

Cloud Virtual Machine

お知らせ・リリースノート

製品ドキュメント



Tencent Cloud

Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

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

Trademark Notice



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

Service Statement

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

カタログ：

お知らせ・リリースノート

製品の動向

パブリックイメージのリリースノート

お知らせ

CentOS 7用の一部のイメージ Pip パッケージ管理ツールの更新のお知らせ

CentOS 8サポート終了についてのお知らせ

SUSE商用版イメージのサポート終了のお知らせ

複数のアベイラビリティーゾーンのCVM価格改定（値下げ）のお知らせ

OrcaTermプロキシIPアドレスの更新についてのお知らせ

シリコンバレー地域の標準型S3 CVMの価格調整

Tencent CloudのLinux イメージ長期脆弱性のリカバリポリシーのお知らせ

Ubuntu10.04イメージのオフラインおよび既存リポジトリ設定に関するお知らせ

Ubuntu14.04 が Tomcat を起動できないのソリューションについてのお知らせ

Windows のCVMが Virtio ENIドライバーをアップグレードすることについてのお知らせ

セキュリティグループの53ポートの設定に関するお知らせ

Windows Server 2003 システムイメージをサポートしないことについてのお知らせ

Windows Server 2008 R2 Enterprise Edition SP1 64ビットシステムイメージのサポート終了のお知らせ

お知らせ・リリースノート

製品の動向

最終更新日： : 2024-04-26 16:46:02

2024 年 4 月

動向名	動向の説明	関連するドキュメンテーション
CVM は年額・月額をサポートします。	年額・月額は CVM の前払い方式で、1 ヶ月分または複数ヶ月分、さらに数年分の料金を一括で前払いするもので、従量課金方式より価格が安いですが、インスタンスの有効期限が切れるまでに早期払い戻しをサポートしていません。	課金方式

パブリックイメージのリリースノート

最終更新日：：2024-03-22 15:25:45

ご注意：

イメージの更新時間はリージョンによって異なる場合があります。ここで提供されるイメージの更新時間は、すべての Tencent Cloud リージョンでイメージの更新が完了した時間です。

Tencent Cloudが提供するパブリックイメージのメンテナンスサイクルは公式に発表されているメンテナンスサイクルと一致します。公式に発表されているメンテナンス時間については、[OSの公式メンテナンスプラン](#)をご参照ください。

OpenCloudOS

OpenCloudOSの更新記録については、[OpenCloudOSイメージ更新ログ](#)をご参照ください。

CentOS

イメージバージョン	イメージ情報	最終更新日	更新内容
CentOS Stream 9x86_64	イメージID： img-9xqekomx 現在のカーネルバージョン：5.14.0-202.el9.x86_64	2022-12-19	最新のパッチでシステムを更新します。
CentOS Stream 8x86_64	イメージID： img-8m9ugrip 現在のカーネルバージョン：4.18.0-348.7.1.el8_5.x86_64	2022-09-16	最新のパッチでシステムを更新します。
Centos 8.5x86_64	イメージID： img-es95t8wj 現在のカーネルバージョン：4.18.0-348.7.1.el8_5.x86_64	2022-11-23	最新のパッチでシステムを更新します。
CentOS 8.4x86_64	イメージID： img-l5eqiljn 現在のカーネルバージョン：4.18.0-348.7.1.el8_5.x86_64	2022-11-07	最新のパッチでシステムを更新します。
CentOS 8.3x86_64	イメージID： img-5w4qozfr 現在のカーネルバージョン：4.18.0-348.7.1.el8_5.x86_64	2022-11-07	最新のパッチでシステムを更新します。
CentOS	イメージID： img-n7nyt2d7	2022-	最新のパッチでシステムを更新

8.2x86_64	現在のカーネルバージョン：4.18.0-348.7.1.el8_5.x86_64	08-24	します。
CentOS 8.0x86_64	イメージID： img-25szkc8t 現在のカーネルバージョン：4.18.0-348.7.1.el8_5.x86_64	2022-03-17	最新のパッチでシステムを更新します。
CentOS 7.9x86_64	イメージID： img-l8og963d 現在のカーネルバージョン：3.10.0-1160.71.1.el7.x86_64	2023-03-06	最新のパッチでシステムを更新します。
CentOS 7.8x86_64	イメージID： img-3la7wngt 現在のカーネルバージョン：3.10.0-1160.62.1.el7.x86_64	2022-04-19	最新のパッチでシステムを更新します。
CentOS 7.7x86_64	イメージID： img-1u6l2i9l 現在のカーネルバージョン：3.10.0-1160.62.1.el7.x86_64	2022-04-22	最新のパッチでシステムを更新します。
CentOS 7.6x86_64	イメージID： img-9qabwvbn 現在のカーネルバージョン：3.10.0-1160.62.1.el7.x86_64	2022-04-28	最新のパッチでシステムを更新します。
CentOS 7.5x86_64	イメージID： img-oikl1tzv 現在のカーネルバージョン：3.10.0-1160.71.1.el7.x86_64	2022-12-02	最新のパッチでシステムを更新します。
CentOS 7.4x86_64	イメージID： img-8toqc6s3 現在のカーネルバージョン：3.10.0-1160.62.1.el7.x86_64	2022-04-19	最新のパッチでシステムを更新します。
CentOS 7.3x86_64	イメージID： img-dkwyg6sr 現在のカーネルバージョン：3.10.0-1160.62.1.el7.x86_64	2022-04-22	最新のパッチでシステムを更新します。
CentOS 7.2x86_64	イメージID： img-31tjrph 現在のカーネルバージョン：3.10.0-1160.83.1.el7.x86_64	2023-03-06	最新のパッチでシステムを更新します。
CentOS 6.10x86_64	イメージID： img-fizif873 現在のカーネルバージョン：2.6.32-754.35.1.el6.x86_64	2022-01-17	最新のパッチでシステムを更新します。
CentOS 6.9x86_64	イメージID： img-i5u2lkoz 現在のカーネルバージョン：2.6.32-754.30.2.el6.x86_64	2022-01-18	最新のパッチでシステムを更新します。

Ubuntu

イメージバージョン	イメージ情報	最終更新日	更新内容
Ubuntu 22.04x86_64	イメージID : img-487zeit5 現在のカーネルバージョン : 5.15.0-56-generic	2022-12-08	最新のパッチでシステムを更新します。
Ubuntu 20.04x86_64	イメージID : img-22trbn9x 現在のカーネルバージョン : 5.4.0-126-generic	2022-09-20	最新のパッチでシステムを更新します。
Ubuntu 18.04x86_64	イメージID : img-pi0ii46r 現在のカーネルバージョン : 4.15.0-193-generic	2022-11-03	最新のパッチでシステムを更新します。
Ubuntu 16.04x86_64	イメージID : img-pyqx34y1 現在のカーネルバージョン : 4.4.0-210-generic	2022-03-21	最新のパッチでシステムを更新します。

Debian

イメージバージョン	イメージ情報	最終更新日	更新内容
Debian 11.4x86_64	イメージID : img-btz2mndd 現在のカーネルバージョン : 5.10.0-16-amd64	2022-09-08	最新のパッチでシステムを更新します。
Debian 11.1x86_64	イメージID : img-4cmp1f33 現在のカーネルバージョン : 5.10.0-19-amd64	2022-11-03	最新のパッチでシステムを更新します。
Debian 10.12x86_64	イメージID : img-7ay90qj7 現在のカーネルバージョン : 4.19.0-21-amd64	2022-09-23	最新のパッチでシステムを更新します。
Debian 10.11x86_64	イメージID : img-h1yvfw1 現在のカーネルバージョン : 4.19.0-22-amd64	2022-11-01	最新のパッチでシステムを更新します。
Debian 10.2x86_64	イメージID : img-qhtfjw1d 現在のカーネルバージョン : 4.19.0-19-amd64	2022-11-01	最新のパッチでシステムを更新します。

Debian 9.13x86_64	イメージID : img-5k0ys7jp 現在のカーネルバージョン : 4.9.0-19-amd64	2022-09-30	最新のパッチでシステムを更新します。
Debian 9.0x86_64	イメージID : img-6rrx0ymd 現在のカーネルバージョン : 4.9.0-19-amd64	2022-11-03	最新のパッチでシステムを更新します。
Debian 8.11x86_64	イメージID : img-2lj11q1f 現在のカーネルバージョン : 3.16.0-11-amd64	2022-11-07	最新のパッチでシステムを更新します。

Red Hat Enterprise Linux

イメージバージョン	イメージ情報	最終更新日	更新内容
Red Hat Enterprise Linux 8.5	イメージID : img-r5xber0b 現在のカーネルバージョン : 4.18.0-425.19.2.el8_7.x86_64	2023-04-27	最新のパッチでシステムを更新します。
Red Hat Enterprise Linux 7.9	イメージID : img-0qhxyz7dl 現在のカーネルバージョン : 3.10.0-1160.88.1.el7.x86_64	2023-04-27	最新のパッチでシステムを更新します。

説明：

CVMを購入したときにRed Hat Enterprise Linux認証に合格したインスタンスタイプを選択した場合は、Red Hat Enterprise Linuxイメージを使用できます。サポートされているイメージタグとインスタンスタイプについては、[Red Hat Enterprise Linux イメージに関するよくあるご質問](#)をご参照ください。

AlmaLinux

イメージバージョン	イメージ情報	最終更新日	更新内容
AlmaLinux 9.0x86_64	イメージID : img-f089mf4l 現在のカーネルバージョン : 5.14.0-70.13.1.el9_0.x86_64	2022-10-27	イメージがリリースされました。

AlmaLinux 8.6x86_64	イメージID : img-jy2bb29p 現在のカーネルバージョン : 4.18.0-372.19.1.el8_6.x86_64	2022-10-25	最新のパッチでシステムを更新します。
AlmaLinux 8.5x86_64	イメージID : img-4ogcw28j 現在のカーネルバージョン : 4.18.0-348.20.1.el8_5.x86_64	2022-09-30	最新のパッチでシステムを更新します。

Fedora

イメージバージョン	イメージ情報	最終更新日	更新内容
Fedora36x86_64	イメージID : img-ge141oql 現在のカーネルバージョン : 5.19.14-200.fc36.x86_64	2022-11-07	最新のパッチでシステムを更新します。
Fedora 37x86_64	イメージID : img-d7j9x59z 現在のカーネルバージョン : 6.0.7-301.fc37.x86_64	2022-11-30	イメージがリリースされました。

FreeBSD

イメージバージョン	イメージ情報	最終更新日	更新内容
FreeBSD 13.1x86_64	イメージID : img-ng3lehjp 現在のカーネルバージョン : 13.1-RELEASE	2022-09-16	最新のパッチでシステムを更新します。
FreeBSD 13.0x86_64	イメージID : img-1lkqxfp 現在のカーネルバージョン : 13.0-RELEASE	2022-09-02	最新のパッチでシステムを更新します。
FreeBSD 12.3x86_64	イメージID : img-j9m732cx 現在のカーネルバージョン : 12.3-RELEASE	2022-01-20	最新のパッチでシステムを更新します。
FreeBSD 12.2x86_64	イメージID : img-pi37fg9j 現在のカーネルバージョン : 12.2-RELEASE	2022-01-20	最新のパッチでシステムを更新します。

FreeBSD 11.4x86_64	イメージID : img-aif2u6pf 現在のカーネルバージョン : 11.4-RELEASE	2022-10-27	最新のパッチでシステムを更新します。
-----------------------	--	------------	--------------------

Rocky Linux

イメージバージョン	イメージ情報	最終更新日	更新内容
Rocky Linux 9.0x86_64	イメージID : img-k1g1wwy9 現在のカーネルバージョン : 5.14.0-70.13.1.el9_0.x86_64	2022-11-25	イメージがリリースされました。
Rocky Linux 8.6x86_64	イメージID : img-no575grb 現在のカーネルバージョン : 4.18.0-372.9.1.el8.x86_64	2022-11-25	最新のパッチでシステムを更新します。
Rocky Linux 8.5x86_64	イメージID : img-qd4bf0jb 現在のカーネルバージョン : 4.18.0-348.20.1.el8_5.x86_64	2022-10-10	最新のパッチでシステムを更新します。

OpenSUSE

イメージバージョン	イメージ情報	最終更新日	更新内容
OpenSUSE Leap 15.4	イメージID : img-aaa4d8d1 現在のカーネルバージョン : 5.14.21-150400.22-default	2022-08-31	イメージがリリースされました。
OpenSUSE Leap 15.3	イメージID : img-1e4uwwol 現在のカーネルバージョン : 5.3.18-59.27-default	2022-11-02	最新のパッチでシステムを更新します。
OpenSUSE Leap 15.2	イメージID : img-i6u3kbtj 現在のカーネルバージョン : 5.3.18-lp152.106-default	2022-01-07	最新のパッチでシステムを更新します。
OpenSUSE Leap 15.1	イメージID : img-4orfj3l 現在のカーネルバージョン : 4.12.14-lp151.28.91-	2021-12-21	最新のパッチでシステムを更新します。

現在のカーネルバージョン：4.12.14- lp151.28.91-default		
--	--	--

Windows

イメージバージョン	イメージ情報	最終更新日	更新内容
Windows Server 2022 IDC 64-bit Chinese	イメージID : img-9lw52tbx	2023-01-06	最新のパッチでシステムを更新します。
Windows Server 2022 IDC 64-bit English	イメージID : img-cg67n3n9	2023-01-06	最新のパッチでシステムを更新します。
Windows Server 2019 IDC 64-bit Chinese	イメージID : img-perxw61f	2023-03-09	最新のパッチでシステムを更新します。
Windows Server 2019 IDC 64-bit English	イメージID : img-1dmc4wwp	2023-03-09	最新のパッチでシステムを更新します。
Windows Server 2016 IDC 64-bit Chinese	イメージID : img-gu1nmb8d	2023-03-09	最新のパッチでシステムを更新します。
Windows Server 2016 IDC 64-bit English	イメージID : img-6fp83vpb	2023-03-09	最新のパッチでシステムを更新します。
Windows Server 2012 R2 IDC 64-bit Chinese	イメージID : img-ixj8o53x	2023-01-06	最新のパッチでシステムを更新します。
Windows Server 2012 R2 IDC 64-bit English	イメージID : img-bpsjt7n	2023-01-06	最新のパッチでシステムを更新します。

お知らせ

CentOS 7用の一部のイメージ Pip パッケージ管理ツールの更新のお知らせ

最終更新日：：2023-06-25 17:52:18

背景情報

一部のTencent Cloud CentOS 7 パブリックイメージには、CentOSディストリビューションに付属するPython 2-pip 8.1.2 がデフォルトでインストールされますが、このバージョンの pip では、ユーザーはインストールする互換性のあるパッケージバージョンを選択できません。デフォルトで最新のパッケージがインストールされます。ただし、pipの最新バージョンと、NumPy などの一般的に使用される一部のアプリケーションツールは、Python 2をサポートしていません、pip をアップグレードするコマンド (pip install pip --upgrade) を実行するとき、または特定のアプリケーションツールをインストールするときに、互換性の問題が発生する可能性があります。この問題を解決するために、Tencent Cloud は CentOS 7 シリーズの一部のイメージのpipを更新しました。

更新内容と範囲

以下の表に、更新された pip を含む CentOS 7パブリックイメージを示します。リスト内のパブリックイメージはデフォルトでPython 2 がインストールされており、pip は pip 8.1.2 から [pip 20.3.4](#)にアップグレードされています。

説明：

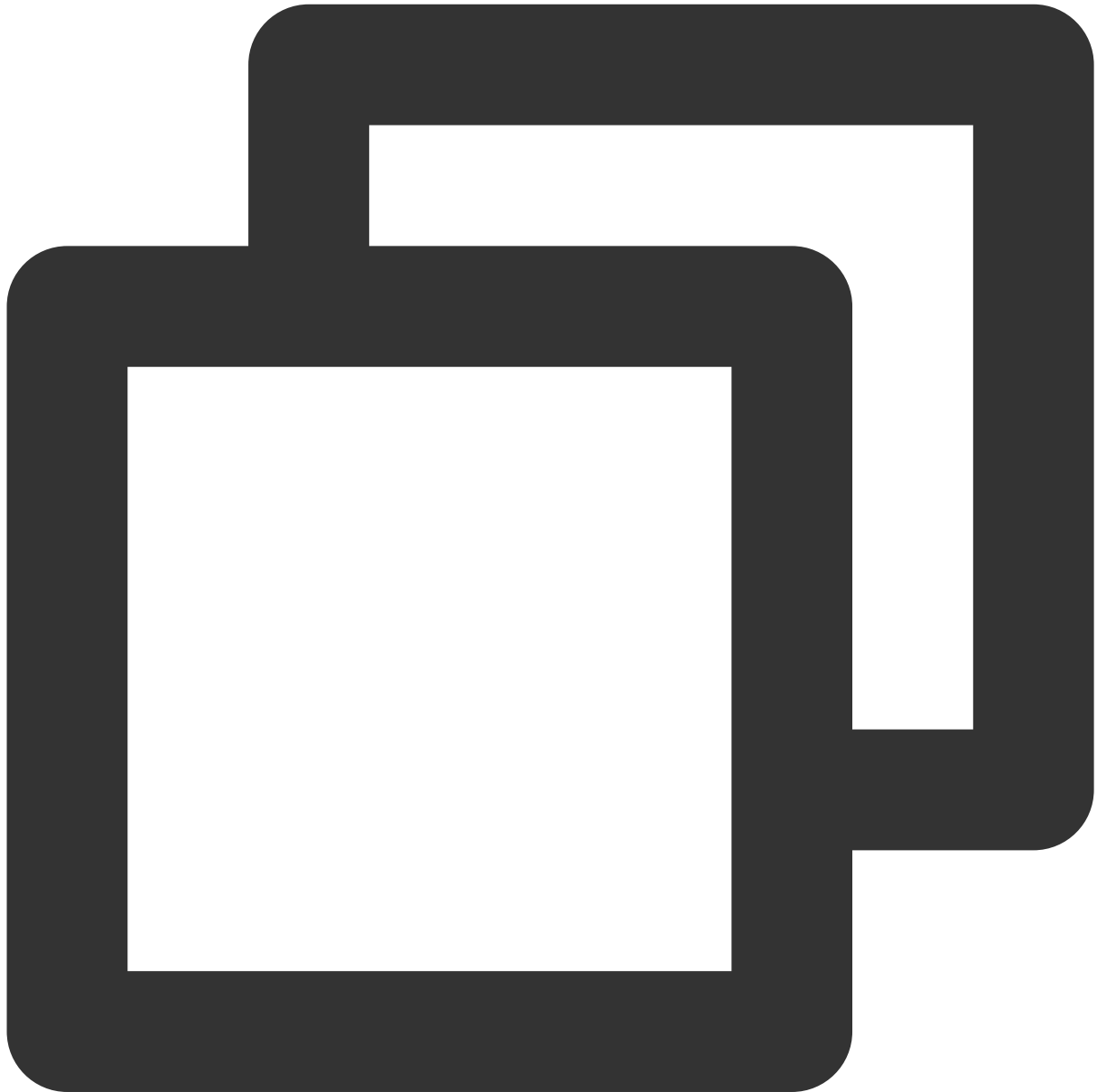
アップグレードは段階的に実行され、2022年12月12日に終了しました。対応するパブリックイメージのアップグレード後に購入したインスタンスは自動的に更新されますが、アップグレード前に購入したインスタンスは更新されません。操作ガイドを参照して手動でアップグレードを行うことができます。

イメージバージョン	イメージID
CentOS 7.9 64-bit	img-180g963d
CentOS 7.6 64-bit	img-9qabwvbn
CentOS 7.9 64-bit+SG1-pv1.5	img-all2luul
CentOS 7.9 64-bit+SG1-pv1.6	img-ojhiw86l
CentOS 7.4(arm64)	img-k4xgkxa5

操作ガイド

pip のアップグレード

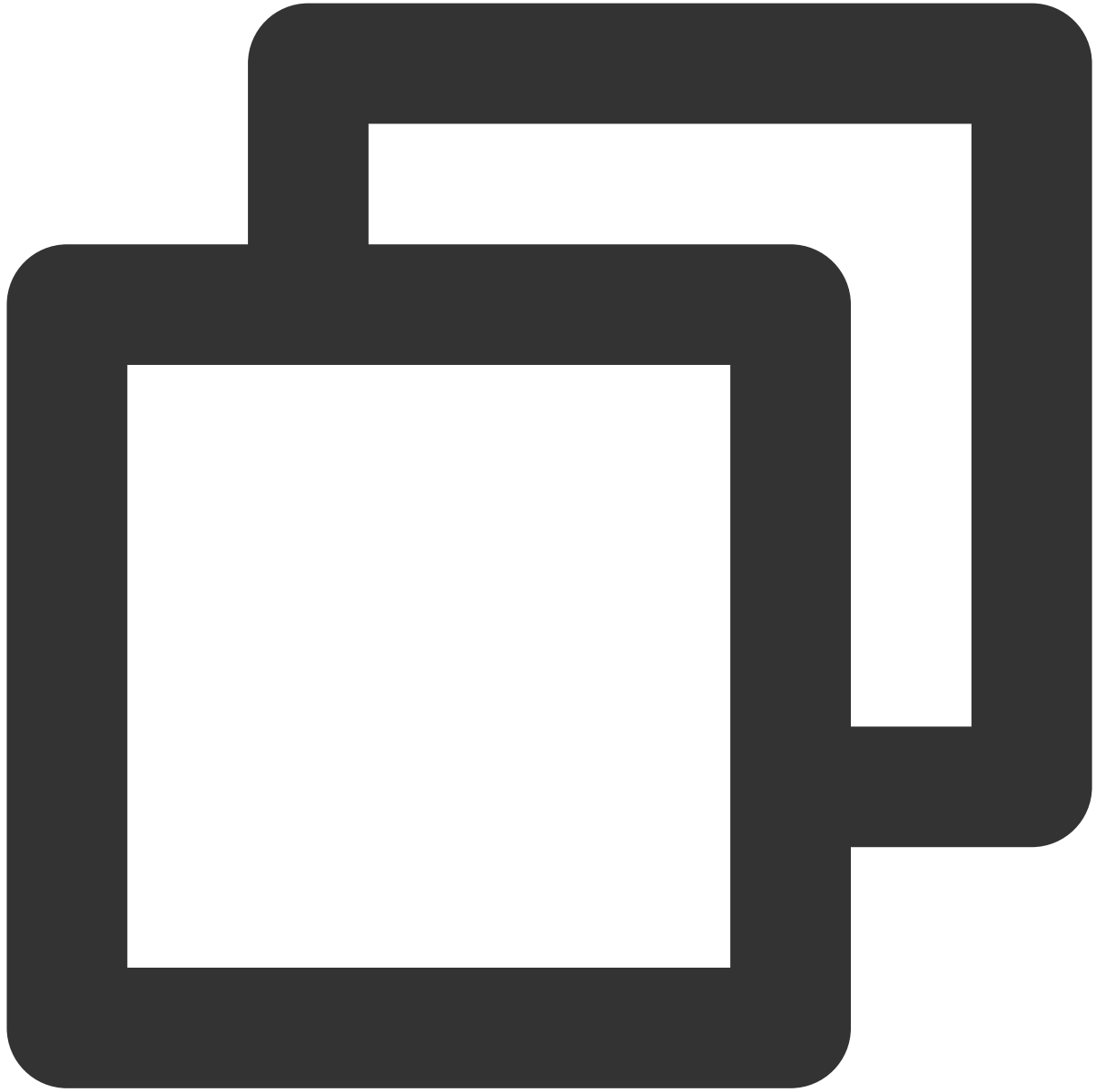
次のコマンドを実行すると、インスタンスの pip バージョンを表示できます。



```
pip --version
```

インスタンスの pip2 のバージョンが pip 9.0 より前の場合、pip をアップグレードするとき、またはアプリケーションツールをインストールするときにエラーが発生する可能性があります。この問題を回避するには、次のコマン

ドを実行して、最初にpipを最新バージョンの pip2 pip 20.3.4 にアップグレードします。



```
pip2 install --upgrade pip==20.3.4
```

pip2のインストール

次のコマンドを実行して、pip2 の最新バージョンをインストールできます。



```
wget https://bootstrap.pypa.io/pip/2.7/get-pip.py  
python2 ./get-pip.py -i http://mirrors.tencentyun.com/pypi/simple --trusted-host mi
```

製品に関するご質問がある場合は、[チケットを送信](#)してください。

CentOS 8サポート終了についてのお知らせ

最終更新日：：2023-08-07 09:58:39

CentOSは、CentOS Linuxプロジェクトのサポートを終了する予定で、2022年1月1日よりCentOS 8のサポートを終了します。CentOS 7は2024年6月30日よりメンテナンスを終了します。詳細については、[CentOS公式お知らせ](#)をご参照ください。

説明事項

当面、Tencent Cloudは、CentOS 8シリーズのイメージをオフラインしないが、CentOS 8シリーズのイメージとOSバージョンの更新を停止します。業務への影響を防ぐために、Tencent Cloudは、以下のイメージバージョンを提供しています。

TencentOS Server：10年以上にわたってTencentがOS分野で蓄積してきたノウハウを生かし、Tencentの膨大な内部業務により検証し精進されてきました。Tencent内部OSの99%以上を占め、Tencentのすべての業務をカバーしています。

OpenCloudOS：OpenCloudOSをお勧めします。そのベーシックライブラリとユーザスペースコンポーネントは、CentOS 8と完全な互換性を持っています。また、1000万以上のノードで検証した結果、カーネルの最適化とエンハンスメントにより、安定性が70%向上し、特定の運用シーンでの性能が50%向上し、ユーザにCentOS 8より優れたソリューションが提供されます。

CentOS StreamおよびUbuntuなどその他のリリースされたバージョン

CentOSをご利用中の場合、お早めに対応するバージョンのOpenCloudOSまたはTencentOS Serverに移行することをお勧めします。移行操作の詳細については、[CentOSのTencentOS Serverへの移行ガイド](#)をご参照ください。

SUSE商用版イメージのサポート終了のお知らせ

最終更新日： : 2022-05-07 16:03:45

Tencent Cloudは2022年1月1日より、SUSE商用版のパブリックイメージおよび対応する認証サービスの新しいサポートの追加を停止します。バージョンは次のとおりです：

SUSE Linux Enterprise Server 12 SP3

SUSE Linux Enterprise Server 12

SUSE Linux Enterprise Server 10

既存のユーザーが引き続きパブリックSUSEイメージを使用する場合は、SUSEのカスタマー担当者に連絡してください。SUSEプロバイダーが、対応するテクニカルサポートをユーザーに提供します。連絡先：

電話：+86-10-6533-9000

メール：sales-inquiries-apac@suse.com

複数のアベイラビリティーゾーンのCVM価格改定（値下げ）のお知らせ

最終更新日：：2022-12-14 09:47:05

Tencent Cloud CVMは2021年3月10日より一部価格の値下げを実施します。今回の価格調整は国内の複数のメインストリームリージョン、アベイラビリティーゾーンおよびオンラインの90%を超えるインスタンスタイプをカバーするものです。具体的な値下げ幅はアベイラビリティーゾーンやインスタンス仕様により異なりますが、最大10%の値下げとなります。

カバーする範囲	説明
アベイラビリティーゾーン	広州6区、北京6区、南京1区、南京2区、南京3区
インスタンスタイプ	標準型S5、標準型SA2、標準型S4、標準メモリ拡張型 S5se、メモリ型M5、コンピューティング型C5、コンピューティング型C4、ビッグデータ型D3、ビッグデータ型D2、High IO型IT5、High IO型IT3

調整の詳細

2021年3月10日より最新価格を適用します。本ドキュメントは価格調整についてのみ説明するものであり、具体的な価格については、公式サイト価格センター、購入ページ、価格計算機の最新価格を基準とします。

2021年3月10日以降、**購入/更新**価格調整の対象となるサブスクリプションや従量課金CVMに、最新の優待価格が適用されます。

説明事項

今回の価格調整は、CVMインスタンス仕様に関わるコンピューティングリソース費用のみを対象とし、ネットワークやクラウドストレージ費用は対象外です。

この告知の適用期間は2021年3月10日から次のCVM価格調整までです。

CVMの最新価格は [料金センター](#) で検索できます。クラウドストレージ、ネットワーク料金の具体的な価格については、[CVM価格計算機](#) で計算してください。

CVMインスタンスタイプに関連する情報の詳細については、[インスタンス仕様](#) をご参照ください。

関連する質問

現在のアカウントに従量課金制のCVMが1台あるのですが、**2021年3月10日以降**、自動的に最新の優待料金が適用されますか。

適用されます。従量課金制のCVM料金は1時間単位の課金ですので、アカウントにすでに作成された従量課金CVMインスタンスについては、公式サイトで最新価格が正式に発表された後、最初の1時間より請求書に最新の優待価格が適用されます。価格の正式な発表時間は、公式サイトおよび請求書の作成時点を基準とします。

イベントで購入したCVMに最新の優待価格は適用されますか。

その他のイベントで購入したCVMには、個別の優遇プランが適用されているため、今回の値下げの対象外です。今回の価格調整は、CVM購入ページ、またはAPIを通じて購入されたインスタンスのみに適用され、イベントなどのその他購入ポータルで購入されたインスタンスには適用されません。

お問い合わせ

ご不明な点がございましたら、[お問い合わせ](#)までお気軽にご連絡ください。Tencent Cloudに対する長年のご愛顧に感謝申し上げます。Tencent Cloudは引き続きさらに費用対効果の高い製品をご提供いたします。

OrcaTermプロキシIPアドレスの更新についてのお知らせ

最終更新日：：2023-07-07 15:34:42

背景情報

OrcaTermサーバーの拡張とアップグレードのため、2021年4月1日以降、orcaTerm プロキシ IPアドレスに新しいCIDRブロックが追加されます。セキュリティグループで新しいorcaTermプロキシIP CIDRブロックとリモートログインポート（デフォルトではポート22）を開いてください

説明：

OrcaTermログインの詳細については、[標準のログイン方法を使用してLinuxインスタンスにログインする（推奨）](#)ドキュメントをご参照ください。

調整の詳細

新しいプロキシIP CIDRブロックは次のとおりです。

81.69.102.0/24

106.55.203.0/24

101.33.121.0/24

101.32.250.0/24

新旧のプロキシIPアドレス/CIDRブロックは並行して使用されます。以下のIPアドレス/CIDR ブロックを含みます：

説明：

セキュリティグループのインバウンド（ソース）ルールで、新旧のプロキシIP CIDRブロックとリモートログインポートが開かれていることを確認してください。

81.69.102.0/24

106.55.203.0/24

101.33.121.0/24

101.32.250.0/24

115.159.198.247

115.159.211.178

119.28.7.195

119.28.22.215

119.29.96.147

211.159.185.38

関連する操作

[標準のログイン方法を使用してLinuxインスタンスにログインする \(推奨\)](#)

[セキュリティグループルールの追加](#)

シリコンバレー地域の標準型S3 CVMの価格調整

最終更新日： : 2020-09-27 17:36:00

シリコンバレー地域のTencent Cloud標準型S3CVMの従量課金価格調整：

OS	値下げ幅
Linux	21パーセント値下げ
Windows	10パーセント値下げ

説明事項

調整後の価格は2020年7月24日より発効します。

このドキュメントは価格調整についてのみ説明しておりますので、具体的な価格については、[CVM 料金計算ツール](#)に移動して見積もりしてください。

ご不明の点があれば、いつでもお気軽に[お問い合わせ](#)ください。

Tencent CloudのLinux イメージ長期脆弱性のリカバリポリシーのお知らせ

最終更新日：：2020-07-01 16:42:25

Tencent Cloudセキュリティセンターは、さまざまなセキュリティ上の脆弱性に細心の注意を払っています。重要なセキュリティの脆弱性が正式にリリースされた後、Tencent Cloudセキュリティセンターはタイムリーに脆弱性に関する情報をフォローアップし、ユーザーに脆弱性情報を公開し、脆弱性の対処方法を提供します。

Tencent Cloud公式イメージの脆弱性修正期間

定期的な脆弱性の修正：Tencent Cloudの公式イメージは、一般的な脆弱性に対して、年に 2 回の頻度で修正を定期的に行います。

危険性が高い脆弱性の修正：危険性が高い脆弱性に対しては、Tencent Cloudは至急に修正し、迅速に顧客に提供します。

脆弱性修正の対象となるイメージの範囲

Tencent Cloudは、イメージに対するセキュリティメンテナンスの原則をアップストリームイメージの公式リリースバージョンと一致させ、公式メンテナンス期間内にあるシステムバージョンに対して、セキュリティメンテナンスを実施します。

CentOS

CentOSは、現在リリースされたメジャーバージョンの最新マイナーバージョンに対するソフトウェアと脆弱性の更新のみをサポートしています。Tencent Cloudのメンテナンス原則は、CentOSの公式メンテナンス原則と一致させ、公式メンテナンス期間内にあるメジャーバージョンの最新マイナーバージョンのみに対して、脆弱性の定期的な修正と高リスクの脆弱性の緊急修正を行います。

以下に、Tencent Cloudの既存のCentOSイメージに関するメンテナンス情報を示します。

CentOS 7.6 64ビット (Centos公式サポート対応)

CentOS 7.5 64ビット (Centos公式サポート対応)

CentOS 7.4 64ビット (Centos公式サポート対応)

CentOS 7.3 64ビット (Centos公式サポート対応)

CentOS 7.2 64ビット (Centos公式サポート対応)

Centos 7.1 64ビット (Centos公式サポート終了)

Centos 7.0 64ビット (Centos公式サポート終了)

Centos 6.9 32/64ビット (Centosは次のバージョンがリリースされるまでサポートを提供し続けます)

Centos 6.8 32/64ビット (Centos公式サポート終了)
Centos 6.7 32/64ビット (Centos公式サポート終了)
Centos 6.6 32/64ビット (Centos公式サポート終了)
Centos 6.5 32/64ビット (Centos公式サポート終了)
Centos 6.4 32/64ビット (Centos公式サポート終了)
Centos 6.3 32/64ビット (Centos公式サポート終了)
Centos 6.2 64ビット (Centos公式サポート終了)
Centos 5.11 32/64ビット (Centos公式サポート終了)
Centos 5.8 32/64ビット (Centos公式サポート終了)

Ubuntu

Ubuntuは、LTSバージョンシステムに対するソフトウェアと脆弱性の更新メンテナンスを長期的に提供します。各LTSシステムのサーバーバージョンは5年間の更新サポートを継続します。Tencent Cloudは、各LTSバージョンのサーバーシステムを公式に提供し、Ubuntuの公式リリースしたものと一致させ、メンテナンス期間内にあるイメージに対して、脆弱性の定期的な更新と高リスクの脆弱性の至急修正を行います。

以下に、Tencent Cloudの既存のUbuntu イメージに関するメンテナンス情報を示します。

Ubuntu 18.04 LTS 64ビット (Ubuntu公式サポート対応)
Ubuntu 16.04 LTS 64ビット (Ubuntu公式サポート対応)
Ubuntu 14.04 LTS 32/64ビット (Ubuntu公式サポート対応)
Ubuntu 12.04 LTS 64ビット (Ubuntu公式サポート終了)
Ubuntu 10.04 LTS 32/64ビット (Ubuntu公式サポート終了)

Debian

Debianは、stableとoldstableの主な2つのブランチシステムを公式にメンテナンスしています。stableは現在の安定版であり、oldstableはその前の安定版です。Debianは、stableシステムに対してソフトウェアと脆弱性の更新を維持します。oldstableに対しては、ボランティアとコミュニティはLTS（長期サポート）のメンテナンスソリューションを提供します。Tencent Cloudのメンテナンスポリシーは、Debianのメンテナンスポリシーと一致させ、Debianの公式メンテナンス対象となるstableブランチシステムのみに対して脆弱性の定期的な修正を行います。

以下に、Tencent Cloudの既存のDebian イメージに関するメンテナンス情報を示します。

Debian 9.0 64ビット (Debian公式サポート対応)
Debian 8.2 32/64ビット (Debianは、2019年6月にこのバージョンのサポートの提供を停止する予定です)
Debian 7.8 32/64ビット (Debian公式サポート終了)
Debian 7.4 64ビット (Debian公式サポート終了)

openSUSE

Tencent Cloudは、openSUSEシステムのライフサイクルに基づき、公式のサポート対象となるシステムに対してイメージの脆弱性の定期的な修正を行います。

以下に、Tencent Cloudの既存のopenSUSE イメージに関するメンテナンス情報を示します。

openSUSE 42.3 (openSUSE公式サポート対応)
openSUSE 13.2 (openSUSE公式サポート終了)
openSUSE 12.3 32/64ビット (openSUSE公式サポート終了)

FreeBSD

FreeBSD 11.0-RELEASE以降、FreeBSDはstableブランチに5年間のメンテナンスを提供します。11.0-RELEASEより前のバージョンの場合、FreeBSDはバージョンに応じて異なるサポートサイクルが提供されます。Tencent Cloudのメンテナンス原則は、FreeBSDの公式メンテナンス原則と一致させます。

以下に、Tencent Cloudの既存のFreeBSDイメージに関するメンテナンス情報を示します。

FreeBSD 11.1 64ビット (FreeBSD公式サポート対応)
FreeBSD 10.1 64ビット (FreeBSD公式サポート終了)

商用バージョンシステム

Tencent Cloudは、商用バージョンシステムの脆弱性の更新とメンテナンスを提供していません。

Ubuntu10.04イメージのオフラインおよび既存リポジトリ設定に関するお知らせ

最終更新日：：2020-05-06 14:59:58

UbuntuはUbuntu 10.04 LTSのメンテナンスを正式に停止したため、そのため、Tencent Cloud もUbuntu10.04 バージョンのパブリックイメージの提供を停止しています。

Ubuntu10.04 LTSのディレクトリツリーは、最新の公式ソースウェアハウスから削除されました。Tencent Cloud のソフトウェアリポジトリは公式サイトと一致するために、公式ソースディレクトリツリーでUbuntu 10.04 LTS のサポートを提供しなくなりました。ユーザーに上位バージョンのイメージを置き換えることを推奨します。

既存のユーザーが Ubuntu 10.04 ソフトウェアソースを引き続き使用したい場合、次の2つの方法を提供します：

方法一：構成ファイルを手動で更新する

ユーザーエクスペリエンスを向上させるために、Tencent Cloud ソフトウェアリポジトリは Ubuntu 10.04 LTSの公式アーカイブソース <http://old-releases.ubuntu.com/ubuntu/> をユーザーに提供します。ユーザーは構成ファイルを手動で変更することにより、当該のリポジトリを使用できます：

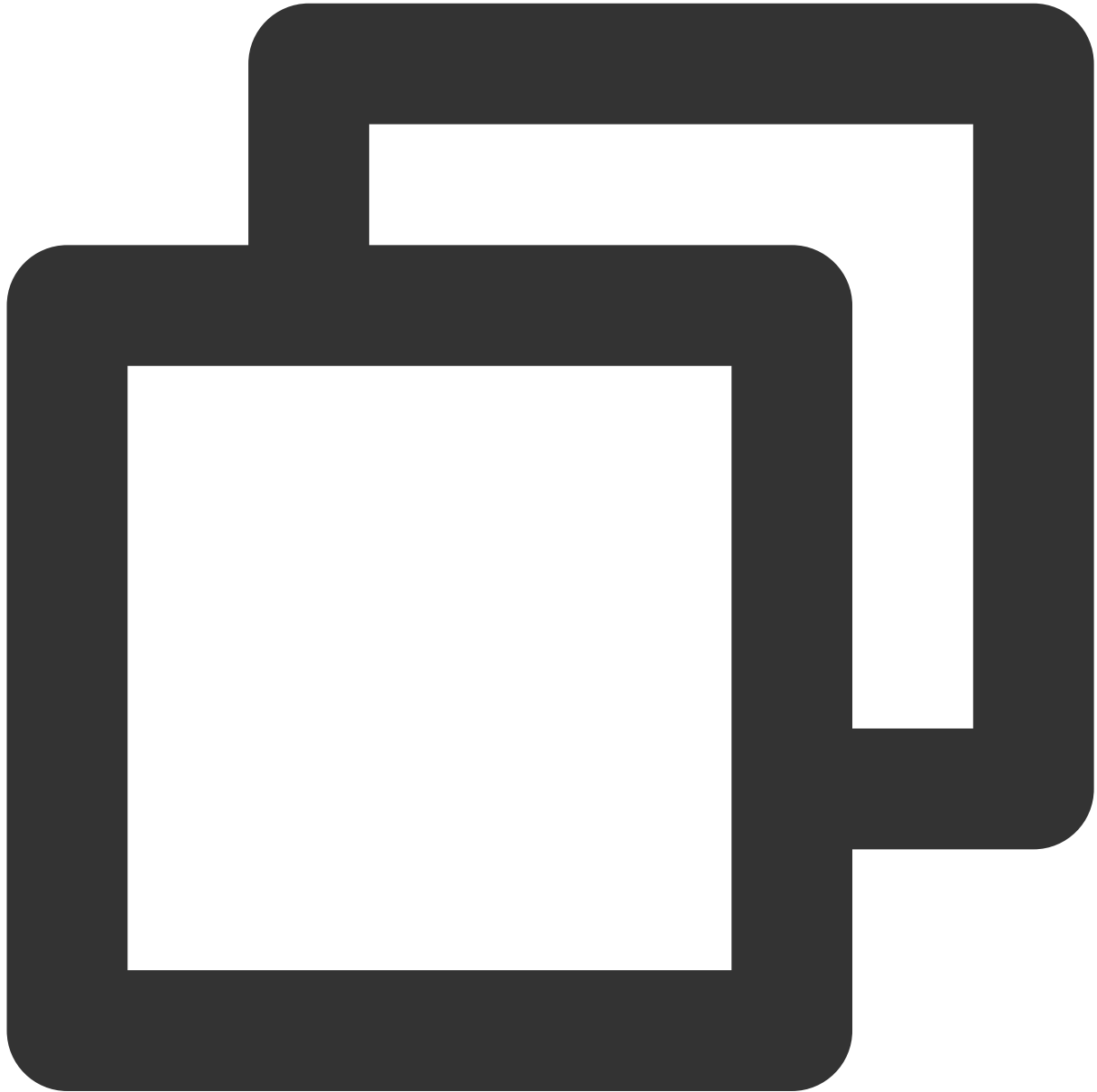
apt のソース構成ファイルを開き `vi /etc/apt/sources.list` 、以下のコードを変更します：



```
deb-src http://mirrors.tencentyun.com/old-archives/ubuntu lucid main restricted uni
deb-src http://mirrors.tencentyun.com/old-archives/ubuntu lucid-updates main restri
deb-src http://mirrors.tencentyun.com/old-archives/ubuntu lucid-security main restr
deb-src http://mirrors.tencentyun.com/old-archives/ubuntu lucid-backports main rest
deb http://mirrors.tencentyun.com/old-archives/ubuntu lucid main restricted univers
deb http://mirrors.tencentyun.com/old-archives/ubuntu lucid-updates main restricted
deb http://mirrors.tencentyun.com/old-archives/ubuntu lucid-security main restricte
deb http://mirrors.tencentyun.com/old-archives/ubuntu lucid-backports main restrict
```

方法二：自動化スクリプトを実行する

Tencent Cloudが提供するスクリプト [old-archive.run](#) を使用して設定するには、当該のファイルを Ubuntu 10.04 Cloud Virtual Machine にダウンロードして、以下のコマンドを実行します：



```
chmod +x old-archive.run  
./old-archive.run
```

Ubuntu14.04 が Tomcat を起動できないのソリューションについてのお知らせ

最終更新日：：2023-03-28 09:46:35

ユーザーの皆様へ

Tencent Cloudは「Tencent Cloud公式サイトから購入したUbuntu14.04 CVMにapt-getを使用してTomcatとHadoopをインストールすると、ポートは正常にリッスンできますが、リクエストに応答できないこと」を検出しました。Tencent Cloudは対応する回避策を提示します。このような状況が発生したら、お勧めの対処方法で回避することをお勧めします。

問題の原因

Java Runtime Environment の [既知の問題](#) に起因する問題です。

問題の分析

TomcatとHadoopはJava言語で開発され、`java.security.SecureRandom`のAPIが使用されています。

このAPIはあるJREの中でデフォルトで `/dev/random` を利用して生成されていますが、`/dev/random` はCPU温度、キーボード等のハードウェアのノイズを受信して、エントロピーを生成します。CVMの仮想マシン環境では、CPU温度などの信号を検知してエントロピーを生成することは困難です。そのため、`cat /dev/random` はほぼブロックされ、TomcatとHadoopが起動できなくなります。

ソリューション

JRE設定を変更する

元の `/etc/java-7-openjdk/security/java.security`（実際のURLに基づく）中の `securerandom.source=file:/dev/urandom` を `securerandom.source=file:/dev/./urandom` に変更して、上記の問題を回避します。

Windows のCVMが Virtio ENI ドライバーをアップグレードすることについてのお知らせ

最終更新日：：2024-01-04 10:31:43

2016年6月–8月中旬に作成されたWindows CVMが極端な状況でインターネットの中断問題を防ぐため（極端な状況は通常業務の運行に影響が出る可能性がある）、我々はアップグレードプログラムを提供してVirtio ENI ドライバーをアップグレードします。下記のアップグレード手順に従ってアップグレードプログラムをインストールするのを強く推奨します。リスタートすればこの問題を解決できます。

Tencent Cloudの利用者は下記のプライベートネットワークアドレスからアップグレードプログラムをダウンロードし、ワンクリックでアップグレードを完成できます。ユーザーは [Windows CVM にログインする](#) 必要があり、内部のイメージウェブサイト

`http://mirrors.tencentyun.com/install/windows/update_netkvm.exe` にアクセスし、ダウンロードしてから直接アップグレードプログラムを実行するか又は保存してから実行します。

下記の情報が表示された場合：ドライバーがアップグレード成功したことを示し、OSをリスタートしてから新しいドライバーが有効になります。

下記の情報が表示された場合：既存のドライバーが問題ないことを示し、アップグレードする必要がありません。

セキュリティグループの53ポートの設定に関するお知らせ

最終更新日：：2022-04-25 19:01:32

概要

ポート53はDNS（Domain Name Server、ドメイン名サーバー）サーバーによって開放され、主にドメイン名の解決に使用されます。DNSサーバーを介してドメイン名とIPアドレス間の変換を実現し、ユーザーはドメイン名を記憶すれば、ウェブサイト迅速にアクセスできます。

『電気通信業務分類ディレクトリ』（2015版）は再帰的なインターネットドメイン名解決サービスが電気通信業務に分類しています（コード番号はB26-1）。すなわち、ドメイン名の再帰的なサービスに従事するには、電気通信業務の許可を取得する必要があります。

関連する政策と法律規制要件

1、ビジネスライセンスを取得していない場合、インターネットドメイン名解決サービスに従事することはできません。

貴社が当該業務に携わっている場合、「エンコードとプロトコル変換業務ライセンス」を取得する必要があります、具体的な取り扱い方法については、所属の省の通信管理局にお問い合わせください。

『電気通信業務許可の管理措置』第四十六条：本管理措置の第十六条の第一項規約および第二十八条の第一項規約により、許可されていない電気通信業務または範囲外の電気通信業務に従事している場合、『中華人民共和国の電気通信規則』第六十九条規約に基づく処罰し、状況が深刻な場合、業務中止と命じられ、電気通信業務経営の不正行為リストに加入されます。

中華人民共和国工業情報化部『インターネットドメイン名の管理措置』第三十六条：ドメイン名解決サービスを提供する場合、企業は関連法律、規制、基準を順守し、対応する技術、サービス、ネットワークおよび情報セキュリティ保証機能を備え、ネットワークおよび情報セキュリティの安全対策を講じ、法律に従ってドメイン名解決ログ、メンテナンスログ及び変更記録を記録及び保存し、解決サービスの品質と解決システムのセキュリティを保証します。電気通信業務に関与している場合、電気通信業務のビジネスライセンスを法律に従って取得する必要があります。

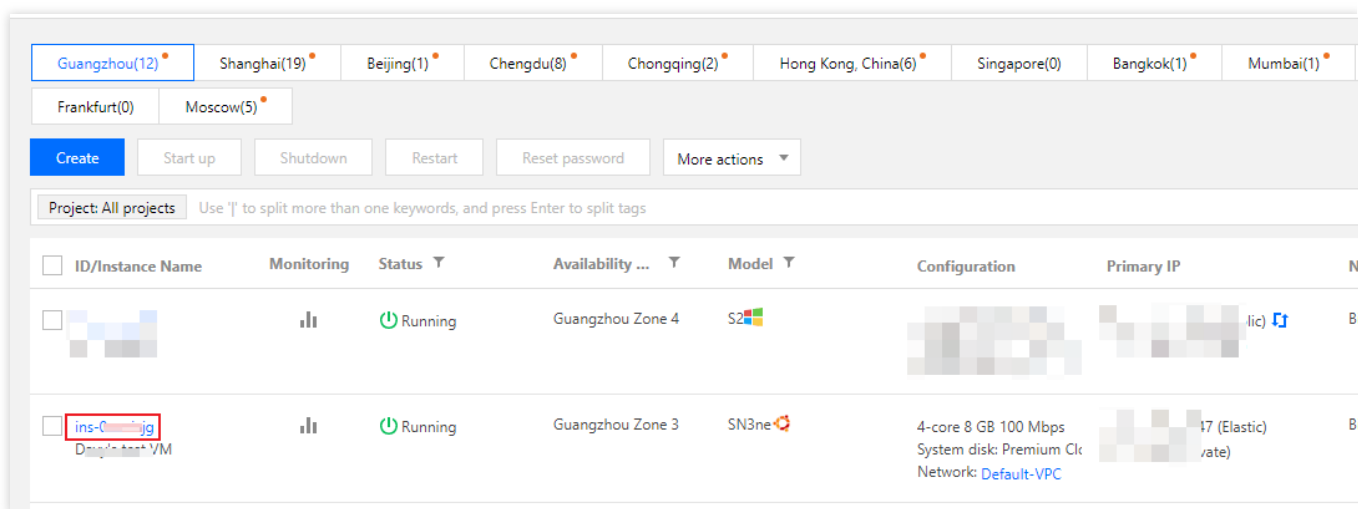
2、Tencent Cloudでは、法律に従ってビジネスライセンスを取得していない、または非経営性インターネット情報サービスICP申告手続きを実行する会社または個人にアクセスや料金請求代理などのサービスを提供することはできません。『電気通信業務許可の管理措置』：第二十四条 アクセスサービスを提供する付加価値電気通信事業者は、次の規制を遵守する必要があります：（三）法律に従ってビジネスライセンスを取得していない、または非経営性インターネット情報サービスICP申告手続きを実行する会社または個人にアクセスや料金請求代理などの

サービスを提供することはできません。

個人（会社）はインターネットドメイン名解決サービスに従事していない場合、サーバーのセキュリティグループポリシーを調整し、インバウンドルールによってポート53を無効にすることをお勧めします。

インバウンドルールによるポート53を無効にする手順

1. [Tencent Cloud Cloud Virtual Machine コンソール](#) にログインします。
2. インスタンスの管理画面で、ポート53を無効にしたいインスタンスを選択し、当該インスタンスの「ID/名称」をクリックします。下図に示すように：



3. インスタンスの詳細画面で、**セキュリティグループ**タブを選択して、インスタンスのセキュリティグループ管理画面に入ります。下図に示すように：

The screenshot shows the 'Security Groups' management page. On the left, the 'Bound to security group' section contains a table with one entry:

Priority	Security Group ID/name	Operation
1	TCP port 22, 80, 443, 3389 and ICMP o...	Unbind

On the right, the 'Rule preview' section shows a list of inbound rules:

Source	Port Protocol	Policy
0.0.0.0/0	UDP:500	Allow
0.0.0.0/0	UDP:4500	Allow
0.0.0.0/0	TCP:3389	Allow
0.0.0.0/0	TCP:22	Allow
0.0.0.0/0	TCP:80,443	Allow
0.0.0.0/0	ICMP	Allow
10.0.0.0/8	ALL	Allow
172.16.0.0/12	ALL	Allow
192.168.0.0/16	ALL	Allow

4. 【Bound to security group】フィールドで、変更するインバウンドルールの「セキュリティグループ ID/名称」を選択します。
5. 「Security Group Rule」画面で、【Inbound rule】タブを選択し、【Add a Rule】をクリックします。下図に示すように：

The screenshot shows the 'Security Group Rule' page for a security group named 'sg-nxqp4gj3(TCP port...)'. The 'Inbound rule' tab is selected. A red box highlights the 'Add a Rule' button. Below the button is a table of existing rules:

<input type="checkbox"/>	Source	Protocol port	Policy	Notes
<input type="checkbox"/>	0.0.0.0/0	UDP:500	Allow	-
<input type="checkbox"/>	0.0.0.0/0	UDP:4500	Allow	-
<input type="checkbox"/>	0.0.0.0/0	TCP:3389	Allow	TCP port 3389 open for Wind
<input type="checkbox"/>	0.0.0.0/0	TCP:22	Allow	TCP port 22 open for Linux C
<input type="checkbox"/>	0.0.0.0/0	TCP:80,443	Allow	Web service HTTP open
<input type="checkbox"/>	0.0.0.0/0	ICMP	Allow	Ping service open
<input type="checkbox"/>	10.0.0.0/8	ALL	Allow	All ports open for private net

6. ポップアップした「Add Inbound rule」ウインドウで、以下の情報を入力します。下図に示すように：

Type	Source ⓘ	Protocol port ⓘ	Policy
Custom ▼	0.0.0.0/0	UDP:53	Refuse ▼
+ New Line			

Completed Cancel

Type：「Custom」を選択します。

Source：「0.0.0.0/0」を入力します。

Protocol port：「UDP:53」を入力します。

Policy：「Refuse」を選択します。

7. 【Completed】をクリックすると、53ポートが無効になります。

よくあるご質問

インターネットドメイン名解決サービスとは。

インターネットドメイン名解決は、インターネットドメイン名とそれに対応するIPアドレスの関係を確立します。

インターネットドメイン名解決サービスは、インターネット上でドメイン名解決サーバーと関連ソフトウェアを構築することにより、インターネットドメイン名に対応するIPアドレスに変換します。ドメイン名解決サービスには、信頼できる解決サービスと再帰的な解決サービスが含まれます。

信頼できる解決サービス：ルートドメイン名、トップレベルドメイン名およびすべてのレベルの他のドメイン名にドメイン名解決サービスを提供することを指します。

再帰的な解決サービス：ローカルキャッシュまたは信頼できる解決サービスシステムを照会することにより、ドメイン名とIPアドレス間の対応関係を実現するサービスを指します。

ここでのインターネットドメイン名解決サービスは、特に再帰的な解決サービスを指します。詳細については『電気通信業務分類ディレクトリ（2015年版）』：B26-1 インターネットドメイン名解決サービスをご参照ください。

インバウンドルールによってポート53を無効にすると、サーバーにどのような影響がありますか。

インターネットドメイン名解決サービスに従事していない場合は、インバウンドルールがポート53を無効にしても、サーバーやビジネスに影響はありません。

個人ではインターネットドメイン名解決サービスに従事できますか。

通信サービスプロバイダーは、法律に基づいて設立された会社である必要があります。個人はこのタイプのサービスに従事することはできません。インターネットドメイン名解決サービス業務に従事するには、「エンコードとプロトコル変換ビジネスライセンス」を申請する必要があります。ビジネスライセンス取得の詳細については、通信管理局にお問い合わせください。

ビジネスライセンスなしでインターネットドメイン名解決サービス業務に従事すると、どのような影響がありますか。

『中華人民共和国の電気通信規則』第六十九条によると：（一）本規制の第七条第三項、または本規則の第五十八条第（一）項に記載されている行為のいずれかの規定に違反して、許可されていない電気通信業務または範囲外の電気通信業務に従事している場合、国务院の情報産業部門、または省、自治区、および直轄市の電気通信管理機関は、機能と権限に応じて修正を命令し、違法所得を没収、違法所得の3倍から5倍の罰金を科します。違法所得がない、または違法な収入が5万元未満の場合、10万元以上100万元未満の罰金が科せられ、状況が深刻な場合、事業を停止するよう命じられます。

Windows Server 2003 システムイメージをサポートしないことについてのお知らせ

最終更新日： : 2020-01-08 17:25:18

利用説明

Microsoftは2015年7月14日からWindows Server 2003 とWindows Server 2003 R2への拡張サポートサービスを停止しました。同時に、Tencent CloudでWindows Server 2003 OS Tencent CVMを実行する場合、この日付以降にはMicrosoftからのアップデートとパッチを取得できません。また、プログラムの互換性、不安定性、セキュリティなどの問題及びリスクに直面します。

業務の安全性と安定性を保障するため、既存のWindows Server 2003のCVMをWindows Server の上位バージョン（例えば、Windows Server 2008 R2 とWindows Server 2012 など）へマイグレーションするのを推奨します。

リスク通知

MicrosoftからWindows Server 2003のアップデートプログラムとパッチを取得できないため、Tencent CloudはOSに関連する問題を解決できません。Windows Server 2003を継続利用する場合、下記のリスクを充分ご了承ください。

1. Windows Server 2003 OSのTencent CVMを継続利用する場合、2015年7月14日以降、Microsoftが提供するアップデートプログラムとパッチを継続取得することはできなくなります。同時に、お客様のアプリケーションと業務はさまざまなリスクに直面します。セキュリティ問題、アプリケーションの非互換性、コンプライアンス要件、および他の非機能問題によって引き起こされる不確定なセキュリティリスクを含み、それに限定されません。
2. 2015年7月14日以降、Windows Server 2003のTencent CVMを継続利用する場合、このOSに対するMicrosoftのサポートの欠如により、故障、セキュリティ問題、非互換性、又はより高い不確定なリストを引き起こす場合、Tencent Cloudはこれに責任を負いません。お客様が該当するリスク、結果、責任を負う必要があります

サービスの知っておくこと

MicrosoftからWindows Server 2003 のアップデートプログラムとパッチを取得できないため、Tencent CloudはOSに関連する問題を解決できません。下記状況はTencent Cloudのサービス品質不良、故障又は責任に属しません。

1. Windows Server 2003を利用しているインスタンスは、障害のリスクが高くなる可能性があります。さまざまなセキュリティ問題、非互換性、または適切に動作できないことが発生し、完全にフリーズする場合があります。
2. Windows Server 2003インスタンスで実行中のアプリケーションが故障した場合、Microsoftパッチをインストールするか、又はMicrosoftからOSレベルのトラブルシューティングサポートを提供して頂くことによって問題を解

決めます。我々はトラブルシューティングの協力のみサポートし、完全な問題解決策を提供することができません。

3. ハードウェアの互換性とドライバー関連の問題に制限されているため、将来新しいTencent CVM はWindows Server 2003イメージをサポートできなくなる可能性があります。

Windows Server 2008 R2 Enterprise Edition SP1 64ビットシステムイメージのサポート 終了のお知らせ

最終更新日：：2023-02-01 10:21:53

利用説明

Microsoftは2020年1月14日からWindows Server 2008関連OSのサポートサービスを停止しました。Tencent Cloudは2020年3月16日からWindows Server 2008 R2 Enterprise Edition SP1 64ビットのパブリックイメージのサービス終了となり、同時に、Tencent CloudでWindows Server 2008 R2 Enterprise Edition SP1 64ビットシステムを使用するCVMはこの日付以降にはMicrosoftからのアップデートとパッチを取得できず、プログラムの互換性、不安定性、セキュリティなどの問題やリスクに直面することになります。

お客様の業務の安全性と安定性を確保するために、既存のWindows Server 2008 R2 Enterprise EditionのCVMをより新しいバージョンのWindows Serverに切り替えることをお勧めします。最新バージョンを推奨します。

リスクを十分に評価して警告を受け、Windows Server 2008 R2 Enterprise Editionを使用してインスタンスの作成またはリーインストール場合は、[カスタムイメージ](#)をインポートすることで、この問題を解決することができます。

リスク通知

MicrosoftからWindows Server 2008のアップデートプログラムとパッチを取得できないため、Tencent CloudはOSに関連する問題を解決できません。Windows Server 2008 R2 Enterprise Edition SP1 64ビットシステムを引き続き利用する場合、下記のリスクを充分ご了承ください。

1. Windows Server 2008 R2 Enterprise Edition SP1 64ビットOSを含むTencent CVMを引き続き利用する場合、2020年3月16日以降、Microsoftが提供するアップデートプログラムとパッチを継続取得することはできなくなります。同時に、お客様のアプリケーションと業務はさまざまなリスクに直面することになります。それはセキュリティ問題、アプリケーションの非互換性、コンプライアンス要件、および他の非機能問題によって引き起こされる不確定なセキュリティリスクを含み、それに限定されません。
2. 2020年3月16日以降、Windows Server 2008のTencent CVMを継続利用する場合、このOSに対するMicrosoftのサポートの欠如により、故障、セキュリティ問題、非互換性、又はより高い不確定なリストを引き起こす場合、Tencent Cloudはこれに責任を負いません。お客様が該当するリスク、結果、責任を負う必要があります。

サービスの知っておくこと

MicrosoftからWindows Server 2008 のアップデートプログラムとパッチを取得できないため、Tencent CloudはOSに関連する問題を解決できません。下記状況はTencent Cloudのサービス品質不良、故障又は責任に属しません。

1. Windows Server 2008 R2 Enterprise Edition SP1 64ビットシステムを利用しているインスタンスは、障害のリスクが高くなり、さまざまなセキュリティ問題、非互換性、または適切に動作できないことが発生し、完全にフリーズする場合があります。
2. Windows Server 2008 R2 Enterprise Edition SP1 64ビットシステムのインスタンスで実行しているアプリケーションが故障し、問題の解決するにはMicrosoftパッチをインストールするか、またはMicrosoftからOSレベルのトラブルシューティングサポートが必要な場合は、当社がトラブルシューティングについて協力するが、完全な問題解決策を提供することができません。
3. ハードウェアの互換性とドライバー関連の問題に制限されているため、将来新しいTencent CVM はWindows Server 2008イメージをサポートできなくなる可能性があります。