

Elasticsearch Service

ES Serverless Guide

Product Documentation





Copyright Notice

©2013-2025 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

STencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by the Tencent corporate group, including its parent, subsidiaries and affiliated companies, as the case may be. 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.

Contents

ES Serverless Guide

Service Overview

Basic Concepts

5-Minute Quick Experience

Quick Start

Creating Indexes

CVM Log Access

TKE Log access

Elastic MapReduce log access

TCHouse-D Cluster Log Access

Customizing Filebeat Data Access

Access Control

Writing Data

Data Query

Index Management

Configuration Management

Alarm Management

ES API References

Related Issues

Kibana Usage Issues

Third-Party Cookie Settings

Field Type Conversion Through Reindex

ES Serverless Guide Service Overview

Last updated : 2024-08-20 16:57:46

Industry Challenges

When using open-source Elasticsearch for log analysis, users often need to estimate cluster configuration based on write traffic, peak write, and storage days, including CPU, memory, and disk size, to ensure smooth business operation. However, as per extensive online operational experience, this method has the following problems: Elastic capability is difficult to adapt to business development. In scenarios such as big promotions and holidays, log data presents obvious peak and trough effects, high write throughput, and high availability requirements, and it is impossible to predict sudden read-write traffic and scale out a cluster in advance, making it difficult to ensure the stability of the Elasticsearch cluster.

Resource costs are high. Insufficient resources affect traffic write during peak periods, and planning cluster capacity based on peak traffic results in resource redundancy and waste during off-peak periods, leading to high costs. Operations and management costs are high. Enterprises need to plan and configure clusters and indices, and build monitoring and alert platforms. Moreover, enterprises have a strong demand for optimizing Ops and management costs with the focus on cost reduction and efficiency improvement, aiming to further reduce these expenses.

Overview

Elasticsearch Serverless service is a one-stop, fully managed Elasticsearch service built by Tencent Cloud based on its proprietary cloud-native Serverless technology architecture. It offers automatic scalability and a completely maintenance-free product capability, effectively addressing the problems of high resource costs caused by peaks and troughs in log analysis, metric monitoring, and other business scenarios. Meanwhile, it is fully compatible with the ELK ecosystem, featuring end-to-end data access, data management, and data visualization product features, providing an out-of-the-box product experience.

At the Enterprise Cloud Adoption and Cloud Computing Integration Industry Conference held on March 29, 2023, Tencent Cloud Elasticsearch Serverless service was awarded the "2022 Trusted Computing Power Service · Leadership Plan" Excellent Case Award.

Benefits and Features

Auto Scaling: It features automatic index-level AS to smoothly handle unexpected traffic growth, reducing high Ops and management costs during peaks and troughs in scenarios like log analysis and observability while ensuring business continuity.

Completely Ops-free: Built-in automatic sharding optimization, intelligent lifecycle management, and failures selfhealing capabilities allow users to create and use indices as needed without worrying about underlying resource configuration, cluster scaling, and index settings, ensuring a completely Ops-free experience.

Cost-saving: Self-developed, low-cost, high-performance, and high-availability storage-compute separation architecture charges based on actual access and storage volumes, enabling pay-as-you-go in the scenario of dynamic matching of service load and resources. This reduces redundant cost expenditures due to idle resources, significantly lowering costs.

Flexible and easy to use: It provides end-to-end one-stop product capability featuring data access, data management, and data analysis and exploration, significantly lowering the barrier to business cloud adoption. Users can achieve minute-level business implementation.

Open integration: It is fully compatible with the ELK ecosystem and retains users' original usage habits, ensuring seamless migration and facilitating rapid cloud adoption. Meanwhile, it connects cloud data sources (such as CVM and TKE) to lower the data access threshold, achieving minute-level business implementation.

Stable and reliable: Cluster configuration and read-write performance are optimized by the backend, reducing fault issues caused by improper use, enhancing stability, and safeguarding business operations.

Contact Us

Scan the code to join Tencent Cloud Big Data Elasticsearch Serverless community group, with occasional activities and exquisite gifts.



Basic Concepts

Last updated : 2024-12-04 15:51:12

This document introduces the basic concepts related to the project space and index in the ES Serverless service.

Project Space

A project space is the basic resource unit in the ES Serverless service. You can create indexes for the same business within a single project space to facilitate index management. To read and write data, use the access address, username, and password for the project space to access the indexes within it.

Index

In the ES Serverless service, an index is the smallest unit for data storage and management. It leverages Tencent Cloud ES's proprietary self-managing index capabilities, including built-in shard auto-optimization, intelligent lifecycle management, and fault self-recovery. Unlike traditional usage methods, you do not need to worry about index rollover or shard size; instead, you can focus solely on data writing, querying, and visual analysis.

Upgrade Notes:

The ES Serverless service has been upgraded to improve user experience, and currently supports unified access addresses and Kibana for managing and accessing multiple indexes, aligning better with traditional usage habits. The differences before and after the upgrade are as follows:

The project spaces created before January 23, 2024, lack independent access control and do not support simultaneous access to multiple indexes in Kibana. Data writing and querying are performed through each index's access address.

For the project spaces created after January 23, 2024, unified management and access for all indexes within the space can be achieved through the project space's access address and Kibana. Additionally, permissions can be configured through a visualized user management feature, allowing you to set permission types and scopes, aligning closely with traditional ES cluster usage to meet various scenarios. The upgrade requires no changes to business code -- simply migrate existing indexes to the new space. We strongly recommend migrating indexes to the new space.

5-Minute Quick Experience

Last updated : 2024-12-04 15:56:05

Overview

The ES Serverless service is a fully managed, cloud-native ES service by Tencent Cloud, built on a self-developed Serverless architecture with no cluster concept. Users can create and use indexes as needed, benefiting from **autoscaling and completely maintenance-free** capabilities, which effectively solve the issue of high resource costs associated with peak and off-peak fluctuations in **log analysis and metric monitoring** scenarios. Fully compatible with the ELK ecosystem, it provides end-to-end data writing, data management, and data visualization features, providing a **plug-and-play log analysis experience**.

Quick Start

The ES Serverless service supports writing data into indexes through methods such as **native ES APIs, Logstash**, **Flink, or Kafka**. If you require log collection for services such as CVM, TKE, or TCHouse-C, a one-stop visualized configuration option is also available. By simply setting up data sources and index information, logs can be collected into indexes for efficient retrieval and analysis. This document will guide you through the full process of **index creation > data writing > retrieval and analysis**, giving you a quick overview of using the ES Serverless service in log analysis scenarios.

Basic Concepts

Before diving into the experience, let us review several relevant basic concepts:

Name	Description
Project space	Project space is a fundamental resource unit in the ES Serverless service. You can create indexes related to the same business within a single project space, facilitating index management.
Index	Index is the smallest unit for data storage and management, providing log storage and near real- time query capabilities. Collected log data can be stored in indexes.
Kibana	Kibana is a data analysis and visualization platform integrated with ES, allowing for log writing, retrieval, and chart creation (such as maps and line charts).
Logs	Logs are records generated during the operation of application systems, including operation logs, access logs, and error logs.

Creating a Space

1. Log in to the ES Serverless console.

2. In the space list, click **Create Project** to enter the project creation page.

3. On the project creation page, configure the following settings:

Project Name: Use this name to identify the project. Follow the naming guidelines provided on the page.

VPC / AZ and Subnet: The project space is created within a VPC to ensure secure access. Select the appropriate

VPC, availability zone, and subnet. if creation is needed, see Create New VPC and Create New Subnet.

Project s same bus	pace is a logical business classification con- iness type in the same project space for jo	cept,You can place logs of the bint analysis.
Region *	🔇 Guangzhou	▼
Project Name *	Supports Chinese characters, letters, di	gits, underscores (_), and
VPC *		✓ ^C
AZ and subnet *	Guangzho 🖌 Select a s	subnet 🗸 🖌
	Subnet change is not supported after Pro can proceed to create a subnet	oject is successfully created. You

4. After completing the information, click **Confirm** to create the project.

Creating an Index

There are two methods to create an index: directly from the Project list page or from the Project Basic page. The following example demonstrates the process on the Project list page.

1. On the Project list page, enter the Quick Access Data page and select your data source. Here, we will use API write as an example.



Cluster Migration		
Self-built ES cluster migration	Tencent Cloud ES cluster migration	
Cloud Product Integration		
© CVM	TKE	
EMR	TCHouse-C	
TCHouse-D	Cceanus	
Custom Integration Create new indexes on	у	
Python SDK write	Java SDK write	

2. Review the writing prompts, then click Next.

1 Data Source > 2 Index Settings	
Description	
ES Serverless supports data write, query, and management using flexible APIs. About Write	
View 🖻	
Next Cancel	

3. On the Index Settings page, enter the basic information and index configuration, then click **Create**.

Region: Select the regional information from the dropdown list.

Project: Choose the project space to organize the index for easier management. If no options are available in the dropdown, click **Create Project** and follow the previous instructions to create one.

Index name: This name will be used for subsequent data writing and querying. Follow the naming prompts shown on the page.

Field mapping: Used to set the field details of the data. You can select **Dynamic creation**, which will automatically generate field settings based on the data you write in, or choose to customize the field settings.

Time field: Select or input a field with a date type from your data. Once the index is created, this field cannot be modified.

Data retention period: The retention period of the data. For example, if it is set to **Limited 30 days**, data will be deleted on the 30th day after being written to the index.

Basic info	
Region *	🔇 Guangzhou 🔻
Project *	futu02(space-0rt1p8yh) 🗸
	If the existing project does not meet your requirements, you can click Create Project
Index name *	Enter an index name - Ort1p8yh
Index configuration	rollover and alias but just specify the index name for read/write operations.
Field mapping	O Dynamic creation Custom
Time field *	Specify the time field
	The time field refers to the date field in the data. This field records the data creation time and cannot be modified after the index is created.
Data retention period	O Limited − 30 + day(s) Permanently stored

Data Writing

1. In the project list, click the name of the desired project to enter the Project Management page.

Note:

Kibana's relevant modules are embedded directly into the Tencent Cloud Console, allowing you to use search and analysis features directly. **Search and Analysis** corresponds to **Discover**, and **Development Tools** corresponds to **Dev Tools**. This embedded feature requires third-party cookies to be enabled in your browser; if you experience issues, please enable third-party cookies. To access Kibana externally for data writing, see Writing Data. Enter the **Development Tools** page.

History Settings Help	
⊘ Log Analysis 1 SET zwu11_0rt1pgub/ search N 0 1	
Alarm 2 + { Management 4 "match_all": {}	
Development Tools	
Workspace Management	
i⊟ Index list	
Access Management	
O Usage Statistics	
Departion Record	

Enter the following statement and click the triangle icon to write data. Each click counts as one data entry (the content within {} represents a complete log entry). You may click several times to generate enough entries for the upcoming data retrieval demonstration.

Data Analysis	History Settings Help	201 - success 361 m
 Log Analysis 	1 GET zxw11-0rt1n8vh/ search	1 + 1
Alarm Management	2 * { 3 * "query": { 4 "match_all": {}	<pre>2 "_index" : ".ds-zxw11-0rt1p8yh-2024.04.19-000001</pre>
 Development Tools 	6 * } 7 8 POST zxw11-0rt1p8yh/_doc	<pre>5 "_version" : 1, 6 "result" : "created", 7* "_shards" : { 8 "total" : 2.</pre>
Workspace Management	10 "id":"090798", 11 "routing_no":"4087",	9 "successful": 2, 10 "failed": 0
i≣ Index list	12 "region":"10002424", 13 "user_name":"user-Ufa9Yee1P", 14 "user_tyne":"01"	11* }, 12 "_seq_no": 0, 13 " primary term": 2
Access	15 "ip":"119.147.10.191",	14 * }
Management	16 "now_local":"gz", 17 "@timestamp":1705648983762	15
O Usage Statistics	18 * }	
Depration Record		

Sample statement:

POST	index name/_doc
{	
"	id":"090798",
"	routing_no":"4087",
"	region":"10002424",
"	user_name":"user-Ufa9Yee1P"
"	user_type":"01",
"	ip":"119.147.10.191",
"	now_local":"gz",
"	@timestamp":1705648983762
}	



Note:

Replace **Index Name** in the statement with your specific index name. If your time field is not **@timestamp**, modify **@timestamp** in the figure to match your custom time field. For batch data entries, see Writing Data.

Retrieval and Analysis

With the data successfully written into the ES Serverless service, the following steps demonstrate how to query this data.

Method 1: Using DSL

1. Copy the example statement below and click the triangle icon to execute a query on the written data.

```
GET index name/_search
{
    "query":{
        "match_all":{}
      }
}
```



2. The returned result below indicates that the data was successfully queried.



Data / trialyolo	History Settings Help		200 - success 102
O Log Analysis	1 GET zxw11-0rt1p8vb/ search	D ② 1 -	{
O Alarm	2 * {	2	"took" : 20,
Alarm	3 • "query": {	3	"timed_out" : false,
Management	4 "match_all": {}	4 -	"_shards" : {
	6 * }	6	"successful" : 1.
	7	7	"skipped" : 0,
lools	<pre>8 POST zxw11-0rt1p8yh/_doc</pre>	8	"failed" : 0
	9 * {	9 *	},
Workspace Management	11 "routing no":"4087".	10 -	"total" : {
· · · · · · · · · · · · · · · · · · ·	12 "region":"10002424",	12	"value" : 1,
:= Index list	<pre>13 "user_name":"user-Ufa9Yee1P",</pre>	13	"relation" : "eq"
P Access	14 "user_type":"01",	14 *	}, """" 1.0
Eq Access	16 "now local":"gz".	16 -	max_score : 1.0, "hits" : [
Management	17 "@timestamp":1705648983762	17 -	{
	18 * }	18	"_index" : ".ds-zxw11-0rt1p8yh-2024.04.19-000001",
G Usage Statistics	19	19	"_type" : "_doc",
Operation Record		20	_id : vgb5j2EB6mpVQIGLDPK_ , "score" : 1.0.
Eg operation record		22 -	source" : {
		23	"id" : "090798",
		24	"routing_no" : "4087",
		25	"region" : "10002424", "user name" : "user-lifa9Vee1P"
		27	"user type" : "01".
		28	"ip" : "119.147.10.191",
		29	"now_local" : "gz",
		30	"@timestamp" : 1/05648983/62
		32 *	}
		33 *	
		34 *	}
		35 *	}

Method 2: Using Discover

1. Click Log Analysis, and select the index just written from the index drop-down list.

Data Analysis				
O Log Analysis	Search		KQL Last 15 minutes	Show dates C Refresh
🙆 Alarm	🗇 - + Add filter			
Management				
Oevelopment	zxw11-0rt1p8yh 🗸	→ •••	No results match your search criteria	
Tools	Q Search field names		g no results inden your search entend	
Workspace Management				
≔ Index list	Filter by type 0	\sim	Expand your time range	
	\checkmark Available fields	0	One or more of the indices you're looking at contains a day	te field. Your query may not match anything
Access Management			in the current time range, or there may not be any data at	all in the currently selected time range. You
management			can try changing the time range to one which contains da	ta.
 Usage Statistics 				
Operation Record				

2. Filter by time. Since the written data is from **January 2024** in this example, select **a year ago** to successfully retrieve data from the past year.



3. You can also enter keywords to retrieve content that matches specific criteria. For example, if you want to retrieve entries where the field **now_local** has the value **gz**.

Click now_local as shown below:

Data Analysis								
O Log Analysis		Sea	rch				KQL	C Refres
🛆 Alarm	; = +	۵	_id		Filter results that contain _id			
Management		G D	_index		Filter results that contain _index	x		
> Development		Ð	_type		Filter results that contain _type			Hide char Hide cha
Tools	Q :	G D	@timestamp		Filter results that contain @times	stamp		
orkspace Management		G D	id		Filter results that contain id			
Index list	Filter	Ð	ip		Filter results that contain ip			
A00005	√ Av	G D	now_local		Filter results that contain now_lo	ocal		
Management	t_id	G D	region		Filter results that contain region	n	14-07-01	2024-08-01
) Usage Statistics	t_in	Ð	routing_no		Filter results that contain routin	ng_no	.4 07 01	2024 00 01
Operation Report	# _30	۲	user_name		Filter results that contain user_r	name		
Operation Record	💼 @t	۲	user_type		Filter results that contain user_1	type	_	
	t id			>	Jan 19, 2024 @ 15:23:03.762	@timestamp: Jan 19, 2024 @ 15:23:03.762 id: 090798	p: 119.14	7.10.191
	t ip					user_type: 01 _id: Vgb5jZEB6mpVQTGiDPRindex: .ds	-zxw11-0rt	lp8yh-
	t no	w_loca	al			2024.04.19-000001 _score:type: _doc		
	t reç	jion						
	t rou	iting_r	no					
	t us	er_nar	ne					
	t us	er_typ	e					

Select : as shown below:



Enter gz and click **Refresh**. All entries with the **now_local** field value of **gz** will be highlighted, as shown below:



For more details on data retrieval and analysis methods, see Data Query.

Quick Start Creating Indexes

Last updated : 2024-12-04 15:59:13

Prerequisites

A Tencent Cloud account has been created. For account creation, see Signing Up. If logging in with a sub-account, ensure that the account has read and write permissions for ES.

Operation Steps

Logging In to Console

1. Log in to the Elasticsearch console.

2. In the top menu bar, select the region. Currently supported regions include Beijing, Shanghai, Guangzhou, Nanjing, Hong Kong (China), Singapore, Tokyo, and Virginia.

3. In the left sidebar, choose Log Analysis under the Serverless mode.

Creating a Project Space

1. Click Create Project.

2. Enter the project space name, which can include 1 - 20 characters, including Chinese characters, letters, digits, underscores, or delimiters (-).

3. Click **Confirm**. Once validated, the project space will be created.

i Project s same bus	pace is a logical busines siness type in the same	s classification concept,You can pla project space for joint analysis.	ace logs of the
Region *	🔇 Guangzhou		•
Project Name *	Supports Chinese ch	aracters, letters, digits, underscore	es (_), and
VPC *			 ✓ ✓
AZ and subnet *	Guangzho	✓ Select a subnet	*
	Subnet change is not s can proceed to create a	supported after Project is successfu a subnet ^{[2}	ully created. You

Note

In Elasticsearch Serverless Log Analysis, you can create an index and subsequently write data via API or access data sources such as CVM and TKE via the Data Access tab of the corresponding index. You can also set up data access during index creation, enabling one-stop access for CVM Log Access, TKE Log Access, and more. The following section explains the index creation process for API-based data writing.

Creating an Index

1. On the ES Serverless Log Analysis homepage, click the **Project Name** to enter the Index List page, then select **Create Index And Integrate Data.**

Data Analysis	Create Index And Integrate [Data		Search by	/ index name, index	ID, or index ta	ıg. Separate multiple keywords w		(
 Log Analysis 	Index Name/ID	Search and A	Index status	Usage Statistics \$	Storage Dura	Tag 🍸	Data Source 🝸	Creatio ‡	Operation
Alarm Management	1000	Q	Normal	Traffic: 0.00 B (yesterday) Storage: 0.00 B (total)	30 day(s)	⊘ 2	TKE cls-irk7xegg	2024-07-15 14	Data Access More
Oevelopment Tools	10.00	Q	Normal	Traffic: 0.00 B (yesterday) Storage: 108.00 B (total)	30 day(s)	\bigtriangledown	Custom Integration	2024-04-19 10	Data Access More
Workspace Management	Total items: 2						10 💙 / pa	ige 📕 🖣	1 / 1 page
Access Management									
O Usage Statistics									
Deration Record									

2. On the create index page, select API writing.

luster Migration	
▲ Self-built ES cluster migration	Tencent Cloud ES cluster migration
Cloud Product Integration	
O CVM	(TKE
EMR	TCHouse-C
TCHouse-D	Cceanus
Custom Integration Create new indexes on	ly
🚱 Python SDK write	Java SDK write

3. If you want to view how to write data to ES Serverless via API, click View Documentation. Then, click Next.

1 Data Source	> 2 Index Settings		
Description			
ES Serverless supports data	write, query, and management using flexible ,	APIs.	
About Write			
Next Cancel			

4. Enter the index settings page and fill in the basic information.

Region: Aligns with the region of project space.

Project Space: Defaults to the current project space.

Index Name: Length of 1 - 100 characters. Lowercase letters, digits, and the following symbols: -, _, ;, @, &, =, !, ', %, \$, ., +, (,) are supported.

Basic IIIIU		
Region *	S Guangzhou	v
Project *		- C
	If the existing project does not meet your requirements, you can click Create	Project
Index name *	Enter an index name	- 0rt1p8yh
Index configuration	Built-in shard auto-tuning, smart rollover, and other proprietary features are name for read/write operations.	provided. You do not need to care about complex operations such as index rollover and alias but just specify the inde
index configuration		
Field mapping	Dvnamic creation Custom	
Field mapping Time field *	Dynamic creation Custom Specify the time field	
Field mapping Time field *	Dynamic creation Custom Specify the time field The time field refers to the date field in the data. This field records the data c	reation time and cannot be modified after the index is created.

5. Fill in index configuration details.

Field Mapping

Dynamic Generation: Enabled by default. When enabled, it automatically parses written data and generates field settings for the index.

Input Sample Auto-Configuration: If Dynamic Generation is disabled, you can use Input Sample Auto-

Configuration to generate field mappings for the index by entering a JSON-formatted data sample. After

confirmation, the platform will validate the input; if the validation is successful, the relevant fields will be mapped in the field mapping table.

Field mapping divides the original data into multiple tokens based on fields (key:value) for indexing. Retrieval relies on this mapping, as detailed below:

Parameter	Description
Field name	The field name in the written data.
Field type	The data type of the field. The interface supports 9 types: text, date, boolean, keyword, long, double, integer, ip, and geo_point. Additional field types are supported in JSON mode . For details, see Official Documentation.
Includes Chinese	Enable this option if the field includes Chinese text and requires Chinese retrieval. When it is enabled, the ik_max_word tokenizer is applied to the text field by default.
Enable indexing	When it is enabled, this field will be indexed for search.



Enable	When it is enabled, this field's values can be analyzed statistically, which will increase index
statistics	storage.

Time Field

The time field refers to a field with the type date in the actual data. Once the index is created, this field cannot be modified.

Note:

By default, the time field enables **indexing** and **statistics**, and these settings cannot be disabled.

Data Storage Duration

You can set the data retention period, with a default of 30 days, or select an option for permanent storage.

Basicillo	
Region *	🔇 Guangzhou 💌
Project *	 C
	If the existing project does not meet your requirements, you can click Create Project
ndex name *	Enter an index name - Ort1p8yh
	Built-in shard auto-tuning, smart rollover, and other proprietary features are provided. You do not need to care about complex operations such as index rollover and alias but just specify the index name for read/write operations.
Index configuration	Change to JSON
Field mapping	O Dynamic creation Custom
Time field *	Specify the time field
	The time field refers to the date field in the data. This field records the data creation time and cannot be modified after the index is created.

6. Once the information is entered correctly, click **Create** to complete the index creation. For the instructions on data writing, see documentation.

CVM Log Access

Last updated : 2024-12-04 16:01:35

Prerequisites

A Tencent Cloud account has been created. For account creation, see Signing up for Tencent Cloud. If logging in with a sub-account, ensure that the account has read and write permissions for ES.

Operation Steps

Logging in to the Console

1. Log in to the Elasticsearch Console.

2. In the top menu bar, select **Region**. Currently supported regions include Beijing, Shanghai, Guangzhou, Nanjing, and Hong Kong (China).

3. In the left sidebar, choose Log Analysis under the Serverless mode.

Creating a Project Space

1. Click Create a project.

2. Enter a **Project Name** for the project, which can include 1–20 characters, consisting of Chinese characters, letters, digits, underscores, or delimiters (-).

3. Click **Confirm**. If the validation is successful, the project space will be created.

 Project s same bu 	pace is a logical business classification concept,You can siness type in the same project space for joint analysis.	place logs of the
Region *	🔇 Guangzhou	
Project Name *	Supports Chinese characters, letters, digits, undersc	ores (_), and
VPC *		 C
AZ and subnet *	Guangzho ✓ Select a subnet	 C
	Subnet change is not supported after Project is succes can proceed to create a subnet 	ssfully created. You

In ES Serverless Log Analysis, you can simply create an index, then use the API for data writing or access data sources such as CVM or TKE via the Data Access tab of the corresponding index. You can also set up data access during index creation for one-stop CVM and TKE log access. The following introduces the one-stop CVM log access process.

CVM Log Access

On the ES Serverless Log Analysis homepage, select CVM to enter the CVM Log Access page.

luster Migration	
Self-built ES cluster migration	Tencent Cloud ES cluster migration
oud Product Integration	
O CVM	🗊 тке
EMR	TCHouse-C
TCHouse-D	Cceanus
ustom Integration Create	new indexes only

Data Source Settings

Region: Required. It represents the region where the CVM is located.

VPC: Required. It represents the private network where the CVM is located. After confirmation, the servers under this VPC will be pulled in.

Select CVM: Select the CVM instance for log collection. Currently, only Linux-based CVMs are supported, and data collection requires Installing TAT Agent.

Collection Path: Set the log directory and file names based on the location of logs on the server. Supports one or more paths. Directory and file names can be specified using exact names or wildcard patterns.

Region *	🔇 Guangzł	hou				~					
VPC *						▼ ¢					
Select CVM 🛈				φ		Selected (1)					
Searching by CVM	instance IDs/insta	nce names/instan	ce tags is supp	orted. Q		Fuzzy search	n by CVM insta	nce IDs or instan	ce names is sup	ported.	
CVM Insta	IP Address	Operating system (j)	Collecto	TencentCloud Automation Tools (j)		CVM In	IP Addr	Operating system (j)	Collecto	Collector Run	
Unnamed Tag 🔊	Public netw Private net	TencentOS	Not insta	Installed	\Leftrightarrow	Unnamed Tag 💽	Public n Private n	TencentOS	Not insta	-	6
<u> </u>											
Collection Path *	/										
	+ Add Path										

Collection Settings

Basic Settings

Collection policy: Supports both full and incremental collection. Once created, the collection policy cannot be modified. Full collection gathers historical log files as well as any logs generated after the Filebeat configuration takes effect; incremental collection only gathers logs generated after the Filebeat configuration takes effect.

Collection and Parsing

Collection Template: If you need a quick setup or trial, select a collection template based on your log output format. After confirming, you can return to the interface and replace the log sample with actual log data to quickly complete the collection parsing setup.

🗸 Data Se	rce > 2 Collection Settings > 3 Index Settings	
Basic Settings		
Collection Policy	Full Collection Incremental Collection	
Collection and	rsing For quick setting, it is recommended to use the collection template.	
Collection Mode	Single Line Multiple Lines	
Extraction Settings	Extraction Image: Second s	
Back	Next Cancel	

Collection Mode: Supports single-line and multi-line modes. Once created, the collection mode cannot be modified. Single-line text log: Each line in the log file represents one log entry, with each log separated by a line break. Multi-line text log: Each log entry consists of multiple lines, such as Java stack trace logs. In this mode, you need to configure a log sample and a line-start regular expression. Filebeat uses the line-start regular expression to identify the beginning of each log entry, treating unmatched parts as part of the current log until the next line start appears. After you enter a log sample, the system automatically generates a line-start regular expression by default. You can also customize the expression, with highlighted content in the input box indicating the matched line-start information. **Note:**

Be sure to use logs from the actual scenarios to facilitate automatic extraction of the line-start regular expression.

Collection and F	Parsing F	For quick setting, it is recommended to use the collection template.
Collection Mode	Single Line	Multiple Lines
Line Header Settings	Sample Log	<pre>1 [2023-09-0100:00:00,000][INF0]java.Lang.Exception:exception.happened 2at.TestPrintStackTrace.f(TestPrintStackTrace.java:1) 3at.TestPrintStackTrace.g(TestPrintStackTrace.java:3) 4at.TestPrintStackTrace.main(TestPrintStackTrace.java:5)</pre>
		Highlighted content is the line header information matched by the regular expression.
	Regular Expression	Automatic Generation O Custom
	for Line Header Match	^\[\d+-\d+:\d+:\d+:\d+\]\(\w+\]\w+\.\w+\.\w+:\w+.\w+: *

Extraction Settings: You can set the extraction mode to full text log, JSON format, or delimiter. Once created, the extraction mode cannot be modified. Details are as follows:



Full Text Log

JSON Format

Delimiter

No key-value extraction is performed on log data, and log content is stored in a field named message. You can perform retrieval and analysis using automatic word segmentation.

For example, a single-line log entry in its original format might be:

Tue Jan 01 00:00:00 CST 2023 Running: Content of processing something

The data collected in the index would be:

massage:Tue Tue Jan 01 00:00:00 CST 2023 Running: Content of processing
something

For logs in standard JSON format, fields can be extracted based on the Key: Value pairs within the log.

Suppose your original JSON log entry is:

{"pid":321,"name":"App01","status":"WebServer is up and running"}

After structuring, this log entry will be transformed as follows:

```
{
    "pid":321,
    "name":"App01",
    "status":"WebServer is up and running"
}
```

For logs with content separated by a fixed delimiter, you can extract key-value pairs based on the specified delimiter. The delimiter can be a single character or a string and can be selected or entered in the console.

Suppose your original log entry is:

321 - App01 - WebServer is up and running

By specifying the delimiter as -, this log will be split into three fields. You can define a unique key to these fields in the extraction results, as shown below:

```
pid: pid
name: App01
status: WebServer is up and running
```

Extraction Results: If the extraction mode is set to JSON format or delimiter, you can enter a log sample, and the system will automatically extract information from it:

For JSON format, the system will automatically populate the extracted Key-Value pairs. If you deselect a field, it will not be written to the index.

For delimiter mode, the system will automatically populate the extracted Values. You can define a unique Key for each Value. If you deselect a field, it will not be written to the index.

Built-in fields: When you configure CVM log collection in the console, Filebeat writes information such as log source and timestamp into the logs as Key-Value pairs. These fields are considered built-in. If a Key name in your business log matches a built-in field name, the content from the business log field will take priority, and the corresponding builtin field will not be written to the index. The meanings of the built-in fields are as follows:

Built-in Field Name	Meaning
log.file.path	Path where the log is stored
host.name	Name of the server hosting the log
host.ip	IP address of the server hosting the log
@timestamp	Time when the log entry was collected



Sample Log *	1 321_App01_WebServer is up and running	
Extraction +	2 fields are subjected from the sample log shour. Click to undate the autoration result	
Result	5 fields are extracted from the sample log above. Click to update the extraction result	
	✓ Key	Value
	🔽 pid	"321"
		"App01"
	- Hane	Appor
	_	
	Status	"WebServer is up and running"
	Built-in Field log.file.path	Example: "/var/log/fun-times.log"
		energies (est, seg, est anneale g
	Built-in Field host.name	Example: "vm_test1"
	Built-in Field host.ip	Example: "192.168.0.1"
		·
	Ruilt-in Field @timestamp	
	M Duit in rieu Wunestamp	Example: "2016-05-23T08:05:34.853Z"
	It a key is unchecked, the corresponding field will not be written to the index.	

Preserve original logs: When it is selected, the original log content prior to parsing will be retained in this field. **Record parsing errors**: If the extraction mode is set to Delimiter, you can choose whether to log parsing errors. When it is selected, error messages will be uploaded to this field as values in case of parsing failures.

Index Settings

Project Space: You can assign indexes for the same business to a specific project space for easier management. **Index Name**: Length of 1 - 100 characters. Lowercase letters, digits, and the following symbols: -, _, ;, @, &, =, !, ', %, \$, ., +, (,) are supported.

Field Map

Dynamic Generation: Enabled by default. When enabled, it automatically parses and generates field settings for the index based on written data.

Input Sample Auto-Configuration: When Dynamic Generation is disabled, you can use Input Sample Auto-

Configuration to generate field mappings for the index by entering a JSON-formatted data sample. After confirmation, the platform will validate the input; if the validation is successful, the relevant fields will be mapped in the field mapping table.

Field mapping divides the original data into individual tokens based on fields (key:value) for indexing. Retrieval relies on this mapping, as detailed below:

Parameter	Description
Field name	The field name in the written data.
Field type	The data type of the field; the interface supports 9 types: text, date, boolean, keyword, long, double, integer, ip, and geo_point. Additional field types are supported in JSON Editing Pattern . For more details, see Official Documentation.
Include Chinese	Enable this option if the field contains Chinese text and requires Chinese retrieval. When it is enabled, the ik_max_word tokenizer is applied to the text field by default.
Enable indexing	When it is enabled, an index will be built for this field, allowing it to be searchable.
Enable statistics	When it is enabled, statistical analysis can be performed on the field values, which will increase index storage.

Time Field

The time field refers to a field with the date type in the actual data. Once the index is created, this field cannot be modified.

Note:

By default, the time field enables indexing and statistics, and these settings cannot be disabled.

Data Storage Duration:

1.1 You can set the data storage duration, with a default of 30 days, or select an option for permanent storage.

Project *	- ¢
	Only projects in the same VPC as the data source can be selected. If the existing project does not meet your requirements, you can click Create Project
ndex name *	Enter an index name
	Built-in shard auto-tuning, smart rollover, and other proprietary features are provided. You do not need to care about complex operations such as ind rollover and alias but just specify the index name for read/write operations.
ndex configuration	
ime field *	Specify the time field
	The time field refers to the date field in the data. This field records the data creation time and cannot be modified after the index is created.
ata retention period	O Limited − 30 + day(s) Permanently stored

1.2 Once all information is correctly entered, click **Create** to complete CVM log collection.

TKE Log access

Last updated : 2024-12-04 16:06:59

Prerequisites

A Tencent Cloud account has been created. For account creation, see signing up. If you log in with a sub-user account, ensure it has read and write permissions on ES.

Operation Steps

Logging in to the Console

1. Log in to the ES console.

2. In the top menu, select **Region**. Currently supported regions include Beijing, Shanghai, Guangzhou, Nanjing, and Hong Kong (China).

3. In the left sidebar, choose Log Analysis under the Serverless mode.

Creating a Project Space

- 1. Click Create a project.
- 2. Enter the **Project Name**, which can include 1 20 characters, including Chinese characters, letters, digits.
- 3. Click **Confirm**. Once validated, the project space will be created.

Create Project		×
same bu	pace is a logical business classification concept, you can place logs of the siness type in the same project space for joint analysis.	
Region *	🔇 Guangzhou 🔻	
Project Name *	Supports Chinese characters, letters, digits, underscores (_), and	
VPC *	✓ Q	
AZ and subnet *	Guangzho 🖌 🖌 Select a subnet 🗸 🖓	
	Subnet change is not supported after Project is successfully created. You can proceed to create a subnet	
	Confirm Cancel	

Note

In Elasticsearch Serverless Log Analysis, you can create an index and subsequently write data via API or access data sources such as CVM and TKE via the Data Access tab of the corresponding index. You can also set up data access during index creation, enabling one-stop access for CVM and TKE log access. Below is the instruction for one-step TKE log access setup.

TKE Log Access

On the ES Serverless Log Analysis homepage, select **TKE** to enter the TKE log access page.

luster Migration	
Self-built ES cluster migration	Tencent Cloud ES cluster migration
loud Product Integration	
O CVM	🔃 ТКЕ
EMR	TCHouse-C
TCHouse-D	Cceanus
Custom Integration Create r	new indexes only

Data Source Settings

Region: The region where the TKE cluster is located.

VPC: Required. The VPC where the TKE cluster is located.

TKE Cluster ID to Be Collected: Required. The ID of the TKE cluster to collect logs from, which should be in a running status and a standard cluster. If you need log collection for Serverless clusters (EKS), contact us via submitting a ticket.

Based on Namespace/Host Path: Required. For **Namespace**, select **Include/Exclude** from the first dropdown, and select one or more namespaces from the second dropdown (multi-select supported, but excluding all namespaces is not allowed). For host path-based collection, enter the **Absolute Path** on the host, for example, /var/log/*.log.

Pod Tag: Optional. You can create multiple Pod labels, which are logically connected using AND.

Container Name: Optional. The specified container name should be within the target cluster and namespace. If it is left empty, Filebeat will collect all containers within the namespace that match the specified Pod tags.

egion *	🔇 Guangzhou 🗸				
/PC *	-	÷		- Ø	
KE cluster to be ollected (€) ★	(in the set			▼ ⁽²⁾	
Log Filtering	O Based on Namespace O Based on Host Path				
	Namespace *	Include 💌	Select a nam	espace	•
	Pod Tag 🕥	Tag name		Separate multiple tag values by co	omm Delete
		New			
	Container Name	Enter the contain	er name. If no co	ontainer name is entered, all containe	

Collection Settings

Basic Settings

Collection Policy: Supports full collection and incremental collection. Once created, the collection policy cannot be modified. Full collection will collect historical logs as well as logs generated after the Filebeat configuration takes effect. Incremental collection will only collect logs generated after the Filebeat configuration becomes active.

Collection Parsing

Collection Template: If you need a quick setup or are testing, you can select a collection template based on your log output format. After confirmation, return to the interface to modify the log sample with actual log data, enabling a fast completion of the collection parsing settings.

🗸 Data S	ource > 2 Collection Settings > 3 Index Settings
Basic Settings	
Collection Policy	Full Collection Incremental Collection
Collection and	Parsing For quick setting, it is recommended to use the collection template-
Collection Mode	Single Line Multiple Lines
Extraction Settings	Extraction Image: Second s
Back	Next Cancel

Collection Mode: Supports both single-line and multi-line modes; once set, the mode cannot be modified. Single-line text log: Each line in the log file represents a single log entry, separated by a newline character. Multi-line text log: Each log entry spans multiple lines, such as Java stack traces. In this mode, you need to configure a log sample and a regex pattern for line beginnings. Filebeat uses the regex to identify the start of each log entry, treating unmatched lines as part of the current log entry until the next matched line beginning appears. Once you enter a log sample, the system automatically generates a default regex pattern for line beginnings. You can also customize this pattern, with highlighted text in the input box indicating the matched line beginnings.

Ensure that actual scenario logs are used to facilitate automatic extraction of the leading line regular expression.



Collection and F	Parsing Fo	or quick setting, it is recommended to use the collection template.
Collection Mode	Single Line	O Multiple Lines
Line Header Settings	Sample Log	<pre>1 [2023-09-0100:00:00][INF0]java.Lang.Exception:exception.happened 2 at TestPrintStackTrace.f(TestPrintStackTrace.java:1) 3 at TestPrintStackTrace.g(TestPrintStackTrace.java:3) 4 at TestPrintStackTrace.main(TestPrintStackTrace.java:5)</pre>
		Highlighted content is the line header information matched by the regular expression.
	Regular Expression	Automatic Generation O Custom
	for Line Header	^/[/d+-/d+:/d+:/d+//[/w+/]/w+/./w+/./w+/./w+/.**
	Match	

Extraction Settings: Extraction mode can be set to full-text log, JSON format, or delimiter-based. Once set, the extraction mode cannot be modified. Details are as follows:

Full-text log

JSON format

Delimiter

No key-value extraction is performed. The log content is stored in a field named message, which can be retrieved and analyzed using automatic tokenization.

For example, a single-line raw log might look like:

Tue Jan 01 00:00:00 CST 2023 Running: Content of processing something

When collected in the index, this data would appear as:

```
massage:Tue Tue Jan 01 00:00:00 CST 2023 Running: Content of processing
something
```

For logs in standard JSON format, we can extract fields based on the Key: Value pairs within the log.

For example, suppose a JSON log entry is as follows:

{"pid":321,"name":"App01","status":"WebServer is up and running"}

After structuring, the log entry will appear as follows:

```
{
    "pid":321,
    "name":"App01",
    "status":"WebServer is up and running"
}
```
For logs with content separated by a fixed delimiter, we can extract key-value pairs based on the specified delimiter. The delimiter can be a single character or a string, which can be selected or entered in the console.

For example, if a log entry is as follows:

321 - App01 - WebServer is up and running

With the delimiter set to -, this log entry will be split into three fields. Unique keys can then be assigned to these fields in the extraction results, as shown below:

```
pid: pid
name: App01
status: WebServer is up and running
```

Extraction Results: When the extraction mode is set to JSON format or Delimiter, a sample log can be provided for automatic extraction:

If the extraction mode is JSON format, the system will automatically populate the extracted Keys and Values. If it is deselected, the respective fields will not be written to the index.

If the extraction mode is Delimiter, the system will automatically populate the extracted Values, allowing you to assign unique Keys to each Value. If it is deselected, the corresponding fields will not be written to the index.

Built-in Fields: When you configure TKE log collection in the console, Filebeat will add information such as the log source and timestamp as Key-Value pairs in the logs. These fields are considered built-in fields. If a Key in your business log matches a built-in field name, the business log field content takes precedence, and the corresponding built-in field will not be added to the index. The meanings of the built-in fields are as follows:

Built-in Field Name	Meaning
log.file.path	Path where the log is stored
kubernetes.pod.ip	IP address of the Pod containing the log
kubernetes.pod.name	Name of the Pod containing the log
kubernetes.node.hostname	Name of the host containing the log
@timestamp	Timestamp of when the log was collected



Sample Log *	1 321_App01_WebServer is up and running	
Extraction *	3 fields are extracted from the sample log above. Click to update the extraction result-	
nesure	✓ Key	Value
	✓ pid	"321"
	✓ name	"Арр01"
	✓ status	"WebServer is up and rupping"
	Built-in Field log.file.path	Example: "/var/log/fun-times.log"
	Built-in Field host.name	Example: "vm_test1"
	Built-in Field host.ip	Example: "192.168.0.1"
	Built-in Field @timestamp	Example: "2016-05-23T08:05:34.853Z"
	If a key is unchecked, the corresponding field will not be written to the index.	

Preserve Original Logs: When it is selected, the original log content, prior to parsing and extraction, will be preserved in this field.

Record Parsing Errors: If the extraction mode is set to Delimiter, you can choose whether to log parsing errors. When it is selected, any errors encountered during parsing will be uploaded to this field as values.

Index Settings

Project Space: You can assign the index to a specific project space for easier management of related business indexes.

Index Name: Supports a length of 1 to 100 characters, including lowercase letters, numbers, -, _, ;, @, &, =, !, ', %, \$, ., +, (,).

Field Mapping

Dynamic generation: Enabled by default. When it is enabled, the system automatically parses the incoming data to generate the field mappings for the index.

Input sample auto-configuration: If Dynamic Generation is disabled, you can use Input Sample Auto-

Configuration to generate the field mappings. Input a sample in JSON format, and the system will automatically validate it. Once validated, the relevant fields will be mapped in the field mapping table.

The field mapping divides the original data into distinct terms by fields (key:value) to construct the index, enabling retrieval based on this mapping. Specific details are as follows:

Parameter	Feature Description
Field name	The name of the field within the data being written.
Field type	The data type of the field. The interface supports 9 types: text, date, boolean, keyword, long, double, integer, ip, and geo_point. Additional field types can be supported in JSON Editing Pattern . For more details, see Official Documentation.
Includes Chinese	Enable this option if the field includes Chinese characters that need to be retrieved. When it is enabled, the text field will use the ik_max_word tokenizer by default.
Enable index	When it is enabled, an index is built for this field to facilitate retrieval.
Enable statistics	When it is enabled, this field's values can be analyzed statistically, which will increase index storage.

Time Field

The time field refers to a field of type date in the actual data. Once the index is created, this field cannot be modified. **Note:**

The time field has **indexing** and **statistics** enabled by default, and these settings cannot be disabled.

Data Storage Duration:

1.1 You can set the storage duration of the data. By default, it is set to retain data for 30 days, though you also have the option to set it to permanent storage.

Project *	т Ф
	Only projects in the same VPC as the data source can be selected. If the existing project does not meet your requirements, you can click Create Project
ndex name *	Enter an index name
	Built-in shard auto-tuning, smart rollover, and other proprietary features are provided. You do not need to care about complex operations such as ind rollover and alias but just specify the index name for read/write operations.
ndex configuration	
ime field *	Specify the time field
	The time field refers to the date field in the data. This field records the data creation time and cannot be modified after the index is created.
Data retention period	O Limited − 30 + day(s) Permanently stored

1.2 Once the information is entered correctly, click **Create** to complete the TKE log collection.

Elastic MapReduce log access

Last updated : 2024-12-04 16:09:26

Prerequisites

A Tencent Cloud account has been created. For account creation, see Signing Up. If logging in with a sub-account, ensure that the account has read and write permissions for ES.

Operation Steps

Logging in to the Console

1. Log in to the ES console.

2. In the left sidebar, choose Log Analysis under the Serverless mode.

Creating a Project Space

1. click Create a project.

2. Enter a **Project Name** for the project, which can include 1 - 20 characters, consisting of Chinese characters, letters, digits, underscores, or delimiters (-).

3. Click **Confirm**. Once validated, the project space will be successfully created.

Create Project	> pace is a logical business classification concept,You can place logs of the siness type in the same project space for joint analysis.
Region *	S Guangzhou 🔻
Project Name *	Supports Chinese characters, letters, digits, underscores (_), and
VPC *	× Ç
AZ and subnet *	Guangzho 🖌 Select a subnet 🖌 🖓
	Subnet change is not supported after Project is successfully created. You can proceed to create a subnet 口
	Confirm Cancel

Note

In ES Serverless Log Analysis, you can simply Create an index, then use the API for data writing or access data sources such as CVM or TKE via the Data Access tab of the corresponding index. Alternatively, you can set up data access during index creation, enabling one-stop access for CVM logs, TKE logs, and Elastic MapReduce (EMR) logs. The following introduces the one-stop EMR log access process.

Elastic MapReduce (EMR) Log Access

1. On the ES Serverless Log Analysis homepage, select **EMR** to enter the EMR Log Access page.

Quick Data Access Select the data source, one-stop create an index, and integrate log data					
Cluster Migration					
Self-built ES cluster migration	Tencent Cloud ES cluster migration				
Cloud Product Integration					
O CVM	(TKE				
EMR	TCHouse-C				
TCHouse-D	Cceanus				
Custom Integration Create new	w indexes only				
Python SDK write	Java SDK write				
API Write					

2. Enter the Data Source settings page, configure the data source, and click **Next** once setup is complete.

Region: Select the region where the EMR cluster is located. If you enter this page from a project space details page, the region aligns with the region of project space by default.

VPC: The Virtual Private Cloud where the EMR cluster is located.

EMR Cluster: The EMR cluster from which logs need to be collected.

Log type: Specify the component runtime logs to collect; for example, task logs can be collected if the YARN component exists in the cluster.

Collection Policy: Supports both full collection and incremental collection. Selecting incremental collection will only collect logs generated after data access setup.

1 Data Source	> 2 Index Settings		
Region *	🔇 Guangzhou	•	
VPC *	vp	, _C	
EMR Cluster (i) *	EMI	· C	
Log type	Running Log This cluster has 4 components.Selected: 4		
	ZOOKEEPER - 3.6.3 HDFS - 3.2.2	VARN - 3.2.2	✓ KNOX - 1.6.1
	✓ Task Log Task logs can be collected only when YARN is installed in the	:luster.	
Collection Policy (j)	Full Collection Incremental Collection		
More settings			

3. Enter the Index Settings page, and configure the index settings.

Region: The project space's region, which aligns with the EMR cluster's region by default.

Project Space: You can assign indexes for the same business to a specific project space for easier management.

Index Name: Length of 1 - 100 characters. Lowercase letters, digits, and the following symbols: -, _, ;, @, &, =, !, ',

%, \$, ., +, (,) are supported.

Field Mapping

Dynamic Generation: Enabled by default. When enabled, it automatically parses and generates field settings for the index.

Input Sample Auto-Configuration: When Dynamic Generation is disabled, you can use Input Sample Auto-

Configuration to generate field mappings for the index by entering a JSON-formatted data sample. After

confirmation, the platform will validate the input; if the validation is successful, the relevant fields will be mapped in the field mapping table.

Field mapping divides the original data into multiple tokens based on fields (key:value) for indexing. Retrieval relies on this mapping, as detailed below:

Parameter	Description
Field name	The field name in the written data.
Field type	The data type of the field; the interface supports 9 types: text, date, boolean, keyword, long, double, integer, ip, and geo_point. Additional field types are supported in JSON mode . For details, see Official Documentation.



Include Chinese	Enable this option if the field contains Chinese text and requires Chinese retrieval. When it is enabled, the ik_max_word tokenizer is applied to the text field by default.
Enable indexing	When it is enabled, this field will be indexed for search.
Enable statistics	When it is enabled, statistical analysis can be performed on the field values, which will increase index storage.

Time Field

The time field refers to a field with the type date in the actual data. Once the index is created, this field cannot be modified.

Note:

By default, the time field enables **indexing** and **statistics**, and these settings cannot be disabled.

Data Storage Duration

You can set the data storage duration, with a default of 30 days, or select permanent storage.

ver and alias but
ver and alias but
and and but
ange to JSON m

TCHouse-D Cluster Log Access

Last updated : 2024-12-04 16:13:12

The ES Serverless service supports collecting logs from the TCHouse-D nodes to facilitate troubleshooting and issue analysis. For more details, see Log Search.

Customizing Filebeat Data Access

Last updated : 2024-12-04 16:15:17

Self-Built Filebeat Data Collection

```
Version Support
Only Filebeat versions 7.10.2 or 7.14.2 are supported.
```

Category	Parameter	Description	Filling Instructions
Elasticsearch template setting	setup.template.enabled	Index template	Boolean type. It can be set to false; currently, this setting is not supported.
	setup.ilm.enabled	Index lifecycle management	Boolean type. It can be set to false; currently, this setting is not supported.
	allow_older_versions	Compatibility with ES versions	Boolean type. It can be set to true or false.
output	protocol	Data transmission protocol	String type. The default value is http, and it can also be set to https.
	hosts	Private network access address for index	Array type. If the protocol is set to http, the port number should be 80. For example, it can be set as ["http://index- xxx.qcloudes.com:80"]; If the protocol is set to https, the port number should be 443. For example, it can be set as ["https://index- xxx.qcloudes.com:443"].

Configuration Description

```
# ====== Filebeat inputs
```

```
-----
```

🕗 Tencent Cloud

filebeat.inputs: - type: log # Change to true to enable this input configuration. enabled: true # Paths that should be crawled and fetched. Glob based paths. paths: - /var/log/*.log # ======= Filebeat modules _____ filebeat.config.modules: # Glob pattern for configuration loading path: \\\${path.config}/modules.d/*.yml # Set to true to enable config reloading reload.enabled: false # Period on which files under path should be checked for changes #reload.period: 10s # ================== Elasticsearch template setting _____ setup.template.enabled: false setup.ilm.enabled: false #template setting's value is set to false by default. If you set it to true, an error will be reported when the configuration is submitted # ======= General _____ # The name of the shipper that publishes the network data. It can be used to group # all the transactions sent by a single shipper in the web interface. #name: # The tags of the shipper are included in their own field with each # transaction published. #tags: ["service-X", "web-tier"] # Optional fields that you can specify to add additional information to the # output. #fields: # env: staging

🔗 Tencent Cloud

```
# ======= Processors
_____
processors:
 - add_host_metadata:
    when.not.contains.tags: forwarded
# ====== Logging
_____
# Sets log level. The default log level is info.
# Available log levels are: error, warning, info, debug
#logging.level: debug
# At debug level, you can selectively enable logging only for some components.
# To enable all selectors use ["*"]. Examples of other selectors are "beat",
# "publisher", "service".
#logging.selectors: ["*"]
output.elasticsearch:
 # Array of hosts to connect to.
 allow_older_versions: true
 protocol: "http"
 hosts: ["Private network access address for index"]
 # Authentication credentials - either API key or username/password.
 username: "your index username"
 password: "your index password"
 indices:
 - index: The_index_name
   when.equals:
    fields.type: log
```

Access Control

Last updated : 2024-12-04 16:21:56

1. In the Project list, click the project name/ID to enter the Basic Info page.

Project Manage and analyze dat	a by project space							
Create space						Search by project name or proje	ct ID. Separate multiple	Q
Name/ID	Search and Analysis	Status	Indexes	Network	Creation time \$	Tag	Operation	
test01	٩	Normal	2		2024-04-19 10:06:	30 🛷 1	Kibana Access contr	rol Delete

2. Then, click Access Management to enter the Access Control page.

Project test01	✓ Projec)
Data Analysis	Basic info Project Name test01 🖉 🕒 Region Guangzhou
Management	Project ID Project ID Network
Oevelopment Tools	Status Normal AZ and subnet Guangzhou Zo
Workspace Management	Creation time 2024-04-19 10:06:30
i⊟ Index list R Access Management	Index Access Control Private access address You can access the index under this space with the address and username password, for example, to perform data writing, search, and analysis,
O Usage Statistics	View Document 🗹
	Kibana access control Public access address Public network access IP setting If you need to access Kibana via the public network, please ensure that your IP address has been set in the IP allowlist. View Document C
	User Management
	Create User Q 2
	Username User Type Password Permissi T Permission Scope C Operation
	elastic P Primary Read/Write All Indexes 2 Change Password Delete
	Iotalitems: I 10 V / page M 4 1 / 1 page V M

3. In the Access Control module, you can perform the following operations:

View the project space's private network access address, which can be used for data writing or querying.

Enable or disable Kibana private network access or public network access.

Modify the allowlist of Kibana public network access addresses. Multiple IP addresses are supported, and are separated by commas, semicolons, or line breaks, in format such as 192.168.0.1,192.168.0.0/24, with a maximum of 50 entries. If you are not aware of the current IP address, click **Click to automatically access the current IP address** to obtain and enter it automatically.

Note

Setting 127.0.0.1 means blocking access for all IPv4 addresses. For security, setting the IP allowlist to 0.0.0.0 is not permitted. If you have special requirements, submit a ticket for assistance.

IP allowlist *	
	Get current IP
	Enter up to 50 IPs separated by comma, semicolon, or line separator, such as 192.168.0.1,192.168.0.0/24
	Note: 127.0.0.1 means blocking access from any IPv4 address. 0.0.0.0 is excluded for security. If you have any special requirements, submit a ticket IZ.

Modify root/sub-user password: On the user management page, click **Change Password** to modify the index access password.

Create User				Search by username	QB
User Type	Password	Permissi 🍸	Permission Scope	Creation time \$ Opera	ation
Primary	***** 🗞 🗗	Read/Write	All Indexes	2024-04-19 10:06:30 Chang	ge Password Delete
					Þ

Modify sub-user permissions: On the user management page, click **Modify Permissions**, then select the permission type and scope. Supported permission types include read-only and read-write, and you can select from all indexes

within this space via a dropdown menu.

Create Oser				search by username	(Q ic
User Type	Password	Permissi 🍸	Permission Scope	Creation time \$	Operation	
Primary	**** & C	₽ Read/Write	All Indexes	2024-04-19 10:06:30	Change Password De	elete
Sub-User	****** 📎 🗗	Read-Only	All Indexes	2024-08-27 17:40:14	Modify Permissions Change Password De	elete
 Total items: 2 				10 💙 / page 🛛 🛤 🖪	1 / 1 page	▶ ▶
Modify P	ermission	Informatic	on			
Modify P Permission Type	ermission O Rea	I nformatic d-Only	on Read/Write			:
Modify P Permission Type Permission Scope	ermission I Rea * All	Informatic	on Read/Write sting and New	Specify Index		

4. Log in to Kibana:

After enabling Kibana public network access and configuring the IP allowlist, click the Kibana public access address to open the Kibana login page. Enter the sub-user's username and password for this space, then click **Log in** to access Kibana.



Writing Data

Last updated : 2024-12-04 16:25:16

Overview

The ES Serverless service supports writing data into indexes through methods such as **ES native APIs, Logstash, Flink, and Kafka**. If you require log collection for services such as CVM, TKE, or TCHouse-C, a one-stop visualized configuration option is also available. By simply setting up data sources and index information, you can collected logs into the indexes for efficient retrieval and analysis. This document provides instructions for writing a single document and writing document in batches using **Kibana** and **Curl commands**.

Access Control

1. In the Project list, click the corresponding project name to enter the Basic Info page.

Project Manage and analyze data b	by project space								
Create space						Search by project na	ne or project ID.	Separate multiple	Q
Name/ID	Search and Analysis	Status	Indexes	Network	Creation time	¢	Tag	Operation	
test01	Q	Normal	2		2024-04-19 10:0	5:30	Ø 1	Kibana Access control Dele	te

2. In the Access Control module, you can view the username and password for the index, private network access address, Kibana private network access address, and Kibana public network access address. You can also configure the Kibana public network access policy.



Project test01	✓ Project 1
Data Analysis Log Analysis	Project Name test01 🖉 🖉 Region Guangzhou
Management	Project ID Network
Development Tools	Status Normal AZ and subnet Guangzhou Zor
Workspace Management	Creation time 2024-04-19 10:06:30
 ⊟ Index list Access Management Ousage Statistics 	Index Access Control Private access address Vou can access the index under this space with the address and username password, for example, to perform data writing, search, and analysis. View Document 🖻
	Kibana access control Public access address P Private access address Kibana Language English Ø
	Public network access IP setting If you need to access Kibana via the public network, please ensure that your IP address has been set in the IP allowlist. View Document 12
	User Management
	Create User Search by username Q 2
	Username User Type Password Permissi T Permission Scope C Operation
	elastic D Primary 😿 D Read/Write All Indexes 2 Change Password Delete
	4
	Total items: 1 10 v / page H 4 1 / 1 page H

3. Access Kibana: The Discover and Dev Tools features of Kibana are embedded in the Tencent Cloud console, allowing you to use retrieval and analysis capabilities directly within the console or access Kibana via an external link. Via Console: In the sidebar of the space details page, click Search and Analysis to enter the relevant page. You can switch between index views by clicking the index pattern dropdown on the left side. Log Search corresponds to Discover, and Development Tools corresponds to Dev Tools.

Note:

Embedded features require third-party cookies to be enabled in your browser. If you encounter issues, please enable third-party cookies in your browser settings.

Search						KQL	Last 30 minutes	Show dates
🗐 — + Add filter								
web_log01-fpfha590 $ \smallsetminus $	••• 🗧 5 his			Jan 19, 2024 @ 15	02:58.567 - Jan 19, 2024 @ 15:32:	58.567 Auto ~		⊗ F
Change index pattern	5							
Q. Filter options	3							
✓ web_log01-fpfha590	دې د							
web_log02-fpfha590								
web_log03-fpfha590		15:05:00	15	5:10:00 1	:15:00	15:20:00	15:25:00	15:30:00
score					⊜timestamp per 30 sei	conds		
Otimestamp	Time 🚽		Document					
t id t io	> Jan 19,	2024 @ 15:23:03.762	<pre>@timestamp: Jan 19, 2024 @ web_log01-fpfha590-2024.01</pre>	0 15:23:03.762 id: 090798 ip: 119.147 .19-000001 _score:type: _doc	.10.191 now_local: gz region: 1	0002424 routing_no: 4087 user	_name: user-Ufa9Yee1P user_type: 0	1 _id: oluiII08RiFvMpqUv9lW _index:
t now_local t region	> Jan 19,	2024 0 15:23:03.762	<pre>\$timestamp: Jan 19, 2024 @ web_log01-fpfha590-2024.01</pre>	9 15:23:83.762 id: 860942 ip: 144.222 .19-000001 _score:type: _doc	.220.82 now_local: gz region: 1	10002424 routing_no: 4381 user	_name: user-EVUH760be user_type: 0	2 _id: 2FuiII0BRiFvMpqUwNl0 _index:
t routing_no t user_name	> Jan 19,	2024 0 15:23:03.762	<pre>@timestamp: Jan 19, 2024 @ web_log01-fpfha590-2024.01</pre>	9 15:23:03.762 id: 097982 ip: 221.105 .19-000001 _score:type: _doc	.83.164 now_local: gz region: 1	10002424 routing_no: 1877 user	_name: user-yZxxqur0w user_type: 0	<pre>3 _id: rNyiII086E4CniuiwALG _index:</pre>
t user_type	> Jan 19,	2024 0 15:23:03.762	@timestamp: Jan 19, 2024 0 web_log01-fpfha590-2024.01	9 15:23:03.762 id: 096693 ip: 25.160. .19-000001 _score:type: _doc	87.200 now_local: gz region: 16	0002424 routing_no: 1098 user_	name: user-vGYxjkVmC user_type: 04	_id: sNyiII086E4CniuiwQI8 _index:
	> Jan 19,	2024 0 15:23:03.762	@timestamp: Jan 19, 2024 @	# 15:23:03.762 id: 197573 ip: 55.24.1	24.47 now_local: gz region: 100	002424 routing_no: 6730 user_n	ame: user-oaII2knlZ user_type: 01	_id: sdyiII0B6E4CniuiwQKs _index: .

Via Kibana Public Network Access Address: Click Kibana public network access address to enter the Kibana

page.

Data Analysis	Basic info
	Project Name 🛛 🖍 🗗 Region Guangzhou
Alarm Management	Project ID D Network
Oevelopment Tools	Status Normal AZ and subnet
Workspace Management	Creation time 2024-04-19 10:06:30
i≣ Index list	Index Access Control
Management	Private access address
O Usage Statistics	You can access the index under this space with the address and username password, for example, to perform data writing, search, and analysis. View Document 🛙
Deration Record	
	Kibana access control
	Public access address https:// bana.qclou 2 Private access address
	Public network access IP setting
	If you need to access Kibana via the public network, please ensure that your IP address has been set in the IP allowlist. View Document 💈
	User Management
	Create User Search by username
	Username User Type Password Permission T Permission Scope Creation time ‡ Operation
	elastic 🖗 Primary User ****** 🎕 🖗 Read/Write All Indexes 2024-04-19 10:06:30 Change Password Delet
	read_only 🖉 Sub-User ******* 🎕 🖉 Read-Only All Indexes 2024-08-27 17:40:14 Modify Permissions Change Password Delet
	Total items: 2 10 🗸 / page 11 🖌 11 / 1 page

On the Kibana login page, enter the username and password, which can be copied directly from the user management page.

Create User					Search by username	(
Username	User Type	Password	Permission T	Permission Scope	Creation time \$	Operation
elastic 🗳	Primary User	****** 🖉 🖗	Read/Write	All Indexes	2024-04-19 10:06:30	Change Password Delete
read_only 🗳	Sub-User	********** 🖉 🗗	Read-Only	All Indexes	2024-08-27 17:40:14	Modify Permissions Change Password Delete

After entering the Kibana page, click the three-bar icon in the upper right corner, then click **Dev Tools** to enter the development tools page.

😽 elastic	Q Search Elastic		٩
E Home			
☆ łome	Home	್ಝಿ Dev tools 🔅 Manage 🐻 Add data	
🖌nalytics 🗸 🗸			
Overvisw Discolvr Dashbilard Cariva: Maps Visualizi Library Mail gement ~	(E) Kibana Visualize & analyze →	Analyze data in dashboards. Search and find insights. Design pixel-perfect presentations. Plot geographic data.	
Dev Tools Stack Management	Ingest your data	🗄 Try our sample data	
	Add data Ingest data from popular apps and services.	Upload a file Import your own CSV, NDJSON, or log file.	
	Manage your data		
	Interact with the Elasticsearch API Skip cURL and use a JSON interface to work with your data in Console.		
	 Display a different page on log in 		

Note:

Kibana public network access includes an allowlist mechanism, meaning that IP addresses not included in the access policy cannot access Kibana, enhancing access security. If the page displays Sorry, you do not have permissions to access, click **Kibana Public Network Access Policy** as shown above. In the pop-up window, click **Get current IP** to enter your current IP address to the allowlist.

)

Set policy fo	or Kibana access over public network
IP allowlist *	127.0.0.1,43.132.141.24,113.108.77.52
	Get current IP Enter up to 50 IPs separated by comma, semicolon, or line separator, such as 192.168.0.1,192.168.0.0/24
	Note: 127.0.0.1 means blocking access from any IPv4 address. 0.0.0.0 is excluded for security. If you have any special requirements, submit a ticket ^{III} .
	Confirm Cancel

Writing a Single Document

Via Kibana Dev Tools

```
POST /index name/_doc
{
    "@timestamp": "2023-09-28T11:06:07.000Z",
    "user":{
        "id" : "8a4f500"
    },
    "message": "Login successful"
}
```

Via Command Line

```
curl -X POST "project space access address/index name/_doc/?pretty" -H
'Content-Type: application/json' -d'
{
    "@timestamp": "2023-09-28T11:06:07.000Z",
    "user": {
```

```
"id": "8a4f500d"
},
"message": "Login successful"
}
```

Project test01	✓ Project	Q			
Data Analysis	Basic info				
 △ Alarm 	Project Name 🛛 test01 🖉 🗳			Region	Guangzhou
Management	Project ID	Ð		Network	
Development Tools	Status Normal			AZ and subnet	Guangzho
Workspace Management	Creation time 2024-04-19 10:	06:30			
∃ Index list	Index Access Control		1		
Access Management	Private access address http	com 🗸 🖬	1		
Osage Statistics	You ca	n access the index under this space with the addres	s and username passwo	ord, for example, to pe	erform data writing, search, and analysis. <mark>View Do</mark> d
Operation Record	Kibana access control				
	Public access address		c D	Private access add	iress
	Public network access IP setting			Kibana Language	English 🖉
		If you need to access Kibana via the public netw that your IP address has been set in the IP allow View Document I2	ork, please ensure list.		

Caution

The PUT /index name/_doc/document ID format cannot be used for writing requests. To specify a document ID, use PUT /index name/_create/document ID . Ensure that the written data includes the **Time Field** set during index creation.

Writing Document in Batches

Via Kibana Dev Tools

```
PUT /index name/_bulk?refresh
{"create":{ }}
```

```
{ "@timestamp": "2023-03-28T11:04:05.000Z", "user": { "id": "vlb44hny" },
"message": "Login attempt failed" }
{"create":{ }}
{ "@timestamp": "2023-03-29T11:06:07.000Z", "user": { "id": "8a4f500d" },
"message": "Login successful" }
{ "create":{ }}
{ "@timestamp": "2023-03-30T11:07:08.000Z", "user": { "id": "l7gk7f82" },
"message": "Logout successful" }
```

Via Command Line

```
curl -X PUT "project space access address/index name/_bulk?refresh&pretty" -H
'Content-Type: application/json' -d'
{"create":{ }}
{ "@timestamp": "2023-03-28T11:04:05.000Z", "user": { "id": "vlb44hny" },
"message": "Login attempt failed" }
{"create":{ }}
{ "@timestamp": "2023-03-29T11:06:07.000Z", "user": { "id": "8a4f500d" },
"message": "Login successful" }
{ "@timestamp": "2023-03-30T11:07:08.000Z", "user": { "id": "l7gk7f82" },
"message": "Logout successful" }
```

Caution

T

The bulk operation only supports create .

Ensure that the written data includes the **Time Field** set during index creation.

Data Query

Last updated : 2024-12-04 16:26:57

Overview

This document introduces data query operations using the Kibana and Curl command line methods.

Access Control

1. In the space list, click the corresponding **Project Name/ID** to enter the Basic Info page.

Project Manage and analyz	ze data by project space							
Create space						Search by project name or pro	ject ID. Separate multiple	Q f
Name/ID	Search and Analysis	Status	Indexes	Network	Creation time	t Tag	Operation	
test01	Q	Normal	2	100	2024-04-19 10:0	6:30 🖉 1	Kibana Access	control Delete

2. In the **Index Access Control** module, you can view the sub-user information (username, password, and permissions), private network access address, Kibana private network access address, and Kibana public network access address. You can also configure the Kibana public network access policy.

Project test01	✓ Project II
Data Analysis	Basic info
Cog Analysis	
Alarm	Project Name Testol 2 P
Management	Project ID Network
Development Tools	Status Normal AZ and subnet Guangzhou Zone
10010	Creation time 2024-04-19 10:06:30
Norkspace Management	
■ Index list	Index Access Control
Access	Private accors address
Management	You can access the index under this space with the address and username password, for example, to perform data writing, search, and analysis.
 Usage Statistics 	View Document 🗳
Operation Record	
	Kibana access control
	Public access address
	Kibana Language English
	Public network access IP setting
	If you need to access Kibana via the public
	network, please ensure that your IP address has been set in the IP allowlist.
	View Document 🗳
	User Management
	Create User Search by username Q
	Username User Type Password Permissi T Permission Scope C Operation
	elastic 🗳 Primary **** Read/Write All Indexes 2 Change Password Delete
	iver puge in a line puge

Access Kibana: The Discover and Dev Tools features of Kibana are embedded in the Tencent Cloud console, allowing you to use retrieval and analysis capabilities directly within the console or access Kibana via an external link.
 Via Console: Click Search and Analysis in the sidebar to enter the relevant page. You can switch between index views by clicking the index pattern dropdown on the left side. Log Search corresponds to Discover, and Development Tools corresponds to Dev Tools.

Search				KQL	🛗 🖌 Last 30 minutes	Show dates C I
) - + Add filter						
web_log01-fpfha590 ~	™ ∈ 5 hits		Jan 19, 2024 @ 15:02:58.567 - Jan 19, 20	024 @ 15:32:58.567 Auto ~		ø H
Change index pattern	5					
Q. Filter options	3					
✓ web_log01-fpfha590	₽					
web_log02-fpfha590	1					
web_log03-fpfha590	15:05:00	15:10:00	15:15:00	15:20:00	15:25:00	15:30:00
g_score			⊜timesta	amp per 30 seconds		
t_type	Time 🗸	Document				
 @timestamp id 	> Jan 19, 2024 @ 15:23:03.	762 @timestamp: Jan 19, 2024 @ 15:23:03.762 id	: 090798 ip: 119.147.10.191 now_local: g	gz region: 10002424 routing_no: 4087 use	er_name: user-Ufa9Yee1P user_type:	01 _id: o1uiII08RiFvMpqUv91W _index:
t ip		web_toget-tp/mase-zet+tet.19-000001 [acon				
t now_local	> Jan 19, 2024 @ 15:23:03.	762 Stimestamp: Jan 19, 2024 @ 15:23:03.762 id web long1_fofba508_2024 @1 19_000001	1: 868942 ip: 144.222.228.82 now_local: g	gz region: 10002424 routing_no: 4381 use	er_name: user-EVUH760be user_type:	02 _id: 2FuiII0BRiFvMpqUwNl0 _index:
t region		#65_10ger (principe for or 100001 _3001	_typeuoo			
t user_name	> Jan 19, 2024 0 15:23:03.	762 #timestamp: Jan 19, 2024 # 15:23:03.762 ic web loc91-fofba509-2024 #1 18-000901 coordinates and the second	: 097982 ip: 221.105.83.164 now_local: g	gz region: 10002424 routing_no: 1877 use	er_name: user-yZxxqurθw user_type:	03 _id: rNyiII086E4CniuiwALG _index:
t user_type		web_t0ge1-1p1na396-2624.61.19-666661 _3C014	atypedoc			
	> Jan 19, 2024 @ 15:23:03.	762 @timestamp: Jan 19, 2024 @ 15:23:03.762 ic	: 096693 1p: 25.160.87.200 now_local: gz	z region: 10002424 routing_no: 1098 user	r_name: user-vGYxjkVmC user_type: 6	4 _id: sNyiII0B6E4CniuiwQI8 _index: .
			2.000			

Note:

Embedded features require third-party cookies to be enabled in your browser. If you encounter any issue, please enable third-party cookie settings in your browser settings.

Via Kibana Public Access Address: Click Kibana public access address to enter the Kibana page.

Data Analysis	Paolo info
O Log Analysis	
🙆 Alarm	Project Name test01 🖉 🖉 Region Guangzhou
Management	Project ID Network
 Development Tools 	Status Normal AZ and subnet
Workspace Management	Creation time 2024-04-19 10:06:30
i⊟ Index list	Index Access Control
Access Management	Private access address
O Usage Statistics	You can access the index under this space with the address and username password, for example, to perform data writing, search, and analysis. View Document 🛙
Depration Record	
	Kibana access control
	Public access address https:// ibana.qclou g Private access address
	Public network access IP setting
	If you need to access Kibana via the public network, please ensure that your IP address has been set in the IP allowlist. View Document 🗳
	User Management
	Create User Search by username Q
	User Type Password Permission, 🍸 Permission Scope Creation time ‡ Operation
	elastic D Primary User ••••••• 🕲 D Read/Write All Indexes 2024-04-19 10:06:30 Change Password Delete
	read_only 🖉 Sub-User ******** 🎕 🖉 Read-Only All Indexes 2024-08-27 17:40:14 Modify Permissions Change Password Delete
	Total items: 2 10 🗸 / page 📕 ┥ 1 / 1 page 🕨 🕅

On the Kibana login page, enter the username and password, which can be copied directly from the user management page.

Create User					Search by username	C
Username	User Type	Password	Permission T	Permission Scope	Creation time \$	Operation
elastic 🕒	Primary User	Ø р	Read/Write	All Indexes	2024-04-19 10:06:30	Change Password Delete
read_only 🕒	Sub-User	********* 夜 🗗	Read-Only	All Indexes	2024-08-27 17:40:14	Modify Permissions Change Password Delete

After entering the Kibana page, click the three-bar icon in the upper right corner, and select **Discover** to access the search and analysis page.



Note:

Kibana public network access includes an allowlist mechanism, meaning that IP addresses not included in the access policy cannot access Kibana, enhancing access security. If the page displays Sorry, you do not have permissions to access, you can click **Kibana public network access policy** as shown above. In the pop-up window, click **Get current IP** to enter your current IP address to the allowlist.

Set policy f	or Kibana access over public network	×
IP allowlist *	127.0.0.1,43.132.141.24,113.108.77.52	
	Get current IP Enter up to 50 IPs separated by comma, semicolon, or line separator, such as 192.168.0.1,192.168.0.0/24	
	Note: 127.0.0.1 means blocking access from any IPv4 address. 0.0.0.0 is excluded for security. If you have any special requirements, submit a ticket ^{III} .	
	Confirm Cancel	

Retrieval and Analysis

Via Command Line

```
curl -X GET "index access address/index name/_search?pretty" -H 'Content-Type:
application/json' -d'
{
    "query": {
    "term": {
        "user.id": "kimchy"
     }
}
```

Via Discover

On the Discover page, you can perform time filtering, keyword searches, and other operations:

🖫 🗸 Search			KOL 🗐 🗸 Last 1 year Show dates	GF
😨 — + Add filter				
	ooo (29 hits	Sep 20, 2022 @ 00:00:00.000 - Sep 20, 2023 @ 20:49:16.218 Auto ~	Hic
Q Search field names		25		
Filter by type 0	~	20		
Available fields	7	3 10 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5		
t _index		0 2022-10-01 2022-	11-01 2022-12-01 2023-01-01 2023-02-01 2023-03-01 2023-04-01 2023-06-01 2023-06-01 2023-07-01 2023-08-01 2023-08-01	1
#_score			@timestamp per week	
t_type		Time 🗸	Document	
t message		> Sep 8, 2023 @ 19:06:07.006	@timestamp: Sep 8, 2823 @ 19:06:87.000 message: Login successful user.id: 8a4f500d _id: Rgehsoo8BUqp7yINP2wo _index: .ds-test123-afb83rjo-2823.09.20-00000 _score:type: _doc	01
		> Sep 8, 2023 @ 19:06:07.000	@timestamp: Sep 8, 2023 @ 19:06:07.000 message: Login successful user.id: 8a4f500d _id: WEqhsoo8DpTtuj9NQLq6 _index: .ds-test123-afb83rjo-2023.09.20-00000 _score:type: _doc	101
		> Sep 8, 2023 @ 19:06:07.006	@timestamp: Sep 8, 2023 @ 19:06:07.000 message: Login successful user.id: 8a4f500d _id: KCyhso08StANxiHsRHq8 _index: .ds-test123-afb83rjo-2023.09.20-0000t _score:type: _doc	101
		> Sep 8, 2023 @ 19:06:07.006	etimestamp: Sep 8, 2023 @ 19:06:07.000 message: Login successful user.id: 8a4f500d _id: CK2hsooBHZc5x221STBa _index: .ds-test123-afb83rjo-2023.09.20-0000t _score:type: _doc	101
		> Sep 8, 2023 @ 19:06:07.006	@timestamp: Sep 8, 2023 @ 19:86:07.000 message: Login successful user.id: 8a4f500d _id: 1QehsooBBUqp7yINUKzk _index: .ds-test123-afb83rjo-2023.09.20-00000 _score:type: _doc	101
		> Sep 8, 2023 @ 19:06:07.006	@timestamp: Sep 8, 2023 @ 19:86:87.000 message: Login successful user.id: 8a4f500d _id: 4yyhsooBStANxiHsPFsU _index: .ds-test123-afb83rjo-2023.09.20-00000 _score:type: _doc	101
		> Sep 8, 2023 @ 19:06:07.000	etimestamp: Sep 8, 2023 @ 19:06:07.000 message: Login successful user.id: 8a4f500d _id: KQehsoo80Pi3bQX5PamK _index: .ds-test123-afb83rjo-2023.09.20-00000(101

Via Dev Tools

Perform data queries using DSL. An example is as follows:

```
GET /index_name/_search
{
    "query": {
        "term": {
            "user.id": "kimchy"
        }
    }
}
```

Via Kibana Dashboard

After entering Kibana, select **Dashboard** in the left sidebar to start data visualization. You can quickly create charts by dragging and dropping elements.



Index Management Configuration Management

Last updated : 2024-12-04 16:28:21

The Elasticsearch Serverless service provides configuration management features for indexes, allowing you to quickly view an index's configuration on the configuration management page. You can also modify index configurations to quickly adapt to business growth.

Viewing the Index Configuration

Upon entering this page, the default view mode displays information such as field mappings and data storage duration.

Field mapping	Field name	Field type	Include Chinese characters (i)	Enable index (j)	Enable statistics (j)
	field1	text 🗸			-
	field2	text 🗸			-
	Dynamic creation @timestamp	date	-		
Time field *	@timestamp				
Data retention period	Limited - 30 + day(s)	Permanently stored			

Additionally, you can click **Change to JSON mode** in the upper right corner to view the current index configuration in JSON format.

1	{	
2	"mappings": {	
3	"properties": {	
4	"field1": {	
5	"analyzer": "standard",	
6	"index": true,	
7	"type": "text"	
8	},	
9	"field2": {	
10	"analyzer": "standard",	
L1	"index": true,	
12	"type": "text"	
L3		
14	}	
15	}	
16	}	

Modifying the Index Configuration

Click **Modify configuration** in the lower left corner to enter the edit mode, allowing you to adjust index configuration settings, such as field mappings or data storage duration.

ndex configuration					41	Change to JSON model
ield mapping	Field name	Field type (j)	Include Chinese characters (j)	Enable index (j)	Enable statistics	
	field1	text 🗸			-	8
	field2	text 🗸			-	8
	Dynamic creation @timestamp	date	-			Settings
	+ Add field					
ïme field ∗	@timestamp					
	\bigcirc Limited $-$ 20 + day(c)	Permanently stored				

When you change to JSON mode, the left-side panel displays the current configuration for the live index, making it easy to review active settings. The right-side panel provides an input box for modifying configuration settings. Enter



the corresponding configuration information to be modified in the input box. Once the modification is

successful, the corresponding index configuration items will be updated.

<pre>1 { 2 "mappings": { 3 "properties": { 4 "field1": { 5 "analyzer": "standard", 6 "index": true, 7 "type": "text" 8 }, 9 "field2": { 10 "analyzer": "standard", 11 "index": true, 12 "type": "text" 13 } 14 } 15 </pre>	rent configuration	Modify configuration	
	<pre>1 { 2 "mappings": { 3 "properties": { 4 "field1": { 5</pre>	<pre>1 { 2 "mappings": { 3 "properties": {} 4 } 5 }</pre>	Cancel Forma

Alarm Management

Last updated : 2024-12-04 16:38:41

The ES Serverless service supports alarm management, allowing you to configure alarm policies for specific objects in the console. These policies periodically perform retrieval and analysis on indexes within monitored objects. When query results meet trigger conditions, an alarm notification is sent (currently supported via email and WeCom), enabling timely detection of issues. This feature supports keyword alarms, such as the number of the term error within logs over a specified time range, and metric monitoring, such as determining whether the maximum value of a numeric field exceeds a set threshold within a specified time range. This capability enhances observability in log analysis scenarios, enabling quick issue detection and resolution.

Operation Steps

Prerequisites

1. Log in to the ES Serverless console.

2. In the space list, click the corresponding space name.

Project test01	✓ Project ID	Q			
Data Analysis	Create			Search by alarm name, alarm ID, or alarm object. So	eparate multiple keywords
O Log Analysis	Alarm Name/ID	Status 🝸	Alarm Object	Alarm Channel	Operation
 Alarm Management 					
Oevelopment Tools					
Workspace Management					
i≣ Index list					
Access Management			No alarm ru	le exists in this project.Create Now	
O Usage Statistics					
Operation Record					
	Total items: 0			10 🗸 / page	H ◀ 1 /1 page 1

Creating an Alarm

Basic Information

1. In the left sidebar, click Alarm Management, then click Create.

2. Enter an alarm name, with a length of 1–50 characters. Digits, letters, Chinese characters, underscores, and delimiters - are supported.

3. Select an alarm object, with support for indexes within the current space.

Note:

Indexes that are still being created cannot be selected.

Alarm Rules

1. Query statement:

Supported operators include count, average, sum, max, and min, with count as the default.

When the operator is count, all fields can be selected. The expression supports equal to, not equal to, belong to,

not belong to, existing, and no existing.

If the expression is **equal to or not equal to**, you need to enter a corresponding value, with support for a single string only.

If the expression is **belong to or not belong to**, you need to enter an array of values, with at least one entry, separated by commas.

When the operator is **average, sum, max, or min**, only numeric fields, such as long, integer, short, double, and float, can be selected.

2. Query range: Defaults to data written within the last 5 minutes. Supports units in minutes and hours.

3. Query frequency: Defaults to querying every 1 minute. Supports units in minutes and hours.

4. Trigger condition: The expression supports Greater than, Greater than or equal to, equal to, Equal to less

than, Less than, and Between. The default is set to greater than, with a default value of 100.

Alarm Notification

1. Email:

To ensure the accuracy of the alarm address, enter the email address and complete a Captcha verification.

If the email address is changed, a new Captcha will need to be requested.

2. WeCom: Enter the WeCom bot webhook address.

Note:

The WeCom bot webhook address should start with the prefix https://qyapi.weixin.qq.com .


Basic info	
√larm Name ★	Enter the alarm name.
	1-50 characters of English letters, Chinese characters, numbers, dashes (-) or underscores (_) are supported.
larm Object *	Select the destination index.
Alarm Rule	
Query Statistics	
Query * Statement	count • Select the field. • Select the opera • Separate multiple values with corr
Query *	lact - S + min Y Data written in
Scope	Only data written on the last day can be queried.
Scope Query * Frequency	Only data written on the last day can be queried. Rollover once per - 1 + min V Once
Scope Query Frequency rigger ondition Narm Notifica Email W	Only data written on the last day can be queried. Rollover once per Image: the minimum of the last day can be queried. When the number of queried data entries is Greater than 100 , trigger the alarm. ation WeCom Lark DingTalk
Scope Query Frequency rigger Narm Notifica Email W Email Address	Construction
Scope Query Frequency Gondition Condition Charm Notifica Email W Email Address Verification Code	Converties Only data written on the last day can be queried. Rollover once per When the number of queried data entries is Greater than Once When the number of queried data entries is Greater than Image: Converties WeCom Lark DingTalk Enter the email address. Enter the verification code. Send Code

3. Once all information is verified, click **Create** to complete the alarm creation.

Alarm Content

When an alarm is triggered, you will receive the following information:

Title: Tencent Cloud Elasticsearch Serverless Service Alarm Triggered.

Content:

[Alarm] Dear Tencent Cloud user, your Tencent Cloud account (Account ID: xxx) using the Elasticsearch Serverless service triggered an alarm at {Time} (UTC+8).

Alarm Name: {Corresponding Alarm Name}

Alarm Object: {Corresponding Index Name}

Alarm Management

1. On the Alarm Management page, you can view details and the status of your configured alarm policies.

2. To disable or delete an alarm, click More in the operation column.

3. To edit an alarm policy, click Edit.

ES API References

Last updated : 2024-12-04 16:40:46

Using APIs via Command Line or Clients Such as Filebeat

API URI	Supported Method	Description		
/_bulk	PUT and POST	For more details, see Bulk API.		
/{index}/_bulk	PUT and POST	For more details, see Bulk API.		
/{index}/_doc/{id}	PUT and POST	For more details, see Index API.		
/{index}/_doc	POST	For more details, see Index API.		
/{index}/_create/{id}	PUT and POST	For more details, see Index API.		
/{index}/_mapping	GET	For more details, see Get mapping API.		
/{index}/_msearch	POST and GET	For more details, see Multi search API.		
/_msearch	POST and GET	For more details, see Multi search API.		
/{index}/_count	POST and GET	For more details, see Count API.		
/{index}/_search POST and GET		For more details, see Search API.		

Using APIs via Kibana

API URI	Supported Method	Description			
/{index}/_bulk	PUT and POST	For more details, see Bulk API.			
/{index}/_doc/{id}	PUT and POST	For more details, see Index API.			
/{index}/_doc	POST	For more details, see Index API.			
/{index}/_create/{id}	PUT and POST	For more details, see Index API.			
/_security/user/_has_privileges	POST and GET	For more details, see Has privileges API.			
/{index}/_field_caps	POST and GET	For more details, see Field capabilities API.			



/{index}/_flush	POST and GET	For more details, see Flush API.			
/{index}/_mapping	GET	For more details, see Get mapping API.			
/{index}/_mappings	GET	For more details, see Get mapping API.			
/{index}/_refresh	POST and GET	For more details, see Refresh API.			
/_resolve/index/{name}	GET	For more details, see Resolve index API.			
/{index}/_count	POST and GET	For more details, see Count API.			
/{index}/_msearch	POST and GET	For more details, see Multi search API.			
/{index}/_search	POST and GET	For more details, see Search API.			
/_async_search/{id}	GET	-			
/{index}/_async_search	POST	-			
/_security/_authenticate GET		For more details, see Authenticate API.			

Related Issues Kibana Usage Issues

Last updated : 2024-12-04 17:36:10

How to Set a Field to geo_point Type and Draw a Map?

Before writing data, set the type of the specified field to geo_point in the mapping. After the data is written, go to **Maps** in the Kibana sidebar to enter the map drawing interface.

Note:

Manually set the field to geo_point type; otherwise, it may be automatically mapped to an incorrect type, preventing the map from being drawn.

Where can I Find Kibana's Coordinate Map Feature?

You can use the Clusters and grids option in Maps to aggregate specific fields.

How to Distinguish and Display Different Value Ranges for Fields Aggregated by Metrics?

You can adjust the **Fill color** setting: In **Layer settings**, scroll down to find the **Layer Style** module. For **Fill color**, select by value, and select the key to differentiate. Then, in as number, select an appropriate gradient color.

After Metrics are Displayed, How can I Identify the Value Ranges Represented by Different Colors on the Map?

Click the arrow in the middle of the corresponding layer under LAYERS to display the value ranges (this arrow is hidden by default and only appears when you hover over it).

After Metrics are Displayed, the Points are Large and Overlap the Base Map Labels, Hiding Place Names. How can I Adjust this?

Click **Road map** in **Layer**, then select **Edit layer settings**. In **Layer settings**, set the base map display priority to top.

Third-Party Cookie Settings

Last updated : 2024-12-04 16:47:23

To use the console retrieval and analysis capabilities, your browser should support third-party cookies. Common browser settings are as follows:

Chrome

- 1. Open the Chrome browser.
- 2. Click More Options in the upper right corner



3. Click Settings > Privacy and security > Third-party cookies > Allow third-party cookies.

0	Settings	Q Search settings
G	You and Google	
©=	Autofill and passwords	
0	Privacy and security	Take the Privacy Guide
Ø	Performance	
Ô	Appearance	Get started No thanks
۹	Search engine	
	Default browser	Safety Check
U	On startup	Chrome regularly checks to make sure your browser has the safest settings. Go to Safety Check
×A	Languages	we in let you know in anything needs your review.
₹	Downloads	Privacy and security
Ť	Accessibility	Delete browsing data
e,	System	Delete history, cookies, cache, and more
ð	Reset settings	Privacy Guide Review key privacy and security controls
÷	Extensions	Third-party cookies
0	About Chrome	
		Customize the info used by sites to show you ads
		Security Safe Browsing (protection from dangerous sites) and other security settings
		Image: Site settings Site settings Controls what information sites can use and show (location, camera, pop-ups, and more)

← Thir	d-party cookies	⑦ ♀ Search	-
Manage th	the types of information sites can use to track you as you brow	se.	
Allo	w third-party cookies	^	-
٩	Sites can use cookies to improve your browsing experience to remember items in your shopping cart	, for example, to keep you signed in or	
٩	Sites can use cookies to see your browsing activity across of personalize ads	lifferent sites, for example, to	
O Bloc	k third-party cookies in Incognito mode	~	,
O Bloo	k third-party cookies	~	

Safari

- 1. Open Safari on your Mac computer.
- 2. Go to **Safari Browser** > **Settings** to open the settings interface.



3. In the Privacy settings, uncheck **Prevent cross-site tracking** and **Manage Website Data**.

				Privacy						
ငို ပ္ပဲ General	Tabs Auto	Fill Passwords	Q Search	Security	Privacy	Websites	O Profiles	کی Extensions	දිරි}දුරු Advanced	
	Website t	tracking: 🗌 Pı	event cro	ss-site tra	cking					
	Hide IP address: 🗹 Hide IP address from trackers									
		Yo liki IP	ur IP addre e your locat address fro	ss can be us tion. To prot om known tr	sed to dete ect this inf ackers. Le	ermine perse formation, S arn more	onal inform Safari can h	nation, ide your		
	Webs	ite data: Mar	nage Web	site Data						
	Private B	rowsing: 🗹 Re	equire Tou	ich ID to v	iew locke	ed tabs				
Advanced Settings	3							About Sa	afari & Privac	х у

Field Type Conversion Through Reindex

Last updated : 2024-12-04 16:50:23

Overview

When you create an index in the ES Serverless service, a time field should be specified, and its type should be set to date . When you synchronize data from an existing ES cluster to an index in the ES Serverless service, if the field in the data has the same name as the time field but a different type, the write operation will fail. In this case, you can use the Reindex API to convert the field type.

Process Description

1. Create the target index for reindexing, and set the type of the field to date if the field has the same name as the time field in the ES Serverless service index.

2. Use the reindex API to synchronize the existing data to the target index.

Example

1. Suppose we need to synchronize data from the source_index to an index in the ES Serverless service (where
the time field is @timestamp). Upon checking the field configuration of source_index, we find that in
source_index, the field @timestamp is of type keyword. In this case, attempting to synchronize the data
will result in a write error.

GET source index (manning	1 - {
de risour de_ macky_mapping	2 * "source_index" : {
	3 - "mappings" : {
	4. dynamic templates" · [
	6 message_full" : {
	7 "match" : "message_full",
	8 - "mapping" : {
	9- "fields" : {
	10 - "keyword" · {
	11
	12 Use use use use and use use and use use and use use use and use
	12 Cype : Keyword
	13* }
	14 * },
	15 "type" : "text"
	16 - }
	17 - }
	18 - 1 3
	10 - 5
	20 message : {
	21 "match" : "message",
1	22 - "mapping" : {
	23 "type" : "text"
	24 * }
	25 - }
	26 *
	27 - 1 5
	29- "ctnings" + [
	29 "match_mapping_type" : "string",
	30 - "mapping" : {
	31 "type" : "keyword"
	32 • }
	33 * }
	34 * }
	35
	26 - Innonontios" · [
	27 elimeters
	37 · · · · · · · · · · · · · · · · · · ·
	38 "type" : "keyword"
	39 * \$,
	40- "field1" : {
	41 "type" : "text"
	42 * }
	43 * 3
w the number of deguments in source, index	

2. View the number of documents in source_index.



mapping as date .



```
POST _reindex
{
    "source": {
        "index": "source_index"
    },
    "dest": {
        "index": "dest_index"
    }
}
```



5. In this case, searching dest_index will retrieve the data that was synchronized from source_index .

