Intelligent EdgeFabric

FAQ

Issue 01

Date 2021-01-21



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2021. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions


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

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

Contents

1 Edge Node FAQs....1
1.1 What Do I Do If an Edge Node Is Faulty?....1
1.2 What Are the Fault Scenarios of Edge Nodes?....7
1.3 What Do I Do If Edge Node Management Fails?....7
1.4 What Do I Do If an Error Occurs During GPU Driver Installation?....15
1.5 How Do I Obtain the Latest Device Properties After Device Properties Are Updated?....16
1.6 What Operations Can I Perform After a Device Is Associated with a Node?....16
1.7 Does an Edge Node Support Multiple GPUs?....16
1.8 Can I Change the GPU on a Running Edge Node?....17
1.9 How Is Edge Environment Security Protected?....17
1.10 Why Cannot I View Monitoring Data on an Edge Node?....18
1.11 How Can I Restore a Deleted Edge Node?....19
1.12 What Is the Impact of IP Address Changing on an Edge Node?....19
1.13 What Do I Do If the NTP Configuration Cannot Be Modified?....19
1.14 How Do I Synchronize Time with the NTP Server?....20
1.15 How Do I Obtain the IP Addresses of IEF Cloud Services?....21
2 Edge Application FAQs....23
2.1 What Do I Do If an Application Fails to Be Delivered to an Edge Node?....23
2.2 What Do I Do If a Containerized Application Fails to Be Started on an Edge Node?....26
2.3 What Do I Do If a Containerized Application Fails to Be Upgraded?....30
2.4 What Do I Do If a Container Image Fails to Be Pulled?....31
2.5 Why Cannot I View Application Logs and System Logs?....35
2.6 How Do I Know Whether a Function Is Successfully Executed?....36
2.7 What Can I Do If a Function Fails to Start?....36
2.8 Why Do I Need to Use nvidia-gpu-installer.sh to Install the GPU Driver? What Is the Difference Between This Method and the Method of Installing the GPU Driver in the OS?....37
2.9 How Do Applications Schedule GPU Resources?....37
2.10 How Do I Control the Disk Space Occupied by a Container Engine?....38
3 Edge-Cloud Message FAQs....39
3.1 What Is Route Management?....39
3.2 What Is an Endpoint in Route Management?....39
3.3 What Is a Route?....39
3.4 Why Does a Route Fail to Be Created?....39

 Copyright © Huawei Technologies Co., Ltd.

3.5 What Can I Do If a Message Fails to Be Forwarded over a Route? 40
3.6 What Is the Impact of Disabling a Route? 40
4 Network Management FAQs 41
4.1 How Does an Edge Node Connect to IEF? 41
4.2 What Additional Settings Are Required If the Proxy Is Enabled? 41
5 Basic Concept FAQs 43
5.1 What Is Intelligent EdgeFabric? 43
5.2 What Benefits Does IEF Bring? 43
5.3 What Are the Main Application Scenarios of IEF? 43
5.4 What Is Edge Function? 44
5.5 What Is Function Dependency? What Is the Relationship Between the Dependency and Functions? 44
5.6 What Functions Are Supported by IEF? 44
5.7 What Are the Function Running Modes (Remote Control and Long-term Running)? 44
6 Others 45
6.1 Region and AZ 45
6.2 What Are the Specifications of Edge Nodes Supported by IEF? 46
6.3 What Are the Application Scenarios of Functions and Containers? 48
6.4 What Are the Differences Between Device Properties and Device Twins? 48
6.5 What Programming Language Is Required for IEF Development? 48
6.6 Do I Need to Prepare Edge Nodes by Myself? 48
6.7 Can I Still Use the Previously Delivered Applications After My Account Is in Arrears? 48
6.8 What Are the Differences Between IEF and IoT Edge? 49
6.9 How Do I Configure IEF Permissions for an IAM User? 49
6.10 What Do I Do If an Agency Fails to Be Automatically Created? 50

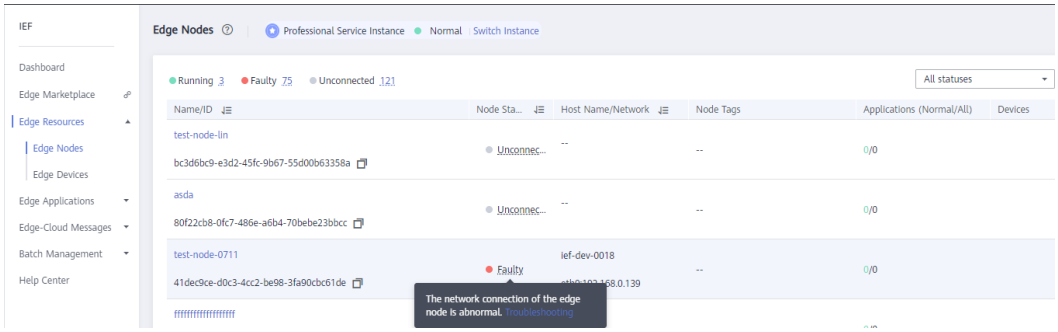
 Copyright © Huawei Technologies Co., Ltd.

1 Edge Node FAQs

1.1 What Do I Do If an Edge Node Is Faulty?

Symptom

An edge node is in the **Faulty** state, and the fault cause is displayed when the cursor is hovered over Faulty.



Fault Locating

Locate the cause of the edge node fault as follows.

 Copyright © Huawei Technologies Co., Ltd.

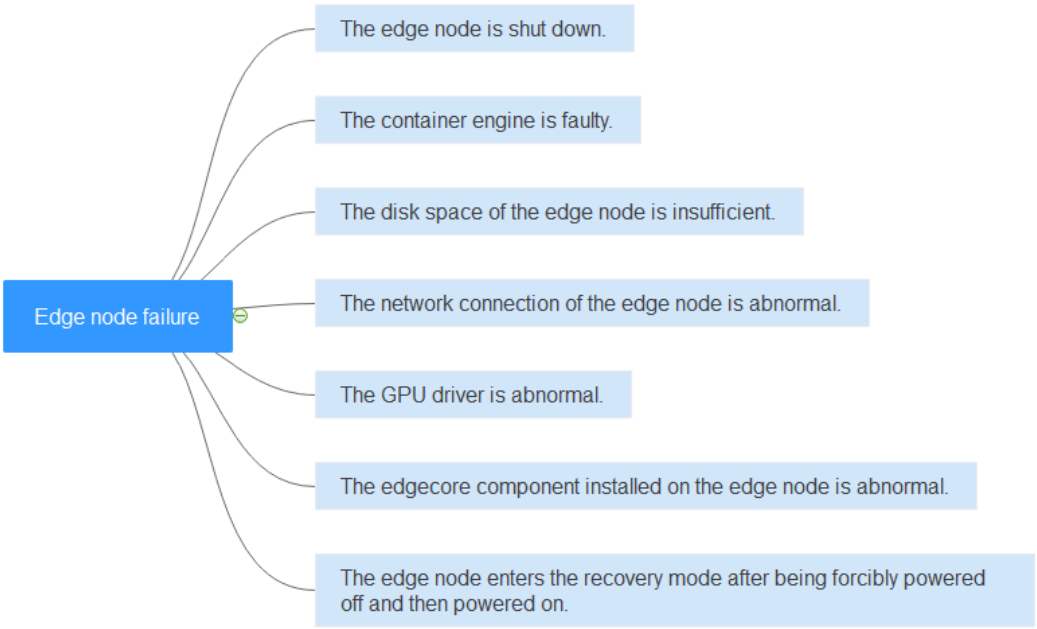


Table 1-1 Fault locating

Possible Cause	Solution
The edge node is shut down.	**Edge Node Is Shut Down**
A container engine fault occurs, for example, the container engine is not started or the container engine service is abnormal.	**Local Container Engine of the Edge Node Is Abnormal**
The node disk space is insufficient.	• **Container Disk Space of the Edge Node Is Insufficient** • **/opt/IEF Disk Space of the Edge Node Is Insufficient** • **/var/IEF/sys/log Disk Space of the Edge Node Is Insufficient**
The network connection of the edge node is abnormal.	**Network Connection of the Edge Node Is Abnormal**
The GPU driver is abnormal.	**GPU Driver Is Abnormal**
The edgecore component installed on the edge node is abnormal.	**edgecore Is Abnormal**

 Copyright © Huawei Technologies Co., Ltd.

Possible Cause	Solution
The edge node enters the recovery mode after being forcibly powered off and then powered on.	System Enters the Recovery Mode

Edge Node Is Shut Down

When the edge node is shut down, it cannot report its status to IEF. In this case, IEF determines that the edge node is faulty. Therefore, keep the edge node running.

CAUTION

IEF is billed by the number of edge applications instead of the number of edge nodes. If an edge node is faulty, the edge applications deployed on this node still incur charges even if they are in the abnormal state. Therefore, if you do not need to use services temporarily, delete the corresponding applications from IEF instead of stopping the edge node.

Local Container Engine of the Edge Node Is Abnormal

The startup and running of the IEF core component (edgecore) depend on the container engine. Therefore, if the container engine is abnormal, the edgecore component cannot be started.

Solution

1. Run **docker version** to check whether the container engine is normal. If the container engine is abnormal, run **systemctl restart docker** to restart it.
2. Run **docker ps** to check whether the container engine is available. If the container engine is not available, restart or reinstall it.

CAUTION

Do not forcibly power off the edge node. Otherwise, data files on the edge node may be lost or damaged, which can cause node faults.

Container Disk Space of the Edge Node Is Insufficient

Solution

1. Log in to the edge node. Run the following command to check the usage of the disk mounted to the container running on the edge node:

   df -h

 Copyright © Huawei Technologies Co., Ltd.

2. Delete unnecessary files to release the disk space.

   rm *File name*

/opt/IEF Disk Space of the Edge Node Is Insufficient

Solution

1. Log in to the edge node. Run the following command to check the usage of the disk space allocated to **/opt/IEF**:

   df -h

2. Delete unnecessary files to release the disk space.

   rm *File name*

/var/IEF/sys/log Disk Space of the Edge Node Is Insufficient

Solution

1. Log in to the edge node. Run the following command to check the usage of the disk space allocated to **/var/IEF/sys/log**:

   df -h

2. Delete unnecessary files to release the disk space.

   rm *File name*

Network Connection of the Edge Node Is Abnormal

Identification Method

1. Run the following command on the edge node to obtain the IP address for accessing IEF:

   cat /opt/IEF/Edge-core/conf/edge.yaml | grep ws-url

   Information similar to the following is displayed:

   ```
   ws-url: wss://ief2-edgeaccess.cn-north-4.myhuaweicloud.com:443/
   ```

   In the preceding command output, **9911beac-7a98-455f-98ad-bca7a96eb4b7.cn-dg-1.huaweiief.com** indicates the address to be obtained. The address varies depending on the region.

2. Run the **curl** command to check whether the edge node can connect to IEF.

   curl -i -v -k https://ief2-edgeaccess.cn-north-4.myhuaweicloud.com

   - If no command output is displayed, the network between the edge node and IEF is disconnected.
   - If the information similar to the following is displayed, the network connection is normal:

     ```
     * About to connect() to ief2-edgeaccess.cn-north-4.myhuaweicloud.com port 443 (#0)
     * About to connect() to 9911beac-7a98-455f-98ad-bca7a96eb4b7.cn-dg-1.huaweiief.com (#0)
     *   Trying 49.4.115.239...
     * Connected to ief2-edgeaccess.cn-north-4.myhuaweicloud.com (*.*.*.*) port 443 (#0)
     * Initializing NSS with certpath: sql:/etc/pki/nssdb
     * skipping SSL peer certificate verification
     * NSS: client certificate not found (nickname not specified)
     * SSL connection using TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
     * Server certificate:
     * subject: OID.1.1.1.4=42701fe87611496e80c824778c9857ca,OID.
     1.1.1.3=op_svc_ief_container1:88125631e95e4d3fbdfa7e6ced0f9dd4,OID.1.1.1.2=cn-
     ```

 Copyright © Huawei Technologies Co., Ltd.

```
north-4:42701fe8761
1496e80c824778c9857ca:op_cfe_kubelet,OID.
1.1.1.1=op_svc_ief_container1,CN=paas.placement.certs.secret OSS3.0 CA,OU=OSS & Service
Tools Dept,O="Huawei Technologies
Co., Ltd",L=ShenZhen,ST=GuangDong,C=CN
* start date: Apr 29 16:00:00 2019 GMT
* expire date: Apr 29 16:00:00 2049 GMT
* common name: paas.placement.certs.secret OSS3.0 CA
> GET / HTTP/1.1
.....
```

Possible Causes and Solutions

1. The domain name resolution is abnormal.

   Run the following command to check whether the domain name can be resolved:

   ping ief2-edgeaccess.cn-north-4.myhuaweicloud.com

   If the domain name cannot be resolved into an IP address, run the following command to check whether the DNS server configuration was modified:

   cat /etc/resolv.conf

   Solution:

   - Configure a correct DNS server. The DNS server with IP address 114.114.114.114 is recommended.
   - Obtain the correct IP address resolved from the domain name, and configure the IP address in the host file to temporarily work around this problem.

2. A proxy problem occurs.

   If the proxy mode is used, check whether the proxy is correctly configured.

   - Check whether a proxy is configured for the edge node.

     Run the following commands:

     env| grep proxy

     env| grep PROXY

   - Check whether a proxy is configured for edgecore.

     Run the following command:

     cat /opt/IEF/Cert/user_config | grep PROXY

   If the proxy mode is not used, run the preceding commands to check that the proxies are configured.

3. The network connection is not stable.

   Check whether the network connection of the edge node is normal and stable. If the network connection is unstable, the edge node status switches between **Faulty** and **Running**.

GPU Driver Is Abnormal

Solution

Check whether the GPU driver can be properly loaded.

lsmod |grep -e nvidia -e nvidia-uvm

If the command output contains the following three lines or the first two lines of information, the GPU driver is completely installed.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-1 Command output

```
root@huawei:/home/huawei# lsmod |grep -e nvidia -e nvidia-uvm
nvidia_uvm            786432  0
nvidia              14032896  1 nvidia_uvm
ipmi_msghandler        53248  2 ipmi_devintf,nvidia
```

/var/IEF/nvidia/bin/nvidia-smi

Figure 1-2 Successful installation of the GPU driver

```
root@ecs-ocr:/lib/modules/4.4.0-104-generic/kernel/drivers/video# nvidia-smi
Tue Aug 28 10:07:54 2018
+-----------------------------------------------------------------------------+
| NVIDIA-SMI 384.81                 Driver Version: 384.81                    |
|-------------------------------+----------------------+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
|===============================+======================+======================|
|   0  Tesla P4            Off  | 00000000:00:0C.0 Off |                    0 |
| N/A   36C    P0    24W /  75W |      0MiB /  7606MiB |      0%      Default |
+-------------------------------+----------------------+----------------------+
|   1  Tesla P4            Off  | 00000000:00:0D.0 Off |                    0 |
| N/A   35C    P0    23W /  75W |      0MiB /  7606MiB |      0%      Default |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                       GPU Memory |
|  GPU       PID   Type   Process name                             Usage      |
|=============================================================================|
|  No running processes found                                                 |
+-----------------------------------------------------------------------------+
```

If the GPU driver is not properly installed, install it by following the procedure described in **Installing a GPU Driver**.

edgecore Is Abnormal

Check whether the edgecore status is normal.

systemctl status edgecore

If the edgecore component is faulty, the possible causes are as follows:

- Port 8883 or 1883 is occupied.

  Check whether port 8883 or 1883 of your edge node is occupied. If port 8883 or 1883 is occupied, release the port and run the **systemctl restart edgecore** command to restore edgecore.

- The container engine is abnormal.

  Run **systemctl status docker** to check whether the container engine is normal. If the container engine is abnormal, run **systemctl restart docker** to restart it.

- A firewall issue. For details, see **Port 8883 Is Disabled by the Firewall**.

System Enters the Recovery Mode

If an edge node is forcibly powered off and then powered on, there is a possibility that the system enters the recovery mode. Check whether the **/opt/IEF** directory is normal. If any file in this directory is lost, the edge node will be faulty.

The **/opt/IEF** directory is abnormal if any of the following errors occurs:

The **systemctl status edgecore** command output indicates that the edgecore status is abnormal, and the **systemctl restart edgecore** command output indicates that the edgecore service does not exist.

 Copyright © Huawei Technologies Co., Ltd.

The **systemctl status edgelogger** command output indicates that the edgelogger status is abnormal, and the **systemctl restart edgelogger** command output indicates that the edgelogger service does not exist.

The **systemctl status edgemonitor** command output indicates that the edgemonitor status is abnormal, and the **systemctl restart edgemonitor** command output indicates that the edgemonitor service does not exist.

Solution

Start your edge node in normal mode. If an edge node is powered off abnormally, files on the edge node may be damaged or lost. Therefore, do not perform this operation. If this fault occurs, **submit a service ticket**.

1.2 What Are the Fault Scenarios of Edge Nodes?

An edge node has the following fault scenarios:

- Container engine fault, for example, container engine not started or container engine service exception
- Insufficient node disk space
- Network connection failure
- GPU driver exception

1.3 What Do I Do If Edge Node Management Fails?

Symptom

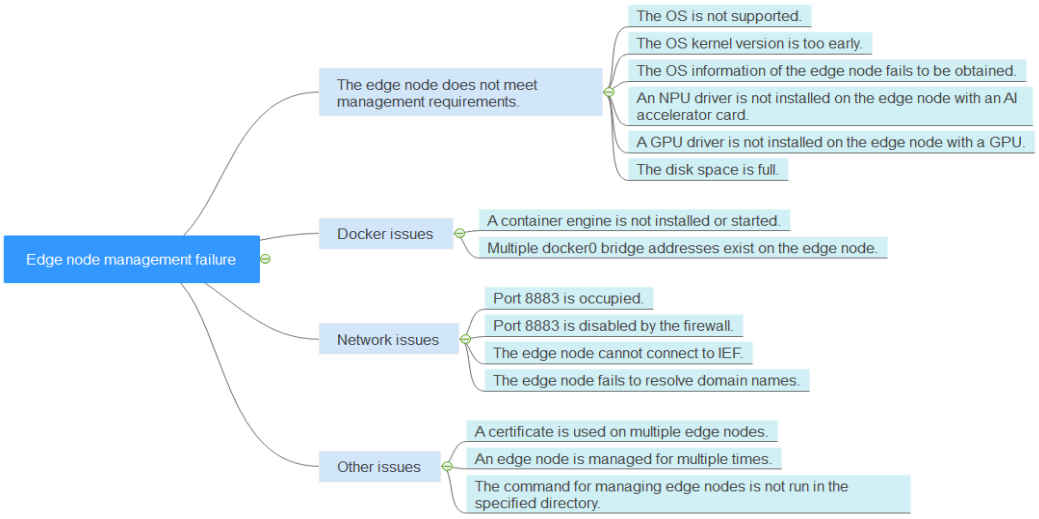
The edge node cannot be managed on IEF.

Fault Locating

There are many causes for edge node management failures. The most common cause is that the edge node does not meet management requirements of IEF or the network is inaccessible. Follow the steps in the following figure to locate the cause of the edge node management failure.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-3 Fault locating



You can run edgectl to check whether the edge node meets the management requirements. Before running edgectl, check whether the edgectl package exists in the **/opt/edge-installer** directory.

- If the package exists, you do not need to download it again.
- If the package does not exist, log in to the IEF console and download the tool of the corresponding version, for example, **edgectl_*x.x.x_x*_x86_64.tar.gz**, from **Edge O&M Tool** on the right of the **Dashboard** page. Then, decompress the package in the **/opt/edge-installer** directory.

Run the following commands to check whether the edge node meets the management requirements:

chmod +x /opt/edge-installer/edgectl

./opt/edge-installer/edgectl diagnose installation

- If the edge node does not meet the requirements, information similar to the following is displayed. You can locate and rectify the fault based on the error code in the message. For details, see **Error Code Overview**.

```
Failed to get Docker version.
ERROR6102: Make sure that Docker is running.
For more information, see IEF documentation.

+--------------------------------+
| Installation diagnose failed. |
+--------------------------------+
```

- If the edge node meets the requirements, the following information is displayed: In this case, you can continue to locate the fault based on **Table 1-2**.

```
+---------------------------------+
| Installation diagnose succeed. |
+---------------------------------+
```

 Copyright © Huawei Technologies Co., Ltd.

Table 1-2 Fault locating

Possible Cause	Solution
The edge node does not meet management requirements.	**Edge Node Does Not Meet Management Requirements** **OS Is Not Supported** **OS Kernel Version Is Too Early** **OS Information of the Edge Node Fails to Be Obtained** **NPU Driver Is Not Installed on the Edge Node with an AI Accelerator Card** **GPU Driver Is Not Installed on the Edge Node with a GPU** **Disk Space Is Full**
Docker issues	**Container Engine Is Not Installed or Started** **Multiple docker0 Bridge Addresses Exist on the Edge Node**
Network issues	**Port 8883 Is Occupied** **Port 8883 Is Disabled by the Firewall** **Edge Node Cannot Connect to IEF** **Edge Node Fails to Resolve Domain Names**
Other issues	**A Certificate Is Used on Multiple Edge Nodes** **An Edge Node Is Managed for Multiple Times** **Command for Managing Edge Nodes Is Not Run in the Specified Directory**

Edge Node Does Not Meet Management Requirements

Edge Agent can be installed only on edge nodes that meet requirements listed in **Table 1-3**.

Table 1-3 Edge node requirements

Item	Specifications
OS	• x86_64 architecture Ubuntu 16.04 LTS (Xenial Xerus), Ubuntu 18.04 LTS (Bionic Beaver), CentOS 7.x and RHEL 7.x, Kylin 4.0.2, NewStart CGSL v5.5, and NeoKylin v7.0 • Armv7i (Arm32) architecture Raspbian GNU/Linux 9 (stretch) • AArch64 (Arm64) architecture Ubuntu 18.04.2 LTS (Bionic Beaver)
Memory	≥ 256 MB

 Copyright © Huawei Technologies Co., Ltd.

Item	Specifications
CPU	≥ 1 vCPU
Hard disk	≥ 1 GB
GPU (optional)	The GPU models on the same edge node must be the same. **NOTE** Currently, only NVIDIA GPUs, such as Tesla P4, P40, and T4, are supported. If a device equipped with GPU hardware is registered as an edge node, you can choose not to enable its GPUs.
Container engine (mandatory when containerized applications are deployed)	The Docker version must be later than 17.06. Docker 18.06.3 is recommended. (However, Docker 18.09.0 is not recommended as it has a serious bug. For details, see **https://github.com/docker/for-linux/issues/543**. If this version has been installed, upgrade it at the earliest possible opportunity. This issue has been resolved in Docker 18.09.0.60 embedded in Atlas 500 AI edge stations.) **NOTICE** After Docker is installed, configure the Docker process to start at host startup. This configuration prevents system exceptions caused by Docker startup failures after the host is restarted.
Glibc	The Glibc version must be later than 2.17.
Port	Edge nodes need to use the following ports. Ensure that these ports are available. • 8102: used for reporting edge node logs to AOM • 8149: used for reporting monitoring data of edge nodes to AOM • 8065: used for reporting edge node alarms to AOM • 443: used by edge nodes to interwork with IEF • 8883: used by the built-in MQTT Broker • 1883: port used by the external MQTT Broker • 20004: used by edge nodes to report messages to DIS

OS Is Not Supported

Check whether your OS is supported by IEF by referring to **Table 1-3**. Do not use the Linux OS of the Chinese edition.

OS Kernel Version Is Too Early

Check whether the OS and kernel version of your edge node meet the requirements described in **Table 1-3**.

 Copyright © Huawei Technologies Co., Ltd.

You can run the following commands to check whether your OS kernel version is too early:

sh /opt/edge-installer/conf/script/parse_user_config.sh node_id

If an error is reported, the OS kernel version is too early. Upgrade the kernel version or install an OS listed in **Table 1-3**, and then manage the edge node again.

OS Information of the Edge Node Fails to Be Obtained

View the IEF software installation logs. If the **os** field in the last line of the following output is empty, the OS information fails to be obtained.

```
2020-01-11 17:00:46.341 +08:00 DEBUG :0 init logger...
2020-01-11 17:00:46.341 +08:00 INFO config/config.go:45 New file source added for configuration: /opt/edge-installer/conf/config.yaml
2020-01-11 17:00:46.341 +08:00 INFO config/config.go:45 New file source added for configuration: /opt/edge-installer/conf/logging.yaml
2020-01-11 17:00:46.351 +08:00 INFO pkg/installer.go:24 start to install
2020-01-11 17:00:46.386 +08:00 INFO placementclient/placementclient.go:61 http_proxy:ProxyNotSet, https_proxy:ProxyNotSet
2020-01-11 17:00:46.437 +08:00 INFO httpclient/httpsclient.go:182 https_proxy:
2020-01-11 17:00:46.479 +08:00 INFO util/util.go:446 system cert file[/opt/IEF/Cert/system/sys_private_cert_crypto.crt] and system key file[/opt/IEF/Cert
/system/sys_private_cert_crypto.key] have been inited
2020-01-11 17:00:46.479 +08:00 INFO pkg/installer.go:46 ------------------install---------------
2020-01-11 17:00:46.479 +08:00 INFO deploy/bootstrap.go:48 install precheck success.
2020-01-11 17:00:46.479 +08:00 INFO deploy/bootstrap.go:54 install preprocess start
2020-01-11 17:00:46.479 +08:00 INFO deploy/deploy.go:39 install preprocess start
2020-01-11 17:00:46.501 +08:00 INFO util/util.go:192 get arch success
2020-01-11 17:00:46.502 +08:00 INFO util/util.go:216 os type is:"euleros"
2020-01-11 17:00:46.502 +08:00 INFO util/util.go:432 installer version [1.0.6]
2020-01-11 17:00:46.516 +08:00 INFO placementclient/placementclient.go:113 body : {"arch":"x86_64","installer_version":"1.0.6","os":"euleros"}
```

NPU Driver Is Not Installed on the Edge Node with an AI Accelerator Card

If you try to register an edge node of the AI accelerator card type, make sure that the edge node supports NPUs and has an NPU driver installed.

Run the following command on your edge node:

ls /dev/davinci_manager /dev/hisi_hdc /dev/davinci*

If the file does not exist, no NPU driver is installed. Install an NPU driver.

GPU Driver Is Not Installed on the Edge Node with a GPU

If you try to register an edge node of the GPU type, make sure that the edge node supports GPUs and has a GPU driver installed.

Check whether the GPU driver can be properly loaded.

lsmod |grep -e nvidia -e nvidia-uvm

If the command output contains the following three lines or the first two lines of information, the GPU driver is completely installed.

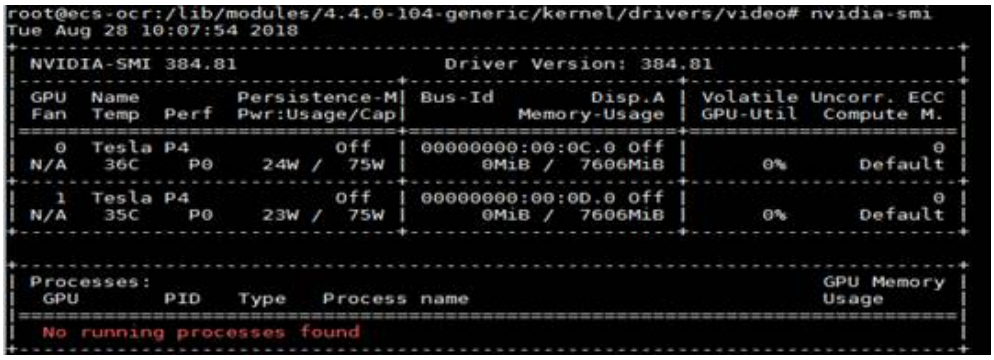
Figure 1-4 Command output

```
root@huawei:/home/huawei# lsmod |grep -e nvidia -e nvidia-uvm
nvidia_uvm            786432  0
nvidia              14032896  1 nvidia_uvm
ipmi_msghandler        53248  2 ipmi_devintf,nvidia
```

 Copyright © Huawei Technologies Co., Ltd.

/var/IEF/nvidia/bin/nvidia-smi

Figure 1-5 Successful installation of the GPU driver



If the GPU driver is not properly installed, install it by following the procedure described in **Installing a GPU Driver**.

Disk Space Is Full

The IEF software cannot be installed on the edge node if the disk space is full. Run the following command to check the disk space:

df -h

lsblk

Ensure that the disk usage of the following directories is not nearly 100%. For details about the disk space requirements, see **Table 1-3**.

- /opt/IEF
- /opt/edge-installer
- /opt/IEFpack
- /var/IEF

Container Engine Is Not Installed or Started

Run the following command to check whether a container engine is started:

systemctl status docker

- If the container engine information is not displayed, the container engine is not installed. Install a container engine based on the requirements listed in **Table 1-3**.
- If the container engine is not started, run the following command to start it:

  systemctl restart docker

  Check the container engine status again.
  - If the container engine is started properly, manage the edge node again.
  - If the container engine cannot be started, restore or reinstall it.

Multiple docker0 Bridge Addresses Exist on the Edge Node

Two docker0 bridge addresses are generated after a container with container engine GUI is used. As a result, the docker0 bridge registration fails when IEF is

 Copyright © Huawei Technologies Co., Ltd.

managing the edge node, causing an IEF software installation failure. To rectify the fault, delete the redundant docker0 bridge address and reinstall the IEF software on the edge node.

You can run the following command to query the docker0 bridge address:

ip addr show | grep docker0

If multiple IP addresses are displayed, multiple docker0 bridges exist. Retain the IP address starting with 172 and delete other redundant docker0 bridge addresses.

Port 8883 Is Occupied

Run the following command to check whether port 8883 is occupied:

netstat -npl | grep 8883

The IEF core component (edgecore) depends on port 8883. If port 8883 is occupied, the edgecore component fails to be installed.

After IEF is properly installed, the edgecore component listens at port 8883. Therefore, ensure that port 8883 is not occupied.

```
[root@chenyong-production-64981 zyl]# netstat -npl | grep 8883
tcp6       0      0 :::8883                 :::*                    LISTEN      7703/edge_core
[root@chenyong-production-64981 zyl]#
```

Port 8883 Is Disabled by the Firewall

Check the firewall status on the edge node.

systemctl status firewalld

firewall-cmd --state

In the command output, **notrunning** indicates that the firewall is disabled and **running** indicates that the firewall is enabled.

If the firewall is enabled, enable port 8883 or disable the firewall.

- To enable port 8883, run the following commands:
  firewall-cmd --add-port=8883/tcp --permanent
  systemctl restart firewalld
- To disable the firewall, run the following commands:
  systemctl disable firewalld
  systemctl stop firewalld

Edge Node Cannot Connect to IEF

Run the following command to check whether the edge node can connect to IEF:

curl -i -k -v https://ief2-edgeaccess.cn-north-4.myhuaweicloud.com:443/

If no command output is displayed, the edge node is disconnected from IEF. Check the network and ensure that the edge node can connect to IEF.

 Copyright © Huawei Technologies Co., Ltd.

Edge Node Fails to Resolve Domain Names

Ensure that your edge node can resolve the following domain names:

- Domain name of the region where IEF is located, for example, **ief2-placement.cn-north-4.myhuaweicloud.com** or **ief2-placement.cn-north-1.myhuaweicloud.com**. You can run the **cat /opt/IEF/Cert/user-config** command to query the domain name of your region.
- ief2-edgeaccess.cn-north-4.myhuaweicloud.com

Run the **ping** command to check whether the domain name can be resolved. For example:

```
ping ief2-edgeaccess.cn-north-4.myhuaweicloud.com
ping ief2-placement.cn-north-4.myhuaweicloud.com
```

If the domain name cannot be resolved, reconfigure a DNS server. The DNS server with IP address **114.114.114.114** is recommended.

A Certificate Is Used on Multiple Edge Nodes

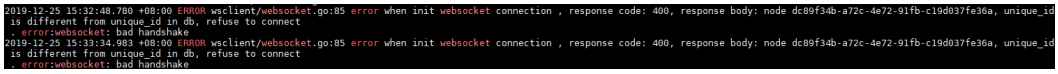
The same certificate is loaded on multiple edge nodes, and one of these nodes is in the **Running** state.

The edge nodes registered on the IEF console must correspond to the actual edge nodes. Do not create only one edge node on the IEF console and load the installation package and certificate downloaded from the IEF console to multiple edge nodes.

Run the following command to check whether the certificate is repeatedly used:

cat /var/IEF/sys/log/edge_core.log | grep websocket

The certificate is repeatedly used if a message indicating that node xxx has been occupied is displayed. (**xxx** indicates the ID of the edge node.)



An Edge Node Is Managed for Multiple Times

- The uninstall operation is not correctly performed before the edge node is managed again. To be specific, the edge node is deleted only on the IEF console, but the IEF software is not uninstalled from the edge node.

  Run the following commands to check whether the IEF components on the edge node are running:

  systemctl status edgecore

  systemctl status edgemonitor

  systemctl status edgelogger

  If the edge node fails to be managed but the preceding components are still running, the components are not correctly uninstalled from the edge node. Run the following command to uninstall the components:

  cd /opt/edge-installer; sudo ./installer -op=uninstall

  Note that the following misoperation may occur:

 Copyright © Huawei Technologies Co., Ltd.

To manage the edge node again, rename the original **/opt** directory of the node **/opt_old**, create a new **/opt** directory, and manage the node based on the guide provided by IEF. When the node management fails, an uninstall operation is performed. The system prompts that the uninstallation is successful but the preceding components are still running. This is because the IEF components you uninstalled are not those installed in the **/opt_old** directory. In this case, restore the **/opt** directory, uninstall the IEF components, and then manage the edge node again. However, do not perform this operation to manage an edge node again.

- IEF components on the edge node are not completely uninstalled.

  If the uninstallation is complete but the management still fails, restart the edge node and try again.

Command for Managing Edge Nodes Is Not Run in the Specified Directory

The installation command is as follows:

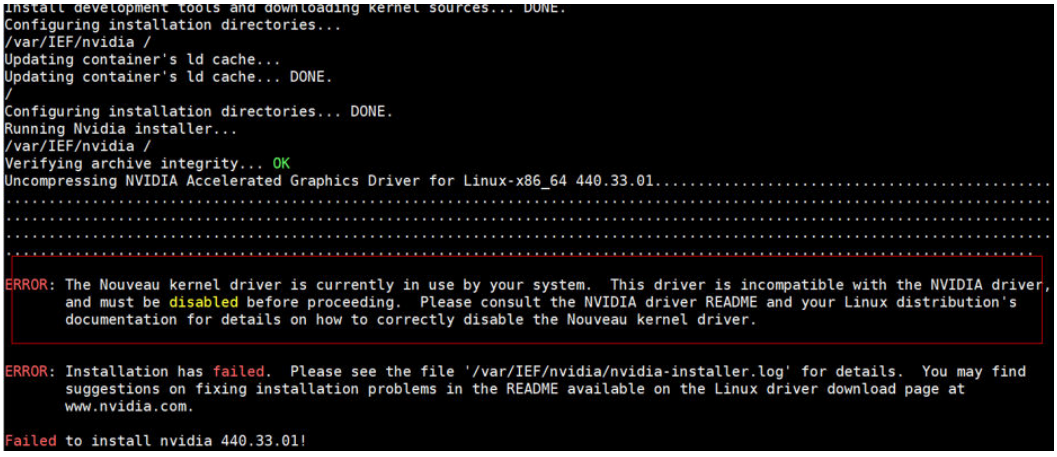
cd /opt/edge-installer; sudo ./installer -op=install

The **cd /opt/edge-installer** command must be run to ensure that the installation command is run in the **edge-installer** directory.

1.4 What Do I Do If an Error Occurs During GPU Driver Installation?

Symptom

An error is reported when the **nvidia-gpu-installer.sh** script is executed to install the GPU driver.



Analysis

Nouveau is a video card driver that runs in most Linux operating systems. This driver is incompatible with the NVIDIA driver. Therefore, it must be disabled before the GPU driver installation.

 Copyright © Huawei Technologies Co., Ltd.

Solution

The following describes how to disable Nouveau running in Ubuntu 16.04. For other OSs, you can search for the corresponding solution.

1. Open the **blacklist-nouveau.conf** file in the **/etc/modprobe.d/** directory.

   sudo gedit /etc/modprobe.d/blacklist.conf

   Enter the password, and add the following line to blacklist the graphics driver embedded in Ubuntu:

   ```
   blacklist nouveau
   ```

2. Run the following command to make the configuration to take effect:

   sudo update-initramfs -u

3. Run the following command to restart the OS:

   sudo reboot

4. Run the following command to stop the lightdm service:

   sudo service lightdm stop

5. Run the following command to check whether Nouveau is disabled:

   lsmod | grep nouveau

   If no command output is displayed, Nouveau is disabled successfully.

1.5 How Do I Obtain the Latest Device Properties After Device Properties Are Updated?

- If device properties are written into container images through environment variables, you need to update the environment variables of the container and deliver them to the container again for the modification to take effect. This mode is not recommended because it is not flexible.
- If you obtain device information by calling the API provided by IEF, you can use the API for querying edge device details to obtain the latest device properties. For details about the API, see **Querying Details About an Edge Device**.

1.6 What Operations Can I Perform After a Device Is Associated with a Node?

- After a device is created, you can query device information by using device management APIs under applications. In this way, containers can obtain device information more convenient.
- After a device is associated with a node, the device can be directly controlled in the cloud by creating and updating the device twin.

1.7 Does an Edge Node Support Multiple GPUs?

An edge node supports multiple GPUs of the same type.

 Copyright © Huawei Technologies Co., Ltd.

1.8 Can I Change the GPU on a Running Edge Node?

Yes. To change a GPU, perform the following operations:

1. Run the following command to stop the IEF Agent service:

   systemctl stop edgecore

   systemctl stop edgedaemon

2. Change the GPU and reinstall the GPU driver. For details about how to install the GPU driver, see **Installing a GPU Driver**.

3. Run the following command to start the IEF Agent service:

   systemctl start edgecore

   systemctl start edgedaemon

1.9 How Is Edge Environment Security Protected?

IEF provides a security solution under edge-cloud synergy.

- IAM authentication

  Agencies can be created in Identity and Access Management (IAM) to allow edge nodes to access HUAWEI CLOUD resources such as Application Operations Management (AOM), Software Repository for Container (SWR), and DIS.

- Edge node security

  Edge Agent creates dedicated service users whose accessible directories and permissions are limited. Users can upload logs and monitoring information to the cloud based on their requirements.

- Edge-cloud synergy communication security

  Edge Agent initiates a request to IEF for establishing a bidirectional encrypted channel. Messages exchanged between devices and IEF are authenticated and encrypted by certificates.

- Cloud security

  The frontend anti-DDoS protects the cloud against malicious attacks.

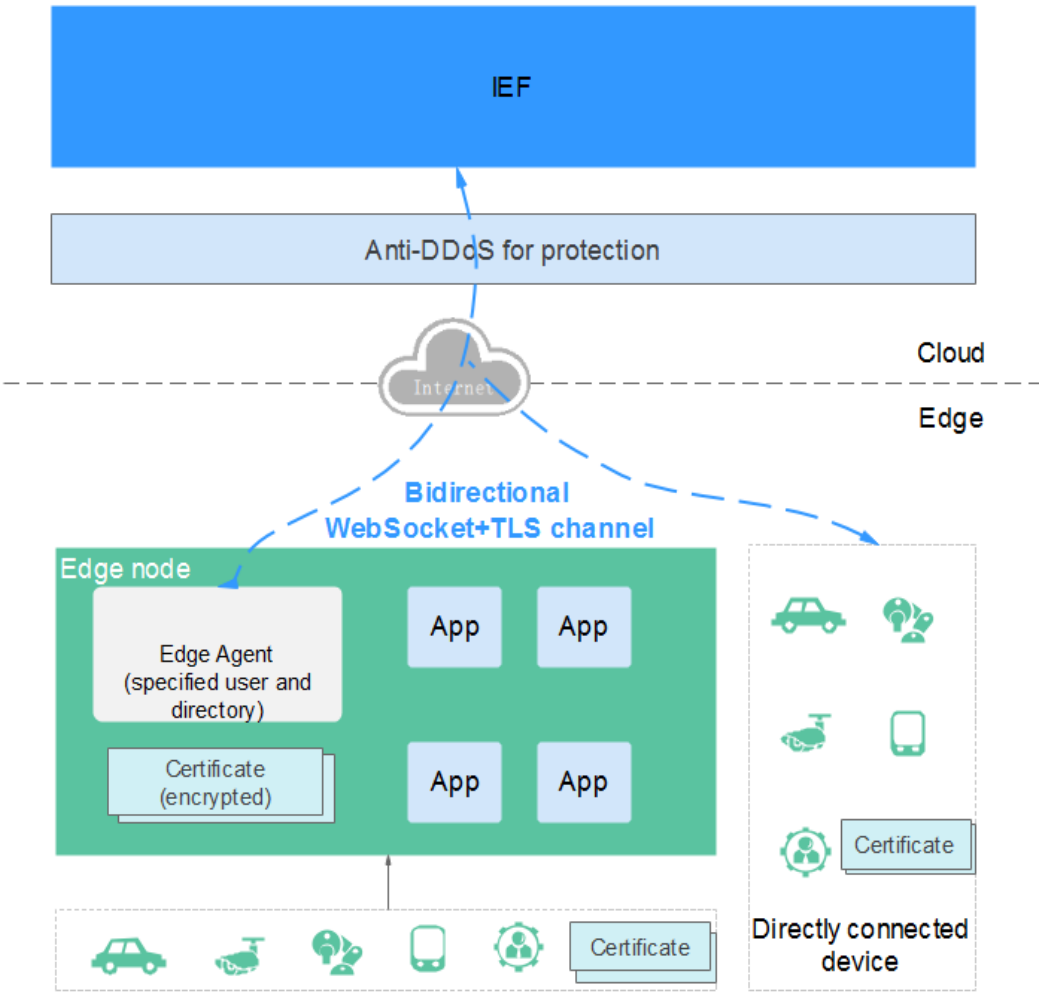
  A unique access certificate is issued for each edge node. Bidirectional communication is authenticated and encrypted by certificates.

- Device security

  Edge devices use certificates for identity authentication.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-6 IEF security solution



1.10 Why Cannot I View Monitoring Data on an Edge Node?

Analysis

No agency is created for IEF or no agency is configured for an edge node group. Therefore, IEF cannot report monitoring data of edge devices to the Application Operations Management (AOM) service. As a result, no data is displayed on the monitoring page of the edge node.

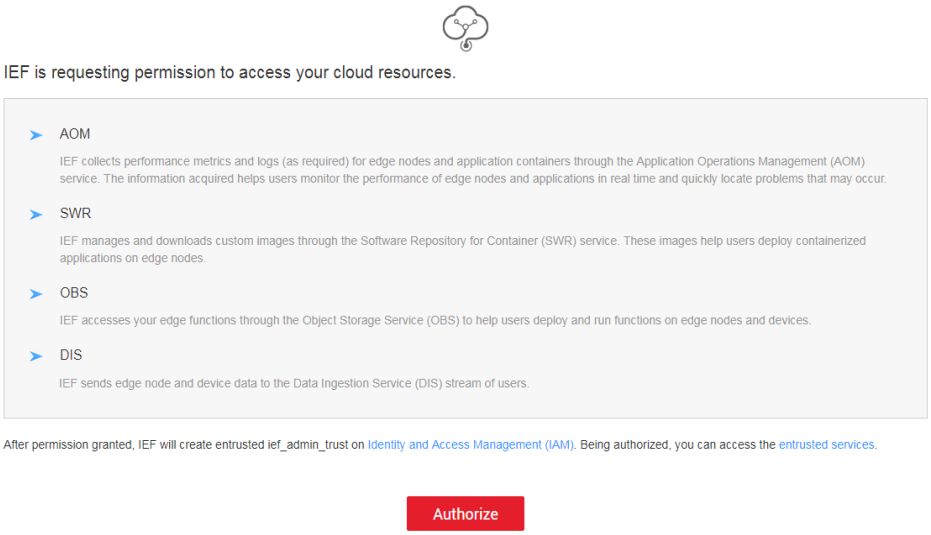
Solution

Step 1 Create an agency for IEF.

1. A dialog box indicating agency creation is displayed when you enter the IEF console the first time.
2. Click **Authorize**. An agency is automatically created.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-7 Automatically creating an agency



Step 2 An agency is automatically configured when you create a node on IEF.

----End

1.11 How Can I Restore a Deleted Edge Node?

After an edge node is deleted, you must register a new edge node instead of directly managing the deleted edge node on IEF again. For details, see **Registering an Edge Node**.

1.12 What Is the Impact of IP Address Changing on an Edge Node?

The IP address changing on an edge node does not affect the product.

IEF uses the node ID to uniquely identify an edge node. After an edge node is managed on IEF, it periodically reports information such as its status to IEF and also synchronizes its IP address to IEF.

1.13 What Do I Do If the NTP Configuration Cannot Be Modified?

The ntpd process may not be started on the edge node. Run the **systemctl restart ntpd** command on the edge node and modify the NTP configuration again.

 Copyright © Huawei Technologies Co., Ltd.

1.14 How Do I Synchronize Time with the NTP Server?

Background

If you use IEF to manage your edge node, ensure that the time of the edge node is consistent with the UTC time. Otherwise, the monitoring data and logs of the edge node may be inaccurate.

You can select a proper NTP server for time synchronization to ensure time consistency.

Prerequisites

Network Time Protocol daemon (ntpd) has been installed on the edge node. For example, you have installed ntpd by running the **yum install -y ntp** command on the edge node running CentOS.

Procedure

Step 1 Log in to a Linux ECS.

Step 2 Run the following command to open the **ntp.conf** file:

vim /etc/ntp.conf

Step 3 Add the following statement to configure the NTP server:

server *Domain name of the NTP server*

Example:

server 0.pool.ntp.org

Step 4 Run either of the following command to start the NTP service:

SUSE OS:

service ntp restart

CentOS:

systemctl restart ntpd

NOTE

Run the appropriate command based on the OS running on the ECS.

Step 5 Run the following command to check whether the time of the ECS is synchronized with that of the NTP server:

ntpq -p

If "*" is displayed, the time has been synchronized.

NOTE

It takes several minutes to perform NTP time synchronization for the first time.

 Copyright © Huawei Technologies Co., Ltd.

Step 6 Set the NTP service to run automatically during system startup:

SUSE OS:

chkconfig ntp on

CentOS:

chkconfig ntpd on

----End

1.15 How Do I Obtain the IP Addresses of IEF Cloud Services?

If you need to manage your edge node on IEF, ensure that the edge node can communicate with IEF, SWR, and OBS. If a firewall exists in the environment where your edge node is located, obtain the IP addresses of these cloud services based on the domain names listed in **Table 1-4** and use the IP addresses and port numbers to configure the firewall. This configuration enables the edge node to access IEF, SWR, and OBS.

You can ping the domain name of a service to obtain its IP address. For example:

```
$ ping ief2-placement.cn-north-4.myhuaweicloud.com

Pinging ief2-placement.cn-north-4.myhuaweicloud.com [119.3.227.164] with 32 bytes of data:
```

Table 1-4 Access domain names used by edge nodes

Region	Domain Name	Port
CN North-Beijing1	ief2-placement.cn-north-1.myhuaweicloud.com	443
	ief2-edgeaccess.cn-north-1.myhuaweicloud.com	443
	ief2-telemetry.cn-north-1.myhuaweicloud.com	8102, 8149, and 8065
	swr.cn-north-1.myhuaweicloud.com	443
	obs.cn-north-1.myhuaweicloud.com	443
	ief-agent-software.obs.cn-north-1.myhuaweicloud.com	443
CN North-Beijing4	ief2-placement.cn-north-4.myhuaweicloud.com	443
	ief2-edgeaccess.cn-north-4.myhuaweicloud.com	443
	ief2-telemetry.cn-north-4.myhuaweicloud.com	8102, 8149, and 8065

Copyright © Huawei Technologies Co., Ltd.

Region	Domain Name	Port
	swr.cn-north-4.myhuaweicloud.com	443
	obs.cn-north-4.myhuaweicloud.com	443
	ief-software-north-4.obs.cn-north-4.myhuaweicloud.com	443
CN South-Guangzhou	ief-placement.cn-south-1.myhuaweicloud.com	443
	ief-edgeaccess.cn-south-1.myhuaweicloud.com	443
	ief-telemetry.cn-south-1.myhuaweicloud.com	8102, 8149, and 8065
	swr.cn-south-1.myhuaweicloud.com	443
	obs.cn-south-1.myhuaweicloud.com	443
	ief-software-south-1.obs.cn-south-1.myhuaweicloud.com	443
CN East-Shanghai1	ief-placement.cn-east-3.myhuaweicloud.com	443
	ief-edgeaccess.cn-east-3.myhuaweicloud.com	443
	ief-telemetry.cn-east-3.myhuaweicloud.com	8102, 8149, and 8065
	swr.cn-east-3.myhuaweicloud.com	443
	obs.cn-east-3.myhuaweicloud.com	443
	ief-software-east-3.obs.cn-east-3.myhuaweicloud.com	443
CN East-Shanghai2	ief2-placement.cn-east-2.myhuaweicloud.com	443
	ief2-edgeaccess.cn-east-2.myhuaweicloud.com	443
	ief2-telemetry.cn-east-2.myhuaweicloud.com	8102, 8149, and 8065
	swr.cn-east-2.myhuaweicloud.com	443
	obs.cn-east-2.myhuaweicloud.com	443
	ief-software-east-2.obs.cn-east-2.myhuaweicloud.com	443

 Copyright © Huawei Technologies Co., Ltd.

2 Edge Application FAQs

2.1 What Do I Do If an Application Fails to Be Delivered to an Edge Node?

Symptom

An application cannot be delivered to an edge node.

Fault Locating

Troubleshooting methods are sorted based on the occurrence probability of the possible causes. You are advised to check the possible causes from high probability to low probability to quickly locate the cause of the problem.

Figure 2-1 Fault locating

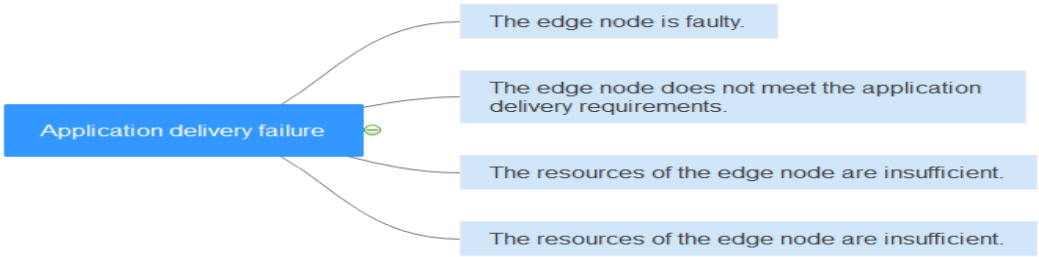


Table 2-1 Fault locating

Possible Cause	Solution
The edge node is faulty.	Log in to the IEF console, choose **Edge Resources** > **Edge Nodes**, and check the edge node status. If the edge node is faulty, rectify the fault by referring to **1.1 What Do I Do If an Edge Node Is Faulty?**.

 Copyright © Huawei Technologies Co., Ltd.

Possible Cause	Solution
The edge node does not meet the application delivery requirements.	**Edge Node Does Not Meet the Application Delivery Requirements**
The resources of the edge node are insufficient.	**Edge Node Resources Are Sufficient**
The container image fails to be pulled.	For details, see **2.4 What Do I Do If a Container Image Fails to Be Pulled?**.

Edge Node Does Not Meet the Application Delivery Requirements

Check the resource information of the edge node.

Step 1 Check the type of the edge node.

1. If the application needs to use NPU and GPU resources, check whether the type of the edge node is correctly selected.
2. Run the **docker ps** command on the edge node to check whether the NPU container (npu-device-plugin) and GPU container (gpu-device-plugin) are running properly.

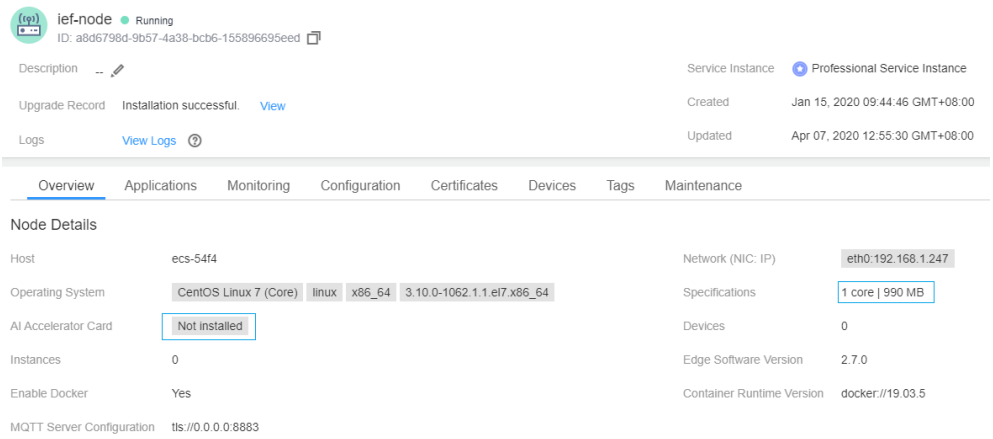
   If you manage the edge node for the first time, rectify the fault by following the procedure described in **2.2 What Do I Do If a Containerized Application Fails to Be Started on an Edge Node?**.
3. Check whether the GPU and NPU resources are used by any application running on the edge node and whether the node has remaining GPU and NPU resources.

Step 2 Check whether the edge node specifications (CPU and memory information) displayed on the IEF console are correct. If the memory size is displayed as 0, check whether the edge node uses the OS of the Chinese edition. IEF supports only the OS of the English edition. If the OS of the Chinese edition is used, IEF cannot obtain memory information or deliver applications to the edge node. In this case, you need to reinstall the OS and manage the edge node again.

CAUTION

Before the OS reinstallation, securely store the installation package and certificate file you downloaded from IEF. If they are not stored, you must delete the edge node and register a new edge node.

Copyright © Huawei Technologies Co., Ltd.



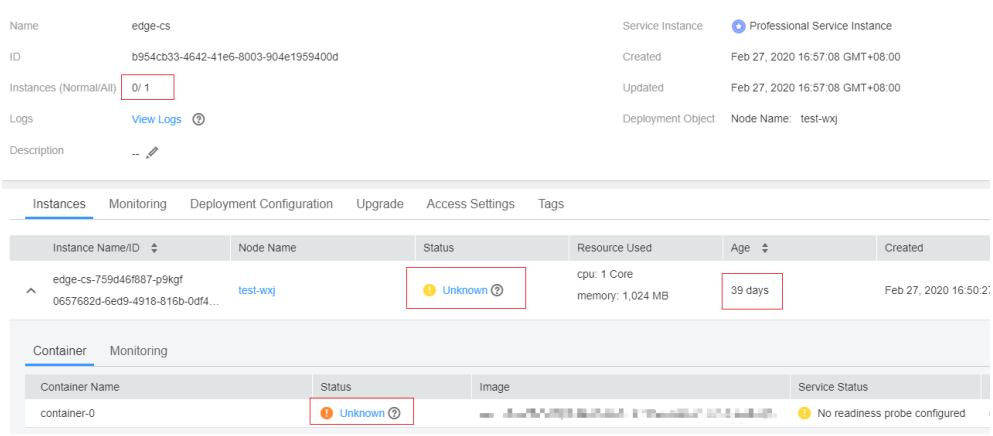
Step 3 If you want to deliver a containerized application, check whether a container engine is enabled on your edge node. If a container engine is not enabled, the containerized application cannot be delivered.

----End

Edge Node Resources Are Sufficient

Step 1 Check the cause of the container exception.

Hover the cursor over the instance status to view the cause of the application delivery failure.

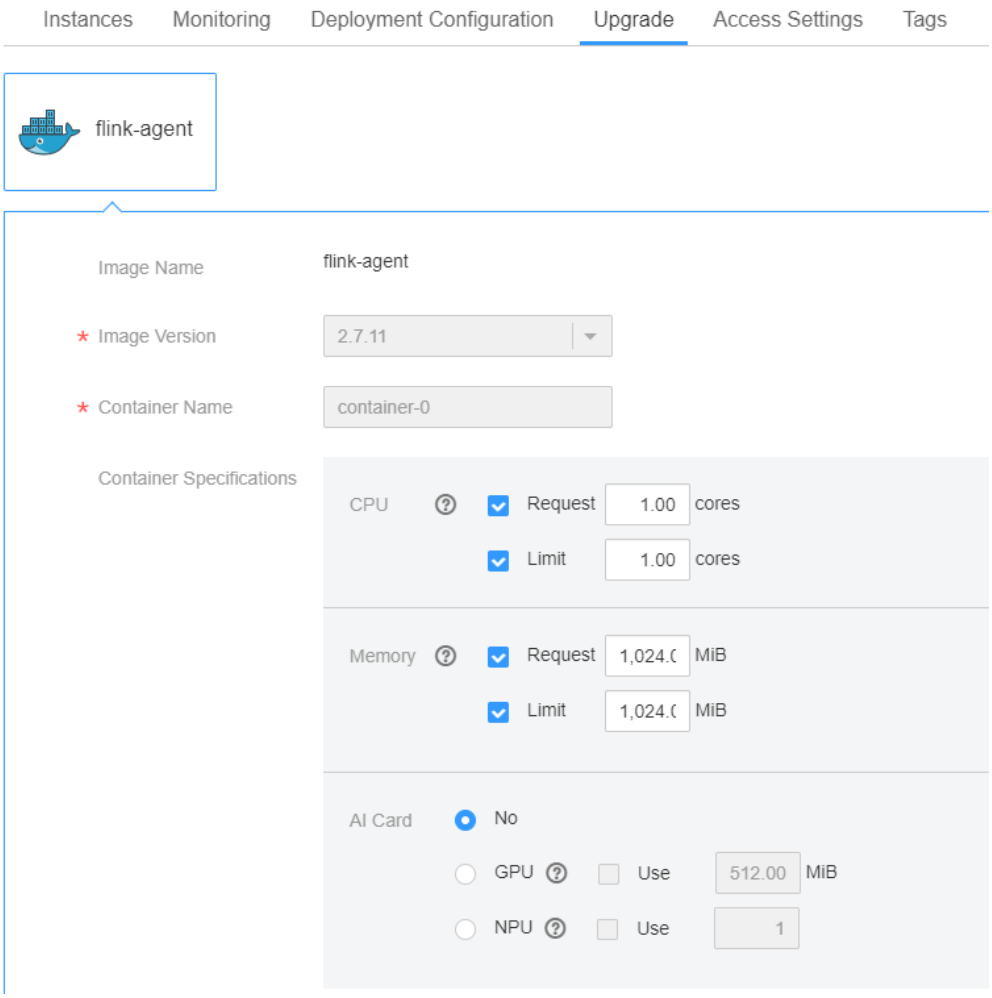


Step 2 Check the size of the resources requested by the application.

Check whether the available resources on the edge node meet the resources requested by the application. Ensure that the edge node resources are sufficient.

The following figure shows how to check the amount of resources requested by the application.

 Copyright © Huawei Technologies Co., Ltd.



----End

2.2 What Do I Do If a Containerized Application Fails to Be Started on an Edge Node?

Symptom

A containerized application cannot be started on an edge node.

Fault Locating

Troubleshooting methods are sorted based on the occurrence probability of the possible causes. You are advised to check the possible causes from high probability to low probability to quickly locate the cause of the problem.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-2 Fault locating

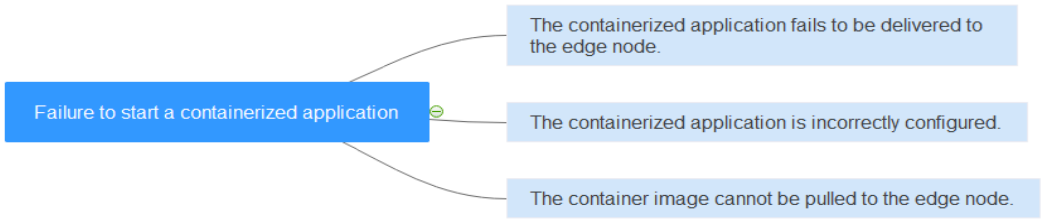


Table 2-2 Fault locating

Possible Cause	Solution
The containerized application fails to be delivered to the edge node.	For details, see **2.1 What Do I Do If an Application Fails to Be Delivered to an Edge Node?**.
The containerized application is incorrectly configured.	**Containerized Application Is Incorrectly Configured**
The container image cannot be pulled to the edge node.	For details, see **2.4 What Do I Do If a Container Image Fails to Be Pulled?**.

Containerized Application Is Incorrectly Configured

Step 1 Log in to the edge node.

Step 2 Run the following command to check whether the container is running:

sudo docker ps | grep *Application name*

Run the following command to check whether the container exits abnormally:

sudo docker ps -a | grep *Application name*

Run the preceding two commands repeatedly to check whether the container keeps restarting.

- If the status of your application cannot be queried, go to **Step 3**.
- If your container restarts repeatedly, run the following command to query logs:

  **ID=`sudo docker ps -a | grep** *Application name* **| awk '{print $1}'** `

  sudo docker logs $ID

  The application logs are displayed, based on which you can locate the cause of repeated container restarts. The possible causes are as follows:

  – Image errors

    The image is in error, or the image does not match the system. You can perform the following operations to verify the image on the edge node:

 Copyright © Huawei Technologies Co., Ltd.

i. Obtain edge node images.

docker images

ii. Find your image and obtain the image ID.

iii. Run the **docker run** command to run the container. Different startup commands may be required based on service requirements.

- Startup parameter errors

  Check whether the startup parameters are correct.

- Directory mounting errors

  If the image needs to access a special directory on the edge node, ensure that the directory has been mounted during the delivery.

- NPU issues

  If your application needs to use NPU resources, ensure that you have selected the NPU resources when delivering the application.

  NPU resources are occupied by applications that are not delivered by IEF, resulting in insufficient resources. IEF cannot identify the NPU usage of non-IEF applications. Therefore, check that NPU resources are sufficient.

- Resource issues

  Ensure that the **Limit** values of the CPU and memory resources requested when the application is delivered are sufficient. (If the amount of resources requested by the container exceeds the **Limit** value, the container will be killed repeatedly.) You can conduct verification by setting **Limit** to a larger value.

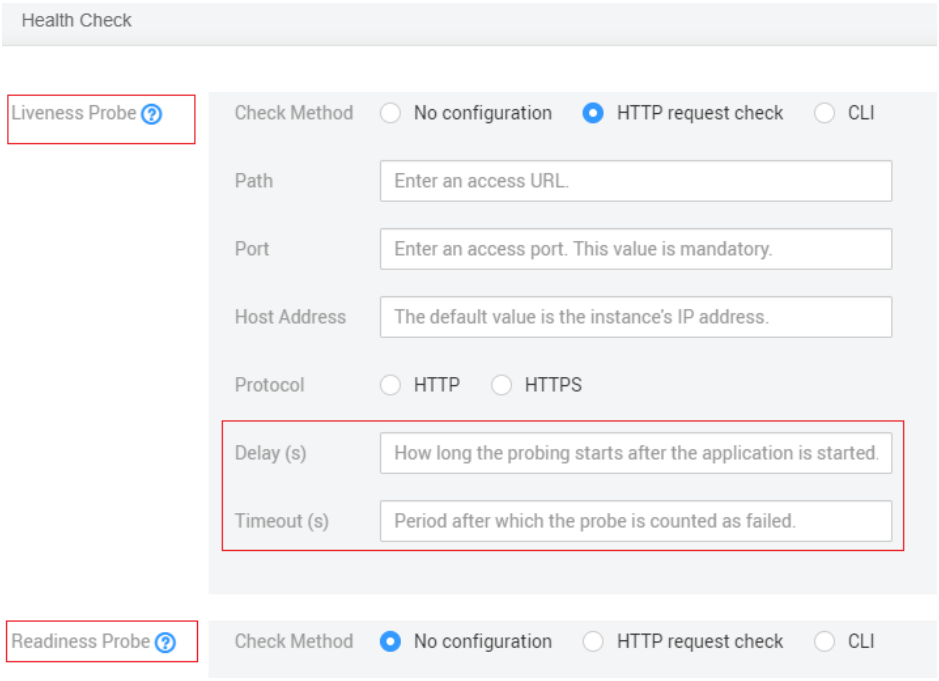
- Health check issues

  If you have configured the health check, ensure that the health check mode is correctly configured. If the health check mode is incorrectly configured, the health check will fail and the container will be restarted repeatedly.

  To check the health check mode, log in to the IEF console, choose **Edge Applications** > **Containerized Applications**, click **Upgrade** in the row of your application, and view the health check configuration in the **Advanced Settings** area. Check whether the liveness probe and readiness probe of your application are correctly configured.

  To verify this problem, you can update the application without configuring the health check and check whether the application restarts repeatedly.

 Copyright © Huawei Technologies Co., Ltd.



- Health check interval issues

  Check how long it takes for the application to start properly and how long it takes for the system to return health check results.

  The health check delay indicates the interval between the time when the application is delivered and the time when a health check is started. If the interval is too short, a health check may start before the application is ready. In this case, the application fails the health check continuously and the container is restarted repeatedly, resulting in a vicious cycle.

  The health check timeout indicates the interval between the time when the health check is started and the time when a response is returned. If no response is returned within the interval, the health check is counted as failed. If the configured health check timeout period is shorter than the time required for the interface to return the result, the health check fails continuously and the application is restarted repeatedly. (This problem may occur when the edge node performance is poor or the service volume on the application is large.)

Step 3 Check whether the application is successfully delivered.

1. Run the following command to switch to the **root** user:

   sudo su

2. Query application logs.

   cat /var/IEF/sys/log/edge_core.log | grep *Application name*

If logs are displayed, the application has been successfully delivered. The possible cause is that the container image fails to be pulled. Locate the fault by referring to **2.4 What Do I Do If a Container Image Fails to Be Pulled?**.

If no log is displayed, **submit a service ticket**.

----End

 Copyright © Huawei Technologies Co., Ltd.

2.3 What Do I Do If a Containerized Application Fails to Be Upgraded?

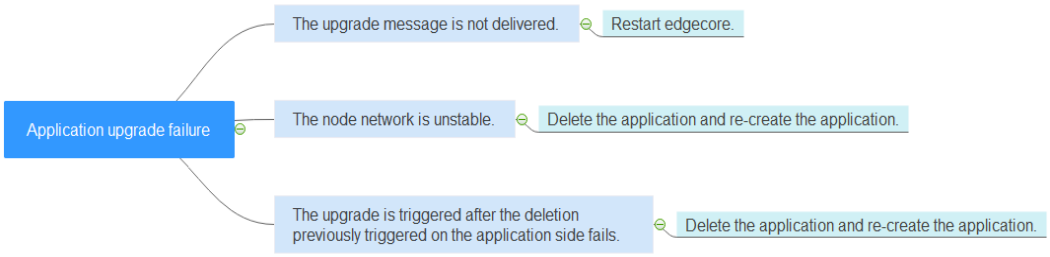
Symptom

A containerized application is upgraded on the IEF console, but the application is not upgraded on the edge node where it is deployed. Therefore, the upgrade fails.

Fault Locating

Troubleshooting methods are sorted based on the occurrence probability of the possible causes. You are advised to check the possible causes from high probability to low probability to quickly locate the cause of the problem.

Figure 2-3 Fault locating



1. Possible cause 1: The upgrade message is not delivered. In this case, restart edgecore. For details, see **Restarting edgecore**.
2. Possible cause 2: The node network is unstable, and the application is in the **Terminating** state. In this case, delete the application from the IEF console and create the application again.
3. Possible cause 3: The upgrade is triggered after the deletion previously triggered on the application side fails. In this case, delete the application from the IEF console and create the application again.

Restarting edgecore

Log in to the edge node, and run the following command to restart the edgecore process:

systemctl restart edgecore

Submitting a Service Ticket

If the problem persists, **submit a service ticket**.

 Copyright © Huawei Technologies Co., Ltd.

2.4 What Do I Do If a Container Image Fails to Be Pulled?

Symptom

An image in SWR cannot be pulled to an edge node.

Fault Locating

Figure 2-4 shows the major causes of the failure to pull the container image. You can locate the fault based on Table 2-3.

Figure 2-4 Fault locating

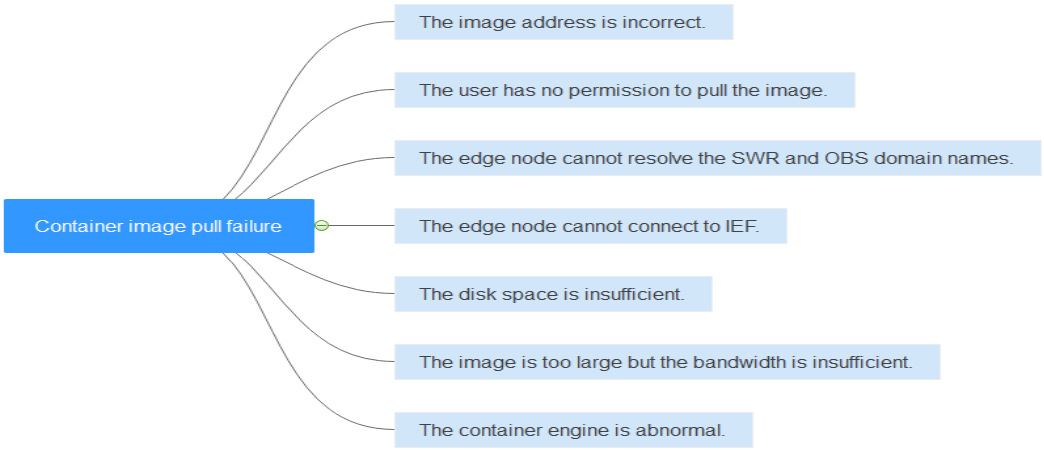


Table 2-3 Fault locating

Possible Cause	Solution
The image address is incorrect.	**Image Address Is Incorrect**
The user has no permission to pull the image.	**User Has No Permission to Pull the Image**
The edge node cannot resolve the SWR and OBS domain names.	**Edge Node Cannot Resolve the SWR and OBS Domain Names**
The edge node cannot connect to IEF.	**Edge Node Cannot Connect to IEF**
The disk space is insufficient.	**Insufficient Disk Space**

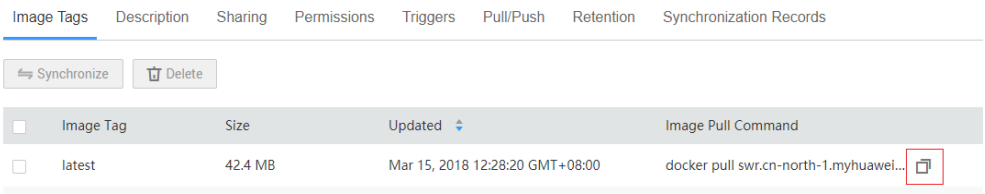
Copyright © Huawei Technologies Co., Ltd.

Possible Cause	Solution
The image is too large but the bandwidth is insufficient.	**Image Is Too Large but the Bandwidth Is Insufficient**
The container engine is abnormal.	**Container Engine Is Abnormal**

Image Address Is Incorrect

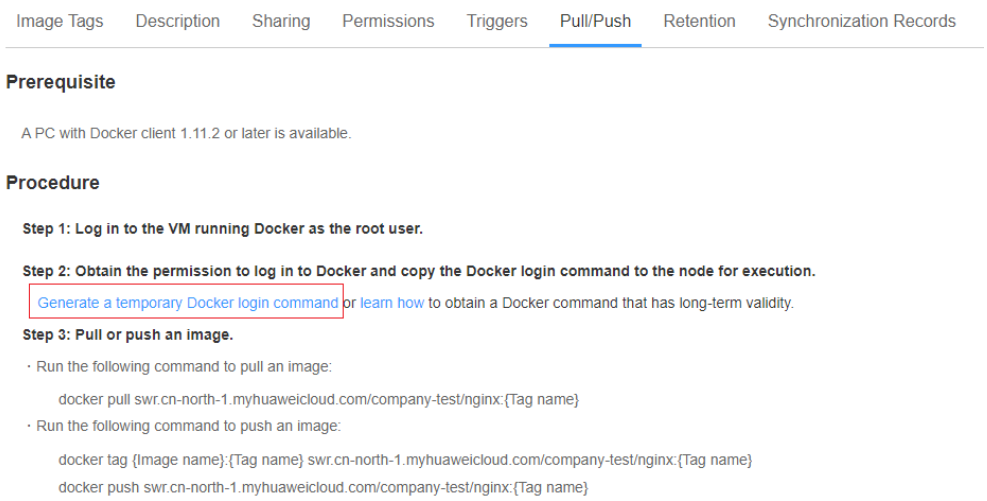
Check whether the image address is correct. If the address is incorrect, change it to a correct one.

1. Log in to the SWR console.
2. In the navigation pane, choose **My Images**. On the page displayed, click the image that fails to be pulled.
3. In the same row as the image tag, click  to copy its pull command.



User Has No Permission to Pull the Image

Obtain and run the login command to pull the image. If the login fails or the image cannot be pulled, you do not have the permission.



 Copyright © Huawei Technologies Co., Ltd.

Edge Node Cannot Resolve the SWR and OBS Domain Names

As SWR images are actually stored in OBS, check that the edge node has permissions to access both SWR and OBS. Otherwise, images cannot be pulled.

Check whether your node can resolve the SWR and OBS domain names. If the domain names cannot be resolved, images fail to be pulled.

- Check method 1:

  View logs on the edge node.

  cat /var/IEF/sys/log/edge_core.log| grep lookup

- Check method 2:

  Run the following commands on the edge node:

  ping swr.cn-north-4.myhuaweicloud.com

  ping obs.cn-north-4.myhuaweicloud.com

  Check whether the domain names can be resolved into corresponding IP addresses. If the domain names can be resolved but the login to SWR is suspended, check the domain name resolution mode of your container engine. If the domain names cannot be resolved into corresponding IP addresses, perform the following steps to check whether the DNS server configuration was modified:

  – If the mapping between the domain names and IP addresses is configured in the local hosts file, check whether the configuration is correct.

    cat /etc/hosts | grep swr

    cat /etc/hosts | grep obs

    If the hosts file configuration is incorrect, the domain name resolution will fail. In this case, resolve the domain name on the host whose hosts file is correct to obtain a correct IP address and then configure the IP address in the hosts file on your edge node.

  – If you use the DNS server configured in the **/etc/resolv.conf** file to resolve domain names, check whether the DNS server configuration is correct and whether the DNS server can resolve the preceding SWR and OBS domain names.

    Note that if IEF and the container engine are accessed through a public network, the DNS server with the IP address set to **114.114.114.114** is used in Chinese mainland. Ensure that your DNS server is correctly configured so that the domain names can be resolved within the validity period.

    If multiple DNS server IP addresses (including **114.114.114.114**) are configured but the container engine still cannot resolve domain names, you are advised to retain only **114.114.114.114** and comment out the other DNS server IP addresses.

  – If a proxy server is configured, check whether the proxy server can resolve the SWR and OBS domain names.

    - Open two terminals on your edge node.

      On one terminal, run **ping swr.cn-north-4.myhuaweicloud.com**.

      On the other terminal, run **tcpdump -nn -i eth0 udp port 53** to capture packets.

 Copyright © Huawei Technologies Co., Ltd.

Check the sequence of using DNS servers and the domain name resolution result to determine the DNS server by which the domain name is resolved. (If the hosts file is configured, domain name resolution is not performed.)

- On one terminal, run **docker login** *XXX* (temporary login command copied from SWR).

  On the other terminal, run **tcpdump -nn -i eth0 udp port 53** to capture packets.

  Check the sequence of using DNS servers and the domain name resolution result to determine the DNS server by which the domain name is resolved. (If the hosts file is configured, domain name resolution is not performed.)

- Check whether the DNS servers used in the preceding two steps are the same and whether the domain names are resolved. If the DNS servers used in the two steps are different, modify the **/etc/resolv.conf** file and configure the hosts file.

Edge Node Cannot Connect to IEF

Step 1 Check whether the network connection between the edge node and SWR is normal.

On the edge node, run the following commands:

curl -i -k -v www.baidu.com

curl -i -k -v swr.cn-north-4.myhuaweicloud.com

curl -i -k -v obs.cn-north-4.myhuaweicloud.com

NOTE

The domain name varies depending on regions.

If the network is inaccessible, check your network policies to determine whether the edge node can connect to external networks. If the network is accessible but the Docker login command is suspended, repeat **Edge Node Cannot Resolve the SWR and OBS Domain Names** to check the resolution of the SWR domain name.

If the SWR domain name can be resolved, check the external network access mode configured for the edge node to determine whether your container can access external networks. Confirm the following problems:

1. Check whether a proxy is configured for the edge node.

   env| grep proxy

   env| grep PROXY

2. Check whether a proxy is configured for the container engine.

   systemctl show --property=Environment docker

   If a proxy is used for external network access, ensure that the proxy configuration of your node and container engine is correct.

Step 2 Log in to SWR again and pull the image.

 Copyright © Huawei Technologies Co., Ltd.

If a message indicating an authentication failure is displayed, **submit a service ticket**.

----End

Insufficient Disk Space

Run the following command to query the disk usage:

df -h

Check the available disk space in **/var/lib/docker/*** on the edge node. Then, compare the available disk space with the size of your image (the actual image size is generally greater than that displayed on the SWR console) to determine whether the space is sufficient for pulling the image. If the disk space is insufficient, an error is reported during image pull.

Image Is Too Large but the Bandwidth Is Insufficient

Check the image size and external network bandwidth to determine whether the image pull will time out.

For example, if the image size is 1 GB and the download speed of the edge node is about 200 kbit/s, it takes about 85.3 minutes (1024 MB/0.2 MB = 5,129s) to pull the image. This duration is much longer than the normal delivery duration of an application. In this case, the application cannot obtain the image.

To solve this problem, you are advised to pull the image to the edge node and then deliver the application.

Container Engine Is Abnormal

If an error is reported when you run the **docker pull** command, you can search for the solution to solve the error on the Internet. This is because the container engine versions installed by users may be different and have some performance defects.

You can also restart the container engine to work around this problem.

systemctl restart docker

To avoid this problem, you are advised to install the container engine versions recommended by IEF. For details about the container engine version requirements, see **Constraints**.

2.5 Why Cannot I View Application Logs and System Logs?

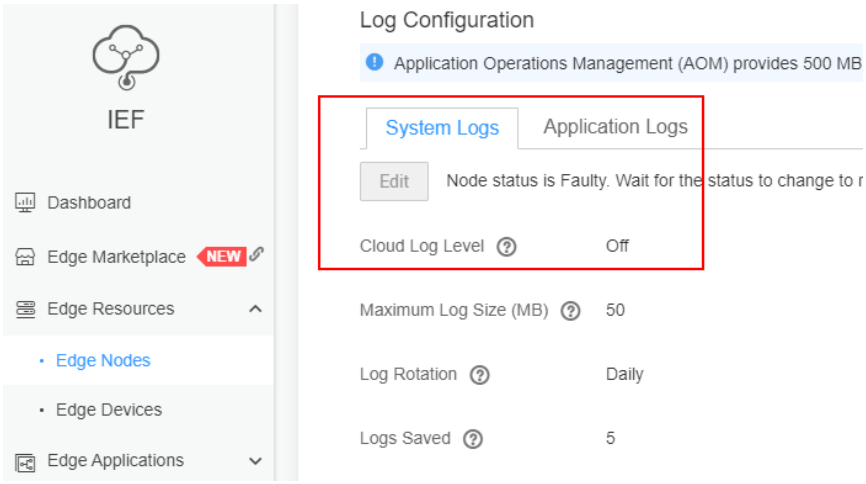
To enable edge nodes to report application logs and system logs to AOM, you must enable the log function and ensure that the NTP configurations on the edge nodes are the same as those in HUAWEI CLOUD.

If logs are unavailable on AOM, the possible causes are as follows:

1. The log function is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Log in to the IEF console. In the navigation pane, choose **Edge Resources** > **Edge Nodes**. Click the edge node name to access the edge node details page. Then, click the **Configuration** tab, and enable the log function under the **Log Configuration** area.



2. The time zone of the edge node is incorrect.

   Modify the NTP server settings of the edge node to be the same as those in HUAWEI CLOUD. For details, see **Does HUAWEI CLOUD Provide the NTP Server and How Can I Install It?**.

2.6 How Do I Know Whether a Function Is Successfully Executed?

Check the function status. If the function is in the Running state, it is Successfully executed.

2.7 What Can I Do If a Function Fails to Start?

Symptom

A function fails to start and its status is **Error**.

Analysis

- Function startup environments (Python 2.7 and Python3.6) are unavailable on edge nodes.
- The function code has a defect and fails to be compiled during calling.
- An exception occurs during function execution.

Solution

1. Install a function runtime environment.
2. Check the function code and rectify the defect to ensure successful compilation.

 Copyright © Huawei Technologies Co., Ltd.

3. View the startup logs (**python***.log**) of the function that is connected to the application monitoring module. Check the error information and rectify the fault accordingly.

2.8 Why Do I Need to Use nvidia-gpu-installer.sh to Install the GPU Driver? What Is the Difference Between This Method and the Method of Installing the GPU Driver in the OS?

- Before managing edge nodes by IEF, use the **nvidia-gpu-installer.sh** script provided by IEF to install the driver of the corresponding version. If the GPU driver has been installed in the current OS, uninstall it first. The GPU drivers installed using the two methods are mutually exclusive and cannot be used properly.
- The drivers installed by using the two methods are essentially the same.

  After the **nvidia-gpu-installer.sh** script downloads and installs the GPU driver, it will build the installed GPU driver as an image and finally run a GPU plug-in container. In this way, the GPU driver can be shared by other service containers. However, if the GPU driver is installed in the host OS, containers cannot obtain the GPU driver from the host.

2.9 How Do Applications Schedule GPU Resources?

- IEF allows multiple applications to share the same GPUs.
- IEF allows a single application to use multiple GPUs.
- GPU resources are scheduled based on the GPU memory capacity in pre-allocation mode but not real-time allocation mode.
- If the GPU memory required by an application is smaller than that of a single GPU, GPU resources can be scheduled in shared mode. To be specific, sort the remaining memory sizes of GPUs in ascending order and allocate the first GPU that meets the resource requirement to the application. For example, there are three GPUs A, B, and C. Each GPU provides 8 GB memory. The remaining memory sizes of the three GPUs are 2 GB, 4 GB, and 6 GB, respectively. Application A requires 3 GB GPU memory. In this case, GPU B is allocated to this application.
- If the GPU memory required by an application is greater than that of a single GPU, multiple GPUs will be allocated to the application. To be specific, the total memory capacity of the selected GPUs is allocated to the application even if the total memory is greater than the memory required by the application. For example, there are three GPUs A, B, and C. Each GPU provides 8 GB memory. The remaining memory sizes of the three GPUs are 8 GB, 8 GB, and 6 GB, respectively. Application B requires 14 GB GPU memory. In this case, the total memory of GPUs A and B is allocated to this application, and any other applications cannot schedule the memory of GPU A or B.

 Copyright © Huawei Technologies Co., Ltd.

2.10 How Do I Control the Disk Space Occupied by a Container Engine?

You can control the disk space occupied by a container engine by editing the **daemon.json** file.

Prerequisites

A CentOS is used.

Procedure

Run the following command to open the **daemon.json** file:

vi /etc/docker/daemon.json

Set **storage-driver** to **devicemapper** and set **dm.basesize** under **storage-opts** to the maximum disk space that Docker can use. In the following example, the disk space of the container engine is limited to 10 GB.

```
{
   "storage-driver": "devicemapper",
   "storage-opts": [
      "dm.basesize=10G"
   ]
}
```


Copyright © Huawei Technologies Co., Ltd.

3 Edge-Cloud Message FAQs

3.1 What Is Route Management?

Route management enables messages to be forwarded from a specified source endpoint to a specified destination endpoint based on the configured routes. Currently, the following scenarios are supported:

1. Edge file service: A route from SystemREST to ServiceBus, in which REST Gateway APIs are called to obtain file services on edge nodes.
2. Edge message delivery service: A route from SystemREST to SystemEventBus, in which REST Gateway APIs are called to send messages to SystemEventBus (MQTT Broker) on edge nodes.
3. Device data forwarding service: A route from SystemEventBus to DIS/API Gateway, in which SystemEventBus forwards the edge device data bound to edge nodes to DIS or a specified API Gateway address.

3.2 What Is an Endpoint in Route Management?

An endpoint is a logical data connection point that sends or receives data.

3.3 What Is a Route?

A route defines how data is forwarded from a source endpoint to a destination endpoint.

3.4 Why Does a Route Fail to Be Created?

A route cannot be created because it may not meet specified requirements. When creating a route, conform to the following requirements:

- If the route contains an MQTT topic, the topic name cannot contain special characters and must be unique.
- If the route contains DIS information, the DIS stream must be in the **Running** state.

 Copyright © Huawei Technologies Co., Ltd.

- If the route contains API Gateway information, the API Gateway address must be in the correct format.

3.5 What Can I Do If a Message Fails to Be Forwarded over a Route?

If the number of forwarding failures increases, the message fails to be forwarded to the specified destination endpoint. Click the number of forwarding failures to view the failure details (specially the error code). Then, determine whether the backend service of the destination endpoint is unreachable based on the error code and rectify the fault accordingly.

3.6 What Is the Impact of Disabling a Route?

After a route is disabled, the messages that meet the route conditions will not be forwarded to the destination endpoint. The messages can be forwarded only after the route is enabled again.

 Copyright © Huawei Technologies Co., Ltd.

4 Network Management FAQs

4.1 How Does an Edge Node Connect to IEF?

An edge node can connect to IEF over the Internet, VPN, or Direct Connect. Select connection modes based on your service scenarios. If you have requirements on data security and data transmission performance, you can connect edge nodes to the cloud over Direct Connect or VPN.

4.2 What Additional Settings Are Required If the Proxy Is Enabled?

If the proxy is enabled for edge nodes, proxy settings must be configured on edge nodes and containerized applications.

NOTE

Currently, only HTTP proxy is supported.

Settings on Edge Nodes

Add the HTTP_PROXY and HTTPS_PROXY parameters to the **/opt/IEF/Cert/user_config** file.

Run the following command to open the **/opt/IEF/Cert/user_config** file, and add the two parameter settings. Note that **http://192.168.0.70:8888** in the following example must be replaced with the actual network proxy address.

vi /opt/IEF/Cert/user_config

```
"SYSTEM_LOG_FILE_SIZE":"50M",
"SYSTEM_LOG_LEVEL":"off",
"SYSTEM_LOG_ROTATE_NUM":"5",
"SYSTEM_LOG_ROTATE_PERIOD":"daily"
"HTTP_PROXY":"http://192.168.0.70:8888",
"HTTPS_PROXY":"http://192.168.0.70:8888"
```

 Copyright © Huawei Technologies Co., Ltd.

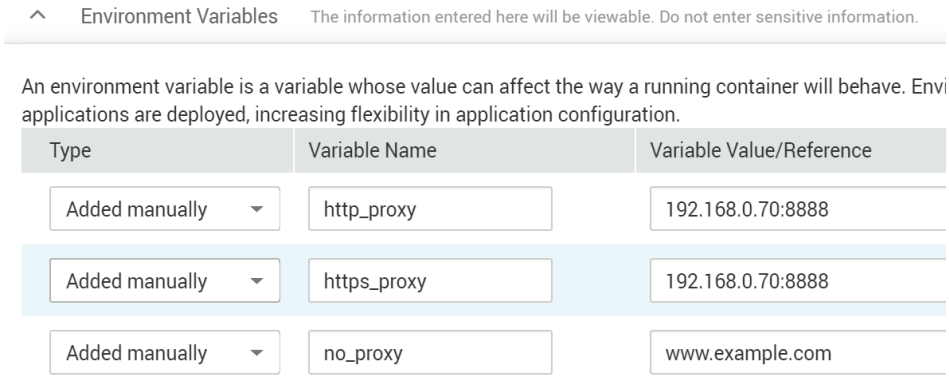
After modifying the configuration file, run the installation commands on edge nodes.

If the network proxy requires username and password authentication, prefix the username and password to the proxy address. For example, change **http://192.168.0.70:8888** to the following format:

http://**username:paasword@**192.168.0.70:8888

Settings on Containerized Applications

If the proxy is enabled for an edge node, the containerized application deployed on the node must be configured with proxy addresses before it accesses the external network. You can configure proxy-related environment variables when creating a containerized application.



In the preceding figure, **http_proxy** and **https_proxy** are the network proxy addresses used by the edge node. Replace them with the actual network proxy addresses.

The **no_proxy** variable specifies the website or IP address that needs to ignore the proxy. To be specific, such an address does not use a proxy server.

 Copyright © Huawei Technologies Co., Ltd.

5 Basic Concept FAQs

5.1 What Is Intelligent EdgeFabric?

Intelligent EdgeFabric (IEF) is a service that can manage edge nodes, extend cloud applications to the edge nodes, and associate edge and cloud data. It enables remote control, data processing, analysis, and intelligence of edge computing resources. IEF also provides unified on-cloud O&M capabilities, such as device/application monitoring and log collection, to offer a complete edge computing solution that contains integrated services under edge and cloud synergy.

5.2 What Benefits Does IEF Bring?

IEF provides a series of device-cloud synergy services, including remote device management and stream processing, which solves customer problems on latency-sensitive services, bandwidth-sensitive services, and services requiring high security and compliance.

- Latency-sensitive services

  IEF provides services such as data processing and application intelligence within close proximity to quickly respond to real-time services.
- Bandwidth-sensitive services

  IEF provides data preprocessing to prevent a large amount of data from being transmitted to the cloud, reducing investments on IT infrastructure (including bandwidth).
- Services requiring high security and compliance

  IEF provides functions such as local data processing and analysis to meet customers' security and compliance requirements. This is because data of such services cannot be transmitted to the cloud.

5.3 What Are the Main Application Scenarios of IEF?

IEF applies to latency-sensitive services, bandwidth-sensitive services, and services requiring high security and compliance, including but not limited to the following typical application scenarios:

 Copyright © Huawei Technologies Co., Ltd.

- Visual product inspections
- Predictive maintenance

5.4 What Is Edge Function?

Edge function is a serverless computing service provided by IEF for edge nodes. It can deliver the functions in FunctionGraph to edge nodes for running.

5.5 What Is Function Dependency? What Is the Relationship Between the Dependency and Functions?

A function dependency is a file that a function depends on when running, such as a third-party library or an AI training model. A dependency can be mounted to the execution directory of a function through function configuration. When the function is running, it can call the dependency.

5.6 What Functions Are Supported by IEF?

Currently, Python 2.7 and Python 3.6 functions can be deployed on edge nodes. In later versions, IEF will be enhanced to support scheduling of all functions supported in the cloud to edge nodes.

5.7 What Are the Function Running Modes (Remote Control and Long-term Running)?

As the edge functions run on the devices of users, they have special running environments and scenarios. When creating a function on the IEF console, you can select **Remote control** or **Long-term running** for **Running Mode**.

- A long-term running function can support long-term and continuous running of edge nodes.
- A remote control function provides more flexibility for users. Such a function uses the event-triggered mechanism, and therefore users can control the function lifecycle.

 Copyright © Huawei Technologies Co., Ltd.

6 Others

6.1 Region and AZ

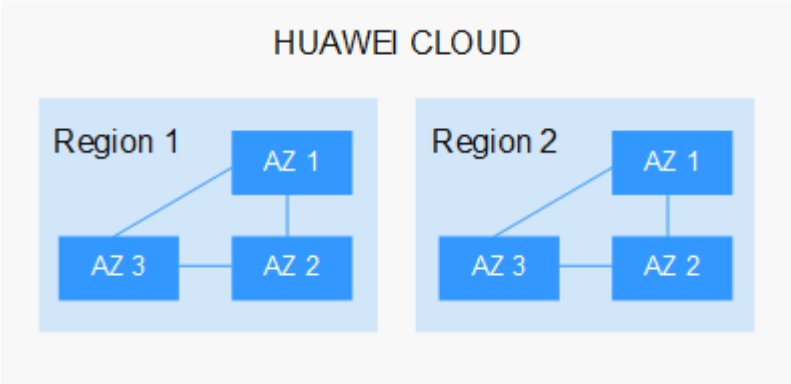
Concept

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified into universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides specific services for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to support cross-AZ high-availability systems.

Figure 6-1 shows the relationship between regions and AZs.

Figure 6-1 Regions and AZs



 Copyright © Huawei Technologies Co., Ltd.

HUAWEI CLOUD provides services in many regions around the world. Select a region and AZ based on requirements.

Selecting a Region

When selecting a region, consider the following factors:

- Location

  It is recommended that you select the closest region for lower network latency and quick access. Regions within the Chinese mainland provide the same infrastructure, BGP network quality, as well as resource operations and configurations. Therefore, if your target users are on the Chinese mainland, you do not need to consider the network latency differences when selecting a region.

  - If your target users are in Asia Pacific (excluding the Chinese mainland), select the **AP-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
  - If your target users are in Africa, select the **AF-Johannesburg** region.
  - If your target users are in Europe, select the **EU-Paris** region.
  - If your target users are in Latin America, select the **LA-Santiago** region.

    NOTE

    The **LA-Santiago** region is located in Chile.

- Resource price

  Resource prices may vary in different regions. For details, see **Product Pricing Details**.

Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.
- For low network latency, deploy resources in the same AZ.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see **Regions and Endpoints**.

6.2 What Are the Specifications of Edge Nodes Supported by IEF?

Intelligent EdgeFabric (IEF) supports the following edge node specifications:

 Copyright © Huawei Technologies Co., Ltd.

Table 6-1 Edge node requirements

Item	Specifications
OS	• x86_64 architecture Ubuntu 16.04 LTS (Xenial Xerus), Ubuntu 18.04 LTS (Bionic Beaver), CentOS 7.x and RHEL 7.x, Kylin 4.0.2, NewStart CGSL v5.5, and NeoKylin v7.0 • Armv7i (Arm32) architecture Raspbian GNU/Linux 9 (stretch) • AArch64 (Arm64) architecture Ubuntu 18.04.2 LTS (Bionic Beaver)
Memory	≥ 256 MB
CPU	≥ 1 vCPU
Hard disk	≥ 1 GB
GPU (optional)	The GPU models on the same edge node must be the same. **NOTE** Currently, only NVIDIA GPUs, such as Tesla P4, P40, and T4, are supported. If a device equipped with GPU hardware is registered as an edge node, you can choose not to enable its GPUs.
Container engine (mandatory when containerized applications are deployed)	The Docker version must be later than 17.06. Docker 18.06.3 is recommended. (However, Docker 18.09.0 is not recommended as it has a serious bug. For details, see **https://github.com/docker/for-linux/issues/543**. If this version has been installed, upgrade it at the earliest possible opportunity. This issue has been resolved in Docker 18.09.0.60 embedded in Atlas 500 AI edge stations.) **NOTICE** After Docker is installed, configure the Docker process to start at host startup. This configuration prevents system exceptions caused by Docker startup failures after the host is restarted.
Glibc	The Glibc version must be later than 2.17.
Port	Edge nodes need to use the following ports. Ensure that these ports are available. • 8102: used for reporting edge node logs to AOM • 8149: used for reporting monitoring data of edge nodes to AOM • 8065: used for reporting edge node alarms to AOM • 443: used by edge nodes to interwork with IEF • 8883: used by the built-in MQTT Broker • 1883: port used by the external MQTT Broker • 20004: used by edge nodes to report messages to DIS

 Copyright © Huawei Technologies Co., Ltd.

6.3 What Are the Application Scenarios of Functions and Containers?

- Functions have more lightweight runtime engines than containers. If your edge node resources are limited (the memory is smaller than 128 MB), you are advised to use functions.
- If the service logic of your edge applications is event-driven, you are advised to use functions. In this way, functions can respond to service requirements in near real-time through the event-triggered mechanism.
- Containers enjoy more prosperous ecosystem and greater portability, which can help your containerized applications seamlessly switch to other runtime environments. In addition, containers can isolate resources better.

6.4 What Are the Differences Between Device Properties and Device Twins?

Device properties indicate static device information, such as device names and IP addresses.

Device twins indicate dynamic control information of devices, such as the temperature detected by a temperature sensor and the humidity detected by a humidity sensor. You can control edge devices by modifying expected values in their device twins. You can obtain the real status of an edge device according to the actual value reported by the device.

6.5 What Programming Language Is Required for IEF Development?

IEF allows containerized applications and functions to be deployed on edge nodes, and manages these applications and functions.

- Containerized applications can be developed in any programming language.
- Python 2.7 and Python 3.6 functions can be deployed on edge nodes.

6.6 Do I Need to Prepare Edge Nodes by Myself?

Yes. Edge nodes must meet requirements described in **Requirements**.

6.7 Can I Still Use the Previously Delivered Applications After My Account Is in Arrears?

If your account is in arrears, your applications will be frozen and enter a retention period. (The retention period varies depending on the account. You can query the retention period in the Billing Center.) During the retention period, you can view

 Copyright © Huawei Technologies Co., Ltd.

application details on the IEF console but cannot perform any other operation. If you still do not complete the renewal or payment after the retention period has ended, the applications will be forcibly deleted.

For example:

1. When your account was in arrears on Dec 10, 2019, a retention period (for example, 15 days) started and billing stopped. During the retention period, you can only view application details but cannot perform any other operation.
2. If the account was still in arrears after the retention period ended on Dec 25, 2019, all applications under the account were forcibly deleted.

6.8 What Are the Differences Between IEF and IoT Edge?

- IEF provides users with integrated services under edge-cloud synergy. With powerful application management and edge-cloud synergy, IEF can deliver applications from the cloud to the edge in a unified manner, and manage, monitor, and maintain applications in the cloud.
- IoT Edge is mainly used for edge device management. It can connect to devices using various protocols and clean data at the edge.

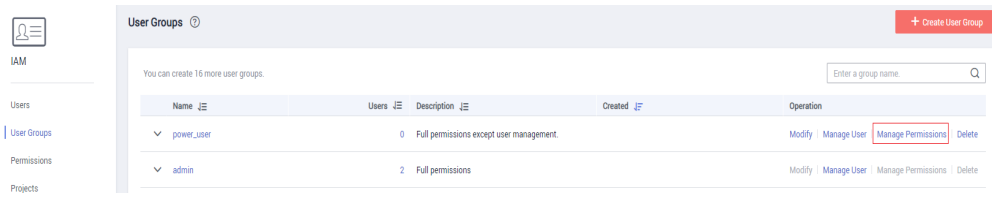
6.9 How Do I Configure IEF Permissions for an IAM User?

IEF does not support fine-grained permission management using Identity and Access Management (IAM). You are advised to log in to IEF using an account. If you need to log in to IEF as an IAM user, assign permissions defined in the **Tenant Administrator** policy to the IAM user.

IAM users without permissions may fail to register edge nodes and create applications.

Step 1 Log in to the IAM console. Choose **User Groups** from the navigation pane, and choose **Manage Permissions** in the same row as the target user group.

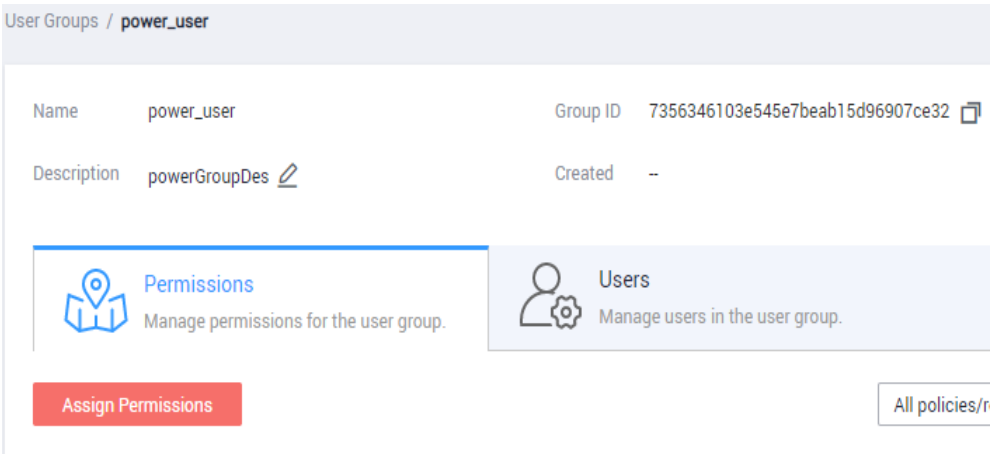
Figure 6-2 User group list



Step 2 On the **Permissions** tab page, click **Assign Permissions** above the permission list.

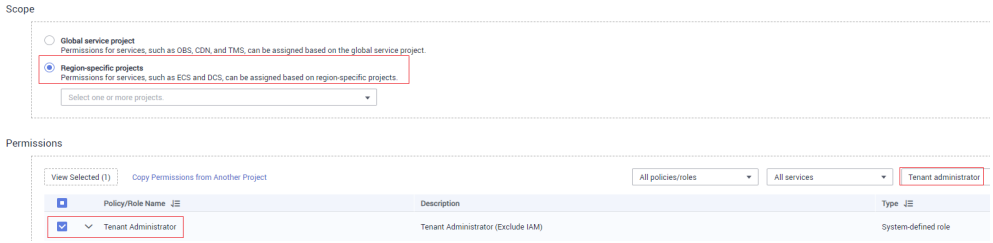
 Copyright © Huawei Technologies Co., Ltd.

Figure 6-3 Permissions tab page



Step 3 Select a region-specific project, search for **Tenant Administrator**, select it, and click **OK**.

Figure 6-4 Selecting permissions



----End

6.10 What Do I Do If an Agency Fails to Be Automatically Created?

If an IAM user does not have sufficient permissions, an agency cannot be automatically created. To solve this problem, assign permissions defined in the **Tenant Administrator** policy to the IAM user. For details, see **Creating a User and Granting Permissions**.

 Copyright © Huawei Technologies Co., Ltd.