# Cloud Virtual Machine

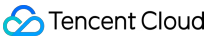
# 実践チュートリアル

## 製品ドキュメント

## 著作権声明



## 商標に関する声明





## サービス声明

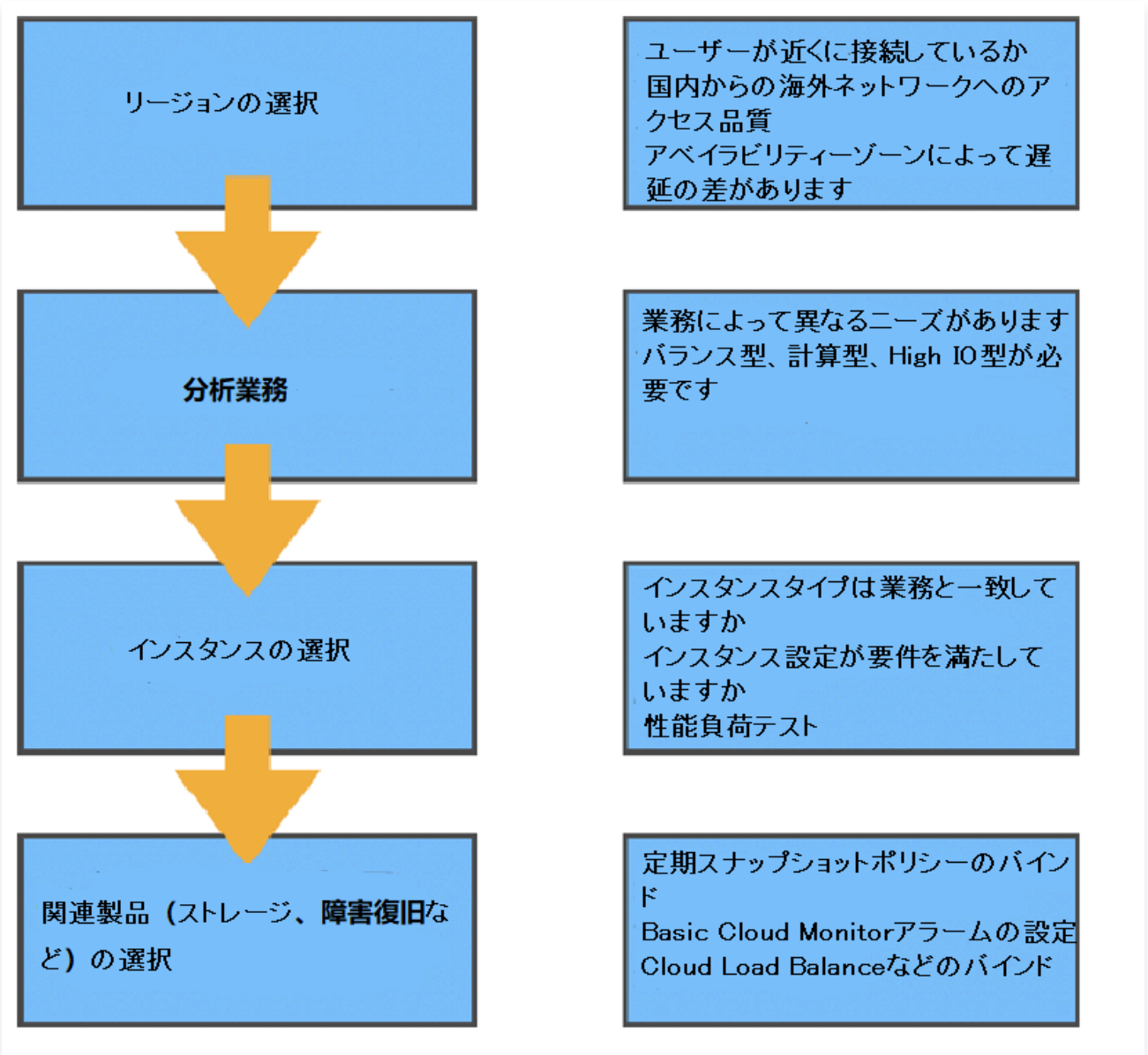
本ドキュメントは、お客様にTencent Cloudの全部また一部の製品・サービスの概要をご紹介することを目的としておりますが、一部の製品・サービス内容は変更される可能性があります。お客様がご購入されるTencent Cloud製品・サービスの種類やサービス基準などは、お客様とTencent Cloudとの間の締結された商業契約に基づきます。別段の合意がない限り、Tencent Cloudは本ドキュメントの内容に関して、明示または黙示の一切保証もしません。

# カタログ：

# 実践チュートリアル
# CVMの選定ガイド
# CVM選定の概要

最終更新日：：2023-04-21 14:42:05

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




## リージョンとアベイラビリティーゾーン

### リージョン

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

### アベイラビリティーゾーン

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

## インスタンスタイプ

Tencent Cloudはさまざまなタイプのインスタンスを提供しており、各インスタンスタイプには複数のインスタンス仕様が含まれています。アーキテクチャに応じて、x86Compute、ARMCompute、ベアメタルCompute、異種Compute(GPU/FPGA)、Batch Computeなどに分けられます。特性・機能により、標準型、計算型、メモリ型、High IO型、ビッグデータ型などに分けられます。ここでは、インスタンスの特性・機能に応じて区分しており、詳細情報は次のとおりです：

#### 標準型

標準型インスタンスの各性能パラメータはバランスが取れており、WebサイトやMiddlewareといったほとんどの通常業務に適しています。標準型インスタンスの主なシリーズは次のとおりです。

- SおよびSAシリーズ：SシリーズはIntelコアであり、SAシリーズはAMDコアです。SAシリーズと比較して、同じ世代および構成のSシリーズは、より強力なシングルコアパフォーマンスを備えていますが、SAシリーズはよりコストパフォーマンスに優れています。
- ストレージ最適化型S5seシリーズ：最新の仮想化テクノロジーSPDKに基づいて、ストレージプロトコルスタックのみを最適化し、CBSの機能を全面的に引き上げるので、大規模データベースやNoSQLデータベースなどのIOバウンド型サービスに適しています。
- ネットワーク最適化型SN3neシリーズ：プライベートネットワークの最大送受信能力は600万ppsで、パフォーマンスは標準型S3インスタンスの約8倍です。プライベートネットワークの帯域幅は最大25Gbpsをサポートしており、プライベートネットワーク帯域幅は標準型S3に比べて2.5倍にもなります。これは、弾幕、ライブストリーミング、ゲームといった高ネットワークパケットの送受信シナリオに適しています。

#### 計算型

計算型Cシリーズインスタンスは、最高のシングルコアコンピューティング性能を備えており、バッチ処理、ハイパフォーマンスコンピューティング、大規模ゲームサーバーなど、コンピューティング集約型アプリケーションに適しています。例えば、高トラフィックのWebフロントエンドサーバー、MMO（マッシブリー・マルチプレイヤー・オンライン）ゲームサーバーおよびその他のコンピューティング集約型サービスなど。

メモリ型

メモリ型Mシリーズのインスタンスは大容量メモリという特徴を持ち、CPUとメモリの比率が1：8で、メモリ価格が最も安く、主に高性能データベース、分散メモリキャッシュなど、大容量メモリ操作や検索、コンピューティングを必要とするMySQL、Redisなどのアプリケーションに適しています。

High IO型

High IO型ITシリーズインスタンスデータディスクはローカルディスクストレージであり、最新のNVME SSDストレージを搭載し、高いランダムIOPS、高スループット、低アクセスレイテンシーといった特徴を備えており、低コストで非常に高いIOPSを提供します。ハードディスクの読み取り・書き込みや遅延に対して高い要件のある高性能データベースなど、例えば、高性能のリレーショナルデータベース、ElasticsearchといったIOバウンド型業務などのI/Oバウンド型アプリケーションに適しています。

> 説明：
> ITシリーズインスタンスのデータディスクはローカルストレージであるため、データが失われるリスクがあります（ホストがダウンした場合など）。お客様のアプリケーションにデータ信頼性アーキテクチャがない場合は、CBSをデータディスクとして選択できるインスタンスの使用を強く推奨します。

ビッグデータ型

ビッグデータ型Dシリーズインスタンスはマスストレージリソースを搭載し、高スループットという特徴を備えており、Hadoop分散コンピューティング、大量のログ処理、分散ファイルシステム、大型データウェアハウスなど、スループット集約型アプリケーションに適しています。

> 説明：
> ビッグデータモデルDシリーズインスタンスのデータディスクはローカルディスクであるため、データが失われるリスクがあります（ホストがダウンしている場合など）。アプリケーションにデータ信頼性アーキテクチャがない場合は、CBSをデータディスクとして選択できるインスタンスの使用を強く推奨します。

異種Compute

異種コンピューティングインスタンスはGPU、FPGAなどの異種ハードウェアを搭載し、リアルタイムの高速並列計算と浮動小数点演算機能を備え、ディープラーニング、科学計算、ビデオコーデック、グラフィックワークステーションなどの高性能アプリケーションに適しています。
NVIDIA GPUシリーズのインスタンスは、主流のT4/V100や最新世代のA100などを含めたNVIDIA Teslaシリーズの GPUを採用しており、優れた汎用コンピューティング機能を提供します。ディープラーニングのトレーニング/推論、計算科学などのアプリケーションシナリオでのベストな選択肢です。

Cloud Physical Machine2.0

Cloud Physical Machine2.0は、Tencent Cloudの最新仮想化テクノロジーに基づいて開発された究極のパフォーマンスを備えたECSベアメタルCVMです。Cloud Physical Machine2.0は、仮想マシンの柔軟性と物理マシンの高い安定性を兼ね備え、NetworkingやデータベースといったTencent Cloudの全製品とシームレスに統合します。Cloud Physical Machine2.0インスタンスマトリックスは、標準、High IO、ビッグデータおよび異種Computeのシナリオを網羅し、クラウド専用の高性能かつ安全に分離された物理サーバークラスターを分単位で構築できます。同時に、サードパーティの仮想化プラットフォームをサポートでき、高度にネストされた仮想化テクノロジーによって、AnyStackのハイブリッドデプロイを実現し、先進的かつ効率的なハイブリッドクラウドソリューションを構築することができます。

高性能Computeクラスター

高性能Computeクラスターは、Cloud Physical Machine2.0をコンピューティングノードとして使用し、高速RDMA相互接続ネットワークサポートを提供するクラウド上のComputeクラスターです。自動車シミュレーション、流体力学、分子動力学といった大規模なコンピューティングシナリオを幅広くサポートできます。また、大規模な機械学習トレーニングなどのシナリオをサポートできる、高性能の異種リソースを提供します。

CVMのインスタンスタイプの関連情報の詳細については、インスタンス仕様 をご参照ください。

## 一般的なビジネスシナリオのタイプ選択に関する推奨事項

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

| | | | |
|---|---|---|---|
| ビッグデータ | HadoopES | ビッグデータ業務はマスストレージを必要とし、IOスループットに所定の要件があるため、専用のビッグデータ型Dシリーズをお勧めします（ローカルディスクモデルはデータが失われるリスクがあるため、データのバックアップに注意してください）。 | ビッグデータ型Dシリーズ |
| 高性能Compute | StarCCMW RF-Chem | 高性能Computeの業務には、究極とも言える単一マシンの計算機能が必要であるとともに、効率的なマルチマシン拡張も必要です。高速RDMAネットワークを搭載した高性能Computeクラスターまたは計算型インスタンスファミリーをお勧めします。 | 高性能Computeクラスター計算型Cシリーズ |
| 仮想化 | KvmOpenStack | 仮想化アプリケーションでは、クラウド上のサーバーが、パフォーマンスのオーバーヘッドを追加することなく、ネストされた仮想化の機能を備え、仮想化機能を従来の物理マシンと一貫性のある状態に保つ必要があります。Cloud Physical Machine2.0製品をお勧めします。 | 高性能ComputeクラスターCloud Physical Machine2.0 |
| ビデオレンダリング | UnityUE4 | ビデオレンダリングシナリオには、DirectXやOpenGLなどのグラフィック・画像処理APIのサポートが必要です。 GPUレンダリングタイプGN7vwをお勧めします。 | GPUレンダリング型GN7vw |
| AI Compute | TensorFlow CUDA | AI Compute業務には並列処理機能が必要であり、GPUコンピューティング機能やグラフィックメモリに対する明確な要件があります。 | GPU計算型高性能Computeクラスター |

# 関連製品

## 一般的なクラウド製品のマッチングに関する推奨事項

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

わせることをお勧めします。


## 他のクラウド製品

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

- スナップショット
  スナップショットは、手軽で効率的なデータ保護サービスであり、非常に重要で効果的なデータ障害復旧対策でもあります。日常的なデータバックアップ、迅速なデータリカバリ、本番データの複数レプリカアプリケーション、迅速なデプロイ環境といったビジネスシナリオで使用することをお勧めします。スナップショットの作成には少額の料金がかかります。詳細については、スナップショットの料金概要 をご参照ください。
- TCOP
  クラウドリソースのTCOPアラームの設定は、業務の保証にとって同様に重要な役割を果たします。TCOPを使用して、クラウド製品のリソース使用率、アプリケーション性能やクラウド製品の実行状況を全面的に理解することができます。TCOPは、マルチインデックスモニタリング、カスタムアラーム、クロスリージョン/クロスプロジェクトインスタンスのグループ化、カスタムモニタリング、視覚化DashboardおよびPrometheusホスティングサービスといった機能もサポートします。クラウド製品に生じた緊急事態をタイムリーに制御かつ対処できるよう支援することによって、システムの安定性を高め、運用・保守の効率を向上させ、運用・保守のコストを削減します。
- CLB
  業務にシングルポイントのオペレーショナルリスクを発生させたくない場合は、CLBの設定を選択できます。CLBサービスは、仮想サービスアドレス(VIP)を設定することにより、同じリージョンにある複数のCVMリソー

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

## 関連ドキュメント

- リージョンとアベイラビリティーゾーン
  – インスタンス仕様

# 課金モデルの選択

最終更新日：：2021-02-02 19:44:55

Tencent Cloud CVM インスタンスには、従量課金とスポットインスタンスの2通りの課金方法があります。

- 従量課金：CVMインスタンスの柔軟な課金モードであり、実際に使用したリソース量に応じて料金が請求されます。従量課金により、いつでも要件を満たすためにリソースを有効化したりリリースしたりすることができます。秒単位まで正確で、前払いの必要がなく、1時間ごとに決済されます。この課金モードは、Eコマースでのフラッシュセールなど、デバイスのニーズが瞬時に大幅に変動したユースケースに最適です。
- スポットインスタンス：CVMの新しいインスタンス運用モードで、従量課金モードと同様に、後払いモード（秒単位で請求され、1時間ごとに決済）に属します。スポットインスタンスは、需要に応じて時間単価が変動します。従量課金と比較して大幅な割引があり、同じ仕様の従量課金制インスタンスの価格の約10%～20%です。ただし、スポットインスタンスは、在庫不足または他のユーザーからの競争入札により、システムによって自動的にインスタンスをリサイクルされる場合があります。

従量課金とスポットインスタンスの両方の課金方法は、さまざまなシナリオでユーザーの要件を満たすことができます。詳細については、課金方法 をご覧ください。

# インスタンスタイプの選択

最終更新日：：2020-03-03 10:13:16

さまざまな顧客の異なるユースケースの要件を満たすために、Tencent Cloudは、次のユースケースでのインスタンスタイプの選択肢を提案しています。

| ユースケースタイプ | 推奨インスタンスタイプ | 説明 |
| --- | --- | --- |
| 個人ウェブサイト | 標準型インスタンス | 中小規模のWebアプリケーション、中小規模のデータベースなどの汎用ワークロードに適しています。 |
| 企業ウェブサイト/ Eコマース/App | 標準型インスタンス | 中小規模のWebアプリケーション、中小規模のデータベースなどの汎用ワークロードに適しています。 |
| リレーショナルデータベース/分散式キャッシュ | メモリ型インスタンス | 大量のメモリ操作、ルックアップ、およびコンピューティングを必要とするユースケースに適しています。 |
| NoSQLデータベース | ハイIO型インスタンス | MongoDB、クラスターデータベースなど、ディスクの読み取り/書き込みおよびレイテンシー要件の高いI/O集約型ユースケースに適しています。 |
| 高性能コンピューティング | • コンピューティング型インスタンス<br>• コンピューティングネットワーク強化型インスタンス | 大型PCゲーム/高性能エンジニアリング科学アプリケーション/ビデオコーデックなど、高いコンピューティングリソースの消費を必要とするユースケースに適しています。 |
| 高性能PCゲーム | • コンピューティング型インスタンス<br>• コンピューティングネットワーク強化型インスタンス | 大型PCゲーム/高性能エンジニアリング科学アプリケーション/ビデオコーデックなど、高いコンピューティングリソースの消費を必要とするユースケースに適しています。 |
| モバイルゲーム/ブラウザーゲーム | • コンピューティング型インスタンス | 大型PCゲーム/高性能エンジニアリング科学アプリケーション/ビデオコーデックなど、高いコンピューティングリソースの消費を必要とするユースケースに適しています。 |

| | | |
|---|---|---|
| | • コンピューティングネットワーク強化型インスタンス | |
| ライブブロードキャスト | • 標準ネットワーク強化型インスタンス<br>• コンピューティングネットワーク強化型インスタンス | 25G ENIを搭載することで、ネットワークパフォーマンスは通常の万兆データセンターの2.5倍になり、帯域幅が大きくなり、レイテンシーが短くなります。 |
| 金融 | CVM Dedicated Host標準型インスタンス | 通常の標準型と比較して、物理サーバーを専用し、リソースを隔離し、安全かつ制御可能で、CVM仕様をカスタマイズ可能です。セキュリティが規格に適合し、金融業界のより厳しい規制要件を満たします。 |
| 科学コンピューティング | GPUコンピューティング型インスタンス | 深層学習や、流体力学コンピューティング、金融コンピューティング、ゲノミクス研究、環境分析、高性能コンピューティングなどの科学コンピューティング、およびその他のサーバー側GPUのワークロードコンピューティングに適しています。 |
| 機械学習 | GPUコンピューティング型インスタンス | 深層学習や、流体力学コンピューティング、金融コンピューティング、ゲノミクス研究、環境分析、ハイパフォーマンスコンピューティングなどの科学コンピューティング、およびその他のサーバー側GPUのワークロードのコンピューティングに適しています。 |
| レンダリング | GPUレンダリング型インスタンス | 非線形編集、ビデオコーデック、グラフィックス加速視覚化、3Dデザインなどの GPUレンダリングシナリオに適しています。 |
| Hadoop/Spark/Elastic Search | ビッグデータインスタンス | Hadoop（HDFS/MapReduce/Spark/Hiveなど）分散式コンピューティング、超並列処理（MPP）データウェアハウスなどのシナリオ、B8ログまたはデータ処理アプリケーションなどに適しています。 |

その他のユースケースについては、インスタンス仕様 をご参照ください。

# ストレージメディアの選択

最終更新日：：2025-07-18 12:01:15

インスタンスを設定するときに、ローカルディスクまたはCloud Block Storageをシステムディスクまたはデータディスクとして選択できます。ストレージメディアを選択する前に、ローカルディスク 及びCloud Block Storage 両方の特徴およびユースケースの違いをよく理解してください。

ご注意：

- 選択したインスタンスの仕様に応じて、購入ページに表示されるシステムディスクとデータディスクのタイプが異なります。例えば、高IOインスタンスタイプを選択したユーザだけがSSDローカルディスクを選択できます。
- ローカルディスクを使用するCVMインスタンス（システムディスクとデータディスクを含む）は、設定（CPU、メモリ、ディスク）のアップグレードをサポートしません、帯域幅のアップグレードのみをサポートします。
- システムディスクのメディアタイプは、購入後に変更できません。

ストレージメディア（SATA HDDローカルディスク、NVME SSDローカルディスク、高性能CBS及びSSD CBS）の違いとユースケースを次の表に示します。

| ストレージメディア | 優位性 | 適用ケース |
| --- | --- | --- |
| NVME SSD ローカルディスク（高 IO モデル IT3、IT5 などでのみサポート） | 低遅延：マイクロ秒のアクセス遅延を提供します。 | 一時的な読み取りキャッシュとして使用：NVME SSD ローカルディスクのランダムリード性能（4KB/8KB/16KBランダム読み取り）は高性能で、MySQL、Oracle などのリレーショナルデータベースの読み取り専用スレーブデータベースとして最適です。<br>メモリのコストはソリッドステートディスクに比べ高額であることから、NVME SSD ローカルディスクをRedis、Memcache などのキャッシュタイプサービスのセカンダリキャッシュとしても使用できます。<br>注意：NVME SSD ローカルディスクには単一障害点リスクが存在することから、データの可用性を確保するために、アプリケーション層でデータの冗長性を確保することをお勧めします。またコアビジネスにはSSD CBSを使用することをお勧めします。 |
| SATA HDD ローカルディスク（ビッグデータモデル | • 低価格で、コールドデータのバックアップ、アーカイブなど | EMR などのビッグデータ処理など大きなファイルのシーケンシャルリード/ライトシナリオに最適です。 |

| | | |
|---|---|---|
| D2 などでのみサポート) | のサービスに使用できます。<br>• 高スループット：ローカルのメカニカルハードディスクのスループットを提供します。 | |
| 高性能CBS | I/Oシナリオの90%に適しており、高品質、低価格のベストチョイスです。 | 中小規模データベース、Webサーバーなどのシナリオに最適で、長期的に安定したIOパフォーマンスの出力を提供します。コアビジネスのテスト、開発調整環境のIO要件を満たしています。 |
| SSD CBS | 高性能と高いデータ信頼性：業界最高レベルのNVMeソリッドステートストレージをディスクメディアとして使用します。I/O集約型サービスに適しており、長期的に安定した、超高パフォーマンスの単一ディスクを提供します。 | 次のシナリオに適用可能：<br>• 中規模および大規模データベース：MySQL、Oracle、SQL Serverなど、数百万行のテーブルを含む中規模および大規模のリレーショナルデータベースアプリケーションをサポートします。<br>• コアサービスシステム：高いデータ信頼性を必要とするI/O集約型などのコアサービスシステム。<br>• ビッグデータ分析：TB、PBレベルのデータに対する分散処理機能を提供します。データ分析、データマイニング、ビジネスインテリジェンスなどの領域に適しています。 |

- CBSのタイプ、ケースの詳細ついては、Cloud Block Storageタイプ をご参照ください。
- CBSの価格情報については、Cloud Block Storage価格一覧 をご参照ください。

# ネットワークの計画

最終更新日：：2020-03-03 10:27:04

Tencent Cloud のVirtual Private Cloud(VPC)は、Tencent Cloud上でユーザーによってカスタマイズされる論理的に隔離されたネットワークスペースです。VPCでは、ユーザーはIPレンジ、IPアドレス、およびルーティングポリシーなどを自由に定義できますので、VPCを選択していただくことをお薦めします。
ユーザーがTencent Cloud VPCをより使いやすくするために、Tencent Cloudは以下のネットワーク計画に関するの提案をご提供します。

## VPC数の確定

- 既知の特性：
  - プライベートネットワーク間はデフォルトでは相互通信ができません。異なるプライベートネットワーク間の相互通信が必要な場合、ピアリング接続 またはクラウドコネクトネットワーク（CCN） を使ってください。
  - デフォルトでは、同じVPCの異なるアベイラビリティーゾーン間でプライベートネットワークが相互接続できます。
- 関連提案：
  - サービスには複数のリージョンでシステムをデプロイする必要がある場合、複数のVPCを使用する必要があります。アクセスのレイテンシーを低減し、アクセス速度を上げるには、お客様に近いリージョンでVPCを作成することができます。
  - 現在のリージョンに複数のサービスがデプロイされており、異なるサービス間でネットワークを隔離させたい場合、サービスごとに現在のリージョンで対応するVPCを作成することができます。
  - 複数のリージョンでデプロイする要件がなく、サービス間でネットワークを隔離させる要件もない場合、1つのVPCのみを使用することもできます。

## サブネット化の確定

- 既知の特性：
  - サブネットはVPC内のIPアドレスブロックであり、VPC内のすべてのクラウドリソースはサブネットにデプロイする必要があります。
  - 同じVPCでサブネットIPレンジが重複することはできません。
  - 現在、Tencent Cloud VPCは、10.a.0.0 / 8（aは0–255に属する）、172.b.0.0 / 16（bは0–31に属する）、および192.168.0.0/16の3つのプライベートIPレンジをサポートしています。
  - VPCが正常に作成されると、IPレンジは変更できません。
- 関連提案：
  - VPCのサブネット計画のみであり、基幹ネットワークまたはIDCとのネットワーク通信が発生しない場合、上記IPレンジのいずれかを選択してサブネットを新規作成できます。

- 基幹ネットワークとの通信が必要な場合は、必要に応じて10.[0～47].0.0/16およびそのサブセットのネットワークを作成してください。
- VPNの確立が必要な場合、エンドIPレンジ(VPC IPレンジ)と対向側IPレンジ(お客様のIDC IPレンジ)は重複できないため、サブネットを新規作成する場合、対向側IPレンジを避ける必要があります。
- IPレンジを分割する際に、IPレンジのIP容量、つまり使用可能なIPの数も考慮する必要があります。
- 最後に、同じVPCのサービス内のサービスモジュールをもとにサブネットを細分化することをお勧めします。たとえば、サブネットAはWeb層に使用し、サブネットBをロジック層に使用し、サブネットCをDB層に使用することは、ネットワークACLと連携してアクセス制御とフィルタリングするのに便利です。

## ルーティングポリシーの確定

- 既知の特性:
  –ルートテーブルは一連のルーティングルールで設定され、VPC内のサブネットのアウトバウンドトラフィック方向を制御ために使用されます。
  –各サブネットはルートテーブルに関連付ける必要があり、また1つのルートテーブルにのみ関連付けることができます。
  - 各ルートテーブルは、複数のサブネットに関連付けることができます。
  - ユーザーがVPCを作成する際に、デフォルトのルートテーブルが自動的に生成されます。デフォルトのルートテーブルは、VPCのプライベートネットワークが相互接続することを意味します。
- 関連提案:
  - サブネットのトラフィック方向で特別な制御を行う必要がない場合、デフォルトでVPCのプライベートネットワークが相互接続する場合、デフォルトのルートテーブルを使用でき、カスタマイズのルーティングポリシーを設定する必要はありません。
  - サブネットのトラフィック方向に特別な制御が必要な場合は、公式サイトで ルートテーブル の使用詳細をご参照ください。
- VPCの詳細については、Virtual Private Cloud をご参照ください。

# セキュリティグループの設定

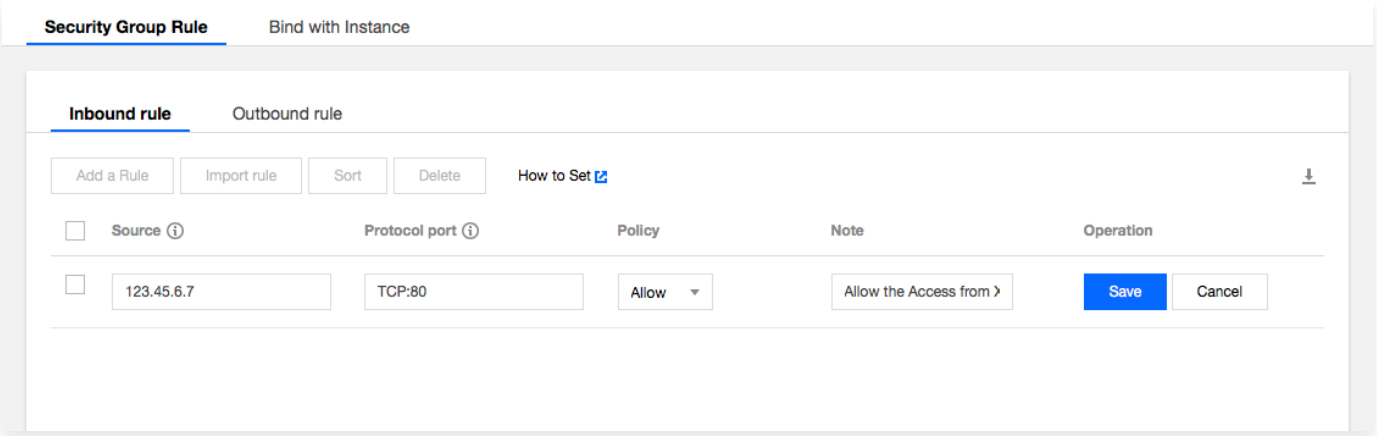
最終更新日：：2022-07-27 16:25:30

このドキュメントでは、新しいセキュリティグループの作成を例に、インスタンスのカスタマイズ設定の際に、Tencent Cloudが提供するセキュリティグループルールを使用してセキュリティグループの初回設定を行う方法についてご説明します。セキュリティグループに関するより多くの操作は、CVMコンソールのセキュリティグループ画面で行うことができます。詳細については、セキュリティグループの概要 をご参照ください。

## セキュリティグループの設定

1. セキュリティグループの設定の際は、実際のニーズに応じて、下図のように新しいセキュリティグループを選択します。

   > 説明：
   > 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。




2. 実際のニーズに応じて、オープンにしたいIP/ポートにチェックを入れます。
   セキュリティグループの新規作成には以下のルールを提供します。
   - ICMP：ICMPプロトコルをオープンにし、パブリックネットワークPingサーバーを許可します。
   - TCP:80：ポート80をオープンにし、HTTPによるWebサービスへのアクセスを許可します。
   - TCP:22：ポート22をオープンにし、SSHLのLinux CVMへのリモート接続を許可します。
   - TCP:443：ポート443をオープンにし、HTTPSによるWebサービスへのアクセスを許可します。
   - TCP:3389：ポート3389をオープンにし、RDPのWindows CVMへのリモート接続を許可します。
   - プライベートネットワークをオープン：プライベートネットワークをオープンにし、異なるクラウドリソース間のプライベートネットワークが互換性（IPv4）を有することを許可します。

> 説明：

- オープンにしたいIP/ポートにチェックを入れると、**セキュリティグループのルール**に詳細なセキュリティグループのインバウンド/アウトバウンドルールが表示されます。
- 業務上、他のポートをオープンにする必要がある場合は、セキュリティグループの応用例 を参照して セキュリティグループの新規作成 を行うこともできます。セキュリティ上の観点から、Tencent Cloudはなるべく業務に必要なポートのみをオープンにすることで不要なリスクを避けることをお勧めしています。

## セキュリティグループのルール

インバウンドルール：セキュリティグループに関連付けられたCVMへの到達が許可されたインバウンドトラフィックを表します。
アウトバウンドルール：CVMから出るアウトバウンドトラフィックを表します。

- セキュリティグループ内ルールの優先順位：位置が上のものほど優先順位が高くなります。
- CVMがルールのないセキュリティグループにバインドされている場合、すべてのインバウンド、アウトバウンドトラフィックはデフォルトで拒否されます（ルールがある場合は、ルールが優先的に発効します）。
- 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、セキュリティグループの優先順位は数字が小さいものほど優先順位が高くなります。
- 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、優先順位が最も低いセキュリティグループのルール発効はデフォルトで拒否されます。

## セキュリティグループの制限

制限の詳細については、セキュリティグループに関する制限 をご参照ください。

# 環境構築
# 環境構築の概要

最終更新日：：2021-08-12 11:00:57

## シナリオ

このドキュメントでは、CVMにさまざまな開発環境を構築する方法について説明します。CVMをお持ちでない場合は、CVM購入ページ にアクセスして購入してください。

## 操作手順

次のドキュメントを参照して、開発環境を手動でデプロイするか、Tencent Cloud Marketplace イメージを直接使用してワンクリックでデプロイするかを選択できます。

- Linux 環境の構築
- LAMP 環境の構築
- Java Web 環境の構築
- WIPM 環境の構築
- Node.js 環境の構築

環境構築中に問題が発生した場合、 環境構築に関する一般的な問題 ドキュメントをご参考ください。

# IISサービスをインストールする

最終更新日：：2023-05-09 16:40:04

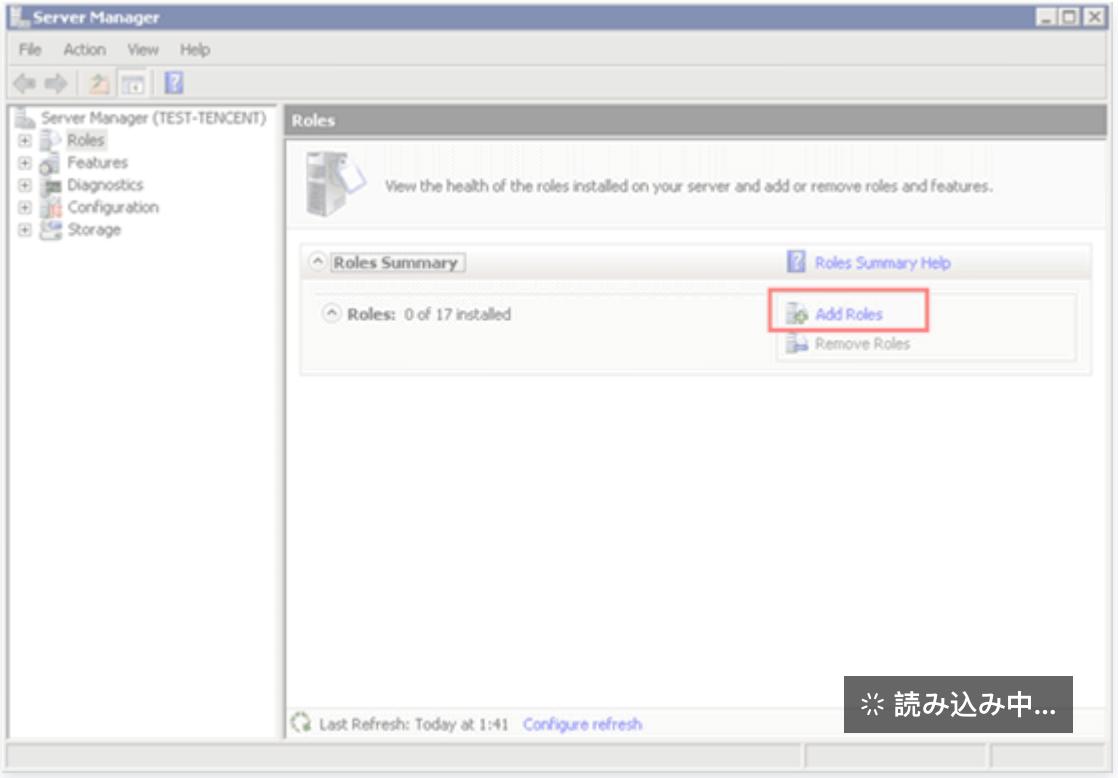
本ドキュメントはWindows 2012 R2 バージョンOSとWindows 2008 バージョンOSでのIISの追加とインストールするプロセスについて説明します。

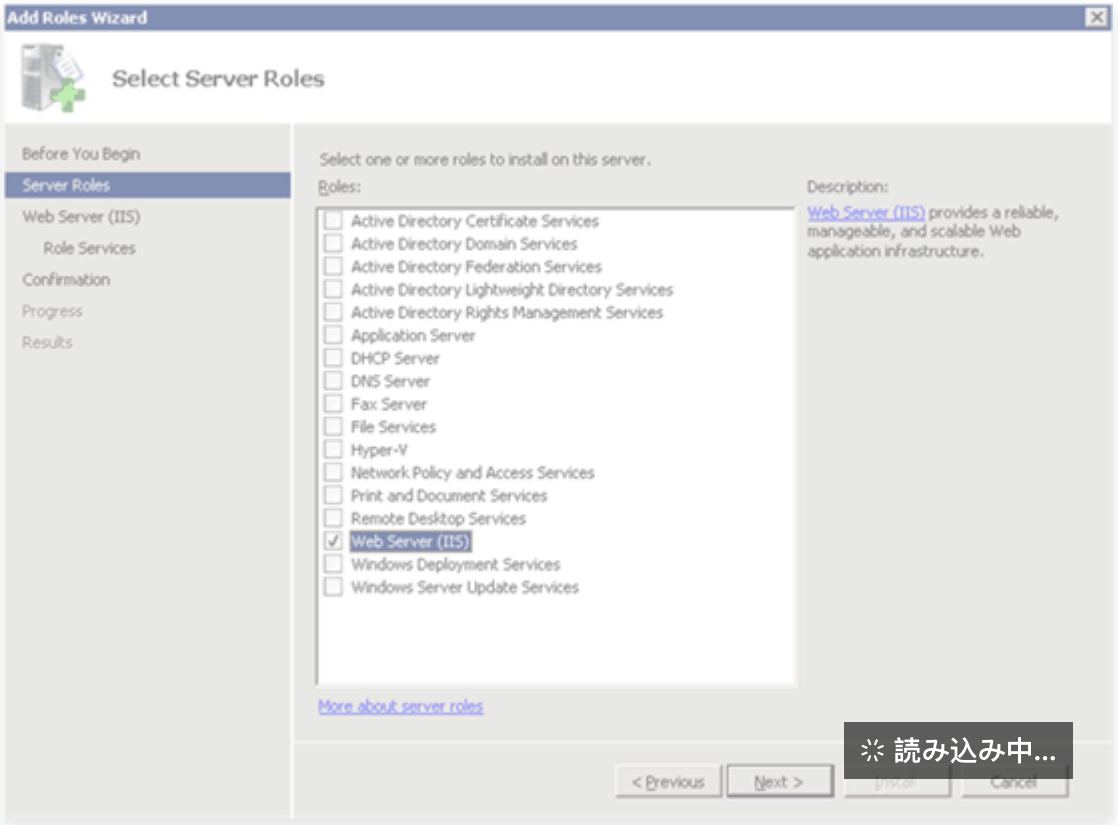
## Windows 2012 R2 バージョン

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

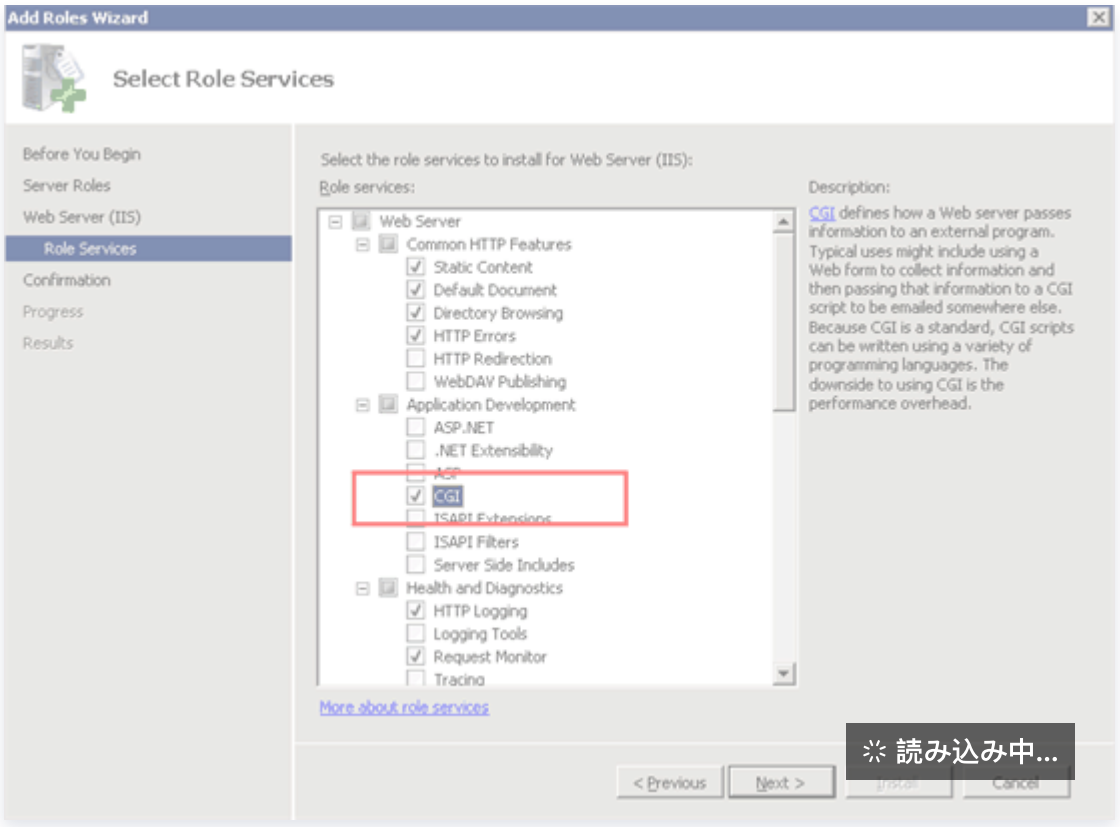
## Windows 2008 バージョン

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

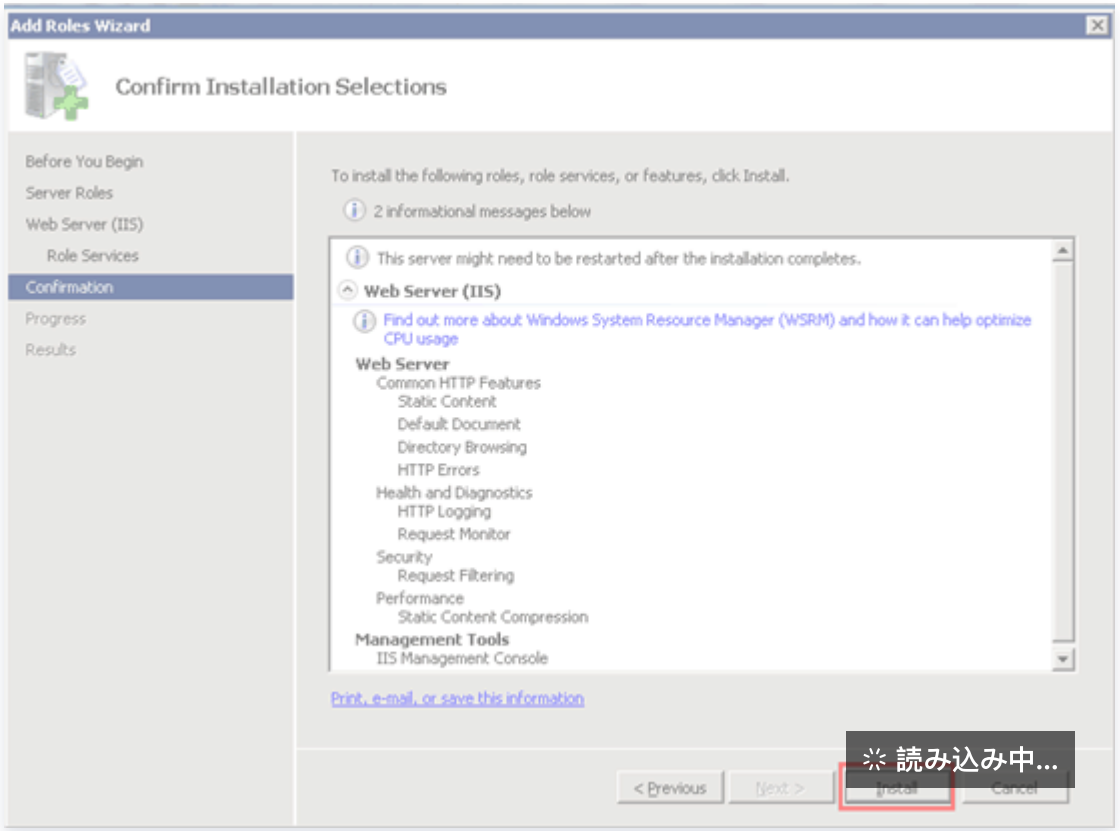


3. 「役割サービス(Role Services」)を選択する時に、「CGI」オプションをチェックします。




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



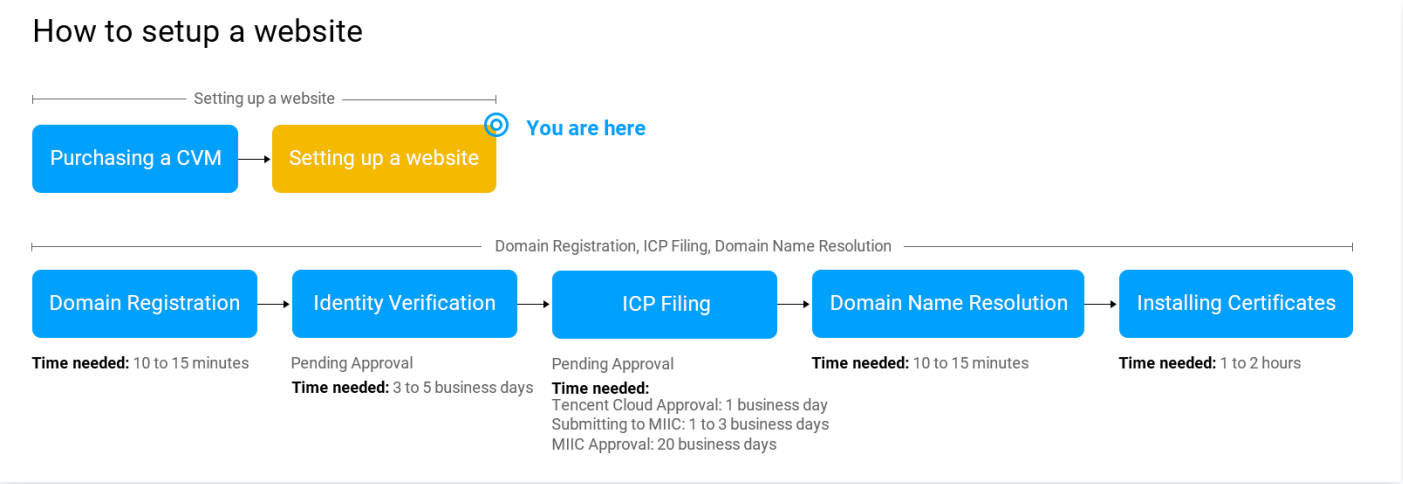
5. ブラウザーを介してWindows CVMのパブリックネットワークIPにアクセスして、IISサービスが正常に実行しているかどうかを確認します。下記のように表示されたら、IISのインストールと設定が成功したことを示しています。

# ウェブサイトの構築
# ウェブサイト構築の概要

最終更新日：：2022-06-29 15:53:06

CVMの購入が完了したら、購入したサーバーにご自分のウェブサイトやフォーラムを構築することができます。

> 説明：
> またLighthouseを使用すれば、「ワンクリックでのサイト構築」もでき、手動での設定が不要になります。作成時に必要なアプリケーションイメージを選択するだけで、個人のウェブサイトを構築することができます。詳細については、Lighthouseの購入方法 をご参照ください。




## 構築方法

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

| 比較項目 | イメージのデプロイ | 手動構築 |
| --- | --- | --- |
| 構築方法 | Tencent クラウドマーケットのシステムイメージから直接インストールしてデプロイすることを選択します。 | 必要なソフトウェアを手動でインストールすると、カスタマイズが可能です。 |
| 特徴 | 付属のソフトウェアのバージョンは比較的固定されています。 | 付属バージョンもフレキシブルに選択することができます。 |
| 所要時間 | 比較的短い時間で、ワンクリックでデプロイできます。 | 比較的時間がかかり、手動で関連ソフトをインストールする必要があります。 |

| | | |
|---|---|---|
| 難易度 | 比較的簡単です。 | ソフトウェアパッケージのバージョンとインストール方法について、ある程度理解している必要があります。 |

## サイトの構築

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

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

| | | |
|---|---|---|
| | | ザーは、個人またはグループでのウェブサイト開発のプラットフォームとしてDrupalを使用することができます。 |
| Ghost | Ghostの手動構築 | Ghostは、Node.jsをベースとして開発されたオープンソースのブログプラットフォームです。すばやいデプロイや簡素化されたオンライン公開プロセスといった機能的特徴により、ユーザーはGhostを使用すれば、個人のブログをすばやく作成することができます。 |
| Microsoft SharePoint 2016 | Microsoft SharePoint 2016の構築 | Microsoft SharePointとは、Microsoft SharePoint Portal Serverの略称で、企業がインテリジェントなポータルサイトを開発できるようにするためのポータルサイトです。このサイトではチームやナレッジとシームレスにつながることができ、ユーザーは関連情報をビジネスプロセスで有効活用し、業務をより効率的に進められるようになります。 |

## 関連する操作

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

# ウェブサイトの構築

最終更新日：：2021-08-12 11:02:11

このドキュメントを参照して、CVM上に独自のWebサイトを構築できます。CVMをお持ちでない場合は、CVM購入ページから購入できます。

## 手順1：Web サイトをデプロイする

Webサイトを手動でデプロイできます。次のドキュメントをご参照ください。

- Webサイトの構築方法
- 個人ブログサイトをWordPressで構築する
- Discuz! フォーラムを構築する
- Drupal サイトを構築する
- Ghostでブログを簡単開設

Webサイトの構築時に問題が発生した場合は、 Webサイト構築に関するFAQドキュメントを参照して問題のトラブルシューティングを行ってください。

## 手順2：Webサイトを公開する

構築されたWebサイトをインターネットに公開し、ユーザーがアクセスできるようにするには、ドメイン名の登録と解析、およびICP登録（中国本土で運用されているWebサイトの場合）を完了する必要があります。

# WordPress個人サイトの構築
# WordPress個人サイトの手動構築（Linux）

最終更新日：：2025-09-05 16:20:02

## 操作シナリオ

WordPressはPHP言語で開発されたブログプラットホームです。WordPressにより個人のブログプラットホームを構築することが可能です。本節はCentOS 7.6 OSのTencent Cloud CVMを例とし、手動でWordPressの個人サイトを構築することについて説明します。
WordPressの個人ブログを構築するには、Linux コマンド（例：CentOS環境におけるYUMによるソフトウェアをインストールする 等の常用コマンドに詳しい必要があります。また、インストールするソフトウェアの利用およびバージョン間の互換性を把握することも必要です。

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

## ソフトウェアのバージョン

本節で構築するWordPress個人サイトの構成バージョンとその説明は次のとおりです：

- Linux：Linux OS、本ドキュメントはCentOS 7.6を例として説明します。
- Nginx：Webサーバー、本節ではNginx 1.17.5を例に説明します。
- MariaDB：データベース、本ドキュメントはMariaDB 10.4.8を例として説明します。
- PHP：スクリプト言語、本ドキュメントはPHP 7.2.22を例とします。
- WordPress：ブログプラットフォーム、本節ではWordPress 5.0.4を例に説明します。

## 操作手順

### ステップ1：CVMにログインする

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

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

### ステップ2：手動でLNMP環境を構築する

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

て、基本的な環境を構築できます。

## ステップ3：データベースを構成する

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

1. 以下のコマンドを実行し、MariaDBに入ります。

```
mysql
```

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

```
CREATE DATABASE wordpress;
```

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

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

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

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

5. 以下のコマンドを実行し、rootアカウントのパスワードを設定します。

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

```
ALTER USER root@localhost IDENTIFIED VIA mysql_native_password USING
PASSWORD('パスワードを入力してください')。
```

6. 以下のコマンドを実行し、すべての構成を有効にします。

```
FLUSH PRIVILEGES;
```

7. 以下のコマンドを実行し、MariaDBを終了します。

```
\q
```

## 手順4：WordPressをインストールして設定する

### WordPressのダウンロード

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

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

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

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

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

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

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

### WordPress設定ファイルの変更

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

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

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

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

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

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

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

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

## ステップ5： WordPress インストールの確認

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

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

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

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

| 必要な情報 | 説明 |
| --- | --- |
| サイトのタイトル | WordPressウェブサイト名。 |
| ユーザー名 | WordPress 管理者の名前。セキュリティのために、 adminと異なる名前を設定することをお勧めします。デフォルトユーザー名であるadmin と比べては、当該名前は一層クラックしにくいようにする必要があります。 |

| | |
|---|---|
| パスワード | デフォルトの強いパスワードまたはカスタマイズパスワードを使用できます。既存のパスワードを重複に使用せず、パスワードを安全の場所に保管してください。 |
| メール | 通知を受信するためのメールアドレスです。 |

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

## 関連する操作

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

## よくあるご質問

CVMの使用中に問題が発生した場合は、下記のドキュメントを参照しながら実際状況に合わせ分析した上で問題を解決することが可能です。

- CVMのログインに関する問題は、パスワードとキー 、ログインとリモート接続 ドキュメントをご参照ください。
- CVMのネットワークに関する問題は、 IPアドレス 、ポートとセキュリティグループ ドキュメントをご参照ください。
- CVMのハードディスクに関する問題は、システムディスクとデータディスク ドキュメントをご参照ください。

# WordPress個人サイトの手動構築（Windows）

最終更新日：：2022-05-06 16:57:27

## 概要

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

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

## ソフトウェアバージョン

WordPressの個人サイトは、PHP 5.6.20以降のバージョンおよびMySQL 5.0以降のバージョンで構築できます。セキュリティを強化するために、WordPressの個人サイトを構築するとき、PHP 7.3以降のバージョンおよびMySQL 5.6以降のバージョンを選択してインストールすることをお勧めします。
このドキュメントでは、構築するWordPressの個人サイトの構成バージョンおよびその説明は次のとおりです：

- Windows：Windows OSです。このドキュメントでは、64ビットの中国語版のWindows Server 2012 R2 Data Center Editionを例として説明します。
- IIS：Webサーバーです。このドキュメントでは、IIS 8.5を例として説明します。
- MySQL：データベースです。このドキュメントでは、MySQL 8.0.19を例として説明します。
- PHP：スクリプト言語です。このドキュメントでは、PHP 7.1.30を例として説明します。
- WordPress：ブログプラットフォームです。このドキュメントでは、WordPress 5.9を例として説明します。

## 操作手順

### ステップ1：CVMにログインする

RDPファイルを使用したWindowsインスタンスへのログイン（推奨）。
また、実際の操作習慣に応じて、リモートデスクトップとの接続によるWindowsインスタンスへのログイン。

### 手順2：WIPM環境を構築する

WIPM環境の手動構築 を参照して、以下のとおり操作します：

1. IISサービスをインストールします。
2. PHP 5.6.20以降のバージョンの環境をデプロイします。

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

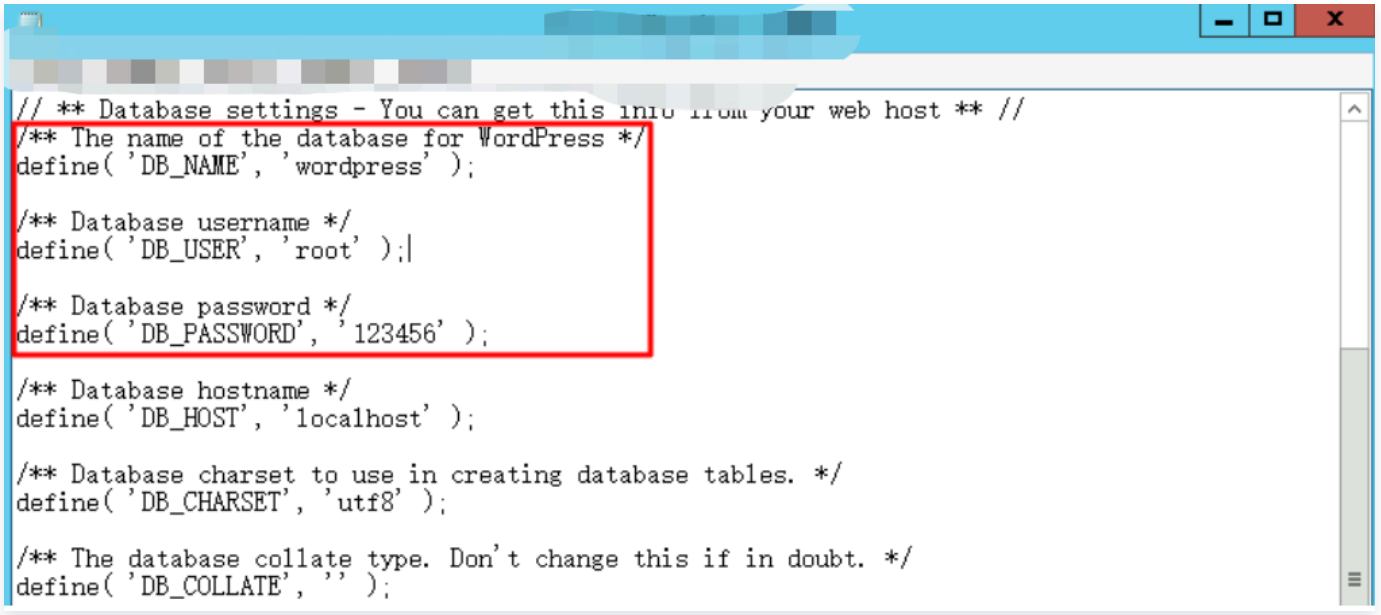
## 手順3：WordPressをインストールして設定する

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

1. WordPressをダウンロードして、WordPressインストールパッケージをCVMに解凍します。
   例えば、WordPressインストールパッケージを `C:\wordpress` ディレクトリに解凍します。
2. > > MySQL 5.6 Command Line Clientをクリックして、MySQLTencent Cloud Command Line Interfaceクライアントを開きます。
3. MySQL Tencent Cloud Command Line Interfaceクライアントでは、次のコマンドを実行して、WordPressデータベースを作成します。
   例えば、「wordpress」データベースを作成します。

```
create database wordpress;
```

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




6. `wp-config.php` ファイルを保存します。

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

## ステップ4：WordPressの設定を確認する

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

| 必要な情報 | 説明 |
| --- | --- |
| サイトタイトル | WordPressウェブサイト名です。 |
| ユーザー名 | WordPress管理者の名前です。セキュリティのために、adminと異なる名前を設定することをお勧めします。デフォルトユーザー名であるadminと比べて、この名前はクラックしにくいです。 |

| | |
|---|---|
| パスワード | 強力なデフォルトパスワードまたはカスタマイズパスワードを使用できます。既存のパスワードを再利用しないでください。また、パスワードを安全な場所に保管してください。 |
| Eメール | 通知を受け取るために使用されるEメールアドレスです。 |

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

## よくあるご質問

CVMの使用中に問題が発生した場合は、下記のドキュメントを参照しながら実際状況に合わせ分析した上で問題を解決することが可能です:

- CVMのログインに関する問題については、パスワードとキー 、ログインとリモート接続 をご参照ください。
- CVMのネットワークに関する問題については、IPアドレス 、ポートとセキュリティグループ をご参照ください。
- CVMのハードディスクに関する問題については、システムディスクとデータディスク をご参照ください。

# Discuz!フォーラムの構築
# Discuz!フォーラムの手動構築

最終更新日：：2022-05-10 11:38:10

## 概要

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

## ソフトウェアのバージョン

この記事で作成したDiscuz!フォーラムソフトウェアのバージョンと説明は次の通り：

- Linux：Linux OS、本ドキュメントはCentOS 7.6を例として説明します。
- Apache：Webサーバー、この記事では、 Apache 2.4.15 を例として説明します。
- MariaDB：データベース、この記事では、 MariaDB 5.5.60を例として説明します。
- PHP：スクリプト言語、この記事では、PHP 5.4.16を例として説明します。
- Discuz!：フォーラムウェブサイトソフトウェア、この記事では、Discuz! X3.4を例として説明します。

## 操作手順

### ステップ1：CVMにログインする

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

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

### 手順2：LAMP環境を構築する

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

#### 必要ソフトウェアをインストールして設定する

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

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

2. 下記のコマンドを順に実行して、サービスを起動します。

```
systemctl start httpd
```

```
systemctl start mariadb
```

```
systemctl start php-fpm
```

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

> ⚠ ご注意：
> - MariaDBに初めてログインする前に、次のコマンドを実行してユーザーパスワードの入力と基本設定を行います。
> - rootパスワードの入力を求めるプロンプトが初めて表示されたら、 Enterを押して rootパスワード設定手順に直接進みます。rootパスワードは設定の際、デフォルトでは画面に表示されません。画面上の指示に従ってその他の基本構成を順に完了してください。

```
mysql_secure_installation
```

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

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

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

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

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

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

MariaDB [(none)]>
```

5. 次のコマンドを実行し、 MariaDBデータベースを終了します。

```
\q
```

## 環境設定の検証

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

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

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

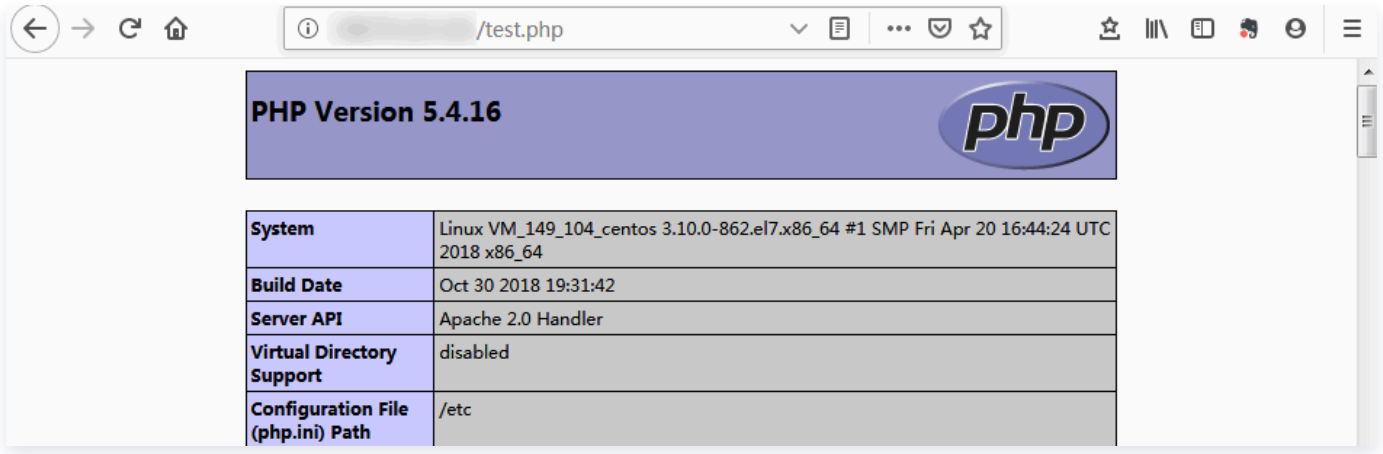
2. iキーを押して編集モードに切り替え、次のように書き込みます。

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

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

```
http://CVMのパブリックIP/test.php
```

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




## 手順3：Discuz!のインストールと設定

### Discuz!をダウンロードする

次のコマンドを実行して、インストールパッケージをダウンロードします。

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

### インストールの準備作業

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

   ```
   cd DiscuzX
   ```

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

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

3. 次のコマンドを実行して、他のユーザーに書き込み権限を割り当てます。

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

### Discuz!をインストールする

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

> 説明:
> 本ドキュメントでは、インストール手順のみ示しています。低いバージョンであるというセキュリティアラートが表示された場合、より高いバージョンのイメージを使用することを推奨します。

2. 同意するをクリックして、インストール環境の確認ページに進みます。
3. 現在のステータスが正常であることを確認して、 次のステップをクリックし、実行環境の設定ページに進みます。
4. クリーンインストールを選択して、次のステップをクリックし、データベースの作成ページに進みます。
5. 画面上の指示に従って、情報を記入し、Discuz!のデータベースを作成します。

> ご注意:
> - 必要なソフトウェアのインストール で設定したrootアカウントとパスワードを利用してデータベースに接続し、システムメールボックス、管理者アカウント、パスワード、およびEmailを設定してください。
> - 管理者ユーザーとパスワードを覚えておいてください。

6. 次のステップをクリックしてインストールを開始します。
7. インストールが完了したら、フォーラムのインストールが完了しました。ここをクリックしてアクセスしてくださいをクリックすれば、フォーラムにアクセスできます。

## 関連操作

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

## よくあるご質問

CVMの使用中に問題が発生した場合は、下記のドキュメントを参照しながら実際状況に合わせ分析した上で問題を解決することが可能です。

- CVMのログインに関する問題は、パスワードとキー 、ログインとリモート接続 ドキュメントをご参照ください。
- CVMのネットワークに関する問題は、 IPアドレス 、ポートとセキュリティグループ ドキュメントをご参照ください。
- CVMのハードディスクに関する事項については、システムディスクとデータディスク をご参照ください。

# Ghostブログの手動構築

最終更新日：：2021-11-01 15:45:25

## 操作シナリオ

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

## ソフトウェアバージョンの例

ここでGhostブログの作成に使用するOSおよびソフトウェアのバージョンと説明は次のとおりです。

- OS：ここではUbuntu 20.04を例として説明します。
- Nginx：Webサーバー。ここではNginx 1.18.0を例として説明します。
- MySQL：データベース。ここではMySQL 8.0.25を例として説明します。
- Node.js：実行環境。ここではNode.js 14.17.0バージョンを例として説明します。
- Ghost：オープンソースブログプラットフォーム。ここではGhost 4.6.4バージョンを例として説明します。

## 前提条件

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

## 操作手順

### ステップ1：Linuxインスタンスにログインする

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

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

### 手順2：新規ユーザーの作成

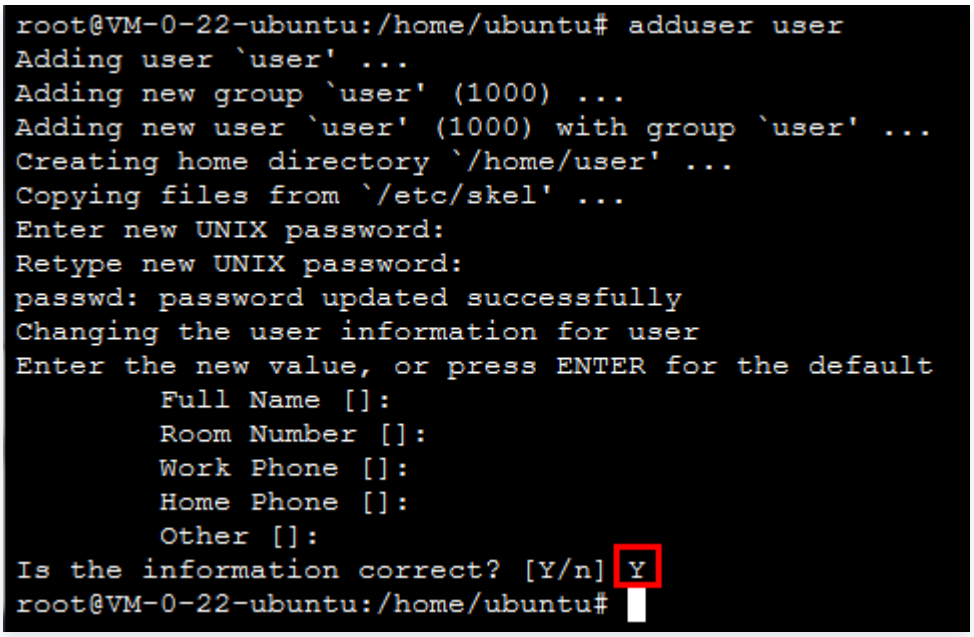
1. Ubuntu OSのCVMにログインした後、Ubuntuシステムでrootユーザーを使用してログイン を参照して、rootユーザーに切り替えてください。

2. 以下のコマンドを実行し、新規ユーザーを作成します。ここでは `user` を例とします。

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

```
adduser user
```

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




6. 以下のコマンドを実行し、ユーザー権限を追加します。

```
usermod -aG sudo user
```

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

```
su - user
```

## 手順3：インストールパッケージの更新

以下のコマンドを順に実行して、インストールパッケージを更新します。

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

```
sudo apt-get update
```

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

## 手順4：環境の構築

### Nginxのインストールと設定

以下のコマンドを実行し、Nginxをインストールします。

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

### MySQLのインストールと設定

1. 以下のコマンドを実行し、MySQLをインストールします。

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

2. 以下のコマンドを実行し、MySQLに接続します。

   ```
   sudo mysql
   ```

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

   ```
   CREATE DATABASE ghost_data;
   ```

4. 以下のコマンドを実行し、rootアカウントのパスワードを設定します。

   ```
   ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY
   'rootアカウントパスワード入力';
   ```

5. 以下のコマンドを実行し、MySQLを終了します。

```
\q
```

### Node.jsのインストールと設定

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

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

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

2. 以下のコマンドを実行し、Node.jsをインストールします。

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

### Ghost-CLIのインストール

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

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

## 手順5：Ghostのインストールと設定

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

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

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

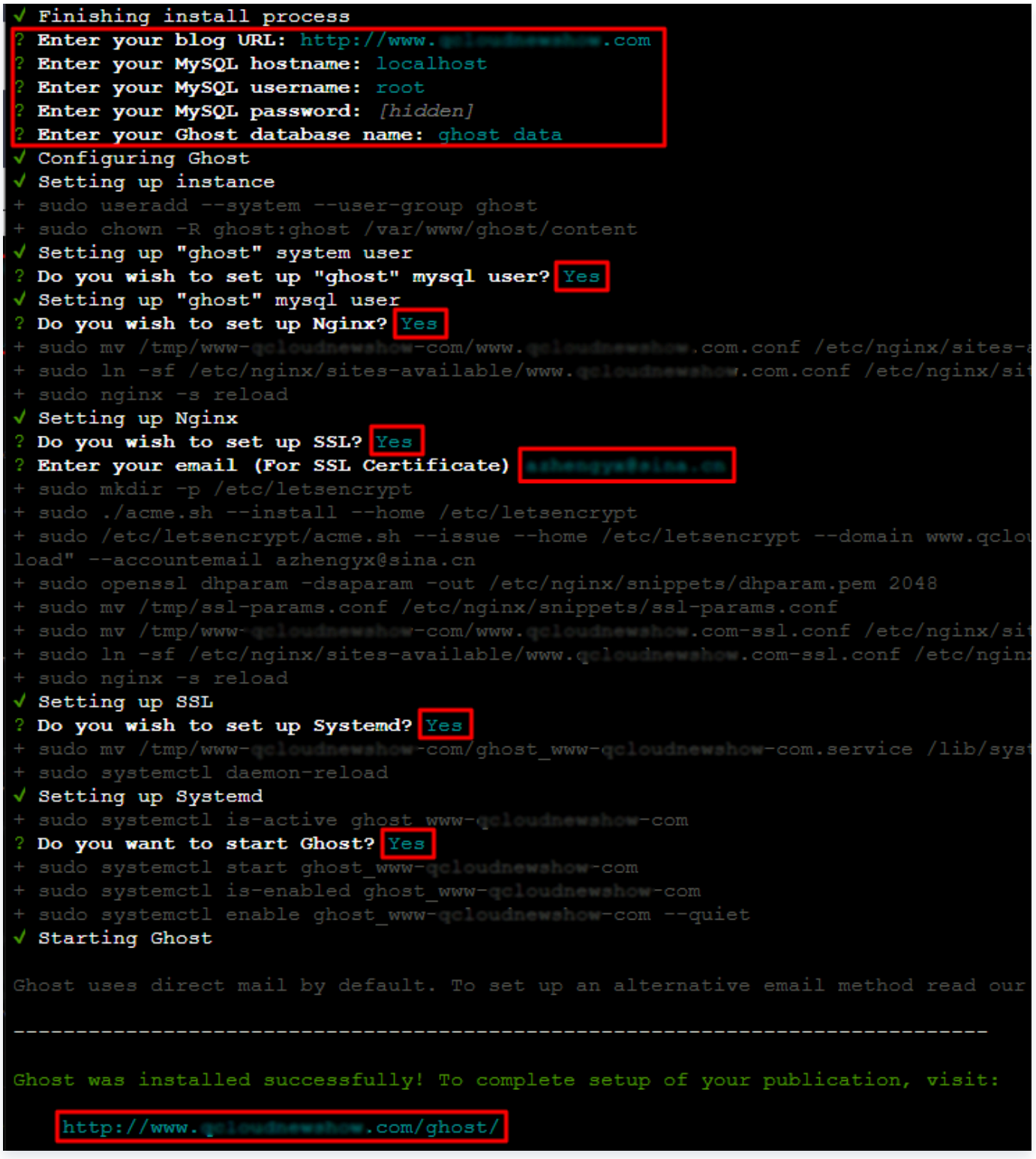
```
sudo chmod 775 /var/www/ghost
```

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

2. 以下のコマンドを実行し、インストールプログラムを実行します。

```
ghost install
```

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

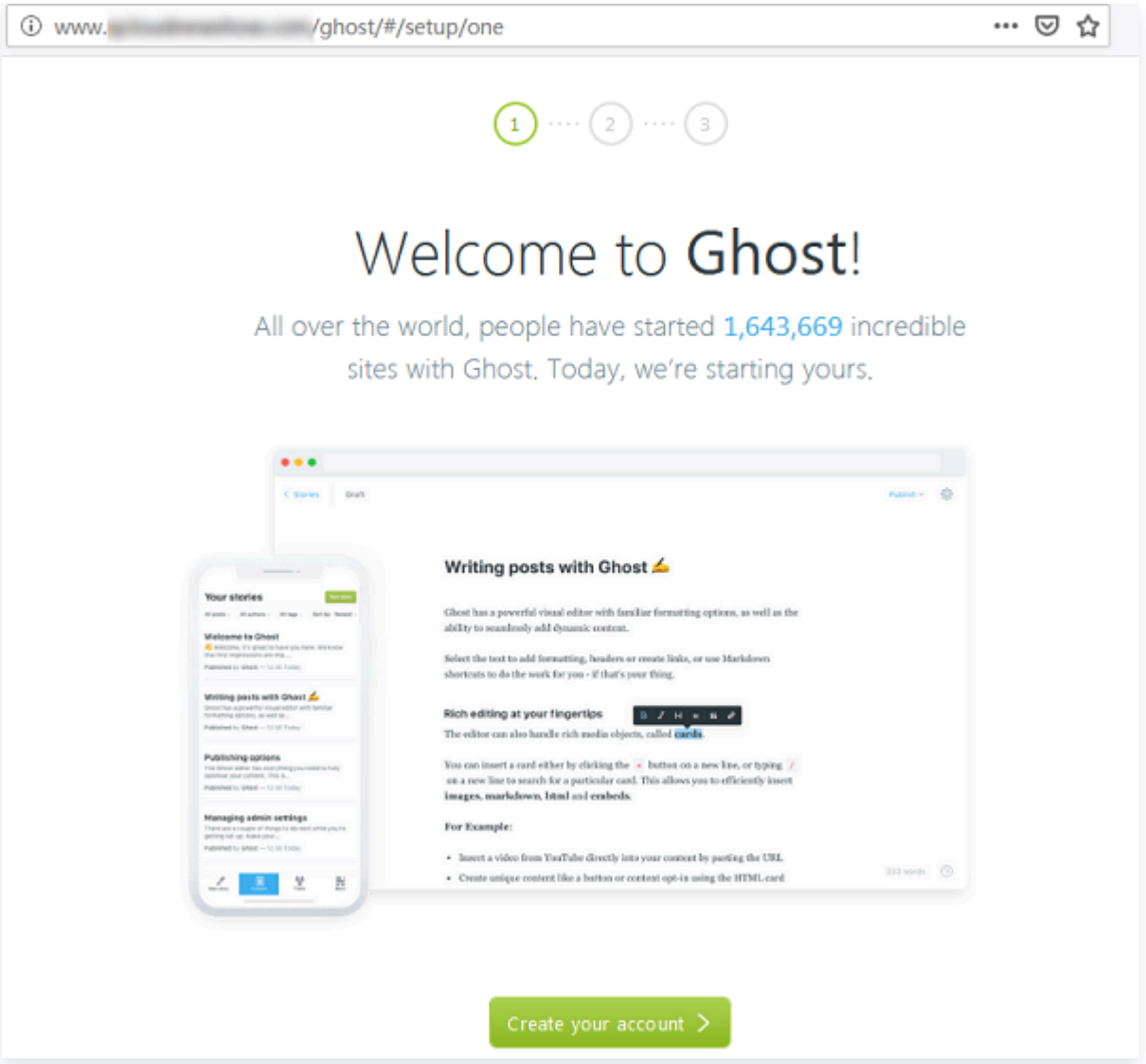



主要な設定は次のとおりです。

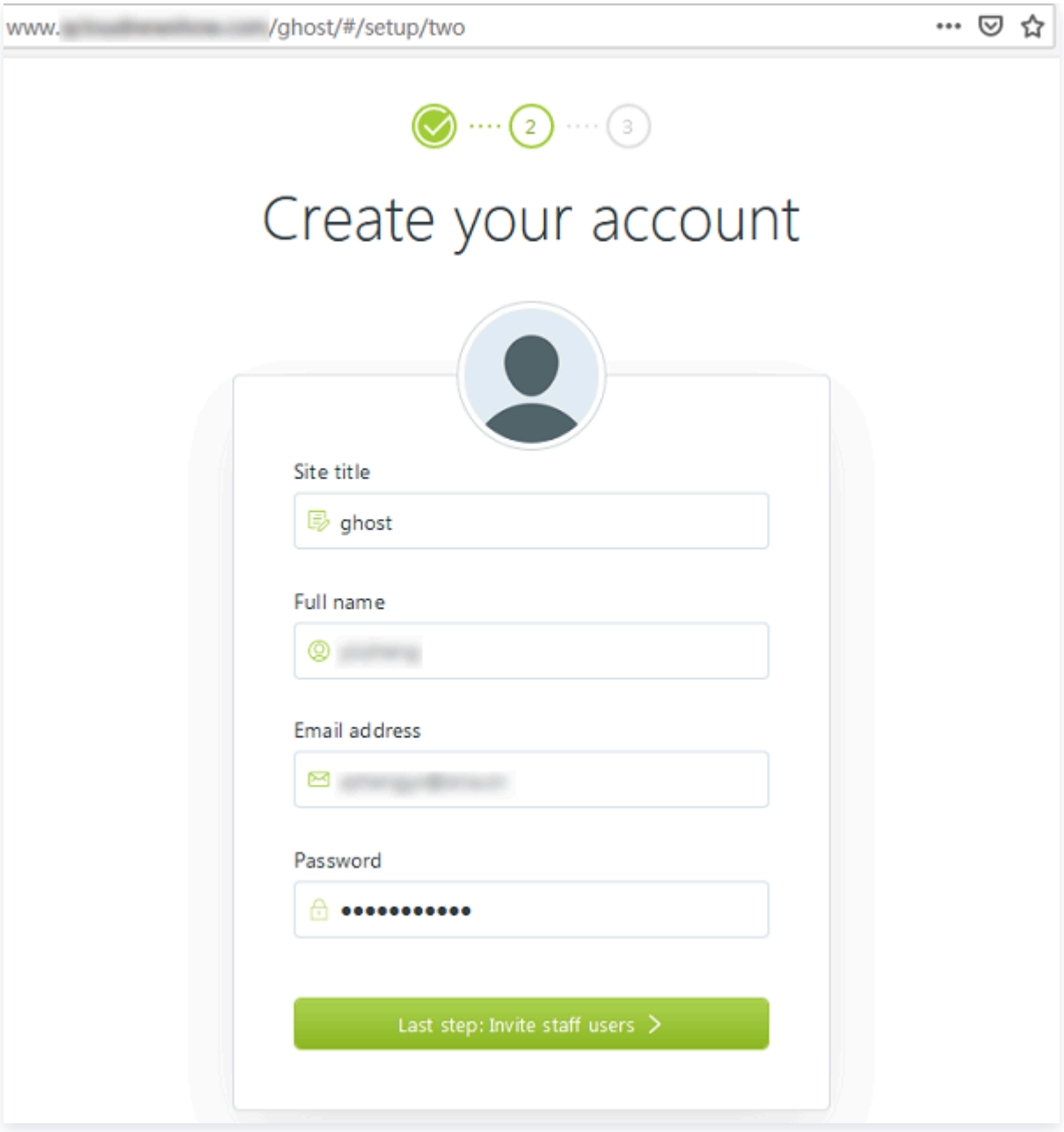
1. Enter your blog URL：解決済みのドメイン名を入力します。`http://(ドメイン名)` を入力してください。
2. Enter your MySQL  hostname：データベース接続アドレスを入力します。`localhost` を入力し、Enterを押してください。
3. Enter your MySQL username：データベースのユーザー名を入力します。`root` を入力し、Enterを押してください。
4. Enter your MySQL password：データベースのパスワードを入力します。 rootアカウントのパスワード設定 で設定済みのパスワ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

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

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

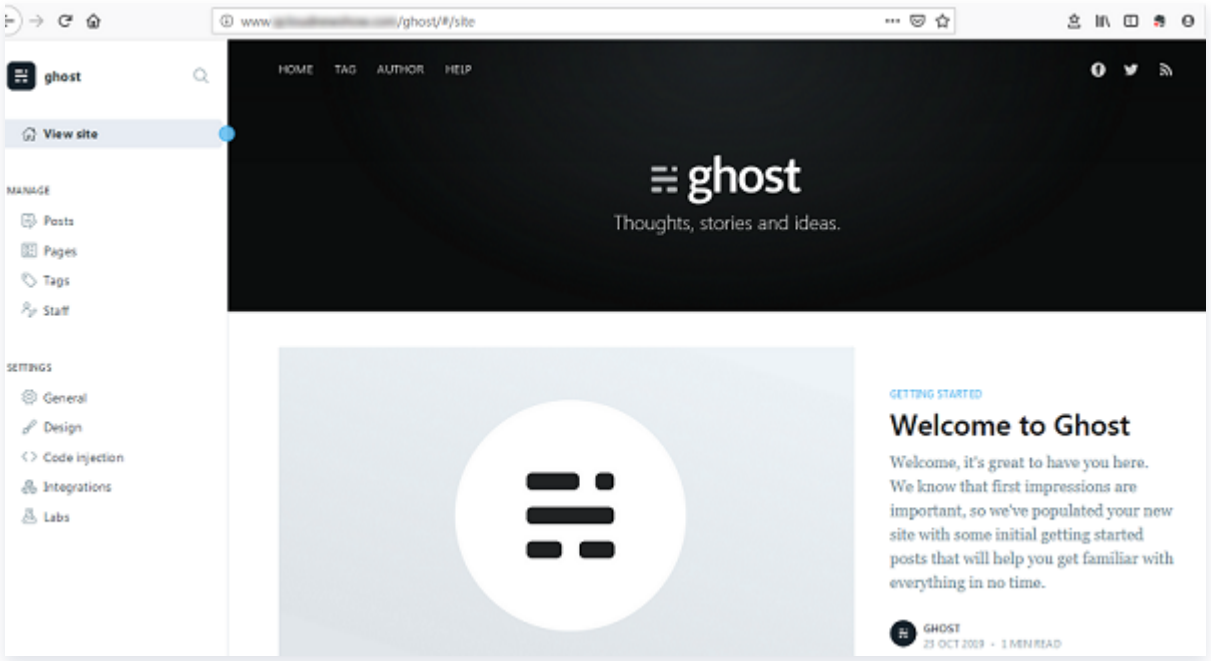


8. 関連情報を入力し、【Last step】をクリックします。下図に示します。

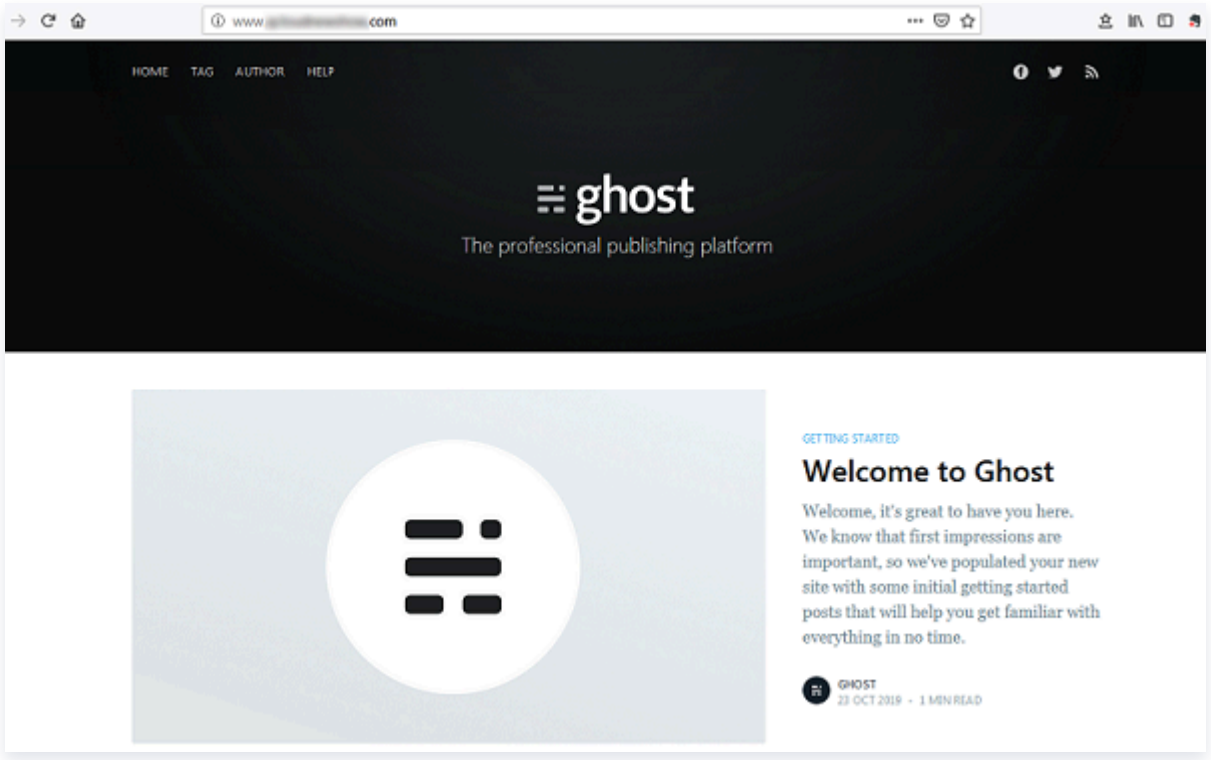



9. 他の人を招待して一緒にブログを作成することもでき、この手順をスキップすることもできます。

10. 管理インターフェースに入ると、ブログの管理を開始できます。下図に示します。




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




## よくあるご質問

CVMの使用中に問題が発生した場合は、下記のドキュメントを参照して、実際の状況に応じて問題を分析して解決できます。

- CVMのログインに関する問題は、パスワードとキー 、ログインとリモート接続 ドキュメントをご参照ください。
- CVMのネットワークに関する問題は、 IPアドレス 、ポートとセキュリティグループ ドキュメントをご参照ください。
- CVMのハードディスクに関する問題は、システムディスクとデータディスク ドキュメントをご参照ください。

# アプリケーションの構築
# FTPサービスの構築
# LinuxインスタンスでのFTPサービスの構築

最終更新日：：2025-11-21 15:37:37

## 概要

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

## ソフトウェアのバージョン

本文では、作成したFTPサービスのコンポーネントバージョンは次のとおりです：

- Linux OS ： 本節では、公開イメージCentOS 7.6を例に説明します。
- Vsftpd：本節では、vsftpd 3.0.2を例に説明します。

## 操作手順

### ステップ1：CVMにログインする

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

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

### 手順2：vsftpdのインストール

1. 次のコマンドを実行し、vsftpdをインストールします。

```
yum install -y vsftpd
```

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

```
systemctl enable vsftpd
```

3. 次のコマンドを実行し、FTPサービスを起動します。

```
systemctl start vsftpd
```

4. 次のコマンドを実行し、サービスが起動されているかどうかを確認します。

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

次の結果が表示され、FTPサービスが正常に開始されたことを示します。

```
[root@VM_0_117_centos ~]# systemctl start vsftpd
[root@VM_0_117_centos ~]# netstat -antup | grep ftp
tcp6       0      0 :::21                   :::*                    LISTEN      5123/vsftpd
```

このとき、vsftpdはデフォルトで匿名アクセスモードを有効化しており、ユーザー名およびパスワードを必要とすることなくFTPサーバーにログインできます。この方法でFTPサーバーにログインするユーザーには、ファイルを変更またはアップロードする権限がありません。

## 手順3：vsftpdの設定

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

```
useradd ftpuser
```

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

```
passwd ftpuser
```

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

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

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

4. 次のコマンドを実行して、ディレクトリの権限を変更します。

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

5. 次のコマンドを実行し、「vsftpd.conf」ファイルを開きます。

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

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

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

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

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

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

```
#listen_ipv6=YES
```

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

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

```
pasv_max_port=45000
```

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

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

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

```
systemctl restart vsftpd
```

## 手順4：セキュリティグループの設定

FTPサービスを構築した後、実際に使用するFTPモードに従って、Linux CVMにインバウンドルールをインターネットにオープンする必要があります。詳細については、セキュリティグループルールの追加 をご参照ください。
ほとんどのクライアント端末はLANにあり、IPアドレスが変換されたものです。FTPのアクティブモードを選択した場合は、クライアントマシンが真のIPアドレスを取得したことを確認してください。取得していない場合、クライアントがFTPサーバーにログインできない場合があります。

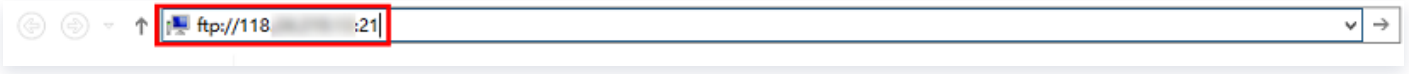
- アクティブモードの場合：ポート21を開きます。
- パッシブモードの場合：ポート21と、および 設定ファイルの変更 で設定されている`pasv_min_port`から`pasv_max_port`までのすべてのポートを開きます。（本節では、ポート40000～45000を開きます）。

## 手順5：FTPサービスの検証

FTPクライアントソフトウェア、ブラウザ、またはファイルエクスプローラなどのツールを使用してFTPサービスを検証できます。本節では、クライアントのファイルエクスプローラを例に説明します。

1. クライアントのInternet Explorerを開き、ツール>インターネットオプション>詳細設定を選択し、選択したFTPモードに応じて変更します：
   - アクティブモードの場合：「パッシブFTPを使用する」のチェックを外します。
   - パッシブモードの場合：「パッシブFTPを使用する」のチェックを入れます。
2. 次の図に示すように、クライアントでWindowsエクスプローラーを開き、アドレスボックスに次のアドレスを入力して、Enterキーを押します：

```
ftp://云服务器公网IP:21
```




3. ポップアップされた「ログインID」画面に vsftpdを設定する で設定されたユーザー名とパスワードを入力します。
   本節で使用するユーザー名が「ftpuser」、パスワードが「tf7295TFY」です。
4. ログインが成功したら、ファイルをアップロード及びダウンロードできます。

# 付録

## FTPのアクティブモードの設定

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

```
anonymous_enable=NO        #匿名ユーザーのログインを禁止する
local_enable=YES           #ローカルユーザーのログインを許可する
chroot_local_user=YES      #すべてのユーザーがルートディレクトリのみにアクセスするよ
うに制限する
chroot_list_enable=YES     #例外ユーザーリストを有効にする
chroot_list_file=/etc/vsftpd/chroot_list   #ユーザーリストファイルを指定しま
す。このリストのユーザーの権限はルートディレクトリに限定されていません
listen=YES                 #IPv4 socketsをリスニングする
#行の先頭に#を付けて、次のパラメータをコメントアウトします
#listen_ipv6=YES           #IPv6 socketsのリスニングをオフにする
#次のパラメータを追加する
allow_writeable_chroot=YES
local_root=/var/ftp/test #ローカルユーザーがログインした後の常駐するディレクトリを
設定する
```

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

## FTPクライアントからのファイルアップロード処理がエラー

### 問題の説明

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

```
553 Could not create file
```

## ソリューション

1. 次のコマンドを実行し、サーバーのディスク領域の使用率を確認します。

   ```
   df -h
   ```

   - ディスクに十分な空き容量がない場合、ファイルをアップロードできないため、ディスク上の大容量のファイルを削除することをお勧めします。
   - ディスク容量が十分な場合は、次のステップを実行してください。

2. 次のコマンドを実行し、FTP ディレクトリへの書き込み権限があるかどうかを確認します。

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

   - 戻された結果に「w」がない場合は、当該ユーザーに書き込み権限がないことを示し、次のステップを実行してください。
   - 返された結果の中に `w` があれば、チケットを提出 してフィードバックしてください。

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

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

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

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

# WindowsインスタンスでのFTPサービスの構築

最終更新日：：2022-05-07 15:41:38

## 概要

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

## ソフトウェアバージョン

このドキュメントでは、構築したFTPサービスのソフトウェアバージョンは次のとおりです。

- Windows OS、このドキュメントでは Windows Server 2012 を例として説明します。
- IIS：Web サーバー、このドキュメントでは IIS 8.5 を例として説明します。

## 操作手順

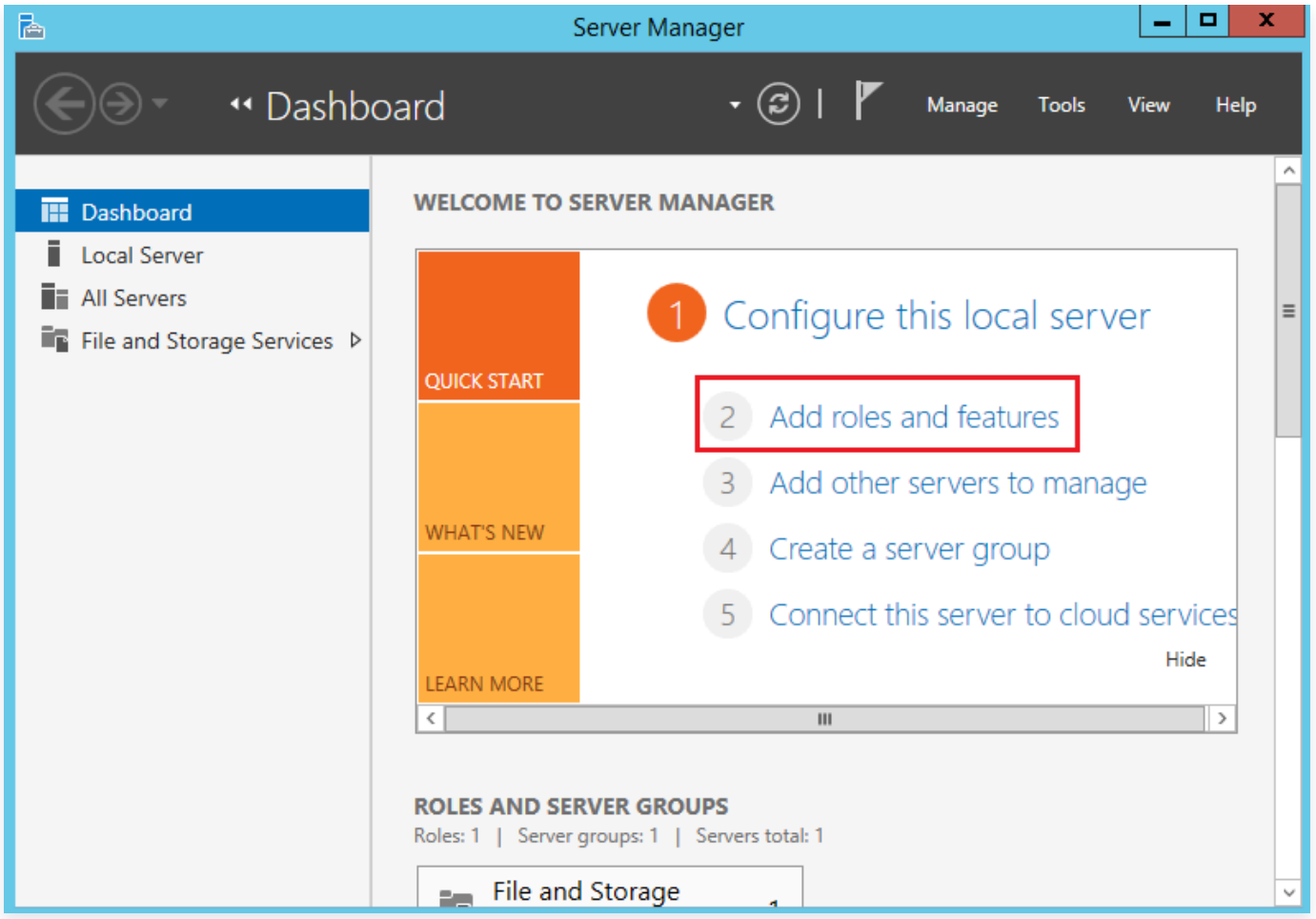
### 手順１： CVMにログインする

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

### 手順2：IIS にFTPサービスをインストールする

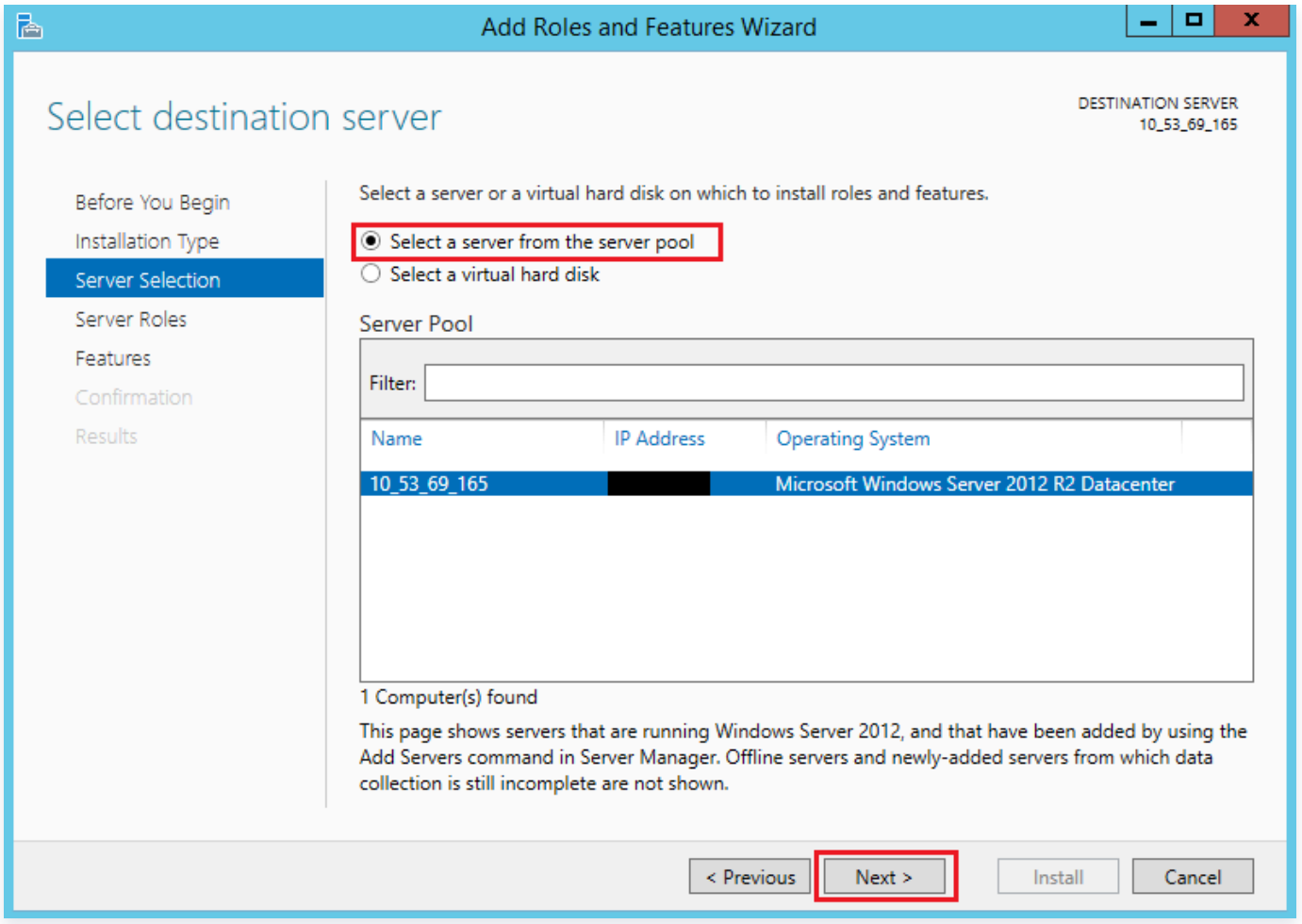
1. OSインターフェースで、  をクリックして、サーバーマネージャーを開きます。

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

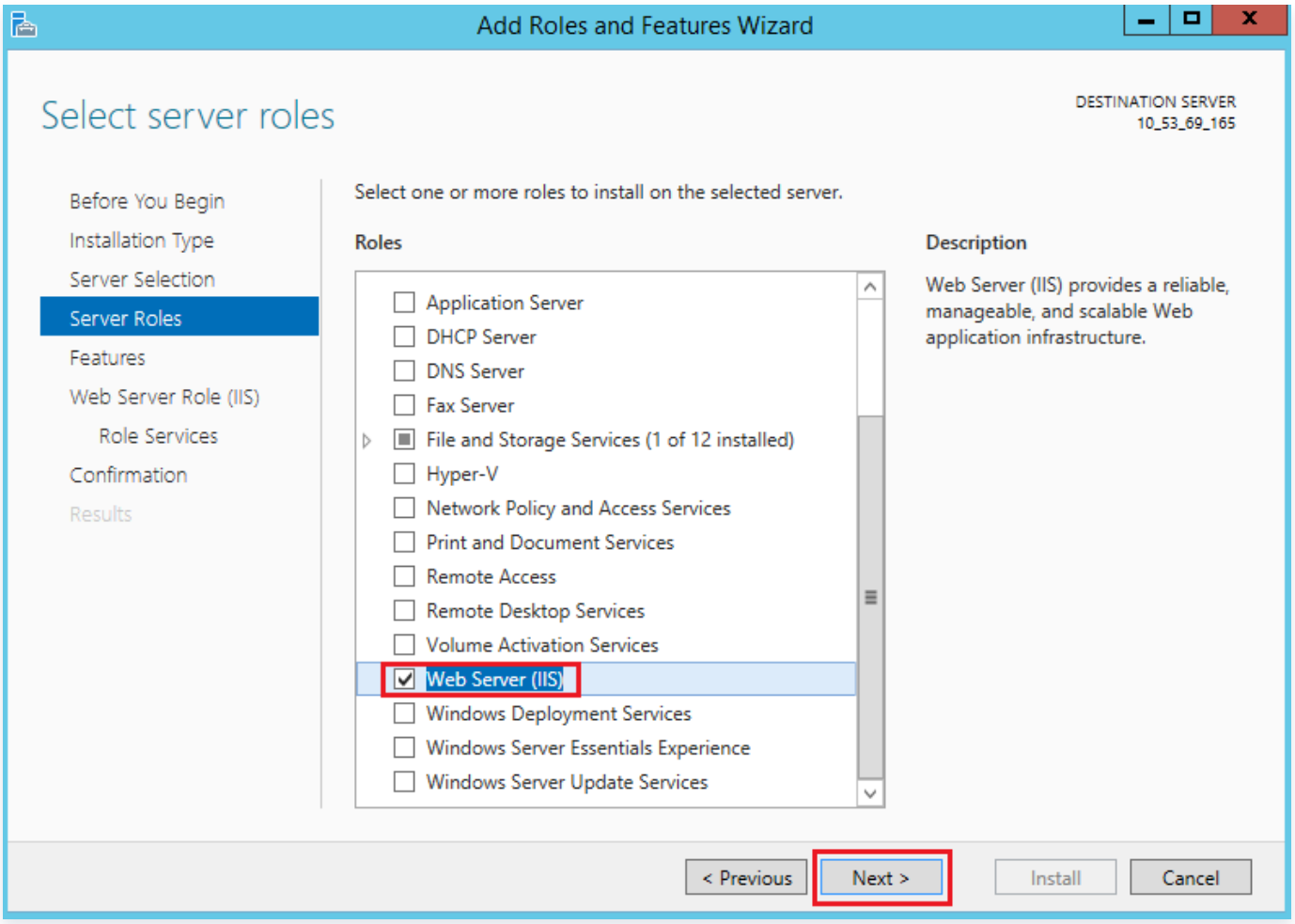



3. 「役割と機能の追加ウィザード」で、次へをクリックして、「インストールの種類の選択」画面に入ります。
4. 「インストールの種類の選択」画面で、役割ベースまたは機能ベースのインストールを選択して、次へをクリックします。

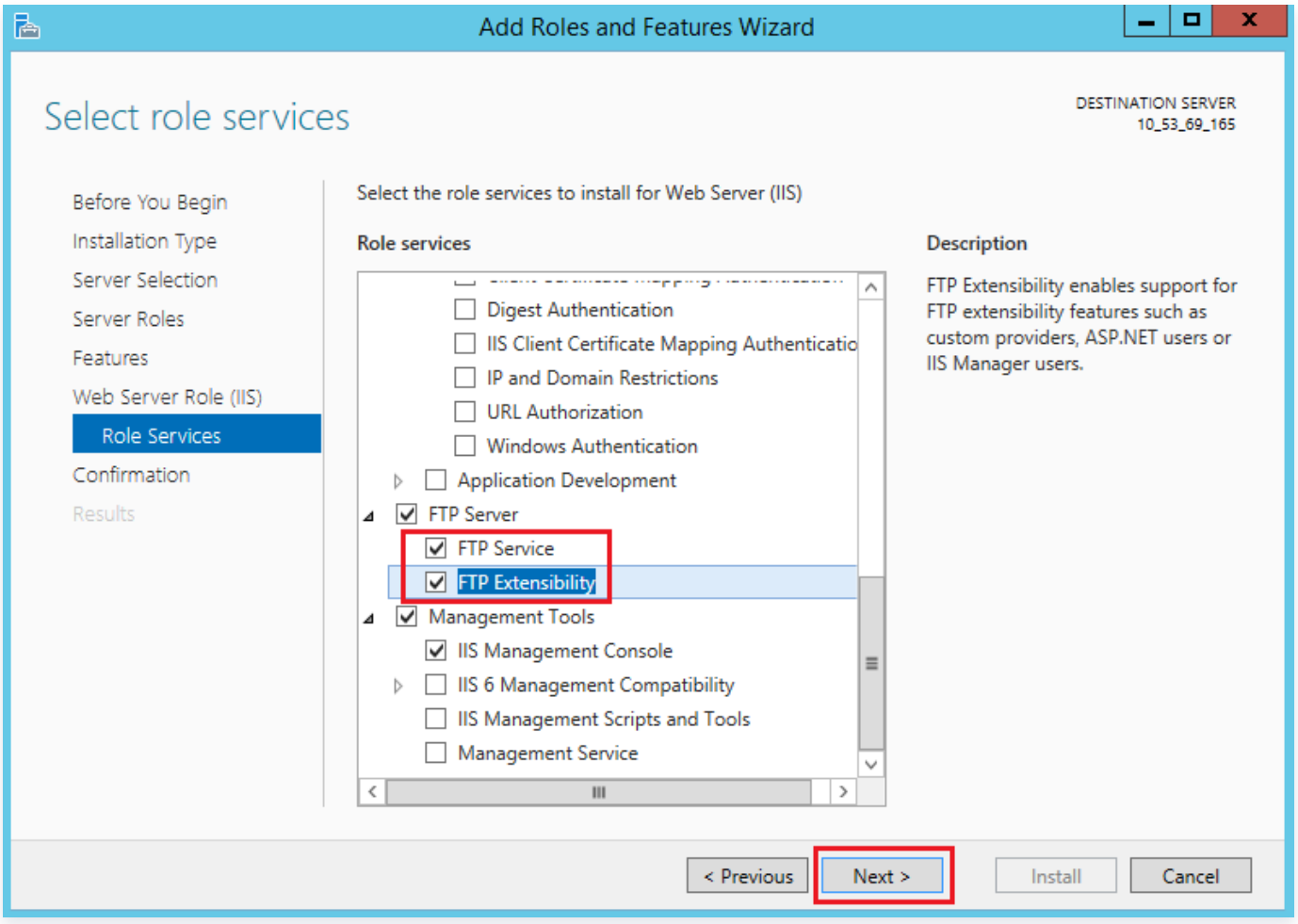
5. 「対象サーバーの選択」画面で、デフォルト設定を保持して、次へをクリックします。次の図に示すように:




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




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

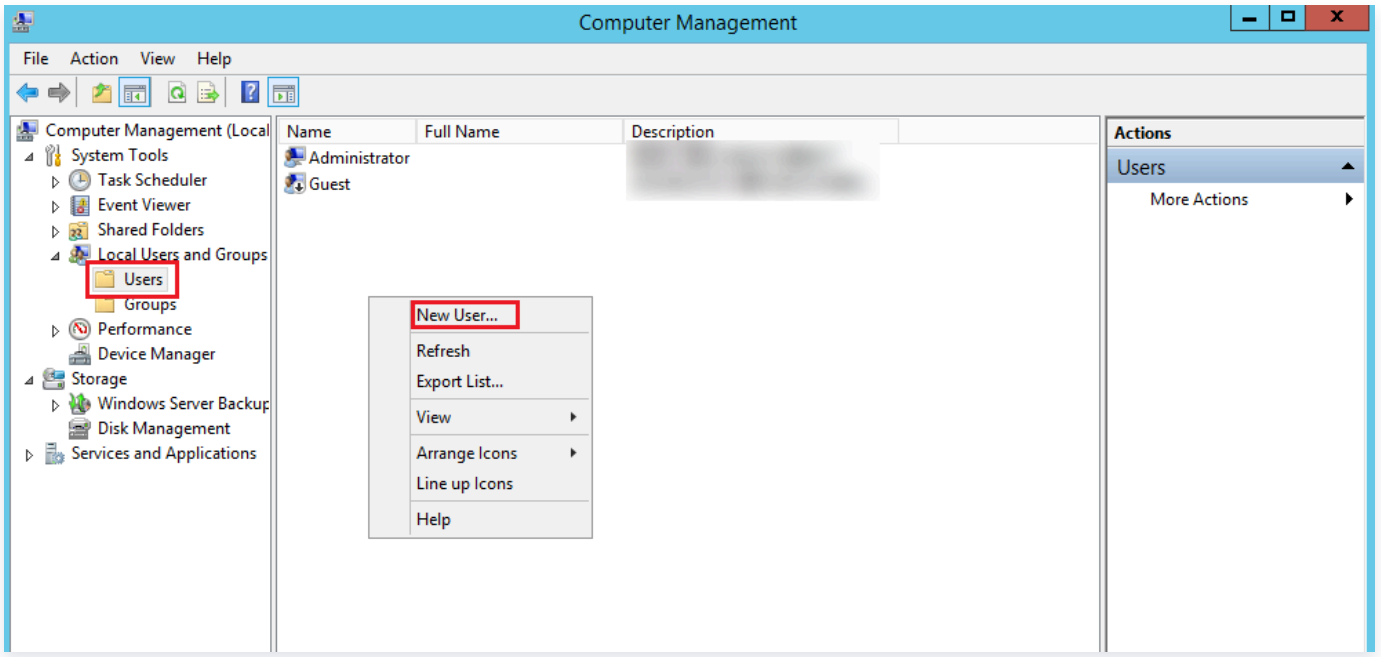



9. インストールをクリックして、 FTP サービスのインストールを開始します。
10. インストールが完了したら、閉じるをクリックします。

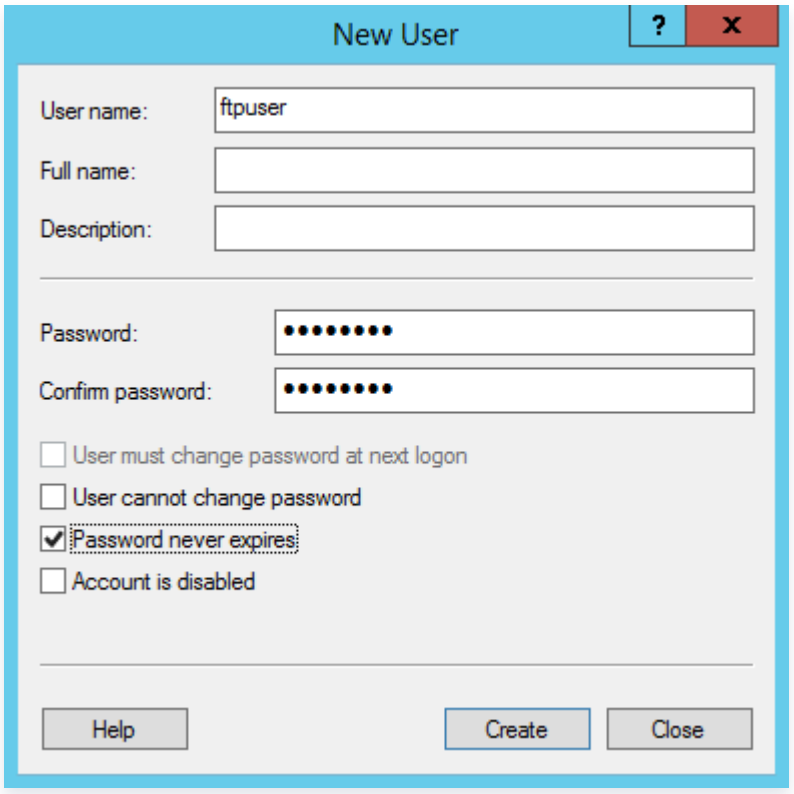
## 手順3： FTP ユーザー名とパスワードを作成する

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

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




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




主なパラメータは次の通り:

- ユーザー名: カスタム。このドキュメントでは、 `ftpuser` を例として説明します。
- パスワードと確認パスワード: カスタム。パスワードには大文字と小文字、数字を全て含める必要があります。このドキュメントでは、 `tf7295TFY` を例として説明します。

- ユーザは次回ログオン時にパスワードの変更が必要のチェックを外し、パスワードを無制限にするにチェックを入れます。
  実際のニーズに応じてチェックしてください。このドキュメントではパスワードを無制限にすることを例として説明します。

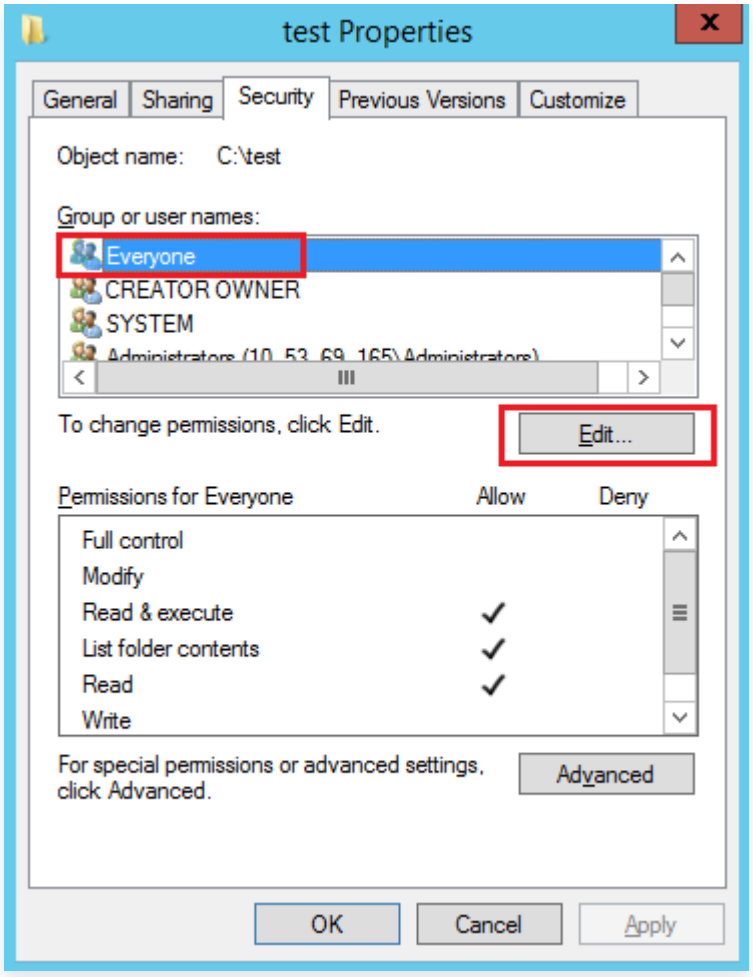
5. 閉じるをクリックし、「新しいユーザー」ウィンドウを閉じた後に、リストに作成された `ftpuser` ユーザーを確認できます。

## 手順4：共有フォルダーのアクセス権限を設定する

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

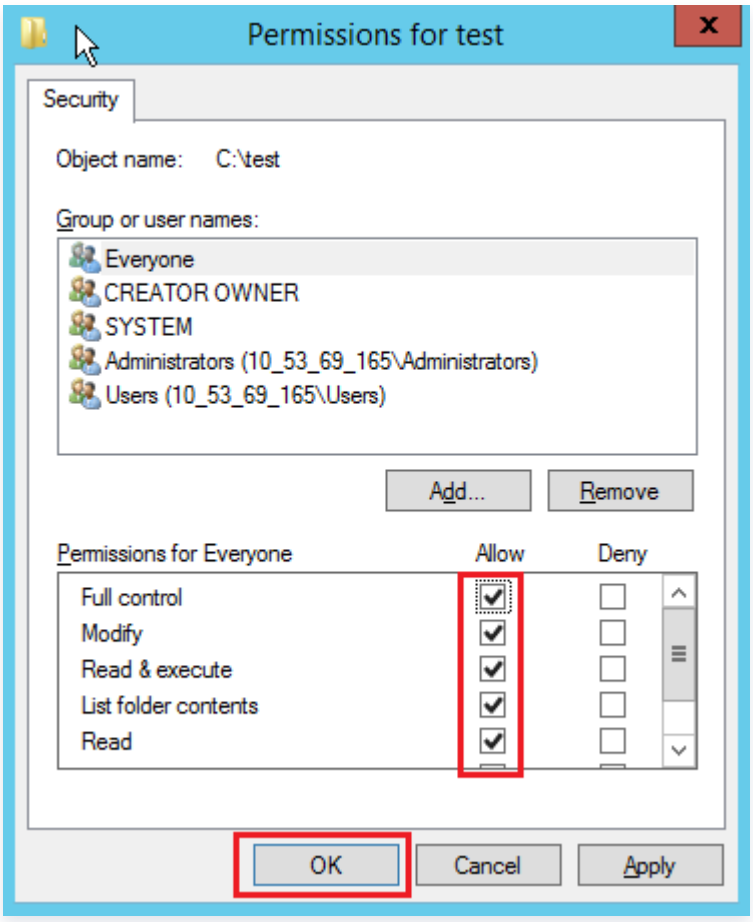
1. OSインターフェースで、  をクリックして、「PC」を開きます。
2. Cドライブで、 `test` フォルダーを選択して右クリックし、プロパティを選択します。
3. 「test プロパティ」ウィンドウで、セキュリティタグを選択します。
4. `Everyone` ユーザーを選択し、編集をクリックします。次の図に示すように：
   「グループまたはユーザー名」に `Everyone` が含まれていない場合は、Everyone Userの追加 を参考して

ユーザーを追加してください。




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

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

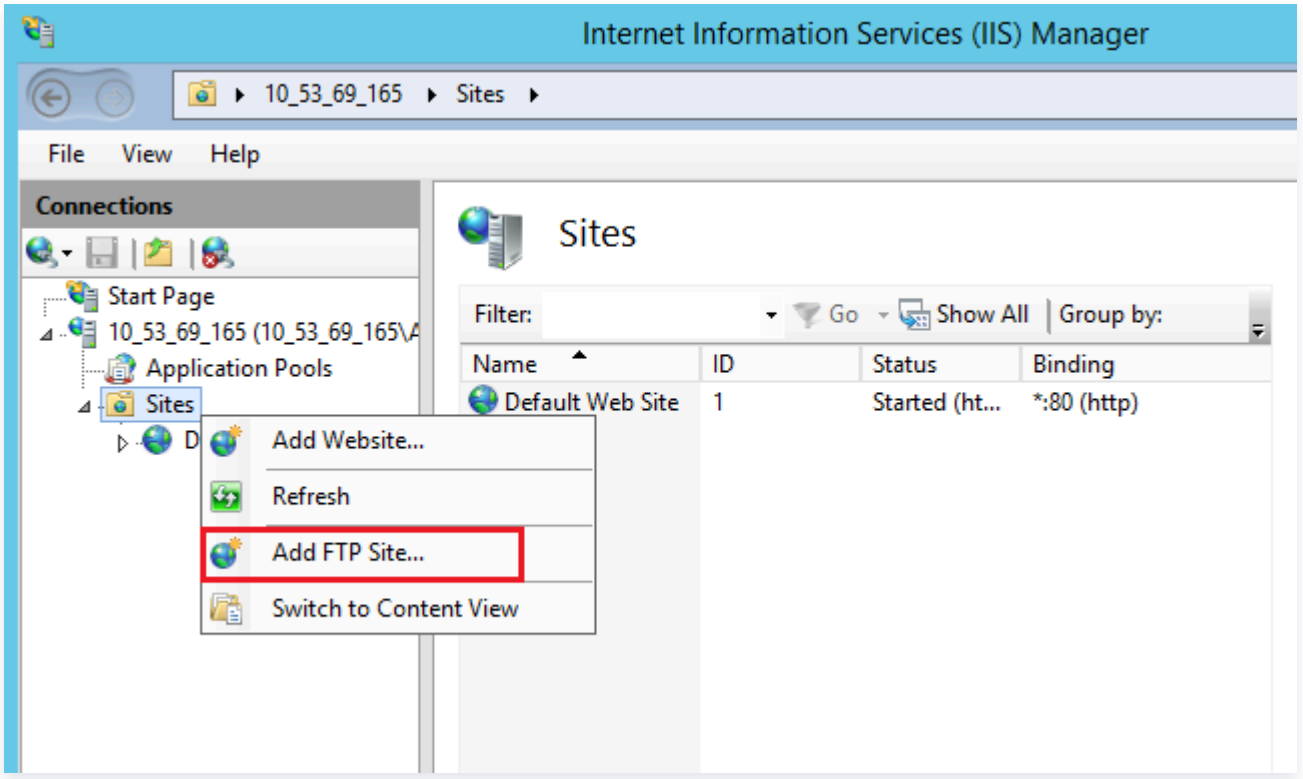



6. 「test プロパティ」ウィンドウで、【OK】をクリックして設定を完了します。

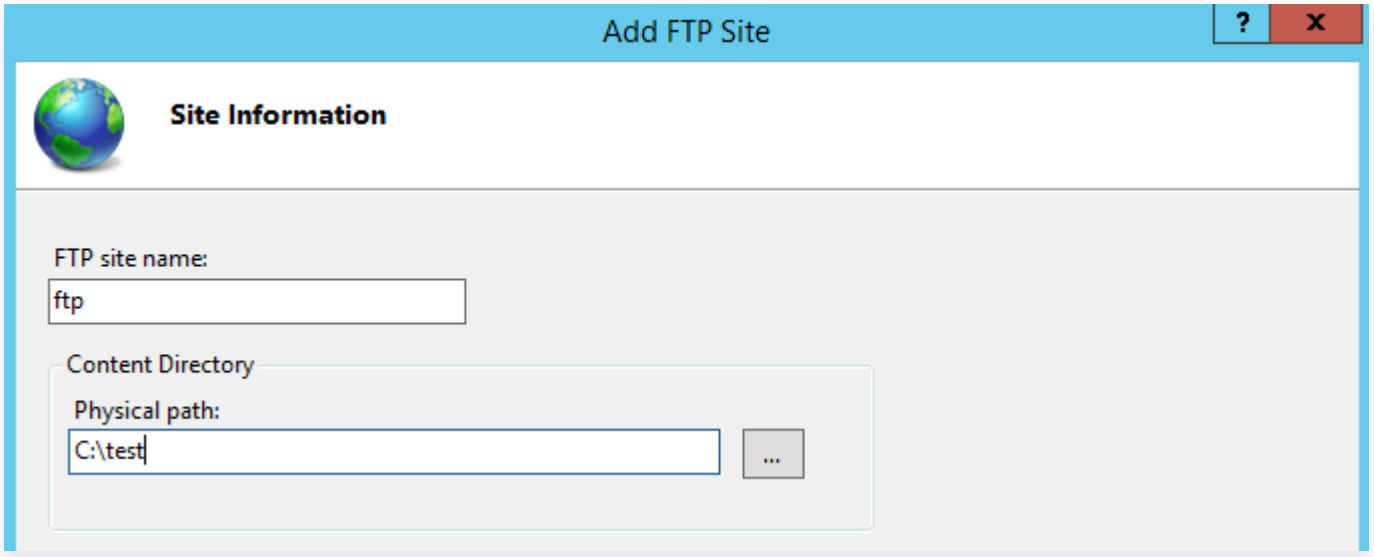
## 手順5： FTPサイトを追加する

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

に示すように：

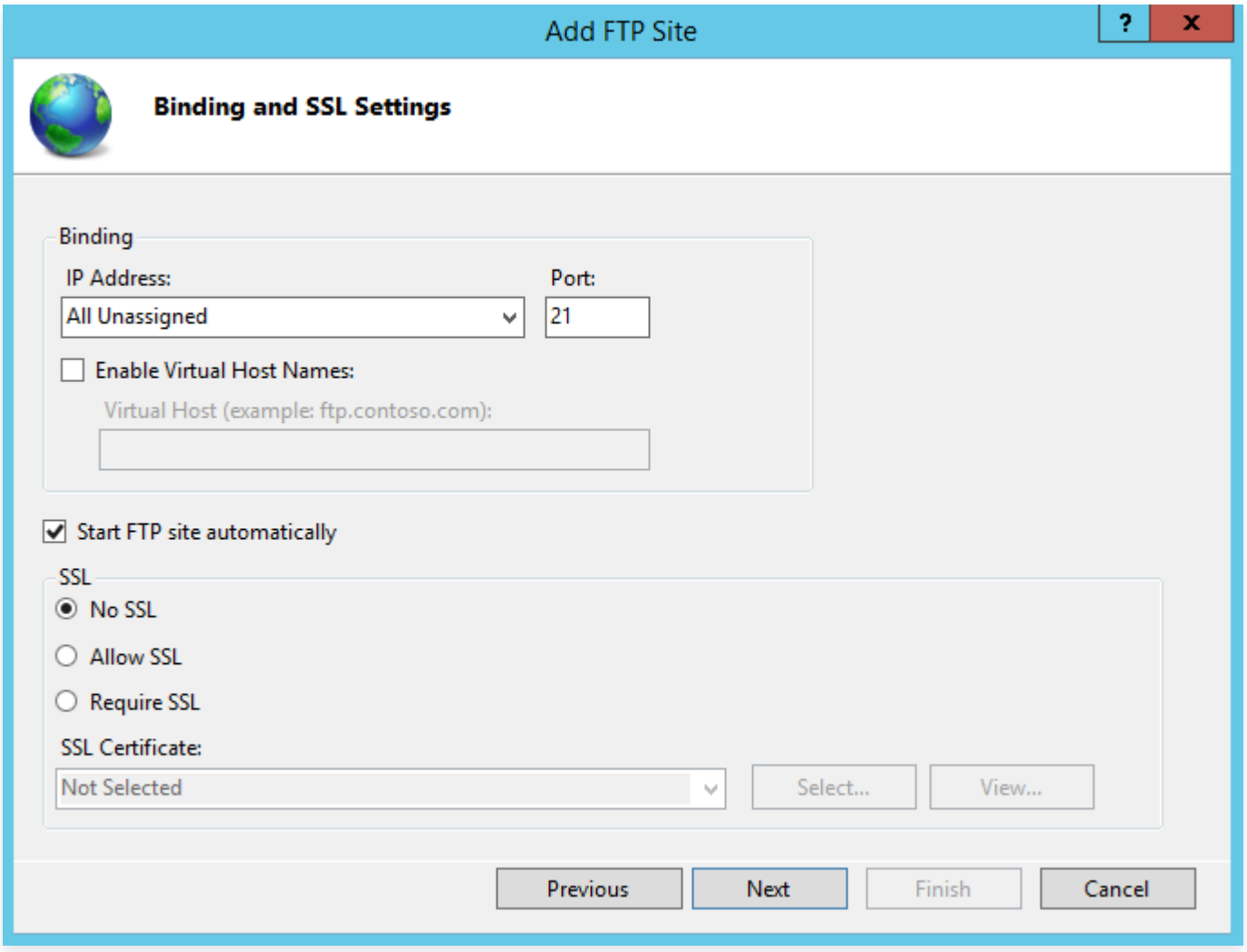



3. 「サイト情報」画面で、以下の情報を参考して設定し、次へをクリックします。次の図に示すように：




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

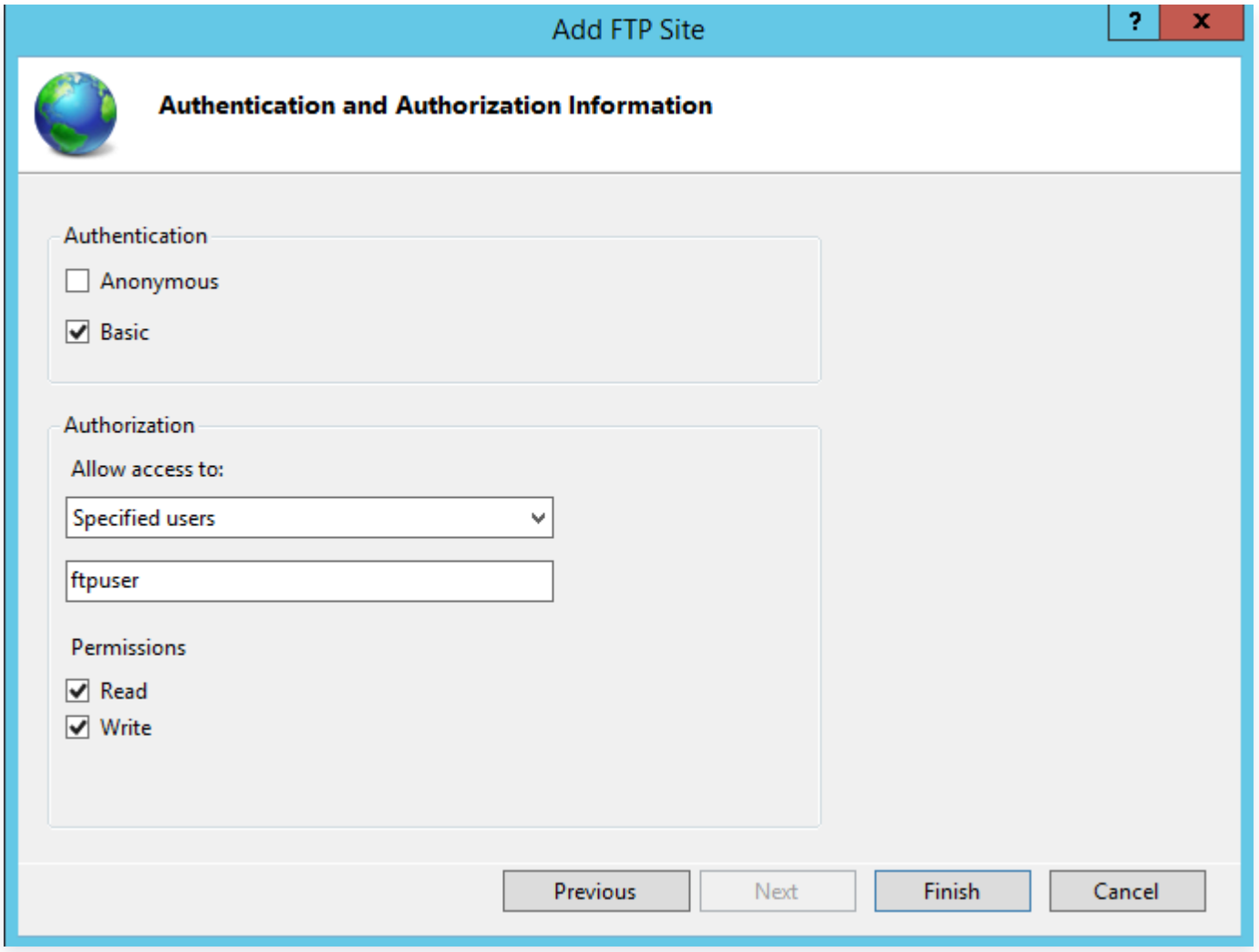
4. 「バインドと SSL の設定」画面で、以下の情報を参考して設定し、次へをクリックします。次の図に示すように：




主な構成パラメータ情報は下記の通り：

- バインド：IP アドレスのデフォルト選択はすべて未割り当てで、デフォルトのポート番号は21（FTP のデフォルトのポート番号）であり、カスタムポート番号を設定できます。
- SSL：必要に応じて選択してください、このドキュメントではSSL 無しを例としています。
  - SSL　無し：SSL暗号化は必要ありません。
  - SSL の許可：FTPサーバーによるクライアントとの非SSLおよびSSL接続のサポートを許可します。
- SSL が必要：　FTPサーバーとクライアント間の通信にはSSL暗号化が必要です。
  許可あるいは必要を選択した場合、「SSL証明書」で既存のSSL証明書を選択するか、サーバー証明書の作成 を参考してSSL証明書を作成することもできます。

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




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

- 権限：必要に応じて権限を設定してください。本文では読み取りと書き込み権限の設定を例として説明します。
  - 読み取り：許可されたユーザーがディレクトリからコンテンツを読み取ることができます。
  - 書き込み：許可されたユーザーがディレクトリに書き込むことができます。

6. 完了をクリックして、 FTP サイトを作成できます。

## 手順6：セキュリティグループとファイアウォールを設定する

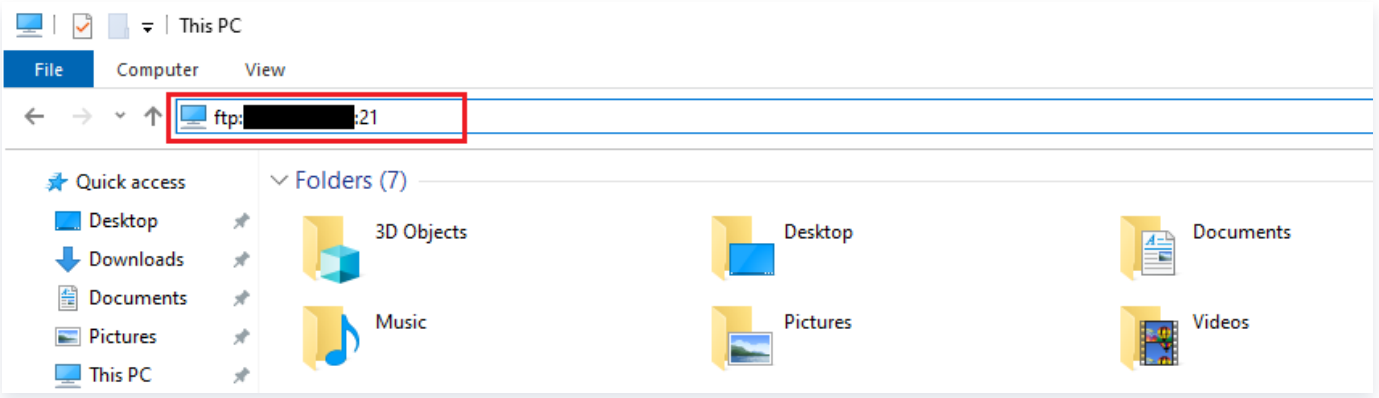
1. FTPサイトの構築が完了したら、FTPアクセスモードに対応して、FTPサイトを追加するときに、ポートをバインドするためのインバウンドルールを許可してください。
   - アクティブモード：ポート20と21を開きます。
   - パッシブモード：ポート21および 1024 ~ 65535（たとえば、ポート5000~6000）の間のポートを開きます。
     対応するインバウンドルールを追加する方法については、セキュリティグループルールの追加 をご参照ください。
2. （オプション）Microsoft公式ドキュメント を参考して FTP サイトのファイアウォールサポートを設定することにより、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

## 手順7：FTP サイトをテストする

FTP クライアントソフトウェア、ブラウザー或はファイルエクスプローラーなどのツールを利用してFTP サービスをテストできます。本文ではクライアント側のファイルエクスプローラーを例として説明します。

1. 実際の使用状況に応じて、 IE ブラウザを設定してください:
   - FTPサイトファイアウォールが構成されています（アクティブモード）：
     クライアントの IEブラウザを開き、ツール > インターネットオプション > 詳細設定を選択し、パッシブFTP(ファイアウォールおよびDSLモデム互換用)を使用するのチェックを外して、【OK】ボタンをクリックします。
   - FTPサイトファイアウォールが構成されていません（パッシブモード）：
     1.1.1 FTP サーバーの IE ブラウザを開き、ツール > インターネットオプション > 詳細設定 を選択し、パッシブFTP(ファイアウォールおよびDSLモデム互換用)を使用するのチェックを外して、【OK】ボタンをクリックします。
     1.1.2 クライアントの IEブラウザを開き、ツール > インターネットオプション > 詳細設定を選択し、パッシブFTP(ファイアウォールおよびDSLモデム互換用)を使用するのチェックを外して、【OK】ボタンをクリックします。
2. 次の図に示すように、クライアントでWindowsエクスプローラーを開き、アドレスボックスに次のアドレスを入力して、Enterキーを押します。

```
ftp://CVMパブリックIP:21
```

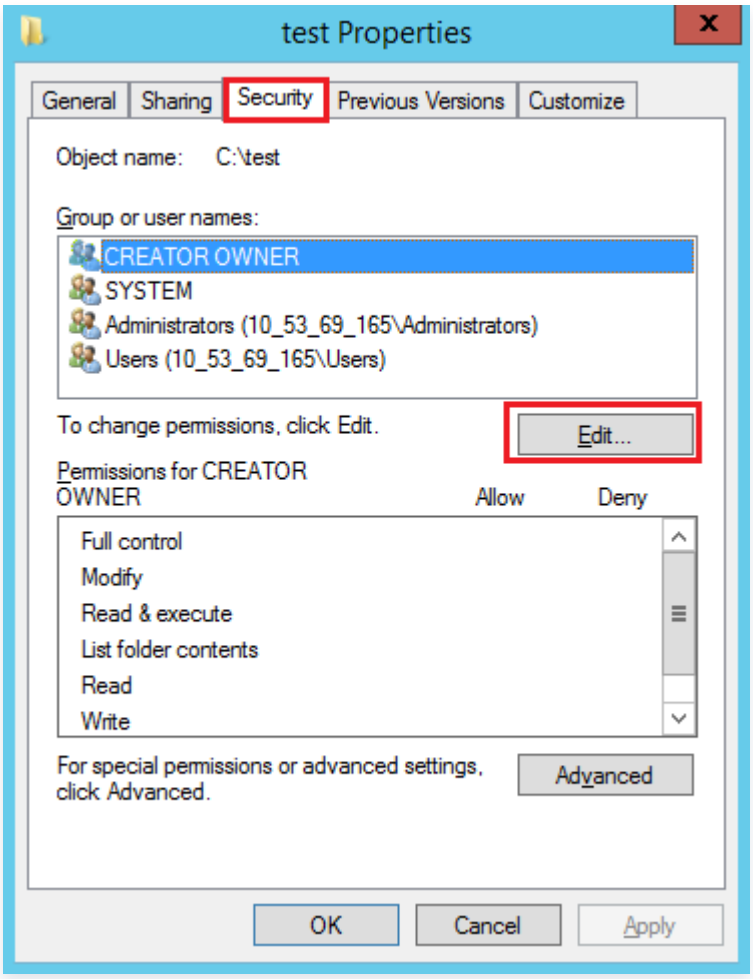



3. ポップアップされた「ログイン」ウィンドウで、 FTP ユーザー名とパスワードの作成 で設定されたユーザー名とパスワードを入力します。
   このドキュメントで使用されるユーザー名は `ftpuser` で、パスワードは `tf7295TFY` です。
4. ログインが成功したら、ファイルをアップロード及びダウンロードできます。

# 付録

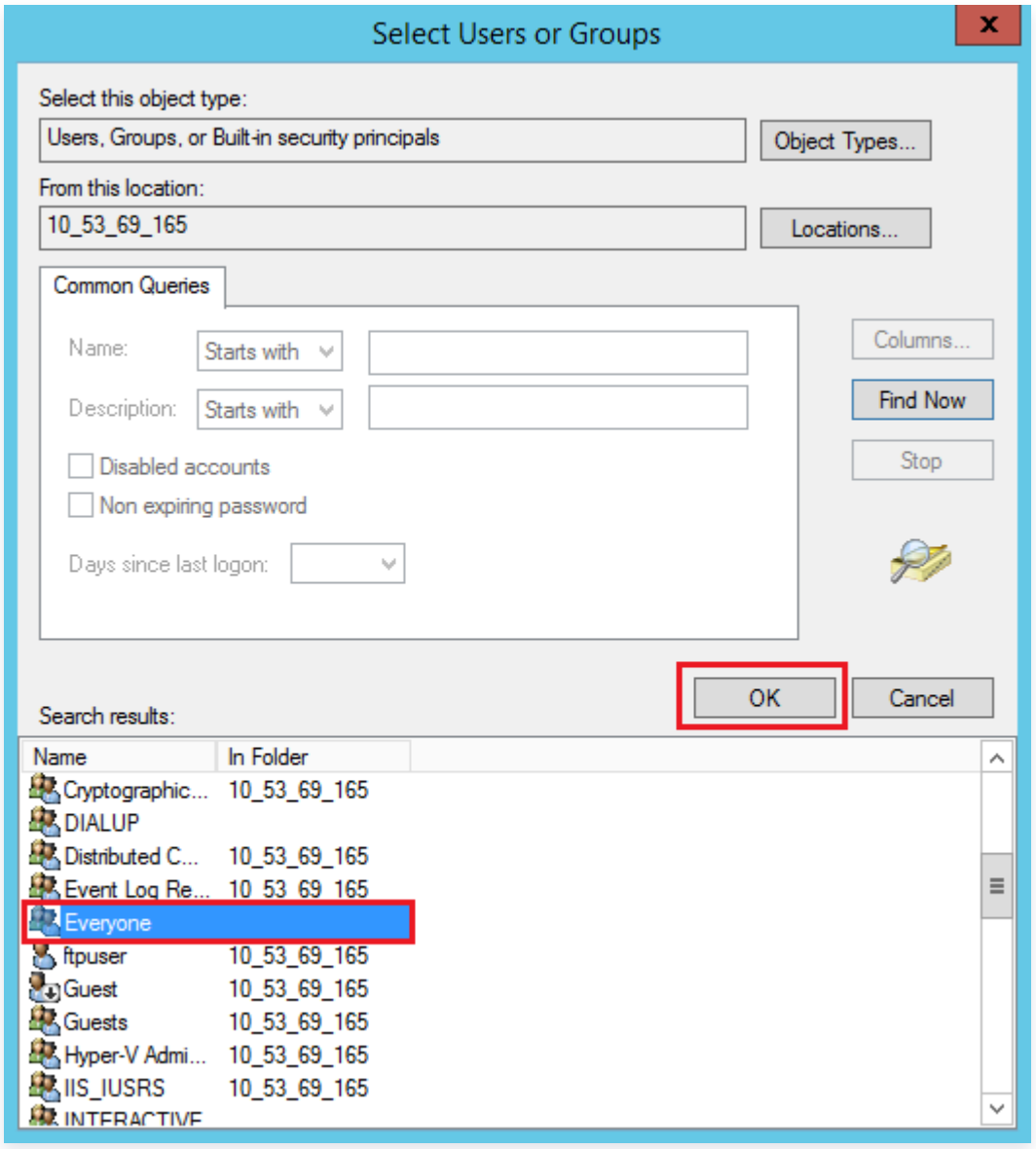
## Everyone ユーザーを追加する

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

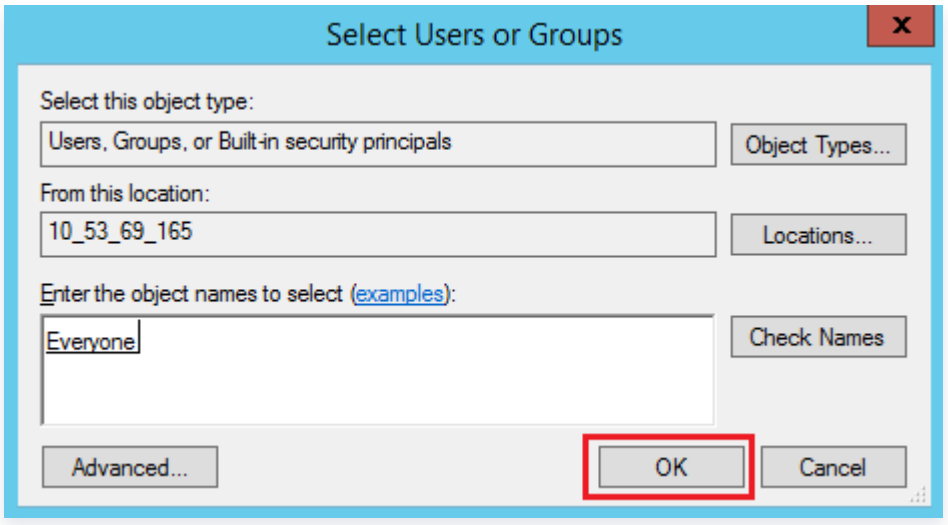



2. 「権限テスト」画面で、追加をクリックします。
3. 「ユーザーまたはグループの選択」画面で、詳細設定をクリックします。
4. 表示される「ユーザーまたはグループの選択」画面で、今すぐ検索をクリックします。

5. 検索結果に `Everyone` を選択し、【OK】をクリックします。次の図に示すように:



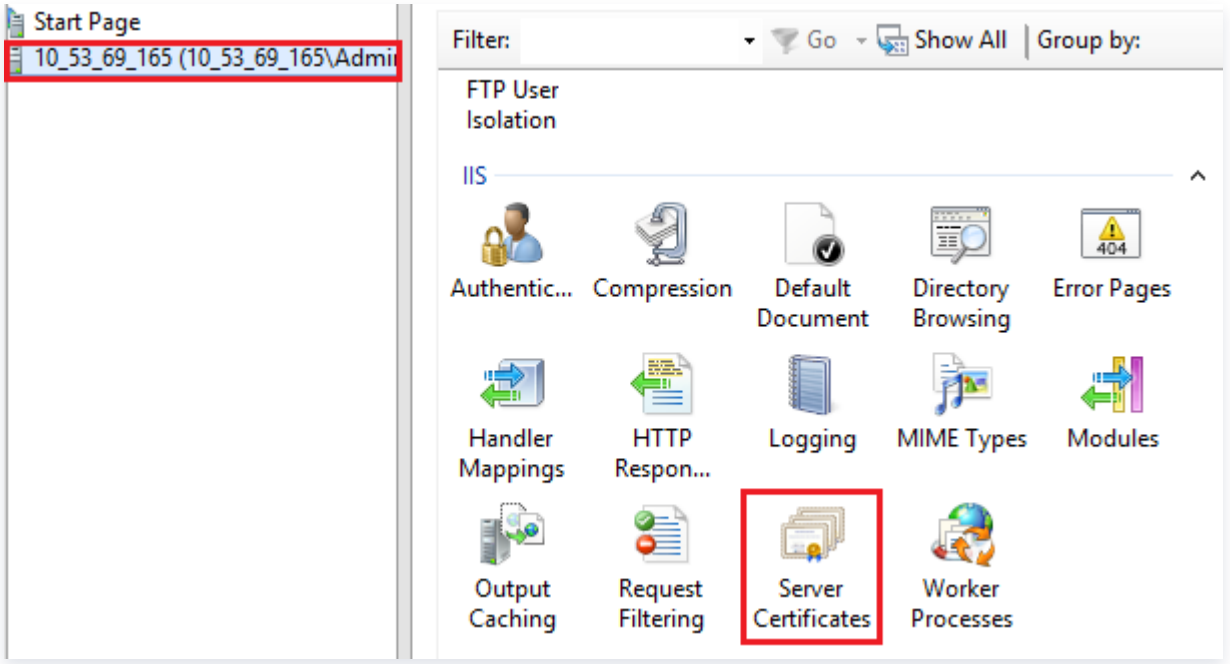

6. 「ユーザーまたはグループの選択」画面で、【OK】をクリックしてEveryoneユーザー追加できます。次の図に示すように:




手順5 に進み 、 `Everyone` ユーザーの権限を設定します。

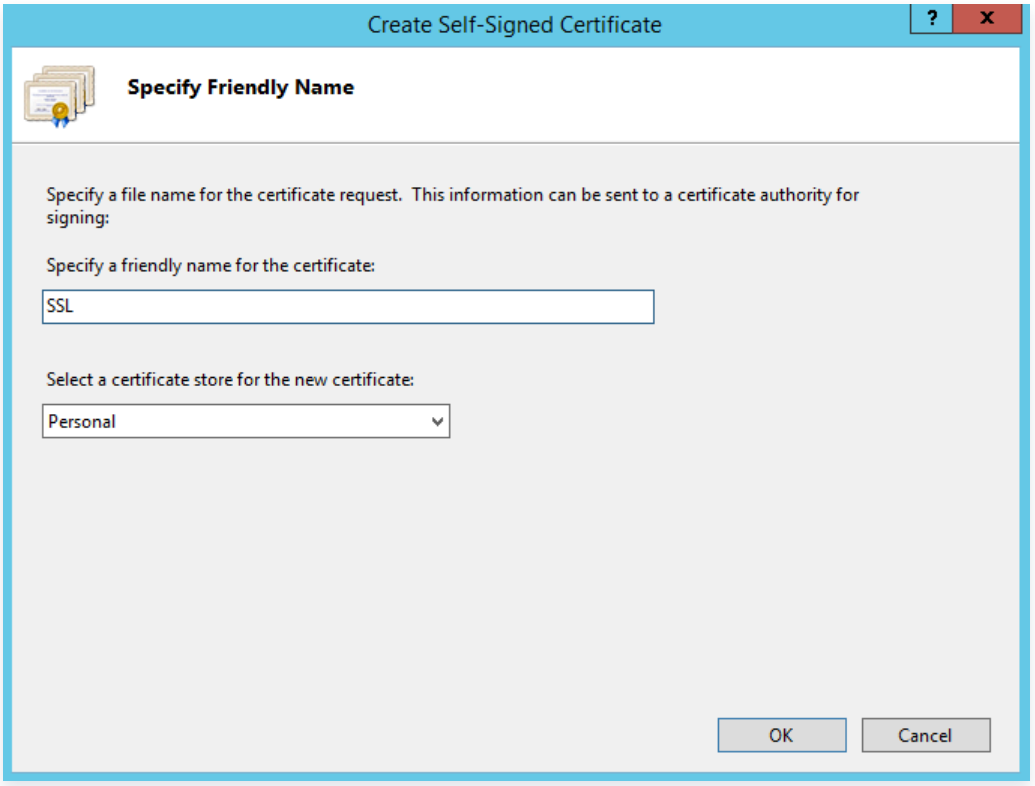
## サーバー証明書の作成

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




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

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




5. 【OK】をクリックして、サーバー証明書を作成します。

# NTPサービス
# NTPサービスの概要

最終更新日：：2022-05-07 16:03:47

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

## プライベートネットワーク NTP サーバー

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

## パブリックネットワークNTPサーバー

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

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

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

```
time5.cloud.tencent.com
```

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

# Linuxインスタンス：NTPサービスの設定

最終更新日：：2022-03-07 11:41:48

## 操作シナオリ

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

## 注意事項

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

## 操作手順

### NTPDサービスのインストール

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

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

- 次の結果が返される場合、NTPDがインストールされていることを意味します。

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

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

```
yum -y install ntp
```

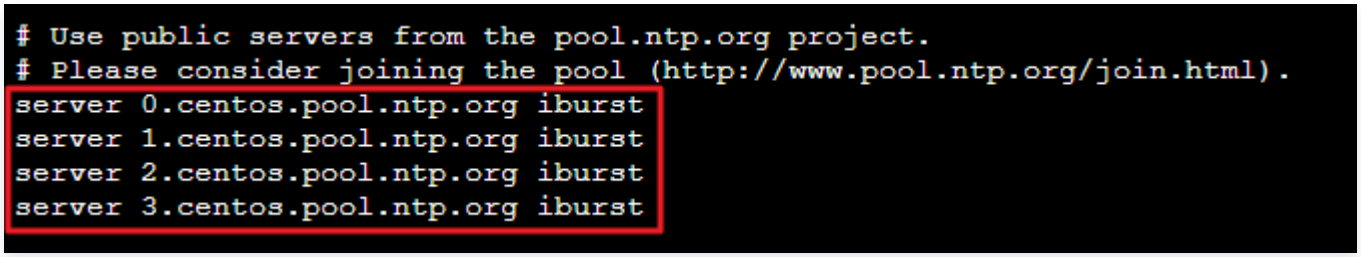
NTPDはデフォルトでクライアントモードを使用します。

## NTPの設定

1. 次のコマンドを実行して、NTPサービスの構成ファイルを開きます。

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

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




3. 「Esc」キーを押し、:wqを入力し、ファイルを保存して閉じます。

## NTPDの起動

次のコマンドを実行して、NTPDサービスを再起動します。

```
systemctl restart ntpd.service
```

## NTPDステータスの確認

次のコマンドを実行して、必要に応じて NTPDのステータスを確認します。

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

```
netstat -nupl
```

以下のような結果が返されると、正常にリッスンされていることを意味します。

```
[root@VM_0_136_centos ~]# netstat -nupl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
udp        0      0 172.30.0.136:123        0.0.0.0:*                           999/ntpd
udp        0      0 127.0.0.1:123           0.0.0.0:*                           999/ntpd
udp6       0      0 fe80::5054:ff:fec2::123 :::*                                999/ntpd
udp6       0      0 ::1:123                 :::*                                999/ntpd
[root@VM_0_136_centos ~]#
```

- 次のコマンドを実行して、NTPDステータスが正常かどうかを確認します。

```
service ntpd status
```

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

```
[root@VM_0_136_centos ~]# service ntpd status
Redirecting to /bin/systemctl status ntpd.service
● ntpd.service - Network Time Service
   Loaded: loaded (/usr/lib/systemd/system/ntpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2019-08-07 15:23:25 CST; 5min ago
  Process: 997 ExecStart=/usr/sbin/ntpd -u ntp:ntp $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 999 (ntpd)
   CGroup: /system.slice/ntpd.service
           └─999 /usr/sbin/ntpd -u ntp:ntp -g

Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c01d 0d kern kernel time sync enabled
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: ntp_io: estimated max descriptors: 1024, initia... 16
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 0 lo 127.0.0.1 UDP 123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 1 eth0 172.30.0.136 UDP 123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 2 lo ::1 UDP 123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 3 eth0 fe80::5054:ff:fec2:11...123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listening on routing socket on fd #20 for inter...tes
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c016 06 restart
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c012 02 freq_set kernel 0.467 PPM
Aug 07 15:23:34 VM_0_136_centos ntpd[999]: 0.0.0.0 c615 05 clock_sync
Hint: Some lines were ellipsized, use -l to show in full.
[root@VM_0_136_centos ~]#
```

次のコマンドを実行して、より詳細なNTPサービス情報を取得します。

```
ntpq -p
```

以下のような結果が返されます:

```
[root@VM_0_136_centos ~]# ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 108.[redacted]  .INIT.          16 u    -   64    0    0.000    0.000   0.000
 193.[redacted]  194.[redacted]   2 u    6   64   17  277.831    3.940   5.588
*185.[redacted]  194.[redacted]   2 u   68   64   16  201.280    1.729   0.263
 193.[redacted]  194.[redacted]   2 u   69   64   16  293.382    1.003   0.441
 169.[redacted]  100.[redacted]   2 u    3   64   17    6.607    9.897   0.461
[root@VM_0_136_centos ~]#
```

- remote：このリクエストに応答するNTPサーバの名前。
- refid：NTP サーバが使用する上位NTPサーバです。

- st：リモートサーバーの階層。サーバーのストラタムは、1から16まで、高から低に設定できます。負荷やネットワークの輻輳を軽減するため、原則としてストラタム1サーバーへの直接接続は避けることが推奨されています。
- when：最後に成功したリクエストから経過した秒数。
- poll：ローカルサーバーとリモートサーバー間の同期間隔（秒単位）。NTPを最初に実行すると、pollの値が小さく、サーバと同期頻度が高いため、できるだけ早く正しい時間範囲に調整することをお勧めします。調整後、pollの値は徐々に増加し、同期頻度は減少します。
- reach：サーバーに接続できるかどうかをテストするために使用される8進数。接続が成功するたびに、reachの値が増加します。
- delay：ローカルマシンからNTPサーバーに同期要求を送信する往復時間。
- offset：NTPを介してホストとタイムソース間のミリ秒（ms）単位の時間差。オフセットが0に近いほど、ホストとNTPサーバーの時間が近くなります。
- jitter：統計に使用される値。特定の連続したコネクション数の場合のオフセットの分布を集計します。つまり、絶対値が小さいほど、ホスト時間は正確になります。

## NTPD を自動起動に設定する

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

```
systemctl enable ntpd.service
```

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

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

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

```
systemctl disable chronyd.service
```

## NTPDセキュリティ強化

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

```
interface ignore wildcard
```

```
interface listen eth0
```

# Linuxインスタンス：ntpdateからntpdへの変換

最終更新日：：2022-05-07 15:42:08

## 操作シナオリ

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

## 前提条件

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

## 操作手順

### NTPDateをNTPDに手動で変換する

#### NTPDateのシャットダウン

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

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

2. 次のコマンドを実行して、NTPDate設定を更新します。

```
crontab /tmp/cronfile
```

3. 次のコマンドを実行して、`rc.localファイルを変更します。

```
vim rc.local
```

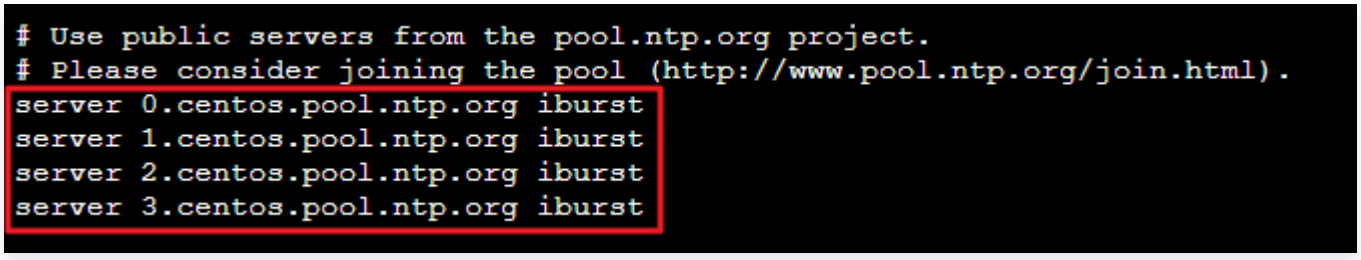
4. 「i」を押して編集モードに切り替え、ntpupdateの設定行を削除します。
5. 「Esc」キーを押して、:wqを入力し、ファイルを保存してから戻ります。

#### NTPDの設定

1. 次のコマンドを実行して、NTPサービスの設定ファイルを開きます。

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

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




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

## NTPDateをNTPDへ自動変換

1. `ntpd_enable.sh` スクリプトをダウンロードします。

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

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

```
sh ntpd_enable.sh
```

# Windowsインスタンス：NTPサービスの設定

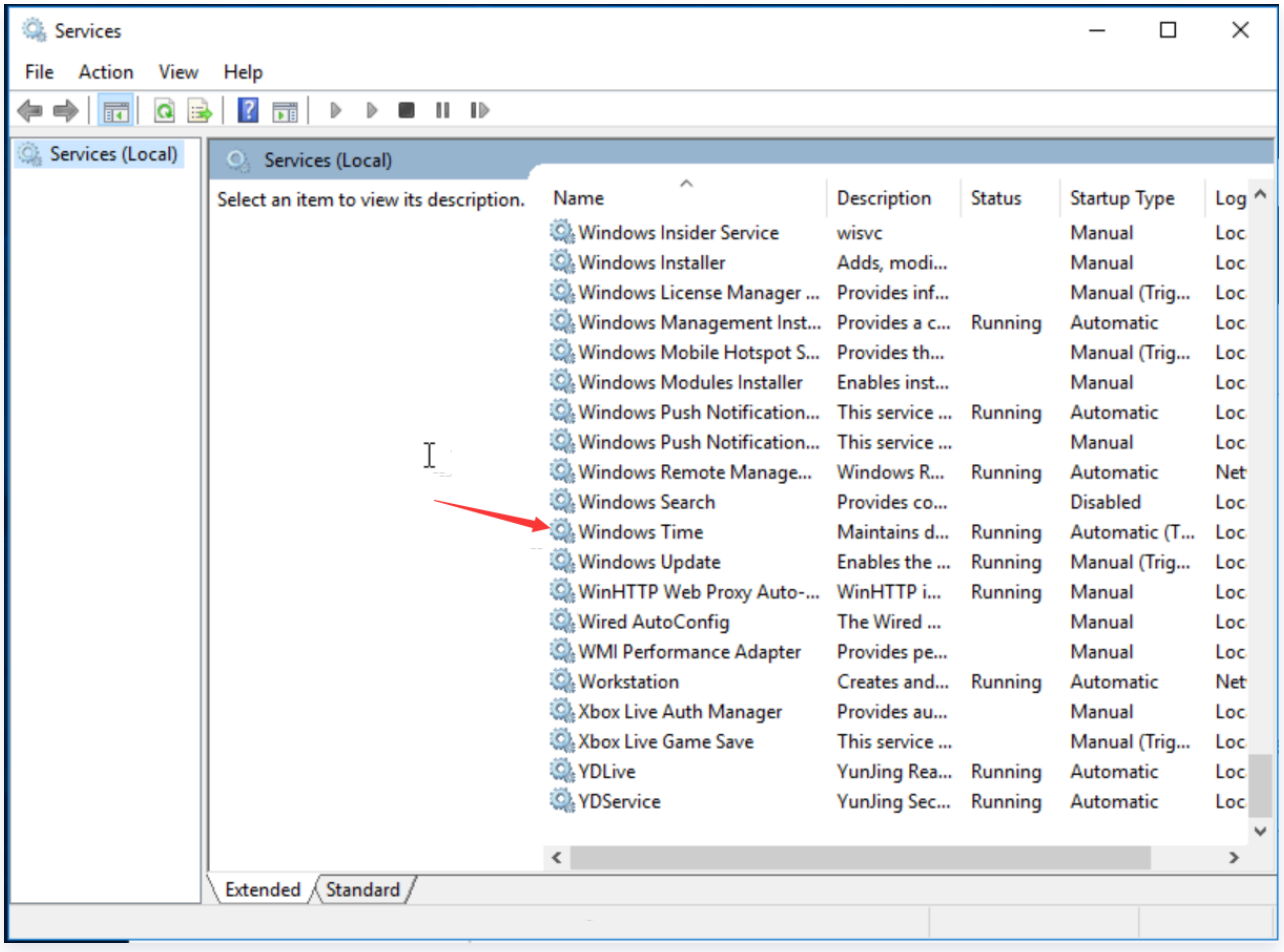
最終更新日：：2021-08-03 10:20:28

## ユースケース

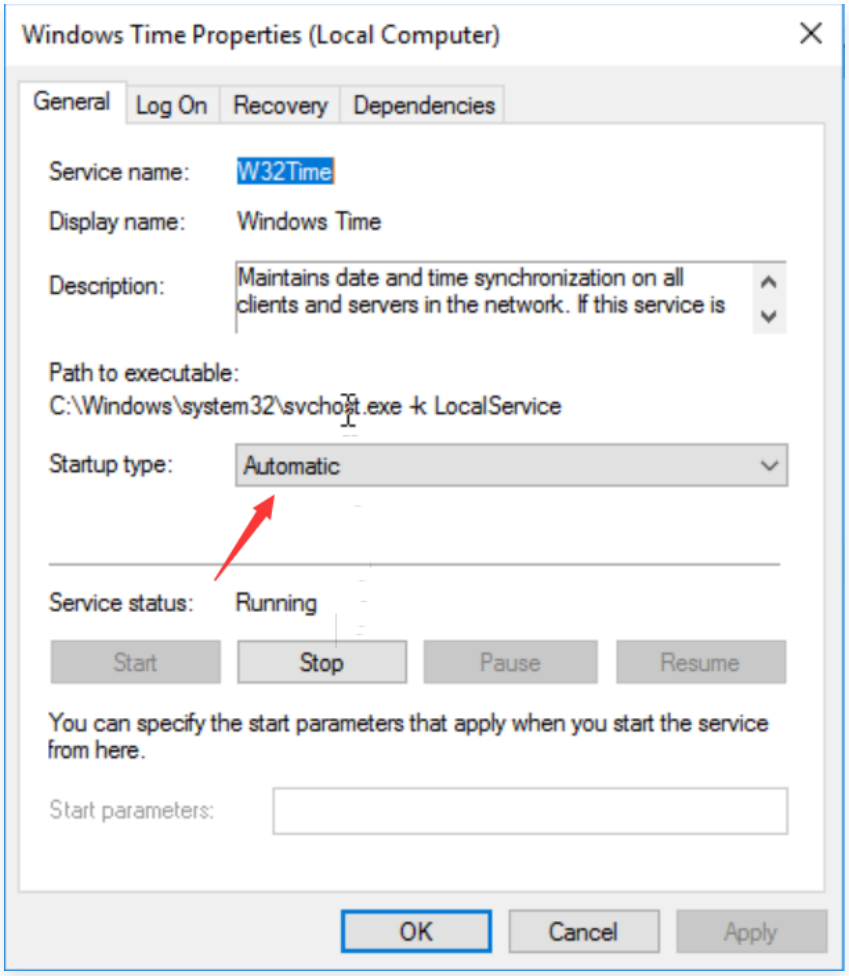
このドキュメントでは、Windows ServerでNTPサービスを有効にし、クロックソースサーバーのアドレスを変更する方法について説明します。
Windowsタイムサービス（Windows Time service、 W32Time）は、ローカルシステムとクロックソースサーバー間の時刻を同期するために使用されます。 ネットワークタイムプロトコル（NTP）を使用して、ネットワーク全体でコンピューターのクロックを同期します。 以下では、Windows Server 2016を例として、クライアントとコマンドラインを使用してNTPサービスを有効にし、クロックソースサーバーアドレスを変更する方法につ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

## 操作手順

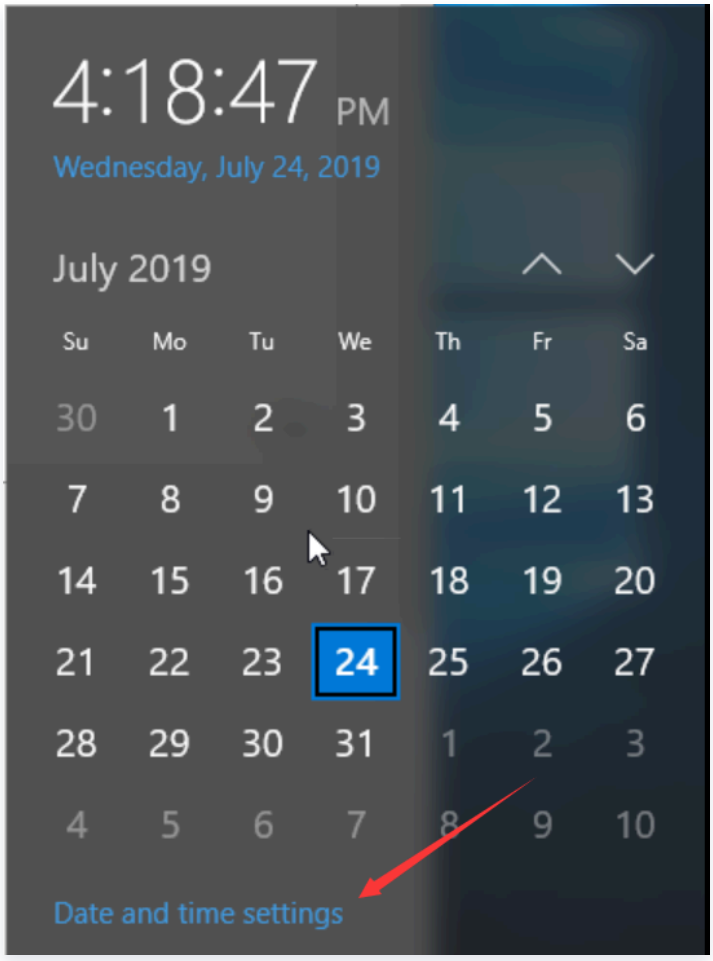
1. Windowsインスタンスへのリモートログイン 。
2. 「管理 > サービス > Windows Time」をクリックします。



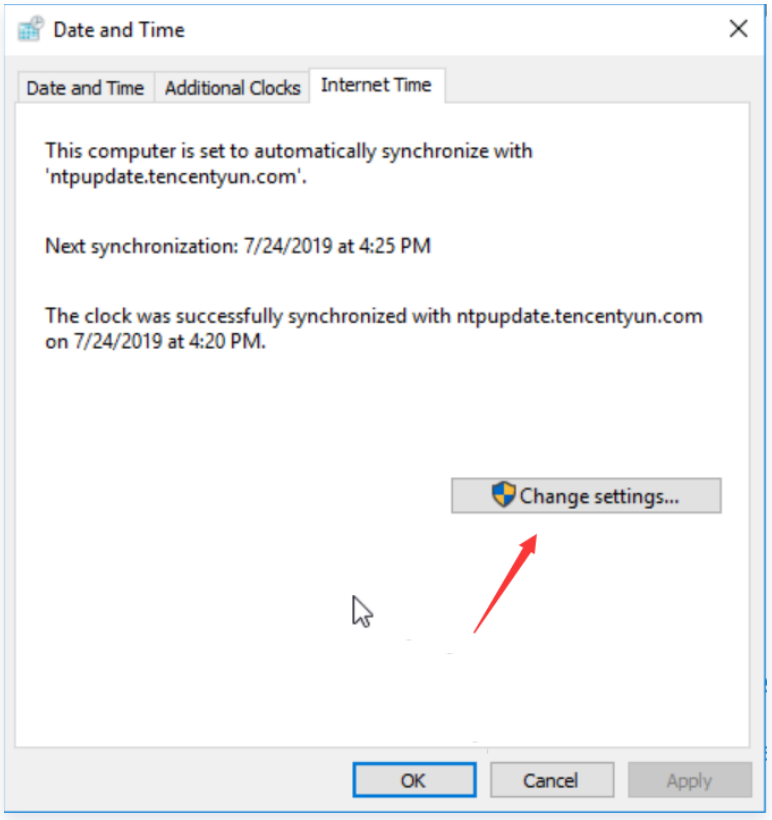
3. 起動の種類は「自動」に設定されています。サービスが起動されていない場合は、「起動」をクリックします。



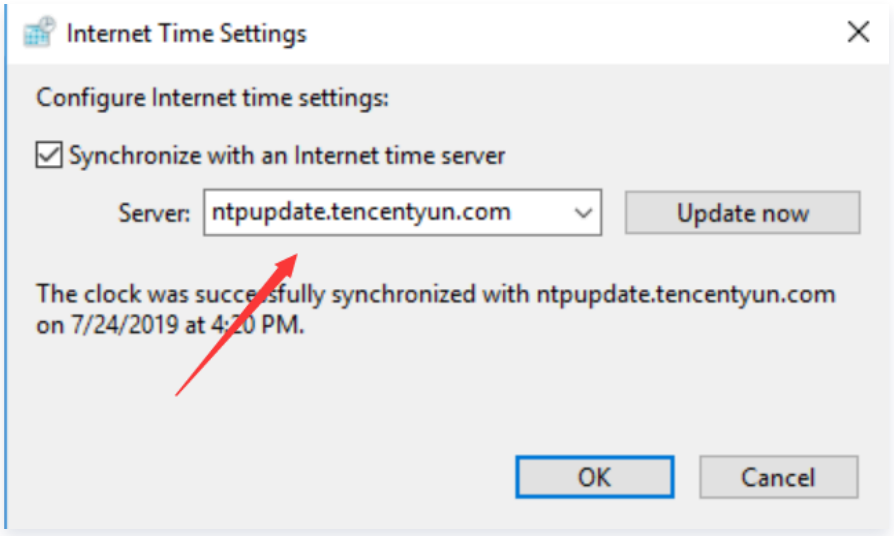
4. タスクバーの通知領域で、時刻をクリックし、「日付けと時刻」をクリックします。



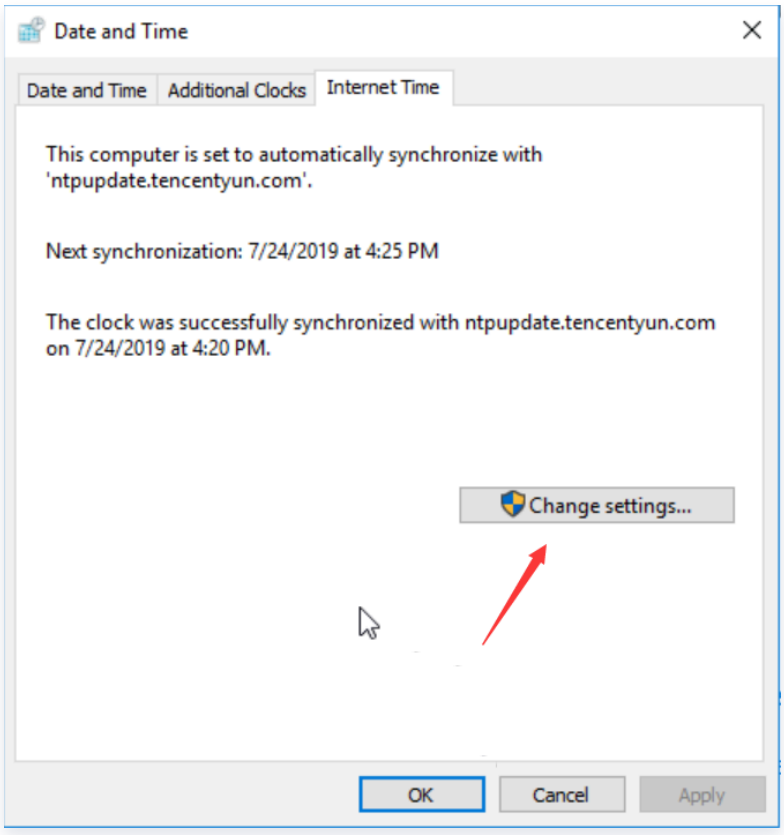
5. 「インターネット時刻」タグに切り替えて、設定の変更をクリックします。




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




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



# Dockerの構築

最終更新日：：2025-06-19 16:13:37

## 概要

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

> 説明：
> - Windows Subsystem for Linux（以下、WSL）は、Windows Server 2022システムの中でいくつかの制限があります。システムカーネルの完全性の原因で、WSL 1はLinux Dockerを実行できません。WSL 2はLinux Dockerを実行できますが、ハードウェアが二次仮想化をサポートするのが必要で、通常のCVM（Lighthouseを含む）は二次仮想化をサポートしていません。ですからWSL 1もWSL 2も通常のWindows CVM上ではLinux Dockerを実行できません。
> - Windowsの通常のCVM（Lighthouseを含む）はInstall Docker Desktop on Windowsをサポートしていません。Windowsのベアメタル物理マシンの場合は、Server 2022システムを選択することをお勧めします。詳細な情報については、関連ドキュメント マイクロソフト公式ドキュメント – コンテナ用のWindowsの準備 を参照して設定してください。

## デモ用オペレーティングシステム

本記事では、CVMインスタンスオペレーティングシステムとして、Tencent Cloudのパブリックイメージである TencentOS Server 4、TencentOS Server 3、CentOS 8.2、CentOS 7.9、Ubuntu 22.04、Debian 12.5、OpenCloudOS 9.0、OpenCloudOS 8.0を例に使用しています。
TencentOS Server 2.4 (TK4) オペレーティングシステムを使用している場合、イメージにはDockerが事前にインストールされており、再度インストールする必要はありません。詳細は、Dockerの使用について を参照に直接使用開始できます。

## 前提条件

Linux CVMを購入済みであること。

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

## 操作手順

### Dockerのインストール

ご使用のオペレーティングシステムのバージョンに応じて、以下の操作手順を実行してください:

1. 標準方式を使用してLinuxインスタンスにログイン（推奨）します。
2. Dockerのインストール。

### TencentOS Server 4

1. このバージョンのオペレーティングシステムのパブリックイメージには、Tencent CloudのDockerリポジトリが事前に設定されています。以下のコマンドを実行して、Dockerをインストールできます。

```
sudo yum install docker -y
```

2. 以下のコマンドを実行して、Dockerを起動します。

```
sudo systemctl start docker
```

3. 以下のコマンドを実行して、インストール結果を確認します。

```
sudo docker info
```

以下の情報が返された場合、インストール済みです。

```
Kernel Version: 6.6.47-12.tl4.x86_64
Operating System: TencentOS Server 4.2
OSType: linux
Architecture: x86_64
CPUs: 2
Total Memory: 1.669GiB
Name: VM-1-43-tencentos
ID: e2e75c93-4bcb-4b5e-9f59-33594f4d7f0a
Docker Root Dir: /var/lib/docker
Debug Mode: false
Experimental: false
Insecure Registries:
 127.0.0.0/8
Live Restore Enabled: true
```

### TencentOS Server 3

1. このバージョンのオペレーティングシステムのパブリックイメージには、Tencent CloudのDocker-ceリポジトリが事前に設定されています。以下のコマンドを実行してDockerをインストールできます。

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

2. 以下のコマンドを実行して、Dockerを起動します。

```
sudo systemctl start docker
```

3. 以下のコマンドを実行して、インストール結果を確認します。

```
sudo docker info
```

以下の情報が返された場合、インストール済みです。

```
Kernel Version: 5.4.241-1-tlinux4-0017.7
Operating System: TencentOS Server 3.2 (Final)
OSType: linux
Architecture: x86_64
CPUs: 2
Total Memory: 1.673GiB
Name: VM-1-33-tencentos
ID: c9427f12-0a4c-43f6-8e34-6dae619252f4
Docker Root Dir: /var/lib/docker
Debug Mode: false
Experimental: false
Insecure Registries:
 127.0.0.0/8
Live Restore Enabled: false
```

### CentOS 8.2

1. 以下のコマンドを実行して、Dockerリポジトリを追加し、Tencent Cloudリポジトリとして設定します。

```
sudo dnf config-manager --add-
repo=https://mirrors.cloud.tencent.com/docker-
ce/linux/centos/docker-ce.repo
sudo sed -i "s/download.docker.com/mirrors.tencentyun.com\/docker-
ce/g"  /etc/yum.repos.d/docker-ce.repo
```

2. 以下のコマンドを実行して、追加したDockerリポジトリを確認します。

```
sudo dnf list docker-ce
```

3. 以下のコマンドを実行して、Dockerをインストールします。

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

4. 以下のコマンドを実行して、Dockerを起動します。

```
sudo systemctl start docker
```

5. 以下のコマンドを実行して、インストール結果を確認します。

```
sudo docker info
```

以下の情報が返された場合、インストール済みです。

```
Kernel Version: 4.18.0-305.3.1.el8.x86_64
Operating System: CentOS Linux 8 (Core)
OSType: linux
Architecture: x86_64
CPUs: 2
Total Memory: 3.587GiB
Name: VM-2-14[illegible]
ID: 7GLW:CZKW:POYY:[illegible]
Docker Root Dir: /var/lib/docker
Debug Mode: false
Registry: https://index.docker.io/v1/
Labels:
Experimental: false
Insecure Registries:
 127.0.0.0/8
Live Restore Enabled: false
```

CentOS 7.9

1. 以下のコマンドを実行して、Dockerリポジトリを追加し、Tencent Cloudリポジトリとして設定します。

```
sudo yum-config-manager --add-
repo=https://mirrors.cloud.tencent.com/docker-
```

```
ce/linux/centos/docker-ce.repo
sudo sed -i "s/download.docker.com/mirrors.tencentyun.com\/docker-
ce/g"  /etc/yum.repos.d/docker-ce.repo
```

2. 以下のコマンドを実行して、追加したDockerリポジトリを確認します。

```
sudo yum list docker-ce
```

3. 以下のコマンドを実行して、Dockerをインストールします。

```
sudo yum install -y docker-ce
```

4. 以下のコマンドを実行して、Dockerを起動します。

```
sudo systemctl start docker
```

5. 以下のコマンドを実行して、インストール結果を確認します。

```
sudo docker info
```

以下の情報が返された場合、インストール済みです。

```
Kernel Version: 3.10.0-1160.108.1.el7.x86_64
Operating System: CentOS Linux 7 (Core)
OSType: linux
Architecture: x86_64
CPUs: 2
Total Memory: 3.607GiB
Name: VM-1-10-centos
ID: 8e9f79bf-4cc8-48db-9646-5335698358e4
Docker Root Dir: /var/lib/docker
Debug Mode: false
Experimental: false
Insecure Registries:
 127.0.0.0/8
Live Restore Enabled: false
```

### Ubuntu 22.04

1. 以下のコマンドを実行して、Dockerリポジトリを追加します。

```
sudo apt-get update
sudo apt-get install ca-certificates curl -y
sudo install -m 0755 -d /etc/apt/keyrings
sudo curl -fsSL https://mirrors.cloud.tencent.com/docker-
ce/linux/ubuntu/gpg -o /etc/apt/keyrings/docker.asc
sudo chmod a+r /etc/apt/keyrings/docker.asc
echo   "deb [arch=$(dpkg --print-architecture) signed-
by=/etc/apt/keyrings/docker.asc]
https://mirrors.cloud.tencent.com/docker-ce/linux/ubuntu/ \
  $(. /etc/os-release && echo "$VERSION_CODENAME") stable" |
sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt-get update
```

2. 以下のコマンドを実行して、Dockerをインストールします。

```
sudo apt-get install docker-ce docker-ce-cli containerd.io docker-
buildx-plugin docker-compose-plugin
```

3. 以下のコマンドを実行して、Dockerを起動します。

```
sudo systemctl start docker
```

4. 以下のコマンドを実行して、インストール結果を確認します。

```
sudo docker info
```

以下の情報が返された場合、インストール済みです。

```
Kernel Version: 5.15.0-107-generic
Operating System: Ubuntu 22.04 LTS
OSType: linux
Architecture: x86_64
CPUs: 2
Total Memory: 1.886GiB
Name: VM-3-38-ubuntu
ID: 259cce5e-0fa8-47ae-aeac-9255e6089b6e
Docker Root Dir: /var/lib/docker
Debug Mode: false
Experimental: false
Insecure Registries:
 127.0.0.0/8
Live Restore Enabled: false
```

Debian 12.5

1. 以下のコマンドを実行して、Dockerリポジトリを追加します。

```
sudo apt-get update
sudo apt-get install ca-certificates curl -y
sudo install -m 0755 -d /etc/apt/keyrings
sudo curl -fsSL https://mirrors.cloud.tencent.com/docker-
ce/linux/debian/gpg -o /etc/apt/keyrings/docker.asc
sudo chmod a+r /etc/apt/keyrings/docker.asc
echo   "deb [arch=$(dpkg --print-architecture) signed-
by=/etc/apt/keyrings/docker.asc]
https://mirrors.cloud.tencent.com/docker-ce/linux/debian/ \
  $(. /etc/os-release && echo "$VERSION_CODENAME") stable" |
sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt-get update
```

2. 以下のコマンドを実行して、Dockerをインストールします。

```
sudo apt-get install docker-ce docker-ce-cli containerd.io docker-
buildx-plugin docker-compose-plugin
```

3. 以下のコマンドを実行して、Dockerを起動します。

```
sudo systemctl start docker
```

4. 以下のコマンドを実行して、インストール結果を確認します。

```
sudo docker info
```

以下の情報が返された場合、インストール済みです。

```
Kernel Version: 6.1.0-23-amd64
Operating System: Debian GNU/Linux 12 (bookworm)
OSType: linux
Architecture: x86_64
CPUs: 2
Total Memory: 3.636GiB
Name: VM-0-3-debian
ID: dc83cb1f-137b-4968-aafd-f81111db71ec
Docker Root Dir: /var/lib/docker
Debug Mode: false
Experimental: false
Insecure Registries:
 127.0.0.0/8
Live Restore Enabled: false
```

### OpenCloudOS 9.0

1. 以下のコマンドを実行して、Dockerをインストールします。

```
sudo yum install docker -y
```

2. 以下のコマンドを実行して、Dockerを起動します。

```
sudo systemctl start docker
```

3. 以下のコマンドを実行して、インストール結果を確認します。

```
sudo docker info
```

以下の情報が返された場合、インストール済みです。

```
Kernel Version: 6.6.34-9.oc9.x86_64
Operating System: OpenCloudOS 9.2
OSType: linux
Architecture: x86_64
CPUs: 4
Total Memory: 7.384GiB
Name: VM-0-44-opencloudos
ID: c9c5b9a9-915b-4956-815f-e65d937b059a
Docker Root Dir: /var/lib/docker
Debug Mode: false
Experimental: false
Insecure Registries:
 127.0.0.0/8
Live Restore Enabled: true
```

### OpenCloudOS 8.0

1. 以下のコマンドを実行して、Dockerリポジトリを追加し、Tencent Cloudリポジトリとして設定します。

```
sudo dnf config-manager --add-
repo=https://mirrors.cloud.tencent.com/docker-
ce/linux/centos/docker-ce.repo
sudo sed -i "s/download.docker.com/mirrors.tencentyun.com\/docker-
ce/g"  /etc/yum.repos.d/docker-ce.repo
```

2. 以下のコマンドを実行して、追加したDockerリポジトリを確認します。

```
sudo dnf list docker-ce
```

3. 以下のコマンドを実行して、Dockerをインストールします。

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

4. 以下のコマンドを実行して、Dockerを起動します。

```
sudo systemctl start docker
```

5. 以下のコマンドを実行して、インストール結果を確認します。

```
sudo docker info
```

以下の情報が返された場合、インストール済みです。

```
Kernel Version: 5.4.119-20.0009.32
Operating System: OpenCloudOS 8.10
OSType: linux
Architecture: x86_64
CPUs: 4
Total Memory: 7.392GiB
Name: VM-0-44-opencloudos
ID: 1fea4104-2f1e-4c61-9a97-43b2dfb56c8e
Docker Root Dir: /var/lib/docker
Debug Mode: false
Experimental: false
Insecure Registries:
 127.0.0.0/8
Live Restore Enabled: false
```

## Dockerの使用

Dockerを使用するための基本的なコマンドは次のとおりです：

- Dockerデーモンを管理します。
  - Dockerデーモンを実行します：

    ```
    sudo systemctl start docker
    ```

  - Dockerデーモンを停止します：

    ```
    sudo systemctl stop docker
    ```

  - Dockerデーモンを再起動します：

    ```
    sudo systemctl restart docker
    ```

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

  ```
  sudo docker pull nginx
  ```

  > ⚠ 注意：

> docker pullコマンドで「Get "https://registry-1.docker.io/v2/": xxxxx (Client.Timeout exceeded while awaiting headers)」というエラーが表示された場合、ネットワークの問題が起きたことを示しています。Tencent Cloudのイメージソースを利用してDockerを加速する を参考にリポジトリを変更することをお勧めします。

- タグの変更：イメージタグを変更して、違いを記憶させることができます。

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

- 既存イメージを確認します：

```
sudo docker images
```

- イメージを強制的に削除します：

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

- コンテナを管理します。
  - 実行してコンテナに入る：

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

その中で、`ImageId` は `docker images` コマンドを実行することで取得できます。現在のSSH接続ウィンドウを直接終了するか、「Ctrl+pとCtrl+q」のショートカットキーを押すことで、入ったコンテナをバックグラウンドに移動させます。

  - バックグラウンドで実行されているコンテナ内で新しいbashプロセスを実行する：

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

exitコマンドを実行してbashプロセスを終了します。

  - バックグラウンドのコンテナを確認する：

```
sudo docker ps     # 実行中のコンテナを確認します。
sudo docker ps -a     # 全てのコンテナを確認します。
```

  - 終了したコンテナを再起動する：

```
docker start <コンテナID>
```

終了したコンテナは `sudo docker ps -a` コマンドで確認できます。コマンド出力のSTATUS列に「Exited」が含まれているものが終了したコンテナです。

- コンテナをイメージ化します:

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

例:

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

## イメージの作成

1. 次のコマンドを実行して、Dockerfileファイルを開きます。

```
sudo vim Dockerfile
```

2. iを押して編集モードに切り替え、次の内容を追加します。

```
#ベースイメージのソースを宣言します。
FROM tencentyun/nginx:v2
#イメージの所有者を宣言します。
MAINTAINER DTSTACK
#RUNの後ろには、コンテナを実行する前に実行する必要のあるコマンドが続きます。
Dockerfileは127行を超えることはできないため、コマンドが多い場合は、スクリプトに記
述して実行することをお勧めします。
RUN mkdir /dtstact
RUN apt update && apt install -y iputils-ping
#ブートコマンドです。ここでの最後のコマンドは、フォアグラウンドで継続的に実行できる
コマンドである必要があります。そうでない場合、コンテナはバックグラウンドで実行され、
コマンドの実行が終了した時点でログアウトします。
ENTRYPOINT ping cloud.tencent.com
```

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

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

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

```
sudo docker images
```

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

```
sudo docker run -d nginxos:v1          #コンテナをバックグラウンドで実行します。
sudo docker ps                         #現在実行中のコンテナを確認します。
sudo docker ps -a                      #実行されていないコンテナを含むすべてのコンテナを確認します。
sudo docker logs CONTAINER ID/IMAGE    #先ほど実行したコンテナが表示されない場合は、コンテナIDまたはコンテナ名でブートログを確認し、トラブルシューティングを行います。
```

7. 次のコマンドを順に実行して、イメージを作成します。

```
sudo docker commit fb2844b6**** nginxweb:v2 #commitパラメータの後に、コンテナID、作成する新しいイメージの名前とバージョン番号を追加します。
sudo docker images                         #ローカル（ダウンロード済みおよびローカルで作成された）イメージを一覧表示します。
```

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

> ⚠ 注意：
> - ここでは、サーバーが https://registry-1.docker.io に正常にアクセスできる必要があります。それ以外の場合、タイムアウトエラーが報告されます。
> - タイムアウトエラーの解決方法は、アクセス可能な他のリポジトリにプッシュすることです。例えば、 Tencent Cloud Tencent Container Registry にプッシュするなど。

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

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

# 可視化ページの構築
# Ubuntu可視化インターフェースの構築

最終更新日：：2025-09-05 17:15:02

## 概要

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

## 前提条件

Ubuntu OSを搭載した Linux インスタンスを購入しました。

## 操作手順

### インスタンスセキュリティグループの設定

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

### ソフトウェアパッケージのインストール

Ubuntu 18.04

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

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

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

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

4. 次のコマンドを実行して VNC をインストールします。

```
apt-get install vnc4server
```

### Ubuntu 20.04

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

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

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

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

4. 次のコマンドを実行して VNC をインストールします。

```
apt-get install tightvncserver
```

### Ubuntu 22.04

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

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

3. デスクトップ環境をインストールします。

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

4. 次のコマンドを実行して VNC をインストールします。

```
sudo apt install tightvncserver
```

## VNCの構成

Ubuntu 18.04

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

```
vncserver
```

次のような結果が返された場合は、VNCが正常に起動されたことを示します。

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

You will require a password to access your desktops.

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

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

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

2. 次のコマンドを実行して、VNC 構成ファイルを開きます。

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

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

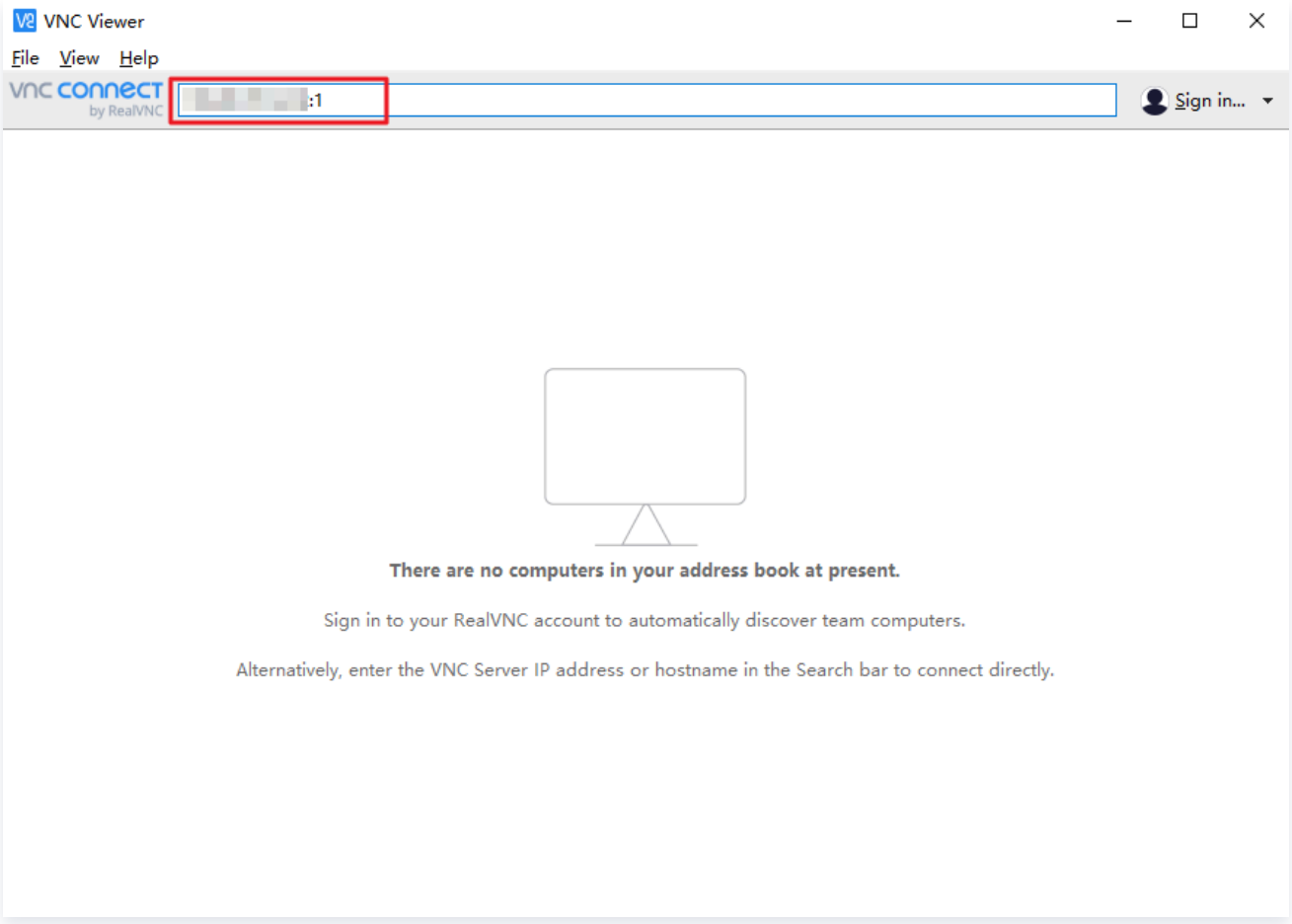
```
#!/bin/sh
export XKL_XMODMAP_DISABLE=1
export XDG_CURRENT_DESKTOP="GNOME-Flashback:GNOME"
export XDG_MENU_PREFIX="gnome-flashback-"
gnome-session --session=gnome-flashback-metacity --disable-
acceleration-check &
```

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

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

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

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




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

## Ubuntu 20.04

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

```
vncserver
```

次のような結果が返された場合は、VNCが正常に起動されたことを示します。

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

You will require a password to access your desktops.

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

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

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

2. 次のコマンドを実行して、VNC 構成ファイルを開きます。

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

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

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

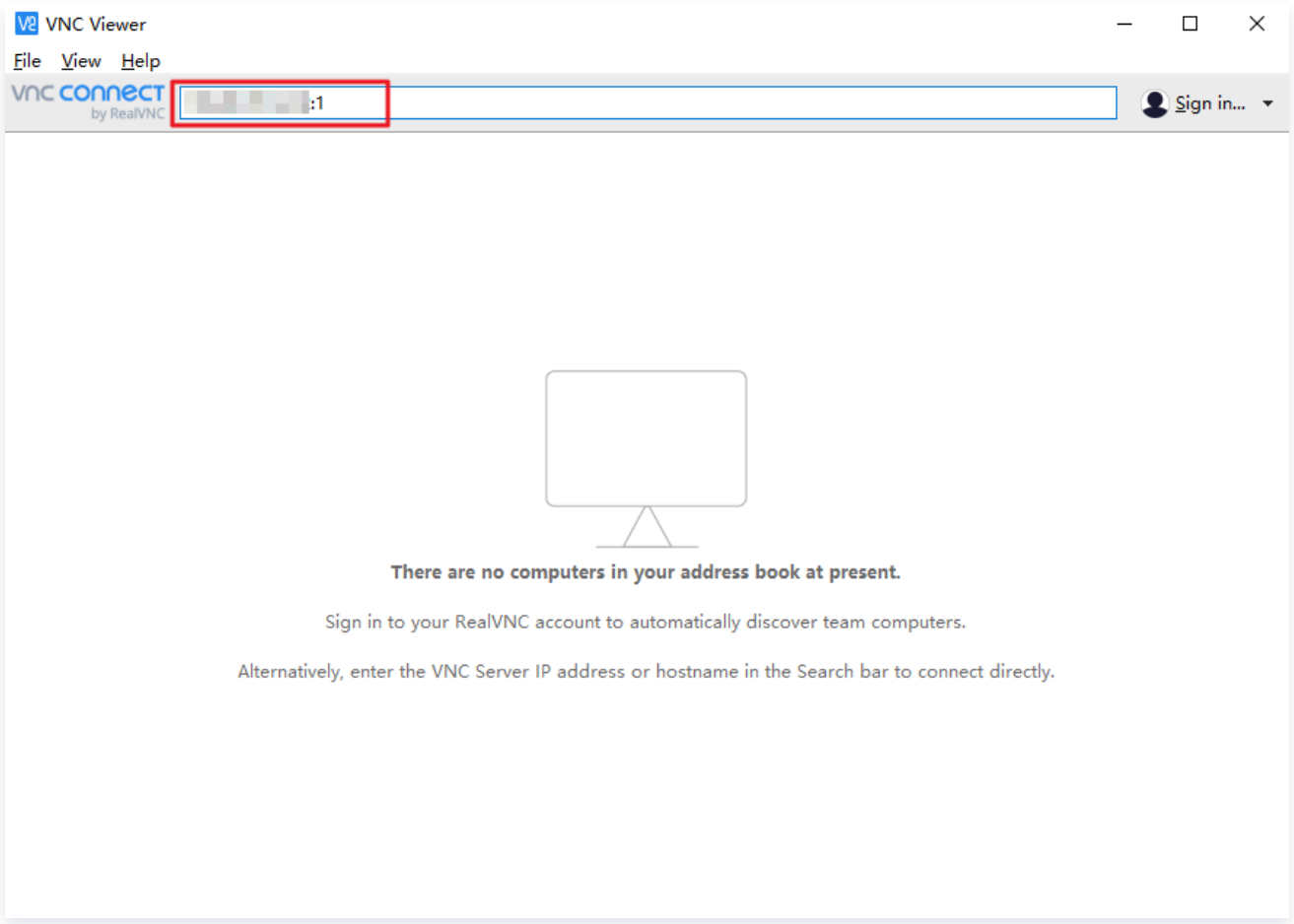
4. Escを押し、**:wq**を入力して、ファイルを保存して戻ります。
5. 次のコマンドを実行して、デスクトッププロセスを再起動します。

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

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

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

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




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

## Ubuntu 22.04

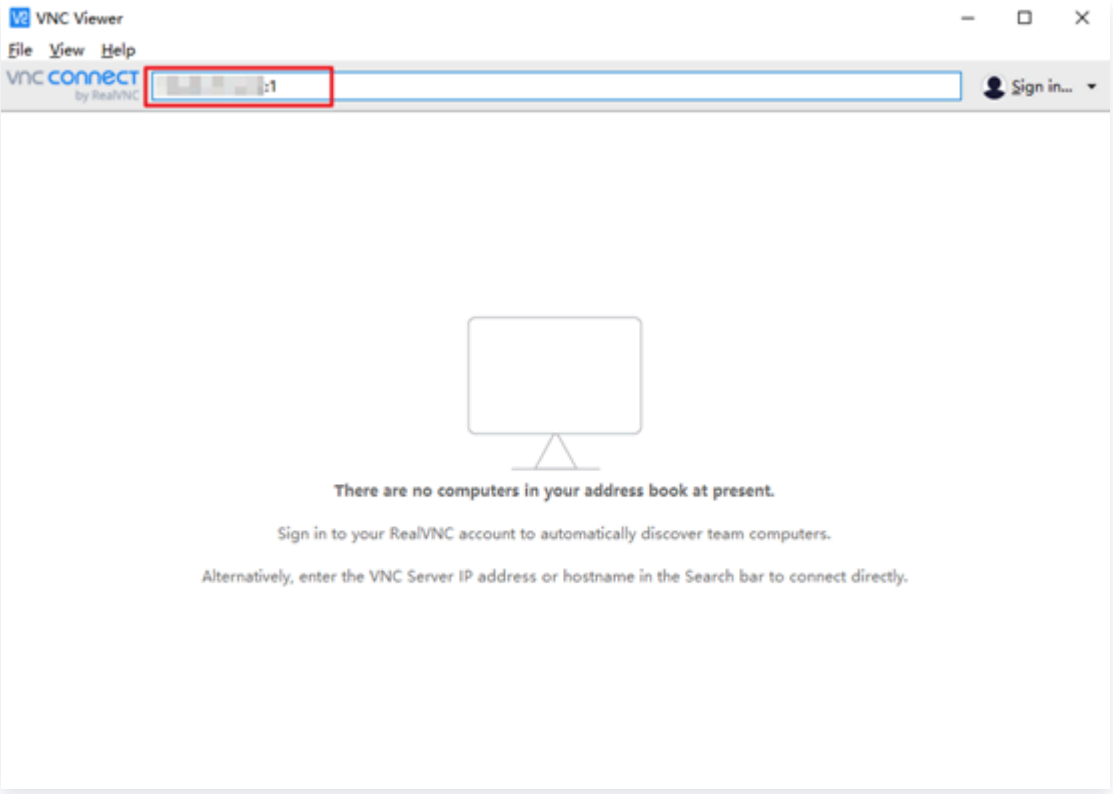
1. 次のコマンドを実行してVNCサービスを起動し、パスワードを設定します。

```
vncserver
```

次のような結果が返された場合は、VNCが正常に起動されたことを示します。

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

You will require a password to access your desktops.

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

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

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

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




4. ポップアップしたダイアログボックスで **Continue **をクリックします。
5. 前の手順で作成したパスワードを入力し、OK をクリックします。

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

付録:

Chrome をインストールする:

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

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

- .deb ファイルをインストールする

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

# CentOS可視化インターフェースの構築

最終更新日：：2022-07-12 10:50:32

## 操作シナリオ

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

## 説明事項

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

## 操作手順

実際に使用するCVMのOSに応じて、次の手順を参照して操作を行ってください。

### CentOS 8.2

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

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

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

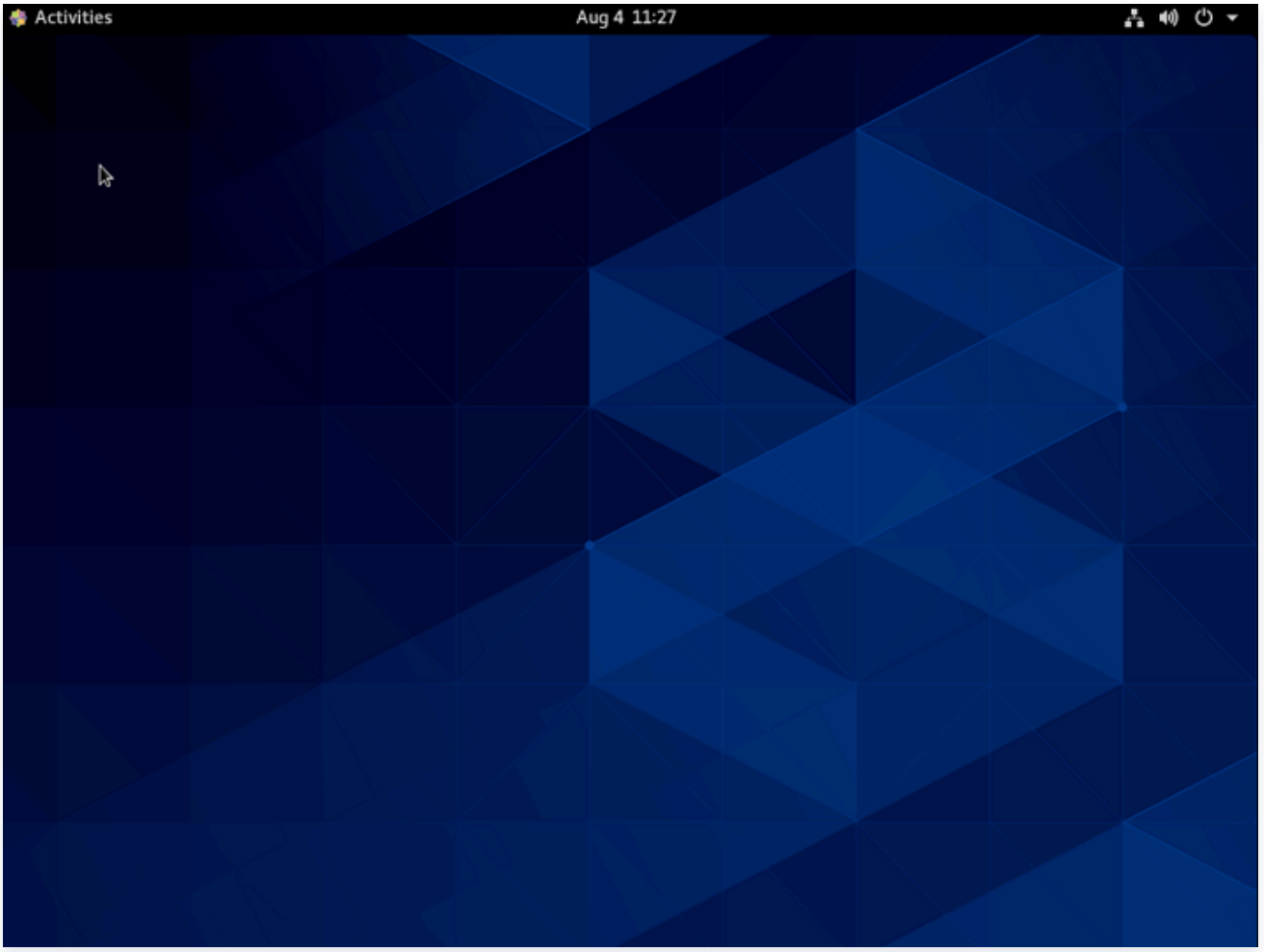
```
systemctl set-default graphical
```

4. 以下のコマンドを実行して、インスタンスを再起動します。

```
reboot
```

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

下図に示します。




CentOS 7.9

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

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

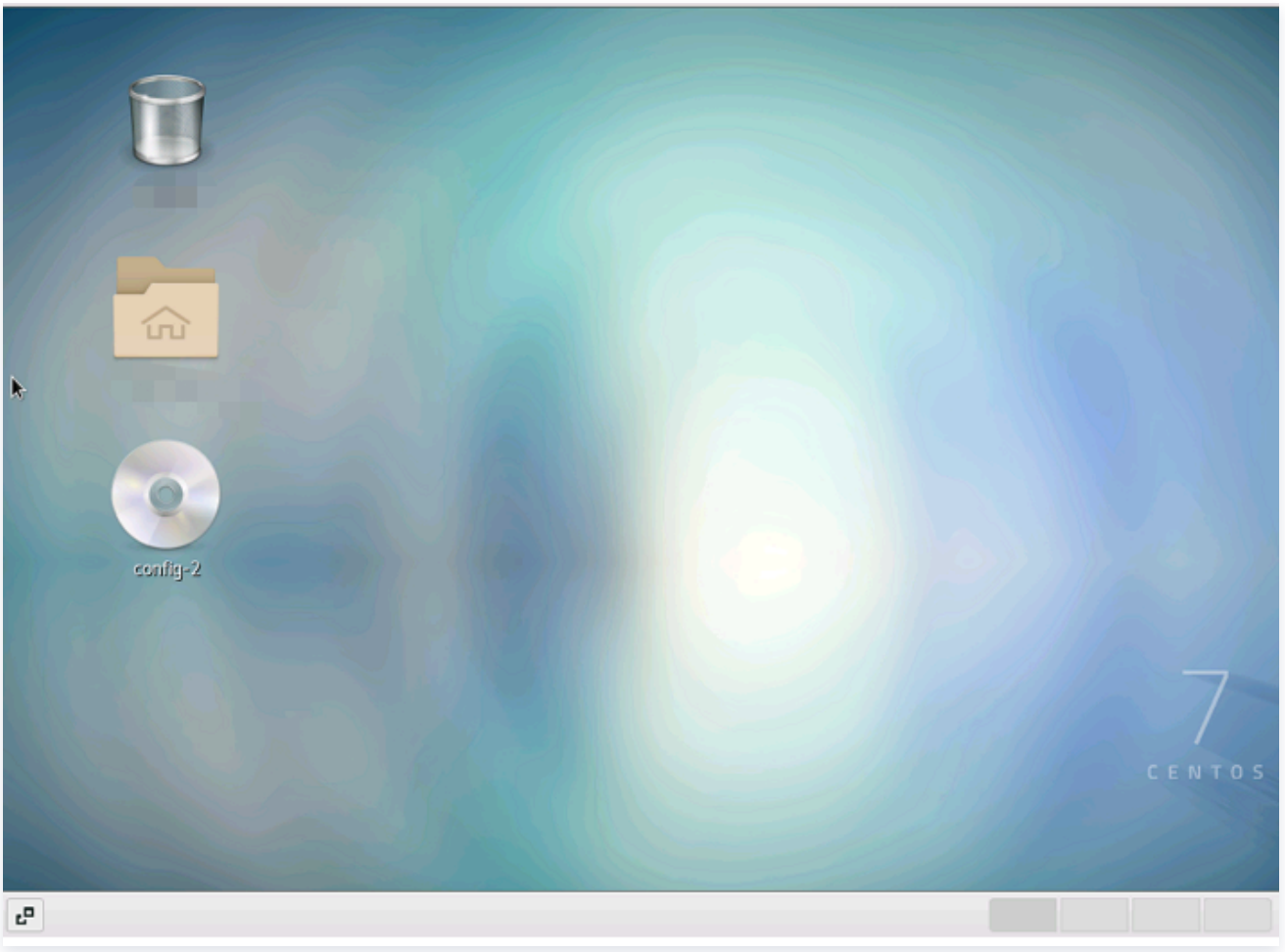
3. 以下のコマンドを実行し、デフォルトのグラフィックインターフェースを設定します。

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

4. 以下のコマンドを実行して、インスタンスを再起動します。

```
reboot
```

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



# ローカルファイルをCVMへアップロード
# ローカルファイルをCVMへアップロードする方法

最終更新日：：2022-07-07 16:19:39

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

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

ローカルコンピュータのOSがWindowsであり、購入したCVMのOSがLinuxの場合は、WinSCP方式でファイルをCVMにアップロードすることができます。

> 説明：
> アップロードしたいファイルが36KB未満で、なおかつテキストファイルの場合はファイルをCVMにアップロードする方式をお勧めします。コンソール上での簡単な操作でファイルをアップロードできます。

## 次の操作

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

## 問題が発生した場合

ご不便をおかけして申し訳ございません。チケットを提出 してお問い合わせください。もしくは先に関連ドキュメントをご参照の上、問題の特定および対処を行っていただくこともできます。
以下は、CVMをご使用中のユーザーからのよくあるご質問です。先にドキュメントをご参照の上、問題の特定および対処を行っていただくことをお勧めします。

- CVMのログインパスワードを忘れました。
  インスタンスのパスワードをリセット をご参照ください。
- CVMにログインできません。
  Windowsインスタンスにログインできない または Linuxインスタンスにログインできない をご参照ください。

# WindowsシステムからMSTSC経由でWindowsインスタンスへファイルをアップロード

最終更新日：：2022-03-24 15:19:52

## 概要

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

## 前提条件

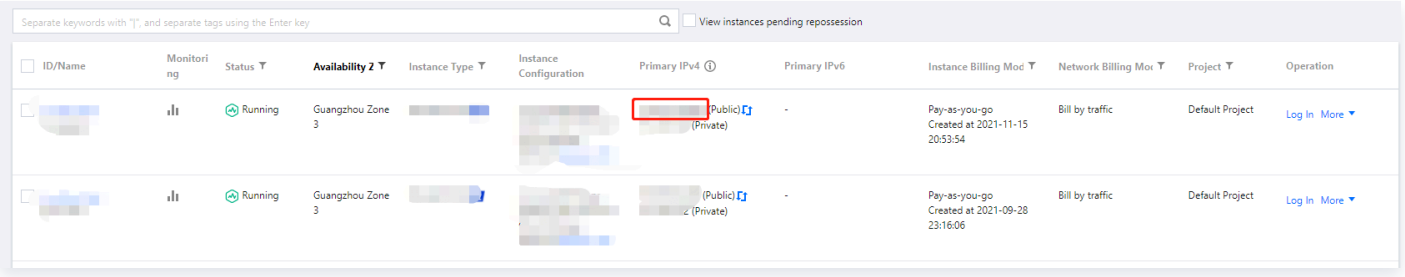
Windows CVM がパブリックネットワークにアクセスできることを確認してください。

## 操作手順

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

### パブリックIPの取得

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




### ファイルのアップロード

1. ローカルコンピュータで、ショートカットキーWindows + Rを使用して実行ウィンドウを開きます。
2. ポップアップした「実行」ウィンドウでmstscと入力し、OKをクリックして「リモートデスクトップ接続」ダイアログボックスを開きます。

3. 「リモートデスクトップ接続」ダイアログボックスで、CVMパブリックIPアドレスを入力し、オプションをクリックします。
4. 通常タブで、CVMのパブリックネットワークのIPアドレスとユーザー名Administratorを入力します。
5. ローカルリソースタブを選択し、詳細情報をクリックします。
6. 下図のように、ポップアップした「ローカルデバイスとリソース」ウィンドウで、ドライブモジュールを選択し、Windows CVMにアップロードしたいファイルが存在するローカルディスクにチェックを入れ、OKをクリックします。
7. ローカル設定完了後、接続をクリックし、ポップアップした「Windowsセキュリティ」ウィンドウで、インスタンスのログインパスワードを入力し、Windows CVMにリモートログインします。
8. Windows CVMで、  を選択し、開いたウィンドウでこのコンピュータをクリックすると、CVMにマウントされているローカルディスクを確認することができます。
9. ダブルクリックしてマウントされたローカルハードディスクを開き、Windows CVMの他のハードディスクにコピーする必要があるローカルファイルをレプリケートすると、ファイルのアップロード操作は完了です。
例えば、ローカルハードディスク(F)のAファイルをWindows CVMのCドライブにレプリケートします。

## ファイルのダウンロード

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

# MacOSシステムからMRD経由でWindowsインスタンスへファイルをアップロード

最終更新日：：2021-12-27 11:18:37

## シナリオ

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

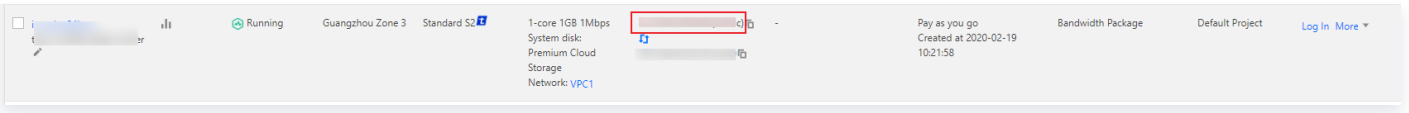
## 前提条件

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

## 操作手順

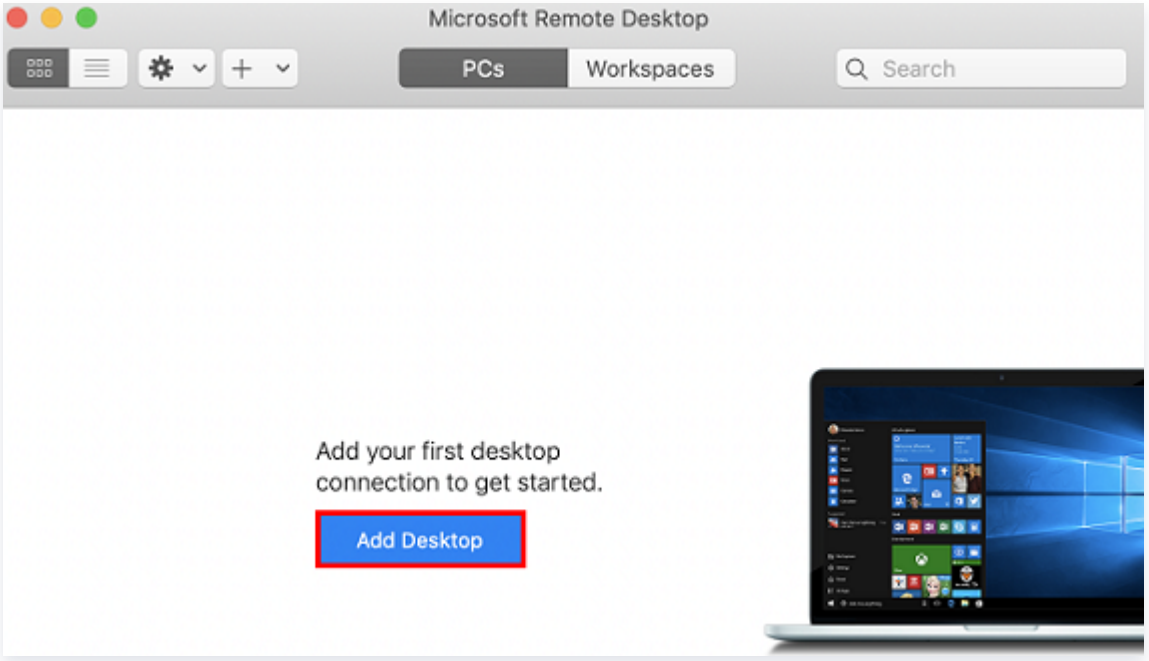
### パブリックIPを取得する

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

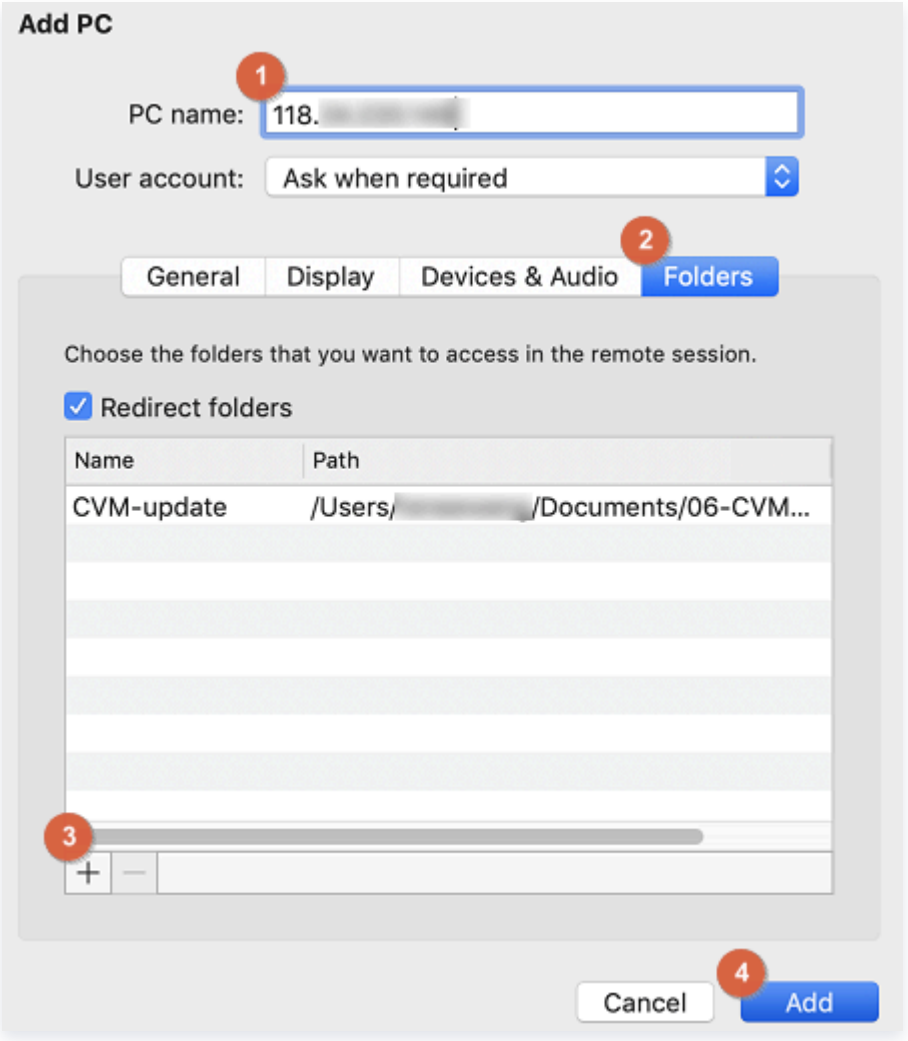



### ファイルをアップロードする

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




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



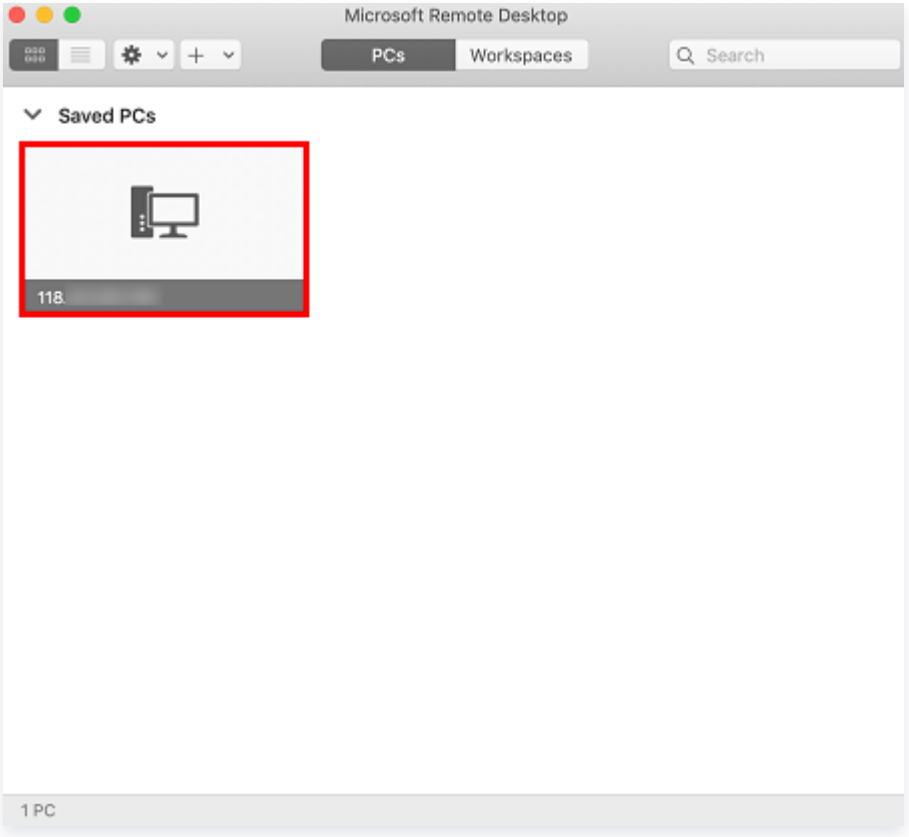
2.1 「PC name」に CVMのパブリックIPアドレスを入力します。

2.2 Foldersをクリックして、フォルダリストに切り替えます。

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

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

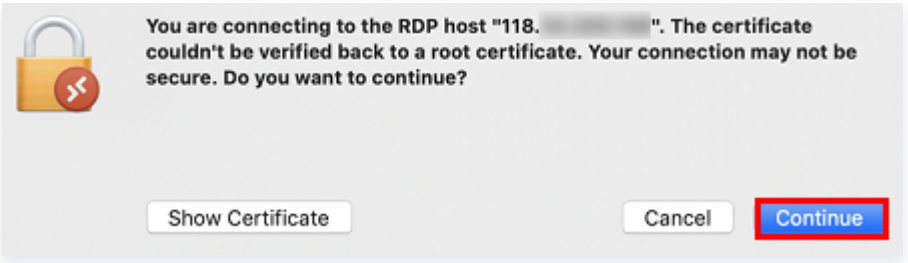
2.5 他のオプションはデフォルト設定のままにして、接続を作成します。
ウィンドウで作成された接続を確認できます。次の図に示すように:



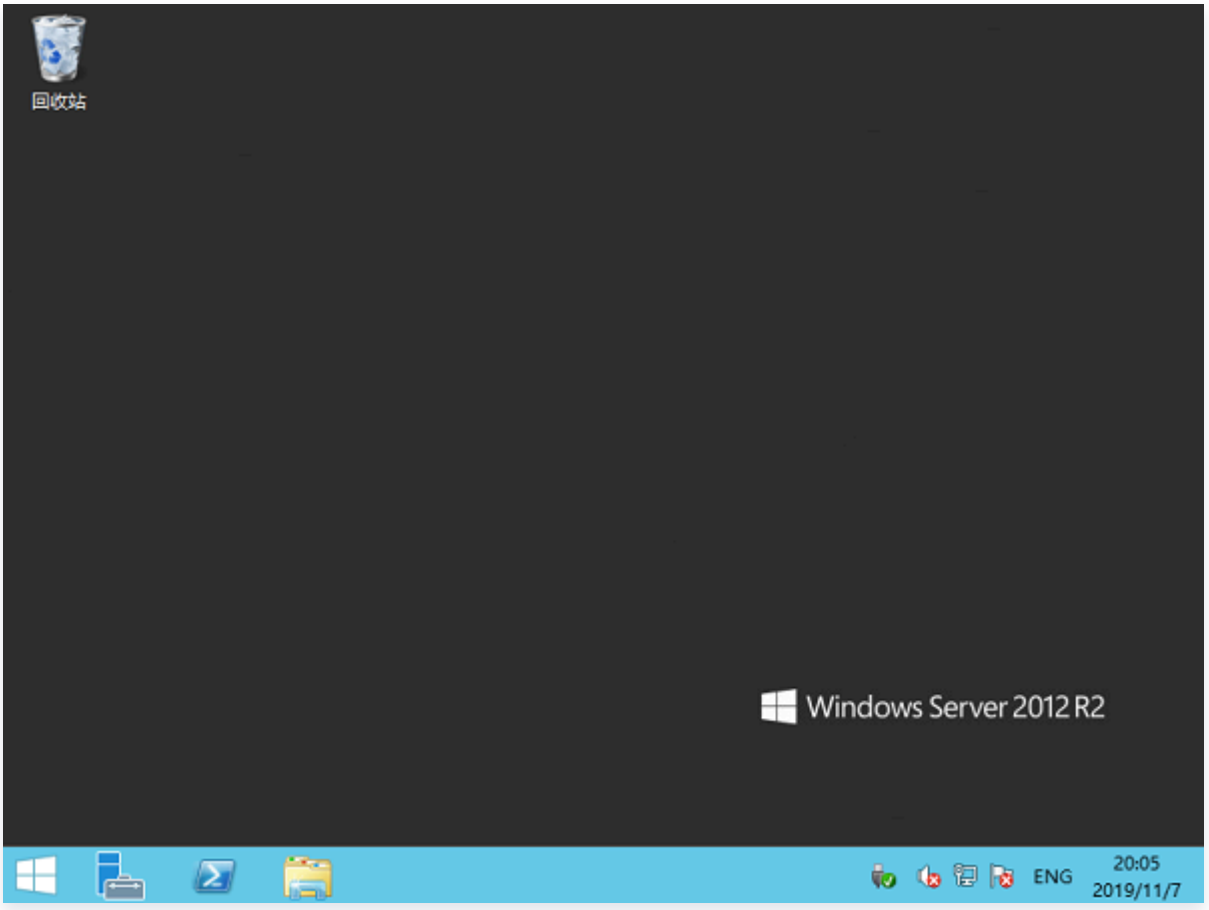

3. 新しく作成した接続をダブルクリックして開き、表示されるダイアログボックスでプロンプトに従って、CVMのアカウントとパスワードを入力し、Continueをクリックしてください。

> 説明:
> - Windows CVMのデフォルトアカウントは `Administrator` です。
> - システムのデフォルトパスワードを使用してインスタンスにログインする場合は、サイト内メール にアクセスしてパスワードを取得してください。
> - パスワードを忘れた場合、インスタンスパスワードのリセット を行ってください。

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




接続が成功すると、次のページが表示されます。




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

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

## ファイルをダウンロードする

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

# LinuxシステムからRDP経由でWindowsインスタンスへファイルをアップロード

最終更新日：：2021-10-27 17:20:01

## 操作シナリオ

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

> 説明：
> - ローカルLinuxマシンはビジュアルインターフェースを構築する必要があり、構築しないとrdesktopが使えません。
> - ここではLinuxマシンのOSに、CentOS 7.6を使用した場合を例として取り上げます。OSのバージョンによって手順が異なる場合がありますので、実際の業務状況に応じてドキュメントを参照して操作を行ってください。

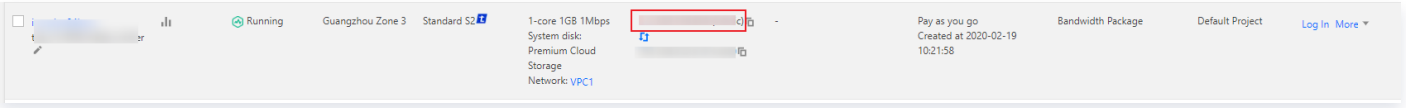
## 前提条件

Windows CVMを購入済みであること。

## 操作手順

### パブリックIPの取得

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




### rdesktopのインストール

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

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

```
-1.8.3.tar.gz
```

最新のインストールパッケージが必要な場合は、GitHub rdesktopページ にアクセスし、最新のインストールパッケージを検索して、コマンドラインで最新のインストールパスに置き換えることができます。

2. 次のコマンドを順番に実行して、インストールパッケージを解凍し、インストールディレクトリに入ります。

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

```
cd rdesktop-1.8.3
```

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

```
./configure
```

```
make
```

```
make install
```

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

```
rdesktop
```

## ファイルのアップロード

1. 次のコマンドを実行して、CVMと共有するフォルダを指定します。

```
rdesktopCVMパブリックIP  -u CVMアカウント -pCVMログインパスワード -r disk:指定された共有フォルダ名=ローカルフォルダパス
```

> **説明:**
> - CVMのアカウントはデフォルトで `Administrator` となります。
> - システムのデフォルトパスワードを使用してインスタンスにログインする場合は、サイト内メッセージ に進んで取得してください。
> - パスワードを忘れた場合は、インスタンスのパスワードをリセット してください。

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

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

共有が成功すると、Windows CVMのインターフェースが開きます。

左下隅にある  > このコンピュータを選択し、CVMシステムインターフェースで共有フォルダを表示することができます。

2. ダブルクリックして共有フォルダを開き、Windows CVMの他のハードディスクにアップロードする必要があるローカルファイルをレプリケートすると、ファイルのアップロード操作は完了です。
例えば、 `share` フォルダ内のAファイルをWindows CVMのCドライブにレプリケートします。

## ファイルのダウンロード

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

# WindowsシステムからWinSCP経由でLinuxインスタンスへファイルをアップロード

最終更新日：：2022-03-21 17:38:47

## 概要

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

## 前提条件

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

## 操作手順

### WinSCP にログインする

1. WinSCPを開くと、「WinSCPログイン」ダイアログボックスが表示されます。
2. ログインパラメータを設定する：
   - プロトコル：オプションSFTPまたはSCPのうちどちらでも構いません。
   - ホスト名：CVMのパブリックIPです。CVMコンソール にログインすると、対応するCVMのパブリックIPが確認できます。
   - ポート：デフォルトは22です。
   - ユーザー名：CVMにログインするためのユーザー名です。

   > 説明：
   > Linuxインスタンスのデフォルトの管理者ユーザー名はroot、Ubuntuシステムのインスタンスはubuntuです。Ubuntu OSをお使いの場合は、Ubuntuシステムでrootユーザーでインスタンスにログインするをを参照して構成した後、rootを使用してログインしてください。

   - パスワード：ユーザー名に対応するパスワードです。
     - システムのデフォルトパスワードを使用してインスタンスにログインする場合は、サイト内メール にアクセスしてパスワードを取得してください。
     - パスワードを忘れた場合は、インスタンスのパスワードをリセット してください。
3. ログインをクリックして、「WinSCP」ファイル転送インターフェースに入ります。

## ファイルのアップロード

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

## ファイルのダウンロード

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

# LinuxまたはMacOSシステムからSCP経由でLinuxインスタンスへファイルをアップロード

最終更新日：：2022-07-08 18:53:29

## 概要

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

## 前提条件

Linux CVMを購入済みであること。

## 操作手順

### パブリックIPの取得

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


### ファイルのアップロード

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

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

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

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

> **説明：**

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

2. yesを入力してからEnterを押してアップロードを確認し、ログインパスワードを入力すると、アップロードが完了します。
   - システムのデフォルトパスワードを使用してインスタンスにログインする場合は、サイト内メール にアクセスしてパスワードを取得してください。
   - パスワードを忘れた場合は、インスタンスのパスワードをリセット してください。

## ファイルのダウンロード

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

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

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

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

# LinuxシステムからFTP経由でCVMへファイルをアップロード

最終更新日：：2020-07-23 17:27:10

## 操作シナリオ

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

## 前提条件

Cloud Virtual Machine(CVM)にFTPサービスを構築済み。

- FTPを使用してファイルをLinux CVMにアップロードするには、Linux CVMでFTPサービスの構築 をご参照ください。
- FTPを使用してファイルをWindows CVMにアップロードするには、Windows CVMでFTPサービスの構築 をご参照ください。

## 操作手順

### CVMへの接続

1. 次のコマンドを実行し、FTPサービスをインストールします。

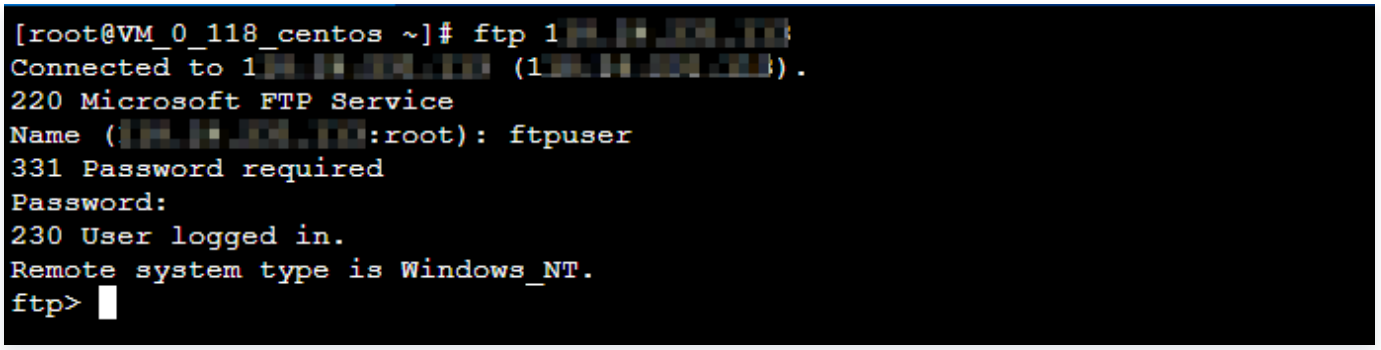
   > **説明：**
   > LinuxシステムのローカルPCにFTPサービスがインストールされている場合は、このステップをスキップして次に進んでください。

   ```
   yum -y install ftp
   ```

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

   ```
   ftp CVMのIPアドレス
   ```

次の画面に進むと、接続は正常に確立されています。




## ファイルのアップロード

次のコマンドを実行して、ローカルファイルをCVMにアップロードします。

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

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

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

## ファイルのダウンロード

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

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

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

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

# WindowsシステムからFTP経由でCVMへファイルをアップロード

最終更新日：：2022-07-27 11:43:01

## 操作シナリオ

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

## 前提条件

Cloud Virtual Machine(CVM)にFTPサービスを構築済み。

- FTPを使用してファイルをLinux CVMにアップロードするには、Linux CVMでFTPサービスの構築 をご参照ください。
- FTPを使用してファイルをWindows CVMにアップロードするには、Windows CVMでFTPサービスの構築 をご参照ください。

## 操作手順

### CVMへの接続

1. オープンソースソフトウェアFileZillaをローカルでダウンロードしてインストールします。

> 説明：
> バージョン3.5.3のFileZillaを使用してFTP経由でファイルをアップロードすると、アップロードが失敗する場合があります。公式WebサイトからFileZillaのバージョン3.5.1または3.5.2をダウンロードして使用することをお勧めします。

2. FileZillaを開きます。
3. FileZillaウィンドウで、ホスト、ユーザー名、パスワード、ポートなどの情報を入力して、クイック接続をクリックします。

設定情報の説明：

- ホスト：CVMのパブリックIPです。 CVMコンソール のインスタンス管理画面で、CVMのパブリックIPを確認できます。
- ユーザー名：FTPサービスの構築 で設定されたFTPユーザーのアカウントです。 図では、「ftpuser1」を例に説明します。
- パスワード：FTPサービスの構築 で設定されたFTPユーザーアカウントに対応するパスワードです。
- ポート：FTPリスニングポートです。デフォルトは21です。
  接続が成功したら、リモートCVMサイトでファイルを表示できます。

## ファイルのアップロード

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

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

## ファイルのダウンロード

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

# ネットワークパフォーマンステスト
# ネットワークパフォーマンステストの概要

最終更新日：：2021-10-27 11:57:15

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

- netperfを使用したテスト
- DPDKを使用したテスト

# netperfを使用したテスト

最終更新日：：2025-09-08 17:25:33

## 操作シナリオ

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

## ツールの紹介

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

```
sar -n DEV 1
02:41:03 PM     IFACE   rxpck/s   txpck/s    rxkB/s    txkB/s
rxcmp/s   txcmp/s  rxmcst/s
02:41:04 PM      eth0 1626689.00      8.00  68308.62      1.65
0.00      0.00      0.00
02:41:04 PM        lo      0.00      0.00      0.00      0.00
0.00      0.00      0.00
02:41:04 PM     IFACE   rxpck/s   txpck/s    rxkB/s    txkB/s
rxcmp/s   txcmp/s  rxmcst/s
02:41:05 PM      eth0 1599900.00      1.00  67183.30      0.10
0.00      0.00      0.00
02:41:05 PM        lo      0.00      0.00      0.00      0.00
0.00      0.00      0.00
```

フィールドの解釈は次のとおりです。

| フィールド | 単位 | 説明 |
| --- | --- | --- |
| rxpck/s | pps | 1秒あたりの受信パケット数、すなわち受信pps |
| txpck/s | pps | 1秒あたりの送信パケット数、すなわち送信pps |
| rxkB/s | kB/s | 受信帯域幅 |

| | | |
|---|---|---|
| txkB/s | kB/s | 送信帯域幅 |

# テストシーンおよびパフォーマンス指標

## テストシーン

| テストシーン | クライアント側のコマンド実行 | SAR 監視指標 |
|---|---|---|
| UDP 64 | `netperf -t UDP_STREAM -H <server ip> -l 10000 -- -m 64 -R 1 &` | PPS |
| TCP 1500 | `netperf -t TCP_STREAM -H <server ip> -l 10000 -- -m 1500 -R 1 &` | 帯域幅 |
| TCP RR | `netperf -t TCP_RR -H <server ip> -l 10000 -- -r 32,128 -R 1 &` | PPS |

## パフォーマンス指標

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

# 操作手順

## テスト環境の準備

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

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

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

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

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

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

## パケット送信パフォーマンスのテスト

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

```
pkill netserver && pkill netperf
```

2. このうちサーバーaをクライアント側、 サーバーbとサーバーcをサーバー側とします。サーバー側で以下のコマンドを実行し、netserverを実行します。

```
netserver
```

   - 返された結果が下図のとおりであれば、他のnetserverプロセスがまだ存在することを表します。手順1 中のコマンドを実行し、該当のプロセスを停止してください。

```
[root@VM-2-8-centos ~]# netserver
Unable to start netserver with  'IN(6)ADDR_ANY' port '12865' and family AF_UNSPEC
[root@VM-2-8-centos ~]#
```

   - 返された結果が下図のとおりであれば、netserverの実行に成功したことを表します。続けて次の操作を行ってください。

```
[root@VM-2-8-centos ~]# netserver
Starting netserver with host 'IN(6)ADDR_ANY' port '12865' and family AF_UNSPEC
[root@VM-2-8-centos ~]#
```

3. テストシーン で提供されたコマンドをクライアント側で実行し、クライアント側のパケット送信パフォーマンスがそれ以上向上しなくなるまでnetperfプロセスを増減し続けます。

> 説明:
> コマンド実行を繰り返す必要があり、かつserver ipには異なるサーバーIPを使用する必要があります。1つのプロセスが最大パフォーマンスに達しない場合は、テスト支援スクリプト を実行し、プロセスを一括して開始することができます。

4. クライアント側で以下のコマンドを実行し、クライアント側のパケット送信パフォーマンスの変化を観察し、最大値をとります。

```
sar -n DEV 1
```

得られた結果に基づき、パフォーマンス指標 を参照して分析を行うことで、CVMの高スループットネットワークパフォーマンスを測定することができます。

## パケット受信パフォーマンスのテスト

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

```
pkill netserver && pkill netperf
```

2. このうちサーバーaをサーバー側、 サーバーbとサーバーcをクライアント側とします。サーバー側で以下のコマンドを実行し、netserverを実行します。

```
netserver
```

   - 返された結果が下図のとおりであれば、他のnetserverプロセスがまだ存在することを表します。手順1中のコマンドを実行し、該当のプロセスを停止してください。

```
[root@VM-2-8-centos ~]# netserver
Unable to start netserver with  'IN(6)ADDR_ANY' port '12865' and family AF_UNSPEC
[root@VM-2-8-centos ~]#
```

   - 返された結果が下図のとおりであれば、netserverの実行に成功したことを表します。続けて次の操作を行ってください。

```
[root@VM-2-8-centos ~]# netserver
Starting netserver with host 'IN(6)ADDR_ANY' port '12865' and family AF_UNSPEC
[root@VM-2-8-centos ~]#
```

3. テストシーン で提供されたコマンドをクライアント側で実行し、クライアント側のパケット送信パフォーマンスがそれ以上向上しなくなるまでnetperfプロセスを増減し続けます。

> 説明:

> コマンド実行を繰り返す必要があり、クライアント側はそれぞれnetperfを開始します。1つのプロセスが最大パフォーマンスに達しない場合は、テスト支援スクリプト を実行し、プロセスを一括して開始することができます。

4. サーバー側で以下のコマンドを実行し、サーバー側のパケット受信パフォーマンスの変化を観察し、最大値をとります。

```
sar -n DEV 1
```

得られた結果に基づき、パフォーマンス指標 を参照して分析を行うことで、CVMの高スループットネットワークパフォーマンスを測定することができます。

# 付録

## テスト支援スクリプト

このスクリプトを実行すると、複数のnetperfプロセスを迅速に開始することができます。

```
#!/bin/bash
count=$1
for ((i=1;i<=count;i++))
do
    echo "Instance:$i-------"
    # 下記のコマンドはテストシーンの表内のコマンドに置き換え可能です
    # -Hの後にサーバーのIPアドレスを入力します。
    # -lの後にテスト期間を入力します。netperfが途中で終了しないように、期間を10000に設定します。
    netperf -t UDP_STREAM -H <server ip> -l 10000 -- -m 64 -R 1 &
done
```

# DPDKを使用したテスト

最終更新日：：2023-06-30 15:28:14

## 概要

このドキュメントでは、DPDK を使用してCVM インスタンスの高スループットネットワークパフォーマンスをテストする方法について説明します。

## 操作手順

### DPDKのコンパイルとインストール

1. 2つのテストサーバーが必要です。サーバーは Linux CVM 構成のカスタマイズ の指示に従って購入できます。ここではテストサーバーにCentOS 8.2 OSを使用します。
2. 順にテストサーバーにログインし、以下のコマンドを実行してDPDKツールをダウンロードします。CVMへのログイン方法については、 標準ログイン方式を使用してLinuxインスタンスにログイン（推奨） をご参照ください。。

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

```
wget http://git.dpdk.org/dpdk/snapshot/dpdk-17.11.tar.gz
```

```
tar -xf dpdk-17.11.tar.gz
```

```
mv dpdk-17.11 dpdk
```

3. txonlyエンジンを変更し、各DPDKのパケット送信CPUのUDPトラフィック用ポートを、複数のストリームを発生させるよう変更します。
   - 以下のコマンドを実行し、 `dpdk/app/test-pmd/txonly.c` ファイルを変更します。

```
vim dpdk/app/test-pmd/txonly.c
```

i を押して編集モードに入り、以下の内容を変更します。
3.1.1 `#include "testpmd.h"を見つけます。 次の内容を次の行に追加します。

```
RTE_DEFINE_PER_LCORE(struct udp_hdr, lcore_udp_hdr);
```

```
RTE_DEFINE_PER_LCORE(uint16_t, test_port);
```

結果は次のようになります：

```
#include "testpmd.h"
RTE_DEFINE_PER_LCORE(struct udp_hdr, lcore_udp_hdr);
RTE_DEFINE_PER_LCORE(uint16_t, test_port);

#define UDP_SRC_PORT 1024
#define UDP_DST_PORT 1024
```

3.1.2 `ol_flags |= PKT_TX_MACSEC;` を見つけます。 次の内容を次の行に追加します。

```
/* dummy test udp port */
memcpy(&RTE_PER_LCORE(lcore_udp_hdr), &pkt_udp_hdr,
sizeof(pkt_udp_hdr));
```

3.1.3 `for (nb_pkt = 0; nb_pkt < nb_pkt_per_burst; nb_pkt++) {` を見つけ、これを以下の内容に置き換えます。

```
RTE_PER_LCORE(test_port)++;
RTE_PER_LCORE(lcore_udp_hdr).src_port =
rte_cpu_to_be_16(2222);
RTE_PER_LCORE(lcore_udp_hdr).dst_port =
rte_cpu_to_be_16(rte_lcore_id() * 2000 +
RTE_PER_LCORE(test_port) % 64);
```

結果は次のようになります：

```
if (txp->tx_ol_flags & TESTPMD_TX_OFFLOAD_INSERT_QINQ)
        ol_flags |= PKT_TX_QINQ_PKT;
if (txp->tx_ol_flags & TESTPMD_TX_OFFLOAD_MACSEC)
        ol_flags |= PKT_TX_MACSEC;

/* dummy test udp port */
memcpy(&RTE_PER_LCORE(lcore_udp_hdr), &pkt_udp_hdr, sizeof(pkt_udp_hdr));


for (nb_pkt = 0; nb_pkt < nb_pkt_per_burst; nb_pkt++) {
        RTE_PER_LCORE(test_port)++;
        RTE_PER_LCORE(lcore_udp_hdr).src_port = rte_cpu_to_be_16(2222);
        RTE_PER_LCORE(lcore_udp_hdr).dst_port = rte_cpu_to_be_16(rte_lcore_id() * 2000 + RTE_PER_LCORE(test_port) % 64);

        pkt = rte_mbuf_raw_alloc(mbp);
        if (pkt == NULL) {
        nomore_mbuf:
                if (nb_pkt == 0)
                        return;
                break;
        }
```

3.1.4 `copy_buf_to_pkt(&pkt_udp_hdr, sizeof(pkt_udp_hdr), pkt,` を見つけ、これを以下の内容に置き換えます。

```
copy_buf_to_pkt(&RTE_PER_LCORE(lcore_udp_hdr),
sizeof(RTE_PER_LCORE(lcore_udp_hdr)), pkt,
```

結果は次のようになります:

```
copy_buf_to_pkt(&eth_hdr, sizeof(eth_hdr), pkt, 0);
copy_buf_to_pkt(&pkt_ip_hdr, sizeof(pkt_ip_hdr), pkt,
                sizeof(struct ether_hdr));
copy_buf_to_pkt(&RTE_PER_LCORE(lcore_udp_hdr), sizeof(RTE_PER_LCORE(lcore_udp_hdr)), pkt,
                sizeof(struct ether_hdr) +
                sizeof(struct ipv4_hdr));
```

Esc を押し、:wq を入力して変更を保存し、終了します。

- 以下のコマンドを実行し、 `dpdk/config/common_base` ファイルを変更します。

```
vim dpdk/config/common_base
```

i を押して編集モードに入り、 `CONFIG_RTE_MAX_MEMSEG=256` を見つけて、これを1024に変更します。変更が完了すると、以下のようになります。

```
CONFIG_RTE_LIBRTE_EAL=y
CONFIG_RTE_MAX_LCORE=128
CONFIG_RTE_MAX_NUMA_NODES=8
CONFIG_RTE_MAX_MEMSEG=1024
CONFIG_RTE_MAX_MEMZONE=2560
CONFIG_RTE_MAX_TAILQ=32
```

i を押して編集モードに入り、 CONFIG_RTE_MAX_LCORE=128`を見つけて、システムのCPU コアの数が128より大きい場合は、256に変更できます。変更が完了すると、以下のようになります。

```
CONFIG_RTE_LIBRTE_EAL=y
CONFIG_RTE_MAX_LCORE=256
CONFIG_RTE_MAX_NUMA_NODES=8
CONFIG_RTE_MAX_MEMSEG=256
CONFIG_RTE_MAX_MEMZONE=2560
CONFIG_RTE_MAX_TAILQ=32
```

Esc を押し、:wq を入力して変更を保存し、終了します。

> **説明:**
> 受信側および送信側テストサーバーの両方で上記の構成ファイルを変更する必要があります。以下のコマンドを使用すると、変更されたファイルを相手側に送信し、変更の重複を避けることができま

す。

```
scp -P 22 /root/dpdk/app/test-pmd/txonly.c root@<IPアドレス
>:/root/dpdk/app/test-pmd/
scp -P 22 /root/dpdk/config/common_base root@<IPアドレス
>:/root/dpdk/config
```

4. 以下のコマンドを実行し、 `dpdk/app/test-pmd/txonly.c` のIPアドレスを、テストサーバーのIPに変更します。

```
vim dpdk/app/test-pmd/txonly.c
```

i を押して編集モードに入り、以下の内容を見つけます。

```
#define IP_SRC_ADDR (198U << 24) | (18 << 16) | (0 << 8) | 1;
#define IP_DST_ADDR (198U << 24) | (18 << 16) | (0 << 8) | 2;
```

数字の198、18、0、1をサーバーのIPに置き換えます。SRC_ADDRは送信側の IP、DST_ADDRは受信側のIPとします。

5. サーバーのOSに応じて以下のコマンドを実行し、numaライブラリをインストールします。

CentOS

```
yum install numactl-devel
```

Ubuntu

```
apt-get install libnuma-dev
```

6. `dpdk/` ディレクトリで以下のコマンドを実行し、KNIを無効化します。

```
sed -i  "s/\(^CONFIG_.*KNI.*\)=y/\1=n/g" ./config/*
```

7. OS が新しいカーネルバージョン (5.3 など) を使用している場合は、次のコマンドを実行して差異をシールドしてください。

```
sed -i "s/\(^WERROR_FLAGS += -Wundef -Wwrite-strings$\)/\1 -Wno-address-of-packed-member/g" ./mk/toolchain/gcc/rte.vars.mk
```

```
sed -i "s/fall back/falls through -/g" ./lib/librte_eal/linuxapp/igb_uio/igb_uio.c
```

8. 以下のコマンドを実行し、DPDKをコンパイルします。

```
make defconfig
```

```
make -j
```

## ラージページメモリの構成

以下のコマンドを実行し、ラージページメモリを構成します。

```
echo 4096 > /sys/kernel/mm/hugepages/hugepages-2048kB/nr_hugepages
```

エラー情報が表示された場合は、ラージページメモリが不足していることを表します。次の例のように、コマンド構成の調整が可能です。

```
echo 2048 > /sys/kernel/mm/hugepages/hugepages-2048kB/nr_hugepages
```

## カーネルモジュールのロードおよびインターフェースのバインド

> 説明:
> この手順ではPythonを使用する必要があります。 Python公式サイト にアクセスして、適切なバージョンをダウンロードしてインストールします。ここではPython 3.6.8を例とします。

1. VNCを使用してLinuxインスタンスにログイン します。ENIドライバーが igb_uio ユーザー モードドライバーにバインドされた後は、SSH キーまたは IP アドレスではなく、VNC またはコンソール経由でのみ ENI にア

クセスできます。

2. 次のコマンドを順に実行し、UIOモジュールをロードし、virtioインターフェイスをバインドします。

```
ifconfig eth0 0
```

```
ifconfig eth0 down
```

```
modprobe uio
```

```
insmod /root/dpdk/build/kmod/igb_uio.ko
```

```
cd /root/dpdk/usertools/
```

```
python3 dpdk-devbind.py --bind=igb_uio 00:05.0
```

> 説明:
> コマンドの中の00.05.0はサンプルアドレスです。以下のコマンドを実行し、ENIの実際のアドレスを取得してください。
>
> ```
> python3 dpdk-devbind.py -s
> ```

テストが完了したら、次のコマンドを実行してENIを復元します。

```
cd /root/dpdk/usertools/
```

```
python3 dpdk-devbind.py --bind=virtio-pci 00:05.0
```

```
ifconfig eth0 up
```

## 帯域幅とスループットのテスト

説明:
- テストコマンドはtxpktsパラメータを使用してパケットのサイズを制御します。テスト帯域幅は1430B、テストppsは64Bをそれぞれ使用します。
- この手順で提供されるコマンドパラメータは CentOS 8.2に適用されます。その他のシステムイメージバージョンを使用する場合は、実際のシーンに応じてパラメータを調整した後、再度テストを行う必要があります。例えば、CentOS 7.4のカーネルバージョンが3.10の場合、CentOS 8.2 のカーネルバージョン4.18との間に性能差が存在するため、帯域幅テストコマンドの中の `nb-cores` を2に変更することができます。コマンドのパラメータに関するその他の情報については、 testpmd-command-line-options をご参照ください。

1. 次のコマンドを実行して、送信側で testpmdをtxonlyモードで起動し、受信側でrxonlyモードを有効にします。
   - 送信側:

```
/root/dpdk/build/app/testpmd  -l 8-191 -w 0000:00:05.0 -- --
burst=128 --nb-cores=32 --txd=512 --rxd=512 --txq=16 --rxq=16  --
forward-mode=txonly --txpkts=1430 --stats-period=1
```

説明:
このうち `-l 8-191 -w 0000:00:05.0` これら 2 つのパラメータはテスト環境の実際の値に置き換える必要があります。

   - 受信側:

```
/root/dpdk/build/app/testpmd -l 8-191 -w 0000:00:05.0 -- --
burst=128 --nb-cores=32 --txd=512 --rxd=512 --txq=16 --rxq=16 --
forward-mode=rxonly --stats-period=1
```

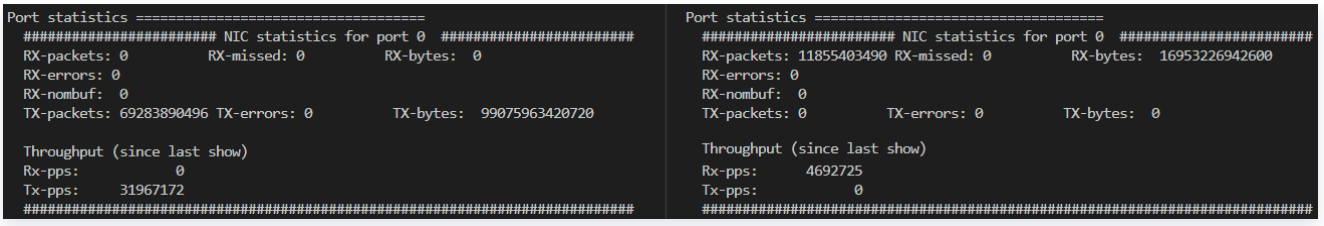
2. 次のコマンドを実行し、ppsをテストします(UDP 64B パケット)。
   - 送信側:

```
/root/dpdk/build/app/testpmd -l 8-191 -w 0000:00:05.0 -- --
burst=128 --nb-cores=32 --txd=512 --rxd=512 --txq=16 --rxq=16  --
forward-mode=txonly --txpkts=64 --stats-period=1
```

   - 受信側:

```
/root/dpdk/build/app/testpmd -l 8-191 -w 0000:00:05.0 -- --
burst=128 --nb-cores=32 --txd=512 --rxd=512 --txq=16 --rxq=16  --
forward-mode=rxonly --stats-period=1
```

テスト結果は以下のとおりです：




## ネットワーク帯域幅の計算

受信側のPPSとテストパケットの長さに基づいて、現在のネットワークの受信帯域幅を計算することができます。公式は次のとおりです。

PPS × packet length × 8bit/B × $10^{-9}$ = 帯域幅
テストで得られたデータと合わせて、得られた現在の帯域幅は次のとおりです。

4692725pps × 1430B × 8bit/B × $10^{-9}$ ≈ 53Gbps

説明：

- パケット長は1430Bで、14Bイーサネットヘッダー、8B CRC、20B IPヘッダーが含まれます。
- テスト結果のRx-ppsは瞬間統計値であり、複数回のテストによって平均値を求めることで、より正確な結果を得ることができます。

# ネットワーク性能のテスト

最終更新日：：2021-10-27 17:20:01

## 概要

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

## ネットワークパフォーマンスのテストメトリクス

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

## ツールの基本情報

| メトリック | 説明 |
| --- | --- |
| TCP-RR | Netperf |
| UDP-STREAM | Netperf |
| TCP-STREAM | Netperf |
| 帯域幅 | iperf |
| ppsの確認 | sar |
| ENIキューの確認 | ethtool |

## 操作手順

### テスト環境の構築

### テストサーバーの準備

- イメージ：CentOS 7.4 64ビット
- 仕様：S3.2XLARGE16
- 数量：1

テストサーバーのIPアドレスが10.0.0.1と想定します。

### コンパニオントレーニングサーバーの準備

- イメージ：CentOS 7.4 64ビット
- 仕様：S3.2XLARGE16
- 数量：8

コンパニオントレーニングサーバーのIPアドレスが10.0.0.2～10.0.0.9と想定します。

### テストツールのデプロイ

> ⚠ ご注意：
> テスト環境を構築し、その環境でテストを実行するときは、rootユーザーの権限があることを確認してください。

1. 次のコマンドを順番に実行して、コンパイル環境およびシステム状態監視ツールをインストールします。

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

2. 次のコマンドを実行して、Netperf圧縮パッケージをダウンロードします。
Githubからも最新バージョン： Netperf をダウンロードできます。

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

3. 次のコマンドを実行して、Netperf圧縮パッケージを解凍します。

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

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

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

5. 次のコマンドを実行して、インストールが成功したかどうかを確認します。

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

「ヘルプ」が表示された場合、インストールは成功しています。

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

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

7. 次のコマンドを実行して、インストールが成功したかどうかを確認します。

```
iperf -h
```

「ヘルプ」が表示された場合、インストールは成功しています。

## 帯域幅テスト

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

### テストサーバー

次のコマンドを実行します。

```
iperf -s
```

### コンパニオントレーニングサーバー

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

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

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

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

## UDP-STREAMテスト

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

### テストサーバー

次のコマンドを実行して、ネットワークのpps値を確認します。

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

### コンパニオントレーニングサーバー

次のコマンドを実行します。

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

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

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

## TCP-RRテスト

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

### テストサーバー

次のコマンドを実行して、ネットワークのpps値を確認します。

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

### コンパニオントレーニングサーバー

次のコマンドを実行します。

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

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

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

## テストデータ分析

### sarツールのパフォーマンス分析

#### 分析データのサンプル

```
02:41:03 PM     IFACE   rxpck/s   txpck/s    rxkB/s    txkB/s   rxcmp/s
txcmp/s  rxmcst/s
02:41:04 PM      eth0 1626689.00      8.00  68308.62      1.65      0.00
0.00      0.00
02:41:04 PM        lo      0.00      0.00      0.00      0.00      0.00
0.00      0.00

02:41:04 PM     IFACE   rxpck/s   txpck/s    rxkB/s    txkB/s   rxcmp/s
txcmp/s  rxmcst/s
02:41:05 PM      eth0 1599900.00      1.00  67183.30      0.10      0.00
0.00      0.00
02:41:05 PM        lo      0.00      0.00      0.00      0.00      0.00
0.00      0.00

02:41:05 PM     IFACE   rxpck/s   txpck/s    rxkB/s    txkB/s   rxcmp/s
txcmp/s  rxmcst/s
02:41:06 PM      eth0 1646689.00      1.00  69148.10      0.40      0.00
0.00      0.00
02:41:06 PM        lo      0.00      0.00      0.00      0.00      0.00
0.00      0.00
```

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

### フィールドの説明

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

## iperfツールのパフォーマンス分析

### 分析データのサンプル

```
    [ ID] Interval           Transfer     Bandwidth
    [  5]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec
sender
    [  5]   0.00-300.03 sec  6.88 GBytes   197 Mbits/sec
receiver
    [  7]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec
sender
    [  7]   0.00-300.03 sec  6.45 GBytes   185 Mbits/sec
receiver
    [  9]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec
sender
    [  9]   0.00-300.03 sec  6.40 GBytes   183 Mbits/sec
receiver
    [ 11]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec
sender
    [ 11]   0.00-300.03 sec  6.19 GBytes   177 Mbits/sec
receiver
    [ 13]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec
sender
```

```
    [ 13]   0.00-300.03 sec  6.82 GBytes   195 Mbits/sec
receiver
    [ 15]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec
sender
    [ 15]   0.00-300.03 sec  6.70 GBytes   192 Mbits/sec
receiver
    [ 17]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec
sender
    [ 17]   0.00-300.03 sec  7.04 GBytes   202 Mbits/sec
receiver
    [ 19]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec
sender
    [ 19]   0.00-300.03 sec  7.02 GBytes   201 Mbits/sec
receiver
    [SUM]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec
sender
    [SUM]   0.00-300.03 sec  53.5 GBytes  1.53 Gbits/sec
receiver
```

### フィールドの説明

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

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

## 関連する操作

### 複数のnetperfインスタンスの起動スクリプト

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

```
#!/bin/bash
```

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

# その他の実践チュートリアル
# CVMからプライベートネットワーク経由で のCOSへのアクセス

最終更新日：：2023-06-30 15:28:14

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

## アクセス方法

Tencent Cloud内でCOSへのアクセス用のサービスを展開している場合、リージョンごとのアクセス方法には次のような違いがあります。

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

## プライベートネットワークアクセスの判定方法

この手順によって、CVMがプライベートネットワーク経由でCOSにアクセスするかどうかをテストすることができます。
CVM上で `nslookup` コマンドを使用してCOSドメイン名を解決します。プライベートネットワークIPが返された場合は、CVM がプライベートネットワーク経由でCOS にアクセスすることを示します。そうでない場合はパブリックネットワーク経由でのアクセスです。

1. バケットの概要 の説明に従ってバケットのアクセスドメインを取得して記録します。
2. インスタンスにログインし、nslookupコマンドを実行します。 `examplebucket-1250000000.cos.ap-guangzhou.myqcloud.com` が宛先バケットのアドレスであると仮定して、次のコマンドを実行します。

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

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

> 説明：

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

```
nslookup examplebucket-1250000000.cos.ap-guangzhou.myqcloud.com
Server:   10.138.224.65
Address:  10.138.224.65  #53
Name:     examplebucket-1250000000.cos.ap-guangzhou.myqcloud.com
Address:  10.148.214.13
Name:     examplebucket-1250000000.cos.ap-guangzhou.myqcloud.com
Address:  10.148.214.14
```

## 接続性のテスト

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

## 関連する操作

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

# Windowsインスタンスのディスク領域管理

最終更新日：：2020-09-10 14:59:25

## 操作シナリオ

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

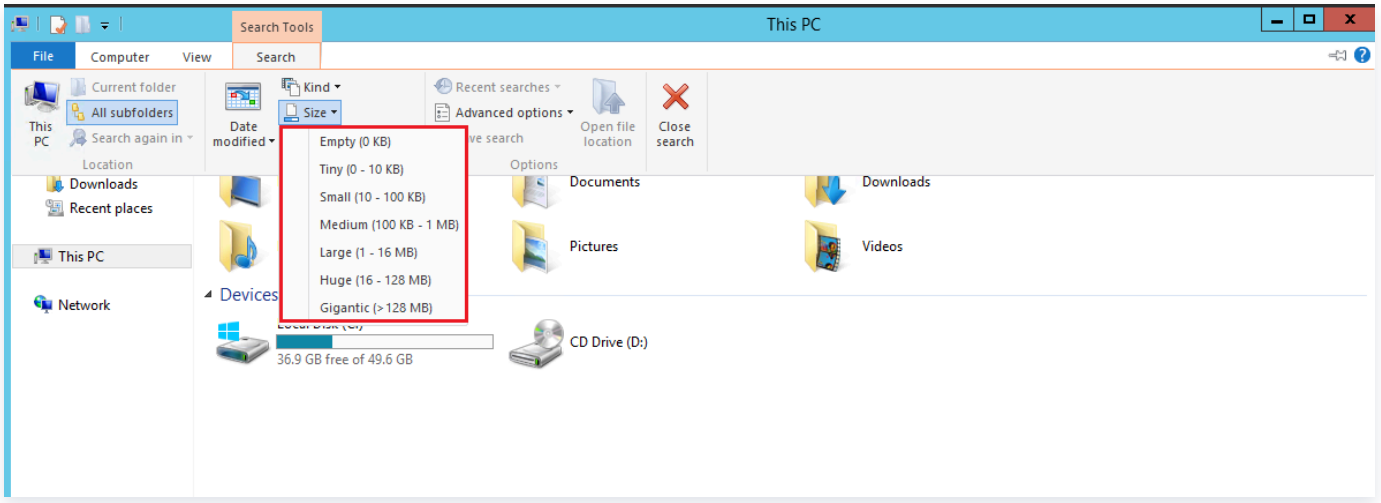
## 操作手順

### ディスクの空き容量を増やす

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

#### 大容量ファイルの削除

1. RDPファイルを使用してWindowsインスタンスにログイン（推奨） します。また、実際の操作方法により、リモートデスクトップ接続を使用してWindowsインスタンスにログイン することもできます。
2. 下部ツールバーの  を選択して、「このコンピュータ」ウィンドウを開きます。
3. 「このコンピュータ」で、クリーンアップするディスクを選択し、Crtl+Fを押して検索ツールを開きます。
4. 検索 > サイズを選択し、システムで設定されたサイズに基づいてメニューから必要に応じてファイルをフィルタリングします。以下の通りです。

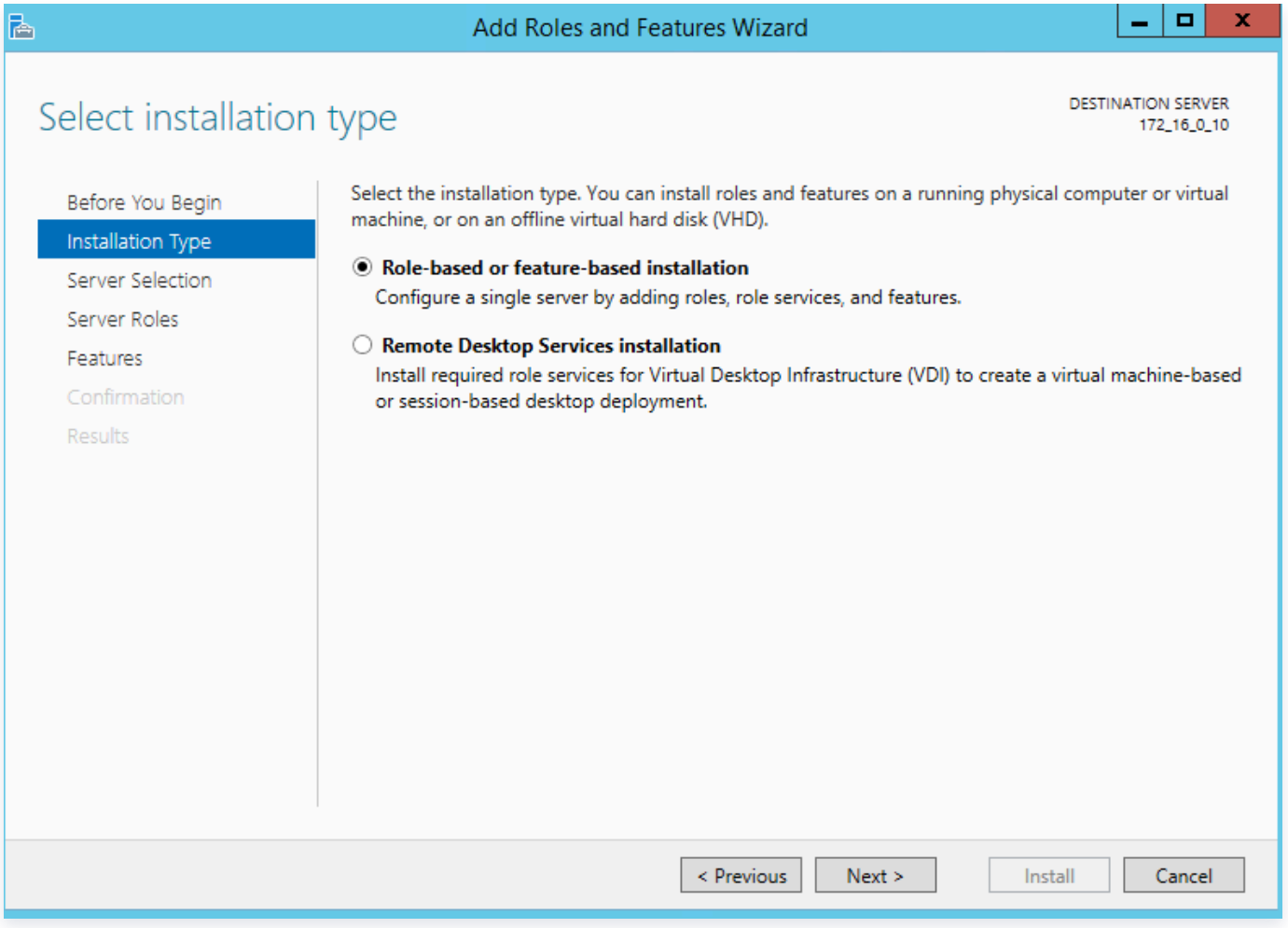



> **説明：**
> 「このコンピュータ」の右上隅にある検索ボックスで、ファイルのサイズをカスタマイズして検索することもできます。例：

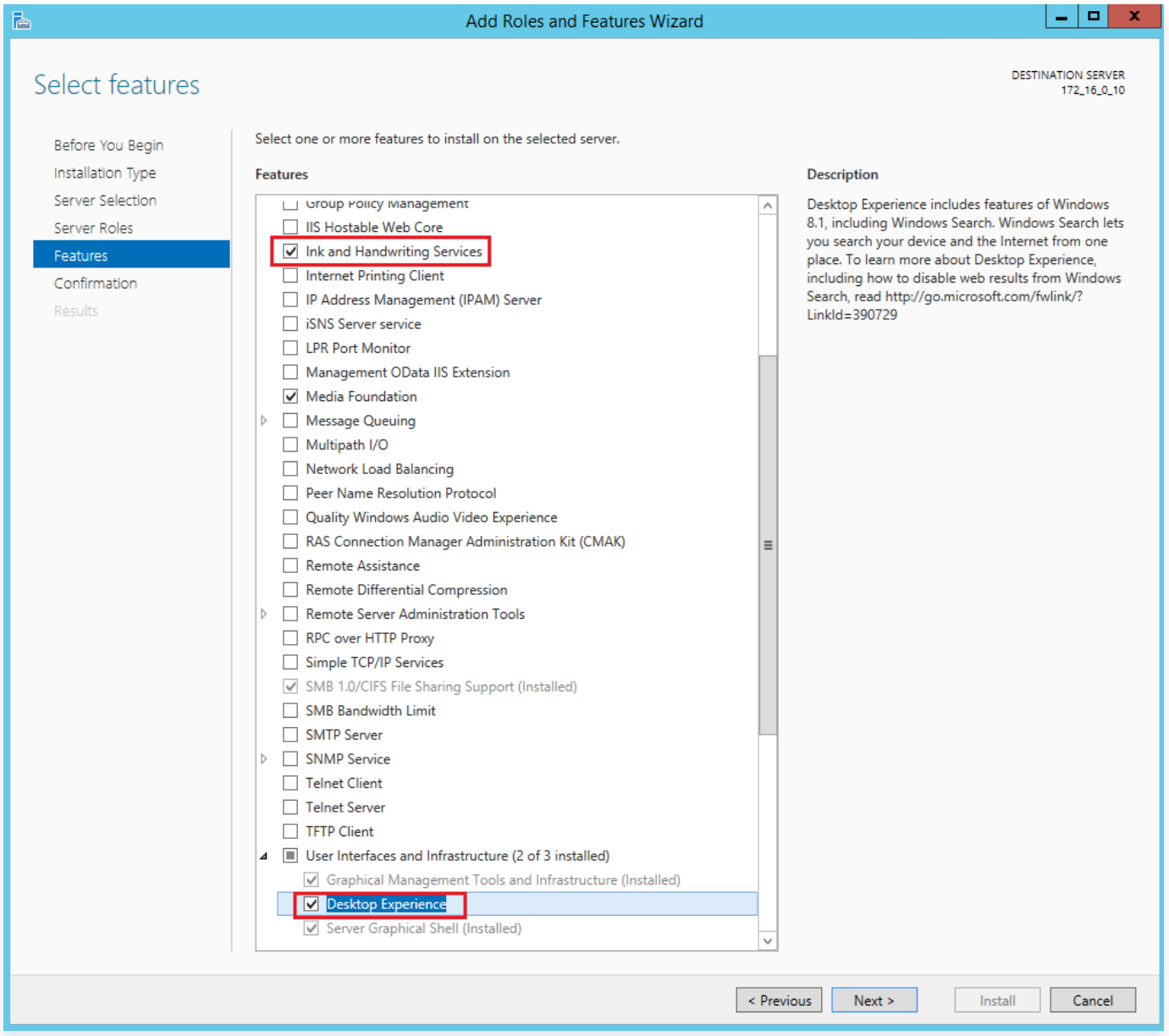
- 「サイズ：>500M」と入力すると、ディスクの500Mを超えたファイルが検索されます。
- 「サイズ：>100M<500M」と入力すると、ディスクの100Mを超えて且つ500M未満のファイルが検索されます。

## 不要ファイルの削除

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



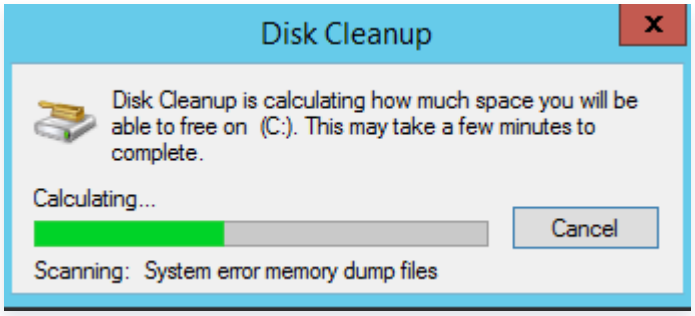

5. 「機能の選択」画面で「インクと手書きサービス」と「デスクトップエクスペリエンス」をチェックし、表示されたプロンプトボックスで【OK】をクリックします。以下の通りです。




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

7. を選択し、右上隅の をクリックします。検索ボックスにディスク管理を入力して検索します。

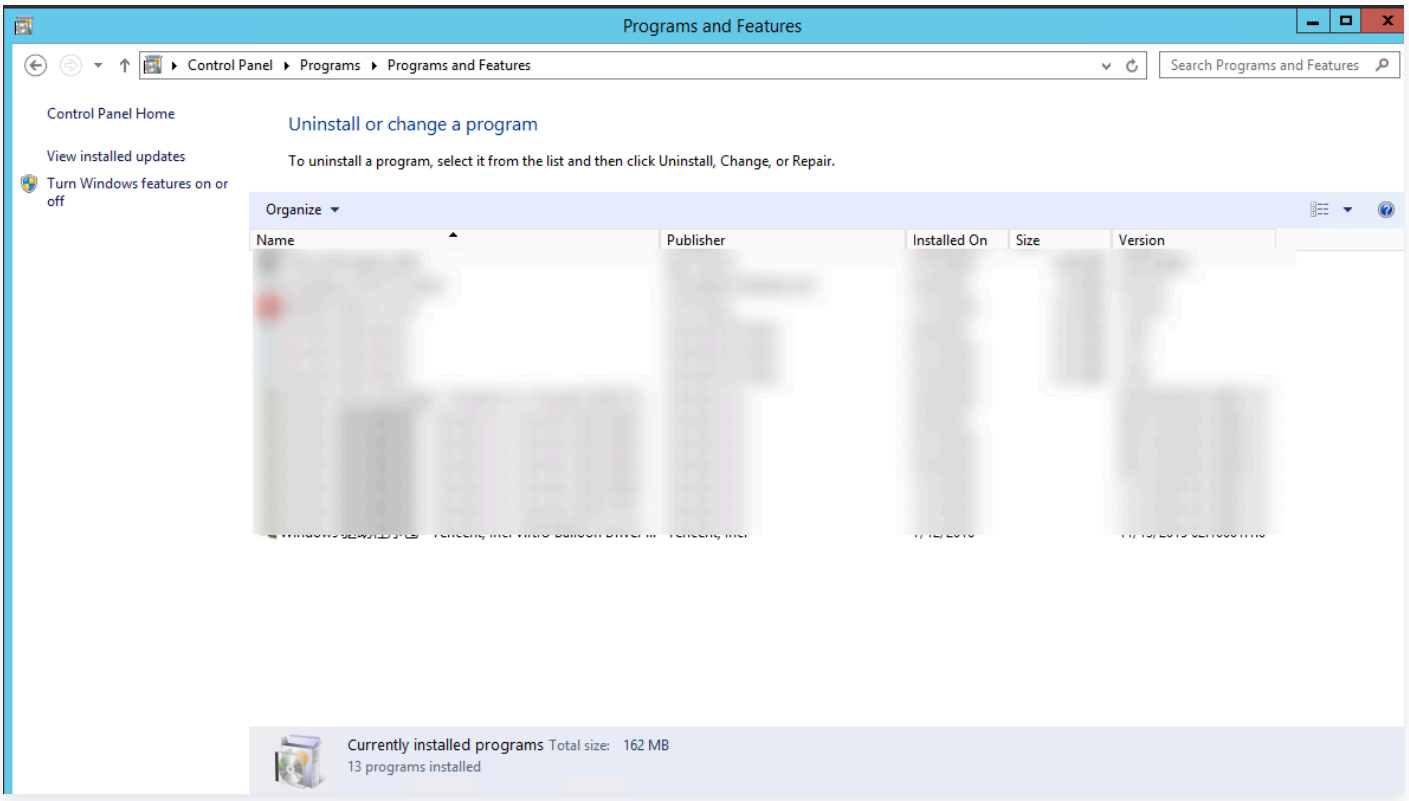
8. 表示された「ディスククリーンアップ」ウィンドウで、対応するディスクを選択してクリーンアップを開始します。以下の通りです。



# ディスクの日常的な保守

## 定期的にプログラムを削除する

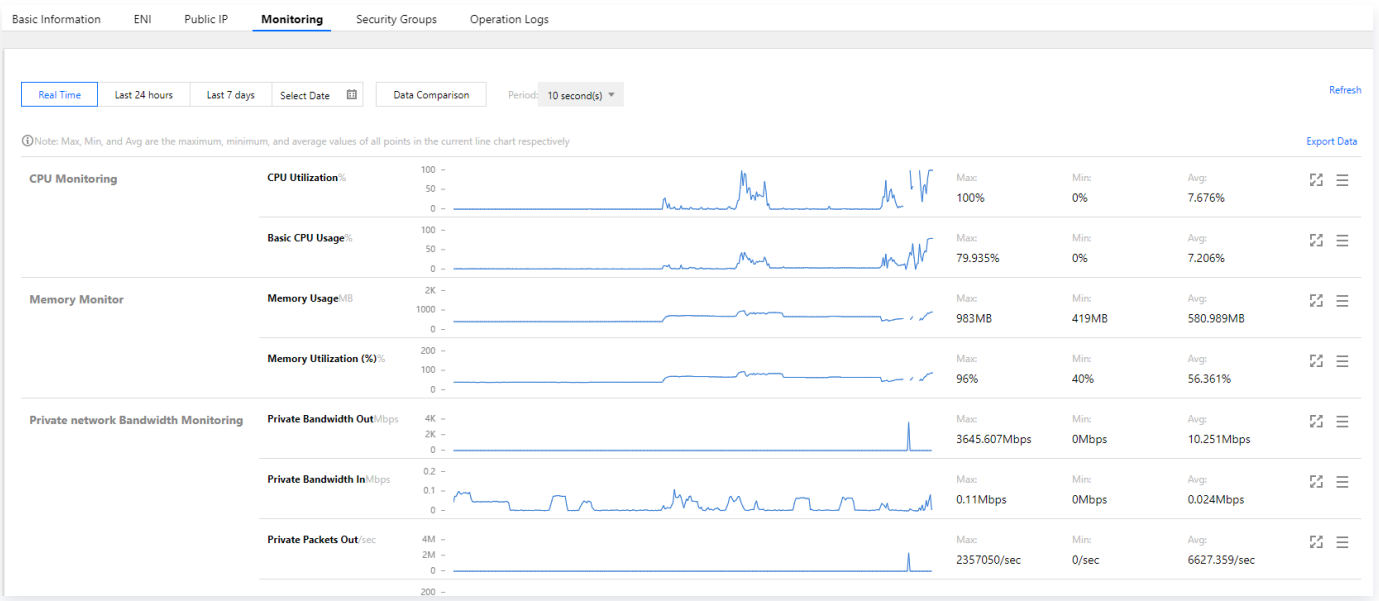
「コントロールパネル」の「プログラムのアンインストールまたは変更」を選択して、使用しなくなったプログラムを定期的にクリーンアップできます。以下の通りです。




## コンソールでディスク使用状況を表示する

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

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



# CVMでのWindowsシステムADドメインの構築

最終更新日：：2025-09-05 16:59:36

## 概要

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

## 前提条件

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

## インスタンスネットワーク環境

- グループネットワーク情報：ネットワークタイプはVirtual Private Cloud (VPC)を採用し、スイッチハブのプライベートネットワークセグメントは10.0.0.0/16です。
- ドメイン名情報：例示のインスタンスのドメイン名は `example.com` です。DCのCVMインスタンスのIPアドレスは10.0.5.102で、クライアントのCVMインスタンスのIPアドレスは10.0.5.97です。

> ⚠ ご注意：
> ADドメインの構築後、CVMインスタンスが常に同じIPアドレスを使用していることを確認してください。IPアドレスが変更されるとアクセスに異常が発生する可能性があります。

## 関連概念

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

- DC：Domain Controllers。ドメインコントローラです。
- DN：Distinguished Name。識別名です。

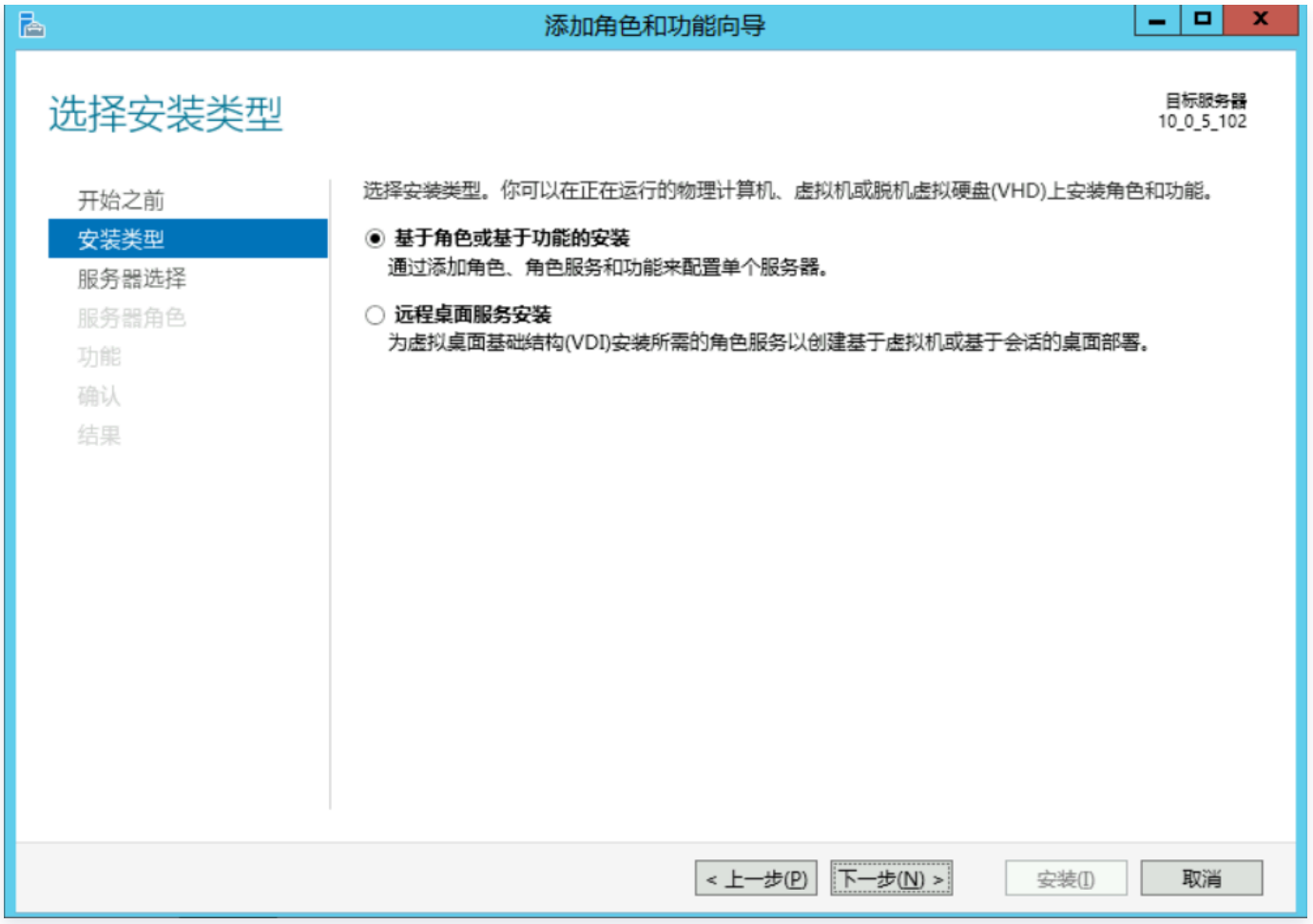
- OU：Organizational Unit。組織単位です。
- CN：Canonical Name。正式名称です。
- SID：Security Identifier。セキュリティ識別子です。

## 操作手順

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

### ADドメインコントローラのデプロイ

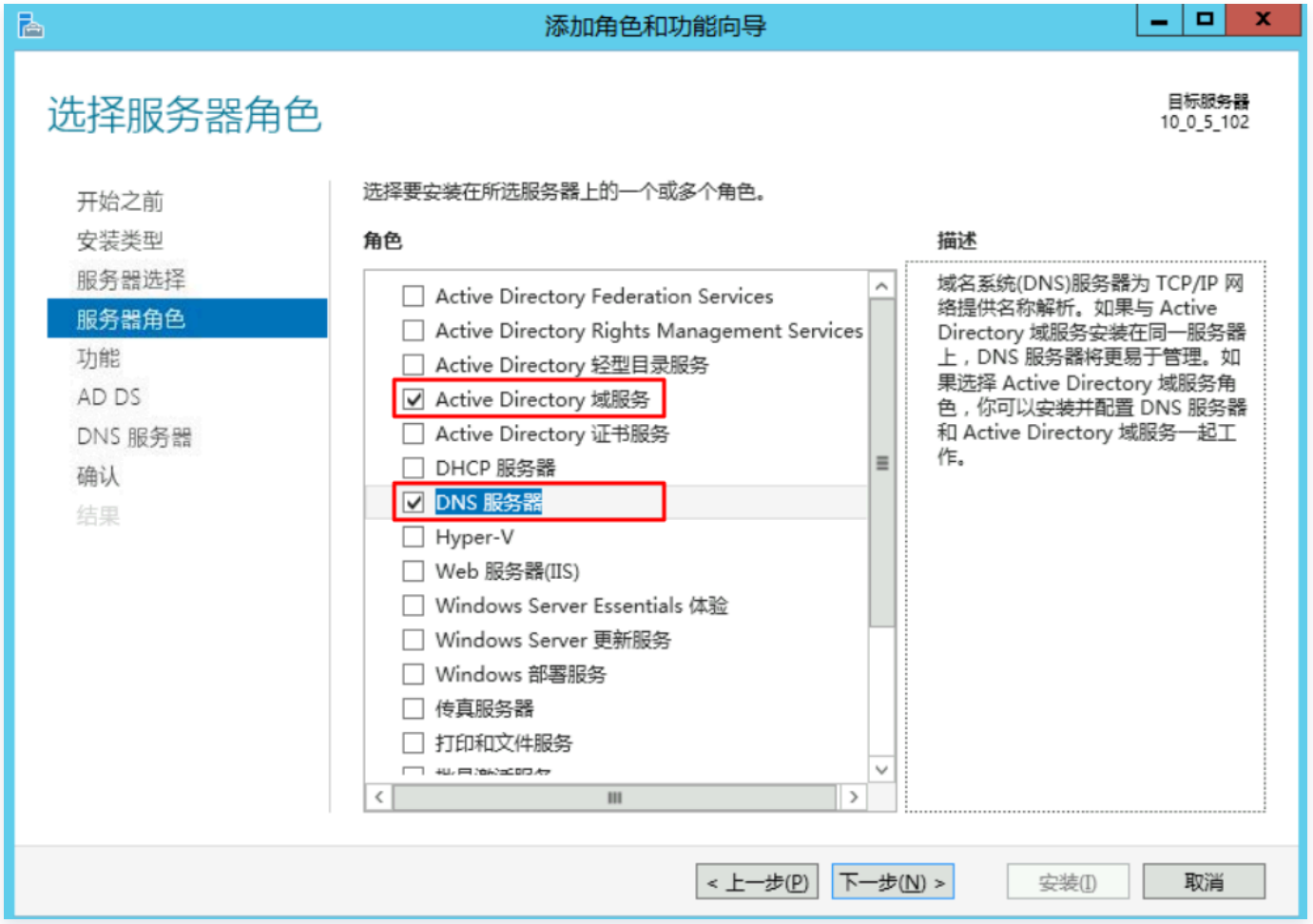
1. DCにするインスタンスにログインします。詳細については、標準方式を使用してWindowsインスタンスにログイン をご参照ください。
2. オペレーティングシステムのインターフェースで、  をクリックして、サーバーマネージャーを開きます。
3. ロールと機能の追加をクリックすると、「ロールと機能の追加ウィザード」ウィンドウがポップアップします。
4. 「インストールタイプの選択」インターフェースで、ロールまたは機能に基づくインストールを選択して、[次のステップ]を連続して2回クリックします。下図のとおりです。




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

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

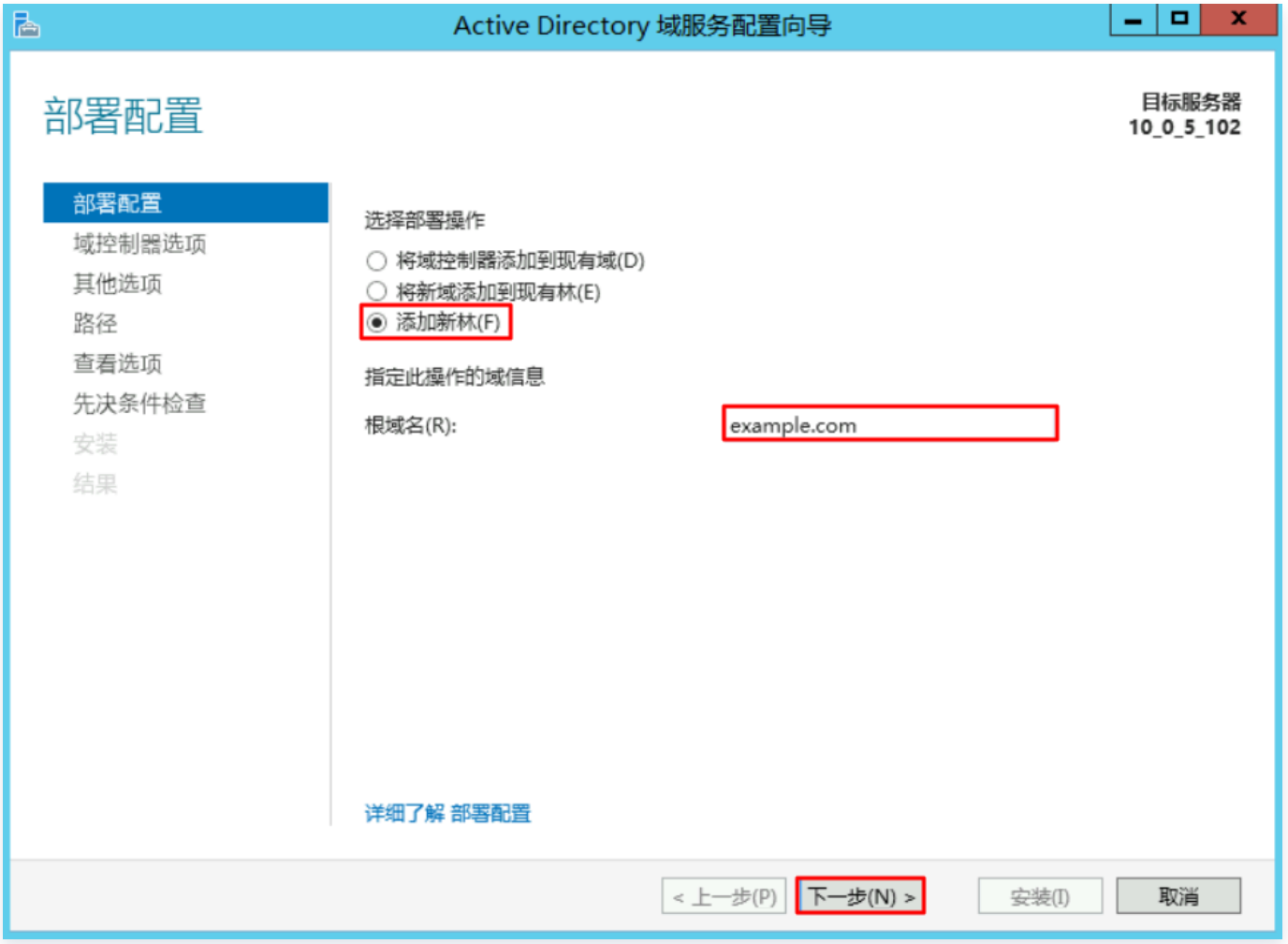
います。




6. デフォルトの設定を維持したまま、次へを4回続けてクリックします。
7. 情報の確認ページで、インストールをクリックします。
   インストールの完了後、「ロールおよび機能の追加」ダイアログボックスを閉じます。
8. オペレーティングシステムのインターフェースで、  をクリックして、サーバーマネージャーを開きます。
9. サーバーマネージャーのウィンドウで、  をクリックして、このサーバーをドメインコントローラに変更するを選択します。下図のとおりです。


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

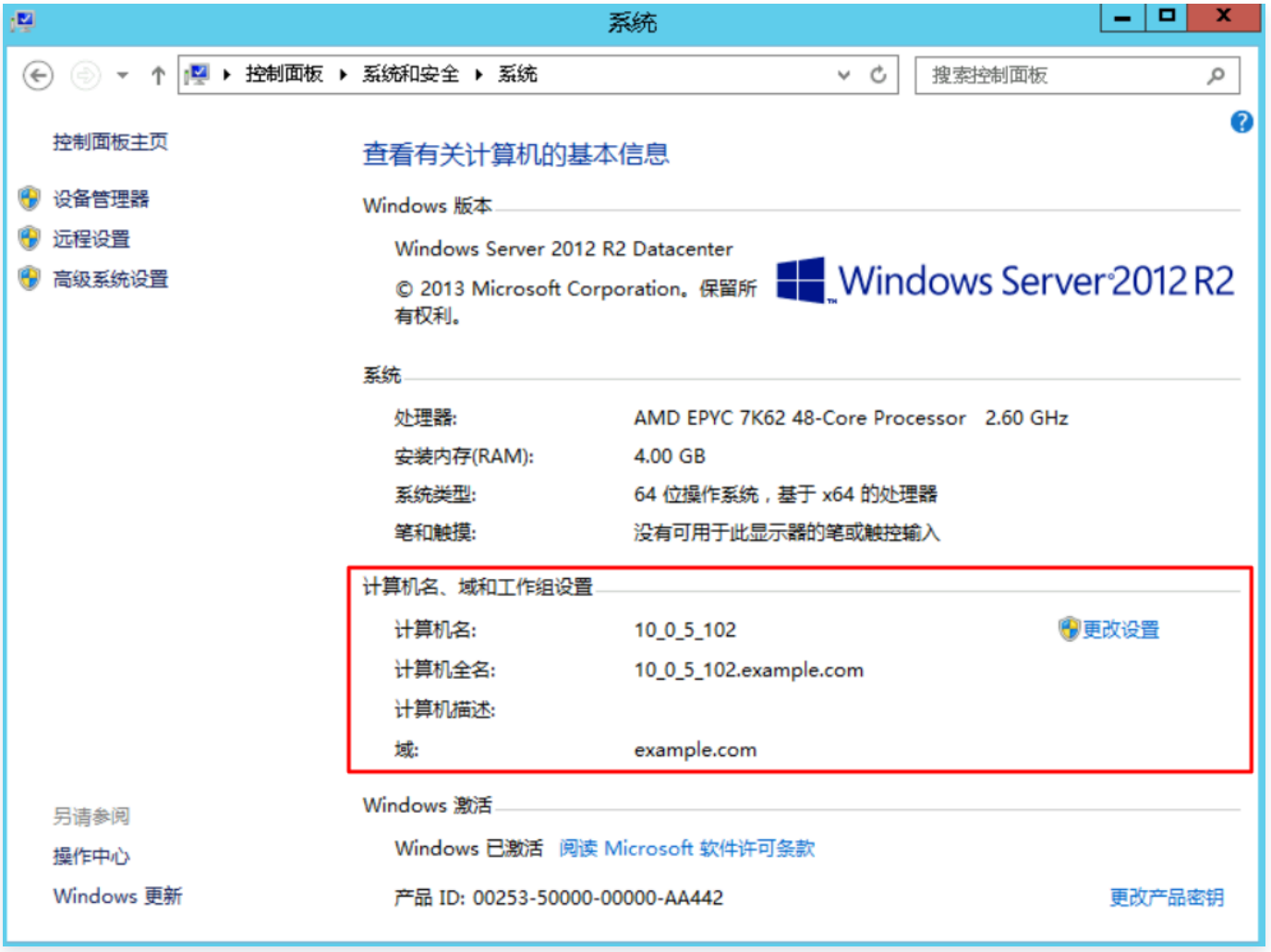
す。下図のとおりです。




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


12. デフォルトの設定を維持したまま、次へを4回続けてクリックします。
13. 「前提条件の検査中」で、インストールをクリックしてADドメインサーバーのインストールを開始します。インストールが完了すると自動的にインスタンスが再起動し、インスタンスに再接続すると、コントロールパ

ネル > システムとセキュリティ > システムにインストール結果が表示されます。下図のとおりです。

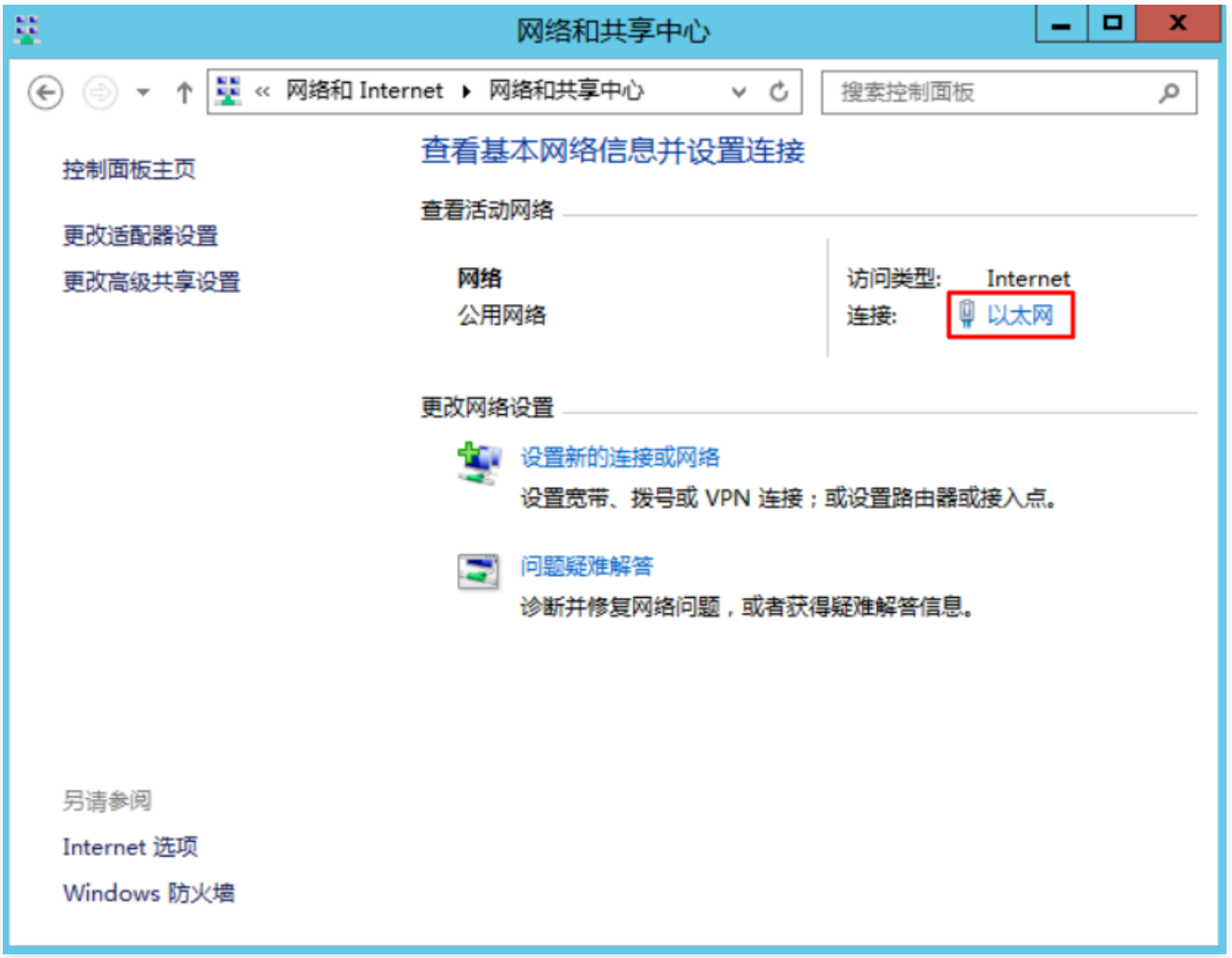



## クライアントSIDの変更

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

## クライアントのADドメインへの追加

1. クライアントにするインスタンスにログインします。詳細については、標準方式を使用してWindowsインスタンスにログイン をご参照ください。
2. DNSサーバーアドレスを変更します。
   2.1 コントロールパネル > ネットワークとインターネット > ネットワークと共有センターの順に開いて、「ネットワークと共有センター」画面でイーサネットをクリックします。下図のとおりです。

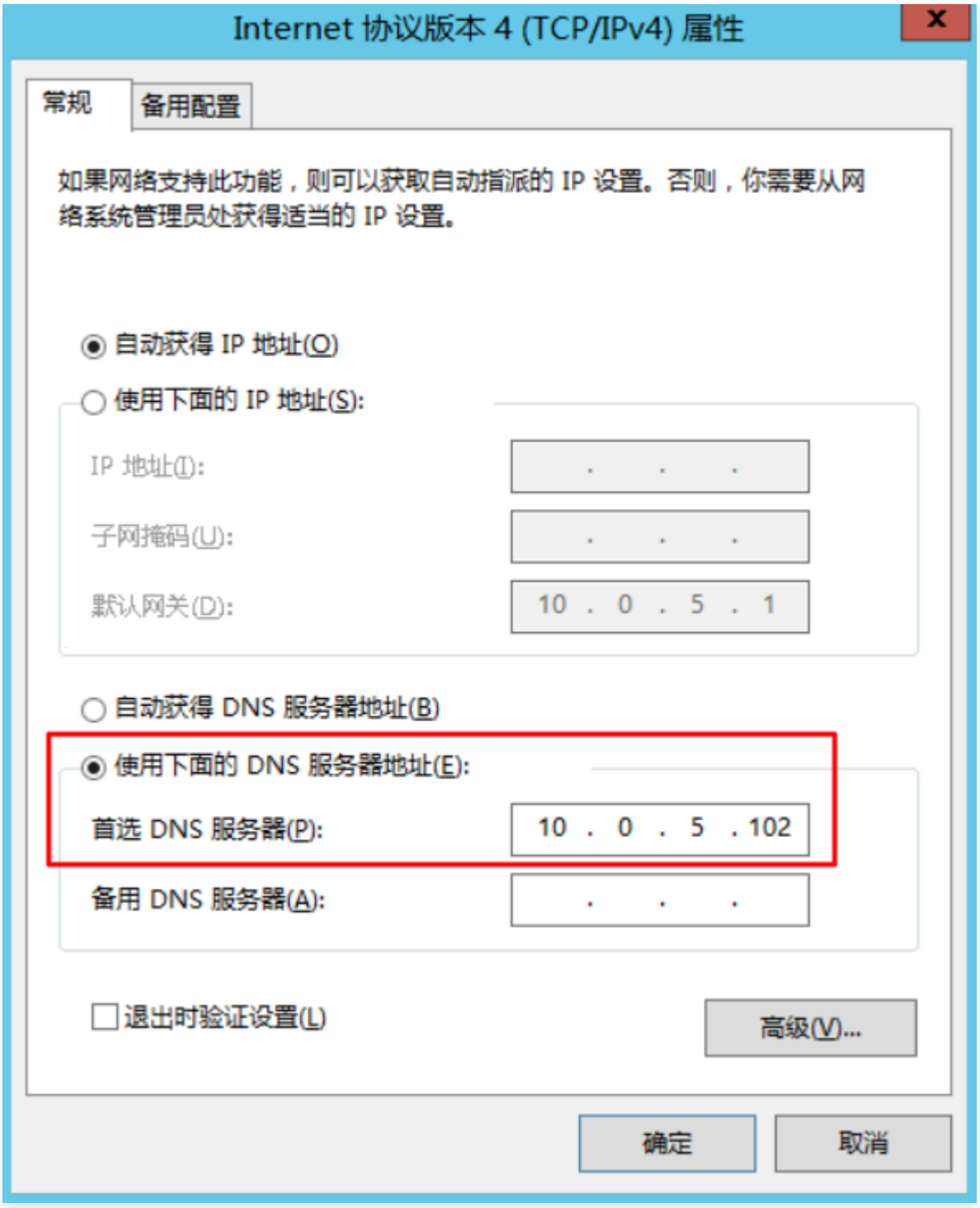



2.2 「イーサネットのステータス」画面で、属性をクリックします。

2.3 「イーサネットの属性」画面で「Internetプロトコルバージョン4（TCP/IPv4）」を選択して、属性をクリックします。

2.4 「Internetプロトコルバージョン4（TCP/IPv4）の属性」画面で、「以下のDNSサーバーアドレスを使用する」を選択して、最初に選択したDNSサーバーアドレスの設定をDCインスタンスのIPアドレスにします

（ここでは `10.0.5.102` ）。下図のとおりです。




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

2.5 OKをクリックして、変更を保存します。

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

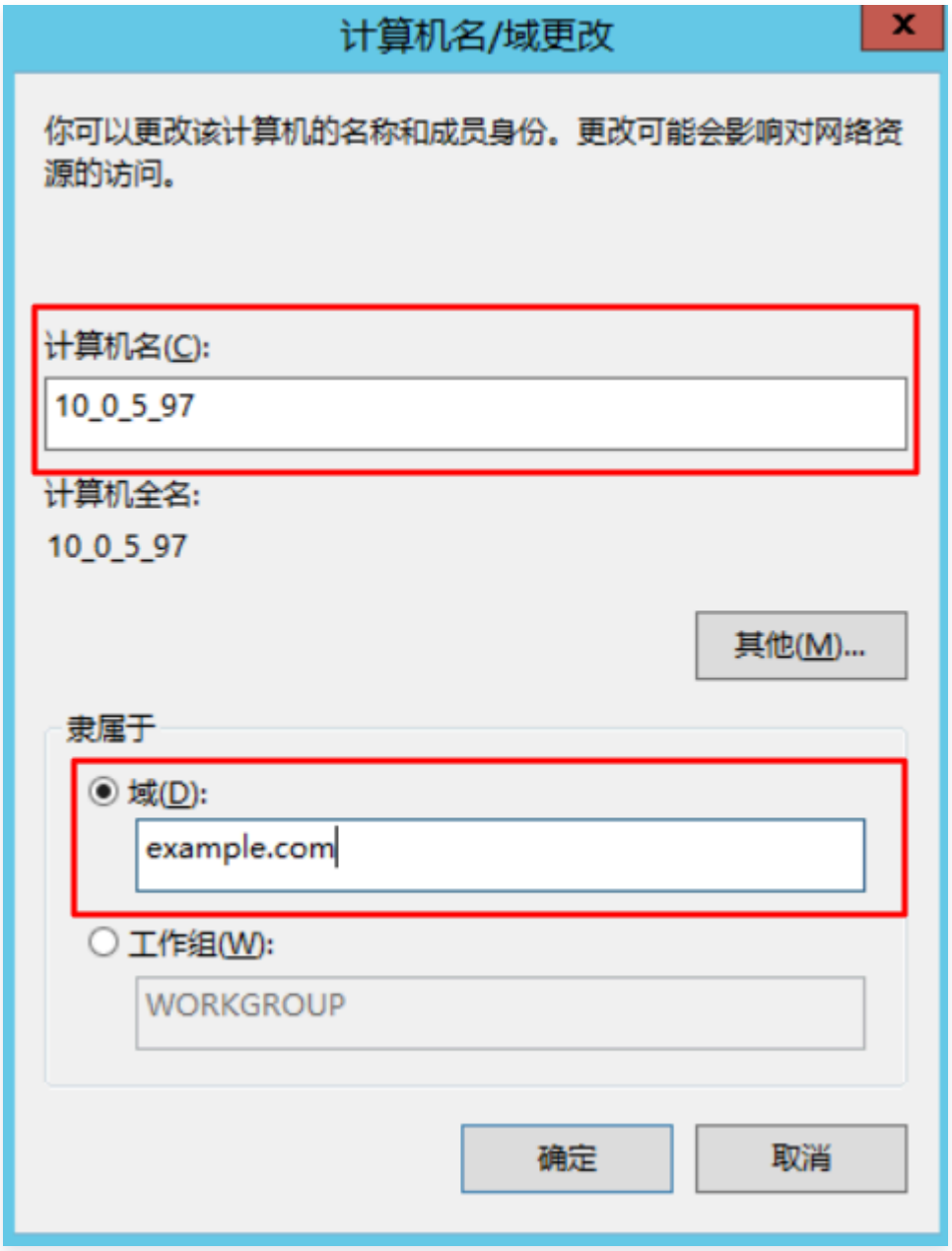
```
ping example.com
```

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


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

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


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




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

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


9. OKをクリックして、インスタンスを再起動して設定を有効にします。

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

# Linuxインスタンスのデータ復元

最終更新日：：2022-05-06 16:57:28

## 概要

このドキュメントでは、CentOS 8.0を搭載したTencent Cloud CVMを例として取り上げ、オープンソースツール Extundelete を使用して誤って削除されたデータをすばやくリカバーする方法について説明します。
Extundeleteは、誤って削除されたファイルシステムタイプext3およびext4のファイルのリカバーをサポートしますが、具体的なリカバーの度合いは、削除後に書き込みによって上書きされるかどうか、メタデータがjournalに保存されるかどうかなどの要因に関連します。データのリカバーを必要とするファイルシステムがシステムディスクにあり、常にサービスプロセスまたはシステムプロセスがファイルを書き込んでいる場合、リカバーの可能性は低くなります。

> 説明：
> Tencent Cloudは、スナップショットの作成、カスタマイズイメージの作成 および Cloud Object Storage などのデータストレージ方法を提供しています。データセキュリティを向上させるために、定期的にデータバックアップを行うことをお勧めします。

## 準備作業

データリカバーに関連する操作を実行する前に、次の準備を完了してください：

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

## 操作手順

1. 次の2つの方法を使用して、Extundeleteをインストールします：

### コンパイルされたバイナリプログラムをダウンロードします（推奨）

1. 次のコマンドを実行して、コンパイルされたバイナリプログラムを直接ダウンロードできます。

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

2. 次のコマンドを実行して、ファイルの権限を付与します。

```
chmod a+x extundelete
```

### 手動によるコンパイルとインストール

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

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

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

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

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

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

3. 次のコマンドを実行して、v1.0.tar.gzファイルを解凍します。

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

4. 次のコマンドを実行して、コンパイルしてインストールします。

```
cd extundelete-1.0
```

```
./configure
```

```
make
```

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

```
cd ./src
```

2. 次のコマンドを実行して、データのリカバーを試みます。

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

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

# LinuxシステムでのUSB/IPによるリモートUSBデバイス共有

最終更新日：：2021-03-26 15:39:38

## シナリオ

USB/IP カーネルに統合されたオープンソースのプロジェクトで、Linux環境ではUSB/IPを介してUSBデバイスをリモートで共有できます。このドキュメントでは、次の環境バージョンを例に、USB/IPを使用してUSBデバイスをリモートで共有する方法をデモします。
USB Client：CentOS 7.6 OSのCVM
USB Server：Debian OSのローカルコンピュータ

## 注意事項

USB/IPのインストール方法とカーネルモジュール名は、Linux OSのディストリビューションによって異なります。現在のLinux OSがUSB/IP機能をサポートしているかどうかを確認してください。

## 操作手順

### USB Serverを設定する

1. ローカルPCで次のコマンドを順に実行して、USB/IPをインストールし、関連するカーネルモジュールをロードします。

```
sudo apt-get install usbip
sudo modprobe usbip-core
sudo modprobe vhci-hcd
sudo modprobe usbip_host
```

2. USBデバイスを挿入し、次のコマンドを実行して、利用可能なUSBデバイスを確認します。

```
usbip list --local
```

たとえば、Feitian USBキーがローカルPCに挿入されると、次の結果が返されます。

```
busid 1-1.3(096e:031b)
Feitian Technologies, Inc.: unknown product(096e:031b)
```

3. busid値を記録し、以下のコマンドを順に実行して、リスニングサービスを有効にし、USB/IPポート番号を指定して、USBデバイスを共有します。

```
sudo usbipd -D [--tcp-port PORT]
sudo usbip bind -b [busid]
```

たとえば、指定されたUSB/IPポート番号が3240（つまり、USB/IPのデフォルトポート）で、busidが `1-1.3` の場合、次のコマンドを実行します。

```
sudo usbipd -D
sudo usbip bind -b 1-1.3
```

4.（オプション）次のコマンドを実行してSSHトンネルを作成し、ポートでリスニングします。

> 説明：
> パブリックIPのないローカルPCは、この手順を実行してください。ローカルPCにパブリックIPがある場合は、この手順をスキップしてください。

```
ssh -Nf -R <Specified USB/IP port>:localhost:<Specified USB/IP port>
root@your_host
```

`your_host` はCVMのIPアドレスを示します。
たとえば、USB/IPのポート番号が3240で、CVMのIPアドレスが192.168.15.24の場合、次のコマンドを実行します。

```
ssh -Nf -R 3240:localhost:3240 root@192.168.15.24
```

## USBクライアントを設定する

> 説明：
> 以下の手順では、パブリックIPアドレスのないローカルPCを例に説明します。ローカルPCにパブリックIPアドレスがある場合は、次の手順の `127.0.0.1` をローカルPCのパブリックIPアドレスに置き換えます。

1. 標準のログイン方法を使用してLinuxインスタンスにログインする（推奨）。
2. 次のコマンドを順に実行して、USB/IPソースをダウンロードします。

```
rpm --import https://www.elrepo.org/RPM-GPG-KEY-elrepo.org
rpm -ivh http://www.elrepo.org/elrepo-release-7.0-
3.el7.elrepo.noarch.rpm
```

3. 次のコマンドを順に実行して、USB/IPをインストールします。

```
yum -y install kmod-usbip usbip-utils
modprobe usbip-core
modprobe vhci-hcd
modprobe usbip-host
```

4. 次のコマンドを実行して、CVMの利用可能なUSBデバイスを確認します。

```
usbip list --remote 127.0.0.1
```

たとえば、Feitian USBキーの情報を見つけて、次の結果が返されます。

```
 Exportable USB devices
 ======================
 -127.0.0.1 1-1.3: Feitian Technologies, Inc.: unknown
product(096e:031b):/sys/devices/platform/scb/fd500000.pcie/pci0000:00/
0000:00:00.0/0000:01:00.0/usb1/1-1/1-1.3:(Defined at Interface level)
(00/00/00)
```

5. 次のコマンドを実行して、USBデバイスをCVMにバインドします。

```
usbip attach --remote=127.0.0.1 --busid=1-1.3
```

6. 次のコマンドを実行して、現在のUSBデバイスリストをクエリーします。

```
lsusb
```

下記のような情報が返された場合は、共有が成功したことを示しています。

```
Bus 002 Device 002:ID096e:031b Feitian Technologies, Inc.
Bus 002 Device 001:ID1d6b:0002 Linux Foundation 2.0 root hub
```

```
Bus 001 Device 001:ID1d6b:0001 Linux Foundation 1.1 root hub
```

# WindowsシステムでのRemoteFXによるUSBデバイスリダイレクト

最終更新日：：2022-05-26 12:01:52

## ユースケース

RemoteFxは、Windows デスクトッププロトコル（RDP）のアップグレード版です。RDP8.0以降は、RemoteFxを使用して、RDPデータチャネルを介してローカルUSBデバイスをリモートデスクトップにリダイレクトして、CVMがUSBデバイスを使用できない問題を解決できます。
このドキュメントでは、次の環境バージョンを例として、RDPのRemoteFx USBリダイレクト機能を有効にしてUSBデバイスをCVMにリダイレクトする方法を説明します。

- クライアント：Windows 10 OS
- サーバー：Windows Server 2016 OS

## 使用制限

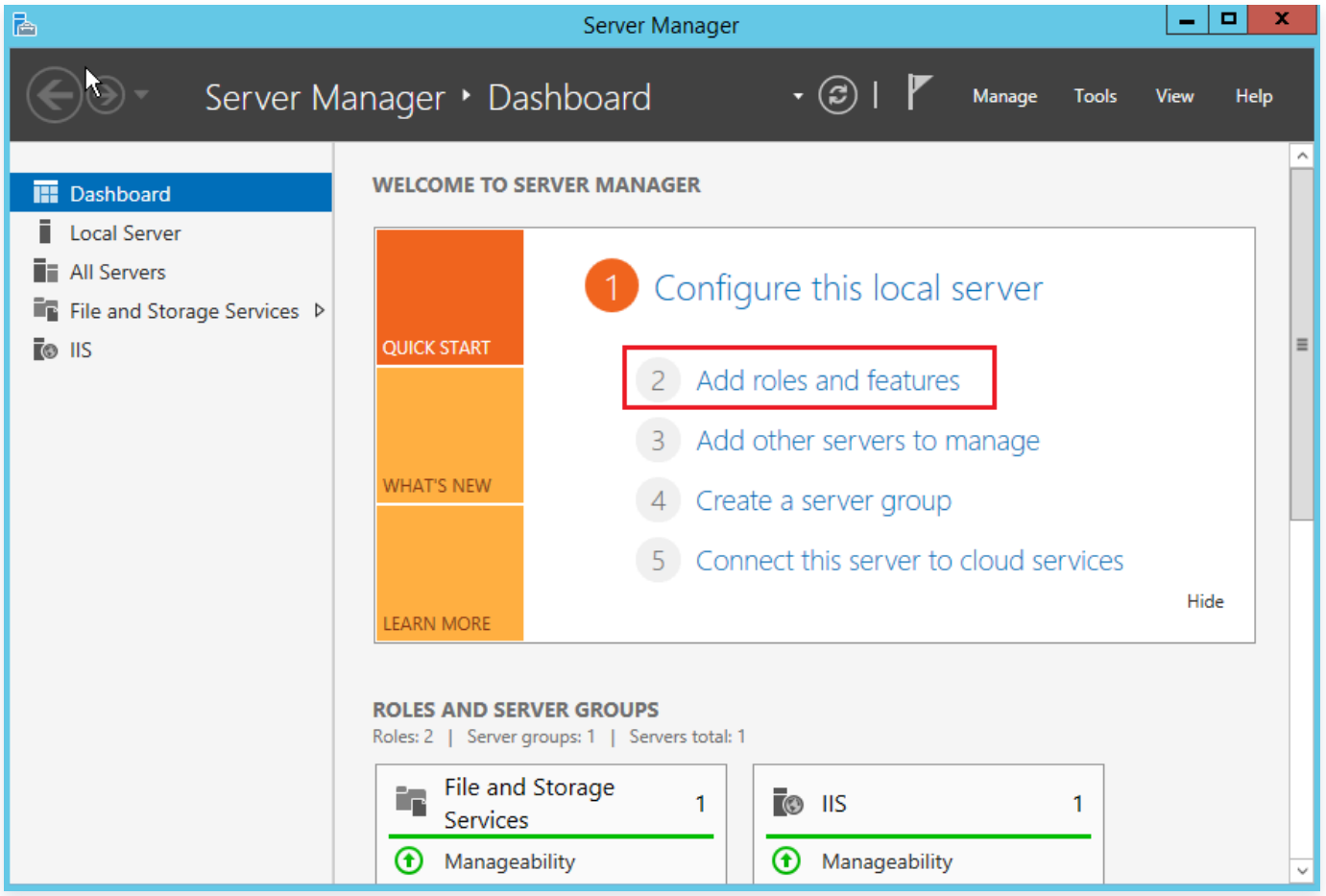
RDP 8.0以降のバージョンは、RemoteFX USB Redirection機能をサポートしているため、Windows 8、Windows 10、Windows Server 2016、およびWindows Server 2019がこの機能をサポートしています。ローカルPCのOSバージョンが上記のバージョンのいずれかである場合、RDP 8.0 Updateパッチをインストールする必要はありません。ローカルPCのOSバージョンがWindows 7またはWindows Vistaの場合は、マイクロソフトの公式Webサイト にアクセスして、RDP 8.0更新パッチを入手してインストールしてください。

## 操作手順

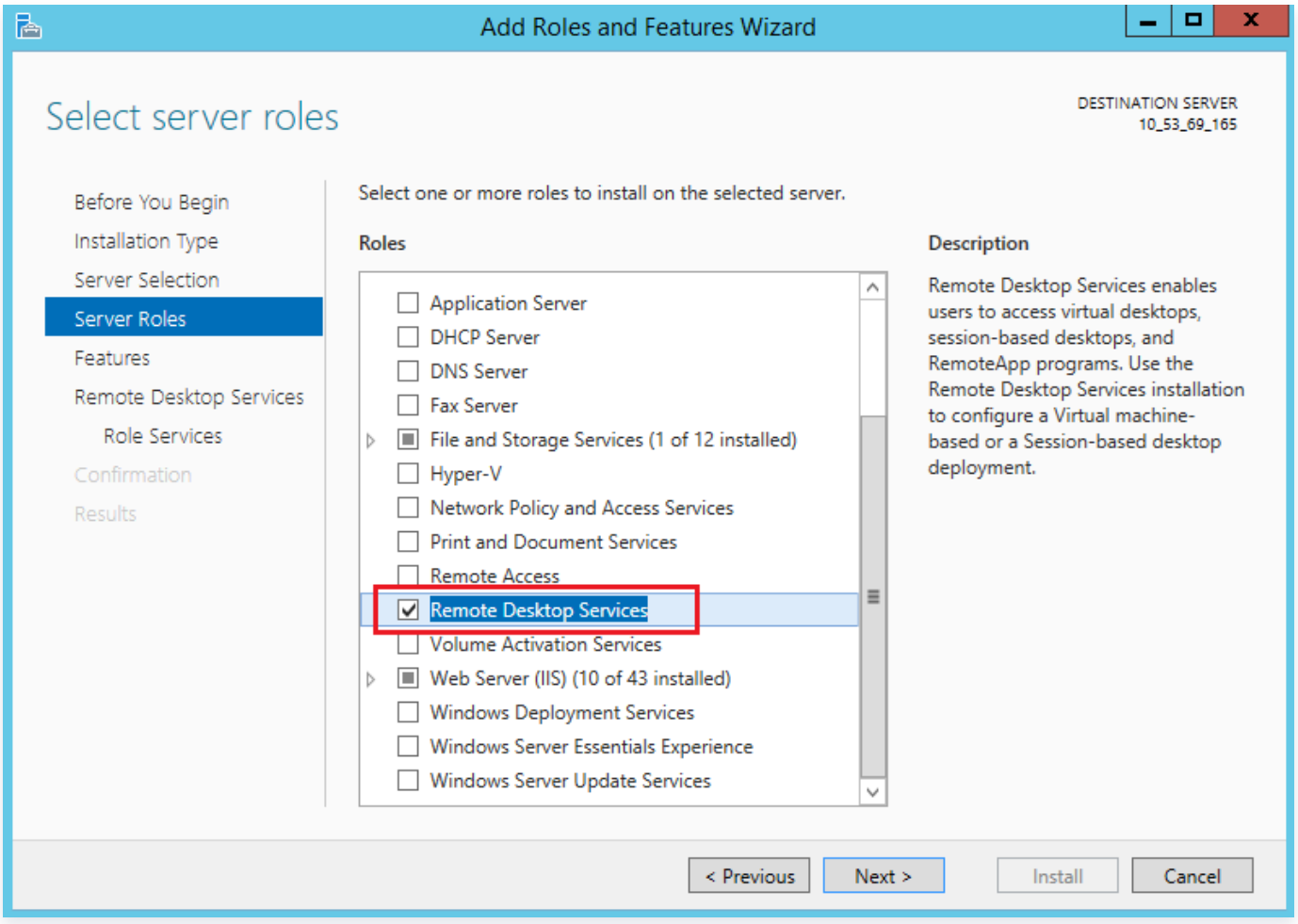
### サーバーを設定する

1. RDPファイルを利用してWindowsインスタンスにログインする（推奨）。
2. OSの画面で、  をクリックして、サーバーマネージャーを選択して、サーバーマネージャーを開きます。

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

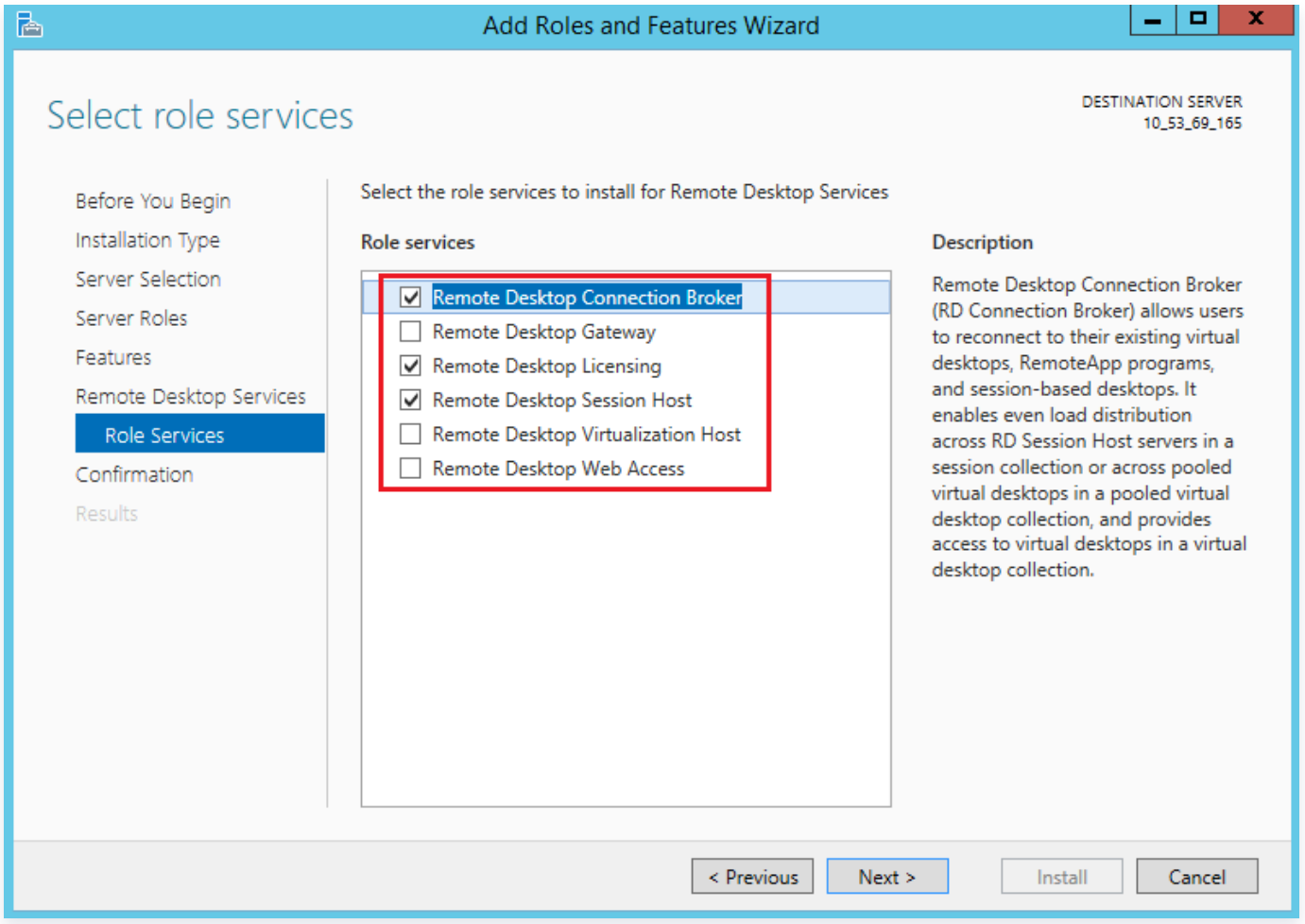



4. ポップアップされた「役割と機能の追加ウィザード」画面で、次へをクリックして、「インストールの種類を選択」画面に入ります。
5. 「インストールの種類を選択」画面で、役割ベースまたは機能ベースのインストールを選択して、次へをクリックします。
6. 「対象サーバーの選択」画面で、デフォルト設定のままにして、次へをクリックします。
7. 「サーバーのロールを選択」画面で、次の図に示すように、リモートデスクトップサービスを選択し、次へをクリックします。



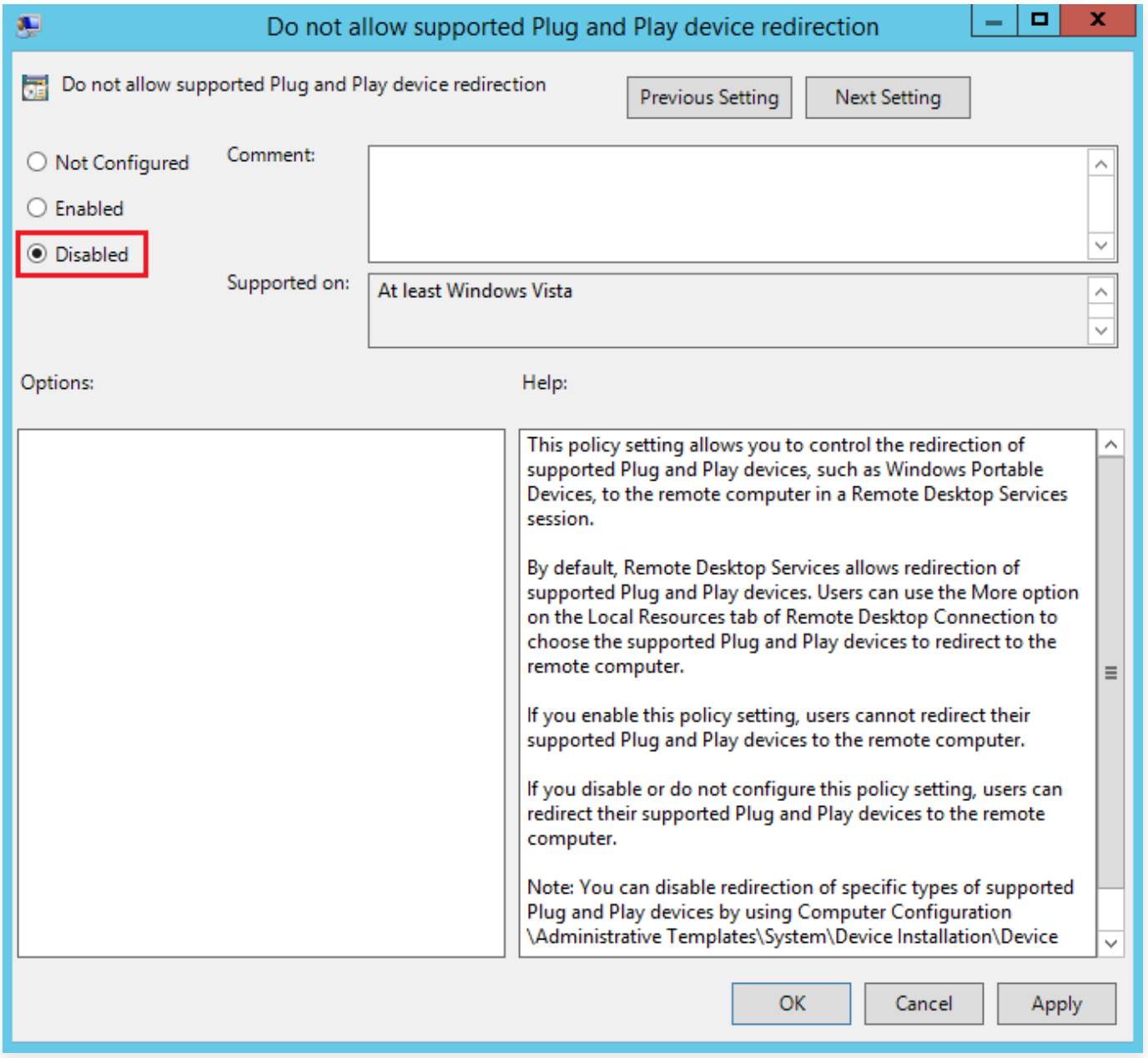

8. デフォルト設定のままにして、次へを2回クリックします。
9. 「役割サービスの選択」画面で、次の図に示すように、リモートデスクトップセッションホスト、リモートデスクトップ接続ブローカー、およびリモートデスクトップライセンスにチェックをいれて、ポップアップされ

た画面で機能の追加をクリックします。




10. 次へをクリックします。
11. インストールをクリックします。
12. インストールが完了すると、CVMを再起動します。
13. OS画面で、  をクリックし、gpedit.mscを入力して、Enterキーを押して、「ローカルグループポリシーエディター」を開きます。
14. 左側のナビゲーションツリーで、次の図に示すように、コンピューターの設定>管理用テンプレート>Windowsコンポーネント>リモートデスクトップサービス> リモートデスクトップセッションホスト>デバイスとリソースのリダイレクトを選択し、サポートされているプラグ アンド プレイ デバイスのリダイレクトを

許可しないをダブルクリックして開きます。

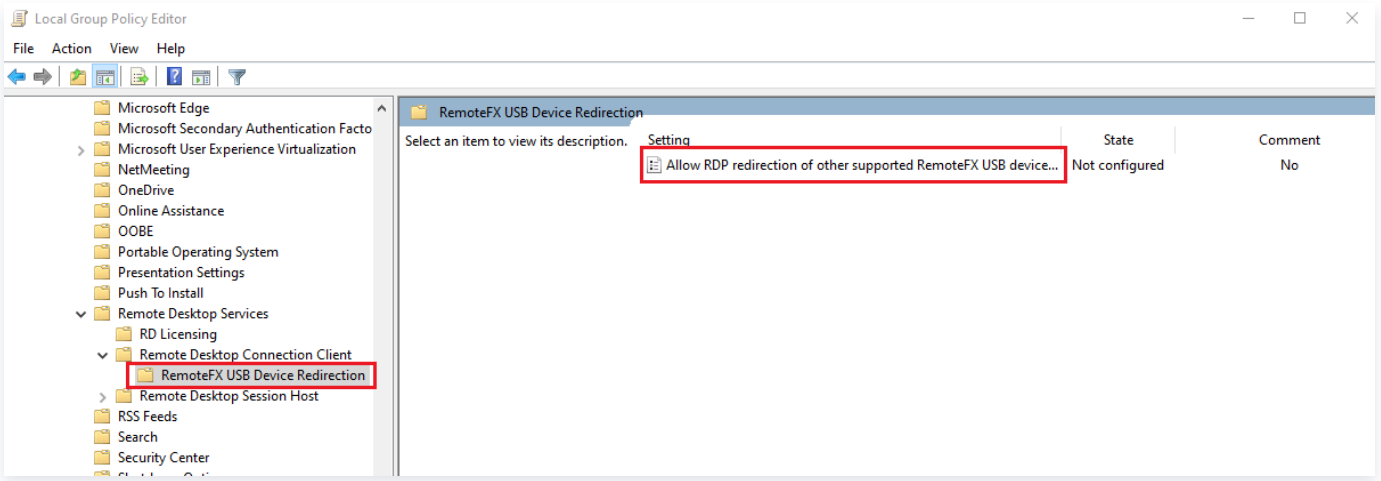



15. ポップアップされた画面で、次の図に示すように、無効を選択し、OKをクリックします。
16. CVMを再起動します。

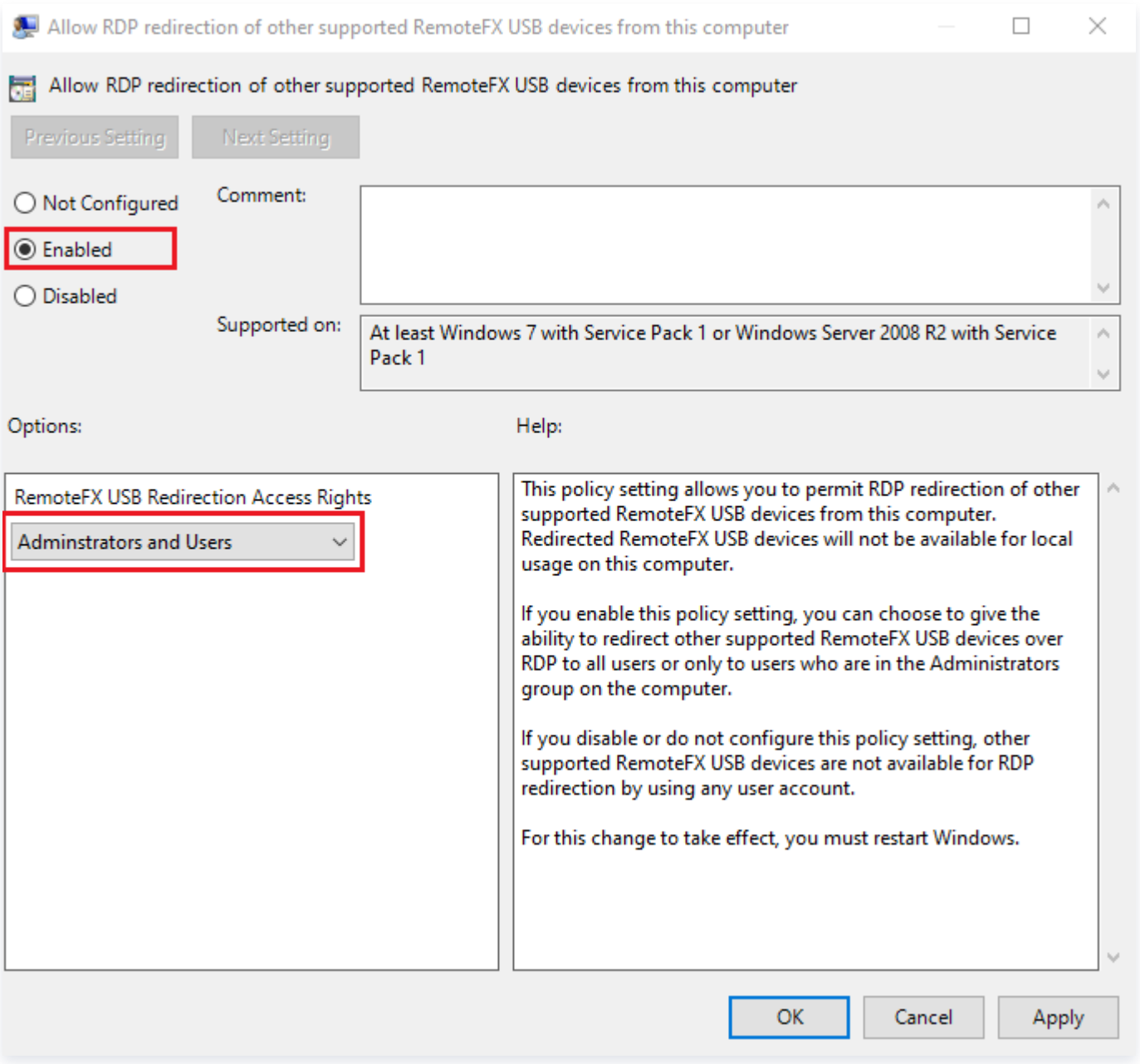
## クライアントを設定する

1. ローカルコンピュータで、  を右クリックし、実行を選択し、実行ダイアログボックスを開きます。
2. 実行ダイアログボックスでgpedit.mscと入力し、OKをクリックして「ローカルグループポリシーエディター」を開きます。
3. 左側のナビゲーションツリーで、次の図に示すように、コンピューターの設定 > 管理用テンプレート > Windowsコンポーネント > リモートデスクトップサービス > リモートデスクトップセッションホスト > RemoteFx USBデバイスリダイレクトを選択します。サポートされている他の RemoteFX USB デバイスの、

このコンピューターからの RDP リダイレクトを許可するをダブルクリックして開きます。



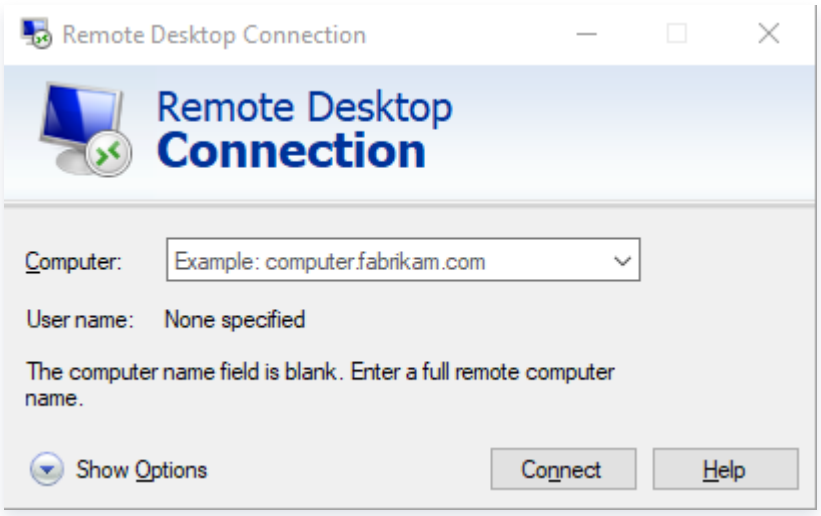

4. ポップアップされた画面で、次の図に示すように、有効を選択し、RemoteFx USBリダイレクトのアクセス権限を管理者とユーザーに設定します。



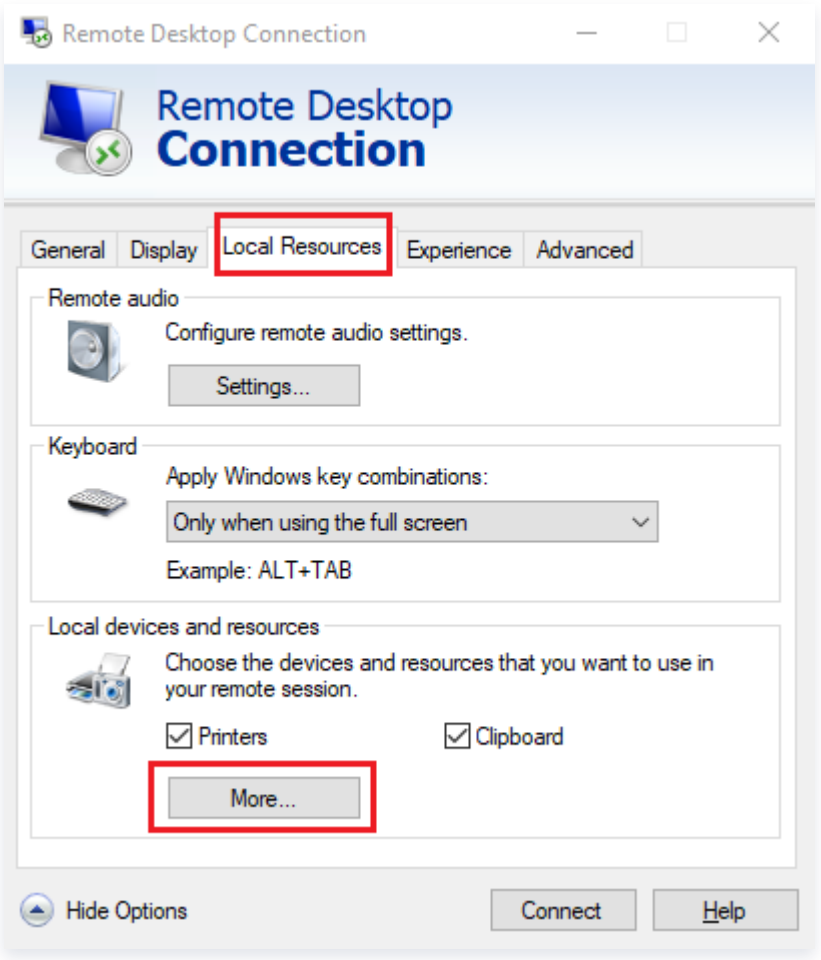

5. OKをクリックします。
6. ローカルPCを再起動します。

## 設定結果を確認する

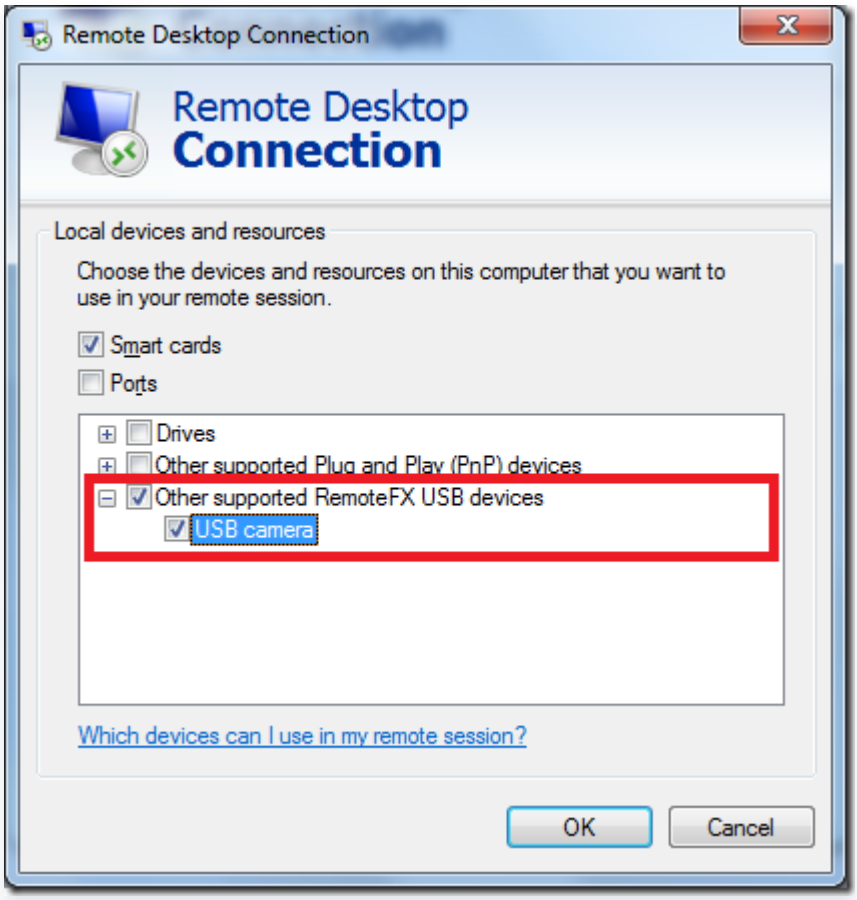
1. ローカルPCで、USBデバイスを挿入し、  を右クリックして、実行を選択して、実行ダイアログボックスを開きます。
2. 実行ダイアログで、次の図に示すように、mstscと入力し、Enterキーを押して、リモートデスクトップ接続ダイアログボックスを開きます。



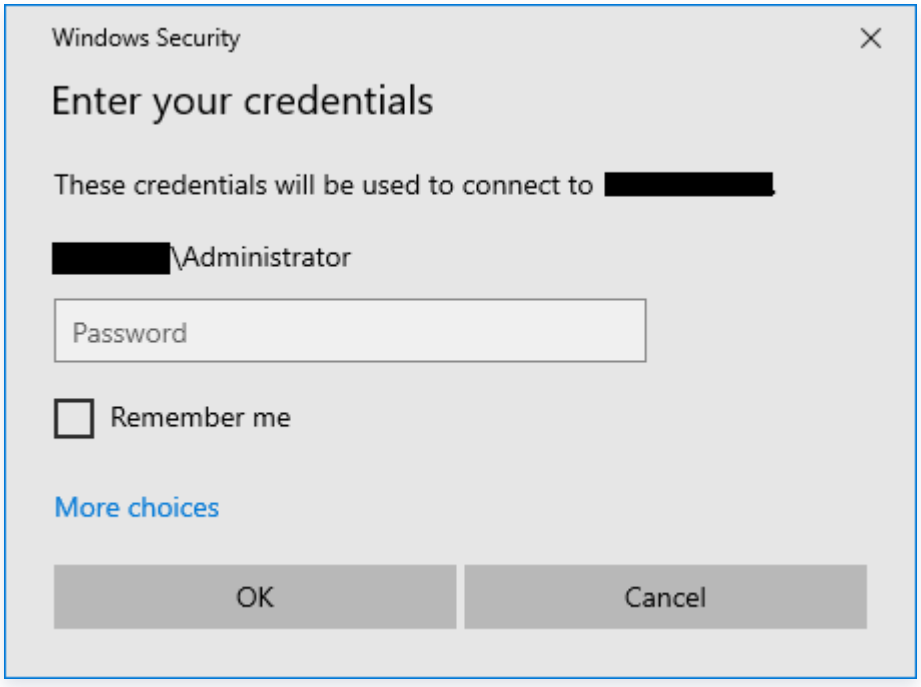

3. コンピュータの後に、Windowsサーバーのパブリックipアドレスを入力し、オプションをクリックします。
4. ローカルリソースタブを選択し、「ローカルデバイスとリソース」列の詳細をクリックして、次の図に示すように、ローカルデバイスとリソースの画面が表示されます。




5. ポップアップされたローカルデバイスとリソースの画面で、その他のサポートされているRemoteFX USBデバイスを展開し、挿入されたUSBデバイスを選択して、OKをクリックします。

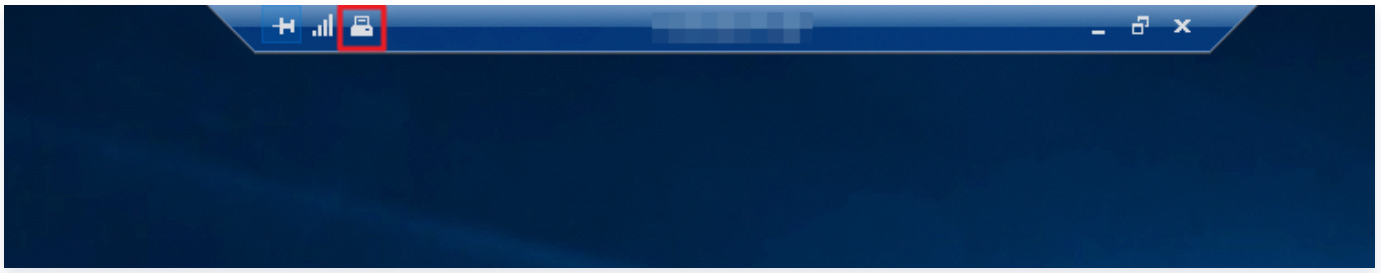



6. 接続をクリックします。
7. ポップアップされた「Windowsセキュリティ」画面で、次の図に示すように、インスタンスの管理者アカウントとパスワードを入力します。



8. OKをクリックして、Windowsインスタンスにログインします。

   Windows インスタンスの操作画面の上部に が表示されると、設定が成功したことを示します。



## 関連操作

Windows RDPプロトコルは、一般的に使用されるUSBデバイスに対してより最適化された接続パフォーマンスを提供できます。つまり、RemoteFx機能を有効にすることなく、ドライブやカメラなどのデバイスを直接マッピングできます。よく使われていないUSBデバイスは、RemoteFX USBリダイレクト機能によってのみ実現できます。よく使われていないUSBデバイスは、以下を参照して、対応するリダイレクト方法を選択できます。

| Device | Support Status | Redirection Method |
|---|---|---|
| All-in-One Printer | Supported | RemoteFX USB Redirection |
| Printer | Supported | Easy Print |
| Scanner | Supported | RemoteFX USB Redirection |
| Biometric | Supported while in session<br>*Not supported during logon* | RemoteFX USB Redirection |
| PTP Camera | Supported | Plug and Play Device Redirection |
| MTP Media Player | Supported | Plug and Play Device Redirection |
| Webcam | Supported (LAN only) | RemoteFX USB Redirection |
| VoIP Telephone/Headset | Supported (LAN only) | RemoteFX USB Redirection |
| Audio (not a USB composite device) | Supported | Audio Redirection |
| CD or DVD Drive | Supported for read operations | Drive Redirection |
| Hard Drive or USB Flash Drive | Supported | Drive Redirection |
| Smart Card Reader | Supported | Smart Card Redirection |
| USB-to-Serial | Supported | RemoteFX USB Redirection |
| USB Network Adapter (also includes some personal digital assistants) | Blocked | N/A |
| USB Display | Blocked | N/A |
| USB Keyboard or Mouse | Supported | Input Redirection |

# Tencent SGX機密コンピューティング環境の構築

最終更新日：：2025-07-18 12:02:27

## 概要

ここでは、M6ceインスタンスでTencent SGXコンフィデンシャル・コンピューティング環境を構築する方法と、Intel SGXSDKを使用してSGX機能を検証する方法をデモンストレーションします。

## 前提条件

M6ceインスタンス が作成され、ログインしていること。
-インスタンスの作成方法については、購入画面でインスタンスを作成 をご参照ください。
-インスタンスのログイン方法については、標準ログイン方式を使用してLinuxインスタンスにログイン（推奨）をご参照ください。

> 説明：
> ここでの手順は、OSがTencentOS Server 3.1(TK4)のインスタンスを使用した例であり、OSのバージョンが異なると手順も異なる場合がありますので、実際の状況に応じて操作してください。

## 操作手順

1. 次のコマンドを実行して、kernelバージョンをチェックします。

```
uname -a
```

kernelが5.4.119-19.0008より低いバージョンかどうかを確認します。
- 「はい」の場合は、次のコマンドを実行して、kernelを更新してください。

```
yum update kernel
```

- 「いいえ」の場合は、次の手順に進んでください。

2. 次のコマンドを実行して、SGX runtimeに必要なパッケージをインストールします。

```
yum install \
 libsgx-ae-le libsgx-ae-pce libsgx-ae-qe3 libsgx-ae-qve \
 libsgx-aesm-ecdsa-plugin libsgx-aesm-launch-plugin libsgx-aesm-pce-
plugin libsgx-aesm-quote-ex-plugin \
```

```
 libsgx-dcap-default-qpl libsgx-dcap-default-qpl-devel libsgx-dcap-ql
libsgx-dcap-ql-devel \
 libsgx-dcap-quote-verify libsgx-dcap-quote-verify-devel libsgx-
enclave-common libsgx-enclave-common-devel libsgx-epid-devel \
 libsgx-launch libsgx-launch-devel libsgx-pce-logic libsgx-qe3-logic
libsgx-quote-ex libsgx-quote-ex-devel \
 libsgx-ra-network libsgx-ra-uefi libsgx-uae-service libsgx-urts sgx-
ra-service \
sgx-aesm-service
```

説明:
SGX AESMサービスのデフォルトのインストールディレクトリは、`/opt/intel/sgx-aesm-service` です。

3. 次のコマンドを実行して、Intel SGXSDKをインストールします。

```
yum install sgx-linux-x64-sdk
```

説明:
Intel SGXSDKのデフォルトのインストールディレクトリは、/ `opt/intel/sgxsdk` です。Intel SGXSDK ユーザーマニュアルを参照して、SGXプログラムを開発することができます。

4. SGX runtimeとIntel SGXSDKのインストールが完了したら、インスタンスを再起動してください。詳細については、インスタンスの再起動 をご参照ください。
5. Tencent Cloud SGXリモートアテステーションサービスを構成します。
Tencent Cloud SGXリモートアテステーションサービスは、リージョン化デプロイを採用しています。SGX CVMインスタンスが配置されているリージョンでTencent Cloud SGXリモートアテステーションサービスにアクセスすれば、最高のカスタマーエクスペリエンスを体験できます。Intel SGXSDKをインストールすると、リモートアテステーションサービスのデフォルト構成ファイル `/etc/sgx_default_qcnl.conf` が自動的に生成されます。SGX CVMインスタンスが配置されているリージョンのTencent Cloud SGXリモートアテステーションサービスに適応するように、以下の手順に従ってこのファイルを手動で変更してください。

説明:
- 現在、北京、上海および広州リージョンのみで、Tencent Cloud SGXリモートアテステーションサービスがサポートされています。
- Intel Ice Lakeは、Intel SGX DCAPベースのリモートアテステーション方式のみをサポートし、Intel EPIDリモートアテステーション方式はサポートしていません。

VIMエディタを使用して、`/etc/sgx_default_qcnl.conf`を以下のように変更します。

```
# PCCS server address
PCCS_URL=https://sgx-dcap-server-tc.[Region-
ID].tencent.cn/sgx/certification/v3/
# To accept insecure HTTPS cert, set this option to FALSE
USE_SECURE_CERT=TRUE
```

`[Region-ID]`をSGX CVMインスタンスが配置されているリージョンのIDに置き換えてください。 例: 北京リージョンの変更例は次のとおりです。

```
# PCCS server address
PCCS_URL=https://sgx-dcap-server-
tc.bj.tencent.cn/sgx/certification/v3/
# To accept insecure HTTPS cert, set this option to FALSE
USE_SECURE_CERT=TRUE
```

上海リージョンの変更例は次のとおりです。

```
# PCCS server address
PCCS_URL=https://sgx-dcap-server-
tc.sh.tencent.cn/sgx/certification/v3/
# To accept insecure HTTPS cert, set this option to FALSE
USE_SECURE_CERT=TRUE
```

広州リージョンの変更例は次のとおりです。

```
# PCCS server address
PCCS_URL=https://sgx-dcap-server-
tc.gz.tencent.cn/sgx/certification/v3/
# To accept insecure HTTPS cert, set this option to FALSE
USE_SECURE_CERT=TRUE
```

## SGX機能の検証例

### 例1：Enclaveの起動

Intel SGXSDKは、SGX機能を検証するためのSGXサンプルコードを提供します。デフォルトのディレクトリは、`/opt/intel/sgxsdk/SampleCode`です。この例のコード(SampleEnclave)の効果は、Enclaveを起動し

て、インストールされたSGXSDKが正常に使用されているか、また、SGX CVMインスタンスの機密メモリリソースが使用可能かどうかを検証することです。

1. 次のコマンドを実行して、Intel SGXSDKに関連する環境変数を設定します。

```
source /opt/intel/sgxsdk/environment
```

2. 次のコマンドを実行して、サンプルコードSampleEnclaveをコンパイルします。

```
cd /opt/intel/sgxsdk/SampleCode/SampleEnclave && make
```

3. 次のコマンドを実行して、コンパイルされた実行可能ファイルを実行します。

```
./app
```

以下のような結果が返されれば、起動に成功しています。

```
[root@VM-8-14-centos SampleEnclave]# ./app
Checksum(0x0x7ffcb9b49a30, 100) = 0xfffd4143
Info: executing thread synchronization, please wait...
Info: SampleEnclave successfully returned.
Enter a character before exit ...
```

## 例2：SGXリモートアテステーション

Intel SGXのcode treeは、SGXリモートアテステーション機能(DCAP)を検証するためのサンプルコードを提供します。この例は、Quoteを発行および検証するためのもので、Quote Generator(QuoteGenerationSample)とQuote Verifier(QuoteVerificationSample)が含まれます。

1. 次のコマンドを実行して、Intel SGXSDKに関連する環境変数を設定します。

```
source /opt/intel/sgxsdk/environment
```

2. 次のコマンドを順に実行してgitをインストールし、Intel SGX DCAP code treeをダウンロードします。

```
cd /root && yum install git
```

```
git clone
https://github.com/intel/SGXDataCenterAttestationPrimitives.git
```

3. 次のコマンドを順に実行して、Quote GeneratorのサンプルコードQuoteGenerationSampleをコンパイルして実行します。

   3.1 QuoteGenerationSampleディレクトリに入ります。

```
cd
/root/SGXDataCenterAttestationPrimitives/SampleCode/QuoteGeneratio
nSample
```

   3.2 QuoteGenerationSampleをコンパイルします。

```
make
```

   3.3 QuoteGenerationSampleを実行し、Quoteを発行します。

```
./app
```

4. 次のコマンドを実行して、QuoteVerifierのサンプルコードQuoteVerificationSampleをコンパイルします。

```
cd
/root/SGXDataCenterAttestationPrimitives/SampleCode/QuoteVerificationS
ample && make
```

5. 次のコマンドを実行して、QuoteVerificationSample Enclaveに署名します。

```
sgx_sign sign -key Enclave/Enclave_private_sample.pem -enclave
enclave.so -out enclave.signed.so -config Enclave/Enclave.config.xml
```

6. 次のコマンドを実行して、QuoteVerificationSampleを実行し、Quoteを検証します。

```
./app
```

以下のような結果が返されれば、検証に成功しています。

```
[root@VM-8-14-centos QuoteVerificationSample]# ./app
Info: ECDSA quote path: ../QuoteGenerationSample/quote.dat

Trusted quote verification:
        Info: get target info successfully returned.
        Info: sgx_qv_set_enclave_load_policy successfully returned.
        Info: sgx_qv_get_quote_supplemental_data_size successfully returned.
        Info: App: sgx_qv_verify_quote successfully returned.
        Info: Ecall: Verify QvE report and identity successfully returned.
        Info: App: Verification completed successfully.
        Info: Supplemental data version: 3

============================================

Untrusted quote verification:
        Info: sgx_qv_get_quote_supplemental_data_size successfully returned.
        Info: App: sgx_qv_verify_quote successfully returned.
        Info: App: Verification completed successfully.
        Info: Supplemental data version: 3
```

# M6pインスタンスへの永続メモリの設定

最終更新日：：2022-03-16 17:10:24

## 概要

ここでは、M6pインスタンスで永続メモリを構成する方法についてご説明します。
##インスタンス構成
ここでは、次の構成のCVMインスタンスを使用します。取得に関する情報については、実際の状況によります。

- インスタンス仕様：メモリ型M6pインスタンスM6p.LARGE16（4 コア 16GB）。その他の仕様については、メモリ型 M6p をご参照ください。
- オペレーティングシステム： TencentOS Server 3.1(TK4)。

> 説明：
> インスタンスには、次のオペレーティングシステムを使用することをお勧めします。
> - TencentOS Server 3.1
> - CentOS 7.6およびそれ以降のバージョン
> - Ubuntu 18.10およびそれ以降のバージョン

## 前提条件

M6pインスタンス が作成され、ログインしていること。
–インスタンスの作成方法については、購入画面でインスタンスを作成 をご参照ください。
–インスタンスのログイン方法については、標準ログイン方式を使用してLinuxインスタンスにログイン（推奨）をご参照ください。

## Intel® Optane™ DC BPSハードウェア(PMEM)モードのご紹介

### Memoryモード

Memoryモードでは、通常のDRAMがアクセス頻度の高いデータのキャッシュとして機能し、永続メモリはバックアップメモリとして使用され、高速なキャッシュの管理操作はメモリコントローラが自動的に処理します。

### ADモード

M6pモデルはこのモードを採用しています。M6pモデルでは、プラットフォーム側でBPSハードウェアをADモードで構成し、CVMにパススルーして使用します。ADモードでは、アプリケーションはPMEMデバイスをメモリとして使用したり、ローカルのSSDディスクとして使用したりすることができます。

## 操作手順

### PMEM初期化

インスタンスを初めて使用する場合は、次のコマンドを順に実行して、PMEMデバイスを初期化します。すでにPMEMの初期化を実行している場合は、この手順をスキップしてください。

```
yum install -y ndctl
```

```
ndctl destroy-namespace all --force
```

> 説明:
> 最大仕様のインスタンスには2つのregionがあります。次のコマンドを実行した後、region0をregion1に置き換えて、コマンドを再実行してください。

```
ndctl disable-region region0
```

```
ndctl init-labels all
```

```
ndctl enable-region region0
```

## ADモードでのPMEMの構成

実際のニーズに応じて、永続メモリをメモリまたはローカルSSDディスクとして使用できます。

### メモリとして使用

PMEMは、上位レイヤのアプリケーション（redisなど）に永続メモリを割り当てるためのキャラクタデバイスとして使用できます。memkindなどのPMDKフレームワークの機能によって使用できます。構成方法は以下のとおりです。

1. 次のコマンドを実行して、キャラクタデバイスを生成します。

   ```
   ndctl create-namespace -r region0 -m devdax
   ```

   返された結果を下図に示します。これは、`dax0.0` キャラクタデバイスが生成されたことを示しています。

```
[root@VM-11-3-centos ~]# ndctl create-namespace -r region0 -m devdax
{
  "dev":"namespace0.0",
  "mode":"devdax",
  "map":"dev",
  "size":"61.04 GiB (65.54 GB)",
  "uuid":"71cceaeb-[illegible]",
  "daxregion":{
    "id":0,
    "size":"61.04 GiB (65.54 GB)",
    "align":2097152,
    "devices":[
      {
        "chardev":"dax0.0",
        "size":"61.04 GiB (65.54 GB)",
        "target_node":0,
        "mode":"devdax"
      }
    ]
  },
  "align":2097152
}
```

最大仕様のインスタンスには2つのregionがあります。最大仕様のインスタンスを使用する場合は、次のコマンドを同時に実行してください。

```
ndctl create-namespace -r region1 -m devdax -f
```

構成が完了すると、`/dev` ディレクトリに `dax0.0` キャラクタデバイスが生成され、永続メモリにマッピングできます。

2. 次のコマンドを実行して、永続メモリサイズを確認します。

```
ndctl list -R
```

実行結果は下図に示すように:

```
[root@VM-11-3-centos ~]# ndctl list -R
[
  {
    "dev":"region0",
    "size":66584576000,
    "available_size":0,
    "max_available_extent":0,
    "type":"pmem",
    "iset_id":10248187106440278,
    "persistence_domain":"memory_controller"
  }
]
```

### 拡張機能（オプション）

この手順で機能を拡張し、次のコマンドを順に実行することで、PMEMを使用してCVMのメモリを拡張することができます。

1. 上位バージョンのカーネル（5.1以上かつKMEM DAXドライバーを使用、例：TencentOS Server 3.1のカーネル）のサポートにより、devdaxモードのPMEMをさらにkmemdaxに構成すると、PMEMを使用して、CVMのメモリを拡張することができます。

```
yum install -y daxctl
```

```
daxctl migrate-device-model
```

```
reboot
```

```
daxctl reconfigure-device --mode=system-ram --no-online dax0.0
```

実行結果は下図に示すように：

```
[root@VM-11-3-centos ~]# daxctl reconfigure-device --mode=system-ram --no-online dax0.0
[
  {
    "chardev":"dax0.0",
    "size":65542291456,
    "target_node":0,
    "mode":"system-ram"
  }
]
```

2. 次のコマンドを実行して、システムメモリの拡張状況を確認します。

```
numactl -H
```

実行結果は下図に示すように：

```
[root@VM-11-3-centos ~]# numactl -H
available: 1 nodes (0)
node 0 cpus: 0 1 2 3
node 0 size: 77962 MB
node 0 free: 76586 MB
node distances:
node   0
  0:  10
```

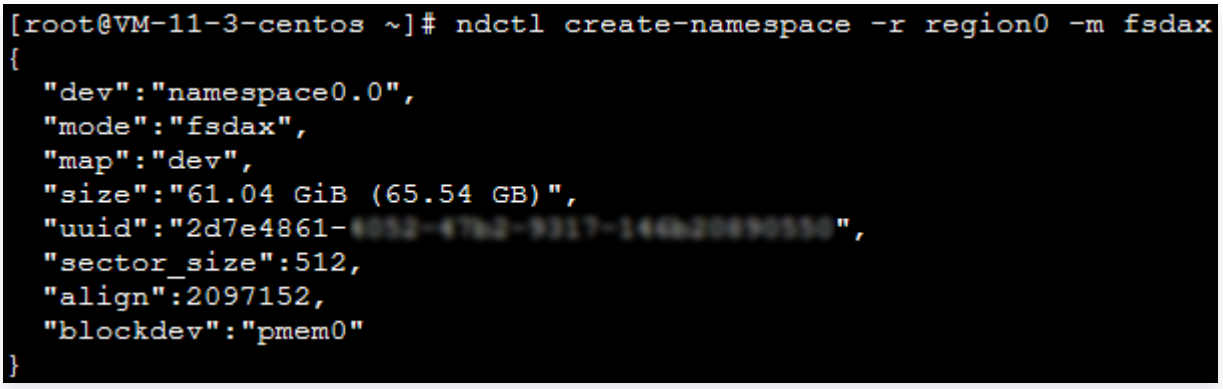
### ローカルSSDディスクとして使用

ADモードのPMEMは、高速ブロックデバイスとして構成することもでき、ファイルシステムの作成やベアディスクの読み取り・書き込み操作など、一般的なブロックデバイスとして使用できます。構成方法は以下のとおりです。

1. 次のコマンドを実行して、`/dev` ディレクトリにpmem0ブロックデバイスを生成します。

```
ndctl create-namespace -r region0 -m fsdax
```

実行結果は下図に示すように:




最大仕様のインスタンスには2つのregionがあります。最大仕様のインスタンスを使用する場合は、次のコマンドを同時に実行してください。

```
ndctl create-namespace -r region1 -m fsdax -f
```

2. 次のコマンドを順に実行して、ファイルシステムを作成するか、マウントして使用します。

2.1 ファイルシステムを作成します。

```
mkfs.ext4 /dev/pmem0
```

返された結果を下図に示します。これは、ファイルシステムの作成が成功したことを示しています。

```
[root@VM-11-3-centos ~]# mkfs.ext4 /dev/pmem0
mke2fs 1.45.6 (20-Mar-2020)
Creating filesystem with 16001536 4k blocks and 4005888 inodes
Filesystem UUID: ce9da959-[illegible]
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624, 11239424

Allocating group tables: done
Writing inode tables: done
Creating journal (65536 blocks): done
Writing superblocks and filesystem accounting information: done
```

2.2 `/mnt/` にマウントします。

```
mount -o dax,noatime /dev/pmem0 /mnt/
```

## 参考資料

- Intel® Optane™ DC Persistent Memory
- Linux Provisioning for Intel® Optane™ Persistent Memory

# PythonによるクラウドAPI呼び出しでカスタムイメージを一括共有

最終更新日：：2023-06-25 18:00:02

## 操作步骤

このドキュメントでは、Python SDKを使用してAPIを呼び出し、サブユーザーを通じてCVMのカスタムイメージを一括でまとめて共有する方法について説明します。同様のニーズがある場合、またはSDKの使用方法を知りたい場合は、このドキュメントをご覧ください。

## 前提条件

- サブユーザーを作成しました。そのサブユーザーは CVM およびクラウド APIに対するすべての権限を持ちます。
- サブユーザーの作成方法については、 サブユーザーの作成 をご参照ください。
- サブユーザーに権限を付与する方法については、サブユーザー権限の設定 をご参照ください。このドキュメントでは、サブユーザーに `QcloudCVMFullAccess` と `QcloudAPIFullAccess` のプリセットポリシーを付与します。
- サブユーザーの SecretId と SecretKey を作成します。操作手順については、アクセスキー をご参照ください。作成したSecretId と SecretKeyを適切に保存する必要があります。
- 共有するカスタムイメージがあります。カスタムイメージを作成する必要がある場合は、 カスタムイメージの作成 をご参照ください。

## 操作手順

### Pythonのインストール

1. 次のコマンドを実行して、Python 3.6 以降が現在のCVMインスタンスにインストールされているかどうかを確認します。インストールされている場合は、このステップをスキップしてください。

```
python --version
```

2. CVMインスタンスに Python がインストールされていない場合。
   - CentOS 上の CVM インスタンスの場合は、次のコマンドを実行して Python をインストールします。

```
yum install python3
```

- Ubuntu または Debian上のCVM インスタンスの場合は、次のコマンドを実行して Python をインストールします。

```
sudo apt install python3
```

- 他のOS上の CVM インスタンスの場合は、 Python 公式ウェブサイト にアクセスし、Python 3.6 以降をダウンロードし、インストールパッケージを Linux サーバーにアップロードし、パッケージを解凍して Python をインストールします。

3. インストールが完了したら、次のコマンドを実行して Python のバージョンを確認します。

```
python --version
```

## コード作成

1. ターゲットマシン上に `test.py` ファイルを作成し、次のコードを入力します。

```
import json
from tencentcloud.common import credential
from tencentcloud.common.profile.client_profile import ClientProfile
from tencentcloud.common.profile.http_profile import HttpProfile
from tencentcloud.common.exception.tencent_cloud_sdk_exception import
TencentCloudSDKException
from tencentcloud.cvm.v20170312 import cvm_client, models
# デフォルトでは、環境変数 TENCENTCLOUD_SECRET_ID および
TENCENTCLOUD_SECRET_KEY を読み取り、secretId および SecretKey を取得しま
す。
# 認証情報の管理方法の詳細については、
https://github.com/TencentCloud/tencentcloud-sdk-
python#%E5%87%AD%E8%AF%81%E7%AE%A1%E7%90%86をご覧ください
cred = credential.EnvironmentVariableCredential().get_credential()
httpProfile = HttpProfile()
httpProfile.endpoint = "cvm.tencentcloudapi.com"
clientProfile = ClientProfile()
clientProfile.httpProfile = httpProfile
# この例では南京が使用されています。 実際の状況に応じてリージョンを変更します。 た
とえば、上海の場合、リージョンを「ap-shanghai」に変更します。
aria = 'ap-nanjing'
client = cvm_client.CvmClient(cred,aria, clientProfile)
def img_share(img_id,img_name,accountids):
```

```
 try:
     req1 = models.ModifyImageSharePermissionRequest()
     params1 = {
         "ImageId": img_id,
         "AccountIds": accountids,
         "Permission": "SHARE"
     }
     req1.from_json_string(json.dumps(params1))

     resp1 = client.ModifyImageSharePermission(req1)
     response1 = json.loads(resp1.to_json_string())
     print(img_name,'共有成功! ',response1)
 except TencentCloudSDKException as err:
     print(img_name,'共有失敗!',err)
try:
 req = models.DescribeImagesRequest()
 params = {
     "Filters": [
         {
             "Name": "image-type",
             "Values": ["PRIVATE_IMAGE"]
         }
     ],
     "Limit": 100
 }
 req.from_json_string(json.dumps(params))
 resp = client.DescribeImages(req)
 response = json.loads(resp.to_json_string())
 img_num = response["TotalCount"]
 print('イメージリストを取得中....')
 share_config = input('1.すべてのイメージを共有します\n\n2.. 共有するイメージを決定します\n\n1 または 2 を入力して Enter キーを押します。 デフォルト値: 2: ') or '2'
 accountids = input('イメージを共有するユーザーの UIN を入力し、複数のUINをカンマで区切ってください: ').split(",")
 for i in range(img_num):
     basic = response['ImageSet'][i]
     img_id = basic['ImageId']
     img_name = basic['ImageName']
     if share_config == '1':
```

```
            img_share(img_id,img_name,accountids)
        elif share_config == '2':
            print('イメージID: ',img_id,'イメージ名: ',img_name)
            share_choice = input('このイメージを共有するかどうか y/n:') or 'y'
            if share_choice == 'y':
                img_share(img_id,img_name,accountids)
            elif share_choice == 'n':
                continue
            else:
                print('正しいオプションを入力してください! ! ')
        else:
            print('正しいオプションを入力してください! ! ')
    except TencentCloudSDKException as err:
     print(err)
```

- SecretId と SecretKey： 前提条件 で作成したサブユーザーのSecretIdとSecretKey に置き換えてください。
- aria：共有するカスタムイメージが存在する実際のリージョンに置き換えてください。詳細については、共通パラメータ をご覧ください。

2. ターゲットマシンで次のコマンドを実行してコードを実行します。

画面上の指示に従って1または2を入力(すべてのイメージを同時に共有するか、イメージを 1 つずつ選択して共有するかを選択)、ピアアカウントIDを入力します。ピアアカウント所有者に アカウント情報 ページに移動してアカウントIDを取得するように通知できます。
イメージが正常に共有されると、対応する数の RequestID が返されます。

## 関連する API ドキュメント

このドキュメントで使用されるAPIは DescribeImages と ModifyImageSharePermission です。

# PAWSのパケットロス改善方法

最終更新日：：2025-11-13 17:57:25

## 背景

`tcp_tw_recycle` は、TIME-WAIT状態の接続を迅速に回収するために使用されます。しかし、特定の状況において、特にネットワークにNAT（ネットワークアドレス変換）が存在する場合、`tcp_tw_recycle` がPAWSパケットロスを引き起こす原因となるため、無効にすることをお勧めします。
以下は、`tcp_tw_recycle` を無効にし、`tcp_tw_bucket` を設定する手順について説明します。

## 操作手順

### `tcp_tw_recycle` を無効にする

#### 一時的に無効にする

```
sudo sysctl -w net.ipv4.tcp_tw_recycle=0
```

#### 恒久的に無効にする

1. `/etc/sysctl.conf` ファイルを編集し、以下の行を追加または変更します：

   ```
   net.ipv4.tcp_tw_recycle = 0
   ```

2. 次に、設定を有効にします：

   ```
   sudo sysctl -p
   ```

### `tcp_tw_bucket` を設定する

`tcp_tw_bucket` は、TIME-WAIT状態の接続バケットの数を設定するために使用されます。この値を増やすことで、システムが大量のTIME-WAIT状態の接続をより効果的に処理できるようになります。

#### 一時的に設定

```
sudo sysctl -w net.ipv4.tcp_max_tw_buckets=4096
```

#### 恒久的に設定

1. `/etc/sysctl.conf` ファイルを編集し、以下の行を追加または変更します：

```
net.ipv4.tcp_max_tw_buckets = 4096
```

2. 次に、設定を有効にします：

```
sudo sysctl -p
```

## その他の最適化

前記の2つのパラメータ以外に、TCP接続処理の最適化に役立つ他のカーネルパラメータがあります：

### ファイルディスクリプタ数の上限の増加

```
sudo sysctl -w fs.file-max=100000
```

### システムで開けるファイル数の増加

`/etc/security/limits.conf` ファイルを編集し、以下の行を追加または変更します：

```
* soft nofile 65535
* hard nofile 65535
```

### システムで確立できる接続数上限の増加

```
sudo sysctl -w net.core.somaxconn=65535
```

### SYNキュー長の増加

```
sudo sysctl -w net.ipv4.tcp_max_syn_backlog=65535
```

### TIME-WAIT状態のタイムアウト時間の短縮

```
sudo sysctl -w net.ipv4.tcp_fin_timeout=15
```

## 設定の検証

以下のコマンドを使用して、設定が有効になっているかを検証できます：

```
sysctl -a | grep tcp_tw
```

```
sysctl -a | grep file-max
sysctl -a | grep somaxconn
sysctl -a | grep tcp_max_syn_backlog
sysctl -a | grep tcp_fin_timeout
```

## サービスの再起動

特定のサービス（Webサーバーやデータベースなど）を最適化する場合、新しいカーネルパラメータを有効化するため、そのサービスを再起動することをお勧めします。

# LinuxでGRUBを使用してカーネルパラメータを追加する方法

最終更新日：： 2025-11-25 11:27:56

## 操作シナリオ

このドキュメントでは、Tencent Cloud CVM上でGRUBを使用してカーネルパラメータを追加する方法について説明します。GRUBブートローダーを使用していて、カーネルパラメータの変更または追加を行いたい場合は、GRUBの設定ファイルを編集します。以下に、特定のディストリビューションにおいてGRUBの設定ファイルにカーネル起動パラメータを追加する方法を示します。

## OSの例

このドキュメントで使用するCVMインスタンスのOSは、CentOS 7.9、Ubuntu 24.04、OpenCloudOS 9、TencentOS Server 3.X/TencentOS Server 4.Xを例とします。

## 前提条件

Linux CVMを購入済みであること。まだCVMを購入されていない場合は、Linux CVMの設定 をご参照ください。

## 操作手順

OpenCloudOS 9およびTencentOS Server 3.X/TencentOS Server 4.Xシステムでは、業界で主流となっているgrub blscfg機能が導入されており、デフォルト設定は固定形式で `/boot/loader/entries/` 配下の対応するエントリファイルに書き込まれます。そのため、共通設定ファイルである `/etc/default/grub` を変更しても、特定バージョンのカーネルパラメータには影響しません。現在は、grubbyツールを使用して対応するカーネルパラメータを変更する必要があります。
ご使用のOSバージョンに応じて、以下の操作手順を実行してください。

1. 通常の方法でのLinuxインスタンスへログイン（推奨） 。
2. カーネル起動パラメータを追加します。

### CentOS 7.9

1. 以下のコマンドを実行して、 `/etc/default/grub` ファイルを編集します。

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

2. iキーを押して編集モードに切り替え、 `GRUB_CMDLINE_LINUX` の行を見つけます。 `GRUB_CMDLINE_LINUX` の末尾に `“name=value”` の形式でカーネルパラメータを追加します。例：今回追加する

カーネルパラメータは `systemd.debug-shell=1` です。

```
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL="serial console"
GRUB_TERMINAL_OUTPUT="serial console"
GRUB_CMDLINE_LINUX="net.ifnames=0 biosdevname=0 console=ttyS0,115200 console=tty0 panic=5 crashkernel=2G-8G:256M,8G-16G:512M,16G-:768M intel_idle.max_cstat
e=1 intel_pstate=disable processor.max_cstate=1 amd_iommu=on iommu=pt systemd.debug-shell=1"
GRUB_DISABLE_RECOVERY="true"
GRUB_SERIAL_COMMAND="serial --speed=9600 --unit=0 --word=8 --parity=no --stop=1"
```

3. Escキーを押し、:wqと入力して、ファイルを保存し終了します。
4. 以下のコマンドを実行して、Kernelの設定を再生成します。

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

5. 以下のコマンドを実行して、インスタンスを再起動します。

```
reboot
```

6. 以下のコマンドを実行して、変更したか確認します。

```
cat /proc/cmdline
```

結果に追加したパラメータが含まれていれば、追加完了です。

```
[root@VM-3-11-centos ~]# cat /proc/cmdline
BOOT_IMAGE=/boot/vmlinuz-3.10.0-1160.119.1.el7.x86_64 root=UUID=4b499d76-769a-40a0-93dc-4a31a59add28 ro net.ifnames=0 biosdevname=0 console=ttyS0,11520
0 console=tty0 panic=5 crashkernel=2G-8G:256M,8G-16G:512M,16G-:768M intel_idle.max_cstate=1 intel_pstate=disable processor.max_cstate=1 amd_iommu=on io
mmu=pt systemd.debug-shell=1
```

## Ubuntu 24.04

1. 以下のコマンドを実行して、 `/etc/default/grub` ファイルを編集します。

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

2. iキーを押して編集モードに切り替え、 `GRUB_CMDLINE_LINUX_DEFAULT` の行を見つけます。 `GRUB_CMDLINE_LINUX_DEFAULT` の末尾に `“name=value”` の形式でカーネルパラメータを追加します。
例：今回追加するカーネルパラメータは `systemd.debug-shell=1` です。

```
root@VM-1-22-ubuntu:/home/ubuntu# cat /etc/default/grub
# If you change this file, run 'update-grub' afterwards to update
# /boot/grub/grub.cfg.
# For full documentation of the options in this file, see:
#   info -f grub -n 'Simple configuration'

GRUB_DEFAULT=0
GRUB_TIMEOUT_STYLE=hidden
GRUB_TIMEOUT=0
GRUB_DISTRIBUTOR=`( . /etc/os-release; echo ${NAME:-Ubuntu} ) 2>/dev/null || echo Ubuntu`
GRUB_CMDLINE_LINUX_DEFAULT="splash=silent showopts crashkernel=2G-8G:256M,8G-16G:512M,16G-:768M net.ifnames=0 biosdevname=0 console=ttyS0,115200 console=tty0 panic=5
_idle.max_cstate=1 intel_pstate=disable processor.max_cstate=1 amd_iommu=on iommu=pt systemd.debug-shell=1"
GRUB_CMDLINE_LINUX=""
```

3. Escキーを押し、:wqと入力して、ファイルを保存し終了します。
4. 以下のコマンドを実行して、Kernelの設定を再生成します。

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

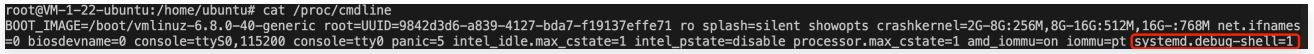
5. 以下のコマンドを実行して、インスタンスを再起動します。

```
reboot
```

6. 以下のコマンドを実行して、変更したか確認します。

```
cat /proc/cmdline
```

結果に追加したパラメータが含まれていれば、追加完了です。




## OpenCloudOS 9

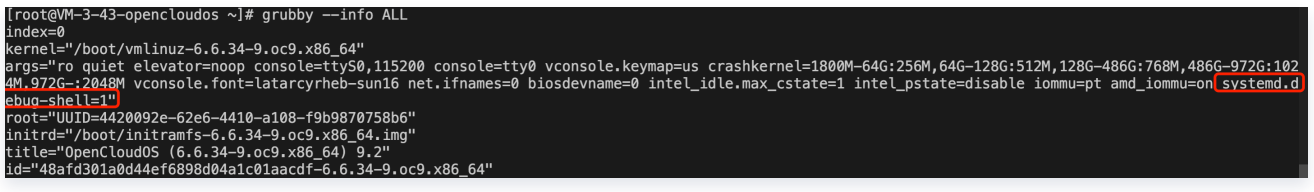
1. 以下のコマンドを実行して、カーネルパラメータを追加します。

```
grubby --update-kernel=ALL --args="systemd.debug-shell=1"
```

2. 以下のコマンドを実行して、追加したか検証します。

```
grubby --info ALL
```

以下の図のように追加したパラメータが表示されれば、追加完了です。




3. 以下のコマンドを実行して、インスタンスを再起動します。

```
reboot
```

4. 以下のコマンドを実行して、変更したか確認します。

```
cat /proc/cmdline
```

結果に追加したパラメータが含まれていれば、追加完了です。

```
[root@VM-3-43-opencloudos ~]# cat /proc/cmdline
BOOT_IMAGE=(hd0,msdos1)/boot/vmlinuz-6.6.34-9.oc9.x86_64 root=UUID=4420092e-62e6-4410-a108-f9b9870758b6 ro quiet elevator=noop console=ttyS0,115200 con
sole=tty0 vconsole.keymap=us crashkernel=1800M-64G:256M,64G-128G:512M,128G-486G:768M,486G-972G:1024M,972G-:2048M vconsole.font=latarcyrheb-sun16 net.if
names=0 biosdevname=0 intel_idle.max_cstate=1 intel_pstate=disable iommu=pt amd_iommu=on systemd.debug-shell=1
```

## TencentOS Server 3.X/TencentOS Server 4.X

1. 以下のコマンドを実行して、カーネルパラメータを追加します。

```
grubby --update-kernel=ALL --args="systemd.debug-shell=1"
```

2. 以下のコマンドを実行して、追加したか検証します。

```
grubby --info ALL
```

以下の図のように追加したパラメータが表示されれば、追加完了です。

```
[root@VM-1-43-tencentos ~]# grubby --info ALL
index=0
kernel="/boot/vmlinuz-5.4.119-19.0009.44"
args="ro quiet elevator=noop console=ttyS0,115200 console=tty0 vconsole.keymap=us crashkernel=1800M-64G:256M,64G-128G:512M,128G-486G:768M,486G-972G:102
4M,972G-:2048M vconsole.font=latarcyrheb-sun16 net.ifnames=0 biosdevname=0 intel_idle.max_cstate=1 intel_pstate=disable iommu=pt amd_iommu=on systemd.d
ebug-shell=1"
root="UUID=d00529a6-48bf-42cf-b76d-8209f3f6a1ee"
initrd="/boot/initramfs-5.4.119-19.0009.44.img"
title="TencentOS Server (5.4.119-19.0009.44) 3.1 (Final)"
id="134db59853e94d83aa743112d302ddff-5.4.119-19.0009.44"
index=1
```

3. 以下のコマンドを実行して、インスタンスを再起動します。

```
reboot
```

4. 以下のコマンドを実行して、変更したか確認します。

```
cat /proc/cmdline
```

結果に追加したパラメータが含まれていれば、追加完了です。

```
[root@VM-1-43-tencentos ~]# cat /proc/cmdline
BOOT_IMAGE=(hd0,msdos1)/boot/vmlinuz-5.4.119-19.0009.44 root=UUID=d00529a6-48bf-42cf-b76d-8209f3f6a1ee ro quiet elevator=noop console=ttyS0,115200 cons
ole=tty0 vconsole.keymap=us crashkernel=1800M-64G:256M,64G-128G:512M,128G-486G:768M,486G-972G:1024M,972G-:2048M vconsole.font=latarcyrheb-sun16 net.ifn
ames=0 biosdevname=0 intel_idle.max_cstate=1 intel_pstate=disable iommu=pt amd_iommu=on systemd.debug-shell=1
[root@VM-1-43-tencentos ~]#
```

# blscfg機能を無効にし、従来のカーネルパラメータ設定ファイルを読み込む

`/etc/default/grub` に `GRUB_ENABLE_BLSCFG=true` が設定されている場合、システムがgrub blscfg機能を使用していることを意味します。blscfg機能を無効にし、従来のカーネルパラメータ設定ファイルを使用してパラメータを追加したい場合は、`/etc/default/grub` に `GRUB_ENABLE_BLSCFG=false` と設定する必要があります。

## 操作手順

説明:

- この方法は、TencentOS Server 3.1, TencentOS Server 3.2など、比較的新しいRHEL系のディストリビューションに適用されます。
- この方法は、CentOS 7と同様の従来のgrub方式を引き続き使用し、デフォルトで `/etc/default/grub` の設定パラメータを読み込みます。

### TencentOS Server 3.X/TencentOS Server 4.X

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

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

2. iキーを押して編集モードに切り替え、`GRUB_CMDLINE_LINUX` の行を見つけます。`GRUB_CMDLINE_LINUX` の末尾に `“name=value”` の形式でカーネルパラメータを追加します。例：今回追加するカーネルパラメータは `systemd.debug-shell=1` です。


3. Escキーを押し、:wqと入力して、ファイルを保存し終了します。
4. 以下のコマンドを実行して、blscfg機能を無効にします。

```
sed -i "s/GRUB_ENABLE_BLSCFG=true/GRUB_ENABLE_BLSCFG=false/g"
/etc/default/grub
```

5. 以下のコマンドを実行して、Kernelの設定を再生成します。

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

6. 以下のコマンドを実行して、インスタンスを再起動します。

```
reboot
```

7. 以下のコマンドを実行して、変更したか確認します。

```
cat /proc/cmdline
```

結果に追加したパラメータが含まれていれば、追加完了です。