Log Tank Service

Best Practices

Issue	01
Date	2023-07-19

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Analyzing Huawei Cloud ELB Access Logs for O&M Insights

Introduction

When distributing external traffic, Elastic Load Balance (ELB) logs details of HTTP and HTTPS requests, such as URIs, client IP addresses and ports, and status codes.

You can use ELB access logs for auditing or search for logs by time and keyword. You can also obtain external access statistics by running SQL aggregation queries. For example, you can check the number of requests with 404 responses within a certain day, or analyze the unique visitors (UVs) or page views (PVs) within a week.

Prerequisites

You have purchased and used a load balancer.

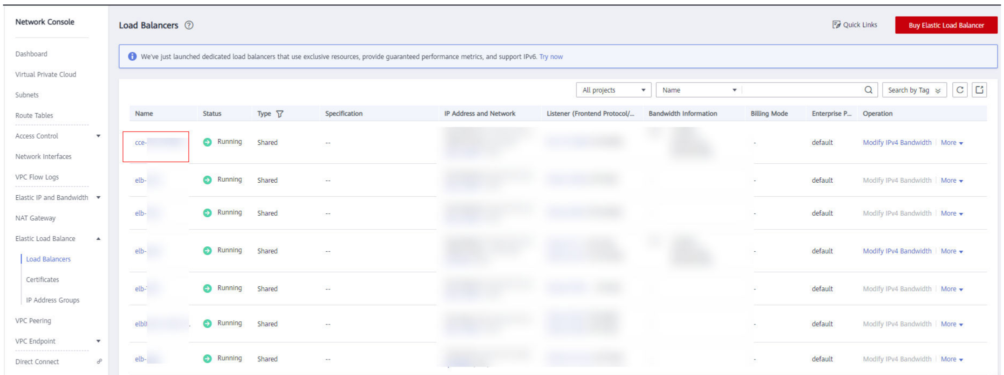
Restrictions

- ELB access logs only record layer 7 requests sent to the dedicated and shared load balancers. Layer 4 shared load balancing is not logged.

Procedure

Step 1 Report ELB access logs to LTS.

1. Log in to the management console.
2. Click 📍 in the upper left corner to select the desired region and project.
3. Click ☰ in the upper left corner and choose **Networking** > **Elastic Load Balance**.
4. On the **Load Balancers** page, click the name of a load balancer.



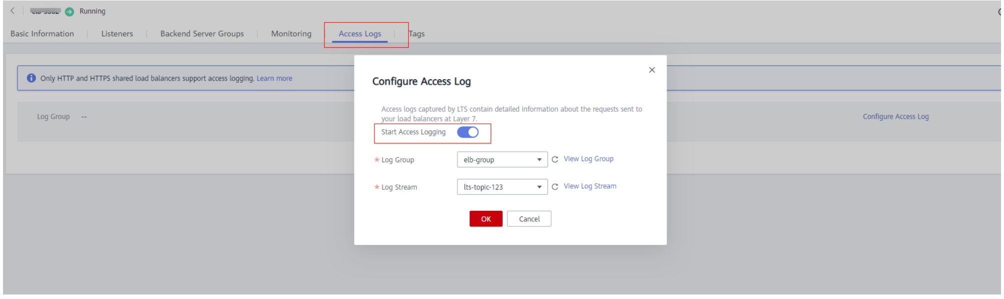
Load Balancers

We've just launched dedicated load balancers that use exclusive resources, provide guaranteed performance metrics, and support IPv6. Try now

Name	Status	Type	Specification	IP Address and Network	Listener (Frontend Protocol/...	Bandwidth Information	Billing Mode	Enterprise P...	Operation
cce-[redacted]	Running	Shared	--	[redacted]	[redacted]	[redacted]	-	default	Modify IPv4 Bandwidth | More
elb-[redacted]	Running	Shared	--	[redacted]	[redacted]		-	default	Modify IPv4 Bandwidth | More
elb-[redacted]	Running	Shared	--	[redacted]	[redacted]		-	default	Modify IPv4 Bandwidth | More
elb-[redacted]	Running	Shared	--	[redacted]	[redacted]	[redacted]	-	default	Modify IPv4 Bandwidth | More
elb-[redacted]	Running	Shared	--	[redacted]	[redacted]		-	default	Modify IPv4 Bandwidth | More
elbl[redacted]	Running	Shared	--	[redacted]	[redacted]		-	default	Modify IPv4 Bandwidth | More
elb-[redacted]	Running	Shared	--	[redacted]	[redacted]		-	default	Modify IPv4 Bandwidth | More

5. On the **Access Logs** tab, click **Configure Access Log**. Enable access logging, and select an LTS log group and log stream. If necessary, create a log group and a log stream first.

Figure 1-1 Reporting ELB access logs to LTS



Only HTTP and HTTPS shared load balancers support access logging. Learn more

Log Group --

Configure Access Log

Configure Access Log

Access logs captured by LTS contain detailed information about the requests sent to your load balancers at Layer 7.

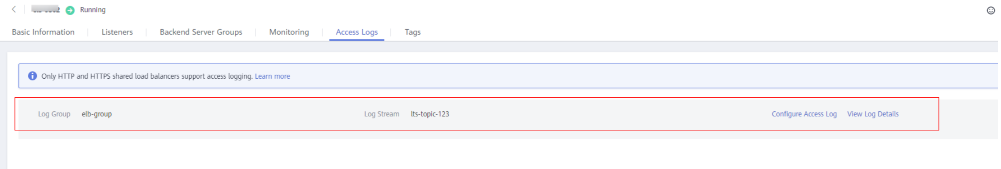
Start Access Logging

* Log Group: elb-group — View Log Group

* Log Stream: lts-topic-123 — View Log Stream

6. Click **OK**.

Figure 1-2 Access logs reported



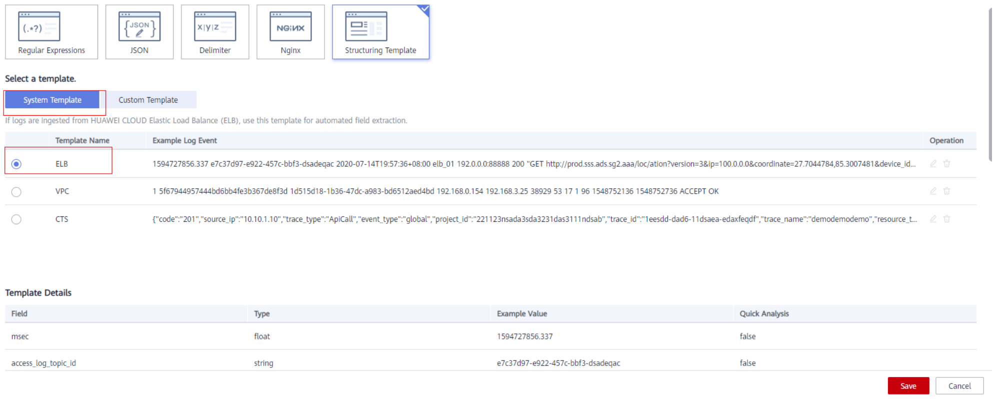
Only HTTP and HTTPS shared load balancers support access logging. Learn more

Log Group elb-group

Log Stream lts-topic-123

Step 2 Go to the log stream details page on the LTS console, choose **Log Configuration** in the navigation pane on the left, and click the **Log Structuring** tab. Select **Structuring Template** and select the ELB system template for log structuring. You can enable **Quick Analysis** if needed.

Figure 1-3 Selecting the ELB structuring template



Select a template.

If logs are ingested from HUAWEI CLOUD Elastic Load Balance (ELB), use this template for automated field extraction.

	Template Name	Example Log Event	Operation
●	ELB	1594727856.337 e7c37d97-e922-457c-bbf3-dsadeqac 2020-07-14T19:57:36+08:00 elb_01 192.0.0.0:88888 200 "GET http://prod.sss.ads.sg2.aaa/loc/ation?version=3&ip=100.0.0.0&coordinate=27.7044784,85.3007481&device_id...	
○	VPC	1 5f67944957444bd6bb4fe3b367de8f3d 1d515d18-1b36-47dc-a983-bd6512aed4bd 192.168.0.154 192.168.3.25 38929 53 17 1 96 1548752136 1548752736 ACCEPT OK	
○	CTS	{"code":"201","source_ip":"10.10.1.10","trace_type":"ApiCall","event_type":"global","project_id":"221123nsada3sda3231das3111ndsab","trace_id":"1eesdd-dad6-11dsaea-edaxfeqdf","trace_name":"demodemodemo","resource_t...	

Template Details

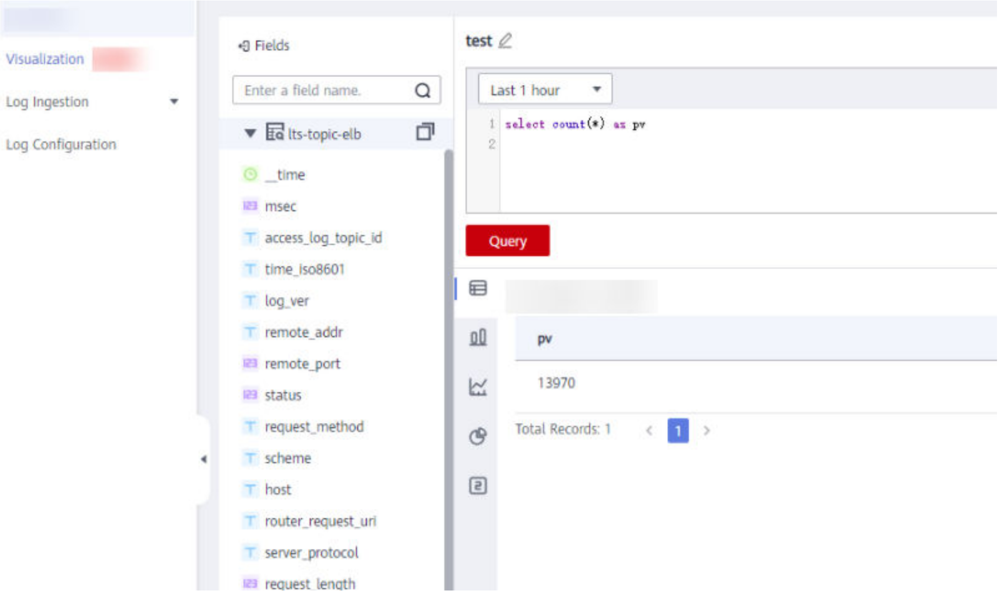
Field	Type	Example Value	Quick Analysis
msec	float	1594727856.337	false
access_log_topic_id	string	e7c37d97-e922-457c-bbf3-dsadeqac	false

Step 3 On the log stream details page, click **Visualization** and run SQL queries. For details about how to visualize query results, see "Log Structuring".

- To count the PVs within a week, run the following SQL statement:

```
select count(*) as pv
```

Figure 1-4 PVs



```
select count(*) as pv
```

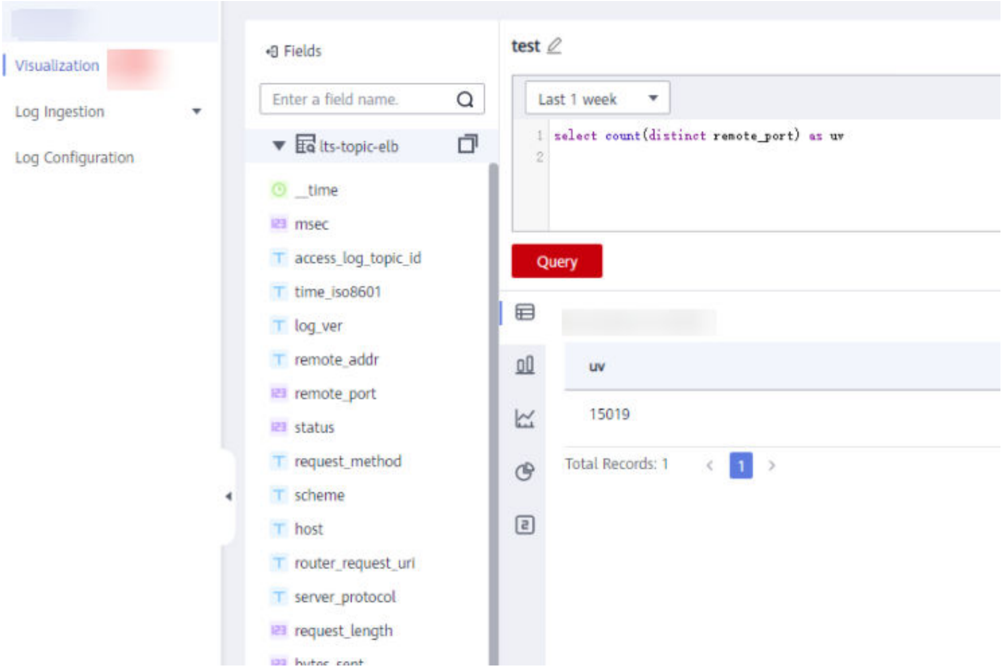
pv
13970

Total Records: 1 ‹ 1 ›

- To count the UVs within a week, run the following SQL statement:

```
select count(distinct remote_port) as uv
```

Figure 1-5 UVs



```
select count(distinct remote_port) as uv
```

uv
15019

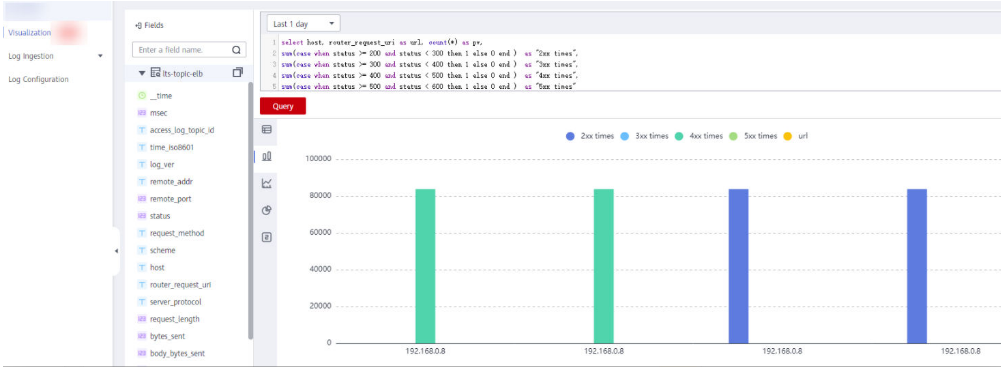
Total Records: 1 ‹ 1 ›

- Statistics on 2xx/3xx/4xx/5xx (return codes) returned by all URIs in one day are collected to show the service execution result. The SQL query and analysis statements are as follows:

```
select host, router_request_uri as url, count(*) as pv,
sum(case when status >= 200 and status < 300 then 1 else 0 end )  as "2xx times",
sum(case when status >= 300 and status < 400 then 1 else 0 end )  as "3xx times",
sum(case when status >= 400 and status < 500 then 1 else 0 end )  as "4xx times",
sum(case when status >= 500 and status < 600 then 1 else 0 end )  as "5xx times"
group by host, router_request_uri
order by pv desc
limit 100
```

You can visualize the results in a table, bar chart, line chart, pie chart, or number chart. **Figure 1-6** presents the results in a bar chart.

Figure 1-6 Response codes



```
select host, router_request_uri as url, count(*) as pv,
sum(case when status >= 200 and status < 300 then 1 else 0 end )  as "2xx times",
sum(case when status >= 300 and status < 400 then 1 else 0 end )  as "3xx times",
sum(case when status >= 400 and status < 500 then 1 else 0 end )  as "4xx times",
sum(case when status >= 500 and status < 600 then 1 else 0 end )  as "5xx times"
```

----End

2 Analyzing Huawei Cloud WAF Logs for O&M Insights

Introduction

Web Application Firewall (WAF) examines all HTTP and HTTPS requests to detect and block attacks such as SQL injections, cross-site scripting (XSS), Trojan upload, and command or code injections. You can check the access and attack logs for real-time decision-making, device O&M, and service trend analysis.

Prerequisites

- You have purchased and used a WAF instance.

Restrictions

- WAF logging is available only for cloud WAF instances.

Procedure

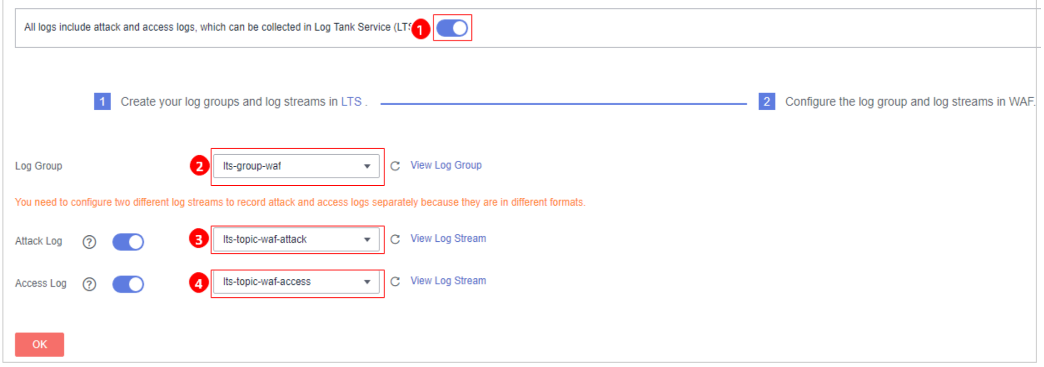
Step 1 Add a website to WAF.

1. Log in to the management console.
2. Click 📍 in the upper left corner to select the desired region and project.
3. Click ☰ in the upper left corner and choose **Security** > **Web Application Firewall**.
4. Add the domain name by referring to "Add a Domain Name to WAF".

Step 2 Enable WAF logging to collect WAF logs to LTS..

1. On the WAF console, choose **Events** in the navigation pane and click the **Configure Logs** tab. Enable logging and select a log group and log stream. If necessary, create a log group and a log stream first.
2. Click **OK**.

Figure 2-1 Configuring logs



All logs include attack and access logs, which can be collected in Log Tank Service (LTS

1 Create your log groups and log streams in LTS .

2 Configure the log group and log streams in WAF.

Log Group: lts-group-waf — View Log Group

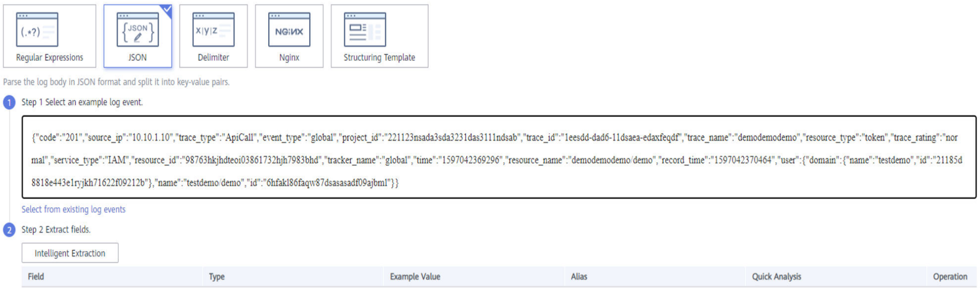
You need to configure two different log streams to record attack and access logs separately because they are in different formats.

Attack Log: lts-topic-waf-attack — View Log Stream

Access Log: lts-topic-waf-access — View Log Stream

Step 3 Go to the log stream details page on the LTS console, choose **Log Configuration** in the navigation pane on the left, and click the **Log Structuring** tab. Select **JSON**, select a sample log event, and complete the configuration.

Figure 2-2 Configuring logs in JSON format



Parse the log body in JSON format and split it into key-value pairs.

1 Step 1 Select an example log event.

```
{"code":"201","source_ip":"10.10.1.10","trace_type":"ApiCall","event_type":"global","project_id":"221123nsada3sda3231das3111ndsab","trace_id":"1eesdd-dad6-11dsaea-edaxfeqdf","trace_name":"demodemodemo","resource_type":"token","trace_rating":"normal","service_type":"IAM","resource_id":"98763hkjhdteoi03861732hjh7983bhd","tracker_name":"global","time":"1597042369296","resource_name":"demodemodemo/demo","record_time":"1597042370464","user":{"domain":{"name":"testdemo","id":"21185d8818e443e1ryjkh71622f09212b"},"name":"testdemo/demo","id":"6hfakl86faqw87dsasasadf09ajbml"}}
```

Select from existing log events

2 Step 2 Extract fields.

Intelligent Extraction

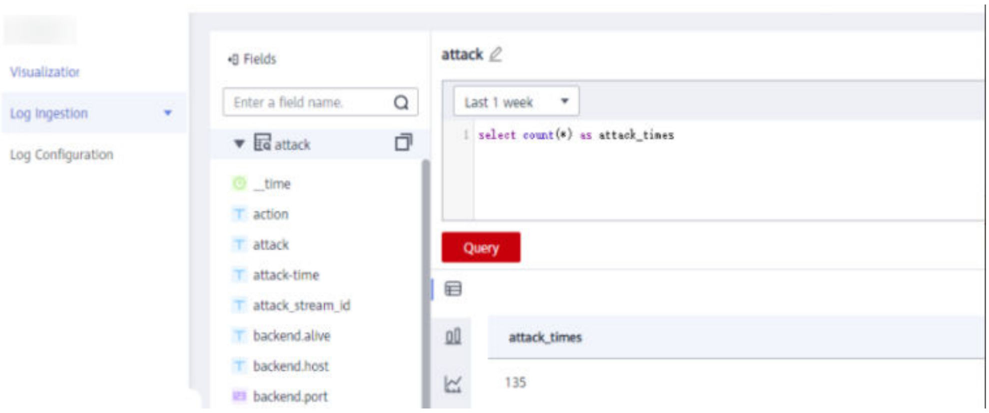
Field	Type	Example Value	Alias	Quick Analysis	Operation

Step 4 On the log stream details page, click **Visualization** and run SQL queries. For details about how to visualize query results, see "Log Structuring".

- To count the number of attacks within a week, run the following SQL statement:

```
select count(*) as attack_times
```

Figure 2-3 Number of attacks within a week



```
select count(*) as attack_times
```

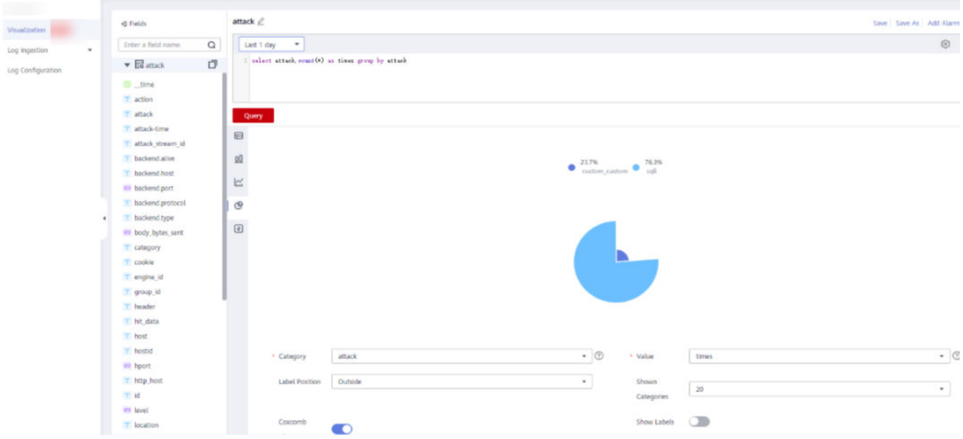
attack_times
135

- To count the number of attacks by type in one day, run the following SQL statement:

```
select attack,count(*) as times group by attack
```

You can visualize the results in a table, bar chart, line chart, pie chart, or number chart. The following figure presents the results in a pie chart.

Figure 2-4 Number of attacks by type



```
select attack,count(*) as times group by attack
```

Category: attack

Value: times

Label Position: Outside

Shown Categories: 20

Coxcomb

Show Labels

----End

3 Analyzing Application Run Logs (in Log4j Format)

Introduction

Log4j is Apache's open-source project used for logging. We can calculate the number and proportion of logs at different levels, or gather statistics on services from run logs.

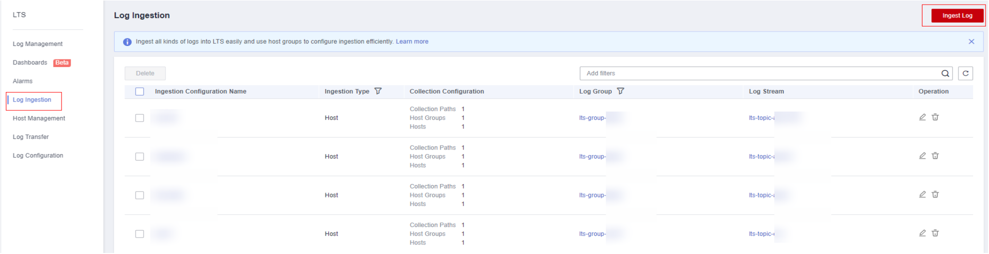
For example, you can know the transaction volume of an offering on a day from logs such as the following:

```
2020-12-28_21:10:48.081 [http-nio-8083-exec-6] INFO  discounted shoes - num is :9
```

Procedure

Step 1 Log in to the LTS console and choose **Log Ingestion** in the navigation pane.

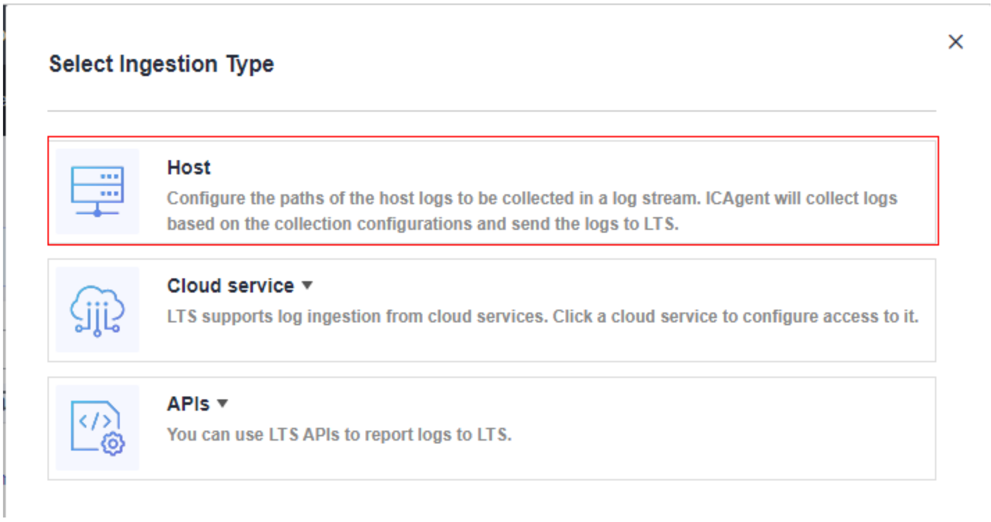
Step 2 Click **Ingest Log** in the upper right corner.



Ingest all kinds of logs into LTS easily and use host groups to configure ingestion efficiently. Learn more

Ingestion Configuration Name	Ingestion Type	Collection Configuration	Log Group	Log Stream	Operation
[redacted]	Host	Collection Paths 1 Host Groups 1 Hosts 1	lts-group-[redacted]	lts-topic-[redacted]	
[redacted]	Host	Collection Paths 1 Host Groups 1 Hosts 1	lts-group-[redacted]	lts-topic-[redacted]	
[redacted]	Host	Collection Paths 1 Host Groups 1 Hosts 1	lts-group-[redacted]	lts-topic-[redacted]	
[redacted]	Host	Collection Paths 1 Host Groups 1 Hosts 1	lts-group-[redacted]	lts-topic-[redacted]	

Step 3 On the **Select Ingestion Type** page, select **Host**.



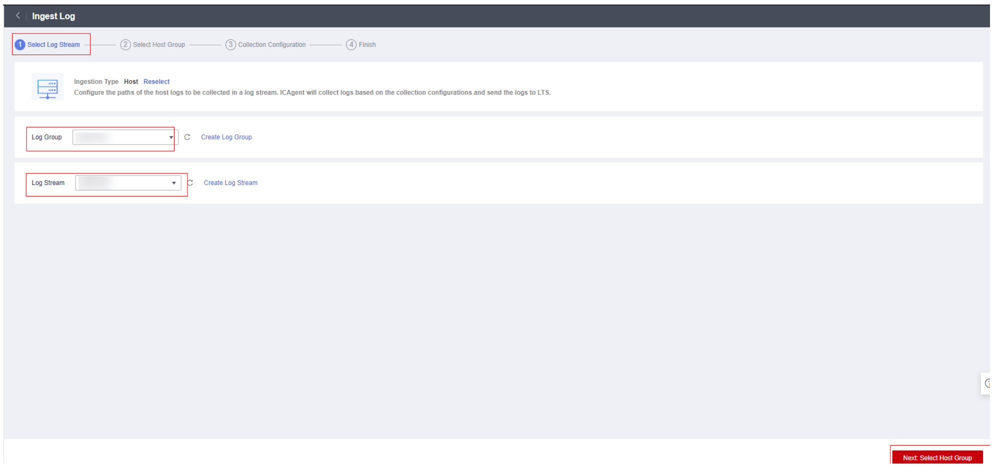
Host
Configure the paths of the host logs to be collected in a log stream. ICAgent will collect logs based on the collection configurations and send the logs to LTS.

Cloud service ▾
LTS supports log ingestion from cloud services. Click a cloud service to configure access to it.

APIs ▾
You can use LTS APIs to report logs to LTS.

Step 4 Select a log stream.

1. Select a log group from the drop-down list of **Log Group**. If there are no desired log groups, click **Create Log Group** to create one.
2. Select a log stream from the drop-down list of **Log Stream**. If there are no desired log streams, click **Create Log Stream** to create one.
3. Click **Next: Select Host Group**.



Ingestion Type Host Reselect
Configure the paths of the host logs to be collected in a log stream. ICAgent will collect logs based on the collection configurations and send the logs to LTS.

Log Group

Log Stream

Step 5 Select host groups.

1. Select one or more host groups from which you want to collect logs. If there are no desired host groups, click **Create** above the host group list to create one. For details, see "Managing Host Groups".

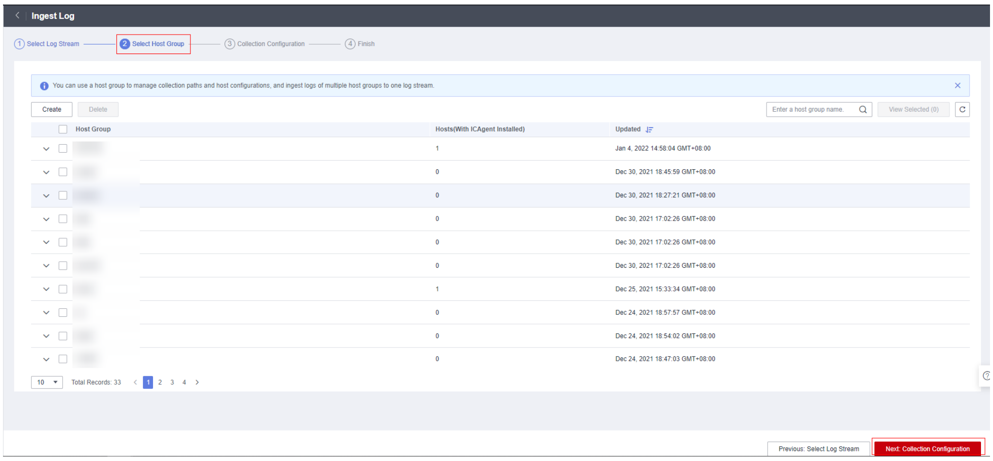
   NOTE

   You can choose not to select a host group in this step, but associate a host group with the ingestion configuration after you finish the procedure here. To do this, either:

   – Choose **Host Management** in the navigation pane, click the **Host Groups** tab, and make the association, or

   – Choose **Log Ingestion** in the navigation pane, click an ingestion configuration, and make the association on the details page.

2. Click **Next: Collection Configuration**.



Ingest Log

You can use a host group to manage collection paths and host configurations, and ingest logs of multiple host groups to one log stream.

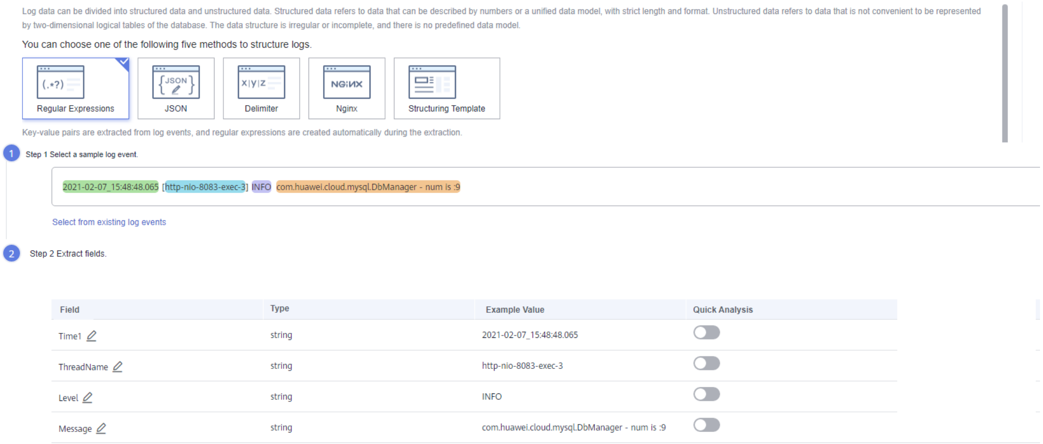
	□ Host Group	Hosts(With ICAgent Installed)	Updated
⌄	□ [redacted]	1	Jan 4, 2022 14:58:04 GMT+08:00
⌄	□ [redacted]	0	Dec 30, 2021 18:45:59 GMT+08:00
⌄	□ [redacted]	0	Dec 30, 2021 18:27:21 GMT+08:00
⌄	□ [redacted]	0	Dec 30, 2021 17:02:26 GMT+08:00
⌄	□ [redacted]	0	Dec 30, 2021 17:02:26 GMT+08:00
⌄	□ [redacted]	0	Dec 30, 2021 17:02:26 GMT+08:00
⌄	□ [redacted]	1	Dec 25, 2021 15:33:34 GMT+08:00
⌄	□ [redacted]	0	Dec 24, 2021 18:57:57 GMT+08:00
⌄	□ [redacted]	0	Dec 24, 2021 18:54:02 GMT+08:00
⌄	□ [redacted]	0	Dec 24, 2021 18:47:03 GMT+08:00

Step 6 Configure the collection.

1. Configure the collection parameters. For details, see "Configuring Collection".
2. Click **Submit**.

Step 7 On the log stream details page, choose **Log Configuration** in the navigation pane and click the **Log Structuring** tab. On the page displayed, select **Regular Expressions**, select a log event, and extract four fields: **Time1**, **ThreadName**, **Level**, and **Message**, as shown in **Figure 3-1**.

Figure 3-1 Structuring logs with regular expressions



Log data can be divided into structured data and unstructured data. Structured data refers to data that can be described by numbers or a unified data model, with strict length and format. Unstructured data refers to data that is not convenient to be represented by two-dimensional logical tables of the database. The data structure is irregular or incomplete, and there is no predefined data model.

You can choose one of the following five methods to structure logs.

Key-value pairs are extracted from log events, and regular expressions are created automatically during the extraction.

1 Step 1 Select a sample log event.

```
2021-02-07_15:48:48.065 [http-nio-8083-exec-3] INFO com.huawei.cloud.mysql.DbManager - num is :9
```

2 Step 2 Extract fields.

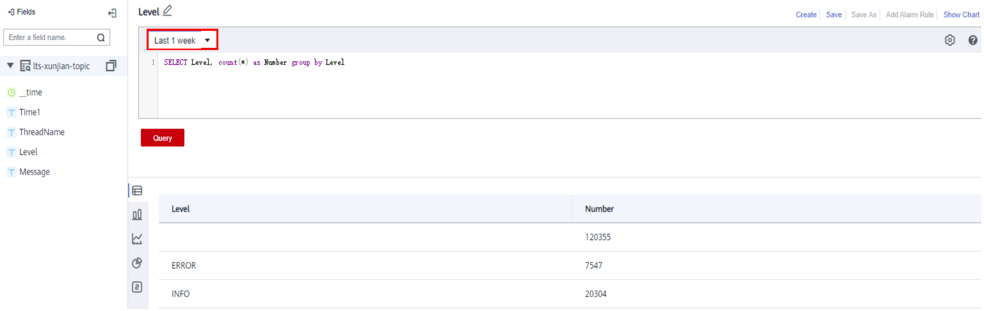
Field	Type	Example Value	Quick Analysis
Time1	string	2021-02-07_15:48:48.065	○
ThreadName	string	http-nio-8083-exec-3	○
Level	string	INFO	○
Message	string	com.huawei.cloud.mysql.DbManager - num is :9	○

Step 8 On the log stream details page, click **Visualization** and run SQL queries. For details about how to visualize query results, see "Log Structuring".

- To query the error type distribution in the last seven days, run the following SQL statement:

```
SELECT Level, count(*) as Number group by Level
```

Figure 3-2 Error type distribution



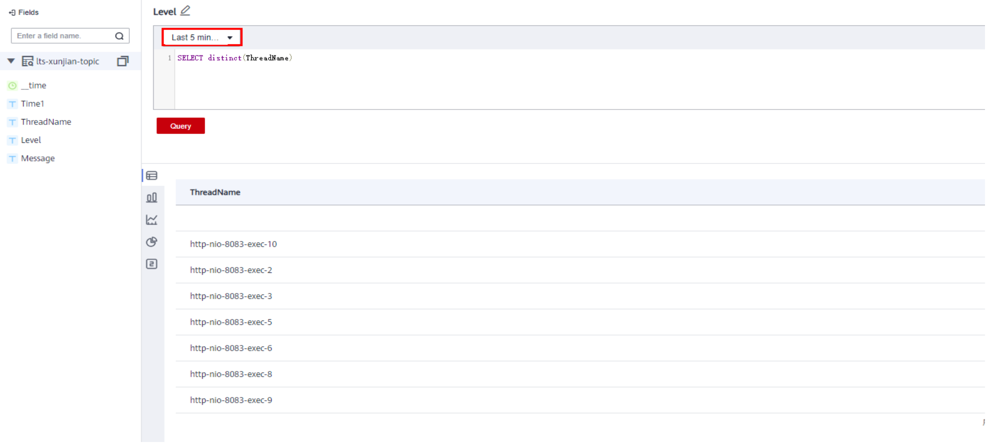
```
SELECT Level, count(*) as Number group by Level
```

Level	Number
	120355
ERROR	7547
INFO	20304

- To query the running threads in the last 5 minutes, set the time range to **Last 5 minutes** and run the following SQL statement:

```
SELECT distinct(ThreadName)
```

Figure 3-3 Running threads



```
SELECT distinct(ThreadName)
```

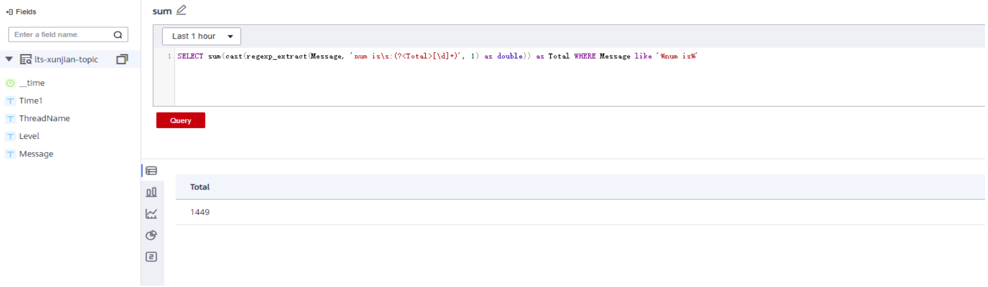
ThreadName
http-nio-8083-exec-10
http-nio-8083-exec-2
http-nio-8083-exec-3
http-nio-8083-exec-5
http-nio-8083-exec-6
http-nio-8083-exec-8
http-nio-8083-exec-9

- To query the total transaction volume of a product, run the following SQL statement:

```
SELECT sum(cast(regexp_extract(Message, 'num is\s:(?<Total>[\d]+)', 1) as double)) as Total WHERE Message like '%shoes%'
```

The query looks for fuzzy match, and the following is an example query result.

Figure 3-4 Total transaction volume



```
SELECT sum(cast(regexp_extract(Message, 'num is\s:(?<Total>[\d]+)', 1) as double)) as Total WHERE Message like '%num is%'
```

Total
1449

----End