ診断

セキュリティグループ（ポート）検証ツール

セキュリティグループの設定の問題を検出された場合、セキュリティグループ(ポート)検証ツール 中の**Open all ports**機能を利用して、関連するポートを開放し、再度ログインを試みます。ポートを開放してもまだログインできない場合、以下の内容を参照して原因を特定します。

トラブルシューティング

ネットワーク接続を検査する

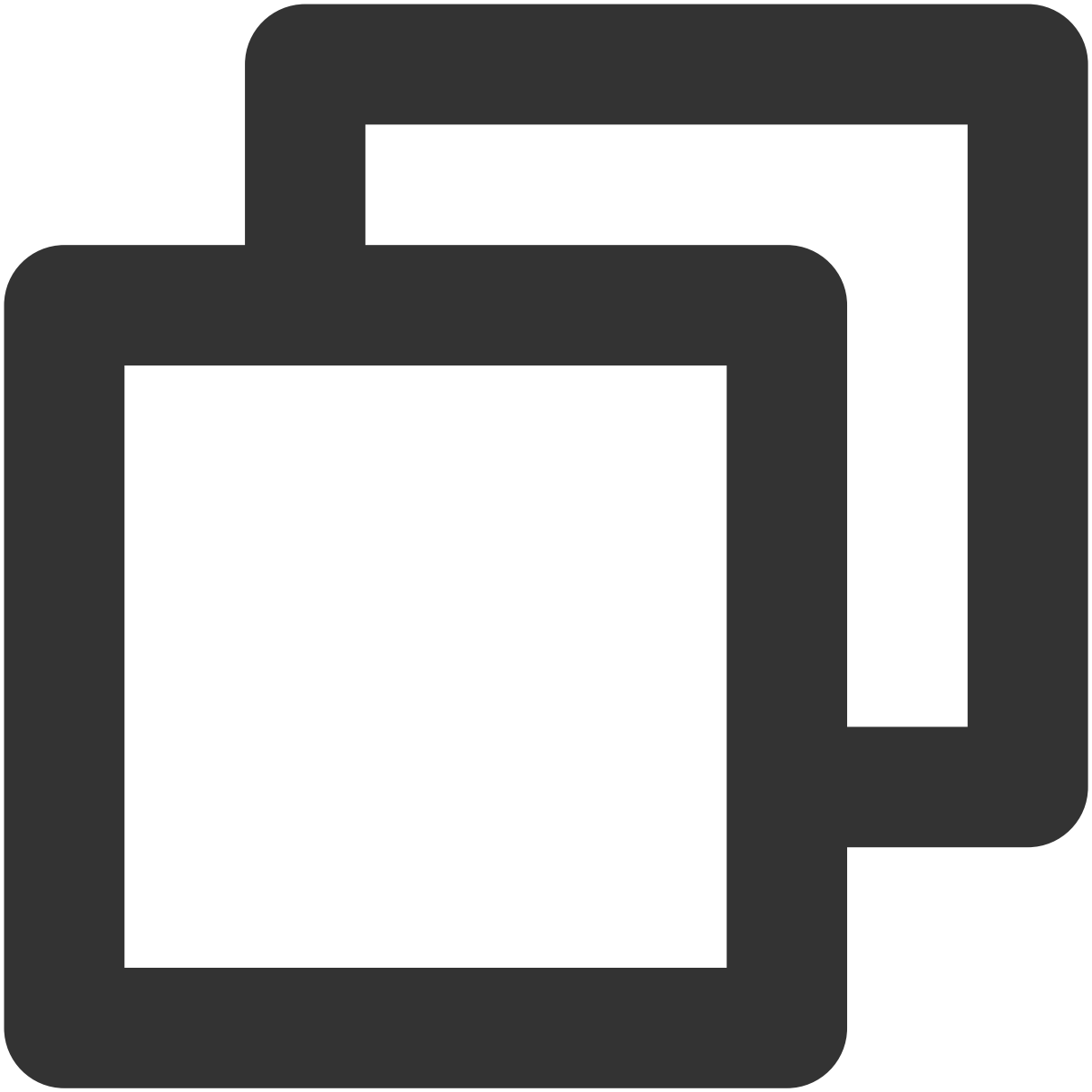
ローカルのPingコマンドを通じて、ネットワーク接続をテストすることができます。同時に、異なるネットワーク環境（異なるIPレンジ或いはキャリア）のコンピューターでテストを行い、ローカルネットワークの問題なのか、サーバーの問題なのかを確認できます。

1. ローカルコンピューターでコマンドラインツールを開きます。

Windows システム：**スタート > 実行**をクリックし、**cmd**を入力すると、コマンドラインダイアログボックスが表示されます。

Mac OS システム：Terminalツールを開きます。

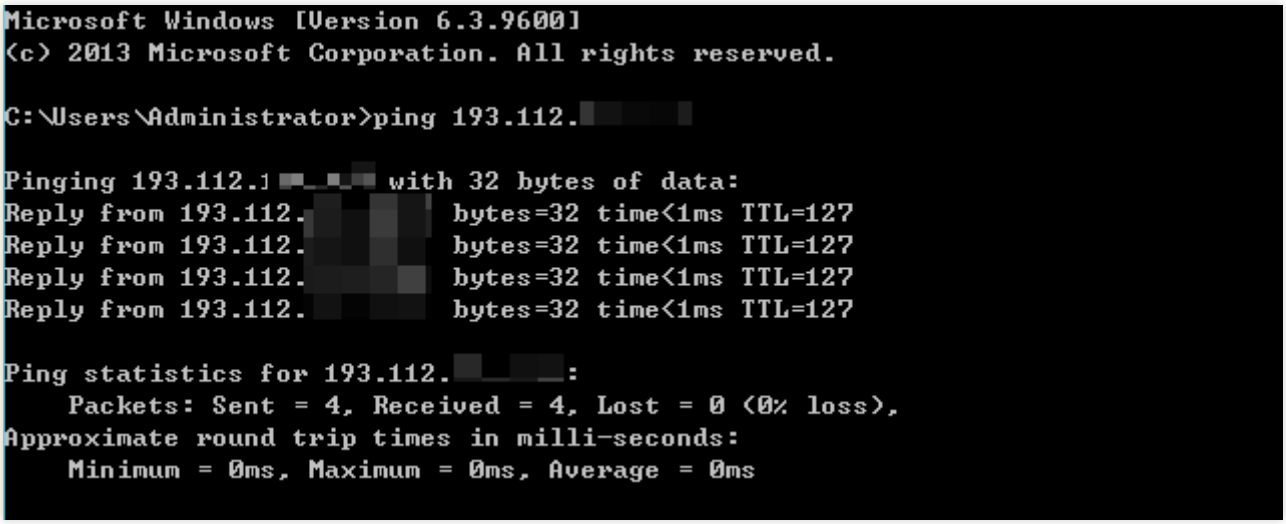
2. 以下のコマンドを実行して、ネットワーク接続をテストします。



```
ping + CVM インスタンスのパブリックIP アドレス
```

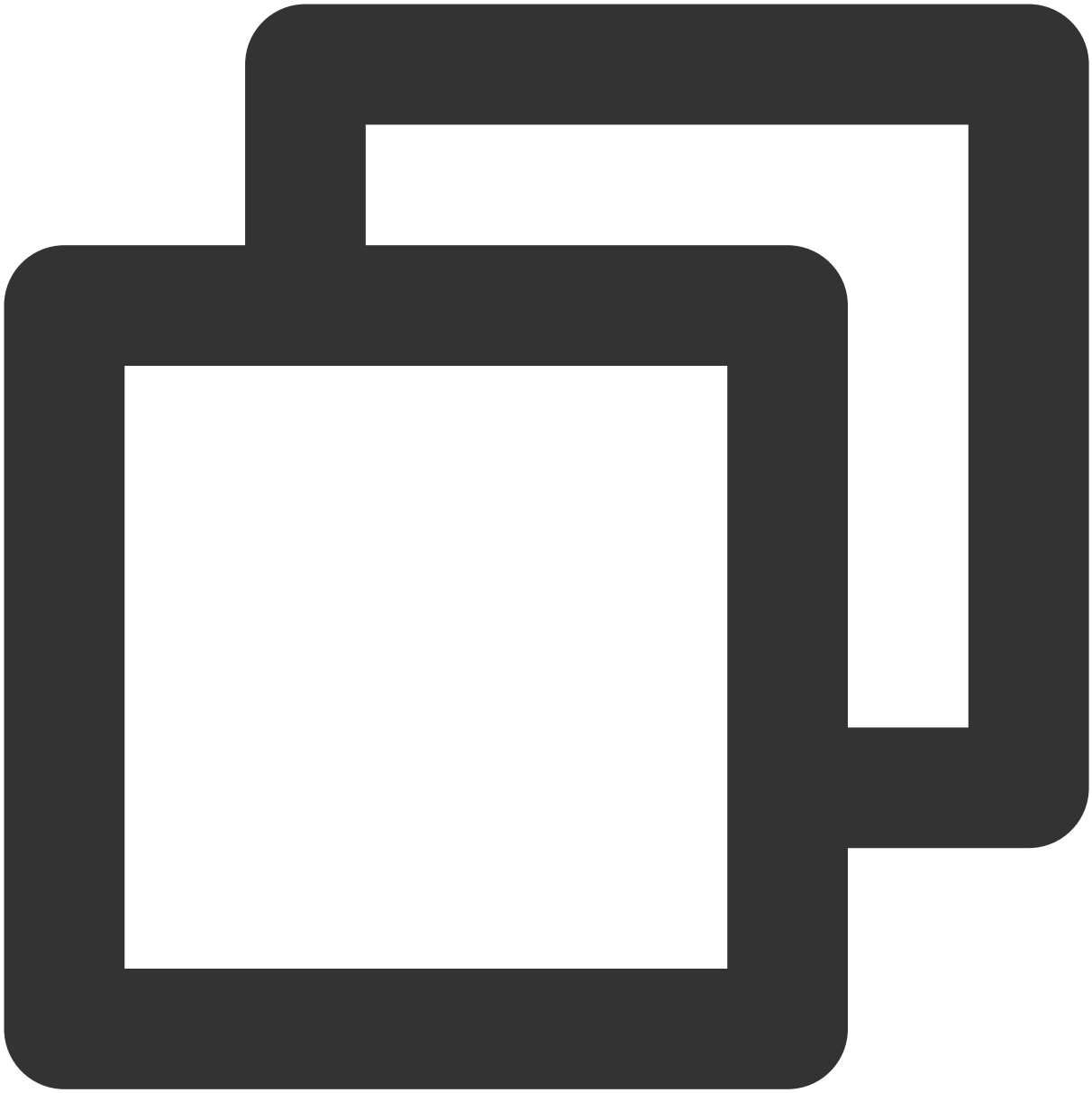
例えば、`ping 139.199.XXX.XXX` コマンドを実行します。

ネットワークが正常な場合、次の果が返されます。リモートデスクトップサービス設定を検査 してください。



ネットワークに異常がある場合、**要求がタイムアウトしました**が提示された場合、インスタンスIPアドレスのPingの失敗 を参照して検査してください。

3. 以下のコマンドを実行し、**Enter**キーを押して、リモートポートの開放状態をテストし、ポートにアクセスできるかどうかを判断します。

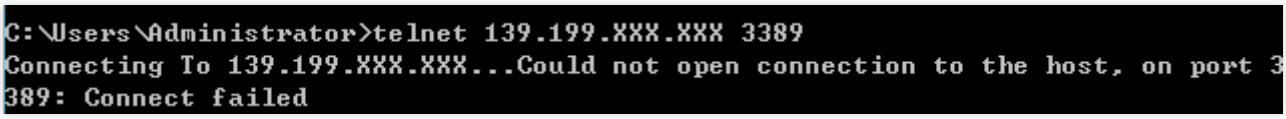


```
telnet + CVM インスタンスのパブリックIP アドレス + ポート番号
```

例えば、`telnet 139.199.XXX.XXX 3389` コマンドを実行します。下記画像に示すように：

正常状態：ブラックスクリーン、カーソルキーのみ表示されます。これはリモートポート(3389)にアクセスできることを示しています。インスタンスのリモートデスクトップサービスが有効になっているかどうかを確認 してください。

異常状態：接続失敗は、下記画像に示すようになります。これはネットワークに問題があることを示しています。問題のあるネットワークの該当部分を検査してください。



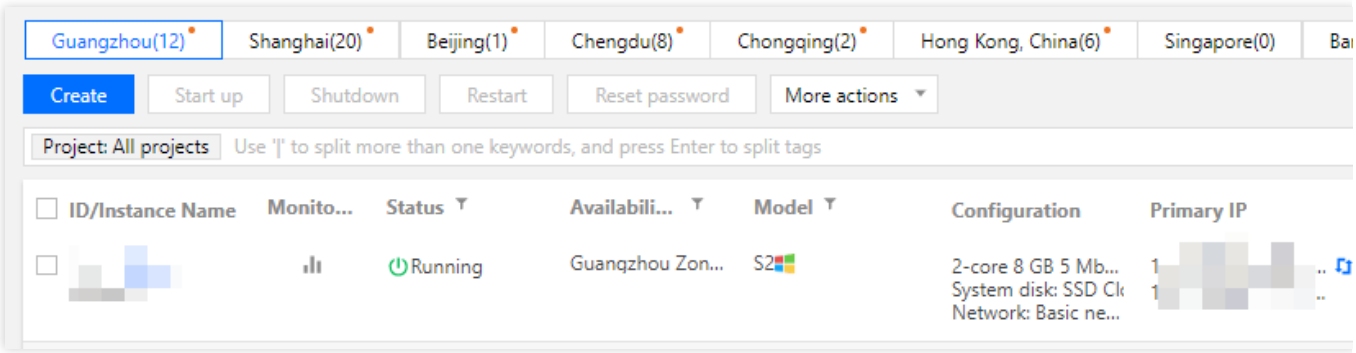
リモートデスクトップサービスの設定を検査する

VNCを介してCVMにログインする

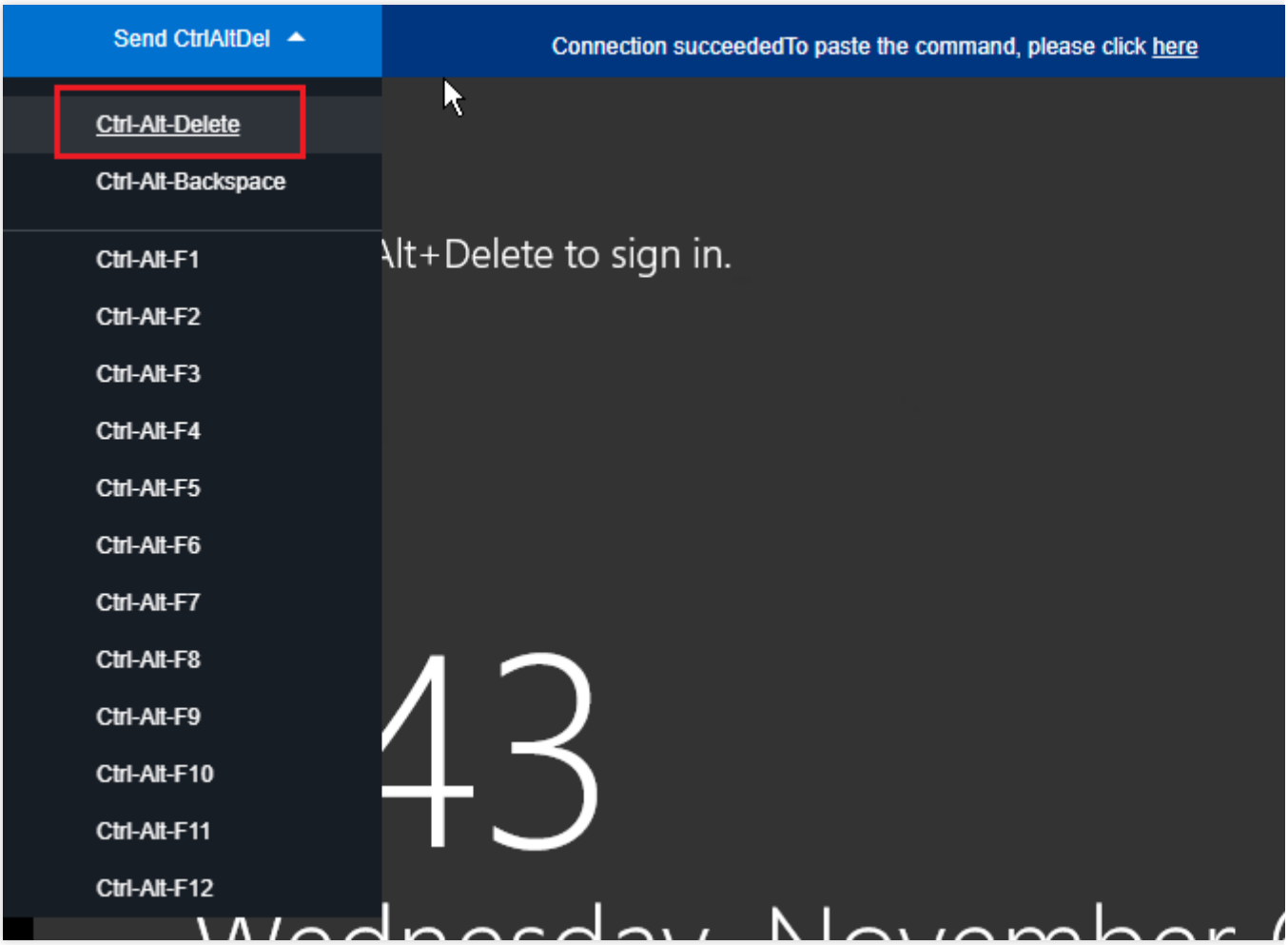
説明：

標準方式でCVMにログインできない場合、VNC方式を使用することをお勧めします。

1. CVMコンソール にログインします。
2. チェックするCVMを選択し、**ログイン**をクリックします。下記画像に示すように：

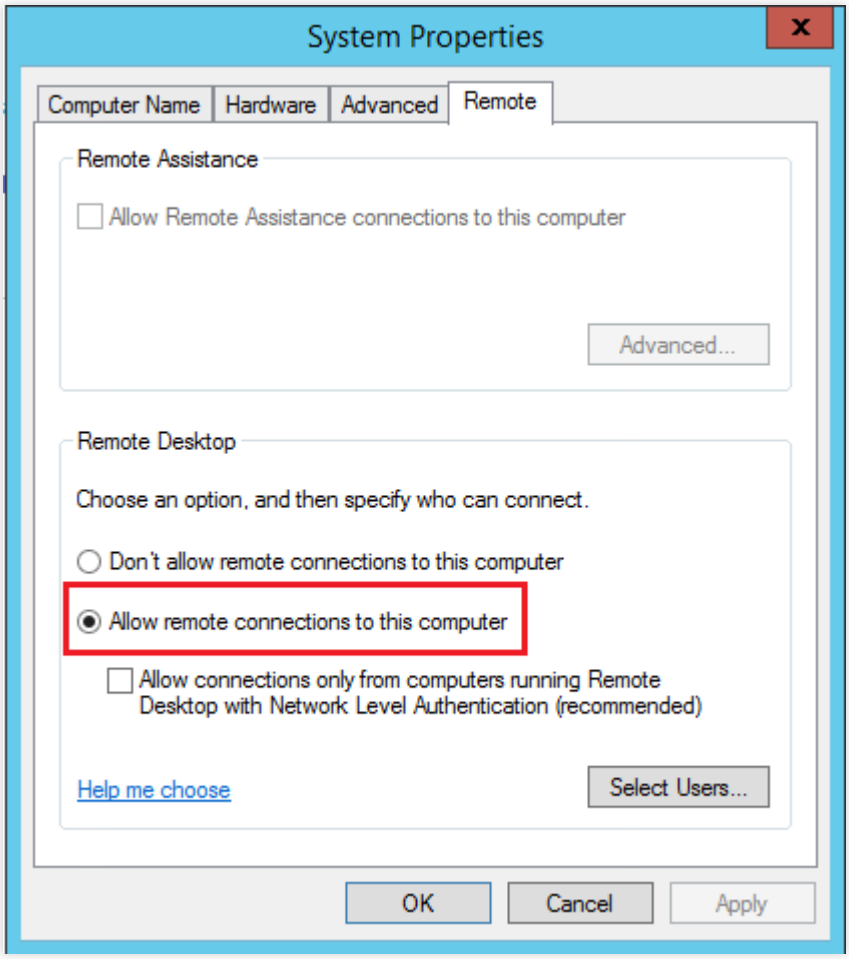


3. ポップアップした「Windowsインスタンスにログインする」ウィンドウで、**その他の方式(VNC）**を選択し、**すぐにログインする**をクリックします。
4. ポップアップしたログインウィンドウで、左上隅にある「Sent CtrlAltDe」を選択し、**Ctrl-Alt-Delete** をクリックすると、システムログイン画面に入ります。下図の通りです。



CVMのリモートデスクトップ設定が有効になっているかどうかを確認する

1. CVMで、**PC>プロパティ**を右クリックして、「システム」ウィンドウを開きます。
2. 「システム」ウィンドウで、**システムの詳細設定**を選択して、「システムのプロパティ」ウィンドウを開きます。
3. 「システムのプロパティ」ウィンドウで、**リモート**タブを選択して、「リモートデスクトップ」機能欄の**このコンピューターへのリモート接続を許可する**をチェックしているかどうかを確認します。下記画像に示すのように：



はい、リモート接続設定が有効になっています。リモートアクセスポートが開いているかどうかを確認 してください。

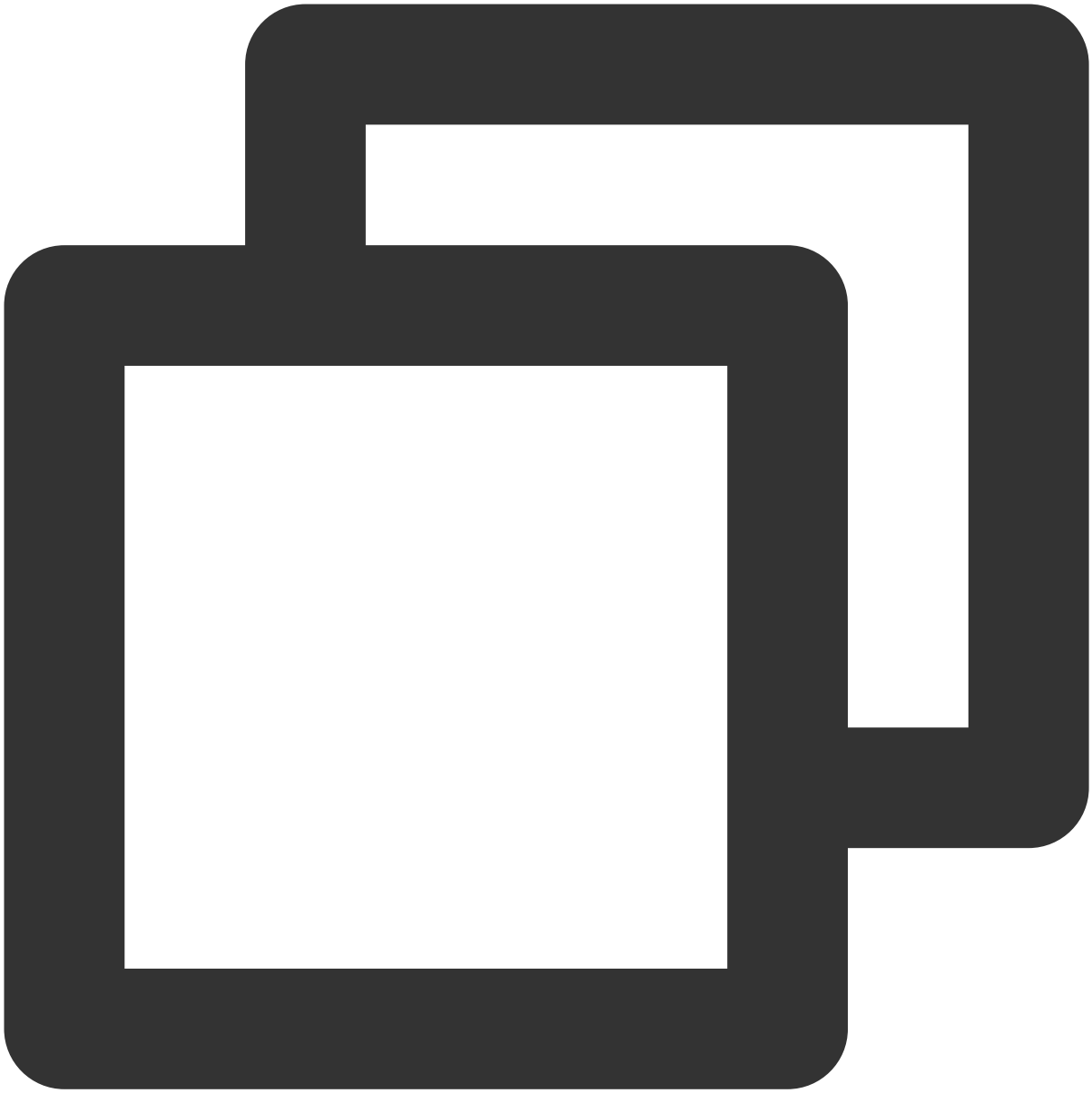
いいえ、**このコンピューターへのリモート接続を許可する**をチェックし、もう一度インスタンスにリモート接続して、接続が成功したかどうかを確認します。

リモートアクセスポートが開いているかどうかを確認する

1. CVMで、

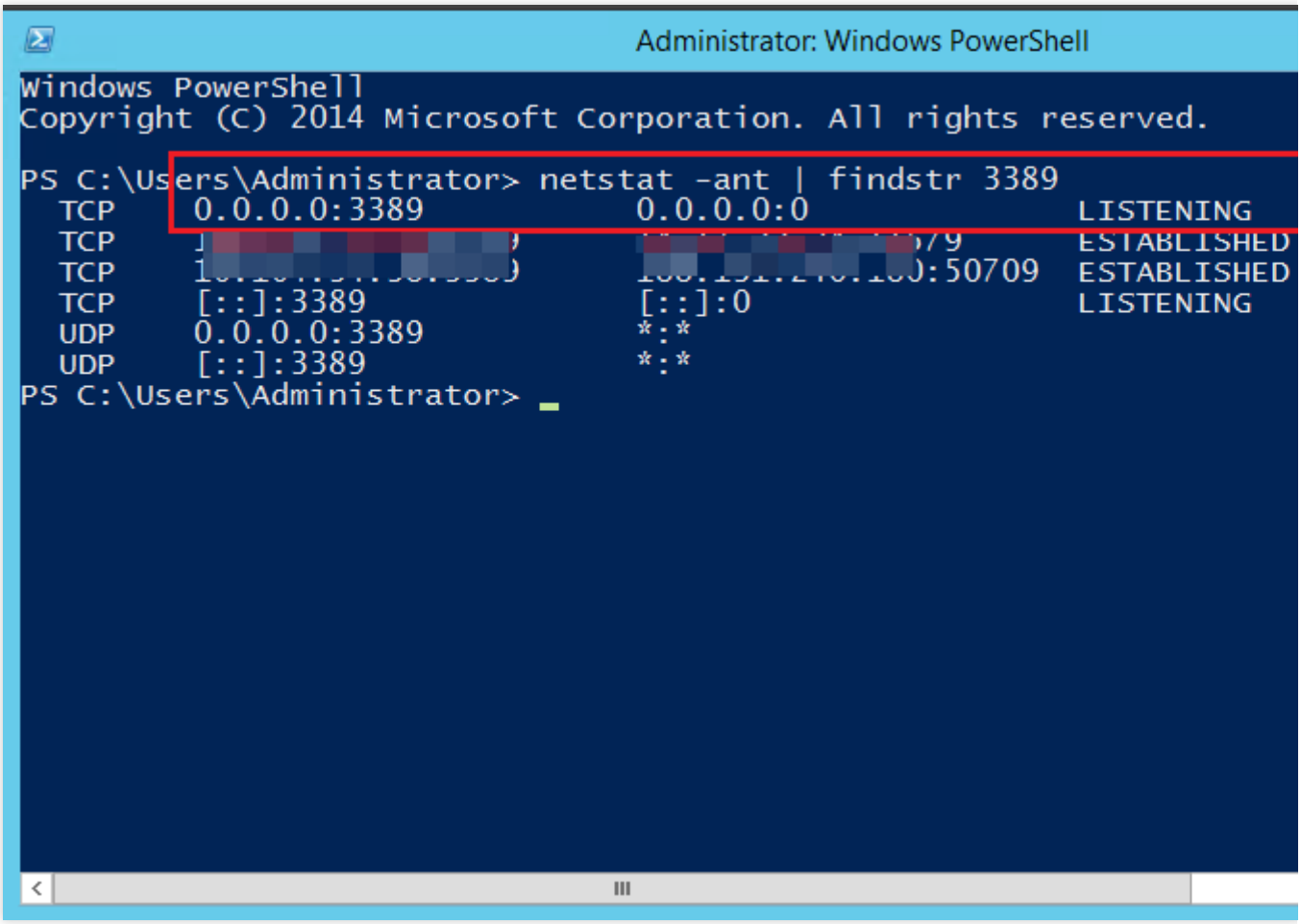
をクリックして、「Windows PowerShell」ウインドウを開きます。

2. 「Windows PowerShell」ウィンドウで、以下のコマンドを実行し、リモートデスクトップの運行状態を確認します（デフォルトでは、リモートデスクトップサービスのポート番号が3389です）。



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

以下のような結果が返されたら、正常状態であることを示します。リモートデスクトップを再起動 してください。もう一度インスタンスにリモート接続して、接続が成功したかどうかを確認できます。



接続が表示されない場合は、異常状態であることを示し、レジストリのリモートポートが一致するかどうかを確認してください。

レジストリのリモートポートが一致するかどうかを確認する

ご注意：

このステップでは、 **TCP PortNumber**と **RDP Tcp PortNumer** が同じであるかどうかを確認します。

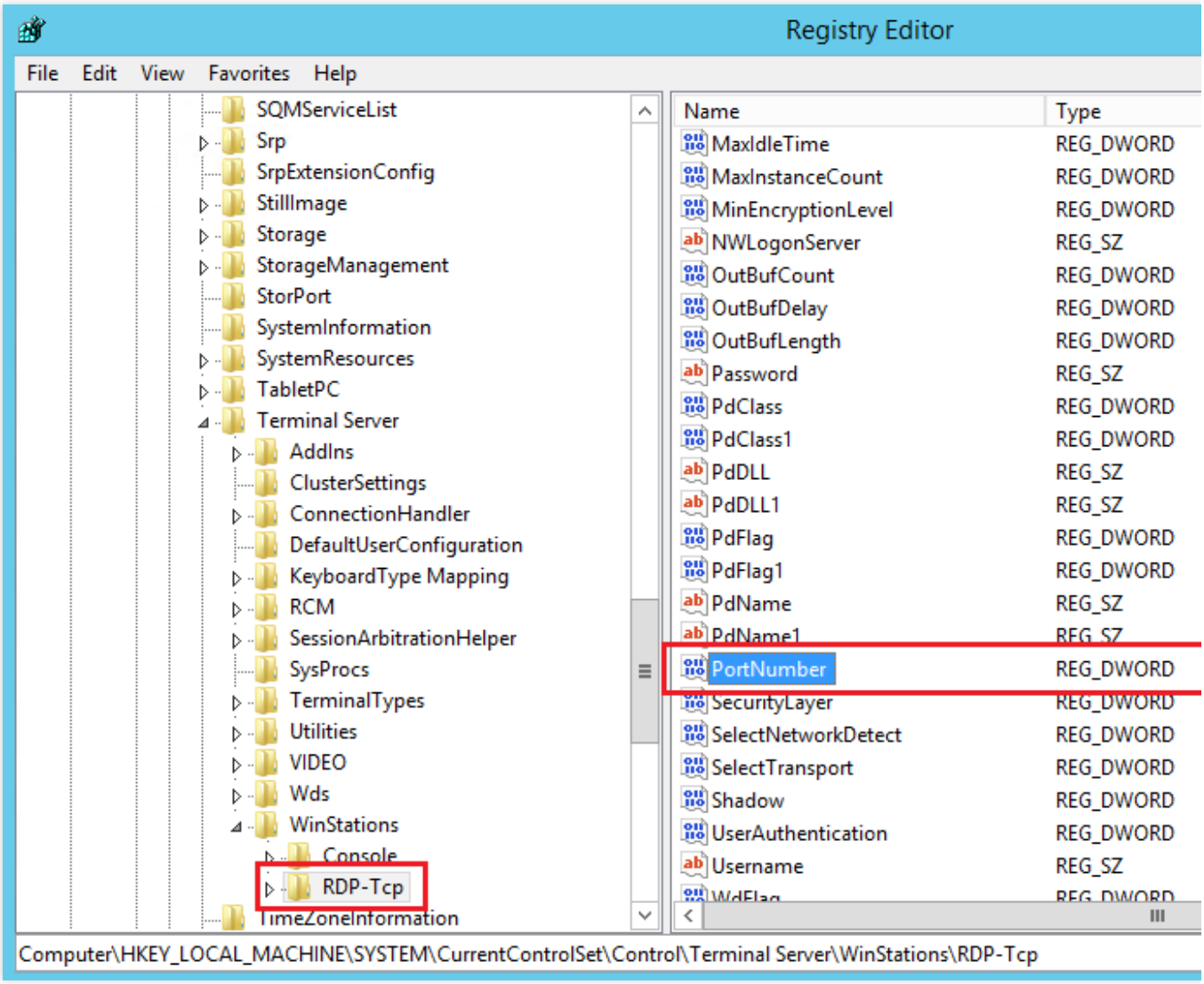
1. CVMで、

をクリックし、

を選択して、 **regedit**を入力して、**Enter**キーを押して、「レジストリエディター」ウィンドウを開きます。

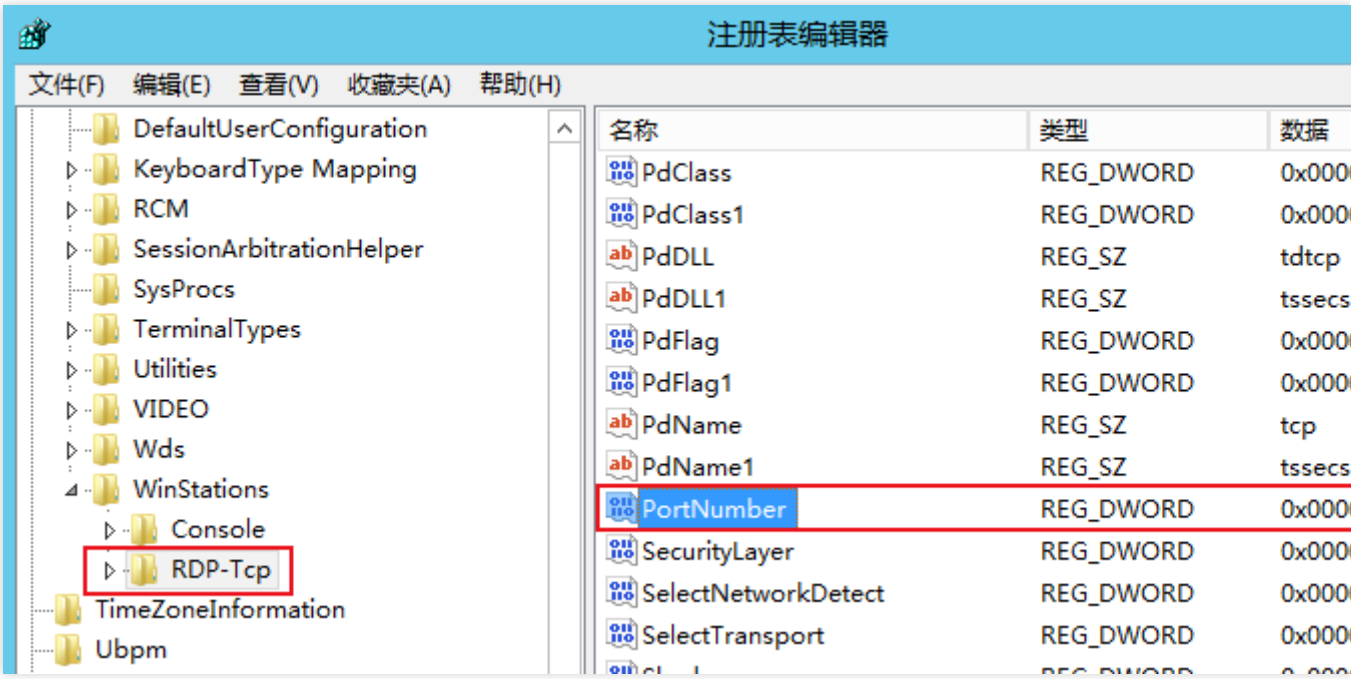
2. 左側のレジストリナビゲーションで、**HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Control** > **Terminal Server** > **Wds** > **rdpwd** > **Tds** > **tcp**の順でディレクトリを展開します。

3. **tcp**でPortNumberを見つけて、PortNumberデータ（ポート番号、デフォルトが3389）を記入します。下記画像に示すように：



4. 左側のレジストリナビゲーションで、**HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Control** > **Terminal Server** > **WinStations** > **RDP-Tcp**の順でディレクトリを展開します。

5. **RDP-Tcp**でPortNumberを見つけて、**RDP-Tcp**中のPortNumberデータ（ポート番号）が**tcp**中のPortNumberデータ（ポート番号）と同じかどうかを確認します。下記の画像に示すように：



同じでない場合、ステップ 6 を実行してください。

同じ場合は、リモートログインサービスを再起動 してください。

6.**RDP-Tcp**中のPortNumberをダブルクリックします。

6. ポップアップしたダイアログボックスで、「値データ」を0 - 65535の間で未使用ポートに変更して、**TCP PortNumber**と**RDP Tcp PortNumer**のポート番号を一致させて、**OK**クリックします。

7. 変更後、CVMコンソール でインスタンスを再起動します。もう一度インスタンスにリモート接続して、接続が成功したかどうかを確認します。

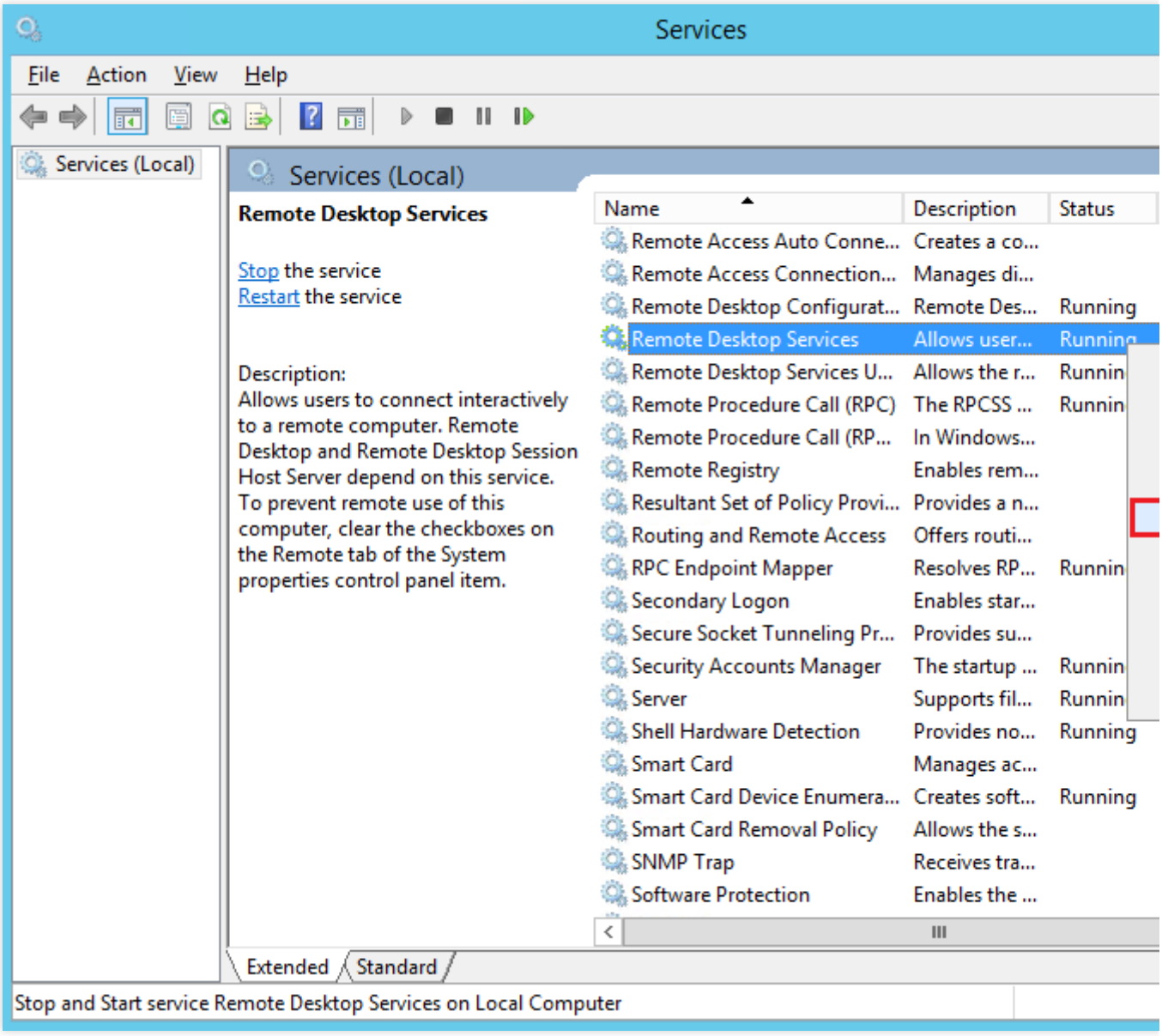
リモートログインサービスを再起動する

1. CVMの中で、

をクリックし、

を選択して、 **services.msc**を入力して、**Enter**キーを押して、「サービス」ウィンドウを開きます。

2. 「サービス」ウィンドウで、**リモートデスクトップサービス**を見つけて右クリックします。**再開**を選択して、リモートログインサービスを再起動します。下記の画像に示すように：



その他の操作

上記操作を行ってもリモートでログインできない場合は、 チケットを送信 してフィードバックしてください。

Linuxインスタンス関連
Linuxインスタンス登録失敗

最終更新日：：2023-04-21 14:51:10

このドキュメントでは主にLinuxインスタンスが接続できない場合のトラブルシューティング方法と、Linuxインスタンスに接続できない主な原因について解説し、問題のトラブルシューティング、特定および解決について説明します。

問題の特定

自己診断ツールの使用

Tencent Cloudは、帯域幅、ファイアウォールおよびセキュリティグループの設定などの一般的な問題が原因であるかどうかを判断するのに役立つ自己診断ツールを提供しています。 障害の70%はツールで特定でき、検出された問題をもとにログインできない原因となっている可能性のある障害を特定できます。
1. セルフチェック をクリックし 、自己診断ツールを開きます。
2. ツールインターフェースのプロンプトに基づき、診断したいCVMを選択し、**検出開始**をクリックします。

自動化アシスタントを使用してコマンドを送信

自動化アシスタントを使用してインスタンスにコマンドを送信し、トラブルシューティングと問題の特定を行うことができます。使用手順は次のとおりです。
1. CVMコンソール にログインし、インスタンスリストでインスタンスIDをクリックします。
2. インスタンス詳細ページで**コマンドの実行**タブを選択し、**コマンドの実行**をクリックします。
3. ポップアップした「コマンドの実行」ウィンドウで、必要に応じてコマンドを選択し、**コマンドの実行**をクリックすると、コマンドを実行してその結果を確認することができます。
例えば、新コマンド `df -TH` を入力して**コマンドの実行**をクリックすると、インスタンスにログインせずに結果を確認することができます
自動化アシスタントについてより詳しい情報をお知りになりたい場合は、自動化アシスタント をご参照ください。
説明：
トラブルシューティングツールによって確認できない問題については、CVMに VNC方式でログイン し、段階ごとにトラブルシューティングを実施することをお勧めします。

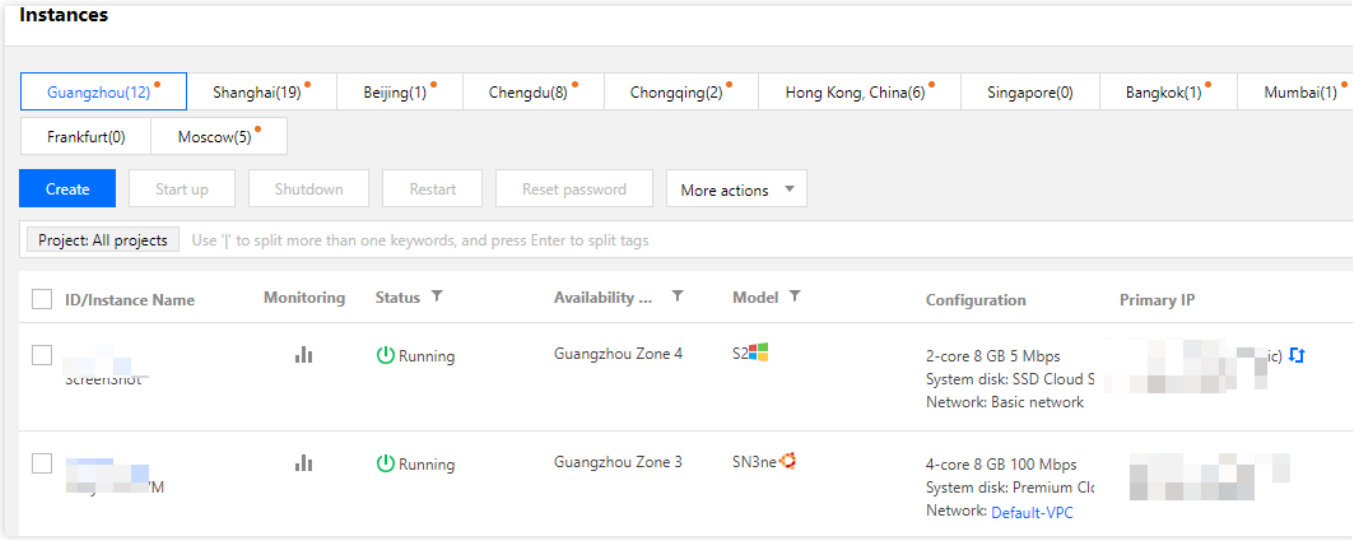
考えられる原因

Linuxインスタンスにログインできない主な原因：
SSHの問題によりログインできない
パスワードの問題によりログインできない
帯域幅利用率が高すぎる
サーバー負荷が高い
セキュリティグループルールが不適切

障害処理

VNC 方式を介したログイン

標準の方法（Orcaterm）または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できない場合は、Tencent Cloud VNCを介してログインし、障害の原因を特定できます。
1. CVMコンソール にログインします。
2. 下図のように、インスタンスの管理画面で、ログインしたいインスタンスを選択し、**ログイン**をクリックします。



3. ポップアップした「標準ログイン | Linuxインスタンス」ウィンドウで、**VNCログイン**を選択します。
説明：
ログイン中に、パスワードを忘れた場合は、コンソールでこのインスタンスのパスワードをリセットできます。具体的な操作については、インスタンスのパスワードをリセット ドキュメントをご参照ください。
4. ユーザー名とパスワードを入力してログインします。

SSH問題によりログインできない

障害事象：SSHを使用してLinuxインスタンスにログイン した場合に、「接続できません」または「接続に失敗しました」と表示される。

処理手順：SSH方式を介してLinuxインスタンスにログインできない ドキュメントを参照してトラブルシューティングを行います。

パスワードの問題によりログインできない

障害事象：パスワードの入力ミス、パスワードを忘れた、パスワードのリセットに失敗したなどの理由で正常にログインできない。
対処方法：Tencent Cloudコンソール でこのインスタンスのパスワードをリセットし、インスタンスを再起動してください。
処理手順：インスタンスのパスワードをリセットする方法については、インスタンスのパスワードをリセット ドキュメントをご参照ください。

帯域幅利用率が高すぎる

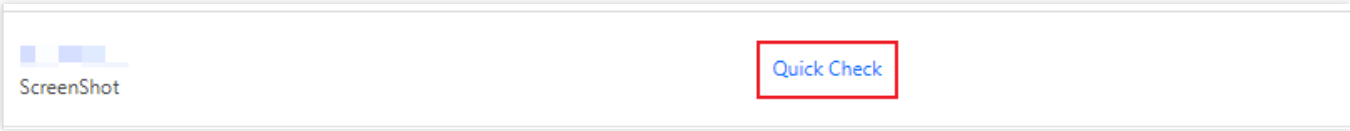
障害事象：自己診断ツールによって、帯域幅利用率が高すぎることが問題だと表示された。
処理手順：
1. VNCログイン によってインスタンスにログインします。
2. 帯域幅の利用率が高いためログインできない ドキュメントを参照し、インスタンスの帯域幅使用状況および障害の処理について確認します。

サーバー負荷が高い

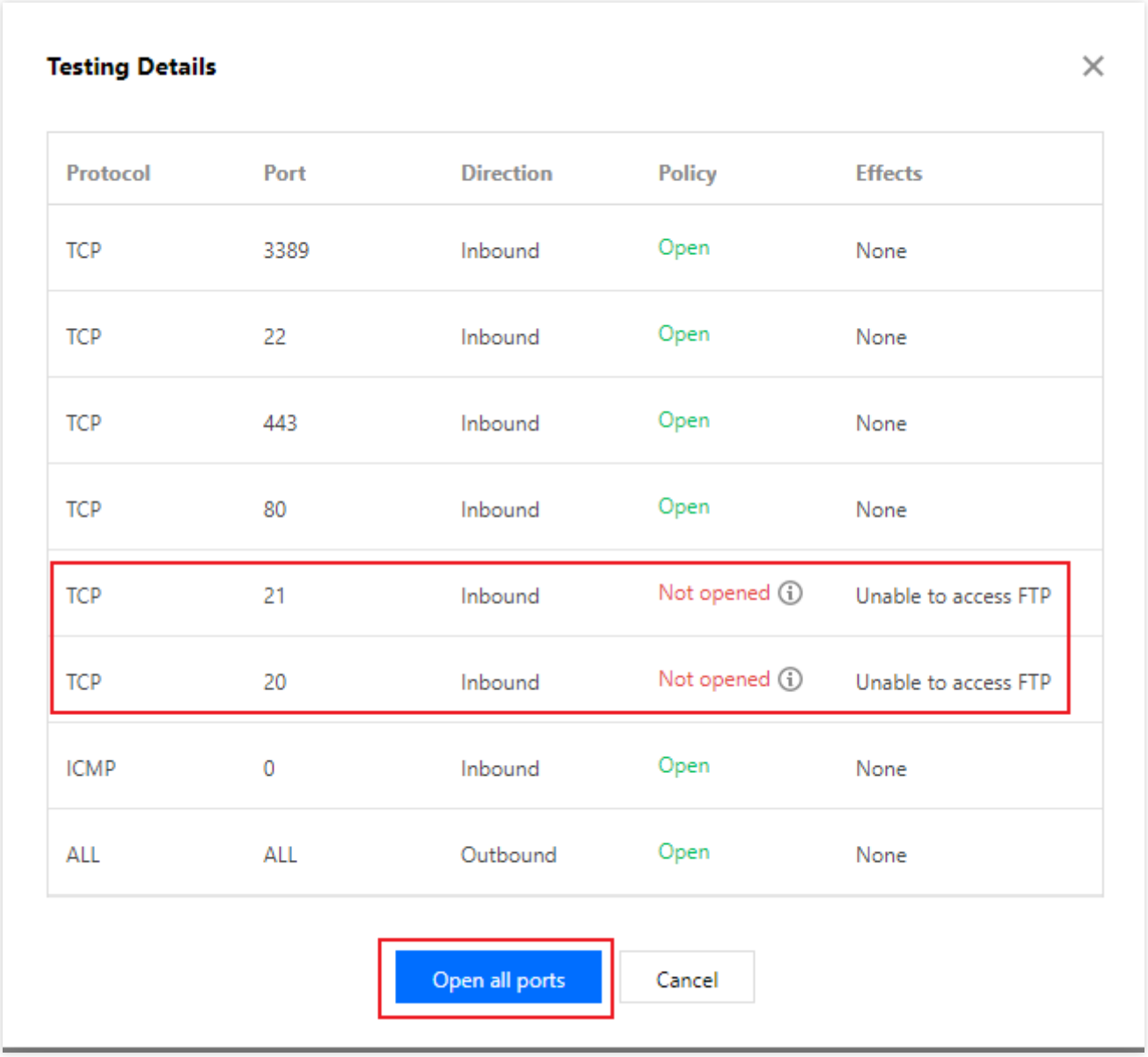
障害事象：セルフチェックツールまたはTCOPによって、サーバーのCPU負荷が高いためにシステムがリモート接続できなくなっている、またはアクセスが非常に遅くなっていると表示された。
考えられる原因：ウイルスやトロイの木馬、サードパーティ製のウイルス対策ソフト、アプリケーションプログラムの異常、ドライバーの異常、またはソフトウェアのバックエンドでの自動更新によってCPU占有率が高くなり、CVMにログインできない、またはアクセスが遅いといった問題が発生している。
処理手順：
1. VNCログイン によってインスタンスにログインします。
2. Linuxインスタンス：CPUとメモリ占用率が高いため、ログインできない ドキュメントを参照し、「タスクマネージャー」で負荷の高いプロセスを特定します。

セキュリティグループルールが不適切

障害事象：セルフチェックツールでのチェックの結果、セキュリティグループルールが不適切なためにログインできないことがわかった。
処理手順：セキュリティグループ（ポート）検証ツール によってチェックを行います。



セキュリティグループポート設定の問題であると判断された場合は、ツールの**ワンクリック開放**機能を使用してポートを開放できます。



セキュリティグループルールのカスタム設定を行いたい場合は、セキュリティグループルールの追加 ドキュメントをご参照の上、セキュリティグループルールを再設定してください。

その他ソリューション

上述のトラブルシューティングを行っても、Linuxインスタンスに接続できない場合は、セルフチェック結果を保存し、チケットを提出してフィードバックしてください。

LinuxインスタンスをSSHで登録できない

最終更新日：：2021-10-27 17:33:36

説明：
この文章はコミュニティから寄せられたものであり、参考までにご提供します。Tencent Cloud関連製品とは関係がありません。
ここに記載された関連のファイル操作は、必ず慎重に実行してください。必要に応じて、スナップショット作成などの方法でデータバックアップを行うことができます。

現象の説明

SSHを使用してLinuxインスタンスにログイン を行った際、「接続できません」または「接続に失敗しました」と表示され、Linuxインスタンスに正常にログインできません。

問題の特定および処理

SSHを使用したLinuxインスタンスへのログインが失敗し、エラー情報が返された場合は、エラー情報を記録し、次のよくあるエラー情報から当てはまるものを探し、迅速に問題を特定して、手順を参照し解決することができます。
SSHログインエラーUser root not allowed because not listed in AllowUsers

問題の原因

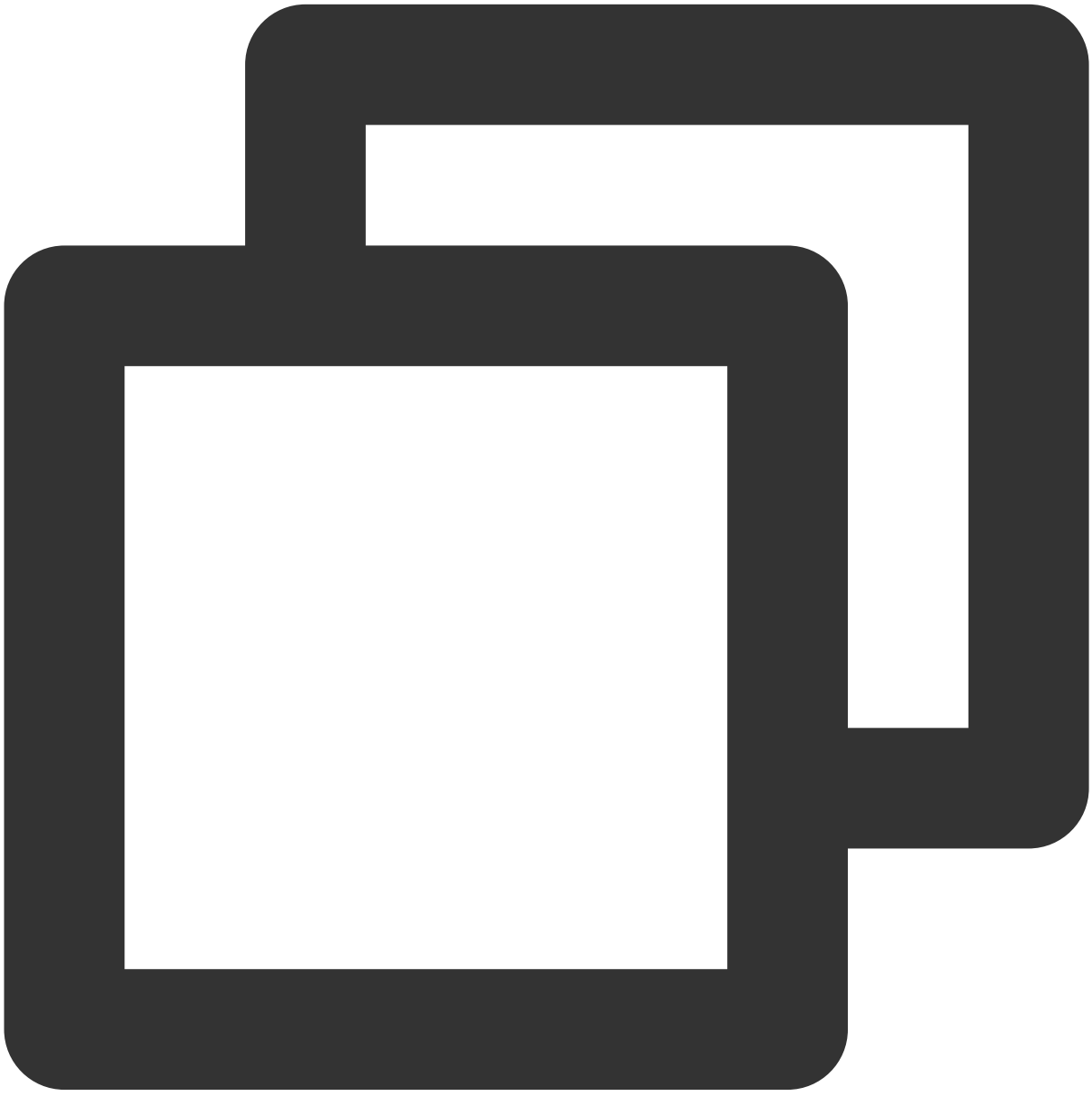
この問題は通常、SSHサービスがユーザーログイン制御パラメータをアクティブにし、ログインユーザーを制限しているために起こります。パラメータの説明は次のとおりです。
AllowUsers：ログインが許可されているユーザーのホワイトリストであり、このパラメータが記述されているユーザーのみログインできます。
DenyUsers：ログインが拒否されているユーザーのブラックリストであり、このパラメータが記述されているユーザーはすべてログインが拒否されます。
AllowGroups：ログインが許可されているユーザーグループのホワイトリストであり、このパラメータが記述されているユーザーグループのみログインできます。
DenyGroups：ログインが拒否されているユーザーグループのブラックリストであり、このパラメータが記述されているユーザーグループはすべてログインが拒否されます。
説明：
拒否ポリシーの優先順位は許可ポリシーより上になります。

解決方法

1. 処理手順 を参照し、SSHで設定した `sshd_config` ファイルに進み、 設定を確認します。
2. ユーザーログイン制御パラメータを削除し、SSHサービスを再起動すれば完了です。

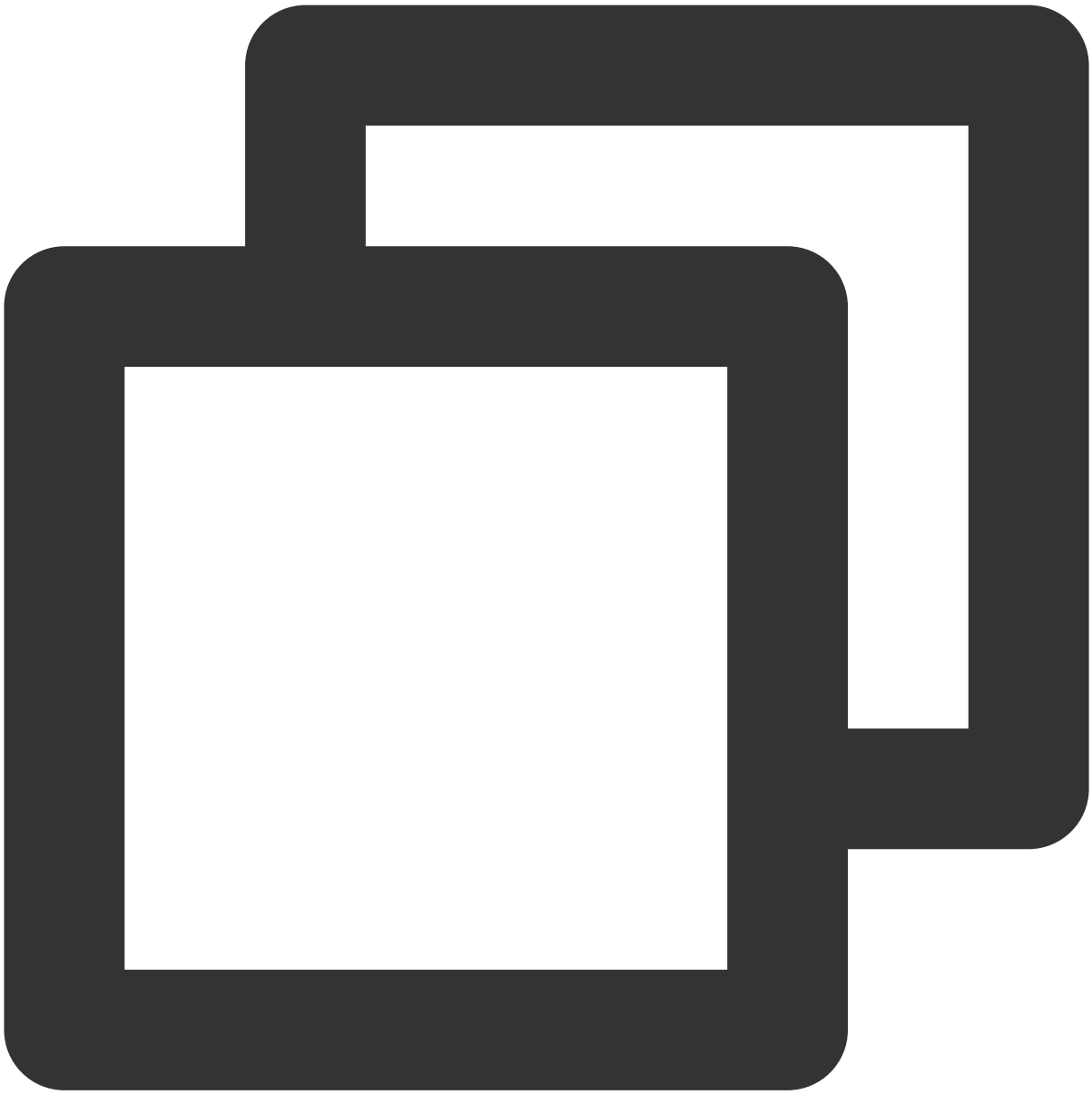
処理手順

1. VNC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、VIMエディタを使用して `sshd_config` 設定ファイルに進みます。



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

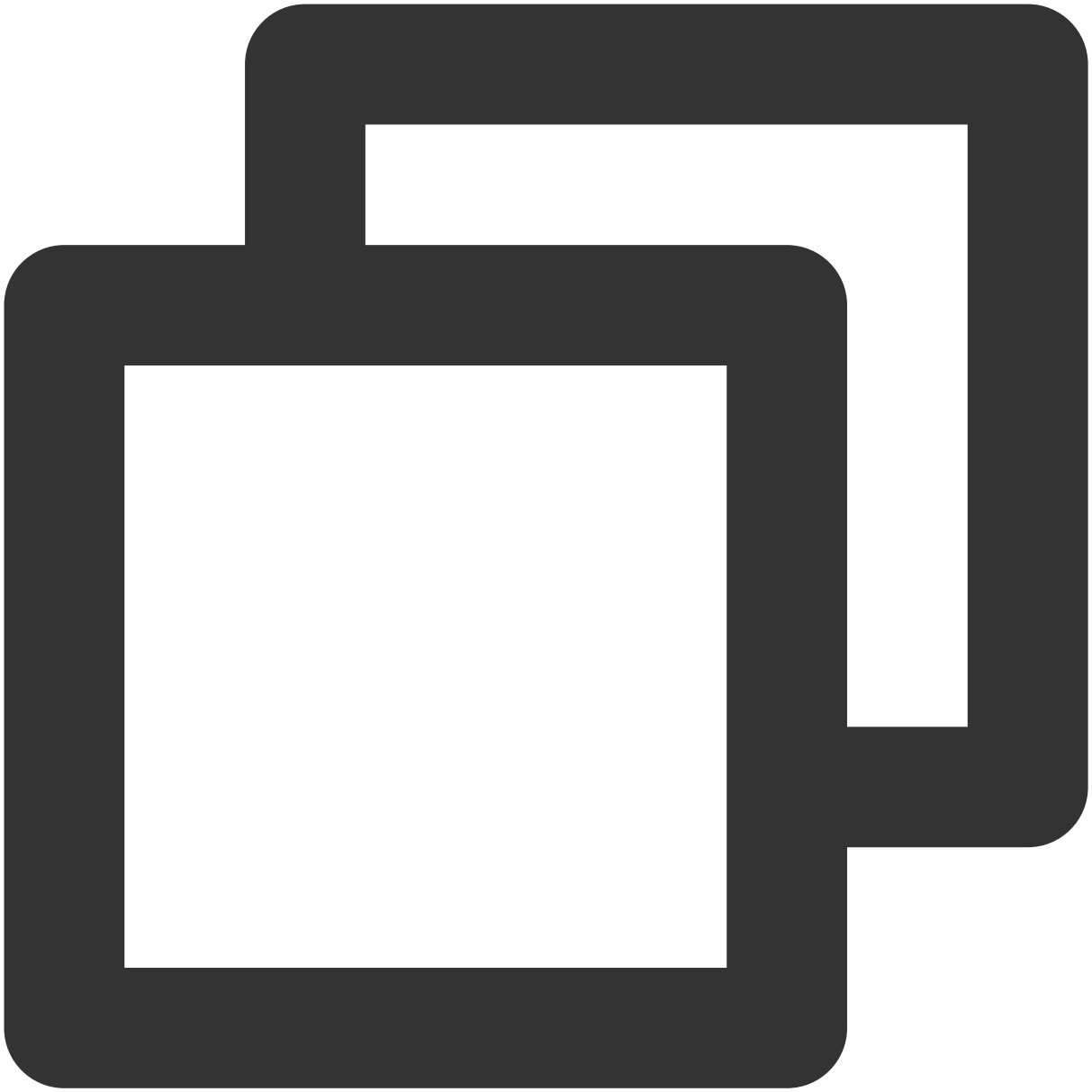
3. **i**を押して編集モードに入り、以下の設定を探して削除するか、または各行の先頭に `#` を追加してコメントします。



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

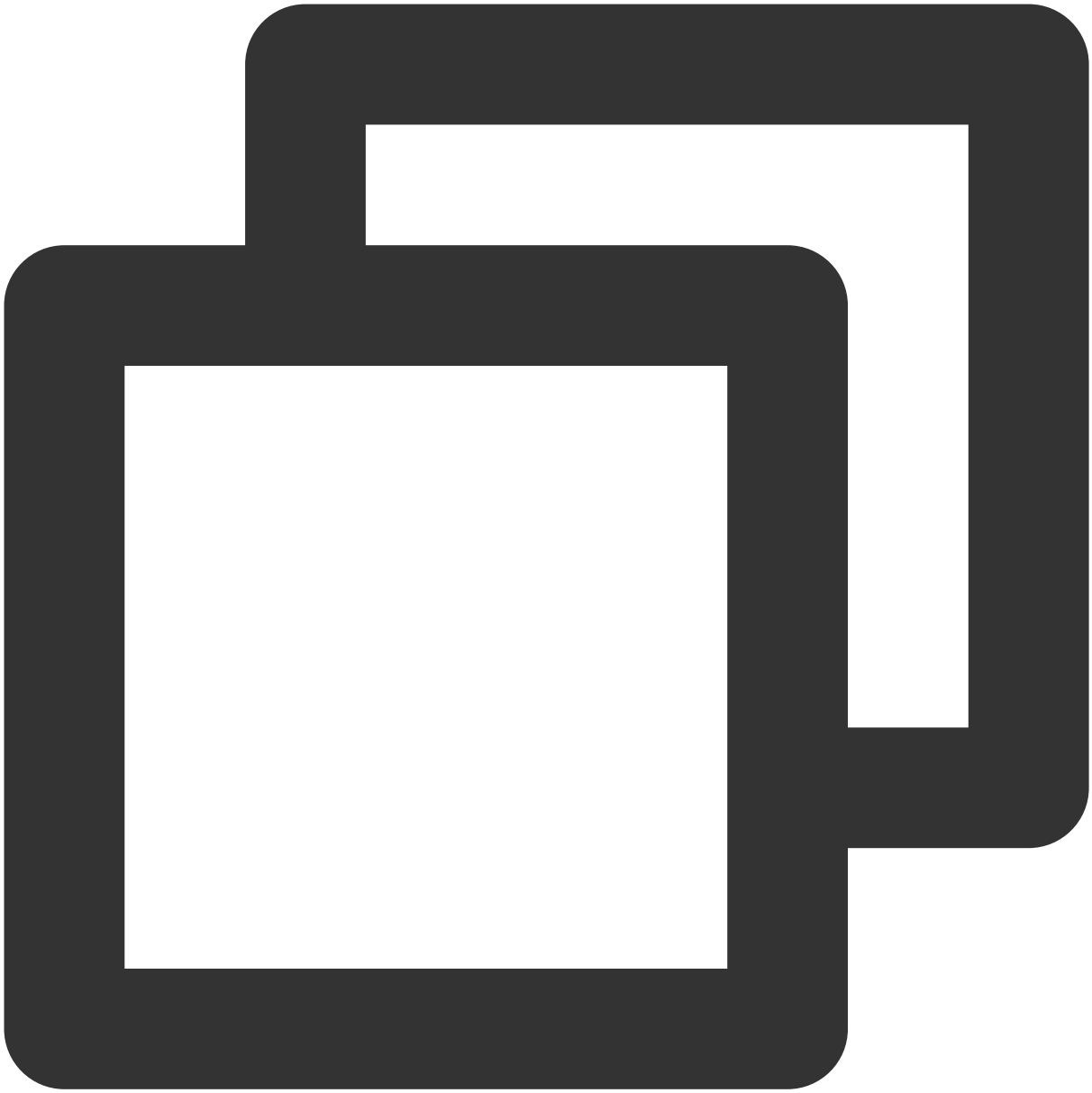
4. **Esc**を押して編集モードを終了し、**:wq**を入力して変更を保存します。
5. 実際に使用するOSに応じて以下のコマンドを実行し、SSHサービスを再起動します。

CentOS



```
systemctl restart sshd.service
```

Ubuntu



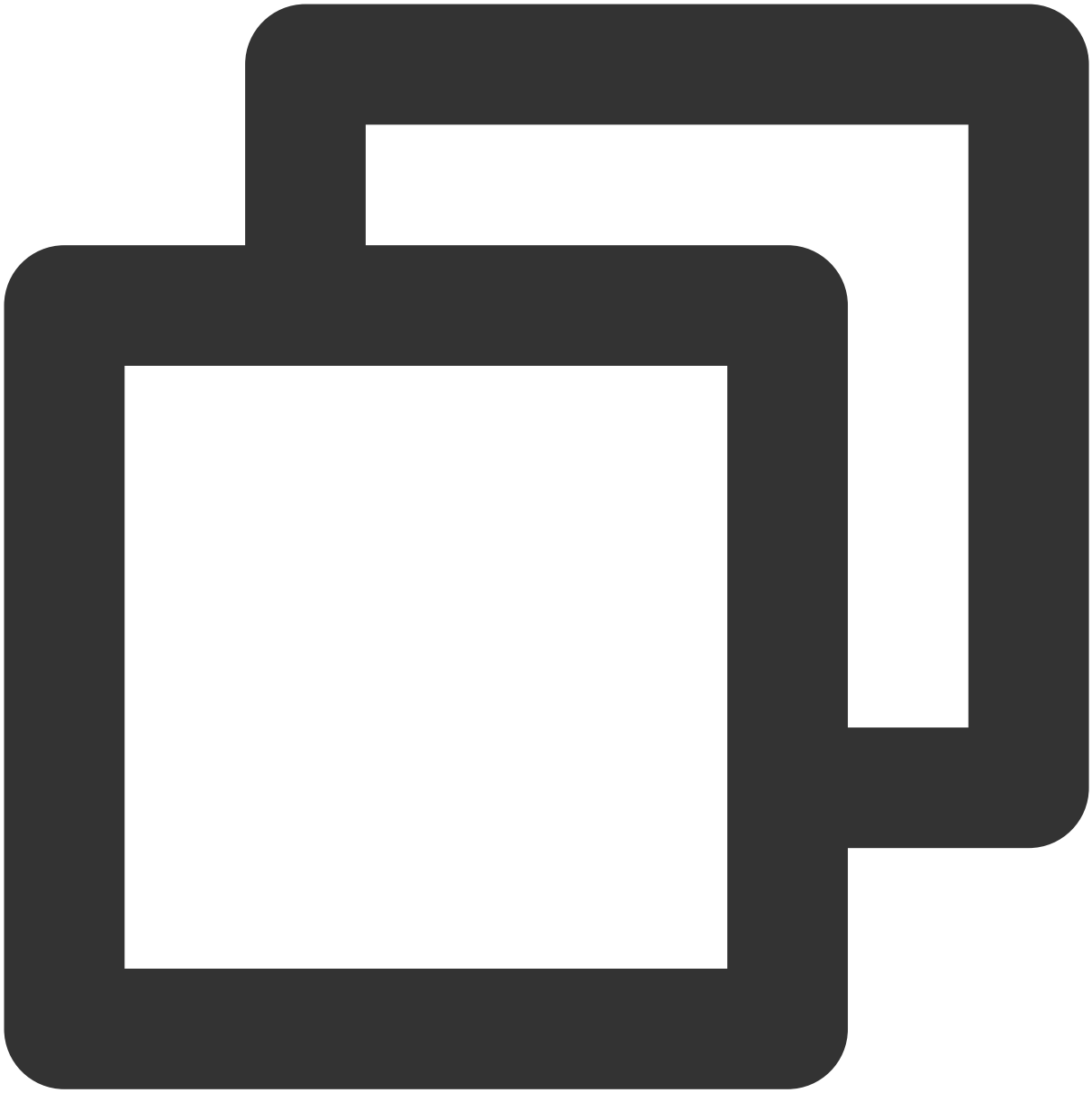
```
service sshd restart
```

SSHサービスを再起動すると、SSHを使用してログインできるようになります。詳細については SSH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。

SSHログインエラーDisconnected:No supported authentication methods available

現象の説明

SSHを使用してログインする際に、次のエラー情報が表示されます。



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

問題の原因

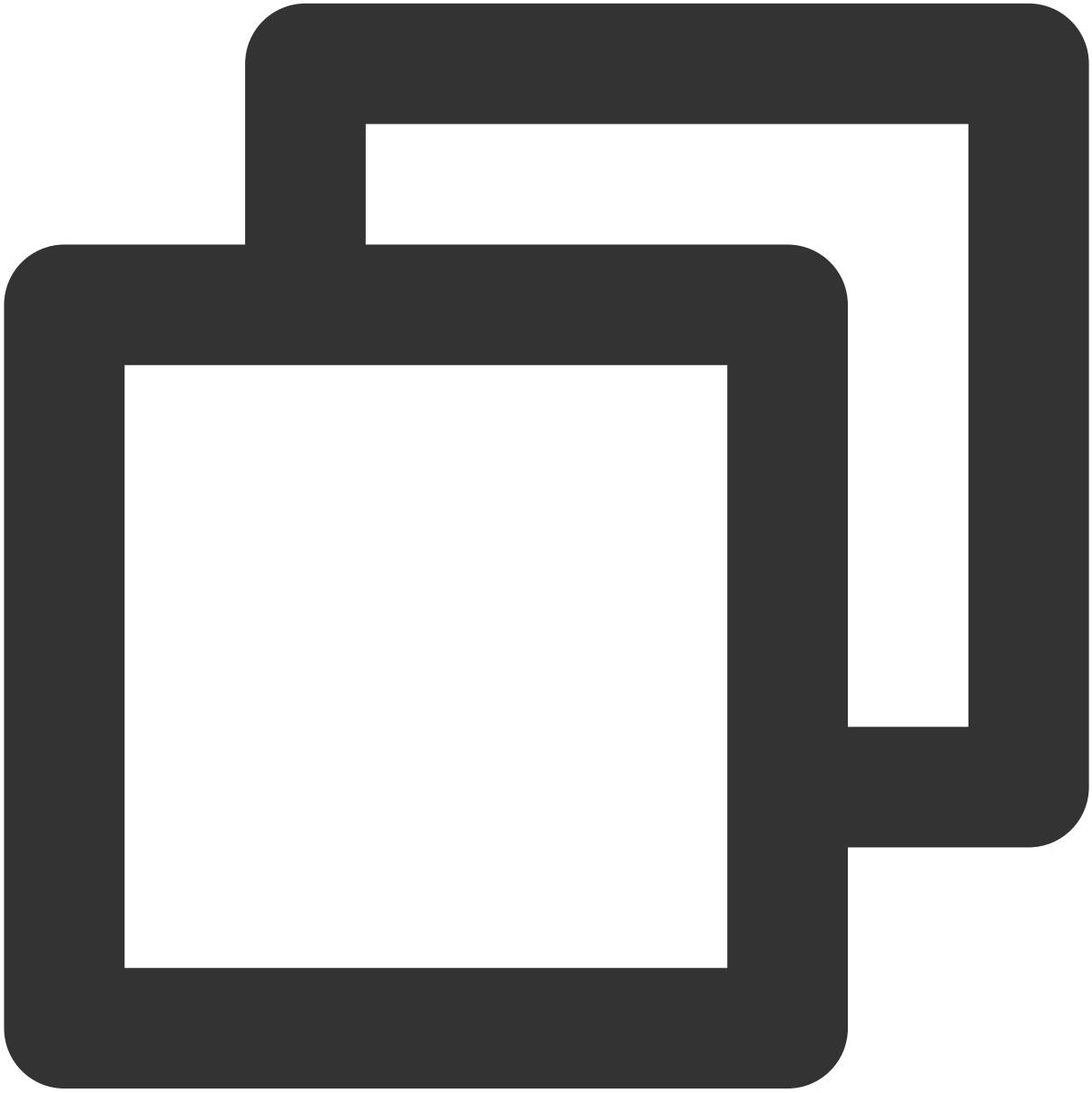
SSHサービスによって `PasswordAuthentication` パラメータが変更され、パスワード認証ログインが無効になったことが原因です。

解決方法

1. 処理手順 を参照し、SSHで設定した `sshd_config` ファイルに進みます。
2. `PasswordAuthentication` パラメータを変更し、SSHサービスを再起動すれば完了です。

処理手順

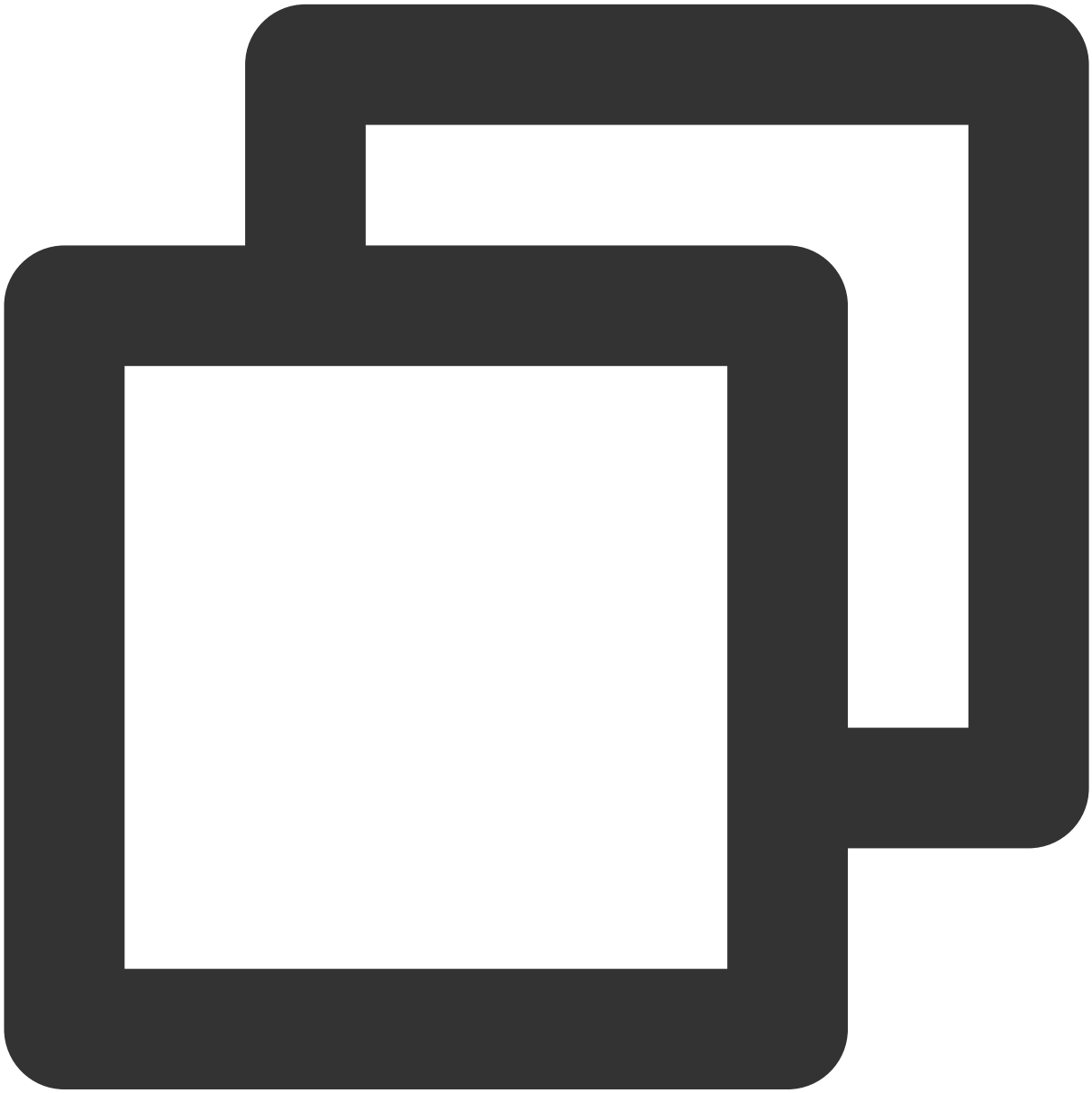
1. VNCを使用してLinuxインスタンスにログイン します。
2. 以下のコマンドを実行し、VIMエディタを使用して `sshd_config` 設定ファイルに進みます。



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

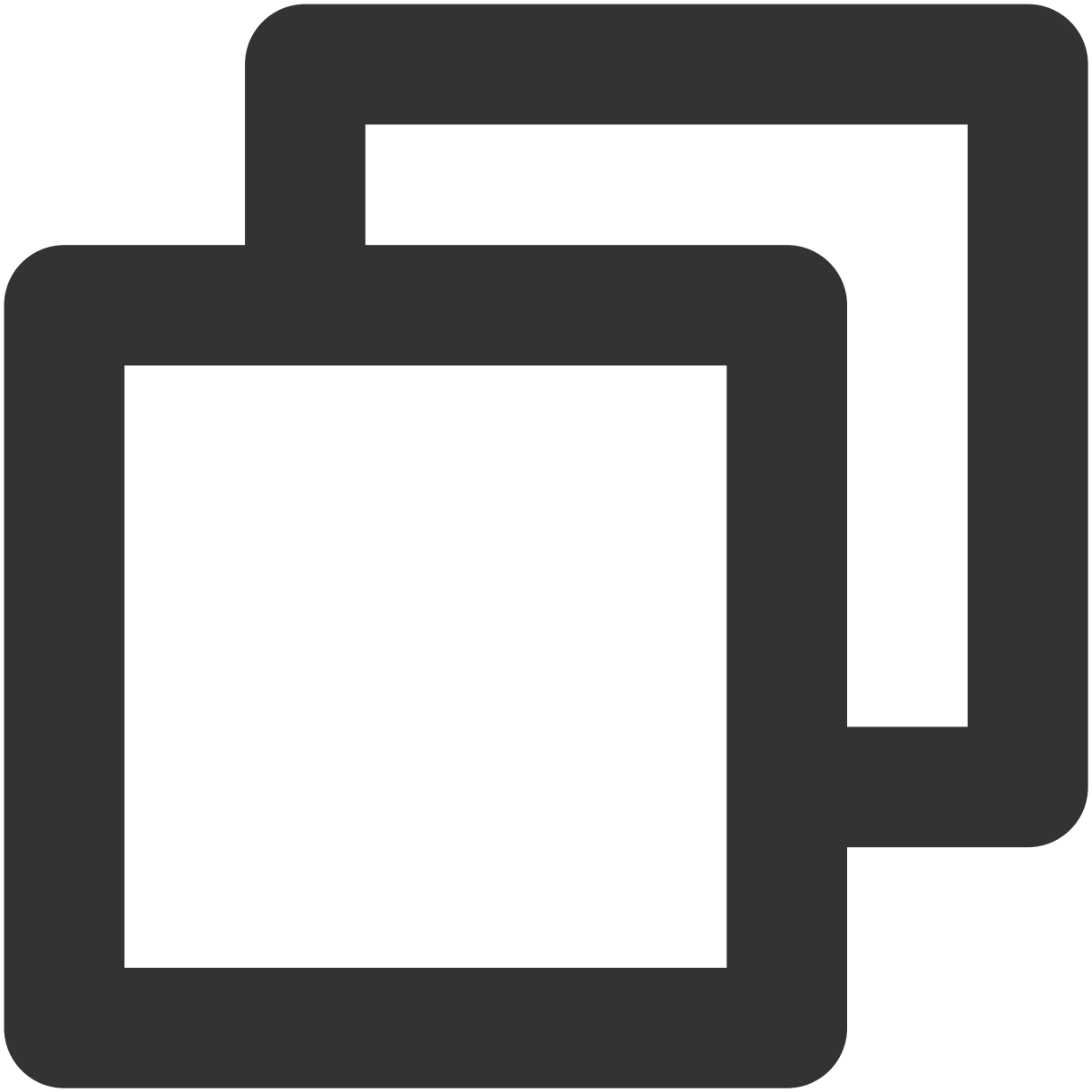
3. **i**を押して編集モードに入り、 `PasswordAuthentication no` を `PasswordAuthentication yes` に変更します。
4. **Esc**を押して編集モードを終了し、**:wq**を入力して変更を保存します。
5. 実際に使用するOSに応じて以下のコマンドを実行し、SSHサービスを再起動します。

CentOS



```
systemctl restart sshd.service
```

Ubuntu



```
service sshd restart
```

SSHサービスを再起動すると、SSHを使用してログインできるようになります。詳細については SSH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。

SSHログインエラーssh_exchange_identification: read: Connection reset by peer

現象の説明

SSHを使用してログインする際に、エラー情報「ssh_exchange_identification: read: Connection reset by peer」が表示されます。もしくは次のエラー情報が表示されます。

"ssh_exchange_identification: Connection closed by remote host"
"kex_exchange_identification: read: Connection reset by peer"
"kex_exchange_identification: Connection closed by remote host"

問題の原因

このタイプの問題が発生する原因は多くありますが、よくある原因は次の数種類です。
ローカルアクセス制御によって接続が制限されている
Fail2banやdenyhostなど、何らかの侵入防止ソフトウェアによってファイアウォールルールが変更された
sshd設定で最大接続数が制限されている
ローカルネットワークに問題がある

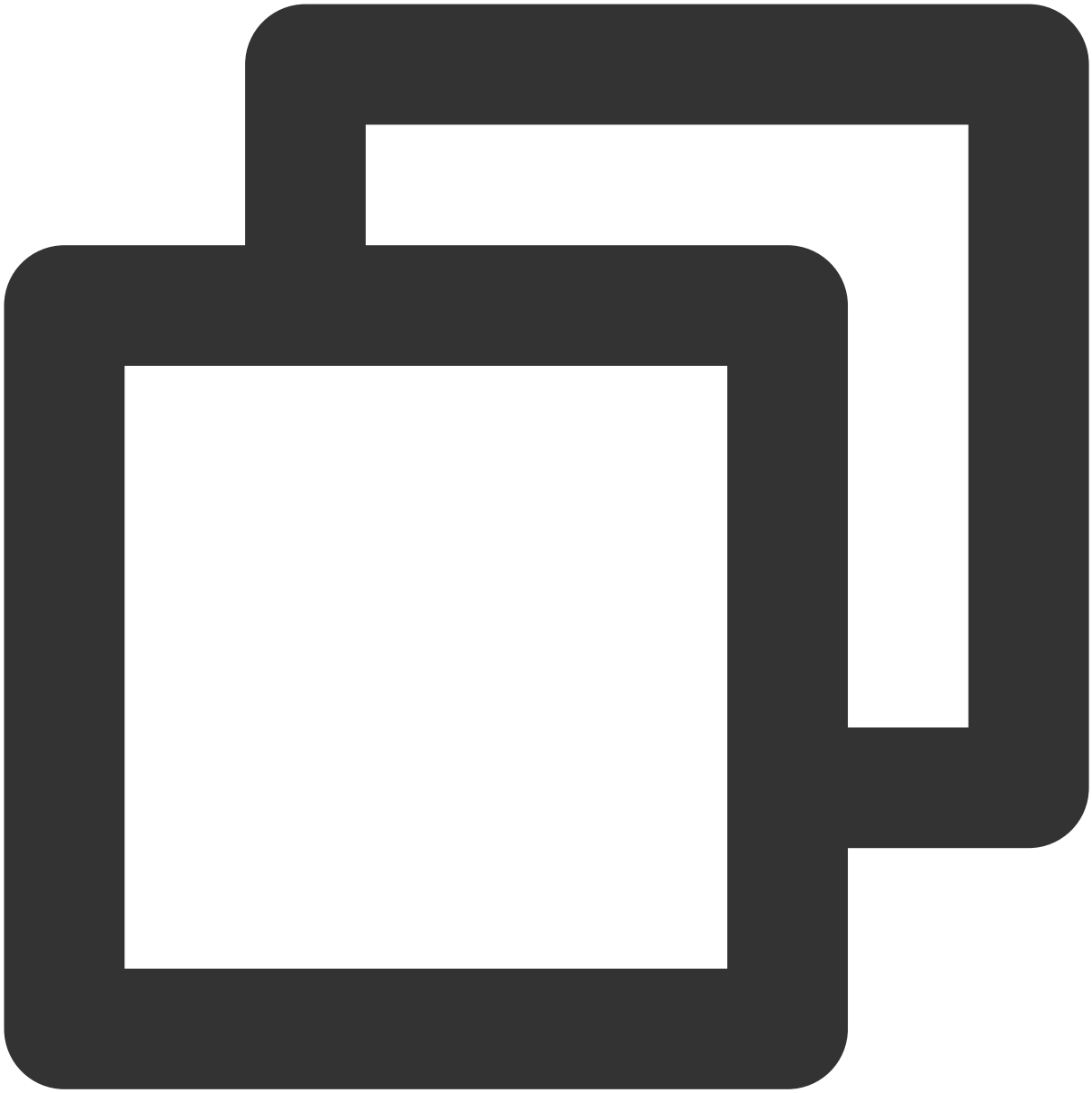
解決方法

処理手順 を参照し、アクセスポリシー、ファイアウォールルール、sshd設定、ネットワーク環境などいくつかの面から問題を特定し、解決します。

処理手順

アクセスポリシー設定の確認と調整

Linuxでは `/etc/hosts.allow` および `/etc/hosts.deny` ファイルによってアクセスポリシーを設定することができ、2つのファイルはそれぞれ許可ポリシーと拒否ポリシーに対応しています。例えば、 `hosts.allow` ファイルでホスト信頼ルールを設定し、 `hosts.deny` ファイルでその他のすべてのホストを拒否することができます。 `hosts.deny` を例にとると、拒否ポリシーの設定は次のようになります。



```
in.sshd:ALL                         # すべてのssh接続を拒否
in.sshd:218.64.87.0/255.255.255.128      # 218.64.87.0--127のsshを拒否
ALL:ALL                             # すべてのTCP接続を拒否
```

VNCを使用してLinuxインスタンスにログイン し、 `/etc/hosts.deny` ファイルおよび `/etc/hosts.allow` ファイルを確認し、確認結果に基づいて次の処理方法を選択してください。

設定に誤りがあった場合は必要に応じて変更してください。変更後すぐに有効になります。

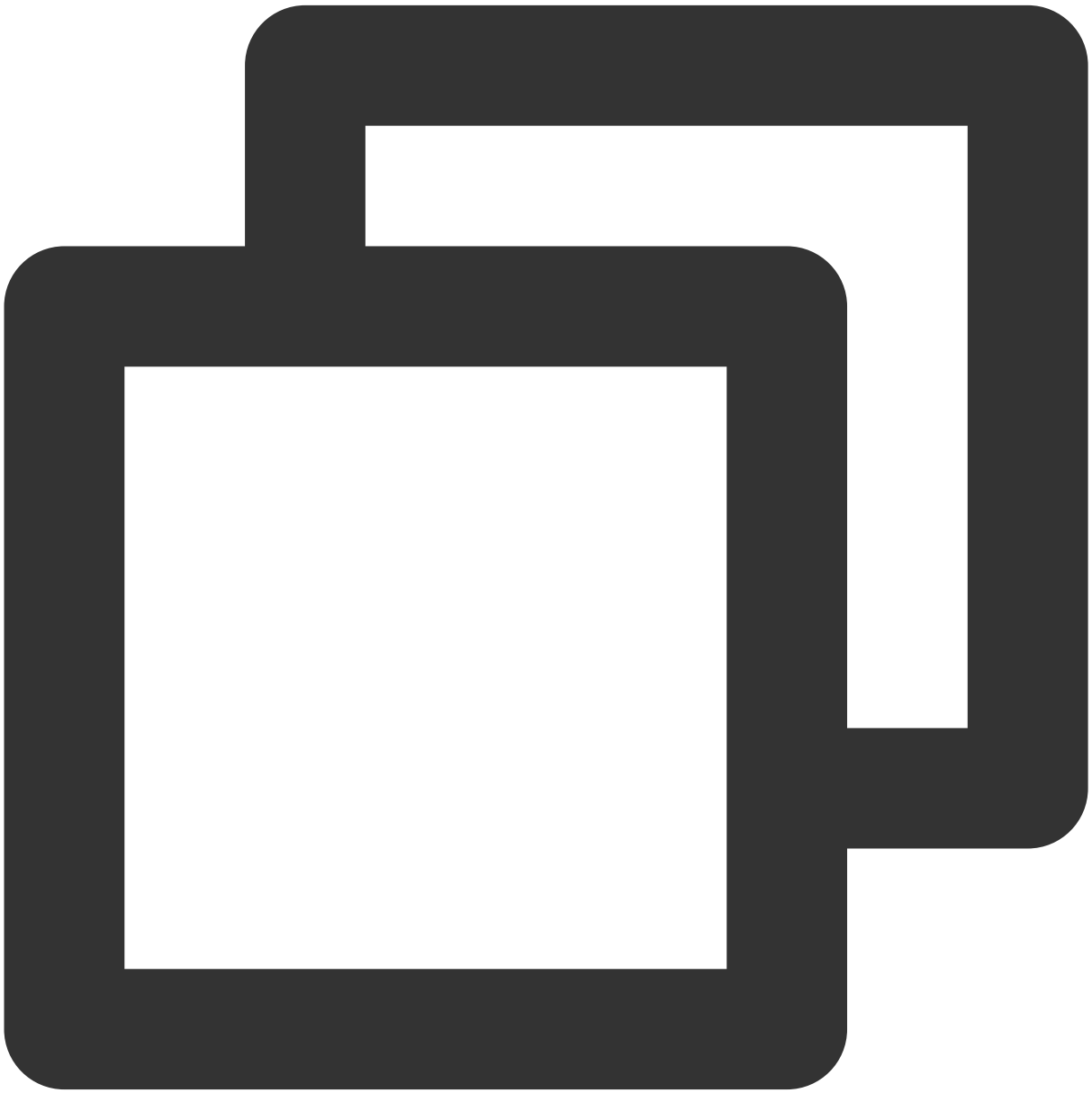
未設定、または設定に誤りがなかった場合は、次の手順に進んでください。

説明：

アクセスポリシーを設定していない場合、デフォルトのファイルはすべてブランクであり、すべての接続が許可されています。

iptablesファイアウォールルールの確認

Fail2banやdenyhostなど、何らかの侵入防止ソフトウェアの使用を含めて、iptablesファイアウォールルールが変更されたかどうかを確認します。以下のコマンドを実行して、ファイアウォールがSSH接続を拒否したことがあるかどうかを確認します。

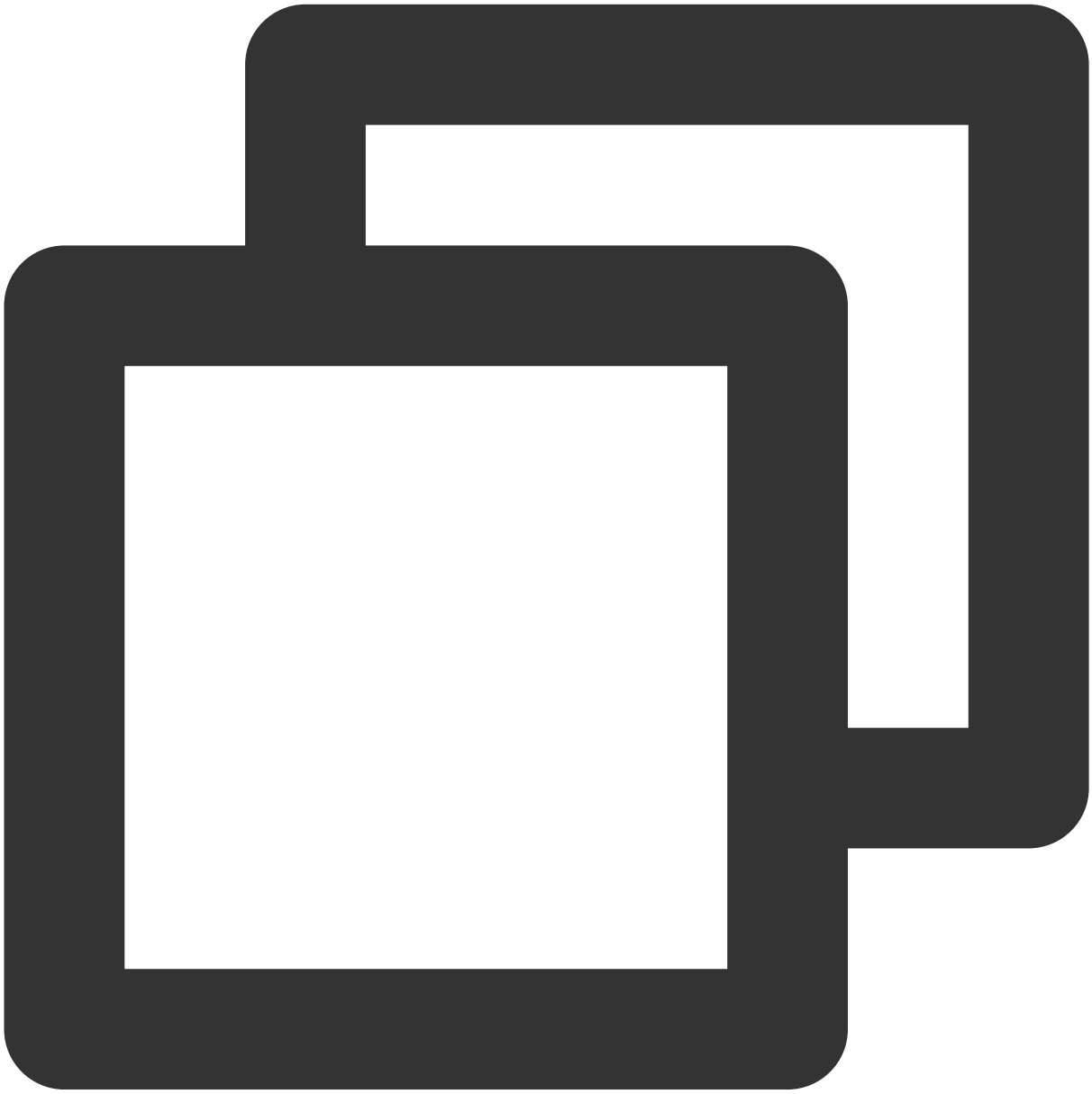


```
sudo iptables -L --line-number
```

SSH接続が拒否されていた場合は、対応するソフトウェアのホワイトリストなどの関連ポリシーによって、ご自身で設定を行ってください。
SSH接続が拒否されていなかった場合は、次の手順に進んでください。

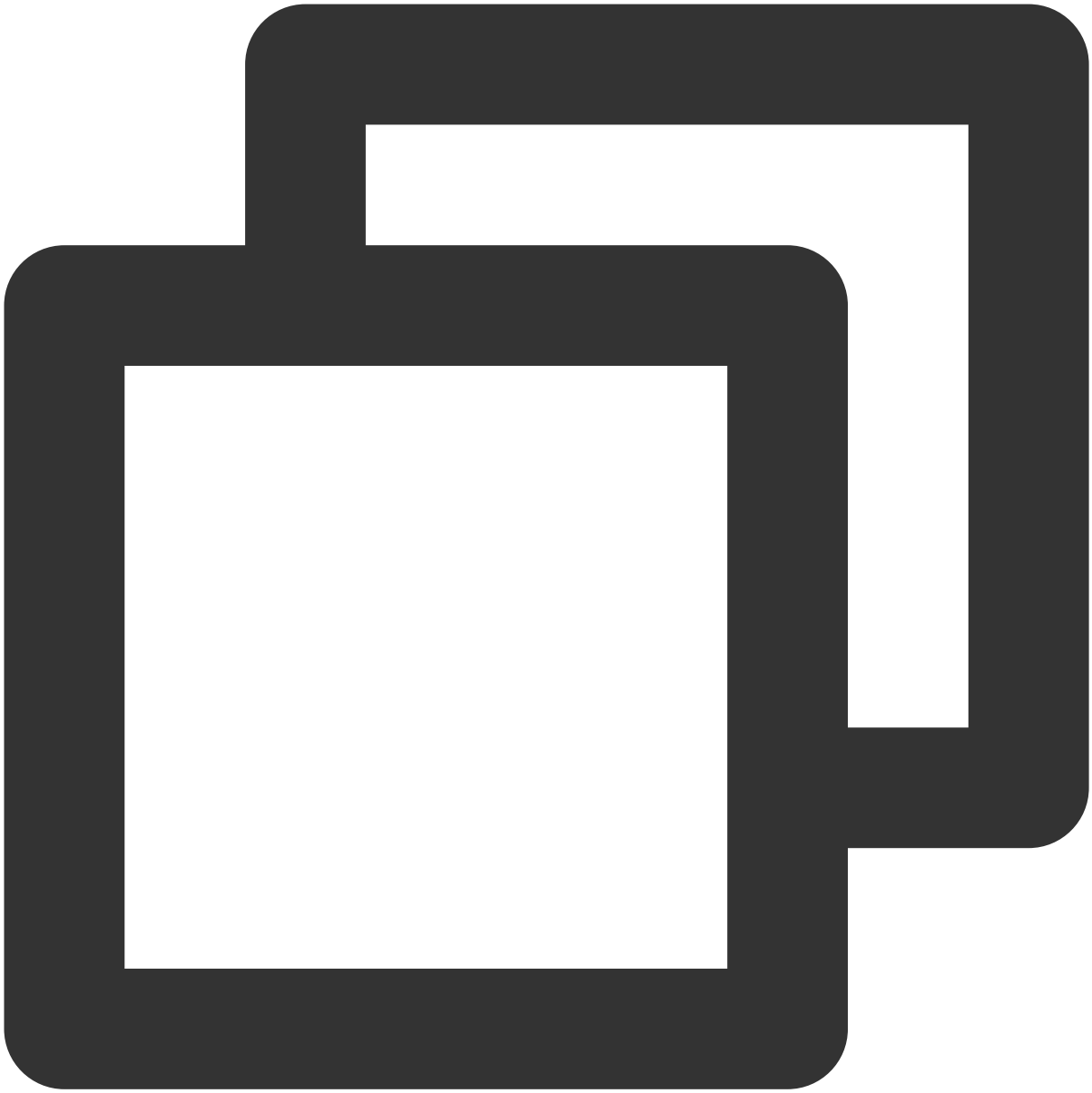
sshd設定の確認と調整

1. 以下のコマンドを実行し、VIMエディタを使用して `sshd_config` に進み、ファイルを設定します。



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

2. `MaxStartups` の値を調整する必要があるかどうかを確認します。 `sshd_config` 設定ファイル内の `MaxStartups` によって許可する最大接続数を設定します。短時間に多くの接続を確立したい場合は、この値を適宜調整する必要があります。
調整が必要な場合は、以下の手順を参照して変更してください。
2.1.1 **i を押して編集モードに入り、変更完了後にEscを押して編集モードを終了し、:wq**を入力して変更を保存します。
説明：
MaxStartupsは10:30:100がデフォルト設定であり、SSH保護プロセスの、アイデンティティ認証を経ない同時接続の最大数を指定します。10:30:100とは、10番目の接続以降、接続数が100に達するまで、30%の確率（漸増）で新たな接続を拒否することを表します。
2.1.2 以下のコマンドを実行し、sshdサービスを再起動します。



```
service sshd restart
```

調整の必要がない場合は、次の手順に進んでください。

ネットワーク環境のテスト

1. プライベートIPアドレス を使用してログインしているかどうかを確認します。
「はい」の場合は、パブリックIP に切り替えてから再度試してください。
「いいえ」の場合は、次の手順に進んでください。
2. 他のネットワーク環境を使用して、正常に接続されるかをテストします。

「はい」の場合は、インスタンスを再起動後にVNCを使用してインスタンスにログインしてください。
「いいえ」の場合は、テスト結果に基づいてネットワーク環境の問題を解決してください。
ここまででSSHログインの問題が解決されていない場合は、システムカーネルに異常が生じているか、またはその他の潜在的な原因による可能性があります。問題の処理を進めるため、チケットを提出 してご連絡ください。
SSHログインエラーPermission denied, please try again

現象の説明

rootユーザーがSSHを使用してLinuxインスタンスにログインする際、エラー情報「Permission denied, please try again」が表示されます。

問題の原因

システムによってSELinuxサービスがアクティブ化されたか、またはSSH サービスによって `PermitRootLogin` 設定が変更されたことによるものです。

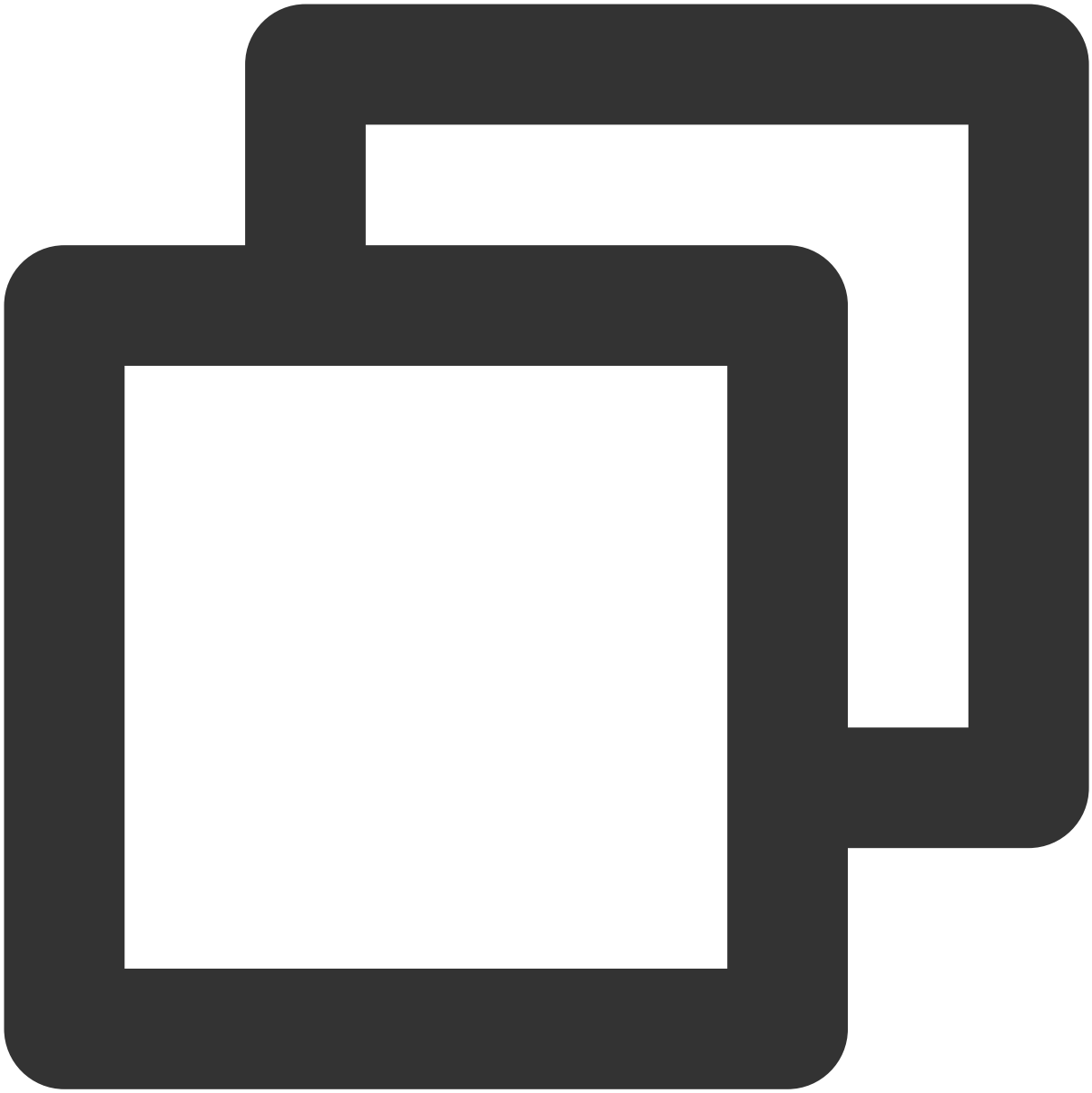
解決方法

処理手順 を参照し、SELinuxサービスおよびSSH設定ファイル `sshd_config` の `PermitRootLogin` パラメータを確認し、問題の原因を確認して問題を解決します。

処理手順

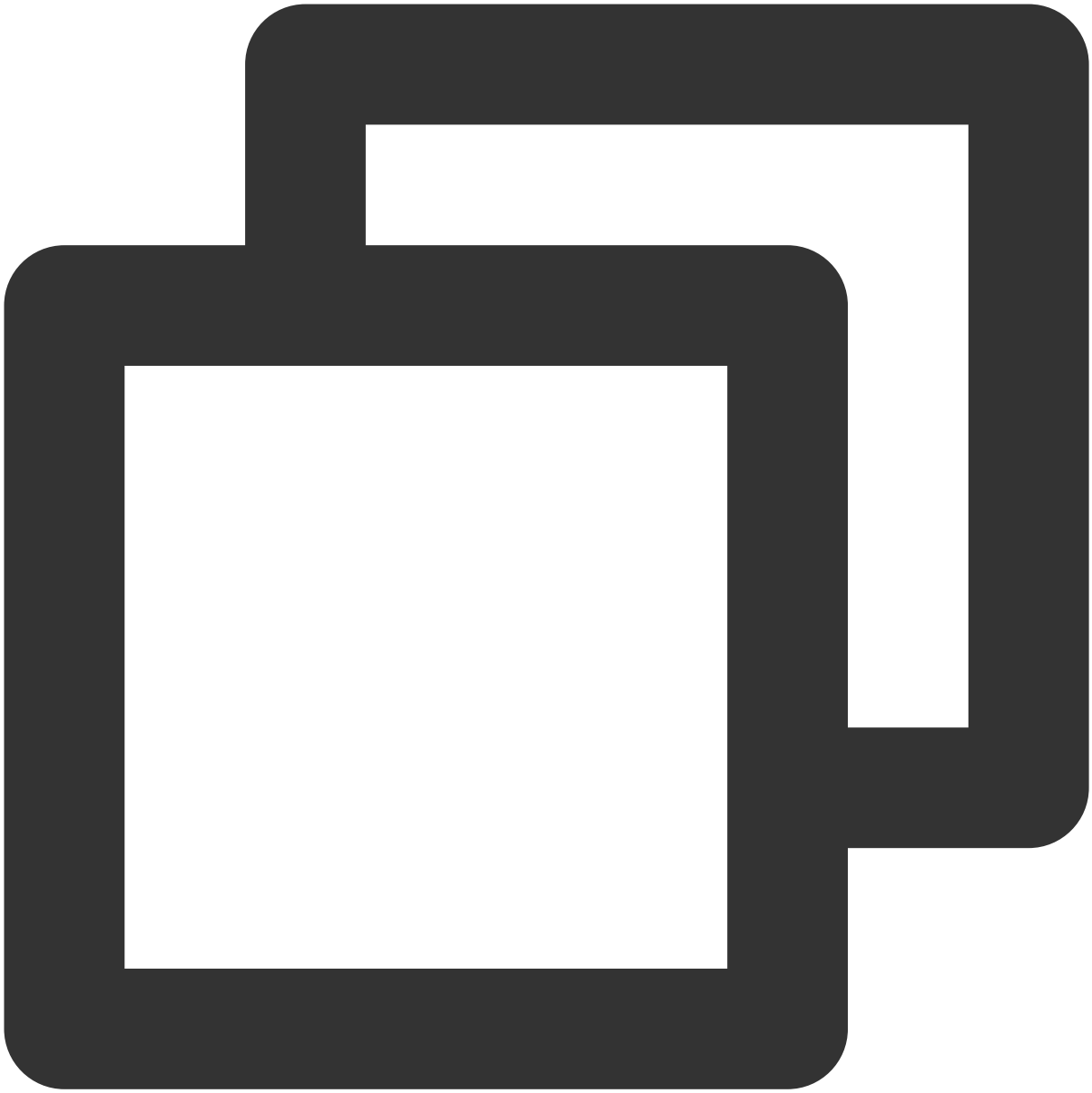
SELinuxサービスの確認と無効化

1. VNC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、現在のSELinuxのサービスステータスを確認します。



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

返されたパラメータが `enabled` であれば有効な状態であり、 `disabled` であれば無効な状態です。有効な状態であれば次のように表示されます。

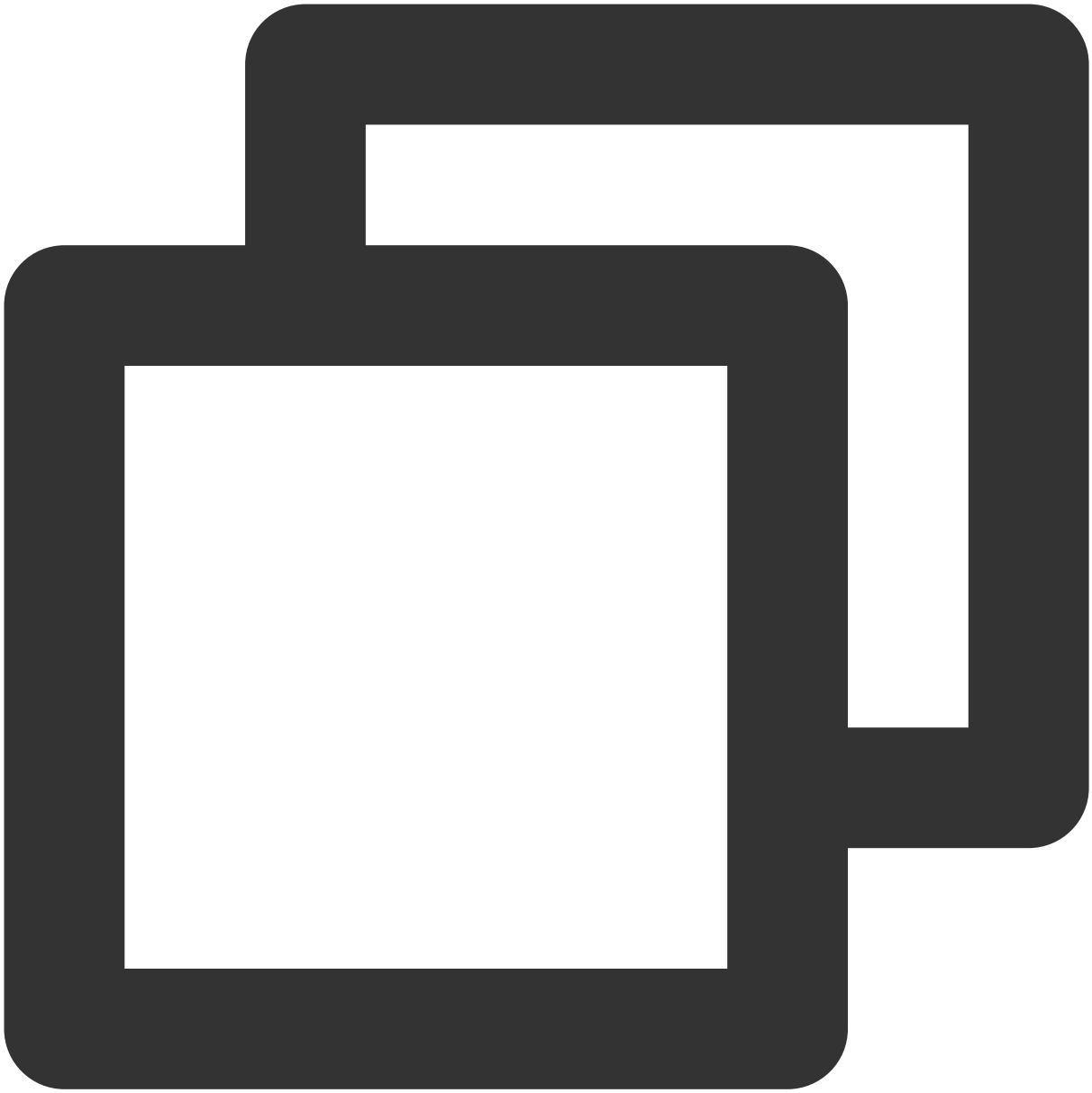


```
SELinux status:       enabled
```

3. 実際の状況に応じて、SELinuxサービスを一時的または永続的に無効化します。

SELinuxサービスを一時的に無効化

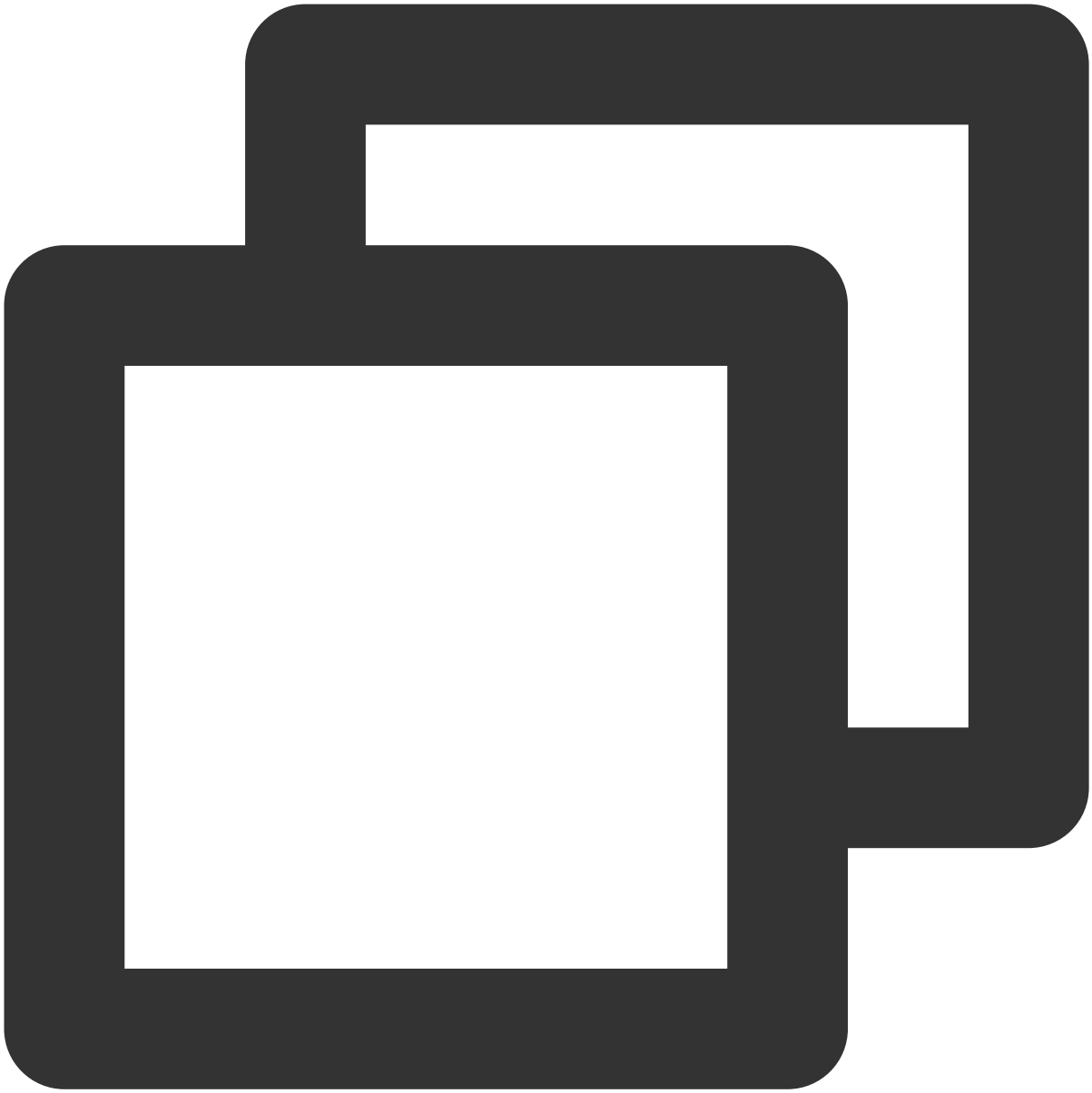
以下のコマンドを実行し、SELinuxサービスを一時的に無効化します。変更はリアルタイムに有効となり、システムまたはインスタンスを再起動する必要はありません。



```
setenforce 0
```

SELinuxサービスを永続的に無効化

以下のコマンドを実行し、SELinuxサービスを無効化します。



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

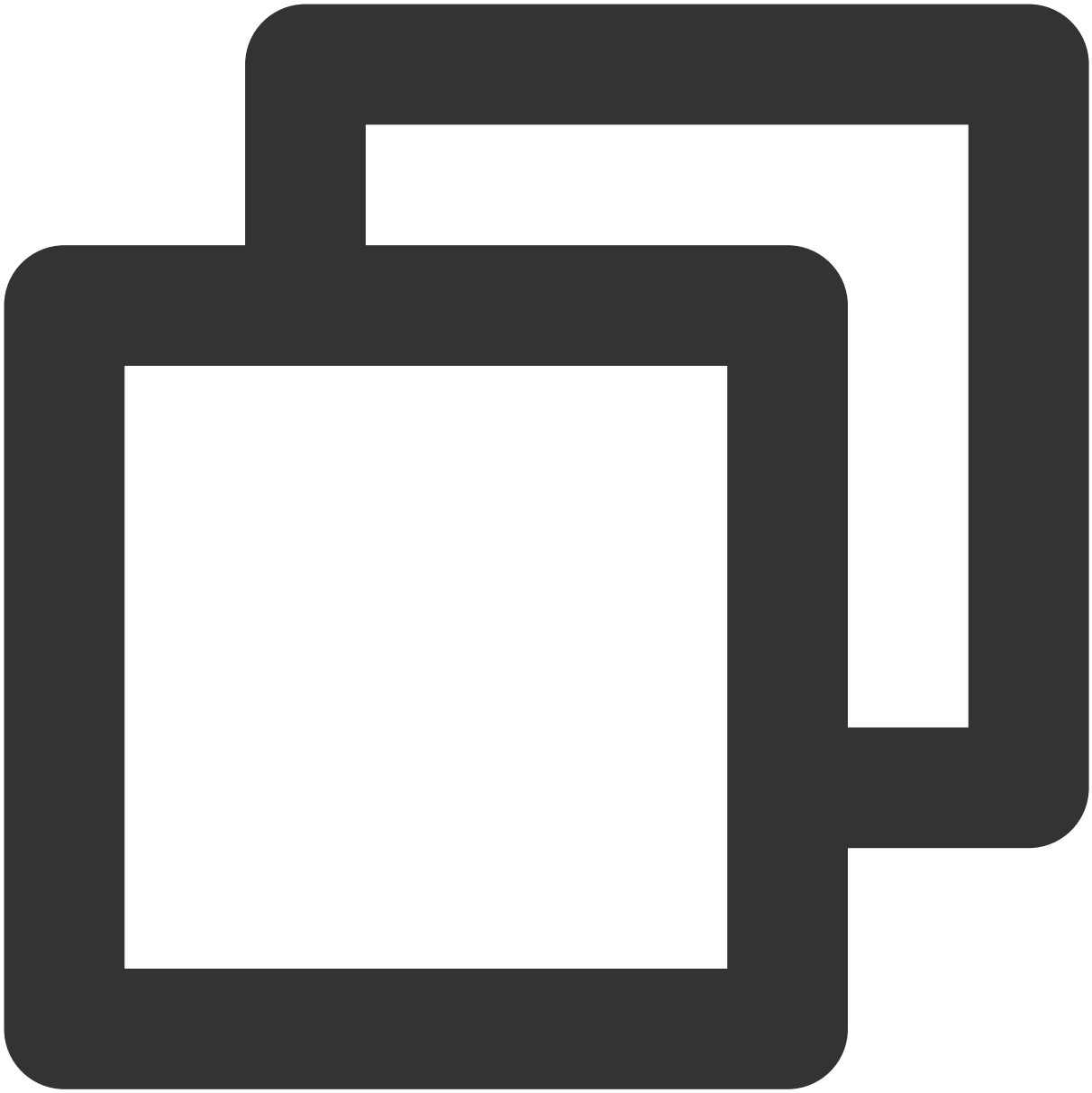
ご注意：

このコマンドはSELinuxサービスがenforcing状態の場合にのみ適用されます。

コマンド実行後にシステムまたはインスタンスを再起動し、変更を有効にする必要があります。

sshd設定の確認と調整

1. VNC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、VIMエディタを使用して `sshd_config` 設定ファイルに進みます。



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

3. **i**を押して編集モードに入り、 `PermitRootLogin no` を `PermitRootLogin yes` に変更します。

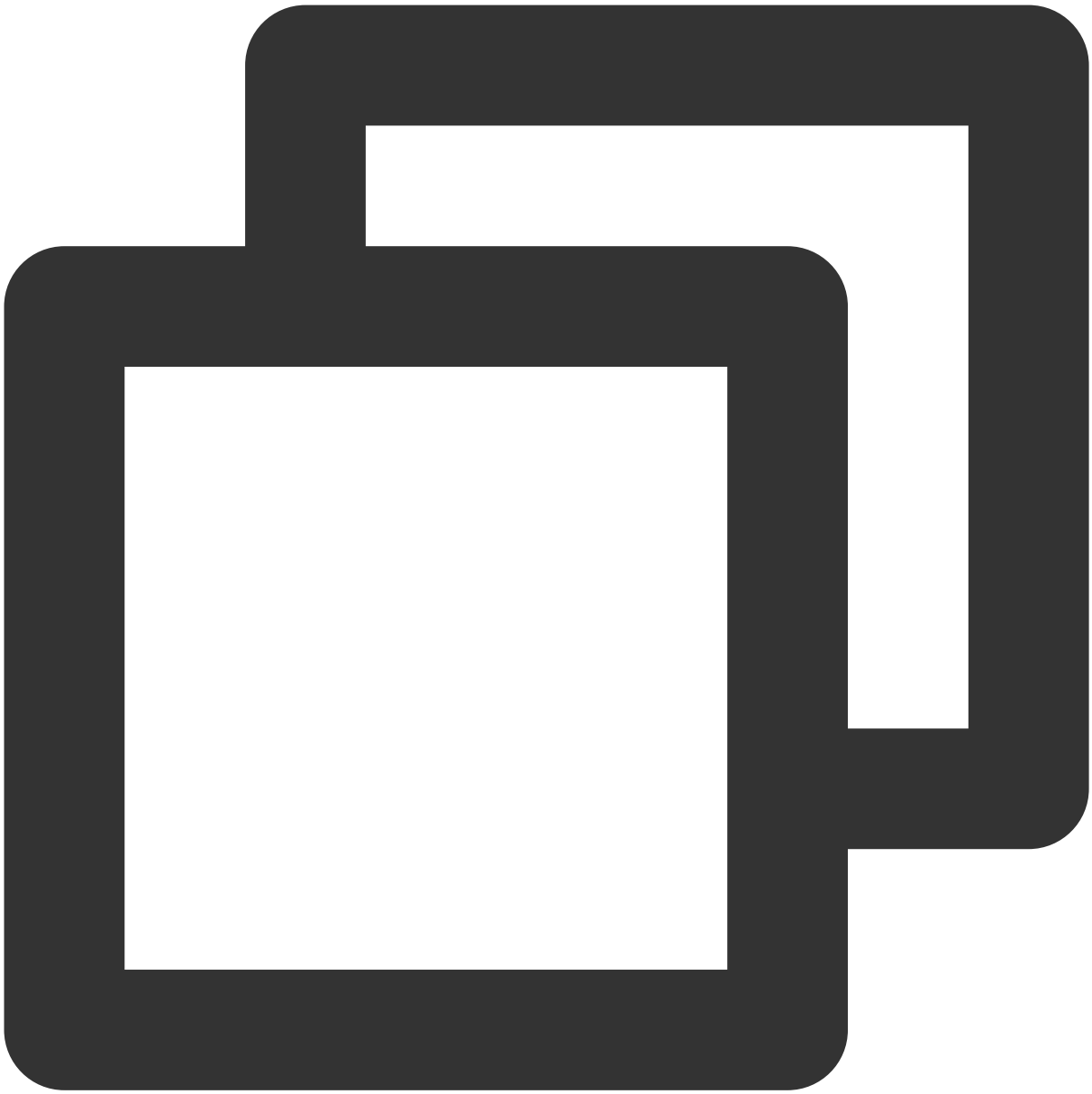
説明：

`sshd_config` でこのパラメータが設定されていない場合、rootユーザーログインがデフォルトで許可されます。

このパラメータはrootユーザーがSSHを使用してログインする場合にのみ影響し、rootユーザーがその他の方法でインスタンスにログインする場合には影響しません。

4. **Esc**を押して編集モードを終了し、**:wq**を入力して変更を保存します。

5. 以下のコマンドを実行して、SSHサービスを再起動します。



```
service sshd restart
```

SSHサービスを再起動すると、SSHを使用してログインできるようになります。詳細については SSH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。

SSHログイン時エラーToo many authentication failures for root

現象の説明

SSHを使用してログインする際、ログイン時にパスワードを複数回入力すると、エラー情報「Too many authentication failures for root」が返され、接続が中断されます。

問題の原因

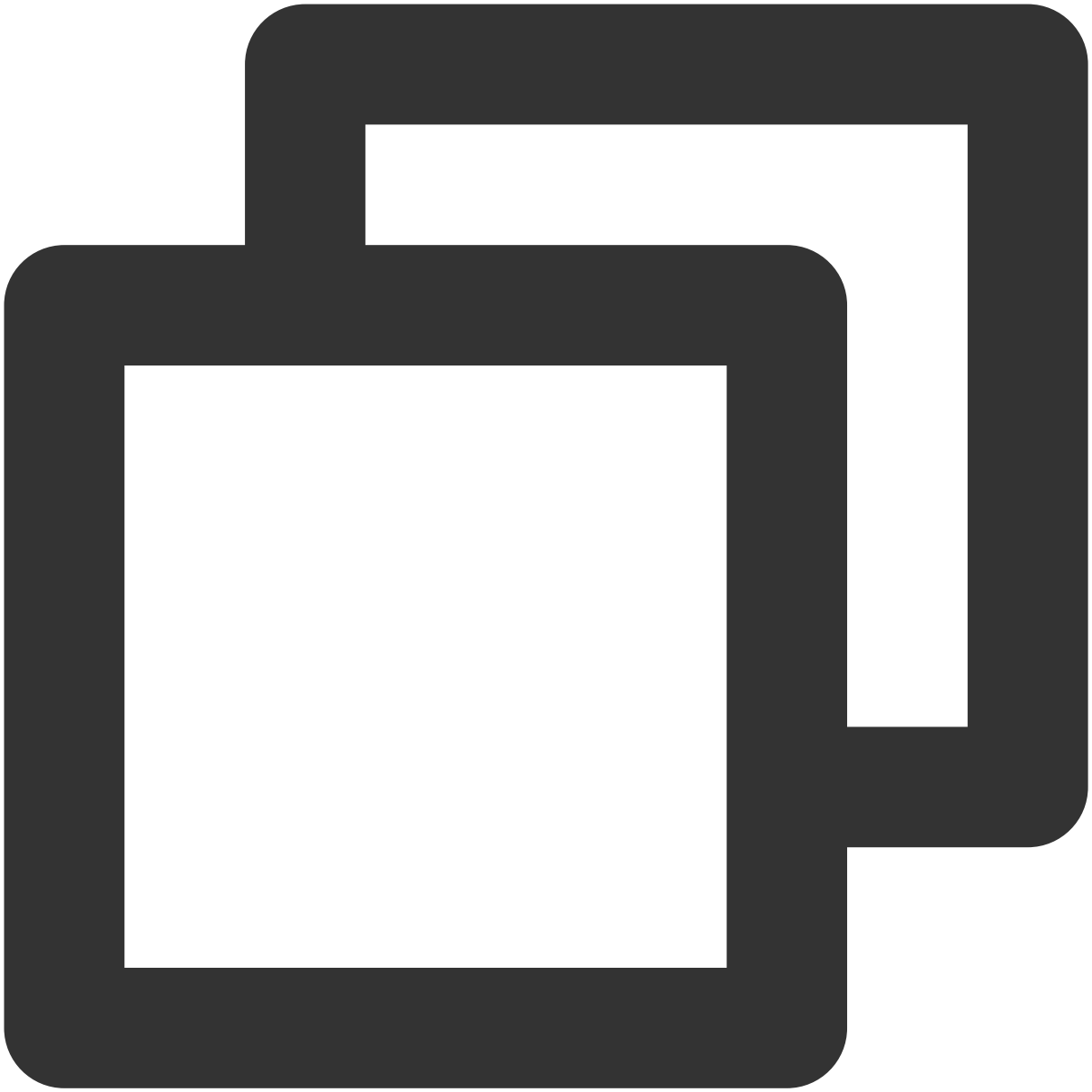
間違ったパスワードを複数回連続して入力し、SSHサービスのパスワードリセットポリシーをトリガーしたことが原因です。

解決方法

1. 処理手順 を参照し、SSHで設定した `sshd_config` ファイルに進みます。
2. SSHサービスのパスワードリセットポリシーの `MaxAuthTries` パラメータ設定を確認して変更し、SSHサービスを再起動すれば完了です。

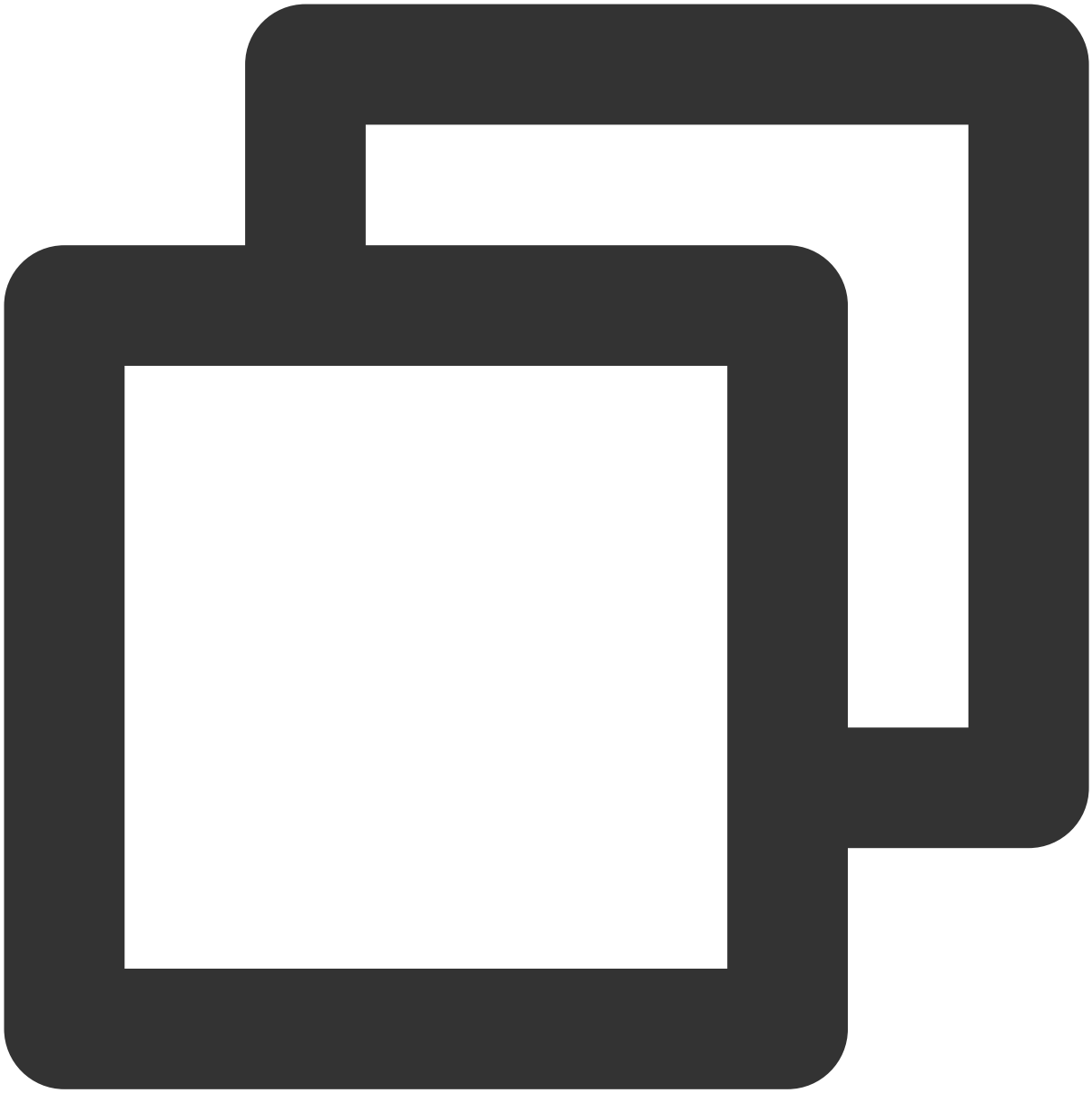
処理手順

1. VNC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、VIMエディタを使用して `sshd_config` 設定ファイルに進みます。



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

3. 以下に類似した設定が含まれていないか確認します。



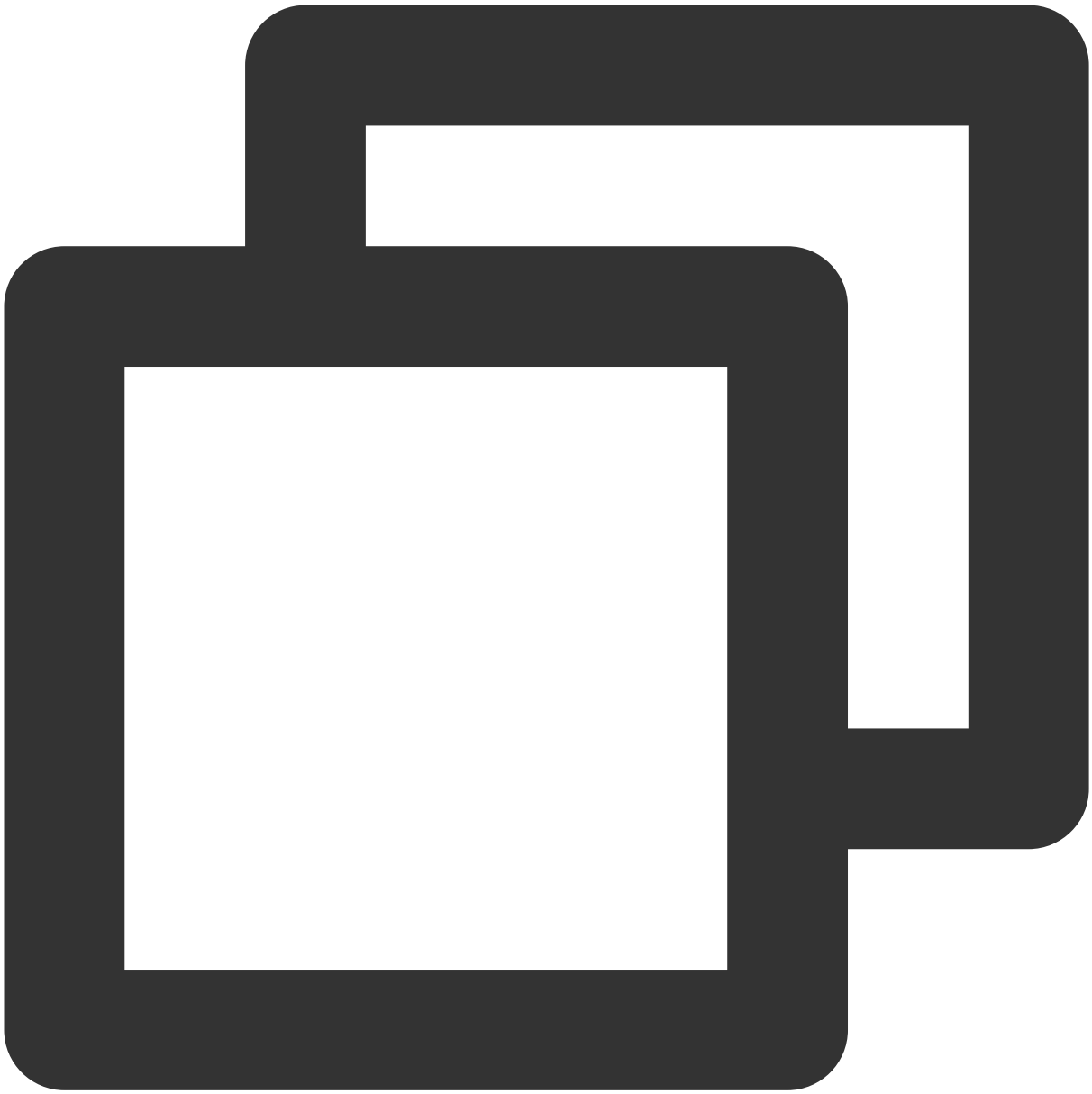
```
MaxAuthTries 5
```

説明：

このパラメータはデフォルトではアクティブになっておらず、ユーザーが毎回SSHを使用してログインする際に、間違ったパスワードを連続して入力できる回数を制限するために用いられます。設定した回数を超えるとSSH接続が切断され、関連のエラー情報が表示されます。ただし、関連のアカウントはロックされず、SSHログインを再び使用することができます。

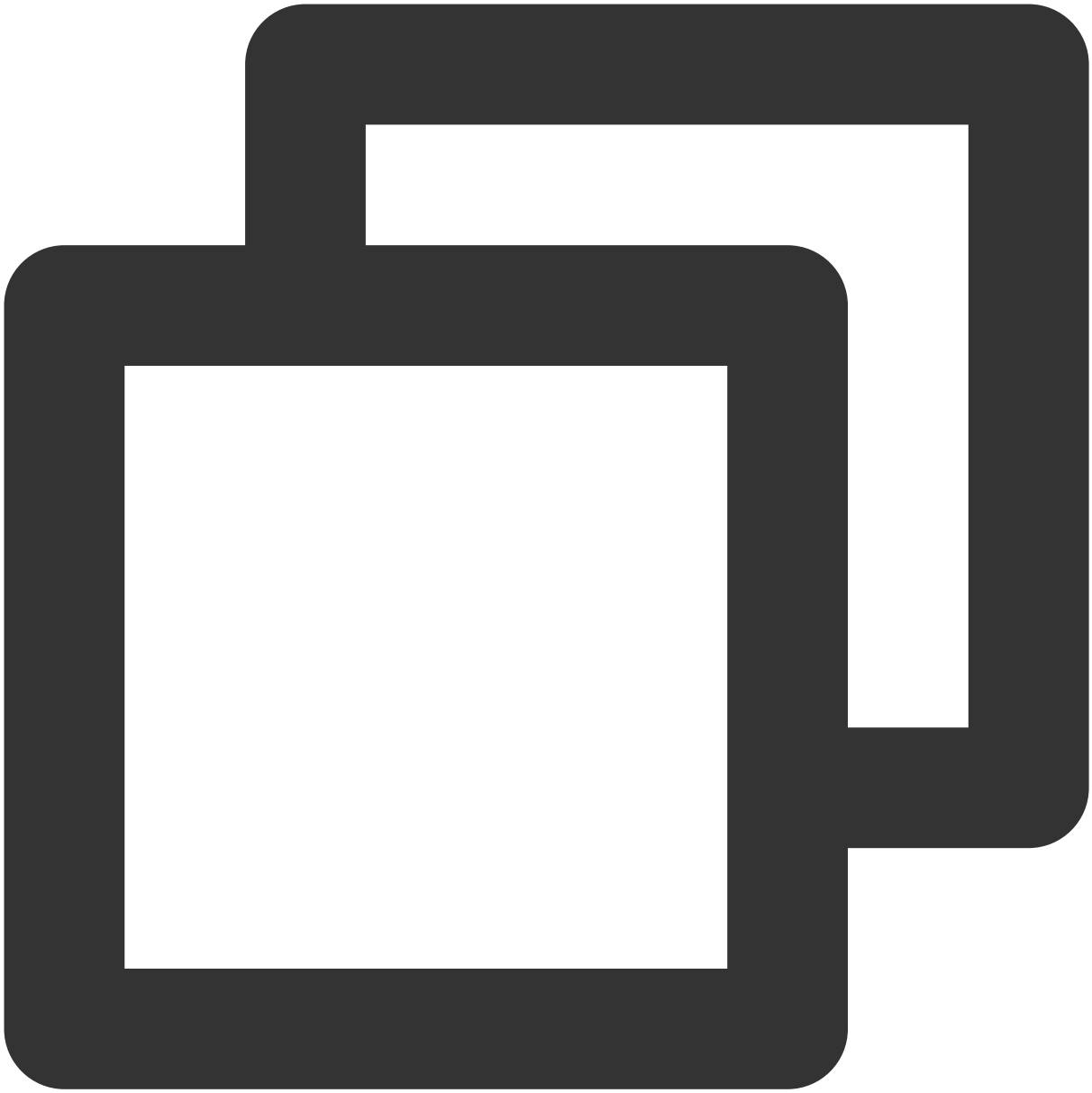
実際の状況に応じて、設定を変更するかどうかを決定してください。変更が必要な場合は `sshd_config` 設定ファイルのバックアップを作成しておくことをお勧めします。

4. **i**を押して編集モードに入り、以下の設定を変更するか、または行の先頭に `#` を追加してコメントします。



```
MaxAuthTries <間違ったパスワードの入力を許可する回数>
```

5. **Esc**を押して編集モードを終了し、**:wq**を入力して変更を保存します。
6. 以下のコマンドを実行し、SSHサービスを再起動します。



```
service sshd restart
```

SSHサービスを再起動すると、SSHを使用してログインできるようになります。詳細については SSH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。

SSH起動時エラーerror while loading shared libraries

現象の説明

Linuxインスタンスが SSHサービスを起動すると、以下に類似したエラー情報がsecureログファイル内に表示されるか、または直接返されます。

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

問題の原因

SSHサービスの稼働が依存する関連のシステムライブラリファイルが失われたか、または権限設定などの異常によるものです。

解決方法

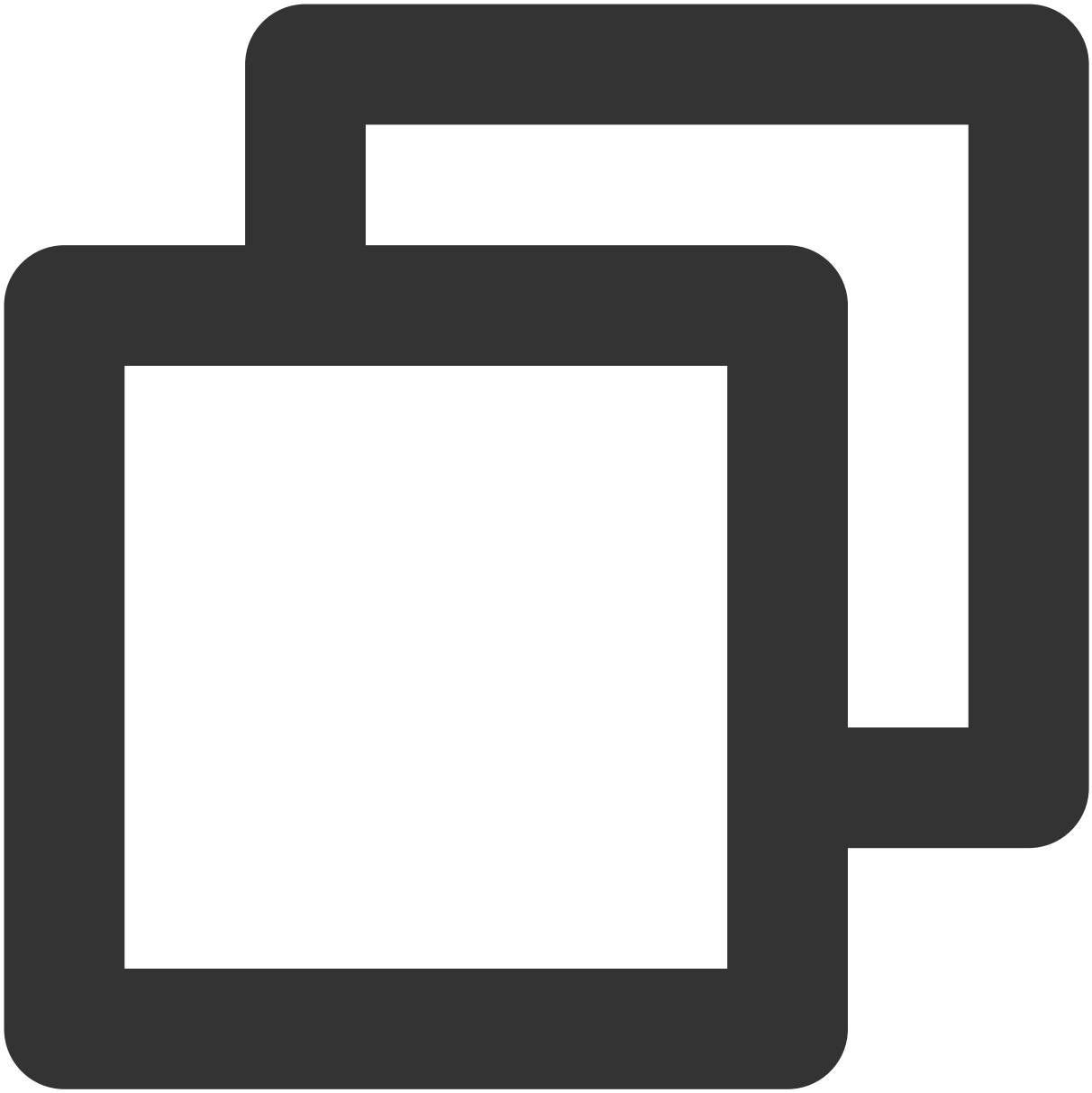
処理手順 を参照して、システムライブラリファイルを確認し、修復を行います。

処理手順

説明：
ここではlibcrypto.so.10ライブラリファイルの異常処理を例にとりますが、その他のライブラリファイル異常の処理方法もこれに類似しています。実際の状況に応じて操作を行ってください。

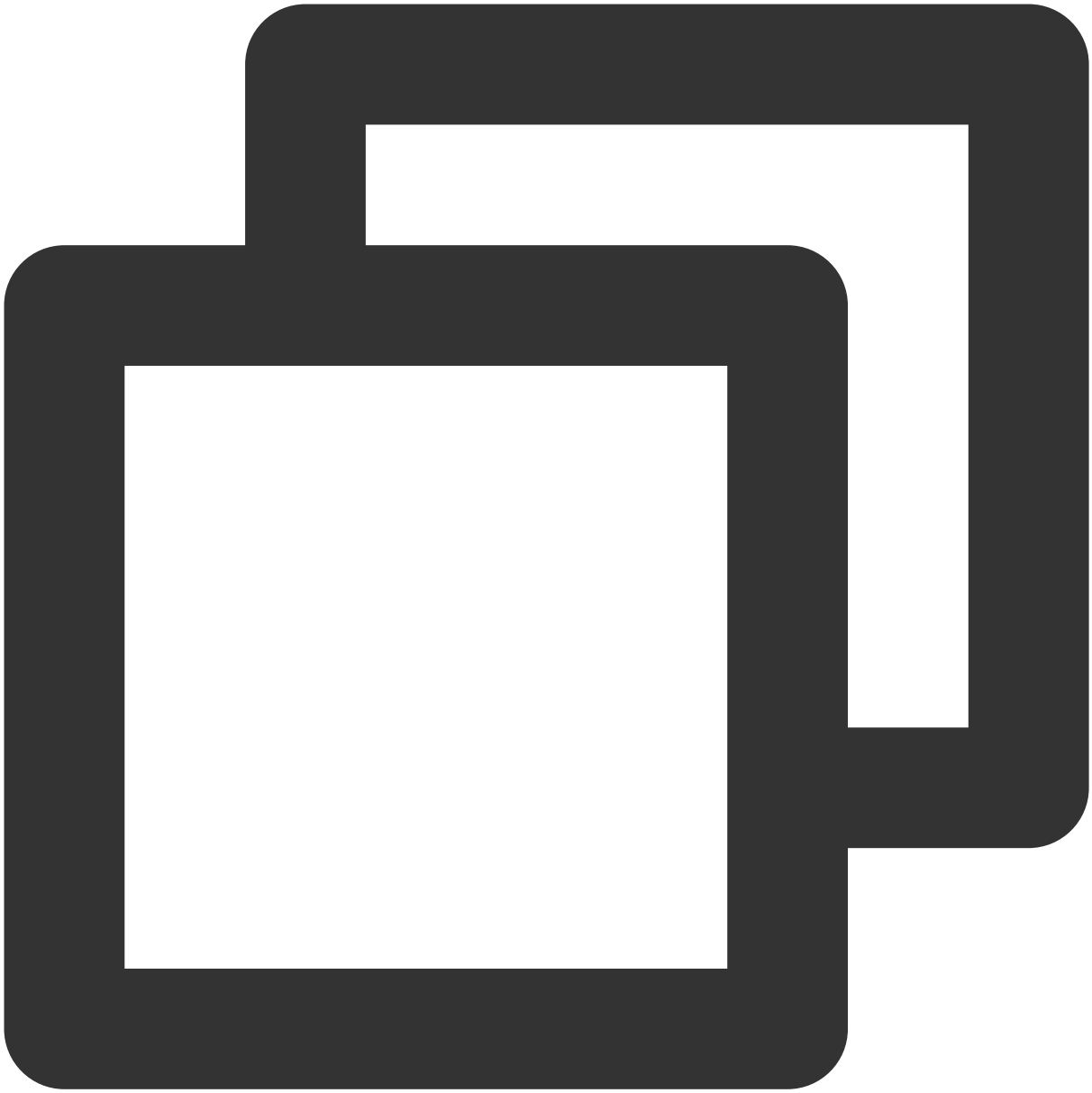
ライブラリファイル情報を取得する

1. VNC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、libcrypto.so.10ライブラリファイル情報を確認します。



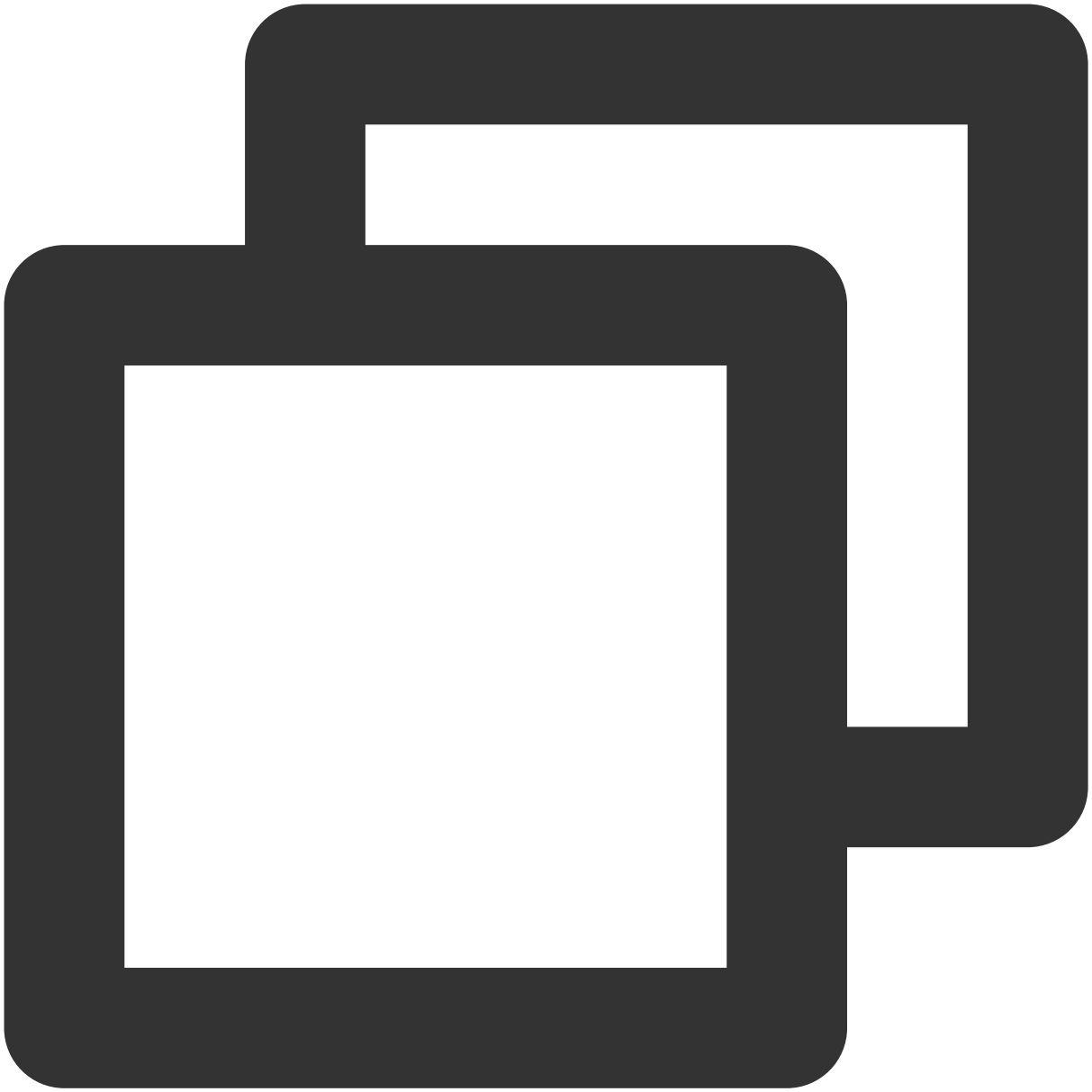
```
ll /usr/lib64/libcrypto.so.10
```

以下に類似した情報が返された場合、`/usr/lib64/libcrypto.so.10` は `libcrypto.so.1.0.2k` ライブラリファイルのソフトリンクであることを表します。



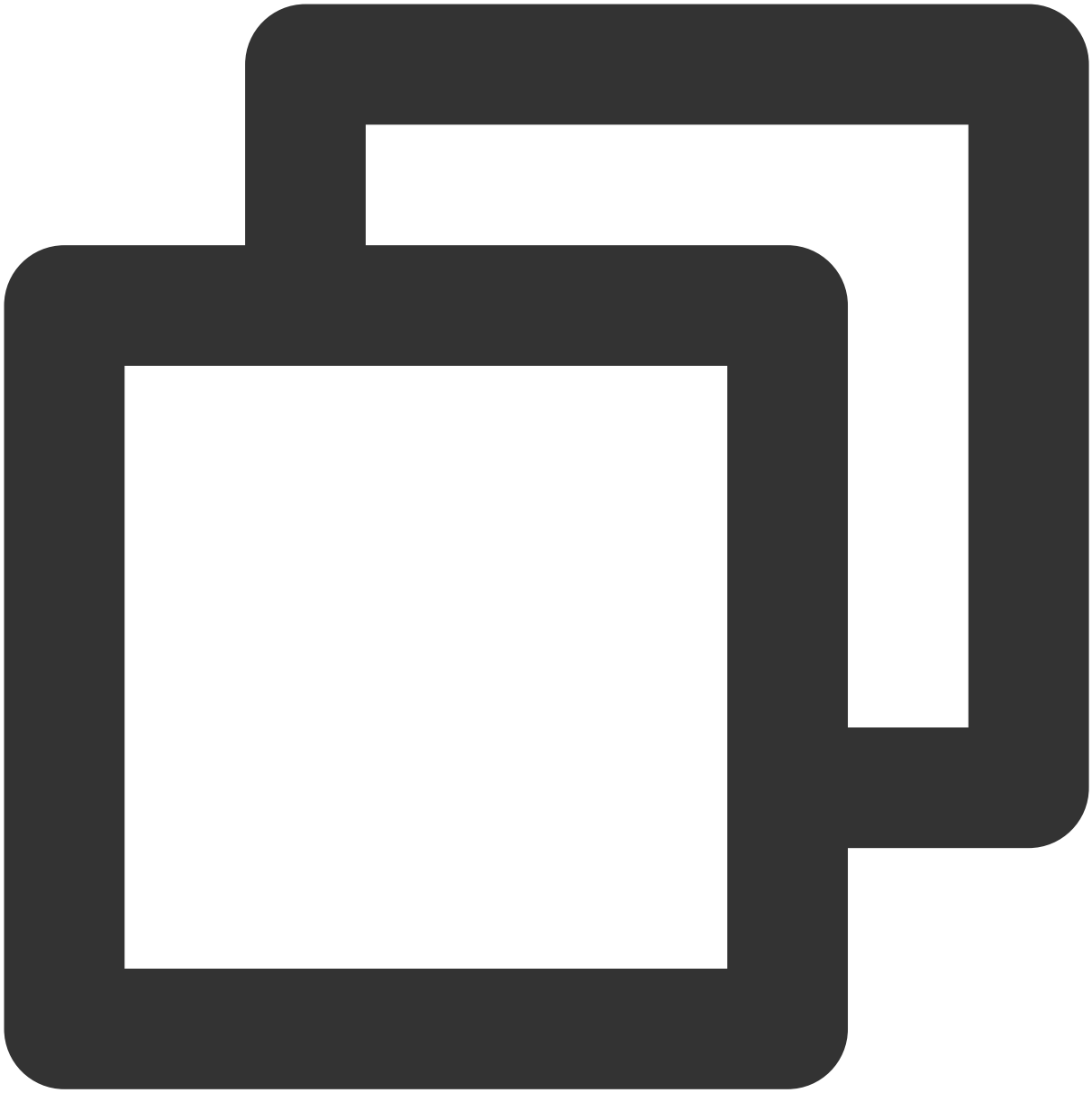
```
lrwxrwxrwx 1 root root 19 Jan 19  2021 /usr/lib64/libcrypto.so.10 -> libcrypto.so.1
```

3. 以下のコマンドを実行し、 `libcrypto.so.1.0.2k` ライブラリファイル情報を確認します。



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

以下に類似した情報が返されます。



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

4. 正常なライブラリファイルのパス、権限、グループなどの情報を記録し、以下の方法で処理を行います。

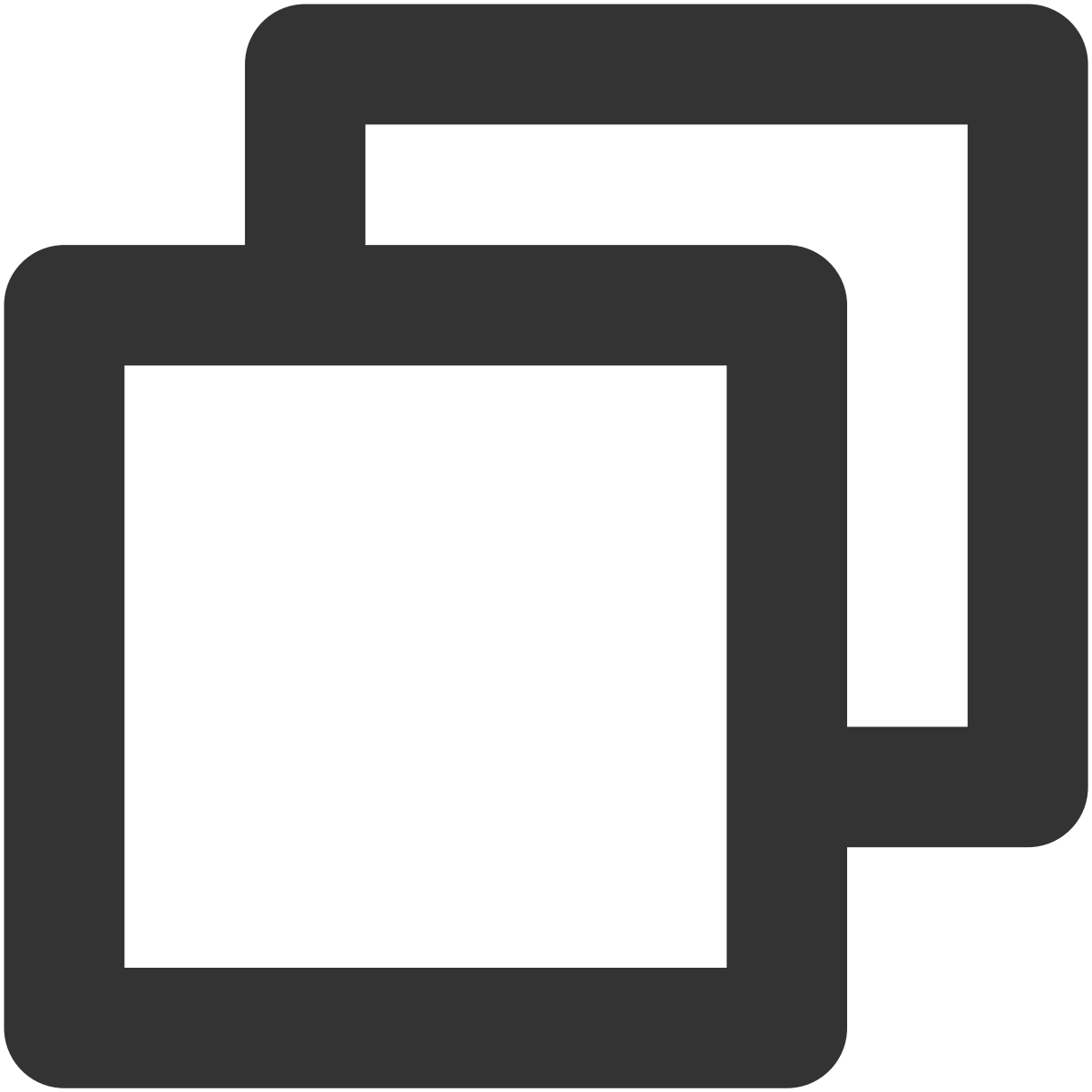
ライブラリファイルの検索と置換

外部ファイルのアップロード

スナップショットロールバックによるリカバリ

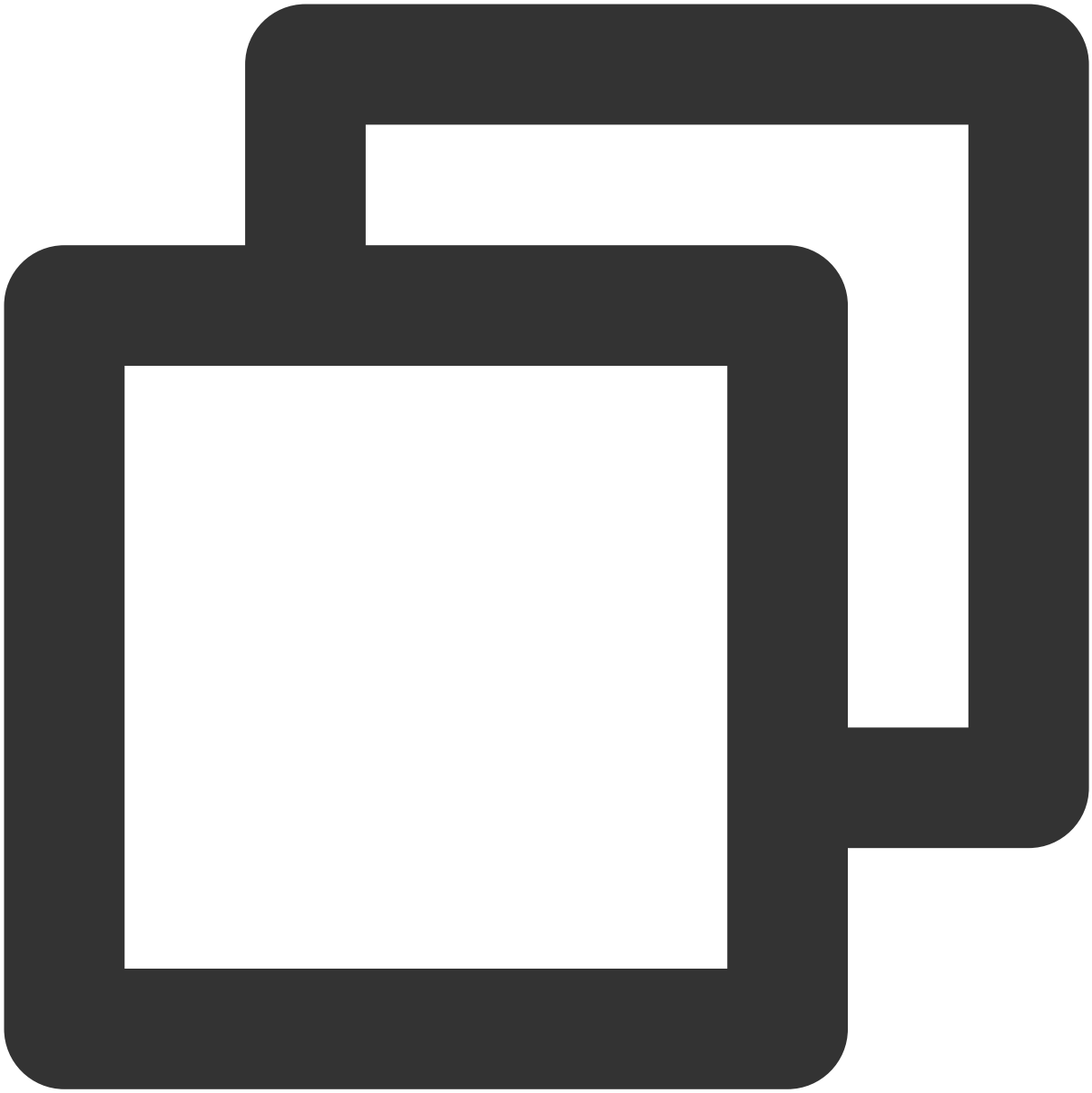
ライブラリファイルの検索と置換

1. 以下のコマンドを実行し、 `libcrypto.so.1.0.2k` ファイルを検索します。



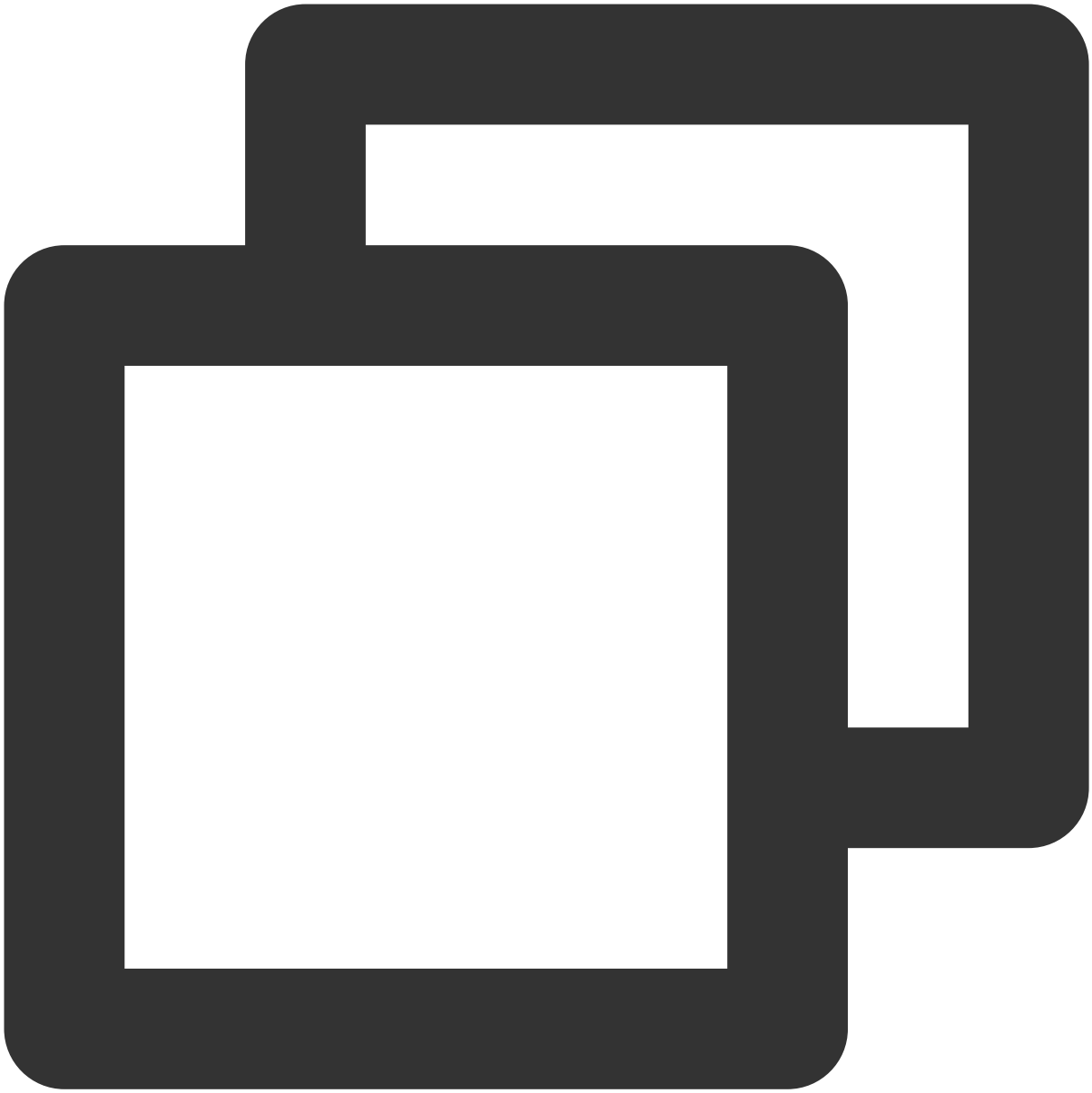
```
find / -name libcrypto.so.1.0.2k
```

2. 返された結果に基づいて以下のコマンドを実行し、ライブラリファイルを正常なディレクトリにコピーします。

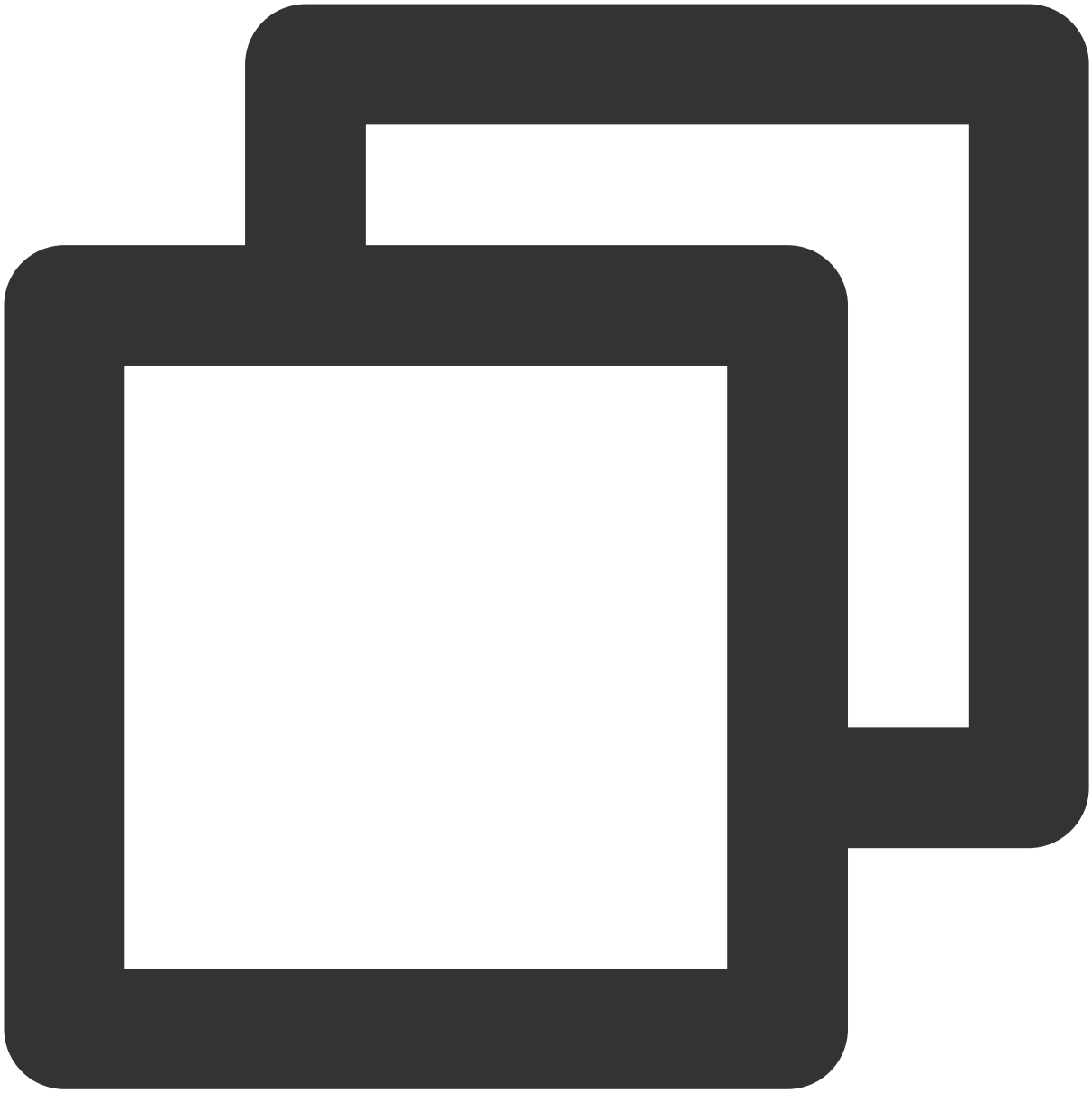


```
cp <手順1で取得したライブラリファイルの絶対パス> /usr/lib64/libcrypto.so.1.0.2k
```

3. 以下のコマンドを順に実行し、ファイルの権限、所有者、グループを変更します。

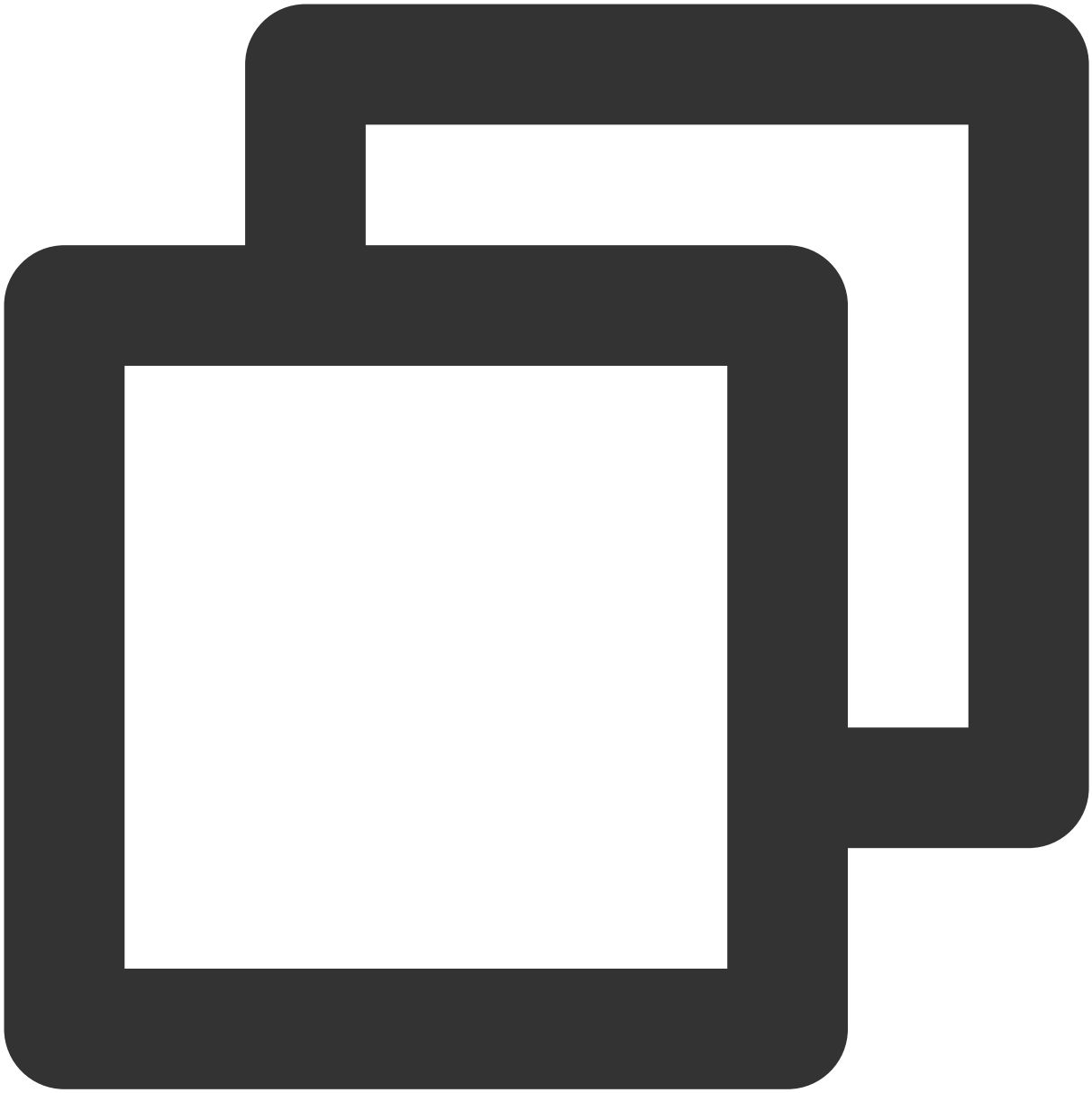


```
chmod 755 /usr/lib64/libcrypto.so.1.0.2k
```



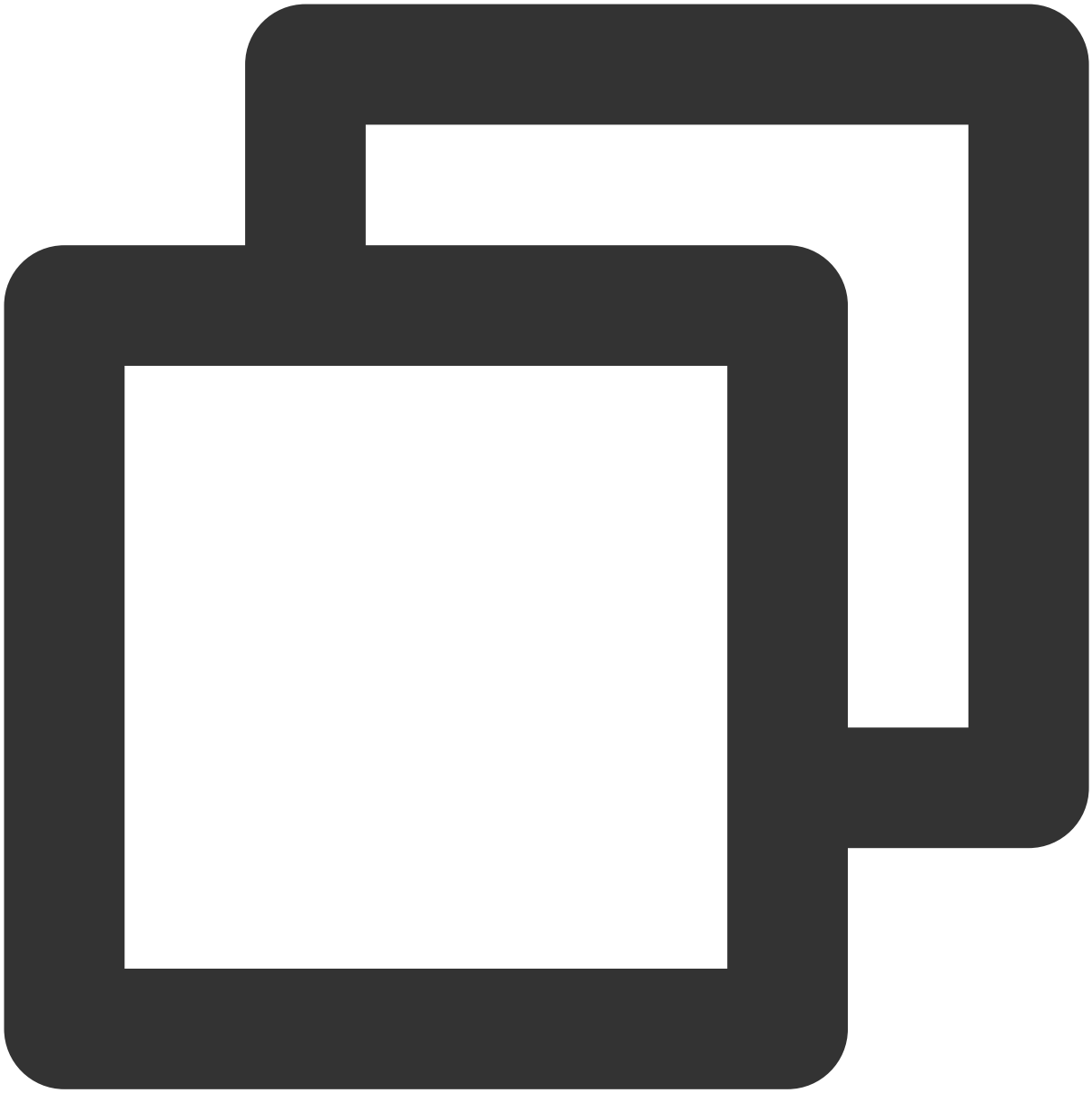
```
chown root:root /usr/lib64/libcrypto.so.1.0.2k
```

4. 以下のコマンドを実行し、ソフトリンクを作成します。



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

5. 以下のコマンドを実行し、SSHサービスを起動します。



```
service sshd start
```

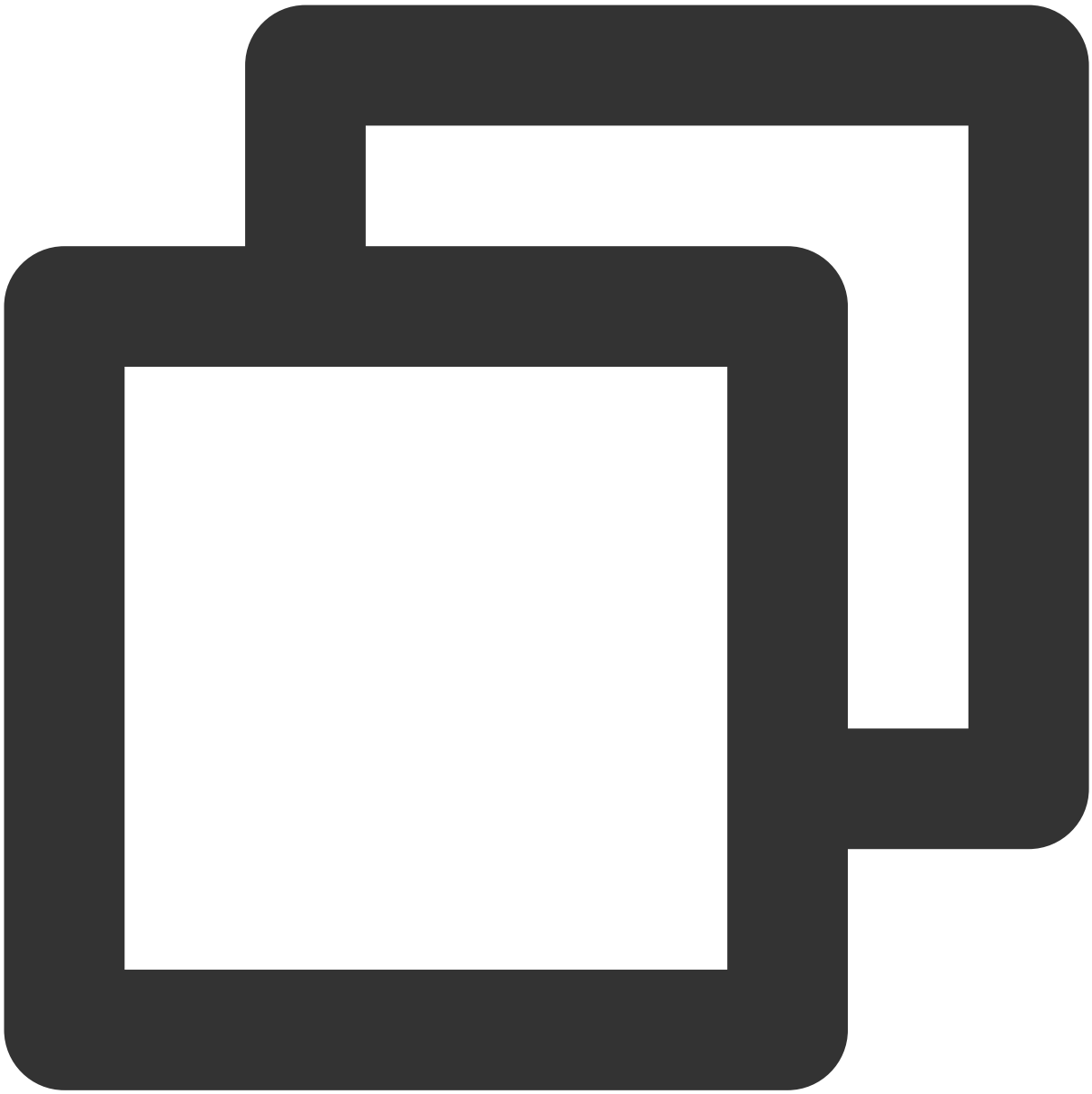
外部ファイルのアップロード

1. FTPソフトウェアにより、他の正常なサーバー上の `libcrypto.so.1.0.2k` のライブラリファイルを、目的のサーバーの `\\tmp` ディレクトリにアップロードします。

説明：

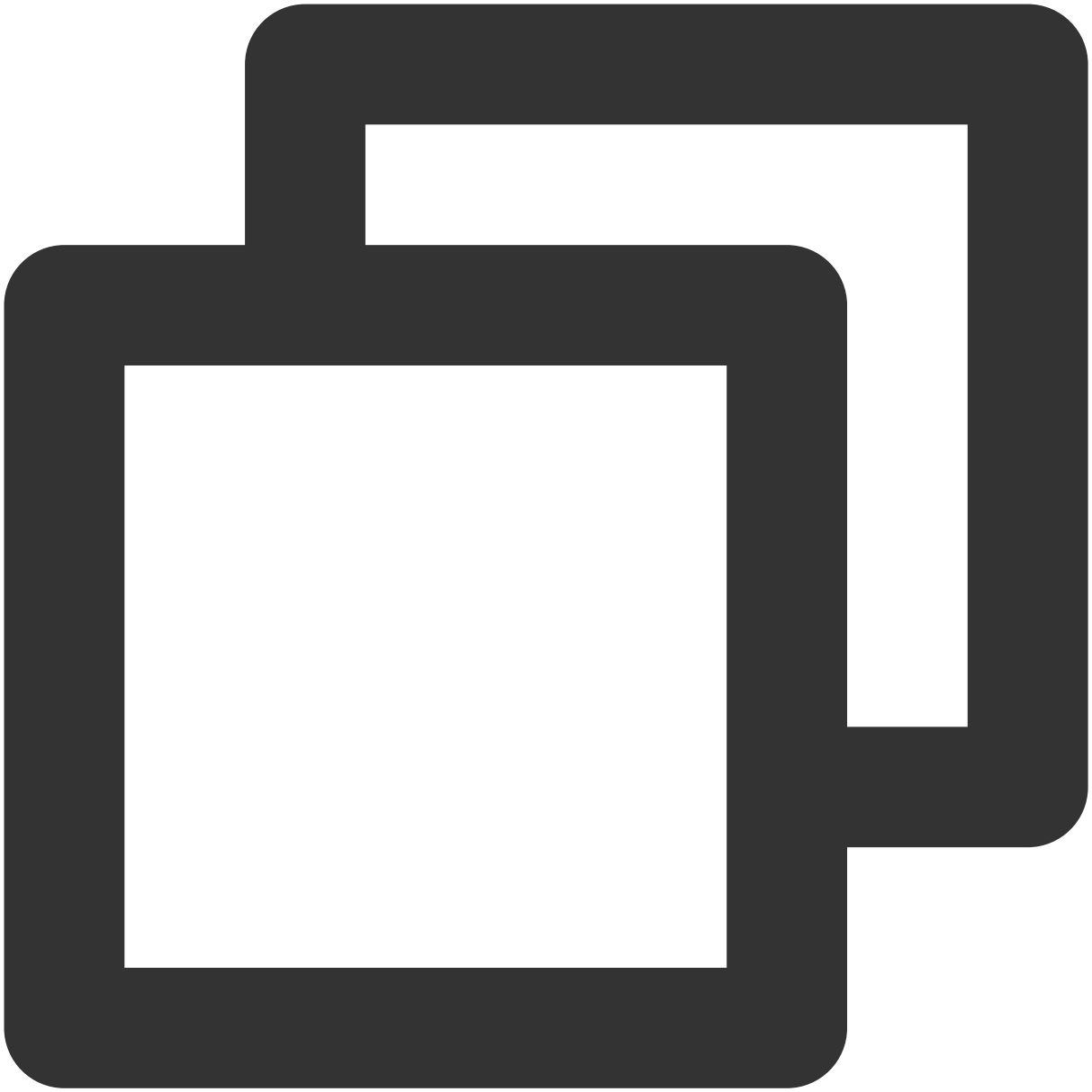
ここでは目的のサーバーの `\\tmp` ディレクトリへのアップロードを例にとりますが、実際の状況に応じて変更することができます。

2. 以下のコマンドを実行し、ライブラリファイルを正常なディレクトリにコピーします。

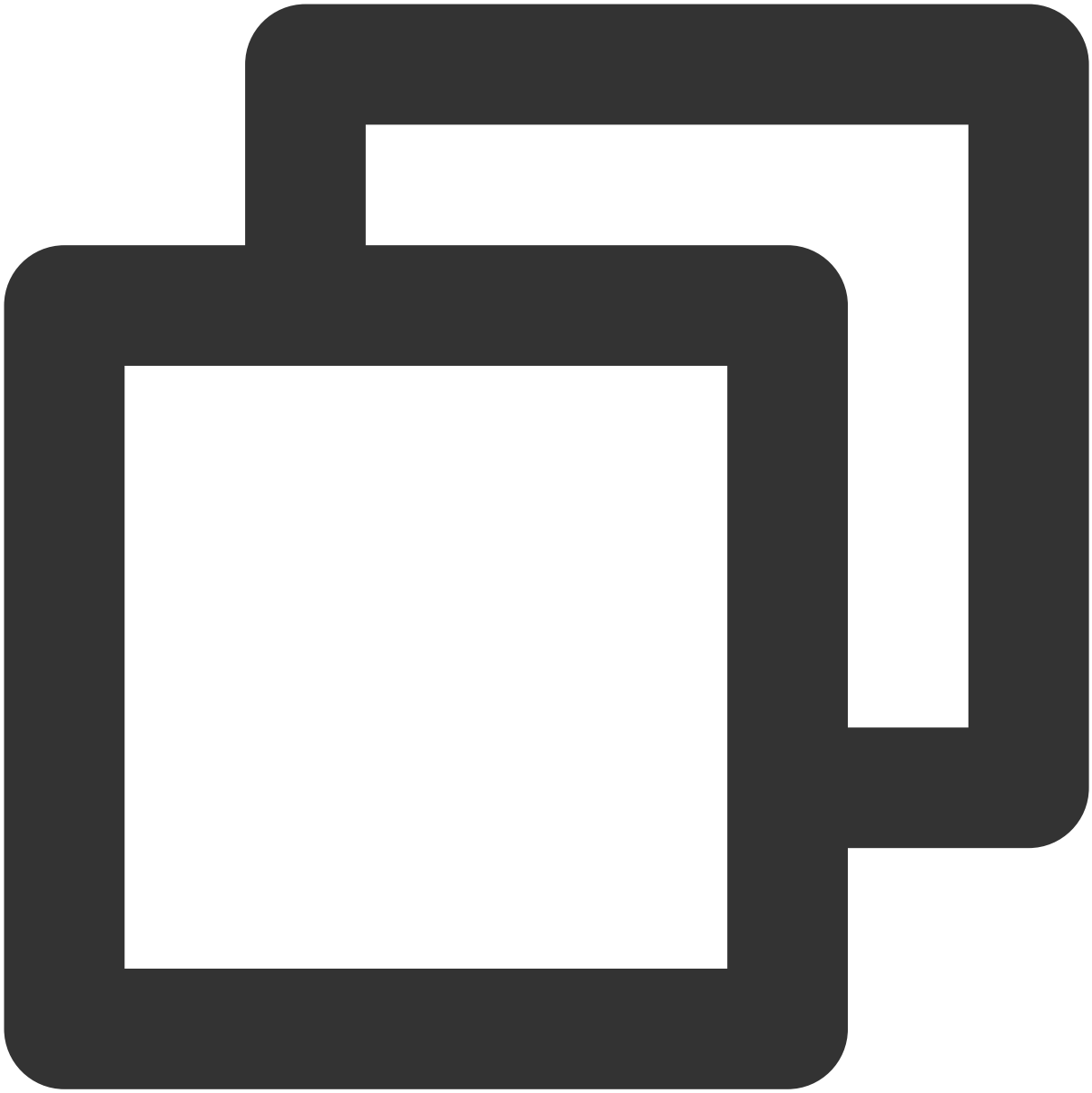


```
cp /tmp/libcrypto.so.1.0.2k /usr/lib64/libcrypto.so.1.0.2k
```

3. 以下のコマンドを順に実行し、ファイルの権限、所有者、グループを変更します。

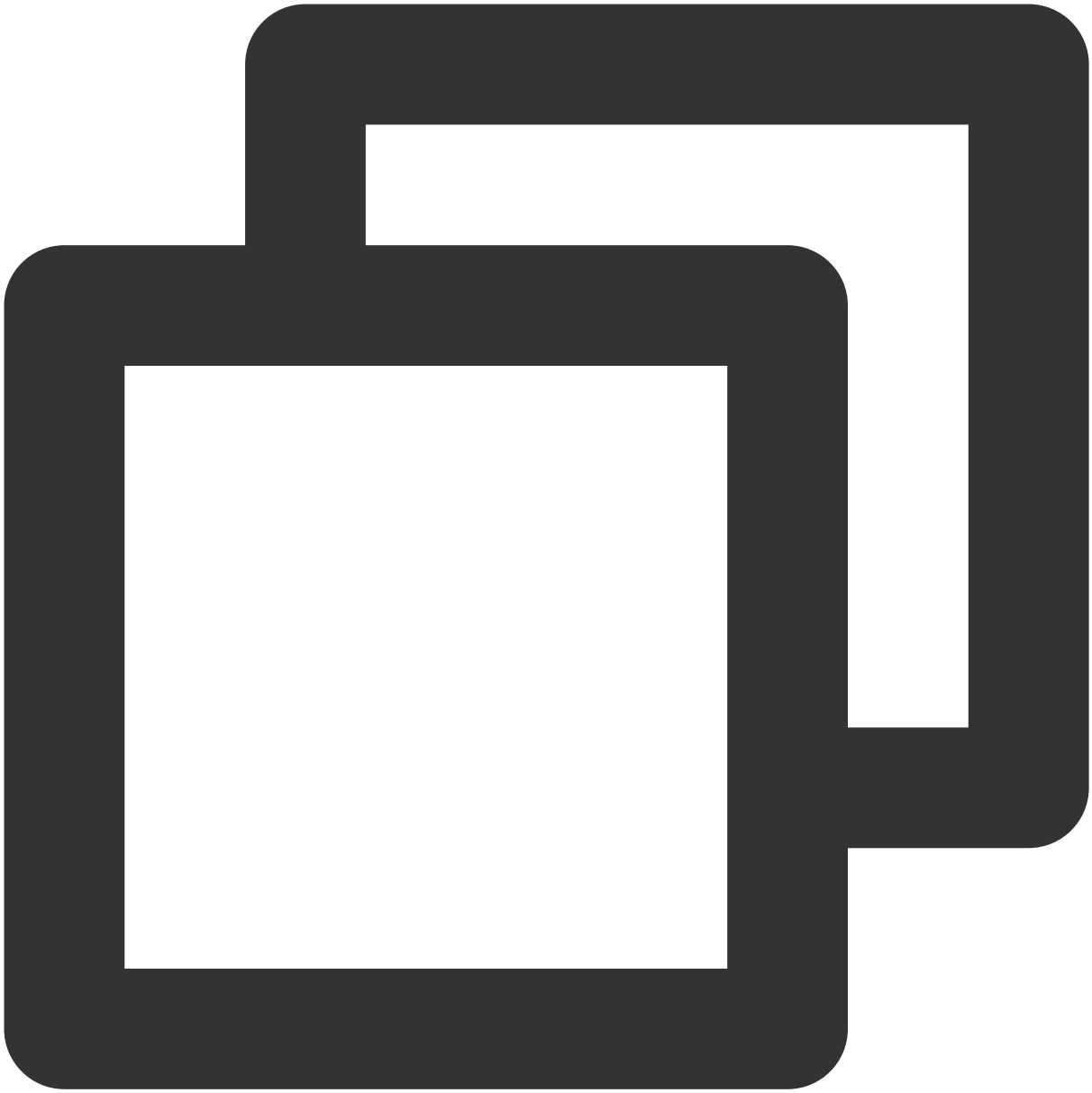


```
chmod 755 /usr/lib64/libcrypto.so.1.0.2k
```



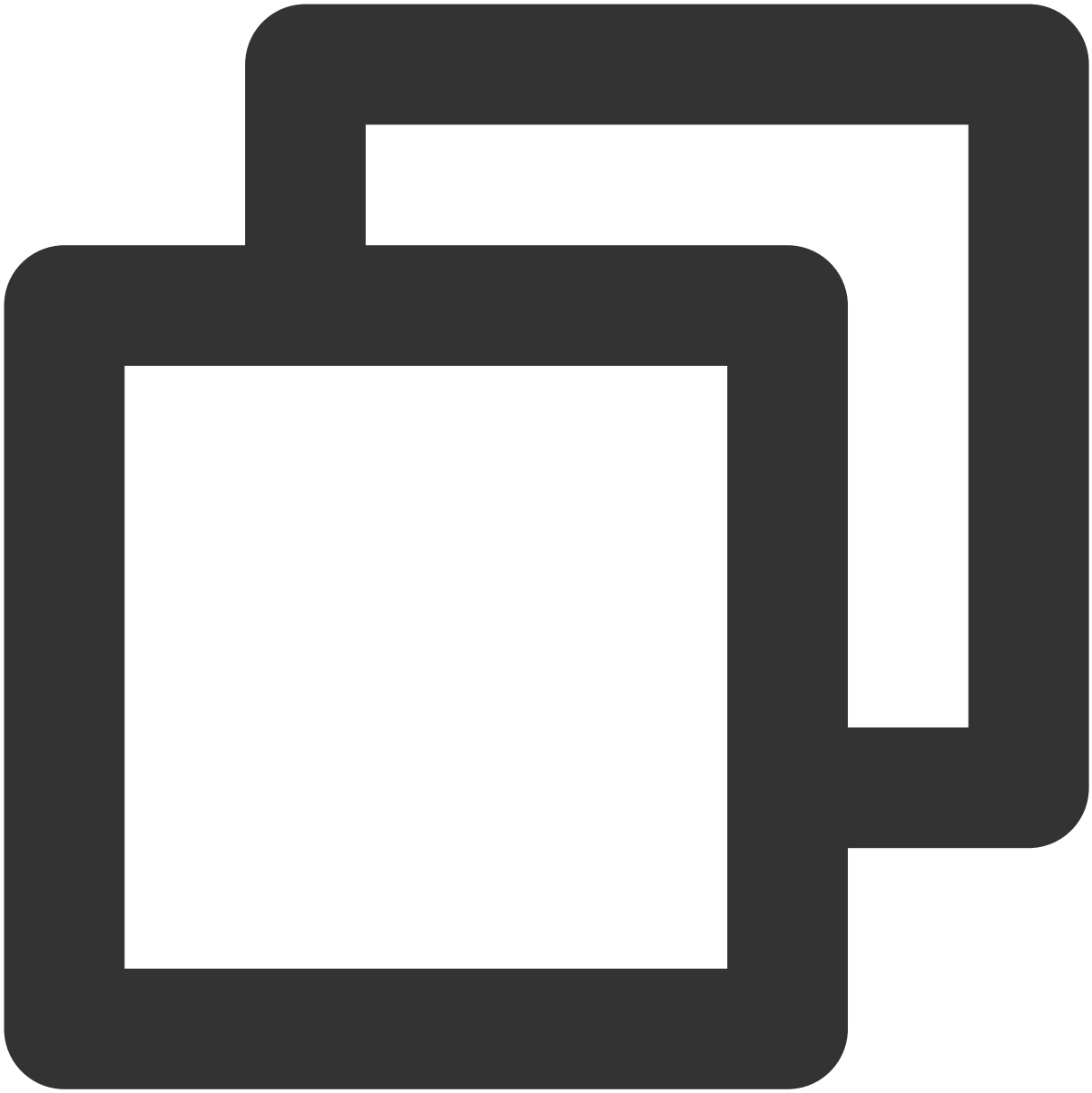
```
chown root:root /usr/lib64/libcrypto.so.1.0.2k
```

4. 以下のコマンドを実行し、ソフトリンクを作成します。



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

5. 以下のコマンドを実行し、SSHサービスを起動します。



```
service sshd start
```

スナップショットロールバックによるリカバリ

インスタンスシステムディスクの過去のスナップショットをロールバックすることで、ライブラリファイルをリカバリすることができます。詳細については、スナップショットからのデータロールバック をご参照ください。

ご注意：

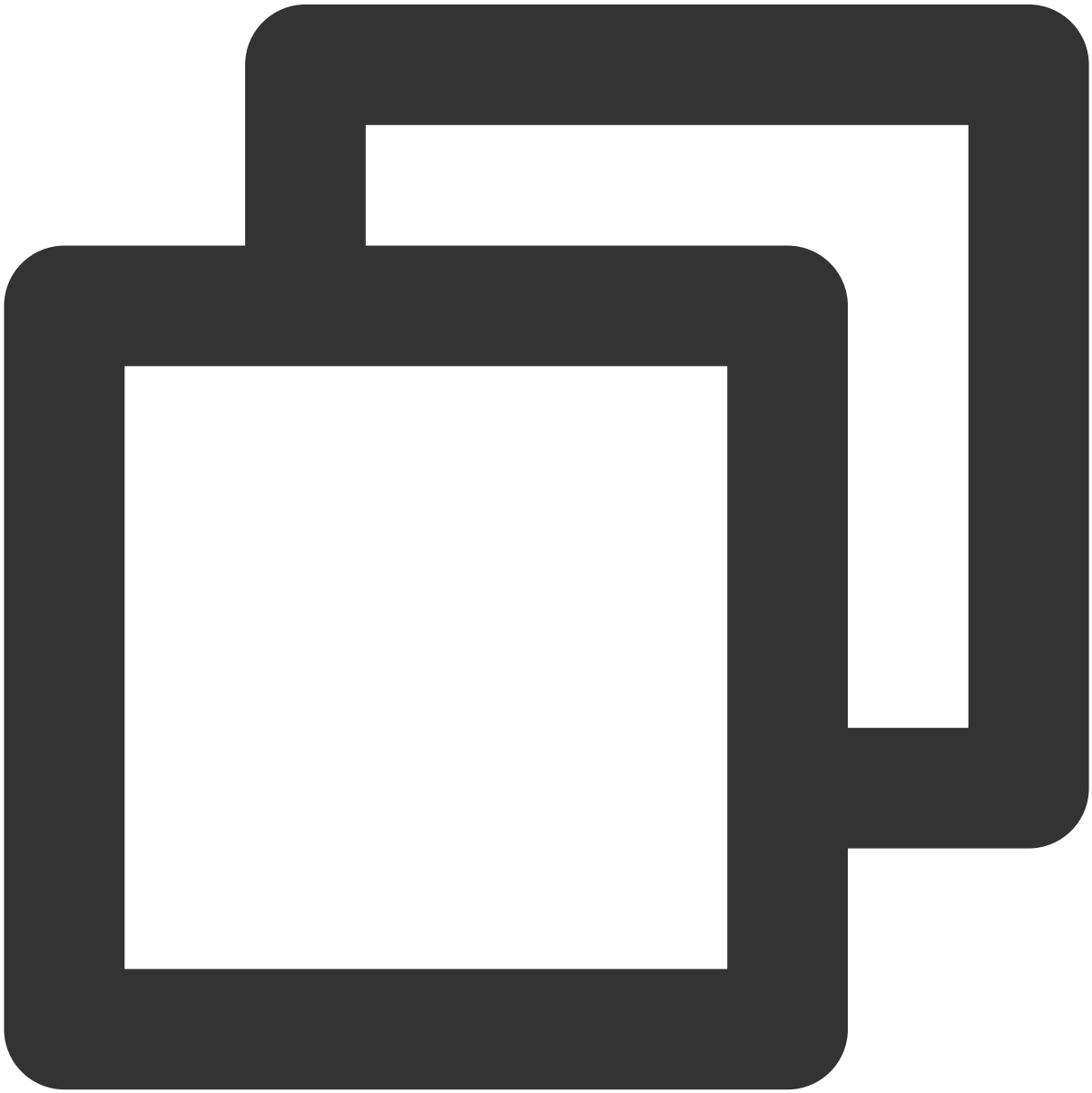
スナップショットロールバックを行うと、スナップショット作成後のデータが失われる場合がありますので、慎重に操作してください。

SSHサービスが正常に稼働するまで、スナップショット作成時間の近い方から遠い方の順に、一度ずつロールバックを試すことをお勧めします。ロールバックを行ってもSSHサービスが正常に稼働しない場合は、それらの時点でシステムにすでに異常が生じていたことを意味します。

SSHサービス起動時エラー fatal: Cannot bind any address

現象の説明

Linuxインスタンスが SSHサービスを起動すると、以下に類似したエラー情報がsecureログファイル内に表示されるか、または直接返されます。



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

問題の原因

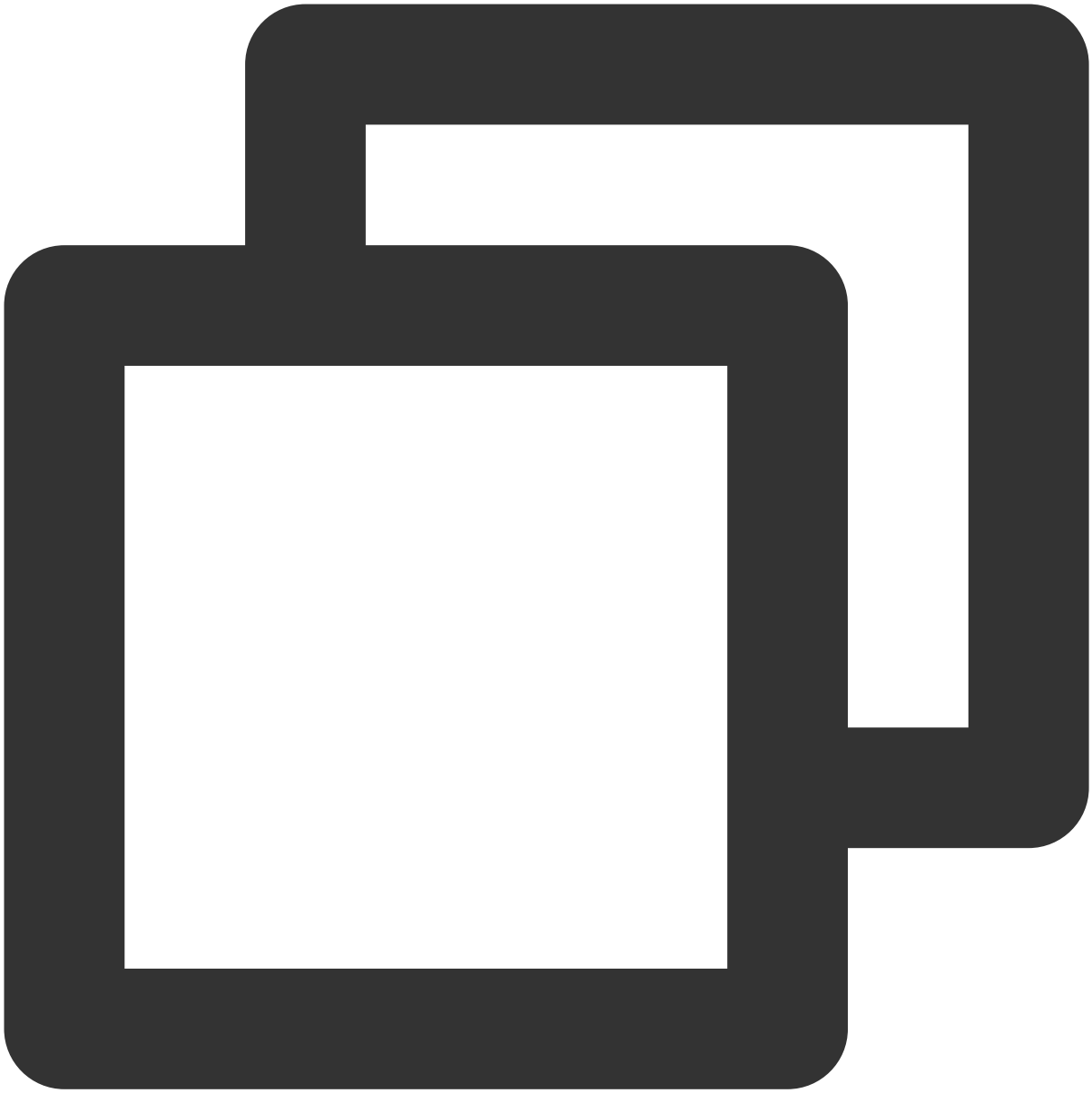
SSHサービスの `AddressFamily` パラメータ設定が不適切なことによるものです。 `AddressFamily` パラメータは運用時に使用するプロトコルスイートの指定に用いられます。パラメータがIPv6のみを設定し、一方でシステム内ではIPv6がアクティブになっていない、またはIPv6の設定が無効になっている場合、この問題が起こる可能性があります。

解決方法

1. 処理手順 を参照して、SSHで設定した `sshd_config` ファイルに進み、 設定を確認します。
2. `AddressFamily` パラメータを変更し、SSHサービスを再起動すれば完了です。

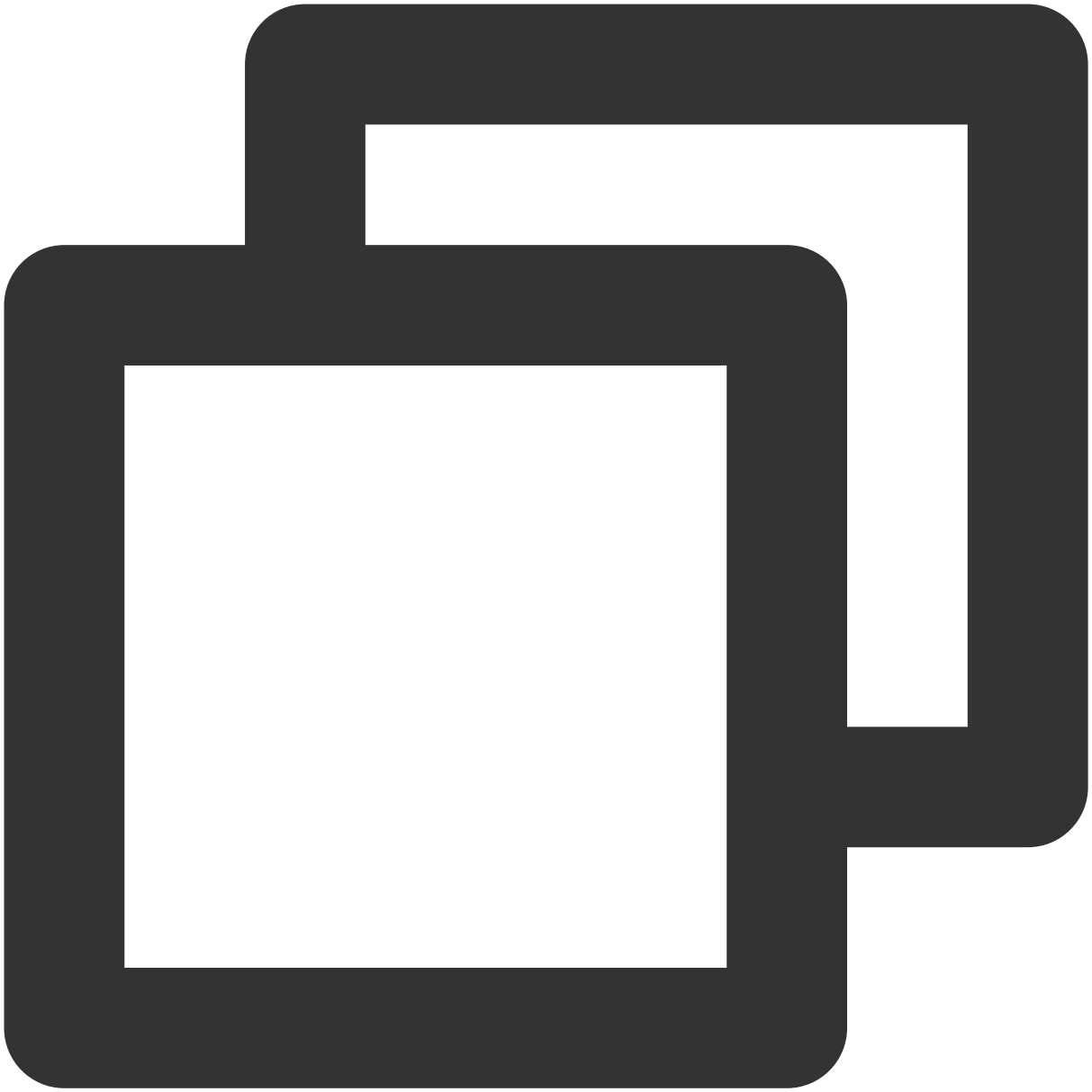
処理手順

1. VNC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、VIMエディタを使用して `sshd_config` 設定ファイルに進みます。



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

3. 以下に類似した設定が含まれていないか確認します。



```
AddressFamily inet6
```

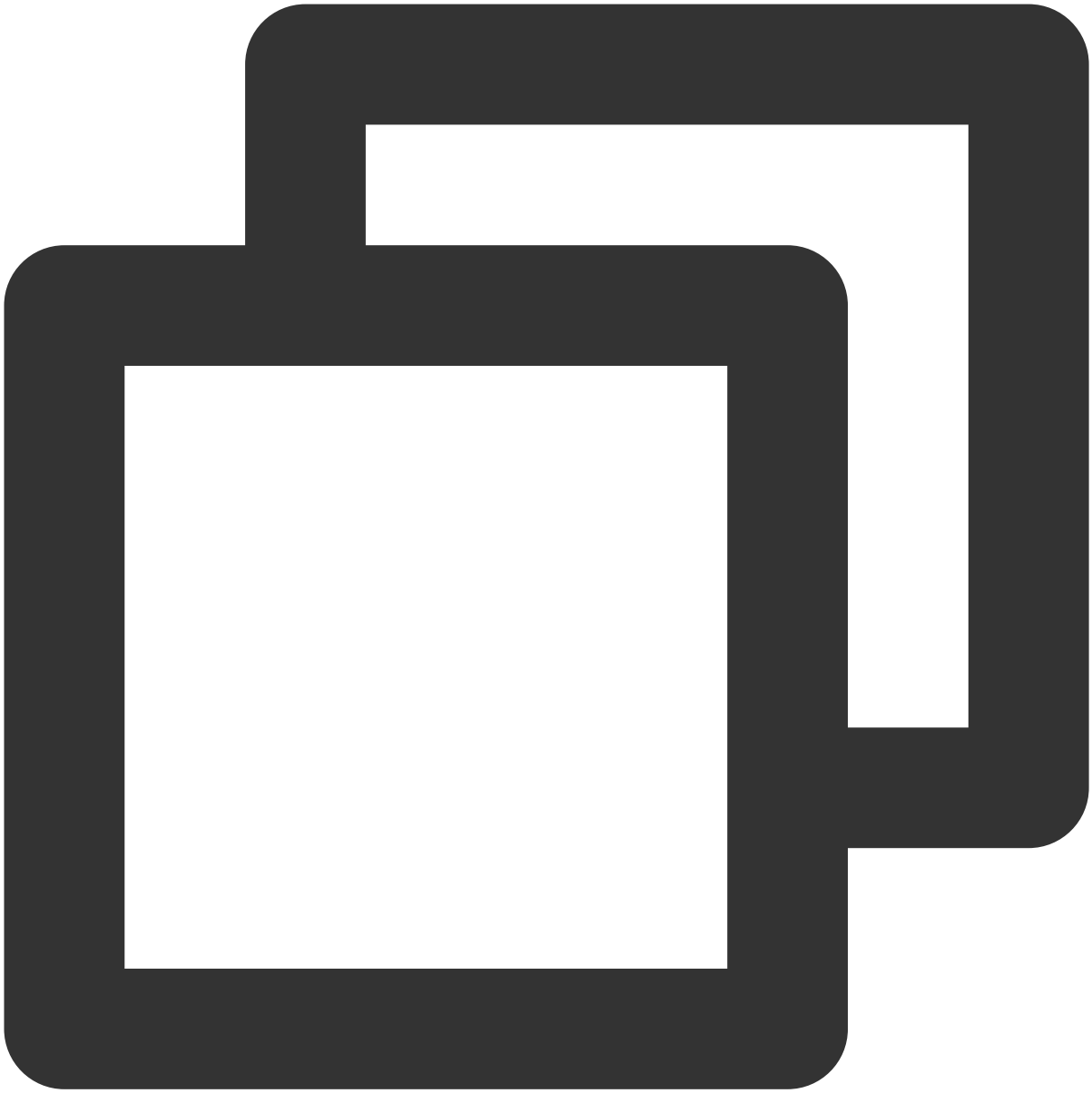
よく用いられるパラメータの説明は次のとおりです。

inet：IPv4プロトコルスイートを使用します。デフォルト値です。

inet6：IPv6プロトコルスイートを使用します。

any：IPv4およびIPv6プロトコルスイートを同時にアクティブにします。

4. **i**を押して編集モードに入り、次の設定に変更するか、または行の先頭に `#` を追加してコメントします。

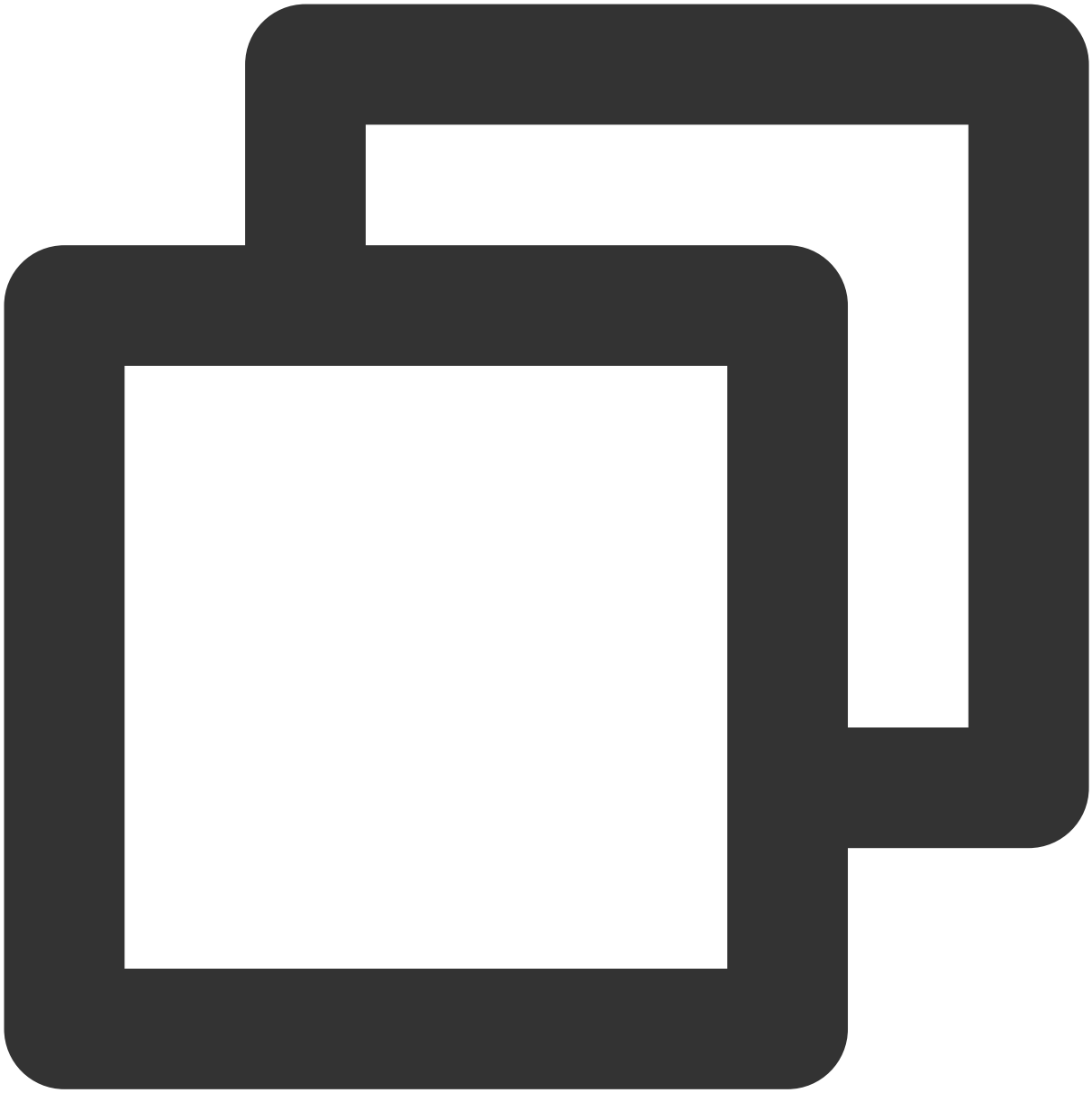


```
AddressFamily inet
```

ご注意：

`AddressFamily` パラメータは `ListenAddress` より前に設定しなければ有効になりません。

5. **Esc**を押して編集モードを終了し、**:wq**を入力して変更を保存します。
6. 以下のコマンドを実行し、SSHサービスを再起動します。



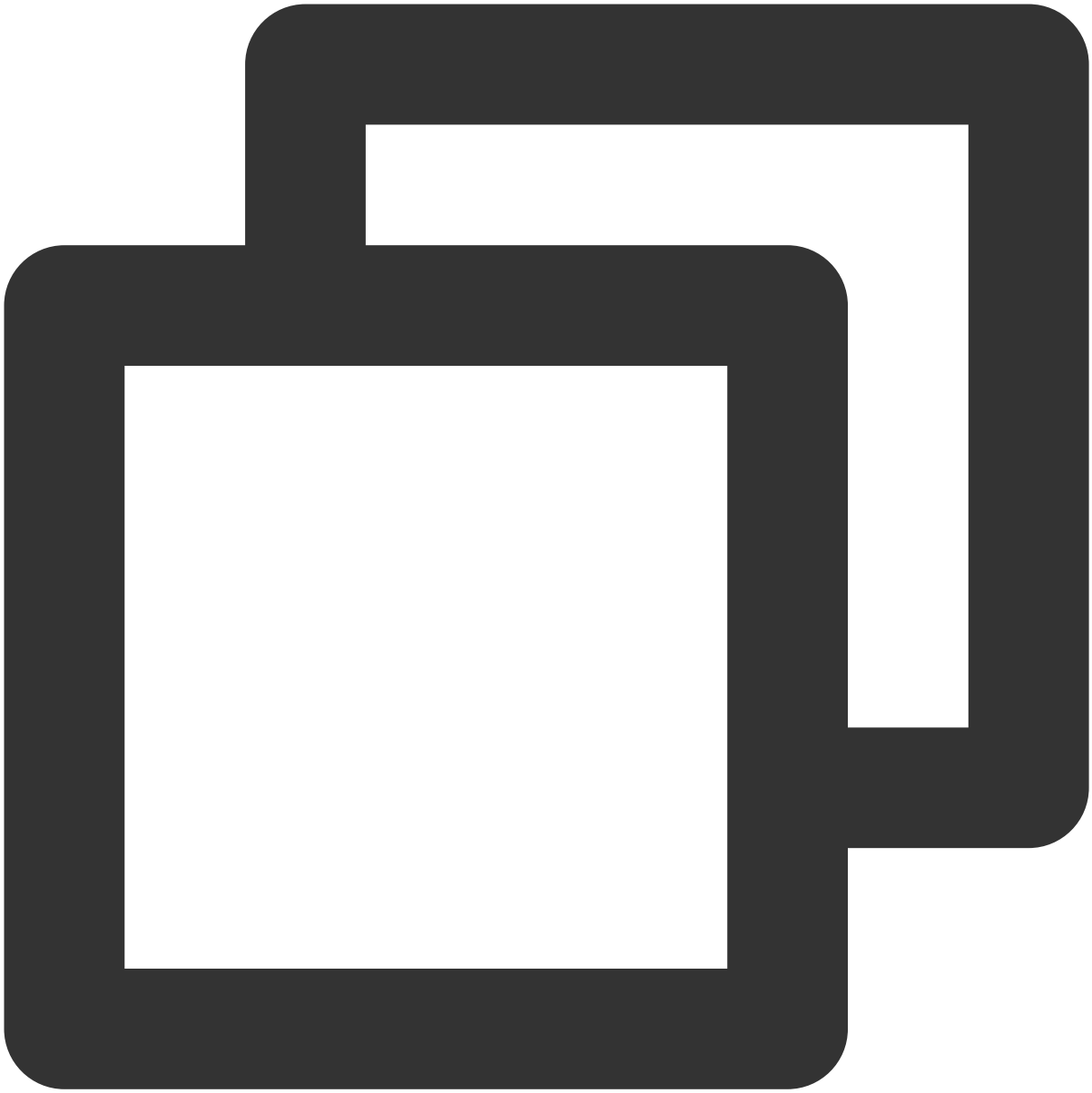
```
service sshd restart
```

SSHサービスを再起動すると、SSHを使用してログインできるようになります。詳細については SSH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。

SSHサービス起動時エラー Bad configuration options

現象の説明

Linuxインスタンスが SSHサービスを起動すると、以下に類似したエラー情報がsecureログファイル内に表示されるか、または直接返されます。



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

問題の説明

設定ファイルにファイルコードまたは設定エラーなどの異常が存在することによるものです。

解決方法

処理手順で提示される以下の処理項目を参照し、sshd_config`設定ファイルを修復します。
エラー情報に対応した設定ファイル変更

外部ファイルのアップロード
SSHサービスの再インストール
スナップショットロールバックによるリカバリ

処理手順

エラー情報に対応した設定ファイル変更

エラー情報の中でエラーのある設定が明確に示されている場合は、VIMエディタによって `/etc/ssh/sshd_config` 設定ファイルを直接変更することができます。他のインスタンスの正しい設定ファイルを参照し、変更を行うことができます。

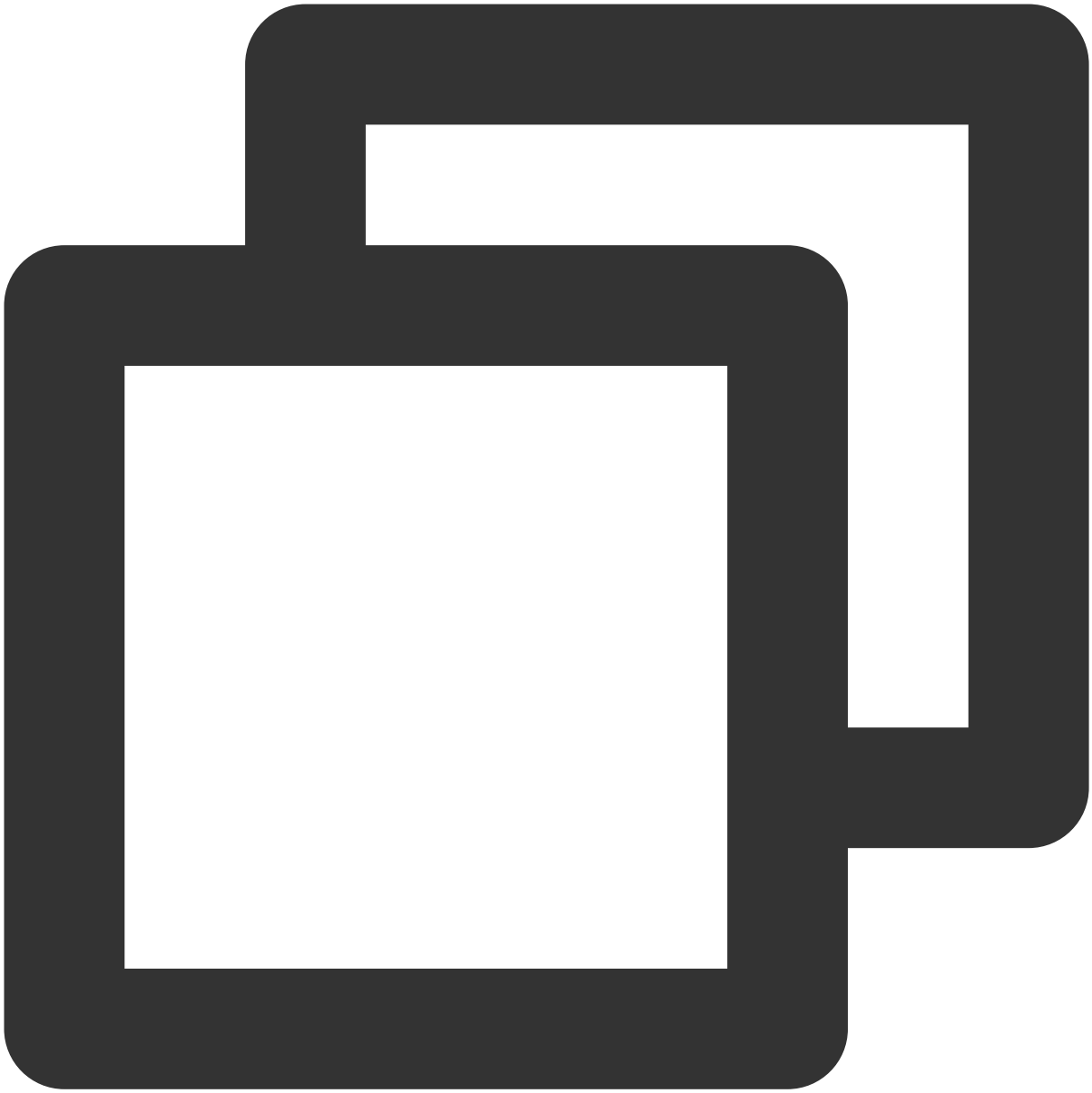
外部ファイルのアップロード

1. FTPソフトウェアにより、他の正常なサーバー上の `/etc/ssh/sshd_config` のライブラリファイルを、目的のサーバーの `\\tmp` ディレクトリにアップロードします。

説明：

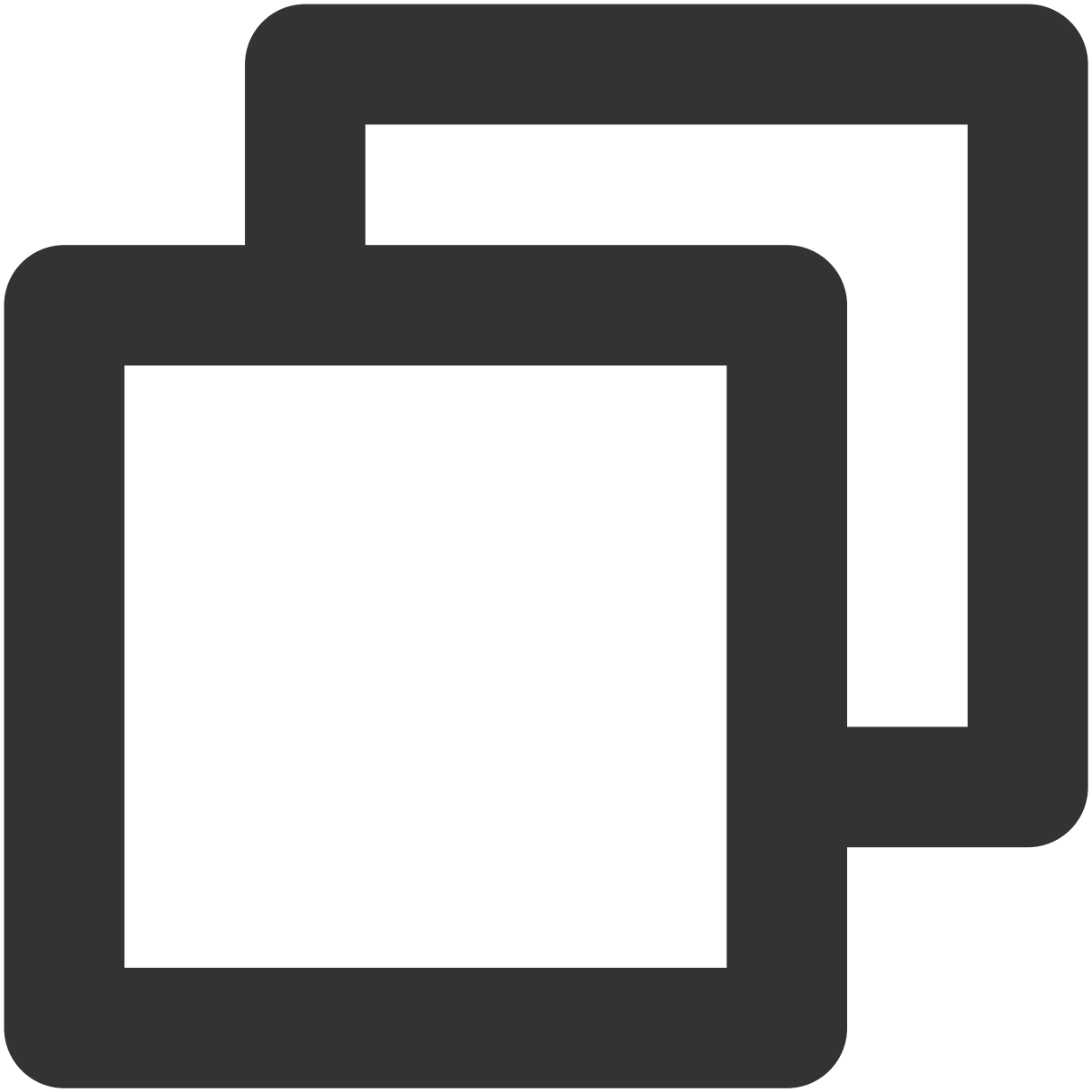
ここでは目的のサーバーの `\\tmp` ディレクトリへのアップロードを例にとりますが、実際の状況に応じて変更することができます。

2. 以下のコマンドを実行し、ライブラリファイルを正常なディレクトリにコピーします。



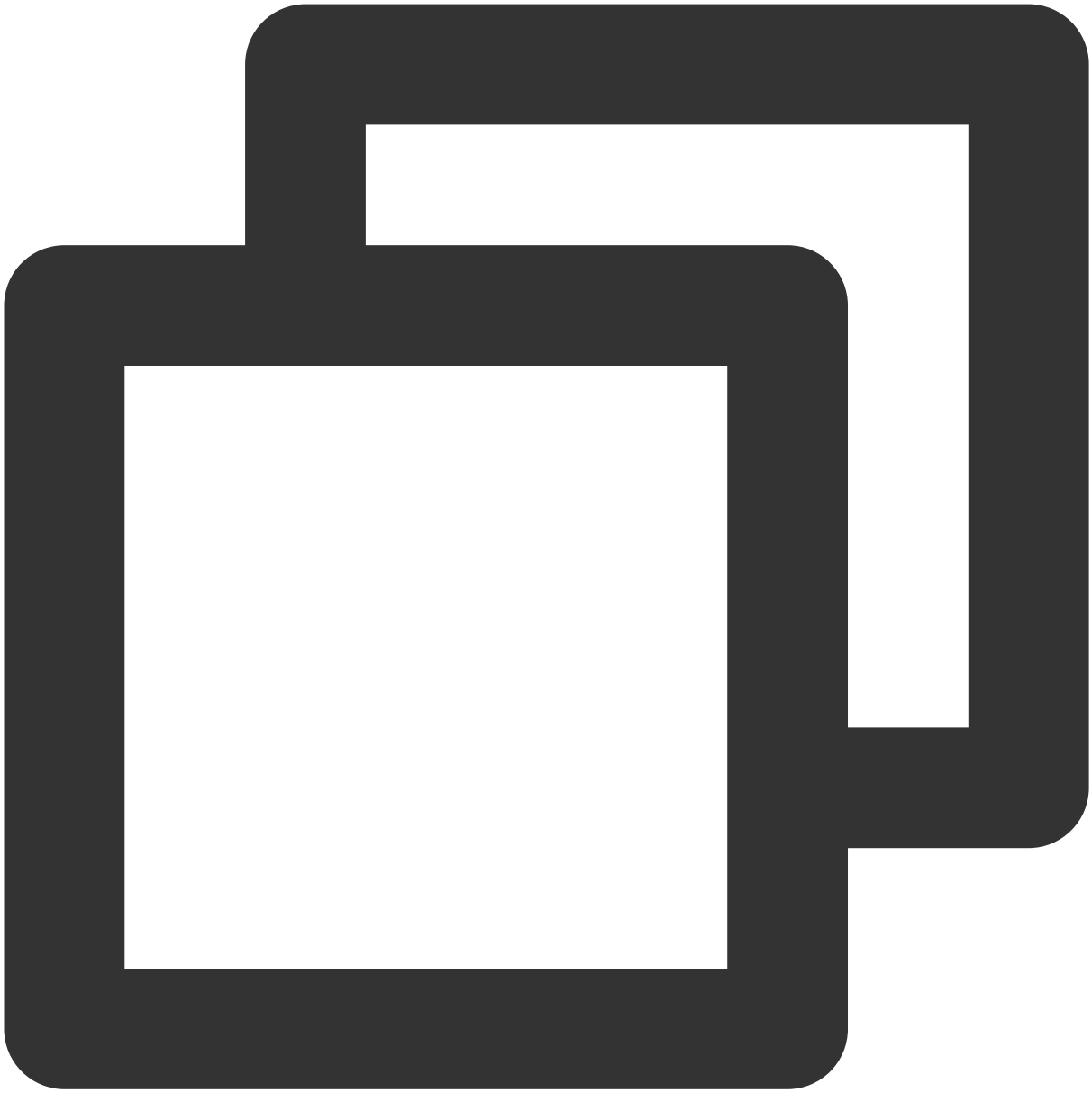
```
cp /tmp/sshd_config /etc/ssh/sshd_config
```

3. 以下のコマンドを順に実行し、ファイルの権限、所有者、グループを変更します。



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

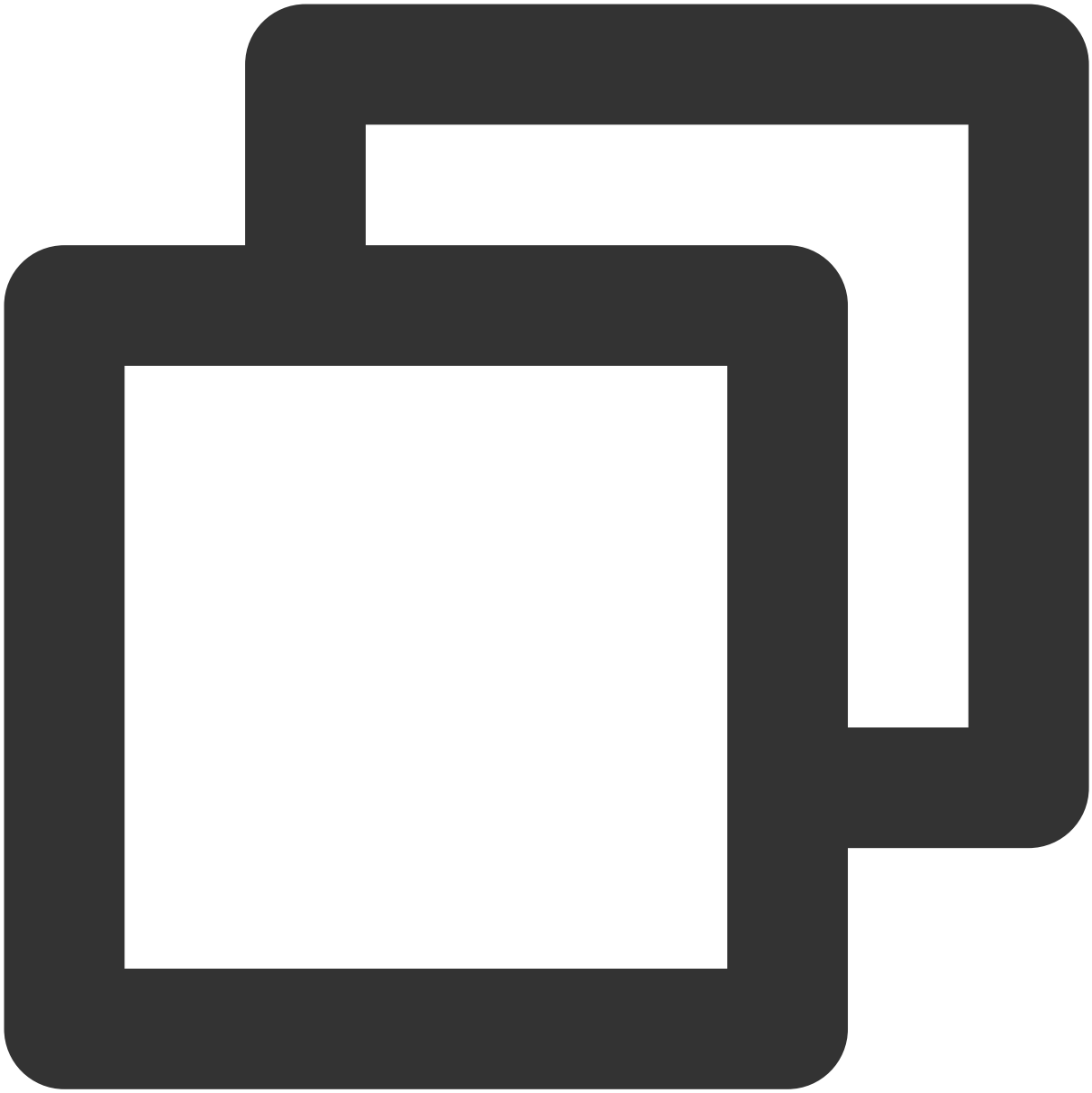
4. 以下のコマンドを実行し、SSHサービスを起動します。



```
service sshd start
```

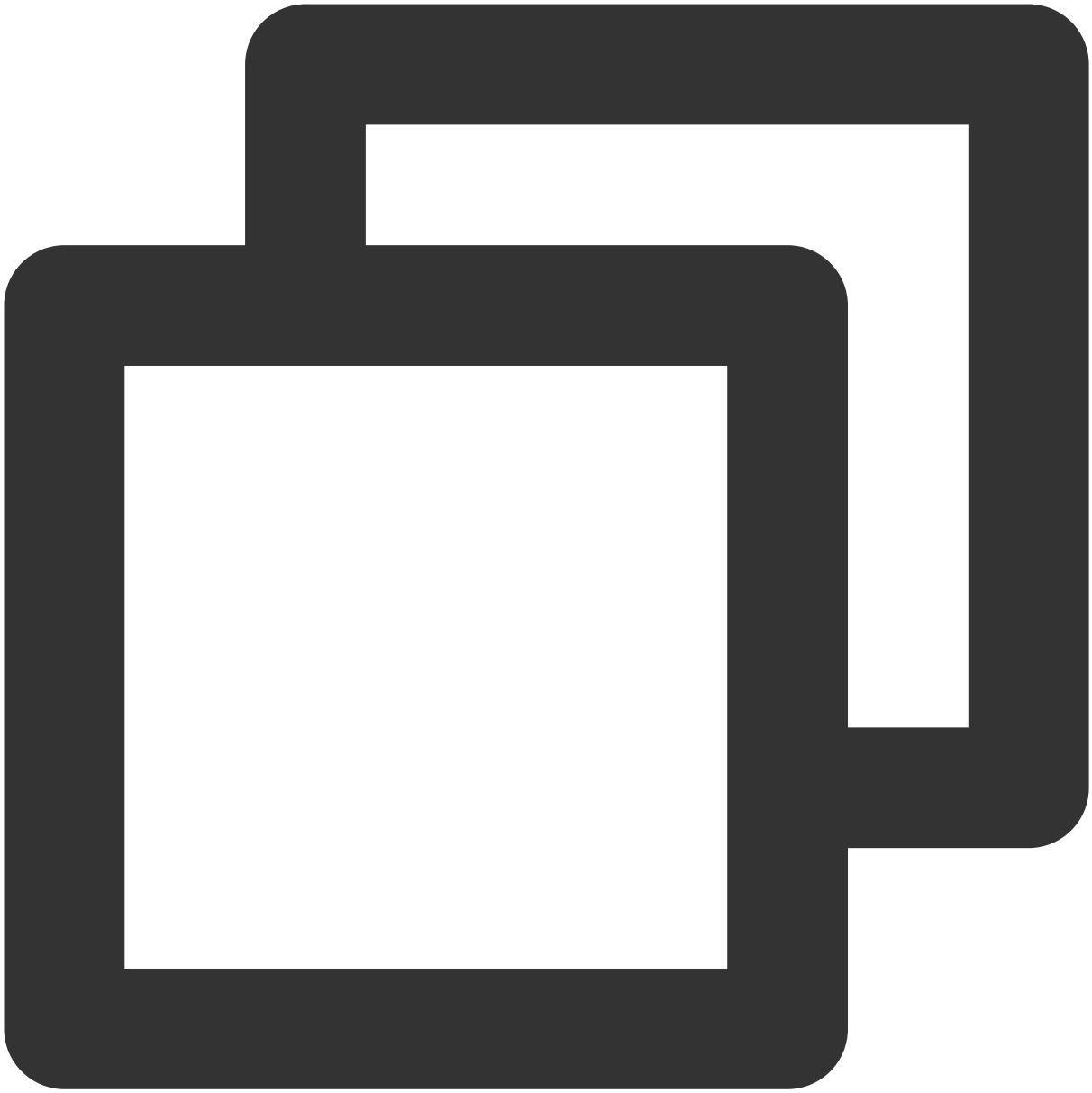
SSHサービスの再インストール

1. VNC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、SSHサービスをアンインストールします。



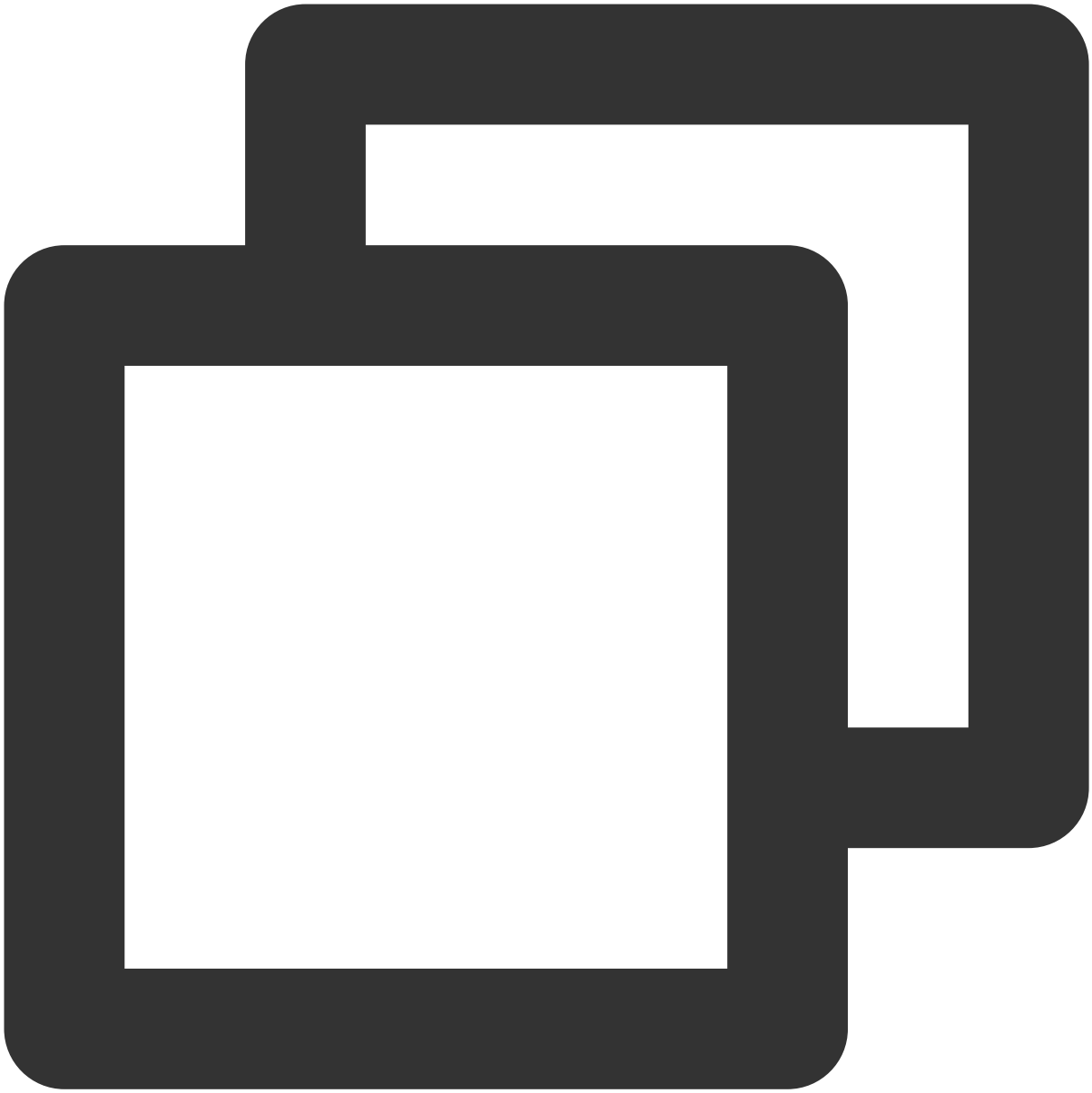
```
rpm -e openssh-server
```

3. 以下のコマンドを実行し、SSHサービスをインストールします。



```
yum install openssh-server
```

4. 以下のコマンドを実行し、SSHサービスを起動します。



```
service sshd start
```

スナップショットロールバックによるリカバリ

インスタンスシステムディスクの過去のスナップショットをロールバックすることで、ライブラリファイルをリカバリすることができます。詳細については、スナップショットからのデータロールバック をご参照ください。

ご注意：

スナップショットロールバックを行うと、スナップショット作成後のデータが失われる場合がありますので、慎重に操作してください。

SSHサービスが正常に稼働するまで、スナップショット作成時間の近い方から遠い方の順に、一度ずつロールバックを試すことをお勧めします。ロールバックを行ってもSSHサービスが正常に稼働しない場合は、それらの時点でシステムにすでに異常が生じていたことを意味します。

若您的问题仍未解决，请通过 提交工单 联系我们寻求帮助。

Linuxインスタンス：CPUまたはメモリの使用率が高いためログインできない

最終更新日：：2022-06-29 15:44:13

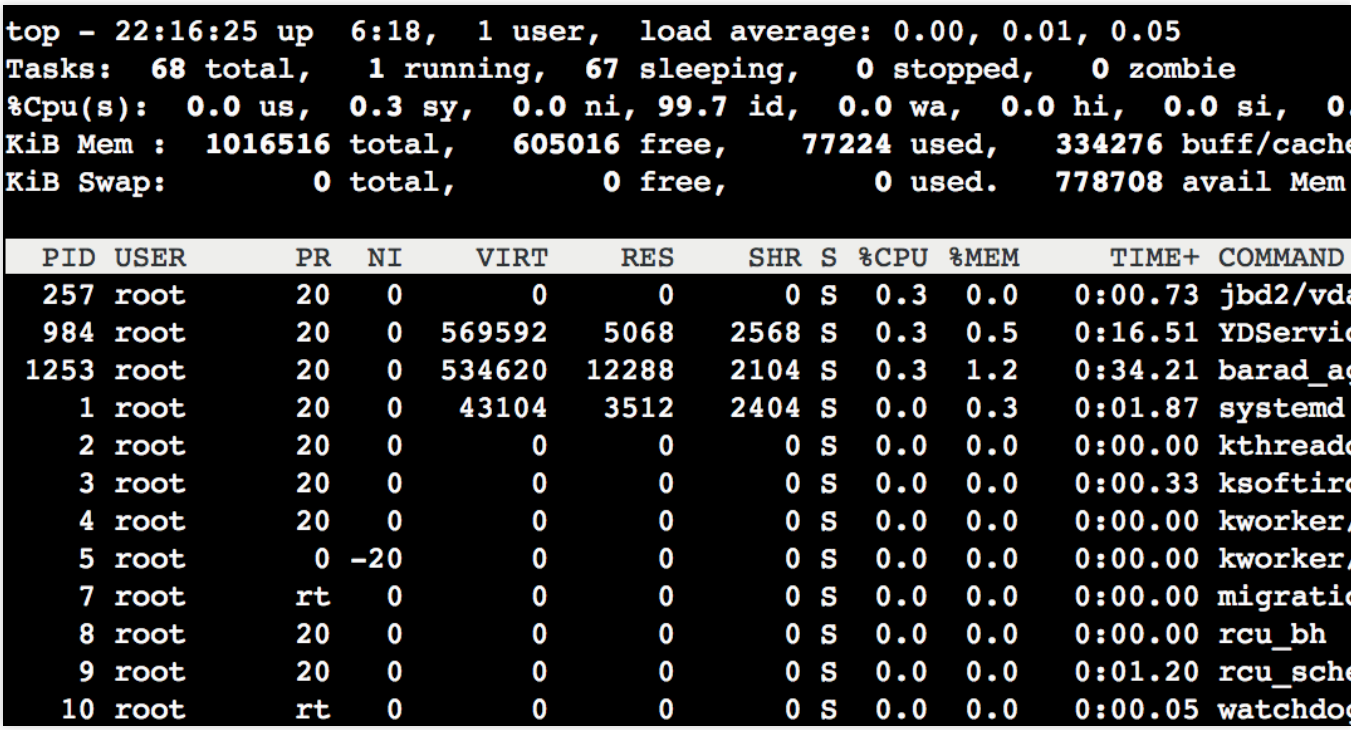
このドキュメントではLinux CVMがCPUまたはメモリの占有率が高いためにログインできない問題のトラブルシューティングおよび対処法についてご説明します。

考えられる原因

CPUまたはメモリの使用率が高すぎると、サービスの応答速度が遅くなる、サーバーにログインできないなどの問題が起こりやすくなります。一方、CPUまたはメモリの使用率が高くなる原因としては、ハードウェアの要因、システムのプロセス、業務のプロセス、トロイの木馬やウイルスなどの要因が考えられます。 Cloud Monitor を使用して、CPUまたはメモリ使用率の閾値アラートを作成し、CPUまたはメモリ使用率が閾値を超えた場合に速やかに通知されるようにすることができます。

特定ツール

Top：Linuxシステムで一般的に使用される監視ツールです。プロセスレベルでのCPUまたはメモリ使用状況をリアルタイムに取得するために用いられます。以下の図はtopコマンドの出力情報の例です。



```
top - 22:16:25 up  6:18,  1 user,  load average: 0.00, 0.01, 0.05
Tasks:  68 total,   1 running,  67 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.3 sy,  0.0 ni, 99.7 id,  0.0 wa,  0.0 hi,  0.0 si,  0
KiB Mem :  1016516 total,   605016 free,    77224 used,   334276 buff/cache
KiB Swap:        0 total,        0 free,        0 used.   778708 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  257 root      20   0       0      0      0 S   0.3   0.0   0:00.73 jbd2/vda
  984 root      20   0  569592   5068   2568 S   0.3   0.5   0:16.51 YDServic
 1253 root      20   0  534620  12288   2104 S   0.3   1.2   0:34.21 barad_ag
    1 root      20   0   43104   3512   2404 S   0.0   0.3   0:01.87 systemd
    2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kthreadd
    3 root      20   0       0      0      0 S   0.0   0.0   0:00.33 ksoftirq
    4 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kworker/
    5 root       0 -20       0      0      0 S   0.0   0.0   0:00.00 kworker/
    7 root      rt   0       0      0      0 S   0.0   0.0   0:00.00 migratio
    8 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_bh
    9 root      20   0       0      0      0 S   0.0   0.0   0:01.20 rcu_sche
   10 root      rt   0       0      0      0 S   0.0   0.0   0:00.05 watchdog
```

Topコマンドの出力情報は主に2つのパートに分かれています。上半分はCPUおよびメモリリソースの全体的な使用状況を表しています。

1行目：システムの現在時刻、現在のログインユーザー数およびシステムの負荷。

2行目：システムの総プロセス数、実行中のプロセス数、ハイバネーション、スリープ、ゾンビプロセスの数。

3行目：CPUの現在の使用状況。

4行目：メモリの現在の使用状況。

5行目：Swap領域の現在の使用状況。

下半分はプロセスの次元でリソースの占有状況を表しています。

PID：プロセスのID。

USER：プロセスの所有者。

PR：プロセスの優先順位 NI：NICE値。NICE値が小さいほど優先順位が高くなります。

VIRT：使用している仮想メモリのサイズ。単位はKB。

RES：現在使用中のメモリのサイズ。単位はKB。

SHR：使用している共有メモリのサイズ。単位はKB。

S：プロセスの状態。

%CPU：更新時間間隔内にプロセスが使用したCPU時間のパーセンテージ。

%MEM：更新時間間隔内にプロセスが使用したメモリのパーセンテージ。

TIME+：プロセスが使用したCPU時間。精度は0.01s。

COMMAND：プロセス名。

障害処理

CVMにログイン

実際のニーズに応じてログイン方式を選択し、CVMにログインします。

サードパーティのソフトウェアによってLinux CVMにリモートログインします。

ご注意：

Linux CVMがCPU高負荷状態にある場合、ログインできない状態になる可能性があります。

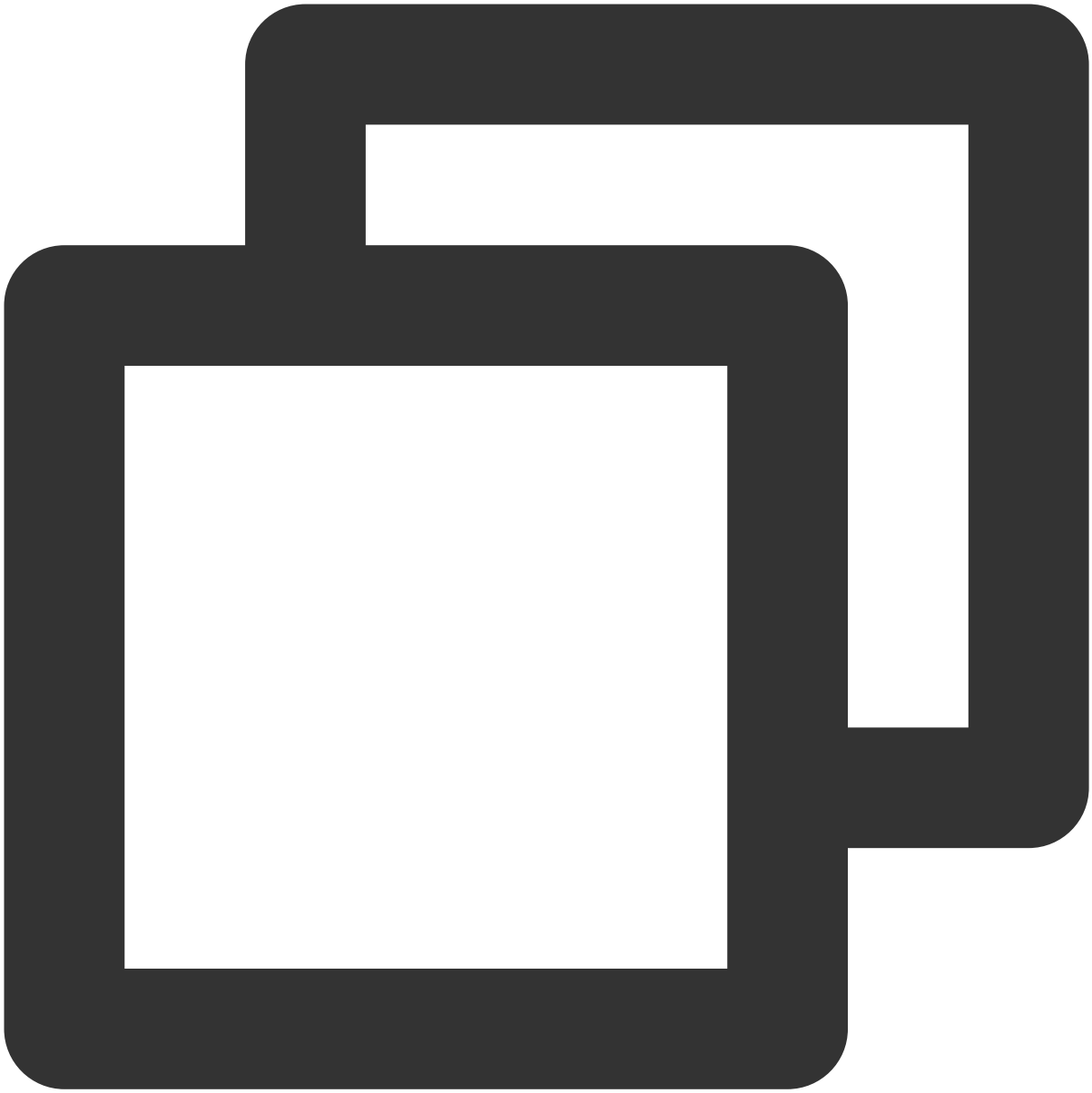
VNCを使用してLinuxインスタンスにログイン します。

ご注意：

Linux CVMがCPU高負荷状態にある場合でも、コンソールで正常にログインできます。

プロセスの占有状況の確認

次のコマンドを実行し、システムの負荷を確認するとともに、 `%CPU` 列と `%MEM` 列に基づいて、比較的多くのリソースを占有しているプロセスを確定します。



```
top
```

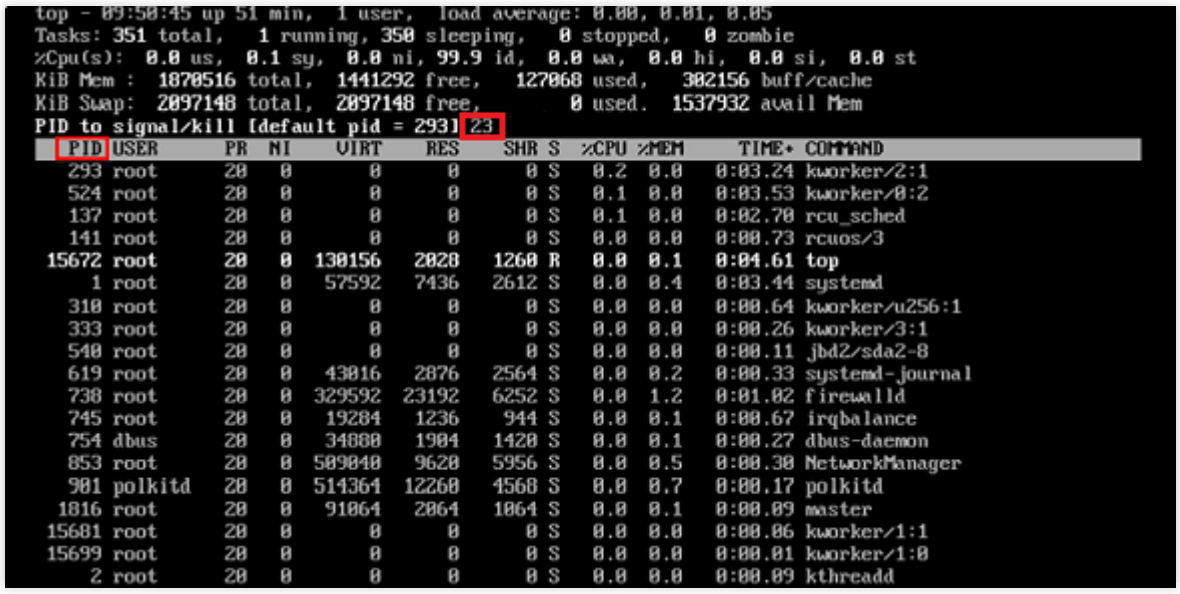
プロセスの分析

タスクマネージャー内のプロセスに基づき、分析とトラブルシューティングを行って、それに応じた対処法をとります。
業務プロセスが大量のCPUまたはメモリリソースを占有している場合は、業務プログラムがスペースを最適化しているかどうかを分析し、最適化またはサーバー設定のアップグレード を行うことをお勧めします。

異常なプロセスが大量のCPUまたはメモリリソースを占有している場合は、インスタンスがウイルスに感染している可能性があります。プロセスを自ら終了するか、またはセキュリティソフトを使用してウイルスの検出と駆除を行い、必要に応じてデータをバックアップし、システムの再インストールを行うことをご検討ください。
Tencent Cloudのコンポーネントプロセスが大量のCPUまたはメモリリソースを占有している場合は、さらなる問題特定と処理を行うため、チケットを提出 してご連絡ください。
一般的なTencent Cloudコンポーネントには次のものがあります。
sap00x：セキュリティコンポーネントプロセス
Barad_agent：監視コンポーネントプロセス
secu-tcs-agent：セキュリティコンポーネントプロセス

プロセスの終了

1. 分析した、リソースを占有しているプロセスの状況に応じて、終了する必要があるプロセスのPIDを記録します。
2. `k` を入力します。
3. 下図のように、終了する必要があるプロセスのPIDを入力し、**Enter**を押します。
ここではPIDが23のプロセスの終了を例にとります。



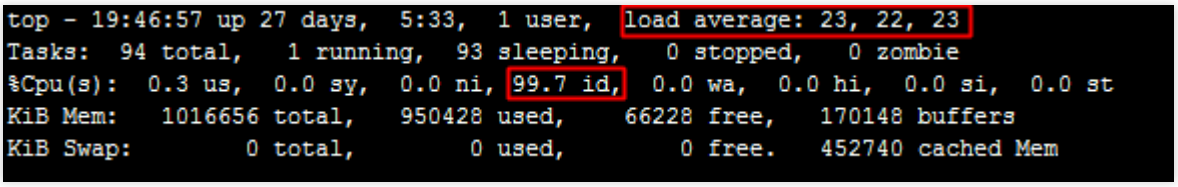
ご注意：
Enterを押した後に `kill PID 23 with signal [15]:` が表示された場合は、続けて**Enter**を押し、デフォルトの設定を維持します。
4. 操作が正常に完了すると、画面に `Send pid 23 signal [15/sigterm]` というメッセージが表示されます。**Enter**を押して確認すれば完了です。

その他の関連障害

CPUがアイドル状態にもかかわらず高負荷な場合の対処

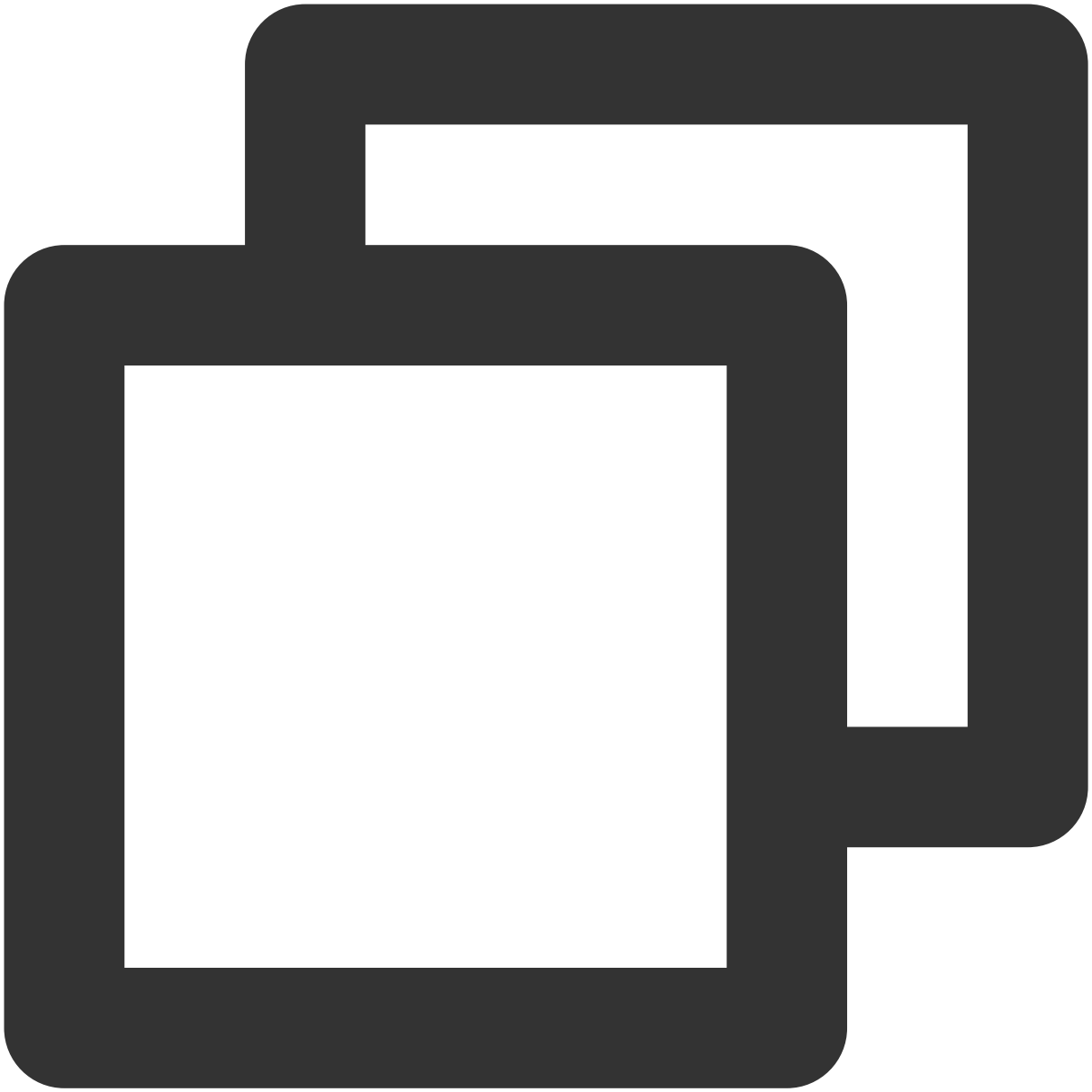
問題の説明

Load averageはCPU負荷の評価であり、その値が高いほど、そのタスクキューが長く、実行待ちのタスクが多いことを表しています。
topによる観察で、下図に類似したものが示された場合は、CPUがアイドル状態にもかかわらず、load averageが非常に高いことを表します。

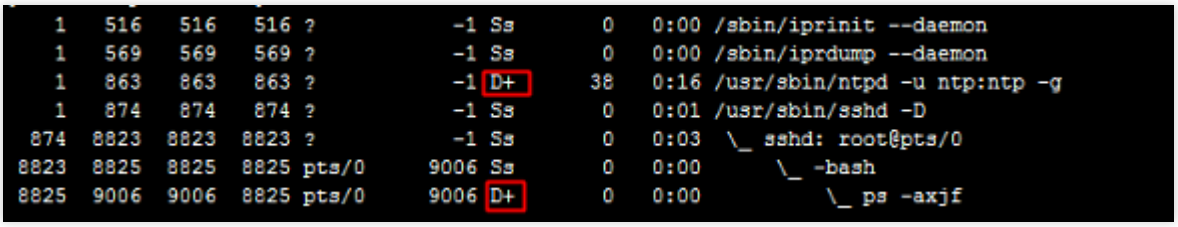


処理方法

下図のように、次のコマンドを実行してプロセスの状態を確認し、D状態のプロセスがないかどうかをチェックします。



```
ps -axjf
```



説明：

D状態とは中断できないスリープ状態を指します。この状態のプロセスは強制終了することができず、自ら終了することもできません。

プロセスにD状態が多く発生している場合は、プロセスの依存リソースを元に戻すか、またはシステムを再起動することで解決できます。

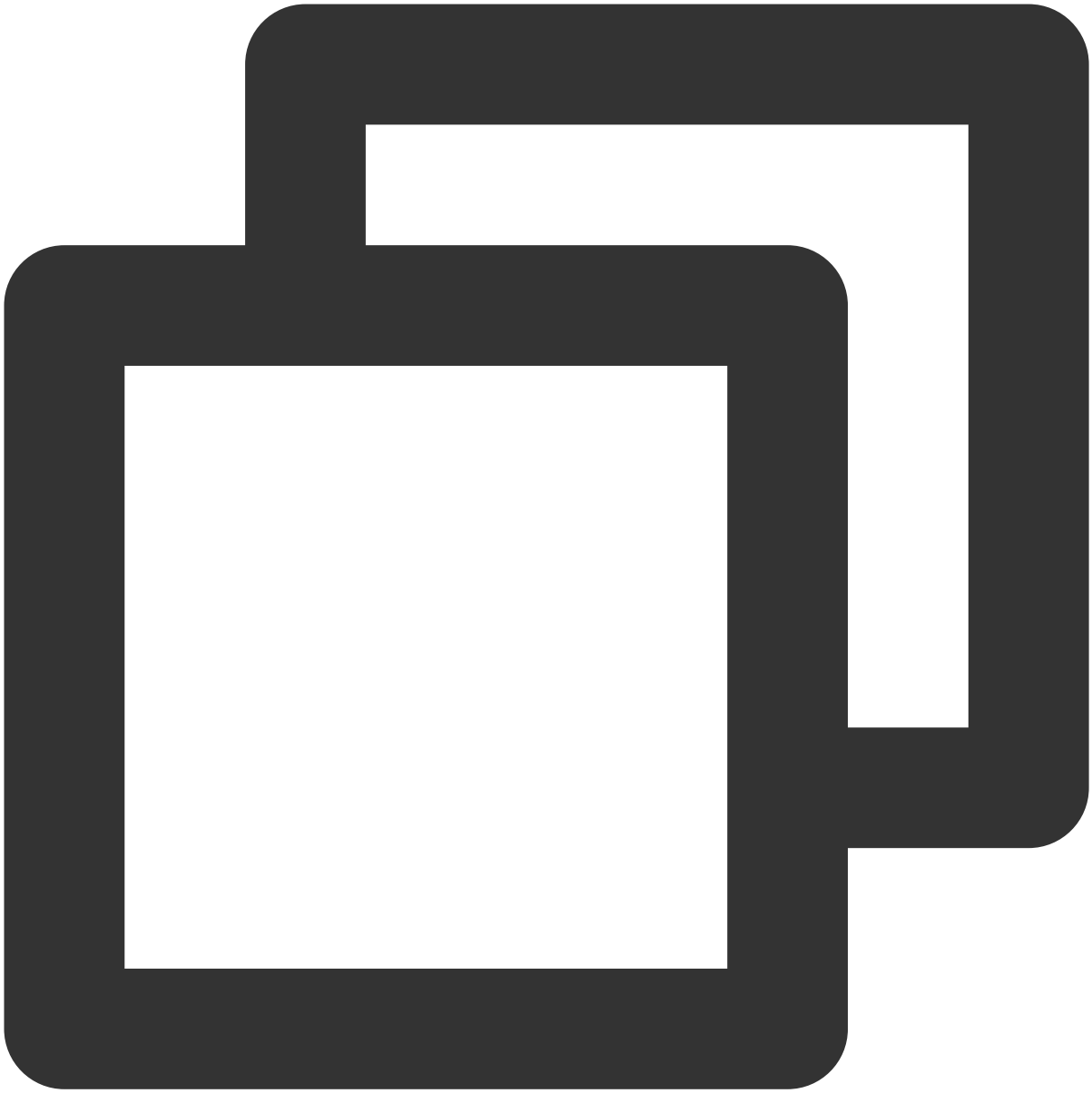
Kswapd0プロセスによるCPU占有が比較的高い場合の対処

問題の説明

Linuxシステムはページングのメカニズムによってメモリを管理すると同時に、ディスクの一部を分割して仮想メモリに充てています。一方、kswapd0はLinuxシステムの仮想メモリ管理においてページ切り替えを担当するプロセスです。システムのメモリが不足している場合、kswapd0は頻繁にページ切り替え操作を行います。ページ切り替え操作はCPUリソースを非常に消費するため、このプロセスは多くのCPUリソースを継続的に占有します。

処理方法

1. 次のコマンドを実行し、kswapd0プロセスを見つけます。



```
top
```

2. kswapd0プロセスの状態を観察します。

継続して非スリープ状態にあり、なおかつ実行時間が比較的長く、比較的多くのCPUリソースを継続的に占有している場合は、 ステップ3を実行し、メモリの占有状況を確認してください。

3. `vmstat` 、 `free` 、 `ps` などのコマンドを実行し、システム内のプロセスのメモリ占有状況を照会します。

メモリの占有状況に応じて、システムの再起動または不要かつ安全なプロセスの終了を行います。si、soの値が比較的高い場合は、システムに頻繁なページ切り替え操作が存在し、現在のシステムの物理メモリがニーズを満たせなくなっていることを示しています 。システムメモリのアップグレードをご検討ください。

Linuxインスタンス：ポートの問題によるログインができない

最終更新日：：2023-06-08 17:03:09

このドキュメントでは、Cloud Virtual Machineがポートの問題によりリモートログインできない場合のトラブルシューティングと解決案について説明します。

説明：

以下の操作では、 CentOS 7.6 システムを使用したCVMを例として説明します。

検証ツール

Tencent Cloudが提供するツールを使用して、ログインできない問題はポートとセキュリティグループの設定に関連しているかどうかを判断することができます：

自己診断

インスタンスポート検証ツール

セキュリティグループの設定の問題が検出された場合は、インスタンスポート検証ツール 中の**Port Verification** 機能を介して、関連するポートを開放し、再度ログインを試みます。ポートを開放してもまだログインできない場合、以下の内容を参照して原因を特定します。

トラブルシューティング

ネットワーク接続の状態を確認する

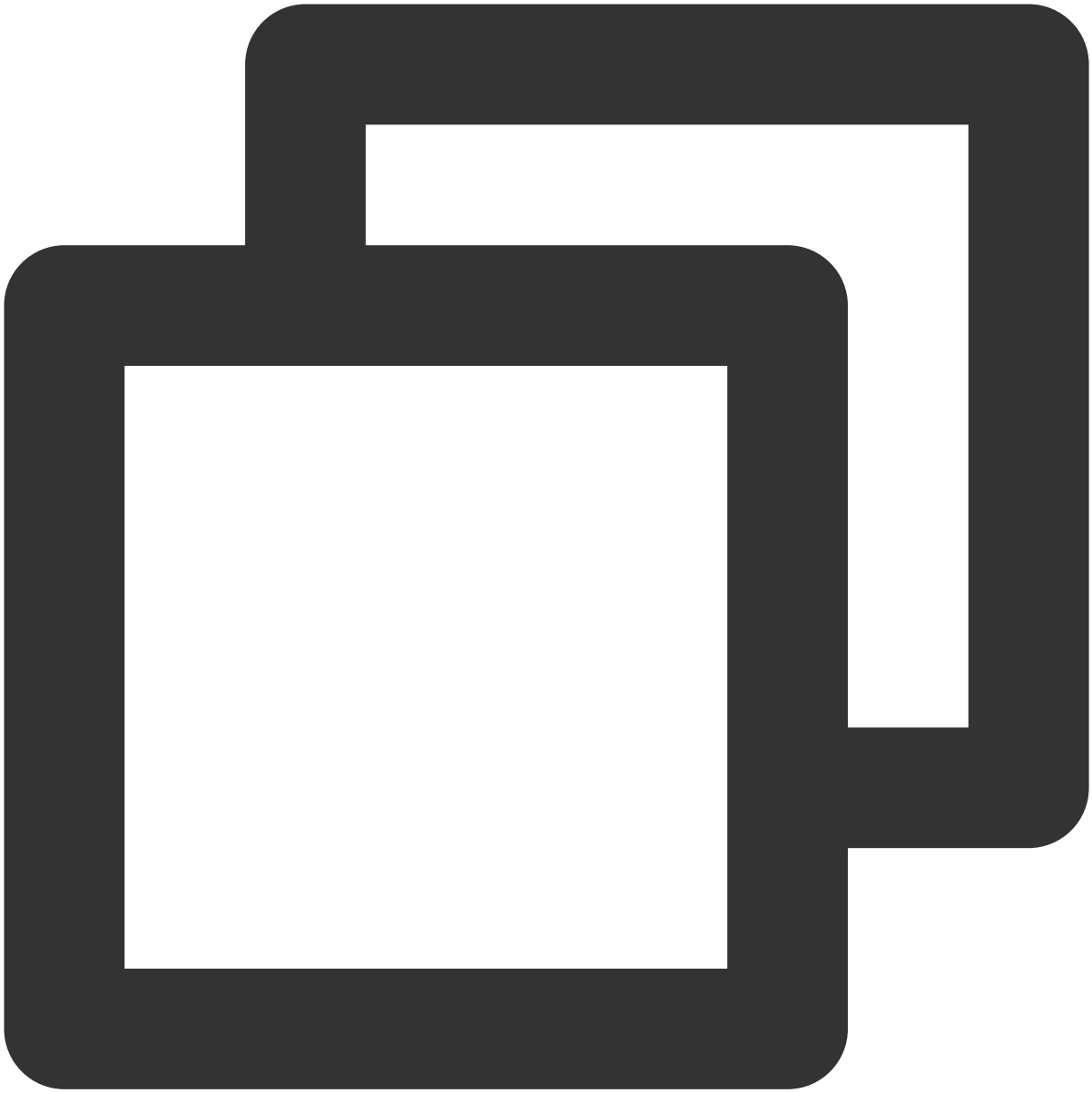
Pingコマンドを使用して、ネットワーク接続をテストすることができます。同時に、異なるネットワーク環境（異なるIPレンジ或いはキャリア）のコンピューターでテストを行い、ローカルネットワークの問題なのか、サーバーの問題なのかを確認できます。

1. ローカルコンピューターでコマンドラインツールを開きます。

Windows システム：スタート>ファイル名を指定して実行をクリックし、「cmd」と入力すると、コマンドラインダイアログボックスが表示されます。

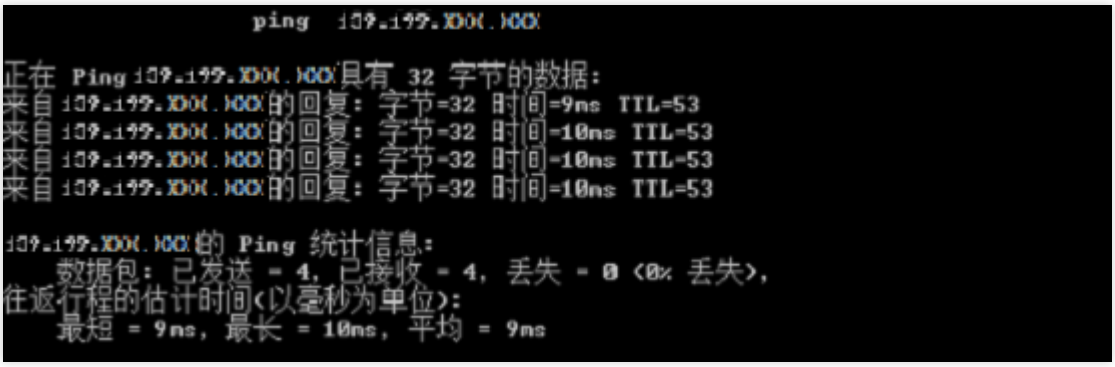
Mac OS：Terminalツールを開きます。

2. 以下のコマンドを実行して、ネットワーク接続をテストします。



```
ping + CVM インスタンスのパブリックIP アドレス
```

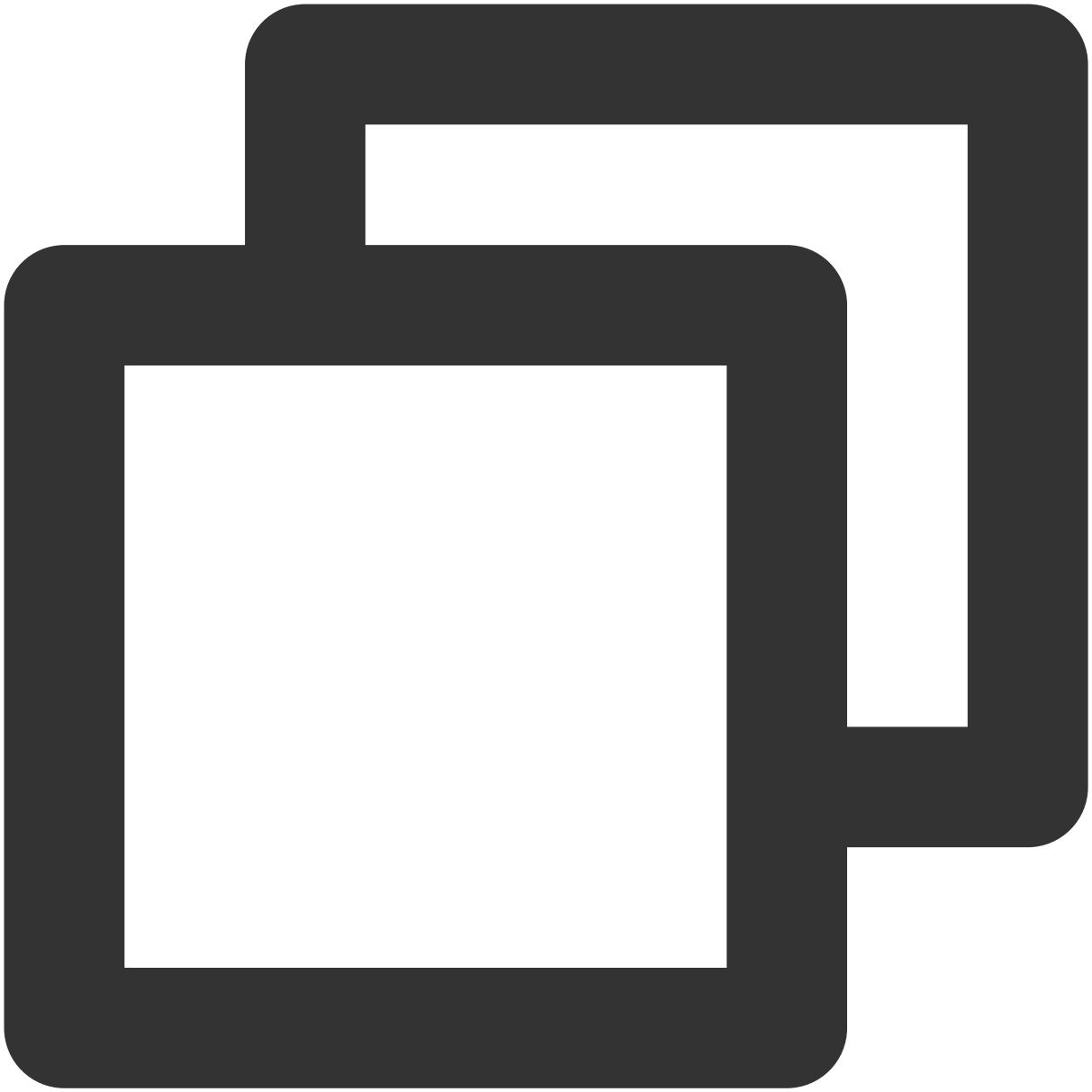
インスタンスのパブリックIPアドレスを取得する方法については、 パブリックIPアドレスの取得 をご参照ください。たとえば、 `ping139.199.XXX.XXX` コマンドを実行します。
ネットワークが正常であれば、次のような結果が返されます。



「要求がタイムアウトしました」と表示される場合、ネットワーク接続に問題があることを表しています。この場合、インスタンスIPアドレスへの Ping の失敗 ドキュメントを参考にトラブルシューティングを行ってください。

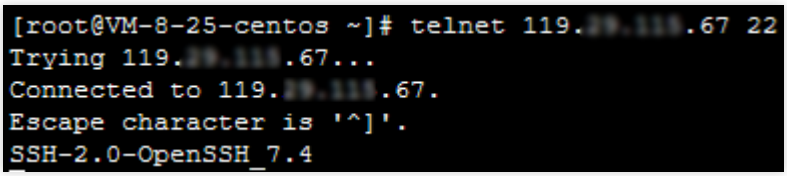
インスタンスポートの接続を確認する

1. VNCを使用してCVM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。
2. 以下のコマンドを実行し、**Enter**キーを押して、リモートポートの開放状態をテストし、ポートにアクセスできるかどうかを判断します。

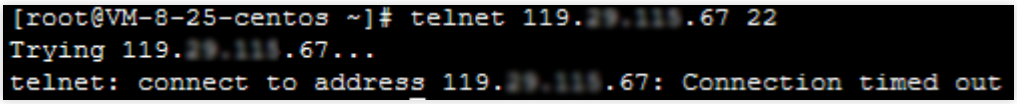


```
telnet + CVM インスタンスのパブリックIP アドレス + ポート番号
```

例えば、 `telnet 119.XX.XXX.67 22` コマンドを実行して、ポート番号22への接続をテストします。
通常の状況：次の図に示すような情報が返され、ポート22にアクセスできます。



異常な状況：次の図に示すような情報が返され、ポート22にアクセスできないことを示します。インスタンスのファイアウォールまたはセキュリティグループがポート22を許可しているかどうかなど、問題のあるネットワークの対応する部分を確認してください。



sshdサービスを確認する

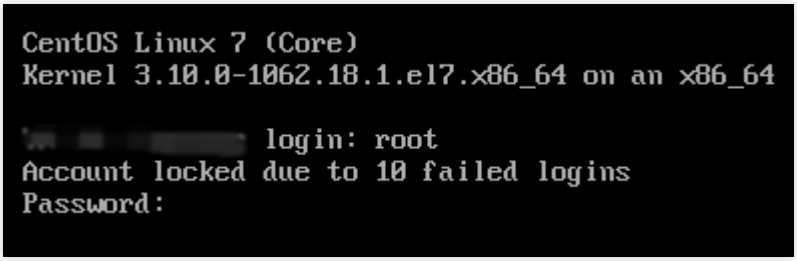
SSHを使用してLinuxインスタンスにログイン すると、「接続できない」「接続に失敗しました」というメッセージが表示された場合、sshdポートが監視されていないか、sshdサービスが開始されていないことが原因である可能性があります。この場合、SSH経由でLinuxインスタンスにログインできない時の解決策ドキュメントを参考にトラブルシューティングを行ってください。

Linuxインスタンス：VNCログインエラー Module is unknown

最終更新日：：2023-06-08 17:19:36

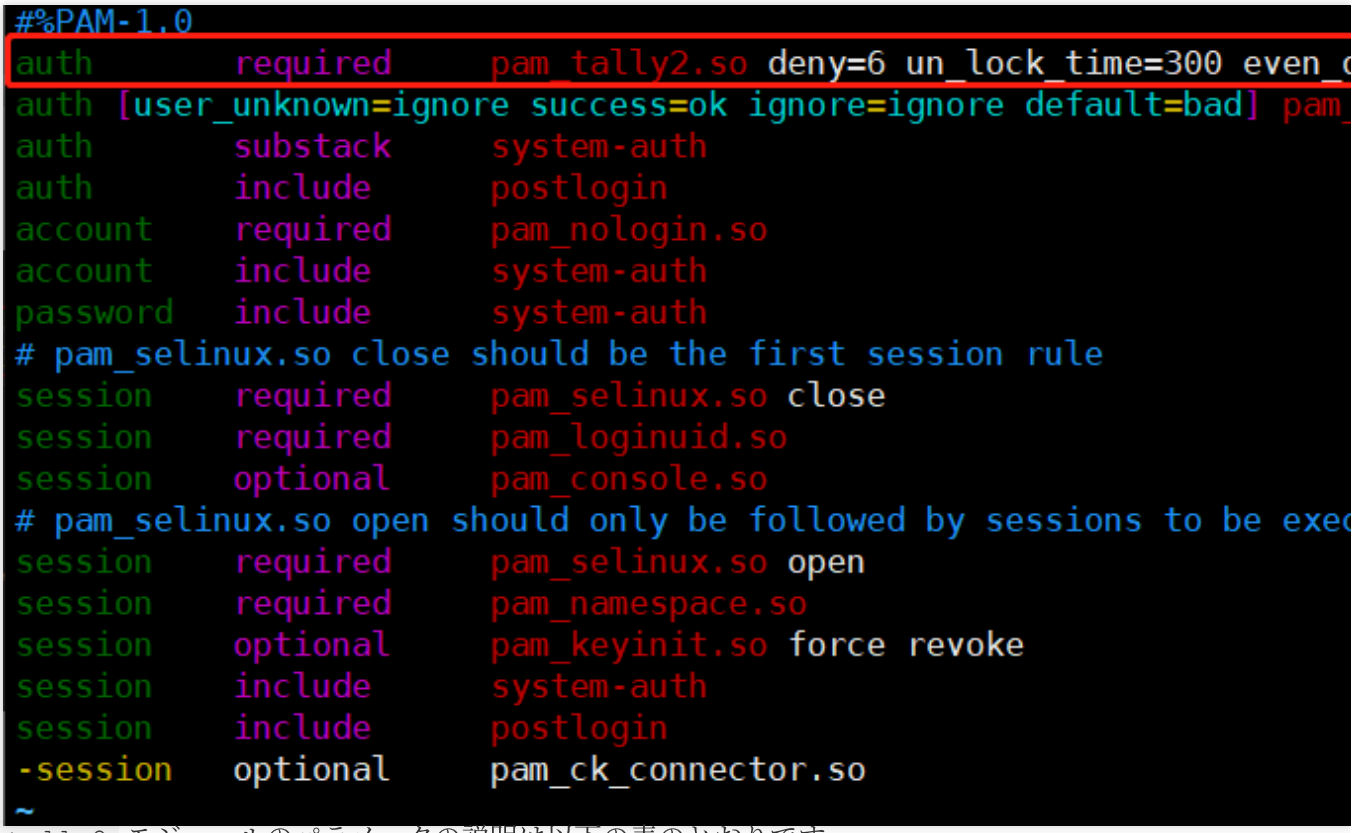
現象の説明

VNCを使用してCVMに正常にログインできず、ログインパスワードを入力する前にエラーメッセージ「Account locked due to XXX failed logins」が表示される（下図参照）。



考えられる原因

VNCを使用したログインでは `/etc/pam.d/login` というpamモジュールを呼び出して検証を行います。一方、login設定ファイルには `pam_tally2.so` モジュールの認証が存在します。 `pam_tally2.so` モジュールの機能は、LinuxユーザーがN回連続して誤ったパスワードを入力してログインを行った場合、自動的にX分間ロック、または永続的にロックを行うものです。このうち永続的なロックは手動で解除する必要があり、これを行わなければロックされたままとなります。
ログインの失敗が設定された試行回数を超えた場合、ログインアカウントは一定の時間ロックされるほか、総当たり攻撃が行われた場合はアカウントがロックされてログインできなくなる可能性もあります。下図は設定されているログイン試行可能回数です。



`pam_tally2` モジュールのパラメータの説明は以下の表のとおりです。

パラメータ	説明
deny=n	ログイン失敗回数がn回を超えた後はアクセスが拒否されます。
lock_time=n	ログイン失敗後にロックされる時間（秒）。
un lock_time=n	ログイン失敗回数が制限を超えた後、ロック解除に要する時間。
no_lock_time	ログファイル /var/log/faillog 中に .fail_locktime フィールドが記録されていません。
magic_root	rootユーザー（uid=0）がこのモジュールを呼び出した場合、カウンターの数値は増えません。
even_deny_root	rootユーザーのログイン失敗回数がdeny=n回を超えた後はアクセスが拒否されます。
root_unlock_time=n	even_deny_root に対応するオプション。このオプションを設定した場合の、rootユーザーのログイン失敗回数が制限を超えた後のロック時間。

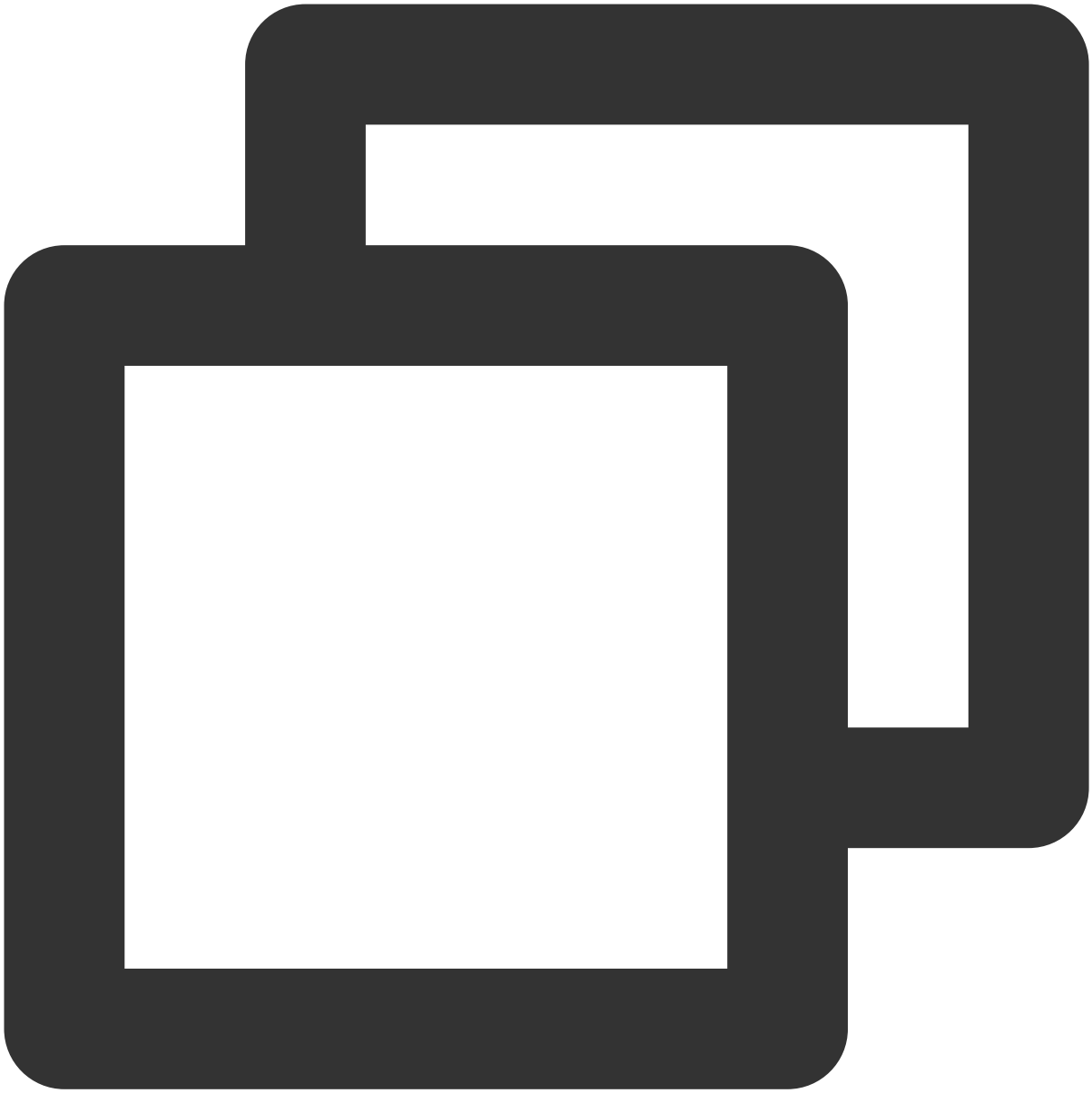
解決方法

1. 処理手順 を参照し、login設定ファイルに入り、 `pam_limits.so` モジュール設定に一時的なコメントを付加します。

2. アカウントがロックされた原因を確認し、セキュリティポリシーを強化します。

処理手順

1. SSHを使用したCVMインスタンスへのログインを試してください。詳細については SSH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。
ログインに成功した場合は次の手順に進みます。
ログインに失敗した場合は、単一ユーザーモードを使用する必要があります。
2. ログイン成功後、次のコマンドを実行してログ情報を確認します。

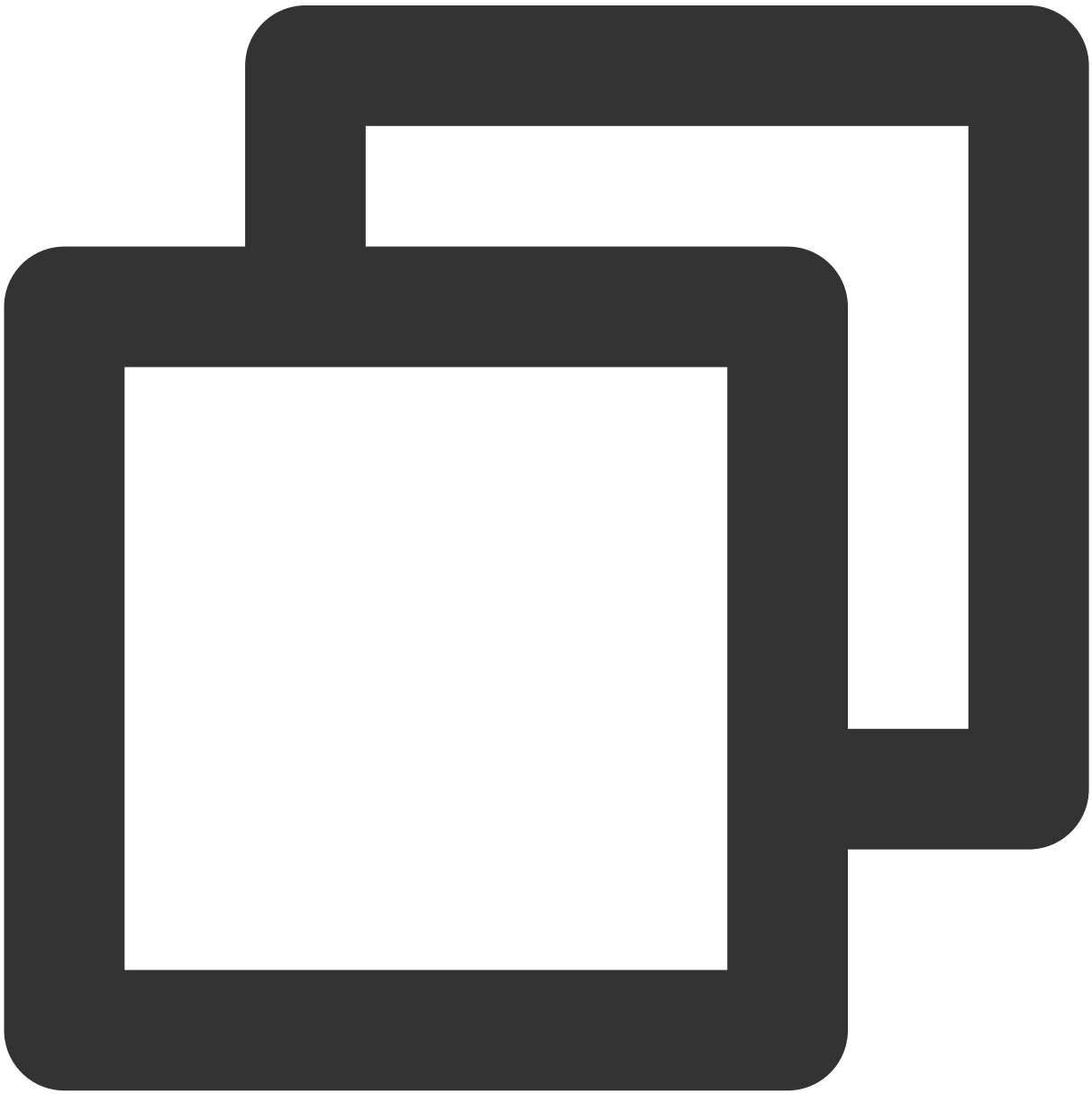


```
vim /var/log/secure
```

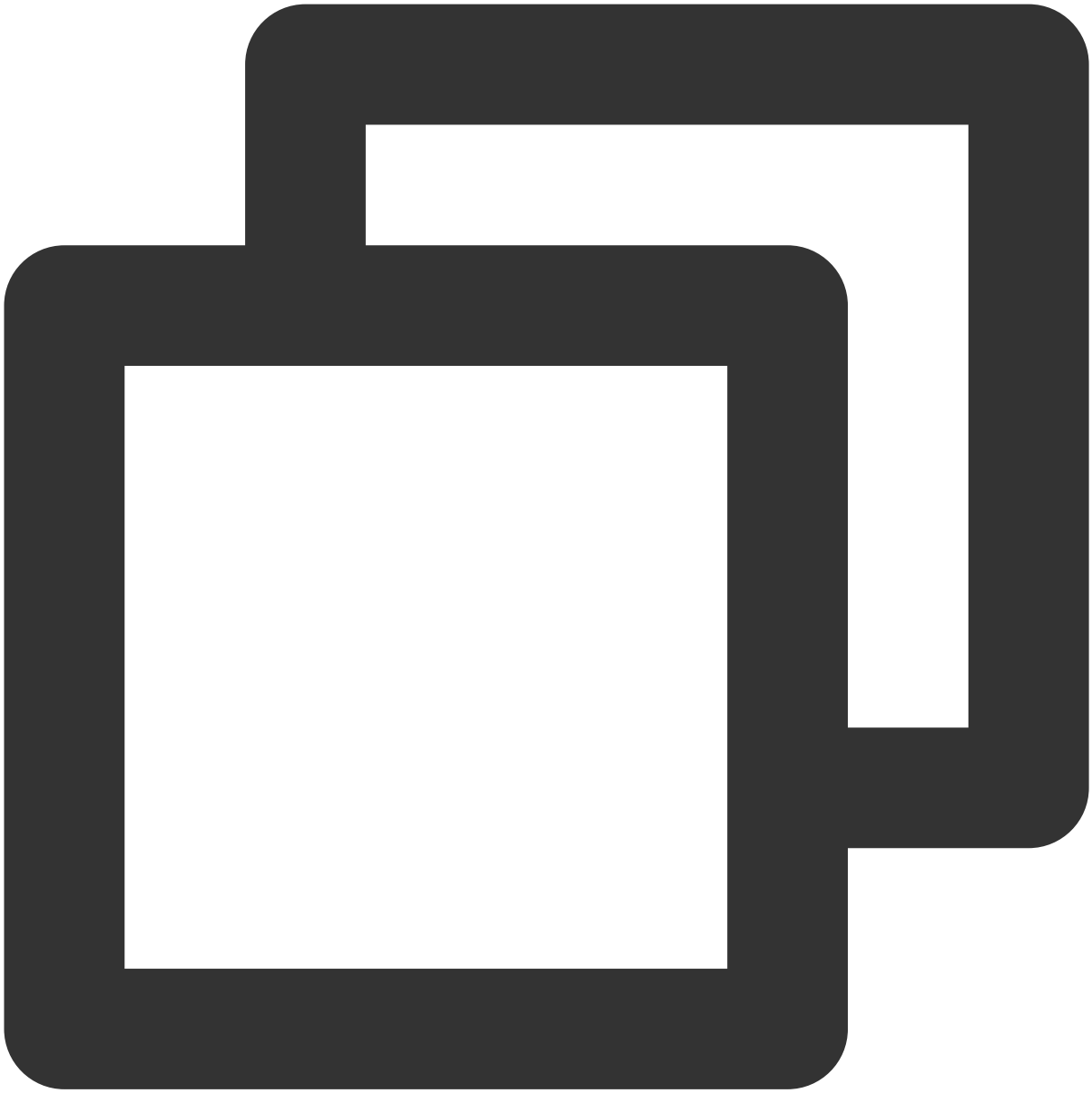
このファイルは一般的にセキュリティに関する情報の記録に用いられ、このうち大部分の記録はユーザーのCVMログインの関連ログです。下図のように、情報の中から `pam_tally2` のあるエラーメッセージを取得することができます。

```
Oct 28 17:14:45 VM-96-4-centos sshd[16704]: Failed password for invalid user dell from 202.153
Oct 28 17:14:45 VM-96-4-centos sshd[16704]: Received disconnect from 202.153.37.205 port 13069
Oct 28 17:14:45 VM-96-4-centos sshd[16704]: Disconnected from 202.153.37.205 port 13069 [preau
Oct 28 17:14:59 VM-96-4-centos login: pam_tally2(login:auth): user root (0) tally 12, deny 2
Oct 28 17:14:59 VM-96-4-centos login: pam_succeed_if(login:auth): requirement "uid >= 1000" no
Oct 28 17:15:01 VM-96-4-centos login: FAILED LOGIN 2 FROM tty1 FOR root, Authentication failur
Oct 28 17:15:01 VM-96-4-centos login: pam_tally2(login:auth): unknown option: un_lock_time=300
Oct 28 17:15:03 VM-96-4-centos login: pam_tally2(login:auth): user root (0) tally 13, deny 2
Oct 28 17:15:04 VM-96-4-centos sshd[16738]: pam_unix(sshd:auth): authentication failure; logna
ost=203.213.66.170  user=root
```

3. 順に次のコマンドを実行し、`/etc/pam.d` に入り、ログの中のpamモジュールエラーのキーワード `pam_tally2` を検索します。



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

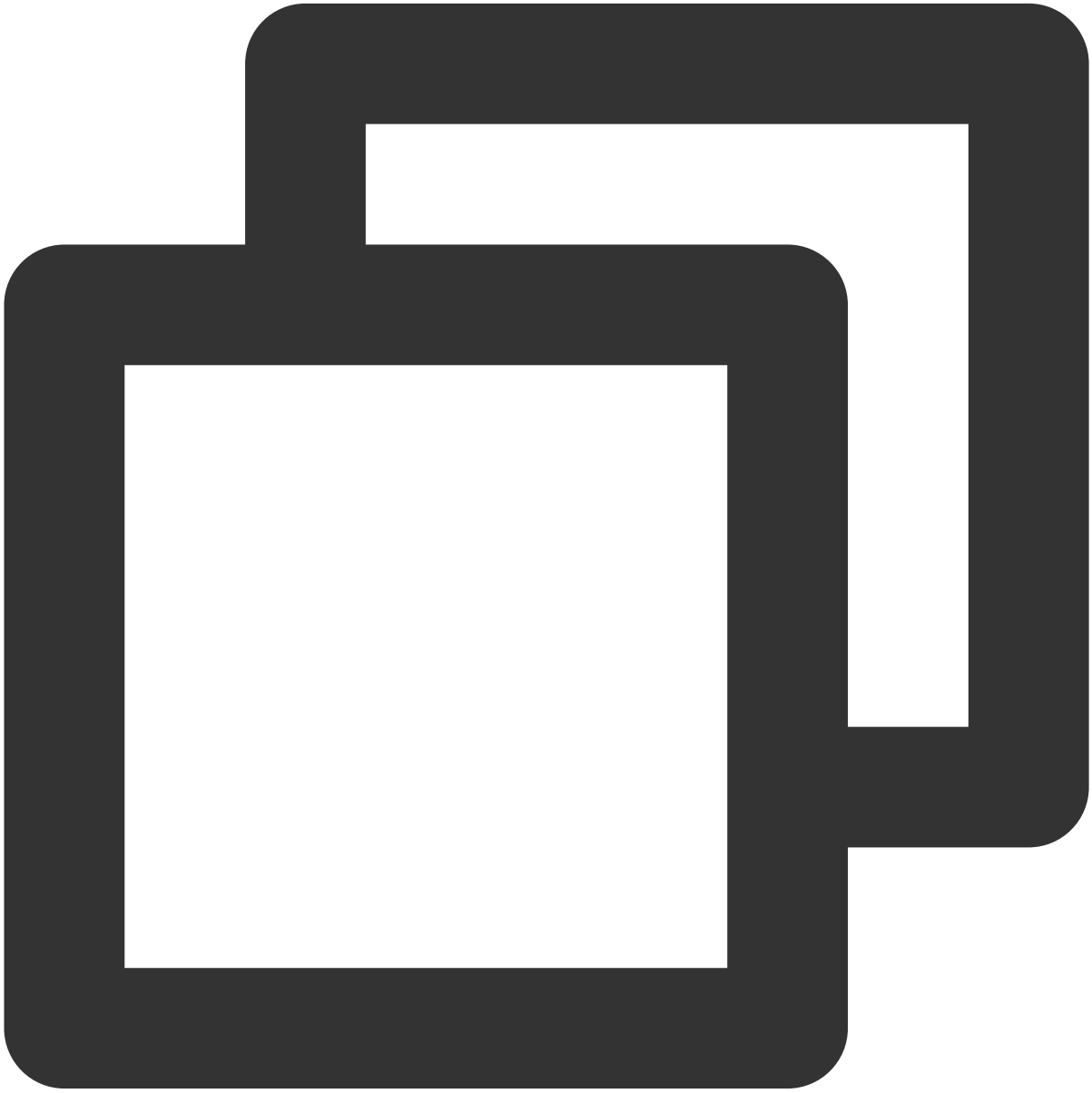


```
find . | xargs grep -ri "pam_tally2" -l
```

下図のような情報が表示される場合は、`login` ファイルにおいてこのパラメータが設定されていることを表します。

```
bash-4.2# find . |  xargs grep -ri "pam_tally2" -l
./login
./login
bash-4.2# _
```

4. 次のコマンドを実行し、`pam_tally2.so` モジュール設定に一時的なコメントを付加します。設定を完了すると、ログインできるようになります。



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

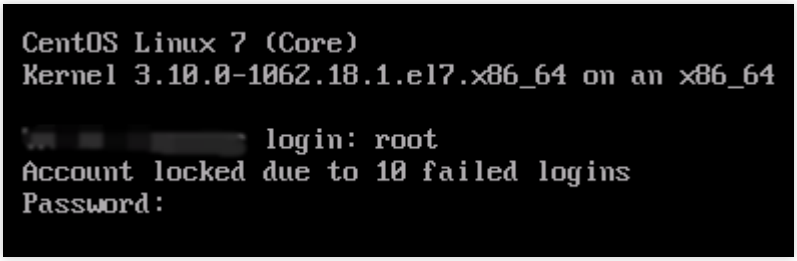
5. アカウントのロックが人為的な誤操作によるものか、総当たり攻撃によるものかを確認します。総当たり攻撃によって起こった場合は、次の方法でセキュリティポリシーを強化することを推奨します。
CVMのパスワードを変更し、大文字、小文字、特殊記号、数字を組み合わせた12～16桁の複雑なランダムパスワードを設定します。詳細については、インスタンスのパスワードをリセット をご参照ください。
CVM内の使われていないユーザーを削除します。
sshdのデフォルトの22ポートを1024～65525の間の他の非常用ポートに変更します。詳細については、CVMリモートデフォルトポートの変更 をご参照ください。
CVMのセキュリティグループに関連付けられているルールを管理し、業務およびプロトコルに必要なポートのみをオープンにし、すべてのプロトコルおよびポートをオープンにはしないことを推奨します。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。
mysql、redisなどのパブリックネットワークにコアアプリケーションサービスポートへのアクセスを開放することは推奨しません。 関連するポートをローカルアクセスに変更、または外部ネットワークアクセス禁止にすることができます。
「雲鏡」、「雲鎖」などの保護ソフトウェアをインストールし、リアルタイムアラームを追加して、異常なログイン情報を速やかに取得できるようにします。

Linuxインスタンス：VNCログインエラー Account locked due to XXX failed logins

最終更新日：：2023-06-08 17:22:38

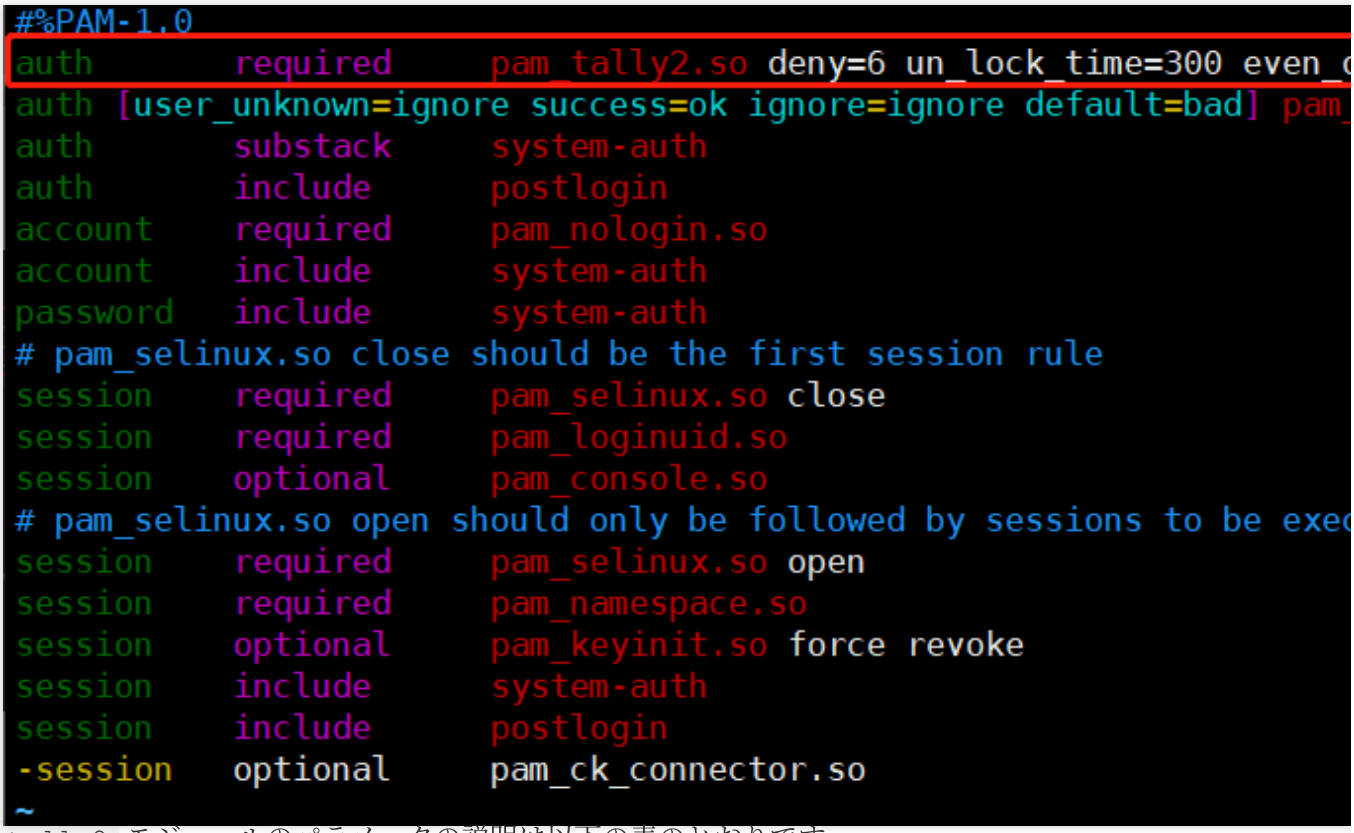
現象の説明

VNCを使用してCVMに正常にログインできず、ログインパスワードを入力する前にエラーメッセージ「Account locked due to XXX failed logins」が表示される（下図参照）。



考えられる原因

VNCを使用したログインでは `/etc/pam.d/login` というpamモジュールを呼び出して検証を行います。一方、login設定ファイルには `pam_tally2.so` モジュールの認証が存在します。 `pam_tally2.so` モジュールの機能は、LinuxユーザーがN回連続して誤ったパスワードを入力してログインを行った場合、自動的にX分間ロック、または永続的にロックを行うものです。このうち永続的なロックは手動で解除する必要があり、これを行わなければロックされたままとなります。
ログインの失敗が設定された試行回数を超えた場合、ログインアカウントは一定の時間ロックされるほか、総当たり攻撃が行われた場合はアカウントがロックされてログインできなくなる可能性もあります。下図は設定されているログイン試行可能回数です。



`pam_tally2` モジュールのパラメータの説明は以下の表のとおりです。

パラメータ	説明
deny=n	ログイン失敗回数がn回を超えた後はアクセスが拒否されます。
lock_time=n	ログイン失敗後にロックされる時間（秒）。
un lock_time=n	ログイン失敗回数が制限を超えた後、ロック解除に要する時間。
no_lock_time	ログファイル /var/log/faillog 中に .fail_locktime フィールドが記録されていません。
magic_root	rootユーザー（uid=0）がこのモジュールを呼び出した場合、カウンターの数値は増えません。
even_deny_root	rootユーザーのログイン失敗回数がdeny=n回を超えた後はアクセスが拒否されます。
root_unlock_time=n	even_deny_root に対応するオプション。このオプションを設定した場合の、rootユーザーのログイン失敗回数が制限を超えた後のロック時間。

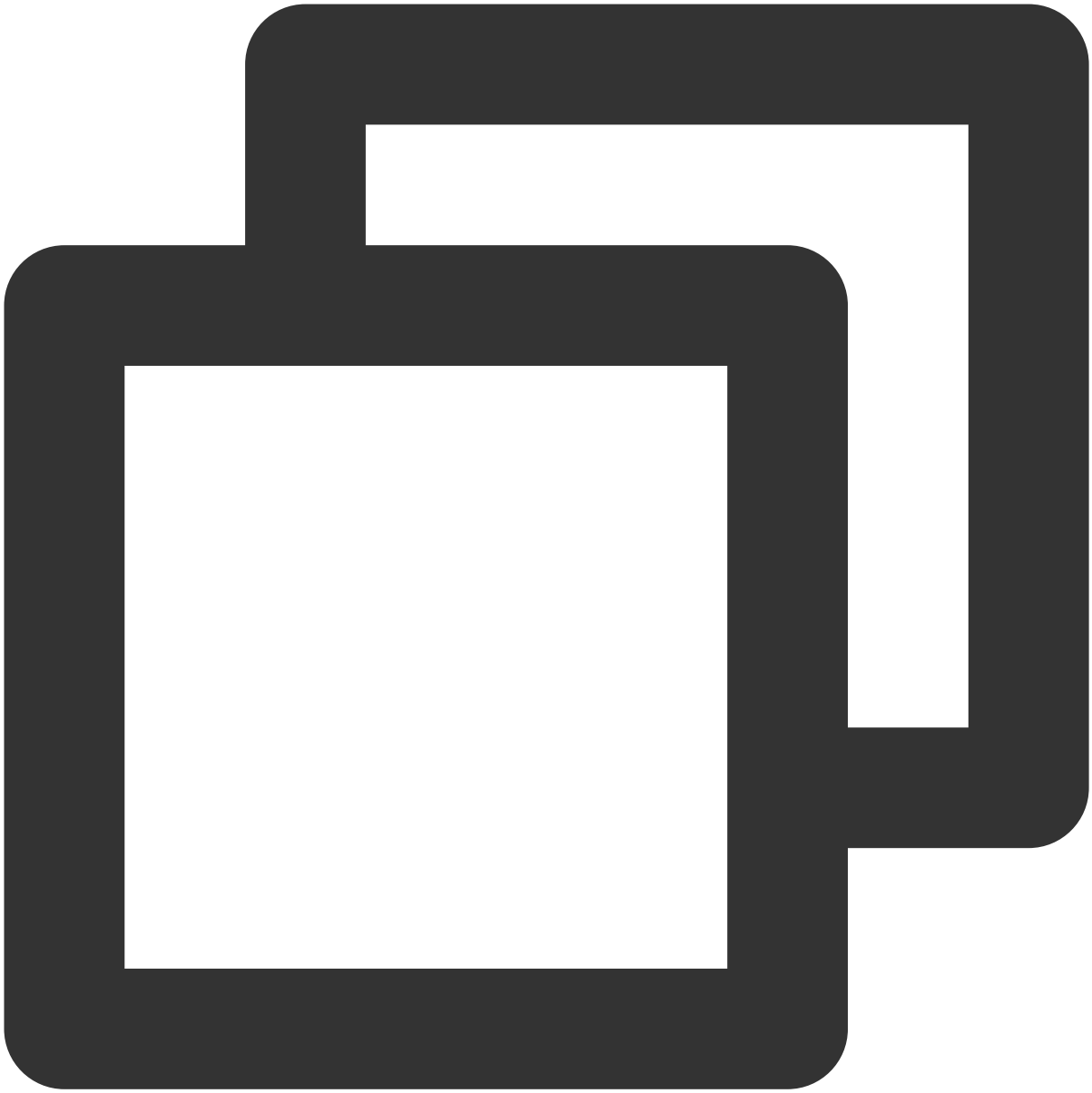
解決方法

1. 処理手順 を参照し、login設定ファイルに入り、 `pam_limits.so` モジュール設定に一時的なコメントを付加します。

2. アカウントがロックされた原因を確認し、セキュリティポリシーを強化します。

処理手順

1. SSHを使用したCVMインスタンスへのログインを試してください。詳細については SSH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。
ログインに成功した場合は次の手順に進みます。
ログインに失敗した場合は、単一ユーザーモードを使用する必要があります。
2. ログイン成功後、次のコマンドを実行してログ情報を確認します。

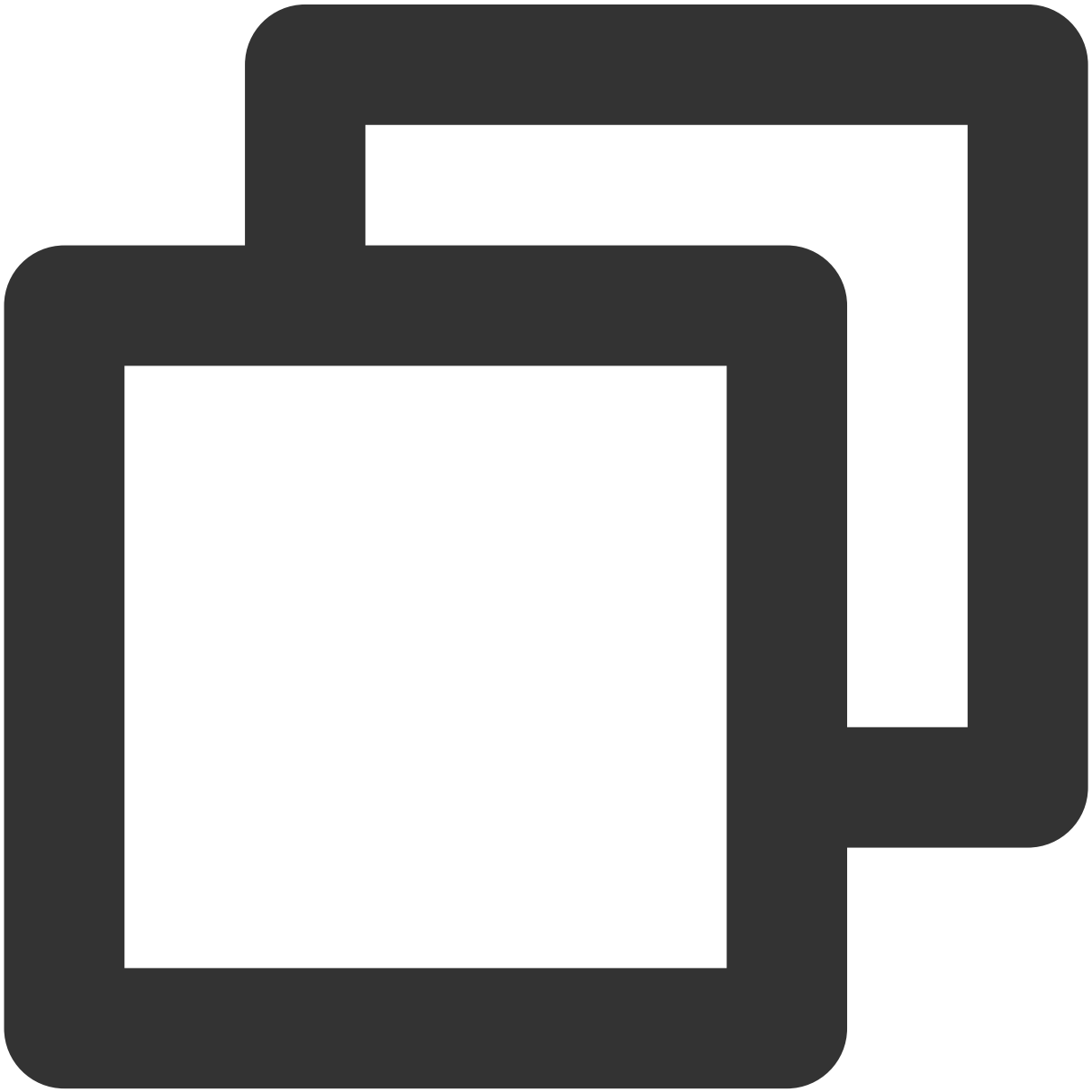


```
vim /var/log/secure
```

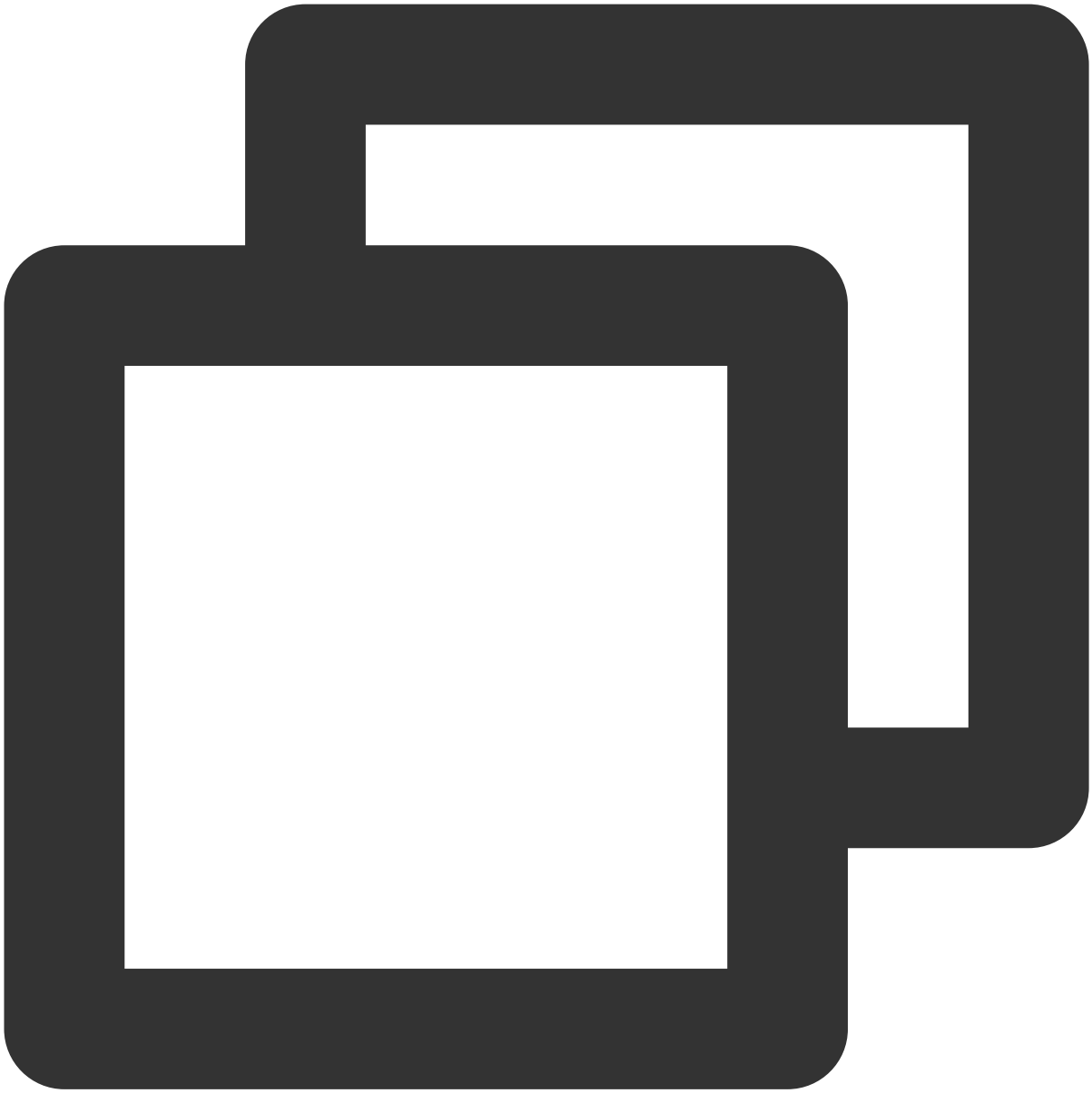
このファイルは一般的にセキュリティに関する情報の記録に用いられ、このうち大部分の記録はユーザーのCVMログインの関連ログです。下図のように、情報の中から `pam_tally2` のあるエラーメッセージを取得することができます。

```
Oct 28 17:14:45 VM-96-4-centos sshd[16704]: Failed password for invalid user dell from 202.153.3
Oct 28 17:14:45 VM-96-4-centos sshd[16704]: Received disconnect from 202.153.37.205 port 13069:1
Oct 28 17:14:45 VM-96-4-centos sshd[16704]: Disconnected from 202.153.37.205 port 13069 [preauth
Oct 28 17:14:59 VM-96-4-centos login: pam_tally2(login:auth): user root (0) tally 12, deny 2
Oct 28 17:14:59 VM-96-4-centos login: pam_succeed_if(login:auth): requirement "uid >= 1000" not
Oct 28 17:15:01 VM-96-4-centos login: FAILED LOGIN 2 FROM tty1 FOR root, Authentication failure
Oct 28 17:15:01 VM-96-4-centos login: pam_tally2(login:auth): unknown option: un_lock_time=300
Oct 28 17:15:03 VM-96-4-centos login: pam_tally2(login:auth): user root (0) tally 13, deny 2
Oct 28 17:15:04 VM-96-4-centos sshd[16736]: pam_unix(sshd:auth): authentication failure; logname=
ost=203.213.66.170  user=root
```

3. 順に次のコマンドを実行し、`/etc/pam.d` に入り、ログの中のpamモジュールエラーのキーワード `pam_tally2` を検索します。



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

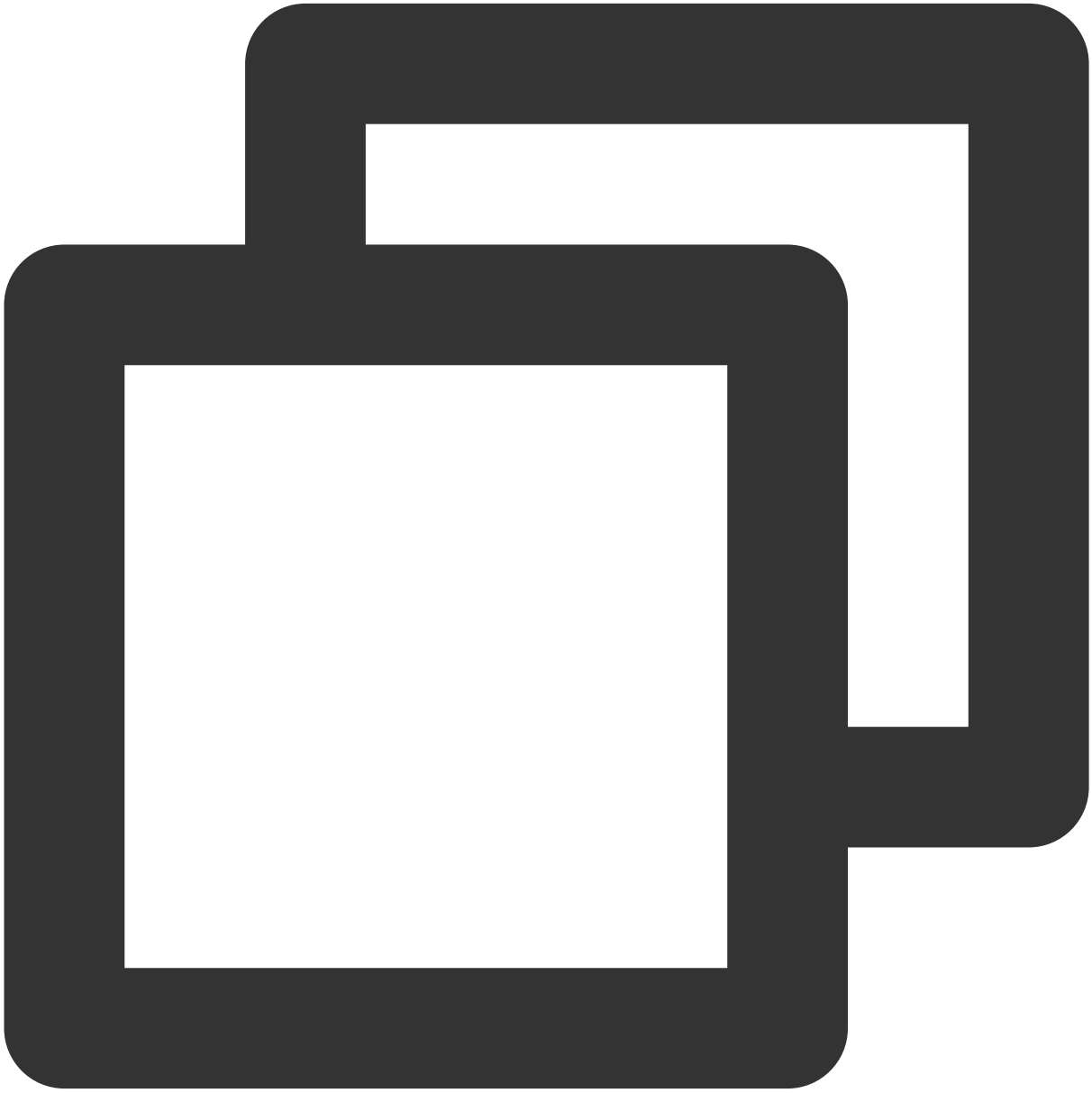


```
find . | xargs grep -ri "pam_tally2" -l
```

下図のような情報が表示される場合は、`login` ファイルにおいてこのパラメータが設定されていることを表します。

```
bash-4.2# find . |  xargs grep -ri "pam_tally2" -l
./login
./login
bash-4.2# _
```

4. 次のコマンドを実行し、 `pam_tally2.so` モジュール設定に一時的なコメントを付加します。設定を完了すると、ログインできるようになります。



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

5. アカウントのロックが人為的な誤操作によるものか、総当たり攻撃によるものかを確認します。総当たり攻撃によって起こった場合は、次の方法でセキュリティポリシーを強化することを推奨します。
CVMのパスワードを変更し、大文字、小文字、特殊記号、数字を組み合わせた12～16桁の複雑なランダムパスワードを設定します。詳細については、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内の使われていないユーザーを削除します。
sshdのデフォルトの22ポートを1024～65525の間の他の非常用ポートに変更します。詳細については、CVMリモートデフォルトポートの変更 をご参照ください。
CVMのセキュリティグループに関連付けられているルールを管理し、業務およびプロトコルに必要なポートのみをオープンにし、すべてのプロトコルおよびポートをオープンにはしないことを推奨します。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。
mysql、redisなどのパブリックネットワークにコアアプリケーションサービスポートへのアクセスを開放することは推奨しません。 関連するポートをローカルアクセスに変更、または外部ネットワークアクセス禁止にすることができます。
「雲鏡」などの保護ソフトウェアをインストールし、リアルタイムアラームを追加して、異常なログイン情報を速やかに取得できるようにします。

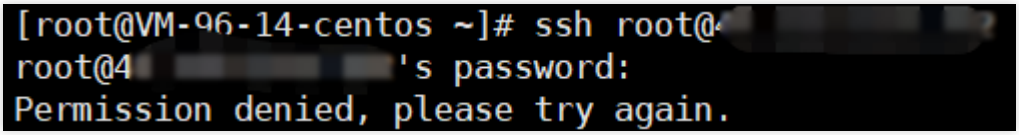
Linuxインスタンス：VNCへのログインに正しいパスワードを入力しても応答がありません

最終更新日：：2023-06-08 17:27:24

現象の説明

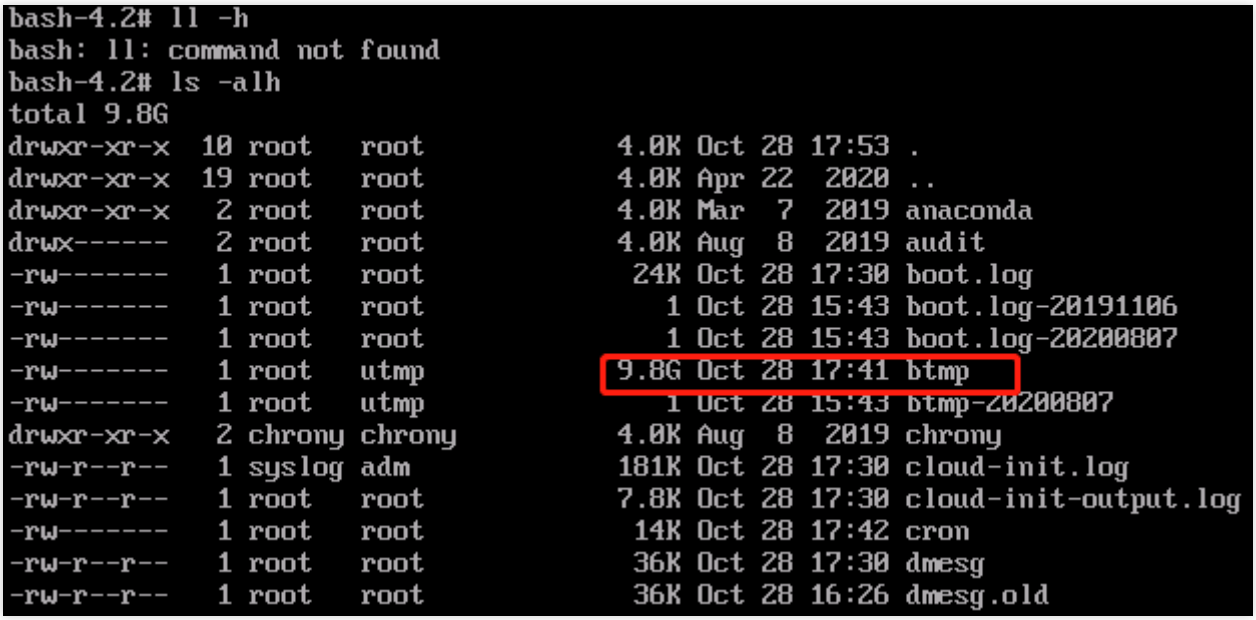
VNCを使用してCVMにログインする際、正しいパスワードを入力してもログインできず、しばらくしてからエラーメッセージ“Hint：Caps Lock on”が表示される（下図参照）。

また、SSHを使用したリモートログインの際、エラーメッセージ“Permission denied,please try again.”が表示される（下図参照）。



考えられる原因

頻繁な総当たり攻撃によって `/var/log/btmp` のログ容量が大きくなりすぎたことが原因の可能性があります。このファイルはエラーログインのログの記録に用いられ、容量が大きすぎるとログイン時のログ書き込みに異常が生じ、正常なログインができなくなります。下図に示します。

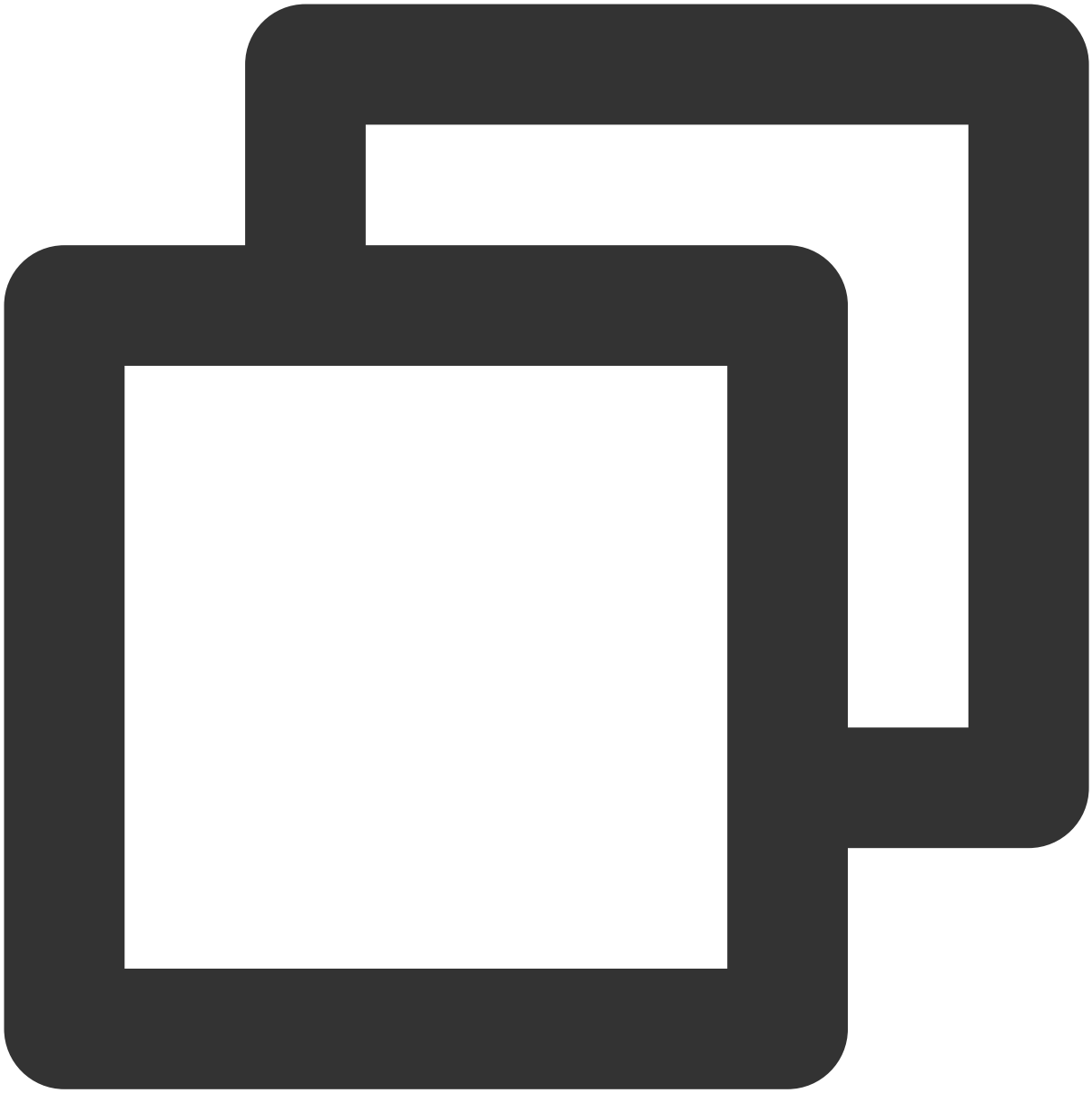


解決方法

1. 処理手順 を参照し、ログファイル `/var/log/btmp` の容量が大きすぎないか確認します。
2. 総当たり攻撃によるものかどうかを確認し、セキュリティポリシーを強化します。

処理手順

1. SSHを使用したCVMインスタンスへのログインを試してください。詳細については SSH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。
ログインに成功した場合は次の手順に進みます。
ログインに失敗した場合は、単一ユーザーモードを使用する必要があります。
2. `/var/log` に入り、ログファイル `/var/log/btmp` の容量を確認します。
3. ログファイル `/var/log/btmp` の容量が大きすぎる場合は、次のコマンドを実行し、btmpログの内容をクリアします。ログファイルをクリアすると、ログインできるようになります。



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

4. アカウントのロックが人為的な誤操作によるものか、総当たり攻撃によるものかを確認します。総当たり攻撃によって起こった場合は、次の方法でセキュリティポリシーを強化することを推奨します。
CVMのパスワードを変更し、大文字、小文字、特殊記号、数字を組み合わせた12〜16桁の複雑なランダムパスワードを設定します。詳細については、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内の使われていないユーザーを削除します。
sshdのデフォルトの22ポートを1024〜65525の間の他の非常用ポートに変更します。詳細については、CVMリモートデフォルトポートの変更 をご参照ください。

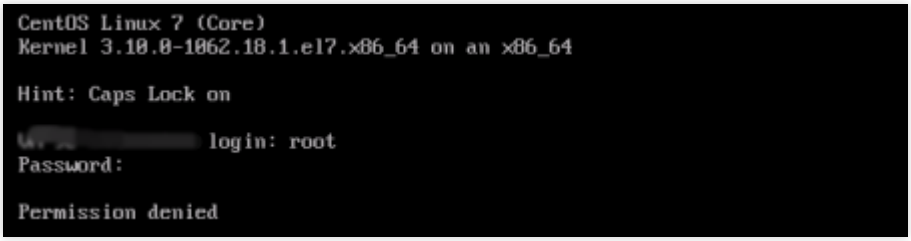
CVMのセキュリティグループに関連付けられているルールを管理し、業務およびプロトコルに必要なポートのみをオープンにし、すべてのプロトコルおよびポートをオープンにはしないことを推奨します。詳細については、セキュリティグループルールの追加 をご参照ください。
mysql、redisなどのパブリックネットワークにコアアプリケーションサービスポートへのアクセスを開放することは推奨しません。 関連するポートをローカルアクセスに変更、または外部ネットワークアクセス禁止にすることができます。
「雲鏡」、「雲鎖」などの保護ソフトウェアをインストールし、リアルタイムアラームを追加して、異常なログイン情報を速やかに取得できるようにします。

Linuxインスタンス：VNCまたはSSHログインエラー Permission denied

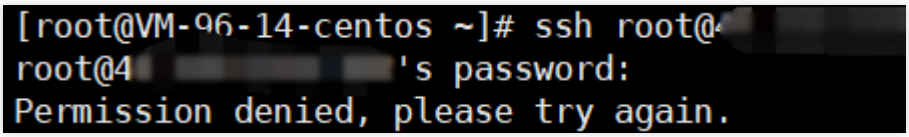
最終更新日：：2023-06-08 17:34:41

現象の説明

VNCまたはSSHログインを使用する際、エラーメッセージ“Permission denied”が表示される。
VNCログインエラーは下図のように表示されます。

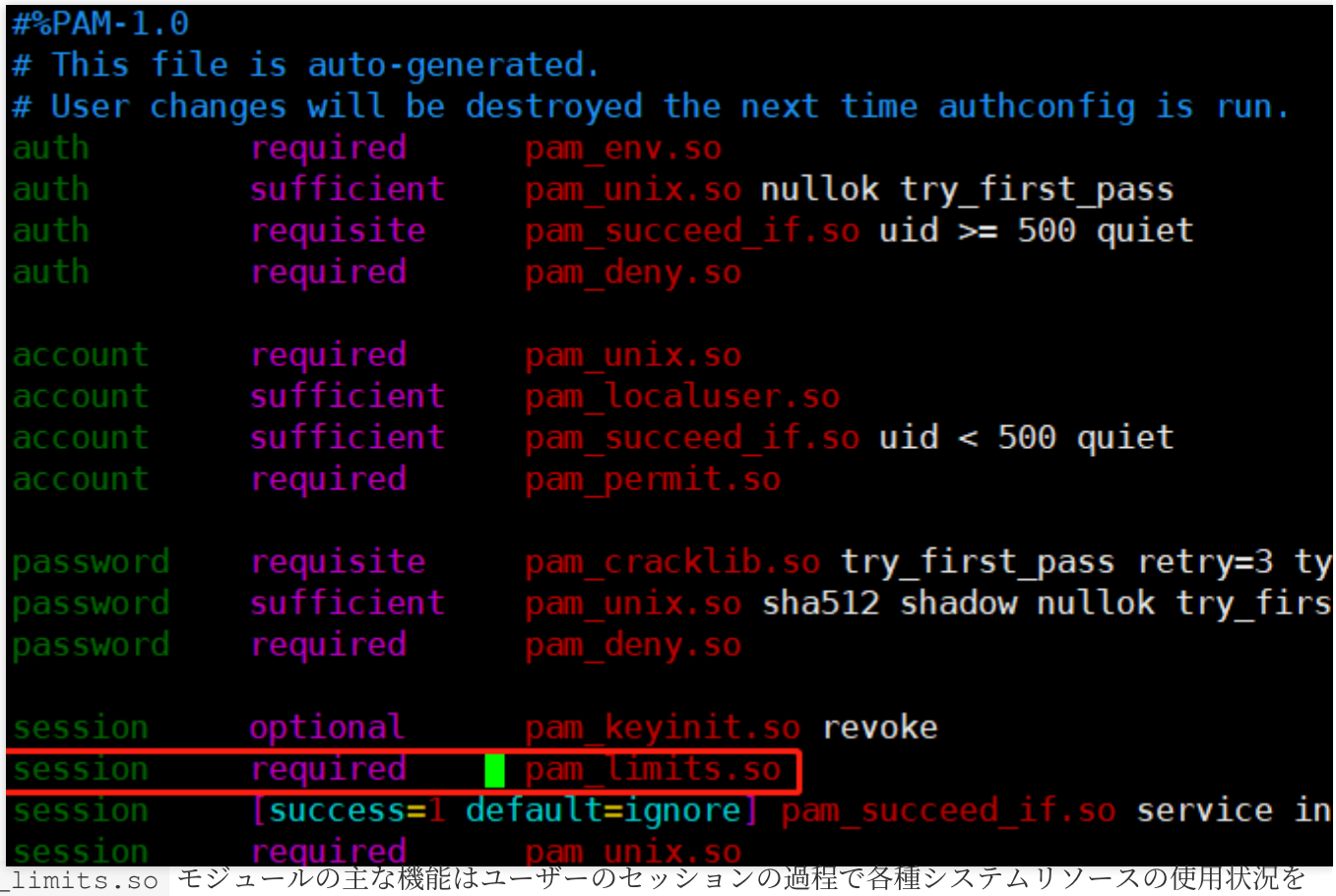


SSHログインエラーは下図のように表示されます。



考えられる原因

VNCまたはSSHを使用したログインでは `/etc/pam.d/login` というpamモジュールを呼び出して検証を行います。 `/etc/pam.d/login` の設定において、デフォルトでは `system-auth` モジュールをインポートして認証を行い、 `system-auth` モジュールはデフォルトで `pam_limits.so` モジュールをインポートして認証を行います。 `system-auth` のデフォルト設定は下図のとおりです。



`pam_limits.so` モジュールの主な機能はユーザーのセッションの過程で各種システムリソースの使用状況を制限することです。デフォルトではこのモジュールの設定ファイルは `/etc/security/limits.conf` であり、この設定ファイルはユーザーが使用可能な最大ファイル数、最大スレッド数、最大メモリなどのリソース使用量を規定しています。パラメータの説明は下表のとおりです。

パラメータ	説明
soft nofile	開くことができるファイルディスクリプタの最大数（ソフトリミット）。
hard nofile	開くことができるファイルディスクリプタの最大数（ハードリミット）。この設定値を超えることはできません。
fs.file-max	システムクラスにおいて開くことができるファイルハンドラ（カーネル中のstruct file）の数量。システム全体に対する制限であり、ユーザーに対してのものではありません。
fs.nr_open	1つのプロセスで割り当て可能な最大ファイルディスクリプタ数（fd個数）。

正常にログインできない原因は、設定ファイル `/etc/security/limits.conf` 中のrootユーザーが開くことのできるファイルディスクリプタの最大数の設定にエラーがあることによる可能性があります。 正しい設定は `soft nofile ≤ hard nofile ≤ fs.nr_open` の関係を満たしていなければなりません。

解決方法

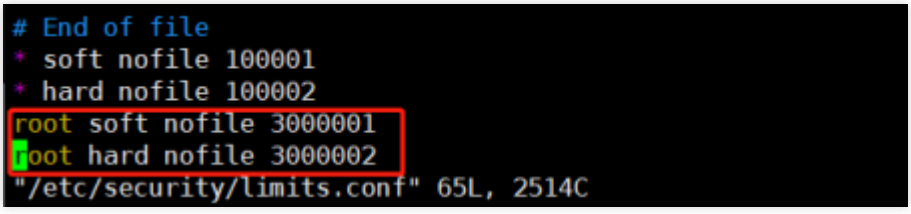
処理手順 を参照し、 `soft nofile` 、 `hard nofile` および `fs.nr_open` を正しい設定に修正します。

処理手順

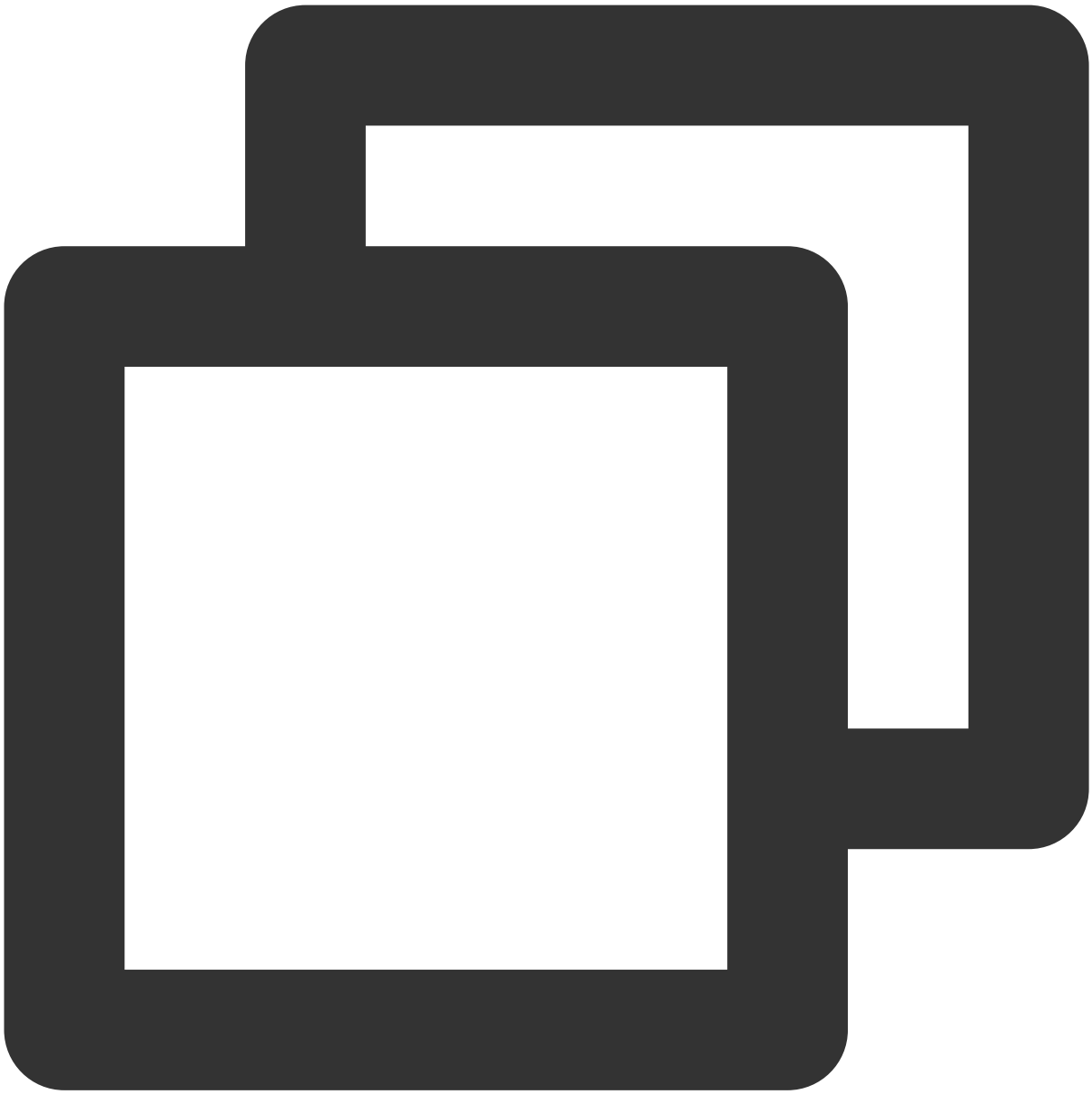
1. SSHを使用したCVMインスタンスへのログインを試してください。詳細については SSHを使用してLinuxインスタンスにログイン をご参照ください。
ログインに成功した場合は次の手順に進みます。
ログインに失敗した場合は、単一ユーザーモードを使用する必要があります。
2. パラメータ `soft nofile` 、 `hard nofile` および `fs.nr_open` の値が `soft nofile ≤ hard nofile ≤ fs.nr_open` の関係を満たしているかどうかを確認します。
次のコマンドを実行し、 `soft nofile` および `hard nofile` の値を確認します。

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

ここでの取得結果は3000001と3000002です。下図のように表示されます。

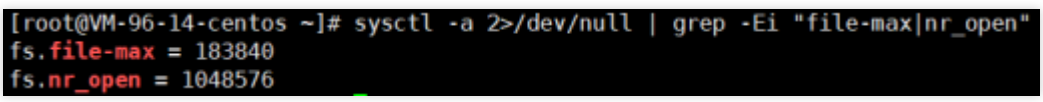


次のコマンドを実行し、 `fs.nr_open` の値を確認します。



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

ここでの取得結果は1048576です。下図のように表示されます。



3. `/etc/security/limits.conf` ファイルを修正し、次の設定をファイルの末尾に追加または修正します。

`root soft nofile` :100001

`root hard nofile` :100002

4. `/etc/sysctl.conf` ファイルを修正し、次の設定をファイルの末尾に追加または修正します。

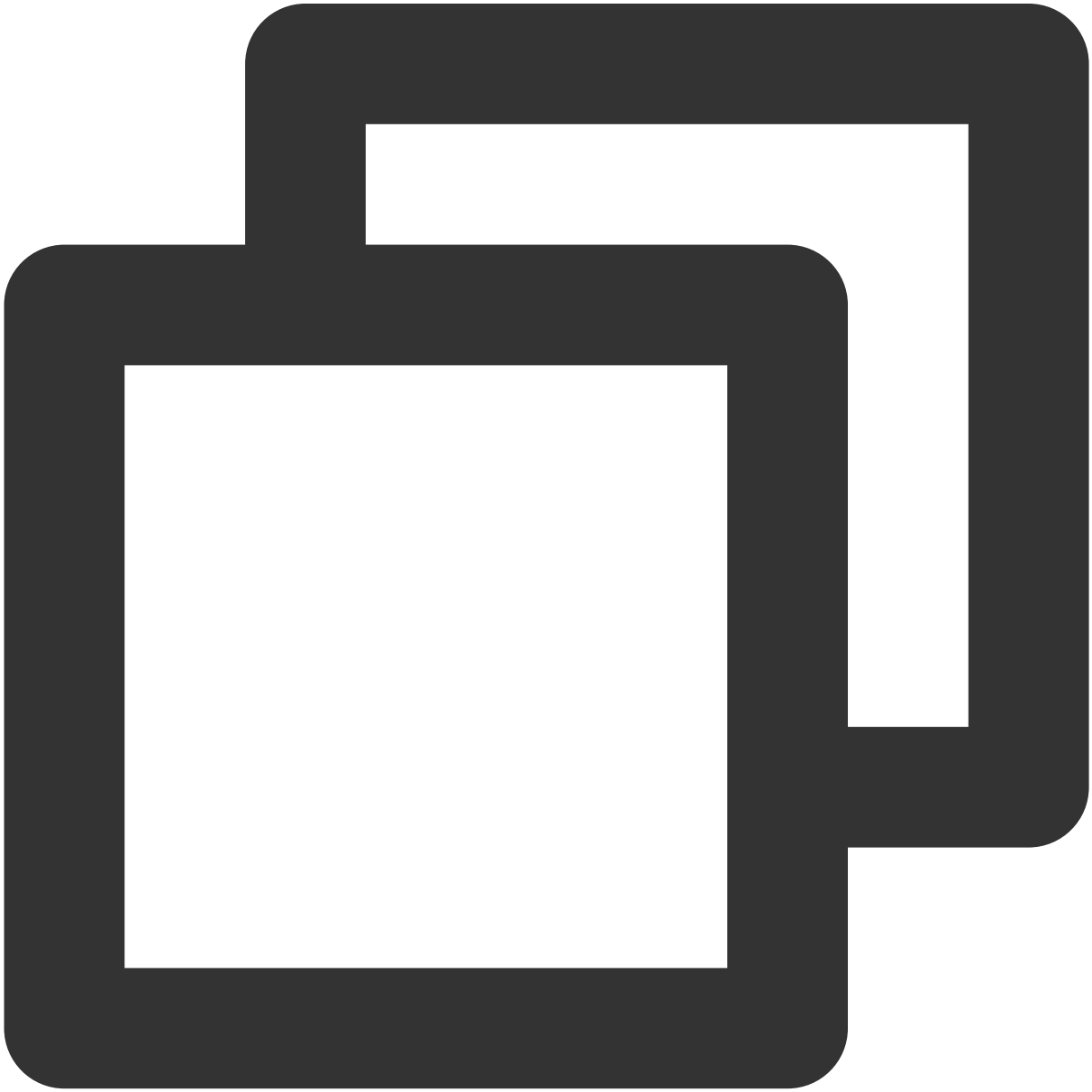
説明：

`soft nofile ≤ hard nofile ≤ fs.nr_open` の関係を満たしている場合は、この手順は必須ではありません。システムの最大制限が不足している場合に再調整することができます。

`fs.file-max` = 2000000

`fs.nr_open` = 2000000

5. 次のコマンドを実行すると、設定は直ちに有効になります。設定を完了するとログインできるようになります。



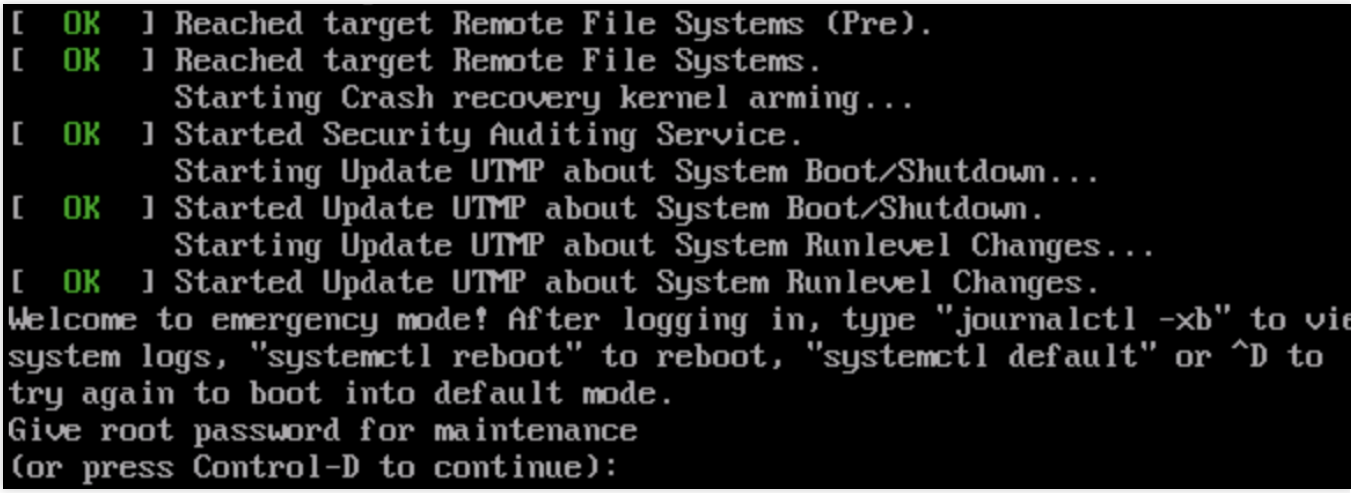
```
sysctl -p
```

Linuxインスタンス：/etc/fstabの設定エラーによるログイン不能

最終更新日：：2023-06-08 17:54:51

現象の説明

SSHでLinux CVMへの正常なリモートログインができず、VNC方式でログインすると、システムの起動失敗が確認され、下図のように「Welcome to emergency mode」というメッセージが表示されます。



考えられる原因

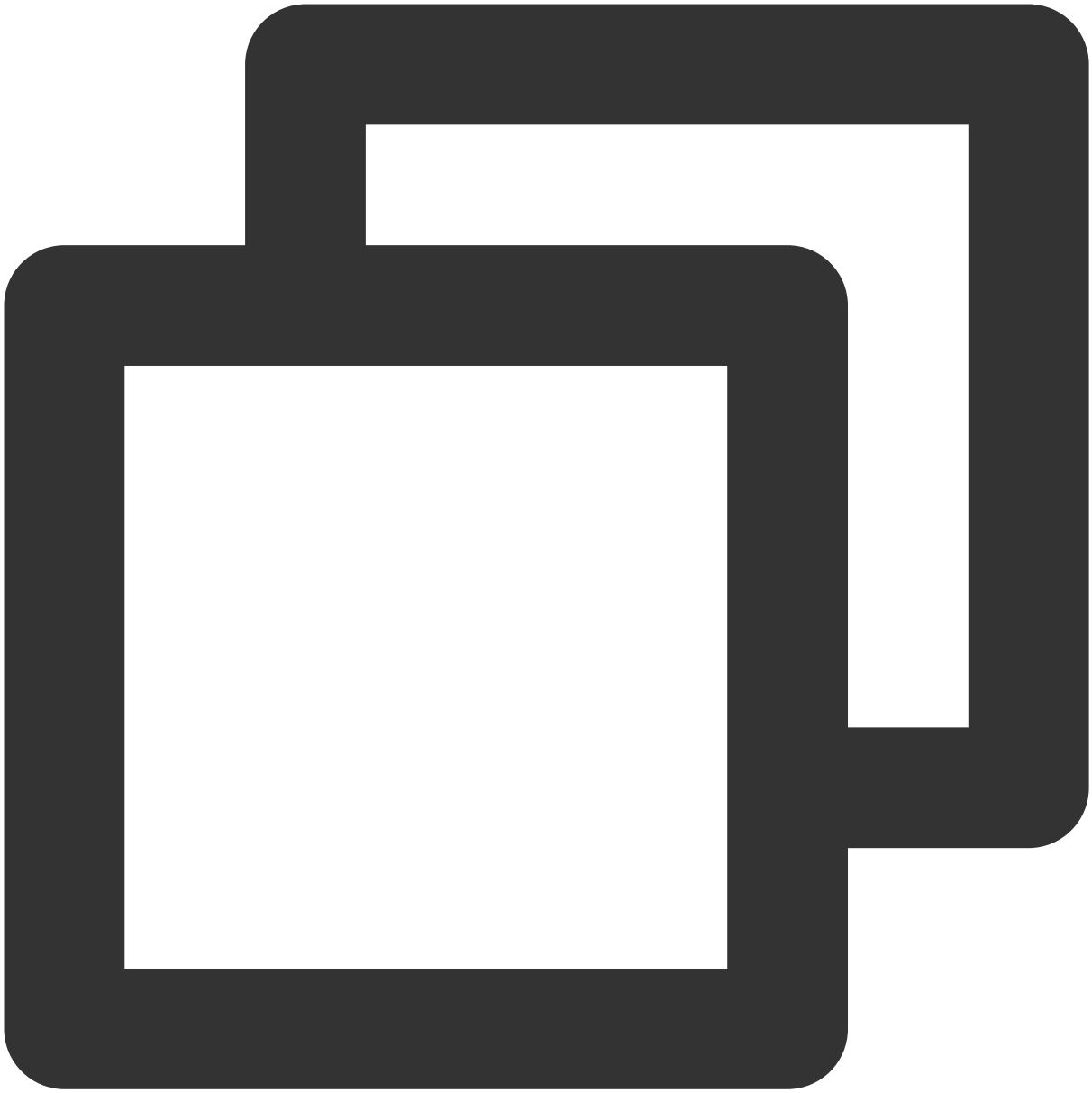
`/etc/fstab` の設定が不適切であることが原因という可能性があります。
例えば、 `/etc/fstab` においてディスクがデバイス名で自動的にマウントされるように設定されている場合も、CVMを再起動するとデバイス名が変わってしまい、システムが正常に起動しなくなることがあります。

解決方法

処理手順 を参照して `/etc/fstab` 設定ファイルを修復し、サーバーを再起動してから検証します。

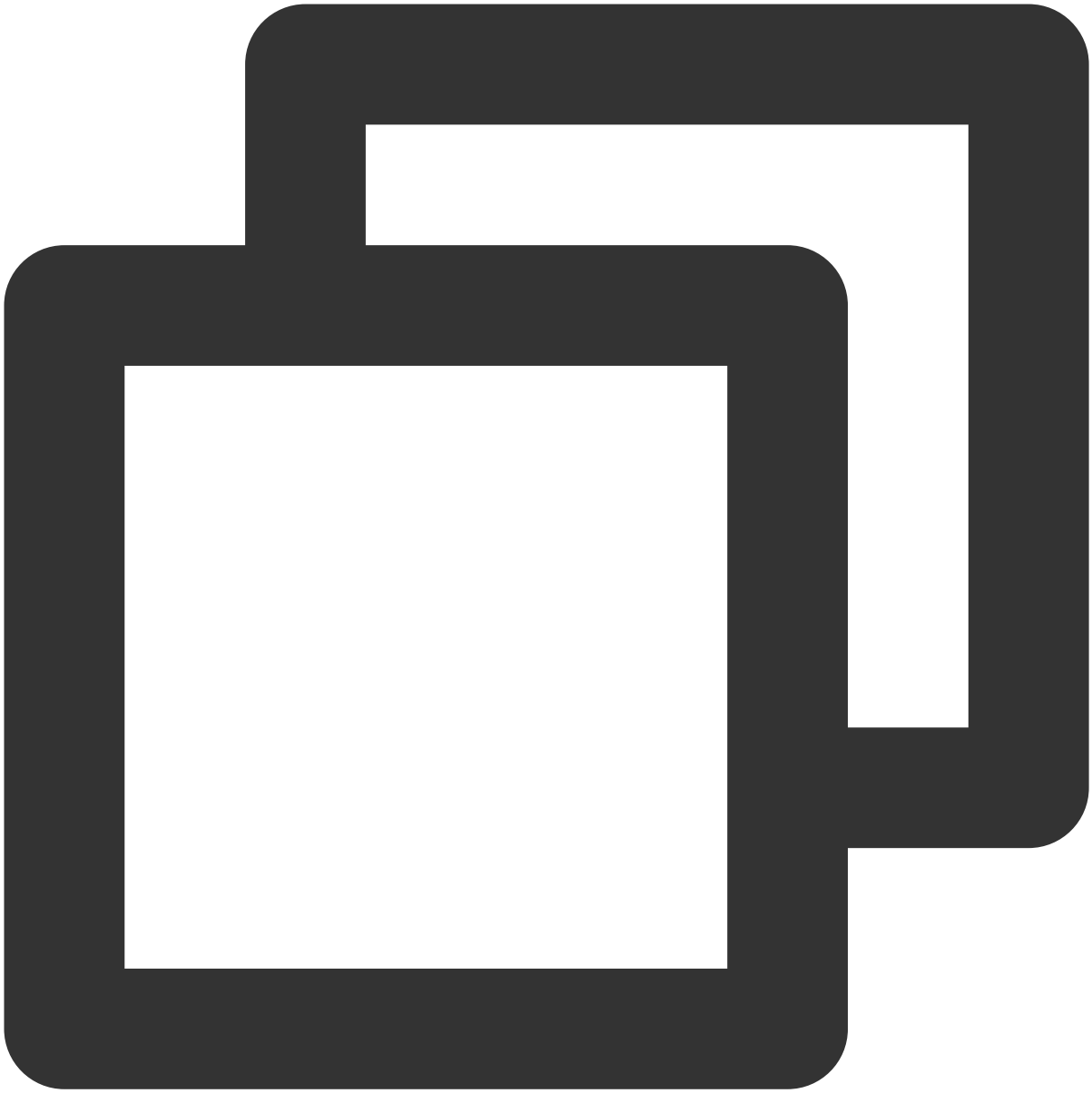
処理手順

インスタンスにアクセスし、この問題を処理する方法は2つあります。
方法1：VNCを使用したログイン（推奨）
方法2：レスキューモードの使用
1. VNCを使用してLinuxインスタンスにログイン します。
2. VNCインターフェースに進み、現象の説明 のようなインターフェースが表示されたら、rootアカウントのパスワードを入力し、**Enter**を押してサーバーにログインしてください。
入力されたパスワードは、デフォルトでは表示されません。
アカウントのパスワードをお持ちでない場合、または忘れてしまった場合は、方法2を参照して処理してください。
3. 以下のコマンドを実行し、`/etc/fstab` ファイルのバックアップを取ります。ここでは、`/home` ディレクトリへのバックアップを例に取ります。



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

4. 以下のコマンドを実行し、VIエディタを使用して `/etc/fstab` ファイルを開きます。

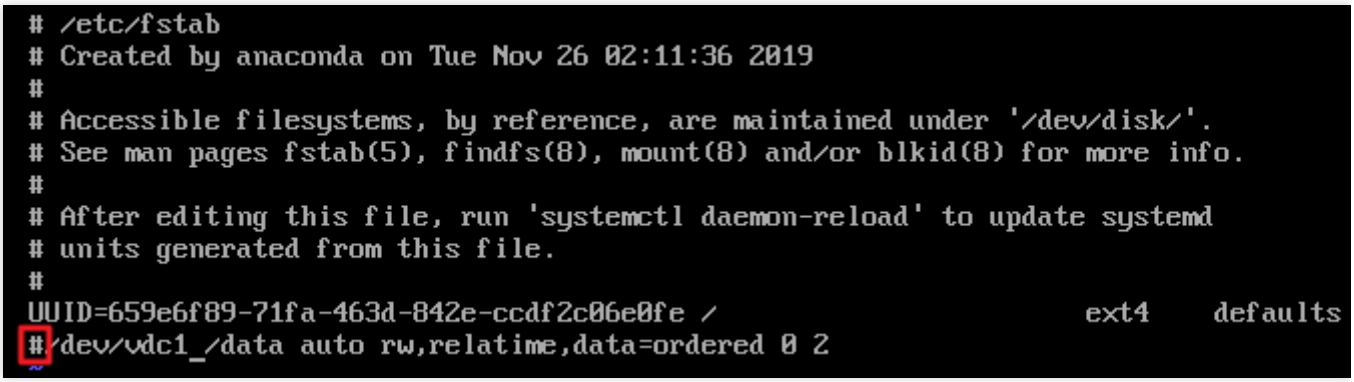


```
vi /etc/fstab
```

5. 下図に示すように、**i**を押して編集モードに入り、カーソルを設定エラーの行の先頭に移動させ、 `#` を入力して行の設定についてコメントアウトします。

説明：

設定エラーを特定できない場合は、システムディスク以外のマウントされているすべてのディスクの設定についてコメントアウトし、サーバーが正常な状態に戻った後に ステップ8 を参照して設定することをお勧めします。



6. **Esc**を押して**:wq** と入力した後、**Enter**を押して設定を保存し、エディタを終了します。
7. コンソールからインスタンスを再起動し、正常に起動、ログインできるかどうかを検証します。

説明：

コンソールからインスタンスを再起動します。具体的な手順については、インスタンスの再起動 をご参照ください。

8. ログインに成功した後、ディスクの自動マウントの設定が必要な場合は、/etc/fstabファイルの設定 を参照し、対応する設定を行ってください。

1. レスキューモードの使用 を参照し、インスタンスレスキューモードに入ります。

ご注意：

レスキューモードの使用によるシステム修復 手順の中の `mount` と `chroot` の関連コマンドを実行し、業務そのものにアクセスできることを確認する必要があります。

2. 方法1の ステップ3 - ステップ6 に従って、 `/etc/fstab` ファイルの修復を行います。
3. レスキューモードの終了を参照し、インスタンスのレスキューモードを終了します。
4. インスタンスがレスキューモードを終了すると、シャットダウン状態になります。インスタンスの起動 を参照してシステムを起動し、起動後に正常にログインできることを確認してください。
5. ログインに成功した後、ディスクの自動マウントの設定が必要な場合は、/etc/fstabファイルの設定 を参照し、対応する設定を行ってください。

Linuxインスタンス：sshd設定ファイル権限に関する問題

最終更新日：：2023-06-08 17:38:23

##故障について
SSHを使用してLinuxインスタンスにログインすると、「ssh_exchange_identification: Connection closed by remote host」または「no hostkey alg」が出現する。

考えられる原因

`/var/empty/sshd` および `/etc/ssh/ssh_host_rsa_key` 設定ファイルの権限が変更されるなど、sshd設定ファイルの権限が変更されたため、SSHを使用したログインができなくなっている可能性があります。

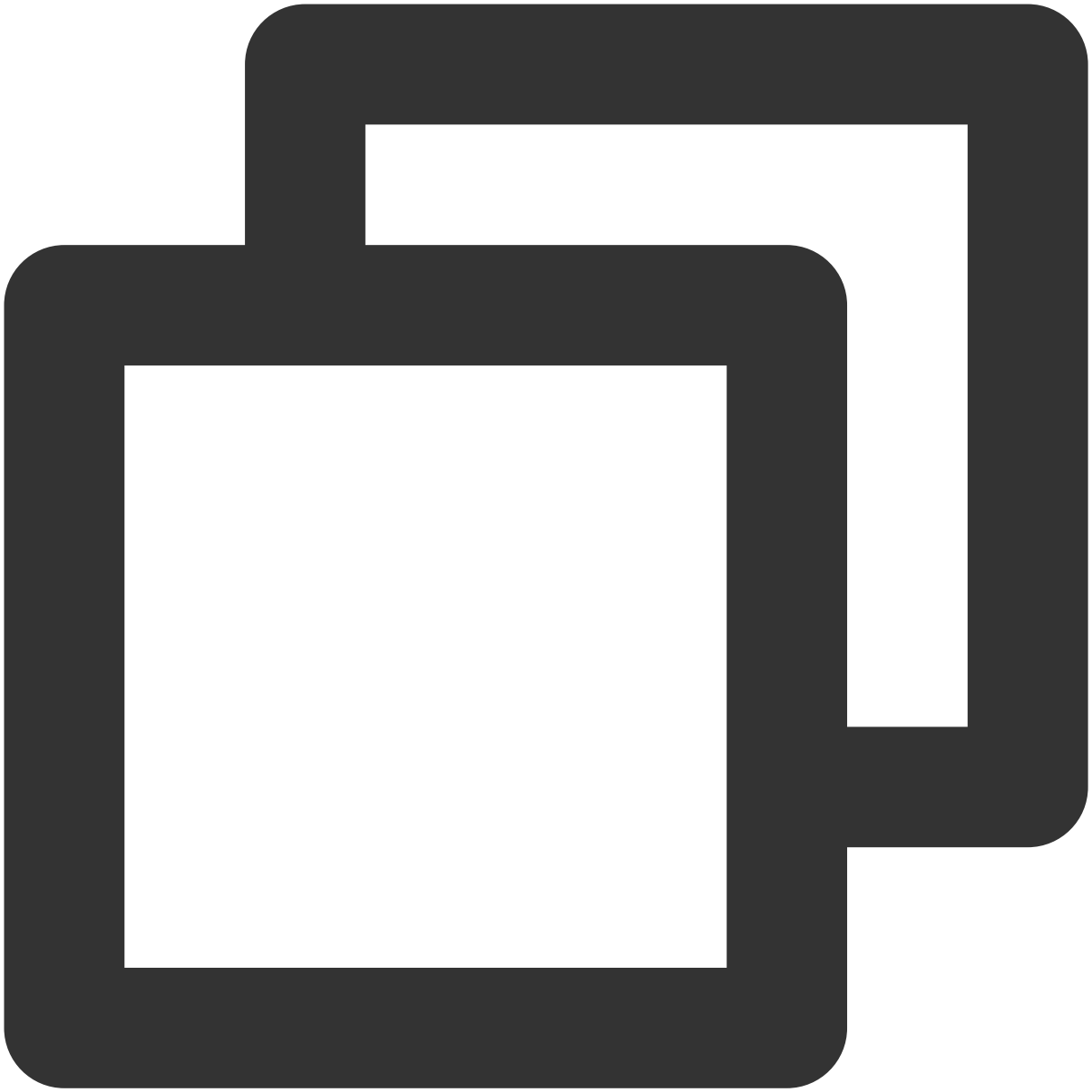
ソリューション

実際のエラー情報に応じて対応する手順を選択し、設定ファイルの権限を修正します。
エラー情報が「ssh_exchange_identification: Connection closed by remote host」である場合は、/var/empty/sshd ファイル権限の修正 手順をご参照ください。
エラー情報が「no hostkey alg」である場合は、/etc/ssh/ssh_host_rsa_key ファイル権限の修正 手順をご参照ください。

処理手順

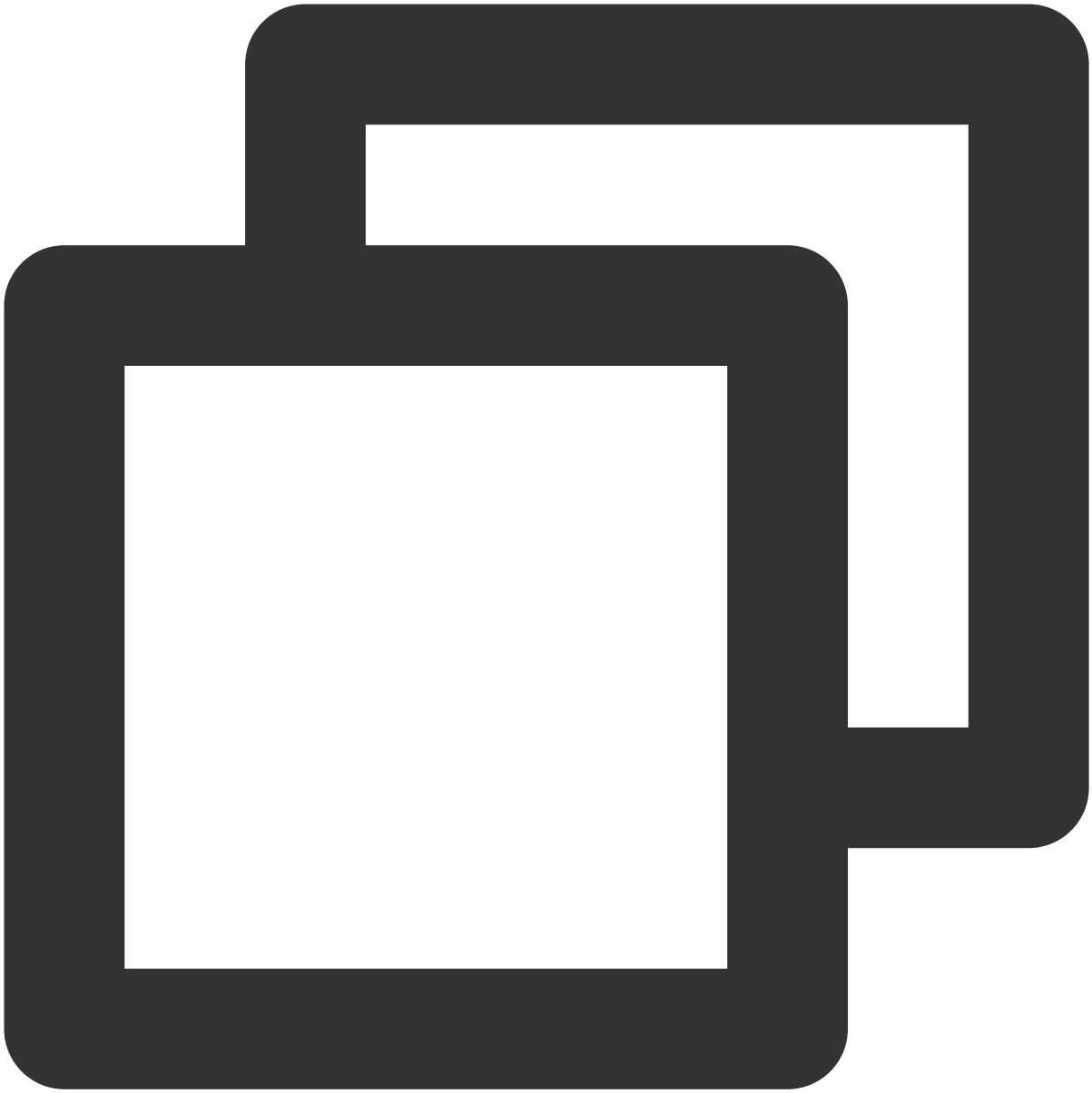
/var/empty/sshd ファイル権限の修正

1. VNCを使用してLinuxインスタンスにログイン。
2. 次のコマンドを実行し、エラーの原因を確認します。



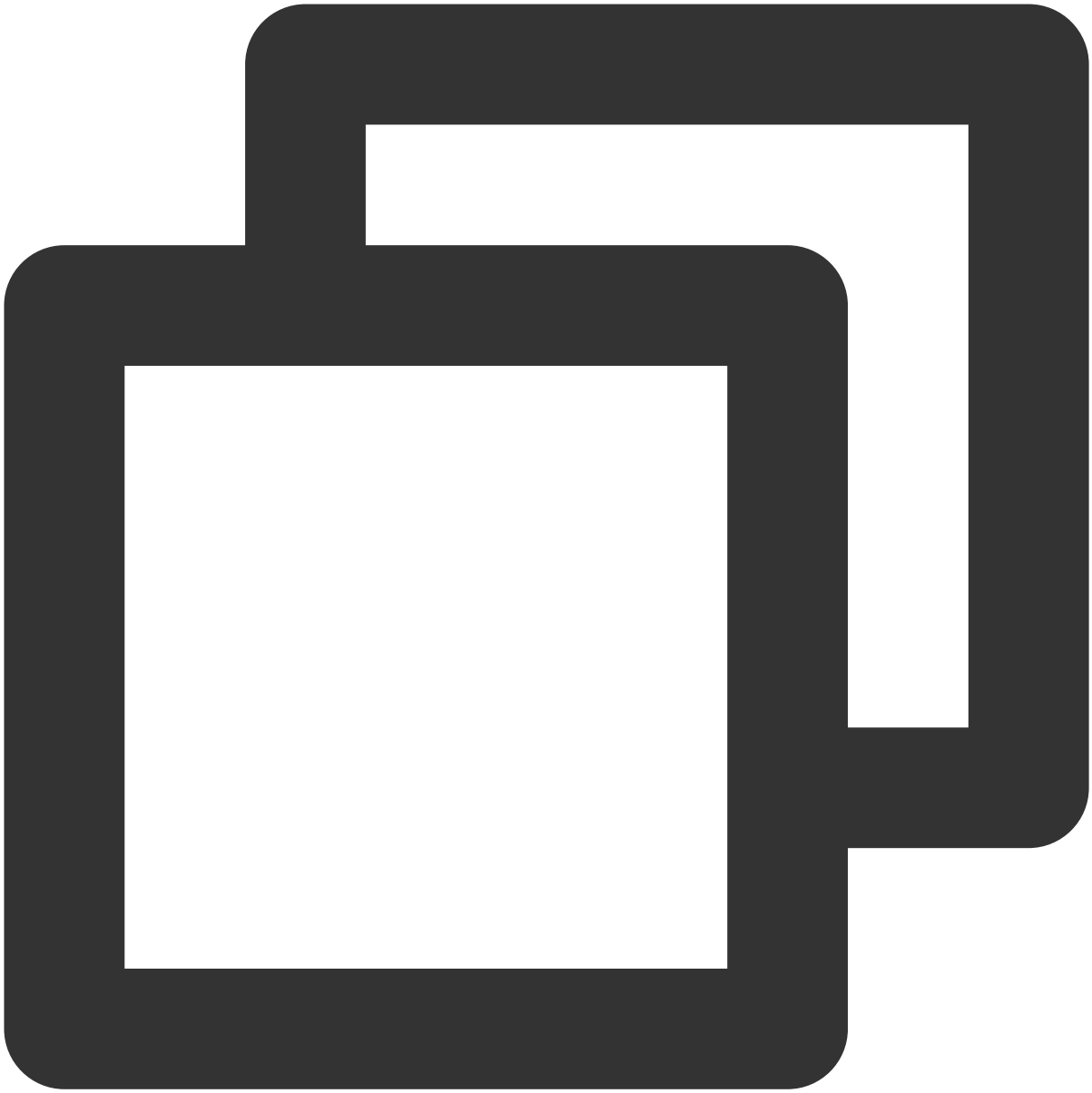
```
sshd -t
```

次のような情報が返されます：



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

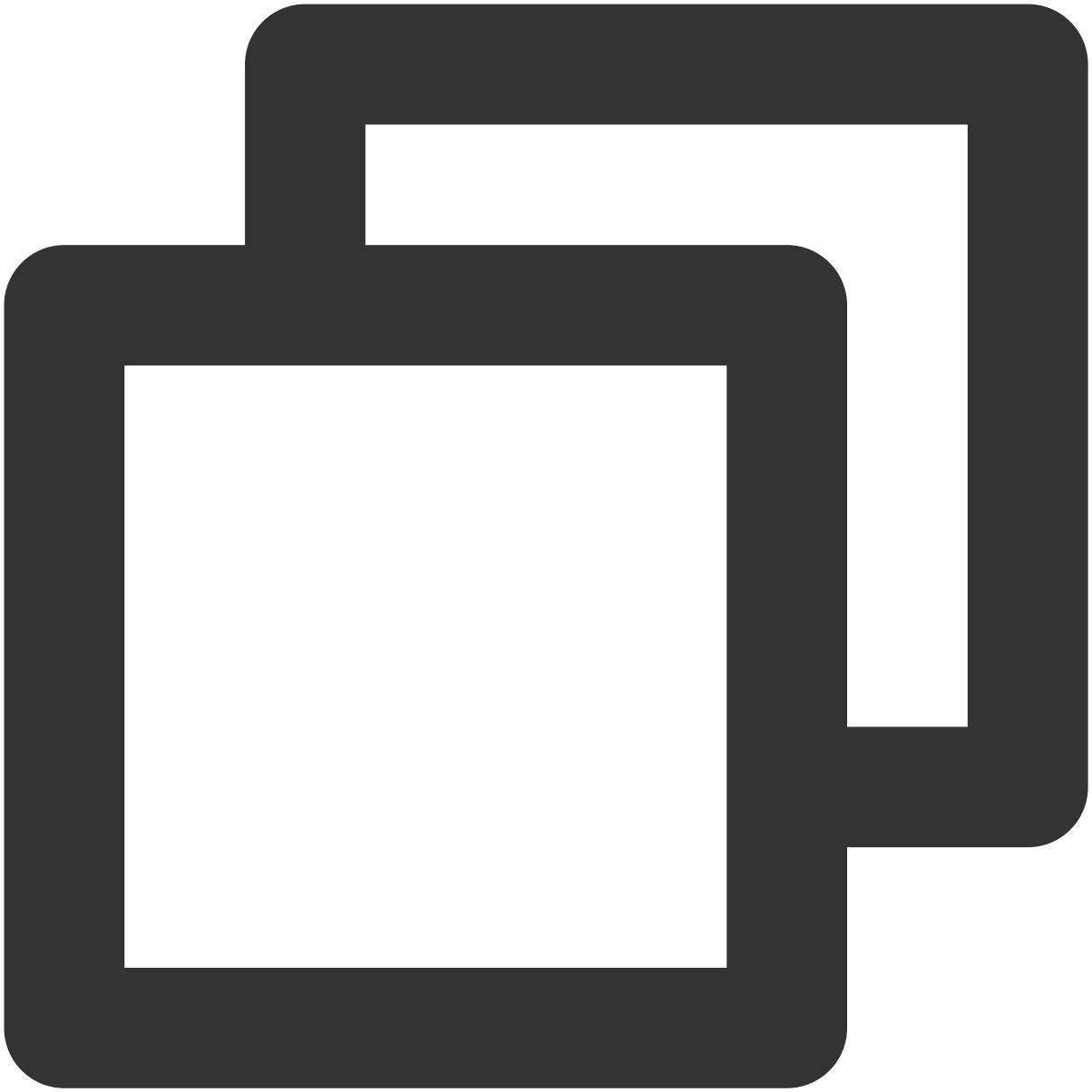
3. 次のコマンドを実行し、`/var/empty/sshd/` ファイル権限を修正します。



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

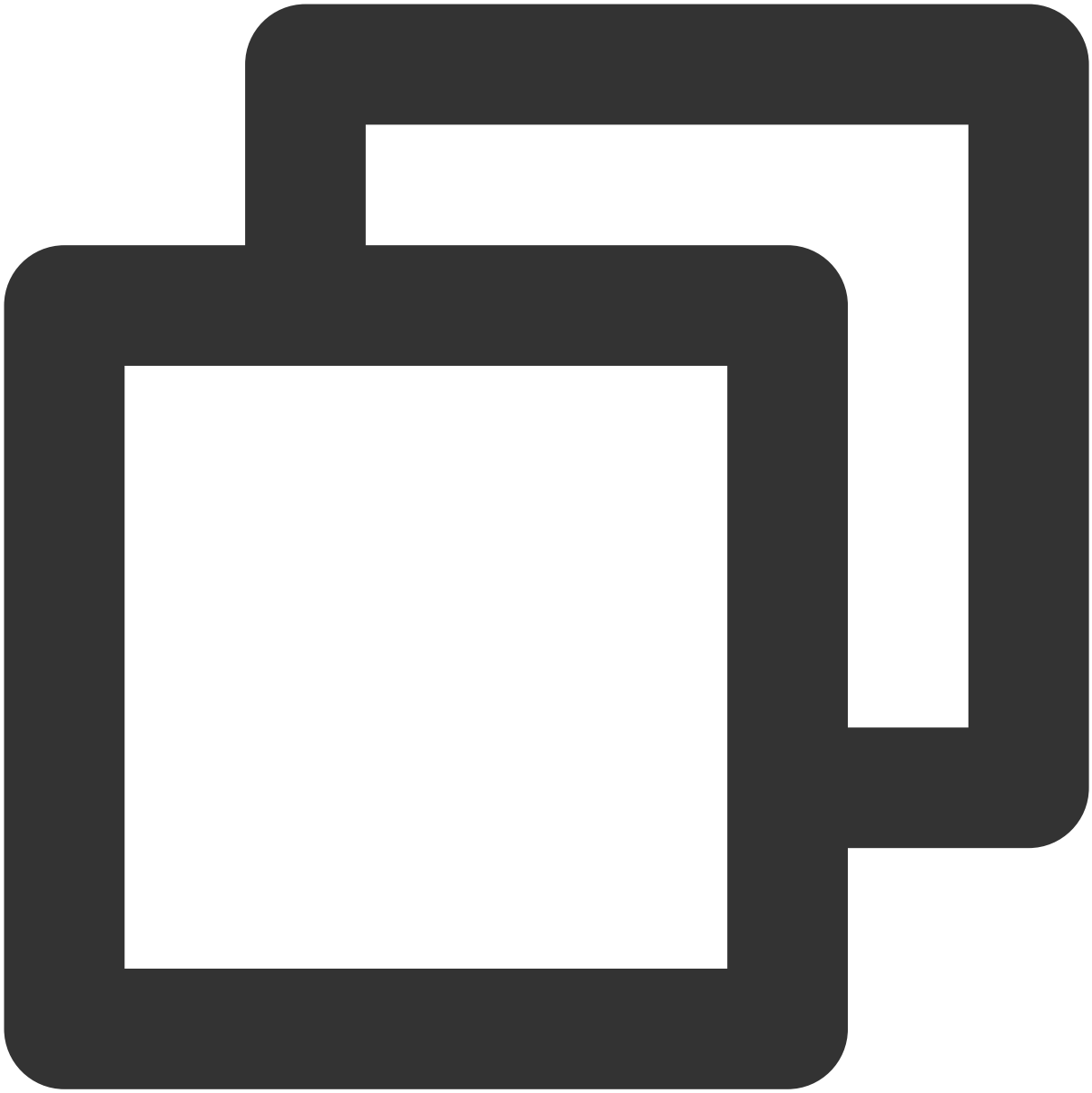
/etc/ssh/ssh_host_rsa_key ファイル権限の修正

1. VNCを使用してLinuxインスタンスにログイン。
2. 次のコマンドを実行し、エラーの原因を確認します。



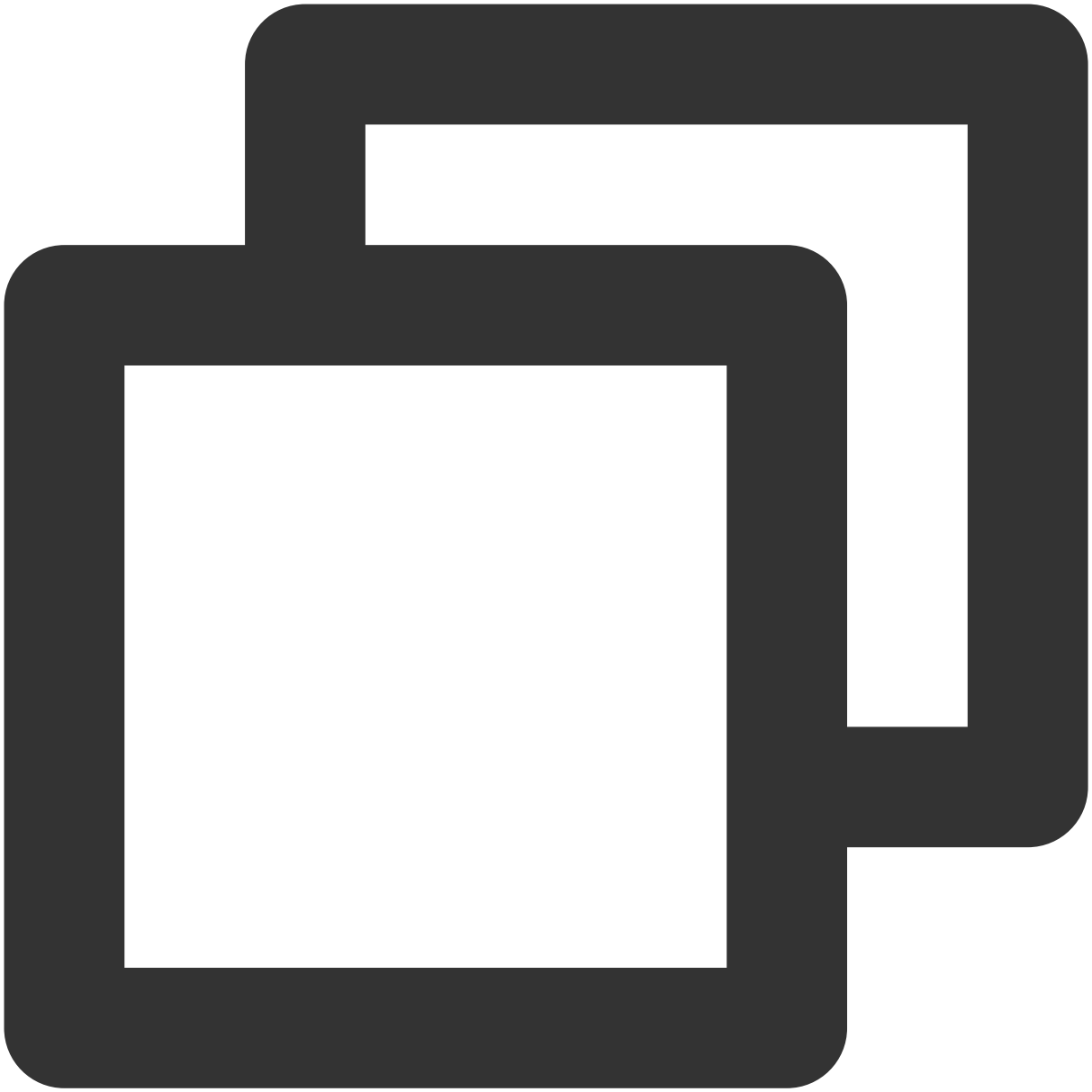
```
sshd -t
```

返される情報には次のようなフィールドが含まれます。



```
"/etc/ssh/ssh_host_rsa_key are too open"
```

3. 次のコマンドを実行し、`/etc/ssh/ssh_host_rsa_key` ファイル権限を修正します。



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

Linuxインスタンス：/etc/profile コールが無限ループする場合

最終更新日：：2023-06-08 17:41:26

##故障について
SSHを使用してLinuxインスタンスにログインする際、SSHコマンドが「Last login:」関連情報を出力した後にロックされました。

考えられる原因

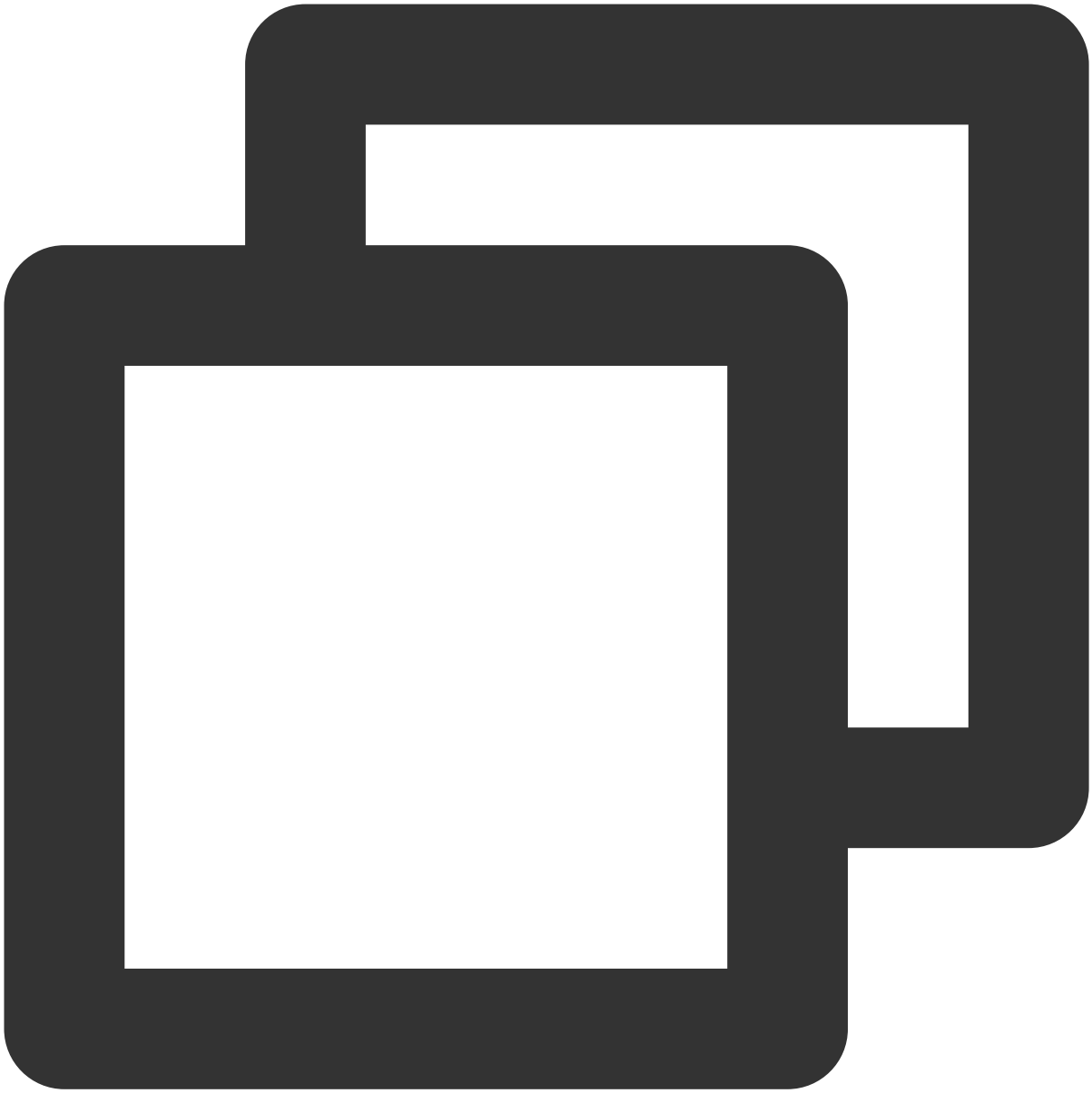
`/etc/profile` ファイルが変更されたことにより、 `/etc/profile` 内に `/etc/profile` をコールする現象が発生した可能性があります。そうなると、コールが無限ループ状態になり、ログインができなくなります。

ソリューション

処理手順 を参照し、 `/etc/profile` ファイルをチェックして修復します。

処理手順

1. VNCを使用してLinuxインスタンスにログイン。
2. 以下のコマンドを実行し、 `/etc/profile` ファイルを確認します。



```
vim  /etc/profile
```

3. `/etc/profile` ファイル内に `/etc/profile` 関連コマンドが含まれるかどうかをチェックします。
含まれる場合は、次の手順に進んでください。
含まれない場合は、チケットを提出 して連絡し、サポートを受けてください。
4. **i**で編集モードに入り、 `/etc/profile` 関連コマンドの前に `#` を追加してそのコマンドにコメントします。
5. **Esc**を押して編集モードを終了し、**:wq**を入力して変更を保存します。
6. 再度 SSHを使用してLinuxインスタンスにログイン でログインします。

サーバーが隔離されたためログインできない

最終更新日：：2022-04-07 16:31:02

このドキュメントでは、CVMはパブリックネットワークから分離されている場合に、ログインできない問題を解決する方法について説明します。

故障について

CVMは現在の法律や規制に違反しているため、分離されている可能性があります。以下の方法を使用して、CVMが分離されているかどうかを確認できます。
CVMがパブリックネットワークから分離されると、サイト内メール またはSMSを介して分離されていることを通知します。
「CVMコンソール」(https://console.tencentcloud.com/cvm/index) の中の「監視/ステータス」バーに、CVMのステータスが分離されていることが示されます。

問題の原因

CVMには規制違反またはリスクイベントが発生すると、ルールに違反したマシンを部分的に分離されます（プライベートネットワークのログインポート22、36000、3389を除き、他のネットワークアクセスは全て分離されます。開発者はジャンプサーバーを使用してサーバーにログインできます）。
詳細については、[クラウドセキュリティ違反レベルの分類とペナルティの説明]をご参照ください。

ソリューション

1. サイト内メール或はSMSの指示に従って、違反しているコンテンツを削除します。セキュリティリスクを対処し、必要に応じてシステムを再インストールします。
2. 個人の行動による違反ではない場合は、サーバーは悪意のある侵入があった可能性があります。 これを解決するには、ホストセキュリティをご参照ください。
3. セキュリティリスクを排除し、違反しているコンテンツを削除した後、チケットを送信 して、カスタマサービスに連絡して分離を解除させます。

帯域幅の利用率が高いためログインできない

最終更新日：：2024-01-05 14:21:54

このドキュメントでは、Linux と Windows CVMは帯域幅の使用量が高すぎることにより、リモートで接続できない時のトラブルシューティング方法と解決方法について説明します。

障害の現象

Tencent Cloud CVMコンソール にログインして、CVMの帯域幅監視データには、帯域幅の使用率が高すぎてCVMに接続できないことを示していることがわかります。
セルフ診断 ツールで帯域幅の使用量が高すぎると診断されました。

トラブルシューティング

1. 実際に使用するCVMインスタンスに対応し、VNCを使用してログインします：
Windowsインスタンス： VNCを使用してWindowsインスタンスにログインします
Linuxインスタンス：VNCを使用してLinuxインスタンスにログインします
2. CVMのトラブルシューティングと問題への対処：
Windows CVM
Linux CVM
VNCを使用してWindows CVMにログインした後、以下の操作を実行してください：
説明：
以下の操作では、 Windows Server 2012システムを使用したCVMを例として説明します。
1. CVMで、

クリックし、**タスクマネージャー**を選択して、「タスクマネージャー」を開きます。
2. **性能**タブを選択し、**リソースモニターを開く**をクリックします。
3. 開いた「リソースモニター」で、どのプロセスがより多くの帯域幅を消費しているかを確認します。実際の業務に基づいて、プロセスが正常に動作しているかを判断します。
帯域幅を大量に消費するプロセスが業務プロセスである場合、アクセス量の変化によるか、および容量を最適化する必要があるか、或は CVM設定をアップグレード する必要があるかどうかを確認します。
帯域幅を大量に消費するプロセスが異常なプロセスである場合は、ウイルス或はトロイの木馬が原因である可能性があります。プロセスを自分で終了する或はセキュリティソフトウェアを使用してウイルスを駆除できます。データのバックアップ後にシステムを再インストールすることもできます。

ご注意：

Windowsシステムでの多くのウイルスプログラムはシステムプロセスに偽装されています。**タスクマネージャー>プロセス**のプロセス情報を使用して初期識別を行います：

通常のシステムプロセスは完全な署名と説明があり、ほとんどはC:\\Windows\\System32ディレクトリにあります。ウイルスプログラムの名前はシステムプロセスの名前と同じかもしれませんが、署名や説明がなく、場所も通常ではないところにあります。

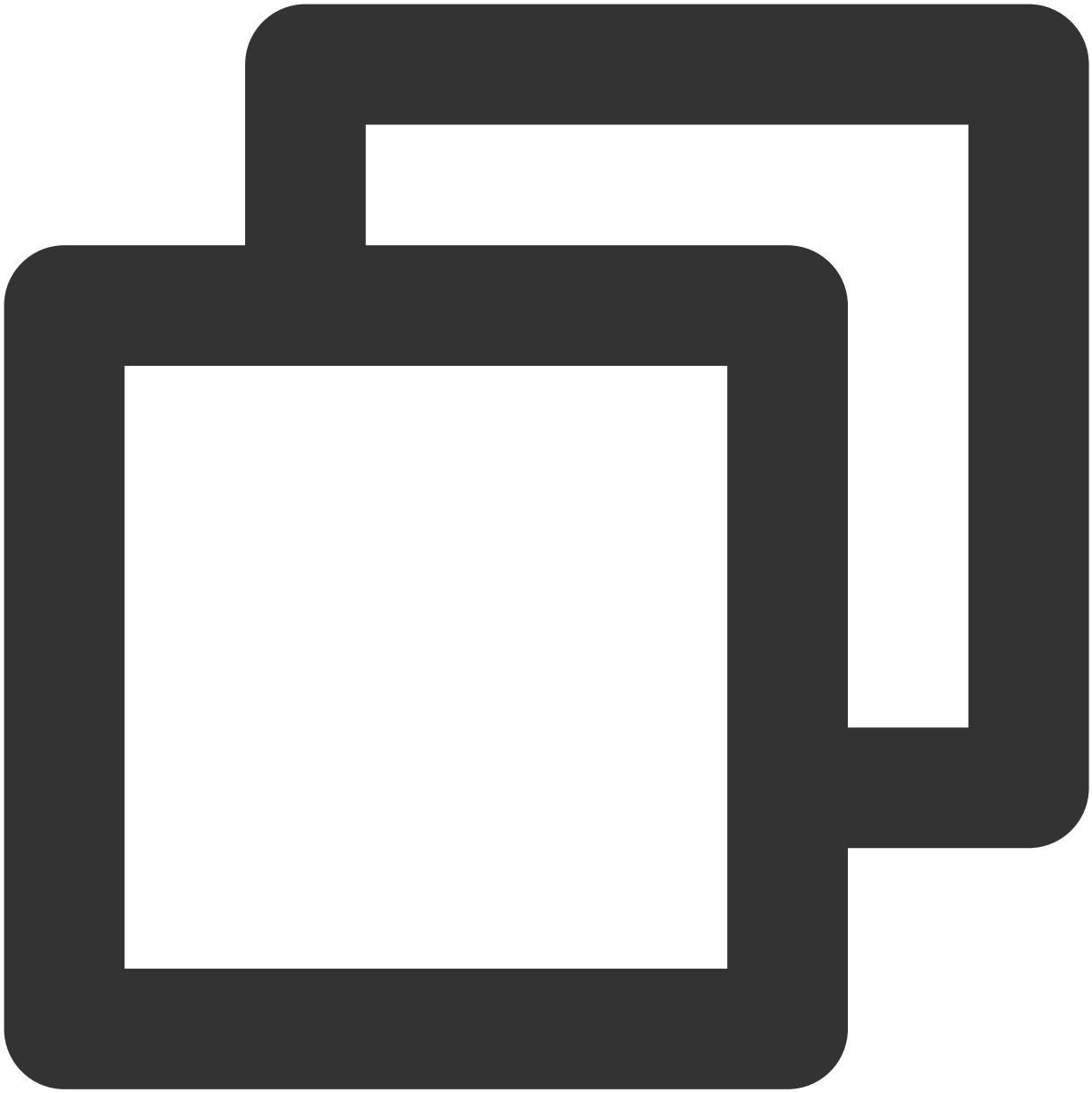
帯域幅を大量に消費するプロセスがTencent Cloudコンポーネントプロセスである場合は、チケットを送信 してお問い合わせください。問題に対処し、解決策を特定できるよう支援します。

VNCを使用してLinux CVMにログインした後、以下の操作を実行してください：

説明：

以下の操作では、CentOS 7.6システムを使用したCVMを例として説明します。

1. 以下のコマンドを実行して、iftop ツール（iftop ツールはLinux CVMのトラフィック監視ツール）をインストールします。

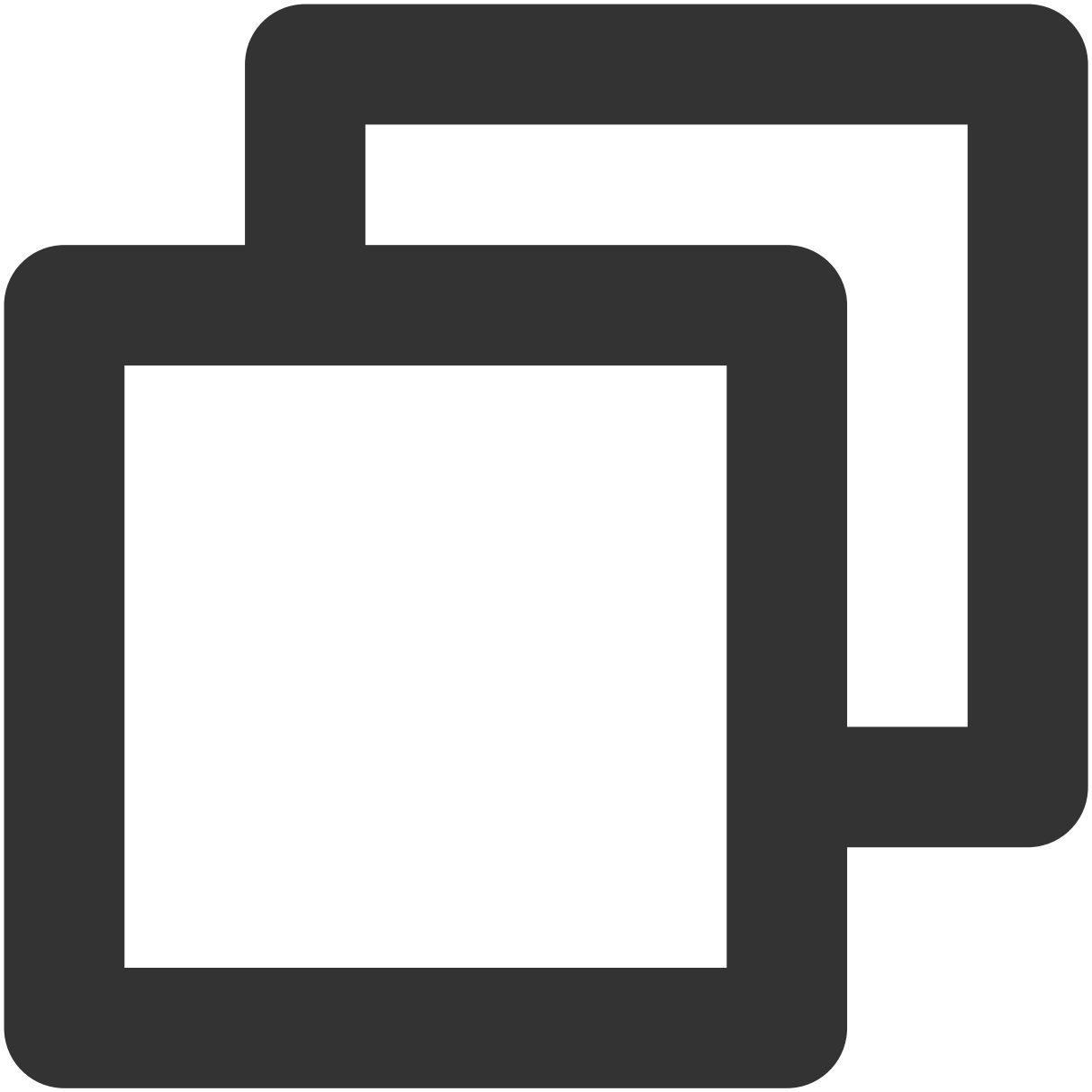


```
yum install iftop -y
```

説明：

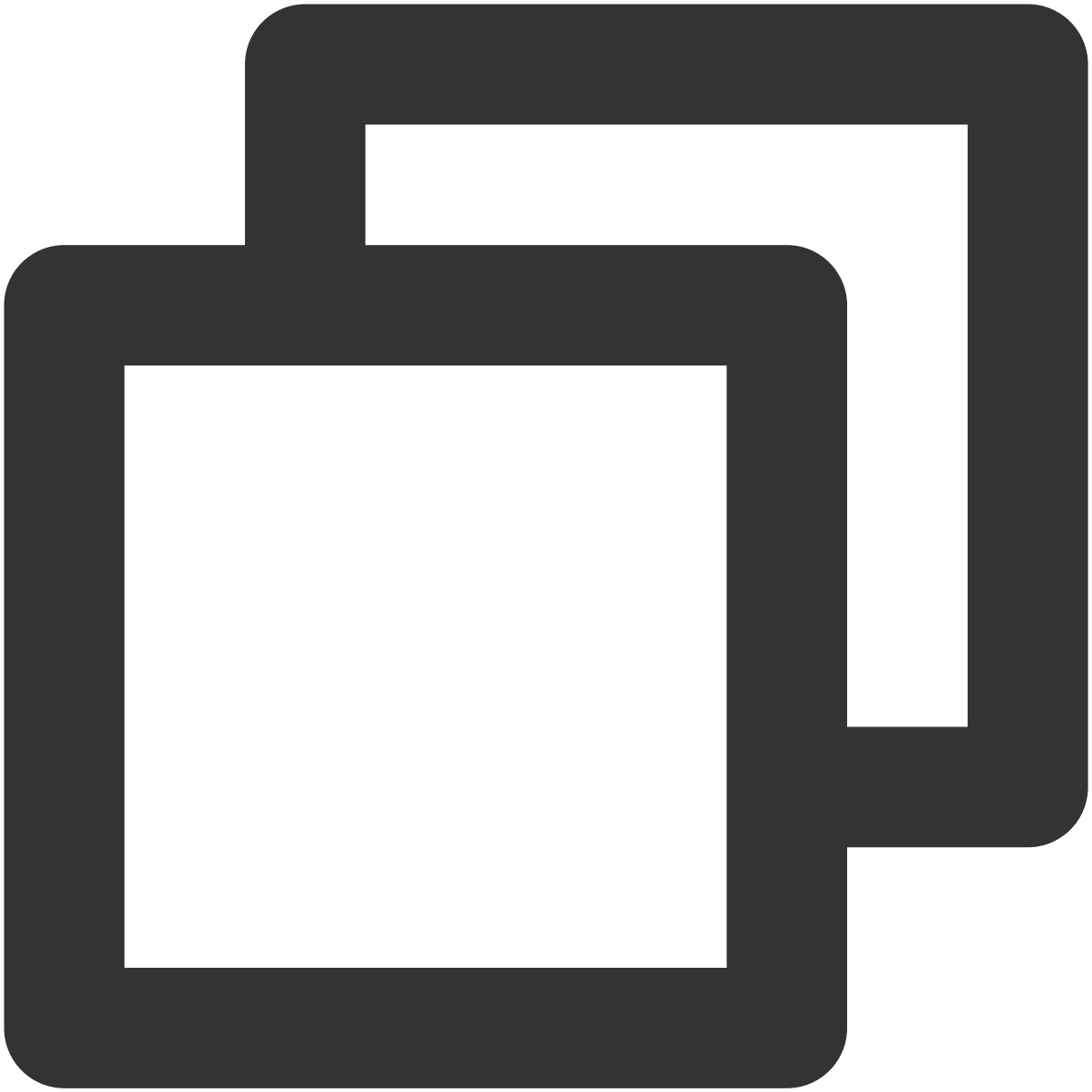
Ubuntuシステムの場合、 `apt-get install iftop -y` コマンドを実行してください。

2. 以下のコマンドを実行し、lsofをインストールします。

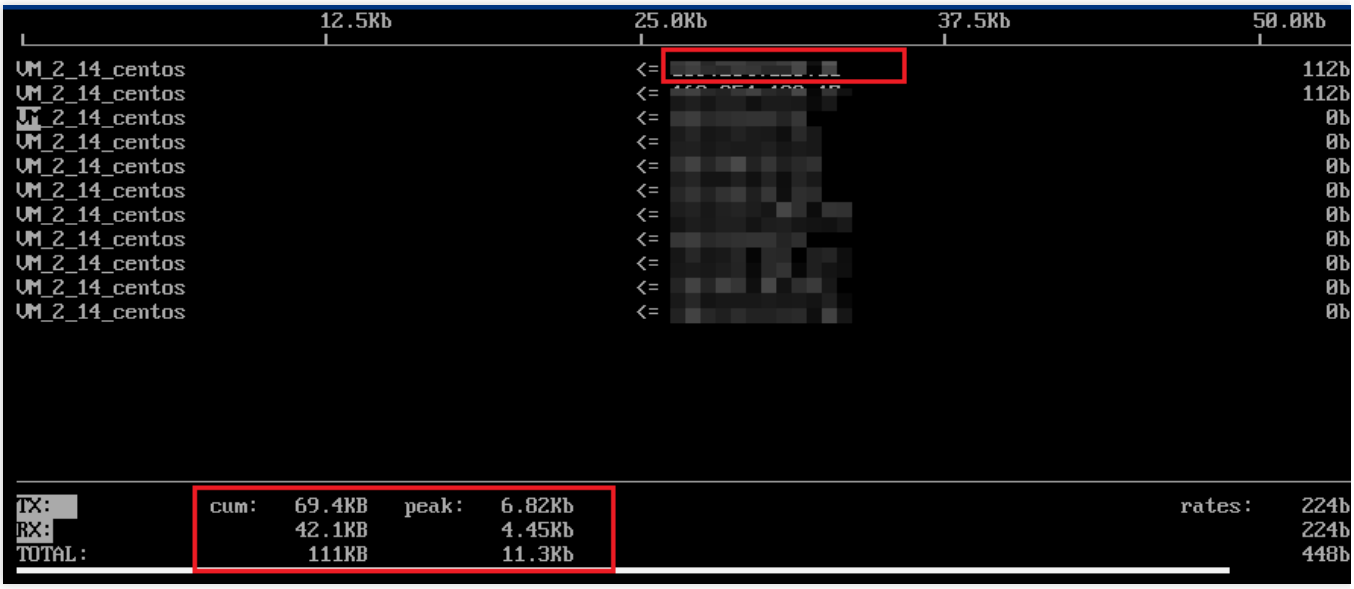


```
yum install lsof -y
```

3. 以下のコマンドを実行し、 iftopを実行します。 下図に示すとおりです：



```
iftop
```



`<=` 、 `=>` はトラフィックの方向を示します

TX は送信トラフィックを示します

RX は受信トラフィックを示します

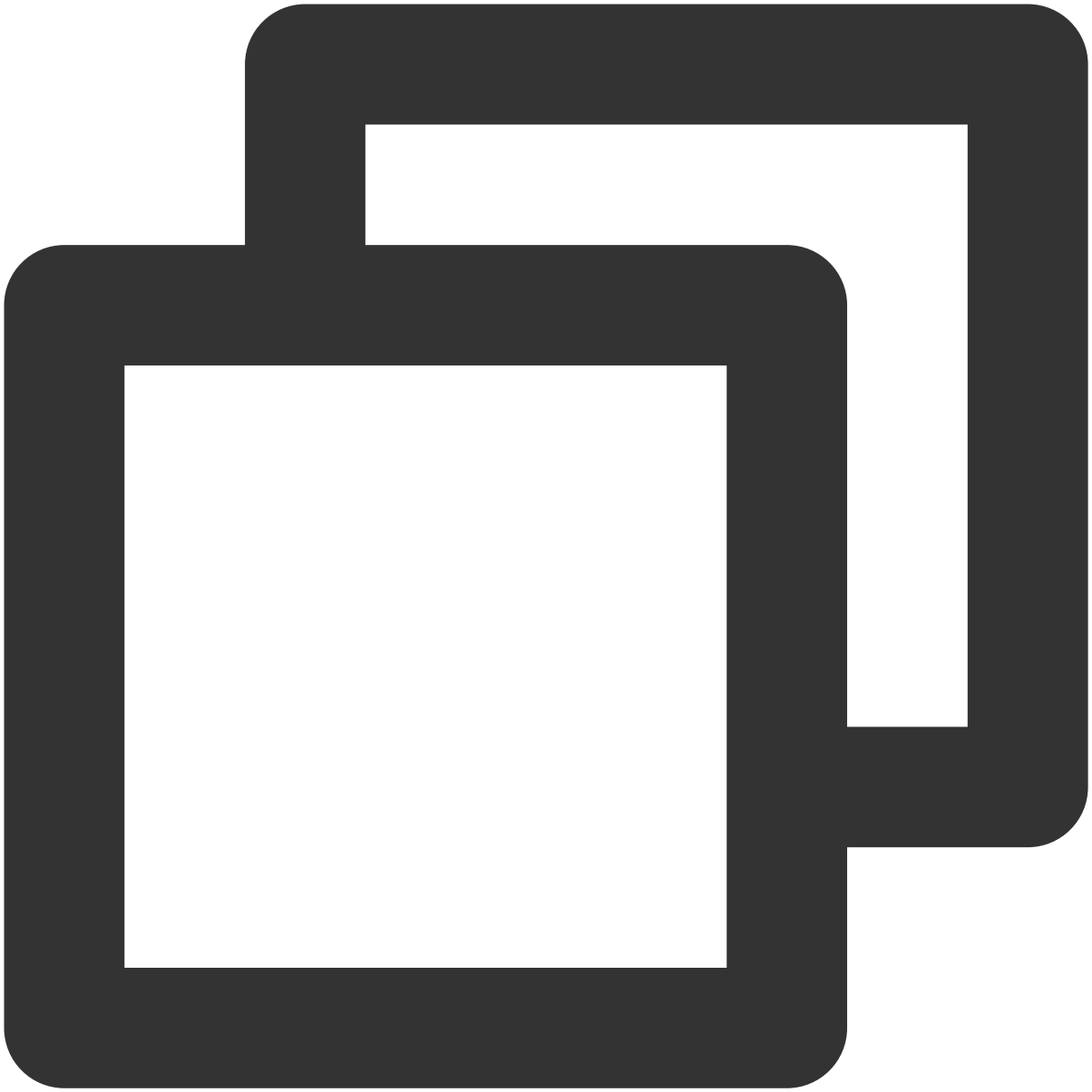
TOTALは総トラフィックを示します

Cumはiftopを実行を開始した瞬間から現在までの総トラフィックを示します

peak はトラフィックのピークを示します

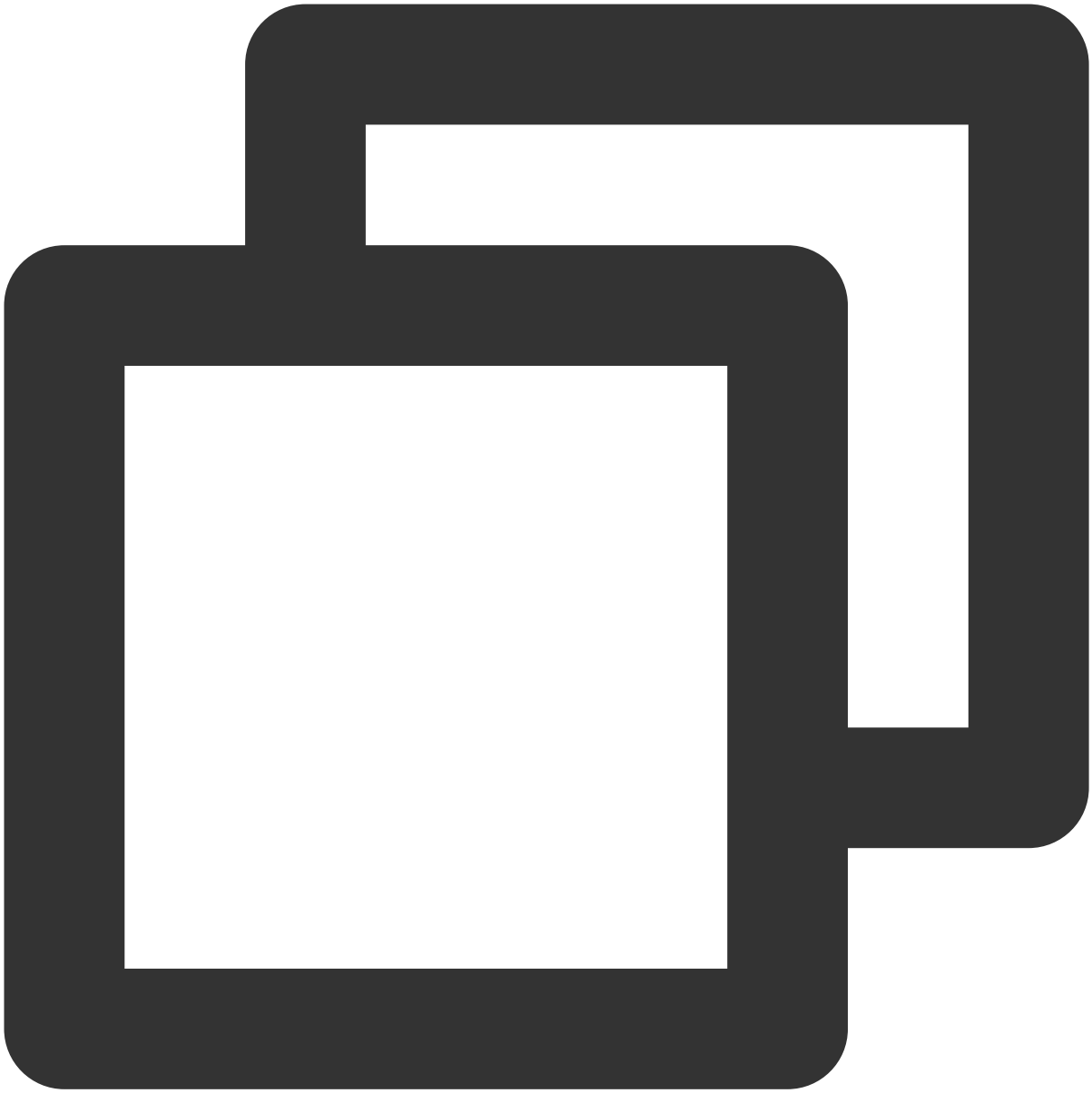
rates はそれぞれ過去2s、10sと40s間の平均トラフィックを示します

4. iftop で消費されたトラフィックのIPに従って、以下のコマンドを実行して、このIPに接続されているプロセスを確認します。



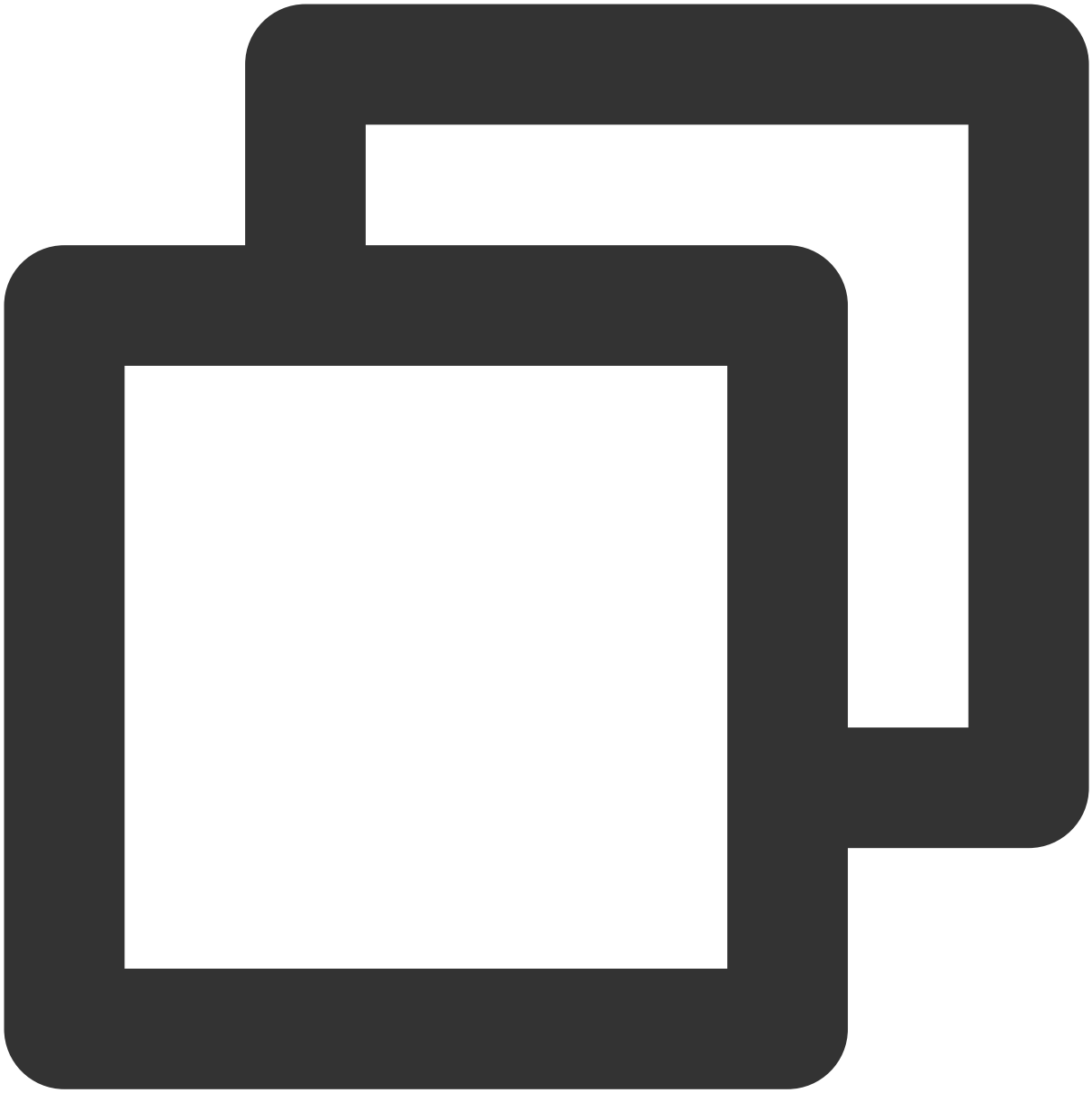
```
lsof -i | grep IP
```

例えば、消費されたトラフィックのIPが201.205.141.123の場合、以下のコマンドを実行します：



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

次の結果が返される場合、CVM帯域幅は主にSSHプロセスによって消費されることが分ります。



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

5. 帯域幅を消費するプロセスを確認して、プロセスが正常に動作しているかを判断します。
帯域幅を大量に消費するプロセスが業務プロセスである場合、アクセス量の変化によるか、および容量を最適化する必要があるか、或は CVM設定をアップグレード する必要があるかどうかを確認します。
帯域幅を大量に消費するプロセスが異常なプロセスである場合は、ウイルス或はトロイの木馬が原因である可能性があります。プロセスを自分で終了する或はセキュリティソフトウェアを使用してウイルスを駆除できます。データのバックアップ後にシステムを再インストールすることもできます。

帯域幅を大量に消費するプロセスがTencent Cloudコンポーネントプロセスである場合は、チケットを送信 してお問い合わせください。問題に対処し、解決策を特定できるよう支援します。
対象側IPアドレスの所在地を重点的にチェックすることをお勧めします。IP138検索サイトでIPアドレス所在地を検索できます。対象側IPのアドレスの所在地が海外である場合は、リスクが高く、重点的に注意してください。

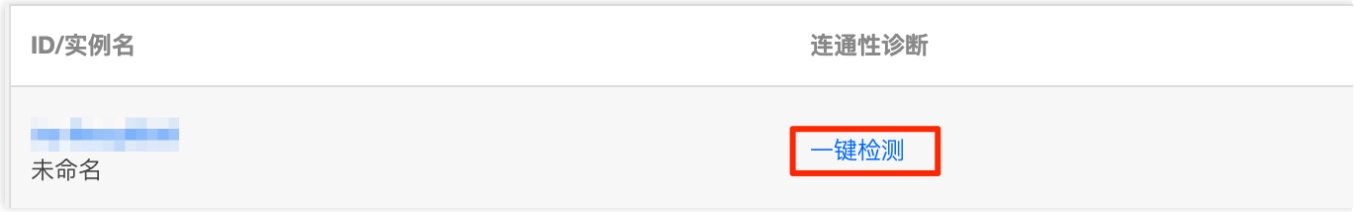
セキュリティグループの設定が原因でリモート接続できない

最終更新日：：2022-05-26 18:50:48

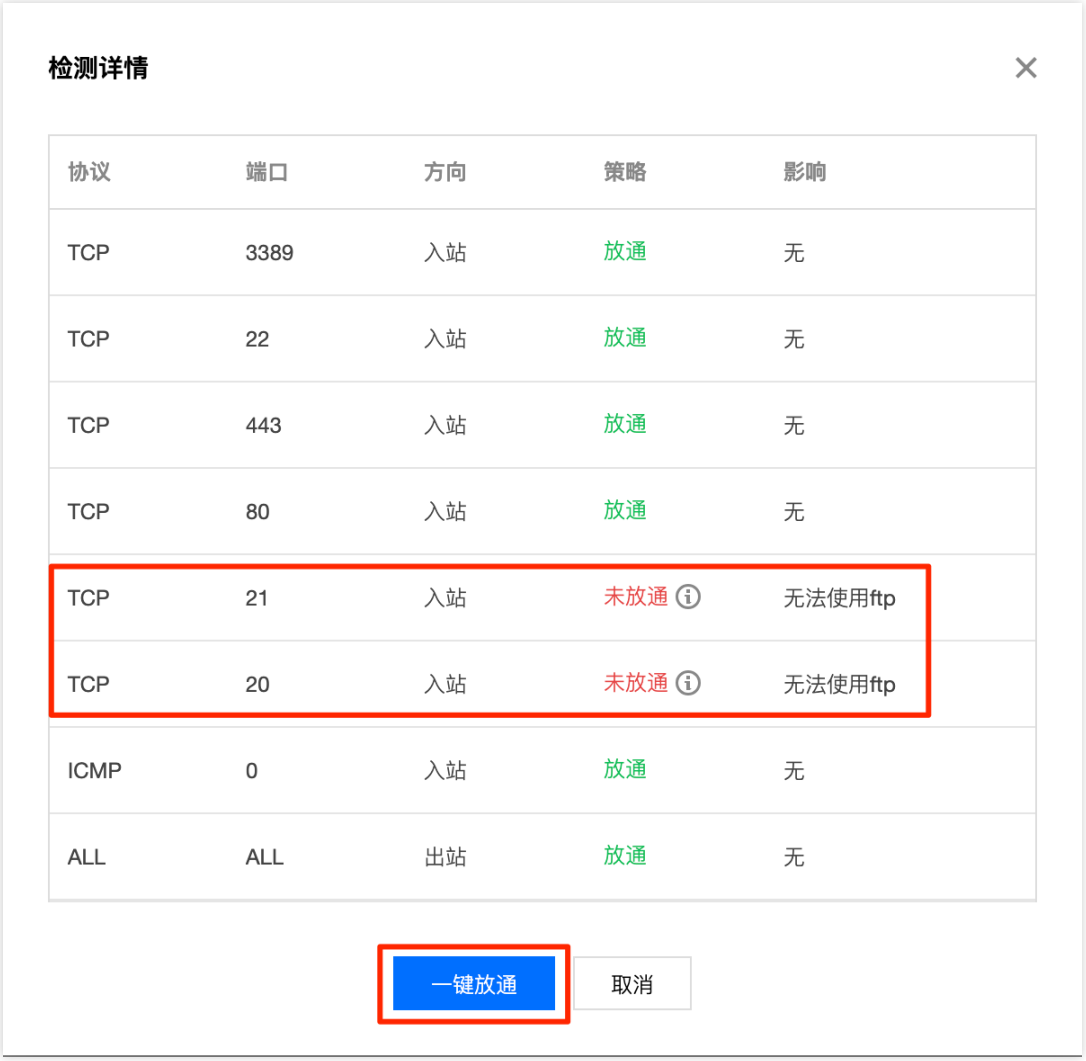
本ドキュメントでは、CVMはセキュリティグループの設定が原因で、リモート接続できない問題のトラブルシューティング方法と解決案について説明します。

検証ツール

Tencent Cloudが提供する セキュリティグループ（ポート）検証ツール を使用して、リモート接続できないことがセキュリティグループの設定に関連しているかどうかを判断できます。
1. セキュリティグループ（ポート）検証ツール にログインします。
2. **Port Verification**画面で、検出対象のインスタンスを選択し、**Quick Check**をクリックします。 下記画像に示すように：



このインスタンスが開放していないポートを検出された場合、**Open all ports**機能を利用して、サーバーで一般的に使用されるポートを開放し、リモートログインを再試行します。



セキュリティグループの設定を変更する

検証ツールを利用して、セキュリティグループのポート設定に問題があることが確認されたら、**Open all ports**機能を利用してCVMの一般的に使用されるポートをインターネットにを開放したくない、またはリモートログインポートをカスタマイズする必要がある場合、セキュリティグループのインバウンドとアウトバウンドルールをカスタマイズして、リモート接続の問題を解決できます。 詳細の操作については、セキュリティグループルールの変更をご参照ください。

LinuxインスタンスのVNC使用およびレスキューモードを使用したトラブルシューティング

最終更新日：：2022-07-21 18:01:18

通常、Linuxシステムの問題のほとんどは、VNC方式とレスキューモードを使用したトラブルシューティングで解決することができます。ここでは、この2つの方法を用いて、SSHログインができない、システムの障害発生などに対しトラブルシューティングを行う方法についてご説明します。インスタンスのトラブルシューティングと修復の方法について学ぶことができます。

トラブルシューティングツール

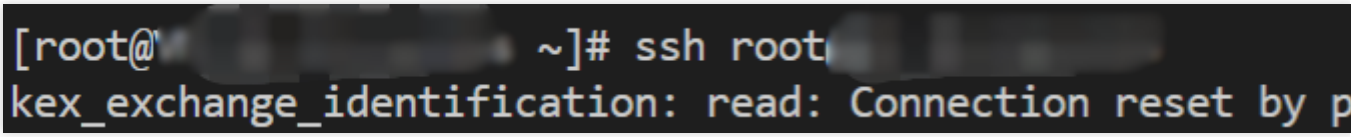
VNCログインは、Webブラウザを使ってCVMにリモート接続する方法であり、通常は、正常なSSHリモートログインができない場合に使用します。VNCログイン方式を使用すると、CVMのステータスの直接観察やシステム内の設定ファイルの変更といった操作が可能です。
レスキューモードは、通常、Linuxシステムが正常に起動しない場合やVNCでログインできない場合に使用します。一般的なユースケースとしては、fstab設定の異常、重要なシステムファイルの欠落、lib動的ライブラリファイルの破損/欠落などがあります。

問題の特定および処理

VNC方式によるSSHログインのトラブルシューティング方法

現象の説明

SSHを使用してLinuxインスタンスにログインすると、下図のように、「ssh_exchange_identification: Connection closed by remote host」というエラー情報が表示されます。



考えられる原因

kex_exchange_identificationフェーズでのconnection resetエラーは、通常、ssh関連のプロセスが開始されたことを意味しますが、sshd設定ファイルの権限が変更されているなど、設定に異常がある可能性があります。

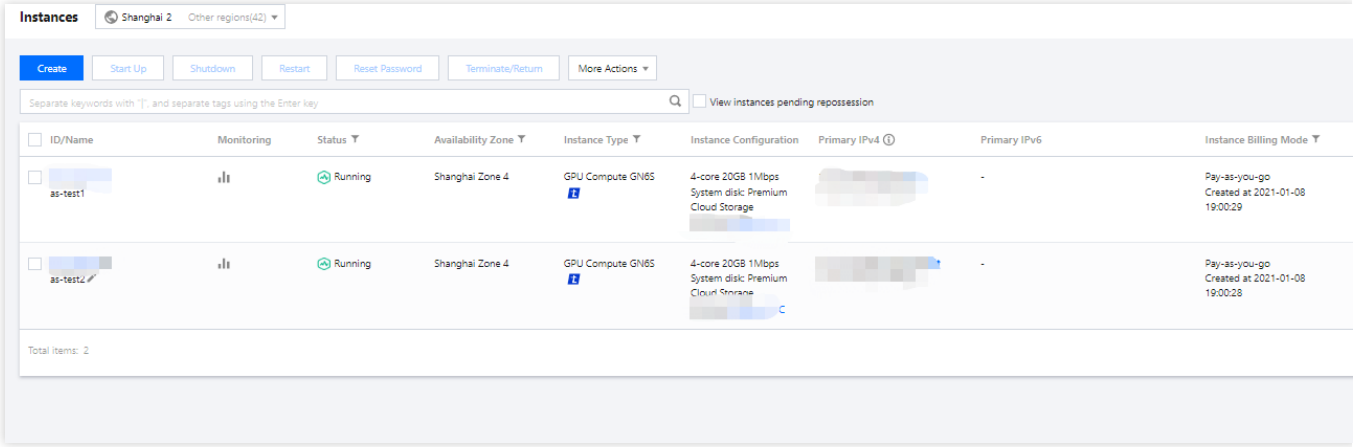
解決方法

処理手順 を参照し、sshdのプロセスをチェックして、問題を特定して解決します。

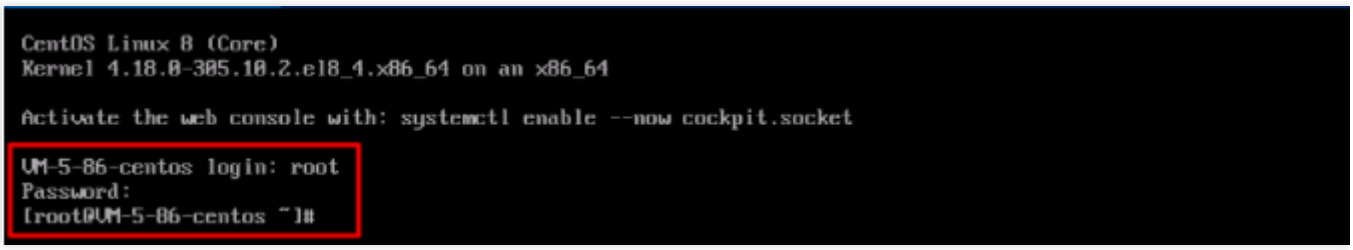
処理手順

以下の手順を参照し、VNCを使用してLinuxインスタンスにログインします。

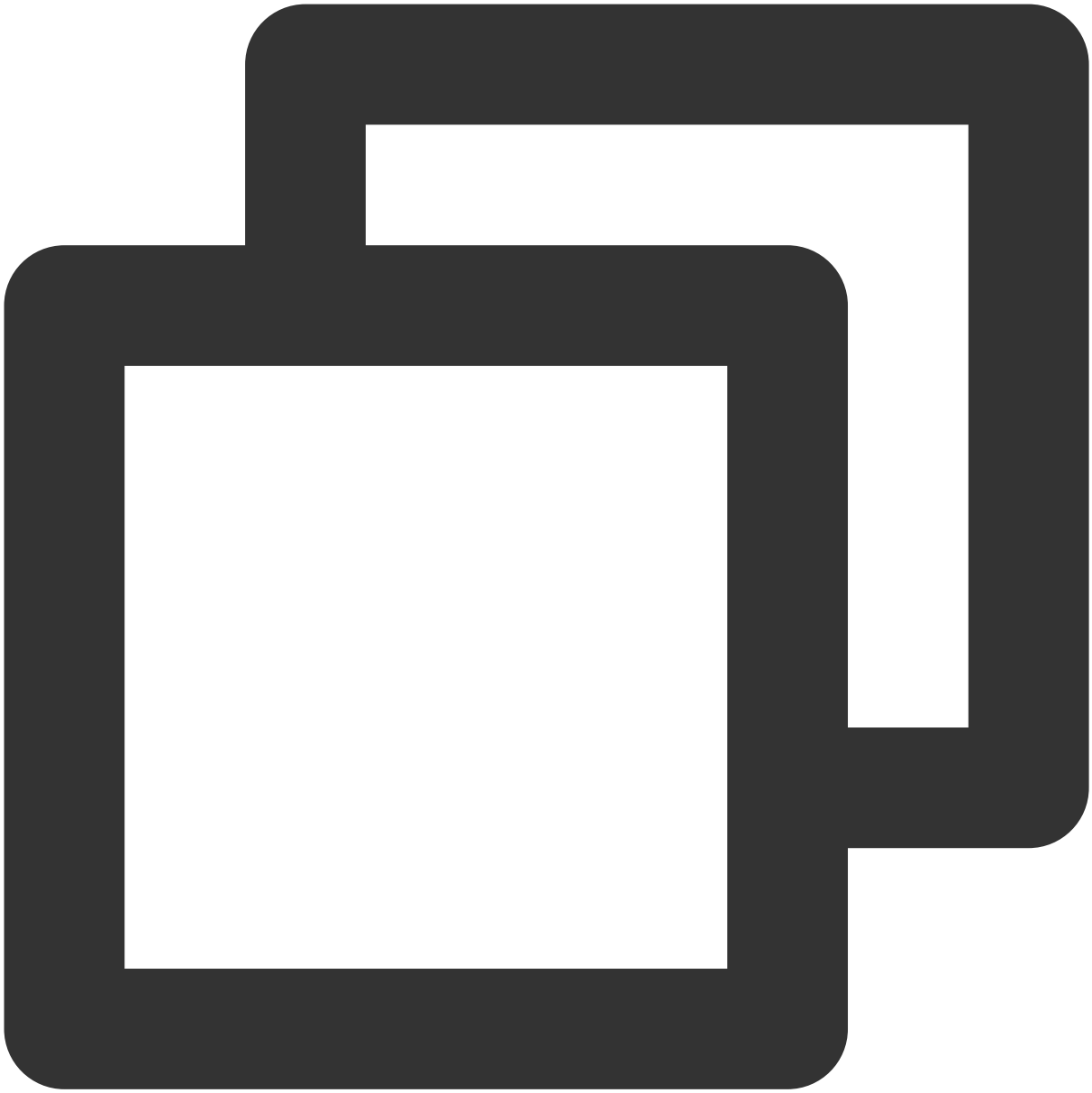
1. 下
図に示すよ
うに、CVMコンソール にログインし、ログインしたいLinux CVMを見つけて、右側の**ログイン**をクリックします。



2. 開いた「標準ログイン | Linuxインスタンス」ウィンドウで、**VNCログイン**をクリックします。
3. 「login」の後にユーザー名を入力し、**Enter**を押します。「Password」の後にパスワードを入力し、**Enter**を押します。下図のようになれば、ログインに成功しています。



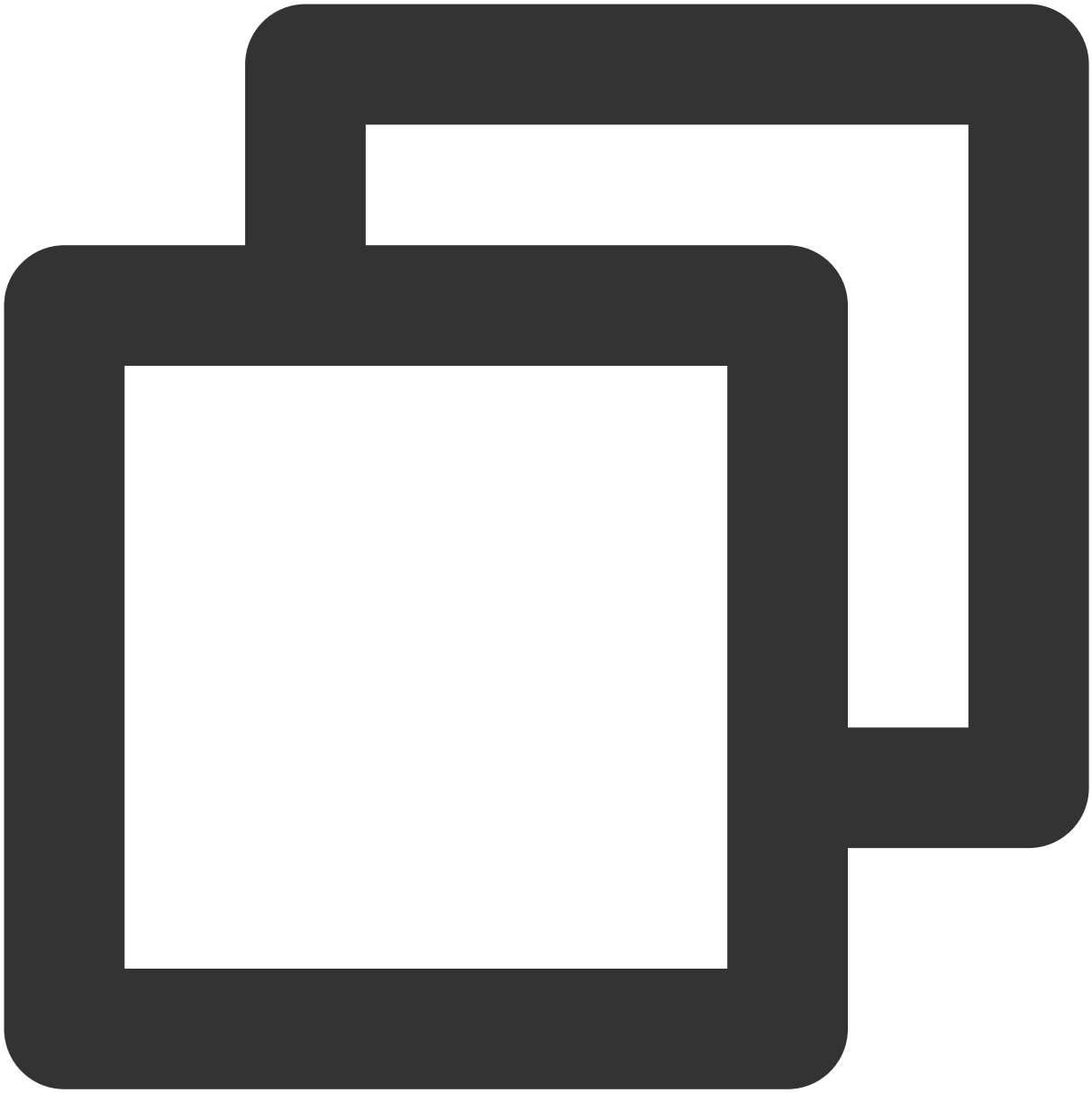
4. 以下のコマンドを実行し、sshdプロセスが正常に動作しているか確認します。



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

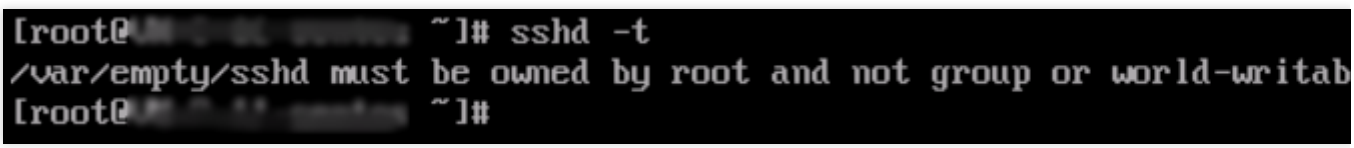
下図のような結果が返されれば、sshdプロセスは正常です。

5. 次のコマンドを実行し、エラーの原因を確認します。

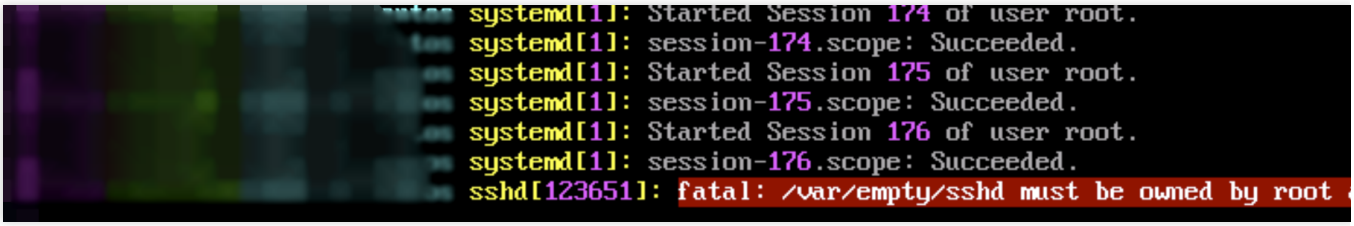


```
sshd -t
```

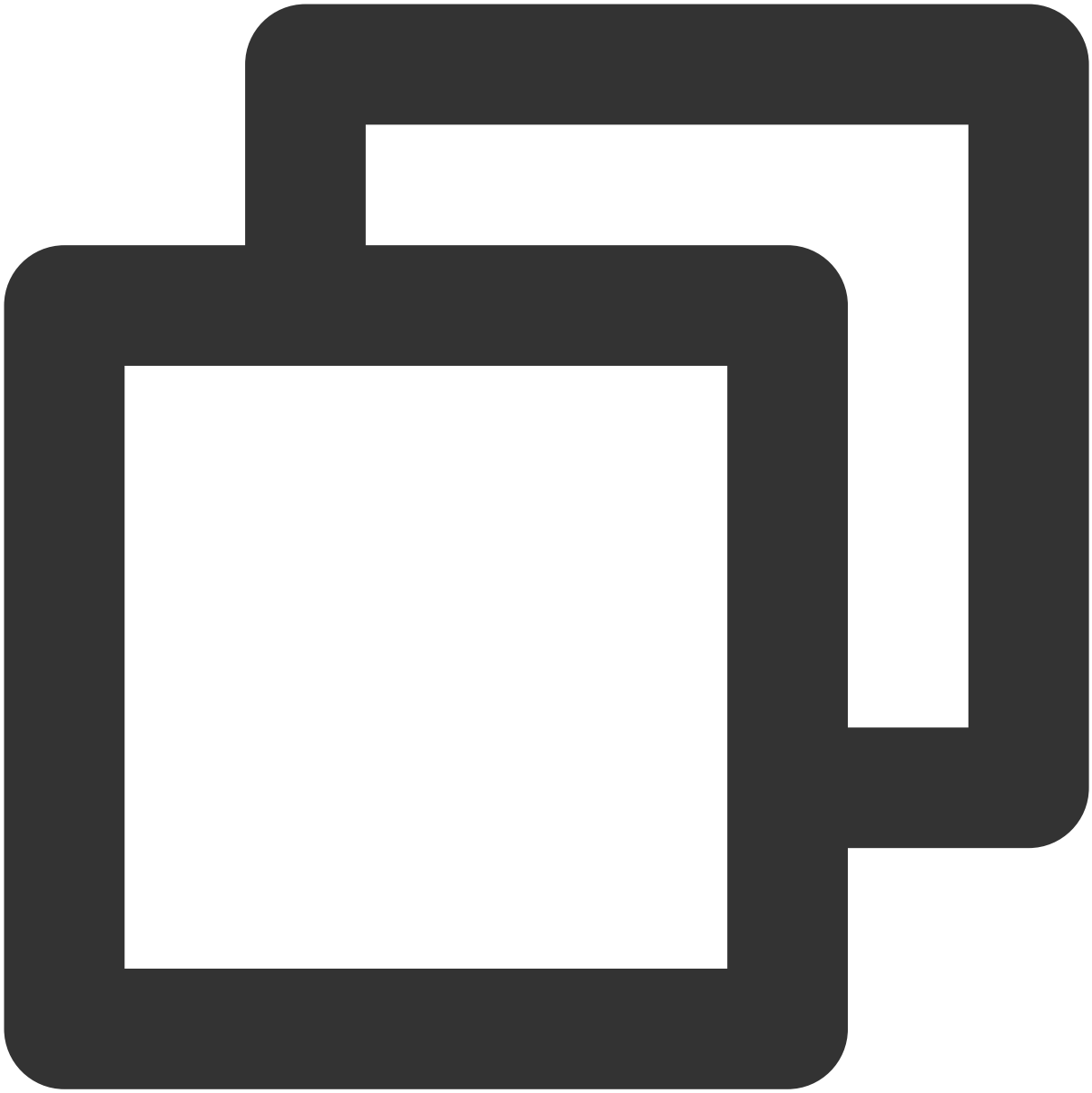
下図のような情報、"/var/empty/sshd must be owned by root and not group or world-writable.
"が返された場合、エラーの原因は、 `/var/empty/sshd/` の権限の問題である可能性があります。



また、下図に示すように、`/var/log/secure` ログにあるエラー情報を確認することで、トラブルシューティングを支援することができます。

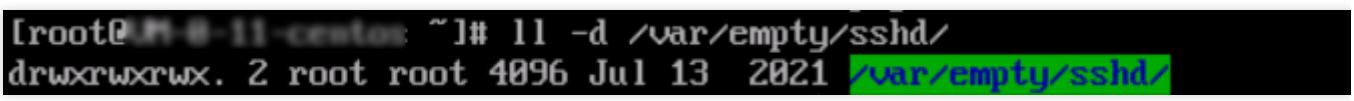


6. 次のコマンドを実行して、`/var/empty/sshd` ディレクトリの権限を確認します。

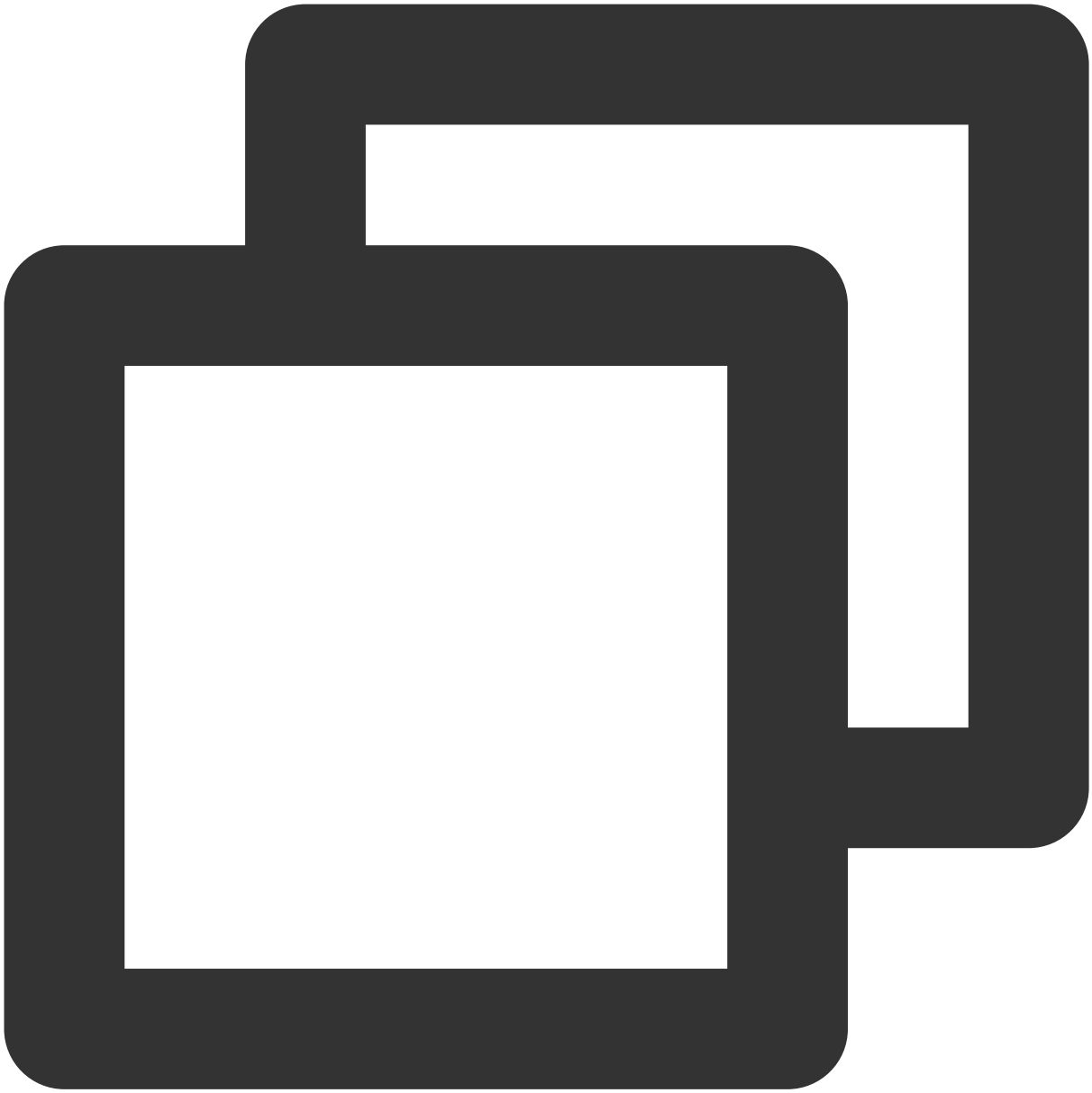


```
ll -d /var/empty/sshd/
```

下図のような結果が返されます。権限が777に変更されたことがわかります。



7. 次のコマンドを実行し、 `/var/empty/sshd/` ファイル権限を変更します。



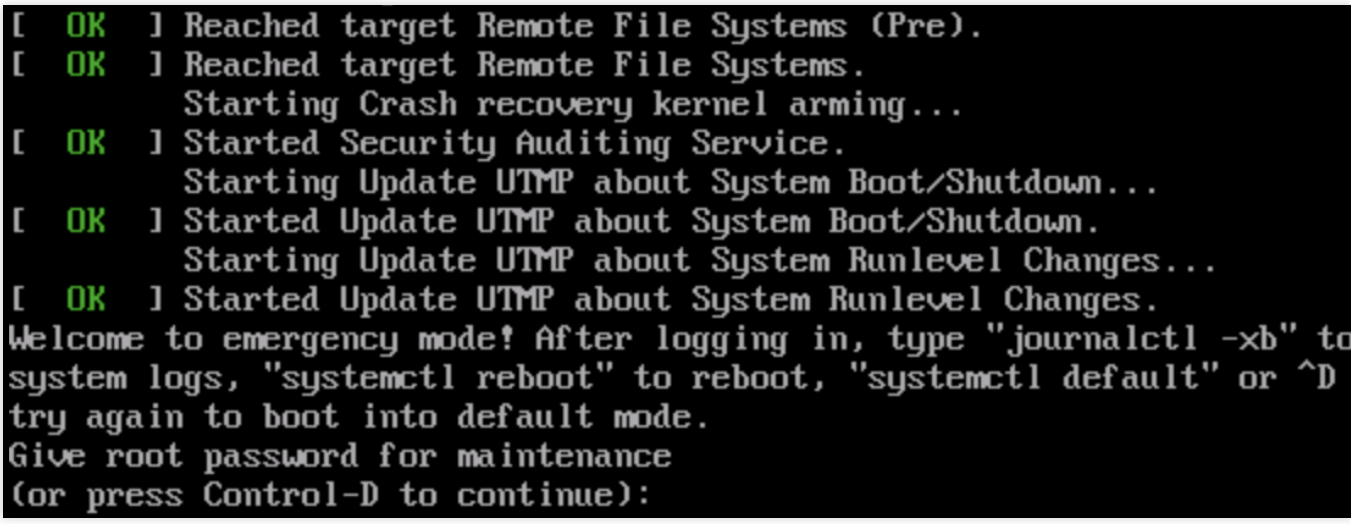
```
chmod 711 /var/empty/sshd/
```

SSHを使用してLinuxインスタンスにログイン を参照してテストを行うと、正常にインスタンスにリモートログインできるようになります。

VNC方式によるLinuxシステムの起動失敗のトラブルシューティング

現象の説明

SSHでLinux CVMへの正常なリモートログインができず、VNC方式でログインすると、システムの起動失敗が確認され、下図のように「Welcome to emergency mode」というメッセージが表示されます。



考えられる原因

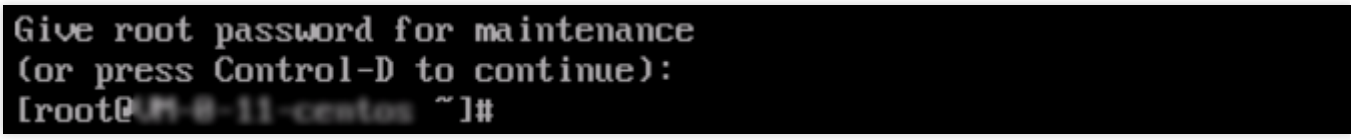
`/etc/fstab` の設定が不適切であることが原因という可能性があります。
例えば、 `/etc/fstab` においてディスクがデバイス名で自動的にマウントされるように設定されている場合も、CVMを再起動するとデバイス名が変わってしまい、システムが正常に起動しなくなることがあります。

解決方法

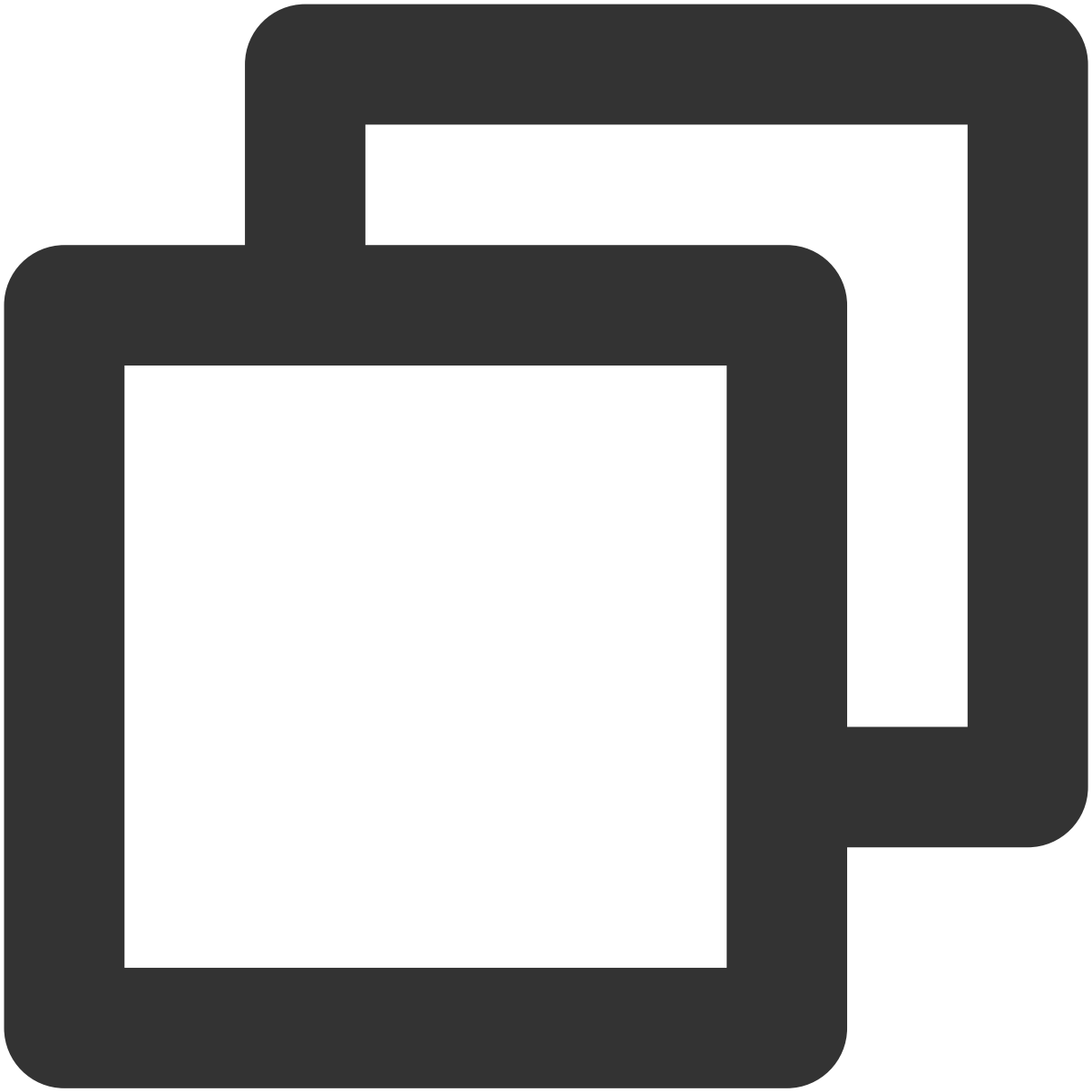
処理手順 を参照して `/etc/fstab` 設定ファイルを修復し、サーバーを再起動してから検証します。

処理手順

1. 処理手順1 を参照し、VNCを使用してLinuxインスタンスにログインします。
2. 下図に示すように、VNCインターフェースに進み、現象の説明 のようなインターフェースが表示されたら、rootアカウントのパスワードを入力し、**Enter**を押してサーバーにログインしてください。入力されたパスワードは、デフォルトでは表示されません。



3. システムに入った後、以下のコマンドを実行し、fstabファイル内のボリュームラベル情報が正しいかどうかを確認します。

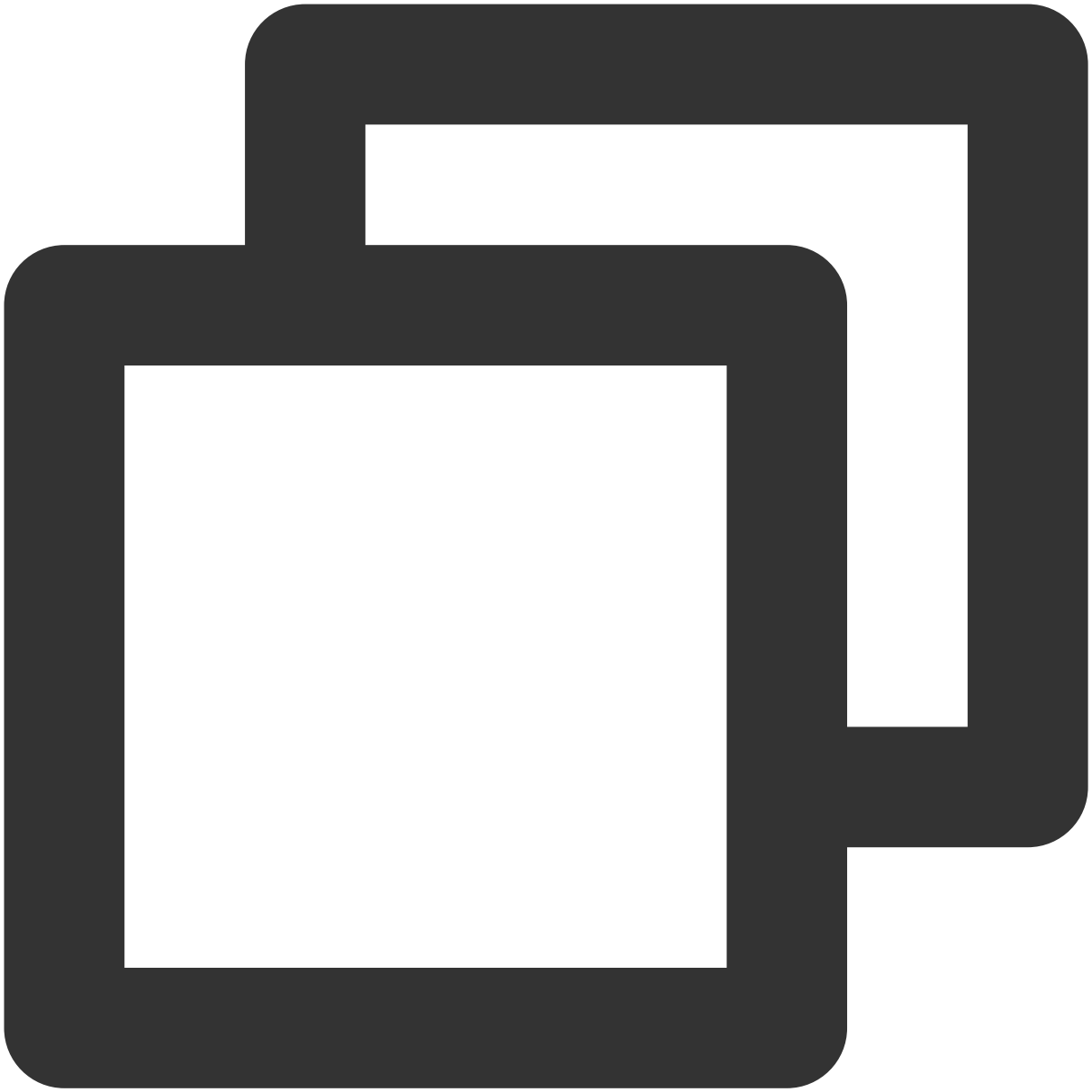


```
lsblk
```

下図のような結果が返されます。ファイル内ボリュームラベル情報に誤りがあります。

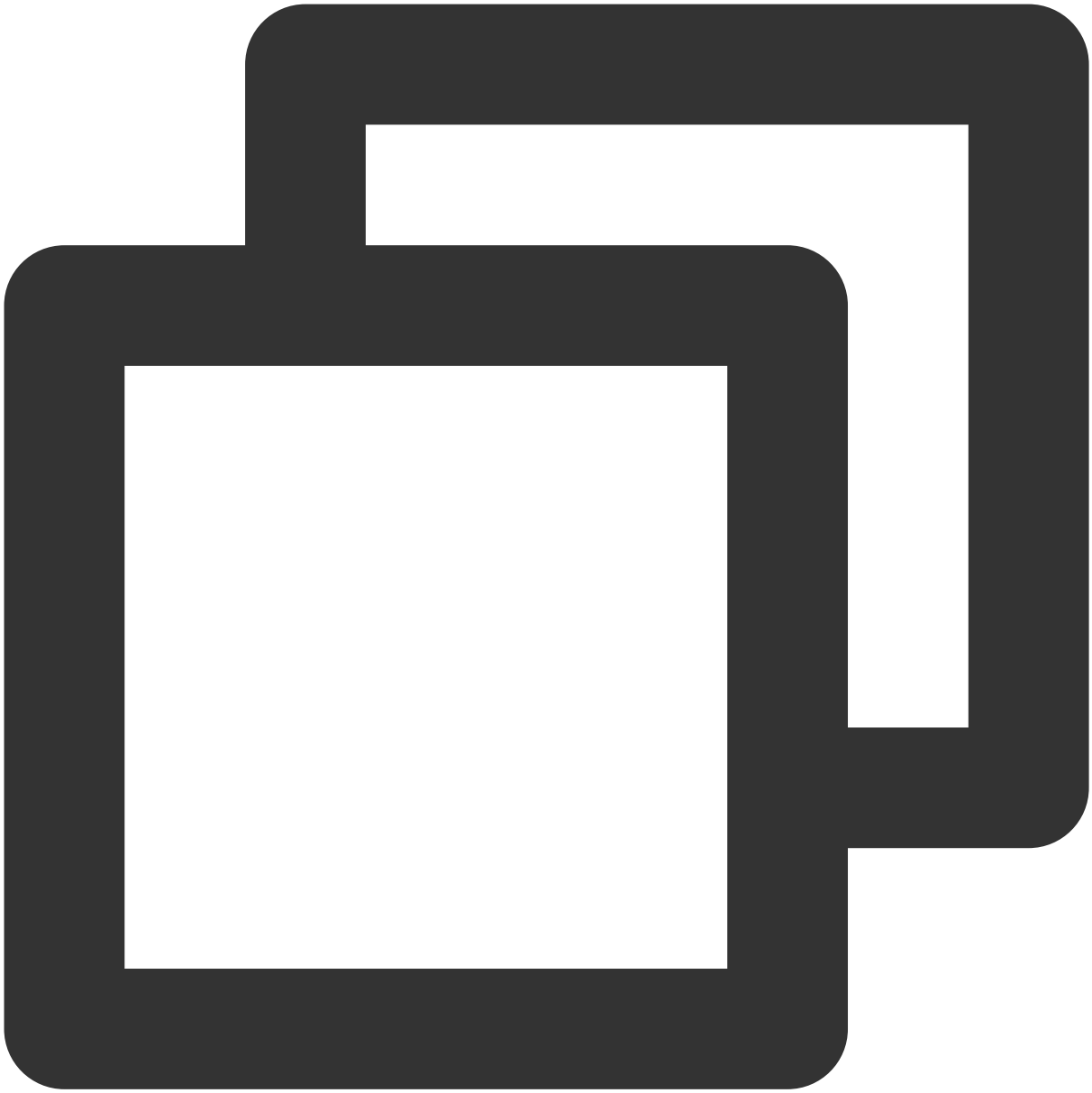
```
[root@V                    ~]# lsblk
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sr0     11:0    1 184.1M  0 rom
vda    253:0    0    50G  0 disk
└─vda1 253:1    0    50G  0 part /
[root@                     ~]# cat /etc/fstab

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

4. 以下のコマンドを実行し、fstabファイルのバックアップを取ります。



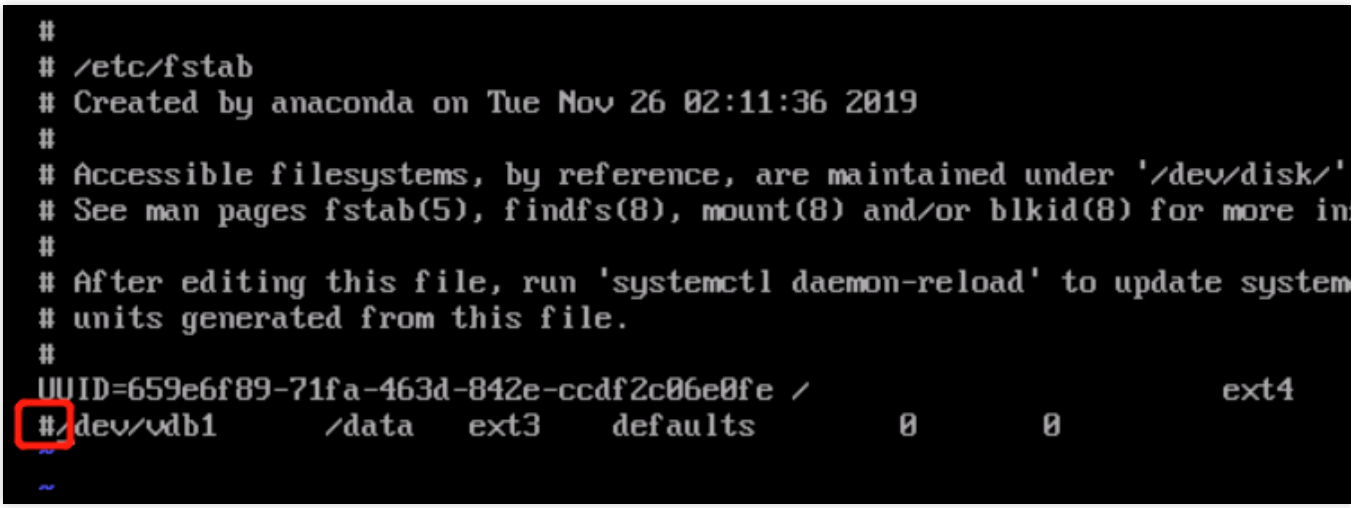
```
cp /etc/fstab /home
```

5. 以下のコマンドを実行し、VIエディタを使用して `/etc/fstab` ファイルを開きます。



```
vi /etc/fstab
```

6. 下図に示すように、**i**を押して編集モードに入り、カーソルを設定エラーの行の先頭に移動させ、 `#` を入力して行の設定についてコメントアウトします。



7. **Esc**を押して**:wqと入力した後、Enter**を押して設定を保存し、エディタを終了します。
8. コンソールからインスタンスを再起動します。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。
9. 正常に起動、ログインできるかどうかを検証します。

レスキューモードによるLinuxシステムの起動失敗のトラブルシューティング

現象の説明

下図に示すように、Linuxシステムが再起動後に起動せず、多数のFAILED起動失敗の項目が情報に表示されています。

考えられる原因

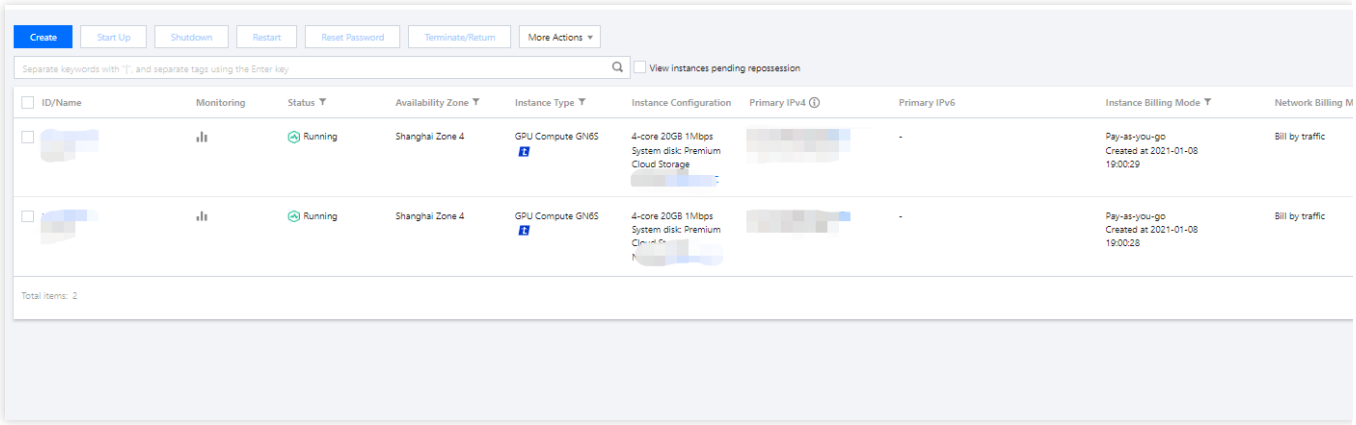
binファイルやlibファイルなど、重要なシステムファイルの欠落が原因で起動に失敗することがあります。

解決方法

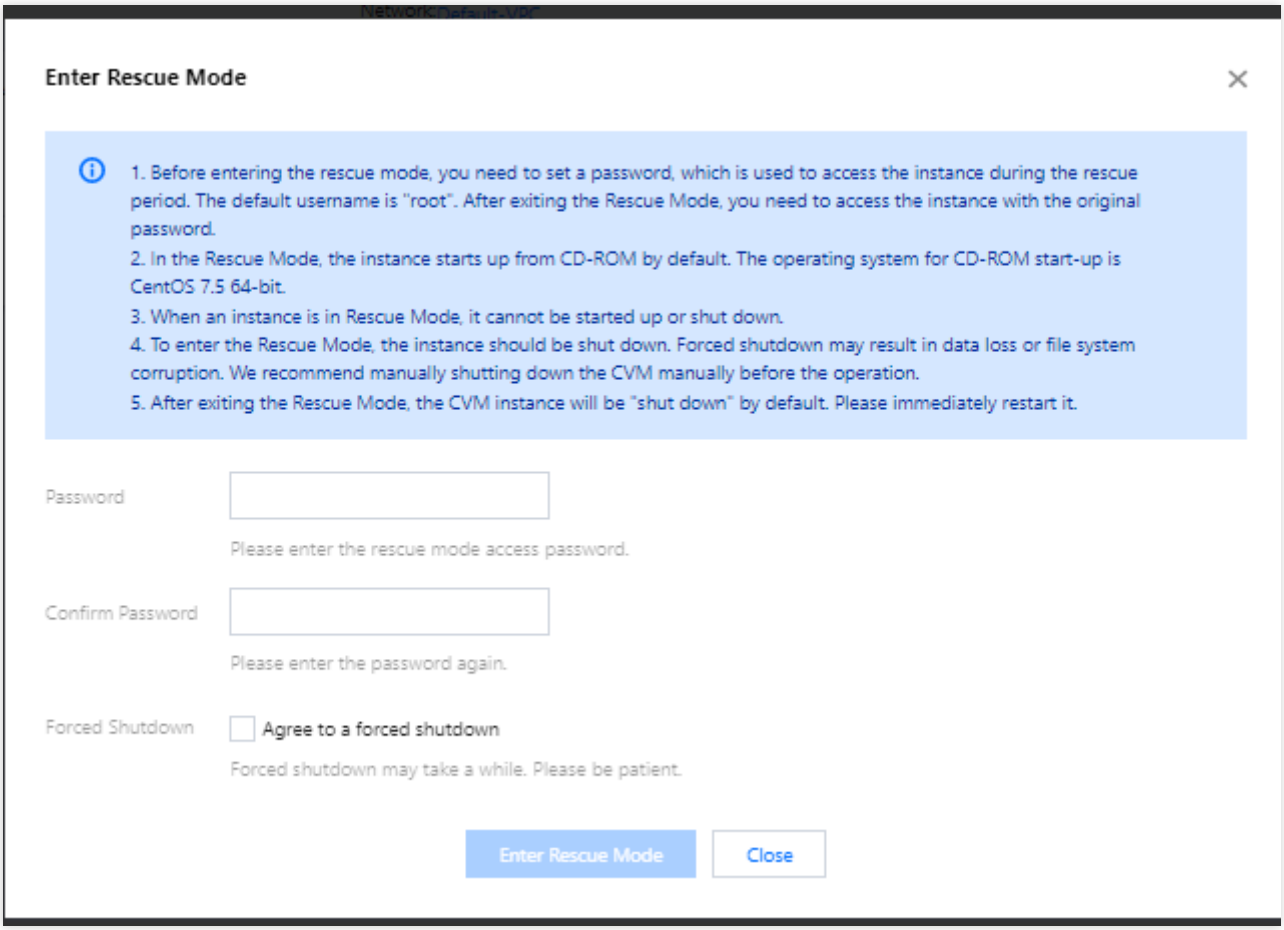
処理手順 を参照し、コンソールからインスタンスレスキューモードに入り、トラブルシューティングと修復を行います。

処理手順

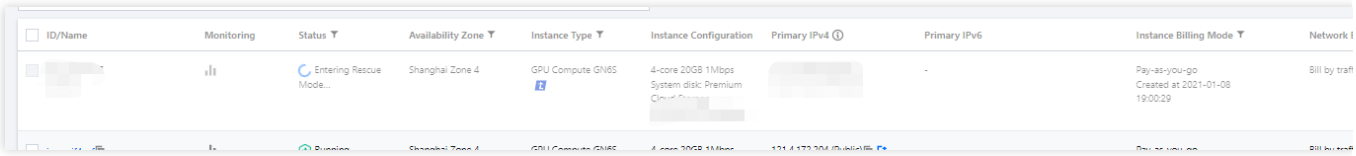
1. レスキューモード開始前に、誤操作などによる影響を防止するため、インスタンスをバックアップすることを強くお勧めします。CBSでは スナップショットの作成 を介してバックアップでき、ローカルシステムディスクでは カスタムイメージの作成 を介してイメージをバックアップできます。
2. 下図に示すように、CVMコンソール にログインし、「インスタンス」ページで、インスタンスが配置されている行の右側の**その他 > 運用保守と検査 > レスキューモードの開始**を選択します。



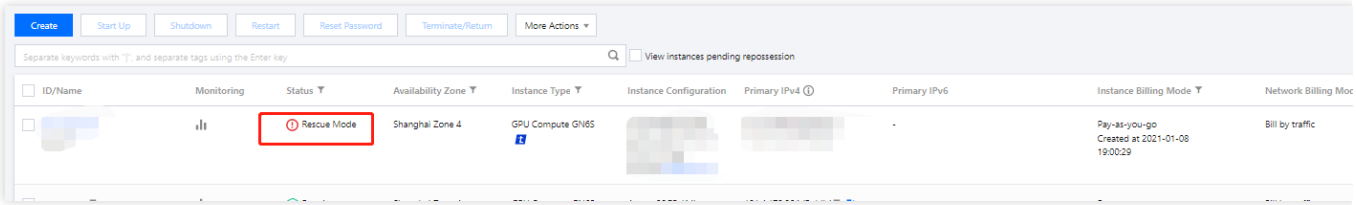
3. 下図に示すように、ポップアップした「レスキューモードの開始」ウィンドウで、レスキューモード中にインスタンスにログインするためのパスワードを設定します。



4. **レスキューモードの開始**をクリックすると、インスタンスのステータスが「レスキューモードの開始」に変わります。下図のように、通常、この処理は数分以内に完了します。

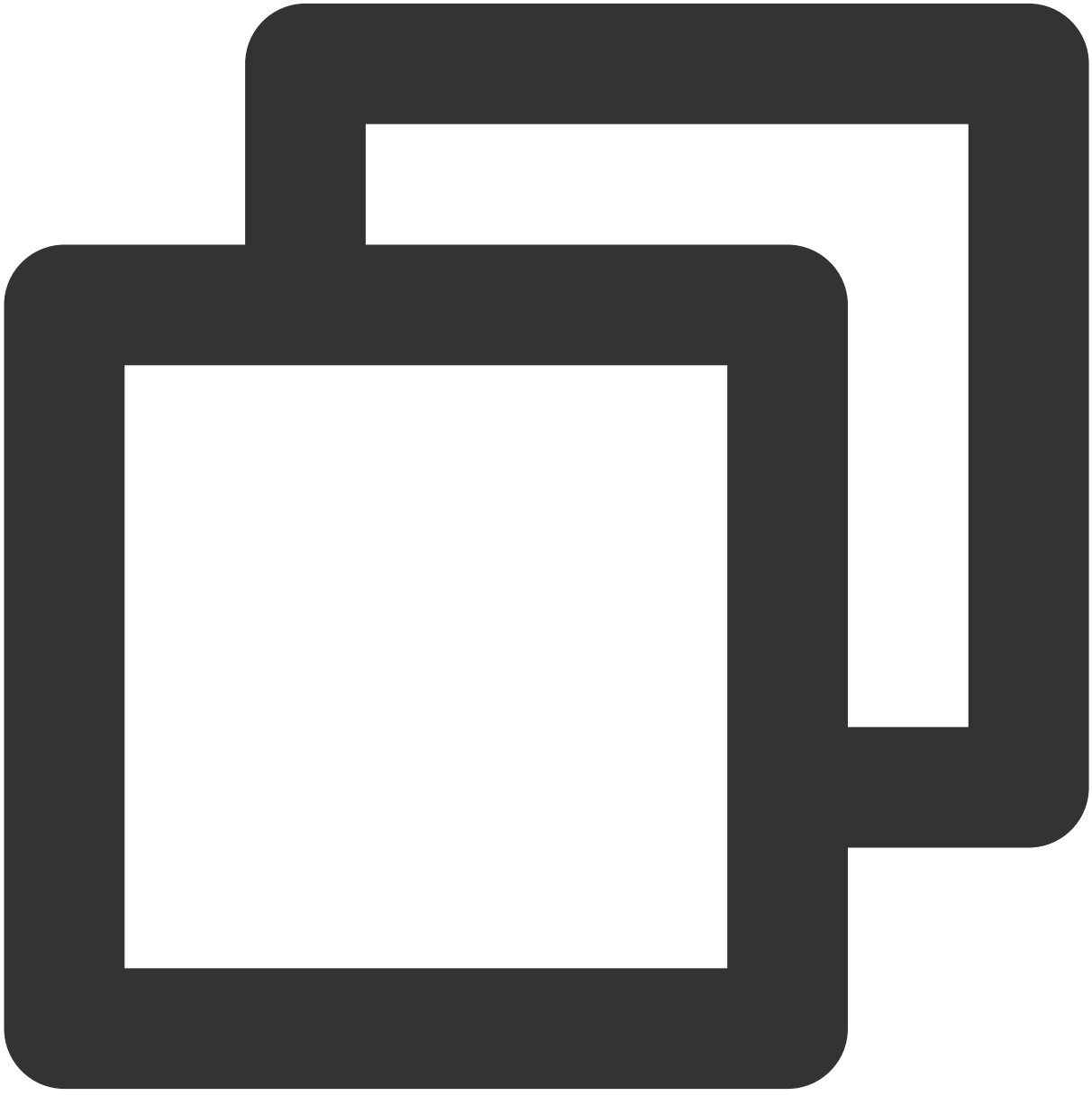


レスキューモードが正常に開始された後、下図に示すように、インスタンスのステータスが赤いエクスクラメーションマーク付きの「レスキューモード」に変更します。

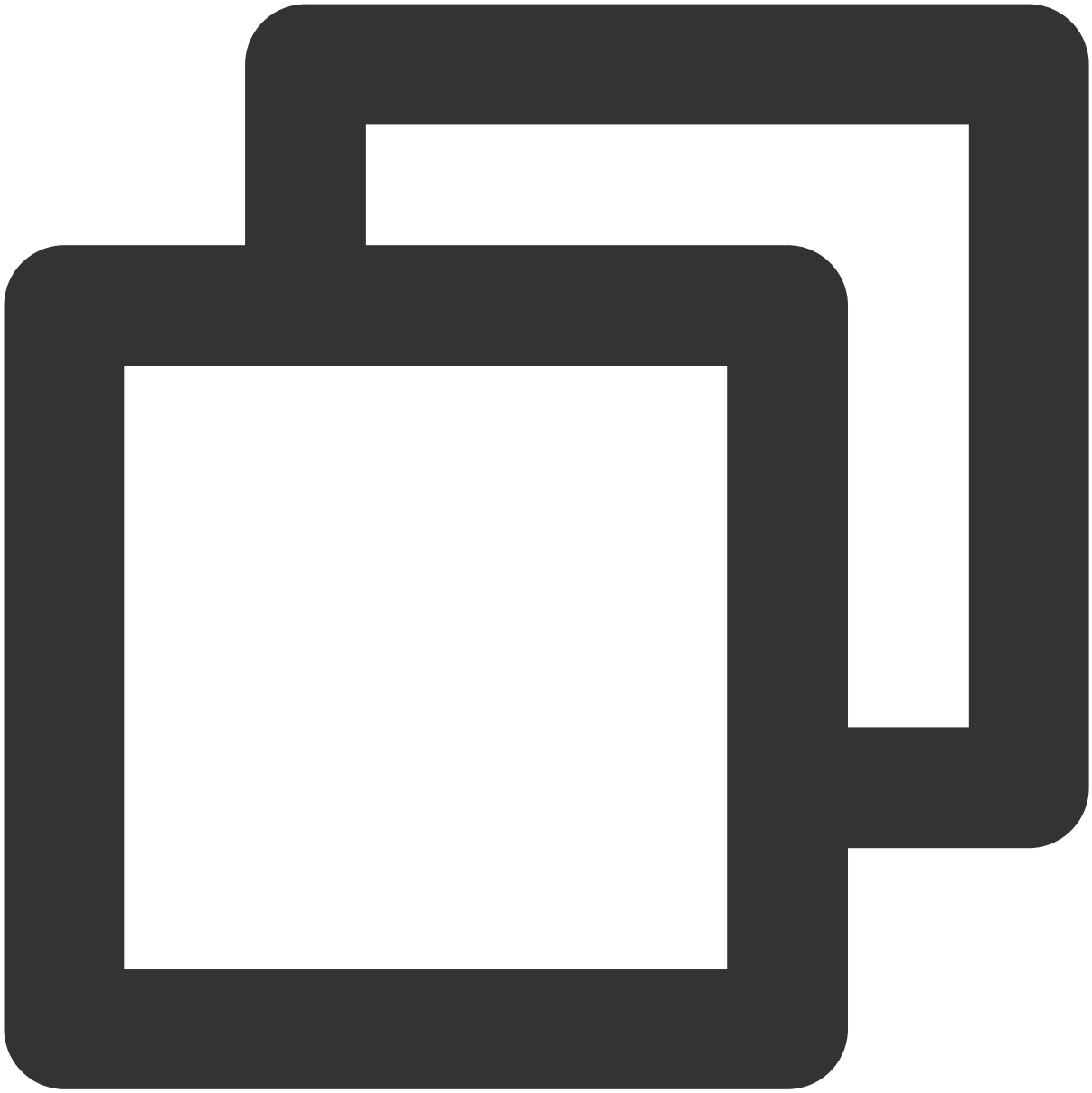


5. `root` アカウントおよび ステップ3 で設定したパスワードを使用し、次の方式でインスタンスにログインします。
インスタンスにパブリックIPが有る場合は、SSHを使用してLinuxインスタンスにログイン をご参照ください。

インスタンスにパブリックIPがない場合は、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。
6. ここでは、VNC方式によるログインを例に取ります。ログインに成功したら、下記のコマンドを実行し、システムディスクのルートパーティションをマウントします。
説明：
レスキューモードでのインスタンスのシステムディスクデバイス名はvda、ルートパーティションはvda1で、デフォルトではマウントされていません。

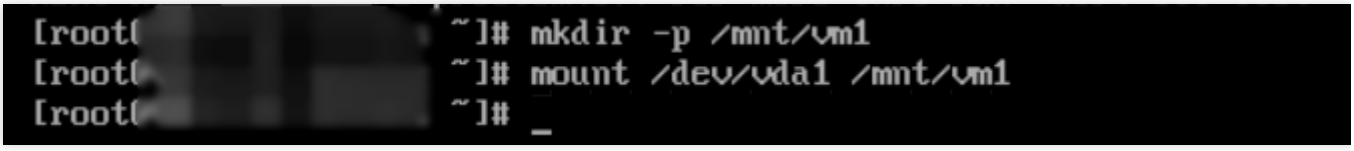


```
mkdir -p /mnt/vm1
```

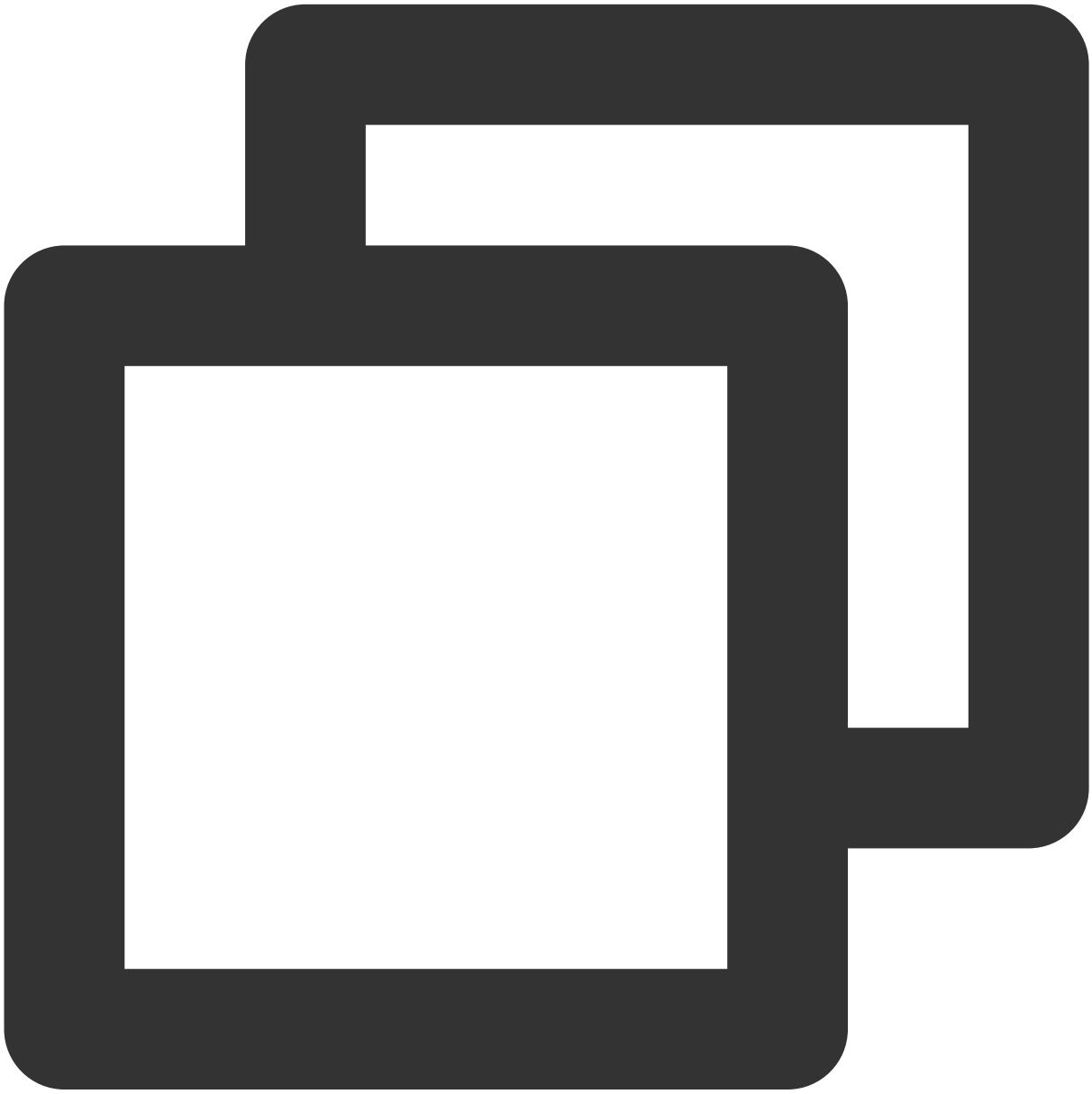


```
mount /dev/vda1 /mnt/vm1
```

実行が完了すると、下図のような結果が返されます。



7. マウントに成功したら、元のシステムルートパーティション内のデータを操作できるようになります。`mount -o bind` コマンドを使用して元のファイルシステムのサブディレクトリの一部をマウントし、かつ `chroot` コマンドを使用して指定のルートディレクトリでコマンドを実行することもできます。具体的な操作コマンドは次のとおりです。



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

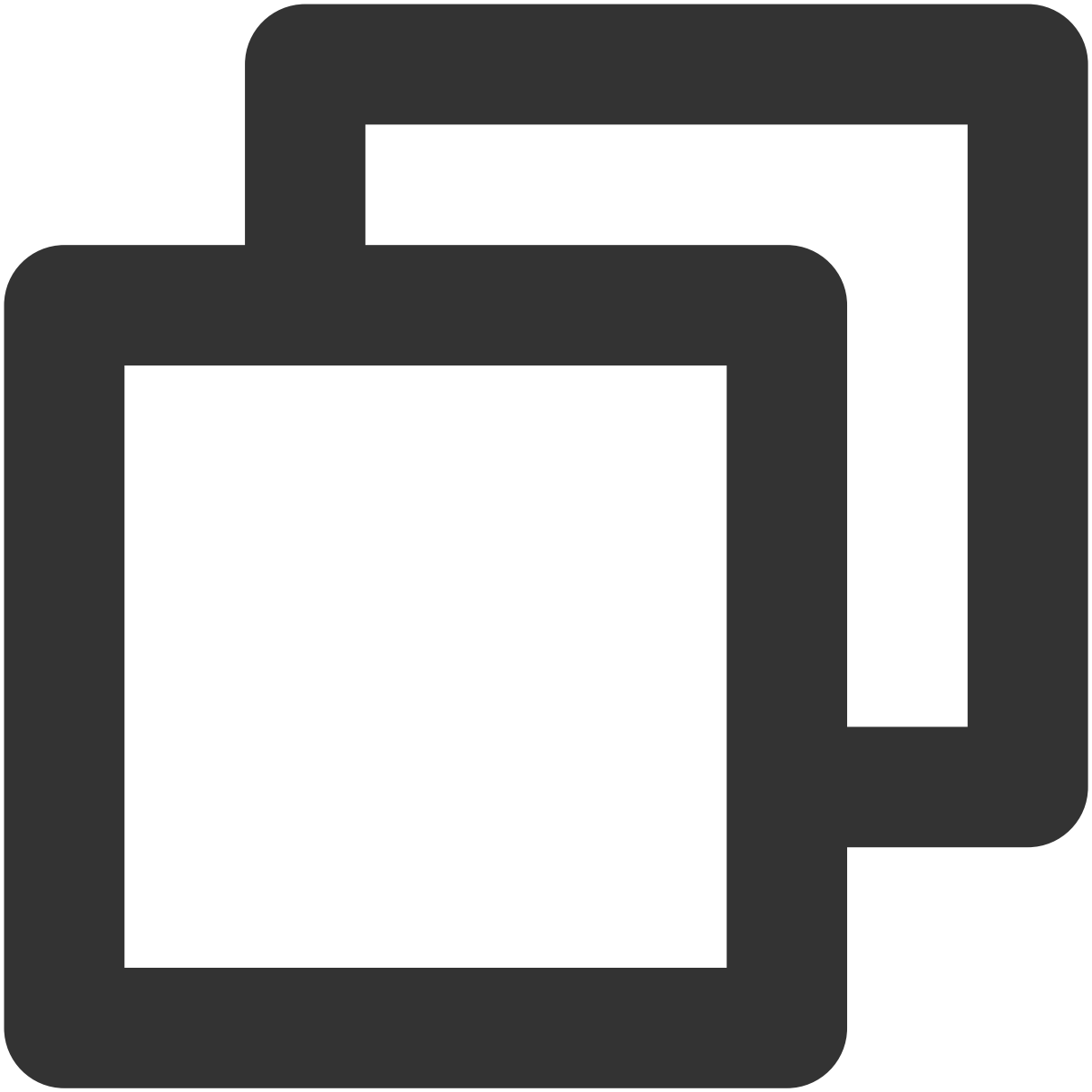
`chroot` コマンドを実行する場合。
エラー情報がなければ、 `cd /` コマンドで続行できます。
下図のようなエラー情報が表示された場合は、ルートディレクトリが正常に切り替えられていないので、 `cd /mnt/vm1` を実行してルートパーティションのデータを確認します。

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

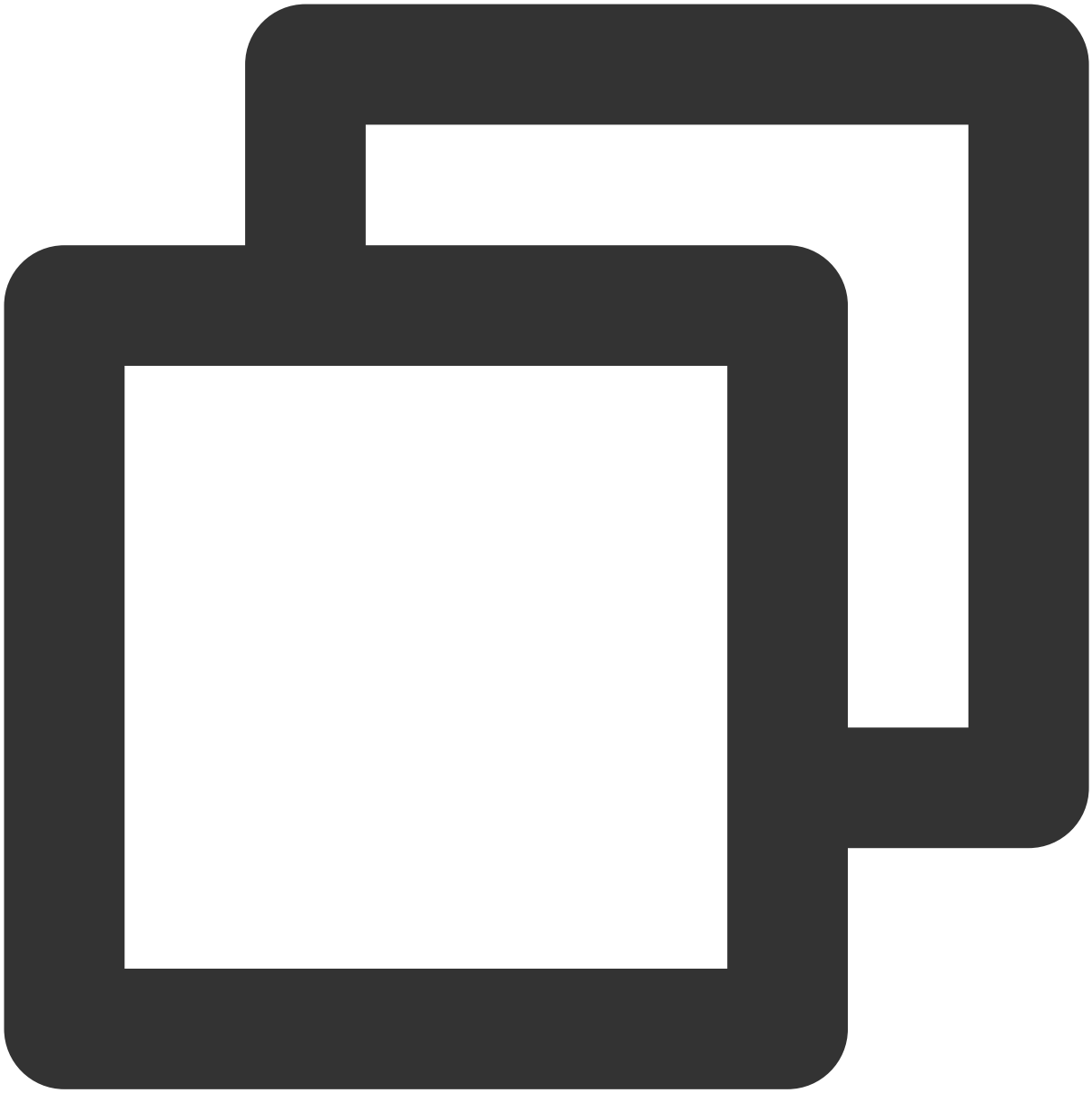
8. 下図に示すように、このコマンドは、元のシステムルートパーティションの `/usr/bin` ディレクトリにある、削除されたすべてのファイルを表示することができます。

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

9. この時点で、同じOSの正常なマシンを作成して以下のコマンドを実行し、正常なシステムの `/usr/bin` ディレクトリにあるファイルを圧縮して異常なマシンへリモートでコピーすることができます。
正常なマシン：以下のコマンドを順次実行します。



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



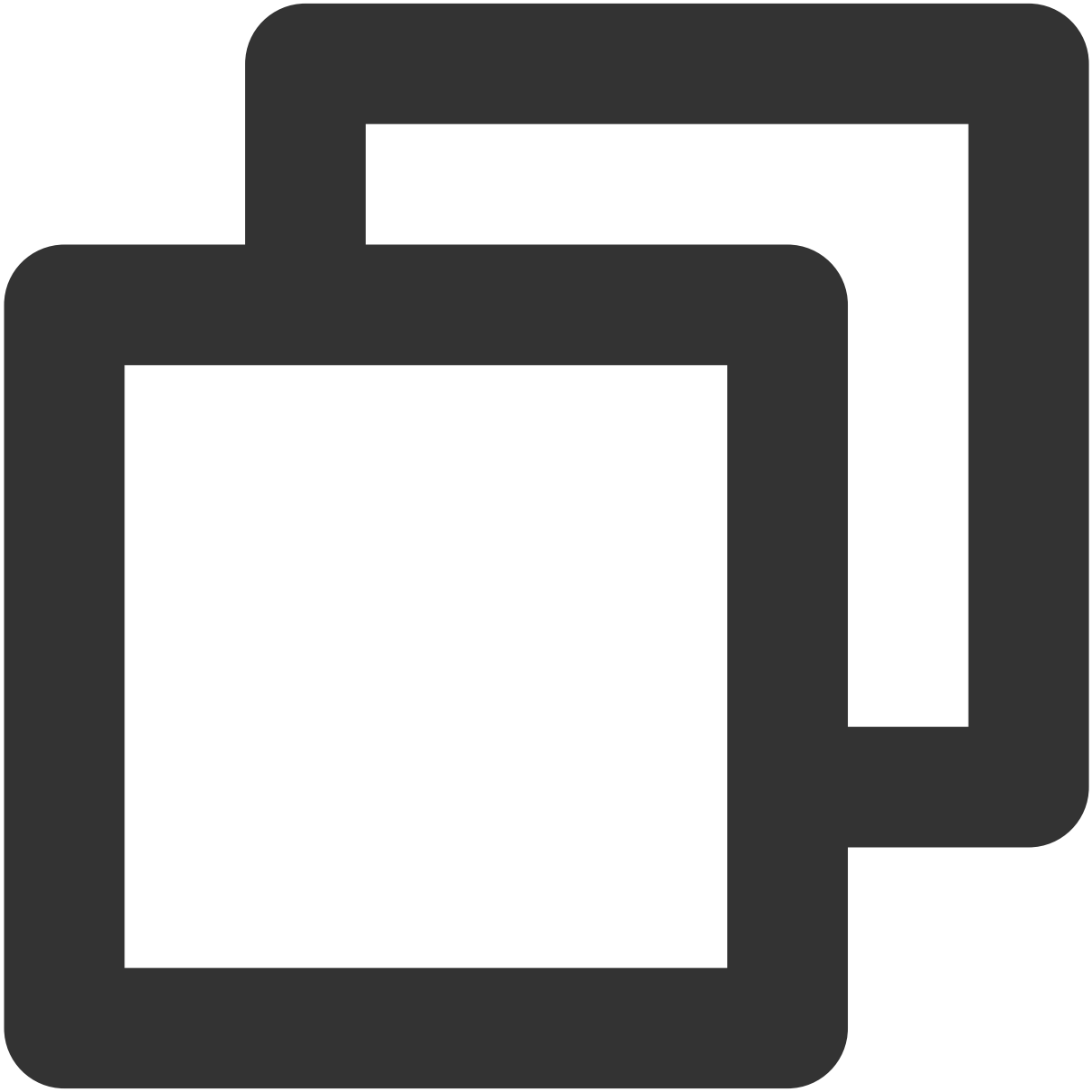
```
scp bin.tar.gz root@異常インスタンスip：/mnt/vm1/usr/bin/
```

説明：

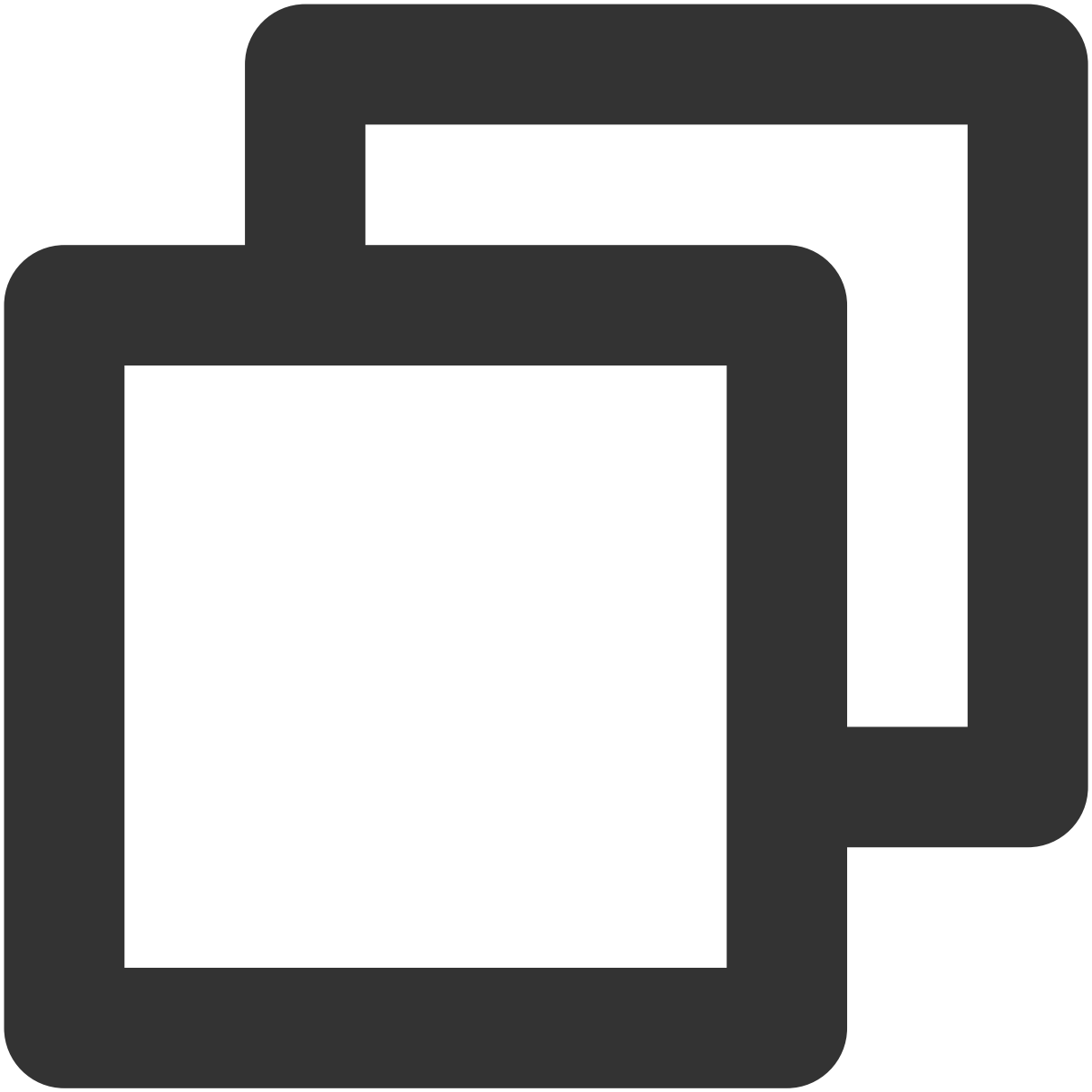
パブリックIPをお持ちの方はパブリックネットワーク経由でコピーできますが、パブリックIPをお持ちでない方は、プライベートネットワーク経由でコピーする必要があります。

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

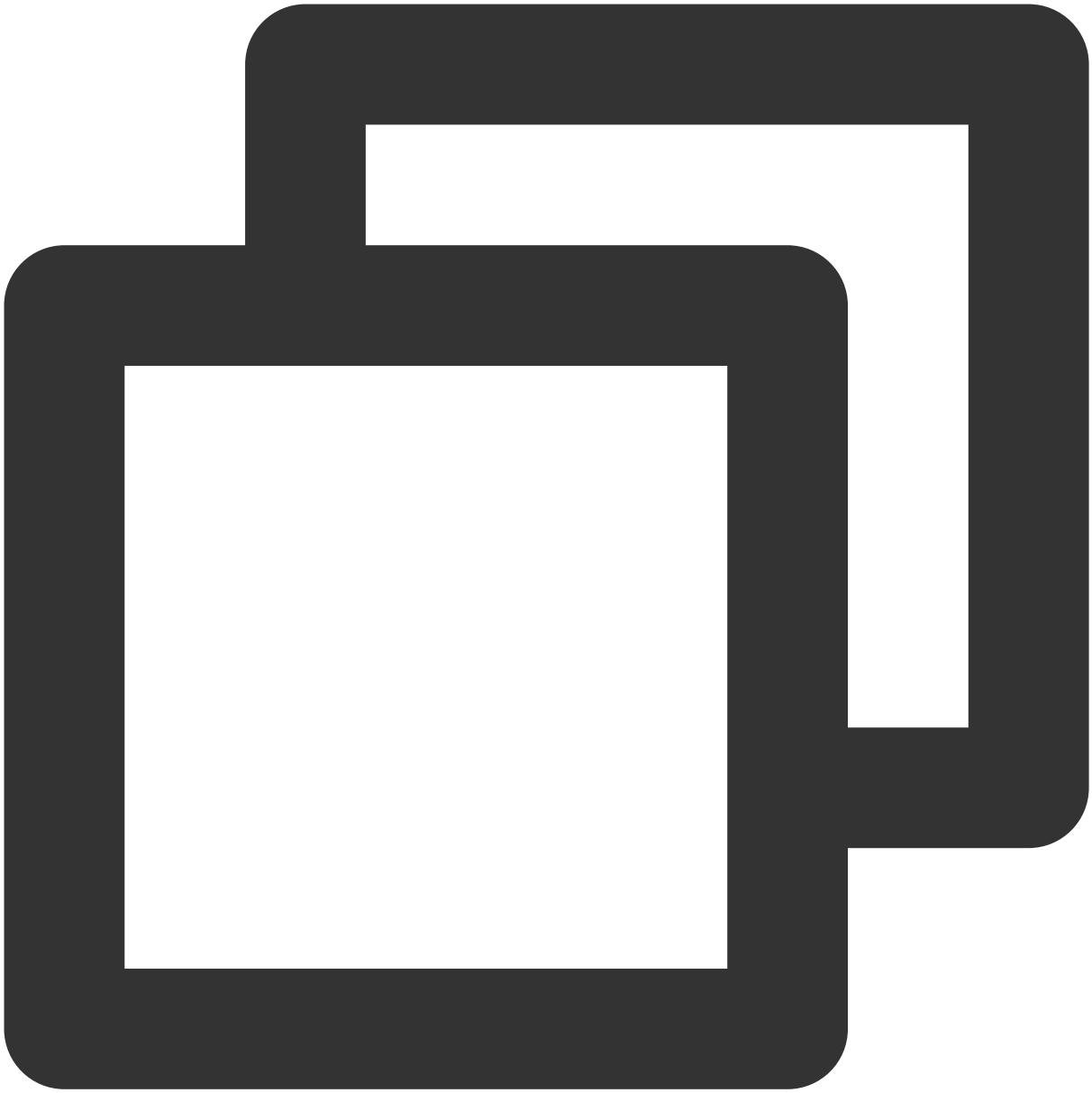
異常なマシン：レスキューモードでは、以下のコマンドが順次実行されます。



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

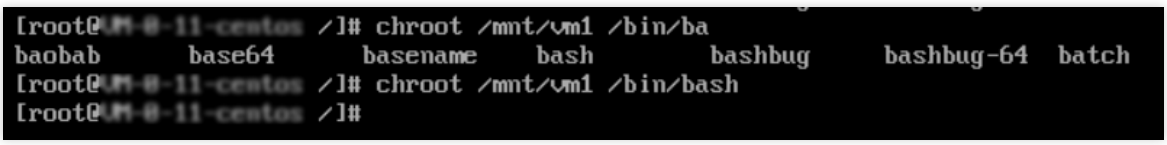


```
tar -zxvf bin.tar.gz
```

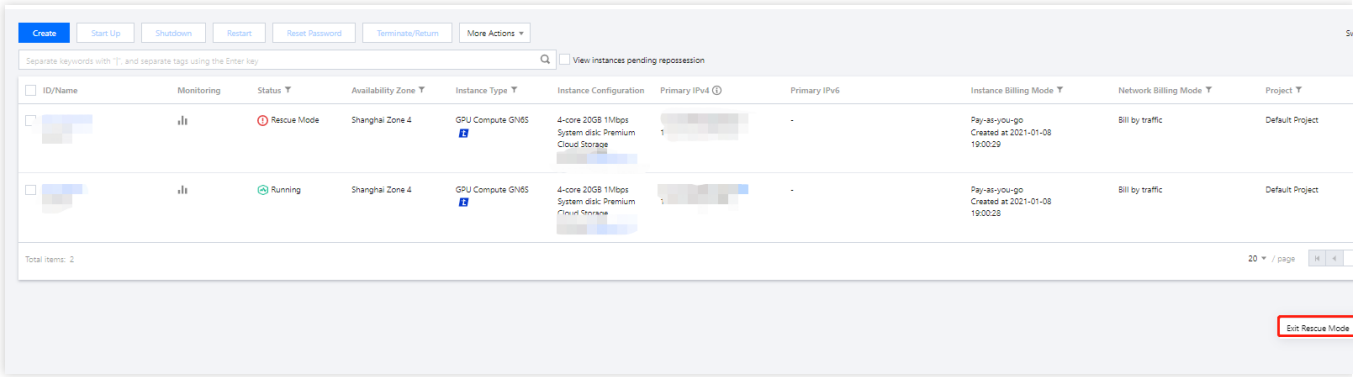


```
chroot /mnt/vm1 /bin/bash
```

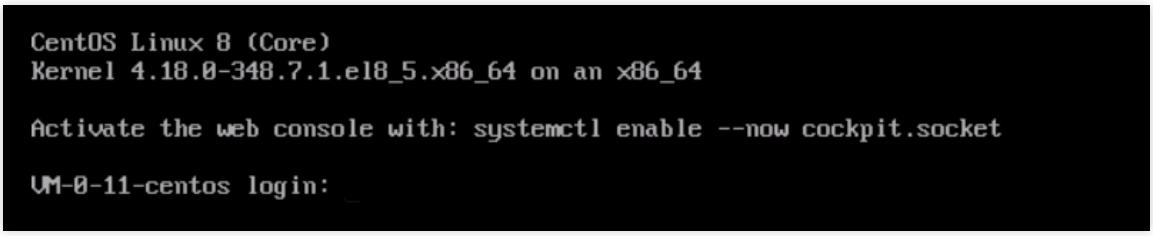
実行結果は、下図のように示されます。



10. 下図に示すように、インスタンスの修復が完了したら、インスタンスが配置されている行右側のその他 > 運用保守と検査 > レスキューモードの終了を選択します。



11. レスキューモード終了後、インスタンスはシャットダウン状態になり、起動後にシステム検証が行われます。下図のようになった場合、システムはすでに復元されています。



CVMの再起動またはシャットダウンは失敗しましたの原因と対処

最終更新日：：2020-10-20 17:08:22

CVMをシャットダウンまたは再起動すると、障害が発生する可能性があります。不具合や障害が発生した場合は、次の手順を実行して問題のトラブルシューティングを行ってください。

考えられる原因

CPUまたはメモリの使用率が高すぎます。
Linux CVMがACPI管理プログラムをインストールしていません。
Windows CVMのシステムアップデートに時間がかかりすぎます。
初めてWindows CVMを購入した時、まだ初期化は完了していません。
インストールされているサポート対象外のソフトウェア、 またはトロイの木馬ウイルスに感染しました。

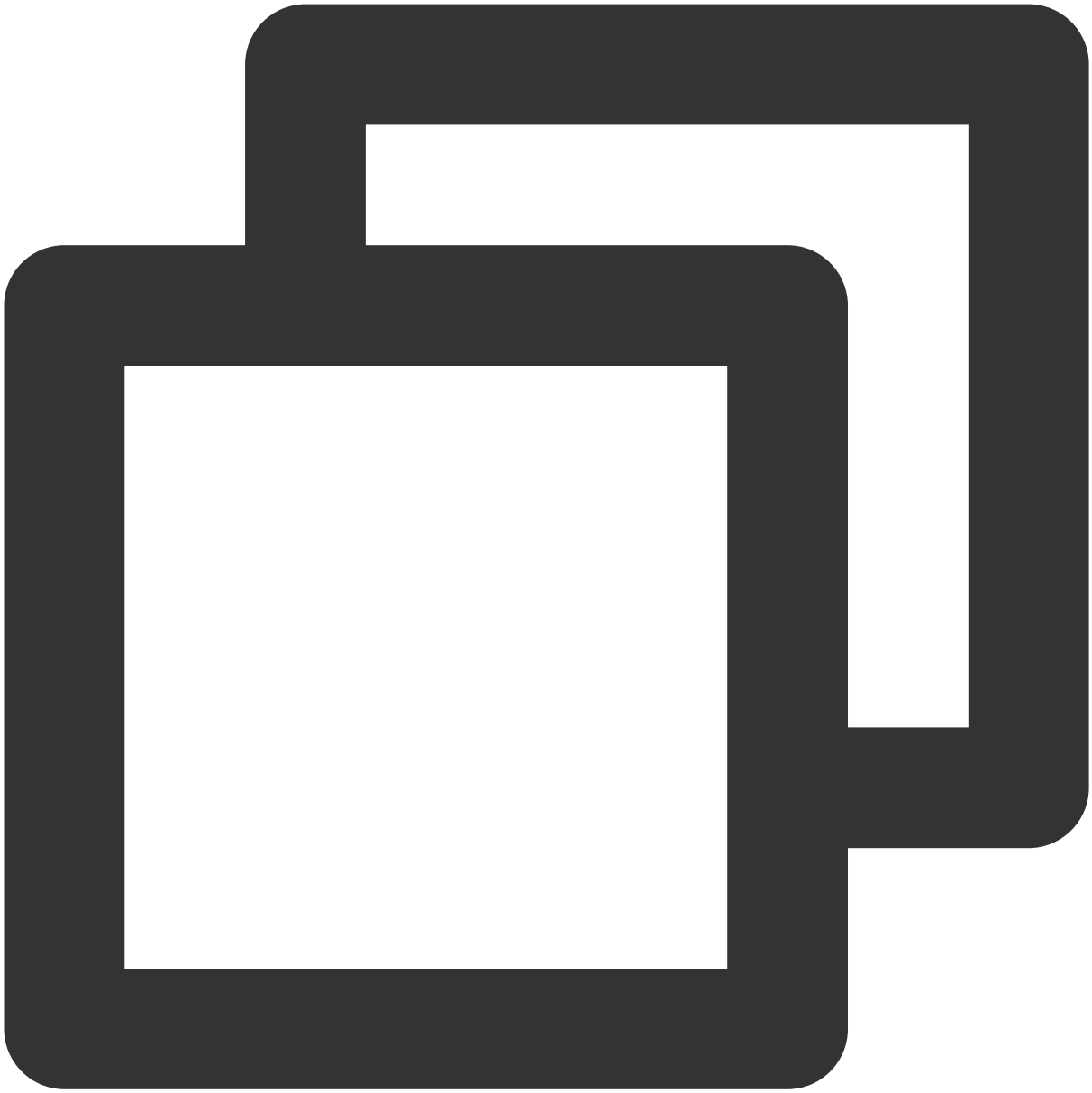
トラブルシューティング

CPU・メモリの使用率を確認する

1. CVMのOSに基づいて、CPU・メモリの使用率を確認します。
Windows CVMの場合：CVMで、「タスクバー」を右クリックして、**タスクマネージャー**を選択します。
Linux CVMの場合： `top` コマンドを実行し、 `%CPU` 列と `%MEM` 列の情報を確認します。
2. 実際のCPU・メモリの使用率によって、CPUまたメモリの使用率が高いプロセスを終了します。
上記の操作を実行してもCVMをシャットダウンまたは再起動できない場合は、強制終了/再起動 を実行してください。

ACPI管理プログラムをインストールしているかを確認する

説明：
この操作はLinux CVMに適用します。
次のコマンドを実行して、ACPIプロセスが存在するかどうかを確認します。



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

ACPIプロセスが存在する場合、強制終了/再起動 を実行してください。

ACPIプロセスが存在しない場合、ACPI管理プログラムをインストールしてください。詳細な操作については、Linux電源管理設定 をご参照ください。

WindowsUpdateが実行しているかを確認する

説明：

この操作はWindows CVMに適用します。

Windows CVMのOSインターフェースで、**スタート > コントロールパネル > Windows Update** をクリックし、パッチまたはプログラムが更新されているかどうかを確認します。
Windowsがあるパッチ操作を実行する場合、システムのシャットダウン時にいくつかの処理を行います。更新時間が長すぎるため、シャットダウン/再起動に失敗する可能性があります。Windowsの更新が完了するのを待ってから、CVMをシャットダウンまたは再起動することをお勧めします。
パッチやプログラムが更新されていない場合は、強制終了/再起動 を実行してください。

CVMの初期化が完了したかどうかを確認する

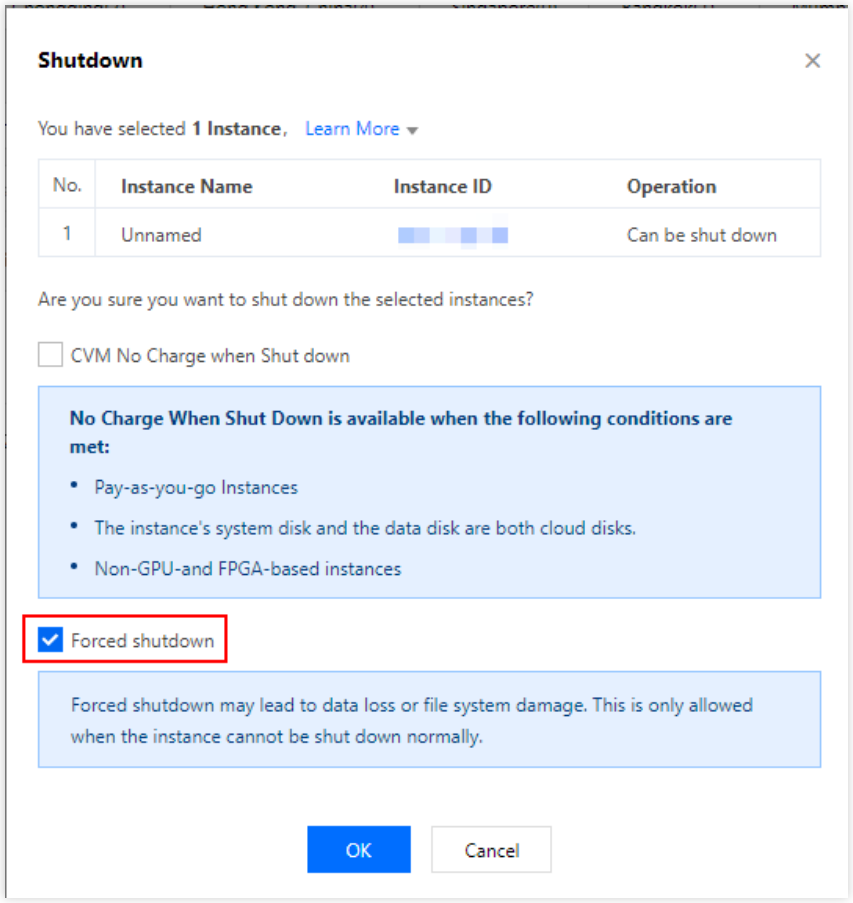
説明：
この操作はWindows CVMに適用します。
Windows CVMを初めて購入する場合、システムはSysprepを使用してイメージを配布するため、初期化に時間がかかる場合があります。初期化が完了する前に、Windowsはシャットダウンおよび再起動操作を無視します。
購入したWindows CVMが初期化中の場合、Windows CVMの初期化が完了してから、CVMをシャットダウンまたは再起動することをお勧めします。
初期化が完了すると、強制終了/再起動 を実行してください。

インストールしたソフトウェアが正常に作動するかどうかを確認する

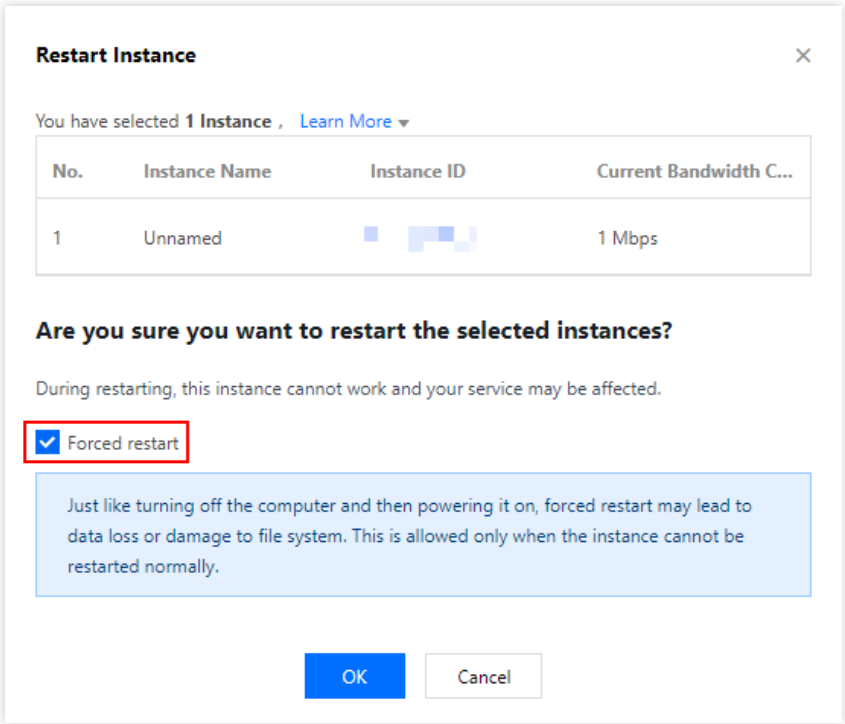
検査ツールまたはウイルス対策ソフトウェアを使用して、CVMにインストールしたソフトウェアが正常に作動するか、トロイの木馬、またはウイルスに感染しているかどうかを確認します。
異常が発生した場合、システムが破損して、シャットダウンと再起動が失敗する可能性があります。このソフトウェアをアンインストールし、セキュリティソフトウェアを利用してスキャンするか、データバックアップ後、システムを再インストールすることをお勧めします。
異常が見つからない場合、強制終了/再起動 を実行してください。

強制終了/再起動

説明：
Tencent Cloudは強制終了/再起動機能を提供し、複数回試行した後にCVMのシャットダウンまたは再起動に失敗した場合に使用できます。この機能を使用すると、CVMの強制終了または再起動が可能になりますが、データの損失やファイルシステムの損傷を引き起こす可能性があります。
1. CVMコンソール にログインします。
2. インスタンス管理ページで、シャットダウンまたは再起動するCVMを選択します。
CVMのシャットダウン：**その他 > インスタンス状態 > シャットダウン**をクリックします。
CVMの再起動：**その他 > インスタンス状態 > 再起動**をクリックします。
3. ポップアップダイアログボックスで、**強制シャットダウン**または**強制再起動**を選択し、**確定**をクリックします。
強制シャットダウンを選択した場合、次の図に示すように：



強制再起動を選択した場合、次の図に示すように：



Network Namespaceを作成できない

最終更新日：：2020-03-03 18:59:23

問題の説明

新しいネットワークネームスペース（Network Namespace）を構築するコマンドを実行する時に、実行されるコマンドがフリーズし、続けることができません。Dmesg のメッセージプロンプト：“unregister_netdevice: waiting for lo to become free. Usage count = 1”

問題の原因

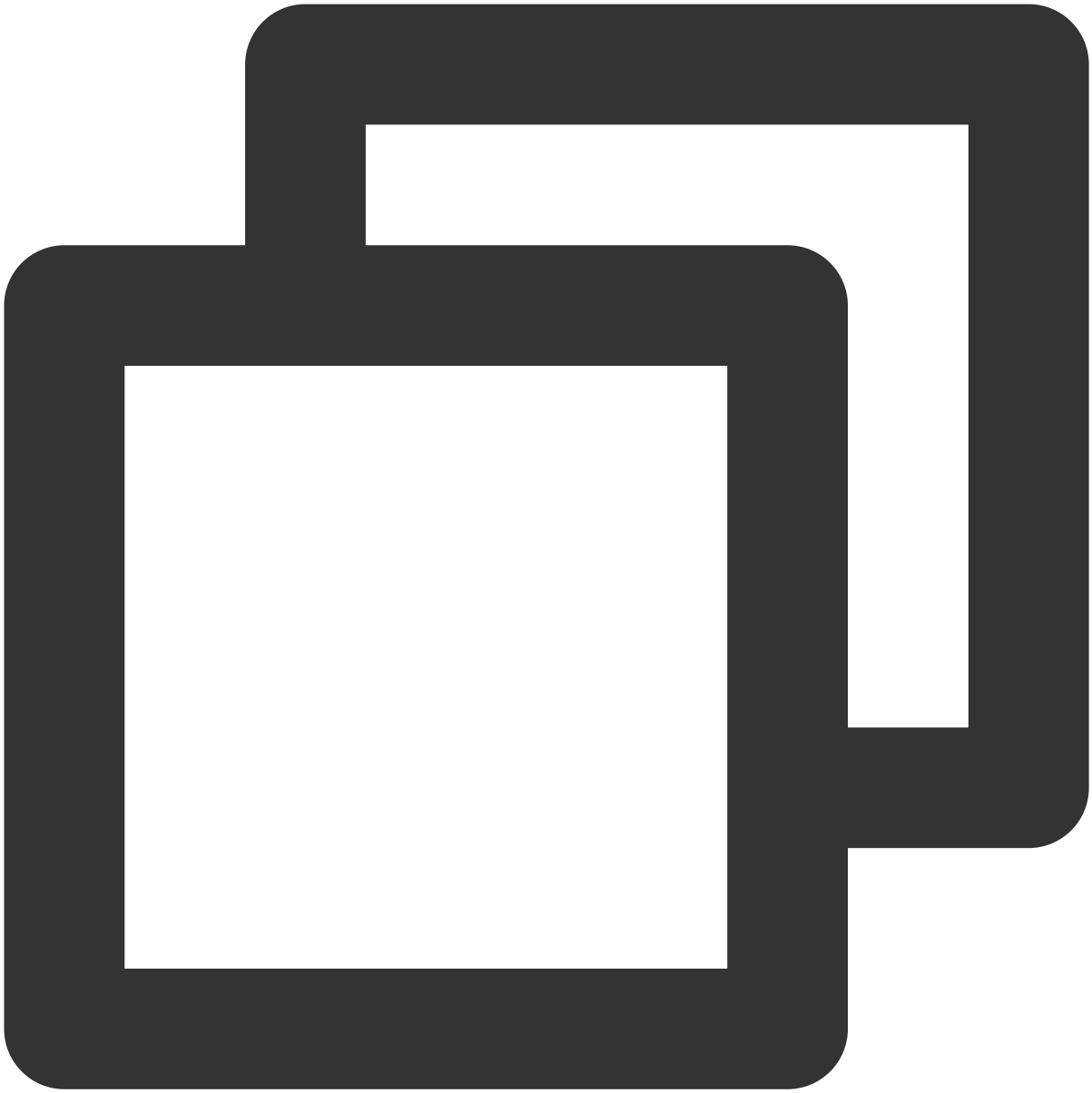
当該問題はカーネルbugです。現在、下記のカーネルバージョンには当該bugが存在しています。
Ubuntu 16.04 x86_64のカーネルバージョンが4.4.0-91-genericです
Ubuntu 16.04 x86_32のカーネルバージョンが4.4.0-92-genericです

ソリューション

カーネルバージョンを4.4.0-98-genericにアップグレードすること。当該バージョンでこのbugが解決されています。

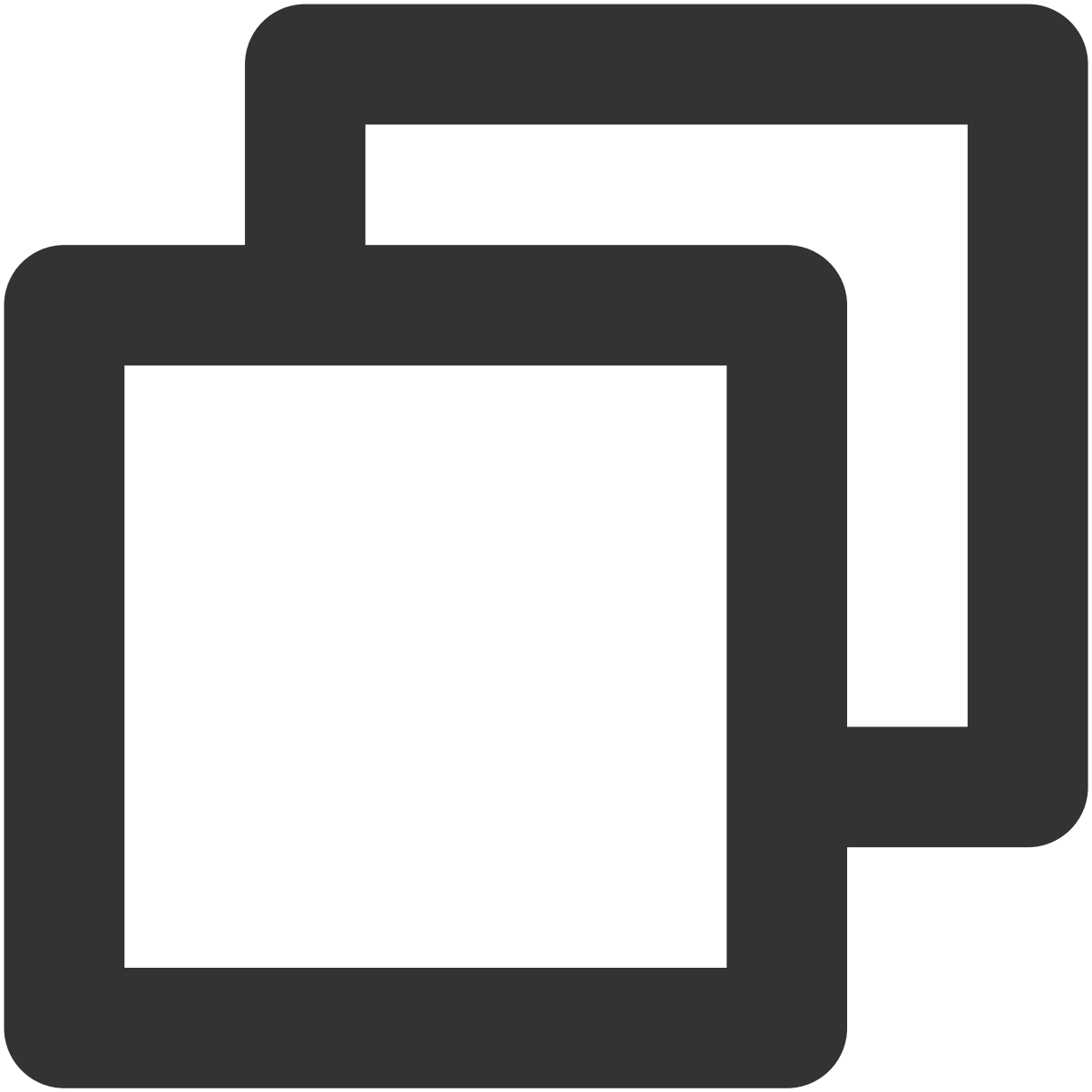
処理手順

1. 下記のコマンドを実行し、現在のカーネルバージョンを確認します。



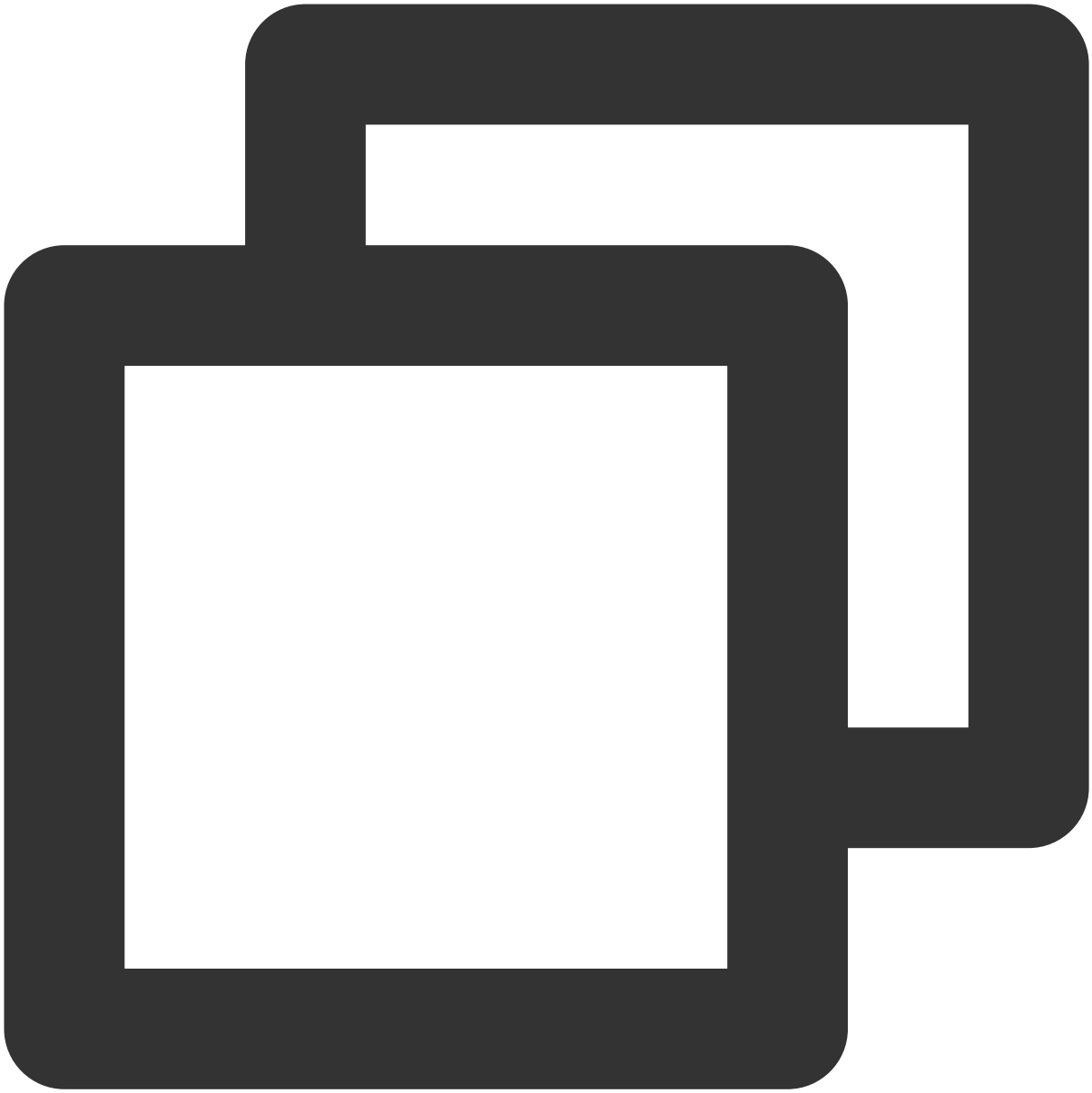
```
uname -r
```

2. 下記のコマンドを実行し、 4.4.0-98-genericのアップグレードバージョンがあるかを確認します。



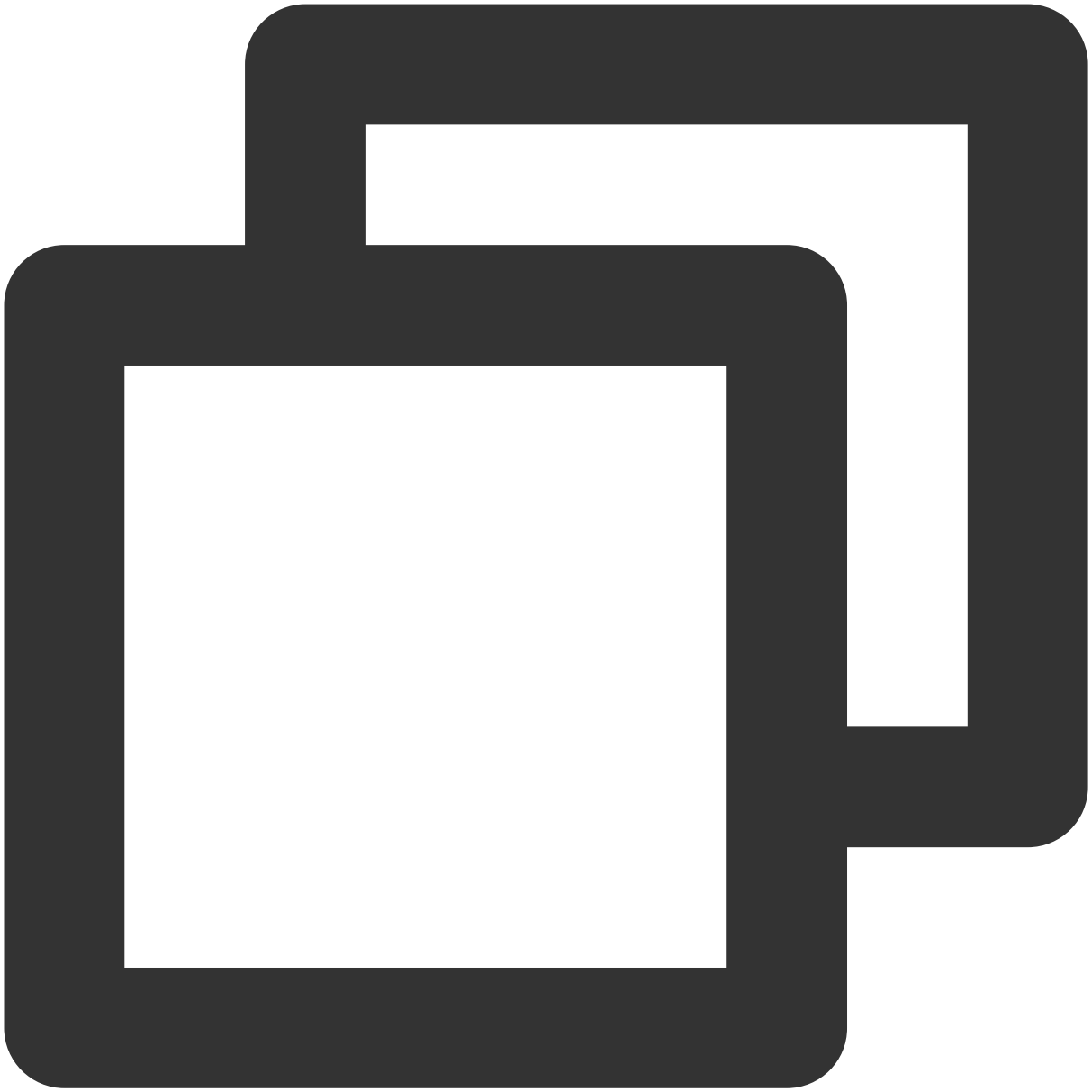
```
sudo apt-get update
sudo apt-cache search linux-image-4.4.0-98-generic
```

下記の情報が表示された場合は、ソースに当該バージョンがあり、アップグレードすることが可能であることを示します。



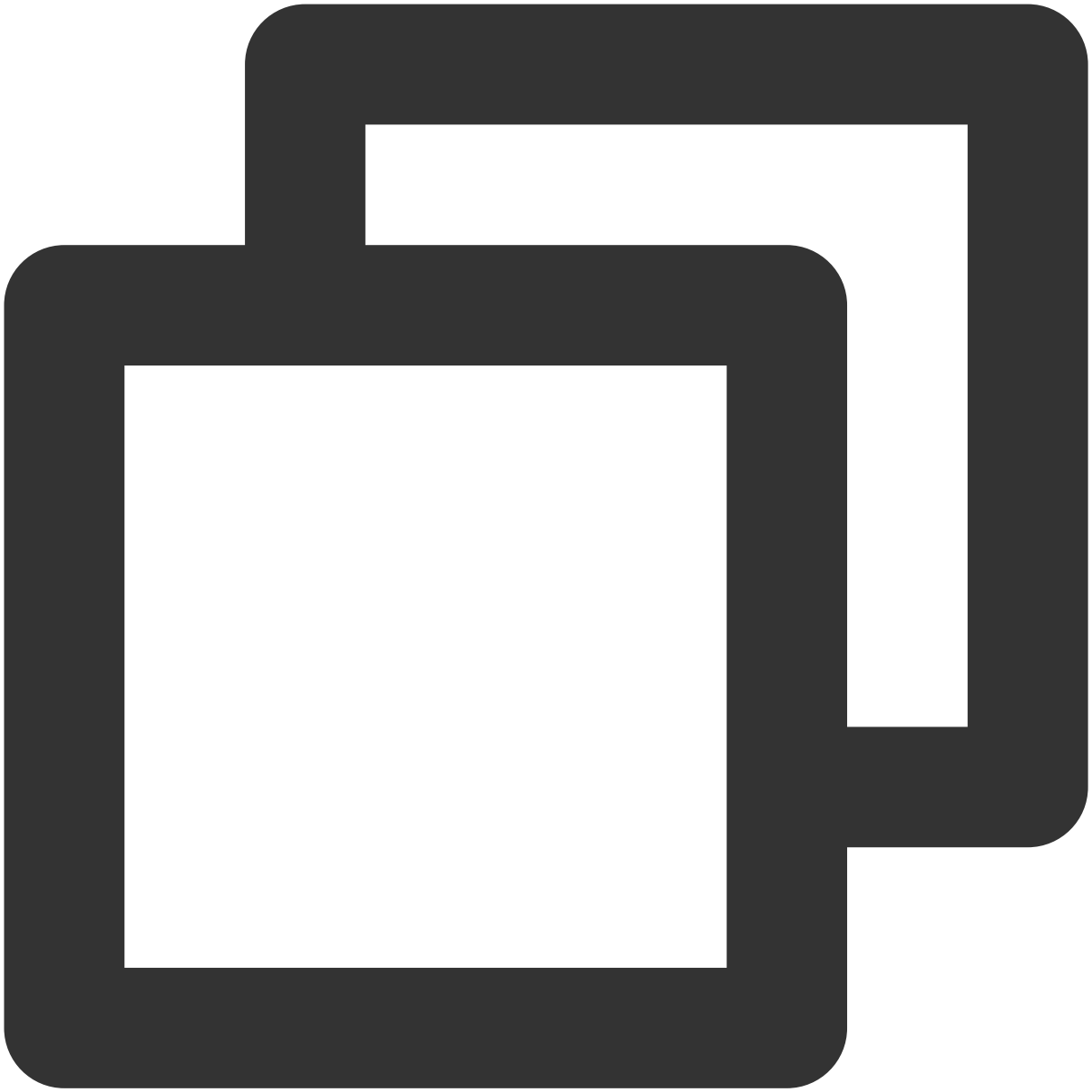
```
linux-image-4.4.0-98-generic - Linux kernel image for version 4.4.0 on 64 bit x86 S
```

3. 下記のコマンドを実行し、新しいバージョンのカーネルとそれに対応するHeaderパッケージをインストールします。



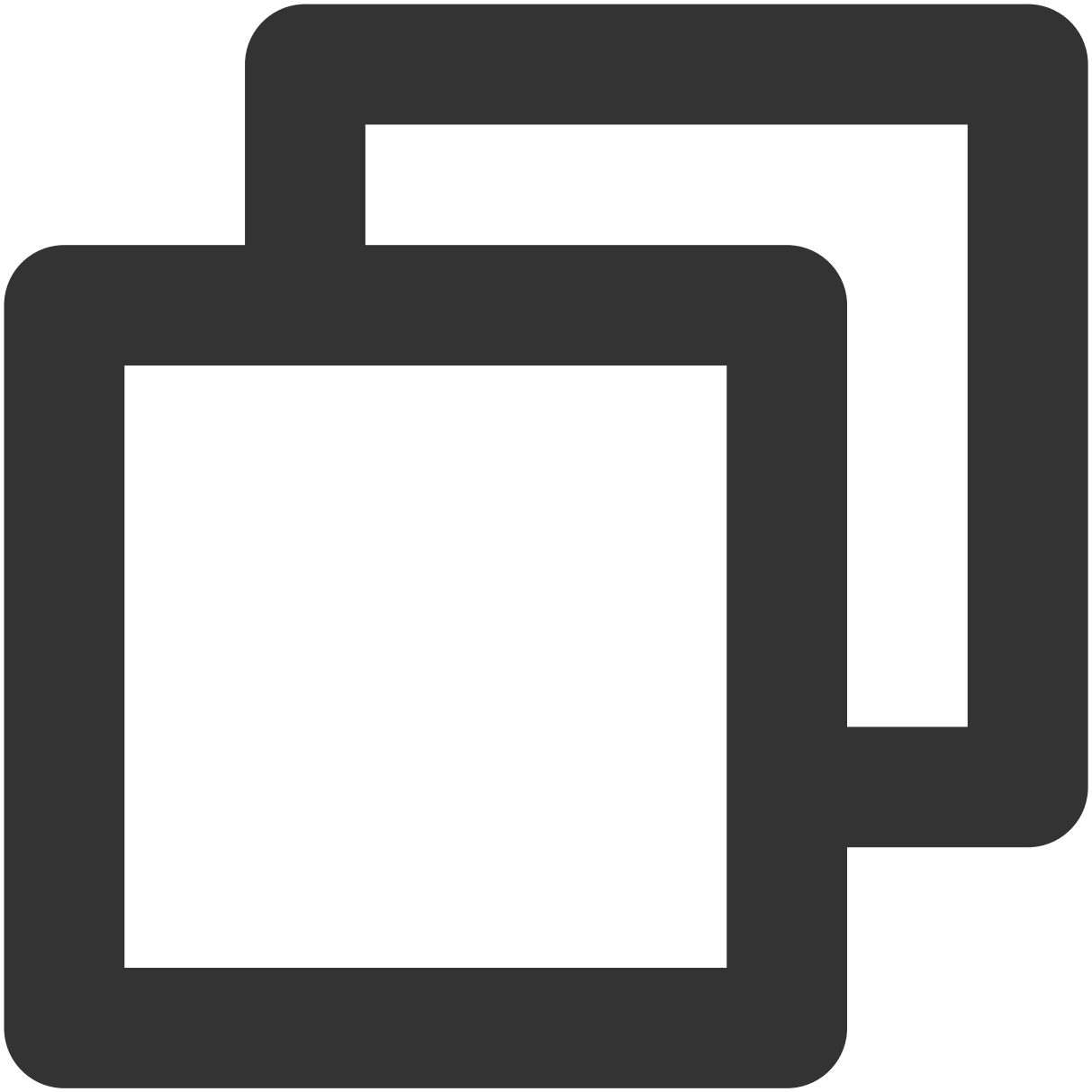
```
sudo apt-get install linux-image-4.4.0-98-generic linux-headers-4.4.0-98-generic
```

4. 下記のコマンドを実行し、システムを再起動します。



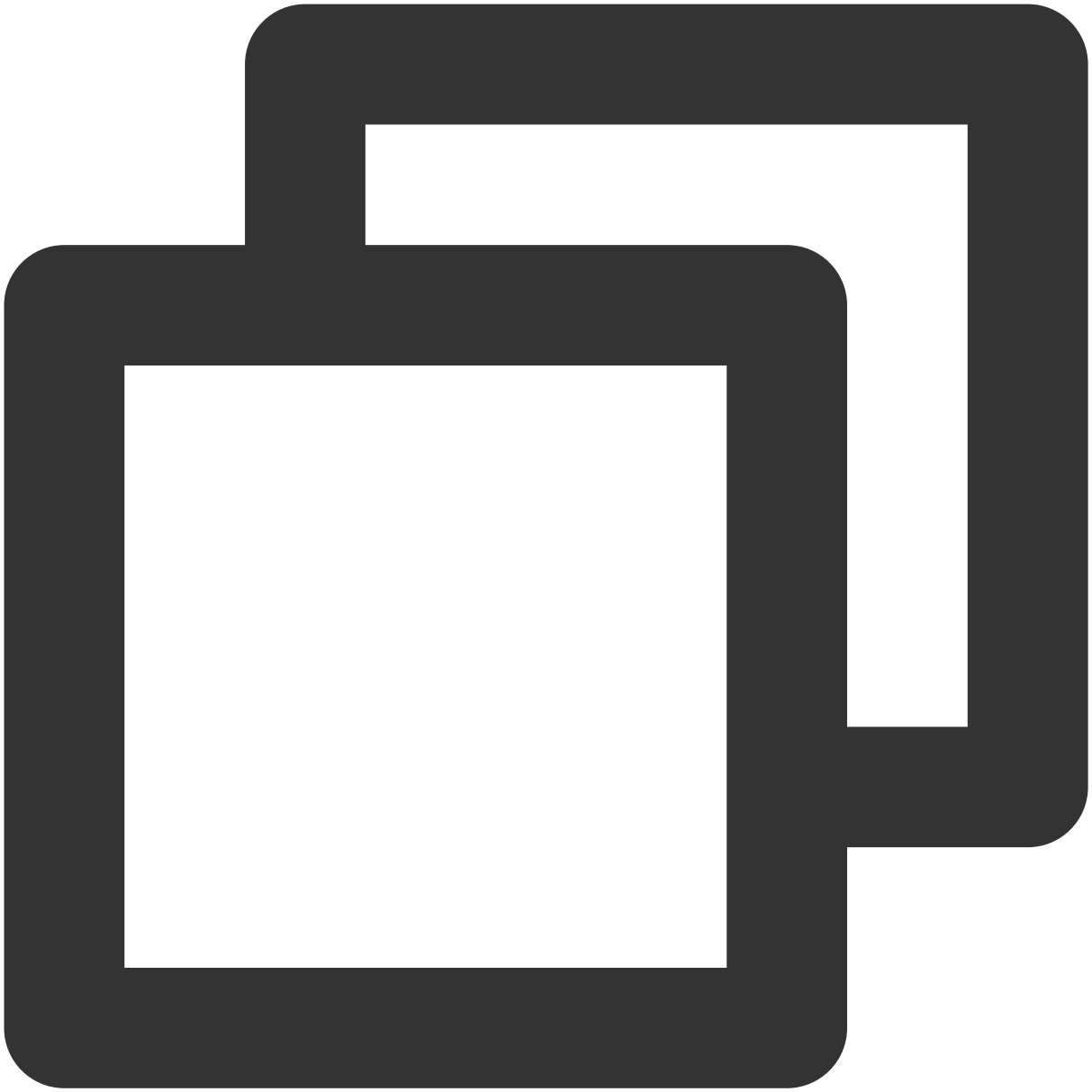
```
sudo reboot
```

5. 下記のコマンドを実行し、システムに入り、カーネルバージョンを確認します。



```
uname -r
```

下記のような結果が表示された場合は、バージョン更新に成功したことを示しています。



```
4.4.0-98-generic
```

カーネルおよび IO 関連問題

最終更新日：：2021-08-31 17:07:41

インスタンス自己検出を使用する場合、検出レポートからインスタンスの異常を取得できます。 このテキストでは、主にインスタンス自己検出レポート中のカーネルとIOに関連する問題事象、原因および対処手順を紹介します。

カーネル問題の特定および処理

障害事象

カーネルに関連する障害は、マシンのログイン不能や異常な再起動を引き起こす可能性があります。

考えられる原因

カーネル hung_task

hung task メカニズムは、カーネルスレッドkhungtaskdによって実装され、khungtaskdはTASK_UNINTERRUPTIBLE状態のプロセスを監視します。 `kernel.hung_task_timeout_secs` （デフォルトは120秒）時間内にD状態であり続ける場合、 hung taskプロセスのスタック情報が出力されます。
`kernel.hung_task_panic=1` に設定すると、カーネル panic がトリガーされ、マシンが再起動します。

カーネルのソフトロックアップ soft lockup

soft lockup とは CPU がカーネルコードに占有され、他のプロセスが実行できないことをいいます。soft lockup を検出する原理は、各 CPU に一定時間内に実行されるカーネルスレッド [watchdog/x]を割り当てることであり、このスレッドが一定時間内（デフォルトは `2*kernel.watchdog_thresh` 、3.10カーネル `kernel.watchdog_thresh` のデフォルトは10秒）に実行されない場合は、 soft lockupが発生したことを意味します。
`kernel.softlockup_panic=1` に設定すると、カーネル panic がトリガーされ、マシンが再起動します。

カーネル panic

カーネルの異常な crash は、マシンの再起動を引き起こします。一般的なカーネル panic シナリオは次のとおりです：
カーネルに hung_task が出現し、かつ `kernel.hung_task_panic=1` に設定した場合。
カーネルにソフトロックアップ soft lockup が出現し、かつ `kernel.softlockup_panic=1` に設定した場合。
カーネル bug がトリガーされた場合。

対処手順

カーネルに関連する問題の調査および対処手順が複雑な場合は、チケットを提出 し、問題をさらに特定し処理することをお勧めします。

ハードディスク問題の特定および処理

ハードディスク inode がフルになる

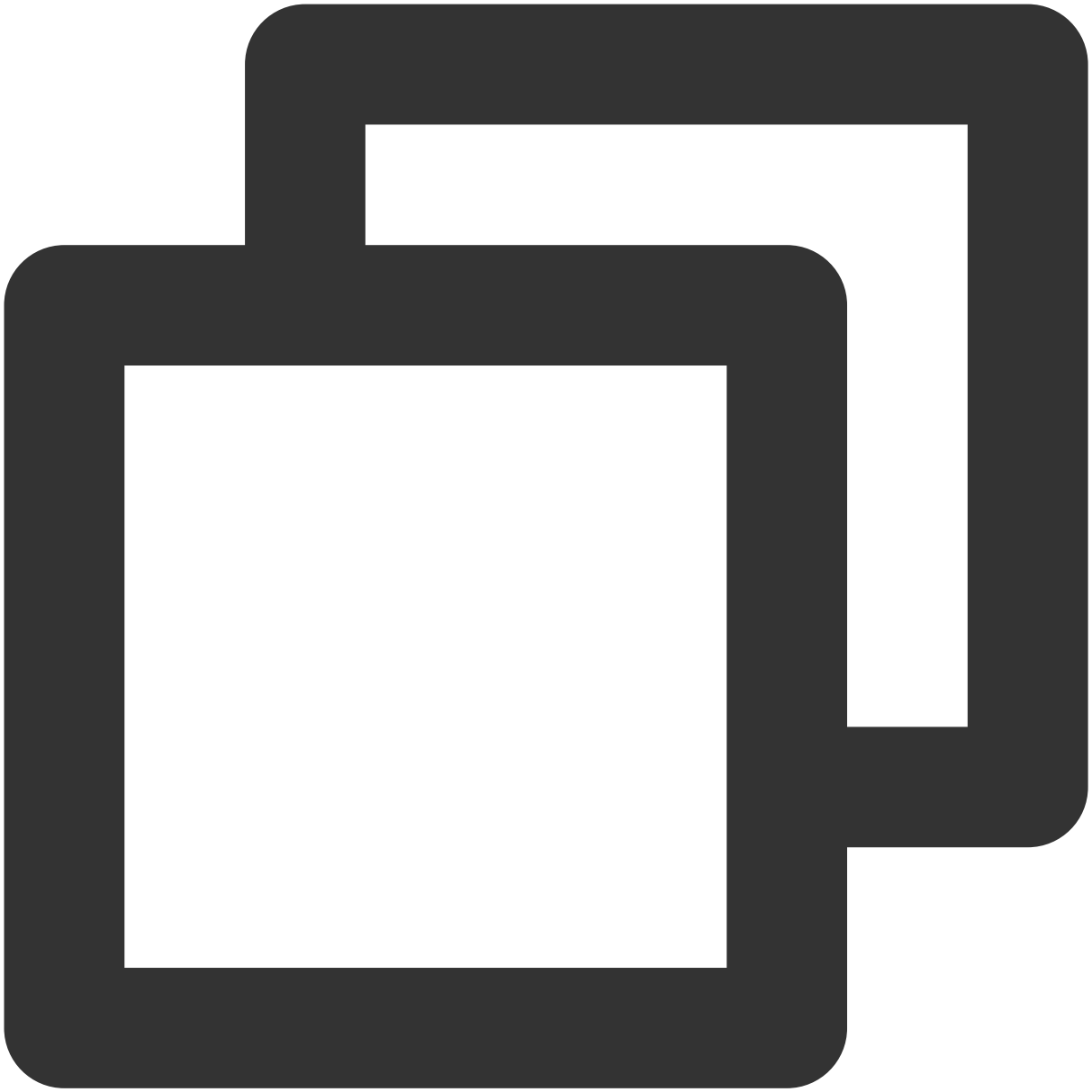
障害事象：新しいファイルを作成すると、「No space left on device」 というエラー情報が表示され、かつ `df -i` コマンドを使用すると、 inode容量使用率100%表示される。
考えられる原因： ファイルシステム inode が枯渇している。
対処手順：使用する必要のないファイルを削除するか、またはハードディスクを拡張します。

ハードディスク容量使用率がフルである

障害事象：新しいファイルを作成すると、「No space left on device」 というエラー情報が表示され、かつ `df -h` コマンドを使用すると、 ディスク容量使用率100%表示される。
考えられる原因： ハードディスク容量が枯渇している。
対処手順：使用する必要のないファイルを削除するか、またはハードディスクを拡張します。

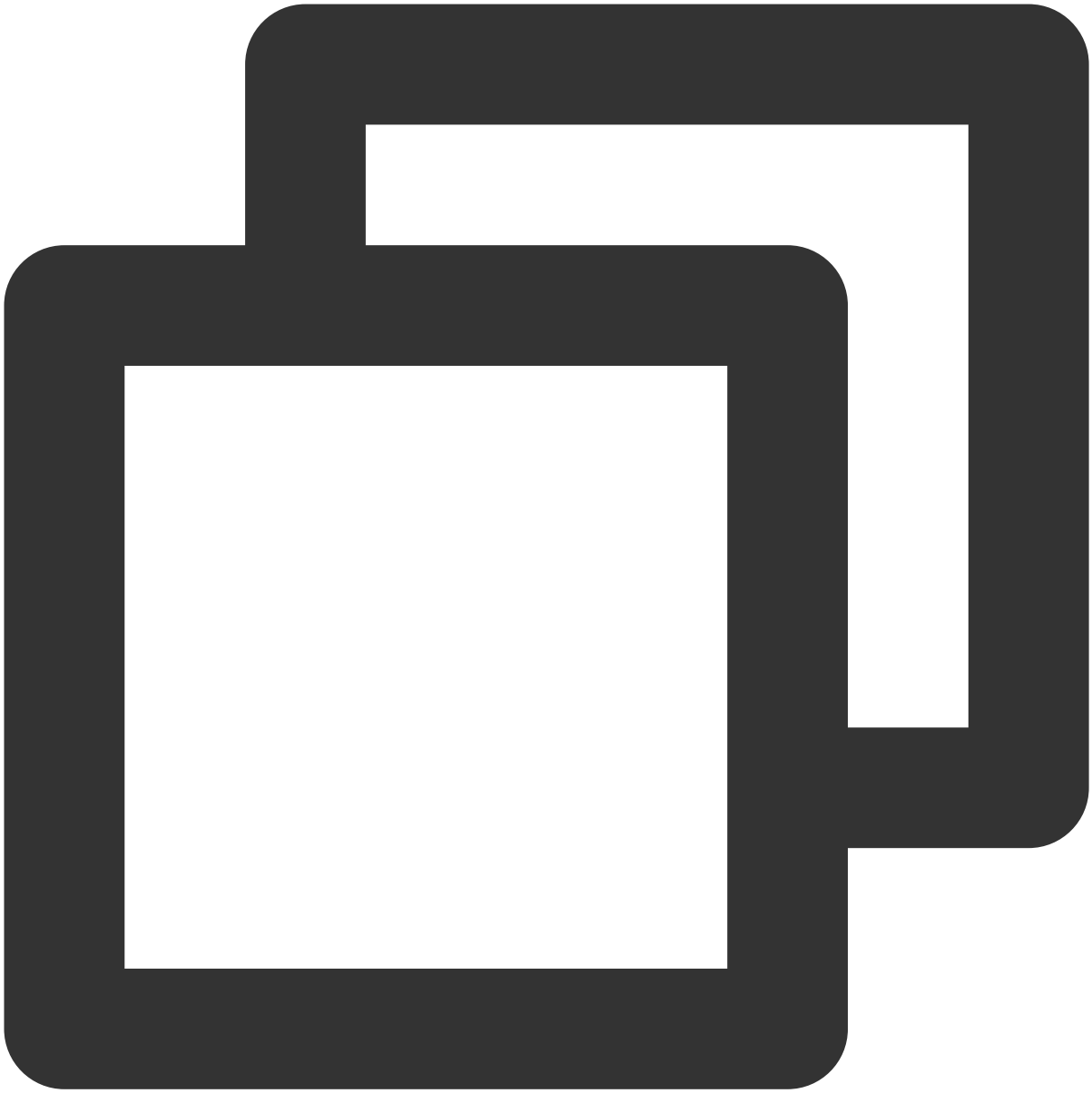
ハードディスクが読み取り専用となる

障害事象： ファイルシステムがファイルの読み取りしかできなくなり、新たなファイルを作成できない。
考えられる原因： ファイルシステムが破損している。
対処手順：
1. ハードディスクデータをバックアップするためのスナップショットを作成します。詳細は スナップショットの作成 をご参照ください。
2. ハードディスクのタイプに応じて、対応する対処手順を実行します：
システムディスク
データディスク
インスタンスを直接再起動します。詳細は インスタンスの再起動 をご参照ください。
1. 次のコマンドを実行し、読み取り専用ディスクに対応するファイルシステムのタイプを表示します。



```
lsblk -f
```

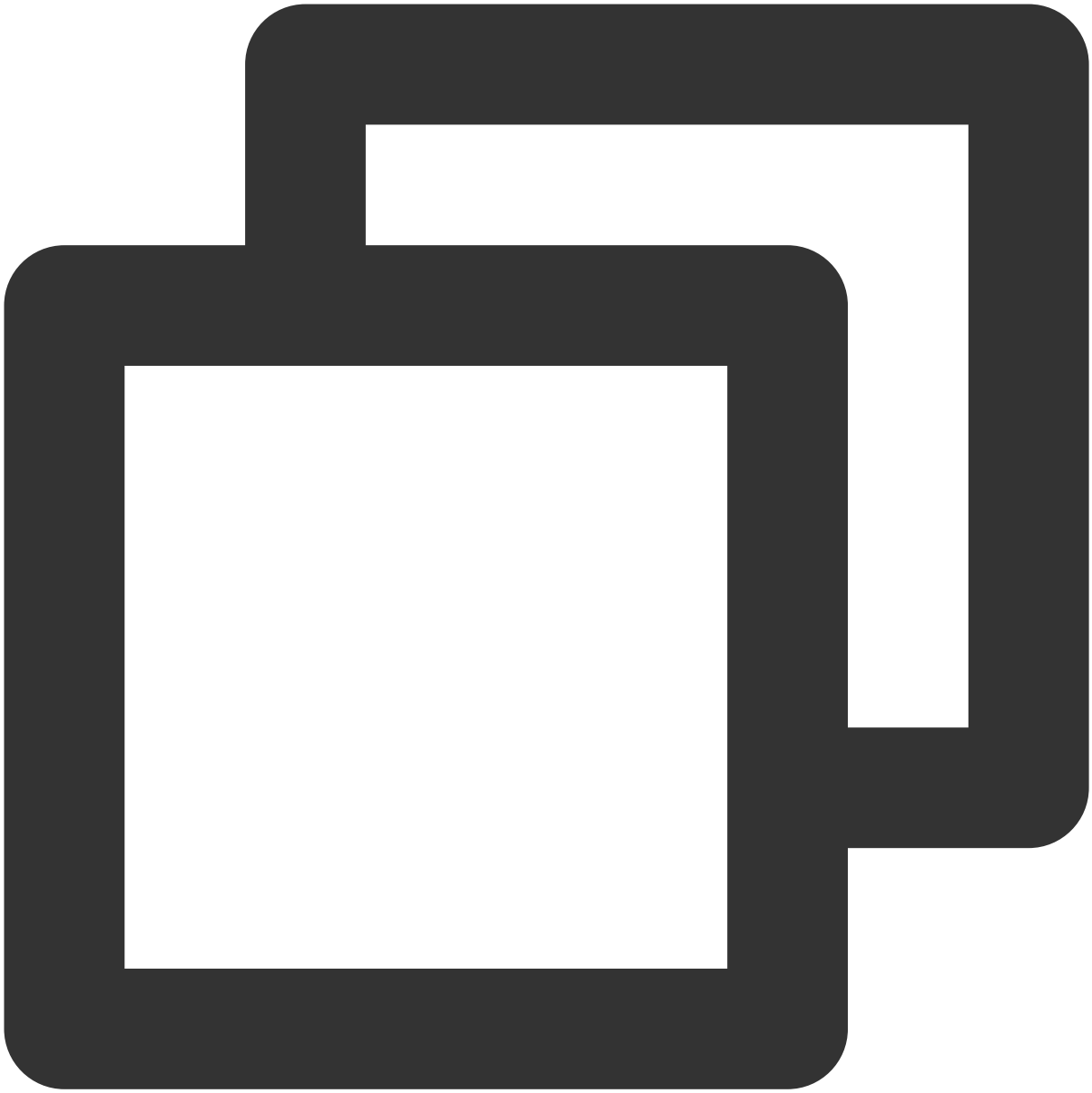
2. 次のコマンドを実行し、データディスクをアンインストールします。



```
umount <対応するディスクマウントパス>
```

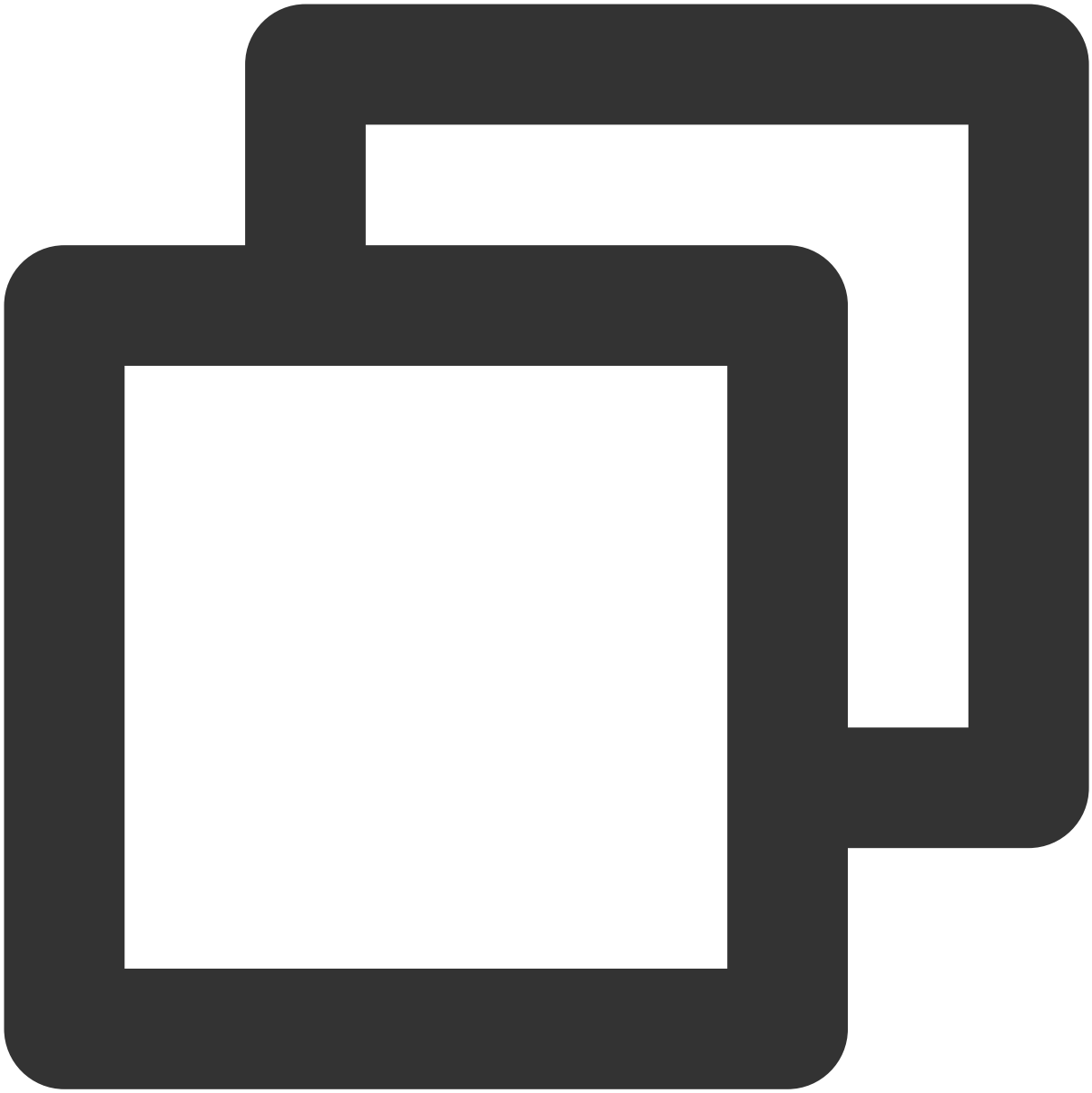
3. ファイルシステムのタイプに応じて、次のコマンドを実行し、修復を行います：

ext3/ext4 ファイルシステムでは、次のコマンドを実行します：



```
fsck -y /dev/対応ディスク
```

xfs ファイルシステムでは、次のコマンドを実行します：



```
xfs_repair /dev/対応ディスク
```

ハードディスク %util が高い

障害事象：インスタンスにラグが発生し、SSHまたはVNCを使用したログインに時間がかかる、または応答しない。
考えられる原因：IO負荷が高く、ハードディスク %util が100%に達している。
対処手順： IO 負荷が合理的かどうかを確認し、かつ IO の読み取りと書き込みを減らすか、またはより高性能なハードディスクに交換するかを評価する必要があります。

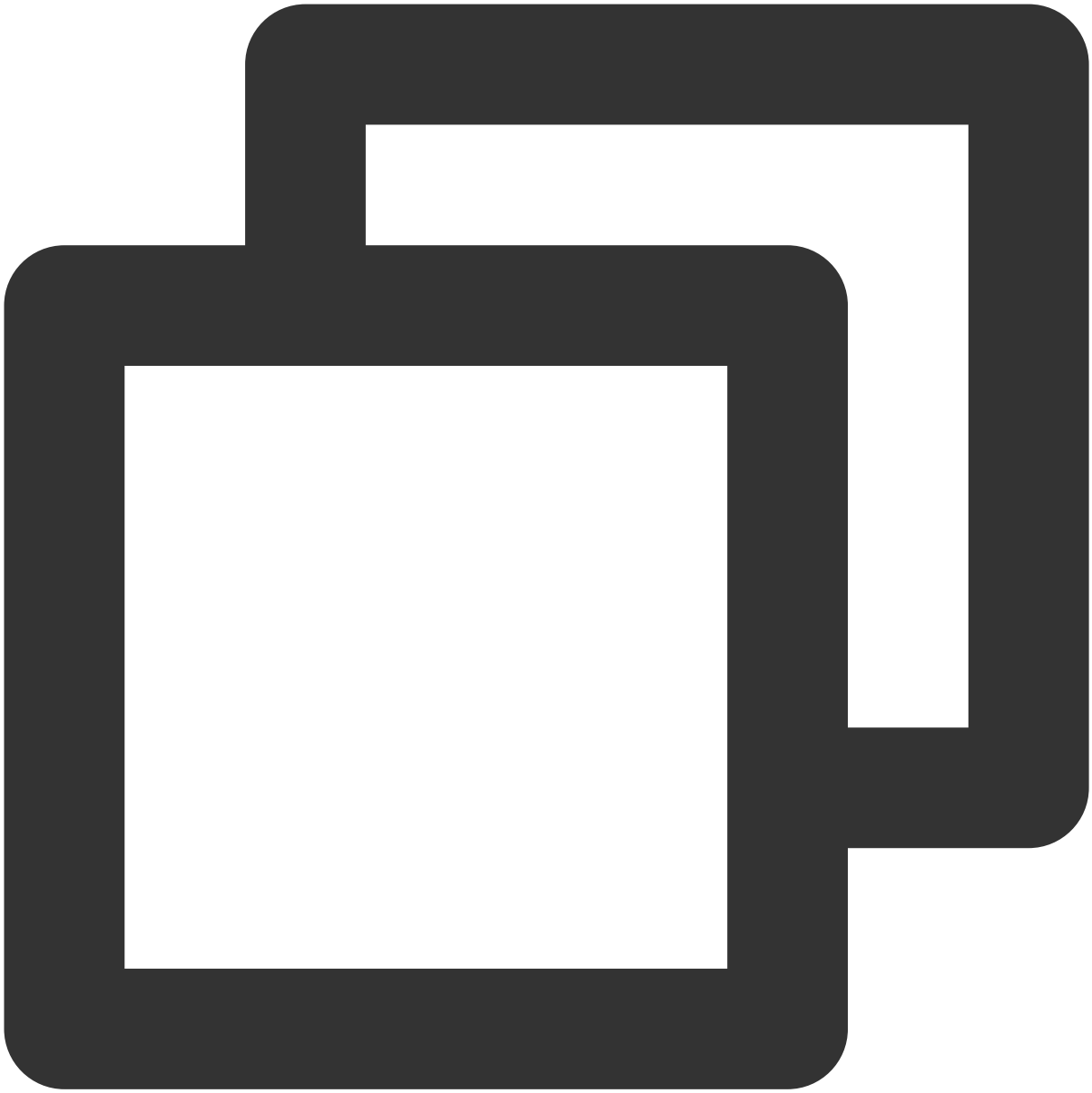
システムbinまたはlibソフトリンクの欠如

最終更新日：：2022-05-06 11:46:50

##故障について
コマンドの実行またはシステム起動のプロセスで、コマンドが見つからないか、またはlibファイルが見つからないなどのエラー情報が発生します。

考えられる原因

以下に示すとおり、CentOS 7、CentOS 8、Ubuntu 20などのシステムのbin、sbin、lib、lib64はソフトリンクです。



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

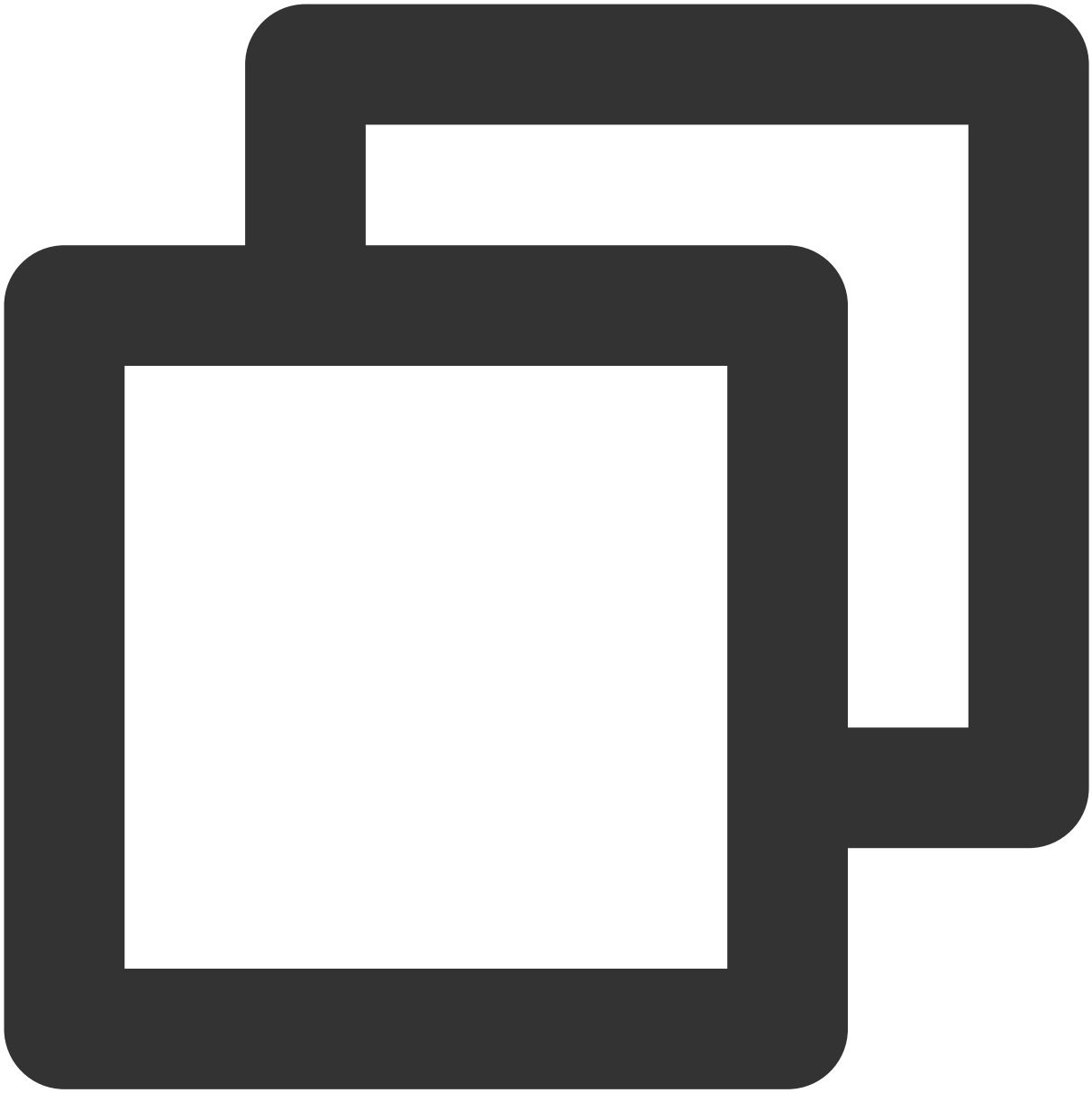
ソフトリンクが削除された場合は、コマンドの実行またはシステム起動のプロセスでエラーが発生します。

ソリューション

処理手順 を参照して、必要なソフトリンクを調べて作成してください。

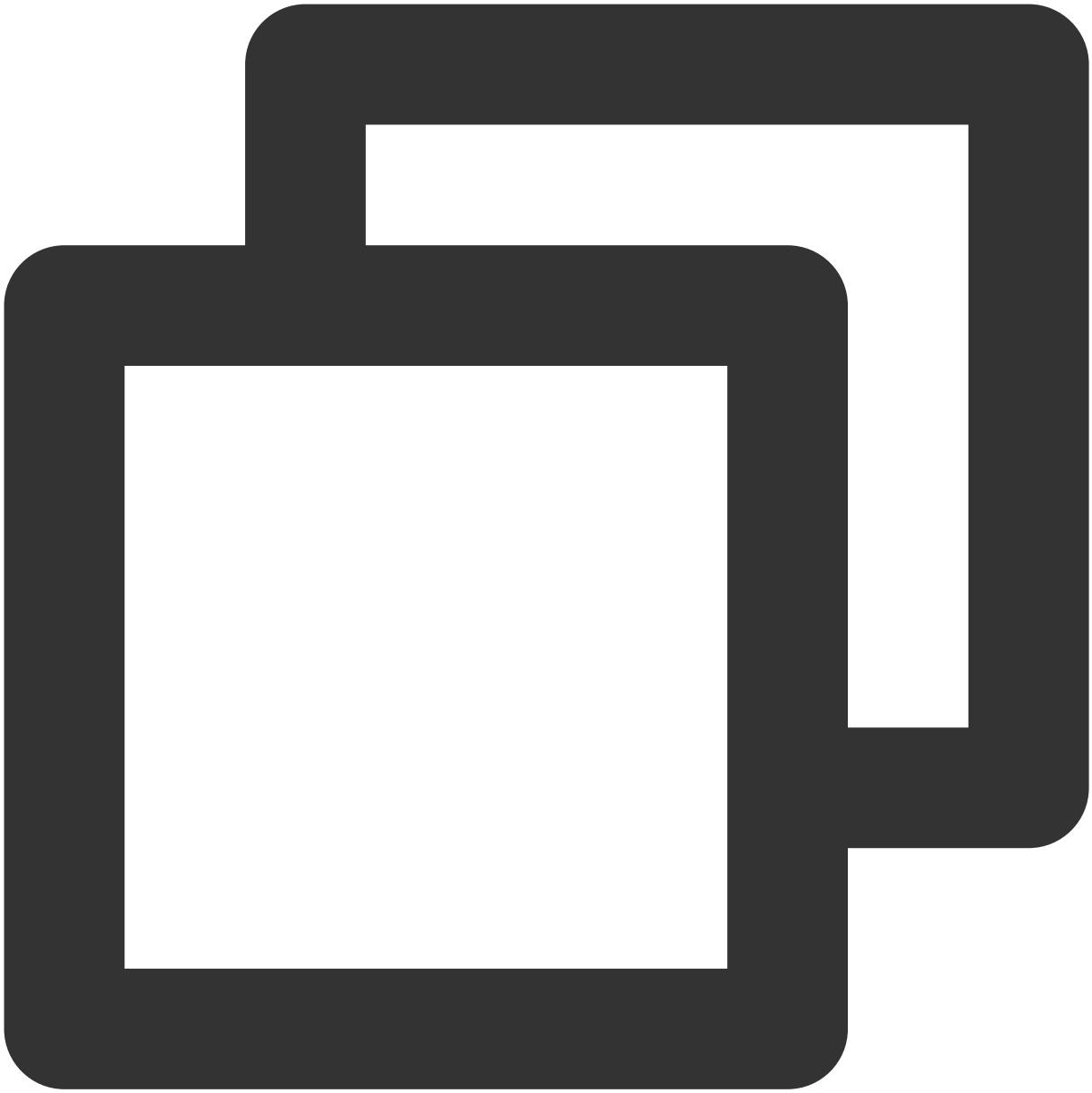
処理手順

1. レスキューモードに進みます。
2. その中の `mount` 、 `chroot` などのコマンドを実行します。そのうち、 `chroot` コマンドを実行した場合：
エラーがある場合は、 `cd /mnt/vm1` を実行します。
エラーがない場合は、 `cd /` を実行します。
3. 以下のコマンドを実行して、対応するソフトリンクがあるかどうかを確認します。



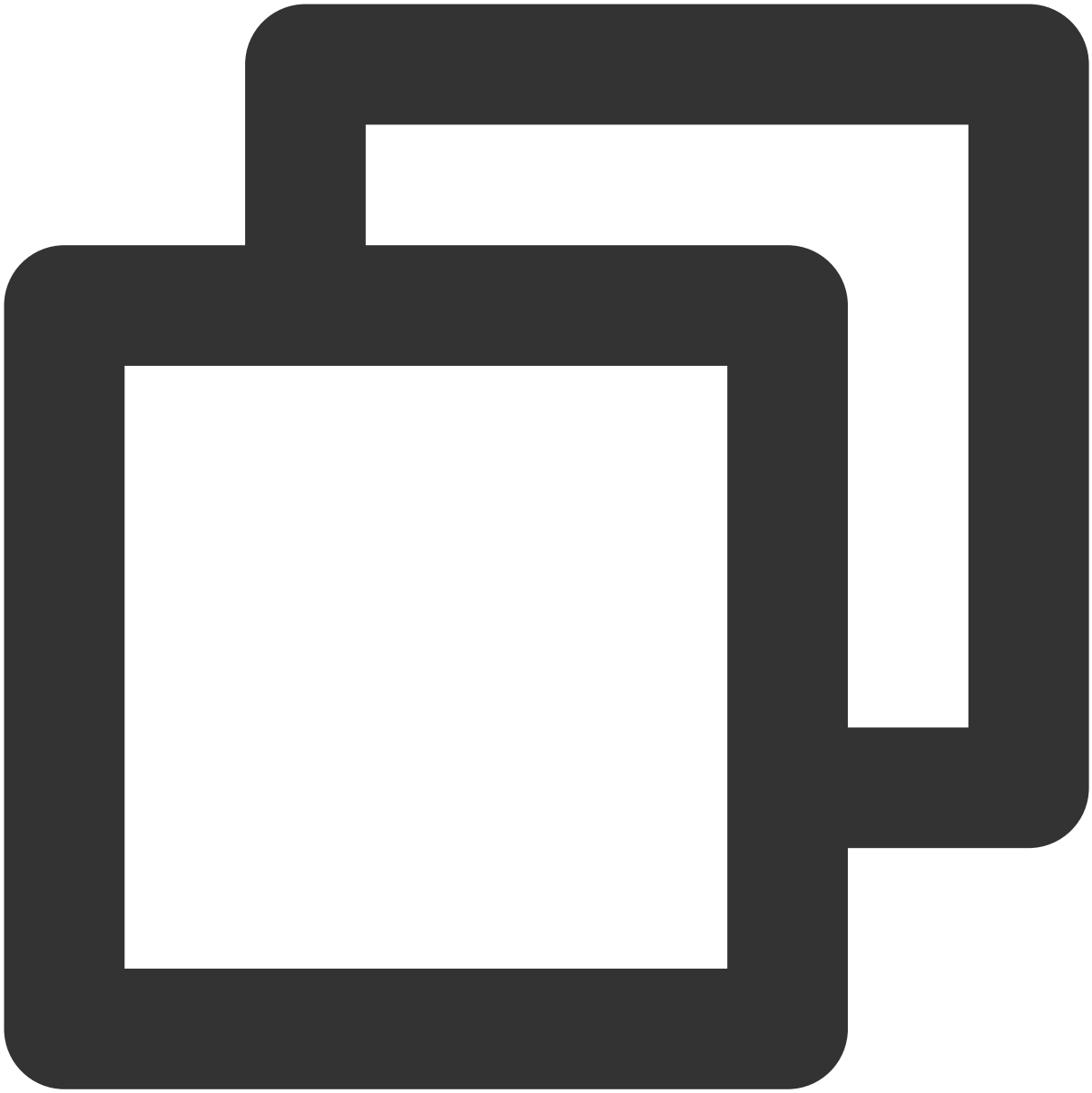
```
ls -al / | grep -E "lib|bin"
```

ソフトリンクがある場合は、チケットを提出 して連絡し、サポートを受けてください。
ソフトリンクがない場合は、必要に応じて以下のコマンドを実行して、対応するソフトリンクを作成してください。



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

4. 以下のコマンドを実行して、ソフトリンクをチェックします。



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

エラー情報がない場合は、ソフトリンクの修正に成功しています。

5. レスキューモードを終了して、システムを起動します。

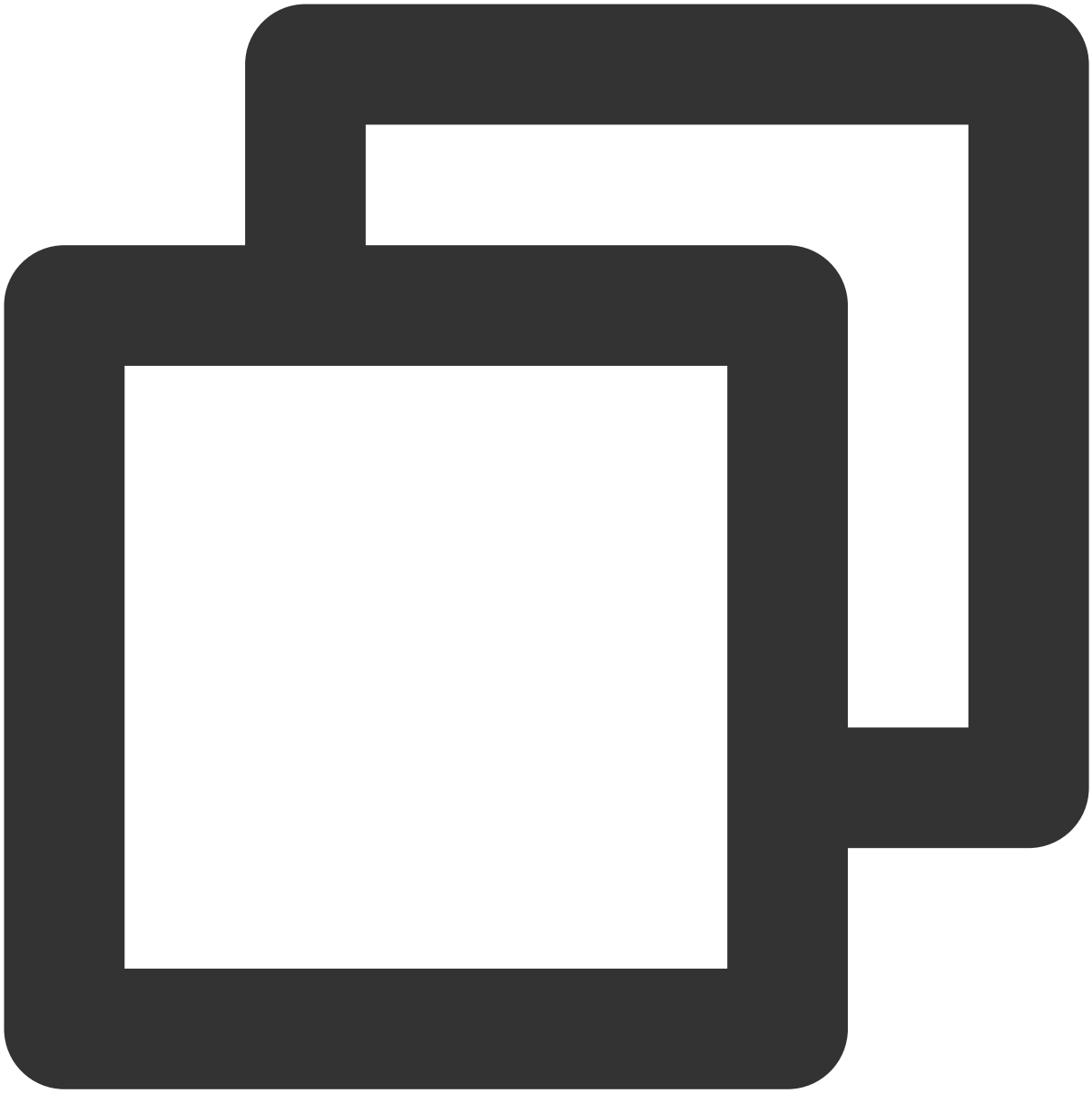
CVMにウイルス侵入が疑われる場合

最終更新日：：2022-05-06 11:46:50

CVMは弱いパスワード、オープンソースコンポーネントの脆弱性などの問題が原因でハッカーに侵入される可能性があります。本文では、CVMがウイルスに侵入されているかどうかを判断する方法とその解決方法を紹介します。

問題の特定

SSH方式を使用 または VNC方式を使用 してインスタンスにログイン後、以下の方法でCVMがウイルスに侵入されているかどうかを判断します。
rc.local に悪意のあるコマンドが追加されている
以下のコマンドを実行し、 `rc.local` ファイルを確認します。

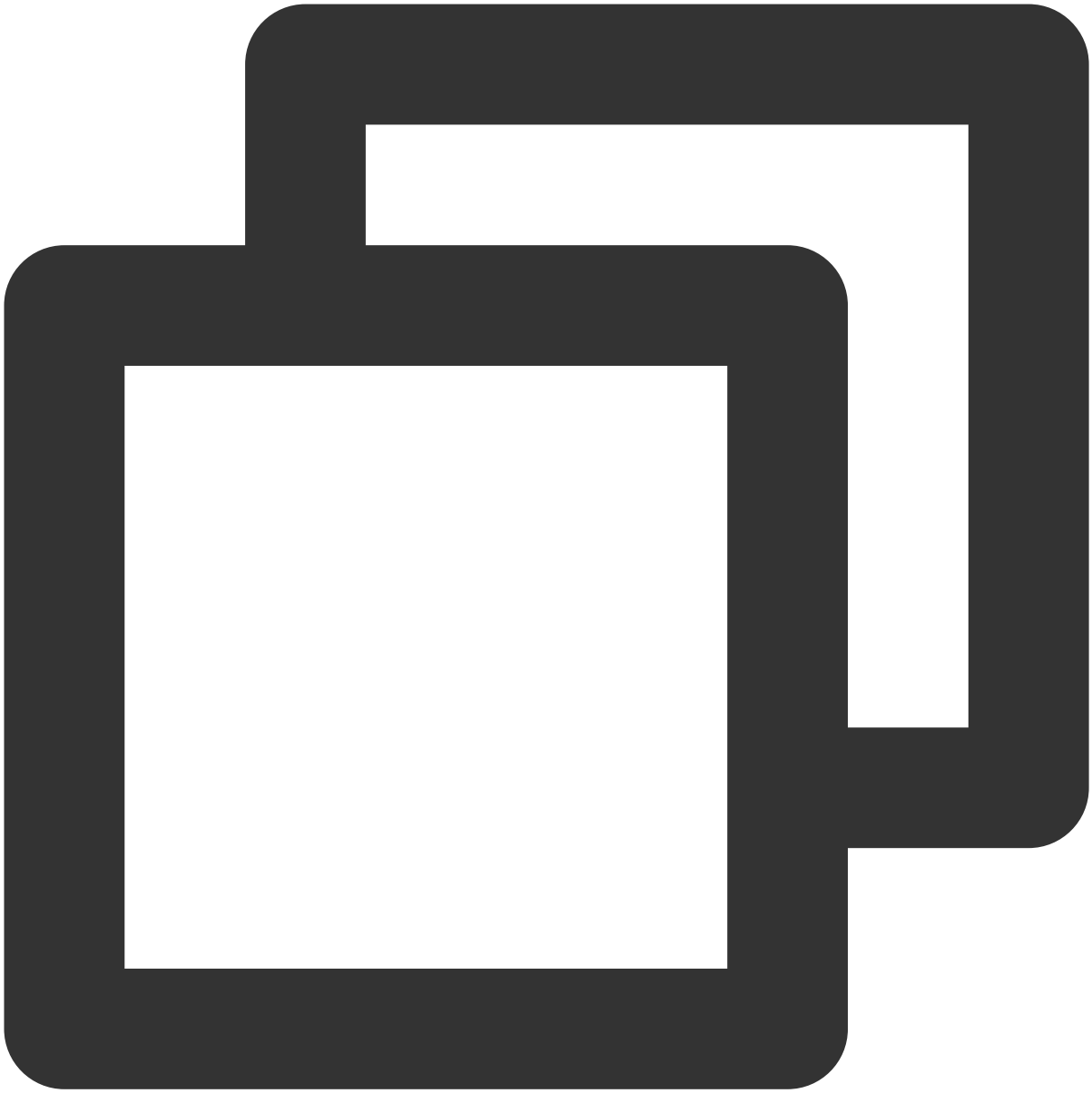


```
cat /etc/rc.local
```

例えば、出力情報が `wget xx` 、 `/tmp/xx` など、業務またはお知らせのイメージに追加していないコマンドであった場合、CVMは高い確率でウイルスに侵入されています。

crontab に悪意のあるタスクが追加されている

以下のコマンドを実行し、現在のスケジュール表を列挙します。

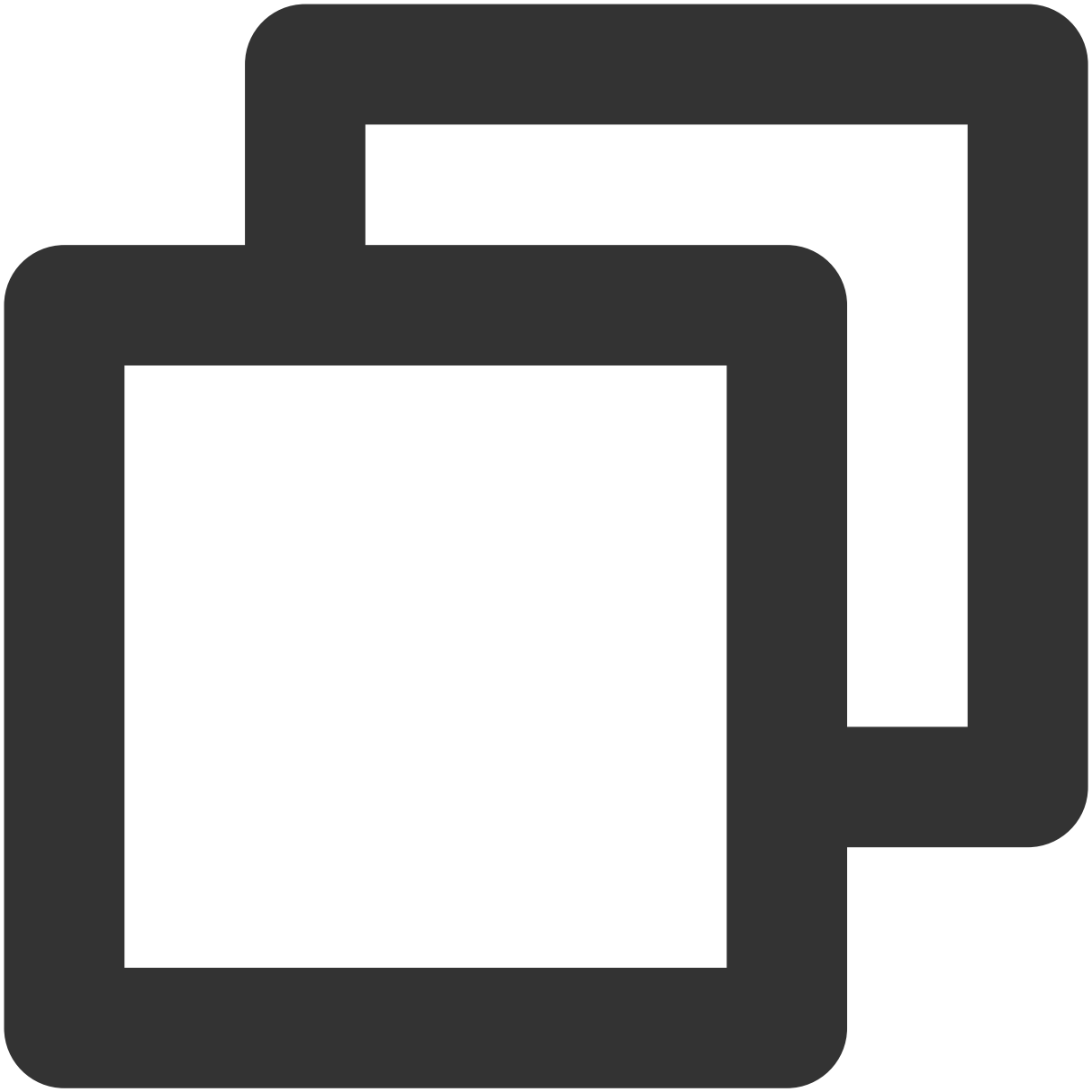


```
crontab -l
```

例えば、出力情報が `wget xx` 、 `/tmp/xx` など、業務またはお知らせのイメージに追加していないコマンドであった場合、CVMは高い確率でウイルスに侵入されています。

ld.so.preloadで動的ライブラリのハイジャックが増加しています

以下のコマンドを実行し、 `/etc/ld.so.preload` ファイルを確認します。

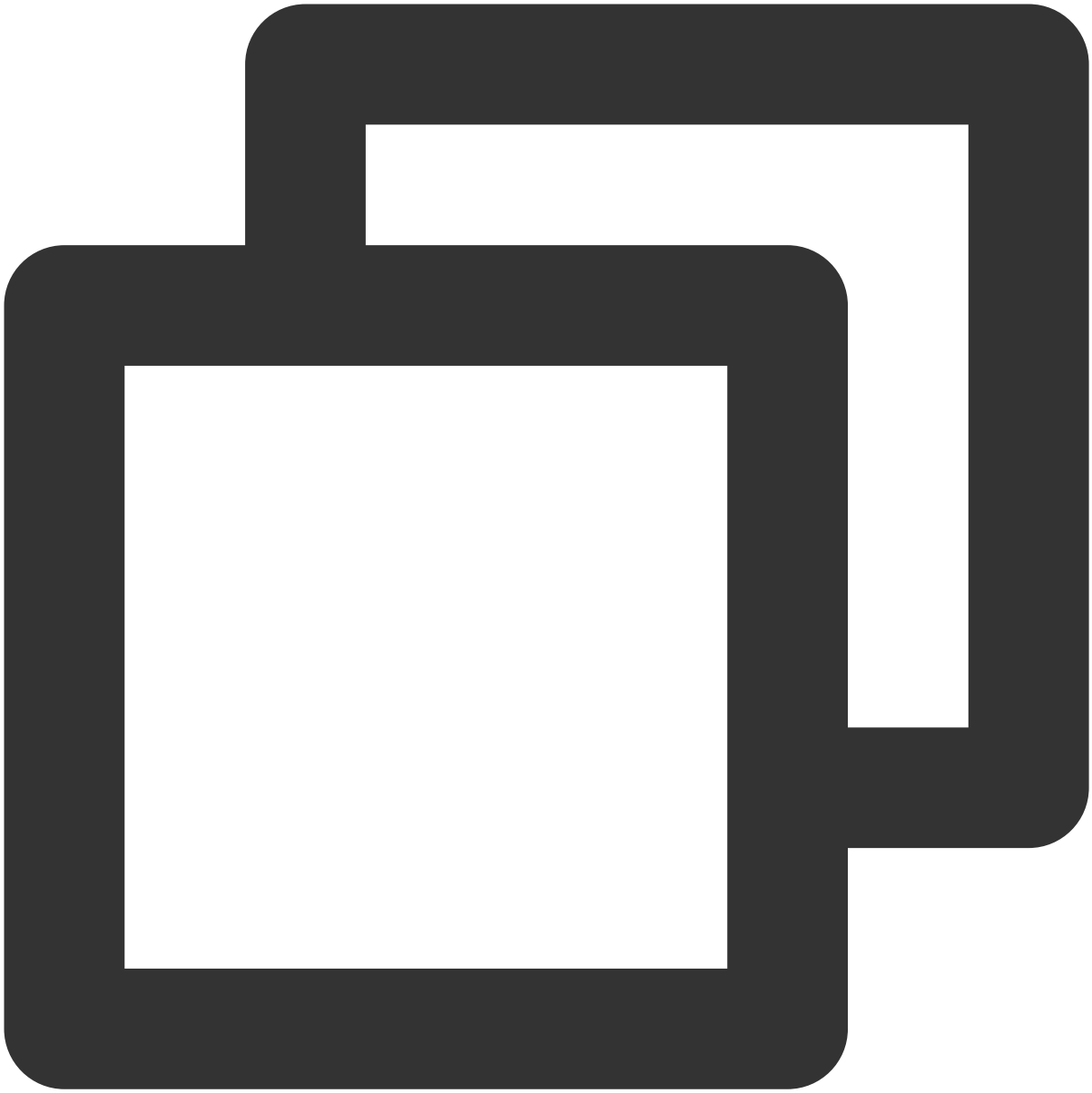


```
cat /etc/ld.so.preload
```

出力情報が業務で追加していない動的ライブラリであった場合、CVMは高い確率でウイルスに侵入されています。

sysctl.conf にラージページメモリが設定されています

以下のコマンドを実行し、ラージページメモリの使用状況を確認します。



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

0以外で、かつ業務自体のプログラムと使用していないラージページメモリを出力した場合、CVMは高い確率でウイルスに侵入されています。

処理手順

1. スナップショットの作成 を参照し、システムデータのバックアップを完了します。

2. システムの再インストール を参照して、インスタンスシステムを再インストールし、以下の処置を参照してセキュリティポリシーを強化します。
CVMのパスワードを変更し、大文字、小文字、特殊記号、数字を組み合わせた12～16桁の複雑なランダムパスワードを設定します。詳細については、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内の使われていないユーザーを削除します。
sshdのデフォルトの22ポートを1024～65525の間の他の非常用ポートに変更します。詳細については、CVMリモートデフォルトポートの変更 をご参照ください。
CVMのセキュリティグループに関連付けられているルールを管理し、業務およびプロトコルに必要なポートのみをオープンにし、すべてのプロトコルおよびポートをオープンにはしないことを推奨します。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。
mysql、redisなどのパブリックネットワークにコアアプリケーションサービスポートへのアクセスを開放することは推奨しません。 関連するポートをローカルアクセスに変更、または外部ネットワークアクセス禁止にすることができます。
「雲鏡」、「雲鎖」などの保護ソフトウェアをインストールし、リアルタイムアラームを追加して、異常なログイン情報を速やかに取得できるようにします。

ファイル作成のエラー no space left on device

最終更新日：：2022-05-06 11:46:50

##故障について
Linux CVMで新しいファイルを作成するときに、「no space left on device」のエラーが発生する。

考えられる原因

ディスク容量が満杯
ファイルシステム `inode` が満杯
df duが不一致
ファイルを削除済みだが、対応するファイルハンドラを持つプロセスがまだ残っており、ディスク容量がかなりの間リリースされていない。
mountマウントネスト。例えば、システムディスクの `/data` ディレクトリが大容量を使用し、さらに `/data` をマウントポイントとしてその他のデータディスクにマウントすると、システムディスクでdf duが一致しない場合がある。

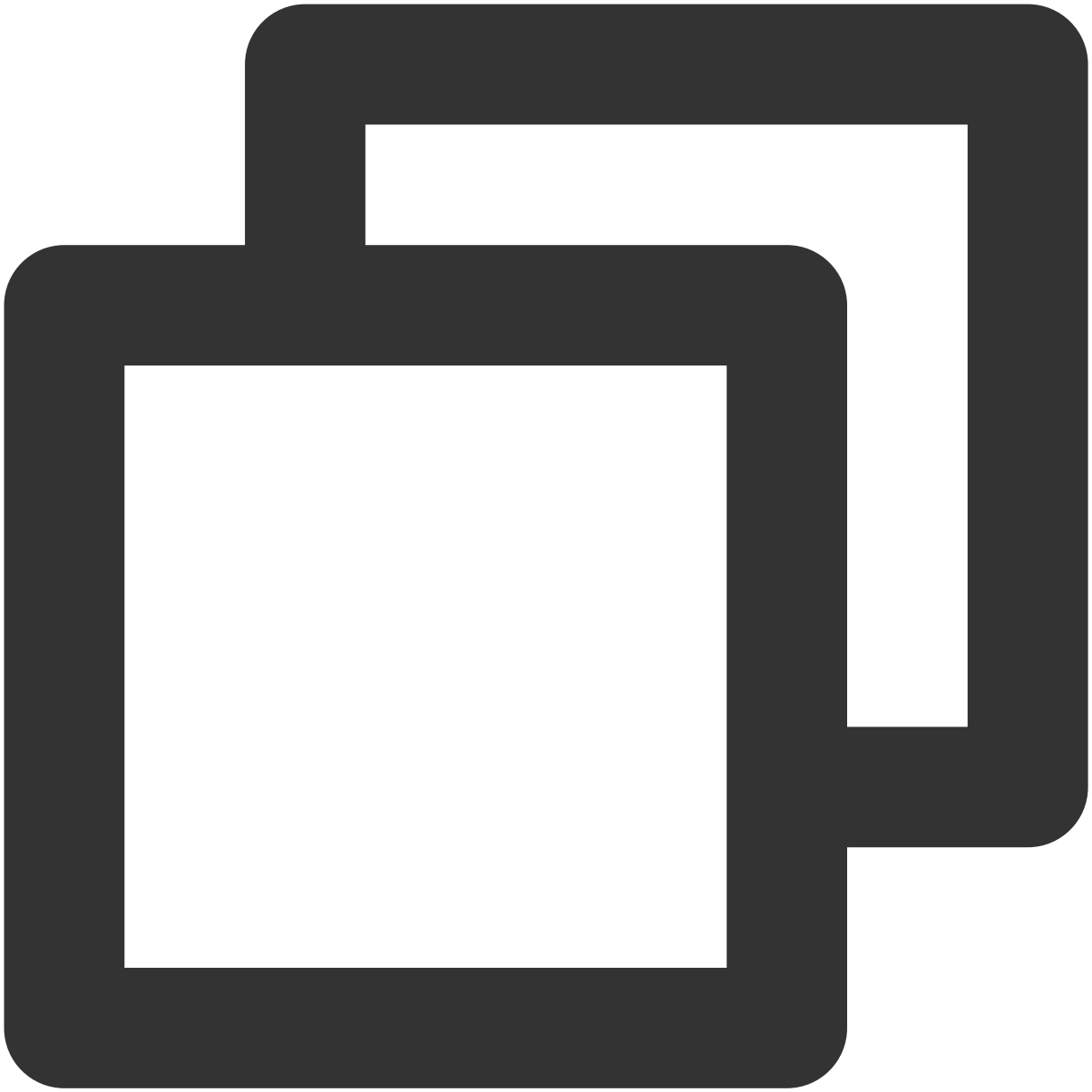
ソリューション

処理方法 を参照し、問題を調査および解決してください。

処理方法

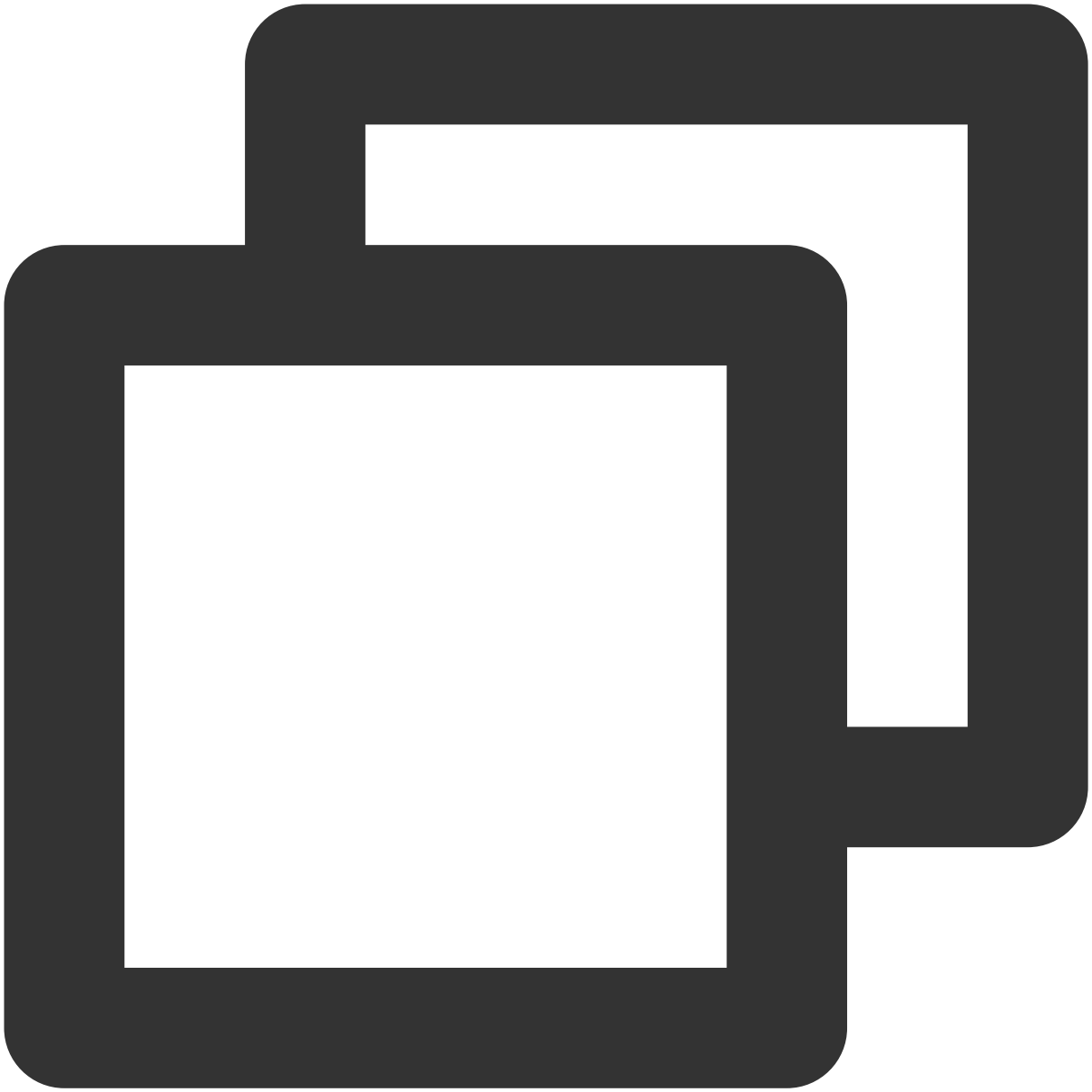
ディスク容量が満杯の問題を解決

1. CVM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 をご参照ください。
2. で以下のコマンドを実行し、ハードディスク使用率を確認します。



```
df -h
```

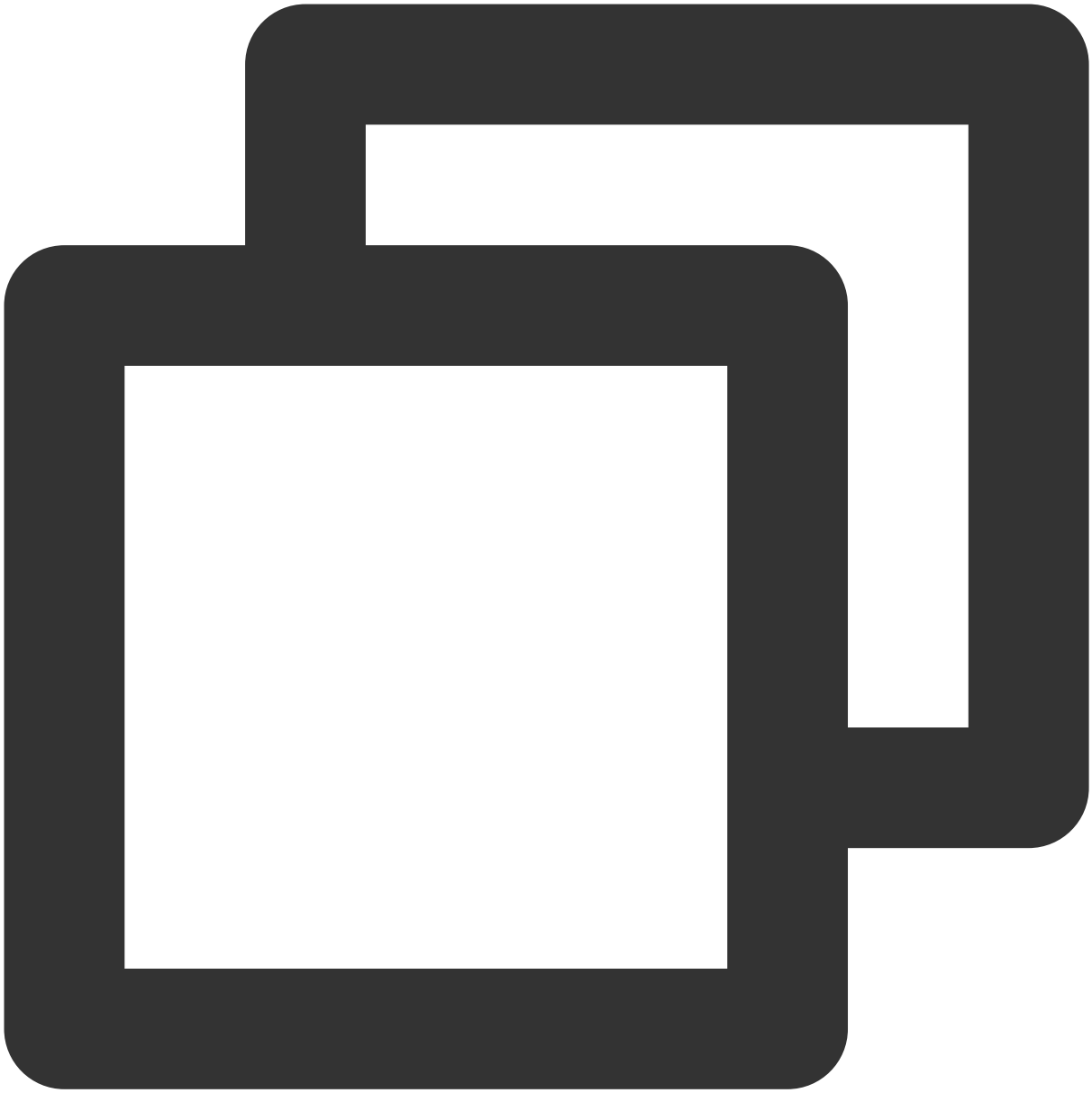
3. ハードディスク使用率の高いマウントポイントを特定し、さらに以下のコマンドを実行してそのマウントポイントに入ります。



```
cd対応マウントポイント
```

例えば、cdシステムディスクマウントポイントが必要な場合、 `cd /` を実行します。

4. 以下のコマンドを実行し、使用容量の大きいディレクトリを検索します。



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

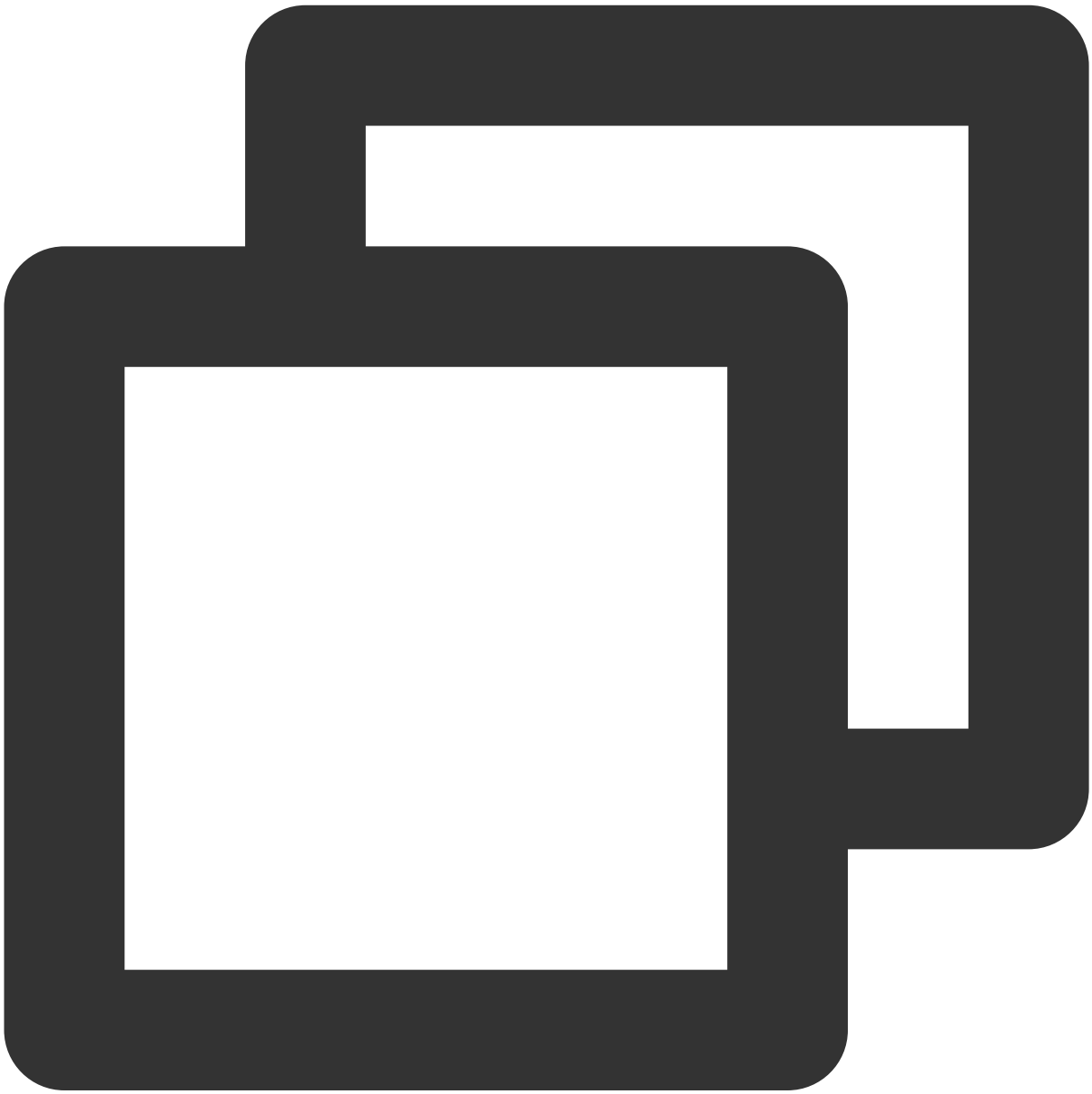
使用容量最大を検知したディレクトリの容量状況に応じて、以下の手順を実行します。

ディレクトリ容量がハードディスク総容量より大幅に低い場合、df duが不一致の問題を解決 手順を参照して引き続き問題を調査してください。

ディレクトリ容量が大きい場合、手順2 を実行して使用容量が大きいファイルを特定し、総合的なビジネス状況により削除するかどうかを評価してください。削除できない場合、CBS拡張 からハードディスクストレージ容量を拡張してください。

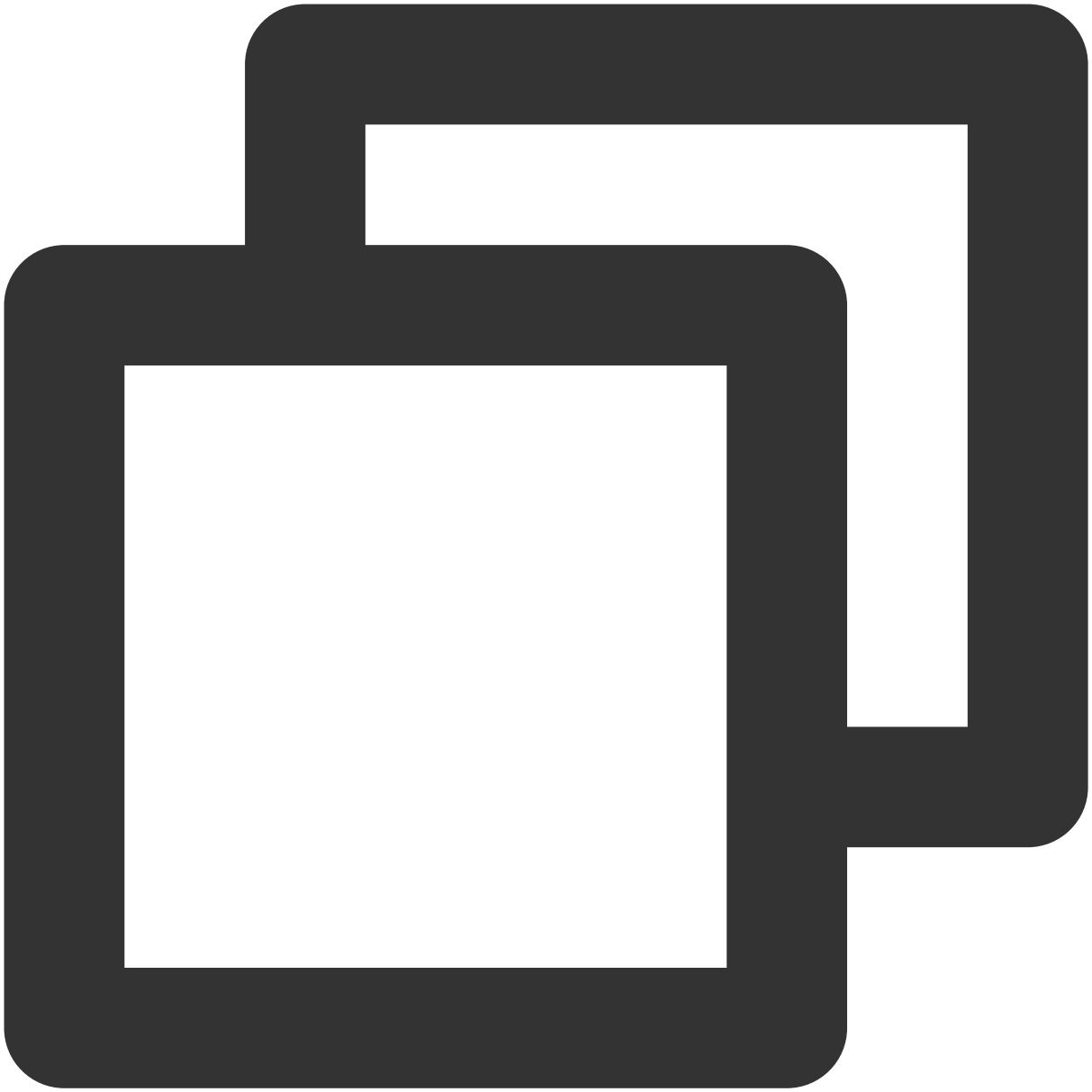
ファイルシステムinodeが満杯の問題を解決

1. CVM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 をご参照ください。
2. で以下のコマンドを実行し、ハードディスク使用率を確認します。



```
df -h
```

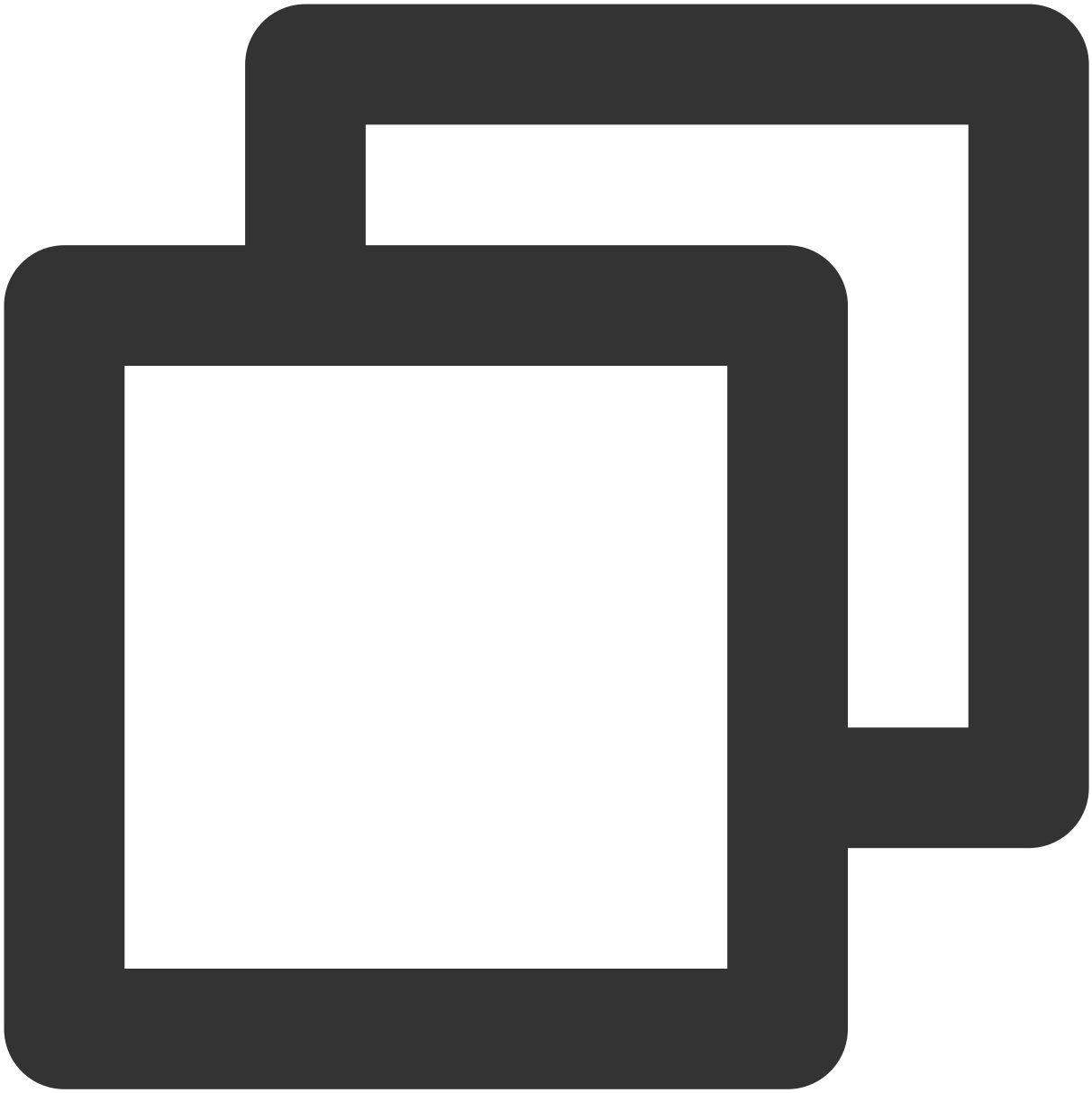
3. ハードディスク使用率の高いマウントポイントを特定し、さらに以下のコマンドを実行してそのマウントポイントに入ります。



```
cd対応マウントポイント
```

例えば、cdシステムディスクマウントポイントが必要な場合、 `cd /` を実行します。

4. 以下のコマンドを実行し、ファイル個数が最多のディレクトリを検索し、この問題を解決します。このコマンドは時間がかかるため、少々お待ちください。

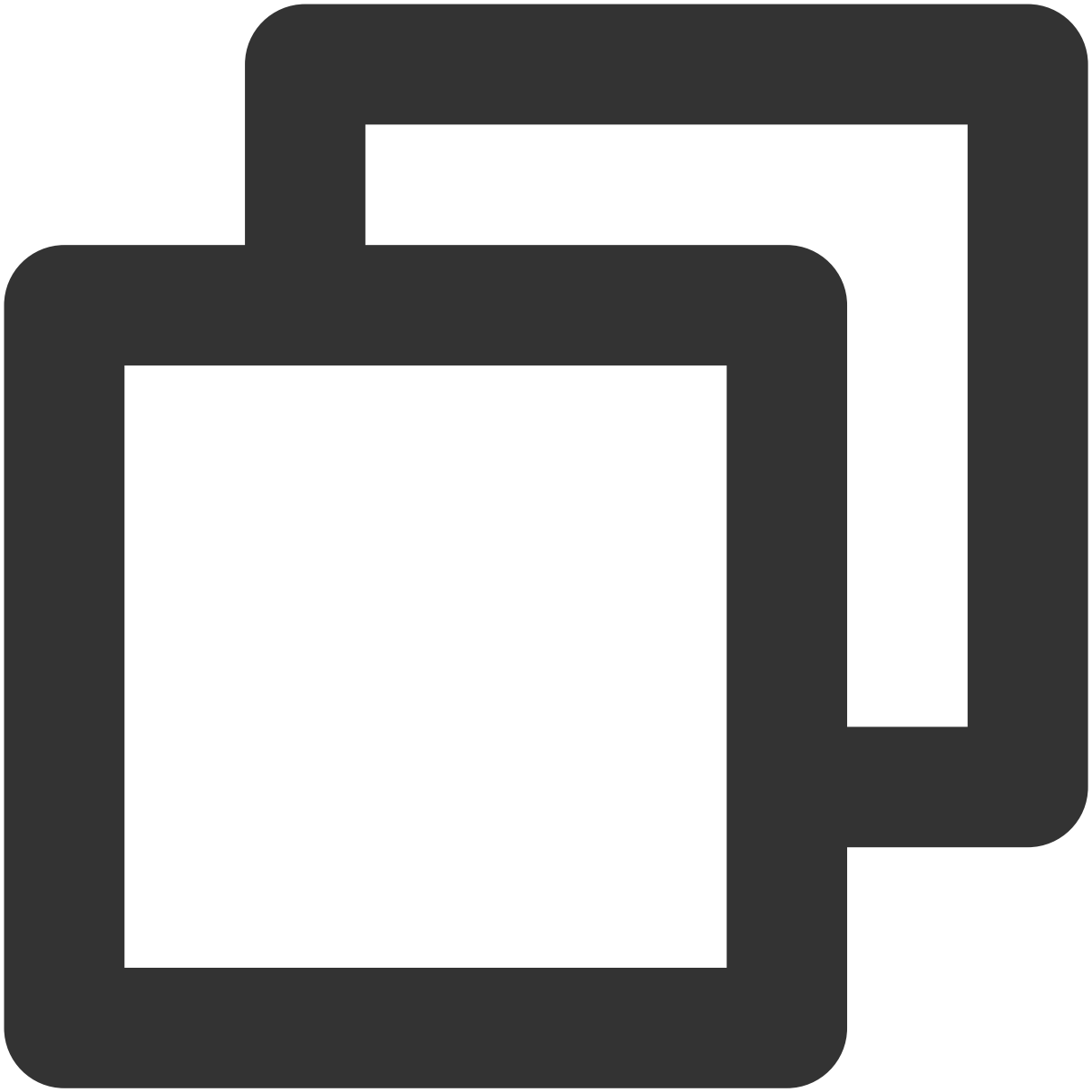


```
find / -type f | awk -F / -v OFS=/ '{$NF="";dir[$0]++}END{for(i in dir)print dir[i]
```

df duが不一致という問題を解決

プロセスがファイルハンドラを占用する問題を解決

以下のコマンドを実行し、占用しているファイルのプロセスを確認します。



```
lsof | grep delete
```

リターン結果に応じて、以下の手順を実行します。

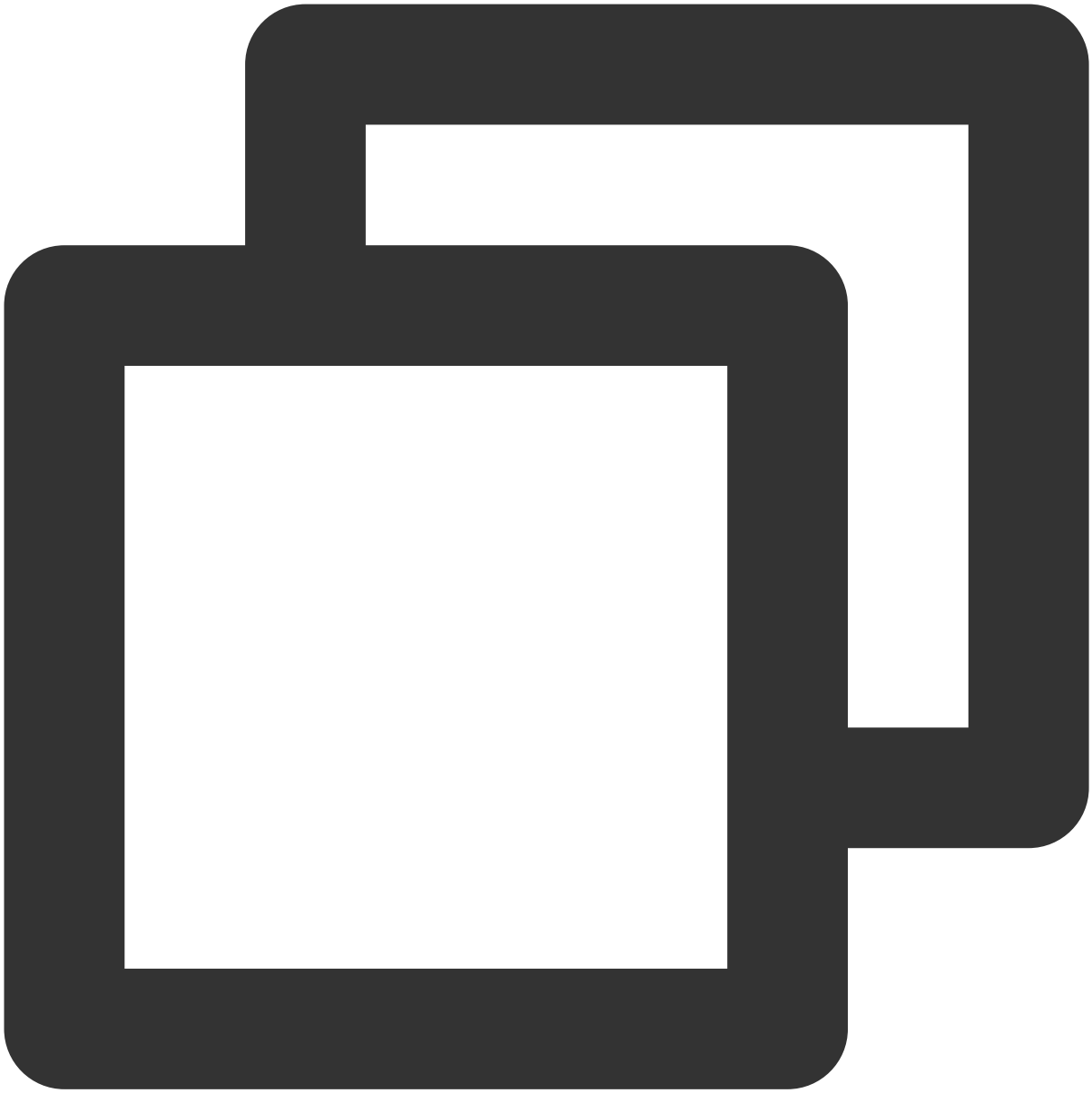
kill対応プロセス。

サービスを再起動します。

ファイルハンドラを占用するプロセスが多い場合、サーバーを再起動することができます。

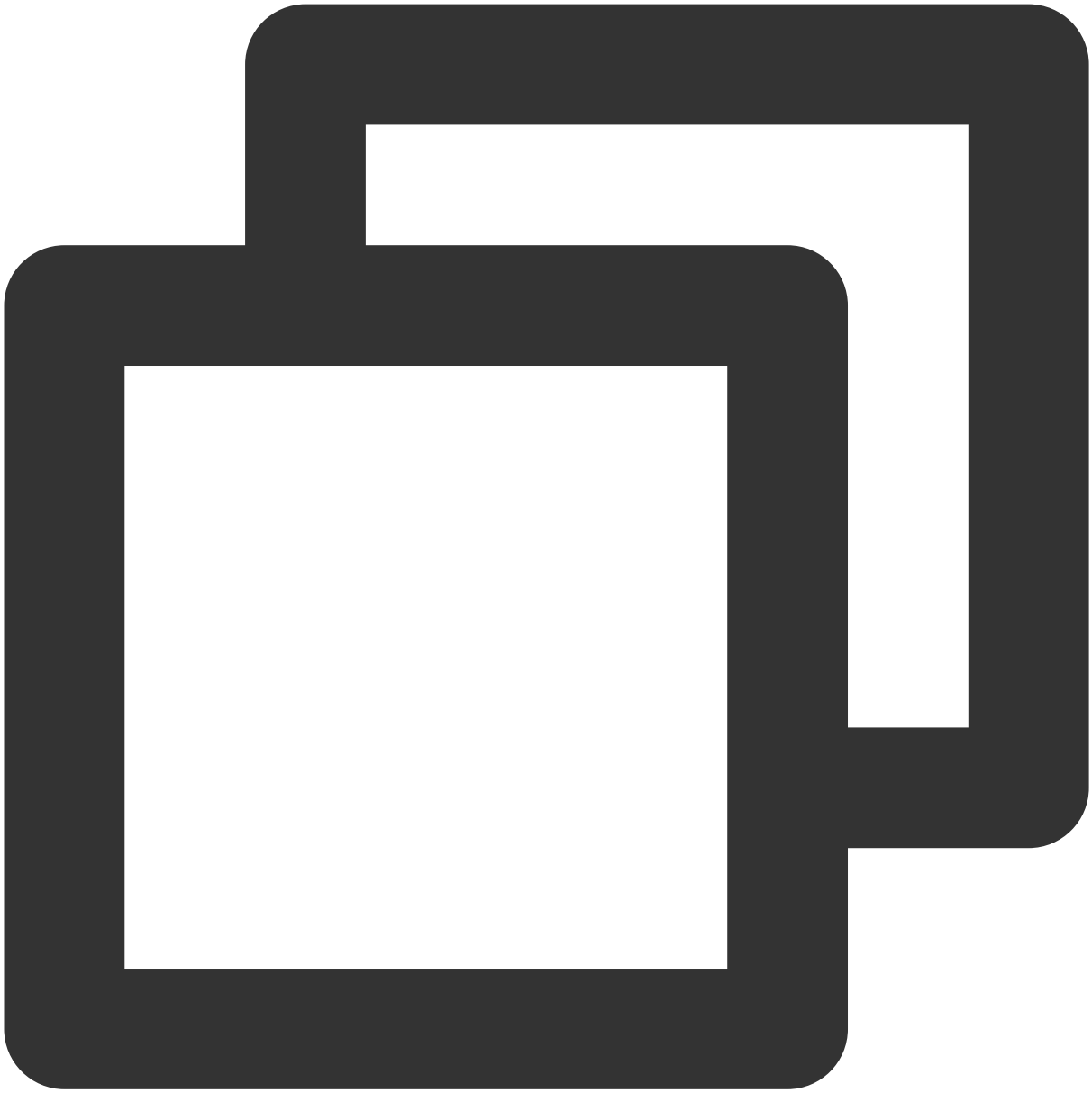
mountマウントネストの問題を解決

1. mountコマンドを実行し、使用容量が大きい磁気ディスクを `/mnt` にマウントします。例：



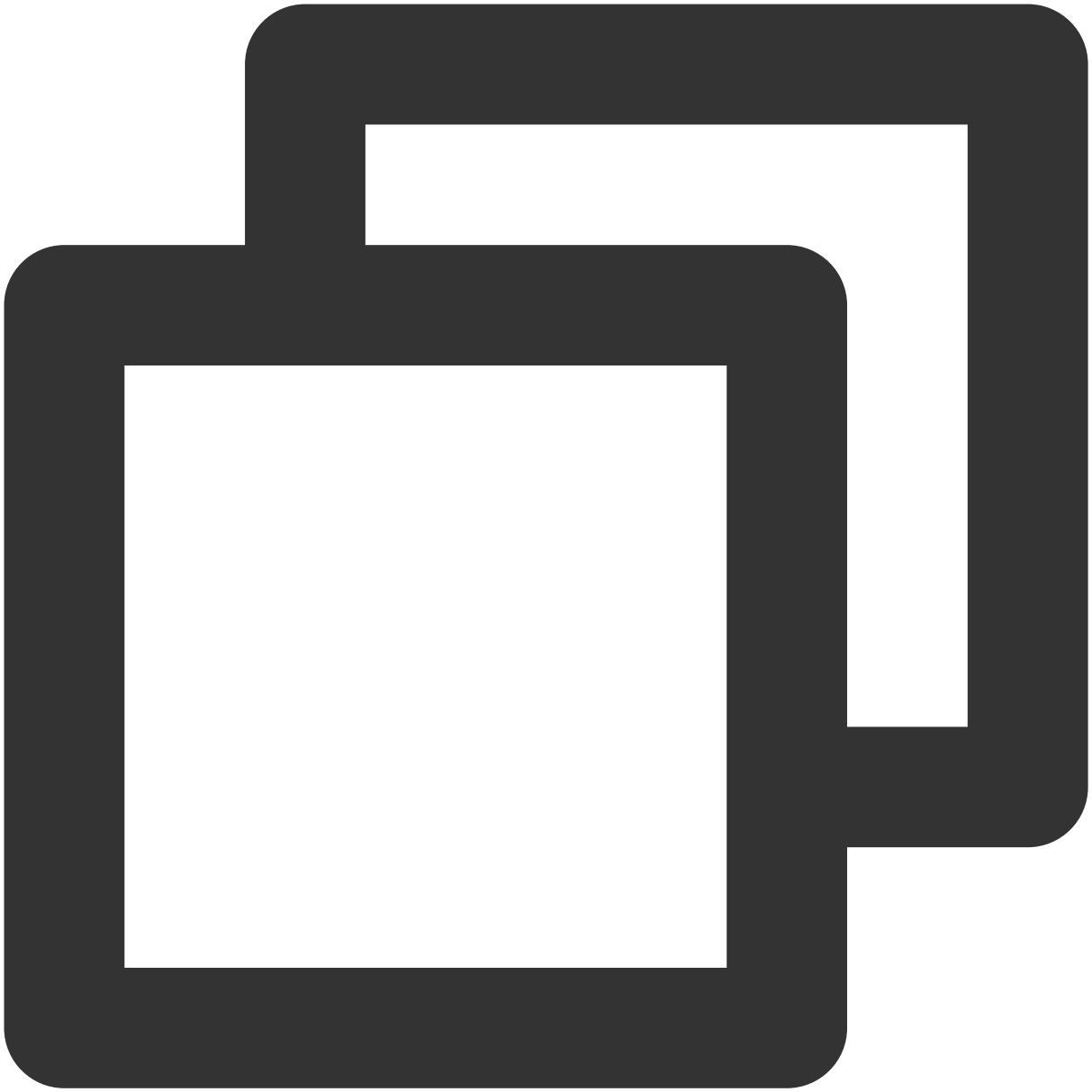
```
mount /dev/vda1 /mnt
```

2. 以下のコマンドを実行し、`/mnt` に入ります。



```
cd /mnt
```

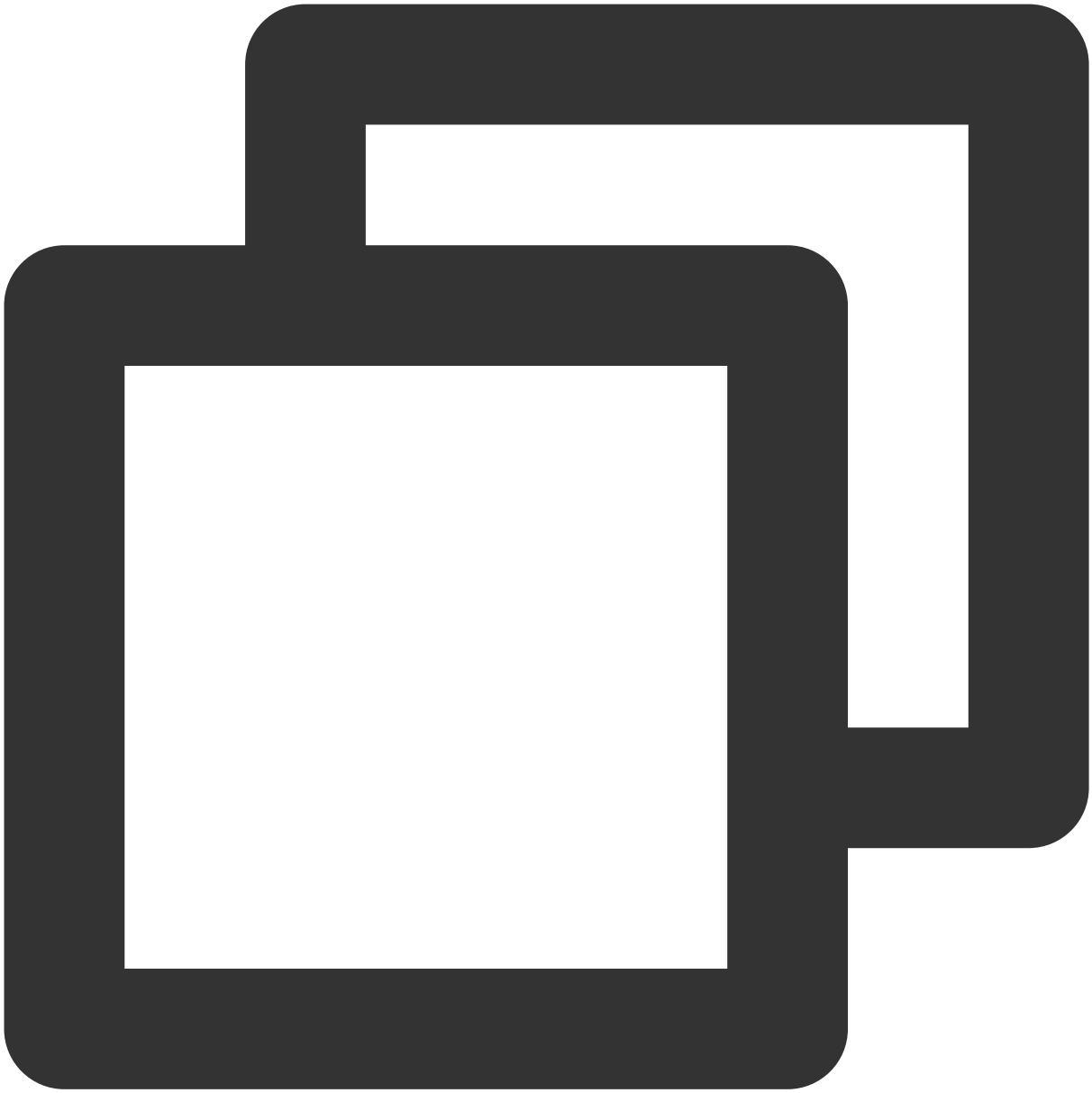
3. 以下のコマンドを実行し、使用容量の大きいディレクトリを検索します。



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

リターン結果に応じて、総合的なビジネス状況によりディレクトリまたはファイルを削除するかどうかを評価します。

4. umountコマンドを実行し、磁気ディスクをマウント解除します。例：



```
umount /mnt
```

ネットワーク関連の故障
国際リンクレイテンシー

最終更新日：：2022-07-26 17:41:55

問題の説明

北米リージョンのCVMにログインする時レイテンシーが長すぎます。

問題の分析

国内の国際ルーティング出口の数が少ないおよびその他要因により、並列処理数が高くなると、国際リンクが非常に混雑になり、アクセスが不安定になります。Tencent Cloudはすでにこの問題ををキャリアに報告しています。
現在、北米リージョンのCVMを購入して、中国国内で管理及びメンテナンスする必要がある場合、中国香港リージョンで購入したCVMを経由して、北米リージョンのCVMにログインすることで問題を解決できます。

ソリューション

1. 中国香港リージョンのWindows CVMを購入して、「ジャンプサーバー」として利用します。
ご注意：
「カスタマイズ設定」ページの「1.リージョンとモデル選択」で、**中国香港**リージョンを選択します。
ここをクリックして購入する >>
Windows CVMは、北米リージョンにあるWindowsとLinuxのCVMへのログインをサポートしているので、購入することを推奨します。
中国香港リージョンのWindows CVMを購入する場合、1Mbps以上の帯域幅を購入する必要があります。そうしないと、ジャンプサーバーにログインできません。
2. 購入が成功した後、実際のニーズに応じて、中国香港リージョンのWindows CVMのログイン方法を選択する：
RDPファイルを利用してWindows CVMにログインする
リモートデスクトップを利用してWindows CVMにログインする
VNC を利用してWindows CVMにログインする
3. 中国香港リージョンのWindows CVMで、実際のニーズに応じて、北米リージョンにあるCVMへのログイン方式を選択する：
北米リージョンのLinux CVMにログインします。
標準ログイン方式を利用してLinux CVM にログインする

リモートデスクトップを利用してLinux CVMにログインする
VNCを利用してLinux CVMにログインする
北米リージョンのWindows CVMにログインします。
RDPファイルを利用してWindows CVMにログインする
リモートデスクトップを利用してWindows CVMにログインする
VNCを利用してWindows CVMにログインする

ウェブサイトにアクセスできません

最終更新日：：2020-09-10 17:47:51

このドキュメントでは、ウェブサイトにアクセスできない問題を特定してトラブルシューティングする方法について説明します。

可能な原因

ネットワークの問題、ファイアウォールの設定、サーバーの負荷が高すぎるなどの原因によって、ウェブサイトにアクセスできなくなっています。

故障の処理

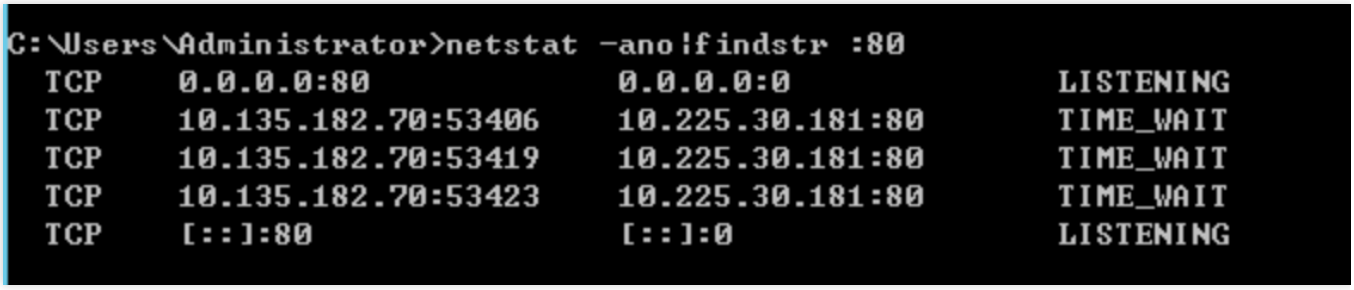
サーバー関連問題のトラブルシューティング

サーバーのシャットダウン、ハードウェアの故障、CPU/メモリ/帯域幅の使用率が高すぎるなどの原因によって、ウェブサイトにアクセスできなくなる可能性があります。そのため、順次にサーバーの稼働状態、CPU/メモリ/帯域幅の使用状況をトラブルシューティングすることをおすすめします。
1. CVMコンソール にログインし、インスタンスの管理ページでインスタンスが正常に実行しているかどうかを確認します。
正常に実行している場合は、ステップ2 を実行してください。
正常に実行していない場合は、CVMインスタンスをリスタートしてください。
2.
インスタンスのID/インスタンス名をクリックし、該当するインスタンスの詳細ページに入ります。

3. **モニタニング**タブを選択し、CPU/メモリ/帯域幅の使用状況を確認します。
CPU/メモリの使用率が高すぎる場合は、Windowsインスタンス：CPUとメモリの使用率が高すぎるためログイン不能 と Linuxインスタンス：CPUとメモリの使用率が高すぎるためログイン不能 を参照して調べてください。
帯域幅の使用率が高すぎる場合は、帯域幅の占有率が高すぎるためログイン不能を参照して調べてください。
CPU/メモリ/帯域幅の使用状況が正常である場合は、ステップ4 を実行してください。
4.
次のコマンドを実行し、Webサービスに対応するポートが正常に監視されているかを確認します。

説明：
HTTPサービスによく使われている80ポートを例として、操作について説明します。
Linuxインスタンス：`netstat -ntulp |grep 80` コマンドを実行します。

Windowsインスタンス：CMDコマンドラインツールを立ち上げ、`netstat -ano|findstr :80` コマンドを実行します。



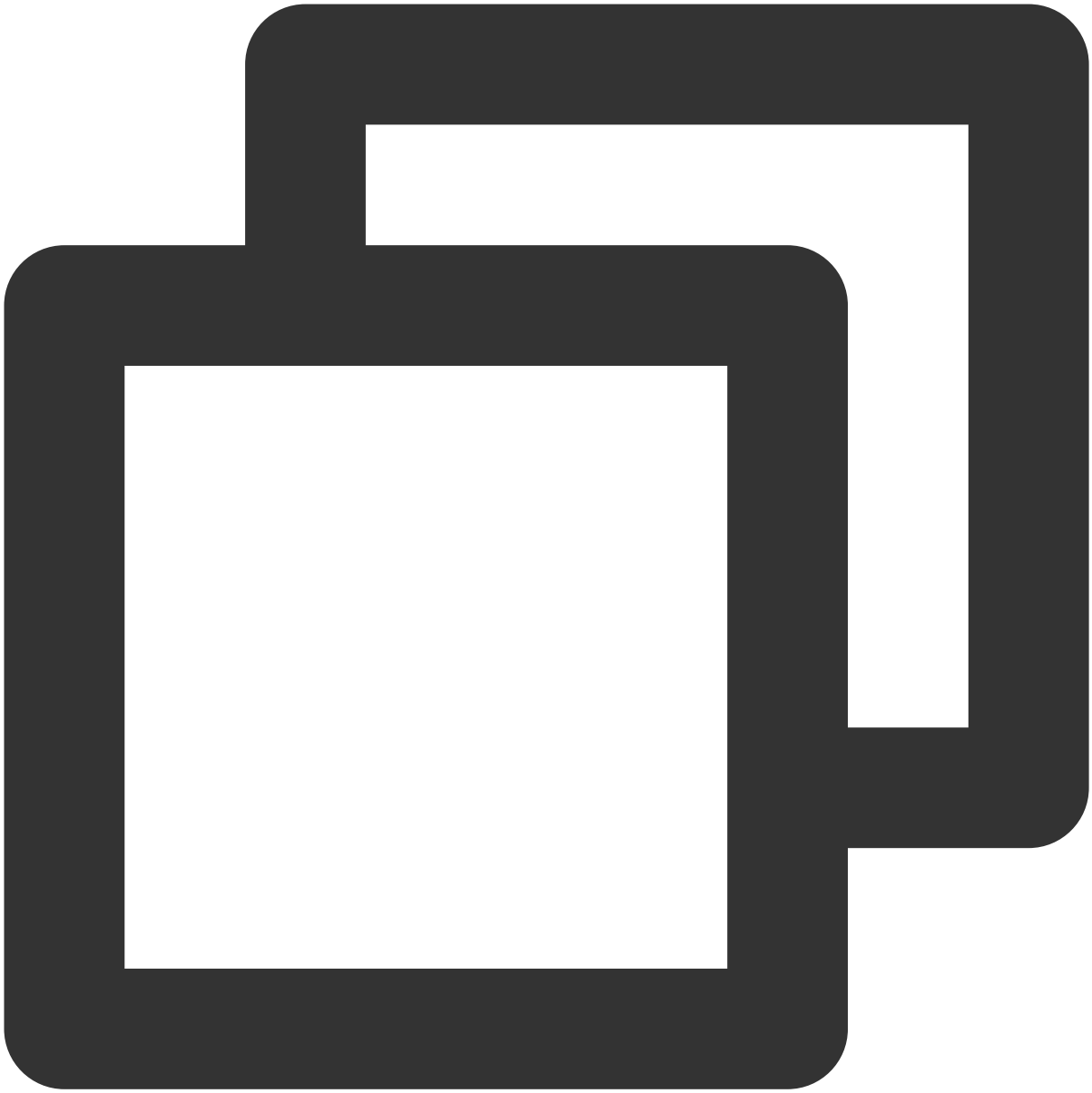
ポートが正常に監視されている場合は、ステップ5 を実行してください。
ポートが正常に監視されていない場合は、Webサービスプロセスが起動されているか、または正常に構成されているかを確認してください。

5.
Webサービスプロセスに対応するポートがパスできるかどうかと、ファイアウォールの設定を確認します。

Linuxインスタンス：iptablesが80ポートをインターネットにオープンしているかどうかを確認するために、`iptables -vnL` コマンドを実行します。
80ポートをインターネットにオープンしている場合は、ネットワーク関連問題のトラブルシューティング を実行してください。
80ポートをインターネットにオープンしていない場合は、`iptables -I INPUT 5 -p tcp --dport 80 -j ACCEPT` コマンドを実行して、80ポートをオープンしてください。
Windowsインスタンス：OSのインターフェースで、【スタート】>【コントロールパネル】>【ファイアウォール設定】をクリックし、Windowsファイアウォールが無効になっているかを確認します。
- 無効になっている場合は、ネットワーク関連問題のトラブルシューティング を実行してください。
- 無効になっていない場合は、ファイアウォール設定をオフにしてください。

ネットワーク関連問題のトラブルシューティング

ウェブサイトにアクセスできないのは、ネットワーク関連問題が原因である可能性もあります。次のコマンドを実行し、ネットワークにパケットロスや高いレイテンシーがあるかどうかを確認してください。



対象サーバーのパブリックIPをpingします

次のような結果が返された場合は、パケットロスや高いレイテンシーがあることを示しているため、MTRを使ってさらにトラブルシューティングしてください。具体的な操作は、CVMのネットディレーとパケットロス をご参照ください。

```
[redacted]MB0:~ chenhuiping$ ping 193.112.12.138
[redacted]2.12.138 (193.112.12.138): 56 data bytes
64 bytes from 193.112.12.138: icmp_seq=0 ttl=43 time=161.240 ms
64 bytes from 193.112.12.138: icmp_seq=1 ttl=43 time=161.996 ms
64 bytes from 193.112.12.138: icmp_seq=2 ttl=43 time=164.837 ms
64 bytes from 193.112.12.138: icmp_seq=3 ttl=43 time=215.650 ms
64 bytes from 193.112.12.138: icmp_seq=4 ttl=43 time=166.375 ms
64 bytes from 193.112.12.138: icmp_seq=5 ttl=43 time=160.576 ms
64 bytes from 193.112.12.138: icmp_seq=6 ttl=43 time=161.016 ms
64 bytes from 193.112.12.138: icmp_seq=7 ttl=43 time=164.129 ms
64 bytes from 193.112.12.138: icmp_seq=8 ttl=43 time=192.682 ms
64 bytes from 193.112.12.138: icmp_seq=9 ttl=43 time=163.376 ms
64 bytes from 193.112.12.138: icmp_seq=10 ttl=43 time=161.859 ms
^C
--- 193.112.12.138 ping statistics ---
11 packets transmitted, 11 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 160.576/170.340/215.650/16.765 ms
```

パケットロスや高いレイテンシーがない場合は、 セキュリティグループ設定の関連問題のトラブルシューティング を実行してください。。

キュリティグループ設定の関連問題のトラブルシューティング

セキュリティグループとは、関連するインスタンスのインバウンド・アウトバウンドトラフィックを制御できる仮想ファイアウォールのことです。そのルールは、プロトコルやポート、ポリシーなどを指定できます。Webプロセス関連のポートをインターネットにオープンしていない場合も、ウェブサイトにアクセスできなくなります。

1. CVMコンソール にログインし、「インスタンスリスト」ページでインスタンスのID/インスタンス名をクリックすることで、該当するインスタンスの詳細ページに入ります。

2. **セキュリティグループ**タブを選択し、Webプロセス関連のポートをインターネットにオープンしているかどうかと、バインドされているセキュリティグループと該当するセキュリティグループのインバウンド・アウトバウンドルールを確認します。

オープンしている場合は、 ドメイン名、ICP申告のトラブルシューティングと関係問題の解析 を実行してください。

オープンしていない場合は、Webプロセス関係のポートをインターネットにオープンするために、セキュリティグループの設定を変更してください。

ドメイン名、ICP申告のトラブルシューティングと関連問題の解析

サーバー関連問題、ネットワーク関連問題 と セキュリティグループ設定の関連問題 をトラブルシューティングしたあと、CVMのパブリックIPを使ってアクセスしてください。IPアドレスでアクセスでき、ドメイン名でアクセスできない場合は、ドメイン名のICP申告や解析の問題による可能性があります。

1. 中華人民共和国工業情報化部の規定によるところ、許可を受けず、ICP申告を取得せずにインターネット情報サービスに従事するウェブサイトは、その行為が違法的なものとなります。ウェブサイトの正常な永続稼働に影響しないために、ウェブサイトを立ち上げる場合は、まずはICP申告を行い、通信管理局からICP申告番号を取得してから、ウェブサイトをアクセスできるようにしてください。

ドメイン名がICP申告を取得していない場合は、 ドメイン名のICP申告 を実行してください。
Tencent Cloudのドメイン名サービスを使用している場合は、 ドメイン名管理コンソール にログインして該当するドメイン名を確認できます。
ドメイン名がICP申告を取得している場合は、ステップ2 を実行してください。
2.
解析発効についてを参照し、関連する問題を解析し、トラブルシューティングします。

ウェブサイトにアクセスできないという問題が解決された場合、タスクは終了します。
ウェブサイトにアクセスできないという問題が解決されていない場合は、 作業依頼書の提出でフィードバックしてください。

ウェブサイトのアクセスラグ

最終更新日：：2020-03-03 19:09:30

問題説明

ウェブサイトにアクセスする際に、ネット渋滞が発生し、スピードが低下しています。

問題解析

HTTPリクエストの全プロセスは、ドメイン名の解析、TCP接続の確立、リクエストの送信、サーバーによるリクエストの受信・処理・処理結果の返し、ブラウザによるHTMLコードの解析・ほかのリソースへのリクエスト、およびページのレンダリング・表示を含んでいます。そのうち、HTTPリクエストはユーザーのローカルクライアント、クライアントとサーバー間のネットワークノード、そしてサーバーを通過しています。この三つの段階のいずれかに問題が発生した場合、ウェブサイトにアクセスする際のスピードが低下する可能性があります。

ソリューション

ロカールクライアントの確認

1. ロカールクライアントで 華佗診断分析システム にアクセスし、ローカルから各ドメイン名にアクセスするスピードをテストします。
2. テスト結果に基づいて、ロカールネットワークに問題があるかどうかを確認します。
例えば、テスト結果が下図に示すようになっている場合は、

The following are the test results of Tencent's domain name.	
inews.qq.com	Normal network , 194 milliseconds delay
www.qq.com	Normal network , 128 milliseconds delay
3g.qq.com	Normal network , 140 milliseconds delay
mail.qq.com	Normal network , 99 milliseconds delay
user.qzone.qq.com	Normal network , 98 milliseconds delay
r.qzone.qq.com	Normal network , 203 milliseconds delay
w.qzone.qq.com	Normal network , 188 milliseconds delay
ptlogin2.qq.com	Normal network , 96 milliseconds delay
check.ptlogin2.qq.com	Normal network , 189 milliseconds delay
ui.ptlogin2.qq.com	Normal network , 91 milliseconds delay
i.mail.qq.com	Normal network , 129 milliseconds delay
v.qq.com	Normal network , 129 milliseconds delay
The following are the test results of other's domain name.	
c.3g.163.com	Normal network , 143 milliseconds delay
weibo.com	Normal network , 211 milliseconds delay
www.baidu.com	Normal network , 94 milliseconds delay
www.sina.com.cn	Normal network , 138 milliseconds delay
www.taobao.com	Normal network , 136 milliseconds delay

結果から各ドメイン名にアクセスする時のレイテンシーを確認し、ネットワークが正常であるかどうかを確認できます。
正常でない場合は、問題を確定して解決するように、ネットワークサービスのプロバイダーに連絡ください。
正常である場合は、ネットワークリンクの確認 を実行してください。

ネットワークリンクの確認

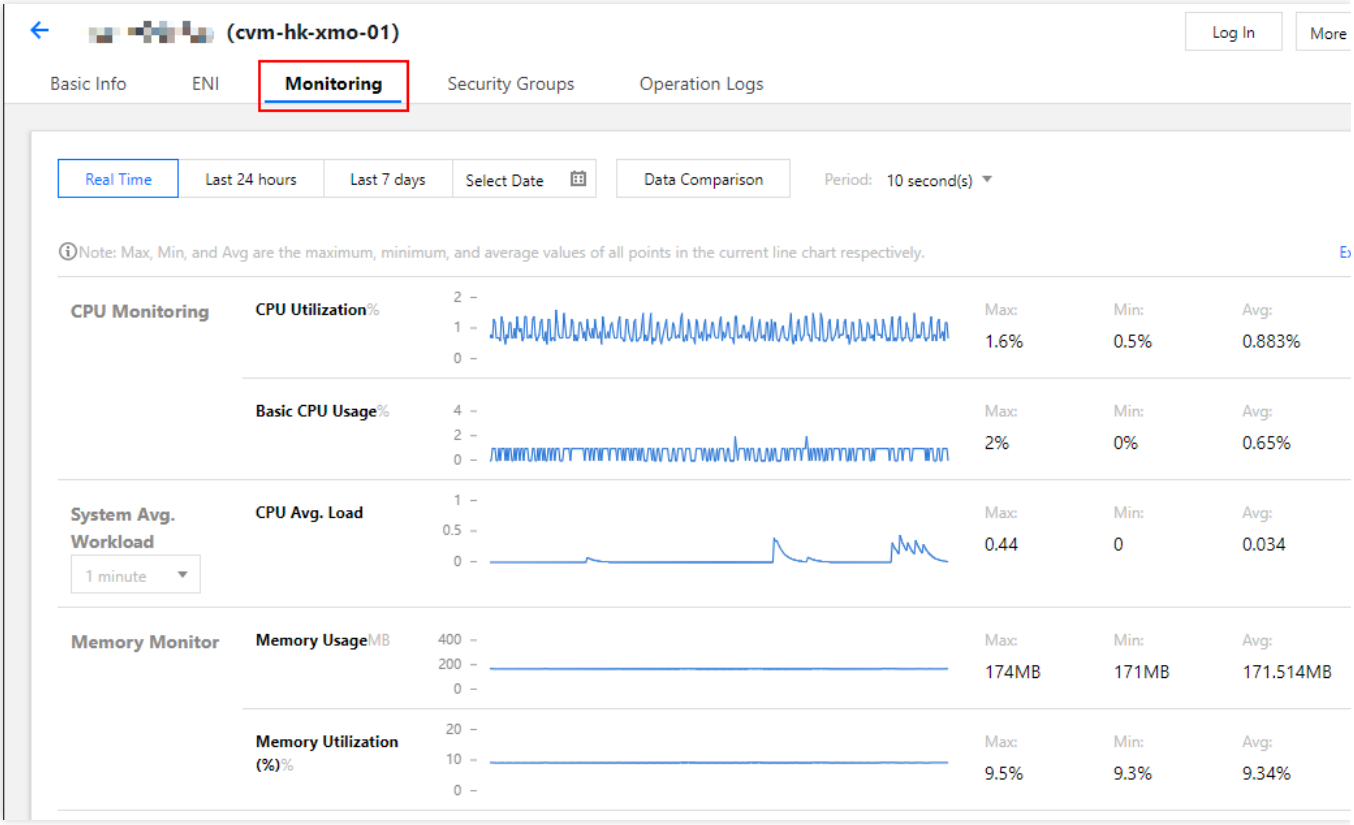
1. ローカルクライアントでサーバーのパブリックIPをpingすることで、パケットロスや高いレイテンシーがあるかどうかを確認してください。

パケットロスや高いレイテンシーがある場合は、MTRを使って診断してください。具体的な操作は、サーバーのネットワークディレーとパケットロスの処理 をご参照ください。
パケットロスや高いレイテンシーがない場合は、ステップ2を実行してください。
2.
`dig/nslookup` コマンドを使ってDNSの解析を確認し、DNS解析による問題であるかどうかをトラブルシューティングします。

直接にパブリックIPを使って該当のページにアクセスし、ウェブサイトにアクセスする際のネット渋滞とスピード低下の原因がDNSにあるかどうかを調べることもできます。
そうである場合は、DNS解析を確認してください。具体的な操作は、 解析発効についてをご参照ください。
そうでない場合は、 サーバーの確認 を実行してください。

サーバーの確認

1. CVMコンソール にログインします。
2. 確認するインスタンスのID/インスタンス名を選択し、該当するインスタンスの詳細ページに入ります。
3. 下図に示すように、インスタンスの詳細ページで【モニタニング】タブを選び、インスタンスのリソース利用状況を確認します。



CPU/メモリの使用率が高すぎる場合は、Windowsインスタンス：CPUとメモリの使用率が高すぎるためログイン不能と Linuxインスタンス：CPUとメモリの使用率が高すぎるためログイン不能 を参照して調べてください。

帯域幅の使用率が高すぎる場合は、帯域幅の占有率が高すぎるためログイン不能]を参照して調べてください。
インスタンスのリソース利用が正常である場合は、 ほかの問題の確認 を実行してください。

ほかの問題の確認

インスタンスのリソース利用状況に基づいて、サーバー負荷によるリソース消費の増加であるかどうかを判断します。
そうである場合は、サービスプログラムを最適化するか、サーバー構成のアップデートを行うことをおすすめします。新しいサーバーを購入して、既存のサーバーの負荷を分担させることもできます。
そうでない場合は、ログファイルを確認し、問題を特定してから指向性のある最適化を実行することをおすすめします。

ネットワークカードマルチキュー設定エラーの場合

最終更新日：：2022-05-06 11:46:50

故障について

CVMネットワークカードマルチキュー設定でエラーが発生します。

考えられる原因

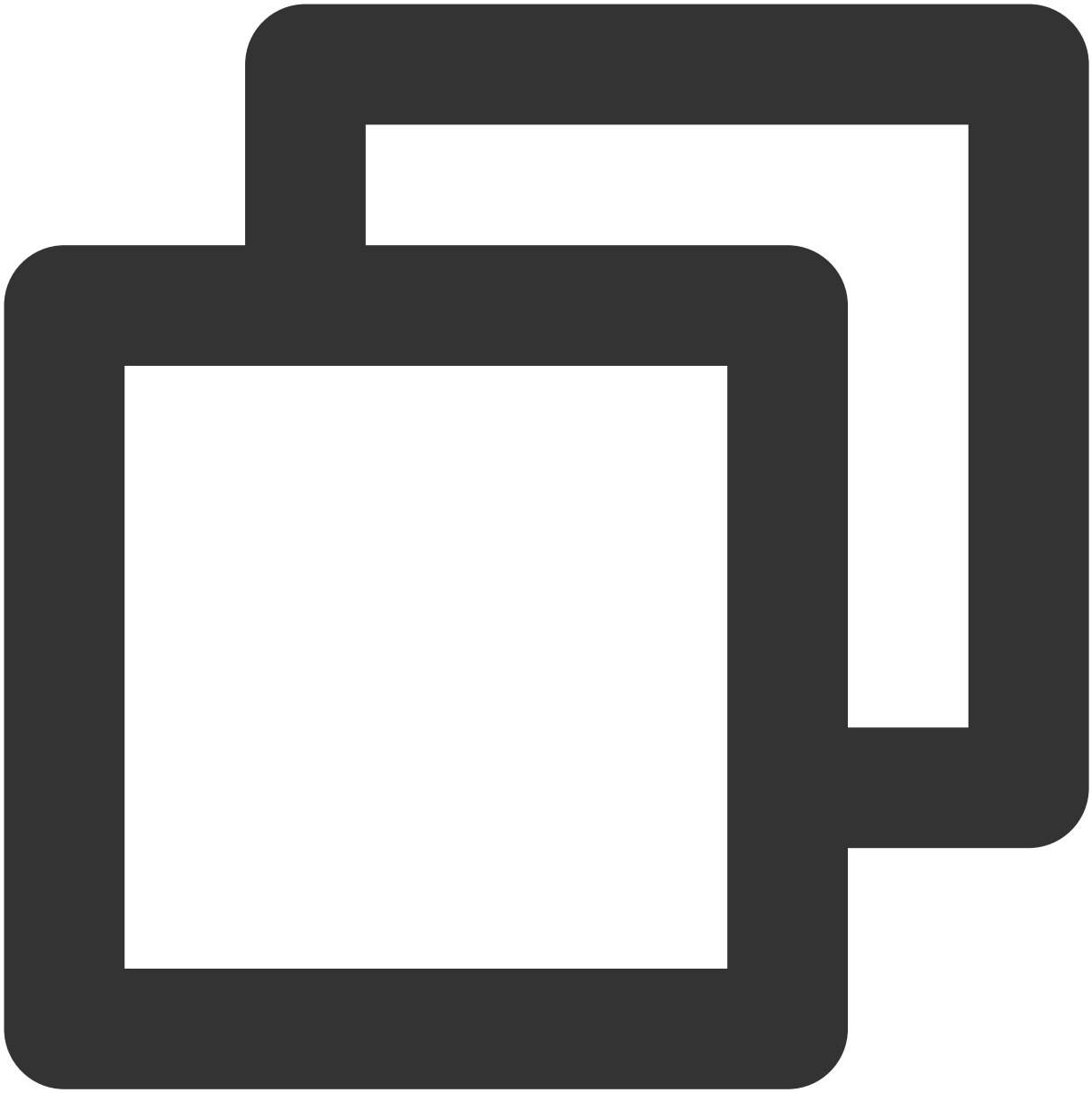
CVMはネットワークカードマルチキューをデフォルトで設定します。この方式ではネットワークカードを切断してそれぞれのCPUに配置し、ネットワーク処理性能を向上させることができます。人為的な変更があった場合、ネットワークカードマルチキュー設定でエラーが発生する可能性があります。

ソリューション

処理手順 を参照し、ENIキューの個数を修正してください。

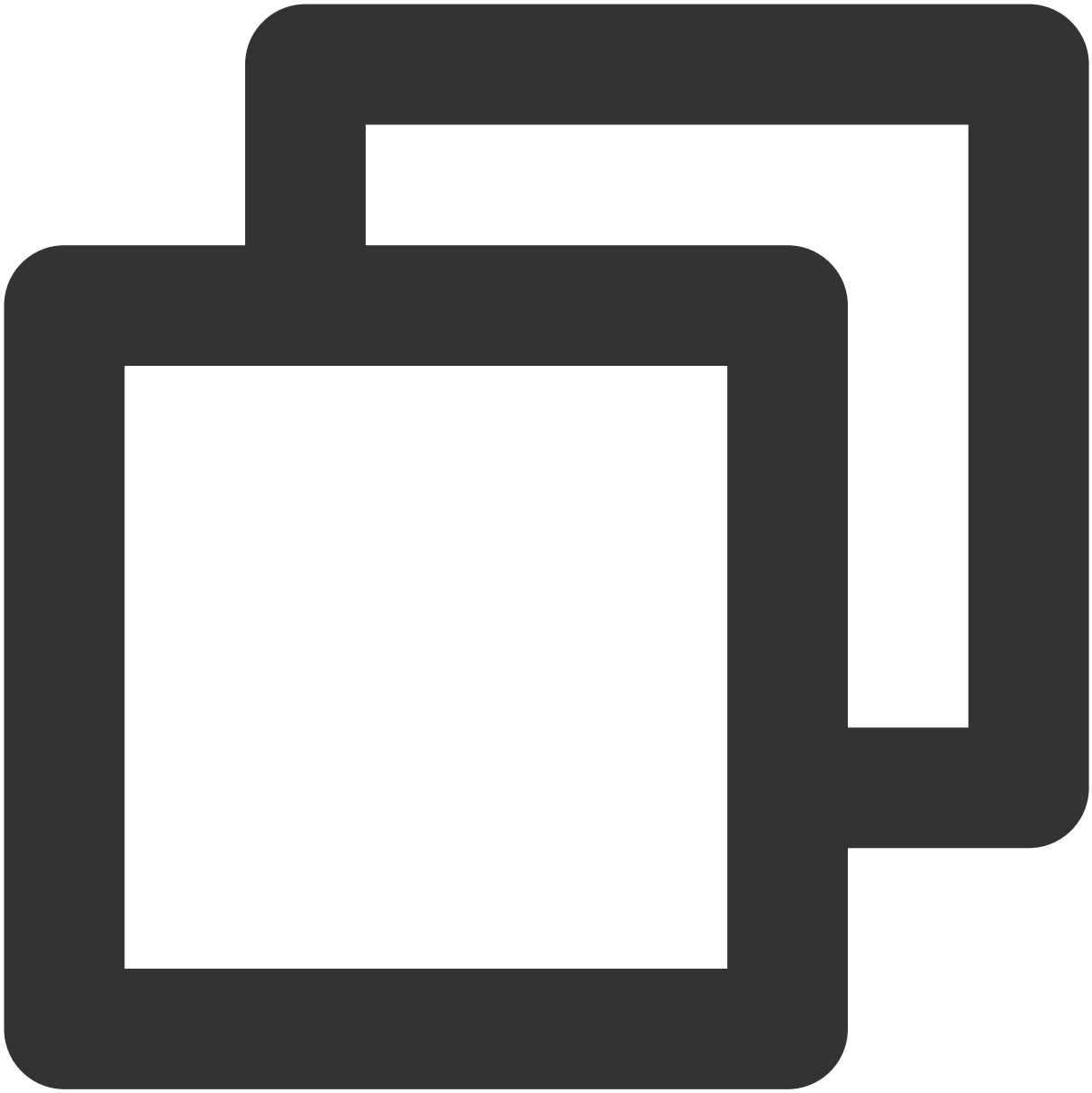
処理手順

以下の手順におけるCVMのデフォルトのメインネットワークカードは `eth0` で、ENIキューの個数は2です。
1. 以下のコマンドを実行し、現在のENIキューの個数を確認します。



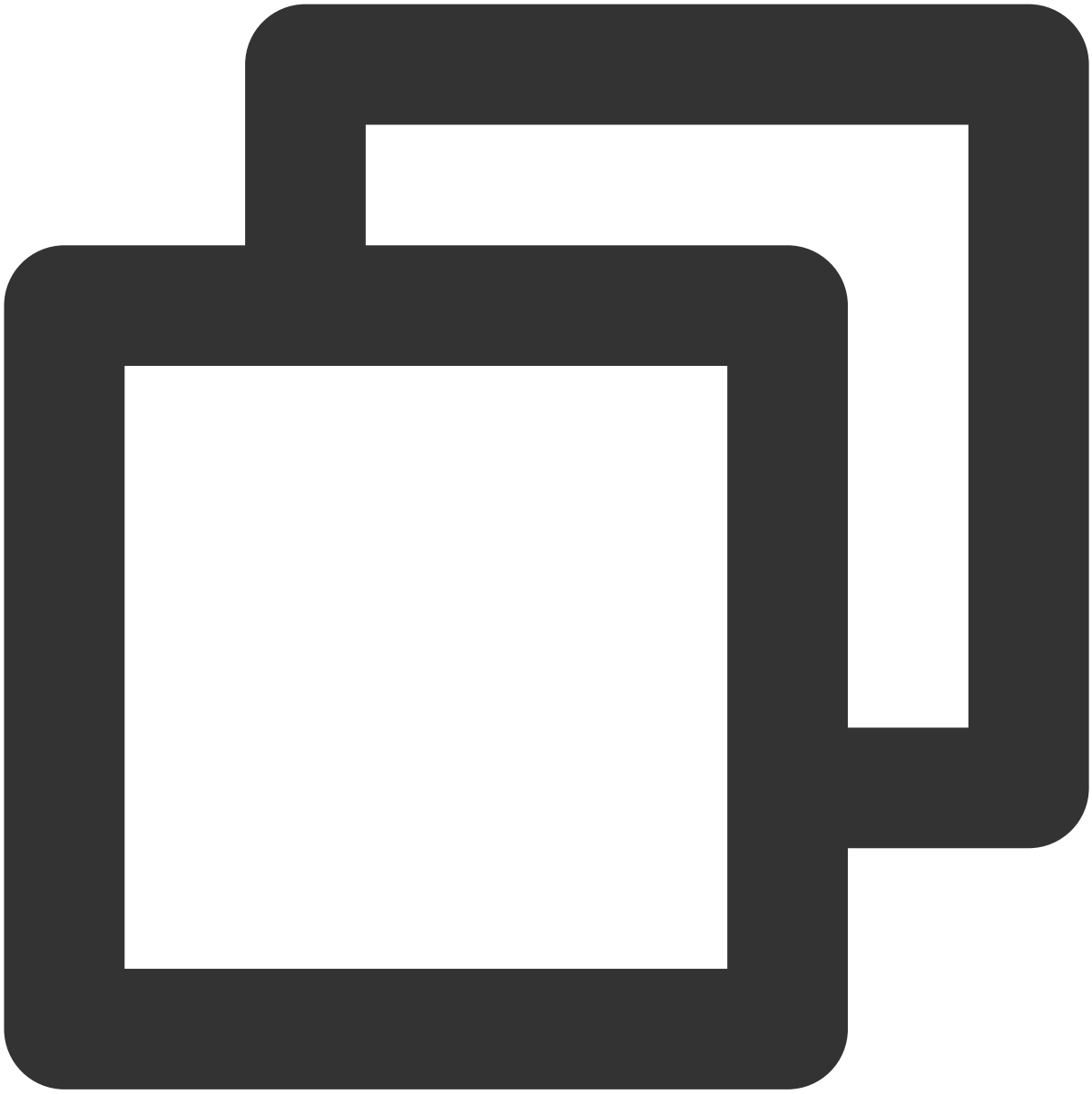
```
ethtool -l eth0
```

以下の結果がリターンされ、現在のキューの個数がENIキューの最大個数より小さいことが示されます。設定が適切でない場合、修正する必要があります。



```
Channel parameters for eth0:
Pre-set maximums:
RX:             0
TX:             0
Other:          0
Combined:       2          ### サーバーがサポートするENIキューの最大個数
Current hardware settings:
RX:             0
TX:             0
Other:          0
Combined:       1         ###現在設定しているENIキューの個数
```

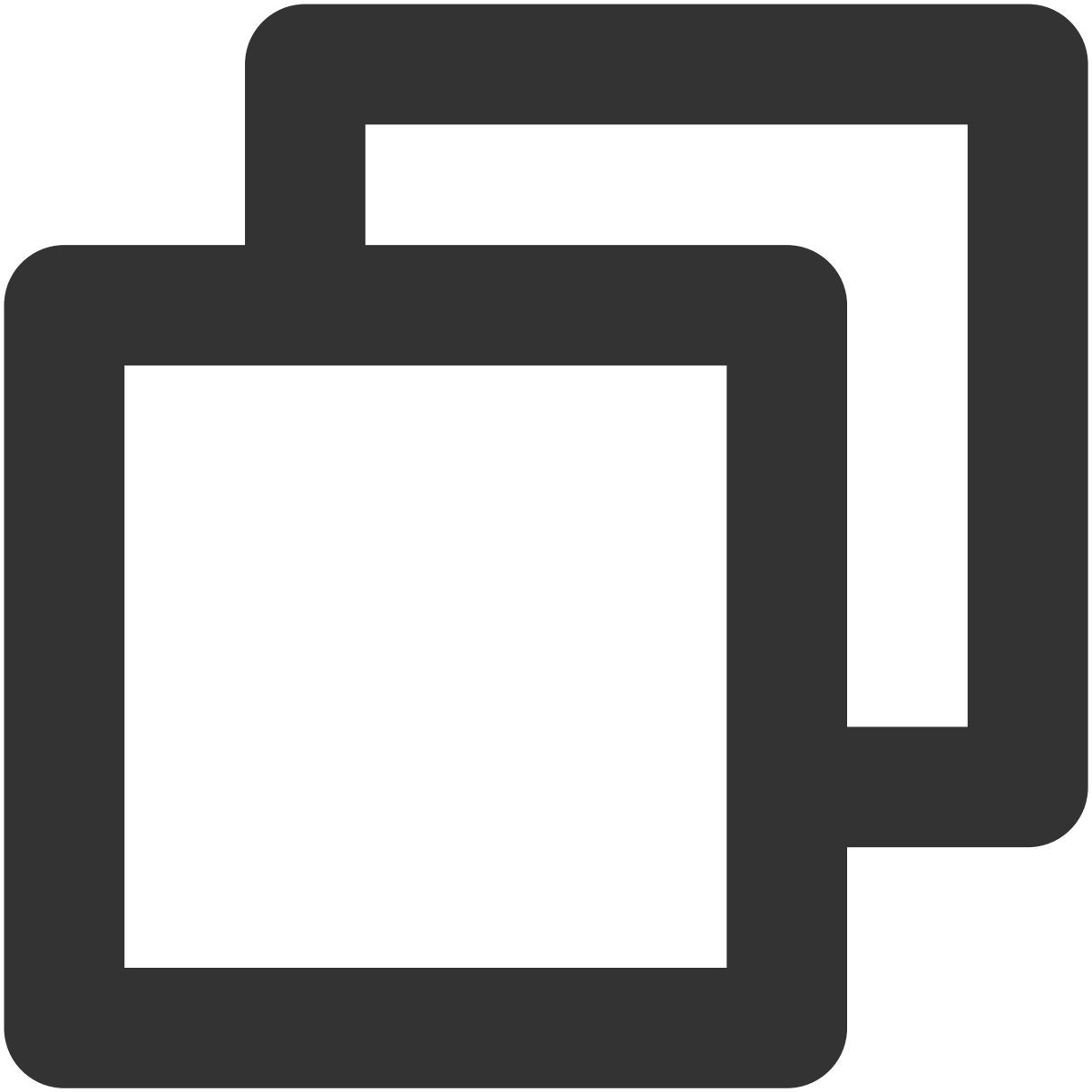
2. 以下のコマンドを実行し、現在のENIキューの個数を設定します。



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

コマンドでキュー個数を2に設定します。実際の状況に応じて調整することができ、設定値はサーバーがサポートするENIキューの最大個数です。

3. 以下のコマンドを実行し、現在のENIキューの個数設定をチェックします。



```
ethtool -l eth
```

サーバーがサポートするENIキューの最大個数が現在設定しているENIキューの個数と同じであれば、設定は成功です。

CVMネットワークディレーとパケットロス

最終更新日：：2022-05-06 14:57:08

問題の説明

ローカルでCVMにアクセスするか、あるいはCVMで他のネットワークリソースにアクセスする時にインターネットのラグが発生しました。 `ping` コマンドを使用して、パケットロスや高いレイテンシーを発見しました。

問題の分析

バックボーンリンクの輻輳、リンクノードの故障、サーバー負荷が高い、システムの設置問題などの原因により、パケットロスや高いレイテンシーを引き起こす可能性があります。CVM自体のの原因を除外した後、MTRを使用してより詳細な診断を行うことができます。
MTRはネットワーク診断ツールであり、このツールで診断されたレポートを通じて、ネットワーク問題が発生する原因を確認することができます。

対処方法

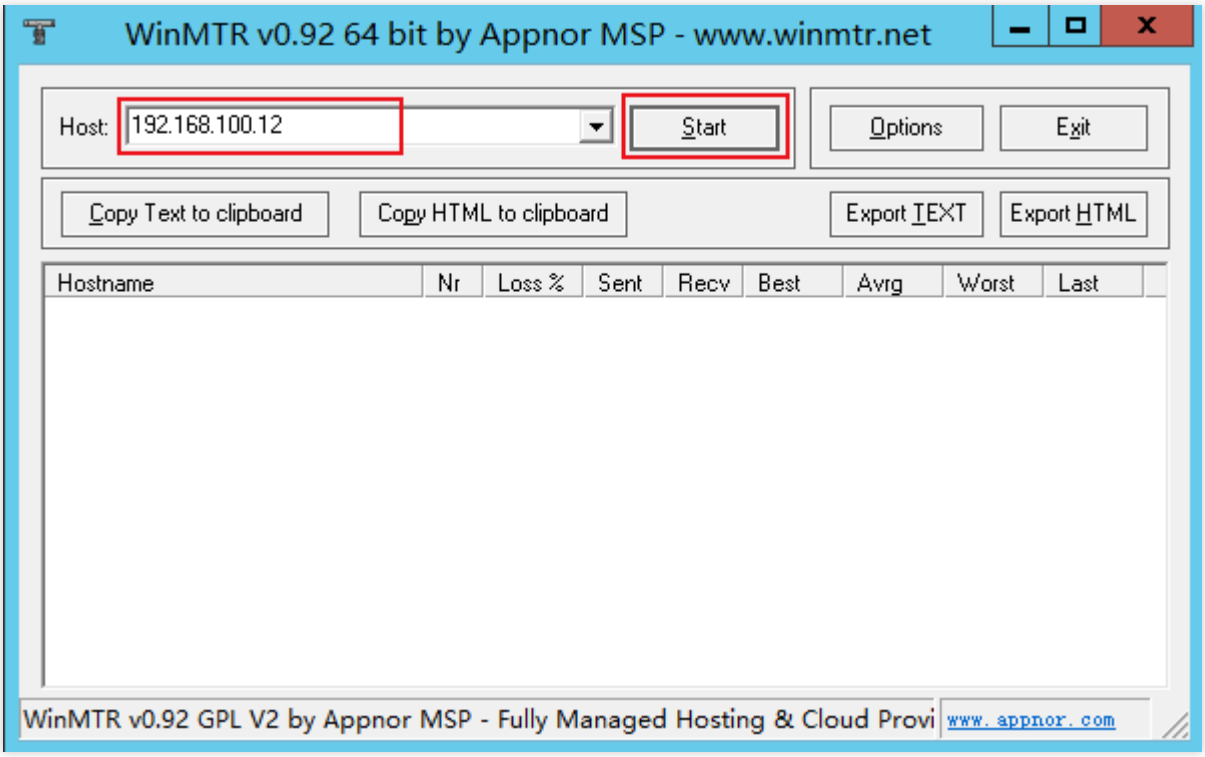
ここではLinuxとWindows CVMを例に取り、MTRの使用方法およびMTRのレポート結果に対する分析方法について説明します。
説明：
ローカルまたはCVMでPingが無効になっている場合、MTRは結果を返しません。
MTRを実行しているホストOSに応じて、MTRの紹介と使用方法をご参照てください。
WinMTRの説明および使用（Windows OS）
MTRの説明および使用（Linux OS）
WinMTR：はWindows に適応する無料なインターネット診断ツールであり、Pingとtracertのすべての機能を統合し、グラフィカルインターフェースがあり、各ノードの応答時間とパケットロスの状況を確認することができます。

WinMTRをインストールする

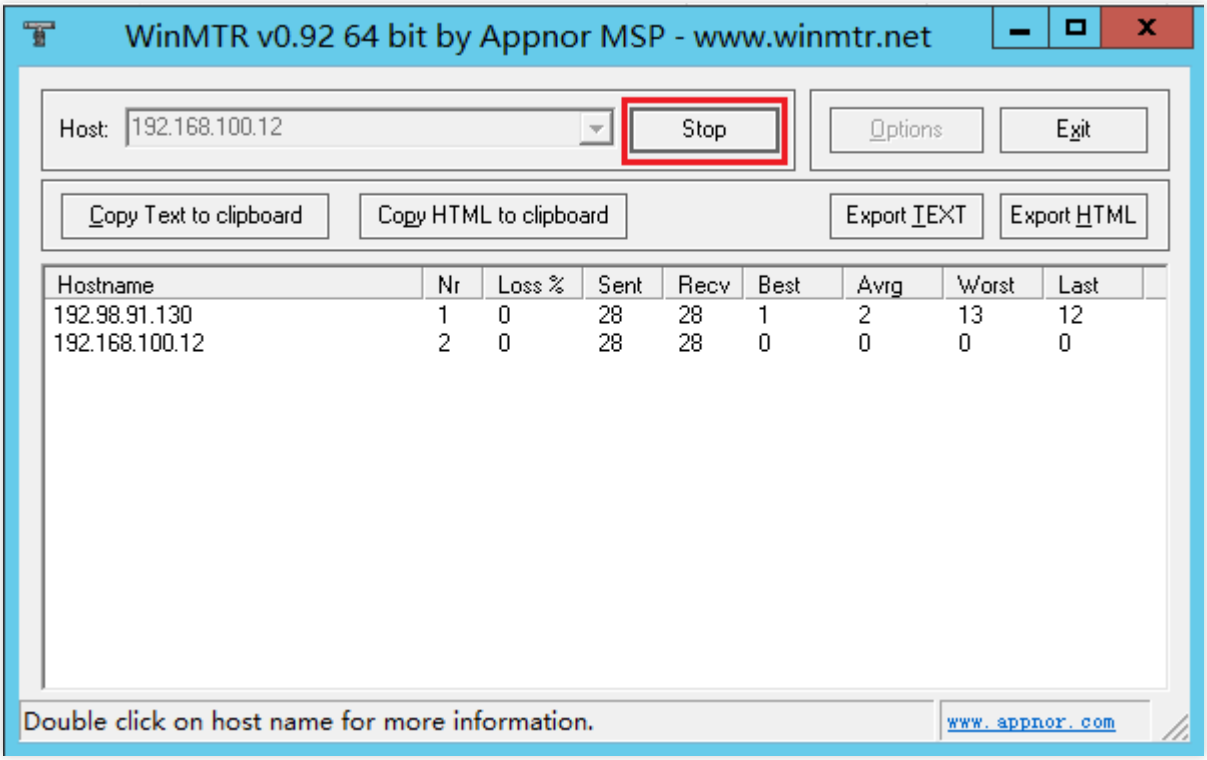
1. Windows CVMにログインします。
2. OSインターフェースで、ブラウザーで公式Webサイト（または合法的なチャネル）にアクセスし、対応するOSタイプのWinMTRインストールパッケージをダウンロードする。
3. WinMTRインストールパッケージを解凍/圧縮する。

WinMTRの使用

1. WinMTR.exeをダブルクリックして、WinMTRツールを開く。
2. 下図に示すように、WinMTRウィンドウのHostフィールドに、対象のサーバーIPまたはドメイン名を入力し、**Start**をクリックします。



3. 下図に示すように、実際の状況に応じて、WinMTRが一定時間実行されるのを待って、**Stop**をクリックし、テストを終了します。



テスト結果の情報は以下の通り：

Hostname：宛先サーバーに経由した各ホストIPまたは名称です。

Nr：経由したノード数です。

Loss%：対応するノードのパケットロス率です。

Sent：送信したデータパッケージ数です。

Recv：受信した応答数です。

Best：最短の応答時間です。

Avrg：平均応答時間です。

Worst：最長の応答時間です。

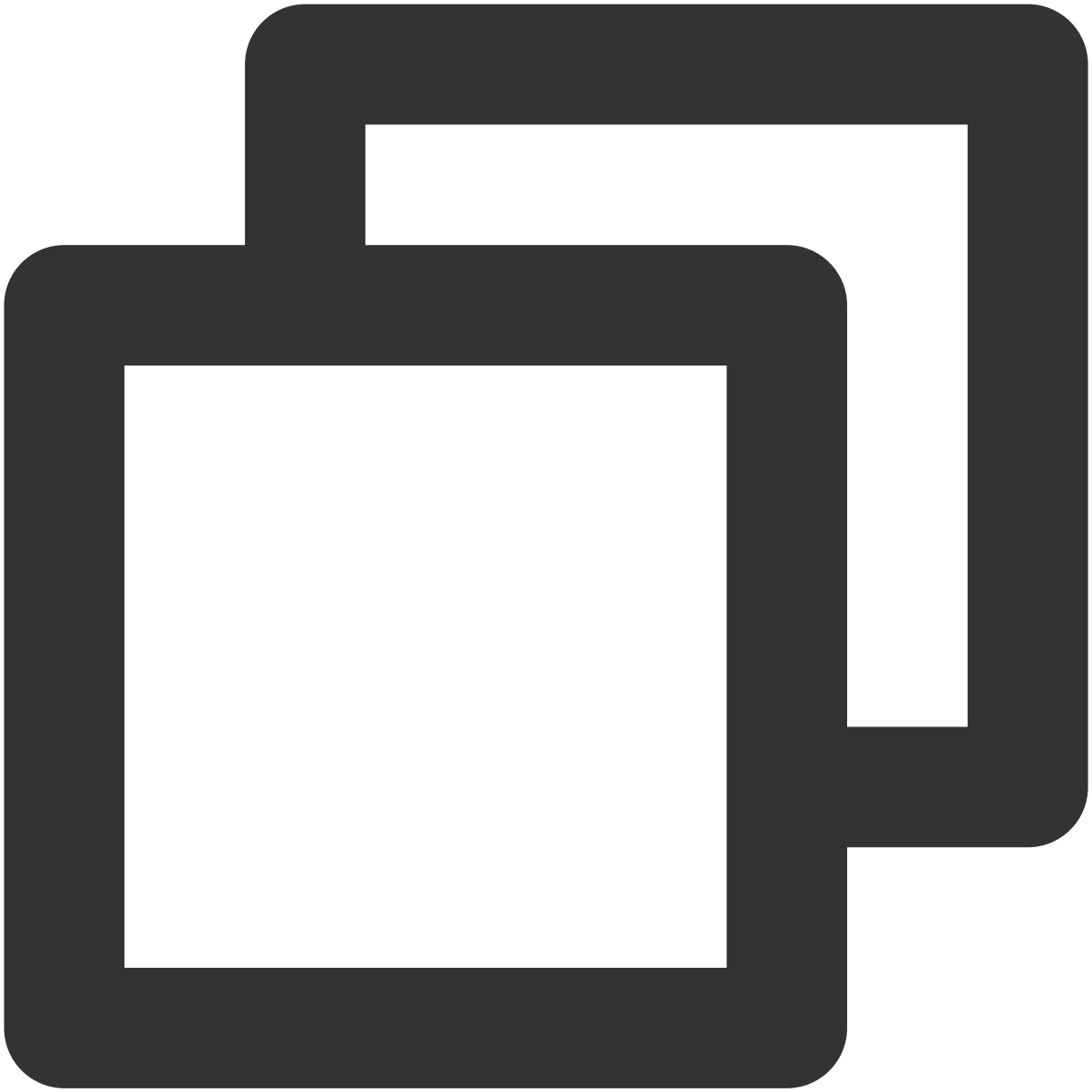
Last：直近の応答時間です。

MTR：Linuxプラットフォームでインターネットを診断するツールで、Ping、traceroute、nslookup の機能を承継して、デフォルトでICMP パッケージを利用して二つのノードの間のネットワーク接続状態をテストします。

MTRをインストールする

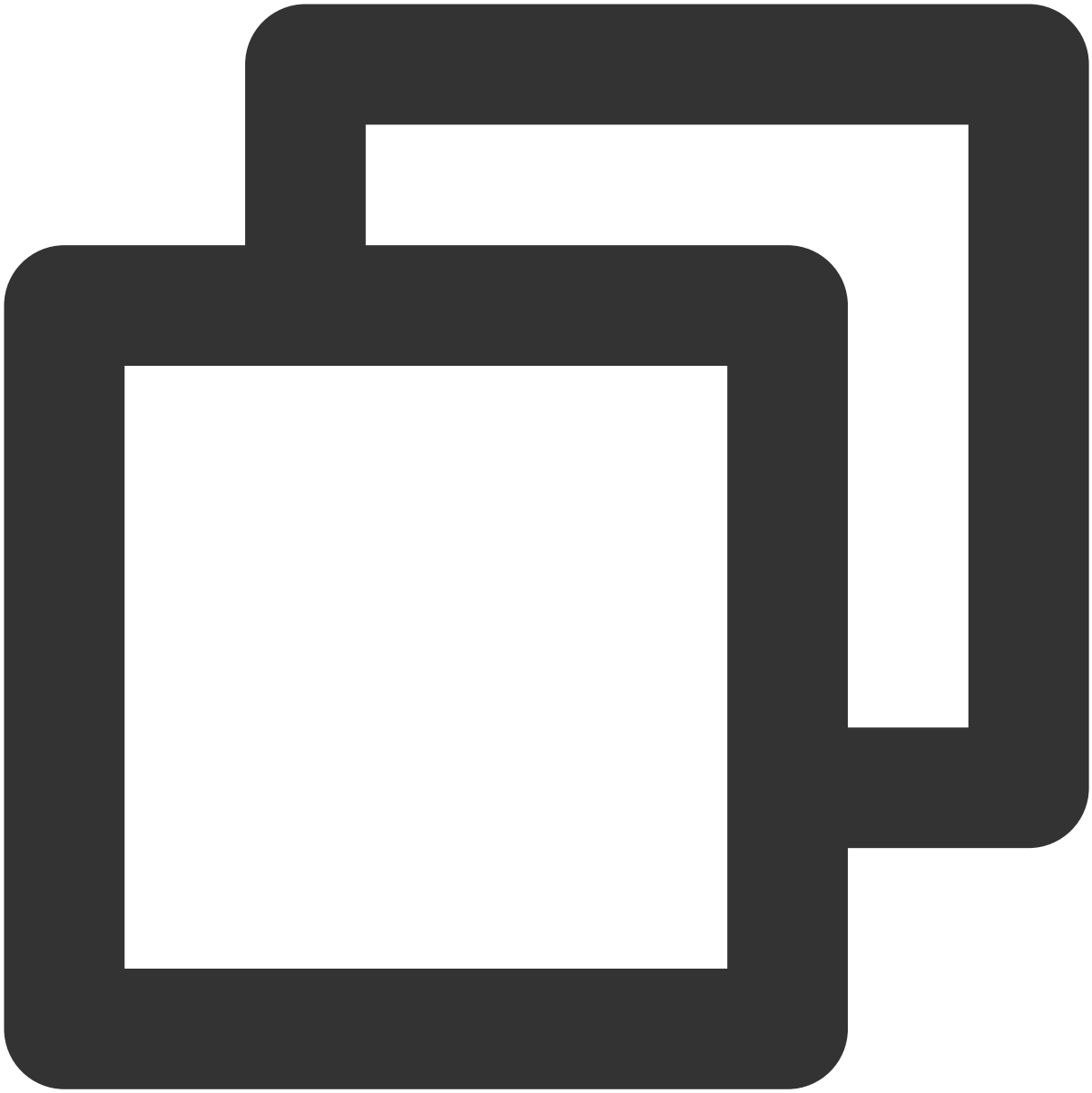
既存のLinux が発行したバージョンは事前にMTRをインストールしました。Linux CVMはMTRをインストールしていない場合は、以下のようなコマンドを実行してインストールします：

CentOS OS：



```
yum install mtr
```

Ubuntu OS：



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

MTR 相関パラメータの説明

-h/--help：ヘルプメニューを表示する

-v/--version：MTR のバージョン情報を表示する

-r/--report：結果はレポートとして出力する

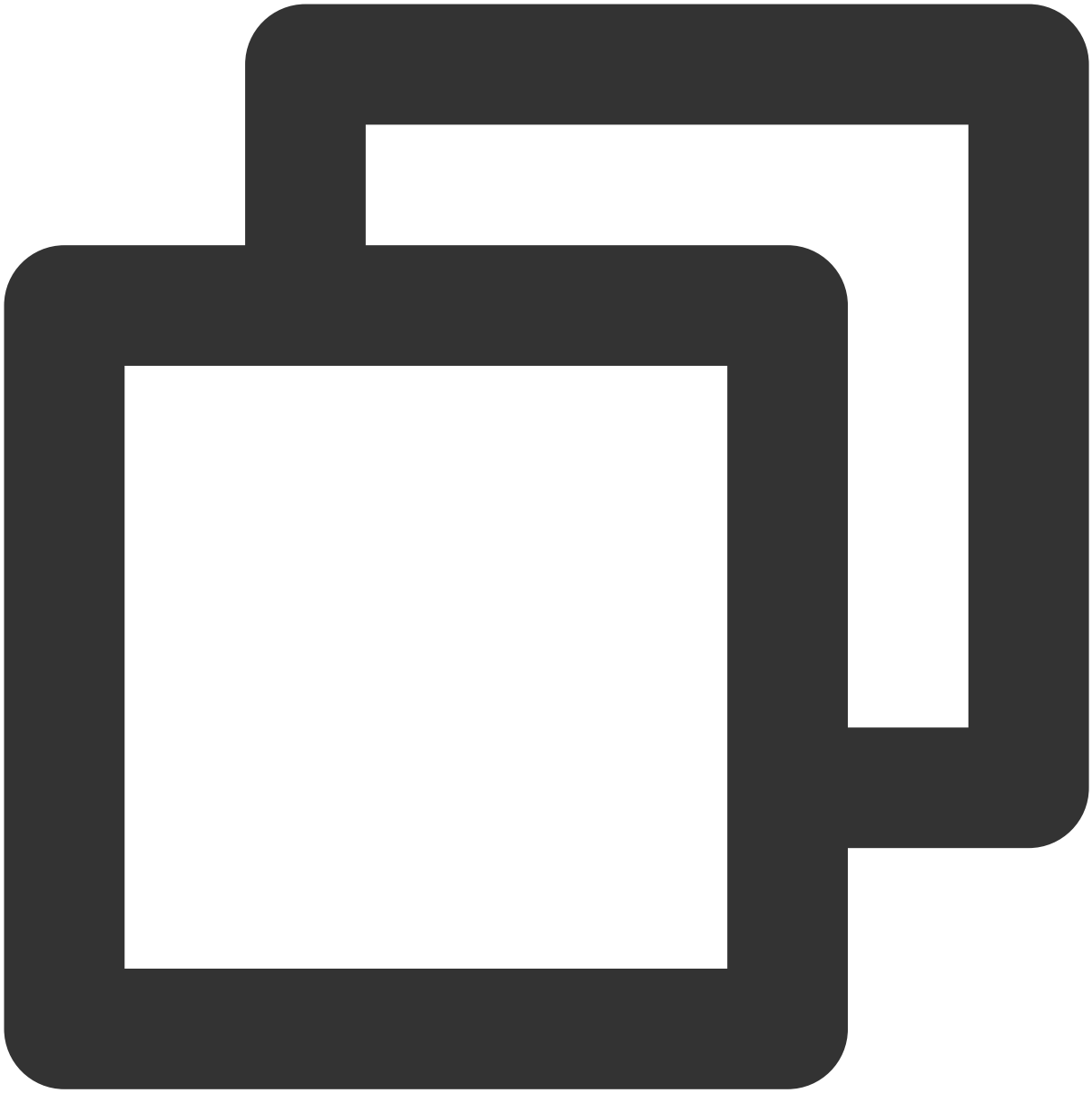
-p/--split：**--report**とは対照的に、各追跡の結果を個別にリスト表示する

-c/--report-cycles：毎秒で発送するデータパッケージの数を設置し、デフォルトでは10となる

-s/--psize：パッケージのサイズを設置する
-n/--no-dns：IPアドレスに対してドメイン名の解析を行わない
-a/--address：ユーザーはデータパッケージの発送IPアドレスを設定します、重要ユーザーが単一のホスト上に複数のIPアドレスをもつケース
-4：IPv4
-6：IPv6

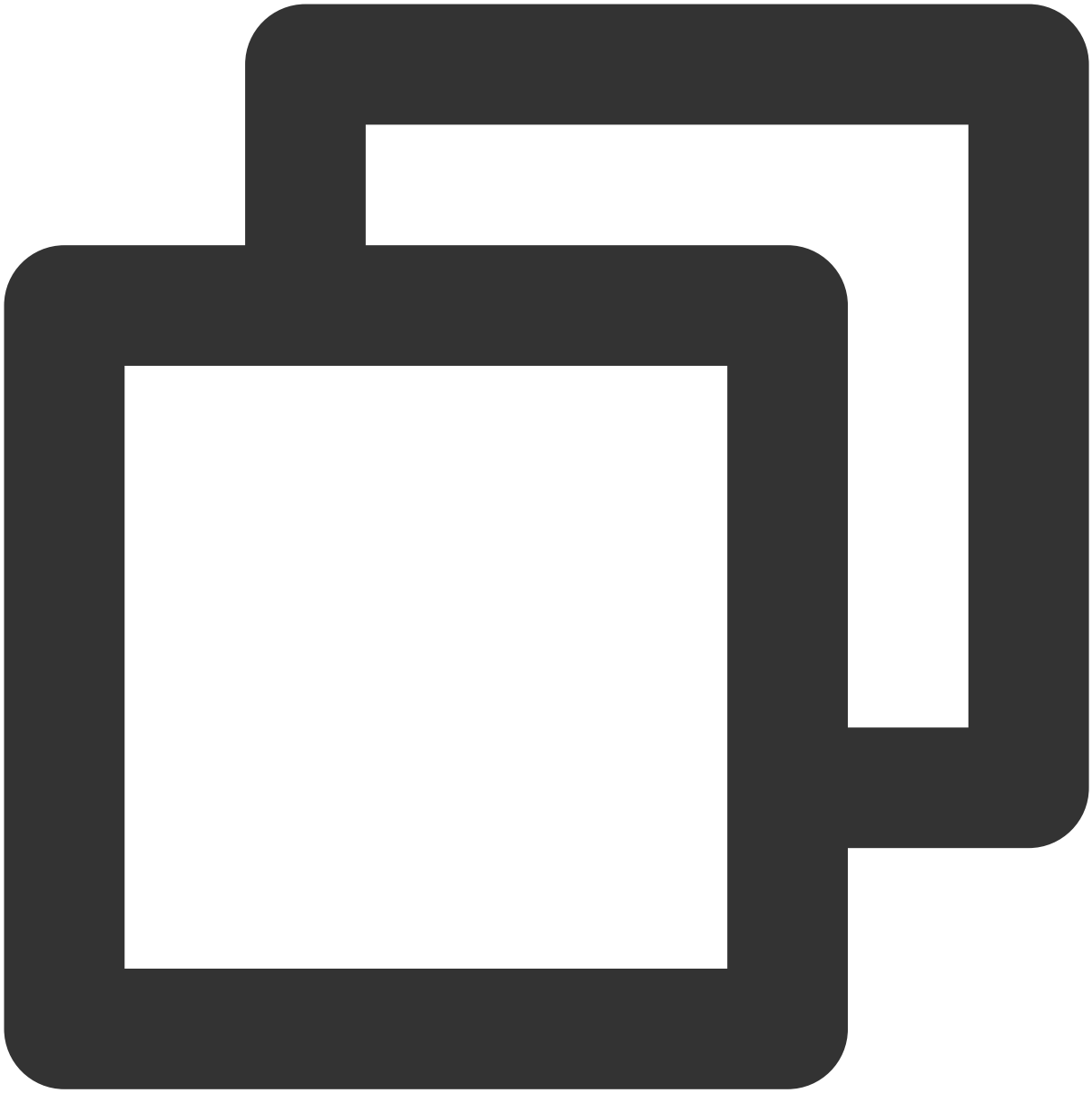
ユースケース

ローカルでIPが119.28.98.39のサーバーを例とします。
以下のコマンドを実行して、レポートとしてのMTRの診断結果を出力します。



```
mtr 119.28.98.39 --report
```

次のような情報が返されます：



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

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

主な出力情報は以下のように：

HOST：ノードのIP アドレスまたはドメイン名です。

Loss%：パケットロス率です。

Snt：毎秒で発送したデータパッケージの数です。

Last：直近の応答時間です。

Avg：平均応答時間です。

Best：最短の応答時間です。

Wrst：最長の応答時間です。

StDev：の標準偏差、偏差値は大きいほど、各データパッケージが該当ノードでの応答時間の差が大きくなる。

レポートの結果分析と処理

説明：

ネットワーク状況の非対称性によってローカルからサーバーへのネットワークの問題が発生した場合は、双方向のMTR データ（ローカルからCVMおよびCVMからローカル）を収集することをお勧めします。

1. レポートの結果により、宛先サーバーIPはパケットロスが発生したかどうかを確認する。

宛先サーバーはパケットロスが発生していない場合は、ネットワークの接続は正常です。

宛先サーバーはパケットロスが発生した場合は、ステップ2 を実行してください。

2. レポート結果を確認し、最初にパケットロスが発生したノードを特定します。

宛先サーバーでパケットロスが発生した場合は、原因は宛先サーバーのネットワークの設定が不適切であることにより、宛先サーバーのファイアウォールの設定を確認してください。

パケットロスが最初の三ジャンプで発生した場合は、ローカルキャリアのネットワークの問題であるため、その時は他のアドレスにアクセスする時も同じ問題があるかどうかをチェックしてください。同じ問題が存在する場合は、キャリアに問い合わせください。

パケットロスが頻繁に発生し、確実にネットワークが不安定である場合は、チケットを提出 して問い合わせを行い、エンジニアが特定し易いように、テストのスクリーンキャプチャを添付してください。

CVMネットワークアクセスパケット損失

最終更新日：：2022-05-06 11:46:50

このテキストでは、主にCVMアクセスパケット損失の問題を引き起こす可能性のある主な理由と、対応するトラブルシューティングと対処方法を紹介します。

考えられる原因

CVMネットワークアクセスパケット損失の問題について考えられる理由は次のとおりです：
速度制限のトリガーによるTCP パケット損失
速度制限のトリガーによるUDP パケット損失
ソフトウェア割り込みのトリガーによるパケット損失
UDP 送信バッファがフル
UDP 受信バッファがフル
TCP すべての接続キューがフル
TCP リクエストのオーバーフロー
接続数が上限に到達
iptables policy 関連ルールの設定

前提条件

問題を特定し対処する前にインスタンスにログインする必要があります。詳細は、 Linuxインスタンスにログイン および Windowsインスタンスにログイン をご参照ください。

トラブルシューティング

速度制限のトリガーによるTCP パケット損失

CVMインスタンスには複数の仕様があり、仕様ごとにネットワーク性能が異なります。インスタンスの帯域幅やパケットがインスタンス仕様に対応する基準を超過した場合、プラットフォーム側の速度制限がトリガーされ、パケット損失を引き起こすことがあります。トラブルシューティングと対処手順は次のとおりです：
1. インスタンスの帯域幅とパケットを確認します。
Linux インスタンスでは、 `sar -n DEV 2` コマンドを実行して帯域幅とパケットを確認することができます。 `rxpck/s` と `txpck/s` 指標は送受信パケット、 `rxkB/s` と `txkB/s` 指標は送受信帯域幅です。

2. 取得した帯域幅とパケットデータを使用してインスタンス仕様を比較し、インスタンス仕様の性能ボトルネックに達していないかどうかを確認します。
ボトルネックに達している場合は、インスタンス仕様をアップグレードするか、または業務量を調整する必要があります。
インスタンス仕様の性能ボトルネックに達していない場合は、チケットを提出し、問題をさらに特定し対処することができます。

速度制限のトリガーによるUDP パケット損失

速度制限のトリガーによるTCP パケット損失手順を参考に、インスタンス仕様の性能ボトルネックによるパケット損失かどうかを判断します。
ボトルネックに達している場合は、インスタンス仕様をアップグレードするか、または業務量を調整する必要があります。
インスタンス仕様の性能ボトルネックに達していない場合は、プラットフォームのDNSリクエストに対する追加的な頻度制限が原因である可能性があります。インスタンス全体の帯域幅やパケットがインスタンス仕様の性能ボトルネックに達している場合は、DNSリクエストの速度制限がトリガーされ、UDPパケット損失が発生する可能性があります。チケットを提出して処理を更に特定することができます。

ソフトウェア割り込みのトリガーによるパケット損失

オペレーティングシステムが `/proc/net/softnet_stat` の二列目のカウント値の増加を検出した場合は、「ソフトウェア割り込みによるパケット損失」と判断することができます。インスタンスがソフトウェアの割り込みをトリガーしパケット損失が引き起こされた場合は、次の手順でトラブルシューティングを行い、対処することができます：
RPSが有効化されているかどうかを確認する：
有効化されている場合は、カーネルパラメータ `net.core.netdev_max_backlog` が小さすぎるとパケット損失が引き起こされることから、大きくする必要があります。カーネルパラメータの詳細情報については、Linuxインスタンスで一般的に使用されるカーネルパラメータの説明をご参照ください。
有効化されていない場合は、CPU シングルコアのソフトウェア割り込み負荷が高いことによって、データが速やかに送受信できない事象が引き起こされていないかどうかを確認します。もしそうであれば：
RPSの有効化を選択し、ソフトウェア割り込みの割り当てをより均衡にします。
業務プロセスがソフトウェア割り込みの不均衡を引き起こしているかどうかを確認します。

UDP 送信バッファがフル

インスタンスが UDP バッファ不足によりパケット損失を引き起こしている場合は、次の手順でトラブルシューティングを行い対処することができます：
1. `ss -nump` コマンドを使用して UDP 送信バッファがフルかどうかを確認します。
2. フルである場合は、カーネルパラメータ `net.core.wmem_max` と `net.core.wmem_default` を大きくし、UDP プログラムを再起動して有効にします。カーネルパラメータの詳細情報については、Linux インスタンスで一般的に使用されるカーネルパラメータの説明をご参照ください。

3. それでもパケット損失の問題が解消されない場合は、 `ss -nump` コマンドを使用して送信バッファが期待どおりに増大していないことを確認できます。この場合は、ビジネスコードがsetsockoptを介してSO_SNDBUFを設定しているかどうかを確認する必要があり、そうであれば、コードを変更して SO_SNDBUFを増大させてください。

UDP 受信バッファがフル

インスタンスが UDP バッファ不足によりパケット損失を引き起こしている場合は、次の手順で対処することができます：

1. `ss -nump` コマンドを使用して UDP 受信バッファがフルかどうかを確認します。
1. フルである場合は、カーネルパラメータ `net.core.rmem_max` と `net.core.rmem_default` を大きくし、UDP プログラムを再起動して有効にします。カーネルパラメータの詳細情報については、 Linux インスタンスで一般的に使用されるカーネルパラメータの説明 をご参照ください。
2. それでもパケット損失の問題が解消されない場合は、 `ss -nump` コマンドを使用して受信バッファが期待どおりに増大していないことを確認できます。この場合は、ビジネスコードがsetsockoptを介して SO_RCVBUFを設定しているかどうかを確認する必要があり、そうであれば、コードを変更して SO_RCVBUFを増大させてください。

TCP すべての接続キューがフル

TCP すべての接続キューの長さは `net.core.somaxconn` および業務プロセスが listen を呼び出す時に渡される backlog パラメータの内の小さい方の値となります。インスタンスに TCP すべての接続キューがフルであることによるパケット損失が発生した場合は、次の手順で対処することができます：

1. カーネルパラメータ `net.core.somaxconn` を大きくします。カーネルパラメータの詳細情報については、 Linux インスタンスで一般的に使用されるカーネルパラメータの説明 をご参照ください。
2. 業務プロセスが backlog パラメータを渡したかどうかを確認します。渡している場合は、 backlog パラメータを相応に大きくします。

TCP リクエストのオーバーフロー

TCPのデータ受信時に、socket が user によってロックされている場合、データは backlog キューに送信されます。 このプロセスに失敗すると、TCPリクエストのオーバーフローが引き起こされパケット損失が発生します。通常は、業務プログラムのパフォーマンスが正常であると想定されることから、次の方法を参照して、システムレベルからトラブルシューティングを行い対処することができます：

業務プログラムが setsockopt を介して buffer サイズを自動的に設定しているかどうかを確認する：

設定しており、かつその値が小さい場合は、業務プログラムを修正し、さらに大きな値を指定するか、または setsockopt を介させずにサイズを指定することができます。

説明：

setsockopt の値はカーネルパラメータ `net.core.rmem_max` と `net.core.wmem_max` によって制限されます。業務プログラムを調整すると同時に、 `net.core.rmem_max` と `net.core.wmem_max` を同期的に調整することができます。調整後に業務プログラムを再起動し、設定を有効にします。

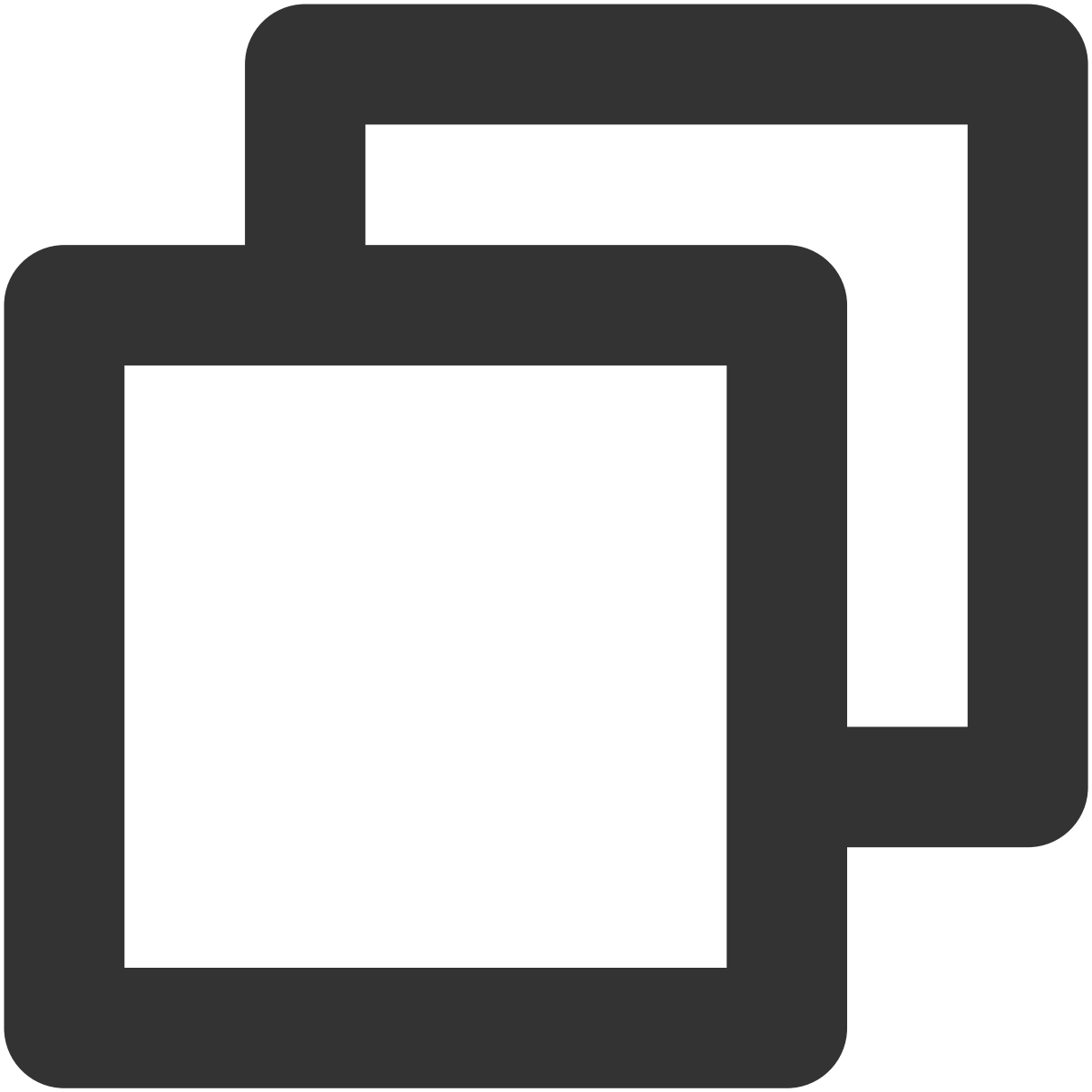
設定していない場合は、 カーネルパラメータ `net.ipv4.tcp_mem` 、 `net.ipv4.tcp_rmem` および `net.ipv4.tcp_wmem` を大きくすることで TCP socket のレベルを調整することができます。
カーネルパラメータの修正については、 Linux インスタンスで一般的に使用されるカーネルパラメータの説明 をご参照ください。

接続数が上限に到達

CVMインスタンスには複数の仕様があり、仕様ごとに接続数性能指標が異なります。インスタンスの接続数がインスタンス仕様に対応する基準を超過した場合、プラットフォームの速度制限がトリガーされ、パケット損失を引き起こすことがあります。対処手順は次のとおりです：
説明：
接続数とはホストに保存されるCVMインスタンスのセッション数であり、 TCP、UDPとICMPが含まれます。この数値はCVMインスタンスで `ss` や `netstat` コマンドを介して取得されたネットワーク接続数よりも大きくなります。
インスタンスの接続数を確認して、 インスタンス仕様 を比較し、インスタンス仕様の性能ボトルネックに達していないかどうかを確認します。
ボトルネックに達している場合は、インスタンス仕様をアップグレードするか、または業務量を調整する必要があります。
インスタンス仕様の性能ボトルネックに達していない場合は、チケットを提出 して処理を更に特定することができます。

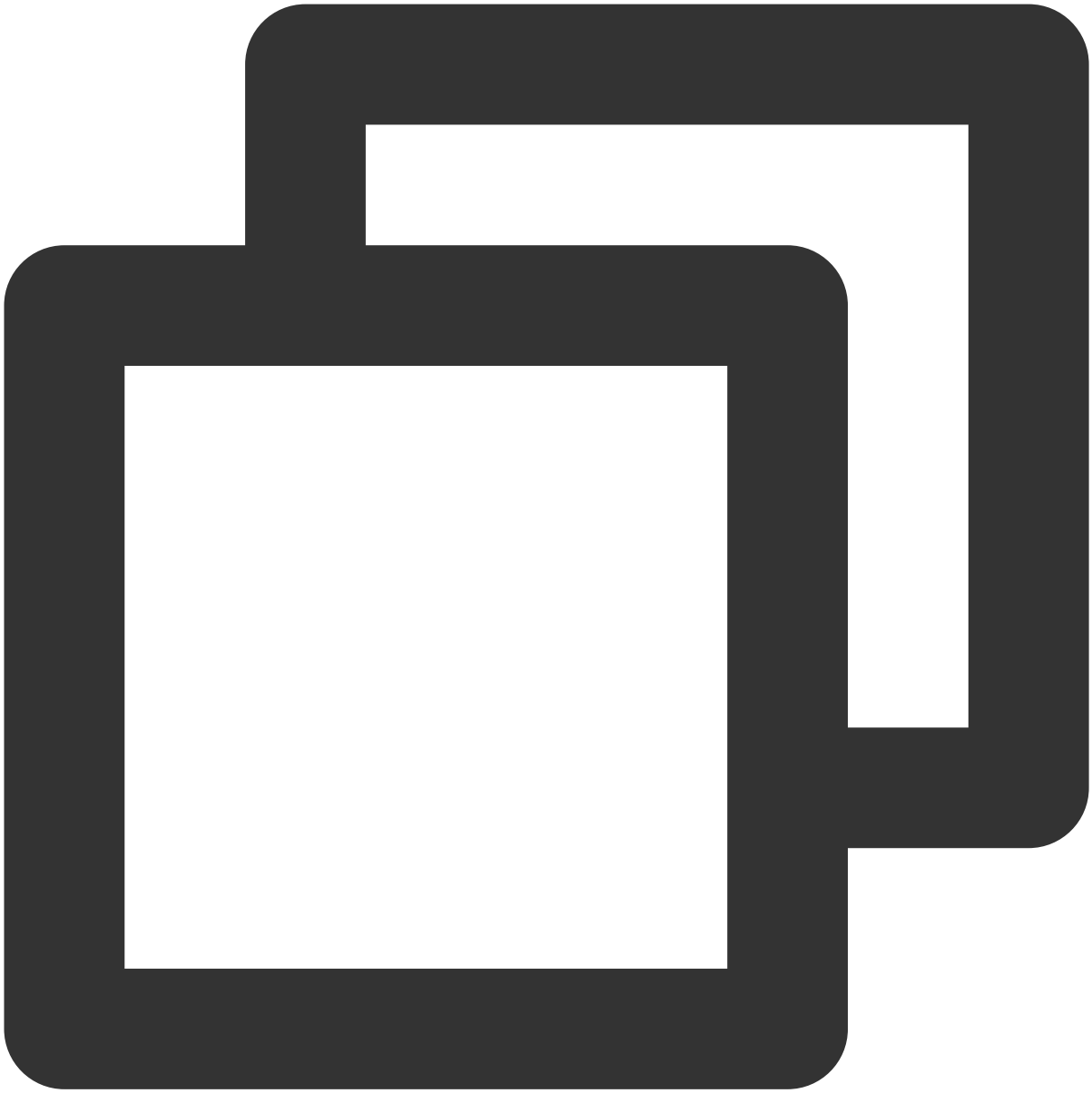
iptables policy関連ルールの設定

CVMのiptablesに関連ルールを設定していない場合、iptables policy関連ルールを設定するとCVMに到達したパケットがすべて破棄される可能性があります。処理手順は以下のとおりです。
1. 以下のコマンドを実行し、iptables policy ルールを確認します。



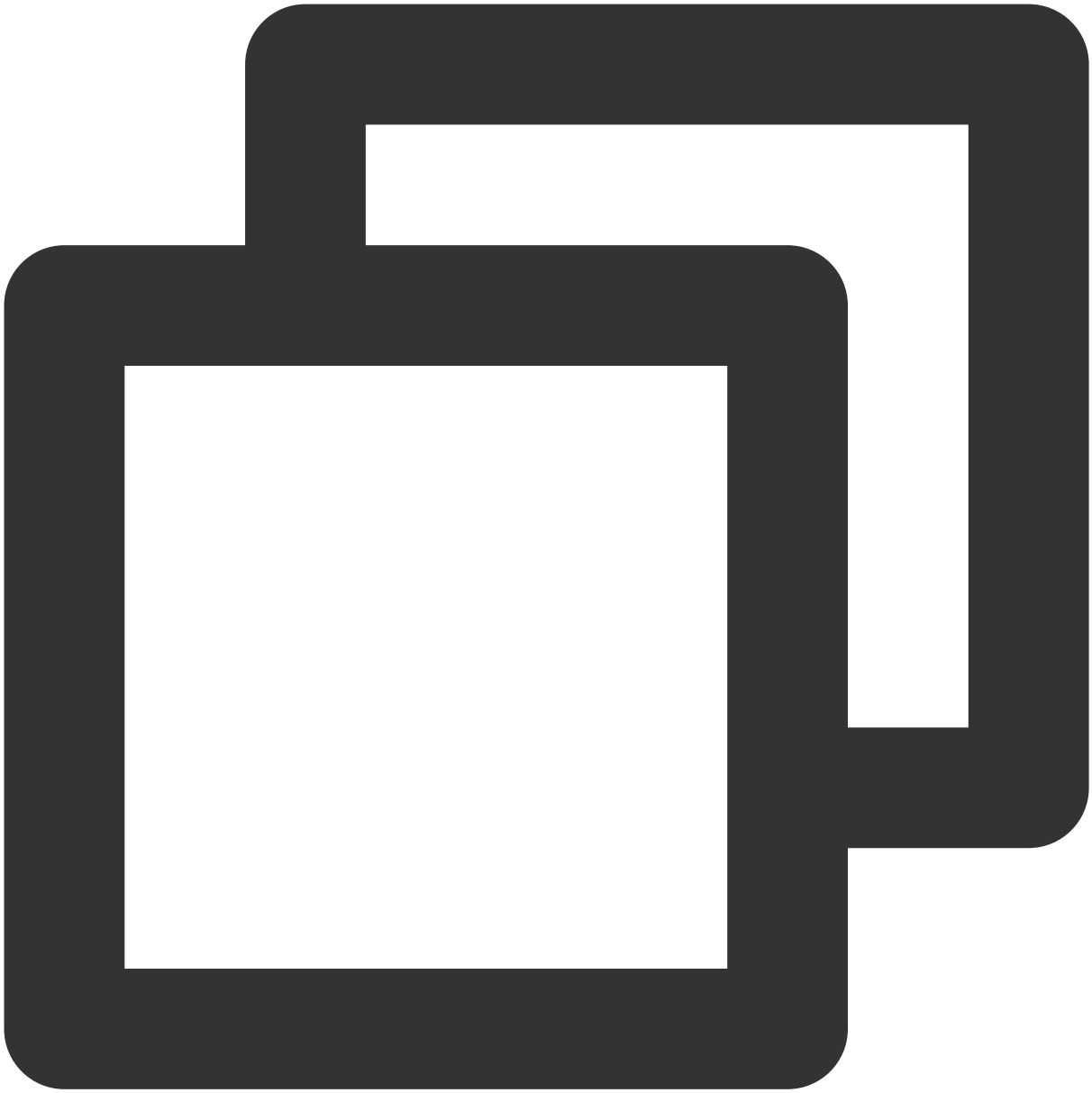
```
iptables -L | grep policy
```

iptables policyルールはデフォルトではACCEPTです。INPUTチェーンpolicyがACCEPTでない場合、サーバーに到達したパケットがすべて破棄されます。例えば、以下の結果がリターンされた場合、CVMへのパケットがすべて破棄されたことを意味します。



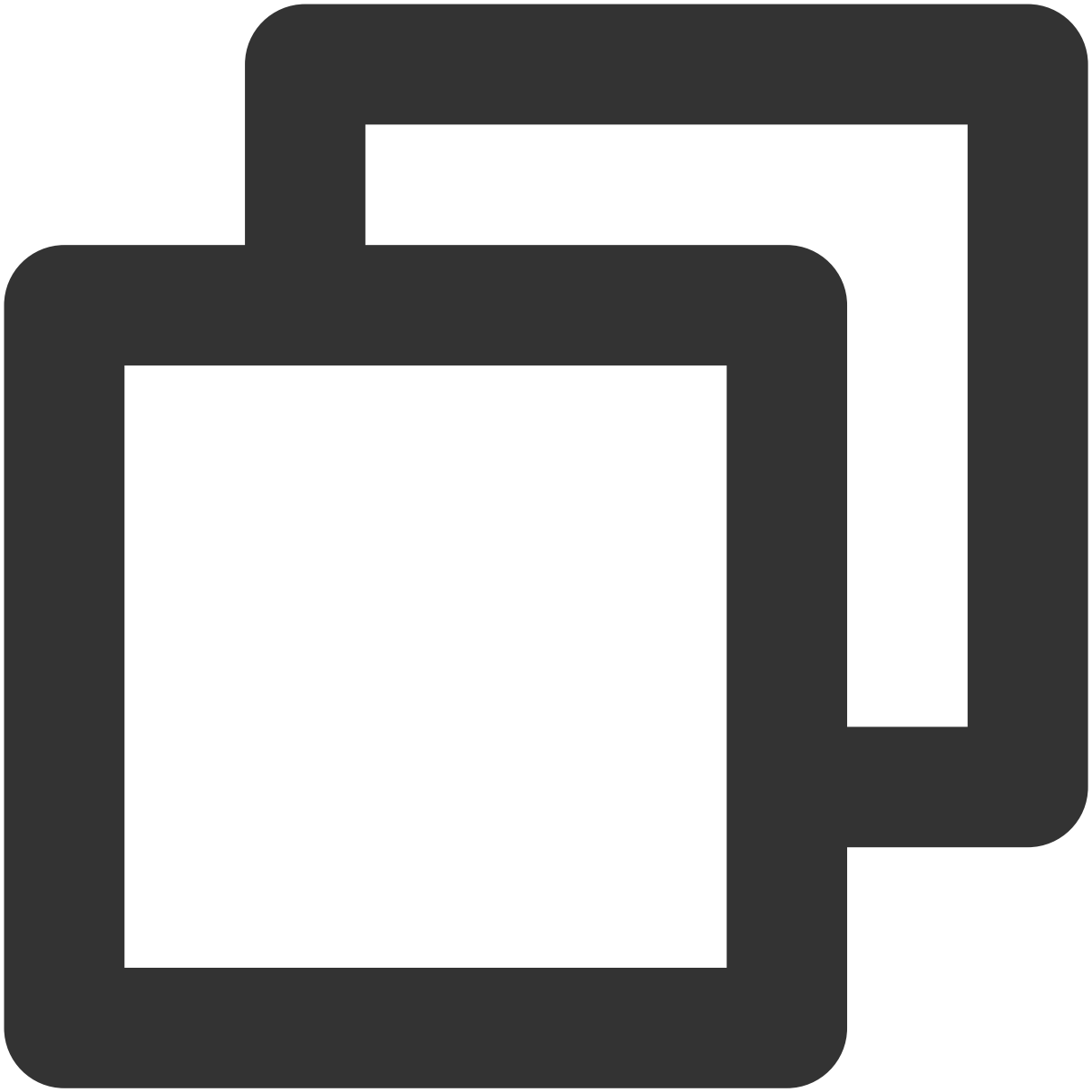
```
Chain INPUT (policy DROP)
Chain FORWARD (policy ACCEPT)
Chain OUTPUT (policy ACCEPT)
```

2. 以下のコマンドを実行し、必要に応じて `-P` の後ろの値を変更します。



```
iptables -P INPUT ACCEPT
```

変更後、手順1 のコマンドを再度実行して確認できます。以下の結果がリターンされるはずです。



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

インスタンス IP アドレスを ping できない

最終更新日：：2023-02-01 16:43:58

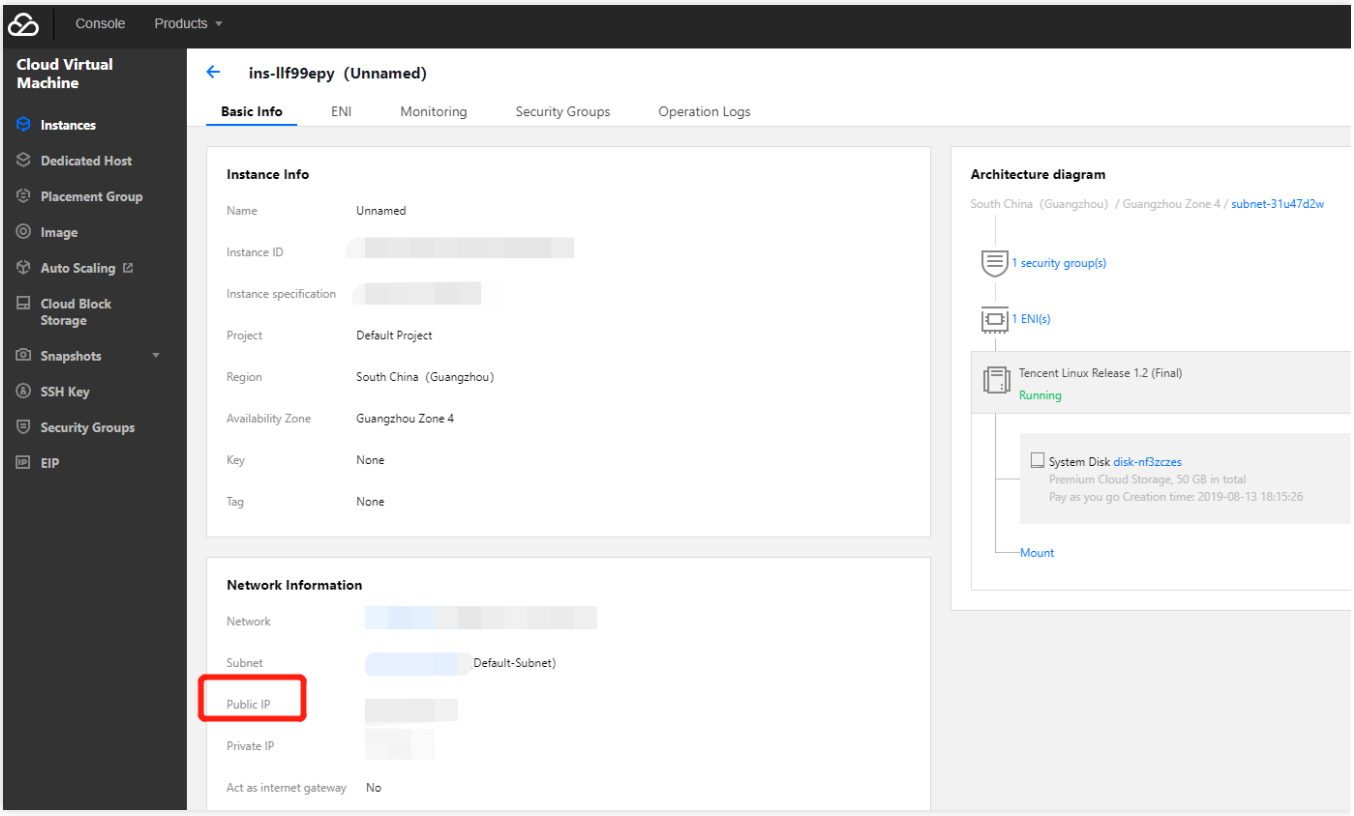
障害の現象

ローカルホストからインスタンスにpingが通らない場合は、以下のような原因が考えられます：
ターゲットサーバーの設定が正しくない
ドメイン名が正しく解析されていない
リンク障害
ローカルネットワークが正常に動作している前提で（他のウェブサイトへのpingが通る）、下記の操作によりトラブルシューティングを実施します：
インスタンスにはパブリックIPアドレスが設定されているかを確認
セキュリティグループの設定を確認
システム設定を確認
その他の操作

実施手順

インスタンスにはパブリックIPアドレスが設定されているかを確認します

説明：
インスタンスにパブリックIPアドレスが設定されている場合のみ、Internet上の他のコンピュータと通信できます。インスタンスにパブリックIPアドレスが設定されていない場合、プライベートIPアドレスでは外部からインスタンスへのpingが通りません。
1. CVMコンソール にログインします。
2. 「インスタンスリスト」画面で、下図に示すように、pingを実行したいインスタンスID/インスタンス名を選択し、下図にしめされているように、そのインスタンスの詳細画面に入ります：

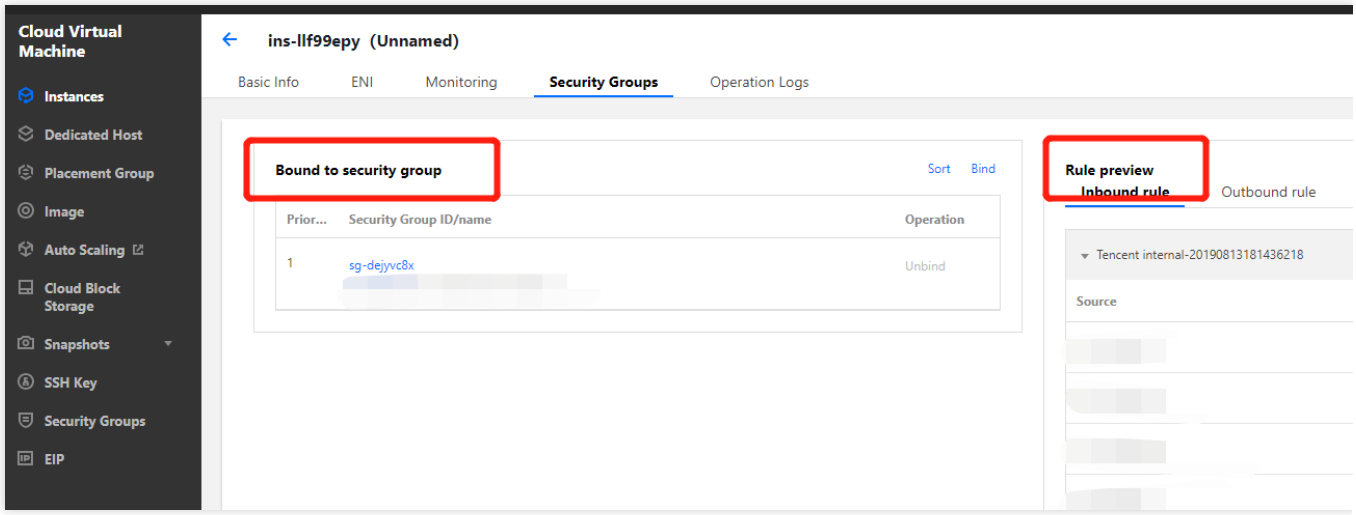


3. 「ネットワーク情報」欄で、インスタンスにパブリックIPアドレスが設定されているかを確認します。
設定されている場合、セキュリティグループの設定を確認 してください。
設定されていない場合、EIPでクラウドリソースをバインディング してください。

セキュリティグループの設定を確認します

セキュリティグループは仮想ファイアウォールであり、関連付けられているインスタンスのインバウンドトラフィックとアウトバウンドトラフィックを制御することができます。セキュリティグループのルールでは、プロトコル、ポート、ポリシーなどを指定することができます。pingはICMPプロトコルを使用するため、インスタンスと関連を付けたセキュリティグループではICMPを許可しているかを確認する必要があります。以下の操作を実施し、インスタンスで使用されているセキュリティグループ、およびインバウンドルールとアウトバウンドルールの詳細を確認してください。

1. CVMコンソール にログインします。
2. 「インスタンスリスト」画面で、セキュリティグループを設定するインスタンスのID/インスタンス名を選択して、そのインスタンスの詳細画面に入ります。
3. **セキュリティグループ**タブを選択し、下図に示すように、対象インスタンスのセキュリティグループ管理画面に入ります。



4. インスタンスで使用されているセキュリティグループ、およびインバウンドルールとアウトバウンドルールの詳細を確認することにより、インスタンスと関連を付けたセキュリティグループではICMPを許可しているかを判断します。
許可している場合、システム設定を確認 してください。
許可しない場合、ICMPプロトコルのポリシーを許可するように設定してください。

[システム設定を確認します

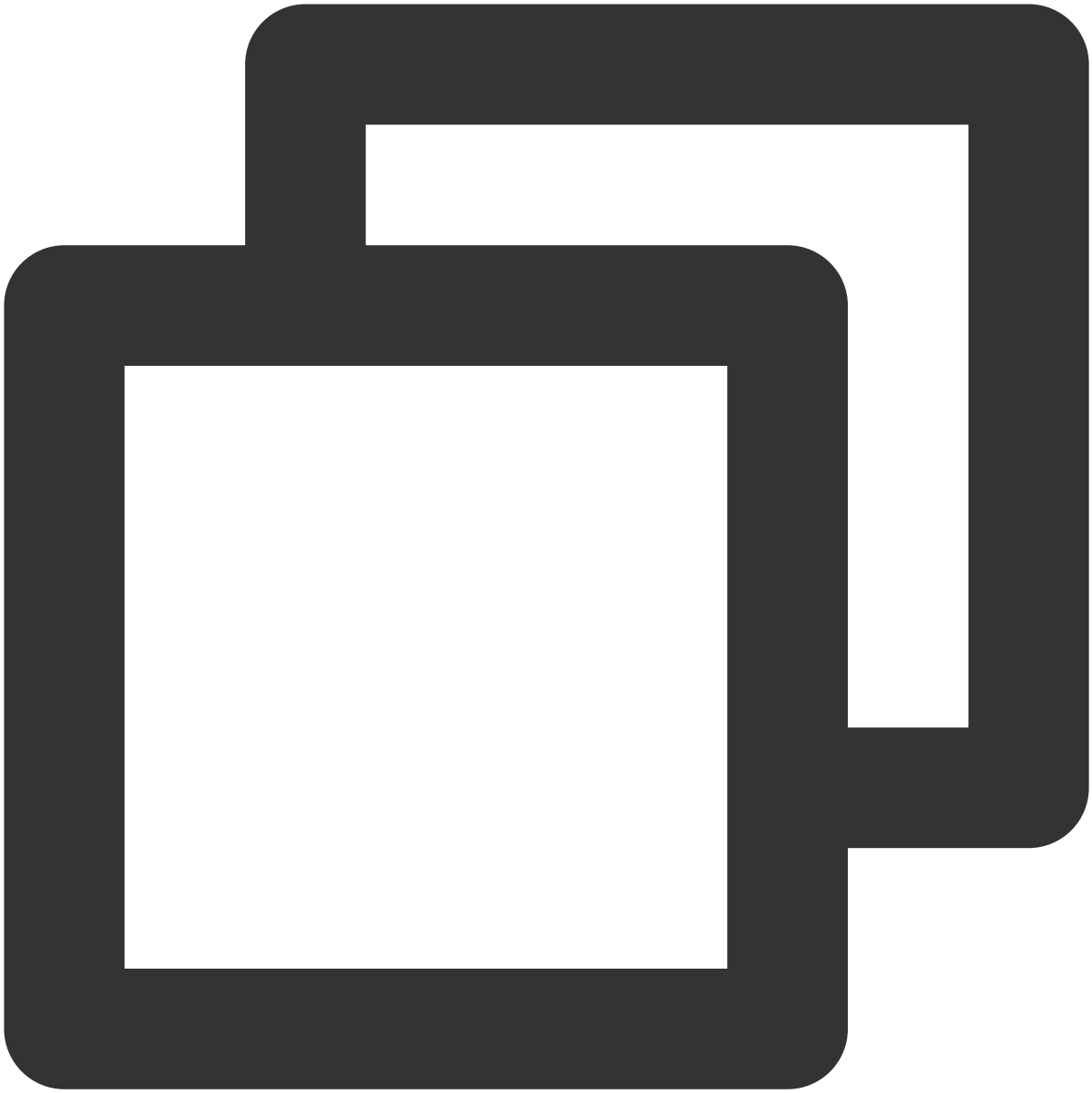
インスタンスのOSタイプを判断して、確認方法を選択します。
Linux OSの場合、Linuxカーネルのパラメータとファイアウォールの設定を確認 してください。
Windows OSの場合、Windowsのファイアウォールの設定を確認 してください。ファイアウォールに問題がなければ、Windowsのネットワーク設定をリセット してください。

Linuxカーネルのパラメータとファイアウォールの設定を確認します

説明：
Linux OSではpingが許可されるかは、カーネルとファイアウォールの両方の設定によります。いずれかが禁止されている場合、pingパケットが「Request timeout」になります。

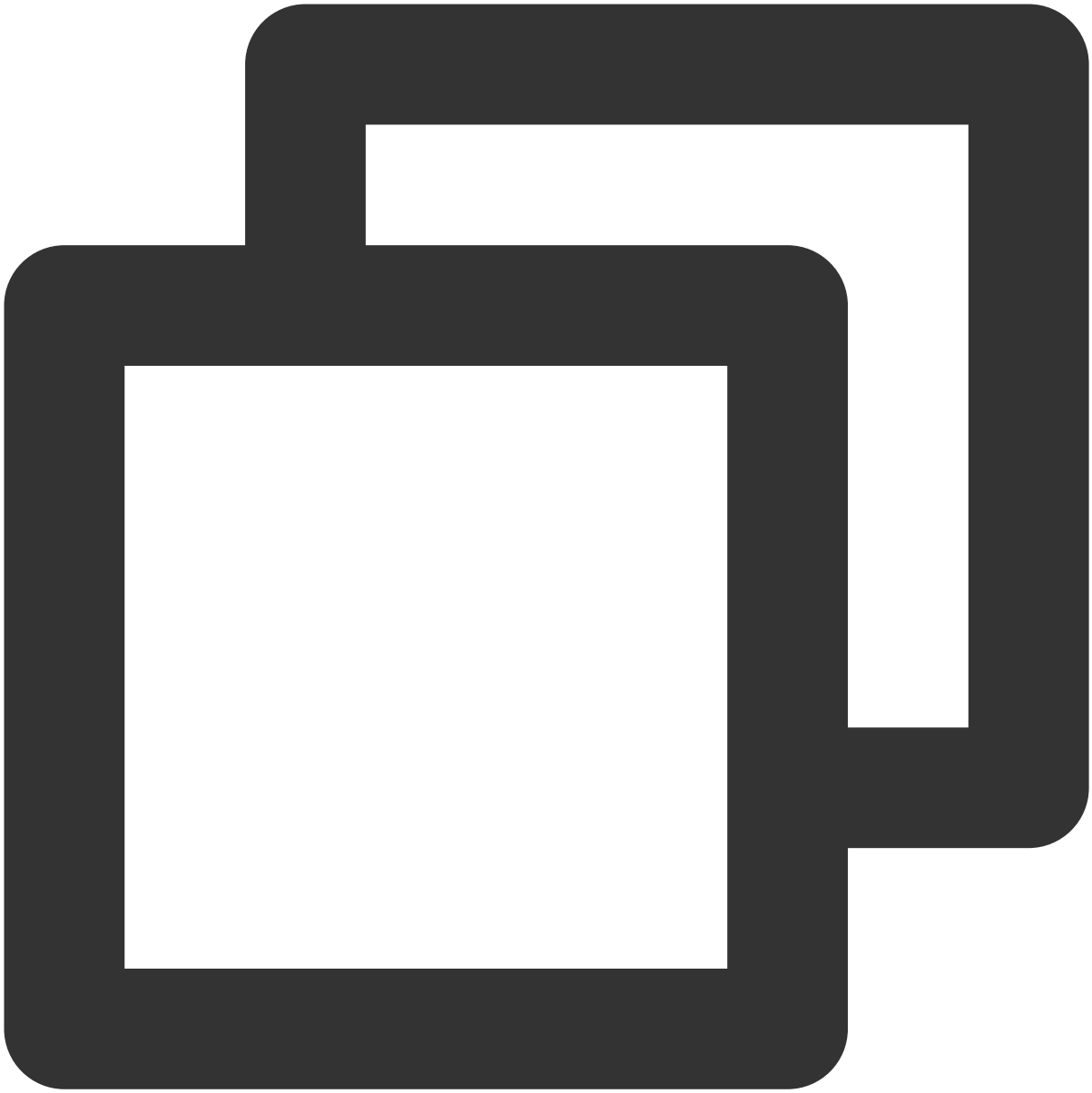
カーネルパラメータicmp_echo_ignore_allを確認します

1. VNCでインスタンスにログインします。詳しくは以下をご参照ください。
VNCによるLinuxインスタンスへのログイン
VNCによるWindowsインスタンスへのログイン
2. 下記のコマンドを実行し、システムのicmp_echo_ignore_allの設定を確認します。



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

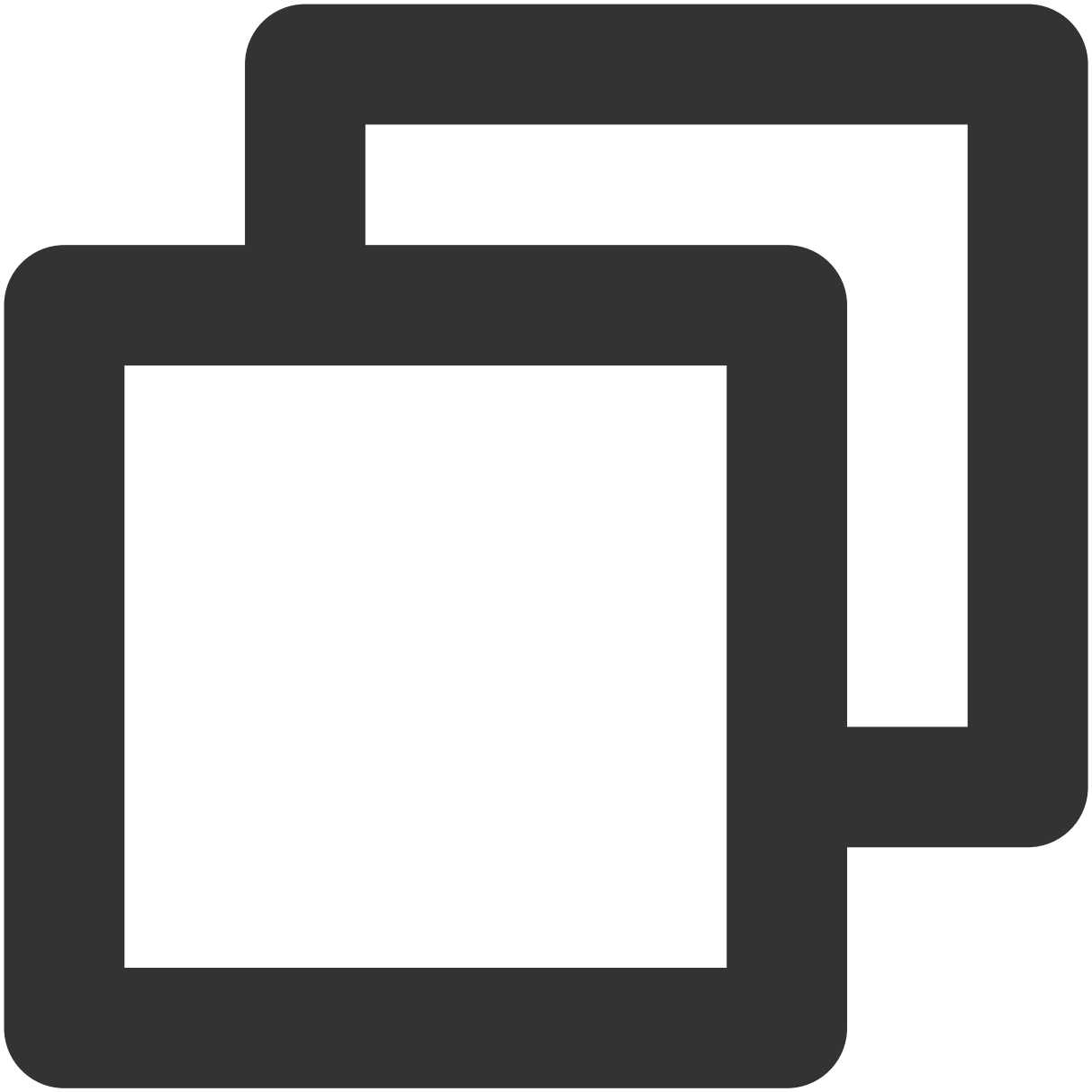
0が返された場合、システムではすべてのICMP Echoリクエストが許可されるため、ファイアウォールの設定を確認 してください。
1が返された場合、システムではすべてのICMP Echoリクエストが拒否されるため、手順3 を実施してください。
3. 下記のコマンドを実行し、カーネルパラメータicmp_echo_ignore_allの設定を変更します。



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

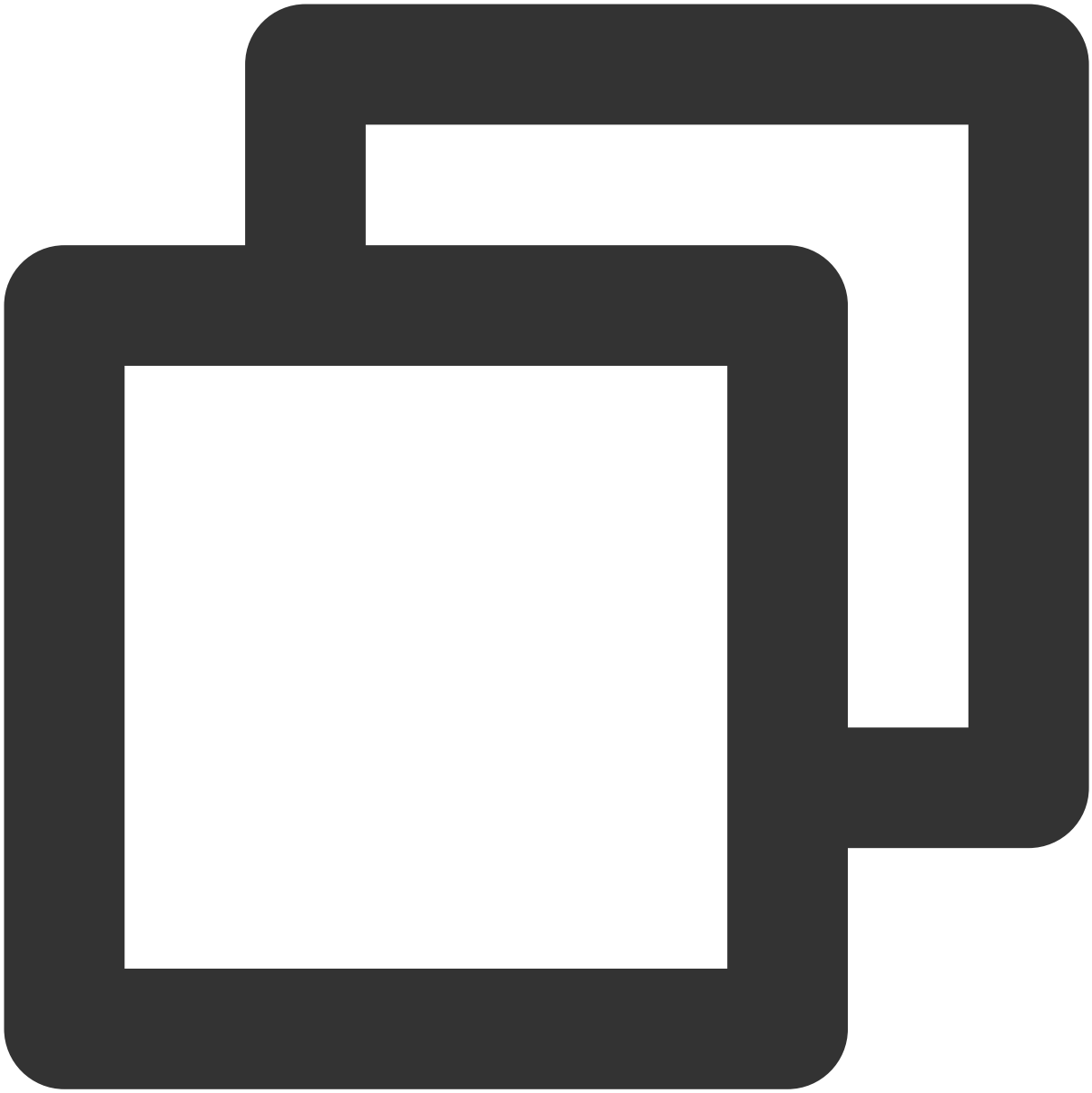
ファイアウォールの設定を確認します

下記のコマンドを実行して、現在のサーバーのファイアウォールルールおよび該当するICMPルールが禁止されているかを確認します。



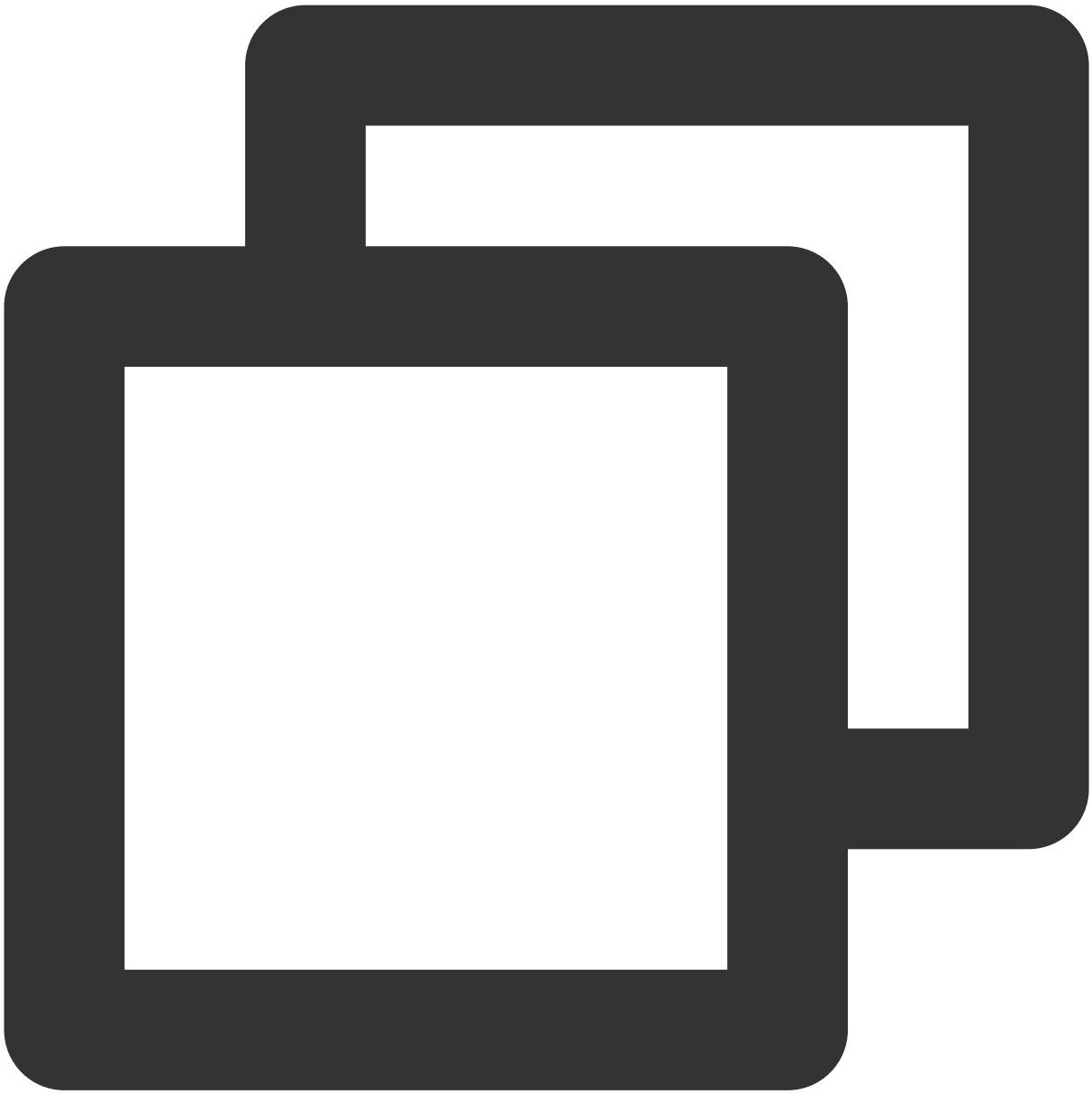
```
iptables -L
```

以下が返された場合、該当するICMPルールが禁止されていません。



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

返された結果は、ICMPに対応するルールが禁止されている場合は、下記のコマンドを実行して、対応するルールを有効にします。



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

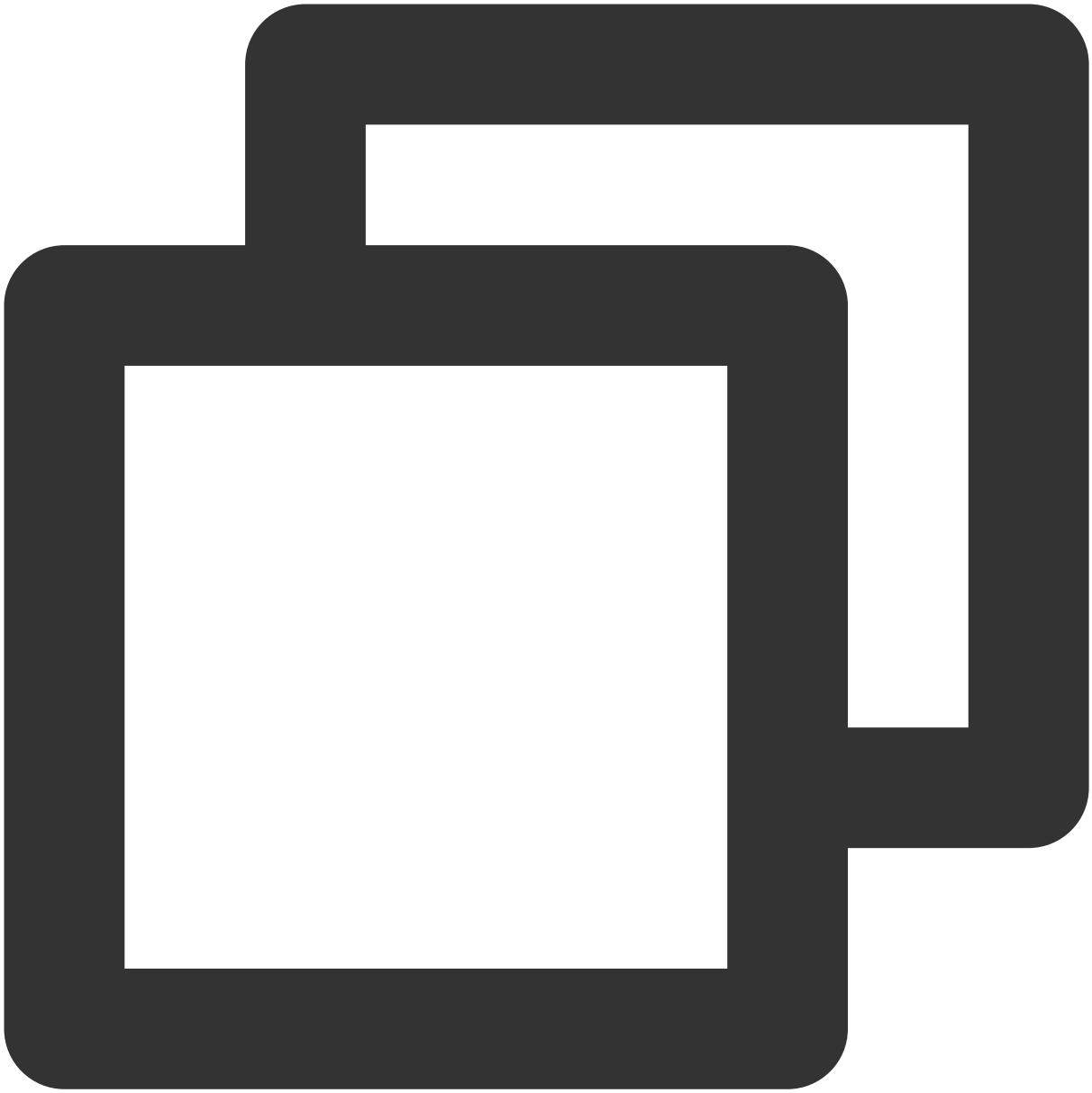
Windowsファイアウォールの設定を確認します

1. インスタンスにログインします。

2. **コントロールパネル**を起動し、**Windows Defender ファイアウォールの設定**を選択します。
3.「Windows Defender ファイアウォール」画面で、**高度な設定**を選択します。
3. 表示された「セキュリティが強化されたWindows Defender ファイアウォール」ウィンドウで、ICMPに関するアウトバウンドとインバウンドのルールが禁止されているかを確認します。
下図に示すように、ICMPに関するアウトバウンドとインバウンドのルールが無効になっている場合は、ルールを有効にしてください。

Windowsのネットワーク設定をリセットします

1. ご利用のVPCネットワークではDHCPがサポートされているかを確認してください（2018年6月以降に作成したVPCネットワークの場合、DHCPがサポートされています）。サポートされていない場合、ネットワーク設定における静的IPが正しいかを確認してください。
2. DHCPがサポートされている場合、DHCPに割り当てられたプライベートネットワークIPが正しいかを確認してください。正しくない場合、公式サイトのログイン機能（VNCでログイン）を使用し管理者としてPowerShellを起動し、DHCPコンポーネントがIPを再取得するように、 `ipconfig /release` と `ipconfig/renew` （マシンを再起動する必要はありません）を実行してみてください。
3. DHCPに割り当てられたプライベートネットワークIPが正しいが、依然としてpingが通らない場合、スタートメニューから**ファイル名を指定して実行**を起動し、 `ncpa.cpl` を入力して[OK]をクリックします。ローカル接続を起動し、LANカードを無効にしてから有効にします。
4. 上記の方法を試しても問題を解決できない場合は、管理者としてCMDで以下のコマンドを実行してマシンを再起動します。



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

その他の操作

上記の方法を試しても問題を解決できない場合、以下の内容をご参照ください。
ドメイン名へのpingが通らない場合は、ウェブサイトの設定を確認してください。
パブリックネットワークIPへのpingが通らない場合は、インスタンスの情報と双方向のMTRデータ（ローカルからCVMへ、CVMからローカルへ）を添付し、チケットを提出 してエンジニアに連絡してください。
MTRの利用方法については、サーバーネットワーク遅延とパケットロスの処理 をご参照ください。

ドメイン名を解析できない（CentOS 6.x システム）

最終更新日：：2020-01-08 16:35:32

事象の説明

CentOS 6.x OSのCVMを再起動するか、 `service network restart` コマンドを実行した後、CVMはドメイン名を解析できない場合があります。また、 `/etc/resolv.conf` 設定ファイルを表示すると、DNS情報がクリアされていることがわかりました。

考えられる原因

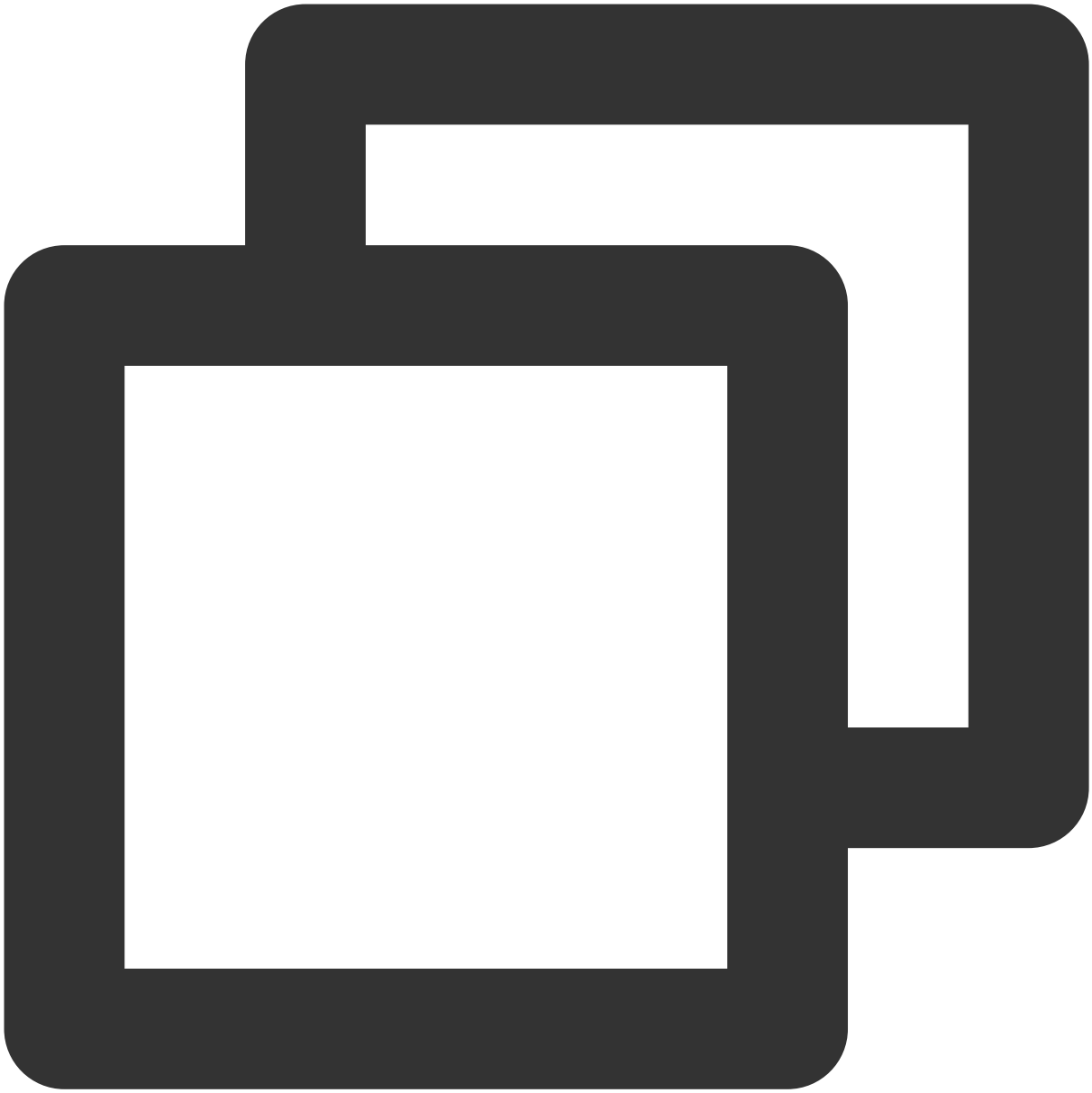
CentOS 6.x OSでは、grep のバージョンが異なるため、initscriptsのバージョンが 9.03.49-1 より低い場合、バグがあります。

解決方法

initscriptsを最新バージョンにアップグレードし、DNS情報を再生成します。

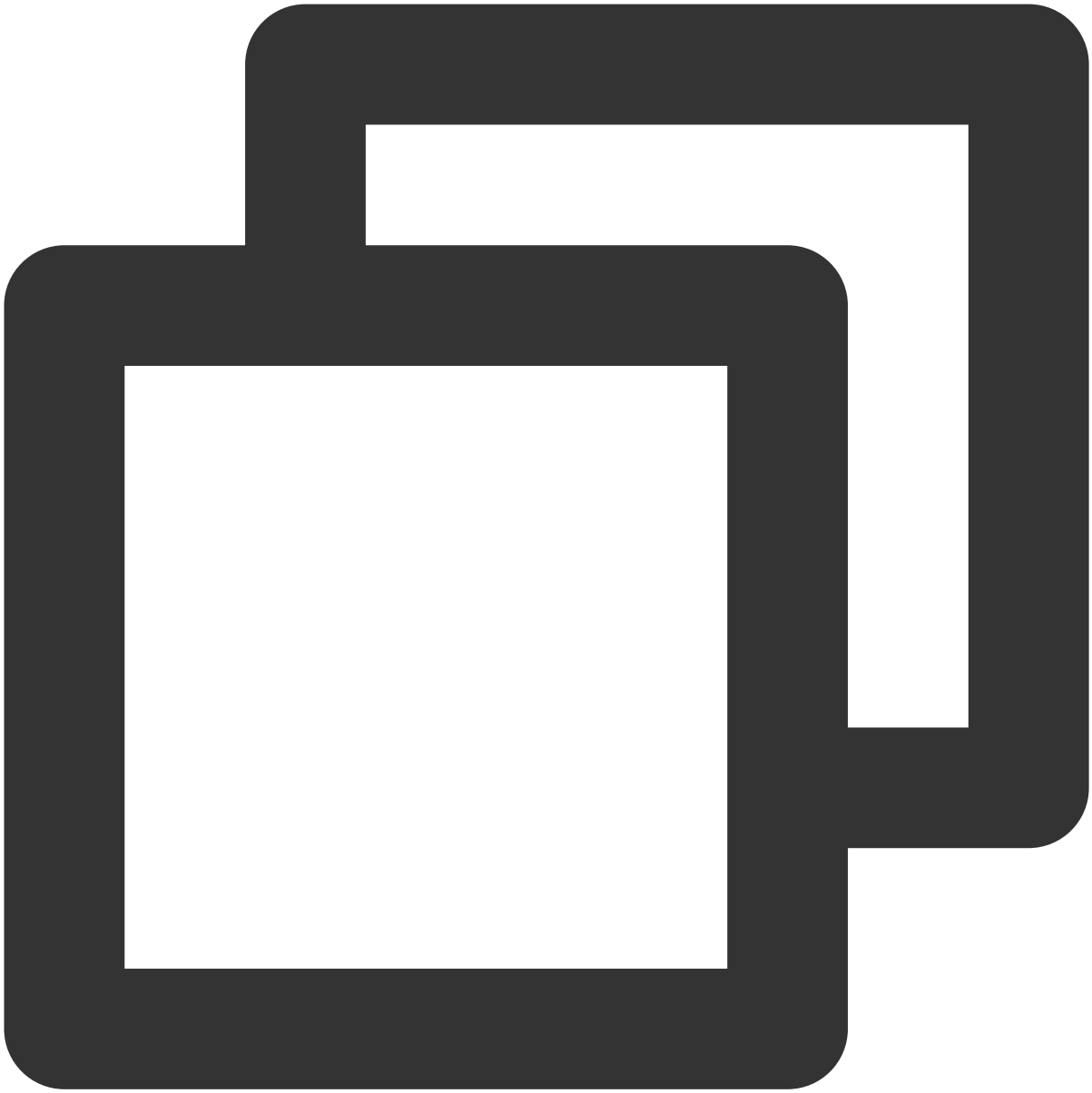
処理手順

1. CVM にログインします。
2. 次のコマンドを実行して、initscripts のバージョンを確認し、9.03.49-1より低いバージョン（バグが潜在する）であるかを確認します。



```
rpm -q initscripts
```

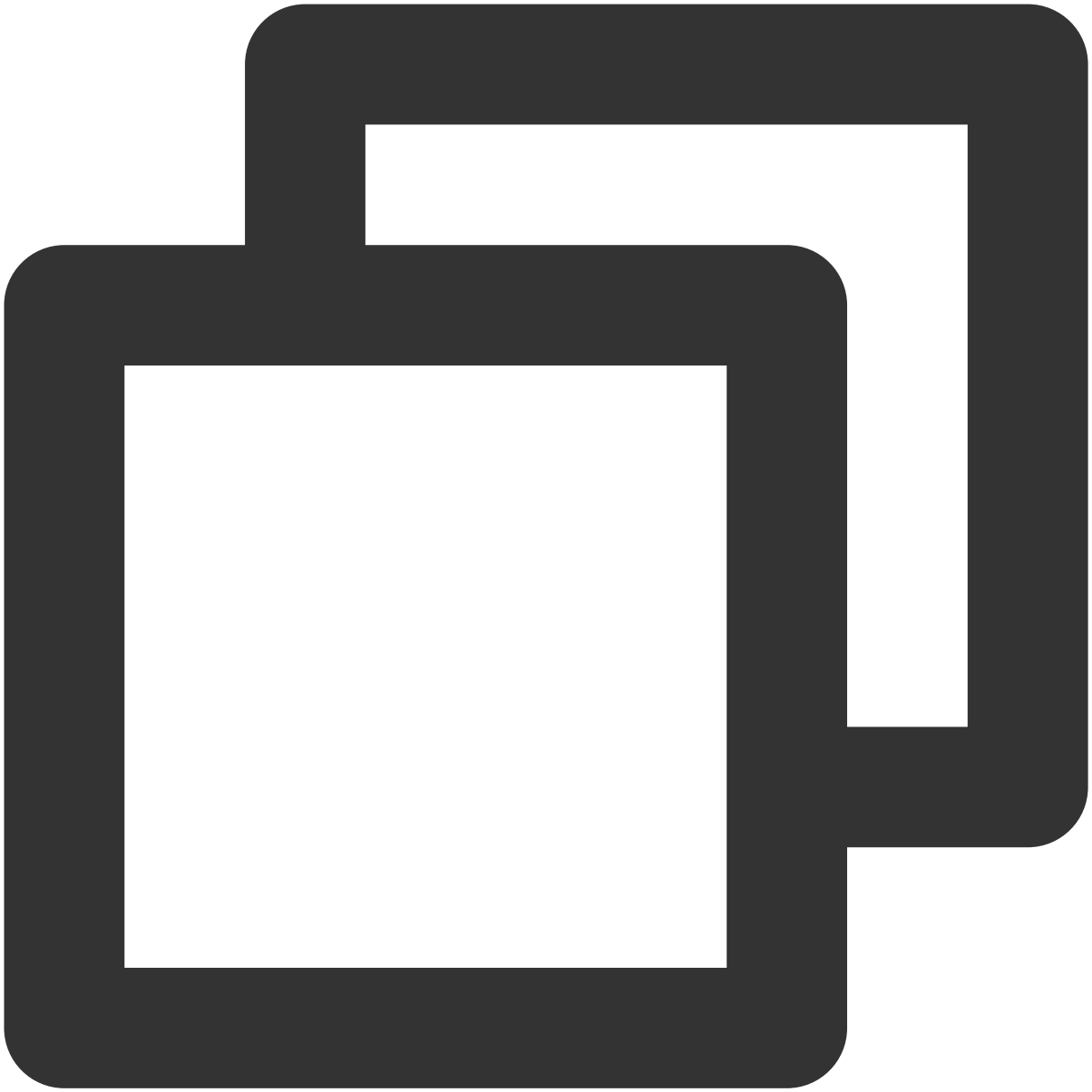
次のような情報が返されます：



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

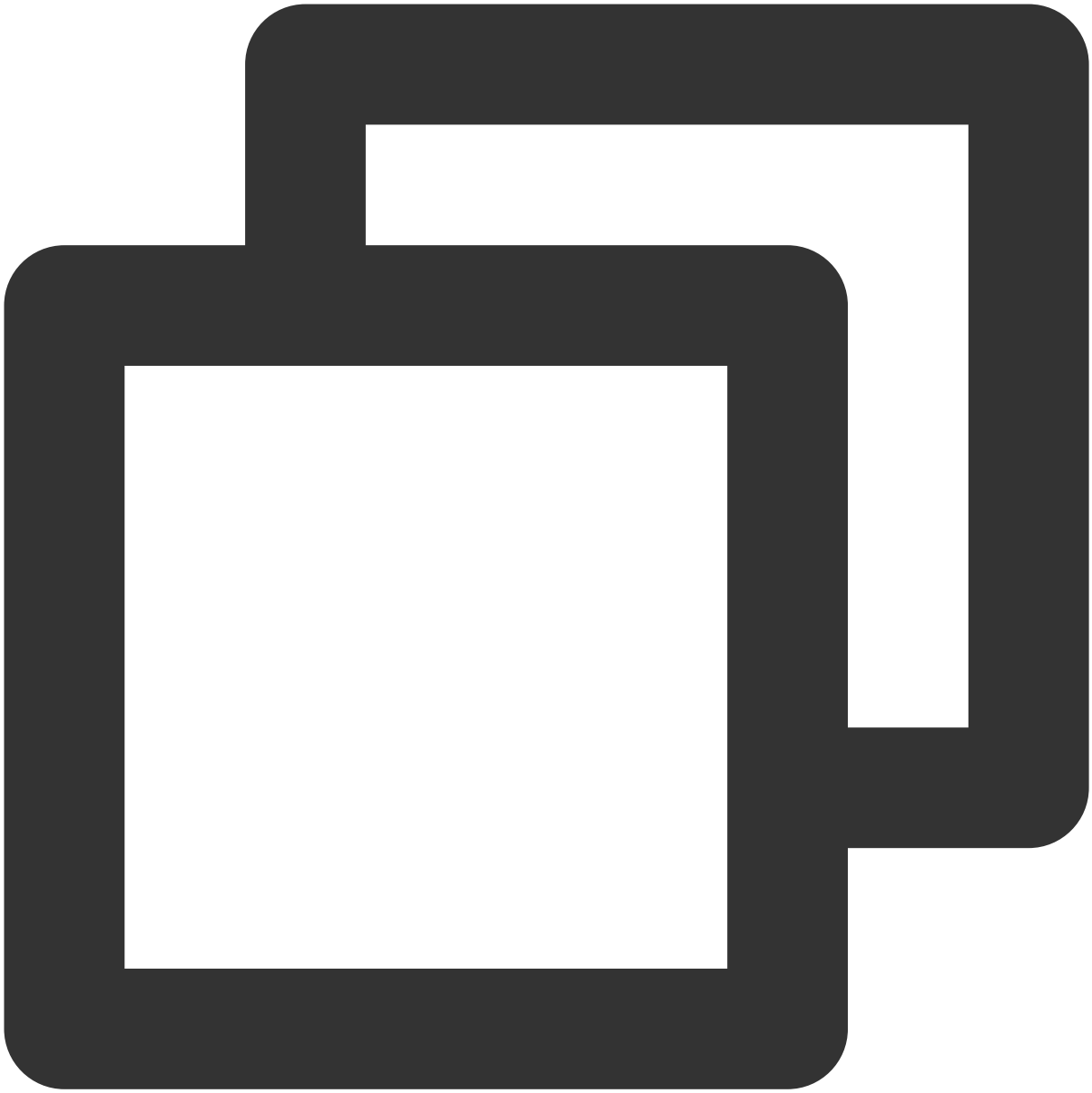
initscriptsのバージョンがinitscripts-9.03.40-2 であり、既存の問題バージョン（initscripts-9.03.49-1）より低く、DNS 情報がクリアになるリスクがあることが分かります。

3. 次のコマンドを実行して、initscripts を最新バージョンにアップグレードし、DNS 情報を再生成します。



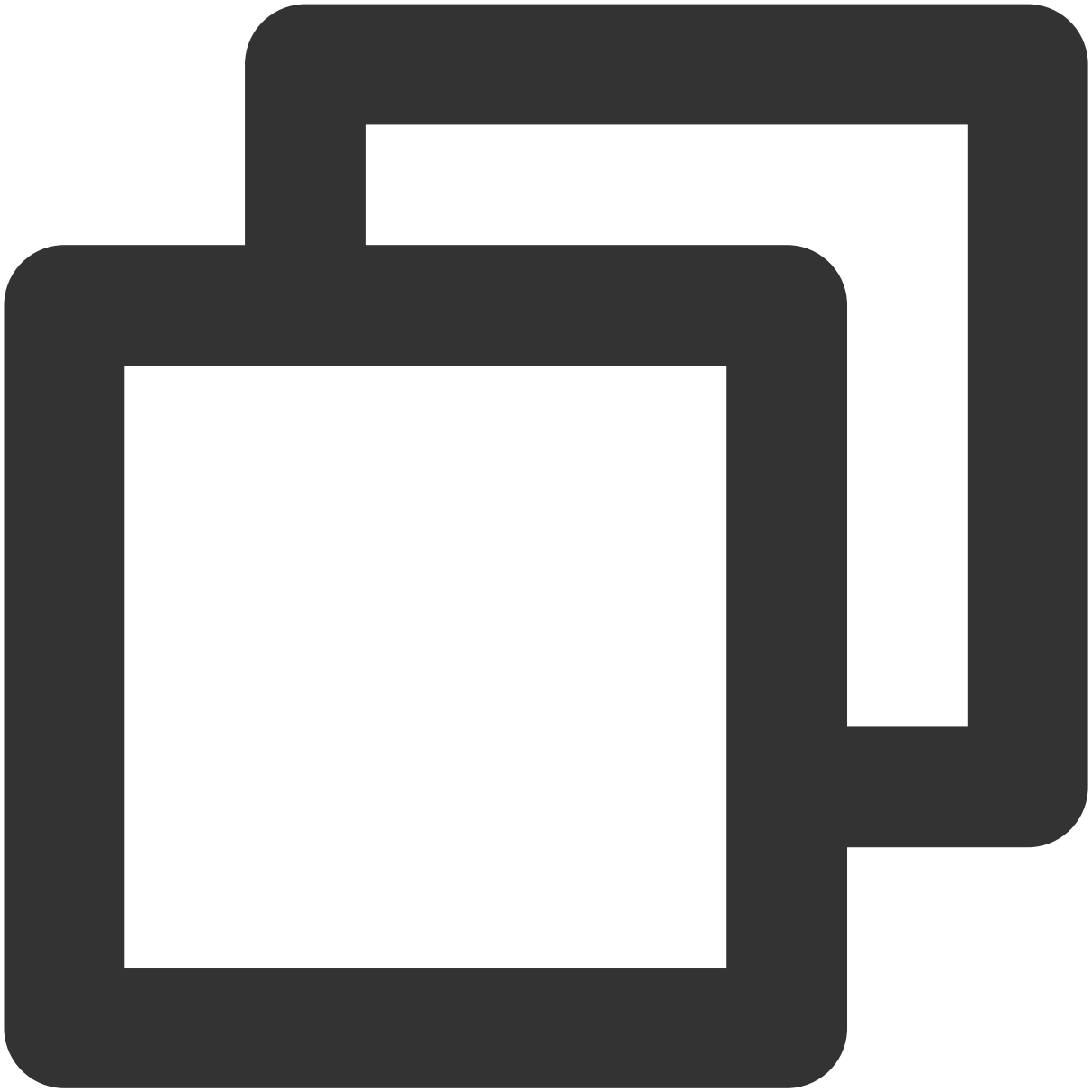
```
yum makecache
yum -y update initscripts
service network restart
```

4. アップグレードが完了したら、次のコマンドを実行して、initscripts のバージョン情報を確認し、アップグレードが成功したかどうかを確認します。



```
rpm -q initscripts
```

次のような情報が返されます：



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

表示されたバージョンは以前のバージョンと異なり、initscripts-9.03.49-1バージョンより高く、アップグレードが成功していることが分かります。