

# Cloud Virtual Machine

## 操作ガイド

## 製品ドキュメント



Tencent Cloud

## Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

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

## Trademark Notice



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

## Service Statement

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

## カタログ：

### 操作ガイド

操作ガイド一覧

ご利用制限一覧

便利な機能

コンソールのページビューの切り替え

### インスタンス

インスタンスを作成

インスタンス作成ガイドライン

CVM購入ページからのインスタンスの作成

カスタムイメージによるインスタンスの作成

同じ構成のインスタンスの購入

インスタンスを作成するためのAPI Explorerのベストプラクティススクリプトの生成

モデル比較の有効化

インスタンス起動テンプレートの管理

一括連続命名または指定文字列パターン命名

Linuxインスタンスにログインする

標準ログイン方式を使用してLinuxインスタンスにログインする（推奨）

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

SSHを使用してLinuxインスタンスにログインする

VNCを使用してLinuxインスタンスにログインする

モバイルデバイスを使用してLinuxインスタンスにログインする

Windowsインスタンスにログインする

標準方式を使用してWindowsインスタンスにログイン（推奨）

RDPファイルを使用してWindowsインスタンスにログインする

リモートデスクトップ接続を使用してWindowsインスタンスにログインする

VNCを使用してWindowsインスタンスにログインする

モバイルデバイスからWindowsインスタンスにログインする

設定を調整する

インスタンス構成の変更

ネットワーク構成の変更

プロジェクト設定の調整

インスタンス構成変更の提案

情報の確認

インスタンス情報の確認

インスタンスメタデータのクエリ

- インスタンスの名前変更
- インスタンスのパスワードのリセット方法
- インスタンス IP アドレスを管理する
  - プライベートIPアドレスの取得とDNSの設定
  - プライベートIPアドレスの変更
  - パブリックIPアドレスの取得
  - パブリックIPアドレスの変更
  - パブリックIPアドレスを取り戻す
- セキュリティグループの変更
- 従量課金インスタンスの年額・月額課金への変換
- インスタンスの検索
- インスタンスリストのエクスポート
- インスタンスの起動
- インスタンスのシャットダウン
- インスタンスの再起動
- インスタンスの休止
- システムをリインストールする
- TATを使用してコマンドを実行し
- インスタンスの破棄/返却
  - インスタンスの廃棄/返却の概要
  - コンソールを使用したインスタンスの破棄/返却
- インスタンスの削除保護の有効化
- インスタンスを回収する又はインスタンスの復元
- スポットインスタンスの管理
- スポットインスタンスの回収状態を確認する
- 停止済み従量課金インスタンスの非課金化
- インスタンスロールの管理
- リザーブドインスタンス
  - リザーブドインスタンスの分割
  - リザーブドインスタンスのマージ
- イメージ
  - カスタムイメージの作成
  - カスタムイメージの共有
  - カスタマイズイメージの共有を取り消す
  - カスタムイメージの削除
  - イメージのコピー
  - イメージのインポート
    - イメージのインポートの概要

イメージの強制インポート

イメージのエクスポート

CentOS Linux関連操作

CentOSの移行 TencentOS Serverガイド

サービス移行

オンライン移行

オンライン移行の概要

移行ガイド

オンライン移行ガイド

オンライン移行：クライアントからの移行元のインポート

オンライン移行：コンソールでのワンクリック移行

マイグレーションツールの説明

互換性とツール設定の説明

移行時間予測チュートリアル

課金説明

オフライン移行

お問い合わせ

メンテナンスタスク

メンテナンスタスクの概要

メンテナンスタスクタイプと対処ポリシー

メンテナンスタスクの確認

メンテナンスポリシーの承認とメンテナンスの時間枠の指定

プリセット承認ポリシーの設定

メンテナンスタスクアラート通知の設定

Cloud Block Storage

CBSスケールアウト

ディスクメディアの調整

CBSのパフォーマンスの調整

ネットワーク

VPCサービス切替

一般的なパブリックIPアドレス

EIP

ENI

パブリックネットワークゲートウェイの構成

EIP直通

セキュリティ

セキュリティグループ

セキュリティグループの概要

- セキュリティグループの作成
- セキュリティグループルールの追加
- インスタンスをセキュリティグループに関連付ける
- セキュリティグループ
  - セキュリティグループのコピー
  - セキュリティグループの優先順位の調整
- セキュリティグループルールの管理
  - セキュリティグループルールの表示
  - セキュリティグループルールの変更
  - セキュリティグループルールの削除
  - セキュリティグループルールのエクスポート
- セキュリティグループの応用例
  - サーバーの通常ポート
- 機密性の高い操作に対する保護機能を強化
- ログインパスワードの管理
- SSHキーの管理
- スプレッドプレイズメントグループ
- 25番ポートのブロック解除
- タグ
  - タグを使用したインスタンスの管理
  - タグ編集
- 監視とアラーム
  - インスタンスの監視データを取得する
  - アラームの作成
- Cloud Access Managementの例

# 操作ガイド

## 操作ガイド一覧

最終更新日：：2023-02-24 18:21:47

このドキュメントでは、CVMインスタンスおよびインスタンスに関連する操作について説明します。

## CVMの購入と使用

CVMインスタンスを初めて購入して使用する場合は、以下の手順に従って開始することをお勧めします。

1. CVMインスタンスの概念を理解するには：[CVMの概要](#) をご参照ください。
2. 適切なCVMモデルを選択して購入します。CVMインスタンスを個人ユーザーとして初めて使用する場合は、[Linuxインスタンスの構成](#) をご参照ください。
3. 購入したCVMインスタンスにログインします。購入したインスタンスの種類に応じて、[Windowsインスタンスへのログイン](#) または [Linuxインスタンスへのログイン](#) を選択することが可能です。

## CVM設定の調整

CVMを購入した後、ニーズの変化によりCVMのディスクタイプやネットワークなどの設定を調整する可能性があります。その場合は、下記のドキュメントを参考にし操作を完了することができます。

[インスタンス設定の調整](#)

[ネットワーク設定の調整](#)

[プロジェクト設定の調整](#)

[システムの再インストール](#)

## パスワードとキーのリセット

CVMのパスワードを忘れた場合、またはキーを紛失した場合は、次のドキュメントを参照して、パスワードまたはキーをリセットしてください。

[インスタンスパスワードのリセット](#)

[SSHキーの作成](#)

## インスタンスの更新と課金方法

[インスタンスの更新](#)

## カスタムイメージの作成、インポートまたは削除

[イメージ](#) はCVMインスタンスを起動するためにすべての必要な情報を提供します。現在、Tencent Cloudは「パブリックイメージ」、「カスタムイメージ」、および「共有イメージ」という3種類のイメージを提供します。以下ではイメージがサポートされている操作について説明します。

[カスタムイメージの作成](#)

[カスタムイメージの削除](#)

[イメージのインポート](#)

[イメージのコピー](#)

## トラブルシューティング

CVMインスタンスにログインできない場合、または応答が遅いなどの問題が発生している場合は、下記のドキュメントを参照してトラブルシューティングを行うことができます。

[CVMインスタンスにログインできない問題の解決策](#)

[CVMネットワーク遅延とパケット損失](#)

# ご利用制限一覧

最終更新日：：2024-05-16 10:56:30

## CVM インスタンスの購入に関するアカウント制限

ユーザーはTencent Cloudアカウントの登録を行う必要があります。登録ガイドについては、[Tencent Cloudアカウントの登録](#)をご参照ください。

従量課金のCVMが作成されると、システムは1時間分のCVM使用料をデポジットとしてアカウント残高に凍結され、請求書の支払いを行うための十分な資金がアカウントにあることを確認する必要があります。

## CVMインスタンスの使用制限

仮想化ソフトウェアのインストールと再仮想化は、現時点ではサポートされていません（VMwareやHyper-Vのインストールなど）。

サウンドカードを使用したり、外部ハードウェアデバイス（USBフラッシュドライブ、外付けディスク、USBトークンなど）をマウントしたりすることはできません。

パブリックゲートウェイは現在、Linuxシステムのみをサポートしています。

## CVMインスタンスの購入制限

各ユーザーが各アベイラビリティゾーンで購入可能な従量課金制のCVMインスタンスの総数は30台～60台です。購入可能数は、CVM購入ページにアクセスして確認してください。

詳細については、[CVMインスタンスの購入制限](#)をご参照ください。

## イメージの使用に関する制限

パブリックイメージ：使用制限なし。

カスタムイメージ：リージョンごとに最大500のカスタムイメージがサポートされます。

共有イメージ：各カスタムイメージは、最大500人のTencent Cloudユーザーと共有することができます。カスタムイメージは、ソースアカウントと同じリージョンのアカウントとのみ共有できます。

詳細については、[イメージの種類](#)をご参照ください。

## ENI 制限

CPUとメモリの構成に基づいて、CVMインスタンスにアタッチできるENIの最大数は、ENIにアタッチできるプライベートIPの最大数とは異なります。ENIと単一のENI IPのクォータ数は以下のとおりです：

**ご注意：**

1つのENI にアタッチする IP の数は、ENIにアタッチできるIPの数の上限を表すのみで、上限に応じてEIPクォータを提供することをお約束するものではありません。アカウントのEIPクォータは、[EIP使用制限](#) に従って提供されます。

CVMインスタンスにアタッチできるENIの数

CVMインスタンスの単一のENIにアタッチできるプライベートIPの数

モデル	インスタンスタイプ	ENIクォータ							
		CPU : 1コア	CPU : 2コア	CPU : 4コア	CPU : 6コア	CPU : 8コア	CPU : 10コア	CPU : 12コア	CPU : 14コア
標準型	標準型 S5	2	4	4	-	6	-	-	-
	標準ストレージ拡張型 S5se	-	-	4	-	6	-	-	-
	標準型 SA2	2	4	4	-	6	-	-	-
	標準型 S4	2	4	4	-	6	-	-	-
	標準ネットワーク最適化型 SN3ne	2	4	4	-	6	-	8	-
	標準型 S3	2	4	4	-	6	-	8	-
	標準型 SA1	2	2	4	-	6	-	-	-
	標準型 S2	2	4	4	-	6	-	8	-
	標準型	2	4	4	-	6	-	8	-

	S1								
High IO型	High IO型IT5	-	-	-	-	-	-	-	-
	High IO型IT3	-	-	-	-	-	-	-	-
メモリ型	メモリ型M5	2	4	4	-	6	-	8	-
	メモリ型M4	2	4	4	-	6	-	8	-
	メモリ型M3	2	4	4	-	6	-	8	-
	メモリ型M2	2	4	4	-	6	-	8	-
	メモリ型M1	2	4	4	-	6	-	8	-
コンピューティング型	コンピューティング型C4	-	-	4	-	6	-	-	-
	コンピューティングネットワーク拡張型CN3	-	-	4	-	6	-	-	-
	コンピューティング型C3	-	-	4	-	6	-	-	-
	コンピューティング型C2	-	-	4	-	6	-	-	-
GPUモデル	GPUコン	-	-	-	-	-	-	-	

	ピュー ティン グ型 GN6								
	GPUコ ン ピュー ティン グ型 GN6S	-	-	4	-	6	-	-	-
	GPUコ ン ピュー ティン グ型 GN7	-	-	4	-	6	-	-	-
	GPUコ ン ピュー ティン グ型 GN8	-	-	-	4	-	-	-	8
	GPUコ ン ピュー ティン グ型 GN10X	-	-	-	-	6	-	-	-
	GPUコ ン ピュー ティン グ型 GN10Xp	-	-	-	-	-	6	-	-
FPGA モデル	FPGAア クセラ レー ション 型FX4	-	-	-	-	-	6	-	-
ビッグ	ビッグ	-	-	-	-	6	-	-	-

データ型	データ型D3								
	ビッグデータ型D2	-	-	-	-	6	-	-	-
	ビッグデータ型D1	-	-	-	-	6	-	-	-
ベアメタル型CVM		ENIをアタッチすることはできません							

モデル	インスタンスタイプ	単一ネットワークカードにプライベートネットワークIPクォータをバインドします							
		CPU : 1コア	CPU : 2コア	CPU : 4コア	CPU : 6コア	CPU : 8コア	CPU : 10コア	CPU : 12コア	CPU : 14コア
標準型	標準型S5	6	10	10	-	20	-	-	-
	標準ストレージ拡張型S5se	-	-	20	-	20	-	-	-
	標準型SA2	6	10	10	-	20	-	-	-
	標準型S4	6	10	10	-	20	-	-	-
	標準ネットワーク最適化型SN3ne	6	10	10	-	20	-	30	-
	標準型S3	6	10	10	-	20	-	30	-
	標準型SA1	メモリ=1G :	10	メモリ=8G :	-	20	-	-	-

		2メモリ >1G : 6		10メモリ =16G : 20					
	標準型 S2	6	10	10	-	20	-	30	-
	標準型 S1	6	10	10	-	20	-	30	-
High IO型	High IO 型IT5	-	-	-	-	-	-	-	-
	High IO 型IT3	-	-	-	-	-	-	-	-
メモリ 型	メモリ 型M5	6	10	10	-	20	-	30	-
	メモリ 型M4	6	10	10	-	20	-	30	-
	メモリ 型M3	6	10	10	-	20	-	30	-
	メモリ 型M2	6	10	10	-	20	-	30	-
	メモリ 型M1	6	10	10	-	20	-	30	-
コン ピュー ティン グ型	コン ピュー ティン グ型C4	-	-	10	-	20	-	-	-
	コン ピュー ティン グネッ トワー ク拡張 型CN3	-	-	10	-	20	-	-	-
	コン ピュー	-	-	10	-	20	-	-	-

	ティン グ型C3								
	コン ピュー ティン グ型C2	-	-	10	-	20	-	-	-
GPU モデル	GPUコ ン ピュー ティン グ型 GN2	-	-	-	-	-	-	-	-
	GPUコ ン ピュー ティン グ型 GN6	-	-	-	-	-	-	-	-
	GPUコ ン ピュー ティン グ型 GN6S	-	-	10	-	20	-	-	-
	GPUコ ン ピュー ティン グ型 GN7	-	-	10	-	20	-	-	-
	GPUコ ン ピュー ティン グ型 GN8	-	-	-	10	-	-	-	30
	GPUコ ン ピュー ティン	-	-	-	-	20	-	-	-

	グ型 GN10X								
	GPUコ ン ピュー ティン グ型 GN10Xp	-	-	-	-	-	20	-	-
FPGA モデル	FPGAア クセラ レー ション 型FX4	-	-	-	-	-	20	-	-
ビッグ データ 型	ビッグ データ 型D3	-	-	-	-	20	-	-	-
	ビッグ データ 型D2	-	-	-	-	20	-	-	-
	ビッグ データ 型D1	-	-	-	-	20	-	-	-
ベアメタル型CVM	ENIをアタッチすることはできません								

## 帯域幅制限

アウトバウンド帯域幅の上限 (ダウストリーム帯域幅) :

次のルールは、2020年2月24日00:00以降に作成されたインスタンスに適用されます。

ネットワーク課金モデル	インスタンス		帯域幅設定範囲 (Mbps)
	インスタンス課金モデル	インスタンスの設定	
トラフィック課金	従量課金インスタンス	ALL	0 - 100
帯域幅課金	従量課金インスタンス	ALL	0 - 100

共有帯域幅	ALL	0 - 2000
-------	-----	----------

次のルールは、2020年2月24日00:00より前に作成されたインスタンスに適用されます。

ネットワーク課金モデル	インスタンス		帯域幅設定範囲 (Mbps)
	インスタンス課金モデル	インスタンスの設定	
トラフィック課金	従量課金インスタンス	ALL	0 - 100
帯域幅課金	従量課金インスタンス	ALL	0 - 100
共有帯域幅	ALL		0 - 2000

インバウンド帯域幅の上限（アップストリーム帯域幅）：

ユーザーが購入した固定帯域幅が10Mbpsを超える場合、Tencent Cloudは購入した帯域幅に等しいパブリックネットワークインバウンド帯域幅を割り当てます。

ユーザーが購入した固定帯域幅が10Mbps未満の場合、Tencent Cloudは10Mbpsのパブリックネットワークインバウンド帯域幅を割り当てます。

## ディスクに関する制限

制限タイプ	制限の説明
エラスティッククラウドディスク機能	2018年5月以降、CVMインスタンスと一緒に購入したデータディスクはすべてエラスティッククラウドディスクとなり、CVMからのアンインストールと再マウントに対応します。この機能は、すべての <a href="#">アベイラビリティゾーン</a> でサポートされています。
クラウドディスクのパフォーマンス制限	I/O仕様は、入力と出力の両方のパフォーマンスに同時に適用されます。 例えば、1TB SSDの最大ランダムIOPSが26,000の場合、読み取りと書き込みの両方のパフォーマンスがこの値に達する可能性があることを意味します。同時に、複数のパフォーマンス制限により、この例では使用するブロックサイズが4KBまたは8KBの場合、IOPSは最大26,000 IOPSに達する可能性があります。ブロックサイズが16KBの場合、I/Oは最大IOPS値に達することはできません (スループットは既に260MB/秒の制限に達しています)。
単一CVMインスタンスにアタッチできるエラスティッククラウド	最大20個。

ディスクの数	
1つのリージョンにおけるスナップショットのクォータ	64 + リージョン内のクラウドディスクの数 * 64 (個)。
クラウドディスクをCVMインスタンスにアタッチするための前提条件	CVM インスタンスとクラウドディスクは、同じアベイラビリティゾーンにある必要があります。
スナップショットロールバックの制限	スナップショットデータは、スナップショットが作成されたクラウドディスクにのみロールバックできます。
スナップショットを使用したクラウドディスクの作成 - タイプ制限	データディスクのスナップショットのみが新しいエラスティッククラウドディスクの作成に使用できます。
スナップショットを使用したクラウドディスクの作成 - サイズ制限	スナップショットを使用して新しいクラウドディスクを作成する場合は、新しいクラウドディスクの容量は、スナップショットのソースディスクより大きくする必要があります。

## セキュリティグループに関する制限

CVMインスタンスは、同じリージョン内のセキュリティグループにのみ関連付けることができます。

セキュリティグループは、あらゆる [ネットワーク環境](#) におけるCVMインスタンスに適用できます。

各ユーザーは各リージョンの各プロジェクト下に最大で50個のセキュリティグループを設定することができます。

セキュリティグループには、最大100個のインバウンドまたはアウトバウンドルールを構成することができます。

1つのCVMインスタンスを複数のセキュリティグループに関連付けることができ、1つのセキュリティグループを複数のCVMインスタンスに関連付けることができます。

クラシックネットワーク上のCVMインスタンスに関連付けられたセキュリティグループは、Tencent Cloudのリレーショナルデータベース（MySQL、MariaDB、SQL Server、PostgreSQL）、NoSQLデータベース（Redis、Memcached）から（またはこれら宛て）のデータパケットをフィルタリングできません。このようなインスタンスのトラフィックをフィルタリングする必要がある場合は、iptablesを使用するか、クラウドファイアウォール製品を購入すると行うことができます。

関連するクォータ制限を下表に示します。

機能説明	制限
セキュリティグループ数	50個/リージョン
セキュリティグループごとのルール数	100件/インバウンド方向、100件/アウトバウンド方向
各セキュリティグループに関連付けることができるCVMインスタンスの数	2000個
各CVMインスタンスに関連付けることができるセキュリティグループの数	5個
各セキュリティグループが参照できるセキュリティグループID数	10個

## VPCに関する制限

リソース	制限（個）
各アカウントの各リージョン内のVPC数	20
各VPC内のサブネット数	100
各VPCに関連付けることができるクラシックネットワークタイプのCVMインスタンスの数	100
各VPC内のルーティングテーブル数	10
各サブネットに関連付けることができるルーティングテーブル数	1
各ルーティングテーブルのルーティングポリシー数	50
各VPCのHAVIPデフォルトクォータ数	10

# 便利な機能

## コンソールのページビューの切り替え

最終更新日：：2023-04-11 15:05:41

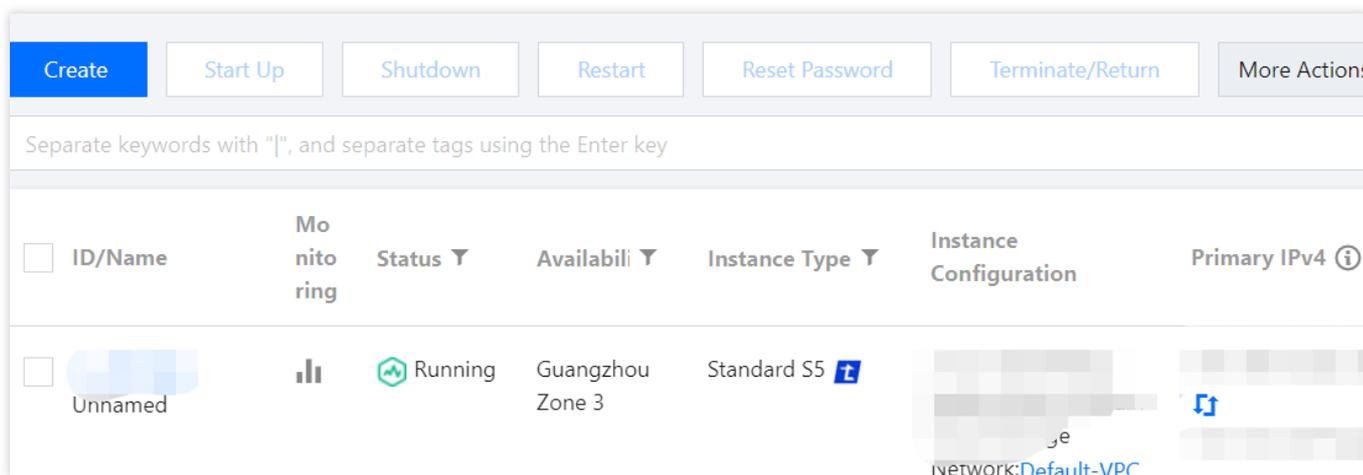
### 概要

CVMコンソールのインスタンスリスト画面は、タブとリストビューをサポートしています。この記事参照して、画面ビューを切り替えることができます。

タブビューには、自動的に検出を開始するインスタンスセルフ検出ツール、インスタンス情報へのすばやいアクセス、高頻度操作用ポータルなどの利点があります。CVMの数が5台以下の場合は、タブビューを使用することをお勧めします。

### 操作手順

1. CVMコンソールにログインし、左側のナビゲーションバーで **インスタンス** を選択します。
2. 「インスタンス」画面で、画面右側にある「**タブビューへ切り替え**」をクリックすると、ビューを切り替えることができます。下図のとおりです。



3. タブビューの切り替えに成功すると、下図のようになります。

タブビューで、インスタンスのヘルスステータス情報、インスタンスの詳細情報をすばやく取得し、インスタンス管理操作を行うことができます。

Instance ID	 
Availability Zone	Guangzhou Zone 3
IP	
Instance Billing Mode	Pay-as-you-go <a href="#">Modify billing mode</a>
Bandwidth billing mode	Bill by traffic <a href="#">Modify billing mode</a>
Instance Configuration	Standard S5 - 2C 4G <a href="#">Adjust Model and Specs</a>
Operating System	TencentOS Server 2.6 (Final) <a href="#">Reinstall the System</a>
Creation Time	2022-03-03 12:12:06

<b>Basic Information</b>	ENI	Public IP	Monitoring	Security Groups
--------------------------	-----	-----------	------------	-----------------

**説明：**

複数のCVMインスタンスがある場合、画面右側にある「[リストビューへ切り替え](#)」をクリックして、リストビューに切り替えることができます。

# インスタンス インスタンスを作成 インスタンス作成ガイドライン

最終更新日：：2023-04-11 17:14:39

このドキュメントでは、基本的な操作から高度なカスタマイズ機能まで、CVMインスタンスを作成する方法について詳しく説明します。

CVM購入ページを介したCVMインスタンスの作成は、最も一般的に使用される方法です。これにより、業務上のニーズに合わせて柔軟に設定項目を選択できます。詳細については、[CVM 購入ページからのインスタンスの作成](#)をご参照ください。

使い慣れたOS、アプリケーションプログラム、またはその他の構成を使用する場合は、最初にカスタムイメージを作成し、インスタンスの作成時にそれを選択して効率を高めることができます。詳細については、[イメージを使用してインスタンスの作成](#)をご参照ください。

現在のインスタンスと同じ構成のインスタンスを購入する場合は、同じ構成のインスタンスを直接作成することができます。詳細については、[同じ構成のインスタンスの購入](#)をご参照ください。

# CVM購入ページからのインスタンスの作成

最終更新日：2023-04-21 15:33:22

## 概要

このドキュメントでは、カスタム設定モードを例として、Tencent Cloud Virtual Machine (CVM) インスタンスを作成する方法について説明します。

## 前提条件

CVMインスタンスを作成する前に、次の手順を完了する必要があります。

[Tencent Cloudアカウントの登録](#) を行い。

ネットワークタイプがVPCのCVMインスタンスを作成するには、ターゲットリージョンで [VPCの作成](#) を行い、VPCのターゲットアベイラビリティーゾーンで [サブネットの作成](#) を行う必要があります。

システムによって自動的に作成されたデフォルトのプロジェクトを使用しない場合は、[プロジェクトの作成](#) を行う必要があります。

システムによって自動的に作成されたデフォルトのセキュリティグループを使用しない場合は、ターゲットリージョンで [セキュリティグループの作成](#) を行い、業務上の必要性を満たすセキュリティグループルールを追加する必要があります。

Linuxインスタンスの作成時にSSHキーペアをバインドしたい場合は、ターゲットプロジェクト下で [SSHキーの作成](#) を行う必要があります。

カスタムイメージを使用してCVMインスタンスを作成する場合は、[カスタムイメージの作成](#) または [イメージのインポート](#) を行う必要があります。

## 操作手順

1. [Tencent Cloud公式サイト](#) にログインし、**製品>コンピューティングとコンテナ>Cloud Virtual Machine** を選択して、**今すぐ購入** をクリックしてCVM購入ページに進みます。

**カスタマイズ設定**：特定のシナリオでの使用に適し、ユーザーが特定のニーズに合わせて簡単にCVMインスタンスを購入するのに役立ちます。

2. 画面の指示に従って次の情報を設定します。

カテゴリー	入力必須/オプション	設定説明

	シ ョ ン	
課金モデル	入力 必須	<p>実際のニーズに応じて選択してください。</p> <p><b>従量課金</b>：CVMインスタンスの柔軟な料金体系であり、eコマースでの買い占めなど、デバイスの需要が瞬間的に大きく変動するシナリオに適しています。</p> <p><b>スポットインスタンス</b>：CVMインスタンスの提供形態の一つであり、ビッグデータコンピューティング、ロードバランシングを使用したオンラインサービス、Webサイトサービスなどのシナリオに適しており、一般的な価格帯は従量課金制インスタンスの10%～20%です。</p> <p>課金モデルの詳細については、<a href="#">課金モデルの説明</a> をご参照ください。</p>
リージョン/アベイラビリティゾーン	入力 必須	<p>リージョン：アクセスレイテンシを最小限に抑え、アクセス速度を向上させるために、エンドユーザーに最も近いリージョンを選択することをお勧めします。</p> <p>アベイラビリティゾーン：実際のニーズに応じて選択してください。複数のCVMを購入する必要がある場合は、異なるアベイラビリティゾーンを選択することで障害復旧効果を実現することをお勧めします。</p> <p>リージョンとアベイラビリティゾーンの選択の詳細については、<a href="#">リージョンとアベイラビリティゾーン</a> をご参照ください。</p>
インスタンス	入力 必須	<p>Tencent Cloudでは、基盤となるハードウェアに基づいて最適化されたさまざまなインスタンスタイプが用意されています。</p> <p>インスタンスの詳細については、<a href="#">インスタンス仕様</a> をご参照ください。</p>
イメージ	入力 必須	<p>Tencent Cloudはパブリックイメージ、カスタムイメージ、共有イメージを提供しています。<a href="#">イメージタイプ</a> をご参照のうえイメージを選択してください。</p>
システムディスク	入力 必須	<p>OSのインストールに使用されます。容量はデフォルトで50GBです。リージョンによって、選択可能なクラウドディスクの種類が異なります。実際の画面の指示に従って選択してください。</p> <p>クラウドディスクの詳細については、「<a href="#">Cloud Disk Types</a>」をご参照ください。</p>
データディスク	オプ ショ ン	<p>CVMインスタンスのストレージ容量を拡張し、効率的で信頼性の高いストレージデバイスを提供するために使用されます。データディスクはデフォルトでは追加されません。</p> <p>クラウドディスクの詳細については、「<a href="#">Cloud Disk Types</a>」をご参照ください。</p>
定期スナップショット	オプ ショ ン	<p>システムディスクまたはデータディスクに定期スナップショットポリシーを設定できます。定期スナップショットの詳細については、<a href="#">定期スナップショット</a> をご参照ください。</p>
数量	入力 必須	<p>購入が必要なCVMの数を示します。</p>

3. 次へ：ネットワークとホストの設定をクリックして、インスタンス設定ページに入ります。

4. 画面の指示に従って次の情報を設定します。

カテゴリー	入力必須/オプション	設定説明
ネットワーク	入力必須	<p>Tencent Cloud上に構築された、論理的に隔離されているネットワークスペースを示します。1つのVirtual Private Cloud(VPC)は、少なくとも1つのサブネットで作成されます。システムは各リージョンにデフォルトのVPCとサブネットを提供します。</p> <p>既存のVPC/サブネットが要件を満たしていない場合は、VPCコンソールでVPCまたはサブネットを作成できます。</p> <p><b>注：</b> デフォルトでは、同じVPC内のリソースはプライベートネットワークを介して相互接続されます。</p> <p>CVMインスタンスを購入するときは、CVMインスタンスとそのサブネットが同じアベイラビリティゾーンにあることを確認してください。</p>
パブリックIP	オプション	<p>CVMインスタンスがパブリックネットワークにアクセスする必要がある場合は、CVMにパブリックIPを割り当てる必要があります。CVMインスタンスの作成時にパブリックIPを割り当てるか、またはCVM作成後に <a href="#">EIP</a> を設定できます。</p> <p><b>注意：</b> 無料で割り当てられた独立したパブリックIPアドレスはインスタンスからバインド解除できません。このIPアドレスをバインド解除するには、このパブリックIPをEIPに変換して再びバインド解除を行ってください。EIPの詳細については、<a href="#">Elastic IP (EIP)</a> をご参照ください。</p> <p>以下の2つのケースについては、現時点では独立したパブリックIPアドレスの割り当てはサポートしておりません。詳細については、実際の購入ページをご参照ください。</p> <p>IPリソースは売り切れました リソースは一部地域でのみご利用いただけます</p>
帯域課金モデル	入力必須	<p>Tencent Cloudは以下の2つの異なるネットワーク課金モデルが用意されています。実際のニーズに応じて0Mbpsより大きい値を設定してください。</p> <p><b>トラフィック使用量による課金：</b>実際に使用されているトラフィックに基づいて課金されます。ピーク帯域幅を制限することで、予期せぬトラフィックによって生じる料金を回避することができ、瞬時帯域幅がこの値を超えるとパケットロスが発生します。この課金モデルは、ネットワークトラフィックが大きく変動するシナリオに適しています。</p> <p><b>共有帯域幅パッケージによる課金：</b>業務中のパブリックネットワークのトラフィックピークが異なる時間帯に分散しているとき、共有帯域幅パッケージによって帯域幅の集約課金を実現できます。これは、大規模な業務やパブリックネットワークのさまざまなインスタンスがトラフィックピークシフトを形成できるシナリオに適しています。現在、共有帯域幅パッケージはベータ版テスト段階です。ご利用を希望される場合は、<a href="#">チケットを提出</a>してください。</p> <p>詳細については、<a href="#">パブリックネットワーク課金モデル</a> をご参照ください。</p>

帯域幅の値	オプション	必要に応じて、CVMインスタンスのパブリックネットワーク帯域幅上限を設定することができます。詳細については、 <a href="#">パブリックネットワーク帯域幅上限</a> をご参照ください。
セキュリティグループ	入力必須	<p>使用できるセキュリティグループがない場合は、セキュリティグループの新規作成を選択できます。</p> <p>使用できるセキュリティグループがすでにある場合は、既存のセキュリティグループを選択できます。</p> <p>セキュリティグループの詳細については、<a href="#">セキュリティグループ</a>をご参照ください。</p>
タグ	オプション	必要に応じてタグをインスタンスに追加し、クラウドリソースの分類、検索および集約に使用することができます。詳細については、 <a href="#">タグ</a> をご参照ください。
インスタンス名	オプション	<p>ユーザーが定義して、作成する必要があるCVMの名前を示します。</p> <p>インスタンス名を定義しない場合は、インスタンス作成後のインスタンス名は「名前無し」になります。</p> <p>インスタンス名を定義する場合は、このインスタンス名称は128文字以内に制限する必要があります。さらに <a href="#">一括連続命名または文字列パターン命名</a> することができます。</p> <p><b>注：</b>この名前はコンソールにのみ表示されます。CVMインスタンスのホスト名ではありません。</p>
ログイン方法	入力必須	<p>ユーザーがCVMにログインするための方法を設定します。実際のニーズに応じて設定してください。</p> <p><b>パスワードの設定：</b>インスタンスのログインパスワードをカスタマイズします。</p> <p><b>キーの関連付け（Linuxインスタンスのみサポート）：</b>SSHキーをインスタンスと関連付けると、SSHキーを介してより安全にCVMにログインできます。使用できるキーがない場合、または既存のキーが適切でない場合は、「今すぐ作成」をクリックしてキーを作成できます。SSHキーの詳細については、<a href="#">SSHキー</a>をご参照ください。</p> <p><b>パスワードの自動生成：</b>自動生成されたパスワードは <a href="#">サイト内メール</a> に送信されます。</p>
インスタンスの終了保護	オプション	デフォルトでは無効になっています。必要に応じて有効にすることができます。「インスタンスの終了保護」機能を有効化するとコンソールまたはAPI経由でインスタンスを終了することはできません。詳細については、 <a href="#">インスタンスの終了保護の有効化</a> をご参照ください。
セキュリティ強化	オプション	<b>Anti-DDoS</b> と <b>Cloud Workload Protection</b> 機能はデフォルトで有効になっています。ユーザーがCVMセキュリティ保護システムを構築してデータ漏洩を防ぐのに役立ちます。
TCOP	オプション	TCOP機能はデフォルトで有効になっています。コンポーネントをインストールすること

	ショ ン	で、CVM監視指標を取得し、それらを監視アイコン形式で表示できるほか、カスタムアラームしきい値などの設定がサポートされています。さらに、3次元CVMデータ監視、インテリジェントなデータ分析、リアルタイムな障害アラート、およびデータレポートのカスタマイズ構成などの機能も提供します。これにより、ユーザーは業務とCVMのヘルス状態を正確に把握できます。
高度な設定	オプ ショ ン	<p>実際のニーズに応じてインスタンスにより多くの設定を行うことができます。</p> <p><b>ホスト名</b>：ユーザーは、CVM OS内のコンピュータ名をカスタマイズできます。CVMインスタンスが作成されたら、CVMにログインしてホスト名を表示できます。</p> <p><b>所属プロジェクト</b>：デフォルトのプロジェクトが選択されています。必要に応じて既存のプロジェクトを選択して、さまざまなCVMインスタンスを管理するために使用されます。</p> <p><b>CAMロール</b>：ロールを設定した後にロールによってCVMにTencent Cloud内のサービス、操作およびリソースのアクセス権限を付与します。詳細については、<a href="#">インスタンスロールの管理</a>をご参照のうえ設定してください。</p> <p><b>プレイスメントグループ</b>：必要に応じてインスタンスをプレイスメントグループに追加し、ビジネスの可用性を向上させることができます。詳細については、<a href="#">プレイスメントグループ</a>をご参照のうえ設定してください。</p> <p><b>カスタムデータ</b>：カスタムデータを指定することでインスタンスを設定します。設定されたスクリプトは、インスタンスの起動時に実行されます。一度に複数のCVMインスタンスを購入すると、カスタムデータはすべてのCVMインスタンスで実行されます。Linux OSではShell形式、Windows OSではPowerShell形式がサポートされており、最大16KBのオリジナルデータが保存可能です。詳細については、<a href="#">カスタムデータ</a>をご参照ください。注：カスタムデータの設定は、cloud-initサービスを使用する特定のパブリックイメージにのみ適用されます。詳細については、<a href="#">Cloud-Init</a>をご参照ください。</p>

5. **次へ：設定情報の確認**をクリックして、設定情報の確認ページに進みます。

6. 購入したCVM情報と各設定の料金明細を確認します。

7. 「『Tencent Cloudサービス利用規約』に同意する」を読んでチェックを入れます。

8. 実際のニーズに応じて、次の操作を実行できます。

**起動テンプレートとして保存の選択**：このインスタンスの設定を起動テンプレートとして保存します。起動テンプレートを使用してインスタンスをすばやく作成できます。詳細は、[インスタンス起動テンプレートの管理](#)をご参照ください。

**API Explorerベストプラクティススクリプトの作成**を選択：選択した設定に対応するOpenAPIベストプラクティススクリプトコードを発行して、同じ設定のCVMを購入する際に使用できるように保存することができます。詳細については、[インスタンスを作成するためのAPI Explorerのベストプラクティススクリプトの生成](#)をご参照ください。

9. **今すぐ購入またはアクティブ化**をクリックし、支払いを完了します。

支払いが完了すると、[CVMコンソール](#)にアクセスし、お客様のCVMを確認することができます。

CVMインスタンス名、パブリックIPアドレス、プライベートIPアドレス、ログイン名、初期ログインパスワードなどの情報は、[サイト内メール](#)の形でアカウントに送信されます。これらの情報を使用してインスタンスへのロ

グイン、管理ができます。また、CVMのセキュリティを確保するためにできるだけ早くCVMのログインパスワードを変更してください。

# カスタムイメージによるインスタンスの作成

最終更新日：2023-04-11 18:06:06

## 概要

カスタムイメージを使用して同じOS、アプリケーション、およびデータを有するCVMインスタンスを簡単に作成し、業務またはデリバリー効率を向上させることができます。このドキュメントでは、カスタムイメージを使用してインスタンスを作成する方法について説明します。

## 前提条件

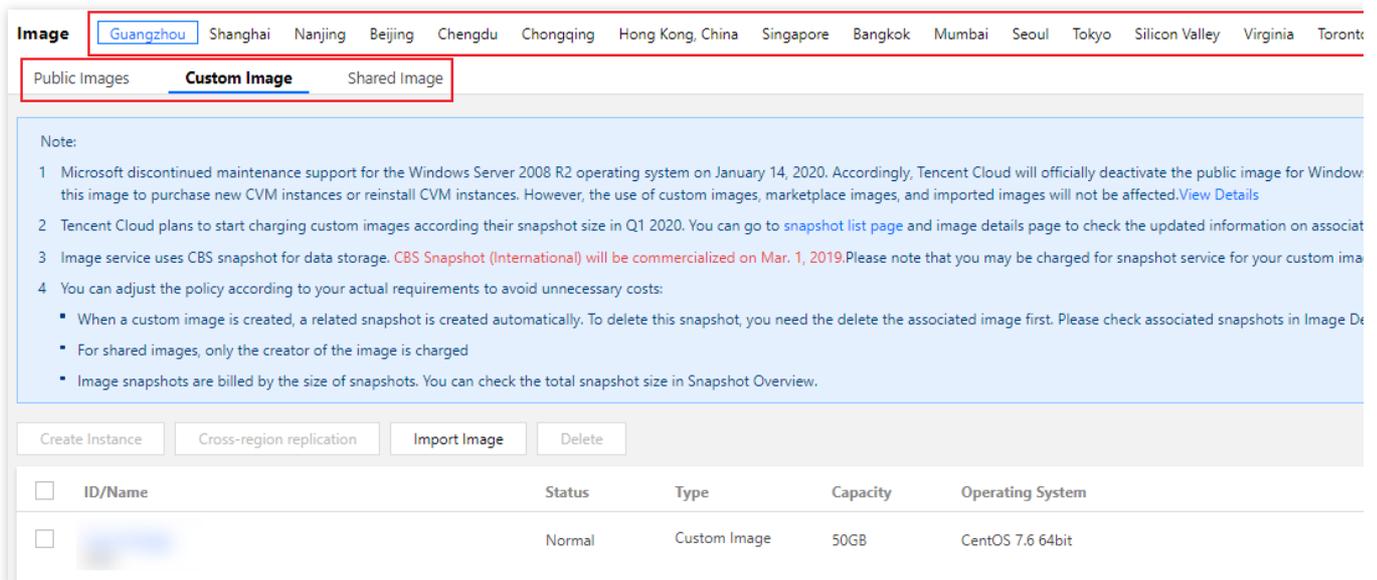
インスタンスを作成する必要があるアカウントとリージョンにすでにカスタムイメージが作成されている。まだカスタムイメージを作成されていない場合は、以下の方法を参考にしてください。

イメージにある状態	ソリューション
ローカルコンピューターまたはその他のプラットフォーム上にイメージがある	ローカルコンピューターまたはその他のプラットフォーム上にイメージがあるローカルコンピューターまたは他のプラットフォームのシステムディスクイメージファイルをCVMインスタンスのカスタムイメージにインポートします。詳細については、 <a href="#">イメージのインポートの概要</a> をご参照ください。
カスタムイメージはありませんが、テンプレートとして使用できるインスタンスがある	詳細な操作については、 <a href="#">カスタムイメージの作成</a> をご参照ください。
その他のリージョンにカスタムイメージがある	インスタンスを作成するターゲットリージョンにカスタムイメージをコピーします。詳細については、 <a href="#">イメージのコピー</a> をご参照ください。
その他のアカウントにカスタムイメージがある	インスタンスを作成するアカウントとカスタムイメージを共有します。詳細については、 <a href="#">カスタムイメージの共有</a> をご参照ください。

## 操作手順

- [CVMコンソール](#) にログインします。
- 左側のナビゲーションメニューで [イメージ](#) をクリックし、イメージ管理ページに進みます。

3. イメージページの上部でリージョンを選択します。
4. イメージソースに基づいてタブを選択し、イメージリストページに進みます。  
パブリックイメージタブ：パブリックイメージページに進みます。  
カスタムイメージタブ：カスタムイメージページに進みます。  
共有イメージタブ：共有イメージページに進みます。
5. ターゲットイメージの操作列で、**インスタンスの作成**をクリックします。



6. ポップアップしたダイアログボックスで、**OK**をクリックします。
7. 画面上の指示に従って、インスタンスを構成および作成します。  
リージョンフィールドとイメージフィールドが自動的に入力されます。必要に応じてインスタンスのその他の情報を設定してください。詳細については [CVM購入ページからのインスタンスの作成](#) をご参照ください。

#### 説明：

選択したカスタムイメージに1個或いは複数個のデータディスクスナップショットが含まれている場合、システムは自動的にこれらのスナップショットを基に同じ数量のクラウドディスクをデータディスクとして作成し、各クラウドディスクの容量は対応するスナップショットと同じになります。クラウドディスクの容量を増やすことはできますが、減らすことはできません。

## 関連ドキュメント

[RunInstances API](#) を呼び出して、カスタムイメージを使用してインスタンスを作成することもできます。

#### 説明：

CVMインスタンス全体のイメージを使用してインスタンスを作成する場合は、まず [DescribeImages API](#) を呼び出してイメージに関連付けられているスナップショットIDを取得してから、[RunInstances API](#) を呼び出してスナップショットIDパラメータを渡します。そうしないと、作成されたクラウドディスクと対応するスナップショットIDが

一致せず、スナップショットデータをロールバックできず、データディスク上にデータがないため、正常にマウントできません。

# 同じ構成のインスタンスの購入

最終更新日：：2023-04-13 10:45:05

## 概要

CVMコンソールが提供する「同じ構成の購入」または「インスタンス起動テンプレート」機能を使用して、CVMインスタンスのすばやい作成、時間の節約、特定シナリオでの水平スケーリング効率の向上を実現できます。

## 操作手順

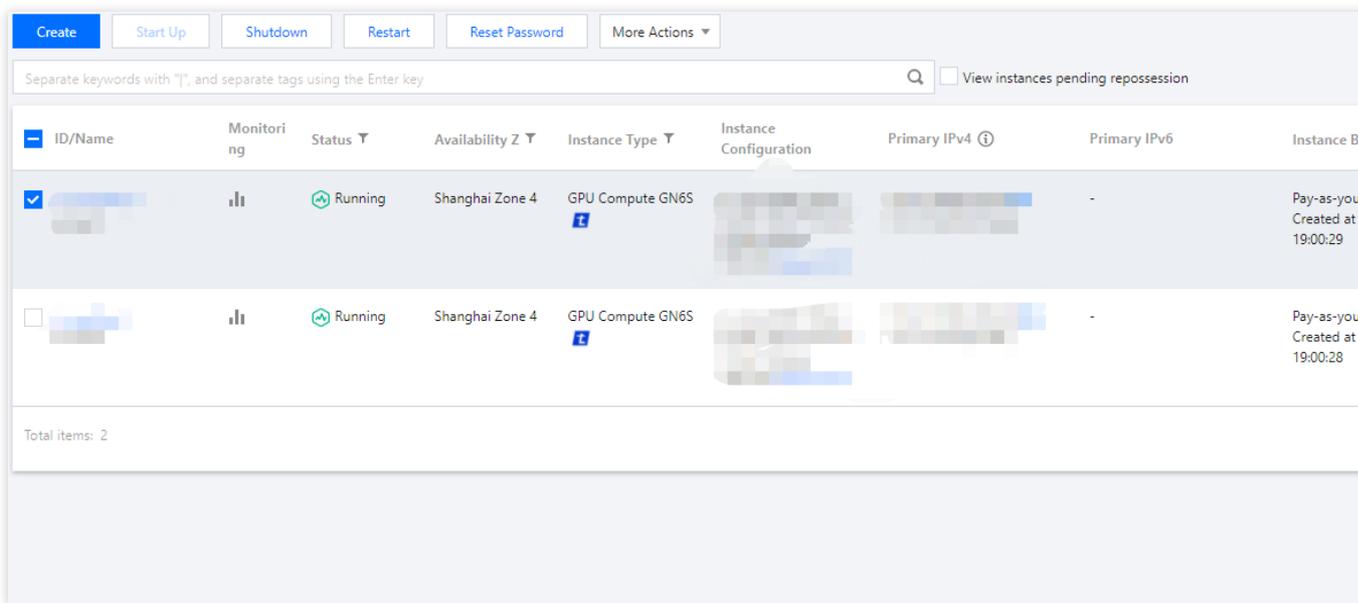
### 同じ構成のインスタンスの作成

1. [CVMコンソール](#) にログインします。
2. インスタンス管理画面の上方でリージョンを選択します。
3. インスタンスの管理画面で、実際に使用されているビューモードに従って操作します。

リストビュー

タブビュー

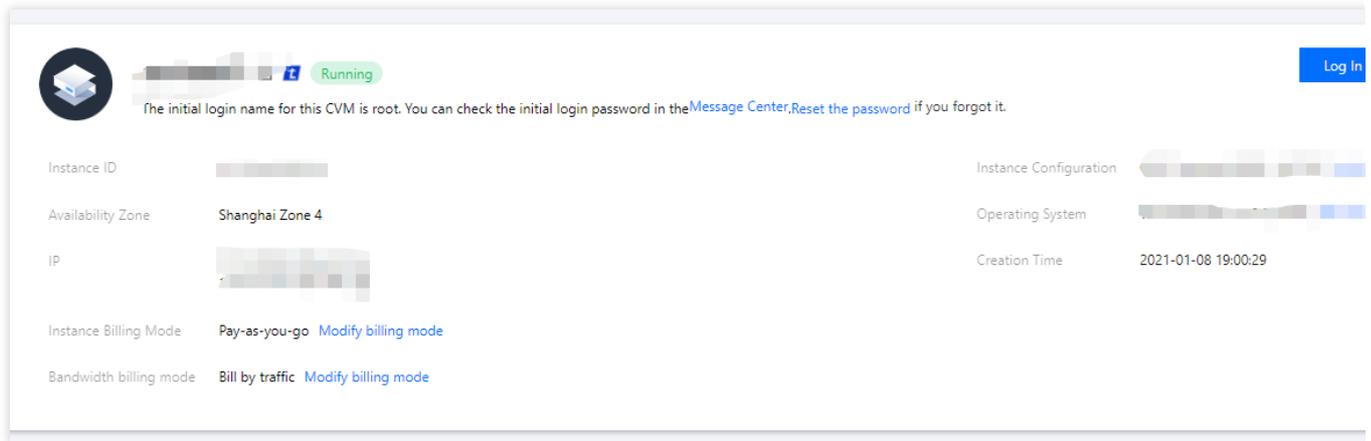
ターゲットインスタンスを見つけて、下図に示すように、[操作]列でさらに > 同じ構成の購入 をクリックします。



ID/Name	Monitoring	Status	Availability Z	Instance Type	Instance Configuration	Primary IPv4	Primary IPv6	Instance Billing
<input checked="" type="checkbox"/>		Running	Shanghai Zone 4	GPU Compute GN6S			-	Pay-as-you-Created at 2 19:00:29
<input type="checkbox"/>		Running	Shanghai Zone 4	GPU Compute GN6S			-	Pay-as-you-Created at 2 19:00:28

Total items: 2

ターゲットインスタンスのページで、下図に示すように、画面の右上隅にある **その他の操作 > 同じ構成の購入** をクリックします。



4. CVMの購入数量を設定し、自動選択したその他の構成を確認します。

実際のニーズに応じて、購入するCVMのパラメータ設定を調整することもできます。

5. 「『Tencent Cloudサービス利用規約』と『返金ルール』に同意する」、または「『Tencent Cloudサービス利用規約』に同意する」を読んでチェックを入れます。

6. **今すぐ購入**または**アクティブ化**をクリックし、支払いを完了します。

### インスタンス起動テンプレートを使用したインスタンスの作成

既存のインスタンス起動テンプレートを使用して、インスタンスをすばやく作成できます。詳細については、[インスタンス起動テンプレートを使用したインスタンスの作成](#)をご参照ください。

# インスタンスを作成するためのAPI Explorer のベストプラクティススクリプトの生成

最終更新日：：2023-04-11 18:17:50

## 概要

Tencent Cloudは、CVM購入ページで選択した構成に対応するインスタンスを作成するための OpenAPIベストプラクティスのスクリプトコードの生成をサポートしています。コードを保存して、同じ構成のCVMインスタンスを購入できます。

## 前提条件

Tencent Cloud公式ウェブサイトログインし、[CVMインスタンスのカスタム設定購入ページ](#)に入ります。必要に応じてCVMインスタンスの設定を選択し、設定情報の確認ページに入ります。パラメータの設定方法については、[CVM購入ページからのインスタンスの作成](#)をご参照ください。

## 操作手順

1. 設定情報の確認ページで、API Explorerのベストプラクティススクリプトの生成をクリックします。次の図に示すように：

### Custom Configuration

**1. Select Model**      **2. Complete Configuration**      **3. Confirm Configuration**

Please make sure port 22 and the ICMP protocol are allowed in the current security group. Otherwise, you will not be able to remotely log in to or ping the CVM. You have not set the CVM password. An auto-generated password will be sent to your internal message. You can reset your password on CVM console. [View](#)

▼ **Region and model** Guangzhou Zone 4; S5.SMALL2 (Standard S5, 1-core 2 GB)

▼ **Image** Public image; CentOS 8.0 64bit

▼ **Storage and Bandwidth** 50 GB system disk; By Traffic: 1Mbps

▼ **Security Groups** [blurred]

▼ **Set Information** Login by password (random)

▼ **Advanced Settings**

---

Selected Model S5.SMALL2(Standard S5, 1-core, 2 GB)      Configuration Fee  USD/hr (Billing Details)

Amount       Network Fee  SD/GB

2. 「API Explorerのベストプラクティススクリプトの生成」ダイアログボックスには、次の情報が表示されます。次の図に示すように：

## Generate API Explorer Reusable Scripts

This feature will generate OpenAPI best practices based on your configuration. [View Details](#)

The instance password is not displayed here for security reasons. Please modify it by yourself.

### API Workflow

Legend:  Task Execution API \*Required

- RunInstances Creates one or more CVM instances
  - InstanceChargeType: "POSTPAID\_BY\_HOUR"
  - Region: "ap-guangzhou"
  - Placement: {"Zone": "ap-guangzhou-4", "ProjectId": 0}
  - VirtualPrivateCloud: {"AsVpcGateway": false, "Vpclid": "..."}
  - InstanceType: "S5.SMALL2"
  - ImageId: "img-25szkc8t"
  - SystemDisk: {"DiskSize": 50, "DiskType": "CLOUD\_PREMIUM"}
  - InternetAccessible: {"InternetMaxBandwidthOut": 1, "PublicIp": "..."}

### API Script

Java	Python
Java	
1	<code>import com.tencent</code>
2	<code>import com.tencent</code>
3	<code>import com.tencent</code>
4	<code>import com.tencent</code>
5	
6	<code>import com.tencent</code>
7	<code>import com.tencent</code>
8	
9	<code>public class RunIns</code>
10	<code>{</code>
11	<code>    public static v</code>
12	<code>        try{</code>
13	
14	<code>            Credent</code>
15	
16	<code>        ...</code>

**APIワークフロー：**選択した設定に基づいて、RunInstances インターフェースの説明と実際のパラメータを提供します。そのうち、\* でマークされたパラメータは、インターフェースの必須パラメーターです。データにカーソルを合わせると、完全に表示されます。

**APIスクリプト：**JavaおよびPythonプログラミング言語でコードを生成します。必要に応じて[Java]または[Python]タブを選択し、右上隅にある**Copy Script**をクリックしてスクリプトコードを取得します。保存したコードを使用して、同じ設定のCVMインスタンスを購入できます。

#### 説明：

セキュリティ上の理由から、インスタンスのパスワードはページまたはスクリプトコードに表示されません。パスワードはご自身で変更してください。

API Explorerプラクティススクリプトは、有効期限の一括設定をサポートしていません。インスタンスの作成後に個別に設定できます。

# モデル比較の有効化

最終更新日：2024-07-09 15:00:58

## 操作シーン

CVM を購入する際には、**モデル比較ツール**を有効にし、複数のモデルの構成パラメータ、性能指標、価格などを水平比較することができます。その同時に、選択したモデルの構成に応じて、最適なモデルをインテリジェント的に推薦し、適切な CVM を効率的に購入するお手伝いをします。

## 操作手順

1. Tencent Cloud の公式サイトにログインし、CVM の [カスタム構成購入ページ](#)に入ります。
2. **モデル比較機能**を有効にし、下図に示すように、モデルの仕様を追加します。

The screenshot shows the 'Instance configurations' page. At the top, there are filters for 'All CPU cores' and 'All MEMs', a search bar, and a 'Hide sold out specifications' checkbox. Below these are tabs for 'Architecture' (X86 computing, Heterogeneous Computing) and 'Instance family' (Standard, MEM-optimized, Compute, High IO, Preferential). The 'Model' section has tabs for 'All models', 'Standard SA5', 'Standard S8', 'Standard SA4', 'Standard S6', and 'Standard S5' (which is selected and has a 'Recommend' badge). A 'Selected model' box shows 'Selected model: S5.MEDIUM2 (Standard S5, 2C2G)'. A 'Comparison Enabled' button is highlighted with a red box. Below this is a table of instance specifications:

Add	Instance	Specifications	vCPU	MEM	CPU Clock Spee...	Processor	Private net...	Reference fee...
<input checked="" type="checkbox"/>	Standard S5 (23% off) Adequate Inventory	S5.MEDIUM2	2Core	2GB	2.5GHz/3.1GHz	Intel Xeon Cascade Lake 8255...	1.5Gbps	
<input type="checkbox"/>	Standard S5 (23% off) Adequate Inventory	S5.MEDIUM4	2Core	4GB	2.5GHz/3.1GHz	Intel Xeon Cascade Lake 8255...	1.5Gbps	
<input type="checkbox"/>	Standard S5 (23% off) Adequate Inventory	S5.MEDIUM8	2Core	8GB	2.5GHz/3.1GHz	Intel Xeon Cascade Lake 8255...	1.5Gbps	
<input type="checkbox"/>	Standard S5 (23% off) Low Inventory View more	S5.LARGE4	4Core	4GB	2.5GHz/3.1GHz	Intel Xeon Cascade Lake 8255...	1.5Gbps	
<input type="checkbox"/>	Standard S5 (23% off) Adequate Inventory	S5.LARGE8	4Core	8GB	2.5GHz/3.1GHz	Intel Xeon Cascade Lake 8255...	1.5Gbps	

Total 21 items

3. **比較開始**をクリックすると、下図に示すように、モデル比較ページがポップアップ表示されます。

The screenshot displays the 'Selected Models' comparison tool. At the top, three models are selected: S5.MEDIUM2 (2 cores, 2 GB), SAS.MEDIUM4 (2 cores, 4 GB), and SAS.4XLARGE32 (16 cores, 32 GB). The 'Model Comparison Settings' panel on the left is active, with 'Highlight Differences' checked and 'Hide Identical Items' unchecked. The 'Recommend' panel on the right suggests 'SAS.MEDIUM4' as the best model. The main table provides a detailed comparison of specifications across three categories: Basic Information, Compute, and Network. The 'More Information' section lists 'Other Availability Zones in the Current Region' for each model.

Category	S5.MEDIUM2	SAS.MEDIUM4	SAS.4XLARGE32
<b>Basic Information</b>			
Availability Zone	Seoul Zone 1	Seoul Zone 1	Seoul Zone 1
Architecture	X86 computing	X86 computing	X86 computing
Instance Family	Standard S5	Standard SAS	Standard SAS
Instance Specifications	S5.MEDIUM2	SAS.MEDIUM4	SAS.4XLARGE32
vcpu	2 cores	2 cores	16 cores
MEM	2GB	4GB	32GB
<b>Compute</b>			
Processor	Intel Xeon Cascade Lake E255C/Intel Xeon Cooper Lake	AMD EPYC Bergamo	AMD EPYC Bergamo
CPU Clock Speed/Turbo Boost	2.5GHz/3.3GHz	-/3.3GHz	-/3.3GHz
GPU	-	-	-
GPU memory	-	-	-
Whether to support specifying the number of threads bound with CPU	Supported	Supported	Supported
<b>Network</b>			
Private Network Broadband	15Gbps	15Gbps	5Gbps
Packets in/out	800k PPS	250k PPS	1400k PPS
Whether to support IPv6	Supported	Supported	Supported
<b>Image</b>			
Public image	OpenCloudOS, TencentOS, CentOS, Windows, Ubuntu, Debian, CentOS Stream, Red Hat, AlmaLinux, CoreOS, openSUSE, Rocky Linux, FreeBSD, Fedora	OpenCloudOS, TencentOS, CentOS, Windows, Ubuntu, Debian, CentOS Stream, Red Hat, AlmaLinux, CoreOS, openSUSE, Rocky Linux, FreeBSD, Fedora	OpenCloudOS, TencentOS, CentOS, Windows, Ubuntu, Debian, CentOS Stream, Red Hat, AlmaLinux, CoreOS, openSUSE, Rocky Linux, FreeBSD, Fedora
<b>Data Storage</b>			
Supported system disk types	Balanced SSD, Enhanced cloud SSD, Premium cloud disk, Cloud SSD	Balanced SSD, Enhanced cloud SSD	Enhanced cloud SSD, Balanced SSD
Supported data disk types	Enhanced cloud SSD, Balanced SSD, Premium cloud disk, Cloud SSD	Enhanced cloud SSD, Balanced SSD	Enhanced cloud SSD, Balanced SSD
Whether to support NVME disk	Not supported	Not supported	Not supported
Number of data disks that can be mounted	20	20	20
Data Backup	Supported	Supported	Supported
<b>More Information</b>			
Other Availability Zones in the Current Region	Seoul Zone 2	-	-
Other Regions/Availability Zones	Guangzhou: Guangzhou Zone 3, Guangzhou Zone 4, Guangzhou Zone 6, Guangzhou Zone 7 Shanghai: Shanghai Zone 2, Shanghai Zone 4, Shanghai Zone 5, Yun Rong Technology CDZ Shanghai Zone 1 Nanjing: Nanjing Zone 1, Nanjing Zone 3 Hong Kong (China): Hong Kong Zone 2, Hong Kong Zone 3 Taiwan (China): Taipei Zone 1 Beijing: Beijing Zone 3, Beijing Zone 5, Beijing Zone 6, Beijing Zone 7 Singapore: Singapore Zone 1, Singapore Zone 3, Singapore Zone 4, GRM CDZ Singapore Zone 1 Bangkok: Bangkok Zone 2 Jakarta: Jakarta Zone 1, Jakarta Zone 2 Silicon Valley: Silicon Valley Zone 1, Silicon Valley Zone 2 Chengdu: Chengdu Zone 1, Chengdu Zone 2 Chongqing: Chongqing Zone 1 Frankfurt: Frankfurt Zone 1, Frankfurt Zone 2 Tokyo: Tokyo Zone 1, Tokyo Zone 2 Mumbai: Mumbai Zone 2 Virginia: Virginia Zone 2 Sao Paulo: Sao Paulo Zone 1	Guangzhou: Guangzhou Zone 6, Guangzhou Zone 7 Shanghai: Shanghai Zone 5, Shanghai Zone 8 Nanjing: Nanjing Zone 1, Nanjing Zone 3 Hong Kong (China): Hong Kong Zone 2, Hong Kong Zone 3 Beijing: Beijing Zone 6, Beijing Zone 7, Beijing Zone 8 Singapore: Singapore Zone 2, Singapore Zone 3, Singapore Zone 4 Jakarta: Jakarta Zone 2 Silicon Valley: Silicon Valley Zone 2 Chengdu: Chengdu Zone 1 Frankfurt: Frankfurt Zone 1, Frankfurt Zone 2 Tokyo: Tokyo Zone 2 Virginia: Virginia Zone 1, Virginia Zone 2	Guangzhou: Guangzhou Zone 6, Guangzhou Zone 7 Shanghai: Shanghai Zone 5, Shanghai Zone 8 Nanjing: Nanjing Zone 1, Nanjing Zone 3 Hong Kong (China): Hong Kong Zone 2, Hong Kong Zone 3 Beijing: Beijing Zone 6, Beijing Zone 7 Singapore: Singapore Zone 2, Singapore Zone 3 Jakarta: Jakarta Zone 2 Silicon Valley: Silicon Valley Zone 2 Chengdu: Chengdu Zone 1, Frankfurt Zone 2 Tokyo: Tokyo Zone 2 Virginia: Virginia Zone 1, Virginia Zone 2

複数のモデルを追加し、すべてのパラメータを水平比較することができます。

同じ項目を非表示にし、異なる項目を強調することができます。

選択したモデルに応じて最適なモデルをインテリジェント的に推薦します。

ローカルでのアーカイブと共有のために、共有比較結果をエクスポートすることができます。

4. 購入をクリックします。CVM の購入ページに入り、情報を設定します。

# インスタンス起動テンプレートの管理

最終更新日：：2024-03-14 14:41:10

## 操作ケース

インスタンス起動テンプレートには、Cloud Virtual Machine (CVM) インスタンス作成に必要なコンフィギュレーション情報（インスタンスパスワードを除く）が保存されており、指定したインスタンス起動テンプレートを使用してインスタンスを素早く作成し、効率性と操作性を向上させることができます。この文書では、迅速なインスタンス作成のために、CVM コンソールからインスタンス起動テンプレートを作成、管理、使用方法について説明します。

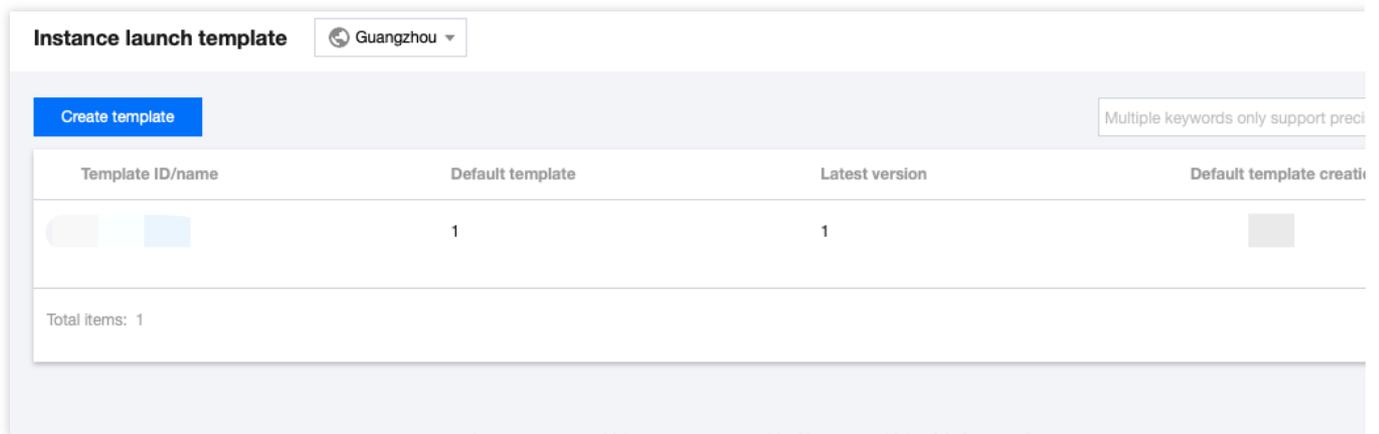
## 使用説明

インスタンス起動テンプレートの作成に成功した後に、コンフィギュレーションを変更することができません。インスタンス起動テンプレートは、1つ以上のバージョンを作成し、各バージョンに異なるコンフィギュレーション情報を設定することができます。インスタンス起動テンプレートを使用してインスタンスを作成する時に使用されるデフォルトのバージョンを指定することができます。

## 操作手順

### インスタンステンプレートの作成と表示

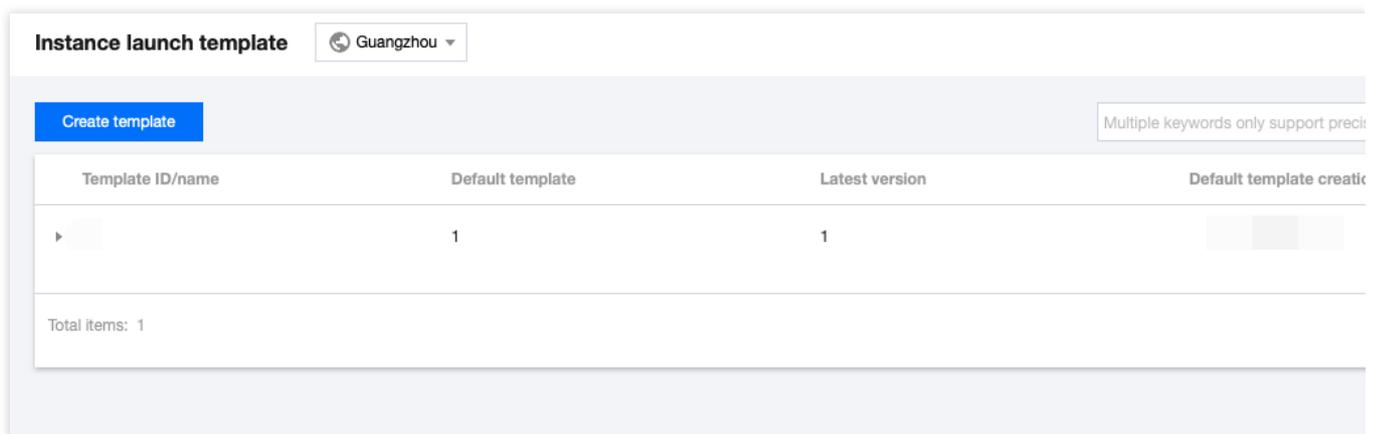
- [Cloud Virtual Machine コンソール](#) にログインし、左側のナビゲーションバーで **インスタンス起動テンプレート** を選択します。
- インスタンス起動テンプレートページで、**テンプレート新規作成** をクリックします。
- インスタンス起動テンプレートの新規作成ページに入り、**テンプレート名** 及び **テンプレート説明** をカスタマイズして入力することができます。その他のコンフィギュレーションは [購入ページからインスタンスを作成する](#) を参照して設定してください。
- コンフィギュレーション情報の確認** のステップで、『**Tencent Cloud サービス契約**』と『**購入に関する注意事項**』を読み、同意するチェックボックスにチェックを入れ、\*\* **今すぐ作成** をクリックすればよいです。作成に成功すると、コンソールでインスタンス起動テンプレートを確認できます。下図のとおりです。



テンプレート ID をクリックすると、テンプレートの詳細ページに移動して詳細情報を表示できます。

## インスタンステンプレートバージョンの作成

1. インスタンス起動テンプレートページで、バージョンを新規作成するテンプレートが所在する行の右側にあるバージョンの**新規作成**を選択します。下図のとおりです。



2. インスタンス起動テンプレートの新規作成ページに入り、[購入ページからインスタンスを作成する](#)を参照して設定してください。

3. コンフィギュレーション情報の確認\*\*のステップで、『Tencent Cloud サービス契約』と『購入に関する注意事項』を読み、同意するチェックボックスにチェックを入れます。

オリジナルコンフィギュレーションの比較を選択し、ポップアップ表示される「オリジナルコンフィギュレーションの比較」ウィンドウで、新しいバージョンとオリジナルインスタンス起動テンプレートの違いを確認します。下図のとおりです。

### Instance Startup Template

1 Select basic configurations 2 Configure network and host 3 Confirm configuration

#### Selected configurations

**Basic and instance configurations**

CVM billing mode	Monthly subscription	Region	Guangzhou	Availability zone	
Instance	SA5.LARGE16 (Standard SA5, 4C16G)	Image		System disk	
Data disk	Not set				

**Network and security group**

Network		Subnet		Public IP	
Bandwidth billing mode		Line type		Security group	

**Other settings** SSH key pair

[Generate API Explorer best practice scripts](#)

Auto-renewal  When there is sufficient balance in the account and the device expires, monthly Auto-renewal ⓘ  
After purchase, you can modify the automatic renewal cycle in the console. [Configure automatic renewal](#) ⓘ  
Automatic renewal takes precedence over voucher deduction. [Voucher overview](#) ⓘ

Terms and Agreement  I have read and agree to "Tencent Cloud Service Terms", "Refund Policy"

Selected SA5.LARGE16 (Standard SA5, 4C16G) Period 1 month Quantity - 1 +

4. 間違いがないことを確認したら、**今すぐ作成**をクリックすればよいです。

作成に成功した後、**インスタンス起動テンプレート**ページで、テンプレートが所在する行の前にある



をクリックすると、展開されたリストでバージョンを表示することができます。

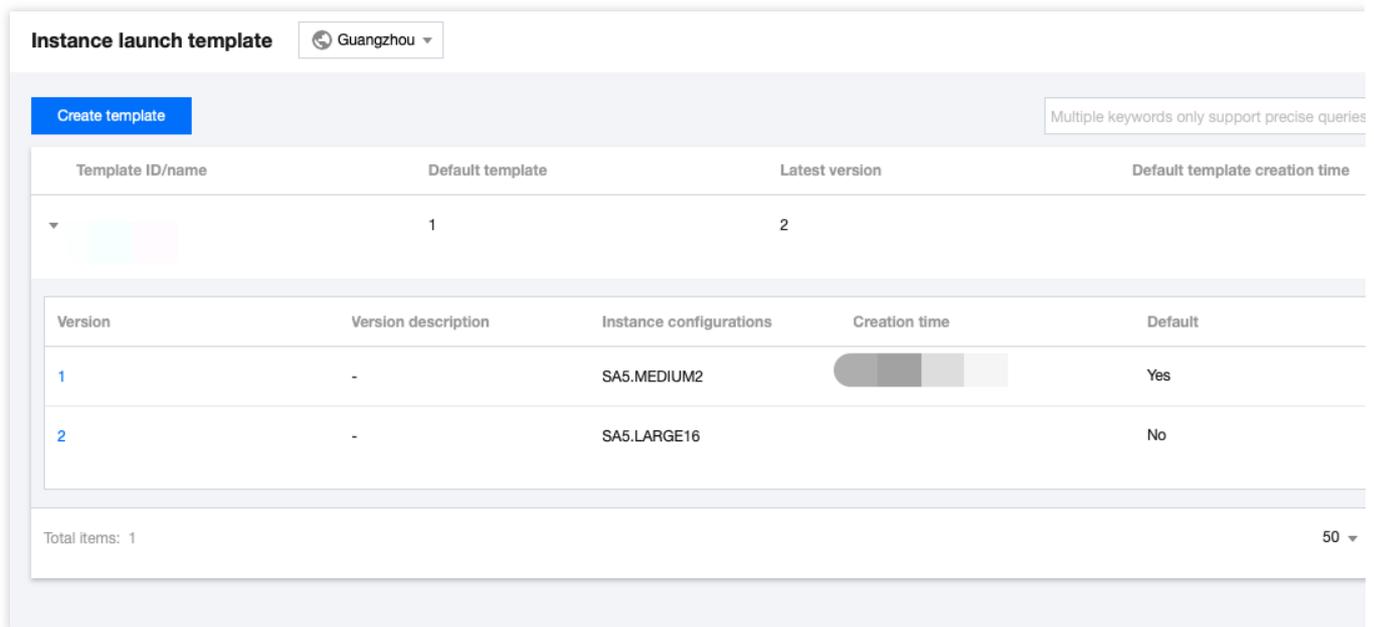
## インスタンステンプレートのデフォルトバージョンの指定

1. **インスタンス起動テンプレート**ページで、テンプレートが所在する行の前にある



をクリックします。

2. 展開されたリストで、設定するバージョンの右側にある**デフォルトに設定**をクリックします。下図のとおりです。



3. ポップアップ表示されるデフォルトテンプレートの設定ウィンドウで、**確認**をクリックします。

## インスタンステンプレートを使用してインスタンスを作成する

1. インスタンス起動テンプレートページで、テンプレートが所在する行の右側にある**インスタンス新規作成**を選択します。

### 説明：

インスタンスの作成は、デフォルトでインスタンス起動テンプレートの**デフォルトバージョン**のコンフィギュレーションを使用します。また、テンプレートが所在する行の前にある



をクリックし、展開されたリストで、他のバージョンを選択してインスタンスを作成することができます。

2. **CVM**の新規作成ページの**コンフィギュレーション情報の確認**ステップで、**オリジナルコンフィギュレーションの比較**を選択し、ポップアップ表示される「**オリジナルコンフィギュレーションの比較**」ウィンドウで、インスタンスとインスタンス起動テンプレートの違いを確認することができます。

3. 間違いがないことを確認した後、『**Tencent Cloud サービス契約**』と『**購入に関する注意事項**』を読み、**同意する** チェックボックスにチェックを入れ、**有効にする** をクリックすればよいです。

## インスタンス起動テンプレートの削除

1. インスタンス起動テンプレートページで、削除するインスタンス起動テンプレートが所在する行の右側にある**削除**を選択します。

2. ポップアップ表示される**削除**ウィンドウで、**確認**をクリックすればよいです。

## 関連ドキュメンテーション

[購入ページからインスタンスを作成する](#)

# 一括連続命名または指定文字列パターン命名

最終更新日：2022-07-28 10:37:09

## 概要

複数のインスタンスを作成する過程で、インスタンス名/ホスト名をある程度規則的にしたい場合に、一括作成時のインスタンス拡張子数字の自動昇順機能や、パターン文字列を指定する機能を提供しており、購入画面と Tencent Cloud API という2つの方法から実装することができます。

n個のインスタンスを購入する必要があり、「CVM+シーケンス番号」のようなインスタンス名/ホスト名（インスタンスCVM1、CVM2、CVM3など）を発行したい場合、[拡張子数字の自動昇順](#)を使用すれば実装できます。

n個のインスタンスを作成し、インスタンス名/ホスト名にシーケンス番号を付け、シーケンス番号をxからインクリメントするよう指定する必要がある場合は、[単一パターン文字列の指定](#)で実装できます。

複数のプレフィックスを持つn個のインスタンス名/ホスト名を作成し、それぞれのプレフィックスでシーケンス番号を指定したい場合は、[単一パターン文字列の指定](#)で実装できます。

## 適用範囲

このドキュメントは、[インスタンス名の設定](#)と[ホスト名の設定](#)に適用されます。

## 操作手順

### 説明：

以下の操作手順は、インスタンス名を設定する例です。ホスト名を設定する手順は、設定する名前のタイプによって若干異なります。

### 拡張子数字の自動昇順

この機能を使用すると、一括購入したインスタンスに同じプレフィックスと番号がインクリメントされるインスタンス名に設定できます。

### ご注意：

作成に成功したインスタンスのデフォルトのシーケンス番号は1からインクリメントされ、開始のシーケンス番号を指定することはできません。

以下の操作は3つのインスタンスを購入し、これらのインスタンスに「CVM+シーケンス番号」の形式で名前を付けることを想定しています。（すなわちインスタンスの名称はCVM1、CVM2とCVM3となる）

購入ページの操作

API の操作

1. [インスタンスの作成](#) を参照して、3つのインスタンスを購入し、「ネットワークとホストの設定」の中で「プレフィックス+シーケンス番号」の命名規則でインスタンスの名称を記入し、すなわちインスタンス名称を `CVM` と記入します。下図に示す通り：

The screenshot shows the '2. Complete Configuration' step of the CVM creation process. It includes sections for Security Groups, Project, Tag, and Instance Name. The 'Instance Name' field is highlighted with a red box and contains the text 'CVM'. Below the 'Instance Name' field, there is a note: 'Supports batch sequential naming or pattern string-based naming. You can enter up to 63 characters remaining.' The 'Login Methods' section at the bottom shows 'SSH Key Pair' selected.

2. ページの指示に従い、支払いを完了します。

Tencent Cloud API [RunInstances](#) で、該当するフィールドを設定します。

インスタンス名：InstanceNameフィールドに `CVM` を指定します。

ホスト名：HostNameフィールドに `CVM` を指定します。

## パターン文字列の指定

この機能を使用すると、一括購入したインスタンスは、指定したシリアル番号を持つ複雑な形式で名前を付けることができます。必要に応じて、インスタンス名に1つ以上のパターン文字列を使用して設定できます。

パターン文字列が指定されたインスタンス名は：`**{R:x}`の形式で、xで生成したインスタンス名の開始番号を示します。

## 単一パターン文字列の指定

以下の操作では3つのインスタンスを作成し、3から始まる昇順の番号を付けたいと想定しています。

購入ページの操作

API の操作

1. [インスタンスの作成](#) を参照してインスタンスを購入し、「ネットワークとホストの設定」の中で「**プレフィックス+パターン文字列の指定{R:x}**」という命名規則でインスタンスの名称を記入し、すなわちインスタンス名称を `CVM{R:x}` と記入します。下図に示す通り：

The screenshot displays the '2. Complete Configuration' step of the CVM creation process. It includes sections for Security Groups, Project, Tag, Instance Name, and Login Methods. The 'Instance Name' field is highlighted with a red border and contains the text 'CVM{R:3}'. Below it, a note states: 'Supports batch sequential naming or pattern string-based naming. You can enter up to 63 characters remaining.' The 'Login Methods' section has 'SSH Key Pair' selected.

2. ページの指示に従い、支払いを完了します。

Tencent Cloud API [RunInstances](#) で、該当するフィールドを設定します。

インスタンス名：InstanceNameフィールドに `CVM {R:3}` を指定します。

ホスト名：HostNameフィールドに `CVM` を指定します{R:3}。

### 複数のパターン文字列の指定

以下の操作例は、3つのインスタンスを作成し、インスタンス名称に `cvm`、`Big`、`test` プレフィックスを含み、かつ `cvm` と `Big` プレフィックスの後にはシーケンス番号を付け、シーケンス番号はそれぞれ13と2からインクリメントします（すなわちインスタンス名称は `cvm13-Big2-test`、`cvm14-Big3-test`、`cvm15-Big4-test` となる）。

購入ページの操作

API の操作

1. [インスタンスの作成](#) を参照して3つのインスタンスを購入します。「ネットワークとホストの設定」ページで「**プレフィックス+パターン文字列の指定{R:x}-プレフィックス+パターン文字列の指定{R:x}-プレフィックス**」と

この命名規則でインスタンス名を記入し、すなわちインスタンス名を `cvm{R:13}-Big{R:2}-test` と記入します。下図に示す通り：

The screenshot shows the '2. Complete Configuration' step of the Tencent Cloud console. The 'Instance Name' field is highlighted with a red border and contains the value `cvm{R:13}-Big{R:2}-test`. Below the field, it says 'Supports batch sequential naming or pattern string-based naming. You can enter up to 60 characters remaining.' Other visible fields include 'Security Groups' (Existing Security Groups), 'Project' (DEFAULT PROJECT), and 'Login Methods' (SSH Key Pair).

2. ページの指示に従い、支払いを完了します。

Tencent Cloud API [RunInstances](#) で、該当するフィールドを設定します。

インスタンス名：InstanceNameフィールドに `cvm{R:13}-Big{R:2}-test` を指定します。

ホスト名：InstanceNameフィールドに `cvm{R:13}-Big{R:2}-test` を指定します。

## 検証機能

[拡張子数字の自動昇順](#) または [パターン文字列の指定](#) でインスタンスの一括作成を実装したら、以下の操作によって検証することができます。

### 設定したインスタンス名の検証

[CVMコンソール](#) にログインし、新規作成したインスタンスを確認すると、下図のように、一括購入したインスタンスが設定したルールに従って命名されていることが確認できます。

<input type="checkbox"/> ID/Name	Monitoring	Availability Zone ▼	Instance Type ▼	Instance Configuration	Primary IPv6	Instance Billing Mode ▼
<input type="checkbox"/>  cvm15-Big4-test		Nanjing Zone 1	Standard S5 	1-core 2GB 1Mbps System disk: Premium Cloud Storage Network: 	-	Pay as you go Created at 2021-03-11 16:33:47
<input type="checkbox"/>  cvm14-Big3-test		Nanjing Zone 1	Standard S5 	1-core 2GB 1Mbps System disk: Premium Cloud Storage Network: 	-	Pay as you go Created at 2021-03-11 16:33:44
<input type="checkbox"/>  cvm13-Big2-test		Nanjing Zone 1	Standard S5 	1-core 2GB 1Mbps System disk: Premium Cloud Storage Network:	-	Pay as you go Created at 2021-03-11 16:33:41

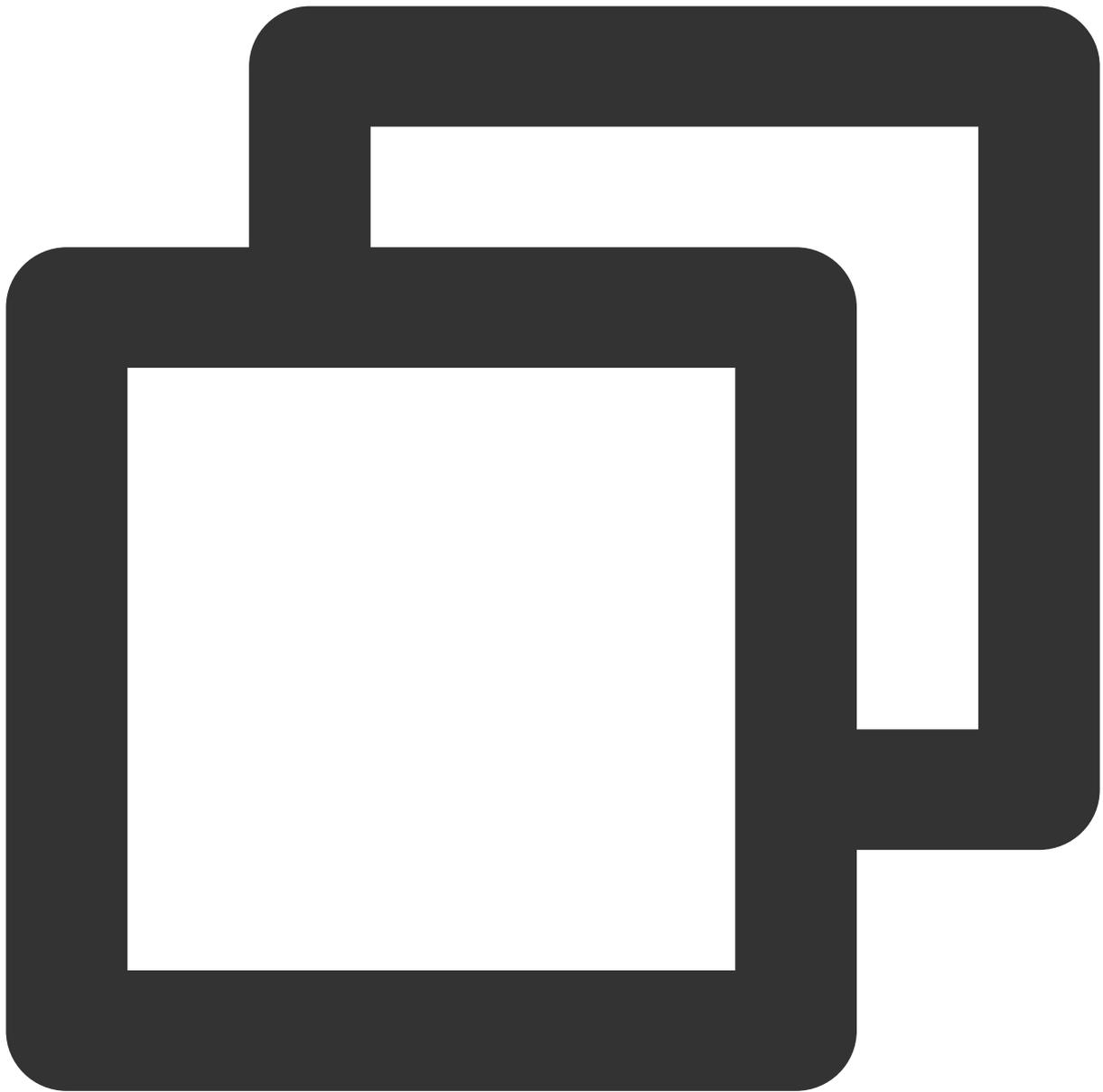
## 設定したホスト名の検証

1. Cloud Virtual Machineのインスタンスを再起動し、ログインします。
2. インスタンスのOSの種類により、異なる操作手順を選択します。

Linux インスタンス

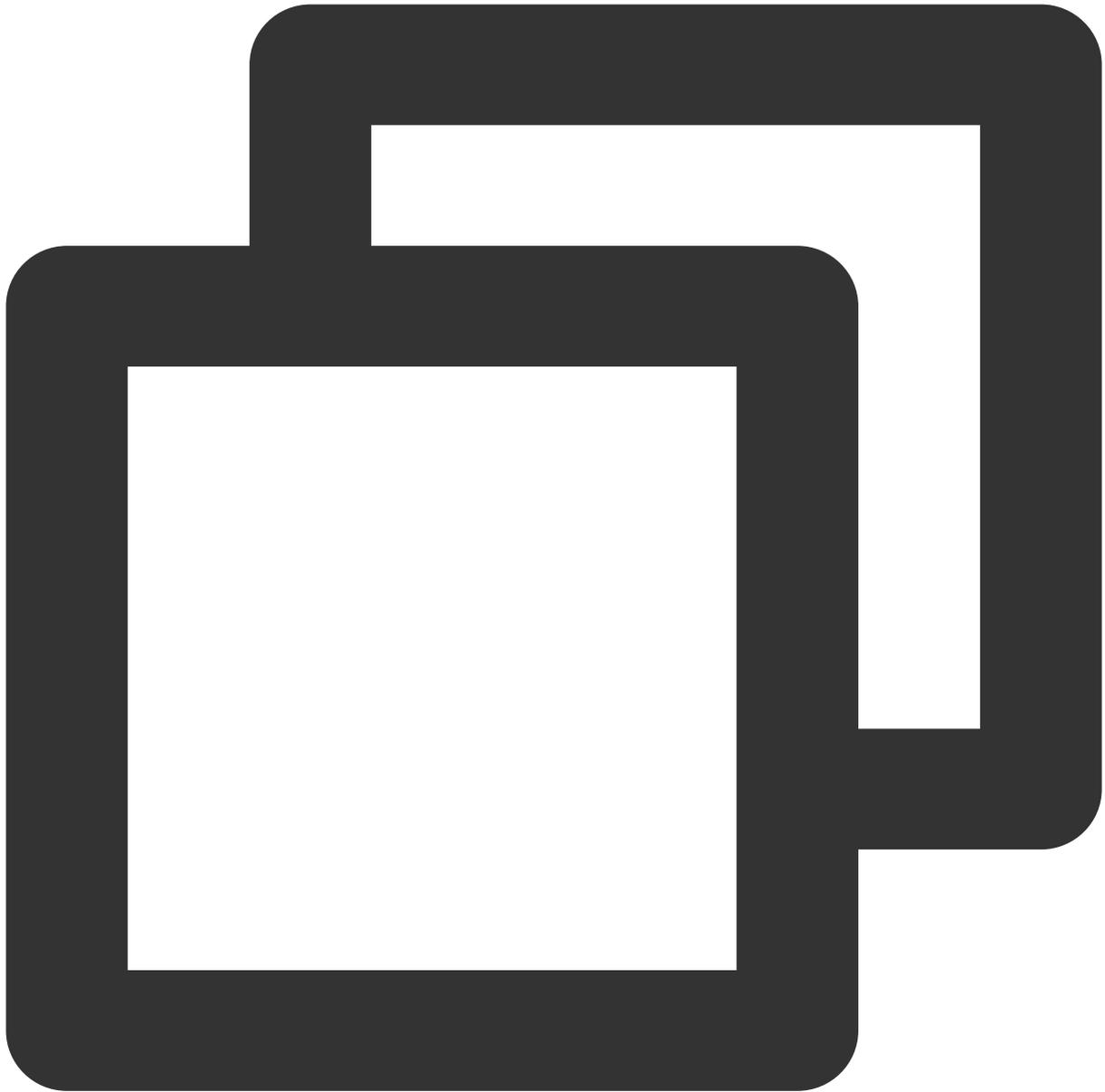
Windows インスタンス

OSのインターフェースで以下のコマンドを実行します。



```
hostname
```

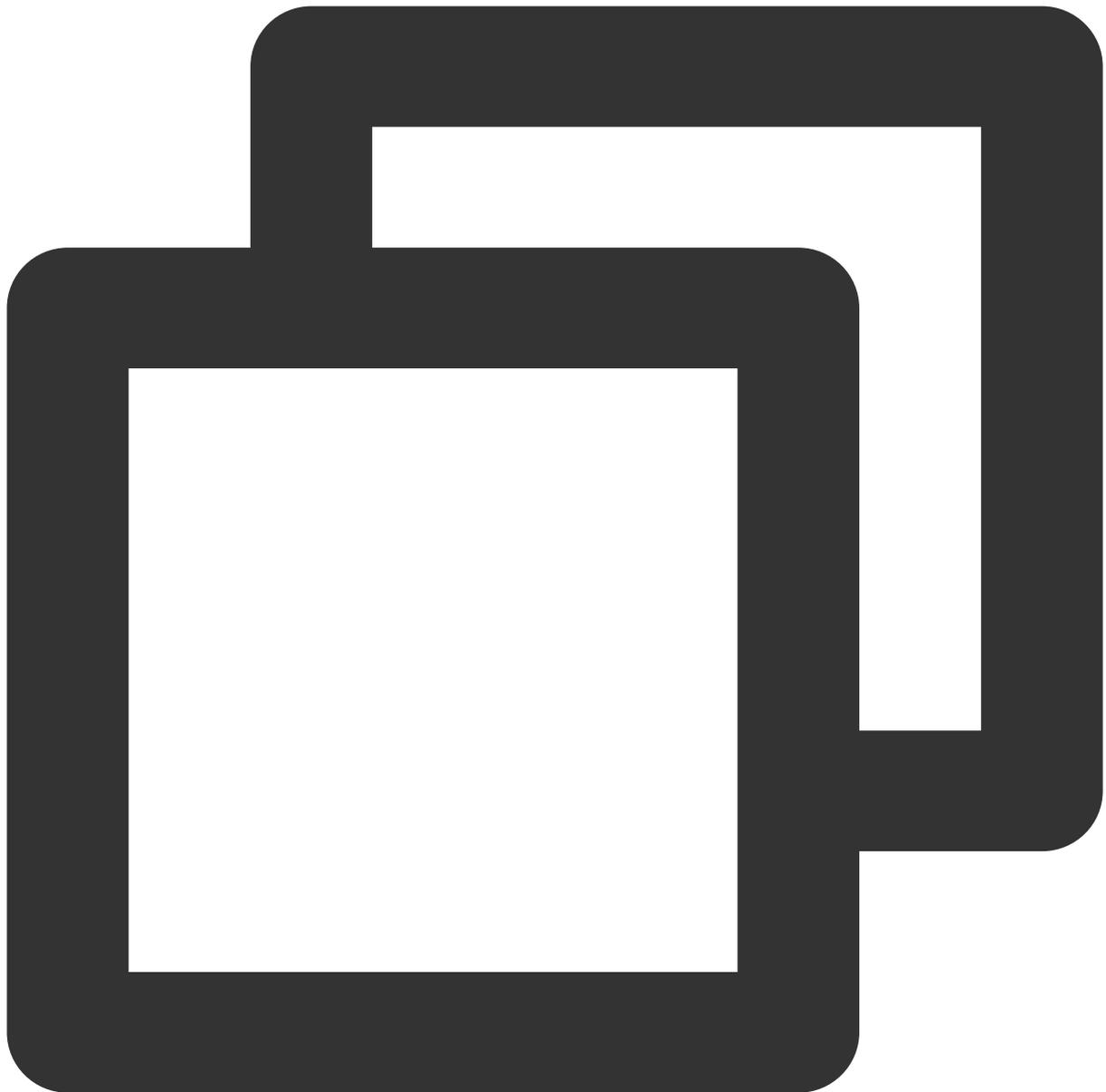
CMDコマンドラインツールを開き、以下のコマンドを実行します。



```
hostname
```

3. `hostname` コマンドで返された結果を確認します。

以下のような結果が返ってくれば、設定は成功しています。



```
cvm13-Big2-test
```

4. [ステップ1](#) - [ステップ3](#) を繰り返し、他の一括購入インスタンスを順に検証します。

# Linuxインスタンスにログインする 標準ログイン方式を使用してLinuxインスタ ンスにログインする（推奨）

最終更新日：：2023-04-12 10:30:04

## 概要

WebShellはTencent Cloudが推奨するログイン方法です。ローカルOSがWindows、Linux、Mac OSのいずれであっても、インスタンスのパブリックIPを購入している限り、WebShell経由でインスタンスにログインすることができます。このドキュメントでは、WebShell経由でLinuxインスタンスにログインする方法について説明します。

WebShellの利点は下記の通り：

コピーのショートカットキーをサポートします。

マウスホイールのスクロール機能をサポートします。

中国語入力をサポートします。

セキュリティが高い、ログインするたびにパスワードまたはキーを入力する必要があります。

## 認証方式

パスワードまたはキーです。

## 前提条件

Linuxインスタンスにログインするための管理者のアカウントとパスワード（またはキー）を取得済みであること。

インスタンス作成時に、システムによるパスワードのランダム発行を選択した場合は、[サイト内メール](#)からパスワードを取得してください。

ログインパスワードを設定済みの場合は、そのパスワードを使用してログインしてください。パスワードを忘れた場合は、[インスタンスのパスワードをリセット](#)してください。

キーがインスタンスに関連付けられている場合、そのキーを使用してログインできます。キーに関する詳細については、[SSHキー](#)をご参照ください。

CVMインスタンスはパブリックIPをすでに購入しており、インスタンスに関連付けられたセキュリティグループの中で、送信元がWebShellのプロキシIPとなるリモートログインポート（デフォルトは22）を開放しています。

クイック設定でCVMインスタンスを購入した場合は、デフォルトでポート開放しました。

カスタム設定でCVMインスタンスを購入した場合は、[セキュリティグループの応用例](#)を参照して、ポートを手動で開くことができます。

## 操作手順

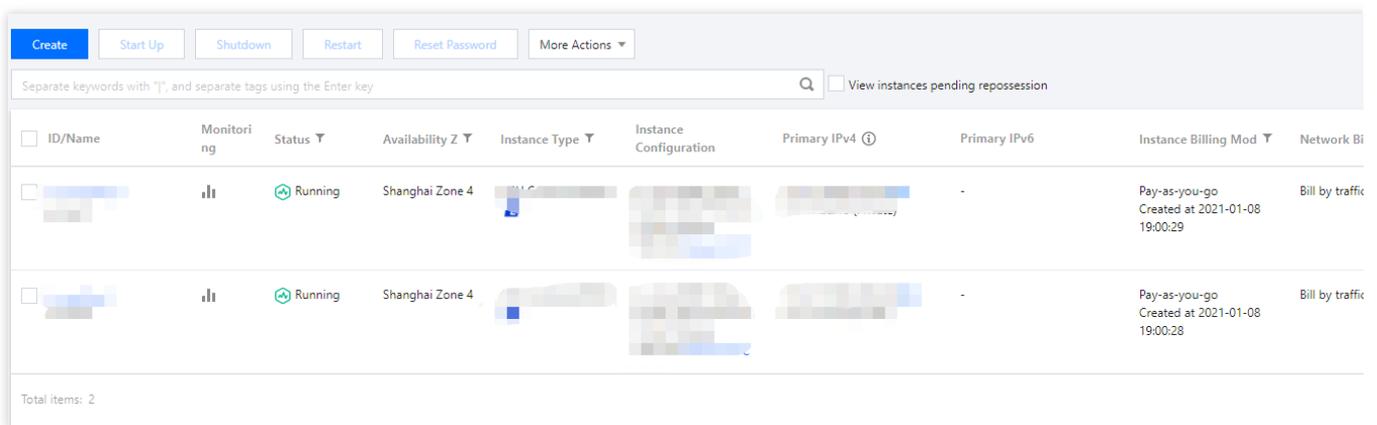
1. [CVMコンソール](#) にログインします。

2. インスタンスの管理画面で、実際に使用されているビューモードに従って操作します。

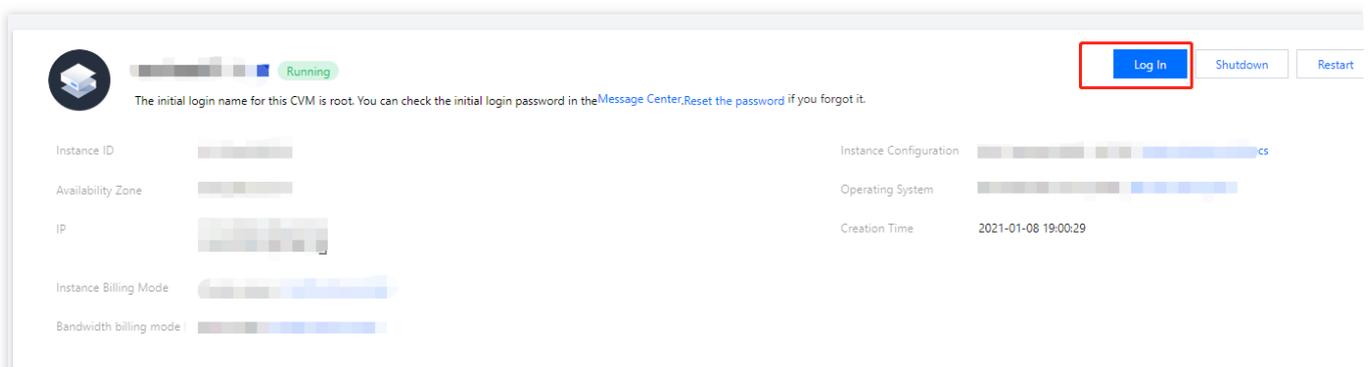
リストビュー

タブビュー

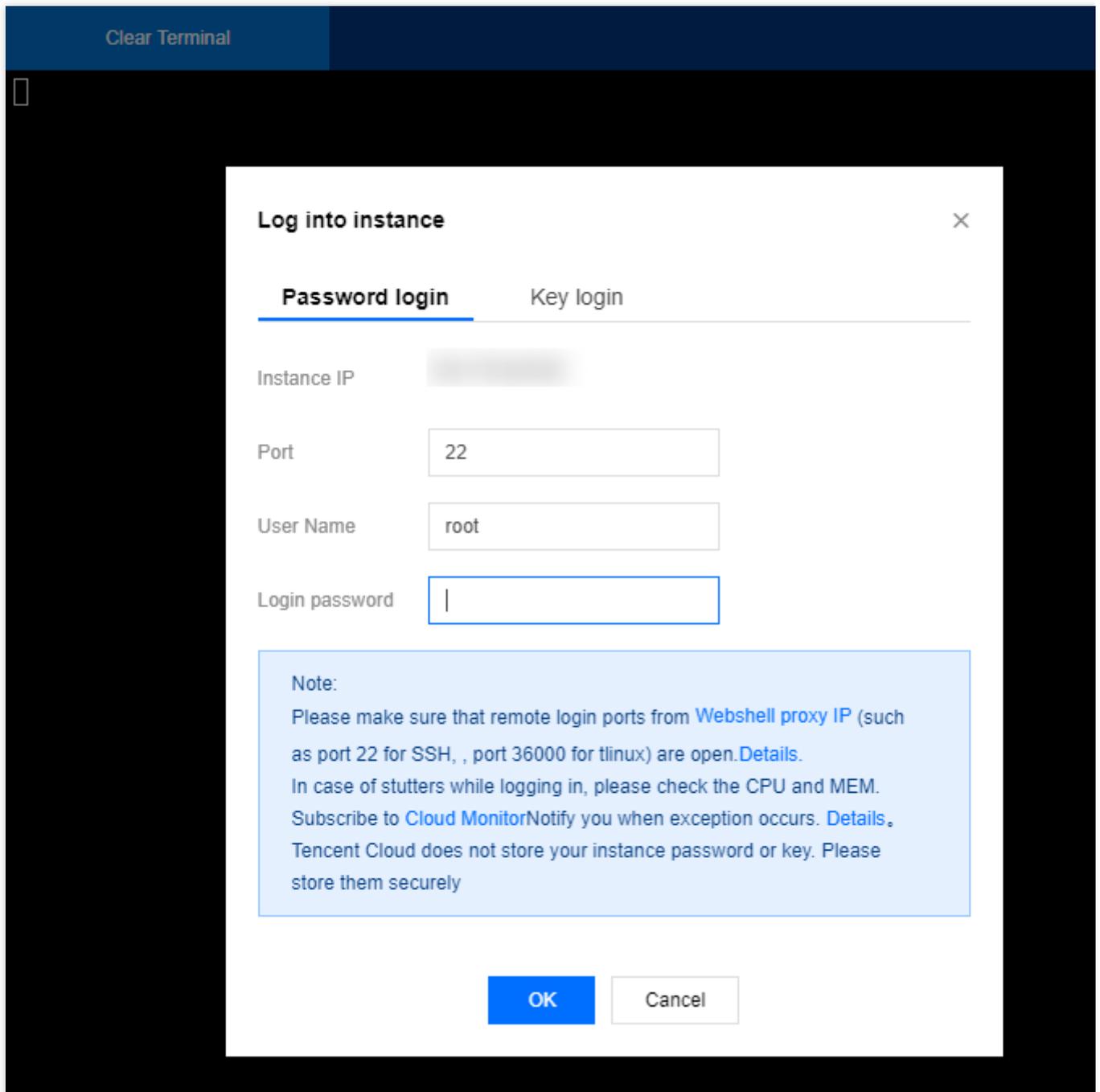
下図に示すように、ログインするLinux CVMインスタンスを選択し、画面右側にある**ログイン**をクリックします。



下図に示すように、ログインするLinux CVM インスタンスのタブを選択し、**ログイン**をクリックします。



3. 下図に示すように、開いた「標準ログイン | Linuxインスタンス」ウィンドウで、実際のニーズに応じてパスワードでログインまたはキーでログイン方式のいずれかを選択し、ログインします。



以下の説明を参照して、ログインに必要な情報を入力してください。

**ポート**：デフォルトのポート番号は22番です。必要に応じて入力してください。

**ユーザー名**：Linuxインスタンスのデフォルトのユーザー名はroot（Ubuntuシステムインスタンスのデフォルトのユーザー名はubuntu）です。必要に応じて入力してください。

**パスワード**：[前提条件](#)のステップで取得したログインパスワードを入力します。

**キー**：インスタンスに関連付けられているキーを選択します。

4. **ログイン**をクリックすると、Linuxインスタンスにログインできます。

ログインに成功すると、下図に示すように、WebShellインターフェースに以下のプロンプトが表示されます。

```
* Socket connection established *  
Last login: [redacted] 2018 from [redacted]  
[root@V[redacted]os ~]#
```

## 後続の操作

CVMにログインした後、個人用Webサイトまたはフォーラムを構築したり、その他の操作を実行したりできます。関連操作については、下記をご参照ください：

[WordPress 個人用サイトを構築する](#)

[Discuz!フォーラムを手動で構築する](#)

## 関連ドキュメント

[インスタンスのパスワードをリセット](#)

[SSHキーの管理](#)

# 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

最終更新日： : 2023-04-13 10:59:30

## 概要

このドキュメントでは、PuTTYソフトウェアを例として、リモートログインソフトウェアを使用してWindowsからLinuxインスタンスにログインする方法について説明します。

## 対応OS

Windows

## 認証方式

パスワードまたはキーです。

## 前提条件

インスタンスにログインするための管理者アカウント及びパスワード(またはキー)を取得しました。

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

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

CVMインスタンスはすでにパブリックIPを購入されており、このインスタンスは22番ポート（クイック設定で購入したCVMインスタンスの場合、デフォルトで開放している）を開放しました。

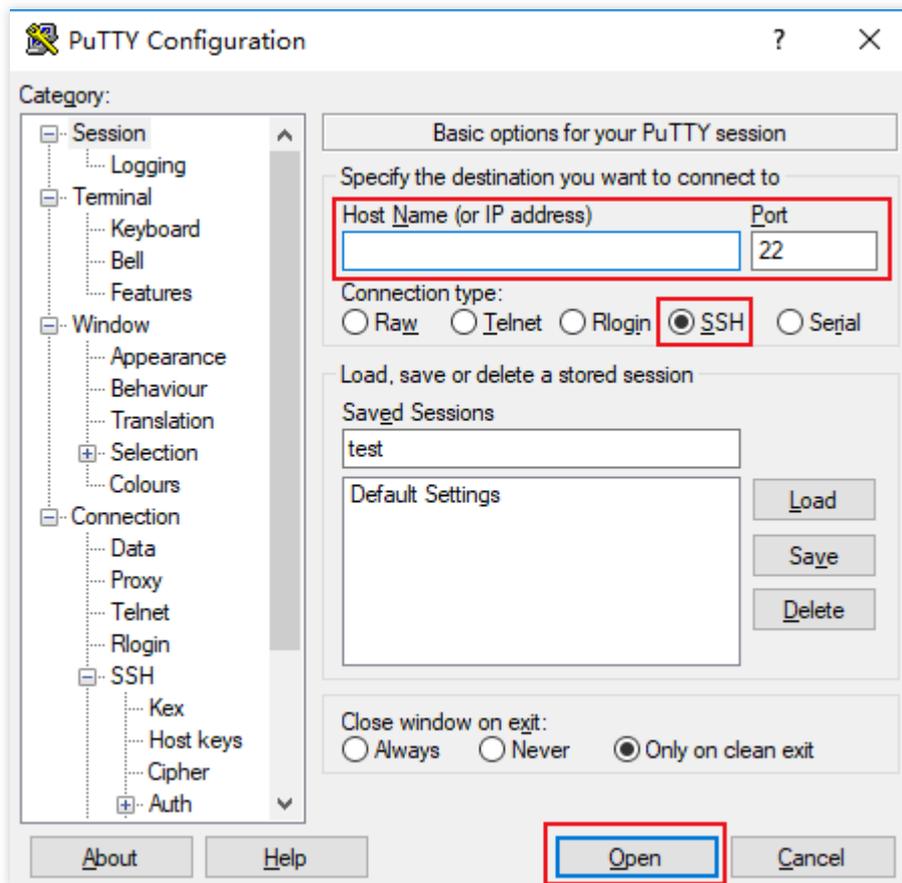
## 操作手順

パスワードでログインする

キーでログインする

1. リモートログオンクライアントソフト「PuTTY」をダウンロードします。
2. **putty.exe**をダブルクリックして、PuTTYクライアントを開きます。

3. PuTTY Configuration ウィンドウで、次の内容を入力します。次の図に示すように：



パラメータは次のとおりです：

**Host Name (or IP address)** : CVMのパブリックIPアドレスです。(CVMコンソールにログインし、インスタンスリストと詳細画面でパブリックIPを取得できます)。

**Port** : CVMのポート。「22」である必要があります。

**Connect type** : 「SSH」を選択します。

**Saved Sessions** : testなどのセッション名を入力します。

「Host Name」を設定した後、「Saved Sessions」を設定して保存します。「Saved Sessions」の下に保存されているセッション名をダブルクリックしてCVMにログインできます。

4. **Open**をクリックして「PuTTY」インターフェースに入り、「login as:」というコマンドプロンプトが表示されます。

5. 「login as」の後にユーザー名を入力し、**Enter**キーを押します。

6. 「Password」の後にパスワードを入力し、**Enter**キーを押します。

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。次の図に示すように：



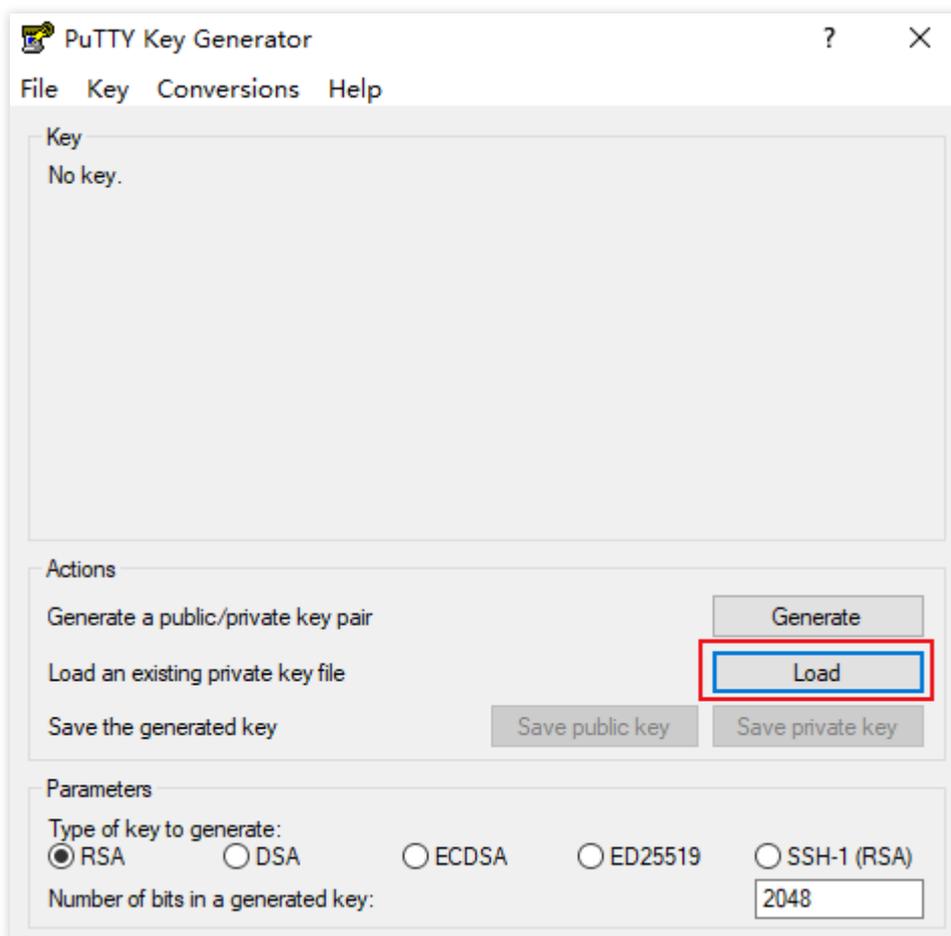
ログインが完了すると、コマンドプロンプトの左側に現在ログインしているCVMに関する情報が表示されます。

1. リモートログオンクライアントソフト「PuTTY」をダウンロードします。putty.exeとputtygen.exeの両方をそれぞれダウンロードしてください。

2. **puttygen.exe**をダブルクリックして、PuTTY Keyクライアントを開きます。

3. **Load**をクリックし、ダウンロードした秘密鍵が保存されているパスを選択して開きます。キーペアを作成した後、秘密鍵をダウンロードして保持する必要があります。詳細については、[SSHキーの管理](#)をご参照ください。

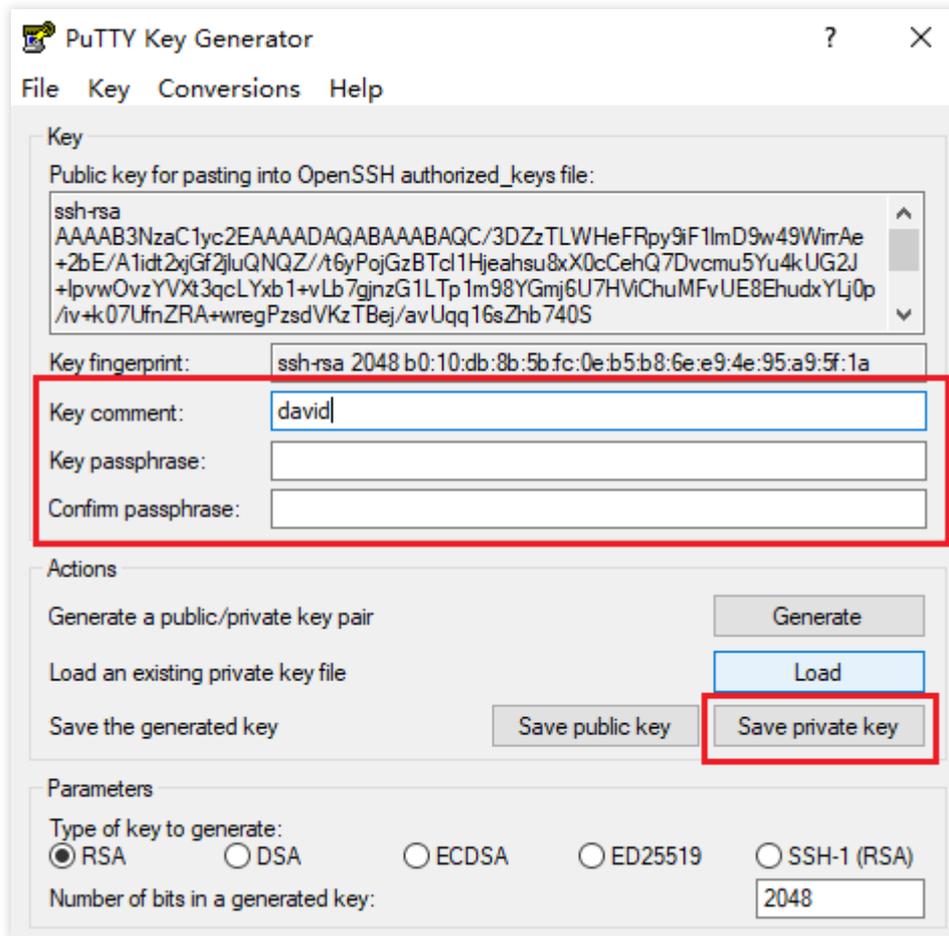
例えば、davidという名前の秘密鍵ファイルを選択して開きます。



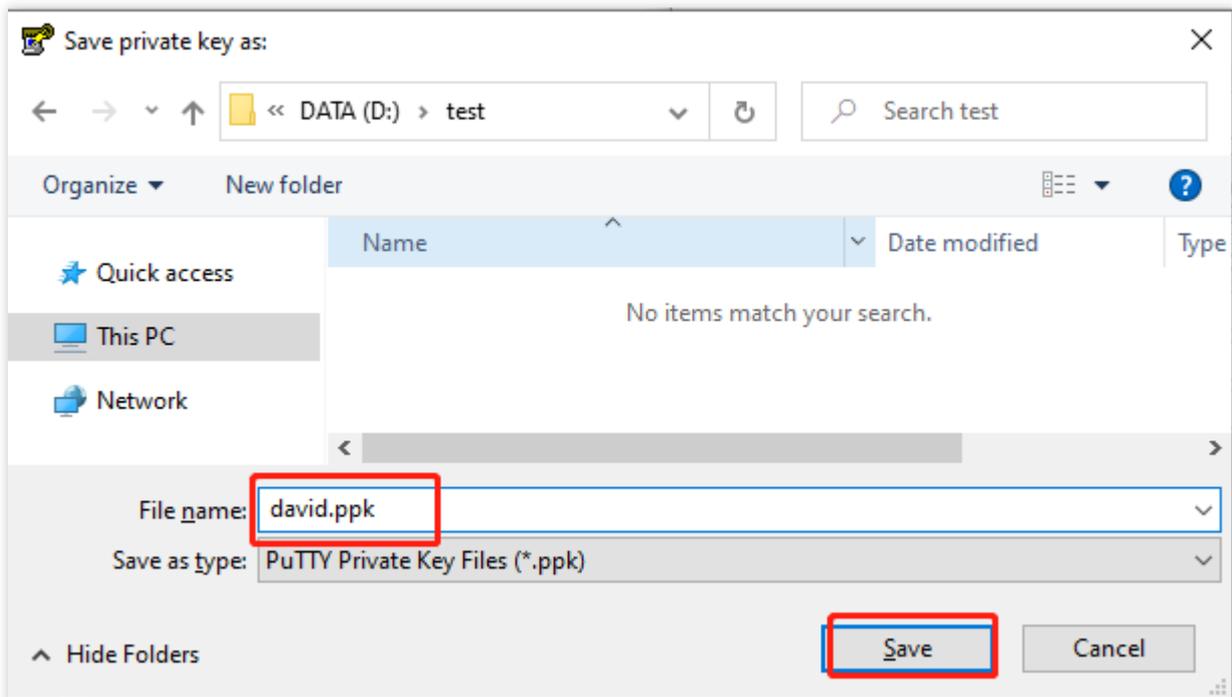
4.

PuTTY Key Generator

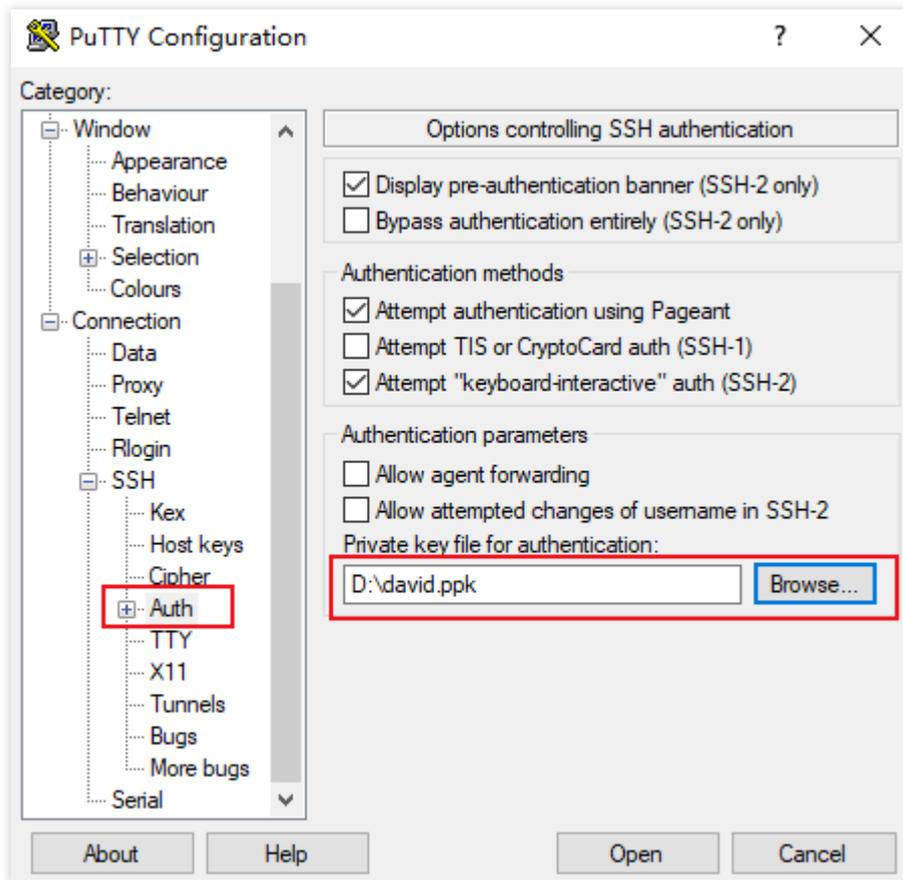
ウィンドウにキー名を入力し、PuTTY が秘密鍵の暗号化に使用するパスワードを設定します（オプション）。設定が完了したら、【Save private key】をクリックします。次の図に示すように：



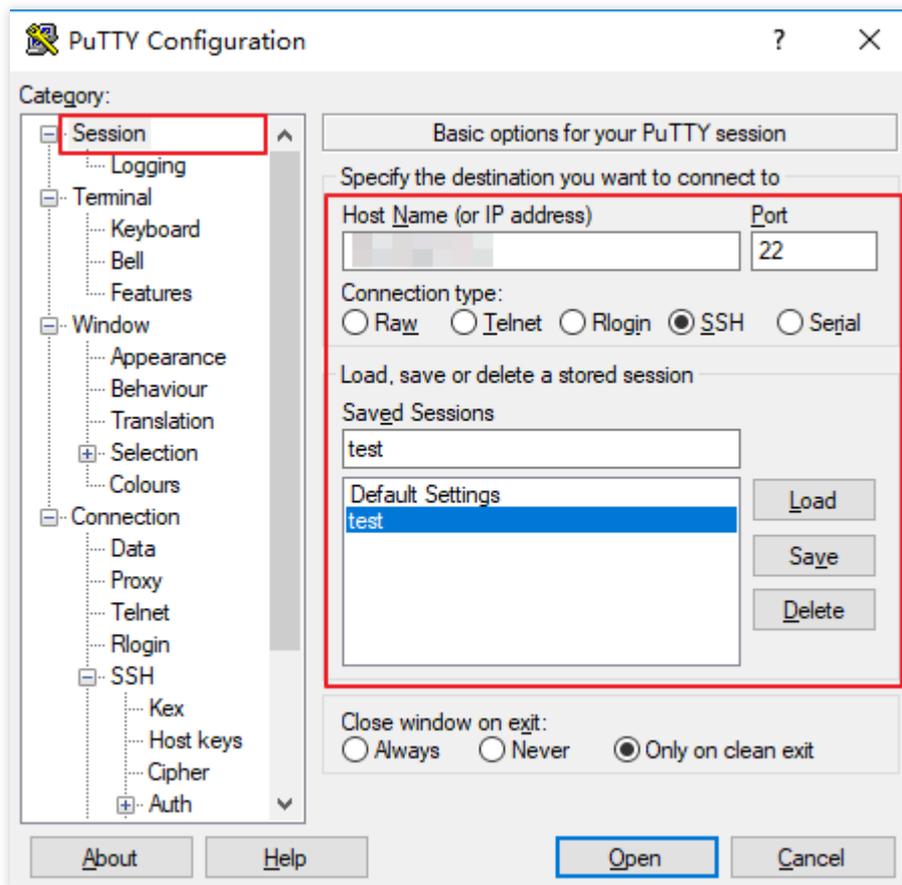
5. ポップアップウィンドウで、キーを保存するパスを選択します。ファイル名フィールドに「Key Name.ppk」と入力して、Saveをクリックします。例えば、david秘密鍵ファイルをdavid.ppkキーファイルとして保存します。次の図に示すように：



6. **putty.exe**をダブルクリックして、PuTTYクライアントを開きます。
7. 左側のナビゲーションバーで、**Connection>SSH>Auth**を選択して、Auth設定インターフェースに入ります。
8. **Browse**をクリックし、キーが保存されているパスを選択して開きます。次の図に示すように：



9. Session設定インターフェースに切り替えて、CVM IP、ポート、および接続タイプを設定します。次の図に示すように：



**Host Name (IP address)** : CVMのパブリックIPアドレスです。 [CVMコンソール](#)にログインし、インスタンスリストと詳細画面でパブリックIPを取得できます。

**Port** : CVMのポート。「22」である必要があります。

**Connect type** : 「SSH」を選択します。

**Saved Sessions** : testなどのセッション名を入力します。

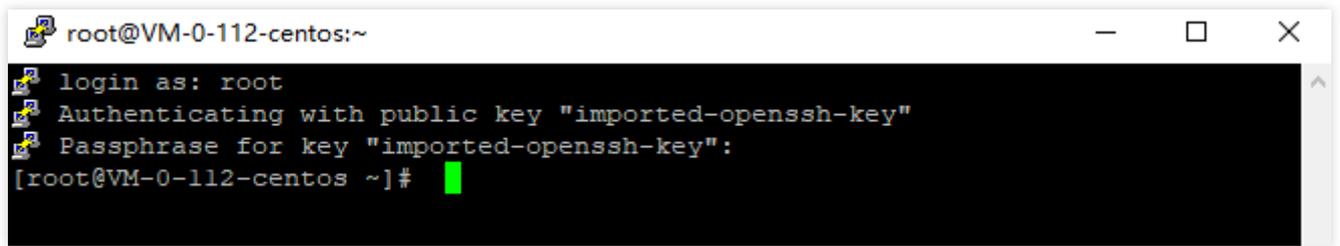
「Host Name」を設定した後、「Saved Sessions」を設定して保存します。「Saved Sessions」の下に保存されたセッション名をダブルクリックしてCVMにログインできます。

10. **Open**をクリックして「PuTTY」インターフェースに入り、「login as:」というコマンドプロンプトが表示されます。

11. 「login as」の後にユーザー名を入力し、**Enter**キーを押します。

12. [ステップ4](#)に従って暗号化された秘密鍵のパスワードを設定する場合は、「Passphrase for key "imported-openssh-key":」の後にパスワードを入力し、Enterを押してください。

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。次の図に示すように：

A terminal window titled 'root@VM-0-112-centos:~' showing the steps of an SSH login. The text displayed is: 'login as: root', 'Authenticating with public key "imported-openssh-key"', 'Passphrase for key "imported-openssh-key":', and finally '[root@VM-0-112-centos ~]#'. A green cursor is visible at the end of the last line.

```
root@VM-0-112-centos:~  
login as: root  
Authenticating with public key "imported-openssh-key"  
Passphrase for key "imported-openssh-key":  
[root@VM-0-112-centos ~]#
```

ログインが完了すると、コマンドプロンプトの左側に現在ログインしているCVMに関する情報が表示されます。

## その後の操作

CVMにログインした後、個人用Webサイトまたはフォーラムを構築したり、その他の操作を実行したりできます。詳細については、下記のドキュメントをご参照ください：

[WordPress 個人用サイトを構築する](#)

[Discuz!フォーラムを手動で構築する](#)

# SSHを使用してLinuxインスタンスにログインする

最終更新日：2023-06-25 17:49:49

## ユースケース

このドキュメントでは、SSHキーを使用して、ローカル Linux、Mac OS、または Windowsサーバーから Linux インスタンスにログインする方法について説明します。

## サポートされているOS

Linux、Mac OS または Windows (Windows 10 および Windows Server 2019 を含む)

## 認証方式

パスワードまたはキーです。

## 前提条件

インスタンスにログインするための管理者アカウントとパスワード (またはキー) を取得しました。

Linux インスタンスの管理者アカウントは通常、デフォルトでは `root` にし、Ubuntu システムは `ubuntu` です。実際の状況に応じて変更できます。

システムのデフォルトパスワードを利用してインスタンスにログインする場合は、[サイト内メール](#) に移動してパスワードを取得してください。

[キーを使用してログイン](#) する場合は、キーを作成してこのCVMインスタンスに関連付ける必要があります。さらに詳細な操作については、[SSHキー](#) をご参照ください。

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

CVMインスタンスはすでにパブリックIPを購入されており、このインスタンスは22番ポート(クイック設定で購入したCVMインスタンスの場合、デフォルトで開放している)を開放しました。

## 操作手順

パスワードでログインする

キーでログインする

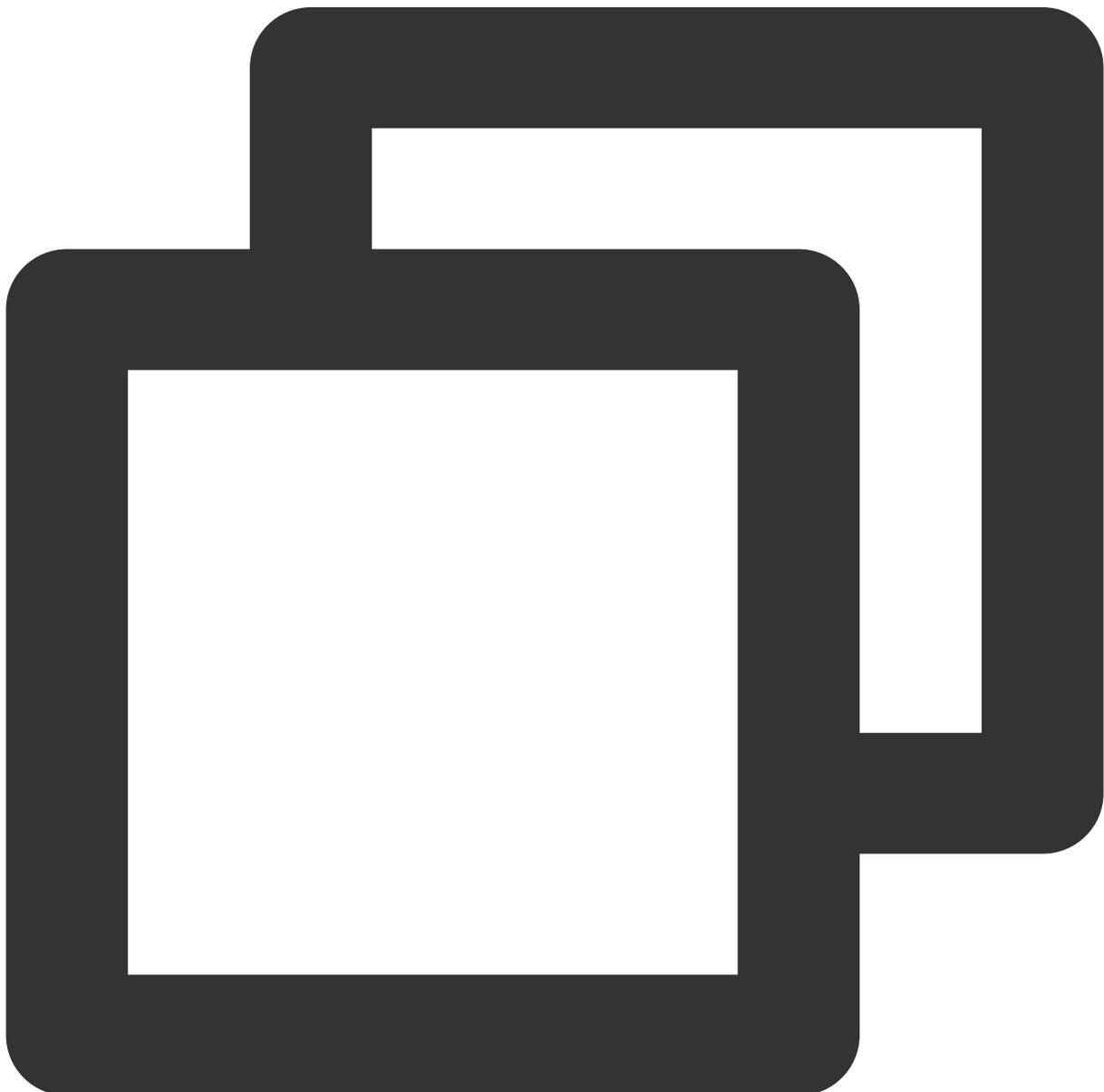
1. 次のコマンドを実行して、Linux CVMに接続します。

**説明：**

ローカルコンピューターが Mac OSを実行している場合は、次のコマンドを実行する前に、システム付属のターミナルを開く必要があります。

ローカルコンピューターが Linuxを実行している場合は、次のコマンドを直接実行できます。

ローカルコンピューターがWindows 10またはWindows Server 2019を実行している場合は、次のコマンドを実行する前に、コマンドプロンプト（CMD）を開く必要があります。



```
ssh <username>@<hostname or IP address>
```

`username` は、前提条件で取得されたデフォルトのアカウントです。

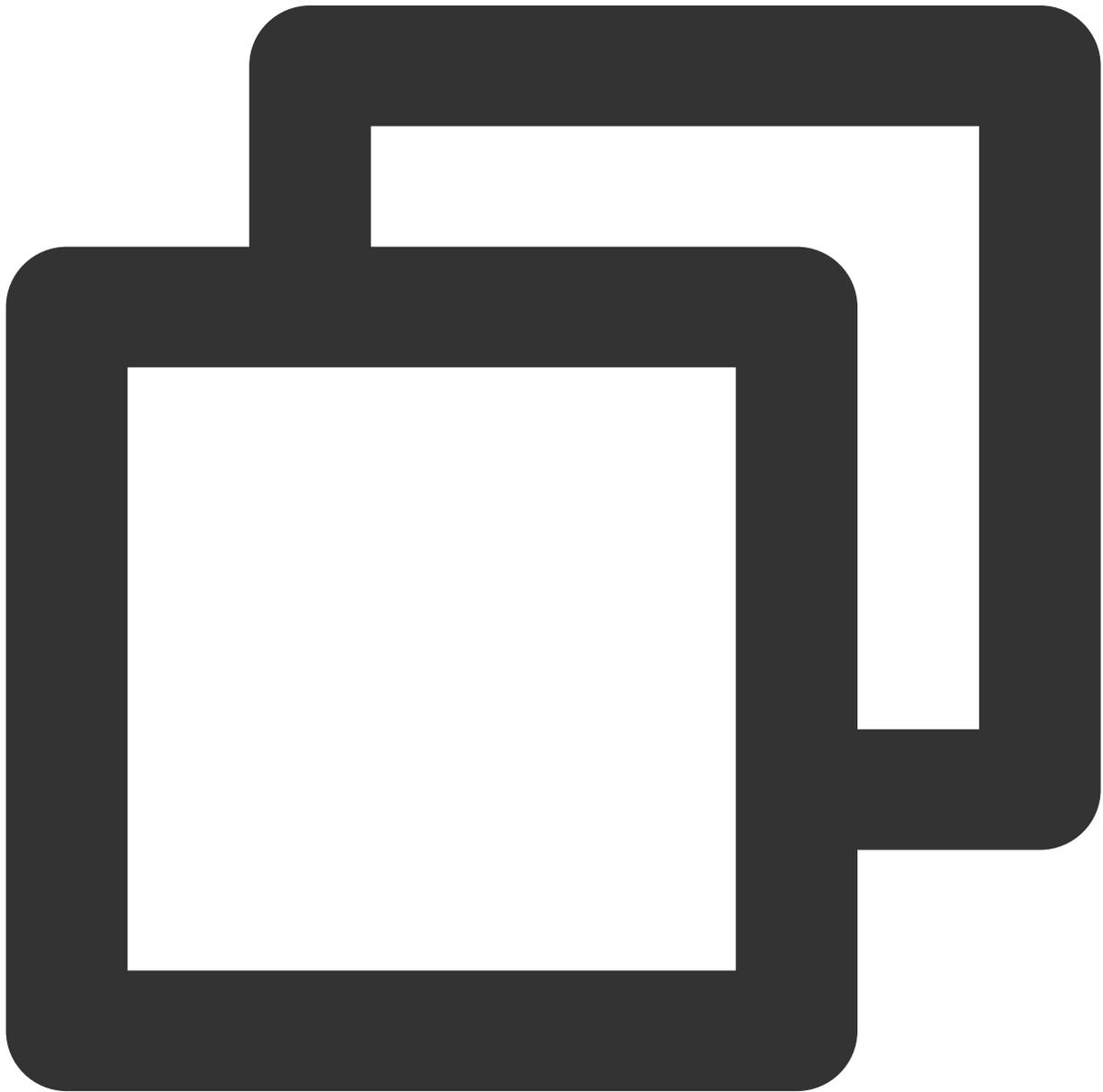
`hostname or IP address` は Linux インスタンスのパブリックIPアドレス或いはカスタムドメイン名です。

2. 取得したパスワードを入力し、**Enter**キーを押してログインを完了します。

1. 次のコマンドを実行して、プライベートキーファイルに本人だけ読み取り権限を付与します。

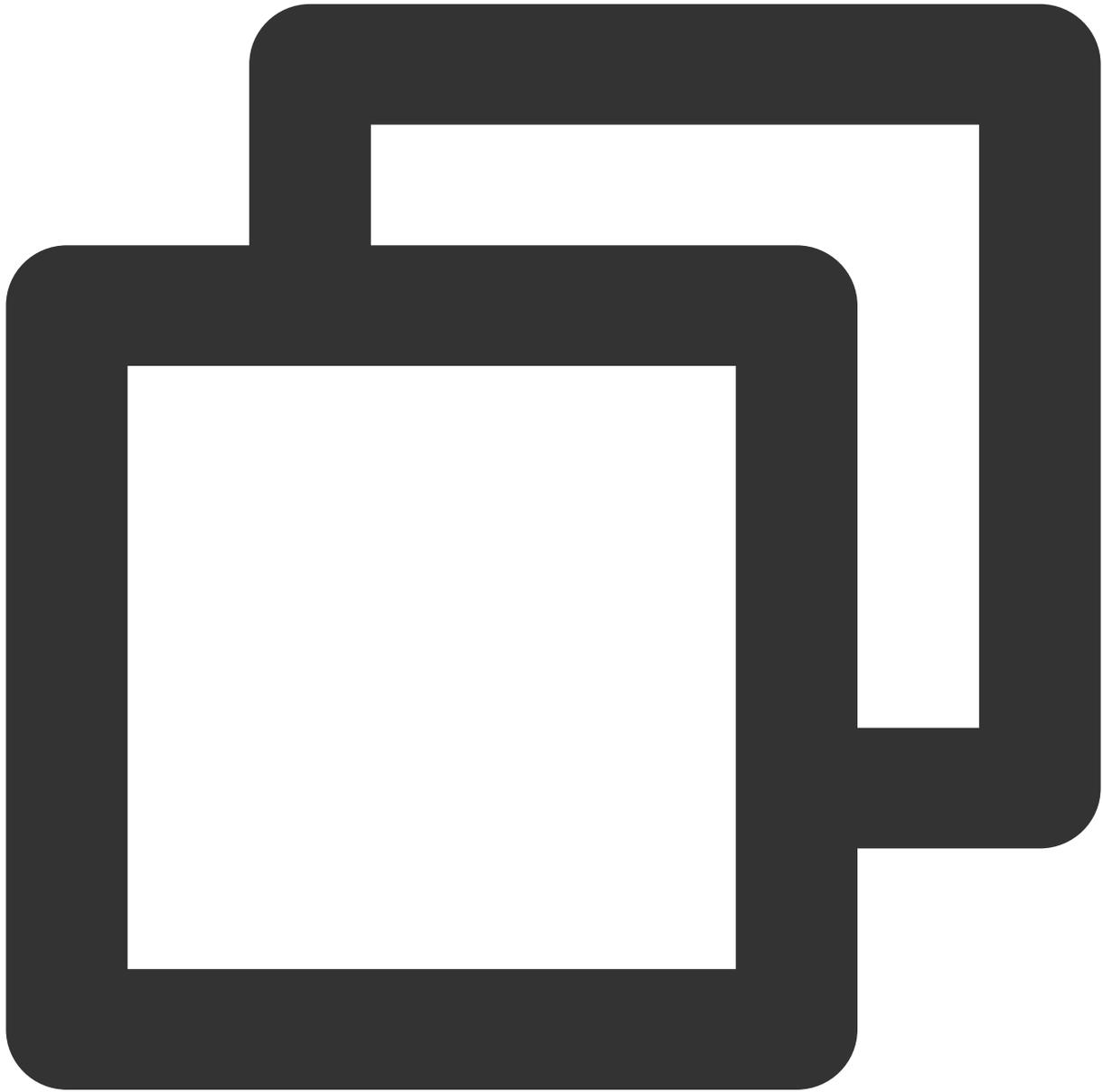
ローカルコンピューターが Mac OSを実行している場合は、次のコマンドを実行する前に、システム付属のターミナルを開く必要があります。

ローカルコンピューターが Linuxを実行している場合は、次のコマンドを直接実行できます。

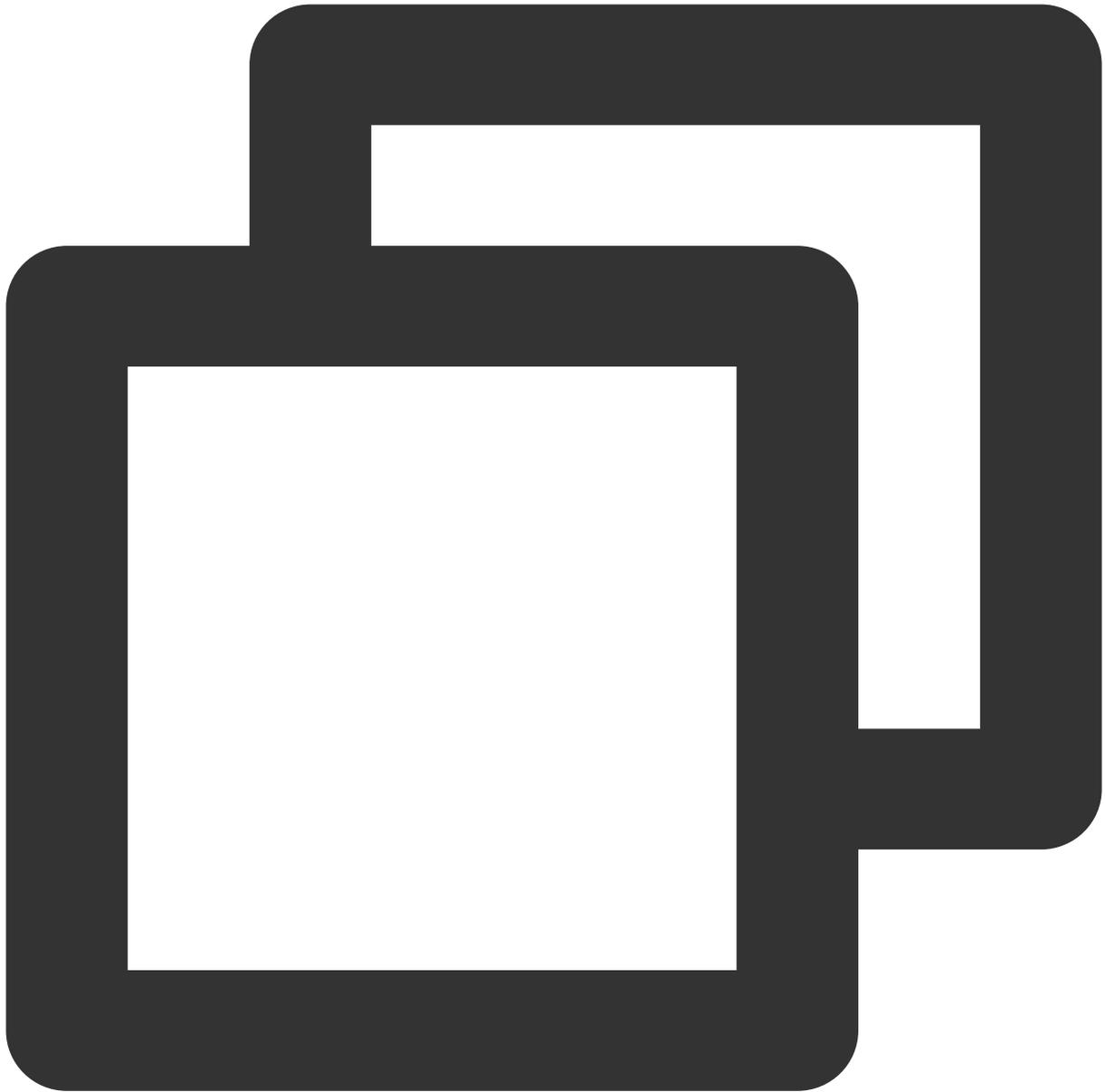


```
chmod 400 <ダウンロードしたCVMに関連するプライベートキーの絶対パス>
```

ローカルコンピューターがWindows 10を実行している場合は、次のコマンドを実行する前に、コマンドプロンプト (CMD) を開く必要があります。

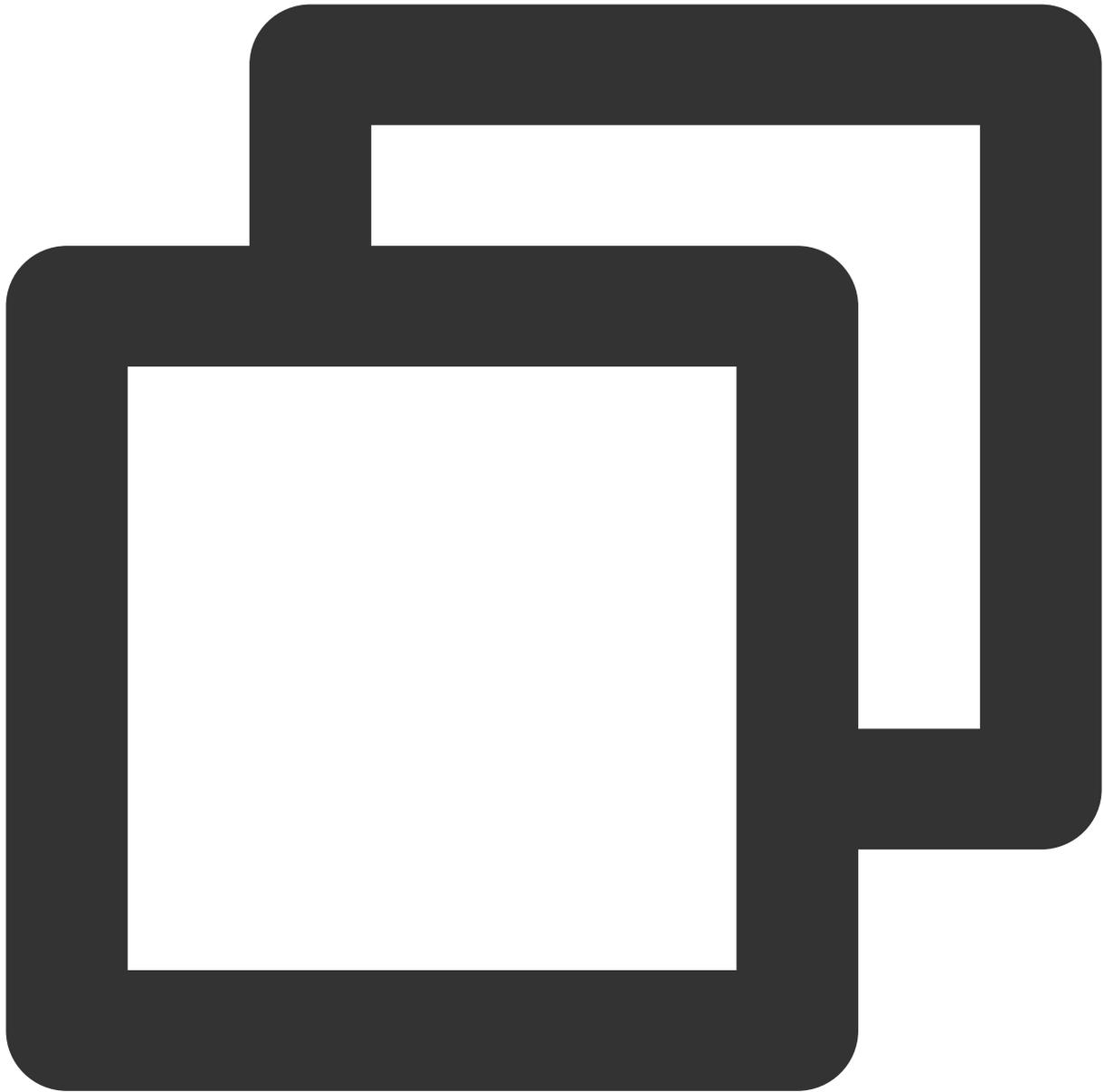


```
icacls <ダウンロードしたCVMに関連するプライベートキーの絶対パス> /grant <システムのユーザーアカ
```



```
icacls <ダウンロードしたCVMに関連するプライベートキーの絶対パス> /inheritancelevel:r
```

2. 次のコマンドを実行してリモートログインします。



```
ssh -i <ダウンロードしたCVMに関連するプライベートキーの絶対パス> <username>@<hostname or IP
```

`username` は、前提条件で取得したデフォルトのアカウントです。

`hostname or IP address` は Linux インスタンスのパブリックIPアドレス或いはカスタムドメイン名です。

例えば、 `ssh -i "Mac/Downloads/shawn_qcloud_stable.pem" ubuntu@192.168.11.123` コマンドを実行して、Linux CVMにリモートログインします。

## その後の操作

CVMにログインした後、個人用Webサイトまたはフォーラムを構築したり、その他の操作を実行したりできます。詳細については、下記のドキュメントをご参照ください：

[WordPress 個人用サイトを構築する](#)

[Discuz!フォーラムを手動で構築する](#)

# VNCを使用してLinuxインスタンスにログインする

最終更新日： : 2023-04-11 18:55:38

## 概要

VNC接続は、Tencent Cloudが提供するWebブラウザ経由でCVMにリモート接続する方式です。クライアントにリモートデスクトップサービスがインストールされていないかまたはリモートデスクトップ接続ができない場合や、いかなる方法でも接続できない場合は、ユーザーはVNCを介してCVMにログインし、CVMの状態を観察し、かつCVMアカウントから基本的なCVM管理操作を行うことができます。

## 使用制限

VNC経由でログインしたCVMは現在、コピー・ペースト機能、中国語入力ソフト、およびファイルのアップロードまたはダウンロードをサポートしていません。

VNC経由でCVMにログインする場合は、Chrome、Firefox、IE 10以降などの主流のブラウザを使用する必要があります。

VNC接続は専用端末です。つまり、一度に1人のユーザーだけがVNCクライアントを使用してCVMに接続できません。

## 前提条件

インスタンスにログインするための管理者アカウントとパスワードを取得しました。インスタンス作成時に、システムによるパスワードのランダム発行を選択した場合は、サイト内メールにアクセスしてパスワードを取得してください。

インスタンス作成時に、システムによるパスワードのランダム発行を選択した場合は、[サイト内メッセージ](#)にアクセスして取得してください。

ログインパスワードを設定済みの場合は、そのパスワードを使用してログインしてください。パスワードを忘れた場合は、[インスタンスのパスワードをリセット](#)してください。

## 操作手順

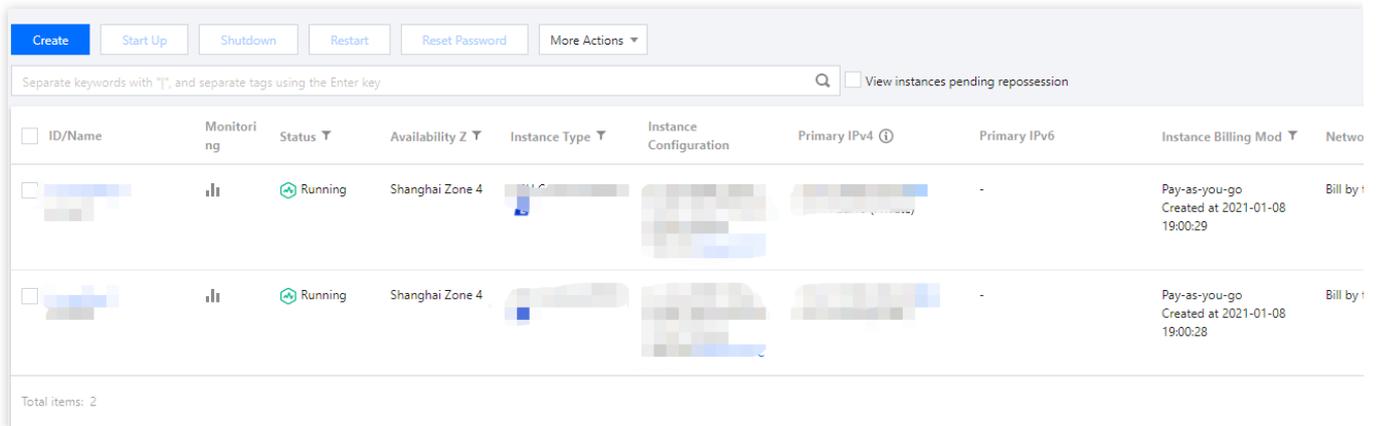
1. [CVMコンソール](#)にログインします。

2. インスタンスの管理画面で、実際に使用されているビューモードに従って操作します。

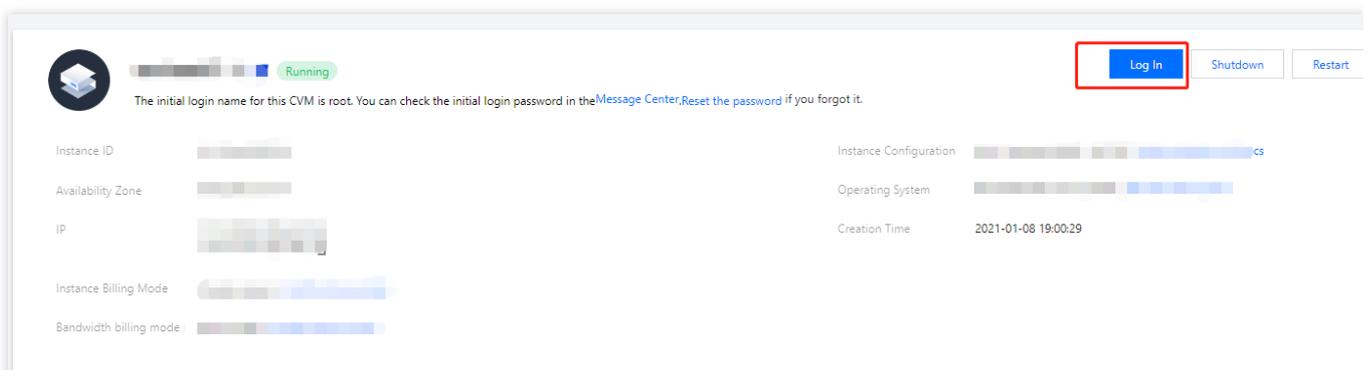
リストビュー

タブビュー

下図に示すように、インスタンスの管理ページで、ログインする Linux CVM インスタンスを選択し、ログインをクリックします。



下図に示すように、ログインしたいLinux CVMタブを選択し、ログインをクリックします。



3. 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。下図のとおりです。

**Log into Linux instance** ×

Standard login method **Recommended** [Login failed?](#)

Supports copy-paste, Chinese input method. Make sure SSH port (TCP:22) is open.

[Log In Now](#)

**Alternative login methods (VNC)**

Copy-paste and Chinese input are not supported.

Note: If VNC login is selected, please enable MFA secondary verification to increase security level.

[Log In Now](#)

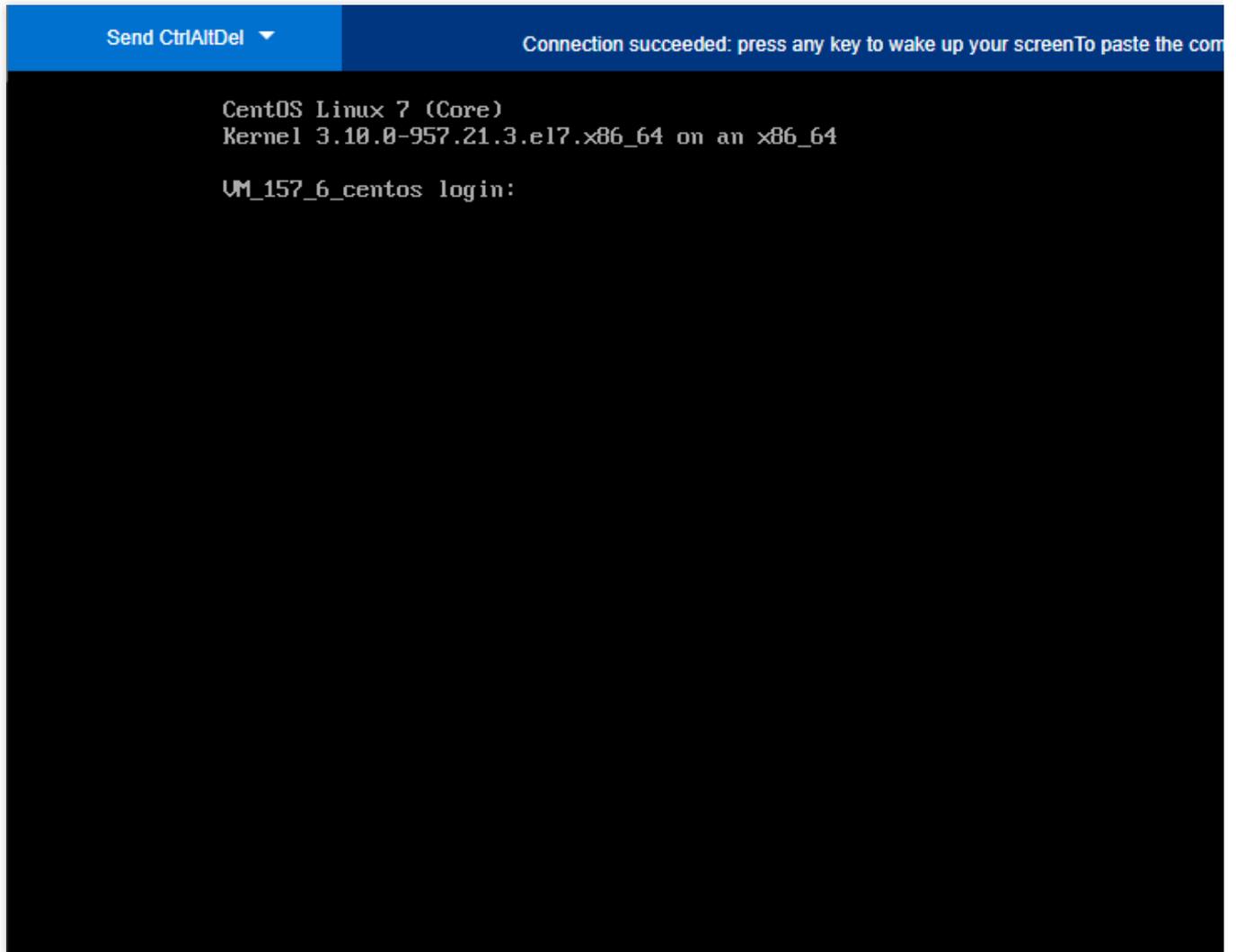
Additional login methods: [Log into Linux CVM](#) [↗](#)

4. 開いたウィンドウの中で、「login」の後ろにユーザー名を入力し、**Enter**を押します。

Linuxインスタンスのデフォルトのユーザー名は `root`、Ubuntuシステムインスタンスのデフォルトのユーザー名は `ubuntu` になります。必要に応じて入力してください。

5. 「Password」の後にパスワードを入力し、**Enter**キーを押します。

入力したパスワードはデフォルトでは表示されません。ログイン完了後、以下に示すように、現在ログインしているCVMの情報がコマンドプロンプトの左側に表示されます。



## その後の操作

CVMにログインした後、個人用Webサイトまたはフォーラムを構築したり、その他の操作を実行したりできます。詳細については、下記のドキュメントをご参照ください：

[Linuxの一般的な操作およびコマンド](#)

[WordPress 個人用サイトを構築する](#)

[Discuz!フォーラムを手動で構築する](#)

# モバイルデバイスを使用してLinuxインスタンスにログインする

最終更新日： : 2023-04-13 10:48:09

## 概要

このドキュメントでは、さまざまなモバイルデバイスからLinuxインスタンスにログインする方法について説明します。ここで使用する接続ツールは、次のとおりです。

iOSデバイス：ここではTermius-SSH clientを例として使用します。

Android デバイス：ここではJuiceSSHを例として使用します。

## 該当するモバイルデバイス

iOSおよびAndroidデバイス

## 前提条件

CVMインスタンスの状態が「実行中」であること。

インスタンスにログインするための管理者のアカウントとパスワード（またはキー）を取得済みであること。

システムのデフォルトパスワードを使用してインスタンスにログインする場合は、最初に [サイト内メール](#) に移動してパスワードを取得してください。

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

CVMインスタンスはすでにパブリックIPを購入されており、このインスタンスは22番ポート（クイック設定で購入したCVMインスタンスの場合、デフォルトで開放している）を開放しました。

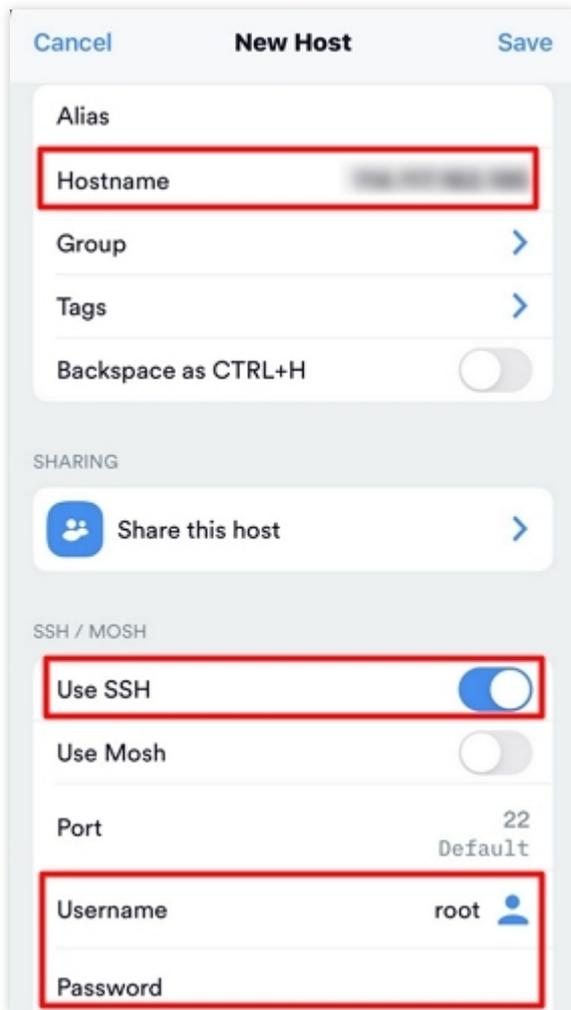
## 操作手順

実際に使用しているモバイルデバイスに基づいて、以下の方法でインスタンスにログインしてください。

iOS デバイス

Android デバイス

1. App StoreからTermius-SSHクライアントをダウンロードし、プロンプトに従って登録します。
2. ホーム画面でNew Hostをクリックします。
3. 「New Host」 ページに進み、以下のログイン情報を設定します。下図のとおりです。



**Hostname** : CVM インスタンスのパブリックIP アドレス。取得方法については、[パブリックIPアドレスの取得](#)をご参照ください。

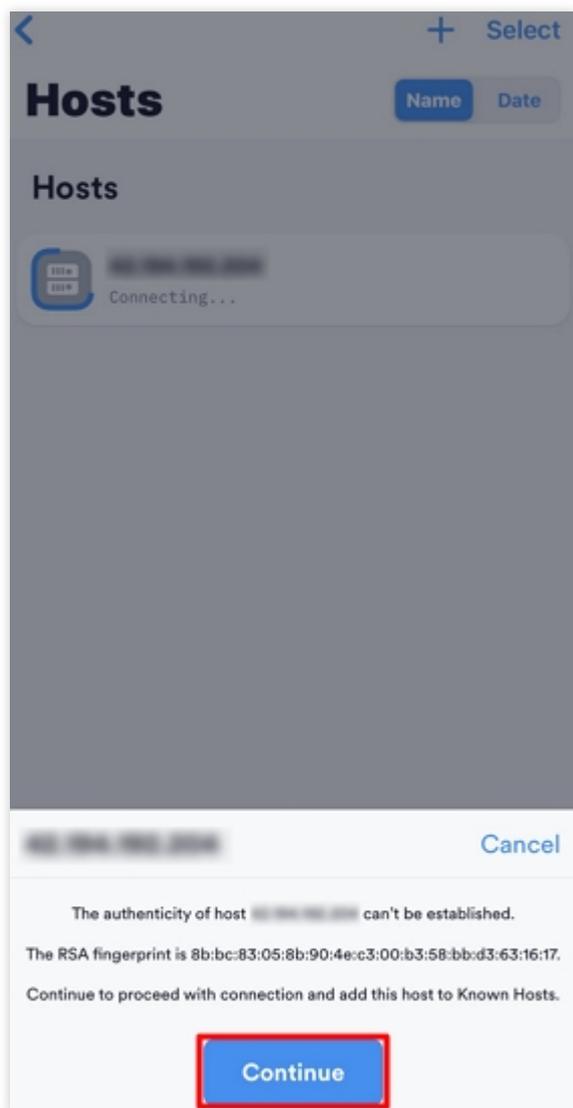
**Use SSH** : デフォルトで有効になっています。

**Username** : 管理者アカウントrootを入力します。Ubuntu OSを使用する場合、管理者アカウントはubuntuになります。

**Password** : インスタンスのログインパスワードを入力します。

4. ページ右上隅の**Save**をクリックしてログイン設定を保存します。

5. 「Hosts」 ページでログイン情報を選択し、ページ下部のポップアップウィンドウで**Continue**をクリックしてログインを確認します。下図のとおりです。



5. 以下の画面が表示されればログイン成功です。

```
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Jun  7 16:10:01 2021 from 98.209.8.12
2
[root@VM-12-4-centos ~]#
```

## 認証情報の新規作成

1. JuiceSSHをダウンロードしてインストールします。
2. ホーム画面で「接続」を選択し、「認証」タブをクリックします。
3. 「認証」タブで、ページの右下隅にある+をクリックします。
4. 「認証の新規作成」ページで、ログインアカウントとパスワードを設定します。

**ニックネーム**：カスタム認証名、オプション。

**ユーザー名**：管理者アカウントのrootを入力します。Ubuntu OSを使用する場合、管理者アカウントはubuntuになります。

**設定（オプション）** を選択し、ポップアップウィンドウにインスタンスのログインパスワードを入力します。

5. ページの右上隅にある✔をクリックすると、認証を新規作成できます。

## 接続の新規作成

1. ホーム画面で「接続」を選択し、「接続」ページの右下隅にある+をクリックします。
2. 「接続の新規作成」ページで、以下のログイン情報を設定します。

**ニックネーム**：カスタム接続名、オプション。

**タイプ**：「SSH」を選択します。

**アドレス**：CVMインスタンスのパブリックIP アドレス。取得方法については、[パブリックIPアドレスの取得](#)をご参照ください。

**認証**：[認証情報の新規作成](#)の手順で追加した認証情報を選択します。

**ポート**：ポート22を入力します。

残りのパラメータはデフォルト設定のままにしておいてください。

3. ページ下部の**グループに追加**をクリックして、ログイン設定を保存します。

## インスタンスへのログイン

1. 「接続」 ページで、ログインするインスタンスを選択し、ポップアップウィンドウで**同意する**をクリックします。
2. 以下の画面が表示されればログイン成功です。

```
Activate the web console with: systemctl enable --now cockpit.socket  
[root@VM-2-6-centos ~]#
```

# Windowsインスタンスにログインする 標準方式を使用してWindowsインスタンスに ログイン（推奨）

最終更新日：：2023-04-11 18:37:02

## 概要

ここでは、標準ログイン方式(WebRDP)を使用してWindowsインスタンスにログインする方法についてご説明します。

### 説明：

この方式はローカルマシンのOSを区別せず、コンソールからWindowsインスタンスへの直接ログインをサポートしています。

## 前提条件

Windowsインスタンスにリモートログインするには、インスタンスの管理者アカウントとパスワードを取得する必要があります。

ログインパスワードを設定済みの場合は、そのパスワードを使用してログインしてください。パスワードを忘れた場合は、[インスタンスのパスワードのリセット方法](#) してください。

インスタンス作成時に、システムによるパスワードのランダム発行を選択した場合は、[サイト内メール](#) にアクセスして初期パスワードを取得してください。

CVMインスタンスはパブリックIPがすでに購入され、インスタンスに関連付けられたセキュリティグループの中で、送信元がWebShellのプロキシIPとなるリモートログインポート（デフォルトは3389）を開放しています。

クイック設定でCVMインスタンスを購入した場合、ポートはデフォルトで開かれます。

カスタム設定経由でCVMインスタンスを購入した場合は、[セキュリティグループの応用例](#) を参照して、ポートを手動で開くことができます。

インスタンスのパブリックネットワーク帯域幅が5Mbit/s以上であることを確認してください。そうでない場合、リモートデスクトップの応答が遅くなる可能性があります。ネットワーク帯域幅の調整が必要な場合は、[ネットワーク構成の変更](#) をご参照ください。

## 操作手順

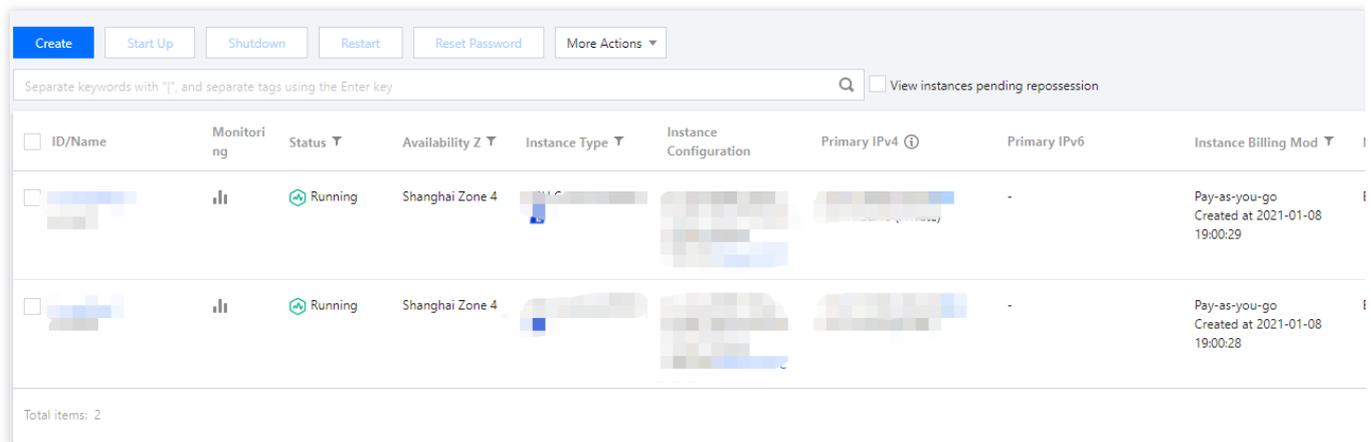
1. [CVMコンソール](#) にログインします。

2. インスタンスの管理画面で、実際に使用されているビューモードに従って操作します。

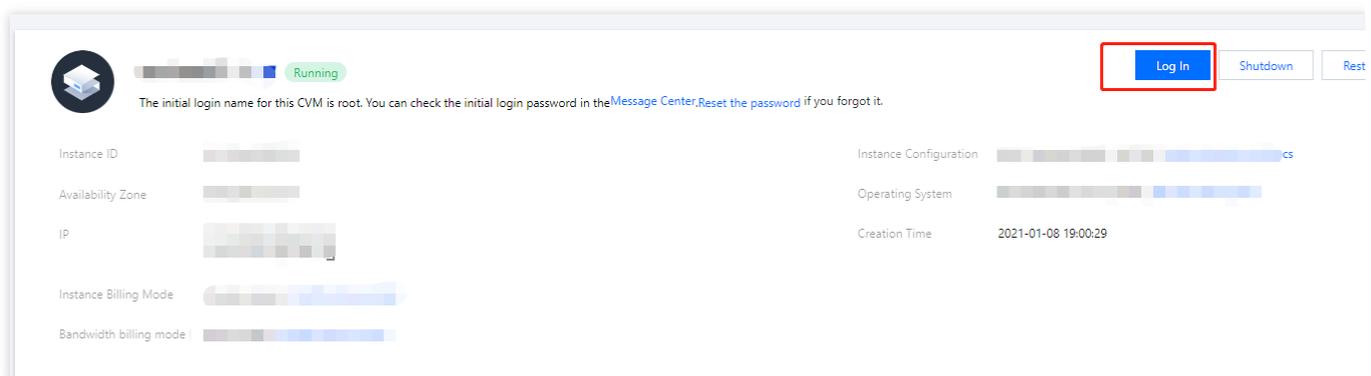
リストビュー

タブビュー

下図のように、ログインする Windows CVM インスタンスを選択し、右側にあるログインをクリックします。



下図のように、ログインする Windows CVM インスタンスのタブを選択し、ログインをクリックします。



3. 開いた「標準ログイン | Windows インスタンス」ウィンドウに、実際の状況に応じてログイン情報を入力します。

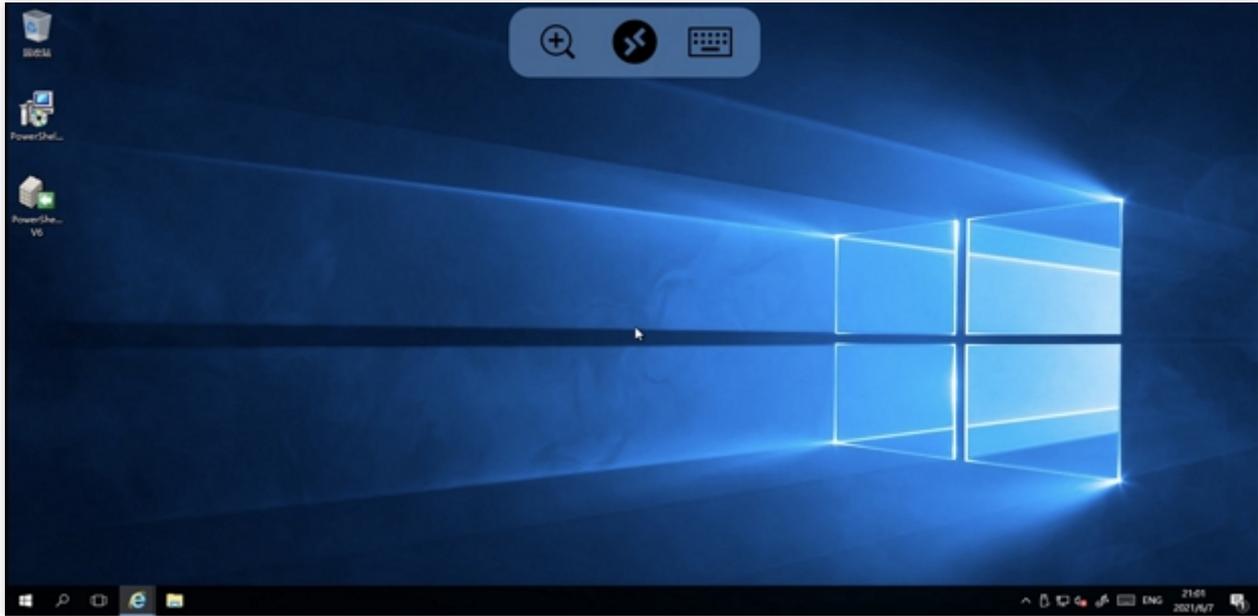
**ポート**：デフォルトは3389です。必要に応じて入力してください。

**ユーザー名**：Windows インスタンスのデフォルトのユーザー名は Administrator です。必要に応じて入力してください。

**パスワード**：前提条件のステップで取得したログインパスワードを入力します。

4. ログインをクリックすると、Windows インスタンスにログインできます。

ここでは、OSがWindows Server 2016 Data center Edition 64ビット英語版であるCVMを例とします。ログインに成功すると以下のような画面が表示されます。



## 関連ドキュメント

[インスタンスのパスワードのリセット方法](#)

[ネットワーク設定の調整](#)

# RDPファイルを使用してWindowsインスタンスにログインする

最終更新日： : 2023-04-20 17:37:53

## ご注意：

WebRDPは、Windowsインスタンスのデフォルトのログイン方法です。ローカルのログインクライアントをダウンロードすることなく、CVMコンソールからワンクリックでWindowsインスタンスにログインできます。ログイン方式については、[標準方式を使用してWindowsインスタンスにログイン（推奨）](#)をご参照ください。

## 概要

RDPはRemote Desktop Protocolの略称であり。お客様のローカルコンピュータがリモートコンピュータに接続できるようにするためにMicrosoftが開発したマルチチャンネルプロトコルです。Tencent Cloudは、Windows CVMへのログインにRDP方式を推奨しています。このドキュメントは、RDPファイルを使用してWindowsインスタンスにログインする方法について説明します。

## サポートされるシステム

Windows、Linuxと Mac OSは全てRDPを使用してCVMにログインすることができます。

## 前提条件

Windowsインスタンスにリモートログインするには、インスタンスの管理者アカウントとパスワードを取得する必要があります。

インスタンス作成時に、システムによるパスワードのランダム発行を選択した場合は、[サイト内メール](#)にアクセスしてパスワードを取得してください。

ログインパスワードを設定済みの場合は、そのパスワードを使用してログインしてください。パスワードを忘れた場合は、[インスタンスのパスワードをリセット](#)してください。

CVMインスタンスはパブリックIPがすでに購入され、インスタンスに関連付けられたセキュリティグループの中で、送信元がWebShellのプロキシIPとなるリモートログインポート（デフォルトは3389）を開放しています。

クイック設定でCVMインスタンスを購入した場合、ポートはデフォルトで開かれます。

カスタム設定経由でCVMインスタンスを購入した場合は、[セキュリティグループの応用例](#)を参照して、ポートを手動で開くことができます。

インスタンスのパブリックネットワーク帯域幅が 5Mbit/s 以上であることを確認してください。そうでない場合、リモートデスクトップの応答が遅くなる可能性があります。ネットワーク帯域幅の調整が必要な場合は、[ネットワーク設定の調整](#) をご参照ください。

## 操作手順

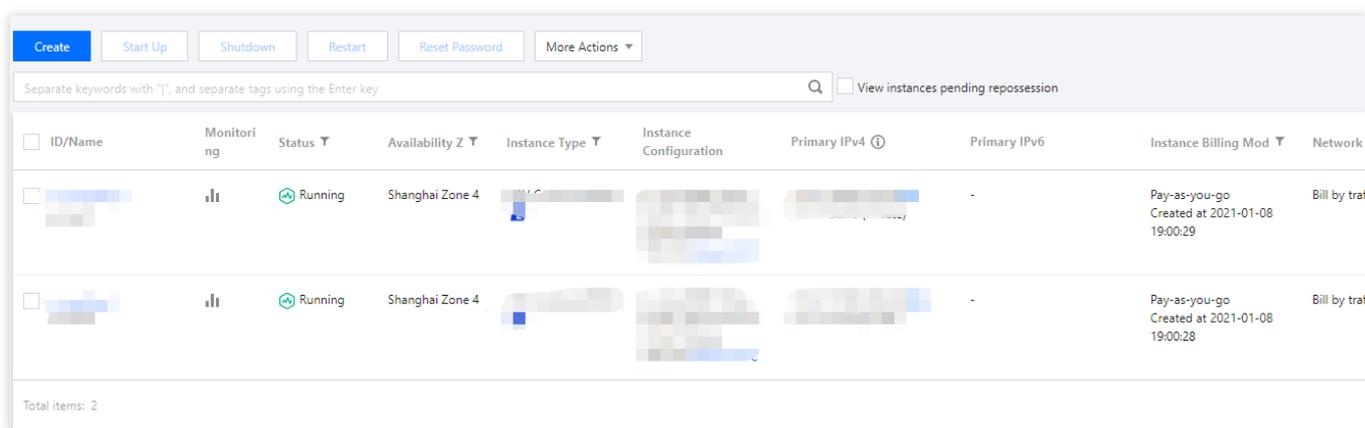
Windows システム

Linux システム

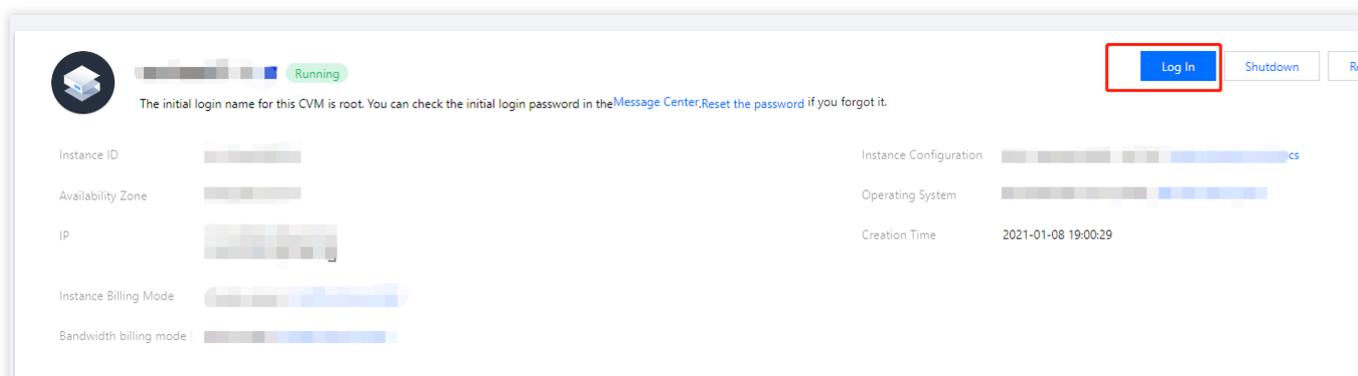
MacOS システム

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画面で、実際に使用されているビューモードに従って操作します。

**リストモード：**インスタンスの管理ページで、ログインするWindows CVM インスタンスを選択して、右側にある **ログイン** をクリックします。



**タブモード：**下図のように、ログインしたいWindows CVMタブを選択し、**ログイン** をクリックします。



3. 開いた「標準ログイン | Windowsインスタンス」ウィンドウの中から、**RDPファイルのダウンロード**を選択し、RDPファイルをローカルにダウンロードします。

**説明：**

リモートデスクトップ接続で使われているポート番号を変更した場合は、RDPファイルを変更し、IPアドレスの後ろに：ポートを追加する必要があります。

### Log into Windows instance

Log in with RDP file Recommended Login failed

Download and run the RDP file to log into Remote Desktop. Please ensure that the remote login port (TCP:3389) is open.

Note: copy and paste is supported.

1. For Windows OS, please click the button below to download RDP file. For details , please see [Logging into Windows Instance.](#)
2. For Linux system, please install [rdesktop.](#)
3. For MacOS, please install [Microsoft Remote Desktop for Mac.](#)

Alternative login methods (VNC)

Copy-paste and Chinese input are not supported.

Note: If VNC login is selected, please enable MFA secondary verification to increase security level.

[Log In Now](#)

More methods: [Log into Windows CVM](#)

4. ローカルにダウンロードしたRDPファイルをダブルクリックして開き、パスワードを入力します。最後に「OK」をクリックすればリモート接続が許可されます。

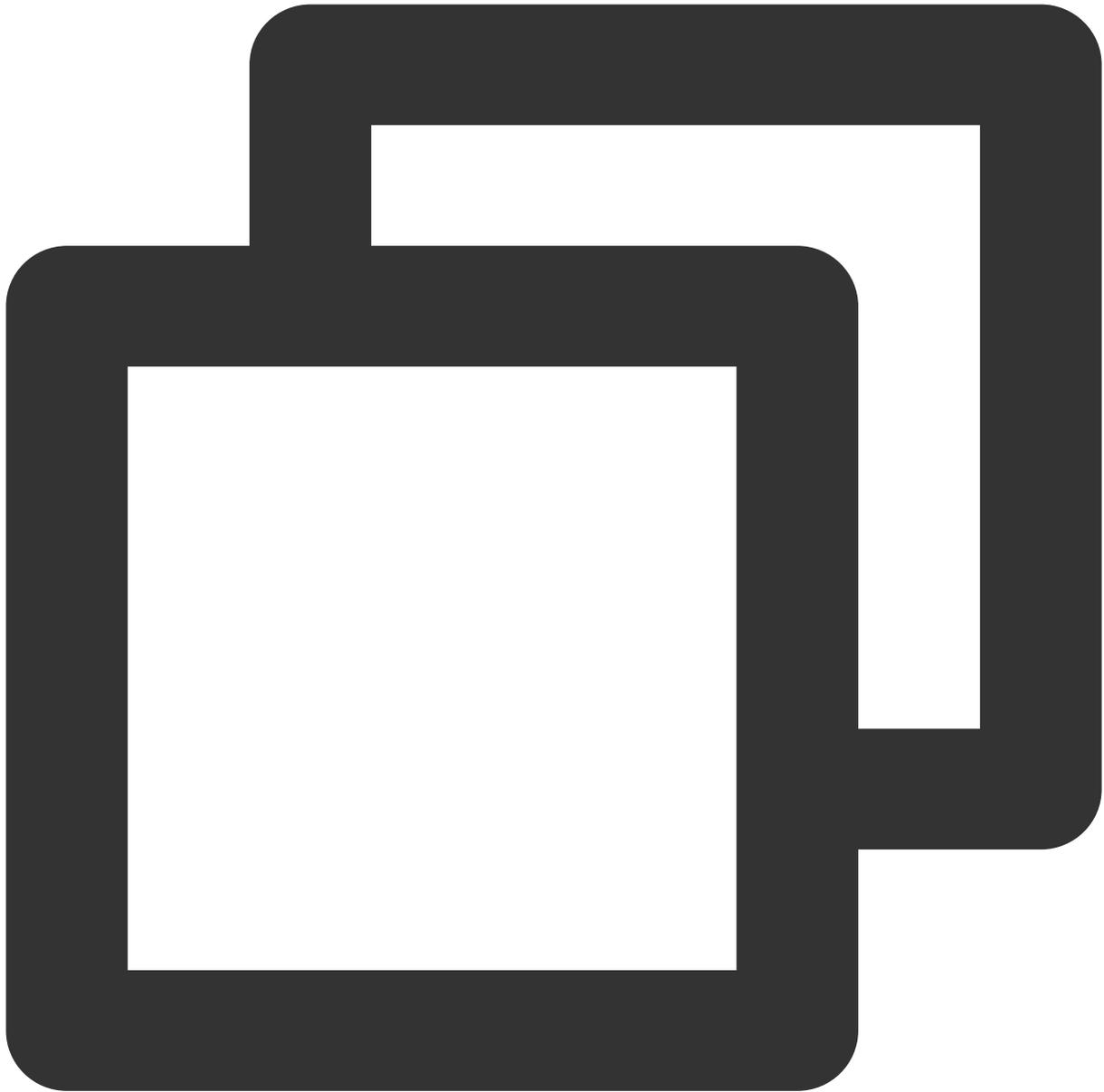
システムのデフォルトパスワードを使用してインスタンスにログインする場合は、[サイト内メール](#)にアクセスしてパスワードを取得してください。

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

#### 説明：

リモートデスクトップクライアントとしてrdesktopを使用することをお勧めします。詳細については、[rdesktop公式説明](#)をご参照ください。

1. 以下のコマンドを実行し、rdesktop がインストールされているかどうかを確認します。



```
rdesktop
```

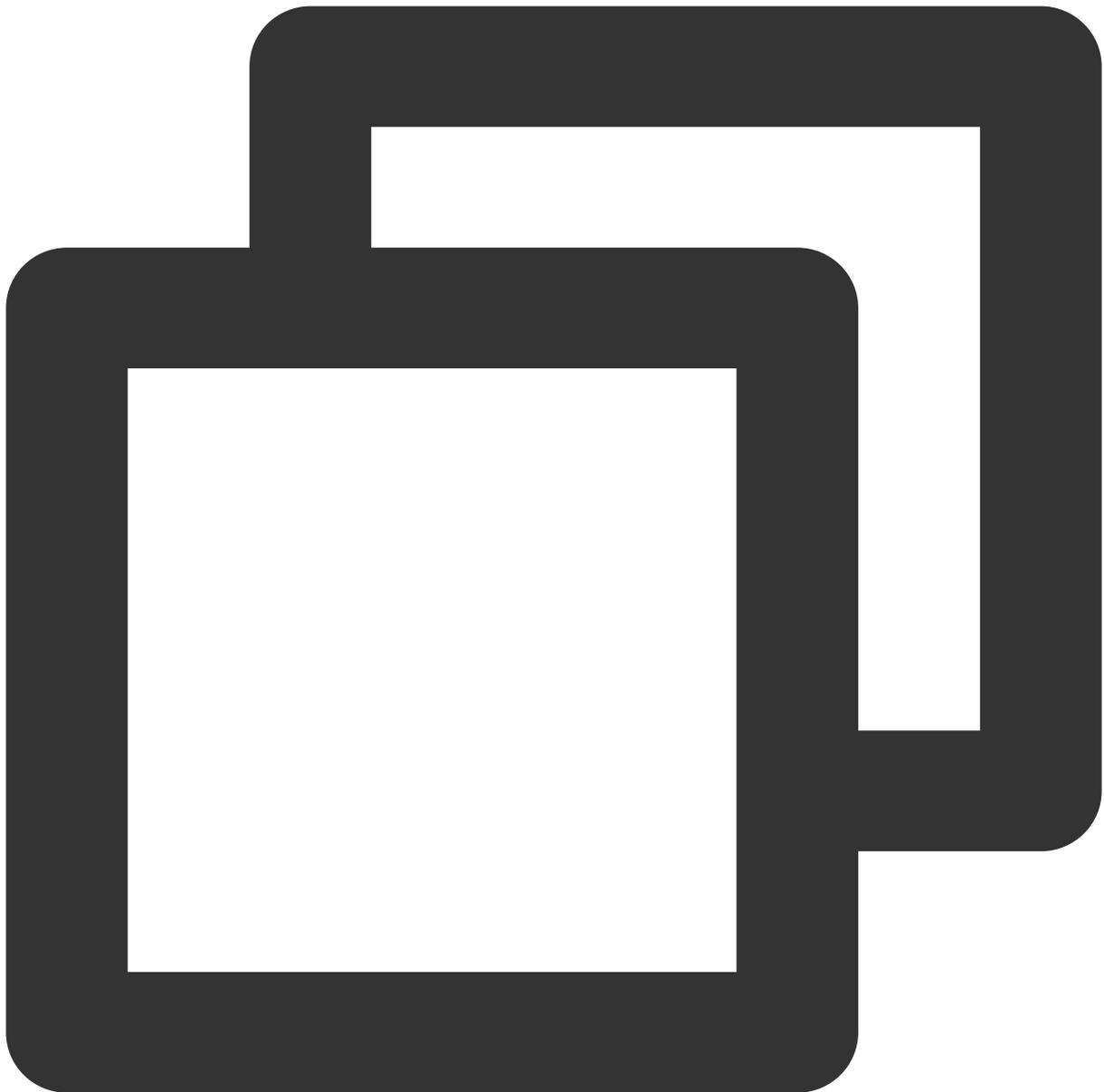
rdesktopをインストールしている場合、[ステップ4](#)を実行してください。

command not foundというプロンプトが表示された場合、rdesktopをインストールされていないことを示し、[ステップ2](#)を実行してください。

2.

ターミナル

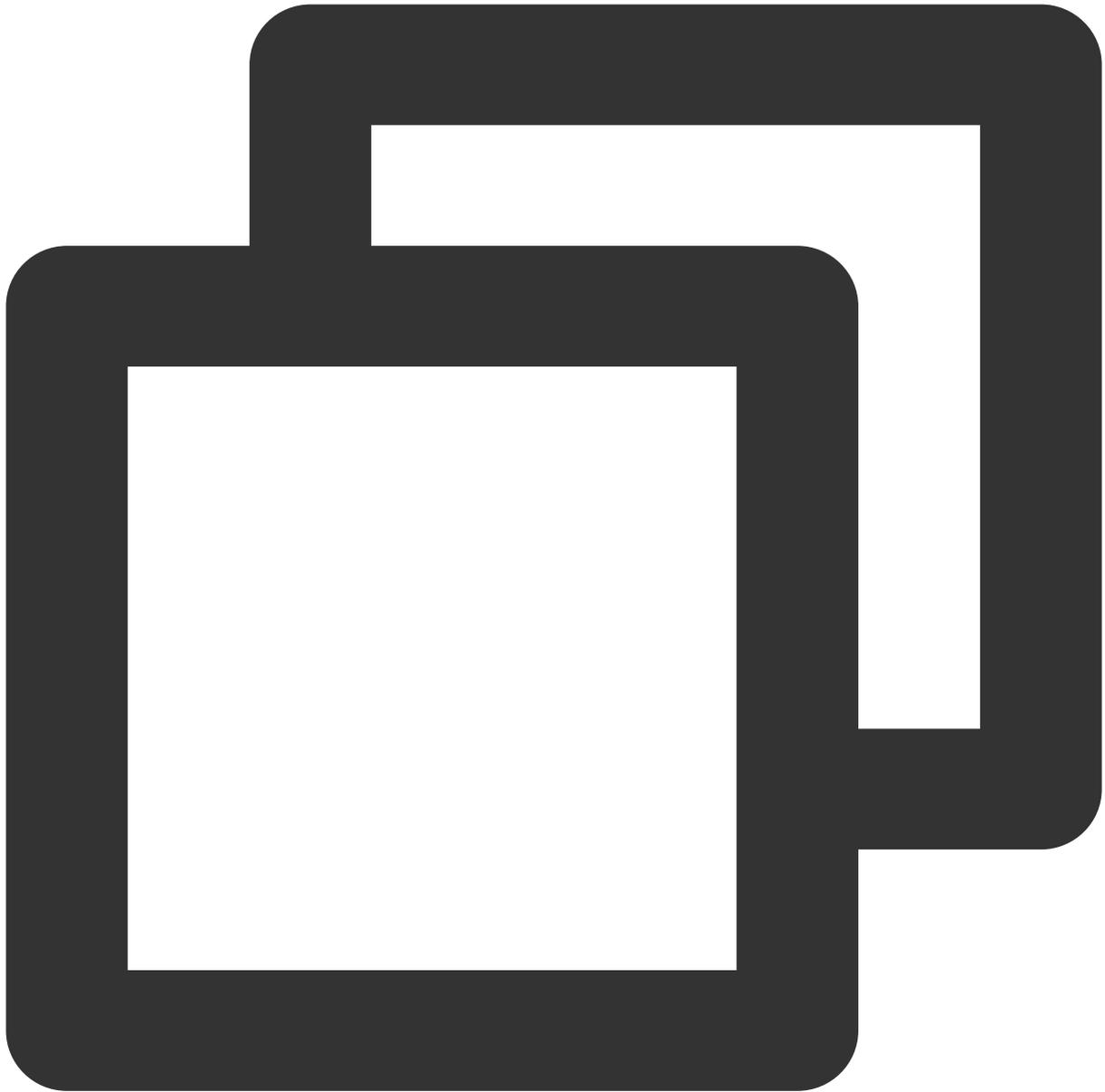
ウィンドウで以下のコマンドを実行してrdesktopインストールパッケージをダウンロードします。この手順はrdesktop 1.8.3バージョンを例とします。



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

最新のインストールパッケージが必要な場合は、[GitHub rdesktopページ](#) にアクセスして最新のインストールパッケージをさがし、コマンドラインを最新のインストールパスに置き換えます。

3. rdesktopをインストールするディレクトリで、以下のコマンドを実行し、rdesktopを解凍してインストールします。



```
tar xvzf rdesktop-<x.x.x>.tar.gz ##x.x.xをダウンロードしたバージョン番号に置き換えます
cd rdesktop-1.8.3
./configure
make
make install
```

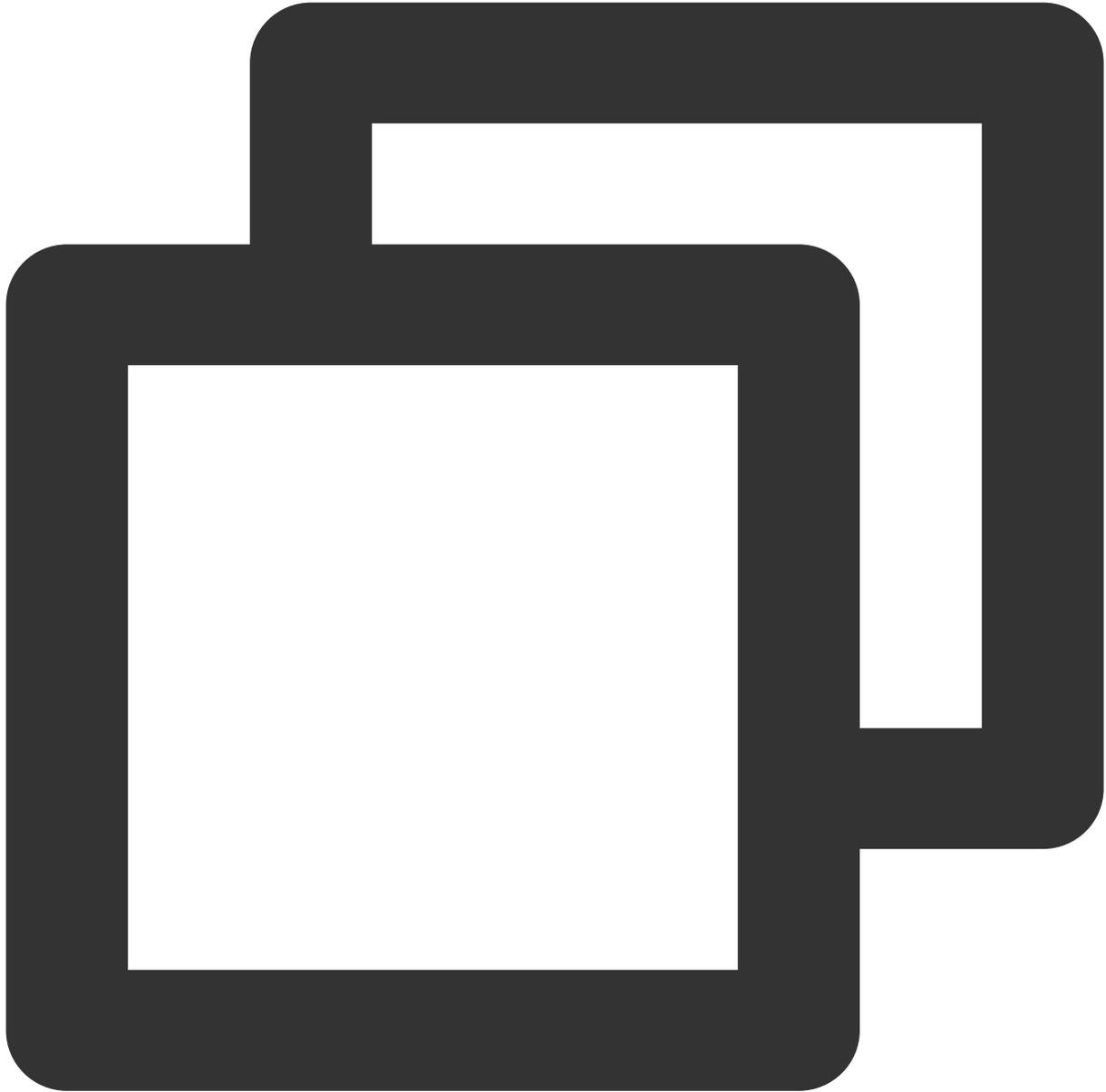
4.

以下

のコマンドを実行してWindowsインスタンスにリモートで接続できます。

**説明：**

例の中のパラメータをご自分のパラメータに変更してください。



```
rdesktop -u Administrator -p <your-password> <hostname or IP address>
```

`Administrator` は前提条件で入手した管理者アカウントです。

`<your-password>` は設定されたログインパスワードです。

システムのデフォルトパスワードを使用してインスタンスにログインする場合、[サイト内メール](#) からパスワードを取得してください。パスワードを忘れた場合、[インスタンスのパスワードをリセット](#) してください。

`<hostname or IP address>` は、お客様のWindowsインスタンスのパブリックIPまたはカスタムドメイン名となります。インスタンスのパブリックIPの取得方法は、[パブリックIPアドレスの取得](#) をご参照ください。

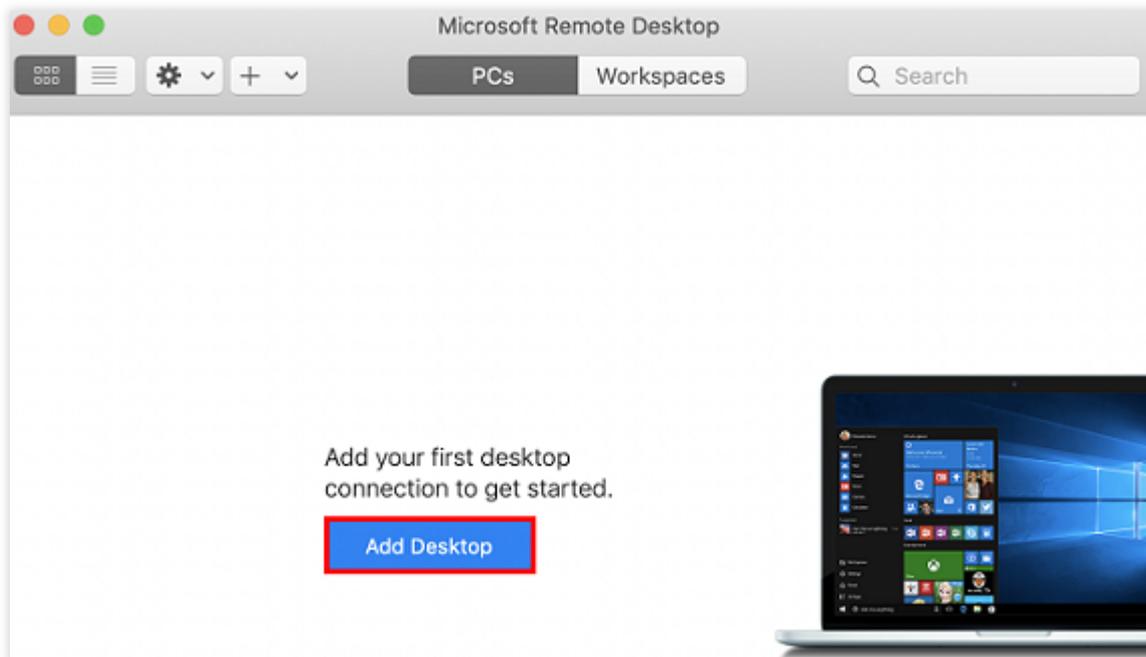
**説明：**

以下の操作は Microsoft Remote Desktop for Mac の例です。マイクロソフトは2017年にRemote Desktopクライアントのダウンロードリンクの提供を正式に停止し、現在は、子会社のHockeyAppがベータ版を配布しています。

[Microsoft Remote Desktop Beta](#) でベータ版をダウンロードすることができます。

以下の操作は、Windows Server 2012 R2 OSのCVMインスタンスに接続する方法を例に説明します。

1. Microsoft Remote Desktop for Mac をローカルコンピューターにダウンロードしてインストールします。
2. MRDを起動して、下図に示すように**Add Desktop**をクリックします。



3. 表示された「Add Desktop」ウィンドウで、以下の手順に従って、接続を作成します。下図に示すように：

**Add PC**

PC name: 118. [REDACTED]

User account: Ask when required

General | Display | Devices & Audio | Folders

Friendly name: Optional

Group: Saved PCs

Gateway: No gateway

Bypass for local addresses

Reconnect if the connection is dropped

Connect to an admin session

Swap mouse buttons

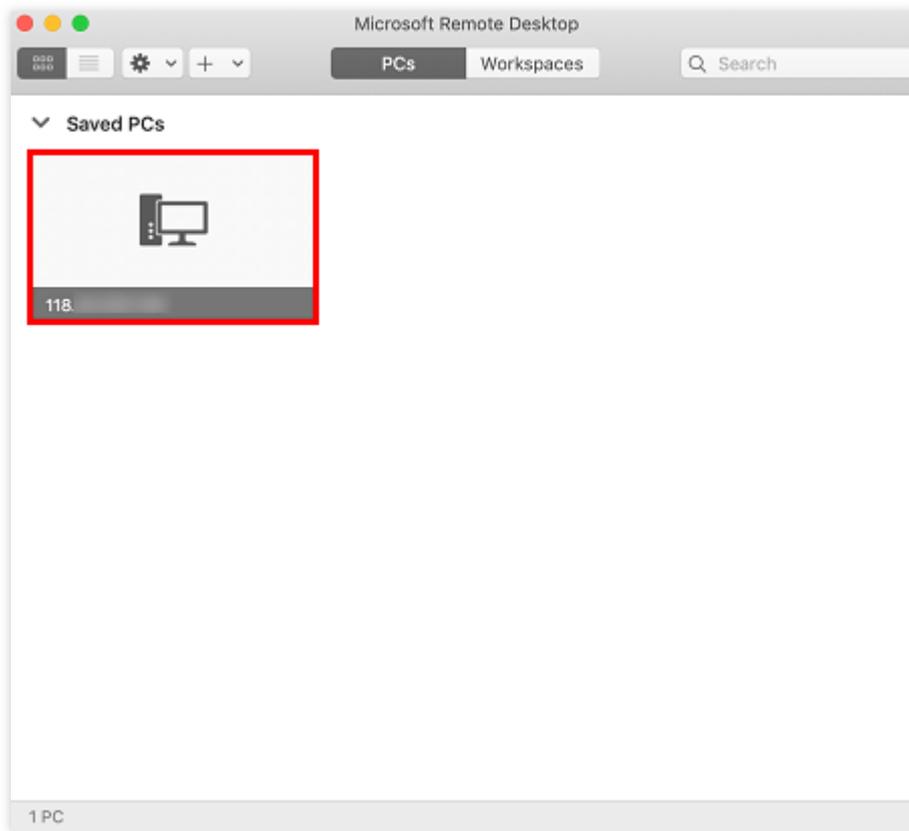
Cancel Add

3.1 「PC name」にCVMインスタンスのパブリックIPアドレスを入力します。パブリックIPアドレスを取得する方法の詳細については、[パブリックIPアドレスの取得](#)をご参照ください。

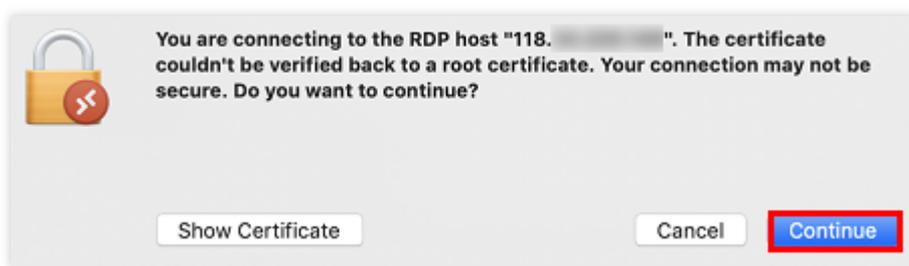
3.2 **Add**をクリックします。

3.3 他のオプションはデフォルト設定のまま、接続が作成されます。

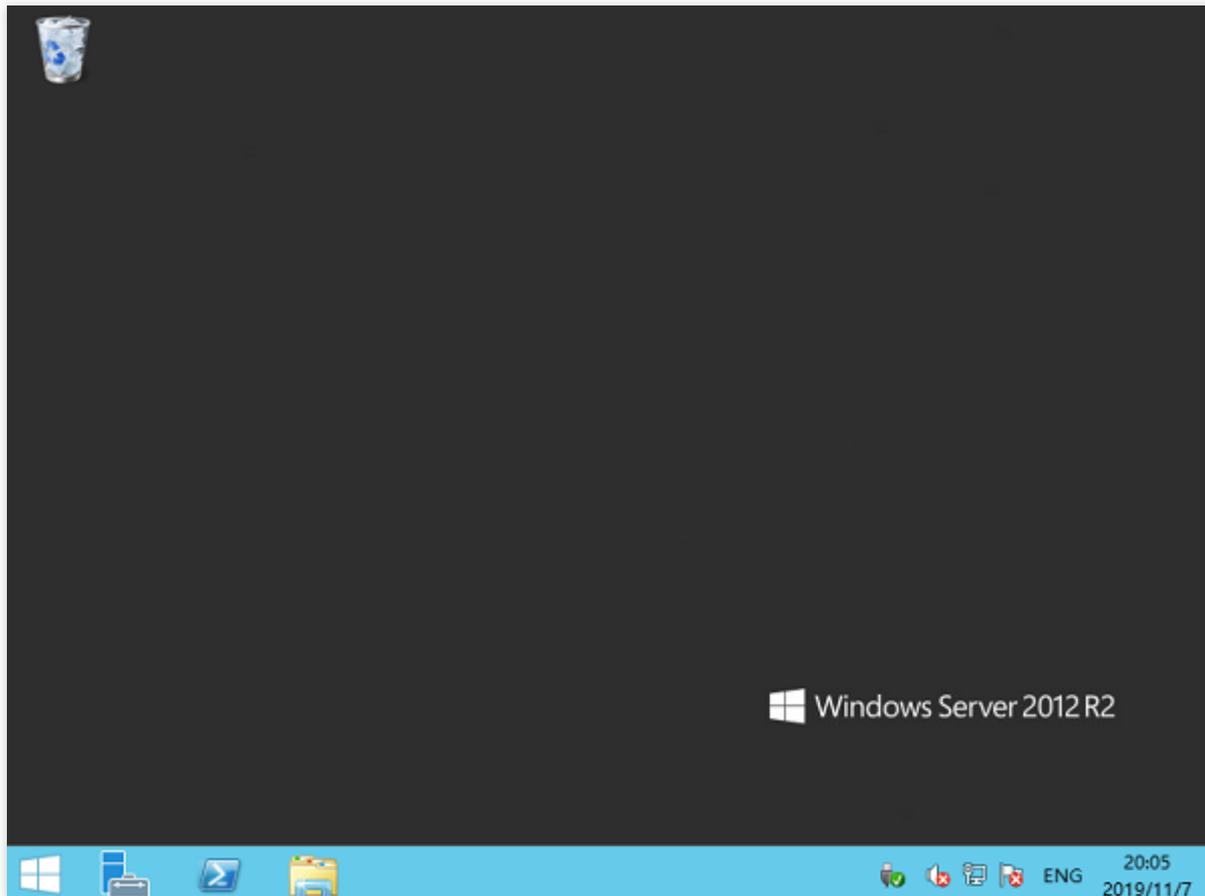
ウィンドウで作成された接続を確認できます。下図に示すように：



4. 新規作成した接続をダブルクリックして開き、ポップアップウィンドウでプロンプトに従って、CVMのアカウントとパスワードを入力し、**Continue**をクリックします。
5. システムのデフォルトパスワードを使用してインスタンスにログインする場合は、[サイト内メール](#)にアクセスしてパスワードを取得してください。
6. パスワードを忘れた場合は、[インスタンスのパスワードをリセット](#)してください。
7. 下図のように、ポップアップしたウィンドウで**Continue**をクリックして、接続を確認します。



接続に成功すると、次のページが表示されます。



## RDP帯域幅制限の説明

利用可能なネットワーク帯域幅は、RDP経由のログインやCVMの使用体験に直接影響し、アプリケーションプログラムやディスプレイ解像度ごとに、各々のネットワーク構成が必要です。マイクロソフトは、それぞれのユースケースでRDPを使用する時のインスタンスの最小帯域幅要件を提供しています。下表を参照して、インスタンスのネットワーク設定が業務のニーズを確実に満たすようにしてください。そうでない場合、遅延などの問題が発生する可能性があります。

### 説明：

インスタンスの帯域幅を調整したい場合は、[ネットワーク設定の調整](#)をご参照ください。

以下のデータは、解像度が1920x1080で、デフォルトのグラフィックモードとH.264/AVC 444グラフィックモードを同時に採用する単一のモニター構成に適用されます。

シナリオ	デフォルトモード	H.264/AVC 444 モード	シナリオ説明
休眠	0.3Kbps	0.3Kbps	ユーザーがすでに作動を一次停止し、アクティブな画面更新が発生していない状態。
Microsoft	100 -	200 - 300	ユーザーがMicrosoft Word、印刷、図形のペーストをアクティブ

Word	150 Kbps	Kbps	に使用中で、ドキュメント間の切り替えも行っている状態。
Microsoft Excel	150 - 200Kbps	400 - 500Kbps	ユーザーがMicrosoft Excelをアクティブに使用中で、同時に公式や図表が含まれた複数のセルを更新している状態。
Microsoft PowerPoint	4 - 4.5Mbps	1.6 - 1.8Mbps	ユーザーがMicrosoft PowerPoint、印刷、ペーストをアクティブに使用中。またコンテンツが豊富な図形を変更中で、スライドショー効果も使用している状態。
Web閲覧	6 - 6.5Mbps	0.9 - 1Mbps	ユーザーがグラフィックコンテンツが豊富なウェブサイトをアクティブに閲覧中（横方向および縦方向にページをスクロール）で、その中に複数の静止画や動画が含まれている状態。
画像ライブラリ	3.3 - 3.6Mbps	0.7 - 0.8Mbps	ユーザーが画像ライブラリアプリケーションプログラムをアクティブに使用中。画像の閲覧、スケーリング、サイズの調整、回転を行っている状態。
ビデオ再生	8.5 - 9.5Mbps	2.5 - 2.8Mbps	ユーザーがスクリーンの半分を占有する30FPSのビデオを視聴中。
フルスクリーンビデオ再生	7.5 - 8.5Mbps	2.5 - 3.1Mbps	ユーザーがフルスクリーンに最大化した30FPSのビデオを視聴中。

# リモートデスクトップ接続を使用して Windowsインスタンスにログインする

最終更新日： : 2023-04-11 18:28:31

## 概要

ここでは、Windowsシステムのローカルコンピュータでのリモートデスクトップを介したWindowsインスタンスへのログイン方法について説明します。

## サポートされているOS

Windows

## 前提条件

Windowsインスタンスにリモートログインするには、インスタンスの管理者アカウント番号と対応するパスワードを獲得する必要があります。

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

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

お客様のCVMインスタンスはパブリックIPをすでに購入しており、3389番ポートが開いています(このポートは、クイック設定で購入したCVMインスタンスに対してデフォルトで開いています)。

## 操作手順

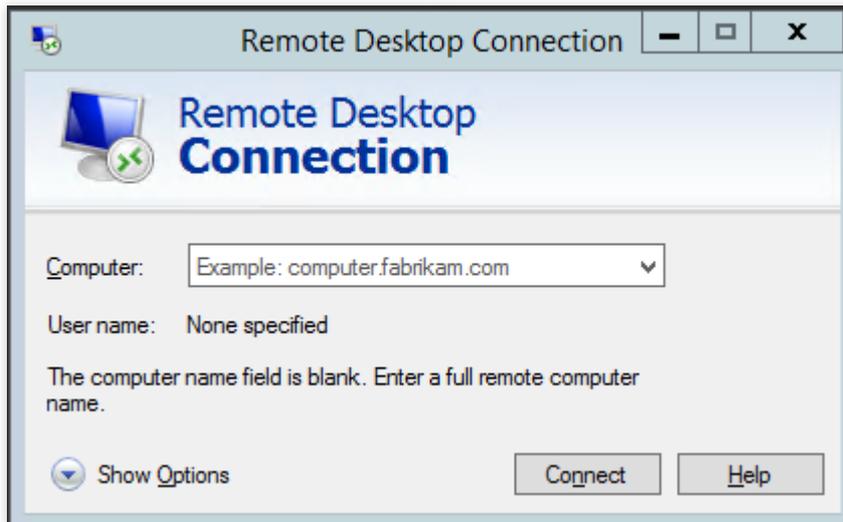
### 説明：

以下Windows7OSを例にとって、操作手順を説明します。

1. 下図に示すように、ローカルのWindowsコンピュータで、



をクリックし、**プログラムとファイルの検索欄**に**mstsc**と入力し、**Enter**を押して、リモートデスクトップ接続ダイアログボックスを開きます。

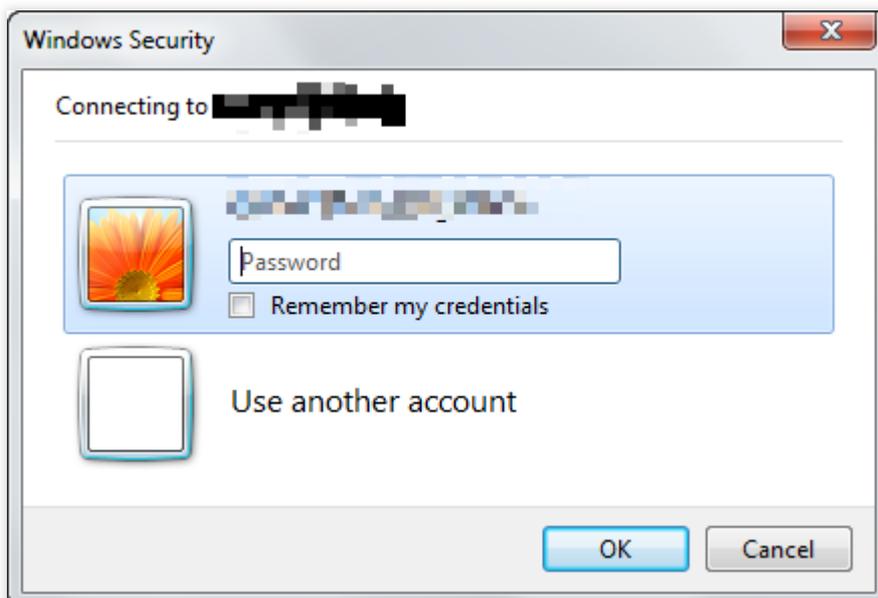


2. 「コンピュータ」の後にWindowsサーバーのパブリックIPを入力し、**接続**をクリックします。 [パブリックIPアドレスの取得](#)を参考にサーバーのパブリックIPを取得できます。
3. 下図に示すように、ポップアップした「Windowsセキュリティ」ウィンドウに、インスタンスの管理者アカウントとパスワードを入力します。

**説明：**

「このリモート接続を信頼しますか。」というダイアログボックスが表示されたら、「このコンピューターへの接続について今後確認しない」にチェックを入れ、**接続**をクリックします。

Windows CVMインスタンスのデフォルトの管理者アカウントは `Administrator` で、パスワードは[前提条件](#)を参考に取得できます。



4. OKをクリックすると、Windowsインスタンスにログインできます。

# VNCを使用してWindowsインスタンスにログインする

最終更新日： : 2023-04-11 18:22:45

## 概要

VNC接続は、Tencent Cloudが提供するWebブラウザ経由でCVMにリモート接続する方式です。クライアントにリモートデスクトップサービスがインストールされていないかまたはリモートデスクトップ接続ができない場合や、いかなる方法でも接続できない場合は、ユーザーはVNCを介してCVMにログインし、CVMの状態を観察し、かつCVMアカウントから基本的なCVM管理操作を行うことができます。

## 使用制限

VNC経由でログインしたCVMは現在、コピー・ペースト機能、中国語入力ソフト、およびファイルのアップロードまたはダウンロードをサポートしていません。

VNC経由でCVMにログインする場合は、Chrome、Firefox、IE 10 以降などの主流のブラウザを使用する必要があります。

VNC接続は専用端末です。つまり、一度に1人のユーザーだけがVNCクライアントを使用してCVMに接続できます。

## 前提条件

Windowsインスタンスにリモートログインするには、インスタンスの管理者アカウント番号と対応するパスワードを獲得する必要があります。

インスタンス作成時に、システムによるパスワードのランダム発行を選択した場合は、[サイト内メール](#)からパスワードを取得してください。

ログインパスワードを設定済みの場合は、そのパスワードを使用してログインしてください。パスワードを忘れた場合は、[インスタンスのパスワードをリセット](#)してください。

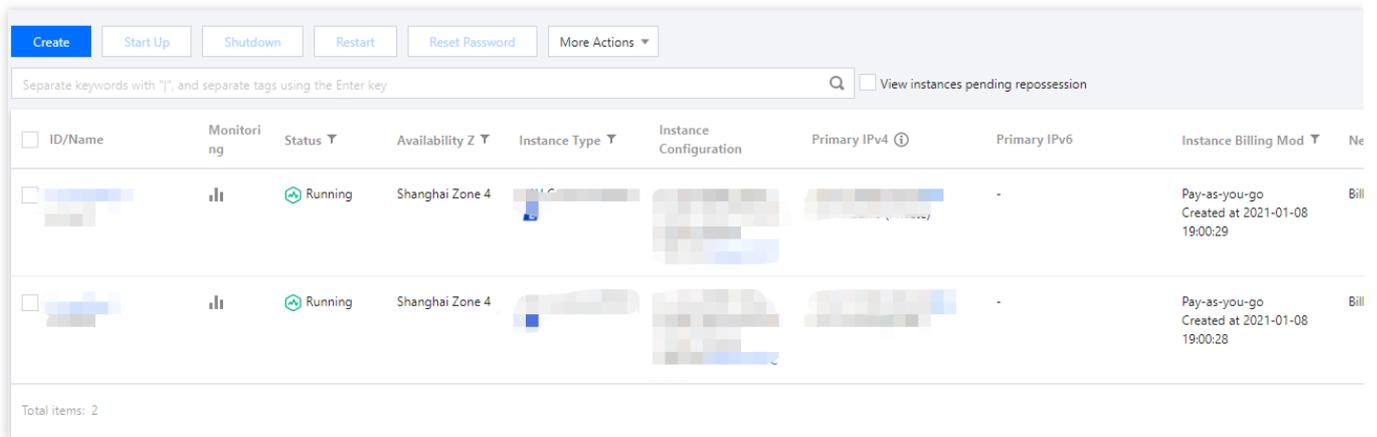
## 操作手順

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画面で、ログインするWindows CVMインスタンスを選択し、[ログイン](#)をクリックします。

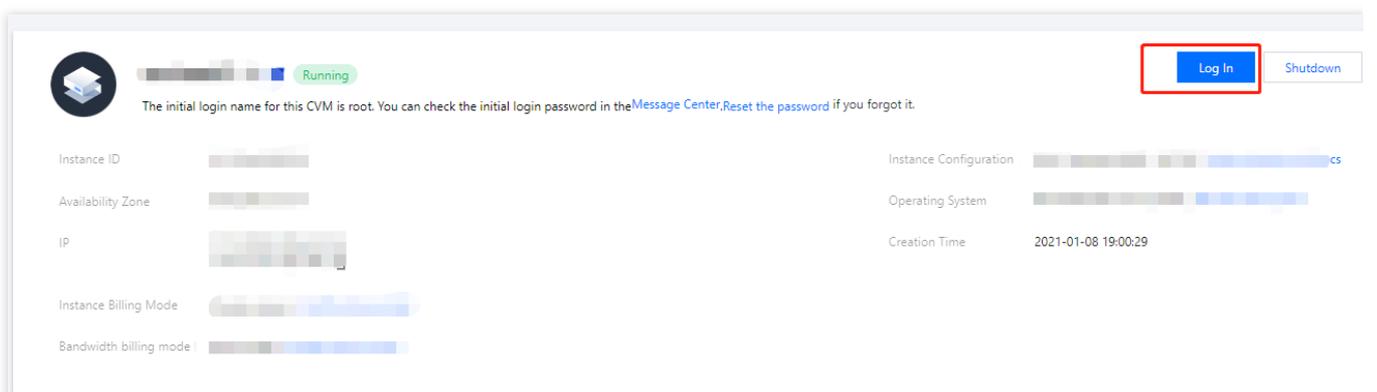
リストビュー

タブビュー

下図のように、ログインしたいWindows CVMを探し、右側にある**ログイン**をクリックします。



下図のように、ログインしたいWindows CVMタブを選択し、**ログイン**をクリックします。



3. 開いた「標準ログイン | Windows インスタンス」ウィンドウの中から、**VNCログイン**を選択します。下図のとおりです。

## Log into Windows instance

Log in with RDP file **Recommended**

[Login fa](#)

Download and run the RDP file to log into Remote Desktop. Please ensure that the remote login port (TCP:3389) is open.

Note: copy and paste is supported

For Windows OS, please click the button below to download RDP file. For details , please see [Log into Windows instances](#) [↗](#)

[Download RDP file](#)

2. For Linux system, please install [rdesktop](#) [↗](#)

3. For MacOS, please install [Microsoft Remote Desktop for Mac](#) [↗](#)

### Alternative login methods (VNC)

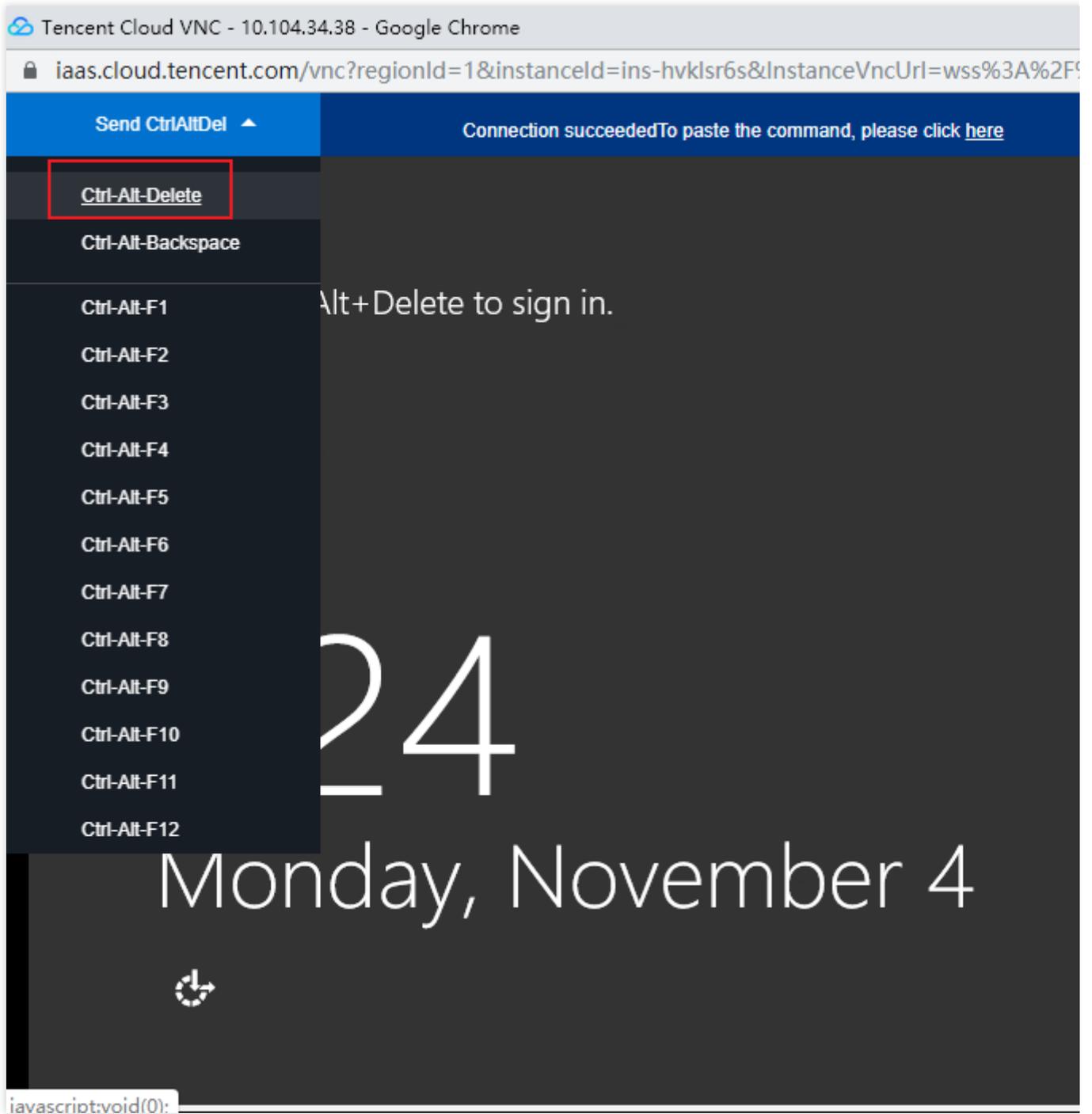
Copy-paste and Chinese input are not supported.

Note: If VNC login is selected, please enable MFA secondary verification to increase security level.

[Log In Now](#)

Additional login methods: [Log into Windows CVM](#) [↗](#)

4. 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入ります。下図のとおりです。



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。

# モバイルデバイスからWindowsインスタンスにログインする

最終更新日： : 2023-04-13 15:26:32

## 概要

このドキュメントでは、Microsoftリモートデスクトップクライアントを使用してさまざまなモバイルデバイスからWindows インスタンスにログインする方法について説明します。

## サポートされているモバイルデバイス

iOSおよびAndroidデバイス

## 前提条件

CVMインスタンスの状態が「実行中」であること。

インスタンスにログインするための管理者のアカウントとパスワードを取得済みであること。

システムのデフォルトパスワードを使用してインスタンスにログインする場合は、[サイト内メール](#)に移動してパスワードを取得してください。

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

CVMインスタンスはパブリックIPをすでに購入しており、3389番ポートが開いています(このポートは、クイック設定で購入したCVMインスタンスに対してデフォルトで開いています)。

## 操作手順

### 説明：

この操作手順では、iOSデバイスを例とします。Androidデバイスの実際の操作手順と大差ありません。

1. Microsoftリモートデスクトップをダウンロードして、RD Clientを起動します。
2. 「PC」 ページで、右上隅の + を選択し、ポップアップメニューから**Add PC**をクリックします。
3. 「Add PC」 ページで、以下のログイン情報を設定します。

**PC名:** CVMインスタンスのパブリックIPアドレス。取得方法については、[パブリックIPアドレスの取得](#)をご参照ください。

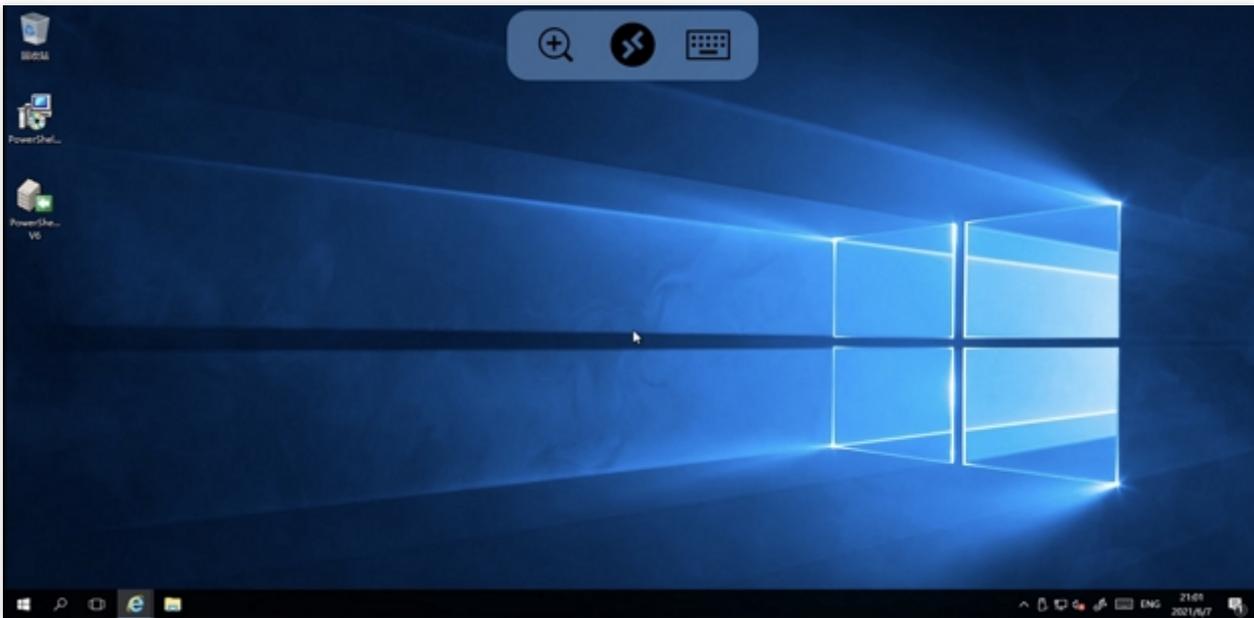
**ユーザーアカウント:** デフォルトでは、「Ask when required」が選択されています。

4. 入力完了後、**Save**をクリックします。
5. 「PC」 ページで、ログインするインスタンスを選択し、ポップアップウィンドウにインスタンスの管理者アカウントとパスワードを入力します。

**管理者アカウント**：Windowsインスタンスの管理者アカウントは `Administrator` です。

**パスワード**：インスタンスのログインパスワードを入力します。

6. **Continue**をクリックします。次のような画面が表示されている場合は、Windowsインスタンスへのログインに成功したことを意味します。



# 設定を調整する インスタンス構成の変更

最終更新日：：2023-04-13 15:28:07

## 概要

Tencent Cloud CVMインスタンスのハードウェアデバイスは、迅速かつ柔軟に調整できます。このドキュメントでは、インスタンス構成のアップグレード、ダウングレード、およびモデルに跨る構成変更に関する操作方法および関連注意事項について説明します。

## 前提条件

インスタンスの状態が「シャットダウン」または「実行中」の場合、構成を変更できます。インスタンスが実行中の場合、強制的にシャットダウンして再起動すると、変更が有効になります。

### ご注意：

インスタンスが**シャットダウン**状態の場合は、コンソールで変更を直接実行できます。

インスタンスが実行中の場合は、オンラインで構成を変更できます。操作完了後、強制シャットダウンを確認する必要があります。インスタンスの再起動後に変更が有効になります。

インスタンスの構成をオンラインで**一括変更**可能です。一括変更操作を実行するときに、**実行中**のインスタンスがある場合は、インスタンスを強制的にシャットダウンする必要があります。インスタンスの再起動後に変更が有効になります。

## 制限事項と影響

### 構成変更実行時の制限事項

システムディスクとデータディスクの両方とも**CBSクラウドディスク**であるインスタンスのみが、構成の変更をサポートします。

#### 構成のアップグレード

回数無制限、アップグレードはすぐに有効になります。

#### 構成のダウングレード

従量課金インスタンスは、ダウングレード回数に制限がなく、いつでも構成をダウングレードすることができます。

インスタンスファミリー間での構成変更：データ移行を必要とせずに、インスタンスファミリー間で構成を変更できます。

構成を変更する場合、変更が可能なインスタンスタイプは、現在のアベイラビリティーゾーンがターゲット仕様を提供するかどうかに関連しています。次の考慮点と制限に注意してください：

スポットインスタンスは、クロスモデルの構成変更をサポートしていません。

専用インスタンスは、クロスモデルの構成変更をサポートしていません。構成変更の範囲は、インスタンスが配置されている専用ホストの残りのリソースの影響を受けます。

GPU や FPGA などの異種インスタンスは、インスタンスファミリー間で構成を変更するためのソースまたはターゲットインスタンスタイプとして使用できません。

**クラシックネットワークを構成するインスタンス**はVirtual Private Cloudのみをサポートするインスタンスへの変更をサポートしません。

ターゲットインスタンスタイプが、現在のインスタンスタイプ用に構成されているCBSタイプをサポートしていない場合、構成を変更できません。

ターゲットインスタンスタイプが、現在のインスタンスタイプ用に構成されているイメージタイプをサポートしていない場合、構成を変更できません。

ターゲットインスタンスタイプが、現在のインスタンスタイプ用に構成されているENIまたはENI数量をサポートしていない場合、構成を変更できません。詳細については、[Usage Limits](#) をご参照ください。

ターゲットインスタンスタイプが、現在のインスタンスタイプ用に構成されているパブリックネットワーク帯域幅の上限をサポートしていない場合、構成を変更できません。詳細については、[パブリックネットワーク帯域幅の上限](#) をご参照ください。

## 影響

一部のインスタンスのプライベートIP アドレスは、構成変更後に変更される場合があります。プライベートIP アドレスが変更されると、関連する情報が調整ページに表示されます。そのような情報が表示されない場合、プライベートIPアドレスは変更されていません。

## 操作手順

### 説明：

業務に変更が生じた場合は、インスタンス構成を変更できます。

構成をアップグレードする場合は、構成のアップグレードに伴い発生する可能性のある料金をお支払いください。

構成をダウングレードする場合は、払い戻しの詳細を確認してください。CVMインスタンスを強制的にシャットダウンして再起動すると、新しい構成はすぐに有効になります。

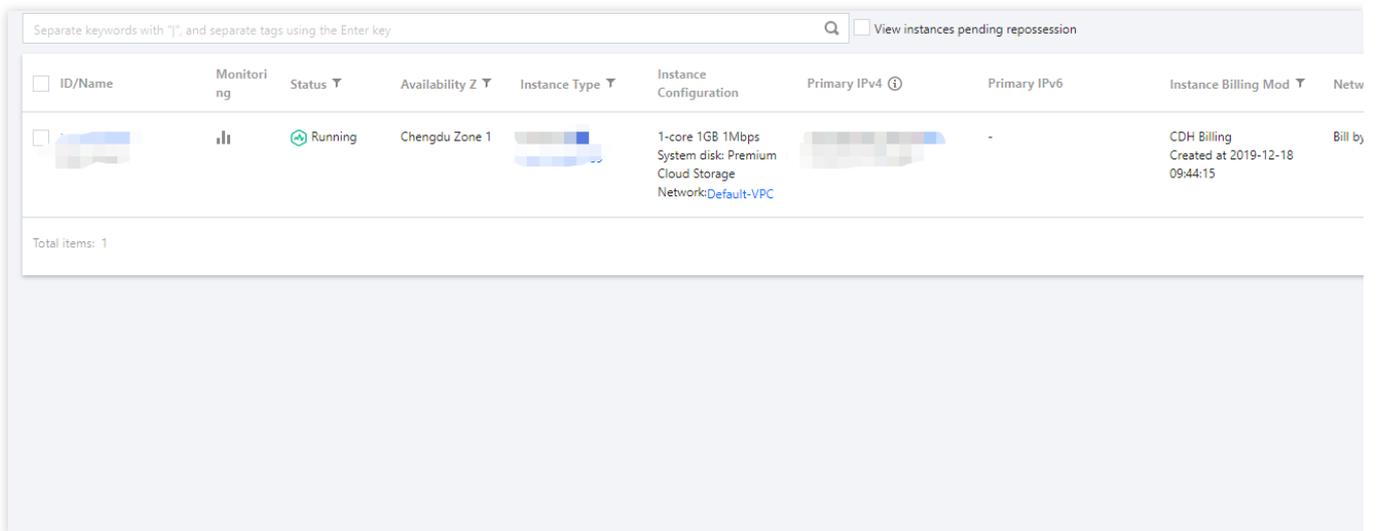
コンソールから

APIから

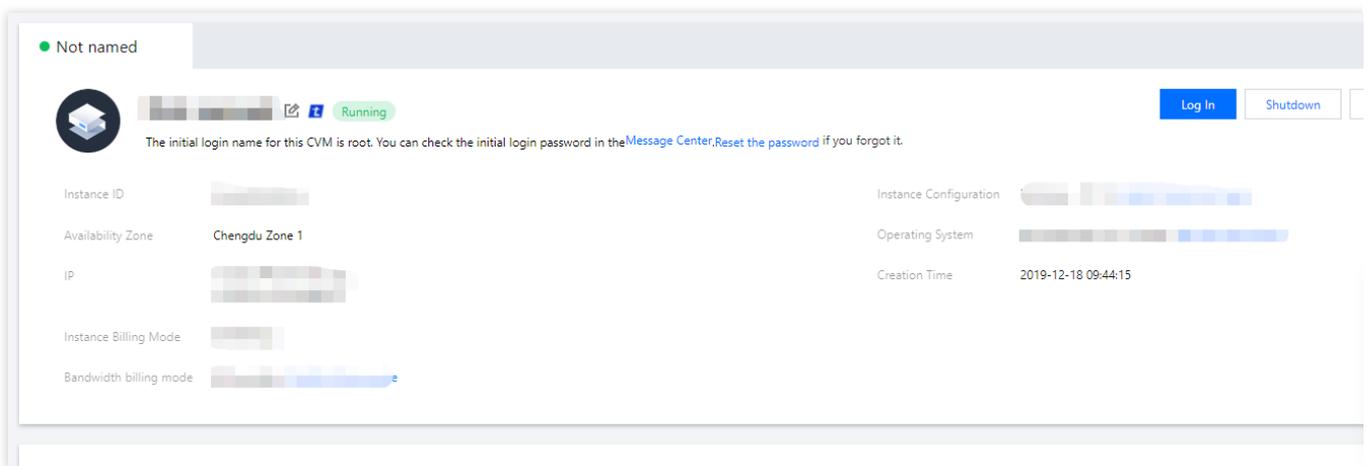
### 単一インスタンスの構成の変更

1. [CVMコンソール](#)にログインし、[CVMページ](#)に移動します。
2. 実際に使用するビューモードに従って操作します。

リストビュー：リストビュー：下図のように、ターゲットインスタンスを選択し、画面右のメニューからさらに>  
[リソース調整](#)>[構成の変更](#)をクリックします。



下図のように、下図のように、ターゲットインスタンスのページで、画面の右上隅にある[その他の操作](#)>[リソース調整](#)>[構成の変更](#)を選択します。



3. 下図のように、「ターゲット構成の選択」ページで、インスタンスのステータスと動作を確認し、[必要なモデル](#)と[インスタンス仕様](#)を選択し、[仕様とパフォーマンスパラメータ](#)を確認して、[次へ](#)をクリックします。



**Adjust Configuration**

✔ Select target configuration > ✔ Billing Details > 3 Shutdown CVM

ⓘ You need to shutdown the instance for the current operation:

- To avoid data loss, we will shut down the instance before adjusting the configuration. Your business will be interrupted during shut down so please take necessary precautions.
- Forced shutdown may result in data loss or file system corruption. We recommend manually shutting down CVM manually before the operation.
- Forced shutdown may take a while. Please be patient.

Forced shutdown \*  Agree to a forced shutdown

Previous step Adjust Now

現在のインスタンスがシャットダウンされている場合、次のプロンプトが表示されます。

**Adjust Configuration**

✔ Select target configuration > ✔ Billing Details > 3 Shutdown CVM

ⓘ You need to shutdown the instance for the current operation, and all selected instances are shut down.

Previous step Adjust Now

5. **変更を開始**をクリックして注文ページに移動し、支払いを完了します。

ResetInstancesType r インターフェースを使用してインスタンスで構成できます。詳細については、[インスタンス構成の調整 API ドキュメント](#)をご参照ください。

# ネットワーク構成の変更

最終更新日：：2023-04-13 15:18:40

## 概要

Tencent Cloudは必要に応じて、パブリックネットワーク課金モデルまたはパブリックネットワーク帯域幅の変更をサポートし、変更はすぐに有効になります。制限と価格の詳細については、[パブリックネットワーク課金方式の変更](#)をご参照ください。

## 操作手順

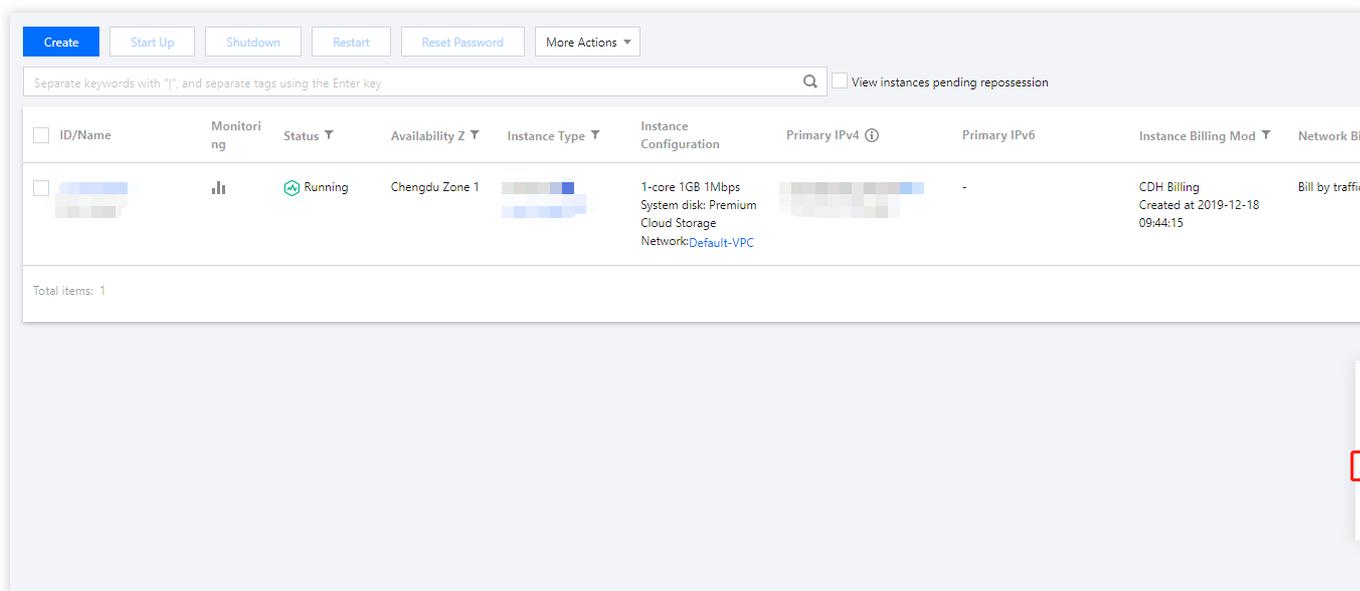
1. [CVMコンソール](#)にログインし、「インスタンス」ページの上部で、帯域幅を変更するCVMインスタンスが存在するリージョンを選択します。

2. インスタンスの管理画面で、実際に使用されているビューモードに従って操作します。

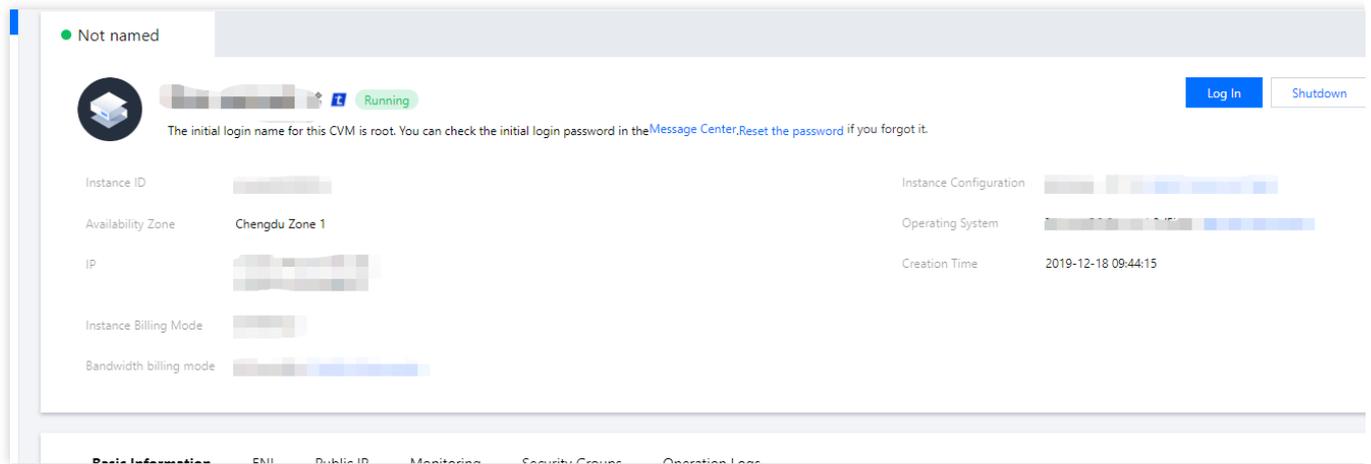
リストビュー

タブビュー

下図のように、対象のCVMインスタンスの行の右側にあるさらに>[リソース調整](#)>[ネットワークを調整](#)を選択します。



下図のように、対象のCVMインスタンスのページの右上隅にある[その他の操作](#)>[リソース調整](#)>[ネットワークを調整](#)を選択します。



3. ポップアップした「ネットワークを調整」ダイアログボックスで、必要に応じてパブリックネットワーク課金モデルまたはパブリックネットワーク帯域幅を調整します。

ネットワーク課金モデル：Tencent Cloudはトラフィック課金と帯域幅課金という2つの異なる課金モデルが用意されています。帯域幅課金モデルは、**利用した時間単位で課金される**仕組みです。

ターゲット帯域幅制限：Tencent Cloudは、**専用型パブリックネットワーク**と**共有型パブリックネットワーク**（帯域幅パッケージによって課金され、現在ベータテストの段階）という2つのネットワーク構成を提供しています。このドキュメントでは、専用型パブリックネットワークの構成へ変更、つまり単一CVMインスタンスの帯域幅上限の変更を例に取り上げます。

#### 説明：

帯域幅上限の詳細については、[パブリックネットワーク帯域幅上限](#) をご参照ください。

4. ターゲット課金モデルを選択するか、ターゲット帯域幅の値を設定して、**OK**をクリックします。

## 関連ドキュメント

[パブリックネットワーク課金方式の変更](#)

[パブリックネットワーク課金方式](#)

[Product Pricing](#)

[パブリックネットワーク帯域幅の上限](#)

# プロジェクト設定の調整

最終更新日：：2023-04-12 14:31:32

## 概要

プロジェクト機能は、プロジェクトごとにクラウドリソースを管理するために使用されます。CVMインスタンスを作成するときは、それをプロジェクトに割り当てる必要があります。Tencent Cloudは、CVMインスタンスの作成後に、ユーザーがインスタンスを新たなプロジェクトに再割り当てすることをサポートしています。

### ご注意：

インスタンスを新たなプロジェクトに割り当てる場合は、まずプロジェクトを新規作成してください。プロジェクトを作成する方法の詳細については、[Project Management](#) をご参照ください。

## 操作手順

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画面で、実際に使用されているビューモードに従って操作します。

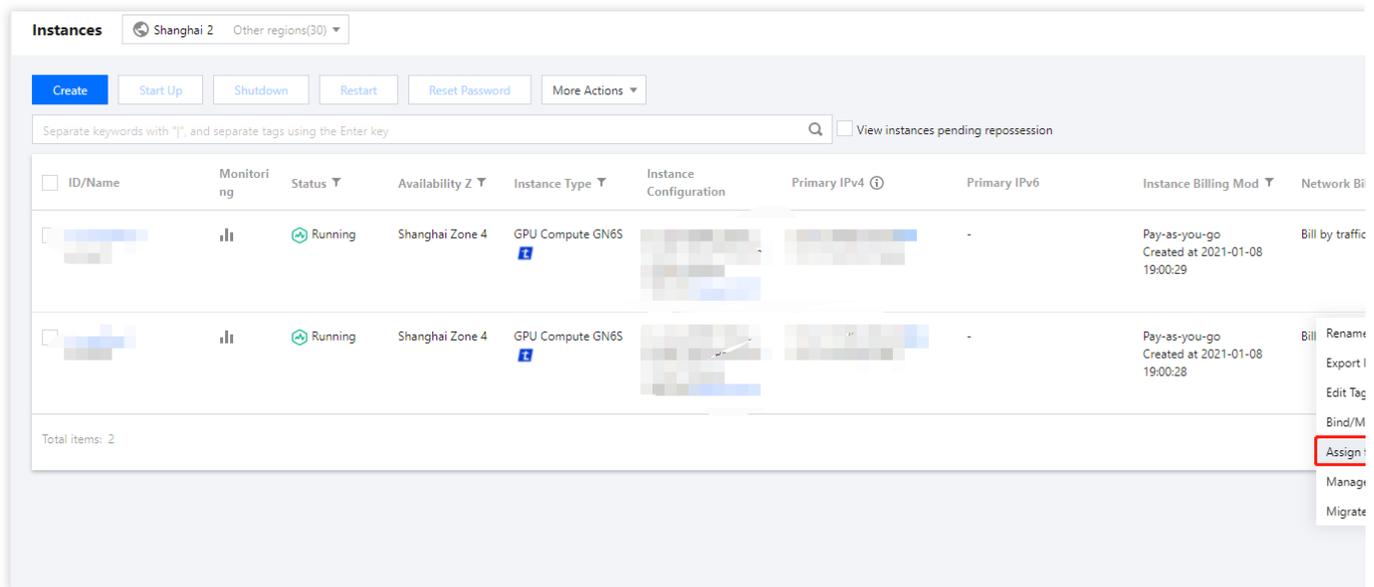
リストビュー

タブビュー

インスタンスリストで新たなプロジェクトに再割り当てする必要があるCVMインスタンスを選択し、右側の**その他** > **インスタンス設定** > **プロジェクトに割り当てる** をクリックします。

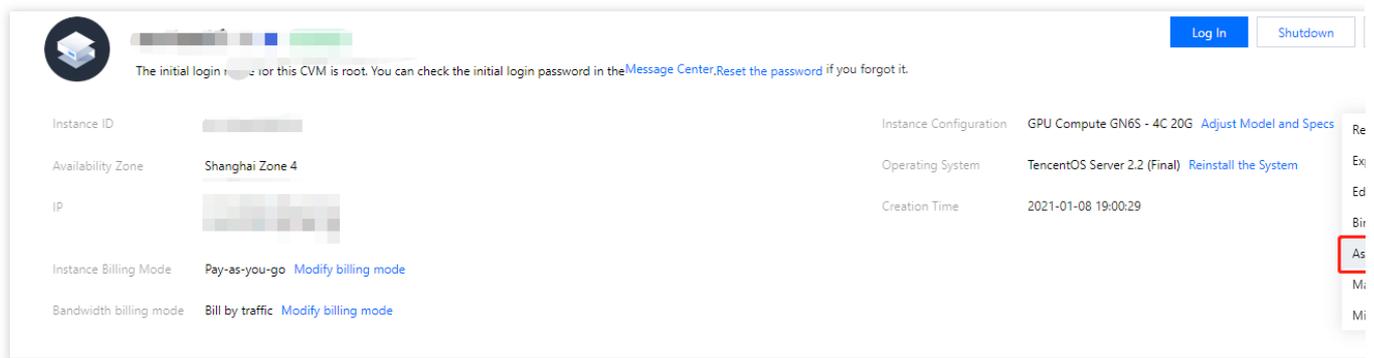
### 説明：

複数のCVMインスタンスを新たなプロジェクトに再割り当てする必要がある場合は、それらを選択し、画面上部にある**その他の操作** > **インスタンス設定** > **プロジェクトに割り当てる** をクリックします。



The screenshot shows the 'Instances' page in the Tencent Cloud console. At the top, there are buttons for 'Create', 'Start Up', 'Shutdown', 'Restart', 'Reset Password', and 'More Actions'. Below these is a search bar and a checkbox for 'View instances pending repossession'. The main area contains a table with columns: ID/Name, Monitoring, Status, Availability Z, Instance Type, Instance Configuration, Primary IPv4, Primary IPv6, Instance Billing Mod, and Network Bi. Two instances are listed, both in 'Running' status. A context menu is open for the second instance, with the 'Assign Instance to Project' option highlighted in red.

下図に示すように、新たなプロジェクトに再割り当てする必要があるCVMページで、ページ右上コーナーの**その他操作** > **インスタンスの設定** > **プロジェクトへの割り当て**を選択します。



The screenshot shows the configuration page for a CVM instance. At the top right, there are 'Log In' and 'Shutdown' buttons. Below the instance ID, there is a note about the initial login password. The page is divided into two columns of configuration details. The left column includes Instance ID, Availability Zone (Shanghai Zone 4), IP, Instance Billing Mode (Pay-as-you-go), and Bandwidth billing mode (Bill by traffic). The right column includes Instance Configuration (GPU Compute GN6S - 4C 20G), Operating System (TencentOS Server 2.2 (Final)), and Creation Time (2021-01-08 19:00:29). A context menu is open on the right side, with the 'Assign Instance to Project' option highlighted in red.

3. ポップアップした「プロジェクトに割り当てる」ウィンドウで、新たなプロジェクト名を選択し、**OK**クリックすると、プロジェクトへの割り当て操作が完了します。

### Assign to Project ✕

You've selected 1 instance. [Collapse](#)

ID/Name	Instance Type	Instance Configuration
	GPU Compute GN6S	4-core 20GB 1Mbps System disk: Premium Cloud Storage Network:vpc-mzg9lleo

Search by project name/description 🔍

Project Name	Description

# インスタンス構成変更の提案

最終更新日：：2023-04-13 10:54:38

## 概要

Tencent Cloudは、直近3日間のCVMインスタンスの負荷状況に基づき、それに対応するインスタンスの設定を調整するための提案を行います。この提案は Cloud Monitorによって収集されたCPU、メモリなどの監視データを基に分析を行って得られたものであり、実際の状況を踏まえて、インスタンス構成を変更するかどうかを決定できます。

## 説明事項

インスタンスの設定を調整するための提案はインスタンスの直近3日間の平均負荷データ（5分ごとにデータを統計）を基に得られたものであり、CPU使用率とメモリ使用率が瞬間的に急激に上昇しているインスタンスではなく、一定時間内のワークロードが安定しているインスタンスに適用されます。

本機能はGPU、FPGAなどの異種モデルおよびCloud Physical Machineには適用されません。アラート作成を介してインスタンスの使用状況を能動的に監視できます。

この提案は参考に過ぎず、インスタンスの使用状況を監視するために高い要件が設定される場合は、Cloud Monitorを使用して能動的に監視することをお勧めします。

## 操作手順

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に移動します。
2. インスタンスリストページで、インスタンスのモニタリングバーに



警告アイコンが表示されている場合は、対応するインスタンスに構成を変更するための提案があります。

3.



警告アイコンをクリックすると、「構成変更に関するアドバイス」ウィンドウがポップアップします。

4. 「構成変更に関するアドバイス」ウィンドウに、このインスタンスの使用状況に基づき推奨されるターゲットモデルが表示されます。「その他推奨モデルを表示する」にチェックを入れれば、その他推奨モデルを表示できます。

5. 提案に従ってインスタンスの構成を変更する必要がある場合は、「インスタンス構成変更費用についての説明を読んで同意しました」にチェックを入れ、変更を開始をクリックします。

# 情報の確認

## インスタンス情報の確認

最終更新日：：2023-06-28 11:30:24

### 概要

ユーザーがCVMインスタンス情報を確認しやすいように、Tencent Cloudは下記の3種類の確認方法を提供しています。

コンソールの [概要](#) ページでアカウントにおけるCVMインスタンス総数及びそれらの稼動状態、各リージョンのリソース数、クォータ等の情報を確認します。

コンソール [CVM](#) ページで、特定リージョン内のすべてのCVMインスタンスに関する情報を確認します。インスタンス詳細ページであるCVMインスタンスの詳細情報を確認します。

### 前提条件

[CVMコンソール](#)にログインします。

### 操作手順

#### インスタンス概要情報の確認

左側ナビゲーションバーで、[概要](#) を選択し、CVM概要ページに移動します。

当該ページでは、確認可能な情報、及び実行可能な操作は下記を含んでいます。

CVM状態（即ちCVMの総数）、7日以内に期限切れになるインスタンス数、ごみ箱のインスタンス数、正常なサーバー数。

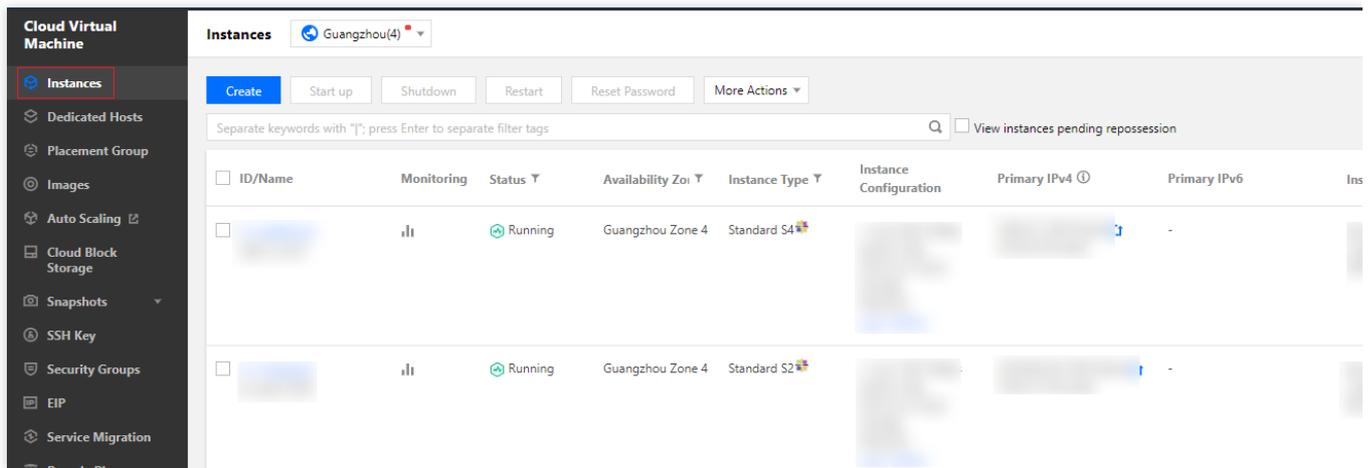
更新待ちCVMリスト、当該ページでCVMを更新できます。

リソース数とクォータ。各リージョンの従量課金CVM、カスタムイメージ及びスナップショットクォータ情報を確認できます。また、当該ページでクォータを申請できます。

クロスリージョンでクラウドリソースをサーチします。

#### CVMリスト情報の確認

下図のように、左側ナビゲーションバーで、[インスタンス](#) を選択し、インスタンスリストページに移動します。



このページでは、ID/インスタンス名、監視、ステータス、アベイラビリティゾーン、インスタンスタイプ、設定、メインIPv4アドレス、メインIPv6アドレス、インスタンス課金モデル、ネットワーク課金モデルおよび所属プロジェクトなどを含む情報操作を確認できます。

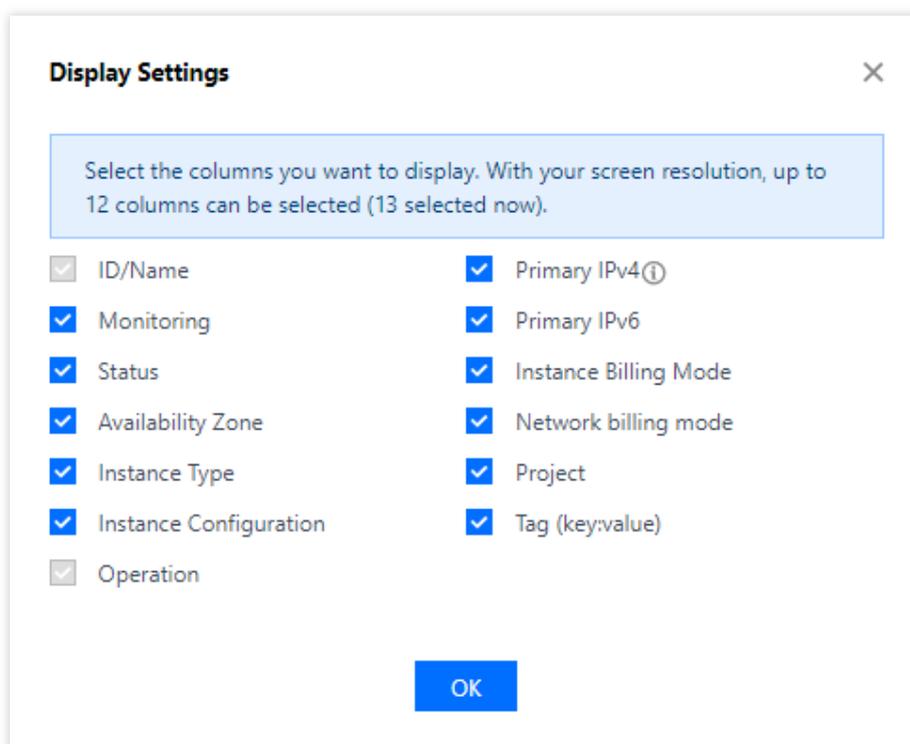
#### 説明：

実際のニーズに応じて使用できます [コンソールインスタンスのページビューへの切替](#)。

下図のように、右上コーナーの



をクリックし、ポップアップした「カスタムリストフィールド」ウィンドウで表示したいリストの詳細情報を選択します。



## インスタンス詳細情報の確認

1. **インスタンス** の管理ページ上部で、リージョンを選択します。
2. 詳細を確認しようとするインスタンスを見つけ、ID/インスタンス名をクリックし、インスタンス詳細ページに入ります。下図の通りです。

インスタンス詳細ページで、インスタンス情報、アーキテクチャ図、ネットワーク情報、設定情報、イメージ情報、課金情報、Elastic Network Interface (ENI)、監視、セキュリティグループ、操作ログなどを確認できます。

The initial login name for this CVM is root. You can check the initial login password in the [Message Center](#), [Reset the password](#) if you forgot it.

Instance ID	[REDACTED]	Instance Configuration
Availability Zone	Chengdu Zone 1	Operating System
IP	[REDACTED]	Creation Time
Instance Billing Mode	CDH Billing	
Bandwidth billing mode	Bill by traffic <a href="#">Modify billing mode</a>	

**Basic Information**   ENI   Public IP   Monitoring   Security Groups   Operation Logs

### Instance Information

Name	[REDACTED]	Project	Default Project
Instance ID	[REDACTED]	Tags	None <a href="#">✎</a>
UUID	[REDACTED]	Key	None
Instance Specification	[REDACTED]	Placement Group	None
Region	Chengdu	Role	None <a href="#">✎</a>
Availability Zone	Chengdu Zone 1		

### Network Information

# インスタンスメタデータのクエリ

最終更新日：：2023-07-19 10:51:48

インスタンスメタデータは、インスタンスに関連するデータを指します。実行中のインスタンスを構成または管理するために使用できます。

## 説明：

インスタンスのメタデータにはログイン後にのみアクセスできますが、データは暗号化されていません。インスタンスにアクセスできる人員はいずれもそのメタデータを表示できます。そのため、機密データを保護するために適切な予防措置を講じる必要があります。

## インスタンスメタデータの分類

Tencent Cloudは現在、次のメタデータを提供しています。

データ	説明	バージョン
instance-id	インスタンスID	1.0
instance-name	インスタンス名	1.0
uuid	インスタンスID	1.0
local-ipv4	インスタンスのプライベートIP アドレス	1.0
public-ipv4	インスタンスのパブリックIPアドレス	1.0
mac	インスタンスのeth0デバイスの MAC アドレス	1.0
placement/region	インスタンスのリージョン	2017年9月19日更新
placement/zone	インスタンスのアベイラビリティーゾーン	2017年9月19日更新
network/interfaces/macs/\${mac}/mac	インスタンスネットワークインターフェースのデバイ	1.0

	スアドレス	
network/interfaces/macs/\${mac}/primary-local-ipv4	インスタンスネットワークインターフェースのプライマリプライベートIPアドレス	1.0
network/interfaces/macs/\${mac}/public-ipv4s	インスタンスネットワークインターフェースのパブリックIPアドレス	1.0
network/interfaces/macs/\${mac}/vpc-id	インスタンスネットワークインターフェースのVPC ID	2017年9月19日更新
network/interfaces/macs/\${mac}/subnet-id	インスタンスネットワークインターフェースのサブネットID	2017年9月19日更新
network/interfaces/macs/\${mac}/local-ipv4s/\${local-ipv4}/gateway	インスタンスネットワークインターフェースのゲートウェイアドレス	1.0
network/interfaces/macs/\${mac}/local-ipv4s/\${local-ipv4}/local-ipv4	インスタンスネットワークインターフェースのプライベートIPアドレス	1.0
network/interfaces/macs/\${mac}/local-ipv4s/\${local-ipv4}/public-ipv4	インスタンスネットワークインターフェースのパブリックIPアドレス	1.0
network/interfaces/macs/\${mac}/local-ipv4s/\${local-ipv4}/public-ipv4-mode	インスタンスネットワークインターフェースのパブリックネットワークモード	1.0
network/interfaces/macs/\${mac}/local-ipv4s/\${local-ipv4}/subnet-mask	インスタンスネットワークインターフェースのサブネットマスク	1.0
payment/charge-type	インスタンスの料金プラン	2017年9月19日更新
payment/create-time	インスタンスの作成時間	2017年9月19日更新
payment/termination-time	インスタンスの終了時間	2017

		年9 月19 日更 新
app-id	インスタンスが属するユーザーの AppId	2017 年9 月19 日更 新
as-group-id	インスタンスのAuto ScalingグループID	2017 年9 月19 日更 新
spot/termination-time	スポットインスタンスの終了時間	2017 年9 月19 日更 新
instance/instance-type	インスタンス仕様	2017 年9 月19 日更 新
instance/image-id	インスタンスのイメージ ID	2017 年9 月19 日更 新
instance/security-group	インスタンスに関連付けられているセキュリティグループの情報	2017 年9 月19 日更 新
instance/bandwidth-limit-egress	インスタンスのプライベートネットワークの送信帯域幅制限(Kbit/s)	2019 年9 月29 日更 新

instance/bandwidth-limit-ingress	インスタンスのプライベートネットワークの受信帯域幅制限(Kbit/s)	2019年9月29日更新
cam/security-credentials/\${role-name}	CAMロールポリシーによって生成される一時的な認証情報。インスタンスがCAMロールに関連付けられている場合にのみ取得できます。\${role-name} を実際のCAMロール名に変更する必要があります。それ以外の場合は、`404` が返されます。	2019年12月11日更新
volumes	インスタンスストレージ	1.0

### 説明：

上記テーブルにおける `${mac}` および `${local-ipv4}` フィールドはそれぞれインスタンスに指定されたネットワークインターフェースのMACアドレスとプライベートIPアドレスを表します。

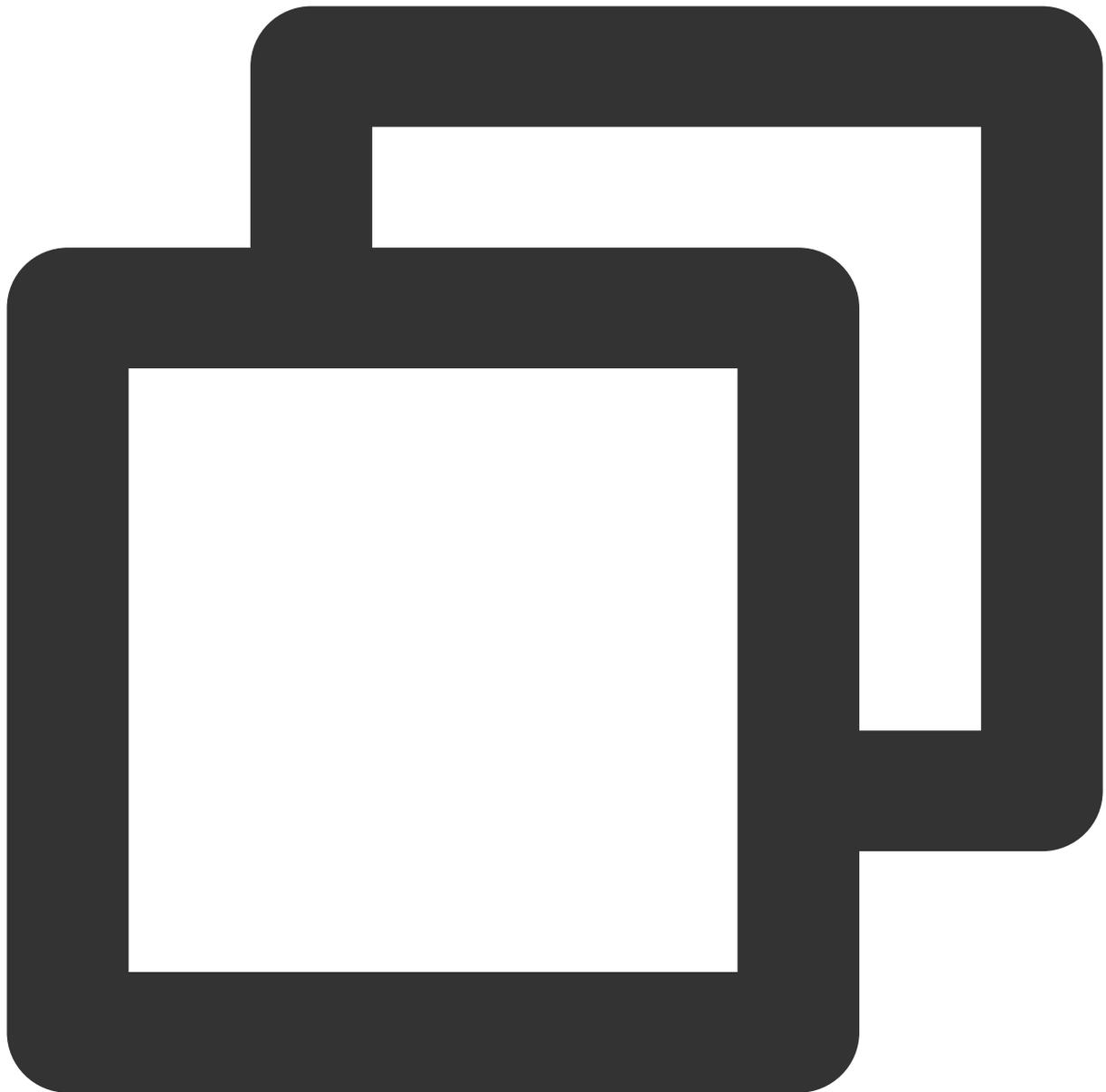
リクエストの宛先URLアドレスは、大文字と小文字を区別する必要があります。返されたリクエストの結果に従って、新しいリクエストの宛先URLアドレスを作成する必要があります。

返された配置データは、新しいバージョンで変更されています。以前のバージョンのデータを使用する必要がある場合、以前のバージョンのパスを指定するか、バージョンのパスを指定しないことによりバージョン1.0のデータにアクセスすることができます。返された配置データの詳細については、[リージョンとアベイラビリティゾーン](#)をご参照ください。

## インスタンスメタデータのクエリ

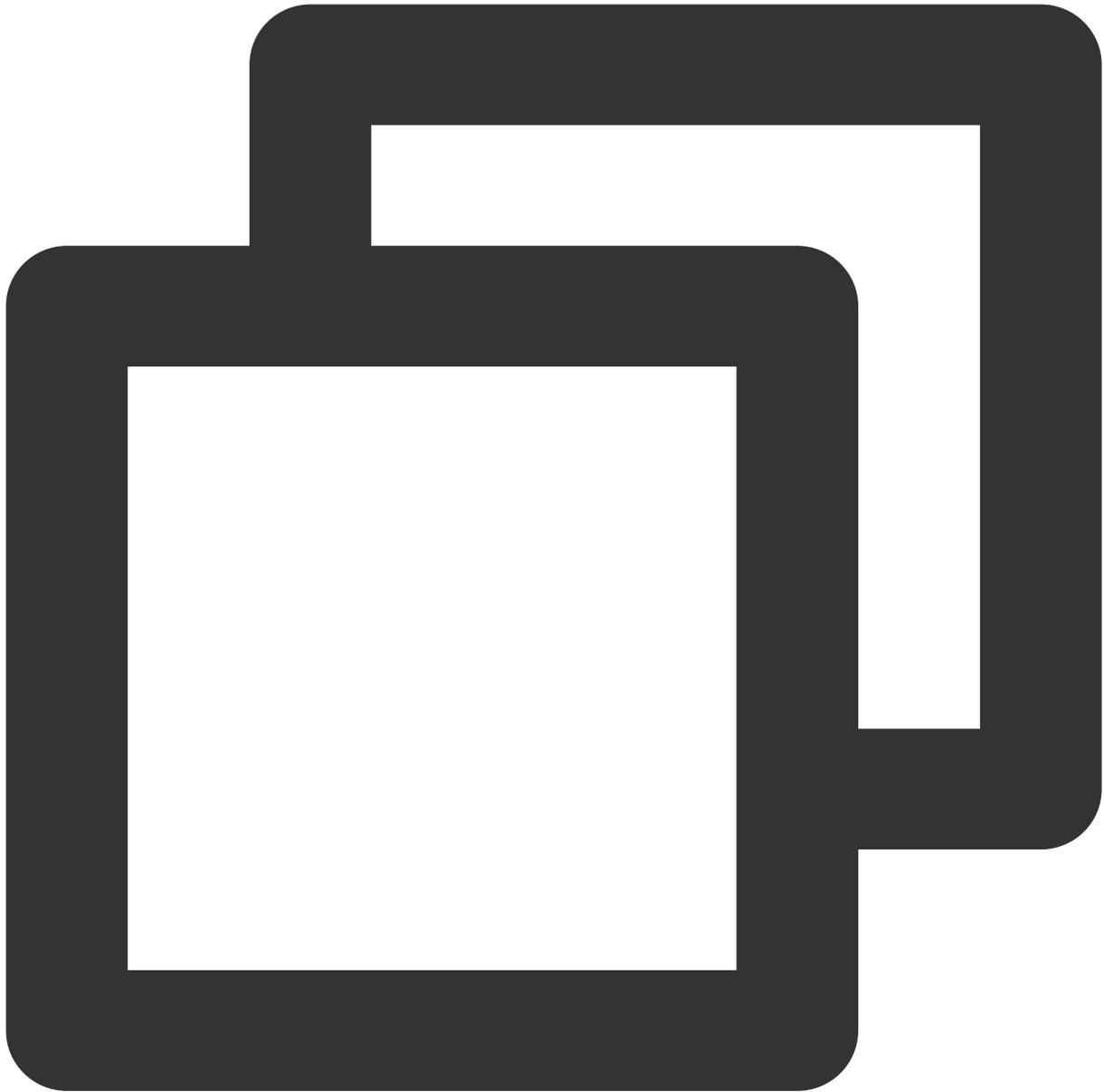
インスタンスにログインすると、インスタンスのローカルIPアドレスやパブリックIPアドレスなどのメタデータにアクセスして、外部アプリケーションとの接続を管理できます。

実行中のインスタンス内部からすべてのカテゴリーのインスタンスメタデータを確認するには、次のURIを使用してください。



```
http://metadata.tencentyun.com/latest/meta-data/
```

cURLツールまたはHTTP GETリクエストを介してメタデータにアクセスできます。例：



```
curl http://metadata.tencentyun.com/latest/meta-data/
```

リソースが存在しない場合、HTTPエラーコード「404 Not Found」が返されます。

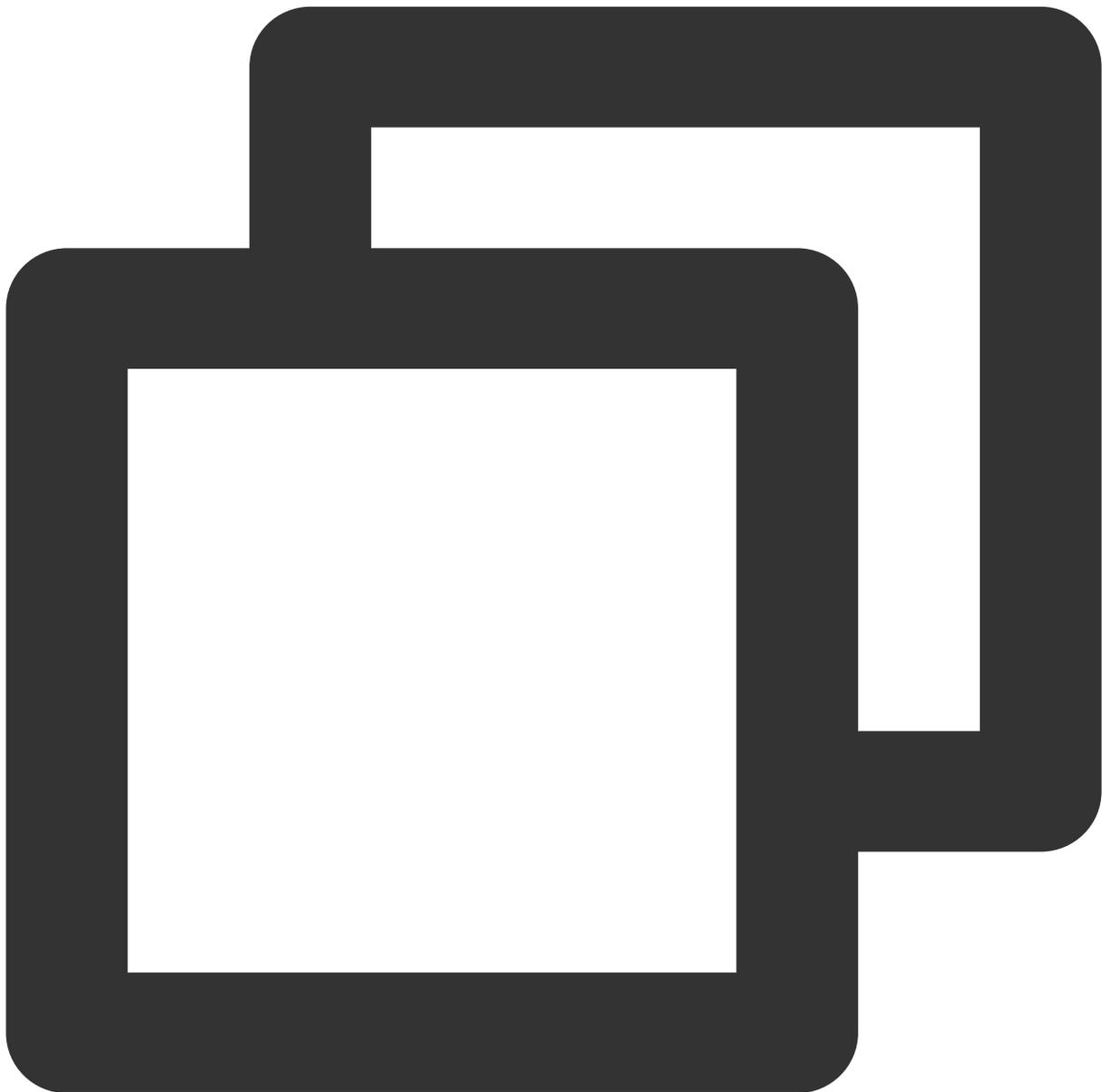
メタデータ関連の操作はすべて、**インスタンスにログインした後**のみ実行できます。まずインスタンスにログインしてください。詳細については、[Windowsインスタンスへのログイン](#) または [Linuxインスタンスへのログイン](#) をご参照ください。

### メタデータクエリ例

以下の例では、メタデータのバージョン情報を取得する方法を説明します。

**ご注意：**

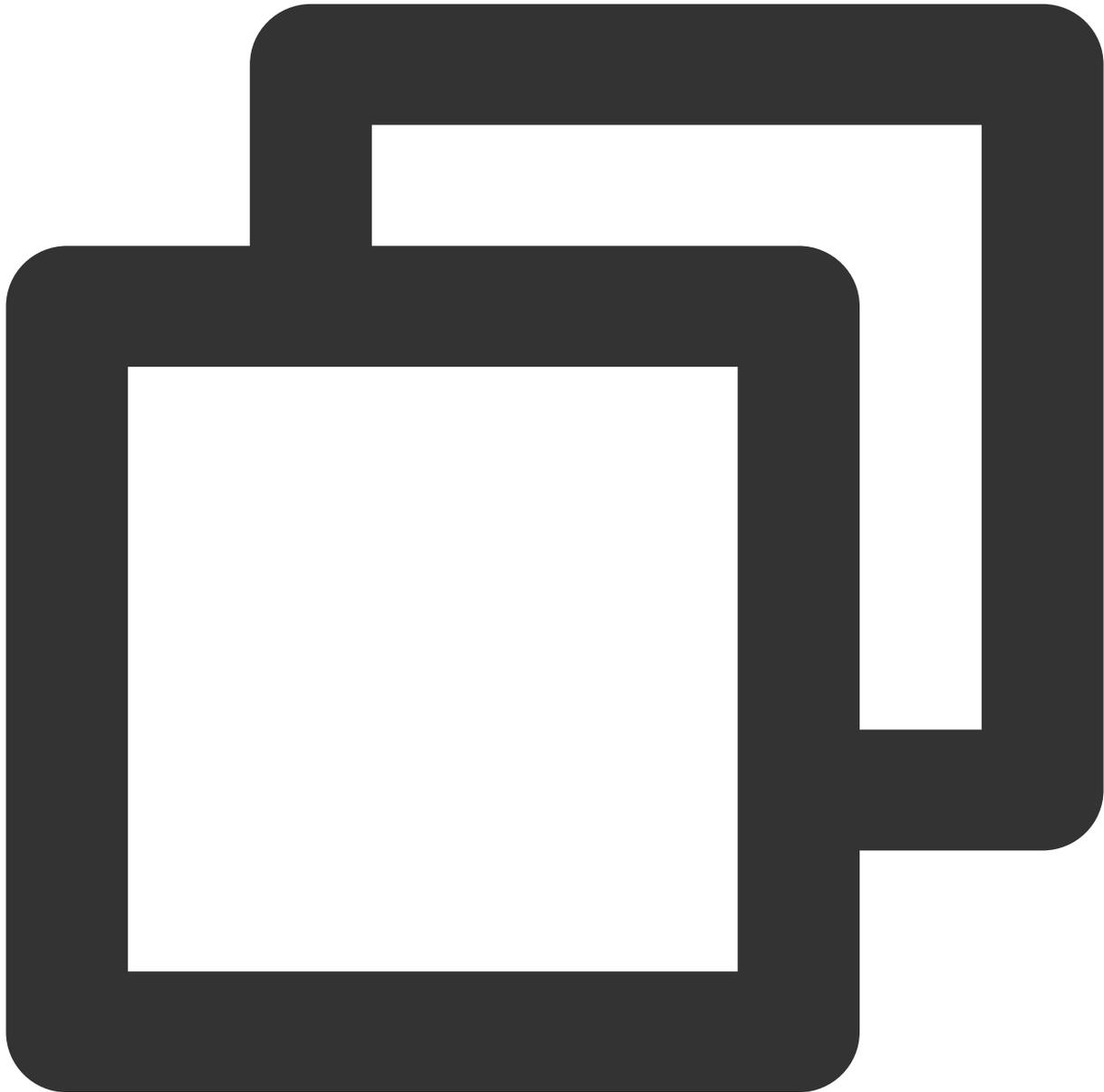
Tencent Cloudがメタデータのアクセスパスまたは返されたデータを変更する時、新しいメタデータのバージョンをリリースします。お客様のアプリケーションプログラムまたはスクリプトが以前のバージョンの構造または返されたデータに依存している場合、指定された初期のバージョンを使用してメタデータにアクセスできます。バージョンを指定しない場合、デフォルトでバージョン1.0がアクセスされます。



```
[qcloud-user]# curl http://metadata.tencentyun.com/  
1.0  
2017-09-19  
latest
```

```
meta-data
```

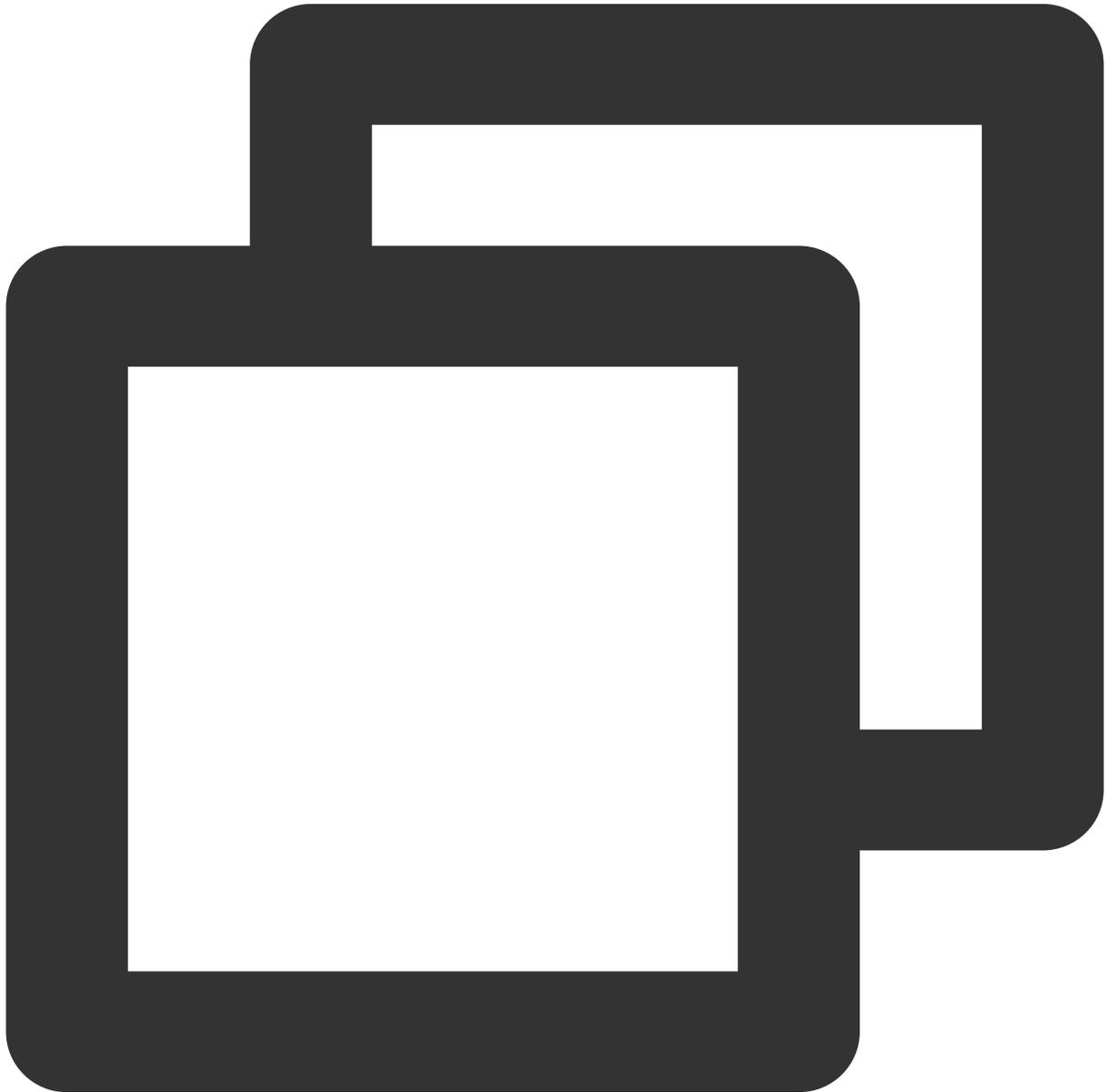
以下の例では、メタデータのバージョン情報を取得する方法を説明します。そのうち「/」で終わる単語はディレクトリを表し、「/」で終わらない単語はアクセスデータを表します。具体的なアクセスデータの意味は、前文のインスタンスメタデータの分類をご参照ください。



```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/  
instance-id  
instance-name  
local-ipv4  
mac
```

```
network/  
placement/  
public-ipv4  
uuid
```

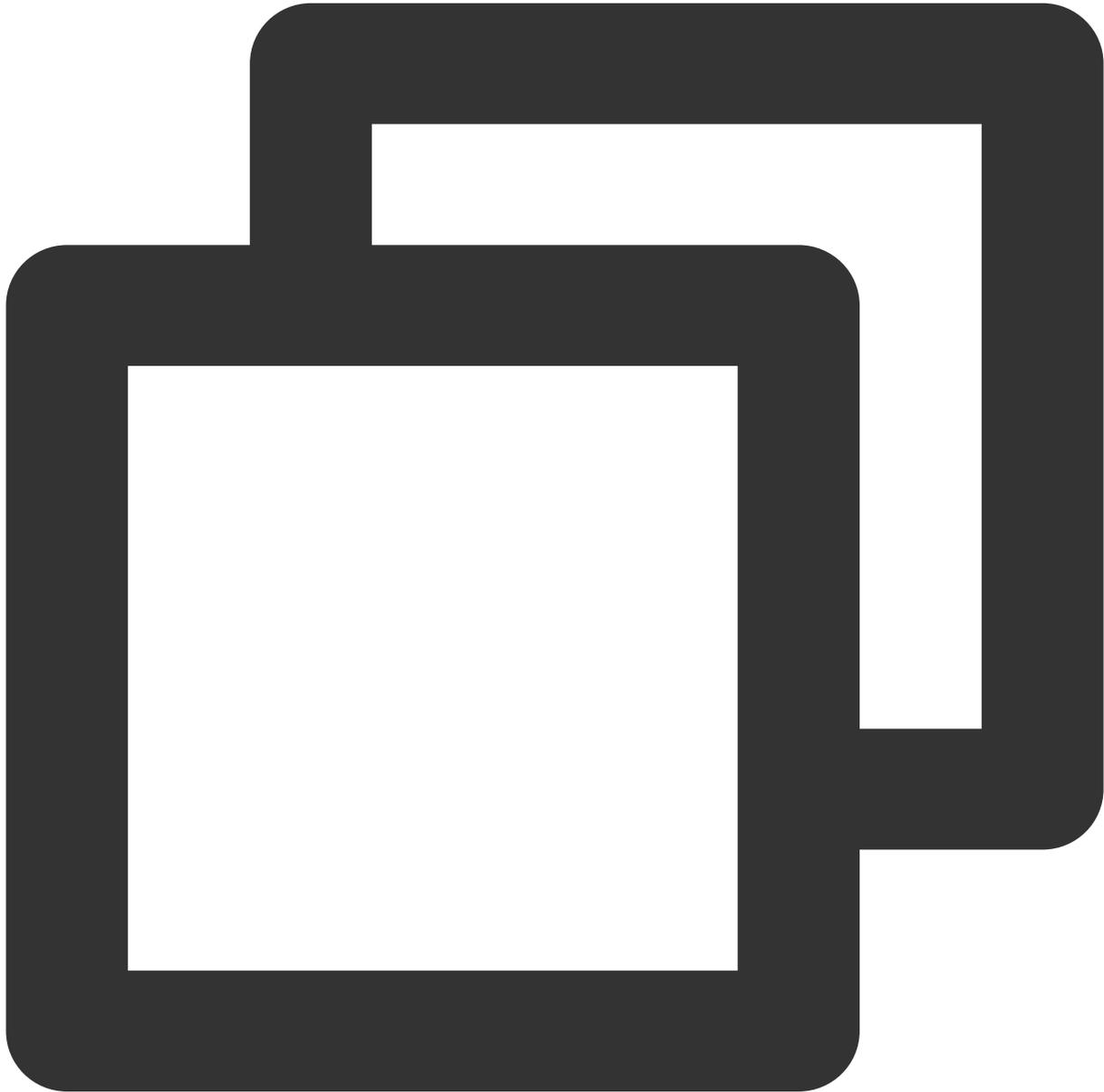
以下の例では、インスタンスの物理的な位置情報を取得する方法を説明します。返されるデータと物理的な位置情報の関係については、[リージョンとアベイラビリティゾーン](#)をご参照ください。



```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/placement/region  
ap-guangzhou
```

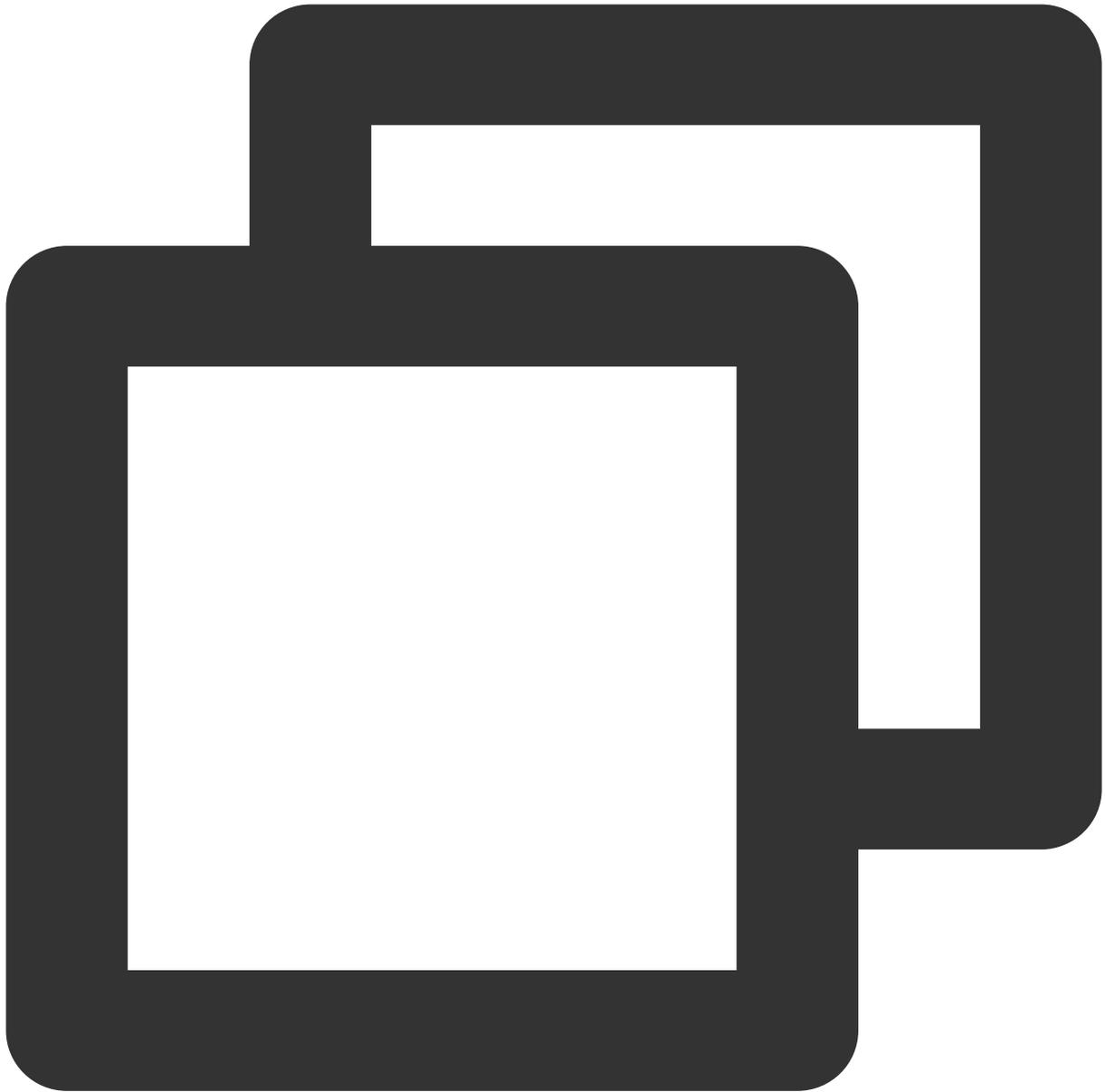
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/placement/zone
ap-guangzhou-3
```

以下の例では、インスタンスのプライベートIPアドレスを取得する方法を説明します。インスタンスに複数のENIがある場合、eth0デバイスのネットワークアドレスが返されます。



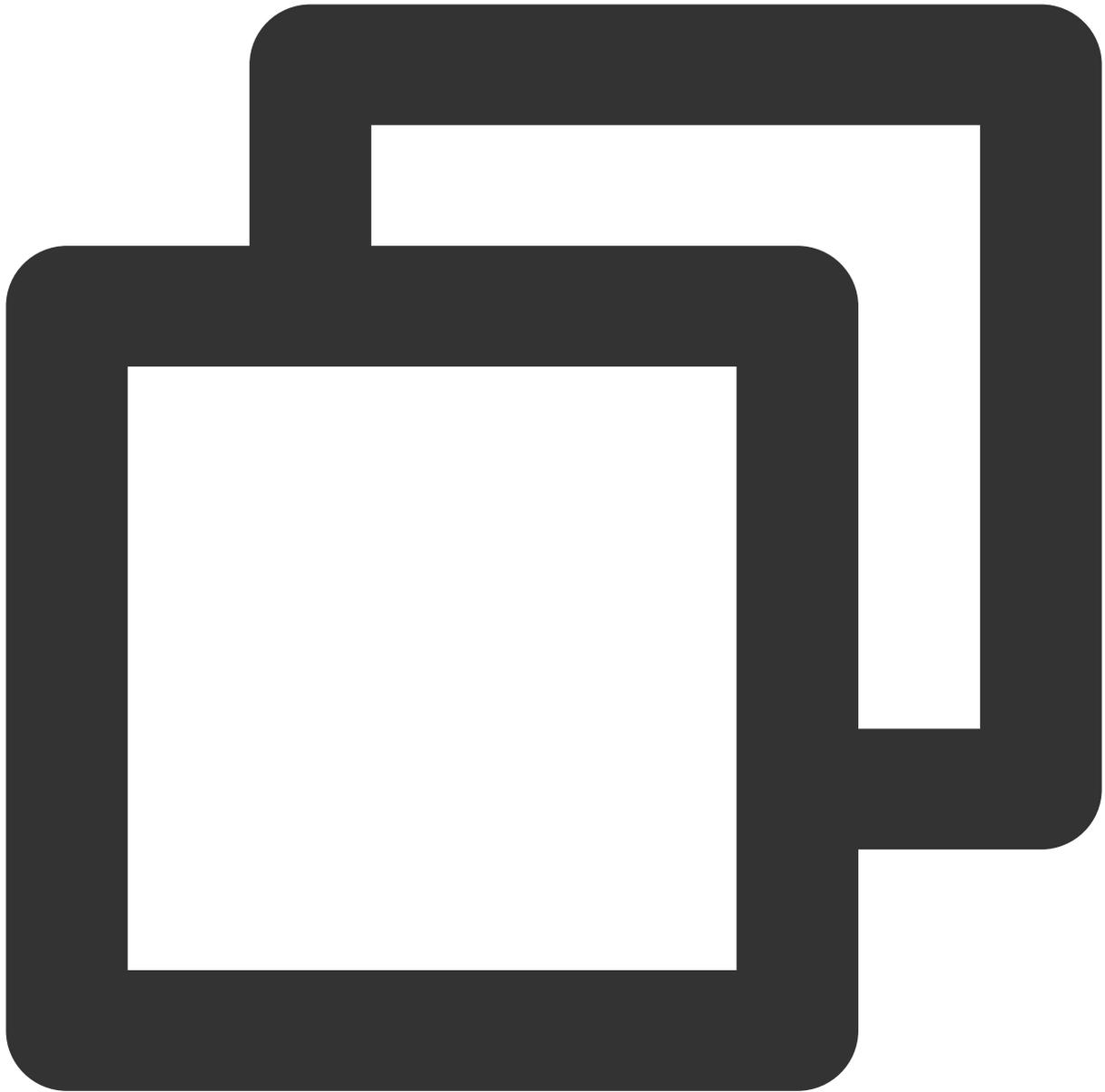
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/local-ipv4
10.104.13.59/
```

以下の例では、インスタンスのパブリックIPアドレスを取得する方法を説明します。



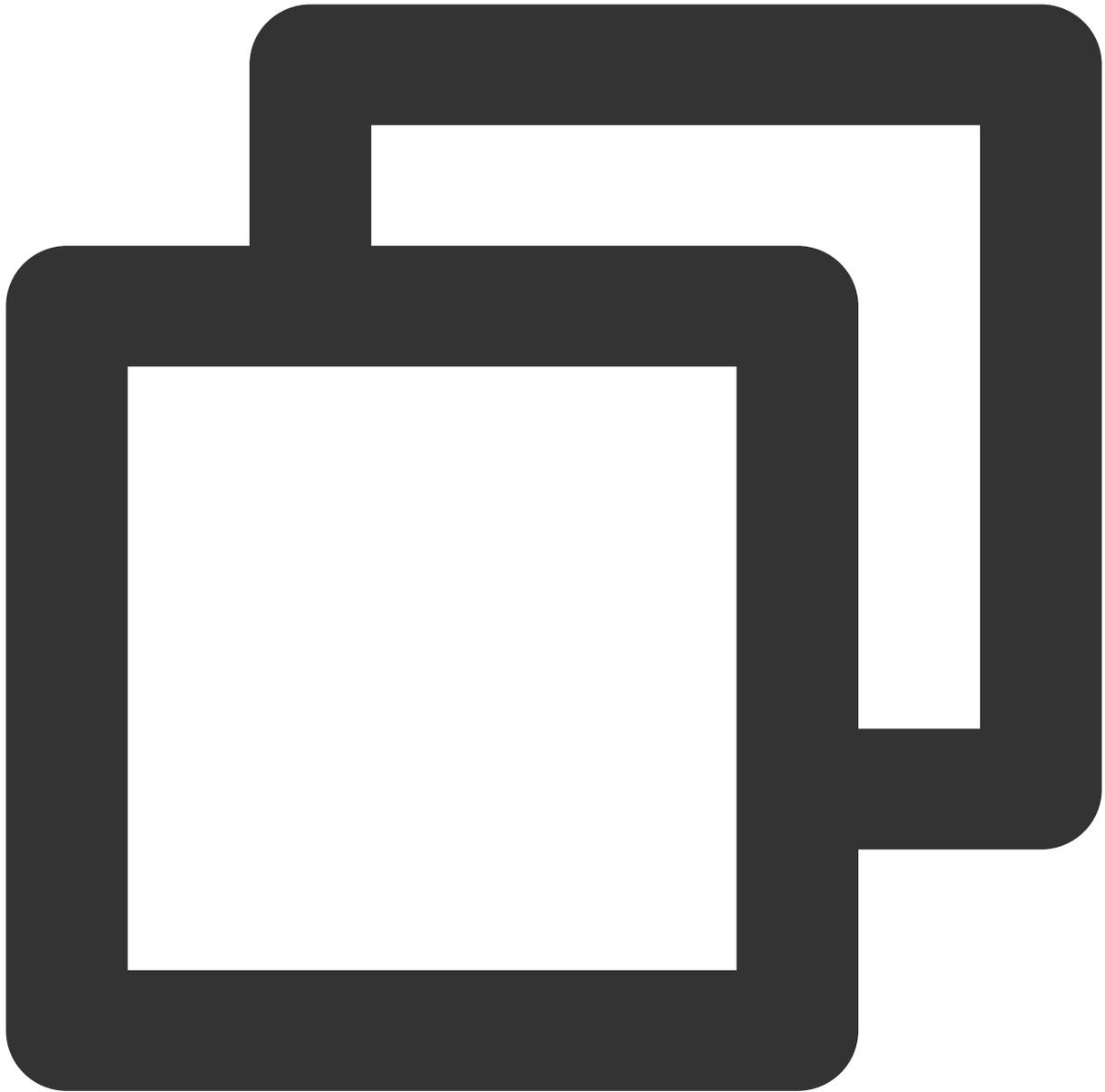
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/public-ipv4  
139.199.11.29
```

以下の例では、インスタンス ID を取得する方法を説明します。インスタンス ID はインスタンスの一意の識別子です。



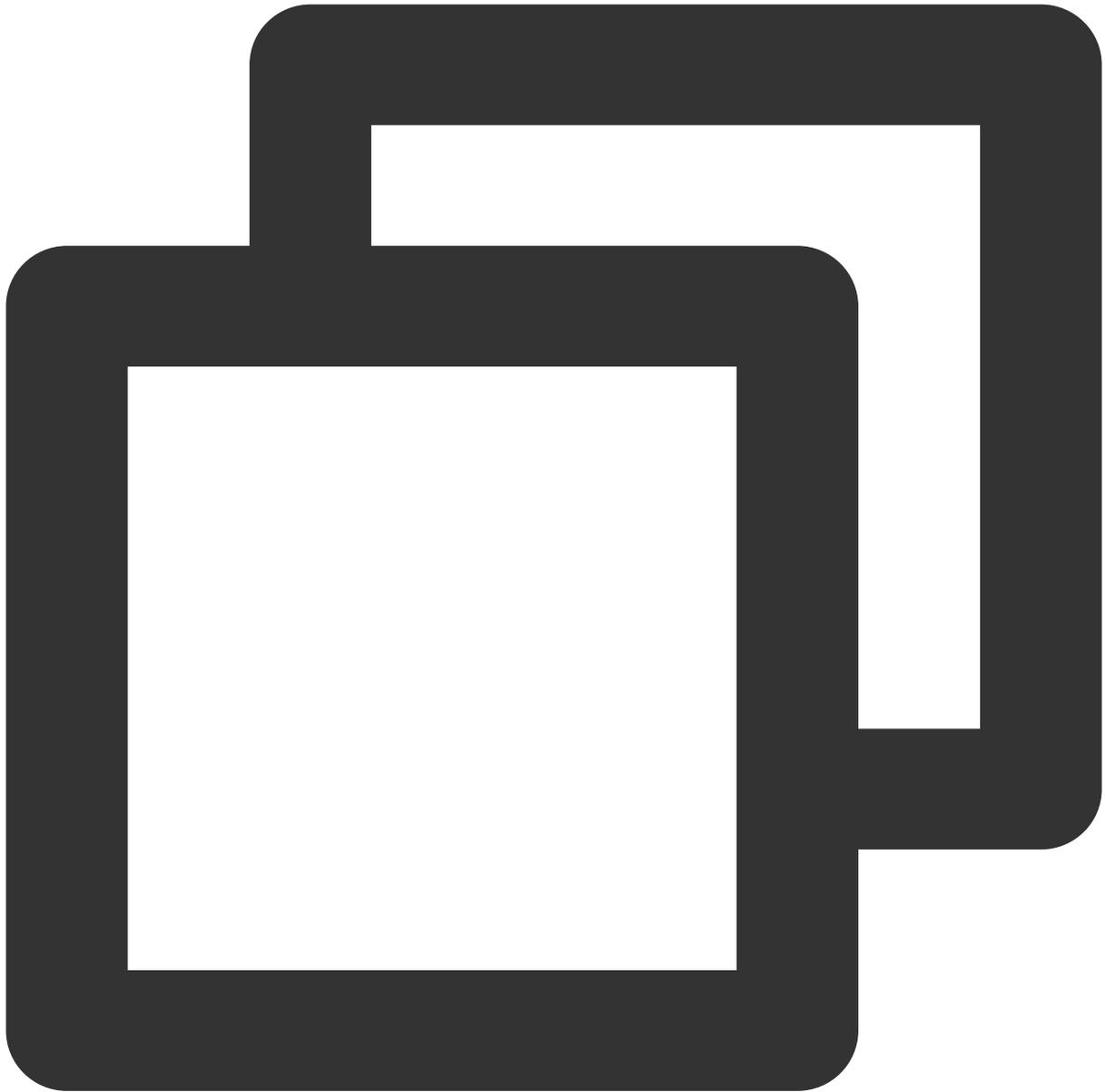
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/instance-id  
ins-3g445roi
```

以下の例では、インスタンスUUIDを取得する方法を説明します。インスタンスUUIDはインスタンスの一意の識別子とすることができますが、インスタンスIDを使用してインスタンスを識別することをお勧めします。



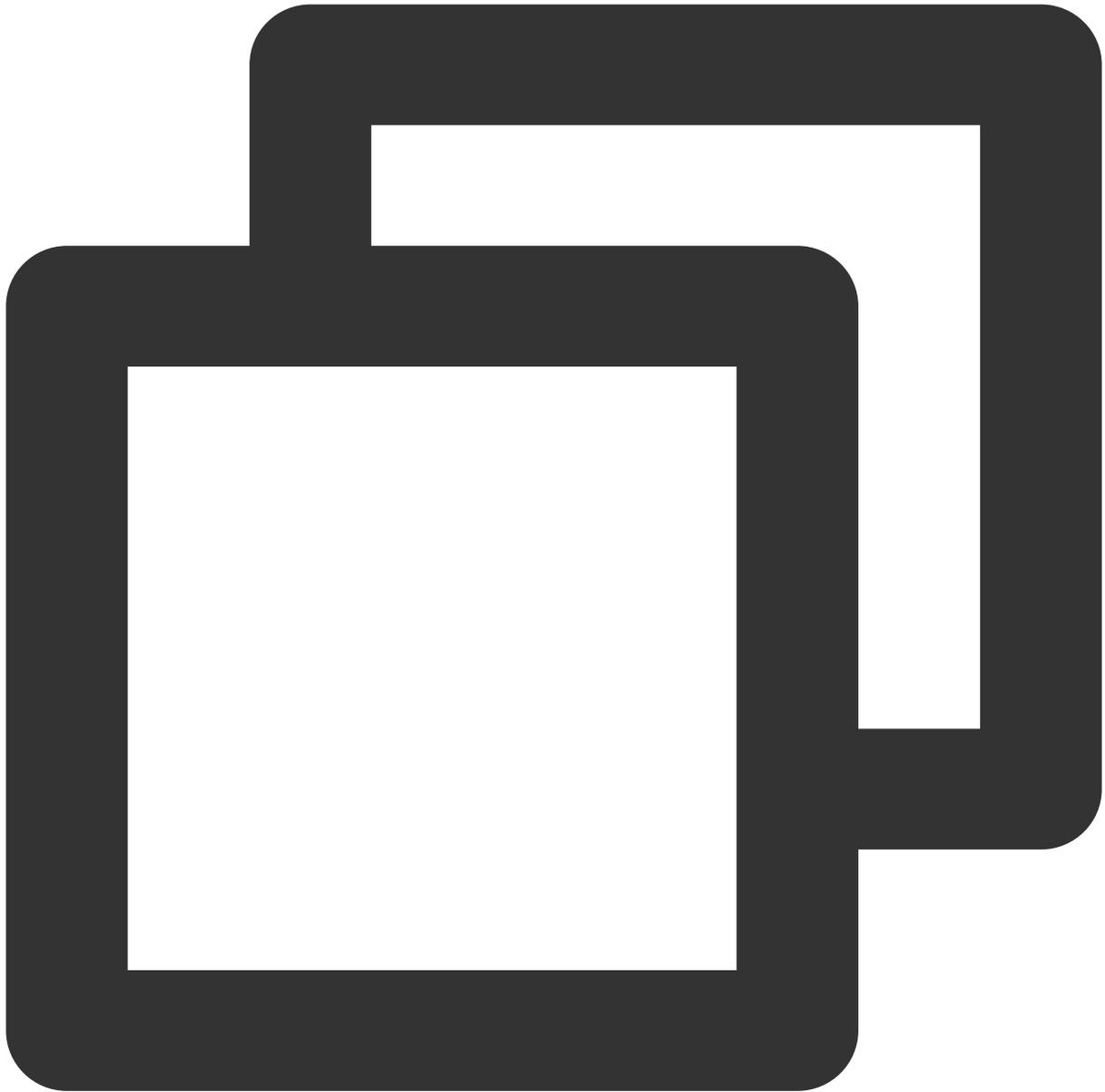
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/uuid  
cfac763a-7094-446b-a8a9-b995e638471a
```

以下の例では、インスタンスのeth0デバイスのMACアドレスを取得する方法を説明します。



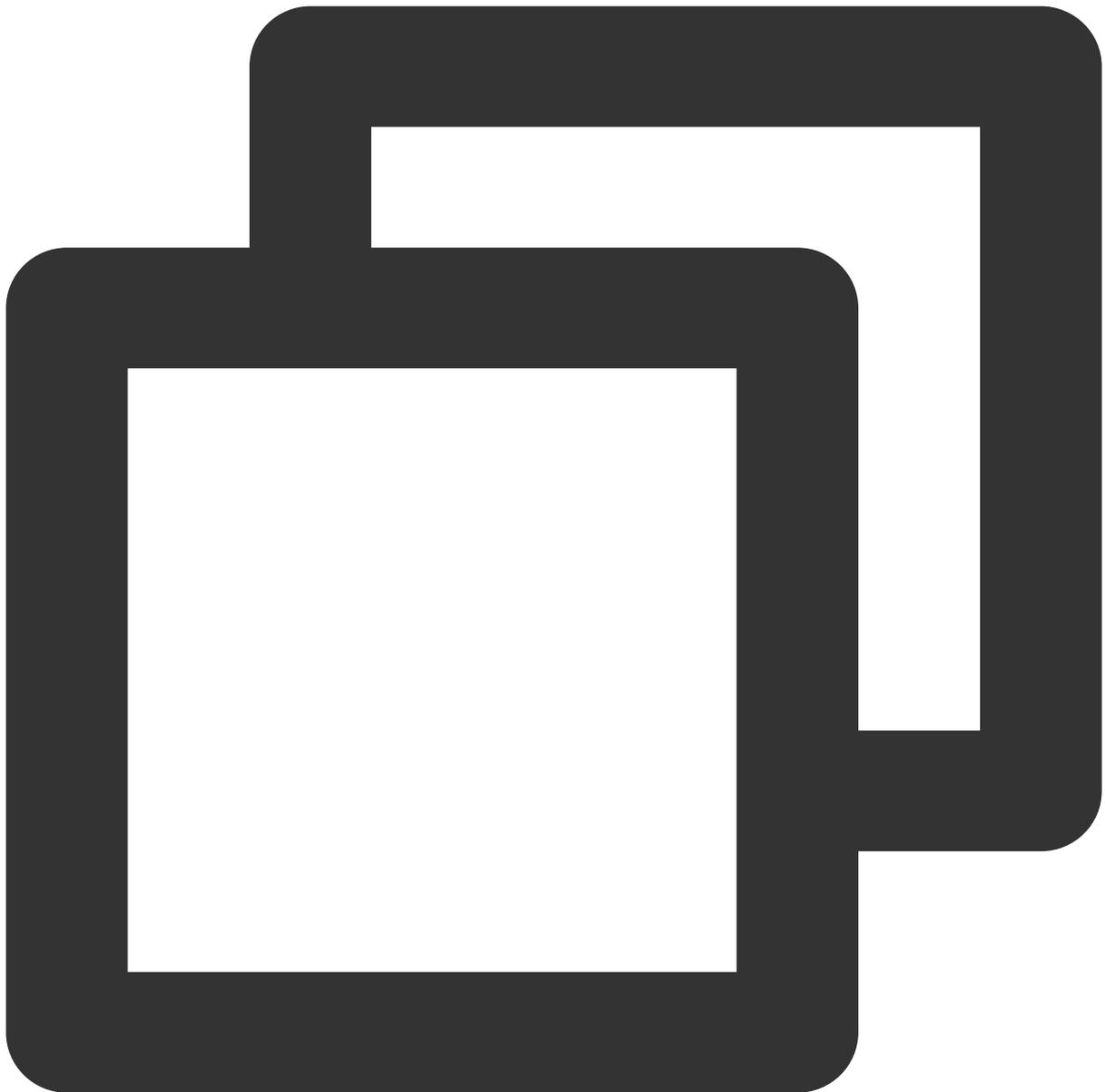
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/mac  
52:54:00:BF:B3:51
```

以下の例では、インスタンスのENI情報を取得する方法を説明します。複数枚のENIは複数行のデータを返し、各行のデータはENI1枚のデータディレクトリです。



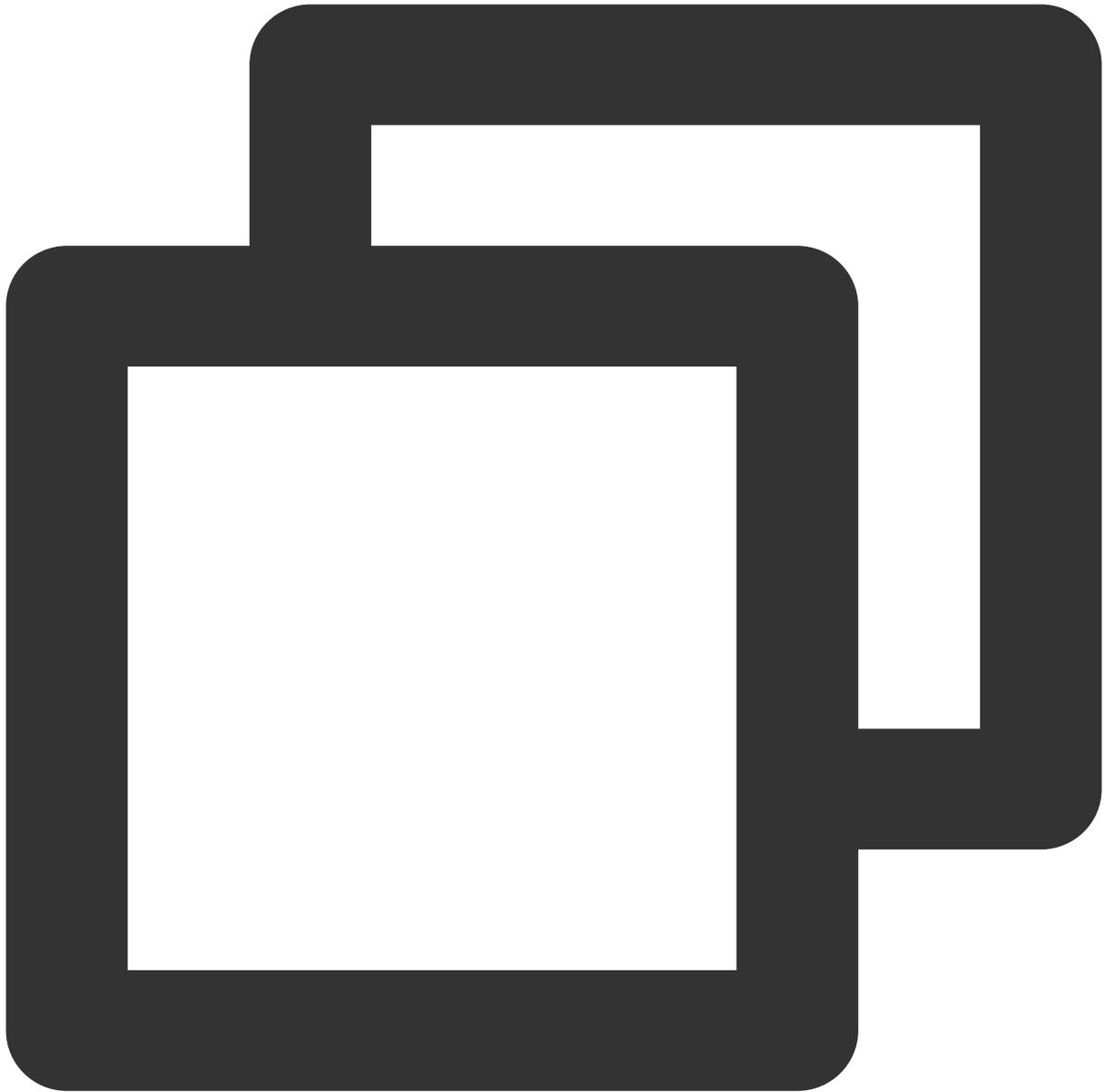
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfa  
52:54:00:BF:B3:51/
```

以下の例では、指定されたENIの情報を取得する方法を説明します。



```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfa
local-ipv4s/
mac
vpc-id
subnet-id
owner-id
primary-local-ipv4
public-ipv4s
local-ipv4s/
```

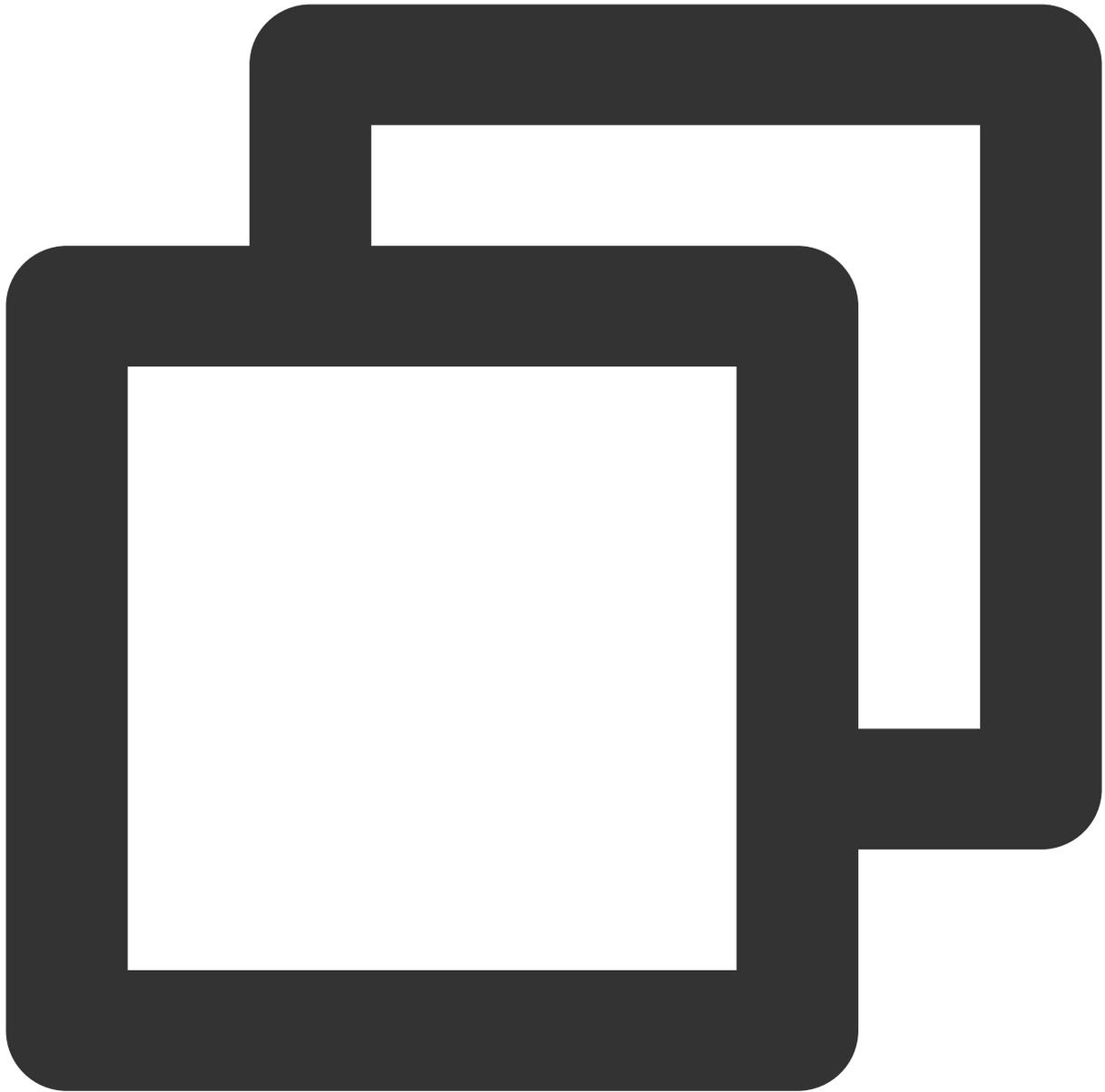
以下の例では、指定されたENIのVPC情報を取得する方法を説明します。



```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfa  
vpc-ja82n9op
```

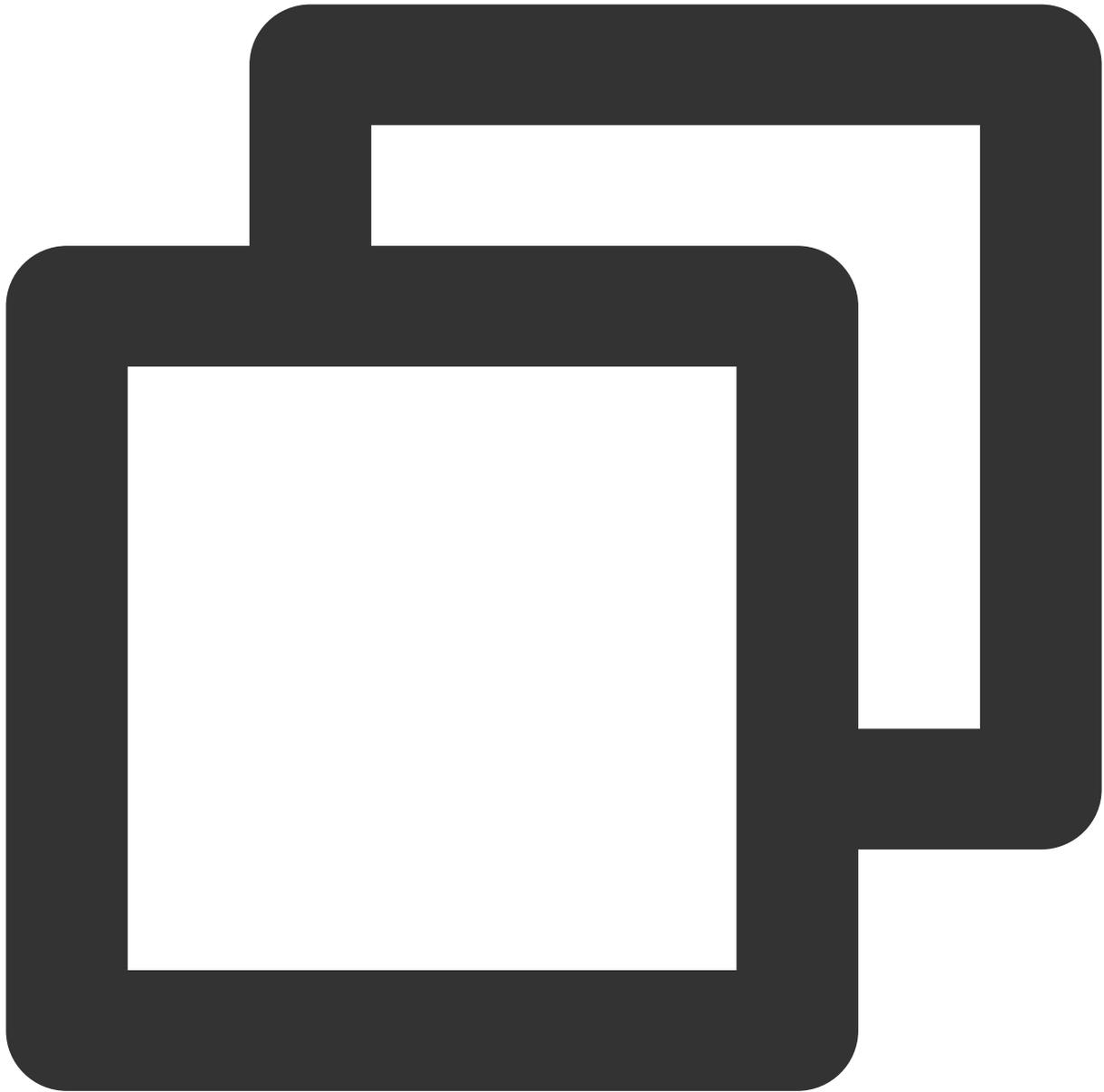
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfa  
subnet-ja82n9op
```

以下の例では、指定されたENIにバインドされたプライベートIPアドレスのリストを取得する方法を説明します。ENIが複数のプライベートIPアドレスにバインドされている場合、複数行のデータが返されます。



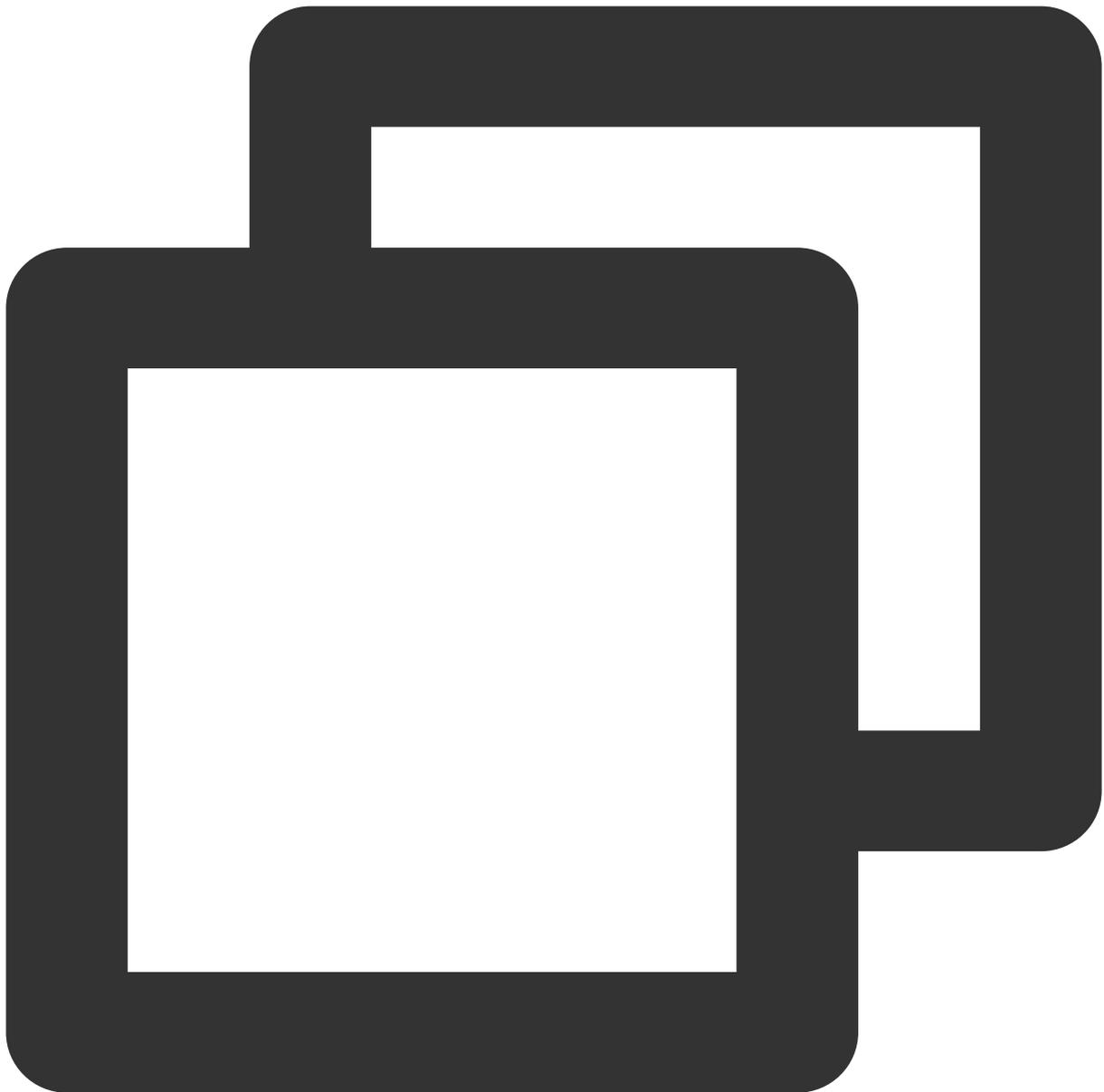
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfa  
10.104.13.59/
```

以下の例では、プライベートIPアドレスの情報を取得する方法を説明します。



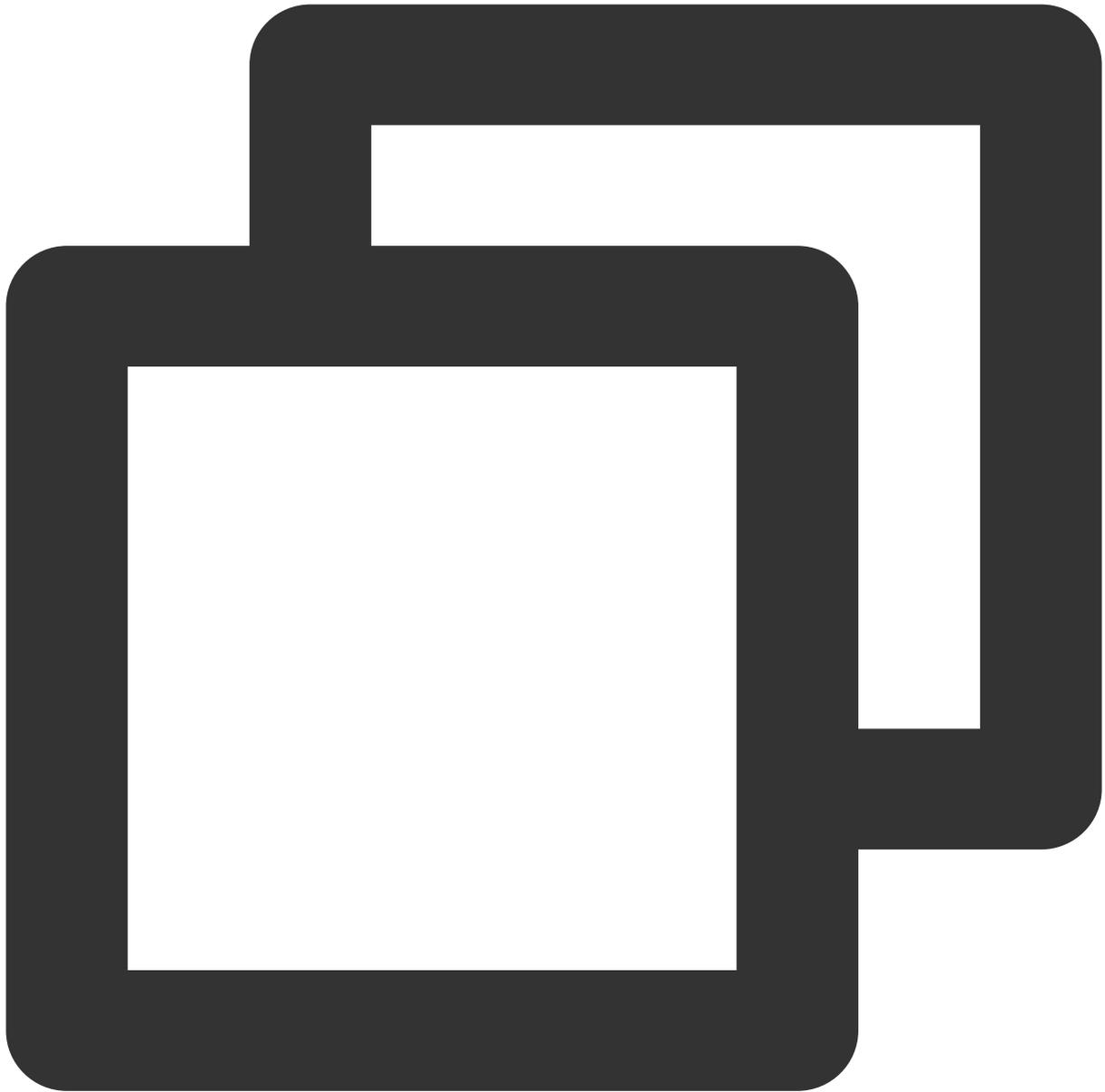
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfa
gateway
local-ipv4
public-ipv4
public-ipv4-mode
subnet-mask
```

以下の例では、プライベートIPアドレスのゲートウェイを取得する方法を説明します。VPCモデルのみがこのデータをクエリできます。VPCモデルの詳細については、[Virtual Private Cloud](#) をご参照ください。



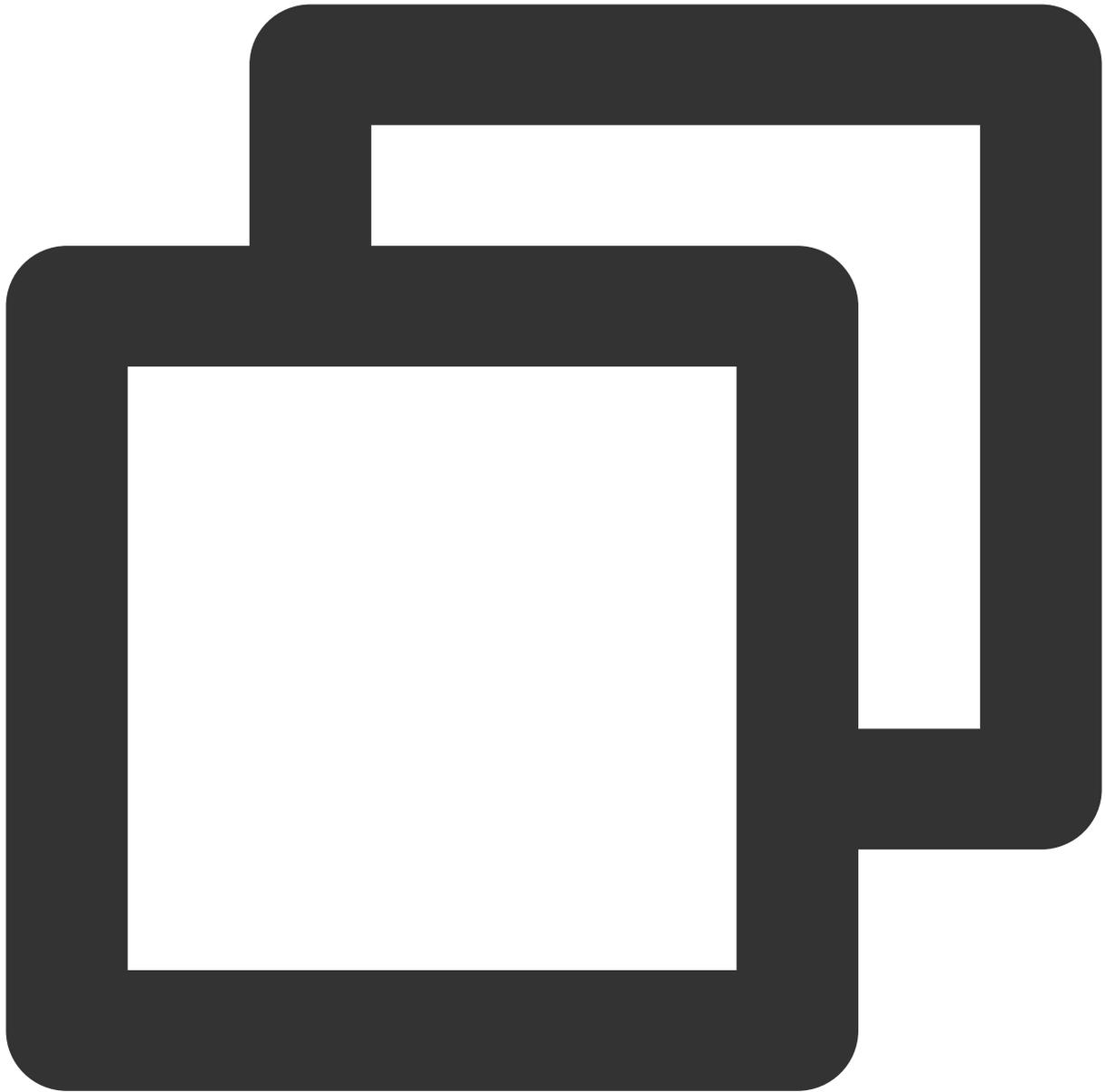
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfa  
10.15.1.1
```

以下の例では、プライベートIPアドレスがパブリックネットワークにアクセスするために使用するアクセスモードを取得する方法を説明します。VPCモデルのみがこのデータをクエリできます。クラシックネットワークタイプのCVMインスタンスは、パブリックネットワークゲートウェイを介してパブリックネットワークにアクセスします。



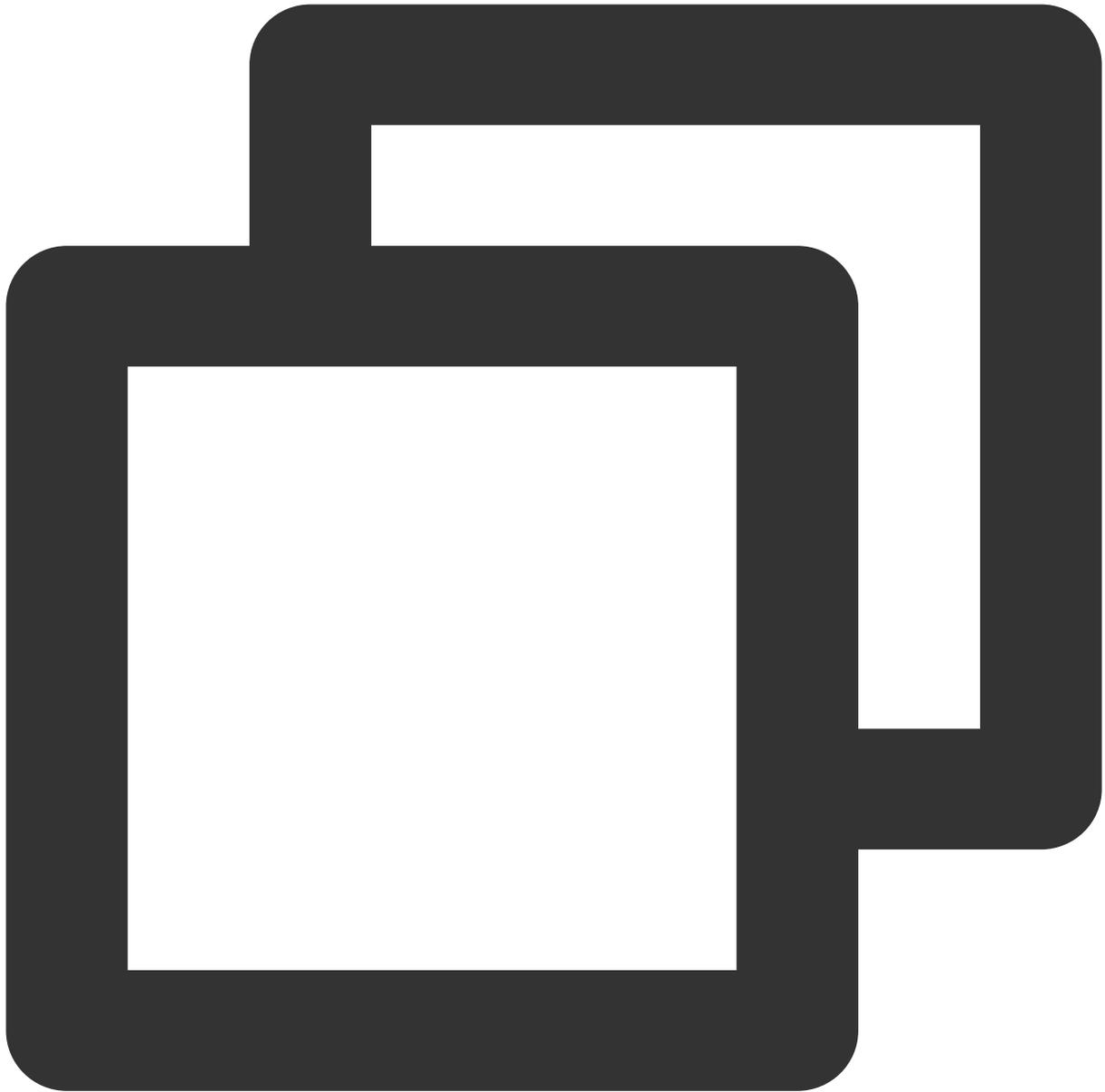
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfa  
NAT
```

以下の例では、プライベートIPアドレスにバインドされたパブリックIPアドレスを取得する方法を説明します。



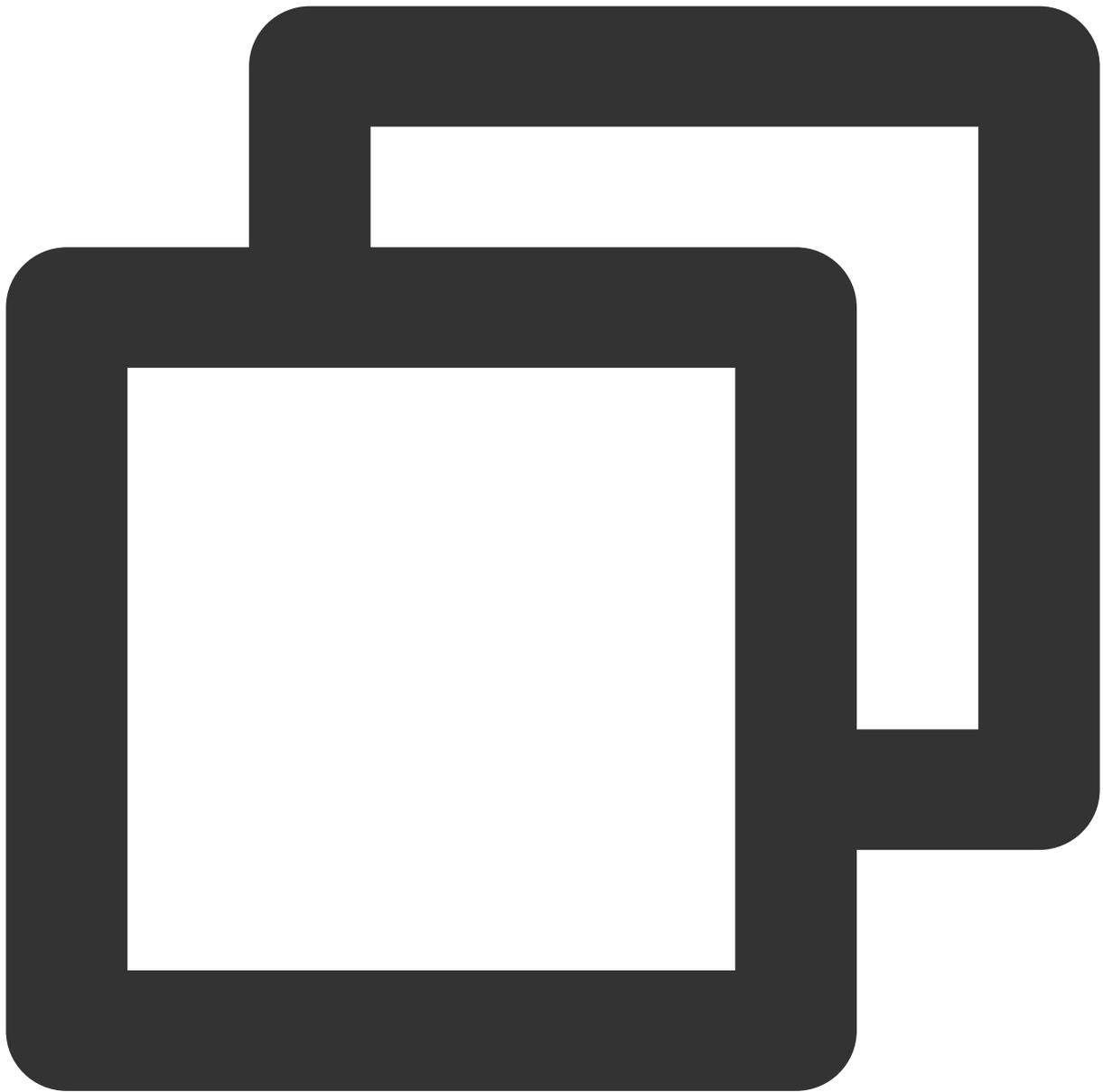
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfa  
139.199.11.29
```

以下の例では、プライベートIPアドレスのサブネットマスクを取得する方法を説明します。



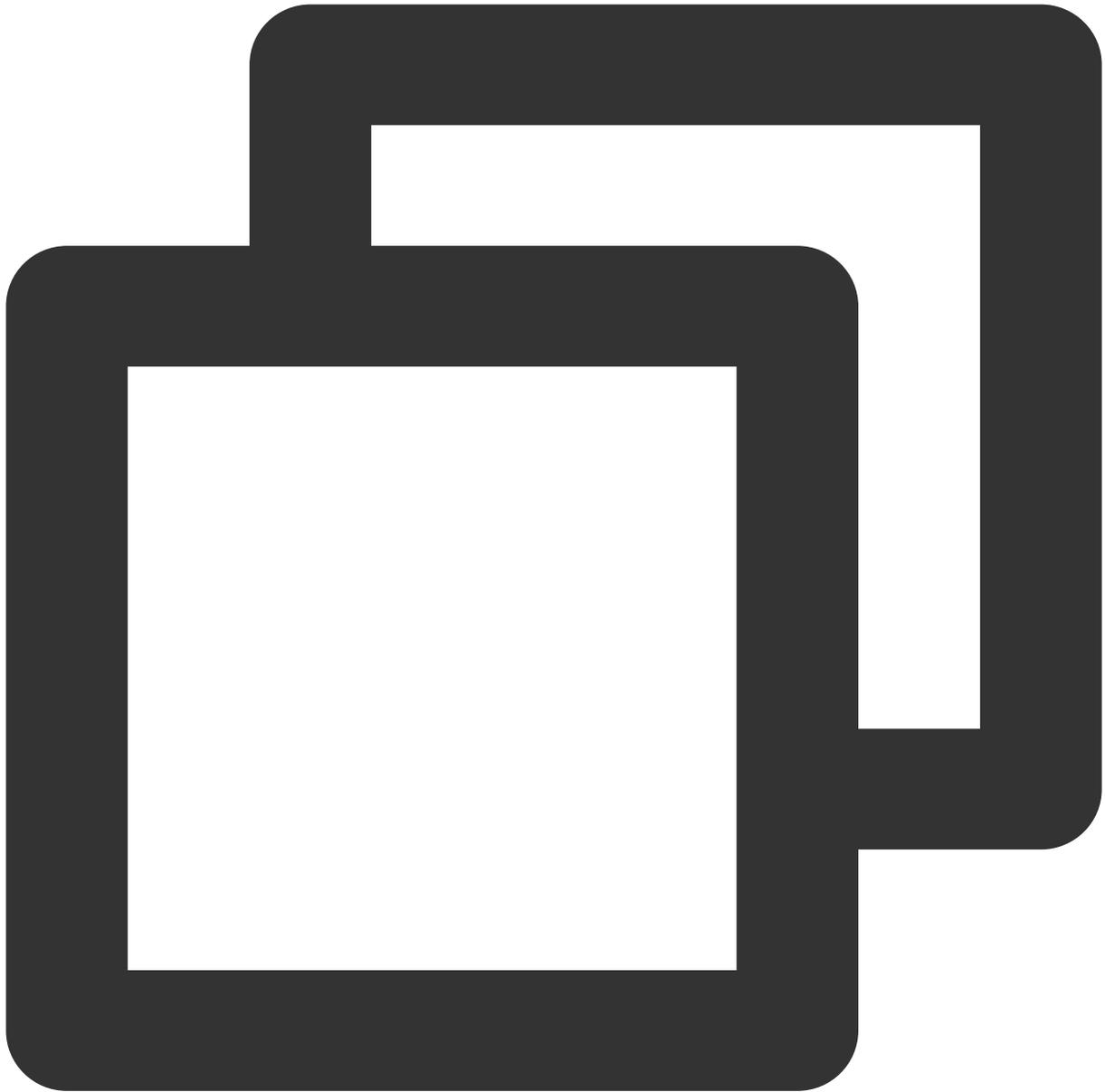
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfa  
255.255.192.0
```

以下の例では、インスタンスの課金方法を取得する方法を説明します。



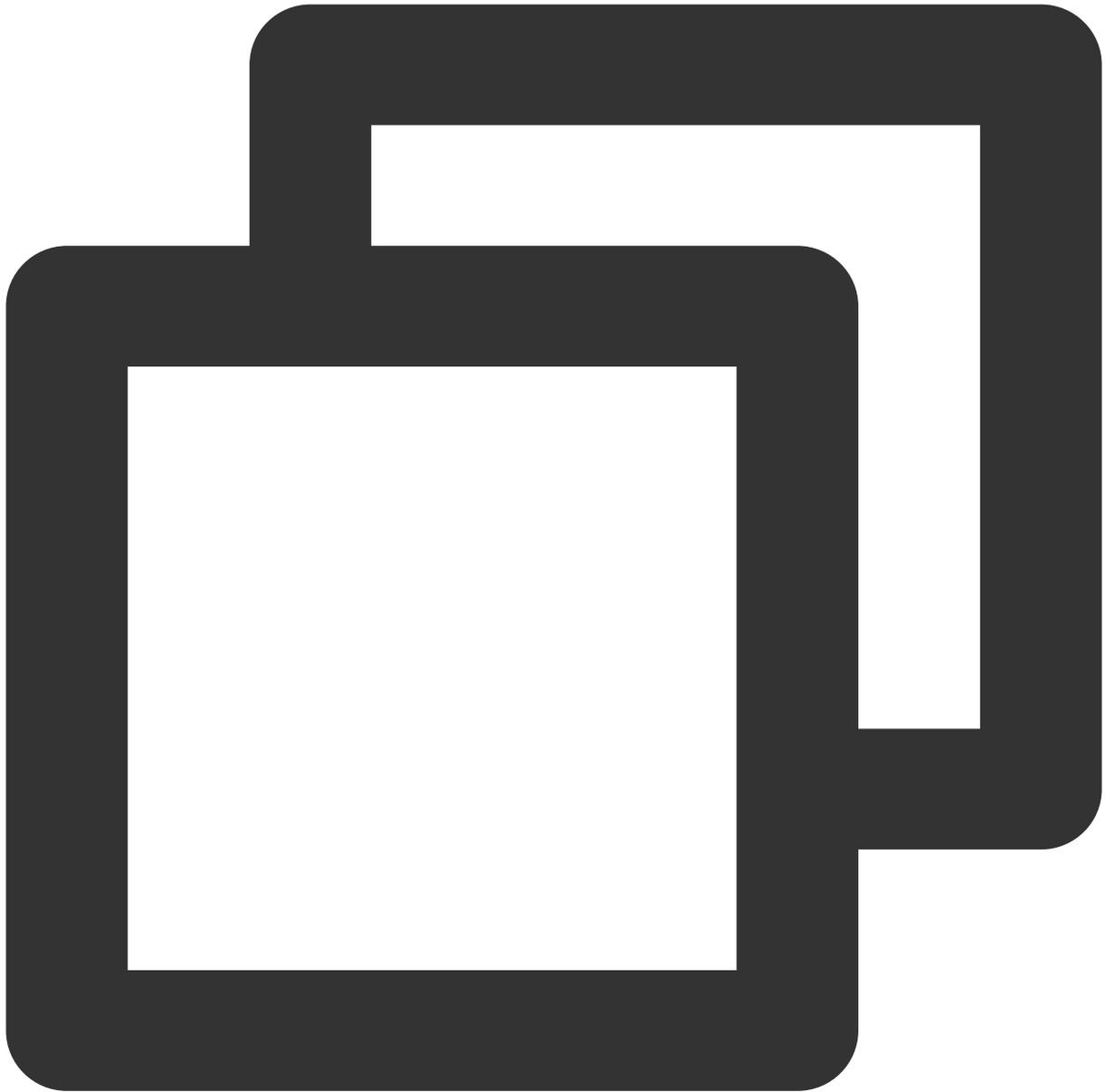
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/payment/charge-  
POSTPAID_BY_HOUR
```

以下の例では、インスタンスの作成時間を取得する方法を説明します。



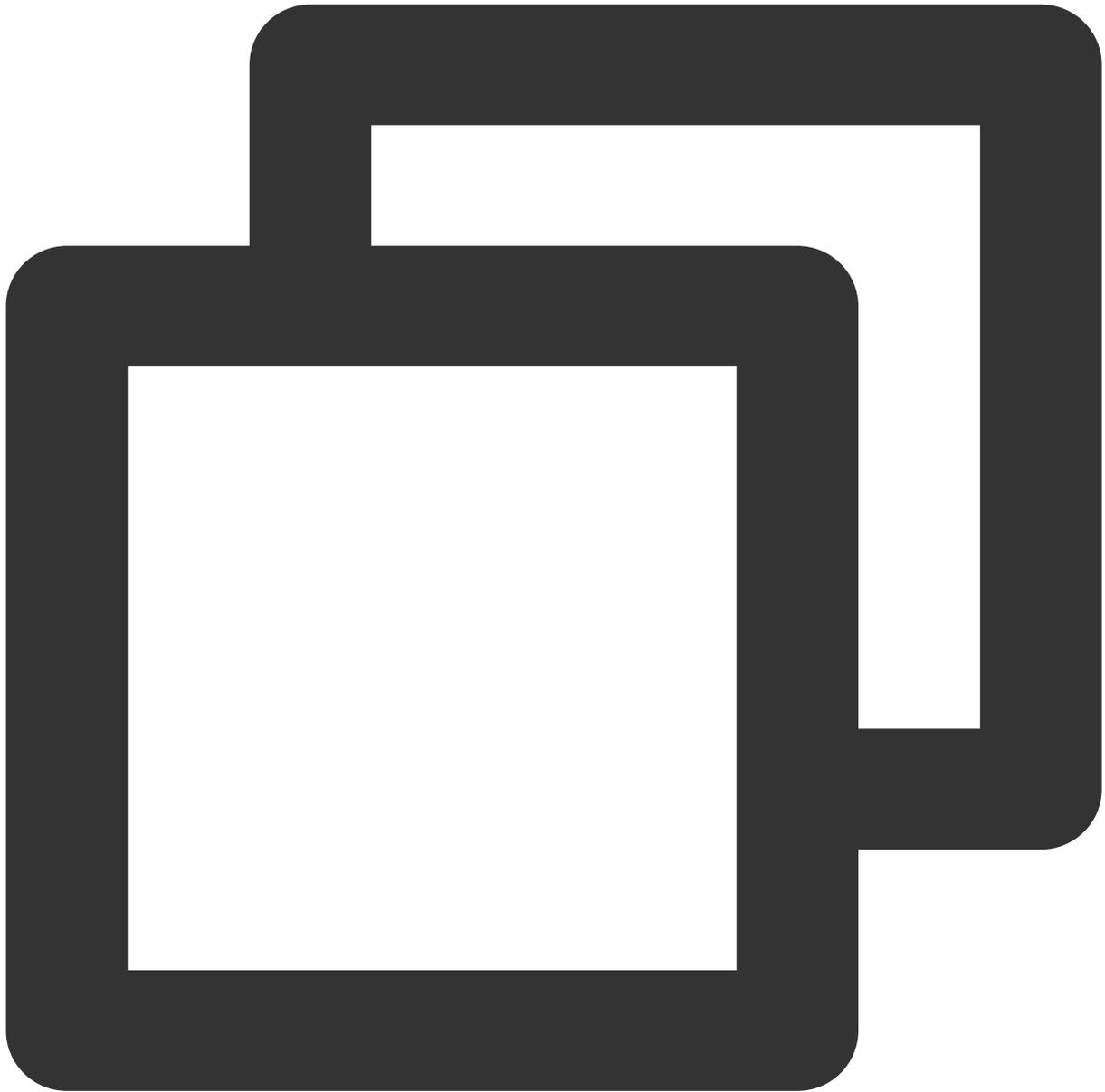
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/payment/create-2018-09-18 11:27:33
```

以下の例では、スポットインスタンスの終了時間を取得する方法を説明します。



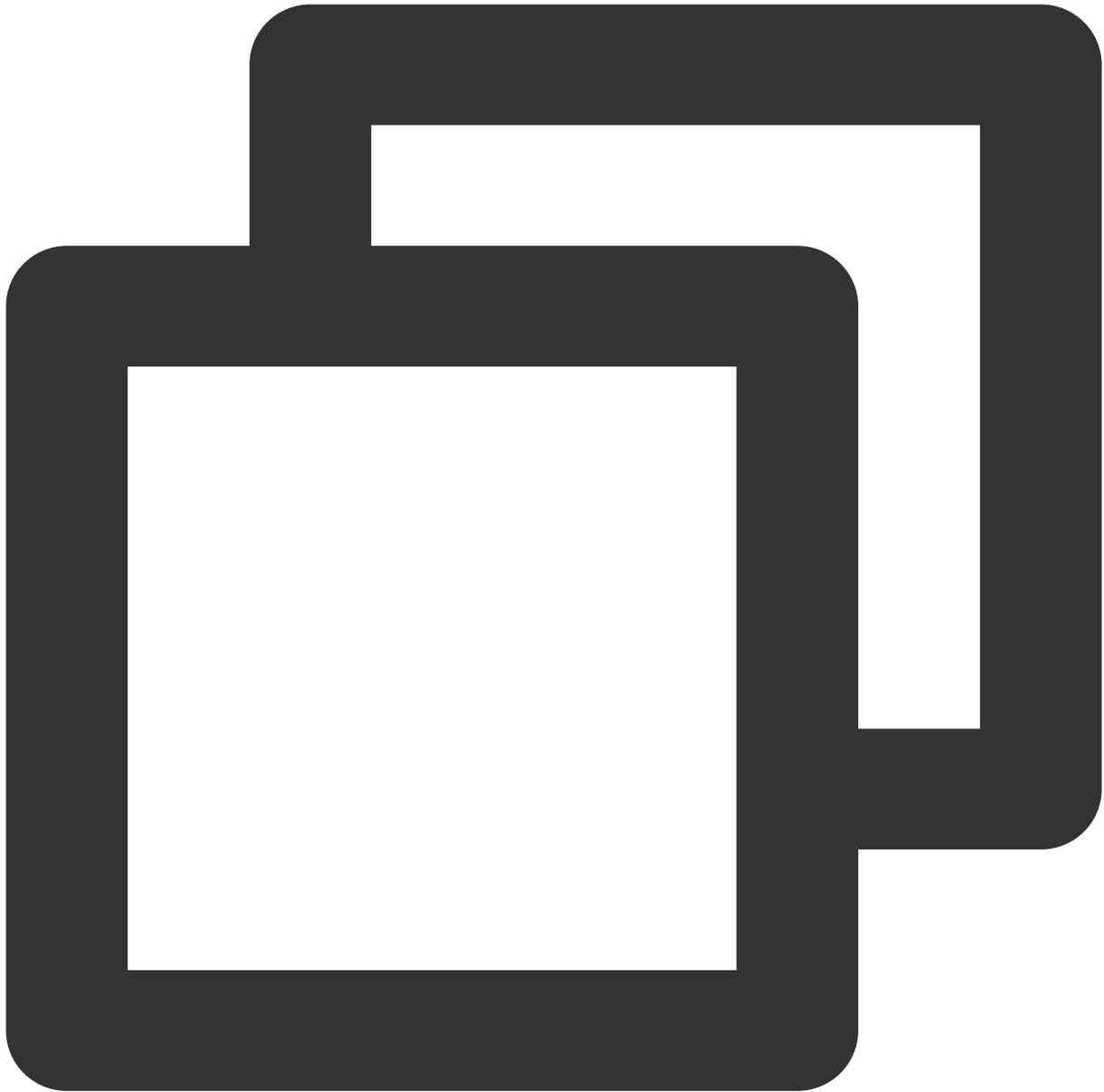
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/spot/terminatio  
2018-08-18 12:05:33
```

以下の例では、CVMが属するアカウントAppIdを取得する方法を説明します。



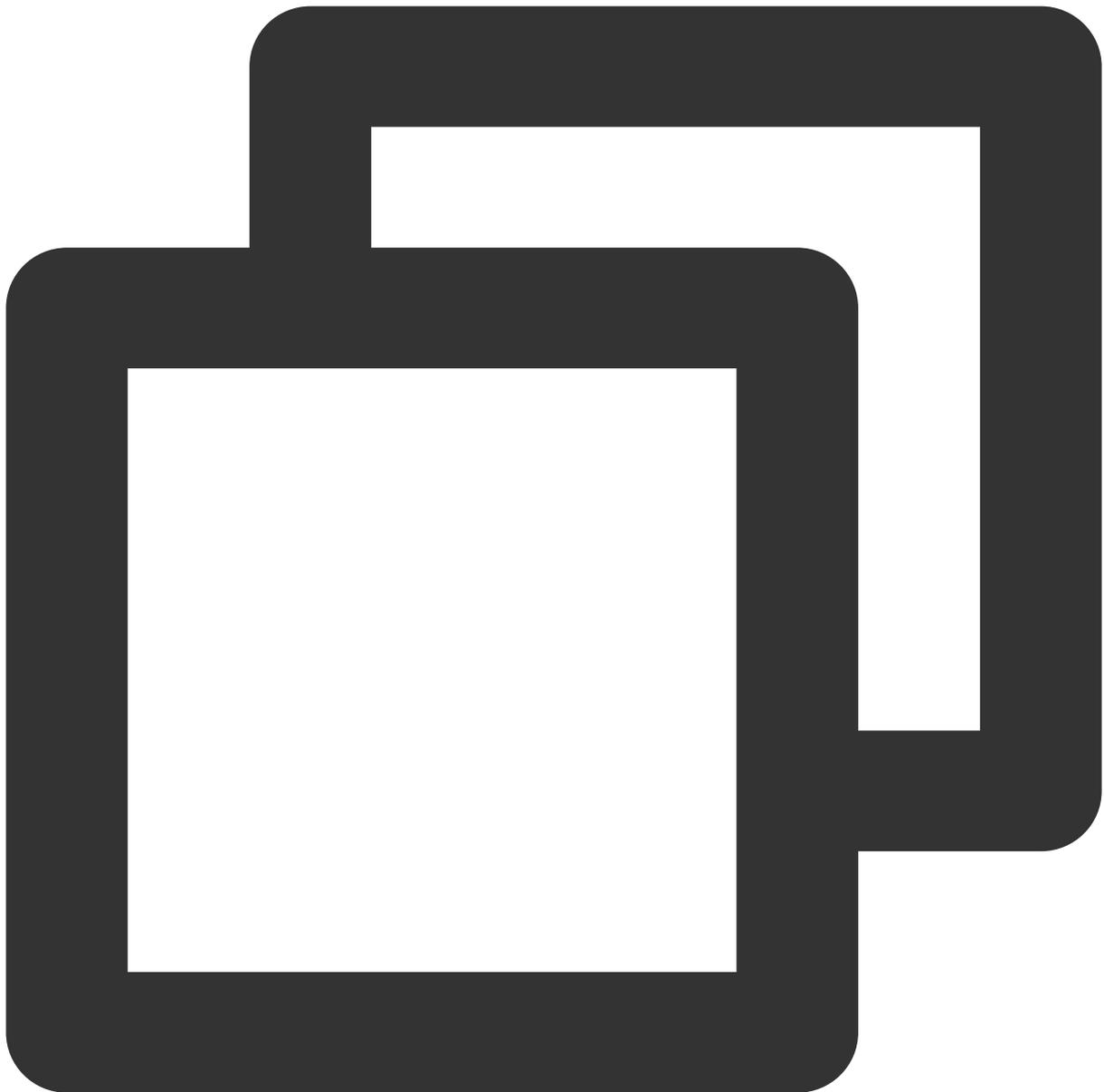
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/app-id  
123456789
```

以下の例では、インスタンスが属する CAM ロールによって生成された一時的な認証情報を取得する方法を説明します。この例では、ロール名は「CVMas」です。



```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/cam/security-cr
{
  "TmpSecretId": "AKIDoQMxA6cW447p225cIt9NW8dhA1dw15UvxxxxxxxxxUqR1Eb5_",
  "TmpSecretKey": "Q9z24VucjF4xQQN1PEsH3xxxxxxxxxxgA=",
  "ExpiredTime": 1615590047,
  "Expiration": "2021-03-12T23:00:47Z",
  "Token": "xxxxxxxxxxxx",
  "Code": "Success"
}
```

以下の例では、インスタンスストレージをクエリする方法を説明します。



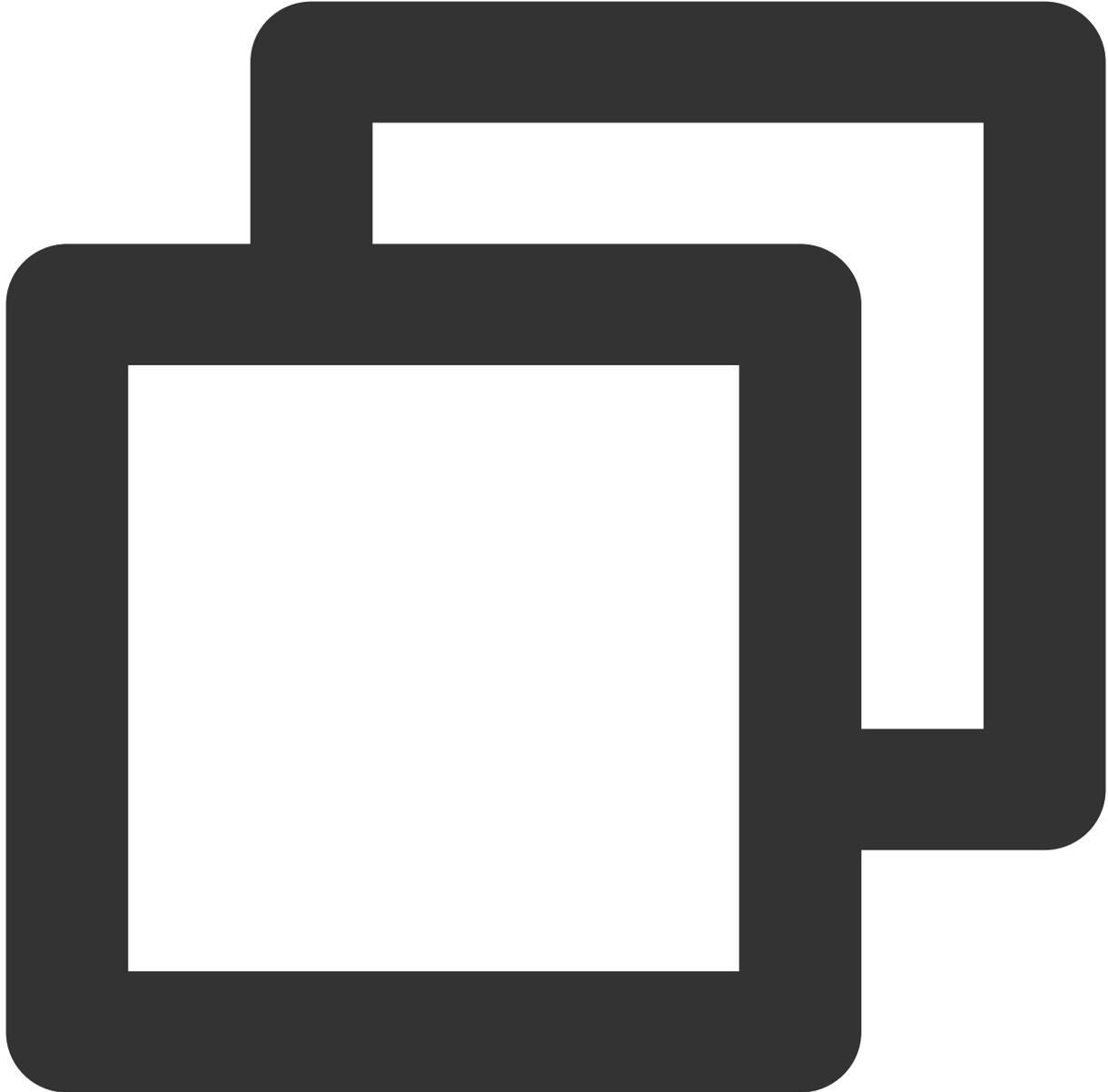
```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/volumes  
disk-xxxxxxx/
```

## インスタンスユーザーデータのクエリ

インスタンスの作成時にインスタンスユーザーデータを指定できます。cloud-initが設定されたCVMインスタンスはこのデータにアクセスできます。

## ユーザーデータの検索

インスタンスにログイン後、以下の方法でユーザーデータにアクセスできます。



```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/user-data  
179, client, shanghai
```

# インスタンスの名前変更

最終更新日：：2023-03-03 11:40:46

## 概要

ユーザーがコンソールで CVM インスタンスを管理し、各インスタンスを名前からすばやく簡単に見つけられるようにするために、Tencent Cloudは各インスタンスのネーミングをサポートし、インスタンスの名前をいつでも変更でき、新しい名前はすぐに有効になります。

## 操作手順

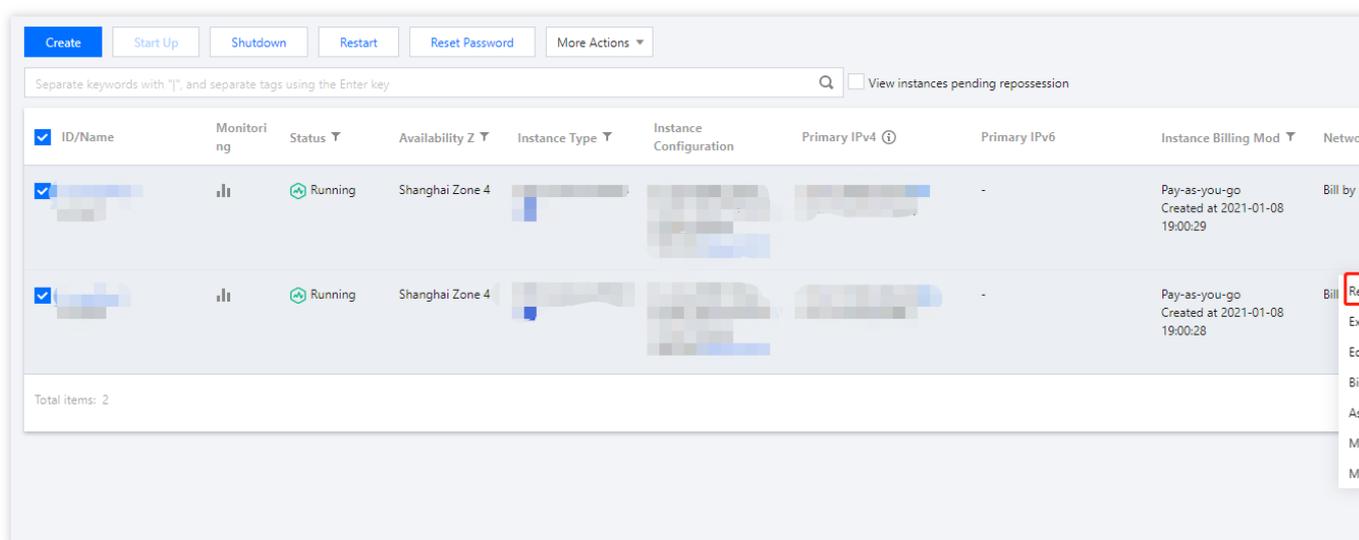
インスタンスの管理画面で、実際に使用されているビューモードに従って操作します。

リストビュー

タブビュー

### 単一インスタンスの名前変更

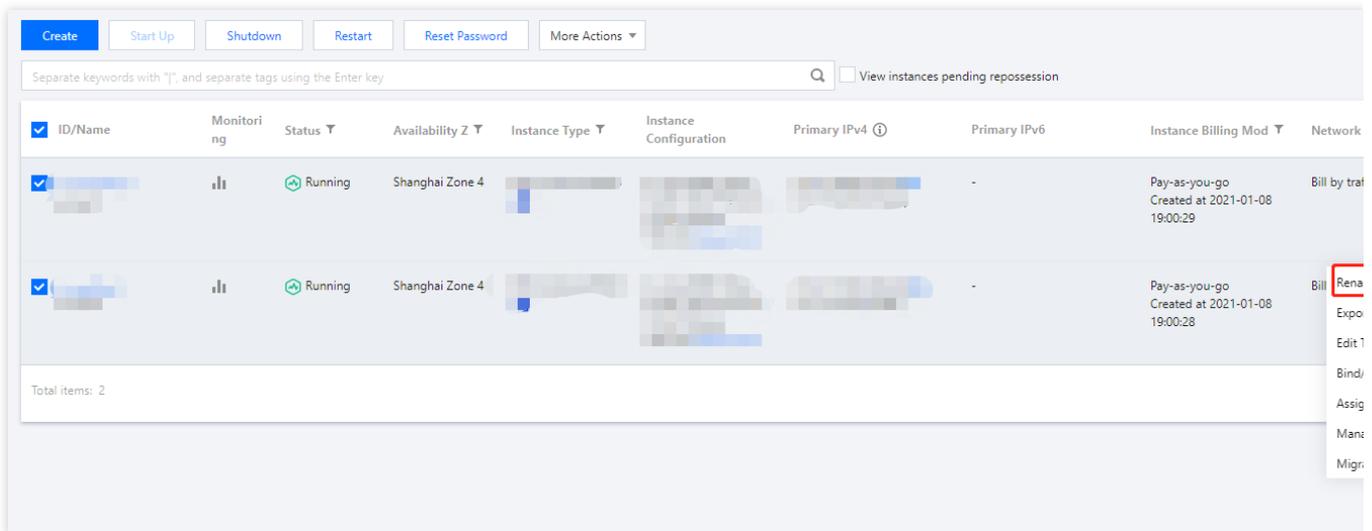
1. [CVMコンソール](#) にログインします。
2. 下図のように、インスタンスリストで、名前を変更したいインスタンスを選択し、画面右のメニューからさらに [>インスタンス設定>名前変更](#) をクリックします。



3. ポップアップウィンドウで、新しいインスタンス名を入力し、**OK** をクリックします。これで名前の変更が完了します。

### 複数インスタンスの名前変更

1. [CVMコンソール](#)にログインします。
2. 下図のように、インスタンスリストで、名前を変更したい複数のインスタンスを選択し、画面上部のメニューバーから**その他の操作>インスタンス設定>名前変更**をクリックします。

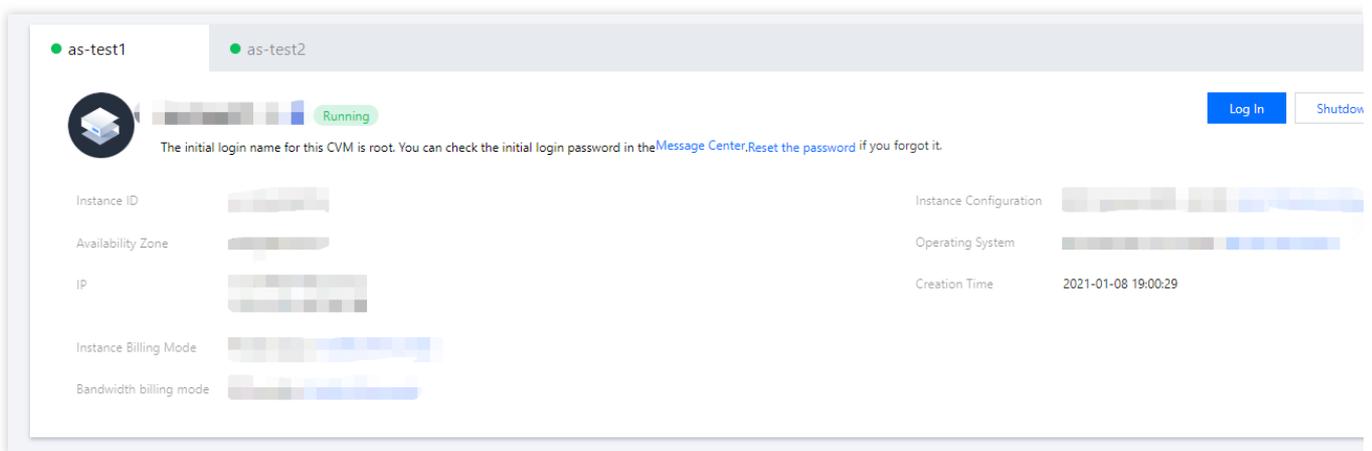


3. ポップアップウィンドウで、新しいインスタンス名を入力し、**OK**をクリックします。これで名前の変更が完了します。

#### 説明：

この方法で変更された複数のインスタンスの名前はすべて同じになります。

1. [CVMコンソール](#)にログインします。
2. 下図のように、インスタンスの名称を変更したいCVMタブを選択し、画面右上コーナーの**その他操作>インスタンス設定>名称変更**を選択します。



3. ポップアップウィンドウで、新しいインスタンス名を入力し、**OK**をクリックします。これで名前の変更が完了します。

# インスタンスのパスワードのリセット方法

最終更新日：：2023-03-03 11:55:53

## 概要

CVMインスタンスのログインパスワードを忘れた場合は、コンソールでリセットすることができます。このドキュメントでは、コンソールでインスタンスのログインパスワードをリセットする方法について説明します。

### ご注意：

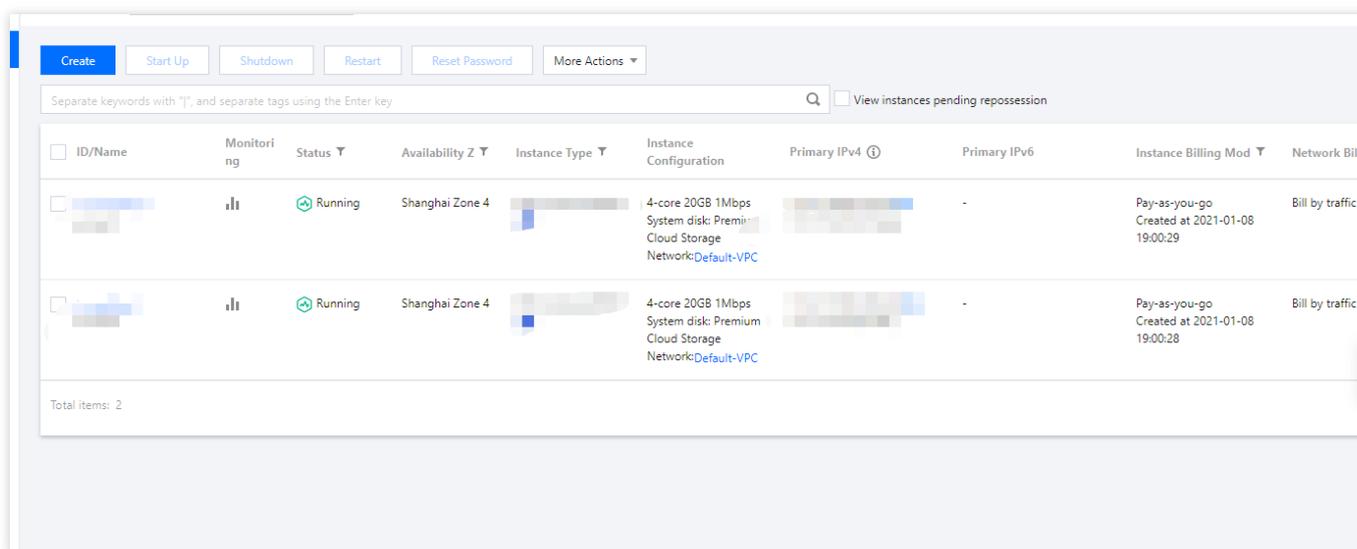
インスタンスが「シャットダウン」状態である場合、ログインパスワードを直接リセットできます。インスタンスがまだ実行中の場合、コンソールでログインパスワードをリセットすると強制的にシャットダウンされます。データが失われるのを防ぐため、あらかじめ操作時間の計画を立てておいてください。業務時間外やオフピーク時にパスワードをリセットすることをお勧めします。

## 操作手順

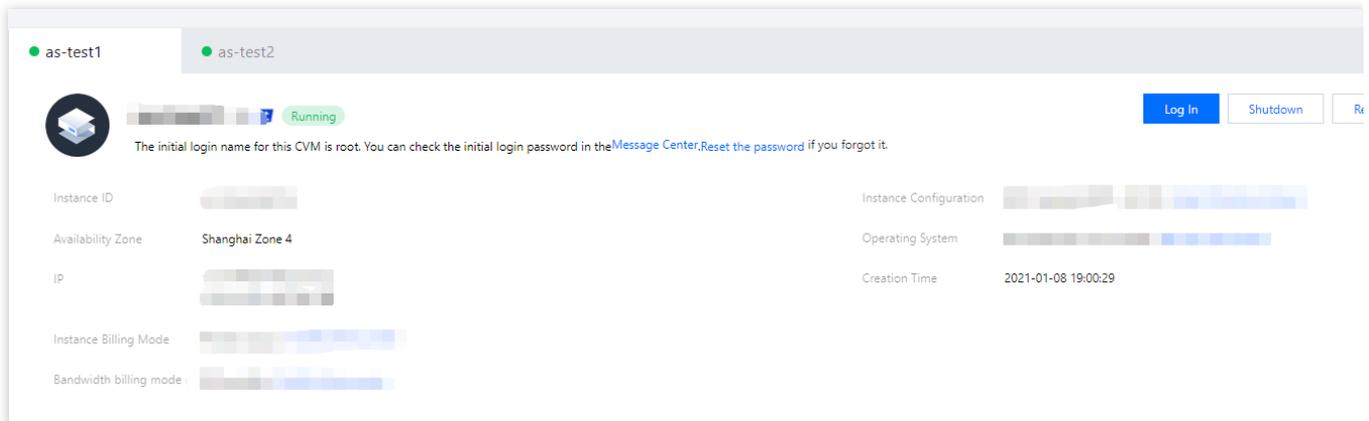
単一インスタンスのパスワードのリセット

複数インスタンスのパスワードのリセット

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画面で、実際に使用されているビューモードに従って操作します。  
リストビュー：下図のように、パスワードをリセットしたいCVMインスタンスを選択し、画面右のメニューからさらに>パスワード/キー>パスワードをリセットをクリックします。



**タブビュー**：下図のように、パスワードをリセットしたいCVMページで、**パスワードをリセット**ボタンをクリックします。



3. 下図のように、ポップアップウィンドウで、「ユーザー名」のタイプを選択し、パスワードをリセットしたいユーザー名と、対応する「新しいパスワード」と「パスワードの確認」を入力して、**次へ**をクリックします。

#### ご注意：

そのうち「ユーザー名」タイプのデフォルトは「システムデフォルト」であり、対応するOSのデフォルトユーザー名（Windowsシステムのデフォルトユーザー名は Administrator、Ubuntuシステムのデフォルトユーザー名は ubuntu、その他のバージョンのLinuxシステムのデフォルトは root）が使用されます。別のユーザー名を指定する必要がある場合は、「ユーザー名の指定」を選択し、対応するユーザー名を入力してください。

## Reset Password ✕

**1** Set Password > **2** Shutdown CVM

You've selected 1 instance. [Collapse](#)

ID/Name	Instance Type	Instance Configuration
	Standard S5	1-core 1GB 1Mbps System disk: Premium Cloud Storage Network

Username

New Password

Please enter the instance password

Confirm Password

Please enter the instance password again

**i** It may take some time for the new password to take effect. If you cannot log in with the new password, please wait and try again later.

4. インスタンスの状態に従ってパスワードをリセットします。

下図のように、状態が「**実行中**」であるインスタンスのパスワードをリセットするには、「**強制シャットダウンに同意**」にチェックを入れ、**パスワードをリセット**ボタンをクリックします。これでパスワードのリセットは完了です。

### Reset Password ✕

✓ Set Password > 2 Shutdown CVM

**i** You need to shutdown the instance for the current operation:

- To avoid data loss, we will shut down the instance before adjusting the configuration. Your business will be interrupted during shut down so please take necessary precautions before continuing.
- Forced shutdown may result in data loss or file system corruption. We recommend manually shutting down CVM manually before the operation.
- Forced shutdown may take a while. Please be patient.

Forced shutdown \*  Agree to a forced shutdown

[Previous step](#) [Reset Password](#)

下図のように、状態が「シャットダウン」であるインスタンスのパスワードをリセットするには、パスワードをリセットボタンをクリックします。これでパスワードのリセットは完了です。

### Reset Password ✕

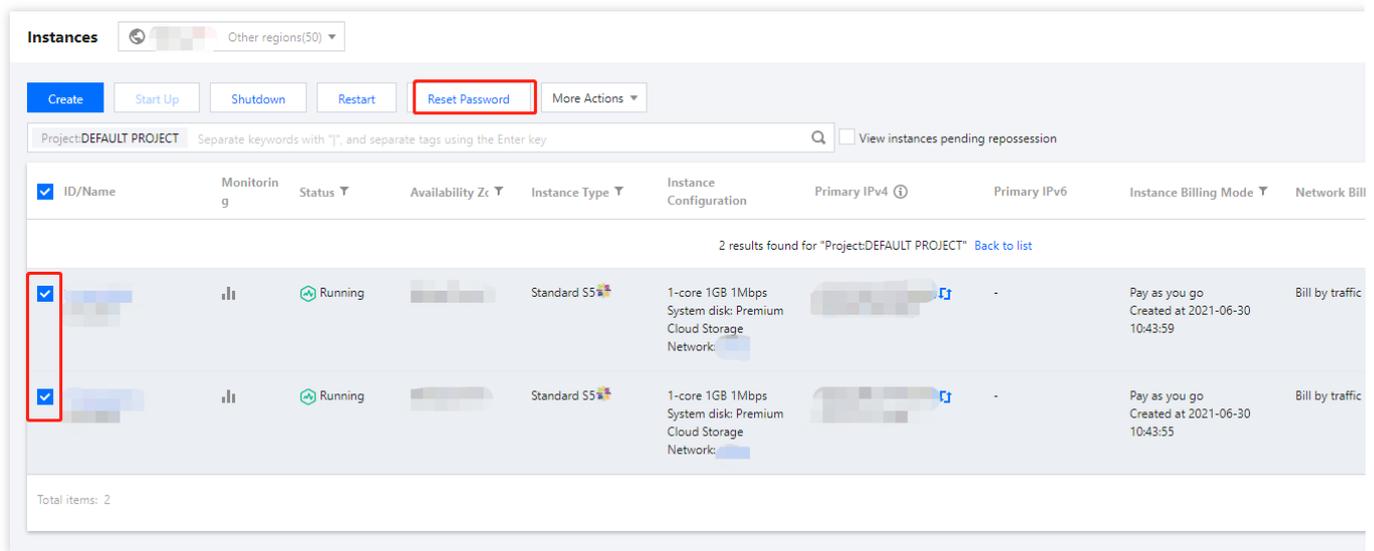
✓ Set Password > 2 Shutdown CVM

**i** You need to shutdown the instance for the current operation, and all selected instances are shut down.

[Previous step](#) [Reset Password](#)

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、パスワードをリセットするCVMインスタンスを選択し、画面上部のメニューバーからパスワードをリセットボタンをクリックします。



3. 下図のように、「パスワード設定」手順で、「ユーザー名」のタイプを選択し、パスワードをリセットしたいユーザー名と、対応する「新しいパスワード」と「パスワードの確認」を入力して**次へ**をクリックします。

#### ご注意：

そのうち「ユーザー名」タイプのデフォルトは「システムデフォルト」であり、対応するOSのデフォルトユーザー名（Windowsシステムのデフォルトユーザー名は Administrator、Ubuntuシステムのデフォルトユーザー名は ubuntu、その他のバージョンのLinuxシステムのデフォルトは root）が使用されます。別のユーザー名を指定する必要がある場合は、「ユーザー名の指定」を選択し、対応するユーザー名を入力してください。

### Reset Password ×

**1 Set Password** > **2 Shutdown CVM**

You've selected 2 instances. [Collapse](#)

ID/Name	Instance Type	Instance Configuration
[Redacted]	Standard S5	1-core 1GB 1Mbps System disk: Premium Cloud Storage Network: [Redacted]
[Redacted]	Standard S5	1-core 1GB 1Mbps System disk: Premium Cloud Storage Network: [Redacted]

Username:

New Password:

Please enter the instance password

Confirm Password:

Please enter the instance password again

**i** It may take some time for the new password to take effect. If you cannot log in with the new password, please wait and try again later.

4. インスタンスの状態に従ってパスワードをリセットします。

下図のように、状態が「**実行中**」であるインスタンスのパスワードをリセットするには、「**強制シャットダウンに同意**」にチェックを入れ、**パスワードをリセット**ボタンをクリックします。これでパスワードのリセットは完了です。

### Reset Password ✕

✓ Set Password > 2 Shutdown CVM

**i** You need to shutdown the instance for the current operation:

- To avoid data loss, we will shut down the instance before adjusting the configuration. Your business will be interrupted during shut down so please take necessary precautions before continuing.
- Forced shutdown may result in data loss or file system corruption. We recommend manually shutting down CVM manually before the operation.
- Forced shutdown may take a while. Please be patient.

Forced shutdown \*  Agree to a forced shutdown

[Previous step](#) [Reset Password](#)

下図のように、状態が「シャットダウン」であるインスタンスのパスワードをリセットするには、パスワードをリセットボタンをクリックします。これでパスワードのリセットは完了です。

### Reset Password ✕

✓ Set Password > 2 Shutdown CVM

**i** You need to shutdown the instance for the current operation, and all selected instances are shut down.

[Previous step](#) [Reset Password](#)

## よくある質問

Windowsインスタンスのパスワードのリセットに失敗した場合は、[CVMパスワードリセット失敗](#)、または[パスワードが無効](#)を参照してトラブルシューティングを行うことができます。

# インスタンス IP アドレスを管理する

## プライベートIPアドレスの取得とDNSの設定

最終更新日： : 2023-04-13 10:51:02

### 概要

このドキュメントでは、インスタンスのプライベートIPアドレスを取得し、プライベートDNSを設定する方法について説明します。

### 操作手順

#### インスタンスのプライベートIPアドレスの取得

コンソールを利用した取得

API を利用した取得

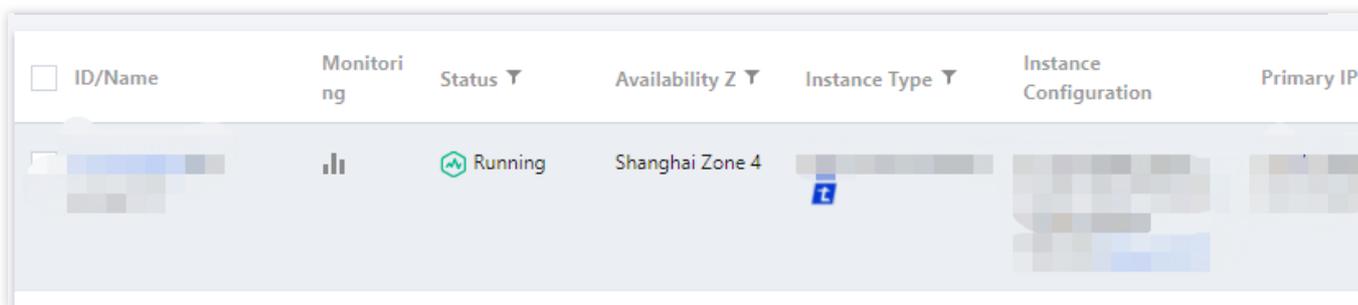
インスタンスメタデータを利用した取得

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、実際に使用されているビューモードに従って操作します。

**リストビュー**：下図のように、プライベートIPを表示したいインスタンスを選択し、マウスを「プライマリIPv4アドレス」列に移動して、

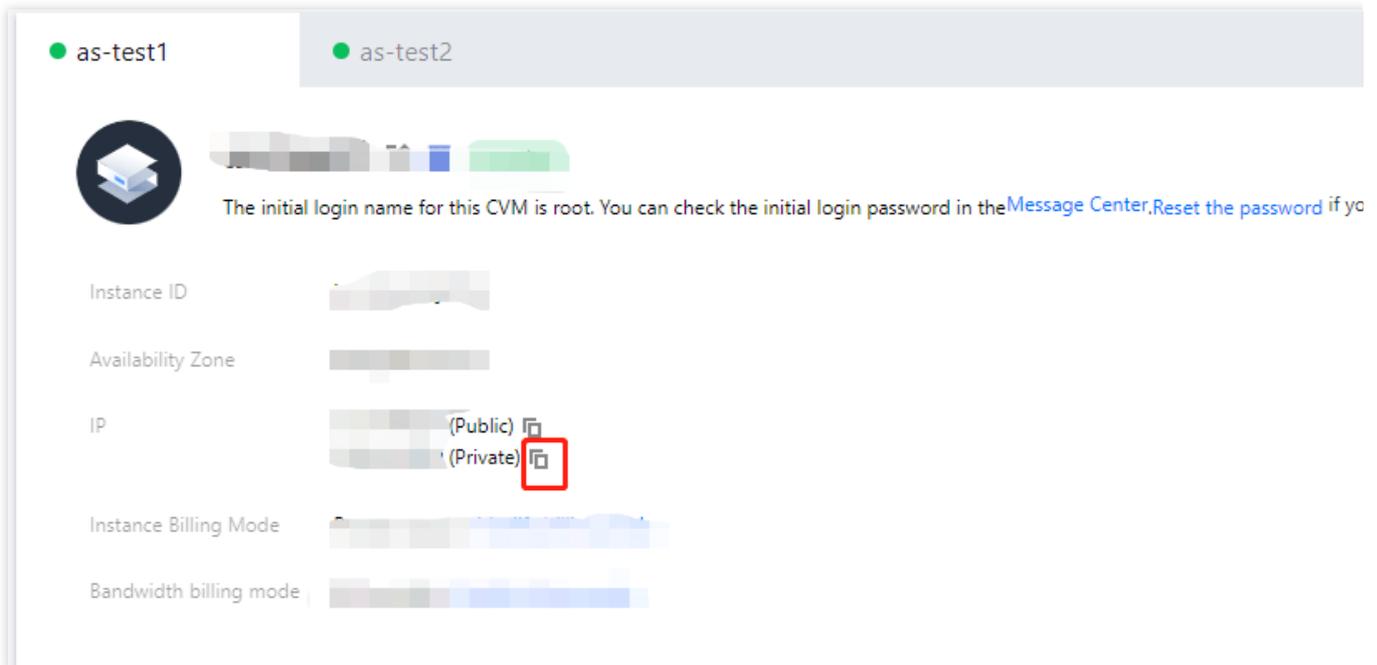
 をクリックすれば、プライベートIPをコピーできます。



ID/Name	Monitoring	Status	Availability Z	Instance Type	Instance Configuration	Primary IPv4
[Redacted]	[Redacted]	Running	Shanghai Zone 4	[Redacted]	[Redacted]	[Redacted]

**タブビュー**：下図のように、インスタンスページで、「IPアドレス」のプライベートネットワークアドレス後の

 をクリックすれば、プライベートIPをコピーできます。



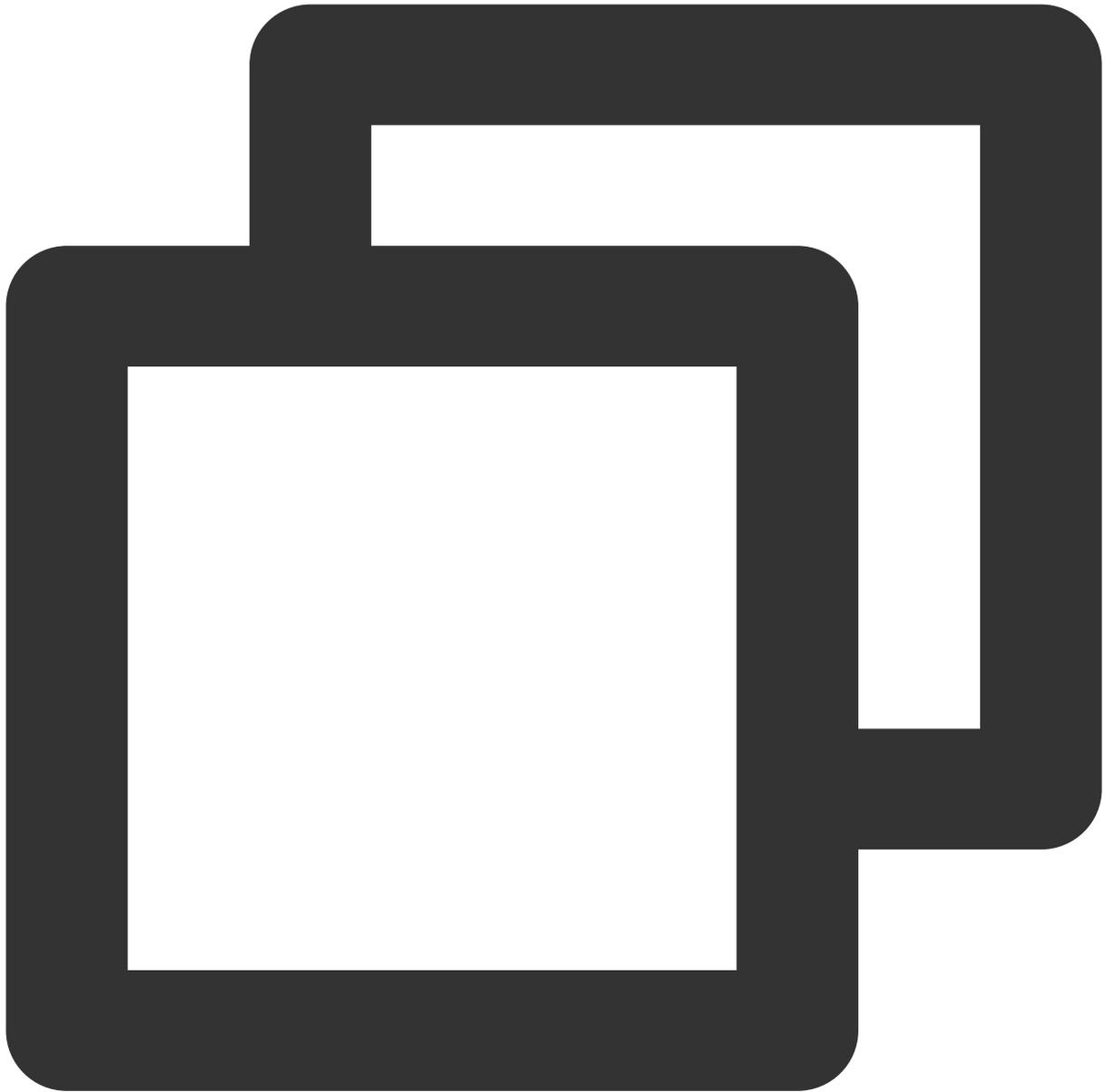
[DescribeInstances](#) インターフェースをご参照ください。

1. CVMにログインします。
2. cURLツールまたはHTTPのGETリクエストを介して、インスタンスのメタデータにアクセスします。

**説明：**

以下の操作は、cURLツールを例とします。

次のコマンドを実行し、プライベートIPを取得します。



```
curl http://metadata.tencentyun.com/meta-data/local-ipv4
```

下図のように、返される情報はプライベートIPアドレスです。

```
[root@UM_58_27_centos ~]# curl http://metadata.tencentyun.com/meta-data/local-ipv4  
10.XXX.XX.27
```

インスタンスメタデータのさらに詳細な情報については、[インスタンスメタデータの確認](#)をご参照ください。

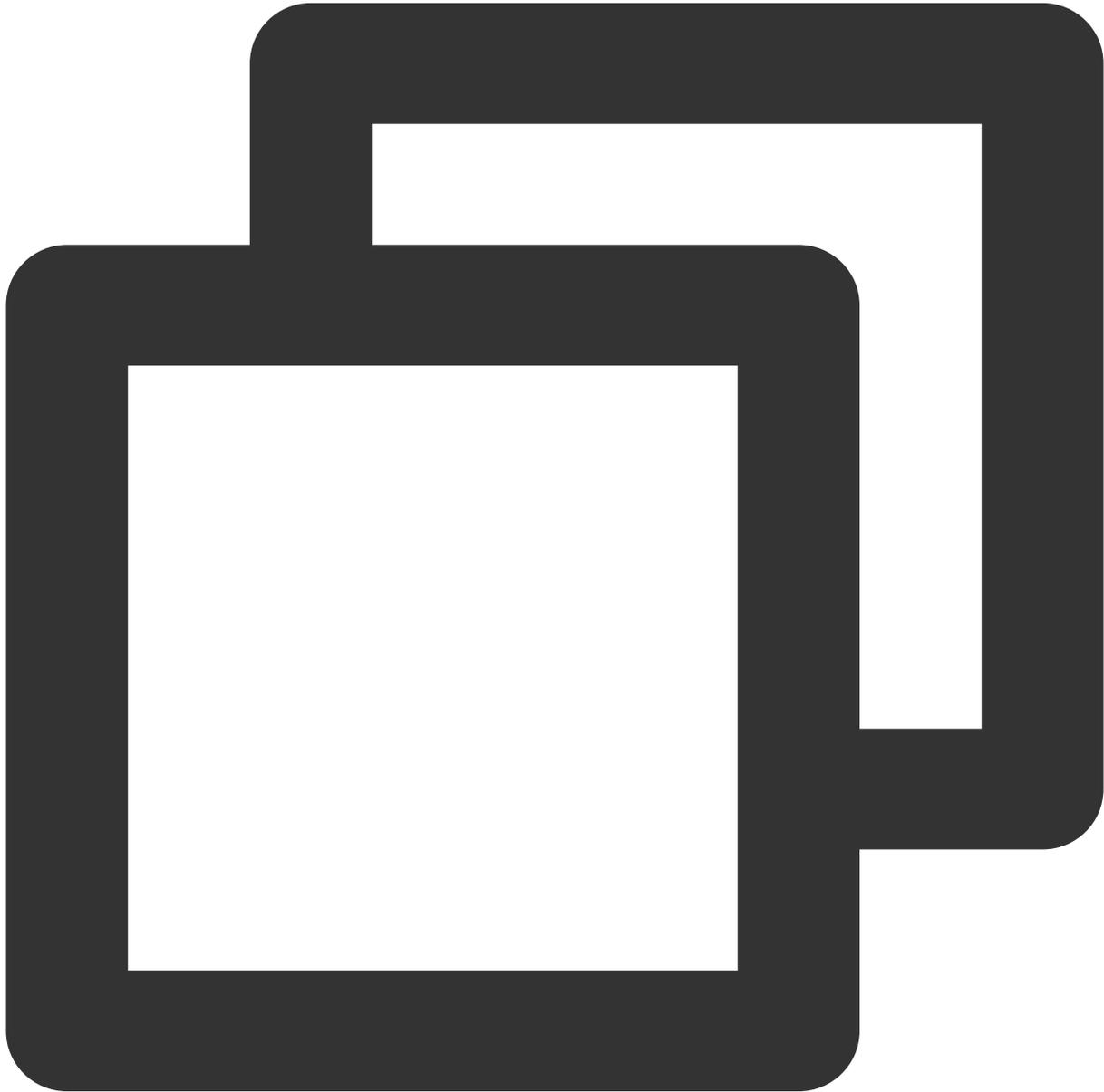
## プライベートネットワークDNSの設定

ネットワーク解析にエラーが発生した場合、CVMのOSの種類に応じてプライベートネットワークDNSを手動で設定できます。

Linux システム

Windows システム

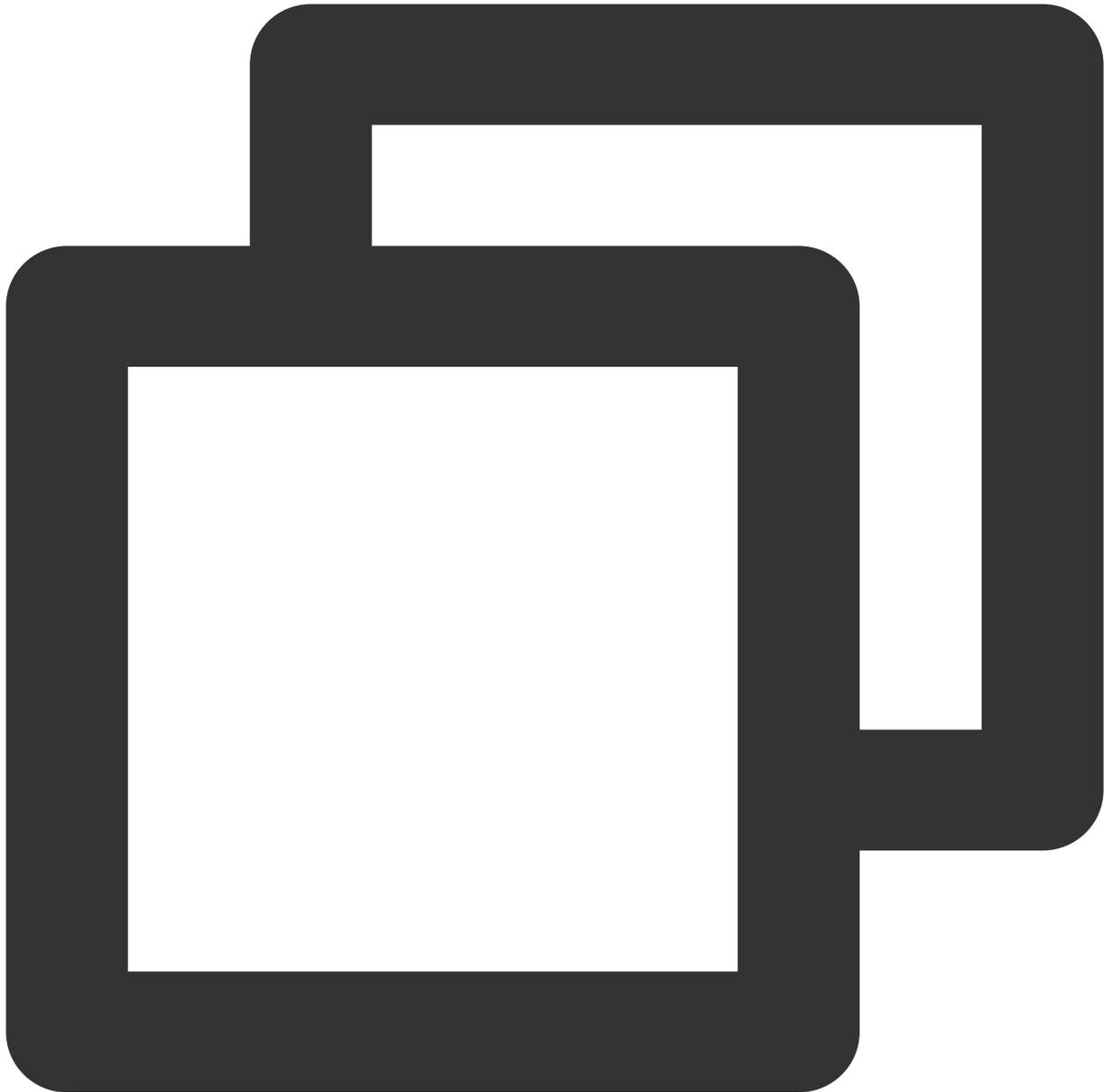
1. Linux CVMにログインします。
2. 次のコマンドを実行して、 `/etc/resolv.conf` ファイルを開きます。



```
vi /etc/resolv.conf
```

3. 「i」キーを押して編集モードに切り替え、[プライベートネットワークDNS](#)に対応するリージョンに従ってDNS IPを変更します。

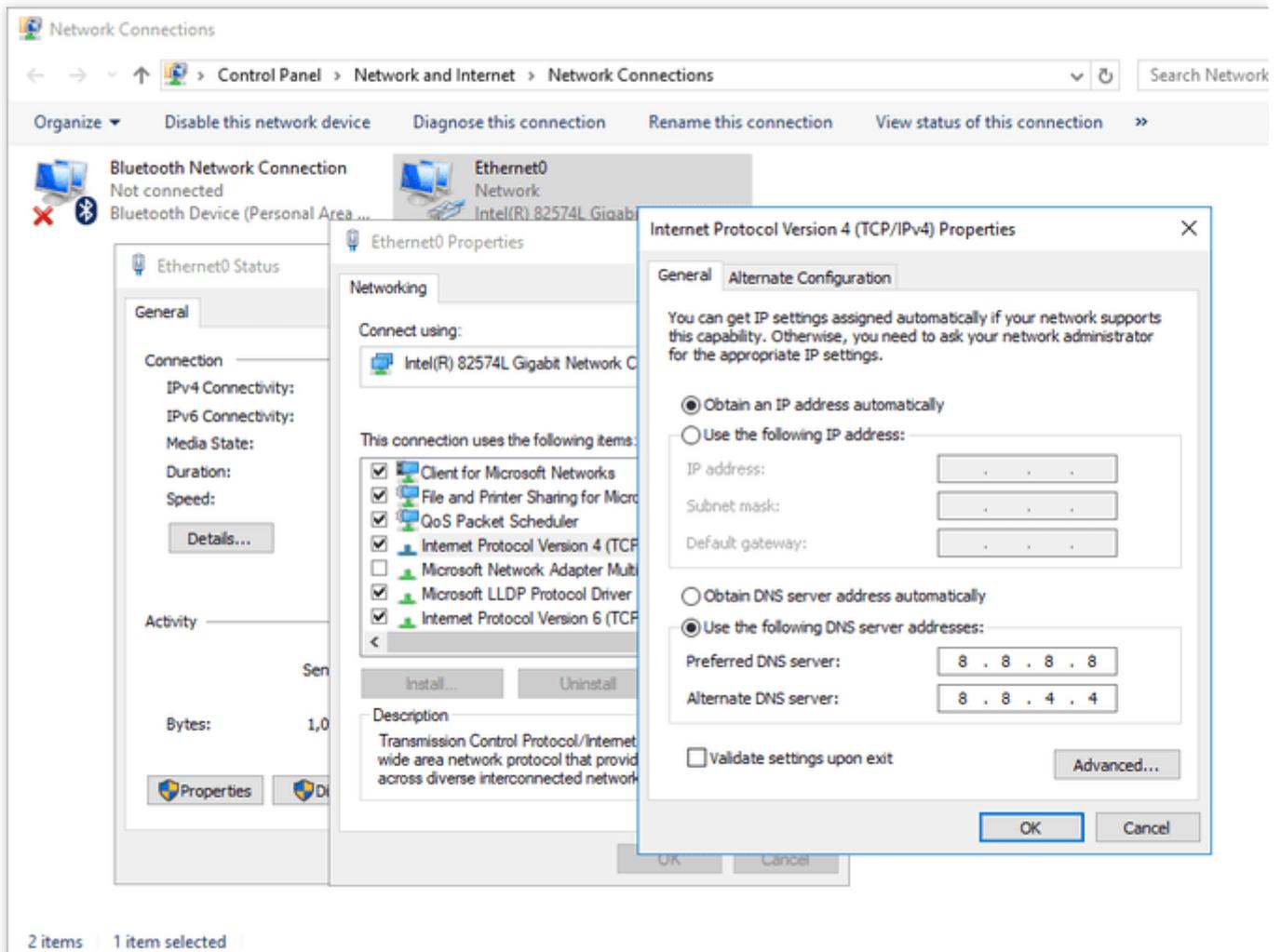
たとえば、プライベートネットワークDNS IPを北京リージョンのプライベートネットワークDNSサーバーに変更します。



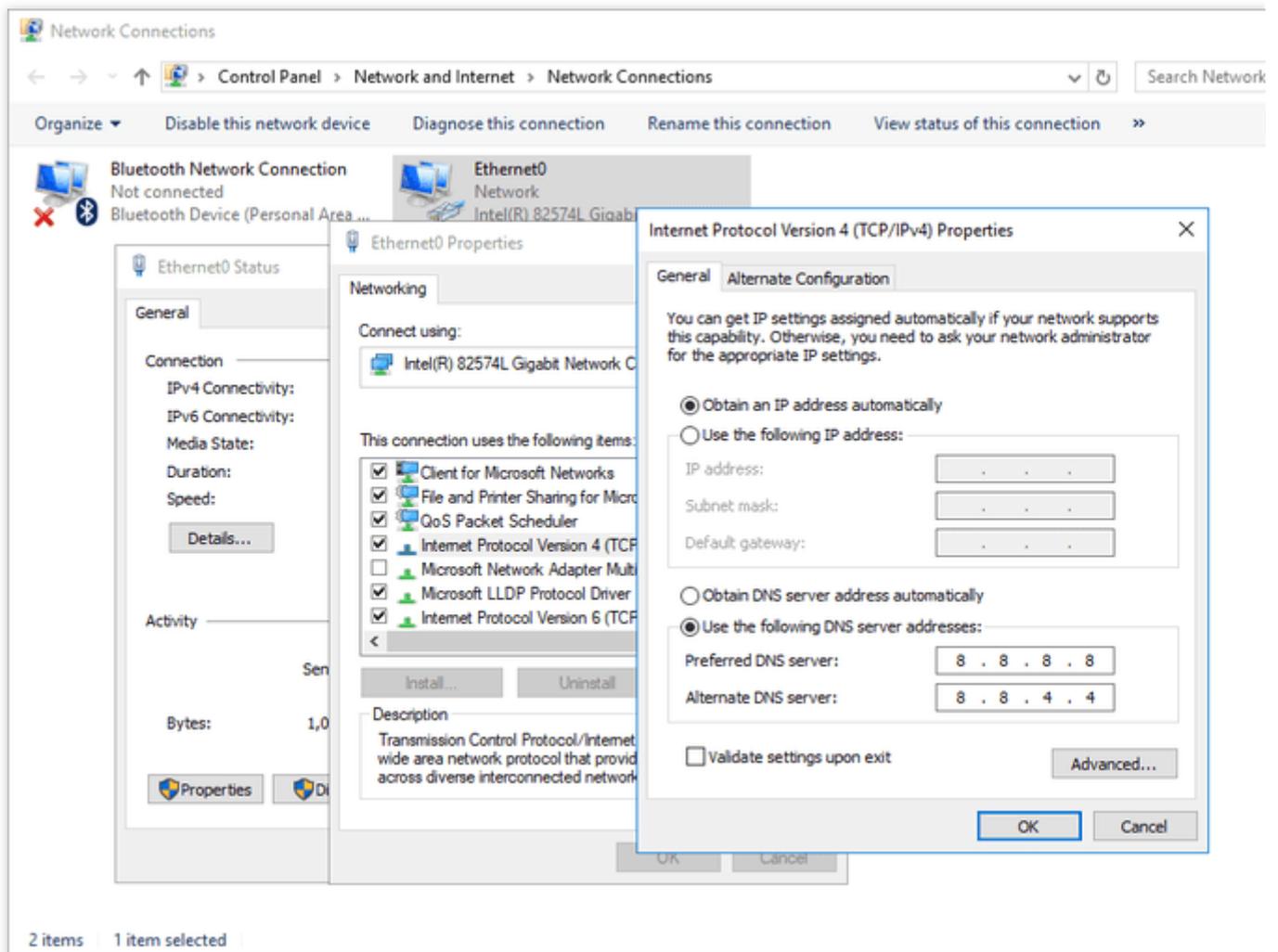
```
nameserver 10.53.216.182
nameserver 10.53.216.198
options timeout:1 rotate
```

4. **Esc**キーを押して、**:wq**を入力し、ファイルを保存して戻ります。

1. Windows CVMにログインします。
2. OSのインターフェースで、**コントロールパネル > ネットワークと共有センター > アダプターの設定の変更**を開きます。
3. **イーサネット**を右クリックして、**プロパティ**を選択し、「イーサネットのプロパティ」ウィンドウを開きます。
4. 下図のように、「イーサネットのプロパティ」ウィンドウで、**インターネットプロトコルバージョン4 (TCP/IPv4)** をダブルクリックして開きます。



5. 次の**DNSサーバーのアドレスを使う** にチェックをして、**プライベートネットワーク DNS** に対応するリージョンに従ってDNS IPを変更します。



6. **OK**をクリックします。

# プライベートIPアドレスの変更

最終更新日：：2024-07-05 16:57:38

## ユースケース

コンソールで、プライベート ネットワーク内のクラウド サーバー (クラウド仮想マシン、CVM) インスタンスのイントラネット IP を直接変更できます。このドキュメントでは、クラウド サーバー コンソールでプライベート ネットワーク内の CVM インスタンスのイントラネット IP を変更する方法を説明します。

## 制限条件

プライマリENIのプライマリIPを変更すると、関連するCVMが自動的に再起動されます。セカンダリENIのプライマリ IPは変更できません。

## 操作手順

1. [CVMコンソール](#) にログインします。
2. プライベートIPを変更するインスタンスのリージョンを選択し、インスタンスのID/名前をクリックして、インスタンスの詳細画面に入ります。
3. **ENI** タブを選択して、

 をクリックしてプライマリENIを展開します。

4. プライマリENIの操作列で、**プライマリIPの変更** をクリックします。
5. 「プライマリIPの変更」ダイアログボックスで、新しいIPアドレスを入力してから **【OK】** をクリックします。変更は、インスタンスの再起動後に有効になります。

### ご注意：

現在のサブネットCIDRに属するプライベートIPのみ入力できます。

# パブリックIPアドレスの取得

最終更新日：2023-03-03 15:01:54

## 概要

このドキュメントは、コンソール、API、およびインスタンスメタデータでパブリックIPアドレスを取得する方法について説明します。

## 操作手順

コンソールを利用した取得

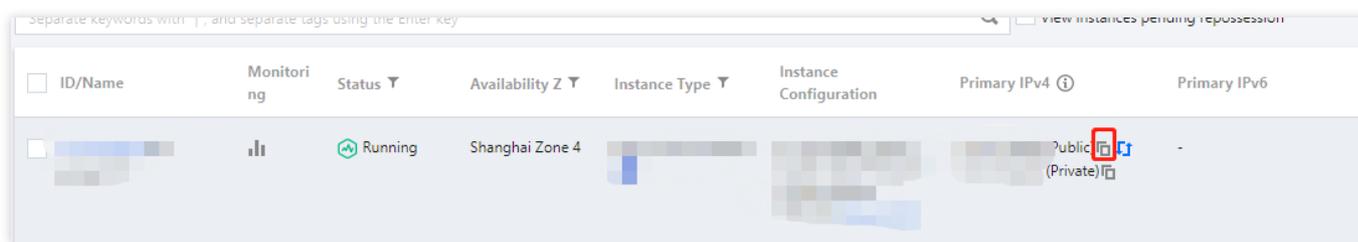
API を利用した取得

インスタンスメタデータを利用した取得

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画面で、実際に使用されているビューモードに従って操作します。

**リストビュー：**下図のように、マウスをプライマリ IPアドレス列に移動し、

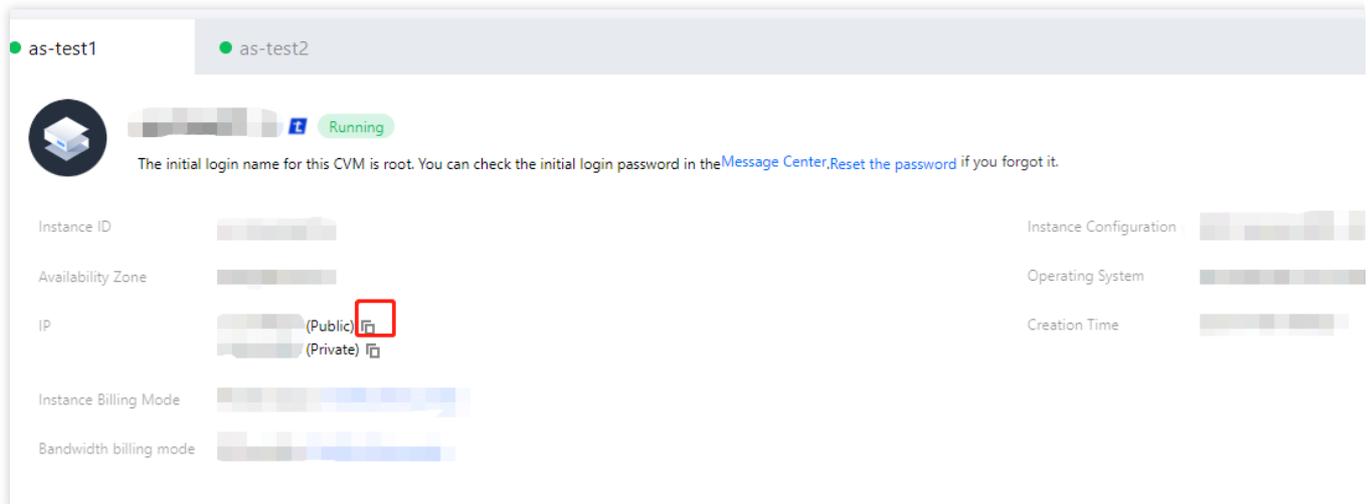
 をクリックすれば、このIPアドレスをコピーできます。



ID/Name	Monitoring	Status	Availability Z	Instance Type	Instance Configuration	Primary IPv4	Primary IPv6
[blurred]	[blurred]	Running	Shanghai Zone 4	[blurred]	[blurred]	[blurred] Public (Private)	-

**タブビュー：**下図のように、インスタンスページで、「IPアドレス」のパブリックネットワークアドレス後の

 をクリックすれば、パブリックIPをコピーできます。



### ご注意：

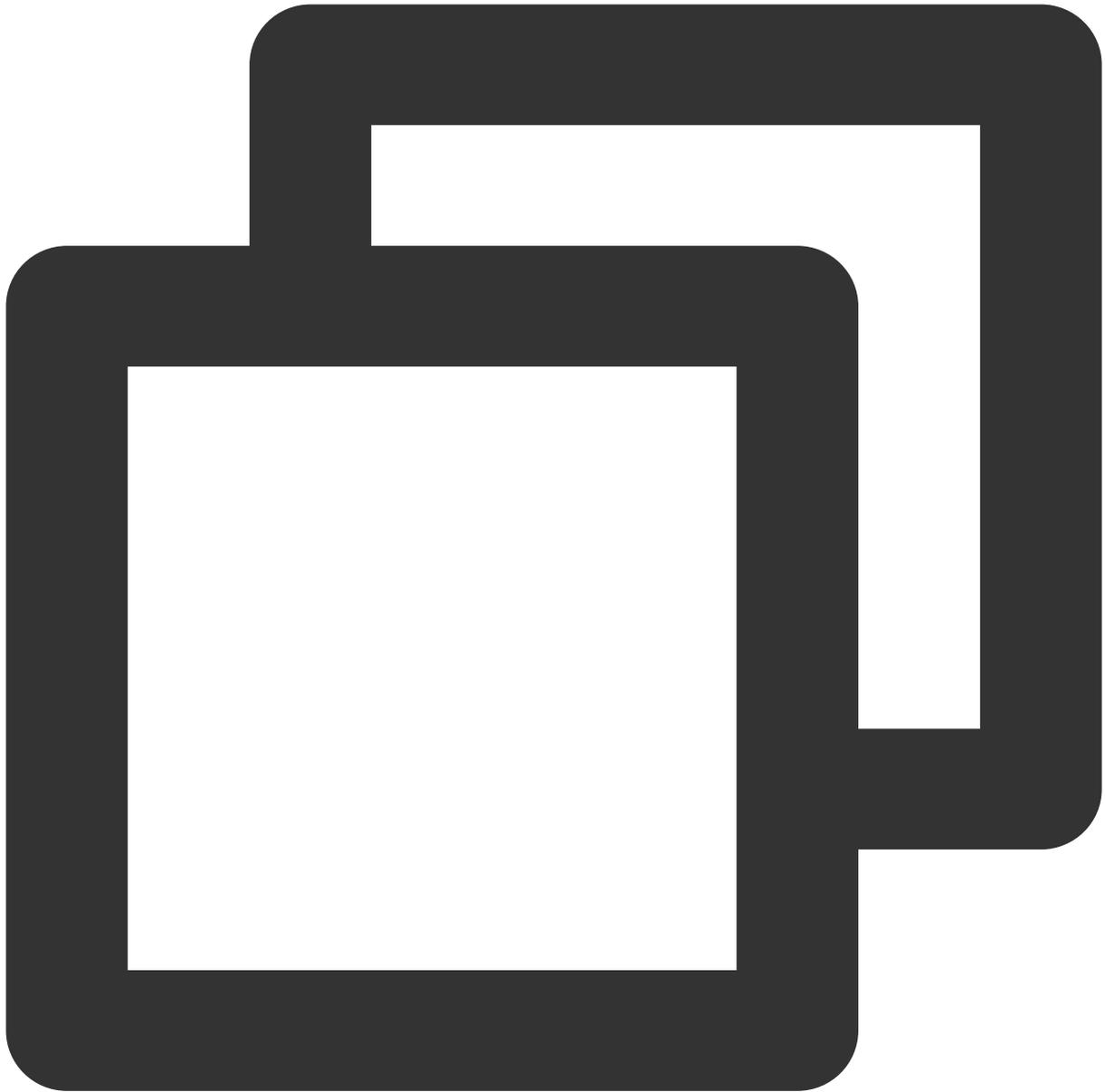
パブリックIPアドレスは、NATを介してプライベートIPアドレスにマッピングされるため、インスタンス内部でネットワークインターフェースのプロパティを（`ifconfig` (Linux) または `ipconfig` (Windows) コマンドを介して）確認しても、パブリックIPアドレスは表示されません。インスタンス内部からインスタンスのパブリックIPアドレスを確認したい場合は、[インスタンスメタデータを利用した取得](#)をご参照ください。

詳細については、[DescribeInstances](#) をご参照ください。

1. CVMインスタンスにログインします。

具体的なログイン方法については、標準ログイン方法を使用した [Linuxインスタンスへのログイン](#) および標準ログイン方法を使用した [Windowsインスタンスへのログイン](#) をご参照ください。

2. cURLツールまたはHTTPのGETリクエストを介してmetadataにアクセスし、パブリックIPアドレスを取得します。



```
curl http://metadata.tencentyun.com/meta-data/public-ipv4
```

戻り値に次のような構造がある場合は、パブリックIPアドレスを確認できます。

```
[root@UM_58_27_centos ~]# curl http://metadata.tencentyun.com/meta-data/public-ipv4  
115.██.77.82
```

詳細については、[インスタンスメタデータの確認](#)をご参照ください。

# パブリックIPアドレスの変更

最終更新日：：2023-03-03 15:12:56

## 概要

このドキュメントでは、CVMインスタンスのパブリックIPアドレスを変更する方法について説明します。

## 注意事項

各アカウントは、同じリージョンのCVMインスタンスのパブリックIPアドレスを1日に最大3回変更できます。

各インスタンスのパブリックIPは、**1回だけ変更できます**。

元のパブリックIPは、**変更後にリリースされます**。

## 前提条件

[CVMコンソール](#)にログインしました。

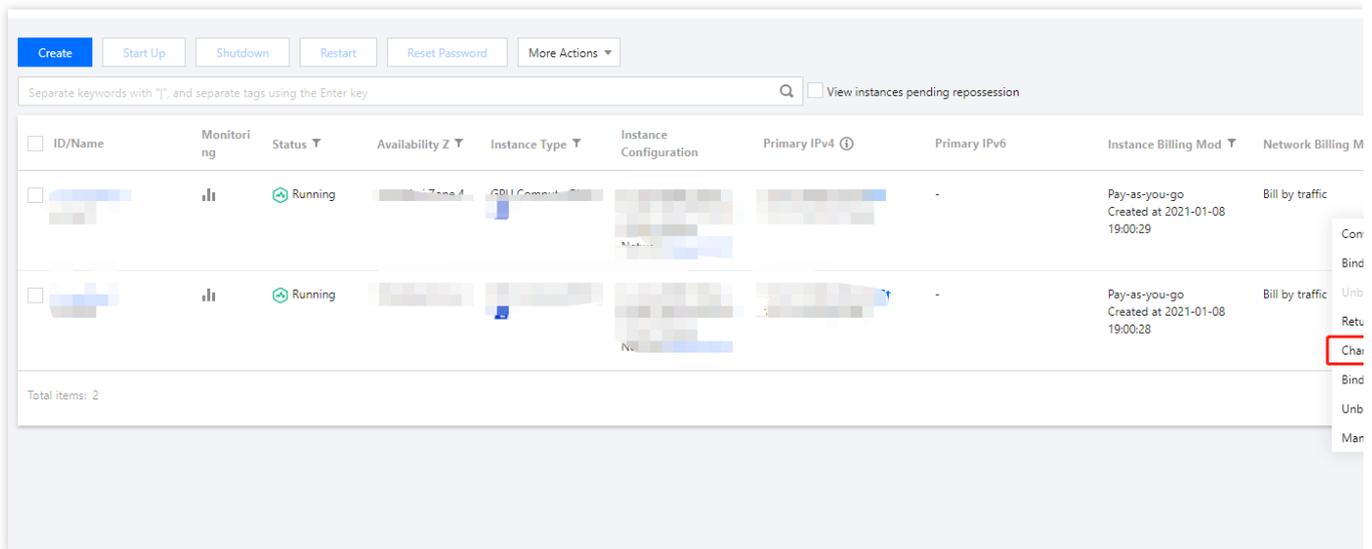
## 操作手順

インスタンスの管理画面で、実際に使用されているビューモードに従って操作します。

リストビュー

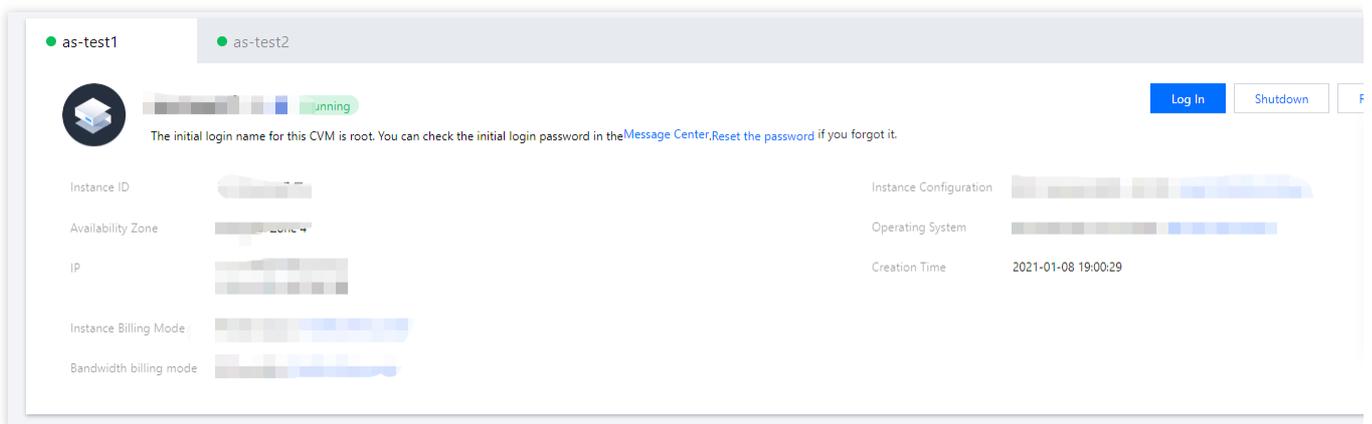
タブビュー

1. 下図のように、パブリックIPアドレスを変更するCVMインスタンスを選択し、さらに**> IP/ENI>パブリックIPを変更**を選択します。



2. 「IPの変更」ダイアログボックスで、**OK**をクリックして変更を完了します。

1. 下図のように、パブリックIPアドレスを変更するインスタンスの詳細ページに移動して、**その他の操作>IP/ENI>パブリックIPを変更**を選択します。



2. 「IPの変更」ダイアログボックスで、**OK**をクリックして変更を完了します。

# パブリックIPアドレスを取り戻す

最終更新日：：2023-03-03 15:17:29

## ユースケース

このドキュメントでは、使用したことがあって、まだ他のユーザーに割り当てられていないパブリックIPアドレスを取り戻す方法について説明します。

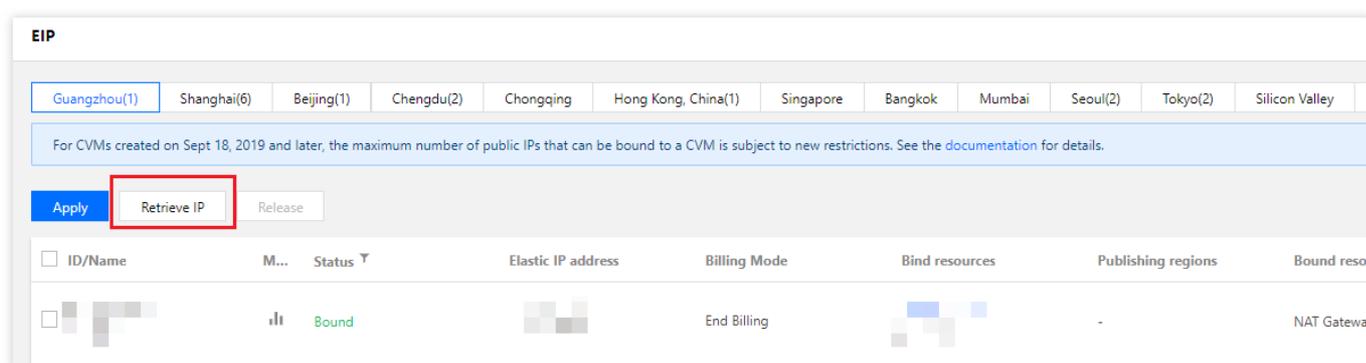
## 注意事項

取り戻したIPはEIPであり、EIPの合計数は製品のクォータの合計を超えてはいけません。

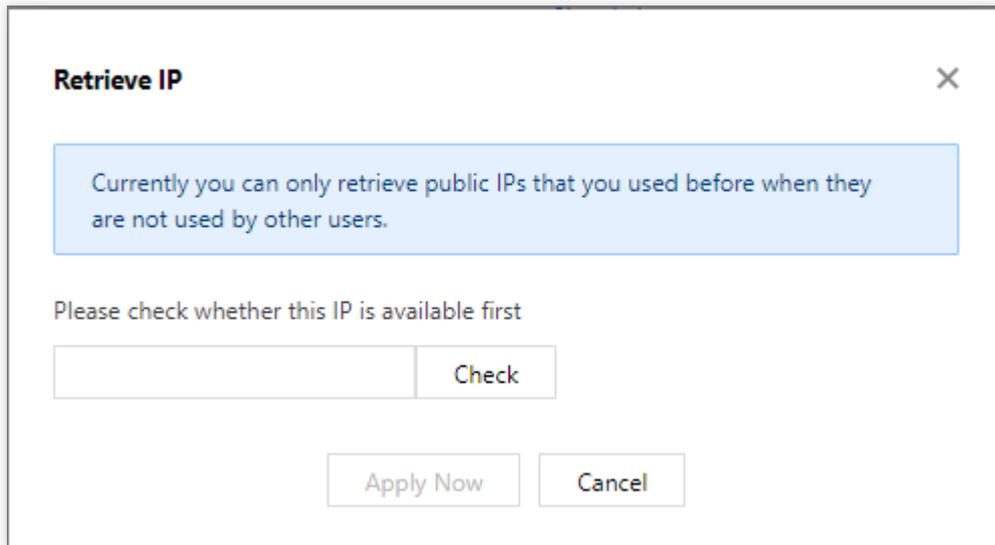
各アカウントは、各地域で1か月あたり最大3回まで特定のIPアドレスを申請できます。

## 操作手順

1. **CVMコンソール**にログインします。
2. 左側のナビゲーションメニューバーから **【Public IP】** タブをクリックし、「EIP」管理ページに入ります。
3. **【Retrieve IP】** をクリックします。下図に示すように：



4. 「Retrieve IP」ダイアログボックスで、パブリックIPアドレスを入力し、**【Query】** をクリックし、IPを取り戻すことを申請できるかどうかを確認します。下図に示すように：



**Retrieve IP** ✕

Currently you can only retrieve public IPs that you used before when they are not used by other users.

Please check whether this IP is available first

はいの場合、【Apply Now】をクリックします。

いいえの場合、申請したIPアドレスがすでに使用されていることを意味し、取り戻すことができません。この場合、別のIPアドレスを申請するか、【Cancel】をクリックして画面を閉じます。

# セキュリティグループの変更

最終更新日：：2023-04-10 15:32:09

## 概要

セキュリティグループは、インスタンスの仮想ファイアウォールとして機能し、1つまたは複数のCVMのネットワークアクセス制御を設定するために使用され、Tencent Cloudが提供する重要なネットワークセキュリティ分離方法です。CVMインスタンスを作成する際に、そのインスタンスのセキュリティグループを設定する必要があります。Tencent CloudはユーザーがCVMインスタンスを作成した後にインスタンスが属するセキュリティグループを変更することをサポートしています。

### ご注意：

インスタンスを新しいセキュリティグループに設定したい場合は、先にセキュリティグループを新規作成してください。具体的な操作については、[セキュリティグループの作成](#)をご参照ください。

## 前提条件

[CVMコンソール](#)にログインしました。

## 操作手順

### 設定されたセキュリティグループの変更

インスタンス管理ページで、実際に使用されているビューモードに従って操作します。

リストモード

タブモード

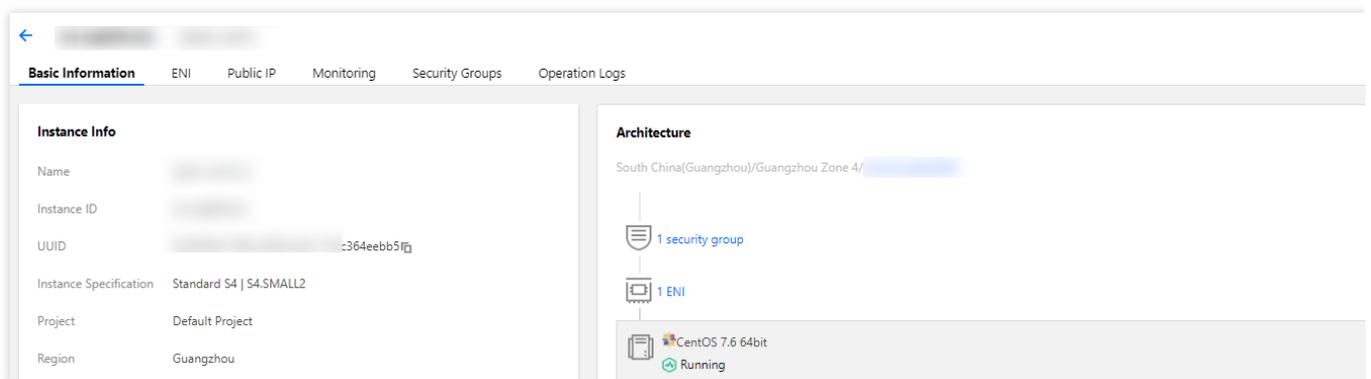
1. 下図に示すように、インスタンスの管理ページで、新しいセキュリティグループを設定する必要があるCVMインスタンスを選択し、さらに>セキュリティグループ>セキュリティグループの設定をクリックします。

ID/Name	Monitoring	Status	Availability Zone	Instance Type	Instance Configuration	Primary IPv4	Primary IPv6	Instance Billing Mode	Network bill
[blurred]	[icon]	Running	Guangzhou Zone 4	Standard S4	1-core 2GB 1Mbps System disk: Premium Cloud Storage Network: Lab1-VPC01	[blurred]	-	Pay as you go Created at 2020-05-09 09:56:13	Bandwidth P
[blurred]	[icon]	Running	Guangzhou Zone 4	Standard S2	1-core 1GB 1Mbps System disk: Premium Cloud Storage Network: Lab1-VPC01	[blurred]	-	Pay as you go Created at 2020-05-09 09:14:39	Bandwidth P
[blurred]	[icon]	Running	Guangzhou Zone 4	Standard S2	1-core 1GB 1Mbps System disk: Premium Cloud Storage	[blurred]	-	Pay as you go Created at 2020-05-09 09:14:06	Bandwidth P

2. ポップアップウィンドウで、新しいセキュリティグループ名にチェックを入れ（複数選択可）、**Confirm**をクリックするとセキュリティグループを変更することができます。

1. インスタンスの管理ページで、新しいセキュリティグループを設定する必要があるCVMインスタンスのタブを選択します。

2. 下図に示すように、インスタンス詳細ページで、右上の**その他の操作 > セキュリティグループ > セキュリティグループの設定**を選択します。

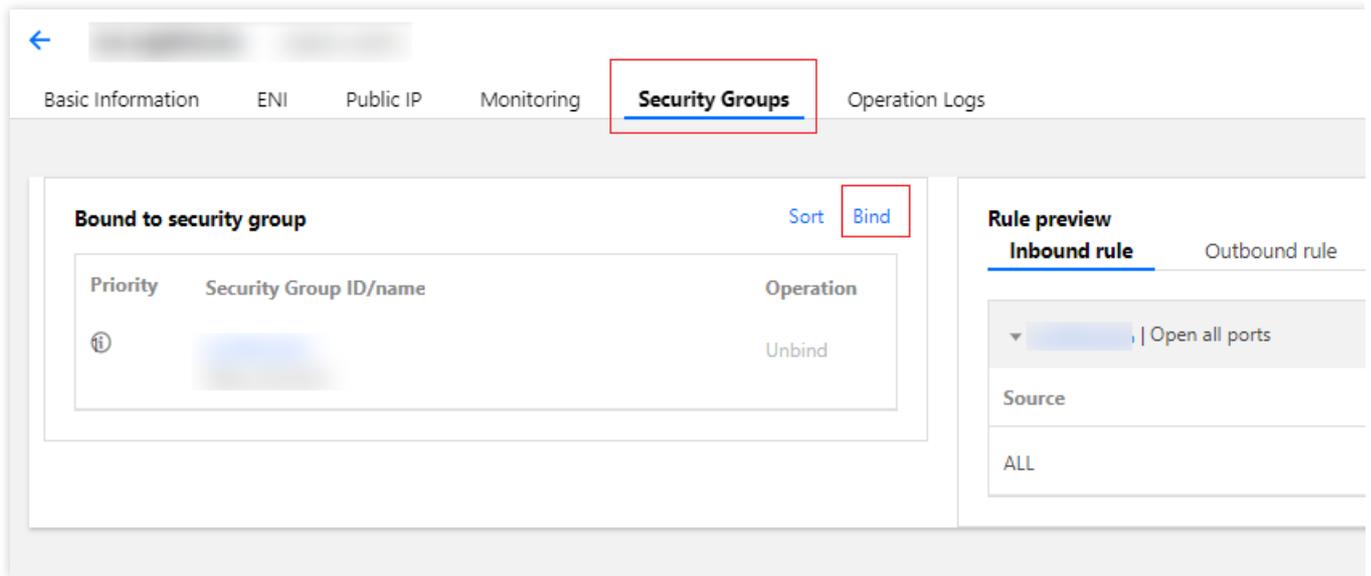


3. ポップアップウィンドウで、新しいセキュリティグループ名にチェックを入れ（複数選択可）、**Confirm**をクリックします。

## インスタンスに関連付けられたセキュリティグループの変更

1. インスタンスの管理ページで、セキュリティグループに関連付ける必要があるCVMインスタンスID/名前をクリックし、このインスタンスの詳細ページに進みます。

2. 下図に示すように、インスタンス詳細ページで、**セキュリティグループ**タブを選択し、「Bound security groups」欄で**Bind**をクリックします。



3. 下図に示すように、ポップアップウィンドウで、実際のニーズに基づいて関連付けるセキュリティグループにチェックを入れ、OKをクリックしてセキュリティグループとの関連付け操作を完了します。

### Security Groups

Projects All projects ▾

Select a security group

Enter the security group name or ID Q

<input type="checkbox"/>	ID/Name	Notes
<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		

Selected (4)

	ID/Name	Notes	
⇅			✕
⇅			✕
⇅			✕
⇅			✕

OK Cancel

# 従量課金インスタンスの年額・月額課金への変換

最終更新日：2024-03-14 14:43:59

## 操作ケース

Cloud Virtual Machine (CVM) をより便利にご利用いただくために、Tencent Cloud では、CVM の従量課金インスタンスを年額・月額課金インスタンスに変換する機能を開放しており、一時的に使用される従量課金インスタンスを長期的かつ安定的にご利用いただける年額・月額課金インスタンスに変換します。変換操作は、CVM のコンソールと TencentCloud API で行うことができます。このドキュメントでは、CVM のコンソールで従量課金インスタンスを年額・月額課金インスタンスに変換する機能の操作について説明します。

## 変換ルール

CVM のコンソールでは、課金方式の変換機能を提供しています。具体的なルールは以下のとおりです。

従量課金インスタンスを個々・一括に年額・月額課金インスタンスに変換することができます。

従量課金インスタンスを年額・月額課金インスタンスに変換する際に、リニューアルオーダーが発生します。課金方式の変換を有効にするには、このオーダーの支払いプロセスを完了する必要があります。

支払いが行われなかった場合、または支払いが失敗した場合は、お客様の [オーダーセンター](#) ページでオーダーを確認して処理することができます。

課金方式を従量課金から年額・月額課金に変換する CVM は、5 日以内の理由なしの払い戻しをサポートしません。

課金方式の変換と支払いが成功すると、インスタンスは直ちに年額・月額で課金されます。新しい年額・月額課金インスタンスの開始時刻は、変換が成功した時刻とします。

支払いが成功するまで、このインスタンスに対して課金方式の変換を繰り返して実行することはできません。

支払いが成功するまでに、インスタンスの設定情報が変更され（設定の調整/システムの再インストール/帯域幅の調整/ディスクの調整など）、新しいオーダーの金額とインスタンスが一致せず、未払いオーダーの支払いが禁止される場合は、まず [オーダーセンター](#) で現在の未払いオーダーをキャンセルしてから、新しい変換操作を実行する必要があります。

従量課金から年額・月額課金への変換機能は、インスタンスとディスクを同期的に変換する課金方式をサポートしています。インスタンス課金方式の変換後、標準アカウントタイプ (bill-by-IP) の通常のパブリックネットワーク IP の時間帯域幅の課金方式と、従来のアカウントタイプ (bill-by-CVM) の時間帯域幅の課金方式は、年額・月額の帯域幅課金方式の自動変換をサポートしており、それ以外のネットワーク帯域幅課金方式は変更されません。

## 使用制限

使用可能なゾーンの年額・月額課金の残りのクォータが、変換する従量課金インスタンス数より少ない場合は、変換をサポートしません。

従量課金インスタンス以外のインスタンスは、変換をサポートしません。

ビッドインスタンスは、変換をサポートしません。

インスタンスネットワークの課金方式が帯域幅の使用時間に基づくため、現在、変換をサポートしません。

クラウドマーケットイメージを使うインスタンスは、変換をサポートしません。

バッチ型インスタンス BC1、BS1 は、変換をサポートしません。

従量課金インスタンスに未完了の変換オーダーがある場合は、変換をサポートしません。

従量課金インスタンスに定時破棄が設定された場合は、変換をサポートしません。変換が必要な場合は、定時破棄をキャンセルしてから、再度変換してください。

## 操作手順

1. [Cloud Virtual Machine コンソール](#) にログインします。

2. 実際のニーズに応じて、インスタンス管理ページで、異なるインスタンス変換操作を選択します。

個々のインスタンスの変換

複数のインスタンスの変換

インスタンス管理ページで、実際に使用するビュー方式に応じて操作します。

**リストビュー**：右側の操作バーで、**その他 > インスタンス設定 > 従量課金から年額・月額課金への変換**を選択します。下図のとおりです。

**説明**：

また、変換するインスタンスにチェックを入れ、上部にある**その他の操作 > インスタンス設定 > 従量課金から年額・月額課金への変換**を選択することができます。

ID/Name	Monitoring	Status	Availability	Instance type	Instance configuration	Primary IPv4	Primary IPv6	Instance billing mode	Network billing
<input type="checkbox"/> ins-k3fb1gme gardennchen_test_allinone			Guangzhou Zone 6	Standard S6	2-core 2GB 5Mbps System disk:Balanced SSD Network:Default-VPC	139.199.178.169 (Public) 172.16.49.107 (Private)	-	Pay-as-you-go Created at 2023-10-19 10:44:47	Bill by traffic
<input type="checkbox"/> ins-e6vvka4g test_languange__1			Guangzhou Zone 6	Standard S6	2-core 4GB 5Mbps System disk:Balanced SSD Network:Default-VPC	43.138.202.25 (Public) 172.16.48.11 (Private)	-		
<input type="checkbox"/> ins-0dmgspc4 diluzhang			Guangzhou Zone 3	Standard S5	2-core 4GB 0Mbps System disk:Balanced SSD Network:Default-VPC	172.16.16.13 (Private)	-		
<input type="checkbox"/> ins-lhqgt4ro echochang在测试			Guangzhou Zone 3	Standard SA2	2-core 4GB 5Mbps System disk:Balanced SSD Network:Default-VPC	1.12.60.154 (Public) 172.16.16.17 (Private)	-		

- Rename
- Instance termination protection
- Export instances
- Edit tags
- Bind/modify role
- Assign to project
- Switch from Pay-as-you-go to Monthly Subscription**
- Manage instance placement group
- Migrate to CDH

タブビュー：インスタンスページで、右上にある**その他の操作 > インスタンス設定 > 従量課金から年額・月額課金への変換**を選択します。下図のとおりです。

The initial login name is root. If you select "Random password" when purchasing the instance, check the password in [Message Center](#). You can [reset the password](#) if you forget it.

Running
Log in
Shutdown
Restart
Reset password
Terminate/Return
More actions

**Basic information**
ENI
Public IP
Monitoring
Security groups
Operation logs
Run commands

**Instance information**

Name:  

Instance ID:  

UUID:  

Instance specification: Standard S6 | S6.MEDIUM2

Instance termination protection: Disabled

Project: Default Project

Tags: None

Key:  

Placement group: None

Region: Guangzhou

1 security group

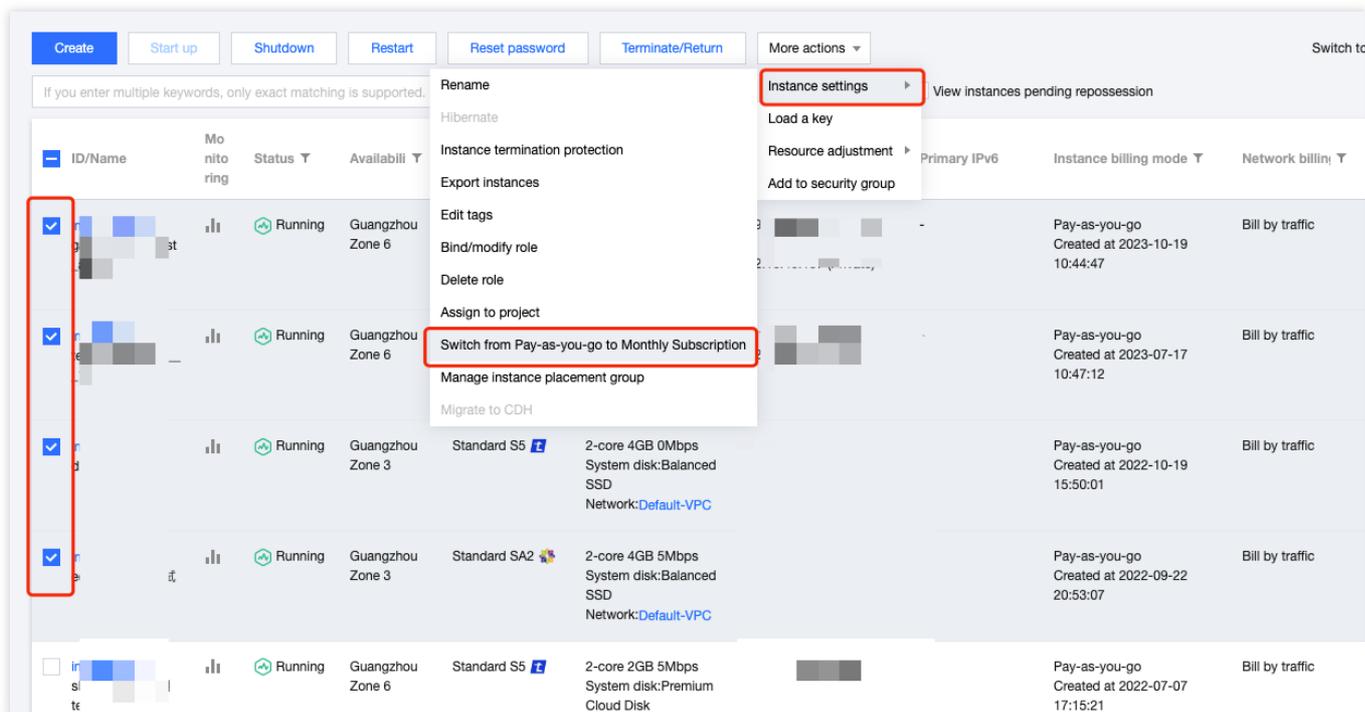
1 ENI

jadhewzg

- Rename
- Instance termination protection
- Export instances
- Edit tags
- Bind/modify role
- Assign to project
- Switch from Pay-as-you-go to Monthly Subscription**
- Manage instance placement group
- Migrate to CDH

変換するすべてのインスタンスにチェックを入れ、上部にあるの**その他の操作 > インスタンス設定 > 従量課金から年額・月額課金への変換**をクリックします。そうすると、インスタンスの課金方式を一括に変換することができます。下図のとおりです。

操作できないインスタンスには理由が表示されます。



3. ポップアップ表示される**従量課金から年額・月額課金への変換ウィンドウ**で、実際のニーズに応じてリニューアル時間及び自動リニューアルの可否を設定します。下図のとおりです。

## Switch to Monthly Subscription

You've selected 1 instance. [Collapse](#)

ID/Name	Instance type	Instance configuration	New expiry time	Disc
	Standard S6	2-core 2GB 5Mbps System disk:Balanced SSD Network:vpc-9679ku27	202	

When you switch from Pay-as-you-go to Monthly Subscription, both the billing mode of instance and disk will be changed. For bandwidth billing details, see [Switching Rules](#).  
The displayed discount is the highest discount for all instances.

Renewal period \*  1  2  3  1 year  2 years  3 years  4 years  5 years

Auto-renewal  Auto-renew the device every month when my account has sufficient balance

Storage  Switch to Monthly Subscription as well

Fee

I have read and agreed to [Rules on Switching from Pay-as-you-go to Monthly Subscription](#).

Change now

Close

リニューアル時間：年額・月額課金に変換した後の購入時間を選択します。複数インスタンスの一括変換の場合は、同じ購入時間しか設定できません。

自動リニューアル：ニーズに応じて自動リニューアルを選択します。

4. 従量課金から年額・月額課金への変換に関するルールを読み、同意するチェックボックスにチェックを入れて、**今すぐ変換**をクリックします。このインスタンスに未完了の変換オーダーがない場合は、自動的に支払いページにジャンプします。

5. ページの指示に従って支払いを完了すると、変換操作は完了します。

## よくある質問

変換処理中に問題が発生した場合は、[よくある質問](#) > [課金関連](#) ドキュメントを参照してください。

# インスタンスの検索

最終更新日：2023-03-03 15:57:20

## シナリオ

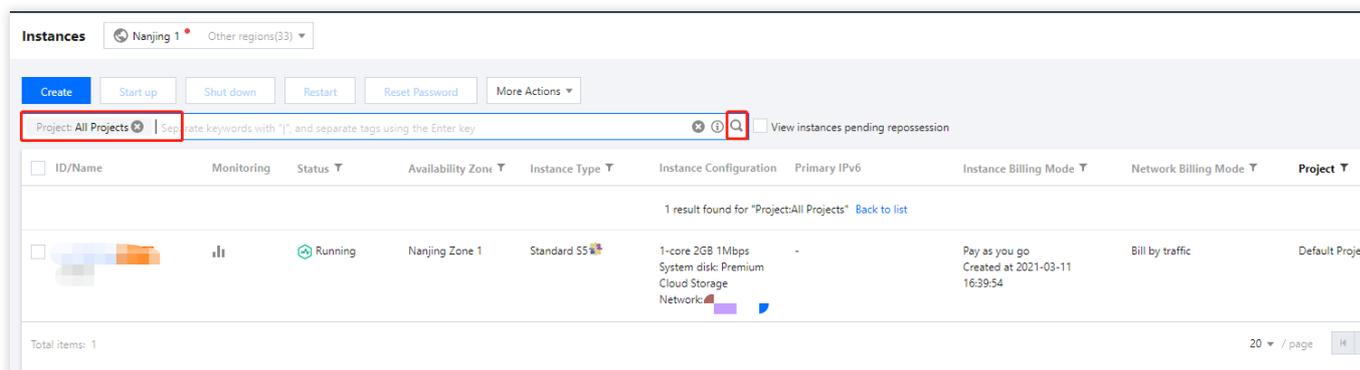
デフォルトでは、CVMコンソールは現在のリージョン内のすべてのプロジェクトのインスタンスを表示します。現在のリージョンでインスタンスをすばやく検索できるように、Tencent CloudはCVM検索機能を提供します。現在、所属するプロジェクト、インスタンスの課金方法、インスタンスタイプ、アベイラビリティゾーン、IP、インスタンスID、インスタンス名などのリソース属性によってインスタンスをフィルタリングすることが可能です。

## 操作手順

1. [CVMコンソール](#) にログインします。
2. 必要に応じて、検索ボックスに検索したいキーワードとなる言葉を入力します。

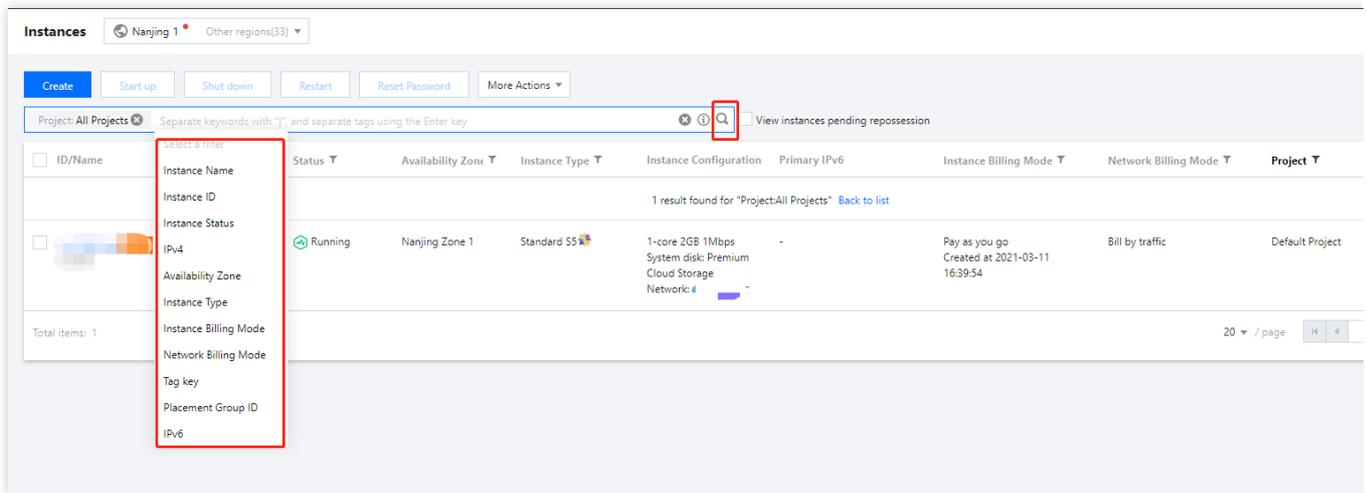
 をクリックして検索します。  
キーワードを入力し、

 をクリックします。下図の通りです。



検索するリソースディメンション（所属するプロジェクト、インスタンスの課金方法、インスタンスタイプなど）を選択し、

をクリックします。下図の通りです。



3. 検索構文の詳細については、

をクリックしてインスタンスを検索するための構文を確認することができます。インスタンスを検索するための構文の詳細については、次の図をご参照ください。

	Enter Format	Example	Display in Search Box	Description
Single key-word	[Keyword]	10.0.0.1	10.0.0.1 Use ' ' to split more than one keyword	List all instances including the keyword "10.0
Multiple key-words	[Keyword] [Enter key ↵] [Keyword]	10.0.0.1 www.123.com 192.169.23.54	10.0.0.1   www.123.com   192.169.23.45	List all instances that include all the three keywords "10.0.0.1", "www.123.com" and "192.169
Single re-source type	[Resource type]: [Keyword]	IP: 10.0.0.1	IP: 10.0.0.1 Use ' ' to split more than one key	List all instances whose IP is "10.0.0.1"
Multiple re-source types	[Resource type]: [Keyword] [Enter key ↵] [Resource type]: [Keyword]	Availability Zone: Hong Kong Zone 2 Project: Default	Availability Zone: Hongkon...   Project: Defau	List all instances whose "Availability Zone" is "Kong Zone 2" and "Project" is "Default"
Single re-source type and multiple keywords	[Resource type]: [Keyword]   [Keyword]	CVM Status: Creating   Shutdown	CVM Status: Creating   Shu... Use ' ' to split	List all instances whose "CVM Status" is "Cre or "Shutdown"
Pasted contents	{pasted contents}	112.11.22.33 112.11.22.34 112.11.22.53	112.11.22.33   112.11.22.3... Use ' ' to split	List all instances include the keywords "112.11.22.33", "112.11.22.34" or "112.11.22.!

# インスタンスリストのエクスポート

最終更新日：：2023-03-03 16:06:37

## 概要

コンソールでリージョンのCVMインスタンスリストをエクスポートでき、エクスポートするリストフィールドもカスタマイズできます。最大27のフィールドを選択できます。現在エクスポートできるフィールドは：ID、インスタンス名、状態、リージョン、アベイラビリティゾーン、インスタンスタイプ、OS、イメージID、CPU、メモリ、帯域幅、パブリックネットワークIP、プライベートネットワークIP、システムディスクの種類、システムディスクサイズ、データディスクの種類、データディスクサイズ、所属ネットワーク、所在サブネット、関連VPC、作成時間、有効期限、インスタンスの課金方法、プロジェクト、専用ホストID、およびタグを含みます。

## 操作手順

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上部で、リージョンを選択し、実際に使用するビューモードに従って操作します。

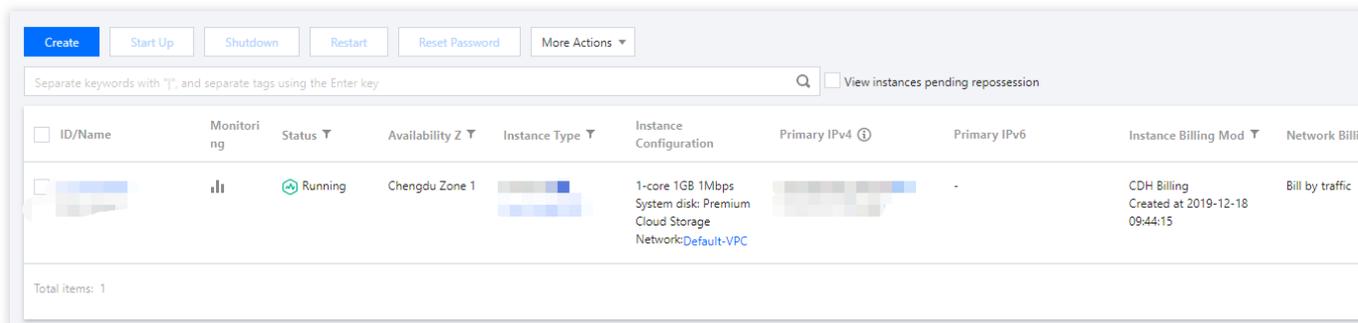
リストビュー

タブビュー

下図のように、インスタンスリストの右上隅にある



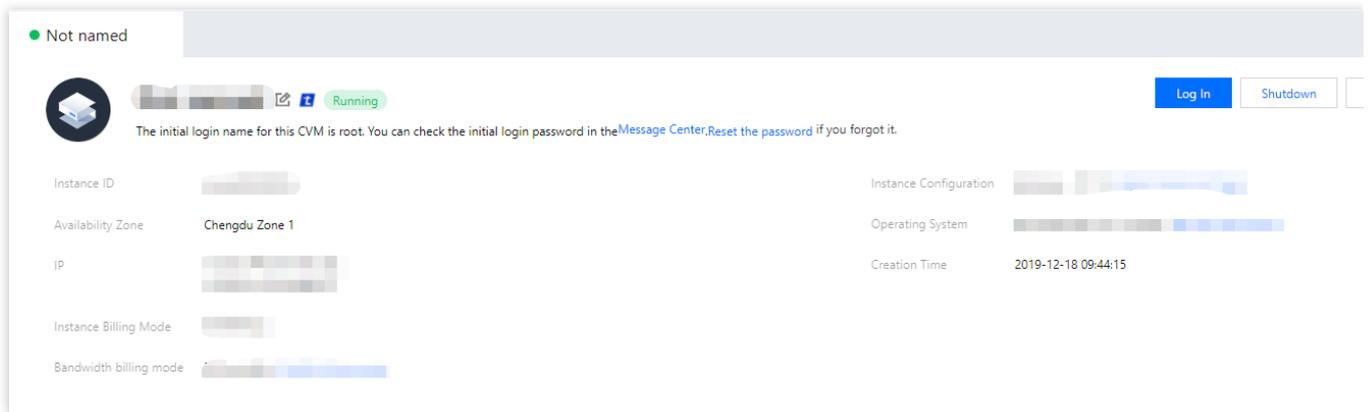
をクリックします。



下図のように、インスタンスページ右上部の



をクリックします。



3. 下図のように、表示された「インスタンスをエクスポート」ウィンドウで、エクスポートするフィールドを選択し、「OK」をクリックします。

### Export instances ✕

Select All

<input type="checkbox"/> ID	<input checked="" type="checkbox"/> Bandwidth (Mbps)
<input type="checkbox"/> Instance Name	<input checked="" type="checkbox"/> Primary public IPv4
<input checked="" type="checkbox"/> Status	<input checked="" type="checkbox"/> Primary private IPv4
<input checked="" type="checkbox"/> Region	<input checked="" type="checkbox"/> Primary IPv6
<input checked="" type="checkbox"/> Availability Zone	<input checked="" type="checkbox"/> System Disk Type
<input checked="" type="checkbox"/> Instance Type	<input checked="" type="checkbox"/> System disk size (GB)
<input checked="" type="checkbox"/> CPU (core)	<input checked="" type="checkbox"/> Data Disk Type
<input checked="" type="checkbox"/> MEM (GB)	<input checked="" type="checkbox"/> Data disk size (GB)
<input checked="" type="checkbox"/> Operating System	<input checked="" type="checkbox"/> Network type
<input checked="" type="checkbox"/> Image ID	<input checked="" type="checkbox"/> VpcId
<input checked="" type="checkbox"/> VPC name	
<input checked="" type="checkbox"/> Subnet ID	
<input checked="" type="checkbox"/> Subnet name	
<input checked="" type="checkbox"/> Creation Time	
<input checked="" type="checkbox"/> Expiry Time	
<input checked="" type="checkbox"/> Instance Billing Mode	
<input checked="" type="checkbox"/> Network billing mode	
<input checked="" type="checkbox"/> Project	
<input checked="" type="checkbox"/> Dedicated Host ID	
<input checked="" type="checkbox"/> Tag	

Export range  All Instance  
 Only export search result  
 Selected Instance

# インスタンスの起動

最終更新日：2023-04-10 18:46:16

## 概要

本テキストではCVMコンソールおよびTencent Cloud APIを介してシャットダウン状態のインスタンスを起動する方法について説明します。

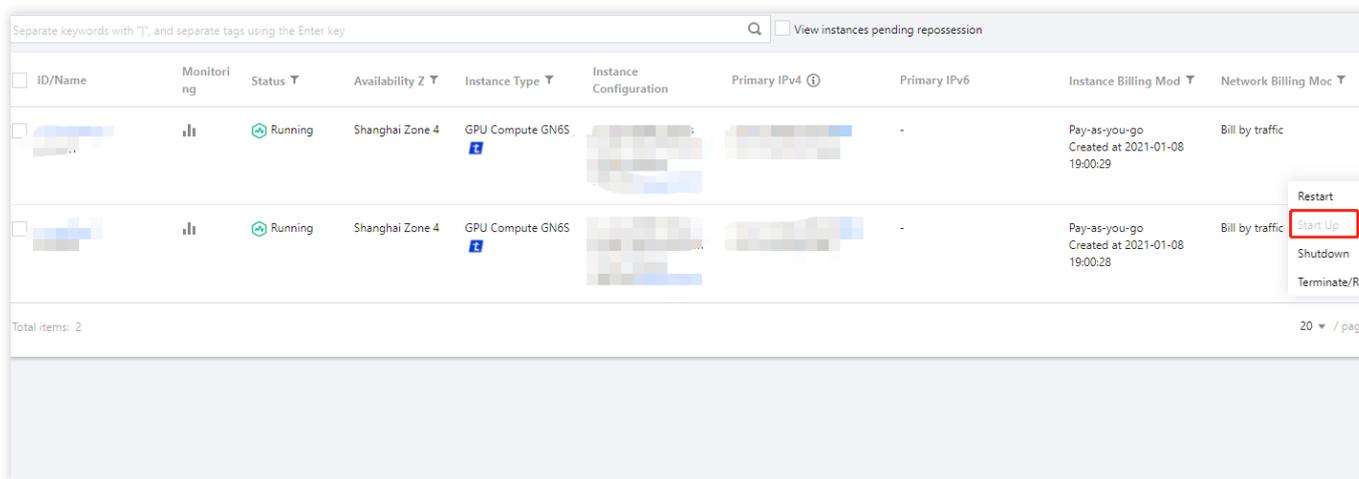
## 操作手順

コンソールを介したインスタンスの起動

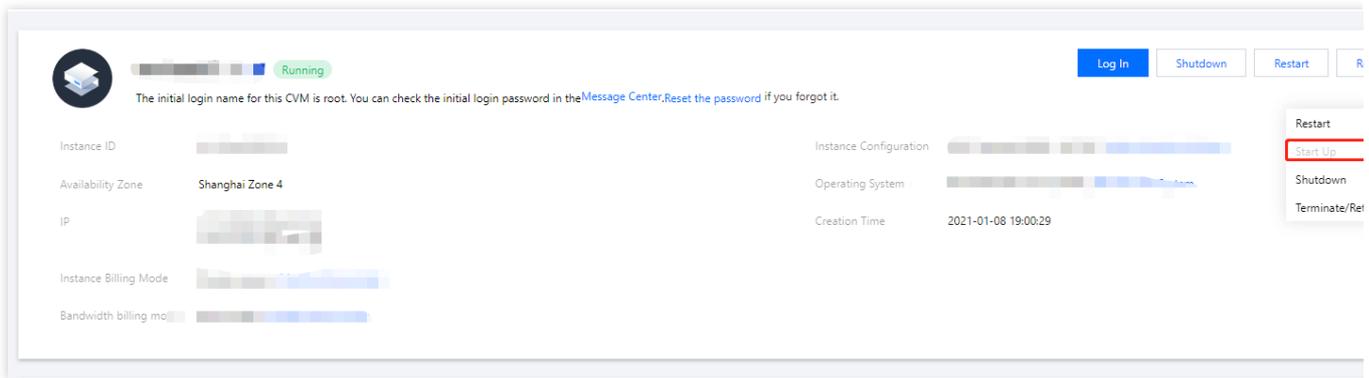
API を介したインスタンスの起動

### 単一インスタンスの起動

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画面で、実際に使用されているビューモードに従って操作します。  
リストビュー：下図のように、起動したいインスタンスを選択し、画面右のメニューからさらに **> インスタンス状態 > 起動** を選択します。

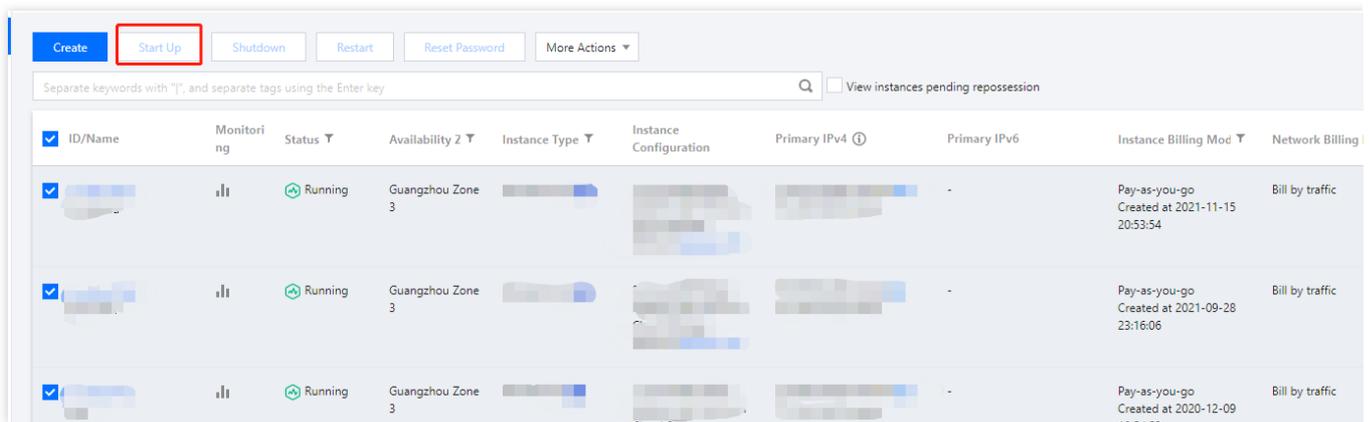


タブビュー：下図のように、起動したいインスタンスページで、右上コーナーの**起動**を選択します。



## 複数インスタンスの起動

下図のように、すべての起動したいインスタンスにチェックを入れ、リスト上部で、**起動**をクリックすれば、インスタンスを一括起動できます。



[StartInstances](#) インターフェースをご参照ください。

## 後続の操作

インスタンスが起動状態である場合のみ、次の操作を実行できます。

**インスタンスにログイン**：インスタンスのOSに基づき、[Linuxインスタンスにログイン](#) または [Windowsインスタンスにログイン](#) します。

**Cloud Block Storage (CBS) の初期化**：マウントされたCBSのフォーマット、パーティションおよびファイルシステムの作成などの初期化操作を実行します。

# インスタンスのシャットダウン

最終更新日：2023-04-12 10:53:05

## 概要

ユーザーはインスタンスサービスを停止する必要がある場合、または構成を変更するためにシャットダウンを実行する必要がある場合、インスタンスをシャットダウンできます。インスタンスをシャットダウンすることはローカルコンピューターのシャットダウンに相当します。

## 注意事項

システムコマンド (Windows OSおよび Linux OSでのshutdownコマンド) または Tencent Cloud コンソールを使用して、インスタンスをシャットダウンできます。コンソールでシャットダウンプロセスを表示して、問題が発生しているかどうかを確認することをお勧めします。

シャットダウン後、インスタンスはサービスを提供しなくなります。シャットダウンする前に、CVMがサービス要求の受信を停止していることを確認してください。

インスタンスを通常シャットダウンする場合、状態は先に「シャットダウン中」に変更し、シャットダウン後「シャットダウン済み」に変更します。シャットダウンプロセスに時間がかかりすぎる場合は、例外が発生する可能性があります。詳細については、[システムのシャットダウン](#) を参照し、強制シャットダウンを回避します。

インスタンスをシャットダウンした後、すべてのストレージは引き続きインスタンスに接続され、すべてのディスクデータは保持されますが、メモリ内のデータは失われます。

インスタンスをシャットダウンしても、その物理属性は変更されません。インスタンスのパブリックIPとプライベートIPも変更されません。[Elastic IP](#) とインスタンスの間の関連付けが維持されます。ただし、サービスの中断により、これらのIPにアクセスするとエラー応答が返されます。[Classiclink](#) の関係は変更されません。

シャットダウンするインスタンスが [CLBインスタンスのバックエンドサーバークラスター](#) に該当する場合は、シャットダウン後にサービスの提供を継続できません。

ヘルスチェックポリシーが設定されている場合、シャットダウンされたインスタンスは自動的にブロックされ、リクエストは転送されなくなります。ヘルスチェックポリシーが設定されていない場合、クライアントに502エラーが返される場合があります。詳細については、[ヘルスチェックのトラブルシューティング](#) をご参照ください。

シャットダウンされたインスタンスが [Auto Scalingグループ](#) にある場合は、Auto Scaling サービスはシャットダウンされたインスタンスを動作不良としてマークし、Auto Scaling グループから移動させ、代替インスタンスを起動することがあります。さらに詳細な情報については、[Auto Scaling](#) をご参照ください。

## 操作手順

コンソールを介したインスタンスのシャットダウン

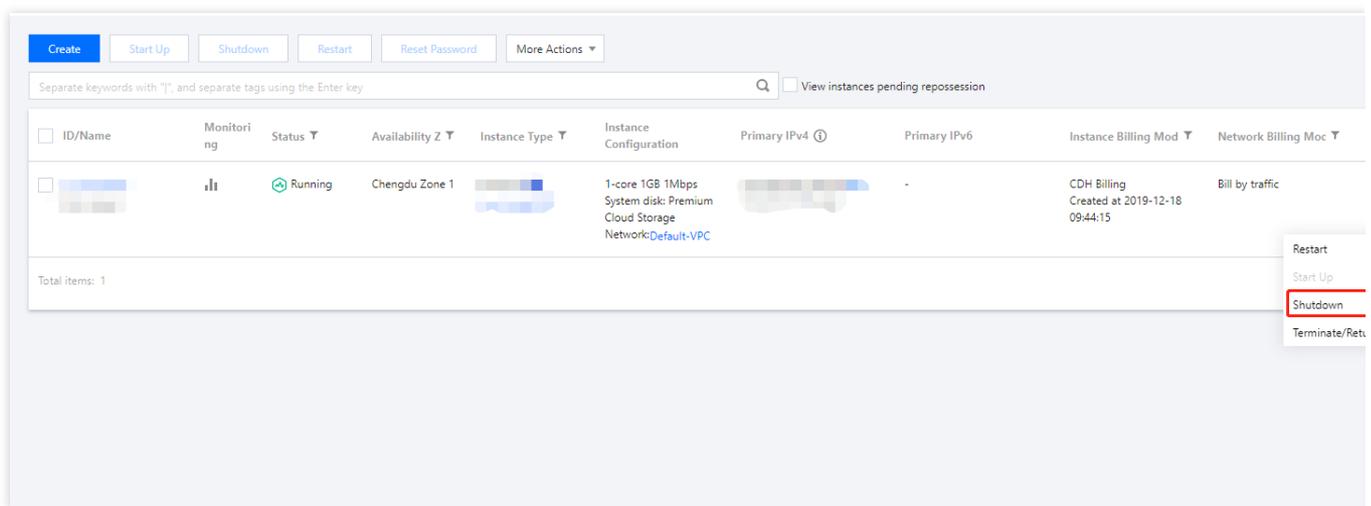
API を介したインスタンスのシャットダウン

### 単一インスタンスのシャットダウン

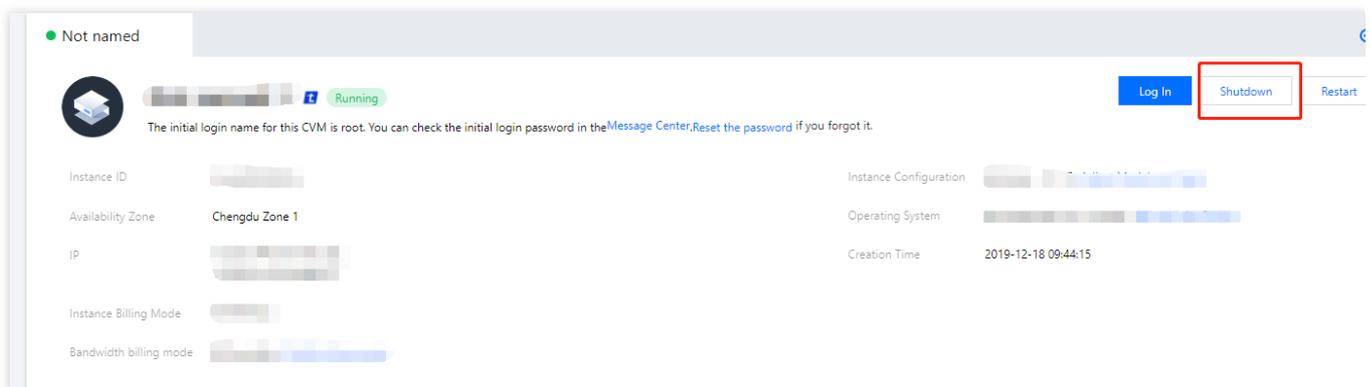
1. [CVMコンソール](#)にログインします。

2. インスタンスの管理画面で、実際に使用されているビューモードに従って操作します。

**リストビュー**：下図のように、シャットダウンしたいインスタンスを選択し、画面右のメニューからさらに **> インスタンスの状態 > シャットダウン** を選択します。



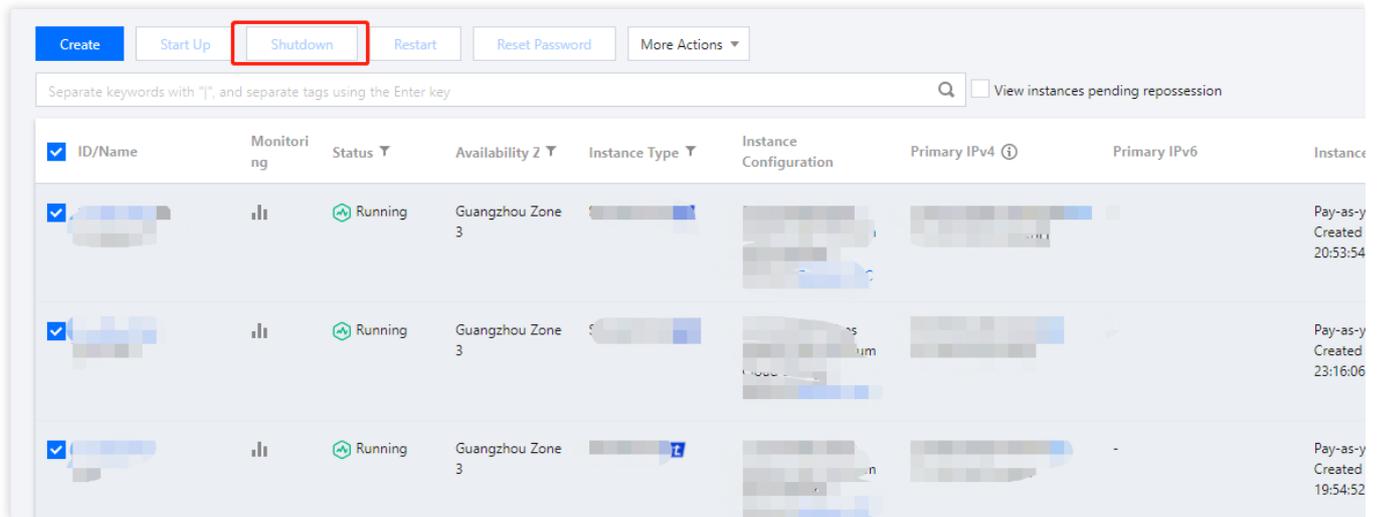
**タブビュー**：下図のように、シャットダウンしたいインスタンスのページで、画面の右上隅にある **その他の操作 > インスタンスの状態 > シャットダウン** をクリックします。



### 複数インスタンスのシャットダウン

1. [CVMコンソール](#)にログインします。

2. 下図のように、シャットダウンするすべてのインスタンスを選択し、リストの上部にある**シャットダウン**をクリックすれば、インスタンスを一括シャットダウンできます。



#### 説明：

シャットダウンできないインスタンスについて原因が表示されます。

[StopInstances](#) インターフェースをご参照ください。

## 後続の操作

インスタンスがシャットダウンされている場合にのみ、下記の属性を変更できます。

**インスタンス構成（CPU、メモリ）**：インスタンスタイプを変更するには、[インスタンス構成の変更](#)をご参照ください。

**パスワードの変更**：[ログインパスワード](#)をご参照ください。

**SSH キーのロード**：[SSH キー](#)をご参照ください。

# インスタンスの再起動

最終更新日：2023-03-03 16:16:35

## 概要

CVMインスタンスを再起動することは、それを維持するための一般的な方法です。インスタンスの再起動はローカルコンピューターのOSを再起動することと同じです。このドキュメントでは、インスタンスを再起動する方法について説明します。

## 注意事項

**再起動の準備：**インスタンスは再起動中にサービスを提供できないため、CVMを再起動する前に、サービスリクエストの受信が一時停止していることを確認してください。

**再起動の操作方法：**インスタンスで再起動コマンド（たとえば、Windowsでの再起動コマンドやLinuxでのRebootコマンドなど）を実行する代わりに、Tencent Cloudが提供する再起動操作を使用してインスタンスを再起動することを推奨します。

**再起動時間：**通常、インスタンスの再起動には数分しかかかりません。

**インスタンスの物理的特性：**インスタンスの再起動操作は、インスタンスの物理的特性を変えません。インスタンスのパブリックIP、プライベートIP、保存されているいかなるデータも変更されません。

**課金について：**インスタンスを再起動しても、新しいインスタンスの請求期間が開始されることはありません。

## 操作手順

次の方法でインスタンスを再起動できます。

コンソールからインスタンスの再起動

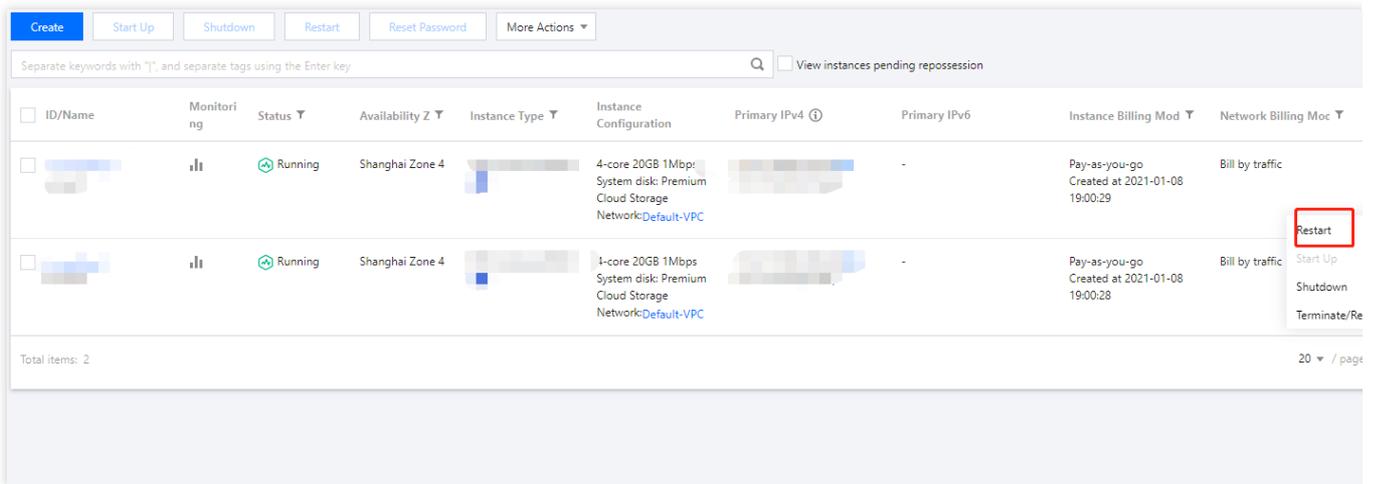
API によるインスタンスの再起動

### 単一インスタンスの再起動

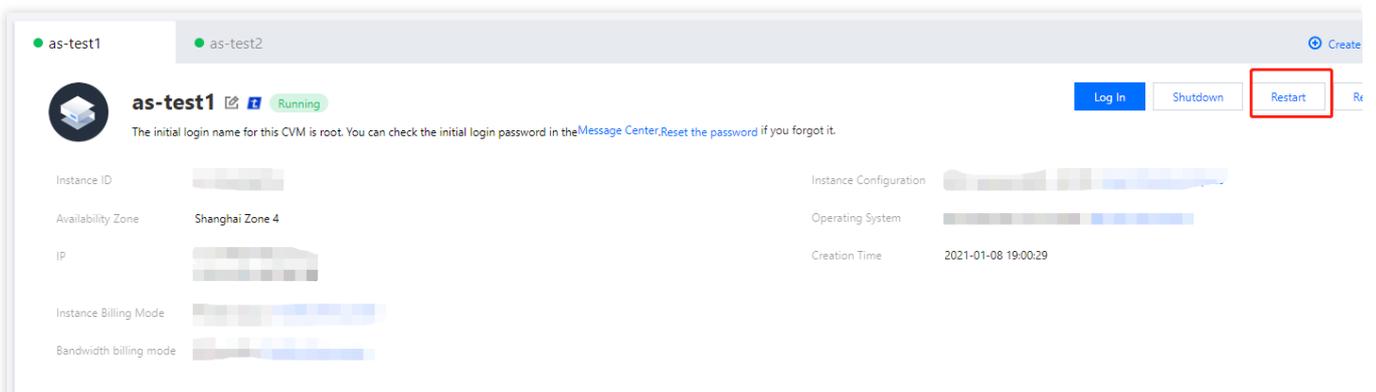
1. [CVMコンソール](#) にログインします。

2. インスタンスの管理画面で、実際に使用されているビューモードに従って操作します。

**リストビュー：**下図のように、再起動するインスタンスを選択し、画面右のメニューからさらに>インスタンスの状態>再起動をクリックします。

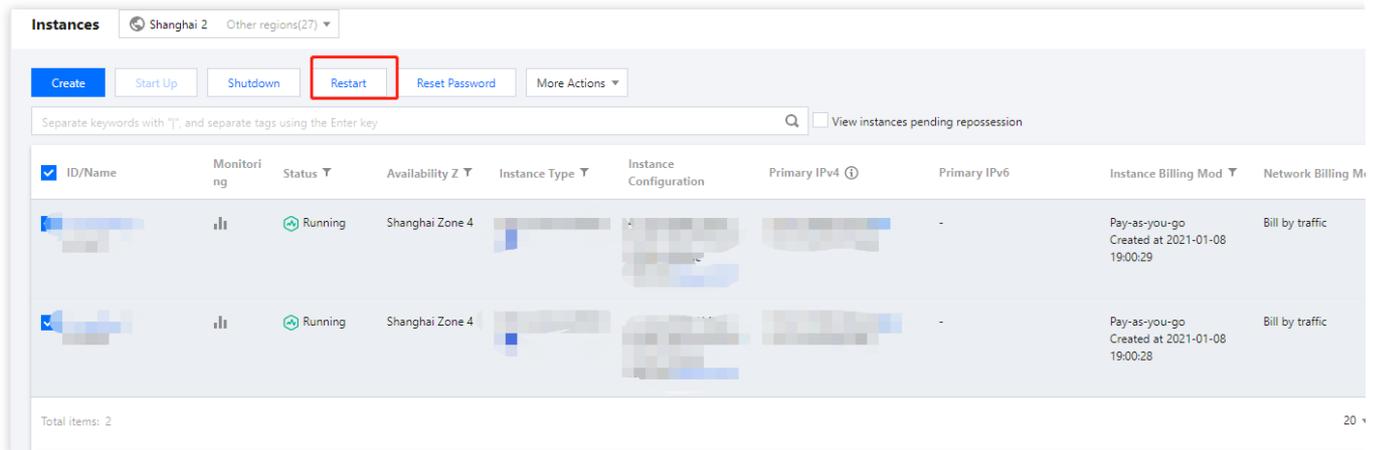


タブビュー：下図のように、再起動するインスタンスのページで、画面の右上隅にある再起動をクリックします。



## 複数インスタンスの再起動

1. CVMコンソールにログインします。
2. 下図のように、再起動するすべてのインスタンスを選択し、ページ上部にある再起動をクリックしてインスタンスを一括で再起動できます。インスタンスが再起動できない場合は、その理由が表示されます。



### 説明：

単一インスタンスもこの方法で再起動できます。

詳細については、[RebootInstances インターフェース](#) をご参照ください。

# インスタンスの休止

最終更新日：：2023-03-14 15:31:49

## ユースケース

インスタンスを休止状態にすると、オペレーティングシステムはメモリ内のデータ（オペレーティングシステムで実行されている各アプリケーションとその使用状況）をインスタンスのシステムディスクに保存します。ユーザーがインスタンスを次回起動すると、オペレーティングシステムは前回保存したメモリデータを読み取り、休止前のCVMインスタンスの実行状態に自動的に復元されます。

シャットダウンとの違いは、シャットダウン後のインスタンスを再起動すると、オペレーティングシステムがバックグラウンドサービスとアプリケーションサービスを再起動するということです。

ある時間帯でインスタンスを実行する必要がなく、特定の操作（設定調整やシステムの再インストール）も行う必要がない場合、インスタンスを休止状態にすることをおすすめします。

## 使用の前提条件

1. インスタンスの休止は現在、国際ステーションシリコンバレー地域が利用できますが、今後、他の地域も利用できるようになります；
2. 今のところ、標準型S3インスタンスおよびメモリが150 GIB未満のものが休止機能をオンにすることができます。他のインスタンスタイプへの適用についてまだ開発中です；
3. イメージはカスタムイメージ：Ubuntu20、CentOS 8.xであり、休止機能をオンにすることができます；
4. システムディスクはクラウドディスクであり、休止機能をオンにすることができます；
5. インスタンスに休止agentを実装しました。

## 注意事項

1. インスタンスの作成時に休止機能をオンにすると、この機能をオフにすることはできません；
2. インスタンスの作成時に休止機能がオフになっている場合、インスタンスを休止状態にすることはできません；
3. 従量課金の場合は、「休止状態に入ると課金されない」と「インスタンス保留状態に入っても課金される」がサポートされますが、スポットインスタンスでは休止状態に入っても課金されます。
4. インスタンスの作成時に休止状態がオンになっている場合、次の操作はサポートされません：  
構成の調整がサポートされません。

システムの再インストールがサポートされません。

スナップショットの作成がサポートされていません。

ディスク媒体の調整がサポートされません。

カスタムイメージの作成がサポートされません。

5. Auto Scalingグループ内のインスタンスは休止をサポートしていません。

### ご注意：

1. インスタンス内で休止操作が行われた場合、休止料金がかかります。

2. 休止に失敗すると、インスタンスは自動的に「実行中」状態になります。

## 操作手順

1. 作成時に休止状態をオンにする。

インスタンスを作成するときは、まず休止機能をオンにします。オンにしないと、インスタンスを休止状態にすることはできません。

2. 休止agentのインストール。

cvmインスタンスの内部にログインします。

agentスクリプトのダウンロード：`wget https://store-1252113659.cos.na-siliconvalley.myqcloud.com/suspend.py`

agentのインストール：

centosマシンの場合：`python3 suspend.py`

ubuntuマシンの場合：`sudo python3 suspend.py`

3. インスタンスを休止状態にする。

CVMインスタンスが休止状態になり、休止agentがインストールされると、実行中のインスタンスを休止状態にすることができます。

CVMコンソール-インスタンスとイメージ-インスタンスページにアクセスし、休止したいインスタンスを選択し、「インスタンスの設定-休止」をクリックします；

従量課金されたインスタンスでは、「休止状態に入ると課金されない」と「インスタンス保留状態に入っても課金される」を選ぶことができますが、スポットインスタンスでは休止状態に入っても課金されます。

OKをクリックすると、インスタンスはstopped状態になります。インスタンスを起動する必要がある場合は、スタートアップを選択してください。

# システムをリインストールする

最終更新日：2023-04-28 17:34:15

## 概要

システムを再インストールすると、インスタンスが起動直後の初期状態に復元されます。これは、インスタンスがシステムの障害に遭った時の重要なリカバー手段です。次のドキュメントでは、OSの再インストール方法について説明します。

CVMは、次の2種類の再インストール方法を提供します。

**同じプラットフォームでの再インストール：**CVMは、どのリージョンでも同じプラットフォームでの再インストールが可能です。

たとえば、LinuxからLinuxに再インストールする場合や、WindowsからWindowsに再インストールする場合。

**-異なるプラットフォーム間の再インストール：**中国大陸のみをサポートします（中国香港を含めない）。

たとえば、LinuxからWindowsに再インストールする場合や、WindowsからLinuxに再インストールする場合。

### 説明：

現在、新しく追加されたすべてのCloud Block Storage（CBS）インスタンスとローカルディスクインスタンスは、異なるプラットフォームでのシステムの再インストールをサポートしています。既存の20GBローカルディスクインスタンスの一部は、コンソールでのクロスプラットフォームの再インストールをサポートしていません。これらのローカルディスクインスタンスを使用するユーザーは、[チケットを提出](#)して申請する必要があります。スポットインスタンスはシステムの再インストールをサポートしていません。

## 注意事項

**再インストールの準備：**システムを再インストールすると、システムディスクの内容が失われるため、再インストールする前にシステムディスクの重要な情報をバックアップする必要があります。システムの実行データを保持する必要がある場合は、システムを再インストールする前に[カスタムイメージを作成](#)して、このイメージを選択して再インストールすることを推奨します。

**イメージ選択に関する推奨事項：**Tencent Cloudより提供されるイメージまたはカスタムイメージを使用して再インストールすることを推奨します。ソースが不明なイメージやその他のソースのイメージを使用することは推奨されません。システムディスクを再インストールする時には、他の操作を実行しないでください。

**インスタンスの物理的特性：**インスタンスのパブリックIPは変更されません。

**インスタンス仕様の制限：**お客様のインスタンスがWindows 2016や2019の関連バージョンのイメージを使用して再インストールする必要がある場合、インスタンスメモリは2Gより大きくする必要があります。

**課金について：**システムディスクのサイズが調整された場合（CBSのみがサポートされる）は、CBSの課金標準に従って課金します。詳細については、[ディスク価格](#)をご参照ください。

-**後続作業**：システムディスクを再インストールした後、データディスクのデータは保留され、影響を受けませんが、使用するには再マウントする必要があります。

## 操作手順

次の方法でOSを再インストールできます。

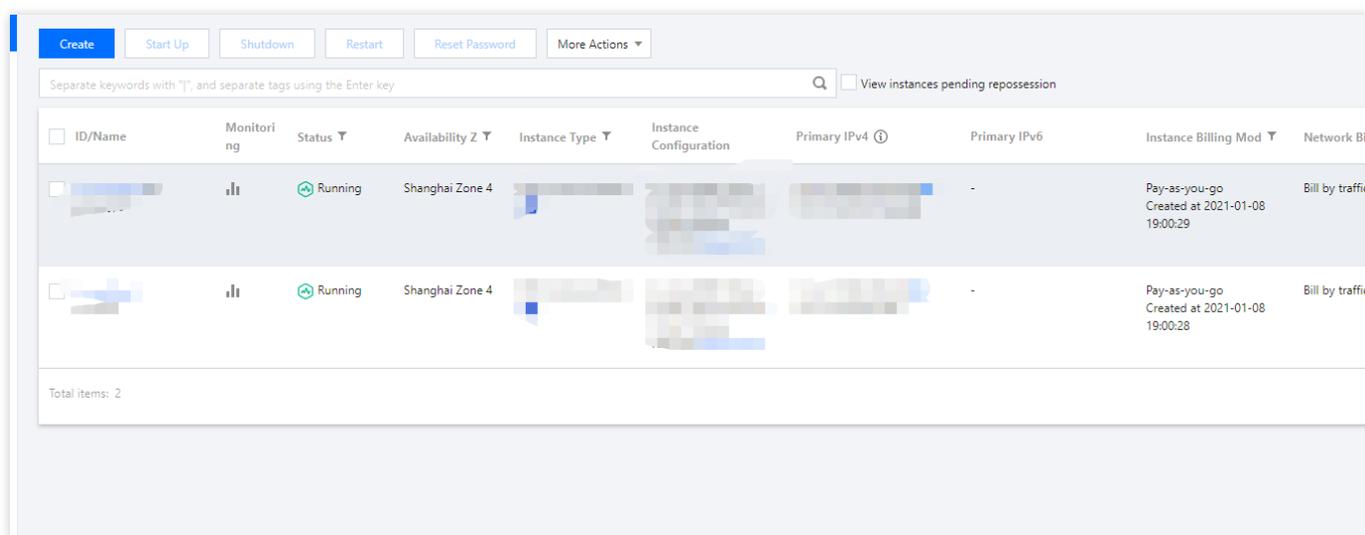
コンソールを使用したシステムの再インストール

APIを使用したシステムの再インストール

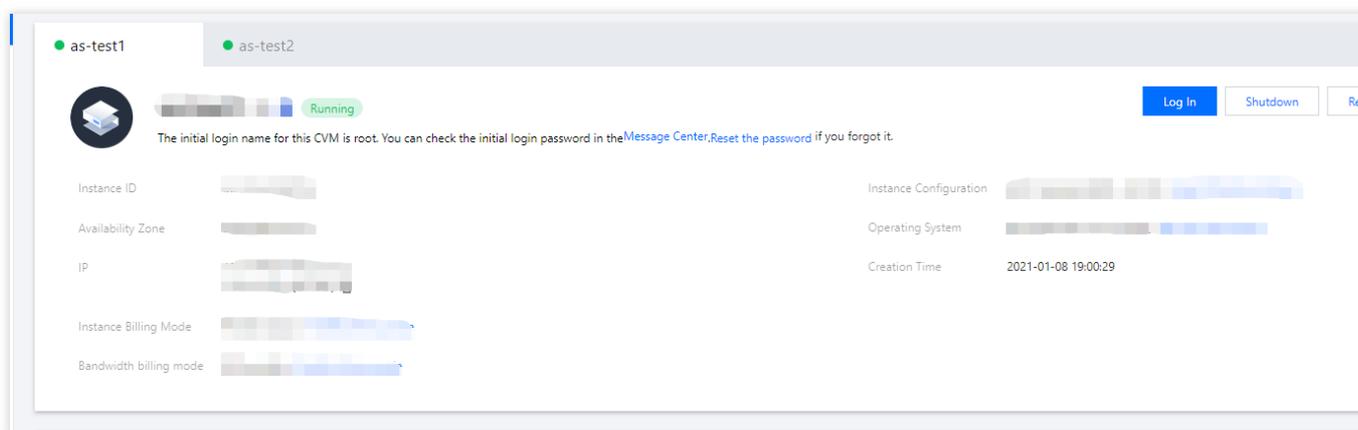
1. [CVMコンソール](#)にログインします。

2. インスタンスの管理画面で、実際に使用されているビューモードに従って操作します。

**リストビュー**：下図のように、システムを再インストールしたいインスタンスの行で、**その他 > システムの再インストール**を選択します。



**タブビュー**：下図のように、システムを再インストールしたいインスタンスページで、右上コーナーの**その他操作 > システムの再インストール**を選択します。



3. ポップアップした「システムの再インストール」ウィンドウで、「システム再インストール時の注意事項」を読み、**次へ**をクリックします。

4. 下図のように、現在のインスタンスを使用したイメージまたはその他のイメージを使用することを選択し、インスタンスのログイン方法を設定して、**OK**をクリックします。

**説明：**

なお、イメージタイプが**カスタムイメージ**または**共有イメージ**である場合に限り、ログイン方法として**イメージ設定の保持**を選択することができます。

## Reinstall system

Heads up > **2** Configuration

You've selected 1 instance. [Collapse](#)

ID/name	Instance type	Operating system	System disk
	S6 2-core 4GB	OpenCloudOS Server 8	Balanced SSD 5

- Create a snapshot or image to back up your data before continuing, so as to avoid data loss. [Operation guide](#)
- Data in the instance data disk will not be cleared. But you need to mount the disk manually after reinstallation to it. [Operation guide](#)
- If the current system disk size is too small to meet the requirements, please expand the capacity. [Disk capacity](#)

Image type  Current image  Public image  Custom image  Shared image  Marke

Target image OpenCloudOS Server 8/

Login methods  Set password  Bind key  Follow image

Username root

New password

Security reinforcement  Activate Anti-DDoS Protection and Cloud Workload Protection for free. [About Security Reinf](#)

Cloud monitoring  FREE cloud monitoring, analysis, alarming, and server monitoring metrics (component installa required) [About Cloud Monitor](#)

Fees

Back

OK

[ResetInstance](#) インターフェース をご参照ください。

## 後続の操作

ご利用のCVMはシステムが再インストールされる前にすでにデータディスクがマウントされており、また、システム再インストールのタイプが異なるプラットフォームの再インストールとなる場合、次のドキュメントを参照して、元のOSにあるデータディスクデータを読み込む必要があります。

[LinuxをWindowsに再インストールした後に元のEXTタイプのデータディスクを読み込む](#)

[WindowsをLinuxに再インストールした後に元のNTFSタイプのデータディスクを読み込む](#)

# TATを使用してコマンドを実行し

最終更新日：：2023-07-10 11:39:25

## 概要

Tencent Cloud Automation Tools (TAT) はCVM、Lighthouseインスタンス向けに設計されたセネイティブな運用保守および展開ツールです。TATは、インスタンスにリモート接続しなくても、Shellコマンドを自動的に一括実行して、自動化スクリプトの実行、プロセスのポーリング、ソフトウェアのインストール/アンインストール、アプリケーションの更新、パッチのインストールなどのタスクを完了することができます。TATの詳細については、[概要](#)をご参照ください。

このドキュメントは、TATを使用してコマンドを実行し、インスタンスを管理する方法について説明します。

## 前提条件

CVMインスタンスは、TATエージェントをインストールする必要があります。詳細については、[TATのインストール](#)をご参照ください。

### 説明：

既存のCVMインスタンスの一部は現時点でTATの使用をサポートしていませんが、今後、すべてのインスタンスでTATがサポートされる予定です。

## 操作手順

コマンドの作成と実行およびコマンドの実行ステータスの確認には、次のドキュメントをご参照ください：

[コマンドの作成](#)

[コマンドの実行](#) または [ログイン不要のコマンド実行](#)

[コマンドの実行ステータスのクエリ](#)

# インスタンスの破棄/返却

## インスタンスの廃棄/返却の概要

最終更新日：：2024-04-10 10:14:43

このドキュメントでは、インスタンスの廃棄およびリリースの概要と操作方法について説明します。その他期限切れ情報については、[期限切れのリマインダー](#)をご参照ください。

### 概要

特定のインスタンスが必要でない場合は、インスタンスを廃棄することができます。廃棄されたインスタンスはごみ箱に投入されますが、これらのインスタンスはさまざまなユースケースやニーズに応じて更新、復元、またはリリースできます。

#### ご注意：

ユーザーのアカウントが支払い延滞である場合、復元する前に、従量課金のインスタンスに対して先に料金を補充してください。

### 廃棄/返却方式

従量課金のインスタンスタイプでは、インスタンスの廃棄およびリリースは次の方式があります：

**自主廃棄**：支払い延滞なしの従量課金タイプのインスタンスに対しては、手動で廃棄することができます。従量課金タイプのインスタンスがごみ箱で最大2時間保持され、その後完全にリリースされます。

**定時廃棄**：従量課金タイプのインスタンスに対して定時廃棄を設定します。将来の時点でインスタンスを定時廃棄するように設定し、廃棄時間が秒単位まで設定できます。定時廃棄に設定されているインスタンスはごみ箱に入らず、すぐにリリースされます。定時廃棄の前に、随時に [定時廃棄を取り消す](#) ことができます。

**期限切れ/支払い延滞の場合の自動廃棄**：従量課金タイプのインスタンスは残高が0未満の状態です。2時間+15日間続いた後、自動的にリリースされます（最初の2時間には料金は続いて差し引かれますが、次の15日間にはシャットダウンされ、料金の差し引きが停止します。支払い延滞の従量課金インスタンスはごみ箱に投入されないため、インスタンスリストで確認できる）。指定された時間内に [更新](#) をした場合、引き続き使用できます。

タイプ	自主廃棄（支払い延滞なし）	定時廃棄（支払い延滞なし）	期限切れ/支払い延滞の場合の自動廃棄
従量課金タイプのインスタンス	廃棄後、ごみ箱で最大2時間保持され、期限が切れた後に復元されない	定時廃棄のインスタンスを設定し、設定された時間になるとごみ箱に投	インスタンスが支払い延滞した後、最初の2時間には料金は続いて差し引かれ、インスタンスが使用できますが、次の15日間にはシャットダウンされ、料金の差し引きが停止します。支払い延滞の従量課金インスタンスはごみ箱に投入されません。この

	場合はリリースされます。	入せず、直接リリースされます。	間、更新していない場合は、インスタンスはリリースされます。
年額・月額タイプのインスタンス	早期廃棄はサポートされていません	定時廃棄に関連しません	期限切れで廃棄されたインスタンスはゴミ箱に入り、最大7日間保管されます。期間が満了するまでにリカバリーされない場合は、インスタンスは解放されます。

## 関連影響

インスタンスが廃棄状態になると、インスタンスのデータ、Elastic IP、および課金には次のような影響が及びます：

**課金関係**：インスタンスが廃棄中またはリリースされた状態になると、このインスタンスに関する費用は発生しません。

**インスタンスデータ**：マウントされているローカルディスクとElastic Cloud Block Storage以外のものは同時にリリースされ、データが回復できないため、事前にバックアップしておいてください。Elastic CBSは独自のライフサイクルに従います。

**Elastic IP**：インスタンスが廃棄されたElastic IP（セカンダリENIのIPを含む）は継続的に保持されますが、アイドルIPには費用がかかりますので、保持する必要がない場合は、直ちにリリースしてください。

## 操作手順

インスタンスは次のように自主廃棄/返却できます：

コンソールを使用したインスタンスの廃棄/返却に関する詳細情報は、[コンソールを使用したインスタンスの廃棄/返却](#)をご参照ください。

APIを使用したインスタンスの廃棄/返却に関する詳細情報は、[TerminateInstancesインターフェース](#)をご参照ください。

# コンソールを使用したインスタンスの破棄/返却

最終更新日： : 2022-07-12 16:15:19

## 概要

ここでは、課金モデルが従量課金であるCVMインスタンスをコンソールを介して破棄/返却することについてご説明します。

### ご注意：

CVMインスタンスの破棄/返却による影響については、[関連する影響](#)をご参照ください。

## 操作手順

### 従量課金タイプのインスタンスの破棄とリリース

従量課金タイプのインスタンスに対しては、直ちに廃棄するか、または定時廃棄にすることができます。

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画面で、実際に使用されているビューモードに従って操作します。

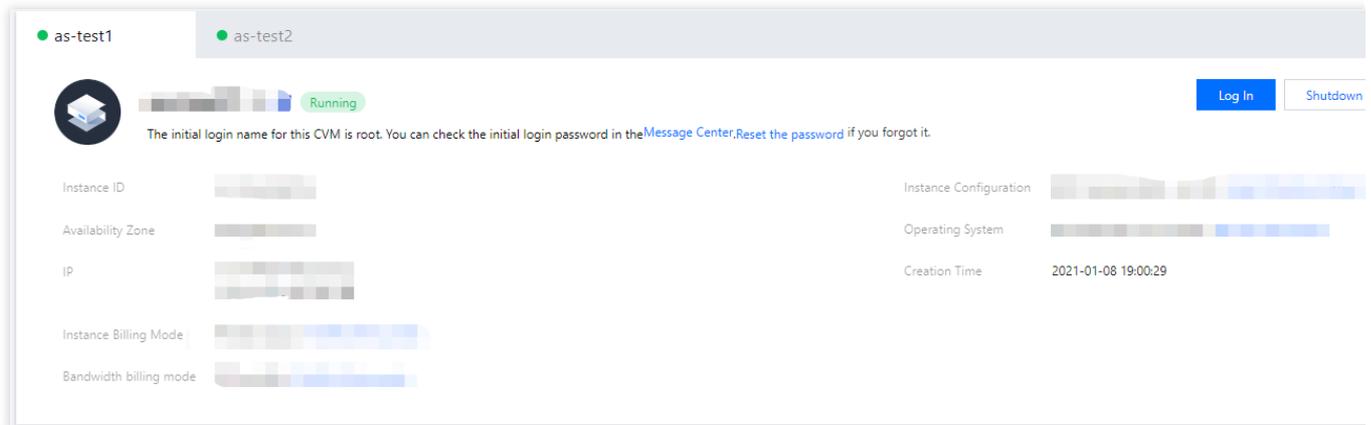
下図に示すように、**リストビュー**：インスタンスを破棄する必要がある行の右側にある**その他 > インスタンスのステータス > 破棄/返却**を選択します。

ID/Name	Monitoring	Status	Availability Zone	Instance Type	Instance Configuration	Primary IPv4	Primary IPv6	Instance Billing Model	Net
[Redacted]	[Icon]	Running	Shanghai Zone 2	[Redacted]	[Redacted]	[Redacted]	-	Pay-as-you-go Created at 2021-01-08 19:00:29	Bill I
[Redacted]	[Icon]	Running	Shanghai Zone 4	[Redacted]	[Redacted]	[Redacted]	-	Pay-as-you-go Created at 2021-01-08 19:00:28	Bill I

複数のインスタンスを同時に破棄する必要がある場合は、インスタンスにチェックを入れ、リスト上部の**その他**

の操作 > **破棄/返却**を選択すれば完了です。

下図に示すように、**タブビュー**：破棄するインスタンス画面で、画面右上隅の**破棄/返却**をクリックします。



3. ポップアップした「破棄/返却」ウィンドウで、インスタンスを**今すぐ破棄**または**時間を指定して破棄**することを選択できます。

**直ちに廃棄**：直ちに廃棄することを選択した場合、リソースを直ちにリリースするか、または2時間後にリソースするかを選択できます。直ちにリリースすることを選択した場合、このインスタンスに関連するデータはクリアされ、復元不能になります。

**定時廃棄**：定時廃棄を選択した場合、定時廃棄の時間を設定する必要があります。期限切れになると、インスタンスは定期的に廃棄・リリースされ、且つ復元不能になります。

4. 破棄方法を選択したら、**次へ**をクリックして、破棄および保持されている実際のリソースと関連リソースを確認します。

5. リソースの破棄を確認したら、**破棄の開始**をクリックします。

## 関連する操作

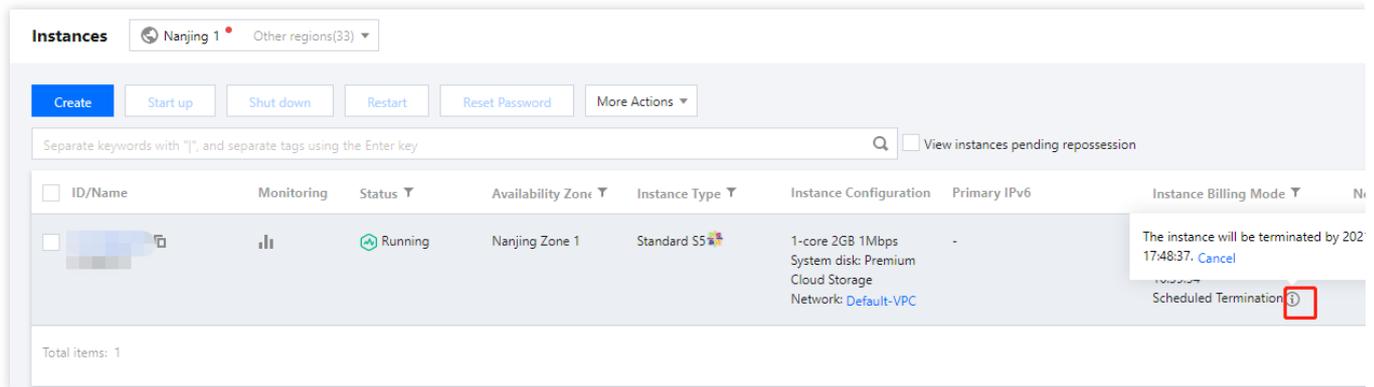
### 定時廃棄を取り消す

1. **CVMコンソール**にログインします。

2. 下図に示すように、インスタンスリストから定時廃棄を取り消すインスタンスを特定し、**インスタンスの課金モード**列から**定時廃棄**を特定し、マウスマウスカーソルを

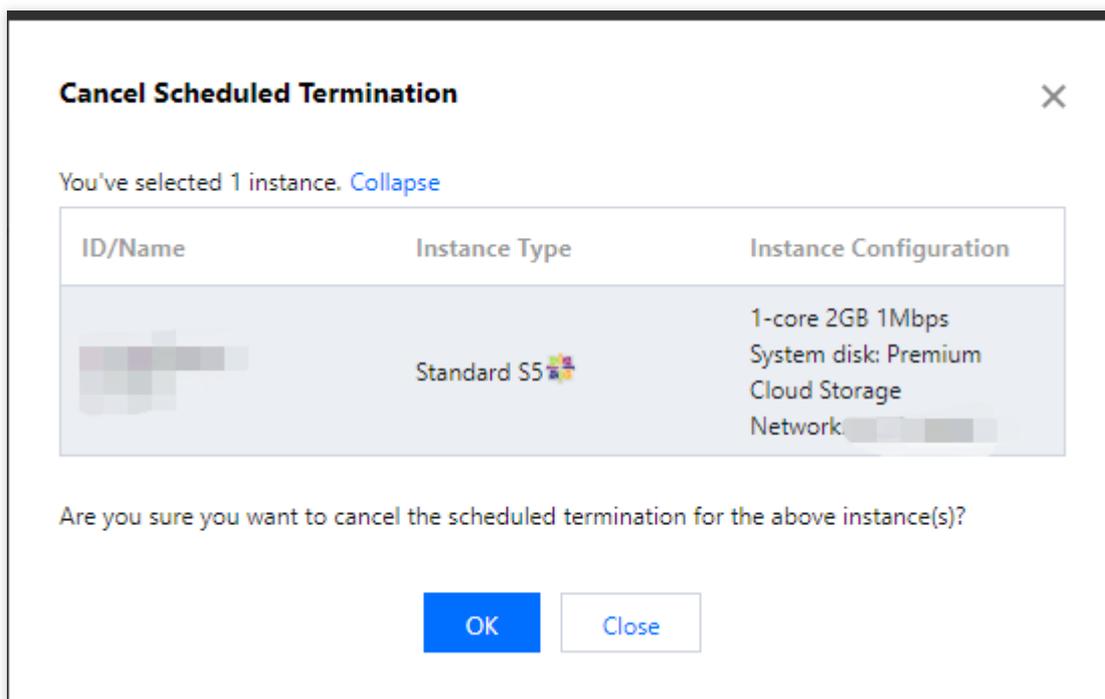


に置くと定時廃棄のプロンプトボックスが表示されます。



3. 破棄をクリックすると、「時間を指定して破棄」のキャンセルを確認するプロンプトボックスが表示されます。

4. 下図に示すように、ポップアップしたプロンプトボックスで、「時間を指定して破棄」をキャンセルするインスタンスの情報を確認し、**OK**をクリックすると、「時間を指定して破棄」のキャンセルが直ちに有効になります。



# インスタンスの削除保護の有効化

最終更新日：2022-07-07 16:19:38

## 操作シナリオ

通常の状態下で、あるインスタンスが不要になった場合は、コンソールまたはAPIでインスタンスの削除操作を行うことができます。意図せずインスタンスを削除してしまうことを防ぐため、インスタンスの削除保護を有効にすることができます。有効にすると、コンソールおよびAPIによってインスタンスを削除することができなくなります。インスタンスの削除が必要なことが確認できている場合は、インスタンスの削除保護を無効にしてから削除操作を行うことができます。

インスタンスの削除保護を有効にすることで、業務データインスタンスの保存を保障し、意図せずインスタンスを削除してしまうことを防ぐことができます。ここではコンソール上でインスタンスの削除保護を有効化または無効化する方法についてご説明します。

## 説明事項

新規購入したインスタンスおよび既存のインスタンスでは、インスタンスの削除保護はデフォルトで無効になっています。必要に応じて有効化することができます。

インスタンスの削除保護はシステムレベルでの削除に対しては無効です。例えば、従量課金インスタンスが支払い遅延のためにシャットダウン後に削除される場合などです。

## 操作手順

### インスタンスの削除保護の有効化

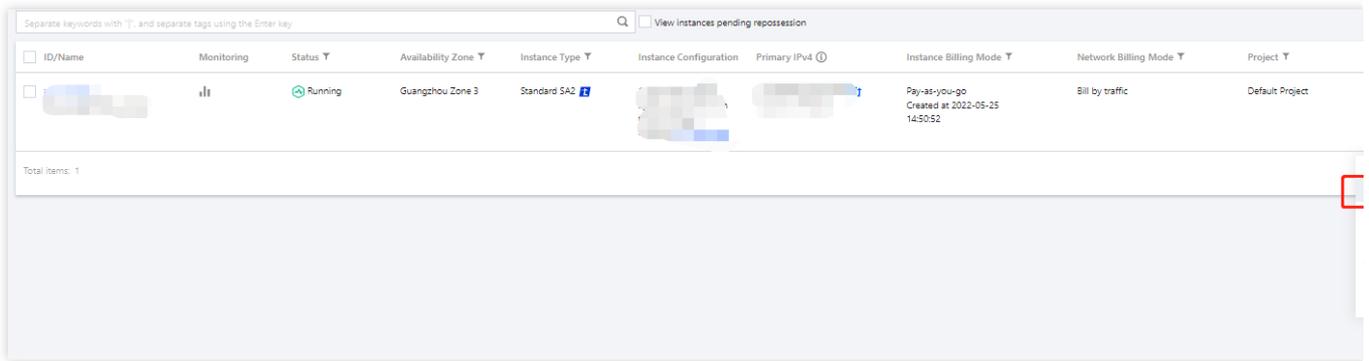
既存のインスタンスの削除保護の有効化

新規購入インスタンスの削除保護の有効化

1. [CVMコンソール](#) にログインします。
2. 実際のニーズに応じて、単一または複数のインスタンスの削除保護を有効化することができます。

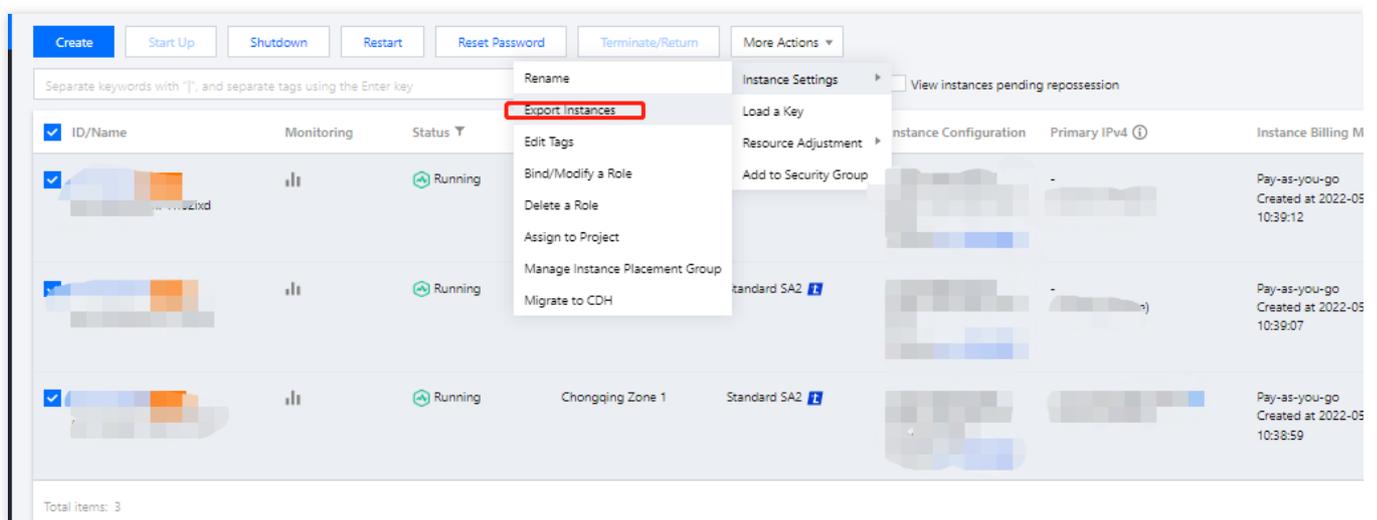
#### 単一のインスタンスの削除保護の有効化：

下図のように、「インスタンス」ページで、インスタンスの削除保護を有効化したいインスタンスを見つけ、その行の右側の**その他** > **インスタンス設定** > **インスタンスの削除保護の設定**を選択します。



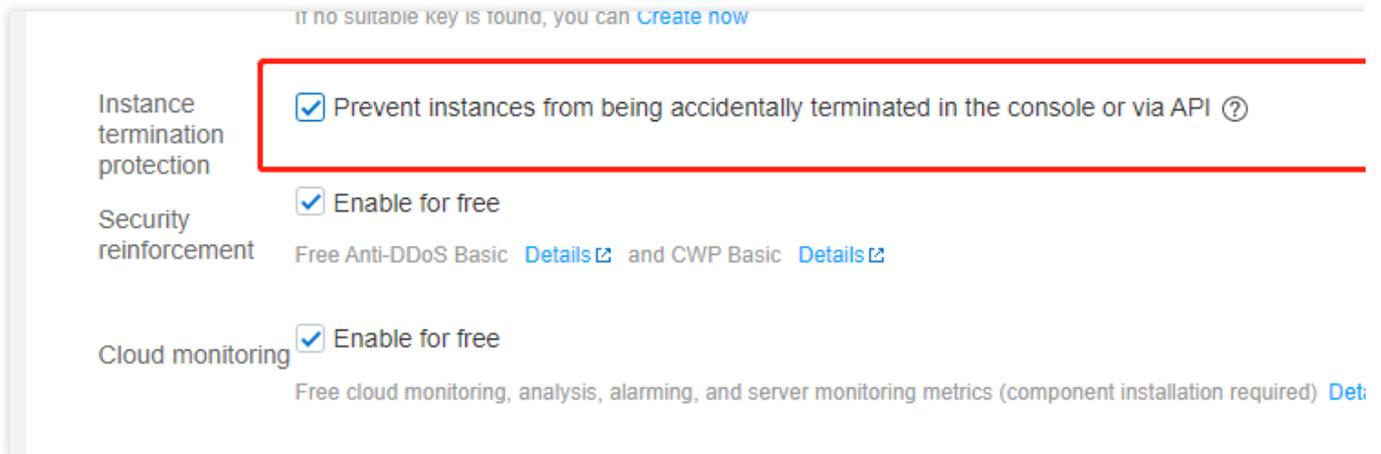
### インスタンスの削除保護の一括有効化：

下図のように、「インスタンス」ページで、インスタンスの削除保護を有効化したいインスタンスにチェックを入れ、リスト上方の**その他 > インスタンス設定 > インスタンスの削除保護の設定**を選択します。



3. ポップアップした「インスタンスの削除保護の設定」ウィンドウで、「有効」を選択し、**OK**をクリックすれば、インスタンスの削除保護の有効化が完了します。

インスタンスの新規購入時に、下図のように「カスタム設定」を選択し、「2. ホストの設定」手順で「インスタンスの削除保護」にチェックを入れます。



## 説明：

その他のパラメータ設定については、[購入画面でインスタンスを作成](#)をご参照ください。

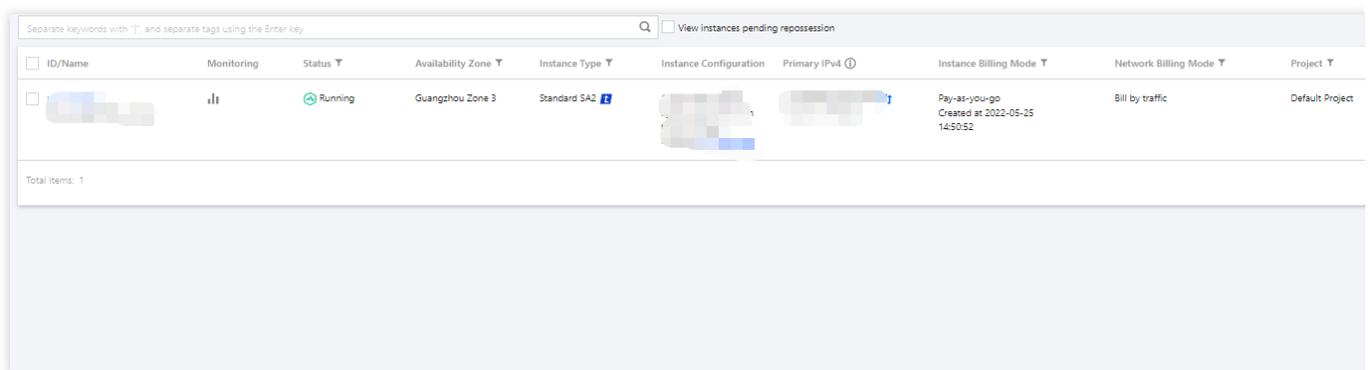
## インスタンスの削除保護の無効化

インスタンスが削除可能であることが確認できている場合は、次の手順を参照し、インスタンスの削除保護を無効にしてから削除操作を行ってください。

1. [CVMコンソール](#) にログインします。
2. 実際のニーズに応じて、単一または複数のインスタンスの削除保護を無効化することができます。

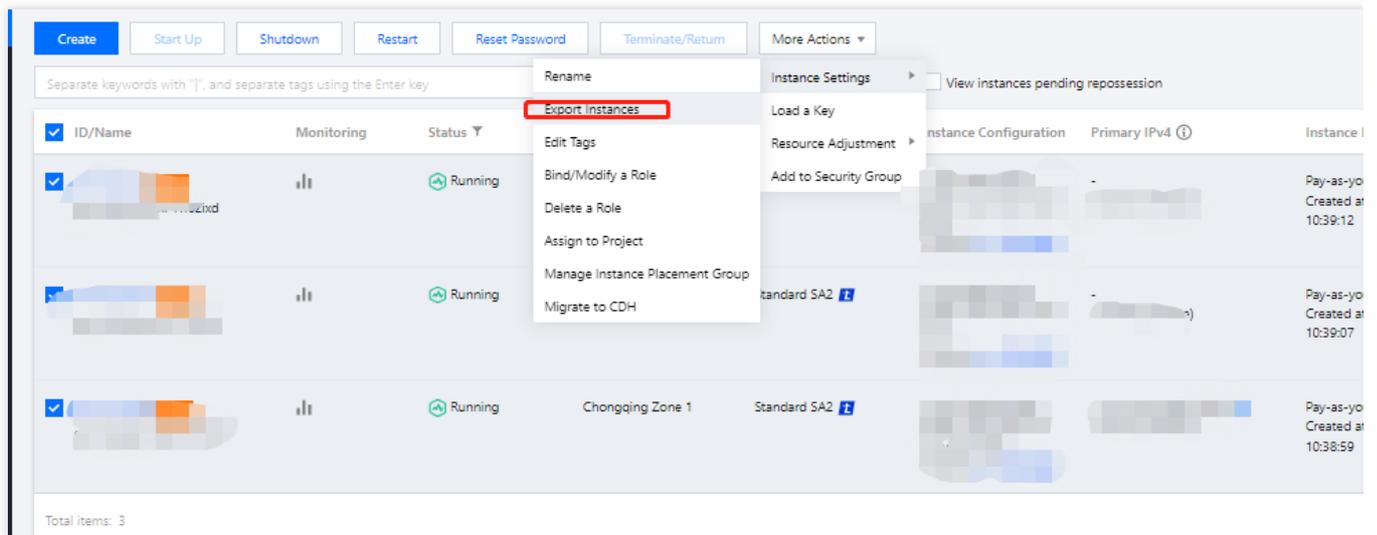
### 単一のインスタンスの削除保護の有効化：

下図のように、「インスタンス」ページで、インスタンスの削除保護を有効化したいインスタンスを見つけ、その行の右側の**その他 > インスタンス設定 > インスタンスの削除保護の設定**を選択します。



### インスタンスの削除保護の一括有効化：

下図のように、「インスタンス」ページで、インスタンスの削除保護を有効化したいインスタンスにチェックを入れ、リスト上方の**その他 > インスタンス設定 > インスタンスの削除保護の設定**を選択します。



3. ポップアップした「インスタンスの削除保護の設定」ウィンドウで、「無効」を選択し、**OK**をクリックすれば、インスタンスの削除保護の無効化が完了します。

## 関連ドキュメント

[購入画面でインスタンスを作成](#)

[インスタンスの削除/返却](#)

# インスタンスを回収する又はインスタンスの復元

最終更新日：：2023-07-27 14:36:40

このドキュメントでは、インスタンスの回収メカニズムとインスタンスリカバリの操作方法について説明します。詳細については、[支払い延滞の説明](#)をご参照ください。

## インスタンス回収の説明

Tencent Cloudゴミ箱はCVMインスタンスの回収メカニズムです。インスタンスの回収について次の通りです。

**従量課金インスタンス**：手動で終了するか、スケジュールされた時間に終了する従量課金インスタンスは、ゴミ箱に移動されます。延滞が発生した場合、従量課金インスタンスには回収メカニズムがないため、支払い延滞が2時間+15日を過ぎると、インスタンスのリソースが直接リリースされます。

ゴミ箱に移動するインスタンスの説明については、次のとおりです。

従量課金インスタンスはゴミ箱に移動します

**保持時間**：支払い延滞がない場合、ユーザーが手動で終了したインスタンスはゴミ箱に2時間保持されます。

**期限切れ処理**：期日までに更新されていないインスタンスの場合、保持期間を超えた時点でシステムがインスタンスリソースを解放し、自動的に[インスタンスの破棄/返却](#)を開始して、復元できなくなります。インスタンスにバインドされているElastic IPは保持されます。このElastic IPが不要になった場合は、速やかに解放してください。

**マウント関係**：インスタンスがゴミ箱に入った後、Cloud Load Balancer、Cloud Block Storage、Classiclinkとのマウント関係は自動的に終了しません。

**操作の制限**：ゴミ箱内のインスタンスについては、[更新の再開](#)、[インスタンスの破棄/返却](#)と[イメージの作成](#)（特殊モデルを除く）操作のみを行うことができます。

### ご注意：

料金の支払いを滞納している場合、ゴミ箱から従量課金インスタンスを復元することはできません。このインスタンスを復元するには、最初に更新料を支払う必要があります。

従量課金インスタンスはゴミ箱に最大2時間保存されるため、インスタンスを継続して使用できるように、インスタンスを時間内に更新および復元する必要があります

料金の支払いを滞納している場合、従量課金インスタンスはゴミ箱に入らないため、CVMのインスタンスリストページで確認する必要があります。支払い延滞が2時間+15日を過ぎても更新されない場合、インスタンスはリリースされます。

## インスタンスの復元

1. [CVMコンソール]にログインし、左側のナビゲーションバーで**ごみ箱**> **インスタンスごみ箱**を選択します。
2. 「インスタンスごみ箱」画面で、実際のニーズに応じた操作方法を選択します。

単一インスタンスの復元

インスタンスの一括復元

リストで復元する必要があるインスタンスを見つけ、**復元**をクリックして操作し、更新の支払いを完了します。  
リスト内の復元する必要があるすべてのインスタンスにチェックを入れ、トップにある**一括復元**をクリックすれば、更新の支払いは完了です。

# スポットインスタンスの管理

最終更新日：2023-05-15 10:48:14

## 概要

このドキュメントでは、スポットインスタンスの管理及び購入方法などをご説明させていただきます。現在、スポットインスタンスは下記の3種類の方法を通じて利用することができます。

**CVMコンソール**：CVM購入ページでは、スポットインスタンスモードがサポートされています。

**BatchComputeコンソール**：BatchComputeコンソールでジョブ送信およびコンピューティング環境作成時に、スポットインスタンスを選択できます。

**TencentCloud API**：スポットインスタンスパラメーターが [RunInstanceインターフェース](#) に追加されました。

## 操作手順

CVMコンソール

Batch Computeコンソール

クラウド API

- [CVM購入ページ](#)にログインします。
- 下図に示すように、課金方法は**スポットインスタンス**を選択します。

1. Select Model      2. Complete Configuration      3. Confirm Configuration

Billing Mode    Pay as you go    **Spot Instances**    Detailed Comparison

Region

Guangzhou	Shanghai	<b>Nanjing</b> <small>Promo</small>	Beijing	Chengdu	Chongqing	Taipei, China <small>NEW</small>
Singapore	Bangkok	Jakarta <small>NEW</small>	Mumbai	Seoul	Tokyo	Silicon Valley
Toronto	Frankfurt	Moscow	São Paulo <small>NEW</small>			

Tencent Cloud products in different regions cannot communicate via private network. Selecting the region closest to your customers can reduce a speed. CVM's region cannot be changed after the creation. . [View My CVM Region](#) [Detailed Comparison](#)

Availability Zone    Random AZ    Nanjing Zone 1 Promo    Nanjing Zone 2 Promo    Nanjing Zone 3 Promo

3. 実際のニーズと画面の指示に従って、リージョン、アベイラビリティゾーン、ネットワークタイプ、インスタンスなどの構成情報を選択します。
  4. 購入するスポットインスタンスの情報と各構成アイテムの費用の詳細を確認します。
  5. アクティブ化をクリックして支払いを行います。
- 支払いが完了した後、[CVM コンソール](#) にログインしてスポットインスタンスを確認できます。

## BatchCompute機能の説明

### 非同期インターフェース

ジョブの送信またはコンピューティング環境の作成、予想されるコンピューティング環境のインスタンス数を変更する場合、BatchComputeは非同期の形式でリクエストを処理します。つまり、在庫、価格などの理由で現在のリクエストを満たせない場合は、満たせるようになるまでスポットインスタンス型リソースを申請し続けます。インスタンスをリリースしたい場合は、BatchComputeコンソールで予想されるコンピューティング環境のインスタンス数を調整する必要があります。CVMコンソールでインスタンスをリリースすると、BatchComputeコンソールは、予想されるインスタンス数に達するまでインスタンスを自動的に作成します。

### クラスターモデル

BatchComputeインスタンスのコンピューティング環境は、スポットインスタンスのバッチを1つのクラスターとして維持することをサポートします。スポットインスタンスの希望する数、構成、および最高指値を送信するだけで、コンピューティング環境は、予想される数量に達するまでスポットインスタンスを自動的にかつ継続的に適用します。中断が発生した後も補充数量の申請が自動的に再開されます。

### 固定価格

現段階では固定割引モデルを採用しており、パラメータを現在の市場価格以上の値に設定する必要があります。市場価格の詳細については、[スポットインスタンス](#) をご参照ください。

### 使用手順

1. [BatchComputeコンソール](#) にログインします。
2. コンピューティング環境管理ページで任意のリージョン（例えば広州リージョンなど）を選択し、**新規作成** をクリックします。  
コンピューティング環境の作成ページに進みます。
3. 下図に示すように、「課金タイプ」を**スポットインスタンス**に設定し、実際のニーズに応じて、必要なモデル、イメージ、名前、目標数量などの情報を選択します。

### New computing environment

Name	<input type="text"/>						
Region	Guangzhou						
Availability Zone	<input checked="" type="radio"/> Guangzhou Zone 3 <input type="radio"/> Guangzhou Zone 4 <input type="radio"/> Guangzhou Zone 6 <input type="radio"/> Guangzhou Zone 7						
Billing Type	<input type="radio"/> Regular Instance <input checked="" type="radio"/> Spot Instance						
Resource Scheduling Mode	<input checked="" type="radio"/> Compute Resource Pool <input type="radio"/> Specified Models						
Bidding Policy	Follow market price						
Model Type	<input type="checkbox"/> General (2.3~2.5 GHz) <input type="checkbox"/> Compute (3.2~3.4 GHz) <input type="checkbox"/> All Models						
Instance Configuration	Please select a model type System disk (Premium Cloud Storage 50 GB), data disk (No data disk), bandwidth (No public network bandwidth), password (system)						
Available Models	The selected models are available in the current region.						
Image	<input type="text" value="Public Images"/> <input type="text" value="Please select"/> You must select the images that have installed and configured Cloud-init. ⓘ						
Expected quantity	<input type="text" value="0"/>						
Tag configuration	<table><thead><tr><th>Tag key</th><th>Tag value</th><th>Operation</th></tr></thead><tbody><tr><td><input type="text" value="Please select"/></td><td><input type="text" value="Please select"/></td><td><input type="button" value="x"/></td></tr></tbody></table> <a href="#">Add</a>	Tag key	Tag value	Operation	<input type="text" value="Please select"/>	<input type="text" value="Please select"/>	<input type="button" value="x"/>
Tag key	Tag value	Operation					
<input type="text" value="Please select"/>	<input type="text" value="Please select"/>	<input type="button" value="x"/>					
<a href="#">More configurations</a>							
<input type="button" value="OK"/>	<input type="button" value="Cancel"/>						

4. **OK**をクリックして、作成を完了します。

作成が完了したら、[BatchCompute コンソール](#)で新しいコンピューティング環境を確認できます。また、コンピューティング環境内のCVMインスタンスも同期的に作成されており、このコンピューティング環境の[アクティビティログ](#)と[インスタンスリスト](#)でインスタンスの作成の進行状況を確認できます。

RunInstance インターフェースにおける[InstanceMarketOptionsRequest](#)パラメータはスポットインスタンスの使用モード（有効または無効）を指定し、関連情報を構成できます。

**同期インターフェース**：現在、RunInstanceが提供している同期リクエストインターフェースは一回限り使用できます。即ち、申請が失敗（在庫不足、請求価格が市場価格以下）した場合は直ちに失敗を戻し、引き続き申請をしません。

**固定価格**：現段階では固定割引モデルを採用しており、パラメータを現在の市場価格以上の値に設定する必要があります。市場価格の詳細については、[スポットインスタンス](#)をご参照ください。

## サンプルシナリオの説明

顧客は広州三区における一つのインスタンスを保有しており、当該インスタンスの課金モードが時間単位で課金する入札モードです。詳細な内容は以下の通りです。

最高入札額：0.0923ドル/時間

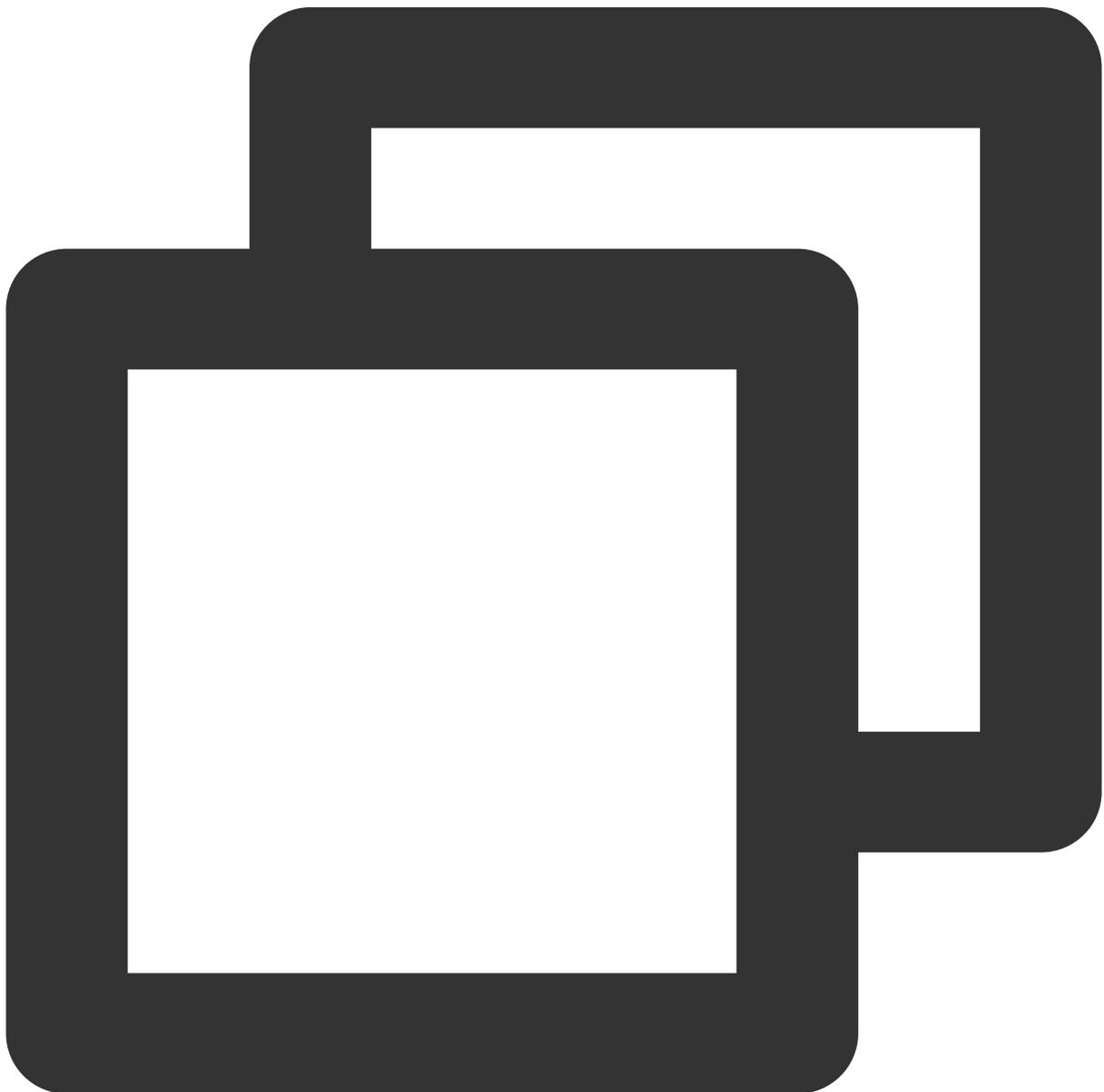
入札リクエストモード：1回限りのリクエスト

イメージ ID：img-pmqg1cw7

選択するモデル：2C4G二世世代標準型（S2.MEDIUM4）

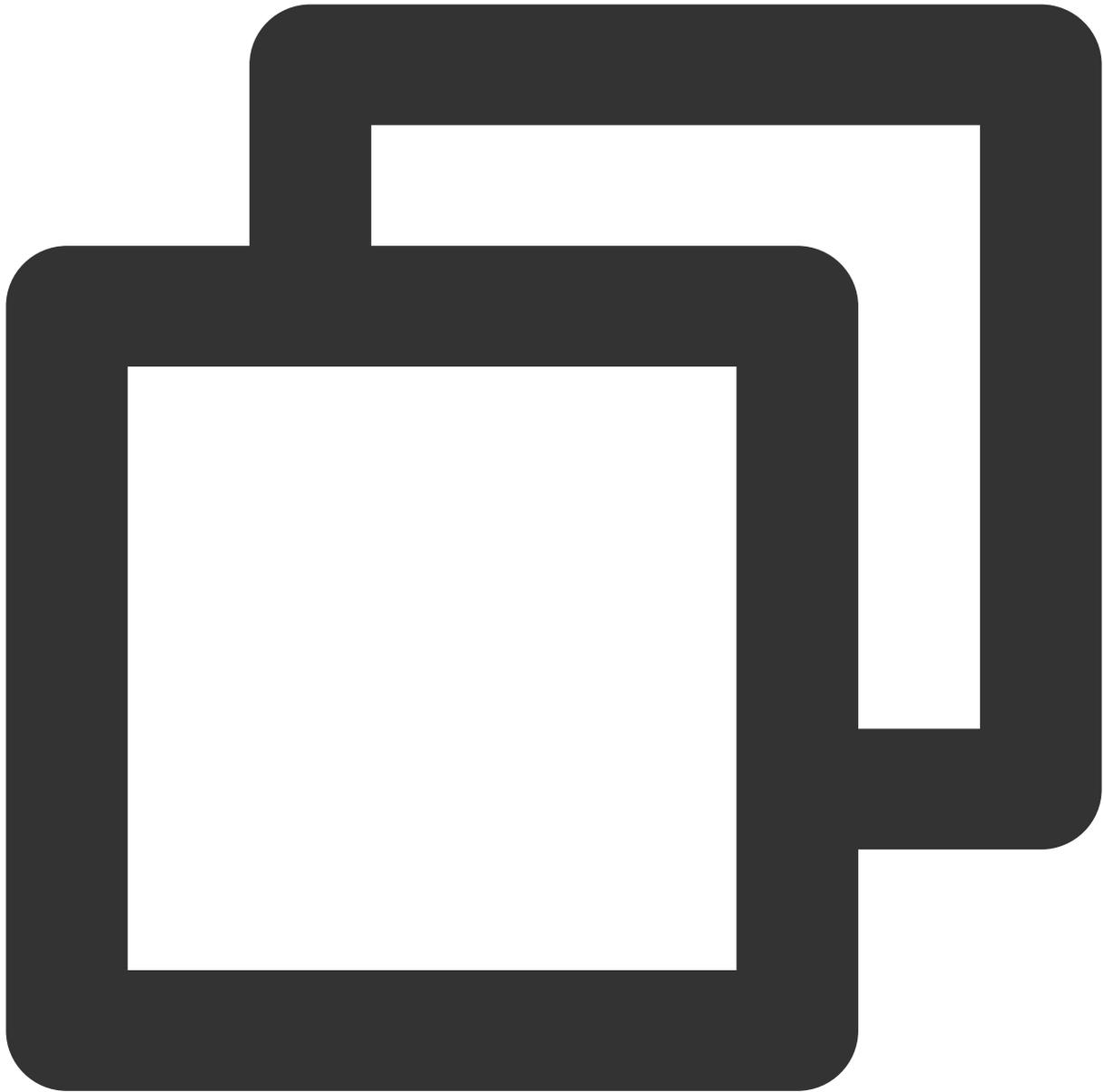
購入数：1台

## リクエストパラメータ



```
https://cvm.tencentcloudapi.com/?Action=RunInstances
&Placement.Zone=ap-guangzhou-3
&InstanceChargeType=SPOTPAID
&InstanceMarketOptions.MarketType=spot
&InstanceMarketOptions.SpotOptions.MaxPrice=0.0923
&InstanceMarketOptions.SpotOptions.SpotInstanceType=one-time
&ImageId=img-pmqg1cw7
&InstanceType=S2.MEDIUM4
&InstanceCount=1
&<パブリックリクエストパラメータ>
```

## リターンパラメータ



```
{
  "Response":{
    "InstanceIdSet": [
      "ins-1vogaxgk"
    ],
    "RequestId": "3c140219-cfe9-470e-b241-907877d6fb03"
  }
}
```

# スポットインスタンスの回収状態を確認する

最終更新日：：2023-04-12 11:00:46

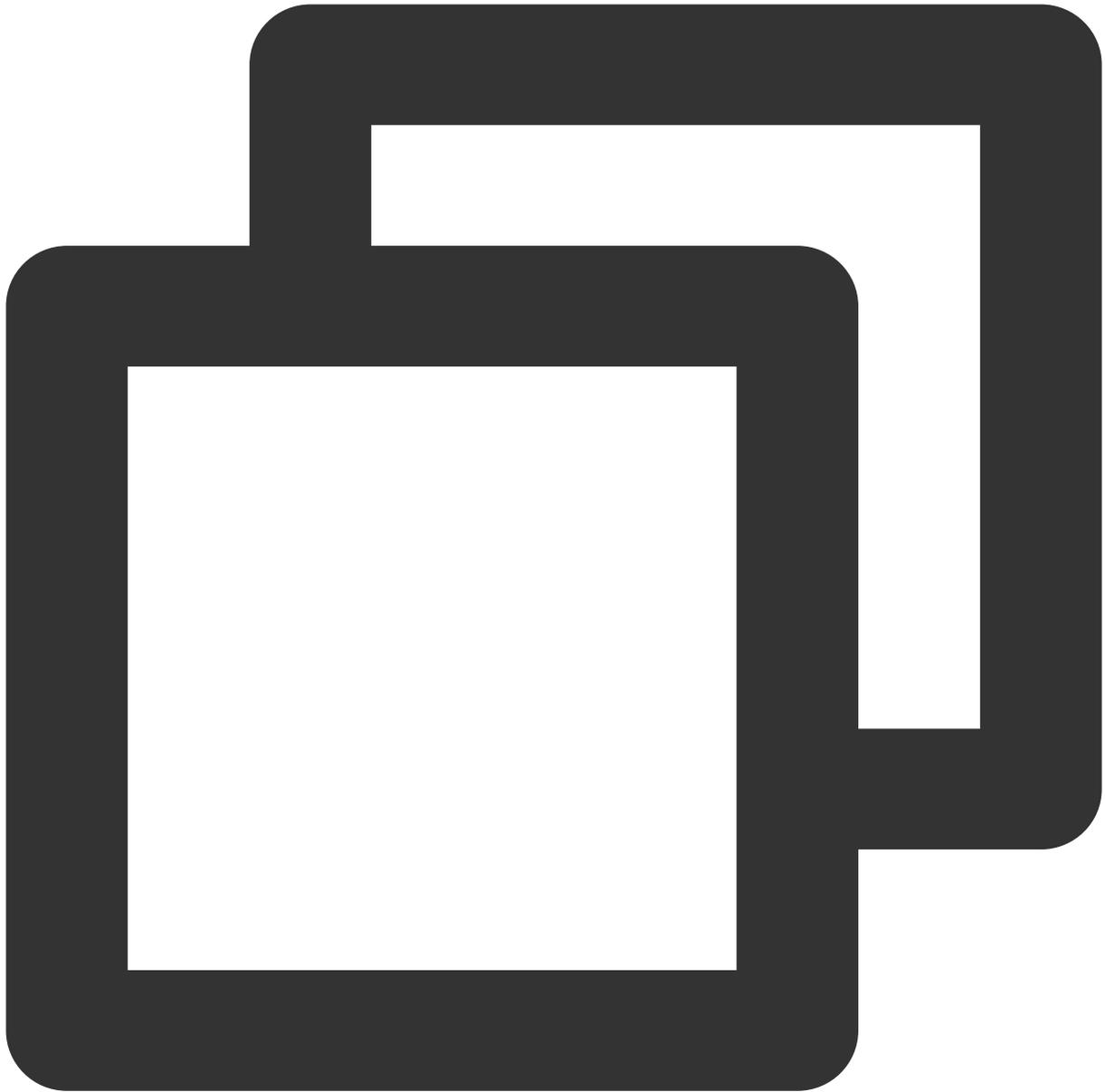
スポットインスタンスは、価格または在庫などの理由によりTencent Cloud によって自動的に回収されることがあります。インスタンスが回収される前にユーザーがカスタム操作を実行できるように、インスタンス内部からMetadata メカニズムを介して回収状態を取得するためのインターフェースが提供されています。詳細内容は下記の通りです。

## メタデータ

インスタンスメタデータは、インスタンスに関するデータで、実行中のインスタンスを設定または管理するために使用します。インスタンス内部からインスタンスメタデータにアクセスして取得できます。詳細については、[インスタンスメタデータの確認](#)をご参照ください。

## メタデータを介したスポットインスタンスの回収ステータス情報の取得

スポットインスタンスの回収状態に関する情報を取得するには、cURLツールまたはHTTP GETリクエストを介してメタデータにアクセスできます。

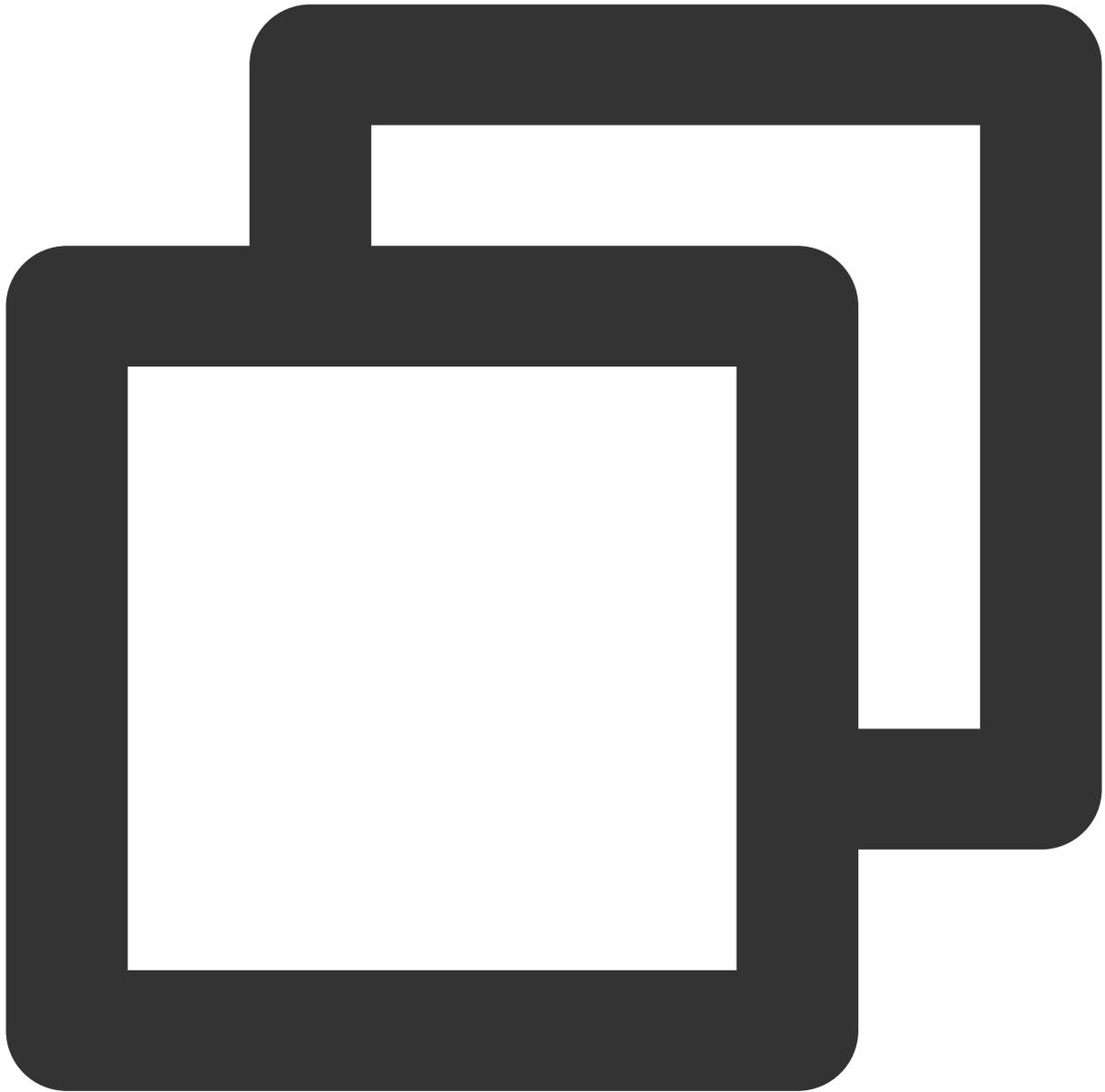


```
curl metadata.tencentyun.com/latest/meta-data/spot/termination-time
```

以下のような情報が返ってきた場合は、スポットインスタンスの回収時間を意味します。

**説明：**

スポットインスタンスのオペレーティングシステムによって設定された回収時間。タイムゾーンの標準はUTC+8です。



2018-08-18 12:05:33

404 not foundエラーが表示された場合、インスタンスがスポットインスタンスではないか、まだ回収をトリガーしていないことを意味します。

操作の詳細については、[インスタンスメタデータの確認](#)をご参照ください。

# 停止済み従量課金インスタンスの非課金化

最終更新日：：2023-05-10 15:32:34

## 概要

停止済みインスタンスの非課金化は、従量課金インスタンスはシャットダウン操作によって**シャットダウン**状態になった後、インスタンス（CPU、メモリ）の料金が請求されなくなり、クラウドディスク（システムディスクとデータディスク）、パブリックネットワーク帯域幅やイメージ等のコンポーネントは引き続き課金されます。

### ご注意：

[停止済みインスタンスの非課金化] 機能を有効にすると、インスタンスのCPU、メモリは**保存されない**、パブリックIPアドレスは**自動的にリリース**されます。その他機能、使用制限、および影響については、[停止済み従量課金インスタンスの非課金化](#)をご参照ください。

## 操作手順

### コンソールからインスタンスをシャットダウンする

1. [CVMコンソール](#) にログインします。

2. 実際のニーズに応じて、適切な操作方法を選択してください

単一インスタンスのシャットダウン：

2.1.1 シャットダウンするインスタンスを選択し、右側の操作欄で【さらに】>【インスタンス状態】>【シャットダウン】をクリックします。

2.1.2 **【停止済みインスタンスの非課金化】**を選択し、**【OK】**をクリックします。

インスタンスがこの機能をサポートしていない場合、インスタンスリストに「停止済みインスタンスの非課金化をサポートしていません」と表示されます。

複数インスタンスのシャットダウン：

2.1.1 シャットダウンするインスタンスをすべて選択し、リストの上部にある**【シャットダウン】**をクリックすると、インスタンスを一括シャットダウンできます。

シャットダウンできないインスタンスには原因が表示されます。

2.1.2 **【停止済みインスタンスの非課金化】**を選択し、**【OK】**をクリックします。

インスタンスがこの機能をサポートしていない場合、インスタンスリストに「停止済みインスタンスの非課金化をサポートしていません」と表示されます。

### APIを使ってインスタンスをシャットダウンする

StopInstances APIを使用してインスタンスをシャットダウンできます。詳細については、[StopInstances](#)をご参照ください。次のパラメータを追加します。

パラメータ名	選択 必須	タイプ	説明
StoppedMode	いい え	String	<p>「停止済みインスタンスの非課金化」機能は、従量課金制のインスタンスでのみ利用できます。</p> <p><b>有効な値:</b> KEEP_CHARGING：停止したインスタンスも引き続き課金されます。 STOP_CHARGING：停止したインスタンスには料金が発生しません。</p> <p><b>デフォルト値:</b> KEEP_CHARGING</p>

# インスタンスロールの管理

最終更新日：2022-03-16 16:54:44

## 操作シナリオ

CAM (Cloud Access Management) のロールは一組の権限を持つ仮想ロールで、Tencent Cloud中のサービスをダウンロードし、操作およびリソースのアクセス権限をロールに付与するために使用します。CAMのロールはCVMインスタンスに関連付けられ、インスタンス内でTencent Cloudセキュリティ証明書サービスSTSの一時キーに基づき他のクラウド製品のAPIにアクセスすることができます (一時キーは周期的に更新されます)。この方法を使用すると、直接SecretKeyを使用して権限制御を実行するのとは比べ、アカウント下のSecretKeyセキュリティの安全性が強化され、CAMの機能を活用して制限と権限付与をより緻密に管理することができます。

ここでは、インスタンスロールのバインド、変更および削除などの、インスタンスロールの管理方法について説明します。

## 機能のメリット

インスタンスのためにCAMのロールをバインドすると、以下の機能およびメリットが加わります。

STS一時キーを使用すると、Tencent Cloudの他のクラウドサービスにアクセスできます。

異なるインスタンスに異なる権限付与ポリシーが含まれるロールを付与すると、インスタンスは異なるクラウドリソースに対する異なるアクセス権限を持つことができ、より緻密な権限制御が実現します。

自分でインスタンス中にSecretKeyを保存する必要はありません。修正ロールの権限付与によって権限を変更することができ、インスタンスが備えているアクセス権限を迅速にメンテナンスすることができます。

## 利用説明

インスタンスは `cvm.qcloud.com` のロールを含むロールのバインドのみをサポートしています。詳細については、[ロールの基本概念](#) をご参照ください。

インスタンスのネットワークタイプは専用ネットワークVPCである必要があります。

1つのインスタンスは一度に1つのCAMロールの権限付与のみをサポートしています。

インスタンスロールをバインド、変更および削除しても、別料金は発生しません。

## 操作手順

### インスタンスロールのバインド/変更

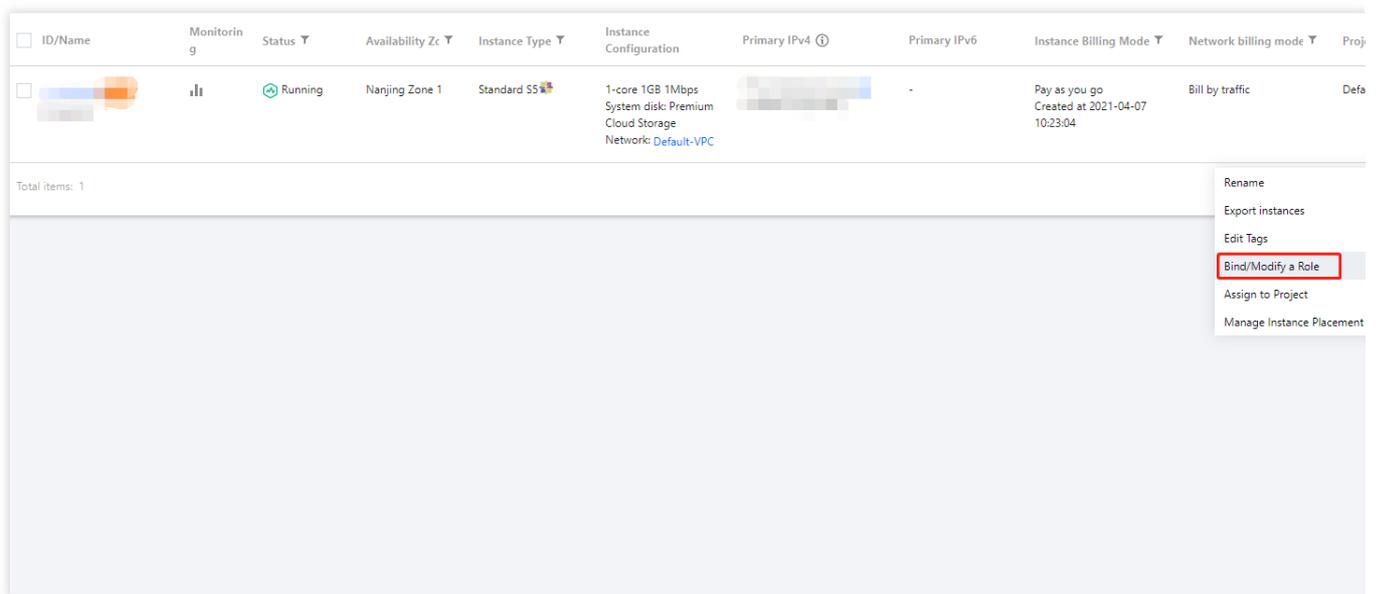
単一インスタンスロールのバインド/変更

複数インスタンスロールのバインド/変更

1. [CVMコンソール](#)にログインし、左側のナビゲーションバーで**インスタンス**を選択します。

2. インスタンスの管理画面で、実際に使用されているビューモードに従って操作します。

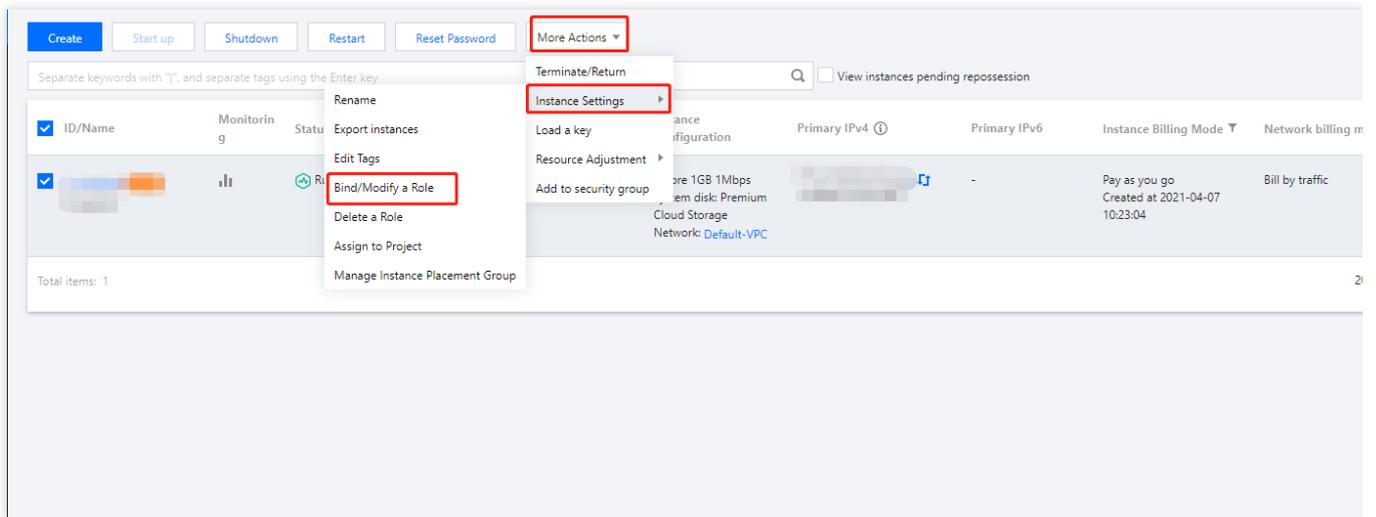
**リストビュー**：ロールをバインドまたは変更する必要があるCVMの行の右側にある**その他>インスタンス設定>ロールのバインド/変更**を選択します。下図のとおりです。



**タブビュー**：CVM画面で、画面の右上隅にある**その他>インスタンス設定>ロールのバインド/変更**を選択します。

3. ポップアップした「ロールのバインド/変更」ウィンドウで、バインドするロールを選択して、**OK**をクリックすれば完了です。

1. 「インスタンス」リスト画面で、ロールをバインドまたは変更する必要があるCVMにチェックを入れ、トップにある**その他の操作>インスタンス設定>ロールのバインド/変更**をクリックします。下図のとおりです。



2. ポップアップした「ロールのバインド/変更」ウィンドウで、バインドするロールを選択して、**OK**をクリックすれば完了です。

#### 説明：

この方法で変更された複数のインスタンスでは、ロールが同じになります。

## インスタンスロールの削除

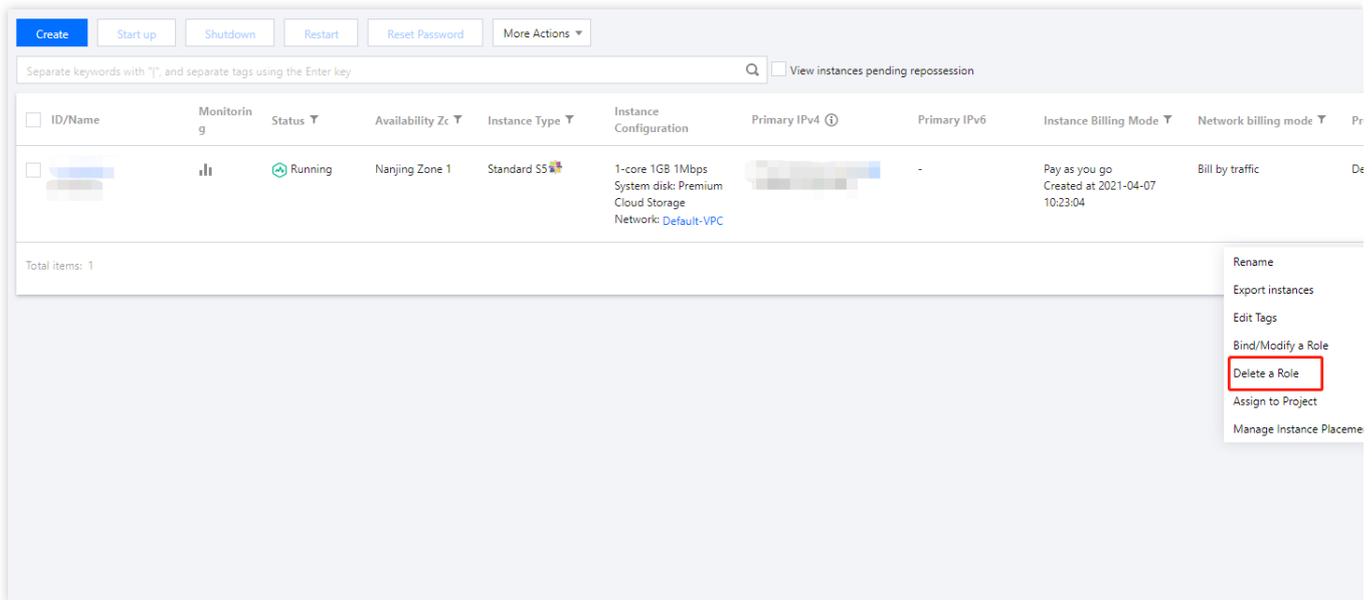
単一インスタンスロールの削除

複数インスタンスロールの削除

1. [CVMコンソール](#) にログインし、左側のナビゲーションバーで**インスタンス**を選択します。

2. インスタンスの管理画面で、実際に使用されているビューモードに従って操作します。

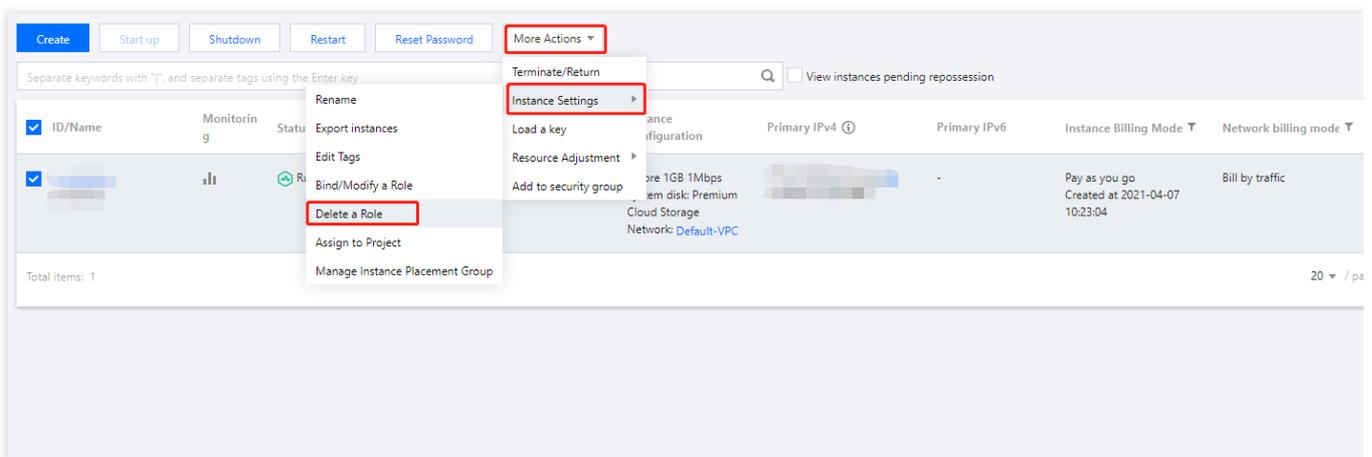
**リストビュー**：ロールを削除する必要があるCVMの行の右側にある**その他>インスタンス設定>ロールの削除**を選択します。下図のとおりです。



タブビュー：CVM画面で、画面の右上隅にある**その他の操作>インスタンス設定>ロールの削除**を選択します。

3. ポップアップした「ロールの削除」ウィンドウで、**OK**をクリックすれば完了です。

1. 「インスタンス」リスト画面で、ロールを削除する必要があるCVMにチェックを入れ、トップにある**その他の操作>インスタンス設定>ロールの削除**をクリックします。下図のとおりです。



2. ポップアップした「ロールの削除」ウィンドウで、**OK**をクリックすれば完了です。

# リザーブドインスタンス

## リザーブドインスタンスの分割

最終更新日：：2022-06-13 18:20:58

### 操作シナリオ

リザーブドインスタンスを使用する柔軟性を満たすために、リザーブドインスタンスを、対応する仕様の従量課金制インスタンスと一致する、より小さな **変換係数** の複数のリザーブドインスタンスに分割できます。

### リザーブドインスタンス分割のルールと制限

1c1g 1c2g 2c4g仕様のモデルは分割をサポートしません。

インスタンスサイズの変更をサポートしますが、インスタンスタイプの変更をサポートしません。

同じAvailability Zoneをサポートしますが、リザーブドインスタンスのリージョンまたはAvailability Zoneの変更をサポートしません。

ターゲットのリザーブドインスタンス変換係数の総数は、元のリザーブドインスタンス変換係数の総数と同じである必要があります。

分割を許可する前に、CPU：メモリの比率が同じであることを確認してください。

最大100の分割をサポートします。

### 操作手順

1. Cloud Virtual Machine (CVM)コンソールにログインします。
2. 左側ナビゲーションバーで、リザーブドインスタンスをクリックします。
3. リザーブドインスタンスのページで、分割するリザーブドインスタンスの操作列の下にある分割をクリックします。
4. リザーブドインスタンス分割のウィンドウで、新しく分割されたリザーブドインスタンス名を入力し、CPU、メモリ、およびインスタンスの数を選択します。

### 実行結果

分割操作が完了すると、元のリザーブドインスタンスの状態は**期限切れ**になり、生成された新しいリザーブドインスタンスの状態は**有効**になります。

## 用語の解釈

変換係数：インスタンスパフォーマンスの強みです。通常、vCPUの数によって異なり、リザーブドインスタンスの分割とマージに使用されます。変換係数=vCPUの数

変換係数の総数=インスタンスタイプの変換係数\*リザーブドインスタンスの数。分割/マージの前後で、変換係数の総数は同じである必要があります。

# リザーブドインスタンスのマージ

最終更新日：2022-06-13 18:20:58

## 操作シナリオ

リザーブドインスタンスを使用する柔軟性を満たすために、複数のリザーブドインスタンスを、対応する仕様の従量課金制インスタンスと一致する、より大きな **変換係数** の1つのリザーブドインスタンスにマージできます。

## リザーブドインスタンスマージのルールと制限

リザーブドインスタンスは**有効**の状態となっています。

リザーブドインスタンスは同じ**Availability Zone**にある必要があります。

リザーブドインスタンスの支払いタイプは同じです。

リザーブドインスタンスのOSプラットフォーム(Windows/linux)と終了時刻は同じである必要があります。

1c1g 1c2g 2c4g仕様のモデルはマージをサポートしません。

インスタンスサイズの変更をサポートしますが、インスタンスタイプファミリーの変更をサポートしません。

リザーブドインスタンスのリージョンまたは**Availability Zone**の変更をサポートしません。

ターゲットのリザーブドインスタンス変換係数の総数は、元のリザーブドインスタンス変換係数の総数と同じである必要があります。

マージを許可する前に、CPU：メモリの比率が同じであることを確認してください。

## 操作手順

1. Cloud Virtual Machine (CVM)コンソールにログインします。
2. 左側ナビゲーションバーで、リザーブドインスタンスをクリックします。
3. リザーブドインスタンスのページで、マージするリザーブドインスタンスの操作列の下にあるマージをクリックします。
4. リザーブドインスタンスマージのウィンドウで、マージされるリザーブドインスタンスを選択して、新しくマージされたリザーブドインスタンス名を入力します。

## 実行結果

マージ操作が完了すると、元のリザーブドインスタンスの状態は**期限切れ**になり、生成された新しいリザーブドインスタンスの状態は**有効**になります。

## 用語の解釈

変換係数：インスタンスパフォーマンスの強みです。通常、vCPUの数によって異なり、リザーブドインスタンスの分割とマージに使用されます。変換係数=vCPUの数

変換係数の総数=インスタンスタイプの変換係数\*リザーブドインスタンスの数。分割/マージの前後で、変換係数の総数は同じである必要があります。

# イメージ

## カスタムイメージの作成

最終更新日： : 2024-05-16 11:07:36

### 概要

Tencent Cloudが提供するパブリックイメージを使用するだけでなく、カスタムイメージを作成することもできます。カスタムイメージを作成した後、Tencent Cloudコンソールでこのイメージと同一構成のTencent Cloud CVMインスタンスをすばやく作成することができます。

#### 説明：

イメージの基盤となるデータストレージは、CBSスナップショットサービスを使用します。

カスタムイメージを作成する場合、デフォルトでイメージに関連付けられたスナップショットが作成されます。カスタムイメージを保持すると一定のスナップショット料金が発生します。詳細については、[Billing Overview](#) をご参照ください。

### 注意事項

各リージョンは、最大500個のカスタムイメージをサポートします。

Linuxインスタンスにデータディスクがあっても、システムディスクにのみイメージを作成する場合は、`/etc/fstab` にデータディスク構成が含まれていないことを確認してください。そうしないと、このイメージで作成したインスタンスを正常に起動できません。

イメージの作成には10分以上かかる場合があります。具体的な時間はインスタンスのデータサイズによって異なります。業務への影響を避けるためには、事前に関連準備を行ってください。

コンソールまたはAPIでCBMインスタンスを使用してカスタムイメージを作成することはできません。CVMインスタンスを使用してカスタムイメージを作成することができます。

Windowsインスタンスがドメインに参加し、ドメインアカウントを使用する必要がある場合は、カスタムイメージを作成する前に、Sysprep操作を実行し、インスタンスがドメイン参加後にSIDが一意になるようにしてください。詳細については、[Sysprepを実行してドメイン参加後のCVMの一意のSIDを確保](#) をご参照ください。

### 操作手順

コンソールからのカスタムイメージの作成

API経由でカスタムイメージの作成

## インスタンスのシャットダウン (オプション)

1. [CVMコンソール](#) にログインし、対応するインスタンスのシャットダウンが必要かどうかを確認します。

### ご注意：

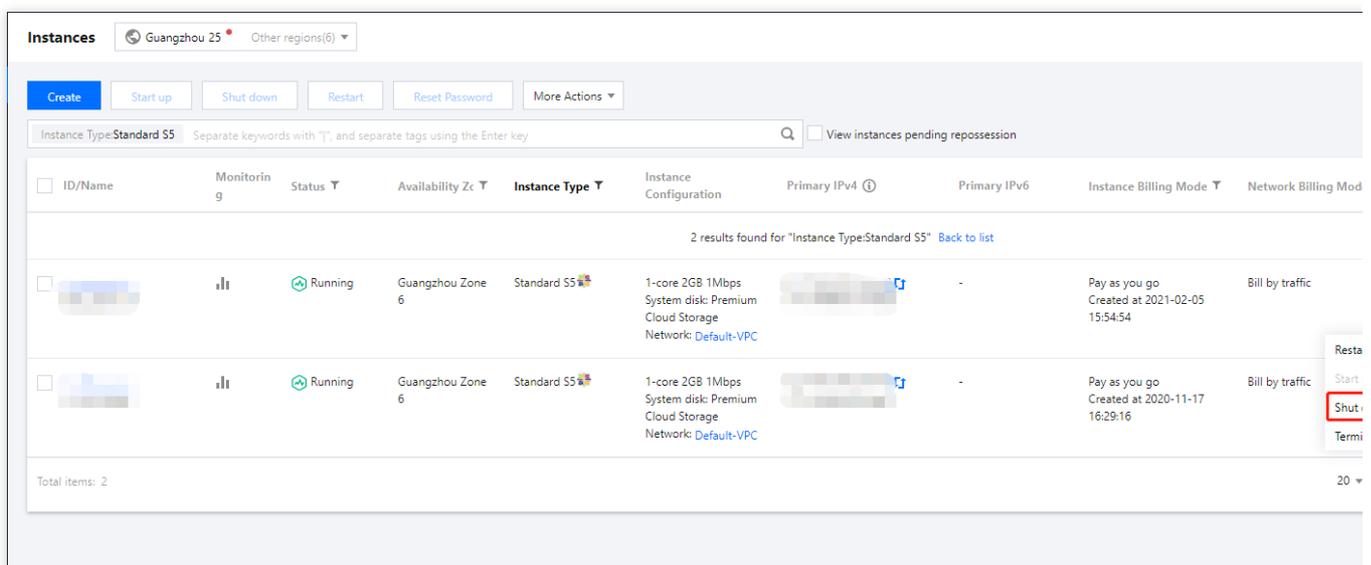
2018年7月以降にパブリックイメージを元に作成されたインスタンス（システムディスクはCBS）はオンラインイメージ制作（インスタンスをシャットダウンせずにイメージを制作すること）をサポートしています。これ以外でのインスタンスは、インスタンスをシャットダウンしてからイメージを制作し、イメージが現在のインスタンスデプロイ環境と完全に一致するようにしてください。

インスタンスをシャットダウンする必要がある場合は、次の手順に進みます。

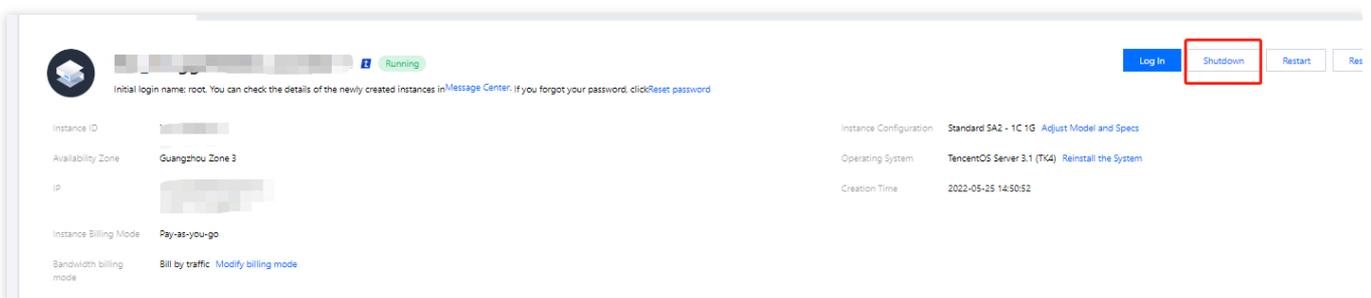
インスタンスをシャットダウンする必要がない場合は、[カスタムイメージの作成](#)に進んでください。

2. インスタンスの管理画面で、実際に使用されているビューモードに従って操作します。

**リストビュー：**下図に示すように、ターゲットインスタンスの行の右側にある **さらに > インスタンス状態\*** > **シャットダウン** をクリックします。



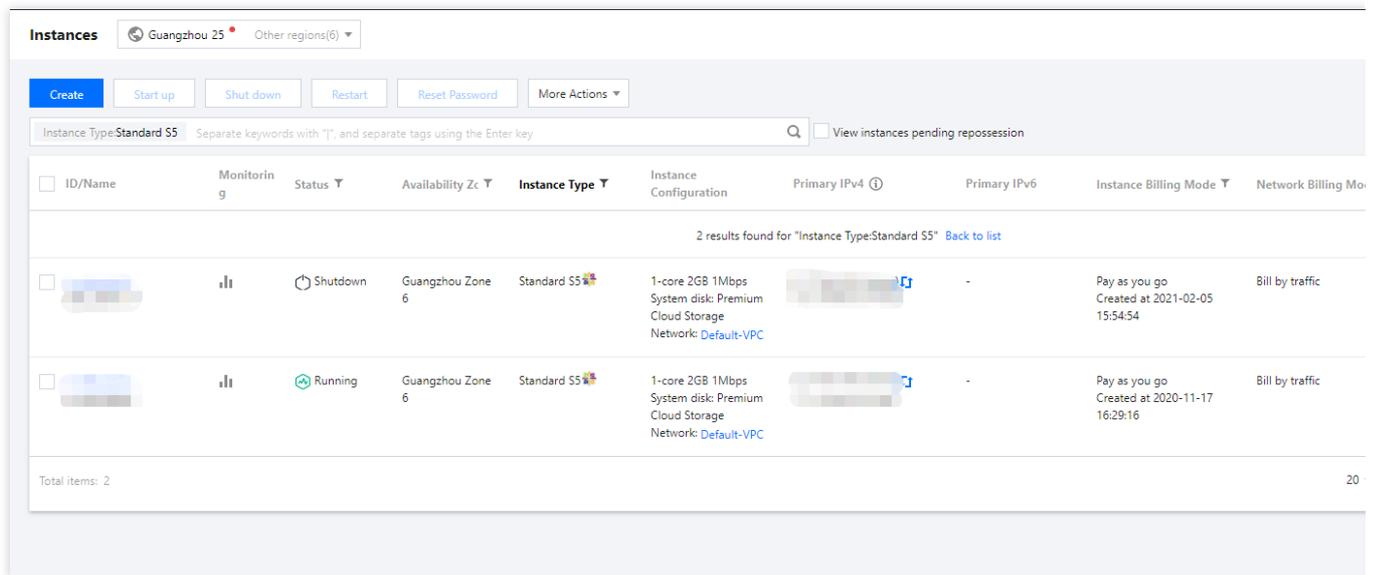
**タブビュー：**下図に示すように、インスタンス詳細ページで **シャットダウン** をクリックします。



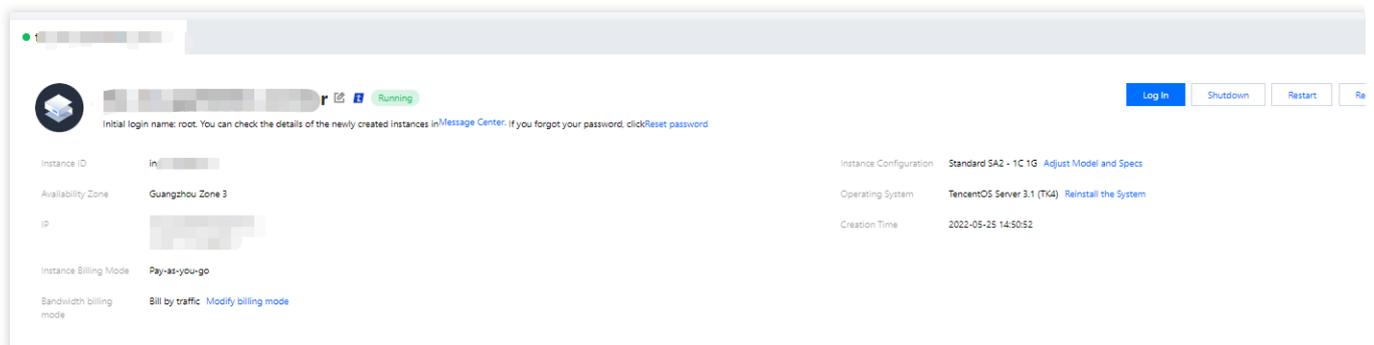
## カスタムイメージの作成

1. インスタンスの管理画面で、実際に使用されているビューモードに従って操作します。

リストビュー：ターゲットインスタンスの行の右側にあるさらに > **イメージの作成** をクリックします。下図に示すとおりです：



タブビュー：画面の右上隅にある**その他の操作 > イメージの作成** を選択します。下図に示すとおりです：



2. ポップアップ画面で構成を完了してください。

**イメージ名とイメージの説明**：名称と説明をカスタマイズします。

**タグ**：必要に応じてインスタンスのタグを追加できます。タグは、クラウドリソースの分類、検索、および集約に使用されます。詳細については、[タグ](#) をご参照ください。

**説明**：

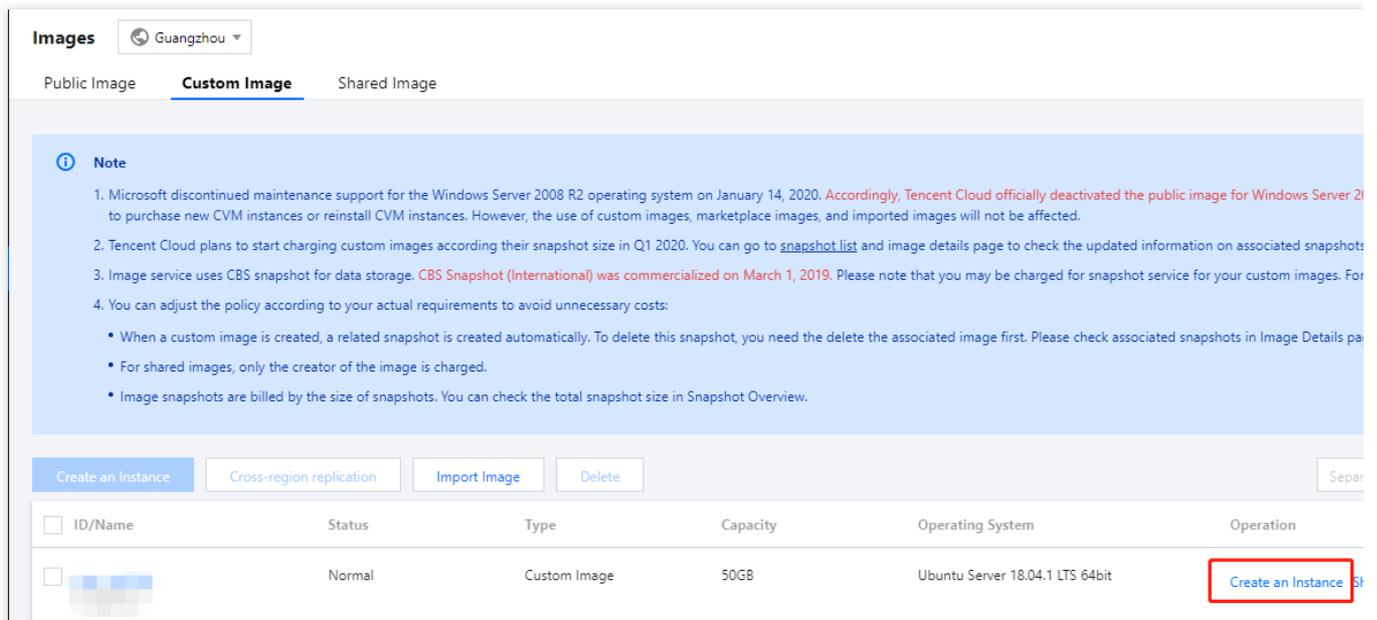
システムディスクとデータディスクを含むカスタムイメージを作成するには、[チケットを送信](#) してください。

3. イメージの作成をクリックすると、作成が完了します。

左側のナビゲーションバーで **イメージ** をクリックすると、「イメージ」ページでイメージの作成の進行状況を確認できます。

### カスタムイメージを利用したインスタンスの作成（オプション）

イメージの作成が完了すると、イメージリストで作成したイメージを選択し、右側にある**CVMインスタンスを作成** をクリックして、イメージと同じ構成のサーバーを購入できます。



**Images** Guangzhou

Public Image **Custom Image** Shared Image

**Note**

1. Microsoft discontinued maintenance support for the Windows Server 2008 R2 operating system on January 14, 2020. Accordingly, Tencent Cloud officially deactivated the public image for Windows Server 2008 R2 to purchase new CVM instances or reinstall CVM instances. However, the use of custom images, marketplace images, and imported images will not be affected.
2. Tencent Cloud plans to start charging custom images according to their snapshot size in Q1 2020. You can go to [snapshot list](#) and image details page to check the updated information on associated snapshots.
3. Image service uses CBS snapshot for data storage. **CBS Snapshot (International) was commercialized on March 1, 2019.** Please note that you may be charged for snapshot service for your custom images. For more information, see [CBS Snapshot \(International\)](#).
4. You can adjust the policy according to your actual requirements to avoid unnecessary costs:
  - When a custom image is created, a related snapshot is created automatically. To delete this snapshot, you need to delete the associated image first. Please check associated snapshots in Image Details page.
  - For shared images, only the creator of the image is charged.
  - Image snapshots are billed by the size of snapshots. You can check the total snapshot size in Snapshot Overview.

Create an Instance Cross-region replication Import Image Delete

ID/Name	Status	Type	Capacity	Operating System	Operation
	Normal	Custom Image	50GB	Ubuntu Server 18.04.1 LTS 64bit	Create an Instance

CreateImage APIを使用してカスタムイメージを作成することができます。詳細については、[CreateImage](#)をご参照ください。

## ベストプラクティス

### データディスク上のデータ移行

新しいインスタンスを起動する同時に、元のインスタンスのデータディスクのデータを保持する必要がある場合、最初にデータディスクの [スナップショット](#) を作成してください。新しいインスタンスを起動する時に、このデータディスクのスナップショットを使用して新しいCBSデータディスクを作成します。

詳細については、[スナップショットを使用してクラウドディスクの作成](#)をご参照ください。

# カスタムイメージの共有

最終更新日：2024-05-16 10:48:25

## 概要

**共有イメージ**とは、ご自分で作成済みの **カスタムイメージ** を他の **Tencent Cloud アカウント** と共有することをいいます。他の Tencent Cloud アカウントから共有イメージを手軽に取得し、そこから必要なコンポーネントを取得して、カスタムコンテンツを追加することができます。

### ご注意：

Tencent Cloud はその他の Tencent Cloud アカウントの共有イメージの整合性またはセキュリティを保証することはできません。ソース元が確かな共有イメージのみ、使用されることをお勧めします。

## 注意事項

イメージごとに最大500のTencent Cloudアカウントと共有することができます。

共有イメージは名前や説明を変更することはできません。CVMのインスタンス作成時、またはインスタンスシステムの再ストール時のみ使用できます。

その他のTencent Cloudアカウントに共有したイメージは、自身のイメージクォータを占有しません。

その他のTencent Cloudアカウントに共有したイメージは削除できますが、先にこのイメージのすべての共有を取り消す必要があります。共有を取り消す操作については、**カスタムイメージの共有を取り消す** をご参照ください。取得した共有イメージは削除できません。

イメージは、Tencent Cloudアカウントが同じリージョン内の相手との共有をサポートしています。異なるリージョンの相手と共有する場合は、先にイメージを異なるリージョンにコピーしてから、共有する必要があります。取得した共有イメージを、さらに別のTencent Cloudアカウントに共有することはできません。

## 操作手順

### ルートアカウントのアカウントIDの取得

Tencent Cloudの共有イメージは、相手側端末のルートアカウントの一意のIDによって識別されます。次の方法で、ルートアカウントのアカウントIDを取得するように相手に通知することができます。

1. **CVMコンソール** にログインします。
2. 右上隅のアカウント名をクリックし、**アカウント情報** を選択します。
3. 「アカウント情報」管理ページで、ルートアカウントのアカウントIDを確認および記録します。
4. 取得したアカウントIDを自分に送信するように相手に通知します。

## 共有イメージ

コンソールによる共有

API による共有

1. CVMコンソールにログインし、左側のナビゲーションバーで **イメージ** を選択します。
2. **カスタムイメージ** タブを選択し、カスタムイメージ管理ページに進みます。
3. カスタムイメージリストで、共有したいカスタムイメージを選択し、右側の **共有** をクリックします。
4. 表示された「共有イメージ」ウィンドウで、相手ルートアカウントのアカウントIDを入力し、**共有** をクリックします。
5. **CVMコンソール** にログインし、**イメージ** > **共有イメージ** を選択して、共有したイメージを確認できることを相手に通知します。

複数のTencent Cloudアカウントに共有したい場合は、上記の手順を繰り返してください。

ModifyImageSharePermissionインターフェースを使用して、イメージを共有することができます。詳細については [ModifyImageSharePermission](#) をご参照ください。

## 関連する操作

### Lighthouseとのイメージ共有

Lighthouseとのカスタムイメージの共有、またはLighthouseのカスタムイメージのCVMとの共有によって、サービスの高速なオフライン移行を実現できます。共有済みのイメージを使用して、インスタンスをすばやく作成し、必要なコンポーネントを取得したり、そこからカスタムコンテンツを追加したりすることもできます。

# カスタマイズイメージの共有を取り消す

最終更新日：2022-04-14 15:17:59

## ユースケース

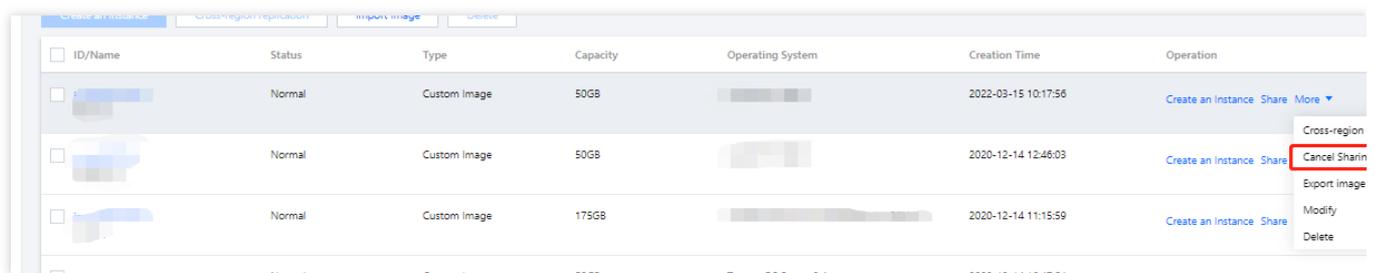
このドキュメントは、共有カスタマイズイメージを解除する方法を説明します。ユーザーはほかのユーザーと共有されているイメージの共有状態をいつでも終了でき、ほかのユーザーと共有しないことを決定できます。この操作はほかのユーザーがこの共有イメージを利用して作成したインスタンスに影響しませんが、他のユーザーがこのイメージを確認したり、このイメージを利用して新しいインスタンスを作成したりすることができません。

## 操作手順

コンソールを利用して共有を解除する

APIを利用して共有を解除する

1. CVMコンソールにログインします。左側ナビゲーションバーで、**イメージ**をクリックします。
2. **カスタマイズイメージ**タブを選択して、カスタマイズイメージ管理画面に入ります。
3. カスタマイズイメージリストから、共有を解除するカスタマイズイメージを選択して、**その他 > 共有を解除する**をクリックします。



4. 新しい画面で、解除する対向側アカウントの唯一IDを選択して、**共有を解除する**をクリックします。確認した後、イメージ共有の解除を完了します。

ModifyImageSharePermission インターフェースを利用して、共有イメージを解除できます。詳細については、[イメージ共有情報の修正](#)をご参照ください。

# カスタムイメージの削除

最終更新日：：2023-05-10 16:13:56

## ユースケース

このドキュメントでは、カスタムイメージを削除する方法について説明します。

## 注意事項

カスタムイメージを削除する前に、次の点に注意してください。

カスタムイメージを削除すると、それを使用して新しいCVMインスタンスを作成することはできなくなります。既に起動されているインスタンスには影響しません。このイメージから起動されたすべてのインスタンスを削除する場合は、[インスタンスの回収](#) または [インスタンスの終了/リリース](#) をご参照ください。

他のユーザーと共有されているカスタムイメージは削除できません。削除する前にすべての共有を解除する必要があります。詳細については、[カスタムイメージの共有解除方法](#) をご参照ください。

カスタムイメージのみを削除できます。パブリックイメージと共有イメージは削除できません。

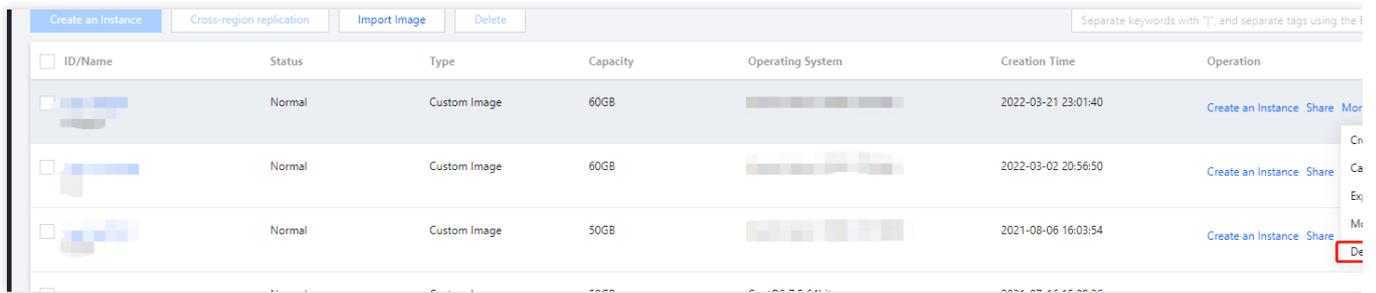
## 操作手順

コンソールからイメージを削除する

API経由でイメージを削除する

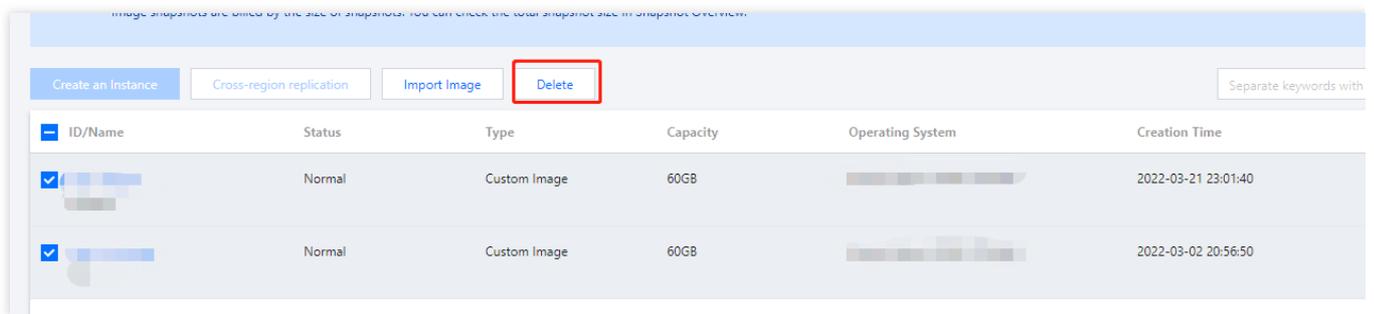
1. CVMコンソールにログインします。左側のナビゲーションバーで [イメージ](#) をクリックします。
2. [カスタムイメージ](#) タブを選択して、カスタムイメージ管理ページに進みます。
3. 実際のニーズに基づいてカスタムイメージを削除する方法を選択します。

**単一のイメージの削除**：イメージリストで削除するカスタムイメージを見つけて、**さらに > 削除** をクリックします。



ID/Name	Status	Type	Capacity	Operating System	Creation Time	Operation
[Redacted]	Normal	Custom Image	60GB	[Redacted]	2022-03-21 23:01:40	Create an Instance Share More
[Redacted]	Normal	Custom Image	60GB	[Redacted]	2022-03-02 20:56:50	Create an Instance Share More
[Redacted]	Normal	Custom Image	50GB	[Redacted]	2021-08-06 16:03:54	Create an Instance Share More

複数のイメージの削除：イメージリストで削除するすべてのカスタムイメージを選択し、上部の**削除**をクリックします。



ID/Name	Status	Type	Capacity	Operating System	Creation Time
[Redacted]	Normal	Custom Image	60GB	[Redacted]	2022-03-21 23:01:40
[Redacted]	Normal	Custom Image	60GB	[Redacted]	2022-03-02 20:56:50

4. [OK] をクリックします。

削除できない場合は、理由が表示されます。

ユーザーはDeleteImagesインターフェースを使用してイメージを削除します。詳細については、[イメージの削除](#)をご参照ください。

# イメージのコピー

最終更新日：2023-04-25 18:14:48

## コピーの概要

### 一般的な手順

イメージのコピーには、**カスタムイメージ - クロスリージョンレプリケーション**と**共有イメージ - 同一リージョンレプリケーション**の2つの機能が含まれています。

イメージコピー機能	利点	説明
カスタムイメージ - クロスリージョンレプリケーション	ユーザーが <b>クロスリージョン</b> で同じCVMインスタンスをすばやくデプロイできるようにします	クロスリージョンでカスタムイメージをコピーし、そのイメージを新しいリージョンにコピーしてCVMを作成できます
共有イメージ - 同一リージョンレプリケーション	ユーザーが共有イメージをカスタムイメージにコピーできるようにします。より柔軟に使用できます	コピーされたカスタムイメージには特別な制限はなく、他のカスタムイメージの機能を備えています

### コピーの説明

カスタムイメージは、クロスリージョンレプリケーションをサポートします。共有イメージは、同一リージョンレプリケーションをサポートします。

#### リージョン制限：

中国本土リージョン、その他の国および地域内でのイメージコピーをサポートしています。中国本土リージョンから他の国および地域にイメージをコピーしたい場合、または他の国および地域から中国本土リージョンにイメージをコピーしたい場合は、[チケットを提出](#)してください。

イメージコピーの機能自体は、無料で使うことができますが、コピーされたカスタムイメージを保持するために一定のスナップショット料金が発生します。

イメージのコピーは10分から30分かかります。

イメージ全体は現在、クロスリージョンレプリケーションをサポートしていません。

## コピーの方法

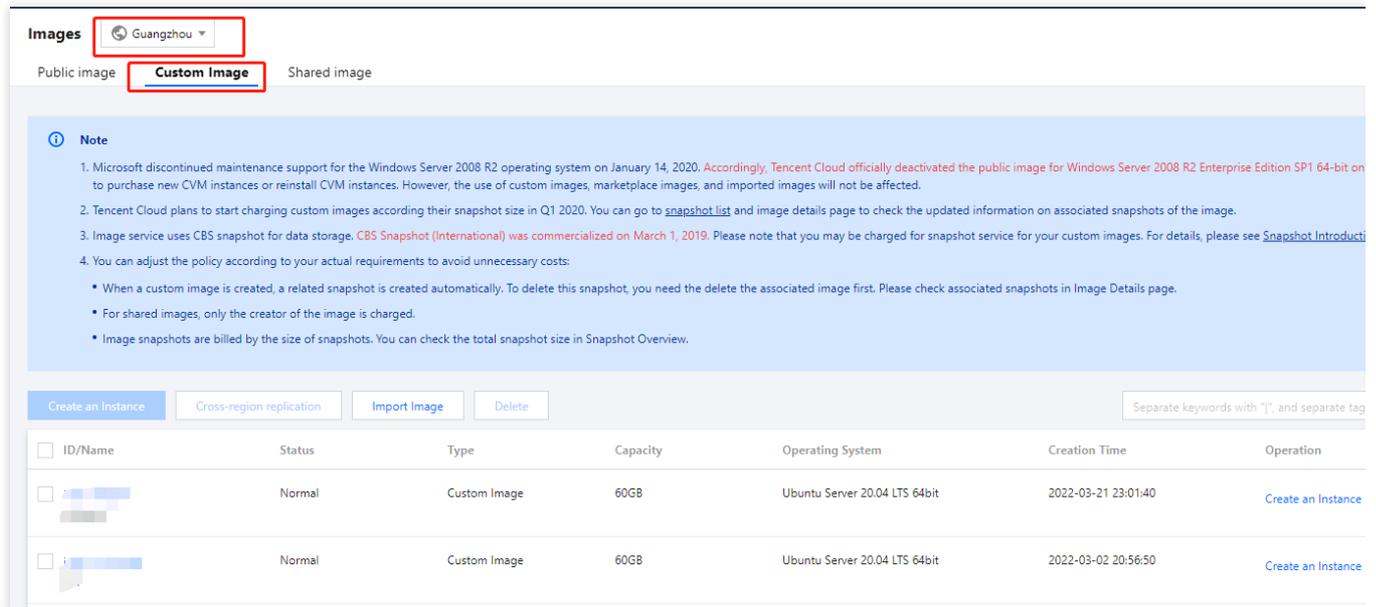
### カスタムイメージ-クロスリージョンレプリケーション

コンソール経由でイメージをコピーする

API経由でイメージをコピーする

1. [CVMコンソール](#) にログインします。
2. 左側のナビゲーションメニューで、[イメージ](#) をクリックして、イメージ管理画面に入ります。
3. コピーしたい元のイメージが存在するリージョンを選択して、[カスタムイメージタブ](#) をクリックします。下図に示すとおりです：

例えば、広州リージョンを選択します。



4. イメージをコピーする必要があるインスタンスを見つけて、画面右側のメニューからさらに [> クロスリージョンレプリケーション](#) をクリックします。
  5. コピー先のリージョンを選択し、**OK** をクリックします。  
コピーが成功すると、コピー先のリージョンのイメージリストに、同じ名前で異なるIDのイメージが表示されます。
  6. コピー先のリージョンに切り替えて、そのリージョンのイメージリストに、コピーされたイメージを選択し、[インスタンスの作成](#) をクリックして同じのCVMインスタンスを作成できます。
- [Synclmages](#) インターフェースを使用してイメージをコピーすることができます。詳細については、[Synclmages](#) をご参照ください。

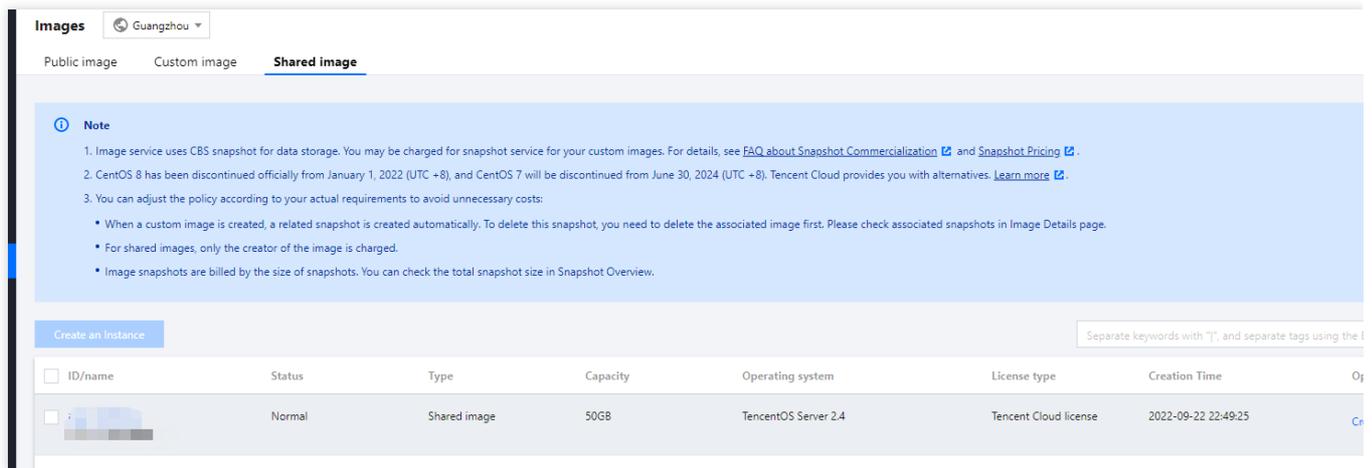
## 共有イメージ - 同一リージョンレプリケーション

コンソール経由でイメージをコピーする

API を使用してイメージをコピーする

1. [CVMコンソール](#) にログインします。
2. 左側のナビゲーションメニューで、[イメージ](#) をクリックして、イメージ管理画面に入ります。
3. コピーしたい元のイメージが存在するリージョンを選択して、[共有イメージタブ](#) をクリックします。下図に示すとおりです：

例えば、広州リージョンを選択します。



4. イメージをコピーする必要があるインスタンスを見つけて、画面右側のメニューからさらに > 同一リージョンレプリケーションをクリックします。

5. コピー先のリージョンを選択し、**OK**をクリックします。

コピーが成功すると、コピー先のリージョンのイメージリストに、同じ名前で異なるIDのイメージが表示されます。

6. カスタムイメージタブを切り替えて、コピーされたイメージを選択し、**インスタンスの作成**をクリックして同じのCVMインスタンスを作成できます。コピーされたカスタムイメージには特別な制限はなく、他のカスタムイメージの機能を備えています。

Synclmagesインターフェースを使用してイメージをコピーすることができます。詳細については、[Synclmages](#)をご参照ください。

# イメージのインポート

## イメージのインポートの概要

最終更新日：：2023-04-03 12:06:12

[カスタマイズイメージの作成](#) 機能を使用する以外に、Tencent Cloudはインポート機能もサポートしています。ローカルまたは他のプラットフォームのサーバーのシステムディスクにあるイメージファイルをCloud Virtual Machine (CVM) のカスタマイズイメージにインポートできます。イメージをインポートした後、それを使用してCVMを作成したり、既存のCVMシステムをリインストールしたりできます。

## インポートの準備

事前にインポート要件を満たすイメージファイルを準備してください。

Linuxシステムタイプのイメージ制限

Windowsシステムタイプのイメージ制限

イメージ属性	条件
OS	CentOS、CentOS Stream、Ubuntu、Debian、OpenSUSE、CoreOS、FreeBSD、AlmaLinux、Rocky Linux、Fedora、Kylin、UnionTech、TencentOSリリースバージョンに基づくイメージです。 32ビットと64ビットの両方のOSがサポートされています。
イメージ形式	RAW、VHD、QCOW2、VMDKのイメージ形式をサポートします。 <code>qemu-img info imageName   grep 'file format'</code> を利用してイメージ形式を確認します。
ファイルシステムのタイプ	GPTパーティションはサポートされていません。
イメージのサイズ	イメージの実際のサイズは50Gを超えることはできません。 <code>qemu-img info imageName   grep 'disk size'</code> を利用して、イメージの実際のサイズを確認します。 イメージのvsizeは500Gを超えることはできません。 <code>qemu-img info imageName   grep 'virtual size'</code> を利用して、イメージのvsizeを確認します。 注記： イメージをインポートする時のサイズはQCOW2形式に変換したイメージ情報に準じます。
ネットワーク	デフォルトでは、Tencent Cloudはインスタンスにeth0ネットワークインターフェースを提供します。

	ユーザーはインスタンスのmetadataサービスを使用して、インスタンスのネットワーク設定を確認できます。詳細については、 <a href="#">インスタンスのメタデータをご参照ください</a> 。
ドライバー	イメージに仮想化プラットフォームKVMのVirtioドライバーをインストールする必要があります。詳細については、 <a href="#">LinuxでのVirtioドライバーの確認</a> をご参照ください。 イメージにcloudinitをインストールする必要があります。詳細については、 <a href="#">Linuxでのイメージインポートによるcloudinitのインストール</a> をご参照ください。 他の原因で、イメージにcloudinitをインストールできない場合、 <a href="#">イメージの強制インポート</a> を参照して、自分でインスタンスを設定してください。
カーネルの制限	イメージにはネイティブカーネルが推奨されます。カーネルを変更すると、イメージをCVMにインポートできなくなる場合があります。
地域の制限	現在、上海金融区、深セン金融区では、その他の地域のCloud Object Storage (COS) サービスからのイメージのインポートをサポートしていません。

イメージ属性	条件
OS	Windows Server 2008関連バージョン、Windows Server 2012関連バージョン、Windows Server 2016関連バージョン、Windows Server 2019関連バージョン、Windows Server 2022関連バージョン 32ビットと64ビットの両方のOSがサポートされています。
イメージ形式	RAW、VHD、QCOW2、VMDKのイメージ形式をサポートします。 <code>qemu-img info imageName   grep 'file format'</code> を利用してイメージ形式を確認します。
ファイルシステムのタイプ	MBRパーティションを使用するNTFSファイルシステムのみをサポートします。 GPTパーティションをサポートしません。 ロジックボリュームマネージャー (LVM) をサポートしません。
イメージのサイズ	イメージの実際のサイズは50Gを超えることはできません。 <code>qemu-img info imageName   grep 'disk size'</code> を利用して、イメージの実際のサイズを確認します。 イメージのvsizeは500Gを超えることはできません。 <code>qemu-img info imageName   grep 'virtual size'</code> を利用して、イメージのvsizeを確認します。 注記： イメージをインポートする時のサイズはQCOW2形式に変換したイメージ情報に準じます。

ネットワーク	デフォルトでは、Tencent Cloudはインスタンスにローカルエリア接続ネットワークインターフェースを提供します。 ユーザーはインスタンスのmetadataサービスを使用して、インスタンスのネットワーク設定を確認できます。詳細については、 <a href="#">インスタンスメタデータ</a> をご参照ください。
ドライバ	イメージにはバーチャル化プラットフォームKVMのVirtioドライバーをインストールする必要があります。WindowsシステムにはデフォルトでVirtioドライバーがインストールされていませんが、ユーザーはWindows Virtioドライバーをインストールして、ローカルイメージをエクスポートすることができます。Windows Virtioドライバーのダウンロードアドレスは次のとおりです。実際のネットワーク環境に応じてダウンロードしてください。 パブリックネットワークダウンロードアドレス： <a href="http://mirrors.tencent.com/install/windows/virtio_64_1.0.9.exe">http://mirrors.tencent.com/install/windows/virtio_64_1.0.9.exe</a> プライベートネットワークダウンロードアドレス： <a href="http://mirrors.tencentyun.com/install/windows/virtio_64_1.0.9.exe">http://mirrors.tencentyun.com/install/windows/virtio_64_1.0.9.exe</a>
地域の制限	現在、上海金融区、深セン金融区では、その他の地域のCOSサービスからのイメージのインポートをサポートしていません。
その他	インポートされたWindowsシステムイメージは、 <a href="#">Windowsアクティベーション</a> サービスを提供しません。

## インポート手順

1. **CVM** コンソールにログインし、左側ナビゲーションバーの **イメージ** をクリックします。
2. **カスタマイズイメージ** を選択し、**イメージのインポート** をクリックします。
3. 操作インターフェースの要件に基づき、まず **COSのアクティブ化**、次に **bucketの作成** を実行し、イメージファイルをbucketに **オブジェクトのアップロード** して、**イメージファイルURLの取得** を実行します。
4. **次のステップへ** をクリックします。
5. 実際の状況に応じて、リストを記入し、**インポート開始** をクリックします。

### ご注意：

入力したCOSのURLが正確であることを確認してください。

インポートの成功または失敗は、いずれも **内部メッセージ** の形式で通知されます。

## インポートに失敗する

コンソールでイメージのインポート操作を実行した後、何らかの理由でタスクが失敗する場合があります。タスクが失敗した場合は、以下の内容に基づいて問題のトラブルシューティングを行います。

## 注意事項

このドキュメントによって、失敗の原因をトラブルシューティングする前に、[内部メッセージの管理ページ](#)のメッセージサブスクリプションで製品サービスに関連する通知をサブスクリプションしていることを確保します。これにより、失敗の原因を含む内部メッセージ、SMS、および電子メールを確実に受信することができます。

### ご注意：

メッセージセンターで製品サービスに関連する情報をサブスクリプションしないと、インポートに成功/失敗する内部メッセージを受信できません。

## トラブルシューティング

次の内容を参考に、対応するエラー情報のトラブルシューティングを実行することができます。具体的なエラープロンプトとエラーの説明については、[エラーコード](#)をご参照ください。

### InvalidUrl：COSリンクの無効

InvalidUrlエラーが発生します。エラーメッセージ：イメージのインポートページに間違ったCOSリンクが記入されています。次の原因が考えられます：

入力したイメージリンクは [Tencent Cloud COS](#) のイメージリンクではありません。

COSのオブジェクトアドレスにはパブリック読み取り権限、プライベート書き込み権限がありません。

COSファイルのアクセス権限はプライベート読み取りですが、署名の有効期限が切れています。

### ご注意：

署名のあるCOSファイルのリンクには一度しかアクセスできません。

海外地域でイメージをインポートする場合、別の地域からのCOSリンクが使用されます。

### ご注意：

現在、海外地域からインポートされたイメージサービスは、同一地域のCOSサーバーのみをサポートします。つまり、同一地域のCOSリンクを使用してインポートしてください。

ユーザーのイメージファイルが削除されました。

COSリンクが無効であるというエラーメッセージが表示された場合、上記の原因に基づいて問題のトラブルシューティングを行います。

### InvalidFormatSize：形式またはサイズの条件は不適合である

InvalidFormatSizeエラーが発生します。エラーメッセージ：事前にインポートされるイメージの形式またはサイズは、Tencent Cloudのイメージインポート機能の制限を満たしません。制限は以下の通りです：

イメージのインポートは `qcow2`、`vhd`、`vmdk`、`raw` という4種類の形式のイメージファイルをサポートしています。

イメージをインポートするファイルの実際のサイズが50GB（`qcow2`形式に変換したイメージファイルに基づく）を超えることはできません。

イメージをインポートするシステムディスクのサイズが500GBを超えることはできません。

イメージの形式またはサイズの条件が不適合であるというエラーメッセージを受信した場合：

[Linuxイメージの作成](#) に記載しているイメージ形式の変換内容に基づいて、イメージファイルを適切なファイル形式に変換し、イメージ内容を簡素化して、サイズの制限を満たしてからイメージを再インポートします。

[オフラインインスタンス移行](#) 機能を利用してインスタンスを移行することもできます。この機能は最大500GBのイメージファイル移行をサポートしています。

**VirtioNotInstall** : Virtioドライバーの未インストール

**VirtioNotInstall**エラーが発生します。エラーメッセージ：事前にインポートされたイメージにはVirtioドライバーがインストールされていません。Tencent CloudがKVM仮想化テクノロジーを利用して、ユーザーがインポートしたイメージにVirtioドライバーがインストールされている必要があります。一部のユーザーがカスタマイズされたLinux OSを除き、ほとんどのLinux OSには既にVirtioドライバーがインストールされています。Windows OSでは、ユーザーはVirtioドライバーを手動でインストールしてください：

Linuxイメージのインポートについては、ドキュメント [Linux OSでのVirtioドライバーの確認](#) をご参照ください。

Windowsイメージのインポートについては、ドキュメント [Windowsイメージの作成](#) を参照して、Virtioドライバーをインストールしてください。

**CloudInitNotInstalled** : cloud-initプログラムの未インストール

**CloudInitNotInstalled**エラーが発生します。エラーメッセージ：事前にインポートされたイメージにcloud-initプログラムがインストールされていません。Tencent Cloudはオープンソースプログラムcloud-initを利用してCVMの初期化を実行するため、cloud-initプログラムがインストールされていない場合、CVMの初期化に失敗することがあります。

Linuxイメージのインポートについては、ドキュメント [Linux OSへのcloud-initのインストール](#) をご参照ください。

Windowsイメージのインポートについては、ドキュメント [Windows OSへのcloudbase-initのインストール](#) をご参照ください。

cloud-init/cloudbase-initをインストールした後、関連ドキュメントに従って構成ファイルを置き換えて、CVMを起動する時に正しいデータソースからデータを取得できます。

**PartitionNotPresent** : パーティション情報の損失

**PartitionNotPresent**エラーが発生します。エラーメッセージ：インポートされたイメージは不完全です。この場合は、イメージの作成時にブートパーティションが含まれているかどうかを確認してください。

**RootPartitionNotFound** : ルートパーティションの損失

**RootPartitionNotFound**エラーが発生します。エラーメッセージ：インポートしたイメージにはルートパーティションを含むことが検出されていません。この場合は、イメージファイルを確認してください。考えられる原因は次のとおりです：

インストールパッケージファイルがアップロードされました。

データディスクイメージがアップロードされました。

ブートパーティションイメージがアップロードされました。

間違ったファイルがアップロードされました。

**InternalError** : 未知のエラー

**InternalError**が発生します。エラーメッセージ：イメージインポートサービスにはエラーの原因が記録されていません。この場合は、弊社カスタマーサービスまでご連絡ください。技術担当者が顧客の問題をできるだけ早く解決するお手伝いをします。

## エラーコード

エラーコード	エラーの原因	推奨される解決策
InvalidUrl	無効なCOSリンク	COSリンクはインポートされたイメージリンクと同じであるかどうかを確認します。
InvalidFormatSize	形式またはサイズの条件は不適合です	イメージは <b>インポートの準備</b> 中の <b>イメージの形式</b> と <b>イメージのサイズ</b> の制限を満たす必要があります。
VirtioNotInstall	virtioドライバーがインストールされていません	イメージにvirtioドライバーをインストールする必要があります。 <b>インポートの準備</b> 中のドライバー部分をご参照ください。
PartitionNotPresent	パーティションの情報が見つかりません	イメージの作成方法が間違っているため、イメージが破損する可能性があります
CloudInitNotInstalled	cloud-initがインストールされていません	Linuxイメージにcloud-initをインストールする必要があります。 <b>インポートの準備</b> 中の <b>ドライバー</b> 部分をご参照ください。
RootPartitionNotFound	ルートパーティションが検出されていません	イメージの作成方法が間違っているため、イメージが破損する可能性があります
InternalError	他のエラー	カスタマサービスにお問い合わせください

# イメージの強制インポート

最終更新日：：2023-06-15 14:57:10

## 操作シナリオ

ユーザーのLinuxイメージはある原因で [cloudinitのインストール](#) できなくなった場合は、**強制的にイメージをインポートする**機能を使用してインポートを完成させます。ユーザーが強制的にイメージをインポートする場合、Tencent CloudはユーザーのCVMに対して初期化を設定できなくなります。ユーザーはTencent Cloudが提供している設定ファイルに基づいてスクリプトを設定してCVMを設定する必要があります。このドキュメントは強制的にイメージをインポートしてCVMを設定する方法について説明します。

## 制限条件

[イメージのインポート](#) 時、Linux イメージをインポートする制限（cloudinit 以外）を満たす必要があります。

インポートしたイメージのOSパーティションが残っています。

インポートしたイメージはリモート利用可能な脆弱性が存在できません。

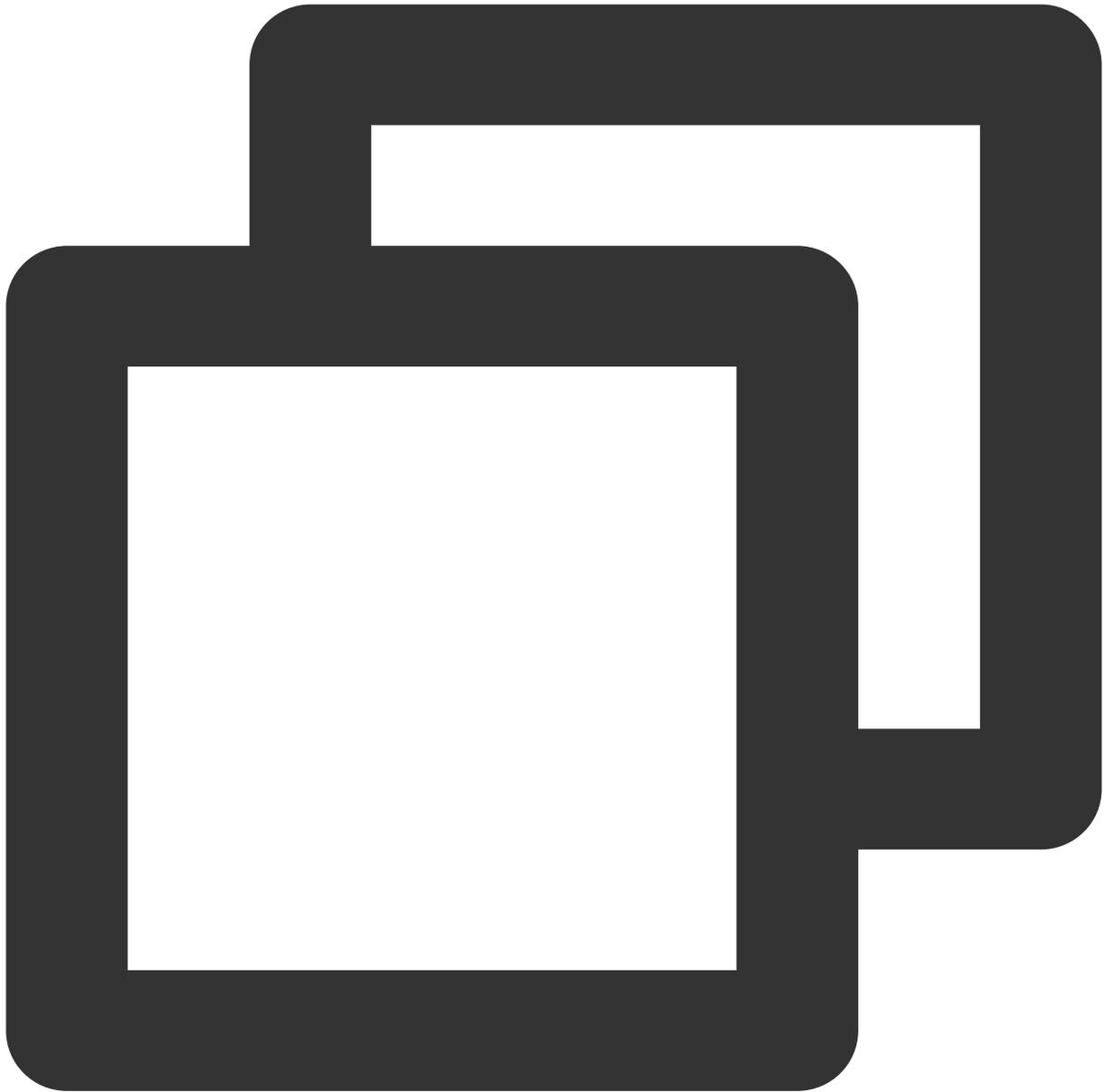
イメージを強制的にインポートして、インスタンスが成功に作成した後にユーザーがパスワードを変更することをお勧めします。

## 操作手順

ユーザーが強制的にイメージをインポートする時に、cloudinitを使用していないため、自動的に設定することができません。Tencent Cloudは設定情報を含むcdromデバイスを提供して、ユーザーが自分で設定できます。ユーザーはcdromをマウントする必要があり、`mount_point/qcloud_action/os.conf` 情報を読み取って設定します。ユーザーはほかの設定データとUserDataを利用するニーズがある場合、直接 `mount_point/` 配下のファイルを読み取ることができます。

### 設定ファイルos.confの内容

os.conf の基本内容は以下のようになります：



```
hostname=VM_10_20_xxxx  
password=GRSgae1fw9frsG.rfrF  
eth0_ip_addr=10.104.62.201  
eth0_mac_addr=52:54:00:E1:96:EB  
eth0_netmask=255.255.192.0  
eth0_gateway=10.104.0.1  
dns_nameserver="10.138.224.65 10.182.20.26 10.182.24.12"
```

**説明：**

以上の情報はパラメータ名のみ参考する意味があり、パラメータ値は単なる事例になります。

os.conf に各パラメータの意味は以下の通り：

パラメータ名	パラメータ意味
hostname	ホスト名
password	暗号化したパスワード
eth0_ip_addr	eth0 ENIのLAN IP
eth0_mac_addr	eth0 ENIの MAC アドレス
eth0_netmask	eth0 ENIのサブネットマスク
eth0_gateway	eth0 ENIのゲートウェイ
dns_nameserver	DNS 解析サーバー

## 設定スクリプトの解析

### 注意事項

スクリプトはスタートアップする時、自動的に実行されます、OSのタイプに基づいてこの要件を実現してください。

スクリプトは `/dev/cdrom` をマウントする必要がある、マウントポイントの `qcloud_action/os.conf` ファイルを読み取って、設定情報を取得します。

Tencent Cloudが `cdrom` に入力したパスワードは暗号化されたパスワードであり、ユーザーは `chpasswd -e` 方式を使用して設定します。

**暗号化されたパスワードには特別な文字が含まれる可能性があります、まずファイルの中に入力してから、**

**`chpasswd -e < passwd_file` 方式で設定することを推奨します。**

強制的にイメージをインポートして作成したインスタンスを使用して再びイメージを作成する時に、インスタンスを正確に設定することを保証するために、スクリプトが実行されることを確認する必要があります。インスタンスの中でcloudinitをインストールすることもできます。

### 事例

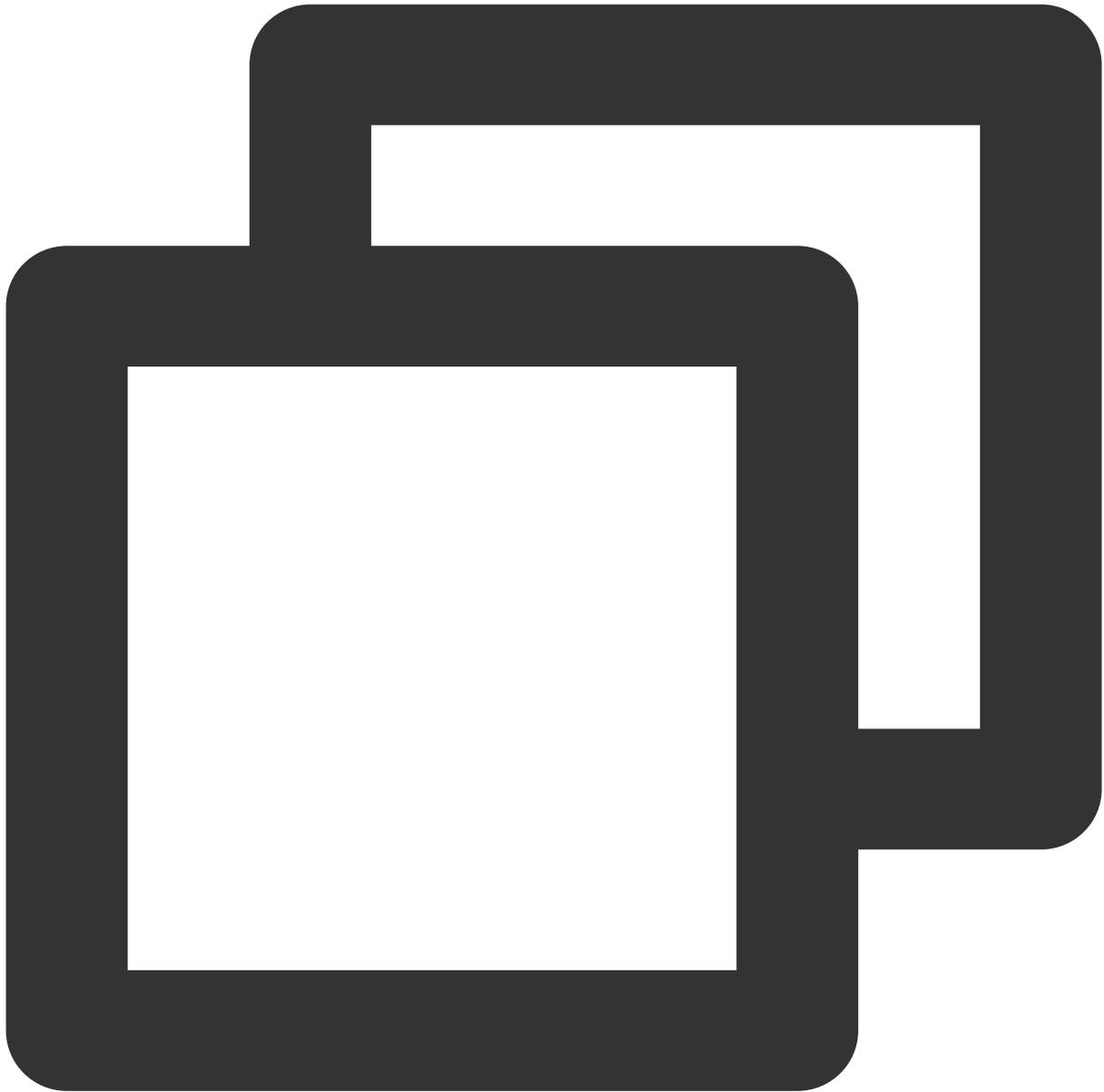
Tencent CloudはCentOSに基づいてサンプルスクリプトを提供します。ユーザーはサンプルスクリプトに基づいて、独自のイメージ設定スクリプトを作成できます。作成中、以下の点を注意してください：

**イメージをインポートする前にこのスクリプトをOSに正しく設置する必要があります。**

このスクリプトは全てのOSに適しているのではなく、ユーザーは自分のOSに応じて修正する必要があります。

1. 以下スクリプトを例として、`os_config` スクリプトを作成する。

ユーザーは実際状況に応じて `os_config` スクリプトを修正します。

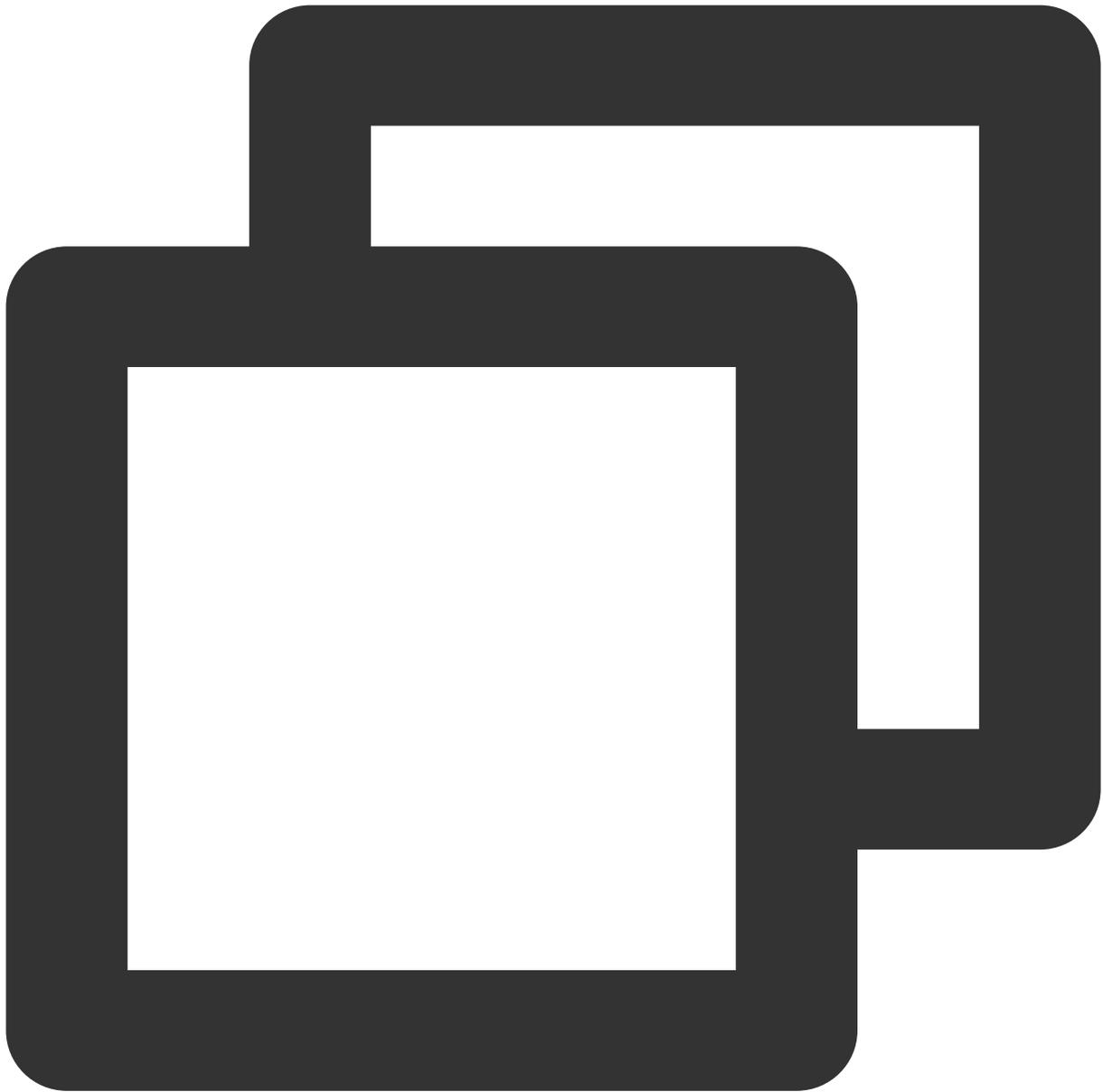


```
#!/bin/bash
### BEGIN INIT INFO
# Provides:          os-config
# Required-Start:    $local_fs $network $named $remote_fs
# Required-Stop:
# Should-Stop:
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: config of os-init job
# Description:       run the config phase without cloud-init
### END INIT INFO
```

```
#####user settings#####
cdrom_path=`blkid -L config-2`
load_os_config() {
    mount_path=$(mktemp -d /mnt/tmp.XXXX)
    mount /dev/cdrom $mount_path
    if [[ -f $mount_path/qcloud_action/os.conf ]]; then
        . $mount_path/qcloud_action/os.conf
        if [[ -n $password ]]; then
            passwd_file=$(mktemp /mnt/pass.XXXX)
            passwd_line=$(grep password $mount_path/qcloud_action/os.conf)
            echo root:${passwd_line#*=} > $passwd_file
        fi
        return 0
    else
        return 1
    fi
}
cleanup() {
    umount /dev/cdrom
    if [[ -f $passwd_file ]]; then
        echo $passwd_file
        rm -f $passwd_file
    fi
    if [[ -d $mount_path ]]; then
        echo $mount_path
        rm -rf $mount_path
    fi
}
config_password() {
    if [[ -f $passwd_file ]]; then
        chpasswd -e < $passwd_file
    fi
}
config_hostname(){
    if [[ -n $hostname ]]; then
        sed -i "/^HOSTNAME=.*d" /etc/sysconfig/network
        echo "HOSTNAME=$hostname" >> /etc/sysconfig/network
    fi
}
config_dns() {
    if [[ -n $dns_nameserver ]]; then
        dns_conf=/etc/resolv.conf
        sed -i '/^nameserver.*d' $dns_conf
        for i in $dns_nameserver; do
            echo "nameserver $i" >> $dns_conf
        done
    fi
}
```

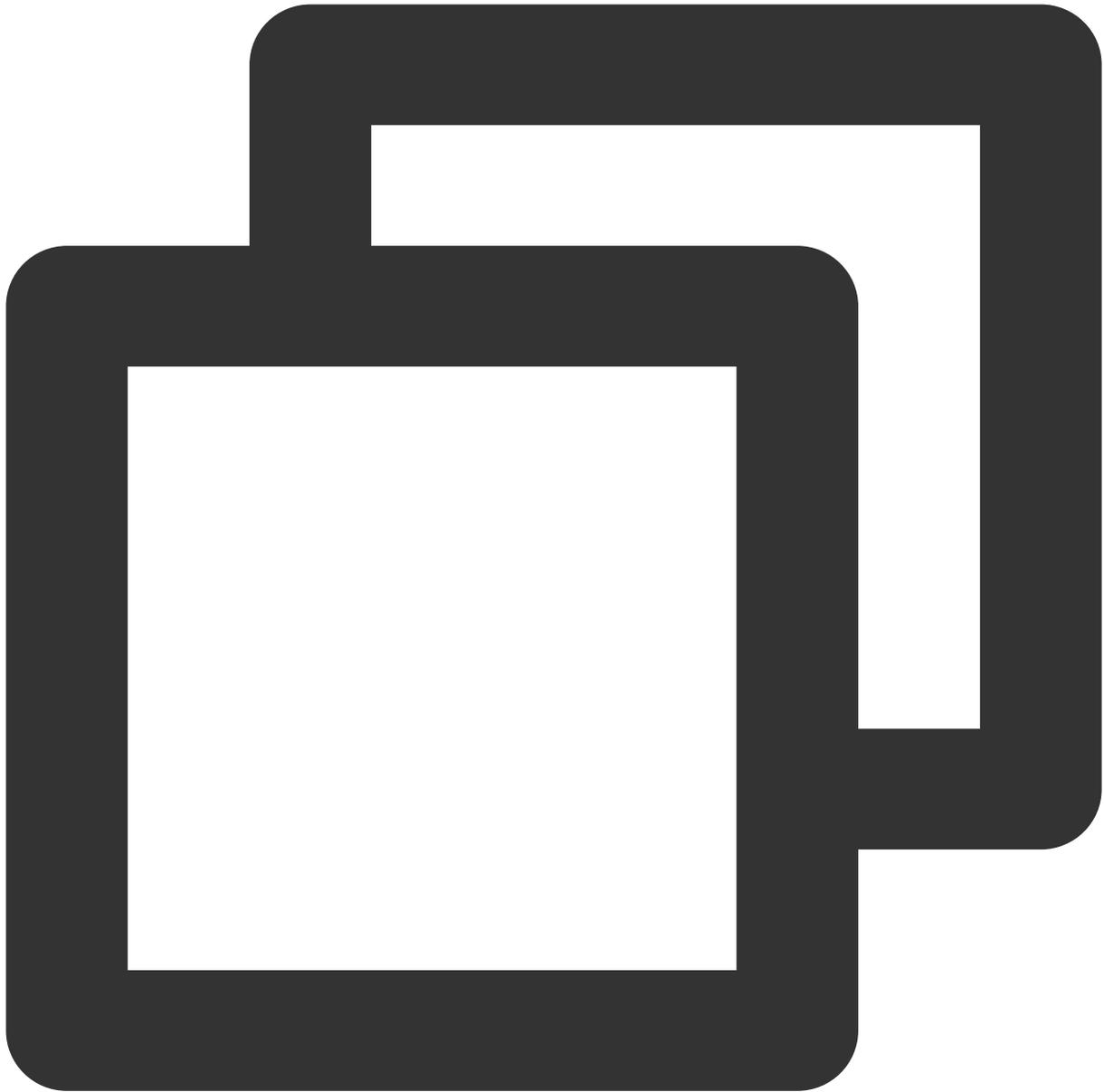
```
}
config_network() {
    /etc/init.d/network stop
    cat << EOF > /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
IPADDR=$eth0_ip_addr
NETMASK=$eth0_netmask
HWADDR=$eth0_mac_addr
ONBOOT=yes
GATEWAY=$eth0_gateway
BOOTPROTO=static
EOF
    if [[ -n $hostname ]]; then
        sed -i "/^${eth0_ip_addr}.*\/d" /etc/hosts
        echo "${eth0_ip_addr} $hostname" >> /etc/hosts
    fi
    /etc/init.d/network start
}
config_gateway() {
    sed -i "s/^GATEWAY=.*\/GATEWAY=$eth0_gateway" /etc/sysconfig/network
}
#####init#####
start() {
    if load_os_config ; then
        config_password
        config_hostname
        config_dns
        config_network
        cleanup
        exit 0
    else
        echo "mount ${cdrom_path} failed"
        exit 1
    fi
}
RETVAL=0
case "$1" in
start)
    start
    RETVAL=$?
;;
*)
    echo "Usage: $0 {start}"
    RETVAL=3
;;
esac
exit $RETVAL
```

2. `/etc/init.d/` ディレクトリに `os_config` スクリプトを設置して、以下のコマンドを実行します。



```
chmod +x /etc/init.d/os_config  
chkconfig --add os_config
```

3. 以下のコマンドを実行し、`os_config` は起動サービスに追加されたかどうかを確認します。



```
chkconfig --list
```

**説明：**

ユーザーはスクリプトが正しく実行されたことを確認する必要があります。イメージをインポートした後、SSHを利用してインスタンスへの接続ができなかったり、ネットワークに接続できなかった場合、コンソールを利用してインスタンスに接続し、スクリプトを再実行して、問題をトラブルシューティングしてください。それでも処理できない場合は、カスタマーサービスにお問い合わせください。

# イメージのエクスポート

最終更新日：：2023-06-25 17:49:49

## 概要

Tencent Cloudは作成済みのカスタムイメージの **COS** バケット内へのエクスポートをサポートしています。この機能によって必要なイメージをエクスポートすることができます。

## 前提条件

**COSコンソール** ですでにCOSサービスをアクティブ化していること。

エクスポートするカスタムイメージが存在するリージョンでバケットを作成済みであること。詳細については、[バケットの作成](#) をご参照ください。

## 注意事項

**Windows** イメージなどの商用イメージをエクスポートすることはできません。

カスタムイメージのシステムディスクおよびデータディスク1枚あたりの容量は500GBを超えることはできません。

CVMインスタンス全体のイメージをエクスポートする場合、CVMインスタンスには5つを超えるデータディスクを含めることはできません。

## 料金

CVMとCOSなどの他のサービスを同時に使用する場合は、実際に使用するサービスの課金ルールに従って料金が計算されます。

料金詳細は以下の通りです：

シナリオ	料金	説明ドキュメント
イメージをCOSバケットにエクス	ストレージ料金。イメージをCOSバケットに保存すると、ストレージ料金が発生します。COSはオブジェクトサイズを計算し、ターゲットオブジェクトのストレージタイプとリージョンに基づいて料金が請求されます。	<a href="#">ストレージ料金</a>

ポートする	リクエスト料金。イメージをCOSバケットにエクスポートすると、書き込みリクエストの料金が発生します。COSは書き込みリクエストの回数を計算し、それに応じて料金が請求されます。	リクエスト料金
	トラフィック料金。イメージをCOSバケットにエクスポートすると、アップストリームトラフィックが発生します。COSはトラフィック量を計算します。プライベートネットワークのアップストリームトラフィックとパブリックネットワークのアップストリームトラフィックは無料です。	トラフィック料金
COSバケットからイメージをダウンロードする	リクエスト料金。COSバケットからイメージをダウンロードすると、書き込みリクエストの料金が発生します。COSは書き込みリクエストの回数を計算し、それに応じて料金が請求されます。	リクエスト料金
	トラフィック料金。COSバケットからイメージをダウンロードすると、ダウンストリームトラフィックが発生します。COSはトラフィック量を計算します。プライベートネットワークのダウンストリームトラフィックは無料ですが、パブリックネットワークのダウンストリームトラフィックは有料です。	流量費用

## 操作手順

1. CVMコンソールにログインし、左側のナビゲーションバーで **イメージ** をクリックします。
2. 「イメージ」 ページの上方で、エクスポートするカスタムイメージが存在するリージョンを選択し、**カスタムイメージ** タブをクリックします。
3. 下図に示すように、エクスポートするイメージを見つけて、画面右のメニューから **さらに > イメージのエクスポート** をクリックします。
4. 「イメージのエクスポート」 画面が表示され、この画面で次の設定を行います。下図のように：

### Export image

**Steps to export an image**

1. You need to activate COS object storage service; [Cloud Object Storage](#)
2. Create a COS Bucket in advance in the region where the image is located; [Bucket](#)
3. Please make sure that you've allowed CVM to access COS; [Access Management](#)

Image Name	1234
Region	Chongqing
System platform	TencentOS
Architecture	x86_64
Operating System	TencentOS Server 2.4
COS Bucket	<input type="text" value="Select Bucket"/> ⓘ Please select a COS Bucket
Prefix of the files to export	<input type="text" value="1234"/> ⓘ Please enter the prefix of files to be exported
	<input checked="" type="checkbox"/> Agree to authorize CVM to access my COS Bucket

**COS Bucket** : エクスポートするイメージが存在するバケットを選択します。バケットがエクスポートするイメージと同じリージョンにあることを確認してください。

**エクスポートファイルのプレフィックス名** : エクスポートファイルのプレフィックス名をカスタマイズします。

「CVMに私のCOS Bucketへのアクセス権限を付与することに同意します」にチェックを入れます。

5. **OK**をクリックすると、イメージのエクスポートを開始します。

6. ポップアップウィンドウで**OK**をクリックします。

エクスポートにかかる時間は、イメージファイルのサイズとエクスポートタスクキューの長さによって異なりますので、しばらくお待ちください。エクスポートタスクが完了すると、イメージファイルはターゲットバケット内に保存されます。 [バケットリスト](#) ページに進み、ターゲットバケットIDをクリックしてバケットの詳細ページに移動できます。バケットの詳細ページで、 `カスタムプレフィックス名_xvda.raw` という名前のファイルがエクスポートされたイメージファイルになります。

## よくある質問

### 1. COSのパブリックネットワークのダウンストリームトラフィックはどのようにして発生され、請求されますか。

パブリックネットワークのダウンストリームトラフィックとは、インターネットを通じてデータをCOSからクライアントに転送する際に発生するトラフィックを指します。ユーザーが**オブジェクトリンク**からオブジェクトを直接ダウンロードした場合、または**静的Webサイトのエンドポイント**を介してオブジェクトを閲覧した場合に発生するトラフィックがパブリックネットワークダウンストリームトラフィックに該当し、それに対応する料金がパブリックネットワークダウンストリームトラフィック料金です。請求の詳細については、[課金項目](#) および [製品価格](#) のページに掲載しておりますので、ご覧ください。

### 2. COSコンソール、ツール、API、SDKなどの方式でファイルをダウンロードした場合、パブリックネットワークのダウンストリームトラフィック料金は発生しますか。

COS へのアクセスによって生成されるトラフィック（プライベートネットワークトラフィックまたはパブリックネットワークトラフィック）はご利用の方式に関係なく、同一リージョンのクラウド製品からCOSにアクセスする場合にのみ、デフォルトでプライベートネットワークを使用するため、パブリックネットワークのダウンストリームトラフィック料金は発生しません。プライベートネットワークアクセスを識別する方法の詳細については、[プライベートネットワークとパブリックネットワークアクセス](#) のページに掲載しておりますので、ご覧ください。

### 3. COSはパブリックネットワークトラフィックをどのように区別していますか。

パブリックネットワークのダウンストリームトラフィックとは、インターネットを通じてデータをCOSからクライアントに転送する際に発生するトラフィックを指します。例えば、COSに保存されているファイルをCOSコンソール経由でダウンロードする場合、ツールによってオブジェクトへのアクセスやダウンロードを行う場合、またはブラウザを使用してオブジェクトのプレビューを行う場合、オブジェクトアドレスまたはカスタムドメイン名を使用してオブジェクトにアクセスおよびダウンロードを行う場合などは、いずれもパブリックネットワークのダウンストリームトラフィックが発生します。詳細については、[プライベートネットワークとパブリックネットワークアクセスの判断](#) のページに掲載しておりますので、ご覧ください。

### 4. プライベートネットワーク経由でCOSにアクセスすると料金が発生しますか。

プライベートネットワーク経由でCOSにアクセスする場合、**トラフィック料金は発生しませんが**、**ストレージ容量とリクエスト回数**については関連の料金が発生します。詳細については、[課金項目](#) のページに掲載しておりますので、ご覧ください。

# CentOS Linux関連操作

## CentOSの移行 TencentOS Serverガイド

最終更新日：：2023-04-25 17:59:34

### ユースケース

CentOSは、CentOS Linuxプロジェクトのメンテナンスを正式に停止する予定があります。CentOS 8とCentOS 7のメンテナンスを次の表に示します。詳細については、[CentOS公式発表](#)をご参照ください。

OSバージョン	メンテナンス停止時間	使用者への影響
CentOS 8	2022年01月01日	メンテナンスを停止すると、問題の修正や機能の更新を含むソフトウェアのメンテナンスやサポートを受けることができなくなります。
CentOS 7	2024年06月30日	

それを考慮して、新しいCVMインスタンスを購入する場合は、TencentOS Serverイメージを使用することをお勧めします。CentOSインスタンスを使用している場合は、このドキュメントを参照してTencentOS Serverに入れ替えてください。

### バージョン説明

**移行元サーバーでサポートされるオペレーティングシステムのバージョン：**

次のCentOS 7シリーズをサポートします。

CentOS 7.2 64ビット、CentOS 7.3 64ビット、CentOS 7.4 64ビット、CentOS 7.5 64ビット、CentOS 7.6 64ビット、CentOS 7.7 64ビット、CentOS 7.8 64ビット、CentOS 7.9 64ビット

次のCentOS 8シリーズをサポートします：

CentOS 8.0 64ビット、CentOS 8.2 64ビット、CentOS 8.4 64ビット

**移行元サーバーの推奨OS：**

CentOS 7シリーズはTencentOS Server 2.4(TK4)へ移行することをお勧めします。

CentOS 8シリーズはTencentOS Server 3.1(TK4)へ移行することをお勧めします。

**ご注意：**

CentOS 7.2およびCentOS 7.3のパブリックイメージにはデフォルトで32ビットパッケージが含まれている場合があるため、アップグレードを実行する前に手動で削除する必要があります。

## 注意事項

移行は次の場合にはサポートされません：

グラフィカルインターフェイスがインストールされた場合。

i686のrpmパッケージがインストールされた場合。

次のような場合は移行後のビジネスが正常に機能しなくなる場合があります：

ビジネスプログラムにはサードパーティ製のrpmパッケージにインストールされ、それに依存している場合。

ビジネスプログラムが特定のバージョンのカーネルに依存しているか、独自にカーネルモジュールをコンパイルしている場合。

移行後のターゲットバージョンは5.4カーネルベースのtkernel4です。このバージョンは、CentOS 7およびCentOS 8のカーネルバージョンよりも更新されており、新しいバージョンでは古い機能に変更される場合があります。

ビジネスプログラムは特定のgccバージョンに依存している場合。

現在、TencentOS Server 2.4にはgcc 4.8.5がデフォルトでインストールされ、TencentOS Server 3.1にはgcc 8.5がデフォルトでインストールされています。

移行が終了したら、TencentOS Serverカーネルに入るには再起動する必要があります。

移行はディスクに影響がなくOSレベルのアップグレードだけで、他の操作が実行されません。

## リソース要件

利用可能なメモリが500MB以上。

システムディスクの空き容量が10GB以上。

## 操作手順

### 移行準備

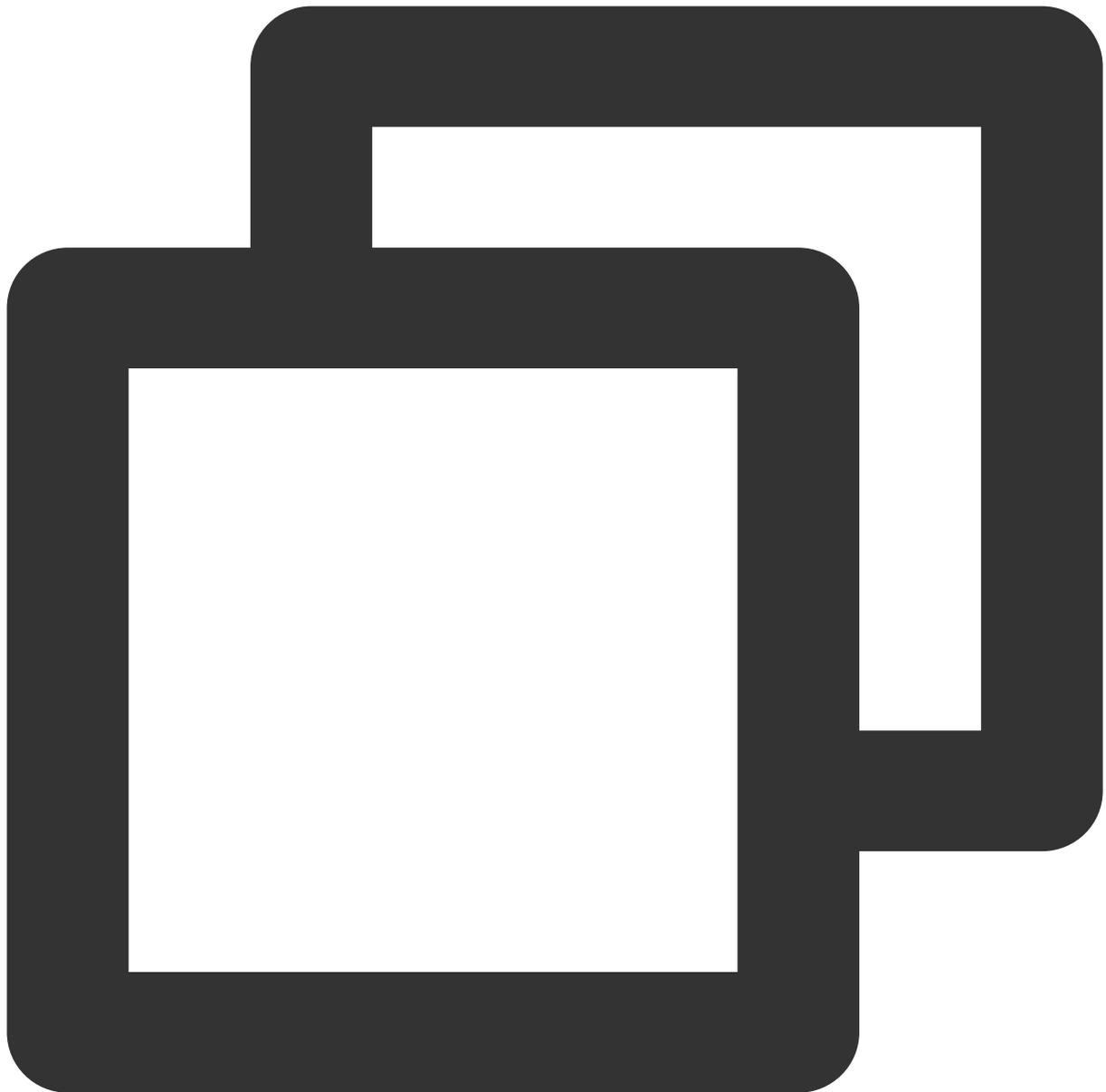
1. 移行操作は可逆的ではありません。ビジネスデータの安全性を確保するために、移行を実行する前に[スナップショットの作成](#)を使用してシステムディスクのデータをバックアップすることをお勧めします。
2. i686のrpmパッケージをチェックし、手動でアンインストールします。

### 移行の実行

CentOS 7シリーズはTencentOS Server 2.4（TK4）へ移行します

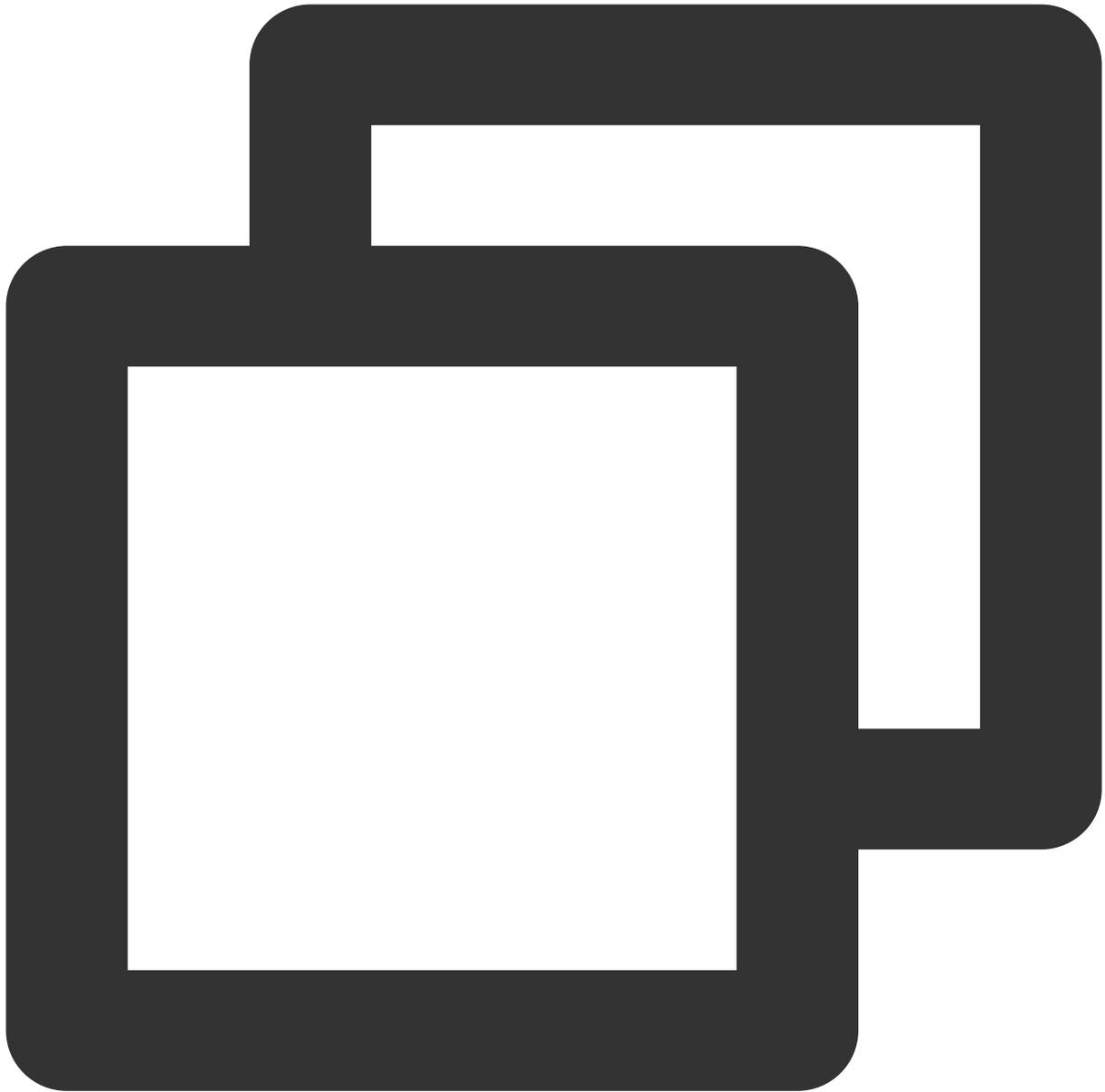
CentOS 8シリーズはTencentOS 3.1（TK4）へ移行します。

1. 移行先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. 次のコマンドを実行して、Python 3をインストールします。



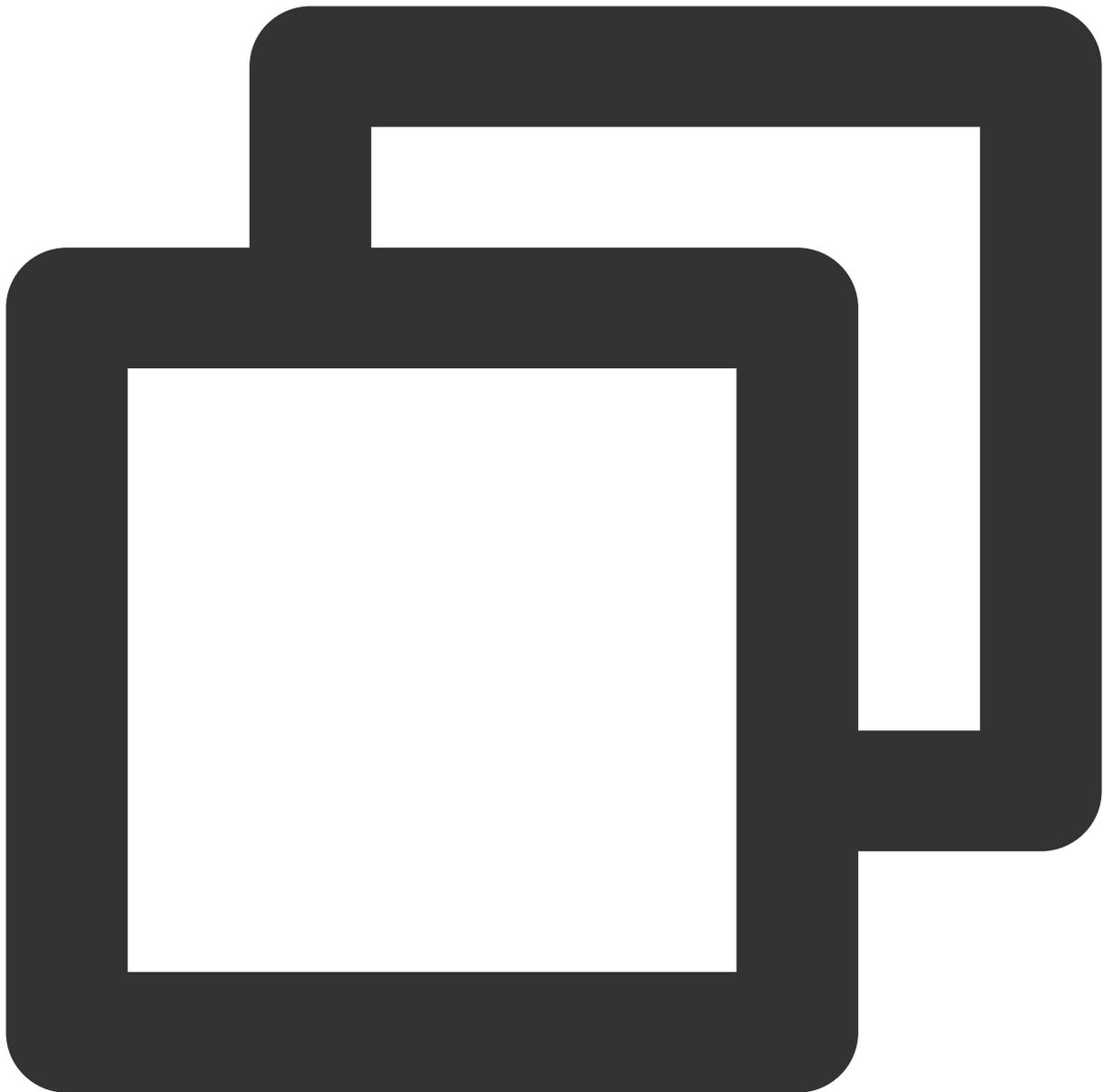
```
yum install -y python3
```

3. 移行ツールの取得には以下のコマンドを実行します。



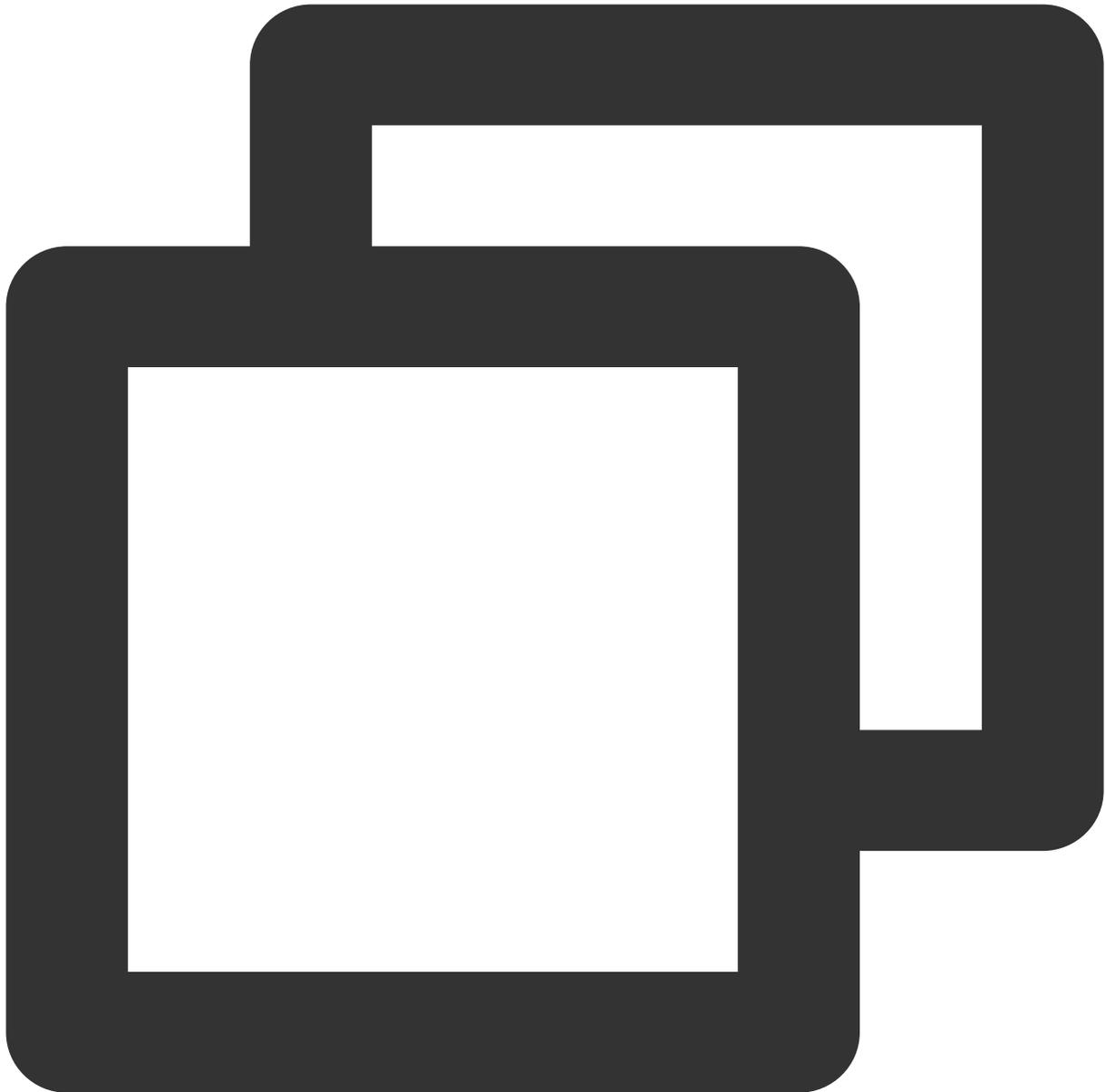
```
wget http://mirrors.tencent.com/tencentos/2.4/tlinux/x86_64/RPMS/migrate2tencentos-
```

4. 移行ツールのインストールには以下のコマンドを実行します。このコマンドは、`/usr/sbin`の下で `migrate2tencentos.py`を作成します。



```
rpm -ivh migrate2tencentos-1.0-4.tl2.noarch.rpm
```

5. 移行の開始には以下のコマンドを実行します。

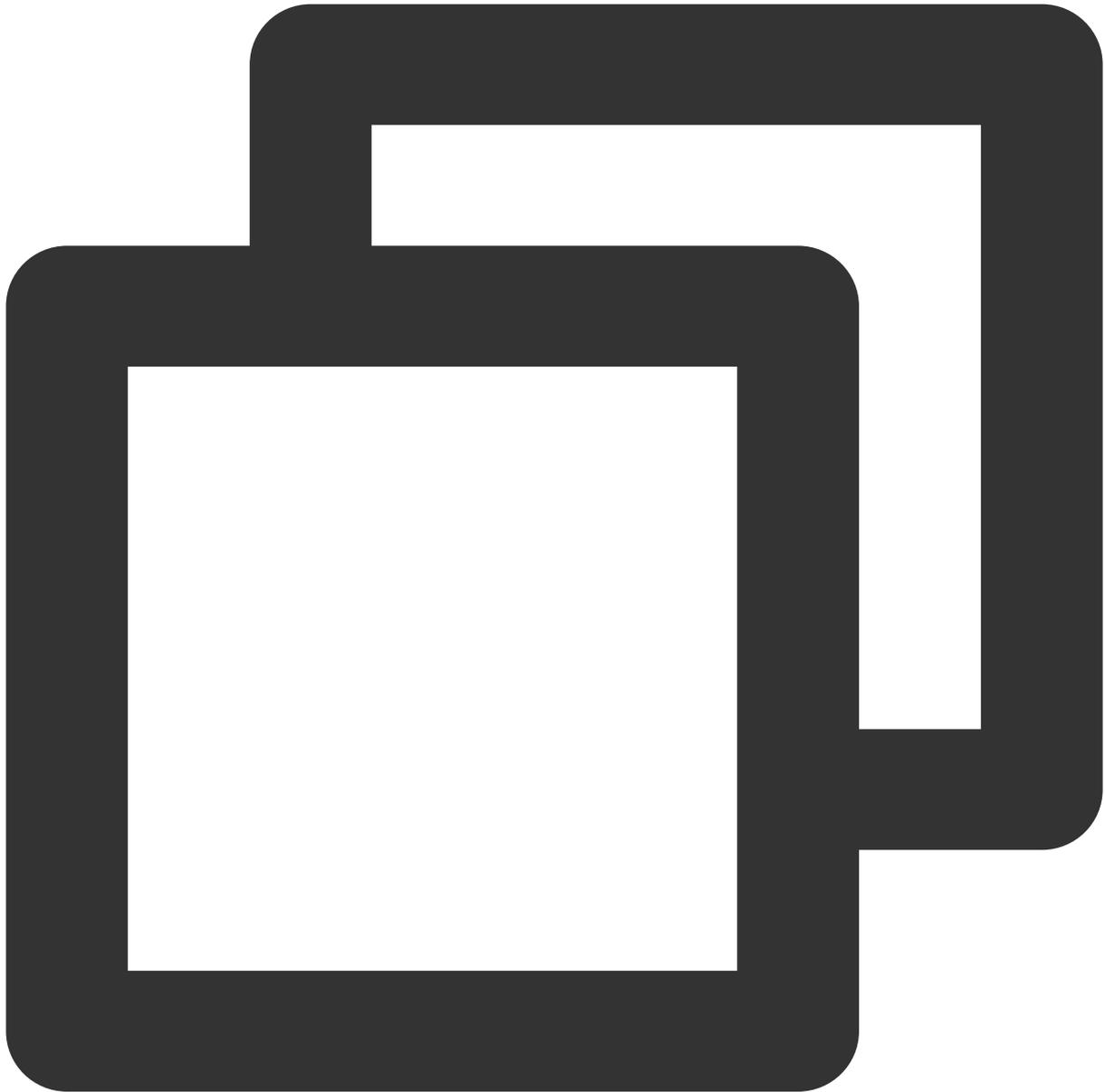


```
python3 /usr/sbin/migrate2tencentos.py -v 2.4
```

移行には時間がかかります。しばらくお待ちください。スクリプトの実行が完了し、次の図に示すような情報が出力されると、移行が完了したことを意味します。

```
Metadata Cache Created  
Switch complete. TencentOS recommends rebooting this system.  
[root@VM-2-43-centos ~]# █
```

6. 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。
7. 移行結果のチェック。
  - 7.1 os-releaseのチェックには以下のコマンドを実行します。

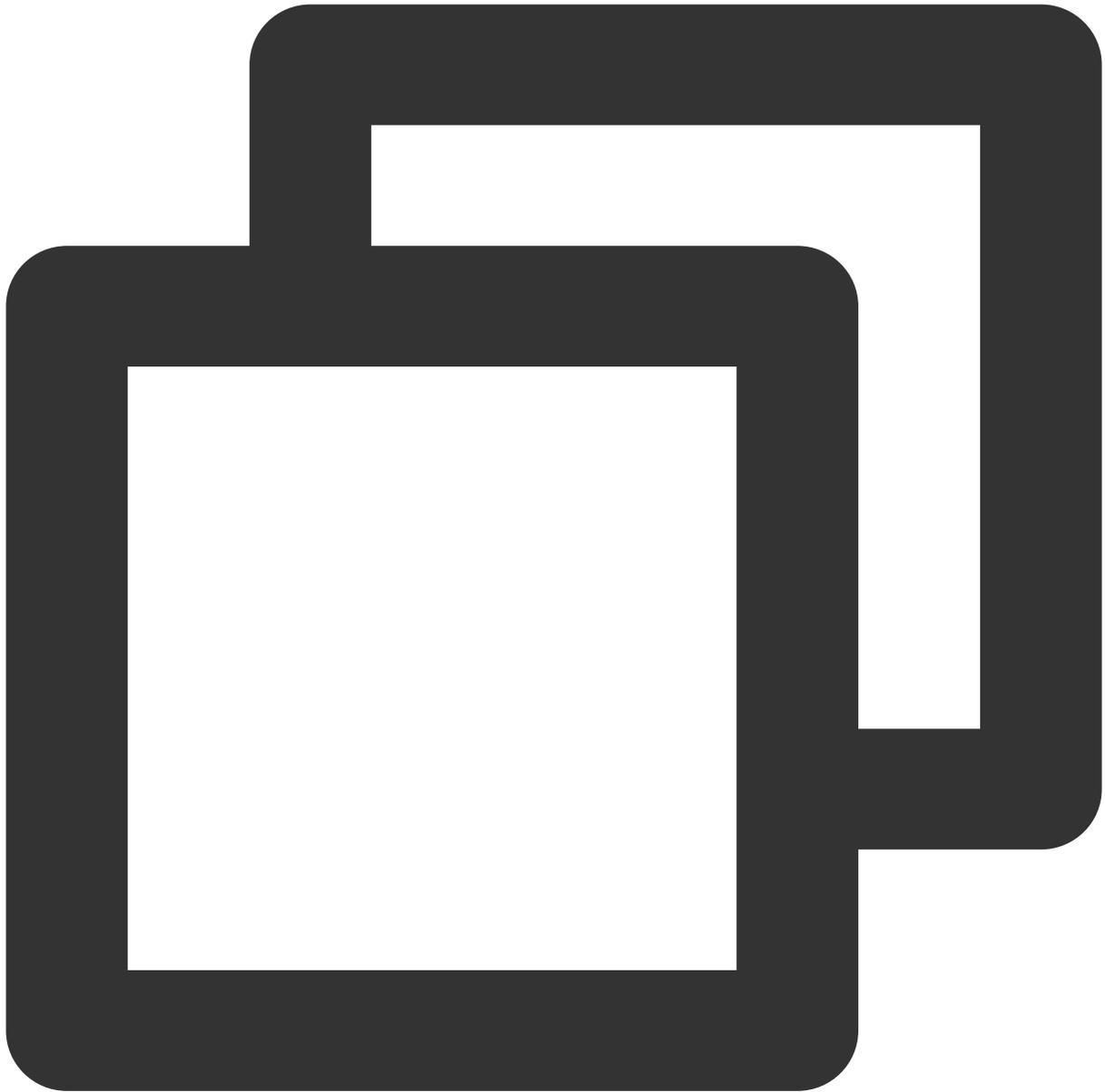


```
cat /etc/os-release
```

下図に示す情報を返します：

```
[root@VM-2-43-centos ~]# cat /etc/os-release
NAME="TencentOS Server"
VERSION="2.4"
ID="tencentos"
ID_LIKE="rhel fedora centos tlinux"
VERSION_ID="2.4"
PRETTY_NAME="TencentOS Server 2.4"
ANSI_COLOR="0;31"
CPE_NAME="cpe:/o:tencentos:tencentos:2"
HOME_URL="https://cloud.tencent.com/product/ts"
```

7.2 カーネルのチェックには以下のコマンドを実行します。



```
uname -r
```

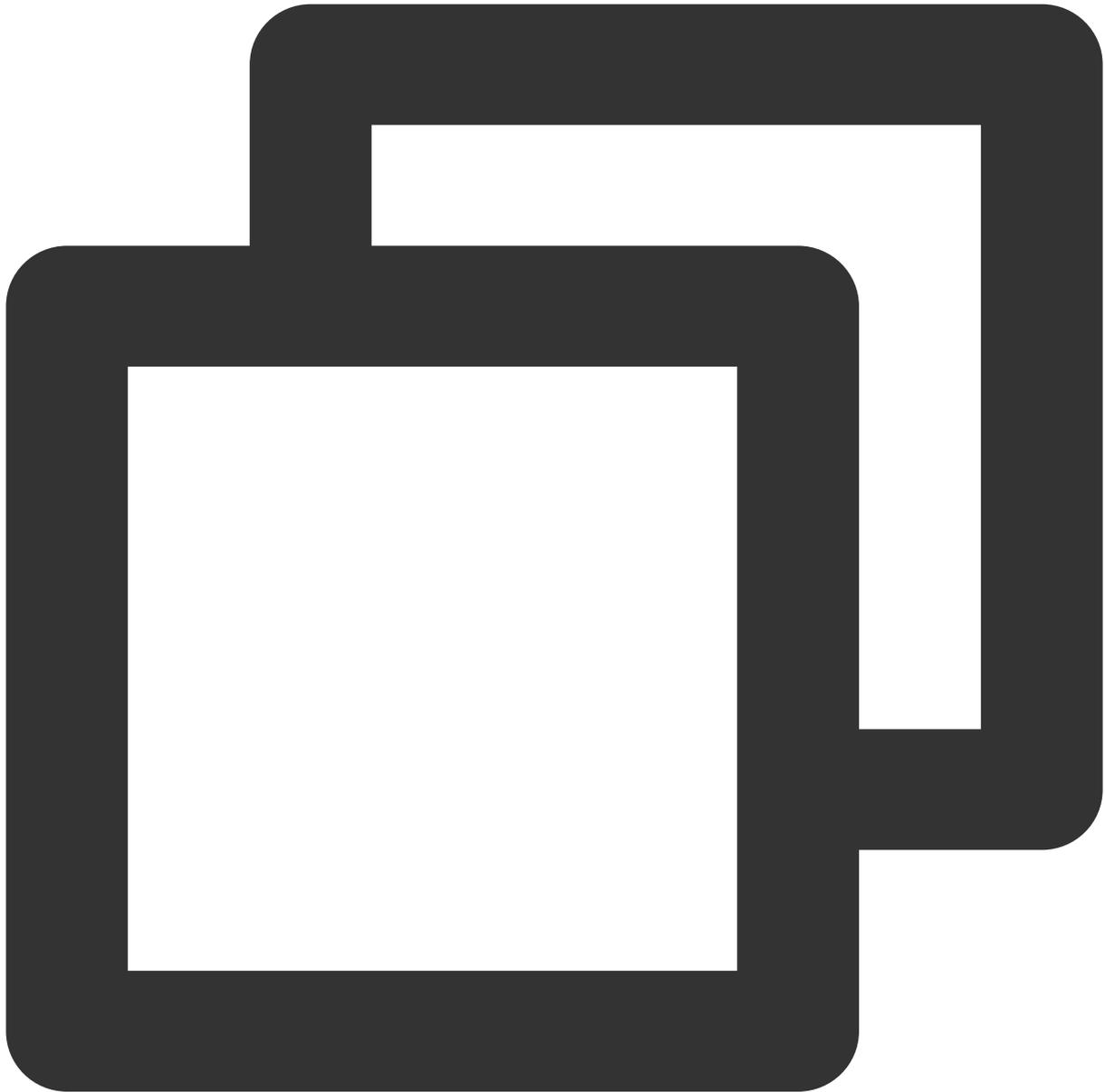
下図に示す情報を返します：

```
[root@VM-2-43-centos ~]# uname -r  
5.4.119-19-0009.1  
[root@VM-2-43-centos ~]# █
```

説明：

カーネルはデフォルトでyumの最新バージョンです。実際に返された結果を基準にしてください。このドキュメントでは、図のバージョンを例として説明します。

8. yumのチェックには以下のコマンドを実行します。

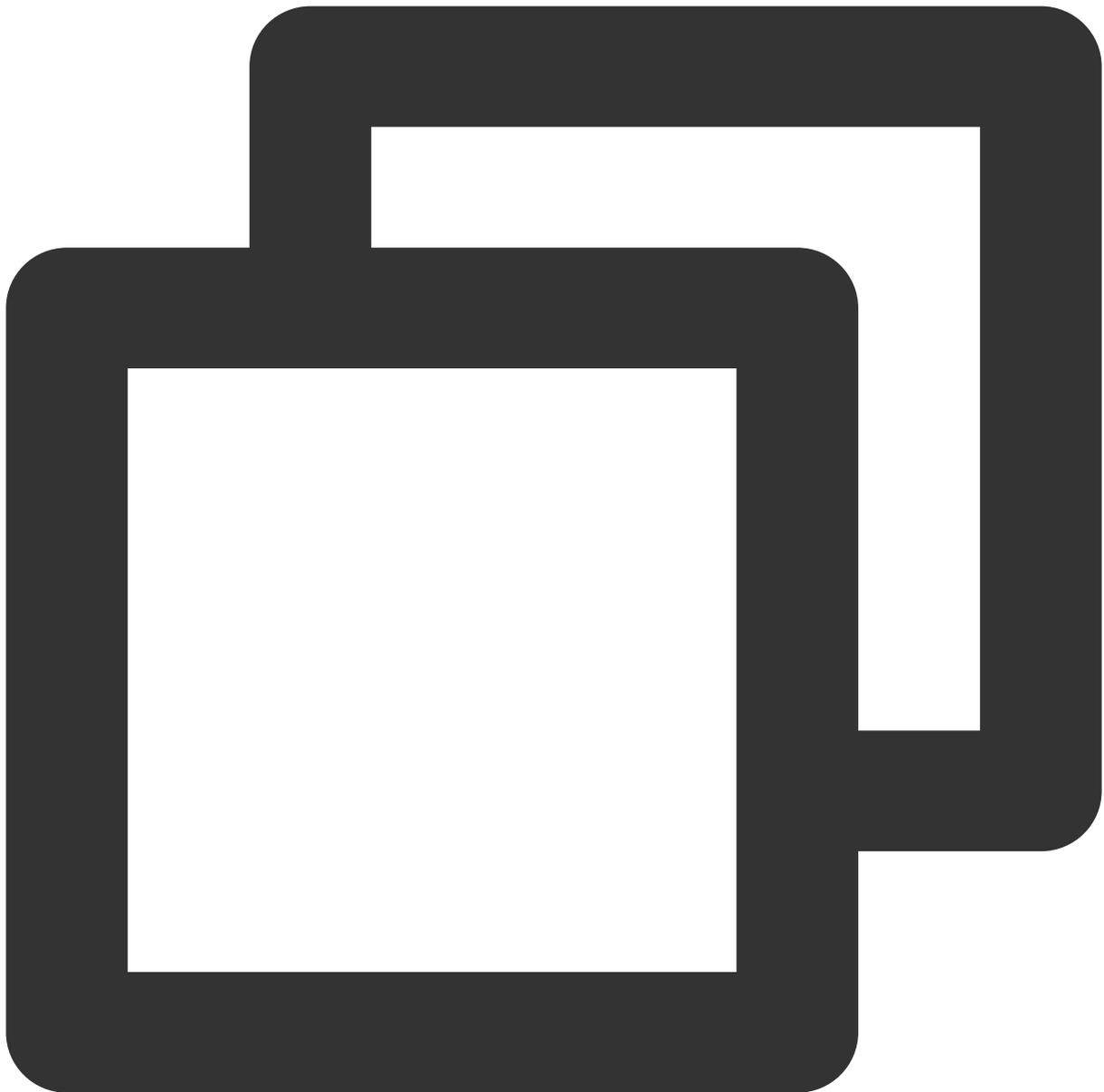


```
yum makecache
```

下図に示す情報を返します：

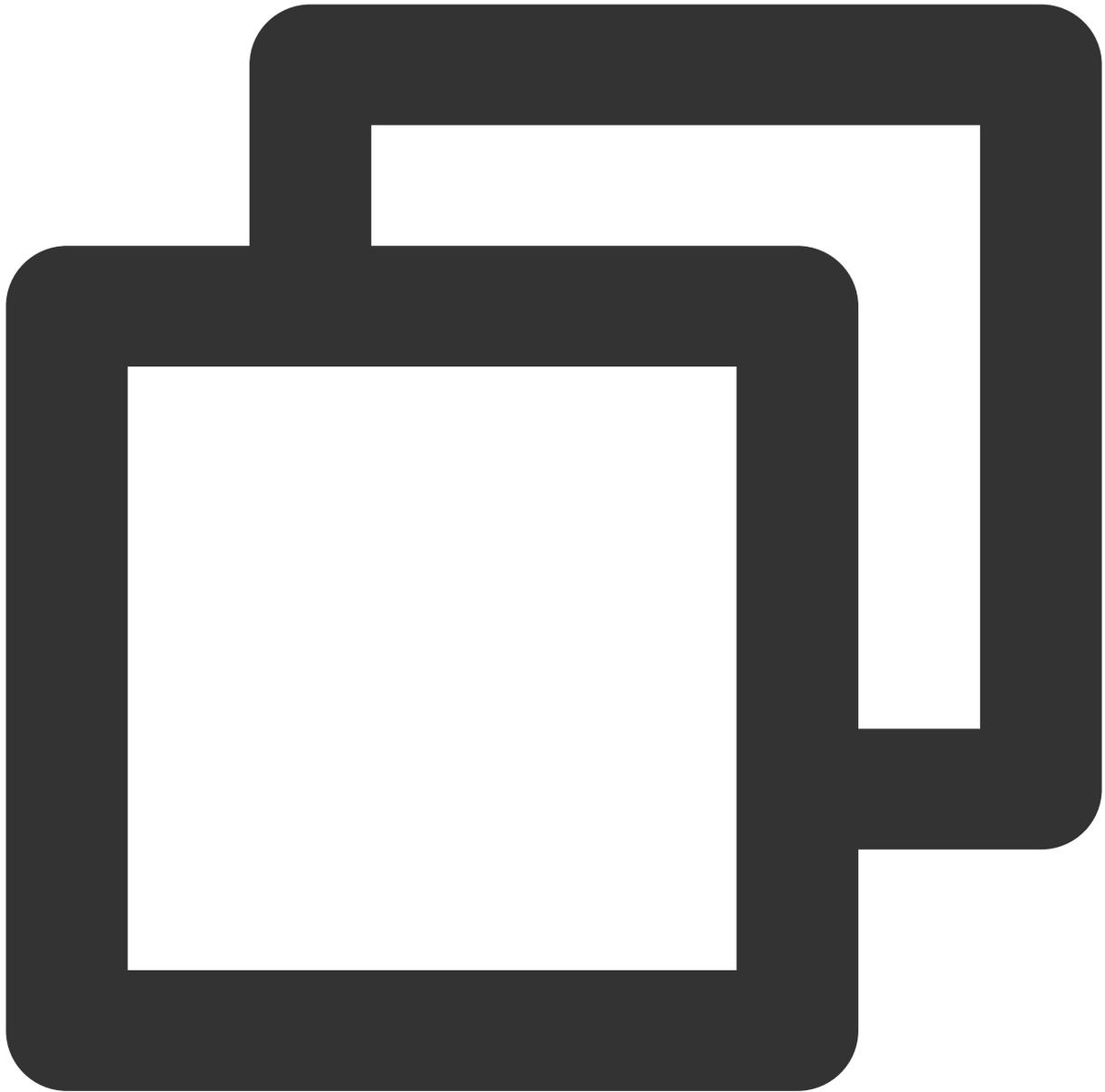
```
[root@VM-2-43-centos ~]# yum makecache
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
* epel: mirrors.tencentyun.com
* tlinux: mirrors.tencentyun.com
* tlinux-extras: mirrors.tencentyun.com
* tlinux-os: mirrors.tencentyun.com
* tlinux-updates: mirrors.tencentyun.com
epel
tlinux
tlinux-extras
tlinux-os
tlinux-tkernel4
tlinux-updates
Metadata Cache Created
[root@VM-2-43-centos ~]#
```

1. 移行先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. 次のコマンドを実行して、Python 3をインストールします。



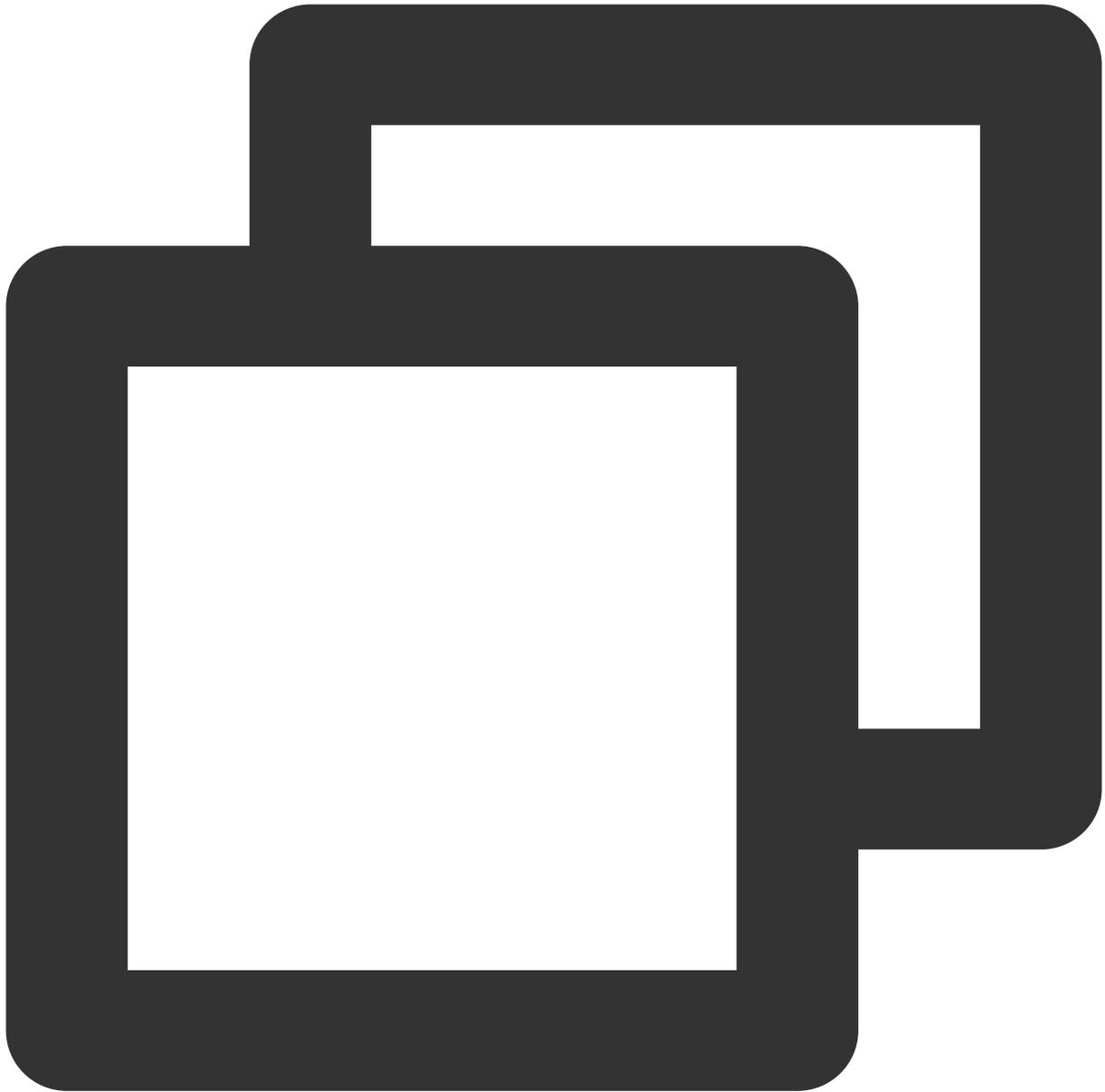
```
yum install -y python3
```

3. 移行ツールの取得には以下のコマンドを実行します。



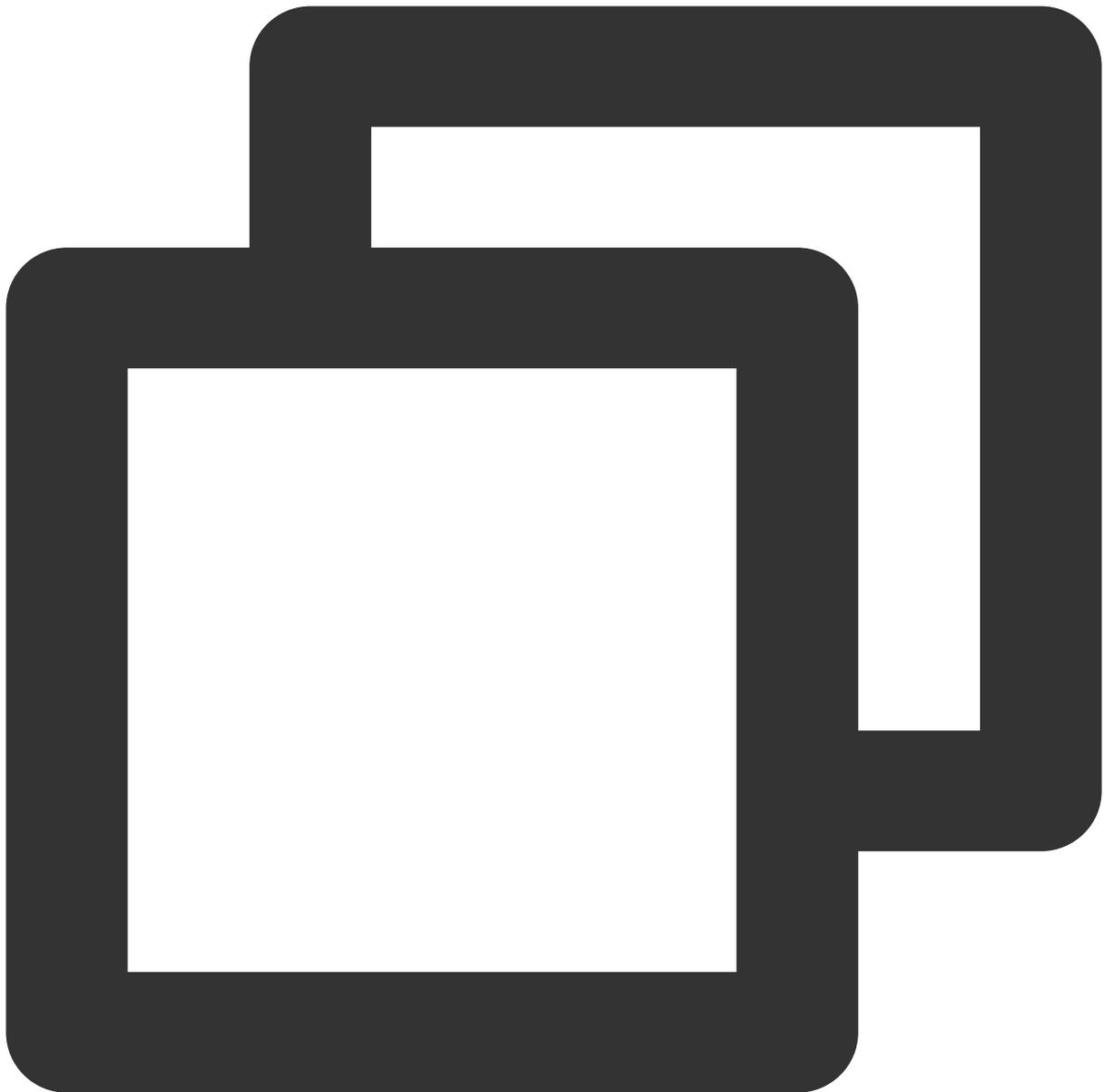
```
wget http://mirrors.tencent.com/tlinux/3.1/Updates/x86_64/RPMS/migrate2tencentos-1.
```

4. 移行ツールのインストールには以下のコマンドを実行します。このコマンドは、`/usr/sbin`の下で `migrate2tencentos.py`を作成します。



```
rpm -ivh migrate2tencentos-1.0-4.tl3.noarch.rpm
```

5. 移行の開始には以下のコマンドを実行します。

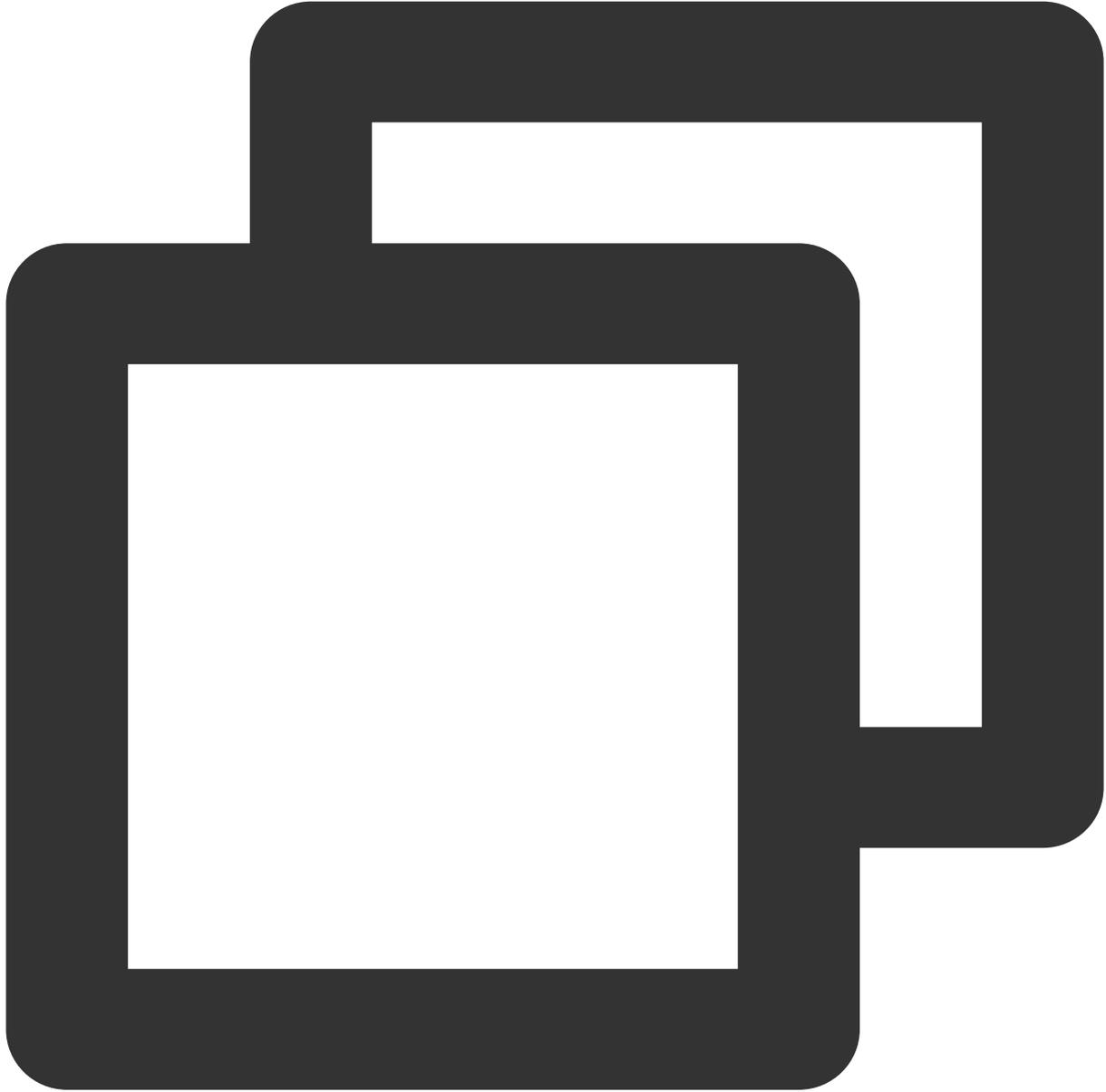


```
python3 /usr/sbin/migrate2tencentos.py -v 3.1
```

移行には時間がかかります。しばらくお待ちください。スクリプトの実行が完了し、次の図に示すような情報が出力されると、移行が完了したことを意味します。

```
Metadata cache created.  
Switch complete. TencentOS recommends rebooting this system.  
[root@VM-2-2-centos ~]# █
```

6. 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。
7. 移行結果のチェック。
  - 7.1 os-releaseのチェックには以下のコマンドを実行します。

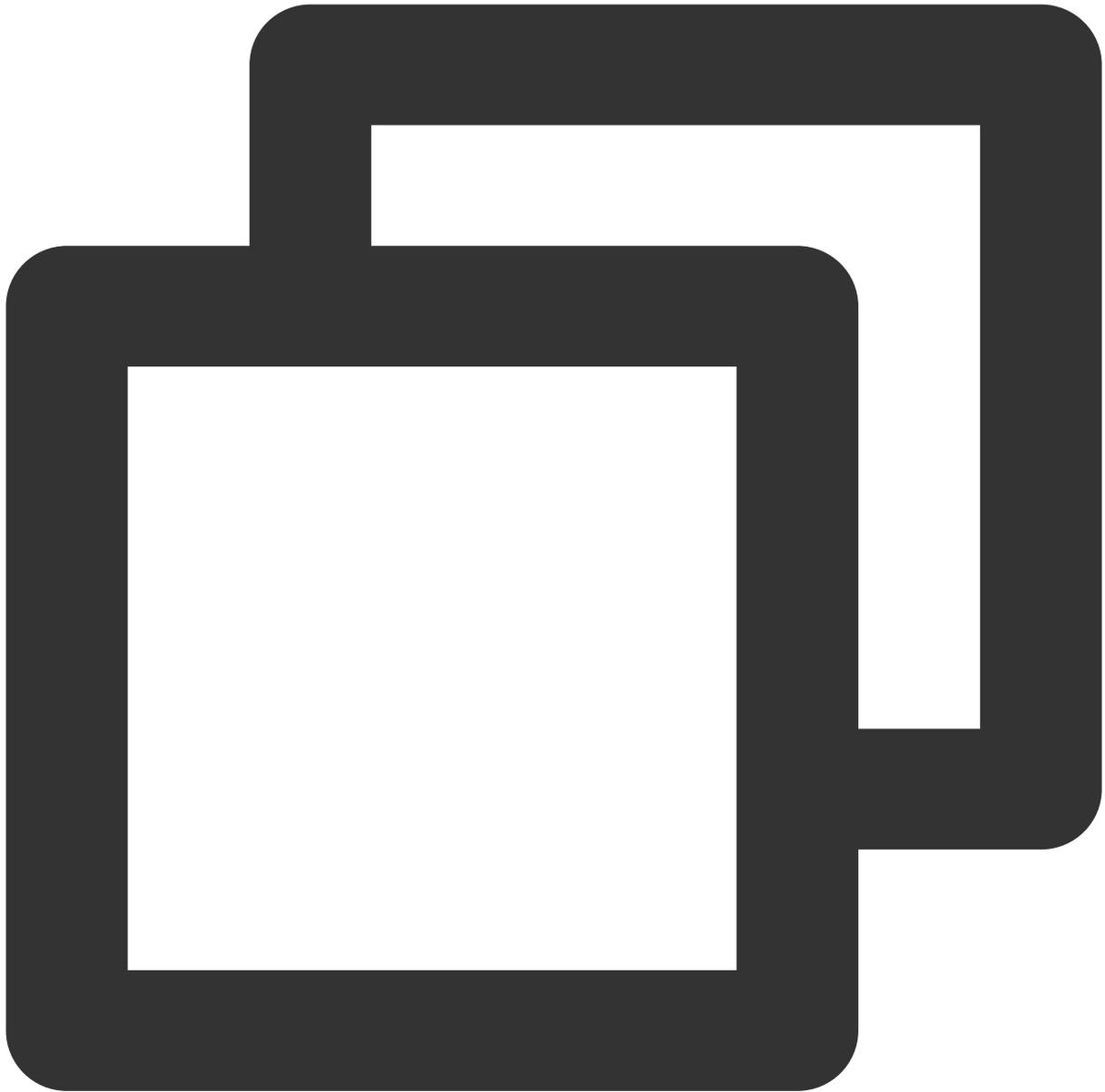


```
cat /etc/os-release
```

下図に示す情報を返します：

```
[root@VM-2-2-centos ~]# cat /etc/os-release
NAME="TencentOS Server"
VERSION="3.1 (Final)"
ID="tencentos"
ID_LIKE="rhel fedora centos"
VERSION_ID="3.1"
PLATFORM_ID="platform:el8"
PRETTY_NAME="TencentOS Server 3.1 (Final)"
ANSI_COLOR="0;31"
CPE_NAME="cpe:/o:tencentos:tencentos:3"
HOME_URL="https://cloud.tencent.com/product/ts"
```

7.2 カーネルのチェックには以下のコマンドを実行します。



```
uname -r
```

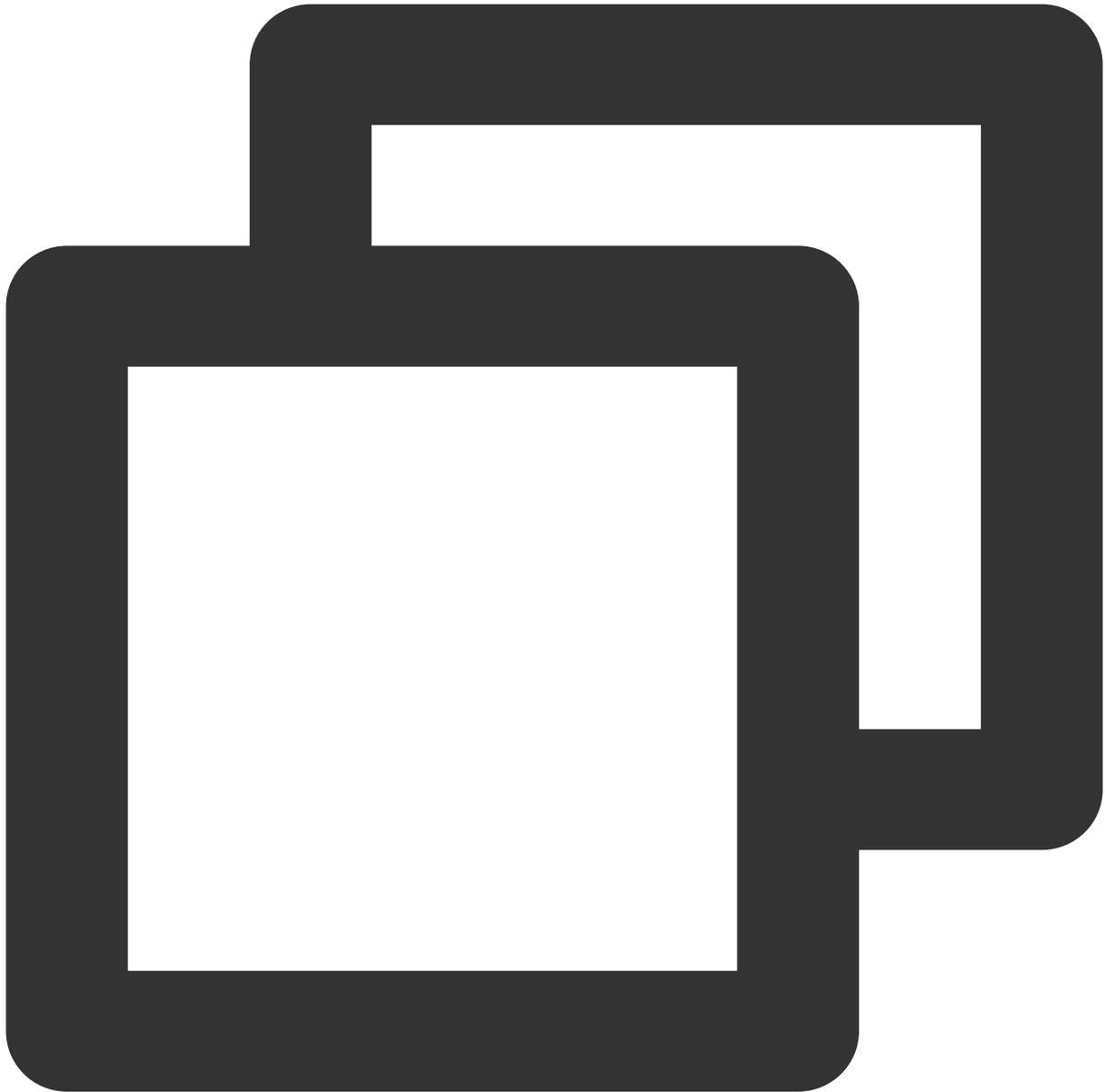
下図に示す情報を返します：

```
[root@VM-2-2-centos ~]# uname -r  
5.4.119-19-0009.1  
[root@VM-2-2-centos ~]# █
```

説明：

カーネルはデフォルトでyumの最新バージョンです。実際に返された結果を基準にしてください。このドキュメントでは、図のバージョンを例として説明します。

8. yumのチェックには以下のコマンドを実行します。



```
yum makecache
```

下図に示す情報を返します：

```
[root@VM-2-2-centos ~]# yum makecache
TencentOS Server 3.1 - TencentOS
TencentOS Server 3.1 - Updates
TencentOS Server 3.1 - TencentOS-AppStream
TencentOS Server 3.1 - Base
TencentOS Server 3.1 - AppStream
TencentOS Server 3.1 - Extras
TencentOS Server 3.1 - PowerTools
Extra Packages for TencentOS Server 3.1 - x86_64
Extra Packages for TencentOS Server 3.1 Modular - x86_64
Metadata cache created.
[root@VM-2-2-centos ~]# █
```

# サービス移行

## オンライン移行

### オンライン移行の概要

最終更新日：2023-07-27 10:58:56

オンライン移行とは、稼働中のシステムを停止することなく、サーバーまたは仮想マシン上のシステム、サービスプログラムなどを、自社のデータセンター(IDC)または他のクラウドプラットフォームなどの移行元環境から Tencent Cloud に同期または移行することです。

Tencent Cloud は「go2tencentcloud」移行ツールを提供します。移行ツールを移行元サーバーで実行すると、移行元サーバーで実行されているすべてのシステムとサービスアプリケーションを Tencent Cloud の移行先 CVM に移行することができます。この移行ツールを使用すると、イメージの制作、アップロード、インポートなどの煩雑な準備作業を行う必要がなくなり、ソースデータをクラウドに直接移行できます。業務のクラウド化、異なるクラウドプラットフォーム間での移行、クロスアカウントまたはクロスリージョン移行、およびハイブリッドクラウド展開に関する企業のビジネス要件を満たすことができます。

#### 説明：

ソースサーバーの形式は、物理サーバー、仮想マシン、または別のクラウドプラットフォーム上のクラウドサーバーにすることができます。その他のクラウドプラットフォームには、AWS、Google Cloud Platform、VMware、Alibaba Cloud、Huawei Cloud などの仮想マシンプラットフォームが含まれますが、これらに限りません。

## ユースケース

オンライン移行は、次のシナリオに適用できます(これに限定されません)。

ITアーキテクチャのクラウド化

ハイブリッドクラウドアーキテクチャの展開

クラウド間移行

アカウント間またはリージョン間での移行

## オフライン移行との違い

オフライン移行では、移行元サーバーでシステムディスクまたはデータディスクのイメージを作成してから、イメージを Cloud Virtual Machine (CVM) または Cloud Block Storage (CBS) に移行する必要があります。オンライン移行はイメージを作成する必要がなく、移行元サーバーで移行ツールを直接実行して、移行元サーバーで実行されているすべてのシステムとサービスアプリケーションを Tencent Cloud の移行先 CVM に移行することができます。

## 移行の開始

オンライン移行方法は大きく2種類あります。必要に応じて適切な移行方法を選択してください。

移行方法	概要	ユースケース	特徴
<a href="#">オンライン移行：クライアントからの移行元のインポート</a>	ソースインスタンスにログインし、ツールを使用して移行元をインポートし、コンソールで移行タスクを作成して移行を完了します。	パブリックネットワークおよびプライベートネットワーク経由での移行 他のクラウドプラットフォームからTencent Cloudへの移行 顧客のデータセンターからTencent Cloudへの移行	高い互換性
<a href="#">オンライン移行：コンソールでのワンクリック移行</a>	コンソールにログインして本人確認完了後、移行元をワンクリックでインポートし、移行タスクを作成します。	移行元サーバーにログインする必要はありません パブリックネットワーク経由での移行 クラウド間移行：ソースインスタンスがAlibaba Cloudにあるシナリオに適用されます。	ワンクリックで一括移行

## よくあるご質問

詳細については、[サービスの移行](#)をご参照ください。

# 移行ガイド

## オンライン移行ガイド

最終更新日：：2023-07-27 10:58:56

オンライン移行は、稼働中のシステムを停止することなく、サーバーまたは仮想マシン上のシステム、サービスプログラムなどを、自社のデータセンター(IDC)または他のクラウドプラットフォームなどの移行元環境から Tencent Cloudに移行または同期することをサポートします。

オンライン移行方法は大きく2種類あります。必要に応じて適切な移行方法を選択してください。

移行方法	概要	ユースケース	特徴
<a href="#">オンライン移行：クライアントからの移行元のインポート</a>	ソースインスタンスにログインし、ツールを使用して移行ソースをインポートし、コンソールで移行タスクを作成して移行を完了します。	パブリックネットワークおよびプライベートネットワーク経での移行 他のクラウドプラットフォームからTencent Cloudへの移行 顧客のデータセンターからTencent Cloudへの移行	高い互換性
<a href="#">オンライン移行：コンソールでのワンクリック移行</a>	コンソールにログインして本人確認完了後、移行元をワンクリックでインポートし、移行タスクを作成します。	パブリックネットワーク経由での移行 クラウド間移行:ソースインスタンスがAlibaba Cloudにあるシナリオに適しています	ワンクリックで一括移行 コンソールでの操作

# オンライン移行：クライアントからの移行元のインポート

最終更新日：2023-12-05 10:55:42

このドキュメントでは、クライアントから移行元をインポートして、移行元サーバーを Tencent Cloud CVM に移行する方法について説明します。

## 移行ワークフロー

クライアントから移行元をインポートする手順は以下のとおりです。



## 移行手順

### 手順1：移行の準備

[APIキー管理](#) ページに移動してキーを作成し、`SecretId` と `SecretKey` を取得します。

-移行時に既存のアプリケーションに影響しないように、移行元サーバー上のアプリケーションを一時停止してデータをバックアップすることをお勧めします。

移行元サーバー：スナップショット機能またはその他の方法を使用して、移行元サーバー上のデータをバックアップできます。移行元サーバーは、移行されるサーバーです。

移行先CVM：[スナップショットの作成](#)などの方式を選択して、移行先CVMのデータをバックアップできます。サブアカウントを使用してコンソールで移行を実行する場合、ルートアカウントで [CAMコンソール](#) にログインし、サブアカウントに `QcloudCSMFullAccess` と `QcloudCVMFullAccess` 権限を付与する必要があります。

移行前、実際の状況に基づいて次の構成を確認する必要があります。ご確認いただきたい内容は以下のとおりです：

CVM インスタンスへの移行：移行元サーバーと移行先CVMを確認する必要があります。

CVM イメージへの移行：移行元サーバーのみを確認します。

Linux 移行元サーバー	<ol style="list-style-type: none"> <li>1. Virtio を確認してインストールします。詳細については、<a href="#">LinuxでのVirtioドライバーの確認</a> をご参照ください。</li> <li>2. which rsyncコマンドを実行して、rsync がインストールされているかどうかを確認します。インストールされていない場合は、<a href="#">rsync をインストールする方法</a> の指示に従ってインストールしてください。</li> <li>3. SELinux が有効化されているかどうかを確認します。SELinuxが有効になっている場合は、<a href="#">SELinuxを無効化する方法</a> を参照して無効化してください。</li> <li>4. Tencent Cloud API に移行リクエストを送信した後、API は現在の UNIX 時間を使用して、生成されたトークンを確認します。サーバーのシステム時刻が正しいことを確認してください。</li> </ol>
Windows 移行元サーバー	<ol style="list-style-type: none"> <li>1. Virtio を確認してインストールします。詳細については、<a href="#">WindowsでのVirtioドライバーの確認</a> をご参照ください。</li> <li>2. (オプション)Cloudbase-Init を確認してインストールします。詳細については、<a href="#">Windows への Cloudbase-Init のインストール</a> をご参照ください。移行前に移行元サーバーにインストールするか、移行後にターゲットインスタンスにインストールするかを選択できます。移行前にインストールされている場合は、移行後にネットワークの自動構成やアクティベーションなどの初期化作業が行われます。移行前にインストールされていない場合は、<a href="#">VNC 経由でインスタンスにログイン</a> し、ネットワーク構成を手動で変更する必要があります。</li> </ol>
移行先 CVM	<ol style="list-style-type: none"> <li>1. ストレージ容量：移行先CVMのクラウドディスク（システムディスクとデータディスクを含む）には、移行元サーバーから移行されたデータを保存するための十分な容量が必要です。</li> <li>2. セキュリティグループ：セキュリティグループでポート80、443、および3389を開放します。</li> <li>3. 帯域幅：移行をより円滑に進めるためには、移行元と移行先の両方の環境の帯域幅を最大化することをお勧めします。移行プロセス中に消費されるトラフィックは、移行されたデータの量とほぼ同じになります。必要に応じて、移行前にネットワーク課金モデルを調整します。</li> <li>4. ネットワーク設定：移行元または移行先サーバーが IPv6 のみをサポートし、IPv4 をサポートしていない場合は、<a href="#">client.jsonファイルのパラメータ説明</a> をご参照ください。</li> </ol>

## 説明：

`sudo ./go2tencentcloud_x64 --check` などのツールコマンドを使用して、移行元サーバーを自動的にチェックできます。

デフォルトでは、go2tencentcloudツールは起動時に自動的にチェックを実行します。このチェックをスキップして強制移行する場合は、client.json ファイルの `Client.Extra.IgnoreCheck` フィールドの値を `true` に設定してください。

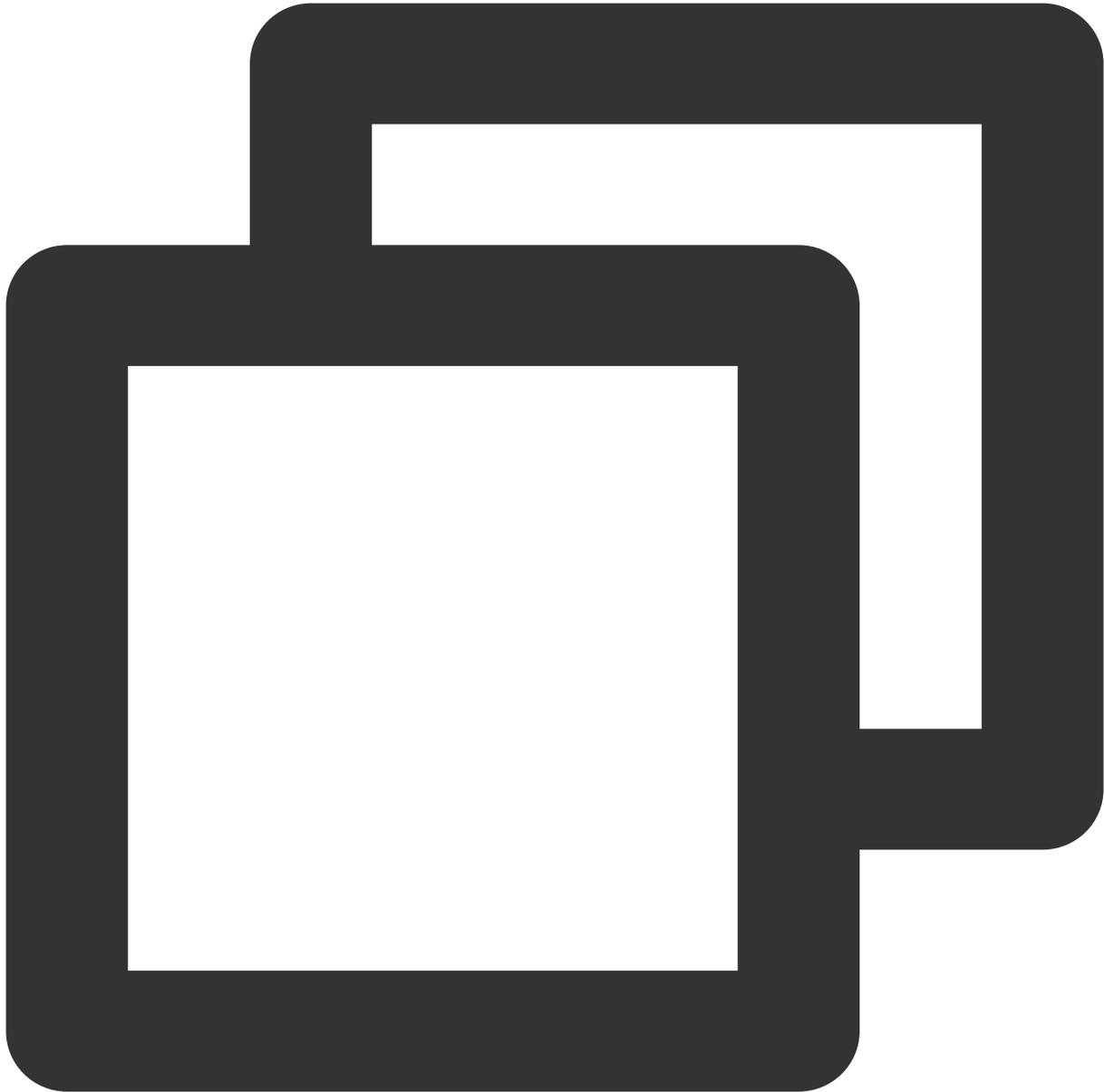
## 手順2：移行元のインポート

### 移行ツールによる移行元のインポート

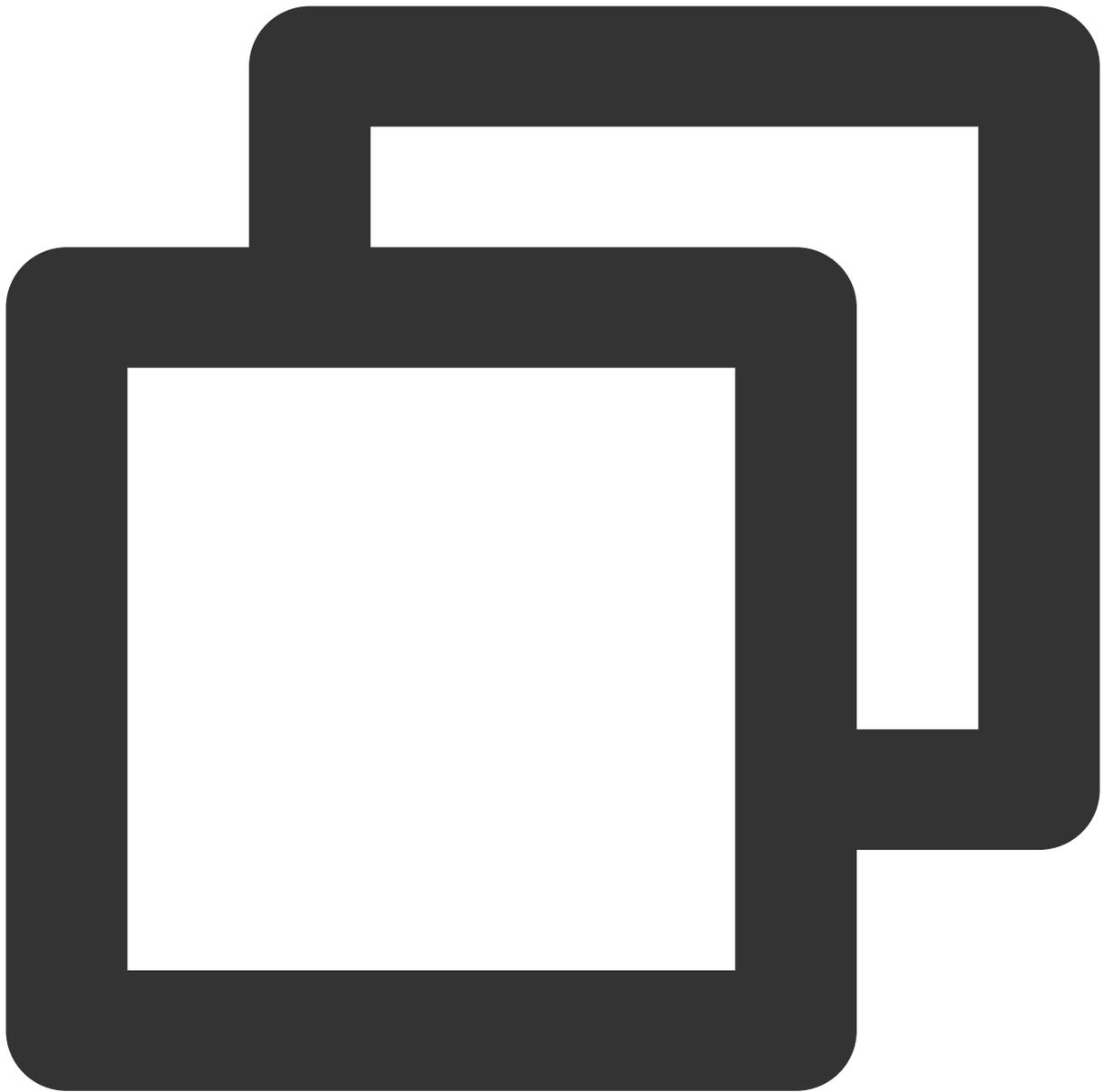
#### Linuxサーバー

## Windowsサーバー

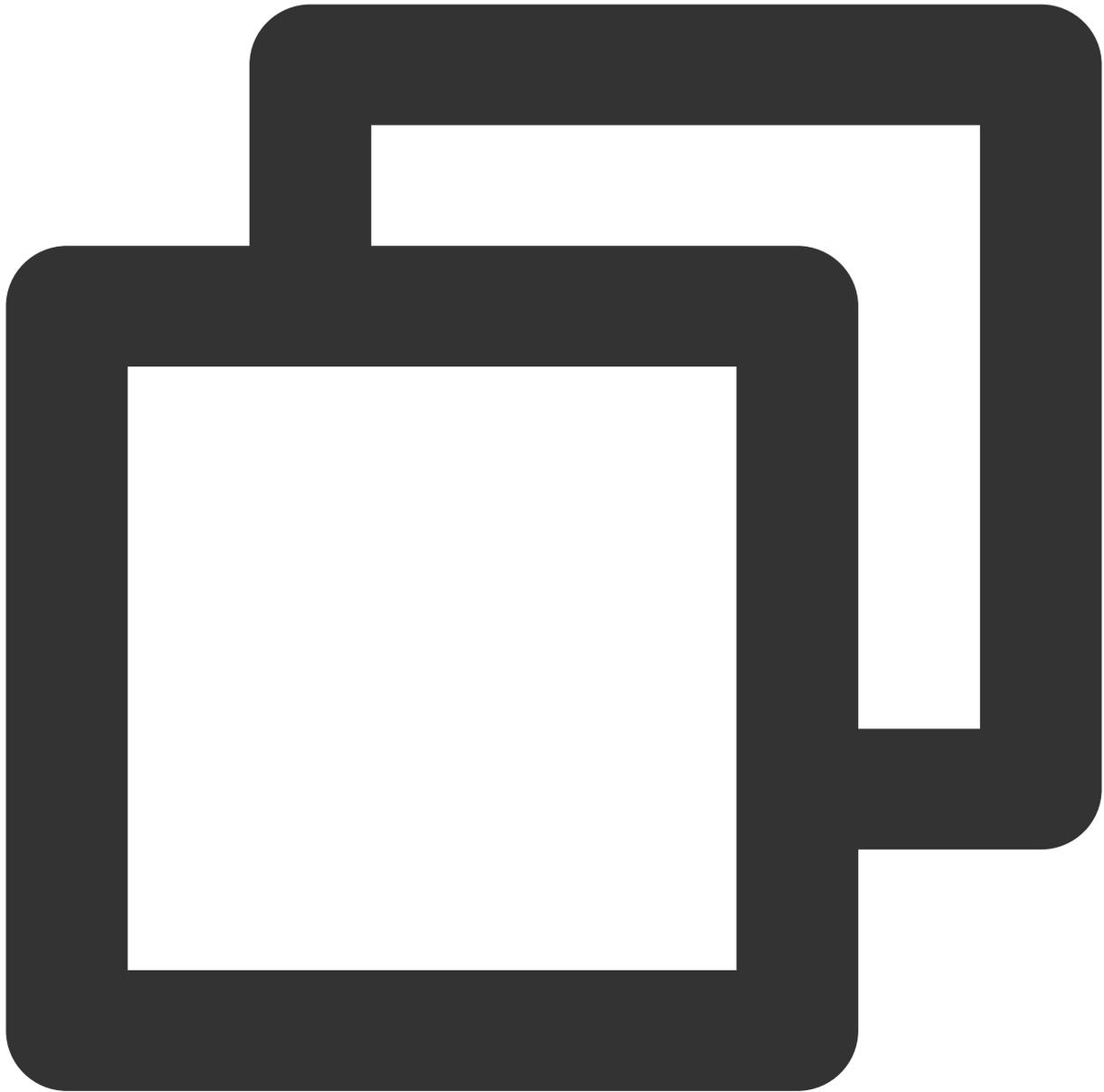
1. 移行元サーバーで次のコマンドを実行して、移行ツール `go2tencentcloud.zip` をダウンロードしてディレクトリに進みます。



```
wget https://go2tencentcloud-1251783334.cos.ap-guangzhou.myqcloud.com/latest/go2ten
```



```
unzip go2tencentcloud.zip
```



```
cd go2tencentcloud/go2tencentcloud-linux
```

**説明：**

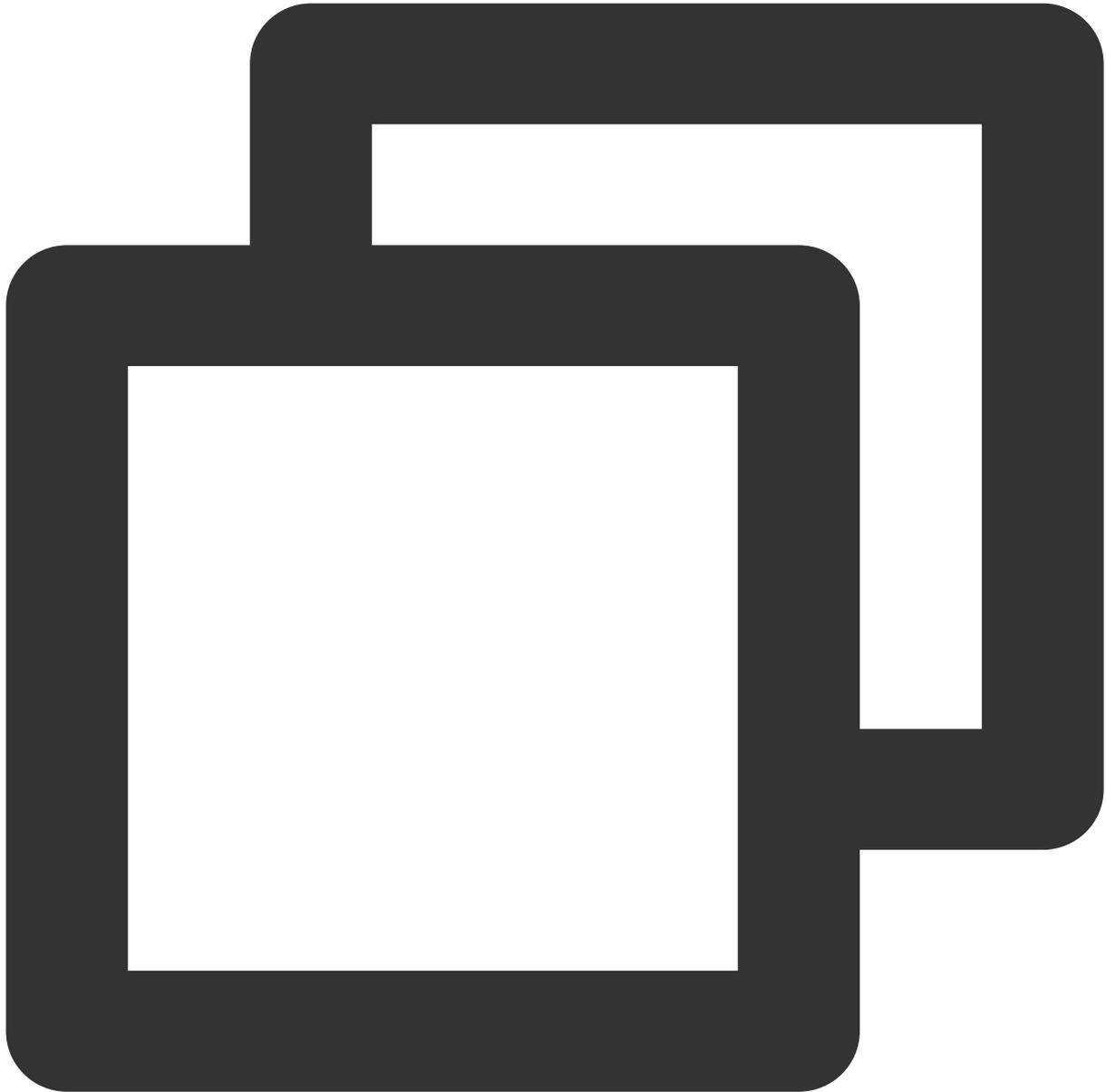
`go2tencentcloud` ディレクトリ下のファイルは移行されません。移行するファイルをこのディレクトリに置かないでください。

2. (オプション) 移行元サーバー上で移行不要のファイルまたはディレクトリを除外します

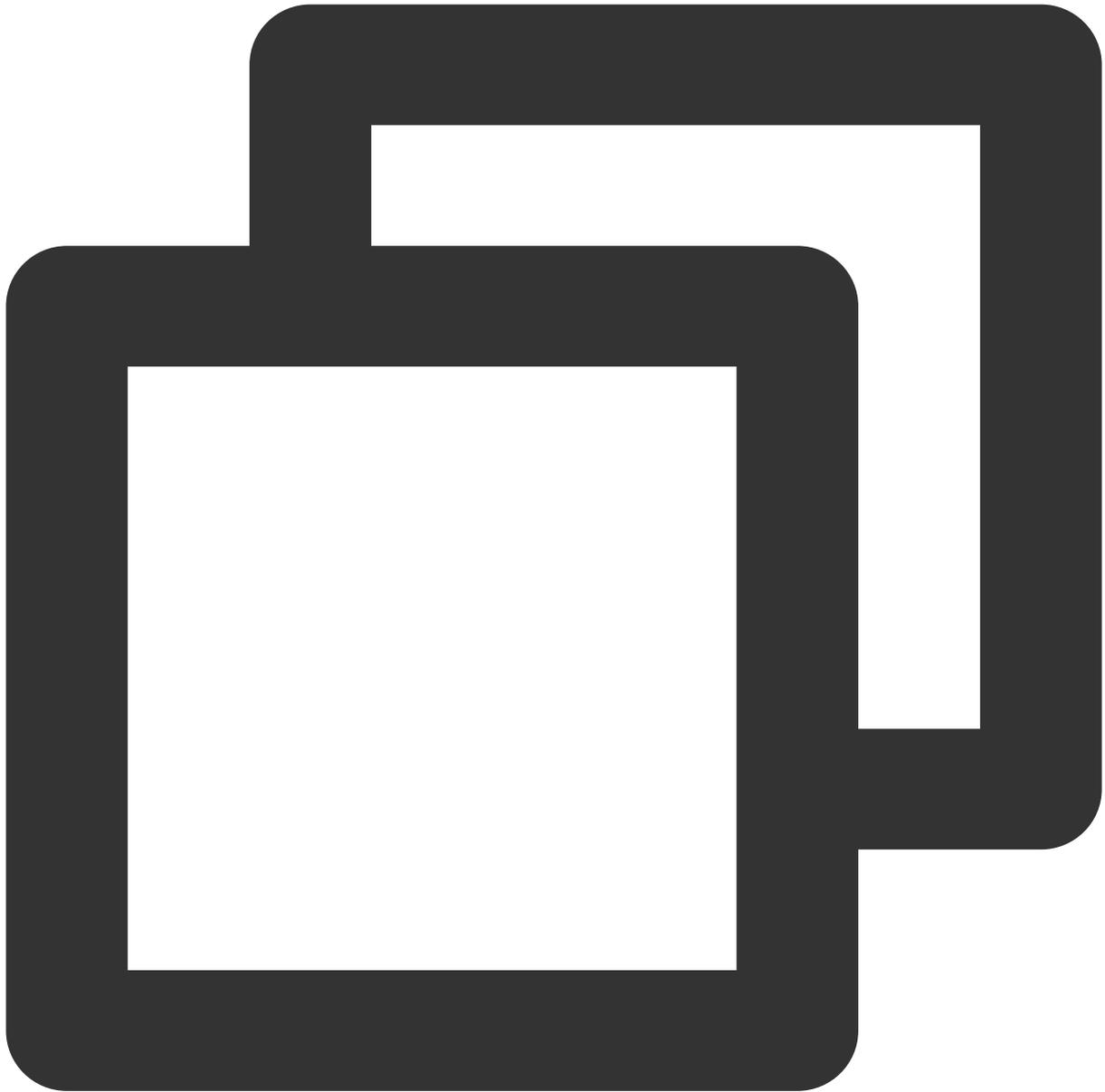
Linux移行元サーバー上で移行不要のファイルおよびディレクトリがある場合、ファイルおよびディレクトリを [rsync\\_excludes\\_linux.txt](#) ファイルに追加できます。

3. 移行元をインポートします。

3.1 例えば、64ビットのLinux移行元サーバーで、root ユーザーとして次のコマンドを順番に実行してツールを実行します。



```
chmod +x go2tencentcloud_x64
```



```
sudo ./go2tencentcloud_x64
```

3.2 [準備事項](#) で取得したアカウントのAPIアクセスキーの `SecretId` および `SecretKey` を入力し、**Enter**を押します。下図に示すとおり：

```
[root@VM-0-28-centos go2tencentcloud]# ./go2tencentcloud_x64
[2021-11-29 10:47:25] Start go2tencentcloud 2.2.3
[2021-11-29 10:47:25] Start loading data...
Please Enter SecretId: 
Please Enter SecretKey: *****
```

次のメッセージが表示されたら、移行元サーバーは正常にインポートされています。CVM コンソールに移動してサーバーを表示できます。

```
[2021-11-29 10:47:54] Load user.json successfully.
[2021-11-29 10:47:54] Load client.json successfully.
[2021-11-29 10:47:54] Calculating the size of file system, please wait...
[2021-11-29 10:47:55] Check environment...
[2021-11-29 10:47:59] Check environment successfully.
[2021-11-29 10:47:59] Start import source server...
[2021-11-29 10:47:59] Import source server [server-03tw3wlr] success
```

1. 移行ツールgo2tencentcloud.zipを移行元サーバーに [ダウンロード](#) またはアップロードします。この圧縮ファイルを解凍してgo2tencentcloudフォルダーを入手し、その中の「go2tencentcloud-windows」を開くと以下のディレクトリが表示されます。

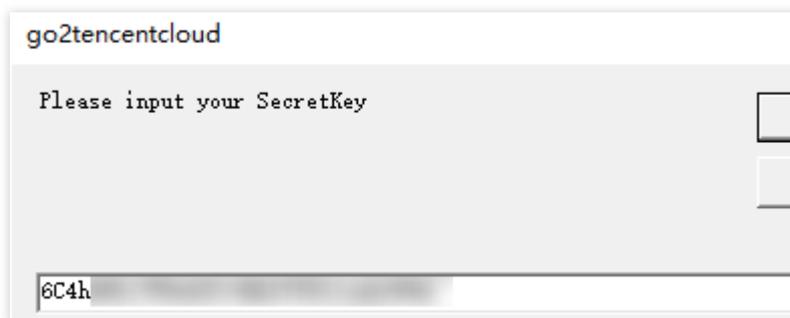
logs	2022/7/6 14:39
client.exe	2022/11/2 14:43
client.json	2022/11/2 14:43
go2tencentcloud_x64.exe	2022/11/2 14:43
user.json	2022/11/2 14:43

2. 以下の方法で「go2tencentcloud\_x64.exe」アプリケーションを実行します。

方法1：「go2tencentcloud\_x64.exe」を右クリックし、管理者権限で「go2tencentcloud\_x64.exe」を実行し、ポップアップした画面でSecretId、SecretKeyを入力します。

方法2：管理者権限でcmdまたはpowershellコマンドライン：cd /d "go2tencentcloud\_x64.exeが所在するディレクトリの絶対パス"を起動し、go2tencentcloud\_x64.exeを実行します。

3. ポップアップした画面で Tencent Cloud API キー (SecretIdと SecretKey) を入力します。



4. 以下のメッセージが表示された場合は、移行元がすでにコンソールにインポートされています。コンソールで移行元を確認できます。

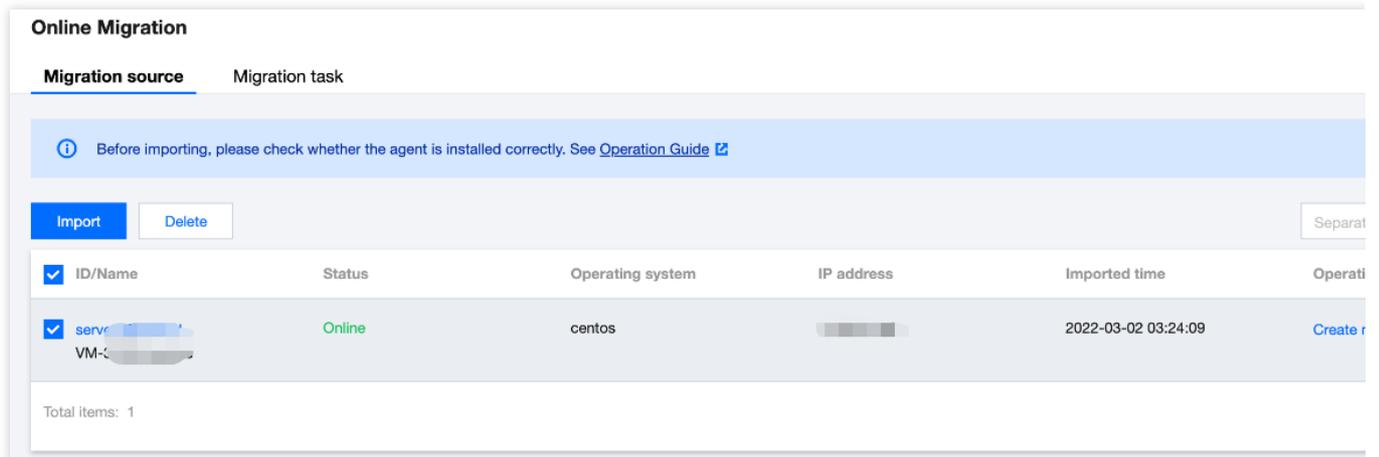
```
[2022-11-02 14:47:20] Start go2tencentcloud 2.2.3
If the input window does not pop up, there may be a problem with your operating system.
Try manually modifying the SecretId and SecretKey fields in user.json[2022-11-02 14:47:34] Load user.json successfully.
[2022-11-02 14:47:34] Load client.json successfully.
[2022-11-02 14:47:34] Calculating the size of file system, please wait...
[2022-11-02 14:47:34] Check environment successfully.
[2022-11-02 14:47:35] Start import source server...
[2022-11-02 14:47:35] Import source server [server-1[redacted]] successfully.
[2022-11-02 14:47:35] Start check migrate job status...
Waiting for a migrate job to be created in the console, Used: 00:00:03
```

#### 説明：

「Import source server successfully」が表示されない場合は、移行元のインポートが失敗したことを意味します。ログ（デフォルトでは移行ツールディレクトリ下にあるlogs/logファイル）を確認して問題を解決した後、移行ツールを再実行して移行元をインポートすることができます。

#### コンソールでの移行元サーバーの確認

[オンライン移行コンソール](#) にログインし、インポートされた移行元を確認します。サーバーのステータスは**オンライン**となっています。下図に示すとおり：



The screenshot shows the 'Online Migration' interface. At the top, there are two tabs: 'Migration source' (selected) and 'Migration task'. Below the tabs is a blue information banner with an 'i' icon and the text: 'Before importing, please check whether the agent is installed correctly. See [Operation Guide](#)'. Below the banner are two buttons: 'Import' (blue) and 'Delete' (white). To the right of these buttons is a 'Separate' button. Below the buttons is a table with the following columns: 'ID/Name', 'Status', 'Operating system', 'IP address', 'Imported time', and 'Operati'. The table contains one row with the following data: 'serv... VM-...', 'Online', 'centos', a masked IP address, '2022-03-02 03:24:09', and 'Create r'. Below the table, it says 'Total items: 1'.

### ご注意：

移行元を正常にインポートした後、移行タスクの実行が完了するまで、インスタンス内の移行ツールを停止しないでください。停止すると、移行元がオフラインになり、移行タスクを完了できません。

## 手順3：移行タスクの作成

### 1. 移行タスクの作成

[オンライン移行コンソール](#) にログインし、対象の移行元がある行の右側の**移行タスクの作成**をクリックします。**移行タスクの作成**画面が表示されます。この画面で以下の情報を参照して設定します。下図に示すとおり：

### Create migration task ✕

Selected: 1 Migration source [Collapse](#)

ID/name	Status	Operating system
[blurred]	Online	windows

▲ Basics

Target region ▼

Task name

Task description

Target type  CVM image  CVM instance

Image name

Network mode  Public network  Private network

Configure incremental sync  When it is enabled, you can configure the incremental sync duration.

Scheduled start time  If it's not selected, only the task is created.

▶ Advanced (Optional)

移行タスクの詳細設定内容は、以下のとおりです。

基本オプション：

アイテム	入力必須	説明
移行先リージョン	はい	移行元サーバーの移行先となる Tencent Cloudリージョン。リー

		<p>ジョンの詳細については、<a href="#">リージョンとアベイラビリティゾーンドキュメント</a>をご参照ください。</p>
タスク名	はい	移行タスクの名前。
タスクの説明	いいえ	移行タスクの説明。
ターゲットタイプ	はい	<p>Tencent Cloud に移行する移行元サーバーのターゲットタイプを設定します。</p> <p><b>CVMイメージ</b>：移行完了後、移行元サーバーのCVMイメージが生成されます。</p> <p>イメージ名：移行元に対して生成されるターゲットCVM イメージの名前。名前がすでに存在する場合は、移行タスク ID が名前に追加されます。</p> <p><b>CVMインスタンス</b>：移行先リージョン内のCVMインスタンスを移行先として選択します。</p> <p>移行先インスタンス：移行先インスタンスと移行元サーバーには同じOSを使用することをお勧めします。例えば、CentOS 7 移行元サーバーを移行するには、移行先として CentOS 7 CVM を選択します。</p>
ネットワークモード	はい	<p>データを転送するために使用されるネットワークタイプを設定します。</p> <p><b>パブリックネットワーク経由のデータ転送</b>：移行先CVMまたはリレーインスタンスにデータを移行および転送する場合は、パブリックネットワークを使用します。</p> <p><b>プライベートネットワーク経由のデータ転送</b>：移行先CVMまたはリレーインスタンスにデータを移行および転送する場合は、プライベートネットワークを使用します。詳細については、<a href="#">プライベート</a></p>

		<p>トネットワーク経由の移行をご参照ください。</p> <p>Virtual Private Cloud (VPC) : CVMイメージに移行する場合、リレーインスタンスはVPC内に作成されます。</p> <p>サブネット : CVMイメージに移行する場合、リレーインスタンスはサブネット内に作成されます。</p>
移行方法	はい	<p>Linux インスタンスの場合:</p> <p><b>Linuxファイルレベルの移行</b> : 移行の粒度はファイルレベルであり、互換性は高く、転送効率は比較的低くなります。</p> <p><b>Linuxブロックレベルの移行</b> : 移行の粒度はディスクのロジックストレージユニットの「ブロック」レベルであり、転送効率は高く、互換性は比較的低くなります。</p> <p><b>Windowsブロックレベルの移行</b> : 移行の粒度はディスクのロジックストレージユニットの「ブロック」レベルであり、Windows移行では、互換性が高く、転送効率が高いブロックレベルの移行がデフォルトで採用されています。</p>
増分同期の構成	いいえ	<p>増分同期時間をカスタマイズし、データを継続的に同期し、移行の配信時間を柔軟に制御します。</p> <p><b>無効化</b> : 移行ツールによって増分移行を自動的に認識して実行し、通常は1回実行されます。</p> <p><b>有効化</b> : 増分同期の実行時間を自由に選択でき、ツールは増分データをTencent Cloudに継続的に同期します。タスクリストで増分同期を手動で停止することもできます。</p>
予約実行時間	いいえ	<p>移行タスクを作成後、設定した時間に自動的に移行タスクを開始し</p>

ます。予約実行時間は最短で現在時刻の10分後に設定できます。

高度な設定（オプション）：

アイテム	入力必須	説明
転送速度制限 (KB/s)	いいえ	移行中、データ転送の帯域幅の上限(0 ~ 25600 KB/s)。デフォルトでは0に設定されています。現在、Windows移行はこのオプションをサポートしていません。
Checksum 検証	いいえ	有効にすると、データの整合性チェックが強化されますが、転送速度は遅くなる場合があります。現在、Windows移行はこのオプションをサポートしていません。

## 2. 移行タスクの起動

説明：

スケジュールされたタスクは、この手順をスキップすることができます。移行タスクは、スケジュールされた時刻に移行を自動的に実行します。

移行タスクを作成した後、**移行タスク**タブをクリックして移行タスクを確認することができます。下図に示すとおり：

The screenshot shows the 'Online Migration' console with the 'Migration task' tab selected. A message at the top states: 'If the migration task fails, please check the migration logs. See Operation Guide'. Below this are 'Start/restart' and 'Delete' buttons. A table lists migration tasks with columns for Task ID/name, Task status, Source ID/Name, Target region, Destination, and Ope. One task is shown with ID 'migrate-1c7k0gh1 test-task', status 'Pending start up', source 'server-r8lbz6wd VM-32-69-centos', and target region 'Guangzhou'. A 'Separat' button is visible on the right. At the bottom, it says 'Total items: 1'.

タスクの右側にある**開始/リトライ**をクリックしてタスクを開始し、表示された画面から**OK**をクリックすると、移行タスクを開始できます。このとき、タスクのステータスは「移行中」に変わります。下図に示すとおり：

**Online Migration**

Migration source **Migration task**

*i* If the migration task fails, please check the migration logs. See [Operation Guide](#)

Start/restart Delete Separate

<input type="checkbox"/> Task ID/name	Task status	Source ID/Name	Target region	Destination	Op
<input type="checkbox"/> migrate-1c7k0gh1 test-task	Migrating	server-r8lbz6wd VM-32-69-centos	Guangzhou		Cre

Total items: 1

**ご注意：**

移行先がCVM インスタンスの場合、移行開始後に移行先CVMは移行モードに入ります。移行を完了して移行モードが終了するまで、移行先CVMに対してシステムの再インストール、シャットダウン、破棄、パスワードのリセットなどの操作を行わないでください。

移行先がCVMイメージの場合、移行開始後にアカウント下に `do_not_delete_csm_instance` という名前のリレーインスタンスが作成されます。移行が完了して、今回作成されたリレーインスタンスが自動的に破棄されるまで、リレーインスタンスに対してシステムの再インストール、シャットダウン、破棄、パスワードのリセットなどの操作を行わないでください。

**手順4：移行後のチェック****1. コンソールで移行の進行状況の確認**

移行タスクのステータスが**成功**になると、移行処理が正常に完了したことを示します。下図に示すとおり：

**Online Migration**

Migration source **Migration task**

*i* If the migration task fails, please check the migration logs. See [Operation Guide](#)

Start/restart Delete Separate

<input type="checkbox"/> Task ID/name	Task status	Source ID/Name	Target region	Destination	Op
<input type="checkbox"/> migrate-1c7k0gh1 test-task	Successful	server-r8lbz6wd VM-32-69-centos	Guangzhou		Cre

Total items: 1

**説明：**

データ転送に必要な時間は、移行元データのサイズ、ネットワーク帯域幅などの要因に左右されます。移行が完了するまでお待ちください。

移行タスクの開始後、移行タスクのある行で**一時停止**をクリックすると、移行タスクを停止できます。

移行ツールはデータ転送の中断からの再開をサポートしています。タスクの一時停止後、**開始/リトライ**をクリックすると、前回一時停止したポイントから移行を継続できます。

移行タスクはデータ転送段階での一時停止のみサポートしています。コンソールでの移行タスク中に**一時停止**をクリックすると、移行ツールはデータ転送段階でデータの転送を一時停止します。

移行中に消費時間が長くなりすぎ、今回の移行を中止したい場合は、まず移行タスクを一時停止してから**削除**をクリックすると、今回の移行タスクをキャンセルすることができます。

## 2. 移行後のチェック

### 移行に失敗した場合：

-ログファイル（デフォルトでは移行ディレクトリ下のログファイル）に出力されている内容を確認し、操作ガイドまたは [サーバー移行に関するよくあるご質問](#) ドキュメントを参照し、問題のトラブルシューティングを行ってください。問題を解決した後、移行タスクの操作列で**開始/リトライ**をクリックすると、移行タスクを再開できます。

### 移行に成功した場合：

移行先がCVMの場合は、移行先CVMが正常に起動できるか、移行先CVMのデータが移行元サーバーと一致しているか、ネットワークが正常か、他のシステムサービスが正常かなどを確認してください。

移行先がCVMイメージの場合は、移行タスクのある行の**CVMイメージID**をクリックし、[CVMイメージページ](#)に進むとこのイメージの情報を確認でき、このイメージを使用してCVMインスタンスを作成することができます。

ご質問がある場合や移行エラーが発生した場合は、[サービス移行に関するFAQ](#)を参照するか、[お問い合わせ](#) ください。

# オンライン移行：コンソールでのワンクリック移行

最終更新日：：2023-07-27 11:21:18

このドキュメントでは、コンソールの「ワンクリック移行」方法を通じて移行元サーバーを Tencent Cloud CVM に移行する方法について説明します。

## 概要

ワンクリック移行は [オンライン移行](#) を簡潔化したソリューションであり、移行元サーバーへのログインやツールのダウンロードなどの複雑な操作が不要になり、ワンクリックで移行タスクを一括作成し、移行元サーバー上の OS やアプリケーションなどのデータを Tencent Cloud に一括移行することができます。

ワンクリック移行は、Linux と Windows の両方の OS をサポートします。また、Tencent Cloud CVM コンソールのオンライン移行ページで移行の進行状況を確認することもできます。

## 制限事項

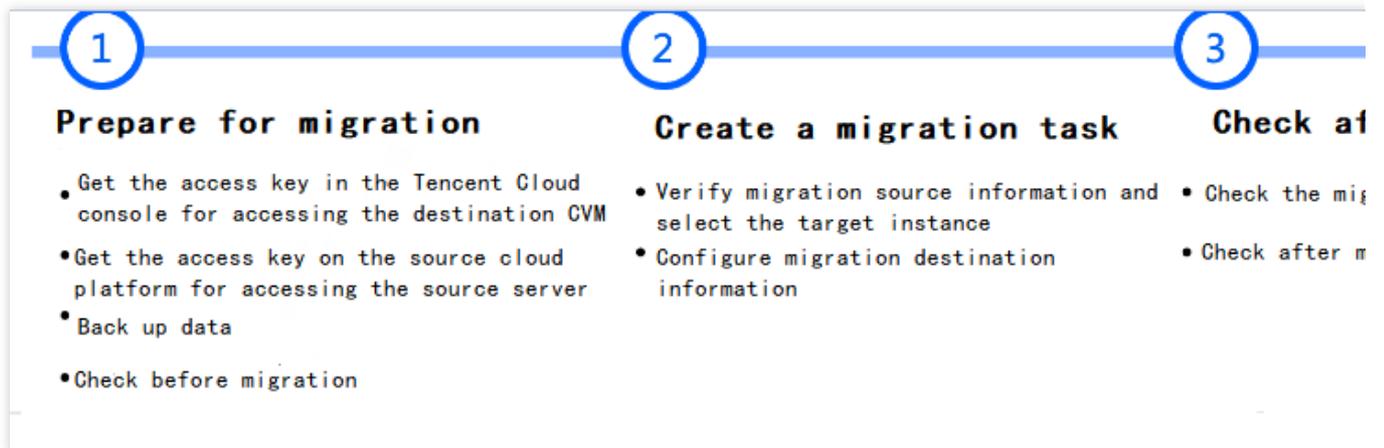
「ワンクリック移行」方法を使用するには、移行元サーバーでクラウドアシスタント (Alibaba Cloud ECS Cloud Assistant など) をインストールし、パブリック IP を構成し、VPC (クラシックネットワークをサポートしない) を使用する必要があります。

現在、ワンクリック移行では Alibaba Cloud サーバーの Tencent Cloud への移行のみをサポートしており、他のプラットフォームはサポートしません。

コンソールのワンクリック移行機能は継続的に最適化されているため、現在は特定のシナリオでのみサポートされています。ご要望を満たせない場合、[オンライン移行：クライアントから移行元のインポート](#) 方法を使用することをお勧めします。この移行方法はより強力な互換性を持っています。

## 移行ワークフロー

コンソールのワンクリック移行によるオンライン移行の流れを次の図に示します。



## 移行手順

### 手順1：移行の準備

#### Tencent Cloud コンソールからアクセスキーを取得します

CAM コンソールの [APIキー管理](#) ページでAPI キーを作成し、\*\*SecretId と SecretKey \*\*を取得します。詳細については、[アクセスキー](#) をご参照ください。

#### 説明：

サブアカウントを使用してコンソールで移行を実行する場合、ルートアカウントで [CAMコンソール](#) にログインし、サブアカウントにQcloudCSMFullAccess とQcloudCVMFullAccess 権限を付与する必要があります。

#### 移行元クラウドプラットフォームでアクセスキーを取得します

Alibaba CloudのAccessKeyIdとAccessKeySecretを取得する手順は以下の通りです：

1.1 Alibaba Cloud RAM コンソールにログインして、**Identities > Users** ページに入ります。

1.2 **Create User** をクリックし、アクセス方法から**OpenAPI Access** (他のアクセス方法を選択しても有効にならない) を選択して、作成を確認した後、AccessKeyId と AccessKeySecret の情報を保存します。詳細な操作手順については、[RAM ユーザーの準備](#) をご参照ください。

1.3 ユーザリストから作成したユーザに**権限を追加**します。ECS 読み取り専用権限 (AliyunECSReadOnlyAccess) と ECS クラウドアシスタント管理権限 (AliyunECSAssistantFullAccess) を追加します。詳細な操作手順については、[Grant permissions to a RAM user](#) をご参照ください。

#### 移行元サーバーのアプリケーションの一時停止 (オプション)

移行中に既存のアプリケーションへの影響を回避するために、移行元サーバー上のすべてのアプリケーションを停止することをお勧めします。

#### 移行元サーバーと移行先CVM上のデータのバックアップ (オプション)

移行前に次の方法でデータをバックアップすることをお勧めします。

移行元サーバー：スナップショット機能またはその他の方法を使用して、移行元サーバー上のデータをバックアップできます。

移行先CVM：[スナップショットの作成](#)などの方式を選択して、移行先CVMのデータをバックアップできます。

### 移行先CVMの確認

移行先がCVMインスタンスの場合は、移行先のCVMを確認する必要があります。

移行先CVM	<ol style="list-style-type: none"><li>1. ストレージ容量：移行先CVMのクラウドディスク（システムディスクとデータディスクを含む）には、移行元サーバーから移行されたデータを保存するための十分な容量が必要です。</li><li>2. セキュリティグループ：セキュリティグループでポート80、443、および3389を開放します。</li><li>3. 帯域幅：移行をより円滑に進めるためには、移行元と移行先の両方の環境の帯域幅を最大化することをお勧めします。移行プロセス中に消費されるトラフィックは、移行されたデータの量とほぼ同じになります。必要に応じて、移行前にネットワーク課金モデルを調整します。</li><li>4. ネットワーク設定：移行元または移行先サーバーがIPv6のみをサポートし、IPv4をサポートしていない場合は、<a href="#">client.jsonファイルのパラメータ説明をご参照ください</a>。</li></ol>
--------	--

### ワンクリック移行ページに入ります

1.1 CVMコンソールにログインし、[サービス移行](#) > [オンライン移行](#) ページに入ります。移行元のインポートをクリックして、[移行元のインポート](#) ページに移動します。

1.2 [ワンクリック移行](#)を選択して、移行タスクを一括で作成することができます。

### 手順2：移行タスクの作成

#### 1. タスクの設定

タスクの名前と説明を入力します。

#### 2. 移行元の設定

移行元のサービスプロバイダーはデフォルトではAlibaba Cloud ECSを選択します。移行元サーバーへのアクセス権限を持っていることを確認するために、下図に示すように、Alibaba CloudアカウントのAccessKeyとSecretKey（[取得方法](#)）を入力して検証する必要があります：

#### ご注意：

キーを大切に保管してください。移行完了後に、キーを削除または無効化することをお勧めします。

## 2 Migration source information

Service provider

Alibaba Cloud ECS

AccessKey \*

Enter the AccessKey

SecretKey \*

Enter the SecretKey

Make sure the key pair has permission to access the source instance.

Verify

### 3. 移行先の設定

移行先のサービスプロバイダーはデフォルトではTencent Cloud CVMを選択します。**Tencent Cloud CVMの権限を取得**するために、Tencent Cloud APIキーのSecretIdとSecretKey（[取得方法](#)）を入力する必要があります。[APIキー管理](#) からキーの情報をそのままコピーできます。APIキーが正しくなければ、移行に失敗しますので、APIキーが正しいことを確認してください。

#### ご注意：

キーを大切に保管してください。移行完了後に、キーを削除または無効化することをお勧めします。

### Migration destination information

Service provider

Tencent Cloud CVM

[Create SecretId and SecretKey](#)

SecretId \*

Enter the SecretId

SecretKey \*

Enter the SecretKey

The SecretId and SecretKey are used to grant permission to the migration tool to access Tencent Cloud CVM.

### 4. 移行情報の設定

4.1 移行元の情報を確認したら、**移行元の追加**をクリックして、ポップアップした画面から移行するインスタンスを選択します。

4.2 画面の左上隅でリージョンを選択し、**リージョン内のインスタンスリスト**を取得します。リージョンの後の数字はインスタンスの数を示します。

4.3 移行するインスタンスを選択して、それが右側の**選択済み**リストに追加されます。

#### 説明：

**マルチインスタンス、マルチリージョン**の一括移行がサポートされます。移行元を複数回追加することができます。

現在、最大5つのインスタンスを一括移行できます。

4.4 **OK**をクリックすると、移行元情報リストに移行待ちのインスタンス情報が表示されます。操作列で**移行先の追加**をクリックし、移行先の情報を設定できます。

4.5 **移行先の追加**画面で、リージョンと移行先のタイプを設定します。

アイテム	入力必須	説明
移行先リージョン	はい	移行元サーバーの移行先となるTencent Cloudリージョン。リージョンについては、 <a href="#">リージョンとアベイラビリティゾーン</a> をご参照ください。
移行先タイプ	はい	Tencent Cloud に移行する移行元サーバーのターゲットタイプを設定します。 <b>CVMイメージ</b> ：移行完了後、移行元サーバーのCVMイメージが生成されます。イメージ名：移行元に対して生成されるターゲットCVMイメージの名前。イメージ名がターゲットリージョンにすでに存在する場合、移行タスクはイメージ名にタスクIDを自動的に追加します。 <b>CVMインスタンス</b> ：移行先リージョン内のCVMインスタンスを移行先として選択します。移行先インスタンス：移行先CVMインスタンスと移行元サーバーには同じOSを使用することをお勧めします。例えば、CentOS 7 移行元サーバーを移行する場合、移行先としてCentOS 7 CVMを選択します。さらに、移行先CVMインスタンスのシステムディスクとデータディスクの容量は、移行元サーバーの容量よりも大きい必要があります。

5. 「**新規作成**」をクリックして移行タスクを開始します。次のようなメッセージが表示されますので、ご注意ください。

移行元でタスクの実行が時間かかりますので、しばらく経ってからコンソールで進捗状況を確認できます。

移行元サーバー環境の異常や誤った情報により移行元のインポートに失敗した場合、Tencent Cloudコンソールに失敗の原因を表示しない可能性があります。この場合、タスクを再作成するか、[オンライン移行]をご利用ください。

### 手順3：移行後の確認

## 1. 移行状態と進行状況の確認

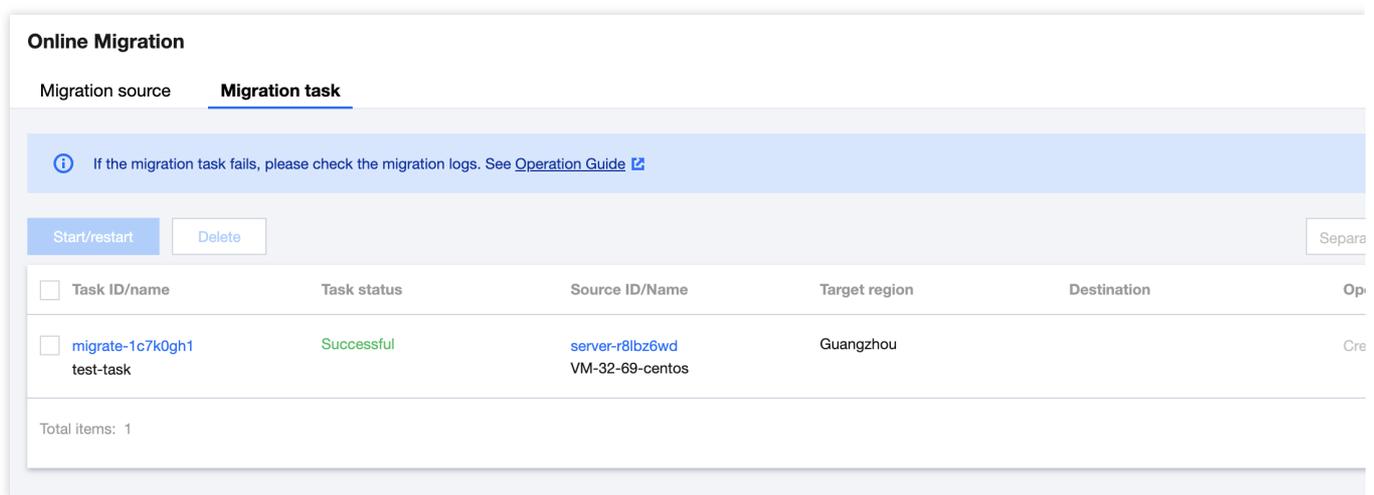
正常に作成された移行タスクは自動的に実行されます。[移行元ページ](#)で移行元の情報を確認できます。また、[移行タスク](#) ページでタスクの進行状況を確認できます。

移行先がCVMの場合、移行開始後に移行先CVMは移行モードに入ります。移行を完了して移行モードが終了するまで、移行先CVMに対してシステムの再インストール、シャットダウン、破棄、パスワードのリセットなどの操作を行わないでください。

移行先がCVMイメージの場合、移行開始後にアカウント下に `do_not_delete_csm_instance` という名前のリレーインスタンスが作成されます。移行が完了して、今回作成されたリレーインスタンスが自動的に破棄されるまで、リレーインスタンスに対してシステムの再インストール、シャットダウン、破棄、パスワードのリセットなどの操作を行わないでください。

## 2. 移行タスクの完了を待つ

移行タスクのステータスが**成功**になると、移行処理が正常に完了したことを示します。下図に示すとおり：



The screenshot shows the 'Online Migration' console. The 'Migration task' tab is selected. A message states: 'If the migration task fails, please check the migration logs. See Operation Guide'. Below this are 'Start/restart' and 'Delete' buttons. A table lists migration tasks with columns: Task ID/name, Task status, Source ID/Name, Target region, Destination, and Op. One task is listed with ID 'migrate-1c7k0gh1 test-task', status 'Successful', source 'server-r8lbz6wd VM-32-69-centos', target region 'Guangzhou', and destination 'Cre'. A 'Total items: 1' indicator is at the bottom.

Task ID/name	Task status	Source ID/Name	Target region	Destination	Op
<input type="checkbox"/> migrate-1c7k0gh1 test-task	Successful	server-r8lbz6wd VM-32-69-centos	Guangzhou		Cre

### 説明：

データ転送の消費時間は、移行元データのサイズ、ネットワーク帯域幅などの要因に左右されます。移行が完了するまでお待ちください。

移行タスクの開始後、移行タスクのある行で**一時停止**をクリックすると、移行タスクを停止できます。

移行ツールはデータ転送の中断からの再開をサポートしています。タスクの一時停止後、**開始/リトライ**をクリックすると、前回一時停止したポイントから移行を継続できます。

移行タスクはデータ転送段階での一時停止のみサポートしています。コンソールでの移行タスク中に**一時停止**をクリックすると、移行ツールはデータ転送段階でデータの転送を一時停止します。

移行中に消費時間が長くなりすぎ、今回の移行を中止したい場合は、まず移行タスクを一時停止してから**削除**をクリックすると、今回の移行タスクをキャンセルすることができます。

## 3. 移行後のチェック

### 移行に失敗した場合：

ログファイル（デフォルトでは移行ディレクトリ下のログファイル）に出力されている内容を確認し、操作ガイドまたは [サーバー移行に関するよくあるご質問](#) ドキュメントを参照し、問題のトラブルシューティングを行って

ください。問題を解決した後、移行タスクの操作列で**開始/リトライ**をクリックすると、移行タスクを再開できます。

**移行に成功した場合：**

移行先がCVMの場合は、移行先CVMが正常に起動できるか、移行先CVMのデータが移行元サーバーと一致しているか、ネットワークが正常か、他のシステムサービスが正常かなどを確認してください。

移行先がCVMイメージの場合は、移行タスクのある行の「CVMイメージID」をクリックし、[CVMイメージページ](#)に進むとこのイメージの情報を確認でき、このイメージを使用してCVMインスタンスを作成することができます。

ご質問がある場合や移行エラーが発生した場合は、[サービス移行に関するFAQ](#)を参照するか、[お問い合わせ]ください。

# マイグレーションツールの説明

## 互換性とツール設定の説明

最終更新日：：2023-05-17 15:26:47

### サポートされているオペレーティングシステム

現在オンラインマイグレーションツールがサポートする移行元サーバーのOSは以下を含みますが、これらのOSに限定されません。

Linux OS	Windows OS
CentOS 5/6/7/8	Windows Server 2008 Windows Server 2012 Windows Server 2016 Windows Server 2019 Windows Server 2022
Ubuntu 10/12/14/16/18/20	
Debian 7/8/9/10	
SUSE 11/12/15	
openSUSE 42	
Amazon Linux AMI	
Red Hat 5/6/7/8	
Oracle Linux 5/6/7/8	

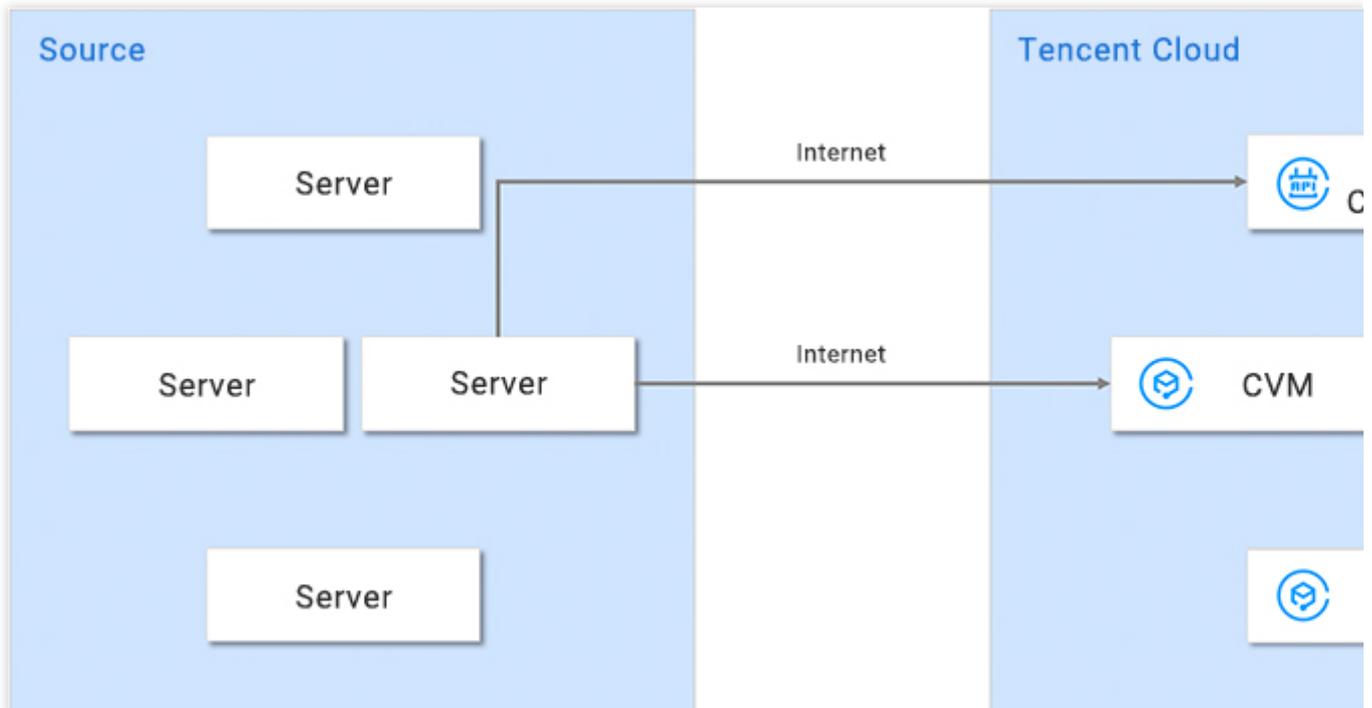
### サポートされているマイグレーションモード

パブリックネットワークマイグレーションモード

プライベートネットワークマイグレーションモード

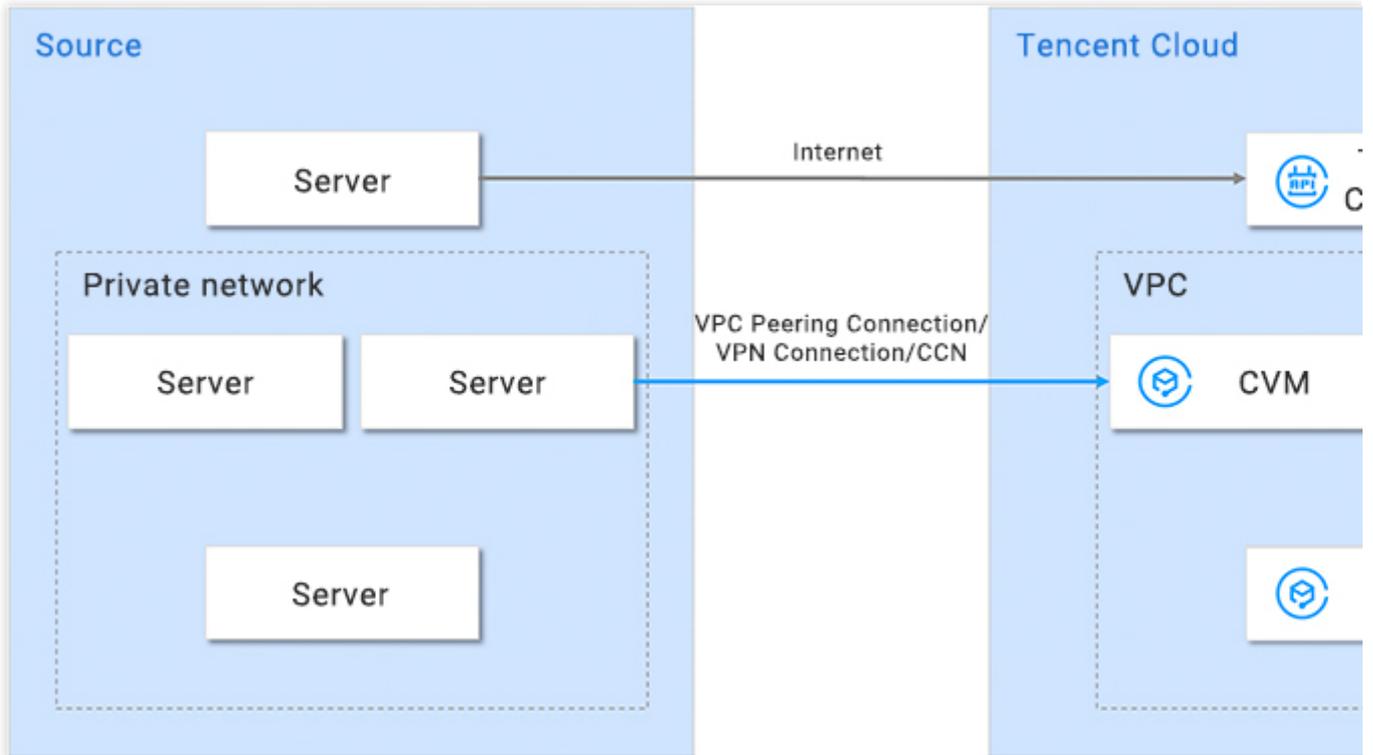
お客様の移行元サーバーと移行先CVMの両方にパブリックネットワークアクセス機能がある場合は、パブリックネットワークマイグレーションモードを使用してマイグレーションができます。

現在のパブリックネットワークマイグレーションモードでは、移行元サーバーはインターネット経由でTencent Cloud APIにアクセスし、マイグレーションリクエストを送信するとともに、データを移行先CVMに転送して、移行元サーバーをTencent Cloudの移行先CVMにマイグレーションします。パブリックネットワークマイグレーションモードを下図に示します：

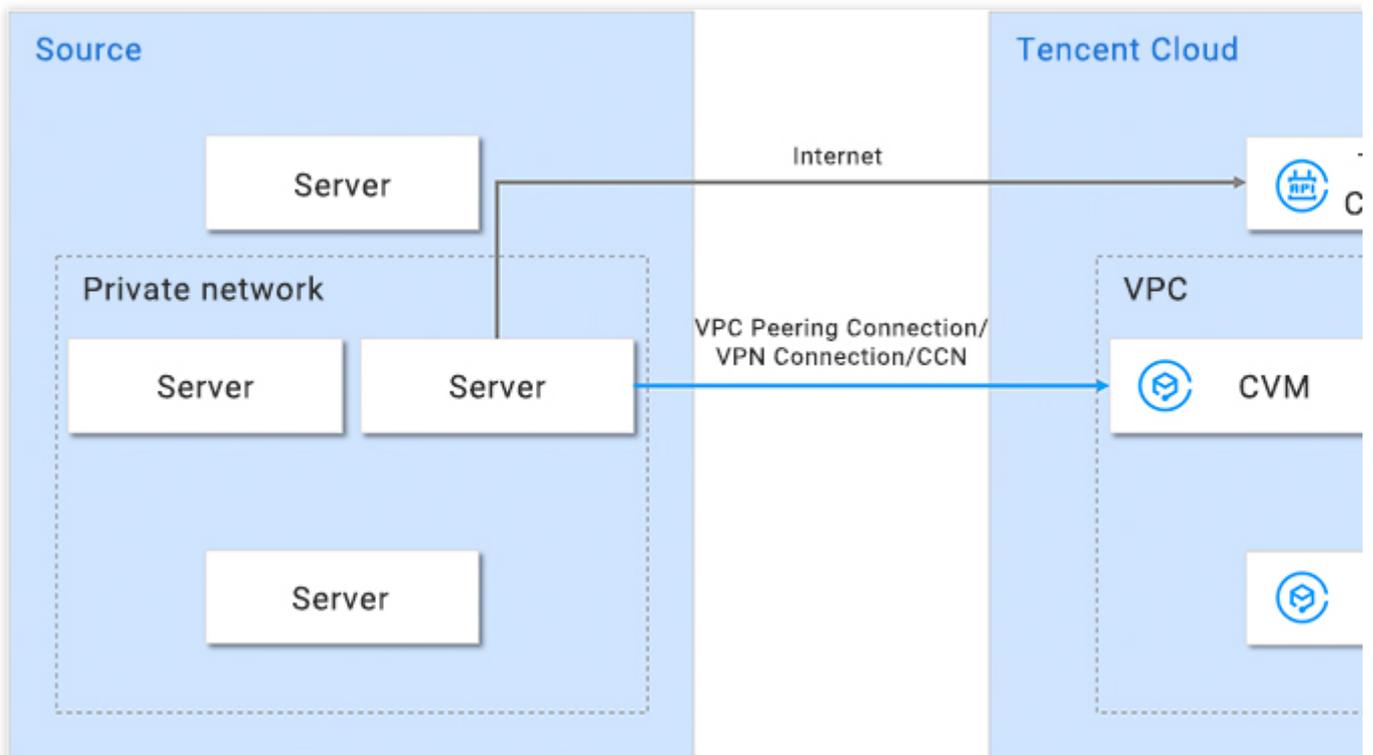


お客様の移行元サーバーまたは移行先CVMがプライベートネットワークまたはVPCにあり、移行元サーバーがインターネット経由で移行先クラウドサーバーとの接続を直接確立できない場合は、ツールのプライベートネットワークマイグレーションモードを使用してマイグレーションができます。[VPCピアリング接続](#)、[VPN接続](#)、[CCN](#)または[ダイレクト接続](#)といった方法で、移行元サーバーと移行先CVM間で接続チャネルを確立する必要があります。

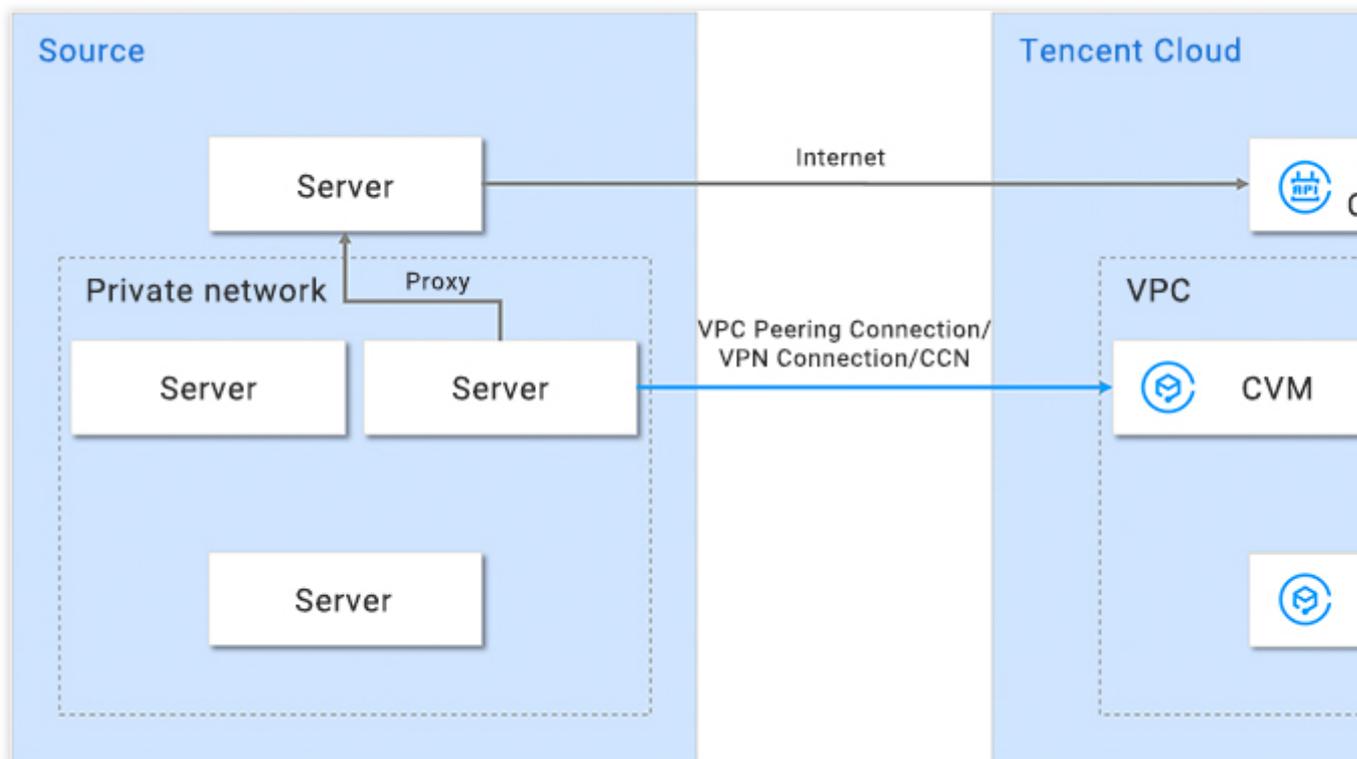
**シナリオ1：**（このシナリオは、[ツールを使用したマイグレーション](#)のみをサポートする）お客様の移行元サーバーまたは移行先CVMがパブリックネットワークにアクセスできない場合は、まずパブリックネットワークアクセス機能を備えたホスト（ゲートウェイなど）を介してインターネット経由でTencent Cloud APIにアクセスすることにより、マイグレーションリクエストを発することができます。次に、接続チャネルを介して移行先CVMにデータを送信してマイグレーションします。このシナリオでは、移行元サーバーと移行先CVMにパブリックネットワークへのアクセス機能は必要ありません。



**シナリオ2**：お客様の移行元サーバーがパブリックネットワークにアクセスできる場合、まずインターネット経由で移行元サーバー上のTencent Cloud APIにアクセスしてマイグレーションリクエストを発してから、次に接続チャンネルを介して移行先CVMにデータを送信してマイグレーションすることができます。このシナリオでは、移行元サーバーにパブリックネットワークへのアクセス機能が必要ですが、移行先CVMには必要ありません。



**シナリオ3**：お客様の移行元サーバーがプロキシ経由でパブリックネットワークにアクセスできる場合は、まずネットワークプロキシ経由で移行元サーバー上のTencent Cloud APIにアクセスしてマイグレーションリクエストを発することができます。次に、接続チャンネルを介して移行先CVMにデータを送信してマイグレーションします。このシナリオでは、移行元サーバーと移行先CVMにパブリックネットワークへのアクセス機能は必要ありません。



## 圧縮パッケージファイルの説明

go2tencentcloud.zip を解凍後のファイルの説明は次のとおりです：

ファイル名	説明
go2tencentcloud-linux.zip	Linux OSのマイグレーション圧縮パッケージです。
go2tencentcloud-windows.zip	Windowsシステムのマイグレーション圧縮パッケージ。
readme.txt	ディレクトリ概要ファイルです。
release_notes.txt	マイグレーションツールの変更ログです。

go2tencentcloud-linux.zip を解凍後のファイルの説明は次のとおりです：

ファイル名	説明

go2tencentcloud_x64	64ビット Linux OS用の移行ツールの実行可能プログラム。
go2tencentcloud_x32	32ビット Linux OS用の移行ツールの実行可能プログラム。
user.json	マイグレーション時のユーザー情報です。
client.json	マイグレーションツールの設定ファイルです。
rsync_excludes_linux.txt	rsync構成ファイル。Linuxシステムで移行する必要のないファイルとディレクトリを除外します。

go2tencentcloud-windows.zip を解凍後のファイルの説明は次のとおりです：

ファイル名	説明
go2tencentcloud_x64.exe	64ビットのWindowsシステムのマイグレーションツールで実行可能なプログラムです。
user.json	マイグレーション時のユーザー情報です。
client.json	マイグレーションツールの設定ファイルです。
client.exe	Windowsシステムの移行で実行可能なプログラムです。

### ご注意：

設定ファイルは削除できません。設定ファイルはgo2tencentcloudの実行可能なプログラムと同じ階層のディレクトリ下に置いてください。

### user.json ファイルパラメータの説明

user.json設定ファイルの説明は下表のとおりです：

パラメータ名	タイプ	入力必須かどうか	説明
SecretId	String	はい	APIにアクセスするためにアカウントで使用されるSecretIdです。詳細については、 <a href="#">アクセスキー</a> をご参照ください。
SecretKey	String	はい	APIにアクセスするためにアカウントで使用されるSecretIdです。詳細については、 <a href="#">アクセスキー</a> をご参照ください。

### client.json ファイルパラメータの説明

client.json設定ファイルの一部の説明は下表のとおりです：

パラメータ名	タイプ	入力	説明

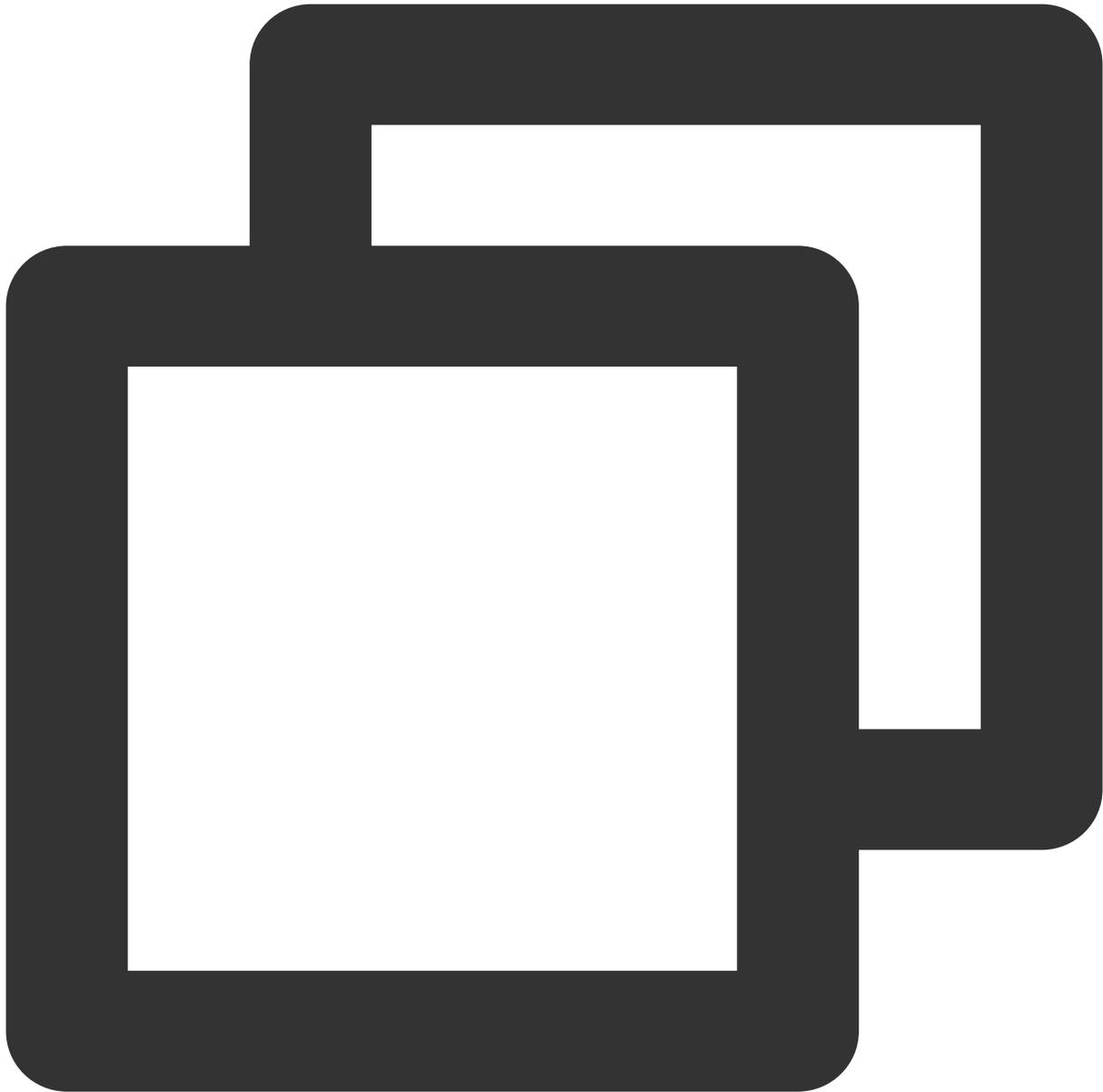
		必須かどうか	
Client.Extra.IgnoreCheck	Bool	いいえ	デフォルト値は <code>false</code> であり、マイグレーションツールはデフォルトではツールの実行開始時に移行元サーバーの環境を自動的にチェックします。チェックを省略したい場合は、 <code>true</code> に設定してください。
Client.Extra.Daemon	Bool	いいえ	デフォルト値は <code>false</code> です。バックグラウンドでマイグレーションツールを実行する必要がある場合、 <code>true</code> に設定してください。
Client.Net.Proxy.Ip	String	いいえ	デフォルト値はNULLです。マイグレーションシナリオがプライベートネットワークのマイグレーション <a href="#">シナリオ3</a> である場合、ネットワークプロキシのIPアドレスを設定してください。
Client.Net.Proxy.Ipv6	Bool	いいえ	デフォルト値は <code>false</code> です。IPv6（マイグレーション時に移行元または移行先にはIPv6のIPしかないなど）でデータを転送する場合、このオプションに <code>true</code> を設定してください。そうしないと、マイグレーションのトラフィックはIPv4で転送されます。
Client.Net.Proxy.Port	String	いいえ	デフォルト値はNULLです。マイグレーションシナリオがプライベートネットワークのマイグレーション <a href="#">シナリオ3</a> である場合、ネットワークプロキシポートを設定してください。
Client.Net.Proxy.User	String	いいえ	デフォルト値はNULLです。マイグレーションシナリオがプライベートネットワークのマイグレーション <a href="#">シナリオ3</a> で、ネットワークプロキシには認証が必要である場合、ネットワークプロキシユーザー名を設定してください。
Client.Net.Proxy.Password	String	いいえ	デフォルト値はNULLです。マイグレーションシナリオがプライベートネットワークのマイグレーション <a href="#">シナリオ3</a> で、ネットワークプロキシには認証が必要である場合、ネットワークプロキシパスワードを設定してください。

**説明：**

上記のパラメータを除き、`client.json`ファイルのその他の設定項目は通常は入力不要です。

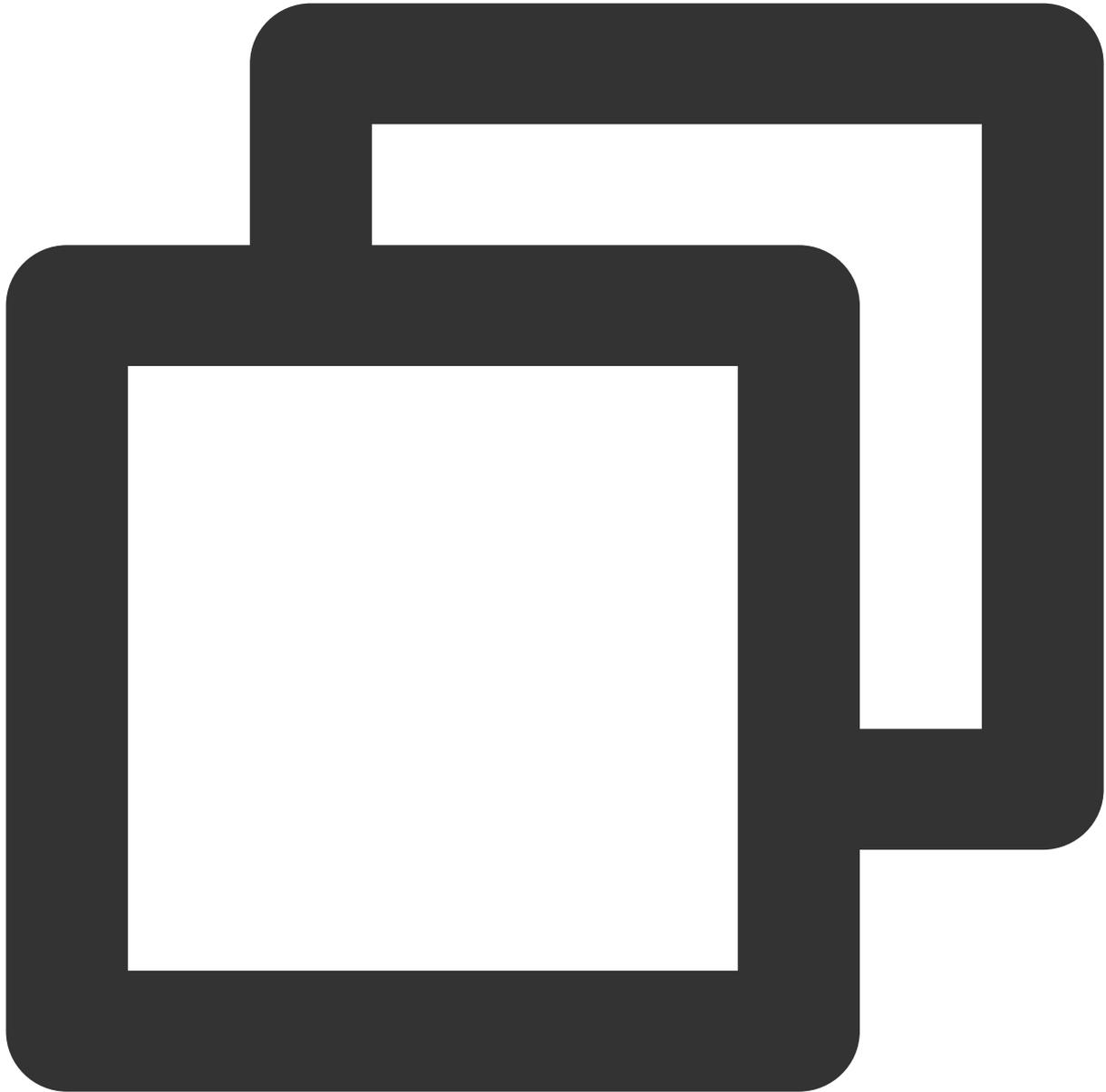
**rsync\_excludes\_linux.txtファイル説明**

このファイルは、移行や転送が不要なLinuxの移行元サーバーのファイル、または指定されたディレクトリにある設定ファイルを除外するために使用されます。次のディレクトリとファイルはデフォルトで除外されていますので、**設定を削除または変更しないでください。**



```
/dev/*  
/sys/*  
/proc/*  
/var/cache/yum/*  
/lost+found/*  
/var/lib/lxcfs/*  
/var/lib/docker-storage.btrfs/root/.local/share/gvfs-metadata/*
```

他のディレクトリやファイルを削除する必要がある場合は、このファイルの最後に内容を追加してください。例えば、`/mnt/disk1` にマウントされているデータディスクのすべての内容は削除されます。



```
/dev/*  
/sys/*  
/proc/*  
/var/cache/yum/*  
/lost+found/*  
/var/lib/lxcfs/*  
/var/lib/docker-storage.btrfs/root/.local/share/gvfs-metadata/*  
/mnt/disk1/*
```

## ツールの実行パラメータの説明

パラメータオプション	説明
--help	ヘルプ情報を印刷します。
--check	移行元サーバーをチェックします
--log-file	ログファイルの名前を設定します。デフォルトはlogです。
--log-level	ログ出力レベルです。値の範囲は1 (ERRORレベル)、2 (INFOレベル)、3 (DEBUGレベル) です。デフォルト値は2です。
--version	バージョン番号を印刷します。
--clean	マイグレーションタスクを中止します。

# 移行時間予測チュートリアル

最終更新日：2022-05-07 16:28:41

このドキュメントでは、オンラインマイグレーションによって、ソースサーバー上のシステム、アプリケーションプログラムなどを自分で作成したコンピューターーム（IDC）やクラウドプラットフォームなどのソース環境からTencent Cloud CVMに移行する場合にかかる時間を予測する方法についてご紹介します。

移行時間は主に移行中のデータ転送速度の影響を受けます。移行元サーバーから移行先リージョンのサーバー間の転送速度をテストすることで、移行時間を予測できます。

## 異なるシナリオにおける移行時間の予測

### シナリオ1

移行タスクの移行先タイプがCVMの場合、移行時間は主に実際のデータ転送時間であると予測されます。

例えば、移行元サーバーの移行対象の全ディスクデータの実際の使用量が50GB、アウトバウンド帯域幅が100Mbpsの場合、全体の移行時間は1.14時間と予測されます。手順は次のとおりです：

#### 1. 単位の換算

実際のブロードバンド速度をMB/sに換算します。 $100\text{Mbps} = 100 / 8 = 12.5\text{MB/s}$

実際のディスクデータ量をMBに換算します。 $50\text{GB} = 50 \times 1024 = 51200\text{MB}$

#### 2. 実際のデータ移行時間の推定

$51200 / 12.5 = 4096\text{秒} = 1.14\text{時間}$

### シナリオ2

移行タスクの移行先タイプがCVMイメージの場合、移行時間には主に実際のデータ転送時間およびイメージ制作時間が含まれます。

例えば、移行元サーバーの移行対象の全ディスクデータの実際の使用量が50GB、アウトバウンド帯域幅が100Mbpsの場合、全体の移行時間は1.23時間と予測されます。手順は次のとおりです：

#### 1. 単位の換算

実際のブロードバンド速度をMB/sに換算します。 $100\text{Mbps} = 100/8 = 12.5\text{MB/s}$

実際のディスクデータ量をMBに換算します。 $50\text{GB} = 50 \times 1024 = 51200\text{MB}$

#### 2. 実際のデータ移行時間の推定

$51200 / 12.5 = 4096\text{秒} = 1.14\text{時間}$

#### 3. イメージ制作時間です。制作速度は約160MB/s

$51200 / 160 = 320\text{秒} = 0.089\text{時間}$

#### 4. 総移行時間

$1.14+0.089=1.23\text{時間}$ 。

## 関連操作：データ転送速度のテスト

**iperf3**ツールを使用してデータ転送速度をテストすることができます。例えば、クライアントからサーバーまでのデータ転送の帯域幅、速度などをテストします。

### 転送速度の影響因子

移行元サーバーのアウトバウンド帯域幅と移行先インスタンスのインバウンド帯域幅。

例えば、移行元サーバーのアウトバウンド帯域幅が50Mbps、移行先インスタンスのインバウンド帯域幅が100Mbpsの場合、理論上、実際の転送速度は50Mbpsを超えることはありません。

移行中は常に帯域幅を完全に占有するわけではありません。移行中は移行先のインスタンス（または中継インスタンス）のインバウンド帯域幅を動的に調整することができます。

移行元サーバーと移行先インスタンスが異なるリージョンにある場合、同じリージョンにある場合と比べて転送速度は遅くなります。

#### 説明：

コンソールによるオンラインマイグレーションの場合、移行先がCVMイメージであれば、移行中に中継インスタンス（名称はdo\_not\_delete\_csm\_instance）が作成されることがあります。帯域幅上限は50Mbpsです。

移行中はコンソール上で移行先のインスタンス（または中継インスタンス）のインバウンド帯域幅を動的に調整し、移行速度を制御することができます。

### Tencent Cloud Linux CVMに移行する場合の速度テスト

例えば、コンソールのオンラインマイグレーション機能により、サーバーをTencent Cloud CentOS 7.5インスタンスに移行する場合、その転送速度のテスト手順は次のようになります：

1. 移行先リージョンに従量課金のCentOS 7.5インスタンスを作成します。

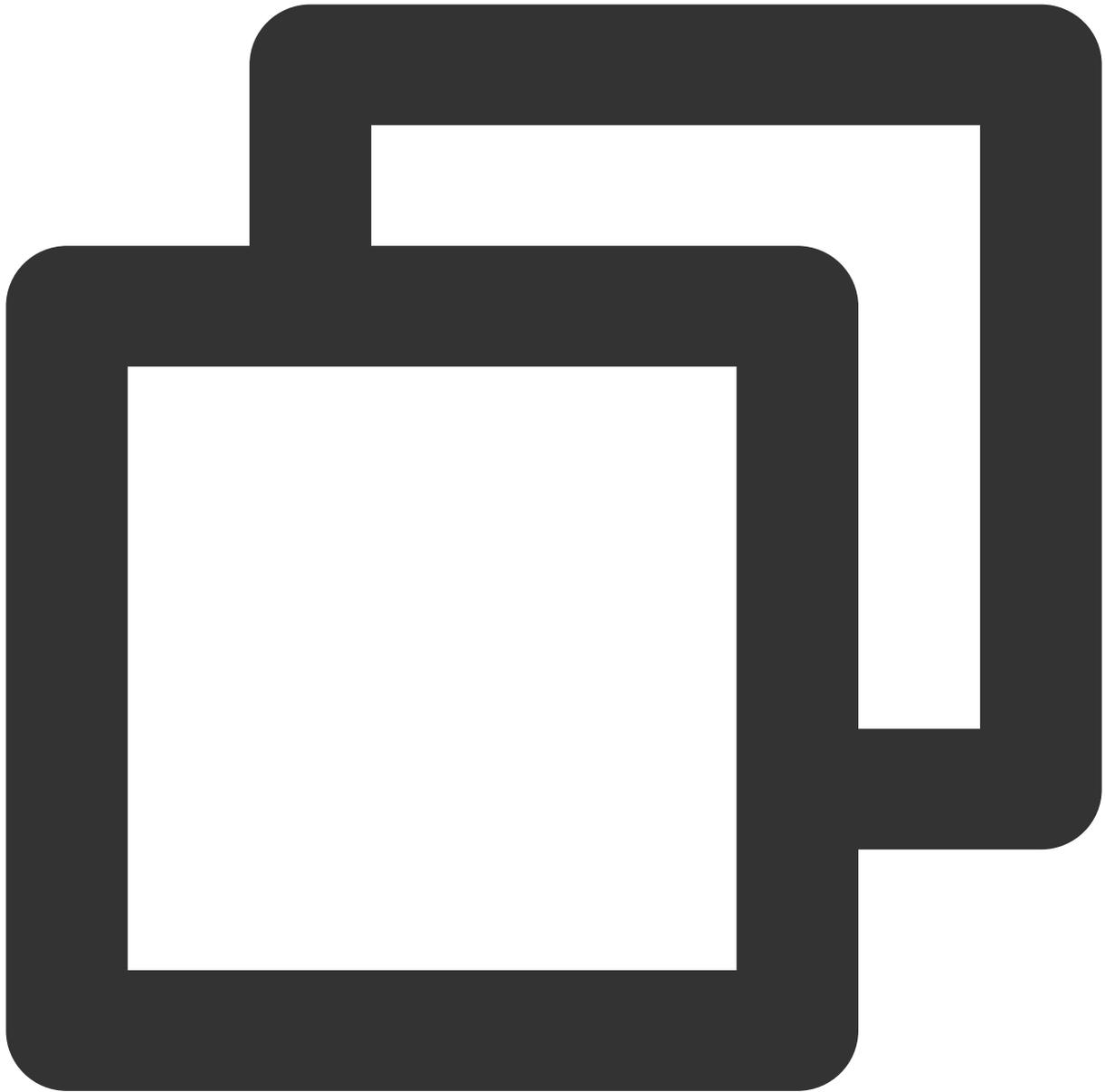
#### 説明：

移行先がCVMイメージであれば、移行中にCentOS 7.5の中継インスタンスが作成されることがあります。速度のテストを行いたい場合は、標準型かつCPU、メモリ構成が比較的低いマシンモデルを選択し、実際の移行時のシナリオにより近づけて行うことをお勧めします。

iperf3サーバーのデフォルトポートはTCP 5201であり、テストするCentOS 7.5インスタンスのセキュリティグループのインバウンド方向にTCP 5201ポートを追加および開放してください。

2. 移行先のテストインスタンスと移行元サーバーにそれぞれiperf3ツールをインストールします。

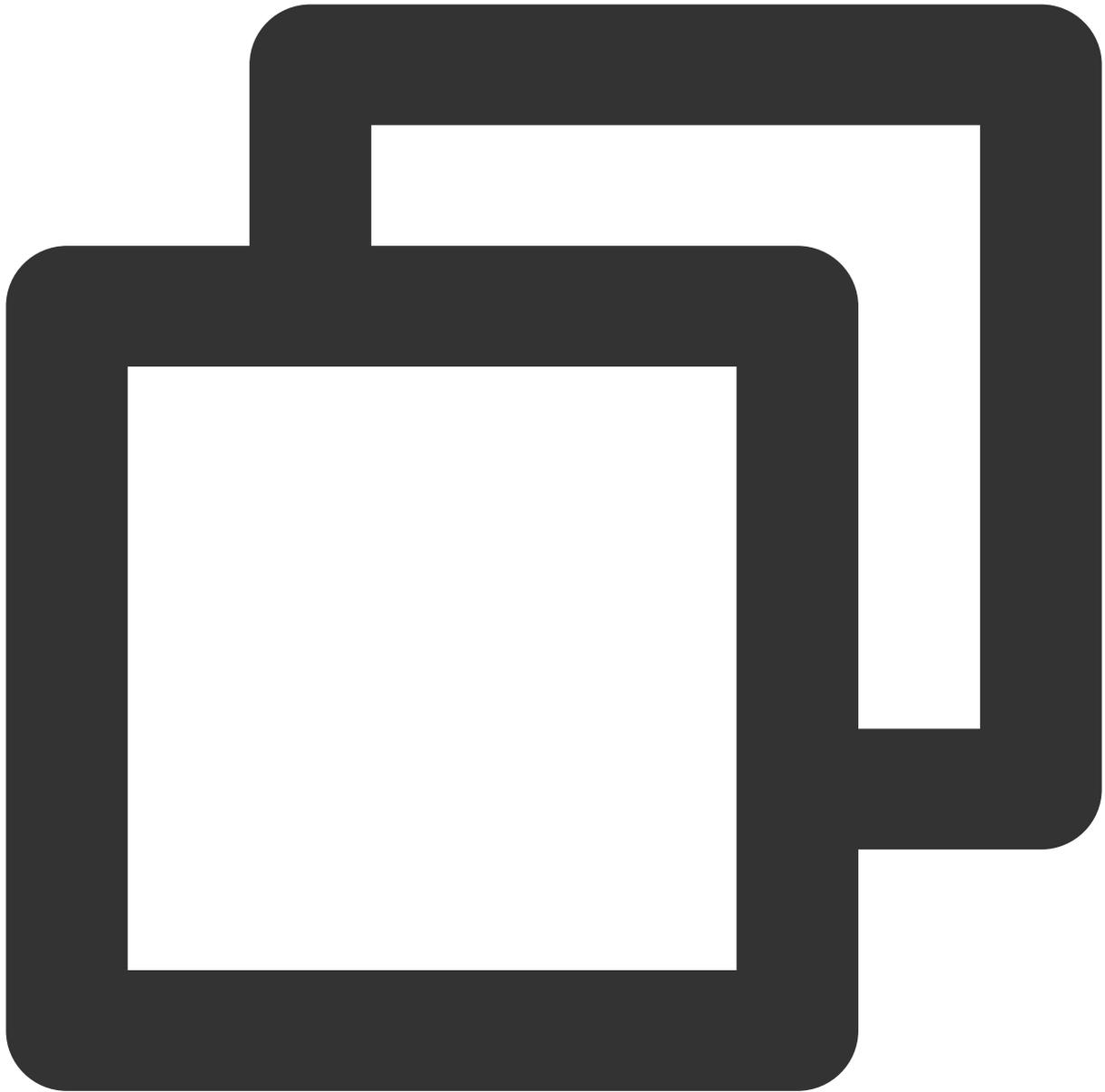
次のコマンドを実行し、移行先のCentOS 7.5インスタンスにiperf3ツールをインストールします。



```
yum -y install iperf3
```

移行元サーバーにiperf3ツールをインストールします。移行元サーバーのLinuxリリースバージョンに応じて、対応するインストールコマンドを使用してiperf3ツールをインストールしてください。

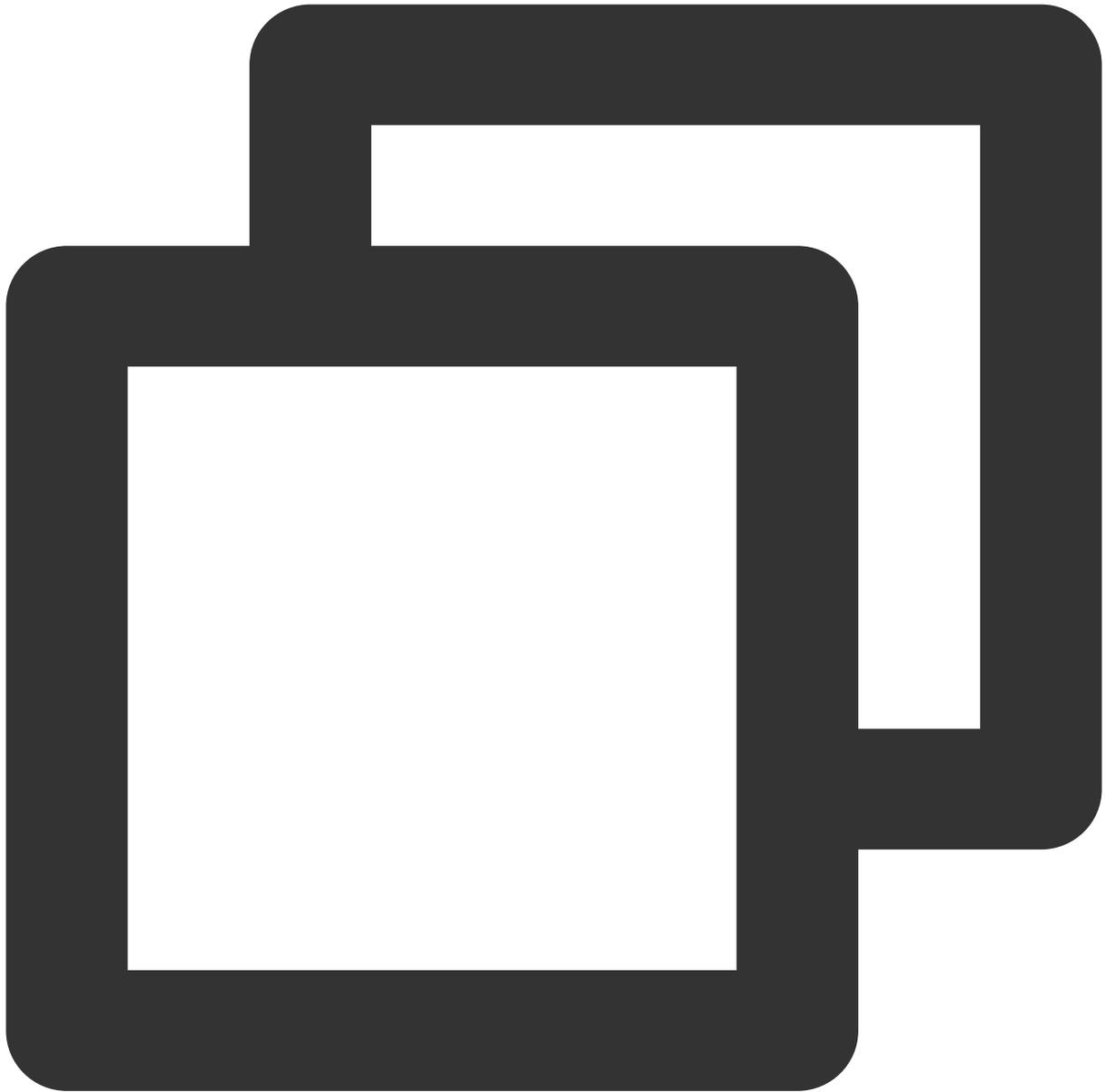
3. 次のコマンドを実行し、移行先のCentOS 7.5テストインスタンスのiperf3をサーバーとして起動します。



```
iperf3 -s
```

「Server listening on 5201」などのメッセージが返されれば、起動は成功です。

4. 次のコマンドを実行し、移行元サーバーでiperf3をクライアントとして起動します。



```
iperf3 -c [移行先インスタンスIP]
```

返されるテスト結果は次のように表示され、移行元サーバーとCentOS 7.5テストインスタンス間の転送速度はおよそ111Mbpsであることがわかります。

```
[root@VM-0-48-centos ~]# iperf3 -c   
Connecting to host   
[ 4] local 10.0.0.48 port 50682 connected to   
[ ID] Interval          Transfer          Bandwidth          R  
[ 4] 0.00-1.00    sec    24.2 MBytes    203 Mbits/sec    6  
[ 4] 1.00-2.00    sec    12.1 MBytes    101 Mbits/sec    4  
[ 4] 2.00-3.00    sec    12.0 MBytes    101 Mbits/sec    5  
[ 4] 3.00-4.00    sec    12.1 MBytes    102 Mbits/sec    4  
[ 4] 4.00-5.00    sec    11.9 MBytes    100 Mbits/sec    4  
[ 4] 5.00-6.00    sec    12.1 MBytes    101 Mbits/sec    4  
[ 4] 6.00-7.00    sec    12.2 MBytes    102 Mbits/sec    4  
[ 4] 7.00-8.00    sec    12.1 MBytes    101 Mbits/sec    5  
[ 4] 8.00-9.00    sec    12.0 MBytes    101 Mbits/sec    5  
[ 4] 9.00-10.00   sec    12.1 MBytes    101 Mbits/sec    4  
- - - - -  
[ ID] Interval          Transfer          Bandwidth          R  
[ 4] 0.00-10.00   sec    133 MBytes    111 Mbits/sec    5  
[ 4] 0.00-10.00   sec    133 MBytes    111 Mbits/sec
```

# 課金説明

最終更新日：2023-04-28 17:34:15

サービスの移行は無料ですが、移行ツールの使用についてはトランジットインスタンス、ネットワークなどの料金がかかる場合があります。このドキュメントでは、サービスの移行を使用するときに発生する料金と課金方法について説明します。

## トランジットインスタンス

移行先がCVMイメージの場合、移行開始後にお客様のアカウントの下に「do\_not\_delete\_csm\_instance」と呼ばれるトランジットが作成され、インスタンス料金とクラウドディスク料金などが発生します。

課金方式：[従量課金](#)

移行が完了するまでトランジットインスタンスの再インストール、シャットダウン、破棄、パスワードのリセットなどは行わないでください。移行が完了すると、今回作成されたトランジットインスタンスが自動的に破棄されます。

## パブリックネットワークトラフィック

オンライン移行には、次のようなトラフィックが発生します。料金は次のとおりです。

パブリックネットワークを使用した移行では、移行元のインスタンスが固定帯域幅の場合、追加料金は発生しません。移行先はインバウンドトラフィックであり、料金は発生しません。

パブリックネットワークを使用した移行では、移行元のインスタンスが使用量に応じて課金されている場合、移行元のインスタンスにネットワーク料金が発生します。移行先はインバウンドトラフィックであり、料金は発生しません。

[VPCピアリング接続](#)、[VPN接続](#)、[CCN](#) または [ダイレクト接続](#) などの方法を介して接続チャネルを確立します。

費用については具体的なネットワーク料金をご参照ください。

# オフライン移行

最終更新日：2023-06-25 17:55:06

このドキュメントでは、インスタンスとデータをオフラインで移行する方法について説明します。

## 概要

サービス移行は、企業のクラウド移行を加速することに役立つ、Tencent Cloud によって開発された移行プラットフォームです。この移行プラットフォームを使用すると、OS、アプリケーション、およびアプリケーションデータをソースサーバーからCloud Virtual Machine (CVM) インスタンスまたはCloud Block Storage (CBS) インスタンスに移行できます。これは、クラウド化、クロスクラウド移行、クロスアカウントまたはクロスリージョン移行、およびハイブリッドクラウド展開に対する企業のニーズを満たすのに役立ちます。

サービス移行には、オフラインとオンラインの両方の移行がサポートされます。オフライン移行は、次の2つのタイプに分かれます。

**CVMへの移行**：システムディスクイメージ（または必要に応じてシステムディスクイメージとデータディスクイメージの両方）を特定のCVMインスタンスに移行できます。

**CBSへの移行**：データディスクイメージを指定のクラウドディスクに移行できます。

## 前提条件

オフライン移行には、Cloud Object Storage (COS) のサポートが必要です。所在リージョンでCOSが利用可能であることを確認してください。

現在COSでサポートされているリージョンについては、[リージョンとアクセスドメイン名](#)をご参照ください。

## 準備作業

### ご注意：

現在、Tencent Cloudのサービス移行でサポートされているイメージ形式は、qcow2、vhd、vmdk、およびrawです。伝送と移行の時間を短縮するために、圧縮イメージ形式を使用することをお勧めします。

アップロードするイメージは、宛先CVMインスタンスと同じリージョンのCOSバケットに保存する必要があります。さらに、COSバケットはパブリック読み取りアクセスを許可する必要があります。

システムディスクイメージとデータディスクイメージの両方をインポートする必要がある場合は、対応する数のデータディスクをターゲットインスタンスにマウントする必要があります。

ターゲットディスクの容量はソースディスクの容量以上である必要があります。

オフライン移行では、スナップショットファイル (-00000.vmdkなどのファイル名を持つスナップショットファイル) の移行はサポートされていません。

イメージ制作ドキュメントに従って、ソースサーバーのイメージを作成します。

Windows の場合は、[Windowsイメージの作成](#) をご参照ください。

Linux の場合は、[Linuxイメージの作成](#) をご参照ください。

作成したイメージファイルをCOSにアップロードします。

イメージサイズが大きいため、ブラウザからアップロードすると失敗する場合があります。イメージをアップロードするには COSCMD ツールを使用することをお勧めします。操作の詳細については、[COSCMD ツール](#) をご参照ください。

他のクラウドプラットフォームからエクスポートされたイメージが圧縮パッケージ (.tar.gz ファイルなど) である場合、それらをCOSに直接アップロードできます。

アップロードしたイメージのCOSアドレスを取得します。

[COSコンソール](#) に移動し、アップロードしたイメージファイルを見つけて、イメージファイルの詳細ページで一時リンクをコピーします。

移行するCVMまたはCBSインスタンスを用意します。

[CVMの購入に進む](#)

[CBS購入ガイドライン](#)

## 操作手順

CVMへの移行

CBSへの移行

1. CVMコンソールにログインし、左側ナビゲーションの [サービス移行](#) をクリックします。
2. 「オフライン移行」 ページで「CVMに移行」 をクリックします。
3. 「CVMに移行」 画面が表示されます。この画面で準備を完了し、「次へ」 をクリックします。
4. リージョンを選択し、タスク名、COS リンク、移行先のCVMインスタンスなどの情報を入力します。下図に示すとおりです。

### Migrate to CVM

✓ Preparation > 2 Configuration

**Note:** when you migrate your server to a CVM instance, all data in the system disk of the CVM are overwritten. You need to shut down the CVM before migration.

- Before you start, create a snapshot to back up your data to avoid data loss. [Learn more](#)
- Data disks of the destination CVM are not cleared. But you need to attach the disks manually after the migration. [Learn more](#)

Region:

**Note:** the region must be the same as the COS bucket region selected when you uploaded the image

Task name:

COS link:

Enter the link of the image file in COS

Please select instances to migrate

ID/Name	Operating system	IP address	Configuration
<input type="checkbox"/>	TencentOS Server 2.2 (Final)		1-core 1 GB 1Mbps System disk: Premium Cloud Storage Network: test

Total items: 1      20 / page      1 / 1 page

Add data disk image

5. **完了**をクリックすると、移行タスクを正常に作成します。

移行中に**サービス移行** ページを終了または閉じることができます。また、いつでもこのページに戻って移行の進捗状況を確認することができます。

- CVMコンソールにログインし、左側ナビゲーションの **サービス移行** をクリックします。
- 「オフライン移行」 ページで「CBSに移行」 をクリックします。
- 「CBSに移行」 画面が表示されます。この画面で準備を完了し、「次へ」 をクリックします。
- リージョンを選択し、タスク名、COS リンク、移行先のCBSインスタンスなどの情報を入力します。下図に示すとおりです。

### Migrate to CBS

Preparation > **2 Configuration**

**Note:** when you migrate a disk to a Tencent Cloud cloud disk, all data in the destination cloud disk are cleared and cannot be recovered. Before you start, please create a snapshot to back up your data to avoid data loss. For details, please see [Operation Guide](#)

Region:

**Note:** the region must be the same as the COS bucket region selected when you uploaded the image

Task name:

COS link:

Enter the link of the image file in COS

Please select the destination cloud disk

ID/Name	Status	Capacity	Type
No data yet			

Total items: 0      20 / page      1 / 1 page

5. 完了をクリックすると、移行タスクを正常に作成します。

移行中に [サービス移行](#) ページを終了または閉じることができます。また、いつでもこのページに戻って移行の進捗状況を確認することができます。

## よくあるご質問

詳細については、[サービス移行](#)をご参照ください。

# お問い合わせ

最終更新日：：2023-05-12 17:11:45

弊社WEBサイトをご覧いただき、誠にありがとうございます。

サービスの移行中に問題が発生した場合、または改善提案やご意見などがある場合は、いつでもお気軽に弊社までご連絡くださいませ！

## チケットシステム

弊社の製品をご使用中にトラブルが発生した場合は、Tencent Cloudコンソールにログインし、画面の指示に従ってチケットを送信できます。お問い合わせ内容の確認後、担当者より、できるだけ早くご連絡させていただきます。

チケットリンク:

サポートチケットの送信：[チケットの送信](#)

チケットステータスの照会：[チケットリスト](#)

# メンテナンスタスク

## メンテナンスタスクの概要

最終更新日：：2023-01-31 16:19:42

メンテナンスタスク機能は、標準化されたCVMトラブルシューティング、認定されたメンテナンスサービスをユーザーに提供することを目的とします。

インスタンスの実行パフォーマンスと安定性を向上させ、基盤となるプラットフォームの安全で効率的な運用を確保するために、プラットフォームは基盤となるホストおよびプラットフォームアーキテクチャをオンラインで定期的にメンテナンスおよびアップグレードします。この期間中、CVMは通常どおり安定して動作し、業務プログラムを中断することなく、プラットフォームのアップグレードによるパフォーマンスの向上させることができます。

メンテナンスタスクは、ユーザーがCVMインスタンスのさまざまな緊急事態をリアルタイムに制御および処理し、潜在的なサーバーダウンのリスクを事前に回避し、メンテナンス効率を向上させるとともに、ユーザーのメンテナンスコストを削減することができます。ユーザーは、独自の業務特性および運用・メンテナンスのシナリオに合わせて、異常インスタンスの重要データをタイムリーにバックアップし、安定した業務運用を保証できます。また、メンテナンスタスクは、ユーザーが実際のニーズに応じて事前設定された承認ポリシーを策定したり、クラウドAPIを介して接続して、CVMの障害や隠れた危険シナリオに対応する柔軟で制御可能な自動運用・メンテナンス機能を構築することをサポートします。

## 機能のメリット

### 無償有効化

メンテナンスタスク機能は、デフォルトで完全にオープンになり、追加購入なしで無料で使用できます。CVMインスタンスを作成して使用した後、[メンテナンスタスクコンソール](#)にログインし、現在のユーザーが属するCVMインスタンスの完全なメンテナンスタスクレコードを表示できます。

### 異常、隠れた危険シナリオの全面的なカバー

CVMインスタンスのさまざまな予期せぬ異常（たとえば、基盤となるホストの突然の異常サーバーダウンによるCVMの異常な再起動）、運用上の隠れた危険（基盤となるホストのさまざまなソフトウェア・ハードウェア障害の隠れた危険に対する事前予測）、ハードディスクの異常/警告（ローカルディスクインスタンスのハードディスク使用の異常/早期警告）、およびプラットフォーム計画内のメンテナンスとアップグレードのタスクをカバーします。

### 柔軟な設定

独自の業務シナリオと運用・メンテナンス要件に基づいて、複数の事前設定された承認ポリシーの設定をサポートします。各ポリシーは、さまざまなコンピューティング製品インスタンスファミリーに関連付けることができ、

CVMタグによる高速バインディングをサポートします。

## 柔軟な接続

メンテナンスタスクは、ユーザーに柔軟で便利な使用方法を提供します。メンテナンスタスクコンソールを提供するだけでなく、ユーザーが事前設定された承認ポリシー、クラウドAPIを介して、自動メンテナンスおよび承認された接続を行うこともサポートします。

## ユースケース

### インスタンス異常のリアルタイム検出、高速リカバー

CVMインスタンスのさまざまな異常情報は、お客様に通知をタイムリーにプッシュし、対応するメンテナンスタスクを作成します。ユーザーは、メンテナンスタスクコンソールにログインし、影響を受けたインスタンスのリカバー状況に注意を払い、タイムリーにリスクを回避して、安定した業務運用を保証できます。

### インスタンスの隠れた危険のリアルタイム監視、事前回避

現在正常に稼働しているが、プラットフォームによって基盤となるホストにソフトウェア・ハードウェアの隠れた危険性が監視されたり、プラットフォーム計画内に実行待ちのメンテナンスタスクが存在したりするCVMインスタンスの場合、ユーザーは関連情報をリアルタイムに検出し、メンテナンス計画を策定し、ピークの少ない業務時間帯にタイムリーに承認して、隠れた危険を事前に回避し、潜在的なサーバーダウンのリスクを排除できます。

### CVM異常シナリオでの自動運用・メンテナンス

ユーザーは、事前設定された承認ポリシー、クラウドAPIを介してすばやく接続できます。CVMが新しいメンテナンスタスクおよびアラームイベントをトリガーすると、自動運用・メンテナンス機能を使用して、障害の自己修復を実現し、運用・メンテナンスの効率を向上できます。

## 使用制限

メンテナンスタスク機能は現在、CVM、CVM Dedicated Host (CDH)およびベアメタルCVMに適用され、その他の製品はまだサポートされていません。

# メンテナンスタスクタイプと対処ポリシー

最終更新日：2023-01-31 16:19:42

プラットフォームによってインスタンスの可用性と運用パフォーマンスに影響を与える異常状態（たとえば、基盤となるホストの突然の異常サーバーダウン、または基盤となるホストの潜在的なソフトウェアとハードウェアの障害を事前に予測してサーバーダウンのリスクを事前に回避するなど）が監視されると、プラットフォームは、ただちにメンテナンスプロセスを開始し、対応するメンテナンスタスクを記録し、影響を受けるインスタンスの障害または隠れた危険の通知をユーザーにプッシュします。関連する通知を受け取った後、[メンテナンスタスクコンソール](#)にタイムリーに移動し、異常インスタンスの修復時間と処理の進行状況を確認し、プラットフォームが異常インスタンスを修復して通常の運用状態をリカバーすることを承認できます。

**CVM**インスタンスのメンテナンスタスクは、トリガーの理由に従って分類され、次の複数のタイプに分けることができます。各タスクタイプの具体的な意味、対策、およびオプションの承認ポリシーを次の表に示します：

## メンテナンスタスクの分類

タスクタイプ	タスクの意味	対策	オプションの承認ポリシー
インスタンスの動作異常	インスタンスの基盤となるホストの突然のソフトウェア・ハードウェア障害またはシステムエラーにより、インスタンスの異常サーバーダウンまたは再起動が発生します。	異常な動作タイプのインスタンスのメンテナンスタスクがトリガーされることを監視すると、プラットフォームは直ちに関連するメンテナンス操作を実行し、異常なインスタンスを再起動して、インスタンスの可用性をすばやくリカバーします。インスタンスの自動再起動が完了するまで待機し、メンテナンスタスクステータス更新の進行状況に注意することをお勧めします。	メンテナンスタスクの現在の状態に応じて、次の対処ポリシーを決定します： タスクが「処理中」の状態である場合、プラットフォームは、異常インスタンスに対して関連するメンテナンス操作を緊急に実行しています。メンテナンスが完了すると、タスクステータスがタイムリーに同期更新され、関連する通知がプッシュされます。 タスクが「終了」の状態である場合、異常インスタンスの自動再起動が完了して動作を再開し、インスタンスとアプリケーションが正常に戻るかどうかを確認できます。
インスタ	インスタンスは現在正常に実行されています	できるだけ早くメンテナンスを完了して、基盤となるソフトウェ	インスタンスの基盤となる隠れた危険の修復方法に応じて、次

<p>インスタンス動作の隠れた危険</p>	<p>が、インスタンスホストまたは基盤となるプラットフォームにソフトウェア・ハードウェアの隠れた危険があることが監視されると、インスタンスパフォーマンスジッター、異常サーバーダウンのリスクを引き起こす可能性があります。</p>	<p>ア・ハードウェアの隠れた危険を回避し、潜在的なサーバーダウンのリスクを回避するために、事前に業務データをバックアップし、できるだけ早くメンテナンスタスクコンソールに移動することをお勧めします：</p> <ol style="list-style-type: none"> <li>1. (オプション) インスタンスデータのバックアップを実行します。</li> <li>2. プラットフォームがただちにメンテナンスを開始したり、48時間以内に予定されたメンテナンス時間を予約したりすることが承認されます。</li> <li>3. 予定されたメンテナンス時間に、システムが自動的にメンテナンスを開始するまで待ちます。</li> </ol>	<p>の方法を選択して処理を承認できます：</p> <p>オンライン移行承認（インスタンスをシャットダウンする必要はなく、移行プロセス中にCVMに短期間の高負荷またはネットワークジッターが発生する可能性があります。</p> <p>シャットダウンメンテナンスの承認（インスタンスを再起動し、すばやくリカバーします）。</p> <p><b>注意：</b></p> <ol style="list-style-type: none"> <li>1. たとえば、ユーザーが48時間以上承認していない場合、システムはデフォルトで、予定されたメンテナンス時間にメンテナンスを開始します。</li> <li>2. ローカルディスクインスタンスは現在、再起動後のすばやくリカバーをサポートしておらず、基盤となるハードウェアの隠れた危険をリカバーするためにより長いメンテナンス期間が必要です。必要に応じて、ユーザーは、ローカルディスクインスタンスの再デプロイを選択して、隠れた危険をすばやく回避できます（ローカルディスクデータは保持できません）。</li> </ol>
<p>インスタンスのハードディスクの異常</p>	<p>インスタンスのローカルハードディスクに突如の障害が発生すると、インスタンスのI/Oパフォーマンスが低下したり、ハードディスク機能が損傷したりする可能性があります。</p>	<p>できるだけ早くメンテナンスを完了して、異常ハードディスクの可用性をリカバーするために、事前に業務データをバックアップし、できるだけ早くメンテナンスタスクコンソールに移動することをお勧めします。</p> <ol style="list-style-type: none"> <li>1. (オプション) インスタンスデータのバックアップを実行します。</li> <li>2. プラットフォームがただちに異常ハードディスクを交換したり、48時間以内に予定されたメンテナンス時間を予約したりすることが承認されます。</li> </ol>	<p>ローカルディスクインスタンスの異常ハードディスクの修復方法に応じて、次の方法を選択して処理を承認できます。</p> <p>オンラインでのディスク交換（インスタンスは、異常ハードディスクをオンラインで交換します。メンテナンスプロセス中、異常ハードディスクのI/Oは短時間、一時的に使用できなくなります。処理完了後、プロンプトに従って新しいディスクをマウントして使用することができます）。</p>

		<p>3. プラットフォームが異常ハードディスクの交換を完了するのを待ち、リカバー通知の操作プロンプトに従って、交換後のローカルハードディスクを再マウントして使用します。</p>	<p>シャットダウンによるディスク交換（インスタンスは、異常ハードディスクを交換するためにシャットダウンする必要があります。ローカルディスクのデータを保持する可能性があります。ローカルディスクのデータを保持する可能性がありますが、より長いメンテナンスサイクルが必要です）。</p> <p>（オプション）ディスク破棄による移行：ローカルディスクのインスタンスを再デプロイし、ローカルディスクのデータを保持できません。分レベルでインスタンスの可用性をすばやくリカバーします。</p>
<p>インスタンスハードディスクの警告</p>	<p>インスタンスのローカルハードディスクが破損したり、寿命が近づいたりする可能性があります。そのため、インスタンス I/O 異常またはディスクオフラインなどのデータレベルの異常が発生する可能性があります。</p>	<p>できるだけ早くメンテナンスを完了して、ローカルハードディスクの潜在的な障害のリスクを排除するために、事前に業務データをバックアップし、できるだけ早くメンテナンスタスクコンソールに移動することをお勧めします。</p> <ol style="list-style-type: none"> <li>（オプション）インスタンスデータのバックアップを実行します。</li> <li>プラットフォームがただちに隠れた危険のあるハードディスクを交換したり、48時間以内に予定されたメンテナンス時間を予約したりすることが承認されます。</li> <li>プラットフォームが異常ハードディスクの交換を完了するのを待ち、リカバー通知の操作プロンプトに従って、交換後のローカルハードディスクを再マウントして使用します。</li> </ol>	<p>ローカルディスクインスタンスの異常ハードディスクの修復方法に応じて、次の方法を選択して処理を承認できます。</p> <p>オンラインでのディスク交換（インスタンスは、異常ハードディスクをオンラインで交換します。メンテナンスプロセス中、異常ハードディスクの I/O は短時間、一時的に使用できなくなります。処理完了後、プロンプトに従って新しいディスクをマウントして使用することができます）。</p> <p>シャットダウンによるディスク交換（インスタンスは、異常ハードディスクを交換するためにシャットダウンする必要があります。ローカルディスクのデータを保持する可能性がありますが、より長いメンテナンスサイクルが必要です）。</p> <p>（オプション）ディスク破棄による移行：ローカルディスクのインスタンスを再デプロイし、ローカルディスクのデータを保持できません。分レベルでインスタンスの可用性をすばやくリカバーします。</p>

<p>インスタンスのネットワーク接続異常</p>	<p>インスタンスの基盤となるネットワーク接続の突然の障害により、インスタンスのネットワークジッタが発生したり、異常ネットワーク接続が発生したりする可能性があります。</p>	<p>異常なネットワーク接続タイプのインスタンスのメンテナンスタスクがトリガーされることを監視すると、プラットフォームはただちに基盤となるネットワークに対して関連するメンテナンス操作を実行し、異常インスタンスのネットワーク接続の可用性をリカバーします。</p> <p>インスタンスのネットワーク接続の自動修復が完了するまで待機し、メンテナンスタスクステータス更新の進行状況に注意することをお勧めします。</p>	<p>メンテナンスタスクの現在の状態に応じて、次の対処ポリシーを決定します：</p> <p>タスクが「処理中」の状態である場合、プラットフォームは、異常インスタンスの基盤となるネットワークに対して関連するメンテナンス操作を緊急に実行しています。メンテナンスが完了すると、タスクステータスがタイムリーに同期更新され、関連する通知がプッシュされます。タスクが「終了」の状態である場合、異常インスタンスのネットワーク接続が正常に戻り、インスタンスとアプリケーションが正常に戻るかどうかを確認できます。</p>
<p>インスタンスメンテナンスのアップグレード</p>	<p>インスタンスのパフォーマンスおよびセキュリティを向上させるために、インスタンスは、基盤となるホストアーキテクチャ、ソフトウェアのアップグレードなどの理由により、オンラインメンテナンスを開始する必要があります。</p>	<p>できるだけ早くメンテナンスを完了して、インスタンスのパフォーマンスおよびセキュリティを向上させるために、事前に業務データをバックアップし、できるだけ早くメンテナンスタスクコンソールに移動することをお勧めします。</p> <ol style="list-style-type: none"> <li>1. (オプション) インスタンスデータのバックアップを実行します。</li> <li>2. プラットフォームがただちにメンテナンスを開始したり、48時間以内に予定されたメンテナンス時間を予約したりすることが承認されます。</li> <li>3. 予定されたメンテナンス時間に、システムが自動的にメンテナンスを開始するまで待ちます。</li> </ol>	<p>次の承認方法を選択できます：</p> <p>オンラインメンテナンス（インスタンスをシャットダウンする必要はなく、メンテナンスプロセス中にCVMに短期間の高負荷またはネットワークジッターが発生する可能性があります。</p> <p><b>注意：</b> ユーザーが48時間以上承認していない場合、システムはデフォルトで、予定されたメンテナンス時間にメンテナンスを開始します。</p>

## タスクのステータス

タスクのステータス	意味

承認待ち	ユーザーの承認を待って、ユーザーは承認されたメンテナンス方法とメンテナンス時間を選択できます。ハードディスク以外のメンテナンスタスクに対して、ユーザーが48時間以上承認していない場合、システムはデフォルトで、予定されたメンテナンス時間にメンテナンスを開始し、メンテナンスタスクを処理中ステータスに変更します。
予約済み	ユーザーは操作を承認し、メンテナンス時間を予約しました。タスク作成から48時間以内に、システムのデフォルトの予定されたメンテナンス時間を変更できます。
処理中	メンテナンスタスクを実行しています。
終了	メンテナンスタスクが処理されました。
回避済み	インスタンスに未完了のメンテナンスタスクがある場合、ユーザーがインスタンスの返却、破棄、構成の調整などを実行するとき、メンテナンスタスクプロセスを回避するために中断されます。
キャンセル済み	今回のメンテナンスタスクがシステムによってキャンセルされました。

# メンテナンスタスクの確認

最終更新日：：2023-05-12 17:44:55

## 概要

このドキュメントでは、CVMコンソールで保留中および履歴のメンテナンスタスクのリストと詳細なトラブルシューティング情報を表示する方法について説明します。

## 操作手順

1. CVMコンソールにログインし、左側ナビゲーションバーのメンテナンスタスク > [タスクリスト](#) を選択します。
2. 「メンテナンスタスク」リストページで、リスト上方のフィルタリング条件を選択し、必要なメンテナンスタスクリストを取得します。
3. メンテナンスタスクIDをクリックすれば、メンテナンスタスク詳細ページに移動し、その他情報を確認できます。

# メンテナンスポリシーの承認とメンテナンスの時間枠の指定

最終更新日： : 2023-05-12 17:48:34

## 概要

ここではTencent Cloudコンソールからメンテナンスタスクに応じた具体的なメンテナンスポリシーを選択し、メンテナンス実行日時を予約する方法について説明します。

## 操作手順

1. CVMコンソールにログインし、左側ナビゲーションバーの**Maintenance task** > **Task List** をクリックします。
2. メンテナンスタスクの行の右側にある**Authorize/Schedule**をクリックします。
3. ポップアップしたウィンドウで、タスクのメンテナンスポリシーおよびメンテナンス時間を選択します。

### 説明：

タスクタイプに応じて承認するメンテナンス方式を決定します。詳細については、[メンテナンスタスクタイプと対処ポリシー](#)をご参照ください。

「メンテナンス時間の予約」を設定しない場合は、デフォルトで直ちにメンテナンスが開始されます。

4. **OK**をクリックし、メンテナンスポリシーの承認を完了します。

# プリセット承認ポリシーの設定

最終更新日：2023-05-12 17:53:55

## 概要

特定のタグの下のすべてのCVMインスタンスに対して、プリセットメンテナンス承認ポリシーを設定できます。メンテナンスタスクが生成されると、手動で承認する必要なく、設定済みのプリセットポリシーに従って処理されます。このドキュメントでは、CVM コンソールでプリセットメンテナンス承認ポリシーを設定する方法について説明します。

## 操作手順

1. CVMコンソールにログインし、左側ナビゲーションバーから **Maintenance Task > Preset authorization policy** をクリックします。
2. 「Preset authorization policy」 ページで、**Create** をクリックします。「Create Preset Authorization Policy」 画面が表示されます。
3. 「Create Preset Authorization Policy」 画面で、プリセット承認を実行する必要がある製品タイプ、指標、対応するプリセット承認ポリシーを選択し、対応するタグを付けます。
4. **OK** をクリックすれば、プリセットメンテナンス承認ポリシーが作成できます。タグに関連付けられたインスタンスは、メンテナンスタスク生成後に、デフォルトでプリセットポリシーを使用してメンテナンス処理を実行します。

# メンテナンスタスクアラート通知の設定

最終更新日：2023-06-25 17:56:20

## 概要

CVM インスタンスのメンテナンスタスクにアラームを設定できます。障害発生時に、電子メール、ショートメッセージ、電話などのチャンネルを介して即座に措置を講じるよう通知します。このドキュメントでは、[EventBridge](#) を使用して、[EventBridge](#) コンソールで CVM インスタンスのアラーム通知を設定する方法について説明します。

## 操作手順

1. [EventBridge](#) コンソール にログインし、[EventBridge](#) の [アクティブ化](#) の指示に従ってサービスをアクティブ化します。
2. 左側のサイドバーで [Event Rule](#) を選択し、「Event Rule」 ページの上部でターゲットリージョンとイベントバスを選択して、**Create Event Rule** をクリックします。
3. 「Create Event Rule」 ページで、次の操作を実行します。
  - 3.1 下図に示すように、「Basic Information」 で、**ルール名**を入力します。

← **Create event rule**

**1 Rule pattern** > **2 Delivery target**

**Basic information**

Region: Guangzhou

Event Bus: [dropdown]

Rule name \*: [input field]

Rule description: [input field]

Tag:  Enable

Data conversion:  [info icon]

3.2 下図に示すように、「Event Pattern」で、次の情報を参照して「イベントマッチング」パラメータを設定し、その他のパラメータを必要に応じて設定します。

**Event matching** Edit event matching rule in JSON and test the rule by using the event sample. [Examples](#)

Mode: **Template** Custom events

Tencent Cloud service: Cloud Virtual Machine

Event Type: Please select

- All events
- Disk read-only
- Kernel failure
- OOM
- ping unreachable
- Server restarted
- Packet loss caused by over-li

Rule preview

Filters events published to EventBridge according to the specified rule

```
1 {
2   "source": "cvm.cloud.tencent",
3   "type": [
4     "cvm:ErrorEvent:DiskReadOnly"
5   ]
6 }
7
```

Correct JSON

Test match rule Edit match rule

**Tencent Cloud service**：ドロップダウンリストから**CVM**を選択します。

**Event Type**：必要に応じて、ドロップダウンリストからオプションを選択します。

3.3 **Next**をクリックします。

3.4 「Delivery target」で、必要に応じて「Trigger method」ドロップダウン リストからオプションを選択します。

「トリガーモード」は**Cloud Log Service (CLS)**を選択する場合、[CLSログターゲット](#)を参照して設定を行うことができます。

「トリガーモード」は**Notification message**を選択する場合、[メッセージプッシュターゲット](#)を参照して設定を行うことができます。

4. **Complete**をクリックし、設定を完了します。

# Cloud Block Storage

## CBSスケールアウト

最終更新日： : 2023-06-30 15:28:14

### 概要

クラウドディスクはクラウド上の拡張可能なストレージデバイスです。ユーザーは、クラウドディスクの作成後、いつでも容量を拡張して、データを失うことなくストレージ容量を増やすことができます。

クラウドディスクを拡張した後、パーティションとファイルシステムを拡張する必要があります。拡張した容量を既存のパーティションに分割したり、別々の新しいパーティションにフォーマットしたりすることができます。

#### ご注意：

MBRパーティションは、最大2TBの容量のディスクをサポートします。2TBを超える容量のディスクをパーティション分割する場合は、新しいデータディスクを作成してマウントし、GPTパーティション形式を使用してデータを新しいディスクにコピーすることをお勧めします。

### データディスクの拡張

クラウドディスクがデータディスクの場合、次の3つの方法で拡張することができます。

#### ご注意：

CVMに同じ容量・種類の複数のクラウドディスクが接続されている場合、[データディスクの区分](#)に示す方法で区分できます。拡張するデータディスクを選択後、次の手順に従ってその容量を拡張します。

CVMコンソールを介した拡張（推奨）

CBSコンソールを介した拡張

APIを介した拡張

1. [CVMコンソール](#)にログインします。
2. ターゲットCVMの右側にある[さらに>リソース調整>CBSを拡張](#)をクリックします。
3. 「CBSを拡張」画面が表示されます。この画面で拡張するデータディスクを選択し、[次へ](#)をクリックします。
4. 目標容量（現在の容量以上である必要があります）を設定し、[次へ](#)をクリックします。
5. 注意事項を読み、[変更を開始](#)をクリックします。下図に示すように：

**Expand Cloud Disks**

1 Select the Target Cloud Disk > 2 Adjust Capacity > 3 Extend Partition and File System

**i** After expansion, log in to the instance and check whether the file system has been automatically expanded. If not, you need to manually extend the file system and partition as instructed in [Expanding Cloud Disks](#).

Back Adjust Now

6. ターゲットCVMのOSに応じて、[パーティションとファイルシステム \(Windows\) を拡張する](#)、または [パーティションとファイルシステム \(Linux\) を拡張する](#) 必要があり、拡張された容量を既存のパーティションに割り当てるか、独立した新しいパーティションにフォーマットします。

1. [CBSコンソール](#) にログインします。

2. ターゲットCBSの右側にある [さらに>スケールアウト](#) をクリックします。

3. 必要な新しい容量を選択します（現在の容量以上である必要があります。）。

4. お支払いをしてください。

5. ターゲットCVMのOSに応じて、[パーティションとファイルシステム \(Windows\) を拡張する](#)、または [パーティションとファイルシステム \(Linux\) を拡張する](#) 必要があり、拡張された容量を既存のパーティションに割り当てるか、独立した新しいパーティションにフォーマットします。

「ResizeDisk」API を使用して、指定したクラウドディスクを拡張できます。詳細については、[ResizeDisk](#) をご参照ください。

## システムディスクの拡張

1. [CVMコンソール](#) にログインし、ターゲットCVMの右側にある [さらに>リソース調整>CBSを拡張](#) をクリックします。

2. 「CBSを拡張」画面が表示されます。この画面で拡張するデータディスクを選択し、[次へ](#) をクリックします。

3. 目標容量（現在の容量以上である必要があります）を設定し、[次へ](#) をクリックします。

4. 次の拡張方法で拡張操作を完了します。

CVMコンソールを介した拡張

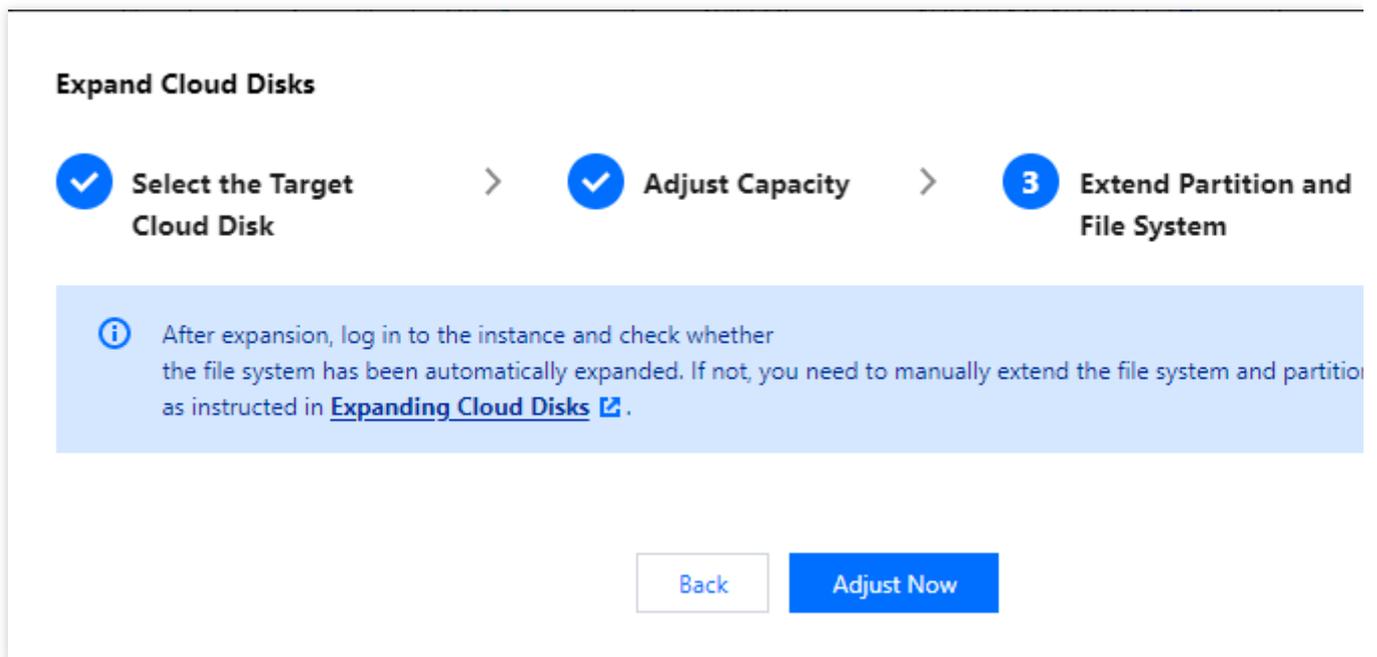
CBSコンソールを介した拡張

## APIを介した拡張

### 説明：

CVMは、インスタンスをシャットダウンせずにクラウドシステムディスクの拡張をサポートします。

1. **パーティションとファイルシステムの拡張**タブで注意事項を読み、**変更を開始**をクリックします。下図に示すように：



2. コンソールで容量拡張を完了し、インスタンスにログインしてファイルシステムが自動的に拡張されたかどうかを確認してください。そうでない場合は、[オンラインでのシステムディスクとファイルシステムの拡張](#)の説明に従ってパーティションとファイルシステムを拡張します。

1. [CBSコンソール](#) にログインします。
2. ターゲットCBSの右側にある **さらに>スケールアウト** をクリックします。
3. 必要な新しい容量を選択します（現在の容量以上である必要があります。）。
4. お支払いをしてください。
5. ターゲットCVMのOSに応じて、[パーティションとファイルシステム（Windows）を拡張する](#)、または [パーティションとファイルシステム（Linux）を拡張する](#) が必要あり、拡張された容量を既存のパーティションに割り当てるか、独立した新しいパーティションにフォーマットします。

`ResizeInstanceDisks` インターフェースを使用して、指定した非エラスティックディスクを拡張できます。詳細については [ResizeInstanceDisks](#) をご参照ください。

## 関連する操作

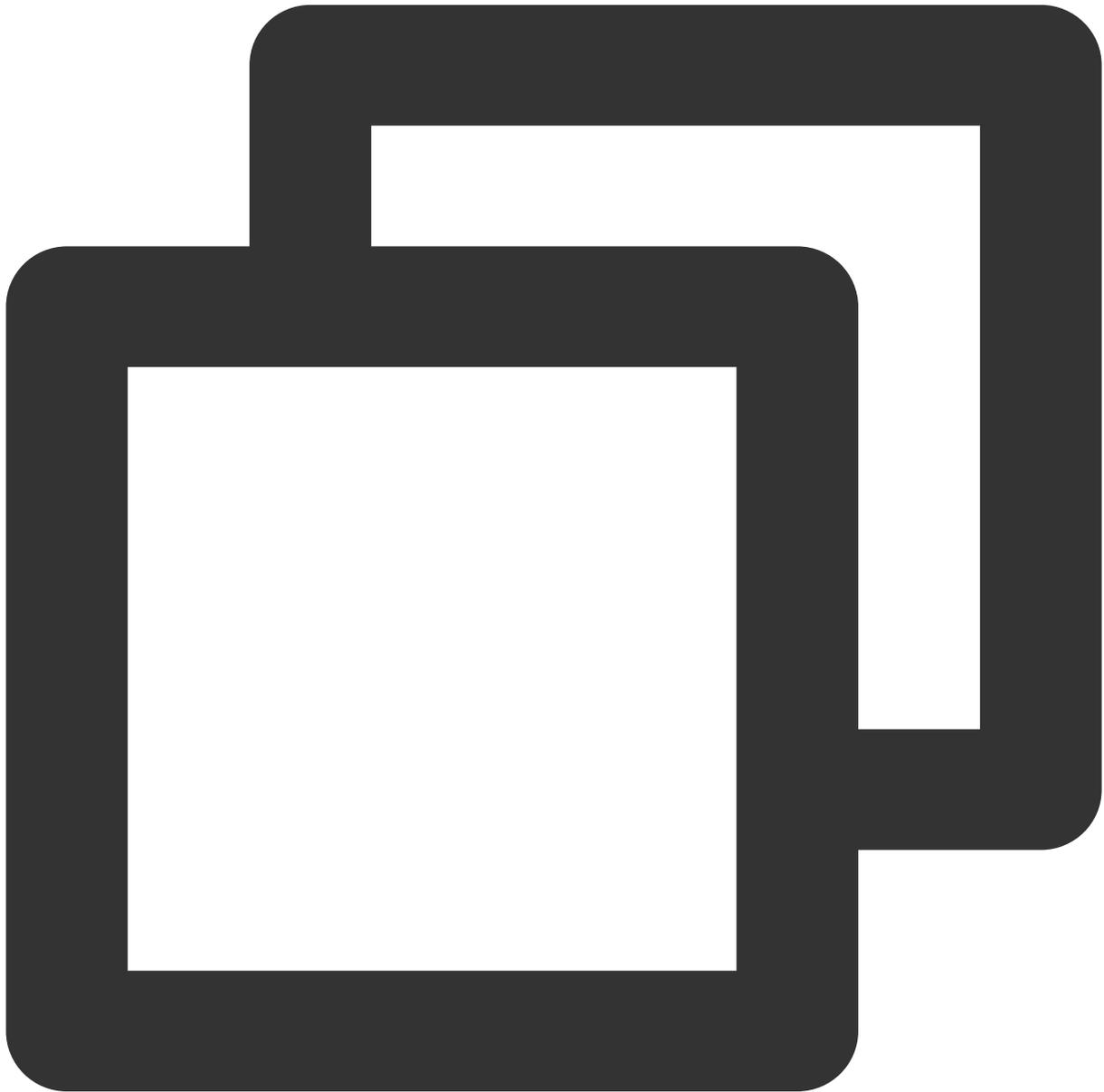
### データディスクの区分

CVM OSに応じてクラウドディスクを確認します。

Linux

Windows

1. [Linuxインスタンスにログイン](#) します。
2. 次のコマンドを実行して、クラウドディスクとデバイス名の間の対応関係を確認します。



```
ls -l /dev/disk/by-id
```

次の情報が表示されます：

```
[root@VM_63_126_centos ~]# ls -l /dev/disk/by-id/  
total 0  
lrwxrwxrwx 1 root root 9 Mar  1 17:31 virtio-disk-35t32l8g -> ../../vdf  
lrwxrwxrwx 1 root root 9 Mar  1 17:31 virtio-disk-je13nl0g -> ../../vdc  
lrwxrwxrwx 1 root root 9 Mar  1 17:31 virtio-disk-jwz43lpg -> ../../vde  
lrwxrwxrwx 1 root root 9 Mar  1 17:31 virtio-disk-punhzcju -> ../../vdd
```

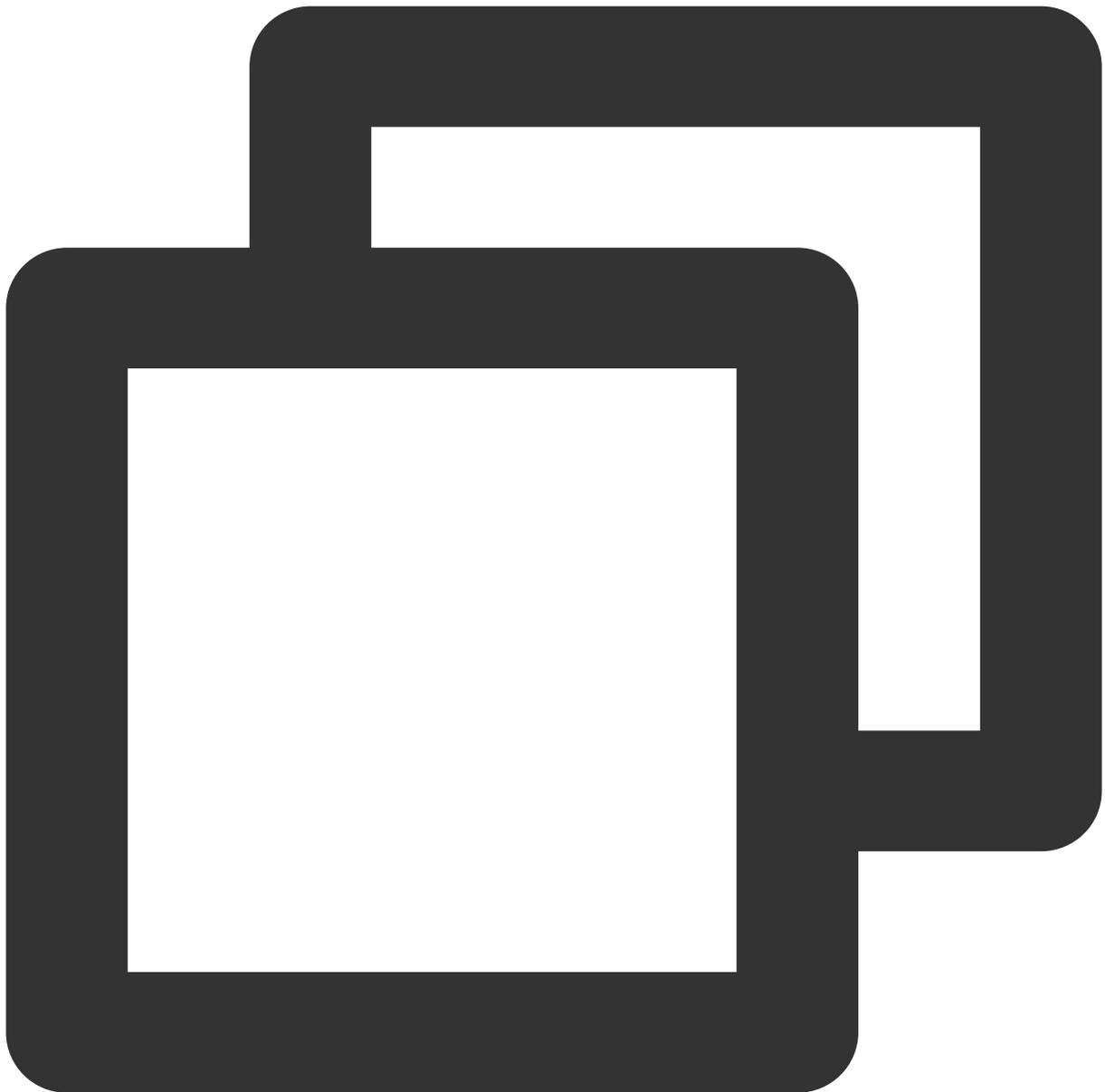
そのうち、`disk-xxxx` はクラウドディスクの ID で、[CBS コンソール](#) に進み確認できます。

1. [Windows インスタンスにログイン](#) します。
- 2.



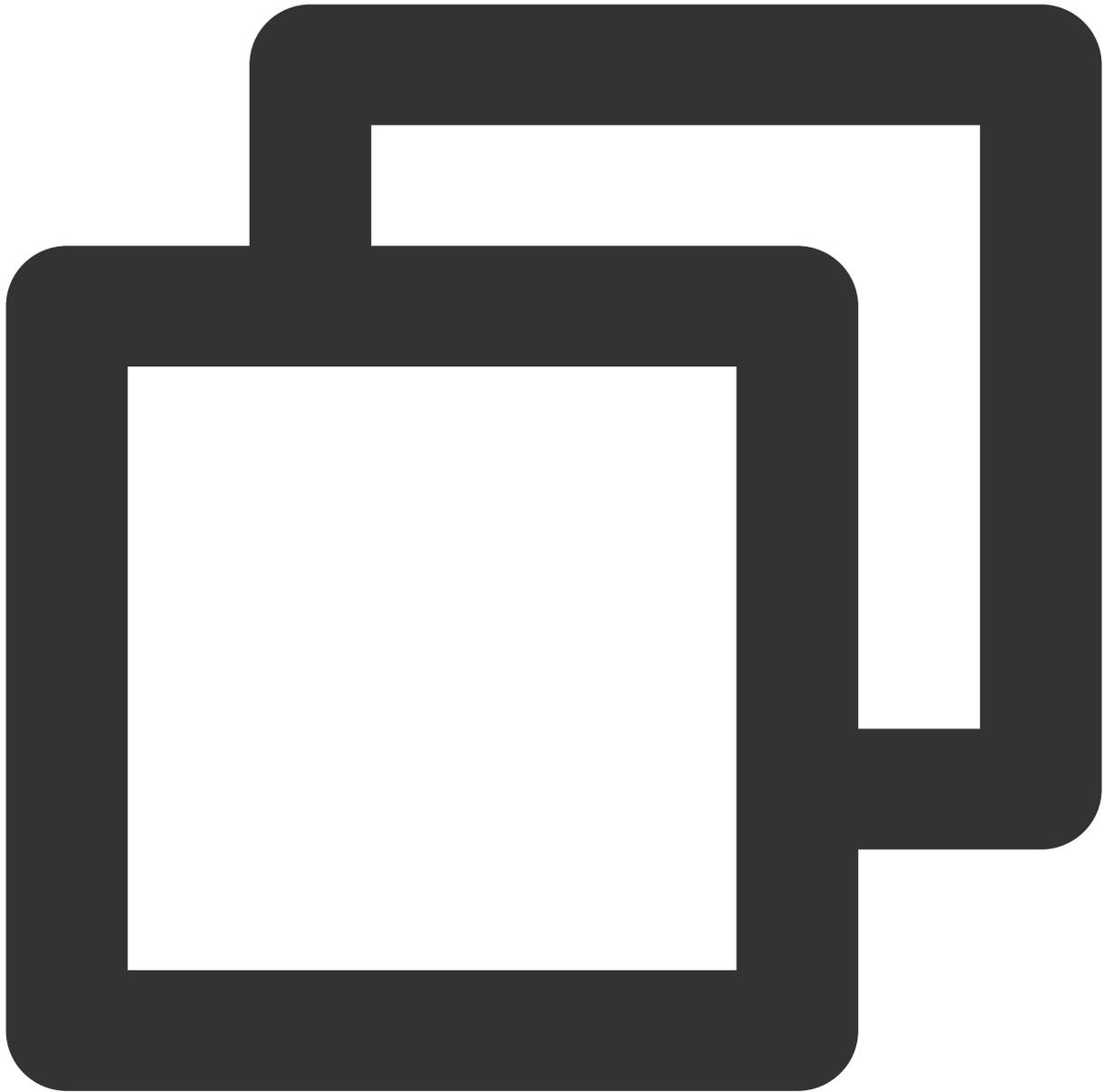
を右クリックして、**実行** を選択します。

3. 「実行」ウィンドウで `cmd` と入力して **Enter** を押します。
4. 次のコマンドを実行して、クラウドディスクとデバイス名の間に対応関係を確認します。



```
wmic diskdrive get caption,deviceid,serialnumber
```

または、次のコマンドを実行します。



```
wmic path win32_physicalmedia get SerialNumber,Tag
```

次の情報が表示されます：

```
C:\Users\Administrator>wmic diskdrive get caption,deviceid,serialnumber
Caption                DeviceID                SerialNumber
Red Hat VirtIO SCSI Disk Device  \\.\PHYSICALDRIVE0
Red Hat VirtIO SCSI Disk Device  \\.\PHYSICALDRIVE1  disk-hmvcnqrm
```

そのうち、 `disk-xxxx` はクラウドディスクの ID で、[CBS コンソール](#) に進み確認できます。

## Cloudinit 構成の確認

CVM OSに応じてクラウドディスクを確認します。

### Linux インスタンスのCloudinit 構成の確認

ディスク拡張後、[Linuxインスタンスにログイン](#)して、`/etc/cloud/cloud.cfg` に`growpart`および`resizefs`の設定項目が含まれているかどうか確認します。

「はい」の場合、その他の操作の必要はありません。下図に示すように：

```
cloud_init_modules:
- migrator
- bootcmd
- write-files
- growpart
- resizefs
- set_hostname
- update_hostname
- ['update_etc_hosts', 'once-per-instance']
- rsyslog
- users-groups
- ssh
```

**growpart**：パーティションをディスクサイズまで拡張します。

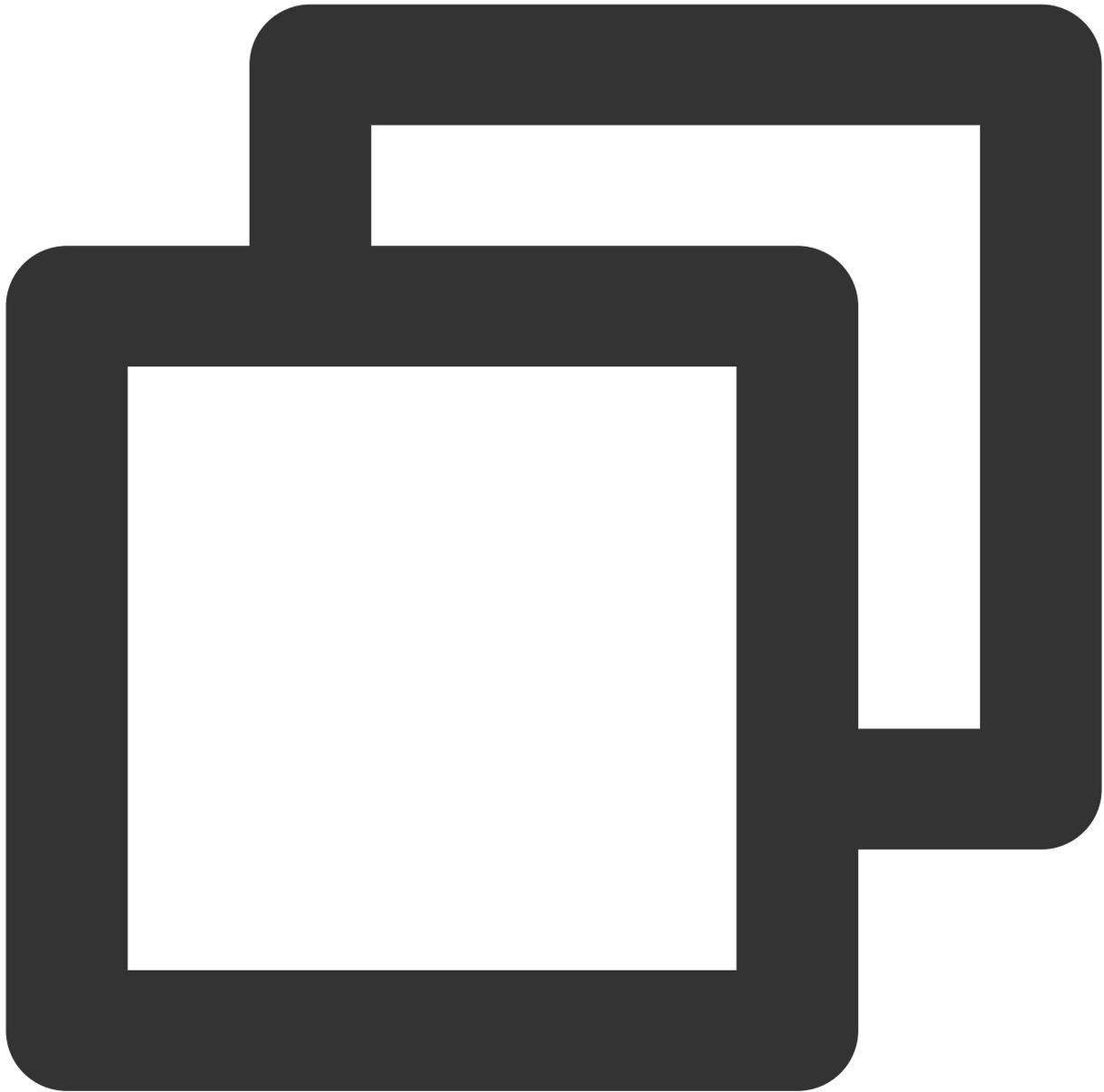
**resizefs**： / パーティション内のファイルシステムをパーティションサイズに拡張または調整します。

「いいえ」の場合、ターゲットCVMのOSに応じて、手動でファイルシステムとパーティションを拡張する必要があります。[パーティションとファイルシステムの拡張 \(Linux\)](#)を実行する必要があります。拡張された容量を既存のパーティションに割り当てるか、独立した新しいパーティションにフォーマットします。

### Windows インスタンスのCloudinit 構成の確認

ディスク拡張後、[Windowsインスタンスにログイン](#)して、`C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf\cloudbase-init.conf` のpluginに`ExtendVolumesPlugin`設定項目が含まれているかどうか確認してください。

「はい」の場合は、マシンを再起動してください。`cloudbase-init` はボリュームを自動的に拡張し、Cパーティションの後ろにある空き領域をCパーティションに追加します。Cパーティションと空き領域の間に他のパーティションがあってはいけないことに注意してください。マシンを再起動したくない場合、Cパーティションと空き領域の間に他のパーティションがある場合、または「cloudbase-init」がサードパーティのセキュリティソフトウェアによってブロックされている場合は、次の powershell コマンドを手動で実行する必要があります。



```
$DiskOps="@  
select disk 0  
select volume c  
extend  
exit  
@"  
$DiskOps | diskpart.exe | Out-Null
```

「いいえ」の場合、ターゲットCVMのOSに応じて、手動でファイルシステムとパーティションを拡張する必要があります。[パーティションとファイルシステムの拡張 \(Windows\)](#) を実行する必要があり、拡張された容量を既存

のパーティションに割り当てるか、独立した新しいパーティションにフォーマットします。

# ディスクメディアの調整

最終更新日：2022-05-26 18:36:43

## 操作シナリオ

Tencent Cloud CVMは、ストレージハードウェアメディアの調整をサポートしています。ストレージハードウェアメディアを調整することにより、異なる業務のストレージ要件に柔軟に対応できます。

Tencent Cloudは、[CBS](#) および [ローカルディスク](#) の2種類のブロックストレージを提供します。現在、ローカルディスクからCBSへの変更をサポートします。本ドキュメントでは、ディスクメディアの調整方法と関連する注意事項について説明します。

ローカルディスクCVMには次の制限があります：

ホストリソースの影響を受けるため、構成をカスタマイズできません。

スナップショットや作成の加速などの機能はサポートされていません。

データの信頼性が低い。

長時間にわたるホスト障害の影響を受けます。

ローカルディスクを持つCVMの制限を解除したい場合は、アカウントの既存のローカルディスクを持つCVMをクラウドディスクを持つCVMに変更できます。

## 前提条件

### CVMの状態

この操作は、CVMが**終了**状態の時のみ実行できます。まずは、CVMをシャットダウンしてください。

### CVMの制限

入札型CVMは、ローカルディスクからCBSへの変更をサポートしていません。

ビッグデータモデル、高IOモデルはローカルディスクからCBSへの変更をサポートしていません

ベアメタル型インスタンスはローカルディスクからCBSへの変更をサポートしていません。

### CVMの設定

CVMのシステムディスクまたはデータディスクには、少なくとも1つの「**通常ローカルディスク**」または「**SSDローカルディスク**」がある場合のみ、ローカルディスクをCBSに変更できます。

CVMが配置されているアベイラビリティゾーンで使用できるCBSタイプがあり、且つ現在のインスタンスのローカルディスクサイズはCBSのサポート範囲内である場合のみ、ローカルディスクをCBSに変更できます。

CVMのシステムディスクとデータディスクの両方がローカルディスクである場合、ローカルディスクをCBSに調整すると、CVMの**すべての**ローカルディスクがCBSに調整されます。部分的な調整はサポートされていません。

各ディスクのクラウドディスクタイプを個別に設定できます。

つまり、完全なローカルディスクのCVMでディスクメディアタイプを変更する場合、システムディスクのみCBS

に調整することまたはデータディスクのみCBSに調整することはサポートされていません。すべてのディスクに調整する必要があります。

ディスクのメディアタイプを変更しても、ディスクのサイズは変わりません。メディアタイプを変更した後、[CBSの拡張](#) からディスクのサイズを調整できます。

ローカルディスクをCBSに変更しても、CVMのライフサイクル、インスタンスID、プライベート/パブリックIP、ディスクデバイス名及びマウントポイントは変更されません。

## 注意事項

ローカルディスクをCBSに変更する操作にはデータコピーの方式を採用して、ローカルディスク上のデータをCBSシステムにコピーしますので、ソースのローカルディスクのサイズおよびデータ転送速度の制限を受けます。この操作の完了には時間がかかります。しばらくお待ちください。

ローカルディスクをCBSに変更することのみが可能です。ローカルディスクをすでにCBSに変更している場合、このCBSをローカルディスクに戻すことはできません。

変更が完了した後、データが失われていないかどうかを確認するために、CVMを起動してログインすることをお勧めします。

## 操作手順

1. [CVMコンソール](#) にログインし、インスタンス管理ページに進みます。

### 説明：

CVMが「無効」状態の場合は、直接 [手順3](#) を実施します。

2. (オプション) 調整対象のCVMの右側で、**その他>インスタンス状態>シャットダウン**を選択して、シャットダウン操作を実行します。

3.

調整対象のCVMの右側で、**その他>リソース調整>ディスクメディアタイプの調整**をクリックします。

4. **ディスクメディアの調整**ダイアログボックスで、システムディスク/データディスクに調整したいターゲットCBSタイプを選択し、同意のチェックボックスをONにすると、**すぐに変換する**をクリックします。

5. 情報を確認し、支払いが必要な注文を完了して、プロセスが完了するまで待ちます。

# CBSのパフォーマンスの調整

最終更新日：2022-01-10 18:16:19

Cloud Block Storage (CBS) のパフォーマンスは、通常ではCBSの容量と相関性があります。CBSがパフォーマンスの最大値に達しない時は、容量を調整することによってパフォーマンスを向上させることができます。このうち、拡張型SSDのCBSは、パフォーマンスがベーシックパフォーマンスの最大値に達した後に、追加パフォーマンスを設定してベーシックパフォーマンスの制限を超えることができます。条件を満たしている場合、必要に応じていつでも追加パフォーマンスを設定して調整することができます。詳細については、[拡張型SSD CBSパフォーマンスの説明](#)をご参照ください。

## ご注意：

現在は**拡張型SSD CBS**のみがパフォーマンスの個別調整をサポートしています。

**ベーシックパフォーマンス** が最大値に達したので、**追加パフォーマンス** を個別調整することができます。

CBSパフォーマンス調整期間は、業務の実施や通常の使用には影響を与えません。

## CBSパフォーマンス調整費用の説明

### パフォーマンスのアップグレード

CBS従量制課金について：すぐに有効になります。新たに設定した価格で課金計算を開始します。

### パフォーマンスのダウングレード

CBS従量制課金について：すぐに有効になります。新たに設定した価格で課金計算を開始します。

## パフォーマンスのアップグレード

### コンソールを使用したパフォーマンスのアップグレード

前提条件を満たす場合、次の手順でパフォーマンスをアップグレードできます。

1. [CBSコンソール](#) にログインします。
2. リージョンを選択し、パフォーマンスを調整するCBSを選択します。
3. 対象のCBSの**その他**>**パフォーマンス調整**を選択します。
4. ポップアップした「パフォーマンス調整」ウィンドウで調整する対象の設定を選択します。
5. 説明を確認して、調整を開始します。

### APIを使用したパフォーマンスのアップグレード

ModifyDiskExtraPerformanceインターフェースを使用して、指定したクラウドディスクのパフォーマンスをアップグレードできます。具体的な操作については、[CBSの追加パフォーマンスの調整](#)をご参照ください。

## パフォーマンスのダウングレード

### コンソールを使用したパフォーマンスのダウングレード

前提条件を満たす場合、次の手順でパフォーマンスをダウングレードできます。

1. [CBSコンソール](#) にログインします。
2. リージョンを選択し、パフォーマンスを調整するCBSを選択します。
3. 対象のCBSの**その他**>**パフォーマンス調整**を選択します。
4. ポップアップした「パフォーマンス調整」ウィンドウで調整する対象の設定を選択します。
5. 説明を確認して、調整を開始します。

### APIを使用したパフォーマンスのダウングレード

ModifyDiskExtraPerformanceインターフェースを使用して、指定したクラウドディスクのパフォーマンスをダウングレードできます。具体的な操作については、[CBSの追加パフォーマンスの調整](#)をご参照ください。

# ネットワーク VPCサービス切替

最終更新日：：2024-03-26 14:58:53

## 操作シナリオ

Tencent Cloud上のネットワークは基幹ネットワークとプライベートネットワークに分かれ、両者はユーザーにそれぞれ優れたサービスを提供します。これに基づいて、より柔軟なサービスを提供し、ネットワーク管理を容易にします。

ネットワーク間の切り替え

**基幹ネットワークからVPCへの切り替え**：Tencent Cloudは単一のCVMおよび複数のCVMの基幹ネットワークからVPCへの切り替えサービスをご提供いたします。

**VPC AからVPC Bへの切り替え**：Tencent Cloudは単一のCVMおよび複数のCVMのVPC AからVPC Bへの切り替えサービスをご提供いたします。

カスタマイズIPの設定

自身でインスタンスの元のプライベートIPおよびHostName能力を保持することを選択します

## 前提条件

移行前に、プライベート/パブリックネットワークのCLBおよびすべての補助Elastic Network Interface (ENI) のバインドを自身で解除し、プライマリENIの補助IPをリリースしてください。移行後に再びバインドします。

## 操作手順

### インスタンスのネットワーク属性の判断

1. [CVMコンソール](#)にログインします。
2. 「インスタンス」リストページで、実際に使用されているビューモードに従い、ネットワークを切り替えたいターゲットインスタンスを確認します。

リストビュー

タブビュー

下図に示すように、「インスタンス設定」に表示されているネットワークが「基幹ネットワーク」であれば、そのインスタンスが所属するネットワークは基幹ネットワークです。

Create Start up Shutdown Restart Reset Password More Actions ▾						
Separate keywords with " "; press Enter to separate filter tags						
ID/Name	Monitoring	Status ▾	Availability Zone ▾	Instance Type ▾	Instance Configuration	
<input checked="" type="checkbox"/> ins		Running Terminated instances failed	Guangzhou Zone 3	Standard S3	1-core 1GB 10I System disk: Pi Cloud Storage Network: Classic network	

「基本情報」の中の「ネットワーク情報」に表示されているネットワークが「基幹ネットワーク」であれば、そのインスタンスが所属するネットワークは基幹ネットワークです。

#### ご注意：

基幹ネットワークからVPCへの切り替え後は元に戻せません。CVMからVPCへの切り替え後、その他の基幹ネットワークのクラウドサービスとは相互接続できません。

基幹ネットワークからVPCに切り替える前に、移行したい基幹ネットワークCVMと同一リージョンのVPC、ならびに同一のアベイラビリティゾーンのサブネットワークを事前に作成しておく必要があります。具体的には [VPCの作成](#) をご参照ください。

インスタンスのネットワーク属性を把握した後は、必要に応じて [VPCへの切り替え](#) 手順を参照し、対応する操作を行ってください。

## VPCへの切り替え

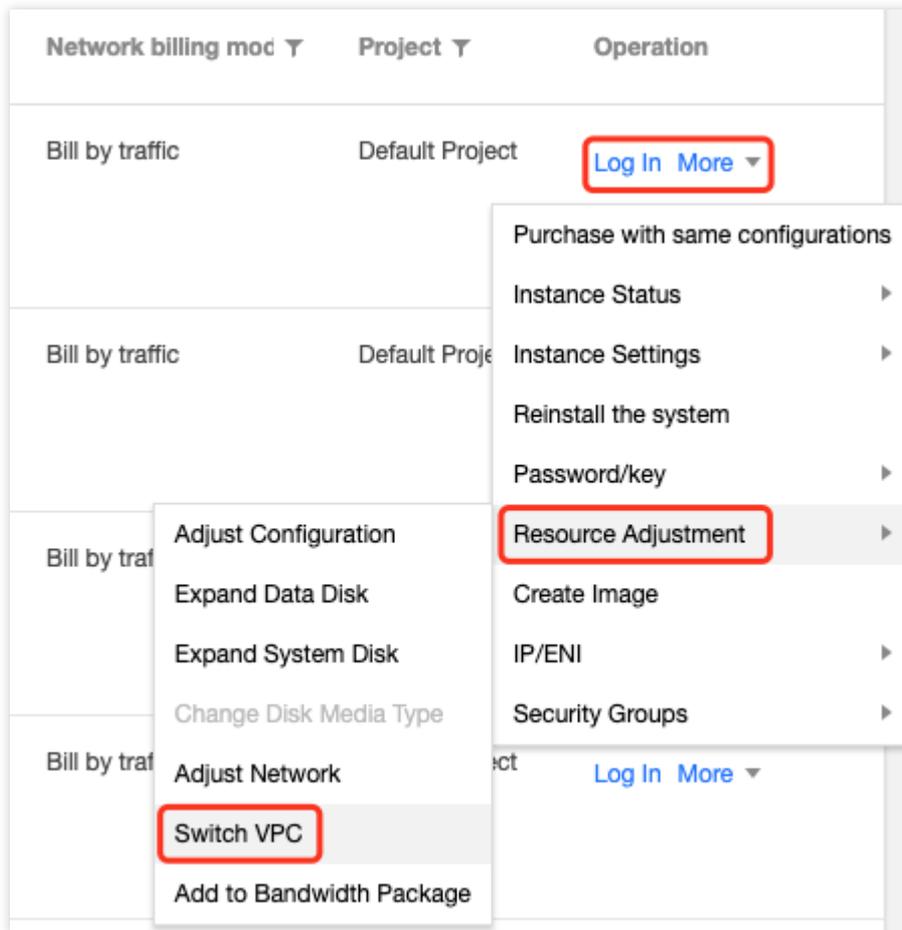
- [CVMコンソール](#) にログインします。
- 「インスタンス」ページで、ターゲットインスタンスをVPCに切り替えます。

リストビュー

タブビュー

### 単一インスタンスのVPCへの切り替え

下図に示すように、ネットワークを切り替えたいターゲットインスタンスを選択し、右側の操作バーで、**その他 > リソース調整 > VPCへの切り替え** を選択します。



### 複数インスタンスのVPCへの切り替え

下図に示すように、ターゲットインスタンスのVPCへの一括切り替えを行う必要がある場合は、ネットワークを切り替えたいインスタンスにチェックを入れ、インスタンスリストの上方で、**その他の操作 > リソース調整 > VPCへの切り替え**を選択します。

#### ご注意：

CVMのネットワークタイプを一括で切り替える場合は、選択するCVMが必ず同一のアベイラビリティーゾーンになければなりません。

The screenshot shows the Tencent Cloud console interface for managing instances. At the top, there are buttons for 'Create', 'Start up', 'Shutdown', 'Restart', 'Reset Password', and 'More Actions'. The 'More Actions' dropdown menu is open, showing options like 'Terminate/Return', 'Instance Settings', 'Load a key', 'Resource Adjustment', and 'Add to security group'. The 'Resource Adjustment' option is highlighted with a red box. Below the menu, a table lists instances. The first instance is selected, and a context menu is open over it, showing 'Adjust Network' and 'Switch VPC' options, both highlighted with red boxes. The table columns include 'ID/Name', 'Monitoring', 'Status', 'Availability Z', and 'Instance'.

下図に示すように、ネットワークを切り替えたいターゲットインスタンスのタブを選択し、右上隅の**その他の操作** > **リソース調整** > **VPCへの切り替え**を選択します。

The screenshot shows the details of a newly created instance named 'Unnamed'. The instance is in a 'Running' state. The 'Basic Information' tab is selected, showing details like Name, Instance ID, UUID, and Instance Specification. The instance is located in Guangzhou Zone 3. The console also shows options for 'Log In', 'Shutdown', and 'Restart'.

3. ポップアップした「VPCへの切り替え」ウィンドウで、注意事項を確認し、**次のステップ**をクリックします。
4. VPCおよび対応するサブネットワークを選択し、**次のステップ**をクリックします。

### Switch VPC

✓ Preparation > 2 Select Network > 3 Set IP > 4 Shutdown

VPC VPC1(vpc-p

Please select a subnet in Guangzhou Zone 3.

Search by subnet name/ID

Name	ID	CIDR	Amount
<input checked="" type="radio"/> test0723	subnet	192.168	240

Previous step Next Close

5. 実際のニーズに応じて、下図のように現在選択されているサブネットワークでプライベートIPアドレスおよびHostNameオプションを設定します。

### Switch VPC

✓ Preparation > ✓ Select Network > **3 Set IP** > 4 Shutdo

Instance IP Address

Instance Name	Instance ID	Pre-allocate IP
[Redacted]	ins-98tsl77k	Auto allocated if it's left

Migrate to VPC [Redacted]

Subnet [Redacted]

Retain original private IP  No  Yes  
You can choose to obtain a new private IP or retain the original private IP.

HostName Options \*  Reset HostName  Retain original HostName of the instance  
While switching VPC, you can choose to reset the instance HostName or retain the old HostN

[Previous](#) [Next](#) [Close](#)

主なパラメータは次のとおりです：

**IPアドレスの事前割り当て：**インスタンスの元のプライベートIPを保持しない場合、「IPアドレスの事前割り当て」と入力してください。入力されていない場合、システムが自動的に割り当てます。

**インスタンスの元のプライベートIPを保持するかどうか：**必要に応じてインスタンスの元のプライベートIPアドレスを保持するかどうかを選択することができます。

**HostNameオプション：**必要に応じてインスタンスの元のHostNameを保持するかどうかを選択することができます。

6. 下図に示すように、**次へ**をクリックして、シャットダウンプロンプトに従って操作を行い、**移行開始**をクリックし、コンソールページでインスタンスの変更ステータスを「インスタンスのvpc属性変更」とします。

#### ご注意：

移行プロセスでは、ホストのインスタンスを再起動する必要があります。その他の操作は行わないでください。移行後、インスタンスの稼働状態を注意深くチェックし、プライベートネットワークのアクセスおよびリモートログインが正常かどうかチェックしてください。

☐ cvm15-Big4-test   Running  Tokyo Zone 1  S2  1-core 1 GB 1 Mbps  
System disk: Premium Cl  
Network: tes123  Bill by traffic

[ModifyInstances...](#)

# 一般的なパブリックIPアドレス

最終更新日：2023-04-11 18:11:13

## 概要

このドキュメントでは、一般的なパブリックIPアドレスを使用する方法についてご紹介いたします。一般的なパブリックIPはCloud Virtual Machineの購入時にのみ割り当てられます。CVMとの関連付けを解除することはできません。購入時に割り当てられていない場合は、取得することができません。

### 説明：

従来アカウントタイプでは、CVMからEIPの関連付けを解除すると、各アカウントは一般的なパブリックIPアドレスを1日あたり10回無料で再割り当てできます。

現在、一般的なパブリックIPアドレスは、General BGP IPのみサポートしています。

## 操作ガイド

次の一般的なパブリックIP機能を使用することができます。

機能タイプ	操作シナリオ	関連ドキュメント
パブリックIPアドレスの復元	誤操作によってパブリックIPアドレス（Elastic IPと一般的なパブリックIPを含む）をリリースまたは返却した場合は、パブリックIPコンソールで復元でき、復元後のパブリックIPはElastic IPとなります。	-
一般的なパブリックIPをEIPに変換	CVMの一般的なパブリックIPをElastic IPに変換すると、変換後のElastic IPはいつでもCVMと関連付けおよび関連付け解除できるため、パブリックIPの柔軟な管理をさらに手軽に実現できます。	-
パブリックIPの変更	CVMの一般的なパブリックIPを変更し、変更後、元のパブリックIPはリリースされます。	<a href="#">CVMコンソールにおけるパブリックIPの変更</a>
ネットワーク帯	必要に応じて、帯域幅または課金モデルを変更できます。変更が完了した時点ですぐに反映されます。	<a href="#">ネットワーク設定の調整</a>

域幅の調  
整

# EIP

最終更新日：：2022-09-23 16:23:58

## ユースケース

ElasticパブリックIPアドレス（EIP）は、Elastic IPアドレスまたはElastic IPと呼ばれます。ダイナミッククラウドコンピューティングのために設計した静的なIPアドレスであり、あるリージョンにおいて、固定パブリックIPアドレスと指します。EIPを使用すると、アドレスをアカウント内の別のインスタンスまたは [NAT Gatewayインスタンス](#) にマッピングでき、インスタンスの故障を避けられます。本ドキュメントはEIPの使用方法について紹介します。

### EIPを申請する

1. [CVMコンソール](#) にログインしました。
2. 左側ナビゲーションバーで、[Public IP](#) をクリックし、EIPの管理画面にアクセスします。
3. EIPの管理画面で、[申請](#) をクリックします。リージョンを選択し、数量も記入します。
4. 申請が完成した後、申請したEIPをリストに表示され、この時はまだ未バインド状態になっています。

### EIPにクラウド製品をバインドする

1. [CVMコンソール](#) にログインしました。
2. 左側ナビゲーションバーで、[Public IP](#) をクリックし、EIPの管理画面にアクセスします。
3. EIPの管理画面で、バインドする必要があるクラウド製品のEIP を選択し、[バインド](#) をクリックします。

#### ご注意：

- バインドする時に、EIP がすでにインスタンスにバインドされている場合は、最初にバインドを解除します。
4. ポップアップボックスでバインドするクラウド製品のタイプを選択し、対応するクラウド製品インスタンスIDを選択し、[バインディング]ボタンをクリックして、クラウド製品とのバインディングを完成させます。

### EIPにクラウド製品をバインド解除する

1. [CVMコンソール](#) にログインしました。
2. 左側ナビゲーションバーで、[Public IP](#) をクリックし、EIPの管理画面にアクセスします。
3. EIPの管理画面で、バインド解除する必要があるクラウド製品のEIPを選択し、[バインド解除](#) をクリックします。
4. [OK](#) をクリックします。

#### ご注意：

バインド解除が完成した後、クラウド製品のインスタンスが新しいパブリックネットワークIPにアサインされ、バインディング前のパブリックネットワークIPと一致しない場合があります。

## EIPをリリースする

1. [CVMコンソール](#) にログインしました。
2. 左側ナビゲーションバーで、**Public IP** をクリックし、EIPの管理画面にアクセスします。
3. EIPの管理画面で、リリースする必要があるクラウド製品のEIPを選択し、**詳細>リリース**をクリックします。
4. **OK**をクリックし、リリースを完成させます。

## 帯域幅を調整する

1. [CVMコンソール](#) にログインしました。
2. 左側ナビゲーションバーで、**Public IP** をクリックし、EIPの管理画面にアクセスします。
3. EIPの管理画面で、帯域幅を調整する必要があるEIP を選択し、**帯域幅を調整する**をクリックします。
4. 帯域幅を調整する画面で、目標帯域幅値を調整します。
5. **OK**をクリックし、調整を完成させます。

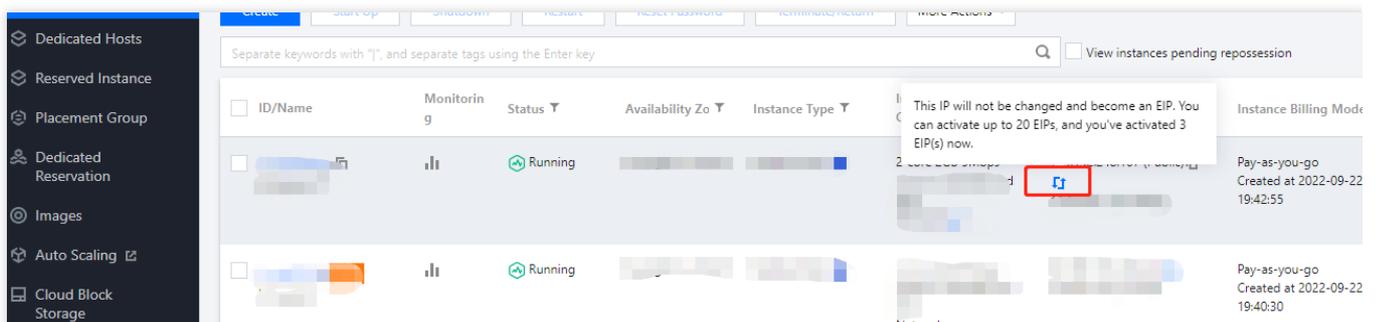
## パブリックネットワークIPをEIPに置き換える

Cloud Virtual Machine (CVM) のインスタンスを購入する際と同時に購入したパブリックネットワークIPは普通のパブリックネットワークIPであり、Elastic機能を持たない、つまりマウントまたはアンマウントされることができません。以下のような操作手順に従って、普通のパブリックネットワークIPをEIPに置き換えることができます。

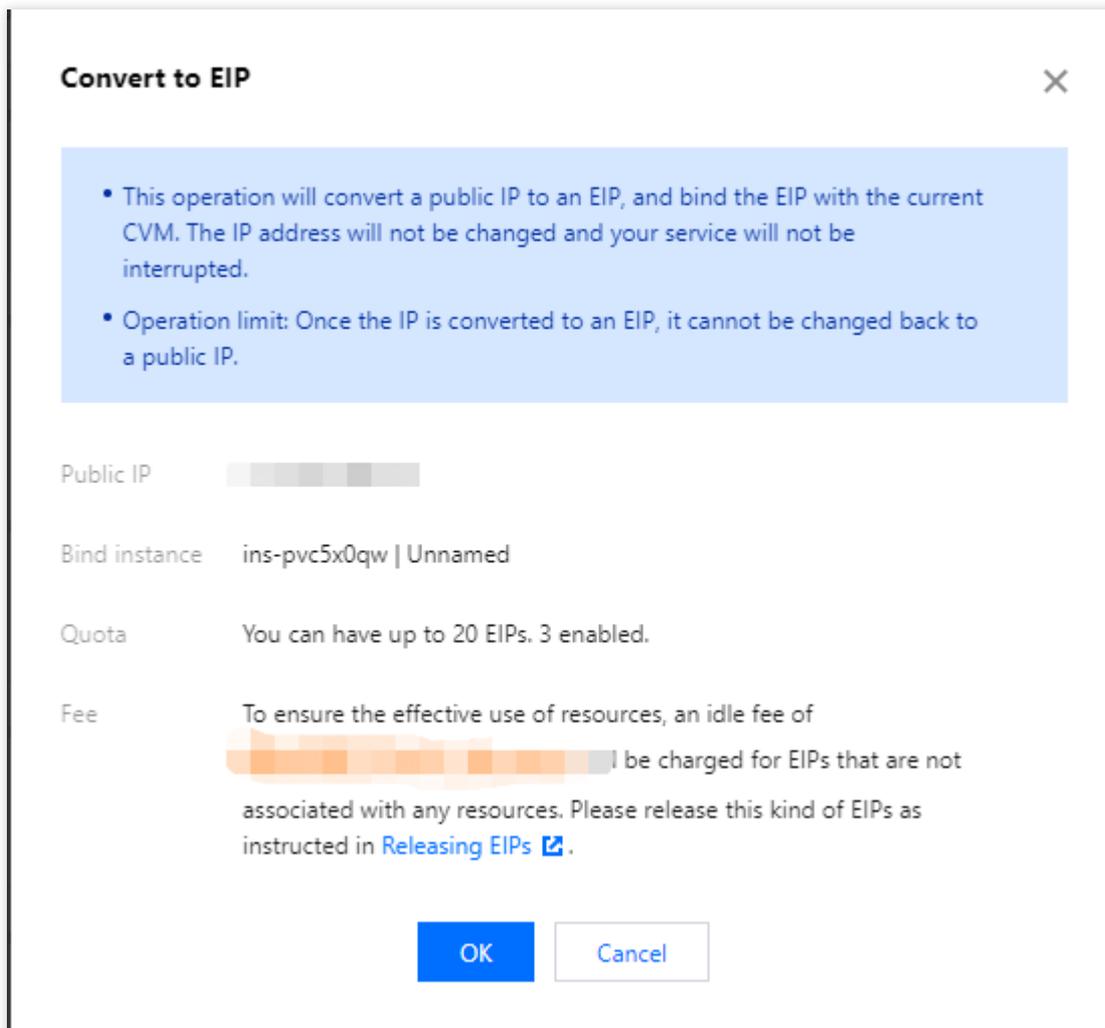
1. 左側ナビゲーションバーで、**インスタンス** をクリックし、インスタンスの管理画面にアクセスします。
2. EIPに置き換えたいインスタンスを選択し、



をクリックします。下図に示すように：



3. ポップアップの「EIPに置き換える」ウィンドウで、**置き換えを確定する**をクリックします。



## 異常をチェックする

EIPはネットワーク通信異常が発生した可能性があり、原因は以下のように：

EIPにクラウド製品がバインドされていません。バインドの方法は [EIPにクラウド製品のバインド](#) をご参照ください。

セキュリティポリシーが無効です。有効なセキュリティポリシー（セキュリティグループまたはネットワークACL）があるかどうかを確認します。バインドされたクラウド製品のインスタンスにセキュリティポリシーがあれば、例えば：8080ポートにアクセスを禁止すると、EIPの8080ポートにはアクセスできません。

# ENI

最終更新日：：2023-05-12 17:22:54

CVMインスタンスのENIを設定するには、次の手順に従います。

1. [ENIを作成します](#)。

ENIの作成が完了したら、「[ENIの表示](#)」ページでENIの詳細情報を確認できます。

2. [CVMインスタンスにENIをアタッチして構成する必要があります。\(重要\)](#)

3. CVM およびVPCルートテーブルを設定します。

4. プライベートIPを割り当てます。

5. [Virtual Private Cloud](#) コンソールにログインします。

6. 画面左側のナビゲーションバーで「[ENI](#)」をクリックして、[ENIリストページ](#)に進みます。

7. 「[ENI ID/名前](#)」をクリックすると、詳細情報が表示されます。

8. 「[IP Management](#)」をクリックして、詳細ページに進みます。

9. 「[Assign private IP](#)」をクリックして、IPアドレスの割り当て方法(自動割り当てまたは手動入力。手動入力を選択した場合は、適切なプライベート IP を入力する必要がある)を選択し、「[OK](#)」をクリックします。

10. ENI を管理します。

[プライベートIPの解放](#)

[CVMインスタンスからENIをデタッチする](#)

[ENIの削除](#)

[EIPをENIに関連付ける](#)

[ENIからEIPの関連付けを解除する](#)

[プライマリプライベートIPの変更](#)

[ENIのサブネットの変更](#)

# パブリックネットワークゲートウェイの構成

最終更新日：：2023-02-16 10:20:28

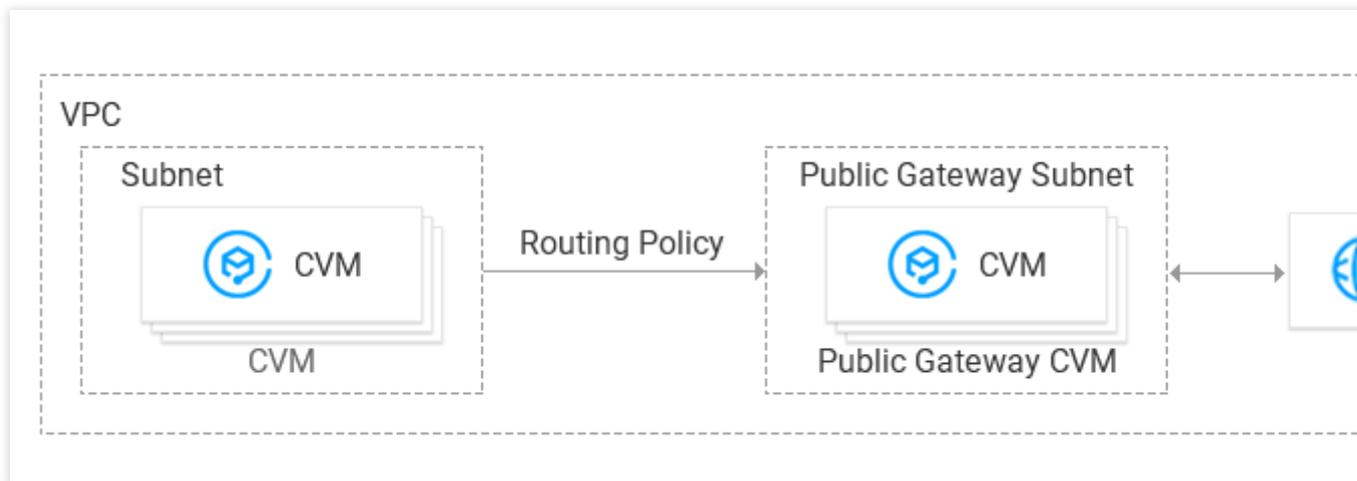
## 警告：

単一のCloud Virtual Machine (CVM) をパブリックゲートウェイとして使用すると、シングルポイントリスクがあるため、本番環境では [NAT Gateway](#) を使用することをお勧めします。

注意：2019年12月06日以降、Tencent Cloudは、CVMの購入ページでのパブリックゲートウェイの選択と設定をサポートしません。必要に応じて、このドキュメントでの設定に従って、ご自身で設定してください。

## 概要

Tencent Cloud VPCの一部のCVMに共通のパブリックネットワークIPがないが、パブリックネットワークにアクセスする必要がある場合は、パブリックネットワークIP（共通のパブリックネットワークIPまたはElasticパブリックネットワークIP）を備えたCVMを使用してパブリックネットワークにアクセスできます。パブリックゲートウェイCVMは、アウトバウンドトラフィックのソースアドレス変換を実行します。他のすべてのCVMがパブリックネットワークにアクセスするトラフィックは、パブリックゲートウェイCVMを通過した後、ソースIPがパブリックゲートウェイCVMのパブリックネットワークIPアドレスに変換されます。下図の通りです：



## 前提条件

すでに [CVMコンソール](#) ログインしています。

パブリックゲートウェイCVMは、配置されているサブネット上にないルートの転送要求のみを転送できるため、パブリックゲートウェイCVMは、パブリックゲートウェイを使用してパブリックネットワークにアクセスする必要があるCVMと同じサブネット内に存在することはできません。

パブリックゲートウェイCVMはLinux CVMである必要があります。Windows CVMをパブリックゲートウェイとして使用することはできません。

## 操作手順

### 手順1：Elasticパブリックネットワークへのバインディング（オプション）

#### 説明：

パブリックゲートウェイとして使用されるCVMにすでにパブリックネットワークIPアドレスがある場合は、この手順をスキップして次の手順を完了してください。

1. [CVMコンソール](#)にログインし、左側ナビゲーションバーでは、[ElasticパブリックネットワークIP](#)をクリックして、ElasticパブリックネットワークIP管理ページへ進みます。
2. インスタンスをバインディングする必要があるElasticパブリックネットワークIPのアクションバーの下にある**その他** > **バインディング**を選択します。



3. 「リソースのバインディング」ポップアップボックスで、パブリックゲートウェイとして選択されたCVMインスタンスを選択してバインディングします。

### Bind resources

Please select the resource to be bound with the EIP eip-3pul2wy4.

CVM Instances  NAT Gateway  ENI  Highly Available Virtual IP

Enter a name or ID

	Instance ID/Name	Availability Zone	Private IP	Bound public IP
<input checked="" type="radio"/>		Guangzhou Zone 3		
<input type="radio"/>		Guangzhou Zone 3		
<input type="radio"/>		Guangzhou Zone 4		

## 手順2：ゲートウェイが配置されているサブネットのルートテーブルの設定

### ご注意：

ゲートウェイサブネットと共通サブネットを同じルートテーブルにアソシエイトすることはできません。独立したゲートウェイルートテーブルを作成し、ゲートウェイサブネットをこのルートテーブルにアソシエイトしてください。

1. [カスタマイズルートテーブルの作成](#)。
2. 作成後、サブネットへのアソシエイトアクションが要求されます。パブリックゲートウェイサーバーが配置されているサブネットを直接アソシエイトすることができます。

### Associate Subnet

Select the subnet to associate

Subnet ID/name	Subnet CIDR Block/...	Route table associat...
<input checked="" type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		

Note: each subnet can only be bound with one route table. Once you click "Confirm", the existing route table will be replaced with: lab-rt

### 手順3：共通サブネットのルートテーブルの設定

共通サブネットのルートテーブルを設定します。デフォルトでルーティングがパブリックゲートウェイCVMを経由することで、共通サブネット内のCVMがパブリックゲートウェイのルーティング転送機能によってパブリックネットワークにアクセスできるように設定します。

共通CVMが配置されているサブネットのルートテーブルに、次のルーティングポリシーを追加します：

ターゲット側：アクセスするパブリックネットワークアドレス。

ネクストホップタイプ：CVM。

ネクストホップ：手順1でElasticパブリックネットワークIPにバインディングされたCVMインスタンスのプライベートネットワークIP。

具体的な操作については、[ルーティングポリシーの設定](#)をご参照ください。

### Add a route

Destination	Next hop type	Next hop	Notes
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="CVM"/>	<input type="text" value=""/> <a href="#">Create a CVM</a>	<input type="text"/>

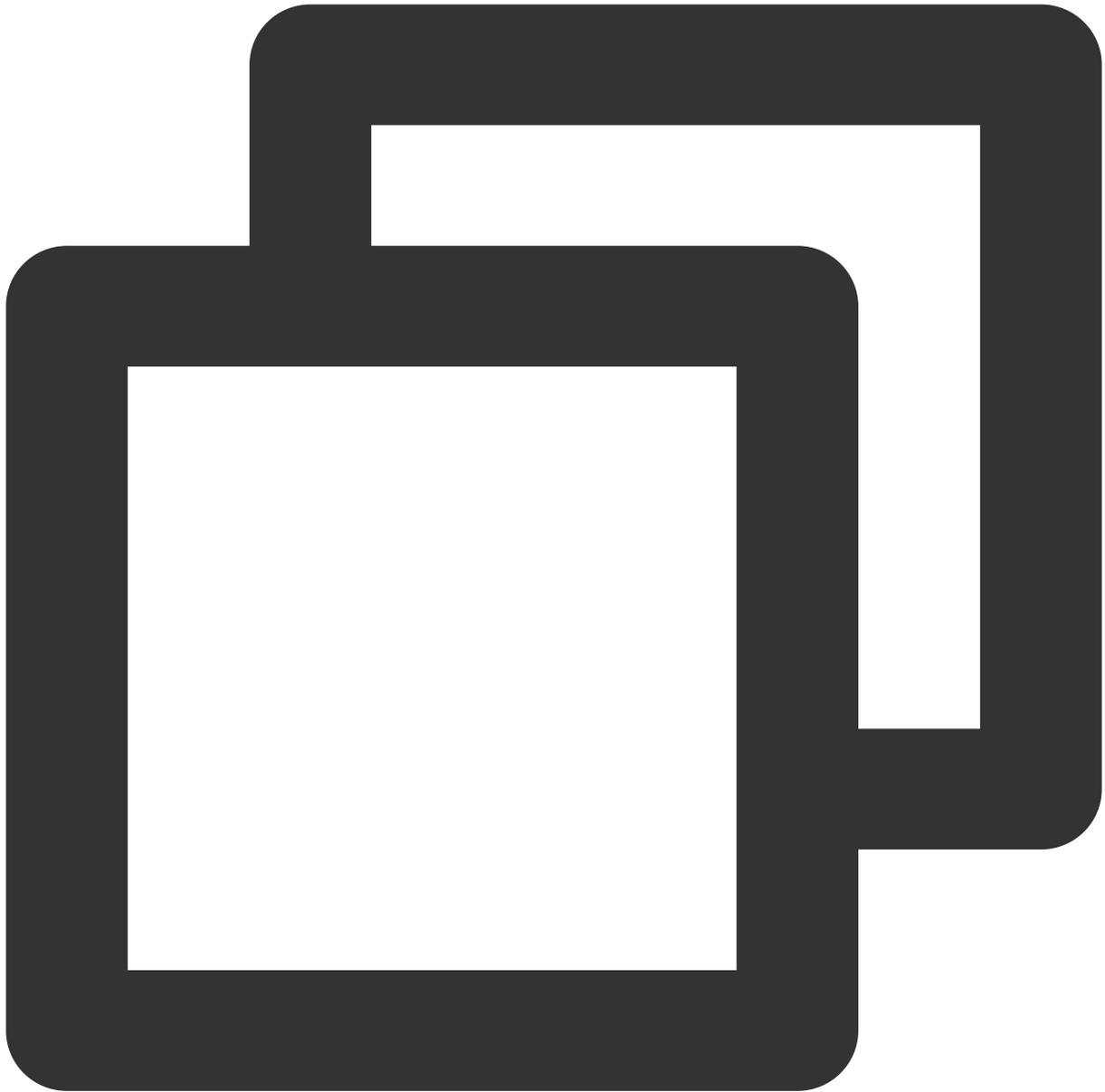
+ Add a line

Routing policies controls the traffic flow in the subnet. For details, please see [Configuring Routing Policies](#).

## 手順4：パブリックゲートウェイの設定

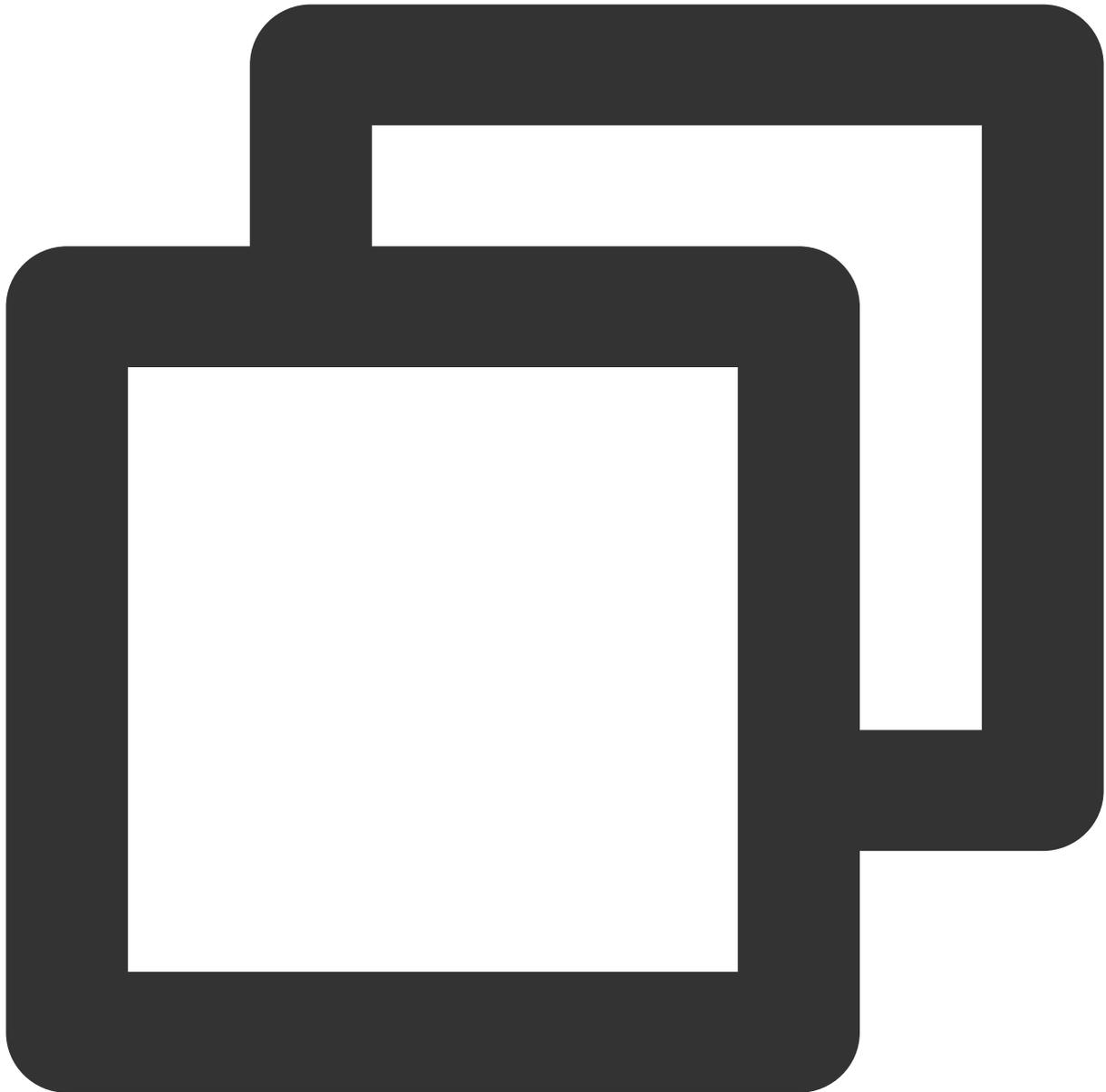
1. [パブリックゲートウェイCVM](#) にログインし、次の操作を実行してネットワーク転送およびNATプロキシ機能を有効にします。

1.1 次のコマンドを実行して、`usr/local/sbin` ディレクトリにスクリプト `vpcGateway.sh` を新規作成します。



```
vim /usr/local/sbin/vpcGateway.sh
```

1.2 **i**を押して編集モードに切り替え、次のコードをスクリプトに書き込みます。

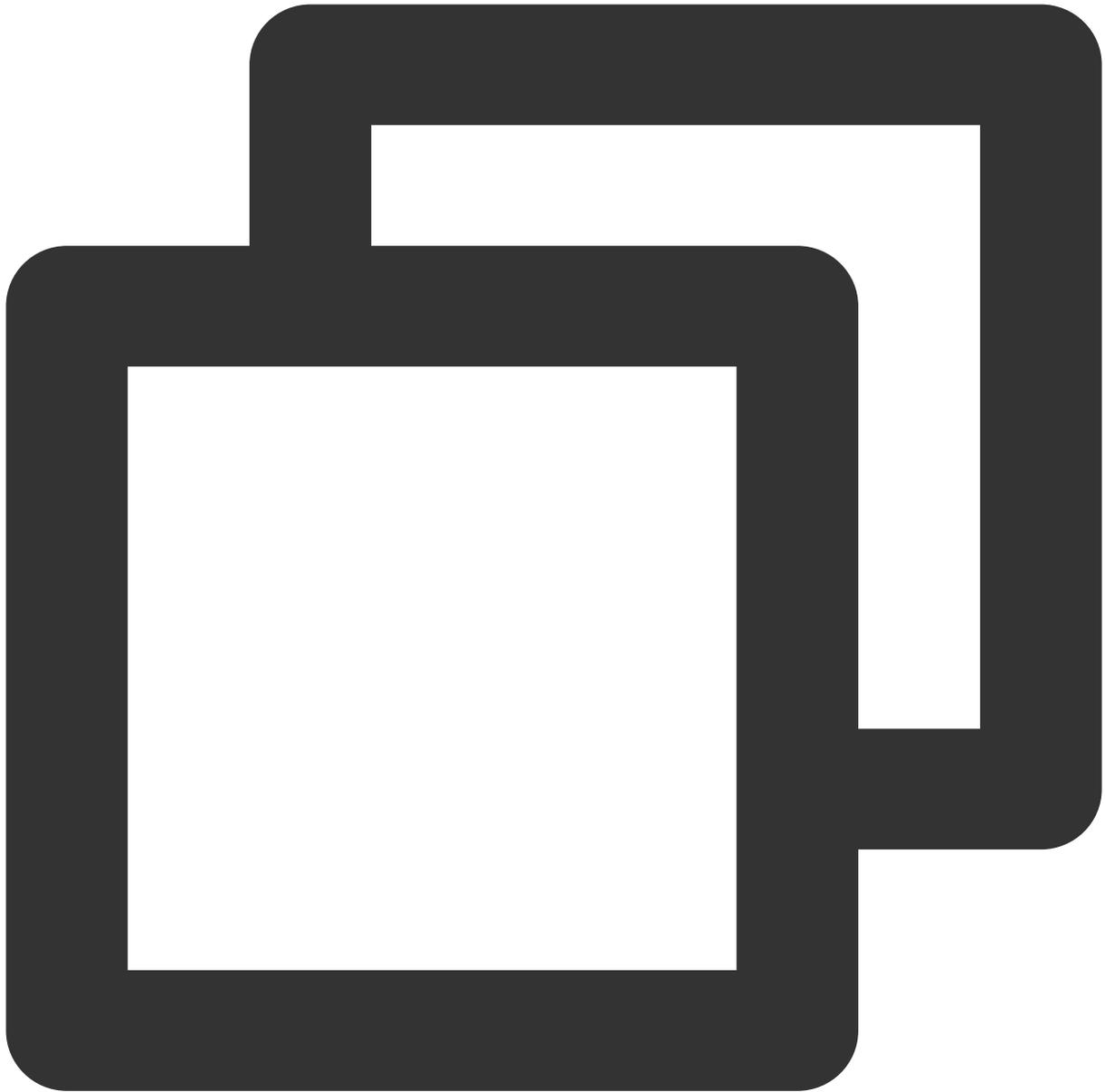


```
#!/bin/bash
echo "-----"
echo "`date`"
echo "(1)ip_forward config....."
file="/etc/sysctl.conf"
grep -i "^net\\.ipv4\\.ip_forward\\.*" $file &>/dev/null && sed -i \\
's/net\\.ipv4\\.ip_forward\\.*/net\\.ipv4\\.ip_forward = 1/' $file || \\
echo "net.ipv4.ip_forward = 1" >> $file
echo 1 > /proc/sys/net/ipv4/ip_forward
[ `cat /proc/sys/net/ipv4/ip_forward` -eq 1 ] && echo "-->ip_forward:Success" || \\
echo "-->ip_forward:Fail"
```

```
echo "(2)Iptables set....."
iptables -t nat -A POSTROUTING -j MASQUERADE && echo "-->nat:Success" || echo "-->n
iptables -t mangle -A POSTROUTING -p tcp -j TCPOPTSTRIP --strip-options timestamp &
echo "-->mangle:Success" || echo "-->mangle:Fail"
echo "(3)nf_contrack config....."
echo 262144 > /sys/module/nf_contrack/parameters/hashsize
[ `cat /sys/module/nf_contrack/parameters/hashsize` -eq 262144 ] && \
echo "-->hashsize:Success" || echo "-->hashsize:Fail"
echo 1048576 > /proc/sys/net/netfilter/nf_contrack_max
[ `cat /proc/sys/net/netfilter/nf_contrack_max` -eq 1048576 ] && \
echo "-->nf_contrack_max:Success" || echo "-->nf_contrack_max:Fail"
echo 10800 >/proc/sys/net/netfilter/nf_contrack_tcp_timeout_established \
[ `cat /proc/sys/net/netfilter/nf_contrack_tcp_timeout_established` -eq 10800 ] \
&& echo "-->nf_contrack_tcp_timeout_established:Success" || \
echo "-->nf_contrack_tcp_timeout_established:Fail"
```

1.3 **Esc**を押し、**:wq**を入力して、ファイルを保存して戻ります。

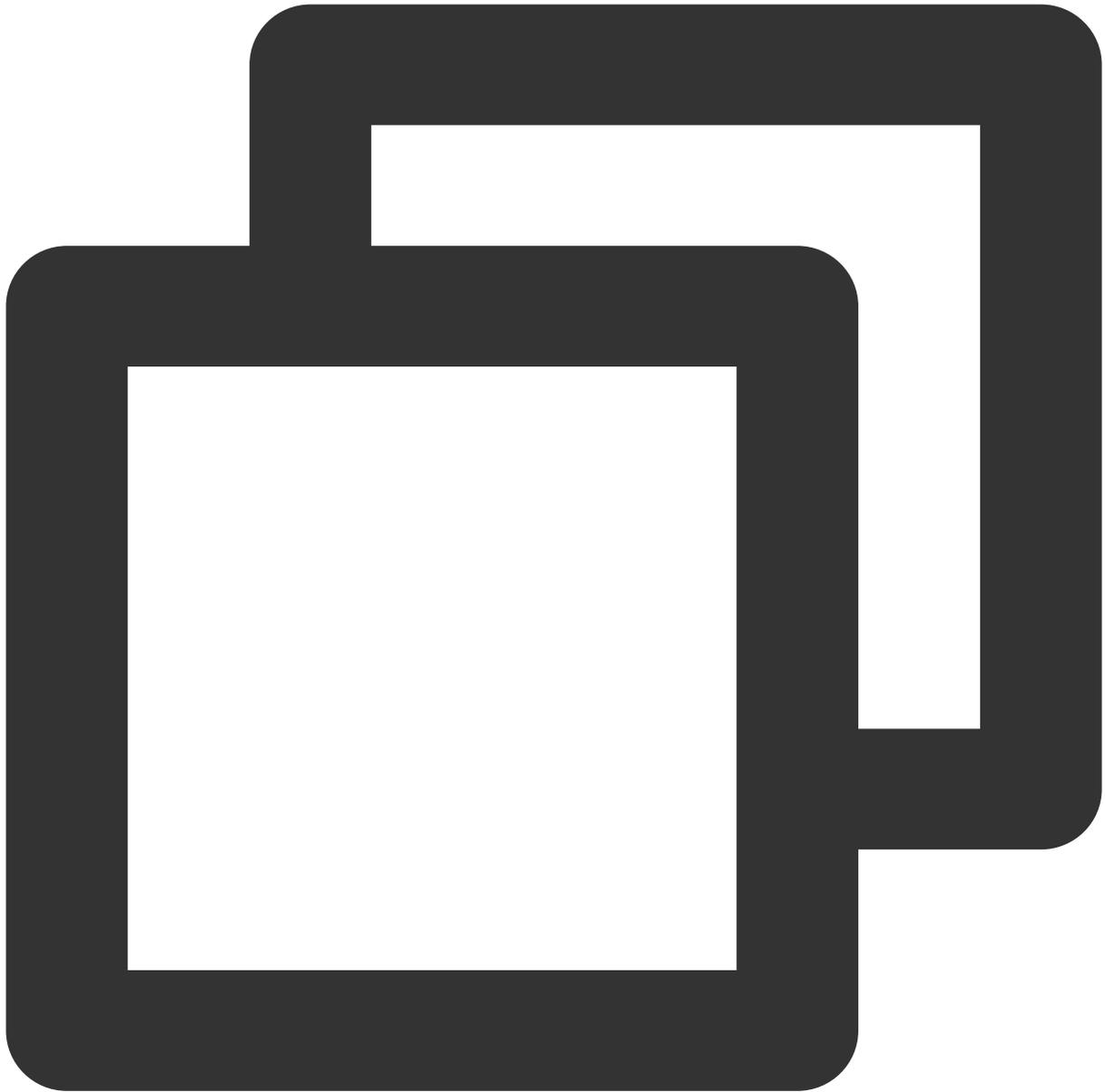
1.4 次のコマンドを実行して、スクリプトファイルの権限を設定します。



```
chmod +x /usr/local/sbin/vpcGateway.sh
echo "/usr/local/sbin/vpcGateway.sh >/tmp/vpcGateway.log 2>&1" >> /etc/rc.local
```

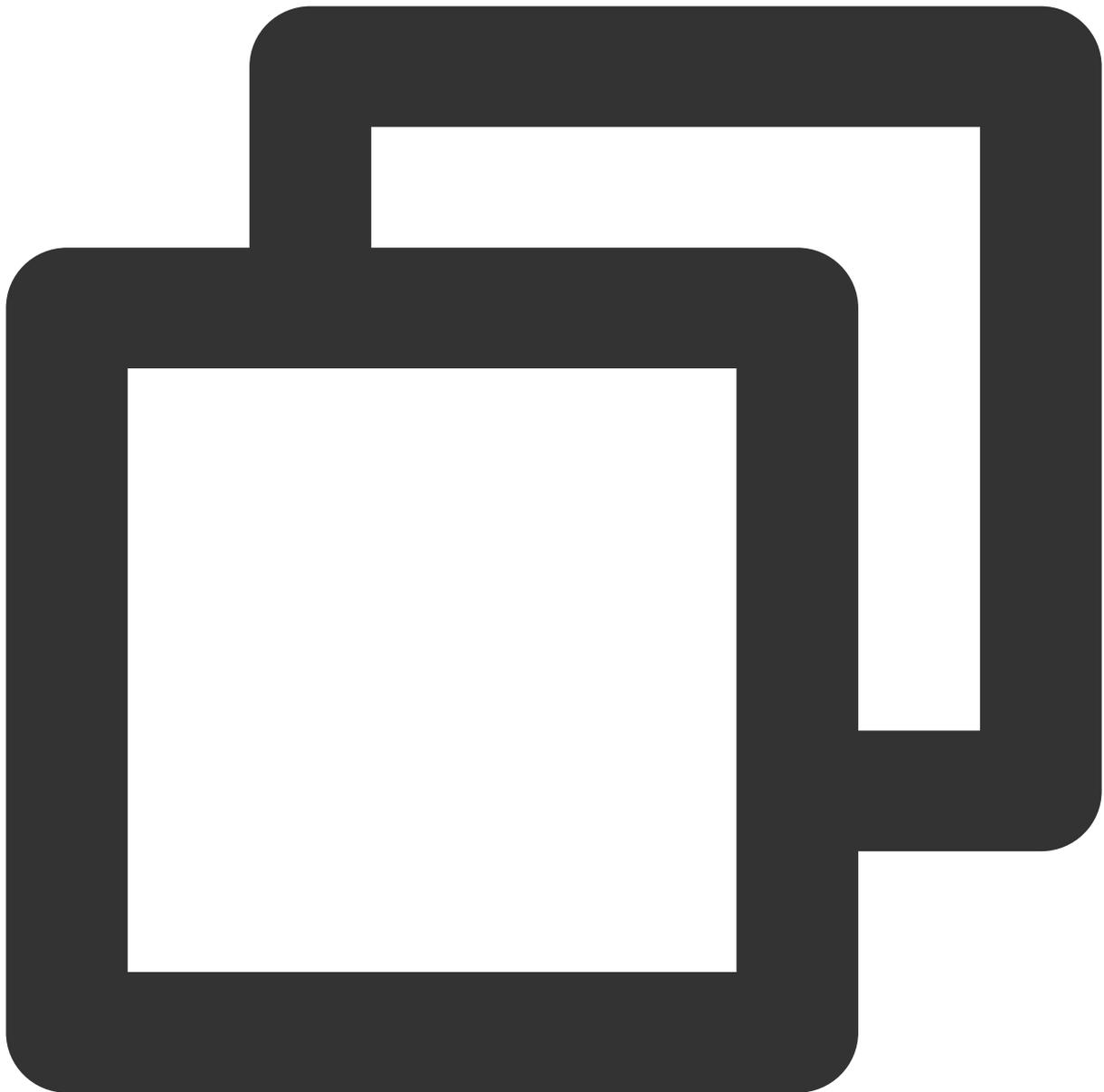
## 2. パブリックゲートウェイのrpsの設定：

2.1 次のコマンドを実行して、`usr/local/sbin` ディレクトリにスクリプト `set_rps.sh` を新規作成します。



```
vim /usr/local/sbin/set_rps.sh
```

2.2 **i**を押して編集モードに切り替え、次のコードをスクリプトに書き込みます。



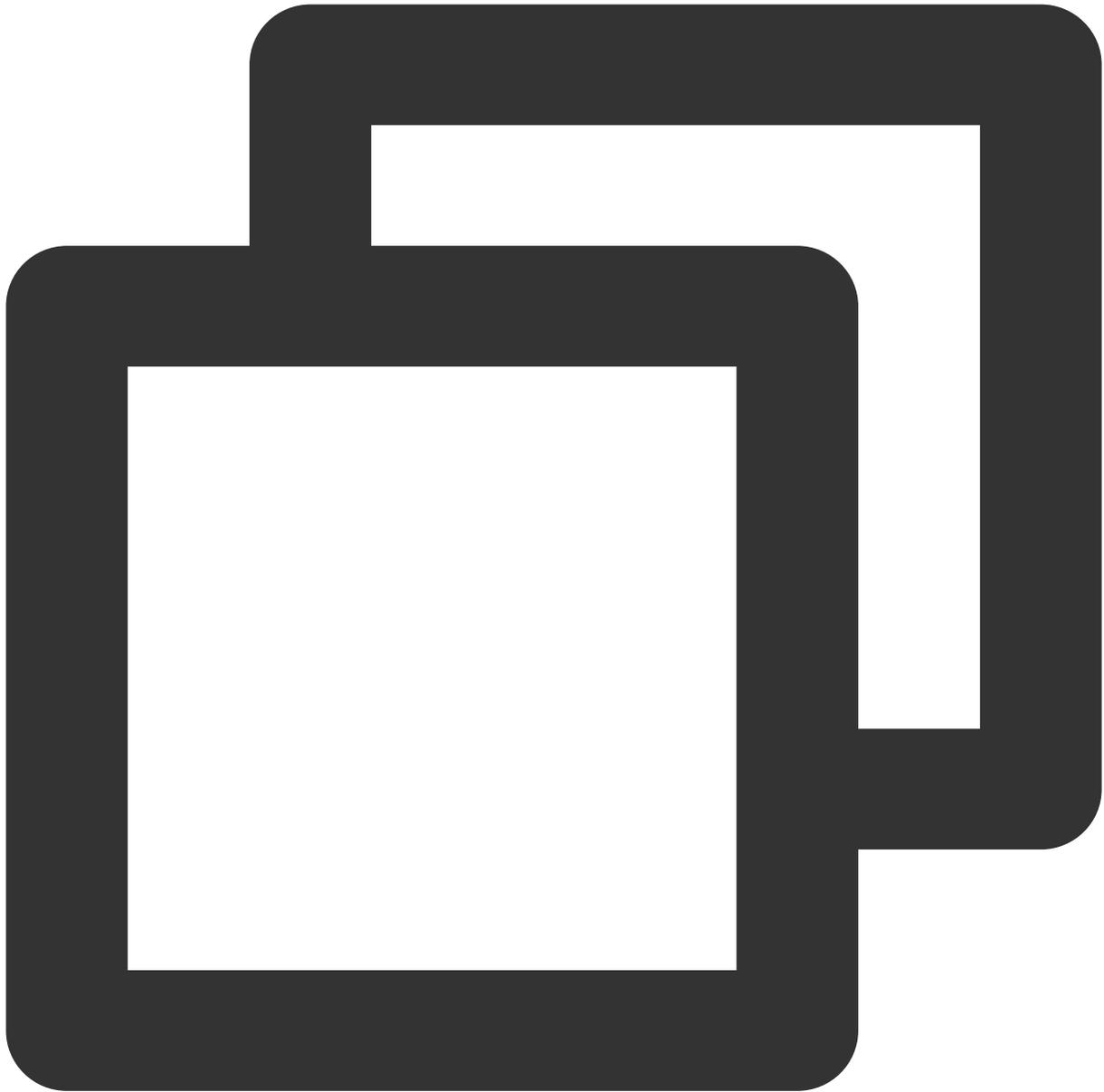
```
# !/bin/bash
echo "-----"
date
mask=0
i=0
total_nic_queues=0
get_all_mask() {
local cpu_nums=$1
if [ $cpu_nums -gt 32 ]; then
mask_tail=""
mask_low32="ffffffff"
```

```
idx=$((cpu_nums / 32))
cpu_reset=$((cpu_nums - idx * 32))
if [ $cpu_reset -eq 0 ]; then
mask=$mask_low32
for ((i = 2; i <= idx; i++)); do
mask="$mask,$mask_low32"
done
else
for ((i = 1; i <= idx; i++)); do
mask_tail="$mask_tail,$mask_low32"
done
mask_head_num=$((2 ** cpu_reset - 1))
mask=$(printf "%x%s" $mask_head_num $mask_tail)
fi
else
mask_num=$((2 ** cpu_nums - 1))
mask=$(printf "%x" $mask_num)
fi
echo $mask
}
set_rps() {
if ! command -v ethtool &>/dev/null; then
source /etc/profile
fi
ethtool=$(which ethtool)
cpu_nums=$(cat /proc/cpuinfo | grep processor | wc -l)
if [ $cpu_nums -eq 0 ]; then
exit 0
fi
mask=$(get_all_mask $cpu_nums)
echo "cpu number:$cpu_nums mask:0x$mask"
ethSet=$(ls -d /sys/class/net/eth*)
for entry in $ethSet; do
eth=$(basename $entry)
nic_queues=$(ls -l /sys/class/net/$eth/queues/ | grep rx- | wc -l)
if (($nic_queues == 0)); then
continue
fi
cat /proc/interrupts | grep "LiquidIO.*rxtx" &>/dev/null
if [ $? -ne 0 ]; then # not smartnic
#multi queue don't set rps
max_combined=$(
$ethtool -l $eth 2>/dev/null | grep -i "combined" | head -n 1 | awk '{print $2}'
)
#if ethtool -l $eth goes wrong.
[[ ! "$max_combined" =~ ^[0-9]+$ ]] && max_combined=1
if [ ${max_combined} -ge ${cpu_nums} ]; then
```

```
echo "$seth has equally nic queue as cpu, don't set rps for it..."
continue
fi
else
echo "$seth is smartnic, set rps for it..."
fi
echo "eth:$seth queues:$nic_queues"
total_nic_queues=$((total_nic_queues + $nic_queues))
i=0
while (($i < $nic_queues)); do
echo $mask >/sys/class/net/$seth/queues/rx-$i/rps_cpus
echo 4096 >/sys/class/net/$seth/queues/rx-$i/rps_flow_cnt
i=$((i + 1))
done
done
flow_entries=$((total_nic_queues * 4096))
echo "total_nic_queues:$total_nic_queues flow_entries:$flow_entries"
echo $flow_entries >/proc/sys/net/core/rps_sock_flow_entries
}
set_rps
```

2.3 **Esc**を押して、**:wq**を入力し、ファイルを保存して戻ります。

2.4 次のコマンドを実行して、スクリプトファイルの権限を設定します。



```
chmod +x /usr/local/sbin/set_rps.sh
echo "/usr/local/sbin/set_rps.sh >/tmp/setRps.log 2>&1" >> /etc/rc.local
chmod +x /etc/rc.d/rc.local
```

3. 上記の設定が完了すると、パブリックゲートウェイCVMをリスタートして設定を有効にし、パブリックネットワークIPがないCVMで、パブリックネットワークに正常にアクセスできるかどうかをテストします。

# EIP直通

最終更新日：2023-05-12 17:42:20

## ユースケース

ユーザーがEIP経由でインターネットにアクセスする場合は、NATモードまたはEIP直通モードを選択することができます。デフォルトはNATモードです。

NATモードでは、EIPはローカルマシンで表示されません。

EIP直通モードでは、EIPはローカルマシンで表示され、設定ごとに毎回手動でEIPアドレスを追加する必要がないため、開発コストを最小限に抑えることができます。

NATモードは、ほとんどのニーズを満たすことができますが、CVMインスタンス内でパブリックIPを確認する場合は、EIP直通モードを使用する必要があります。

## 使用制限

現在、EIP直通モードはベータテスト期間中であり、ホワイトリストに登録されているユーザーのみ利用でき、VPC内のデバイスのみをサポートしています。この機能をご利用になりたい場合は、[チケットを提出](#)してください。

NATゲートウェイは、直通モードが有効になっているEIPとバインドできますが、直通効果はありません。

CVMでは、EIP直通モードとNATゲートウェイを同時に有効にすることはできません。CVMが存在するサブネットに関連付けられたルーティングテーブルが、NATゲートウェイを介してパブリックネットワークにアクセスするルーティングポリシーを設定している場合、CVMのEIPを介して直通機能を実現できません。[NATゲートウェイとEIPの優先順位を調整](#)することで、CVMがEIPを介してパブリックネットワークにアクセスできるようになります。この場合、EIP直通機能を実現できます。

## 操作手順

EIP直通モードを使用するには、コンソールでEIPを有効にし、OS内でIPをENIに追加する必要があります。また、アプリケーションに基づいてOSでルーティングを構成する必要があります。そのため、プライベートネットワークトラフィックがプライベートIPを通過し、パブリックネットワークトラフィックがパブリックIPを通過するように、IPを構成するためのスクリプトを提供します。

### 説明：

具体的なアプリケーションに応じてルーティングを構成してください。

### Linux CVMでEIP直通を構成する

**説明：**

Linuxスクリプトは、CentOS 6以降およびUbuntuをサポートします。

Linuxスクリプトは、プライマリENI (eth0)のみをサポートし、現在、セカンダリENIはサポートしません。

プライマリENIにバインドされているパブリックIPがEIPでない場合は、先にパブリックIPアドレスをEIPに変換する必要があります。詳細については、[パブリックIPからEIPへの変換](#)をご参照ください。

**シナリオ**

Linuxスクリプトは、次のシナリオに適用できます。プライベートIPとパブリックIPの両方がプライマリENI (eth0) にバインドされ、パブリックネットワークアドレスがパブリックIPを介してアクセスされ、プライベートネットワークアドレスがプライベートIPを介してアクセスされます。

**手順1：EIP直通スクリプトをダウンロードする**

EIP直通モードを有効にするプロセスを開始すると、ネットワークの中断を引き起こす可能性があります。そのため、事前にEIP直通用のスクリプトをダウンロードしてCVMにアップロードする必要があります。次のいずれかの方法でスクリプトを取得できます。

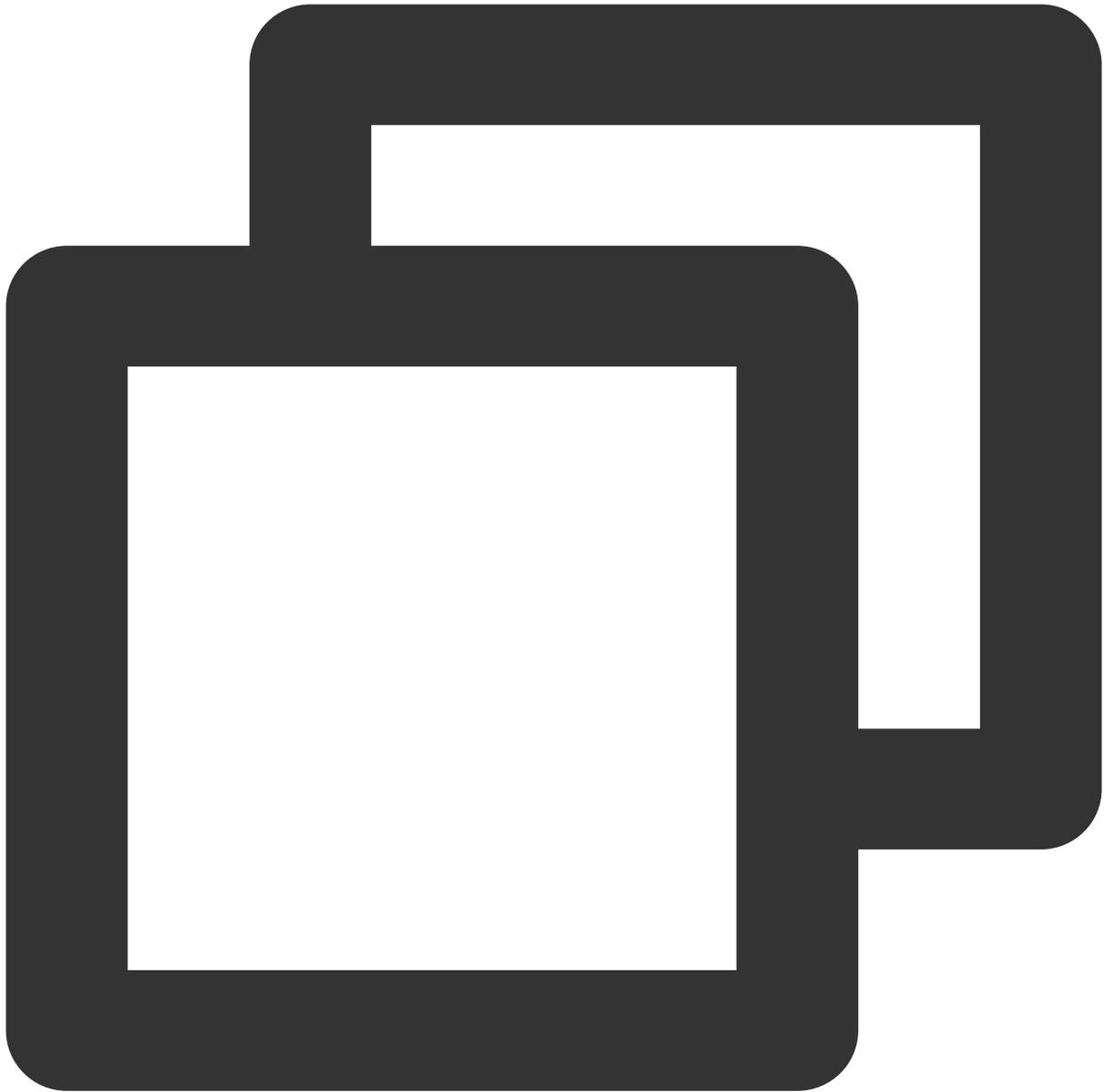
**方式1：EIP直通スクリプトをアップロードする**

1.1 EIP直通の構成スクリプトをダウンロードします。

1.2 Linuxスクリプトをローカルにダウンロードした後、EIP直通が必要なCVMにアップロードします。

**方法2：コマンドを直接使用する**

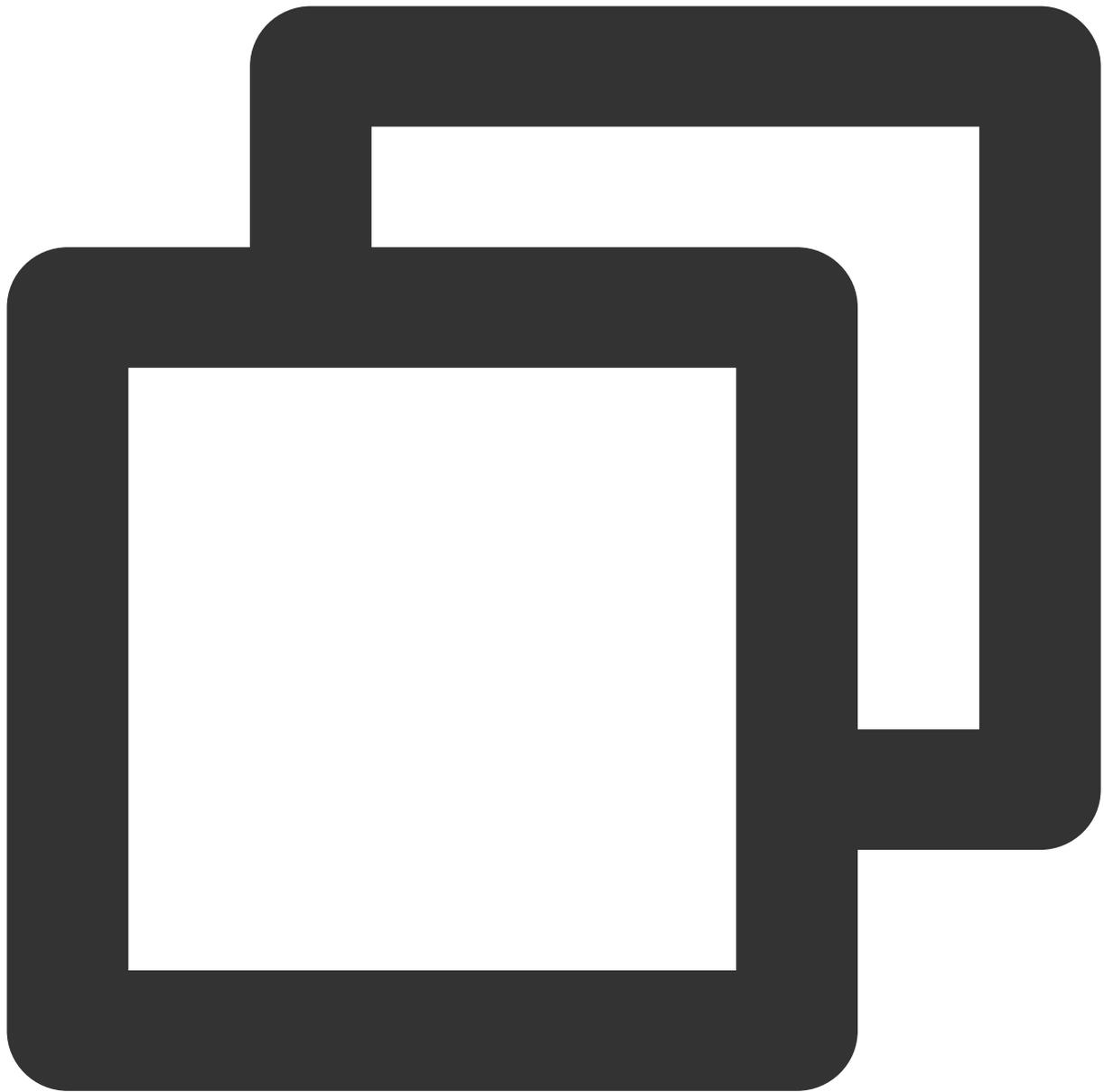
CVMにログインし、CVMで次のコマンドを実行してスクリプトをダウンロードします。



```
wget https://network-data-1255486055.cos.ap-guangzhou.myqcloud.com/eip_direct.sh
```

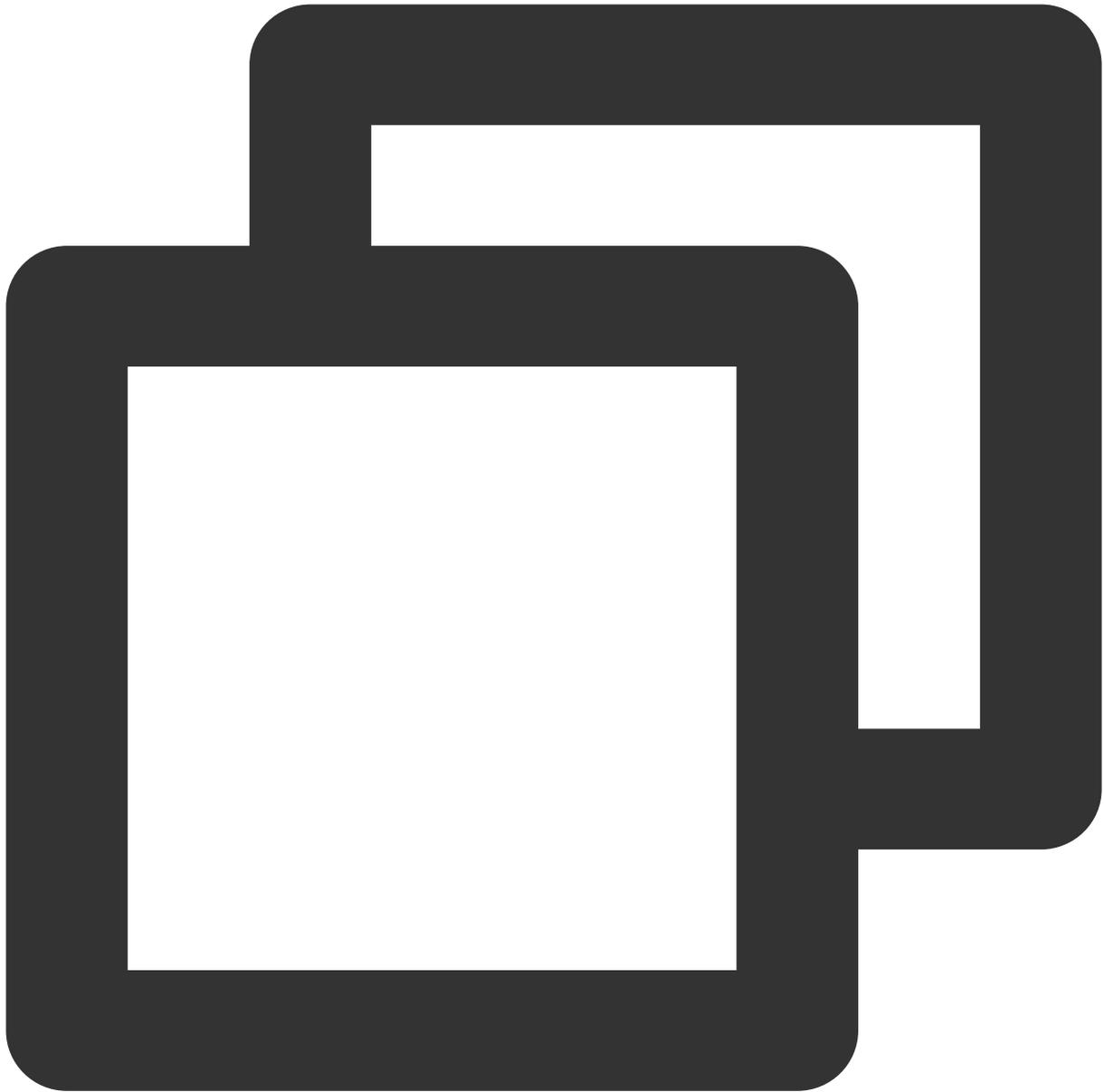
## 手順2：EIP直通スクリプトを実行する

1. EIP直通が必要なCVMにログインします。
2. EIP直通スクリプトを実行します。詳細手順：
  - 2.1 次のコマンドを実行して、実行権限を追加します。



```
chmod +x eip_direct.sh
```

2.2 次のコマンドを実行して、スクリプトを実行します。



```
./eip_direct.sh install XX.XX.XX.XX
```

そのうち、`XX.XX.XX.XX`はEIPアドレスで、オプションです。入力しない場合、`./eip_direct.sh install` を直接実行します。

### 手順3：EIP直通を有効にする

1. [EIPコンソール](#) にログインします。
2. ターゲットEIPを見つけ、右側の操作バーで【More】 > 【Direct connection】 をクリックします。

## Windows CVMでEIP直通を構成する

### 説明：

WindowsでEIP直通を使用するには、プライベートIPとパブリックIPそれぞれ1枚のENIが必要です。パブリックIPをプライマリENIにバインドし、プライベートIPをセカンダリENIにバインドします。

WindowsでEIPを構成するプロセスに、インターネットに接続できない場合があります。この場合、[VNCを介してWindowsインスタンスにログイン](#)することをお勧めします。

プライマリENIにバインドされているパブリックIPがEIPでない場合は、先にパブリックIPアドレスをEIPに変換する必要があります。詳細については、[パブリックIPアドレスのEIPアドレスへの変換](#)をご参照ください。

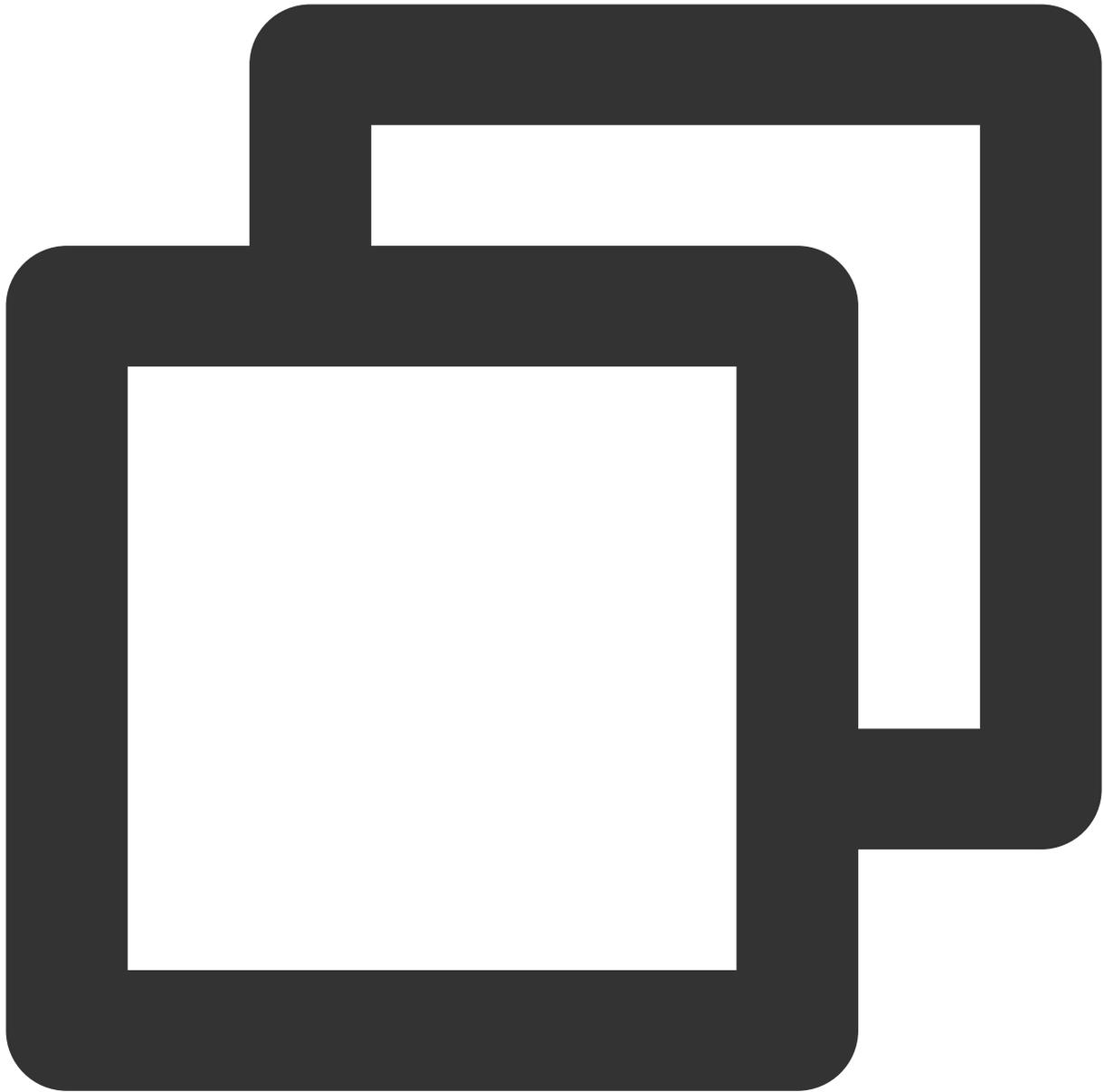
### シナリオ

Windowsスクリプトは、次のシナリオに適用できます。パブリックネットワークトラフィックはプライマリENIを通過し、プライベートネットワークトラフィックはセカンダリENIを通過します。

### 手順1：EIP直通スクリプトをダウンロードする

EIP直通モードを有効にするプロセスを開始すると、ネットワークの中断を引き起こす可能性があります。そのため、事前にEIP直通用のスクリプトをダウンロードしてCVMにアップロードする必要があります。

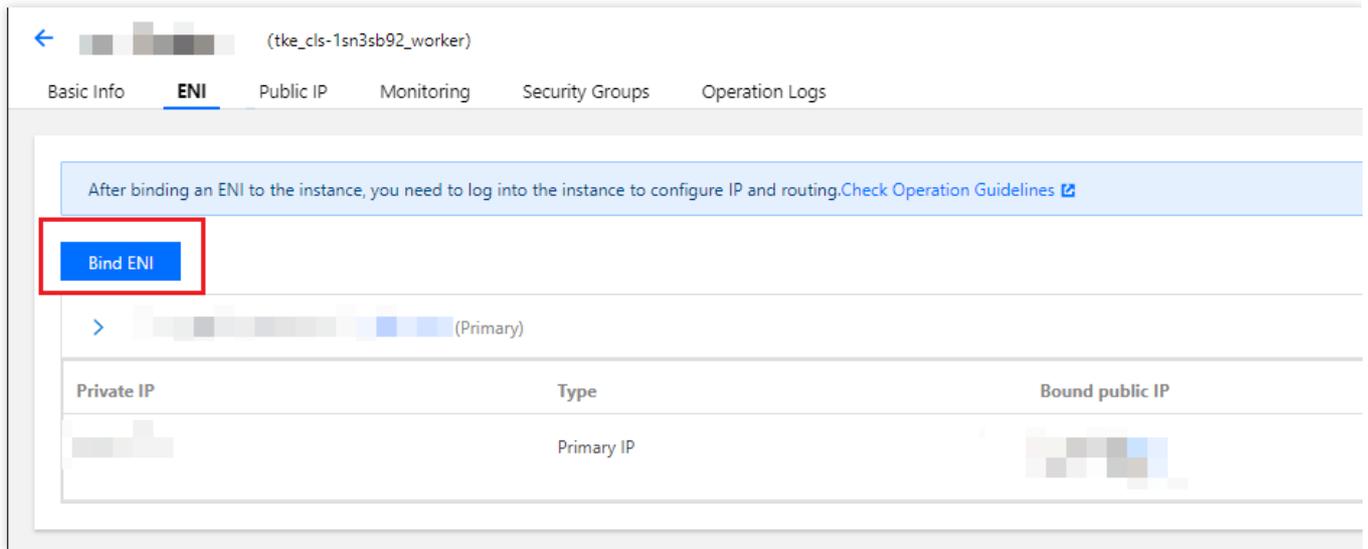
CVMのブラウザで次のリンクを開いて、EIP直通スクリプトのダウンロードを行ってください。



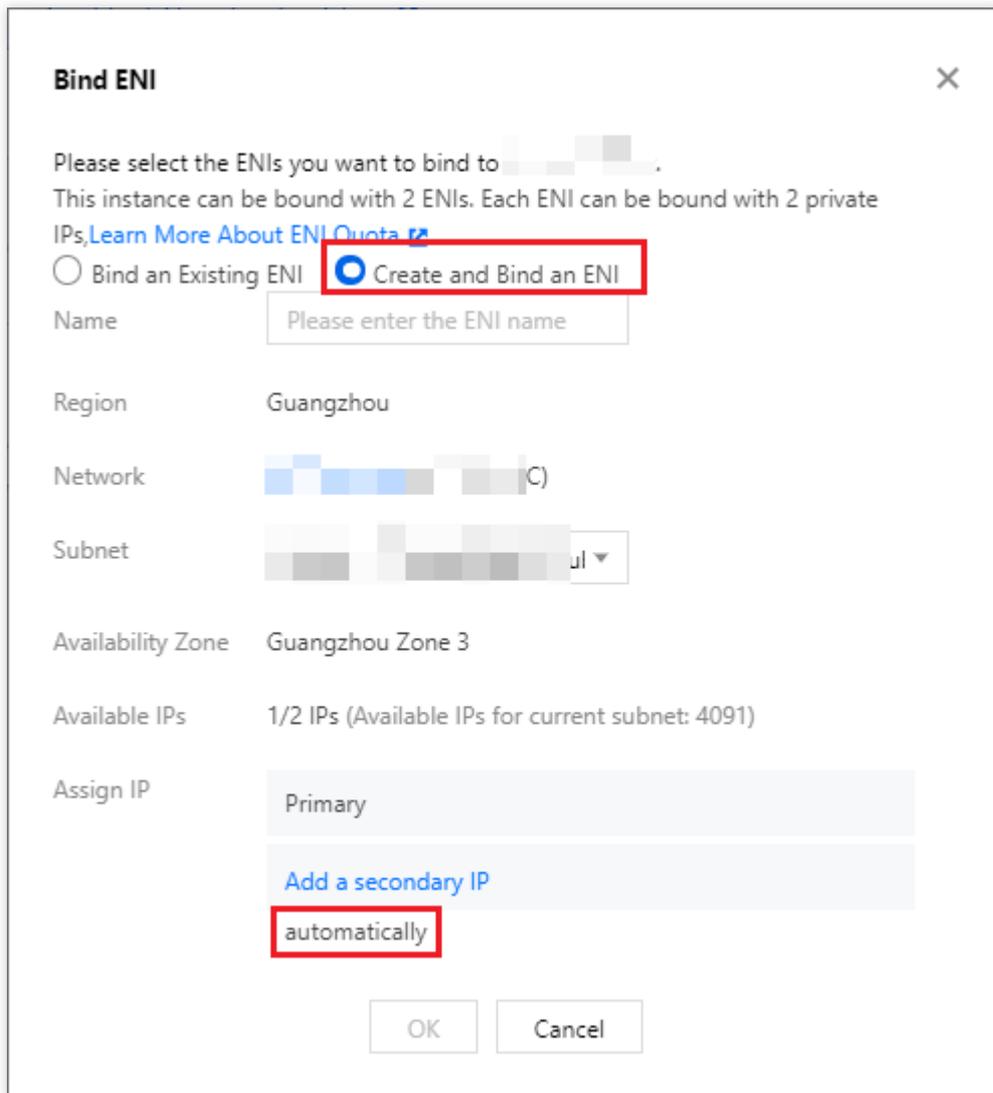
```
https://windows-1254277469.cos.ap-guangzhou.myqcloud.com/eip_windows_direct.bat
```

## 手順2：セカンダリENIを構成する

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で、構成するCVM IDをクリックし、詳細ページに進みます。
3. 【ENI】 タブを選択し、【Bind ENI】 をクリックし、プライマリENIと同じサブネットのENIを新規作成します。



4. ポップアップボックスで、【Create and Bind an ENI】を選択し、関連情報を入力し、【Assign IP】のセクションで【Automatic Assignment】を選択し、【OK】をクリックします。



**Bind ENI** ✕

Please select the ENIs you want to bind to [redacted].  
This instance can be bound with 2 ENIs. Each ENI can be bound with 2 private IPs. [Learn More About ENI Quota](#)

Bind an Existing ENI  **Create and Bind an ENI**

Name

Region Guangzhou

Network [redacted] (C)

Subnet [redacted] ul ▼

Availability Zone Guangzhou Zone 3

Available IPs 1/2 IPs (Available IPs for current subnet: 4091)

Assign IP

Primary

[Add a secondary IP](#)

**automatically**

### 手順3：プライマリENIのEIP直通を構成する

1. [EIPコンソール](#) にログインします。
2. プライマリENIにバインドされているEIPを見つけて、右側の操作バーで【More】 > 【Direct Connection】 をクリックします。

### 手順4：CVMでIPを構成する

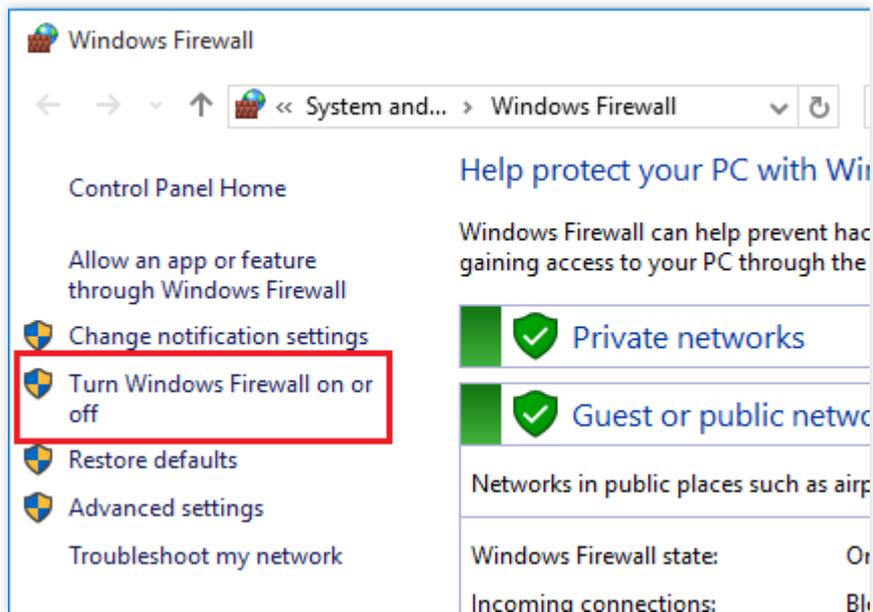
1. CVMにログインします。この操作により、パブリックネットワークが切断される可能性があります。したがって、[VNCを介してWindowsインスタンスにログイン](#)する必要があります。
2. OSのインターフェースで、左下の

  
を選択し、

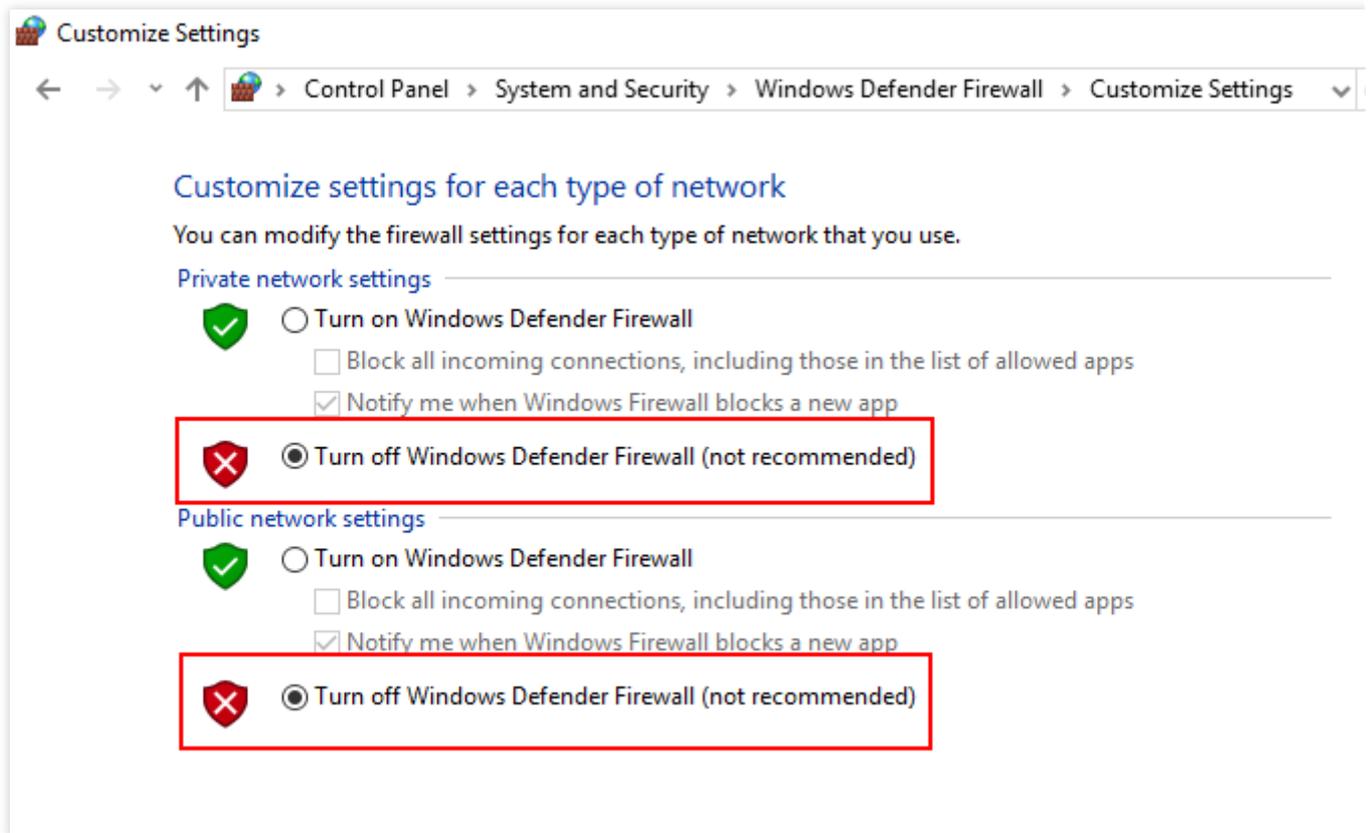


をクリックして、「Windows PowerShell」ウィンドウを開き、`firewall.cpl` を入力してEnterキーを押すと、「Windows ファイアウォール」ページを開きます。

3. 画面左側の項目から **Windows ファイアウォールの有効化または無効化** をクリックします。「設定のカスタマイズ」画面が表示されます。



4. 「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」のいずれか、もしくは両方で **Windows ファイアウォールを無効にする（推奨されません）** を選択し、【OK】をクリックします。



5. [手順1](#)でダウンロードしたスクリプトをダブルクリックして実行し、パブリックIPアドレスを入力して、Enterキーを2回押します。

6. 「Windows PowerShell」ウィンドウで `ipconfig` を入力してEnterキーを押すと、プライマリENI上のIPv4アドレスがパブリックネットワークアドレスに変更されていることが分かります。

#### 説明：

EIP直通が有効になっている場合、プライマリENIに再度プライベートIPを構成しないでください。構成した場合、CVMはパブリックネットワークにアクセスできなくなります。

# セキュリティ

## セキュリティグループ

### セキュリティグループの概要

最終更新日：：2022-06-29 11:06:37

セキュリティグループは、ステートフルパケットをフィルタリングする機能を備えた仮想ファイアウォールです。CVM、Cloud Load Balancer(CLB)、クラウドデータベースなどのインスタンスを設定するネットアクセス制御、インスタンスレベルのインバウンド・アウトバウンドトラフィックの制御のために使用されます。ネットワークセキュリティに対する重要な隔離手段です。

セキュリティグループルールを設定することにより、セキュリティグループ内のインスタンスのインバウンドおよびアウトバウンドトラフィックを許可または拒否できます。

### セキュリティグループの特徴

セキュリティグループは、論理グループであり、同一リージョン内にある同じネットワークセキュリティ分離要件を持つCVM、ENI、TencentDBなどのインスタンスを同じセキュリティグループ内に追加することができます。セキュリティグループにルールが追加されていない場合、デフォルトではすべてのトラフィックが拒否されます。お客様が適切な許可ルールを追加してください。

セキュリティグループはステートフルであり、許可されたインバウンドトラフィックに対して、自動的にアウトバウンドも許可され、逆の場合も同じです。

いつでもセキュリティグループルールを変更できます。新しいルールはすぐに有効になります。

### 使用制限

セキュリティグループの使用制限とクォータについては、[使用制限一覧](#)のセキュリティグループに関連する制限の章をご参照ください。

### セキュリティグループルール

#### 構成要素

セキュリティグループルールの構成要素は、以下のことを含みます：

ソース：ソースデータ（インバウンド）またはターゲットデータ（アウトバウンド）のIPアドレス。

プロトコルタイプとプロトコルポート：プロトコルタイプは、TCP、UDPなどです。

ポリシー：許可または拒否。

## ルールの優先順位

セキュリティグループ内のルールは、優先順位があります。リストの一番上が、最も優先順位が高くなります。下になるほど優先順位は低くなります。

ルールに競合がある場合、優先順位の高いルールがデフォルトで優先されます。

特定のセキュリティグループにバインドされたインスタンスに入る/出るトラフィックがある場合、セキュリティグループルールリストの一番上にあるルールから順に最後までマッチングを実行します。特定のルールのマッチングに成功した（通過許可/通過拒否）場合は、このルール以降のルールのマッチングを停止します。

## 複数のセキュリティグループ

1つのインスタンスを1つまたは複数のセキュリティグループにバインドすることができます。インスタンスを複数のセキュリティグループにバインドする場合は、複数のセキュリティグループが一番上から一番下まで順にマッチングを実行します。いつでもセキュリティグループの優先順位を調整することができます。

## セキュリティグループテンプレート

セキュリティグループを新規作成する際に、Tencent Cloudが提供する2つのセキュリティグループテンプレートのいずれかを選択できます。

すべてのポートを開放：すべてのインバウンドおよびアウトバウンドトラフィックの通過が許可されます。

主要なポートを開放：ポートTCP 22（Linux SSHログインの場合）、ポート80および443（Webサービスの場合）、ポート3389（Windowsリモートログインの場合）、ICMPプロトコル（Pingコマンドの場合）、およびプライベートネットワークをインターネットにオープンします。

### 説明：

提供されたセキュリティグループテンプレートがお客様の要求を満たさない場合は、カスタムセキュリティグループを新規作成することができます。詳細については、[セキュリティグループの作成](#)、[セキュリティグループの適用例](#)をご参照ください。

アプリケーション層(HTTP/HTTPS)に対するセキュリティ保護要件がある場合は、別途、[Tencent Cloud Web Application Firewall \(WAF\)](#) を購入することができます。WAFはアプリケーション層のWebセキュリティ保護を提供し、Web脆弱性攻撃、悪意あるクローラやCC攻撃などの行為を食い止め、サイトやWebアプリケーションのセキュリティを保護します。

## 使用手順

セキュリティグループの使用手順は下図のとおりです：



## セキュリティグループのベストプラクティス

### セキュリティグループの作成

APIを介してCVMを購入する場合、セキュリティグループを指定することをお勧めします。セキュリティグループが指定されていない場合、システムによって自動的に生成されたデフォルトのセキュリティグループが使用されます。またデフォルトのセキュリティグループは削除できません。デフォルトのルールはすべてのIPv4をオープンすることであり、作成された後に状況に応じて変更することができます。

インスタンス保護ポリシーを変更する必要がある場合は、新しいセキュリティグループを作成するのではなく、既存のルールを変更することをお勧めします。

### ルールの管理

ルールを変更したい場合は、まず現在のセキュリティグループをエクスポートしてバックアップすることができます。新たなルールに悪影響がある場合は、以前のセキュリティグループルールをインポートして復元することができます。

複数のセキュリティグループルールが必要となる場合には、[パラメータテンプレート](#)を使用してください。

### セキュリティグループと関連付ける

インスタンスごとに個別のセキュリティグループを設定する必要がなく、同じ保護要件を持つインスタンスを同じセキュリティグループに追加することができます。

過剰な数のセキュリティグループを1つのインスタンスにバインドすることを回避してください。セキュリティグループルール同士の競合により、ネットワークに接続できなくなる場合があります。

# セキュリティグループの作成

最終更新日： : 2023-05-12 18:01:04

## シナリオ

セキュリティグループは、CVMインスタンスの仮想ファイアウォールとして機能し、各CVMインスタンスは少なくとも1つのセキュリティグループに関連付ける必要があります。CVMインスタンスを作成する際に、セキュリティグループを作成したことがない場合には、Tencent Cloudは、デフォルトのセキュリティグループを作成するための「**すべてのポートを開放する**」と「**22、80、443、3389ポートとICMPプロトコルを開放する**」の2つのテンプレートが用意されています。詳細については、[セキュリティグループの概要](#)をご参照ください。

デフォルトのセキュリティグループがニーズを満たさない場合は、本ドキュメント内の説明に従って独自のセキュリティグループを作成することもできます。このドキュメントでは、CVMコンソールでセキュリティグループを作成する方法について説明します。

## 操作手順

1. [CVMコンソール](#) にログインします。
2. 左側のナビゲーションバーで[セキュリティグループ](#)をクリックすると、セキュリティグループ管理ページに進みます。
3. セキュリティグループ管理ページで【リージョン】を選択し、【Create】をクリックします。
4. 「Create security group」ページで、次の設定を完了します。次の図に示すとおり：

**Create a security group** [X]

Template: Open all ports

Name: Open all ports-2020030517310818894

Project: DEFAULT PROJECT

Notes: All ports open for both Internet and private network (HIGH-RISK)

[Display template rule](#)

OK Cancel

テンプレート:ニーズに合った最適なテンプレートを選んでください。一目で分かるように以下で図にまとめました:

テンプレート	説明	備考
すべてのポートを開放	デフォルトではすべてのポートが開いています。セキュリティ上の問題が発生する可能性があります。	-
22、80、443、3389ポートとICMPプロトコルを開放	デフォルトでは22、80、443、3389ポートとICMPプロトコルを開放し、すべてのポートはプライベートネットワークで開いています。	セキュリティグループ内のインスタンスはWebサービスを配備する必要があります。
カスタマイズ	セキュリティグループの作成が完了した後、必要に応じてセキュリティグループルールを自ら追加します。操作の詳細については、 <a href="#">セキュリティグループルールの追加</a> をご参照ください。	-

名前:セキュリティグループの名前をカスタマイズします。

プロジェクト:デフォルトで「デフォルトプロジェクト」が選択されていますが、後で管理しやすいようにその他のプロジェクトを指定することができます。

備考:カスタム。セキュリティグループの簡単な説明。

5. **【OK】** をクリックして、セキュリティグループの作成を完了します。

セキュリティグループのテンプレートとして「Custom」を選択した場合は、セキュリティグループを作成した

後、【Add rules now】をクリックして [セキュリティグループルールを追加](#) できます。

# セキュリティグループルールの追加

最終更新日：：2020-11-02 11:38:23

## 概要

セキュリティグループは、パブリックネットワークまたはプライベートネットワークからのアクセス要求を受け入れるかどうかを管理するために使用されます。セキュリティ上の理由から、ほとんどのインバウンドトラフィックはデフォルトで拒否されます。セキュリティグループの作成際には「すべてのポートを開放」テンプレートまたは「22、80、443、3389ポートおよびICMPプロトコルを開放」テンプレートを選択した場合、選択したテンプレートのタイプに応じて、システムが一部の通信ポートにセキュリティグループのルールを自動的に追加します。詳細については、[セキュリティグループの概要](#)をご参照ください。

このドキュメントでは、セキュリティグループルールを追加して、セキュリティグループ内のCVMインスタンスからパブリックネットワークまたはプライベートネットワークへのアクセスを許可または拒否する方法について説明します。

## 注意事項

セキュリティグループルールは、IPv4およびIPv6ルールをサポートします。  
**すべてのポートを開放し**、IPv4とIPv6の両方のトラフィックが許可されます。

## 前提条件

セキュリティグループが作成されました。具体的な操作については、[セキュリティグループの作成](#)をご参照ください。

CVMインスタンスが許可または拒否する必要があるパブリックネットワークまたはプライベートネットワークへのアクセスはすでに了解します。セキュリティグループのルール設定に関する適用例の詳細については、[セキュリティグループの適用例](#)をご参照ください。

## 操作手順

1. [CVMコンソール](#)にログインします。
2. 左側のナビゲーションバーで、[セキュリティグループ](#)をクリックすると、セキュリティグループ管理ページに進みます。

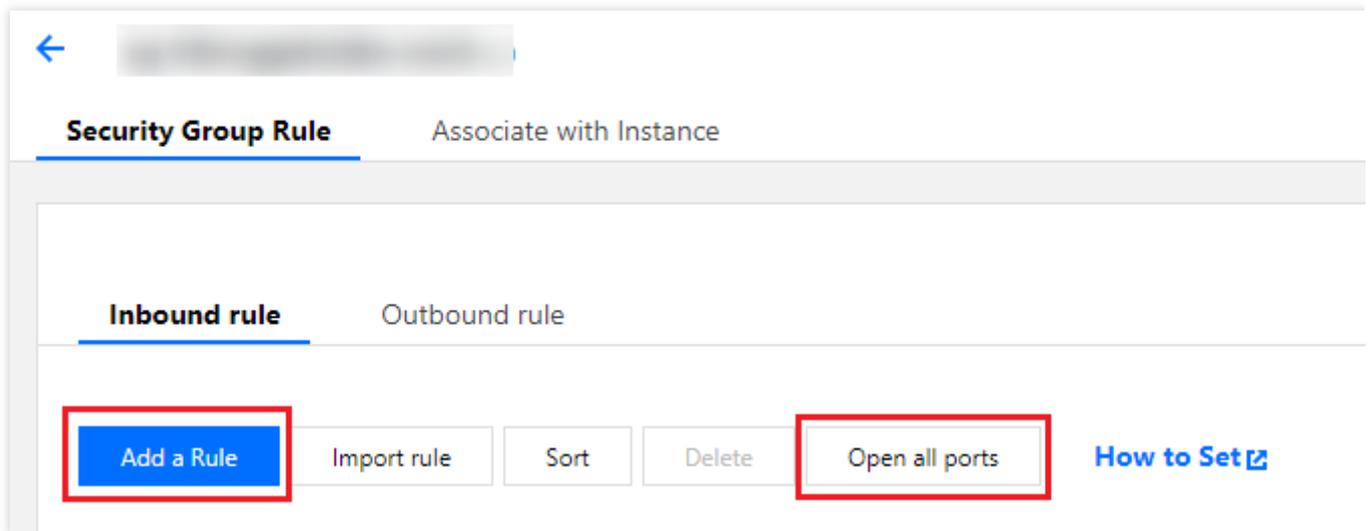
3. セキュリティグループ管理ページで、**リージョン**を選択し、ルールを設定するセキュリティグループを見つけます。

4. 「操作」列の「Modify Rules」をクリックします。

5.

セキュリティグループルールページで

、「Inbound rules」をクリックし、実際のニーズに応じて次のいずれかの方法を選択してルールを追加します。<



#### 説明：

次の操作は方式2：「ルールの追加」を例にします。

方式1：すべてのポートを開放します。この方法は、ICMPプロトコルルールを設定せずに、すべてのトラフィックがポート20、21、22、80、443、および3389とICMPプロトコルを通過する場合に最適です。

方式2：ルールを追加します。この方法は、上記以外の複数のプロトコルとポートを使用する必要がある場合に最適です。

6. ポップアップウィンドウで、ルールを設定します。

### Add Inbound rule

Type	Source <span style="font-size: small;"> ⓘ</span>	Protocol port <span style="font-size: small;"> ⓘ</span>	Policy	Notes
Custom ▼	IP or IP ranges, etc. (IPv4 / IPv6)	For example, UDP:53, TCP:80,443 or TCP:8	Allow ▼	
+ New Line				

Completed
Cancel

ルールの追加に関する主なパラメータは下記の通りです。

**タイプ**：デフォルトでは「カスタム」が選択されますが、「Windowsログイン」テンプレート、「Linuxログイン」テンプレート、「Ping」テンプレート、「HTTP(80)」テンプレートおよび「HTTPS(443)」テンプレートなどの他のシステムルールテンプレートを選択することもできます。

**ソース**：トラフィックのソース（インバウンドルール）またはターゲット（アウトバウンドルール）としては、下記選択肢のいずれかを指定してください。

指定のソース/ターゲット	説明
単一のIPv4アドレスまたはIPv4アドレス範囲	CIDR表記法を使用します（例： <code>203.0.113.0</code> 、 <code>203.0.113.0/24</code> または <code>0.0.0.0/0</code> 。そのうち、 <code>0.0.0.0/0</code> はすべてのIPv4アドレスにマッチングしていることを表します）。
単一のIPv6アドレスまたはIPv6アドレス範囲	CIDR表記法を使用します （例： <code>FF05::B5</code> 、 <code>FF05:B5::/60</code> 、 <code>::/0</code> または <code>0::0/0</code> 。そのうち、 <code>::/0</code> または <code>0::0/0</code> はすべてのIPv6アドレスにマッチングしていることを表します）。
セキュリティグループIDの引用。以下のセキュリティグループのIDを引用できます： 現在のセキュリティグループ その他のセキュリティグループ	現在のセキュリティグループは、CVMに関連付けられたセキュリティグループIDを表します。 その他のセキュリティグループは、同一エリア内の同一プロジェクト下の別のセキュリティグループIDを表します。 <b>説明</b> ： セキュリティグループのID引用は拡張機能であり、オプションとして利用することができます。引用されるセキュリティグループのルールは現在のセキュリティグループに追加されません。

	セキュリティグループルールを設定するとき、ソース/ターゲットにセキュリティグループIDが入力されると、パブリックIPアドレスを除き、このセキュリティグループIDに関連付けられているCVMインスタンス、ENIのプライベートIPアドレスをソース/ターゲットとすることを示します。
パラメーターテンプレート内のIPアドレスオブジェクトまたはIPアドレスグループオブジェクトを引用します	-

**プロトコルポート**：プロトコルタイプとポート範囲を記入します。プロトコルタイプはTCP、UDP、ICMP、ICMPv6およびGREをサポートします。また [パラメータテンプレート](#) のプロトコル/ポートまたはプロトコル/ポートグループを引用してもよい。プロトコルポートは次の形式をサポートします。

TCP:80 のような単一ポート。

TCP:80,443 のような複数のポート。

TCP:3306-20000 のようなポート範囲。

TCP:ALL のようなすべてのポート。

**ポリシー**：デフォルトで「許可」が選択されます。

許可：このポートへのトラフィックが許可されます。

拒否：データパケットを直接破棄し、いかなる応答情報も戻しません。

**備考**：ユーザー設定が可能で、今後管理のため、ルールを簡単に記述します。

7.

【Complete】をクリックし、セキュリティグループのインバウンドルールの追加を完了します。

8. セキュリティグループルールページで、「Outbound rule」をクリックし、[ステップ5-ステップ7](#)を参照して、セキュリティグループのアウトバウンドルールの追加を完了します。

# インスタンスをセキュリティグループに関連付ける

最終更新日： : 2023-05-15 10:25:25

## 説明：

セキュリティグループは、CVM、ENI、TencentDB for MySQL、およびCLBに関連付けることができます。このドキュメントでは、セキュリティグループをCVMインスタンスに関連付ける方法について説明します。

## 概要

セキュリティグループは、単一または複数のCVMインスタンスのネットワークアクセス制御を設定するために使用され、ネットワークを守る非常に高度なセキュリティソリューションです。必要に応じて、CVMインスタンスを1つ以上のセキュリティグループに関連付けることができます。以下では、コンソールでCVMインスタンスをセキュリティグループに関連付ける方法について説明します。

## 前提条件

CVMインスタンスが作成されました。

## 操作手順

1. [CVMコンソール](#) にログインします。
2. 左側のナビゲーションバーで、[セキュリティグループ](#) をクリックして、セキュリティグループ管理ページに進みます。
3. セキュリティグループ管理ページで、[地域](#) を選択し、ルールの設定を必要とするセキュリティグループを見つけます。
4. ルールの設定を必要とするセキュリティグループの行では、操作列の **Manage Instances** をクリックして、関連付けるインスタンスページに進みます。
5. **Add Instance** をクリックします。
6. 「Add Instance」ダイアログボックスで関連付けるインスタンスを選択し、**OK** をクリックします。

## 説明：

複数のセキュリティグループをインスタンスに関連付けると、関連付けた順序で実行されます。セキュリティグループの優先順位を調整するには、[セキュリティグループの優先順位の調整](#) をご参照ください。

## 後続の操作

特定の地域で利用可能なすべてのセキュリティグループを一覧表示するには、セキュリティグループのリストをクエリできます。

操作の詳細については、[セキュリティグループの表示](#)をご参照ください。

CVMインスタンスとセキュリティグループの関連付けを解除したい場合は、CVMインスタンスをセキュリティグループから削除できます。

操作の詳細については、[セキュリティグループから削除](#)をご参照ください。

セキュリティグループが不要になった場合は、削除できます。セキュリティグループが削除されると、セキュリティグループ内のすべてのルールが同時に削除されます。

操作の詳細については、[セキュリティグループの削除](#)をご参照ください。

# セキュリティグループ

## セキュリティグループのコピー

最終更新日： : 2023-05-15 16:47:23

### シナリオ

次の場合には、セキュリティグループをコピーする必要があります。

リージョンAにセキュリティグループsg-Aを作成し、リージョンBのインスタンスに対してsg-Aと同じルールを使用する必要があるとします。新しいセキュリティグループを最初から作成する代わりに、セキュリティグループsg-AをリージョンBへ直接コピーすることができます。

サービスに新しいセキュリティグループルールを実行する必要がある場合は、バックアップとして古いセキュリティグループルールをコピーすることができます。

### 注意事項

デフォルトでは、セキュリティグループをコピーすると、元のセキュリティグループと同じインバウンドルールとアウトバウンドルールでコピーが作成され、このセキュリティグループに関連付けられたインスタンスはコピーされません。

複数のプロジェクト、リージョンにわたってセキュリティグループをコピーできます。

### 操作手順

1. [CVMコンソール](#) にログインします。
2. 左側のナビゲーションバーで、[セキュリティグループ](#) をクリックして、セキュリティグループ管理ページに進みます。
3. セキュリティグループ管理ページで、[リージョン](#) を選択し、コピーするセキュリティグループを見つけます。
4. ターゲットセキュリティグループの横にある **【More】** > **【Clone】** をクリックします。
5. 「Clone security group」画面が表示されます。この画面で **【Target project】** と **【Target region】** を選択し、新しいセキュリティグループの **【New name】** を入力します。 **【OK】** をクリックします。

# セキュリティグループの優先順位の調整

最終更新日：：2023-04-10 18:36:38

## 概要

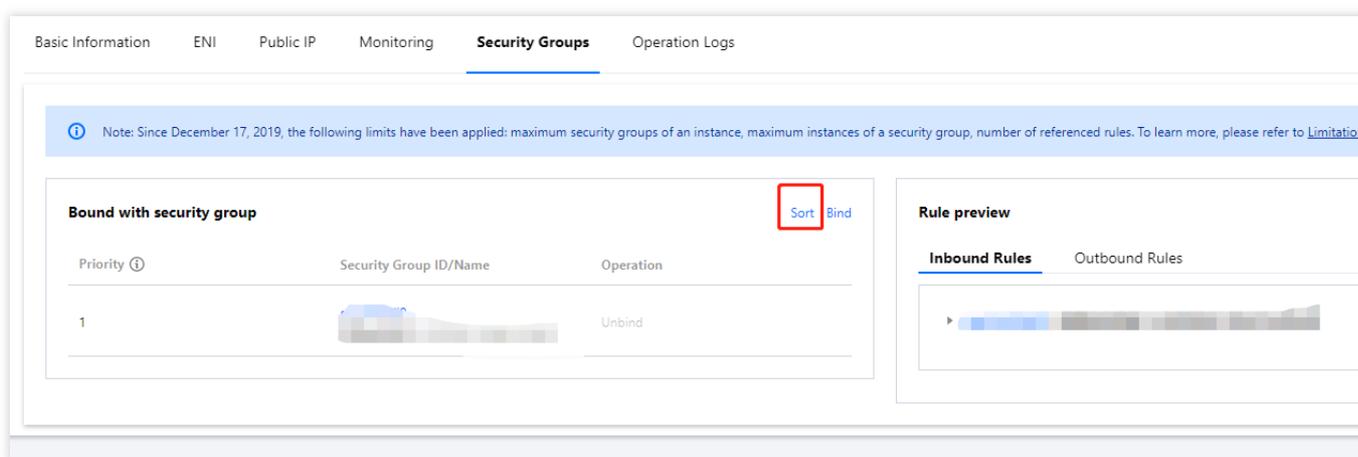
1つのCVMインスタンスは、複数のセキュリティグループに関連付けることができます。複数のセキュリティグループをインスタンスに関連付けると、これらのセキュリティグループは優先順位に基づいて実行されます。以下の操作によりセキュリティグループの優先順位を調整することができます。

## 前提条件

CVMインスタンスは、2つ以上のセキュリティグループに関連付けられています。

## 操作手順

1. [CVMコンソール](#) にログインします。
2. インスタンス管理画面で、CVMインスタンスIDをクリックして詳細ページに移動します。
3. [セキュリティグループ](#) タブをクリックして、セキュリティグループ管理ページに入ります。
4. 「Bound security groups」 モジュールで **Sort** をクリックします。



5. 次のアイコンをクリックし、上下にドラッグし、セキュリティグループの優先順位を調整します。リストでの順位が高いほどセキュリティグループの優先順位が高くなります。

 Note: Since December 17, 2019, the following limits have been applied: maximum security groups of an instance, m

### Bound with security group

Security Group ID/Name



Security Group ID/Name

Save

Cancel

6. 調整が完了したら、**Save**をクリックします。

# セキュリティグループルールの管理

## セキュリティグループルールの表示

最終更新日：：2023-05-10 15:16:14

### シナリオ

セキュリティグループルールを追加した後、コンソールでその詳細を表示できます。

### 前提条件

セキュリティグループを作成し、少なくとも1つのルールを追加しました。

セキュリティグループの作成とセキュリティグループルールの追加について、[セキュリティグループの作成](#)と[セキュリティグループルールの追加](#)をご参照ください。

### 操作手順

1. [CVMコンソール](#) にログインします。
2. 左側のナビゲーションバーで、[セキュリティグループ](#) をクリックして、セキュリティグループ管理ページに進みます。
3. セキュリティグループ管理ページで、[リージョン](#) を選択して、ルールを表示するセキュリティグループを見つけます。
4. ルールを表示するセキュリティグループIDをクリックして、セキュリティグループルールページに進みます。
5. セキュリティグループルールページで、[インバウンド/アウトバウンドルールタブ](#) をクリックして、すべてのインバウンドルールとアウトバウンドルールを表示できます。

# セキュリティグループルールの変更

最終更新日：：2023-05-12 17:28:34

## シナリオ

不適切なセキュリティグループルールを使っていた場合、セキュリティに深刻なリスクをもたらす可能性があります。たとえば、セキュリティグループルールは特定のポートへのアクセスを制限しません。セキュリティグループ内の不適切なルールを変更することで、CVMインスタンスのネットワークセキュリティを確保できます。このドキュメントでは、セキュリティグループルールを変更する方法について説明します。

## 前提条件

セキュリティグループが作成され、ルールにこのセキュリティグループが追加されました。

セキュリティグループの作成とセキュリティグループルールの追加について、[セキュリティグループの作成](#)と[セキュリティグループルールの追加](#)をご参照ください。

## 操作手順

1. [CVMコンソール](#) にログインします。
2. 左側のナビゲーションバーで、[セキュリティグループ](#)をクリックして、セキュリティグループ管理ページに進みます。
3. セキュリティグループ管理ページで、[リージョン](#)を選択して、ルールを変更するセキュリティグループを見つけます。
4. ルールを変更するセキュリティグループの行で、「操作」列の【Modify rule】をクリックして、セキュリティグループルールページに進みます。
5. セキュリティグループルールの方向（インバウンド/アウトバウンド）に応じて、【Inbound rules】または【Outbound rules】タブをクリックします。
6. 変更するルールを見つけ、「操作」列の【Edit】ボタンをクリックして、既存のルールを変更します。

### 説明：

セキュリティグループルールを変更した後、CVMインスタンスを再起動する必要はありません。

# セキュリティグループルールの削除

最終更新日：：2023-05-15 10:55:20

## シナリオ

セキュリティグループルールが不要になった場合は、削除できます。

## 前提条件

セキュリティグループが作成され、ルールにこのセキュリティグループが追加されました。

セキュリティグループの作成とセキュリティグループルールの追加について、[セキュリティグループの作成](#) と [セキュリティグループルールの追加](#) をご参照ください。

CVMインスタンスが、パブリックネットワークまたはプライベートネットワークからのアクセスを許可または禁止する必要がないことを確認しました。

## 操作手順

1. [CVMコンソール](#) にログインします。
2. 左側のナビゲーションバーで、[セキュリティグループ](#) をクリックして、セキュリティグループ管理ページに進みます。
3. セキュリティグループ管理ページで、[リージョン](#) を選択して、ルールを削除するセキュリティグループを見つけます。
4. ルールを削除するセキュリティグループの行で、「操作」列の **Modify rule** をクリックして、セキュリティグループルールページに進みます。
5. セキュリティグループルールの方向（インバウンド/アウトバウンド）に応じて、**Inbound rules** または **Outbound rules** タブをクリックします。
6. 削除するセキュリティグループルールを見つけて、操作列の **Delete** をクリックします。
7. その後表示されるダイアログで、**OK** をクリックします。

# セキュリティグループルールのエクスポート

最終更新日：2023-06-30 15:28:14

## シナリオ

セキュリティグループルールをエクスポートし、バックアップ用にローカルに保存できます。

## 操作手順

1. [CVMコンソール](#) にログインします。
2. 左側のナビゲーションバーで、[セキュリティグループ](#) をクリックして、セキュリティグループ管理ページに進みます。

**Virtual Private Cloud**

- Network Topology Map
- Virtual Private Cloud
- Subnet
- Route Tables
- IP and Interface
- Shared Bandwidth Pack
- NAT Gateway
- Peering Connections
- VPN Connection
- Private Link
- Direct Connect Gateway
- Cloud Connect Network
- Security**
  - Security Group**
  - Network ACL
  - Parameter Template

**Security groups** Guangzhou 4 All projects

Create Delete Edit tags

<input type="checkbox"/>	ID/Name	Associated inst...	Remark
<input type="checkbox"/>	[blurred]	2	default security grou...
<input type="checkbox"/>	[blurred]	3	[blurred]
<input type="checkbox"/>	[blurred]	4	Custom Template
<input type="checkbox"/>	[blurred]	9	System created secu...

Total items: 4

3. セキュリティグループ管理ページで、リージョンを選択して、ルールをエクスポートするセキュリティグループを見つけます。

The screenshot shows the Tencent Cloud console interface. On the left is a dark sidebar with a navigation menu. The 'Security' section is expanded, and 'Security Group' is highlighted with a red box. The main content area is titled 'Security groups' and shows a dropdown menu for 'Guangzhou 4' (also highlighted with a red box) and a project selector set to 'All projects'. Below the dropdown is a table of security groups with columns for ID/Name and checkboxes. A 'Total items: 4' label is visible at the bottom of the table. The dropdown menu is open, showing a 'Recently Visited' section with a grid of region options. The regions listed include Jakarta 4, Tokyo 7, Silicon Valley 5, South China, Hong Kong/Macao/Taiwan (China), Southeast, Guangzhou 4, Hong Kong, China 6, Jakarta 4, Qingyuan 6, Taiwan, China 2, Western U, East China, North America, Silicon Vall, Shanghai 21, Toronto 2, Jinan 1, Southwest, Hangzhou, North China, Chengdu 6, Nanjing 20, Beijing 34, Chongqing, Fuzhou 1, Shijiazhuang, Hefei, Europe, Southeast Asia, Frankfurt 1, Singapore 12, Northeast, and Bangkok 4.

4. ルールをエクスポートするセキュリティグループID/名をクリックして、セキュリティグループルールページに進みます。

5. セキュリティグループルールページで、**Inbound rules/Outbound rules**タブをクリックします。

6. 画面の右上にある

 をクリックし、セキュリティグループルールをファイルにエクスポートし、ローカルデバイスに保存します。

**Inbound rules**    Outbound rules

[Add rule](#)   [Import rule](#)   [Sort](#)   [Edit all](#)   [Delete](#)   [Open all common ports](#)   [How to Set](#)    [Search](#)

<input type="checkbox"/>	Source  	Protocol+Port 	Policy	Remark	Mo
<input type="checkbox"/>	[blurred]	[blurred]	Allow		202
<input type="checkbox"/>	[blurred]	[blurred]	Allow		202
<input type="checkbox"/>	[blurred]	[blurred]	Allow		202
<input type="checkbox"/>	[blurred]	[blurred]	Allow		202
<input type="checkbox"/>	[blurred]	[blurred]	Allow		202
<input type="checkbox"/>	[blurred]	[blurred]	Allow		202
<input type="checkbox"/>	[blurred]	[blurred]	Allow		202

Total items: 6

# セキュリティグループの応用例

最終更新日：2022-12-26 10:41:53

セキュリティグループの設定は、Cloud Virtual Machines (CVM) へのアクセスを管理するために使用され、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設定することにより、お客様のCVMにアクセスできるかまたは他のネットワークリソースにアクセスできるかどうかを設定できます。

デフォルトでは、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は次のとおりです。

**データセキュリティのため、セキュリティグループのインバウンドルールは拒否ポリシーであり、外部ネットワークへのリモートアクセスを禁止します。** CVMに外部からアクセスする必要がある場合は、対応するポートのインバウンドルールを許可にする必要があります。

セキュリティグループのアウトバウンドルールは、お客様のCVMが外部ネットワークリソースにアクセスできるかどうかを設定するために用います。「すべてのポートを開放する」または「ポート22、80、443、3389を開放し、ICMPプロトコルを許可する」を選択した場合、セキュリティグループのアウトバウンドルールはすべてのポートを開放します。カスタムセキュリティグループルールを選択した場合、アウトバウンドルールはデフォルトで「すべて拒否」となるので、対応するポートのアウトバウンドルールを許可にして、外部ネットワークリソースにアクセスできるようにする必要があります。

## 一般的なユースケース

このドキュメントでは、セキュリティグループのいくつかの一般的なユースケースを紹介します。以下のケースが要件を満たしている場合は、対応するユースケースの推奨設定に従ってセキュリティグループを直接設定できます。

### シナリオ 1：SSH経由でLinux CVMにリモート接続する

**事例：**Linux CVMを作成し、SSH経由でCVMにリモート接続したい場合。

**解決策：**[セキュリティグループルールの追加](#)を行うときに、「タイプ」で「Linuxログイン」を選択し、ソースがWebShellプロキシIPであるプロトコルポート22を開放し、LinuxSSHログインを許可します。

また、実際のニーズに応じて、すべてのIPを解放するか、またはIP（IPセグメント）を指定して、SSH経由でCVMにリモート接続できるIPソースを設定することもできます。

方向	タイプ	ソース	プロトコル ポート	ポリシー
インバウンド 方向	Linux ログイン	すべてのIP：0.0.0.0/0 WebShellプロキシIP：詳細については、 <a href="#">OrcatermプロキシIPアドレスの置き換えに関する通知</a> をご参照ください IPの指定：指定するIPまたはIPセグメントを入力します	TCP:22	許可

## シナリオ2：RDP経由でWindows CVMにリモート接続する

**事例：**Windows CVMを作成し、RDP経由でCVMにリモート接続したい場合。

**解決策：**セキュリティグループルールの追加を行うときに、「タイプ」で「Windowsログイン」を選択し、ソースがWebRDPプロキシIPのポート3389を開放し、Windowsリモートログインを許可します。

また、実際のニーズに応じて、すべてのIPを解放するか、またはIP（IPセグメント）を指定して、RDP経由でCVMにリモート接続できるIPソースを設定することもできます。

方向	タイプ	ソース	プロトコルポート	ポリシー
インバウンド方向	Windowsログイン	すべてのIP：0.0.0.0/0 WebRDPプロキシIP： 81.69.102.0/24 106.55.203.0/24 101.33.121.0/24 101.32.250.0/24 IPの指定：指定するIPまたはIPセグメントを入力します	TCP:3389	許可

## シナリオ3：パブリックネットワークがCVMにpingできるようにする

**事例：**CVMを構築し、このCVMと他のCVM間の通信ステータスが正常であるかどうかをテストしたい場合。

**解決策：**pingプログラムを使用してテストを行います。手順は、セキュリティグループルールの追加を行うときに、「タイプ」で「Ping」を選択し、ICMPプロトコルポートを開放して、その他のCVMがICMPプロトコルを介してCVMにアクセスすることを許可します。

また、実際のニーズに応じて、すべてのIPを解放するか、またはIP（IPセグメント）を指定して、ICMPプロトコルを介したCVMへのアクセスを許可するIPソースを設定することもできます。

方向	タイプ	ソース	プロトコルポート	ポリシー
インバウンド	Ping	すべてのIP：0.0.0.0/0 IPを指定：指定したIPまたはIPセグメントを入力します	ICMP	許可

## シナリオ4：Telnetを介してCVMにリモートログイン

**事例：**Telnetを介してCVMにリモートログインしたい場合。

**解決策：**Telnetを介してCVMにリモートログインする必要がある場合は、セキュリティグループルールの追加を行うときに、以下のセキュリティグループのルールを設定する必要があります。

方向	タイプ	ソース	プロトコルポート	ポリシー

インバウンド 方向	カスタマイズ	すべての IP : 0.0.0.0/0 IPを指定 : 指定したIPまたはIPセグメントを入力します	TCP:23	許可
--------------	--------	---	--------	----

### シナリオ5 : HTTPまたはHTTPSを介してWebサービスへのアクセスを開く

**事例 :** お客様がウェブサイトを構築し、ユーザーにHTTPまたはHTTPSを介してお客様が構築したウェブサイト  
にアクセスしてほしい場合。

**解決策 :** HTTPまたはHTTPSを介してCVMにアクセスする必要がある場合は、[セキュリティグループルールの追加](#)  
を行うときに、実際のニーズに応じて以下のセキュリティグループのルールを設定する必要があります。

パブリックネットワーク上のすべてのIPにこのウェブサイトへのアクセスを許可します

方向	タイプ	ソース	プロトコルポート	ポリシー
インバウンド	HTTP (80)	0.0.0.0/0	TCP:80	許可
インバウンド	HTTPS (443)	0.0.0.0/0	TCP:443	許可

パブリックネットワークの一部のIPアドレスがこのウェブサイトへのアクセスを許可します。

方向	タイプ	ソース	プロトコル ポート	ポリ シー
インバ ウンド	HTTP (80)	ウェブサイトへのアクセスが許可されているIPアドレスま たはIPアドレスセグメント	TCP:80	許可
インバ ウンド	HTTPS (443)	ウェブサイトへのアクセスが許可されているIPアドレスま たはIPアドレスセグメント	TCP:443	許可

### シナリオ6 : 外部IPが指定ポートにアクセスすることを許可する

**事例 :** 業務をデプロイした後、指定されたサービスポート (例 : 1101) に外部からアクセスできるようにしたい  
場合。

**解決策 :** [セキュリティグループルールの追加](#)を行うときに、「タイプ」で「カスタム」を選択し、プロトコル  
ポート1101を開放して、指定された業務ポートへの外部アクセスを許可します。

また、実際のニーズに応じて、すべてのIPを解放するか、またはIP (IPセグメント) を指定して、指定されたサー  
ビスポートのIPソースへのアクセスを許可することもできます。

方向	タイプ	ソース	プロトコル ポート	ポリ シー
インバウ ンド	カスタマ イズ	すべてのIP : 0.0.0.0/0 IPを指定 : 指定したIPまたはIPセグメントを入 力します	TCP:1101	許可

## シナリオ7：外部IPアドレスから指定したポートへのアクセスを拒否する

**事例：**業務をデプロイした後、指定されたサービスポート（例：1102）に外部からアクセスされないようにしたい場合。

**解決策：**セキュリティグループルールの追加を行うときに、「タイプ」で「カスタム」を選択し、プロトコルポート1102を構成し、「ポリシー」を「拒否」に設定して、指定されたサービスポートへの外部アクセスを拒否します。

方向	タイプ	ソース	プロトコルポート	ポリシー
インバウンド	カスタマイズ	すべてのIP：0.0.0.0/0 IPを指定：指定したIPまたはIPセグメントを入力します	TCP:1102	拒否

## シナリオ8：CVMが特定の外部IPへのアクセスのみを許可

**事例：**CVMが特定の外部IPアドレスのみアクセスできるようにします。

**ソリューション：**以下の設定を参照し、次の2つのアウトバンドのセキュリティグループルールを追加します。

CVMインスタンスが特定の外部IPアドレスにアクセスできるようにします。

インスタンスが任意のプロトコルを介してパブリックIPアドレスにアクセスすることを禁止します。

### ご注意：

アクセスを許可するルールは、アクセスを拒否するルールより優先する必要があります。

方向	タイプ	ソース	プロトコルポート	ポリシー
アウトバンド	カスタマイズ	CVMがアクセスできる特定のパブリックIPアドレス	必要なプロトコルとポート	許可
アウトバンド	カスタマイズ	0.0.0.0/0	ALL	拒否

## シナリオ9：CVMが特定の外部IPにアクセスすることを拒否する

**事例：**CVMが外部の特定のIPアドレスにアクセスできないようにします。

**解決策：**次の構成を参照して、セキュリティグループルールを追加してください。

方向	タイプ	ソース	プロトコルポート	ポリシー
アウトバンド	カスタマイズ	インスタンスからのアクセスを拒否する特定のパブリックIPアドレス	ALL	拒否

## シナリオ10：FTPを使用してファイルをアップロードまたはダウンロードする

**事例：**FTPソフトウェアを利用して、CVMにファイルをアップロードまたはダウンロードする場合。

**解決策：**次の構成を参照して、セキュリティグループルールを追加してください。

方向	タイプ	ソース	プロトコルポート	ポリシー
インバウンド	カスタマイズ	0.0.0.0/0	TCP:20-21	許可

## 複数シーンの組み合わせ

実際のシナリオでは、業務ニーズに応じて複数のセキュリティグループルールを設定する必要がある可能性があります。例えば、インバウンドルールまたはアウトバウンドルールを同時に設定します。CVM1台は、1つまたは複数のセキュリティグループにバインドできます。CVMが複数のセキュリティグループにバインドされている場合、複数のセキュリティグループが上から下に順番にマッチングが実行されます。セキュリティグループの優先度はいつでも変更できます。セキュリティグループルールの優先度の説明については、[ルールの優先度の説明](#)をご参照ください。

# サーバーの通常ポート

最終更新日：2020-07-30 13:41:28

このドキュメントでは、サーバーでよく使うポートの説明です。Windowsにおけるより多くのサービスアプリケーションポートの詳細については、Microsoft公式サイトのドキュメント ([Windowsのサービス概要及びネットワークポートの要件](#)) をご参照ください。

ポート	サービス	説明
21	FTP	FTPサーバーでオープンされているポート、アップロードとダウンロードに使われます。
22	SSH	22ポートはSSHポートであり、通常のCommand Line InterfaceモードによるLinuxシステムサーバーへのリモート接続に使われています。
25	SMTP	SMTPサーバーでオープンされているポート、メールの送信に使われています。
80	HTTP	サイトサービスに使われています。例えば、IIS、Apache、Nginx等は外部アクセスを提供しています。
110	POP3	110ポートはPOP3（メールプロトコル3）サービスのためにオープンされています。
137、 138、139	NETBIOS プロトコル	ポート137および138は、マイネットワーク経由でファイルを転送するためのUDPポートです。 139ポート：このポート経由で確立された接続はNetBIOS/SMBサービスの取得を試みます。このプロトコルは、WindowsおよびSAMBAでのファイルとプリンターの共有に使用されます。
143	IMAP	143ポートは主に「Internet Message Access Protocol」v2（Internetメッセージアクセスプロトコルであり、IMAPと略称する）に使われており、POP3と同じように、電子メールを受信するためのプロトコルです。
443	HTTPS	Webブラウジング用のポートであり、暗号化とセキュリティポートを介した転送を提供できるもう1種のHTTPです。
1433	SQL Server	1433ポートはSQL Serverのデフォルトポートです。SQL ServerサービスはTCP-1433とUDP-1434の2つのポートを使っています。そのうち、ポート1433はSQL Serverが外部サービスを提供するために使用され、ポート1434はリクエスタに対してSQL ServerがどのTCP/IPポートを使っているかを返信することに使われています。
3306	MySQL	3306ポートはMySQLデータベースのデフォルトポートであり、MySQLは外部サービスを提供するために使われています。

3389	Windows Server Remote Desktop Services (リモートデスクトップサービス)	3389ポートはWindows Server リモートデスクトップのサービスポートです。このポートを介して、「リモートデスクトップ」接続ツールでリモートサーバーに接続することができます。
8080	プロキシポート	8080ポートは80ポートと同様に、WWW プロキシサービスに使われています。特定のWebサイトにアクセスする場合、またはプロキシサーバーを使う場合、よくURLに「:8080」ポート番号を追加します。また、Apache Tomcat Webサーバーがインストールされた後のデフォルトのサービスポートはポート8080です。

# 機密性の高い操作に対する保護機能を強化

最終更新日：2023-05-15 11:03:07

## 概要

現在、CVMは機密性の高い操作に対する保護機能を提供しています。この機能を有効にしたら、機密性の高い操作を実行する前に、身元確認を完了する必要があります。

機密性の高い操作に対する保護機能は、シャットダウン、再起動、VNCログイン、パスワードのリセット、インスタンスの終了、システムの再インストール、構成の調整、キーの読み込み、VPCの切り替えなど、アカウントリソースのセキュリティを効果的に保護することができます。

## 操作保護機能の有効化

[セキュリティ設定コンソール](#)で操作保護機能を有効にすることができます。詳細については、[Operation Protection](#)をご参照ください。

## 操作保護の検証

操作保護機能が有効になっている場合は、機密性の高い操作を実行する前に、検証を完了する必要があります。

操作保護のために**多要素認証 (MFA)**が有効になっている場合、MFAデバイス上に表示される6桁の確認コードを入力する必要があります。

操作保護のために**SMS認証**が有効になっている場合、携帯電話宛てに送信されたSMSに記載のある確認コードを入力する必要があります。

# ログインパスワードの管理

最終更新日：2023-05-15 11:38:05

## 概要

Cloud Virtual Machine のアカウントとパスワードは、CVM にログインするための資格情報です。本ドキュメントでは、CVM にログインする時にパスワードを使用および管理する方法について説明します。

## 制限条件

パスワードを設定する場合、以下の制限条件を満たす必要があります：

**Linux インスタンス**：パスワードの長さは8～30文字で、12文字以上のパスワードを推奨し、「/」で始めることはできず、少なくとも3つの項目（英小文字 `a～z`、英大文字 `A～Z`、数字 `0～9` および記号 `() ~!@#$%^&*~+=_ | {} [ ] ; ' < > , . ? /`）を含む必要があります。

**Windows インスタンス**：パスワードの長さは12～30文字で、「/」で始めることはできず、少なくとも3つの項目（英小文字 `a～z`、英大文字 `A～Z`、数字 `0～9` および記号 `() ~!@#$%^&*~+=_ | {} [ ] ; ' < > , . ? /`）を含む必要があり、ユーザー名を含むことができません。

## 操作手順

### 初期パスワードの設定

CVMの購入時に選択した構成方法が異なると、初期パスワードの設定も異なります。

[カスタム設定](#) によるインスタンスの作成: 作成時に、初期パスワードの設定方法はログインモードによって異なります。

ログインモード	説明
ランダムパスワードの生成	アカウントに関連付けられているメールアドレスとコンソールの <a href="#">サイト内メール</a> に初期パスワードのメッセージが送信されます。
キーの関連付け	ユーザー名とパスワードによるログインは、デフォルトで無効になっています。パスワードを使用するには、CVMコンソールにログインして <a href="#">パスワードをリセット</a> してください。
カスタムパスワード	設定したパスワードが初期パスワードです。

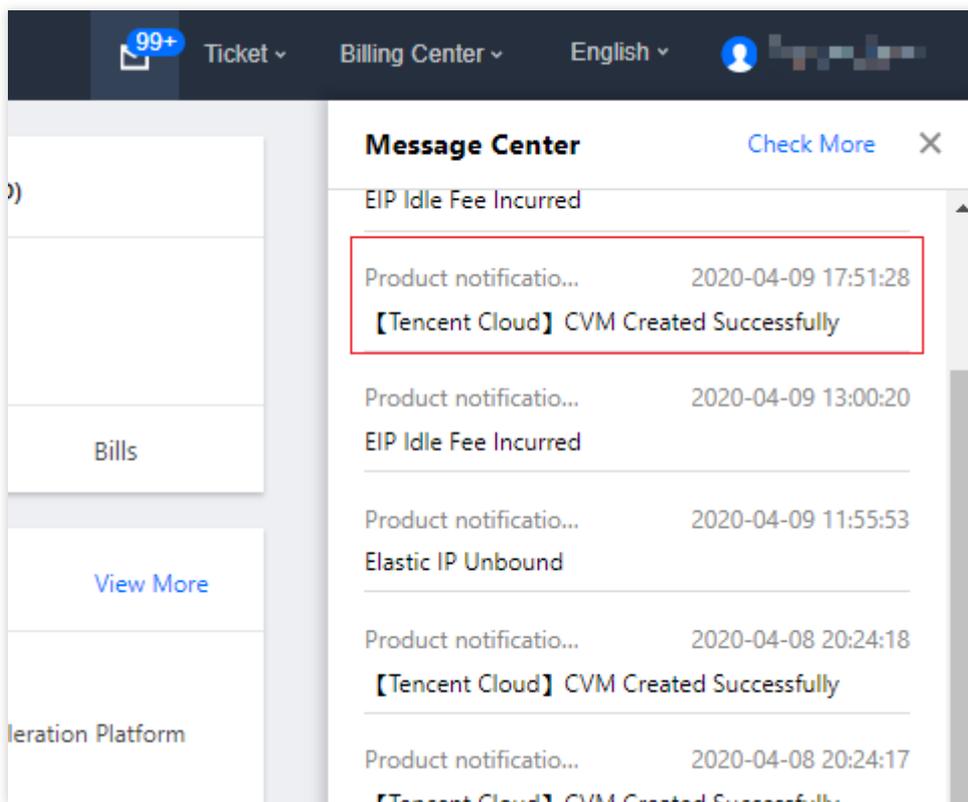
## パスワードの確認

システムによって自動生成されたランダムパスワードは、電子メールおよびコンソールの [サイト内メール](#) を通じて送信されます。以下の操作はサイト内メールを例として説明します。

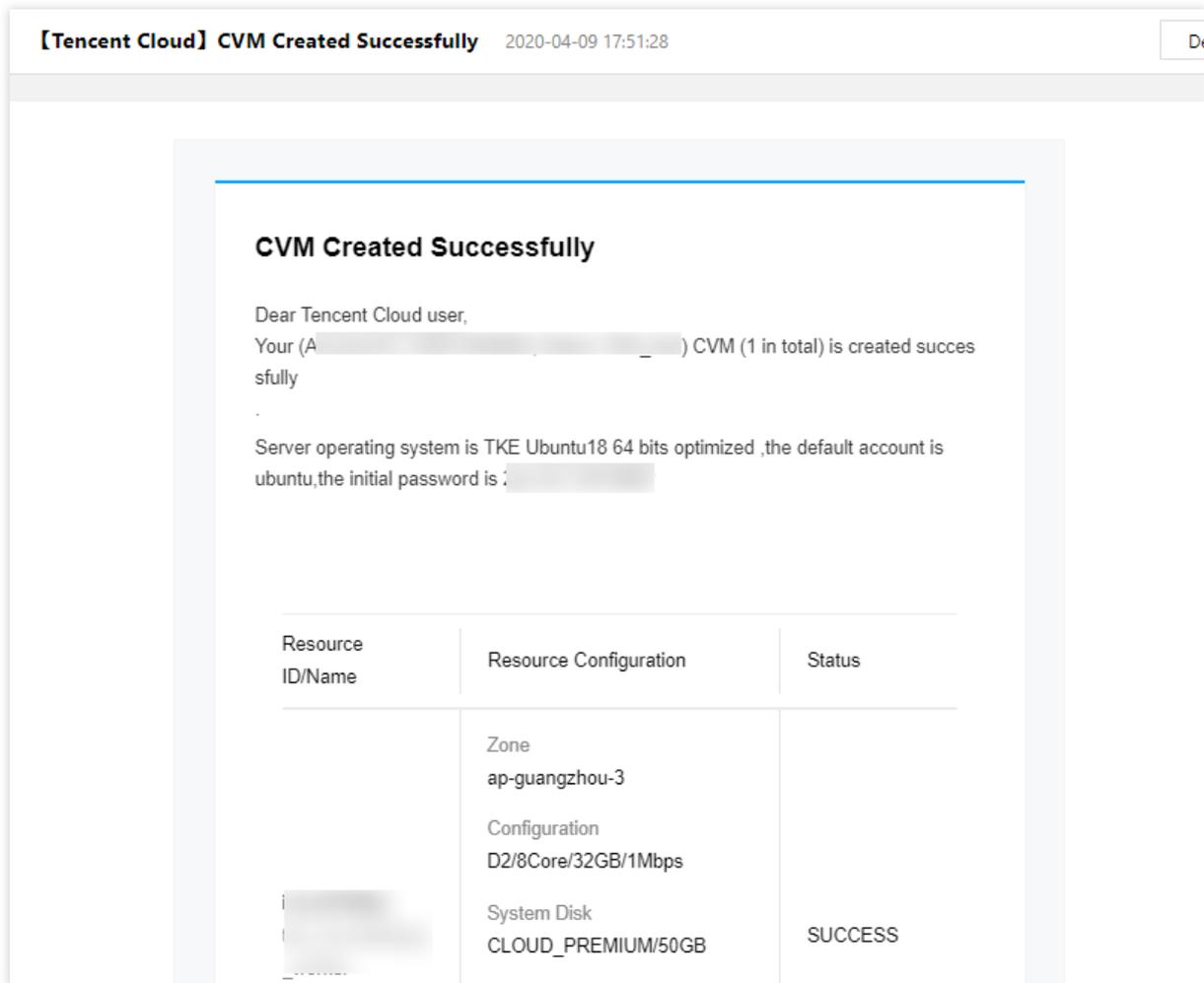
1. [CVMコンソール](#) にログインします。
2. 右上の



をクリックし、その製品情報を選択します。下図の通りです：



この製品の情報画面にアクセスし、パスワードを確認できます。



## パスワードのリセット

詳細については、[インスタンスパスワードのリセット](#) をご参照ください。

# SSHキーの管理

最終更新日：：2023-06-30 15:28:14

## 概要

このドキュメントでは、SSHキーの作成、バインド、バインド解除、変更、削除など、SSH キーペアを使用したインスタンスへのログインに関連する一般的な操作について説明します。

### ご注意：

SSH キーは、シャットダウンされた CVM インスタンスにのみバインドまたはバインド解除できます。CVM インスタンスをシャットダウンする方法については、[インスタンスのシャットダウン](#)をご参照ください。

## 操作手順

### SSHキーの作成

1. CVMコンソールにログインし、左側のナビゲーションバーで **SSHキー** を選択します。
2. **SSHキー**管理画面で**作成**をクリックします。
3. 「SSHキーを作成」画面が表示されます。「**SSHキーを作成**」画面でキーを設定します。下図に示すように：

**Create an SSH key** [X]

Creation method  Create a new key pair  Import existing public keys

Key Name   
25 more characters allowed

Tag (Optional)   [X]  
+ Add

**i** We will not keep your private key information. Be sure to save the private key downloaded after creation.

OK Cancel

#### 作成方法：

「新しいキーペアを作成します」を選択した場合は、キー名を入力してください。

「既存の公開鍵を使用します」を選択した場合は、キー名と既存の公開鍵情報を入力してください。

#### ご注意：

パスワードが不要な公開鍵を使用する必要があります。そうしないと、コンソールでインスタンスにログインできません。

**キー名:** 名前をカスタマイズします。

**タグ (オプション)：** 必要に応じてキーのタグを追加できます。タグは、リソースの分類、検索、および集約に使用できます。詳細については [タグ](#) をご参照ください。

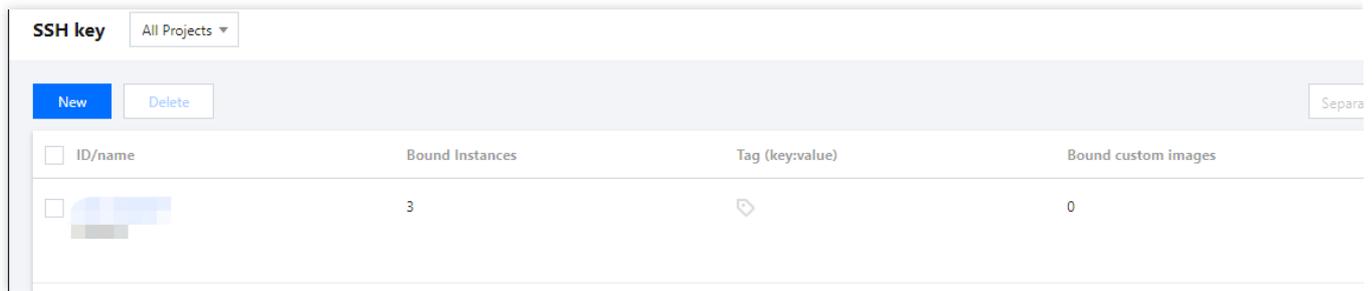
4. **OK** をクリックすると、作成が完了します。

#### ご注意：

**OK** をクリックすると秘密鍵が自動的にダウンロードされます。Tencent Cloud は秘密鍵の情報を保管しませんので、ご自身で大切に保管してください。秘密鍵が失われた場合は、キーを再作成して、対応するインスタンスにバインドできます。

#### インスタンスへのキーのバインド

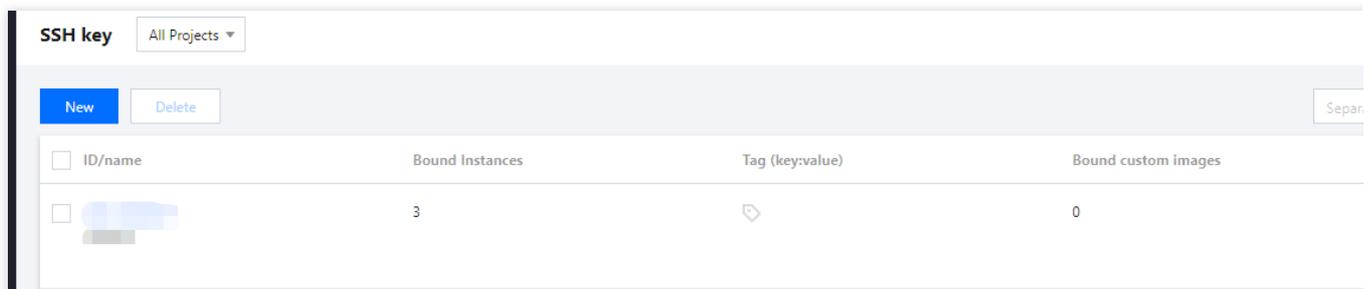
1. CVM コンソールにログインし、左側のナビゲーションバーで **SSH キー** を選択します。
2. 下図に示すように、「SSH キー」ページで、ターゲットキーの右側にある **インスタンスをバインドする** をクリックします。



3. ポップアップウィンドウで、リージョンとターゲットCVMインスタンスを選択し、**バインド**をクリックします。

### インスタンスからキーのバインドを解除

1. CVMコンソールにログインし、左側のナビゲーションバーで **SSHキー** を選択します。
2. 下図に示すように、ターゲットキーの右側にある**インスタンスのバインドを解除する**をクリックします。

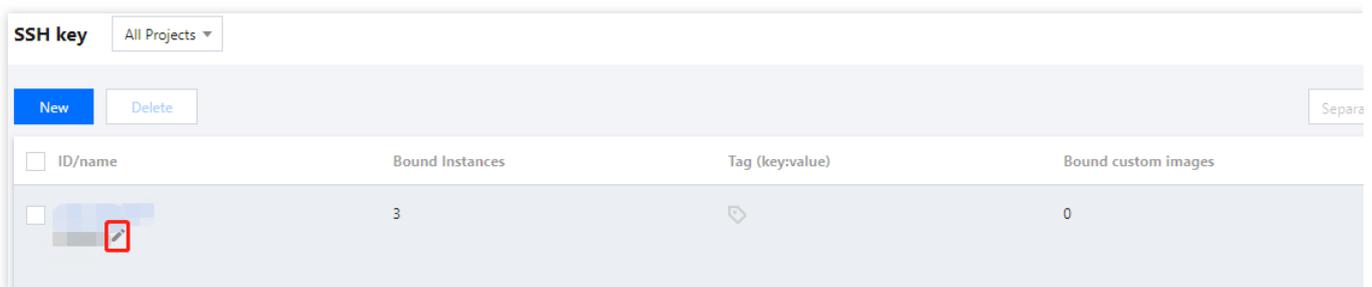


3. ポップアップウィンドウで、リージョンとターゲットCVMインスタンスを選択し、**バインド解除**をクリックします。

### SSHキーの名前または説明の変更

1. CVMコンソールにログインし、左側のナビゲーションバーで **SSHキー** を選択します。
2. 「SSHキー」 ページで、キー名の右側にある

を選択します。下図に示すように：



3. ポップアップウィンドウで、新しいキーの名前と説明を入力し、**OK**をクリックします。

## SSHキーの削除

### ご注意：

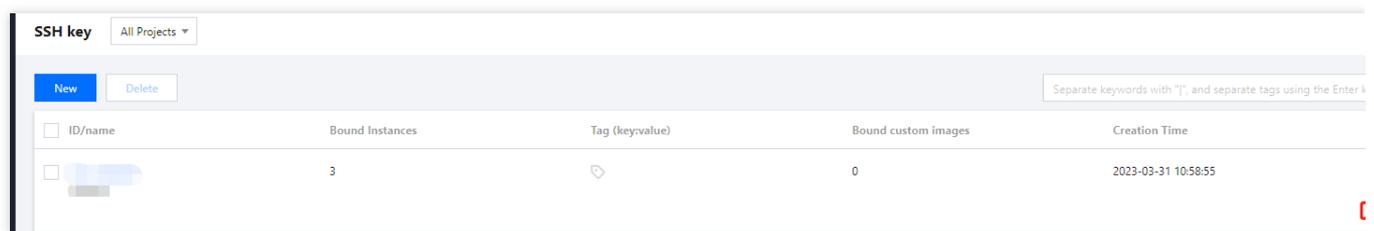
CVMインスタンスまたはカスタムイメージにバインドされているSSHキーは削除できません。

1. CVMコンソールにログインし、左側のナビゲーションバーで **SSHキー** を選択します。
2. 「SSHキー」 ページで、必要に応じてキーを個別または一括で削除することができます。

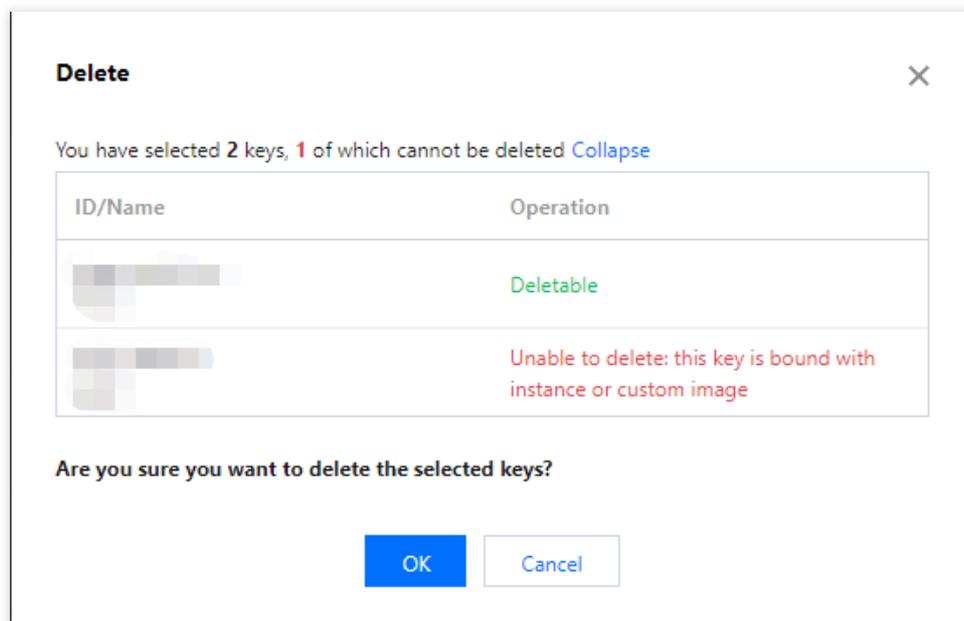
キーの個別削除

キーの一括削除

1. 下図に示すように、削除したいSSHキーの右側にある**削除**をクリックします。



2. 「削除」画面が表示されます。「削除」画面で**OK**をクリックします。
  1. 削除するキーをすべて選択し、ページ上部にある**削除**をクリックしてキーを一括削除します。
  2. 「削除」画面が表示されます。「削除」画面で**OK**をクリックします。下図のように：  
選択したキーペアに削除できないキーペアが含まれている場合、この操作は削除可能なキーペアに対してのみ行われます。



## 関連操作

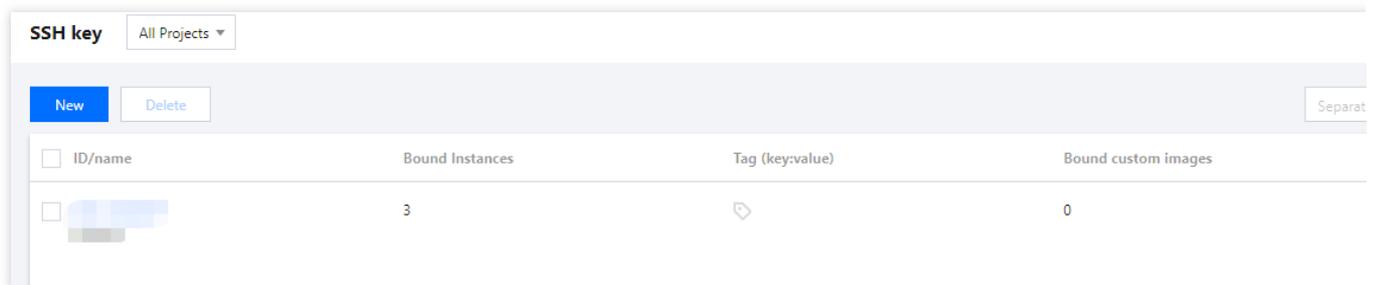
## SSHキーを使用したLinux CVMへのログイン

1. SSHキーの作成。
2. インスタンスへのキーのバインド。
3. SSHキーを使用したLinuxインスタンスへのログイン。

### キータグの編集

SSHキーのタグを追加、変更、および削除する方法については、次の手順を参照してください。タグの詳細については、[タグ](#)をご参照ください。

1. 「SSHキー」 ページでキーの右側にある **タグ編集** をクリックします。下図のように：



2. 「タグ編集」画面が表示されます。「タグ編集」画面で必要に応じて設定してください。
3. **OK** をクリックします。

# スプレッドプレイスメントグループ

最終更新日：：2023-05-15 17:35:42

## シナリオ

このドキュメントでは、スプレッドプレイスメントグループを管理する方法について説明します。スプレッドプレイスメントグループの詳細については、[プレイスメントグループ](#)をご参照ください。

## 操作手順

### プレイスメントグループを作成する

1. [CVMプレイスメントグループコンソール](#) にログインします。
2. **新規作成** をクリックします。
3. 表示されるダイアログボックスで、プレイスメントグループの名前を入力し、プレイスメントグループのレイヤーを選択します。
4. **【OK】** ボタンをクリックして作成を完了します。

### プレイスメントグループでインスタンスを起動する

1. [CVM購入画面](#) に移動します。
  2. 画面の指示に従って、購入手続きを進めてください。
- 購入する際は、次の操作を実行してください。

CVMを設定する時、**詳細設定** をクリックし、**インスタンスをスプレッドプレイスメントグループに追加する** にチェックを入れ、既存のプレイスメントグループを選択します。

既存のプレイスメントグループが適切でない場合、コンソールで [プレイスメントグループを作成](#) できます。構成情報を確認する際、このプレイスメントグループに追加する必要があるインスタンスの総数を入力します。この総数はプレイスメントグループにより定められた上限を超えることはできません。

### インスタンスのプレイスメントグループを変更する

#### 説明：

現在、プレイスメントグループの名前変更のみがサポートされています。

1. [CVMプレイスメントグループコンソール](#) にログインします。
2. ターゲットプレイスメントグループのIDまたは名前にマウスカーソルを合わせて、

 をクリックします。

3. 表示されるダイアログボックスで、新しい名前を入力します。
4. **OK**ボタンをクリックすると変更が完了します。

## プレースメントグループを削除する

### 説明：

プレースメントグループを置き換える必要がある場合、またはプレースメントグループが不要になった場合は、削除できます。削除する前に、このプレースメントグループで実行されているすべてのインスタンスを終了する必要があります。

1. [CVMプレースメントグループコンソール](#) にログインします。
2. 削除するプレースメントグループの行で、**インスタンス数**をクリックし、インスタンス管理画面に進み、プレースメントグループ内のすべてのインスタンスを終了します。
3. プレースメントグループコンソールに戻り、削除するプレースメントグループを選択して、削除をクリックします。
4. 表示されるダイアログボックスで、**OK**をクリックすると、削除が完了します。  
プレースメントグループを単一または一括で削除できます。

# 25番ポートのブロック解除

最終更新日：：2023-05-15 16:51:57

## 概要

このドキュメントでは、25番ポートのブロック解除方法について説明します。

## 注意事項

各Tencent Cloudアカウントは、最大で5つのインスタンスのポートのブロックを解除できます。サードパーティのSMTPサーバーに接続して電子メールを送信する場合は、必ず25番ポートのみを使用してください。SMTPプロトコルを使用してCVM経由で直接メールを送信していることが判明した場合は、Tencent CloudはTCPポート25番を永久にブロックし、関連するサービスの提供を停止または終了する権利を有します。

## 操作手順

1. [Tencent Cloud](#) コンソールにログインします。
2. 右上隅にあるアカウント名をクリックし、[安全管理](#) を選択します。
3. 左側のサイドバーで、「Unblock port 25」をクリックして、25番ポートのブロック解除ページに進みます。
4. 「Apply for unblocking port 25」をクリックします。
5. ブロックを解除する必要があるリージョンとCVMインスタンスを選択します。「I have read and accepted "Port 25 Protocol"」にチェックを入れます。下の図に示すように：

### 説明：

25番ポートのブロックを解除する前に、現在のアカウントのブロック解除クォータを使い切っていないことを確認してください。「Application for Unblocking TCP Port 25」画面の左下で残りのクォータを確認できます。

### Application for Unblocking TCP Port 25 ✕

Note: In order to improve the performance for sending emails from Tencent Cloud IP addresses, your CVMs are restricted from accessing the external TCP Port 25 by default. You can apply for unblocking your CVMs. A maximum of 5 unblocking operations are allowed for each account.

Select Region South China (Guangzhou) ▾

Select a CVM

in [blurred]

[blurred]

[blurred]

Total: 3 item(s) 1/1 ▾

ⓘ Remaining quota: 4 times

I have read and accepted "Port 25 Protocol"

OK Cancel

6. **OK**をクリックしてブロックを解除できます。

# タグ

## タグを使用したインスタンスの管理

最終更新日：：2023-05-15 17:50:19

### 概要

タグは、リソースを簡単に識別できるようにTencent Cloudが提供するキーと値のペアです。タグを使用すると、さまざまな方面（例えばサービス、目的、担当者など）からCVM リソースを簡単に管理および分類できます。Tencent Cloudはユーザーが設定したタグを使用しません。タグはCVMリソースを管理するためにのみ使用されます。

### 使用制限

タグを使用する場合、次の制限に注意してください。

数量制限：各クラウドリソースは、最大 50 個のタグを適用できます。

タグキーの制限：

タグキーは、`qcloud`、`tencent`、または `project` で始めることはできません。

タグキーの長さは最大255文字で、数字、アルファベットと`+.=@-`のみ使うことができます。

タグ値には、最大127文字の数字、アルファベット、`+.=@-`を含めることができます。必要に応じて空のままにすることができます。

### 操作方法とユースケース

#### ユースケース

ある企業が6つのCVM インスタンスを購入した場合、これらの6つのインスタンスの使用部門、業務範囲、担当者に関する情報は次のとおりです。

インスタンス instance-id	使用部門	業務範囲	担当者
ins-abcdef1	Eコマース	マーケティングキャンペーン	張三
ins-abcdef2	Eコマース	マーケティングキャンペーン	王五
ins-abcdef3	ゲーム	ゲーム A	張四
ins-abcdef4	ゲーム	ゲーム B	王五

ins-abcdef5	エンターテインメント	ポストプロダクション	王五
ins-abcdef6	エンターテインメント	ポストプロダクション	張三

ins-abcdef1 を例として、このインスタンスに次のタグを追加できます：

タグキー	タグ値
dept	ecommerce
business	mkt
owner	zhangsan

同様に、他のインスタンスも、使用部門、業務範囲、担当者の違いによって対応するタグを設定できます。

## CVM コンソールでタグを設定する

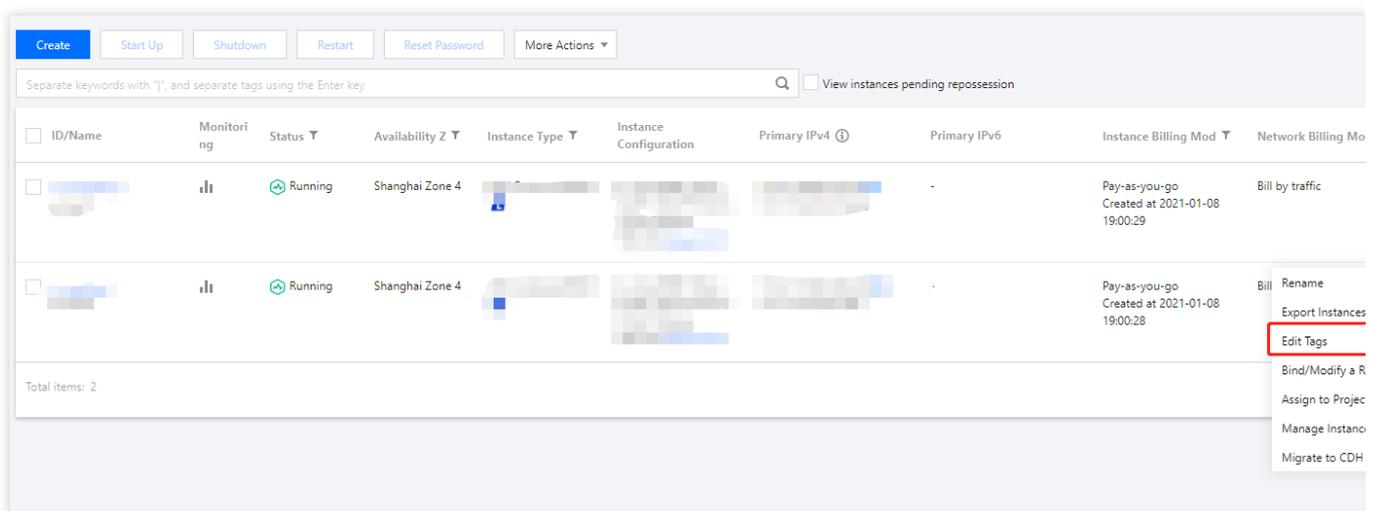
上記のケースを例として、タグキーとタグ値の設定が完了した後、CVMコンソールにログインしてタグを設定できます。

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画面で、実際に使用されているビューモードに従って操作します。

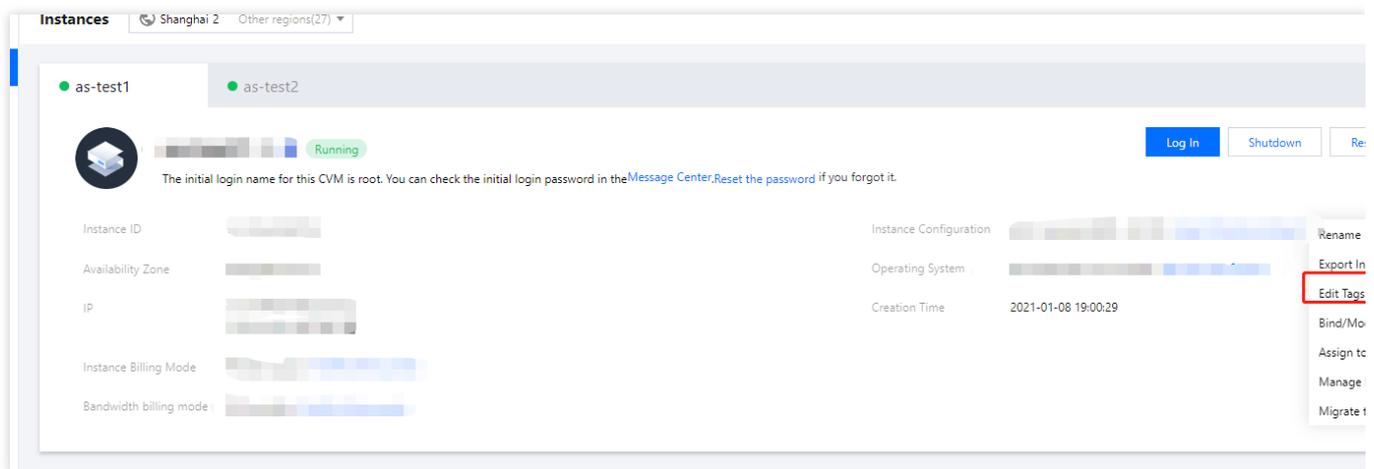
リストビュー

タブビュー

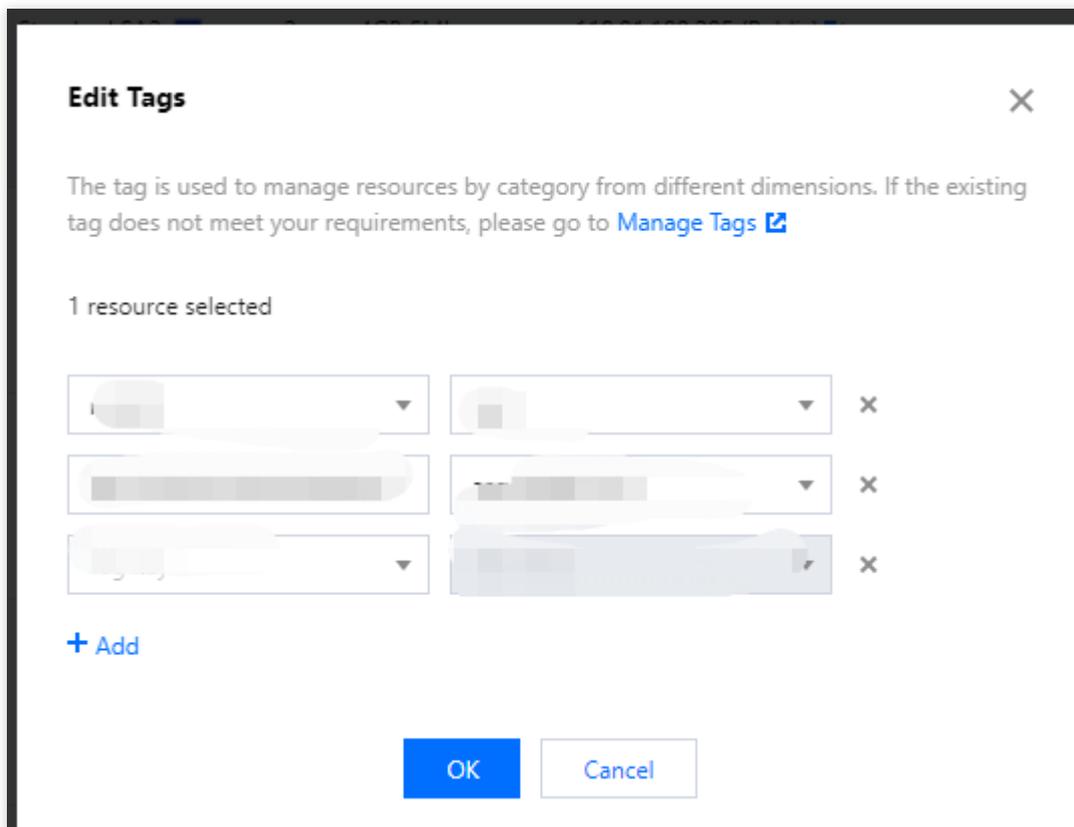
下図のように、タグを編集したいインスタンスを選択し、さらに>インスタンス設定>タグ編集をクリックします。



下図のように、タグを編集したいインスタンスを選択し、右上コーナーのその他の操作>インスタンス設定>タグ編集をクリックします。



3. 下図のように、表示される「you have selected 1 resource」ウィンドウで、タグを設定します。  
例えば、**3つのタグキーと値のペア**を ins-abcdef1 インスタンスに追加できます。



4. OKをクリックします。編集が成功したことを示すメッセージが表示されます。

### タグキーを使用してインスタンスをフィルタリングする

タグキーでインスタンスをフィルタリングするには、次の手順に従います。

1. 検索ボックスで、**タグキー**を選択します。
2. **タグキー**：の後にタグキーを入力し、



をクリックして検索を実行します。

タグキーを複数同時に指定してインスタンスをフィルタリングすることができます。たとえば、検索ボックスにタグキー: key1|key2 と入力して、タグキーkey1または key2 にバインドされているインスタンスをフィルタリングできます。

# タグ編集

最終更新日：2023-05-16 09:40:56

## 概要

このドキュメントでは、リソースのタグを編集する方法について説明させていただきます。

## 使用制限

タグの編集にはいくつかの制限事項があります。

数量制限：各クラウドリソースは、最大 50 個のタグを適用できます。

タグキーの制限：

タグキーは、`qcloud`、`tencent`、または `project` で始めることはできません。

タグキーには、`数字`、`アルファベット` と `+.=@-` のみを含めることができます。長さは255文字を超えることはできません。

タグ値の制限：タグ値には、最大127文字の数字、アルファベット、`+.=@-` を含めることができます。必要に応じて空のままにすることができます。

## 前提条件

[CVMコンソール](#) にログインしました。

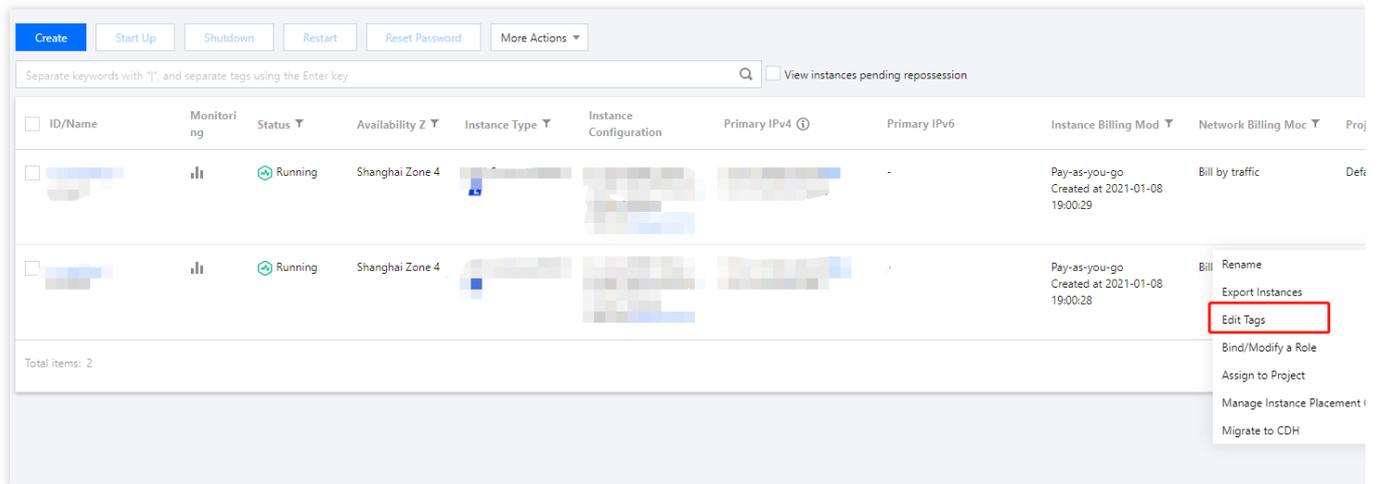
## 操作手順

個々のインスタンスのタグ編集

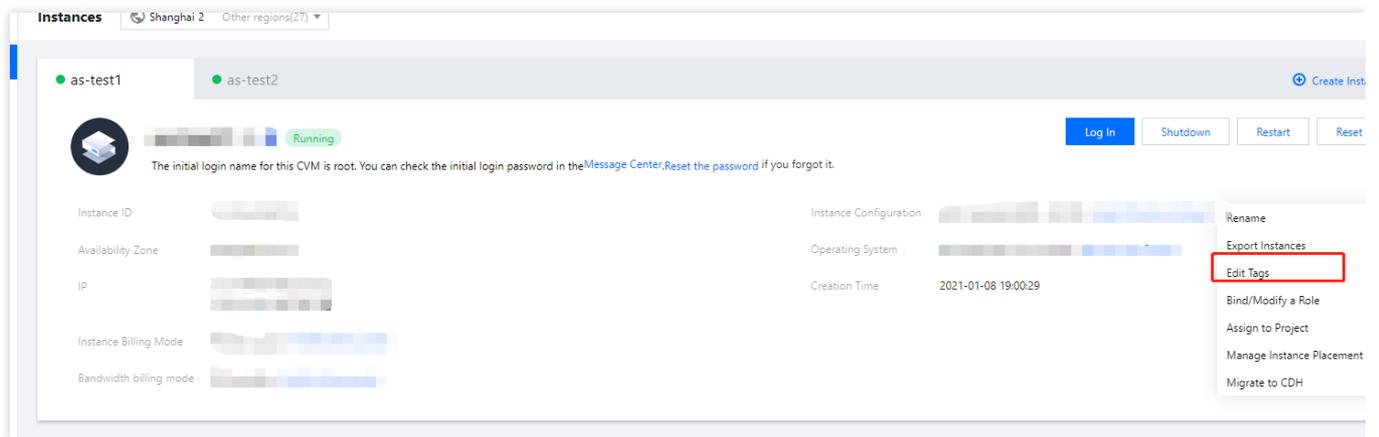
複数インスタンスのタグ編集

1. インスタンスの管理画面で、実際に使用されているビューモードに従って操作します

**リストビュー**：下図のように、タグを編集したいインスタンスを選択し、さらに **> インスタンス構成 > タグ編集** をクリックします。



タブビュー：下図のように、タグを編集したいインスタンスを選択し、画面の右上隅にある**その他の操作 > インスタンス構成 > タグ編集**をクリックします。

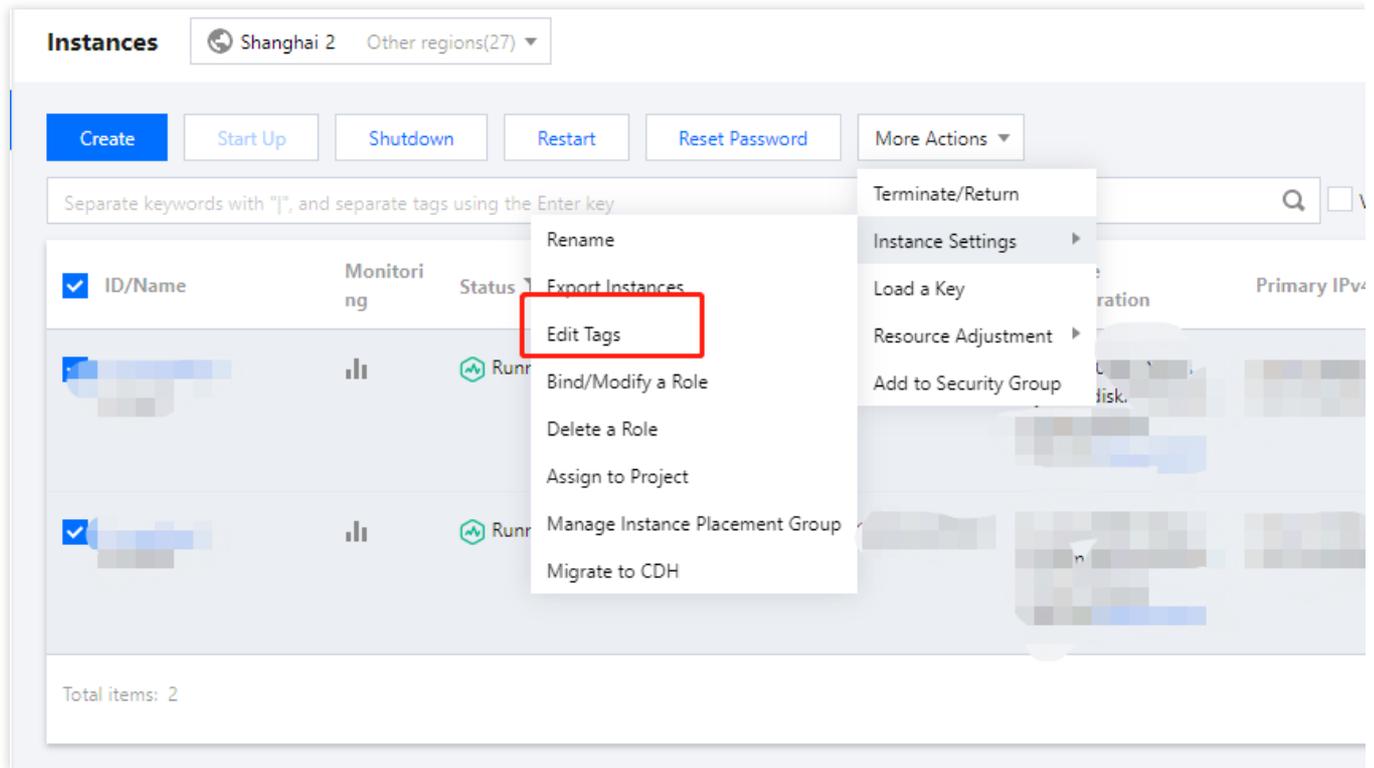


2. 表示されるダイアログボックスで、実際のニーズに応じてタグを追加、変更、または削除できます。

#### 説明：

一度に最大20個のリソースタグを編集できます。

1. 下図のように、インスタンスの管理画面で、タグを編集したいインスタンスを選択し、上部の**その他の操作 > タグ編集**をクリックします。



2. 表示されるダイアログボックスで、実際のニーズに応じてタグを追加、変更、または削除できます。

## 参照ドキュメント

タグの使用方法については、[タグでインスタンスを管理する](#) をご参照ください。

# 監視とアラーム

## インスタンスの監視データを取得する

最終更新日： : 2023-02-24 15:36:24

### 操作シナリオ

Tencent Cloudは、デフォルトではすべてのユーザーにクラウド監視機能を提供し、ユーザーが手動でアクティブ化する必要がありません。クラウド監視にデータの収集と監視を開始させるには、ユーザーはいずれかのTencent Cloud製品を使用する必要があります。このドキュメントでは、インスタンスを取得してデータを監視する方法について説明します。

### 操作手順

クラウド製品コンソールを介して取得する

クラウド監視コンソールを介して取得する

APIを介して取得する

#### 説明：

CVMに搭載されているコンソールに個別の監視データ読み取り機能ページが提供されています。このページでは、ユーザーはCVMインスタンスのCPU、メモリ、ネットワーク帯域幅、ディスク、その他の監視データを表示でき、表示期間を自由に調整できます。

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、監視データを表示するのインスタンスIDをクリックして、対象インスタンスの詳細ページに入ります。
3. [監視]タブをクリックして、インスタンスの監視データを取得します。

#### 説明：

クラウド監視コンソールは、すべての製品監視データの統合エントリーであり、ユーザーは、CVMのCPU、メモリ、ネットワーク帯域幅、ディスクなどの監視データを表示し、表示期間を自由に調整できます。

1. [クラウド監視コンソール](#) にログインします。
2. 左側のナビゲーションツリーで、[クラウド製品監視]> [CVM]を選択して、[CVM-基本監視]管理ページに入ります。
3. 監視データを表示するのインスタンスIDをクリックして、監視の詳細ページに入り、インスタンス監視データを取得します。

ユーザーは、GetMonitorDataインターフェースを使用して、すべて製品の監視データを取得できます。詳細については、[指標監視データの取り込み](#) をご参照ください。



# アラームの作成

最終更新日：：2022-07-27 14:42:35

## 操作シナリオ

Basic Cloud MonitorでサポートされているCVMリソースのパフォーマンス消費系のインジケータにしきい値アラームを設定することができます。また、CVMインスタンスまたはプラットフォームの基盤となるインフラストラクチャのサービスステータスに、イベントアラームを設定することもできます。異常が発生した場合は、メール、Short Message Service、電話などのチャンネルを通じて、講じる対策について速やかにお知らせします。アラームを適切に作成すると、アプリケーションの堅牢性と信頼性を向上させることができます。ここでは、アラームの作成方法についてご説明します。アラームの関連情報については、[アラームポリシーの新規作成](#)をご参照ください。

## 操作手順

1. Basic Cloud Monitorコンソールにログインし、左側ナビゲーションバーの**アラーム設定** > **アラームポリシー** を選択します。
2. 「アラームポリシー」 ページで、**新規作成**をクリックします。
3. ポップアップした「アラームポリシーの新規作成」ウィンドウで、下表に基本情報、アラームルールおよび通知テンプレートの新規作成の設定について説明しておりますので、ご参照ください。

設定タイプ	設定項目	説明
基本情報	ポリシー名	カスタムポリシー名です。
	備考	カスタムポリシーの備考です。
	監視タイプ	クラウド製品の監視タイプをサポートします。
	ポリシータイプ	監視する必要があるクラウド製品のポリシータイプを選択します。
	ポリシーが属するプロジェクト	属するプロジェクトを設定すると、アラームポリシーリストにおけるプロジェクトの下にあるアラームポリシーをすばやくフィルタリングできます。
設定アラームルール	アラームオブジェクト	インスタンスIDを選択すると、このアラームポリシーが選択したインスタンスにバインドされます。

		<p>タグを選択すると、このアラームポリシーがタグの下のすべてのインスタンスにバインドされます。</p> <p>インスタンスグループを選択すると、このアラームポリシーが選択したインスタンスグループにバインドされます。</p> <p>すべてのオブジェクトを選択すると、このアラームポリシーは、現在のアカウントに権限があるすべてのインスタンスにバインドされます。</p>
	トリガー条件	<p>手動構成（インジケータアラーム）</p> <p>アラームトリガー条件：インジケータ、比較関係、しきい値、統計周期および持続周期で構成されるセマンティック条件です。トリガー条件の詳細を展開し、チャートのインジケータの変化傾向に応じて、適切なアラームしきい値を設定できます。</p>
		<p>手動構成（イベントアラーム）</p> <p>クラウド製品リソースまたは基盤となるインフラストラクチャサービスに異常が発生した場合、イベントアラームを作成して、講じる対策について速やかにお知らせすることができます。</p>
		<p>テンプレートの選択</p> <p>テンプレートボタンを選択し、ドロップダウンリストから構成済みテンプレートを選択します。具体的な構成については、<a href="#">トリガー条件テンプレートの構成</a>をご参照ください。</p>
構成アラーム通知（オプション）	通知テンプレート	<p>システムプリセットの通知テンプレートはデフォルトでバインドされています（受信者はルートアカウント管理者であり、受信チャンネルはShort Message Serviceとメールです）。各アラームポリシーは、最大3つの通知テンプレートにのみバインドできます。通知テンプレートの構成の詳細については、<a href="#">通知テンプレート</a>をご参照ください。</p>

4. 入力が完了したら、**完了**をクリックすればOKです。

# Cloud Access Managementの例

最終更新日： : 2022-05-26 18:53:47

## 操作シナリオ

Cloud Access Management (CAM) ポリシーを利用して、Cloud Virtual Machine (CVM) のコンソールで特定リソースの確認・利用権限をユーザーに付与します。本ドキュメントは特定リソースの確認・利用権限を例として、コンソールの特定部分のポリシーの利用方法をユーザーに提供します。

## 操作事例

### CVM の完全な読み書きポリシー

CVM インスタンスを作成・管理する権限をユーザーに持たせることを希望する場合、このユーザーに QcloudCVMFullAccess のポリシーを利用させます。このポリシーはユーザーに CVM、VPC (Virtual Private Cloud)、CLB (Cloud Load Balance) と MONITOR のすべてのリソースの操作権限を持たせることにより、この目標を達成します。

具体的な操作手順は下記の通り：

[権限付与管理](#) を参照して、プリセットポリシー QcloudCVMFullAccess をユーザーに認証します。

### CVM の読取専用ポリシー

ユーザーに CVM インスタンスのクエリー権限を持たせて作成、削除、起動/シャットダウン権限を持たせないことを希望する場合、ユーザーに QcloudCVMInnerReadOnlyAccess のポリシーを利用させます。このポリシーはユーザーに別々で次の操作によって目標を達成します、CVMですべて単語「Describe」を始まる操作とすべて単語「Inquiry」を始まる操作に操作権限を持たせます。具体的な操作手順は下記の通り：

[権限付与管理](#) を参照して、プリセットポリシー QcloudCVMInnerReadOnlyAccess をユーザーに認証します。

### CVM 関連リソースの読取専用ポリシー

ユーザーに CVM インスタンス及び関連リソース (VPC、CLB) へのクエリー権限だけ持たせて作成、削除、起動/シャットダウンなど操作権限を持たせないことを希望する場合、このユーザーに QcloudCVMReadOnlyAccess のポリシーを利用させます。このポリシーはユーザーに次の操作権限を持たせることにより、この目標を達成します。

CVM で単語「Describe」を始まるすべての操作と単語「Inquiry」を始まるすべての操作。

VPC で単語「Describe」を始まるすべての操作、単語「Inquiry」を始まるすべての操作と単語「Get」を始まるすべての操作。

CLB で単語「Describe」を始まるすべての操作。

Monitor ですべての操作。

具体的な操作手順は下記の通り：

[権限付与管理](#) を参照して、プリセットポリシー `QcloudCVMReadOnlyAccess` をユーザーに認証します。

## Elastic Cloud Block Storage関連のポリシー

CVM コンソールのCloud Block Storage情報を表示できるようにし、CBSの作成・利用などの権限をユーザーに持たせることを希望する場合、まず下記の操作をポリシーに追加してから、またこのポリシーをユーザーに関連することによって実現できます。

**CreateCbsStorages**：CBSを作成します。

**AttachCbsStorages**：指定されたElastic CBSを指定されたCVMにマウントします

**DetachCbsStorages**：指定されたElastic CBSをアンマウントします。

**ModifyCbsStorageAttributes**：指定されたCBSの名称或いは項目 ID を修正します。

**DescribeCbsStorages**：CBSの詳細情報をクエリーします。

**DescribeInstancesCbsNum**：CVMにマウント済のElastic CBSの数量とマウントできるElastic CBS数量の合計をクエリーします。

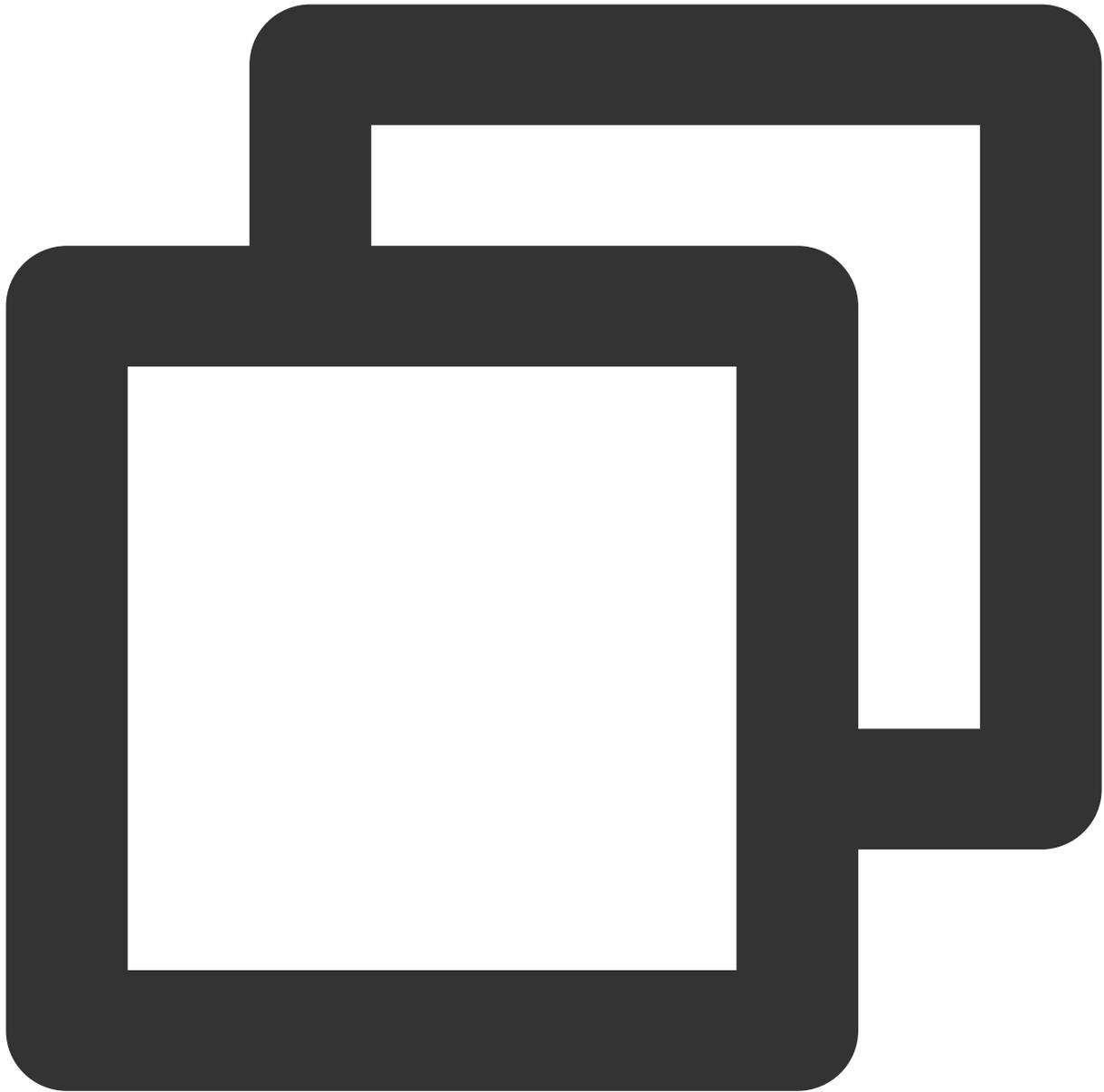
**RenewCbsStorage**：指定されたElastic CBSを更新します。

**ResizeCbsStorage**：指定されたElastic CBSをスケールアウトします。

具体的な操作手順は下記の通り：

1. [ポリシー](#) に基づいて、CVM コンソール内のCBS情報を確認するとCBSを作成・利用するなどの権限のカスタマイズポリシーを作成します。

ポリシー内容は下記のポリシー文法を参照して設定できます：



```
{
  "version": "2.0",
  "statement": [
    {
      "effect": "allow",
      "action": [
        "name/cvm:CreateCbsStorages",
        "name/cvm:AttachCbsStorages",
        "name/cvm:DetachCbsStorages",
        "name/cvm:ModifyCbsStorageAttributes",
        "name/cvm:DescribeCbsStorages"
      ]
    }
  ]
}
```

```
    ],  
    "resource": [  
        "qcs::cvm::uin/1410643447:*"  
    ]  
  }  
]  
}
```

2. 作成したポリシーを検索し、このポリシー行の「操作」列で、**ユーザ/グループの関連**をクリックします。
3. ポップアップされた「ユーザー/ユーザーグループの関連」ウィンドウで、権限付与に必要なユーザ/グループを選択し、**OK**をクリックします。

### セキュリティグループの関連ポリシー

ユーザーがCVM コンソールのセキュリティグループを確認・利用できることを希望する場合、下記の操作をポリシーに追加してから、このポリシーをユーザーに関連することによって実現できます。

**DeleteSecurityGroup**：セキュリティグループを削除します。

**ModifySecurityGroupPolicys**：セキュリティグループのすべてのポリシーを置き換えます。

**ModifySingleSecurityGroupPolicy**：セキュリティグループの単一ポリシーを修正します。

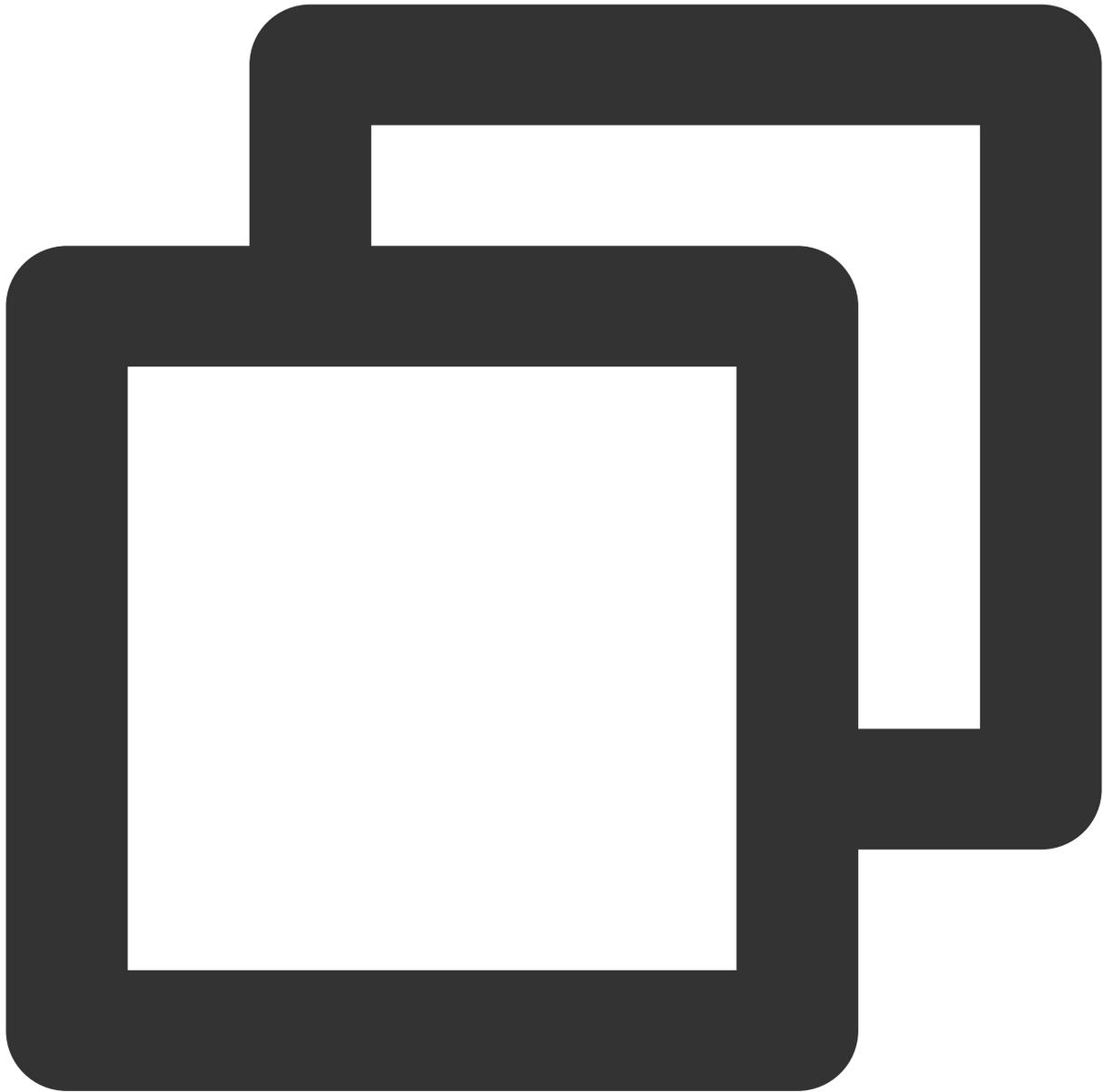
**CreateSecurityGroupPolicy**：セキュリティグループポリシーを作成します。

**DeleteSecurityGroupPolicy**：セキュリティグループポリシーを削除します。

**ModifySecurityGroupAttributes**：セキュリティグループの属性を修正します。

具体的な操作手順は下記の通り：

1. **ポリシー** に基づいて、ユーザーが CVM コンソールでセキュリティグループの作成、削除、修正などの権限を持つことを可能にするのカスタマイズポリシーを作成します。  
ポリシー内容は下記のポリシー文法を参照して設定できます：



```
{
  "version": "2.0",
  "statement": [
    {
      "action": [
        "name/cvm:ModifySecurityGroupPolicys",
        "name/cvm:ModifySingleSecurityGroupPolicy",
        "name/cvm:CreateSecurityGroupPolicy",
        "name/cvm>DeleteSecurityGroupPolicy"
      ],
      "resource": "*"
    }
  ]
}
```

```
    "effect": "allow"
  }
]
}
```

- 作成したポリシーを検索し、このポリシー行の「操作」列で、**ユーザ/グループの関連**をクリックします。
- ポップアップされた「ユーザー/ユーザグループの関連」ウィンドウで、権限付与に必要なユーザ/グループを選択し、**OK**をクリックします。

## Elastic IPアドレスの関連ポリシー

ユーザーが CVM コンソールでElastic IPアドレスを確認・利用できることを希望する場合、まず下記の操作をポリシーに追加してから、このポリシーをユーザーに関連することによって実現できます。

**AllocateAddresses** : アドレスを VPC 又は CVM にアサインします。

**AssociateAddress** : Elastic IPアドレスをインスタンス或いはネットワークインターフェースに関連します。

**DescribeAddresses** : CVM コンソールのElastic IP アドレスを確認します。

**DisassociateAddress** : Elastic IPアドレスは、インスタンス或いはネットワークインターフェースの関連を取り消します。

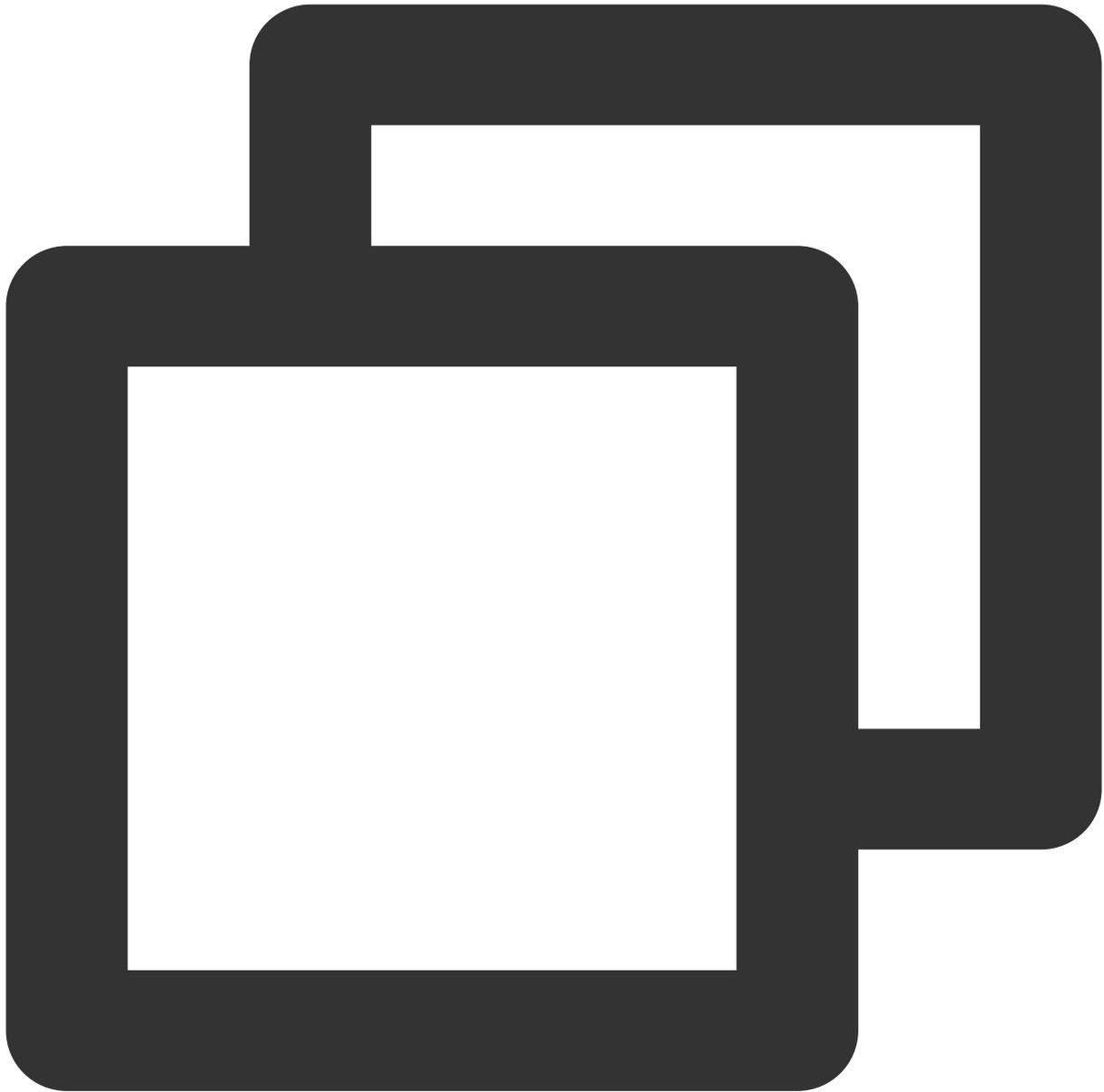
**ModifyAddressAttribute** : Elastic IPアドレスの属性を修正します。

**ReleaseAddresses** : Elastic IPアドレスを解除します。

具体的な操作手順は下記の通り：

- [ポリシー](#) に基づいて、カスタマイズポリシーを作成します。

このポリシーはユーザーが CVM コンソールでElastic IPアドレスを表示でき、インスタンスにアサインすること、インスタンスに関連することを許可しますが、Elastic IPアドレスの属性を修正したり、Elastic IPアドレスの関連を解除したり、Elastic IPアドレスの権限をリリースしたりすることはできません、ポリシー内容は下記のポリシー文法を参照して設定できます：



```
{
  "version": "2.0",
  "statement": [
    {
      "action": [
        "name/cvm:DescribeAddresses",
        "name/cvm:AllocateAddresses",
        "name/cvm:AssociateAddress"
      ],
      "resource": "*",
      "effect": "allow"
    }
  ]
}
```

```
}  
]  
}
```

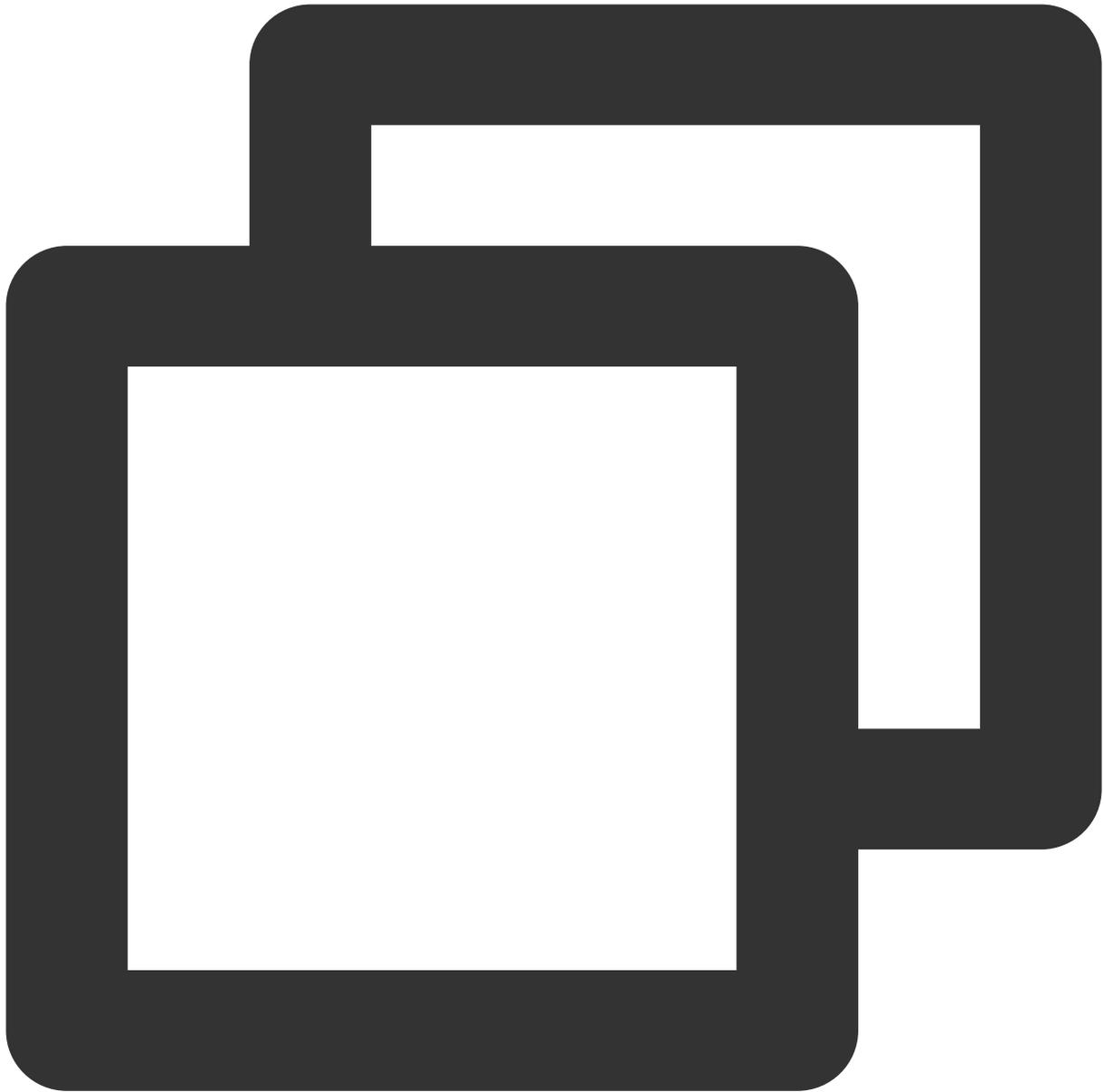
2. 作成したポリシーを検索し、このポリシー行の「操作」列で、**ユーザ/グループの関連**をクリックします。
3. ポップアップされた「ユーザ/ユーザグループの関連」ウィンドウで、権限付与必要なユーザ/グループを選択し、**OK**をクリックします。

### ユーザーに特定 CVM への操作権限を付与するポリシー

ユーザーに特定 CVM への操作権限を付与することを希望する場合、下記のポリシーをユーザーに関連することによって実現できます。具体的な操作手順は下記の通り：

1. **ポリシー**に基づいて、カスタマイズポリシーを作成します。

このポリシーはユーザーに ID が ins-1、リージョンが広州 のCVM インスタンスへの操作権限を持たせることを許可します。ポリシー内容は下記のポリシー文法を参照して設定できます：



```
{
  "version": "2.0",
  "statement": [
    {
      "action": "cvm:*",
      "resource": "qcs::cvm:ap-guangzhou::instance/ins-1",
      "effect": "allow"
    }
  ]
}
```

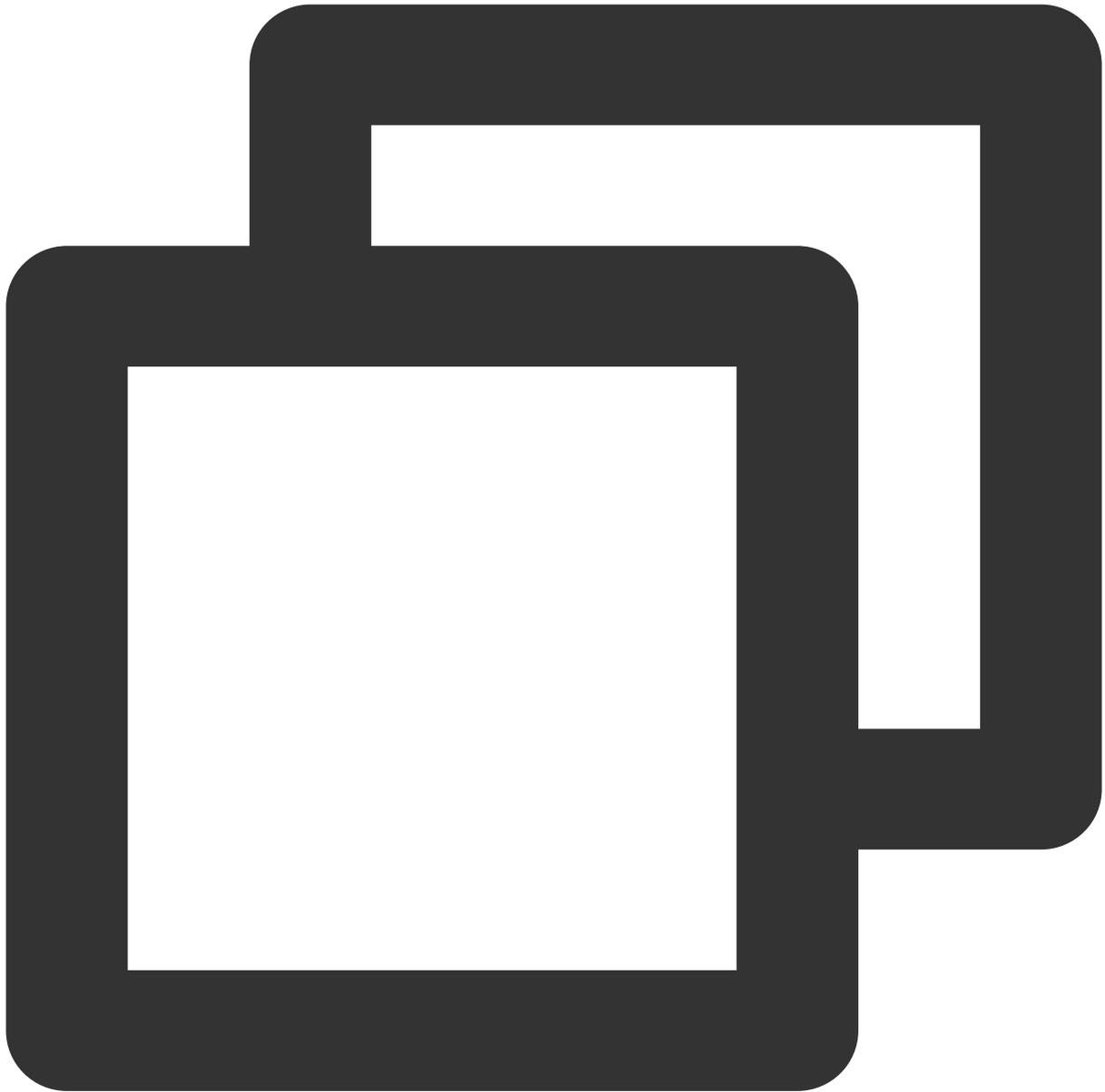
2. 作成したポリシーを検索し、このポリシー行の「操作」列で、**ユーザ/グループの関連**をクリックします。
3. ポップアップされた「ユーザ/ユーザグループの関連」ウィンドウで、権限付与必要なユーザ/グループを選択し、**OK**をクリックします。

### ユーザーに特定リージョンのCVM への操作権限を付与するポリシー

ユーザーに特定リージョンの CVM への操作権限を付与することを希望する場合、下記のポリシーをユーザーに関連することによって実現できます。具体的な操作手順は下記の通り：

1. **ポリシー** に基づいて、カスタマイズポリシーを作成します。

このポリシーはユーザーに広州リージョンの CVM への操作権限を持たせることを許可します、ポリシー内容は下記のポリシー文法を参照して設定できます：



```
{
  "version": "2.0",
  "statement": [
    {
      "action": "cvm:*",
      "resource": "qcs::cvm:ap-guangzhou::*",
      "effect": "allow"
    }
  ]
}
```

- 作成したポリシーを検索し、このポリシー行の「操作」列で、**ユーザ/グループの関連**をクリックします。
- ポップアップされた「ユーザ/ユーザグループの関連」ウィンドウで、権限付与に必要なユーザ/グループを選択し、**OK**をクリックします。

## サブアカウントに CVM のすべての権限を（支払い権限以外）付与する

仮に、企業アカウント（CompanyExample, ownerUin が12345678）が一つのサブアカウント（Developer）があります。このサブアカウントが企業アカウントのCVM サービスに対するすべての権限（例え作成、管理などすべての操作）を持たせることが必要であり、ただし支払い権限は含めません（注文できるが支払いできません）。

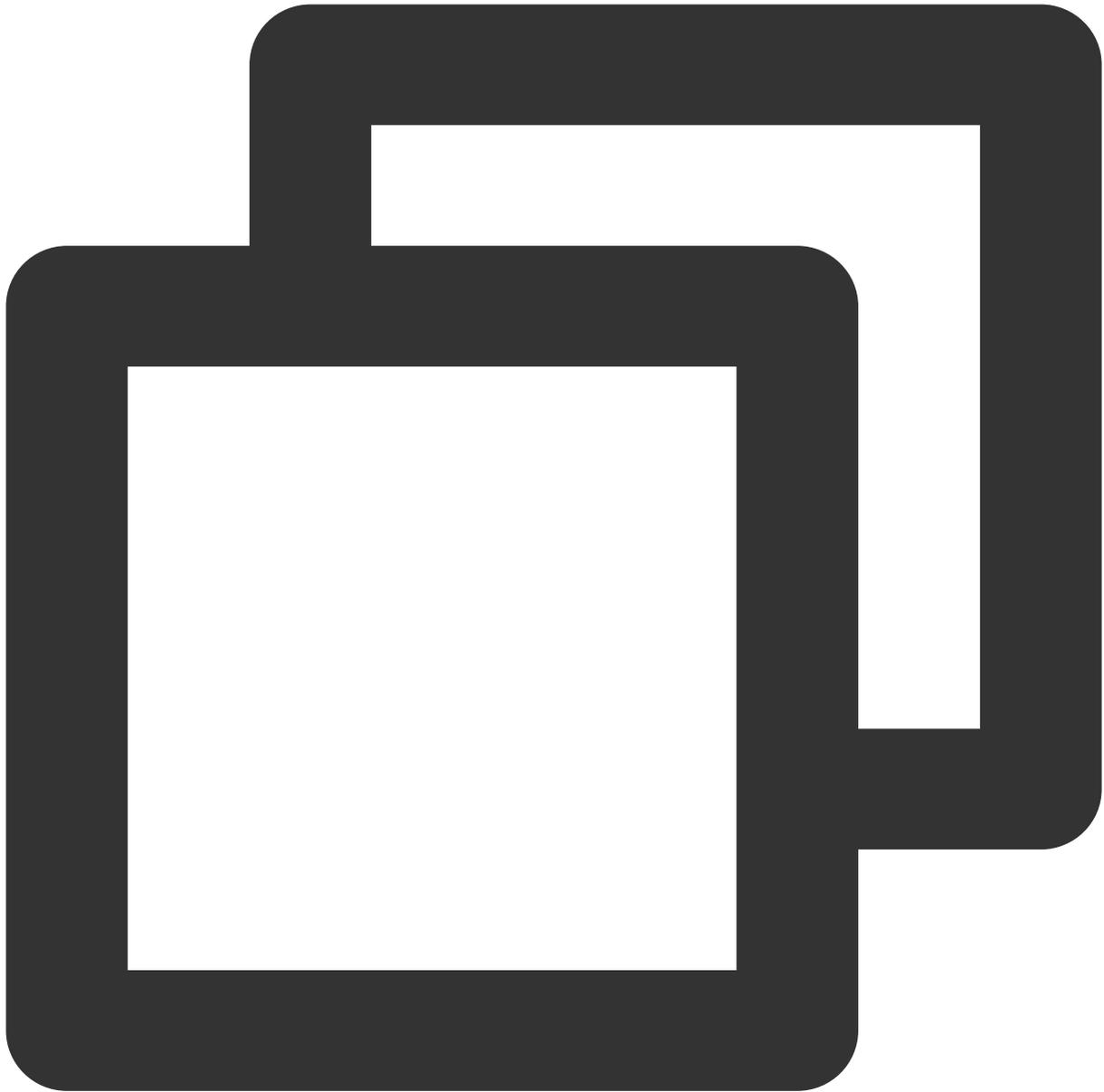
下記の二つのソリューションによって実現します：

### ソリューション A

企業アカウント CompanyExample は直接プリセットポリシー QcloudCVMFullAccess をサブアカウント Developer に付与します。権限付与方式は [権限付与管理](#) をご参照ください。

### ソリューション B

1.1 下記のポリシー文法に基づいて、[カスタマイズポリシー](#) を作成します。



```
{  
"version": "2.0",  
"statement": [  
  {  
    "effect": "allow",  
    "action": "cvm:*",  
    "resource": "*"   
  }  
]  
}
```

1.2 このポリシーをサブアカウントに付与します、権限付与方式は [権限付与管理](#) をご参照ください。

## サブアカウントにプロジェクト管理の操作権限を付与する

仮に、企業アカウント（CompanyExample, ownerUin 为12345678）は一つのサブアカウント（Developer）があります。プロジェクトに基づいてサブアカウントにコンソールでリソース管理権限を付与する必要があります。

具体的な操作手順は下記の通り：

1. 業務権限に基づいてプロジェクト管理のカスタマイズポリシーを作成します

詳細情報は [ポリシー](#) をご参照ください。

2. [権限付与管理](#)を参照して、作成したカスタマイズポリシーをサブアカウントに付与します。

サブアカウントがプロジェクトを管理する時に、権限なしの提示があった場合は、例えば、スナップショット、イメージ、VPC、Elasticパブリックネットワーク IP などの製品を確認する時に権限なしを提示されました。サブアカウントに QcloudCVMAccessForNullProject、QcloudCVMOrderAccess と QcloudCVMLaunchToVPC のプリセットポリシーを付与できます。権限付与方式は[権限付与管理](#)をご参照ください。

## カスタマイズポリシー

プリセットポリシーが要件を満たせないと予測した場合、カスタマイズポリシーを作成することによって目標を達成します。

具体的な操作手順は [ポリシー](#) をご参照ください。

CVM関連のポリシー文法の詳細については、[権限付与ポリシー文法](#) をご参照ください。。