Elastic Compute Service (ECS)

ユーザガイド

ユーザガイド

概要

クイックリファレンス

この記事では、ECS 管理コンソールで ECS を使用する際に参照できるクイックリファレンスを示します。

必読: ECS 操作説明書

- ECSを使用する際の考慮事項

インスタンスへのログイン

Linux インスタンスへのログイン

SSHキーペアでインスタンスにのログイン

Windows インスタンスへのログイン

インスタンスのログインパスワード (マネジメントターミナルのパスワードではなく) を忘れた場合は、インスタンスのパスワードのリセットを実行してください。

ディスクの操作

- クラウドディスク購入後のデータディスクのアタッチ方法

オペレーティングシステムの変更

以下のような システムディスクの変更 が可能です：

Windows から Linux へ、Linux から Windows への変更。

既存バージョンから別のバージョンへ、たとえば、Windows Server 2008 から Windows Server 2012 への変更。

イメージの変更。たとえば、カスタムイメージまたは共有イメージへの変更。

イメージとスナップショットの使用

異なるリージョンを跨る イメージのコピー 。

構成やアプリケーションの自動更新ポリシーを作成する場合、自動スナップショットポリシーの作成 。

イントラネット通信を有効にする

- セキュリティグループを使用してイントラネット通信を有効にする方法 。

上記の質問に対する回答は、左側のナビゲーションペインで対応するノードをクリックしてください。

ECS を使用する際の考慮事項

ECS インスタンスを適切に実行するために、使用する前に以下の考慮事項をすべてお読みください。

禁止

アリババクラウドは以下を禁止しています。

- フロースルーサービスにインスタンスを使用する。違反があれば、インスタンスのシャットダウンやロックアウト、サービスの終了まで処罰されます。
- SELinuxを有効にする。
- ハードウェア関連のドライバをアンインストールする。
- ネットワークアダプタのMACアドレスを任意に変更します。

一般的なオペレーティングシステムに関する考慮事項

- 4GB以上のRAMを搭載したECSの場合、32ビットOSが最大4GBのRAMをサポートするため、64ビットOSを使用することをお勧めします。現在利用可能な64ビットシステムは次のとおりです。
    - Aliyun Linux
    - CoreOS
    - CentOS
    - Debian
    - FreeBSD
    - OpenSUSE
    - SUSE Linux
    - Ubuntu
    - Windows
- 32ビットWindows OSは、最大4コアのCPUをサポートします。
- WindowsインスタンスでWebサイトを構築するにはメモリが2GB以上必要です。また、1 vCPUでメモリ 1GBの構成は、MySQLサービスを起動することができません。
- サービスの継続性を確保し、サービスのダウンタイムを回避するには、OSの起動時にサービスアプリケーションの自動起動を有効にします。
- I / Oに最適化されたインスタンスの場合は、 **aliyun-service** プロセスを停止しないでください。
- カーネルやOSの更新は控えてください。

Linuxの制限事項

安定しシステムを稼働させるために、以下を**実行しない**でください：

- デフォルトの /etc/issueファイルの内容を変更します。このファイルを変更すると、管理コンソールボタンが使用できなくなります。
- /etc、/sbin、 /bin、/boot、 /dev、/usr、 /libなどのディレクトリのパーミッションを変更します。不適切なアクセス許可の変更によりエラーが発生する可能性があります。
- Linux **ルート**アカウントの名前を変更、削除、または無効にする。
- Linuxカーネルで他の操作をコンパイルまたは実行します。
- **NetWorkManager** サービスを有効にします。このサービスは、システムの内部ネットワークサービスと競合し、ネットワークエラーを引き起こします。

Windowsの制限事項

- 組み込みの **shutdownmon.exe** プロセスを閉じないでください。これにより、Windowsサーバーの再起動が遅れることがあります。
- **Administrator** アカウントの名前を変更、削除、または無効にしないでください。
- 仮想メモリの使用はお勧めしません。

ECS API 製品と使用制限

特に別段の指定がない限り、下記表に記載されているすべてのリソース制限は一つのリージョンとなります。

項目	一般的なユーザーに対する制約	例外適用方法
ECS リソースの作成に関するユーザー制約	現時点ではありません	
ユーザーがインスタンスを作成できるゾーン数	1 オンラインゾーン	チケットにてお問い合わせください
ユーザーがディスクを作成できるゾーン数	ユーザーがインスタンスを作成できるゾーン数とユーザーがインスタンスを持っているゾーン数を加算して、重複分を差し引いた数	上位設定はありません
ユーザーのデフォルトの従量課金インスタンスタイプ	ecs.t1.small (1 コア 1G)	チケットにてお問い合わせください
	ecs.s1.small (1 コア 2G)	
	ecs.s1.medium (1 コア 4G)	
	ecs.s2.small (2 コア 2G)	
	ecs.s2.large (2 コア 4G)	
	ecs.s2.xlarge (2 コア 8G)	
	ecs.s3.medium (4 コア 4G)	
	ecs.s3.large (4 コア 8G)	
	ecs.m1.medium (4 コア 16G)	
すべてのリージョンでユーザーのデフォルトの従量課金インスタンスクォータ	10	チケットにてお問い合わせください
単一インスタンスに対するディスククォータ	17個のシステムディスクと16個のデータディスク	上位設定はありません
従量課金のエフェメラルディスクのサポート	サポートされています	チケットにてお問い合わせください
単一のエフェメラルディスクの容量	20～1,024 GB	上位設定はありません
単一インスタンスに対するエフェメラルディスクの合計サイズ	2,048 GB	上位設定はありません
スナップショット数	64	上位設定はありません
単一の汎用クラウドディスクの容量	5～2,000 GB	上位設定はありません

ユーザーが利用できるシステムイメージのリスト	公式 Web サイトで販売されているイメージのリスト (現在 10 イメージ)	チケットにてお問い合わせください
エラスティックネットワークインターフェイス（ENI）の数	100	上位設定はありません
一つのカスタムイメージを共有可能なアカウント数	50	チケットにてお問い合わせください
インターネットアクセス用のインバウンド帯域幅	最大 200 Mbps	上位設定はありません
インターネットアクセス用のアウトバウンド帯域幅	最大 200 Mbps	上位設定はありません
単一セキュリティグループで許容されるインスタンス数	1000	上位設定はありません
単一セキュリティグループに対する権限付与ルール数	100	上位設定はありません
ユーザーのセキュリティグループクォータ	100	チケットにてお問い合わせください
単一インスタンスが所属できるセキュリティグループの最大数	5	上位設定はありません
イメージおよびインスタンスタイプに関する制約	メモリが 4 GB 以上のインスタンスでは 32 ビットイメージを使用できません	例外がありません
システムディスクとデータディスクの間の関係	システムディスクがクラウドディスクの場合、すべてのデータディスクをクラウドディスクにする必要があります	上位設定はありません
購入可能な従量課金クラウドディスクの合計数	ECS インスタンスクォータ * 5	チケットにてお問い合わせください
汎用クラウドディスクの容量	5 ~ 2,000 GB	上位設定はありません
従量課金クラウドディスクの作成に関するユーザー制約	ユーザーは実名認証に合格する必要があります (購入の場合のみ)	
システムディスクのアタッチポイントの範囲	/dev/xvda	上位設定はありません
データディスクのアタッチポイントの範囲	/dev/xvd[b-z]	上位設定はありません
単一ユーザーに対する EIP 数	20	チケットにてお問い合わせください
EIP の利用可能な帯域幅	0 ~ 200 Mbps	チケットにてお問い合わせください
単一ユーザーに対する VPC 数	5	チケットにてお問い合わせください
VPC のオプション CIDR 範囲	192.168.0.0/16、172.16.0.0/12、およびこれら	チケットにてお問い合わせください

	のサブネット	
単一 VPC に対する VSwitch 数	24	上位設定はありません
RouteTable あたりの RouteEntry 数	48	チケットにてお問い合わせください
単一の SSD クラウドディスクの容量	20～2,048 GB	上位設定はありません
単一の Ultra クラウドディスクの容量	20～2,048 GB	上位設定はありません
単一のエフェメラル SSD の容量	5~800 GB	上位設定はありません
インスタンスに対するエフェメラル SSD の合計容量	1,024 GB	上位設定はありません

上記の表に記載されている以外にも、ECSはサポートしていません。

- サウンドカードアプリケーション。
- ハードウェアドングル、USBドライブ、外部ハードドライブ、および銀行が発行するUSBセキュリティキーなどの外部ハードウェアデバイスのインストール。
- SNATおよびその他のIPパケットアドレス変換サービス。これを実現するには、外部VPNまたはプロキシを使用します。
- マルチキャストプロトコル。マルチキャストサービスが必要な場合は、ユニキャストポイントツーポイント方式を推奨します。
- VMwareを使用する場合など、仮想アプリケーションのインストールまたはそれに続く仮想化。

VPCの制限については、* VPC製品紹介の制限事項を参照してください。

インスタンスへのログイン

Management Terminal (VNC) を使用した ECS インスタンスへの接続

Management Terminal (別名 **VNC**) は、他のリモート接続ツール (Putty、Xshell、SecureCRT など) が利用できないときに、ECS インスタンス (Linux または Windows) に遠隔接続できる便利なツールです。ツールに習熟すると、問題解決にも手軽に利用することができます。

シナリオ

帯域幅を購入したかどうかにかかわらず、**Management Terminal** から ECS インスタンスに接続することができます。**Management Terminal** はほかにも、以下のシナリオをはじめ、さまざまなケースに適用できます。

ECS インスタンスの起動速度が遅いときに、進行を確認する場合 (例: セルフチェックが起動した場合)

ECS インスタンスでのソフトウェア設定エラーが原因で、リモート接続 (Putty など) に失敗し、ファイアウォールを再設定する場合 (例: 誤操作によりファイアウォールが有効化されている場合)

アプリケーションによる CPU や帯域幅の使用率が高く、リモート接続が妨げられているときに、ECS インスタンスに接続して異常なプロセスを終了させる場合 (例: ボットネット攻撃によって CPU または帯域幅が完全に占有されている場合)

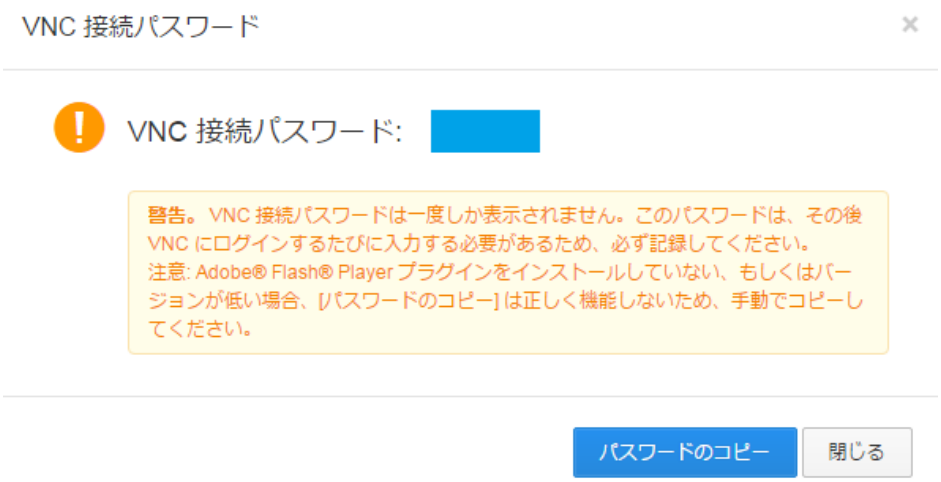
手順

[**ECS 管理コンソール**] にログインします。

接続する ECS インスタンスに移動し、右側の [**VNC**] をクリックします。

次の説明に従って、**Management Terminal** に接続します。

- **Management Terminal** に初めて接続する場合は、以下の手順に従います。
  a. 表示される [**VNC 接続パスワード**] ダイアログボックスにある、パスワードをコピーします。このダイアログボックスは一度しか表示されませんが、接続パスワードは **Management Terminal** への接続時に毎回要求されるため、**保存しておいてください。**



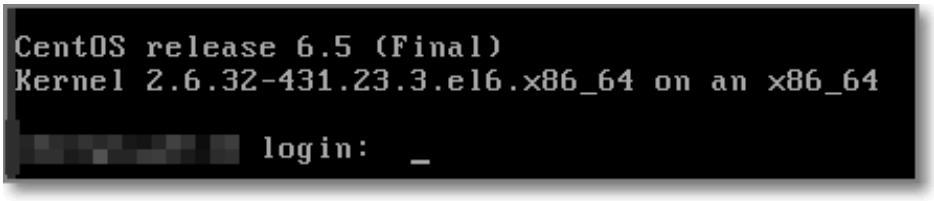
b. [**閉じる**] をクリックし、[**VNC 接続パスワード**] ダイアログボックスを閉じます。
c. 次に表示される [**VNC パスワードの入力**] ダイアログボックスで、コピーした接続パスワードを入力し、[**OK**] をクリックして **Management Terminal** に接続します。

- 過去に **Management Terminal** に接続したことがある場合は、[**VNC パスワードの入力**] ダイアログボックスが表示されます。接続パスワードを入力し、[**OK**] をクリックして **Management Terminal** に接続します。
- パスワードを忘れた場合は、次の手順に従って **Management Terminal** に接続します。
  a. **パスワードを変更**します。
  b. **Management Terminal** インターフェイスの左上にある [**リモートコマンドの送信**] をクリックし、[**管理端末への接続**] をクリックします。
  c. 表示される [**VNC パスワードの入力**] ダイアログボックスで、新しいパスワードを入力し、接続を終了します。

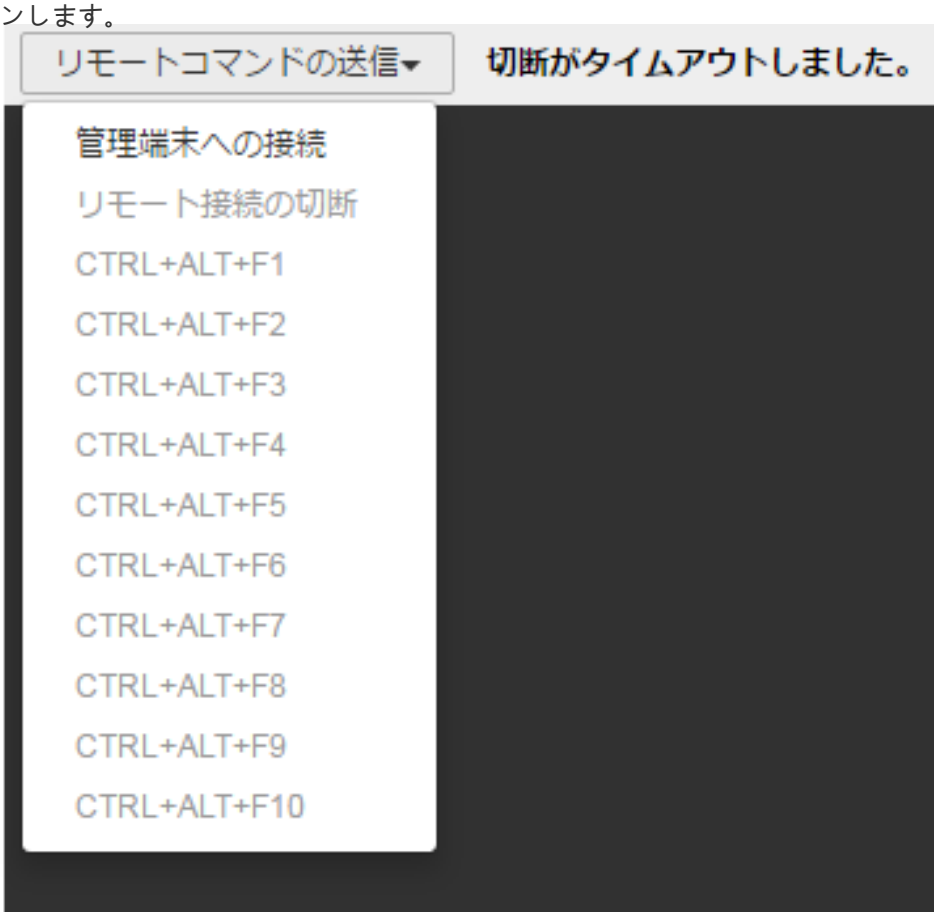
次の手順に従って、インスタンスに接続します。

Linux インスタンスには、ユーザー名（“root”）とパスワードを入力して接続します。
画面が真っ黒なままの場合は、Linux インスタンスがスリープモードになっています。マウスクリックするか、いずれかのキーを押すと、表示が変わります。
複数の Linux インスタンスを操作している場合は、[**リモートコマンドの送信**]、[

Ctrl+Alt+Fx] (“**Fx**“ は “**F1**“ から “**F10**“ までのいずれかのキー) の順にクリックし、管理端末を切り替えてください。



Windows インスタンスには、**Management Terminal** インターフェイスの左上にある [**リモートコマンドの送信**] をクリックし、[**Ctrl+Alt+Delete**] をクリックして、ログオン画面にアクセスします。ユーザー名 (“Administrator”) とパスワードを入力してログオンします。



パスワードの変更

[**VNC 接続パスワード**] ダイアログボックスに表示されるパスワードではなく、使い慣れたパスワードを使いたい場合、またはパスワードを忘れてしまった場合は、接続パスワードの変更が可能です。

注意: 変更後、新しい VNC 接続パスワードを有効にするにはインスタンスを再起動する必要があります。再起動するとインスタンスの動作が停止し、業務が中断されるので、 パスワードを変更する際はご注意くださ

い。

1. [**ECS 管理コンソール**]にログインします。
2. 接続する ECS インスタンスに移動し、右側の [**VNC**] をクリックします。
3. 表示される [**VNC 接続パスワード**] または [**VNC パスワードの入力**] ダイアログボックスを閉じ、**Management Terminal** インターフェイスの右上にある [**管理端末のパスワードの変更**] をクリックします。

4. 新しいパスワードを入力します。パスワードは、大文字、小文字、数字、またはそれらを組み合わせ、6 文字で構成してください。特殊文字は使用できません。
5. 管理コンソールで **インスタンスを再起動**し、新しいパスワードを有効にします。インスタンス内で再起動しても有効にはなりません。

よくある質問

Management Terminal は排他的ですか。
はい。1 人のユーザーの使用中に、他のユーザーが使用することはできません。

パスワードを変更したら、Management Terminal からログオンできなくなりました。なぜでしょうか。
(インスタンス内からではなく) 管理コンソールで**インスタンスを再起動**し、パスワードを有効にする必要があります。

ログオンした後、画面が真っ暗です。どのようにすればよいでしょうか。
真っ暗な画面は、インスタンスがスリープモードであることを示します。

- Linux インスタンスの場合は、いずれかのキーを押すと起動します。
- Windows インスタンスの場合は、リモートコマンド [**Ctrl+Alt+Delete**] を送信するとログオンインターフェイスに戻ります。

Management Terminal にアクセスできません。どのようにすればよいでしょうか。
Chrome を使用して管理コンソールにログオンし、**F12** を押して開発者ツールを開き、コンソール内の情報を確認して問題を分析してください。

IE8.0 または Firefox を使用していますが、Management Terminal を開くことができないのはなぜですか。
IE は 10 以降のみをサポートしています。Firefox の一部のバージョンはサポートしていません。この問題を解決するには、最新の IE バージョンをダウンロードするか、代わりに Chrome を使用してください。Chrome は、より適切に管理コンソールをサポートしています。}

SSH キーペア使用のインスタンスログイン

キーペアを使用してLinuxインスタンスにログオンする方法は、ローカルオペレーティングシステムによって異なります。

- Windows の場合
- Linux または SSH コマンド対応する OS

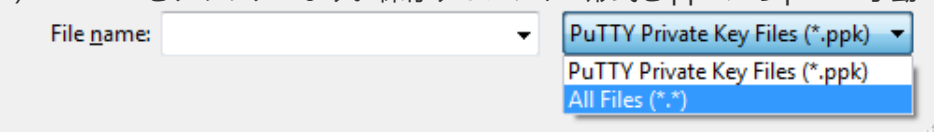
Windows の場合

本セクションでは、一般的なSSHツールのPuTTYとPuTTYgenを例として、WindowsシステムからLinuxインスタンスにログオンするためにキーペアを使用する方法を示します。

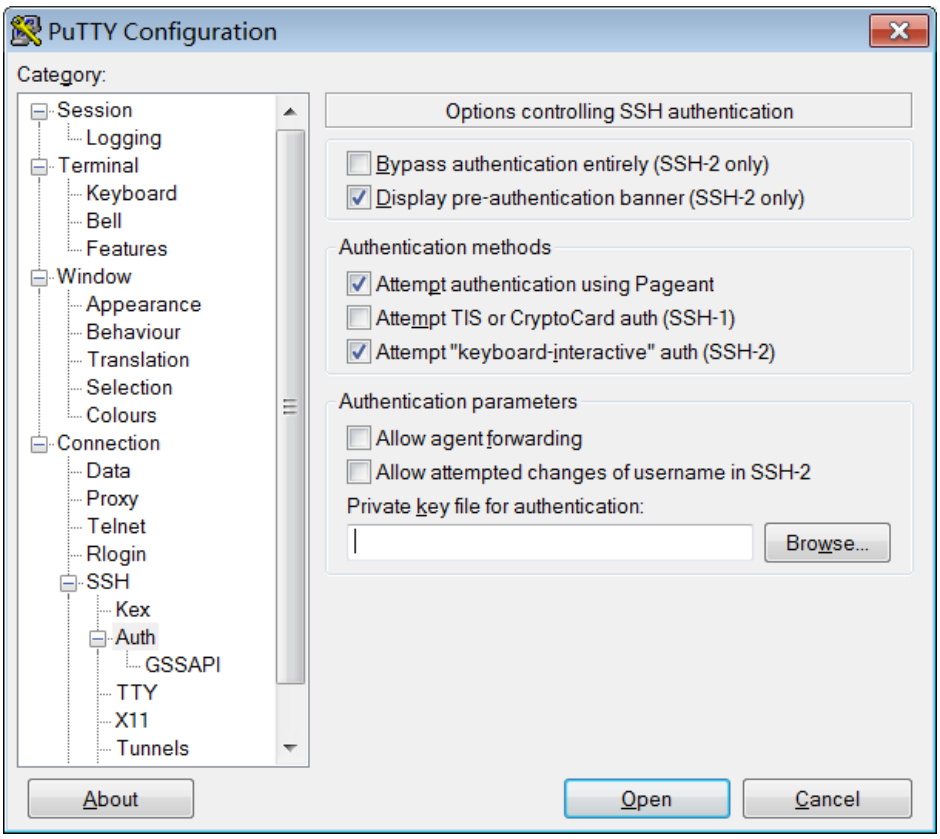
操作手順

1) 予めPuTTY と PuTTYgen をダウロードしインストールしておく必要があります。また、SSH キーペアが登録済みの Linux インスタンスを準備して置く必要もあります。
http://www.chiark.greenend.org.uk/~sgtatham/putty/
2) PuTTYgen を実行します。
3) Type of key to generate の下の、 SSH-2 RSA を選択します。

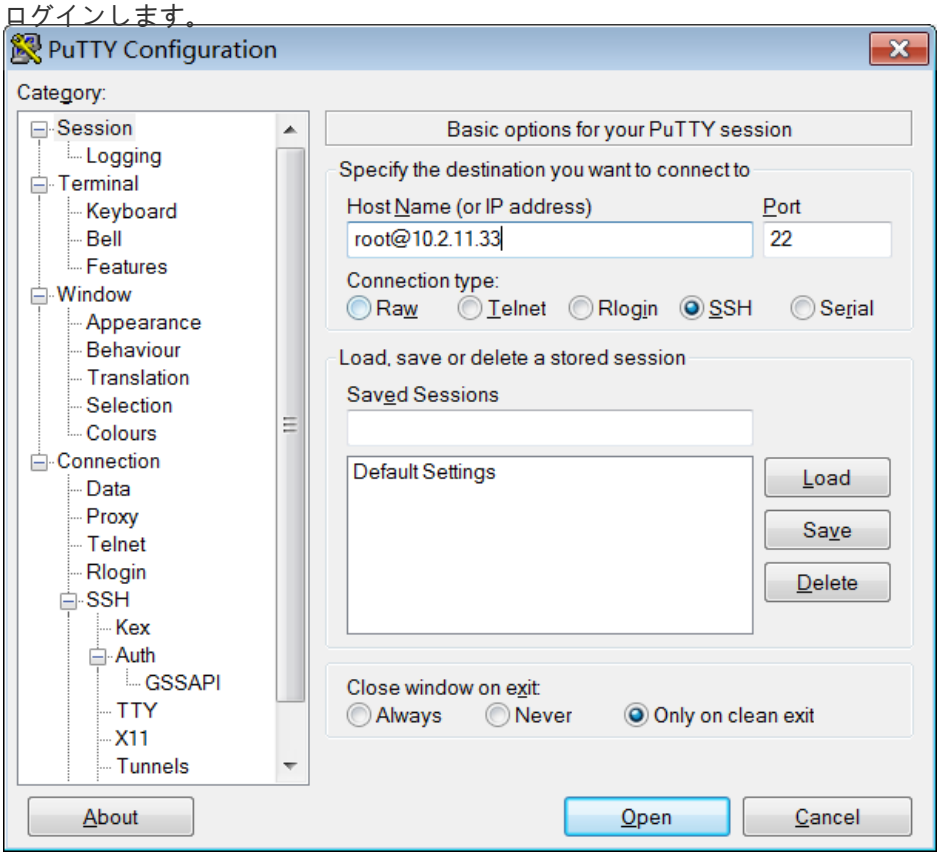
4) “Load” をクリックします。保存するファイル形式を.ppk から.pemへ手動で変更をしてください。



5) ” Open” をクリックし、既存の秘密鍵を選択し、” OK” をクリックします。
6) ” Save private key” による秘密鍵を保存します。警告のメッセージが表示後、” Yes” をクリックします。
7) 秘密鍵の名前を指定します。(.ppk という拡張子が自動的に追加されます。)
8) Putty Client を実行します。
9) “Connection” -> “SSH” -> “Auth” の順で選択し、 “Browse...” をクリックし、作成された .ppk ファイルを選択します。



10) “Session” をクリックし、“Host Name” を入力します。” open” をクリックしてインスタンスにログインします。



Linux または SSH コマンド対応する OS

ここではSShコマンドをサポートしているLinuxインスタンスや他のシステム(例えばMobaXterm for Windowsなど)でのキーペアを使用してのログイン方法を説明します。

必須要件

インスタンスに紐付けられたLinuxインスタンスが必要です。 詳しくは 「インスタンス作成時に SSH キーペアを使用する方法 」 または 「SSH キーペアのバインド/バインド解除方法」を参照してください。

操作手順

プライベートキーが保存してあるディレクトリーに移動します。 例えば, /root/xxx.pemなど。

xxx.pemのxxxはユーザご自身のプライベートキーに変更してください。

chmod コマンドでプライベートキーの属性を変更してください。: chmod 400 xxx.pem。

ssh コマンドでインスタンスに接続します。: ssh root@10.10.10.100 –i /root/xxx.pem。

上記例でIPアドレスは10.10.10.100となっていますが、ユーザご利用の環境にて適宜読み替えてください。

Linux インスタンスへのログイン

Linux インスタンスへのログイン

使用するローカル OS によって、ECS インスタンスへのリモートログインに用いるユーティリティは異なります。下表に、インスタンスへのリモートログインに用いるユーティリティを示します。

ローカル OS	インスタンスOS	ログイン方法			
		マネジメントターミナル	Putty	SSH コマンドライン	SSH Control Light
Linux	Linux			√	

Windows		√	√		
Mac		√		√	
iPhone					√
Android スマートフォン					√

Windows からのログイン

ECS インスタンスの作成後に、以下の方法のいずれかでインスタンスにログインします。

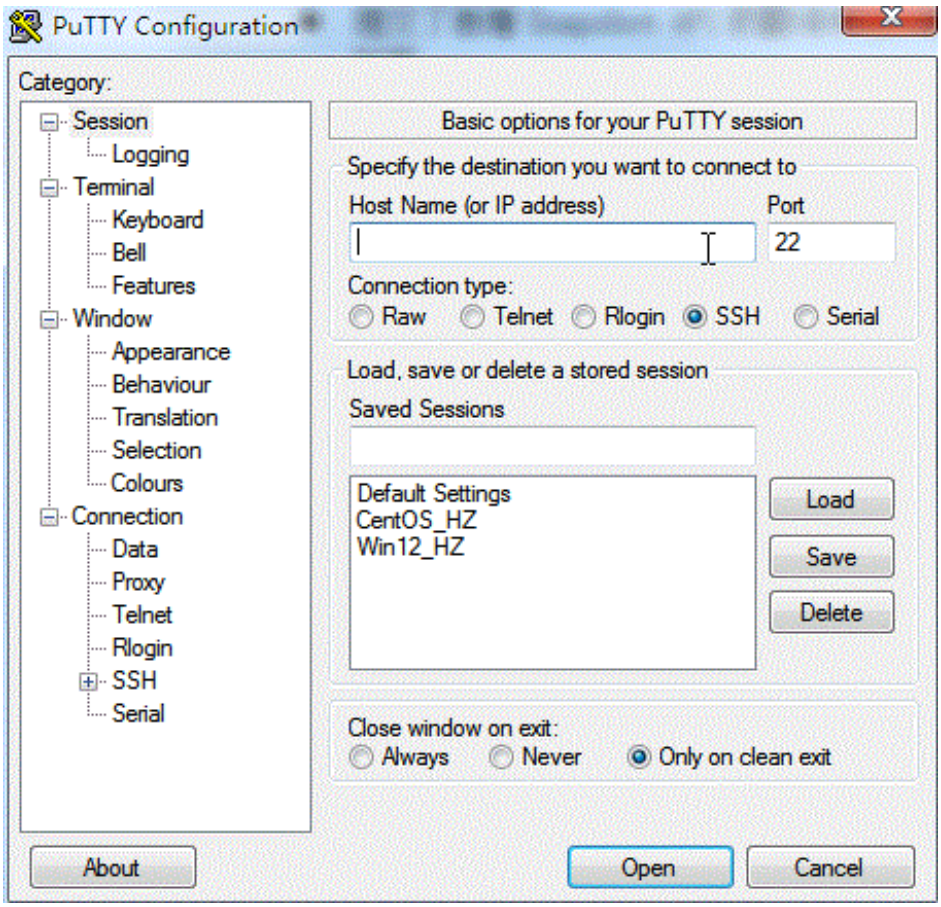
- **リモートログインソフトウェア** (Putty など): この方法を使用する前に、インターネットから対象のインスタンスにアクセスできることを確認してください。ただし、インスタンスの作成時に帯域幅を購入していない場合は、このリモートデスクトップ接続方法を利用できません。代わりにマネジメントターミナルを使用できます。
- **マネジメントターミナル**: 帯域幅を購入したかどうかにかかわらず、管理コンソールの [**マネジメントターミナル**] からインスタンスにログインできます。

リモート接続アプリケーションの使用

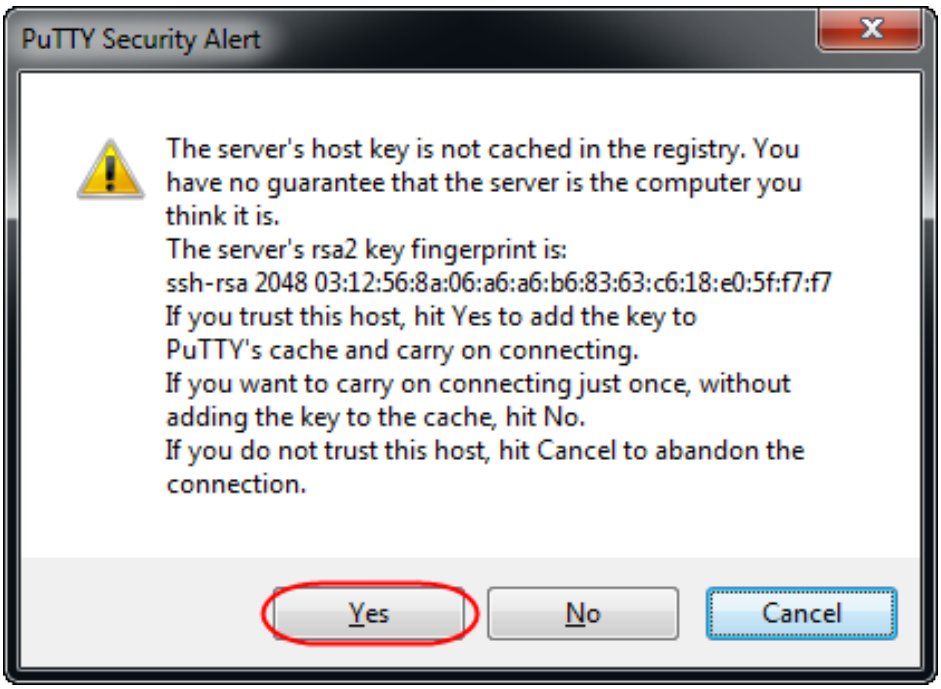
各種のリモート接続ユーティリティは、使用法がよく似ています。このドキュメントでは、Putty を例に、インスタンスへのリモートログイン方法を説明します。Putty は無料で使いやすいユーティリティです。http://www.putty.org/ でダウンロードすることができます。

1. Putty.exe を起動します。
2. インスタンスのパブリック IP アドレスを [**Host Name (or IP address)**] に入力します。
   - デフォルトポート **22** を使用します。
   - [**Connection Type**] で [**SSH**] を選択します。
   - [**Saved Sessions**] にセッション名を入力し、[**Save**] をクリックします。こうすることで、次回、IP アドレスを入力せずに直接セッションを読み込むことができます。

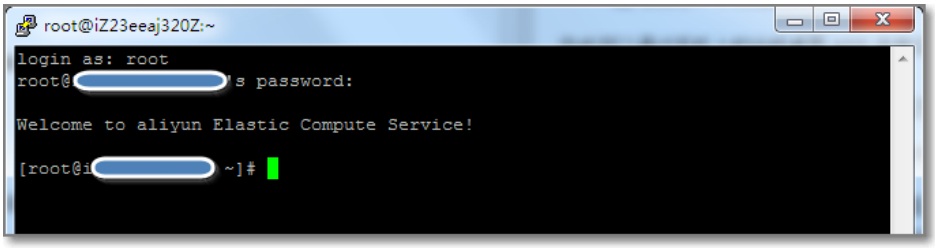
   [**Open**] をクリックして接続します。



初回接続時に、次のメッセージが表示されます。[**Yes**] をクリックします。



5. プロンプトに応じて、Linux ECS インスタンスのユーザー名とパスワードを入力します。パスワードは画面に表示されません。**Enter** キーを押します。



これでインスタンスに正常に接続され、操作を行うことができます。

マネジメントターミナルの使用

マネジメントターミナルは、他のリモート接続ツール (Putty、Xshell、SecureCRT など) が利用できないときに、インスタンスにログインするために使用できる便利なツールです。適切な技術力を持つユーザーにとって、手軽に問題解決に利用できるセルフサービスツールです。

シナリオ

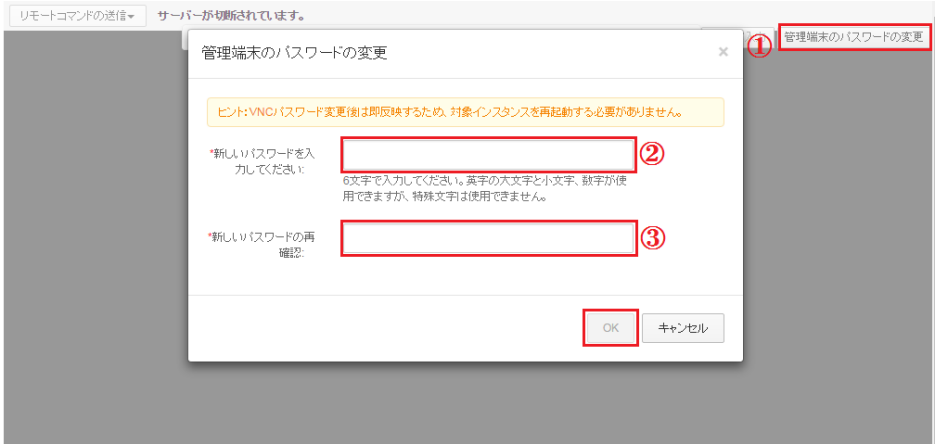
帯域幅を購入したかどうかにかかわらず、[**マネジメントターミナル**] からインスタンスにログインすることができます。マネジメントターミナルはほかにも、以下のシナリオをはじめ、さまざまなケースに適用できます。

- インスタンス起動速度が遅いときに、進行を確認する必要がある場合 (例: セルフチェックの実行時)。
- インスタンスでのソフトウェア設定エラーが原因で、リモート接続 (Putty など) に失敗し、ファイアウォールの再設定が必要な場合 (例: 誤操作によるファイアウォールの有効化)。
- アプリケーションによる CPU や帯域幅の使用率が高く、リモート接続が妨げられているために、インスタンスにログインして異常なプロセスを終了させる必要がある場合 (例: ボットネット攻撃に帰因するプロセスにより CPU または帯域幅が完全に占有されている場合)。

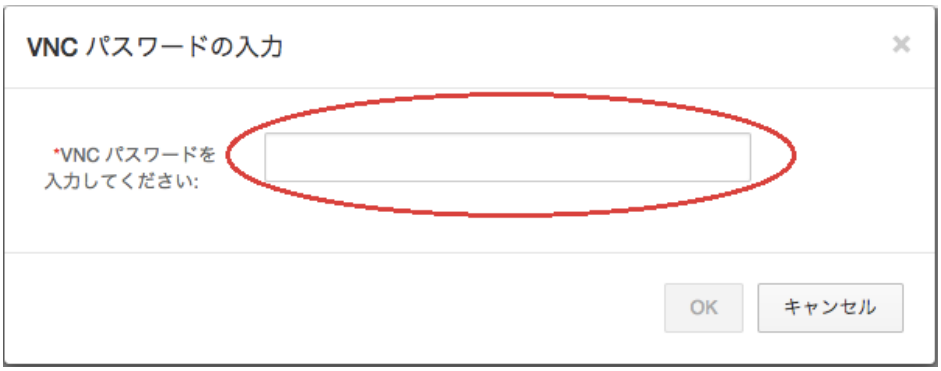
手順

1. ECS 管理コンソール にログインします。
2. 接続するインスタンスに移動します。
3. 右側で [**VNC**] をクリックします。

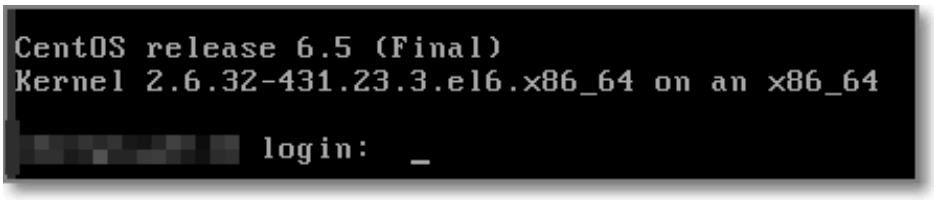
4. 初回のログイン時に、マネジメントターミナルのパスワードの入力が求められます。このプロンプトは 1 回のみ表示されます。マネジメントターミナルにログインする際は、毎回このパスワードを入力する必要があります。**パスワードは忘れないよう、メモしておきます。**
   パスワードを忘れた場合は、右上の [**管理端末のパスワードの変更**] をクリックします。



左上の [**リモートコマンドの送信**] をクリックし、[**管理端末への接続**] をクリックします。マネジメントターミナルパスワードを入力し、インスタンスに接続します。



ユーザー名とパスワードを入力して、ログインします。画面が真っ黒なままの場合は、Linux インスタンスがスリープモードになっています。マウスクリックするか、いずれかのキーを押すと、表示が変わります。



Linux または Mac OS X からのログイン

SSH コマンドを使用してインスタンスに直接接続します。例: ssh root@*インスタンスのパブリック IP アドレス*。次に、root ユーザーのパスワードを入力します。

モバイルアプリからのログイン

スマートフォンにインストールしたリモートデスクトップアプリからログインすることができます。たとえ

ば、iPhone ユーザーは App Store から **SSH Control Light** をダウンロードし、それを使用して Linux インスタンスにログインできます。

ログインパスワードを忘れた場合は、どうしたらよいですか

インスタンスのログインパスワード (マネジメントターミナルのパスワードではなく) を忘れた場合は、「パスワードのリセット」を参照してください。

Windows インスタンスへのログイン

使用するローカル OS によって、ECS インスタンスへのリモートログインに使用するユーティリティは異なります。下表に、インスタンスへのリモートログインに用いるユーティリティを示します。

ローカル OS	インスタンス OS	ログインユーティリティ			
		マネジメントターミナル	MSTSC	rdesktop	モバイル MSTSC アプリ
Linux	Windows			√	
Windows		√	√		
Mac		√	√		
iPhone					√
Android スマートフォン					√

Windows からのログイン

このセクションでは、ローカルの Windows OS から Windows インスタンスにログインする方法について説明します。

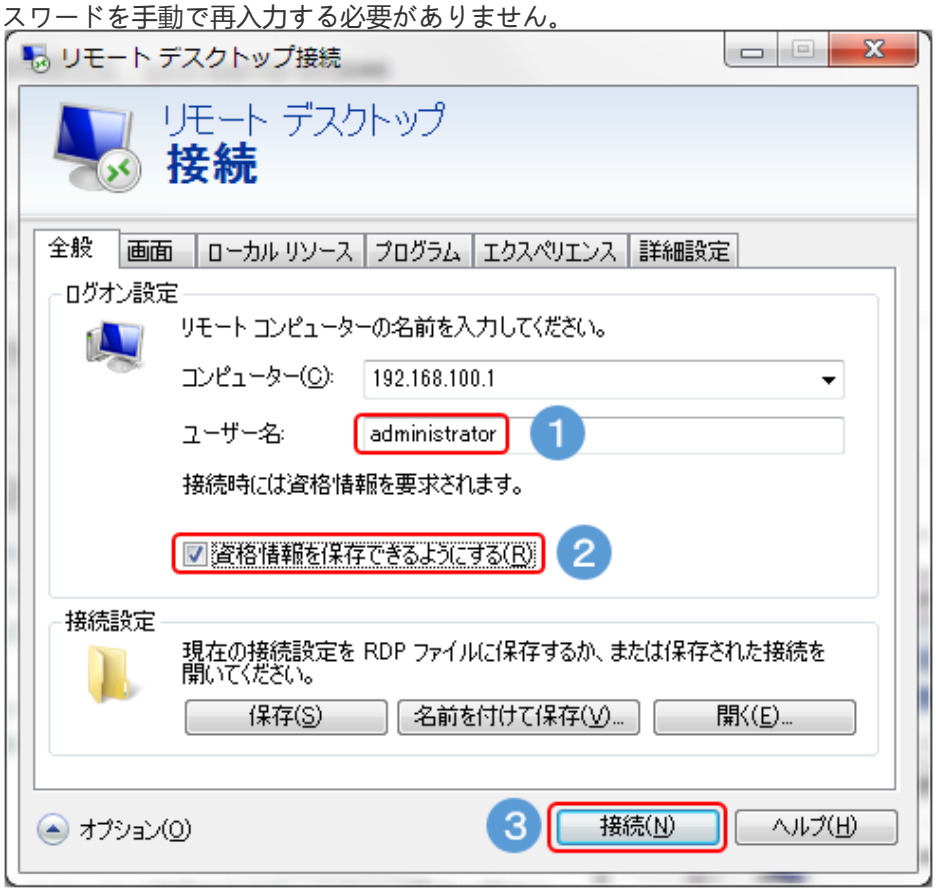
ECS インスタンスの作成後に、以下の方法のいずれかでサーバーにログインします。

- **Microsoft ターミナルサービスクライアント(MSTSC)**: この方法を使用する前に、インターネットから対象のインスタンスにアクセスできることを確認してください。ただし、インスタンスの作成時に帯域幅を購入していない場合は、このリモートデスクトップ接続方法を利用できません。
- **管理コンソールの マネジメントターミナル**: 帯域幅を購入したかどうかにかかわらず、管理コンソールの [**マネジメントターミナルに接続**] からインスタンスにログインできます。

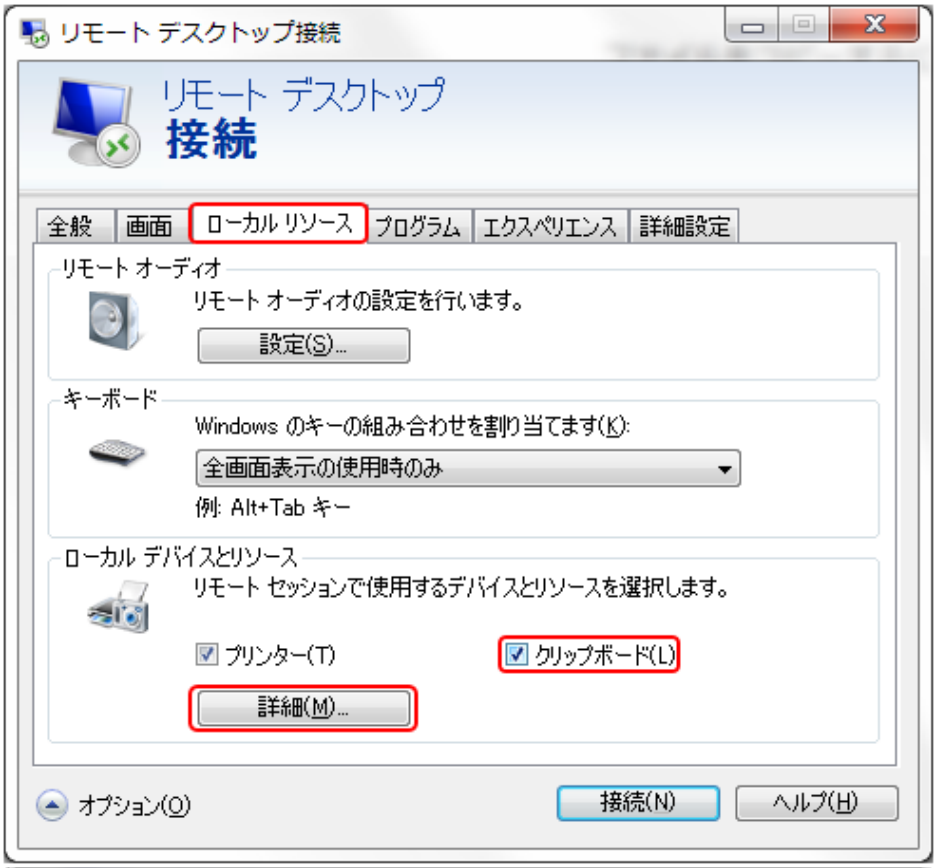
MSTSC の使用

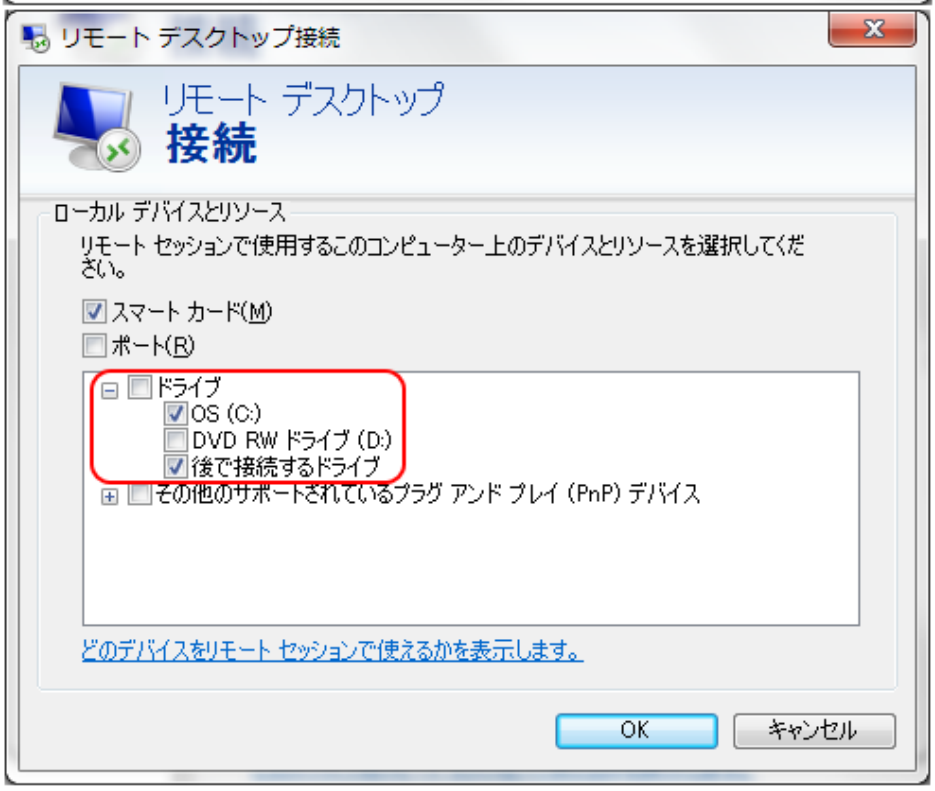
1. [**スタート**]、[**リモートデスクトップ接続**] の順に選択するか、[**スタート**]、[**検索**] の順に選択し「**mstsc**」と入力します。また、ショートカットキー **Win+R** で [ファイル名を指定して実行] ウィンドウを開き、「**mstsc**」と入力して Enter キーを押し、リモートデスクトップ接続を開始する方法もあります。
2. [**リモートデスクトップ接続**] ダイアログボックスに、インスタンスのパブリック IP アドレスを入力します。[**オプション**] をクリックします。

   ユーザー名を入力します。デフォルト値は **Administrator** です。[**資格情報を保存できるようにする**] をクリックします。次に [**接続**] をクリックします。この方法では、後でログインする際に、パスワードを手動で再入力する必要がありません。



ローカルファイルをインスタンスにコピーしやすくするために、MSTSC からローカルコンピューターリソースの共有を有効化できます。[**ローカルリソース**] タブをクリックします。通常は、[**クリップボード**] チェックボックスを選択する必要があります。ただし、[クリップボード] オプションを選択しても、インスタンスに直接コピーできるのはローカルテキストメッセージのみであり、ファイルはコピーできません。
ファイルをコピーするには、[**詳細**] をクリックし、[ドライブ] を選択して、ファイルを格納するディスクを指定します。





5. [**画面**] タブで、リモートデスクトップウィンドウのサイズを設定できます。通常は [**全画面表示**] に設定します。
6. [**OK**] をクリックし、[**接続**] をクリックします。

これでインスタンスに正常に接続され、操作を行うことができます。

マネジメントターミナルの使用

マネジメントターミナルは、他のリモート接続ツール (Putty、Xshell、SecureCRT など) が利用できないときに、インスタンスにログインするために使用できる便利なツールです。適切な技術力を持つユーザーにとって、手軽に問題解決に利用できるセルフサービスツールです。

シナリオ

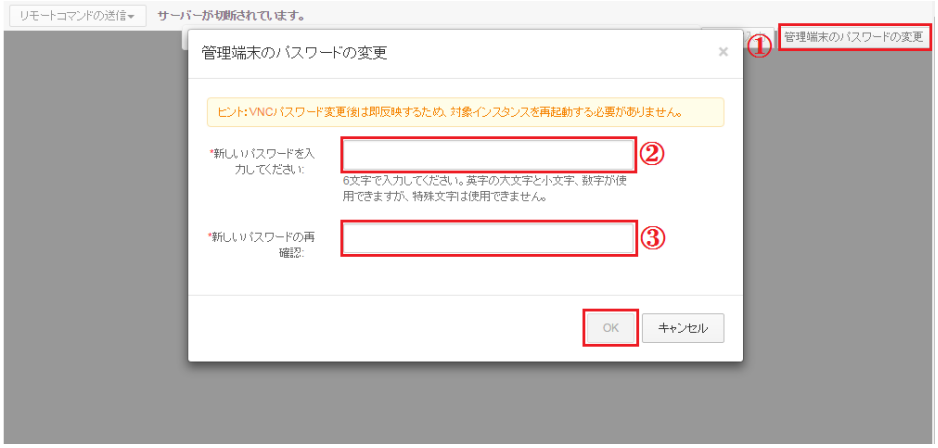
帯域幅を購入したかどうかにかかわらず、[**VNC**] からインスタンスにログインすることができます。VNCはほかにも、以下のシナリオをはじめ、さまざまなケースに適用できます。

- インスタンス起動速度が遅いときに、進行を確認する必要がある場合 (例: セルフチェックの実行時)。
- インスタンスでのソフトウェア設定エラーが原因で、リモート接続 (Putty など) に失敗し、ファイアウォールの再設定が必要な場合 (例: 誤操作によるファイアウォールの有効化)。
- アプリケーションによる CPU や帯域幅の使用率が高く、リモート接続が妨げられているために、インスタンスにログインして異常なプロセスを終了させる必要がある場合 (例: ボットネット攻撃に帰因するプロセスにより CPU または帯域幅が完全に占有されている場合)。

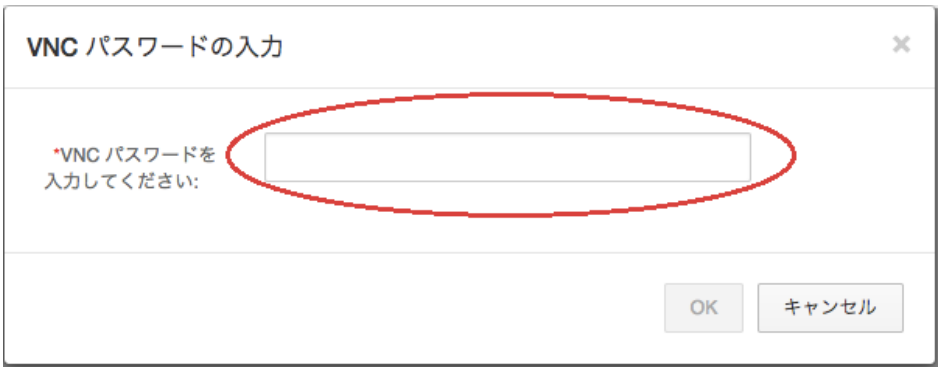
手順:

1. [ECS 管理コンソール] にログインします。
2. 接続するインスタンスに移動します。
3. 右側の[**VNC**]をクリックします。

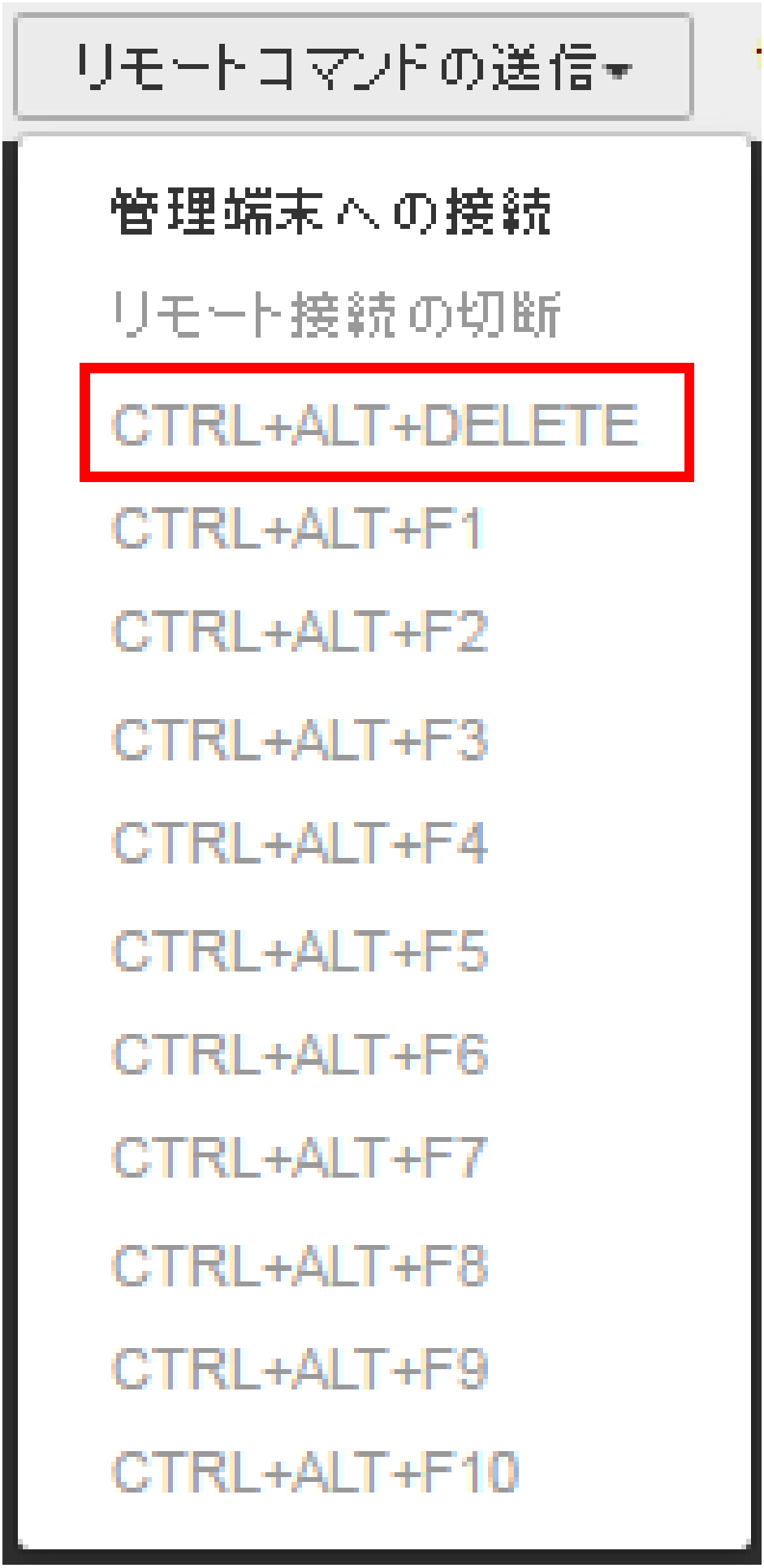
4. 初回のログイン時に、マネジメントターミナルのパスワードの入力が求められます。このプロンプトは 1 回のみ表示されます。マネジメントターミナルにログインする際は、毎回このパスワードを入力する必要があります。**パスワードは忘れないよう、メモしておきます。**
   パスワードを忘れた場合は、右上の [**管理端末のパスワードの変更**] をクリックします。



左上の [**リモートコマンドの送信**] をクリックし、[**管理端末への接続**] をクリックします。マネジメントターミナルパスワードを入力し、インスタンスに接続します。



マネジメントターミナルインターフェイスで、リモートコマンド **Ctrl+Alt+Delete** を送信します。Windows サーバーインスタンスへのログインインターフェイスが表示されます。ユーザー名とパスワードを入力して、ログインします。


リモートコマンドの送信
管理端末への接続
リモート接続の切断
CTRL+ALT+DELETE
CTRL+ALT+F1
CTRL+ALT+F2
CTRL+ALT+F3
CTRL+ALT+F4
CTRL+ALT+F5
CTRL+ALT+F6
CTRL+ALT+F7
CTRL+ALT+F8
CTRL+ALT+F9
CTRL+ALT+F10

Linux からのログイン

リモート接続ユーティリティで、リモートログインを実行することができます。帯域幅を購入していない場合は、インスタンスに接続する前に、管理コンソールにログインする必要があります。

リモート接続アプリケーションの使用

Linux システムから Windows インスタンスにリモートログインする場合は、互換性のあるリモートデスクトップ接続ユーティリティを使用する必要があります。rdesktop の使用をお勧めします。

rdesktop を起動して、次のコマンドを入力します (例中のパラメーター値は、実際のデータに置き換えてください)。

```
rdesktop -u administrator -p password -f -g 1024*720 192.168.1.1 -r clipboard:PRIMARYCLIPBOARD -r
disk:sunray=/home/yz16184
```

以下に引数の説明を示します。

- -u はユーザー名です。Windows インスタンスのデフォルトユーザー名は、administrator です。
- -p は Windows インスタンスのログインパスワードです。
- -f は全画面表示がデフォルトの表示であることを示します。全画面表示モードから切り替えるには、Ctrl + Alt + Enter キーを使用します。
- -g は解像度です。結合部の “*” が省略されている場合、デフォルト解像度は全画面表示です。
- 192.168.1.1 は該当する Windows インスタンスの IP アドレスに置き換えてください。
- -d はドメイン名です。たとえば INC ドメインであれば、このパラメーターは “-d inc” になります。
- -r はマルチメディアリダイレクトです。たとえば、サウンドを有効にするには、-r sound を使用し、ローカルサウンドカードを使用する場合は、-r sound : local を使用します。また、Udisk を有効にするには、-r disk:usb=/mnt/usbdevice を使用します。
- -r clipboard:PRIMARYCLIPBOARD: このパラメーターを使用すると、ローカル Linux システムとリモート Windows インスタンスとの間でテキストを直接コピーアンドペーストすることができます。漢字もサポートされます。
- -r disk:sunray=/home/yz16184: これは、ローカル Linux システム上の特定のディレクトリが Windows ハードディスクにマップされることを表します。これにより、Samba や FTP を介さずにファイルを転送できます。

マネジメントターミナルの使用

操作手順はローカル Windows OS の場合と同じです。

Mac OS X からのログイン

Mac OS X 用のリモートデスクトップ接続ユーティリティをダウンロードし、インストールしてください。.

モバイルアプリからのログイン

スマートフォンにインストールしたリモートデスクトップアプリからログインすることができます。たとえば、iPhone ユーザーは App Store から **Microsoft リモートデスクトップ**をダウンロードし、それを使用して Windows インスタンスにログインできます。

ログインパスワードを忘れた場合は、どうしたらよいですか。

インスタンスのログインパスワード (マネジメントターミナルのパスワードではなく) を忘れた場合は、「パスワードのリセット」を参照してください。

モバイルデバイス上からインスタンスへの接続

このドキュメントでは、モバイルデバイス上のECSインスタンスに接続する方法について説明します。手順は、インスタンスのオペレーティングシステムによって異なります。

> Linuxインスタンスへの接続：iOSデバイス上のLinuxインスタンスへの接続方法を記述する例としてSSH Control Liteを、JuiceSSHをAndroidデバイス上のLinuxインスタンスに接続する方法について説明しています。
>
> Windowsインスタンスに接続する：Microsoft Remote Desktopを例として、iOSまたはAndroidデバイス上のWindowsインスタンスに接続する方法を説明します。

Linuxインスタンスに接続する

前提条件

インスタンスに接続する前に、次の点を確認してください。

- インスタンスの状態は **Running** です。
- インスタンスにはパブリックIPアドレスがあり、パブリックネットワークからアクセスできます。
- インスタンスのログインパスワードを設定済みです。パスワードが失われた場合は、インスタンスパスワードをリセットする必要があります。
- インスタンスのセキュリティグループには、次のセキュリティグループルールがあります。

ネットワ	NIC	ルールの	承認ポリ	プロトコ	ポート範	認可タイ	権限オブ	優先

ークのタイプ		方向	シー	ルタイプ	囲	プ	ジェクト	
VPC	設定不要	インバウンド	許可する	SSH（22）	22/22	アドレスフィールドへのアクセス	0.0.0.0/0	1
クラシック	インターネット							

- 適切なアプリをダウンロードしてインストールしました：
  - iOSデバイスにはSSH Control Liteがインストール済みになっています。
  - Android搭載端末にはJuiceSSHがインストール済みになっています。

手順

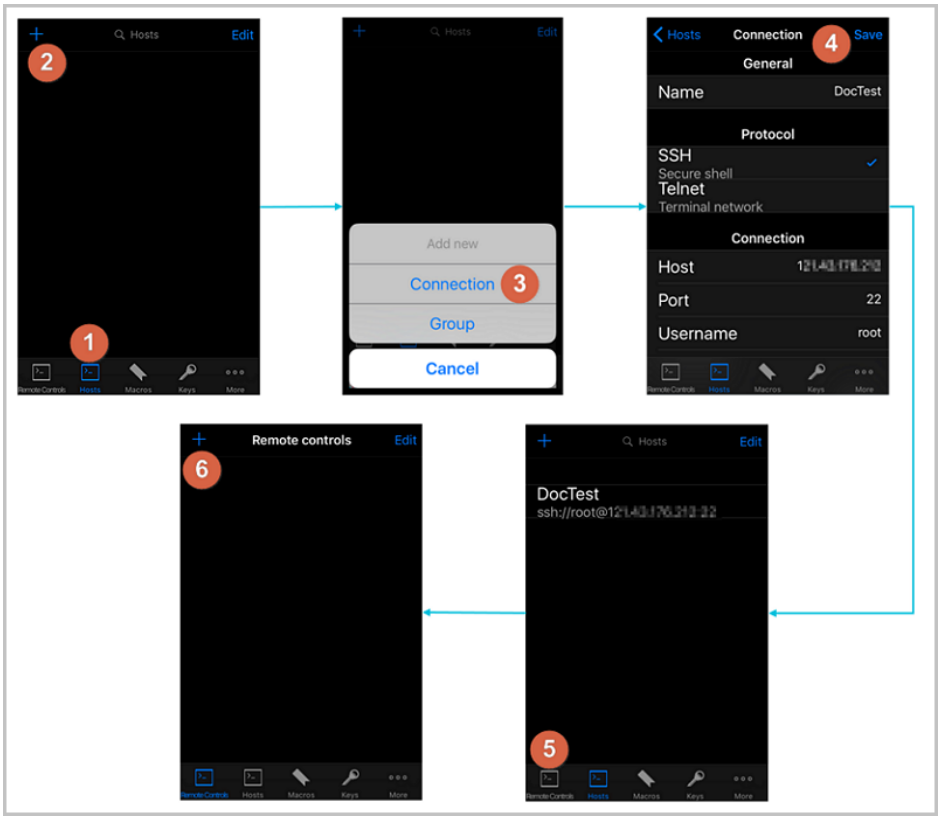
iOSデバイスについては、SSH Control Liteを使用したLinuxインスタンスへの接続を参照してください。この例では、ユーザー名とパスワードが認証に使用されます。

Androidデバイスの場合は、JuiceSSHを使用してLinuxインスタンスに接続を参照してください。この例では、ユーザー名とパスワードが認証に使用されます。

SSH Control Liteを使用してLinuxインスタンスに接続する

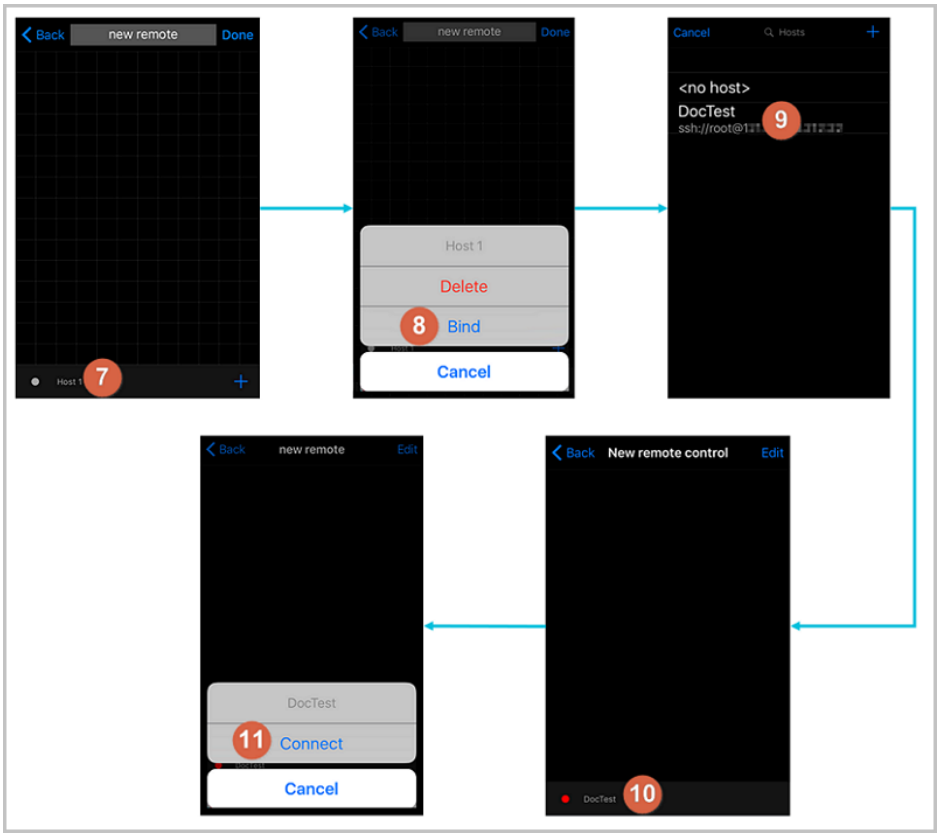
SSH Control Liteを使用してLinuxインスタンスに接続するには、次の手順を実行します。

1. **SSH Control Lite** を起動し、 **Hosts** をタップします。
2. **Hosts** ページの左上隅にある **+** アイコンをタップします。
3. アクションシートで、**Connection**をタップします。
4. **Connection**ページで、接続情報を設定し、**Save**をタップします。次の接続情報が必要です。
   - **Name**：ホスト名を指定します。 この例では、**DocTest**が使用されています。
   - **Protocol**：デフォルト値 **SSH** を使用してください。
   - **Host** ：接続するLinuxインスタンスのパブリックIPアドレスを入力します。
   - **Port**：SSHプロトコルのポート番号を入力します。**この例では22** が使用されています。
   - **Username**：ユーザー名は **root** と入力します。
   - **Password**：インスタンスのログオンパスワードを入力します。
5. ツールバーで、 **Remote Controls** をタップします。
6. **Remote Controls**ページで、左上隅の **+** アイコンをタップしてリモート接続セッションを作成します。 この例では、**New remote**が使用されています。
   次の図は、手順1～6を示しています。



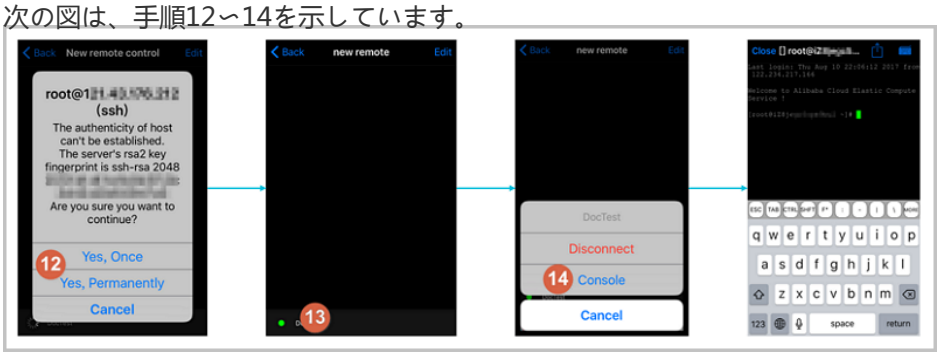
7. **New remote**ページで、 **Host1** をタップします。
8. アクションシートで、 **Bind** をタップします。
9. 新しいLinuxインスタンスを選択します。この例では、 *DocTest* を選択します。
10. **New Remote**ページで、**Done**をタップして**Edit**モードに切り替え、 **DocTest** をタップします。
11. アクションシートで、 **Connect** をタップします。

次の図は、手順7～11を示しています。



12. アクションシートで、**Yes, Once**または**Yes, Permanently**を選択します。接続が成功すると、**DocTest** の前のインジケータが緑色に変わります。
13. **New remote**ページで、 **DocTest** をタップします。
14. アクションシートで、 **Console** をタップしてLinuxインスタンスコンソールを開きます。

次の図は、手順12～14を示しています。

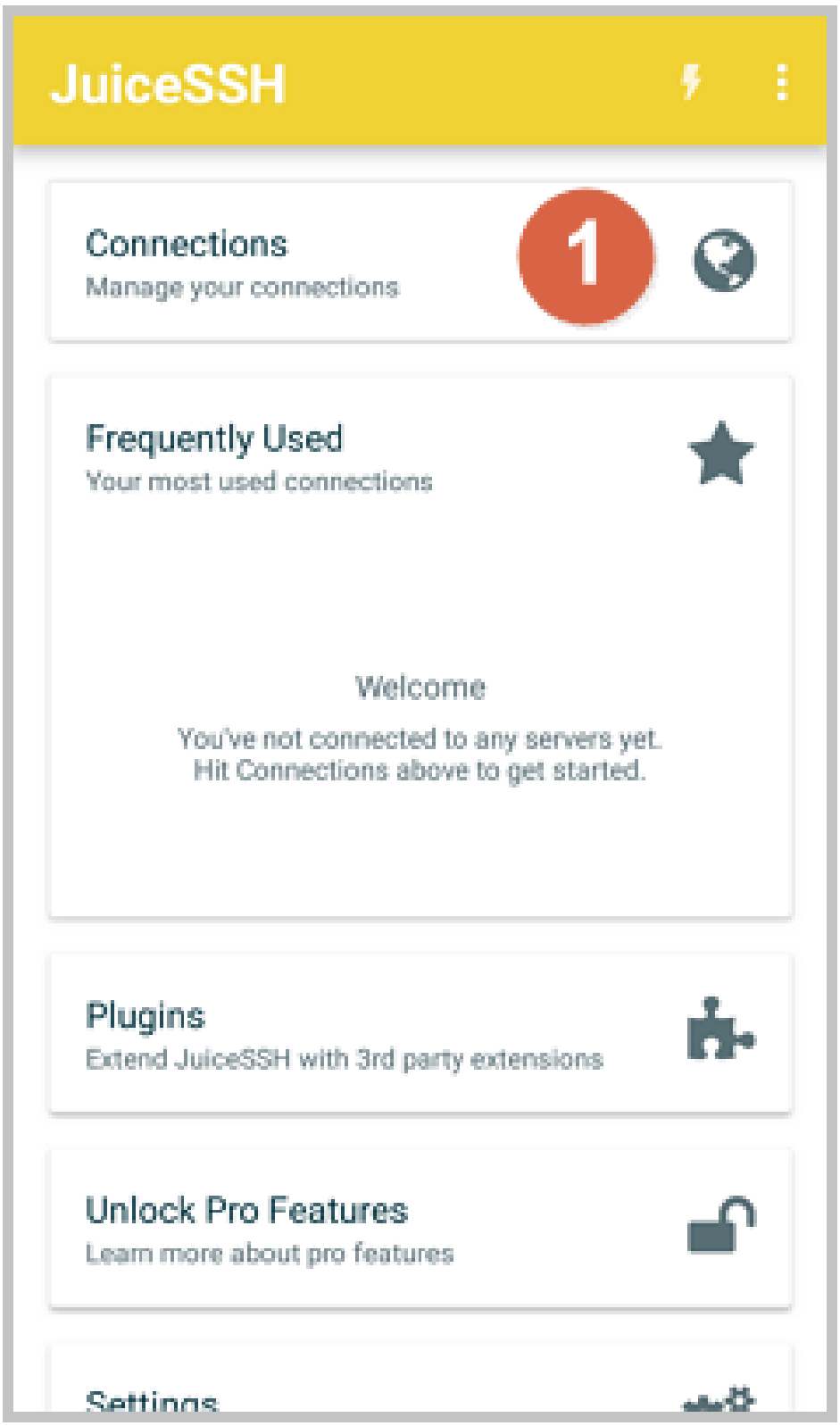


この手順で、Linuxインスタンスに接続可能です。

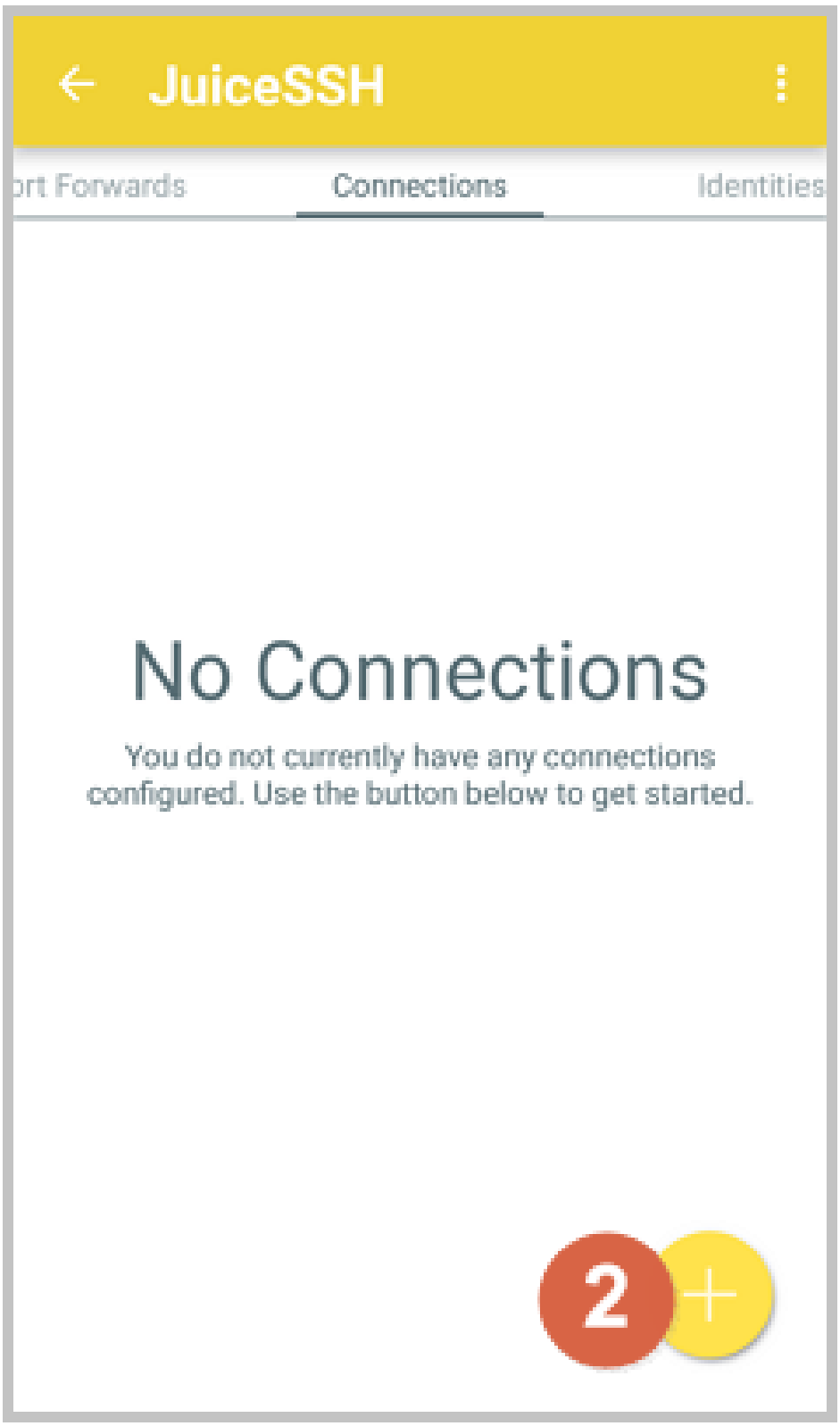
JuiceSSHを使用してLinuxインスタンスに接続する

JuiceSSHを使用してLinuxインスタンスに接続するには、次の手順を実行します。

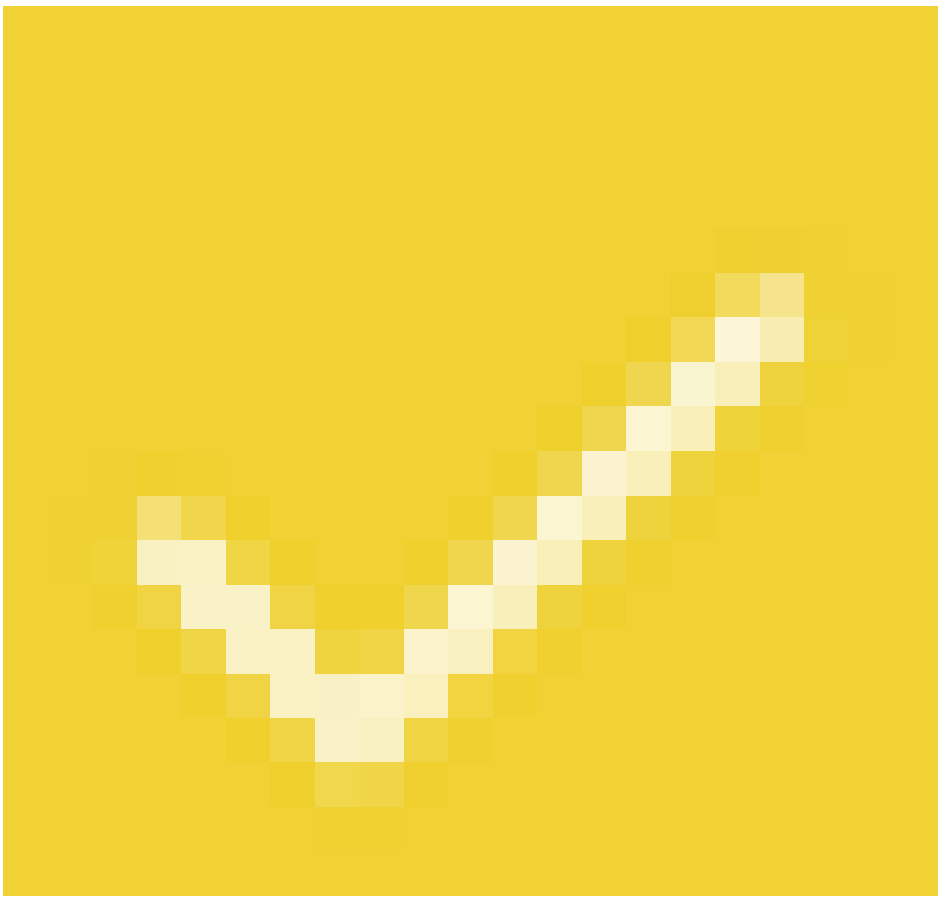
1. **JuiceSSH** を起動し、**Connections**をタップします。



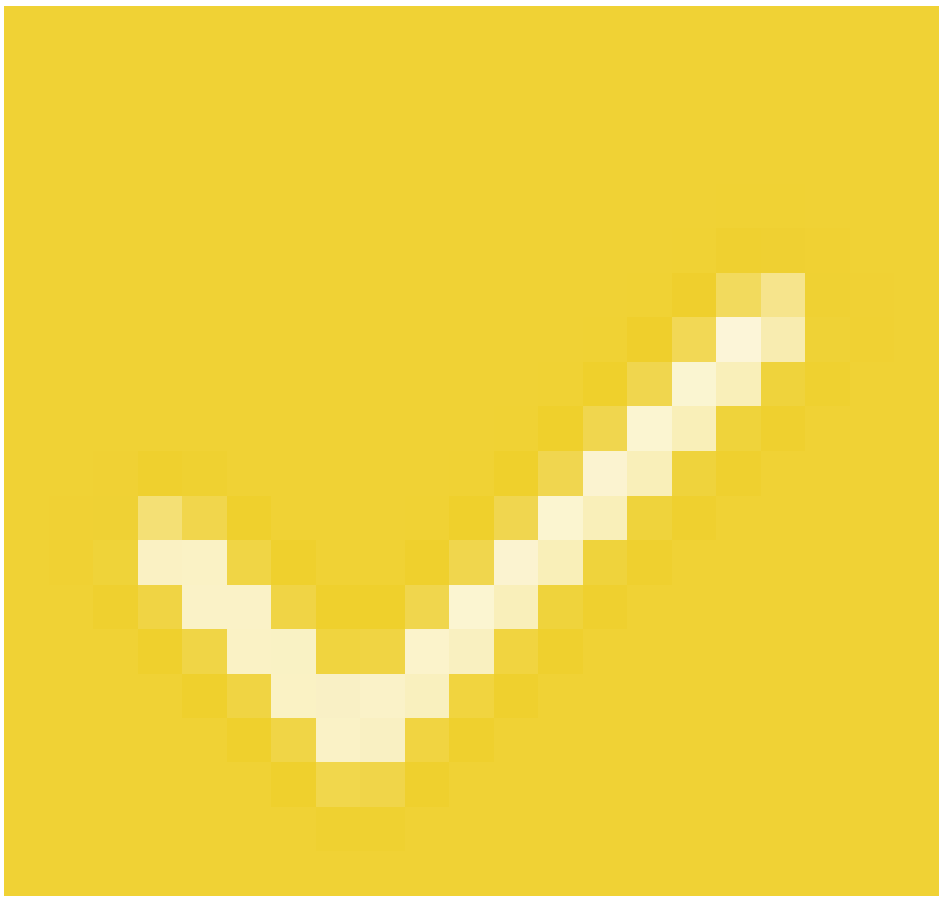
2. **Connections**タブで、 **+** アイコンをタップします。



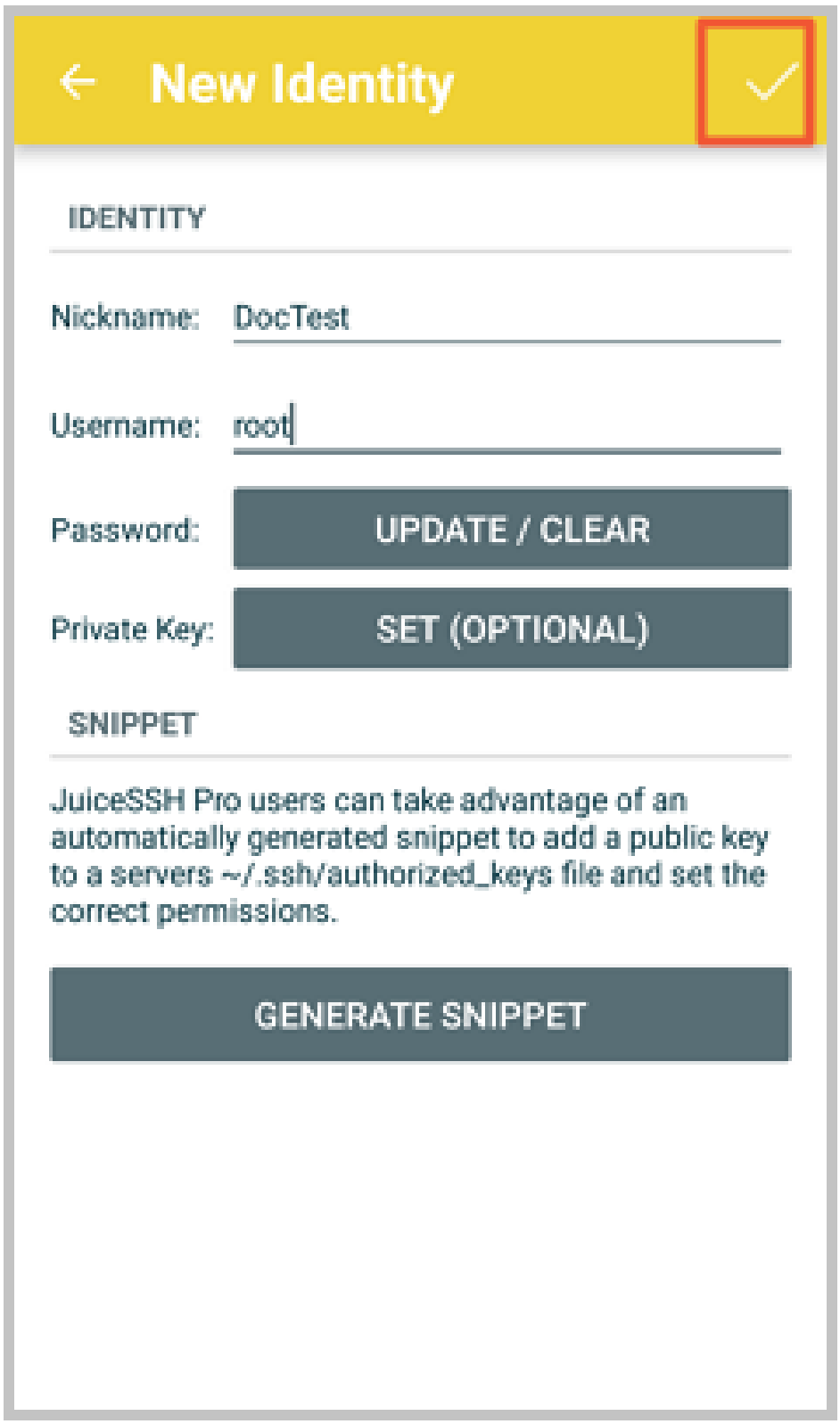
3. **New Connection**ページで接続情報を追加します。


icon.次の接続情報が必要です。

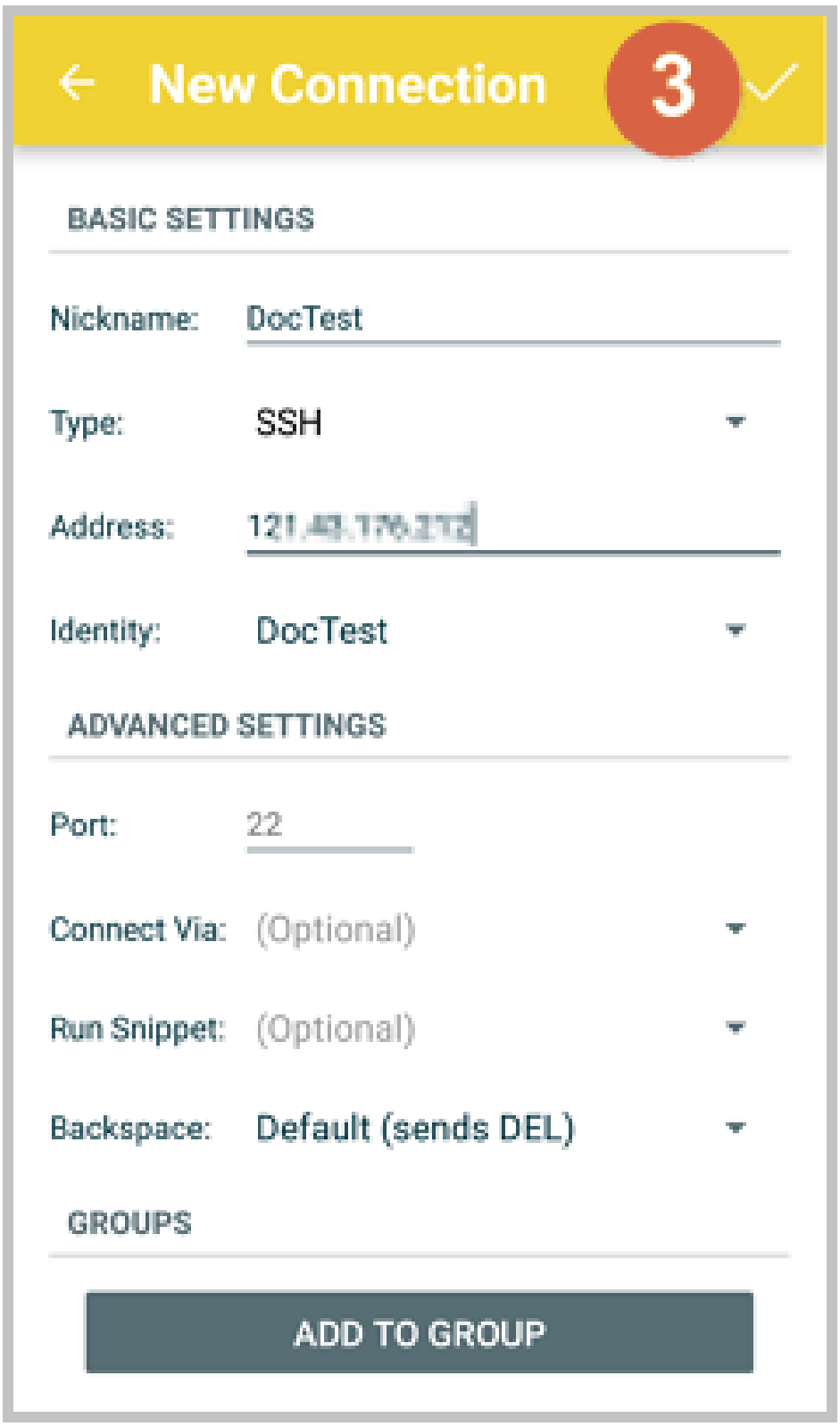
- **Name** ：接続セッションの名前を指定します。この例では、**DocTest**が使用されています。
- **Type**：デフォルト値 **SSH** を使用します。
- **Address**：接続するLinuxインスタンスのパブリックIPアドレスを入力します。
- **Identity**を設定するには、次の手順を実行します。
    a. **ID** をタップし、ドロップダウンリストで**New**をタップします。
    b. **New Identity**ページで、次の情報を追加します。



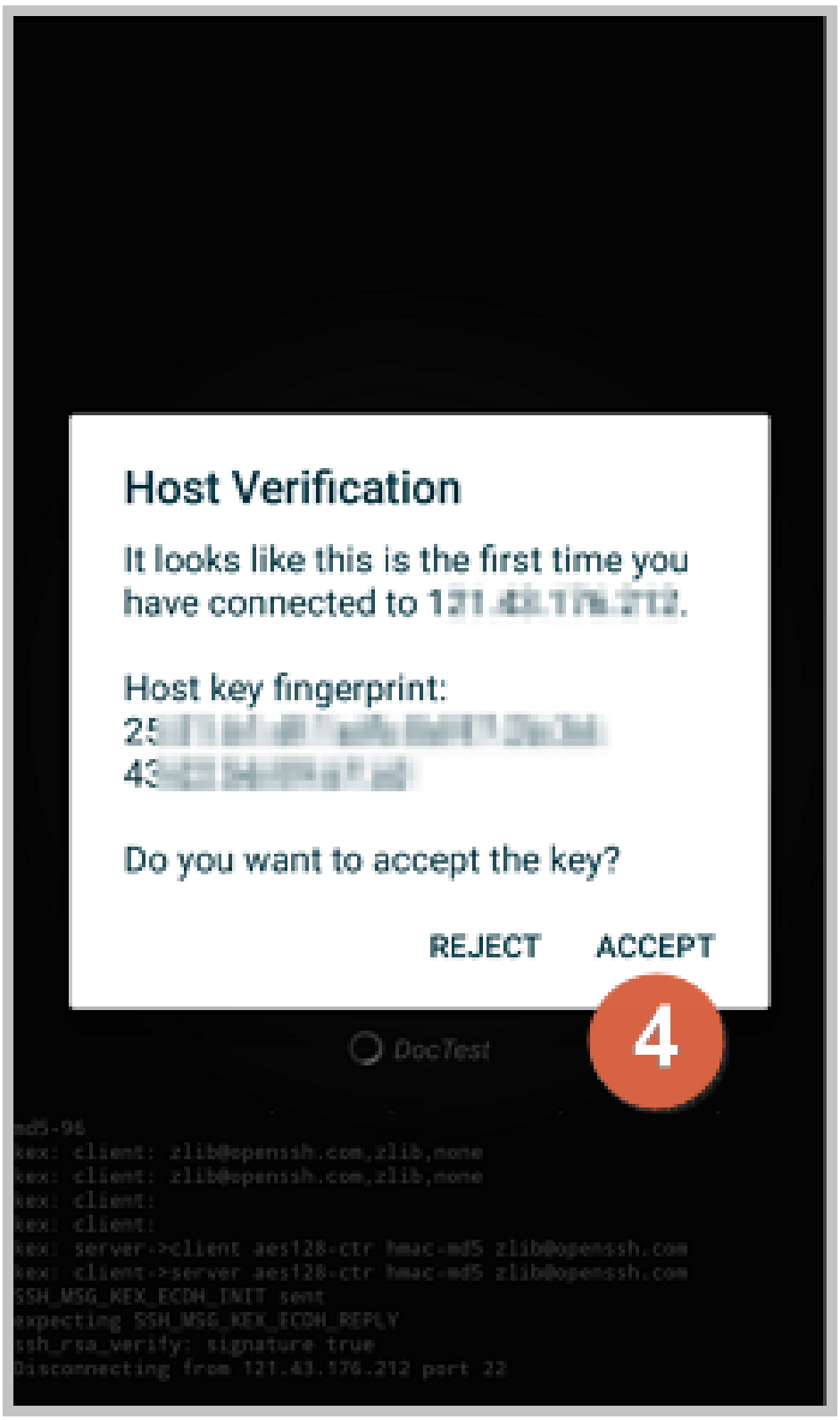
- **NickName**：オプション。管理を容易にするためにニックネームを設定することができます。この例では、**DocTest**が使用されています。
- **Username**：ユーザー名は **root** と入力します。
- **Password**： **SET (OPTIONAL)** をタップし、インスタンスのログオンパスワードを入力します。



- **Port**：SSHプロトコルのポート番号を入力します。この例では、 **22** が使用されています。

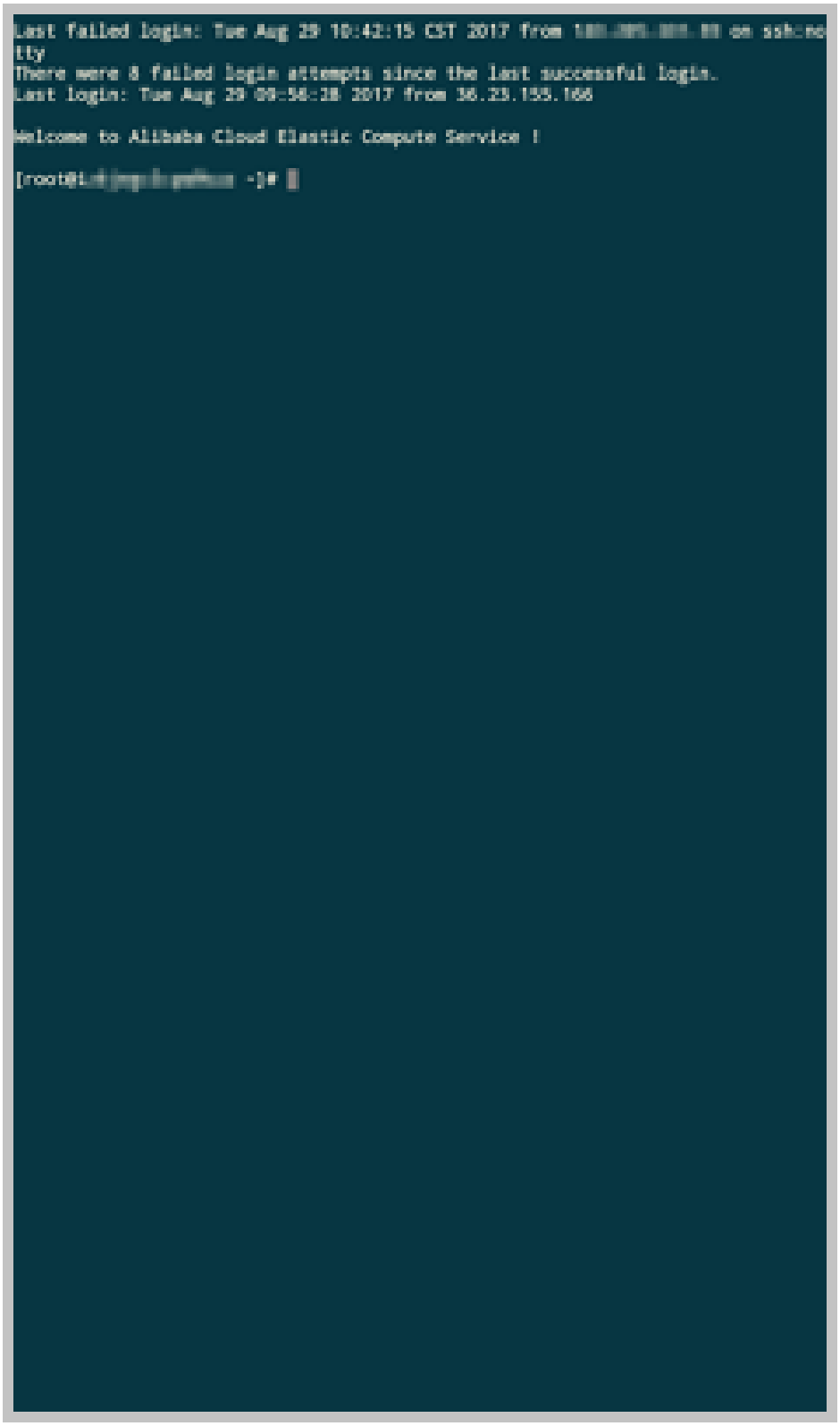


4. メッセージを確認し、 **ACCEPT** をタップします。



5. （オプション）最初の接続の場合、アプリケーションはフォント設定などのヒントを提供します。メッセージを確認し、 **[OK]** をタップしてください。

この手順で、Linuxインスタンスに接続可能です。



Windowsインスタンスに接続する

このセクションでは、アプリケーションを使用してモバイルデバイス上のWindowsインスタンスに接続する方法を説明するために、Microsoft Remote Desktopを例として取り上げます。

前提条件

インスタンスに接続する前に、次の点を確認してください。

- インスタンスの状態は **Running** です。
- インスタンスにはパブリックIPアドレスがあり、パブリックネットワークからアクセスできます。
- インスタンスのログインパスワードを設定済みです。パスワードが失われた場合は、**インスタンスパスワードをリセットする**必要があります。
- インスタンスのセキュリティグループには、**次のセキュリティグループルール**があります。

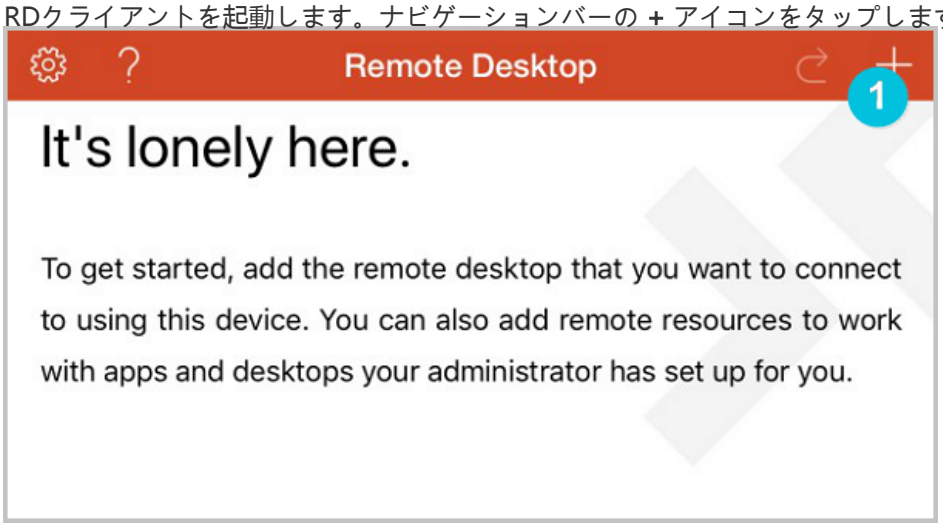
ネットワークのタイプ	NIC	ルールの方向	承認ポリシー	プロトコルタイプ	ポート範囲	認可タイプ	権限オブジェクト	優先
VPC	設定不要	インバウンド	許可する	RDP（3389）	3389/3389	アドレスフィールドへのアクセス	0.0.0.0/0	1
クラシック	インターネット							

- Microsoft Remote Desktopをダウンロードしてインストールします。
  - iOSデバイスの場合は、**iTunes**からアプリをダウンロードしてください。
  - Android搭載端末の場合は、**Google Play**からアプリをダウンロードしてください。

手順

Microsoftリモートデスクトップを使用してWindowsインスタンスに接続するには、以下の手順を実行します。

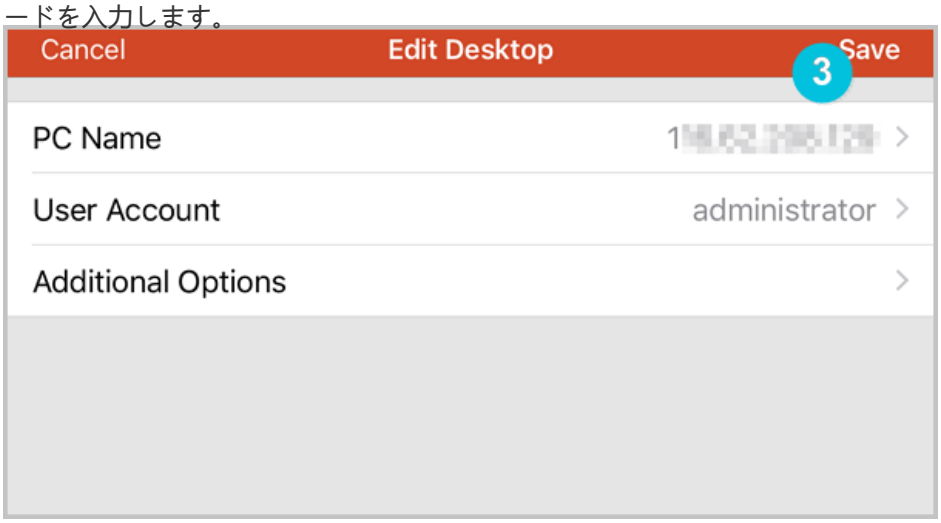
RDクライアントを起動します。ナビゲーションバーの **+** アイコンをタップします。



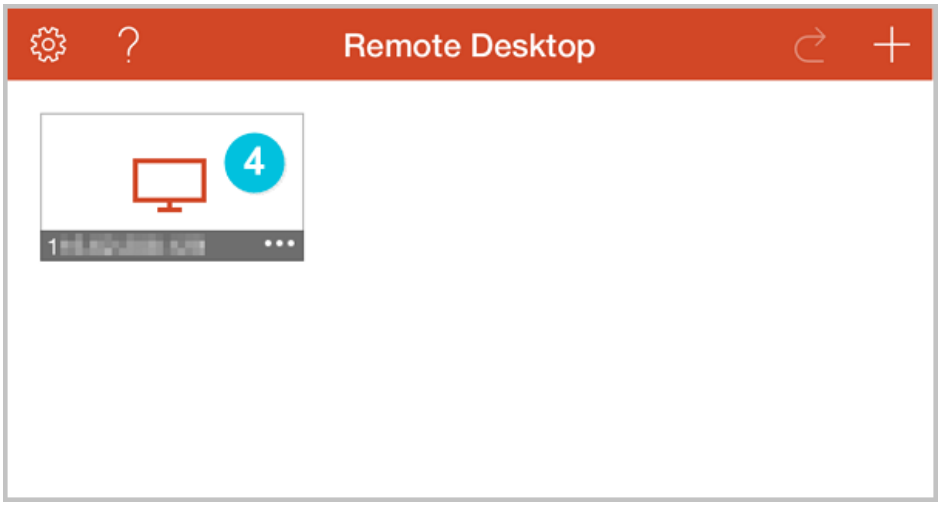
Add Newページで、**Desktop**を選択します。

[**Edit Desktop**]ページで接続情報を入力し、[**Save**]をタップします。次の接続情報が必要です。

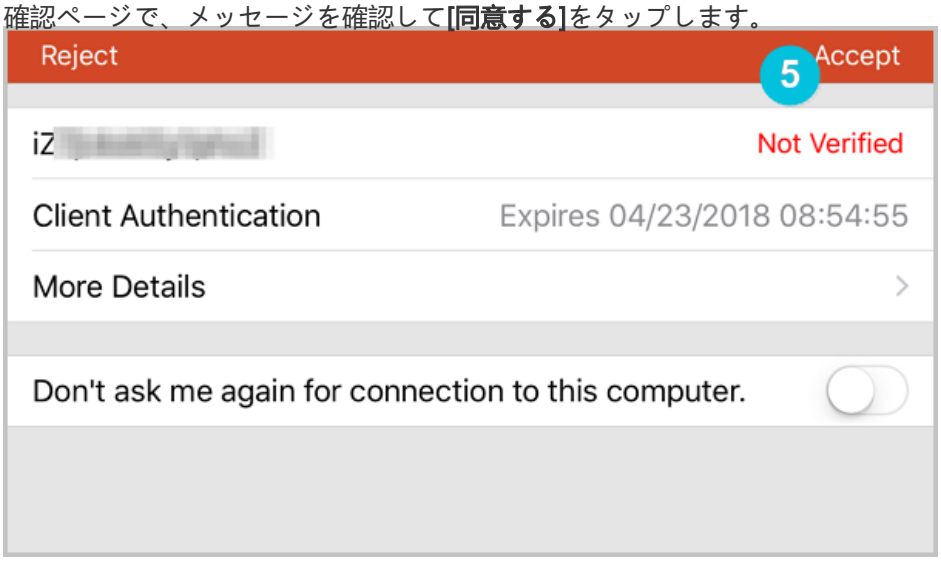
- **PC name**：接続するWindowsインスタンスのパブリックIPアドレスを入力します。
- **User Account**：Windowsインスタンスのアカウント名 *administrator* とログオンパスワードを入力します。



Remote Desktopページで、Windowsインスタンスのアイコンをタップします。



確認ページで、メッセージを確認して**[同意する]**をタップします。



この手順で、Linuxインスタンスに接続可能です。

インスタンス

インスタンスの作成

インスタンスの作成

インスタンスの作成

Linux インスタンス、Windows インスタンス、またはカスタムイメージからインスタンスを作成できます。詳細は下記を参照して下さい。

- 新しいインスタンスを作成する手順については、「クイックスタート」 を参照してください。
- カスタムイメージからインスタンスを作成する手順については、「イメージを使用したインスタンスの作成」を参照してください。

gn5インスタンスを作成する

gn5タイプファミリーの紹介

gn5型のさまざまな型の詳細については、Elastic Compute Service*Product Introduction*インスタンスタイプファミリー を参照してください。

gn5型のインスタンスを作成する

ECS（Elastic Compute Service）のクイックスタートで ステップ 2. インスタンスの作成で説明した手順に従って、gn5タイプファミリのインスタンスを作成します。インスタンスを作成するときは、次の項目に注意してください。

- **リージョン**: 現在、GN5は次の地域で利用可能です：中国東部1、中国東部2、中国北部2、中国南部1、米国東部1（バージニア）、米国西部1、香港、アジア・パシフィックSE 1、アジア太平洋SE 2、ドイツ1
- **ネットワークタイプ**: **VPC**は、仮想プライベートクラウドネットワークでgn5を使用できるため選択します。
- **インスタンスタイプ**: **Generation Ⅲ**の下にある**GPU Compute Type gn5)**を選択します。
- **ネットワーク帯域幅**: 必要に応じてピーク帯域幅を選択します。

  Windows 2008 R2イメージを使用していて、gn5タイプのインスタンスに接続する場合は、ECSコンソールにある**管理端末**を使用してgn5タイプのインスタンスに接続できないため、インスタンスのインターネットアクセスを有効にする必要があります。インターネットIPアドレ

スをインスタンスに割り当てる場合は、ピーク帯域幅を0 Mbpsに設定しないでください。

- **イメージ**: 必要に応じてイメージを選択します。

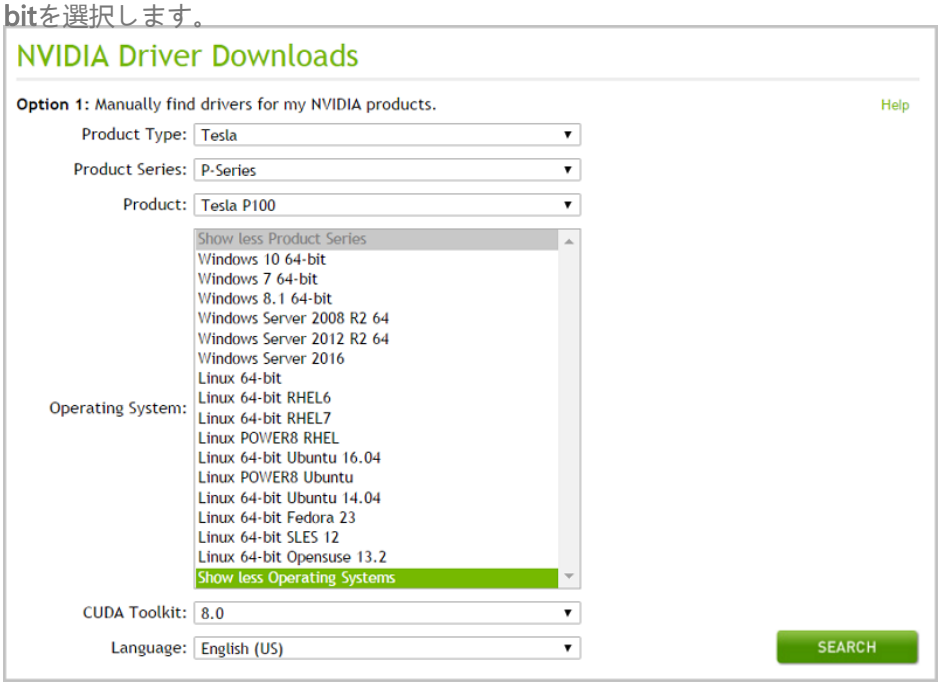
GPUドライバをダウンロードしてインストールする

gn5タイプファミリのインスタンスを使用する前に、そのインスタンスのGPUドライバをインストールする必要があります。手順に従って、GPUドライバをダウンロードしてインストールします。

オペレーティングシステムとP100 GPUに対応するドライバをダウンロードするには、NVIDIA公式サイトを参照してください。ダウンロードURL: http://www.nvidia.com/Download/index.aspx?lang=en-us.

手動でインスタンスのドライバを検索します。パラメータを次のように設定します。

- **製品タイプ**: Tesla
- **製品シリーズ**: P-Series
- **製品**: Tesla P100
- **オペレーティングシステム**: インスタンスイメージによる対応バージョン
  - オペレーティングシステムがドロップダウンリストに表示されない場合は、ドロップダウンリストの下部にある**すべてのオペレーティングシステムの表示**をクリックします。
  - インスタンスがリストにないLinuxイメージを使用する場合は、**Linux 64-bit**を選択します。

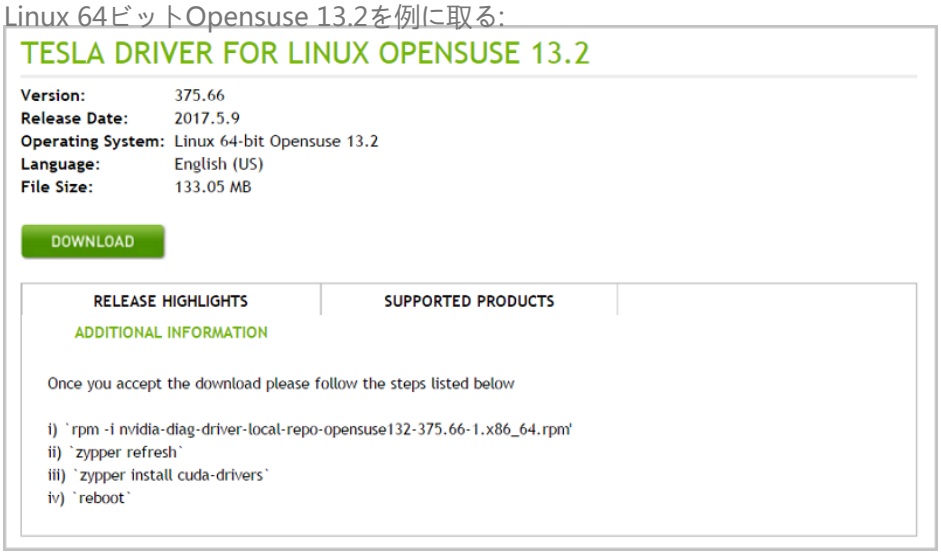


検索をクリックします。

情報を確認したら、**ダウンロード**をクリックしてください。

GPUドライバをインストールするには、ダウンロードページに**ADDITIONAL INFORMATION**を入力します。

Linux 64ビットOpensuse 13.2を例に取る:



Notes

Windows 2008 R2以前のバージョンの場合、GPUドライバのインストール後、EC Sコンソールで**接続**をクリックして、**管理端末**を入力すると、**管理端末** は黒い画面またはスタートアップインターフェイスになります。インスタンスがインターネットにアクセスできる場合は、マイクロソフトが開発したリモートデスクトッププロトコルなどの他のプロトコルを使用して、ECSインスタンスにリモートで接続する必要があります。

イメージを使用したインスタンスの作成

既存の ECS インスタンスと同じオペレーティングシステム、ソフトウェアアプリケーション、およびデータを持つインスタンスを作成するには、既存の ECS インスタンスのコピーをカスタムイメージとして作成し、それを使用して新しいインスタンスを作成できます。この方法は展開効率を向上させることができます。

前提条件

- イメージとインスタンスが同じリージョンにある場合は、次のいずれかの方法を使用してカスタム

イメージを作成できます。
- イメージのインポート
- インスタンスからカスタムイメージの作成
- スナップショットからカスタムイメージの作成

操作手順

ECS管理コンソールにログインします。

左側のナビゲーションペインで、[**インスタンス**]を選択します。

ページの右上にある[**インスタンスの作成**]をクリックします。

購入ページで、

- 希望する課金方法、対象リージョン、インスタンスタイプ、ネットワークタイプ、およびその他のパラメータを選択します。詳細については、クイックスタート を参照してください。
- カスタムイメージを選択します。

  注：選択したカスタムイメージに複数のデータディスクスナップショットが含まれている場合、同数のデータディスクが自動的に作成されます。デフォルトでは、各データディスクのサイズはソーススナップショットのサイズと同じです。データディスクのサイズを増やすことはできますが、減らすことはできません。

[**今すぐ購入**]をクリックします。

オペレーティングシステムの変更

オペレーティングシステムの変更

管理コンソールを使用して、インスタンスの既存 OS を希望の OS に変換することができます。詳細は、システムディスクの変更（カスタムイメージ） または システムディスクの変更（パブリックイメージ） を参照してください。

注：中国本土以外のリージョンでは、Linux と Windows 間の変換をサポートしていません。インスタンス

がこれらのリージョンにある場合、Linux と Windows 間の変換ができませんが、Windows バージョンの変更、または既存の Linux OS を別の Linux OS に置き換えることができます。

設定のアップグレード

インスタンスのパスワードのリセット

インスタンスのパスワードのリセット

インスタンスを作成する際にパスワードを設定しなかった場合、または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できます。

- Windows インスタンスでは、デフォルトユーザー名は *Administrator* です。
- Linux インスタンスでは、デフォルトユーザー名は *root* です。

> 注意：パスワードがリセット後、インスタンスの再起動が必要です。サービスへの影響を最小限にするため、リセット操作はメンテナンスの時間で実施することをお勧めします。

手順は次のとおりです。

1. ECS 管理コンソールにログインします。
2. 左側のナビゲーションバーで [**インスタンス**] をクリックします。
3. ページの一番上でリージョンを選択します。
4. 目的のインスタンスを選択します。複数のインスタンスを選択できますが、すべて同じステータスである必要があります。
5. [**パスワードのリセット**] をクリックします。
6. 表示されるダイアログボックスで、新しいパスワードを入力し、[**送信**] をクリックします。
7. パスワードを変更したインスタンスを選択し、[**再起動**] をクリックします。**インスタンス内ではなく、コンソールでインスタンスを再起動しなければ、新しいパスワードは有効になりません。**
8. 表示されるボックスで [OK] をクリックして、インスタンスを再起動します。

インスタンスの起動、表示、停止

この記事では、インスタンスを起動、表示、および停止する方法について説明します。

インスタンスの起動

コンソールでは、実際のサーバーと同じようにインスタンスを起動できます。

1. [ECS 管理コンソール]にログインします。
2. 左側のナビゲーションバーで [**インスタンス**] をクリックします。
3. ページの一番上でリージョンを選択します。
4. 目的のインスタンスを選択します。複数のインスタンスを選択できますが、すべてのインスタンスが同じステータスになっている必要があります。
5. [**起動**] をクリックします。

インスタンスの表示

コンソールを使用して、ユーザーのすべてのインスタンスを表示することができます。次の情報が表示されます。

- 各リージョン内のインスタンスの数と実行ステータス
- 特定のインスタンスに関する情報:
    - 基本、設定、支払い、モニタリングの情報
    - ディスク
    - スナップショット
    - セキュリティグループ

インスタンスを表示する手順は、以下のとおりです。

1. [ECS 管理コンソール]にログインします。
2. [概要] ページで、すべてのリージョンの ECS インスタンスの実行ステータスを確認できます。
3. 特定のインスタンスの詳細を確認するには、左側のナビゲーションバーで [**インスタンス**] をクリックし、ページの一番上でリージョンをクリックします。次に、確認する [**インスタンス**] の名前をクリックします。
4. そのインスタンスについての詳細を確認できます。さらに、ページの右側ではインスタンスの CPU およびネットワーク使用状況をモニターできます。

以下の情報のようなインスタンスに関する様々な情報を確認することができます。

- リージョン
- ゾーン
- 構成の詳細
- 支払い状況
- CPU
- ネットワーク使用

さらにディスク、スナップショットやセキュリティグループの情報も確認できます。

インスタンスの停止

注意:

- インスタンスが停止後でも課金されるため、課金を止めるのはインスタンスのリリースが必要です。
- 停止操作は、[実行中] ステータスのインスタンスに対してのみ行うことができます。
- 停止操作を実行すると、インスタンスが停止し、業務が中断されることになるため、注意してください。

手順は次のとおりです。

1. [ECS 管理コンソール]にログインします。
2. 左側のナビゲーションバーで [**インスタンス**] をクリックします。
3. ページの一番上でリージョンを選択します。
4. 目的のインスタンスを選択します。複数のインスタンスを選択できますが、すべて同じステータスである必要があります。
5. [**停止**] をクリックします。
6. 表示されるダイアログボックスで [**停止**] をクリックし、[**OK**] をクリックします。
7. 携帯電話に送信された検証コードを入力し、[**OK**] をクリックします。

インスタンスの再起動

コンソールでは、実際のサーバーと同じようにインスタンスを再起動できます。

注意:

- 再起動操作は、実行ステータスのインスタンスにのみ実行できます。
- 再起動によってインスタンスの動作が停止し、業務が中断されることになるため、注意して実行してください。

手順は次のとおりです。

1. [**ECS 管理コンソール**] にログインします。
2. 左側のナビゲーションバーで [**インスタンス**] をクリックします。
3. ページの一番上でリージョンを選択します。
4. 目的のインスタンスを選択します。複数のインスタンスを選択できますが、すべて同じステータスである必要があります。
5. [**再起動**] をクリックします。

6. 表示されるダイアログボックスで [**再起動**] をクリックし、[OK] をクリックします。

インスタンスのリリースと自動リリースの無効化

インスタンスのリリース

不要になった従量課金インスタンスは、すぐにリリースすることをお勧めします。従量課金インスタンスは、停止状態でも課金は継続され、リリースによって課金が終了します。

ただし、VPCタイプインスタンスの場合、 **停止済みインスタンスの非課金化**機能を有効にすることができます。この機能を有効にすると、VPCタイプインスタンスは作成後に秒単位で請求され、**停止済み**ステータスのときに請求が停止され、再開すると再び請求が開始されます。インスタンスタイプ料金を除き、この機能は他のECSリソースには適用されません。

不要になったインスタンスは、リリースすることができます。これには、次の 2 つの方法があります。

- 即時リリース: 従量課金インスタンスをすぐにリリースします。
- 時刻指定リリース: 将来のリリース日時を指定して、従量課金インスタンスをリリースします。この日時は、時間単位で設定します。設定をリセットして、前の日時を上書きすることもできます。インスタンスは毎時、正時と 30 分にリリースされますが、システムは指定したリリース日時に基づいて課金を停止することに注意してください。

手順は次のとおりです。

ECS 管理コンソールにログインします。

左側のナビゲーションバーで 「**インスタンス**」をクリックします。

ページの一番上でリージョンを選択します。

インスタンスを選択して、右側のアクション列の「**詳細**」-「**リリース**」をクリックします。

表示されるウィンドウで、リリースタイプとして「**即時リリース**」または「**時刻指定リリース**」を選択します。

「**時刻指定リリース**」 を選択した場合は、自動リリースの有無とリリース日時を指定する必要があります。

「**次へ**]」をクリックし、「**OK**」 をクリックします。

自動リリースの無効化

従量課金インスタンスの自動リリースが不要になった場合は、自動リリース機能の設定を無効にすることができます。

手順は次のとおりです。

ECS 管理コンソールにログインします。

左側のナビゲーションバーで 「**インスタンス**」をクリックします。

ページの一番上でリージョンを選択します。

インスタンスを選択して、右側の 「**詳細**」をクリックします。次に、「**リリース設定**」を選択します。

表示されるウィンドウで、リリースタイプとして「**時刻指定リリース**」を選択します。

「**自動リリース設定**」オプションをオフにします。

7. 「**次へ**」をクリックし、「**OK**」をクリックします。

セキュリティグループへのインスタンスの追加・削除

セキュリティグループへのインスタンスの追加

コンソールでは、セキュリティグループにインスタンスを追加できます。1 つの ECS インスタンスは、最大 5 つのセキュリティグループに属することができます。セキュリティグループにインスタンスを追加すると、そのインスタンスにセキュリティグループルールが自動で適用されます。更新は必要ありません。

1. [**ECS 管理コンソール**] にログインします。
2. 左側のナビゲーションバーで [**インスタンス**] をクリックします。
3. ページの一番上でリージョンを選択します。
4. 目的のインスタンスを選択し、右側のインスタンス名か対応する [**管理**] をクリックして [インスタンスの詳細] ページに移動します。
5. [**セキュリティグループ**] をクリックします。
6. [**セキュリティグループに追加**] をクリックします。表示されるダイアログボックスで、適切なセキ

ュリティグループを選択します。
7. [OK] をクリックします。

セキュリティグループからのインスタンスの削除

ビジネスニーズに基づいて、セキュリティグループからインスタンスを削除できます。1 つのインスタンスは少なくとも 1 つのセキュリティグループに属す必要があります。

1. [**ECS 管理コンソール**] にログインします。
2. 左側のナビゲーションバーで [**インスタンス**] をクリックします。
3. ページの一番上でリージョンを選択します。
4. 目的のインスタンスを選択し、右側のインスタンス名か対応する [**管理**] をクリックして [インスタンスの詳細] ページに移動します。
5. [**セキュリティグループ**] をクリックします。対象のインスタンスが属するセキュリティグループのリストが表示されます。
6. 削除するセキュリティグループを選択し、右側の [**削除**] リンクをクリックします。
7. 表示されるダイアログボックスで、[**OK**] をクリックします。

セキュリティグループの応用例については 適用シナリオ を参照してください。

Management Terminal からインスタンスへのログイン

管理端末からインスタンスへのログイン

管理端末は、他のリモート接続ツール (Putty、Xshell、SecureCRT など) が利用できないときに、Linux または Windows インスタンスへのログインに使用できる便利なツールです。適切な技術力を持つユーザーにとって、手軽に問題解決に利用できるセルフサービスツールです。

シナリオ

帯域幅を購入したかどうかにかかわらず、管理端末からインスタンスにログインすることができます。管理端末はほかにも、以下のシナリオをはじめ、さまざまなケースに適用できます。

インスタンス起動速度が遅いときに、進行を確認する必要がある場合 (例: セルフチェックの実行時)。

インスタンスでのソフトウェア設定エラーが原因で、リモート接続 (Putty など) に失敗し、ファイアウォールの再設定が必要な場合 (例: 誤操作によるファイアウォールの有効化)。

アプリケーションによる CPU や帯域幅の使用率が高く、リモート接続が妨げられているために、インスタンスにログインして異常なプロセスを終了させる必要がある場合 (例: ボットネット攻撃によって CPU または帯域幅が完全に占有された場合)。

手順

ECS 管理コンソール にログインします。

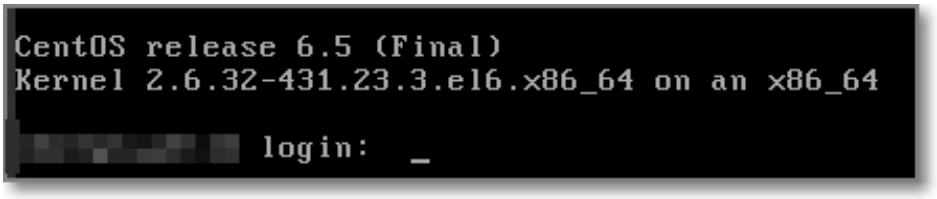
接続するインスタンスに移動します。

右側の [**VNC**] をクリックします。

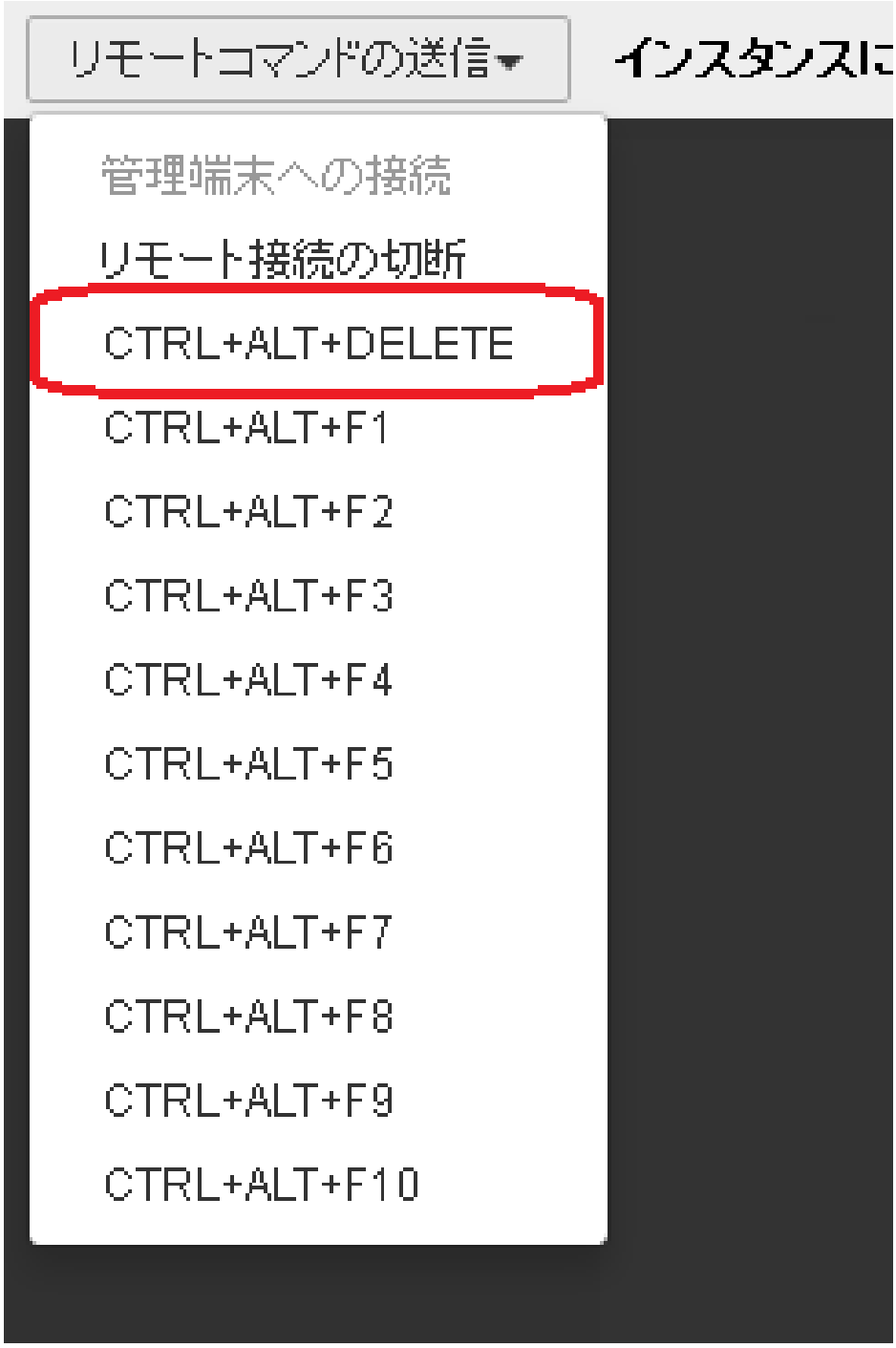
初回のログイン時に、管理端末 (VNC) のパスワードが表示されます。このプロンプトは 1 回のみ表示されます。管理端末にログインする際は、毎回このパスワードを入力する必要があります。**パスワードは忘れないよう、メモしておきます。**
パスワードを忘れた場合、または使い慣れているパスワードを使用したい場合は、右上の [**管理端末のパスワードの変更**] をクリックします。

右上の [**リモートコマンドの送信**] をクリックし、[**管理端末への接続**] をクリックします。管理端末 (VNC) パスワードを入力し、インスタンスに接続します。

Linux インスタンスの場合は、ユーザー名とパスワードを入力して、ログインします。画面が真っ暗な場合は、Linux インスタンスがスリープモードになっています。マウスクリックするか、いずれかのキーを押すと、表示が変わります。
Linux では、Ctrl + Alt + F1 ~ F10 のキーで端末を切り替えることができます。



Windows インスタンスの場合は、管理端末のインターフェイスで、リモートコマンド **Ctrl+Alt+Delete** を送信します。Windows へのログインインターフェイスが表示されます。ユーザー名とパスワードを入力して、ログインします。



パスワードの変更

ECS 管理コンソール にログインします。

接続するインスタンスに移動します。

右側の [**VNC**] をクリックします。

初回のログイン時に、管理端末 (VNC) のパスワードが表示されます。このプロンプトは 1 回のみ表示されます。管理端末にログインする際は、毎回このパスワードを入力する必要があります。**パスワードは忘れないよう、メモしておきます。**
パスワードを忘れた場合、または使い慣れているパスワードを使用したい場合は、右上の [**管理端末のパスワードの変更**] をクリックしてパスワードを変更します。

6 文字までのパスワードを入力します。英字の大文字と小文字、さらに数字をサポートしていますが、特殊文字は使用できません。

管理コンソールから **インスタンスの再起動**を実行し、パスワードを有効にする必要があります。インスタンス内での再起動は無効です。

よくある質問

管理端末は排他的ですか。
はい。1 人のユーザーの使用中に、他のユーザーが使用することはできません。

パスワードの変更後に、管理端末からログインできません。なぜでしょうか。
(インスタンス内からではなく) 管理コンソールからインスタンスを再起動し、パスワードを有効にする必要があります。

ログインした後、画面が真っ暗です。どのようにすればよいでしょうか。
真っ暗な画面は、インスタンスがスリープモードであることを示します。Linux インスタンスの場合は、何かキーを押すと起動します。Windows インスタンスの場合は、リモートコマンド Ctrl+Alt+Del を送信し、ログインインターフェイスに戻ります。

管理端末にアクセスできません。どのようにすればよいでしょうか。
次の手順でトラブルシューティングを行います。Chrome を使用して管理コンソールにログインし、F12 を押して開発者ツールを開き、コンソール内の情報を確認して問題を分析します。

IE8.0 か Firefox を使用していますが、管理端末を開くことができないのはなぜですか。
IE は 10 以降のみをサポートしています。また、Firefox の一部のバージョンはサポートしていません。

この問題を解決するには、最新の IE バージョンをダウンロードするか、代わりに Chrome を使用してください。Chrome は、より適切に管理コンソールをサポートしています。

ECSインスタンスのリリース

ECS インスタンスのリリース(削除)

サブスクリプションタイプと従量課金タイプのリリース方法の違い

- **サブスクリプションの場合：**
  - 手動でリリース（削除）することはできません。
  - ECSの自動更新機能を「OFF」にし、期限が切れた日から15日後インスタンスが停止され、30日後は自動的にリリースされます。

- **従量課金の場合：**
  - 手動でリリースすることができます。
  - 不要になった従量課金のECSインスタンスは、コンソールから手動でリリースすることができます。

操作手順

サブスクリプションECSの場合

サブスクリプションインスタンスのリリース手順をご参照ください。

従量課金ECSの場合

従量課金インスタンスのリリース手順と自動リリースの無効化 をご参照ください。

注意： ECSインスタンスをリリースすると、このECSインスタンスに関連付けられているすべてのリソースが削除されます。また削除されたデータは一切復旧できません。

ECS の更新方法

ECS 有効期限の手動更新

ECS 有効期限の手動更新（再購入）

年単位または月単位のサブスクリプションで課金されるECSインスタンスのみ更新が必要となります。
また有効期限日以降経過期間に応じてインスタンスの稼動ステータス、更新方法が異なります。
詳細は以下のとおりです。

● 期限が切れてから15日以内は、インスタンスは正常に動作します。この期間は自動及び手動でインスタンスを更新できます。

> 例えば、2016年4月25日00:00:00にインスタンスの有効期限が切れたが2016年5月9日に更新が成功した場合において、この更新に対する課金サイクルは2016年4月25日00:00:00から2016年5月25日00:00:00までとなります。

● 期限が切れてから15日以降、インスタンスは強制的に停止状態になります。更新するまでインスタンスにログインできません。この期間は手動更新のみ可能です。

> 例えば、2016年5月10日00:00:00にインスタンスがシャットダウンされたが2016年5月23日08:09:35に更新が成功した場合において、この更新に対する課金サイクルは2016年5月23日08:09:35から2016年6月24日00:00:00となります。

※期限が切れてから15日以降、インスタンスを任意、もしくは更新の失敗により未更新のままの場合、停止から15日後にインスタンスがリリース（削除）されます。削除後はインスタンスを復元することはできませんので、ご注意ください。

手動更新手順

ECS コンソールにログインします。

左側ナビゲーションメニューから「**インスタンス**」をクリックします。

「インスタンスリスト」からリージョンを選択します。インスタンス名、インスタンスID、または

インスタンスのステータスでインスタンスを検索することが可能です。

更新したいサブスクリプションECSインスタンスを選択し、アクションの「**更新**」をクリックしますと、手動更新画面が表示されます。

更新期間を選択し、「**注文**」ボタンをクリックしますと、支払い画面に入ります。「**支払い**」をクリックし、手動更新が完了します。

注意：
・手動更新ができるのは有効期限が切れたインスタンスのみです。
・更新期間は1ヶ月もしくは１年間のみサポートします。

ECS 有効期限の自動更新

自動更新サービスは、サブスクリプションを使用するインスタンスにのみ適用されます。

はじめに

自動更新機能を有効にしている場合、Alibaba Cloudはインスタンスの期限が切れる日付に登録しているクレジットカードに料金を請求します。

ECSインスタンスの購入後からインスタンスが停止される前までに、**サブスクリプション更新**ページで自動更新機能を有効にすることができます。自動更新機能が有効になっている場合：

- 月単位のサブスクリプションインスタンスの有効期限が切れると自動的に一ヶ月で更新されます。
- 年間サブスクリプションインスタンスの有効期限が切れると自動的に一年間で更新されます。

> **注意：**
> 自動更新機能では、毎月の定期購入と年間契約の切り替えはサポートされていません。インスタンスの利用期間を変更する場合 手動更新 機能をご利用ください。

自動更新サービスを有効にすると、

有効期限（T）の7日目、3日目、または1日前にサブスクリプションインスタンスの有効期限が通知されます。

Alibaba Cloud は、有効期限（T）にリンクされたクレジットカードへの使用料を請求します。料金の支払いが失敗した場合、Alibaba Cloud は、支払いが成功するまで、7日目（T + 6）と15日目（T + 14）に再度試みます。3 回の支払いがすべて失敗した場合、インスタンスは停止します。

サブスクリプションの支払いが成功した場合、インスタンスは **期限切れ** ステータスになった日から、次の請求サイクルは有効期限から開始されます。

> たとえば、月額サブスクリプションのインスタンスが 2016 年 4 月 25 日 00:00:00 に期限切れになっていて、2016 年 5 月 9 日に自動的に更新された場合、この更新の請求サイクルは 2016 年 4 月 25 日 00:00:01 ～ 2016 年 5 月 25 日の 00:00:00 です。

3回の支払いがすべて失敗した場合、インスタンスは有効期限の 15 日後に停止します。また、インスタンスが停止されると、サービスの提供が停止され、ログオンしたり、インスタンスにリモート接続することさえできなくなります。この時点で、手動更新のみ選択できます。有効期限の 15 日後にインスタンスが更新されない場合、インスタンスはリリースされ、データは失われます。

自動更新が試行される前に手動でインスタンスを更新すると、インスタンスが更新され、現在の請求サイクルで自動更新が試行されません。インスタンスは次の請求サイクルに入ります。

Alibaba Cloud は、失敗した自動更新の試行ごとに、リンクされたメールアドレスに通知メールを送信します。メールの確認より、更新を忘れることがなく、今後のビジネスへの影響を避けるため

に必要な処置を取ることができます。

自動更新の有効化

自動更新を有効にするには、次の手順を実行します。

[コンソール] にログインします。

ナビゲーションメニューから **[Billing Management]** をクリックします。

[サブスクリプション更新] を選択します。

「**自動更新を有効にする**」をクリックして、自動更新のステータスを変更する画面が表示されます。

自動更新サイクルを選択して、 **[自動更新を有効にする]** をクリックします。

自動更新の無効化

インスタンスの自動更新サービスを無効にするには、次の手順を実行します。

[コンソール]にログインします。

ナビゲーションメニューから **[Billing Management]** をクリックします。

[サブスクリプション更新] を選択します。

自動更新タブにある、対象インスタンスの「**自動更新を変更する**」をクリックして、自動更新のステータスを変更する画面が表示されます。

自動更新を無効に設定して、「**OK**」をクリックします。

VPC における ECS インスタンスのプライベート IP アドレスの変更

VPC ECSインスタンスを作成した後、プライベートIPアドレスを変更したり、ECSインスタンスのVSwitchを変更することもできます。

手順

ECSコンソールへログインします。

左側のナビゲーションペインで、[**インスタンス**]をクリックします。

リージョンをクリックし、ターゲットECSインスタンスのIDをクリックします。

インスタンスの詳細ページで、右上隅の**停止**をクリックします。

設定情報パネルで、**その他**> **プライベートIPアドレスの変更**をクリックします。

[**プライベートIPアドレスの変更**]ダイアログで、次のいずれかの方法でプライベートIPを変更し、**[変更]** をクリックします。

VSwitch ：リストからECSインスタンスの新しいVSwitchを選択します。

VPC内の各VSスイッチは固有のCIDRブロックを有するので、ECSインスタンスのプライベートIPアドレスはVSスイッチの変更と共に自動的に変更される。

プライベートIPアドレス：ECSインスタンスのVSwitchを変更しない場合は、新しいIPアドレスを入力します。

ECSインスタンスを再起動します。

ユーザーデータとインスタンスメタデータ

ECSインスタンスのRAM役割

インスタンス情報の表示

コンソールでは、次の ECS インスタンスを表示できます。

[**概要**]ページで、すべてのリージョンのすべての ESC インスタンスとそのアカウントのステータス。

[**インスタンスリスト**]ページの異なるリージョンにあるすべての ECS インスタンスの情報。

[**インスタンス詳細**]ページの ECS インスタンスの詳細情報。

概要ページでアカウントのすべての ECS インスタンスを表示する

アカウントで作成されたすべての ECS インスタンスの情報は、ECS **概要** ページで表示できます。

ECS インスタンスの総数と異なるステータスのインスタンス数

異なるリージョンのリソース数と異なるステータスの ECS インスタンス数。

ECSコンソールのホームページは、デフォルトで **概要** ページです。

インスタンスリストページの指定されたリージョンにあるすべての ECS インスタンスを表示する

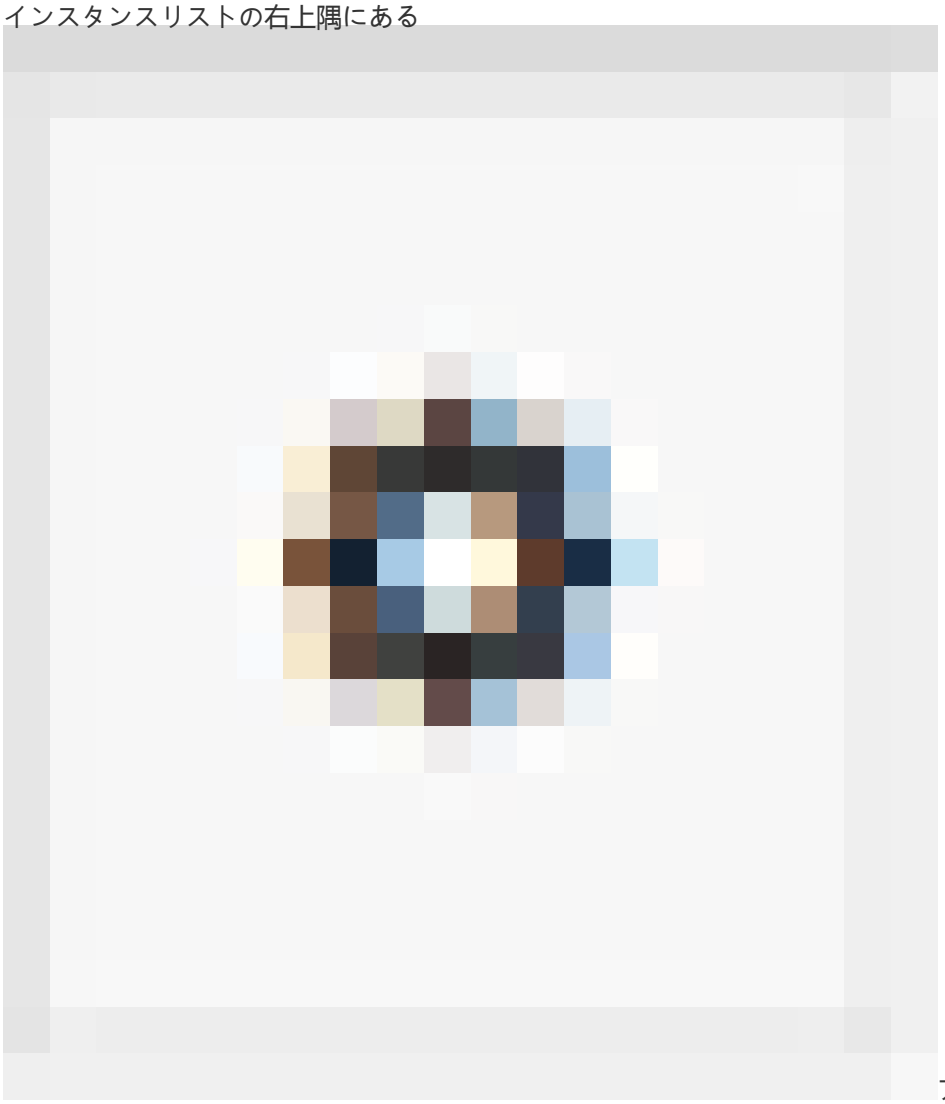
インスタンスリスト ページに移動するには、次の手順を実行します。

ECSコンソール にログオンします。

左側のメニューで、[**インスタンス**]をクリックします。

リージョンを選択してください。

ECS インスタンス ID /名前、ゾーン、IP アドレス、ステータス、ネットワークタイプ、課金方法、アクションなど、選択したリージョンの既存のすべての ECS インスタンスの情報が表示されます。 **表示アイテムの設定** 機能を使用すると、インスタンスの表示情報を表示または非表示にすることができます。

インスタンスリストの右上隅にある  アイコンをクリックします。

表示項目 のダイアログボックスで、表示するインスタンス情報を選択し、 **OK** をクリックします。

インスタンスの詳細ページで ECS インスタンスの詳細を表示する

インスタンスの詳細に移動して、ECS インスタンスの詳細情報を表示することができます。

インスタンスの詳細ページに移動するには、次の手順を実行します。

ECSコンソール にログオンします。

左側のメニューで、[**インスタンス**]をクリックします。

リージョンを選択してください。

詳細を表示する ECS インスタンスを見つけて、そのインスタンス ID をクリックします。

インスタンスの詳細ページでは、次の情報を表示できます。

ECS インスタンス ID、インスタンス名、リージョン、ゾーン、インスタンスタイプ、インスタンスタイプファミリ、イメージ ID、キーペア名 (Linux インスタンスのみに適用)、インスタンス RAM ロール、およびタグを含む * 基本情報 。

CPU、メモリ、I / O 最適化、オペレーティングシステム、IP アドレス、帯域幅の課金方法、現在の帯域幅、および VPC ネットワーク情報 (VPC インスタンスのみに適用されます) を含む * 設定情報 。

請求方法、インスタンスを停止するモード、作成時間、および自動リリーススケジュール (従量課金インスタンスのみに適用されます) を含む **支払い情報** 。

CPU およびネットワークの使用状況を含むモニタリング情報 。

インスタンスの詳細ページから**インスタンスディスク**、**インスタンススナップショット**、**セキュリティグループ**ページに切り替えて、このインスタンスに関連するリソースを表示することもできます。

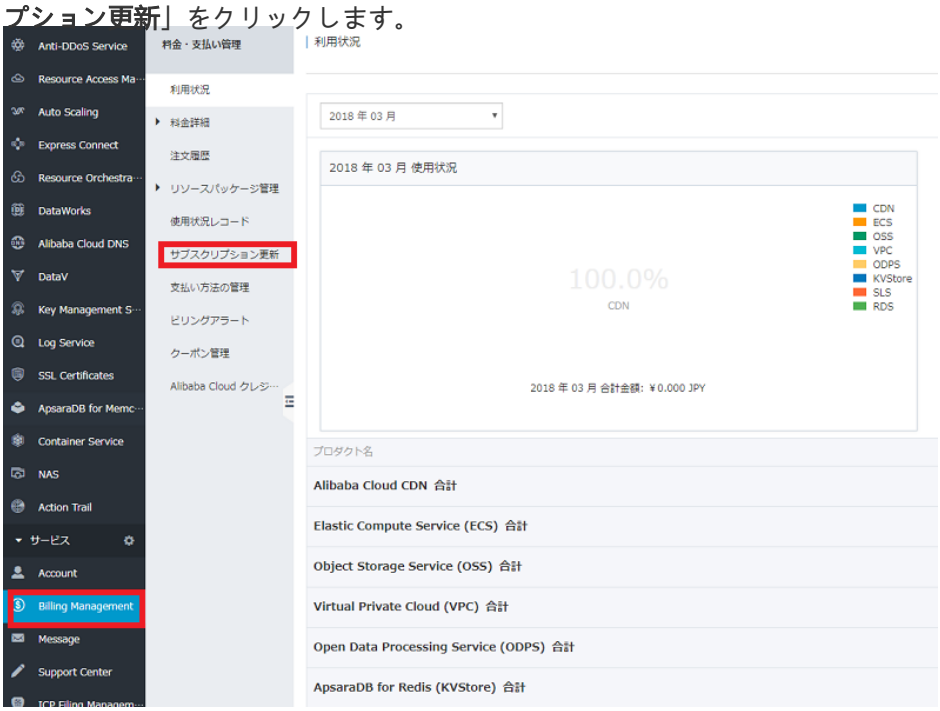
サブスクリプションインスタンスのリリース（削除）

サブスクリプション インスタンスのリリース手順

[ECS コンソール]にログインし、リリースするサブスクリプションインスタンスを選択します。

自動更新の列を確認し、下図のように「**自動更新1ヶ月**」の場合には、更新しない設定が必要です

左側のナビゲーションにある「**Billing Management**」をクリックし、開いた画面の「**サブスクリプション更新**」をクリックします。



新しいタグの中に、「**自動更新**」をクリックし、自動更新のステータスを変更する画面が表示されます。

自動更新を無効に設定して、「**更新しない**」をクリックします。

コンソール画面に戻り、対象ECSの自動更新状態が「**更新しない**」に変更されます。

更新しない状態で、有効期限が切れてから１ヶ月後に自動リリースされます。

ディスク

クラウドディスクの作成

クラウドディスクはデータディスクとも呼ばれ、管理コンソールから購入できます。各ユーザーアカウントが購入できるクラウドディスクは最大 250 個です。各 ECS インスタンスには、32 TB までの容量を持つデータディスクを 16 までアタッチすることができます。

クラウドディスクは以下の手順で購入できます。

1. [**ECS 管理コンソール**] にログインします。
2. 左側のナビゲーションバーで [**インスタンス**] をクリックします。
3. ページの一番上でリージョンを選択します。次に、ページの右上隅にある [**インスタンスを作成**] をクリックします。
4. [**クラウドディスクの購入**] をクリックします。
5. リージョンとゾーンを選択します。
6. クラウドディスクのタイプ、サイズ、数を選択します。次に、ページの右側にある [**今すぐ購入**] をクリックします。

Linux の場合の次のステップ

Linux インスタンスの場合、クラウドディスクをシステムで表示して使用するには、クラウドディスクをアタッチし、パーティションを作成してから、フォーマットする必要があります。

1. データディスクのアタッチの詳細については、「データディスクのアタッチ」を参照してください。
2. パーティションのフォーマットについて、およびアタッチされたデータディスクへの新しいパーティションのアタッチについては、「データディスクのフォーマットとアタッチ」を参照してください。

Windows の場合の次のステップ

Windows インスタンスの場合、クラウドディスクは使用する前にアタッチしてフォーマットする必要があります。

1. データディスクのアタッチの詳細については、「データディスクのアタッチ」を参照してください。
2. アタッチされたデータディスクのフォーマットの詳細については、「データディスクのフォーマット」を参照してください。

スナップショットからのクラウドディスクの作

成

既存の**システムディスク**または**データディスク**のスナップショットを撮り、スナップショットからクラウドディスクを作成できます。新しいディスクは**同じリージョンの同じゾーン**にある任意のインスタンスにアタッチすることができます。

シナリオ

スナップショットからデータにアクセスする必要があるが、ディスクをスナップショットにロールバックしたくない場合は、スナップショットからクラウドディスクを作成し、ディスクからデータにアクセスできます。

たとえば、インスタンスでシステムディスク障害が発生した場合は、既存のスナップショットを使用してクラウドディスクを作成し、ディスクを正常なインスタンスにアタッチすることができます。このようにして、障害のあるインスタンスのデータを復元できます。

ディスクのパフォーマンス

スナップショットから作成されない SSD クラウドディスクとウルトラクラウドディスクは、容量の最大性能を発揮することができます。事前調整は必要ありません。

ただし、スナップショットから作成されたクラウドディスクの場合、ディスクに書き込まれる前に OSS からデータにアクセスする必要があるため、初期パフォーマンスが低下する可能性があります。

プロダクションを使用する前に、すべてのデータブロックに一度だけ書き込みして読み込むことをお勧めします。

前提条件

あなたのインスタンスに**スナップショットの作成**があります。

手順

スナップショットからクラウドディスクを作成するには、次の手順を実行します。

ECS コンソールにログオンします。

ナビゲーションペインで、**スナップショット&イメージ**> **スナップショット**を選択します。

予想されるスナップショットを見つけ、その ID をコピーします。

ナビゲーションペインで、**ブロックストレージ**> **クラウドディスク**を選択します。

[クラウドディスクを追加] をクリックします。

クラウドディスクの作成ページで、次の操作を行います。

i. リージョンとゾーンを選択します。このディスクをインスタンスに接続するには、ディスクが同じリージョンとゾーンにあることを確認してください。
ii. **ストレージの選択****スナップショットでディスクを作成する**をクリックし、必要なスナップショットを選択します。
iii. **購入プラン**では、オプションを選択します。
iv. **概要**を確認してください。
v. **今すぐ購入**をクリックします。
vi. ご注文を確認し、お支払いをしてください。

クラウドディスク ページに戻り、 **クラウドディスクを追加** の横にある更新ボタンをクリックしてください。 作成したばかりのクラウドディスクは、 **ディスク状態**、 **使用中** で見つけます。

フォローアップ作業

クラウドディスクをインスタンスに接続できます。詳細についてはデータディスクのアタッチにご参照ください。

注意：

- Windows ユーザーの場合、コンソールで **アタッチ** をクリックして、新しいクラウドディスクをインスタンスに接続できます。
- Linux ユーザの場合は、 **アタッチ** をコンソールでクリックすると、 mount コマンドを実行する必要があります。

データディスクのアタッチ

データディスクのアタッチ

ECS では、データディスクとして使用されるUltra クラウドディスク、および SSD クラウドディスクのアタ

ッチがサポートされます。データディスクをアタッチする方法には、[インスタンス] メニューを使用するものと、左側のナビゲーションバーにある [ディスク] メニューを使用するものの 2 つがあります。この 2 つの方法について、以下で説明します。

考慮事項

データディスクをアタッチする前には、次の点を考慮します。

- インスタンスは次の条件をすべて満たす必要があります。
  - インスタンスのステータスが [**停止済み**] である。
  - セキュリティコントロールマーカーが [**ロック済み**] でない。
  - インスタンスが料金滞納状態でない。
- クラウドディスクのステータスは [**利用可能**] である必要があります。
- 1 つのインスタンスにはシステムディスクを 1 つまで、データディスクを (すべてのディスクカテゴリを合わせて) 16個までアタッチできます。
- クラウドディスクは、同じゾーンのインスタンスにのみアタッチできます。ゾーンをまたいでアタッチすることはできません。
- クラウドディスクは、一度に 1 つのインスタンスにのみアタッチできます。複数のインスタンスへのアタッチはサポートされていません。
- クラウドディスクは、リージョンおよびゾーンが同じ任意のインスタンス (サブスクリプションまたは従量課金のインスタンス) にアタッチできます。
- クラウドディスクがインスタンスのシステムディスクとして機能している場合、このディスクを個別にアタッチすることはできません。

データディスクをアタッチするには、[**インスタンス**] メニューを使用するか、左側のナビゲーションバーにある [**ディスク**] メニューを使用します。

- 複数のディスクを 1 つのインスタンスにアタッチする必要がある場合は、[**インスタンス**] メニューから実行する方が簡単です。
- ディスクを複数のインスタンスにアタッチする必要がある場合は、[**ディスク**] メニューから実行する方が簡単です。

[インスタンス] メニューの場合

ECS 管理コンソールにログインします。

左側のナビゲーションバーで [**インスタンス**] をクリックします。

ページの一番上でリージョンを選択します。

アタッチするインスタンスの名前をクリックするか、[**インスタンス**] ページの右側にある [**管理**] をクリックします。

左側のナビゲーションバーで [**インスタンスのディスク**] をクリックします。インスタンスに既にアタッチされているディスクが表示されます。

ページの右側にある [**ディスクのアタッチ**] をクリックし、[**接続先デバイス**] と [**データディスク**] をクリックすると、ディスクがアタッチされます。必要に応じて、インスタンスと共にディスクをリリースするかどうかと、ディスクと共にスナップショットをリリースするかどうかを設定します。

- **インスタンスと共にディスクをリリース**: インスタンスをリリースすると、ディスクも同時にリリースされます。
- **ディスクと共に自動スナップショットをリリース**: ディスクをリリースすると、すべての自動スナップショットもリリースされます。ただし、手動で作成したスナップショットは保持されます。データのバックアップのためには、このオプションを**選択しない**ことをお勧めします。

ディスクをアタッチしたら、インスタンスにログインしてディスクパーティションをフォーマットし、新しいパーティションをアタッチする必要があります。詳細については、このページの最下部にある「**次のステップ**」を参照してください。

[Disks] メニューの場合

ECS 管理コンソール にログインします。

左側のナビゲーションバーで [**ディスク**] をクリックします。

ページの一番上でリージョンを選択します。

アタッチするディスクの名前をクリックします。ディスクのステータスは [**利用可能**] である必要があります。[**使用中**] ステータスのディスクはアタッチできません。

ディスクリストの右端で、[**詳細**]、[**アタッチ**] の順にクリックします。

ターゲットのインスタンスとリリースアクションを選択します。

- **インスタンスと共にディスクをリリース**: インスタンスをリリースすると、ディスクも同時にリリースされます。
- **ディスクと共に自動スナップショットをリリース**: ディスクをリリースすると、すべての

自動スナップショットもリリースされます。ただし、手動で作成したスナップショットは保持されます。データのバックアップのためには、このオプションを**選択しない**ことをお勧めします。

ディスクをアタッチしたら、インスタンスにログインしてディスクパーティションをフォーマットし、新しいパーティションをアタッチする必要があります。詳細については、このページの最下部にある「**次のステップ**」を参照してください。

Linux の場合の次のステップ

ディスクをアタッチしたら、インスタンスにログインしてディスクパーティションをフォーマットし、新しいパーティションをアタッチする必要があります。詳しい手順については、「データディスクのフォーマットとアタッチ」を参照してください。

Windows の場合の次のステップ

ディスクをアタッチしたら、インスタンスにログインしてディスクパーティションをフォーマットする必要があります。詳しい手順については、「データディスクのフォーマット」を参照してください。

データディスクのデタッチ

ECSは、ベーシッククラウドディスク、ウルトラクラウドディスク、およびデータディスクとして機能するSSDクラウドディスクの分離をサポートしています。システムディスクを取り外すことはできません。**Instances** ページまたは **Disks** ページでディスクをデタッチします。

注意

使用中ステータスのデータディスクのみを切り離すことができます。

インスタンスのオペレーティングシステムに基づいて、以下を確認してください。

- Linuxインスタンスの場合、インスタンスにログオンし、 umountコマンドを実行してデータディスクをアンマウントします。コマンドを実行した後、ECSコンソールにログオンし、ディスクを取り外します。
- Windowsインスタンスの場合は、ディスクのすべてのファイルシステムで読み取りと書き込み操作を停止し、データの整合性を確保します。そうしないと、読み書き中のデータが失われます。

手続き

[インスタンス]ページ

1. ECS 管理コンソールにログインします。
2. 左側のナビゲーションバーで [**インスタンス**] をクリックします。
3. ページの一番上でリージョンを選択します。
4. インスタンスIDをクリックし、[インスタンスの詳細]ページに移動します。
5. 左側のナビゲーションバーで [**インスタンスのディスク**] をクリックします。インスタンスに既にアタッチされているディスクが表示されます。
6. デタッチするディスクをクリックします。
7. ページの右上隅にある [**デタッチ**] をクリックし、 表示されるダイアログボックスで、[**デタッチの確認**] をクリックします。

インスタンスからデータディスクを正常に切り離しました。

[ディスク]ページ

1. ECS 管理コンソールにログインします。
2. 左側のナビゲーションバーで [**ディスク**] をクリックします。
3. ページの一番上でリージョンを選択します。
4. デタッチするディスクをクリックし、ページの右上隅にある [**デタッチ**] をクリックします。
5. 表示されるダイアログボックスで、[**デタッチの確認**] をクリックします。

インスタンスからデータディスクを正常に切り離しました。

手順の後

インスタンスにアタッチされていなくても、データディスクの代金を支払う必要があります。だから、もうデータディスクが必要ない場合は、データディスクの削除をしてください。

ディスクの再初期化

ディスクの再初期化

ディスクを再初期化すると、ディスクを最初に作成した時点の状態に戻すことができます。

ディスクを再初期化した後は、次のようになります。

- インスタンスのオペレーティングシステムとそのバージョンは保持され、初期状態に戻ります。

- ECS インスタンスの IP アドレスは変更されません。元のシステムディスク上のデータはクリアされますが、インスタンス上のスナップショットの自動バックアップは保持され、インスタンスにアプリケーションをロールバックするために使用できます。

ディスクを再初期化する際は、事前に以下の考慮事項に注意する必要があります。

- ディスクを再初期化すると、そのディスク上のデータは失われます。続行する前に、スナップショットなどを使用して必ずデータをバックアップします。詳細については、「スナップショットの作成」を参照してください。

操作手順

1. ECS 管理コンソール にログインします。
2. 左側のナビゲーションバーで [**インスタンス**] をクリックします。
3. ページの一番上でリージョンを選択します。
4. ディスクを再初期化する前にインスタンスを停止します。ディスクを再初期化するインスタンスを選択し、一番下の [**停止**] をクリックします。
5. インスタンス名をクリックします。左側のナビゲーションバーで [**インスタンスのディスク**] をクリックします。
6. 再初期化するディスクを 1 つ以上選択します。その後、[**ディスクの再初期化**] をクリックします

7. 再初期化が完了したら、ログインのための新しいパスワードを入力します。[**ディスクの再初期化の確認**] をクリックします。

ディスクのロールバック

ディスクのロールバック

ディスクロールバックにより、ディスクのデータを以前のある時点までロールバックできます。

重要:

- スナップショットロールバックは、不可逆的な操作です。ロールバックが完了すると、元のデータを復元することはできません。したがって、この操作を実行する場合は十分に注意してください。
- ディスクロールバックは、インスタンスが停止している場合に実行可能です。

ディスクをロールバックするには、次の手順を実行します。

1. ECS 管理コンソールにログインします。
2. 左側のナビゲーションバーで [**インスタンス**] をクリックします。
3. ページの一番上でリージョンを選択します。
4. ディスクをロールバックする前にインスタンスを停止します。ディスクをロールバックするインスタンスを選択し、一番下の [**停止**] をクリックします。
5. インスタンス名をクリックします。左側のナビゲーションバーで [**スナップショット**] をクリックします。
6. ロールバックするスナップショットを選択します。一度に選択できるスナップショットは 1 つだけです。
7. [**ディスクのロールバック**] をクリックします。
8. 表示されるダイアログボックスで、[OK] をクリックします。

システムディスクの変更 (パブリックイメージ)

システムディスクを変更することによってオペレーティングシステムを別のパブリックイメージに変更できます。例えば、Windows Server 2003 から Windows 2012 に変更できます。

注意: 中国本土以外のリージョンは、Linux と Windows 間での交換をサポートしていません。Linux または Windows は、同じオペレーティングシステムの別のバージョンにのみ交換できます。

システムディスクの変更に関する考慮事項

リスク

- この操作を実行するにはインスタンスを停止する必要があるため、業務は中断されます。したがって、この操作は注意して実行する必要があります。
- 交換後は、新しいシステムディスクに実行環境を再デプロイする必要があります。これは、業務を長時間中断することになる可能性があります。したがって、この操作は注意して実行する必要があります。
- システムディスクを交換すると、元のシステムディスク上の自動スナップショットとデータは失われます。必ず事前にバックアップを作成してください。

注意

- 新しいディスクの自動スナップショットポリシーに合った十分なスナップショットクォータを確保するために、不要なスナップショットを削除することができます。

- システムディスクを変更しても、インスタンスの IP アドレスは変更されません。
- 手動で作成したスナップショットは交換後も保持されます。ただし、ディスク ID が変更されるため、元のシステムディスクから手動で作成したスナップショットを使用して新しいシステムディスクにロールバックすることはできません。保持されたスナップショットを使用してカスタムイメージを作成することはできます。
- システムディスクの交換後、元のディスクは削除されます。

自動スナップショットを保持する

デフォルトの場合、自動スナップショットはディスクと共にリリースされます。自動スナップショットを保持するため、ディスクリリースに伴う自動スナップショットリリースの設定を参照してください。

操作手順

完全なシステムディスク変更する手順は、次の手順が含まれます。

1. 該当システムディスクのスナップショットの作成
2. システムディスクの変更
3. 自動スナップショットポリシーの設定
4. データディスクのアタッチ (Linux インスタンスの場合のみ)

ステップ 1: 該当システムディスクのスナップショットの作成

システムディスクのデータを保持したくない場合は、この手順をスキップしてください。

忙しい時間にスナップショットを作成しないこと。40GBのスナップショットを作成するため約40分掛かりますので、十分な時間を確保してください。

注意: 容量不足でインスタンスが起動しない場合があるため、ディスク・スペースを十分に(最低 1GB) 確保してください。

ECS 管理コンソールにログインします。

左側のナビゲーションバーで [**インスタンス**] をクリックします。次に、ページの一番上でリージョンを選択します。

システムディスクを変更するインスタンスをクリックします。

左側のナビゲーションバーの [**インスタンスのディスク**] をクリックします。

変更するシステムディスクを見つけて [**スナップショットの作成**] をクリックします。

スナップショットの名前を入力します。

左側のナビゲーションバーの[**インスタンスのスナップショット**] をクリックすると、スナップショットの進行状況とステータスを確認できます。

ステップ 2: システムディスクの変更

システムディスクを変更には:

ECS 管理コンソールにログインします。

左側のナビゲーションバーで [**インスタンス**] をクリックします。次に、ページの一番上でリージョンを選択します。

システムディスクを変更する前にインスタンスを停止します。インスタンスリストで、システムディスクを交換するインスタンスを選択し、一番下の [**停止**] をクリックします。

インスタンスが停止したら、インスタンステーブルの右端で [**詳細**]、[**システムディスクの変更**] の順にクリックします。

考慮事項を示すダイアログボックスが表示されます。考慮事項を注意深く読んでから、操作を確認します。

オペレーティングシステムを選択します。

管理者または root のパスワードを設定します。

[**変更の確認**] をクリックします。発生する支出があれば、支払います。

重要なプロンプトが表示されます。注意深く読みます。間違いがないことを確認したら、[**OK**] をクリックします。

ステップ 3: 自動スナップショットポリシーの設定

システムディスクを変更すると、ディスクIDが変更されたため、設定した自動スナップショットポリシーは新しいシステムディスクでは作動しなくなります。この場合、新しいシステムディスクの自動スナップショートポリシーを設定する必要があります。詳細については、ディスクに対する自動スナップショットポリシーの設定 を参考ください。

ステップ 4: データディスクのアタッチ (Linux インスタンスの場合のみ)

Linux インスタンスの場合、システムディスクを変更した後、データディスクを再度アタッチする必要がありますが、パーティションを分割する必要はありません。詳細については **データディスクのアタッチ** を参考してください。

システムディスクの変更 (カスタムイメージ)

システムディスクを変更するときに、オペレーティングシステム、環境設定、および/またはデータを保持する場合は、インスタンスまたはシステムディスクを使用してカスタムイメージを作成し、そのイメージを使用してシステムディスクを変更できます。このドキュメントでは、このシナリオを使用して、システムディスク上のイメージをカスタムイメージに変更する方法について説明します。

システムディスクを変更することによってオペレーティングシステムをカスタムイメージに変更できます。システムディスクをパブリックイメージに変更する方法については、「システムディスクの変更 (パブリックイメージ) 」を参照してください。

- 「インスタンスを使用してカスタムイメージの作成」
- 「スナップショットを使用してカスタムイメージの作成」
- 「別のリージョンからカスタムイメージのコピー」
- 「イメージのインポート」
- 「カスタムイメージの共有」

システムディスクの変更では、インスタンスの IP アドレスを変えることがありません。

注意: 中国本土以外のリージョンは、Linux と Windows 間での交換をサポートしていません。Linux または Windows は、同じオペレーティングシステムの別のバージョンにのみ交換できます。

考慮事項:

- 交換操作を実行するにはインスタンスを停止する必要があるため、業務は中断されます。
- 交換後は、新しいシステムディスクに実行環境を再デプロイする必要がありますので、業務を長時間中断する可能性があります。
- システムディスクを交換すると、元のシステムディスク上の自動スナップショットとデータは失われます。必ず事前にバックアップを作成してください。自動スナップショットを保持するため、**ディスクリリースに伴う自動スナップショットリリースの設定** を参照してください。
- 手動で作成したスナップショットは交換後も保持されます。ただし、ディスク ID が変更されるため、元のシステムディスクから手動で作成したスナップショットを使用して新しいシステムディスクにロールバックすることはできません。保持されたスナップショットを使用してカスタムイメージを作成することはできます。
- システムディスクを交換後、元のディスクは削除されます。
- システムディスクに 1 GB 以上のフリースペースがない場合、交換後インスタンスが起動できない

可能性があります。

操作手順

完全なシステムディスク変更する手順は、次の手順が含まれます。

1. 該当システムディスクのスナップショットの作成
2. スナップショットに基づいてイメージの作成
3. システムディスクの変更
4. 自動スナップショットポリシーの設定
5. データディスクのアタッチ (Linux インスタンスの場合のみ)

システムディスクのデータを保持しないでオペレーティングシステムを変更したい場合は、単に [ステップ 3] に跳ばしてシステムディスクを直接変更できます。

ステップ 1: 該当システムディスクのスナップショットの作成

注意

- システムディスクのデータを保持したくない場合は、この手順をスキップしてください。
- 忙しい時間にスナップショットを作成しないこと。
- 40GBのスナップショットを作成するため約40分掛かりますので、十分な時間を確保してください。
- 容量不足でインスタンスが起動しない場合があるため、ディスク・スペースを十分に(最低 1GB) 確保してください。

ECS 管理コンソールにログインします。

左側のナビゲーションバーで [**インスタンス**] をクリックします。

該当リージョンを選択します。

システムディスクを変更するインスタンスをクリックします。

左側のナビゲーションバーの [**インスタンスのディスク**] をクリックします。

変更するシステムディスクを見つけて [**スナップショットの作成**] をクリックします。

スナップショットの名前を入力します。

左側のナビゲーションバーの[**インスタンスのスナップショット**] をクリックすると、スナップショットの進行状況とステータスを確認できます。

ステップ 2: スナップショットに基づいてイメージの作成

注意:

- システムディスクのデータを保持したくない場合は、この手順をスキップしてください。
- 現在のシステムディスクにデータを保持する場合は、システムディスク上のデータをコピーするイメージを作成必要があります。
- 容量不足でインスタンスが起動しない場合があるため、ディスク・スペースを十分に(最低 1GB) 確保してください。

ステップ 1 で作成したスナップショットを探し、**カスタムイメージの作成** をクリックします。

イメージの名前と説明を入力します。

ナビゲーションバーに戻り、**イメージ**をクリックします。

イメージ作成の進度とステータスを確認できます。

ステップ 3: システムディスクの変更

システムディスクを変更には:

ECS 管理コンソールにログインします。

左側のナビゲーションバーで [**インスタンス**] をクリックします。

該当リージョンを選択します。

システムディスクを変更する前にインスタンスを停止します。インスタンスリストで、システムディスクを交換するインスタンスを選択し、一番下の [**停止**] をクリックします。

インスタンスが停止したら、インスタンステーブルの右端で [**詳細**]、[**システムディスクの変更**] の順にクリックします。

カスタムイメージ をクリックし、ステップ 2 で作成したイメージを選択します。

[**変更の確認**] をクリックします。発生する支出があれば、支払います。

ステップ 4: 自動スナップショットポリシーの設定

システムディスクを変更すると、ディスクIDが変更されたため、設定した自動スナップショットポリシーは新しいシステムディスクでは作動しなくなります。この場合、新しいシステムディスクの自動スナップショットポリシーを設定する必要があります。詳細については、ディスクに対する自動スナップショットポリシーの設定 を参考ください。

ステップ 5: データディスクのアタッチ (Linux インスタンスの場合のみ)

Linux インスタンスの場合、システムディスクを変更した後、データディスクを再度アタッチする必要がありますが、パーティションを分割する必要はありません。詳細については データディスクのアタッチ を参考してください。

ディスクのモニタリング情報の表示

ディスクのモニタリング情報の表示

ディスクの IOPS、BPS などのモニタリング情報を表示することができます。

手順は次のとおりです。

1. ECS 管理コンソールにログインします。
2. モニタリング情報を表示するディスクを選択します。ディスクを特定する方法には、次の 2 つがあります。
   - インスタンスリストのページで、ディスクをアタッチするインスタンスをクリックしてから、[**インスタンスのディスク**] をクリックします。
   - [**ディスクリスト**] でディスクを特定します。
3. [**ディスクのモニタリング**] をクリックすると、IOPS、BPS などのモニタリング情報が表示されます。

注記:

右上隅にある時間の欄を使用して、1 時間、6 時間、1 日、7 日などのモニタリング期間を選択できます。また、モニタリングの開始時間および終了時間をカスタマイズして使用することもできます。

データディスクの削除

データディスクが不要になった場合は、以下を実行して削除することができます。

警告：データディスクの削除は恒久的な操作であり、元に戻すことはできません。一度削除すると、データディスク上の元のデータを復元することはできません。慎重に進めることをお勧めします。

前提条件

データディスクのステータスが **[利用可能]** になっていることを確認します。もし、ステータスが **[使用中]**の場合、ディスクをインスタンスからデタッチするを参照してください。

データディスクに格納されているデータが全てバックアップ済みであることを確認します。そうでない場合、スナップショットを作成して、データのバックアップを行ってください。

手順

データディスクのリリース手順は以下になります。

[ECS 管理コンソール] にログインします。

左側のナビゲーションバーで [**ディスク**] をクリックします。

該当リージョンを選択します。

削除したいディスクを確認し、[**詳細**]、[**削除**] の順にクリックします。

[**削除の確認**] をクリックして削除します。

上記の手順でデータディスクがリリースされます。

スナップショット

スナップショットの作成

手軽にインスタンスのスナップショットを作成して、ある時点のシステムデータのステータスを保存し、データバックアップとしたりイメージを作成したりすることができます。

注記:

- ディスクのスナップショットを初めて作成する場合は、フルスナップショットになるため、比較的長い時間がかかります。
- ディスクのスナップショットを追加で作成する場合、処理は早くなりますが、最後にスナップショットを作成した後に変更されたデータの量に応じて所要時間が変わります。変更されたデータが多ければ多いほど、処理時間は長くなります。
- スナップショットを作成中は、そのディスクのパフォーマンスがわずかに低下する場合があります。スナップショットを作成している間はディスクパフォーマンスが低下するため、業務に直接的な影響が及ぶ可能性があります。影響の程度は、変更されたデータ量に応じて変わります。業務のピーク時間にスナップショットを作成しないでください。
- 自動スナップショットとは異なり、手動で作成したスナップショットは手動で削除するまで保持されます。

手順は次のとおりです。

1. [**ECS 管理コンソール**] にログインします。
2. 左側のナビゲーションバーで [**ディスク**] をクリックします。ディスクのリストが表示されます。
3. スナップショットを作成するディスクを選択します。
4. 一度に選択できるディスクは 1 つだけです。システムディスクとデータディスクの両方を選択できます。
5. [**スナップショットの作成**] をクリックします。
6. スナップショット名を入力して、[**OK**] をクリックします。

左側のナビゲーションバーで [**スナップショット**] をクリックすると、すべてのスナップショットが表示されます。あるいは、[**インスタンス**]、[**インスタンスのスナップショット**] の順に移動すると、特定インスタンスのスナップショットが表示されます。

自動スナップショットポリシーの作成

ディスクに適用する自動スナップショットポリシーを作成し、自動スナップショットの作成日時、繰り返し

日、保持期間などのパラメーターを定義できます。各リージョンに最大 100 までの自動スナップショットポリシーの作成ができます。

手順は次のとおりです。

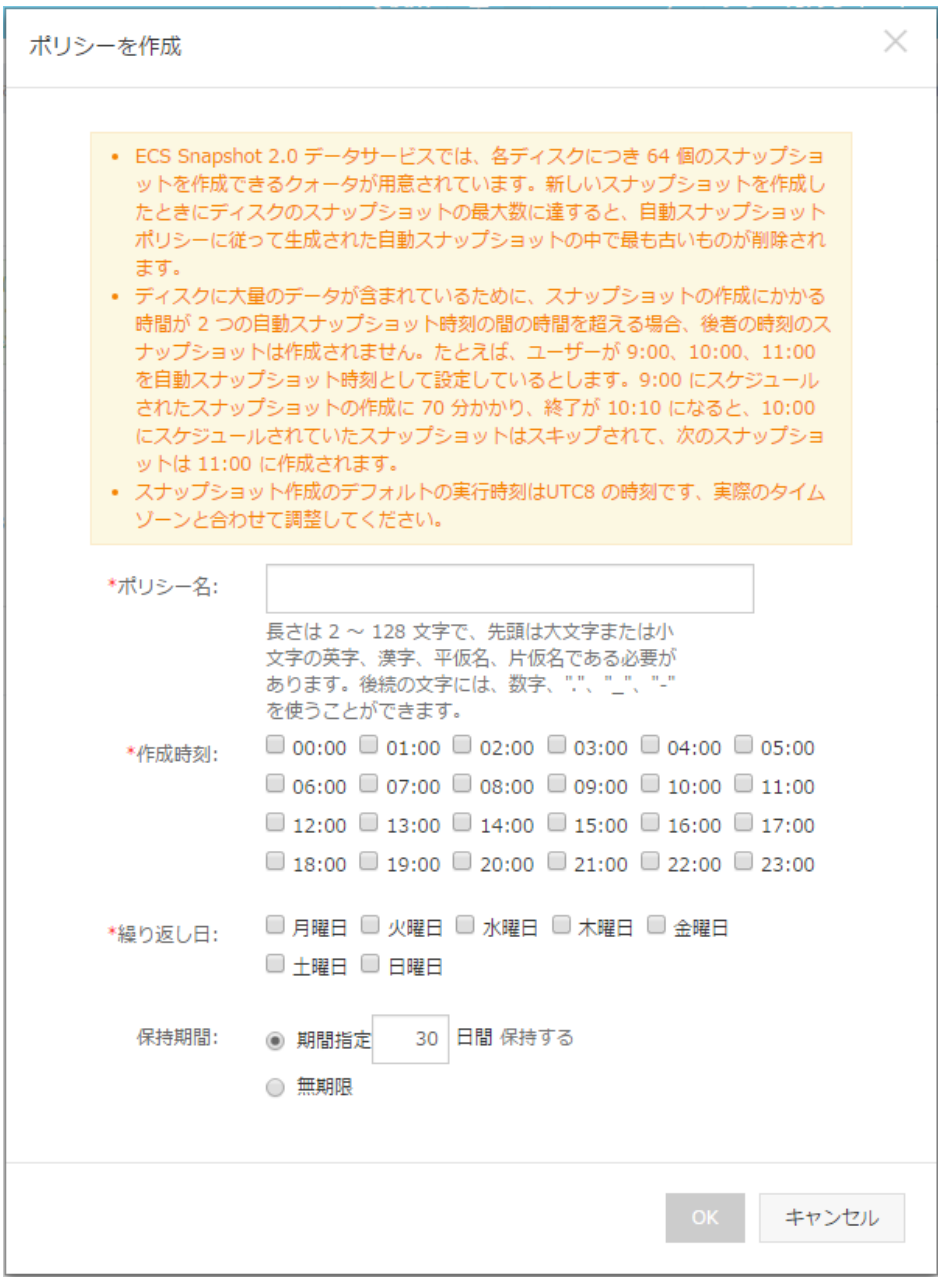
[**ECS 管理コンソール**] にログインします。

左側のナビゲーションバーで、[**スナップショット**]、[**自動スナップショットポリシー**] の順にクリックします。自動スナップショットポリシーのリストが表示されます。

右上の [**ポリシーを作成**] をクリックします。

自動スナップショットポリシーのパラメーターを定義します。

- ポリシー名: 自動スナップショットポリシーの名前です。長さは 2 ~ 128 文字にする必要があります。先頭の文字は大文字または小文字のアルファベットとする必要があります。数字、”_”、”-“を含めることができます。
- 作成時刻: 00:00 ~ 23:00 の 24 時点から、スナップショットの作成時点を指定します。
- 繰り返し日: 月~日までの 7 曜日から、毎週、作成を行う曜日を指定します。
- 期間: スナップショットを保持する日数を 1 ~ 65536 日で指定するか、永続的な保持を指定します。デフォルトは **30** 日です。
- 注意事項: スナップショット作成のデフォルトの実行時刻は **UTC+08:00** です。詳細は作成時刻と繰り返し日の設定に関する注意事項を参照してください。



その後、[OK] をクリックします。

自動スナップショットポリシーの削除

自動スナップショットポリシーが不要になった場合は、そのポリシーを特定し、右側の [**ポリシーの削除**] をクリックします。

ディスクに対する自動スナップショットポリシーの設定

ビジネスニーズに基づいて、ディスクに対する自動スナップショットポリシーを設定することができます。

注意:

- スナップショットの作成は、ディスクの読み書き操作を妨げる場合があります。サービスへの影響を小さくするために、自動スナップショットはサービスの負荷が少ない時間帯に実行することを強くお勧めします。
- 使用されていない汎用クラウドディスクに、自動スナップショットポリシーは適用されません。
- 手動で作成したスナップショットは、自動スナップショットと競合しません。ただし、ディスクが自動スナップショットを実行している場合は、それが完了するまで、手動によるスナップショットの作成を待機する必要があります。

ディスクまたはスナップショットを通じて、自動スナップショットポリシーを設定し実行することができます。

ディスク:
特定のディスクに自動スナップショットポリシーを適用します。

スナップショット:
複数またはすべてのディスクに、統一的な自動スナップショットポリシーを適用します。

ディスクを指定する方法

この方法では、特定のディスクに対する自動スナップショットポリシーを指定します。手順は次のとおりです。

1. ECS 管理コンソールにログインします。
2. 左側のナビゲーションバーで [**ディスク**] をクリックします。
3. リージョンを選択します。
4. ポリシーを実行するディスクを特定し、右側の [**自動スナップショットポリシーの変更**] をクリックします。
5. 自動スナップショット機能を有効にして、必要なスナップショットポリシーを選択することができます。
6. [**OK**] をクリックします。

スナップショットを指定する方法

この方法では、複数のディスクに対する自動スナップショットポリシーを指定します。

1. ECS 管理コンソール](https://ecs.console.aliyun.com/#/home “ECS Console”)にログインします。
2. 左側のナビゲーションバーで、[**スナップショット**]、[**自動スナップショットポリシー**] の順にクリ

ックします。
3. リージョンを選択します。このリージョンの自動スナップショットポリシーが、すべてリスト表示されます。

適用する自動スナップショットポリシーを特定し、右側の [**ディスクの設定**] をクリックします。

自動スナップポリシーを有効にする場合、[**ポリシーが事前設定されていないディスク**] タブをクリックし、目的のディスクを特定して、ディスクの右にある [**自動スナップショットの有効化**] をクリックします。または、複数のディスクを選択し、最下部の [**自動スナップショットの有効化**] をクリックします。

自動スナップポリシーを無効にする場合、[**ポリシーが事前設定されているディスク**] タブをクリックし、目的のディスクを特定して、ディスクの右にある [**自動スナップショットの無効化**] をクリックします。または、複数のディスクを選択し、最下部の [**自動スナップショットの無効化**] をクリックします。

ディスクリリースに伴う自動スナップショットリリースの設定

データディスクのリリース時に自動スナップショットを保持するよう指定すると、そのスナップショットを手動で設定できます。

[**ECS 管理コンソール**] にログインします。

リージョンを選択します。

左側のナビゲーションバーで [**クラウドディスク**] をクリックします。

設定するディスクを特定し、[**詳細**]、[**属性を変更**] の順にクリックします。

[**ディスクと共に自動スナップショットをリリース**] を選択またはキャンセルし、[**OK**] をクリックします。

スナップショットの削除

スナップショットまたは自動スナップショットポリシーを削除することができます。

スナップショットを削除する

スナップショットが不要になったとき、またはスナップショットクォータに達したときは、スナップショットを削除して領域を解放することができます。

注意：

- スナップショットの削除は永続的なアクションであり、元に戻すことはできません。削除が完了すると、元のスナップショットは復元できません。慎重に行ってください。
- スナップショットを使用してカスタムイメージを作成した場合は、スナップショットを削除する前に関連付けられたイメージを削除する必要があります。

スナップショットを削除するには、次の手順を実行します。

[**ECS管理コンソール**] にログオンします。

左側のナビゲーションバーの**スナップショット**> **スナップショット**をクリックします。

リージョンを選択します。

削除するスナップショットを選択します。

ウィンドウの下部にある[**削除**]をクリックします。

[**OK**]をクリックします。

自動スナップショットポリシーを削除する

[**ECS管理コンソール**] にログオンします。

左側のナビゲーションペインで、**スナップショットとイメージ**> **自動スナップショットポリシー**を選択します。

リージョンを選択します。

対象の自動スナップショットポリシーを見つけ、**アクション**列で**自動スナップショットポリシーの削除**をクリックします。

ダイアログボックスで情報を確認し、[**OK**]をクリックします。

作成時刻と繰り返し日の設定に関する注意事項

作成時刻と繰り返し日の設定に関する注意事項

スナップショット作成のデフォルトの実行時刻は **UTC+08:00** の時刻です。
UTC+08:00 以外の地域では、実際のタイムゾーンと合わせて調整する必要があります。

下記の 2 パターンでは **UTC+09:00(大阪、札幌、東京)タイムゾーン**のユーザの調整方法を説明します。

パターン1

スナップショットの希望作成時刻が【0:00以外】の場合

- 作成時刻： 希望作成時刻から 1 時間引いた時刻を設定します。
- 繰り返し日： 希望繰り返し日をそのまま設定します。（考慮する必要はありません）

希望作成時刻 UTC+09:00	**コンソール設定時刻 UTC+08:00**	**希望作成時刻 UTC+09:00**	**コンソール設定時刻 UTC+08:00**
1:00	0:00	13:00	12:00
2:00	1:00	14:00	13:00
3:00	2:00	15:00	14:00
4:00	3:00	16:00	15:00
5:00	4:00	17:00	16:00
6:00	5:00	18:00	17:00
7:00	6:00	19:00	18:00
8:00	7:00	20:00	19:00
9:00	8:00	21:00	20:00
10:00	9:00	22:00	21:00
11:00	10:00	23:00	22:00
12:00	11:00		

パターン2

スナップショットの希望作成時刻が【0:00】の場合

- 作成時刻： 希望作成時刻から 1 時間引き、【23:00】を設定します。
- 繰り返し日： 希望繰り返し日から 1 日前の曜日を設定します。

希望作成時刻 UTC+09:00	**コンソール設定時刻 UTC+08:00**

月曜日 0:00	日曜日 23:00
火曜日 0:00	月曜日 23:00
水曜日 0:00	火曜日 23:00
木曜日 0:00	水曜日 23:00
金曜日 0:00	木曜日 23:00
土曜日 0:00	金曜日 23:00
日曜日 0:00	土曜日 23:00

イメージ

カスタムイメージの作成

スナップショットからカスタムイメージの作成

カスタムイメージを使用すると、ECS インスタンスを効果的に実行できます。カスタムイメージにより、同一の OS と環境データで同時に複数の ECS インスタンスを有効化して、拡張ニーズに柔軟に応えることができます。

カスタムイメージは、ある時点での ECS システムディスクのスナップショットに基づいています。イメージに基づいて作成された複数の ECS インスタンスは、設定が同じ場合も異なる場合もあります。

考慮事項

カスタムイメージを作成する際には以下の制限があります。

- カスタムイメージの作成に使用された ECS の有効期限が切れた場合、またはデータが消去された (スナップショット用のシステムディスクの有効期限が切れるかリリースされた) 場合でも、イメージから作成されたカスタムイメージおよび ECS インスタンスは影響を受けません。ただし、自動スナップショットは、ECS インスタンスがリリースされるとクリアされます。
- カスタムイメージを使用することにより、有効化されている ECS インスタンスの CPU、メモリ、帯域幅、ハードドライブなどの設定をアップグレードすることができます。
- リージョンをまたいでカスタムイメージを使用することはできません。
- カスタムイメージは、年間または月間サブスクリプションか従量課金かを問わず、すべての ECS セールスモードに適用されます。年間または月間サブスクリプションプランにおける ECS インスタンスのカスタムイメージは従量課金インスタンスの作成に使用でき、その逆も同様です。

Linuxインスタンスからイメージを作成する際には、以下の点も制限となります。

- インスタンスが起動しなくなる可能性がありますので、 /etc/fstab は編集しないでください。
- カスタムイメージを作成する際にはすべてのデータディスクをアンマウントすることをお勧めします。
- rootユーザがログインできない状態で、カスタムイメージを作成しないでください。

操作手順

1. **[ECS 管理コンソール]** にログインします。
2. 左側のナビゲーションバーで、**[スナップショット]** をクリックします。スナップショットのリストが表示されます。
3. ページの一番上でリージョンを選択します。
4. ディスクの属性が **[システムディスク]** であるスナップショットを選択します。**[カスタムイメージの作成]** をクリックします。データディスクを使用してカスタムイメージを作成することはできません。

5. 表示されるダイアログボックスで、スナップショット ID を確認できます。
6. データディスクを含める場合、**[データディスクのスナップショットの追加]**を選択することで、複数のデータディスクをイメージに含めることができます。
   注記: ディスク容量を指定しない場合は、デフォルトで 5GB の容量で作成されます。利用可能なスナップショットを選択した場合は、ディスク容量はスナップショットと同じ大きさで作成されま

す。

7. カスタムイメージの名前と説明を入力します。**[作成]** をクリックします。
8. 作成したイメージを確認する場合は、左側のメニューから**[イメージ]**を選択します。

Linux インスタンスイメージのFAQ

ディスクのデタッチ方法およびディスクテーブルデータの削除方法

/dev/hda5 が /mnt/hda5 にアタッチされている場合、次の 3 つのコマンドのいずれかを実行してファイルシステムをデタッチできます。

```
umount /dev/hda5
umount /mnt/hda5
umount /dev/hda5 /mnt/hda5
```

/etc/fstab は、Linux の重要な設定ファイルです。ファイルシステムおよび起動時に接続されているストレージデバイスの詳細が含まれています。指定されたパーティションが VM の起動時にアタッチされることを避けるには、この設定ファイルから該当する行を削除する必要があります。たとえば、起動時に xvdb1 を切断するには、次のステートメントを削除します。

/dev/xvdb1 /leejd ext4 defaults 0 0

データディスクがデタッチされていてカスタムイメージを作成できるかどうかを判断

する方法

自動的にデータディスクをアタッチするステートメント行が fstab ファイルから削除されていることを確認する必要があります。mount コマンドを使用して、アタッチされているすべてのデバイスの情報を表示します。実行結果に、データディスクのパーティションに関する情報が含まれていないことを確認します。

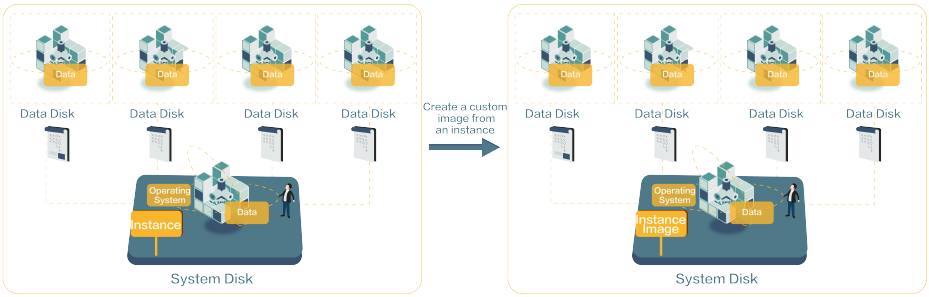
関連する設定ファイル

イメージを作成する前に、次の表に示す重要な設定ファイルが変更されていないことを確認します。変更されていると、新しいインスタンスを起動できません。

設定ファイル	目的	変更した場合のリスク
/etc/issue*, /etc/*-release, /etc/*_version	システムのリリースおよびバージョン	/etc/issue* を変更すると、システムのリリースバージョンを特定できなくなり、インスタンスの作成が失敗します。
/boot/grub/menu.lst, /boot/grub/grub.conf	システムの起動	/boot/grub/menu.lst を変更すると、カーネルのロードが失敗し、システムを起動できません。
/etc/fstab	起動時にパーティションをアタッチ	これを変更すると、パーティションのアタッチが失敗し、システムを起動できません。
/etc/shadow	システムパスワードの保存	このファイルを読み取り専用に設定すると、パスワードファイルを編集できなくなり、インスタンスの作成が失敗します。
/etc/selinux/config	システムのセキュリティポリシー	/etc/selinux/config を変更して SELinux を有効化すると、起動が失敗します。

インスタンスからカスタムイメージの作成

インスタンスからカスタムイメージを作成することができます。インスタンスのシステムディスクとデータディスクを含む全てのディスクをカスタムイメージに複製することが可能です。カスタムイメージを作成中、該当インスタンスの全てのディスクが自動的にスナップショットを作成し、これらのスナップショットが一つのカスタムイメージを構成します。



さらに、スナップショットに基づいてカスタムイメージを作成することもできます。「スナップショットを使用してカスタムイメージを作成する」を参照してください。

注意：

- データのプライバシー侵害を防ぐため、カスタムイメージを作成する前に、ECSインスタンス内のすべての機密データを削除してください。
- 作成中は、インスタンスの状態を変更しないでください。インスタンスを停止、開始、再起動しないでください。
- カスタムイメージにデータディスク上のデータが含まれている場合、ECSインスタンスとともに新しいデータディスクが一緒に作成されます。データディスク上のデータは、マウントデバイスに従って、カスタムイメージ内のデータディスクスナップショットを複製します。
- データディスク上のデータを含むカスタムイメージをエクスポートすることはできません。
- データディスク上のデータを含むカスタムイメージを使用して、システムディスクを置き換えることはできません。

操作手順：

コンソールにログインします。

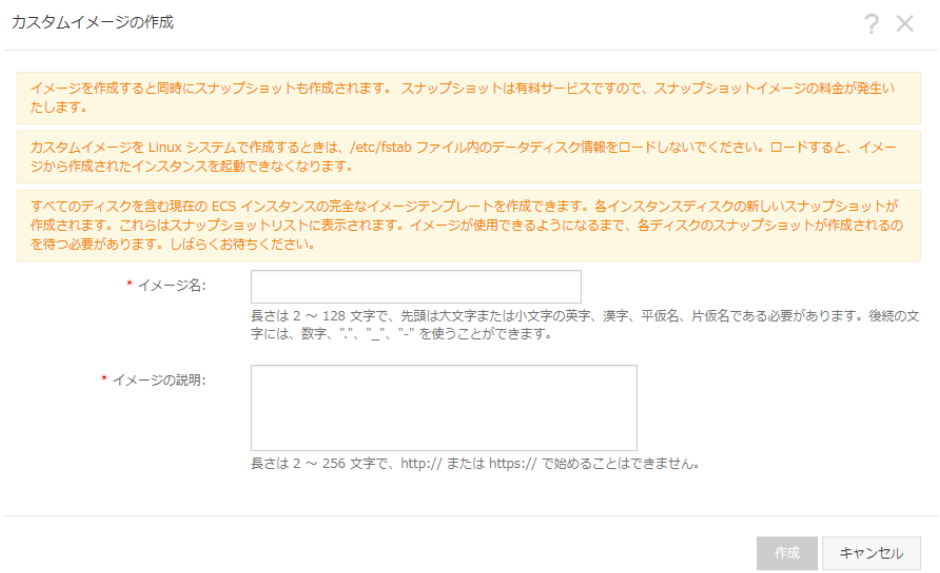
左側ナビゲーションの[**Elastic Compute Service**]、[**インスタンス**]の順でをクリックします。

インスタンスリストページで該当リージョンを選択します。

該当インスタンスを選択し、[**詳細**] - [**カスタムイメージの作成**]をクリックします。

カスタムイメージの作成画面で、イメージ名と説明を入力します。

[**作成**]をクリックします。



全てのディスクのスナップショットが作成後、イメージの使用が可能になります。

Packer を使ってカスタムイメージを作成

Packerは、カスタム画像を作成するのに便利なオープンソースのツールです。主要なオペレーティングシステム上で動作します。このドキュメントでは、Packerをインストールして使用する方法について説明します。Packerを使用すると、 1 行または 2 行のコマンドだけを使用して簡単にカスタムイメージを作成できます。

前提条件

AccessKeyを準備しておく必要があります。詳細は、 AccessKey作成を参照してください。

> 注 :
> AccessKeyには高いレベルのアカウント権限があります。不適切な操作やデータの破損を避けるために、RAMユーザーの作成を実行し、ユーザーのAccessKeyを作成するのRAMユーザーとして機能させることをお勧めします。

カスタム画像を作成する

ステップ1.Packerをインストールする

Packerの公式Packerのダウンロードページにアクセスして、お使いのオペレーティングシステム用の

Packerのバージョンを選択してダウンロードしてください。Packerのインストール方法については、以下の手順を実行するか、公式のPackerのインストールページを参照してください。

LinuxサーバにPackerをインストールするには

CentOS 6.8 64ビットの例

1. Linuxサーバーに接続してログオンします。接続先のサーバがECS Linuxインスタンスの場合は、Linuxインスタンスに接続を参照してください。

   cd / usr / local / binを実行して/ usr / local / binディレクトリに移動します。

   > **注**：/ usr / local / binディレクトリは環境変数ディレクトリです。Packerは、この ディレクトリまたは環境変数に追加された別のディレクトリにインストールできます。

3. wget https：// releases.hashicorp.com / packer / 1.1.1 / packer_1.1.1_linux_amd64.zipを実行して、Packerインストーラーをダウンロードしてください。Packerの他のバージョンのインストーラをダウンロードするには、Packerの公式のPacker のダウンロードページにアクセスしてください。
4. パッケージを解凍するには unzip packer_1.1.1_linux_amd64.zipを実行してください。
5. packer -vを実行して、Packerのインストール状況を確認します。Packerのバージョン番号が返された場合、Packerが正常にインストールされています。エラー command not foundプロンプトが返された場合、Packerは正しくインストールされていません。

WindowsサーバーにPackerをインストールするには

Windows Server 2012 64ビットの例

1. Windowsサーバーに接続してログオンします。接続先のサーバがECS Windowsインスタンスの場合は、Windowsインスタンスに接続を参照してください。
2. 公式のPackerのダウンロードページを開き、64ビットWindows用の適切なPackerインストーラを選択します。
3. パッケージを指定されたディレクトリに解凍し、Packerをインストールします。
4. PATH環境変数でPackerのディレクトリを定義します。
   i. **コントロールパネル**を開きます。
   ii. **すべてのコントロールパネル項目**> **システム**> **高度なシステム設定**を選択します。
   iii. **環境変数**をクリックします。
   iv. システム変数リストで**パス**を検索します。

   この例のように、 C：\ Packerに **Variable Value** にPackerインストールディレクトリを追加してください。複数のディレクトリを半角のセミコロン（；）で区切ります。 **OK** をクリックします。

   Packerのインストール状況を確認するには、CMDで packer.exe -vを実行してください。
   Packerのバージョン番号が返された場合、Packerが正常にインストールされています。エラー command not foundプロンプトが返された場合、Packerは正しくインストールされていません。

ステップ2. Packer テンプレートを定義する

Packerを使用してカスタムイメージを作成するには、まずJSON形式のテンプレートファイルを作成します。テンプレートでAlibaba Cloud イメージビルダーとプロビジョナを作成します。Packerには、カスタム画像のコンテンツ生成モードを設定するときに選択できる多様なプロビジョニング機能があります。次の alicloud JSONファイルでは、Shellプロビジョナを例としてPackerテンプレートの定義方法を示しています。

alicloudという名前のJSONファイルを作成し、次の内容を貼り付けます：

```
 {
"variables": {
"access_key": "{{env `ALICLOUD_ACCESS_KEY`}}",
"secret_key": "{{env `ALICLOUD_SECRET_KEY`}}"
},
"builders": [{
"type":"alicloud-ecs",
"access_key":"{{user `access_key`}}",
"secret_key":"{{user `secret_key`}}",
"region":"cn-beijing",
"image_name":"packer_basic",
"source_image":"centos_7_02_64_20G_alibase_20170818.vhd",
"ssh_username":"root",
"instance_type":"ecs.n1.tiny",
"internet_charge_type":"PayByTraffic",
"io_optimized":"true"
}],
"provisioners": [{
"type": "shell",
"inline": [
"sleep 30",
"yum install redis.x86_64 -y"
]
}]
}
```

注：次のパラメータの値をカスタマイズする必要があります。

パラメータ	説明
access_key	あなたのアクセスキー ID。
secret_key	あなたのシークレットキー。
region	カスタムイメージの作成に使用された一時インスタンスの領域。詳細は、リージョンとゾーンを参照してください。
image_name	カスタムイメージの名前。
source_image	Alibaba Cloudのパブリックイメージリストから基本イメージ名を取得できます。
instance_type	カスタムイメージを作成するために生成された一時インス

	タンスのタイプ。 詳細については、 インスタンスタイプファミリーを参照してください。
internet_charge_type	カスタムイメージを作成するために生成された一時インスタンスのインターネット帯域幅請求方法。オプションの値： - PayByTraffic - PayByBandwidth
provisioners	カスタムイメージの作成に使用されるPacker プロビジョナのタイプ

ステップ3.Packerを使用してカスタムイメージを作成する

次の手順に従って、Packerテンプレートファイルを指定してカスタムイメージを作成します。

1. export ALICLOUD_ACCESS_KEY=your AccessKeyIDコマンドでアクセスキーIDをインポートする。
2. export ALICLOUD_SECRET_KEY=your AccessKeySecretコマンドでシークレットキーをインポートする。
3. packer build alicloud.jsonコマンドでカスタムイメージを作成する。

サンプルは次のように実行されます。サンプルはApsaraDB for Redis含むカスタムイメージを作成し、次のように実行されます。

```
alicloud-ecs output will be in this color.

==> alicloud-ecs: Prevalidating alicloud image name...
alicloud-ecs: Found image ID: centos_7_02_64_20G_alibase_20170818.vhd
==> alicloud-ecs: Start creating temporary keypair: packer_59e44f40-c8d6-0ee3-7fd8-b1ba08ea94b8
==> alicloud-ecs: Start creating alicloud vpc
----------------------------
==> alicloud-ecs: Provisioning with shell script: /var/folders/3q/w38xx_js6cl6k5mwkrqsnw7w0000gn/T/packer-shell257466182
alicloud-ecs: Loaded plugins: fastestmirror
----------------------------
alicloud-ecs: Total 1.3 MB/s | 650 kB 00:00
alicloud-ecs: Running transaction check
----------------------------
==> alicloud-ecs: Deleting temporary keypair...
Build 'alicloud-ecs' finished.

==> Builds finished. The artifacts of successful builds are:
--> alicloud-ecs: Alicloud images were created:

cn-beijing: m-2ze12578be1oa4ovs6r9
```

＃＃ 次のステップ

このカスタムイメージを使用してECSインスタンスを作成できます。詳細については、カスタムイメージを

使用してインスタンスを作成するを参照してください。

参考文献

- 詳細については、Alibaba Cloud GithubのPackerリポジトリであるPacker-プロバイダを参照してください。
- Packerの使用方法の詳細については、Packer オフィシャルドキュメントを参照してください。

イメージのコピー

イメージをコピーすると、複数のリージョンをまたいでイメージを使用できます。

デフォルトでは、リージョンをまたいでカスタムイメージを使用することはできません。ただし、イメージをあるリージョンから別のリージョンにコピーすることはできます。これによって、バックアップイメージのシステムやまったく同じアプリケーション環境を別のリージョンでデプロイできます。

コピーに要する時間は、ネットワークの送信速度とタスクキュー内のタスク数によって決まるため、 慎重に操作の計画を立ててください。

手順

イメージをコピーするための手順は次のとおりです。

ECS 管理コンソールにログインします。

左側のナビゲーションバーで、[**イメージ**] をクリックします。イメージのリストが表示されます。

3. ページの一番上でリージョンを選択します。

コピーするイメージを選択します。イメージのタイプは、[**カスタムイメージ**] である必要があります。次に、イメージテーブルの右端にある [**イメージのコピー**] をクリックします。表示されるダイアログボックスで、イメージ ID を確認できます。

> カスタムイメージが100GB以上ある**イメージコピー**を実行したいときはチケットを起票してください。

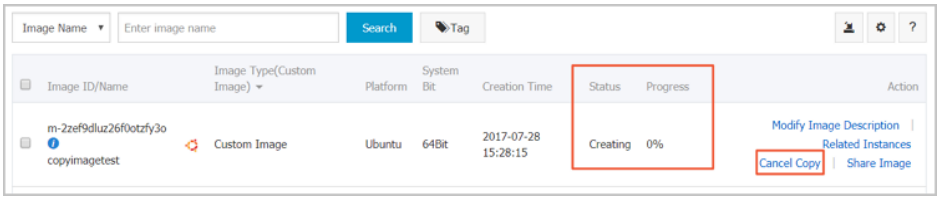
イメージのコピー先であるターゲットリージョンを指定します。

i. ターゲットリージョンを選択します。

ii. ターゲットイメージの名前と説明を入力します。今後の管理する上で名前をつけておくほうが良いでしょう。
iii. **OK**をクリックします。

ターゲットリージョンをクリックして進行状況を確認します。100%と表示されたらイメージコピーは完了です。

> 進行状況が100%ではなくイメージの作成状況が**作成中**になっている場合、**コピーのキャンセル**をクリックしてコピーをキャンセルできます。キャンセルするとイメージ情報はターゲットリージョンから削除されます。



イメージコピーのプロセスに関する詳細は「イメージコピーに関するFAQ」を参照してください。

イメージの共有

カスタムイメージを他のユーザーと共有できます。管理コンソールまたは ECS API を使用することにより、他のアカウントが自分と共有したイメージを照会できます。他のアカウントが共有したイメージを使用して ECS インスタンスを作成できます。

イメージを他のアカウントと共有する前に、そのイメージに機密性のある、または重要なデータやソフトウェアが含まれていないことを確認します。

注意: Alibaba Cloud は、他のアカウントが共有したイメージの完全性またはセキュリティを保証しません。信頼できるアカウントが共有したイメージだけを使用するように注意してください。そのようなイメージを使用して ECS インスタンスを使用する際は、必ず ECS インスタンスにログインして、イメージが安全かつ完全であることを確認します。

考慮事項

制約

- 1 つのイメージを、最大 **50** 人のユーザーと共有できます。
- 共有されたイメージは、イメージクォータの一部としては扱われません。
- 共有されたイメージを使用してインスタンスを作成できるのは、元のイメージと同じリージョンに

限られます。
- イメージを他のアカウントと共有できるのは、そのイメージのオーナーだけです。アカウント A のイメージをアカウント B と共有することはできません。

共有イメージの削除による影響

- カスタムイメージを他のアカウントと共有しても、そのイメージは削除できます。ただし、削除する前に、そのイメージとのすべての関係を削除する必要があります。
- カスタムイメージを共有したアカウントを削除すると、その共有イメージのユーザーは管理コンソールまたは ECS API を使用してイメージを見つけることも、イメージを使用して ECS インスタンスを作成することもできなくなります。
- 共有されたカスタムイメージを削除すると、そのイメージから作成した ECS インスタンスでシステムディスクの再初期化が失敗する可能性があります。

手順

コンソールを使用してイメージを共有する手順は次のとおりです。

1. [**ECS 管理コンソール**] にログインします。
2. 左側のナビゲーションバーで、[**イメージ**] をクリックします。イメージのリストが表示されます。
3. ページの一番上でリージョンを選択します。
4. 共有されたいイメージを選択します。イメージのタイプは、[**カスタムイメージ**] である必要があります。次に、[**イメージの共有**] をクリックします。
5. 表示されたダイアログボックスで、アカウントタイプを選択し、Alibaba Cloud アカウントを入力します。アカウントには次の 2 つのタイプがあります。
    - Alibaba Cloud アカウント: イメージを共有する相手ユーザーの Alibaba Cloud アカウント (ログインアカウント) を入力します。
    - Account ID: イメージを共有する相手ユーザーの Alibaba CloudID を入力します。Account ID は、Alibaba Cloud Web サイトのユーザーセンターで [**アカウント管理**]、[**セキュリティ設定**]、[**アカウントID**] の順にクリックすることによって取得できます。次のリンクからログインできます。
6. [**イメージの共有**] をクリックします。

共有のキャンセル

イメージを共有する許可はキャンセルできます。共有を無効にすると、そのアカウントはイメージの照会、使用ができなくなります。

注意: ECS インスタンスを作成するために他のアカウントが使用していたイメージの共有をキャンセルすると、そのインスタンスのシステムディスクを再初期化できなくなります。

手順は次のとおりです。

1. [**ECS 管理コンソール**]にログインします。

2. 左側のナビゲーションバーで、[**イメージ**] をクリックします。イメージのリストが表示されます。
3. ページの一番上でリージョンを選択します。
4. 共有を停止するイメージを選択します。イメージのタイプは、[**カスタムイメージ**] である必要があります。[**イメージの共有**] をクリックします。
5. このイメージを共有している相手ユーザーのリストを表示できます。アカウントの後ろの [**共有のキャンセル**] をクリックします。

共有しているユーザーのリストの表示

自分のイメージを共有している相手アカウントのリストを照会できます。

イメージを共有しているユーザーのリストをコンソールで照会する手順は、次のとおりです。

1. [**ECS 管理コンソール**] にログインします。
2. 左側のナビゲーションバーで、[**イメージ**] をクリックします。イメージのリストが表示されます。
3. ページの一番上でリージョンを選択します。
4. 表示するイメージを選択します。イメージのタイプは、[**カスタムイメージ**] である必要があります。[**イメージの共有**] をクリックします。
5. このイメージを共有している相手ユーザーのリストを表示できます。

共有されたイメージのリストの表示

他のユーザーから自分に共有されたイメージのリストを照会できます。

共有されているイメージのリストをコンソールで表示する手順は、次のとおりです。

1. [**ECS 管理コンソール**] にログインします。
2. 照会するリージョンを選択します。
3. イメージリストのヘッダーで、[**イメージタイプ**] として [**イメージの共有**] をクリックすると、他のアカウントが自分と共有したイメージのリストが表示されます。

イメージのインポート

イメージインポートの注意事項

インポートされたイメージの有用性を確保し、イメージのインポート効率を向上させるには、イメージをインポートする前に次の点に注意してください。

注意事項は、インスタンスのオペレーティングシステムによって異なります。

- For a Linux image
- For a Windows image

Linuxイメージをインポートする際の注意事項

Linuxイメージをインポートするときは、次の点に注意してください。

制限事項

パスワードの長さは8〜30文字で、3種類の文字（大文字、小文字、数字、特殊文字）が含まれている必要があります。

ファイアウォールは無効になっており、ポート22はデフォルトで有効になっています。

注意

Linuxイメージをインポートする場合は、以下表に記載されている注釈に注意する必要があります。

項目	標準オペレーティングシステムのイメージ	非標準オペレーティングシステムのイメージ
定義	Alibaba Cloudがサポートするオペレーティングシステムの公式ディストリビューションエディション: - CentOS 5,6,7 - Ubuntu 10,12,13,14 - Debian 6,7 - OpenSUSE 13.1 - SUSE Linux 10,11,12 - CoreOS 681.2.0+	非標準のオペレーティングシステムとは、次のいずれかを指します。 - Alibaba Cloudで現在サポートされているオペレーティングシステムのリストに含まれていないオペレーティングシステム - 重要なシステム構成ファイル、システムの基本環境、およびアプリケーションに関して、標準オペレ

		ーティングシステムの要件に準拠していない標準オペレーティングシステム。 非標準オペレーティングシステムのイメージを使用する場合は、次のもののみを選択することができます。 - カスタマイズされたLinux：カスタマイズされたイメージこのタイプのオペレーティングシステムのイメージをインポートすると、Alibaba Cloudはあらかじめ定義された設定基準に従って必要なネットワークまたはパスワードの設定を行います。設定の詳細については、カスタマイズされた Linuxの設定を参照してください。 - その他Linux：Alibaba Cloudは、これらのイメージすべてを他のシステムタイプとして識別します。このようなオペレーティングシステムのイメージをインポートすると、Alibaba Cloudは作成されたインスタンスに対して処理を実行しません。インスタンスの作成が完了したら、コンソールのManagement

		Terminal (VNC) を使用した ECS インスタンスへの接続 機能を使用してインスタンスに接続し、IPアドレス、ルーター、およびパスワードを手動で構成する必要があります。
重要なシステム構成ファイル	- /etc/issue*は変更しないでください。変更されていると、システムの配布を正しく認識できず、システム作成が失敗します。 - /boot/grub/menu.lstは変更しないでください。変更されていると、システムの起動に失敗することがあります。 - /etc/fstabは変更しないでください。これが変更された場合、例外が発生してパーティションがロードされず、システムの起動に失敗する可能性があります。 - /etc/shadowを読み取り専用に変更しないでください。変更されている場合、パスワードファイルは変更できず、システムの起動は失敗します。 - /etc/selinux/configを変更してSELinuxを有効にしないでくだ	標準オペレーティングシステムの要件に準拠していない。

	さい。変更されていると、システムの起動に失敗することがあります。	
システム基本環境の要件	- システムディスクのパーティションを調整しないでください。現在、単一のルートパーティションのみがサポートされています。 - システムディスクに十分な空き容量があることを確認してください。 - 重要なシステムファイル (/sbin, /bin, or /lib*) は変更しないでください。 - イメージをインポートする前に、ファイルシステムの整合性を確認してください。 - ファイルシステム：Linuxイメージは、ext3およびext4ファイルシステムのみをサポートします。MBRが使用されます。	標準オペレーティングシステムの要件に準拠していない。
アプリケーション	インポートしたイメージにqemu-gaをインストールしないでください。インストールされている場合、Alibaba Cloudが必要とするサービスの一部が利用できなくなることがあります。	標準オペレーティングシステムの要件に準拠していない。
ファイル形式	現在、RAW形式とVHD形式のみのイメージがサポートされています。他のフォーマットでイメージを取り込みたい場合は、イメージを取り込む前にuse a tool to convert the formatを使います。伝送容量の小さいVHD形式でイメージをインポートすることをお勧めします。	

ファイルサイズ	イメージをインポートするときのシステムディスクサイズの設定：イメージの仮想ファイルサイズ（使用法ではない）に基づいて、インポートするシステムディスクサイズを構成することをお勧めします。インポートするディスクのサイズは40 GBから500 GBでなければなりません。

Windowsイメージをインポートする際の注意事項

Windowsイメージをインポートするときは、次の注意に注意してください。

制限事項

イメージのインポートでは、複数のネットワークインターフェイスまたはIPv6アドレスの使用はサポートされていません。

パスワードの長さは8〜30文字で、3種類の文字（大文字、小文字、数字、特殊文字）が含まれている必要があります。

XENおよびKVM仮想化プラットフォームドライバをインストールする必要があります。

ファイアウォールは無効になっており、ポート3389はデフォルトで有効になっています。

Windowsオペレーティングシステムのディストリビューションエディション

以下のWindowsオペレーティングシステムのディストリビューションエディションをインポートすることができます。

Microsoft Windows Server 2012 R2 (Standard Edition)

Microsoft Windows Server 2012 (Standard Edition, Data Center Edition)

Microsoft Windows Server 2008 R2 (Standard Edition, Data Center Edition, Enterprise Edition)

Microsoft Windows Server 2008 (Standard Edition, Data Center Edition, Enterprise Edition)

Microsoft Windows Server 2003 (Standard Edition, Data Center Edition, Enterprise Edition), including R2 and with Service Pack 1 (SP1)

Microsoft Windows Server 2003 with Service Pack 1 (SP1) (Standard Edition, Data Center Edition, Enterprise Edition)

注意: Windows XP、Windows 7（Professional EditionとEnterprise Editionの両方）、Windows 8、およびWindows 10はサポートされていません。

システム基本環境の要件

システムディスクと複数のパーティションがサポートされています。

システムディスクに十分な空き容量があることを確認してください。

重要なシステムファイルを変更しないでください。

イメージをインポートする前に、ファイルシステムの整合性を確認してください。

ファイルシステム：NTFSファイルシステムとMBRのみがサポートされています。

アプリケーション

インポートしたイメージにqemu-gaをインストールしないでください。インストールされている場合、Alibaba Cloudが必要とするサービスの一部が利用できなくなることがあります。

サイズとフォーマット

現在、RAW形式とVHD形式のみのイメージがサポートされています。他のフォーマットでイメージを取り込みたい場合は、イメージを取り込む前に イメージファイル形式の変換 を使います。伝送容量が小さいVHD形式でイメージをインポートすることをお勧めします。

イメージをインポートするときのシステムディスクサイズの設定：イメージの仮想ファイルサイズ（使用法ではない）に基づいて、インポートするシステムディスクサイズを構成することをお勧めします。インポートするディスクのサイズは、40 GBから500 GBでなければなりません。

cloud-init のインストール

インポートされたイメージのホスト名、NTP ソース、および yum ソースの設定を正しく行うために、イメージをインポートする前に、オンプレミスサーバ、仮想マシン、またはクラウドホストに cloud-init をインストールすることをお勧めします。

現在、cloud-init は以下の Linux ディストリビューションをサポートしています：

- CentOS
- Debian
- Fedora
- FreeBSD
- Gentoo
- RHEL（Red Hat Enterprise Linux）
- SLES（SUSE Linux Enterprise Server）
- Ubuntu

前提条件

次のプログラムがインストールされていることを確認してください。

git：cloud-init のソースコードパッケージをダウンロードします。

コマンド： yum install git

python2.7：cloud-init の実行とインストールの基礎です。

コマンド： yum install python

pip：python2.7 にはないが、cloud-init が依存しているライブラリをインストールします。

コマンド： yum install python-pip

このドキュメントでは、インストールを説明するために yum を例として使用します。パッケージを管理するために zypper または apt-get を使用している場合、インストール方法は同様になります。

cloud-init のインストール

cloud-init をインストールするには、次の手順を実行します。

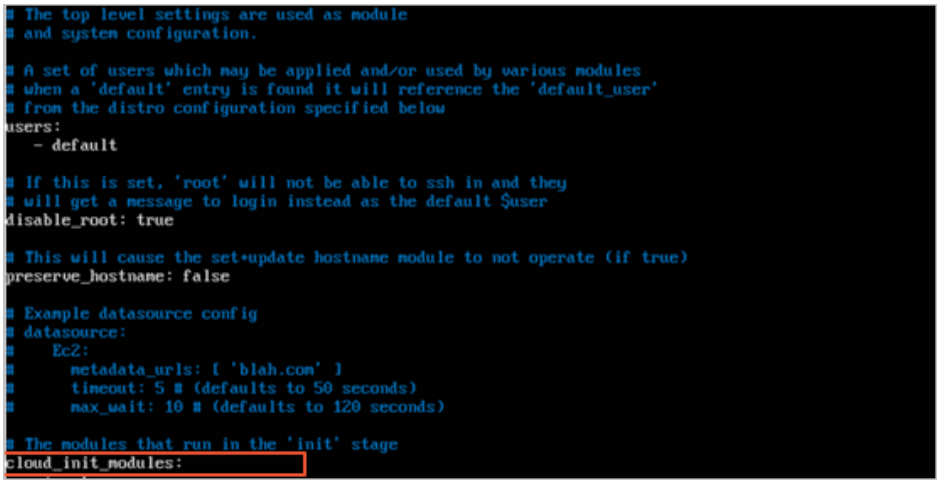
オンプレミスサーバー、仮想マシン、またはクラウドホストに接続します。クラウドホストがECS インスタンスの場合は、Linux インスタンスへのログインを参照してください。

git clone https://git.launchpad.net/cloud-init を実行して、公式サイトから cloud-init のソースコードパッケージをダウンロードしてください。

cd cloud-init を実行して、ディレクトリを cloud-init に変更します。

python setup.py install を実行して、setup.py をインストールします。これは、cloud-init のインストールファイルです。

vi/etc/cloud/cloud.cfg を実行して、設定ファイル cloud.cfg を変更します。



cloud_init_modules の前の内容を以下のように変更してください。

```shell
# Example datasource config
# The top level settings are used as module
# and system configuration.

# A set of users which may be applied and/or used by various modules
# when a 'default' entry is found it will reference the 'default_user'
# from the distro configuration specified below
users:
- default

user:
name: root
lock_passwd: False

# If this is set, 'root' will not be able to ssh in and they
# will get a message to login instead as the above $user
disable_root: false
```

```
# This will cause the set+update hostname module to not operate (if true)
preserve_hostname: false

syslog_fix_perms: root:root

datasource_list: [ AliYun ]

# Example datasource config
datasource:
AliYun:
support_xen: false
timeout: 5 # (defaults to 50 seconds)
max_wait: 60 # (defaults to 120 seconds)
# metadata_urls: [ 'blah.com' ]

# The modules that run in the 'init' stage
cloud_init_modules:
```

トラブルシューティング

注：欠落しているライブラリは、オペレーティングシステムによって異なる場合があります。 pip を使用して不足しているライブラリをインストールすることができます。不足しているライブラリをインストールした後、再度 python setup.py install を実行して setup.py をインストールしてください。

1. ライブラリ6またはライブラリoauthlibがありません。

インストール中に、以下のメッセージが表示されることがあります。 つまり、6つのライブラリが Python にないということです。pip install six を実行して6つのライブラリをインストールします。

```
File "/root/cloud-init/cloudinit/log.py", line 19, in <module>
import six
ImportError: No module named six
)
```

2. インストール中にエラーが発生すると、ライブラリは指定されません。

エラー出力に従って依存関係ライブラリが指定されていない場合、 pip install -r requirements.txt を実行して、cloud-initの requirements.txt ファイルにリストされているすべての依存関係ライブラリをインストールすることができます。

次のステップ

ECS コンソールでイメージのインポートを行うことができます。

イメージ形式の変換

RAW または VHD 形式の画像ファイルのみをインポートできます。他のフォーマットでイメージをインポートする場合は、イメージをインポートする前にフォーマットを変換してください。

このドキュメントでは、qemu-img ツールを使用してイメージファイルを RAW、Qcow2、VMDK、VDI、VHD（vpc）、VHDX、qcow1、QED などの VHD または RAW 形式に変換する方法を紹介します。

さまざまな方法で qemu-img をインストールし、ローカルコンピュータのオペレーティングシステムに基づいてイメージファイル形式を変換することができます。

- Windows
- Linux

Windows

Windows システムに qemu-img をインストールしてイメージファイル形式を変換するには、次の手順を実行します。

1. qemu をダウンロードしてインストールします。ダウンロードアドレス：https://qemu.weilnetz.de/w64/ 。インストールパス：C:\Program Files\qemu。

2. 次の手順を実行して環境変数を作成します（Windows 7 の場合）。

   i. **スタート**> **コンピュータ**を選択し、**プロパティ** を右クリックします。
   ii. 左側のナビゲーションペインで、**高度なシステム設定** をクリックします。
   iii. **システムの属性** ダイアログボックスで、 **詳細設定** タブをクリックし、**環境変数**をクリックします。
      a. **環境変数**ダイアログボックスの**システム変数**で **Path** 変数を見つけ、 **編集** をクリックします。 **Path** 変数が存在しない場合は、 **新規** をクリックします。
      b. 変数値を追加します。
         a. **システム変数の編集**： *C:\Program Files\qemu* を**変数値**に追加します。異なる変数値は、セミコロン（;）で区切られます。
         b. **新しいシステム変数**：**変数名**として *Path* を入力し、**変数値**として *C:¥Program Files¥qemu* を入力します。

Windowsで**コマンド**プロンプトを開き、 qemu-img --helpコマンドを実行します。表示されたら、インストールは成功しています。

コマンドのプロンプトで、 cd [ソースイメージファイルのディレクトリ]コマンドを実行してディレクトリを変更します。たとえば、 cd D:\ ConvertImageのようになります。

コマンドプロンプトで次のコマンドを実行して、イメージファイル形式を変換します。

```
qemu-img convert -f raw -O qcow2 centos.img centos.qcow2
```

コマンドパラメータは次のように記述されています。

- -fの後にソースイメージ形式が続きます。
- -O（大文字が必要です）の後に、変換されたイメージ形式、ソースファイル名、およびターゲットファイル名が続きます。

Linux

qemu-img をインストールしてイメージファイル形式を変換するには、次の手順を実行します。

qemu-img をインストールします。例：

- Ubuntu の場合、 apt install qemu-imgコマンドを実行します。
- CentOS の場合、 yum install qemu-imgコマンドを実行します。

次のコマンドを実行してイメージファイル形式を変換します。

```
qemu-img convert -f raw -O qcow2 centos.img centos.qcow2
```

コマンドパラメータは次のように記述されています。

- -fの後にソースイメージ形式が続きます。
- -O（大文字が必要です）の後に、変換されたイメージ形式、ソースファイル名、およびターゲットファイル名が続きます。

イメージのインポート

物理イメージファイルを ECS 環境にインポートして、カスタムイメージを作成することができます。その後、このイメージを使用して ECS インスタンスを作成できます。

注意: インポートイメージ機能を使用したい場合は、機能を有効するようにサポートチケットを起票してください。

前提条件

- 制限事項や要件については、イメージインポートの注意事項、カスタマイズされたLinuxの設定、イメージ形式の変換 を参照してください。
- OSS を有効化していない場合は、最初に「OSS の有効化」を参照してください。イメージをインポートするには、手動で公式 ECS サービスアカウントに OSS アクセス権限を与える必要があります。
- 同じリージョンの OSS のイメージファイルのみをインポートすることができます。イメージと OSS は 1 つのアカウントに属している必要があります。
- OSS のサードパーティツールクライアント、OSS API、または OSS SDK を使用して、インポートする ECS カスタムイメージと同じリージョン内のバケットにファイルをアップロードします。

操作手順

ECS 管理コンソールにログインします。

左側のナビゲーションバーで、[**スナップショット & イメージ**] > [**イメージ**] をクリックします。

[**イメージのインポート**] をクリックします。

[**イメージのインポート手順**] の三行目にある [**アドレスの確認**] をクリックします。

[**権限付与に同意**] をクリックします。

左側のナビゲーションバーで、[**スナップショット & イメージ**] > [**イメージ**] をクリックします。

リージョンを選択します。

[**イメージのインポート**] をクリックし、イメージインポートフォームに記入します。

イメージのリージョン:
アプリケーションをデプロイするリージョンを選択します。

OSSオブジェクトアドレス：
OSS コンソールからオブジェクトのアドレスをコピーします。

イメージ名:
長さは 2 ~ 128 文字です。先頭には、大文字または小文字の英字、または漢字を使います。数字、”_”、”-“を含めることができます。

オペレーティングシステム:
現在サポートされている OS リリース:

- Windows
- Linux

システムディスクのサイズ:

- Windows システムディスクのサイズ: 40 ~ 500 GB、
- Linux システムディスクのサイズ: 20 ~ 500 GB。

システムアーキテクチャ:
64 ビット OS: x86_64、32 ビット OS: i386。

システムプラットフォーム
現在サポートされている OS リリース:

- Windows: Windows Server 2003、Windows Server 2008、Windows Server 2012
- Linux: CentOS、SUSE、Ubuntu、Debian、FreeBSD、CoreOS
  注意:
  - (Linux エディションのみ) サポートされているエディションを確認するにはチケットを送信してください。
  - イメージの OS が Linux コア上で開発されたカスタムエディションである場合は、チケットを送信して Alibaba Cloud に連絡してください。

イメージの形式:
RAW 形式と VHD パーティションがサポートされます。成功率を高めるために、RAW 形式を使用することをお勧めします。
注意:QEMU イメージを使用して VHD イメージを作成することはできません。

イメージの説明:
イメージの説明を入力します。

[OK] をクリックしてイメージインポートタスクを作成します。

注意:イメージのインポートには、通常は 1-4 時間かかります。タスクにかかる時間は、イメージファイルのサイズと、同時に実行中の他のインポートタスクの数に依存します。タスクの進捗は、インポート領域のイメージリスト内で確認できます。

また、タスクマネージャでイメージインポートタスクを見つけて、キャンセルすることもできます。

次の操作手順

カスタマイズイメージをインポート完了後、イメージを使用したインスタンスの作成 を参照してください。

virtio ドライバーのインストール

サーバー、仮想マシン、またはクラウドホストの イメージのインポート により作成された Linux インスタンスの起動失敗を回避するには、Xen(pv) または virtio ドライバーをオンプレミスにインストールする必要があります。次の手順に従って、ドライバを手動でインストールする必要があるかどうかを確認し、必要に応じて Linux サーバ用の virtio ドライバをインストールして設定します。

手動インストール不要のイメージ

下記のオペレーティングシステムがインポートされた場合、Alibaba Cloud によって自動的に virtio ドライバが処理されますので、一時ファイルシステム（ initramfs、initrd ）の修復 部分から確認してください。

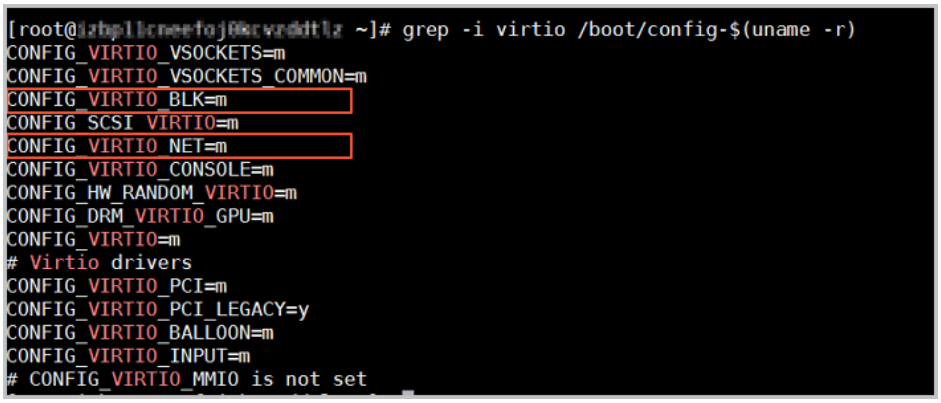
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016
- CentOS 6/7
- Ubuntu 12/14/16
- Debian 7/8/9
- SUSE 11/12

手動インストール必要のイメージ

前述のリストに含まれていない Linux イメージの場合は、イメージをインポートする前にオンプレミスの virtio ドライバをインストールする必要があります。

サーバ上の virtio ドライバの可用性のチェック

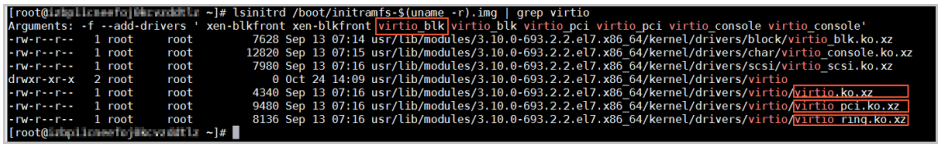
virtio ドライバがすでにサーバのカーネルに組み込まれているかどうかを調べるには grep -i virtio /boot/config-$(uname -r)を実行します。



説明:

- **説明 1**. 出力に VIRTIO_BLKとVIRTIO_NETが存在しない場合、virtio ドライバはカーネルに組み込まれておらず、virtio ドライバのインストールと設定 を実行する必要があります。
- **説明 2**. CONFIG_VIRTIO_BLKとCONFIG_VIRTIO_NETの値が yの場合、virtio ドライバはすでにカーネルに組み込まれています。イメージインポートの注意事項 を確認し、イメージのインポート を実行することができます。
- **説明 3**.CONFIG_VIRTIO_BLKとCONFIG_VIRTIO_NETの値が mの場合、ステップ2に進みます。

lsinitrd /boot/initramfs-$(uname -r).img | grep virtio を実行します。 virtio ドライバが一時ファイル initramfs、initrd に含まれるかどうかを確認します。



説明 :

- **説明 1** 上図のように、virtio_blk ドライバ(その依存関係 virtio.ko、virtio_pci.ko、および virtio_ring.ko) は一時ファイル initramfs に含まれる場合、イメージインポートの注意事項 を確認し、イメージのインポート を実行することができます。
- **説明 2** 一時ファイル initramfs に virtio ドライバが含まれてない場合、イメージをインポートする前に 一時ファイルシステム（ initramfs、initrd ）の修復 する必要があります。

一時ファイルシステムの修復

virtio ドライバがカーネルでサポートされますが、一時ファイルシステムに含まれてない場合は、一時ファイルシステムの修復する必要があります。修復の例を説明します。

- **CentOS/RedHat 5**

```
mkinitrd -f --allow-missing \
```

```
--with=xen-vbd --preload=xen-vbd \
--with=xen-platform-pci --preload=xen-platform-pci \
--with=virtio_blk --preload=virtio_blk \
--with=virtio_pci --preload=virtio_pci \
--with=virtio_console --preload=virtio_console \
```

- **CentOS/RedHat 6/7**

```
mkinitrd -f --allow-missing \
--with=xen-blkfront --preload=xen-blkfront \
--with=virtio_blk --preload=virtio_blk \
--with=virtio_pci --preload=virtio_pci \
--with=virtio_console --preload=virtio_console \
/boot/initramfs-$(uname -r).img $(uname -r)
fi
```

- **Debian/Ubuntu**

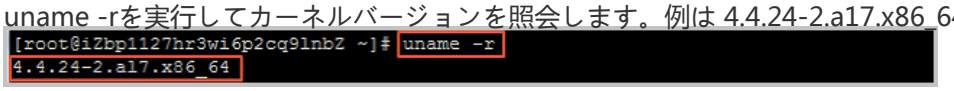
```
echo -e 'xen-blkfront\nvirtio_blk\nvirtio_pci\nvirtio_console' >> \
/etc/initramfs-tools/modules
mkinitramfs -o /boot/initrd.img-$(uname -r)"
```

virtio ドライバのインストール

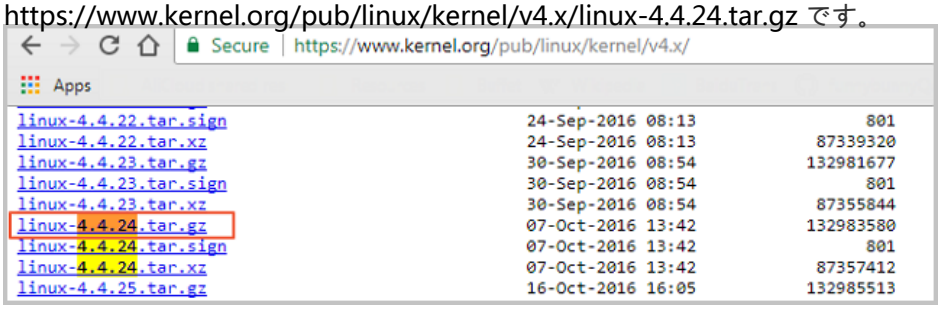
Redhat の例を説明します。

カーネルパッケージのダウンロード

1. カーネルをコンパイルするのに必要なコンポーネントをインストールするには yum install -y ncurses-devel gcc make wgetを実行します。
2. uname -rを実行してカーネルバージョンを照会します。例は 4.4.24-2.a17.x86_64 となります。



3. Linux カーネルアーカイブ から該当バージョンのカーネルソースをダウンロードします。例、カーネルバージョン 4.4.24 のダウンロートリンクは https://www.kernel.org/pub/linux/kernel/v4.x/linux-4.4.24.tar.gz です。



4. cd /usr/src/を実行してディレクトリを変更します。
5. インストールパッケージをダウンロードするには、 wget https://www.kernel.org/pub/linux/kernel/v4.x/linux-4.4.24.tar.gzを実行します。

6. tar -xzf linux-4.4.24.tar.gzを実行してパッケージを解凍します。
7. ln -s linux-4.4.24 linuxを実行してリンクを作成します。
8. cd /usr/src/linuxを実行してディレクトリを変更します。

カーネルのコンパイル

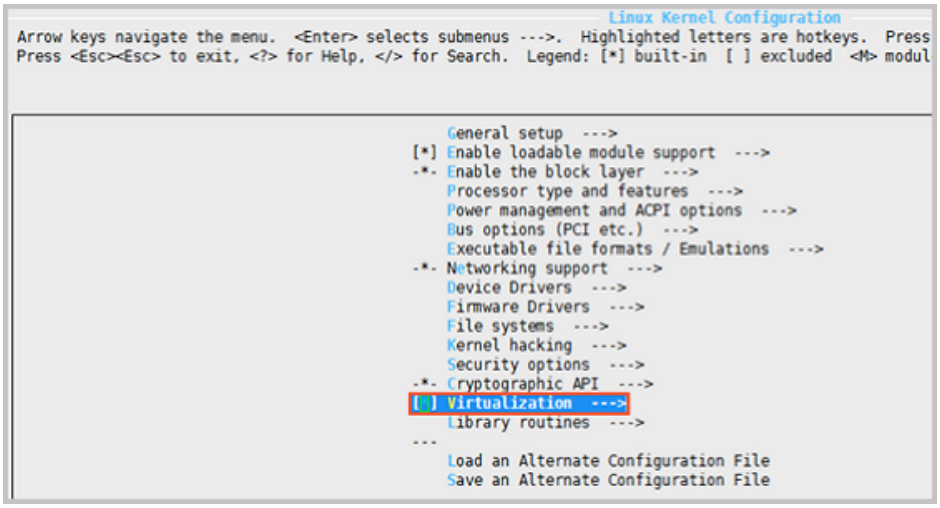
次のコマンドを実行して、ドライバをカーネルにコンパイルします。

```
make mrproper
symvers_path=$(find /usr/src/ -name "Module.symvers")
test -f $symvers_path && cp $symvers_path .
cp /boot/config-$(uname -r) ./.config
make menuconfig
```

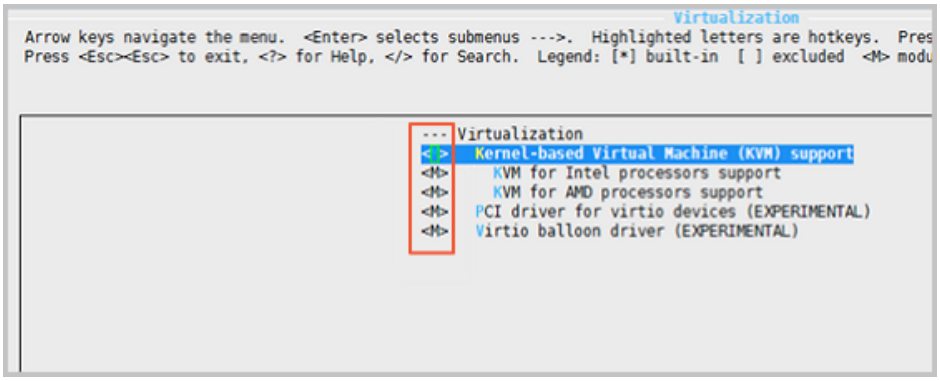
以下のウィンドウで、virtio ドライバの対応する設定を行います。

注意：ドライバをカーネルにコンパイルするには *を選択します。ドライバをモジュールとしてコンパイルするには mを選択します。

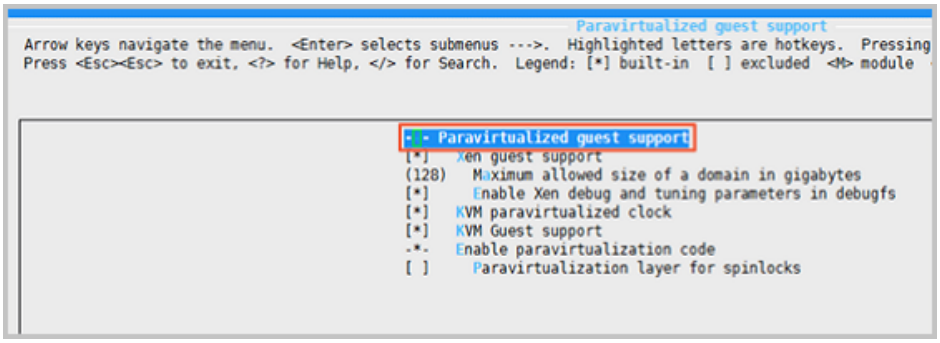
スペースバー を押して **Virtualization** を選択します。



KVM(Kernel-based Virtual Machine)のオプションを選択していることを確認します。




```
 Processor type and features  --->
[*] Paravirtualized guest support --->
--- Paravirtualized guest support
(128) Maximum allowed size of a domain in gigabytes
[*] KVM paravirtualized clock
[*] KVM Guest support
```




```
 Device Drivers  --->
[*] Block devices --->
<M> Virtio block driver (EXPERIMENTAL)
-*- Network device support --->
<M> Virtio network driver (EXPERIMENTAL)
```

** Escキーを押してカーネル設定ウィンドウを終了し、.configファイルに保存します。

virtio ドライバのすべての設定が正しく構成されているかどうかを確認します。

(オプション) 確認後、virtio ドライバの設定が完了してない場合は、次のコマンドを実行して .configファイルを手動で編集します。

```
 make oldconfig
make prepare
make scripts
make
make install
```

virtio ドライバのインストール状況は、次のコマンドで確認できます。

```
find /lib/modules/"$(uname -r)"/ -name "virtio.*" | grep -E "virtio.*"
grep -E "virtio.*" < /lib/modules/"$(uname -r)"/modules.builtin
```

出力に virtio_blk と virtio_pci.virtio_console が含まれている場合、 virtio ドライバは正しくインストールされています。

フォローアップ作業

virtio ドライバをインストール後：

- Alibaba Cloud コンソールに イメージのインポート を実施できます。

カスタムイメージの名前と説明の変更

カスタムイメージの名前と説明の変更

カスタムイメージの説明および名前は、いつでも変更できます。

手順は次のとおりです。

1. ECS 管理コンソールにログインします。
2. 左側のナビゲーションバーで、[**イメージ**] をクリックします。イメージのリストが表示されます。
3. ページの一番上でリージョンを選択します。
4. 編集するイメージを選択します。イメージのタイプは、[**カスタムイメージ**] である必要があります。
5. 名前の変更: イメージ名の上にマウスを移動します。小さいペンアイコンが表示されます。このアイコンをクリックしてイメージ名を変更します。
6. 説明の変更: [**イメージの説明の変更**] をクリックします。

7. [**保存**] をクリックします。

カスタムイメージの削除

不要になったカスタムイメージを削除することができます。

手順

ECS コンソールにログオンします。

左側のナビゲーションペインで、**スナップショット&イメージ> イメージ**を選択します。

リージョンを選択してください。

削除するイメージを選択します。

注：イメージタイプは**カスタムイメージ**でなければなりません。

削除をクリックします。

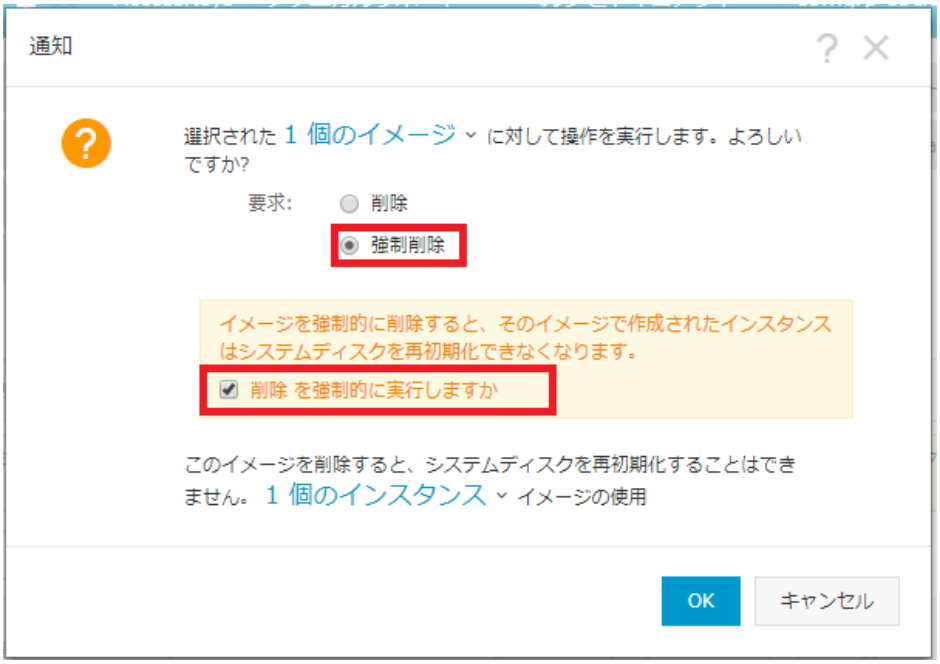
ダイアログボックスで、 [OK] をクリックします。

よくある質問

ECS インスタンスが作成された特定のカスタムイメージを削除できます

か？

はい、**イメージを強制的に削除**することができます。ただし、カスタムイメージが削除された後、インスタンスのシステムディスクを再初期化することはできません。



カスタムイメージのエクスポート

イメージエクスポート機能は、テスト目的またはオフラインプライベートクラウドにカスタムイメージをローカルデバイスにエクスポートする際に使用します。このドキュメントでは、イメージのエクスポート機能の制約と制限について説明し、ECS コンソールでイメージをエクスポートする方法について説明します。

> **注意**:エクスポートされた画像は、カスタムイメージとして同じリージョンである OSS バケットに保存されています。OSS のストレージとダウンロードのトラフィック料金が生成されます。

制限

現在、イメージエクスポート機能には次の制約と制限があります。

- イメージエクスポート機能を使用するには、ホワイトリストに登録が必要です。
- システムディスクスナップショットによって作成されたカスタムイメージをマーケットプレイスか

らエクスポートすることはできません。

データディスクの4つのスナップショットを含むカスタムイメージをエクスポートすることができます。単一データディスクの場合、最大ボリュームは100 GB 未満である必要です。

エクスポートされたイメージファイルのデフォルトの形式は RAW です。

前提条件

チケット を起票し、イメージのエクスポート機能を有効にします。

OSS の有効化とリージョンカスタムイメージが配置されている場所と利用できる OSS のバケットを確認します。OSS の作成方法についてはバケットの作成を参照してください。

カスタムイメージのエクスポート

カスタムイメージをエクスポートするには、次の手順を実行します。

[ECS コンソール]にログインします。

以下の手順に従って、ECS インスタンス ID に OSS リソースへのアクセスを許可します。

i. 左側のナビゲーションペインで**[スナップショット&イメージ]**> **[イメージ]**を選択します。
ii. リージョンを選択します 。
iii. エクスポートするカスタムイメージを探します。**[アクション]**列で、**[イメージのエクスポート]**をクリックします。
iv. **[イメージのエクスポート]**ダイアログボックスで、**[アドレスの確認]**をクリックします。
v. **[クラウドリソースアクセス権限付与]**ウィンドウで、**[権限付与に同意]**をクリックします。ECS コンソールのホームページに戻ります。

左側のナビゲーションペインで、**[スナップショット&イメージ]**> **[イメージ]**を選択します。

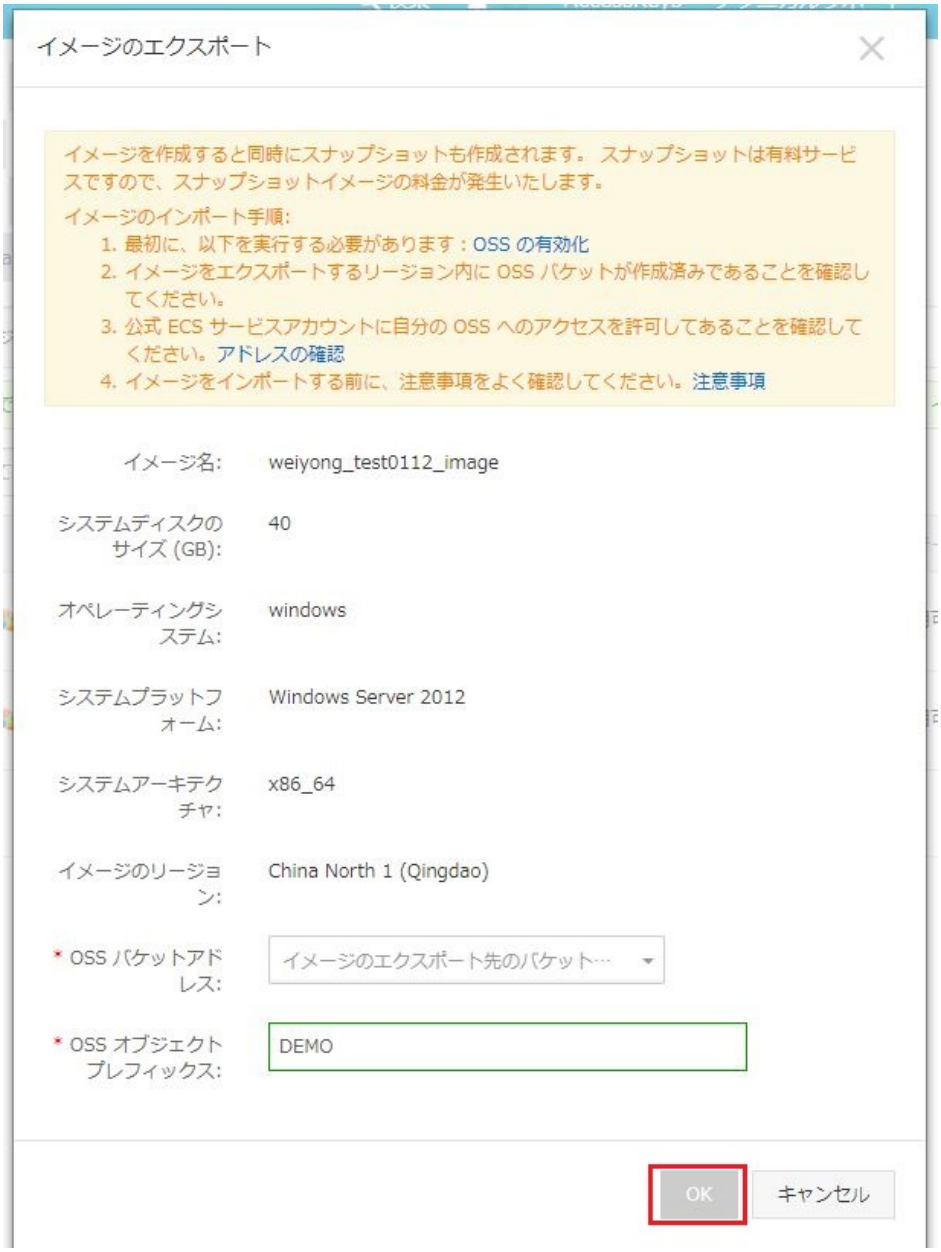
リージョンを選択します 。

エクスポートするカスタムイメージを探します。**[アクション]**列で、**[イメージのエクスポート]**をクリックします。

イメージのエクスポートダイアログボックスで、

- 指定されたリージョンにおける OSS のバケットを選択します。
- エクスポートされたイメージのオブジェクト名のプレフィックスを設定します。接頭辞としてデモを設定した場合、エクスポートした画像ファイルは、OSS バケットで Demo-[自動的に生成されたファイル名]という名前が付けられます。

画像をエクスポートするには、**OK**をクリックしてください。



エクスポートの継続時間は、イメージファイルのサイズとキュー内の他のエクスポートタスクの数によって異なります。エクスポートが完了するまで待ちます。タスク ID に基づいてタスクの進捗状況を照会するには、ECS コンソールの**タスクの管理**ページに移動します。**タスクのステータス**が**タスクが完了しました**の場合、イメージは正常にエクスポートされます。

エクスポートタスクをキャンセルするには、[**タスクの管理**]ページに移動してタスクを見つけ、**タスクのキャンセル**をクリックします。

注意:エクスポート結果を照会するには、[OSS コンソール]にログインします。

次のステップ

エクスポートされたイメージファイルをダウンロードするには、OSS コンソールにログインし、**オブジェクト URL の取得**を参照します。

セキュリティグループ

適用シナリオ

このドキュメントで紹介する例は、**クラシックネットワーク**にのみ該当します。

セキュリティを保証する以外に、セキュリティグループは次のような目的で使用できます。

- 安全なイントラネット通信の提供
- 特定の IP アドレスまたはポートの遮断
- 特定の IP アドレスのリモートログインのみの許可
- インスタンスに特定の IP アドレスへのアクセスのみの許可

安全なイントラネット通信の提供

クラシックネットワークで、異なる ECS インスタンス間でのイントラネット通信にセキュリティグループを使用できます。次の 2 つの状況があります。

- 各インスタンスが同じリージョンに属し、アカウントも同じ
- 各インスタンスが同じリージョンに属しているが、アカウントが異なる

各インスタンスが同じリージョンに属し、アカウントも同じ

セキュリティグループルールを設定することで、リージョンとアカウントが同じであるクラシックネットワーク ECS インスタンス間でのイントラネットを介した通信を許可できます。

同じセキュリティグループ内の ECS インスタンスどうしは、デフォルトでイントラネット通信を行います。

一方、異なるセキュリティグループに属する ECS インスタンスどうしは、デフォルトでイントラネット通信を行いません。

以下の解決策で、イントラネット通信を許可できます。

- 解決策 1: 同じセキュリティグループに ECS インスタンスを配置して、イントラネット通信を許可する。
- 解決策 2: ECS インスタンスが同じセキュリティグループに含まれない場合は、アクセスタイプのセキュリティグループルールを設定して、2 つのセキュリティグループ間でのイントラネット通信を許可します。[**権限付与オブジェクト**] で、他のインスタンスの IP アドレスを追加します。

各インスタンスが同じリージョンに属しているが、アカウントが異なる

セキュリティグループのルールを設定することで、同じリージョン異なるアカウントに属するクラシックネットワーク ECS インスタンスがイントラネット経由で通信できるようにすることができます。

同じで異なるアカウントに属するインスタンス間のイントラネット通信達成するためにリージョン 、各ユーザーは次のことを実行する必要があります。

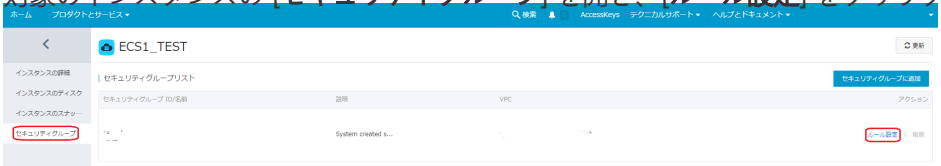
- インバウンドイントラネットに他のユーザーのセキュリティグループを追加します。
- 他のユーザーのセキュリティグループの ECS インスタンスに、そのアカウントのすべてのインスタンスにアクセスする権限を与えます。

注意：インスタンスのセキュリティを確保するため、従来のネットワークタイプのセキュリティグループのイントラネットインバウンドルールを設定する場合は、**セキュリティグループアクセス**が**認証タイプ**の最優先事項です。 **アドレス範囲アクセス** を選択する場合は、CIDR接頭辞 “/32” を持つ IP アドレスを a.b.c.d/32の形式で入力する必要があります。 IPv4 のみがサポートされています。

特定の IP アドレスまたはポートの遮断

セキュリティグループを使用して、特定の IP による ECS インスタンスアクセスを遮断、阻止、ブロックするか、特定のサーバーポートを IP アクセスから遮断します。手順は次のとおりです。

1. [**ECS 管理コンソール**] にログインします。
2. 設定するインスタンスを特定します。
3. 対象のインスタンスの [**セキュリティグループ**] を開き、[**ルール設定**] をクリックします。



4. [**イントラネット入力**] をクリックし、[**セキュリティグループルールを追加**] をクリックします。

5. 権限付与ポリシーに [**拒否**] を選択し、[**権限付与オブジェクト**] に遮断する IP アドレスを入力しま

す。[OK] をクリックします。

6. 特定のポートへのアクセスを制限する (例: 特定の IP アドレスから ECS インスタンスのポート 22 へのアクセスを遮断する) 場合は、権限付与ポリシーに [**拒否**] を選択し、プロトコルタイプに [**TCP**] を選択し、ポート範囲として [**22/22**] を入力して、権限付与オブジェクトには遮断する **IP** アドレスを入力します。その後、[**OK**] をクリックします。

特定の IP アドレスのリモートログインのみの許可

セキュリティグループを設定することで、特定の IP アドレスに対してのみ、インスタンスへのリモートログインを許可できます。インターネットからの流入ルールを設定する必要があります。

Linux インスタンスを例に説明します。特定の IP アドレスからポート 22 へのアクセスを許可します。

1. [**ECS 管理コンソール**] にログインします。
2. 設定するインスタンスを特定します。
3. 対象のインスタンスの [**セキュリティグループ**] を開き、[**ルール設定**] をクリックします。
4. [**インターネット入力**] をクリックし、[**セキュリティグループルールを追加**] をクリックします。
5. 権限付与ポリシーに [**許可**]、プロトコルタイプに [**TCP**] を選択し、ポート範囲として「22/22」を入力します。さらに対象のインスタンスにアクセスできる特定の IP アドレスを入力します (この例では 1.2.3.4)。優先順位は「**1**」を入力します。[**OK**] をクリックします。

6. 他のセキュリティグループルールを追加します。権限付与ポリシーに [**拒否**]、プロトコルタイプに [**TCP**] を選択し、ポート範囲として「22/22」を、権限付与オブジェクトとして「**0.0.0.0/0**」を入力します。優先順位は「**2**」を入力します。

2 つのルールを設定すると、以下の結果が得られます。

- 優先順位 1 のルールに従い、1.2.3.4 からポート 22 へのアクセスリクエストが許可されます。
- 優先順位 2 のルールに従い、他の IP アドレスからポート 22 へのアクセスリクエストが拒否されます。

インスタンスに特定の IP アドレスへのアクセスのみの許可

これを実現するには、まず、あらゆる IP (0.0.0.0/0) へのインターネット出力を拒否するよう設定します。そのうえで、もう 1 つ別のルールを追加し、インスタンスがアクセスする特定の IP に対するインターネット出力を許可します。許可ルールの優先順位を拒否ルールより高くします。

1. [**ECS 管理コンソール**] にログインします。
2. 設定するインスタンスを特定します。
3. 対象のインスタンスの [**セキュリティグループ**] を開き、[**ルール設定**] をクリックします。

4. 権限付与ポリシーに [**拒否**] を選択し、権限付与オブジェクトとして「**0.0.0.0/0**」を入力します。優先順位には 1 以上の値、たとえば **2** を入力します。[**OK**] をクリックします。

5. 別のルールを追加します。権限付与ポリシーに [**許可**] を選択し、権限付与オブジェクトとしてインスタンスがアクセスする特定の IP を入力します。優先順位は「**1**」を入力します。[**OK**] をクリックします。

インスタンスにログインして、ping または telnet でテストを行い、指定した IP 以外の IP アドレスにはアクセスできないことを確認できれば、設定は有効になっています。

デフォルトルール

このドキュメントでは、システムと自分で作成されたセキュリティグループの既定のルールについて説明します。

システムで作成されたセキュリティグループ

システムによって作成されたセキュリティグループには、すべてのICMPポート、TCPポート22、およびTCPポート3389にアクセスするためのルールしかありません。

- すべてのICMPポートは、エラーメッセージと運用情報を送信するために、ルータを含むネットワークデバイスによって使用されます。
- TCPポート22は、SSHを使用してLinuxインスタンスに接続するために使用されます。
- TCPポート3389は、Windowsリモートデスクトップを使用してWindowsインスタンスにリモート接続するために使用されます。

クラシックネットワーク用

クラシックネットワークにおけるデフォルトセキュリティグループのデフォルトルールは次のとおりです。

- **イントラネット**の受信方向すべてを拒否し、**イントラネット**の送信方向すべてを許可します。
- **インターネット**の送信方向すべてを許可し、**インターネット**の受信方向はTCPプロトコルの22ポート(SSH接続用)と3389ポート(リモートデスク接続用)と**ICMPプロトコル**(リモート接続用)のみ許可します。

VPC 用

VPC におけるデフォルトセキュリティグループのデフォルトルールは次のとおりです。

- **イントラネット**受信と**イントラネット**送信の両方とも 0.0.0.0/0 宛てのすべてを許可します。つまり、VPC 内の全インスタンスの相互通信を許可します。
- VPC セキュリティグループルールでは、イントラネットかインターネットかにかかわらず、すべてのルールが**イントラネット**の送信方向と受信方向に対して設定されます。

イントラネット入力 | イントラネット出力

権限付与ポリシー	プロトコルタイプ	ポート範囲	権限付与タイプ	権限付与オブジェクト	説明	プライオリティ
許可	Custom TCP	22/22	アドレスフィールドアクセス	0.0.0.0/0	-	110
許可	Custom TCP	3389/3389	アドレスフィールドアクセス	0.0.0.0/0	-	110
許可	All ICMP	-1/-1	アドレスフィールドアクセス	0.0.0.0/0	-	110

優先度110のルールは、追加するルールによって隠される可能性があります。優先度は1～100の数値にしか設定できません。

カスタムセキュリティグループ用

ユーザー定義のセキュリティグループの場合、既定のセキュリティグループの既定のルールは次のとおりです。

- すべての送信トラフィックに許可します。
- イントラネットとインターネットの両方の受信トラフィックをすべて破棄します。

セキュリティグループの作成

セキュリティグループの作成

セキュリティ分離の重要な方法として、セキュリティグループは仮想的なファイアウォールとして機能し、1つ以上の ECS インスタンスに対するネットワークアクセス制御の設定に用いられます。ECS インスタンスの作成時に、セキュリティグループを選択する必要があります。セキュリティグループルールを追加して、セキュリティグループ内のすべての ECS インスタンスに関するアウトバウンドとインバウンドのネットワークアクセスを制御することもできます。

手順は次のとおりです。

1. ECS 管理コンソール にログインします。
2. 左側のナビゲーションバーで、[**セキュリティグループ**] をクリックします。
3. リージョンを選択します。
4. [**セキュリティグループの作成**] をクリックします。
5. セキュリティグループを作成するダイアログボックスが表示されたら、次の情報を入力します。
   - セキュリティグループ名: 長さは 2 ~ 128 文字とします。名前の先頭は、大文字/小文字の英字または漢字を使います。数字、”_”、”-”を含めることができます。
   - 説明: 長さは 2 ~ 256 文字とします。http:// または https:// を先頭にすることはできません。
   - ネットワークタイプを選択します。クラシックネットワークと VPC という 2 種類のネットワークタイプがあります。VPC を選択する場合は、特定の VPC を選択する必要があります。現在のリージョンで VPC をまだ作成していない場合は、最初の 1 つを作成する必要があります。
6. [OK] をクリックして、セキュリティグループを作成します。

セキュリティグループルールの権限付与

権限を付与されたセキュリティグループルールは、特定のセキュリティグループに属する ECS インスタンスに対して、インターネットやイントラネットを介したインバウンド/アウトバウンドのアクセスを許可または禁止します:

- **VPC ネットワーク**: 入力と出力の設定が可能です。プライベートとインターネットに異なったルールを設定できません。
- **クラシックネットワーク**: インターネットとイントラネットそれぞれに別々の入力と出力のルールが必要です。

変更したセキュリティグループルールは、そのセキュリティグループに関連する ECS インスタンスに自動で適用されます。

事前準備

セキュリティグループを作成します。詳細は、**セキュリティグループの作成** を参照してください。

インスタンスに対するインターネットとイントラネットとプライベートの許可と拒否を知っておく必要があります。

操作手順

[ECS 管理コンソール] にログインします。

左側のナビゲーションバーで、[**セキュリティグループ**] をクリックします。

リージョンを選択します。

ルールを許可するセキュリティグループを特定し、[**ルール設定**] をクリックします。

[**セキュリティグループルールを追加**] をクリックします。

ダイアログボックスで、次のパラメータを設定します。

- **[NICタイプ]**:
  - 対象のセキュリティグループが VPC に属している場合、NICを選択する必要がありません。
    - インスタンスがインターネットにアクセスできる場合、ルールはインターネットとイントラネット両方で有効です。
    - インスタンスがインターネットにアクセスできない場合、ルールはイントラネットでのみ有効です。

  - 対象のセキュリティグループが クラシックネットワークに属している場合、**[インターネット]** または **[イントラネット]** を選択します。
- **[ルールの方向]**:
  - **アウトバウンド**：ECSインスタンスは、イントラネット、プライベートネットワーク、またはインターネットリソースを介して他のECSインスタンスにアクセスします。
  - **インバウンド**：イントラネットまたはプライベートネットワーク内の他のECSインスタンスとインターネットリソースがECSインスタンスにアクセスします。

権限付与ポリシー: **[許可]** または **[拒否]** を選択します。

> **注意**:
> **[拒否]**ポリシーは、応答を返さずにデータパケットを破棄します。 認証ポリシー以外の2つのセキュリティグループが重複している場合は、 **[拒否]** ルールが **[許可]** ルールよりも優先されます。

[プロトコルタイプ] および **[ポート範囲]**: ポート範囲の設定は、選択したプロトコルタイプの影響を受けます。次の表は、プロトコルタイプとポート範囲の関係を示しています。

プロトコルタイプ	ポート範囲	シナリオ
All	-1/-1 はすべてのポートを示します。	両方のアプリケーションが完全に信頼されるシナリオで使用されます。
All ICMP	-1/-1 はすべてのポートを示します。	Pingツールを使用してインスタンスのネットワーク接続ステータスを検出するために使用されます。
All GRE	-1/-1 はすべてのポートを示します。	VPNサービスに使用されます。
Custom TCP	カスタムポートの場合、有効なポート値は1～65535で、 有効なポート範囲の形式は **開始ポート/終了ポート**	1つまたは複数の連続するポートを許可または拒否するために使用されます。
Custom UDP		
SSH	22/22、デフォルトはSSHポート22として表示されます。	Linuxインスタンスへのリモート接続に使用されます。
TELNET	23/23と表示されます。	Telnetを使用してインスタンスにリモートログオンするために使用されます。
HTTP	80/80と表示されます。	このインスタンスは、Webサイトまたは

		Webアプリケーションのサーバーとして使用されます。
HTTPS	443/443と表示されます。	このインスタンスは、HTTPSプロトコルをサポートするWebサイトまたはWebアプリケーションのサーバーとして使用されます。
MS SQL	1433/1433と表示されます。	インスタンスはMS SQLサーバーとして使用されます。
Oracle	1521/1521と表示されます。	インスタンスはOracle SQL Serverとして使用されます。
MySQL	3306/3306と表示されます。	インスタンスはMySQLサーバーとして使用されます。
RDP	3389/3389と表示されます, デフォルトのRDPポートは3389です。	Windowsインスタンスへのリモート接続に使用されます。
PostgreSQL	5432/5432と表示されます。	インスタンスはPostgreSQLサーバとして使用されます。
Redis	6379/6379と表示されます。	インスタンスはRedisサーバーとして使用されます。

ポート25はデフォルトで無効になっており、セキュリティグループルールを追加することで有効にすることはできません。

認可タイプおよび**認可オブジェクト**：認可オブジェクトは認可タイプの設定に影響します。次の表は、それらの関係を示しています。

承認タイプ	**権限オブジェクト**
Address Field Access	*10.0.0.0* または *192.168.0.0 / 24* などのIPまたはCIDRブロック形式を使用します。IPv4アドレスのみがサポートされています。0.0.0.0/0はすべてのIPアドレスを示します
Security Group Access	アカウントまたは別のアカウントのセキュリティグループ内のインスタンスにこのセキュリティグループ内のインスタンスにアクセスする権限を与えます。 • **このアカウントの認証**：アカ

	ウントのセキュリティグループを選択します。 • **他のアカウントの認証** ：ターゲットセキュリティグループIDとアカウントIDを入力します。 **アカウント管理**> **セキュリティ設定**でアカウントIDを表示できます。 VPCネットワークインスタンスの場合、**セキュリティグループアクセス**はプライベートIPアドレスに対してのみ機能します。インターネットIPアドレスへのアクセスを許可する場合は、**アドレスフィールドアクセス**を使用します。

注 :
インスタンスのセキュリティを保証するために、クラシックネットワークタイプのセキュリティグループのイントラネットインバウンドルールを設定する場合、**セキュリティグループアクセス**が**認証タイプ**の最優先事項です。 Address Field Access を選択し、CIDR形式でIPアドレスを入力する場合は、IPアドレスをabcd/32の形式で入力する必要があります。有効なCIDR接頭辞は32だけです。

- **優先度**：1-100。数値が小さいほど優先度が高くなります。優先順位の詳細については、セキュリティグループルールの優先順位を参照してください。

7. OK をクリックして、指定したセキュリティグループにセキュリティグループルールを追加します。

セキュリティグループが有効かどうかの確認

Web サービスのサーバーにセキュリティグループを追加する場合を想定します: TCP 80番からの入力を許可します。

セキュリティグループは通常適用後、すぐに有効になりますが、状況によってはしばらく時間がかかることがあります。

Linux インスタンス

セキュリティグループを Linux インスタンスに適用した場合、以下の手順で有効化されているか確認します。

リモートから ECS へ接続します。

TCP 80 がリッスン中か以下のコマンドで確認します。

```
netstat -an | grep 80
```

以下のように表示される場合、TCP 80 はリッスン中です。

```
tcp       0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
```

ブラウザのアドレスに http://IP address を入力します。ルールが行こうになっている場合、アクセスは成功します。

Windows インスタンス

セキュリティグループを Windows インスタンスに適用した場合、以下の手順で有効化されているか確認します。

リモートから ECS へ接続します。

cmd を実行します。TCP 80 がリッスン中か以下のコマンドで確認します。

```
netstat -aon | findstr :80
```

以下のように表示される場合、TCP 80 はリッスン中です。

```
TCP    0.0.0.0:80         0.0.0.0:0           LISTENING       1172
```

ブラウザのアドレスに http://IP address を入力します。ルールが行こうになっている場合、アクセスは成功します。

セキュリティグループルールの優先順位について

セキュリティグループの **優先度** は 1 から 100 までの数字で決まります。値が小さいほど優先度が高くなります。

ECS インスタンスは、異なるセキュリティグループに属します。一つ以上のグループで、同じプロトコルタイプ、ポート範囲、認証タイプ、認証オブジェクトのルールがある場合、以下のテーブルの動作に従います。詳細は、**結果**列を参照してください。

番号	セキュリティグループルール	優先度	認証ポリシー	結果
i	A	同じ	Allow	B が有効化されます。同じ優先
	B		Drop	

				度であった場合、認証ポリシーは Drop が優先されます。
ii	C	1	Allow	C が有効化されます。優先度が高い方が有効になります。
	D	2	Drop	

セキュリティグループリストの照会

セキュリティグループリストの照会

管理コンソールで、セキュリティグループを照会することができます。手順は次のとおりです。

1. ECS 管理コンソール にログインします。
2. 左側のナビゲーションバーで、[**セキュリティグループ**] をクリックします。
3. リージョンを選択して、そのリージョンの全セキュリティグループを含むリストを表示します。
4. フィルター入力ボックスに VPC ID を入力し、この VPC に属するセキュリティグループをすべて表示できます。

セキュリティグループのプロパティ変更

セキュリティグループの名前と説明を変更することができます。

手順は次のとおりです。

ECS 管理コンソールにログインします。

左側のナビゲーションバーで、[**セキュリティグループ**] をクリックします。

リージョンを選択して、そのリージョンの全セキュリティグループを含むリストを表示します。

変更するセキュリティグループを特定します。次の 2 つの方法が利用できます。

- 名前の変更: 名前の上にマウスを移動して、表示された変更アイコンをクリックし、セキュリティグループ名を変更します。
- 名前と説明の変更: 変更するセキュリティグループの右にある [**変更**] をクリックします。表示されるダイアログボックスで、グループ名と説明を変更できます。

[OK] をクリックして、セキュリティグループを変更します。

セキュリティグループルールの照会

セキュリティグループルールの照会

セキュリティグループルールを照会できます。次の手順で行います。

1. ECS 管理コンソールにログインします。
2. 左側のナビゲーションバーで、[**ネットワーク＆セキュリティ**] > [**セキュリティグループ**] をクリックします。
3. リージョンを選択します。
4. セキュリティグループを選択し、[**ルール設定**] をクリックします。
5. 内容はクラシックネットワークと VPC で異なります。
   - セキュリティグループが VPC の場合は、[**イントラネット入力**] と [**イントラネット出力**] の 2 つのセキュリティグループルールタブが表示されます。
   - セキュリティグループがクラシックネットワークの場合は、[**インターネット入力**]、[**インターネット出力**]、[**イントラネット入力**]、[**イントラネット出力**] の 4 つのセキュリティグループルールタブが表示されます。
6. タブをクリックすると、指定したタイプのセキュリティグループルールが表示されます。

セキュリティグループルールの取り消し

セキュリティグループルールの取り消し

今後適用しないセキュリティグループルールを取り消すことができます。次の手順で行います。

1. ECS 管理コンソールにログオンします。

2. 左側のナビゲーションバーで、[**セキュリティグループ**] をクリックします。
3. リージョンを選択します。
4. ルールを取り消すセキュリティグループを選択し、[**ルール設定**] をクリックします。
5. セキュリティグループの管理ページで、取り消すルールのタイプ:
   VPCの場合は、[**イントラネット入力**]、[**イントラネット出力**] から選択します。
   クラシックネットワークの場合は、 [**インターネット入力**]、[**インターネット出力**]、[**イントラネット入力**]、[**イントラネット出力**] から選択します。
6. セキュリティグループルールを選択し、[**削除**] をクリックします。
7. 表示されるダイアログボックスで、[**OK**] をクリックします。セキュリティグループルールがキャンセルされます。

セキュリティグループの削除

不要になったセキュリティグループは削除できます。

注意:

- 特定のセキュリティグループが ECS インスタンスを含んでいない、または他のセキュリティグループのルールで参照されていない場合は、そのセキュリティグループを削除できます。
- セキュリティグループを削除すると、そのセキュリティグループルールもすべて削除されます。

コンソールを使用してセキュリティグループを削除する手順は、次のとおりです。

ECS 管理コンソールにログインします。

左側のナビゲーションバーで、[**ネットワーク＆セキュリティ**] > [**セキュリティグループ**] をクリックします。

リージョンを選択して、そのリージョンの全セキュリティグループを含むリストを表示します。

1 つまたは複数の (あるいはすべての) セキュリティグループを選択します。

[**削除**] をクリックします。

表示されたダイアログボックスで [**OK**] をクリックし、選択したセキュリティグループを削除します。

セキュリティグループのクローン

Alibaba Cloud では、異なるリージョン間および異なるネットワークタイプ間でのセキュリティグループのクローン作成に対応しています。

適用シナリオ

以下のシナリオでは、セキュリティグループのクローンを作成する必要があります。

リージョン A に SG1 という名前のセキュリティグループを既に作成していて、SG1 と同じルールをリージョン B の ECS インスタンスに適用しようとしています。この場合、リージョン B に新しいセキュリティグループを作成せずに、リージョン B に SG1 のクローンを作成することができます。

クラシックネットワークで SG2 という名前のセキュリティグループを既に作成していて、SG2 と同じルールを VPC ネットワークタイプのインスタンスに適用したい場合、設定の際にVPCを選んで SG2 のクローンを作成することができます。つまり VPC ネットワーク内で SG2 と同じルールの新しいセキュリティグループとなります。

オンラインビジネスアプリケーションを実行する ECS インスタンスに新しいセキュリティグループルールを適用する場合、ルールを変更する前にバックアップとしてセキュリティグループのクローンを作成しておくことをお勧めします。そうすることで、新しいセキュリティグループルールがオンラインビジネスアプリケーションにとってマイナスの影響を及ぼす場合、そのルールの全部または一部を元に戻すことができます。

前提条件

セキュリティグループのネットワークタイプをクラシックから VPC に変更する場合は、まずターゲットリージョンに VPC と VSwitch を作成する必要があります。

手順

セキュリティグループのクローンを作成するには、次の手順に従います。

ECS 管理コンソール にログインします。

左側のナビゲーションペインで、[**ネットワーク & セキュリティ**] > [**セキュリティグループ**] をク

リックします。

[**セキュリティグループリスト**] ページでターゲットリージョンを選択します。

ターゲットセキュリティグループを特定して、[**アクション**] 列で [**クローン**] をクリックします。

[**クローン**] ダイアログボックスで、新しいセキュリティグループに次の情報を設定します。

- **コピー先のリージョン**: 新しいセキュリティグループに適したリージョンを選択します。現時点ではすべてのリージョンがサポートされているわけではありません。サポートされているリージョンはドロップダウンリストに表示されます。
- **セキュリティグループ名**: 新しいセキュリティグループの名前を指定します。
- **ネットワークタイプ**: 新しいセキュリティグループに適したネットワークタイプを選択します。VPC を選択する場合は、ドロップダウンリストから 1 つの VPC を選択します。

[OK] をクリックします。

新しいセキュリティグループが [**セキュリティグループリスト**] に表示されます。

セキュリティグループルールの復元

セキュリティグループルールの復元とは、元のセキュリティグループのルールをターゲットセキュリティグループのルールに完全または部分的に復元するプロセスを表します。具体的には次のとおりです。

完全な復元は、ターゲットセキュリティグループに存在しないルールを元のセキュリティグループから移動し、ターゲットセキュリティグループにのみ存在するルールを元のセキュリティグループに追加することを意味します。復元後、元のセキュリティグループのルールはターゲットセキュリティグループのルールと同じになります。

部分的な復元は、ターゲットセキュリティグループにのみ存在するルールを元のセキュリティグループに追加し、元のグループにのみ存在するルールは無視することを意味します。

制約

セキュリティグループルールの復元には、次の制限があります。

元のセキュリティグループとターゲットセキュリティグループは同じリージョンにある必要があり

ます。

元のセキュリティグループとターゲットセキュリティグループは同じネットワークタイプである必要があります。

優先度が 110 の任意のシステムレベルのセキュリティグループルールがターゲットセキュリティグループに存在する場合、それらは復元時に作成されません。復元後、元のセキュリティグループのルールは予想されるルールと異なる場合があります。システムレベルのセキュリティグループルールが必要な場合は、ルールを手動で作成し、優先度を 100 に設定する必要があります。

ユースケース

オンラインビジネスアプリケーションを実行する ECS インスタンスに新しいセキュリティグループルールを適用する場合、以前のセキュリティグループのクローンをバックアップとして作成し、その中のルールを変更できます。新しいセキュリティグループルールがオンラインビジネスアプリケーションを害する場合、そのルールの全部または一部を復元できます。

前提条件

同じリージョン内の同じネットワークタイプのセキュリティグループを少なくとも 1 つ所有している必要があります。

手順

セキュリティグループのルールを復元するには、次の手順を実行します。

ECS 管理コンソールにログインします。

左側のナビゲーションペインで、[**ネットワークとセキュリティ**] > [**セキュリティグループ**] をクリックします。

[**セキュリティグループリスト**] ページでターゲットリージョンを選択します。

元のセキュリティグループとしてルールを復元するセキュリティグループを探し、[**アクション**] 列で [**ルールの復元**] をクリックします。

[**ルールの復元**] ダイアログボックスで、次の手順を実行します。

i. [**ターゲットセキュリティグループ**] を選択します。元のセキュリティグループとは異なるルールを持つ必要があるターゲットセキュリティグループとしてセキュリティグルー

プを選択します。

ii. [**復元のタイプ**] を選択します。

i. 元のセキュリティグループがターゲットセキュリティグループと同じルールを持つようにする場合は、[**完全に復元**] を選択します。

ii. ターゲットセキュリティグループにのみ存在するルールを元のセキュリティグループに追加するだけの場合は、[**部分的に復元**] を選択します。

iii. [**結果のプレビュー**] 領域で、復元結果をプレビューします。

i. 緑色で表示されているルールはターゲットセキュリティグループにのみ存在します。[**完全に復元**] と [**部分的に復元**] のどちらを選択するかにかかわらず、これらのルールは元のセキュリティグループに追加されます。

ii. 赤色で表示されているルールはターゲットセキュリティグループに存在しないルールです。[**完全に復元**] が選択されている場合、これらのルールは元のセキュリティグループから削除されます。[**部分的に復元**] が選択されている場合、ルールは元のセキュリティグループに維持されます。

[**OK**] をクリックします。

正常に作成されると、[**ルールの復元**] ダイアログボックスが自動的に閉じます。[**セキュリティグループリスト**] で、ルールを復元した元のセキュリティグループを探します。[**アクション**] 列で、[**ルール設定**] をクリックして [**セキュリティグループルール**] ページを開き、更新されたセキュリティグループルールを表示します。

キーペア

SSH キーペアの作成

制限

Alibaba Cloud では RSA 2048bit の SSH キーペアのみ対応しています。

- Alibaba Cloud には SSH キーペアの公開鍵を保管しています。
- キーペアが作成された段階でユーザーが秘密鍵をダウンロードする必要があります。
- 秘密鍵は暗号化されていない PEM の PKCS#8 形式を採用しています。

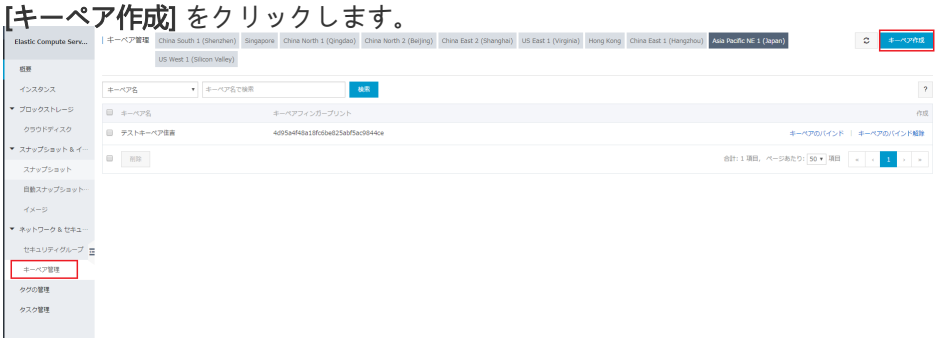
１アカウントの各リージョンにつき、最大 500 個の秘密鍵を作成することができます。

操作手順

[ECS コンソール] にログインします。

ナビゲーションの **[キーペア管理]** をクリックします。

[キーペア作成] をクリックします。



新しくウィンドウを開き、キーペア名を設定すると同時に **[キーペアを自動新規作成]** を選択します。
ECS にバインドされているキーペアを、バインド解除しなくても削除してしまうことは可能ですが、この場合、同じキーペア名称の利用が以後できなくなりますのでご注意ください。
対象となるキーペア名称を指定した場合、コンソールでは【キーペアがすでに存在しています。】というエラーメッセージが表示されます。
キーペアを削除する前に ECS とのバインドの解除を行うことで、同じキーペア名称を繰り返し使用することは可能です。

[OK] をクリックし、秘密鍵をダウンロードします。

注意： 必ず秘密鍵をダウンロードする必要があります。秘密鍵がない場合、ECS にログインすることができません。

キーペア作成後、キーペア管理ページに作成したキーペアの **キーペア名**、**キーペアフィンガープリント** などの情報を確認することができます。

次の操作

SSHキーペア作成後、 SSH キーペアのバインド/バインド解除を参照してください。

SSH キーペアのインポート

他の方法で SSH キーペアを作成し、公開鍵を Alibaba Cloud ECS にインポートすることができます。インポート可能の公開鍵形式は SSH キーペアについて を参照してください。

注意： 秘密鍵はユーザー自身が保管し、Alibaba Cloud にはインポートしないでください。

SSH キーペアをインポートするには、キーペアを作成し、公開鍵を Base64 コーディングの形で Alibaba Cloud ECS にインポートする必要があります。

操作手順

[ECS コンソール] にログインします。

ナビゲーションの **[ネットワーク＆セキュリティ]** - **[キーペア管理]** をクリックします。

[キーペア作成] をクリックします。リージョンを選択し、[**キーペア作成**]をクリックします。

新しくウィンドウを開き、キーペア名を設定すると同時に **[既存鍵をインポート]** を選択し、**公開鍵** を入力します。
ECS にバインドされているキーペアを、バインド解除しなくても削除してしまうことは可能ですが、この場合、同じキーペア名称の利用が以後できなくなりますのでご注意ください。
対象となるキーペア名称を指定した場合、コンソールでは【キーペアがすでに存在しています。】というエラーメッセージが表示されます。
キーペアを削除する前に ECS とのバインドの解除を行うことで、同じキーペア名称を繰り返し使用することは可能です。

OK をクリックし、公開鍵をインポートします。

インポート完了後、キーペア管理ページにインポートしたキーペアの **キーペア名**、**キーペアフィンガープリント** などの情報を確認することができます。

SSH キーペアのバインド/バインド解除

制限

- Linuxインスタンスにのみ適用されます。
- ECSインスタンスが実行中の状態の場合、SSHキーペアをインスタンスにバインドした後にインスタンスの再起動 を実行します。
- インスタンスからキーペアのバインドを解除したら、インスタンスを再起動するを実行してSSHキーペアを無効にする必要があります。
- Linuxのログオンにパスワードベースの認証を使用すると、キーペアがバインドされた後にパスワード認証機能が自動的に無効になります。
- SSHキーペアがアンバインドされた後、接続を成功させるにはインスタンスのパスワードのリセットを実行する必要があります。
- I/Oに最適化されていない世代Iのインスタンスを除いて、インスタンス世代とタイプファミリのすべてのLinuxインスタンスインスタンスタイプファミリーは、SSHキーペアの認証方法をサポートしています。

SSHキーペアをバインドする

SSHキーペアをECSインスタンスにバインドするには、次の手順を実行します。

[ECS コンソール]にログオンします。

左側のナビゲーションペインで、**ネットワークとセキュリティ** > **キーペア**を選択します。

リージョンを選択します。

キーペアを選択し、**インスタンスをバインドする**をクリックします。**バインドインスタンス** ダイアログボックスの**インスタンス選択**ボックスで、1つまたは複数のインスタンスを選択し、アイコン**>**をクリックします。

注意:
インスタンスの選択ボックスでは、グレーのインスタンス名は、WindowsインスタンスまたはGeneration IのI / Oに最適化されていないインスタンスです。これらのインスタンスはSSHキーペアをサポートしていません。

OKをクリックします。

SSHキーペアをアンバインドする

ECSインスタンスからSSHキーペアをバインド解除するには、次の手順を実行します。

[ECS コンソール]にログオンします。

左側のナビゲーションペインで、**ネットワークとセキュリティ** > **キーペア**を選択します。

リージョンを選択します。

SSHキーペアを選択し、**インスタンスをアンバインドする**をクリックします。**インスタンスのアンバインド** ダイアログで、**インスタンスの選択**ボックスで、インスタンスを1つ以上選択し、アイコン**>**をクリックします。

OKをクリックします。

SSH キーペアの削除

SSHキーペアを削除する

キーペアが不要になった場合は、削除することができます。削除されたキーペアは回復できないことに注意してください。キーペアを使用した既存のインスタンスは影響を受けず、削除されたキーペア名はインスタンスに関連付けられたままになります。

キーペアを削除するには、次の手順を参照してください。

[ECSコンソール]にログインします。

左側のナビゲーションペインで、**[ネットワークとセキュリティ]**の下にある**キーペア**をクリックします。

1つまたは複数のキーペアを選択します。

削除> **OK** をクリックします。

注意:

- ECS にバインドされているキーペアを、バインド解除しなくても削除してしまうことは可能ですが、この場合、同じキーペア名称の利用が以後できなくなりますのでご注意ください。対象となるキーペア名称を指定した場合、コンソールでは【キーペアがすでに存在しています。】というエラーメッセージが表示されます。
- キーペアを削除する前に ECS とのバインドの解除を行うことで、同じキーペア名称を繰り返し使用することは可能です。

Elastic Network Interfaces

ENIのアタッチ

ECSコンソールでECSインスタンスを作成するときに、ENIをアタッチすることができます。インスタンスの

作成の詳細については、インスタンスの作成を参照してください。このドキュメントでは、ECSインスタンスの作成時にENIをアタッチする際の注意事項を説明します。

ECSインスタンスの作成時にENIを添付するときは、次の項目を考慮することをお勧めします。

基本設定:

インスタンスタイプ: ENIをサポートするインスタンスタイプを選択します。詳細については インスタンスタイプファミリー を参照してください。

イメージ: 次のイメージのみ、追加設定無しで自動的にENIを認識できます。

- CentOS 7.3 64ビット
- CentOS 6.8 64ビット
- Windows Server 2016データセンターエディション64ビット
- Windows Server 2012 R2データセンターエディション64ビット

他のイメージの場合は、**ENIの設定**を行い、作成したインスタンスがENIを認識できるようにする必要があります。

ネットワーキング:

ネットワーク: **VPC**を選択し、作成済みのVPCとVSwitchを選択します。

Elastic ネットワークインターフェイス: **ENIの追加**をクリックしてENIをアタッチし、ENIを使用するVSwitchを選択します。

> **注意**:
> コンソールによりインスタンスを作成する場合、最大2つのENIをアタッチできます。そのうちの1つはプライマリネットワークインターフェイスで、自動的にアタッチされ、もう1つはセカンダリネットワークインターフェイスです。インスタンスが開始されたら、コンソール インスタンスタイプに基づいて、または AttachNetworkInterface APIを使用して、インスタンスに複数のネットワークインターフェイスを追加できます。

この方法で作成されたセカンダリネットワークインターフェイスを維持する場合は、インスタンスをリリースする前にインスタンスからデタッチするを実行します。

ENI の作成

ECS コンソールで ENI を作成し、インスタンスに ENI を使用できます。このドキュメントでは、ECS コンソールで ENI を作成する方法について説明します。

制限

ENI を作成するには、次の制限があります。

- 各 ENI は VPC の VSwitch に属しなければなりません。
- 各 ENI は 1 つのセキュリティグループに属する必要があります。

前提条件

ENI を作成する前に、次の操作を完了してください。

- VPC の作成、VPC に VSwitch の作成。
- 同じ VPC 内にセキュリティグループの作成。

手順

ENI を作成するには、次の手順を実行します。

ECS コンソールにログインします。

左側のナビゲーションペインで、[**Networks＆Security**]> **Network Interfaces** を選択します。

中国北部 3 リージョンを選択します。

作成をクリックします。

作成ダイアログボックスで、次の設定を完了します。

i. **ネットワークインタフェース名**：ENI の名前を指定します。
ii. **VPC** ：VPC を選択します。

注意：
インスタンスに ENI を接続するときは、ENI を同じ VPC に配置する必要があります。また、ENI を作成した後は、VPC を変更することはできません。

iii. **VSwitch** ：VSwitch を選択します。

注意：

ENI をインスタンスに接続する場合、ENI を同じゾーンに配置する必要がありますが、同じ VSwitch に配置する必要はありません。また、ENI を作成した後は、VSwitch を変更することはできません。

6. **IP** ：ENI のプライベート IP アドレスとして IPv4 アドレスを指定します。IPv4 アドレスは、指定されたVSwitch のC IDR ブロックで使用可能でなければなりません。指定しない場合は、ENI の作成後に、プライベート IP アドレスが ENI に自動的に割り当てられます。
7. **SecurityGroup** ：選択した VPC のセキュリティグループを選択します。
8. **説明**：さらなる管理を容易にするための ENI の簡単な説明を記入します。
9. **OK** をクリックします。

Network Interfaces ページで、テーブルをリフレッシュしてください。新しい ENI が **Available** ステータスになると、それは正常に作成されます。

関連操作

ENI を作成したら、次の操作を実行できます。

- インスタンスに ENI のアタッチ
- ENI の属性の変更
- ENI の削除

API

CreateNetworkInterface

インスタンスに ENI のアタッチ

インスタンスに ENI をアタッチすることができます。このドキュメントでは、ECS コンソールのインスタンスに ENI をアタッチする方法について説明します。

制限

ENI をインスタンスにアタッチするには、次の制限があります。

- セカンダリ ENI はインスタンスにのみアタッチできます。
- ENI は VPC インスタンスにのみアタッチでき、同じ VPC になければなりません。
- ENI とインスタンスの VSwitch は同じである必要はありませんが、同じゾーンになければなりません。

- ENI は **Available** の状態でなければなりません。
- インスタンスは**Stopped**ステータスでなければなりません。
- ENI は、一度に 1 つの VPC インスタンスにのみアタッチできます。ただし、VPC インスタンスは複数の ENI に関連付けることができます。1 つのインスタンスにアタッチできる ENI の最大数の詳細については、インスタンスタイプファミリーを参照してください。

前提条件

ENI をインスタンスにアタッチする前に、次の操作を完了してください。

- ENI の作成。
- ENI が **Available** の状態であることを確認してください。
- インスタンスが複数の ENI に関連付けられることを確認し、インスタンスを停止します。

手順

ENI をインスタンスにアタッチするには、次の手順を実行します。

1. ECS コンソールにログインします。
2. 左側のナビゲーションペインで、[**Networks＆Security**]> **Network Interfaces** を選択します。
3. 中国北部 3 リージョンを選択します。
4. 利用可能な ENI を探し、**操作**列で**アタッチ**をクリックします。
5. **アタッチ** ダイアログボックスでインスタンスを選択し、 **OK** をクリックします。

Network Interfaces ページで、テーブルをリフレッシュしてください。選択された ENI が **InUse** ステータスになると、インスタンスに正常にアタッチされます。

関連操作

ENI がインスタンスにアタッチされた後、次の操作を実行できます。

- インスタンスから ENI のデタッチ、ENI の削除
- ENI 属性の変更
- ENI の設定

API

AttachNetworkInterface

インスタンスから ENI のデタッチ

インスタンスからセカンダリ ENI は削除できますが、プライマリ ENI は削除できません。

制限

セカンダリ ENI をインスタンスからデタッチするには、次の制限があります。

- セカンダリ ENI は **InUse** ステータスでなければなりません。
- インスタンスは **Stop** ステータスでなければなりません。

前提条件

ENI は**インスタンスにアタッチ**しています。ENI をインスタンスからデタッチする前に、**インスタンスを停止**する必要があります。

手順

セカンダリENIをインスタンスからデタッチには、次の手順を実行します。

1. ECS コンソールにログインします。
2. 左側のナビゲーションペインで、**Networks & Security** > **Network Interfaces**を選択します。
3. 中国北部 3 リージョンを選択します。
4. **InUse** ステータスで ENI を探し、 **Operations** 列で **Detach** をクリックします。
5. **Detach** ダイアログボックスで情報を確認し、 **OK** をクリックします。

Network Interfaces ページで、テーブルをリフレッシュしてください。選択された ENI が **Available** ステータスになると、インスタンスから正常にデタッチされます。

関連操作

ENI をインスタンスからデタッチした後、次の操作を実行できます。

- 別インスタンスへの ENI アタッチ
- ENI の削除
- ENI 属性の変更

API

DetachNetworkInterface

ENI 属性の変更

インスタンスのプライマリ ENI ではなくセカンダリ ENI の属性を変更できます。ENI の次の属性を変更できます。

- ENI の名前。
- ENI に関連付けられたセキュリティグループ。1つの ENI が少なくとも 1 つのセキュリティグループに関連付けられている必要があります。ただし、5 つ以上のセキュリティグループに関連付けることはできません。
- ENI の説明。

利用可能 または **利用中** ステータスの ENI の属性を変更することができます。

このドキュメントでは、ECS コンソールで ENI の属性を変更する方法について説明します。

前提条件

ENI の属性を変更する前に、**ENI の作成**を実行してください。

手順

ENI の属性を変更するには、次の手順を実行します。

コンソールにログインします。

左側のナビゲーションペインで、[**Networks＆Security**]> **Network Interfaces** を選択します。

リージョンを選択します。

ENI を探して、**操作**列で**変更**をクリックします。

変更 ダイアログボックスで、次のオプション構成を変更します。

- **ネットワークインタフェース名**：選択した ENI の新しい名前を指定します。
- **セキュリティグループ** ：ENI のセキュリティグループを追加選択するか、セキュリティグループを削除します。
- **説明**：ENI の簡単な説明を記入します。

変更が完了したら、 **[OK]** をクリックします。

API

ModifyNetworkInterfaceAttribute

ENI の削除

ENI を必要としない場合は、削除することができます。ただし、セカンダリ ENI は削除できますが、インスタンスのプライマリ ENI は削除できません。

ENI が削除されると、ENI のプライマリプライベート IP アドレスが自動的にリリースされ、関連するすべてのセキュリティグループから ENI が自動的に削除されます。

制限

利用可能 ステータスでのみ ENI を削除できます。

前提条件

ENI がインスタンスにアタッチしている場合、インスタンスからデタッチします。

手順

ENI を削除するには、次の手順を実行します。

ECS コンソールにログインします。

左側のナビゲーションペインで、[**Networks＆Security**]> **Network Interfaces** を選択します。

リージョンを選択します。

利用可能なENIを見つけ、**操作**列で**削除**をクリックします。

ダイアログボックスで、 **[OK]** をクリックします。

Network Interfaces ページで、テーブルをリフレッシュしてください。ENI が見えなければ正常に削除されています。

API

DeleteNetworkInterface

ECS インスタンスのENIの設定

インスタンスは下記のイメージに該当する場合、Elastic Network Interfaces（ENI）を手動で認識させるように設定する必要はありません。

- CentOS 7.3 64 ビット
- CentOS 6.8 64 ビット
- Windows Server 2016 データセンターエディション 64ビット
- Windows Server 2012 R2 データセンターエディション 64 ビット

インスタンスは上記のイメージに該当しない場合、対象インスタンスを手動で ENI を認識させるように設定する必要があります。

このドキュメントでは、例として CentOS 7.2 64 ビットを実行するインスタンスを使用して、ENI を設定してインターフェイスを認識させる方法を紹介します。

前提条件

ENI を ECS インスタンスにアタッチする必要があります。

手順

ENIを設定するには、次の手順を実行します。

DescribeNetworkInterfacesインターフェイスを使用するか、ECS コンソールにログオンし、ENI

のプライマリプライベート IP アドレス、サブネットマスク、デフォルトルート、および MAC アドレスの属性を取得します。ECS コンソールでこれらの属性を取得するには、次の手順を実行します。

ECS コンソールにログオンする。

左側のナビゲーションペインで、[**Networks＆Security**]> **Network Interfaces** を選択します。

リージョンを選択します。

ネットワークインターフェイスを見つけ、プライマリプライベート IP アドレス、サブネットマスク、デフォルトルート、および MAC アドレスを取得します。

例

```
eth1 10.0.0.20/24 10.0.0.253 00：16：3e：12：e7：27
eth2 10.0.0.21/24 10.0.0.253 00：16：3e：12：16：ec
```

ECS インスタンスに接続

コマンドを実行して、ネットワークインターフェイスの構成ファイルを生成します。

```
cat /etc/sysconfig/network-scripts/ifcfg-[network interface name in the OS]
```

注：

- OS のネットワークインターフェイス名と MAC アドレスの関係に注意してください。
- デフォルトルートは DEFROUTE = no に設定しなければなりません。他のエディションも同じ構成でなければなりません。ifup コマンドを実行すると、ネットワークインタフェースを設定した後、アクティブなデフォルトルート設定が変更されることに注意してください。**例**：

```
# cat /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
BOOTPROTO=dhcp
ONBOOT=yes
TYPE=Ethernet
USERCTL=yes
PEERDNS=no
IPV6INIT=no
```

```
PERSISTENT_DHCLIENT=yes
HWADDR=00:16:3e:12:e7:27
DEFROUTE=no
```

ネットワークインターフェイスを開始するには、次の手順を実行します。

i. dhclient プロセスを起動して DHCP リクエストを開始するには、 if [network interface name in the OS]コマンドを実行します。

例：

```
# ifup eth1
# ifup eth2
```

ii. 応答が受信された後、 ip a コマンドを実行して、ネットワークインターフェイスの IP 割り当てをチェックします。これは、ECS コンソールに表示される情報と一致する必要があります。

例:

```
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
qlen 1000
link/ether 00:16:3e:0e:16:21 brd ff:ff:ff:ff:ff:ff
inet 10.0.0.19/24 brd 10.0.0.255 scope global dynamic eth0
valid_lft 31506157sec preferred_lft 31506157sec
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
qlen 1000
link/ether 00:16:3e:12:e7:27 brd ff:ff:ff:ff:ff:ff
inet 10.0.0.20/24 brd 10.0.0.255 scope global dynamic eth1
valid_lft 31525994sec preferred_lft 31525994sec
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
qlen 1000
link/ether 00:16:3e:12:16:ec brd ff:ff:ff:ff:ff:ff
inet 10.0.0.21/24 brd 10.0.0.255 scope global dynamic eth2
valid_lft 31526009sec preferred_lft 31526009sec
```

ルートテーブルの各ネットワークインターフェイスのメトリックを設定します。この例では、eth1 とeth2 のメトリックパラメータを次のように設定します。

例：

```
 eth1:  gw: 10.0.0.253  metric: 1001
eth2: gw: 10.0.0.253 metric: 1002
```

i. 次のコマンドを実行してメトリックパラメータを設定します。**例**：

```
# ip -4 route add default via 10.0.0.253 dev eth1 metric 1001
# ip -4 route add default via 10.0.0.253 dev eth2 metric 1002
```

ii. route -n コマンドを実行して、設定が成功したかどうかを確認します。**例**：

```
# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 10.0.0.253 0.0.0.0 UG 0 0 0 eth0
0.0.0.0 10.0.0.253 0.0.0.0 UG 1001 0 0 eth1
0.0.0.0 10.0.0.253 0.0.0.0 UG 1002 0 0 eth2
10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth2
169.254.0.0 0.0.0.0 255.255.0.0 U 1002 0 0 eth0
169.254.0.0 0.0.0.0 255.255.0.0 U 1003 0 0 eth1
169.254.0.0 0.0.0.0 255.255.0.0 U 1004 0 0 eth2
```

ルートテーブルを作成するには、次の手順を実行します。

注：
ルートテーブル名としてメトリック値を使用することをお勧めします。

i. コマンドを実行してルートテーブルを作成します。**例**：

```
# ip -4 route add default via 10.0.0.253 dev eth1 table 1001
# ip -4 route add default via 10.0.0.253 dev eth2 table 1002
```

ii. コマンドを実行して、ルートテーブルが正常に構築されているかどうかを確認します。**例**：

```
# ip route list table 1001
default via 10.0.0.253 dev eth1
# ip route list table 1002
default via 10.0.0.253 dev eth2
```

ポリシーベースルーティングを設定するには、次の手順を実行します。

i. コマンドを実行して、ポリシーベースのルーティングを構成します。

例：

```
# ip -4 rule add from 10.0.0.20 lookup 1001
# ip -4 rule add from 10.0.0.21 lookup 1002
```

ii. ip rule list コマンドを実行してルートルールを表示します。

例：

```
# ip rule list
0: from all lookup local
32764: from 10.0.0.21 lookup 1002
32765: from 10.0.0.20 lookup 1001
32766: from all lookup main
32767: from all lookup default
```

これで、ENI 設定が完了しました。

タグ

制約

タグを管理コンソールを使用して、ECSインスタンス、ストレージ、スナップショット、イメージおよびセキュリティグループに付けることができます。

タグには次の制限があります。

- 各タグは、キーと値のペアで構成されます。
- 1 つのインスタンスに、最大 5 個のタグを付けることができます。
- 1 つのインスタンス内で、各タグのタグキーは一意でなければなりません。同一のタグキーを持つタグは、上書きされます。
- タグ情報はリージョンをまたいで波及しません。たとえば、中国東部 1 (杭州) リージョンで作成されたタグは、中国東部 2 (上海) リージョンには表示されません。
- タグ付けを解除し、そのタグが他のリソースにタグ付けされていない場合は、自動的にそのタグが削除されます。

リソースにタブのバインド

アカウントがさまざまな方法で互いに関連付けられた各種類のリソースを管理している場合は、タグをリソースにバインドし、分類および管理できます。

最大 10 個のタグをリソースにバインドすることができます。1 回最大 5 つのタグをリソースにバインド/アンバインドできます。

タグを使用してリソースをバインドするには、次の手順を実行します。

1. ECS 管理コンソールにログインします。
2. 左側のナビゲーションバーでタグバインド可能のプロダクトを選択します。例えば、**インスタンス**、**クラウドディスク**、**スナップショット**、**イメージ**、**セキュリティグループ** です。
3. ページの一番上でリージョンを選択します。
4. リソースリストからタグをバインドするリソースを選択します。
5. リソースはインスタンスの場合、リソースリストの下に、**詳細**、**タグの編集** の順にクリックします。
6. ダイアログボックスでタグを選択または選択解除します。
   - **使用可能なタグ** をクリックし、選択したリソースのタグリストで使用可能なタグを選択します。
   - 選択したリソースに利用可能なタグがない場合は、**作成** をクリックし、**キー** および **値** を設定します。
     - **キー** は必須ですが、**値** はオプションです。
     - **キー** は、aliyun、http：//、https：// で始めることはできません。大文字と小文字を区別せず、64 文字まで使用できます。
     - **値** は http：//、https：// で始めることはできません。大文字と小文字を区別せず、128 文字まで使用できます。それは空にすることができます。
     - リソースの任意のタグ **キー** は一意でなければなりません。既存のものと同じキーを持つタグは上書きされます。
   - 選択されたリソースがすでに 10 個のタグでバインドされている場合、**使用可能なタグ** および **作成** はグレー表示されます。新しいタグをバインドする前に、いくつかのタグのバインドを解除する必要があります。
7. **確認** をクリックします。

タグが正しくバインドされているかどうかを確認するには、リソースの **タグの編集** 機能を使用するか、ECS コンソールの左側のナビゲーションバーで **タグの管理** をクリックします。リソースリストの上部にあるタグ記号内の **タグ名** をクリックすると、リソースをフィルタリングできます。

タグの削除

タグがリソース管理に適用されなくなった場合、タグをリソースからアンバインドすることができます。タグがアンバインドされ、他のリソースにもバインドされなくなった後、タグは自動的に削除されます。

- **タグの削除** 機能は、一度に 1 つまたは複数のタグをインスタンスからアンバインドします。

現在のところ、この機能はインスタンスでのみ使用可能です。他のリソースタイプでは使用できません。

- **タグの編集** 機能は、タグを 1 つずつアンバインドします。毎回、リソースから 5 つのタグまでをアンバインドできます。

タグの削除

現在のところ、 **タグの削除** 機能はインスタンスでのみ使用可能です。

タグの削除手順は下記となります。

1. ECS コンソールにログインします。
2. 左ナビゲーションの **インスタンス** をクリックします。
3. リージョンを選択します。
4. インスタンスリスト内のタグのバインドを解除するインスタンスを選択します。タグでインスタンスをフィルタリングし、目的のインスタンスを選択することもできます。
5. リソースリストの一番下にある **詳細** > **タグの削除** を選択します。
6. **タグの削除** ダイアログボックスで、アンバインドするタグの **タグキー** を入力します
7. **OK** をクリックして、タグのバインドを解除します。

タグが正常にアンバインドされているかどうかを確認するには、インスタンスの **タグの編集** 機能を使用するか、ECS コンソールの左側のナビゲーションバーで **タグ** をクリックします。

タグの編集

タグの編集 機能は、リソースから 1 つまたは複数のタグのバインドを解除します。

タグをバインド解除する手順は下記となります。

1. ECS コンソールにログインします。
2. 左側のナビゲーションバーで、バインド解除操作のリソースタイプを選択します。例えば、**インスタンス**、**クラウドディスク**、**スナップショット**、**イメージ**、**セキュリティーグループ** など。
3. リージョンを選択します。
4. リソースリストで、タグのバインドを解除するリソースを選択します。タグでリソースをフィルタリングし、目的のリソースを選択することもできます。
5. リソースリストの下部にある **タグの編集** をクリックします。
6. **タグの編集** ダイアログボックスで、タグの横にある削除アイコンをクリックします。
7. **確認** をクリックして、タグのバインドを解除します。

タグが正常にアンバインドされているかどうかを確認するには、インスタンスの **タグの編集** 機能を使用するか、ECS コンソールの左側のナビゲーションバーで **タグ** をクリックします。

タグでのフィルタリング

タグがリソースにバインドされた後、次の 2 つの方法を使用してリソースをタグでフィルタリングできます。

リソースリストによるリソースのフィルタリング

リソースをフィルタリングするには、次の手順を参照してください。

1. ECS コンソールにログインします。
2. 左側のナビゲーションペインで、リソースタイプを選択します。**インスタンス**、**クラウドディスク**、**スナップショット**、**イメージ**、**セキュリティグループ** など。
3. リージョンを選択します。
4. リソースリストの上部にある **タグ** をクリックします。
   - キーにバインドされているリソース (複数の値を持つ可能性がある) を取得するには、該当キーをクリックします。
   - キーと値のペア (タグ) にバインドされているリソースを取得するには、該当キーと値をクリックします。コンソールは、キーまたはキーと値のペア (タグ) にバインドされているリソースのリストを返します。

タグでのリソースフィルタリング

リソースをフィルタリングするには、次の手順を参照してください。

1. ECS コンソールにログインします。
2. 左側のナビゲーションペインの **タグ** をクリックします。
3. リージョンを選択します。
4. 検索ボックスにキーを入力し、**検索** をクリックします。

コンソールは、キーにバインドされているリソースのリストを返します。

Resource Access Management (RAM)

Resource Access Management (RAM)

購入した ECS インスタンスを、組織内で複数のユーザーが使用するという状況は珍しくありません。これらのユーザーが同じ Alibaba Cloud アカウントのアクセスキーを共有すると、2 つの問題が生じます。

- 情報漏えいのリスクが高くなる。
- ユーザーのアクセス権限を制限できず、不適切な操作によるセキュリティリスクを招くおそれがある。

Resource Access Management (RAM) は、リソースアクセスを制御するための Alibaba Cloud のサービスです。このサービスを使用すると、ユーザー (従業員、システム、アプリケーションなど) をまとめて管理し、ユーザーがアクセスできるリソースを制御することができます。

RAM はリソースアクセス権限の管理に役立ちます。たとえば、ネットワークセキュリティの管理を強化する

ために、特定のグループに権限付与ポリシーを設定できます。責任者の名前で行われた ECS リソースへのアクセスリクエストでも、元の IP アドレスが企業イントラネット外のものならば拒否する、といったポリシーを規定できます。

グループごとに異なる権限を設定できます。例:

- SysAdmins (システム管理者): このグループには、ECS イメージ、インスタンス、スナップショット、セキュリティグループの作成と管理を実施する権限が必要です。このグループでは、グループメンバーの全員にすべての ECS リソースを操作できる権限を付与するポリシーを割り当てます。
- Developers (開発者): このグループには、インスタンスを使用する権限のみが必要です。このグループでは、グループメンバーの全員に DescribeInstances、StartInstance、StopInstance、CreateInstance、DeleteInstance の各メソッドを呼び出す権限を付与するポリシーを割り当てます。
- あるユーザーが開発者からシステム管理者になった場合は、簡単にそのユーザーを Developers グループから SysAdmins グループに移すことができます。

RAM に関する詳細については、**RAM プロダクトドキュメント** を参照してください。

モニタリング

ECS インスタンスがスムーズに稼動しているかどうかを確認するために、いくつかのディメンションにわたって、ECS インスタンスの実行ステータスをモニターすることができます。

ECS インスタンスの実行状態は、次の 2 つのポータルでモニターできます。

- Instance Details
- CloudMonitor

Instance Details

1. [**ECS 管理コンソール**] にログインします。
2. 左側のナビゲーションバーで [**インスタンス**] をクリックします。次に、ページの一番上でリージョンを選択します。
3. モニター対象のインスタンスを見つけて、そのインスタンス名をクリックします。
4. [**インスタンスの詳細**] ページで、CPU 使用率やアウトバウンド/インバウンドのネットワークトラフィック情報などのモニタリング情報を確認できます。

モニタリング情報の説明は次のとおりです。

CPU: 表示されるモニタリングデータは、インスタンスの CPU 使用率を示します。この数字が大きいと、インスタンスの CPU 負荷も高くなっています。

- Windows インスタンスでは、インスタンスのタスクマネージャーを使用して CPU 使用率を確認できます。CPU 使用率ごとにプログラムがリストされるので、どのプログラムがサーバーの CPU リソースを使用しているかを把握できます。
- Linux インスタンスでは、top コマンドを使用して CPU 使用率の詳細を表示できます。インスタンスにログインして、コマンドラインで top コマンドを実行します。その後、Shift + P キーを押すと CPU 使用率ごとにプログラムがリストされ、どのプロセスが多くの CPU リソースを使用しているか確認できます。

ネットワーク: 表示されるモニタリングデータは、インスタンスのインターネットトラフィックを kbps 単位で表します (1 Mbps = 1,024 kbps)。モニタリングデータはインバウンドとアウトバウンドのインスタンストラフィックを示します。1 Mpbs の帯域幅について、アウトバウンドネットワークトラフィックが 1,024 kbps に達するとき、帯域幅は最大限に使用されています。

CloudMonitor

1. 管理コンソールで、[**プロダクト**]、[**CloudMonitor**] の順に選択するか、[**インスタンスの詳細**] ページで [**アラームルール**] をクリックします。
2. 左側のナビゲーションバーで [**ECS**] をクリックし、モニター対象とするインスタンスの名前を選択します。
3. [**インストールガイド**] をクリックして、インスタンス OS をモニターします。[**モニタリングチャート**] をクリックすると、各種の基本パラメーターが表示されます。[**アラームルール**] をクリックすると、アラームルールを設定できます。

CloudMonitor の詳細については、CloudMonitor プロダクトドキュメントを参照してください。