Cloud Log Service

よくあるご質問

製品ドキュメント



©2013-2026 Tencent Cloud. 著作権を所有しています。

著作権声明

©2013–2026 Tencent Cloud. 著作権を所有しています。

このドキュメントは、Tencent Cloudが著作権を専有しています。Tencent Cloudの事前の書面による許可なしに、いかなる主体であれ、いかなる形式であれ、このドキュメントの内容の全部または一部を複製、修正、盗作、配布することはできません。

商標に関する声明

Tencent Cloud

およびその他のTencent Cloudサービスに関連する商標は、すべてTencentグループ下の関連会社主体により所有しています。また、本ドキュメントに記載されている第三者主体の商標は、法に基づき権利者により所有しています。

サービス声明

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

カタログ:

よくあるご質問
- 健康監視の問題に関する説明
  - インデックス設定について
  - ログアップロード関連
  - 収集設定関連
- 収集関連
  - マシングループに関するよくある質問
  - Machine Group Exception
  - LogListenerに関するよくある質問
  - LogListenerインストール異常問題
  - コンテナログ収集に関するよくある質問
  - 自建K8Sログ収集トラブルシューティングガイド
  - 収集設定に関するよくある質問
  - 収集自己チェックツール利用ガイド
- 検索分析関連
  - ログを検索できない
  - 検索分析エラー
  - 統計分析（SQL）結果の小数点以下桁数が不正確
- その他の問題

©2013-2026 Tencent Cloud. 著作権を所有しています。

よくあるご質問
健康監視の問題に関する説明
インデックス設定について

最終更新日：：2026-10-12 15:06:44

インデックス設定を有効にする方法は何ですか。

インデックス設定は、CLS（Cloud Log Service）を使用して検索分析を行うための必要条件です。インデックスを有効にしていない場合、ログの検索分析は行えません。有効にすることを強く推奨します。

操作手順

1. CLSコンソールにログインします。
2. 左側のナビゲーションバーで**ログトピック**をクリックし、ログトピックリストページに移動します。
3. インデックスを設定する必要があるログトピックのID/名前をクリックし、ログトピック管理ページに移動します。
4. **インデックス設定**タブを選択し、**編集**をクリックして、インデックス設定編集ページに移動します。
5. インデックス状態スイッチをクリックして、インデックスを有効にします。
6. インデックスを有効にした後、全文インデックスまたはキー値をさらに設定できます。
   - 全文インデックス：ログの全文検索をサポートします。
   - キー値インデックス：ログコンテンツ内の指定フィールドに基づく検索をサポートします。この設定の前提条件は、ログ収集設定における抽出モードが構造化抽出モード（つまりログをキー値ペアに解析するモード）であることです。

キーバリューインデックス設定を有効にする方法は何ですか。

キー値インデックスとは、全文インデックスを基に、元のログをフィールド（つまり key:value）ごとに複数のトークンに分割してインデックスを構築し、検索時にキー値方式で検索するものです。ログ検索の効率を最大化するために、有効にすることを強く推奨します。

> ⚠ **注意：**
> キー値インデックスを有効にするための前提条件は、ログ収集設定の抽出モードが構造化抽出モード（つまりログをキー値ペアに解析するモード）であることです。

操作手順

1. CLSコンソールにログインします。
2. 左側のナビゲーションバーで**ログトピック**をクリックし、ログトピックリストページに移動します。
3. インデックスを設定する必要があるログトピックのID/名前をクリックし、ログトピック管理ページに移動します。

©2013-2026 Tencent Cloud. 著作権を所有しています。

4. **インデックス設定**タブを選択し、**編集**をクリックして、インデックス設定編集ページに移動します。
5. キー値インデックススイッチをクリックして、キー値インデックスを有効にします。
6. キー値インデックスを有効にした後、自動設定をクリックすると、システムは収集された最新の1件のログをサンプルとして自動取得し、その中のフィールドをキー値インデックスに解析します。自動設定に基づいて微調整を行い、最終的なインデックス設定情報を迅速に取得できます。

©2013-2026 Tencent Cloud. 著作権を所有しています。

ログアップロード関連

最終更新日：：2026-10-12 15:06:44

プロンプトパラメータエラーへの対処方法は?

このエラーは、APIまたはSDKを介してログをアップロードする際に、リクエスト入力パラメータ が正しく入力されていないことを示しています。パラメータが正しく入力されていることを確認してください。

認証失敗の原因としてどのようなものがありますか?

このエラーは、ログをアップロードする際に認証エラーが発生したことを示しています。この種の問題は、通常、以下のいずれかの原因によって発生します。

エラー原因	解決方法
キーが存在しません。	コンソールでキーが削除または無効化されていないか確認してください。 ステータスが正常な場合は、キーが正しく入力されているか確認し、前後にスペースがないことに注意してください。ここをクリックすると、キー情報を確認できます。
署名エラー	署名の計算に誤りがあります。呼び出し方法の署名方法を参照して、署名の計算プロセスを確認してください。
署名の有効期限切れ	呼び出し方法の署名方法ドキュメントを参照して、署名を再計算してください。
リクエストが承認されていません。	ログアップロード権限がありません。CAMコンソールに移動し、アカウントにCLSログアップロード権限を追加してください。
キーの形式が正しくありません。	キーの形式が正しくありません。ここをクリックして、キー情報を確認できます。
その他	上記の原因をすべて除外してもエラーが継続する場合は、オンラインカスタマーサービス に連絡してチケットを送信してください。

アップロードログのサイズ超過への対処方法は?

単一のログアップロードリクエストにおけるログサイズが制限を超えています。以下の仕様制限に従ってログアップロードサイズを調整してください。

制限項目	説明

©2013-2026 Tencent Cloud. 著作権を所有しています。

ログをアップロードします。	1 つの pb パッケージ内の logGroup は 10 個を超えることはできません。
	1 つの pb パッケージ内の logGroup に含まれるログエントリ数は最大 10000 件で、少なくとも 1 件含まれます。
	log 内の単一 value の最大サイズは 1MB です。
	1 つの pb パッケージ内の logGroup 部分にあるすべての Value のサイズの合計は最大 5MB です。
	1 回のアップロードリクエストのパケット本体は、圧縮前のサイズが 6MB を超えることはできません。

フロー制御や頻度制御が発生するのはなぜですか?

このエラーは、以下の仕様超過が存在することを示しています。

制限項目	説明
書き込み頻度制御	単一ログトピックパーティションの書き込みリクエスト制限：500QPS。
書き込みフロー制御	単一ログトピックパーティションの書き込みトラフィック制限：5MB/s。

ログアップロードの頻度とトラフィックを減らすことをお勧めします。ログアップロードの頻度やトラフィックを変更したくない場合は、ログトピックで 自動分割を有効にする ことをお勧めします。

アップロードリクエストエラーへの対処方法は?

このエラーは、他のアップロードエラーが存在することを示しています。 オンラインカスタマーサービス に連絡して、チケットを送信しフィードバックしてください。

©2013-2026 Tencent Cloud. 著作権を所有しています。

収集設定関連

最終更新日：：2026-10-12 15:06:45

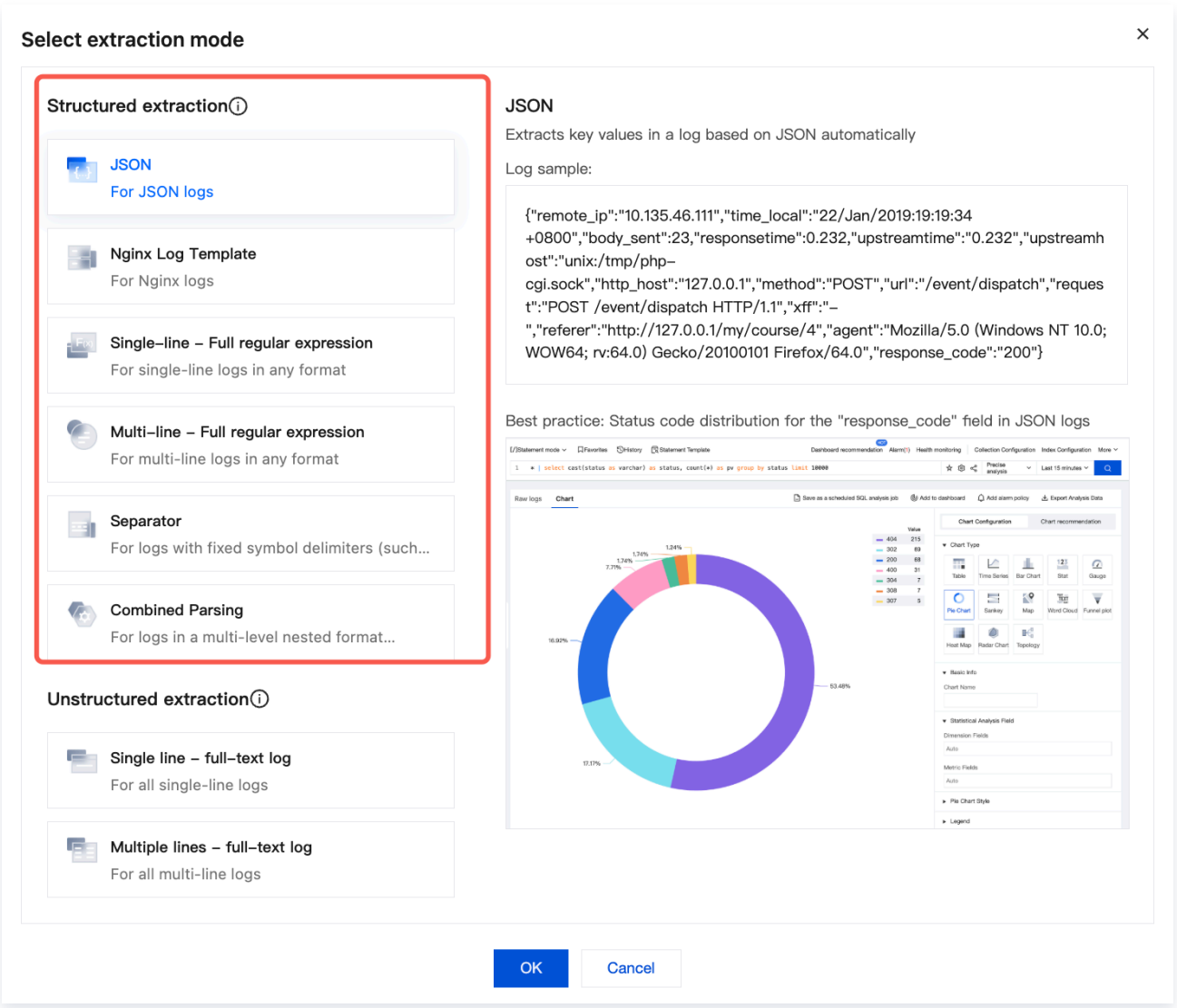
非構造化抽出モードと構造化抽出モードの違い?

非構造化抽出モードとは、収集設定において抽出モードを単一行全文または複数行全文に設定することを指します。このタイプの抽出モードはログをフォーマット解析せず、全文収集を行います。**この抽出モードでは、ログを収集した後は、最もシンプルな全文検索、ログ件数統計、ログ件数アラートのみ実行できます。**
CLSは、ログ内容の特定フィールドに基づくより強力な検索分析、可視化、監視アラートをサポートしています。この機能は、収集したログのフォーマット解析に依存します。つまり、収集設定で**構造化抽出モード**を選択します。**ログの出力形式が統一されている場合は、構造化抽出モード（無料）を設定して、ログ分析エクスペリエンスを最大限に向上させることをお勧めします。**

構造化抽出モードをどのように設定しますか?

1. CLS にログインし、左側のナビゲーションバーで**ログトピック**をクリックして、ログトピック管理ページに移動します。
2. 対象のログトピックを見つけ、**ログトピック名**をクリックしてログトピック設定ページに移動します。
3. **収集設定**タブを選択し、**LogListener収集設定**で抽出モードが単行全文または複数行全文の収集設定を見つけ、クリックして表示し、収集設定詳細ページに移動します。
4. 収集設定詳細ページで、**設定を変更**をクリックして収集設定編集ページに移動します。
5. **抽出モード**設定項目を見つけ、ログ形式に応じて**変更**をクリックし、対応する構造化抽出モードを選択します。

©2013-2026 Tencent Cloud. 著作権を所有しています。



6. 構造化抽出モード

単一行–完全正規表現形式

単一行完全正規表現形式は通常、構造化されたログの処理に使用されます。これは、1つの完全なログから正規表現方式で複数のkey–valueを抽出するログ解析モードを指します。
あるログの元のデータが以下の通りであると仮定します：

```
10.135.46.111 - - [22/Jan/2019:19:19:30 +0800] "GET /my/course/1
HTTP/1.1" 127.0.0.1 200 782 9703 "http://127.0.0.1/course/explore?
filter%5Btype%5D=all&filter%5Bprice%5D=all&filter%5BcurrentLevelId%5
D=all&orderBy=studentNum" "Mozilla/5.0 (Windows NT 10.0; WOW64;
rv:64.0) Gecko/20100101 Firefox/64.0"  0.354 0.354
```

設定されたカスタム正規表現は以下の通りです：

©2013-2026 Tencent Cloud. 著作権を所有しています。

```
(\S+)[^\[]+(\[[^:]+:\d+:\d+:\d+\s\S+)\s"
(\w+)\s(\S+)\s([^"]+)"\s(\S+)\s(\d+)\s(\d+)\s(\d+)\s"([^"]+)"\s"
([^"]+)"\s+(\S+)\s(\S+).*
```

システムが `()` キャプチャグループに基づいて対応するkey-valueを抽出した後、各グループのkey名を以下のようにカスタマイズできます:

```
body_bytes_sent: 9703
http_host: 127.0.0.1
http_protocol: HTTP/1.1
http_referer: http://127.0.0.1/course/explore?
filter%5Btype%5D=all&filter%5Bprice%5D=all&filter%5BcurrentLevelId%5
D=all&orderBy=studentNum
http_user_agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:64.0)
Gecko/20100101 Firefox/64.0
remote_addr: 10.135.46.111
request_length: 782
request_method: GET
request_time: 0.354
request_url: /my/course/1
status: 200
time_local: [22/Jan/2019:19:19:30 +0800]
upstream_response_time: 0.354
```

複数行-完全正規表現形式

複数行-完全正規表現モードは、ログテキスト内の1つの完全なログデータが複数行にまたがる場合（例えばJavaプログラムログ）に適用されます。正規表現によって複数のkey-valueキー値として抽出できるログ解析モードです。key-valueを抽出する必要がない場合は、複数行全文形式を参照して設定してください。複数行-完全正規表現モードを設定する際は、最初にログサンプルを入力し、次にカスタム正規表現を定義する必要があります。設定が完了すると、システムは正規表現内のキャプチャグループに基づいて対応するkey-valueを抽出します。
あるログの元のデータが以下の通りであると仮定します:

```
[2018-10-01T10:30:01,000] [INFO] java.lang.Exception: exception
happened
```

©2013-2026 Tencent Cloud. 著作権を所有しています。

```
    at TestPrintStackTrace.f(TestPrintStackTrace.java:3)
    at TestPrintStackTrace.g(TestPrintStackTrace.java:7)
    at TestPrintStackTrace.main(TestPrintStackTrace.java:16)
```

設定されたカスタム正規表現は以下の通りです：

```
\[\d+-\d+-\w+:\d+:\d+,\d+]\s\[\w+]\s.*
```

先頭行の正規表現は以下の通りです：

```
\[(\d+-\d+-\w+:\d+:\d+,\d+)\]\s\[(\w+)\]\s(.*)
```

抽出されたkeyに基づき、CLSに収集されたデータは以下の通りです：

```
time:  2018-10-01T10:30:01,000`
level:  INFO`
msg: java.lang.Exception: exception happened
    at TestPrintStackTrace.f(TestPrintStackTrace.java:3)
    at TestPrintStackTrace.g(TestPrintStackTrace.java:7)
    at TestPrintStackTrace.main(TestPrintStackTrace.java:16)
```

JSON形式

JSON形式のログでは、最上位層のkeyが対応するフィールド名として自動的に抽出され、最上位層のvalueが対応するフィールド値として自動的に抽出されます。この方法でログ全体が構造化処理され、各完全なログは改行文字\\nを終了識別子とします。
あるJSONログの元のデータが以下の通りであると仮定します：

```
{"remote_ip":"10.135.46.111","time_local":"22/Jan/2019:19:19:34
+0800","body_sent":23,"responsetime":0.232,"upstreamtime":"0.232","u
pstreamhost":"unix:/tmp/php-
cgi.sock","http_host":"127.0.0.1","method":"POST","url":"/event/disp
atch","request":"POST /event/dispatch HTTP/1.1","xff":"-
","referer":"http://127.0.0.1/my/course/4","agent":"Mozilla/5.0
(Windows NT 10.0; WOW64; rv:64.0) Gecko/20100101
Firefox/64.0","response_code":"200"}
```

©2013-2026 Tencent Cloud. 著作権を所有しています。

CLSによる構造化処理後、このログは以下のようになります：

```
agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:64.0) Gecko/20100101
Firefox/64.0
body_sent: 23
http_host: 127.0.0.1
method: POST
referer: http://127.0.0.1/my/course/4
remote_ip: 10.135.46.111
request: POST /event/dispatch HTTP/1.1
response_code: 200
responsetime: 0.232
time_local: 22/Jan/2019:19:19:34 +0800
upstreamhost: unix:/tmp/php-cgi.sock
upstreamtime: 0.232
url: /event/dispatch
xff: -
```

区切り文字形式

区切り文字ログとは、1つのログデータを指定された区切り文字に基づいてログ全体を構造化処理できる形式です。各完全なログは改行文字\\nを終了識別子とします。CLSで区切り文字形式のログを処理する際、分けられた各フィールドに一意のkeyを定義する必要があります。
あるログの元のデータが以下の通りであると仮定します：

```
10.20.20.10 ::: [Tue Jan 22 14:49:45 CST 2019 +0800] ::: GET
/online/sample HTTP/1.1 ::: 127.0.0.1 ::: 200 ::: 647 ::: 35 :::
http://127.0.0.1/
```

ログ解析の区切り文字を `:::` に指定すると、このログは8つのフィールドに分割され、これら8つのフィールドに一意のkeyが定義されます。以下に示します：

```
IP: 10.20.20.10 -
bytes: 35
host: 127.0.0.1
length: 647
referer: http://127.0.0.1/
```

©2013-2026 Tencent Cloud. 著作権を所有しています。

```
request: GET /online/sample HTTP/1.1
status: 200
time: [Tue Jan 22 14:49:45 CST 2019 +0800]
```

©2013-2026 Tencent Cloud. 著作権を所有しています。

収集関連
マシングループに関するよくある質問

最終更新日：：2026-10-12 15:06:44

IPによるマシン追加が反映されない

1. IPに対応するマシンにLogListenerがインストールされているかどうかを確認します。インストール手順については、LogListenerのインストールとデプロイ を参照してください。
2. 収集セルフチェックツールの使用方法 を参照して、LogListenerに異常がないかどうかを確認してください。
3. マシングループに追加されたIPがLogListenerによって認識されたIPと一致しているかどうかを確認します。以下のコードを実行して、LogListenerが検出したIPを確認できます。

Linux

- LogListener バージョンが3.4.0以上の場合：

```
//ハートビートと設定を確認します。
systemctl check loglistener
```

```
[root@VM-32-2-centos ~]# systemctl check loglistener
active
[root@VM-32-2-centos ~]#
```

```
//マシンのIPを確認します。
cd /opt/loglistener/ && grep -n 'agent_ip' conf/loglistener.yaml
```

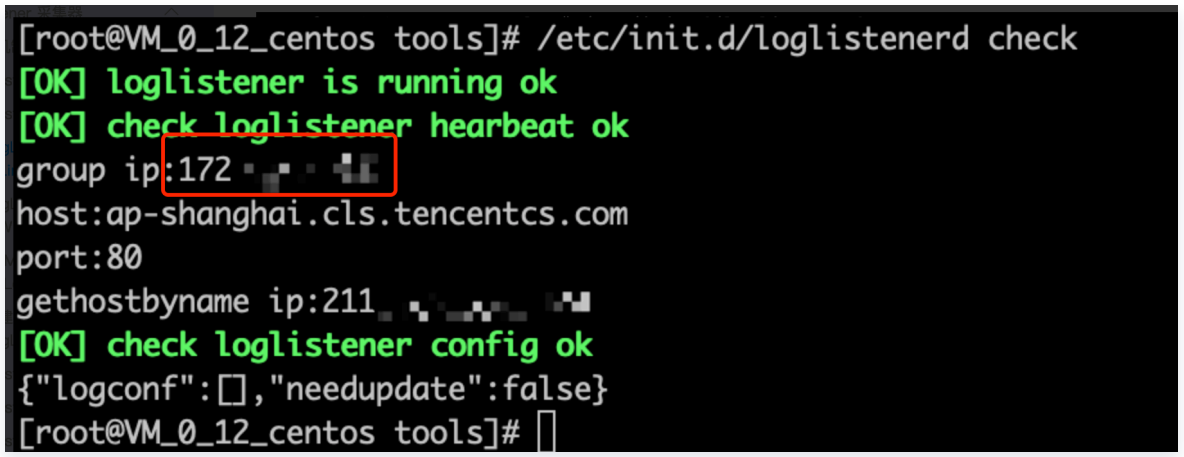
```
[root@VM-32-2-centos ~]# cd /opt/loglistener && grep -n 'agent_ip' conf/loglistener.yaml
3:  agent_ip: 10.
[root@VM-32-2-centos loglistener]#
```

- LogListener バージョンが3.4.0未満の場合：

```
/etc/init.d/loglistenerd check
```

返却データ内で、`group ip` を確認することで、LogListenerが認識したIPを確認できます。以下の図の通りです：

©2013-2026 Tencent Cloud. 著作権を所有しています。



Windows

インストールパス `C:\Program Files (x86)\Tencent\LogListener` を例に、管理者としてWindows PowerShellを実行し、インストールパスで以下のコマンドを実行してLogListenerのハートビートと設定を確認します：

```
.\loglistener_work.exe check
```

返却データ内で、 `group_id` を確認することで、LogListenerが認識したIPを確認できます。以下の図の通りです：



マシン識別子によるマシン追加が反映されない

1. 対象マシンにLogListenerがインストールされているかどうかを確認します。インストール手順については、LogListenerのインストールとデプロイ を参照してください。
2. 収集セルフチェックツールの使用方法 を参照して、LogListenerに異常がないかどうかを確認してください。
3. LogListenerのマシン識別子が、マシングループに設定されているマシン識別子と一致しているかどうかを確認します。以下の手順を参照して、LogListenerのマシン識別子を確認できます。

Linux

- LogListener バージョンが3.4.0以上の場合：インストールパス /opt/loglistener を例に、/opt/loglistener/conf パスで以下のコマンドを実行してLogListener設定ファイルを表示および設定

©2013-2026 Tencent Cloud. 著作権を所有しています。

できます。

```
grep -n 'agent_labels' loglistener.yaml
```

出力がない場合、現在のマシンにマシン識別子が設定されていないことを示します。以下の図の通りです：

```
[root@VM-32-2-centos conf]# grep -n 'agent_labels' loglistener.yaml
[root@VM-32-2-centos conf]#
```

agent_labelsはLogListenerのマシン識別子です。この識別子がマシングループに設定されているものと一致していることを確認してください。

- LogListener バージョンが3.4.0未満の場合：インストールパス `/usr/local/` を例に、`/usr/local/loglistener/etc` パスで以下のコマンドを実行してLogListener設定ファイルを表示および設定できます。

```
vim loglistener.conf
```

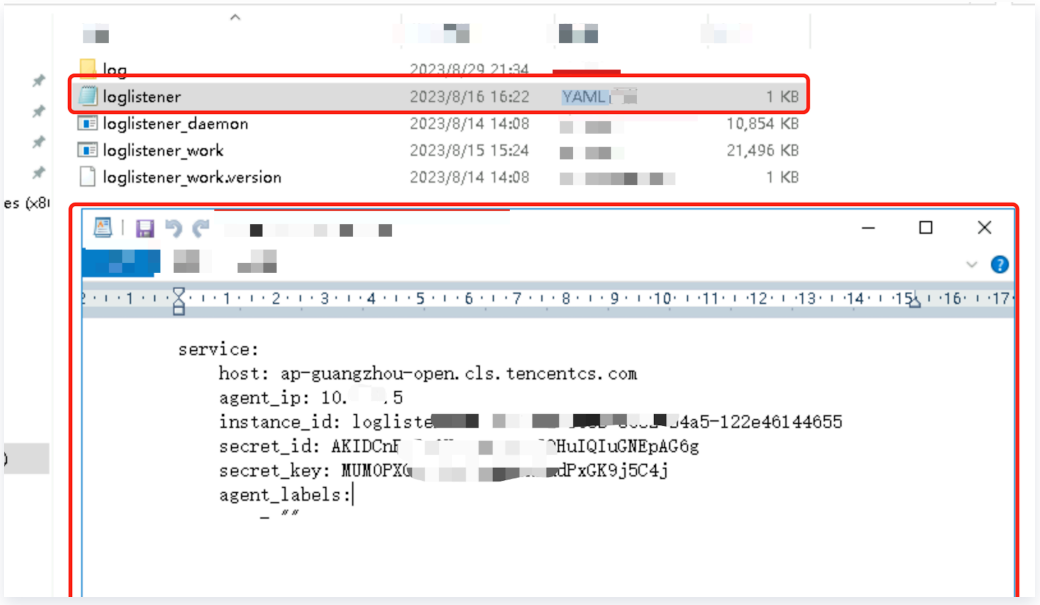
```
<root>
    proxy_host = ap-guangzhou-open.cls.tencentcs.com
    proxy_port = 
    secret_id = AK
    sec
    # This switch use to enable/disable secret_id/... ...ted, default false. (
true/false)
    encryption =
    group_ip = 10.0.0.9
    # define loglistener by labels, separated by ,
    group_label =
    instance_id = loglistener-d69d2c27-d2f4-d584-c45d-954cc83d8489
    pos_file = data/pos.dat
    checkpoint_cache_file = data/checkpoint_cache
    checkpoint_window_size = 1024
    # Max file break points. Warn: modify this value, history breaskpoints will lost.
    max_file_breakpoints = 8192
```

なお、group_labelはLogListenerのマシン識別子です。この識別子がマシングループに設定されているものと一致していることを確認してください。

Windows

インストールパス `C:\Program Files (x86)\Tencent\LogListener` を例に、インストールディレクトリでLogListener設定ファイル loglistener.yaml を見つけ、任意のエディタで開きます。以下の図の通りです：

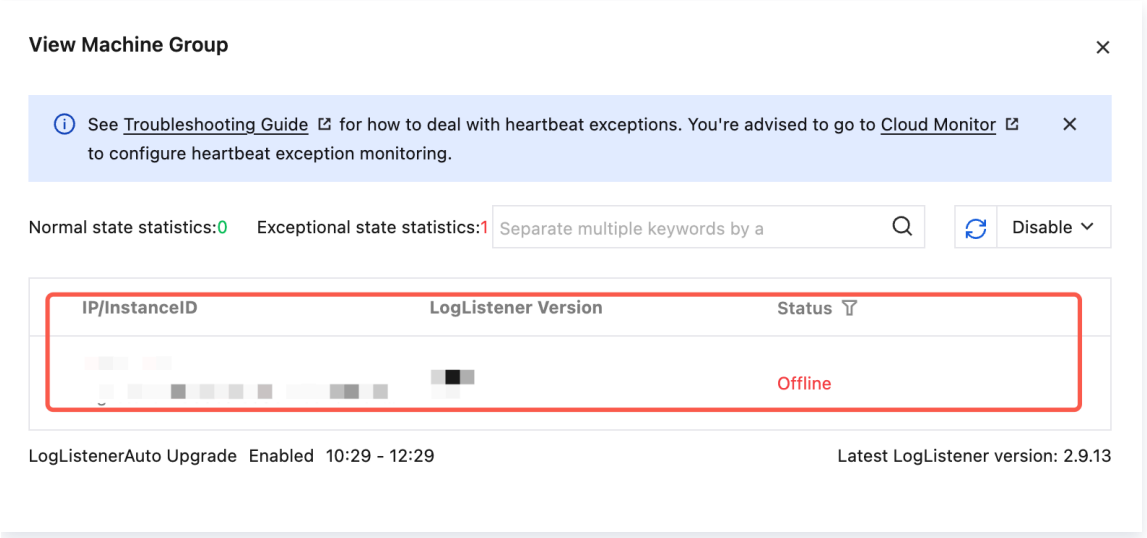
©2013-2026 Tencent Cloud. 著作権を所有しています。



agent_labelはLogListenerのマシン識別子です。この識別子がマシングループに設定されているものと一致していることを確認してください。

マシングループのマシン状態異常の問題

マシングループの設定が完了したら、マシングループ管理ページでマシングループ名をクリックすると、そのマシングループに関連付けられたマシンハートビートを確認できます。ステータスが正常であれば、マシンハートビートが正常に報告されていることを示します。正常でない場合（以下の図を参照）、そのマシン上のLogListenerに異常があることを示します。



ハートビート異常

ステータスがハートビート異常の場合、LogListenerとCLSバックエンド間の接続が切断されていることを示し、LogListenerが正常にログをアップロードできなくなります。以下の方法で接続切断の原因をさらに調査できます：

©2013-2026 Tencent Cloud. 著作権を所有しています。

> **説明**
> LogListener 2.2.4以降のバージョンにのみ適用されます。その他のバージョンについては、低バージョンLogListener異常状態のトラブルシューティング を参照してください。

1. LogListenerクイック診断ツールの使用

LogListenerクイック診断ツールを使用すると、LogListenerが起動しているか、ハートビートが正常か、設定取得が正常かを迅速に診断できます。コマンドラインで以下のコマンドを実行します:

- LogListener バージョンが3.4.0以上の場合:

```
systemctl check loglistener
```

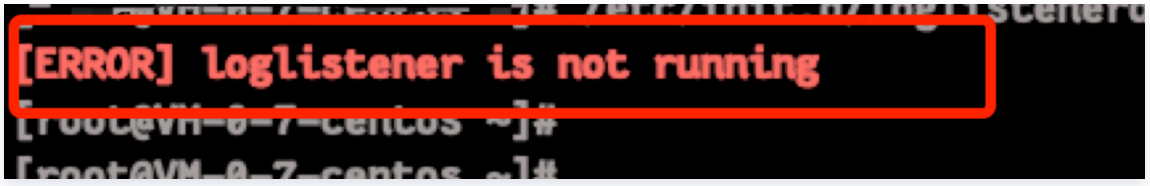
- LogListener バージョンが3.4.0未満の場合:

```
/etc/init.d/loglistenerd check
```

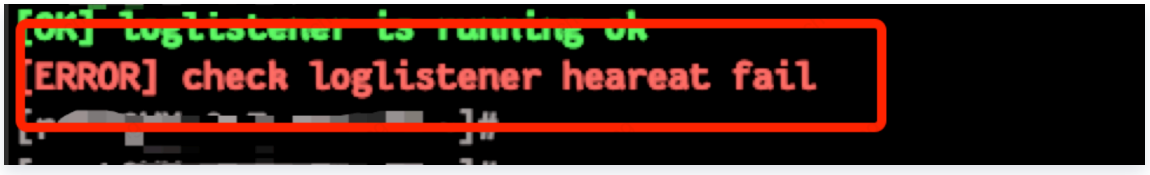
LogListenerが正常に動作している場合、診断ツールが返す結果は以下の図の通りです:

```
[root@VM-32-2-centos ~]#  systemctl check loglistener
active
```

- **LogListenerプロセス異常**: 以下の図に示すような `[ERROR] loglistener is not running` という文字が表示された場合、LogListenerが起動していないことを示します。systemctl start loglistenerを実行して起動してください。その他の操作コマンドについては、LogListenerのよく使う操作 を参照してください。



- **LogListenerハートビート異常**: 以下の図に示すような `[ERROR] check loglistener heareat fail` という文字が表示された場合、LogListenerのハートビートが異常であることを示します。



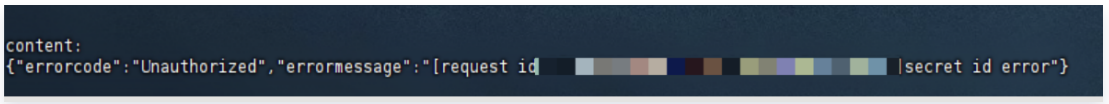
LogListenerのハートビート異常を引き起こす原因は多数あります。最も一般的なケースは以下の通りです:

  - ネットワーク異常です。以下のコマンドを実行してネットワーク環境が接続可能かどうかを確認してください。コマンド内の「cls domain name」はCLSサービスドメインです。利用可能なリージョン ドキュメントを参照して入力してください。

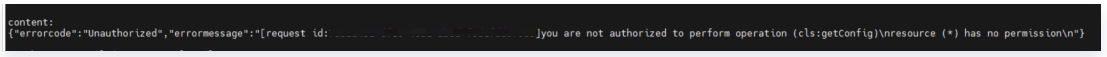
©2013-2026 Tencent Cloud. 著作権を所有しています。

```
telnet <cls domain name> 80
```

- 鍵情報が間違っています。LogListenerのインストールディレクトリに移動して `./bin/check` を実行し、末尾の出力内容が以下のように表示される場合、鍵情報が間違っていることを示します。



- 鍵に権限が不足しています。LogListenerのインストールディレクトリに移動して `./bin/check` を実行し、末尾の出力内容が以下のように表示される場合、鍵に権限が不足していることを示します。ポリシーテンプレートに従って報告権限を設定する必要があります。



2. マシングループのIP設定の確認

マシングループに追加されたIPアドレスが、LogListenerのインストールプロセス中に取得されたIPアドレスと一致しているかどうかを確認します。

1. LogListenerのインストールディレクトリに移動して、以下のコマンドを実行してLogListenerに設定されたIPアドレスを確認してください。

LogListenerバージョン3.4.0以上

> **説明:**
> 特に指定がない場合、LogListenerのインストールディレクトリは通常 `/opt/loglistener` です。

```
grep agent_ip conf/loglistener.yaml
```

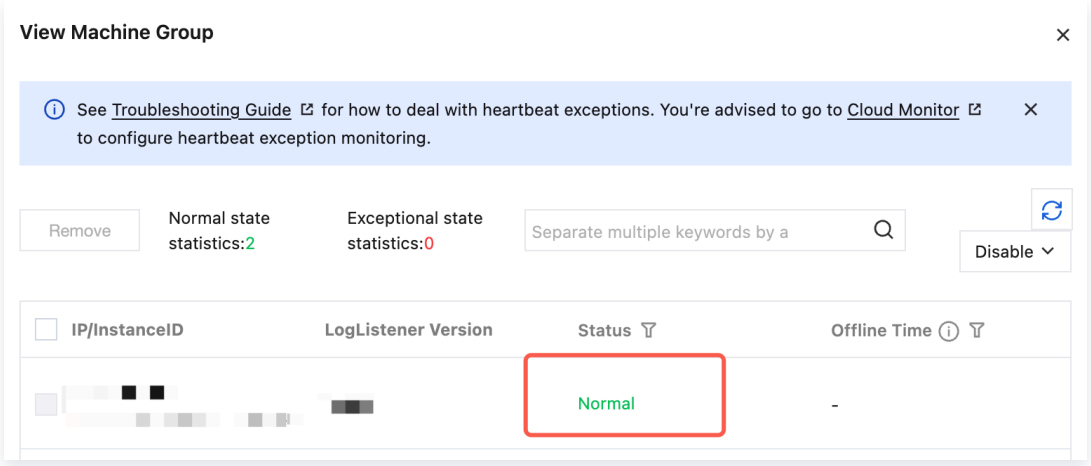
LogListenerバージョン3.4.0未満

> **説明:**
> 特に指定がない場合、LogListenerのインストールディレクトリは通常 `/usr/local/loglistener` です。

©2013-2026 Tencent Cloud. 著作権を所有しています。

```
grep group_ip etc/loglistener.conf
```

2. CLSコンソールにログインし、**マシングループ管理**をクリックし、マシングループに設定されたIPアドレスを確認します。マシングループに設定されたIPアドレスは、LogListenerが取得したIPアドレスと完全に一致している必要があります。



ディレクトリ上限超過

ステータスがディレクトリ制限超過の場合、LogListenerの制限を超えた部分のディレクトリのログが収集できなくなります。以下の方法で修復できます：

1. 以下のコマンドを実行して、現在のLogListenerに関連付けられた収集設定を確認してください。

```
//LogListener バージョンが3.4.0以上の場合
systemctl check loglistener

//LogListener バージョンが3.4.0未満の場合
 /etc/init.d/loglistenerd check
```



2. 上記の返却結果において、logconfig配列には現在のLogListenerのすべての収集設定が含まれています。各収集設定について、wildpathが大量の収集不要なディレクトリを曖昧にヒットする可能性があるかどうかを確認できます。例えば、`/root/**/error.log` のようなルートディレクトリの曖昧なパスです。

©2013-2026 Tencent Cloud. 著作権を所有しています。

3. 最適化対象の収集設定を特定した後、ステップ1の返却データからその収集設定に関連付けられたtopicidを確認し、そのtopicidに基づいてCLSコンソールで対象のログトピックを見つけ、その収集設定を最適化または削除してください。

ファイル上限超過

ステータスがファイル制限超過の場合、LogListenerが監視する収集ファイル数が仕様制限の10000を超えていることを示します。これにより、LogListenerは制限を超えたファイルのログを収集できなくなります。以下の方法で修復できます：

1. 以下のコマンドを実行して、現在のLogListenerに関連付けられた収集設定を確認してください。

```
//LogListener バージョンが3.4.0以上の場合
systemctl check loglistener

//LogListener バージョンが3.4.0未満の場合
 /etc/init.d/loglistenerd check
```



2. 上記の返却結果において、logconfig配列には現在のLogListenerのすべての収集設定が含まれています。各収集設定について、wildpathが大量の収集不要なファイルを曖昧にヒットする可能性があるかどうかを確認できます。例えば、`/root/**/*.log` のような、ルートディレクトリから任意の名前のログファイルを曖昧にマッチングするパスです。
3. 最適化対象の収集設定を特定した後、ステップ1の返却データからその収集設定に関連付けられたtopicidを確認し、そのtopicidに基づいてCLSコンソールで対象のログトピックを見つけ、その収集設定を最適化または削除してください。

CPU上限超過

ステータスがCPU制限超過の場合、LogListenerが占有するCPUが事前に設定されたしきい値を超えていることを示します。以下の方法で調査と修復を行うことができます：

最適化対象の収集ディレクトリ

1. 以下のコマンドを実行して、現在のLogListenerに関連付けられた収集設定を確認してください。

```
//LogListener バージョンが3.4.0以上の場合
systemctl check loglistener
```

©2013-2026 Tencent Cloud. 著作権を所有しています。

```
//LogListener バージョンが3.4.0未満の場合
/etc/init.d/loglistenerd check
```



2. 上記の返却結果において、logconfig配列には現在のLogListenerのすべての収集設定が含まれています。各収集設定について、wildpathが大量の収集不要なファイルを曖昧にヒットする可能性があるかどうかを確認できます。例えば、`/root/**/*.log` のような、ルートディレクトリから任意の名前のログファイルを曖昧にマッチングするパスです。
3. 最適化対象の収集設定を特定した後、ステップ1の返却データからその収集設定に関連付けられたtopicidを確認し、そのtopicidに基づいてCLSコンソールで対象のログトピックを見つけ、その収集設定を最適化または削除してください。

正規表現の最適化

1. 以下のコマンドを実行して、現在のLogListenerに関連付けられた収集設定を確認してください。

```
//LogListener バージョンが3.4.0以上の場合
systemctl check loglistener

//LogListener バージョンが3.4.0未満の場合
 /etc/init.d/loglistenerd check
```



2. 上記の返却結果において、logconfig配列には現在のLogListenerのすべての収集設定が含まれています。fullregexまたはmulti_fullregexフィールドを持つ各収集設定について、正規表現が過度に複雑でないかどうかを確認できます。
3. 最適化対象の収集設定を特定した後、ステップ1の返却データからその収集設定に関連付けられたtopicidを確認し、そのtopicidに基づいてCLSコンソールで対象のログトピックを見つけ、その収集設定を最適化または削除してください。

©2013-2026 Tencent Cloud. 著作権を所有しています。

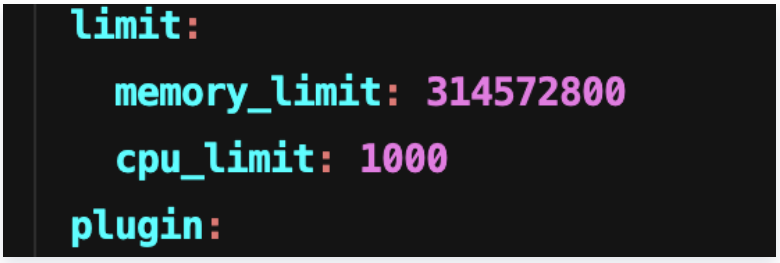
LogListenerのCPU使用率制限の引き上げ

LogListenerバージョン3.4.0以上

1. LogListenerのインストールディレクトリがopt/loglistenerである場合を例に、以下のコマンドを実行してLogListener設定ファイルを開きます：

```
vim conf/loglistener.yaml
```

2. LogListener設定ファイルでcpu_limitを見つけ、必要に応じてCPU使用率の制限を引き上げてください（業務プロセスのリソースを確保した上で、500/1000ずつ段階的に引き上げることを推奨します）。下図の通りです：



3. 設定完了後、保存してLogListenerを再起動してください。

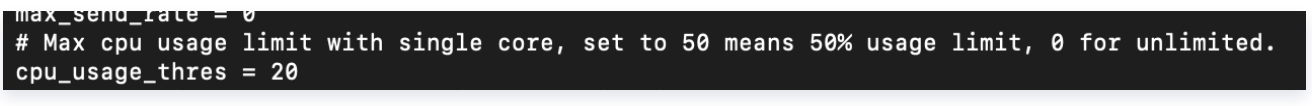
```
systemctl restart loglistener
```

LogListenerバージョン3.4.0未満

1. LogListenerのインストールディレクトリが `/usr/local/loglistener` である場合を例に、以下のコマンドを実行してLogListener設定ファイルを開きます：

```
vim etc/loglistener.conf
```

2. LogListener設定ファイルで `cpu_usage_thres` を見つけ、必要に応じてCPU使用率の制限を引き上げてください（業務プロセスのリソースを確保した上で、500/1000ずつ段階的に引き上げることを推奨します）。下図の通りです：



3. 設定完了後、保存してLogListenerを再起動してください。

©2013-2026 Tencent Cloud. 著作権を所有しています。

```
systemctl restart loglistenerd
```

CPUリソースクォータの引き上げ

K8s環境では、`DaemonSet:tke-log-agent`配下の`Pod: loglistener`のCPU割り当てが十分であることを確認してください。

メモリ上限超過

ステータスがメモリ制限超過の場合、LogListenerが占有するメモリが事前に設定されたしきい値を超えていることを示します。以下の方法で修復できます。

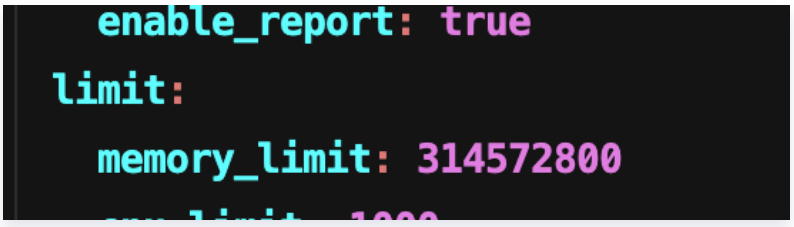
LogListenerバージョン3.4.0以上

1. LogListenerのインストールディレクトリがopt/loglistenerである場合を例に、以下のコマンドを実行してLogListener設定ファイルを開きます。

```
vim conf/loglistener.yaml
```

2. LogListener設定ファイルで`max_mem`（単位：Bytes）を見つけ、必要に応じてメモリ使用量の制限を引き上げてください。下図の通りです：

> **説明：**
> 業務プロセスのメモリリソースが十分であり、業務の安定性に影響を与えないことを確認した上で、現在の値の1～2倍を目安に段階的に引き上げることを推奨します。



3. 設定完了後、保存してLogListenerを再起動してください。

```
systemctl restart loglistener
```

©2013-2026 Tencent Cloud. 著作権を所有しています。

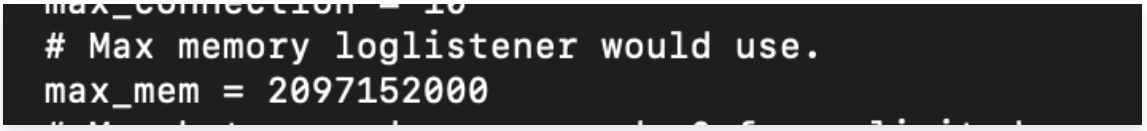
LogListenerバージョン3.4.0未満

1. LogListenerのインストールディレクトリが `/usr/local/loglistener` である場合を例に、以下のコマンドを実行してLogListener設定ファイルを開きます。

```
vim  etc/loglistener.conf
```

2. LogListener設定ファイルで `max_mem` （単位：Bytes）を見つけ、必要に応じてメモリ使用量の制限を引き上げてください。下図の通りです：

> **説明：**
> 業務プロセスのメモリリソースが十分であり、業務の安定性に影響を与えないことを確認した上で、現在の値の1～2倍を目安に段階的に引き上げることを推奨します。



3. 設定完了後、保存してLogListenerを再起動してください。

```
systemctl restart loglistenerd
```

認証失敗

キーの有効性確認

ステータスが認証失敗の場合、LogListenerに設定されたキーが誤っているか、すでに無効になっていることを示します。以下の方法で修復できます。

LogListenerバージョン3.4.0以上

キーはローカル設定ファイルに平文で保存されなくなりました。それでも認証失敗が発生する場合、通常は現在のインスタンスで使用しているキーが無効になっているか、権限が異常であるか、設定が正しく配信されていないことを示します。コンソールキーとマシングループ設定が有効かどうかを確認し、必要に応じてLogListenerを再インストールしてください。

LogListenerバージョン3.4.0未満

©2013-2026 Tencent Cloud. 著作権を所有しています。

1. LogListenerのインストールディレクトリが `/usr/local/loglistener` である場合を例に、以下のコマンドを実行してLogListener設定ファイルを開きます。

```
vim  etc/loglistener.conf
```

2. LogListener設定ファイルで `secret_id` と `secret_key` を見つけ、正しく有効かどうかを判断してください。無効な場合は正しいキー情報に変更してください。下図の通りです：



3. 設定完了後、保存して LogListenerを再起動してください 。

```
 systemctl restart loglistenerd
```

サーバー時刻の正確性

サーバー時間が正確であることを確認してください。そうでない場合、認証失敗を引き起こす可能性があります。

1. Linuxサーバーは以下の方法で確認できます：

```
date
timedatectl status
```

以下の情報を重点的に確認してください：

- Local time：現在のローカル時間が正しいかどうか。
- Time zone：タイムゾーンがサーバー所在地域と一致しているかどうか。例えば、中国本土のリージョンでは通常 Asia/Shanghai です。
- System clock synchronized：yesかどうか。
- NTP service：activeかどうか。

2. タイムゾーンが正しくない場合は、以下のコマンドを実行してタイムゾーンを変更できます（中国本土リージョンを例とします）：

```
sudo timedatectl set-timezone Asia/Shanghai
```

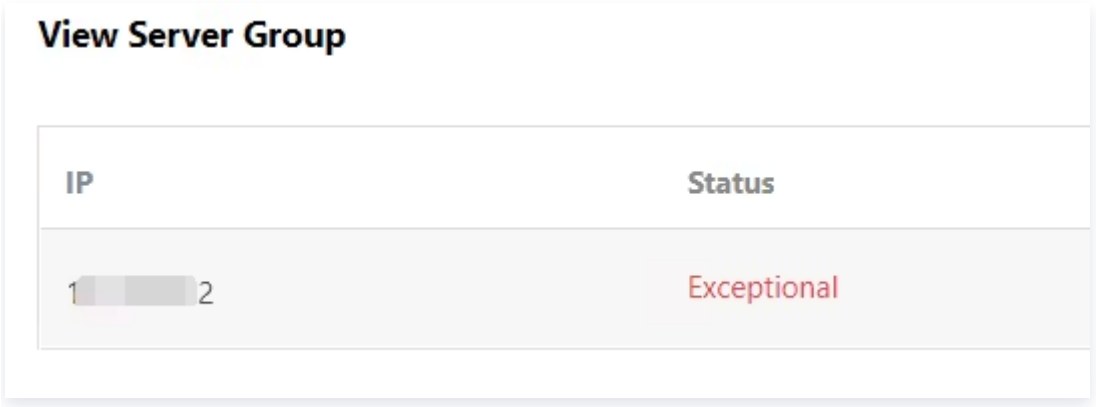
©2013-2026 Tencent Cloud. 著作権を所有しています。

Machine Group Exception

最終更新日：：2024-01-20 17:11:57

Error Description

When the machine group is configured, LogListener may have an exception, such as disconnection from the CLS server and log upload failure. In this case, the machine group is exceptional, as shown below:



Troubleshooting Directions

> **Note:**
> These troubleshooting steps only apply to LogListener 2.2.4 or later. If you're using an earlier version, see Troubleshooting Earlier LogListener Versions.

1. Use the LogListener diagnostic tool

This tool helps you quickly check the LogListener operation, heartbeat and configuration.
Run the following CLI commands.

```
/etc/init.d/loglistenerd check
```

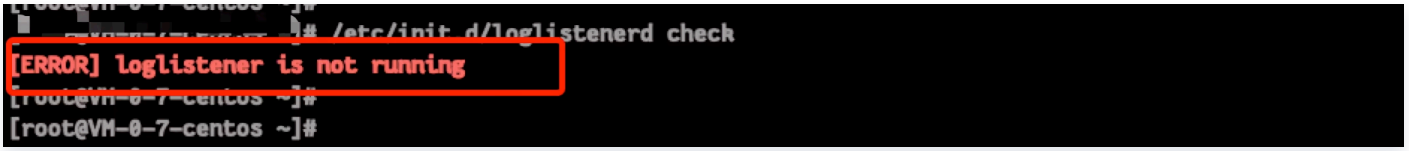
The following output indicates that LogListener is running properly.

```
[root@VM_30_69_centos etc]# sudo /etc/init.d/loglistenerd check
[OK] loglistener is running ok
[OK] check loglistener hearbeat ok
group ip:
host:ap-chengdu.cls.myqcloud.com
port:80
gethostbyname ip:
[OK] check loglistener config ok
{"logconf":[],"needupdate":false}
```

©2013-2026 Tencent Cloud. 著作権を所有しています。

LogListener process exception

If the result returns “[ERROR] loglistener is not running” as shown in the following figure, it indicates that LogListener is not started. Run the `/etc/init.d/loglistenerd start` command to start it. For more information about the operation commands, see Using LogListener.



LogListener heartbeat exception

If the result returns “[ERROR] check loglistener heartbeat fail”, it indicates that LogListener has a heartbeat exception.
Many causes can lead to a LogListener heartbeat exception. Possible causes include:

- Network error

```
telnet <cls domain name> 80
```

Check the network connectivity. For more information about the CLS domain name, see Available Regions.

- Incorrect key

To check the LogListener key, access the LogListener installation directory and run the following command.

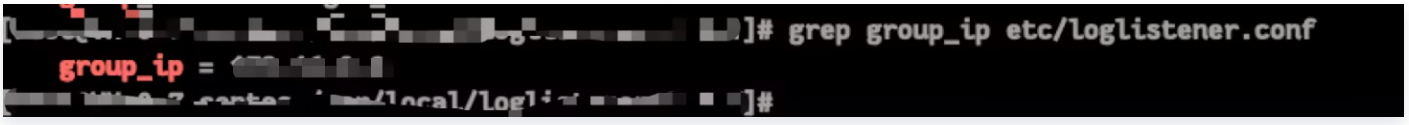
```
grep secret etc/loglistener.conf
```



2. Check for the IP address of the machine group

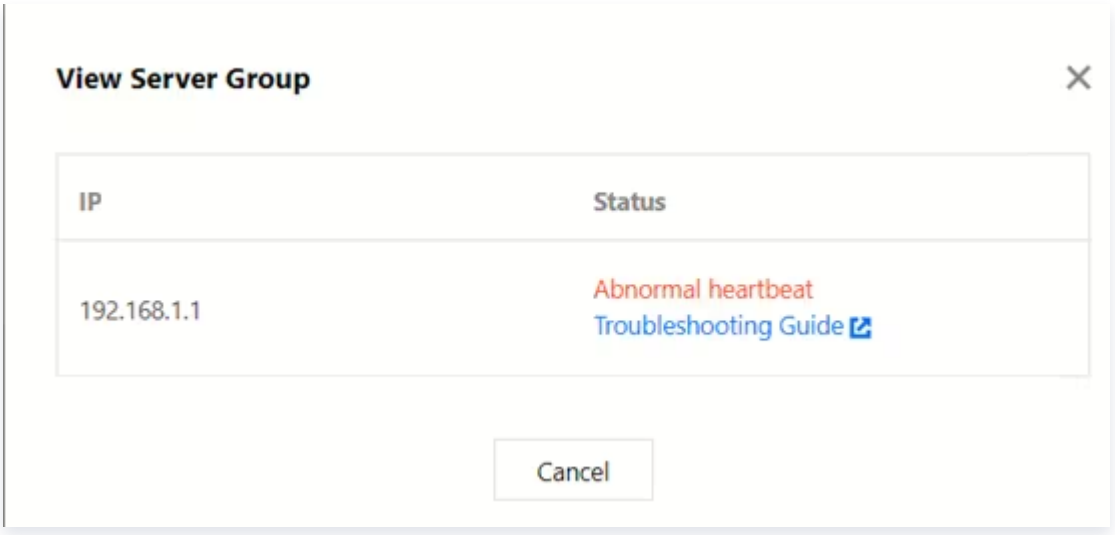
Check that the IP address added to the machine group is the one configured on LogListener during installation. Run the following command to check the IP address configured on LogListener.

```
grep group_ip etc/loglistener.conf
```



©2013-2026 Tencent Cloud. 著作権を所有しています。

Log in to the CLS console, and select **Server Group** in the left sidebar. On the **Server Group Management** page, view and verify that the IP address of the machine group is the same as that configured on LogListener.



©2013-2026 Tencent Cloud. 著作権を所有しています。

LogListenerに関するよくある質問

最終更新日：：2026-10-12 15:06:44

単一ファイルが複数のトピックへの報告をサポートしない理由は何ですか?

LogListener収集プログラムのポリシーは、単一ファイルは1つのトピックにのみアップロードできるというものです。
例えば、topicAとtopicBという2つのファイルがあり、これらの2つのファイルに対して次のように設定します。

- topicAの収集パスを次のように設定します：/data/log/**/*.log
- topicBの収集パスを次のように設定します：/data/log/test/**/*.log、/data/log/**/test*.log、/data/log/**/*.log、またはtopicAの収集パスと類似するパスです。

このシナリオの構成は、2つの収集パスが交差するファイルに対応しますが、データはそのうちの1つのトピックにのみアップロードされます。したがって、異なるログトピックには異なる業務タイプのログを割り当て、収集構成パスを設定する際には、できるだけ正確に情報を構成することをお勧めします。特定のファイルを異なるトピックにアップロードする必要がある場合は、ソフトリンクを使用して実現できます。同じ収集対象に対して異なるソフトリンクを作成し、異なるトピックでそれぞれ異なるソフトリンクパス/ファイルを収集します。

収集パスの設定はどのように行いますか?

現在の収集パスの構成は、パスプレフィックス+「/**/」+ワイルドカードファイル名の形式です。例えば、/data/log + /**/ + *.log ==> /data/log/**/*.logです。
ワイルドカード収集パスを設定する際は、収集パス（プレフィックス部分）をできるだけ正確に設定する必要があります。これにより、収集エージェントはより効率的にサービスを提供できます。収集パスのプレフィックス部分の設定が不正確な場合、収集パスがマッチするパス数が膨大になり、収集エージェントが異常状態に陥り、動作不能になる可能性があります。
例えば、収集パスを//**/*.logに設定した場合、そのプレフィックス部分は「/」となり、この場合、収集プログラムはルートディレクトリ全体をスキャンするため、収集プログラムが動作できなくなります。

推奨されるログローテーション方法は何ですか?

ログのローテーションについては、ローテーション後のファイル名が収集ワイルドカードパスに含まれないようにすることを推奨します。
例えば、設定された収集パスは/var/log/xxxx/**/*.logで、収集対象のログはtest.logです。test.logがtest.2021-07-13.4.logにローテーションされた場合、LogListenerはtest.2021-07-13.4.logがtest.logのローテーションファイルであることを認識し、それに対して引き続きtest.logとしてマークします。したがって、LogListenerが保存するチェックポイントファイルには、test.2021-07-13.4.logというファイルの収集記録はありません。
そして、LogListenerが再起動した後、LogListenerは/var/log/xxxx/**/*.logに従ってファイルをスキャンし、test.2021-07-13.4.logファイルがマッチングルールに合致し、収集記録がなく、新しいファイルであることを検出し、その後再収集します。

©2013-2026 Tencent Cloud. 著作権を所有しています。

したがって、収集ワイルドカードパスがローテーションファイルにマッチしないようにすることをお勧めします。これにより、再起動後にローテーションファイルが再収集されるのを防ぎます。
私たちが推奨するログローテーションの方法は、test.logを収集する必要がある場合、ローテーション後のファイル名をtest.log.2021-07-13.xxxにすることをお勧めします。これにより、*.logにマッチするのを効果的に回避できます。

LogListenerのアップグレードに関する説明

LogListenerの反復プロセスにおいて、収集パスのインターフェースパラメータに変更が行われ、比較的古いバージョン（ver < 2.2.8）で設定された収集パスは、新しいバージョンではサポートされなくなりました。したがって、既存の古いバージョン（ver < 2.2.8）をアップグレードする必要がある場合、収集プログラムのアップグレード後に、コンソールでワイルドカードパス方式により収集パスを再度設定する必要があります。

LogListener収集設定で正規表現収集モードを使用する方法は?

コンソールで収集構成を設定する際に、正規表現関連の収集モードを選択した場合、コンソールには正規表現kv抽出ツールが提供されていますが、このツールは現時点では中国語コンテンツに対する正規表現の自動生成機能を提供していません。中国語テキストに対して正規表現抽出を行う必要がある場合は、正規表現を自分で作成し、コンソールで検証するか、他のサードパーティツールを使用して検証することができます。

LogListenerコレクタを初めて使用して接続する際に、ログがアップロードされない場合の対処方法は?

収集エージェントの設定が正しくないことが原因である可能性があります。よくあるケースは以下の通りです:

- 設定されたサーバードメインが一致しないため、収集エージェントは現在のリージョンの収集設定を取得できず、収集業務は実行されません。
- 収集エージェントはIPマシングループに追加されましたが、収集エージェントにはTagラベル情報も設定されているため、現在のリージョンで収集設定を取得できず、収集業務は実行されません。
- 収集エージェントに設定されたsecret ID/KEYが正しくないか、権限が不足しているため、ログをアップロードできません。
- 環境問題（例えばVPCサブネット内で外部ネットワークが有効になっていない場合）、クロスリージョンアップロードを設定しても有効にはならず、収集エージェントは実際にはローカルリージョンのサーバーと通信します。
- 通常このような場合は、収集エージェントがインストールされているマシンにログインし、収集エージェントのインストールディレクトリに移動して、`./bin/check`コマンドを実行し、以下の内容を確認できます:
- ドメイン名は正しいかどうか。
- ハートビート報告は正常かどうか。
- 収集設定は正しく取得されているかどうか。

マシングループの混在使用により収集が行われない場合の対処方法は?

現在、マシングループは2種類に分かれており、それぞれの使用方法は互いに独立しています:

©2013-2026 Tencent Cloud. 著作権を所有しています。

- IPマシングループでは、マシンのIPをコンソール上で手動でマシングループに追加する必要があります。対応するマシン上のloglistener.confのgroup_labelは空である必要があります。
- Tagマシングループでは、コンソールでマシングループのTagを設定し、対応するマシン上のloglistener.confのgroup_labelを同じTagに設定する必要があります。

上記の2つの使用方法は互換性がありません。混在して使用した場合、収集マシンは正しい収集設定を取得できず、収集が行われない現象が発生します。

LogListenerの収集ポリシーは何ですか?

複数のファイルがキューに並んでLogListenerによって収集される場合、先頭のファイルが最初に収集され、かつそのファイルが特定の時点でファイル末尾まで読み取られた場合にのみ先頭の位置を明け渡します。つまり、すべてのファイルが単位時間内に均等に収集リソースを利用できるわけではありません。
単一ファイルへの書き込み速度が常に収集速度を上回り、かつ収集速度が遅いためにファイルの最新位置まで常に消費できない場合、特定のファイルが長時間または継続的に収集リソースを占有し、その結果、他のファイルが収集プロセスに入れなくなることがあります。

Topicの収集詰まりが深刻な場合の対処方法は?

ある期間内に、単一ファイルの生成速度が収集速度を上回る場合、LogListenerは継続的にこの1つのファイルのみを収集し続け、他のファイルの収集がブロックされる状態に陥ります。

フィルタのルールは何ですか?

フィルターのルールは、マッチした場合に収集し、マッチしなかった場合に破棄するのではありません。マッチしなかったログについては、LogListenerは収集を行いません。

非root権限でLogListenerを起動する方法は?

ユーザーにはroot権限でインストールおよび起動することを推奨します。非root権限でLogListenerを使用する必要がある場合は、非root権限でのLogListenerの起動設定を参照できます。

LogListenerプロセスのコアバインド方法は?

tasksetツールを使用してコアバインドを実行します。`taskset -cp ${cpu number} ${pid>}` 。

LogListenerのメモリ使用量が高すぎる場合の対処とリソース使用の制御方法は?

- 最新のLogListenerバージョンへのアップグレードを推奨します。また、`memory_tight_mode = true` を設定してください。
- CGroupを使用してCPUとメモリの使用を制限します。

LogListenerはシンボリックリンク方式の収集をサポートしていますか?

LogListenerの2.3.0より前のバージョンは、シンボリックリンク方式のログファイルおよびNFS、CIFSなどの共有ファイルディレクトリ上のログファイルの監視をサポートしていません。2.3.0以降のバージョンでは、これらを

©2013-2026 Tencent Cloud. 著作権を所有しています。

すべてサポートしています。

LogListenerは複数のログトピックにデータをアップロードできますか?

- LogListenerは同一リージョン内の複数のログトピックに対してデータを収集できますが、異なるリージョンの複数のログトピックに対する収集はサポートしていません。
- 同じログファイルは1つのトピックにのみ収集できます。

LogListener初期化時にマシングループへ自動参加できますか?

タグマシングループをサポートします。参考ドキュメント: マシングループの管理 。

LogListenerのログアップロードポリシーは何ですか?

- キャッシュされたログ量が4Mを超えています。
- キャッシュされたログの件数が10000件を超えています。
- ファイルの末尾まで読み取ります。

LogListenerがサポートする最大パフォーマンスはどのくらいですか?

- 単行フルテキストログの最大処理能力は115MB/sです。
- 複数行フルテキストログの最大処理能力は40MB/sです。
- JSON形式ログの最大処理能力は25MB/sです。
- CSV形式ログ収集の最大処理能力は50MB/sです。
- 完全正規表現形式ログの最大処理能力は18MB/sです（正規表現の複雑さに関係します）。

サーバーのIPアドレス変更後、LogListenerはどのように適応すればよいですか?

- サーバーがマシン識別子でマシングループにバインドされている場合、ユーザーはLogListenerの設定を変更する必要はありません。サーバーIPを頻繁に変更する必要がある場合は、マシン識別子 を使用してマシングループを設定することをお勧めします。
- サーバーがIPアドレスでマシングループにバインドされている場合、ユーザーは以下の設定変更を行う必要があります:
  a. 設定ファイル内のgroup_ipオプションを変更し、変更後のIPアドレスを入力します。例えば:

```
sed -i '' "s/group_ip *=.*/group_ip = ${group_ip}/"
etc/loglistener.conf
```

  b. LogListenerを再起動します。

```
 /etc/init.d/loglistenerd restart
```

©2013-2026 Tencent Cloud. 著作権を所有しています。

c. IPマシングループを使用している場合は、CLSコンソールにログインし、左側のナビゲーションバーで**マシングループ管理**をクリックし、そのサーバーにバインドされているマシングループ設定を変更し、新しいIPで元のマシンIPアドレスを置き換えて確定します。

©2013-2026 Tencent Cloud. 著作権を所有しています。

LogListenerインストール異常問題

最終更新日：：2026-10-12 15:06:44

CLS Loglistenerのインストールおよび使用方法については、LogListenerインストールガイドドキュメントを参照してください。

考えられる原因

以下原因によりLoglistenerを正しくインストールできない場合があります：

1. カーネルバージョンは64ビットのみをサポートします。
2. インストール方法にエラーが発生しました。
3. 最新の機能はより高いバージョンのLoglistenerに依存します。

処理手順

1. カーネルバージョンを確認します。
   Loglistenerのインストールディレクトリにあるbinディレクトリ内の実行ファイルは、Linux 64ビットカーネルのみをサポートします。**uname -a**コマンドを実行し、カーネルバージョンがx86_64であるかどうかを確認してください。
2. インストール実行コマンドが正しいかどうかを確認します。
   詳細については、LogListenerインストールガイドドキュメントを参照して操作してください。
3. Loglistenerのバージョンを確認します。
   CLSの最新機能は新しいバージョンのLoglistenerに依存する可能性があります。新機能の使用時に異常が発生したことが確認された場合は、Loglistenerの最新バージョンをダウンロードしてください。LogListenerのダウンロードおよび詳細なインストール手順については、LogListenerインストールガイドを参照してください。
4. LogListenerが正常にインストールされたことを確認します。
5. LogListenerクイック診断ツールを使用して、LogListenerプロセス、ハートビート、および設定取得が正常かどうかを確認する方法を参照してください。

©2013-2026 Tencent Cloud. 著作権を所有しています。

コンテナログ収集に関するよくある質問

最終更新日：：2026-10-12 15:06:45

インストールとアップグレード関連

TKEクラスタにログ収集コンポーネントをデプロイする方法を教えてください。

1. TKEコンソールにログインします。
2. 左側のナビゲーションバーで、**運用保守機能管理**をクリックし、機能管理ページに入ります。
3. 操作対象のクラスタを見つけ、**設定**をクリックします。
4. 表示されたウィンドウで、**ログ収集**欄の**編集**をクリックします。
5. **ログ収集を有効にする**にチェックを入れ、**確定**をクリックします。
6. **閉じる**をクリックします。

TKEクラスタ内のログ収集コンポーネントをアップグレードする方法を教えてください。

1. TKEコンソールにログインします。
2. 左側のナビゲーションバーで、**運用保守機能管理**をクリックし、機能管理ページに入ります。
3. アップグレード可能なコンポーネントがあるクラスタを見つけ、**設定**をクリックします。
4. 表示されたウィンドウで、**ログ収集**欄の**編集**をクリックします。
5. **コンポーネントのアップグレード**をクリックします。

ネットワークと権限関連

TencentCloud APIのドメインに接続できない場合、どうすればよいですか?

TKE（Tencent Kubernetes Engine）のログ収集コンポーネントとCLS（Cloud Log Service）間で通信を行うコンポーネント cls-provisioner は、Tencent Cloud API ドメインを使用するため、ドメインへの接続性を確保する必要があります。コンポーネントのデプロイに失敗するなどの問題が発生し、ログに下図のようなエラーが表示されている場合、それはネットワークドメインが不通であることを示しています。



上図に示すように、cls-provisioner の起動に異常が発生しています。ログを確認すると、cls.internal.tencentcloudapi.com のドメインに接続できないことが分かりました。
Tencent Cloud上のマシンでは、デフォルトでTencent Cloudの内部および外部ネットワークのドメインはすべて接続可能です。通常、このような問題が発生する原因は、TKEノードのDNS設定が変更されたことです。以下の2つの方法で修復できます：

- TKEノードマシンのDNS設定にTencent CloudのデフォルトDNSを追加します。

©2013-2026 Tencent Cloud. 著作権を所有しています。

- ホストマシン上のDNSサーバーがcore-dnsである場合、corednsにTencent CloudのDNS解決を追加するだけで対応できます。

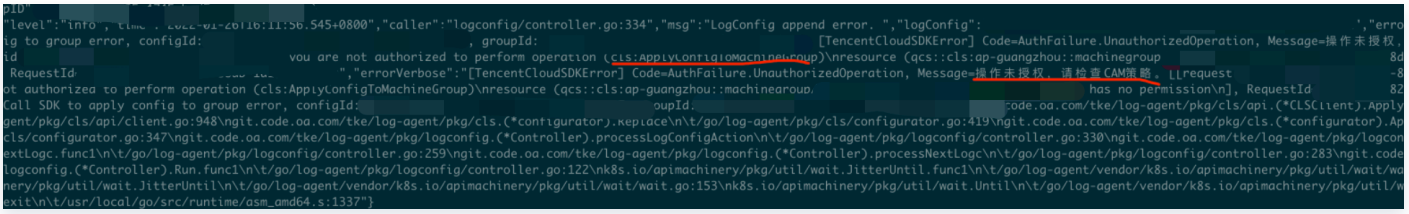
> **説明:**
> TKEクラスタでドメイン名が解決できない問題が発生した場合は、まずTKEノードのDNS設定を確認することをお勧めします。

CLSログアップロード用ドメインに接続できない場合、どうすればよいですか?

ログアップロードのドメインはTencentCloud APIのドメインとは異なります。ログアップロードのドメインは `<region>.cls.tencentcs.com`（外部ネットワーク）および `<region>.cls.tencentyun.com`（内部ネットワーク）です。詳細については、ドメイン ドキュメントを参照してください。
修復方法:
クラスタノードマシンでドメインへのアクセスを確立します。

cls-provisionerとCLS間の通信で未承認と表示された場合、どうすればよいですか?

cls-provisionerとCLSの通信では、通常、次のようなエラーが発生します:



修復方法:
TKEクラスタを作成したアカウントで、ポリシーを事前に設定します。つまり、TKE_QCSRole ロールにQcloudAccessForTKERoleInOpsManagementポリシーを関連付けます。

収集関連

CLSに収集されたログが切り捨てられた場合、どうすればよいですか?

一部のケースでは、ユーザーログの出力タイプは標準出力ですが、CLSに収集されたログが切り捨てられていることが判明します。これは、Dockerのデフォルトのログストレージであるjson-toolに1行あたりのログサイズの制限があり、16Kを超えるログは切り捨てられるためです。
修復方法:
ログ出力を変更し、1行あたりのログ出力が16Kを超えないようにしてください。

ログが重複して収集される場合、どうすればよいですか?

ユーザーがCLSコンソールで検索したところ、一部のログに重複収集が発生していることを確認しました。この場合、まずログ出力のパスを確認し、ログがPV/PVCで作成された永続化ストレージに出力されているかどうかを確認してください。

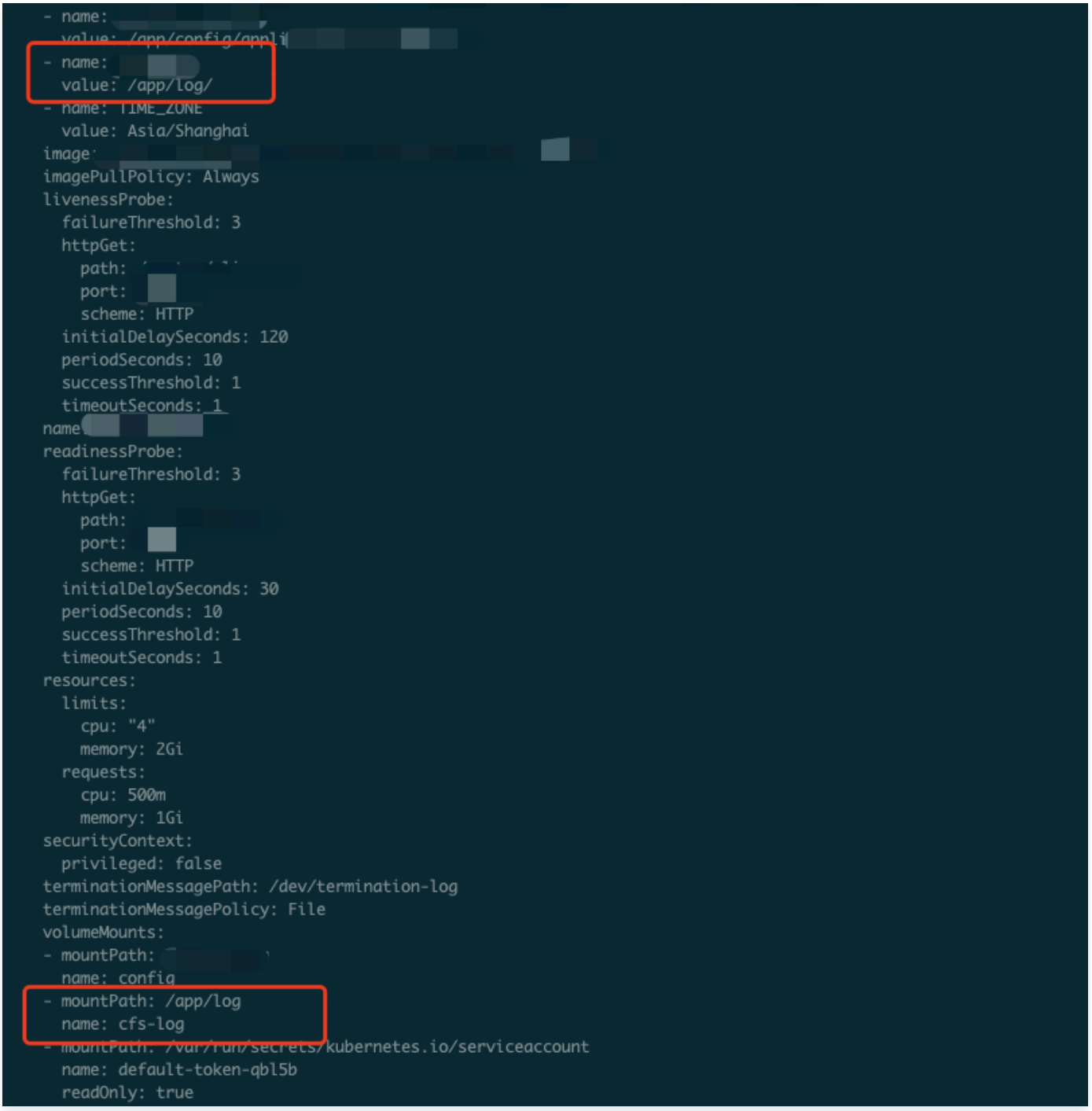
©2013-2026 Tencent Cloud. 著作権を所有しています。

ログが永続化ストレージに出力されている場合、業務Podが再構築されると、ログが再収集される原因となります。以下のコマンドを使用して、Podのyaml定義を確認できます：

```
kubectl get pods <pod_name> -n <namespace> -o yaml | less
```

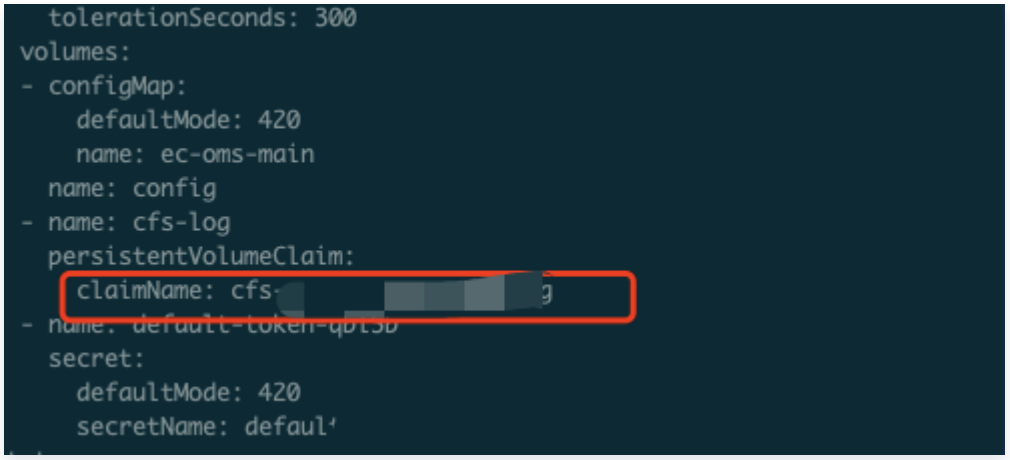
以下のような情報が返された場合、ログが永続化ストレージに出力されていることを示します。

- ビジネスでCFSを使用しており、かつCFSがコンテナにマウントされています。



©2013-2026 Tencent Cloud. 著作権を所有しています。

- CFS宣言を使用しました。



修復方法:

- ログを永続化ストレージに保存する必要がない場合は、コンテナクラスタでログ収集を有効にすることで、ログをCLSに収集できます。
- ログファイルを永続化ストレージに保存する必要がある場合は、CLSコンソールでLogListener収集ルールを設定する際に、収集ポリシーを**増分**収集に変更できます。ただし、増分収集ではすべてのログが収集されるとは限りません。

ログの収集漏れが発生した場合、どうすればよいですか?

Loglistenerは現在、NFS上に保存されたログをサポートしていません。Loglistenerはファイルの更新情報を取得するために、Linuxカーネルイベントをサブスクライブしており、能動的に対象ファイルをスキャンするわけではありません。
NFSファイルの更新情報はNFSサーバー側で処理されるため、クライアント側のローカルカーネルでイベントを生成できず、そのため感知されません。したがって、NFSファイルはリアルタイムに収集できず、収集漏れが発生する可能性があります。

収集設定とPodが一致しない場合、どうすればよいですか?

以下の操作を行うことで調査できます:

1. 以下のコマンドを使用して、Podのlabelが収集設定と一致しているかどうかを確認してください。

```
kubectl get pods <pod_name> -n <namespace> --show-labels
```

   - 一致しています。次の手順を実行してください。
   - 一致していません。正しい内容と照らし合わせて収集設定を修正してください。
2. Podのworkload（Deploymentまたはstatefulsetsなど）が収集設定と一致しているかどうかを確認してください。

©2013-2026 Tencent Cloud. 著作権を所有しています。

```
kubectl get pods -n <namespace> |grep testa
```

- 一致しています。次の手順を実行してください。
- 一致していません。正しい内容と照らし合わせて収集設定を修正してください。

3. 以下のコマンドを使用して、Podのyaml定義を確認し、containerの名前と収集設定で指定されたコンテナ名が一致しているかどうかを確認してください。

```
kubectl get pods <pod_name> -n <namespace> -o yaml
```

- 一致しています。タスクは完了しました。
- 一致していません。正しい内容と照らし合わせて収集設定を修正してください。

収集パスが正しくない場合、どうすればよいですか?

コンテナファイルまたはホストファイルを収集するシナリオでは、収集対象のディレクトリパスが正しいこと、および収集ルールに一致するログが存在することを確認してください。

ログファイルにシンボリックリンクを使用できますか?

コンテナファイル収集のシナリオでは、収集対象のログファイルにシンボリックリンクが存在することはサポートされていません。
Kubernetes環境では、**CLSはコンテナファイルのホスト上の位置を解析することで実現されています。コンテナ内のシンボリックリンク先はコンテナ内のパスを指しているため、収集対象ファイルにシンボリックリンクが存在する場合、正しく到達できません。**
修復方法:
収集ルールのパスとマッチングファイルを、実際にログファイルが存在するパスとファイルに変更し、シンボリックリンクへのマッチングを回避してください。

収集仕様の制限をトリガーするものは何ですか?

Loglistenerによる収集はコンテナ環境ではリソースが制限されるため、監視対象のディレクトリとファイルの数に制限があります:

- 監視ディレクトリ数：5000
- 監視ファイル数：10000

コンテナファイルまたはホストファイルを収集するシナリオでは、このような問題が発生する可能性があります。通常、ユーザーが期限切れのログファイルをクリーンアップしていないため、Loglistenerのログを確認すると、以下のような情報が記録されています:

©2013-2026 Tencent Cloud. 著作権を所有しています。



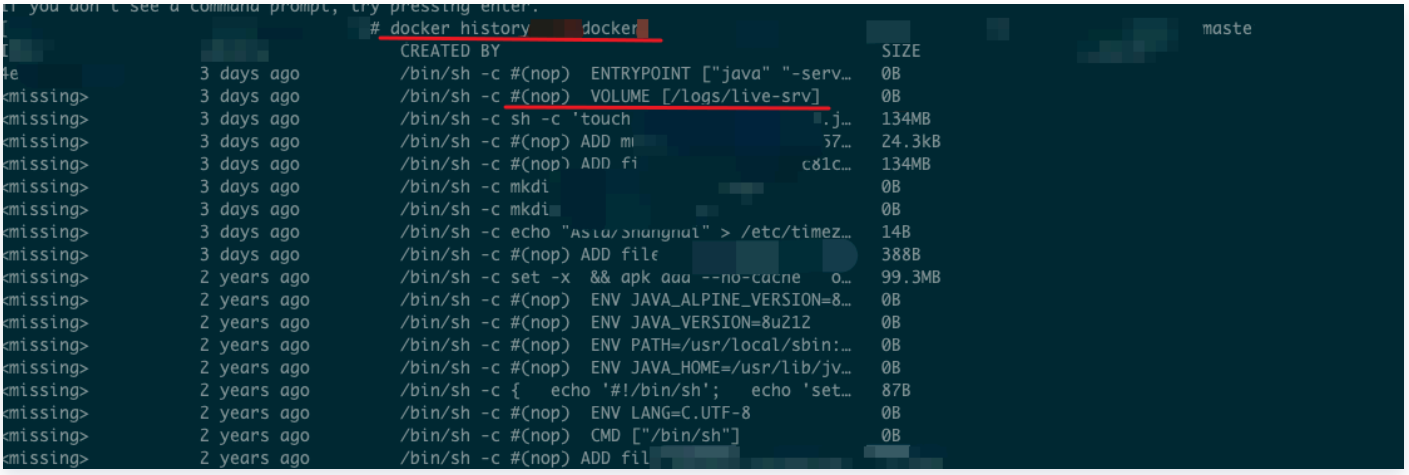
最大制限を超えたファイルとディレクトリは、Loglistenerによって監視対象に含まれないため、一部のユーザーが想定していたログファイルが収集されません。
詳細については、リソースとパフォーマンスの制限のドキュメントを参照してください。
修復方法:
ログディレクトリで `tree` コマンドを使用して、ディレクトリ全体の現在のディレクトリ数とファイル数がLoglistenerの制限に達しているかどうかを確認してください。

- 制限に達していない場合は、ビジネスコンテナが存在するホストの/var/log/tke-log-agentで `tree -L 5` を実行し、マシン全体の粒度が制限に達しているかどうかを確認してください。
  Loglistenerの制限はマシン粒度であるため、特定のコンテナファイル数が閾値に達していなくても、マシン全体の粒度ではすべてのコンテナファイルが制限に達している可能性があります。
- 制限に達した場合は、期限切れのログを速やかにアーカイブし、Loglistenerが監視するディレクトリとファイルによって消費されるリソースを削減してください。

Dockerfileでvolumeを定義した場合、どうすればよいですか?

- Docker環境では、 `docker history $image` コマンドを使用して、イメージのビルド情報を確認します。
- Containerd環境: `crictl inspecti $image` コマンドを使用して、イメージのビルド情報を確認します。

以下の情報が返されます。これにより、Dockerfile内でユーザーがボリューム/logs/live-srvをカスタマイズしており、それがまさにログが存在するディレクトリであることがわかります。この操作は、ログ収集コンポーネントが正しいログファイルを見つけるのを妨げます。



修復方法:

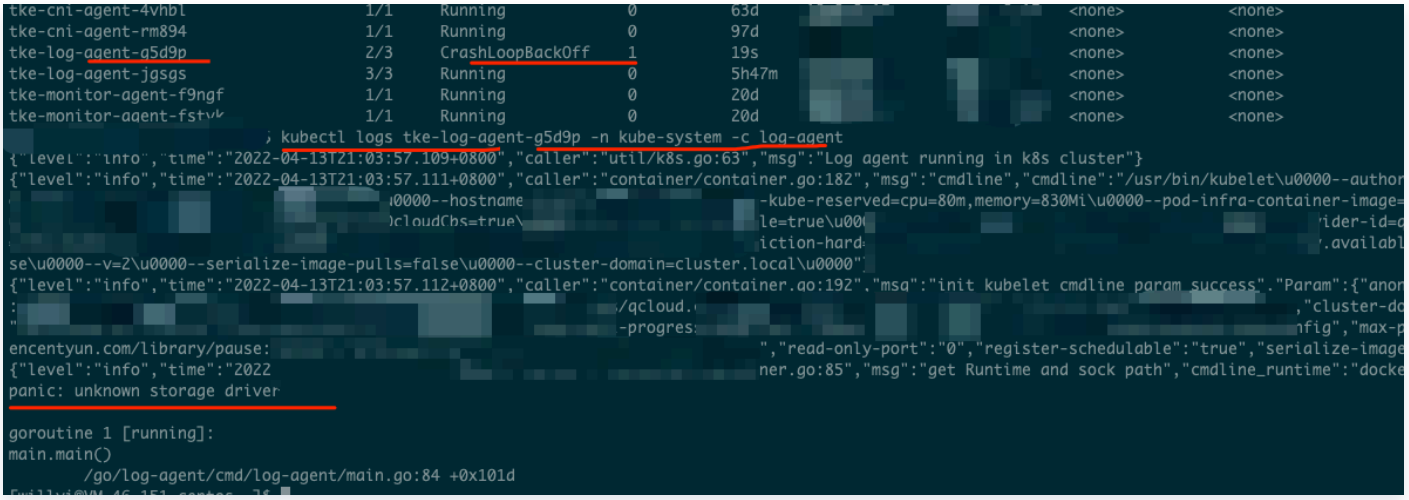
- Dockerfileを変更してvolumeを削除し、イメージを再ビルドしてサービスを再デプロイしてください。
- サービスログの書き込みディレクトリを変更し、Dockerfileで定義されたvolumeパスに書き込まないでください。

©2013-2026 Tencent Cloud. 著作権を所有しています。

その他のご質問

コンテナエンジンタイプの識別エラーが発生した場合、どうすればよいですか?

Docker環境では、一部のシナリオで古いバージョンのバグが発生し、ログ収集コンポーネントが正常に起動できず、panicログが出力されることがあります。
主な原因は、ユーザーがTKEクラスタノードのDocker設定をカスタマイズしたことにより、以下の図に示すエラーが発生することです:



修復方法:

- /etc/docker/daemon.jsonの設定に、`"storage-driver": "overlay2"`を追加します。以下の図に示す通りです:

©2013-2026 Tencent Cloud. 著作権を所有しています。

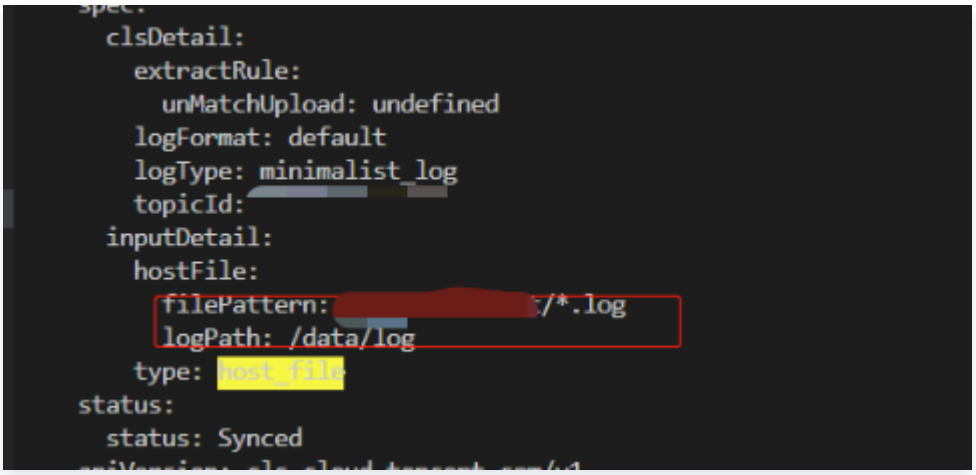
```
[root@VM-0-5-centos ~]# cat /etc/docker/daemon.json
{
  "bridge": "none",
  "debug": false,
  "default-runtime": "runc",
  "exec-opts": [],
  "exec-root": "",
  "graph": "/var/lib/docker",
  "group": "",
  "insecure-registries": [],
  "ip-forward": true,
  "ip-masq": false,
  "iptables": false,
  "ipv6": false,
  "labels": [],
  "live-restore": true,
  "log-driver": "json-file",
  "log-level": "warn",
  "log-opts": {
    "max-file": "10",
    "max-size": "100m"
  },
  "max-concurrent-downloads": 10,
  "registry-mirrors": [
    "https://mirror.ccs.tencentyun.com"
  ],
  "runtimes": {},
  "selinux-enabled": false,
  "storage-driver": "overlay2",
  "storage-opts": [
    "overlay2.override_kernel_check=true"
  ]
}
[root@VM-0-5-centos ~]#
```

- TKEコンソールでログ収集コンポーネントのバージョンをアップグレードします。新しいバージョンの収集コンポーネントではこの問題が修正されているため、Docker設定を変更する必要はありません。

filePatternでサブディレクトリを設定した場合、どうすればよいですか?

以下の図に示すように、ユーザーがfilePatternフィールドパラメータにサブディレクトリを設定しています。この操作により、ログを正常に収集できなくなります。

©2013-2026 Tencent Cloud. 著作権を所有しています。



修復方法:

logPathパラメータでログファイルのディレクトリを設定し、filePatternではファイルタイプパラメータのみを設定し、サブディレクトリは設定しないでください。

©2013-2026 Tencent Cloud. 著作権を所有しています。

自建K8Sログ収集トラブルシューティングガイド

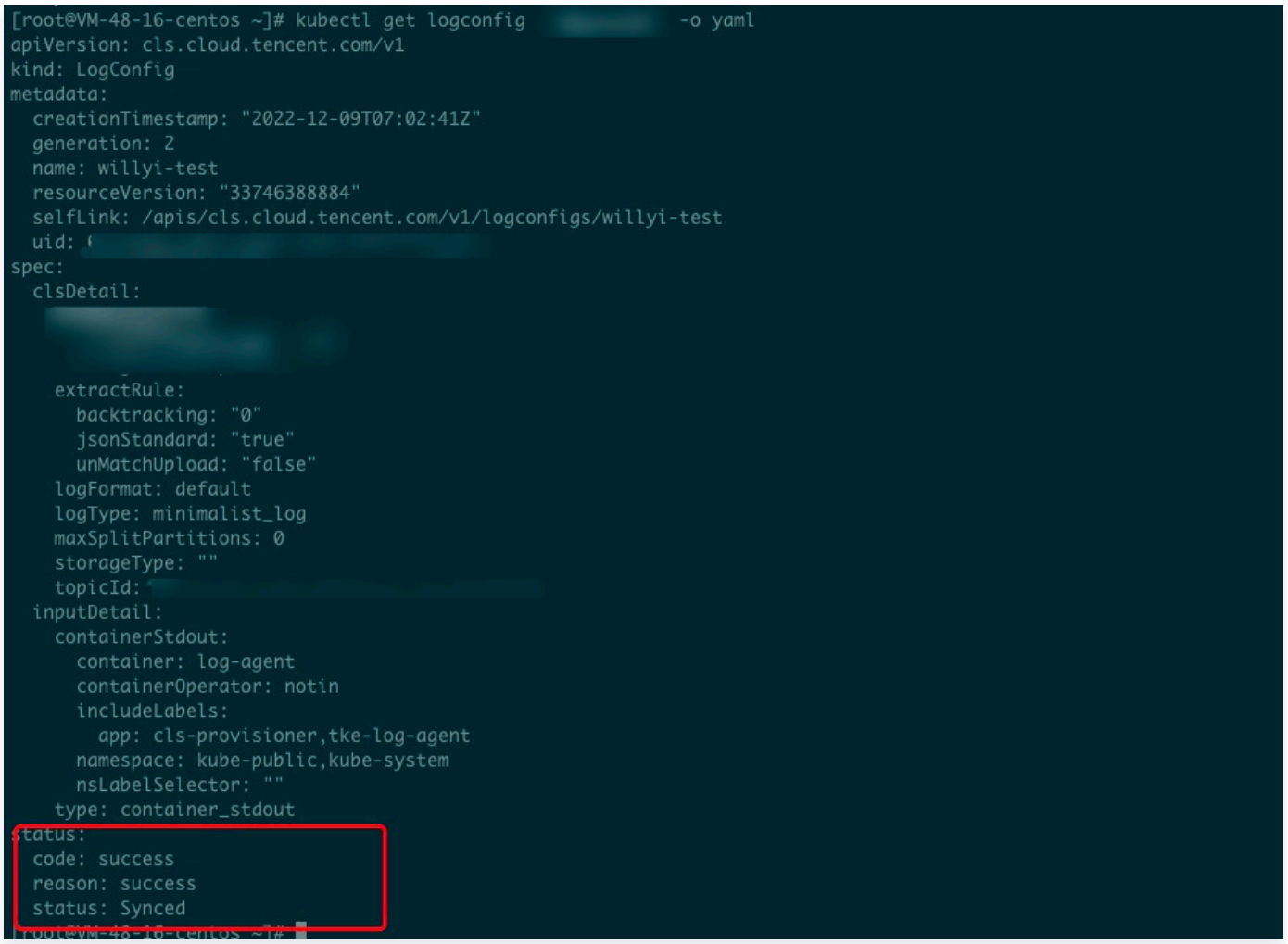
最終更新日：：2026-10-12 15:06:45

自社構築のK8SクラスタにLogListenerをインストールしてデプロイが完了した後、LogConfigを作成するか、コンソールから収集設定を行うことで、ログ収集を開始できます。
ログ収集に異常が発生した場合は、まず以下の手順に従って自己点検してください。

1. logconfigの状態を確認する

- クラスタ内のすべての収集設定を表示するには：kubectl get logconfig
- 特定の収集設定を表示するには：kubectl get logconfig xxx -o yaml
- logconfigの同期状態を確認します。statusがSynced以外の状態はすべて異常であり、異常情報はreasonに記載されます。正常な場合はすべてsuccessの状態です。
  上記のようにlogconfigの状態同期が成功している場合、収集異常の原因は他の側面にあります。以下の図に示す通りです：

©2013-2026 Tencent Cloud. 著作権を所有しています。



同期エラーの原因をさらに詳しく知りたい場合は、cls-provisionerのログを確認してください。

2. cls-provisionerのログを確認する

- cls-provisionerのPodを特定するには：kubectl get pods -n kube-system -o wide |grep cls-provisioner
- ログを確認するには：kubectl logs cls-provisioner-xxx -n kube-system
  以下の図に示す通りです：



cls-provisionerのログを確認して、同期エラーの具体的な原因を調べます。

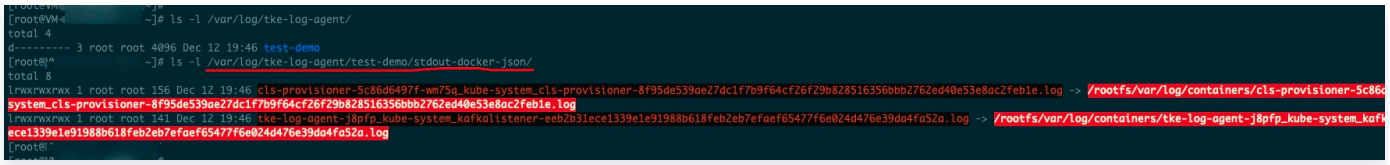
> ⚠ **注意：**
> cls-provisionerコンポーネントの役割は、CLSサーバーと通信し、logconfigの収集設定を変換してCLSサーバーに同期することです。これにより、コレクターはサーバーから収集設定を取得し、正常なログ収集を行うことができます。

3. 収集エンドのログを確認する

©2013-2026 Tencent Cloud. 著作権を所有しています。

収集設定の同期が正常であるにもかかわらず、ログ収集に異常がある場合は、収集側の関連ログを具体的に確認してください。

- シンボリックリンクが正常に作成されたかどうかを確認します。
  標準出力の収集を例に説明します：
  /var/log/tke-log-agent/<収集設定名（logconfig名）>/stdout-docker-json の配下に、収集対象のPodの標準出力ログのシンボリックリンクが作成され、作成後に正常な収集が可能になります。

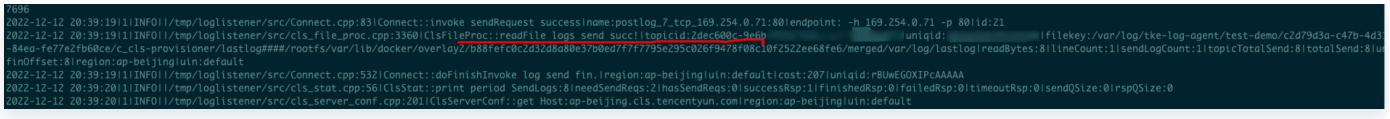


ここではDockerを例にしています。runtimeがcontainerdの場合、パスは /var/log/tke-log-agent/<収集設定名（logconfig名）>/stdout-containerd になります。
コンテナファイル収集のシンボリックリンクの作成方法は以下の通りです：
/var/log/tke-log-agent/<収集設定名（logconfig名）>/
以下の図に示す通りです：



上記の例に従ってシンボリックリンクが正常に作成されているかどうかを確認します。作成されていない場合は異常があります。正常に作成されている場合は、引き続きコレクターloglistenerのログを確認してください。

- コレクターloglistenerのログを確認します。
  kubectl get pods –n kube–system –o wide |grep tke–log–agent
  まず、ログ収集に異常があるPodに対応するホスト上のtke–log–agentのPodを特定し、次にloglistenerのログを確認します。
  kubectl logs tke–log–agent–xxx –n kube–system –c loglistener



上図に示すような **readFile logs send succ!|topicid** の文字列があるかどうかを確認します。ある場合は、ログが対応するtopicに正常に収集されたことを示します。上記の文字列がない場合は、収集に問題があることを示しており、関連する開発担当者に連絡してください。
すでにtopicに収集されているにもかかわらず検索できない場合は、まずtopicの全文インデックスが有効になっているかどうかを確認してください。

©2013-2026 Tencent Cloud. 著作権を所有しています。

収集設定に関するよくある質問

最終更新日：：2026-10-12 15:06:45

完全なログ内容を完全正規表現の収集設定でどのように取得しますか?

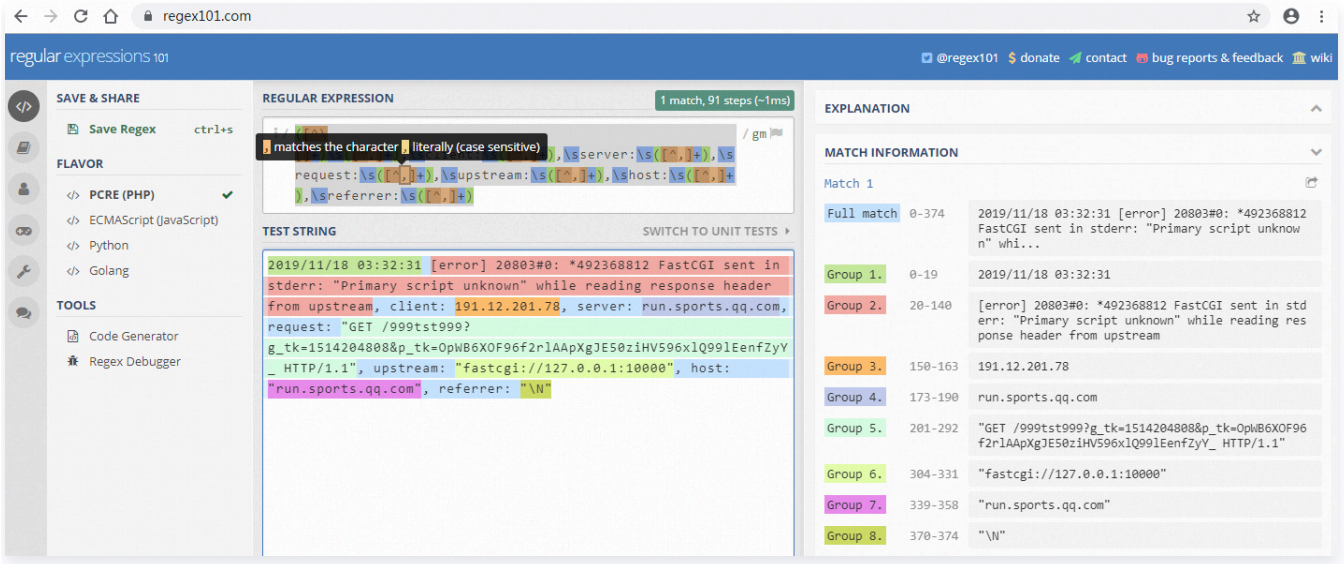
元のログでは、完全なログ形式は以下の通りです:

```
2019/11/18 03:32:31 [error] 20803#0: *492368812 FastCGI sent in stderr:
"Primary script unknown" while reading response header from upstream,
client: 191.12.201.78, server: run.sports.qq.com, request: "GET
/999tst999?
g_tk=1514204808&p_tk=OpWB6XOF96f2rlAApXgJE50ziHV596xlQ99lEenfZyY_
HTTP/1.1", upstream: "fastcgi://127.0.0.1:10000", host:
"run.sports.qq.com", referrer: "\N"
```

以下の正規表現を使用することで、対応するフィールドを抽出できます:

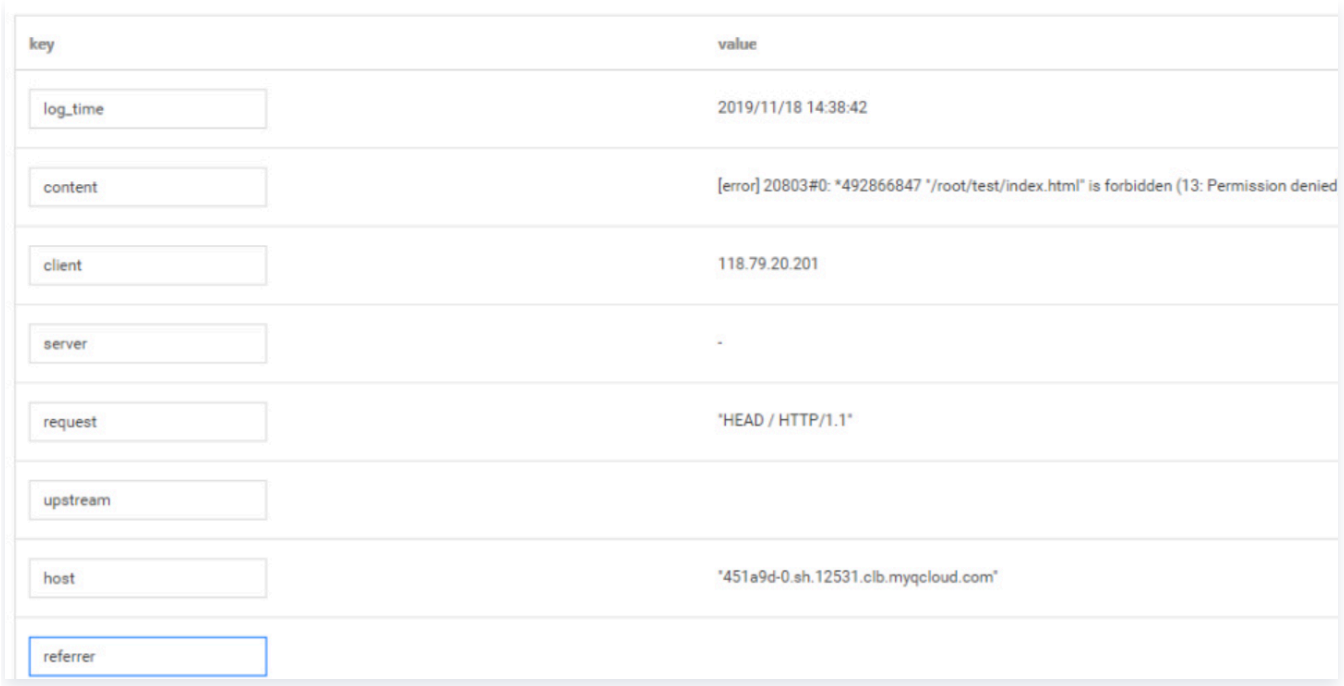
```
([^\
[]+)\s([^,]+),\sclient:\s([^,]+),\sserver:\s([^,]+),\srequest:\s([^,]+),
\supstream:\s([^,]+),\shost:\s([^,]+),\sreferrer:\s([^,]+)
```

元のログをフォーマット化したフィールドは以下の通りです（regex を使用してカスタム正規表現を構築することを推奨します）：



各フィールドは順に以下のように命名されます：log_time、content、client、server、request、upstream、host、referrer。

©2013-2026 Tencent Cloud. 著作権を所有しています。



key	value
log_time	2019/11/18 14:38:42
content	[error] 20803#0: *492866847 "/root/test/index.html" is forbidden (13: Permission denied
client	118.79.20.201
server	-
request	"HEAD / HTTP/1.1"
upstream	
host	"451a9d-0.sh.12531.clb.myqcloud.com"
referrer	

ログ内容のフィールドが一部欠落している場合、どのように収集しますか?

ただし、状況によっては、ログ内の upstream、referrer フィールドが欠落する場合があります。
例えば、upstream がなく、referrer がある場合は以下の通りです:

```
2019/11/18 04:02:38 [error] 20802#0: *492391323 access forbidden by
rule, client: 45.71.63.206, server: admin.sports.qq.com, request: "GET
/index HTTP/1.1", host: "admin.sports.qq.com", referrer:
"http://admin.sports.qq.com/index"
```

または、upstream も referrer もない場合は以下の通りです:

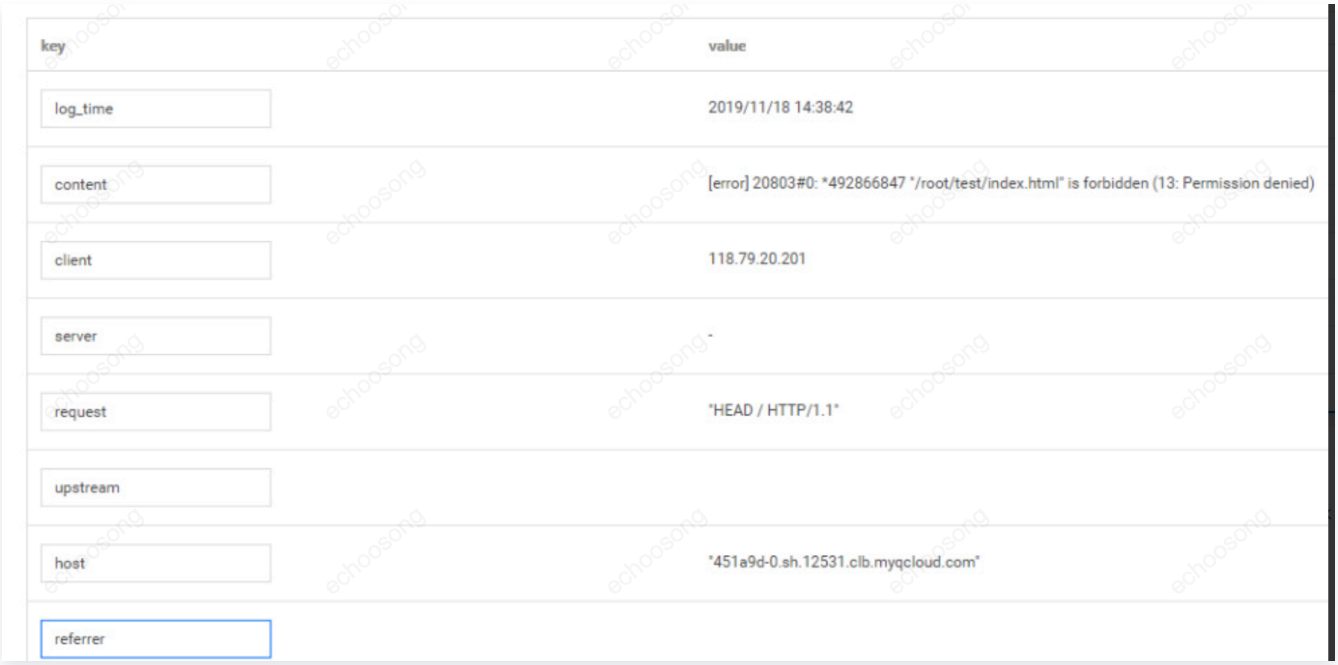
```
2019/11/18 14:38:42 [error] 20803#0: *492866847 "/root/test/index.html"
is forbidden (13: Permission denied), client: 118.79.20.201, server: -,
request: "HEAD / HTTP/1.1", host: "451a9d-0.sh.12531.clb.myqcloud.com"
```

この場合、前述の正規表現では、この2つの欠落シーンに対応できません。
正規表現における `非キャプチャグループ構文(?:x)` と `0回または1回のマッチ?` 構文を組み合わせることで、upstream と referrer が欠落するシーンに対応できると同時に、 `キャプチャグループ` で抽出される番号の一貫性も確保できます。
完全な正規表現は以下の通りです:

©2013-2026 Tencent Cloud. 著作権を所有しています。

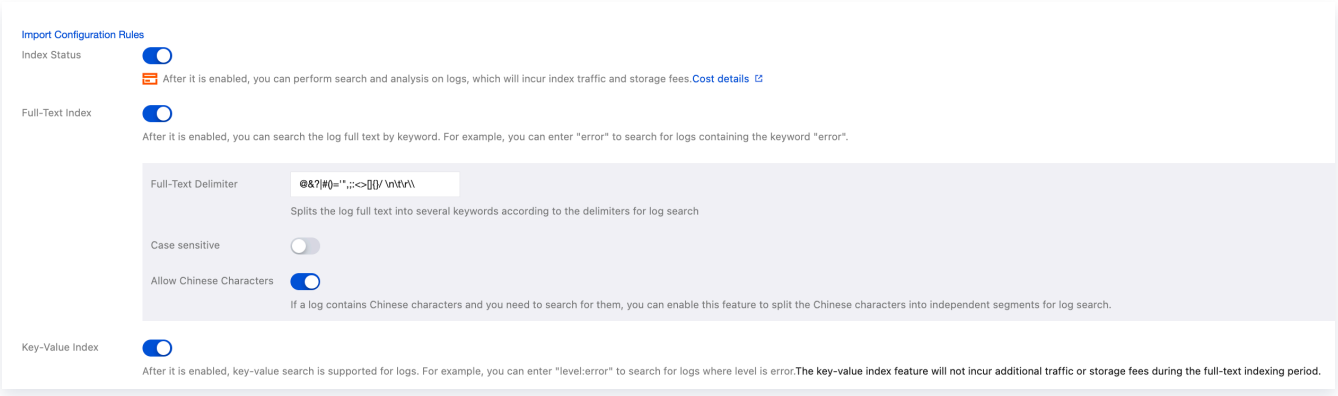
```
([^\
[]+)\s([^,]+),\sclient:\s([^,]+),\sserver:\s([^,]+),\srequest:\s([^,]+)
(?:,\supstream:\s([^,]+))?,\shost:\s([^,]+)(?:,\sreferrer:\s([^,]+))?
```

upstream と referrer がないログに対してテストを実施したところ、CLS収集ページ上の抽出スクリーンショットは以下の通りです:



インデックス設定はどのように行いますか?

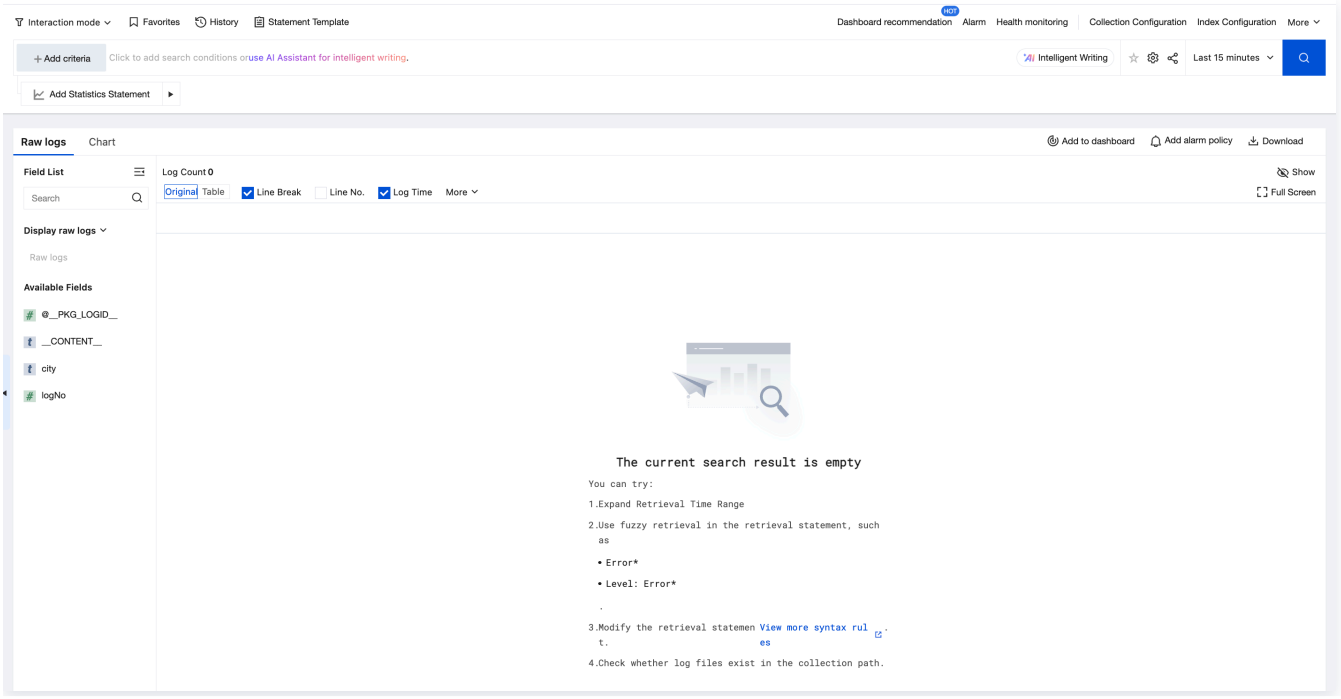
インデックスを有効にして、全文およびキー値インデックスを設定します。



ログはどのように検索しますか?

CLSコンソールでログを検索すると、以下のように表示されます。
検索キーワード: `referrer:admin*`

©2013-2026 Tencent Cloud. 著作権を所有しています。



©2013-2026 Tencent Cloud. 著作権を所有しています。

収集自己チェックツール利用ガイド

最終更新日：：2026-10-12 15:06:45

非TKE環境でのLogListenerログ収集自己チェックツールの使用

注意事項

- **オペレーティングシステム**：Linuxシステムのみをサポートします。
- **実行権限**：ダウンロード後、実行権限を付与する必要があります。`chmod +x loglistener-check` を実行します。
- **前提条件**：実行前に、現在のマシンにLogListenerがインストールされ、実行されていることを確認してください。LogListenerがインストールされていない場合は、インストールおよびアップグレードガイド を参照してください。ツールはLogListenerのインストールディレクトリと設定ファイルを読み取る必要があるため、LogListenerが配置されているマシン上で直接実行することをお勧めします。
- **ネットワーク要件**：ツールの実行時にCLSサービスへアクセスしてバージョンおよび設定の検証を行う必要があります。マシンのネットワークがTencent Cloud関連ドメインへ正常にアクセスできることを確認してください。

ツールのダウンロード

収集セルフチェックツールをダウンロードします。ダウンロードアドレス：`https://mirrors.tencent.com/install/cls/loglistener-check/linux/loglistener-check`

使用を開始

関連コマンド

```
Usage of  ./loglistener-check:
      -h, --help            help for loglistener
      --root_dir string    (optional) install loglistener root dir
(default is /usr/local/loglistener-*)
      --topic string       (optional) topic ID
```

主なパラメータの説明は以下の通りです：

パラメータ	タイプ	必須/任意	説明
`--root_dir`	string	いいえ	LogListener のインストールルートディレクトリを指定します。デフォルト値は `/usr/local/loglistener-*` です（ツールはこのパス

©2013-2026 Tencent Cloud. 著作権を所有しています。

			パターンに一致するインストールディレクトリを自動的に検出します）。 カスタムパスで LogListener をインストールした場合は、完全なインストールパスを手動で指定してください。例えば、デフォルトパスで LogListener 2.7.2 をインストールした場合、そのルートディレクトリは `/usr/local/loglistener-2.7.2` です。
`--topic`	string	いいえ	確認する必要があるログトピック（Topic）の ID を指定します。Topic ID は CLS コンソールのログトピック一覧で取得できます。具体的な操作については ログトピック をご参照ください。 このパラメータを指定しない場合、ツールはこのマシン上で関連付けられているすべてのログトピックをチェックします。指定した場合、その Topic に関連する収集設定のみをチェックし、チェック範囲がより正確になります。

例

チェックツールを使用して、チェックツールが提示する問題を確認し、提供された解決策に基づいて問題を解決します。例えば、デフォルトパラメータを使用したチェック結果の例です。



チェック結果：

- 現在のマシンにインストールされているLogListenerのバージョンが低すぎます。チェックツールが新バージョンを検出したため、アップグレードを推奨します。新バージョンでは多くの問題が修正され、多くの新機能が追加されています。
- inotifyパラメータ設定が推奨値に適合していません。ユーザーによる変更を推奨します。変更しない場合、ログ収集に影響を与える可能性があります。

TKE環境でのLogListenerログ収集自己チェックツールの使用

注意事項

- **オペレーティングシステム**：Linux、macOS、Windowsシステムをサポートします。
- **実行権限**：ダウンロード後、実行権限を付与する必要があります。`chmod +x detect-tool` を実行します。
- **前提条件**：実行前に、kubectlを通じて対象のTKEクラスタへ正常に接続されていることを確認してください。ツールはkubeconfig設定ファイルに依存してクラスタリソースへアクセスします。

©2013-2026 Tencent Cloud. 著作権を所有しています。

- **ネットワーク要件**：ツールの実行時にKubernetes API ServerおよびCLSサービスへのアクセスが必要です。実行環境のネットワークが正常に接続されていることを確認してください。

ツールのダウンロード

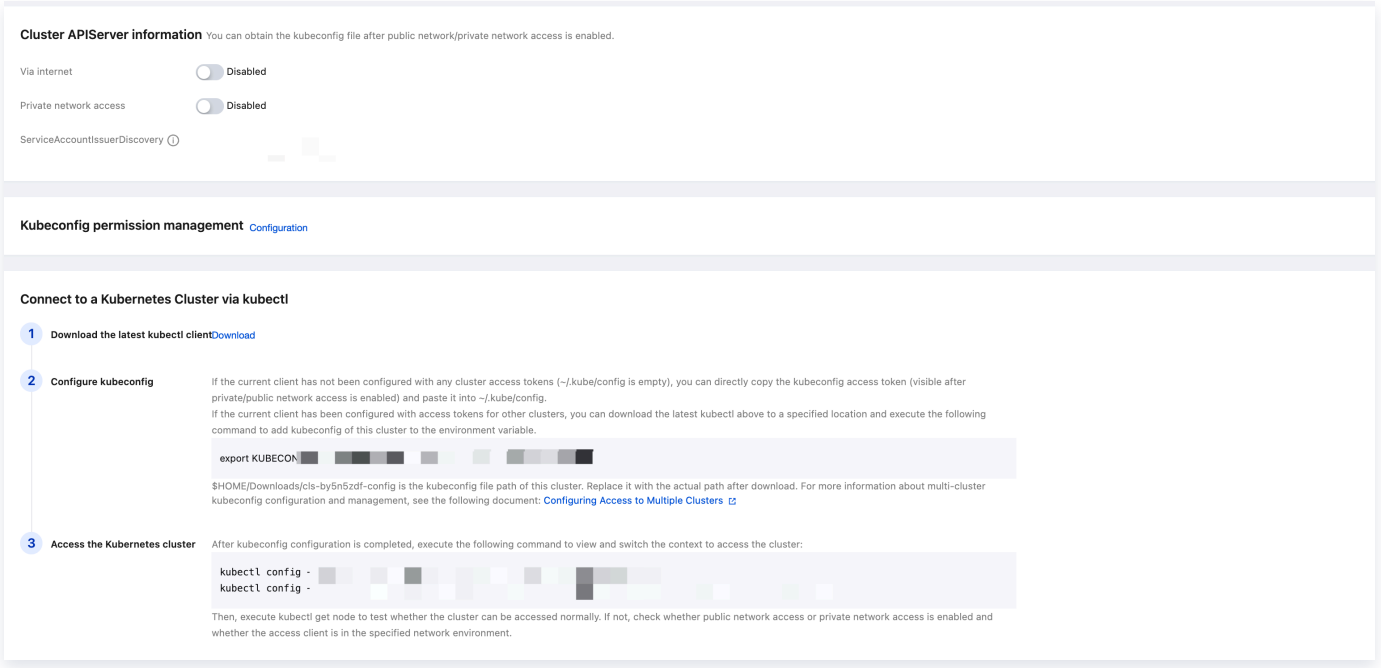
お使いのオペレーティングシステムに応じて、対応するバージョンの収集セルフチェックツールをダウンロードします：

- Linux：`https://mirrors.tencent.com/install/cls/detect-tool/linux/detect-tool`
- macOS：`https://mirrors.tencent.com/install/cls/detect-tool/mac/detect-tool`
- Windows：`https://mirrors.tencent.com/install/cls/detect-tool/windows/detect-tool`

使用を開始

TKEクラスタへの接続

1. TKEコンソール にログインします。
2. 左側のナビゲーションバーで**クラスタ**を選択し、クラスタ管理ページに入ります。
3. 接続するクラスタを見つけ、そのID/名前をクリックして、クラスタ管理ページに入ります。
4. 左側のナビゲーションバーで**基本情報**をクリックし、基本情報ページに移動します。
5. **クラスタ APIServer 情報**欄で、TKEの指示に従い、kubectlを使用してTKEクラスタに接続します。具体的な操作については、Kubeconfigの設定 を参照してください。



関連コマンド

```
Usage of ./detect-tool:
```

©2013-2026 Tencent Cloud. 著作権を所有しています。

```
      --kubeconfig string    (optional) Path to a kubeconfig file,
specifying how to connect to the API server. (default
"/root/.kube/config")
      --logConfig string     (optional) logconfig name
      --namespace string     (optional) pod name namespace
      --pod string           (optional) pod name
      --topic string         (optional) topic id
```

主なパラメータの説明は以下の通りです:

パラメータ	タイプ	必須/任意	説明
`--kubeconfig`	string	いいえ	Kubernetes への接続に使用する設定ファイルのパスです。デフォルト値は `/root/.kube/config` です。通常、kubectl が正常にクラスタへ接続した後は、特別な設定や指定は不要です。
`--logConfig`	string	いいえ	収集設定（LogConfig）名を指定し、検出する収集設定を指定します。`kubectl get logconfigs` コマンドで現在のクラスタ内の収集設定一覧を確認できます。
`--pod`	string	いいえ	Pod名を指定し、検出するPodを指定します。Podを指定した場合は、必ず `--namespace` も指定する必要があります。
`--namespace`	string	いいえ	検出するPodが存在するnamespaceを指定します。namespaceを指定した場合は、必ず `--pod` も指定する必要があります。
`--topic`	string	いいえ	確認する必要があるログトピック（Topic）IDを指定し、そのTopicに関連付けられた収集設定を確認します。1つのクラスタに複数の収集設定が同じTopicに関連付けられている場合があります。Topic IDはCLSコンソールで取得できます。具体的な操作についてはログトピックをご参照ください。

例

チェックツールを使用して、チェックツールが提示する問題を確認し、提供された解決策に基づいて問題を解決してください。

- 示例1：収集設定とPodチェックを指定します。

```
./detect-tool --logConfig=cls-log-config --pod=cls-provisioner-
xxxxxxxxxx --namespace=kube-system
```

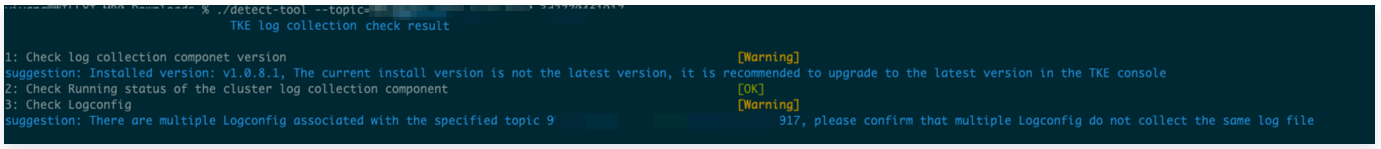
©2013-2026 Tencent Cloud. 著作権を所有しています。



チェック結果：指定されたpodと収集設定ルールが一致しません。

- 示例2：指定topicをチェックします。

```
./detect-tool --topic=1a2763e2-75f9-4a16-b921-1a80e3de7356
```



チェック結果：

- ログコンポーネントのバージョンアップグレードを推奨します。現在のクラスタは最新バージョンではありません。
- 2つの収集設定が1つのtopicに関連付けられています。複数の収集設定が同じファイルを収集しないようにすることをお勧めします。

©2013-2026 Tencent Cloud. 著作権を所有しています。

検索分析関連
ログを検索できない

最終更新日：：2026-10-12 15:06:45

検索ステートメントが空の場合、なぜログを一切検索できないのですか?

検索ステートメントが空の場合、フィルタリング条件がなく、すべてのログを照会することを表します。ログが表示されない場合は、以下の手順でトラブルシューティングできます：

1. **より広い時間範囲を選択し（例えば直近30日）、検索ステートメントを空のままにして、ログがあるかどうかを確認します。**
2. **ログなし**：
   - 現在のログトピックでインデックスが有効になっていない可能性があります。インデックス設定でこのトピックのインデックスを有効にしてください。
   - 以前にログを報告した時点でインデックスが有効になっておらず、ログ報告の完了後にインデックスを有効にしたことが原因である可能性があります。履歴データに対してインデックスを再構築するか、インデックスを有効にした後にログを再収集してください。
   - ログ報告の失敗が原因である可能性があります。LogListenerを使用してログを収集する場合は、マシングループの状態に異常がないか確認してください。SDKなどの方法でログを報告する場合は、SDK自身の出力ログにエラーがないか確認してください。
   - ログ時刻の誤りが原因である可能性があります。ログが未来の時刻に報告されたか、ログトピックの保存期間を既に超えた時刻に報告されています。LogListenerを使用してログを収集する場合は、ログが存在するサーバーの時刻が正しいかどうかを確認してください。カスタムログ時刻を使用している場合は、時刻形式が正しく設定されているかどうかを確認してください。SDKなどの方法でログを報告する場合は、ログ時刻パラメータの渡し方が正しいかどうかを確認してください。
3. **一部の期間にはログがあり、一部の期間にはログがありません**：
   - ログ報告の失敗が原因である可能性があります。LogListenerを使用してログを収集する場合は、マシングループの状態に異常がないか確認してください。SDKなどの方法でログを報告する場合は、SDK自身の出力ログにエラーがないか確認してください。
   - この時間帯には実際にログがない可能性があります。指定された時間帯に自身の業務でログが生成されているかどうかを確認してください。

検索ステートメントが空の場合はログを検索できるのに、検索ステートメントを入力するとログを一切検索できないのはなぜですか?

この問題を引き起こす可能性のある原因は以下の通りです：

- 一部のログ報告が失敗しました：LogListenerを使用してログを収集する場合は、マシングループの状態に異常がないか確認してください。SDKなどの方法でログを報告する場合は、SDK自身の出力ログにエラーがない

©2013-2026 Tencent Cloud. 著作権を所有しています。

か確認してください。

- インデックス設定で単語分割が正しくありません：検索はログの単語分割に基づいています。元のログは、単語分割後に検索条件で指定された「語」を含んでいる場合にのみ検索できます。例えば、errorではerrorMessageを検索できません。errorMessage自体が1つの独立した語であり、errorと等しくないためです。このログを検索するには、ワイルドカードerror*を使用する必要があります。単語分割の詳細な説明と例については、単語分割とインデックスを参照してください。
- 過去のログが最新のインデックス設定を採用していません：インデックス設定を変更した後、その変更は新たに収集されたログにのみ適用されます。インデックス設定ページで前回のインデックス変更時刻を確認できます。検索対象のログがその時刻より前のものである場合、現在のインデックス設定ではその過去のログを検索できない可能性があります。履歴データに対してインデックスを再構築してください。
- LogListenerを使用してログを収集する際に、一部のログが収集段階で解析異常を起こし、LogParseFailureフィールドに保存されています。全文検索を試すか、LogParseFailureフィールドに対してキー値検索を使用してください（LogParseFailureのキー値インデックスを有効にする必要があります）。
- 一部のログはインデックス作成中に異常が発生し、__RAWLOG__フィールドに保存されています。全文検索を試してください。

CLSコンソールではログを検索できるのに、APIを使用するとログを検索できないのはなぜですか?

この問題はAPIのパラメータ渡しの誤りによって発生します。CLSコンソールページでブラウザの開発者ツールを使用して、インターフェースのリクエストパラメータが、お客様がAPIを呼び出す際のパラメータと一致しているかどうかを確認することをお勧めします。最も一般的な問題は、SearchLogインターフェースのFromおよびToパラメータに使用されるUnixタイムスタンプの単位の誤りです。ミリ秒形式のUnixタイムスタンプを使用する必要があり、秒形式はサポートされていません。

©2013-2026 Tencent Cloud. 著作権を所有しています。

検索分析エラー

最終更新日：：2026-10-12 15:06:45

よくあるエラー情報、原因および解決策は以下の通りです：

エラー情報	エラー原因	ソリューション
QueryError [illegal_argument_exception. Cannot search on field [xxx] since it is not indexed.]	フィールドxxxでキー値インデックスが有効になっていないため、クエリできません。	このフィールドに対してキー値インデックスを有効にしてください。詳細についてはキー値インデックスをご参照ください。
QueryError [illegal_argument_exception. Cannot search on Full-Text since it is not indexed.]	全文インデックスが有効になっていません。	全文検索を有効にしてください。詳細については全文インデックスをご参照ください。
QueryError [illegal_argument_exception. syntax error on field [and|or|not], or full text search is closed]	検索条件では小文字の論理演算子はサポートされていません。小文字の論理演算子は通常のフィールドとして全文検索されます。	大文字の論理演算子AND|OR|NOTを使用してください。論理操作が必要ではなく、and|or|notを含むログを全文検索する場合は、全文インデックスを有効にしてください。
QueryError [number_format_exception. For input string: ">"]	数値比較ステートメントの構文エラー。	数値比較記号の前後にスペースなどの特殊記号が存在するかどうかを確認してください。正しい形式はstatus:>400を参照してください。
QueryError [circuit_breaking_exception. Analysis data is too large,please reduce the scope of data query]	クエリデータ量が大きすぎます。	クエリの時間範囲を適切に短縮し、検索条件を正確に指定してください。それでもエラーが発生する場合は、テクニカルサポートにご連絡ください。
QueryError [parse_exception.parse_exception: Cannot parse 'xxx': '*' or '?' not allowed as first character in WildcardQuery	プレフィックスあいまいクエリの使用は許可されていません。例えば、content:*exampleは使用できません。	フィールドを複数の単語に分割するには、単語区切り文字を使用することをお勧めします。詳細については、インデックスの設定をご参照ください。
QueryError [sql_illegal_argument_exception.cannot cast	castは13/Jul/2021:17:04:34形式の日付を変換できません。ISO標準の時刻形式とミリ秒単位の	時間フィールドの形式を変更するか、または__TIMESTAMP__組み

©2013-2026 Tencent Cloud. 著作権を所有しています。

[13/Jul/2021:17:04:34] to [datetime]: failed to parse date field [13/Jul/2021:17:04:34] with format [date_optional_time]]	Unixタイムスタンプのみをサポートします。例えば、yyyy-MM-dd'T'HH:mm:ss.SSSZまたはyyyy-MM-ddです。	込みフィールドを使用してください。
QueryError [verification_exception.Cannot order by non-grouped column [xxx], expected [xxx] or an aggregate function	フィールドxxxで統計が有効になっていないため、ソートに使用できません。	このフィールドに対して統計を有効にしてください。詳細については分析の概要をご参照ください。
QueryError [verification_exception.Cannot use non-grouped column [xxx], expected [xxx]]	フィールドxxxで統計が有効になっていません。	このフィールドに対して統計を有効にしてください。詳細については分析の概要をご参照ください。
QueryError [verification_exception.Field [xxx] of data type [text] cannot be used for grouping]	フィールドxxxで統計が有効になっていないため、groupに使用できません。	このフィールドに対して統計を有効にしてください。詳細については分析の概要をご参照ください。
QueryError [verification_exception.Unknown column [xxx]]	フィールドxxxが存在しません。	このフィールド名が正しいかどうかを確認してください。
QueryError [verification_exception.Unknown function [xxxxxx]]	関数xxxxxxは存在しません。	関数名が正しいかどうかを確認してください。また、一部の関数をHistogram関数と同時に使用した場合にもこのエラーが発生します。この場合、時間補完関数を使用してHistogram関数を置き換えることができます。
QueryError [verification_exception.argument of [FUNCNAME(xxx)] must be [numeric], found value [xxx] type [text]]	FUNCNAME関数に渡すパラメータの型が正しくありません。例えばSUM(level)の場合、levelフィールドがtext型のときにエラーが発生します。	フィールドタイプが関数の要件を満たしているかどうかを確認してください。
QueryError [parse_exception.Failed to parse query [xxx]]	クエリステートメントの構文エラー。	エラー情報で指摘されたエラー位置を確認してください。

©2013-2026 Tencent Cloud. 著作権を所有しています。

QueryError [line X:X: XXX]	クエリステートメントの構文エラー。	エラー情報で指摘されたエラー位置とエラー原因を確認してください。
Internal error. Please try again later RequestId: [7be994d4-xxxx-xxxxx-xxxx-9c38xxxx65de]	CLS内部エラー。	テクニカルサポートに連絡し、エラー情報のRequestIdを提供してください。
SyntaxError[xxx]	SQLステートメントの一部に構文エラーがあります。	エラー情報の詳細な指示を参考に構文エラーを修正してください。なお、line x,column xには検索条件部分（つまり「|」とその前の部分）は含まれません。
SearchTimeout	クエリがタイムアウトしました。	データクエリ範囲とSQLの複雑さを適切に縮小するか、しばらくしてから再試行してください。
LimitExceeded.LogSearch	検索の同時実行数が制限を超えています。	クエリ頻度（APIを含む）を下げて、しばらくしてから再試行してください。現在のクエリ頻度が高くないにもかかわらず、エラーが発生する場合は、テクニカルサポートにご連絡ください。

©2013-2026 Tencent Cloud. 著作権を所有しています。

統計分析（SQL）結果の小数点以下桁数が不正確

最終更新日：：2026-10-12 15:06:45

現象1：小数桁が保持されず、整数部のみ

類似の検索分析ステートメントを使用する場合、小数点以下2桁を保持することが期待されますが、結果には整数部分のみが含まれます：

- 検索分析ステートメント：

```
* | select count_if(status>=400)*100/count(*) as "エラーログの割合"
```

- 結果：

```
0
```

たとえround関数を使用して保持する小数点以下桁数を指定しても、結果には依然として整数部分のみが含まれます：

- 検索分析ステートメント：

```
* | select round(count_if(status>=400)*100/count(*),2) as "エラーログの
割合"
```

- 結果：

```
0
```

原因

SQLでは、整数（bigint）同士で除算を行う場合、結果は依然として整数となり、整数に対してround関数を使用しても無効です。

対処方法

- 方法1：

  四則演算では、乗算を使用して整数（bigint）の1つを小数（double）に変換します。例えば：

©2013-2026 Tencent Cloud. 著作権を所有しています。

```
* | select round(count_if(status>=400)*100.0/count(*),2) as "エラーログ
の割合"
```

- 方法2：

  型変換関数 を使用して整数（bigint）の1つを小数（double）に変換します。例えば：

```
* | select round(cast(count_if(status>=400)*100 as double)/count(*),2)
as "エラーログの割合"
```

現象2：小数桁の保持が不正確

類似の検索分析ステートメントを使用する場合、小数点以下2桁を最終的に保持することが期待されますが、結果には14桁が保持されます：

- 検索分析ステートメント：

```
* | select round(count_if(status>=400)*1.0/count(*),5)*100 as "エラーロ
グの割合"
```

- 結果：

```
99.99900000000001
```

原因

`count_if(status>=400)*1.0/count(*)` の結果型はdoubleです。round関数 を使用した後も結果はdoubleのままであり、さらに演算を行う際に小数桁の正確性を保証できなくなります。

解決方法

すべての演算を完了した後、最終的に小数桁数をまとめて保持します。例えば：

```
* | select round(count_if(status>=400)*100.0/count(*),3) as "エラーログの割
合"
```

©2013-2026 Tencent Cloud. 著作権を所有しています。

その他の問題

最終更新日：：2026-10-12 15:06:45

CLSとは何ですか?

CLS（Cloud Log Service）は、ワンストップのログデータソリューションを提供します。拡張や縮小などのリソース問題を気にする必要はなく、5分で迅速かつ簡単にアクセスでき、ログの収集、保存、加工、検索分析、消費配信、ダッシュボード生成、アラートなどの全方位で安定した信頼性の高いサービスを利用できます。問題の特定と指標監視の効率を全面的に向上させ、ログ運用保守のハードルを大幅に引き下げます。
CLSが主に提供する機能は以下の通りです：

- ログ収集：クロスリージョン、マルチチャネル、マルチプラットフォーム、さまざまなデータソースのログデータを便利かつリアルタイムに収集し、他のさまざまなTencent Cloud製品のログを簡単に収集します。
- ログストレージ：2つのストレージタイプ（リアルタイムストレージと低頻度ストレージ）を提供します。
- ログ検索分析：キーワードを使用してログを検索し、ユーザーが異常ログを迅速に特定するのを支援します。同時に、SQLを使用してログを統計分析し、ログ件数の時間変化傾向、エラーログ比率などの統計指標を取得できます。
- ログデータ加工：ログのフィルタリング、クリーニング、マスキング、エンリッチメント、配信、構造化を行います。
- ログ配信と消費：Tencent Cloudストレージ、ミドルウェアに配信し、ストリームコンピューティングに消費します。
- ダッシュボード：検索分析結果をカスタムDashboardにすばやく生成します。
- アラート：異常ログの秒単位アラートに対応し、電話、SMS、メール、カスタムインターフェースのコールバックなどの方法でユーザーに通知します。

CLSは1つのログをどのように定義しますか?

ログ（Log）は、アプリケーションシステムの実行中に生成される記録データです。例えば、ユーザー操作ログ、インターフェースアクセスログ、システムエラーログなどがあります。ログは通常、テキスト形式でアプリケーションシステムが配置されているマシンに保存されます。1件のシステム実行記録に対応するログは、1行のテキスト（単一行ログ）の場合もあれば、複数行のテキスト（複数行ログ）の場合もあります。
詳細な説明と例については、ログとロググループのドキュメントを参照してください。

ログはどのくらいの期間保存できますか?

CLSはログライフサイクル管理を提供します。ログトピックの作成時にログの有効保存期間を指定でき、1～3600日間の保存または永久保存に対応します。保存期間を過ぎると、データはクリアされ、ストレージ料金は発生しなくなります。

ログセットとログトピックの違いは何ですか?

©2013-2026 Tencent Cloud. 著作権を所有しています。

ログトピック（Topic）は、ログデータをCLS（Cloud Log Service）プラットフォームで収集、保存、検索、分析するための基本単位です。収集された大量のログは、ログトピックを単位として管理されます。これには、収集ルールの設定、保存期間の設定、ログの検索分析、ログのダウンロード/消費/配信などが含まれます。
ログセット（Logset）はログトピックを分類するためのものです。1つのログセットには複数のログトピックを含めることができます。ログセット自体はログデータを一切保存せず、ユーザーがログトピックを管理しやすくするためのものです。
詳細な説明と例については、ログトピックとログセットのドキュメントを参照してください。

1つのログトピックで最大何件のログを収集できますか?

大量のログ収集ニーズに対応するため、1つのログトピックには複数のトピックパーティションが含まれます。各トピックパーティションの書き込みリクエストは最大500QPS、書き込みトラフィックは最大5MB/sです。収集するログ量が多い場合は、トピックパーティションの自動分割機能を有効にすることをお勧めします（デフォルトで有効）。1つのログトピックは最大50個のパーティションを持つことができ、この場合、1つのログトピックの書き込みリクエストは最大50 * 500 = 25000QPS、書き込みトラフィックは最大50 * 5 = 250MB/sです。
ここでの書き込みリクエストと書き込みトラフィックは、単純にログ件数やログ量と等しくなるわけではありません。ログアップロード時には、複数のログが1つのロググループにパッケージ化され、圧縮されます。実際にサポートされるログ件数とログ量は、上記の制限を大幅に上回ります。Loglistenerを使用する場合、ログのパッケージ化と圧縮は自動的に行われるため、具体的なパッケージ化戦略を意識する必要はありません。

インデックスと単語分割とは何ですか?

インデックス設定は、CLS（Cloud Log Service）を使用して検索分析を行うための必要条件です。インデックスを有効にして初めて、ログの検索分析が可能になります。インデックスの作成は、実際には元のログを指定された記号で複数のセグメント（つまり分かち書き）に分割し、分かち書きに対して転置インデックスを作成するプロセスです。
詳細な説明と例については、分かち書きとインデックスのドキュメントを参照してください。

全文インデックスとキーバリューインデックスの違いは何ですか?

- 全文インデックス：全文インデックスは元のログ全体を複数のトークンに分割してインデックスを構築します。検索時はキーワードで直接検索します（つまり全文検索）。例えば、`error`と入力すると、`error`キーワードを含むログを検索することを表します。
- キー値インデックス：キー値インデックスは、元のログをフィールド（つまり key:value）ごとに複数のトークンに分割してインデックスを構築します。検索時はキー値方式で検索します（つまりキー値検索）。例えば、`level:error`と入力すると、`level`フィールドに`error`を含むログを検索することを表します。

詳細な説明と例については、インデックス設定のドキュメントを参照してください。

検索と分析の違いは何ですか?

- 検索：指定された条件に基づいて一致する元のログを検索します。例えば、`status:404`を使用して、レスポンスステータスコードが404のアプリケーションリクエストログを検索します。

©2013-2026 Tencent Cloud. 著作権を所有しています。

- 分析：検索条件に一致するログに対してSQLを使用して統計分析を行います。例えば、`status:404 | select count(*) as logCounts` を使用して、レスポンスステータスコードが404のアプリケーションリクエストログ数を集計します。

詳細な説明と例については、検索分析の概要と構文ルールのドキュメントを参照してください。

ログの検索・分析パフォーマンスはどのようなものですか?

- 検索性能：百億レベルのログに対して、秒単位で結果を返します。
- 分析性能：億レベルのログでは秒単位で結果を返し、百億レベルのログでは1分以内に結果を返します。この性能は分析に使用するSQLの複雑さに大きく依存し、SQLが非常に複雑な場合はこの性能指標を下回る可能性があります。

ログ生成から検索可能になるまでどのくらいかかりますか?

Loglistenerを使用してログを収集する場合、遅延は1分以内です。APIおよびSDKを使用してログを収集する場合、API呼び出しを開始してからログを検索できるようになるまで1分以内です。

サービスがTencent Cloud上にない場合でも、CLSを利用できますか?

使用できます。CLSはログソースに対して制限要件がありません。ログソースとCLSのサーバー間でネットワークが到達可能であれば、ログをCLSに収集できます。CLSがサポートするリージョンおよび対応するドメイン名については、利用可能なリージョン を参照してください。

サーバーのIPアドレス変更後、Loglistenerはどのように適応すればよいですか?

- サーバーがマシン識別子によってマシングループにバインドされている場合、ユーザーはLoglistenerの設定を変更する必要はありません。サーバーIPを頻繁に変更する必要がある場合は、マシン識別子を使用してマシングループを設定することをお勧めします。詳細を見る をクリックしてください。
- サーバーがIPアドレスでマシングループにバインドされている場合、ユーザーは以下の設定変更を行う必要があります：

1. Loglistenerのインストールディレクトリにある/etc/loglistener.confファイルを変更します。ここではインストールディレクトリとして/user/localを例にします：

```
vi /usr/local/loglistener-2.3.0/etc/loglistener.conf
```

2. キーボードでiキーを押して、編集モードに入ります。
3. 設定ファイル内のgroup_ip部分を変更し、変更後のIPアドレスを入力します。
4. 設定を保存してエディタを終了します。具体的な操作手順：**Esc**キーを押し、**:wq**を入力し、**Enter**キーを押します。
5. 以下のコマンドを実行して、Loglistenerを再起動します。

©2013-2026 Tencent Cloud. 著作権を所有しています。

```
/etc/init.d/loglistenerd restart
```

6. CLSコンソールにログインし、左側のナビゲーションバーで**マシングループ管理**をクリックし、このサーバーにバインドされているマシングループの設定を変更し、新しいIPアドレスで元のマシンIPアドレスを置き換え、**確定**をクリックします。

テストアラート通知チャネルのエラーまたはテストメッセージ未受信をどのように調査しますか?

ケース1：ページに「送信失敗」と表示されます
マウスを「送信失敗」に重ねると、エラーコードと詳細な失敗原因を確認できます。一般的なエラーコードは以下の通りです：

エラーコード	意味	調査方法
-1004	この通知チャネルメッセージの送信に失敗しました。	一般的には、受信対象のユーザーまたはユーザーグループに携帯電話やメールアドレスが未設定または未検証であることが原因です。ユーザーリストで確認および設定できます。
-1005	この通知チャネルでは一部のメッセージの送信に失敗しました。例えば、一部のユーザーへの送信が失敗した場合や、一部のチャネルでの送信が失敗した場合があります。	一般的には、受信対象の一部のユーザーまたはユーザーグループに携帯電話やメールアドレスが未設定または未検証であることが原因です。ユーザーリストで確認および設定できます。
-1006	カスタムインターフェースのコールバックでエラーが発生しました。	詳細な失敗原因に基づいてさらに調査してください。よくあるエラーは以下のとおりです： • invalid URI for request：有効なURLアドレスではありません。 • i/o timeout：インターフェースアクセスがタイムアウトしました。インターフェースアドレスと、パブリックネットワーク経由で直接アクセスできるかどうかを確認してください。 • callback custom error with status:xxx：インターフェース応答でエラーが発生しました。インターフェースアドレスとバックエンドサービスが正常かどうかを確認してください。

©2013-2026 Tencent Cloud. 著作権を所有しています。

		• ssrf attack：コールバックインターフェースアドレスは、パブリックネットワークから直接アクセスできるアドレスである必要があります。インターフェースアドレスがTencent Cloudのプライベートネットワークである場合、このエラーが発生する可能性があります。

ケース2：ページに「送信済み」と表示されますが、実際にはテストメッセージを受信していません

受信チャネルに応じて、一般的な原因は以下の通りです：

受信チャネル	原因
メール、SMS、電話	重複通知によるユーザーへの迷惑を避けるため、1日以内に同一ユーザーに対して同一チャネルでテストメッセージを送信できるのは1回のみです。
カスタムインターフェースコールバック（DingTalkおよびFeishuボットアドレス）	テストメッセージがDingTalkおよびFeishuのAPIインターフェース要件を満たしていないため、メッセージは無視されます。この場合、テスト通知チャネル機能は実質的な意味を持ちません。アラームポリシーでDingTalkおよびFeishuのAPI要件に従って適切なリクエストヘッダーとリクエスト内容を設定し、アラームを送信できます。
カスタムインターフェースコールバック（その他のアドレス）	CLSはHTTPレスポンスステータスコードに基づいてメッセージ送信の成否を判断します。カスタムインターフェースに、HTTPレスポンスステータスコードは正常であるものの、他の業務ロジック上の制限が存在するケースがないか確認してください。

©2013-2026 Tencent Cloud. 著作権を所有しています。