

Intelligent EdgeFabric

FAQs

Issue 05
Date 2024-01-19



Copyright © Huawei Technologies Co., Ltd. 2024. 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



HUAWEI 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.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

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?.....	8
1.3 What Do I Do If Edge Node Management Fails?.....	9
1.4 How Do I Obtain the Latest Device Properties After Device Properties Are Updated?.....	19
1.5 What Operations Can I Perform After a Device Is Associated with a Node?.....	19
1.6 Does an Edge Node Support Multiple GPUs?.....	19
1.7 Can I Change the GPU on a Running Edge Node?.....	19
1.8 How Is Edge Environment Security Protected?.....	19
1.9 Why Cannot I View Monitoring Data on an Edge Node?.....	21
1.10 How Can I Restore a Deleted Edge Node?.....	22
1.11 What Is the Impact of IP Address Changing on an Edge Node?.....	22
1.12 What Do I Do If the NTP Configuration Cannot Be Modified?.....	22
1.13 How Do I Synchronize Time with the NTP Server?.....	22
1.14 How Do I Obtain the IP Addresses of IEF Cloud Services?.....	24
1.15 What Do I Do If the Edge Node Space Is Insufficient?.....	26
1.16 How Do I Set Docker Cgroup Driver After Installing Docker on an Edge Node?.....	27
2 Edge Application FAQs.....	28
2.1 What Do I Do If an Application Fails to Be Delivered to an Edge Node?.....	28
2.2 What Do I Do If a Containerized Application Fails to Be Started on an Edge Node?.....	32
2.3 What Do I Do If a Containerized Application Fails to Be Upgraded?.....	35
2.4 What Do I Do If a Container Image Fails to Be Pulled?.....	36
2.5 Why Cannot I View Application Logs and System Logs?.....	41
2.6 How Do Applications Schedule GPU Resources?.....	42
2.7 How Do I Control the Disk Space Occupied by a Container Engine?.....	42
2.8 What Do I Do If a Containerized Application Cannot Access External IP Addresses.....	43
2.9 What Do I Do If the Ascend AI Accelerator Card (NPU) Is Abnormal?.....	44
3 Edge-Cloud Message FAQs.....	46
3.1 What Is Route Management?.....	46
3.2 What Is a Message Endpoint in Route Management?.....	46
3.3 What Is a Route?.....	47
3.4 Why Does a Route Fail to Be Created?.....	47

3.5 What Can I Do If a Message Fails to Be Forwarded over a Route?.....	47
3.6 What Is the Impact of Disabling a Route?.....	47
3.7 What Can I Do If SystemEventBus (MQTT Broker) of an Edge Node Fails to Be Connected?.....	48
4 Network Management FAQs.....	49
4.1 How Does an Edge Node Connect to IEF?.....	49
4.2 What Additional Settings Are Required If the Proxy Is Enabled?.....	49
5 Basic Concept FAQs.....	53
5.1 What Is Intelligent EdgeFabric?.....	53
5.2 What Benefits Does IEF Bring?.....	53
5.3 What Are the Main Application Scenarios of IEF?.....	53
6 Others.....	55
6.1 Region and AZ.....	55
6.2 What Are the Specifications of Edge Nodes Supported by IEF?.....	56
6.3 What Are the Differences Between Device Properties and Device Twins?.....	58
6.4 What Programming Language Is Required for IEF Development?.....	59
6.5 Do I Need to Prepare Edge Nodes by Myself?.....	59
6.6 Can I Still Use the Previously Delivered Applications After My Account Is in Arrears?.....	61
6.7 What Are the Differences Between IEF and IoT Edge?.....	61
6.8 What Do I Do If an Agency Fails to Be Automatically Created?.....	61
6.9 How Can I Deal With Insufficient Permissions?.....	62
6.10 How Will the Multi-AZ Reconstruction of SWR Application Container Image Data Affect IEF?.....	63

1 Edge Node FAQs

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

Symptom


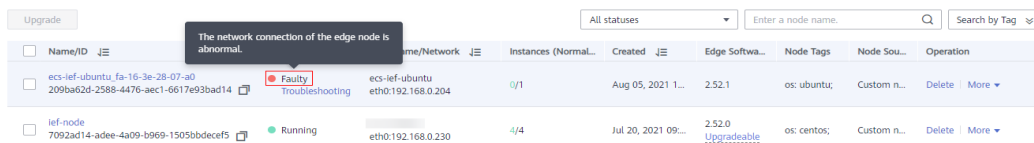


An edge node is in the **Faulty** state, and the fault cause is displayed when the cursor is hovered over  **Faulty**.

Figure 1-1 Node fault



Name/ID	Name/Network	Instances (Normal...)	Created	Edge Softwa...	Node Tags	Node Sou...	Operation
<input type="checkbox"/> ecs-lef-ubuntu_fa-16-3e-28-07-a0 209ba62d-2588-4476-ae1-6617e93bad14	 ecs-lef-ubuntu eth0:192.168.0.204	0/1	Aug 05, 2021 1...	2.52.1	os: ubuntu;	Custom n...	Delete More
<input type="checkbox"/> lef-node 7092ad14-a4ee-4a09-b969-1505bbdecefs	 eth0:192.168.0.230	4/4	Jul 20, 2021 09:...	2.52.0 Upgradeable	os: centos;	Custom n...	Delete More

Fault Locating

Locate the cause of the edge node fault as follows:

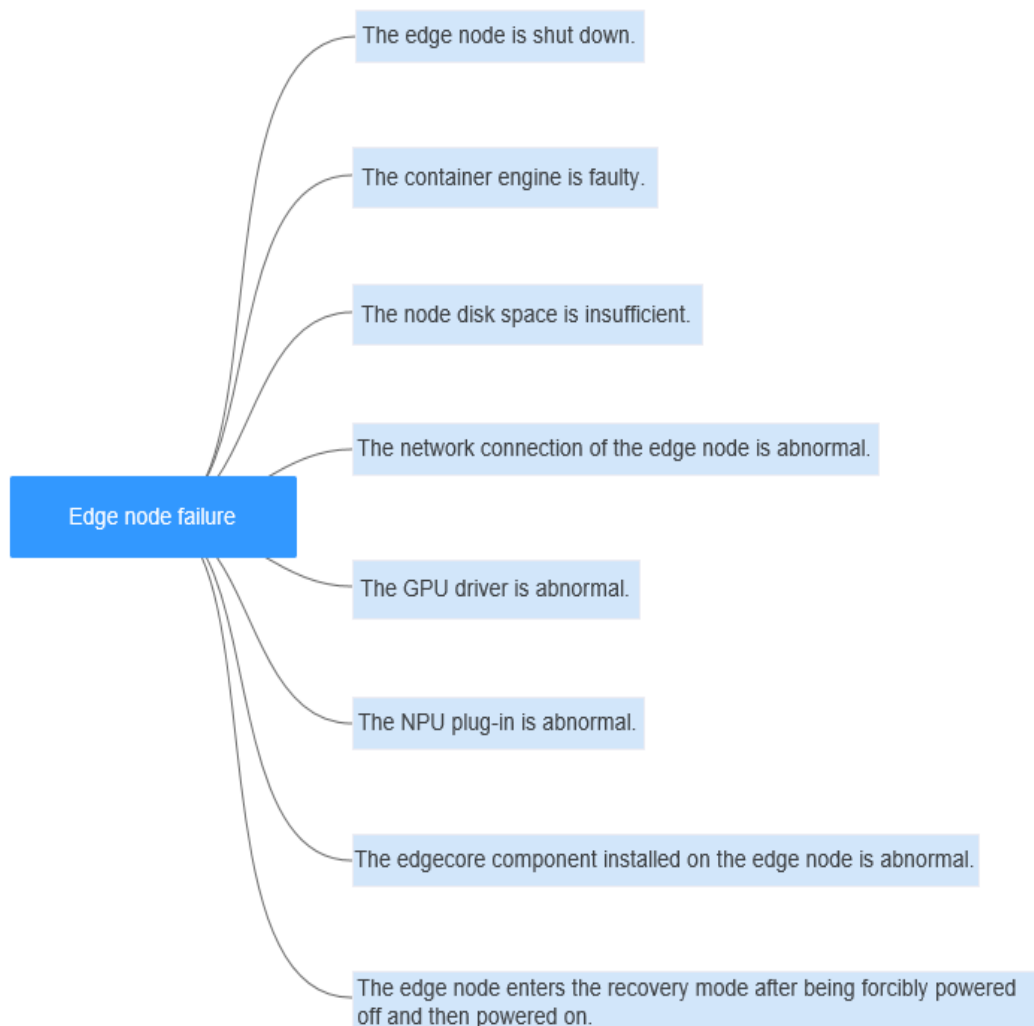


Table 1-1 Fault locating

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.	<ul style="list-style-type: none"> • 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

Possible Cause	Solution
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 NPU plug-in is abnormal.	NPU Plug-in Is Abnormal
The edgecore component installed on the edge node is abnormal.	edgecore Is Abnormal
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**

You are billed for the number of edge applications not 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
```

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:

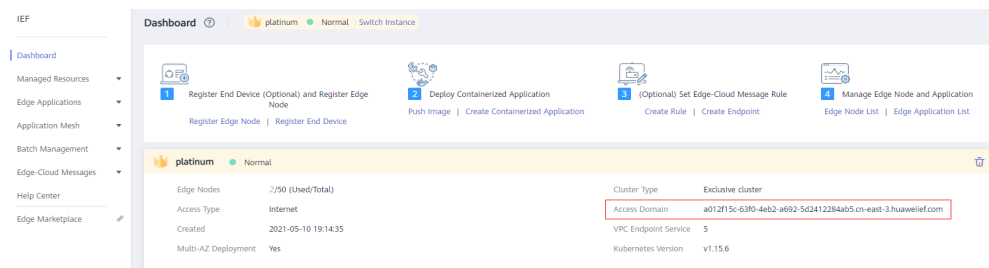
```
cat /opt/IEF/Edge-core/conf/edge.yaml | grep ws-url
```

Information similar to the following is displayed:

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

In the preceding command output,

ief2-edgeaccess.cn-north-4.myhuaweicloud.com indicates the required address. The address varies according to the region. The address format of a platinum service instance is **1fc0704e-229c-4210-9802-75f66aeffe3d.cn-north-4.huaweiief.com**. You can also view the address, that is, **Access Domain**, on the IEF console.

Figure 1-2 Viewing the cloud access domain name

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)
* 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_container1:88125631e9
5e4d3fbdfa7e6ced0f9dd4,OID.1.1.1.2=cn-north-4:42701fe8761
1496e80c824778c9857ca:op_cfe_kubelet,OID.1.1.1.1=op_svc_ief_container1,CN=paas.placement.c
erts.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

Step 1 Install a GPU driver.

Currently, IEF supports only NVIDIA Tesla P4, P40, and T4 GPUs and the GPU drivers that match CUDA Toolkit 8.0 to 11.0.

1. Download the GPU driver. The recommended driver link is as follows:

```
https://www.nvidia.com/content/DriverDownload-March2009/confirmation.php?url=/tesla/440.33.01/NVIDIA-Linux-x86\_64-440.33.01.run&lang=us&type=Tesla
```

2. Run the following command to install the GPU driver:

```
bash NVIDIA-Linux-x86_64-440.33.01.run
```

3. Run the following command to check the GPU driver installation status:

```
nvidia-smi
```

Step 2 Copy GPU driver files to specific directories.

1. Log in to the edge node as user **root**.

2. Run the following command:

```
nvidia-modprobe -c0 -u
```

3. Create directories.

```
mkdir -p /var/IEF/nvidia/drivers /var/IEF/nvidia/bin /var/IEF/nvidia/lib64
```

4. Copy GPU driver files to the directories.

- For CentOS, run the following commands in sequence to copy the driver files:

```
cp /lib/modules/{Kernel version of the current environment}/kernel/drivers/video/nvi* /var/IEF/nvidia/drivers/
```

```
cp /usr/bin/nvidia-* /var/IEF/nvidia/bin/
```

```
cp -rd /usr/lib64/libcuda* /var/IEF/nvidia/lib64/
```

```
cp -rd /usr/lib64/libEG* /var/IEF/nvidia/lib64/
```

```
cp -rd /usr/lib64/libGL* /var/IEF/nvidia/lib64/
```

```
cp -rd /usr/lib64/libnv* /var/IEF/nvidia/lib64/
```

```
cp -rd /usr/lib64/libOpen* /var/IEF/nvidia/lib64/  
cp -rd /usr/lib64/libvdpau_nvidia* /var/IEF/nvidia/lib64/  
cp -rd /usr/lib64/vdpau /var/IEF/nvidia/lib64/
```

- For Ubuntu, run the following commands in sequence to copy the driver files:

```
cp /lib/modules/{kernel version of the current environment}/kernel/  
drivers/video/nvi* /var/IEF/nvidia/drivers/  
cp /usr/bin/nvidia-* /var/IEF/nvidia/bin/  
cp -rd /usr/lib/x86_64-linux-gnu/libcuda* /var/IEF/nvidia/lib64/  
cp -rd /usr/lib/x86_64-linux-gnu/libEG* /var/IEF/nvidia/lib64/  
cp -rd /usr/lib/x86_64-linux-gnu/libGL* /var/IEF/nvidia/lib64/  
cp -rd /usr/lib/x86_64-linux-gnu/libnv* /var/IEF/nvidia/lib64/  
cp -rd /usr/lib/x86_64-linux-gnu/libOpen* /var/IEF/nvidia/lib64/  
cp -rd /usr/lib/x86_64-linux-gnu/libvdpau_nvidia* /var/IEF/nvidia/  
lib64/  
cp -rd /usr/lib/x86_64-linux-gnu/vdpau /var/IEF/nvidia/lib64/
```

You can run the **uname -r** command to view the kernel version of the current environment, for example, **3.10.0-514.e17.x86_64**. Replace the kernel version with the actual value.

```
# uname -r  
3.10.0-514.e17.x86_64
```

5. Run the following command to change the directory permissions:

```
chmod -R 755 /var/IEF
```

----End

NPU Plug-in Is Abnormal

Step 1 Log in to the edge node.

Step 2 Run the following command to check whether the NPU driver container runs properly:

```
docker ps -a |grep npu
```

Step 3 If the container is not in the **Running** status, restart the container.

```
docker restart {container_name}
```

{container_name} indicates the container name.

----End

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.
- 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
- NPU plug-in exception

For details about how to rectify the fault, see [What Do I Do If an Edge Node Is Faulty?](#).

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.

Figure 1-3 Fault locating



Table 1-2 Fault locating

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

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	<p>The language of the operating system must be English.</p> <ul style="list-style-type: none"> • x86_64 architecture Ubuntu LTS (Xenial Xerus), Ubuntu LTS (Bionic Beaver), CentOS, EulerOS, RHEL, Kylin, NewStart CGS Linux, NeoKylin, openEuler, Unity Operating System (UOS), Oracle Linux (OL), Huawei Cloud Euler (HCE), openEuler 23.09 Edge • Armv7i (Arm32) architecture Raspbian GNU/Linux (stretch) • AArch64 (Arm64) architecture Ubuntu LTS (Xenial Xerus), Ubuntu LTS (Bionic Beaver), CentOS, EulerOS, RHEL, Kylin, NewStart CGS Linux, NeoKylin, openEuler, Unity Operating System (UOS), Oracle Linux (OL), Huawei Cloud Euler (HCE), openEuler 23.09 Edge <p>NOTE The openEuler 23.09 Edge operating system is recommended for edge computing scenarios.</p>
Memory	<p>More than 256 MB of memory is recommended as 128 MB of memory is required to run the edge software.</p>
CPU	<p>≥ 1 core</p>
Hard disk	<p>≥ 1 GB</p>
GPU (optional)	<p>The GPU models on the same edge node must be the same.</p> <p>NOTE Currently, NVIDIA Tesla GPUs such as P4, P40, and T4 are supported.</p> <p>If an edge node is equipped with GPUs, you can choose not to enable its GPUs when registering it on IEF.</p> <p>If you choose to enable GPUs of an edge node, the GPU driver has to be installed on the edge node before you can manage it on IEF.</p> <p>Currently, only x86-based GPU nodes can be managed by IEF.</p>

Item	Specifications
NPU (optional)	<p>Ascend AI processors</p> <p>NOTE Currently, edge nodes integrated with Ascend Processors are supported, such as Atlas 300 inference cards, and Atlas 800 inference servers. Supported NPU specifications include Ascend 310P, 310B, Ascend 310P-share, and virtualization partition NPUs..</p> <p>If you choose to enable NPUs of an edge node, ensure that the NPU driver has been installed on it. Currently, Ascend 310 supports only firmware versions 1.3.x.x and 1.32.x.x, for example, 1.3.2.B893. You can run the npu-smi info command to view your firmware version.The NPU driver version must be 22.0.4 or later. You can go to the driver path, for example, /usr/local/Ascend/driver, and run the cat version.info command to view your driver version. If the driver is not installed, contact the device manufacturer for assistance.</p>
Container engine	<p>The Docker version must be later than 17.06. If Docker 1.23 or later is used, set the docker cgroupfs version to 1. Docker HTTP API v2 is not supported.</p> <p>(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.)</p> <p>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.</p> <p>Docker Cgroup Driver must be set to cgroupfs. For details, see How Do I Set Docker Cgroup Driver After Installing Docker on an Edge Node?.</p>
Glibc	The Glibc version must be later than 2.17.
Port	Edge nodes require port 8883, which is the listening port of the built-in MQTT broker on edge nodes. Ensure that this port works properly.
Time synchronization	The time on an edge node must be consistent with the UTC time. Otherwise, the monitoring data and logs of the edge node may be inaccurate. You can select an NTP server for time synchronization. For details, see How Do I Synchronize Time with the NTP Server?

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](#).

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
```

In the preceding command, *node_id* indicates the edge 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 choose to enable GPUs of an edge node, the GPU driver has to be installed on the edge node before you can manage it on IEF. Currently, IEF supports only NVIDIA Tesla P4, P40, and T4 GPUs and the GPU drivers that match CUDA Toolkit 8.0 to 11.0.

Step 1 Install a GPU driver.

Currently, IEF supports only NVIDIA Tesla P4, P40, and T4 GPUs and the GPU drivers that match CUDA Toolkit 8.0 to 11.0.

1. Download the GPU driver. The recommended driver link is as follows:
https://www.nvidia.com/content/DriverDownload-March2009/confirmation.php?url=/tesla/440.33.01/NVIDIA-Linux-x86_64-440.33.01.run&lang=us&type=Tesla
2. Run the following command to install the GPU driver:
bash NVIDIA-Linux-x86_64-440.33.01.run
3. Run the following command to check the GPU driver installation status:
nvidia-smi

Step 2 Copy GPU driver files to specific directories.

1. Log in to the edge node as user **root**.
2. Run the following command:
nvidia-modprobe -c0 -u
3. Create directories.
mkdir -p /var/IEF/nvidia/drivers /var/IEF/nvidia/bin /var/IEF/nvidia/lib64
4. Copy GPU driver files to the directories.
 - For CentOS, run the following commands in sequence to copy the driver files:
**cp /lib/modules/{Kernel version of the current environment}/kernel/drivers/video/nvi* /var/IEF/nvidia/drivers/
cp /usr/bin/nvidia-* /var/IEF/nvidia/bin/
cp -rd /usr/lib64/libcuda* /var/IEF/nvidia/lib64/
cp -rd /usr/lib64/libEG* /var/IEF/nvidia/lib64/
cp -rd /usr/lib64/libGL* /var/IEF/nvidia/lib64/
cp -rd /usr/lib64/libnv* /var/IEF/nvidia/lib64/
cp -rd /usr/lib64/libOpen* /var/IEF/nvidia/lib64/
cp -rd /usr/lib64/libvdpau_nvidia* /var/IEF/nvidia/lib64/
cp -rd /usr/lib64/vdpau /var/IEF/nvidia/lib64/**
 - For Ubuntu, run the following commands in sequence to copy the driver files:
**cp /lib/modules/{Kernel version of the current environment}/kernel/drivers/video/nvi* /var/IEF/nvidia/drivers/
cp /usr/bin/nvidia-* /var/IEF/nvidia/bin/
cp -rd /usr/lib/x86_64-linux-gnu/libcuda* /var/IEF/nvidia/lib64/
cp -rd /usr/lib/x86_64-linux-gnu/libEG* /var/IEF/nvidia/lib64/
cp -rd /usr/lib/x86_64-linux-gnu/libGL* /var/IEF/nvidia/lib64/
cp -rd /usr/lib/x86_64-linux-gnu/libnv* /var/IEF/nvidia/lib64/
cp -rd /usr/lib/x86_64-linux-gnu/libOpen* /var/IEF/nvidia/lib64/
cp -rd /usr/lib/x86_64-linux-gnu/libvdpau_nvidia* /var/IEF/nvidia/lib64/**

```
cp -rd /usr/lib/x86_64-linux-gnu/vdpau /var/IEF/nvidia/lib64/
```

You can run the **uname -r** command to view the kernel version of the current environment, for example, **3.10.0-514.e17.x86_64**. Replace the kernel version with the actual value.

```
# uname -r  
3.10.0-514.e17.x86_64
```

5. Run the following command to change the directory permissions:

```
chmod -R 755 /var/IEF
```

----End

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 (in the active state), 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 managing the edge node, causing a management failure. To rectify the fault, delete the redundant docker0 bridge address and manage the edge node again.

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, edgecore fails to be installed.

After the edge node is properly managed, edgecore listens at port 8883. Therefore, ensure that port 8883 is not occupied.

```
[root@ ~]# netstat -npl | grep 8883
tcp        0      0 172.17.0.1:8883      0.0.0.0:*           LISTEN    18150/edge_core
tcp        0      0 127.0.0.1:8883      0.0.0.0:*           LISTEN    18150/edge_core
```

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, **not running** 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/

In the preceding command, **ief2-edgeaccess.cn-north-4.myhuaweicloud.com** indicates the edgeaccess domain name of the service instance. The domain name varies according to the region. For details, see [Domain Name of the Professional Service Instance](#) or [Domain Name of the Platinum Service Instance](#).

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.

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 **ief-placement.cn-east-3.myhuaweicloud.com**. You can run the **cat /opt/IEF/Cert/user_config** command to query the domain name of your region.
- edgeaccess domain name of the service instance, for example, **ief2-edgeaccess.cn-north-4.myhuaweicloud.com**. This domain name varies according to the region and service instance. For details, see [Domain Name of the Professional Service Instance](#) or [Domain Name of the Platinum Service Instance](#).

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
```

If a message indicating that node **node_id** has been occupied is displayed, the certificate is repeatedly used, as shown below.

```
2019-12-25 15:32:48.780 +08:00 ERROR wsClient/websocket.go:85 error when init websocket connection , response code: 400, response body: node dc89f34b-a72c-4672-91fb-c19d637fe36a, unique_id
is different from unique_id in db, refuse to connect
..error:websocket: bad handshake
2019-12-25 15:33:34.988 +08:00 ERROR wsClient/websocket.go:85 error when init websocket connection , response code: 400, response body: node dc89f34b-a72c-4672-91fb-c19d637fe36a, unique_id
is different from unique_id in db, refuse to connect
..error:websocket: bad handshake
```

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 edlogger
```

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
```

⚠ CAUTION

The following misoperation may occur:

To manage the edge node again, rename the original **/opt** directory of the node **/opt_old**, create the **/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.

- After the uninstallation is complete, delete the managed components, generated logs, and downloaded configuration files.

Figure 1-4 Files in the **/opt** directory

```
[root@ecs-c0e9-gwx215305 log]# vim edge_core.log
[root@ecs-c0e9-gwx215305 log]# cd /opt/
[root@ecs-c0e9-gwx215305 opt]# ll
total 32
drwxr-x--- 3 root root 4096 Jan 14 2021 cloud
drwx--x--x 4 root root 4096 Jan 14 2021 containerd
drwxr-x--- 4 root root 4096 Sep  8 16:11 edge-installer
drwx----- 7 ief ief 4096 Sep  8 16:03 IEF
drwxr-x--- 2 root root 4096 Sep  8 16:03 IEF_firmware
d----- 3 root root 4096 Sep  8 16:03 IEFpack
drwx----- 2 root root 4096 Sep  8 16:03 material
older drwxr-xr-x 4 root root 4096 Jan 14 2021 uvp
```

To delete the managed components shown in the red box, run the **rm -rf /opt/edge-installer**, **rm -rf /opt/IEF**, **rm -rf /opt/IEF_firmware**, **rm -rf /opt/IEFpack**, and **rm -rf /opt/material** commands.

To delete logs, run the **rm -rf /var/IEF** command.

To delete configuration files, run the **rm -rf edge-installer_1.0.10_x86_64.tar.gz ief-node.tar.gz** command.

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

- If end 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 end device information by calling the API provided by IEF, you can use the API for querying end device details to obtain the latest end device properties. For details about the API, see [Querying Details About an End Device](#).

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

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

1.6 Does an Edge Node Support Multiple GPUs?

An edge node supports multiple graphics cards of the same GPU model.

Currently, NVIDIA Tesla P4, P40, and T4 GPUs are supported. For an edge node with GPU hardware, GPUs are not required.

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

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

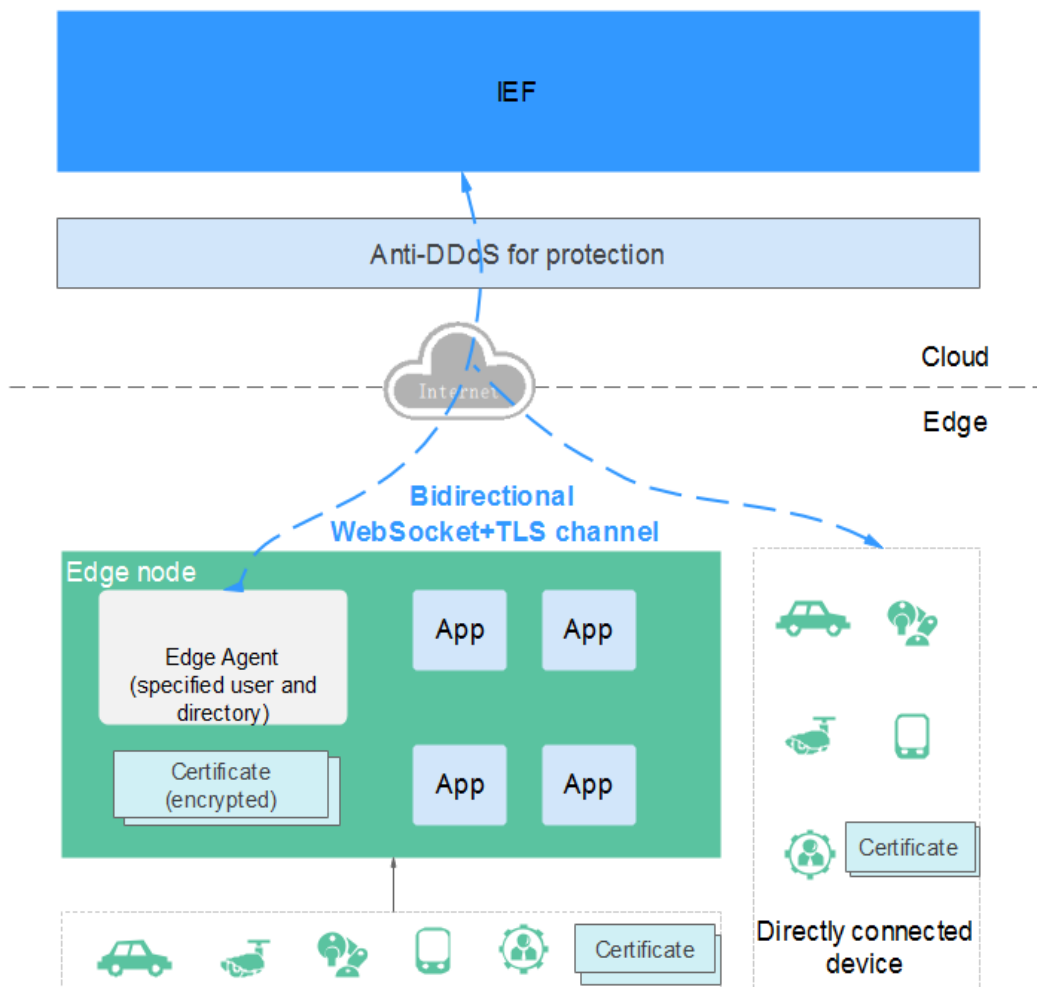
1. Run the following commands to stop the IEF Agent service:
systemctl stop edgecore
systemctl stop edgedaemon
2. Replace the GPU, reinstall the GPU driver, and copy GPU driver files. For details, see [Installing and Configuring a GPU Driver](#).
3. Run the following commands to start the IEF Agent service:
systemctl start edgecore
systemctl start edgedaemon

1.8 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 resources such as Application Operations Management (AOM), Data Ingestion Service (DIS), and SoftWare Repository for Container (SWR).
- 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
End devices use certificates for identity authentication.

Figure 1-5 IEF security solution



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

Analysis

No agency is created or configured for IEF. Therefore, IEF cannot report monitoring data of edge nodes 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.

When you enter the IEF console for the first time, the **Authorize Access** page is displayed. Click **Authorize**. An agency named **ief_admin_trust** is automatically created.

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

----End

1.10 How Can I Restore a Deleted Edge Node?

To restore an edge node that has been deleted, you must register and manage it again. Do not install the EdgeCore installer and configuration file of the deleted edge node on the new edge node. The edge nodes registered on IEF have one-to-one relationships with the physical devices. The EdgeCore installer and configuration file of an edge node can be installed on only one physical device.

References:

- [Registering an Edge Node](#)
- [Managing an Edge Node](#)

1.11 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.

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

The ntpd process may not be started on the edge node. Perform the following steps:

1. Log in to the edge node.
2. Run the **systemctl restart ntpd** command on the edge node to restart the ntpd process.

1.13 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 can run the **rpm -qa | grep ntp** command on CentOS to check whether ntpd is installed. If version information similar to **ntp-x.x.x.centos.x86_64**

is displayed, ntpd has been installed. If no version information is displayed, run the **yum -y install ntp** command to install ntpd.

Procedure

Step 1 Log in to the edge node.

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
```

For details about the NTP server domain name, see [Does Huawei Cloud Provide the NTP Server and How Can I Install It?](#).

Example:

```
server ntp.myhuaweicloud.com
```

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

SUSE OS:

```
service ntpd restart
```

CentOS:

```
systemctl restart ntpd
```

NOTE

Run the appropriate command based on the OS running on the edge node.

Step 5 Run the following command to check whether the time of the edge node 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.

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

SUSE OS:

```
chkconfig ntp on
```

CentOS:

```
chkconfig ntpd on
```

```
----End
```

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

If you need to run your edge node on IEF, ensure that the edge node can communicate with IEF, SWR, OBS, and AOM. 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 and use the IP addresses and port numbers to configure the firewall. This configuration enables the edge node to access IEF, SWR, OBS, and AOM.

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:
```

Domain Name of the Professional Service Instance

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
	swr.cn-north-4.myhuaweicloud.com	443
	op-svc-swr-b051-10-38-19-62-3az.obs.cn-north-4.myhuaweicloud.com	443
	obs.cn-north-4.myhuaweicloud.com	443

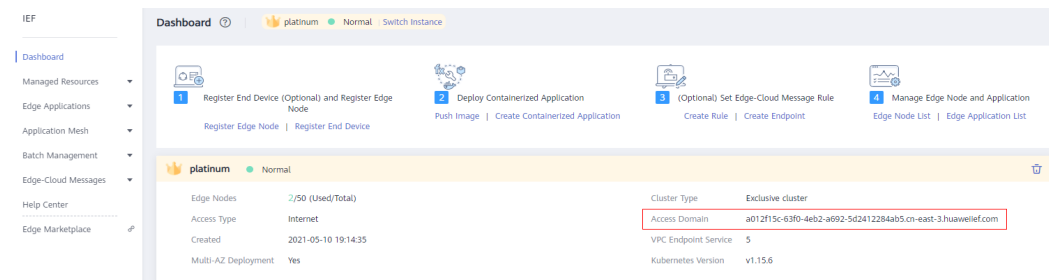
Region	Domain Name	Port
	ief-software-north-4.obs.cn-north-4.myhuaweicloud.com	443
CN South-Guangzhou	ief-placement.cn-south-1.myhuaweicloud.com	443
	ief-edgeaccess.cn-south-1.myhuaweicloud.com	443
	ief-telemetry.cn-south-1.myhuaweicloud.com	8102, 8149, and 8065
	swr.cn-south-1.myhuaweicloud.com	443
	op-svc-swr-b051-10-230-33-197-3az.obs.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
	op-svc-swr-b051-10-147-7-14-3az.obs.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

Domain Name of the Platinum Service Instance

The edgeaccess domain name of the platinum service instance is different from that of the professional service instance. Other domain names of the platinum service instance are the same as those of the [professional service instance](#).

The edgeaccess domain name of each platinum service instance is unique. You can view it on the **Dashboard** page of the console, that is, the value of **Access Domain**.

Figure 1-6 edgeaccess domain name



1.15 What Do I Do If the Edge Node Space Is Insufficient?

According to the [Specifications Requirements](#), the disk size of an edge node must be 1 GB or greater. If the disk space is insufficient during the running of the edge node, you can expand the disk capacity. If the capacity cannot be expanded, perform the following operations to reduce the storage space occupied by the edge node:

Deleting Container Images That Are No Longer Required

1. Run the **docker images** command to view images on the node.
2. Run the **docker rmi \$ImageID** command to delete images that are no longer required.

Reducing the Size of Dumped Logs

1. On the IEF console, click the name of the edge node in the **Edge Nodes** list to enter the details page, and click the **Configuration** tab.
2. In the **Log Configuration** area, click **Edit** under **System Logs** and **Application Logs** to reduce the maximum log size and the number of logs saved.

Reducing the Output of Container Logs

If a large number of logs are generated by containerized applications on the edge node and mounted to the host, the logs may occupy large storage space on the node.

Check whether there are containerized applications that generate a large number of logs. If yes, enter the details page of the containerized application, click the **Upgrade** tab, and choose **Data Storage** under **Advanced Settings** to check

whether logs are mounted to the local volume. If yes, delete the corresponding volume, and update the application. If you do not need to persistently store the mounted content, you are advised to use a local volume of the emptyDir type. For details about how to configure data storage for an edge application, see [Creating an Edge Application](#).

1.16 How Do I Set Docker Cgroup Driver After Installing Docker on an Edge Node?

After installing Docker on an edge node, you must set Docker **Cgroup Driver** to **cgroupfs**. Generally, it is set to **cgroupfs** by default. For other values, perform the following steps to reset it:

- Step 1** Run the **docker info** command to check whether the value of the **Cgroup Driver** parameter is **cgroupfs**. If not, go to the next step.

```
...
Logging Driver: json-file
Cgroup Driver: cgroupfs
Hugetlb Pagesize: 2MB, 1GB (default is 2MB)
Plugins:
Volume: local
Network: bridge host macvlan null overlay
...
```

- Step 2** Run the **vim /etc/docker/daemon.json** command to create a Docker configuration file or edit an existing one (if any).

- Step 3** Add the following content to the configuration file:

```
{
  "exec-opts": ["native.cgroupdriver=cgroupfs"]
}
```

 **NOTE**

If the file contains content, add a comma (,) at the end of the last line before adding the new content.

- Step 4** Run the **systemctl daemon-reload && systemctl restart docker** command to reload the configuration file and restart Docker.

----End

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

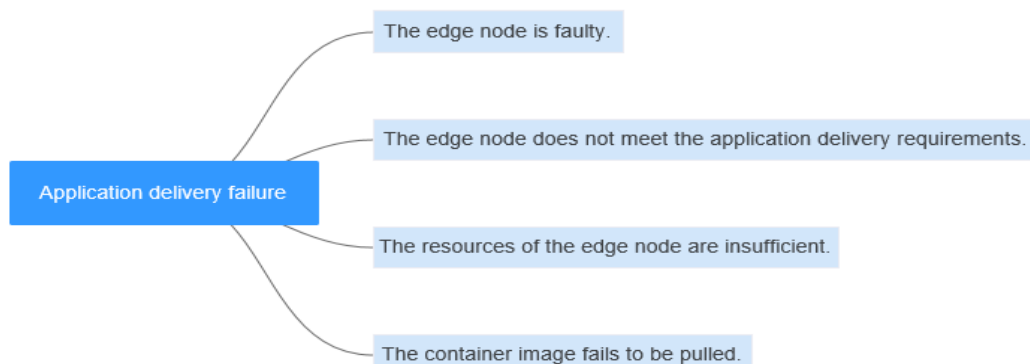


Table 2-1 Fault locating

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

Edge Node Does Not Meet the Application Delivery Requirements

Step 1 Check the resource information 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.

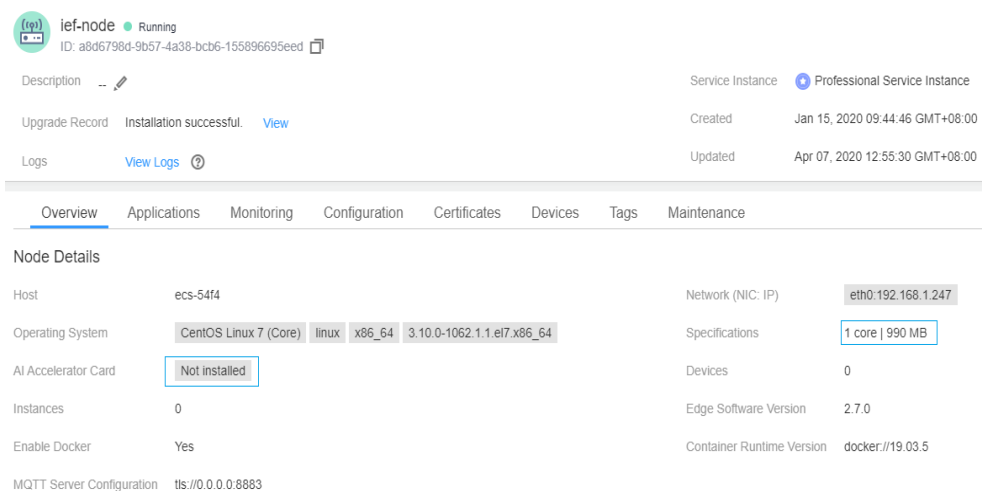
If you manage the edge node for the first time, rectify the fault by following the procedure described in [What Do I Do If a Containerized Application Fails to Be Started on an Edge Node?](#)

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) 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.



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.


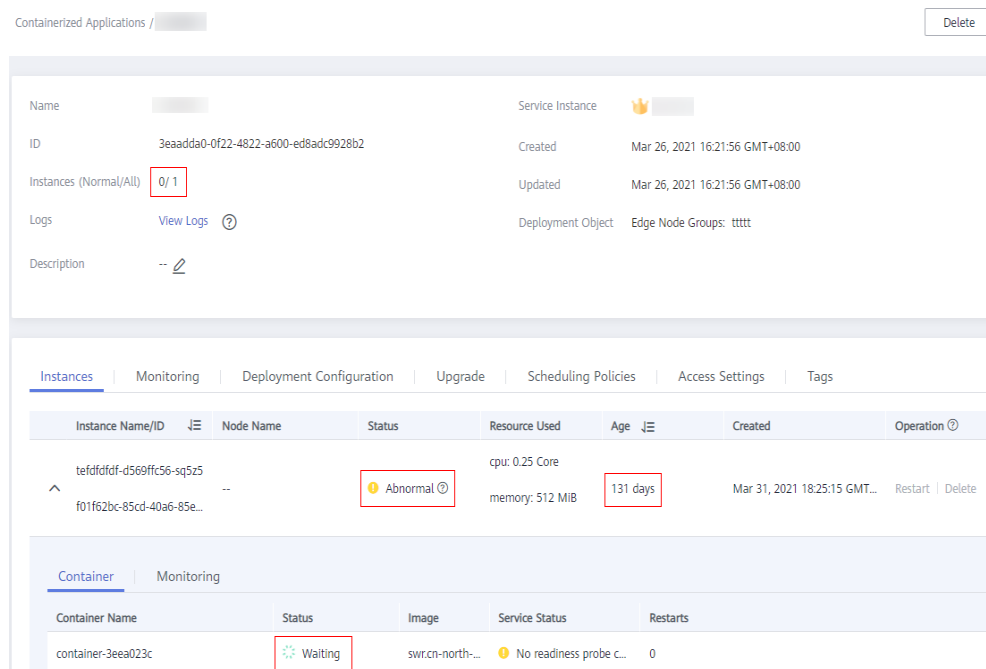
Hover the cursor over the  icon next to the instance status to view the cause of the application delivery failure.

Figure 2-2 Instance list

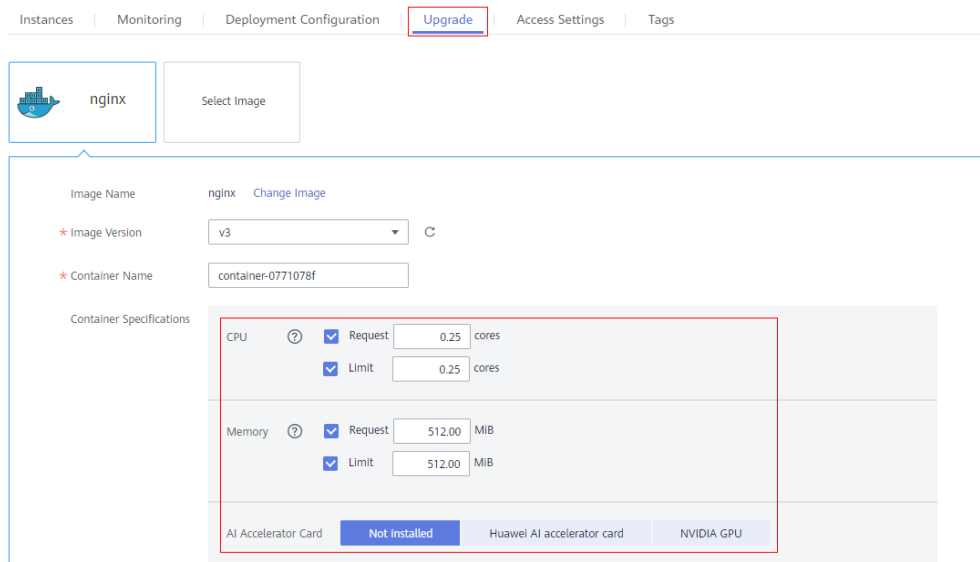


Step 2 Check the size of the resources requested by the application.

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

Figure 2-3 shows how to check the amount of resources requested by the application.

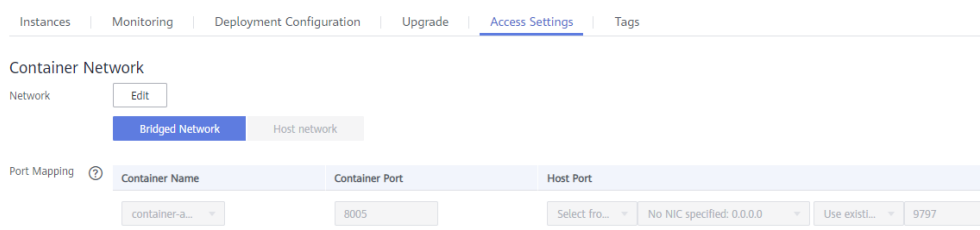
Figure 2-3 Upgrade



Step 3 Check whether a port conflict occurs. If a port conflict occurs, the application instance cannot be started.

Go to the application details page, click the **Access Settings** tab, and check whether the port mapping or host network of the specified port is configured for the application.

Figure 2-4 Access settings



- For a single-instance application:
Set the access mode to **Bridged Network**, and change the port number to an available port on the current node. Alternatively, you can set it to assign ports automatically, and IEF will select an available port for the application.
- For a multi-instance application:
If external access is required for a multi-instance application, you can use the automatic scheduling deployment mode. The application will select a node with an unused port from the edge node group to deploy the instance.

Alternatively, you can set it to assign ports automatically, and IEF will select an available port for the application to avoid port conflicts.

----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.

Figure 2-5 Fault locating

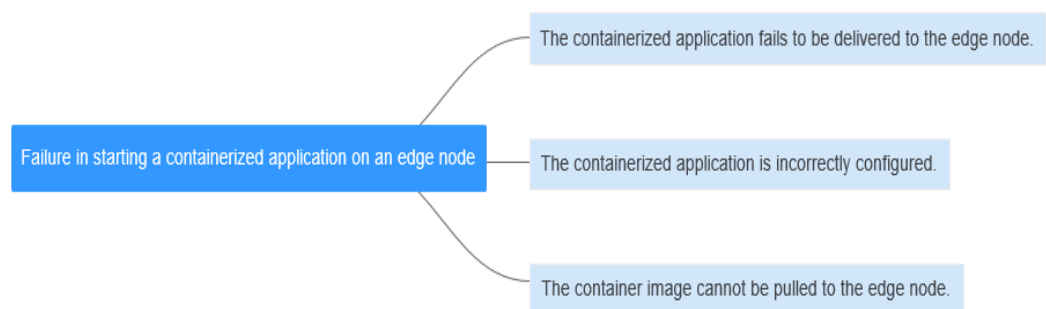


Table 2-2 Fault locating

Possible Cause	Solution
The containerized application fails to be delivered to the edge node.	For details, see 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 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:

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 apply 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** value 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.

Log in to the IEF console, choose **Edge Applications > Containerized Applications**, and click the name of your application. On the details page that is displayed, click the **Upgrade** tab, and choose **Health Check** under **Advanced Settings** to 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.

– 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.

Figure 2-6 Health check configurations

The screenshot displays two configuration panels for health checks. The top panel is for the 'Liveness Probe' and the bottom panel is for the 'Readiness Probe'. Both panels have a 'Check Method' section with radio buttons for 'No configuration', 'HTTP request check', and 'CLI'. The 'Liveness Probe' panel includes input fields for 'Path', 'Port', and 'Host Address', and a 'Protocol' section with radio buttons for 'HTTP' and 'HTTPS'. Below these are 'Delay (s)' and 'Timeout (s)' input fields. The 'Readiness Probe' panel has a 'Check Method' section with radio buttons for 'No configuration', 'HTTP request check', and 'CLI'.

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 [What Do I Do If a Container Image Fails to Be Pulled?](#)

If no log is displayed, [submit a service ticket](#).

----End

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

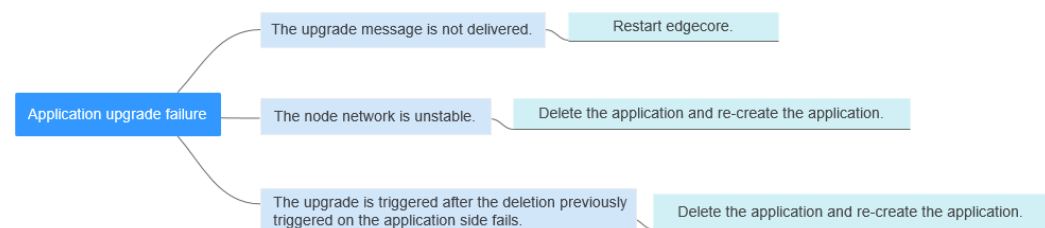
Symptom

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 2-7 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](#).

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 2-8 shows the major causes of the failure to pull the container image. You can locate the fault based on **Table 2-3**.

Figure 2-8 Fault locating

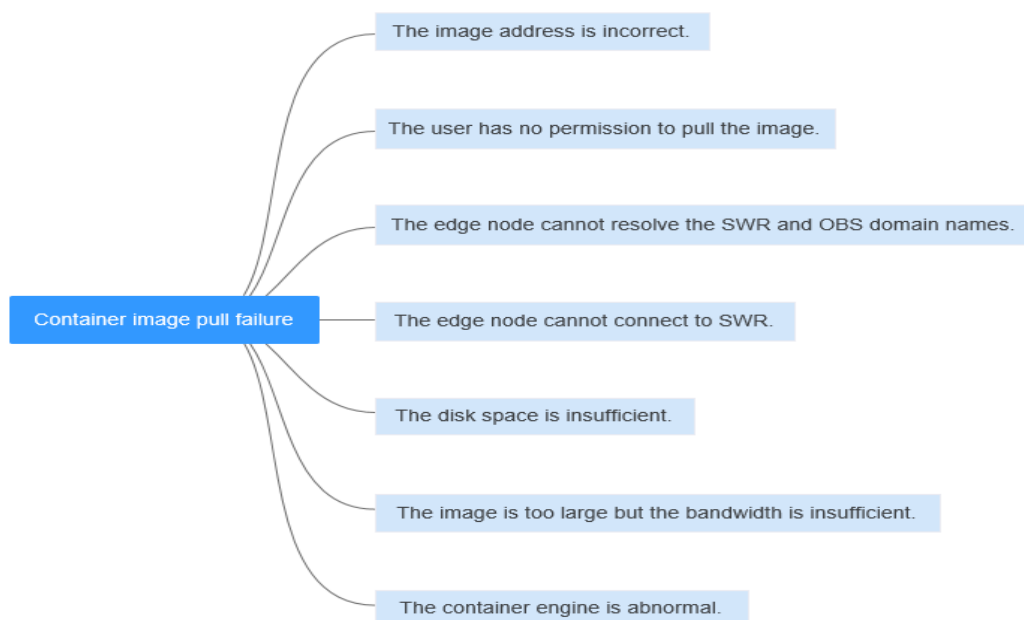


Table 2-3 Fault locating

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

Possible Cause	Solution
The edge node cannot connect to SWR.	Edge Node Cannot Connect to SWR
The disk space is insufficient.	Insufficient Disk Space
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

Perform the following operations to check whether the image address is correct. If the address is incorrect, change it to a correct one.


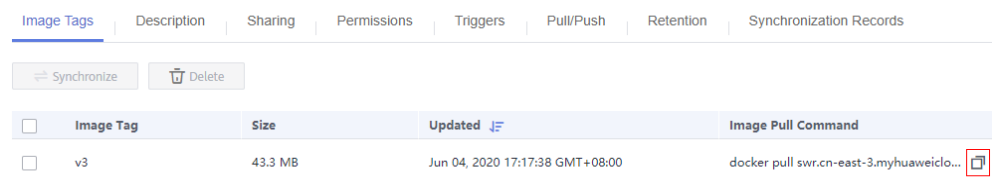
1. Log in to the SWR console.
2. In the navigation pane, choose **My Images**. On the page displayed, click the image that fails to be pulled.
3. On the **Image Tags** tab page, in the same row as the image tag, click  to copy its pull command.

Figure 2-9 Confirming the 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.

Figure 2-10 Obtaining a login command

Image Tags	Description	Sharing	Permissions	Triggers	Pull/Push	Retention	Synchronization Records
------------	-------------	---------	-------------	----------	-----------	-----------	-------------------------

Prerequisite

A PC with container engine 1.11.2 or later is available.

Procedure

Step 1: Log in to the VM running the container engine as the root user.

Step 2: Obtain a login command and run it on the VM to log in to SWR.
[Generate a temporary login command](#) or [learn how to obtain a login command that has long-term validity](#).

Step 3: Pull or push an image.

- Run the following command to pull an image:

```
docker pull swr.cn-east-3.myhuaweicloud.com/ /nginx:{Tag name}
```
- Run the following command to push an image:

```
docker tag {Image name}:{Tag name} swr.cn-east-3.myhuaweicloud.com/ /nginx:{Tag name}
docker push swr.cn-east-3.myhuaweicloud.com/ /nginx:{Tag name}
```

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.
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 SWR

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 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.

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 ($1024 \text{ MB} / 0.2 \text{ MB} = 5,129\text{s}$) 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

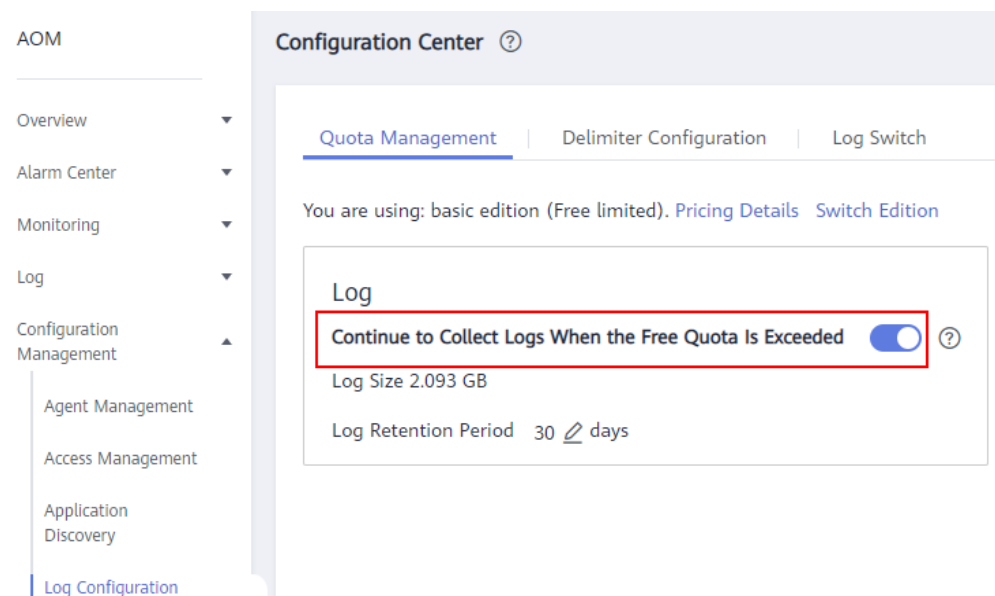
To avoid this problem, you are advised to install the container engine versions recommended by IEF. For details about the container engine version requirements, see [Constraints](#).

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.
Log in to the IEF console. In the navigation pane, choose **Managed Resources > Edge Nodes**. Click an edge node name to access the edge node details page. Then, click the **Configuration** tab, and enable **System Logs** and **Application Logs** under **Log Configuration**.
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](#).
3. The log storage usage exceeds the free quota (500 MB).
AOM offers 500 MB log storage for free every month. If the quota is exceeded, you need to enable **Continue to Collect Logs When the Free Quota Is Exceeded** to view the logs. The excess logs will be billed on a pay-per-use basis. The procedure is as follows:
Log in to the AOM console. In the navigation pane, choose **Configuration Management > Log Configuration**. On the displayed page, enable **Continue to Collect Logs When the Free Quota Is Exceeded**.

Figure 2-11 AOM log settings

2.6 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.

2.7 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"
  ]
}
```

2.8 What Do I Do If a Containerized Application Cannot Access External IP Addresses

Symptom

The edge node can access external IP addresses, but the containerized application cannot access external IP addresses.

Possible Causes

The IP forwarding function of the edge node is not enabled.

Solution

Enable the IP forwarding function on the edge node. The following uses CentOS as an example.

Step 1 Run the following command on the edge node to check whether the IP forwarding function is enabled:

```
cat /proc/sys/net/ipv4/ip_forward
```

If the query result is **1**, the function is enabled, and you need to check other causes. If the query result is **0**, the function is disabled. In this case, go to [Step 2](#).

Step 2 If you only want to enable the function temporarily, run the following command. The temporary solution is applicable to the scenario where the edge node does not restart.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Step 3 To enable it permanently, add **net.ipv4.ip_forward=1** to the **/etc/sysctl.conf** file.

```
vim /etc/sysctl.conf
```

Step 4 Load the file for the change to take effect.


```
sysctl -p  
----End
```

2.9 What Do I Do If the Ascend AI Accelerator Card (NPU) Is Abnormal?

Symptom

The NPU-enabled application fails to be delivered or cannot run.

Solution

If the NPU-enabled application fails to be created:

An application applying for NPU resources must be deployed on a node with the Ascend AI accelerator card enabled. If you deploy an application that applies for NPU resources on a node without an Ascend AI accelerator card enabled during node registration, the system displays a message indicating that the application fails to be created.

As shown in the following figure, select an Ascend AI accelerator card based on the model when registering an edge node.

The screenshot shows a registration form for an edge node. The form includes fields for Service Instance (c-30), Node Name (NPU_NODE), Description (0/255), and Tags. Below the form, there is a message box with an information icon and text: "If you need to deploy NPU or GPU applications, please switch the AI accelerator card type according to your choice. [Edge Node Specifications Requirements](#)". Below the message box, there are three radio button options for "AI Accelerator Card": "Not installed", "Ascend AI accelerator card" (which is selected and highlighted with a red box), and "NVIDIA GPU". Under the "Ascend AI accelerator card" option, there are two sub-options: "Ascend 310" and "Ascend 910".

For a node with Ascend AI accelerator card enabled, you can view the AI accelerator card information and check the healthy chip list on the node details page.

If the NPU-enabled application running status is abnormal:

- Step 1** Ensure that the number of Ascend AI accelerator cards applied for by the current application is not greater than that of healthy chips on the node. Otherwise, the application scheduling will fail.

Check the number of Ascend cards on the **Upgrade** tab page of the containerized application details page:

The screenshot shows the configuration interface for a container. At the top, the 'Image Name' is 'nginx' with a 'Change Image' link. Below it, the 'Image Version' is set to 'latest' and the 'Container Name' is 'container-1f25f1a3'. The 'Container Specifications' section is divided into three parts: CPU, Memory, and AI Accelerator Card. CPU settings show 'Request' and 'Limit' both set to 0.25 cores. Memory settings show 'Request' and 'Limit' both set to 512.00 MIB. The 'AI Accelerator Card' section has three tabs: 'Not installed', 'Ascend AI accelerator card', and 'NVIDIA GPU'. Under the 'Ascend AI accelerator card' tab, there are two radio button options: 'Ascend 310' (selected) and 'Ascend 910'. Each option has a 'Use' label and a text input field containing the number '1'. A red rectangle highlights the 'Ascend 310' radio button and its associated 'Use' field.

Step 2 Log in to the edge node, and check whether the NPU plug-in is normal.

docker ps -a |grep npu-plugin

Step 3 If the container status is abnormal, restart the container.

docker restart \$containerID

Step 4 If the fault persists, go to [What Do I Do If an Application Fails to Be Delivered to an Edge Node?](#) and [What Do I Do If a Containerized Application Fails to Be Started on an Edge Node?](#).

----End

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 Service Bus, 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. End device data forwarding service: A route from SystemEventBus to DIS/API Gateway, in which SystemEventBus forwards the end device data bound to edge nodes to DIS or a specified API Gateway address.

3.2 What Is a Message Endpoint in Route Management?

A message endpoint refers to a party that sends or receives a message. It can be an end device or a cloud service.

IEF provides the following default message endpoints:

- **SystemEventBus**: MQTT broker on an edge node, which can communicate with other endpoints on behalf of the edge node. It can function as a source endpoint to send data to the cloud, or as a destination endpoint to receive messages from the cloud. MQTT topics on the edge node are used as endpoint resources of the MQTT broker.
- **SystemREST**: a REST gateway interface in the cloud. It can function as a source endpoint to send REST requests to the edge. REST request paths are used as endpoint resources of SystemREST.

3.3 What Is a Route?

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

Currently, IEF supports the following message forwarding paths:

- SystemREST -> Service Bus: The REST gateway interface in the cloud is called to obtain file services on edge nodes.
- SystemREST -> SystemEventBus: The REST gateway interface in the cloud is called to send messages to SystemEventBus (MQTT broker) on edge nodes.
- SystemEventBus -> DIS/API Gateway: You can publish end device data to a custom topic in the MQTT broker of an edge node. IEF then forwards the device data to a DIS stream or an API Gateway address. Then, you can extract the data for processing and analysis. You must customize an MQTT topic when creating a message route.

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.
- 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.

Figure 3-1 Disabling

Route Name	Source Endpoint	Destination Endpoint	Status	Forwarded Messages	Created	Operation
ttt	SystemREST Cloud	SystemEventBus Edge	Enabled	Total: 0 Successful: 0 Failed: 0	Dec 06, 2022 09:18:30 GMT+08:00	Disable Delete
--	/fg	fgfg				

Figure 3-2 Enabling

Route Name	Source Endpoint	Destination Endpoint	Status	Forwarded Messages	Created	Operation
ttt	SystemREST Cloud	SystemEventBus Edge	Disabled	Total: 0 Successful: 0 Failed: 0	Dec 06, 2022 09:18:30 GMT+08:00	Enable Delete
--	/fg	/fg				

3.7 What Can I Do If SystemEventBus (MQTT Broker) of an Edge Node Fails to Be Connected?

The MQTT broker functions as the server. You need to start the client process to connect to the MQTT broker to receive or send edge-cloud messages. If the MQTT broker fails to be connected, check the causes based on the following principles:

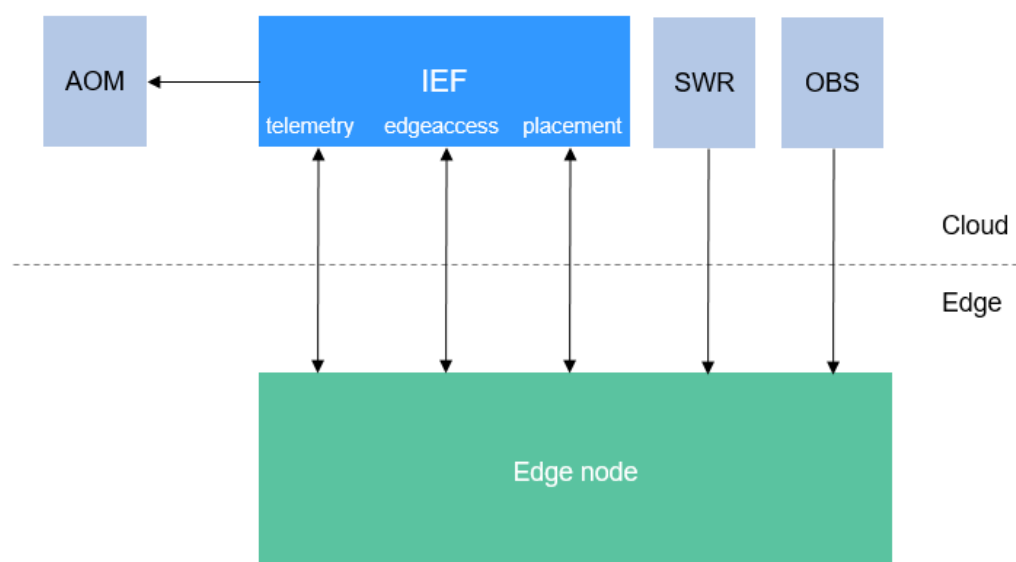
1. Do not use multiple processes with the same client ID to connect to the MQTT broker.
2. Use a correct certificate to set up the connection. For details, see [Performing Security Authentication Using Certificate](#).

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. For details about how to connect edge nodes to IEF through Direct Connect, see [Connecting Edge Nodes to IEF Through Direct Connect or VPN](#).

Figure 4-1 Connecting an edge node to IEF



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, Docker and containerized applications.

 NOTE

Currently, only HTTP proxy is supported.

Settings on Edge Nodes

- If an edge node is registered and managed using a certificate, and the edge node uses a network proxy, add the **HTTP_PROXY** and **HTTPS_PROXY** parameters to the environment variables and configure the **/opt/IEF/Cert/user_config** file.
 - a. Add the **HTTP_PROXY** and **HTTPS_PROXY** parameters to the environment variables. You can set the network proxy through temporary and permanent environment variables.
 - Method 1: Set the environment variables that take effect temporarily. The temporary environment variables take effect only in the current shell.
 - 1) Run the following commands to add the two parameters. Replace **http://192.168.0.70:8888** in the following example with the actual network proxy address.

```
export http_proxy="http://192.168.0.70:8888"
export https_proxy="http://192.168.0.70:8888"
```

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:

```
export http_proxy="http://username:paasword@192.168.0.70:8888"
export https_proxy="http://username:paasword@192.168.0.70:8888"
```
 - 2) After the configuration file is modified, run the installation commands on the edge node.
 - Method 2: Set environment variables that take effect permanently.
 - 1) Run the **vi /etc/profile** commands to add the two parameters. Replace **http://192.168.0.70:8888** in the following example with the actual network proxy address.

```
export http_proxy="http://192.168.0.70:8888"
export https_proxy="http://192.168.0.70:8888"
```

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:

```
export http_proxy="http://username:paasword@192.168.0.70:8888"
export https_proxy="http://username:paasword@192.168.0.70:8888"
```
 - 2) Run the **source /etc/profile** command to make the modified environment variables take effect.
 - 3) After the configuration file is modified, run the installation commands on the edge node.
 - b. 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.

NOTE

Before adding the parameters, upload the downloaded edge node installation tool and configuration file to the specified directory on the edge node and decompress the package. For details, see Node Management > Managing an Edge Node in the *User Guide*.

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",
```

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:password@192.168.0.70:8888
```

- c. After the configuration file is modified, run the installation commands on the edge node.

Settings on Docker Daemon

In certain lab environments, servers do not have permissions to directly connect to external networks. Therefore, network proxies are required. Generally, network proxies are configured in configuration files such as **/etc/environment** and **/etc/profile**, which is applicable to most operations. However, Docker commands cannot use these proxies. For example, if the docker pull operation needs to pull an image from the external network, the following error message is displayed:

```
$ docker pull hello-world  
Unable to find image 'hello-world:latest' locally  
Pulling repository docker.io/library/hello-world  
docker: Network timed out while trying to connect to https://index.docker.io/v1/repositories/library/hello-world/images. You may want to check your internet connection or if you are behind a proxy..
```

- **Solution 1:** Stop the Docker service, and manually start the Docker daemon by using port 2375 to listen to all network interfaces.

```
systemctl stop docker.service
```

```
nohup docker daemon -H tcp://0.0.0.0:2375 -H unix:///var/run/docker.sock  
&
```

- **Solution 2:** Edit the configuration file (**/etc/default/docker** in Ubuntu, or **/etc/sysconfig/docker** in CentOS). However, it is not recommended to configure the daemon process by modifying these configuration files.

```
HTTP_PROXY="http://[proxy-addr]:[proxy-port]/"  
HTTPS_PROXY="https://[proxy-addr]:[proxy-port]/"  
export HTTP_PROXY HTTPS_PROXY
```

- **Solution 3:** Modifications made with this solution are persistent and always take effect. This solution also modifies the default **docker.service** file.

- a. Create an embedded **systemd** directory for the Docker service.

```
mkdir -p /etc/systemd/system/docker.service.d
```

- b. Create the **/etc/systemd/system/docker.service.d/http-proxy.conf** file and add the HTTP_PROXY environment variable to the file. In the

following command, replace **[proxy-addr]** and **[proxy-port]** with the actual proxy address and port number, respectively.

```
[Service]
Environment="HTTP_PROXY=http://[proxy-addr]:[proxy-port]/" "HTTPS_PROXY=https://[proxy-addr]:[proxy-port]/"
```

If there are internal Docker registries that can be accessed without using a proxy, set the **NO_PROXY** environment variable as follows:

```
[Service]
Environment="HTTP_PROXY=http://[proxy-addr]:[proxy-port]/" "HTTPS_PROXY=https://[proxy-addr]:[proxy-port]/" "NO_PROXY=localhost,127.0.0.1,docker-registry.somecorporation.com"
```

- c. Run the following command to update the configurations:
systemctl daemon-reload
- d. Run the following command to restart the Docker service:
systemctl restart docker

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.

Type	Variable Name	Variable Value/Reference	Operation
Added manually	http_proxy	192.168.0.70:8888	Delete
Added manually	https_proxy	192.168.0.70:8888	Delete
Added manually	no_proxy	www.example.com	Delete

⊕ Add Environment Variable

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.

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 edge node/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 end 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 targets at latency-sensitive services, bandwidth-sensitive services, and services requiring high security and compliance, including but not limited to the following typical application scenarios:

- Visual product inspections
- Predictive maintenance

6 Others

6.1 Region and AZ

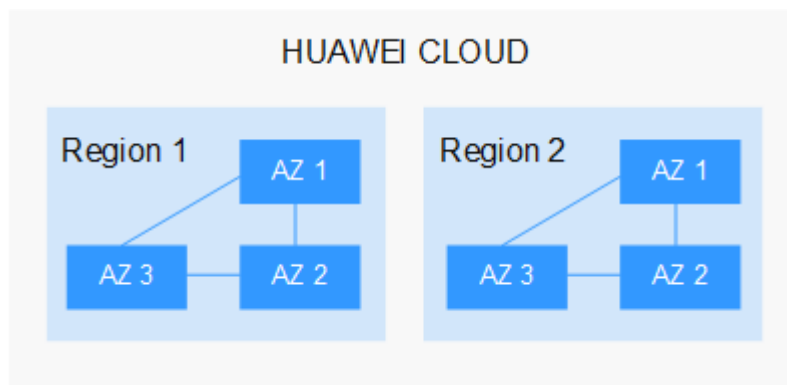
Concept

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



Huawei Cloud provides services in many regions around the world. You can select a region and an AZ based on requirements. For more information, see [Huawei Cloud Global Regions](#).

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.

- If your target users are in Asia Pacific (excluding the Chinese mainland), select the **CN-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 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 lower 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?

IEF supports the following edge node specifications:

Table 6-1 Edge node requirements

Item	Specifications
OS	<p>The language of the operating system must be English.</p> <ul style="list-style-type: none"> • x86_64 architecture Ubuntu LTS (Xenial Xerus), Ubuntu LTS (Bionic Beaver), CentOS, EulerOS, RHEL, Kylin, NewStart CGS Linux, NeoKylin, openEuler, Unity Operating System (UOS), Oracle Linux (OL), Huawei Cloud Euler (HCE), openEuler 23.09 Edge • Armv7i (Arm32) architecture Raspbian GNU/Linux (stretch) • AArch64 (Arm64) architecture Ubuntu LTS (Xenial Xerus), Ubuntu LTS (Bionic Beaver), CentOS, EulerOS, RHEL, Kylin, NewStart CGS Linux, NeoKylin, openEuler, Unity Operating System (UOS), Oracle Linux (OL), Huawei Cloud Euler (HCE), openEuler 23.09 Edge <p>NOTE The openEuler 23.09 Edge operating system is recommended for edge computing scenarios.</p>
Memory	<p>More than 256 MB of memory is recommended as 128 MB of memory is required to run the edge software.</p>
CPU	<p>≥ 1 core</p>
Hard disk	<p>≥ 1 GB</p>
GPU (optional)	<p>The GPU models on the same edge node must be the same.</p> <p>NOTE Currently, NVIDIA Tesla GPUs such as P4, P40, and T4 are supported.</p> <p>If an edge node is equipped with GPUs, you can choose not to enable its GPUs when registering it on IEF.</p> <p>If you choose to enable GPUs of an edge node, the GPU driver has to be installed on the edge node before you can manage it on IEF.</p> <p>Currently, only x86-based GPU nodes can be managed by IEF.</p>

Item	Specifications
NPU (optional)	<p>Ascend AI processors</p> <p>NOTE Currently, edge nodes integrated with Ascend Processors are supported, such as Atlas 300 inference cards, and Atlas 800 inference servers. Supported NPU specifications include Ascend 310P, 310B, Ascend 310P-share, and virtualization partition NPUs..</p> <p>If you choose to enable NPUs of an edge node, ensure that the NPU driver has been installed on it. Currently, Ascend 310 supports only firmware versions 1.3.x.x and 1.32.x.x, for example, 1.3.2.B893. You can run the npu-smi info command to view your firmware version.The NPU driver version must be 22.0.4 or later. You can go to the driver path, for example, /usr/local/Ascend/driver, and run the cat version.info command to view your driver version. If the driver is not installed, contact the device manufacturer for assistance.</p>
Container engine	<p>The Docker version must be later than 17.06. If Docker 1.23 or later is used, set the docker cgroupfs version to 1. Docker HTTP API v2 is not supported.</p> <p>(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.)</p> <p>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.</p> <p>Docker Cgroup Driver must be set to cgroupfs. For details, see How Do I Set Docker Cgroup Driver After Installing Docker on an Edge Node?.</p>
Glibc	The Glibc version must be later than 2.17.
Port	Edge nodes require port 8883, which is the listening port of the built-in MQTT broker on edge nodes. Ensure that this port works properly.
Time synchronization	The time on an edge node must be consistent with the UTC time. Otherwise, the monitoring data and logs of the edge node may be inaccurate. You can select an NTP server for time synchronization. For details, see How Do I Synchronize Time with the NTP Server?

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

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

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

6.4 What Programming Language Is Required for IEF Development?

IEF allows you to deploy and manage containerized applications developed in any programming language on edge nodes.

References:

- [Creating an Edge Application](#)
- [Building a Container Image](#)

6.5 Do I Need to Prepare Edge Nodes by Myself?

Yes. Edge nodes must meet requirements described in [Table 6-2](#).

Table 6-2 Edge node requirements

Item	Specifications
OS	<p>The language of the operating system must be English.</p> <ul style="list-style-type: none">• x86_64 architecture Ubuntu LTS (Xenial Xerus), Ubuntu LTS (Bionic Beaver), CentOS, EulerOS, RHEL, Kylin, NewStart CGS Linux, NeoKylin, openEuler, Unity Operating System (UOS), Oracle Linux (OL), Huawei Cloud Euler (HCE), openEuler 23.09 Edge• Armv7i (Arm32) architecture Raspbian GNU/Linux (stretch)• AArch64 (Arm64) architecture Ubuntu LTS (Xenial Xerus), Ubuntu LTS (Bionic Beaver), CentOS, EulerOS, RHEL, Kylin, NewStart CGS Linux, NeoKylin, openEuler, Unity Operating System (UOS), Oracle Linux (OL), Huawei Cloud Euler (HCE), openEuler 23.09 Edge <p>NOTE The openEuler 23.09 Edge operating system is recommended for edge computing scenarios.</p>
Memory	More than 256 MB of memory is recommended as 128 MB of memory is required to run the edge software.
CPU	≥ 1 core
Hard disk	≥ 1 GB

Item	Specifications
GPU (optional)	<p>The GPU models on the same edge node must be the same.</p> <p>NOTE Currently, NVIDIA Tesla GPUs such as P4, P40, and T4 are supported.</p> <p>If an edge node is equipped with GPUs, you can choose not to enable its GPUs when registering it on IEF.</p> <p>If you choose to enable GPUs of an edge node, the GPU driver has to be installed on the edge node before you can manage it on IEF.</p> <p>Currently, only x86-based GPU nodes can be managed by IEF.</p>
NPU (optional)	<p>Ascend AI processors</p> <p>NOTE Currently, edge nodes integrated with Ascend Processors are supported, such as Atlas 300 inference cards, and Atlas 800 inference servers. Supported NPU specifications include Ascend 310P, 310B, Ascend 310P-share, and virtualization partition NPUs..</p> <p>If you choose to enable NPUs of an edge node, ensure that the NPU driver has been installed on it. Currently, Ascend 310 supports only firmware versions 1.3.x.x and 1.32.x.x, for example, 1.3.2.B893. You can run the npu-smi info command to view your firmware version.The NPU driver version must be 22.0.4 or later. You can go to the driver path, for example, /usr/local/Ascend/driver, and run the cat version.info command to view your driver version. If the driver is not installed, contact the device manufacturer for assistance.</p>
Container engine	<p>The Docker version must be later than 17.06. If Docker 1.23 or later is used, set the docker cgroupfs version to 1. Docker HTTP API v2 is not supported.</p> <p>(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.)</p> <p>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.</p> <p>Docker Cgroup Driver must be set to cgroupfs. For details, see How Do I Set Docker Cgroup Driver After Installing Docker on an Edge Node?.</p>
Glibc	<p>The Glibc version must be later than 2.17.</p>
Port	<p>Edge nodes require port 8883, which is the listening port of the built-in MQTT broker on edge nodes. Ensure that this port works properly.</p>

Item	Specifications
Time synchronization	The time on an edge node must be consistent with the UTC time. Otherwise, the monitoring data and logs of the edge node may be inaccurate. You can select an NTP server for time synchronization. For details, see How Do I Synchronize Time with the NTP Server?

6.6 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 application details on the IEF console but cannot perform any other operation. If your account is still in arrears when the retention period ends, your 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.

6.7 What Are the Differences Between IEF and IoT Edge?

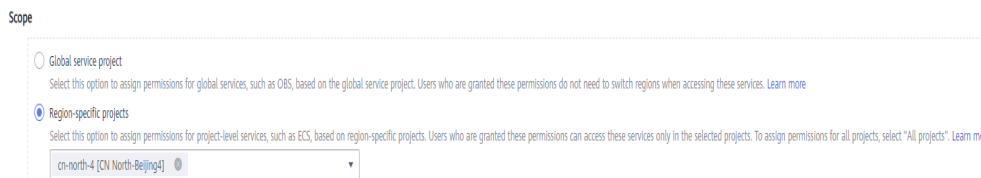
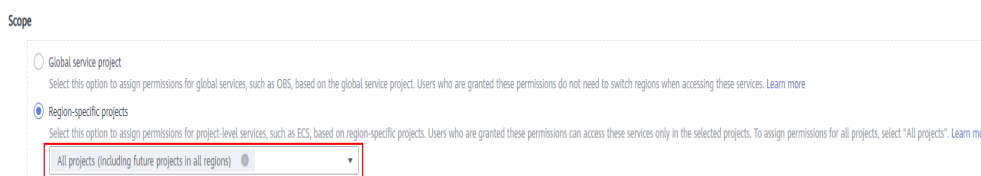
- IEF provides users with integrated services under edge-cloud synergy. With powerful application management and edge-cloud synergy, IEF can deliver applications from the cloud to the edge in a unified manner, and manage, monitor, and maintain applications in the cloud.
- IoT Edge is mainly used for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

6.8 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.

When assigning permissions to a user group, set **Scope** to **Region-specific projects**, and set parameters according to the following rules:

- To assign permissions in certain regions, select one or more specified projects, for example, **cn-north-4 [CN North-Beijing4]**. Note: If you select **All Projects** in this scenario, the authorization will not take effect.
- To assign permissions in all regions, select **All projects**.

Figure 6-2 Assigning permissions in certain regions**Figure 6-3** Assigning permissions in all regions

6.9 How Can I Deal With Insufficient Permissions?

Symptom

IEF resources fail to be created, viewed, updated, or deleted, and a message indicating insufficient permission is displayed.

Possible Causes

- IEF fails to create or update resources:
 - a. The account is in arrears.
 - b. The account is frozen.
 - c. The account does not have the IEF permissions.
- IEF fails to delete resources:
 - a. The account is frozen.
 - b. The account does not have the IEF permissions.
- IEF fails to view resources:
 - a. The account does not have the IEF permissions.

Solution

- Topping up your account
Click **Billing Center** in the upper part of the console to check whether the account balance is less than 0. If it is, click **Top Up** to top up your account.
- Unfreezing your account
Point to the account name on the upper right corner and click **Basic Information**. On the displayed **My Account** page, check whether a message

indicating that the account is frozen is displayed on the **Basic Information** page or the top of the console. If the account is frozen, contact the customer service to unfreeze the account.

- Granting IEF Permissions

Create a user group and users. Grant IEF permissions to them. For details, see [Creating a User and Granting Permissions](#).

6.10 How Will the Multi-AZ Reconstruction of SWR Application Container Image Data Affect IEF?

After the multi-AZ reconstruction of SWR application container image data, check whether IEF is affected by referring to this section.

Application Scope

CN South-Guangzhou, CN East-Shanghai1, and CN North-Beijing4

Application Scenario

When edge nodes access IEF through the air wall, proxy, gateway, or NAT, check whether IEF is affected by the multi-AZ reconstruction of SWR application container image data.

The following table lists the domain names for accessing application container image data in different regions. The checking procedure uses CN North-Beijing4 region as an example.

Region Name	Domain Name for Accessing Application Container Image Data
CN South-Guangzhou	op-svc-swr-b051-10-230-33-197-3az.obs.cn-south-1.myhuaweicloud.com
CN East-Shanghai1	op-svc-swr-b051-10-147-7-14-3az.obs.cn-east-3.myhuaweicloud.com
CN North-Beijing4	op-svc-swr-b051-10-38-19-62-3az.obs.cn-north-4.myhuaweicloud.com

Checking Procedure

- Step 1** Run the following command to check the connection between the edge device and the domain name for accessing the application container image data. If the connection is normal, IEF is not affected by the multi-AZ reconstruction. Skip the subsequent steps.

```
curl -i -k -v op-svc-swr-b051-10-38-19-62-3az.obs.cn-north-4.myhuaweicloud.com
```

Connection output example:

```
* Rebuilt URL to: op-svc-swr-b051-10-38-19-62-3az.obs.cn-north-4.myhuaweicloud.com/  
* Trying 49.4.112.91...  
* Connected to op-svc-swr-b051-10-38-19-62-3az.obs.cn-north-4.myhuaweicloud.com (49.4.112.91) port 80  
(#0)  
> GET / HTTP/1.1  
> Host: op-svc-swr-b051-10-38-19-62-3az.obs.cn-north-4.myhuaweicloud.com  
> User-Agent: curl/7.47.0  
> Accept: */*  
>  
< HTTP/1.1 403 Forbidden  
HTTP/1.1 403 Forbidden  
< Server: OBS  
Server: OBS
```

Step 2 Run the following command on a device that can access the Internet to obtain the IP address for accessing the application container image data:

ping op-svc-swr-b051-10-38-19-62-3az.obs.cn-north-4.myhuaweicloud.com

Output example:

```
ping op-svc-swr-b051-10-38-19-62-3az.obs.cn-north-4.myhuaweicloud.com  
Pinging obs.lz02.cn-north-4.myhuaweicloud.com [49.4.112.91] with 32 bytes of data:  
...
```

Step 3 Modify the forwarding or mapping configuration of the domain name or IP address, including but not limited to the following scenarios:

- For an air wall, add the mapping between IP:Port on the Internet and IP:Port on the intranet. If the **/etc/hosts** mode is previously used, add the mapping between the domain name for accessing the application container image data and the intranet mapping IP address to the **/etc/hosts** file.
- For a proxy, add forwarding rules related to the domain name or IP address for accessing application container image data.
- For a firewall, enable the restriction on the domain name or IP address for accessing the application container image data.

Change the value based on your service environment.

Step 4 Perform step [Step 1](#) again to check whether the domain name for accessing the application container image data can be connected.

----End