SOMANSA

Somansa Network DLP

Mail-i 8.x
Troubleshooting Guide

Contents

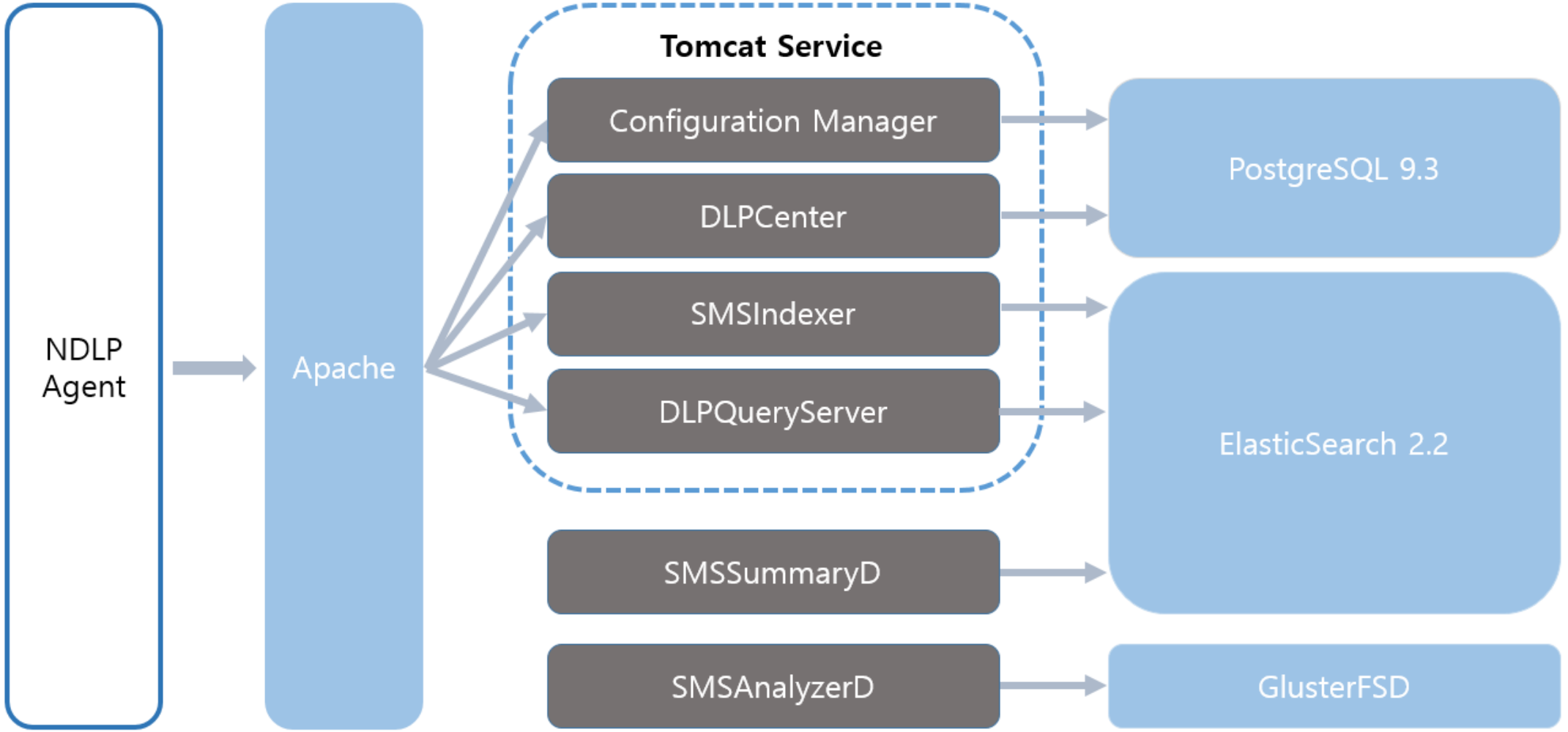
This Document is a Troubleshooting Guide for Mail-i 8.x.

Please contact SOMANSA Support Team for additional questions and support.

Mail-i
Service Introduction

I. Mail-i Service Introduction

1. Mail-i Service Architecture



I. Mail-i Service Introduction

2. Mail-i Service Introduction

Category	Contents
Configuration Manager	Web Services for basic Mail-i configuration
DLPCenter	Web Service for Mail-i Management such as statistics check, log check policy setting
NDLP Agent	Agent to check the packet and process to be logged
DLPQueryServer	Service to view logs in ElasticSearch
SMSIndexer	Service to store agent logs in ElasticSearch
SMSAnalyzerD	Services that analyze file copies stored in GlusterFS
SMSSummaryD	Services that perform statistical work on data stored in ElasticSearch
ElasticSearch	File system that stores Agent's Data
GlusterFS	Services that store copies of files

Mail-i
Troubleshooting Guide

II. Mail-i Troubleshooting Guide

1. Log File Path for Services

Category	Path
CM	/somansa/cm/tomcat/logs/catalina.out
DLPCenter	/somansa/dlpcenter/tomcat/logs/catalina.out
NDLP Agent	/somansa/ndlp/env/default/log/ndlp_agent_YYYYMMDD.rmk
DLPQueryServer	/somansa/common/tomcat_queryserver/logs/catalina.out
SMSIndexer	/somansa/common/tomcat_indexer/logs/catalina.out
SMSAnalyzerD	/somansa/common/log/SMSAnalzyer.out
SMSSummaryD	/somansa/common/log/SMSSummary.out
ElasticSearch	/somansa/data/es_log/SMS_LogServer.log
GlusterFS	/var/log/glusterfs/somansa-data-gfs_data.log

II. Mail-i Troubleshooting Guide

2. Incidents Pages doesn't display

· Primary Causes and Actions

1) DLPQueryServer does not operate or malfunctions

- Check error messages for DLPQueryServer

```
tail -f /somansa/common/tomcat_queryserver/logs/queryserver.log
```

- Service Stop and Start

```
/somansa/common/tomcat_queryserver/bin/shutdown.sh
/somansa/common/tomcat_queryserver/bin/startup.sh
```

- Check process for DLPQueryServer

```
ps -ef |grep tomcat_queryserver
```

2) IP of DLPQueryServer configured at DLPCenter is not correct

- Check configuration file

```
vi /somansa/common/conf/DLPQueryServer.conf
```

- ip=https://DLPQueryServerIP check at configuration values.
- If the value is different, change the value and restart DLPCenter

II. Mail-i Troubleshooting Guide

3-1 Reports Pages doesn't display

· Primary Causes and Actions

1) Check process execution(If it works, move to Step 5)

```
ps -ef |grep SMSSummaryD
```

2) Check crontab registration

```
*/10 * * * * /somansa/common/script/SMSSummaryD_check.sh >> /somansa/common/log/SMSSummaryD_Restart.log 2>&1
```

3) Process Execution

```
/somansa/common/script/SMSSummaryD.sh start
```

4) Check Execution log

```
vi /somansa/common/log/SMSSummaryD.out
```

- Contact SOMANSA Support Team for error logs
- if error logs doesn't exist, restart SMSSummaryD

```
/somansa/common/script/SMSSummaryD.sh stop
/somansa/common/script/SMSSummaryD.sh start
```

II. Mail-i Troubleshooting Guide

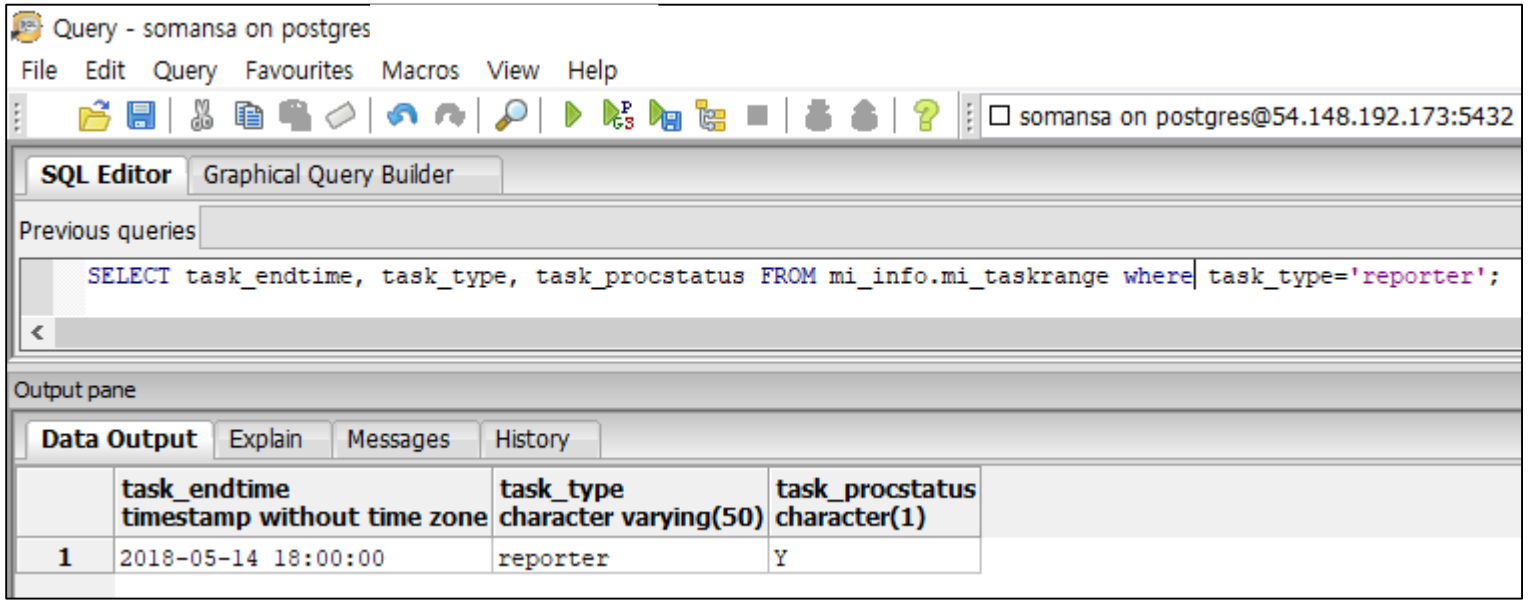
3-2 Reports Pages are not displayed

· Primary Causes and Actions

5) Check status of tasks in DB (PostgreSQL)

- Execute the following query

```
SELECT task_endtime, task_type, task_procstatus FROM mi_info.mi_taskrange where task_type='reporter';
```



- Task can't execute when the value of task_procstatus is N
- In this case, change the value of task_procstatus to Y and restart SMSSummaryD

II. Mail-i Troubleshooting Guide

4-1 Can not analyze the information in the file copy

· Primary Causes and Actions

1) Check process execution (If successful, move to Step 5)

```
ps -ef |grep SMSAnalyzerD
```

2) Check crontab registration

```
*/10 * * * * /somansa/common/script/SMSAnalyzerD_check.sh >> /somansa/common/log/SMSAnalyzerD_Restart.log 2>&1
```

3) Process Execution

```
/somansa/common/script/SMSAnalyzerD.sh start
```

4) Check Execution log

```
vi /somansa/common/log/SMSAnalyzerD.out
```

- Contact SOMANSA Support Team when error logs exist
- If error logs doesn't exist, restart SMSAnalyzerD

```
/somansa/common/script/SMSAnalyzerD.sh stop
/somansa/common/script/SMSAnalyzerD.sh start
```

II. Mail-i Troubleshooting Guide

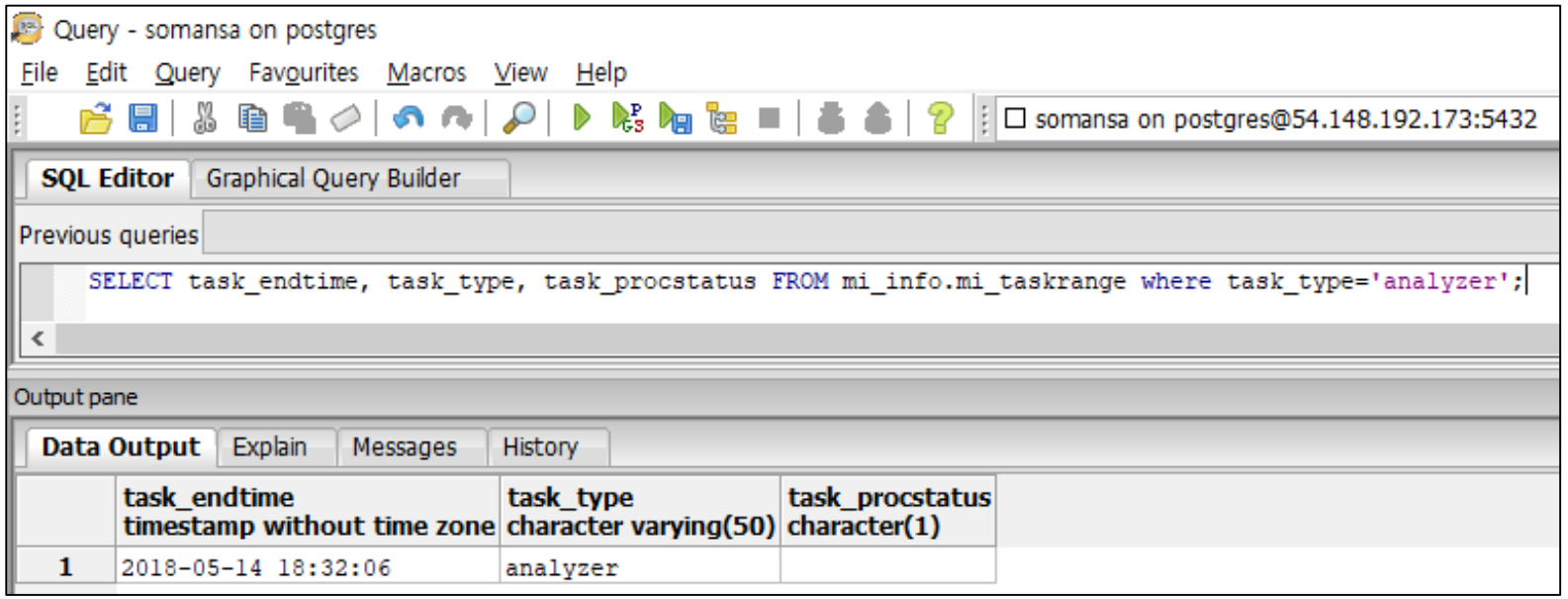
4-2 Can not analyze the information in the file copy

· Primary Causes and Actions

5) Check status of tasks in DB (PostgreSQL)

- Execute the following query

```
SELECT task_endtime, task_type, task_procstatus FROM mi_info.mi_taskrange where task_type='analyzer';
```



- Task_endtime is the time when the pattern analysis has been completed (Updated every 5 seconds)
- Contact SOMANSA Support Team if the time doesn't change after the above measures have been taken

II. Mail-i Troubleshooting Guide

5-1 The Log was Not Saved

· Primary Causes and Actions

1) ElasticSearch does not operate or malfunctions

- Check Process Execution

ps -ef | grep elasticsearch

- If the process does not exist execute Elasticsearch

service elasticsearch start

- Check log when execution fails

tail –f /somansa/data/es_log/SMS_LogServer.log

2) SMSIndexer does not operate or malfunctions

- Check Process Execution

ps -ef | grep tomcat_indexer

- If the process does not exist execute SMSIndexer

/somansa/common/tomcat_indexer/bin/startup.sh

- Check log when execution fails

tail –f /somansa/common/tomcat_indexer/logs/catalina.out

II. Mail-i Troubleshooting Guide

5-2 The Log was Not Saved

· Primary Causes and Actions

3) There are many files created in /somansa/temp_index path when log save fails

- Save Failed files can be saved in ElasticSearch
- Use the following command to save in ElasticSearch

```
java -classpath /somansa/common/bin/SMSIndexerRemainFiles.jar com.somansa.smsindexer.main.Main 3 0 24 "/somansa/temp_index"
```

- If you don't have the SMSIndexerRemainFiles.jar file in the /Somansa/common/bin/ path on Server, please contact the Somansa Support Team.

II. Mail-i Troubleshooting Guide

6. GlusterFS Volume Creation Failed

· Primary Causes and Actions

1) The Firewall may be blocking required ports.

- Check port 49152 to 49156 is allowed in the firewall settings

2) The brick you are trying to connect to is incorrectly connected to another volume.

- The following error occurs when creating a volume

```
failed: Brick: HOSTNAME:/somansa/data/gfs_brick1 not available. Brick may be containing or be contained by an existing brick
```

- If an error message appears, execute /hyboost/init/gfs.init.sh to initialize.
- If the file was executed, the saved file was deleted, so it is not responsible for the lost file.

II. Mail-i Troubleshooting Guide

7. Attached file downloaded as 0KB

· Primary Causes and Actions

1) GlusterFS on the server is unmounted

- Check the port 49152 to 49156 is allowed in the firewall settings

```
mount –t glusterfs HOSTNAME:/gfs_volume/somansa/data/gfs_dat
```

II. Mail-i Troubleshooting Guide

8. Log Export Function Failed

· Primary Causes and Actions

1) Redis does not operate or malfunctions

- Check process execution

ps –ef | grep redis | grep 9800

- Execute the process

/somansa/common/script/redis_check.sh

II. Mail-i Troubleshooting Guide

9. Indexer Service behaves abnormally

· Primary Causes and Actions

1) Occurs when two Indexer services are running

- Check SMSIndexer log

tail –f /Somansa/common/tomcat_indexer/logs/catalina.out

- Continually check if the getConnection() error log is occurring
- Check the process to see if two indexers are running

ps –ef |grep tomcat_indexer

- Check the two indexer PIDs and perform forced termination

kill -9 [PID]

- Restart the indexer service

/somansa/common/tomcat_indexer/bin/startup.sh

2) Error when restarting Indexer service

(java.net.BindException: Address is already in use <null>:8700 error)

- Repeat Step 1

II. Mail-i Troubleshooting Guide

10. Incidents are not logged when selected as Top Level Department

- Primary Causes and Actions

  1) Error occurs when the number of query conditions exceeds 1024

  - Add the line below in the /etc/elasticsearch/elasticsearch.yml file and restart ElasticSearch

    index.query.bool.max_clause_count: 4096