# MapReduce Service (MRS)
# 3.3.1-LTS

# References

**Issue** 01

**Date** 2024-04-30

HUAWEI

**HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.**

### Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

### 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.

## Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

# Contents



# 1 Log Reference

## 1.1 Overview

### Introduction

Logs record system running status and process execution status, serving as a basis for users to collect fault information and helping maintenance engineers check the system status and locate faults.

Log functions include but are not limited to the following:

- Recording system running status and action information
- Detecting and recording internal errors, including the error conditions, environments, and trajectory.

MRS service logs include the logs of the cloud service management modules and tenant-side run logs of each component in the MRS cluster. For details, see **Table 1-2**.

Maintenance engineers can collect system logs of the management and control plane on ManageOne Maintenance Portal to locate faults. They can also log in to the cloud service management VM to view logs.

You can log in to FusionInsight Manager to search for logs of each component in the MRS cluster online or download logs of a specified component or node to the local PC.

This document describes the meaning, format, parameters, and examples of different run logs to help maintenance engineers understand logs and quickly locate faults.

- The "Log Description" section describes the information recorded in a log or the usage of the log.
- The "Log level" section describes the level of a log, as shown in **Table 1-1**.
- The "Log Format" section describes the elements contained in a log.
- The "Log Parameters" section describes parameters included in a log.

**Table 1-1** Log levels

| Level | Description |
| --- | --- |
| TRACE | Records information whose granularity is lower than that of DEBUG. |
| DEBUG | Records the system information and system debugging information. |
| INFO | Records normal running status information about the system and events. |
| WARN | Records exception information about the current event processing. |
| ERROR | Records error information about system running. |
| FATAL | Records critical information about the system. |
| OFF | Indicates that the log output is disabled. |
| NOTICE | Records suitable details and is applicable to the production environment. |
| VERBOSE | Records normal running status information about the system and events. |

NOTE

The log levels supported by different modules are slightly different. For details, see the following sections.

## Log List

**Table 1-2** Log list of each MRS module

| Category | Module | Log Details |
| --- | --- | --- |
| Management and control plane | APIGateway | **APIGateway Log** |
| | Deployer | **Deployer Log** |
| | Database | **Database Log** |
| | ZooKeeper | **ZooKeeper Log** |
| | Console | **Console Log** |
| | Console-Stage | **MRS Service Run Log** |
| Tenant plane | CDL | **CDL Log Overview** |
| | ClickHouse | **ClickHouse Log Overview** |
| | DBService | **DBService Log Overview** |

| Category | Module | Log Details |
| --- | --- | --- |
| | Elasticsearch | **Elasticsearch Log Overview** |
| | Flink | **Flink Log Overview** |
| | Flume | **Flume Log Overview** |
| | FTP-Server | **FTP-Server Log Overview** |
| | HBase | **HBase Log Overview** |
| | HDFS | **HDFS Log Overview** |
| | HetuEngine | **HetuEngine Logs** |
| | Hive | **Hive Log Overview** |
| | Hue | **Hue Log Overview** |
| | loTDB | **IoTDB Log Overview** |
| | Kafka | **Kafka Log Overview** |
| | Knox | **Knox Logs** |
| | Executor | **Executor Logs** |
| | Loader | **Loader Log Overview** |
| | MapReduce | **Introduction to MapReduce Logs** |
| | Oozie | **Oozie Log Overview** |
| | Ranger | **Ranger Log Overview** |
| | Redis | **Redis Log Overview** |
| | Solr | **Solr Log Overview** |
| | Spark | **Spark Log Overview** |
| | Yarn | **Yarn Log Overview** |
| | ZooKeeper | **ZooKeeper Log Overview** |

# 1.2 Log Reference on the Management Plane

## 1.2.1 Log Collection

### Scenario

If an exception occurs, maintenance engineers can log in to ManageOne Maintenance Portal and the service host background to collect system logs of the management plane and locate the fault.

## Prerequisites

- You have obtained the administrator account.
- You have logged in to ManageOne Maintenance Portal.

## Downloading Management Plane Logs on the Web UI

**Step 1** Log in to ManageOne Maintenance Portal using a browser.

- Login with the URL: **https://***Domain name of ManageOne Maintenance Portal*:**31943**. Alternatively, access **https://***Address for accessing the ManageOne unified portal* to log in to the ManageOne unified portal and choose OperationCenter to access ManageOne Maintenance Portal.

  Obtain the domain name of ManageOne Maintenance Portal on the "2.3 Portal" sheet of the deployment parameter table exported from HCC Turnkey during the installation of Huawei Cloud Stack basic services.
- Login using a password: Enter the username and password.

  Default account: bss_admin. To obtain the default password, contact the system administrator or refer to the default password of the ManageOne Maintenance Portal account on the "Type A (Portal)" sheet in ***Huawei Cloud Stack 8.3.1 Account List***.

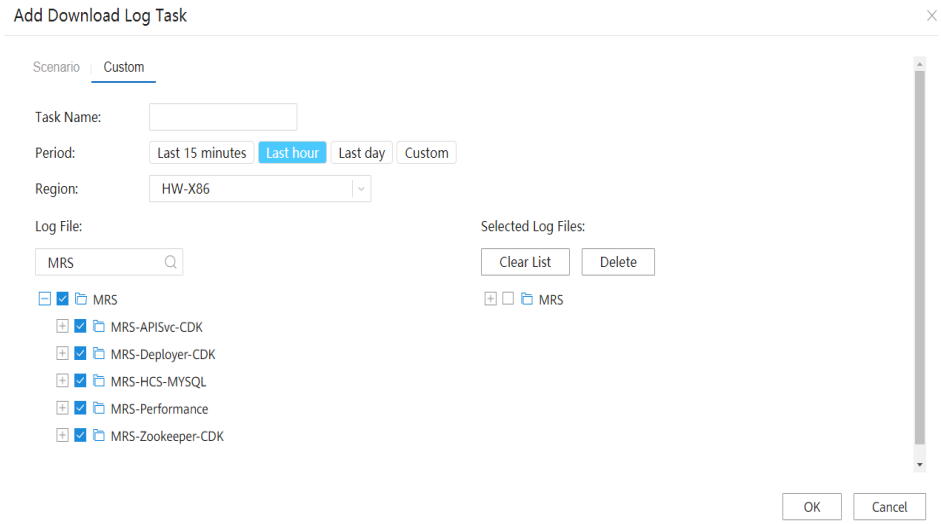
  NOTE

  For ManageOne upgraded from 8.2.0 or an earlier version, the default account name is **admin**.
- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter a PIN.

**Step 2** Choose **O&M** > **Logs** > **Run Logs** > **Management Run Log Download**.

**Step 3** On the displayed page, click **Add Download Log Task**. On the **Add Download Log Task** page, click the **Custom** tab, enter a task name, and set **Period**.

**Step 4** In the **Log File** area, select the target MRS logs and click **OK** to add the download task.




**Step 5** After the download task is successfully added, click **Download** in the **Download File** column to download logs.

**Step 6** Analyze the log error cause and locate the fault.

**----End**

## Viewing Logs by Logging to the Management Host

**Step 1** Log in to the **EICommon-Region-Master-01** VM as user **opsadmin**. For details, see **Logging In to an MRS Management Node**.

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the system administrator.

**Step 2** Switch to the target log directory and view the logs. The log directories are as follows:

- MRS-Performance logs:
  - /var/log/paas/cam-tiller/
  - /var/log/paas/canal/
  - /var/log/paas/cce-agent/
  - /var/log/paas/haproxy-keepalived/
  - /var/log/paas/kubernetes/

**Step 3** Run the following command to query the names of all MRS containers in the cluster and obtain the IP addresses in the **NODE** column:

**kubectl get pods -n mrs -owide**

```
NAME                        READY   STATUS    RESTARTS   AGE     IP           NODE           NOMINATED
NODE   READINESS GATES
mrsapigw-6f56bc476d-c5cs9     1/1     Running   0          19h     10.16.0.69   10.69.26.187   <none>
<none>
mrsapigw-6f56bc476d-smqn8     1/1     Running   0          5d13h   10.16.0.20   10.69.26.197
<none>           <none>
mrsdeployer-5988d78867-2prk6   1/1     Running   0          43h     10.16.0.55   10.69.26.194   <none>
<none>
mrsdeployer-5988d78867-8lb5p   1/1     Running   0          43h     10.16.0.25   10.69.26.197   <none>
<none>
mrsdeployer-5988d78867-gwqb7   1/1     Running   0          43h     10.16.0.86   10.69.26.189
<none>           <none>
```

**Step 4** Log in to the **MRS-Api** or **MRS-Deploy** node using the IP address obtained in **Step 3** as user **opsadmin**. (The node name is the container name starting with **mrsapigw** or **mrsdeployer** in **Step 3**.)

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the system administrator.

**Step 5** Switch to the target log directory and view the logs. The log directories are as follows:

- MRS-Api logs:
  - /var/log/mrs/apigw/hwctrace/
  - /var/log/mrs/apigw/apigateway/
- MRS-Deploy logs:
  - /var/log/mrs/deployer/hwctrace/

- /var/log/mrs/deployer/service-deployer/

**Step 6** Click the **VMs** tab, enter the keyword **MRS_Region_Node** in the search box to search for the VM, and record the IP address of the VM.

NOTE

In the non-DR deployment scenario of the MRS management plane, the ZooKeeper process is deployed on the **MRS_Region_Node** VM. In the cross-AZ DR deployment scenario of the MRS management plane, the ZooKeeper process is deployed on the **MRS-Zookeeper** and **MRS-Zookeeper-DC** VMs.

**Step 7** Log in to the VM as user **opsadmin**.

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the system administrator.

**Step 8** Switch to the target log directory and download the logs. The log directories are as follows:

MRS-ZooKeeper logs:

- /opt/cloud/logs/zookeeper/

**Step 9** Click the **VMs** tab, enter the keyword **MRS_DB** in the search box to search for the VM, and record the IP address of the VM.

**Step 10** Log in to the VM as user **opsadmin**.

Run the **su - root** command to switch to user **root**.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the system administrator.

**Step 11** Switch to the target log directory and download the logs. The log directories are as follows:

MRS-HCS-MySQL logs:

- /data/mysql/logs/

**Step 12** Analyze the log error cause and locate the fault.

**----End**

# 1.2.2 APIGateway Log

## Log Description

The APIGateway log records the process when a user invokes the MRS interface. By viewing the APIGateway log, the system administrator and the maintenance personnel can check the processing result of requests sent from Console or the API Gateway, thereby locating problems quickly.

## Log Level

| Level | Description |
| --- | --- |
| DEBUG | Records the APIGateway working process, including the log information and related parameters of each operation. |
| INFO | Records the working process and related key operations during the APIGateway running. |
| WARN | Records the problems or exceptions that may occur during the running of the system. |
| ERROR | Records errors that occur during the APIGateway running, for example, the APIGateway fails to communicate with the IAM or the ServiceManager. |

## Log Path

You can set the log path of the APIGateway in the **/opt/cloud/MRS-APISvc/conf/config/log4j2.xml** file of the mrsapigw container, as shown in the following:

```
    <RollingFile name="R"
                 filename="/opt/cloud/logs/apigateway/api-gateway.log"
                 filepattern="/opt/cloud/logs/apigateway/api-gateway.log.%i.gz"
                  >
      <PatternLayout pattern="[%d{yyyy-MM-dd HH:mm:ss,SSS Z}] [%-5p] [%t] [%c %L] %enc{%m}
{CRLF}%n" />
      <Policies>
        <SizeBasedTriggeringPolicy
            size="20 MB" />
      </Policies>
      <ChownRolloverStrategy max="50" />
    </RollingFile>
```

The default log path is **/opt/cloud/logs/apigateway/api-gateway.log** in the **mrsapigw** container.

## Log Format

APIGateway logs are classified into the following types:

- [*Log generation time*][*Log level*][*Thread name*][*Invoked function*] *Content*
- [*Log generation time*] [*Log level*] [*Thread name*] [*Invoked function*] [*Request ID*] [*Step*] [*Initiator*] [*Action*] [*Processor*] [*Result*] [*Parameter 1*] [*Parameter 2*] Content

## Log Parameter

| Parameter | Description |
| --- | --- |
| Log generation time | Indicates the time when the log service tool records the log. |
| Log level | The levels include ERROR, WARN, INFO, and DEBUG. |

| Parameter | Description |
| --- | --- |
| Thread name | Records the ID of the thread in the process where the log event occurs. |
| Invoked function | The information includes the address of the running file and the number of lines of the running code. |
| Content | Records the detailed information about the log, including the description and necessary context information. |
| Request ID | Indicates the ID carried in the request sent by the initiator to the processor. |
| Step | The options are as follows:<br>(* indicates the specific service: bigdata):<br>● ***.create_cluster**: creating a cluster<br>● ***.delete_cluster**: deleting a cluster<br>● ***.scale_out**: scaling out a cluster<br>● ***.job**: job-related<br>● ***.data**: data-related<br>● ***.list**: list-related |
| Initiator | It consists of the following modules:<br>● Console<br>● API-GW<br>● BSS |
| Action | Indicated the interaction between the initiator and handler. |
| Processor | It consists of the following modules:<br>● Console<br>● API-GW<br>● iamproxy<br>● BSS<br>● IAM<br>● VPC<br>● ECS<br>● NOVA<br>● FSP |
| Result | The options are as follows:<br>● **SUCCESS**: indicates the task is successfully executed.<br>● **FALSE**: failure<br>● **TIMEOUT**: timeout |

| Parameter | Description |
| --- | --- |
| Parameter 1 | Indicates the ID or name of a cluster or job. |
| Parameter 2 | This parameter is optional. When the result is **FALSE** or **TIMEOUT**, the value of this parameter is the invoking method, function, or address. |

### Example Log

A typical APIGateway log is as follows:

```
[2019-04-29 09:43:05,811 +0800] [INFO ] [http-bio-10.63.38.90-20002-exec-68]
[com.huawei.bigdata.api.emr.controller.ClusterController 4914] [5a336a17-5845-4e3e-9eeb-860e236f332d]
[bigdata.nodeGroups][api]cluster 513d78ef-d40b-48fa-bb41-741437b12223,master node size
Si1.xlarge.4.linux.bigdata,master node number 1
[2019-04-29 09:43:05,811 +0800] [INFO ] [http-bio-10.63.38.90-20002-exec-68]
[com.huawei.bigdata.api.emr.controller.ClusterController 4920] [5a336a17-5845-4e3e-9eeb-860e236f332d]
[bigdata.nodeGroups][api]cluster 513d78ef-d40b-48fa-bb41-741437b12223,analysis core node size
Si1.xlarge.4.linux.bigdata,analysis core node number 1
[2019-04-29 09:44:07,530 +0800] [INFO ] [http-bio-10.63.38.90-20002-exec-68]
[com.huawei.bigdata.api.emr.controller.TagController 373] [listTagsByTalent]Start list all tags for mrs and
predefined
```

## 1.2.3 Deployer Log

### Log Description

Deployer logs record the process in which the Deployer processes requests. By viewing the Deployer log, the system administrator or maintenance personnel can check the running status of the Deployer adapter. Therefore, if a problem occurs during cluster creation, they can quickly locate the problem.

### Log Level

| Level | Description |
| --- | --- |
| DEBUG | Records the Deployer working process, including the log information and related parameters of each operation. |
| INFO | Records the working process and related key operations during the Deployer running. |
| WARN | Records the problems or exceptions that may occur during the running of Deployer. |
| ERROR | Records errors that occur during the Deployer running. |

### Log Path

You can set the **appender.rfa.filename** parameter in the **/opt/cloud/MRS-Deployer/conf/log4j2.properties** file of the corresponding **mrsdeployer** container to set the log path of the MRS Deployer.

The default log file is **/opt/cloud/logs/service-deployer/service-deployer-service-deployer.log** in the container corresponding to **mrsdeployer**.

## Log Format

Log generation time Log level [Thread name] [Class name Line number] Content

## Log Parameter

| Parameter | Description |
| --- | --- |
| Log generation time | Indicates the time when the log service tool records the log. |
| Log level | The levels include ERROR, WARN, INFO, and DEBUG. |
| Thread name | Records the ID of the thread in the process where the log event occurs. |
| Class name Line number | Records the class name and line number of the printed log. |
| Content | Records the detailed information about the log, including the description and necessary context information. |

## Example Log

A typical Deployer log is as follows:

```
2020-12-25 11:00:46,590 INFO [main] [Box.<init> 62] -Database connected.
2020-12-25 11:00:47,471 INFO [main] [PluginManager.<init> 33] -Loading plugin resource-provider com.huawei.mrs.billing.BillingDataConfig
2020-12-25 11:00:47,474 INFO [main] [PluginManager.<init> 33] -Loading plugin facade-controller com.huawei.mrs.billing.BillingDataGenerator
2020-12-25 11:00:47,478 INFO [main] [PluginManager.<init> 33] -Loading plugin runner-impl com.huawei.mrs.box.workflow.ProbeAction
2020-12-25 11:00:47,480 INFO [main] [PluginManager.<init> 33] -Loading plugin workflow-impl com.huawei.mrs.box.workflow.ProbeWorkflow
2020-12-25 11:00:47,482 INFO [main] [PluginManager.<init> 33] -Loading plugin facade-controller com.huawei.mrs.controller.LogLevelController
2020-12-25 11:00:47,483 INFO [main] [PluginManager.<init> 33] -Loading plugin resource-provider com.huawei.mrs.facade.FacadeServiceSubscriber
2020-12-25 11:00:47,494 INFO [main] [PluginManager.<init> 33] -Loading plugin resource-provider com.huawei.mrs.common.util.GlobalExecutorService
2020-12-25 11:00:47,508 INFO [main] [PluginManager.<init> 33] -Loading plugin scheduler-listener com.huawei.mrs.scaling.ScaleJobListener
```

# 1.2.4 Database Log

## Log Description

The Database logs record the operation process information about MySQL databases in MRS. When a problem occurs during metadata read, storage, or modification of an MRS cluster, the system administrator or maintenance personnel can check the Database log to locate the problem.

NOTE

To view database logs, log in as the **root** user.

## Log Level

| Level | Description |
| --- | --- |
| Note | Records the working process and related key operations during the Database running. |
| Warning | Records the problems or exceptions that may occur during the database running. |
| Error | Records errors that occur during the database running. |

## Log Path

You can set the **--log_error** parameter to set the log path of MySQL during MySQL startup.

Log in to the MRS_DB node as user **opsadmin** and switch to user **root** to view database logs. Logs are stored in **/data/mysql/logs/error.log** by default.

## Log Format

[Log generation time] [Thread ID] [Error level] Content

## Log Parameter

| Parameter | Description |
| --- | --- |
| Log generation time | Indicates the time when the log service tool records the log. |
| Thread ID | Records the ID of the thread in the process where the log event occurs. |
| Error level | Error level, which can be Error, Warning, or Note. |
| Content | Records the detailed information about the log, including the description and necessary context information. |

## Example Log

A typical example of the **`hostname`.err** log of the database is as follows:

```
sing the USER and PASSWORD connection options for START
SLAVE; see the 'START SLAVE Syntax' in the MySQL Manual for more information.
2019-05-27 17:11:29 3352 [Warning] Storing MySQL user
name or password information in the master info repository is not secure and is
therefore not recommended. Please consider using the USER and PASSWORD
connection options for START SLAVE; see the 'START SLAVE Syntax' in the MySQL
Manual for more information.
```

```
2019-05-28 07:29:45 3352 [Warning] Aborted connection
13108166 to db: 'unconnected' user: 'mha_mon' host: 'localhost' (Got timeout
reading communication packets)
2019-05-28 17:10:25 3352 [Warning] Storing MySQL user
name or password information in the master info repository is not secure and is
therefore not recommended. Please consider using the USER and PASSWORD
connection options for START SLAVE; see the 'START SLAVE Syntax' in the MySQL
Manual for more information
```

# 1.2.5 ZooKeeper Log

## Log Description

Zookeeper logs record the request processing process of Zookeeper. By viewing the Zookeeper logs, the system administrator or maintenance personnel can check the running status of the Zookeeper adapter. Therefore, if a problem occurs during cluster creation, they can quickly locate the problem.

## Log Level

| Level | Description |
| --- | --- |
| DEBUG | Records the Broker working process, including the log information and related parameters of each operation. |
| INFO | Records the working process and related key operations during the Broker running. |
| WARN | Records the problems or exceptions that may occur during the running of the system. |
| ERROR | Records errors that occur during Broker running. |

## Log Path

The Zookeeper process is deployed on the **MRS_Region_Node** VM. Log in to the MRS_Region_Node node as user **opsadmin** and switch to user **root** to view logs.

The default log file path is **/opt/cloud/logs/zookeeper/zookeeper.log**.

NOTE

In the non-DR deployment scenario of the MRS management plane, the ZooKeeper process is deployed on the **MRS_Region_Node** VM. In the cross-AZ DR deployment scenario of the MRS management plane, the ZooKeeper process is deployed on the **MRS-Zookeeper** and **MRS-Zookeeper-DC** VMs.

## Log Format

[Log generating time] [Thread ID]-[Log level] [Invoked function] Content

## Log Parameter

| Parameter | Description |
| --- | --- |
| Log generation time | Indicates the time when the log service tool records the log. |
| Indicates the thread ID. | Records the ID of the thread in the process where the log event occurs. |
| Log Level | Log level, which can be ERROR(E), WARN(W), INFO(I), or DEBUG(D). |
| Invoked function | Indicates the information about the location where the running file resides, name of the invoked function, and lines of the running code. |
| Content | Records the detailed information about the log, including the description and necessary context information. |

## Example Log

A typical Zookeeper log is as follows:

```
2021-02-25T11:05:02,424 [myid:] - INFO  [CommitProcessor:0:DataTree@767] - type:error, sessionid:0x
cxid:0x2007 zxid:0x100004b1d reqpath:null
2021-02-25T11:05:30,714 [myid:] - INFO  [PurgeTask:DatadirCleanupManager$PurgeTask@138] - Purge
task started.
2021-02-25T11:05:30,714 [myid:] - INFO  [PurgeTask:DatadirCleanupManager$PurgeTask@144] - Purge
task completed.
```

# 1.2.6 Console Log

## Log Description

A Console log is used to record user operations performed on the console page. By viewing the Console log, the system administrator or maintenance personnel can check the processing status of an operation request on the console page.

## Log Level

| Level | Description |
| --- | --- |
| DEBUG | Records the Console working process, including the log information and related parameters of each operation. |
| INFO | Records the working process and related key operations during the Console running. |
| WARN | Records the problems or exceptions that may occur during the running of the system. |

| Level | Description |
| --- | --- |
| ERROR | Records the errors that occur during the console running. Such errors include failures in connecting with the Identity and Access Management (IAM), failures in communicating with the application programming interface (API) gateway, and others. |

## Log Path

The console log path can be configured using Nginx. The format is as follows:

log_format access '$remote_addr - $remote_user [$time_local] "$request" ' '$status $body_bytes_sent "$http_referer" ' ' "$http_user_agent" ' 'upstream_addr $upstream_addr upstream_response_time $upstream_response_time request_time $request_time $gzip_ratio';

The default log path is **/opt/onframework/nginx/logs/access.log**.

NOTE

Log path:

- Log in to Service OM and choose **Services** > **Resource** > **Compute Resource**. Click the **VMs** tab and enter **nginx** in the search box to search for the VM name. Record the IP address of the **NGINX-*xx*** VM.
- Log in to the **NGINX-*xx*** node as user **opsadmin** and switch to user **root** to view specific logs. For details about the default password, see ***Huawei Cloud Stack 8.3.1 Account List*** or contact the system administrator.

## Log Format

[*Log generation time*][*Log level*][*Thread name*][*Invoked function*] *Content*

## Log Parameter

| Parameter | Description |
| --- | --- |
| Log generation time | Indicates the time when the log service tool records the log. |
| Log level | The levels include ERROR, WARN, INFO, and DEBUG. |
| Thread name | Records the ID of the thread in the process where the log event occurs. |
| Invoked function | Indicates the information about the location where the running file resides, name of the invoked function, and lines of the running code. |
| Content | Records the detailed information about the log, including the description and necessary context information. |

### Example Log

A typical Console log sample is as follows:

```
2019-05-08 11:51:02,468 +0800] [WARN ] [WatchDirThread]
[com.huawei.console.passthrough.thread.WatchDirThread:run 131] Begins reloading configuration file.
[2019-05-08 11:51:02,469 +0800] [WARN ] [WatchDirThread]
[com.huawei.console.passthrough.thread.WatchDirThread:run 133] Finished reloading configuration file.
```

## 1.2.7 MRS Service Run Log

### Log Description

Service run logs record requests for external services to access local services. When a permission fault occurs, the system administrator or O&M personnel can view the service run logs to obtain the detailed information about the fault and quickly locate and rectify the fault.

### Log Level

| Level | Description |
| --- | --- |
| ERROR | Records errors that occur during the running of the service. |
| DEBUG | Records the log information and related parameters of each service operation. |
| INFO | Records key steps involved in the service. |
| WARN | Records the problems or exceptions that may occur during the running of the service. |

### Log Path

The default log file path is **/opt/cloud/logs/tomcat/logs/localhost_access_log.txt** of the Console-Stage node.

NOTE

Run the **su - root** command to switch to user **root** and then access the log path. For details about the default password, see ***Huawei Cloud Stack 8.3.1 Account List*** or contact the system administrator.

### Log Format

[Log level] [Log printing time] [IP source] [Access path] [Access time] (Calling method) [Communication protocol] [Response]

### Log Parameter

| Parameter | Description |
| --- | --- |
| Log level | For details, see the log level description. |

| Parameter | Description |
| --- | --- |
| Log printing time | Indicates the time when the log service tool records the log. |
| IP source | Indicates the communication IP address of the visitor. |
| Access Time | Indicates the time when the log service tool records the log. |
| Calling method | Indicates the calling method and path. |
| Communication protocol | Indicates the communication protocol. |
| Response | Indicates the returned communication result. |

### Example Log

A typical example of the **localhost_access_log.txt** file of the service run logs is as follows:

```
[INFO ] 2020-12-26 09:13:17,226 [http-bio-7443-exec-108]  [] - 10.99.32.13 - -
[a377a1a7b99340e5a24df00f8a8ce63d] [26/Dec/2020:09:13:17 +0800] "GET /mrs/rest/api/v1/cluster/
8cce62ac-34fd-4c22-9050-af203787bc07/ssh HTTP/1.1" 200 17 38
[dddae24d2b13441b95e12f3607a0a4e6] - -com.huawei.wcc.secas.Log4JAccessLogValve
```

# 1.3 Tenant-Plane Log Reference

## 1.3.1 Log Collection

### 1.3.1.1 Log Online Search

### Scenario

FusionInsight Manager allows you to search for logs online and view the log content of components to locate faults.

### Procedure

**Step 1** Log in to FusionInsight Manager.

**Step 2** Choose **O&M** > **Log** > **Online Search**.

**Step 3** Configure the parameters listed in **Table 1-3** to search for the logs you need. You can select a default log search duration (including **0.5h**, **1h**, **2h**, **6h**, **12h**, **1d**, **1w**, and **1m**), or click the edit icon to customize **Start Data** and **End Data**.

**Table 1-3** Log search parameters

| Parameter | Description |
| --- | --- |
| Search Content | Keywords or regular expression to be searched for |
| Service | Service or module for which you want to query logs |
| File | Log files to be searched for when only one role is selected |
| Lowest Log Level | Lowest level of logs to be queried. After you select a level, the logs of this level and higher levels are displayed.<br>The levels in ascending order are as follows:<br>TRACE < DEBUG < INFO < WARN < ERROR < FATAL |
| Host Scope | • You can click ... to select hosts.<br>• Enter the host name of the node for which you want to query logs or the IP address of the management plane.<br>• Use commas (,) to separate IP addresses, for example, **192.168.10.10**,**192.168.10.11**.<br>• Use hyphens (-) to indicate an IP address segment if the IP addresses are consecutive, for example, **192.168.10.[10-20]**.<br>• Use hyphens (-) to indicate an IP address segment if the IP addresses are consecutive, and use commas (,) to separate IP address segments, for example, **192.168.10.[10-20,30-40]**.<br>**NOTE**<br>– If this parameter is not specified, all hosts are selected by default.<br>– A maximum of 10 expressions can be entered at a time.<br>– A maximum of 2,000 hosts can be matched for all entered expressions at a time. |
| Advanced Configurations | • **Max Quantity**: maximum number of logs that can be displayed at a time. If the number of queried logs exceeds the value of this parameter, the earliest logs will be ignored. If this parameter is not set, the maximum number of logs that can be displayed at a time is not limited.<br>• **Timeout Duration**: log query timeout duration. This parameter is used to limit the maximum log query time on each node. When the query times out, the query is stopped and the logs that have been searched for are still displayed. |

**Step 4** Click **Search**. Table 1-4 describes the fields in search results.

**Table 1-4** Parameters in search results

| Parameter | Description |
| --- | --- |
| Time | Time when a line of log is generated |
| Host Name | Host name of the node where the log file recording the line of log is located |
| Location | Path of the log file recording the line of log<br>Click the location information to go to the online log browsing page. By default, 100 lines of logs before and 100 lines after the line of log are displayed. You can click **Load More** on the top or bottom of the page to view more logs. Click **Download** to download the log file to the local PC. |
| Line No. | Line number of a line of log in the log file |
| Level | Level of the line of log |
| Log | Log content |

NOTE

You can click **Stop** to forcibly stop the search. You can view the search results in the list.

**Step 5** Click **Filter** to filter the logs to display on the page. **Table 1-5** lists the fields that you can use to filter logs. After you configure these parameters, click **Filter** to search for logs meeting the search criteria. You can click **Reset** to clear the information that you have filled in.

**Table 1-5** Parameters for filtering logs

| Parameter | Description |
| --- | --- |
| Keywords | Keywords of the losg to be searched for |
| Host Name | Name of the host to be searched for |
| Location | Path of the log file to be searched for |
| Started | Start time for logs to be searched for |
| Completed | End time for logs to be searched for |

**----End**

### 1.3.1.2 Downloading Logs from FusionInsight Manager

## Scenario

FusionInsight Manager allows you to batch export logs generated on all instances of each service.

## Procedure

**Step 1** Log in to FusionInsight Manager.

**Step 2** Choose **O&M** > **Log** > **Download**.

**Step 3** Select a log download range:

1. **Service**: Click ... and select a service.
2. **Host**: Enter the IP address of the host where the service is deployed. You can also click ... to select the required host.
3. **Maximum Concurrency**: Set the maximum number of concurrent nodes for log collection as required.
4. Click the edit icon in the upper right corner and configure **Start Time** and **End Time**.

**Step 4** Click **Download**.

The downloaded log package contains the topology information of the start time and end time, helping you quickly find the log you need.

The topology file is named in the format of **topo_<***Topology structure change time***>.txt**. The file contains the node IP address, host name, and service instances that reside on the node. (OMS nodes are identified by **Manager:Manager**.)

Example:

```
192.168.204.124|suse-124|
DBService:DBServer;KrbClient:KerberosClient;LdapClient:SlapdClient;LdapServer:SlapdServer;Manager:Manager;meta:meta
```

**----End**

### 1.3.1.3 Downloading Logs of MRS Cluster Creation Failure from OBS

## Scenarios

If a cluster fails to be created on the MRS management console, administrators can obtain the cluster creation and running logs from OBS for fault locating.

## Procedure

**Step 1** Obtain and install OBS Browser+ by referring to sections "Downloading OBS Browser+" and "Installing OBS Browser+" in *Object Storage Service 3.0 (OBS) 24.3.0h&s Tool Guide (OBS Browser+) (for Huawei Cloud Stack 8.3.1)* in *Object Storage Service 3.0 (OBS) 24.3.0h&s Usage Guide (for Huawei Cloud Stack 8.3.1)*.

**Step 2** In the **Add Account** dialog box, enter the account information based on **Table 1-6** and log in to OBS using the AK.

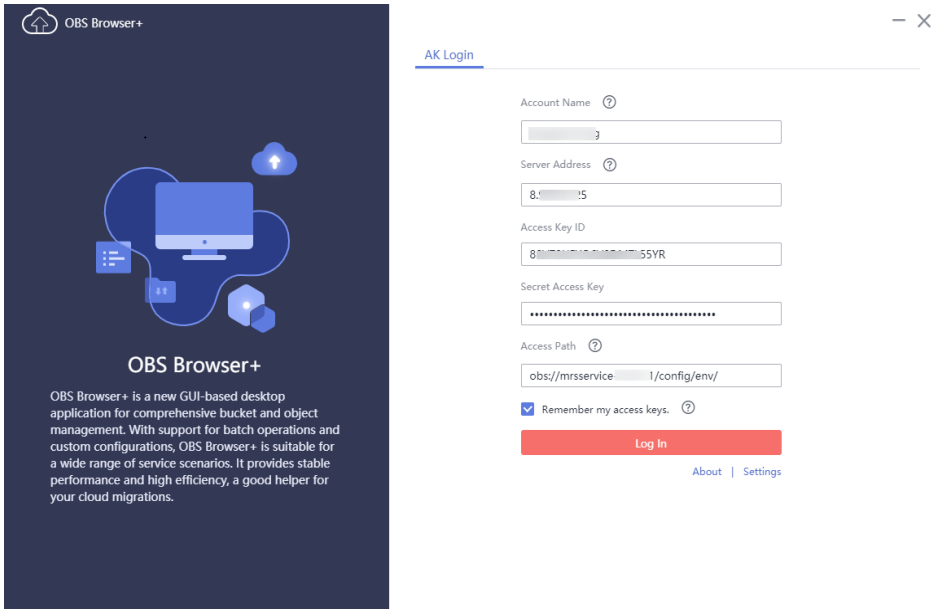


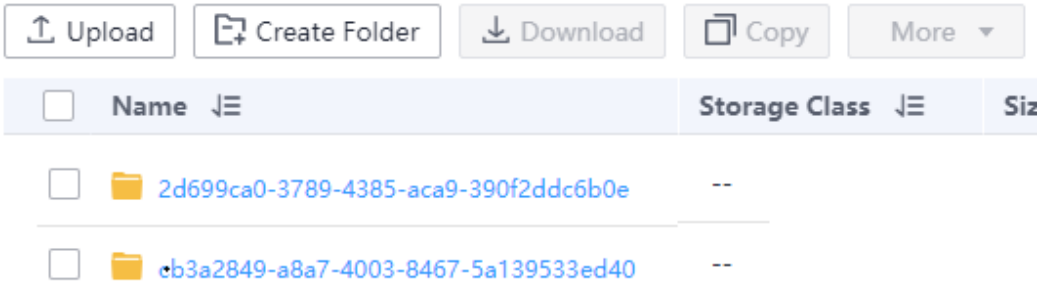

**Table 1-6** Parameters for logging in to OBS

| Parameter | Parameter Description | Example Value | Remarks |
| --- | --- | --- | --- |
| Account Name | Username used for deployment | mrs | Customizable |
| Server Address | OBS server IP address | {obs_address}:443 | *{obs_address}* is the value of **obs_address** on the 1.2 sheet in the LLD file exported from the project in the region domain. |
| Access Key ID | Access key | *xxx* | The AK is globally unique. Contact the system administrator to obtain it. |
| Secret Access Key | Secret Access Key | *xxx* | The SK is globally unique. Contact the system administrator to obtain it. |
| Access Path | Direct access path of the OBS bucket. No redirection is required. | obs://obs-4logcollect-{regionId}/ | *{regionId}* is the value of **region0_id** on the 1.2 sheet in the LLD file exported from the project. |

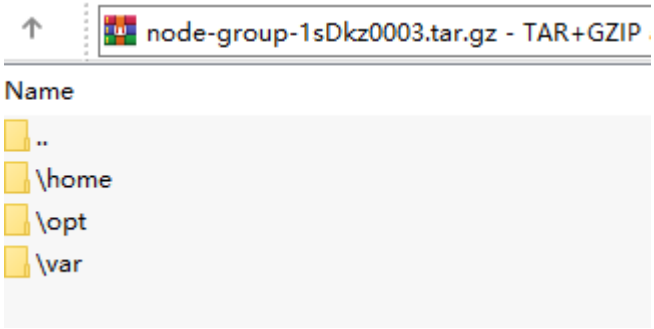
**Step 3** Log in to OBS and go to the file corresponding to the VDC name. Locate the log folder based on the cluster ID of the failed cluster.

You can view the cluster ID in the cluster list on the MRS management console. If a cluster fails to be created, click on the cluster list page and view the ID of the failed cluster in the **Failed Tasks** area.




**Step 4** After confirming the folder based on the date and cluster name, click to download the compressed log file package generated for each node group in the folder to the local PC.

**Step 5** Decompress the package and obtain the log file in the corresponding path for analysis.




**----End**

# 1.3.2 CDL Log Overview

## Log Description

**Log path**: The default log storage path of CDL is **/var/log/Bigdata/cdl/***Role name abbreviation*.

- CDLService: **/var/log/Bigdata/cdl/service** (run logs) and **/var/log/Bigdata/audit/cdl/service** (audit logs).
- CDLConnector: **/var/log/Bigdata/cdl/connector** (run logs).

**Table 1-7** Log list

| Type | File | Description |
| --- | --- | --- |
| Run logs | connect.log | CDLConnector run log. |
| | prestartDetail.log | Log that records cluster initialization before service startup. |
| | startDetail.log | Service startup log. |
| | stopDetail.log | Service stop log. |
| | cleanupDetail.log | Log that records the cleanup execution of services. |
| | check-serviceDetail.log | Log that records the verification of service status after service installation. |
| | cdl-db-operation.log | Log that records database initialization during service startup. |
| | cdl-app-launcher.log | Spark application startup log of CDL data synchronization tasks. |
| | cdl-dc-app-launcher.log | Spark application startup log of CDL data comparison tasks. |
| | serviceInstance-Check.log | Instance check log of CDLService. |
| | connectorInstance-Check.log | Instance check log of CDLConnector. |
| | ModifyDBPasswd.log | Log that records the resetting of the service database password. |
| | modifyDBPwd_yyyy-mm-dd.log | Run log file that records the DBService password change tool. |
| | ranger-cdl-plugin-enable.log | Log that records the enabling or disabling of Ranger authentication. |
| | postinstallDetail.log | Service installation log. |
| | cdl_connector_pidxxx_gc.log.x | CDLConnector garbage collection (GC) log. |
| | cdl_service_pidxxx_gc.log.x | CDLService GC log. |
| | threadDump-CDLConnector-xxx.log | CDLConnector stack log. |
| | threadDump-CDLService-xxx.log | CDLService stack log. |
| Audit log | cdl-audit.log | Service audit log. |

## Log Level

Table 1-8 describes the log levels supported by CDL.

Levels of run logs are FATAL, ERROR, WARN, INFO, and DEBUG from the highest to the lowest priority. Run logs of equal or higher levels are recorded. The higher the specified log level, the fewer the logs recorded.

**Table 1-8** Log levels

| Type | Level | Description |
| --- | --- | --- |
| Run log and audit log | FATAL | Logs of this level record fatal information about system. |
| | ERROR | Logs of this level record error information about system running. |
| | WARN | Logs of this level record exception information about the current event processing. |
| | INFO | Logs of this level record normal running status information about the system and events. |
| | DEBUG | Logs of this level record system running and debugging information. |

To modify log levels, perform the following operations:

**Step 1** Go to the **All Configurations** page of CDL. For details, see **Modifying Cluster Service Configuration Parameters**.

**Step 2** On the menu bar on the left, select the log menu of the target role.

**Step 3** Select a desired log level.

**Step 4** Save the configuration. In the displayed dialog box, click **OK** to make the configurations take effect.

NOTE

The configurations take effect immediately without the need to restart the service.

**----End**

## Log Format

The following table lists the CDL log formats:

**Table 1-9** Log formats

| Type | Format | Example |
| --- | --- | --- |
| Run log | <*yyyy-MM-dd HH:mm:ss,SSS*>\|<*Log level*>\|<*Name of the thread that generates the log*>\|<*Message in the log*>\|<*Location where the log event occurs*> | 2021-06-15 17:25:19,658 \| DEBUG \| qtp2009591182-1754 \| >fill SslConnection@5d04c5a0::SocketChannelEnd-Point@7c011c24{l=/10.244.224.65:21495,r=/10.244.224.83:53724,OPEN,fill=-,flush=-,to=1/30000}{io=0/0,kio=0,kro=1}->SslConnection@5d04c5a0{NOT_HANDSHAKING,eio=-1/-1,di=-1,fill=IDLE,flush=IDLE}~>DecryptedEndPoint@771f2f77{l=/10.244.224.65:21495,r=/10.244.224.83:53724,OPEN,fill=-,flush=-,to=19398/30000}=>HttpConnection@68c5859b[p=HttpParser{s=CONTENT,0 of -1},g=HttpGenerator@536e2de0{s=END}]=>HttpChannelOverHttp@7bf252bd{s=HttpChannelState@38be31e{s=IDLE rs=COMPLETED os=COMPLETED is=IDLE awp=false se=false i=false al=0},r=1,c=true/true,a=IDLE,uri=https://10.244.224.65:21495/api/v1/cdl/monitor/jobs/metrics,age=19382} \| SslConnection.java:614 |

| Type | Format | Example |
| --- | --- | --- |
| Audit log | *<yyyy-MM-dd HH:mm:ss,SSS>|<Log level>|<Name of the thread that generates the log>|<Message in the log>|<Location where the log event occurs>* | 2021-06-15 11:07:00,262 \| INFO \| qtp1846345504-30 \| STARTTIME=2021-06-15 11:06:47.912 ENDTIME=2021-06-15 11:07:00.261 USERIP=10.144.116.198 USER=CDL User INSTANCE=10-244-224-65 OPERATION=Start CDL Job TARGET=CDCJobExecutionResource RESULT=SUCCESS \| CDCAuditLogger.java:93 |

## 1.3.3 ClickHouse Log Overview

### Log Description

**Log path**: ClickHouse logs are stored in **${BIGDATA_LOG_HOME}/clickhouse** by default.

- ClickHouse run logs: **/var/log/Bigdata/clickhouse/clickhouseServer/ *.log**
- Balancer run logs: **/var/log/Bigdata/clickhouse/balance/*.log**
- Data migration logs: **/var/log/Bigdata/clickhouse/migration/${task_name}/clickhouse-copier_{timestamp}_{processId}/copier.log**
- ClickHouse audit logs: **/var/log/Bigdata/audit/clickhouse/clickhouse-server-audit.log**

**Log archiving rules**:

- The automatic compression and archiving function has been enabled for ClickHouse logs. By default, when the size of log files exceeds 100 MB adjustable by referring to **Configuring the Level and File Size of Tenant Plane Logs**, the log files will be automatically compressed.
- The file generated after log files are compressed is named in the format of **<***Original log name***>.[***ID***].gz**.
- A maximum of 10 latest compressed files are reserved by default. The number of compressed files can be configured on Manager.

**Table 1-10** ClickHouse log list

| Log Type | Log File Name | Description |
| --- | --- | --- |
| ClickHouse log | /var/log/Bigdata/clickhouse/clickhouseServer/clickhouse-server.err.log | Path of ClickHouseServer error log files |
| | /var/log/Bigdata/clickhouse/clickhouseServer/checkService.log | Path of key ClickHouseServer run log files |
| | /var/log/Bigdata/clickhouse/clickhouseServer/clickhouse-server.log | |
| | /var/log/Bigdata/clickhouse/clickhouseServer/ugsync.log | User role synchronization tool log |
| | /var/log/Bigdata/clickhouse/clickhouseServer/prestart.log | ClickHouse prestart log |
| | /var/log/Bigdata/clickhouse/clickhouseServer/start.log | ClickHouse startup log |
| | /var/log/Bigdata/clickhouse/clickhouseServer/checkServiceHealthCheck.log | ClickHouse health check log |
| | /var/log/Bigdata/clickhouse/clickhouseServer/checkugsync.log | User role synchronization check log |
| | /var/log/Bigdata/clickhouse/clickhouseServer/checkDisk.log | Path of ClickHouse disk check log files |
| | /var/log/Bigdata/clickhouse/clickhouseServer/backup.log | Path of log files generated when ClickHouse performs the backup and restoration operations on Manager |
| | /var/log/Bigdata/clickhouse/clickhouseServer/stop.log | ClickHouse stop log |
| | /var/log/Bigdata/clickhouse/clickhouseServer/postinstall.log | postinstall.sh script invoking log of ClickHouse |
| | /var/log/Bigdata/clickhouse/clickhouseServer/move_factor_check.log | Check log about whether the remaining space of the ClickHouse local disk is less than the threshold configured in the cold and hot data separation policy |
| | /var/log/Bigdata/clickhouse/clickhouseServer/obs_access_check.log | Log file that records whether the ClickHouse can properly access the OBS |
| | /var/log/Bigdata/clickhouse/clickhouseServer/obs_aksk_check.log | Check log of whether the ClickHouse successfully obtains the temporary delegation credential |

| Log Type | Log File Name | Description |
| --- | --- | --- |
| | /var/log/Bigdata/clickhouse/balance/start.log | Path of ClickHouseBalancer startup log files |
| | /var/log/Bigdata/clickhouse/balance/error.log | Path of ClickHouseBalancer error log files |
| | /var/log/Bigdata/clickhouse/balance/access_http.log | Path of the HTTP log files generated during ClickHouseBalancer running |
| | /var/log/Bigdata/clickhouse/balance/access_tcp.log | Path of the TCP log files generated during ClickHouseBalancer running |
| | /var/log/Bigdata/clickhouse/balance/checkService.log | ClickHouseBalancer service check log |
| | /var/log/Bigdata/clickhouse/balance/postinstall.log | Invoking log of the **postinstall.sh** script of ClickHouseBalancer |
| | /var/log/Bigdata/clickhouse/balance/prestart.log | Path of prestart log files of ClickHouseBalancer |
| | /var/log/Bigdata/clickhouse/balance/stop.log | Path of stop log files of ClickHouseBalancer |
| | /var/log/Bigdata/clickhouse/clickhouseServer/auth.log | ClickHouse service authentication log |
| | /var/log/Bigdata/clickhouse/clickhouseServer/cleanService.log | Log generated when an instance fails to reinstall |
| | /var/log/Bigdata/clickhouse/clickhouseServer/offline_shard_table_manager.log | ClickHouse recommissioning/ decommissioning log |
| | /var/log/Bigdata/clickhouse/clickhouseServer/traffic_control.log | ClickHouse active/standby DR traffic control log |
| | /var/log/Bigdata/clickhouse/clickhouseServer/clickhouse_migrate_metadata.log | ClickHouse metadata migration log |
| | /var/log/Bigdata/clickhouse/clickhouseServer/clickhouse_migrate_data.log | ClickHouse service data migration log |
| | /var/log/Bigdata/clickhouse/clickhouseServer/changePassword.log | ClickHouse user password change log |
| | /var/log/coredump/clickhouse-*.core.gz | Compressed package of memory dump files generated after the ClickHouse process breaks down |

| Log Type | Log File Name | Description |
| --- | --- | --- |
| Data migration log | /var/log/Bigdata/clickhouse/migration/*Data migration task name*/clickhouse-copier_*{timestamp}_{processId}*/copier.log | Run log generated when you use the migration tool by referring to "Using the ClickHouse Data Migration Tool" |
| | /var/log/Bigdata/clickhouse/migration/*Data migration task name*/clickhouse-copier_*{timestamp}_{processId}*/copier.err.log | Error log generated when you use the migration tool by referring to "Using the ClickHouse Data Migration Tool" |
| | /var/log/Bigdata/tomcat/clickhouse/auto_balance/*Data migration task name*/balance_manager.log | Run log generated when one-click balancing is selected by referring to "Using the ClickHouse Data Migration Tool" |
| clickhouse-tomcat log | /var/log/Bigdata/tomcat/clickhouse/web_clickhouse.log | ClickHouse custom UI run log |
| | /var/log/Bigdata/tomcat/audit/clickhouse/clickhouse_web_audit.log | Clickhouse data migration audit log |
| ClickHouse audit log | /var/log/Bigdata/audit/clickhouse/clickhouse-server-audit.log | Path of ClickHouse audit log files |

## Log Level

**Table 1-11** describes the log levels supported by ClickHouse.

Levels of run logs are fatal, error, warning, trace, information, and debug from the highest to the lowest priority. Run logs of equal or higher levels are recorded. The higher the specified log level, the fewer the logs recorded.

**Table 1-11** Log levels

| Level | Description |
| --- | --- |
| fatal | Logs of this level record information about critical errors that will cause applications to exit |
| error | Logs of this level record error information about system running |
| warning | Logs of this level record exception information about the current event processing |
| trace | Logs of this level record trace information about the current event processing |

| Level | Description |
| --- | --- |
| information | Logs of this level record normal running status information about the system and events |
| debug | Logs of this level record system running and debugging information |

To modify log levels, perform the following operations:

**Step 1** Log in to FusionInsight Manager.

**Step 2** Choose **Cluster** > **Services** > **ClickHouse** > **Configurations**.

**Step 3** Select **All Configurations**.

**Step 4** On the menu bar on the left, select the log menu of the target role.

**Step 5** Select a desired log level.

**Step 6** Click **Save**. Then, click **OK**.

**----End**

NOTE

The configurations take effect immediately without the need to restart the service.

## Log Format

The following table lists the ClickHouse log format:

**Table 1-12** Log formats

| Log Type | Format | Example |
| --- | --- | --- |
| ClickHouse run log | <*yyyy-MM-dd HH:mm:ss,SSS*>\|<*Log level*>\|<*Name of the thread that generates the log*>\|<*Message in the log*>\|<*Location where the log event occurs*> | 2021.02.23 15:26:30.691301 [ 6085 ] {} <Error> DynamicQueryHandler: Code: 516, e.displayText() = DB::Exception: default: Authentication failed: password is incorrect or there is no user with such name, Stack trace (when copying this message, always include the lines below):<br>0. Poco::Exception::Exception(std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > const&, int) @ 0x1250e59c |

| Log Type | Format | Example |
| --- | --- | --- |
| clickhouse-tomcat run log | <*yyyy-MM-dd HH:mm:ss,SSS*>\|<*Log level*>\|<*Name of the thread that generates the log*>\|<*Message in the log*>\|<*Location where the log event occurs*> | 2022-08-16 12:55:12,109 \| INFO \| pool-7-thread-1 \| zookeeper is secure. \| com.huawei.bigdata.om.extui.clickhouse.service.impl.QueryServiceImpl.initAuthContext(QueryServiceImpl.java:136) |
| Data migration log | <*yyyy-MM-dd HH:mm:ss,SSS*>\|<*Log level*>\|<*Name of the thread that generates the log*>\|<*Message in the log*>\|<*Location where the log event occurs*> | 2022.08.07 14:41:01.814235 [ 28651 ] {} <Debug> ClusterCopier: Task /clickhouse/copier_tasks/TEST0807_02/tables/dblv85.startsea_zh_imoriginck_new/20201031/piece_4/shards/1 has been successfully executed by 8%2D5%2D226%2D156#20220807124849_28651 |
| Audit log | <*yyyy-MM-dd HH:mm:ss,SSS*>\|*query id*\|<*Log Level*><*Name of the thread that generates the log*>\|<*Message in the log*>\|<*Location where the log event occurs*> | 2022.08.16 20:58:16.723643 [ 11382 ] {cc9554b6-8a26-42e9-8ab8-d848500544e6} <Information> executeQuery_audit [executeQuery.cpp:202] : (0 from 192.168.64.81:45204, user: clickhouse, using experimental parser) select shard_num, host_name, host_address from system.clusters format JSON |

# 1.3.4 Introduction to Containers Logs

## Log Description

**Log path**:

- Run log: **/var/log/Bigdata/containers/container/Container**_*Instance ID*/
- Audit log: **/var/log/Bigdata/audit/containers/container/Container**_*Instance ID*/
- Containers-tomcat log: **/var/log/Bigdata/tomcat/container/**
- Container instance installation and uninstallation log: **/var/log/Bigdata/containers/**

**Log archive rule**: The automatic compression and archive function is enabled for Containers logs. By default, when the total size of all log files exceeds 5 MB (configurable), the log files are automatically compressed into a package named in the format of *Original log file name*-*yyyy-mm-dd_hh-mm-ss*.*No.*.**log.zip**. The number of compressed files to be retained and the compression threshold are configurable.

**Table 1-13** WebContainer log list

| Log Type | Log File | Description |
| --- | --- | --- |
| Run log | blus | Directory for storing BLU run log files |
| | cleanupDetail.log | BLU clearance log file |
| | container-catalina-omm-*hostname*.log | Tomcat run logs |
| | container-catalina-omm-*hostname*.out | Output of the Tomcat console, which is equivalent to the **Catalina.out** log (this log is not compressed in rolling mode). |
| | container-common-omm-*hostname*.log | Containers health monitoring log files |
| | container-gc-omm-*hostname*.log.*ID*.current | GC log of the Tomcat process |
| | container-manager-omm-hostname.log | Management log of the Tomcat process |
| | container-servlet-omm-*hostname*.log | Containers run logs |
| | postinstallDetail.log | Containers installation log |
| | startDetail.log | Containers startup log |
| | stopDetail.log | Containers stop log |
| | container-stack-omm-*hostname*.*time*.log | Stack information before Containers is stopped |
| Containers instance installation and uninstallation log | containers_install.log | Containers instance installation and uninstallation log |
| Containers-tomcat log | sgpaudit.log | Audit log of Sqp management operations in Containers |
| | web_container_audit.log | Audit log of Containers operations |
| | web_container.log | Containers monitoring run log |
| | web_sgp_control.log | Log of the Sgp module in Containers |
| | web_sgp.log | Core run log of the Sgp module in Containers |

| Log Type | Log File | Description |
| --- | --- | --- |
| | backup.log | Containers backup and restoration log |
| | /script/container_script.log | Log about **tool.sh** during BLU deployment in Containers |
| Audit log | container-audit-omm-*hostname*.log | Containers audit log |

## Log Levels

**Table 1-14** describes the log levels provided by Containers.

The log levels are ERROR, WARN, INFO, and DEBUG in descending order of priority. Only logs whose levels are higher than or equal to the specified level are recorded. The higher the log level specified, the fewer the logs are recorded.

**Table 1-14** Log levels

| Level | Description |
| --- | --- |
| ERROR | Logs of this level record error information about system running |
| WARN | Logs of this level record exception information about the current event processing |
| INFO | Logs of this level record normal running status information about the system and events |
| DEBUG | Logs of this level record the system information and system debugging information |

To modify log levels, perform the following operations:

1. Log in to FusionInsight Manager.
2. Choose **Cluster** > **Services** > **Containers**. Click **Configurations** then **All Configurations**.
3. On the menu bar on the left, select the log menu of the target role.
4. Select a desired log level.
5. Click **Save**. In the displayed dialog box, click **OK** to make the configuration take effect.

## Log Formats

The following table lists the Containers log formats:

**Table 1-15** Log formats

| Log type | Format | Example Value |
| --- | --- | --- |
| Run log | <*yyyy-MM-dd HH:mm:ss,SSS*>\|<*Log level*>\|<*Name of the thread that generates the log*>\|<*Message in the log*>\|<*Location where the log event occurs*> | 15/03/16 09:24:48 DEBUG [container-deploy-checker] [task-checker] task: [taskName=com.huawei.dap.container.servlets.operation.deploy.task.DeployTask@2e0bc2ef] [submitTime=1426469087953] [overTime=60000] [taskPriority=LOWEST_PRIORITY] [taskSeqno=10238] done com.huawei.dap.container.servlets.operation.deploy.task.TaskChecker.run(TaskChecker.java:42) |

# 1.3.5 DBService Log Overview

## Log Description

**Log path**: The default storage path of DBService log files is **/var/log/Bigdata/dbservice**.

- GaussDB: **/var/log/Bigdata/dbservice/DB** (GaussDB run log directory), **/var/log/Bigdata/dbservice/scriptlog/gaussdbinstall.log** (GaussDB installation log), and **/var/log/gaussdbuninstall.log** (GaussDB uninstallation log).
- HA: **/var/log/Bigdata/dbservice/ha/runlog** (HA run log directory) and **/var/log/Bigdata/dbservice/ha/scriptlog** (HA script log directory)
- DBServer: **/var/log/Bigdata/dbservice/healthCheck** (Directory of service and process health check logs)

  **/var/log/Bigdata/dbservice/scriptlog** (run log directory), **/var/log/Bigdata/audit/dbservice/** (audit log directory)

Log archive rule: The automatic DBService log compression function is enabled. By default, when the size of logs exceeds 1 MB, logs are automatically compressed into a log file named in the following format: *<Original log file name>-[No.]*.**gz**. A maximum of 20 latest compressed files are reserved.

NOTE

Log archive rules cannot be modified.

**Table 1-16** DBService log list

| Type | Log File Name | Description |
| --- | --- | --- |
| DBServer run log | dbservice_serviceCheck.log | Run log file of the service check script |
| | dbservice_processCheck.log | Run log file of the process check script |

| Type | Log File Name | Description |
| --- | --- | --- |
| | backup.log | Run logs of backup and restoration operations (The DBService backup and restoration operations need to be performed.) |
| | checkHaStatus.log | Log file of HA check records |
| | cleanupDBService.log | Uninstallation log file (You need to uninstall DBService logs.) |
| | componentUserManager.log | Log file that records the adding and deleting operations on the database by users<br>(Services that depend on DBService need to be added.) |
| | install.log | Installation log file |
| | preStartDBService.log | Pre-startup log file |
| | start_dbserver.log | DBServer startup operation log file (DBService needs to be started.) |
| | stop_dbserver.log | DBServer stop operation log file (DBService needs to be stopped.) |
| | status_dbserver.log | Log file of the DBServer status check (You need to execute the **$DBSERVICE_HOME/sbin/status-dbserver.sh** script.) |
| | modifyPassword.log | Run log file that records the DBService password change script |
| | modifyDBPwd_yyyy-mm-dd.log | Run log file that records the DBService password change tool |

| Type | Log File Name | Description |
| --- | --- | --- |
| | dbserver_switchover.log | Log for DBServer to execute the active/standby switchover script (the active/standby switchover needs to be performed) |
| GaussDB run log | gaussdb.log | Log file that records database running information |
| | gs_ctl-current.log | Log file that records operations performed by using the **gs_ctl** tool |
| | gs_guc-current.log | Log file that records operations, mainly parameter modification performed by using the **gs_guc** tool |
| | gaussdbinstall.log | GaussDB installation log file |
| | gaussdbuninstall.log | GaussDB uninstallation log file |
| HA script run log | floatip_ha.log | Log file that records the script of floating IP addresses |
| | gaussDB_ha.log | Log file that records the script of GaussDB resources |
| | ha_monitor.log | Log file that records the HA process monitoring information |
| | send_alarm.log | Alarm sending log file |
| | ha.log | HA run log file |
| DBService audit log | dbservice_audit.log | Audit log file that records DBService operations, such as backup and restoration operations |

## Log Format

The following table lists the DBService log formats.

**Table 1-17** Log format

| Type | Format | Example |
| --- | --- | --- |
| Run log | [<*yyyy-MM-dd HH:mm:ss*>] <*Log level*>: [< *Name of the script that generates the log*: *Line number* >]: < *Message in the log*> | [2020-12-19 15:56:42] INFO [postinstall.sh:653] Is cloud flag is false. (main) |
| Audit log | [<*yyyy-MM-dd HH:mm:ss,SSS*>] UserName:<*Username*> UserIP:<*User IP address*> Operation:<*Operation content*> Result:<*Operation results*> Detail:<*Detailed information*> | [2020-05-26 22:00:23] UserName:omm UserIP:192.168.10.21 Operation:DBService data backup Result: SUCCESS Detail: DBService data backup is successful. |

# 1.3.6 Doris Logs

## Description

**Log path**: Doris logs are stored in **/var/log/Bigdata/doris/***role name* by default.Doris1 logs are stored in **/var/log/Bigdata/doris1/***role name* by default, and others follow the same rule.

- FE: **/var/log/Bigdata/doris/fe** (run logs) and **/var/log/Bigdata/audit/doris/fe** (audit logs)
- BE: **/var/log/Bigdata/doris/be** (run logs)
- DBroker: **/var/log/Bigdata/doris/dbroker** (run logs)
- DBalancer: **/var/log/Bigdata/doris/dbalancer** (run logs)

**Log archive rule**: The automatic compression and archive function is enabled for Doris logs. By default, when a log file exceeds a specified size (which is configurable), the log file is automatically compressed. The naming rule of the compressed log file is as follows: *<Original log file name>-<yyyy-mm-dd_hh-mm-ss>.[ID]*.**log.zip**. A maximum of 20 latest compressed files are retained by default. The number of compressed files and compression threshold can be changed.

**Table 1-18** Doris logs

| Log Type | Log File | Description |
| --- | --- | --- |
| Run log | /fe/fe.out | Standard/Error logs (stdout and stderr) |
| | /fe/fe.log | Main log, including all contents except **fe.out** |

| Log Type | Log File | Description |
| --- | --- | --- |
| | /fe/fe.warn.log | Subset of **fe.log**. Only WARN and ERROR logs are recorded. |
| | /fe/fe-omm-*<Date>*-*<PID>*-gc.log.*<No.>* | GC logs of the FE process |
| | /fe/preStart.log | Work logs before the FE starts |
| | /fe/check_fe_status.log.log | Log file that records whether the FE service is started successfully |
| | /fe/cleanup.log | Cleanup log for FE uninstallation |
| | /fe/start_fe.log | FE process startup log |
| | /fe/stop_fe.log | FE process stop log |
| | /fe/postinstallDetail.log | Work logs generated after the FE is installed and before it starts |
| | /be/be.INFO | Run log of the BE process |
| | be.WARNING | Subset of **be.log**. Only WARN and FATAL logs are recorded. |
| | /be/be-omm-*<Date>*-*<PID>*-gc.log.*<No.>* | GC logs of the BE process |
| | /be/postinstallDetail.log | Work logs generated after BE is installed and before it starts |
| | /be/preStart.log | Work logs before BE starts |
| | /be/cleanup.log | Cleanup log for BE uninstallation |
| | /be/start_be.log | BE process startup log |
| | /be/stop_be.log | BE process stop log |
| | /be/check_be_status.log | Log file that records whether the BE service is started successfully |
| | /be/be.out | Standard/Error output logs of the BE process (stdout and stderr) |
| | /dbroker/start_broker.log | Log file that records the normal start and stop of the DBroker process |
| | /dbroker/stop_broker.log | log file that records start and stop exceptions of the DBroker process |
| | /dbroker/preStart.log | Work log before DBroker starts |
| | /dbroker/cleanup.log | Cleanup log generated during or before DBroker uninstallation |

| Log Type | Log File | Description |
| --- | --- | --- |
| | /dbroker/check_db_status.log | Log file that records whether the DBroker service is started successfully |
| | /dbroker/dbroker-omm-*<Date>*-*<PID>*-gc.log.*<No.>* | GC log of the DBroker process |
| | /dbroker/apache_hdfs_broker.log | Run log of the DBroker process |
| | /dbalancer/access_http.log | Log generated when the DBalancer accesses the FE web UI |
| | /dbalancer/access_tcp.log | Log about the connections to the database through the DBalancer, that is, logs about the connections to the FE |
| | /dbalancer/checkService.log | DBalancer health check log |
| | /dbalancer/error.log | DBalancer error and warning log |
| | /dbalancer/preStart.log | Work log before DBalancer starts |
| | /dbalancer/start.log | DBalancer process startup log |
| | /dbalancer/stop.log | DBalancer process stop log |
| Audit log | fe.audit.log | Audit log, which records all SQL requests received by the FE |

## Log Levels

**Table 1-19** describes the log levels supported by Doris.

The priorities of run log levels are FATAL, ERROR, WARN, and INFO in descending order. Logs whose levels are higher than or equal to a specified level are displayed. The number of displayed logs decreases as the specified log level increases.

**Table 1-19** Log levels

| Level | Description |
| --- | --- |
| FATAL | Logs of this level record program assertion errors |
| ERROR | Logs of this level record error information about system running |
| WARN | Logs of this level record exception information about the current event processing |
| INFO | Logs of this level record normal running status information about the system and events |

To change log levels, perform the following operations:

**Step 1** Log in to FusionInsight Manager and choose **Cluster** > **Services** > **Doris** > **Configurations** > **All Configurations**. The **All Configurations** page of the Doris service is displayed.

**Step 2** On the menu bar on the left, select the log menu of the target role.

**Step 3** Select a desired log level and save the configuration.

**Step 4** Click **Dashboard**, click **More**, and select **Restart Service**. Enter the user password to restart the Doris service.

**----End**

## Log Formats

The following table describes Doris log formats and gives you some examples:

**Table 1-20** Log format

| Log Type | Format | Example |
| --- | --- | --- |
| FE run log | <yyyy-MM-dd HH:mm:ss,SSS><*LogLevel*>(*Thread name*\|*Thread ID*)<*Location where the log event occurs*>\|<*Messages in the log*> | 2023-04-13 11:17:14,371 INFO (tablet stat mgr\|34) [TabletStatMgr.runAfterCatalogReady():125] finished to update index row num of all databases. cost: 0 ms |
| BE run log | <Log level. I for INFO, W for WARN, F for FATAL\|MMdd HH:mm:ss.SSS> <*Thread ID*> <*Location where a log event occurs*> <Messages in the log> | I0413 11:26:03.439189 25248 tablet_manager.cpp:895] begin to build all report tablets info |
| DBroker run log | <MMdd HH:mm:ss.SSS> <*Thread ID*> <*Log Level*><*Messages in the log*> | 2023-04-11 11:43:13 [ main:0 ] - [ INFO ] starting apache hdfs broker.... |

| Log Type | Format | Example |
| --- | --- | --- |
| Audit log | <yyyy-MM-dd HH:mm:ss,SSS[*Operation type*] >\|<Client>\|<User Name>\|<Db Name>\|<State>\|<ErrorCode>\|<ErrorMessage>\|<Time>\|<ScanBytes>\|<ScanRows>\|<ReturnRows>\|<StmtId>\|<QueryId>\|<IsQuery>\|<feIp>\|<br>\<Stmt>\|<CpuTimeMS>\|<SqlHash>\|<peakMemoryBytes>\|<SqlDigest>\|<TraceId>\|<FuzzyVariables> | 2023-04-13 10:49:26,410 [query] \| Client=192.168.64.223:44382\| User=root\|Db=hivedoris\| State=ERR\|ErrorCode=1105\| ErrorMessage=errCode = 2, detailMessage = (192.168.64.78) [INTERNAL_ERROR]failed to init reader for file /user/hive/warehouse/hivedoris.db/test/000000_0, err: [INTERNAL_ERROR]connect to hdfs failed. error: (255), Unknown error 255), reason: NullPointerException: \| Time=67\|ScanBytes=0\| ScanRows=0\|ReturnRows=0\| StmtId=91\| QueryId=e1125283f12c4994-a69e3a323044d681\| IsQuery=true\| feIp=192.168.64.78\| Stmt=select * from test\| CpuTimeMS=0\| SqlHash=3bbc220823c3e757002fb9490196cf84\| peakMemoryBytes=0\| SqlDigest=\|TraceId=\| FuzzyVariables= |

# 1.3.7 Elasticsearch Log Overview

## Log Description

**Default log paths:**

- Run logs: **/var/log/Bigdata/elasticsearch/${Rolename}**
- Audit logs: **/var/log/Bigdata/audit/elasticsearch/${Rolename}**
- Access logs: **/var/log/Bigdata/elasticsearch/${Rolename}**

**Log archive rules:**

- By default, audit logs are stored once every 50 MB. The size of compressed access logs cannot exceed 2 GB.
- By default, run logs are backed up each time when the size of them reaches 50 MB. Run logs are archived every day. The size of compressed run logs cannot exceed 512 MB.

- The parameters for archiving audit logs and run logs can be configured on Manager.
- By default, access logs are stored once every 50 MB. The size of compressed access logs cannot exceed 512 MB.

**Table 1-21** Elasticsearch log list

| Log Type | Log File Name | Description |
| --- | --- | --- |
| Run log | elasticsearch_cluster_deprecation.log | Elasticsearch discard logs |
| | elasticsearch_cluster_index_indexing_slowlog.log | Elasticsearch index slow logs |
| | elasticsearch_cluster_index_search_slowlog.log | Elasticsearch query slow logs |
| | elasticsearch_cluster.log | Elasticsearch cluster logs |
| | es-process-check.log | Elasticsearch health check logs |
| | es-service-check.log | Elasticsearch service check logs |
| | startup.log | Elasticsearch startup logs |
| | shutdown.log | Elasticsearch stop logs |
| | postinstall.log | Elasticsearch installation logs |
| | prestart.log | Elasticsearch startup preparation logs |
| | es-gc.log* | Elasticsearch instance recycling logs |
| | luvector.log | Elasticsearch vector retrieval logs |
| | <Rolename>-threadDump-<date>.log | Elasticsearch instance jstack logs |
| | es-monitor-info.log | Task list, node list, and thread pool logs of the Elasticsearch service. This log is generated only in the active EsMaster instance. |
| Audit log | elasticsearch_cluster-audit.log | Logs for recording index-level operations, such as migrating shards and deleting indexes. |

| Log Type | Log File Name | Description |
| --- | --- | --- |
| Access log | elasticsearch_cluster-access.log | Logs of the access to Elasticsearch REST APIs |

NOTE

The **curl** command uses the preemption authentication mechanism. Specifically, the system sends a basic authentication request without the TGT, and the authentication fails. Then, the system sends an authentication request with the TGT, and the authentication succeeds. Therefore, after the **curl** command is executed, the audit log of Elasticsearch records a failure log and then a success log.

## Log Level

Table 1-22 describes the log levels provided by Elasticsearch. The priorities of log levels are OFF, ERROR, WARN, INFO, DEBUG , and TRACE in descending order. Logs whose levels are higher than or equal to the specified level are printed. The number of printed logs decreases as the specified log level increases.

**Table 1-22** Log levels

| Level | Description |
| --- | --- |
| OFF | Indicates that the log output is disabled. |
| ERROR | Error information about the current event processing |
| WARN | Exception information about the current event processing |
| INFO | Normal running status information about the system and events |
| DEBUG | System information and system debugging information |
| TRACE | Information whose granularity is lower than that of DEBUG |

## Modifying Log Parameters

To modify log archive and log level parameters, perform the following operations:

**Step 1** Log in to Manager.

**Step 2** Choose **Cluster** > *Name of the desired cluster* > **Services** > **Elasticsearch** > **Configurations**.

**Step 3** Select **All Configurations**.

**Step 4** On the menu bar on the left, select the log menu of the target role.

**Step 5** Select the log archive and log level parameter to be modified.

**Step 6** Click **Save**. In the displayed dialog box, click **OK** to make the configurations take effect.

NOTE

The configurations take effect immediately without the need to restart the service.

**----End**

## Log Format

**Table 1-23** Log format

| Type | Format | Example Value |
| --- | --- | --- |
| Run log | <yyyy-MM-dd HH:mm:ss,SSS>\|<Log level>\|<*Name of the thread that generates the log*>\|<*Name of the class*>\|<*Message in the log*>\| | [2019-05-17T19:05:43,085][DEBUG][elasticsearch[EsNode1@192.168.67.60][http_server_worker][T#3]][o.e.a.a.i.a.g.TransportGetAliasesAction] [EsNode1@192.168.67.60] no known master node, scheduling a retry |
| Audit log | <yyyy-MM-dd HH:mm:ss,SSS>\|<Log level>\|<*Name of the thread that generates the log*>\|<*Name of the class*>\|<*Message in the log*>\| | [2019-05-17T11:28:11,524][WARN ][elasticsearch[EsNode1@192.168.67.60][http_server_worker][T#4]][c.h.e.s.a.AuditLogAppender] [EsNode1@192.168.67.60] RemoteAddr=192.168.67.78:47899 UserName=chengyang RequestURL=PUT /_bulk?pretty=true httpStatus=200 result={"index":{"_index":"ngram5","_type":"ngram5","_id":"Mf_Vw2oB66jHx6hPNj_r","status":403,"error":{"type":"cluster_block_exception","reason":"blocked by: [FORBIDDEN/12/index read-only / allow delete (api)];"}}} |
| Access log | <yyyy-MM-dd HH:mm:ss,SSS>\|<Log level>\|<*Name of the thread that generates the log*>\|<*Name of the class*>\|<*Message in the log*>\| | [2020-09-25T16:38:13,570][INFO ][elasticsearch[EsNode1@192.168.67.78][http_server_worker][T#5]][c.h.e.s.a.AccessLog ] [EsNode1@10.162.146.102] {2020-09-25 16:38:13, Sec-Mod, 'GET /_node/monitor/health', ip=/192.168.67.78:45346} |

# 1.3.8 Flink Log Overview

## Log Description

**Log path:**

- Run logs of a Flink job: **${BIGDATA_DATA_HOME}/hadoop/data${i}/nm/containerlogs/application_${appid}/container_{$contid}**

  NOTE

  The logs of executing tasks are stored in the preceding path. After the execution is complete, the Yarn configuration determines whether these logs are gathered to the HDFS directory.

- FlinkResource run logs: **/var/log/Bigdata/flink/flinkResource**
- FlinkServer run logs: **/var/log/Bigdata/flink**
- FlinkServer audit logs: **/var/log/Bigdata/audit/flink/flinkserver**
- Run logs related to FlinkServer HA scripts: **/var/log/Bigdata/audit/flink/flinkserver/ha**

**Log archive rules:**

1. FlinkResource run logs:
   - By default, service logs are backed up each time when the log size reaches 20 MB. A maximum of 20 logs can be reserved without being compressed.
   - You can set the log size and number of compressed logs on the Manager page or modify the corresponding configuration items in **log4j-cli.properties**, **log4j.properties**, and **log4j-session.properties** in *Client installation directory*/**Flink/flink/conf/** on the client.

   **Table 1-24** FlinkResource log list

| Type | Name | Description |
| --- | --- | --- |
| FlinkResource run logs | checkService.log | Health check log |
| | kinit.log | Initialization log |
| | postinstall.log | Service installation log |
| | prestart.log | Prestart script log |
| | start.log | Startup log |

2. FlinkServer service logs, HA-related logs, and audit logs.
   - By default, FlinkServer service logs, HA-related logs, and audit logs are backed up each time when the log size reaches 100 MB. The service logs are stored for a maximum of 30 days, and audit logs are stored for a maximum of 90 days.
   - You can set the log size and number of compressed logs on the Manager page or modify the corresponding configuration items in **log4j-cli.properties**, **log4j.properties**, and **log4j-session.properties** in *Client installation directory*/**Flink/flink/conf/** on the client.

**Table 1-25** FlinkServer log list

| Type | Name | Description |
| --- | --- | --- |
| FlinkServer run logs | checkService.log | Health check log |
| | checkFlinkServer.log | Health check log of FlinkServer |
| | localhost_access_log..*yyyy-mm-dd*.txt | URL log of FlinkServer |
| | start_thrift_server.out | Thrift server startup log |
| | thrift_server_thriftServer_*xxx*.log.last | |
| | cleanup.log | Cleanup log file for instance installation and uninstallation |
| | flink-omm-client-*IP*.log | Job startup log |
| | flinkserver_*yyyymmdd-x*.log.gz | Service archive log |
| | flinkserver.log | Service log |
| | flinkserver---*pidxxxx*-gc.log.*x*.current | GC log |
| | kinit.log | Initialization log |
| | postinstall.log | Service installation log |
| | prestart.log | Prestart script log |
| | start.log | Startup log |
| | stop.log | Stop log |
| | catalina.*yyyy-mm-dd*.log | Tomcat run log |
| | catalina.out | |
| | host-manager.*yyyy-mm-dd*.log | |
| | localhost.*yyyy-mm-dd*.log | |
| | manager.*yyyy-mm-dd*.log | |
| Run log file related to FlinkServer HA scripts | ha.log | HA run log |
| | ha_monitor.log | HA process monitoring log |
| | floatip_ha.log | Floating IP address resource script log |

| Type | Name | Description |
| --- | --- | --- |
| | rcommflinkserver.log | FlinkServer resource script log |
| | checkHaStatus.log | HA process log |
| | checknode.log | HA health status log |
| | rs-sendAlarm.log | HA alarm sending log |
| | flink_roll.log | FlinkServer active/standby switchover log (active/standby switchover required) |
| FlinkServer audit logs | flinkserver_audit_*yyyymmdd-x*.log.gz | Audit archive log |
| | flinkserver_audit.log | Audit log |
| Stack information log | threadDump-<*DATE*>.log | Log printed when instances are restarted or stopped |

## Log Level

Table 1-26 describes the log levels supported by Flink. The priorities of log levels are ERROR, WARN, INFO, and DEBUG in descending order. Logs whose levels are higher than or equal to the specified level are printed. The number of printed logs decreases as the specified log level increases.

**Table 1-26** Log levels

| Level | Description |
| --- | --- |
| ERROR | Error information about the current event processing |
| WARN | Exception information about the current event processing |
| INFO | Normal running status information about the system and events |
| DEBUG | System information and system debugging information |

To modify log levels, perform the following steps:

**Step 1** Go to the **All Configurations** page of Flink by referring to **Modifying Cluster Service Configuration Parameters**.

**Step 2** On the menu bar on the left, select the log menu of the target role.

**Step 3** Select a desired log level.

**Step 4** Save the configuration. In the displayed dialog box, click **OK** to make the configurations take effect.

**----End**

NOTE

- After the configuration is complete, you do not need to restart the service. Download the client again for the configuration to take effect.
- You can also change the configuration items corresponding to the log level in **log4j-cli.properties**, **log4j.properties**, and **log4j-session.properties** in *Client installation directory*/**Flink/flink/conf/** on the client.
- When a job is submitted using a client, a log file is generated in the **log** folder on the client. The default umask value is **0022**. Therefore, the default log permission is **644**. To change the file permission, you need to change the umask value. For example, to change the umask value of user **omm**:
  - Add **umask 0026** to the end of the **/home/omm/.baskrc** file.
  - Run the **source /home/omm/.baskrc** command to make the file permission take effect.

## Log Format

**Table 1-27** Log formats

| Type | Format | Example |
| --- | --- | --- |
| Run log | <*yyyy-MM-dd HH:mm:ss,SSS*>|<*Log level*>|<*Name of the thread that generates the log*>|<*Message in the log*>|<*Location where the log event occurs*> | 2019-06-27 21:30:31,778 \| INFO \| [flink-akka.actor.default-dispatcher-3] \| TaskManager container_e10_1498290698388_0004_02_000007 has started. \| org.apache.flink.yarn.YarnFlinkResourceManager (FlinkResourceManager.java:368) |

# 1.3.9 Flume Log Overview

## Log Description

**Log path**: The default path of Flume log files is **/var/log/Bigdata/***Role name*.

- FlumeServer: **/var/log/Bigdata/flume/flume**
- FlumeClient: **/var/log/Bigdata/flume-client-n/flume**
- MonitorServer: **/var/log/Bigdata/flume/monitor**

**Log archive rule**: The automatic Flume log compression function is enabled. By default, when the size of logs exceeds 50 MB , logs are automatically compressed into a log file named in the following format: *<Original log file name>-<yyyy-mm-*

*dd_hh-mm-ss>.[ID]*.**log.zip**. A maximum of 20 latest compressed files are reserved. The number of compressed files can be configured on the Manager portal.

**Table 1-28** Flume log list

| Type | Name | Description |
| --- | --- | --- |
| Run logs | /flume/flumeServer.log | Log file that records FlumeServer running environment information. |
| | /flume/install.log | FlumeServer installation log file |
| | /flume/flumeServer-gc.log.*<No.>* | GC archive log file of the FlumeServer process |
| | /flume/prestartDvietail.log | Work log file before the FlumeServer startup |
| | /flume/startDetail.log | Startup log file of the Flume process |
| | /flume/stopDetail.log | Shutdown log file of the Flume process |
| | /monitor/monitorServer.log | Log file that records MonitorServer running environment information |
| | /monitor/startDetail.log | Startup log file of the MonitorServer process |
| | /monitor/stopDetail.log | Shutdown log file of the MonitorServer process |
| | function.log | External function invoking log file |
| | /flume/flume-*Username*-*Date*-*pid*-gc.log | GC log file of the Flume process |
| | /flume/Flume-audit.log | Audit log file of the Flume client |
| | /flume/startAgent.out | Process parameter log file generated before Flume startup |
| Stack information log | threadDump-<DATE>.log | The jstack log file to be printed when the NodeAgent delivers a service stop command |

## Log Level

Table 1-29 describes the log levels supported by Flume.

Levels of run logs are FATAL, ERROR, WARN, INFO, and DEBUG from the highest to the lowest priority. Run logs of equal or higher levels are recorded. The higher the specified log level, the fewer the logs recorded.

**Table 1-29** Log level

| Type | Level | Description |
| --- | --- | --- |
| Run log | FATAL | Logs of this level record critical error information about system running. |
| | ERROR | Logs of this level record error information about system running. |
| | WARN | Logs of this level record exception information about the current event processing. |
| | INFO | Logs of this level record normal running status information about the system and events. |
| | DEBUG | Logs of this level record the system information and system debugging information. |

To modify log levels, perform the following operations:

**Step 1** Go to the **All Configurations** page of Flume by referring to **Modifying Cluster Service Configuration Parameters**.

**Step 2** On the menu bar on the left, select the log menu of the target role.

**Step 3** Select a desired log level.

**Step 4** Save the configuration. In the displayed dialog box, click **OK** to make the configurations take effect.

**----End**

NOTE

The configurations take effect immediately without the need to restart the service.

## Log Format

The following table lists the Flume log formats.

**Table 1-30** Log format

| Type | Format | Example |
| --- | --- | --- |
| Run logs | <*yyyy-MM-dd HH:mm:ss,SSS*>|<*Log level*>|<*Name of the thread that generates the log*>|<*Message in the log*>|<*Location where the log event occurs*> | 2014-12-12 11:54:57,316 \| INFO \| [main] \| log4j dynamic load is start. \| org.apache.flume.tools.LogDynamicLoad.start(LogDynamicLoad.java:59) |
| | <*yyyy-MM-dd HH:mm:ss,SSS*><*Username*><*User IP*><*Time*><*Operation*><*Resource*><*Result*><*Detail*> | 2014-12-12 23:04:16,572 \| INFO \| [SinkRunner-PollingRunner-DefaultSinkProcessor] \| SRCIP=null OPERATION=close |

# 1.3.10 FTP-Server Log Overview

## Log Description

**Log path**: The default storage path of FTP-Server log files is **/var/log/Bigdata/ftp-server/**.

**Log archive rule**: The automatic FTP-Server log compression function is enabled. By default, when the size of logs exceeds 50 MB , logs are automatically compressed into a log file named in the following format: ***<Original log file name>-<yyyy-mm-dd_hh-mm-ss>.[ID]*.log.zip**. A maximum of 20 latest compressed files are reserved. The number of compressed files can be configured on FusionInsight Manager.

**Table 1-31** List of FTP-Server logs

| Log Type | Log File Name | Description |
| --- | --- | --- |
| Run log | ftpserver-server.log | FTP-Server system log, which records the logs generated when the FTP-Server system is running |
| Audit log | ftp-server-audit.log | FTP-Server audit log |
| GC log | ftpserver-omm-<DATE>-<PID>-gc.log.0.current | FTP-Server recycling log |
| Script run log | ftpserver-script.log | Run log of the FTP-Server script |
| Process health check log | ftpserver-instance-check.log | Health check log of the FTP-Server process |

## Log levels

Table 1-32 describes the log levels provided by FTP-Server. Log levels are DEBUG, INFO, WARN, ERROR, and FATAL in ascending order. Logs whose levels are higher than or equal to the specified level are printed. The number of printed logs decreases as the specified log level increases.

**Table 1-32** Log levels

| Level | Description |
| --- | --- |
| DEBUG | Logs of this level record the system information and system debugging information. |
| INFO | Logs of this level record normal running status information about the system and events. |
| WARN | Exception information about the current event processing |
| ERROR | Error information about the current event processing |
| FATAL | Fatal error information about the current event processing. |

To modify log levels, perform the following operations:

**Step 1** Log in to FusionInsight Manager.

**Step 2** Choose **Cluster** > *Name of the desired cluster* > **Services** > **FTP-Server** > **Configurations**.

**Step 3** Select **All Configurations**.

**Step 4** On the menu bar on the left, select the log menu of the target role.

**Step 5** Select a desired log level.

**Step 6** Click **Save**. In the displayed dialog box, click **OK** to make the configurations take effect.

NOTE

The configurations take effect immediately without the need to restart the service.

**----End**

## Log Format

The following table lists the FTP-Server log formats.

**Table 1-33** Log formats

| Log Type | Format | Example |
| --- | --- | --- |
| Run log | *<yyyy-MM-dd HH:mm:ss,SSS>*\|*<Log level>*\|*<Name of the thread that generates the log>*\|*<Message in the log>*\|*<Location where the log event occurs>* | 2015-06-29 10:55:39,056 \| INFO \| [main] \| ftp server configuration information: \| org.apache.hadoop.contrib.ftp.HdfsOverFtpServer.Load_config(HdfsOverFtpServer.java:397) |
| | <Log Level>:CST*<yyyy-MM-dd HH:mm:ss>*<*Script that generates the log*>:<*Message in the log*> | INFO : CST 2019-04-15 09:58:04 ftpserver-instance-check.sh : Start to check ftp-server health. |
| Audit log | *<yyyy-MM-dd HH:mm:ss,SSS>*\|*<Log level>*\|*<Name of the thread that generates the log>*\|*<Message in the log>*\|*<Location where the log event occurs>* | 2015-01-26 18:44:42,607 \| INFO \| IPC Server handler 32 on 25000 \| allowed=true ugi=hbase (auth:SIMPLE) ip=/10.177.112.145 cmd=getfileinfo src=/hbase/WALs/hghoulaslx410,21302,1421743096083/hghoulaslx410%2C21302%2C1421743096083.1422268722795 dst=null perm=null \| org.apache.hadoop.hdfs.server.namenode.FSNamesystem$DefaultAuditLogger.logAuditMessage(FSNamesystem.java:7950) |

# 1.3.11 Guardian Log Overview

## Log Description

**Log path**: **/var/log/Bigdata/guardian/token-server**

**Log archive rule**: The automatic compression and archive function is enabled for Guardian run logs. When the total size of all log files exceeds 50 MB (configurable, see **Configuring the Level and File Size of Tenant Plane Logs**), the log files are automatically compressed into a package named in the format of **token-server.log.[***ID***]**. A maximum of 20 latest compressed files are retained. The number of compressed files and compression threshold can be configured.

**Table 1-34** Guardian log list

| Log Type | Log File Name | Description |
| --- | --- | --- |
| Run log | token-server.log | Guardian run log |
| | startDetail.log | Guardian service prestart log |
| | stopDetail.log | Guardian service stop log |
| | gc.log | Guardian service GC log |

## Log Levels

The following table describes the log levels provided by Guardian.

The log levels are ERROR, WARN, INFO, and DEBUG in descending order of priority. Only logs whose levels are higher than or equal to the specified level are recorded. The higher the log level specified, the fewer the logs are recorded.

**Table 1-35** Log levels

| Level | Description |
| --- | --- |
| ERROR | Logs of this level record error information about system running |
| WARN | Logs of this level record exception information about the current event processing |
| INFO | Logs of this level record normal running status information about the system and events |
| DEBUG | Logs of this level record the system information and system debugging information |

To modify log levels, perform the following operations:

**Step 1** Log in to FusionInsight Manager.

**Step 2** Choose **Cluster** > **Services** > **Guardian**. Click **Configurations** then **All Configurations**.

**Step 3** On the menu bar on the left, select the log menu of the target role.

**Step 4** Select a desired log level.

**Step 5** Click **Save** then **OK**.

NOTE

The configurations take effect immediately without the need to restart the service.

**----End**

# 1.3.12 HBase Log Overview

## Log Description

**Log path**: The default storage path of HBase logs is **/var/log/Bigdata/hbase/***Role name*.

- HMaster: **/var/log/Bigdata/hbase/hm** (run logs) and **/var/log/Bigdata/audit/hbase/hm** (audit logs)
- RegionServer: **/var/log/Bigdata/hbase/rs** (run logs) and **/var/log/Bigdata/audit/hbase/rs** (audit logs)
- ThriftServer: **/var/log/Bigdata/hbase/ts2** (run logs, **ts2** is the instance name) and **/var/log/Bigdata/audit/hbase/ts2** (audit logs, **ts2** is the instance name)
- MetricController: **/var/log/Bigdata/hbase/mc** (run logs) and **/var/log/Bigdata/audit/hbase/mc** (audit logs)

**Log archive rule**: The automatic log compression and archiving function of HBase is enabled. By default, when the size of a log file exceeds 30 MB, the log file is automatically compressed. The naming rule of a compressed log file is as follows: <*Original log name*>-<*yyyy-mm-dd_hh-mm-ss*>.[*ID*].**log.zip** A maximum of 20 latest compressed files are reserved. The number of compressed files can be configured on the Manager portal.

**Table 1-36** HBase log list

| Type | Name | Description |
| --- | --- | --- |
| Run logs | hbase-<SSH_USER>-<process_name>-<hostname>.log | HBase system log that records the startup time, startup parameters, and most logs generated when the HBase system is running. |
| | hbase-<SSH_USER>-<process_name>-<hostname>.out | Log that records the HBase running environment information. |
| | <process_name>-<SSH_USER>-<DATE>-<PID>-gc.log | Log that records HBase junk collections. |
| | checkServiceDetail.log | Log that records whether the HBase service starts successfully. |

| Type | Name | Description |
| --- | --- | --- |
| | hbase.log | Log generated when the HBase service health check script and some alarm check scripts are executed. |
| | sendAlarm.log | Log that records alarms reported after execution of HBase alarm check scripts. |
| | hbase-haCheck.log | Log that records the active and standby status of HMaster. |
| | stop.log | Log that records the startup and stop processes of HBase. |
| | ranger-hbase-plugin-enable.log | Log that records Ranger authentication enabling or disabling of the HBase service. |
| | hbase-trace.log | HBase full-link trace log. |
| | rolling-restart-prepare.log | Rolling upgrade log of the HBase service. |
| | startDetail.log | RegionServer startup log. |
| Audit logs | hbase-audit-<process_name>.log | Log that records HBase security audit. |

## Log Level

Table 1-37 describes the log levels supported by HBase. The priorities of log levels are FATAL, ERROR, WARN, INFO, and DEBUG in descending order. Logs whose levels are higher than or equal to the specified level are printed. The number of printed logs decreases as the specified log level increases.

**Table 1-37** Log levels

| Level | Description |
| --- | --- |
| FATAL | Logs of this level record fatal error information about the current event processing that may result in a system crash. |
| ERROR | Logs of this level record error information about the current event processing, which indicates that system running is abnormal. |
| WARN | Logs of this level record abnormal information about the current event processing. These abnormalities will not result in system faults. |

| Level | Description |
| --- | --- |
| INFO | Logs of this level record normal running status information about the system and events. |
| DEBUG | Logs of this level record the system information and system debugging information. |

To modify log levels, perform the following operations:

**Step 1** Go to the **All Configurations** page of the HBase service. For details, see **Modifying Cluster Service Configuration Parameters**.

**Step 2** On the left menu bar, select the log menu of the target role.

**Step 3** Select a desired log level.

**Step 4** Save the configuration. In the displayed dialog box, click **OK** to make the configurations take effect.

NOTE

The configurations take effect immediately without the need to restart the service.

**----End**

## Log Formats

The following table lists the HBase log formats.

**Table 1-38** Log formats

| Type | Component | Format | Example |
| --- | --- | --- | --- |
| Run logs | HMaster | <yyyy-MM-dd HH:mm:ss,SSS>\|<Log Level>\|<*Thread that generates the log*>\|<*Message in the log*>\|<*Location of the log event*> | 2020-01-19 16:04:53,558 \| INFO \| main \| env:HBASE_THRIFT_OPTS= \| org.apache.hadoop.hbase.util.ServerCommandLine.logProcessInfo(ServerCommandLine.java:113) |
| | RegionServer | <yyyy-MM-dd HH:mm:ss,SSS>\|<Log Level>\|<*Thread that generates the log*>\|<*Message in the log*>\|<*Location of the log event*> | 2020-01-19 16:05:18,589 \| INFO \| regionserver21302-SendThread(linux-k6da:24002) \| Client will use GSSAPI as SASL mechanism. \| org.apache.zookeeper.client.ZooKeeperSaslClient$1.run(ZooKeeperSaslClient.java:285) |

| Type | Component | Format | Example |
| --- | --- | --- | --- |
| | ThriftServer | <yyyy-MM-dd HH:mm:ss,SSS>\|<Log Level>\|<*Thread that generates the log*>\|<*Message in the log*>\|<*Location of the log event*> | 2020-02-16 09:42:55,371 \| INFO \| main \| loaded properties from hadoop-metrics2.properties \| org.apache.hadoop.metrics2.impl.MetricsConfig.loadFirst(MetricsConfig.java:111) |
| | MetricController | <yyyy-MM-dd HH:mm:ss,SSS>\|<Log Level>\|<*Thread that generates the log*>\|<*Message in the log*>\|<*Location of the log event*> | 2023-07-29 18:20:16,374 \| WARN \| hotspot-analysis-pool1 \| Start to analysis later because of empty metric map \| com.huawei.hadoop.hbase.metric.analysis.HotspotAnalyzer.analysisHotspot(HotspotAnalyzer.java:118) |
| Audit logs | HMaster | <yyyy-MM-dd HH:mm:ss,SSS>\|<Log Level>\|<*Thread that generates the log*>\|<*Message in the log*>\|<*Location of the log event*> | 2020-02-16 09:42:40,934 \| INFO \| master:linux-k6da:21300 \| Master: [master:linux-k6da:21300] start operation called. \| org.apache.hadoop.hbase.master.HMaster.run(HMaster.java:581) |
| | RegionServer | <yyyy-MM-dd HH:mm:ss,SSS>\|<Log Level>\|<*Thread that generates the log*>\|<*Message in the log*>\|<*Location of the log event*> | 2020-02-16 09:42:51,063 \| INFO \| main \| RegionServer: [regionserver21302] start operation called. \| org.apache.hadoop.hbase.regionserver.HRegionServer.startRegionServ-er(HRegionServer.java:2396) |
| | ThriftServer | <yyyy-MM-dd HH:mm:ss,SSS>\|<Log Level>\|<*Thread that generates the log*>\|<*Message in the log*>\|<*Location of the log event*> | 2020-02-16 09:42:55,512 \| INFO \| main \| thrift2 server start operation called. \| org.apache.hadoop.hbase.thrift2.ThriftServer.main(ThriftServer.java:421) |

| Type | Component | Format | Example |
| --- | --- | --- | --- |
| | MetricController | <yyyy-MM-dd HH:mm:ss,SSS>\|<Log Level>\|<*Thread that generates the log*>\|<*Message in the log*>\|<*Location of the log event*> | - |

# 1.3.13 HDFS Log Overview

## Log Description

**Log path**: The default path of HDFS logs is **/var/log/Bigdata/hdfs/***Role name*.

- NameNode: **/var/log/Bigdata/hdfs/nn** (run logs) and **/var/log/Bigdata/audit/hdfs/nn** (audit logs)
- DataNode: **/var/log/Bigdata/hdfs/dn** (run logs) and **/var/log/Bigdata/audit/hdfs/dn** (audit logs)
- ZKFC: **/var/log/Bigdata/hdfs/zkfc** (run logs) and **/var/log/Bigdata/audit/hdfs/zkfc** (audit logs)
- JournalNode: **/var/log/Bigdata/hdfs/jn** (run logs) and **/var/log/Bigdata/audit/hdfs/jn** (audit logs)
- Router: **/var/log/Bigdata/hdfs/router** (run logs) and **/var/log/Bigdata/audit/hdfs/router** (audit logs)
- HttpFS: **/var/log/Bigdata/hdfs/httpfs** (run logs) and **/var/log/Bigdata/audit/hdfs/httpfs** (audit logs)

**Log archive rule**: The automatic HDFS log compression function is enabled. By default, when the size of logs exceeds 100 MB, logs are automatically compressed into a log file named in the following format: *<Original log file name>-<yyyy-mm-dd_hh-mm-ss.[ID]>***.log.zip**. A maximum of 100 latest compressed files are reserved. The number of compressed files can be configured on Manager.

**Table 1-39** HDFS log list

| Type | Name | Description |
| --- | --- | --- |
| Run log | hadoop-<SSH_USER>-<process_name>-<hostname>.log | HDFS system log, which records most of the logs generated when the HDFS system is running. |
| | hadoop-<SSH_USER>-<process_name>-<hostname>.out | Log that records the HDFS running environment information. |

| Type | Name | Description |
| --- | --- | --- |
| | hadoop.log | Log that records the operation of the Hadoop client. |
| | hdfs-period-check.log | Log that records scripts that are executed periodically, including automatic balancing, data migration, and JournalNode data synchronization detection. |
| | <process_name>-<SSH_USER>-<DATE>-<PID>-gc.log | Garbage collection log file |
| | postinstallDetail.log | Work log before the HDFS service startup and after the installation. |
| | hdfs-service-check.log | Log that records whether the HDFS service starts successfully. |
| | hdfs-set-storage-policy.log | Log that records the HDFS data storage policies. |
| | cleanupDetail.log | Log that records the cleanup logs about the uninstallation of the HDFS service. |
| | prestartDetail.log | Log that records cluster operations before the HDFS service startup. |
| | hdfs-recover-fsimage.log | Recovery log of the NameNode metadata. |
| | datanode-disk-check.log | Log that records the disk status check during the cluster installation and use. |
| | hdfs-availability-check.log | Log that check whether the HDFS service is available. |
| | hdfs-backup-fsimage.log | Backup log of the NameNode metadata. |

| Type | Name | Description |
| --- | --- | --- |
| | startDetail.log | Detailed log that records the HDFS service startup. |
| | hdfs-blockplacement.log | Log that records the placement policy of HDFS blocks. |
| | upgradeDetail.log | Upgrade logs. |
| | hdfs-clean-acls-java.log | Log that records the clearing of deleted roles' ACL information by HDFS. |
| | hdfs-haCheck.log | Run log that checks whether the NameNode in active or standby state has obtained scripts. |
| | <process_name>-jvmpause.log | Log that records JVM pauses during process running. |
| | hadoop-<SSH_USER>-balancer-<hostname>.log | Run log of HDFS automatic balancing. |
| | hadoop-<SSH_USER>-balancer-<hostname>.out | Log that records information of the environment where HDFS executes automatic balancing. |
| | hdfs-switch-namenode.log | Run log that records the HDFS active/standby switchover. |
| | hdfs-router-admin.log | Run log of the mount table management operation |
| | threadDump-<DATE>.log | Instance process stack log |
| Tomcat logs | hadoop-omm-host1.out, httpfs-catalina.<DATE>.log, httpfs-host-manager.<DATE>.log, httpfs-localhost.<DATE>.log, httpfs-manager.<DATE>.log, localhost_access_web_log.log | Tomcat run log |

| Type | Name | Description |
| --- | --- | --- |
| Audit log | hdfs-audit-<process_name>.log<br>ranger-plugin-audit.log | Audit log that records the HDFS operations (such as creating, deleting, modifying and querying files). |
| | SecurityAuth.audit | HDFS security audit log. |

## Log Level

Table 1-40 lists the log levels supported by HDFS. The log levels include FATAL, ERROR, WARN, INFO, and DEBUG. Logs of which the levels are higher than or equal to the set level will be printed by programs. The higher the log level is set, the fewer the logs are recorded.

**Table 1-40** Log levels

| Level | Description |
| --- | --- |
| FATAL | Indicates the critical error information about system running. |
| ERROR | Indicates the error information about system running. |
| WARN | Indicates that the current event processing exists exceptions. |
| INFO | Indicates that the system and events are running properly. |
| DEBUG | Indicates the system and system debugging information. |

To modify log levels, perform the following operations:

**Step 1** Go to the **All Configurations** page of HDFS by referring to **Modifying Cluster Service Configuration Parameters**.

**Step 2** On the left menu bar, select the log menu of the target role.

**Step 3** Select a desired log level.

**Step 4** Save the configuration. In the displayed dialog box, click **OK** to make the configurations take effect.

NOTE

The configurations take effect immediately without restarting the service.

**----End**

## Log Formats

The following table lists the HDFS log formats.

**Table 1-41** Log formats

| Type | Format | Example |
| --- | --- | --- |
| Run log | *<yyyy-MM-dd HH:mm:ss,SSS>*\|*<Log level>*\|*<Name of the thread that generates the log>*\|*<Message in the log>*\|*<Location where the log event occurs>* | 2015-01-26 18:43:42,840 \| INFO \| IPC Server handler 40 on 25000 \| Rolling edit logs \| org.apache.hadoop.hdfs.server.namenode.FSEditLog.rollEditLog(FSEditLog.java:1096) |
| Audit log | *<yyyy-MM-dd HH:mm:ss,SSS>*\|*<Log level>*\|*<Name of the thread that generates the log>*\|*<Message in the log>*\|*<Location where the log event occurs>* | 2015-01-26 18:44:42,607 \| INFO \| IPC Server handler 32 on 25000 \| allowed=true ugi=hbase (auth:SIMPLE) ip=/10.177.112.145 cmd=getfileinfo src=/hbase/WALs/hghoulaslx410,21302,1421743096083/hghoulaslx410%2C21302%2C1421743096083.1422268722795 dst=null perm=null \| org.apache.hadoop.hdfs.server.namenode.FSNamesystem$DefaultAuditLogger.logAuditMessage(FSNamesystem.java:7950) |

# 1.3.14 HetuEngine Logs

## Log Description

**Log paths**

The HetuEngine logs are stored in **/var/log/Bigdata/hetuengine/** and **/var/log/Bigdata/audit/hetuengine/**.

**Log archiving rules**

Log archiving rules use the FixedWindowRollingPolicy policy. The maximum size of a single file and the maximum number of log archive files can be configured. The rules are as follows:

- When the size of a single file exceeds the default maximum value, a new compressed archive file is generated. The naming rule of the compressed archive log file is as follows: *<Original log name>.[ID]*.log.gz.
- Log deletion rules
  - When the total size of compressed run logs of the HetuEngine compute instance reaches the maximum value, the earliest log file is deleted.

    Run logs of HetuEngine compute instances are synchronized to HDFS and retained for 30 days (**log.clean.task.expire-time.day**) by default. The archive path is **hdfs://hacluster/hetuserverhistory/tenant/coordinator**.
  - When the number of other archived log files reaches the maximum value or the total size of compressed log files reaches the maximum value, the earliest log files are deleted.

By default, the maximum size of an audit log file is 30 MB, and the maximum number of log archive files is 20.

By default, the maximum size of a single run log file is 100 MB, and the maximum number of archived log files is 20. The maximum size of a single HetuEngine compute instance run log file is 100 MB, and logs archived in HDFS are retained for 30 days by default.

To change the maximum size of a single run log file or audit log file or change the maximum number of log archive files of an instance, perform the following operations:

**Step 1** Log in to Manager.

**Step 2** Choose **Cluster** > **Services** > **HetuEngine** > **Configurations** > **All Configurations**.

**Step 3** In the parameter list of log levels, search for **logback.xml** to view the current run log and audit log configurations of HSBroker, HSConsole, HSFabric, and QAS.

NOTE

Parameters related to HetuEngine compute instance run logs

- **log.clean.task.enabled**: indicates whether to enable scheduled compute instance log clearing.
- **log.clean.task.expire-time.day**: indicates the expiration time of compute instance logs archived in HDFS. The default value is 30 days.
- **log.max-history**: indicates the maximum retention period of compute instance logs locally. The default value is 7 days.
- **log.clean.task.schedule.plan**: indicates the schedule for automatically clearing compute instance logs. The value is a cron expression. Only a fixed triggering time in a day can be specified.
- **log.max-size**: indicates the maximum size of a single log file of a HetuEngine compute instance. The default value is 100 MB.
- **log.max-total-size**: indicates the maximum size of compressed HetuEngine compute instance log files. The default value is 5 GB.

**Step 4** Select the configuration item to be modified and modify it.

**Step 5** Click **Save**, and then click **OK**. The configuration automatically takes effect after about 30 seconds.

**----End**

**Table 1-42** HetuEngine log list

| Log Category | Log File | Description |
| --- | --- | --- |
| Installation, startup, and stop log | prestart.log | Preprocessing script log before startup |
| | start.log | Startup log |
| | stop.log | Stop log |
| | postinstall.log | Installation log |
| Run log | *Instance name*.log | Run log |
| | *Instance name*_wsf.log | Interface parameter verification log |
| | hdfs://hacluster/hetuserverhistory/*Tenant*/*Coordinator or worker*/*application_ID*/*container_ID*/*yyyyMMdd*/server.log | Run log of the HetuEngine compute instance |
| Status check log | service_check.log | Health check log |
| | service_getstate.log | Status check log |
| | availability-check.log | HetuEngine status check log |
| | haCheck.log | Log generated when the QAS checks the HA status |
| Audit log | *Instance name*-audit.log | Audit log |
| | hsbroker-audit.log | Audit log of HSBroker operations |
| | hsconsole-audit.log | Audit log of HSConsole operations |
| | hsfabric-audit.log | Audit log of HetuEngine operations performed across domains |
| | hdfs://hacluster/hetuserverhistory/*Tenant*/coordinator/*application_ID*/*container_ID*/*yyyyMMdd*/hetuserver-engine-audit.log | Audit log of the HetuEngine compute instance |
| queryInfo log | hdfs://hacluster/hetuserverhistory/*Tenant*/*Coordinator*/*application_ID*/*container_ID*/*yyyyMMdd*/queryinfo.log | queryInfo log of HetuEngine compute instances, which records SQL running statistics. |

| Log Category | Log File | Description |
| --- | --- | --- |
| Clean log | cleanup.log | Script cleanup log |
| Initialization log | hetupg.log | Metadata initialization log |
| | ranger-trino-plugin-enable.log | Operation log of integrating Ranger plug-ins to the HetuEngine kernel |
| Client log | qas_client.log | ZooKeeper client log of the QAS instance |
| Stack information log | threadDump-<*DATE*>.log | Log printed when instances are restarted or stopped |
| Other | hetu-updateKrb5.log | Log generated when the Hive data source configuration is automatically updated after the Hive cluster domain is changed. |
| | hetu_utils.log | Log generated when the preprocessing script calls the tool class to upload files to the HDFS during startup. |

## Log Level

Table 1-43 describes the log levels provided by HetuEngine. The priorities of log levels are OFF, ERROR, WARN, INFO, and DEBUG in descending order. Logs whose levels are higher than or equal to the specified level are printed. The number of printed logs decreases as the specified log level increases.

**Table 1-43** Log levels

| Level | Description |
| --- | --- |
| OFF | Logs of this level record no logs. |
| ERROR | Logs of this level record error information about the current event processing. |
| WARN | Logs of this level record exception information about the current event processing. |
| INFO | Logs of this level record normal running status information about the system and events. |

| Level | Description |
| --- | --- |
| DEBUG | Logs of this level record the system information and system debugging information. |

To change the run log or audit log level of an instance, perform the following steps:

**Step 1** Log in to FusionInsight Manager.

**Step 2** Choose **Cluster** > **Services** > **HetuEngine** > **Configurations** > **All Configurations**.

**Step 3** In the parameter list of log levels, search for **logback.xml** to view the current run log and audit log levels of HSBroker, HSConsole, and HSFabric.

**Step 4** Select a desired log level.

**Step 5** Click **Save**, and then click **OK**. The configuration automatically takes effect after about 30 seconds.

**----End**

To change the HetuEngine Coordinator/Worker log level, perform the following steps:

**Step 1** Log in to FusionInsight Manager.

**Step 2** Choose **Cluster** > **Services** > **HetuEngine** > **Configurations** > **All Configurations**.

**Step 3** In the parameter list of log levels, search for **log.properties** to view the current log levels.

**Step 4** Select a desired log level.

**Step 5** Click **Save**, and then click **OK**. Wait until the operation is successful.

**Step 6** Choose **Cluster** > **Services** > **HetuEngine** > **Instance**, click the HSBroker instance in the role list, and choose **More** > **Restart Instance**.

**Step 7** After the HSBroker instance is restarted, choose **Cluster** > **Services** > **HetuEngine**. On the overview page, click the link next to **HSConsole WebUI** to go to the compute instance page.

**Step 8** Select the compute instances to be restarted and click **Stop**. After all instances are stopped, click **Start** to restart the compute instances.

**----End**

# 1.3.15 Hive Log Overview

## Log Description

**Log path**: The default save path of Hive logs is **/var/log/Bigdata/hive/***role name*, the default save path of Hive1 logs is **/var/log/Bigdata/hive1/***role name*, and the others follow the same rule.

- HiveServer: **/var/log/Bigdata/hive/hiveserver** (run log) and **var/log/Bigdata/audit/hive/hiveserver** (audit log)
- MetaStore: **/var/log/Bigdata/hive/metastore** (run log) and **/var/log/Bigdata/audit/hive/metastore** (audit log)
- WebHCat: **/var/log/Bigdata/hive/webhcat** (run log) and **/var/log/Bigdata/audit/hive/webhcat** (audit log)

**Log archive rule**: The automatic compression and archiving function of Hive is enabled. By default, when the size of a log file exceeds 20 MB (which is adjustable), the log file is automatically compressed. The naming rule of a compressed log file is as follows: <*Original log name*>-<*yyyy-mm-dd_hh-mm-ss*>.[*ID*].**log.zip** A maximum of 20 latest compressed files are reserved. The number of compressed files and compression threshold can be configured.

**Table 1-44** Hive log list

| Log Type | Log File Name | Description |
| --- | --- | --- |
| Run log | /hiveserver/hiveserver.out | Log file that records HiveServer running environment information. |
| | /hiveserver/hive.log | Run log file of the HiveServer process. |
| | /hiveserver/hive-omm-*<Date>*-*<PID>*-gc.log.*<No.>* | GC log file of the HiveServer process. |
| | /hiveserver/prestartDetail.log | Work log file before the HiveServer startup. |
| | /hiveserver/check-serviceDetail.log | Log file that records whether the Hive service starts successfully |
| | /hiveserver/cleanupDetail.log | Cleanup log file about the HiveServer uninstallation |
| | /hiveserver/startDetail.log | Startup log file of the HiveServer process. |
| | /hiveserver/stopDetail.log | Shutdown log file of the HiveServer process. |
| | /hiveserver/localtasklog/omm_*<Date>*_*<Task ID>*.log | Run log file of the local Hive task. |
| | /hiveserver/localtasklog/omm_*<Date>*_*<Task ID>*-gc.log.*<No.>* | GC log file of the local Hive task. |
| | /metastore/metastore.log | Run log file of the MetaStore process. |

| Log Type | Log File Name | Description |
| --- | --- | --- |
| | /metastore/hive-omm-*<Date>*-*<PID>*-gc.log.*<No.>* | GC log file of the MetaStore process. |
| | /metastore/postinstallDetail.log | Work log file after the MetaStore installation. |
| | /metastore/prestartDetail.log | Work log file before the MetaStore startup |
| | /metastore/cleanupDetail.log | Cleanup log file of the MetaStore uninstallation |
| | /metastore/startDetail.log | Startup log file of the MetaStore process. |
| | /metastore/stopDetail.log | Shutdown log file of the MetaStore process. |
| | /metastore/metastore.out | Log file that records MetaStore running environment information. |
| | /webhcat/webhcat-console.out | Log file that records the normal start and stop of the WebHCat process. |
| | /webhcat/webhcat-console-error.out | Log file that records the start and stop exceptions of the WebHCat process. |
| | /webhcat/prestartDetail.log | Work log file before the WebHCat startup. |
| | /webhcat/cleanupDetail.log | Cleanup logs generated during WebHCat uninstallation or before WebHCat installation |
| | /webhcat/hive-omm-<*Date*>-<PID>-gc.log.<*No.*> | GC log file of the WebHCat process. |
| | /webhcat/webhcat.log | Run log file of the WebHCat process |
| Audit log | hive-audit.log<br>hive-rangeraudit.log | HiveServer audit log file |
| | queryinfo.log | HiveServer quer log, which records SQL running statistics and SQL interception information. |
| | metastore-audit.log | MetaStore audit log file. |

| Log Type | Log File Name | Description |
| --- | --- | --- |
| | webhcat-audit.log | WebHCat audit log file. |
| | jetty-<Date>.request.log | Request logs of the jetty service. |

## Log Levels

Table 1-45 describes the log levels supported by Hive.

Levels of run logs are ERROR, WARN, INFO, and DEBUG from the highest to the lowest priority. Run logs of equal or higher levels are recorded. The higher the specified log level, the fewer the logs recorded.

**Table 1-45** Log levels

| Level | Description |
| --- | --- |
| ERROR | Logs of this level record error information about system running. |
| WARN | Logs of this level record exception information about the current event processing. |
| INFO | Logs of this level record normal running status information about the system and events. |
| DEBUG | Logs of this level record the system information and system debugging information. |

To modify log levels, perform the following operations:

**Step 1** Go to the **All Configurations** page of the Yarn service by referring to **Modifying Cluster Service Configuration Parameters**.

**Step 2** On the menu bar on the left, select the log menu of the target role.

**Step 3** Select a desired log level and save the configuration.

NOTE

The Hive log level takes effect immediately after being configured. You do not need to restart the service.

**----End**

## Log Formats

The following table lists the Hive log formats:

**Table 1-46** Log formats

| Log Type | Format | Example |
| --- | --- | --- |
| Run log | <yyyy-MM-dd HH:mm:ss,SSS>\|<LogLevel>\|<Thread that generates the log>\|<Message in the log>\|<Location of the log event> | 2014-11-05 09:45:01,242 \| INFO \| main \| Starting hive metastore on port 21088 \| org.apache.hadoop.hive.metastore.HiveMetaStore.main(HiveMetaStore.java:5198) |
| Audit log | <yyyy-MM-dd HH:mm:ss,SSS>\|<LogLevel>\|<Thread that generates the log>\|<User Name><User IP><Time><Operation><Resource><Result><Detail >\|<Location of the log event > | 2018-12-24 12:16:25,319 \| INFO \| HiveServer2-Handler-Pool: Thread-185 \| UserName=hive UserIP=10.153.2.204 Time=2018/12/24 12:16:25 Operation=CloseSession Result=SUCCESS Detail= \| org.apache.hive.service.cli.thrift.ThriftCLIService.logAuditEvent(ThriftCLIService.java:434) |

# 1.3.16 Hue Log Overview

## Log Description

**Log paths**: The default paths of Hue logs are **/var/log/Bigdata/hue** (for storing run logs) and **/var/log/Bigdata/audit/hue** (for storing audit logs).

**Log archive rules**: The automatic compression and archiving function of the Hue logs is enabled. By default, when the size of a log file (**access.log**, **error.log**, **runcpserver.log**, or **hue-audits.log**) exceeds 5 MB, logs are automatically compressed. A maximum of 20 latest compressed files are reserved. The number of compressed files and compression threshold can be configured.

**Table 1-47** Hue log list

| Type | Log File Name | Description |
| --- | --- | --- |
| Run log | access.log | Access log file |
| | error.log | Error log file |
| | gsdb_check.log | Log file of the GaussDB check information |
| | kt_renewer.log | Log file of Kerberos authentication |
| | kt_renewer.out | Log file of the abnormal Kerberos authentication logs |

| Type | Log File Name | Description |
| --- | --- | --- |
| | runcpserver.log | Log file of operation records |
| | runcpserver.out | Log file of process running exceptions |
| | supervisor.log | Log file of process startup |
| | supervisor.out | Log file of process startup exceptions |
| | dbDetail.log | Log file of database initialization |
| | initSecurityDetail.log | Download initialization log file of the Keytab file |
| | postinstallDetail.log | Work log file generated after the Hue service is installed |
| | prestartDetail.log | Prestart log file |
| | statusDetail.log | Log file of the Hue health status |
| | startDetail.log | Startup log |
| | get-hue-ha.log | Log file of the Hue HA status |
| | get-hue-ha.log.*Date* | Log file of the Hue HA status |
| | hue-ha-status.log | Log file of the Hue HA status monitoring |
| | get-hue-health.log | Log file of the Hue health status |
| | hue-health-check.log | Log file of the Hue health check |
| | hue-refresh-config.log | Log file of the Hue configuration update |
| | hue-script-log.log | Log file of the Hue operations on the Manager console |
| | hue-service-check.log | Log file of the Hue service status monitoring |
| | db_pwd.log | Log that records the changes of the password for Hue to connect to the DBService database |
| | modifyDBPwd_*Date*.log | - |
| | watch_config_update.log | Parameter update log file |
| Audit log | hue-audits.log | Audit log file |

## Log Level

Table 1-48 describes the log levels supported by Hue.

Levels of logs are ERROR, WARN, INFO, and DEBUG from the highest to the lowest priority. Run logs of equal or higher levels are recorded. The higher the specified log level, the fewer the logs recorded.

**Table 1-48** Log levels

| Level | Description |
| --- | --- |
| ERROR | Logs of this level record error information about system running. |
| WARN | Logs of this level record exception information about the current event processing. |
| INFO | Logs of this level record normal running status information about the system and events. |
| DEBUG | Logs of this level record the system information and system debugging information. |

To modify log levels, perform the following operations:

**Step 1** Go to the **All Configurations** page of the Hue service by referring to **Modifying Cluster Service Configuration Parameters**.

**Step 2** In the navigation tree on the left, select **Log** corresponding to the role to be modified.

**Step 3** Select the log level to be changed on the right.

**Step 4** Save the configuration. In the displayed dialog box, click **OK** to make the configurations take effect.

**Step 5** Restart the service or instance whose configuration has expired for the configuration to take effect.

**----End**

## Log Format

The following table lists the Hue log formats:

**Table 1-49** Log formats

| Type | Format | Example |
| --- | --- | --- |
| Run log | *<dd-MM-yy HH:mm:ss,SSS><Location where the log event occurs><Log level><Message in the log>* | [03/Nov/2014 11:57:19 ] middleware \| INFO \| Unloading MimeTypeJSFileFixStrea-mingMiddleware. |
| | *<Log level><Time format><yyyy-MM-dd HH:mm:ss,SSS><Location where the log event occurs><Message in the log>* | INFO : CST 2014-11-06 11:22:52 hue-ha-status.sh : update 4 <= 15:myHostName=10.0.0.250 ACTIVE=10.0.0.250 |
| Audit log | *<UserName><yyyy-MM-dd HH:mm:ss,SSS>< Audit operation description> <Resource parameter> <URL> <Whether to allow> <Audit operation> <IP address>* | {"username": "admin", "eventTime": "2014-11-06 10:28:34", "operationText": "Successful login for user: admin", "service": "accounts", "url": "/accounts/login/", "allowed": true, "operation": "USER_LOGIN", "ipAddress": "10.0.0.250"} |

## 1.3.17 IoTDB Log Overview

**Description**

## Log Description

**Log paths**: The default storage paths of IoTDB logs are **/var/log/Bigdata/iotdb/confignode** and **/var/log/Bigdata/iotdb/iotdbserver** (for run logs) as well as **/var/log/Bigdata/audit/iotdb/iotdbserver** (for audit logs).

**Log archive rule**: The automatic compression and archiving function of IoTDB is enabled. By default, when the size of a log file exceeds 20 MB (which is adjustable), the log file is automatically compressed. The naming rule of the compressed log file is as follows: <*Original log file name*>-<*yyyymmdd*>.*ID*.**log.gz**. A maximum of 10 latest compressed files are reserved. The number of compressed files and compression threshold can be configured.

**Table 1-50** IoTDB log list

| Type | Name | Description |
| --- | --- | --- |
| ConfigNode run log | log_confignode_all.log | ConfigNode instance all log |
| | log_confignode_error.log | ConfigNode instance error log |
| | log-measure.log | ConfigNode instance monitoring log |
| | log-query-debug.log | ConfigNode query debug log |
| | log-query-frequency.log | ConfigNode query frequency log |
| | log-sync.log | ConfigNode synchronization log |
| | log-slow-sql.log | ConfigNode slow SQL log |
| | server.out | ConfigNode instance startup exception log |
| | postinstall.log | ConfigNode process startup log |
| | prestart.log | ConfigNode process startup exception log |
| | service-healthcheck.log | IoTDB database initialization log. |
| | start.log | ConfigNode instance startup log |
| | stop.log | ConfigNode instance stopping log |
| | ConfigNode-threadDump-<timestamp>.log | ConfigNode instance stack log |
| | ConfigNode-gc.log.0.current | ConfigNode instance GC log |
| IoTDBServer run log | log_datanode_all.log | IoTDBServer instance all log |
| | log_datanode_error.log | IoTDBServer instance error log |
| | log_datanode_measure.log | IoTDBServer instance monitoring log |
| | log_datanode_query_debug.log | IoTDBServer query debug log |
| | log_datanode_query_frequency.log | IoTDBServer query frequency log |

| Type | Name | Description |
| --- | --- | --- |
| | log_datanode_sync.log | IoTDBServer synchronization log |
| | log_datanode_slow_sql.log | IoTDBServer slow SQL log |
| | server.out | IoTDBServer instance startup exception log |
| | postinstall.log | IoTDBServer process startup log |
| | prestart.log | IoTDBServer process startup exception log |
| | service-healthcheck.log | IoTDB database initialization log. |
| | start.log | IoTDBServer instance startup log |
| | stop.log | IoTDBServer instance stopping log |
| | IoTDBServer-threadDump-<timestamp>.log | IoTDBServer instance stack log |
| | IoTDBServer-gc.log.0.current | IoTDBServer instance GC log |
| IoTDBServer audit log | log_datanode_audit.log | IoTDBServer audit log |

**Log levels**

Table 1-51 describes the log levels supported by IoTDB.

Levels of logs are ERROR, WARN, INFO, and DEBUG from the highest to the lowest priority. Run logs of equal or higher levels are recorded. The higher the specified log level, the fewer the logs recorded.

**Table 1-51** Log levels

| Level | Description |
| --- | --- |
| ERROR | Logs of this level record error information about system running. |
| WARN | Logs of this level record exception information about the current event processing. |
| INFO | Logs of this level record normal running status information about the system and events. |

| Level | Description |
| --- | --- |
| DEBUG | Logs of this level record the system information and system debugging information. |

To modify log levels, perform the following operations:

1. Go to the **All Configurations** page of the IoTDB service by referring to **Modifying Cluster Service Configuration Parameters**.
2. In the navigation tree on the left, select **Log** corresponding to the role to be modified.
3. Select a desired log level and save the configuration.

NOTE

The IoTDB log level takes effect 60 seconds after being configured. You do not need to restart the service.

## Log Formats

The following table lists the IoTDB log formats:

**Table 1-52** Log formats

| Type | Format | Example |
| --- | --- | --- |
| Run log | <*yyyy-MM-dd HH:mm:ss,SSS*> \| *Log level* \| [*Thread name*] \| *Log information* \| *Log printing class* (*File*:*Line number*) | 2021-06-08 10:08:41,221 \| ERROR \| [main] \| Client failed to open SaslClientTransport to interact with a server during session initiation: \| org.apache.iotdb.rpc.sasl.TFastSaslTransport (TFastSaslTransport.java:257) |
| Audit log | <*yyyy-MM-dd HH:mm:ss,SSS*> \| *Log level* \| [*Thread name*] \| *Log information* \| *Log printing class* (*File*:*Line number*) | 2021-06-08 11:03:49,365 \| INFO \| [ClusterClient-1] \| Session-1 is closing \| IoTDB_AUDIT_LOGGER (TSServiceImpl.java:326) |

# 1.3.18 JobGateway Logs

## Log Description

**Log path**: **/var/log/Bigdata/job-gateway/**

**Log archive rule**: The automatic compression and archive function is enabled for JobGateway run logs. When the total size of all log files exceeds 20 MB (configurable), the log files are automatically compressed into a package named in the format of *Original log file name*-*yyyy-mm-dd*.*No.*.**log.zip**. A maximum of 20

latest compressed files are retained. The number of compressed files and compression threshold can be configured.

**Table 1-53** JobGateway log list

| Log Type | Log File Name | Description |
| --- | --- | --- |
| JobServer run log | job-gateway.log | Service run log |
| | prestart.log | Service prestart log |
| | availability-check.log | Service availability check log |
| | verbose-gc-sp.txt | Service GC log |
| | start-stop.log | Service startup and stop logs |
| | update-multi-service-client.log | Client update logs recorded when multiple services of components related to JobGateway job submission are added |
| | gc.log | Service GC log |
| JobServer audit log | access_log.{yyyy-MM-dd}.log | Service audit log |
| Balance run log | availability-check.log | Service availability check log |
| | error.log | Service error log |
| | prestart.log | Service prestart log |
| | start.log | Service startup log |
| Balance audit log | access_http.log | Service audit log |

## Log Levels

The following table describes the log levels provided by JobGateway. Log level changes on a JobServer are applied dynamically without restarting the JobServer instance.

The log levels are ERROR, WARN, INFO, and DEBUG in descending order of priority. Only logs whose levels are higher than or equal to the specified level are recorded. The higher the log level specified, the fewer the logs are recorded.

**Table 1-54** Log levels

| Level | Description |
| --- | --- |
| ERROR | Logs of this level record error information about system running |
| WARN | Logs of this level record exception information about the current event processing |
| INFO | Logs of this level record normal running status information about the system and events |
| DEBUG | Logs of this level record the system information and system debugging information |

To modify log levels, perform the following operations:

1. Log in to FusionInsight Manager.
2. Choose **Cluster** > **Services** > **JobGateway** and click **Configurations**.
3. Click **All Configurations**.
4. On the menu bar on the left, select the log menu of the target role.
5. Select a desired log level.
6. Click **Save** then **OK**.

# 1.3.19 Kafka Log Overview

## Log Description

**Log paths**: The default storage path of Kafka logs is **/var/log/Bigdata/kafka**. The default storage path of audit logs is **/var/log/Bigdata/audit/kafka**.

- Broker: **/var/log/Bigdata/kafka/broker** (run logs)
- Kafka UI: **/var/log/Bigdata/kafka/ui** (run logs)
- MirrorMaker: **/var/log/Bigdata/kafka/mirrormaker** (run logs)

Log archive rule: The automatic Kafka log compression function is enabled. By default, when the size of logs exceeds 30 MB, logs are automatically compressed into a log file named in the following format: *<Original log file name>-<yyyy-mm-dd_hh-mm-ss>.[ID]*.**log.zip**. A maximum of 20 latest compressed files are retained by default. You can configure the number of compressed files and the compression threshold.

**Table 1-55** Broker log list

| Type | Log File Name | Description |
| --- | --- | --- |
| Run log | server.log | Server run log of the broker process |
| | controller.log | Controller run log of the broker process |
| | kafka-request.log | Request run log of the broker process |
| | log-cleaner.log | Cleaner run log of the broker process |
| | state-change.log | State-change run log of the broker process |
| | kafkaServer-<SSH_USER>-<DATE>-<PID>-gc.log | GC log of the broker process |
| | postinstall.log | Work log after broker installation |
| | prestart.log | Work log before broker startup |
| | checkService.log | Log that records whether broker starts successfully |
| | start.log | Startup log of the broker process |
| | stop.log | Stop log of the broker process |
| | checkavailable.log | Log that records the health check details of the Kafka service |
| | checkInstanceHealth.log | Log that records the health check details of broker instances |
| | kafka-authorizer.log | Broker authorization log |
| | kafka-root.log | Broker basic log |
| | cleanup.log | Cleanup log of broker uninstallation |
| | metadata-backup-recovery.log | Broker backup and recovery log |
| | ranger-kafka-plugin-enable.log | Log that records the Ranger plug-ins enabled by brokers |

| Type | Log File Name | Description |
| --- | --- | --- |
| | server.out | Broker JVM log |
| | audit.log | Authentication log of the Ranger authentication plug-in. This log is archived in the **/var/log/Bigdata/audit/kafka** directory. |
| | threadDump-Broker-xxx.log | Stack log generated when the Broker thread stops abnormally |

**Table 1-56** Kafka UI log list

| Type | Log File Name | Description |
| --- | --- | --- |
| Run log | kafka-ui.log | Run log of the Kafka UI process |
| | postinstall.log | Work log after Kafka UI installation |
| | cleanup.log | Cleanup log of Kafka UI uninstallation |
| | prestart.log | Work log before Kafka UI startup |
| | ranger-kafka-plugin-enable.log | Log that records the Ranger plug-ins enabled by Kafka UI |
| | start.log | Startup log of the Kafka UI process |
| | stop.log | Stop log of the Kafka UI process |
| | start.out | Kafka UI process startup information |
| | checkInstanceHealth.log | Log that records the health check details of KafkaUI instances |
| | threadDump-kafkaUI-xxx.log | Stack log generated when the KafkaUI thread stops abnormally |
| Audit log | audit.log | Audit log of the KafkaUI service |

| Type | Log File Name | Description |
| --- | --- | --- |
| Authentication log | kafka-authorizer.log | Run log file of the open-source authentication plug-in of Kafka.<br>This log is archived in the **/var/log/Bigdata/audit/kafka/kafkaui** directory. |
| | ranger-authorizer.log | Run log of the Ranger authentication plug-in. This log is archived in the **/var/log/Bigdata/audit/kafka/kafkaui** directory. |

**Table 1-57** MirrorMaker log list

| Type | Log File Name | Description |
| --- | --- | --- |
| Run log | mirrormaker.out | MirrorMaker process startup information |
| | mirrormaker.log | Run log of the MirrorMaker process |
| | cleanup.log | Cleanup log of MirrorMaker uninstallation |
| | prestart.log | Work log before MirrorMaker startup |
| | start.log | Startup log of the MirrorMaker process |
| | postinstall.log | Work log after MirrorMaker installation |
| | stop.log | Stop log of the MirrorMaker process |
| | mirrorMaker-omm-***-pid***-gc.log.*.current | MirrorMaker process GC log |
| | checkInstanceHealth.log | Log that records the health check details of MirrorMaker instances |
| | threadDump-MirrorMaker-xxx.log | Stack log generated when the MirrorMaker thread stops abnormally |

## Log Level

Table 1-58 describes the log levels supported by Kafka.

Levels of run logs are ERROR, WARN, INFO, and DEBUG from the highest to the lowest priority. Run logs of equal or higher levels are recorded. The higher the specified log level, the fewer the logs recorded.

**Table 1-58** Log levels

| Level | Description |
| --- | --- |
| ERROR | Logs of this level record error information about system running. |
| WARN | Logs of this level record exception information about the current event processing. |
| INFO | Logs of this level record normal running status information about the system and events. |
| DEBUG | Logs of this level record the system information and system debugging information. |

To modify log levels, perform the following operations:

**Step 1** Go to the **All Configurations** page. See **Modifying Cluster Service Configuration Parameters**.

**Step 2** On the menu bar on the left, select the log menu of the target role.

**Step 3** Select a desired log level.

**Step 4** Save the configuration. In the displayed dialog box, click **OK** to make the configurations take effect.

NOTE

After the log levels of KafkaUI and MirrorMaker are changed, you need to restart the KafkaUI or MirrorMaker instances for the change to take effect. Perform the following operations to restart the instances:

Log in to FusionInsight Manager and choose **Cluster** > **Services** > **Kafka**. Click **Instance**, select the KafkaUI or MirrorMaker instances, click **More**, and select **Restart Instance** to restart the instances.

**----End**

## Log Format

The following table describes the Kafka log format.

**Table 1-59** Log formats

| Type | Format | Example |
| --- | --- | --- |
| Run log | <yyyy-MM-dd HH:mm:ss,SSS>|<Log Level>|<Thread that generates the log>|<Message in the log>|<Full name of the log event invocation class>(<Log file>:<Row>) | 2015-08-08 11:09:53,483 \| INFO \| [main] \| Loading logs. \| kafka.log.LogManager (Logging.scala:68) |
| | <yyyy-MM-dd HH:mm:ss><HostName><Component name><logLevel><Message> | 2015-08-08 11:09:51 10-165-0-83 Kafka INFO Running kafka-start.sh. |

# 1.3.20 Knox Logs

## Log Description

**Log path**: The default storage path of Knox logs is **/var/log/Bigdata/knox/logs**.

**Table 1-60** Knox log list

| Log Type | Log File Name | Description |
| --- | --- | --- |
| Run logs | knox-self-start.log | Knox startup log file, which records most of the logs generated when the Knox system is started |
| | gateway.log | Run logs of Knox |
| Audit logs | gateway-audit.log | Audit log that records Knox's access to Executor or Manager interfaces |

## Log Levels

Table 1-61 describes the log levels provided by Knox. The priorities of log levels are ERROR, WARN, INFO, and DEBUG in descending order. Logs whose levels are higher than or equal to the specified level are printed. The number of printed logs decreases as the specified log level increases.

**Table 1-61** Log levels

| Level | Description |
| --- | --- |
| ERROR | Error information about the current event processing. |
| WARN | Exception information about the current event processing |
| INFO | Logs of this level record normal running status information about the system and events. |
| DEBUG | Logs of this level record the system information and system debugging information. |

## Log Formats

The Knox log format is as follows:

**Table 1-62** Log formats

| Log Type | Format | Example |
| --- | --- | --- |
| Run logs | <yyyy-MM-dd HH:mm:ss,SSS>\|<Log Level>\|<Message in the log> | [2020-12-26 12:19:19] WARN Wait for mount dist over,sleep 3s.(234) |
| Audit logs | <yyyy-MM-dd HH:mm:ss,SSS>\|<Log Level>\|default\|<Message in the log>\|<Location of the log event> | 20/12/30 00:57:07 \|\| da53ab37-8c21-4b19-add9-42de197f68c3\| audit\|170.32.1.45\| MRSWEB\|\|\|access\|uri\|/gateway/mrsweb/mrsmanager/api/v2/session/status?_=1609246591960\| unavailable\|Request method: GET |

# 1.3.21 Executor Logs

## Log Description

**Log path**: The default storage path of Executor logs is **/var/log/Bigdata/executor/logs**.

**Table 1-63** Knox log list

| Type | Log File Name | Description |
| --- | --- | --- |
| Run logs | executor-self-start.log | Executor startup log file, which records most of the logs generated when the Executor system is started |
| | exe.log | Executor run log file |
| Audit logs | authservice.log | Authentication log for the Executor to access the Manager |

## Log Levels

Table 1-64 describes the log levels provided by Executor. The priorities of log levels are ERROR, WARN, INFO, and DEBUG in descending order. Logs whose levels are higher than or equal to the specified level are printed. The number of printed logs decreases as the specified log level increases.

**Table 1-64** Log levels

| Level | Description |
| --- | --- |
| ERROR | Error information about the current event processing. |
| WARN | Exception information about the current event processing |
| INFO | Logs of this level record normal running status information about the system and events. |
| DEBUG | Logs of this level record the system information and system debugging information. |

## Log Formats

The following table lists the Executor log formats:

**Table 1-65** Log formats

| Type | Format | Example |
| --- | --- | --- |
| Run logs | <yyyy-MM-dd HH:mm:ss,SSS>\|<Log Level>\|<Message in the log> | [2020-12-26 12:19:19] WARN Wait for mount dist over,sleep 3s.(234) |

| Type | Format | Example |
| --- | --- | --- |
| Audit logs | <yyyy-MM-dd HH:mm:ss,SSS>\|<Log Level>\|default\|<Message in the log>\|<Location of the log event> | 20/12/30 00:57:07 \|\| da53ab37-8c21-4b19-add9-42de197f68c3\| audit\|170.32.1.45\| MRSWEB\|\|\|access\|uri\|/gateway/mrsweb/mrsmanager/api/v2/session/status?_=1609246591960\| unavailable\|Request method: GET |

## 1.3.22 LakeSearch Logs

**Log paths:**

- SearchServer log path: **/var/log/Bigdata/lakesearch/searchserver**
- SearchFactory log path: **/var/log/Bigdata/lakesearch/searchfactory**

**Log archiving rules**:

By default, service logs are stored every 50 MB or every day, and 20 log files are retained for 30 days and compressed in GZIP format.

**Table 1-66** LakeSearch logs

| Log Type | Log File | Description |
| --- | --- | --- |
| SearchServer logs | cleanup.log | Cleanup log file for instance installation and uninstallation |
| | prestart.log | Startup log |
| | scc.log | Run log of the encryption and decryption framework |
| | searchserver-*.log.gz | Archive package of SearchServer run log |
| | searchserver-gc.log | GC log |
| | searchserver.log | Run log |
| | searchserver-process-check.log | Health check log |
| | searchserver-shutdown.log | Stop log |
| | searchserver-start.log | Startup log |

| Log Type | Log File | Description |
| --- | --- | --- |
| | tomcat_access.log | Log file that records information about all requests for accessing SearchServer |
| SearchFactory Logs | cleanup.log | Cleanup log file for instance installation and uninstallation |
| | postinstall.log | Pre-preparation log after instance installation |
| | prestart.log | Startup log |
| | searchfactory-*.log.gz | Archive package of SearchFactory run log |
| | searchfactory-gc.log | GC log |
| | searchfactory.log | Run log |
| | searchfactory-process-check.log | Health check log |
| | searchfactory-shutdown.log | Stop log |
| | searchfactory-start.log | Startup log |
| | tomcat_access.log | Log file that records information about all requests for accessing SearchFactory |

## Log Level

Table 1-67 describes the log levels of LakeSearch. The priorities of log levels are ERROR, WARN, INFO, DEBUG, and TRACE in the descending order. Logs of a specified level or higher can be printed. If you specify a higher log level, fewer logs will be printed.

**Table 1-67** Log levels

| Level | Description |
| --- | --- |
| OFF | Logs of this level indicate that the log output is disabled. |
| ERROR | Logs of this level record errors about event processing. |
| WARN | Logs of this level record exception information about the current event processing |
| INFO | Logs of this level record normal running status information about the system and events |

| Level | Description |
| --- | --- |
| DEBUG | Logs of this level record the system information and system debugging information |
| TRACE | Logs of this level indicate information whose granularity is lower than that of DEBUG. |

To modify log levels, perform the following operations:

**Step 1** Log in to FusionInsight Manager and choose **Cluster** > **Services** > **LakeSearch**. Click **Configurations** and click **All Configurations**.

**Step 2** On the menu bar on the left, select the log menu of the target role.

**Step 3** Select a desired log level.

**Step 4** Save the configuration. In the displayed dialog box, click **OK** to apply the change.

**----End**

## Log Format

**Table 1-68** Log formats

| Type | Format | Example |
| --- | --- | --- |
| Run log | <yyyy-MM-dd HH:mm:ss,SSS>\|<Log Level>\|<Name of the thread that generates the log>\|<Name of the class that output the log>\|<Host name>\|<Tag>\|<Message in the log>\|<newline> | [2024-01-24T18:57:45,116][WARN ][main][c.h.s.s.w.u.OmSwitch ][hostname][WSF-OM] Can't find the om properties file. |

# 1.3.23 Loader Log Overview

## Log Description

**Log path**: The default storage path of Loader log files is **/var/log/Bigdata/loader/Log category**.

- runlog: /var/log/Bigdata/loader/runlog (run logs)
- scriptlog: /var/log/Bigdata/loader/scriptlog/ (script execution logs)
- catalina: /var/log/Bigdata/loader/catalina (Tomcat startup and stop logs)
- audit: /var/log/Bigdata/loader/audit (audit logs)

**Log archive rule**:

The automatic compression and archiving function are enabled for Loader run logs and audit logs. By default, when the size of a log file exceeds 10 MB, the log file is automatically compressed into a log file named in the following rule: *<Original log file name>-<yyyy-mm-dd_hh-mm-ss>.[ID]***.log.zip**. A maximum of 20 latest compressed files are reserved. The number of compressed files can be configured on the Manager portal.

**Table 1-69** Loader log list

| Log Type | Log File Name | Description |
| --- | --- | --- |
| Run log | loader.log | Loader system log file that records most of the logs generated when the TelcoFS system is running. |
| | loader-omm-***-pid***-gc.log.*.current | Loader process GC log file |
| | sqoopInstanceCheck.log | Loader instance health check log file |
| Audit log | default.audit | Loader operation audit log file that records operations such as adding, deleting, modifying, and querying jobs and user login |
| Tomcat log | catalina.out | Tomcat run log file. |
| | catalina. <yyyy-mm-dd >.log | Tomcat run log file |
| | host-manager. <yyyy-mm-dd >.log | Tomcat run log file |
| | localhost_access_log. <yyyy-mm-dd >.txt | Tomcat run log file |
| | manager <yyyy-mm-dd >.log | Tomcat run log file |
| | localhost. <yyyy-mm-dd >.log | Tomcat run log file |
| Script log | postInstall.log | Loader installation script log file<br>Log file generated during the execution of the Loader installation script (**postInstall.sh**) |

| Log Type | Log File Name | Description |
| --- | --- | --- |
| | preStart.log | Pre-startup script log file of the Loader service During startup of the Loader service, a series of preparation operations are first performed (by executing **preStart.sh**), such as generating the keytab file. This log file records information about these operations |
| | loader_ctl.log | Log file generated when Loader executes the service start and stop script (**sqoop.sh**) |

## Log Level

**Table 1-70** describes the log levels provided by Loader. The priorities of log levels are ERROR, WARN, INFO, and DEBUG in descending order. Logs whose levels are higher than or equal to the specified level are printed. The number of printed logs decreases as the specified log level increases.

**Table 1-70** Log levels

| Level | Description |
| --- | --- |
| ERROR | Error information about the current event processing. |
| WARN | Exception information about the current event processing. |
| INFO | Normal running status information about the system and events. |
| DEBUG | System information and system debugging information. |

To modify log levels, perform the following operations:

**Step 1** Go to the **All Configurations** page of Loader by referring to **Modifying Cluster Service Configuration Parameters**.

**Step 2** On the menu bar on the left, select the log menu of the target role.

**Step 3** Select a desired log level.

**Step 4** Save the configuration. In the dialog box that is displayed, click **OK**. Then restart the service for the configuration to take effect.

**----End**

## Log Formats

The following table lists the Loader log formats.

**Table 1-71** Log formats

| Log Type | Format | Example |
| --- | --- | --- |
| Run log | <yyyy-MM-dd HH:mm:ss,SSS>\|<Log Level>\|<Thread that generates the log>\|<Message in the log>\|<Location of the log event> | 2015-06-29 14:54:35,553 \| INFO \| [localhost-startStop-1] \| ConnectionRequestHandler initialized \| org.apache.sqoop.handler.ConnectionRequestHandler.<init>(ConnectionRequestHandler.java:100) |
| Audit log | <yyyy-MM-dd HH:mm:ss,SSS>\|<Log Level>\|default\|<Message in the log>\|<Location of the log event> | 2015-06-29 15:35:40,969 INFO default: UserName=admin, UserIP=10.52.0.111, Time=2015-06-29 15:35:40,969, Operation=submit, Resource=submission@21, Result=Failure, Detail={[reason:GET_SFTP_SESSION_FAILED:Failed to get sftp session - 10.162.0.35 (caused by: Auth cancel) ]; [config:null]} |

# 1.3.24 Introduction to MapReduce Logs

## Log Description

**Log paths:**

- JobhistoryServer: **/var/log/Bigdata/mapreduce/jobhistory** (run log) and **/var/log/Bigdata/audit/mapreduce/jobhistory** (audit log)
- Container: **/srv/BigData/hadoop/data1/nm/containerlogs/application_${appid}/container_{$contid}**

**Log archive rule**:

The automatic compression and archive function is enabled for MapReduce logs. By default, a log file is automatically compressed when the size of the log file is greater than 50 MB. The name of the compressed log file is in the following format: *<Name of the original log>-<yyyy-mm-dd_hh-mm-ss>.[NO.]***.log.zip**. A maximum of 100 latest compressed files are reserved. The number of compressed files can be configured on the parameter configuration page.

In MapReduce, JobhistoryServer cleans the old log files stored in HDFS periodically. The default storage directory is **/mr-history/done**. **mapreduce.jobhistory.max-age-ms** is used to set the cleanup interval. The default value of this parameter is 1,296,000,000 ms, which indicates 15 days.

**Table 1-72** MapReduce log list

| Type | Name | Description |
| --- | --- | --- |
| Run log | jhs-daemon-start-stop.log | Startup log file of the daemon process |
| | hadoop-<SSH_USER>-jhshadaemon-<hostname>.log | Run log file of the daemon process |
| | hadoop-<SSH_USER>-<process_name>-<hostname>.out | Log that records the MapReduce running environment information |
| | historyserver-<SSH_USER>-<DATE>-<PID>-gc.log | Log that records the garbage collection of the MapReduce service |
| | jhs-haCheck.log | Log that records the active and standby status of MapReduce instances |
| | yarn-start-stop.log | Log that records the startup and stop of the MapReduce service |
| | yarn-prestart.log | Log that records cluster operations before the MapReduce service startup |
| | yarn-postinstall.log | Work log before the MapReduce service startup and after the installation |
| | yarn-cleanup.log | Log that records the cleanup logs about the uninstallation of the MapReduce service |

| Type | Name | Description |
| --- | --- | --- |
| | mapred-service-check.log | Log that records the health check details of the MapReduce service |
| | container_{$contid} | Container log |
| | hadoop-<SSH_USER>-<process_name>-<hostname>.log | MR run log |
| | mapred-switch-jhs.log | MR active/standby switchover log |
| | env.log | Environment information log before the instance is started or stopped |
| Audit log | mapred-audit-jobhistory.log | MapReduce operation audit log |
| | SecurityAuth.audit | MapReduce security audit log |

## Log Level

Table 1-73 describes the log levels supported by MapReduce. The log levels are FATAL, ERROR, WARN, INFO, and DEBUG from high priority to low. Logs whose levels are higher than or equal to the specified level are printed. The number of printed logs decreases as the specified log level increases.

**Table 1-73** Log level

| Level | Description |
| --- | --- |
| FATAL | Logs of this level record critical error information about the current event processing. |
| ERROR | Logs of this level record error information about the current event processing. |
| WARN | Logs of this level record unexpected alarm information about the current event processing. |
| INFO | Logs of this level record normal running status information about the system and events. |
| DEBUG | Logs of this level record the system information and system debugging information. |

To modify log levels, perform the following operations:

**Step 1** Go to the **All Configurations** page of the MapReduce service. For details, see **Modifying Cluster Service Configuration Parameters**.

**Step 2** On the left menu bar, select the log menu of the target role.

**Step 3** Select a desired log level.

**Step 4** Save the configuration. In the displayed dialog box, click **OK** to make the configurations take effect.

NOTE

The configurations take effect immediately without restarting the service.

**----End**

## Log Format

The following table lists the MapReduce log formats.

**Table 1-74** Log format

| Type | Format | Example |
| --- | --- | --- |
| Run log | *<yyyy-MM-dd HH:mm:ss,SSS>*\|*<Log level>*\|*<Name of the thread that generates the log>*\|*<Message in the log>*\|*<Location where the log event occurs>* | 2020-01-26 14:18:59,109 \| INFO \| main \| Client environment:java.compiler=<NA> \| org.apache.zookeeper.Environment.logEnv(Environment.java:100) |
| Audit log | *<yyyy-MM-dd HH:mm:ss,SSS>*\|*<Log level>*\|*<Name of the thread that generates the log>*\|*<Message in the log>*\|*<Location where the log event occurs>* | 2020-01-26 14:24:43,605 \| INFO \| main-EventThread \| USER=omm OPERATION=refreshAdminAcls TARGET=AdminService RESULT=SUCCESS \| org.apache.hadoop.yarn.server.resourcemanager.RMAuditLogger$LogLevel $6.printLog(RMAuditLogger.java:91) |

# 1.3.25 MemArtsCC Logs

## Description

**Log path**: **/var/log/Bigdata/memartscc**

**Archive rule**: Automatic compression and archive is enabled for MemArtsCC run logs. When the size of a log file exceeds 50 MB (the size is configurable), the log file is automatically compressed. The number of compressed files can be retained is configurable.

**Table 1-75** MemArtsCC logs

| Log Type | Log File Name | Description |
| --- | --- | --- |
| Run log | check-sidecar-instance.log | Sidecar health check log |
| | check-worker-instance.log | Worker health check log |
| | sidecarStartDetail.log | Sidecar startup log |
| | sidecarStopDetail.log | Sidecar stop log |
| | workerStartDetail.log | Worker startup log |
| | workerStopDetail.log | Worker stop log |
| Worker log | **cc-worker-console.***Log generation time* | Worker startup log |
| | **ccworker.***Log level.Log generation time* | Worker run log |
| Sidecar log | cc-sidecar-zk.log | ZooKeeper operation log of sidecar |
| | cc-sidecar-bg-task.log | Sidecar backend task log |
| | cc-sidecar-cli.log | Sidecar command execution log |
| | cc-sidecar.log | Sidecar run log |

## Log levels

Table 2 describes the log levels provided by MemArtsCC.

The log levels are ERROR, WARN, INFO, and DEBUG in descending order of priority. Only logs whose levels are higher than or equal to the specified level are recorded. The higher the log level specified, the fewer the logs are recorded.

**Table 1-76** Log levels

| Level | Description |
| --- | --- |
| ERROR | Logs of this level record error information about system running |
| WARN | Logs of this level record exception information about the current event processing |
| INFO | Logs of this level record normal running status information about the system and events |

| Level | Description |
| --- | --- |
| DEBUG | Logs of this level record the system information and system debugging information |

To modify log levels, perform the following operations:

**Step 1** Log in to FusionInsight Manager.

**Step 2** Choose **Cluster** > **Services** > **MemArtsCC**. Click **Configurations** and then **All Configurations**.

**Step 3** On the menu bar on the left, select the log menu of the target role.

**Step 4** Select a desired log level.

**Step 5** Click **Save**. In the displayed dialog box, click **OK** to save the configuration.

**Step 6** Click **Instances**, select all CCSideCar instances, and choose **More** > **Restart Instance**.

NOTE

Upon completing the configuration, a restart of CCSideCar is necessary. There is no need to restart CCWorker.

**----End**

# 1.3.26 Introduction to MOTService Logs

## Log Description

**Log path**:

/var/log/Bigdata/motservice

**Log archiving rules**:

Log archiving rules use the FixedWindowRollingPolicy policy. The maximum size of a single file and the maximum number of log archive files can be configured. The rules are as follows:

- When the size of a single file exceeds the default maximum value, a new compressed archive file is generated. The naming rule of the compressed archive log file is as follows: *<Original log name>.[ID]***.log.gz**.
- When the number of log archive files reaches the maximum value, the earliest log file is deleted.
- By default, the maximum size of a single audit log file or run log file is 20 MB, and the maximum number of archived log files is 20.
- HA run logs are archived every 12 hours by default, and the maximum number of archived log files is 32.

**Table 1-77** MOTService log list

| Log Type | Log File Name | Description |
| --- | --- | --- |
| Run log | scriptlog/checkHaStatus.log | HA check log file |
| | scriptlog/cleanupMOTService.log | MOTService uninstallation log (MOTService uninstallation required) |
| | scriptlog/database_readonly_alarm.log | Alarm log generated when MOTService is in the read-only state |
| | scriptlog/install.log | Installation log |
| | scriptlog/motserver_switchover.log | MOTServer active/standby switchover log (active/standby switchover required) |
| | scriptlog/preStartMOTService.log | MOTService prestart log |
| | scriptlog/start_motserver.log | MOTServer startup log |
| | scriptlog/stop_motserver.log | MOTServer stop log |
| | scriptlog/backup_motserver.log | MOTServier backup and restoration log |
| HA script run log | ha/runlog/ha.log | MOTService HA process log |
| | ha/scriptlog/gaussDB_ha.log | MOTService HA check log |
| | ha/scriptlog/ha.log | HA script run log |
| | ha/scriptlog/ha_monitor.log | Run log of the MOTService ha_monitor process |
| | ha/scriptlog/ha_ssl_cert_detail.log | HA certificate operation log |
| | ha/scriptlog/send_alarm.log | Alarm log |
| | ha/scriptlog/haCertStatus.log | HA certificate status check log |
| | ha/scriptlog/floatip_ha.log | Floating IP address status check log |
| Health check log | healthCheck/motservice_processCheck.log | MOTService process check log |

| Log Type | Log File Name | Description |
| --- | --- | --- |
| | healthCheck/motservice_serviceCheck.log | MOTService health check log |
| Monitoring log | monitor/motservice_metric_collect.log | MOTService metric collection log |
| DB | DB/omm/pg_log/dn_*xxx*/postgresql-*.log | Main run log of the MOTService database |
| | DB/omm/bin | Folder that stores execution logs of client tools, such as gs_ctl and gs_guc |
| | DB/omm/asp_data | Folder that stores persistent metric sampling records of active sessions |
| | DB/omm/pg_audit | MOTService audit log folder |
| | DB/omm/om/gs_install-*.log | MOTService installation log |
| | DB/omm/om/gs_preinstall-*.log | MOTService preinstallation log |
| | DB/omm/om/gs_om-*.log | gs_om execution log |
| | DB/omm/om/gs_local-*.log | All local logs related to installation, preinstallation, and gs_om |
| | DB/omm/gs_profile | Performance log, which can be used to analyze database performance problems |
| logman | logman/logman.log | Backup management log of run logs such as postgresql.log |

### Log levels

Table 1-78 describes the log levels provided by MOTService.

Levels of run logs are **error**, **warning**, **notice**, **info**, and **debug** from the highest to the lowest priority. Run logs of equal or higher levels are recorded. The higher the specified log level, the fewer the logs recorded.

**Table 1-78** Log levels

| Log Type | Level | Description |
| --- | --- | --- |
| Run log | error | Error information about system running |

| Log Type | Level | Description |
| --- | --- | --- |
| | warning | Exception information about the current event processing |
| | notice | Trace information about the current event processing |
| | info | Normal running status of the system and events |
| | debug | System and debugging information |

To change log levels, perform the following operations:

1. Log in to FusionInsight Manager.
2. Choose **Cluster** > **Services** > **MOTService**. Click **Configurations** then **All Configurations**.
3. On the menu bar on the left, select the log menu of the target role.
4. Select a desired log level.
5. Click **Save**. In the **Save Configuration** dialog box displayed, click **OK**.

**Log format**

The MOTService log format is as follows:

**Table 1-79** Log format

| Log Type | Format | Example Value |
| --- | --- | --- |
| Run log | [*<yyyy-MM-dd HH:mm:ss>*] *<Log level>* [*<Name of the script that generates the log:Line number>*] *<Message in the log>* | [2022-08-29 10:51:18] INFO [prestart-motserver.sh:390] Finished to get config info success. (getConfig) |

# 1.3.27 Oozie Log Overview

## Log Description

**Log path**: The default storage paths of Oozie log files are as follows:

- Run log: **/var/log/Bigdata/oozie**
- Audit log: **/var/log/Bigdata/audit/oozie**

**Log archiving rule**: Oozie logs are classified into run logs, script logs, and audit logs. The maximum size of a run log file is 20 MB, and a maximum of 20 run log files can be reserved. The maximum size of an audit log file is 20 MB, and a maximum of 20 audit log files can be reserved.

**Table 1-80** Oozie log list

| Log Type | Log File Name | Description |
| --- | --- | --- |
| Run log | jetty.log | Oozie built-in jetty server log file, which is used to process the request and response information of OozieServlet |
| | jetty.out | Oozie process startup log file |
| | oozie_db_temp.log | Oozie database connection log |
| | oozie-instrumentation.log | Oozie dashboard log file, which records the Oozie running status and configuration information of each component |
| | oozie-jpa.log | openJPa run log file |
| | oozie.log | Oozie run log file |
| | oozie-<SSH_USER>-<DATE>-<PID>-gc.log.0.current | Log file that records the garbage collection of the Oozie service |
| | oozie-ops.log | Oozie operation log file |
| | check-serviceDetail.log | Oozie health check logs |
| | oozie-error.log | Oozie running error logs |
| | threadDump-<DATE>.log | Log file that records stack information when the service process exits normally |
| Script logs | postinstallDetail.log | Work log file generated after the installation and before the startup |
| | prestartDetail.log | Pre-startup log file |
| | startDetail.log | Service startup log file |
| | stopDetail.log | Service stop log file |
| | upload-sharelib.log | Operation logs uploaded by **sharelib** |
| Audit log | oozie-audit.log | Audit log |

## Log Level

**Table 1-81** describes the log levels provided by Oozie.

The priorities of log levels are ERROR, WARN, INFO, and DEBUG in descending order. Logs whose levels are higher than or equal to the set level are printed. The number of printed logs decreases as the configured log level increases.

**Table 1-81** Log levels

| Level | Description |
| --- | --- |
| ERROR | Logs of this level record abnormal information about events that cause process exceptions. |
| WARN | Logs of this level record exception information about the current event processing. |
| INFO | Logs of this level record normal running status information about the system and events. |
| DEBUG | Logs of this level record system information and information about database underlying data transmission. |

To modify log levels, perform the following operations:

**Step 1** Log in to FusionInsight Manager.

**Step 2** Choose **Cluster** > **Services** > **Oozie** and click **Configurations**.

**Step 3** Select **All Configurations**.

**Step 4** On the menu bar on the left, select the log menu of the target role.

**Step 5** Select a desired log level.

**Step 6** Click **Save**, and then click **OK**. The settings take effect after the processing is complete.

**----End**

## Log Formats

The following table lists the Oozie log formats.

**Table 1-82** Log formats

| Log Type | Format | Example |
| --- | --- | --- |
| Run log | *<yyyy-MM-dd HH:mm:ss,SSS><Log level><Location where the log event occurs><Log level><Message in the log>* | 2015-05-29 21:01:45,268 INFO StatusTransitService$StatusTransitRunnable:539 - USER[-] GROUP[-] Released lock for [org.apache.oozie.service.StatusTransitService] |
| Script logs | *<yyyy-MM-dd HH:mm:ss,SSS><Host name > <Log level > <Message in the log>* | 2015-06-01 17:18:03 001 suse11-192-168-0-111 oozie INFO Running oozie service check script |

| Log Type | Format | Example |
| --- | --- | --- |
| Audit log | *<yyyy-MM-dd HH:mm:ss,SSS>|<Log Level>|< Thread name > | Message in the log | Location where the log event occurs* | 2015-06-01 22:38:41,323 \| INFO \| http-bio-21003-exec-8 \| IP [192.168.0.111] USER [null], GROUP [null], APP [null], JOBID [null], OPERATION [null], PARAMETER [null], RESULT [SUCCESS], HTTPCODE [200], ERRORCODE [null], ERRORMESSAGE [null] \| org.apache.oozie.util.XLog.log(XLog.java:539) |

# 1.3.28 Ranger Log Overview

## Log Description

**Log path**: The default storage path of Ranger logs is **/var/log/Bigdata/ranger/***Role name*.

- RangerAdmin: /var/log/Bigdata/ranger/rangeradmin (run logs); /var/log/Bigdata/audit/ranger/rangeradmin (audit logs)
- TagSync: /var/log/Bigdata/ranger/tagsync (run logs)
- UserSync: /var/log/Bigdata/ranger/usersync (run logs)
- RangerKMS: /var/log/Bigdata/ranger/rangerkms (run logs)
- PolicySync: /var/log/Bigdata/ranger/policysync (run logs)

**Log archive rule**: The automatic compression and archive function is enabled for Ranger logs. By default, when the size of a log file exceeds 20 MB, the log file is automatically compressed. The naming rule of the compressed log file is as follows: *<Original log file name>-<yyyy-mm-dd_hh-mm-ss>.[ID]***.log.zip**. A maximum of 20 compressed files are retained.

**Table 1-83** Ranger log list

| Type | Name | Description |
| --- | --- | --- |
| RangerAdmin run log file | access_log.*<DATE>*.log | Tomcat access log |
| | catalina.out | Tomcat service run log |
| | gc-worker-pid*<PID>*-*<Date>*.log.*<ID>* | RangerAdmin garbage collection (GC) log |
| | postinstallDetail.log | Work log generated after an instance is started before installation |
| | prestartDetail.log | Log that records preparations before instance startup |

| Type | Name | Description |
| --- | --- | --- |
| | ranger-admin.log | RangerAdmin run log |
| | ranger_admin_sql.log | RangerAdmin log used to retrieve DBService |
| | startDetail.log | Instance startup log |
| TagSync run log | cleanupDetail.log | Instance clearing log |
| | gc-worker-pid*<PID>*-*<Date>*.log.*<ID>* | GC log file of an instance |
| | postinstallDetail.log | Work log generated after an instance is started before installation |
| | prestartDetail.log | Log that records preparations before instance startup |
| | ranger-tagsync.log | TagSync run log |
| | startDetail.log | Instance startup log |
| | tagsync.out | TagSync run log |
| UserSync run log | auth.log | UnixAuth service run log |
| | cleanupDetail.log | Instance clearing log |
| | gc-worker-pid*<PID>*-*<Date>*.log.*<ID>* | GC log file of an instance |
| | postinstallDetail.log | Work log generated after an instance is started before installation |
| | prestartDetail.log | Log that records preparations before instance startup |
| | ranger-usersync.log | UserSync run log |
| | startDetail.log | Instance startup log |
| RangerKMS run log | access-<host>-*<DATE>*.log | Tomcat access log |
| | threadDump-*<DATE>*.log | JVM GC log of the process |
| | stopDetail.log | Instance stopping log |
| | startDetail.log | Instance startup log |
| | ranger-kms.log | Instance run log |

| Type | Name | Description |
| --- | --- | --- |
| | prestartDetail.log | Log that records preparations before instance startup |
| | catalina.out | Tomcat service run log |
| | postinstallDetail.log | Work log generated after an instance is started before installation |
| PolicySync run log | cleanupDetail.log | Instance clearing log |
| | policysync.out | Instance run log |
| | postinstallDetail.log | Work log generated after an instance is started before installation |
| | prestartDetail.log | Log that records preparations before instance startup |
| | ranger-policysync.log | Instance run log |
| | startDetail.log | Instance startup log |
| | gc-worker-pid*<PID>*-*<Date>*.log.*<ID>* | GC log file of an instance |
| | stopDetail.log | Instance stopping log |
| Audit log | rangeradmin-audit.log | RangerAdmin audit log |

## Log Levels

Table 1-84 describes the log levels provided by Ranger. The priorities of log levels are FATAL, ERROR, WARN, INFO, and DEBUG in descending order. Logs whose levels are higher than or equal to the specified level are printed. The number of printed logs decreases as the specified log level increases.

**Table 1-84** Log levels

| Level | Description |
| --- | --- |
| FATAL | Logs of this level record fatal error information about the current event processing that may result in a system crash. |
| ERROR | Logs of this level record error information about the current event processing, which indicates that system running is abnormal. |

| Level | Description |
| --- | --- |
| WARN | Logs of this level record abnormal information about the current event processing. These abnormalities will not result in system faults. |
| INFO | Logs of this level record normal running status information about the system and events. |
| DEBUG | Logs of this level record the system information and system debugging information. |

To modify log levels, perform the following operations:

**Step 1** Log in to FusionInsight Manager.

**Step 2** Choose **Cluster** > **Services** > **Ranger** > **Configurations**.

**Step 3** Select **All Configurations**.

**Step 4** On the menu bar on the left, select the log menu of the target role.

**Step 5** Select a desired log level.

**Step 6** Click **Save**. In the displayed dialog box, click **OK** to make the configuration take effect.

NOTE

The configurations take effect immediately without the need to restart the service.

**----End**

## Log Formats

The following table lists the Ranger log formats.

**Table 1-85** Log formats

| Type | Format | Example Value |
| --- | --- | --- |
| Run log | *<yyyy-MM-dd HH:mm:ss,SSS>*\|*<Log level>*\|*<Name of the thread that generates the log>*\|*<Message in the log>*\|*<Location where the log event occurs>* | 2020-04-29 20:09:28,543 \| INFO \| http-bio-21401-exec-56 \| Request comes from API call, skip cas filter. \| CasAuthenticationFilter-Wrapper.java:25 |

# 1.3.29 Redis Log Overview

## Log Description

**Log path**

- Default path of Redis logs: **/var/log/Bigdata/redis/role name**
- Default path of Redis-Data-Sync logs: **/var/log/Bigdata/redis/tomcat**
- Path of HTTPS request access logs: **/var/log/Bigdata/redis/catalina**

**Log archive rule**: The automatic compression and archive function is enabled for Redis logs. By default, when the size of a log file exceeds 10 MB, the log file is automatically compressed. The naming rule of the compressed log file is as follows: *<Original log name>.<yyyy-mm-dd_hh-mm-ss>***.log.tar.gz**. The compressed log files are stored in the same directory as the original log files. A maximum of 20 latest compressed log files can be stored.

**Table 1-86** Redis log list

| Type | Name | Description |
| --- | --- | --- |
| Redis process run log | redis.log | Run log file of the main Redis process. |
| | redis_bg.log | Redis log file to start background threads. This log is recorded when bgsave is executed. |
| Script log | prestartDetail.log | Log file generated before the Redis Server is started. |
| | redis_cleanup.log | Log file that records the uninstallation or clearance of the Redis service. |
| | redis_install.log | Redis installation log file. |
| | redis_start.log | Logs that record the latest startup of the Redis process. |
| | redis_stop.log | Log file that records the latest shutdown of the Redis process. |
| Redis cluster management log | web_redis.log | redis-ws run log, which is stored in **/var/log/Bigdata/redis/tomcat/redis** by default |
| | redisweb_audit.log | Audit logs of Redis cluster creation, scale-out, scale-in, and deletion |
| Redis-Data-Sync logs | rds_start.log | Logs that record the latest startup of the Redis-Data-Sync instance. |

| Type | Name | Description |
| --- | --- | --- |
| | rds_stop.log | Logs that record the latest shutdown of the Redis-Data-Sync instance. |
| | redis-data-sync.log | Run logs of the Redis-Data-Sync instance. |
| | redis_install.log | Logs that record Redis-Data-Sync instance installation. |
| | redis_cleanup.log | Logs that record the uninstallation or clearance of the Redis-Data-Sync instance. |
| | redis-data-sync-*username*--pid*xxxx*-gc.log.*x*.current | GC logs. |
| | catalina.out | Tomcat Catalina standard output logs |
| | catalina.*Y-M-D*.log | Catalina logs. |
| | manager.*Y-M-D*.log | Tomcat management logs. |
| | host-manager.*Y-M-D*.log | Logs of virtual Tomcat hosts. |
| | localhost_access_log..*Y-M-D*.txt | HTTPS request access logs. |
| | rds_instance_check.log | Health check log of the Redis-Data-Sync instance |
| | redisDataSyncThread-Dump*.log | Redis-Data-Sync instance stack information |

## Log levels

**Table 1-87** describes the log levels provided by Redis.

Levels of Redis process run logs are warning, notice, verbose, and debug from the highest to the lowest priority. Run logs of equal or higher levels are recorded. The higher the specified log level, the fewer the logs recorded.

The script log levels are ERROR, WARN, INFO, and DEBUG.

Redis cluster management logs: ERROR, WARN, INFO, and DEBUG.

Redis-Data-Sync logs: ERROR, WARN, INFO, and DEBUG.

**Table 1-87** Log levels

| Log Type | Level | Description |
| --- | --- | --- |
| Run logs | warning | Logs of this level record only important information. |
| | notice | Logs of this level record suitable details and are applicable to the production environment. |
| | verbose | Logs of this level record normal running status information about the system and events. |
| | debug | Logs of this level record system running and debugging information. |
| Script logs | ERROR | Logs of this level record error information about system running. |
| | WARN | Exception information about the current event processing |
| | INFO | Logs of this level record normal running status information about the system and events. |
| | DEBUG | Logs of this level record the system information and system debugging information. |
| Redis cluster management log | ERROR | Logs of this level record error information about system running. |
| | WARN | Exception information about the current event processing |
| | INFO | Normal running status information about the system and events. |
| | DEBUG | Logs of this level record the system information and system debugging information. |
| Redis-Data-Sync logs | ERROR | Logs of this level record error information about system running. |
| | WARN | Exception information about the current event processing |
| | INFO | Normal running status information about the system and events. |
| | DEBUG | Logs of this level record the system information and system debugging information. |

To change the run log level of the Redis process, perform the following operations:

**Step 1** Log in to FusionInsight Manager.

**Step 2** Choose **Cluster** > Name of the target cluster and click the **Configurations** tab and then **All Configurations**.

**Step 3** In the navigation pane on the left, choose the *target role* > **Customization** and change the name of **redis.customized.configs** to **loglevel** and the value to the required log level.

**Step 4** Click **Save**. In the displayed dialog box, click **OK**.

**Step 5** Click **Dashboard**, choose **More**, and select **Restart Service** in the upper-right corner to restart the Redis service.

**----End**

## Log Format

The Redis log format is as follows:

**Table 1-88** Log Format

| Log Type | Format | Example |
| --- | --- | --- |
| Run logs | *[yyyy-MM-dd HH:mm:ss] [Process PID] [Role of the Redis process] [Log level] <Log message>[Location where the log event occurs]* | [2019-03-13 17:04:28][014769][M] [notice] The server is now ready to accept connections on port 22400[redis.c:3722] |
| Script logs | *[yyyy-MM-dd HH:mm:ss] <Log level <Log details > [Location where the log event occurs] (Process ID)* | [2019-03-17 09:41:16] INFO Start redis instance success. [175(redis-start.sh)](20469) |
| Redis cluster management log | yyyy-MM-dd HH:mm:ss \| Log level \| Current thread \| Log details \| Log generation location | 2020-07-17 15:53:26,416 \| INFO \| localhost-startStop-1 \| Begin to check redis status. \| com.huawei.redis.om.controller.RedisController.<clinit>(RedisController.java:78) |
| Redis-Data-Sync logs | yyyy-MM-dd HH:mm:ss \| Log level \| Current thread \| Log generation location \| Log details | 2021-09-22 16:58:34.736\|INFO \| localhost-startStop-1\| ConfigurationManager.java:73\| ConfigurationManager initConf start |

Redis process roles include **X**, **C**, **M**, and **S**. **X** indicates Sentinel. **C** indicates a subprocess written by AOF. **M** indicates the master role in the Redis cluster. **S** indicates a slave role in the Redis cluster.

# 1.3.30 RTDService Logs

## Log Description

**Default paths of RTD log files:**

- Path for storing RTDService operation logs and RTDPortal logs: **/var/log/Bigdata/rtd/rtdservice**
- Path for storing RTDService installation logs: **/var/log/Bigdata/rtd/rtdservice/script**

**Log archive rule**: The automatic compression and archive function is enabled for RTD logs. By default, RTD logs are automatically compressed every day into a package named in the format of *Original log file name*-*yyyy-mm-dd_hh-mm-ss*.*ID*.**.log.zip**. By default, the latest 10 compressed files are retained every day. You can set the **appender.all.strategy.max** parameter on FusionInsight Manager to specify the number of compressed files you want to retain.

**Table 1-89** RTD log files

| Log Type | Log File | Description |
| --- | --- | --- |
| RTDService operation log | RTDService.log | Run logs of RTDService |
| | RTDService_error.log | Error log of RTDService |
| | RTDService_audit.log | Audit log of RTDService |
| RTDService installation log | cleanup.log | RTDService uninstallation log |
| | checkHaStatus.log | HA check log |
| | checkinstall.log | Installation and scale-out check log |
| | checknode.log | Health check log of RTDServer instances |
| | postinstall.log | Installation and scale-out log |
| | prestart.log | RTDService prestart log |
| | start.log | RTDService boot log |
| | stop.log | RTDService stop log |
| RTDPortal log | RTDportal.log | Run log of RTDPortal |
| | RTDportal_error.log | Error log of RTDPortal |

## Log Levels

**Table 1-90** describes the log levels supported by RTDService.

The priorities of run log levels are FATAL, ERROR, WARN, INFO, and DEBUG in descending order. Logs whose levels are higher than or equal to a specified level are displayed. The number of displayed log records decreases as the specified log level increases.

**Table 1-90** Log levels

| Level | Description |
| --- | --- |
| FATAL | Logs of this level record fatal error information about the current event processing that may result in a system crash. |
| ERROR | Logs of this level record error information about the current event processing, which indicates that system running is abnormal. |
| WARN | Logs of this level record abnormal information about the current event processing. These abnormalities will not result in system faults. |
| INFO | Logs of this level record normal running status information about the system and events |
| DEBUG | Logs of this level record the system information and system debugging information |

To change log levels, perform the following operations:

1. Log in to Manager.
2. Choose **Cluster** > **Services** > **RTDService**. Click **Configurations** then **All Configurations**.
3. On the menu bar on the left, select the log menu of the target role.
4. Select a desired log level.
5. Click **Save**. In the displayed dialog box, click **OK** to make the configuration take effect.

## Log Formats

The format of RTDService run logs is as follows:

**Table 1-91** Log formats

| Component | Format | Example |
| --- | --- | --- |
| RTDService | <yyyy-MM-dd HH:mm:ss,SSS>\|<LogLevel>\|<*Name of the thread that generates the log*>\|<*Location where the log event occurs*>\|<message&gt in log; | 2015-10-27 08:51:18,477 DEBUG [http-bio-160.136.0.200-21820-exec-630] common.RestResponseBuilder:61 - {"resultCode":0,"resultMessage":null,"result":{"status":"RUNNING","version":"v1.0"}} |

# 1.3.31 Solr Log Overview

## Log Description

**Log path**: The default storage path of Solr log files is **/var/log/Bigdata/solr/***Role name*.

- SolrServerAdmin:
  - **/var/log/Bigdata/solr/SolrServerAdmin** (run logs)
  - **/var/log/Bigdata/solr/SolrHAServer** (run logs)
  - **/var/log/Bigdata/audit/solr/SolrServerAdmin** (audit logs)
- SolrServer1:
  - **/var/log/Bigdata/solr/SolrServer1** (run logs)
  - **/var/log/Bigdata/audit/solr/SolrServer1** (audit logs)
- SolrServer2:
  - **/var/log/Bigdata/solr/SolrServer2** (run logs)
  - **/var/log/Bigdata/audit/solr/SolrServer2** (audit logs)
- SolrServer3:
  - **/var/log/Bigdata/solr/SolrServer3** (run logs)
  - **/var/log/Bigdata/audit/solr/SolrServer3** (audit logs)
- SolrServer4:
  - **/var/log/Bigdata/solr/SolrServer4** (run logs)
  - **/var/log/Bigdata/audit/solr/SolrServer4** (audit logs)
- SolrServer5:
  - **/var/log/Bigdata/solr/SolrServer5** (run logs)
  - **/var/log/Bigdata/audit/solr/SolrServer5** (audit logs)
- HbaseIndexer:
  - **/var/log/Bigdata/solr/HBaseIndexer** (run logs)

**Log archive rule**: The automatic Solr log compression function is enabled. By default, when the size of logs exceeds 5 MB, logs are automatically compressed into a log file named in the following format: *<Original log file name>-<yyyy-mm-*

*dd_hh-mm-ss>.[ID]*.**log.zip**. A maximum of 20 latest compressed files are reserved. The number of compressed files can be configured on the Manager portal.

**Table 1-92** Solr log list

| Log Type | Name | Description |
| --- | --- | --- |
| Run logs | solr-<hostname>.log | Solr system log file, which records most logs generated when the Solr system is running |
| | SolrServer1~5/solr-process-check.log<br>SolrServerAdmin/solr-process-check.log | Solr process check log file |
| | solr-service-check.log | Solr service check log file |
| | SolrServer1~5/solr-startup.log<br>SolrServeAdmin/solr-startup.log | Solr startup log file |
| | SolrServer1~5/solr-stop.log<br>SolrServerAdmin/solr-stop.log | Solr stop log file |
| | SolrServer1~5/solr-<date>_gc.log.<index><br>SolrServerAdmin/solr-<date>_gc.log.<index> | GC log file of the SolrServer instance |
| | solrhaserverDetail.log | Log file that records the startup and stop status check of Solr HA |
| | SolrServer1~5/postinstallDetail.log<br>SolrServerAdmin/postinstallDetail.log | Work log file generated after the Solr service installation and before the Solr service startup |
| | SolrServer1~5/prestartDetail.log<br>SolrServerAdmin~5/prestartDetail.log | Log file that records the preparation before the startup of the Solr service |
| | SolrServer1~5/solr-catalina-<hostname>.log<br>SolrServerAdmin/solr-catalina-<hostname>.log | Catalina engine startup log file |
| | SolrServer1~5/solr-catalina-<hostname>.out<br>SolrServerAdmin/solr-catalina-<hostname>.out | Log that records the environment information required for Catalina engine startup |

| Log Type | Name | Description |
| --- | --- | --- |
| | SolrServer1~5/solr-threadDump-<date>.log<br>SolrServerAdmin/solr-threadDump-<date>.log | Solr instance stack log |
| | ha.log | HA run log |
| | rs-floatip.log | Log file that records the floating IP address configuration |
| | rs-sendAlarm.log | Log file that records HA alarms |
| | ha_monitor.log | HA monitoring log file |
| | hbaseindexer.out | Log that records the running environment information of the HBaseIndexer service |
| | hbaseindexer-service-check.log | HBaseIndexer service check log |
| | HBaseIndexer-threadDump-<date>.log | HBaseIndexer stack log |
| | hbaseindexer-omm-<hostname>.log | HBaseIndexer system log file that records most of the logs generated when HBaseIndexer is running |
| | hbaseindexer-omm-<date>-gc.log.<index> | GC log file of the HBaseIndexers instance |
| | HBaseIndexer/postinstallDetail.log | Work log file generated after the HBaseIndexer service installation and before the HBaseIndexer service startup |
| | HBaseIndexer/prestartDetail.log | Log file that records the preparation before the startup of the HBaseIndexer service |
| | HBaseIndexer/startDetail.log | HBaseIndexer startup log file |
| | HBaseIndexer/stopDetail.log | HBaseIndexer stop log file |
| Audit log | solr-audit-<hostname>.log | Audit log file that records the Solr operations (such as creating, deleting, modifying, and querying files) |

## Log levels

**Table 1-93** describes the log levels provided by Solr.

The priorities of log levels are FATAL, ERROR, WARN, INFO, and DEBUG in descending order. Logs whose levels are higher than or equal to the set level are

printed. The number of printed logs decreases as the configured log level increases.

**Table 1-93** Log levels

| Level | Description |
| --- | --- |
| FATAL | Logs of this level record all log information about the current event processing. |
| ERROR | Error information about the current event processing |
| WARN | Exception information about the current event processing |
| INFO | Logs of this level record normal running status information about the system and events. |
| DEBUG | Logs of this level record the system information and system debugging information. |

To modify log levels, perform the following operations:

**Step 1** Log in to Manager.

**Step 2** Choose **Cluster** > *Name of the desired cluster* > **Service** > **Solr** > **Configuration**.

**Step 3** Select **All Configurations**.

**Step 4** On the menu bar on the left, select the log menu of the target role.

**Step 5** Select a desired log level.

**Step 6** Click **Save**. In the displayed dialog box, click **OK** to make the configuration take effect.

**----End**

## Log Format

The Solr log formats are as follows:

**Table 1-94** Log Format

| Log Type | Format | Example |
| --- | --- | --- |
| Run logs | <*yyyy-MM-dd HH:mm:ss,SSS*>\|<*Log level*>\|<*Name of the thread that generates the log*>\|<*Message in the log*>\|<*Location where the log event occurs*> | 2016-02-18 21:31:24,227 \| INFO \| http-bio-192.168.0.227-21101-exec-9 \| [admin] webapp=null path=/admin/cores params={wt=json&_=1432906471360} status=0 QTime=3 \| org.apache.solr.servlet.SolrDispatchFilter.handleAdminRequest(SolrDispatchFilter.java:757) |
| Audit logs | <*yyyy-MM-dd HH:mm:ss,SSS*>\|<*Log level*>\|<*Name of the thread that generates the log*>\|<*Message in the log*>\|<*Location where the log event occurs*> | 2016-02-18 09:45:00,093 \| INFO \| http-nio-21101-exec-5 \| RemoteAddr=192.168.0.221:37976 UserName=admin ResourceType=Core Detail=wt=json&_=1458612365349 Result=Success \| com.huawei.solr.security.audit.AuditLogAppender.auditLogInfo(AuditLogAppender.java:20) |

# 1.3.32 Spark Log Overview

## Log Description

**Log paths:**

- Executor run log: **${BIGDATA_DATA_HOME}/hadoop/data${i}/nm/containerlogs/application_${appid}/container_{$contid}**

  NOTE

  The logs of running tasks are stored in the preceding path. After the running is complete, the system determines whether to aggregate the logs to an HDFS directory based on the Yarn configuration.

- Other logs: **/var/log/Bigdata/spark**

**Log archiving rule**:

- When tasks are submitted in **yarn-client** or **yarn-cluster** mode, executor log files are stored each time when the size of the log files reaches 50 MB. A maximum of 10 log files can be reserved without being compressed.
- By default, JobHistory log files are compressed and stored once when the file size reaches 100 MB. A maximum of 100 log files are retained.
- By default, JDBCServer log files are compressed and stored once when the file size reaches 100 MB. A maximum of 100 log files are retained.
- By default, IndexServer log files are compressed and stored once when the file size reaches 100 MB. A maximum of 100 log files are retained.

- By default, JDBCServer audit log files are compressed and stored once when the file size reaches 20 MB. A maximum of 20 log files are retained.
- The log file size and the number of compressed files to be reserved can be configured on FusionInsight Manager.

**Table 1-95** Spark log file list

| Log Type | Name | Description |
| --- | --- | --- |
| SparkResource log | spark.log | Spark initialization log |
| | prestart.log | Prestart script log |
| | cleanup.log | Cleanup log file for instance installation and uninstallation |
| | spark-availability-check.log | Spark health check log |
| | spark-service-check.log | Spark service check log |
| JDBCServer log | JDBCServer-start.log | JDBCServer startup log |
| | JDBCServer-stop.log | JDBCServer stop log |
| | JDBCServer.log | JDBCServer run log on the server |
| | jdbc-state-check.log | JDBCServer health check log |
| | jdbcserver-omm-pid***-gc.log.*.current | JDBCServer process GC log |
| | spark-omm-org.apache.spark.sql.hive.thriftserver.HiveThriftProxyServer2-***.out* | JDBCServer process startup log. If the process stops, the **jstack** information is printed. |
| JobHistory log | jobHistory-start.log | JobHistory startup log |
| | jobHistory-stop.log | JobHistory stop log |
| | JobHistory.log | JobHistory running process log |
| | jobhistory-omm-pid***-gc.log.*.current | JobHistory process GC log |
| | spark-omm-org.apache.spark.deploy.history.HistoryServer-***.out* | JobHistory process startup log If the process stops, the **jstack** information is printed. |
| IndexServer log | IndexServer-start.log | IndexServer startup log |
| | IndexServer-stop.log | IndexServer stop log |
| | IndexServer.log | IndexServer run log on the server |

| Log Type | Name | Description |
| --- | --- | --- |
| | indexserver-state-check.log | IndexServer health check log |
| | indexserver-omm-pid***-gc.log.*.current | IndexServer process GC log |
| | spark-omm-org.apache.spark.sql.hive.thriftserver.IndexServerProxy-***.out* | IndexServer process startup log. If the process stops, the **jstack** information is printed. |
| Audit Log | jdbcserver-audit.log<br>ranger-audit.log | JDBCServer audit log |
| queryInfo log | hdfs://hacluster/sparkHistory/yyyy-mm-dd/application_ID/query.log | SQL tasks submitted through **spark-sql** and **spark-beeline**, whose SQL running information is recorded in the queryInfo log file. |
| Native engine log | clickhouse-server.log | INFO log of the Native engine |
| | clickhouse-server.err.log | Error log of the Native engine |

## Log levels

**Table 1-96** describes the log levels provided by Spark. The priorities of log levels are ERROR, WARN, INFO, and DEBUG in descending order. Logs whose levels are higher than or equal to the specified level are printed. The number of printed logs decreases as the specified log level increases.

**Table 1-96** Log levels

| Level | Description |
| --- | --- |
| ERROR | Logs of this level record error information about the current event processing. |
| WARN | Logs of this level record exception information about the current event processing |
| INFO | Logs of this level record normal running status information about the system and events. |
| DEBUG | Logs of this level record the system information and system debugging information. |

To modify log levels, perform the following operations:

NOTE

By default, the service does not need to be restarted after the Spark log levels are configured.

**Step 1** Log in to FusionInsight Manager.

**Step 2** Choose **Cluster** > **Services** > **Spark** and click **Configurations**.

**Step 3** Select **All Configurations**.

**Step 4** On the menu bar on the left, select the log menu of the target role.

**Step 5** Select a desired log level.

**Step 6** Click **Save**. Then, click **OK**.

**----End**

## Log Format

**Table 1-97** Log Format

| Type | Format | Example |
| --- | --- | --- |
| Run log | <*yyyy-MM-dd HH:mm:ss,SSS*>\|<*Log level*>\|<*Name of the thread that generates the log*>\|<*Message in the log*>\|<*Location where the log event occurs*> | 2014-09-22 11:16:23,980 INFO DAGScheduler: Final stage: Stage 0(reduce at SparkPi.scala:35) |

# 1.3.33 Yarn Log Overview

## Log Description

The default paths for saving Yarn logs are as follows:

- ResourceManager: **/var/log/Bigdata/yarn/rm** (run logs) and **/var/log/Bigdata/audit/yarn/rm** (audit logs)
- NodeManager: **/var/log/Bigdata/yarn/nm** (run logs) and **/var/log/Bigdata/audit/yarn/nm** (audit logs)
- TimelineServer: **/var/log/Bigdata/yarn/tls** (run logs) and **/var/log/Bigdata/audit/yarn/tls** (audit logs)

Log archive rule: The automatic compression and archive function is enabled for Yarn logs. By default, when the size of a log file exceeds 50 MB, the log file is automatically compressed. The naming rule of the compressed log file is as follows: *<Original log file name>-<yyyy-mm-dd_hh-mm-ss>.[ID]***.log.zip**. A maximum of 100 latest compressed files are retained. The number of compressed files can be configured on Manager.

**Log archive rule**:

**Table 1-98** Yarn log list

| Log Type | Log File Name | Description |
| --- | --- | --- |
| Run log | hadoop-<SSH_USER>-<process_name>-<hostname>.log | Yarn component log file, which records most of the logs generated when the Yarn component is running |
| | hadoop-<SSH_USER>-<process_name>-<hostname>.out | Log file that records Yarn running environment information |
| | <process_name>-<SSH_USER>-<DATE>-<PID>-gc.log | Garbage collection log file |
| | yarn-haCheck.log | ResourceManager active/standby status detection log file |
| | yarn-service-check.log | Log file that records the health check details of the Yarn service |
| | yarn-start-stop.log | Log file that records the startup and stop of the Yarn service |
| | yarn-prestart.log | Log file that records cluster operations before the Yarn service startup |
| | yarn-postinstall.log | Work log file after installation and before startup of the Yarn service |
| | hadoop-commission.log | Yarn service entry log file |
| | yarn-cleanup.log | Log file that records the cleanup operation during uninstallation of the Yarn service |
| | yarn-refreshqueue.log | Yarn queue refresh log file |
| | upgradeDetail.log | Upgrade log file |
| | stderr/stdin/syslog | Container log file of the applications running on the Yarn service |
| | yarn-application-check.log | Check log file of applications running on the Yarn service |

| Log Type | Log File Name | Description |
| --- | --- | --- |
| | yarn-appsummary.log | Running result log file of applications running on the Yarn service |
| | yarn-switch-resourcemanager.log | Run log file that records the Yarn active/standby switchover |
| | yarn-az-state.log | AZ status log of Yarn |
| | yarn-az-disaster-exercise.log | AZ DR drill log of Yarn |
| | yarn-az-check.log | Yarn AZ check log file |
| | ranger-yarn-plugin-enable.log | Log file that records the enabling of Ranger authentication for Yarn |
| | yarn-nodemanager-period-check.log | Periodic check log of Yarn NodeManager |
| | yarn-resourcemanager-period-check.log | Periodic check log of Yarn ResourceManager |
| | hadoop.log | Hadoop client logs |
| | env.log | Environment information log file before the instance is started or stopped. |
| | tls-daemon-start-stop.log | YARN daemon startup and stop log |
| | tls-leveldb-sync.log | Log that records LevelDB synchronization between the active and standby TimelineServer nodes |
| | threadDump-<process_name>-<thread pid>-<timestamp>.log | Dump log generated when YARN is stopped |
| Audit logs | yarn-audit-<process_name>.log<br>ranger-plugin-audit.log | Yarn operation audit log file |
| | SecurityAuth.audit | Yarn security audit log file |

## Log Level

**Table 1-99** describes the log levels supported by Yarn, including OFF, FATAL, ERROR, WARN, INFO, and DEBUG, from high priority to low. Logs whose levels are higher than or equal to the specified level are printed. The number of printed logs decreases as the specified log level increases.

**Table 1-99** Log levels

| Level | Description |
| --- | --- |
| FATAL | Logs of this level record critical error information about the current event processing. |
| ERROR | Logs of this level record error information about the current event processing. |
| WARN | Logs of this level record exception information about the current event processing. |
| INFO | Logs of this level record normal running status information about the system and events. |
| DEBUG | Logs of this level record the system as well as system debugging information. |

To modify log levels, perform the following operations:

**Step 1** Go to the **All Configurations** page of the Yarn service by referring to **Modifying Cluster Service Configuration Parameters**.

**Step 2** On the menu bar on the left, select the log menu of the target role.

**Step 3** Select a desired log level.

**Step 4** Click **Save Configuration**. In the dialog box that is displayed, click **OK** to make the setting take effect.

NOTE

The configurations take effect immediately without the need to restart the service.

**----End**

## Log Format

The following table lists the Yarn log formats.

**Table 1-100** Log formats

| Log Type | Format | Example |
| --- | --- | --- |
| Run log | <yyyy-MM-dd HH:mm:ss,SSS>\|<Log Level>\|<*Thread that generates the log*>\|<*Message in the log*>\|<*Location of the log event*> | 2014-09-26 14:18:59,109 \| INFO \| main \| Client environment:java.compiler=<NA> \| org.apache.zookeeper.Environment.logEnv(Environment.java:100) |

| Log Type | Format | Example |
| --- | --- | --- |
| Audit log | <yyyy-MM-dd HH:mm:ss,SSS>\|<Log Level>\|<*Thread that generates the log*>\|<*Message in the log*>\|<*Location of the log event*> | 2014-09-26 14:24:43,605 \| INFO \| main-EventThread \| USER=omm OPERATION=refreshAdmin Acls TARGET=AdminService RESULT=SUCCESS \| org.apache.hadoop.yarn.server.resourcemanager.RMAuditLogger$LogLevel $6.printLog(RMAuditLogger.java:91) |

# 1.3.34 ZooKeeper Log Overview

## Log Description

**Log path**: **/var/log/Bigdata/zookeeper/quorumpeer** (Run log), **/var/log/Bigdata/audit/zookeeper/quorumpeer** (Audit log)

**Log archive rule**: The automatic ZooKeeper log compression function is enabled. By default, when the size of logs exceeds 30 MB, logs are automatically compressed into a log file. A maximum of 20 compressed files can be reserved. The number of compressed files can be configured on Manager.

**Table 1-101** ZooKeeper log list

| Log Type | Log File Name | Description |
| --- | --- | --- |
| Run logs | zookeeper-<SSH_USER>-<process_name>-<hostname>.log | ZooKeeper system log file, which records most of the logs generated when the ZooKeeper system is running. |
| | check-serviceDetail.log | Log that records whether the ZooKeeper service starts successfully. |
| | zookeeper-<SSH_USER>-<DATA>-<PID>-gc.log | ZooKeeper garbage collection log file |
| | instanceHealthDetail.log | Log that records the health check details of ZooKeeper instance |
| | zookeeper-omm-server-<hostname>.out | Log indicating that ZooKeeper unexpectedly quits |
| | zk-err-<zkpid>.log | ZooKeeper fatal error log |

| Log Type | Log File Name | Description |
| --- | --- | --- |
| | java_pid<zkpid>.hprof | ZooKeeper memory overflow log |
| | funcDetail.log | ZooKeeper instance startup log |
| | zookeeper-period-check.log | Health check log of the ZooKeeper instance |
| | zookeeper-period-check-java.log | ZooKeeper quota monitoring period check log |
| | threadDump-<process_name>-<thread pid>-<timestamp>.log | Dump log generated when ZooKeeper is stopped |
| Audit Log | zk-audit-quorumpeer.log | ZooKeeper operation audit log |

## Log levels

Table 1-102 describes the log levels supported by ZooKeeper. The priorities of log levels are FATAL, ERROR, WARN, INFO, and DEBUG in descending order. Logs whose levels are higher than or equal to the specified level are printed. The number of printed logs decreases as the specified log level increases.

**Table 1-102** Log levels

| Level | Description |
| --- | --- |
| FATAL | Logs of this level record fatal error information about the current event processing that may result in a system crash. |
| ERROR | Error information about the current event processing, which indicates that system running is abnormal. |
| WARN | Abnormal information about the current event processing. These abnormalities will not result in system faults. |
| INFO | Logs of this level record normal running status information about the system and events. |
| DEBUG | Logs of this level record the system information and system debugging information. |

To modify log levels, perform the following operations:

**Step 1** Go to the **All Configurations** page of the ZooKeeper service by referring to **Modifying Cluster Service Configuration Parameters**.

**Step 2** On the menu bar on the left, select the log menu of the target role.

**Step 3** Select a desired log level.

**Step 4** Click **Save**. In the displayed dialog box, click **OK** to make the configuration take effect.

NOTE

The configurations take effect immediately without the need to restart the service.

**----End**

## Log Format

The following table lists the ZooKeeper log formats.

**Table 1-103** Log Format

| Log Type | Component | Format | Example |
| --- | --- | --- | --- |
| Run logs | zookeeper<br>quorumpeer | <*yyyy-MM-dd HH:mm:ss,SSS*>\|<*Log level*>\|<*Name of the thread that generates the log*>\|<*Message in the log*>\|<*Location where the log event occurs*> | 2020-01-20 16:33:43,816 \| INFO \| main \| Defaulting to majority quorums \| org.apache.zookeeper.server.quorum.QuorumPeerConfig.parseProperties(QuorumPeerConfig.java:335) |
| Audit logs | zookeeper<br>quorumpeer | <*yyyy-MM-dd HH:mm:ss,SSS*>\|<*Log level*>\|<*Name of the thread that generates the log*>\|<*Message in the log*>\|<*Location where the log event occurs*> | 2020-01-20 16:33:54,313 \| INFO \| CommitProcessor:13 \| session=0xd4b0679daea0000 ip=10.177.112.145 operation=create znode target=ZooKeeperServer znode=/zk-write-test-2 result=success \| org.apache.zookeeper.ZKAuditLogger$LogLevel$5.printLog(ZKAuditLogger.java:70) |

# 1.4 Appendix

## 1.4.1 Modifying Cluster Service Configuration Parameters

Modify the configuration parameters of each service on FusionInsight Manager.

**Step 1** You have logged in to FusionInsight Manager.

**Step 2** Choose **Cluster** > *Name of the desired cluster* > **Service**.

**Step 3** Click the specified service name on the service management page.

**Step 4** Click **Configuration**.

The **Basic Configuration** tab page is displayed by default. To modify more parameters, click the **All Configurations** tab. The navigation tree displays all configuration parameters of the service. The level-1 nodes in the navigation tree are service names or role names. The parameter category is displayed after the level-1 node is expanded.

**Step 5** In the navigation tree, select the specified parameter category and change the parameter values on the right.

If you are not sure about the location of a parameter, you can enter the parameter name in search box in the upper right corner. The system searches for the parameter in real time and displays the result.

**Step 6** Click **Save**. In the confirmation dialog box, click **OK**.

**Step 7** Wait until the message **Operation successful** is displayed. Click **Finish**.

The configuration is modified.

Check whether there is any service whose configuration has expired in the cluster. If yes, restart the corresponding service or role instance for the configuration to take effect.

**----End**

Modify the configuration parameters of each service on the cluster management page of the MRS management console.

**Step 1** Log in to the MRS console. In the left navigation pane, choose **Active Clusters** and click a cluster name.

**Step 2** Choose **Components** > *Name of the desired service* > **Service Configuration**.

The **Basic Configuration** tab page is displayed by default. To modify more parameters, click the **All Configurations** tab. The navigation tree displays all configuration parameters of the service. The level-1 nodes in the navigation tree are service names or role names. The parameter category is displayed after the level-1 node is expanded.

**Step 3** In the navigation tree, select the specified parameter category and change the parameter values on the right.

If you are not sure about the location of a parameter, you can enter the parameter name in search box in the upper right corner. The system searches for the parameter in real time and displays the result.

**Step 4** Click **Save Configuration**. In the displayed dialog box, click **OK**.

**Step 5** Wait until the message **Operation successful** is displayed. Click **Finish**.

The configuration is modified.

Check whether there is any service whose configuration has expired in the cluster. If yes, restart the corresponding service or role instance for the configuration to take effect.

**----End**

# 1.4.2 Configuring the Level and File Size of Tenant Plane Logs

## Scenario

You can change the log levels of FusionInsight Manager. For a specific service, you can change the log level and the log file size to prevent the failure in saving logs due to insufficient disk space.

## Impact on the System

The service needs to be restarted for the new configuration to take effect. During the restart, the service is unavailable.

## Changing the FusionInsight Manager Log Level

1. Log in to the active management node as user **omm**.
2. Run the following command to switch the directory:

   **cd ${BIGDATA_HOME}/om-server/om/sbin**
3. Run the following command to change the log level:

   **./setLogLevel.sh** *Log level parameters*

   The priorities of log levels are FATAL, ERROR, WARN, INFO, and DEBUG in descending order. Logs whose levels are higher than or equal to the set level are printed. The number of printed logs decreases as the configured log level increases.

   - **DEFAULT**: The default log level is used.
   - **FATAL**: critical error log level. After this parameter is set, only logs of the **FATAL** level are printed.
   - **ERROR**: error log level. After this parameter is set, logs of the **ERROR** and **FATAL** levels are printed.
   - **WARN**: warning log level. After this parameter is set, logs of the **WARN**, **ERROR**, and **FATAL** levels are printed.
   - **INFO** (default): informational log level. After this parameter is set, logs of the **INFO**, **WARN**, **ERROR**, and **FATAL** levels are printed.
   - **DEBUG**: debugging log level. After this parameter is set, logs of the **DEBUG**, **INFO**, **WARN**, **ERROR**, and **FATAL** levels are printed.

- **TRACE**: tracing log level. After this parameter is set, logs of the **TRACE**, **DEBUG**, **INFO**, **WARN**, **ERROR**, and **FATAL** levels are printed.

NOTE

The log levels of components are different from those defined in open-source code.

4. Download and view logs to verify that the log level settings have taken effect.

## Changing the Service Log Level and Log File Size

NOTE

KrbServer, LdapServer, and DBService do not support the changing of service log levels and log file sizes.

**Step 1** Log in to FusionInsight Manager.

**Step 2** Choose **Cluster** > *Name of the desired cluster* > **Services**.

**Step 3** Click a service in the service list. On the displayed page, click the **Configuration** page.

**Step 4** Click the **All Configurations** tab. Expand the role instance displayed on the left of the page. Click **Log** of the role to be modified.

**Step 5** Search for each parameter and obtain the parameter description. On the parameter configuration page, select the required log level or change the log file size. The unit of the log file size is **MB**.

NOTICE

- The system automatically deletes logs based on the configured log size. To save more information, set the log file size to a larger value. To ensure the integrity of log files, you are advised to manually back up the log files to another directory based on the actual service volume before the log files are cleared according to clearance rules.
- Some services do not support change of the log level on the UI.

**Step 6** Click **Save**. In the **Save Configuration** dialog box, click **OK**.

**Step 7** Download and view logs to verify that the log level settings have taken effect.

**----End**

# 2 Error Code Reference

## 2.1 856000 Failed to Register Nginx

### Error Code Description

This error code may be generated when the DMK login using the Nginx account fails or the Nginx service is abnormal.

### Possible Causes

- Failed to log in to DMK.
- Nginx is abnormal.

### Solution

1. Check whether the DMK login is successful.
   - If yes, go to **2**.
   - If no, go to **3**.
2. Check whether the Nginx service is running properly.
   - If yes, the fault is rectified. Try again.
   - If no, go to **3**.
3. Contact technical support.

## 2.2 856002 Failed to Add a Node for Management

### Error Code Description

If the MRS_Region_Node node does not exist or the password of user **root** is incorrect, the node may fail to be managed.

### Possible Causes

- The MRS_Region_Node node does not exist.
- The password of user **root** of the MRS_Region_Node is incorrect.

### Solution

1. Check whether the MRS_Region_Node node is successfully created.
   - If yes, go to **2**.
   - If no, go to step **4**.
2. Check whether the password of user **root** of the MRS_Region_Node node is correct.
   - If yes, no further action is required.
   - If no, perform **3**.
3. Try with the correct password of user **root**. Check whether the node is successfully added for management.
   - If yes, no further action is required.
   - If no, go to step **4**.
4. Contact technical support.

## 2.3 856003 Failed to Register HAProxy

### Error Code Description

If DMK login fails or the HAProxy service is abnormal, HAProxy registration may fail.

### Possible Causes

- Failed to log in to DMK.
- The HAProxy service is abnormal.

### Solution

1. Check whether the DMK login is successful.
   - If yes, go to **2**.
   - If no, go to **3**.
2. Check whether the Haproxy service is running properly.
   - If yes, the fault is rectified. Try again.
   - If no, go to **3**.
3. Contact technical support engineers.

## 2.4 856005 Failed to Create a CDK VM in DMZ

### Error Code Description

If VM resources are insufficient, CDK VMs in DMZ may fail to be created.

### Possible Causes

The CPU, memory, or disk space is insufficient.

### Solution

1. Check whether the CPU, memory, and disk space are sufficient.
   - If yes, the fault is rectified. Try again.
   - If no, go to **2**.
2. Contact technical support engineers.

## 2.5 856006 Failed to Create a Log Directory

### Error Code Description

When the MRS_Region_Node VM is abnormal or the login using the password of user **root** fails, the DNS fails to be configured on the node.

### Possible Causes

- The MRS_Region_Node VM is abnormal.
- An incorrect password of user **root** is used to log in to the MRS_Region_Node node.

### Solution

1. Check whether the MRS_Region_Node node is normal.
   - If yes, go to **2**.
   - If no, go to **3**.
2. Check whether the password of user **root** of the MRS_Region_Node node is correct.
3. Contact technical support.

## 2.6 856007 Failed to Install MOAgent on a Node

### Error Code Description

If the AgentServer service is abnormal, MOAgent may fail to be installed on the MRS_Region_Node node.

### Possible Causes

The AgentServer service is abnormal.

### Solution

1. Check whether the AgentServer service is running properly.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support.

# 2.7 856008 Failed to Add an XaaS Whitelist to a Node

## Error Code Description

If the ManageOne O&M service is abnormal, the whitelist may fail to be added.

## Possible Causes

The ManageOne O&M service is abnormal.

## Solution

1. Check whether the ManageOne O&M service is normal.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

# 2.8 856009 Failed to Upload an MRS Image File to an OBS Bucket

## Error Code Description

If the OBS service is abnormal, the OBS IP address in the LLD is incorrect, or the image file is incomplete, the image file may fail to be uploaded to OBS.

## Possible Causes

- OBS is abnormal.
- The OBS IP address in the LLD is incorrect.
- The image file is incomplete.

## Solution

1. Check whether the OBS service is running properly.
   - If yes, go to **2**.
   - If no, start the OBS service and try again.
2. Check whether the IP address of the OBS service in LLD is correct.
   - If yes, go to **3**.
   - If no, change the OBS IP address in LLD and try again.
3. Check whether the image file is complete.
   - If yes, go to **4**.
   - If no, replace the image file and try again.
4. Contact technical support engineers.

# 2.9 856011 Failed to Obtain the Information About OBS Public Bucket

## Error Code Description

If the OBS service is abnormal, the OBS bucket information may fail to be obtained.

## Possible Causes

OBS is abnormal.

## Solution

1. Check whether the OBS service is running properly.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

# 2.10 856014 Failed to Register Service Monitoring

## Error Code Description

If the ManageOne O&M service is abnormal, service monitoring registration may fail.

## Possible Causes

The ManageOne O&M service is abnormal.

## Solution

1. Check whether the ManageOne O&M service is normal.

- If yes, try again.
- If no, go to **2**.

2. Contact technical support engineers.

# 2.11 856017 Failed to Inject Microservice Parameters

## Error Code Description

This error may be reported if the configuration file address is incorrect.

## Possible Causes

The configuration file address is incorrect.

### Solution

1. Check whether the configuration file address is correct.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

## 2.12 856019 Failed to Create a Namespace

### Error Code Description

If the CDK service is abnormal, namespaces may fail to be created.

### Possible Causes

The CDK service is abnormal.

### Solution

1. Check whether the CDK service is running properly.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

## 2.13 856020 Failed to Upload the Software Package

### Error Code Description

If the CDK service is abnormal, the software package may fail to be uploaded.

### Possible Causes

The CDK service is abnormal.

### Solution

1. Check whether the CDK service is running properly.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

# 2.14 856021 Failed to Perform Security Hardening for a VM

## Error Code Description

If the IP address of the VM cannot be logged in, the VM security hardening will fail.

## Possible Causes

The VM IP address cannot be used for login.

## Solution

1. Check whether the VM IP address is reachable.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

# 2.15 856024 Failed to Deploy a Microservice

## Error Code Description

This error may be reported if the configuration file address is incorrect.

## Possible Causes

The configuration file address is incorrect.

## Solution

1. Check whether the configuration file address is correct.
   - If yes, try again.
   - If no, go to **2**.
2. Log in to CDK and check whether the task deployment status is normal.
   - If yes, try again.
   - If no, perform **3**.
3. Contact technical support engineers.

# 2.16 856107 Failed to Obtain the Host Group ID

## Error Code Description

If the value of **mrs_compute_host_group** in the parameter template of the MRS host group is incorrect or the host group is not created, the host group ID may fail to be obtained.

## Possible Causes

- The value of **mrs_compute_host_group** in the parameter template of the MRS host group is incorrect.
- The host group is not created.

## Solution

1. Check whether the value of **mrs_compute_host_group** in the basic engineering parameters is correct.
   - If yes, try again.
   - If no, go to **2**.
2. Check whether the corresponding host group has been created.
   - If yes, try again.
   - If no, perform **3**.
3. Contact technical support.

# 2.17 856108 Failed to Register with CMDB and the IP Address Is Unreachable

## Error Code Description

If the CMDB service is abnormal, the CMDB may fail to be registered.

## Possible Causes

The CMDB service is abnormal.

## Solution

1. Check whether the CMDB service is running properly.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

# 2.18 856109 Failed to Obtain the JKS Certificate File

## Error Code Description

The JKS certificate fails to be obtained when the JKS certificate does not exist or the JKS certificate path is incorrect.

## Possible Causes

- The JKS certificate does not exist.
- The JKS certificate path is incorrect.

## Solution

1. Check whether the ManageOne service is running properly.
   - If yes, try again.
   - If no, go to **2**.
2. Check whether the unified password system is normal.
   - If yes, try again.
   - If no, perform **3**.
3. Contact technical support.

# 2.19 856112 Parameter mrs_core2_localdisk_conf Is Mandatory When mrs_core2_hostgroup Is Not Empty

## Error Code Description

This error may be reported when **mrs_core2_hostgroup** is not empty and the **mrs_core2_localdisk_conf** parameter is not set.

## Possible Causes

The **mrs_core2_hostgroup** parameter is not empty, and the **mrs_core2_localdisk_conf** parameter is not set.

## Solution

1. Check whether the **mrs_core2_localdisk_conf** parameter is set when **mrs_core2_hostgroup** is left empty.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

# 2.20 856113 Failed to Deploy the SDR Plug-in

## Error Code Description

If the SDR service is abnormal, the SDR plug-in may fail to be deployed.

## Possible Causes

The SDR service is abnormal.

## Solution

1. Check whether the SDR service is running properly.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

# 2.21 856114 Failed to Register with CMT

## Error Code Description

If the ManageOne OM plane is abnormal, the registration with the CMT may fail.

## Possible Causes

The ManageOne OM plane is abnormal.

## Solution

1. Check whether the ManageOne OM plane is normal.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

# 2.22 856115 Prefix of the Global Domain Name of Non-first OBS Must Start with "OBS-" and Meet the Domain Name Specifications

## Error Code Description

This error may be reported if the global domain name does not start with "OBS-" or does not comply with the domain name specifications.

### Possible Causes

- The global domain name does not start with "OBS-".
- The domain name does not comply with the domain name specifications.

### Solution

1. Check whether the global domain name starts with "OBS-".
   - If yes, try again.
   - If no, go to **2**.
2. Check whether the domain name complies with the domain name specifications.
   - If yes, try again.
   - If no, perform **3**.
3. Contact technical support engineers.

## 2.23 856116 Parameter Cannot Be Left Blank If It Is Mandatory

### Error Code Description

This error may be reported when the parameter is mandatory but left empty.

### Possible Causes

A mandatory parameter is left empty

### Solution

1. Check whether the mandatory parameter is empty.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

## 2.24 856117 Parameters Are Missing

### Error Code Description

This error may occur if the parameter to be uploaded does not exist in the parameter template.

### Possible Causes

The parameter in the uploaded parameter template does not exist.

### Solution

1. Check whether the **key** parameter exists in the basic parameters in the parameter template to be uploaded.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

## 2.25 856114 Failed to Register Cloud Service Monitoring Information

### Error Code Description

This error may be reported when the ManageOne API fails to be called to register a cloud service.

### Possible Causes

- The ManageOne service is abnormal.
- The IP address of ManageOne is incorrect.

### Solution

1. Check whether the service status of ManageOne is normal.
   - If yes, go to **2**.
   - If no, perform **3**.
2. Check whether the IP address of ManageOne is correct.
   - If yes, try again.
   - If no, perform **3**.
3. Contact technical support.

## 2.26 856120 Failed to Create a CCS Tag for a Flavor

### Error Code Description

If the network is abnormal, the CCS tag may fail to be created.

### Possible Causes

The network is abnormal.

### Solution

1. Check whether the network is normal.
   - If yes, try again.
   - If no, go to **2**.

2. Contact technical support engineers.

# 2.27 856121 Failed to Obtain the serviceommatch Label of a Host Group

## Error Code Description

This error may be reported when the host group is abnormal or the serviceommatch label is not added.

## Possible Causes

- The host group is abnormal.
- The serviceommatch label is not added.

## Solution

1. Check whether the host group is normal.
   - If yes, try again.
   - If no, go to **2**.
2. Check whether the **serviceommatch** label is not correctly added.
   - If yes, try again.
   - If no, perform **3**.
3. Contact technical support engineers.

# 2.28 856122 Failed to Install the MySQL Database

## Error Code Description

This error may be reported when user **root** fails to log in to the MRS_DB node.

## Possible Causes

User **root** fails to log in to the MRS_DB node.

## Solution

1. Log in to the active MRS-DB node as user **opsadmin**. For details, see **Logging In to an MRS Management Node**. Run the following command to switch to the **root** user:

   **su - root**

   NOTE

   For details about the default password, see ***Huawei Cloud Stack 8.3.1 Account List*** or contact the system administrator.

   Check whether you can log in to the node.

- If yes, try again.
- If no, go to **2**.

2. Contact technical support.

# 2.29 856123 Failed to Initialize the Database

## Error Code Description

This error may be reported when the MRS database connection account fails to connect to the database or an exception occurs in SQL execution.

## Possible Causes

- The MRS database connection account fails to connect to the database.
- An exception occurs in SQL execution.

## Solution

1. Use the MRS database connection account and password to connect to the database.
   - If yes, try again.
   - If no, go to **2**.
2. Check whether the key information about the SQL execution failure is recorded in the failure log.
   - If yes, try again.
   - If no, go to **3**.
3. Contact technical support.

# 2.30 856124 Failed to Create a Database VM

## Error Code Description

The computing resources of the current host group are insufficient. As a result, the VM status is abnormal after the VM is created.

## Possible Causes

- The current computing resources are insufficient.
- The VM network is abnormal.

## Solution

1. Check whether the computing resources of the current management host group are sufficient.
   - If yes, try again.
   - If no, go to **2**.

2. Log in to Service OM to check whether the MRS_DB VM is running properly and whether the IP address is accessible.
   - If yes, try again.
   - If no, go to **3**.
3. Contact technical support.

# 2.31 856138 Failed to Install and Start ZooKeeper

## Error Code Description

This error may be reported when the login to the MRS_Region_Node node fails.

## Possible Causes

Login to the MRS_Region_Node node fails.

## Solution

1. Log in to ManageOne Maintenance Portal using a browser as a system administrator.
   - URLs: **https://***Domain name of ManageOne Maintenance Portal*:**31943** or **https://***Domain name of ManageOne Unified Portal*
   - Login using a password: Enter the username and password.
     - Default account: bss_admin
     - Default password: See the default password of the account for logging in to ManageOne Maintenance Portal in the "Type A (Portal)" sheet in ***Huawei Cloud Stack 8.3.1 Account List*** .
   - Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter a PIN.
2. Click **Log In**.
3. Click **Service OM** in **Common Links**, and select a region to switch to the **Service OM** page.
4. Choose **Services** > **Compute Resource**. On the **Compute Resource** page, select **VMs**, search for **MRS_Region_Node** in the search box, and obtain its IP address in the **IP Address** column.
5. Log in to the MRS_Region_Node node as user **opsadmin** using the IP address of MRS_Region_Node in **4**. For details about the password, see ***Huawei Cloud Stack 8.3.1 Account List*** . Check whether you can log in to the MRS_Region_Node node.
   - If yes, try again.
   - If no, go to **6**.
6. Contact technical support.

# 2.32 856141 Failed to Change the Host Name of an MRS VM

## Error Code Description

This error is reported when the login to the MRS_Region_Node or MRS_DB node fails.

## Possible Causes

- Login to the MRS_Region_Node node fails.
- Login to the MRS_DB node fails.

## Solution

1. Check whether you can log in to the MRS_Region_Node node as user **opsadmin**.
   - If yes, go to **2**.
   - If no, go to **3**.
2. Check whether you can log in to the MRS_DB node as user **opsadmin**.
   - If yes, try again.
   - If no, go to **3**.
3. Contact technical support.

# 2.33 856142 Failed to Preset the Unified License Information

## Error Code Description

This error may be reported when the ManageOne service is abnormal.

## Possible Causes

The ManageOne service is abnormal.

## Solution

1. Log in to ManageOne Maintenance Portal and check whether the unified license service is normal.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support.

# 2.34 12000029 Failed to Obtain the Quota

## Error Code Description

If the network is abnormal, the quota may fail to be obtained.

## Possible Causes

The network is abnormal.

## Solution

1. Check whether the network is properly connected.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

# 2.35 12000030 Number of Requested Nodes in the Cluster Exceeds the Available Quota

## Error Code Description

This error is reported when the total number of cluster nodes applied for is greater than the available quota.

## Possible Causes

The requested number of nodes in the cluster exceeds the available quota.

## Solution

1. Apply for more node quotas.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

# 2.36 12000031 Number of Requested CPU Cores in the Cluster Exceeds the Available Quota

## Error Code Description

This error is reported when the total number of CPU cores in the cluster is greater than the available CPU quota.

### Possible Causes

The requested number of CPU cores in the cluster exceeds the available quota.

### Solution

1. Apply for more CPU quotas.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

## 2.37 12000032 Number of Requested Memories in the Cluster Exceeds the Available Quota

### Error Code Description

This error is reported when the applied cluster memory is greater than the available memory quota.

### Possible Causes

The applied cluster memory is greater than the available memory quota.

### Solution

1. Apply for more memory quota.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

## 2.38 12000033 Number of Requested Disk Blocks in the Cluster Exceeds the Available Quota

### Error Code Description

This error is reported when the number of applied cluster disks is greater than the available disk quantity quota.

### Possible Causes

The number of applied cluster disks is greater than the available disk quantity quota.

### Solution

1. Apply for more disk block quota.
   - If yes, try again.

- If no, go to **2**.

2. Contact technical support engineers.

# 2.39 12000034 Number of Requested Disk Capacity in the Cluster Exceeds the Available Quota

## Error Code Description

This error is reported when the applied cluster disk capacity is greater than the available disk capacity quota.

## Possible Causes

The applied cluster disk capacity is greater than the available disk capacity quota.

## Solution

1. Apply for a larger disk capacity quota.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

# 2.40 12000045 Insufficient Security Group Quota

## Error Code Description

This error is reported when the security group quota is insufficient.

## Possible Causes

The security group quota is insufficient.

## Solution

1. Apply for more security group quota.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

# 2.41 12000046 Insufficient Security Group Rule Quota

## Error Code Description

This error is reported when the security group rule quota is insufficient.

### Possible Causes

The security group rule quota is insufficient.

### Solution

1. Apply for more security group rule quota.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

## 2.42 12000115 Insufficient ECS Group Quota

### Error Code Description

This error is reported when the ECS group quota is insufficient.

### Possible Causes

The ECS group quota is insufficient.

### Solution

1. Apply for more ECS group quota.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

## 2.43 12000116 Insufficient VPC Quota

### Error Code Description

This error is reported when the VPC quota is insufficient.

### Possible Causes

The VPC quota is insufficient.

### Solution

1. Apply for more VPC quotas.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

# 2.44 12000117 Insufficient Subnet Quota

## Error Code Description

This error is reported when the subnet quota is insufficient.

## Possible Causes

The subnet quota is insufficient.

## Solution

1. Apply for more subnet quotas.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

# 2.45 101 Empty Token

## Error Code Description

This error code may be reported when the token obtained during cluster creation is empty.

## Possible Causes

The **X_AUTH_TOKEN** parameter in the request header is empty.

## Solution

1. Check whether the **X_AUTH_TOKEN** parameter in the request header is empty.
   - If yes, go to **2**.
   - If no, try again.
2. Contact technical support.

# 2.46 102 Failed to Obtain the Area List

## Error Code Description

This error code is displayed when an exception occurs during region list query when creating a cluster.

## Possible Causes

An exception occurs when the **deploy** or **bss** interface is invoked to obtain the region list.

### Solution

1. Check whether the **deploy** service is normal.
   - If yes, try again.
   - If no, go to **2**.
2. Check whether the service is started after restarting the deploy service.
   - If yes, try again.
   - If no, go to **3**.
3. Contact technical support engineers.

## 2.47 104 Tenant ID Is Empty

### Error Code Description

This error may be reported when the parameter is abnormal and the tenant ID is empty.

### Possible Causes

A parameter exception occurs.

### Solution

1. Check whether the parameters are correct.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

## 2.48 12000036 Failed to Obtain the Product Information

### Error Code Description

This error code may be displayed when the network is abnormal and an exception occurs during product information query.

### Possible Causes

The network is abnormal.

### Solution

1. Check whether the network status is normal.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

# 2.49 12000041 Failed to Obtain the Cluster List

## Error Code Description

The deploy service is abnormal when the database is abnormal.

## Possible Causes

- The deploy service is abnormal.
- The database is abnormal.

## Solution

1. Check whether the deploy service status is normal.
   - If yes, go to **2**.
   - If no, go to **3**.
2. Check whether the database is normal.
   - If yes, try again.
   - If no, go to **3**.
3. Contact technical support engineers.

# 2.50 12000003 Cluster Does Not Exist

## Error Code Description

This error code is displayed when the cluster does not exist during the querying of cluster details or expanding the capacity of a cluster based on the cluster ID.

## Possible Causes

The cluster fails to be created and the page is not refreshed. The cluster information is deleted.

## Solution

1. Refresh the page and create a cluster again. The error is cleared.
   - If yes, no further action required.
   - If no, go to **2**.
2. Contact technical support engineers.

# 2.51 12000023 Failed to Obtain Cluster Details

## Error Code Description

This error code is generated when the API service is abnormal due to a database exception.

### Possible Causes

- The API service is abnormal.
- The database is abnormal.

### Solution

1. Check whether the API service status is normal.
   - If yes, go to **2**.
   - If no, go to **3**.
2. Check whether the database is normal.
   - If yes, try again.
   - If no, go to **3**.
3. Contact technical support engineers.

## 2.52 12000042 Failed to Create a Cluster

### Error Code Description

If an exception occurs when you use the preset service account to create an order number, the cluster fails to be created and this error is reported.

### Possible Causes

An exception occurs when the **deploy** or **bss** interface is invoked to create an order ID.

### Solution

1. Check whether the interfaces for creating an order ID are normal.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support.

## 2.53 12000136 Insufficient User Permission

### Error Code Description

This error may be reported if the user does not have the required permission.

### Possible Causes

The user permission is insufficient.

### Solution

1. Log in to ManageOne Maintenance Portal using a browser as the VDC operator .

2. Choose **System** > **VDC List** and click the target VDC name. In the navigation pane on the left, choose **User Groups**. On the displayed page, locate the row that contains the target user group and click **Configure Permissions** in the **Operation** column.

   For details about fine-grained user permissions, see "Cluster Management" > "Managing an MRS ECS/BMS Cluster" > "Synchronizing IAM Users to MRS" in *MapReduce Service (MRS) 3.3.1-LTS User Guide (for Huawei Cloud Stack 8.3.1) in the MapReduce Service (MRS) 3.3.1-LTS Usage Guide (for Huawei Cloud Stack 8.3.1)*.

   Check whether the current user has the permission to create a cluster.

   - If yes, try again.
   - If no, go to **3**.

3. Contact technical support.

# 2.54 12000053 Invalid Order Type

## Error Code Description

This error is not reported when the order type is neither pay-per-use nor yearly/monthly.

## Possible Causes

The order type is neither pay-per-use nor yearly/monthly.

## Solution

1. Check whether the order type is pay-per-use or yearly/monthly.
   - If yes, try again.
   - If no, go to **2**.
2. Contact technical support engineers.

# 2.55 12000027 Failed to Verify the Cluster Subnet

## Error Code Description

If the subnet information is incorrect, this error may occur.

## Possible Causes

The network information is incorrect.

## Solution

1. Check whether the subnet information is correct.
   - If yes, try again.
   - If no, go to **2**.

2. Contact technical support engineers.

# 2.56 12000108 Failed to Verify the EIP When Creating the Cluster

## Error Code Description

This error may be reported if the EIP ID or address is empty, the status is not **down**, or **publicIP** is empty.

## Possible Causes

- The EIP ID and address are empty.
- The status is not **down**.
- **publicIP** is empty.

## Solution

1. Check whether the EIP ID and address are empty.
   - If yes, go to **4**.
   - If no, go to **2**.
2. Check whether the EIP status is **down**.
   - If yes, go to **3**.
   - If no, go to **4**.
3. Check whether **publicIP** is empty.
   - If yes, go to **4**.
   - If no, try again.
4. Contact technical support engineers.

# 2.57 12000028 Total Number of Cores and Task Nodes in a Cluster Cannot Exceed *xxx*

## Error Code Description

The total number of cores and task nodes in a cluster cannot exceed *xxx*.

## Possible Causes

The total number of applied cores and task nodes is greater than the value set in Manager.

## Solution

1. Check whether the total number of applied cores and task nodes is greater than the value set on Manager.

- If yes, adjust the number of nodes and try again.
- If no, go to **2**.

2. Contact technical support engineers.

# 2.58 12000233 Insufficient Cluster Flavor Resources

## Error Code Description

This error may be reported when the flavor resources of the cluster to be applied for are insufficient.

## Possible Causes

The flavor resources are insufficient.

## Solution

1. Check whether the flavor resources are sufficient.
   - If yes, reduce the purchase quantity and try again. Select another instance with different types and flavors, or change the region and AZ.
   - If no, go to **2**.
2. Contact technical support engineers.

# 2.59 12000038 Failed to Obtain the Security Group

## Error Code Description

This error may be reported if the security group does not exist or **projectID** is empty.

## Possible Causes

The security group does not exist or **projectID** is empty.

## Solution

1. Check whether the security group exists.
   - If yes, go to **3**.
   - If no, create a security group and try again.
2. Check whether the **projectID** is empty.
   - If yes, go to **3**.
   - If no, try again.
3. Contact technical support engineers.

# 2.60 12000043 Cluster Name Already Exists

## Error Code Description

If a cluster with the same name already exists when you create a cluster, this error may occur.

## Possible Causes

A cluster with the same name already exists.

## Solution

1. Check whether a cluster with the same name exists.
   - If yes, change the cluster name and try again.
   - If no, go to **2**.
2. Contact technical support engineers.

# 2.61 12000044 Memory Size of the Master Node in the Cluster Is Less Than the Minimum Memory Size

## Error Code Description

This error may be reported when the memory size of the master node in the cluster is less than the minimum memory size.

## Possible Causes

The memory of the master node in the cluster is less than the minimum memory.

## Solution

1. Check whether the memory of the master node is less than the minimum memory.
   - If yes, change the memory size of the master node and try again.
   - If no, go to **2**.
2. Contact technical support engineers.

# 2.62 12000047 Incorrect Disk Type and Size

## Error Code Description

This error may be reported if the disk type and size are incorrect.

### Possible Causes

The disk type and size do not meet the requirements.

### Solution

1. Log in to ManageOne Maintenance Portal using a browser as the VDC operator .
2. Log in to the MRS console, choose **Clusters** > **Active Clusters**, and click the target cluster name.
3. Click the **Nodes** tab. On the displayed page, click the name of the target node in the **Node Group** column.
4. On the **EVS** console, check whether the disk type and size are abnormal.
   - If yes, change the disk type and size and try again.
   - If no, go to **5**.
5. Contact technical support.

## 2.63 12000048 Product Flavor Do Not Exist

### Error Code Description

This error may be reported if the selected product flavor does not exist.

### Possible Causes

The selected product flavor does not exist.

### Solution

1. Check whether the selected product flavor exists.
   - If yes, go to **2**.
   - If no, select another flavor and try again.
2. Contact technical support engineers.

## 2.64 12000050 Incorrect Certificate

### Error Code Description

This error may occur when the certificate is incorrect.

### Possible Causes

Certificate error

### Solution

1. Check whether the certificate is correct.

- If yes, replace the certificate and try again.
- If no, go to **2**.

2. Contact technical support engineers.

# 2.65 12000059 User Key Pair Does Not Exist

## Error Code Description

This error may be reported if the user key pair does not exist.

## Possible Causes

The user key pair does not exist.

## Solution

1. Check whether the user key pair exists.
   - If yes, go to **2**.
   - If no, replace the key pair and try again.
2. Contact technical support engineers.

# 3 Appendix

## 3.1 Logging In to an MRS Management Node

Huawei Cloud Stack provides a security O&M channel through the CLI terminal (an optional module). When you install the security O&M channel, the way of logging in to backend nodes changes. This section describes how to log in to a backend node in different scenarios.

The module provides security O&M capabilities for ManageOne Maintenance Portal, including SSH login without password, command execution or interception, file upload and download, and O&M command audit. The module provides a unified O&M portal. This enhances O&M management, control, and audit, simplifies the remote O&M access process, improves O&M efficiency, and enhances account and password security.

The module is selected by default and can be deselected. It is not upgraded by default and can be added after the upgrade.

**NOTE**

The CLI supports the following accounts in different scenarios:

- Accounts of cloud services where the security O&M channel is not installed can only be used to log in to nodes over SSH.
- Accounts of cloud services where the security O&M channel is installed but that are not reclaimed can only be used to log in to nodes over SSH.
- Accounts of cloud services where the secure O&M channel is installed and that are reclaimed can be used to log in to nodes over SSH by applying for a password because its password has been changed to a random one after reclamation.
- Accounts of cloud services where the secure O&M channel is installed, that are reclaimed, and that have obtained the one-click login permission can be used to log in to nodes through the CLI terminal or over SSH by applying for a password.

### Prerequisites

- You have logged in to ManageOne Maintenance Portal as a system administrator.
- You have obtained the permission to perform operations on the CLI.
- If the command whitelist is enabled, only whitelisted commands can be executed on the CLI. If the function is disabled, any commands can be executed on the CLI.

## Logging In to an MRS Management Node Through the CLI Terminal

**Step 1** Check whether secure O&M channel has been installed.

Choose **O&M** from the main menu and check whether the CLI terminal is displayed in the navigation pane.

- If yes, the secure O&M channel has been installed. Go to **Step 2**.
- If no, the secure O&M channel is not installed. In this case, log in to a management node over SSH. For details, see **Logging In to an MRS Management Node Over SSH**.

**Step 2** Check whether the account has been managed by an external system.

1. Choose **O&M** > **Accounts** from the main menu.
2. Check whether the account for logging in to the backend node has been remotely managed based on information displayed in the **Application/Cloud Service**, **Resource Name**, and **Account Management Party** columns.
   - If yes, use an SSH client, such as PuTTY, to log in to a node.
   - If no, go to **Step 3**.

**Step 3** Use either of the following methods to log in to a backend node:

- Login using SSH

  Apply for permission to use an account password to log in to the node over SSH. For details, see section "Account Request" > "Creating a Request for Obtaining Passwords" in the **Huawei Cloud Stack 8.3.1 O&M Guide**.

- One-click login on the CLI

  a. Choose **O&M** > **CLI** from the main menu.

  b. In the navigation pane on the left, expand the corresponding nodes one by one and check whether the account for logging in to the backend node is displayed.

  - If yes, the account has obtained the permission for one-click login. Go to **Step 4**.
  - If no, apply for the one-click login permission to log in to the node. For details, see section "Account Request" > "Creating a Request for Obtaining Passwords" in the **Huawei Cloud Stack 8.3.1 O&M Guide**. Then, go to **Step 4**.

**Step 4** Click **Execute Command** to log in to the backend node. Then, proceed with other operations.

NOTE

Only commands in the trustlist can be executed. If the following error message is displayed during the execution, contact the administrator to add the commands to the trustlist. For details, see the **Huawei Cloud Stack 8.3.1 O&M Guide**.
Your command is highly risky. Please check the whitelisted commands.

**----End**

## Logging In to an MRS Management Node Over SSH

**Step 1** Log in to ManageOne Maintenance Portal as the system administrator. In the **Common Links** navigation tree, click Service_OM and select a region to go to the Service OM page.

**Step 2** Choose **Services** > **Resource** > **Compute Resource**.

**Step 3** Click the **VMs** tab, enter a keyword in the search box to search for the VM name, for example, **EICommon-Region-Master**, **MRS_DB**, **Console-DB**, or **Console-Static**, and record the IP address of the VM.

**Step 4** Use PuTTY to log in to any VM whose **Status** is **Running** as user **opsadmin**. For example, log in to the **EICommon-Region-Master-01**, **MRS_DB-01**, **Console-DB-01**, or **Console-Static-01** VM.

Obtain the default password by referring to ***Huawei Cloud Stack 8.3.1 Account List*** or contacting the system administrator.

NOTE

If **Status** of all VMs is not **Running**, contact the cluster administrator.

**----End**