

Tencent Kubernetes Engine

TKE登録クラスターガイド

製品ドキュメント



Tencent Cloud

Copyright Notice

©2013-2023 Tencent Cloud. All rights reserved.

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

Trademark Notice



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

Service Statement

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

カタログ：

TKE登録クラスターガイド
メンテナンスガイド
ログ採集

TKE登録クラスターガイド

メンテナンスガイド

ログ採集

最終更新日：：2023-05-09 16:11:28

ここではコンソールの方式でクラスターを登録したログを[Tencent Cloud Log Service \(CLS\)](#) にアクセスさせる方法をご紹介します。

ユースケース

ログ収集機能はTKEがユーザーに提供するクラスター内のログ収集ツールです。クラスター内のサービスまたはクラスターノードの特定のパスファイルのログを [Tencent Cloud Log Service \(CLS\)](#) に送信することができます。ログ収集機能はKubernetesクラスター内のサービスログに保存と分析を行う必要があるユーザーに適用されます。ログ収集機能は各クラスターを手動で有効化して収集ルールを設定する必要があります。ログ収集機能が有効化されると、ログ収集Agentはクラスター内でDaemonSetの形式で実行し、ユーザーがログ収集ルールによって設定した収集源、CLSログトピック、ログ解析方法に基づき、収集源からログを収集し、ログ内容をログ消費側に送信します。

ご使用にあたっての注意事項

クラスターの登録が作成され、かつクラスターが登録された状態は**実行中**です。

現在クラスターが登録されたログは[Tencent Cloud Log Service \(CLS\)](#) に配信することのみサポートしており、その他のログ消費側に送信することはサポートされていません。

有効化の前にクラスターノード上に十分なリソースがあることを保証してください。ログ収集機能を有効化するとクラスターの一部のリソースが占有されます。

占有するCPUリソース：0.11-1.1コア。ログの量が大きすぎる場合は実際の状況に応じてご自身で調整できます。

占有するメモリリソース：24-560MB。ログの量が大きすぎる場合は実際の状況に応じてご自身で調整できます。

ログの長さ制限：単一で512K。それを超える場合は分割されます。

ログ収集機能を使用する場合、Kubernetesクラスター内のノードがログ消費側にアクセスできることを確認してください。TKEはパブリックネットワークおよびプライベートネットワークの2種類の方法を提供してログ配信を行い、ユーザーは業務状況に応じてご自身で選択できます。

パブリックネットワーク配信：クラスターログパブリックネットワークの方式によってCLSに配信します。クラスター内のノードがパブリックネットワークにアクセスする機能を持っている必要があります。

プライベートネットワーク配信：クラスターログはプライベートネットワークの方式によってCLSに配信されます。クラスター内のノードとCLSプライベートネットワークが相互通信している必要があります。このオプションを選択する前に、[お問い合わせ](#)によって確認してください。

概念

ログ収集Agent：TKEはログ情報を収集するAgentに使用されます。Loglistenerを採用し、クラスター内でDaemonSetの方式で実行されます。

ログルール：ユーザーはログルールを使用してログの収集源、ログトピック、ログ解析方式、設定フィルタを指定することができます。

ログ収集はAgentログ収集ルールの変化を監視します。変化したルールは最大10s以内に有効化されます。

複数のログ収集ルールでは複数のDaemonSetを作成することはありませんが、過剰なログ収集ルールはログ収集Agentが占有するリソースを増加させます。

ログソース：コンテナ標準出力、コンテナ内ファイル、ノードファイルの指定が含まれます。

コンテナの標準出力ログを収集する場合、ユーザーはすべてのコンテナ、または指定ワークロードおよび指定Pod Labels内のコンテナサービスログを選択してログの収集源とすることができます。

コンテナのファイルパスログを収集する場合、ユーザーはワークロードまたはPod Labels内のコンテナのファイルパスログを収集源として指定することができます。

ノードのファイルパスログを収集する場合、ユーザーはログの収集源をノードのファイルパスログとして設定することができます。

消費側：ユーザーはCLSのログセットおよびログトピックを選択して消費側とします。

抽出モード：ログ収集Agentは収集したログをシングルラインテキスト、JSON、区切り文字、マルチラインテキストおよび完全な正規表現の形式でユーザーが指定したログトピックに送信することをサポートしています。

フィルタ：フィルタを有効化するとユーザーが指定したルールに基づいて一部のログを収集します。keyは完全一致をサポートし、フィルタリングルールは正規表現のマッチングをサポートします。例えばErrorCode = 404のログのみを収集します。

操作手順

ログ収集の有効化

1. **TKEコンソール**にログインし、左側ナビゲーションバーの**運用保守機能管理**を選択します。
2. **機能管理**ページの上方でリージョンおよび**クラスターの登録**を選択し、ログ収集を有効化する必要があるクラスター右側の**設定**をクリックします。
3. 「機能設定」ページで、ログ収集の**編集**をクリックし、ログ収集を有効化し、**配信方式**を選択してから**OK**をクリックします。

ログルールの設定

1. **TKEコンソール**にログインし、左側ナビゲーションバーの**ログ管理** > **ログルール**を選択します。
2. **機能管理**ページの上方でリージョンおよび**クラスターの登録**を選択し、ログ収集ルールを設定する必要があるクラスターをフィルタリングし、**新規作成**をクリックします。
3. **ログ収集ルールの新規作成**ページで、収集タイプを選択し、ログソースを設定します。現在収集タイプは**コンテナ標準出力**、**コンテナファイルパス**および**ノードファイルパス**をサポートしています。

コンテナ標準出力ログの収集

コンテナ内のファイルログを収集する

ノードファイルログを収集する

コンテナ標準出力収集タイプを選択し、必要に応じてログソースを設定します。このタイプのログソースは一度に複数のNamespaceのワークロードを選択することをサポートします。下図のように表示されます

Type	Container standard output	Container file path	Node file path
Collect the container logs under any service in the cluster. Only logs of Stderr and Stdout are supported.			
Log source	All containers	Specify workload	Specify Pod labels
Namespace	default		
Target	Workload type	<input type="checkbox"/> List	

コンテナファイルパス収集タイプを選択し、ログソースを設定します。下図のように表示されます

Type	<input type="radio"/> Container standard output	<input checked="" type="radio"/> Container file path	<input type="radio"/> Node file path
Collect the file logs of specified containers in the cluster. View Sample			
Log source	<input checked="" type="radio"/> Specify workload	<input type="radio"/> Specify Pod labels	
Workload options	<input type="text" value="default"/>	<input type="text" value="Deployment"/>	
Container name	<input type="text" value="c"/>		
Collection path	<input type="text" value="Log folder. Wildcards are not allowed"/>	<input type="text" value="/"/>	<input type="text" value="Log file name (supports..."/>

ファイルパスの収集はファイルパスおよびワイルドカードルールをサポートしています。例えばコンテナファイルパスが `/opt/logs/*.log` の場合、収集パスを `/opt/logs` 、ファイル名を `*.log` として指定できます。

注意：

選択したキャプチャタイプが「コンテナファイルパス」の場合、対応する「コンテナファイルパス」をソフトリンクにすることはできず、これを行った場合はソフトリンクの実際のパスがキャプチャツール内のコンテナに存在しなくなり、ログキャプチャに失敗します。

ノードファイルパス収集タイプを選択し、ユーザーは実際のニーズに応じてカスタマイズした「metadata」を追加することができます。収集したログ情報を指定したKey-Value形式の「metadata」に追加し、追加のmetadataはログレコードに追加されます。下図のように表示されます。

注意

1つのノードのログファイルは1つのログトピックのみによって収集されます。

Type

Container standard output
Container file path
Node file path

Collect the files under the specified node path in the cluster. [View sample](#)

Log source

Collection path

Log folder (supports wildcard * ar /
Log file name (supports * and ?)

Collection path blacklist

When configuring the blacklist, you can set to ignore specific directories and files during log co
fuzzily matched with wildcards. The LogListener is required to be v2.3.9 or later versions.

When configuring the blacklist, you can set to ignore specific directories and files during log collection.

▼ Hide advanced settings

Custom metadata
Add

Each collected log carries the custom metadata information, and it is reported to the consumer.

パスはファイルパスおよびワイルドカードルールをサポートしています。例えばすべてのファイルパスを `/opt/logs/service1/*.log`、`/opt/logs/service2/*.log` の形式で収集する必要がある場合、収集パスのフォルダを `/opt/logs/service*`、ファイル名を `*.log` として指定できます。

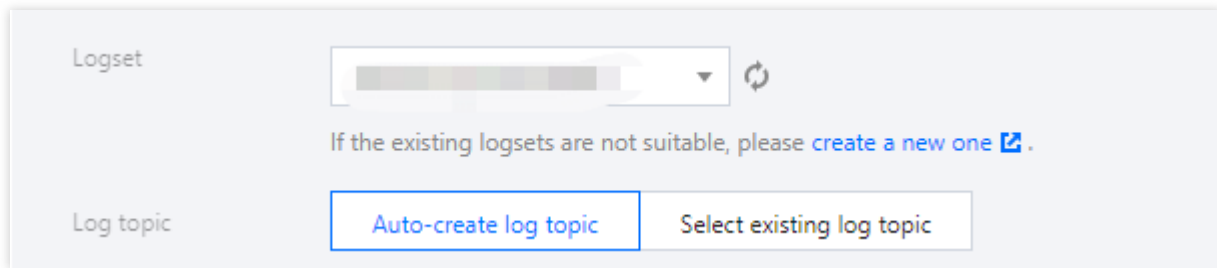
説明：

コンテナの標準出力およびコンテナ内ファイル（非hostPathマウント）については、オリジナルのログ内容以外に、コンテナまたはkubernetesに関連するメタデータ（例：ログを生成するコンテナ ID）を一緒にCLSに報告し、ユーザーがログを確認する時にソースを遡るかコンテナに識別子、特徴（例：コンテナ名、labels）に基づいて検索できるようにします。

コンテナまたはkubernetesに関連するメタデータについては下部の表をご参照ください。

フィールド名	意味
container_id	ログが属するコンテナIDです。
container_name	ログが属するコンテナ名です。
image_name	ログが属するコンテナのイメージ名IPです。
namespace	ログが属するpodのnamespaceです。
pod_uid	ログが属するpodのユーザーIDです。
pod_name	ログが属するpod名です。
pod_label_{label name}	ログが属するpodのlabelです（例えば1つのpodに、app=nginx、env=prodという2つのlabelがある場合、アップロードされたログにはpod_label_app:nginx、pod_label_env:prodという2つのmetedataが添付されます）。

4. ログサービス消費側を設定し、ログセットおよび対応するログトピックを選択し、新規作成および既存のログトピックを選択することができます。下図のように表示されます



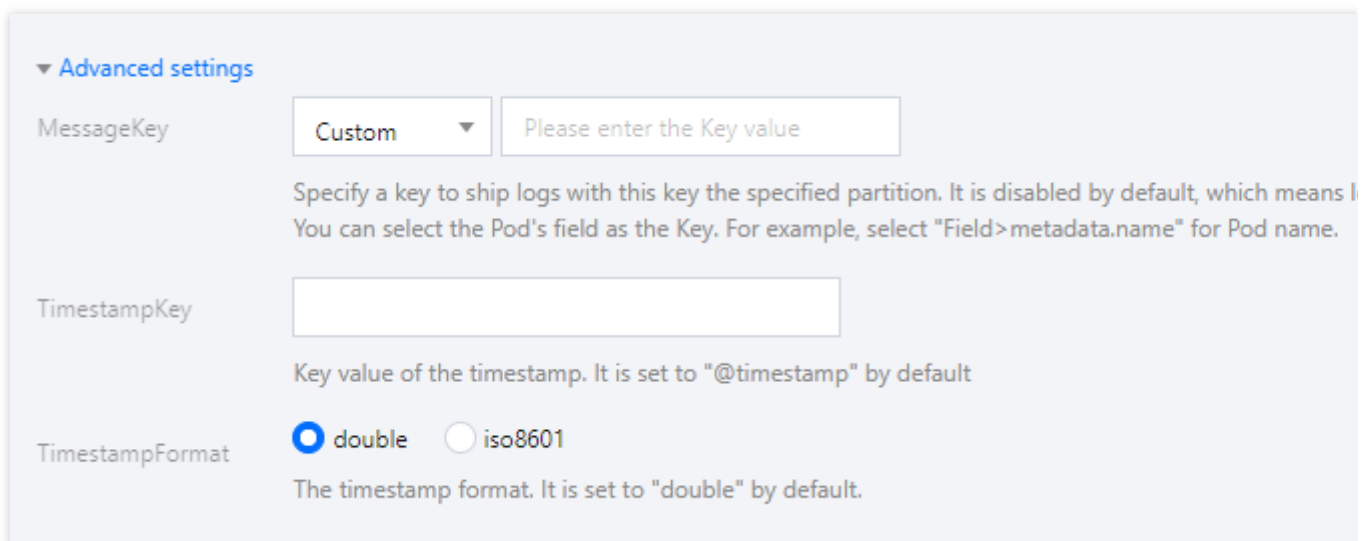
The screenshot shows a configuration panel for logs. At the top, there is a 'Logset' dropdown menu with a refresh icon to its right. Below it, a text instruction reads: 'If the existing logsets are not suitable, please [create a new one](#).' Underneath, there are two buttons for 'Log topic': 'Auto-create log topic' (highlighted with a blue border) and 'Select existing log topic'.

注意

Tencent Cloud Log Service (CLS) は現在同一リージョンのコンテナクラスターのログ収集と報告のみをサポートしています。

ログセット下に500個のログトピックが存在する場合、ログトピックを新規作成することはできません。

5. 高度な設定内でKey値を指定することによってログを指定のパーティションに配信することをサポートしています。この機能はデフォルトで有効化されず、ログはランダムに配信され、有効化すると、同じKey値を持つログは同一のパーティションに配信されます。TimestampKey（デフォルト@timestamp）の入力およびタイムスタンプ形式の指定をサポートしています。下図のように表示されます。

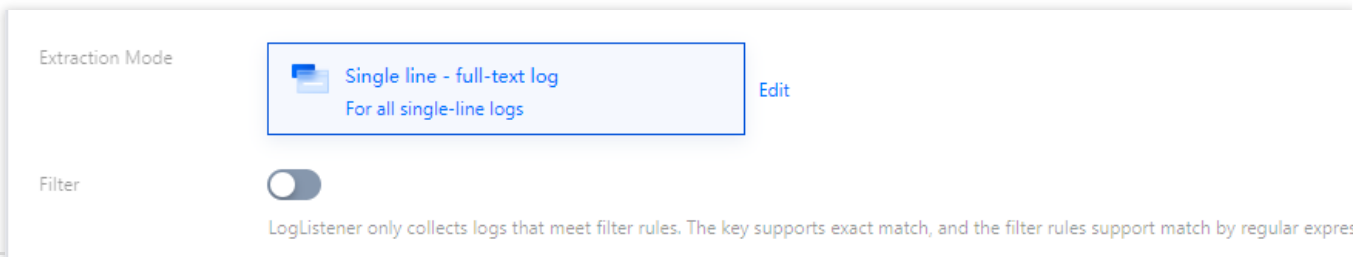


The screenshot shows the 'Advanced settings' section of a configuration interface. It includes three fields: 'MessageKey' with a dropdown set to 'Custom' and an input field 'Please enter the Key value'; 'TimestampKey' with an empty input field; and 'TimestampFormat' with radio buttons for 'double' (selected) and 'iso8601'. Below the MessageKey field, there is explanatory text: 'Specify a key to ship logs with this key the specified partition. It is disabled by default, which means l You can select the Pod's field as the Key. For example, select "Field>metadata.name" for Pod name.'

6. 次へをクリックし、ログ抽出モードを選択します。下図のように表示されます。

注意

現在CLSへの配信のみログ解析方式の設定をサポートしています。



解析モード	説明
フルテキストを1行で記入	1つのログは1行の内容のみを含み、改行コード\\nを1つのログの終了マークとし、各ログ文字列として解析され、インデックスを有効化すると全文検索によってログ内容を検索できる基準とします。
フルテキストを複数行で記入	1つの完全なログが複数行に跨がることを意味し、1行目の正規表現を採用する方式でマッチング済み設定した正規表現にマッチングした場合、1つのログの始まりであると認識します。次別子として表示されます。デフォルトのキー値CONTENTも設定され、ログ時間は収集時間自動生成をサポートしています。
シングルライン-完全な正規表現	1つの完全なログから正規表現形式で複数のkey-valueのログを抽出する解析モードを指し、次にカスタマイズされた正規表現を入力する必要があります。システムは正規表現内に対応するkey-valueを抽出します。正規表現の自動生成をサポートしています。
マルチライン-完全な正規表現	ログテキスト内の複数行にまたがる完全なログデータ（例：Javaプログラムログ）に適用されるkey-valueキー値のログ解析モードを抽出します。まずログサンプルを入力し、次にカスタマイズする必要があります。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の自動生成をサポートしています。
JSON	JSON形式のログは、第1階層のkeyに対応するフィールド名として自動的に抽出します。第2階層の値とします。このような方法によりログ全体の構造化処理を行い、それぞれの完全な識別子とします。
区切り文字	1つのログデータは指定した区切り文字に基づいてログ全体に構造化処理を行い、それぞれを終了識別子とします。ログサービスが区切り文字形式のログ処理を行う時に、各個別のログを構造化する必要があるため、無効フィールド、すなわち収集する必要がないフィールドは空欄を埋める必要があり、フィールドが空であることはサポートしていません。

7. 必要に応じてフィルタを有効化してルールを設定し、完了をクリックすれば、作成が完了します。下図のように表示されます

Filter

LogListener only collects logs that meet filter rules. The key supports exact match, and the filter rules support match by regular expression. Fo

Key	Filter Rule
__CONTENT__	<input type="text" value="Enter content"/> Input cannot be empty

ログルールの更新

1. [TKEコンソール](#)にログインし、左側ナビゲーションバーの[ログ管理](#) > [ログルール](#)を選択します。
2. [ログ収集](#)ページの上方でリージョンおよびクラスタの[登録](#)を選択し、ログ収集ルールを更新する必要があるクラスタをフィルタリングし、右側の[収集ルールの編集](#)をクリックします。下図のように表示されます。

Create

Name	Type	Consumer type	Withdrawal mode	Time created
xxx	Container standard output	CLS	-	2023-02-06 17:12:0

3. 必要に応じて対応する設定を更新し、[完了](#)をクリックし、更新を完了します。

注意

ログセットおよびログトピックは更新できません。

関連ドキュメント

[YAMLでCRDを使用してログ収集を設定する](#)