MapReduce Service

Product Bulletin

Issue	01
Date	2024-09-06

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

HUAWEI 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 Vulnerability Notice

1.1 Guide for Fixing the Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)

This section describes how to fix the Apache log4j2 vulnerability CVE-2021-44228. Currently, you can use either of the following methods to fix the vulnerability:

- **Installing the Patch on Existing Cluster Nodes**
- **Installing the Patch on New Nodes**

Prerequisites

- You have downloaded the patch tool package **MRS_Log4j_Patch.tar.gz** from the OBS path.
- You have determined the active OMS node in the cluster.

  NOTE

  Generally, OMS is deployed on two nodes, master1 and master2. You can use the following commands to determine the active OMS node. The node whose command output contains active is the active OMS node, and the node whose command output contains standby is the standby OMS node.

  For clusters whose version is earlier than MRS 3.*x*, use the following command:

  sh /opt/Bigdata/*/workspace0/ha/module/hacom/script/get_harole.sh

  For clusters whose version is later than MRS 3.*x*, use the following command:

  sh /opt/Bigdata/om-server*/OMS/workspace0/ha/module/hacom/script/get_harole.sh

Installing the Patch on Existing Cluster Nodes

Step 1 Upload **MRS_Log4j_Patch.tar.gz** to the **/home/omm** directory on the active OMS node. For details, see **How Do I Upload a Local File to a Node Inside a Cluster?**.

Step 2 Run the following commands to log in to the active OMS node as user **root**, modify the permission of the patch tool, switch to user **omm**, and decompress the patch tool package to the current directory:

chown omm:wheel -R /home/omm/MRS_Log4j_Patch.tar.gz

su - omm

cd /home/omm

tar -zxf MRS_Log4j_Patch.tar.gz

Step 3 In the **/home/omm/MRS_Log4j_Patch/bin/ips.ini** file, configure the IP addresses (IP addresses of all nodes in the current cluster) of the nodes where the patch is to be installed.

NOTE

Configure one IP address in each line. No empty line is allowed.

Step 4 Run the following scripts to install the patch:

cd /home/omm/MRS_Log4j_Patch/bin

nohup sh install.sh upgrade &

Run the **tail -f nohup.out** command to check the execution status. If "upgrade patch success." is displayed, the execution is complete.

Step 5 Log in to Manager, restart the affected components (you are advised to perform this operation during off-peak hours). For details, see **List of Affected Components**.

Step 6 (Optional) If you want to install the patch for the newly downloaded client, run the following commands to install the patch for the component package first:

su - omm

cd /home/omm/MRS_Log4j_Patch/bin

nohup sh install.sh upgrade_package &

Run the **tail -f nohup.out** command to check the execution status. If "upgrade_package patch success." is displayed, the execution is complete.

After the execution is complete, the client downloaded is the one with the patch installed.

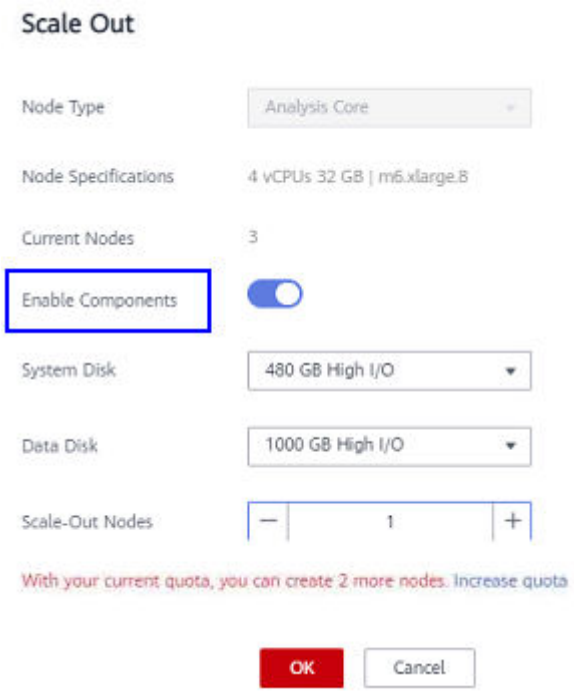
CAUTION

- This step takes a long time, and you do not need to restart the component after performing this step.
- After the patch is installed, do not delete the files related to the patch directory. Otherwise, the patch cannot be uninstalled.

----End

Installing the Patch on New Nodes

Step 1 Disable **Enable Component** during the scale-out.



Step 2 Upload **MRS_Log4j_Patch.tar.gz** to the **/home/omm** directory on the active OMS node. For details, see **How Do I Upload a Local File to a Node Inside a Cluster?**.

Step 3 Run the following commands to log in to the active OMS node as user **root**, modify the permission of the patch tool, switch to user **omm**, and decompress the patch tool package to the current directory:

chown omm:wheel -R /home/omm/MRS_Log4j_Patch.tar.gz

su - omm

cd /home/omm

tar -zxf MRS_Log4j_Patch.tar.gz

Step 4 In the **/home/omm/MRS_Log4j_Patch/bin/ips.ini** file, configure the IP addresses (IP addresses of the new nodes in the current cluster) of the nodes where the patch is to be installed.

NOTE

Configure one IP address in each line. No empty line is allowed.

Step 5 Run the following scripts to install the patch:

cd /home/omm/MRS_Log4j_Patch/bin

nohup sh install.sh upgrade &

Run the **tail -f nohup.out** command to check the execution status. If "upgrade patch success." is displayed, the execution is complete.

Step 6 Log in to Manager and start instances on the new node.

----End

Uninstalling the Patch

Step 1 Log in to the active OMS node as user **root** and run the following commands to uninstall the patch:

su - omm

cd /home/omm/MRS_Log4j_Patch/bin

nohup sh install.sh rollback &

Run the **tail -f nohup.out** command to check the execution status. If "rollback patch success." is displayed, the execution is complete.

Step 2 Log in to Manager, restart the affected components (you are advised to perform this operation during off-peak hours). For details, see **List of Affected Components**.

Step 3 Perform the following operation if you have performed **Step 6** in **Installing the Patch on Existing Cluster Nodes** during patch installation and you want to roll back the modification in the component package:

Log in to the active OMS node as user **root** and run the following commands:

su - omm

cd /home/omm/MRS_Log4j_Patch/bin

nohup sh install.sh rollback_package &

Run the **tail -f nohup.out** command to check the execution status. If "rollback_package patch success." is displayed, the execution is complete.

----End

(Optional) Upgrading the ECS Password Reset Plug-in

Huawei Cloud ECS provides the one-click password reset function. If the password of an ECS is lost or expires, you can use this function to reset the password with a few clicks. The password reset plug-in is a client process running in the ECS and does not provide any external network services. The password reset plug-in CloudResetPwdUpdateAgent uses the Apache Log4j2 component. According to the analysis and verification of Huawei Cloud security lab, the ECS password reset plug-in has no security risks.

To upgrade the Log4j2 version of this plug-in, perform the following steps:

Step 1 Upload **MRS_Log4j_Patch.tar.gz** to the **/home/omm** directory on the active OMS node. For details, see **How Do I Upload a Local File to a Node Inside a Cluster?**.

Step 2 Run the following commands to log in to the active OMS node as user **root**, modify the permission of the patch tool, switch to user **omm**, and decompress the patch tool package to the current directory:

chown omm:wheel -R /home/omm/MRS_Log4j_Patch.tar.gz

su - omm

cd /home/omm

tar -zxf MRS_Log4j_Patch.tar.gz

Step 3 In the **/home/omm/MRS_Log4j_Patch/bin/ips.ini** file, configure the IP addresses (IP addresses of all nodes in the current cluster) of the nodes where the patch is to be installed.

NOTE

Configure one IP address in each line. No empty line is allowed.

Step 4 Perform the following steps based on the node login mode:

- **Password login**

  Run the following command:

  nohup sh install.sh upgrade_resetpwdagent passwd:*Login password* **&**

  For example, if the password is **xyz123**, run the following command:

  nohup sh install.sh upgrade_resetpwdagent passwd:xyz123 &

  Run the **tail -f nohup.out** command to check the execution status. If "upgrade_resetpwdagent patch success." is displayed, the execution is complete.

- **Key login**

  a. Upload the private key file of user **root** to the **/home/omm/MRS_Log4j_Patch/bin** directory and ensure that the owner group of the file is **root:root**. Then, run the following commands:

     chown root:root /home/omm/MRS_Log4j_Patch/bin/*Key file*

     chmod 644 /home/omm/MRS_Log4j_Patch/bin/*Key file*

  b. Run the following commands:

     su - omm

     cd /home/omm/MRS_Log4j_Patch/bin

     nohup sh install.sh upgrade_resetpwdagent privatekey:*Path of the private key file &*

     For example, if the private key file path is **/home/omm/MRS_Log4j_Patch/bin/abc.pem**, run the following command:

     nohup sh install.sh upgrade_resetpwdagent privatekey:/home/omm/MRS_Log4j_Patch/bin/abc.pem &

     Run the **tail -f nohup.out** command to check the execution status. If "upgrade_resetpwdagent patch success." is displayed, the execution is complete.

----End

List of Affected Components

MRS Cluster Version	Affected Component
MRS 3.1.1	Hive, Oozie, Flink, Ranger, and Tez
MRS 3.1.0	Hive, Flink, Spark, Tez, Impala, Ranger, Presto, and Oozie

MRS Cluster Version	Affected Component
MRS 3.0.5	Hive, Flink, Spark, Tez, Impala, Ranger, Presto, Oozie, Storm, and Loader
MRS 3.0.2	Hive, Flink, Spark, Tez, Ranger, Oozie, Storm, and Loader
MRS 2.1.1	Hive, Tez, Storm, Loader, Impala, and Presto
MRS 2.1.0	Loader, Hive, Storm, Presto, Impala, Tez, Spark, and HBase
MRS 1.9.3	Loader, Hive, Tez, Spark, and Flink
MRS 1.9.2	Loader, Hive, Tez, Spark, Flink, and Impala
MRS 1.9.0	Loader, Hive, Spark, and Flink
MRS 1.8.10	Loader and Storm
MRS 1.7.1	Loader and Storm

1.2 MRS Fastjson Vulnerability Remediation Guide

1.2.1 Overview

Symptom

A deserialization remote code execution vulnerability is disclosed in Fastjson 1.2.80 and earlier versions. An attacker can use this vulnerability to bypass the autoType restriction so that they can remotely execute any code.

Impact and Risk

If a service with a vulnerability is attacked, attackers may remotely execute arbitrary code on the service platform.

Preventive Measures and Suggestions

Before any solution is proposed, you are advised to take the following preventive measures:

1. Harden security borders of physical devices to prevent direct access from external networks and attacks to the internal network management plane.
2. Check whether each component node of the platform uses the default password. If yes, change the password.
3. Strengthen the management of account and passwords on the management plane to ensure that the information is not disclosed or spread.
4. Some security vendors have provided preventive measures for this vulnerability. Set blocking rules on the security devices to prevent such attacks.

1.2.2 Impact

Version Involved

MRS 3.x

Involved Modules

- Management plane: This vulnerability is not involved.
- Tenant plane: Manager (Web+Controller+nodeagent), Kafka, and Flink

NOTE

- For MRS 3.1.0.*x*, perform the operations in the following sections:
  - **Remediating Manager Web**
  - **Remediating Manager Controller**
  - **Remediating Manager NodeAgent**
- For MRS 3.1.2.*x*, perform the operations in the following sections:
  - **Remediating Manager Web**
  - **Remediating Manager Controller**
  - **Remediating Manager NodeAgent**
  - **Remediating Kafka**
  - **Remediating Flink**

1.2.3 Remediating Manager Web

Prerequisites

You have obtained the URL and admin account for logging in to FusionInsight Manager.

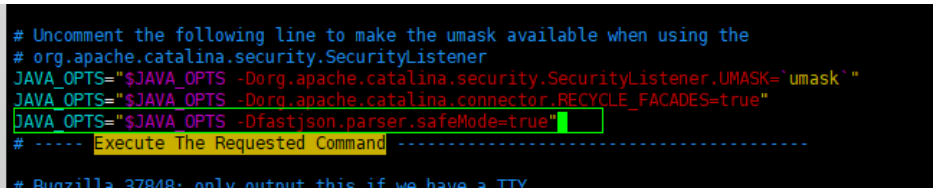
Procedure

Step 1 Log in to the active OMS node as user **omm** and back up the **$OM_TOMCAT_HOME/bin/catalina.sh** file.

cp $OM_TOMCAT_HOME/bin/catalina.sh /tmp

Step 2 Run the **vi $OM_TOMCAT_HOME/bin/catalina.sh** command, find the line where **Execute The Requested Command** is located, and add the following content above the line:

```
JAVA_OPTS="$JAVA_OPTS -Dfastjson.parser.safeMode=true"
```



Step 3 Run the following commands on the active OMS node as user **omm** to restart the Manager Web service:

$OMS_RUN_PATH/workspace/ha/module/harm/plugin/script/tomcat stop

$OMS_RUN_PATH/workspace/ha/module/harm/plugin/script/tomcat start

Step 4 Run the following command to check the process on the active OMS node:

ps -ef |grep tomcat | grep om-server

If the **-Dfastjson.parser.safeMode=true** parameter exists, the vulnerability has been mitigated.

Step 5 Perform **1** and **2** on the standby OMS node as user **omm**.

----End

1.2.4 Remediating Manager Controller

Prerequisites

You have obtained the URL and admin account for logging in to FusionInsight Manager.

Procedure

Step 1 Log in to the active OMS node as user **omm** and back up the **$CONTROLLER_HOME/sbin/controller.sh** file.

cp $CONTROLLER_HOME/sbin/controller.sh /tmp

Step 2 Run the **vi $CONTROLLER_HOME/sbin/controller.sh** command, find the line where **JVM_ARGS=** is located, and add the following content below the line:

```
JVM_ARGS="$JVM_ARGS -Dfastjson.parser.safeMode=true"
```

Step 3 Run the following commands on the active OMS node as user **omm** to restart the Manager Controller service:

sh /opt/Bigdata/om-server/om/sbin/restart-controller.sh

Step 4 Run the following command to check the process on the active OMS node:

ps -ef |grep ControllerService

If the **-Dfastjson.parser.safeMode=true** parameter exists, the vulnerability has been mitigated.

Step 5 Repeat **1** and **2** on the standby OMS node as user **omm**.

----End

1.2.5 Remediating Manager NodeAgent

Prerequisites

You have obtained the URL and admin account for logging in to FusionInsight Manager.

Procedure

Step 1 Log in to the active OMS node as user **omm** and back up the **$NODE_AGENT_HOME/bin/nodeagent_ctl.sh** file.

cp $NODE_AGENT_HOME/bin/nodeagent_ctl.sh /tmp

Step 2 Run the **vi $NODE_AGENT_HOME/bin/nodeagent_ctl.sh** command, find the line where **JVM_ARGS=** is located, and add the following content below the line:

```
JVM_ARGS="$JVM_ARGS -Dfastjson.parser.safeMode=true"
```

Step 3 Perform **1** and **2** on all nodes in the cluster.

You can manually overwrite the modified **$NODE_AGENT_HOME/bin/nodeagent_ctl.sh** file on all nodes as user **omm**.

Step 4 Run the following command on the active OMS node as user **omm** to restart all NodeAgents in the cluster:

$CONTROLLER_HOME/inst/restartAllNoes.sh

Step 5 Log in to the cluster node to check the process.

ps -ef |grep NodeAgent

If the **-Dfastjson.parser.safeMode=true** parameter exists, the vulnerability has been mitigated.

----End

1.2.6 Remediating Kafka

Prerequisites

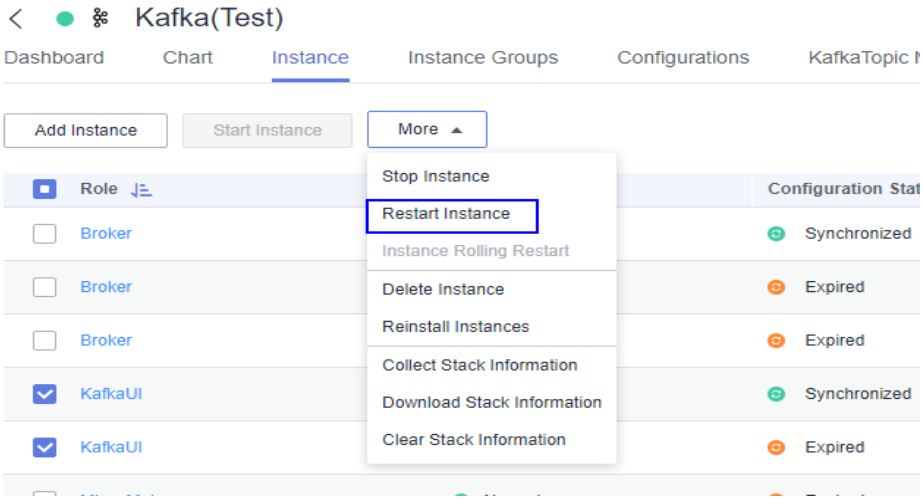
You have obtained the URL and admin account for logging in to FusionInsight Manager.

Procedure

Step 1 Log in to FusionInsight Manager and choose **Cluster** > **Services** > **Kafka**. Click **Configurations** then **All Configurations**. On this sub-tab page, search for the **KAFKAUI_HEAP_OPTS** parameter. Add **-Dfastjson.parser.safeMode=true** to the **Value** column of **KAFKAUI_HEAP_OPT** (leave a space between the existing value and **-Dfastjson.parser.safeMode=true**).

For example, if the existing value is **-Xmx4G -Xms4G**, the new value is **-Xmx4G -Xms4G -Dfastjson.parser.safeMode=true**.

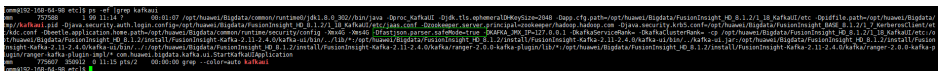
Step 2 Click **Save**. On the **Instance** tab page, select all KafkaUI instances and choose **More** > **Restart Instance**.



Step 3 Log in to any KafkaUI node as user **omm** and check the process:

ps -ef | grep KafkaUI

If the **-Dfastjson.parser.safeMode=true** parameter exists, the vulnerability has been mitigated.



----End

1.2.7 Remediating Flink

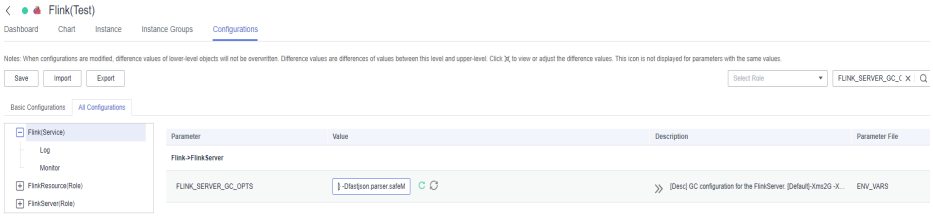
Prerequisites

You have obtained the URL and admin account for logging in to FusionInsight Manager.

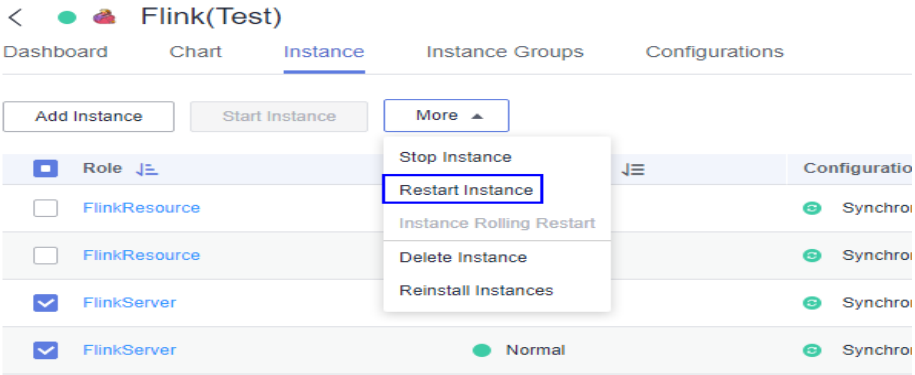
Procedure

Step 1 Log in to FusionInsight Manager and choose **Cluster** > **Services** > **Flink**. Click **Configurations** then **All Configurations**. On this sub-tab page, search for the **FLINK_SERVER_GC_OPTS** parameter, and add **-Dfastjson.parser.safeMode=true** to the **Value** column of **FLINK_SERVER_GC_OPTS**. (Leave a space between the existing value and **-Dfastjson.parser.safeMode=true**.)

For example, if the existing value is *xxx*, the new value is *xxx* **-Dfastjson.parser.safeMode=true**.



Step 2 Click **Save**. On the **Instance** tab page, select all FlinkServer instances and choose **More** > **Restart Instance**.



Step 3 Log in to any FlinkServer node as user **omm** and check the process:

ps -ef | grep FlinkServer

If the **-Dfastjson.parser.safeMode=true** parameter exists, the vulnerability has been mitigated.

----End

2 Version Support Bulletin

2.1 MRS Cluster Version Lifecycle

Version Description

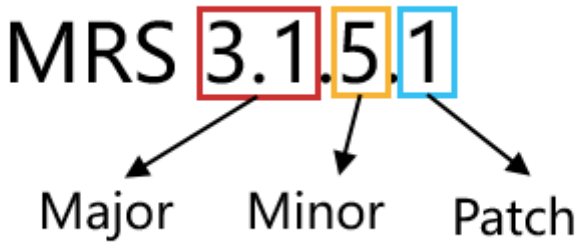
MRS allows you to create clusters of two editions: normal and LTS.

- **Version number of the normal edition**: The format is **a.b.c.d**.

  a.b indicates the major version, **c** indicates the minor version, and **d** indicates the patch version. For example, MRS 3.1.5.1.

  - **a** indicates great changes among major versions.
  - **b** indicates component changes.
  - **c** indicates minor changes, which are forward compatible.
  - **d** indicates the patch version, which is used to rectify faults.

  Figure 2-1 MRS normal cluster version



- **Version number of the LTS edition:** The format is **a.b.c-LTS.d**.

  a.b indicates the major version, **c** indicates the minor version, and **d** indicates the patch version. For example, MRS 3.2.0-LTS.1.

  - **a** indicates great changes among major versions.
  - **b** indicates component changes.
  - **c** indicates minor changes, which are forward compatible.
  - **d** indicates the patch version, which is used to rectify faults.

Figure 2-2 MRS LTS cluster version

Version Support

- **Cluster creation**

  MRS allows you to create two major versions of the same edition.

  For example, you can create clusters of MRS 3.3.0-LTS and MRS 3.2.0-LTS. After MRS 3.3.0-LTS is available for commercial use, clusters of MRS 3.1.x-LTS and earlier versions cannot be created on the console by default. Created MRS 3.1.2-LTS clusters are not affected.

- **Cluster version upgrade**

  The MRS LTS edition supports major version upgrade. By default, only one-major-version upgrade is supported. For example, MRS 3.1.2-LTS can be upgraded to MRS 3.2.0-LTS, and MRS 3.2.0-LTS can be upgraded to MRS 3.3.0-LTS.

- **Cluster patch upgrade**

  If MRS clusters running on the live network have major issues or vulnerabilities in the open-source big data components, you can install patches for these clusters. For details, see **MRS Patch Description**.

Version Constraints

- After a cluster is upgraded, it cannot be rolled back to an earlier version.
- Clusters of the normal edition cannot be upgraded.

Version Release Cycle/Version Lifecycle

Table 2-1 Common terms about version lifecycle

Term	Definition
End of marketing (EOM)	The deployment of a cloud service version is stopped and the cloud service version is no longer deployed on the live network.
End of Full Support (EOFS)	The fixing of common software bugs in a specified cloud service version stops. The support covers only the fixing of mission-critical issues and security issues and the necessary upgrades.

Term	Definition
End of Service (EOS)	The cloud service version is no longer used. The live network version needs to be upgraded to the latest cloud service version.

For a newly released MRS version, the EOM date is two years later, the EOFS date is one year after EOM, and the EOS date is half a year after EOFS.

For example, if MRS 3.3.1-LTS is released on March 30, 2024, its EOM date is March 30, 2026, EOFS date is March 30, 2027, and EOS date is September 30, 2027.

Table 2-2 Version lifecycle of the MRS normal edition

Version	Status	Release Date	EOM Date	EOFS Date	EOS Date
MRS 1.3.x	EOS	2017.3.30	2019.3.30	2020.3.30	2020.9.30
MRS 1.5.x	EOS	2017.9.30	2019.9.30	2020.9.30	2021.3.30
MRS 1.6.x	EOS	2019.6.21	2021.6.21	2022.6.21	2022.12.30
MRS 1.7.x	EOS	2019.12.22	2021.12.22	2022.12.22	2023.6.22
MRS 1.8.x	EOS	2019.11.21	2021.11.21	2022.11.21	2023.5.21
MRS 1.9.x	**EOS**	**2020.3.8**	**2022.3.8**	**2023.3.8**	**2023.9.8**
MRS 2.0.x	EOS	2019.10.11	2021.10.11	2022.10.11	2023.4.11
MRS 2.1.x	**EOS**	**2019.11.13**	**2021.11.13**	**2022.11.13**	**2023.5.13**
FusionInsight 6.5.1	EOS	2020.6.30	2022.6.30	2023.6.30	2023.12.30
MRS 3.0.x	EOS	2020.9.28	2022.9.28	2023.9.28	2024.3.28
MRS 3.1.0	**EOFS**	**2021.5.9**	**2023.5.9**	**2024.5.9**	**2024.11.9**
MRS 3.1.1	EOFS	2021.6.28	2023.6.28	2024.6.28	2024.12.28
MRS 3.1.2	EOM	2022.1.27	2024.1.27	2025.1.27	2025.7.27
MRS 3.1.5	**Released**	**2023.3.28**	**2025.3.28**	**2026.3.28**	**2026.9.28**

NOTE

The versions in bold in the preceding table are the mainstream versions available on the entire cloud platform. Other versions are opened for whitelist users only. To join in the whitelist, contact technical support.

Table 2-3 Version lifecycle of the MRS LTS edition

Version	Status	Release Date	EOM Date	EOFS Date	EOS Date
MRS 3.1.0-LTS	**EOFS**	**2021.3.26**	**2023.3.26**	**2024.3.26**	**2024.9.26**
MRS 3.1.1-LTS	EOFS	2021.6.28	2023.6.28	2024.6.28	2024.12.28
MRS 3.1.2-LTS	**Released**	**2022.6.2**	**2024.6.2**	**2025.6.2**	**2025.12.2**
MRS 3.1.3-LTS	Released	2023.5.12	2025.5.12	2026.5.12	2026.11.12
MRS 3.2.0-LTS	**Released**	**2023.4.27**	**2025.4.27**	**2026.4.27**	**2026.10.27**
MRS 3.3.0-LTS	Released	2023.10.13	2025.10.13	2026.10.13	2027.4.13

NOTE

The versions in bold in the preceding table are the mainstream versions available on the entire cloud platform. Other versions are opened for whitelist users only. To join in the whitelist, contact technical support.

Remarks

The EOS date of historical versions is earlier than August 30, 2024. Versions that have reached their EOS dates will still be provided until August 30, 2024. That is, these versions will not be available after August 30, 2024.

Recommended Action After Version EOX

- Version upgrade: The MRS LTS edition supports in-place version upgrade. You can perform an upgrade based on the specific version upgrade path.
- Cluster migration: The MRS normal edition does not support in-place upgrade. You need to migrate clusters to the latest version.

