

# **Cloud Virtual Machine**



# 製品ドキュメント





#### **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

#### 🔗 Tencent Cloud

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:

トラブルシューティング

#### インスタンス関連障害

CVMインスタンスにログインできない原因や対処法

Windowsインスタンス関連

Windows のインスタンスにログインできない Windowsインスタンス:認証エラーが発生した CVMパスワードリセット失敗、またはパスワードが無効 Windowsインスタンス:リモートデスクトップサービスを使ったログオンを拒否 Windowsインスタンス:ネットワークレベルの認証が必要 Windowsインスタンス:Macリモートログイン異常 Windowsインスタンス:CPUまたはメモリの使用率が高いためログインできない Windowsインスタンス:リモートデスクトップでリモートパソコンに接続できない Windowsインスタンス:お使いの資格情報は機能しませんでした Windowsインスタンス:ポート問題が原因でリモートログインできない Linuxインスタンス関連 LinuxインスタンスをSSHで登録できない Linuxインスタンス:CPUまたはメモリの使用率が高いためログインできない Linuxインスタンス:ポートの問題によるログインができない

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

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

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

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

Linuxインスタンス:/etc/fstabの設定エラーによるログイン不能

Linuxインスタンス:sshd設定ファイル権限に関する問題

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

サーバーが隔離されたためログインできない

帯域幅の利用率が高いためログインできない

セキュリティグループの設定が原因でリモート接続できない

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

CVMの再起動またはシャットダウンは失敗しましたの原因と対処

Network Namespaceを作成できない

カーネルおよび IO 関連問題

システムbinまたはlibソフトリンクの欠如

CVMにウイルス侵入が疑われる場合

ファイル作成のエラー no space left on device

ネットワーク関連の故障

- 国際リンクレイテンシー
- ウェブサイトにアクセスできません
- ウェブサイトのアクセスラグ
- ネットワークカードマルチキュー設定エラーの場合
- CVMネットワークディレーとパケットロス
- CVMネットワークアクセスパケット損失
- インスタンス IP アドレスを ping できない
- ドメイン名を解析できない(CentOS 6.x システム)

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

最終更新日:::2023-05-16 09:54:55

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

# 考えられる原因

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



トラブルシューティング

#### インスタンスタイプを確認する

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

Windows インスタンスにログインできない

Linuxインスタンスにログインできない

#### 診断ツールを使用して原因を特定する

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

#### セルフ診断ツール

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

#### セキュリティグループ(ポート)検証ツール

このツールは、セキュリティグループとポートに関連する故障を診断できます。セキュリティグループ設定に問題 がある場合は、このツールの「すべてのポートを開く」機能を通じて、セキュリティグループの一般的に使用さ れるすべてのポートを開くことができます。

このツールを使用して問題の原因を特定した場合、対応する問題のガイドラインに従って問題を解決することを お勧めします。

#### インスタンスの再起動

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

#### ログイン失敗のその他の一般的な原因

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

#### Windows インスタンス

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

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

Windowsインスタンス:認証エラーが発生した

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

#### Linuxインスタンス

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

後続操作

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

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

### つ

最終更新日:::2023-04-21 15:01:49

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

# 考えられる原因

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

# 自己診断ツールの使用

Tencent Cloudは、Windowsインスタンスに接続できない原因が、帯域幅、ファイアウォールおよびセキュリティ グループの設定などの一般的な問題かどうかを判断するのに役立つ自己診断ツールを提供しています。 障害の 70%はツールで特定でき、検出された問題をもとにログインできない原因となっている可能性のある障害を特定 できます。

1. セルフチェックをクリックし、自己診断ツールを開きます。

2. ツールインターフェースのプロンプトに基づき、診断したいCVMを選択し、検出開始をクリックします。 トラブルシューティングツールによって確認できない問題については、CVMに VNC方式でログイン し、段階ごと にトラブルシューティングを実施することをお勧めします。

### 障害処理

#### VNC 方式を介したログイン

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

1. Tencent Cloud コンソール にログインします。

2. 下図のように、インスタンスの管理画面で、ログインしたいインスタンスを選択し、**ログイン**をクリックしま す。



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

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

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



#### パスワードの問題によりログインできない

**障害事象**:パスワードの入力ミス、パスワードを忘れた、パスワードのリセットに失敗したなどの理由で正常に ログインできない。

**処理手順**:Tencent Cloudコンソール でインスタンスのパスワードをリセットし、インスタンスを再起動してくだ さい。詳細については、インスタンスのパスワードをリセット ドキュメントをご参照ください。

#### 帯域幅利用率が高すぎる

障害事象:自己診断ツールによって、帯域幅利用率が高すぎることが問題だと表示された。

#### 処理手順:

1. VNCログイン によってインスタンスにログインします。

2. 帯域幅の利用率が高いためログインできない ドキュメントを参照し、インスタンスの帯域幅使用状況および障害の処理について確認します。

#### サーバー負荷が高い

**障害事象**:セルフチェックツールまたはTCOPによって、サーバーのCPU負荷が高いためにシステムがリモート接 続できなくなっている、またはアクセスが非常に遅くなっていると表示された。 考えられる原因:ウイルスやトロイの木馬、サードパーティ製のウイルス対策ソフト、アプリケーションプログラ ムの異常、ドライバーの異常、またはソフトウェアのバックエンドでの自動更新によってCPU占有率が高くな り、CVMにログインできない、またはアクセスが遅いといった問題が発生している。

#### 処理手順:

1. VNCログイン によってインスタンスにログインします。

**2.** Windowsインスタンス: CPUとメモリ占用率が高いため、ログインできない ドキュメントを参照し、「タスク マネージャー」で負荷の高いプロセスを特定します。

#### リモートポート設定の異常

**障害事象**:リモート接続ができない、リモートアクセスポートがデフォルトのポートではない、変更されている、 またはポート**3389**が開かない。

問題特定の考え方:pingをインスタンスのパブリックIPに通すことができるかどうか。telnetコマンドによって ポートが開いているかどうかをテストする。

**処理手順**:具体的な操作については、ポート問題が原因でリモートログインできない ドキュメントをご参照くだ さい。

#### セキュリティグループルールが不適切

**障害事象**:セルフチェックツールでのチェックの結果、セキュリティグループルールが不適切なためにログイン できないことがわかった。

**処理手順**: セキュリティグループ(ポート)検証ツール によってチェックを行います。

#### ご注意:

Windowsインスタンスへのリモートログインにはポート3389の開放が必要です。

Protocol	Port	Direction	Policy	Effects
ТСР	3389	Inbound	Not opened 🚯	Unable to log into C
ТСР	22	Inbound	Open	None
ТСР	443	Inbound	Not opened 👔	Unable to use Web
ТСР	80	Inbound	Not opened 👔	Unable to use Web
ТСР	21	Inbound	Not opened 👔	Unable to access FTP
ТСР	20	Inbound	Not opened 👔	Unable to access FTP
ICMP	0	Inbound	Open	None
ALL	ALL	Outbound	Open	None

<br>

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

#### ファイアウォールまたはセキュリティソフトによるログインの異常

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

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

#### ご注意:

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

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

1. VNCログイン によってインスタンスにログインします。

2. OSの画面で、

をクリックし、コントロールパネルを選択し、コントロールパネルウィンドウを開きます。

3. Windowsファイアウォールをクリックし、「Windowsファイアウォール」画面に進みます。

4. 左側のWindowsファイアウォールの有効化または無効化をクリックし、「設定のカスタマイズ」画面に進みます。

5. 「プライベートネットワークの設定」と「パブリックネットワークの設定」を「Windowsファイアウォールを 無効にする」に設定し、**OK**をクリックします。

6. インスタンスを再起動してリモート接続をリトライし、リモートログインに成功するかどうかを確認します。

#### リモートデスクトップ接続における認証エラー

**障害事象**:リモートデスクトップを使用したWindowsインスタンスへの接続とログイン時に、「認証エラーが発 生しました。関数に提供されたトークンは無効です」または「認証エラーが発生しました。要求された関数はサ ポートされていません」というエラーが発生する。

問題の原因: Microsoftは2018年3月にセキュリティ更新をリリースしました。この更新はCredential Security Support Providerプロトコル(CredSSP)に基づいてID認証の過程でリクエストを検証する方法によって、

CredSSPに存在する、リモートでコードが実行される脆弱性を修正するものです。この更新はクライアントと サーバーの両方にインストールする必要があり、そうしなければ「問題の説明」のような状況が発生する可能性 があります。

**処理手順**: セキュリティ更新をインストールする方法で対処することを推奨します。具体的には、Windowsイン スタンス:認証エラーが発生した ドキュメントをご参照ください。

### その他の対処方法

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

# Windowsインスタンス:認証エラーが発生し

最終更新日:: 2023-05-16 10:56:42

## 問題の説明

た

リモートデスクトップ接続クライアントを使用してWindowsインスタンスにログインする場合は、次のエラーが 発生します。

「認証エラーが発生しました。この関数に提供されたトークンは無効です」。

「認証エラーが発生しました。要求された関数はサポートされていません」。

# 問題の分析

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

原因 1:セキュリティ更新プログラムはサーバーにインストールされていますが、クライアントにはインストール されておらず、「強制的に更新されたクライアント」ポリシーが構成されています。

原因**2**: セキュリティ更新プログラムはクライアントにインストールされていますが、サーバーにはインストール されておらず、「強制的に更新されたクライアント」ポリシーが構成されています。

原因**3**: セキュリティ更新プログラムはクライアントにインストールされていますが、サーバーにはインストール されておらず、「緩和」ポリシーが構成されています。

# 対処方法

説明:

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

#### VNC経由でCVMにログインする

1. CVMコンソール にログインします。

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

Guangzhou(12)	Shanghai(20) •	Beijing(1)	Chengdu(8)	Chongqing(2)	Hong Kong, China(6)	Singapore(0)	Bai
Create Start	up Shutdov	vn Restart	Reset password	More actions	s *		
Project: All projects	Use ' ' to split mo	re than one keywo	rds, and press Enter t	to split tags			
D/Instance Nam	ne Monito	Status Y	Availabili 🍸	Model *	Configuration	Primary IP	
	di.	() Running	Guangzhou Zon	S2	2-core 8 GB 5 Mb System disk: SSD Ck Network: Basic ne	1	<b>D</b> 

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



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

#### 解決策1:セキュリティ更新プログラムのインストール(推奨)

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



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

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

→ 設定 > 更新とセキュリティ

Windows 7:

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

をクリックし、表示されたメニューから**設定**をクリックします。

2. 「設定」が表示されます。更新とセキュリティをクリックします。

3. 「更新とセキュリティ」画面が表示されます。画面の左側からWindows Updateをクリックし、右側に表示さ れた**更新プログラムのチェック**をクリックします。

4. 画面の表示に従って、インストールの開始をクリックします。

5. インストールの完了後にインスタンスを再起動すると、更新が完了します。

#### 解決策2.ポリシーの設定変更

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

#### ご注意:

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

をクリックし、gpedit.mscと入力し、Enterを押して、「ローカルグループポリシーエディタ」を開きます。 説明:

ショートカットキー「Win+R」を使用して実行画面を開くこともできます。

2. 左側ナビゲーションツリーで、コンピューターの構成 > 管理用テンプレート>システム > 資格情報の委任を選択 し、暗号化オラクルの修復をダブルクリックします。

3. 「暗号化オラクルの修復」画面が表示されます。**有効**を選択し、保護レベルを脆弱に設定します。

4. OKをクリックして設定を完了します。

#### 解決策3:レジストリの変更

1. OS画面で、

Q

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

説明:

ショートカットキー「Win+R」を使用して実行画面を開くこともできます。

2. 左側ナビゲーションツリーで、順にコンピュータ > HKEY\_LOCAL\_MACHINE > SOFTWARE > Microsoft >

Windows > CurrentVersion > Policies > System > CredSSP > Parameters ディレクトリを開きます。 説明:

ディレクトリパスが存在しない場合は、手動で作成してください。

3. Parametersを右クリックし、新規作成 > DWORD(32ビット)値を選択し、ファイル名を

「AllowEncryptionOracle」とします。

4. 新規作成した「AllowEncryptionOracle」ファイルをダブルクリックし、「数値データ」を「2」に設定し、OK をクリックします。

5. インスタンスを再起動します。

# 関連ドキュメント

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

# CVMパスワードリセット失敗、またはパス ワードが無効

最終更新日:::2023-06-12 17:07:05

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

### 現象の説明

CVMのパスワードをリセットした後、「システムがビジー状態のため、インスタンスはインスタンスパスワードのリセットに失敗しました(7617d94c)」と表示されます。

CVMのパスワードをリセットした後、新しいパスワードは有効にならず、ログインパスワードは古いパスワード のままです。

# 考えられる原因

CVMパスワードリセットが失敗または有効にならなかったことについて考えられる理由は次のとおりです。 CVMの cloudbase-init コンポーネントが破損している、変更されている、禁止されている、または起動して いないことによります。

CVMに360 Safeguardまたは火絨などのサードパーティ製セキュリティソフトウェアをインストールしており、 サードパーティ製セキュリティソフトウェアがパスワードリセットコンポーネント cloudbase-init をブロッ クしたことにより、インスタンスのパスワードリセットが無効になった可能性があります。

# 障害の特定および処理

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

#### cloudbase-initサービスの確認

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

2. OS画面で、





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

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

9.		Services		
File Action View	Help			
♦ ♦ 🖬 🗎 0	🗈 🖬 🚺 🖬 🕨 🖬 🕪			
🔍 Services (Local)	Services (Local)			
	cloudbase-init	Name 🔺	Description	Status
		🔅 App Readiness	Gets apps re	
	Start the service	Application Experience	Processes a	
		🔍 Application Host Helper Ser	Provides ad	Running
	Description:	Application Identity	Determines	
	Cloud Initialization Service	🎑 Application Information	Facilitates t	Running
		🎑 Application Layer Gateway	Provides su	
		🌼 Application Management	Processes in	
		鵒 AppX Deployment Service (	Provides inf	
		鵒 Background Intelligent Tran	Transfers fil	Running
		鵒 Background Tasks Infrastru	Windows in	Running
		🤐 Base Filtering Engine	The Base Fil	Running
		🥋 Certificate Propagation	Copies user	Running
		🔐 cloudbase-init	Cloud Initial	
		CNG Key Isolation	The CNG ke	
		COM+ Event System	Supports Sy	Running
		COM+ System Application	Manages th	Running
		Computer Browser	Maintains a	
		Credential Manager	Provides se	<b>_</b> .
		Cryptographic Services	Provides thr	Running
		DCOM Server Process Laun	The DCOM	Running
		Device Association Service	Enables pair	
		Device Install Service	Enables a c	
		Device Setup Manager	Enables the	Durania
		Disconstin Deligy Service	The Diagram	Running
		Diagnostic Policy Service	The Diagno	Kunning
	Extended Standard			
	· · · · · · · · · · · · · · · · · · ·			

「はい」の場合は、次の手順に進んでください。

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

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

cloudba	se-init Properties (Local Computer)
General Log On I	Recovery Dependencies
Service name:	cloudbase-init
Display name:	cloudbase-init
Description:	Cloud Initialization Service
Path to executable: ''C:\Program Files\&	: Cloudbase Solutions\Cloudbase-Init\bin\OpenStackServi
Startup type:	Automatic 🗸
Service status:	Stopped
Start	Stop Pause Resume
You can specify the from here.	e start parameters that apply when you start the service
Start parameters:	
	OK Cancel Apply

5. 通常タブで、 cloudbase-init の起動タイプが自動に設定されているかどうかを確認します。

「はい」の場合は、次の手順に進んでください。

「いいえ」の場合は、 cloudbase-init の起動タイプを自動に設定してください。

6. ログインタブに切り替え、 cloudbase-init のログインIDでローカルシステムアカウントが選択されている かどうかを確認します。

「はい」の場合は、次の手順に進んでください。

「いいえ」の場合は、 cloudbase-init のログインIDを**ローカルシステムアカウント**に設定してください。 7. 通常タブに切り替え、サービスステータスの起動をクリックし、 cloudbase-init を手動で起動し、エラー が表示されるかどうかを観察します。

「はい」の場合は、CVMにインストールされているセキュリティソフトウェアを確認する を行ってください。 「いいえ」の場合は、次の手順に進んでください。

8. OS画面で、

を右クリックして**実行**を選択し、**実行**画面で**regedit**と入力し、**Enter**を押して「レジストリエディタ」ウィンド ウを開きます。 9. 左側のレジストリナビゲーションに、順にHKEY\_LOCAL\_MACHINE>SOFTWARE>Cloudbase

Solutions>Cloudbase-Initディレクトリが表示されます。

10. **ins-xxx**下のすべての「LocalScriptsPlugin」レジストリを探し、LocalScriptsPluginの数値データが2かどうかを 確認します。

Edit D	WORD (32-bit) Value
Value <u>n</u> ame: LocalScriptsPlugin	
Value data:	Base <u>H</u> exadecimal <u>D</u> ecimal
	OK Cancel

「はい」の場合は、次の手順に進んでください。

「いいえ」の場合は、LocalScriptsPluginの数値データを2に設定してください。

**11. OS**画面で、

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



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

#### CVMにインストールされているセキュリティソフトウェアを確認する

インストールされているセキュリティソフトウェアでフルスキャンを選択し、CVMに脆弱性がないか、および cloudbase-init のコアコンポーネントがブロックされていないかを確認します。

CVMの脆弱性が検出された場合は、修復してください。

コアコンポーネントのブロックが検出された場合は、ブロックを取り消してください。

cloudbase-init コンポーネントの確認および設定の手順は次のとおりです。

1.標準方式を使用してWindowsインスタンスにログイン(推奨)を参照し、目的のWindowsインスタンスにログ インします。 2. 実際にインストールされているサードパーティ製セキュリティソフトウェアに応じて、 cloudbase-init コンポーネントをリカバリし、設定します。

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

最終更新日:::2022-05-26 16:09:18

# 故障について

#### 故障1

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

#### 故障2

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

# 考えられる原因

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

### ソリューション

リモートデスクトップからWindowsインスタンスに接続するときに、故障1 が発生した場合は、リモートデスクトップサービス接続を介したログインを許可するには、Windowsインスタンスで設定されているリストにユー ザーアカウントを追加する必要があります。詳細については、リモートログインを許可する権限の設定をご参照 ください。

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

# 処理手順

#### VNCを利用してCVMにログインする

1. CVMコンソール にログインします。

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

Instances Suangzho	u 25 • Othe	er regions(6) 🔻						
Create Start up	Shut down	n Restart	Reset Password	More Actions 🔻		(i) Q. View instances n	ending repossession	
Separate Reywords with T, and	separate tags	using the enter key					inding reposition	
ID/Name	Monitorin g	Status <b>T</b>	Availability Zc 🔻	Instance Type <b>T</b>	Instance Configuration	Primary IPv4 🤅	Primary IPv6	Instance Bil
-	di	🔿 Running	Guangzhou Zone 4	Standard S5	1-core 2GB 1Mbps System disk: Premium Cloud Storage Network: Default-VPC	a A	-	Pay as you g Created at 2 15:37:31

3. ポップアップウインドウ「Windowsインスタンスにログインする」に、その他の方式(VNC)を選択し、今すぐ ログインをクリックして、CVMにログインします。

**4.** ポップアップしたログイン画面で、左上隅の「リモートコマンドの送信」を選択し、**Ctrl-Alt-Delete**をクリック すると、システムログインインターフェースに入ります。



リモートログインを許可する権限の設定

#### 説明:

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

2

をクリックして、**gpedit.msc**を入力し、**Enter**キーを押して「ローカルグループポリシーエディター」を開きます。

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



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

Allow log on through Remote Desktop Services Properties	?	$\times$
Local Security Setting Explain		
Allow log on through Remote Desktop Services		
Administrators Remote Desktop Users		
Add <u>U</u> ser or Group <u>R</u> emove		
OK Cancel	A	pply

このアカウントがリストにない場合は、手順4に進んでください。

このアカウントがリストにある場合は、チケットを送信してフィードバックしてください。

4.

**ユーザーまたはグループの追加**をクリックして、「ユーザーまたはグループの選択」のウィンドウを開きます。

5. リモートログインに使用するアカウントを入力し、**OK**をクリックします。

6. **OK**をクリックして、ローカルグループポリシーエディターを閉じます。

7. インスタンスを再起動し、このアカウントを使用してWindowsインスタンスへのリモートデスクトップ接続を 再度試してください。

#### リモートログインを拒否する権限の変更

#### 説明:

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

ク をクリック クして、**qpedit.msc**を入力し、**Enter**キーを押して「ローカルグループポリシーエディター」を開きま す。

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

🍯 Local Group Policy Editor	—
<u>File Action View H</u> elp	
🗢 🔿 🙍 📰 🔀 📴 🔒 🛛 🖬	
<ul> <li>Local Computer Policy</li> <li>Computer Configuration</li> <li>Software Settings</li> <li>Windows Settings</li> <li>Name Resolution Policy</li> <li>Scripts (Startup/Shutdowr</li> <li>Deployed Printers</li> <li>Security Settings</li> <li>Create global objects</li> <li>Create global objects</li> <li>Increase a process working set</li> <li>Local Policies</li> <li>Account Policies</li> <li>Account Policies</li> <li>Security Options</li> <li>Security Options</li> <li>Software Restriction Projections</li> <li>Software Restriction Projections</li> <li>Software Restriction Projections</li> <li>Software Restriction Projections</li> <li>Software Addit Policy</li> <li>Software Restriction Projections</li> <li>Advanced Audit Policy</li> <li>Advanced Audit Policy</li> <li>Software Restriction Projections</li> <li>Modify an object label</li> <li>Synchronize directory service data</li> </ul>	urity Settin AL SERVI AL SERVI AL SERVI AL SERVI

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

ユーザーがリストにある場合は、リストからユーザーアカウントを削除し、インスタンスを再起動します。 ユーザーがリストにない場合は、チケットを送信してフィードバックしてください。

# Windowsインスタンス:ネットワークレベルの認証が必要

最終更新日:::2023-05-16 11:12:07

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

### 故障

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

Remote	Desktop Connection
8	The remote computer requires Network Level Authentication, which your computer does not support. For assistance, contact your system administrator or technical support.

トラブルシューティング

#### 説明:

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

#### VNC経由でCVMにログインする

1. CVMコンソール にログインします。

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

Guangzhou(12)	Shanghai(20)	Beijing(1)	Chengdu(8)	Chongqing(2)	Hong Kong, China(6)	Singapore(0)	Bangkok(1)
Create Start u	p Shutdo	wn Restart	Reset password	More actions	. <b>*</b>		
Project: All projects	Use ' ' to split m	ore than one keyw	vords, and press Enter to	split tags			
D/Instance Name	Monito	Status ▼	Availabili T	Model *	Configuration	Primary IP	N
	di	(U) Running	Guangzhou Zon	S2	2-core 8 GB 5 Mb System disk: SSD Ck Network: Basic ne		<b>C1</b> Bil 

3. ポップアップされた「Windowsインスタンスにログインする」ウィンドウで、その他の方式(VNC)を選択し、 **今すぐログイン**をクリックして、CVMにログインします。

4. 表示されるログインウィンドウで、左上隅にある「リモートコマンドの送信」を選択し、Ctrl-Alt-Deleteをク リックして、システムログインインターフェースに入ります。次の図に示すように:



#### レジストリを変更する

1. OSインターフェースで、

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

2. 左側のナビゲーションツリーで、コンピューター > HKEY\_LOCAL\_MACHINE > SYSTEM >

**CurrentControlSet > Control > Lsa**ディレクトリを開き、右側のウィンドウで**Security Packages**を見つけま す。以下に示すように:

Ì				Registry Editor	
File Edi	it View Favorites Help				
File Edi	t       View       Favorites       Help         IDConfigDB       InitialMachineConfig         IPMI       View       Keyboard Layout         View       Keyboard Layout         View       Lsa         View       Lsa         View       Lsa         View       Keyboard Layout         View       Lsa         View       Lsa         View       Keyboard Layouts         View       Lsa         View       Keyboard Layouts         View       Lsa         View       Medialnterfaces         View       MediaProperties         View       MUI         View       NetDiagFx         Viework       Netyoin         Viework       Network         Viework       NetworkSetup         Viework       Notifications         Viework       Notifications         Viework       Viework         Viework       Viework         Viework       Viework         Viework       Viework         Viework       Viework         Viework       Viework         Viework       Viework			Name (Default) auditbasedirectories auditbaseobjects Authentication Packages Bounds crashonauditfail crashonaudit	Type REG_SZ REG_DWORD REG_DWORD REG_MULTI_SZ REG_BINARY REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD
	▶ • • • • • • • • • • • • • • • • • • •		$\overline{}$		
<	III			<	
Computer	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlS	et∖C	ontr	ol\Lsa	

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

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

	Edit Multi-String	x
Value name:		
Value data:		
tspkg		^
<		>
	OK Cance	el

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

Ť					Registry Editor	
File	Edit	View Fav	orites Help			
			ScEvents	^	Name	Туре
		Þ - 🚺	ScsiPort		ab (Default)	REG_SZ
			SecureBoot		ab SecurityProviders	REG_SZ
		▷ ~ ]]	SecurePipeServers			
		Þ - 🚺	SecurityProviders			
			ServiceGroupOrder			
		Þ	ServiceProvider			
		Þ.»	Session Manager			
		D	SNMP			
			SQMServiceList			
		D	Srp			
			SrpExtensionConfig			
		D H	Stillmage			
		D	Storage			
			StorageManagement			
			StorPort			
			Systeminformation			
			System Resources			
			Taminal Sancar	≡		
			Uhom			
			ush			
			ushflags			
			usbstor			
			VAN			
		Þ	Video	$\sim$	<	
Comr						

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

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

· · ·	Edit String
Value name: SecurityProviders	
Value data:	
,creassp.dii	OK Cancel

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

# Windowsインスタンス:Macリモートログイ ン異常

最終更新日:::2022-05-26 16:56:10

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

# 故障について

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

8 - 8	Microsoft Remote Desktop Beta						
∷ ≡ * · + ·	Desktops	Feeds		Q Search			
PC Name		User Account	Gateway	Date Last Connected			
✓ Saved Desktops							
📮 n 1 🖬 San							
• 🛅 ronae				2018年12月6日下			
	119.29.193.24						
y y	You are connecting to the RDP host " <b>I I I I I I I I I I</b>						
	Show Certificate	C	Cancel Continu	ue			

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

トラブルシューティング

#### 説明:

下記操作は Windows Server 2016 を例として説明します。

VNC を使用してCVMにログインする

#### 1. CVMコンソール にログインします。

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

Guangzhou(12)	Shanghai(20) *	Beijing(1)	Chengdu(8)	Chongqing(2)	Hong Kong, China(6)	Singapore(0)	Bangkok(1)	
Create Start u	p Shutdow	n Restart	Reset password	More actions	s 🔻			
Project: All projects Use ' ' to split more than one keywords, and press Enter to split tags								
D/Instance Name	Monito	Status 🍸	Availabili 🍸	Model T	Configuration	Primary IP	Netwo	
	.lı	() Running	Guangzhou Zon	S2	2-core 8 GB 5 Mb System disk: SSD Ck Network: Basic ne	1	📭 Bill by t	

3. ポップアップした「Windowsインスタンスにログインする」ウィンドウで、その他の方式(VNC)を選択し、今 すぐログインをクリックして、CVMにログインします。

4. ポップアップウィンドウで、左上隅にある「リモートコマンドの送信」を選択し、 **Ctrl-Alt-Delete** をクリック して、システムログインインターフェースに入ります。次の図に示すように:


### インスタンスのローカルグループポリシーの変更

1. OSインターフェースで、

ρ

をクリックして、 gpedit.mscを入力し、Enterキーを押して、「ローカルグループポリシーエディター」を開き ます。

説明:

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

 2. 左側のナビゲーションツリーで、コンピューターの構成 > 管理用テンプレート > Windowsコンポーネント > リ モートデスクトップサービス > リモートデスクトップ セッションホスト > セキュリティを選択し、リモート (RDP) 接続に特定のセキュリティ レイヤーの使用を必要とするをダブルクリックします。

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

4. **OK**をクリックし、設定を完了します。

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

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

最終更新日:::2021-08-12 16:33:59

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

### 説明:

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

## 考えられる原因

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

## トラブルシューティング

1. CPUまたはメモリの使用率が高くなるプロセスを特定します。

2. CPUまたはメモリの使用率が高くなるプロセスを分析します。

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

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

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

### ツール

タスクマネージャー:これは、Microsoft Windows OSでアプリケーションとプロセスを管理するためのツールで す。実行中のプロセスの名前、CPU負荷、メモリ使用量、I/Oの詳細、ログインしているユーザー、Windowsサー ビスなど、コンピューターのパフォーマンスと実行中のソフトウェアに関する情報を提供します。 プロセス:システムで実行中のプロセスの一覧です。 パフォーマンス:システムのパフォーマンスに関する全体の統計です。例とえば、全体的なCPU使用量とメモリ 使用率。

**ユーザー**:システムでセッションを持つすべてのユーザーです。

**詳細**: PID、ステータス、CPU使用率、メモリ使用量などの情報を含む、実行中のプロセスの詳細情報を提供します。

サービス:システムのすべてのサービス(実行されていないービスも含む)です。

ソリューション

### VNCを使用してCVMインスタンスにログインする

説明:

CPUまたはメモリの使用率が高いためにCVMインスタンスにログインできない場合は、VNCを使用してWindows インスタンスにログインする ことをお勧めします。

1. CVMコンソール にログインします。

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

Guangzhou(12)	Shanghai(20)	Beijing(1)	Chengdu(8)	Chongqing(2)	Hong Kong, China(6)	Singapore(0)	Bangkok(1)
Create Start	up Shutdow	n Restart	Reset password	More action	s v		
Project: All projects	Use ' ' to split mor	e than one keywo	ords, and press Enter t	to split tags			
D/Instance Nam	ne Monito	Status ▼	Availabili 🍸	Model T	Configuration	Primary IP	Network
	di	() Running	Guangzhou Zon	S2	2-core 8 GB 5 Mb System disk: SSD Ck Network: Basic ne	1	<b>t</b> a Bill by tra 

3. ポップアップされた「Windowsインスタンスにログインする」画面で、その他の方式(VNC)を選択し、すぐに ログインするをクリックして、CVMにログインします。

4. ポップアップされたログインウィンドウで、下図に示すように、左上の「Send CtrlAltDe」を選択し、Ctrl-Alt-Delete をクリックすると、システムログイン画面に入ります。



### プロセスのリソース使用状況を確認する

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



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

CPUまたはメモリをクリックして、プロセスを昇順/降順で並べ替えます。

🕎 Task Manager			-		$\times$
File Options View					
Processes Performance Users Details	Services				
^	18%	11%			
Name	CPU	Memory			
Apps (1)					^
	0.2%	7.5 MD			
> 🔯 Task Manager	0.3%	1.2 MB			
Background processes (16)					
Application Frame Host	0%	2.7 MB			
> 📑 BaradAgent (32 bit)	0%	3.2 MB			
Host Process for Windows Tasks	0%	2.3 MB			
Host Process for Windows Tasks	0%	5.3 MB			
Host Process for Windows Tasks	0%	2.8 MB			
> 💫 Microsoft Distributed Transacti	0%	1.9 MB			
Microsoft Malware Protection C	0%	2.1 MB			
📧 Runtime Broker	0%	4.4 MB			
🔎 Search	0%	51.7 MB			
> 📑 sgagent (32 bit)	0%	1.8 MB			
> 🖶 Spooler SubSystem App	0%	4.2 MB			~
Fewer details				End t	ask

### プロセスを分析する

タスクマネージャーでプロセスを分析して原因を特定し、適切な対策を講じます。

### CPUやメモリリソースを大量に消費しているプロセスはシステムプロセスの場合

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

1. プロセス名を確認する。

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

2. プロセスの実行可能ファイルのパスを確認します。

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



明があります。タスクマネージャで表示するプロセスを右クリックし、ファイルの場所を開くを選択して、特定の 実行可能ファイルの場所 (svchost.exe など)を表示できます。

実行可能ファイルが C:\\Windows\\System32 ディレクトリに配置されていない場合、CVMインスタンスが ウイルスに感染している可能性があります。この場合、手動またはセキュリティソフトを使用してウイルスを検出 し、駆除してください。

実行可能ファイルが C:\\Windows\\System32 ディレクトリにある場合は、システムを再起動するか、安全 だが不要なシステムプロセスを終了します。

通常のシステムプロセスは次のとおりです。

System Idle Process:システムアイドルプロセス。CPUがアイドル状態である時間の割合を表示します。

system:メモリ管理プロセスを示します。

explorer:デスクトップとファイル管理プロセスを示します。

iexplore: Microsoft Internet Explorerのプロセスを示します。

csrss:Microsoftクライアント/サーバー上のランタイムサブシステムを示します。

svchost:DLLを実行するためのシステムプロセスを示します。

Taskmgr:タスクマネージャーを示します。

lsass:ローカルセキュリティ権限サービスを示します。

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

xmr64.exe(マイニングウイルス)などの見慣れない名前のプロセスがCPUまたはメモリリソースを大量に消費し ている場合は、CVMインスタンスがウイルスやトロイの木馬に感染している可能性があります。この場合、検索 エンジンを使用して、トロイの木馬ウイルスプロセスかどうかを検索・確認することをお勧めします。

プロセスがウイルスまたはトロイの木馬の場合は、セキュリティソフトを使用してスキャン・駆除して、必要に応じて、データをバックアップし、OSを再インストールしてください。

プロセスがウイルスやトロイの木馬でない場合は、システムを再起動するか、安全だが不要なプロセスを終了してください。

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

CPU使用率が高いプロセスは、お客様のサービスプロセスである場合、例えば:IIS、HTTPD、PHPとJava な ど、さらに分析することをお勧めします。

たとえば、現在のサービス負荷が大きいかどうかを判断します。

ビジネス負荷が大きい場合は、サーバー構成をアップグレード することをお勧めします。サーバー構成をアップ グレードしない場合は、サービスプログラムを最適化する可能性を検討して、最適化してください。

ビジネス負荷が少ない場合は、サービスエラーログをさらに分析する必要があります。たとえば、不適切なパラ メータ設定によりリソースが無駄になっていないかどうかを確認します。

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

チケットを送信して特定・対処方法について、お問い合わせください。

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

最終更新日:::2022-06-29 15:46:38

## 現象の説明

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

	Neme Rem	ote Desktop Connectio	n			$\times$		
		Remote De	esktop C <b>ion</b>					
Remote	Desktop Connecti	on			_		×	
	Remote Desktop (	can't connect to the ren	note computer f	or one of t	hese reasc	ons:		
	1) Remote access 2) The remote con 3) The remote con	to the server is not ena nputer is turned off nputer is not available o	bled on the network					
	Make sure the rem access is enabled.	note computer is turned	d on and connec	ted to the	network, a	and that	remote	_
					OK	ŀ	Help	

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

- 1) サーバーのリモートアクセスを有効にしていない
- 2) リモートコンピュータがシャットダウンされている
- 3) ネットワーク上でリモートコンピュータが利用できなくなっている

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

考えられる原因

上記が表示された原因には次のものがあります(これらに限定されません。実際の状況に応じて分析を行ってく ださい)。

インスタンスが正常な実行状態にない

パブリックIPがない、またはパブリックネットワーク帯域幅が0

インスタンスをバインドしたセキュリティグループがリモートログインポートを開放していない(デフォルトでは 3389)

リモートデスクトップサービスを起動していない

リモートデスクトップの設定に問題がある

Windowsファイアウォールの設定に問題がある

## トラブルシューティングの手順

### インスタンスが実行状態かどうかをチェックする

1. CVMコンソール にログインします。

2. 下図のように、インスタンスの管理画面で、インスタンスが「実行中」かどうかを確認します。

Instances									
Guangzhou(15)	Shanghai(0)	Beijing(0)	Chengdu(0)	Chongqing(0)	Hong Kong(0)	Singapore(0)	Bangkok(0)	Mumbai(0)	Seoul(1)
Virginia(0) Tor	ronto(1) • Fra	ankfurt(0) N	Aoscow(0)						
<b>Create</b> Start	up Shutd	own Rest	art Reset	password	re actions 🔻				Use ' ' to split
ID/Instance Nan	ne Monit	Status 🝸	Availabilit	. T Model 1	r co	onfiguration	Primary IP		Net
	- di	(U) Running	Guangzhou	Zone 3 SN3ne			na tarihin		Bill

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

### サーバーがパブリックIPを設定しているかどうかをチェックする

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

Inst	ances									
G	uangzhou(15)	Shanghai(0)	Beijing(0)	Chengdu(0)	Chongqing(0)	Hong Kong(0)	Singapore(0)	Bangkok(0)	Mumbai(0)	Seoul(1)
V	irginia(0) Tore	onto(1) Fra	ankfurt(0)	Moscow(0)						
C	reate Start	up Shutde	own Re	start Reset	password Mor	re actions 🔻			U	lse ' ' to split mo
	ID/Instance Nam	e Monit	Status <b>T</b>	Availabilit	. T Model 1	r c	onfiguration	Primary IP		Netwo
		di P	(U) Running	Guangzhou	Zone 3 SN3ne 🛟	1-	-core 2 GB 1 Mbps	193.112.71	.133 (Public) 🚺	Bill by 1

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

### パブリックネットワーク帯域幅を購入しているかどうかをチェックする

パブリックネットワーク帯域幅が0Mbかどうかをチェックします(最少1Mbps)。

「はい」の場合は、ネットワークの調整を参照し、帯域幅を5Mbps以上に調整することをお勧めします。

Instances										
Guangzhou(15)	Shanghai(0)	Beijing(0)	Chengdu(0)	Chongqing(0)	Hong Kong(0)	Singapore(0)	Bangkok(0)	Mumbai(0)	Seoul(1)	Toky
Virginia(0) To	oronto(1) Fr	ankfurt(0)	Moscow(0)							
Create Star	t up Shutd	lown Res	tart Reset	password Mo	re actions 🔻				Use ' ' to split mor	re than on
ID/Instance Nar	me Monit	Status 🔻	Availabilit	. T Model	r Co	onfiguration	Primary IP	2	Networ	k billing r
	- di	(U) Running	Guangzhou	Zone 3 SN3ne 👬	1- sy Ne	core 2 GB 1 Mbps stem cisc.rteman C etwork: VPC2	loud		Bill by tr	affic

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

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

1. CVMコンソールのインスタンス管理ページで、ログインしたいインスタンスID/インスタンス名をクリックし、 そのインスタンスの詳細ページに進みます。

2. 下図のように、セキュリティグループタブで、インスタンスのセキュリティグループがリモートログインポート(デフォルトリモートデスクトップポート:3389)を開放しているかどうかをチェックします。

the latent	er parte en e					
Basic Info	ENI Monitoring	Security Groups	Operation Logs			
Bound to	security group	Sort Bind	Rule preview	Outbound rule		
Prior	Security Group ID/name	Operation		Outbound fule		
1	14 AND 14	Unbind	▼ Open all ports-2			
	Open all ports-2		Source	Port Protocol	Policy	Notes
2	Open all ports	Unbind	0.0.0/0	TCP:3389	Allow	-
			0.0.0.0/0	ALL	Allow	-

「はい」の場合は、リモートデスクトップサービスをチェック してください。

「いいえ」の場合は、対応するセキュリティグループルールを編集し、開放してください。操作方法について は、セキュリティグループルールの追加 をご参照ください。

### リモートデスクトップサービスをチェックする

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

説明:

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

2.

を右クリックし、表示されたメニューからシステムを選択します。

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

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

「はい」の場合は、ステップ5を実行してください。

「いいえ」の場合は、チェックを入れて**OK**をクリックしてください。

5.

を右クリックし、表示されたメニューからコンピュータの管理を選択します。

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

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

「はい」の場合は、ステップ8を実行してください。

「いいえ」の場合はサービスを起動してください。

8.

を右クリックし、表示されたメニューから**実行**を選択します。

9. ポップアップした「実行」ウィンドウでmsconfigと入力し、OKをクリックします。

10. 表示された「システム設定」ウィンドウで、正常に起動にチェックが入っているかを確認します。

「はい」の場合は、Windowsインスタンスのシステム設定をチェック してください。

「いいえ」の場合は、チェックを入れて**OK**をクリックしてください。

### Windowsインスタンスのシステム設定をチェックする

1. VNCを使用してインスタンスにログイン し、Windowsインスタンスのシステム設定のトラブルシューティング を行います。

説明:

次の操作はWindows Server 2012 OSのインスタンスを例に説明します。

2.

を右クリックし、表示されたメニューから\*実行を選択します。

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



Remote L	Desktop S	Services Pro	perties (Local C	omputer)		Х			
General	Log On	Recovery	Dependencies						
Service	name:	TermServi	ce						
Display	Display name:		Remote Desktop Services						
Description: Allows users to connect interactively to a remote computer. Remote Desktop and Remote Desktop									
Path to executable: C:\Windows\System32\svchost.exe -k NetworkService									
Startup	type:	Automatic	;		~	I.			
Service	status:	Running							
						_			
S	Start	Stop	p Pa	use	Resume	Ĺ			
You car from he	Start n specify tl rre.	Stop ne start para	meters that apply	use when you star	Resume t the service				
You car from he Start pa	Start n specify tl re. arameters:	Stop ne start para	meters that apply	use when you star	Resume t the service				
You can from he Start pa	Start n specify tl re. arameters:	Stop ne start para	meters that apply	use when you star	Resume t the service				

「はい」の場合は、ステップ5を実行してください。

「いいえ」の場合は、「起動のタイプ」を「自動」に設定し、「サービスステータス」を「実行中」に設定しま す(**起動**をクリックするとサービスが起動します)。

5.

を右クリックし、表示されたメニューから\*実行を選択します。

6. ポップアップした「実行」ウィンドウに**sysdm.cpl**と入力し、**Enter**を押して、「システムのプロパティ」ウィンドウを開きます。

7. 下図のように、「リモート」タブで、リモートデスクトップの設定が「このコンピュータへのリモート接続を許可する(L)」となっているかどうかをチェックします。

System Properties ×									
Computer Name Hardware Advanced System Protection Remote									
Remote Assistance									
Allow Remote Assistance connections to this computer									
What happens when I enable Remote Assistance?									
Advanced									
Remote Desktop									
Choose an option, and then specify who can connect.									
O Don't allow remote connections to this computer									
Allow remote connections to this computer									
Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)									
Help me choose Select Users									
OK Cancel Apply									

「はい」の場合は、ステップ8を実行してください。

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

8.

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



9. 「コントロールパネル」で、**システムとセキュリティ > Windowsファイアウォール**を選択し、「Windowsファ イアウォール」を開きます。

**10**. 下図のように、「Windowsファイアウォール」でWindowsファイアウォールの状態をチェックします。



「有効」な状態であれば、ステップ11を実行してください。

「無効」な状態であれば、オンラインサポートを通してフィードバックします。

「Windowsファイアウォール」でWindowsファイアウォールによるアプリケーションの許可をクリックし、
 「許可されたアプリケーション」ウィンドウを開きます。

12. 下図のように、「許可されたアプリケーション」ウィンドウで、「許可されたアプリケーションおよび機能(A)」の「リモートデスクトップ」にチェックが入っているかどうかを確認します。



「はい」の場合は、ステップ13を実行してください。

「いいえ」の場合は、「リモートデスクトップ」にチェックを入れ、「リモートデスクトップ」を有効にしてくだ さい。

**13.**「Windowsファイアウォール」でWindowsファイアウォールの有効化または無効化をクリックし、「設定の カスタマイズ」ウィンドウを開きます。

14. 下図のように、「設定のカスタマイズ」ウィンドウで、「プライベートネットワークの設定」と「パブリック ネットワークの設定」を「Windowsファイアウォールを無効にする(非推奨)」に設定します。

<b>.</b>	Lustomiz	e se	lungs	\$ 
←	$\rightarrow$ *	1	1	<ul> <li>Windows Defender Firewall &gt; Customize Settings</li> </ul>
			Cus	stomize settings for each type of network
			Vau	an medify the firmul estimate for each type of network
			Drive	can modify the firewait settings for each type of network that you use.
			Priva	ate network settings
				<ul> <li>Block all incoming connections, including those in the list of allow</li> <li>Notify me when Windows Defender Firewall blocks a new app</li> </ul>
			V	Turn off Windows Defender Firewall (not recommended)
			Pub	lic network settings
				Turn on Windows Defender Firewall
				Block all incoming connections, including those in the list of allow
			_	Notify me when Windows Defender Firewall blocks a new app
			V	Turn off Windows Defender Firewall (not recommended)

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

# Windowsインスタンス:お使いの資格情報は 機能しませんでした

最終更新日:::2022-05-26 15:41:32

## 問題の説明

Windows OSのローカルコンピュータがRDPプロトコル(MSTSCなど)により、リモートデスクトップ接続を使用してWindows CVMにログインすると、次のエラーが表示されます。

お使いの資格情報は機能しませんでした。XXX.XXX.XXX への接続に使用された資格情報は機能しませんでした。新しい資格情報を入力してください。

Windows Security	
Your credentials did not work The credentials that were used to connect Please enter new credentials.	to : did not work.
••••••	
Use another accour	nt
Remember my credentials 🔞 The logon attempt failed	
	OK Cancel

## 処理手順

説明:

Windows Server 2012 OSを例にしていますが、OSのバージョンが異なるため、操作手順の詳細はわずかに異なります。

以下の手順に従ってトラブルシューティングを行い、各手順が実行した後、Windows CVMに再接続して問題が解 決されたか確認します。問題が解決されていない場合は、次の手順に進みます。

### ステップ1:ネットワークアクセスポリシーを変更する

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

2.05画面で、

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

3. 「Windows PowerShell」ウィンドウで、gpedit.mscを入力し、Enterキーを押すと、「ローカルグループポリ シーエディター」を起動します。

4. 左側のナビゲーションで、コンピュータの構成 > ポリシー>Windows の設定 > セキュリティの設定 > ローカル ポリシー > セキュリティ オプションディレクトリを順次展開します。

5. セキュリティオプションのネットワークアクセス:ローカルアカウントの共有とセキュリティモデルを探して 開きます。以下の通りです。

<b>I</b>	Local Group Policy Editor	
File Action View Help		
🗢 🔿 🖄 🖬 🗙 🖬 🔂 🖬		
J Local Computer Policy	Policy	Security Setting
Computer Configuration	B Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Software Settings	B Microsoft network client: Send unencrypted password to third-party SMB s	Disabled
⊿ 🚞 Windows Settings	B Microsoft network server: Amount of idle time required before suspending	15 minutes
Name Resolution Policy	B Microsoft network server: Attempt S4U2Self to obtain claim information	Not Defined
Scripts (Startup/Shutdown)	B Microsoft network server: Digitally sign communications (always)	Disabled
⊿ is Security Settings	B Microsoft network server: Digitally sign communications (if client agrees)	Disabled
Account Policies	B Microsoft network server: Disconnect clients when logon hours expire	Enabled
△ A Local Policies	B Microsoft network server: Server SPN target name validation level	Not Defined
Audit Policy	B Network access: Allow anonymous SID/Name translation	Disabled
Security Ontions	B Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Windows Firewall with Adv.	B Network access: Do not allow anonymous enumeration of SAM accounts a	Disabled
Network List Manager Polic	🛞 Network access: Do not allow storage of passwords and credentials for net	Disabled
Public Key Policies	🛞 Network access: Let Everyone permissions apply to anonymous users	Disabled
Software Restriction Policie	🛞 Network access: Named Pipes that can be accessed anonymously	
Application Control Policie	Wetwork access: Remotely accessible registry paths	System\Current(
IP Security Policies on Loca	📓 Network access: Remotely accessible registry paths and sub-paths	System\Current(
Advanced Audit Policy Cor	🛞 Network access: Restrict anonymous access to Named Pipes and Shares	Enabled
Policy-based QoS	B Network access: Shares that can be accessed anonymously	Not Defined
Administrative Templates	Network access: Sharing an security model for local accounts	Classic - local us
⊿ K User Configuration	🖏 Network security: Allow Local System to use computer identity for NTLM	Not Defined
Software Settings	Retwork security: Allow LocalSystem NULL session fallback	Not Defined
▷ Windows Settings	Retwork security: Allow PKU2U authentication requests to this computer to	Not Defined
Administrative Templates	📓 Network security: Configure encryption types allowed for Kerberos	Not Defined
	📓 Network security: Do not store LAN Manager hash value on next password	Enabled
	Wetwork security: Force logoff when logon hours expire	Disabled
	Wetwork security: LAN Manager authentication level	Not Defined
	Retwork security: LDAP client signing requirements	Negotiate signin
< III >	Retwork security: Minimum session security for NTLM SSP based (includin	Require 128-bit (

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

Network access: Sharing and security model for Io ? ×					
Local Security Setting Explain					
Network access: Sharing and security model for local accounts					
Classic - local users authenticate as themselves					
OK Cancel Apply					

7. Windows CVMに再接続し、接続に成功したか確認します。

はい、タスクは終了しました。

いいえ、ステップ2(資格情報の委任を変更する)を実行してください。

### ステップ2:資格情報の委任を変更する

「ローカルグループポリシーエディター」の左側のナビゲーションバーで、コンピューターの構成 > ポリシー
 > 管理用テンプレート > システム > 資格情報の委任ディレクトリを順次展開します。

2. 資格情報の委任 のNTLMのみのサーバー認証で保存された資格情報の委任を許可するを見つけて有効にしま す。以下の通りです。



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

Allow delegating saved	credentials with NTLM-only server authentication	
Allow delegating saved credentials v	with NTLM-only server authentication Previous Setting Next Setting	g
O Not Configured Comment:		
Enabled	Show Contents	_   □
Supported on:	Add servers to the list:	
	Value	
	TERMSRV/*	
Options:		
Add servers to the list. Show		
Add servers to the list. Show		
Concatenate OS defaults with input a		
	ОК	Can
	proper mutual authentication, delegation of saved credent	ials is
	permitted to Remote Desktop Session Host running on an	
	any domain. If the client is domain-joined, by default the	erot
	delegation of saved credentials is not permitted to any ma	chine.
	If you disable this policy setting, delegation of saved crede	ntials
	is not permitted to any machine.	-
	[	
	OK Cancel	Apply

4. **OK**をクリックします。

5. OS画面で、

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

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

 $\mathbf{\Sigma}$ 

Administrator: Windov Windows PowerShell Copyright (C) 2014 Microsoft Corporation. All rights reserved. PS C:\Users\Administrator> gpupdate /force Updating policy...

Computer Policy update has completed successfully. User Policy update has completed successfully.

7. Windows CVMに再接続し、接続に成功したか確認します。 はい、タスクは終了しました。 いいえ、ステップ3(ローカル資格情報の設定)を実行してください。

### ステップ3:ローカル資格情報の設定

1. OS画面で、

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



User Accounts

2. Windowsの資格情報の下に、現在ログインしているCVMの資格情報があるかどうかを確認します。

ない場合は、次のステップに進み、Windows資格情報を追加します。

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

3. Windows資格情報の追加をクリックして、Windows資格情報追加画面に進みます。以下の通りです。

٥		Add a Windows Credential		
€ ⊚ ◄	↑ 🙋 « Credential Manager ► Add a	v ¢	Search Control Pa	
	Type the address of the website Make sure that the user name and pass Internet or network address (e.g. myserver, server.company.com): User name: Password:	ite or network location and y sword that you type can be used to a	your crede	entials ation.
			0	KCancel

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

CVMのIPアドレスは、CVMインスタンスのパブリックIPアドレスを指します。詳細については、パブリックIPア ドレスの取得 をご参照ください。

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

5. Windows CVMに再接続し、接続に成功したか確認します。

はい、タスクは終了しました。

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

### ステップ4:CVMのパスワード保護共有の無効設定

1. OS画面で、

> コントロールパネル > ネットワークとインターネット > ネットワークと共有センター > 共有の詳細設定の変更 をクリックして、共有設定画面に進みます。以下の通りです。

æ,			Advanced sharing settings
€	9 -	ΥŤ	式 « Network and Sharing Center 🕨 Advanced sharing settings 🛛 🗸 🖒 Search Control Pa
		, ε Ε Ο Α	Change sharing options for different network profiles Windows creates a separate network profile for each network you use. You can choose specific options for each profile. Private (current profile) Guest or Public Guest or Public All Networks Public folder sharing When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders. Turn on sharing so anyone with network access can read and write files in the Public folder: Turn off Public folder sharing (people logged on to this computer can still access these folders) Password protected sharing is on, only people who have a user account and password on thi computer can access shared files, printers attached to this computer, and the Public folders. To give other people access, you must turn off password protected sharing.
			<ul> <li>Turn on password protected sharing</li> <li>Turn off password protected sharing</li> </ul>
			Save changes Cancel

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

3. Windows CVMに再接続し、接続に成功したか確認します。

はい、タスクは終了しました。

いいえ、チケットを送信して問題を報告してください。

# Windows インスタンス:ポート問題が原因 でリモートログインできない

最終更新日:::2023-06-08 16:54:00

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

### 説明:

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

## 検証ツール

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

### セルフ診断

セキュリティグループ (ポート) 検証ツール

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

## トラブルシューティング

### ネットワーク接続を検査する

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

1. ローカルコンピューターでコマンドラインツールを開きます。

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

Mac OS システム: Terminalツールを開きます。

2. 以下のコマンドを実行して、ネットワーク接続をテストします。





ping + CVM インスタンスのパブリックIP アドレス

例えば、 ping 139.199.XXX.XXX コマンドを実行します。

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

Microsoft Windows [Version 6.3.9600] (c) 2013 Microsoft Corporation. All rights reserved. C:\Users\Administrator>ping 193.112. Pinging 193.112.1 💻 💶 with 32 bytes of data: Reply from 193.112. bytes=32 time<1ms TTL=127 Reply from 193.112. bytes=32 time<1ms TTL=127 Reply from 193.112. bytes=32 time<1ms TTL=127 bytes=32 time<1ms TTL=127 Reply from 193.112. Ping statistics for 193.112. Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = Oms, Average = Oms

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

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





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

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

### telnet 139.199.XXX.XXX 3389\_

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

©2013-2022 Tencent Cloud. All rights reserved.



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



リモートデスクトップサービスの設定を検査する

VNCを介してCVMにログインする

説明:

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

1. CVMコンソール にログインします。

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



3. ポップアップした 「Windowsインスタンスにログインする」ウィンドウで、その他の方式(VNC) を選択し、す ぐにログインするをクリックします。

4. ポップアップしたログインウィンドウで、左上隅にある「Sent CtrlAltDe」を選択し、 **Ctrl-Alt-Delete** をクリッ クすると、システムログイン画面に入ります。下図の通りです。



### CVMのリモートデスクトップ設定が有効になっているかどうかを確認する

1. CVMで、**PC>プロパティ**を右クリックして、「システム」ウィンドウを開きます。

2.「システム」ウィンドウで、システムの詳細設定を選択して、「システムのプロパティ」ウィンドウを開きます。

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

	S	ystem Pro	perties		x
Computer Name	Hardware	Advanced	Remote		
Remote Assist	ance				
Allow Rem	ote Assistanc	ce connection	ns to this cor	mputer	
				Advanced	
- Remote Deskt	ор				
Choose an opt	ion, and the	n specify who	o can conne	ct.	
🔿 Don't allow	remote con	nections to th	nis computer		
<ul> <li>Allow remote connections to this computer</li> </ul>					
Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)					
Help me choos	<u>se</u>			Select Users	
OK Cancel Apply					

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

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

### リモートアクセスポートが開いているかどうかを確認する

1. CVMで、

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

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





netstat -ant | findstr 3389

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

	Administrator: Windows PowerShell					
Windows PowerShell Copyright (C) 2014 Microsoft Co	prporation. All rights r	eserved.				
<pre>PS C:\Users\Administrator&gt; nets TCP 0.0.0.0:3389 TCP 10.00.0.0:3389 UDP 0.0.0.0:3389 UDP [::]:3389 PS C:\Users\Administrator&gt; _</pre>	<pre>stat -ant   findstr 3389 0.0.0.0:0</pre>	LISTENING ESTABLISHED ESTABLISHED LISTENING				
<						

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

### レジストリのリモートポートが一致するかどうかを確認する

### ご注意:

このステップでは、 TCP PortNumberと RDP Tcp PortNumer が同じであるかどうかを確認します。 1. CVMで、



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

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

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

<i>i</i>		Registry Editor			
File Edit View Favorites Help					
	^	Name	Туре		
⊳ - 퉲 Srp		🕮 MaxIdleTime	REG_DWORD		
		3 MaxInstanceCount	REG_DWORD		
⊳ - 퉲 StillImage		100 MinEncryptionLevel	REG_DWORD		
b - b Storage		ab NWLogonServer	REG_SZ		
StorageManagement		100 OutBufCount	REG DWORD		
		R OutBufDelay	REG DWORD		
SystemInformation		110 OutBufLength	REG DWORD		
SystemResources		ab Password	REG SZ		
Þ 🕒 TabletPC					
⊿ ↓ Terminal Server		Rig PdClass	REG_DWORD		
⊳ - 🎴 AddIns			REG_DWORD		
ClusterSettings			REG_SZ		
ConnectionHandler			REG_SZ		
DefaultUserConfiguration		100 PdFlag	REG_DWORD		
👂 🌗 KeyboardType Mapping		🕮 PdFlag1	REG_DWORD		
⊳ - 🏭 RCM		ab PdName	REG_SZ		
SessionArbitrationHelper		ab PdName1	REG_SZ		
	≡	8世 PortNumber	REG_DWORD		
TerminalTypes		100 SecurityLayer	REG_DWORD		
⊳ 📲 Utilities		80 SelectNetworkDetect	REG_DWORD		
i - 📙 VIDEO		100 SelectTransport	REG DWORD		
⊳- <mark>]]</mark> Wds		30 Shadow	REG DWORD		
🖌 📲 WinStations		10 UserAuthentication	REG DWORD		
D- Console		ablisername	REG SZ		
⊳ 🚻 RDP-Tcp		WdElag	REG DWORD		
	$\sim$	<	III		
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp					

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

5. **RDP-Tcp**でPortNumberを見つけて、**RDP-Tcp**中のPortNumberデータ(ポート番号)が**tcp**中のPortNumber データ(ポート番号)と同じかどうかを確認します。下記の画像に示すように:
| ₫ <b></b>                  |       | 注册表编辑器              |           |        |
|----------------------------|-------|---------------------|-----------|--------|
| 文件(F) 编辑(E) 查看(V) 收藏夹(A)   | 帮助(H) |                     |           |        |
|                            | ^     | 名称                  | 类型        | 数据     |
| ▷ → ↓ KeyboardType Mapping |       | 100 PdClass         | REG_DWORD | 0x000  |
| Þ-III RCM                  |       | 🔢 PdClass1          | REG_DWORD | 0x000  |
| SessionArbitrationHelper   |       | ab) PdDLL           | REG_SZ    | tdtcp  |
| SysProcs                   |       | ab PdDLL1           | REG_SZ    | tssecs |
| ▷ · Juint TerminalTypes    |       | 👪 PdFlag            | REG_DWORD | 0x000  |
| ⊳ 🦺 Utilities              |       | 100 PdFlag1         | REG_DWORD | 0x000  |
| P - 🦺 VIDEO                |       | ab PdName           | REG_SZ    | tcp    |
| ⊳ - 📕 Wds                  |       | ab PdName1          | REG_SZ    | tssecs |
| ⊿ WinStations              |       | ReportNumber        | REG_DWORD | 0x000  |
| ▷ Lonsole                  |       | BecurityLayer       | REG_DWORD | 0x000  |
| RDP-Tcp                    |       | SelectNetworkDetect | REG DWORD | 0x000  |
|                            |       |                     | REG DWORD | 0x000  |
| Ubpm                       |       |                     |           | 0.000  |

同じでない場合、ステップ6を実行してください。

同じ場合は、リモートログインサービスを再起動 してください。

6.**RDP-Tcp**中のPortNumberをダブルクリックします。

6. ポップアップしたダイアログボックスで、「値データ」を0 - 65535の間で未使用ポートに変更して、TCP

**PortNumber**と**RDP Tcp PortNumer**のポート番号を一致させて、**OK**クリックします。

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

# リモートログインサービスを再起動する

1. CVMの中で、



を選択して、 services.mscを入力して、Enterキーを押して、「サービス」ウィンドウを開きます。 2. 「サービス」ウィンドウで、**リモートデスクトップサービス**を見つけて右クリックします。再開を選択して、リ モートログインサービスを再起動します。下記の画像に示すように:

<b>9</b> ,	Services				
<u>File Action View H</u> elp					
Services (Local) Services (Local)	-				
Remote Desktop Services	Name Descript	ion Status			
	Remote Access Auto Conne Creates	a co			
Stop the service	🥋 Remote Access Connection Manage	s di			
Kestart the service	🎑 Remote Desktop Configurat Remote	Des Running			
	Remote Desktop Services Allows u	iser Running			
Description:	🧠 Remote Desktop Services U Allows t	he r Runnin			
Allows users to connect interactively	🧠 Remote Procedure Call (RPC) The RPC	SS Runnin			
Desktop and Remote Desktop Session	🥋 Remote Procedure Call (RP In Winde	ows			
Host Server depend on this service.	🥋 Remote Registry Enables	rem			
To prevent remote use of this	Resultant Set of Policy Provi Provides	an			
computer, clear the checkboxes on	Routing and Remote Access Offers ro	outi			
properties control panel item.	RPC Endpoint Mapper Resolves	RP Runnin			
	Secondary Logon Enables	star			
	Secure Socket Tunneling Pr Provides	su			
	🔍 Security Accounts Manager 🛛 The star	tup Runnin			
	Server Support:	s fil Runnin			
	Shell Hardware Detection Provides	no Running			
	Smart Card Manage	s ac			
	🧠 Smart Card Device Enumera Creates	soft Running			
	Smart Card Removal Policy Allows t	he s			
	SNMP Trap Receives	; tra			
	Software Protection Enables	the			
	<				
Extended Standard /					
Stop and Start service Remote Desktop Services on Local Comp	uter				

# その他の操作

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

# Linuxインスタンス関連 Linuxインスタンス登録失敗

最終更新日:::2023-04-21 14:51:10

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

# 問題の特定

# 自己診断ツールの使用

Tencent Cloudは、帯域幅、ファイアウォールおよびセキュリティグループの設定などの一般的な問題が原因であ るかどうかを判断するのに役立つ自己診断ツールを提供しています。 障害の70%はツールで特定でき、検出され た問題をもとにログインできない原因となっている可能性のある障害を特定できます。

1. セルフチェックをクリックし、自己診断ツールを開きます。

2. ツールインターフェースのプロンプトに基づき、診断したいCVMを選択し、検出開始をクリックします。

# 自動化アシスタントを使用してコマンドを送信

自動化アシスタントを使用してインスタンスにコマンドを送信し、トラブルシューティングと問題の特定を行う ことができます。使用手順は次のとおりです。

1. CVMコンソール にログインし、インスタンスリストでインスタンスIDをクリックします。

2. インスタンス詳細ページでコマンドの実行タブを選択し、コマンドの実行をクリックします。

3. ポップアップした「コマンドの実行」ウィンドウで、必要に応じてコマンドを選択し、コマンドの実行をク リックすると、コマンドを実行してその結果を確認することができます。

例えば、新コマンド df -TH を入力して**コマンドの実行**をクリックすると、インスタンスにログインせずに結果 を確認することができます

自動化アシスタントについてより詳しい情報をお知りになりたい場合は、自動化アシスタント をご参照ください。

#### 説明:

トラブルシューティングツールによって確認できない問題については、CVMに VNC方式でログイン し、段階ごと にトラブルシューティングを実施することをお勧めします。

考えられる原因

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

# 障害処理

# VNC 方式を介したログイン

標準の方法(Orcaterm)またはリモートログインソフトウェアを使用してLinuxインスタンスにログインできない 場合は、Tencent Cloud VNCを介してログインし、障害の原因を特定できます。

1. CVMコンソール にログインします。

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

nstances									
Guangzhou(12) • Sh	anghai(19) •	Beijing(1) •	Chengdu(8) Cho	ngqing(2	2) • н	ong Kong, China(6) •	Singapore(0)	Bangkok(1)	Mumbai(1)
Frankfurt(0) Moscov	v(5) •								
Create Start up	Shutdown	Restart	Reset password	More	actions 🔻				
Project: All projects Use '	' to split more than	one keywords, ar	nd press Enter to split tags						
ID/Instance Name	Monitoring	Status <b>T</b>	Availability	т	Model 1	Con	figuration	Primary IP	
acreenano	di.	() Running	Guangzhou Zoi	ne 4	S2	2-cc Syst Net	ore 8 GB 5 Mbps em disk: SSD Cloud S work: Basic network		ic) <b>[1</b>
M	,li	U Running	Guangzhou Zoi	ne 3	SN3ne 🧔	4-cc Syst Net	ore 8 GB 100 Mbps tem disk: Premium Ck work: Default-VPC	114	η.

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

ログイン中に、パスワードを忘れた場合は、コンソールでこのインスタンスのパスワードをリセットできます。 具体的な操作については、インスタンスのパスワードをリセット ドキュメントをご参照ください。 4. ユーザー名とパスワードを入力してログインします。

# SSH問題によりログインできない

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



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

#### パスワードの問題によりログインできない

**障害事象**:パスワードの入力ミス、パスワードを忘れた、パスワードのリセットに失敗したなどの理由で正常に ログインできない。

**対処方法**: Tencent Cloudコンソール でこのインスタンスのパスワードをリセットし、インスタンスを再起動して ください。

**処理手順**:インスタンスのパスワードをリセットする方法については、インスタンスのパスワードをリセット ド キュメントをご参照ください。

#### 帯域幅利用率が高すぎる

障害事象:自己診断ツールによって、帯域幅利用率が高すぎることが問題だと表示された。

#### 処理手順:

1. VNCログイン によってインスタンスにログインします。

2. 帯域幅の利用率が高いためログインできない ドキュメントを参照し、インスタンスの帯域幅使用状況および障害の処理について確認します。

#### サーバー負荷が高い

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

考えられる原因:ウイルスやトロイの木馬、サードパーティ製のウイルス対策ソフト、アプリケーションプログラムの異常、ドライバーの異常、またはソフトウェアのバックエンドでの自動更新によってCPU占有率が高くなり、CVMにログインできない、またはアクセスが遅いといった問題が発生している。

#### 処理手順:

1. VNCログイン によってインスタンスにログインします。

2. Linuxインスタンス:CPUとメモリ占用率が高いため、ログインできない ドキュメントを参照し、「タスクマ ネージャー」で負荷の高いプロセスを特定します。

#### セキュリティグループルールが不適切

**障害事象**:セルフチェックツールでのチェックの結果、セキュリティグループルールが不適切なためにログイン できないことがわかった。

**処理手順**:セキュリティグループ(ポート)検証ツール によってチェックを行います。

ScreenShot Quick Check

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

Testing Details				>
Protocol	Port	Direction	Policy	Effects
ТСР	3389	Inbound	Open	None
ТСР	22	Inbound	Open	None
ТСР	443	Inbound	Open	None
ТСР	80	Inbound	Open	None
ТСР	21	Inbound	Not opened 🛈	Unable to access FTP
ТСР	20	Inbound	Not opened 🛈	Unable to access FTP
ICMP	0	Inbound	Open	None
ALL	ALL	Outbound	Open	None
		Open all ports	Cancel	

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

# その他ソリューション

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

# LinuxインスタンスをSSHで登録できない

最終更新日:::2021-10-27 17:33:36

#### 説明:

この文章はコミュニティから寄せられたものであり、参考までにご提供します。Tencent Cloud関連製品とは関係 がありません。

ここに記載された関連のファイル操作は、必ず慎重に実行してください。必要に応じて、スナップショット作成 などの方法でデータバックアップを行うことができます。

# 現象の説明

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

# 問題の特定および処理

SSHを使用したLinuxインスタンスへのログインが失敗し、エラー情報が返された場合は、エラー情報を記録し、 次のよくあるエラー情報から当てはまるものを探し、迅速に問題を特定して、手順を参照し解決することができ ます。

SSHログインエラーUser root not allowed because not listed in AllowUsers

#### 問題の原因

この問題は通常、SSHサービスがユーザーログイン制御パラメータをアクティブにし、ログインユーザーを制限 しているために起こります。パラメータの説明は次のとおりです。

AllowUsers: ログインが許可されているユーザーのホワイトリストであり、このパラメータが記述されている ユーザーのみログインできます。

**DenyUsers**: ログインが拒否されているユーザーのブラックリストであり、このパラメータが記述されている ユーザーはすべてログインが拒否されます。

AllowGroups: ログインが許可されているユーザーグループのホワイトリストであり、このパラメータが記述さ れているユーザーグループのみログインできます。

**DenyGroups**: ログインが拒否されているユーザーグループのブラックリストであり、このパラメータが記述されているユーザーグループはすべてログインが拒否されます。

#### 説明:

拒否ポリシーの優先順位は許可ポリシーより上になります。

#### 解決方法

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

# 処理手順

1. VNCを使用してLinuxインスタンスにログインします。

2. 以下のコマンドを実行し、VIMエディタを使用して sshd\_config 設定ファイルに進みます。



vim /etc/ssh/sshd\_config

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



AllowUsers root test DenyUsers test DenyGroups test AllowGroups root

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





systemctl restart sshd.service

Ubuntu





service sshd restart

SSHサービスを再起動すると、SSHを使用してログインできるようになります。詳細については SSHを使用して Linuxインスタンスにログイン をご参照ください。

# 現象の説明

SSHを使用してログインする際に、次のエラー情報が表示されます。





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

### 問題の原因

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

# 解決方法

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

#### 処理手順

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



vim /etc/ssh/sshd\_config

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

4. Escを押して編集モードを終了し、:wqを入力して変更を保存します。

5. 実際に使用するOSに応じて以下のコマンドを実行し、SSHサービスを再起動します。

CentOS



systemctl restart sshd.service

Ubuntu





service sshd restart

SSHサービスを再起動すると、SSHを使用してログインできるようになります。詳細については SSHを使用して Linuxインスタンスにログイン をご参照ください。

 $\mathsf{SSHu}\mathcal{I}\mathcal{I}\mathcal{I}\mathcal{I}\mathcal{I}\mathsf{SSh}_\mathsf{exchange\_identification: read: Connection reset by peer}$ 

# 現象の説明

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

"kex\_exchange\_identification: read: Connection reset by peer"

"kex\_exchange\_identification: Connection closed by remote host"

# 問題の原因

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

# 解決方法

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

### 処理手順

# アクセスポリシー設定の確認と調整

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





in.sshd:ALL # すべてのssh接続を拒否 in.sshd:218.64.87.0/255.255.128 # 218.64.87.0--127のsshを拒否 ALL:ALL # すべてのTCP接続を拒否

VNCを使用してLinuxインスタンスにログインし、 /etc/hosts.deny ファイルおよ び /etc/hosts.allow ファイルを確認し、確認結果に基づいて次の処理方法を選択してください。 設定に誤りがあった場合は必要に応じて変更してください。変更後すぐに有効になります。 未設定、または設定に誤りがなかった場合は、次の手順に進んでください。 説明: アクセスポリシーを設定していない場合、デフォルトのファイルはすべてブランクであり、すべての接続が許可 されています。

# iptablesファイアウォールルールの確認

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



sudo iptables -L --line-number

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

SSH接続が拒否されていなかった場合は、次の手順に進んでください。

# sshd設定の確認と調整

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



vim /etc/ssh/sshd\_config

2. MaxStartups の値を調整する必要があるかどうかを確認します。 sshd\_config 設定ファイル内

の MaxStartups によって許可する最大接続数を設定します。短時間に多くの接続を確立したい場合は、この値 を適宜調整する必要があります。

調整が必要な場合は、以下の手順を参照して変更してください。

2.1.1 i を押して編集モードに入り、変更完了後にEscを押して編集モードを終了し、:wqを入力して変更を保存します。

説明:

MaxStartupsは10:30:100がデフォルト設定であり、SSH保護プロセスの、アイデンティティ認証を経ない同時接続の最大数を指定します。10:30:100とは、10番目の接続以降、接続数が100に達するまで、30%の確率(漸増)で新たな接続を拒否することを表します。

2.1.2 以下のコマンドを実行し、sshdサービスを再起動します。





service sshd restart

調整の必要がない場合は、次の手順に進んでください。

# ネットワーク環境のテスト

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

「はい」の場合は、インスタンスを再起動後にVNCを使用してインスタンスにログインしてください。

「いいえ」の場合は、テスト結果に基づいてネットワーク環境の問題を解決してください。

ここまででSSHログインの問題が解決されていない場合は、システムカーネルに異常が生じているか、またはその他の潜在的な原因による可能性があります。問題の処理を進めるため、チケットを提出してご連絡ください。 SSHログインエラーPermission denied, please try again

#### 現象の説明

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

#### 問題の原因

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

#### 解決方法

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

#### 処理手順

#### SELinuxサービスの確認と無効化

### 1. VNCを使用してLinuxインスタンスにログインします。

2. 以下のコマンドを実行し、現在のSELinuxのサービスステータスを確認します。





/usr/sbin/sestatus -v

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





SELinux status: enabled

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

SELinuxサービスを一時的に無効化

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





setenforce 0

SELinuxサービスを永続的に無効化 以下のコマンドを実行し、SELinuxサービスを無効化します。





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

# ご注意:

このコマンドはSELinuxサービスがenforcing状態の場合にのみ適用されます。 コマンド実行後にシステムまたはインスタンスを再起動し、変更を有効にする必要があります。

# sshd設定の確認と調整

# 1. VNCを使用してLinuxインスタンスにログインします。

2.以下のコマンドを実行し、VIMエディタを使用して sshd\_config 設定ファイルに進みます。





vim /etc/ssh/sshd\_config

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

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

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

4. Escを押して編集モードを終了し、:wqを入力して変更を保存します。



# 5. 以下のコマンドを実行して、SSHサービスを再起動します。



service sshd restart

SSHサービスを再起動すると、SSHを使用してログインできるようになります。詳細については SSHを使用して Linuxインスタンスにログイン をご参照ください。

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

現象の説明



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

### 問題の原因

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

#### 解決方法

1. 処理手順を参照し、SSHで設定した sshd\_config ファイルに進みます。

2. SSHサービスのパスワードリセットポリシーの MaxAuthTries パラメータ設定を確認して変更し、SSHサービスを再起動すれば完了です。

# 処理手順

1. VNCを使用してLinuxインスタンスにログインします。

2.以下のコマンドを実行し、VIMエディタを使用して sshd\_config 設定ファイルに進みます。





vim /etc/ssh/sshd\_config

3. 以下に類似した設定が含まれていないか確認します。





MaxAuthTries 5

説明:

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

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



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



MaxAuthTries <間違ったパスワードの入力を許可する回数>

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





service sshd restart

SSHサービスを再起動すると、SSHを使用してログインできるようになります。詳細については SSHを使用して Linuxインスタンスにログイン をご参照ください。

SSH起動時エラーerror while loading shared libraries

# 現象の説明

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



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

#### 問題の原因

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

### 解決方法

処理手順 を参照して、システムライブラリファイルを確認し、修復を行います。

#### 処理手順

# 説明:

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

# ライブラリファイル情報を取得する

### 1. VNCを使用してLinuxインスタンスにログインします。

2. 以下のコマンドを実行し、libcrypto.so.10ライブラリファイル情報を確認します。





ll /usr/lib64/libcrypto.so.10

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





lrwxrwxrwx 1 root root 19 Jan 19 2021 /usr/lib64/libcrypto.so.10 -> libcrypto.so.1
3.以下のコマンドを実行し、 libcrypto.so.1.0.2k ライブラリファイル情報を確認します。




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

以下に類似した情報が返されます。





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

4. 正常なライブラリファイルのパス、権限、グループなどの情報を記録し、以下の方法で処理を行います。
 ライブラリファイルの検索と置換
 外部ファイルのアップロード
 スナップショットロールバックによるリカバリ

### ライブラリファイルの検索と置換

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





find / -name libcrypto.so.1.0.2k

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





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

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





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





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

4. 以下のコマンドを実行し、ソフトリンクを作成します。





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

5. 以下のコマンドを実行し、SSHサービスを起動します。





service sshd start

### 外部ファイルのアップロード

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

### 説明:

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



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



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

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





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





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

4. 以下のコマンドを実行し、ソフトリンクを作成します。





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

5. 以下のコマンドを実行し、SSHサービスを起動します。





service sshd start

#### スナップショットロールバックによるリカバリ

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

スナップショットロールバックを行うと、スナップショット作成後のデータが失われる場合がありますので、慎 重に操作してください。 SSHサービスが正常に稼働するまで、スナップショット作成時間の近い方から遠い方の順に、一度ずつロール バックを試すことをお勧めします。ロールバックを行ってもSSHサービスが正常に稼働しない場合は、それらの 時点でシステムにすでに異常が生じていたことを意味します。

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

### 現象の説明

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





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

### 問題の原因

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

### 解決方法

1. 処理手順を参照して、SSHで設定した sshd\_config ファイルに進み、設定を確認します。

2. AddressFamily パラメータを変更し、SSHサービスを再起動すれば完了です。

### 処理手順

1. VNCを使用してLinuxインスタンスにログインします。

2.以下のコマンドを実行し、VIMエディタを使用して sshd\_config 設定ファイルに進みます。





vim /etc/ssh/sshd\_config

3. 以下に類似した設定が含まれていないか確認します。





#### AddressFamily inet6

よく用いられるパラメータの説明は次のとおりです。 inet: IPv4プロトコルスイートを使用します。デフォルト値です。 inet6: IPv6プロトコルスイートを使用します。 any: IPv4およびIPv6プロトコルスイートを同時にアクティブにします。 4. iを押して編集モードに入り、次の設定に変更するか、または行の先頭に # を追加してコメントします。





AddressFamily inet

### ご注意:

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

5. Escを押して編集モードを終了し、:wqを入力して変更を保存します。

6. 以下のコマンドを実行し、SSHサービスを再起動します。





service sshd restart

SSHサービスを再起動すると、SSHを使用してログインできるようになります。詳細については SSHを使用して Linuxインスタンスにログイン をご参照ください。

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

### 現象の説明

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





/etc/ssh/sshd\_config: line 2: Bad configuration options:\\\
/etc/ssh/sshd\_config: terminating, 1 bad configuration options

### 問題の説明

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

### 解決方法

処理手順で提示される以下の処理項目を参照し、sshd\_config`設定ファイルを修復します。 エラー情報に対応した設定ファイル変更 外部ファイルのアップロード SSHサービスの再インストール スナップショットロールバックによるリカバリ

### 処理手順

### エラー情報に対応した設定ファイル変更

エラー情報の中でエラーのある設定が明確に示されている場合は、VIMエディタによっ

て /etc/ssh/sshd\_config 設定ファイルを直接変更することができます。他のインスタンスの正しい設定 ファイルを参照し、変更を行うことができます。

### 外部ファイルのアップロード

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

### 説明:

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

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





cp /tmp/sshd\_config /etc/ssh/sshd\_config

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





chmod 600 /etc/ssh/sshd\_config
chown root:root /etc/ssh/sshd\_config

4. 以下のコマンドを実行し、SSHサービスを起動します。





service sshd start

### SSHサービスの再インストール

- 1. VNCを使用してLinuxインスタンスにログイン します。
- 2. 以下のコマンドを実行し、SSHサービスをアンインストールします。





rpm -e openssh-server

3. 以下のコマンドを実行し、SSHサービスをインストールします。





yum install openssh-server

4. 以下のコマンドを実行し、SSHサービスを起動します。





service sshd start

#### スナップショットロールバックによるリカバリ

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

スナップショットロールバックを行うと、スナップショット作成後のデータが失われる場合がありますので、慎 重に操作してください。 SSHサービスが正常に稼働するまで、スナップショット作成時間の近い方から遠い方の順に、一度ずつロール バックを試すことをお勧めします。ロールバックを行ってもSSHサービスが正常に稼働しない場合は、それらの 時点でシステムにすでに異常が生じていたことを意味します。

若您的问题仍未解决,请通过提交工单联系我们寻求帮助。

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

最終更新日:::2022-06-29 15:44:13

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

# 考えられる原因

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

# 特定ツール

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

top - Tasks %Cpu( KiB M	- 22:1 s: 68 (s): Mem :	6:25 up total, 0.0 us, 1016516	6:18 1 r 0.3	8, 1 use running, sy, 0.0	er, lo 67 sl 0 ni, 9 5016 fr	ad avera eeping, 9.7 id,	age (	e: 0.( 0 sto 0.0 wa	00, 0. opped, a, <b>0.</b> sed.	01, 0.05 0 zomb: 0 hi, 0.0 334276 bi	ie ) si, 0, uff/cache
KiB S	Swap:	0	tota	al,	0 fr	ee,		0 us	sed.	778708 av	vail Mem
PII	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
25	7 root	20	0	0	0	0	S	0.3	0.0	0:00.73	jbd2/vda
984	l root	20	0	569592	5068	2568	S	0.3	0.5	0:16.51	YDServio
1253	3 root	20	0	534620	12288	2104	S	0.3	1.2	0:34.21	barad_a
	l root	20	0	43104	3512	2404	S	0.0	0.3	0:01.87	systemd
2	2 root	20	0	0	0	0	S	0.0	0.0	0:00.00	kthread
3	3 root	20	0	0	0	0	S	0.0	0.0	0:00.33	ksoftire
4	l root	20	0	0	0	0	S	0.0	0.0	0:00.00	kworker
Į	5 root	0	-20	0	0	0	S	0.0	0.0	0:00.00	kworker
	7 root	rt	0	0	0	0	S	0.0	0.0	0:00.00	migratio
8	3 root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcu_bh
9	9 root	20	0	0	0	0	S	0.0	0.0	0:01.20	rcu_sche
1(	) root	rt	0	0	0	0	S	0.0	0.0	0:00.05	watchdo

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

1行目:システムの現在時刻、現在のログインユーザー数およびシステムの負荷。

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

3行目:CPUの現在の使用状況。

4行目:メモリの現在の使用状況。

5行目:Swap領域の現在の使用状況。

下半分はプロセスの次元でリソースの占有状況を表しています。

PID:プロセスのID。

USER:プロセスの所有者。

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

VIRT:使用している仮想メモリのサイズ。単位はKB。

RES:現在使用中のメモリのサイズ。単位はKB。

SHR:使用している共有メモリのサイズ。単位はKB。

S:プロセスの状態。

%CPU:更新時間間隔内にプロセスが使用したCPU時間のパーセンテージ。

%MEM:更新時間間隔内にプロセスが使用したメモリのパーセンテージ。

TIME+:プロセスが使用したCPU時間。精度は0.01s。

COMMAND:プロセス名。

## 障害処理

### CVMにログイン

実際のニーズに応じてログイン方式を選択し、CVMにログインします。 サードパーティのソフトウェアによってLinux CVMにリモートログインします。

### ご注意:

Linux CVMがCPU高負荷状態にある場合、ログインできない状態になる可能性があります。 VNCを使用してLinuxインスタンスにログインします。

### ご注意:

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

### プロセスの占有状況の確認

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





top

### プロセスの分析

タスクマネージャー内のプロセスに基づき、分析とトラブルシューティングを行って、それに応じた対処法をとり ます。

業務プロセスが大量のCPUまたはメモリリソースを占有している場合は、業務プログラムがスペースを最適化しているかどうかを分析し、最適化またはサーバー設定のアップグレードを行うことをお勧めします。

異常なプロセスが大量のCPUまたはメモリリソースを占有している場合は、インスタンスがウイルスに感染して いる可能性があります。プロセスを自ら終了するか、またはセキュリティソフトを使用してウイルスの検出と駆除 を行い、必要に応じてデータをバックアップし、システムの再インストールを行うことをご検討ください。 Tencent Cloudのコンポーネントプロセスが大量のCPUまたはメモリリソースを占有している場合は、さらなる問

題特定と処理を行うため、チケットを提出 してご連絡ください。 一般的なTencent Cloudコンポーネントには次のものがあります。 sap00x:セキュリティコンポーネントプロセス Barad\_agent:監視コンポーネントプロセス

secu-tcs-agent: セキュリティコンポーネントプロセス

### プロセスの終了

1. 分析した、リソースを占有しているプロセスの状況に応じて、終了する必要があるプロセスのPIDを記録します。

2. k を入力します。

3. 下図のように、終了する必要があるプロセスのPIDを入力し、Enterを押します。

ここではPIDが23のプロセスの終了を例にとります。

ton - F	9-59-4	15 5		in 1 uc	an 10a	d arman		• a aa		-	a1 a a5
Tasks:	351 to	ntal.	1	supping.	359 slee	a avere ning.	iyc R	stown	ed.		9 zombie
2Cnu(s)	1: 0.0	a ne.	ค้า	SIL <b>0.0</b>	ni. 99.	9 id.	ด้	асорр Аца.	<u>я</u> ,	้ค	Ahi. AAsi. AAst
KiB Men	15	879516	tot	1441	292 free	127	296	8 used			392156 huff/cache
KiB Sua	un: 71	97148	tot	1. 2097	148 free		00	Noca N	,	1	1532932 auail Mem
PID to	signal	1/111	Ide	ault nid	= 2931	23		o asca			ISSISSE avail field
PID	USER	PE	N	UIRT	RES	SHR	S	ZCPIL 1	2MF		M TIME+ COMMAND
293	root	28		а я	8	B	s	8.2	8.	R	8 8:83.24 kworker/2:1
524	root	28		ล้ ด้	ด้	ñ	š	8.1	й.	Ř	8 8:83.53 kuprker/8:2
137	root	28		ล้ ดั	й	й	š	<u>й.1</u>	й.	Ř	A A:A2.70 rcu sched
141	root	28		ล้ ดั	й	й	š	ด.ด	й.	Ñ	8 8:88.73 rcuos/3
15672	root	28		130156	2028	1260	R	0.0	Й.	1	1 8:84.61 ton
1	root	28		3 57592	7436	2612	S	0.0	ø.	4	4 0:03.44 sustemd
310	root	28		а а	я	Я	s	0.0	Й.	Й	A A:AA.64 kworker/u256:1
333	root	28		ลั ดั	й	й	s	<b>8</b> .0	Й.	.N	8 8:88.26 kworker/3:1
540	root	28		ล้ ดั	ด	ĕ	š	0.0	ø.	.0	0 0:00.11 ibd2/sda2-8
619	root	28		43016	2876	2564	s	0.0	ø.	.2	2 0:00.33 sustend-journal
738	root	28		329592	23192	6252	s	<b>8</b> .8	1.	.2	2 0:01.02 firewalld
745	root	28		19284	1236	944	s	0.0	Â.	.1	1 0:00.67 irgbalance
754	dbus	28		34880	1984	1420	š	0.0	ø.	1	1 0:00.27 dbus-daemon
853	root	28	1	3 509040	9620	5956	ŝ	0.0	0.	.5	5 0:00.30 NetworkManager
981	nolkii	td ZP	1	3 514364	12268	4568	s	0.0	Й.	.7	7 0:00.17 polkitd
1816	root	20		91064	2064	1064	š	0.0	Й.	1	1 0:00.09 master
15681	root	20		3 0	0	0	s	0.0	Ø.	.0	8 8:88.86 kworker/1:1
15699	root	28		а а	ñ	ø	S	0.0	0	.0	8 8:00.01 kworker/1:0
2	root	28		3 0	0	0	S	0.0	0.	.0	8 0:00.09 kthreadd

### ご注意:

**Enter**を押した後に kill PID 23 with signal [15]: が表示された場合は、続けて**Enter**を押し、デフォルトの設定を維持します。

4.操作が正常に完了すると、画面に Send pid 23 signal [15/sigterm] というメッセージが表示され

ます。Enterを押して確認すれば完了です。

# その他の関連障害



### CPUがアイドル状態にもかかわらず高負荷な場合の対処

### 問題の説明

Load averageはCPU負荷の評価であり、その値が高いほど、そのタスクキューが長く、実行待ちのタスクが多い ことを表しています。

topによる観察で、下図に類似したものが示された場合は、CPUがアイドル状態にもかかわらず、load averageが 非常に高いことを表します。

top - 19:46:57 u	up 27 days,	5:33, 1 user,	load average:	23, 22, 23	
Tasks: 94 tota	l, 1 runni	ng, 93 sleeping	, 0 stopped,	0 zombie	
%Cpu(s): 0.3 us	s, 0.0 sy,	0.0 ni, 99.7 id	, 0.0 wa, 0.	0 hi, 0.0 si,	0.0 st
KiB Mem: 1016	656 total,	950428 used,	66228 free,	170148 buffers	3
KiB Swap:	0 total,	0 used,	0 free.	452740 cached	Mem

### 処理方法

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





ps -axjf

1	516	516	516 ?	-1 Ss	0	0:00 /sbin/iprinitdaemon
1	569	569	569 ?	-1 Ss	0	0:00 /sbin/iprdumpdaemon
1	863	863	863 ?	-1 D+	38	0:16 /usr/sbin/ntpd -u ntp:ntp -g
1	874	874	874 ?	-1 Ss	0	0:01 /usr/sbin/sshd -D
874	8823	8823	8823 ?	-1 Ss	0	0:03 \_ sahd: root@pts/0
8823	8825	8825	8825 pts/0	9006 Ss	0	0:00 \bash
8825	9006	9006	8825 pts/0	9006 D+	0	0:00 \_ ps -axjf

### 説明:

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

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

### Kswapd0プロセスによるCPU占有が比較的高い場合の対処

### 問題の説明

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

### 処理方法

1. 次のコマンドを実行し、kswapd0プロセスを見つけます。




top

2. kswapd0プロセスの状態を観察します。

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

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

# Linuxインスタンス:ポートの問題によるロ グインができない

最終更新日:::2023-06-08 17:03:09

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

#### 説明:

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

### 検証ツール

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

#### 自己診断

インスタンスポート検証ツール

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

### トラブルシューティング

#### ネットワーク接続の状態を確認する

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

1. ローカルコンピューターでコマンドラインツールを開きます。

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

**Mac OS**: Terminalツールを開きます。

2. 以下のコマンドを実行して、ネットワーク接続をテストします。





ping + CVM インスタンスのパブリックIP アドレス

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

ping 139-199-X00(.)	900
正在 Ping 137.177.X00(.)00X貝有 32 字节 来自137.177.X00(.)00X的回复: 字节=32 日 来自137.177.X00(.)00X的回复: 字节=32 日 来自137.177.X00(.)00X的回复: 字节=32 日 来自137.177.X00(.)00X的回复: 字节=32 日	的数据: 时间=9ns IIL=53 时间=10ns IIL=53 时间=10ns IIL=53 时间=10ns IIL=53
139.199.X00(.002的 Ping 统计信息: 数据包:已发送 = 4,已接收 = 4, 往返行程的估计时间(以毫秒为单位): 最短 = 9ms,最长 = 10ms,平均 =	丢失 = 8 <0% 丢失>, 9ms

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

#### インスタンスポートの接続を確認する

1. VNCを使用してCVMインスタンスにログインします。詳細については、VNCを使用してLinuxインスタンスにロ グイン をご参照ください。

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





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

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



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



#### sshdサービスを確認する

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

# Linuxインスタンス: VNCログインエラー

# Module is unknown

最終更新日:::2023-06-08 17:19:36

## 現象の説明

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

CentOS Linux 7 (Core) Kernel 3.10.0-1062.18.1.el7.x86\_64 on an x86\_64 login: root Account locked due to 10 failed logins

## 考えられる原因

Password:

VNCを使用したログインでは /etc/pam.d/login というpamモジュールを呼び出して検証を行います。一方、 login設定ファイルには pam\_tally2.so モジュールの認証が存在します。 pam\_tally2.so モジュールの機 能は、LinuxユーザーがN回連続して誤ったパスワードを入力してログインを行った場合、自動的にX分間ロック、 または永続的にロックを行うものです。このうち永続的なロックは手動で解除する必要があり、これを行わなけれ ばロックされたままとなります。

ログインの失敗が設定された試行回数を超えた場合、ログインアカウントは一定の時間ロックされるほか、総当 たり攻撃が行われた場合はアカウントがロックされてログインできなくなる可能性もあります。下図は設定されて いるログイン試行可能回数です。

#%PAM-1.0		
auth	required	<pre>pam_tally2.so deny=6 un_lock_time=300 even_d</pre>
auth [user	_unknown=igno	re success=ok ignore=ignore default=bad]
auth	substack	system-auth
auth	include	postlogin
account	required	pam_nologin.so
account	include	system-auth
password	include	system-auth
<pre># pam_seli</pre>	nux.so close s	should be the first session rule
session	required	pam_selinux.so close
session	required	pam_loginuid.so
session	optional	pam_console.so
<pre># pam_seli</pre>	nux.so open sl	nould only be followed by sessions to be exec
session	required	pam_selinux.so open
session	required	pam_namespace.so
session	optional	<pre>pam_keyinit.so force revoke</pre>
session	include	system-auth
session	include	postlogin
-session	optional	pam_ck_connector.so

pam\_tally2 モジュールのパラメータの説明は以下の表のとおりです。

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

## 解決方法

1. 処理手順を参照し、login設定ファイルに入り、 pam\_limits.so モジュール設定に一時的なコメントを付加 します。 2. アカウントがロックされた原因を確認し、セキュリティポリシーを強化します。

## 処理手順

1. SSHを使用したCVMインスタンスへのログインを試してください。詳細については SSHを使用してLinuxイン スタンスにログイン をご参照ください。

ログインに成功した場合は次の手順に進みます。

ログインに失敗した場合は、単一ユーザーモードを使用する必要があります。

2. ログイン成功後、次のコマンドを実行してログ情報を確認します。





vim /var/log/secure

このファイルは一般的にセキュリティに関する情報の記録に用いられ、このうち大部分の記録はユーザーのCVM ログインの関連ログです。下図のように、情報の中から pam\_tally2 のあるエラーメッセージを取得すること ができます。

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

3.順に次のコマンドを実行し、 /etc/pam.d に入り、ログの中のpamモジュールエラーのキーワード pam\_tally2 を検索します。





find . | xargs grep -ri "pam\_tally2" -l

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

bash-4.2#	find	ł	xargs	grep	$-\mathbf{ri}$	"pam_tally2"	-]
.∕login							
.∕login							
bash-4.2#	_						

4. 次のコマンドを実行し、 pam\_tally2.so モジュール設定に一時的なコメントを付加します。設定を完了す ると、ログインできるようになります。



sed -i "s/.\*pam\_tally.\*/#&/" /etc/pam.d/login

5. アカウントのロックが人為的な誤操作によるものか、総当たり攻撃によるものかを確認します。総当たり攻撃 によって起こった場合は、次の方法でセキュリティポリシーを強化することを推奨します。

CVMのパスワードを変更し、大文字、小文字、特殊記号、数字を組み合わせた12~16桁の複雑なランダムパス ワードを設定します。詳細については、インスタンスのパスワードをリセットをご参照ください。

CVM内の使われていないユーザーを削除します。

sshdのデフォルトの22ポートを1024~65525の間の他の非常用ポートに変更します。詳細については、CVMリ モートデフォルトポートの変更 をご参照ください。

CVMのセキュリティグループに関連付けられているルールを管理し、業務およびプロトコルに必要なポートのみ をオープンにし、すべてのプロトコルおよびポートをオープンにはしないことを推奨します。詳細については、セ キュリティグループルールの追加 をご参照ください。

mysql、redisなどのパブリックネットワークにコアアプリケーションサービスポートへのアクセスを開放すること は推奨しません。 関連するポートをローカルアクセスに変更、または外部ネットワークアクセス禁止にすること ができます。

「雲鏡」、「雲鎖」などの保護ソフトウェアをインストールし、リアルタイムアラームを追加して、異常なログ イン情報を速やかに取得できるようにします。

# Linuxインスタンス:VNCログインエラー

# Account locked due to XXX failed logins

最終更新日:::2023-06-08 17:22:38

## 現象の説明

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

CentOS Linux 7 (Core) Kernel 3.10.0-1062.18.1.el7.x86\_64 on an x86\_64 login: root Account locked due to 10 failed logins

## 考えられる原因

Password:

VNCを使用したログインでは /etc/pam.d/login というpamモジュールを呼び出して検証を行います。一方、 login設定ファイルには pam\_tally2.so モジュールの認証が存在します。 pam\_tally2.so モジュールの機 能は、LinuxユーザーがN回連続して誤ったパスワードを入力してログインを行った場合、自動的にX分間ロック、 または永続的にロックを行うものです。このうち永続的なロックは手動で解除する必要があり、これを行わなけれ ばロックされたままとなります。

ログインの失敗が設定された試行回数を超えた場合、ログインアカウントは一定の時間ロックされるほか、総当 たり攻撃が行われた場合はアカウントがロックされてログインできなくなる可能性もあります。下図は設定されて いるログイン試行可能回数です。

#%PAM-1.0		
auth	required	<pre>pam_tally2.so deny=6 un_lock_time=300 even_d</pre>
auth [user	_unknown=igno	re success=ok ignore=ignore default=bad] pam
auth	substack	system-auth
auth	include	postlogin
account	required	pam_nologin.so
account	include	system-auth
password	include	system-auth
<pre># pam_seli</pre>	nux.so close s	should be the first session rule
session	required	pam_selinux.so close
session	required	pam_loginuid.so
session	optional	pam_console.so
<pre># pam_seli</pre>	nux.so open sl	nould only be followed by sessions to be exec
session	required	pam_selinux.so open
session	required	pam_namespace.so
session	optional	pam_keyinit.so force revoke
session	include	system-auth
session	include	postlogin
-session	optional	pam_ck_connector.so

pam\_tally2 モジュールのパラメータの説明は以下の表のとおりです。

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

## 解決方法

1. 処理手順を参照し、login設定ファイルに入り、 pam\_limits.so モジュール設定に一時的なコメントを付加 します。 2. アカウントがロックされた原因を確認し、セキュリティポリシーを強化します。

## 処理手順

1. SSHを使用したCVMインスタンスへのログインを試してください。詳細については SSHを使用してLinuxイン スタンスにログイン をご参照ください。

ログインに成功した場合は次の手順に進みます。

ログインに失敗した場合は、単一ユーザーモードを使用する必要があります。

2. ログイン成功後、次のコマンドを実行してログ情報を確認します。





vim /var/log/secure

このファイルは一般的にセキュリティに関する情報の記録に用いられ、このうち大部分の記録はユーザーのCVM ログインの関連ログです。下図のように、情報の中から pam\_tally2 のあるエラーメッセージを取得すること ができます。

Oct 28 17:14:45 UM-96-4-centos	sshd[16704]: Failed password for invalid user dell from 202.153.3
Oct 28 17:14:45 VM-96-4-centos	sshd[16704]: Received disconnect from 202.153.37.205 port 13069:11
Oct 28 17:14:45 VM-96-4-centos	sshd[16704]: Disconnected from 202.153.37.205 port 13069 [preauth]
Oct 28 17:14:59 UM-96-4-centos	login: pam_tally2(login:auth): user root (0) tally 12, deny 2
Oct 28 17:14:59 UM-96-4-centos	login: pam_succeed_if(login:auth): requirement "uid >= 1000" not r
Oct 28 17:15:01 VM-96-4-centos	login: FAILED LOGIN 2 FROM tty1 FOR root, Authentication failure
Oct 28 17:15:01 VM-96-4-centos	login: pam_tally2(login:auth): unknown option: un_lock_time=300
Oct 28 17:15:03 VM-96-4-centos	login: pam_tally2(login:auth): user root (0) tally 13, deny 2
Oct 28 17:15:04 VM-96-4-centos	sshd[16730]; pam_unix(ssna;autn); authentication failure; logname
ost=203.213.66.170 user=root	

3.順に次のコマンドを実行し、 /etc/pam.d に入り、ログの中のpamモジュールエラーのキーワード pam\_tally2 を検索します。





#### cd /etc/pam.d



find . | xargs grep -ri "pam\_tally2" -l

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

bash-4.2#	f ind		xargs	grep	-ri	"pam_tally2"	-]
.∕login							
.∕login							
bash-4.2#	_						

**4**. 次のコマンドを実行し、 pam\_tally2.so モジュール設定に一時的なコメントを付加します。設定を完了すると、ログインできるようになります。





5. アカウントのロックが人為的な誤操作によるものか、総当たり攻撃によるものかを確認します。総当たり攻撃 によって起こった場合は、次の方法でセキュリティポリシーを強化することを推奨します。

CVMのパスワードを変更し、大文字、小文字、特殊記号、数字を組み合わせた12~16桁の複雑なランダムパス ワードを設定します。詳細については、インスタンスのパスワードをリセットをご参照ください。

CVM内の使われていないユーザーを削除します。

sshdのデフォルトの22ポートを1024~65525の間の他の非常用ポートに変更します。詳細については、CVMリ モートデフォルトポートの変更 をご参照ください。

CVMのセキュリティグループに関連付けられているルールを管理し、業務およびプロトコルに必要なポートのみ をオープンにし、すべてのプロトコルおよびポートをオープンにはしないことを推奨します。詳細については、セ キュリティグループルールの追加 をご参照ください。

mysql、redisなどのパブリックネットワークにコアアプリケーションサービスポートへのアクセスを開放すること は推奨しません。 関連するポートをローカルアクセスに変更、または外部ネットワークアクセス禁止にすること ができます。

「雲鏡」などの保護ソフトウェアをインストールし、リアルタイムアラームを追加して、異常なログイン情報を 速やかに取得できるようにします。

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

最終更新日:::2023-06-08 17:27:24

### 現象の説明

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



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



## 考えられる原因

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

bash-4.2# 1	1 –h						
bash: ll: c	ommand not	found					
bash-4.2# 1	s -alh						
total 9.8G							
drwxr-xr-x	10 root	root	4.0K	Oct	28	17:53	
drwxr-xr-x	19 root	root	4.0K	Apr	22	2020	
drwxr-xr-x	2 root	root	4.0K	Mar	7	2019	anaconda
drwx	2 root	root	4.0K	Aug	8	2019	audit
-rw	1 root	root	24K	Oct	28	17:30	boot.log
-rw	1 root	root	1	Oct	28	15:43	boot.log-20191106
-rw	1 root	root	1	Oct	28	15:43	boot.log-20200807
-rw	1 root	utmp	9.8G	Oct	28	17:41	btmp
-rw	1 root	utmp	1	Uct	28	15:43	btmp-20200807
drwxr-xr-x	2 chrony	chrony	4.0K	Aug	8	2019	chrony
-rw-rr	1 syslog	adm	181K	Oct	28	17:30	cloud-init.log
-rw-rr	1 root	root	7.8K	0ct	28	17:30	cloud-init-output.log
-rw	1 root	root	14K	0ct	28	17:42	cron
-rw-rr	1 root	root	36K	Oct	28	17:30	dmesg
-rw-rr	1 root	root	36K	Oct	28	16:26	dmesg.old

## 解決方法

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

## 処理手順

1. SSHを使用したCVMインスタンスへのログインを試してください。詳細については SSHを使用してLinuxイン スタンスにログイン をご参照ください。

ログインに成功した場合は次の手順に進みます。

ログインに失敗した場合は、単一ユーザーモードを使用する必要があります。

2. /var/log に入り、ログファイル /var/log/btmp の容量を確認します。

3. ログファイル /var/log/btmp の容量が大きすぎる場合は、次のコマンドを実行し、btmpログの内容をクリ アします。ログファイルをクリアすると、ログインできるようになります。





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

4. アカウントのロックが人為的な誤操作によるものか、総当たり攻撃によるものかを確認します。総当たり攻撃 によって起こった場合は、次の方法でセキュリティポリシーを強化することを推奨します。

CVMのパスワードを変更し、大文字、小文字、特殊記号、数字を組み合わせた12~16桁の複雑なランダムパス ワードを設定します。詳細については、インスタンスのパスワードをリセット をご参照ください。

CVM内の使われていないユーザーを削除します。

sshdのデフォルトの22ポートを1024~65525の間の他の非常用ポートに変更します。詳細については、CVMリ モートデフォルトポートの変更 をご参照ください。 CVMのセキュリティグループに関連付けられているルールを管理し、業務およびプロトコルに必要なポートのみ をオープンにし、すべてのプロトコルおよびポートをオープンにはしないことを推奨します。詳細については、セ キュリティグループルールの追加をご参照ください。

mysql、redisなどのパブリックネットワークにコアアプリケーションサービスポートへのアクセスを開放すること は推奨しません。 関連するポートをローカルアクセスに変更、または外部ネットワークアクセス禁止にすること ができます。

「雲鏡」、「雲鎖」などの保護ソフトウェアをインストールし、リアルタイムアラームを追加して、異常なログ イン情報を速やかに取得できるようにします。

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

最終更新日:::2023-06-08 17:34:41

## 現象の説明

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



SSHログインエラーは下図のように表示されます。



## 考えられる原因

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

#%PAM-1.0		
<pre># This fil</pre>	le is auto-gene	rated.
# User cha	anges will be d	estroyed the next time authconfig is run.
auth	required	pam_env.so
auth	sufficient	pam_unix.so nullok try_first_pass
auth	requisite	pam_succeed_if.so uid >= 500 quiet
auth	required	pam_deny.so
account	required	pam_unix.so
account	sufficient	pam_localuser.so
account	sufficient	<pre>pam_succeed_if.so uid &lt; 500 quiet</pre>
account	required	pam_permit.so
password	requisite	<pre>pam cracklib.so try first pass retry=3 ty</pre>
password	sufficient	pam unix.so sha512 shadow nullok try firs
password	required	pam_deny.so
session	optional	pam_keyinit.so revoke
session	required	pam_limits.so
session	[success=1 d	<pre>efault=ignore] pam_succeed_if.so service in</pre>
session	required	pam unix.so
_limits.so Ŧ	シュールの王な機能は	ユーザーのセッションの過桯で各種システムリソースの使用状況を

制限することです。デフォルトではこのモジュールの設定ファイルは /etc/security/limits.conf であ り、この設定ファイルはユーザーが使用可能な最大ファイル数、最大スレッド数、最大メモリなどのリソース使 用量を規定しています。パラメータの説明は下表のとおりです。

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

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

## 解決方法

<u>処理手順</u>を参照し、 soft nofile 、 hard nofile および fs.nr\_open を正しい設定に修正します。

## 処理手順

1. SSHを使用したCVMインスタンスへのログインを試してください。詳細については SSHを使用してLinuxイン スタンスにログイン をご参照ください。

ログインに成功した場合は次の手順に進みます。

ログインに失敗した場合は、単一ユーザーモードを使用する必要があります。

2.パラメータ soft nofile 、 hard nofile および fs.nr\_open の値が soft nofile ≤ hard nofile ≤ fs.nr\_open の関係を満たしているかどうかを確認します。

次のコマンドを実行し、 soft nofile および hard nofile の値を確認します。





/etc/security/limits.conf

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





#### 次のコマンドを実行し、 fs.nr\_open の値を確認します。



sysctl -a 2>/dev/null | grep -Ei "file-max|nr\_open"

ここでの取得結果は1048576です。下図のように表示されます。

[root@VM-96-14-centos ~]# sysctl -a 2>/dev/null | grep -Ei "file-max|nr\_open" fs.<mark>file-max =</mark> 183840 fs.nr\_open = 1048576

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

root soft nofile :100001

root hard nofile :100002

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

説明:

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

fs.file-max = 2000000

fs.nr\_open = 2000000

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





sysctl -p

# Linuxインスタンス:/etc/fstabの設定エラー によるログイン不能

最終更新日:::2023-06-08 17:54:51

### 現象の説明

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

Γ	OK	]	Reached target Remote File Systems (Pre).
Γ	OK	]	Reached target Remote File Systems.
			Starting Crash recovery kernel arming
Γ	OK	]	Started Security Auditing Service.
			Starting Update UTMP about System Boot/Shutdown
Γ	OK	]	Started Update UTMP about System Boot/Shutdown.
			Starting Update UTMP about System Runlevel Changes
Γ	OK	]	Started Update UTMP about System Runlevel Changes.
Welcome to emergency mode! After logging in, type "journalctl -xb" to vie			
system logs, "systemctl reboot" to reboot, "systemctl default" or ^D to			
try again to boot into default mode.			
Give root password for maintenance			
(or press Control-D to continue):			

## 考えられる原因

/etc/fstab の設定が不適切であることが原因という可能性があります。

例えば、 /etc/fstab においてディスクがデバイス名で自動的にマウントされるように設定されている場合 も、CVMを再起動するとデバイス名が変わってしまい、システムが正常に起動しなくなることがあります。

## 解決方法

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

### 処理手順

©2013-2022 Tencent Cloud. All rights reserved.

インスタンスにアクセスし、この問題を処理する方法は2つあります。

方法1:VNCを使用したログイン(推奨)

方法2:レスキューモードの使用

1. VNCを使用してLinuxインスタンスにログインします。

2. VNCインターフェースに進み、現象の説明 のようなインターフェースが表示されたら、rootアカウントのパス ワードを入力し、Enterを押してサーバーにログインしてください。

入力されたパスワードは、デフォルトでは表示されません。

アカウントのパスワードをお持ちでない場合、または忘れてしまった場合は、方法2を参照して処理してください。

3.以下のコマンドを実行し、 /etc/fstab ファイルのバックアップを取ります。ここでは、 /home ディレクトリへのバックアップを例に取ります。





cp /etc/fstab /home

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




vi /etc/fstab

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

### 説明:

設定エラーを特定できない場合は、システムディスク以外のマウントされているすべてのディスクの設定につい てコメントアウトし、サーバーが正常な状態に戻った後に ステップ8 を参照して設定することをお勧めします。 # /etc/fstab # Created by anaconda on Tue Nov 26 02:11:36 2019 # # Accessible filesystems, by reference, are maintained under '/dev/disk/'. # See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info. # # After editing this file, run 'systemctl daemon-reload' to update systemd # units generated from this file. # UUID=659e6f89-71fa-463d-842e-ccdf2c06e0fe / ext4 defaults #/dev/vdc1\_/data auto rw,relatime,data=ordered 0 2

6. Escを押して:wq と入力した後、Enterを押して設定を保存し、エディタを終了します。

7. コンソールからインスタンスを再起動し、正常に起動、ログインできるかどうかを検証します。

説明:

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

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

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

ご注意:

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

2. 方法1の ステップ3 - ステップ6 に従って、 /etc/fstab ファイルの修復を行います。

3. レスキューモードの終了を参照し、インスタンスのレスキューモードを終了します。

4. インスタンスがレスキューモードを終了すると、シャットダウン状態になります。インスタンスの起動を参照 してシステムを起動し、起動後に正常にログインできることを確認してください。

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

# Linuxインスタンス:sshd設定ファイル権限 に関する問題

最終更新日:::2023-06-08 17:38:23

### ##故障について

SSHを使用してLinuxインスタンスにログインすると、「ssh\_exchange\_identification: Connection closed by remote host」または「no hostkey alg」が出現する。

# 考えられる原因

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

## ソリューション

実際のエラー情報に応じて対応する手順を選択し、設定ファイルの権限を修正します。

エラー情報が「ssh\_exchange\_identification: Connection closed by remote host」である場合は、/var/empty/sshd ファイル権限の修正 手順をご参照ください。

エラー情報が「no hostkey alg」である場合は、/etc/ssh/ssh\_host\_rsa\_key ファイル権限の修正 手順をご参照くだ さい。

# 処理手順

### /var/empty/sshd ファイル権限の修正

1. VNCを使用してLinuxインスタンスにログイン。

2. 次のコマンドを実行し、エラーの原因を確認します。





sshd -t

次のような情報が返されます:





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

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





chmod 711 /var/empty/sshd/

### /etc/ssh/ssh\_host\_rsa\_key ファイル権限の修正

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





sshd -t

返される情報には次のようなフィールドが含まれます。





"/etc/ssh/ssh\_host\_rsa\_key are too open"

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





chmod 600 /etc/ssh/ssh\_host\_rsa\_key

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

最終更新日:::2023-06-08 17:41:26

##故障について

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

# 考えられる原因

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

## ソリューション

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

# 処理手順

1. VNCを使用してLinuxインスタンスにログイン。

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





#### vim /etc/profile

3. /etc/profile ファイル内に /etc/profile 関連コマンドが含まれるかどうかをチェックします。 含まれる場合は、次の手順に進んでください。

含まれない場合は、チケットを提出して連絡し、サポートを受けてください。

4.iで編集モードに入り、 /etc/profile 関連コマンドの前に # を追加してそのコマンドにコメントします。

5. Escを押して編集モードを終了し、:wqを入力して変更を保存します。

6. 再度 SSHを使用してLinuxインスタンスにログイン でログインします。

# サーバーが隔離されたためログインできない

最終更新日:::2022-04-07 16:31:02

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

## 故障について

CVMは現在の法律や規制に違反しているため、分離されている可能性があります。以下の方法を使用して、CVM が分離されているかどうかを確認できます。

CVMがパブリックネットワークから分離されると、サイト内メール またはSMSを介して分離されていることを通知します。

「CVMコンソール」(https://console.tencentcloud.com/cvm/index)の中の「監視/ステータス」バーに、CVMのス テータスが分離されていることが示されます。

## 問題の原因

CVMには規制違反またはリスクイベントが発生すると、ルールに違反したマシンを部分的に分離されます(プラ イベートネットワークのログインポート22、36000、3389を除き、他のネットワークアクセスは全て分離されま す。開発者はジャンプサーバーを使用してサーバーにログインできます)。

詳細については、[クラウドセキュリティ違反レベルの分類とペナルティの説明]をご参照ください。

### ソリューション

1. サイト内メール或はSMSの指示に従って、違反しているコンテンツを削除します。セキュリティリスクを対処 し、必要に応じてシステムを再インストールします。

2. 個人の行動による違反ではない場合は、サーバーは悪意のある侵入があった可能性があります。 これを解決す るには、ホストセキュリティをご参照ください。

3. セキュリティリスクを排除し、違反しているコンテンツを削除した後、チケットを送信して、カスタマサービスに連絡して分離を解除させます。

# 帯域幅の利用率が高いためログインできない

最終更新日:::2024-01-05 14:21:54

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

## 障害の現象

Tencent Cloud CVMコンソール にログインして、CVMの帯域幅監視データには、帯域幅の使用率が高すぎてCVM に接続できないことを示していることがわかります。

セルフ診断ツールで帯域幅の使用量が高すぎると診断されました。

# トラブルシューティング

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

1. CVMで、

クリックし、**タスクマネージャー**を選択して、「タスクマネージャー」を開きます。

2. 性能タブを選択し、リソースモニターを開くをクリックします。

3. 開いた「リソースモニター」で、どのプロセスがより多くの帯域幅を消費しているかを確認します。実際の業務に基づいて、プロセスが正常に動作しているかを判断します。

帯域幅を大量に消費するプロセスが業務プロセスである場合、アクセス量の変化によるか、および容量を最適化 する必要があるか、或は CVM設定をアップグレード する必要があるかどうかを確認します。

帯域幅を大量に消費するプロセスが異常なプロセスである場合は、ウイルス或はトロイの木馬が原因である可能 性があります。プロセスを自分で終了する或はセキュリティソフトウェアを使用してウイルスを駆除できます。 データのバックアップ後にシステムを再インストールすることもできます。

#### ご注意:

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

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

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

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

### 説明:

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

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





yum install iftop -y

説明:

Ubuntuシステムの場合、 apt-get install iftop -y コマンドを実行してください。 2.以下のコマンドを実行し、lsofをインストールします。





yum install lsof -y

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





iftop

		12.5K	b		25	. ӨКЪ	37.5Kb	5	50.0KЪ
UM_2_14_centos UM_2_14_centos UM_2_14_centos UM_2_14_centos UM_2_14_centos UM_2_14_centos UM_2_14_centos UM_2_14_centos UM_2_14_centos UM_2_14_centos UM_2_14_centos					<pre> &lt;&lt; =     &lt; =         &lt; =         &lt; =</pre>				112b 112b Øb Øb Øb Øb Øb
TX: RX: TOTAL:	cum:	69.4KB 42.1KB 111KB	peak:	6.82Kb 4.45Kb 11.3Kb				rates:	224b 224b 448b

<= 、 => はトラフィックの方向を示します

TX は送信トラフィックを示します

RX は受信トラフィックを示します

TOTALは総トラフィックを示します

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

peak はトラフィックのピークを示します

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

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





lsof -i | grep IP

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





lsof -i | grep 201.205.141.123

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





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

5. 帯域幅を消費するプロセスを確認して、プロセスが正常に動作しているかを判断します。 帯域幅を大量に消費するプロセスが業務プロセスである場合、アクセス量の変化によるか、および容量を最適化 する必要があるか、或は CVM設定をアップグレード する必要があるかどうかを確認します。

帯域幅を大量に消費するプロセスが異常なプロセスである場合は、ウイルス或はトロイの木馬が原因である可能 性があります。プロセスを自分で終了する或はセキュリティソフトウェアを使用してウイルスを駆除できます。 データのバックアップ後にシステムを再インストールすることもできます。 帯域幅を大量に消費するプロセスがTencent Cloudコンポーネントプロセスである場合は、チケットを送信してお 問い合わせください。問題に対処し、解決策を特定できるよう支援します。

対象側IPアドレスの所在地を重点的にチェックすることをお勧めします。IP138検索サイトでIPアドレス所在地を 検索できます。対象側IPのアドレスの所在地が海外である場合は、リスクが高く、重点的に注意してください。

# セキュリティグループの設定が原因でリモー ト接続できない

最終更新日:::2022-05-26 18:50:48

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

### 検証ツール

Tencent Cloudが提供する セキュリティグループ(ポート)検証ツール を使用して、リモート接続できないことが セキュリティグループの設定に関連しているかどうかを判断できます。

1. セキュリティグループ (ポート)検証ツール にログインします。

2. Port Verification画面で、検出対象のインスタンスを選択し、Quick Checkをクリックします。 下記画像に示すように:

ID/实例名	连通性诊断
未命名	一键检测

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

佥测详情					×
协议	端口	方向	策略	影响	
TCP	3389	入站	放通	无	
TCP	22	入站	放通	无	
TCP	443	入站	放通	无	
TCP	80	入站	放通	无	
ТСР	21	入站	未放通()	无法使用ftp	
ТСР	20	入站	未放通	无法使用ftp	
ICMP	0	入站	放通	无	
ALL	ALL	出站	放通	无	
		一键放通	取消		

# セキュリティグループの設定を変更する

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

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

最終更新日:::2022-07-21 18:01:18

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

## トラブルシューティングツール

VNCログインは、Webブラウザを使ってCVMにリモート接続する方法であり、通常は、正常なSSHリモートログ インができない場合に使用します。VNCログイン方式を使用すると、CVMのステータスの直接観察やシステム内 の設定ファイルの変更といった操作が可能です。

レスキューモードは、通常、Linuxシステムが正常に起動しない場合やVNCでログインできない場合に使用しま す。一般的なユースケースとしては、fstab設定の異常、重要なシステムファイルの欠落、lib動的ライブラリファ イルの破損/欠落などがあります。

## 問題の特定および処理

VNC方式によるSSHログインのトラブルシューティング方法

#### 現象の説明

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



#### 考えられる原因

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



### 解決方法

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

### 処理手順

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

1.下

図に示すよ

うに、CVMコンソール にログインし、ログインしたいLinux CVMを見つけて、右側の**ログイン**をクリックしま す。

Instances Shang	ghai 2 Other regions(42) 🔻							
Create Start Up	Shutdown Resta	rt Reset Passv	vord Terminate/Return	More Actions *	Q. View instances pendir	ng repossession		
D/Name	Monitoring	Status T	Availability Zone 🔻	Instance Type <b>Y</b>	Instance Configuration	Primary IPv4 🛈	Primary IPv6	Instance Billing Mode 🔻
as-test1	di.	Aunning	Shanghai Zone 4	GPU Compute GN6S	4-core 20GB 1Mbps System disk: Premium Cloud Storage			Pay-as-you-go Created at 2021-01-08 19:00:29
as-test2 🖋	.h	Running	Shanghai Zone 4	GPU Compute GN6S	4-core 20GB 1Mbps System disk: Premium Cloud Storane	-	-	Pay-as-you-go Created at 2021-01-08 19:00:28
Total items: 2								

2. 開いた「標準ログイン | Linuxインスタンス」ウィンドウで、VNCログインをクリックします。

3. 「login」の後にユーザー名を入力し、Enterを押します。「Password」の後にパスワードを入力し、Enterを押 します。下図のようになれば、ログインに成功しています。



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





ps -ef | grep sshd

下図のような結果が返されれば、sshdプロセスは正常です。

[root0UM-0-11-centos ~]# us -ef   grep sshd
root 1173 1 0 22:08 ? 00:00:00 /usr/sbin/sshd -D -oCiphers=aes256-gcm@oper
.com, aes256-ctr, aes256-cbc, aes128-gcm@openssh.com, aes128-ctr, aes128-cbc -oMACs=hmac-sha2-256-et
sh.com,umac-128-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha1,umac-128
IKexAlgorithms=gss-curve25519-sha256-,gss-nistp256-sha256-,gss-group14-sha256-,gss-group16-sha
1oKexAlgorithms=curve25519-sha256,curve25519-sha2560libssh.org,ecdh-sha2-nistp256,ecdh-sha2
e-hellman-group-exchange-sha256, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, dif
-hellman-group-exchange-sha1, diffie-hellman-group14-sha1 -oHostKeyAlgorithms=ecdsa-sha2-nistp2
enssh.com,ecdsa-sha2-nistp384,ecdsa-sha2-nistp384-cert-v01Qopenssh.com,ecdsa-sha2-nistp521,ecds
com,ssh-ed25519,ssh-ed25519-cert-v01@openssh.com,rsa-sha2-256,rsa-sha2-256-cert-v01@openssh.com
010openssh.com,ssh-rsa,ssh-rsa-cert-v010openssh.com -oPubkeyAcceptedKeyTypes=ecdsa-sha2-nistp2
enssh.com,ecdsa-sha2-nistp384,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521,ecds
com,ssh-ed25519,ssh-ed25519-cert-v01@openssh.com,rsa-sha2-256,rsa-sha2-256-cert-v01@openssh.com
010openssh.com,ssh-rsa,ssh-rsa-cert-v010openssh.com -oCASignatureAlgorithms=ecdsa-sha2-nistp256
istp521,ssh-ed25519,rsa-sha2-256,rsa-sha2-512,ssh-rsa
root 2473 1722 0 22:13 ttu1 00:00 grepcolor=auto sshd

5. 次のコマンドを実行し、エラーの原因を確認します。





sshd -t

下図のような情報、"/var/empty/sshd must be owned by root and not group or world-writable.

"が返された場合、エラーの原因は、 /var/empty/sshd/ の権限の問題である可能性があります。



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

systemd[1]: Started Session 174 of user root. systemd[1]: session-174.scope: Succeeded. systemd[1]: Started Session 175 of user root. systemd[1]: session-175.scope: Succeeded. systemd[1]: Started Session 176 of user root. systemd[1]: session-176.scope: Succeeded. systemd[1]: session-176.scope: Succeeded. systemd[1]: fatal: /var/empty/sshd must be owned by root

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





ll -d /var/empty/sshd/

下図のような結果が返されます。権限が777に変更されたことがわかります。

[root@ = ~]# 11 -d /var/empty/sshd/ drwxrwxrwx. 2 root root 4096 Jul 13 2021 <mark>/var/empty/sshd/</mark>

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





chmod 711 /var/empty/sshd/

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

VNC方式によるLinuxシステムの起動失敗のトラブルシューティング

### 現象の説明

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

OK ] Reached target Remote File Systems (Pre). 1 Reached target Remote File Systems. OK Starting Crash recovery kernel arming... 1 Started Security Auditing Service. Ľ OK Starting Update UTMP about System Boot/Shutdown... Γ 1 Started Update UTMP about System Boot/Shutdown. OK Starting Update UTMP about System Runlevel Changes... 1 Started Update UTMP about System Runlevel Changes. E OK Welcome to emergency mode! After logging in, type "journalctl -xb" system logs, "systemetl reboot" to reboot, "systemetl default" or ^D try again to boot into default mode. Give root password for maintenance (or press Control-D to continue):

### 考えられる原因

/etc/fstab の設定が不適切であることが原因という可能性があります。

例えば、 /etc/fstab においてディスクがデバイス名で自動的にマウントされるように設定されている場合 も、CVMを再起動するとデバイス名が変わってしまい、システムが正常に起動しなくなることがあります。

### 解決方法

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

#### 処理手順

1. 処理手順1 を参照し、VNCを使用してLinuxインスタンスにログインします。

 下図に示すように、VNCインターフェースに進み、現象の説明のようなインターフェースが表示されたら、 rootアカウントのパスワードを入力し、Enterを押してサーバーにログインしてください。入力されたパスワード は、デフォルトでは表示されません。

Give root password for maintenance (or press Control-D to continue): [root0 ~]#

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





lsblk

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

[root@ ~]# lsblk NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT 1 184.1M sr0 11:0 0 rom 253:0 0 vda 50G 0 disk Luda1 253:1 0 50G 0 part / [root0 ~]# cat /etc/fstab # # /etc/fstab # Created by anaconda on Tue Nov 26 02:11:36 2019 # # Accessible filesystems, by reference, are maintained under '/dev/disk/'. # See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info. # # After editing this file, run 'systemctl daemon-reload' to update systemd # units generated from this file. # UUID=659e6f89-71fa-463d-842e-ccdf2c06e0fe / ext4 default /dev/vdb1 ∕data ext3 defaults 0 Й ~]# [root@

4. 以下のコマンドを実行し、fstabファイルのバックアップを取ります。





cp /etc/fstab /home

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




vi /etc/fstab

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

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

7. Escを押して:wqと入力した後、Enterを押して設定を保存し、エディタを終了します。

8. コンソールからインスタンスを再起動します。詳細については、インスタンスの再起動 をご参照ください。

9. 正常に起動、ログインできるかどうかを検証します。

レスキューモードによるLinuxシステムの起動失敗のトラブルシューティング

#### 現象の説明

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

1 Reached target Local File Systems (Pre). OK ] Reached target Local File Systems. Starting Restore /run/initramfs on shutdown... Starting Tell Plymouth To Write Out Runtime Data... Starting Create Volatile Files and Directories... [FAILED] Failed to start Restore /run/initramfs on shutdown. See 'systemctl status dracut-shutdown.service' for details. [ OK ] Started Tell Plymouth To Write Out Runtime Data. [FAILED] Failed to start Create Volatile Files and Directories. See 'systemctl status systemd-tmpfiles-setup.service' for details. Starting Security Auditing Service... [FAILED] Failed to start Security Auditing Service. See 'systemctl status auditd.service' for details. Starting Update UTMP about System Boot/Shutdown... [FAILED] Failed to start Update UTMP about System Boot/Shutdown. See 'systemctl status systemd-update-utmp.service' for details. [DEPEND] Dependency failed for Update UTMP about System Runlevel Changes. OK ] Reached target System Initialization. 1 Listening on D-Bus System Message Bus Socket. Γ OK Ε OK ] Listening on Open-iSCSI iscsid Socket. ] Started daily update of the root trust anchor for DNSSEC. E Γ OK ] Started Daily Cleanup of Temporary Directories. ] Started dnf makecache --timer. Г ] Reached target Timers. OK E E ] Listening on ACPID Listen Socket. 1 Listening on SSSD Kerberos Cache Manager responder socket. Ľ Γ OK ] Listening on Open-iSCSI iscsiuio Socket. Γ 1 Reached target Sockets. ] Reached target Basic System. E OK Starting Authorization Manager... ] Started libstoragemgmt plug-in server daemon. OK Γ Γ OK 1 Started Machine Check Exception Logging Daemon. Starting System Security Services Daemon... 1 Started ACPI Event Daemon. E OK Starting Hardware RNG Entropy Gatherer Wake threshold service... [FAILED] Failed to start NTP client/server. See 'systemctl status chronyd.service' for details. Starting VDO volume services... [ OK ] Started D-Bus System Message Bus. Starting Network Manager... [ OK ] Reached target sshd-keygen.target. [FAILED] Failed to start Hardware RNG Entropy Gatherer Wake threshold service. See 'systemctl status rngd-wake-threshold.service' for details. [DEPEND] Dependency failed for Hardware RNG Entropy Gatherer Daemon. [FAILED] Failed to start VDO volume services. See 'systemctl status vdo.service' for details. [ OK ] Started D-Bus System Message Bus.

### 考えられる原因

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

解決方法

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

#### 処理手順

1. レスキューモード開始前に、誤操作などによる影響を防止するため、インスタンスをバックアップすることを強 くお勧めします。CBSでは スナップショットの作成 を介してバックアップでき、ローカルシステムディスクでは カスタムイメージの作成 を介してイメージをバックアップできます。

2. 下図に示すように、CVMコンソール にログインし、「インスタンス」ページで、インスタンスが配置されてい る行の右側のその他 > 運用保守と検査 > レスキューモードの開始を選択します。

Separate keywords with " ", and s	eparate tags using the Ent	er key			Q, View instances pendir	ng repossession			
ID/Name	Monitoring	Status ¥	Availability Zone 🔻	Instance Type ¥	Instance Configuration	Primary IPv4 🕄	Primary IPv6	Instance Billing Mode 🔻	Network Billing
	di	🔿 Running	Shanghai Zone 4	GPU Compute GN65	4-core 20GB 1Mbps System disk: Premium Cloud Storage			Pay-as-you-go Created at 2021-01-08 19:00:29	Bill by traffic
	di	🔿 Running	Shanghai Zone 4	GPU Compute GN6S	4-core 20GB 1Mbps System disk: Premium Clevel Cr.	1000		Pay-as-you-go Created at 2021-01-08 19:00:28	Bill by traffic
Total items: 2									

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

Enter Rescue Mo	ode	×
<ol> <li>1. Before e period. Th password.</li> <li>2. In the R CentOS 7.</li> <li>3. When a</li> <li>4. To entel corruption</li> <li>5. After ex</li> </ol>	entering the rescue mode, you need to set a password, which is used to access the instance during the rescue the default username is "root". After exiting the Rescue Mode, you need to access the instance with the original descue Mode, the instance starts up from CD-ROM by default. The operating system for CD-ROM start-up is 5 64-bit. In instance is in Rescue Mode, it cannot be started up or shut down. If the Rescue Mode, the instance should be shut down. Forced shutdown may result in data loss or file system In. We recommend manually shutting down the CVM manually before the operation. Rescue Mode, the CVM instance will be "shut down" by default. Please immediately restart it.	
Password	Please enter the rescue mode access password.	
Confirm Password	Please enter the password again.	
Forced Shutdown	Agree to a forced shutdown Forced shutdown may take a while. Please be patient.	
	Enter Rescue Mode Close	

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

D/Name	Monitoring	Status 🝸	Availability Zone 🔻	Instance Type 🔻	Instance Configuration	Primary IPv4 🛈	Primary IPv6	Instance Billing Mode 🔻	Network I
- 87	di	C Entering Rescue Mode	Shanghai Zone 4	GPU Compute GN65	4-core 20GB 1Mbps System disk: Premium Cloud Company		-	Pay-as-you-go Created at 2021-01-08 19:00:29	Bill by traff
		<b>A- - -</b>						_	

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

Create Start Up	Shutdown Rest	tart Reset Password	d Terminate/Return	More Actions *				
Separate keywords with " ", and	separate tags using the Ente	r key			Q, View instances pending repossession			
D/Name	Monitoring	Status 🗡	Availability Zone 🔻	Instance Type ¥	Instance Configuration Primary IPv4 🛈	Primary IPv6	Instance Billing Mode 🔻	Network Billing Moc
	di	Rescue Mode	Shanghai Zone 4	GPU Compute GN65	the same		Pay-as-you-go Created at 2021-01-08 19:00:29	Bill by traffic

5. root アカウントおよび ステップ3 で設定したパスワードを使用し、次の方式でインスタンスにログインします。

インスタンスにパブリックIPが有る場合は、SSHを使用してLinuxインスタンスにログインをご参照ください。

インスタンスにパブリックIPがない場合は、VNCを使用してLinuxインスタンスにログイン をご参照ください。 6. ここでは、VNC方式によるログインを例に取ります。ログインに成功したら、下記のコマンドを実行し、シス テムディスクのルートパーティションをマウントします。

### 説明:

レスキューモードでのインスタンスのシステムディスクデバイス名はvda、ルートパーティションはvda1で、デ フォルトではマウントされていません。



mkdir -p /mnt/vm1





mount /dev/vda1 /mnt/vm1

実行が完了すると、下図のような結果が返されます。

Irootl	~]# mkdir -p /mnt/vm1
[rootl	~]# mount /dev/vda1 /mnt/vm1
[root(	~]# _

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



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



chroot コマンドを実行する場合。

エラー情報がなければ、 cd / コマンドで続行できます。

下図のようなエラー情報が表示された場合は、ルートディレクトリが正常に切り替えられていないので、 cd /mnt/vm1 を実行してルートパーティションのデータを確認します。

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

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

<b>bin</b> boot data dev	etc l	home	lib	lib64	lost+found media	mnt	opt	proc	root	run	sbin	srv	sy
[rootQVM-0-11-centos	vm1]# ]	11											
total 72													
lrwxrwxrwx 1 root	root	7 N	ov 3	2020	bin -> usr∕bin								
dr-xr-xr-x. 5 root	root 4	4096 A	pr 14	17:53	boot								
drwxr-xr-x 2 root	root 4	4096 D	ec 10	2019	data								
drwxr-xr-x 19 root	root 3	3260 A	pr 14	18:09	dev								
drwxr-xr-x. 100 root	root 12	2288 A	pr 14	17:53	etc								
drwxr-xr-x. 2 root	root 4	4096 J	un 28	2021	home								
lrwxrwxrwx 1 root	root	7 N	lov 3	2020	lib → usr/lib								
lrwxrwxrwx 1 root	root	9 N	lov 3	2020	lib64 -> usr/lib64	ł							
drwx 2 root	root 16	6384 <b>N</b>	lov 26	2019	lost+found								
drwxr-xr-x. 2 root	root 4	4096 N	lov 3	2020	media								
drwxr-xr-x. 2 root	root 4	4096 N	lov 3	2020	mnt								
drwxr-xr-x. 2 root	root 4	4096 N	lov 3	2020	opt								
dr-xr-xr-x 125 root	root	0 A	pr 14	18:08	proc								
dr-xr-x 5 root	root 4	4096 M	ar 10	19:24	root								
drwxr-xr-x 37 root	root 1	1140 A	pr 14	18:10	run								
lrwxrwxrwx 1 root	root	8 N	ov 3	2020	<b>sbin -&gt;</b> usr∕sbin								
drwxr-xr-x. 2 root	root 4	4096 N	lov 3	2020	srv								
dr-xr-xr-x 13 root	root	0 A)	pr 14	18:12	sys								
drwxrwxrwt. 8 root	root 4	4096 A	pr 14	17:56	tmp								
drwxr-xr-x. 12 root	root 4	4096 J	un 10	2021	usr								
drwxr-xr-x. 20 root	root 4	4096 J	un 10	2021	Var								
[root@VM-0-11-centos	vm1]# o	cd ./u	sr/bi	n⁄									
[rootQVM-0-11-centos	bin]# j	pwd											
/mnt/vm1/usr/bin													
[root@VM-0-11-centos	bin]# 🛛	ls											
[root@VM-0-11-centos	bin]#												
		_											

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





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





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

#### 説明:

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





異常なマシン:レスキューモードでは、以下のコマンドが順次実行されます。



cd /mnt/vm1/usr/bin/





tar -zxvf bin.tar.gz





chroot /mnt/vm1 /bin/bash

実行結果は、下図のように示されます。

[root0/]# chroot /mnt/vm1 /bin/babaobabbase64baobabbase64bashbugbashbugbashbugbashbug-64bach/]# chroot /mnt/vm1 /bin/bash[root0/]#

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

					view instances pendit	ng repossession				
ID/Name	Monitoring	Status T	Availability Zone 🔻	Instance Type 🔻	Instance Configuration	Primary IPv4 🕄	Primary IPv6	Instance Billing Mode T	Network Billing Mode 🔻	Project <b>T</b>
	di	Rescue Mode	Shanghai Zone 4	GPU Compute GN65	4-core 20GB 1Mbps System disk: Premium Cloud Storage	1		Pay-as-you-go Created at 2021-01-08 19:00:29	Bill by traffic	Default Project
	di	A Running	Shanghai Zone 4	GPU Compute GN85	4-core 20GB 1Mbps System disk: Premium Cloud Storage			Pay-as-you-go Created at 2021-01-08 19:00:28	Bill by traffic	Default Project
otal items: 2										20 🔻 / page H

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



# CVMの再起動またはシャットダウンは失敗 しましたの原因と対処

最終更新日:::2020-10-20 17:08:22

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

# 考えられる原因

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

### トラブルシューティング

### CPU・メモリの使用率を確認する

1. CVMのOSに基づいて、CPU・メモリの使用率を確認します。

Windows CVMの場合: CVMで、「タスクバー」を右クリックして、タスクマネージャーを選択します。

Linux CVMの場合: top コマンドを実行し、 %CPU 列と %MEM 列の情報を確認します。

2. 実際のCPU・メモリの使用率によって、CPUまたメモリの使用率が高いプロセスを終了します。

上記の操作を実行してもCVMをシャットダウンまたは再起動できない場合は、強制終了/再起動を実行してください。

### ACPI管理プログラムをインストールしているかを確認する

説明:

この操作はLinux CVMに適用します。

次のコマンドを実行して、ACPIプロセスが存在するかどうかを確認します。





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

ACPIプロセスが存在する場合、強制終了/再起動を実行してください。

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

### WindowsUpdateが実行しているかを確認する

説明:

この操作はWindows CVMに適用します。

Windows CVMのOSインターフェースで、スタート > コントロールパネル > Windows Update をクリックし、

パッチまたはプログラムが更新されているかどうかを確認します。

Windowsがあるパッチ操作を実行する場合、システムのシャットダウン時にいくつかの処理を行います。更新時間が長すぎるため、シャットダウン/再起動に失敗する可能性があります。Windowsの更新が完了するのを待ってから、CVMをシャットダウンまたは再起動することをお勧めします。

パッチやプログラムが更新されていない場合は、強制終了/再起動を実行してください。

### CVMの初期化が完了したかどうかを確認する

### 説明:

この操作はWindows CVMに適用します。

Windows CVMを初めて購入する場合、システムはSysprepを使用してイメージを配布するため、初期化に時間が かかる場合があります。初期化が完了する前に、Windowsはシャットダウンおよび再起動操作を無視します。

購入したWindows CVMが初期化中の場合、Windows CVMの初期化が完了してから、CVMをシャットダウンまた は再起動することをお勧めします。

初期化が完了すると、強制終了/再起動を実行してください。

### インストールしたソフトウェアが正常に作動するかどうかを確認する

検査ツールまたはウイルス対策ソフトウェアを使用して、CVMにインストールしたソフトウェアが正常に作動す るか、トロイの木馬、またはウイルスに感染しているかどうかを確認します。

異常が発生した場合、システムが破損して、シャットダウンと再起動が失敗する可能性があります。このソフト ウェアをアンインストールし、セキュリティソフトウェアを利用してスキャンするか、データバックアップ後、 システムを再インストールすることをお勧めします。

異常が見つからない場合、強制終了/再起動を実行してください。

### 強制終了/再起動

### 説明:

Tencent Cloudは強制終了/再起動機能を提供し、複数回試行した後にCVMのシャットダウンまたは再起動に失敗した場合に使用できます。この機能を使用すると、CVMの強制終了または再起動が可能になりますが、データの損失やファイルシステムの損傷を引き起こす可能性があります。

1. CVMコンソール にログインします。

2. インスタンス管理ページで、シャットダウンまたは再起動するCVMを選択します。

CVMのシャットダウン:その他 > インスタンス状態 > シャットダウンをクリックします。

CVMの再起動:その他 > インスタンス状態 > 再起動をクリックします。

3. ポップアップダイアログボックスで、**強制シャットダウン**または**強制再起動**を選択し、**確定**をクリックしま す。

**強制シャットダウン**を選択した場合、次の図に示すように:

Shutd	own		×
You hav	e selected 1 Instance,	Learn More 🗸	
No.	Instance Name	Instance ID	Operation
1	Unnamed	100 March 100	Can be shut down
Are you	No Charge when Shut	down the selected instances? : down wn is available when the follo	owing conditions are
met • F • 1 • F	t Pay-as-you-go Instances The instance's system di: Non-GPU-and FPGA-bas	sk and the data disk are both cl ed instances	oud disks.
🖌 For	ced shutdown		
For whe	ed shutdown may lead on the instance cannot b	to data loss or file system dam e shut down normally.	age. This is only allowed
		OK Cancel	

**強制再起動**を選択した場合、次の図に示すように:

ou have	selected <b>1 Instance</b> , Le	earn More 🔻	
No.	Instance Name	Instance ID	Current Bandwidth C.
1	Unnamed	1.000	1 Mbps
uring res	<b>u sure you want to</b> starting, this instance can d restart	o restart the selecte	<b>d instances?</b> nay be affected.
uring re:	u sure you want to starting, this instance can d restart	D restart the selecte	d instances?

# Network Namespaceを作成できない

最終更新日:::2020-03-03 18:59:23

# 問題の説明

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

## 問題の原因

当該問題はカーネルbugです。現在、下記のカーネルバージョンには当該bugが存在しています。 Ubuntu 16.04 x86\_64のカーネルバージョンが4.4.0-91-genericです Ubuntu 16.04 x86\_32のカーネルバージョンが4.4.0-92-genericです

## ソリューション

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

### 処理手順

1. 下記のコマンドを実行し、現在のカーネルバージョンを確認します。





uname -r

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





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

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





linux-image-4.4.0-98-generic - Linux kernel image for version 4.4.0 on 64 bit x86 S 3.下記のコマンドを実行し、新しいバージョンのカーネルとそれに対応するHeaderパッケージをインストールし ます。





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

4. 下記のコマンドを実行し、システムを再起動します。





sudo reboot

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





uname -r

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





4.4.0-98-generic

# カーネルおよび IO 関連問題

最終更新日:::2021-08-31 17:07:41

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

### カーネル問題の特定および処理

### 障害事象

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

### 考えられる原因

#### カーネル hung\_task

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

### カーネルのソフトロックアップ soft lockup

soft lockup とは CPU がカーネルコードに占有され、他のプロセスが実行できないことをいいます。soft lockup を 検出する原理は、各 CPU に一定時間内に実行されるカーネルスレッド [watchdog/x]を割り当てることであり、こ のスレッドが一定時間内(デフォルトは 2\*kernel.watchdog\_thresh 、3.10カーネ

ル kernel.watchdog\_thresh のデフォルトは10秒)に実行されない場合は、 soft lockupが発生したことを意 味します。

kernel.softlockup\_panic=1 に設定すると、カーネル panic がトリガーされ、マシンが再起動します。

#### カーネル panic

カーネルの異常な crash は、マシンの再起動を引き起こします。一般的なカーネル panic シナリオは次のとおりです:

カーネルに hung\_task が出現し、かつ kernel.hung\_task\_panic=1 に設定した場合。

カーネルにソフトロックアップ soft lockup が出現し、かつ kernel.softlockup\_panic=1 に設定した場合。 カーネル bug がトリガーされた場合。

### 対処手順

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

### ハードディスク問題の特定および処理

### ハードディスク inode がフルになる

**障害事象**:新しいファイルを作成すると、「No space left on device」 というエラー情報が表示され、かつ df i コマンドを使用すると、 inode容量使用率100%表示される。

考えられる原因: ファイルシステム inode が枯渇している。

対処手順:使用する必要のないファイルを削除するか、またはハードディスクを拡張します。

### ハードディスク容量使用率がフルである

**障害事象**:新しいファイルを作成すると、「No space left on device」 というエラー情報が表示され、かつ df – h コマンドを使用すると、 ディスク容量使用率100%表示される。

考えられる原因: ハードディスク容量が枯渇している。

対処手順:使用する必要のないファイルを削除するか、またはハードディスクを拡張します。

### ハードディスクが読み取り専用となる

**障害事象**: ファイルシステムがファイルの読み取りしかできなくなり、新たなファイルを作成できない。 考えられる原因: ファイルシステムが破損している。

対処手順:

1. ハードディスクデータをバックアップするためのスナップショットを作成します。詳細は スナップショットの 作成 をご参照ください。

2. ハードディスクのタイプに応じて、対応する対処手順を実行します:

システムディスク

データディスク

インスタンスを直接再起動します。詳細は インスタンスの再起動 をご参照ください。

1. 次のコマンドを実行し、読み取り専用ディスクに対応するファイルシステムのタイプを表示します。





lsblk -f

2. 次のコマンドを実行し、データディスクをアンインストールします。





umount <対応するディスクマウントパス>

3. ファイルシステムのタイプに応じて、次のコマンドを実行し、修復を行います: ext3/ext4 ファイルシステムでは、次のコマンドを実行します:





fsck -y /dev/対応ディスク

xfs ファイルシステムでは、次のコマンドを実行します:





xfs\_repair /dev/対応ディスク

### ハードディスク %util が高い

**障害事象**:インスタンスにラグが発生し、SSHまたはVNCを使用したログインに時間がかかる、または応答しない。

考えられる原因: IO負荷が高く、ハードディスク %util が100%に達している。

対処手順: IO 負荷が合理的かどうかを確認し、かつ IO の読み取りと書き込みを減らすか、またはより高性能な ハードディスクに交換するかを評価する必要があります。

# システムbinまたはlibソフトリンクの欠如

最終更新日:::2022-05-06 11:46:50

#### ##故障について

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

## 考えられる原因

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





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

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

ソリューション

処理手順を参照して、必要なソフトリンクを調べて作成してください。

## 処理手順

1. レスキューモードに進みます。

2.その中の mount 、 chroot などのコマンドを実行します。そのうち、 chroot コマンドを実行した場 合:

エラーがある場合は、 cd /mnt/vm1 を実行します。

エラーがない場合は、 cd / を実行します。

3. 以下のコマンドを実行して、対応するソフトリンクがあるかどうかを確認します。




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

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





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

4. 以下のコマンドを実行して、ソフトリンクをチェックします。





chroot /mnt/vm1 /bin/bash

エラー情報がない場合は、ソフトリンクの修正に成功しています。 5. レスキューモードを終了して、システムを起動します。

## CVMにウイルス侵入が疑われる場合

最終更新日:::2022-05-06 11:46:50

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

問題の特定

SSH方式を使用 または VNC方式を使用 してインスタンスにログイン後、以下の方法でCVMがウイルスに侵入さ れているかどうかを判断します。

rc.local に悪意のあるコマンドが追加されている

以下のコマンドを実行し、 rc.local ファイルを確認します。





#### cat /etc/rc.local

例えば、出力情報が wget xx 、 /tmp/xx など、業務またはお知らせのイメージに追加していないコマンド であった場合、CVMは高い確率でウイルスに侵入されています。 crontab に悪意のあるタスクが追加されている 以下のコマンドを実行し、現在のスケジュール表を列挙します。





crontab -1

例えば、出力情報が wget xx 、 /tmp/xx など、業務またはお知らせのイメージに追加していないコマンド であった場合、CVMは高い確率でウイルスに侵入されています。 ld.so.preloadで動的ライブラリのハイジャックが増加しています 以下のコマンドを実行し、 /etc/ld.so.preload ファイルを確認します。





cat /etc/ld.so.preload

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

sysctl.conf にラージページメモリが設定されています

以下のコマンドを実行し、ラージページメモリの使用状況を確認します。





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

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

## 処理手順

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

2. システムの再インストール を参照して、インスタンスシステムを再インストールし、以下の処置を参照してセ キュリティポリシーを強化します。

CVMのパスワードを変更し、大文字、小文字、特殊記号、数字を組み合わせた12~16桁の複雑なランダムパス ワードを設定します。詳細については、インスタンスのパスワードをリセットをご参照ください。

CVM内の使われていないユーザーを削除します。

sshdのデフォルトの22ポートを1024~65525の間の他の非常用ポートに変更します。詳細については、CVMリ モートデフォルトポートの変更 をご参照ください。

CVMのセキュリティグループに関連付けられているルールを管理し、業務およびプロトコルに必要なポートのみ をオープンにし、すべてのプロトコルおよびポートをオープンにはしないことを推奨します。詳細については、セ キュリティグループルールの追加をご参照ください。

mysql、redisなどのパブリックネットワークにコアアプリケーションサービスポートへのアクセスを開放すること は推奨しません。 関連するポートをローカルアクセスに変更、または外部ネットワークアクセス禁止にすること ができます。

「雲鏡」、「雲鎖」などの保護ソフトウェアをインストールし、リアルタイムアラームを追加して、異常なログ イン情報を速やかに取得できるようにします。

# ファイル作成のエラー no space left on

## device

最終更新日:::2022-05-06 11:46:50

#### ##故障について

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

## 考えられる原因

ディスク容量が満杯

ファイルシステム inode が満杯

df duが不一致

ファイルを削除済みだが、対応するファイルハンドラを持つプロセスがまだ残っており、ディスク容量がかなり の間リリースされていない。

mountマウントネスト。例えば、システムディスクの /data ディレクトリが大容量を使用し、さら

に /data をマウントポイントとしてその他のデータディスクにマウントすると、システムディスクでdf duが一 致しない場合がある。

## ソリューション

処理方法を参照し、問題を調査および解決してください。

処理方法

#### ディスク容量が満杯の問題を解決

1. CVMにログインします。詳細については、標準ログイン方式を使用してLinuxインスタンスにログイン をご参照 ください。

2. で以下のコマンドを実行し、ハードディスク使用率を確認します。





df -h

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





cd対応マウントポイント

例えば、cdシステムディスクマウントポイントが必要な場合、 cd / を実行します。 4. 以下のコマンドを実行し、使用容量の大きいディレクトリを検索します。





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

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

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

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

#### ファイルシステムinodeが満杯の問題を解決

1. CVMにログインします。詳細については、標準ログイン方式を使用してLinuxインスタンスにログイン をご参照 ください。

2. で以下のコマンドを実行し、ハードディスク使用率を確認します。



df -h

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





cd対応マウントポイント

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

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





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

#### df duが不一致という問題を解決

#### プロセスがファイルハンドラを占用する問題を解決

以下のコマンドを実行し、占用しているファイルのプロセスを確認します。





lsof | grep delete

リターン結果に応じて、以下の手順を実行します。

kill対応プロセス。

サービスを再起動します。

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

#### mountマウントネストの問題を解決

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





mount /dev/vda1 /mnt

2.以下のコマンドを実行し、 /mnt に入ります。





cd /mnt

3. 以下のコマンドを実行し、使用容量の大きいディレクトリを検索します。





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

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

4. umountコマンドを実行し、磁気ディスクをマウント解除します。例:





umount /mnt

# ネットワーク関連の故障 国際リンクレイテンシー

最終更新日:::2022-07-26 17:41:55

## 問題の説明

北米リージョンのCVMにログインする時レイテンシーが長すぎます。

### 問題の分析

国内の国際ルーティング出口の数が少ないおよびその他要因により、並列処理数が高くなると、国際リンクが非常に混雑になり、アクセスが不安定になります。Tencent Cloudはすでにこの問題ををキャリアに報告しています。

現在、北米リージョンのCVMを購入して、中国国内で管理及びメンテナンスする必要がある場合、中国香港リー ジョンで購入したCVMを経由して、北米リージョンのCVMにログインすることで問題を解決できます。

## ソリューション

1. 中国香港リージョンのWindows CVMを購入して、「ジャンプサーバー」として利用します。

#### ご注意:

「カスタマイズ設定」ページの「1.リージョンとモデル選択」で、**中国香港**リージョンを選択します。

#### ここをクリックして購入する >>

Windows CVMは、北米リージョンにあるWindowsとLinuxのCVMへのログインをサポートしているので、購入することを推奨します。

中国香港リージョンのWindows CVMを購入する場合、1Mbps以上の帯域幅を購入する必要があります。そうし ないと、ジャンプサーバーにログインできません。

2. 購入が成功した後、実際のニーズに応じて、中国香港リージョンのWindows CVMのログイン方法を選択する: RDPファイルを利用してWindows CVMにログインする

リモートデスクトップを利用してWindows CVMにログインする

#### VNC を利用してWindows CVMにログインする

3. 中国香港リージョンのWindows CVMで、実際のニーズに応じて、北米リージョンにあるCVMへのログイン方式 を選択する:

北米リージョンのLinux CVMにログインします。

標準ログイン方式を利用してLinux CVM にログインする



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

## ウェブサイトにアクセスできません

最終更新日:::2020-09-10 17:47:51

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

### 可能な原因

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

### 故障の処理

#### サーバー関連問題のトラブルシューティング

サーバーのシャットダウン、ハードウェアの故障、CPU/メモリ/帯域幅の使用率が高すぎるなどの原因によって、 ウェブサイトにアクセスできなくなる可能性があります。そのため、順次にサーバーの稼働状態、CPU/メモリ/帯 域幅の使用状況をトラブルシューティングすることをおすすめします。

1. CVMコンソール にログインし、インスタンスの管理ページでインスタンスが正常に実行しているかどうかを確認します。

正常に実行している場合は、ステップ2を実行してください。

正常に実行していない場合は、CVMインスタンスをリスタートしてください。

2.

インスタンスのID/インスタンス名をクリックし、該当するインスタンスの詳細ページに入ります。

#### 3. モニタニングタブを選択し、CPU/メモリ/帯域幅の使用状況を確認します。

CPU/メモリの使用率が高すぎる場合は、Windowsインスタンス:CPUとメモリの使用率が高すぎるためログイン 不能 と Linuxインスタンス:CPUとメモリの使用率が高すぎるためログイン不能 を参照して調べてください。 帯域幅の使用率が高すぎる場合は、帯域幅の占有率が高すぎるためログイン不能を参照して調べてください。 CPU/メモリ/帯域幅の使用状況が正常である場合は、ステップ4 を実行してください。

4.

次のコマンドを実行し、Webサービスに対応するポートが正常に監視されているかを確認します。

#### 説明:

HTTPサービスによく使われている80ポートを例として、操作について説明します。

Linuxインスタンス: netstat -ntulp |grep 80 コマンドを実行します。

[root@VM_2_	184_cen	tos ~]# netstat -ntulp  g	rep 80	
tcp	0	0 0.0.0.0:80	0.0.0:*	LISTEN

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

C:\Users	Administrator>netstat	-anolfindstr :80	
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	10.135.182.70:53406	10.225.30.181:80	TIME_WAIT
TCP	10.135.182.70:53419	10.225.30.181:80	TIME_WAIT
TCP	10.135.182.70:53423	10.225.30.181:80	TIME_WAIT
TCP	[::]:80	[::]:0	LISTENING

ポートが正常に監視されている場合は、ステップ5を実行してください。

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

5.

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

Linuxインスタンス: iptablesが80ポートをインターネットにオープンしているかどうかを確認するため

に、 iptables -vnL コマンドを実行します。

80ポートをインターネットにオープンしている場合は、ネットワーク関連問題のトラブルシューティングを実行 してください。

80ポートをインターネットにオープンしていない場合は、 iptables -I INPUT 5 -p tcp --dport 80 j ACCEPT コマンドを実行して、80ポートをオープンしてください。

Windowsインスタンス:OSのインターフェースで、【スタート】>【コントロールパネル】>【ファイアウォール 設定】をクリックし、Windowsファイアウォールが無効になっているかを確認します。

- 無効になっている場合は、ネットワーク関連問題のトラブルシューティングを実行してください。

- 無効になっていない場合は、ファイアウォール設定をオフにしてください。

#### ネットワーク関連問題のトラブルシューティング

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





対象サーバーのパブリックIPをpingします

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

• Bo:~ chenhuiping\$ ping 193.112.12.138 64 bytes from 193.112.12.138: icmp\_seq=0 ttl=43 time=161.240 ms 64 bytes from 193.112.12.138: icmp\_seq=1 ttl=43 time=161.996 ms 64 bytes from 193.112.12.138: icmp\_seq=2 ttl=43 time=164.837 ms 64 bytes from 193.112.12.138: icmp\_seq=3 ttl=43 time=215.650 ms 64 bytes from 193.112.12.138: icmp\_seq=4 ttl=43 time=166.375 ms 64 bytes from 193.112.12.138: icmp\_seq=5 ttl=43 time=160.576 ms 64 bytes from 193.112.12.138: icmp seq=6 ttl=43 time=161.016 ms 64 bytes from 193.112.12.138: icmp\_seq=7 ttl=43 time=164.129 ms 64 bytes from 193.112.12.138: icmp\_seq=8 ttl=43 time=192.682 ms 64 bytes from 193.112.12.138: icmp\_seq=9 ttl=43 time=163.376 ms 64 bytes from 193.112.12.138: icmp\_seq=10 ttl=43 time=161.859 ms 20 - 193.112.12.138 ping statistics ---11 packets transmitted, 11 packets received, 0.0% packet loss cound-trip min/avg/max/stddev = 160.576/170.340/215.650/16.765 ms

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

#### キュリティグループ設定の関連問題のトラブルシューティング

セキュリティグループとは、関連するインスタンスのインバウンド・アウトバウンドトラフィックを制御できる 仮想ファイアウォールのことです。そのルールは、プロトコルやポート、ポリシーなどを指定できます。Webプロ セス関連のポートをインターネットにオープンしていない場合も、ウェブサイトにアクセスできなくなります。 1. CVMコンソール にログインし、「インスタンスリスト」ページでインスタンスのID/インスタンス名をクリック することで、該当するインスタンスの詳細ページに入ります。

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

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

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

#### ドメイン名、ICP申告のトラブルシューティングと関連問題の解析

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

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

Tencent Cloudのドメイン名サービスを使用している場合は、ドメイン名管理コンソール にログインして該当する ドメイン名を確認できます。

ドメイン名がICP申告を取得している場合は、ステップ2を実行してください。

2.

解析発効についてを参照し、関連する問題を解析し、トラブルシューティングします。

ウェブサイトにアクセスできないという問題が解決された場合、タスクは終了します。

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

©2013-2022 Tencent Cloud. All rights reserved.

## ウェブサイトのアクセスラグ

最終更新日:::2020-03-03 19:09:30

## 問題説明

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

### 問題解析

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

## ソリューション

#### ロカールクライアントの確認

1. ロカールクライアントで 華佗診断分析システム にアクセスし、ローカルから各ドメイン名にアクセスするス ピードをテストします。

2. テスト結果に基づいて、ロカールネットワークに問題があるかどうかを確認します。 例えば、テスト結果が下図に示すようになっている場合は、

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

結果から各ドメイン名にアクセスする時のレイテンシーを確認し、ネットワークが正常であるかどうかを確認で きます。

正常でない場合は、問題を確定して解決するように、ネットワークサービスのプロバイダーに連絡ください。 正常である場合は、ネットワークリンクの確認 を実行してください。

#### ネットワークリンクの確認

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



パケットロスや高いレイテンシーがある場合は、MTRを使って診断してください。具体的な操作は、サーバーの ネットワークディレーとパケットロスの処理 をご参照ください。

パケットロスや高いレイテンシーがない場合は、ステップ2を実行してください。

#### 2.

dig/nslookup コマンドを使ってDNSの解析を確認し、DNS解析による問題であるかどうかをトラブルシュー ティングします。

直接にパブリックIPを使って該当のページにアクセスし、ウェブサイトにアクセスする際のネット渋滞とスピード 低下の原因がDNSにあるかどうかを調べることもできます。

そうである場合は、DNS解析を確認してください。具体的な操作は、解析発効についてをご参照ください。 そうでない場合は、サーバーの確認を実行してください。

#### サーバーの確認

1. CVMコンソール にログインします。

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

asic Info ENI	Monitoring	Security Groups Operation Logs			
Real Time Last	24 hours Last 7 day	Select Date 🗐 Data Comparison Period: 10	second(s) 🔻		
DNote: Max, Min, and A	vg are the maximum, minin	um, and average values of all points in the current line chart respective	ely.		
CPU Monitoring	CPU Utilization%	2 -	Max:	Min:	Avg:
2		1 - MARMINIANAN MUNANANANANANANANANANANANANANANANANANANA	MMM 1.6%	0.5%	0.883
	Basic CPU Usage%	4 -	Max:	Min:	Avg:
		2 - 0 - ภัณฑัณฑัณฑัณาาาที่การการแบบบานพระปักทุณหมายไม่พระการการการการการการการการการการการการการก	2%	0%	0.65%
System Avg.	CPU Avg. Load	1 -	Max:	Min:	Avg:
Workload 1 minute		0.5 - 0M	NM 0.44	0	0.034
Memory Monitor	Memory UsageMB	400 -	Max:	Min:	Avg:
		200	174MB	171MB	171.51
	Memory Utilization	20 -	Max:	Min:	Avg:
	(%)%	10	0.50/	0.20/	0.2.40/

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

#### ほかの問題の確認

インスタンスのリソース利用状況に基づいて、サーバー負荷によるリソース消費の増加であるかどうかを判断し ます。

そうである場合は、サービスプログラムを最適化するか、サーバー構成のアップデートを行うことをおすすめし ます。新しいサーバーを購入して、既存のサーバーの負荷を分担させることもできます。

そうでない場合は、ログファイルを確認し、問題を特定してから指向性のある最適化を実行することをおすすめ します。

# ネットワークカードマルチキュー設定エラー の場合

最終更新日:::2022-05-06 11:46:50

## 故障について

CVMネットワークカードマルチキュー設定でエラーが発生します。

## 考えられる原因

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

## ソリューション

処理手順 を参照し、ENIキューの個数を修正してください。

## 処理手順

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





ethtool -l eth0

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





Channel paramete	ers for e	th0:
Pre-set maximums	5:	
RX:	0	
TX:	0	
Other:	0	
Combined:	2	### サーバーがサポートするENIキューの最大個数
Current hardware settings:		
RX:	0	
TX:	0	
Other:	0	
Combined:	1	###現在設定しているENIキューの個数

2. 以下のコマンドを実行し、現在のENIキューの個数を設定します。



ethtool -L eth0 combined 2

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

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




ethtool -l eth

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

# CVMネットワークディレーとパケットロス

最終更新日:::2022-05-06 14:57:08

### 問題の説明

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

### 問題の分析

バックボーンリンクの輻輳、リンクノードの故障、サーバー負荷が高い、システムの設置問題などの原因により、パケットロスや高いレイテンシーを引き起こす可能性があります。CVM自体のの原因を除外した後、MTRを 使用してより詳細な診断を行うことができます。

MTRはネットワーク診断ツールであり、このツールで診断されたレポートを通じて、ネットワーク問題が発生す る原因を確認することができます。

## 対処方法

ここではLinuxとWindows CVMを例に取り、MTRの使用方法およびMTRのレポート結果に対する分析方法について説明します。

#### 説明:

ローカルまたはCVMでPingが無効になっている場合、MTRは結果を返しません。

MTRを実行しているホストOSに応じて、MTRの紹介と使用方法をご参照てください。

WinMTRの説明および使用(Windows OS)

MTRの説明および使用(Linux OS)

WinMTR:はWindows に適応する無料なインターネット診断ツールであり、Pingとtracertのすべての機能を統合 し、グラフィカルインターフェースがあり、各ノードの応答時間とパケットロスの状況を確認することができま す。

#### WinMTRをインストールする

1. Windows CVMにログインします。

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

3. WinMTRインストールパッケージを解凍/圧縮する。

#### WinMTRの使用

1. WinMTR.exeをダブルクリックして、WinMTRツールを開く。

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

🐨 WinMTR v0.92 64	bit by Appnor MSP - www.w	vinmtr.net 🗕 🗖 🗙
Host: 192.168.100.12	.▼ <u>S</u> tart	<u>Options</u> Exit
Copy Text to clipboard	Copy HTML to clipboard	Export <u>T</u> EXT Export <u>H</u> TML
Hostname	Nr Loss % Sent Recv Bes	st Avrg Worst Last
, WinMTR v0.92 GPL V2 by Appr	nor MSP - Fully Managed Hosting &	Cloud Provi www.appnor.com

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

🐨 WinMTR v0.92 64 bit by Appnor MSP - www.winmtr.net 📃 🗖 🗙							
Host: 192.168.100.12		<u> </u>	Stop		<u>O</u> ption:	s	E <u>x</u> it
Copy Text to clipboard Cop	y HTML to	clipboard			Export <u>T</u> E	XT Ex	port <u>H</u> TML
Hostname 192.98.91.130 192.168.100.12	Nr Lo 1 0 2 0	ss % Sent 28 28	Recv 28 28	Best 1 0	Avrg 2 0	Worst 13 0	Last 12 0
Double click on host name for more information.							

テスト結果の情報は以下の通り:

Hostname: 宛先サーバーに経由した各ホストIPまたは名称です。

Nr:経由したノード数です。

\*\*Loss%\*\*:対応するノードのパケットロス率です。

**Sent**:送信したデータパッケージ数です。

Recv:受信した応答数です。

Best:最短の応答時間です。

Avrg:平均応答時間です。

Worst: 最長の応答時間です。

Last:直近の応答時間です。

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

#### MTRをインストールする

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





yum install mtr

Ubuntu OS:





sudo apt-get install mtr

#### MTR 相関パラメータの説明

**-h/--help**:ヘルプメニューを表示する

- -v/--version:MTRのバージョン情報を表示する
- -r/--report:結果はレポートとして出力する
- **-p/--split**:\*\*--report\*\*とは対照的に、各追跡の結果を個別にリスト表示する
- -c/--report-cycles:毎秒で発送するデータパッケージの数を設置し、デフォルトでは10となる

-s/--psize:パッケージのサイズを設置する

**-n/--no-dns**: IPアドレスに対してドメイン名の解析を行わない

-a/--address:ユーザーはデータパッケージの発送IPアドレスを設定します、重要ユーザーが単一のホスト上に複数のIPアドレスをもつケース

- **-4**: IPv4
- -6: IPv6

#### ユースケース

ローカルでIPが119.28.98.39のサーバーを例とします。

以下のコマンドを実行して、レポートとしてのMTRの診断結果を出力します。





mtr 119.28.98.39 --report

次のような情報が返されます:





[root@VM_103_80_centos ~]# mtr 119.28.98.39report							
Start: Mon Feb 5 11:33:34 201	.9						
HOST:VM_103_80_centos	Loss%	Snt	Last	Avg	Best	Wrst	StD
1.  100.119.162.130	0.0%	10	6.5	8.4	4.6	13.7	2
2.  100.119.170.58	0.0%	10	0.8	8.4	0.6	1.1	0
3.  10.200.135.213	0.0%	10	0.4	8.4	0.4	2.5	0
4.   10.200.16.173	0.0%	10	1.6	8.4	1.4	1.6	0
5.  14.18.199.58	0.0%	10	1.0	8.4	1.0	4.1	0
6.  14.18.199.25	0.0%	10	4.1	8.4	3.3	10.2	1
7.  113.96.7.214	0.0%	10	5.8	8.4	3.1	10.1	2
8.   113.96.0.106	0.0%	10	3.9	8.4	3.9	11.0	2

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

主な出力情報は以下のように:

**HOST:**ノードのIP アドレスまたはドメイン名です。

Loss%:パケットロス率です。

Snt:毎秒で発送したデータパッケージの数です。

Last:直近の応答時間です。

Avg:平均応答時間です。

Best:最短の応答時間です。

Wrst:最長の応答時間です。

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

#### レポートの結果分析と処理

説明:

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

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

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

宛先サーバーはパケットロスが発生した場合は、ステップ2を実行してください。

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

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

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

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

## CVMネットワークアクセスパケット損失

最終更新日:::2022-05-06 11:46:50

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

### 考えられる原因

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

### 前提条件

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

### トラブルシューティング

### 速度制限のトリガーによるTCP パケット損失

CVMインスタンスには複数の仕様があり、仕様ごとにネットワーク性能が異なります。インスタンスの帯域幅や パケットがインスタンス仕様に対応する基準を超過した場合、プラットフォーム側の速度制限がトリガーされ、 パケット損失を引き起こすことがあります。トラブルシューティングと対処手順は次のとおりです: 1.インスタンスの帯域幅とパケットを確認します。

Linux インスタンスでは、 sar -n DEV 2 コマンドを実行して帯域幅とパケットを確認することができま す。 rxpck/s と txpck/s 指標は送受信パケット、 rxkB/s と txkB/s 指標は送受信帯域幅です。 2. 取得した帯域幅とパケットデータを使用して インスタンス仕様 を比較し、インスタンス仕様の性能ボトルネッ クに達していないかどうかを確認します。

ボトルネックに達している場合は、インスタンス仕様をアップグレードするか、または業務量を調整する必要が あります。

インスタンス仕様の性能ボトルネックに達していない場合は、チケットを提出し、問題をさらに特定し対処する ことができます。

#### 速度制限のトリガーによるUDP パケット損失

速度制限のトリガーによるTCP パケット損失 手順を参考に、インスタンス仕様の性能ボトルネックによるパケット損失かどうかを判断します。

ボトルネックに達している場合は、インスタンス仕様をアップグレードするか、または業務量を調整する必要が あります。

インスタンス仕様の性能ボトルネックに達していない場合は、プラットフォームのDNSリクエストに対する追加 的な頻度制限が原因である可能性があります。インスタンス全体の帯域幅やパケットがインスタンス仕様の性能ボ トルネックに達している場合は、DNSリクエストの速度制限がトリガーされ、UDPパケット損失が発生する可能 性があります。チケットを提出して処理を更に特定することができます。

#### ソフトウェア割り込みのトリガーによるパケット損失

オペレーティングシステムが /proc/net/softnet\_stat の二列目のカウント値の増加を検出した場合は、 「ソフトウェア割り込みによるパケット損失」と判断することができます。インスタンスがソフトウェアの割り込 みをトリガーしパケット損失が引き起こされた場合は、次の手順でトラブルシューティングを行い、対処するこ とができます:

RPSが有効化されているかどうかを確認する:

有効化されている場合は、カーネルパラメータ net.core.netdev\_max\_backlog が小さすぎるとパケット損 失が引き起こされることから、大きくする必要があります。カーネルパラメータの詳細情報については、 Linuxイ ンスタンスで一般的に使用されるカーネルパラメータの説明 をご参照ください。

有効化されていない場合は、 CPU シングルコアのソフトウェア割り込み負荷が高いことによって、データが速や かに送受信できない事象が引き起こされていないかどうかを確認します。もしそうであれば:

RPSの有効化を選択し、ソフトウェア割り込みの割り当てをより均衡にします。

業務プロセスがソフトウェア割り込みの不均衡を引き起こしているかどうかを確認します。

#### UDP 送信バッファがフル

インスタンスが UDP バッファ不足によりパケット損失を引き起こしている場合は、次の手順でトラブルシュー ティングを行い対処することができます:

1. ss -nump コマンドを使用して UDP 送信バッファがフルかどうかを確認します。

フルである場合は、カーネルパラメータ net.core.wmem\_max と net.core.wmem\_default を大きくし、UDP プログラムを再起動して有効にします。カーネルパラメータの詳細情報については、Linux インスタンスで一般的に使用されるカーネルパラメータの説明 をご参照ください。

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

#### UDP 受信バッファがフル

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

1. ss -nump コマンドを使用して UDP 受信バッファがフルかどうかを確認します。

フルである場合は、カーネルパラメータ net.core.rmem\_max と net.core.rmem\_default を大きく
 U、UDP プログラムを再起動して有効にします。カーネルパラメータの詳細情報については、Linux インスタンスで一般的に使用されるカーネルパラメータの説明 をご参照ください。

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

#### TCP すべての接続キューがフル

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

 カーネルパラメータ net.core.somaxconn を大きくします。カーネルパラメータの詳細情報については、 Linux インスタンスで一般的に使用されるカーネルパラメータの説明 をご参照ください。

2. 業務プロセスが backlog パラメータを渡したかどうかを確認します。渡している場合は、 backlog パラメータを 相応に大きくします。

#### TCP リクエストのオーバーフロー

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

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

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

#### 説明:

**setsockopt**の値はカーネルパラメータ net.core.rmem\_max と net.core.wmem\_max によって制限されま す。業務プログラムを調整すると同時に、 net.core.rmem\_max と net.core.wmem\_max を同期的に調整 することができます。調整後に業務プログラムを再起動し、設定を有効にします。 設定していない場合は、カーネルパラメータ net.ipv4.tcp\_mem 、 net.ipv4.tcp\_rmem および net.ipv4.tcp\_wmem を大きくすることで TCP socket のレベルを調整することができます。

カーネルパラメータの修正については、Linux インスタンスで一般的に使用されるカーネルパラメータの説明 を ご参照ください。

### 接続数が上限に到達

CVMインスタンスには複数の仕様があり、仕様ごとに接続数性能指標が異なります。インスタンスの接続数がインスタンス仕様に対応する基準を超過した場合、プラットフォームの速度制限がトリガーされ、パケット損失を引き起こすことがあります。対処手順は次のとおりです:

#### 説明:

接続数とはホストに保存されるCVMインスタンスのセッション数であり、TCP、UDPとICMPが含まれます。この数値はCVMインスタンスで ss や netstat コマンドを介して取得されたネットワーク接続数よりも大きくなります。

インスタンスの接続数を確認して、 インスタンス仕様 を比較し、インスタンス仕様の性能ボトルネックに達して いないかどうかを確認します。

ボトルネックに達している場合は、インスタンス仕様をアップグレードするか、または業務量を調整する必要が あります。

インスタンス仕様の性能ボトルネックに達していない場合は、チケットを提出して処理を更に特定することがで きます。

### iptables policy関連ルールの設定

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

1. 以下のコマンドを実行し、iptables policy ルールを確認します。





iptables -L | grep policy

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





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

2.以下のコマンドを実行し、必要に応じて -P の後ろの値を変更します。





iptables -P INPUT ACCEPT

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





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

# インスタンス IP アドレスを ping できない

最終更新日:::2023-02-01 16:43:58

### 障害の現象

ローカルホストからインスタンスにpingが通らない場合は、以下のような原因が考えられます:

ターゲットサーバーの設定が正しくない

ドメイン名が正しく解析されていない

リンク障害

ローカルネットワークが正常に動作している前提で(他のウェブサイトへのpingが通る)、下記の操作によりトラ ブルシューティングを実施します:

インスタンスにはパブリックIPアドレスが設定されているかを確認

セキュリティグループの設定を確認

システム設定を確認

その他の操作

実施手順

### インスタンスにはパブリックIPアドレスが設定されているかを確認します

説明:

インスタンスにパブリックIPアドレスが設定されている場合のみ、Internet上の他のコンピュータと通信できま す。インスタンスにパブリックIPアドレスが設定されていない場合、プライベートIPアドレスでは外部からインス タンスへのpingが通りません。

1. CVMコンソール にログインします。

2.「インスタンスリスト」画面で、下図に示すように、pingを実行したいインスタンスID/インスタンス名を選択 し、下図にしめされているように、そのインスタンスの詳細画面に入ります:

Console Products	s <del>*</del>		
Cloud Virtual Machine	← ins-llf99epy	(Unnamed)	
😂 Instances	Basic Info E	NI Monitoring Security Groups Operation Logs	
Oedicated Host	Instance Info		Architecture diagram
🔅 Placement Group	Name	Unnamed	South China (Guangzhou) / Guangzhou Zone 4 / subnet-31u47d2w
◎ Image	Instance ID		
⊕ Auto Scaling ⊠	Instance specification		
Storage	Project	Default Project	1 ENI(s)
I Snapshots ▼	Region	South China (Guangzhou)	Tencent Linux Release 1.2 (Final)
SSH Key     Socurity Groups	Availability Zone	Guangzhou Zone 4	Kunning
EIP	Кеу	None	System Disk disk-nf3zczes
	Tag	None	Premium Cloud Storage, 50 GB in total Pay as you go Creation time: 2019-08-13 18:15:26
			Mount
	Network Information	ion	
	Network		
	Subnet	Default-Subnet)	
	Public IP		
	Private IP		
	Act as internet gatewa	y No	

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

### セキュリティグループの設定を確認します

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

1. CVMコンソール にログインします。

2. 「インスタンスリスト」画面で、セキュリティグループを設定するインスタンスのID/インスタンス名を選択して、そのインスタンスの詳細画面に入ります。

3. セキュリティグループタブを選択し、下図に示すように、対象インスタンスのセキュリティグループ管理画面 に入ります。

Cloud Virtual Machine	← ins-Ilf99epy (Unnamed)		
😔 Instances	Basic Info ENI Monitoring Security Group	s Operation Logs	
Oedicated Host			
🔅 Placement Group	Bound to security group	Sort Bind	Rule preview
💿 Image	Prior Security Group ID/name	Operation	Unbound rule
🛱 Auto Scaling 🖄	1 sq-dejyvc8x	Unbind	▼ Tencent internal-20190813181436218
Cloud Block Storage			Source
Snapshots •			
la SSH Key			
🗐 Security Groups			
IP EIP			

4. インスタンスで使用されているセキュリティグループ、およびインバウンドルールとアウトバウンドルールの 詳細を確認することにより、インスタンスと関連を付けたセキュリティグループではICMPを許可しているかを判 断します。

許可している場合、システム設定を確認 してください。

許可しない場合、ICMPプロトコルのポリシーを許可するように設定してください。

### [システム設定を確認します

インスタンスのOSタイプを判断して、確認方法を選択します。

Linux OSの場合、Linuxカーネルのパラメータとファイアウォールの設定を確認 してください。

Windows OSの場合、Windowsのファイアウォールの設定を確認 してください。ファイアウォールに問題がなければ、Windowsのネットワーク設定をリセット してください。

#### Linuxカーネルのパラメータとファイアウォールの設定を確認します

#### 説明:

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

#### カーネルパラメータicmp\_echo\_ignore\_allを確認します

1. VNCでインスタンスにログインします。詳しくは以下をご参照ください。

VNCによるLinuxインスタンスへのログイン

VNCによるWindowsインスタンスへのログイン

2. 下記のコマンドを実行し、システムのicmp\_echo\_ignore\_allの設定を確認します。





cat /proc/sys/net/ipv4/icmp\_echo\_ignore\_all

0が返された場合、システムではすべてのICMP Echoリクエストが許可されるため、ファイアウォールの設定を確認してください。

1が返された場合、システムではすべてのICMP Echoリクエストが拒否されるため、手順3 を実施してください。 3. 下記のコマンドを実行し、カーネルパラメータicmp\_echo\_ignore\_allの設定を変更します。

![](_page_310_Picture_1.jpeg)

![](_page_310_Picture_2.jpeg)

echo "0" >/proc/sys/net/ipv4/icmp\_echo\_ignore\_all

#### ファイアウォールの設定を確認します

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

![](_page_311_Picture_1.jpeg)

![](_page_311_Picture_2.jpeg)

iptables -L

以下が返された場合、該当するICMPルールが禁止されていません。

![](_page_312_Picture_1.jpeg)

![](_page_312_Picture_2.jpeg)

Chain INPUT (policy ACCEPT) target prot opt source ACCEPT icmp -- anywhere Chain FORWARD (policy ACCEPT) target prot opt source Chain OUTPUT (policy ACCEPT) target prot opt source ACCEPT icmp -- anywhere

destination anywhere destination destination anywhere

icmp echo-request

icmp echo-request

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

![](_page_313_Picture_3.jpeg)

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

#### Windowsファイアウォールの設定を確認します

1. インスタンスにログインします。

2. コントロールパネルを起動し、Windows Defender ファイアウォールの設定を選択します。

3.「Windows Defender ファイアウォール」画面で、高度な設定を選択します。

3. 表示された「セキュリティが強化されたWindows Defender ファイアウォール」ウィンドウで、ICMPに関する アウトバウンドとインバウンドのルールが禁止されているかを確認します。

下図に示すように、ICMPに関するアウトバウンドとインバウンドのルールが無効になっている場合は、ルールを 有効にしてください。

#### Windowsのネットワーク設定をリセットします

1. ご利用のVPCネットワークではDHCPがサポートされているかを確認してください(2018年6月以降に作成した VPCネットワークの場合、DHCPがサポートされています)。サポートされていない場合、ネットワーク設定にお ける静的IPが正しいかを確認してください。

2. DHCPがサポートされている場合、DHCPに割り当てられたプライベートネットワークIPが正しいかを確認して ください。正しくない場合、公式サイトのログイン機能(VNCでログイン)を使用し管理者としてPowerShellを 起動し、DHCPコンポーネントがIPを再取得するように、 ipconfig /release と ipconfig/renew (マシ ンを再起動する必要はありません)を実行してみてください。

3. DHCPに割り当てられたプライベートネットワークIPが正しいが、依然としてpingが通らない場合、スタートメ ニューからファイル名を指定して実行を起動し、 ncpa.cpl を入力して[OK]をクリックします。ローカル接 続を起動し、LANカードを無効にしてから有効にします。

4. 上記の方法を試しても問題を解決できない場合は、管理者としてCMDで以下のコマンドを実行してマシンを再 起動します。

![](_page_315_Picture_1.jpeg)

![](_page_315_Picture_2.jpeg)

reg delete "HKEY\_LOCAL\_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Ne

### その他の操作

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

# ドメイン名を解析できない(CentOS 6.x シ ステム)

最終更新日:::2020-01-08 16:35:32

### 事象の説明

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

### 考えられる原因

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

## 解決方法

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

### 処理手順

1. CVM にログインします。

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

![](_page_317_Picture_1.jpeg)

![](_page_317_Picture_2.jpeg)

rpm -q initscripts

次のような情報が返されます:

![](_page_318_Picture_1.jpeg)

![](_page_318_Picture_2.jpeg)

initscripts-9.03.40-2.e16.centos.x86\_64

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

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

![](_page_319_Picture_1.jpeg)

![](_page_319_Picture_2.jpeg)

yum makecache
yum -y update initscripts
service network restart

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

![](_page_320_Picture_1.jpeg)

![](_page_320_Picture_2.jpeg)

rpm -q initscripts

次のような情報が返されます:

![](_page_321_Picture_1.jpeg)

![](_page_321_Picture_2.jpeg)

initscripts-9.03.58-1.el6.centos.2.x86\_64

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