Migration Center

Tools Guide

Issue	06
Date	2024-07-11

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

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 About Edge

Edge is a tool that collects information about your environment and executes migration commands from MgC.

Feature Switch

The following table lists the Edge feature switches.

Parameter	Description	Value	Location
config.httpclient.verifier	Indicates whether to enable hostname verification, which is used to verify the certificates and domain names used in connections to Edge.	• **NoopHostnameVerifier**: The verification is disabled. • **MustHostnameVerifier**: The verification is enabled.	<*Installation path*>**\Edge\tools\SecAs-1.2.29\webmanagementapps\edge-server-0.0.1\WEB-INF\classes\application.yml**
edge.plugin-ssl-mode	Indicates whether to use the SSL channel to receive Remote Procedure Call (RPC) connections.	• **true**: The SSL channel is used to receive RPC connections. • **false**: The SSL channel is not used to receive RPC connections.	<*Installation path*>**\Edge\tools\SecAs-1.2.29\webmanagementapps\edge-server-0.0.1\WEB-INF\classes\application.yml**

Public Domain Names

The following table lists the public domain names that Edge must be able to access in the AP-Singapore region.

Parameter	Description	Value	Location
edge.iot-host	The IoTDA service address	AP-Singapore: ssl://31f50f5a99.st1.iotda-device.ap-southeast-3.myhuaweicloud.com:8883	<*Installation path*>**\Edge\tools\SecAs-1.2.29\webmanagementapps\edge-server-0.0.1\WEB-INF\classes\application.yml**
edge.mgc-host	The MgC service address	AP-Singapore: https://mgc.ap-southeast-3.myhuaweicloud.com	
edge.vars.sms-agent-url	The SMS bucket address	https://sms-agent-2-0.obs.ap-southeast-1.myhuaweicloud.com	
edge.vars.sms-domain	The SMS public domain name	sms.ap-southeast-3.myhuaweicloud.com	

The following table list the public domain names that Edge must be able to access in the LA-Santiago region.

Parameter	Description	Value	Location
edge.iot-host	The IoTDA service address	LA-Santiago: ssl://eee2b036e2.st1.iotda-device.la-south-2.myhuaweicloud.com:8883	<*Installation path*>**\Edge\tools\SecAs-1.2.29\webmanagementapps\edge-server-0.0.1\WEB-INF\classes\application.yml**
edge.mgc-host	The MgC service address	LA-Santiago: https://mgc.la-south-2.myhuaweicloud.com	
edge.vars.sms-agent-url	The SMS bucket address	https://sms-agent-2-0.obs.ap-southeast-1.myhuaweicloud.com	
edge.vars.sms-domain	The SMS public domain name	sms.ap-southeast-3.myhuaweicloud.com	

2 Installing Edge

2.1 Installing Edge for Windows

Preparations

- Prepare a Windows server for installing Edge in the source intranet environment. The Windows server must:
  - Be able to access the Internet and the domain names of MgC and IoTDA. For details about the domain names to be accessed, see **How Do I Configure WinRM on a Windows Source Server and Troubleshoot WinRM Connection Problems?**
  - Use PowerShell **4.0** or later.
  - Have at least 4 CPUs and 8 GB of memory.
  - Allow outbound traffic on 8883 if the server is in a security group.
  - Disable any antivirus and protection software on the server. This type of software may stop Edge from executing migration commands, resulting in migration failures.

  CAUTION

  Do not install Edge on a source server to be migrated.

  - **High resource consumption**: Edge consumes CPU and memory resources during collection and migration. If a large number of migration tasks are performed by Edge, services on the source server may be affected.
  - **Port occupation**: Edge occupies some ports on the source server, which may affect services on the server.
- **Sign up for a HUAWEI ID and enable Huawei Cloud services**, and obtain an AK/SK pair for the account.
- **Create a migration project** on the MgC console.

Precautions

- The Windows server where Edge is installed must be able to access source servers you want to migrate over the following ports:
  - Windows: port 5985
  - Linux: port 22
- WinRM must be enabled on Windows source servers, and these source servers must be able to access the server where Edge is installed. For more information, see **How Do I Configure WinRM on a Windows Source Server and Troubleshoot WinRM Connection Problems?**

Procedure

Step 1 Log in to the **MgC console** from the Windows server you prepared.

Step 2 In the navigation pane on the left, choose **Tools**.

Step 3 In the **Windows** area, click **Download Installation Package** to download the Edge installation package to the Windows server you prepared.

Step 4 Decompress the downloaded Edge installation package, double-click the Edge installation program, and click **Next**. If the installation program cannot be launched, try to run it in compatibility mode. For details, see **How Do I Run Edge in Compatibility Mode?**.

Step 5 On the **License Agreement** page, read the agreement carefully, select **I accept the terms of the License Agreement**, and click **Next**.

Step 6 Select drive C as the installation directory and click **Install**.

> ⚠ CAUTION
>
> Edge can be installed only in drive C. If you select another disk for installation, Edge may fail to be started.

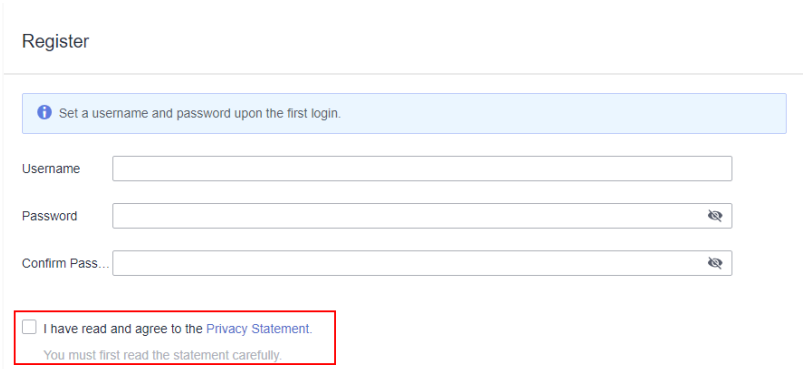
Step 7 After the installation is complete, click **Finish** to open the Edge console and go to the **User Registration** page.

----End

Registering an Account

When you log in to the Edge console for the first time, you must set a username and password. Keep the username and password secure.

Step 1 On the **Register** page, specify a username and password, confirm the password, and click **Privacy Statement**.



Step 2 Read the privacy statement carefully before selecting **I have read and agree to the Privacy Statement**, and click **Register**. Then you need to connect the Edge device to MgC. For details, see **Connecting the Edge Device to MgC**.

----End

3 Edge Discovery

3.1 Connecting the Edge Device to MgC

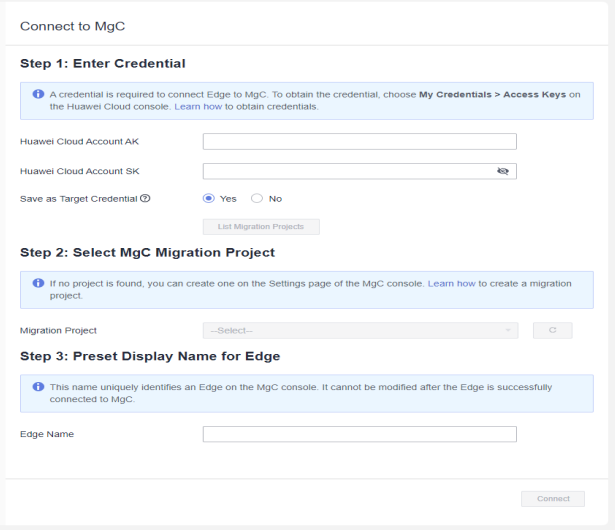
You need to connect the Edge device to MgC, so that Edge can receive commands from MgC for discovering resources and executing migration tasks.

Prerequisites

You have **installed Edge** and registered an account.

Procedure

Step 1 Use the registered username and password to log in to the Edge console. In the navigation pane on the left, choose **Connections to MgC**.



Step 2 In **Step 1: Enter Credential**, enter the AK/SK pair of the Huawei Cloud account used to access MgC, and click **List Migration Projects**. Edge authenticates your identity using the entered AK/SK pair. After the verification is successful, you can go to the next step. If the AK/SK authentication fails, rectify the fault by referring to **What Can I Do If AK/SK Verification Fails?**.

Determine whether to save the entered AK/SK pair as the target credential which will be used for migrating your workloads to Huawei Cloud.

- If you select **No**, the entered AK/SK pair will be deleted after the Edge device is connected to MgC.
- If you select **Yes**, the entered AK/SK pair will be encrypted and saved locally after the connection to MgC is successfully. The AK/SK pair will be delivered to the migration Agent for migrating your workloads to Huawei Cloud.

Step 3 In **Step 2: Select MgC Migration Project**, select a **migration project** from the project drop-down list. Edge will report the collected information about your source resources to this project.

Step 4 In **Step 3: Preset Display Name for Edge**, specify a name for the Edge device, which will be displayed on the MgC console, and click **Next**. Confirm the connection to MgC, and click **OK**.

CAUTION

After the Edge device is connected to MgC, the name you specified here cannot be modified.

Step 5 After the connection is successful, perform the following operations:

- Go to the MgC console and check the connection status of the Edge device and **manage the Edge device**.
- **Add or modify the target credential**.
- **Add the credentials of the source cloud or source servers** for discovery and migration.

----End

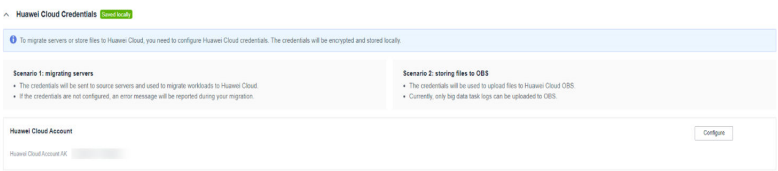
3.2 Managing Huawei Cloud Credentials

The Huawei Cloud credentials are delivered to the migration Agent on source servers for executing migration. If they are missing, your migration workflows cannot run properly.

Adding Huawei Cloud Credentials

If you have chosen not to locally save the Huawei Cloud credentials used for **connecting the Edge device to MgC**, you can add those or other credentials after the connection was complete.

Step 1 Log in to the Edge console, click ⌄ on the left of **Huawei Cloud Credentials**. In the **Huawei Cloud Account** area, click **Configure**.



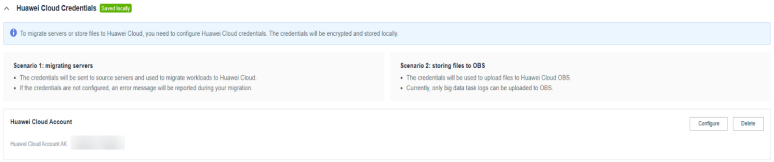
Step 2 In the displayed **Configure Huawei Cloud Credentials** dialog box, enter the AK/SK pair of the Huawei Cloud account you are migrating to and click **Confirm**.

----End

Modifying Huawei Cloud Credentials

If you need to replace the saved Huawei Cloud credentials, you can delete them and add others.

Step 1 Click **Delete** next to the saved credentials. In the displayed dialog box, click **Confirm**.



Step 2 Add other Huawei Cloud credentials by referring to **Adding Huawei Cloud Credentials**.

----End

3.3 Adding Resource Credentials

You need to add credentials for accessing your source resources to Edge, so that Edge can collect information about them and migrate them to Huawei Cloud. Credentials added to Edge are encrypted and stored locally, and will not be synced to MgC.

CAUTION

Credentials you add to Edge are valid for three days. After the validity period expires, you need to add the credentials to Edge again if you still want to discover or migrate the resources.

Prerequisites

Edge has been installed on a device in your source environment, and the Edge device has been connected to MgC.

Authentication Methods

You can add credentials of the following types of resources to Edge: private clouds, servers, and containers. For details about the authentication methods supported for each resource type, see **Table 3-1**.

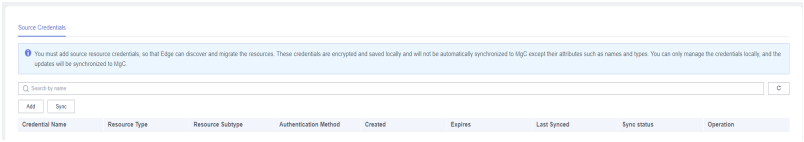
Table 3-1 Authentication methods

Resource Type	Authentication Method	Description
Public cloud	• AK/SK • Configuration file • Username/ Password	• Enter the AK/SK pair used for accessing the cloud platform, such as Huawei Cloud, Alibaba Cloud, AWS, Tencent Cloud, or Azure • Upload the configuration file used to access Google Cloud. The configuration file contains credentials for Google Cloud service accounts, and the file must be in .json format and cannot exceed 4 KB.
Private cloud	Username/ Password	Enter the username and password for logging in to the source private cloud.
Databases	Username/ Password	Enter the username and password of the database.
Windows server	Username/ Password	Enter the username and password for logging in to the server. Then specify **Network Range**, which can be a single IP address or an IP address range. The value can be: • A single IP address, for example, 192.168.10.10/32 • An IP address range, for example, 192.168.52.0/24 • All IP addresses. You need to enter **0.0.0.0/0**.

Resource Type	Authentication Method	Description
Linux server	• Username/Password • Username/Key	• If you select **Username/Password**, enter the username and password for logging in to the server. • If you select **Username/Key**, enter the username and the password of the key file for logging in to the server, and upload the key file in .pem format. **NOTICE** If the key file is not encrypted, you do not need to enter the password. Then specify **Network Range**, which can be a single IP address or an IP address range. The value can be: • A single IP address, for example, 192.168.10.10/32 • An IP address range, for example, 192.168.52.0/24 • All IP addresses. You need to enter **0.0.0.0/0**.
Container	Configuration file	The configuration file must be a .json or .yml file.

Procedure

Step 1 On the Edge console, in the **Source Credentials** area, click **Add**.



Step 2 Select a resource type and authentication method as prompted. Specify a credential name, enter your credentials, and click **Confirm**. After the credential is added, Edge automatically synchronizes the added credential to MgC. You can view the credential details in the credential list.

----End

Synchronizing Credentials

If Edge is disconnected from MgC, you need to manually synchronize added credentials to MgC after the connection is restored. In the **Source Credentials** area, click **Sync**.

3.4 Managing Edge Devices

You can monitor and manage Edge devices connected to MgC on the MgC console.

Prerequisites

Edge has been installed on a device, and the Edge device has been connected to MgC.

Viewing Edge Devices

Step 1 Log in to the **MgC** console.

Step 2 In the navigation pane on the left, choose **Tools**. In the upper left corner of the page, select a **migration project** from the drop-down list to view all Edge devices and their statuses in this project.

The following table describes the device statuses.

Table 3-2 Device status description

Status	Description
Online	The Edge device stays connected with the MgC console.
Offline	The Edge device is disconnected from the MgC console for at least one minute.
Error	The Edge device has been registered with but has not been connected to MgC.
Abnormal	A backend error occurred. Contact Huawei Cloud technical support for help.
Blocked	A backend error occurred. Contact Huawei Cloud technical support for help.

----End

Deleting an Edge Device

Locate the device and click **Delete** in the **Operation** column. In the displayed dialog box, click **OK**.

CAUTION

If Edge is collecting resource information, the device cannot be deleted.

4 Tool Discovery

4.1 Creating a Collection Task

Edge provides multiple types of collectors with you to collect resource specifications and configuration information. This section describes how to use a collector to create a collection task.

Prerequisites

- You have **installed Edge** and registered an account.
- The required **collectors** have been installed.

Procedure

Step 1 Use the registered username and password to log in to the Edge console. In the navigation pane on the left, choose **Tasks**.

Step 2 Click **Create**. On the displayed **Create Task** page, select the collector based on the resources to be collected and click **Next**.

Step 3 In the **Task Info** area, customize the task name. In the **Collector Settings** area, set collector parameters based on **Configuring Collector Parameters**. Parameters with * are mandatory.

Step 4 After the configuration is complete, click **OK**. You can view the data source collection statuses in the task list.

After the data source is successfully collected, obtain the collection results in any of the following ways:

- Click **Download JSON** in the **Operation** column of the task to save the collection result as a JSON file. The file is used to import the collection result to the MgC for application association analysis. For details, see **Importing Tool Discovery Results**.
- Click **Download CSV** in the **Operation** column of the task to locally save the collection result as a CSV file.

- Click **View Storage Path** in the **Operation** column of a task to view the path for saving the discovery results.

----End

4.2 Managing Collectors

The Edge installation package contains some collector installation packages. When the Edge is installed, these collectors are also installed. This section describes how to upgrade a collector and add a collector.

Scenarios

- Offline upgrade: used for updating installed collectors
- Manual upgrade: used for installing or modifying collectors

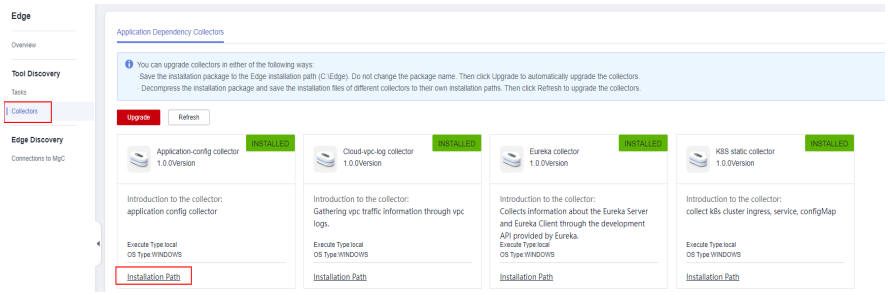
Prerequisites

You have **installed Edge** and registered an account.

Offline Upgrade

Step 1 Use the registered username and password to log in to the Edge console. In the navigation pane, choose **Collectors**.

You can view the types, versions, and installation paths of installed collectors.



Step 2 Log in to the **MgC** console, download the latest Edge installation package and save it to the root directory of the Edge installation directory (for example, C:\Edge). Do not change the name of the installation package. Click **Upgrade**. The system automatically installs and upgrades the collector.

On the **Application Dependency Collectors** tab page, if the version of the installed collector is the latest, the collector has been upgraded.

NOTICE

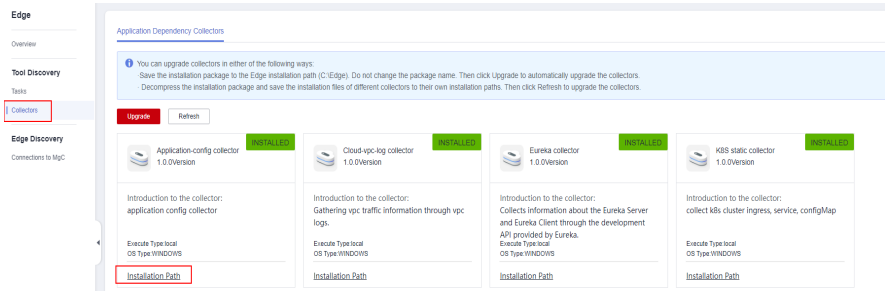
If the installation package contains multiple collectors, all collectors will be upgraded at a time.

----End

Manual Upgrade

Step 1 Use the registered username and password to log in to the Edge console. In the navigation pane, choose **Collectors**.

You can view the types, versions, and installation paths of installed collectors.



Step 2 To add a collector, download the Edge installation package on the **Tools** page of the **MgC** console, manually decompress the package and save the installation file to the collector installation path (for example, C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors), and click **Refresh**. The system automatically installs the collector. On the **Application Dependency Collectors** tab page, if the new collector is displayed, the collector is successfully added.

To modify the collector configuration file, copy and open the collector installation path, find the configuration file, and modify and save it. Then click **Refresh**. The system automatically updates the collector configuration information.

----End

4.3 Configuring Collector Parameters

4.3.1 Kubernetes Static Collector (app-discovery-k8s)

It collects Ingress, service, and ConfigMap information of a Kubernetes cluster. For details about the configuration parameters, see **Table 4-1**.

Table 4-1 Parameters for configuring the Kubernetes static collector

Parameter	Mandatory	Configuration
output_path	No	Enter the storage path of the collection result file (app-discovery-k8s-xxx.csv). If this parameter is left blank, the storage path defaults to <*Collector installation path*>**\output\file**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-k8s\output\file\app-discovery-k8s-xxx.csv

Parameter	Mandatory	Configuration
rules_path	No	Enter the storage path of the collection rule file (a .properties file). If this parameter is left blank, the path defaults to <*Collector installation path*>**\config\rules.properties**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-k8s\config\rules.properties **NOTICE** You are advised to use the default rule file. If you need to customize collection rules, modify the default rule file.
config_path	Yes	Enter the absolute path of the folder that stores the configuration files (in YAML format) of clusters to be collected. **CAUTION** This storage path stores only YAML configuration files of clusters to be collected. Irrelevant YAML files should not be stored here. To obtain the content of a cluster's configuration file, perform the following steps: On a cluster node, run the following command, and copy the returned information to a YAML file. `cat ~/.kube/config` **NOTICE** Only one configuration file can be stored for a Kubernetes cluster.

4.3.2 Kubernetes Conntrack Collector (app-discovery-k8s-conntrack)

The conntrack utility is used to collect the application association topology of a Kubernetes cluster. For details about the configuration parameters, see **Table 4-2**.

Table 4-2 Parameters for configuring the Kubernetes conntrack collector

Parameter	Mandatory	Configuration
output_path	No	Enter the storage path of the collection result file (app-discovery-k8s-conntrack-xxx.csv). If this parameter is left blank, the storage path defaults to <*Collector installation path*>**\output\file**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-k8s-conntrack\output\file\app-discovery-k8s-conntrack-xxx.csv

Parameter	Mandatory	Configuration
rules_path	No	Enter the storage path of the collection rule file (a .properties file). If this parameter is left blank, the path defaults to <*Collector installation path*>**\config\rules.properties**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-k8s-conntrack\config\rules.properties **NOTICE** You are advised to use the default rule file. If you need to customize collection rules, modify the default rule file.
timeout	No	Specify the duration of a single collection, in seconds. The value is an integer ranging from 1 to the value of **period**. If this parameter is not set, half of the value of **period** is used by default.
max_count	No	Specify the maximum number of traffic records that can be collected for a node each time. The value must be an integer greater than or equal to 1. If this parameter is not set, the default value **1,000** is used.
period	No	Specify the collection interval, in minutes. The value is an integer ranging from 1 to 30. If this parameter is not set, the default value **1 m** is used.
time	Yes	Specify the collection duration. If the collection duration exceeds the specified value, the collection stops. The unit can be **m** (minute), **h** (hour), or **d** (day). The value is an integer greater than or equal to 1.
nodes_path	No	Enter the storage path of the access configuration file of the nodes to be collected. If this parameter is left blank, the path defaults to <*Collector installation path*>**\config\nodes.csv**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-k8s-conntrack\config\nodes.csv **NOTICE** You are advised to use the default access configuration file. If you need to customize access information, modify the default file.

Parameter	Mandatory	Configuration
config_path	No	Enter the storage path of the cluster configuration file (.yaml). Alternatively, create a folder called **kube-config** in the **config** directory in the collector installation path and place the cluster configuration file in the folder. In this case, you do not need to set **config_path**, and the storage path defaults to <*Collector installation path*>**\config\kube-config***xxx***.yaml**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-k8s-conntrack\config\kube-config\xxx.yaml To obtain the content of a cluster's configuration file, perform the following steps: On a cluster node, run the following command, and copy the returned information to a YAML file. `cat ~/.kube/config` **NOTICE** Only one configuration file can be stored for a Kubernetes cluster.

4.3.3 Kubernetes Pod Network Collector (app-discovery-k8s-pod-net)

This collector collects the network information of Kubernetes cluster pods to analyze associations between applications. For details about the configuration parameters, see **Table 4-3**.

Table 4-3 Parameters for configuring the Kubernetes pod network collector

Parameter	Mandatory	Configuration
output_path	No	Enter the storage path of the collection result file (app-discovery-k8s-pod-net-xxx.csv). If this parameter is left blank, the storage path defaults to <*Collector installation path*>**\output\file**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-k8s-pod-net\output\file\app-discovery-k8s-pod-net-xxx.csv

Parameter	Mandatory	Configuration
rules_path	Yes	Enter the storage path of the collection rule file (a .properties file). If this parameter is left blank, the path defaults to <*Collector installation path*>**\config\rules.properties**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-k8s-pod-net\config\rules.properties **NOTICE** You are advised to use the default rule file. If you need to customize collection rules, modify the default rule file.
period	Yes	Specify the collection interval. The unit can be **s** (second) or **m** (minute). The value is an integer ranging from 1 to 30.
time	Yes	Specify the collection duration. If the collection duration exceeds the specified value, the collection stops. The unit can be **m** (minute), **h** (hour), or **d** (day). The value is an integer greater than or equal to 1.
config_path	Yes	Enter the storage path of the cluster configuration file (.yaml). **CAUTION** This storage path stores only YAML configuration files of clusters to be collected. Irrelevant YAML files should not be stored here. To obtain the content of a cluster's configuration file, perform the following steps: On a cluster node, run the following command, and copy the returned information to a YAML file. `cat ~/.kube/config` **NOTICE** Only one configuration file can be stored for a Kubernetes cluster.

4.3.4 Process and Network Collector (app-discovery-process-netstat)

This collector collects process and network associations on a node. For details about the configuration parameters, see **Table 4-4**.

Table 4-4 Parameters for configuring the process and network collector

Parameter	Mandatory	Configuration
output_path	No	Enter the storage path of the collection result file (app-discovery-process-netstat-xxx.csv). If this parameter is left blank, the storage path defaults to <*Collector installation path*>**\output\file**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-process-netstat\output\file\app-discovery-process-netstat-xxx.csv
rules_path	No	Enter the storage path of the collection rule file (a .properties file). If this parameter is left blank, the path defaults to <*Collector installation path*>**\config\rules.properties**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-process-netstat\config\rules.properties **NOTICE** You are advised to use the default rule file. If you need to customize collection rules, modify the default rule file.
interval	No	Specify the collection interval, in minutes. The value is an integer ranging from 1 to 30. If this parameter is not set, the default value **1 m** is used.
time	No This parameter is mandatory when **app_only** is set to **false**.	Specify the collection duration. If the collection duration exceeds the specified value, the collection stops. The unit can be **m** (minute), **h** (hour), or **d** (day). The value is an integer greater than or equal to 1.
app_only	No	Specify whether to collect only process information. The options are **true** and **false**. **true** indicates only process information is collected. **false** indicates only network information is collected. The default value is **false**. **CAUTION** If this parameter is set to **false**, the **time** parameter is mandatory.

Parameter	Mandatory	Configuration
nodes_path	No	• If you want to use the default configuration file provided by the collector, leave this parameter empty. Before data collection, you need to fill out the node information to be collected in the default configuration file **nodes.csv**. The path of file is <*Collector installation directory*>**\config\nodes.csv**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-process-netstat\config\nodes.csv • If you want to customize a configuration file, create a CSV file by referring to the default configuration file **nodes.csv**. Set this parameter to the path of the created CSV file. **NOTICE** You are advised to fill out your node information in the default configuration file **nodes.csv**. If you need to customize a configuration file, use the default file as a reference.

4.3.5 Windows Process and Network Collector (app-discovery-process-netstat-win)

This collector collects process and network associations on Windows servers. This collector can run only on Windows. The collector uses the Windows Management Instrumentation (WMI) and SMB protocols to communicate with the Windows servers to be collected. The following required ports must be enabled on the firewall of these Windows servers:

- WMI: TCP port 135 and a larger random port (default: 13475; recommended: 1024-65535)
- SMB: TCP port 445

NOTICE

The collector can collect only the associations between the processes that are identified by running the **netstat** command and have long-term network connections.

Table 4-5 Parameters for configuring the Windows process and network collector

Parameter	Mandatory	Configuration
host_path	Yes	Enter the path to the CSV file that contains Windows server authorization information, for example, **D:\nodes.csv**. You need to prepare the CSV file in advance. In the first row (table header) of the CSV file, enter the parameter names in the following sequence, and enter the parameter values of each Windows server to be collected in the rows below the table header. The **IP**, **USER**, and **PASSWORD** parameters are mandatory. • IP(REQUIRED) • PORT(REQUIRED) • USER(REQUIRED) • PASSWORD(SENSITIVE) • PRI_KEY_PATH(SENS_PATH) • CLUSTER • APPLICATION • BUSINESS_DOMAIN • PASSWORD(ENCRYPTED) • PRI_KEY_PATH(ENCRYPTED) **CAUTION** The provided accounts (username and password) must have the permission to run the **netstat** command on the server.
app_only	No	Specify whether to collect only process information. The options are **true** and **false**. **true** indicates only process information is collected. **false** indicates only network information is collected. The default value is **false**. **CAUTION** If this parameter is set to **false**, the **time** parameter is mandatory.
time	No This parameter is mandatory when **app_only** is set to **false**.	Specify the collection duration. If the collection duration exceeds the specified value, the collection stops. The unit can be **m** (minute), **h** (hour), or **d** (day). The value is an integer greater than or equal to 1.

Parameter	Mandatory	Configuration
interval	No	Specify the collection interval, in minutes. The value is an integer ranging from 1 to 30. If this parameter is not set, the default value **1 m** is used.
output_path	No	Enter the storage path of the collection result file (app-discovery-process-netstat-win-xxx.csv). If this parameter is left blank, the storage path defaults to <*Collector installation path*>**\output\file**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-process-netstat-win\output\file\app-discovery-process-netstat-win-xxx.csv

4.3.6 RabbitMQ Collector (app-discovery-rabbitmq)

This collector connects to the RabbitMQ management plug-in to obtain the information about the RabbitMQ node list, version, queues, and consumer endpoints in queues. For details about the configuration parameters, see **Table 4-6**.

Table 4-6 Parameters for configuring the RabbitMQ collector

Parameter	Mandatory	Configuration
output_path	No	Enter the storage path of the collection result file (app-discovery-rabbitmq-xxx.csv). If this parameter is left blank, the storage path defaults to <*Collector installation path*>**\output\file**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-rabbitmq\output\file\app-discovery-rabbitmq-xxx.csv
password	Yes	Enter the login password.
username	Yes	Enter the username for logging in to the RabbitMQ management plug-in.
server_port	Yes	Enter the RabbitMQ service port, for example, 5672.
plugin_port	Yes	Enter the port of the RabbitMQ management plug-in, for example, 15672.
host	Yes	Enter the IP address for connecting to RabbitMQ, for example, **127.0.0.1**.

4.3.7 Kafka Collector (app-discovery-kafka)

This collector connects to a Kafka node to obtain the IP address, version, and consumer information of the Kafka node. For details about the configuration parameters, see **Table 4-7**.

Table 4-7 Parameters for configuring the Kafka collector

Parameter	Mandatory	Configuration
output_path	No	Enter the storage path of the collection result file (app-discovery-kafka-xxx.csv). If this parameter is left blank, the storage path defaults to <*Collector installation path*>**\output\file**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-kafka\output\file\app-discovery-kafka-xxx.csv
cert_file	No	If **auth** is set to **3**, set this parameter to the absolute path of the **SSL cert_file** file.
ca_file	No	If **auth** is set to **3**, set this parameter to the absolute path of the **SSL ca_file** file.
password	No	Enter the login password.
username	No	If **auth** is set to **2** or **3**, set this parameter to the username for logging in to Kafka.
auth	Yes	Specify the Kafka authentication method. • **0**: indicates no authentication is required. • **1**: indicates the PLAINTEXT authentication. • **2**: indicates the SASL_PLAINTEXT authentication. • **3**: indicates SASL_SSL authentication.
endpoint	Yes	Enter the Kafka connection address, for example, 127.0.0.1:9092.

4.3.8 Eureka Collector (app-discovery-eureka)

This collector collects information about Eureka Servers and Eureka Clients through the development APIs provided by Eureka. For details about the configuration parameters, see **Table 4-8**.

Table 4-8 Parameters for configuring the Eureka collector

Parameter	Mandatory	Configuration
output_path	No	Enter the storage path of the collection result file (app-discovery-eureka-xxx.csv). If this parameter is left blank, the storage path defaults to <*Collector installation path*>**\output\file**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-eureka\output\file\app-discovery-eureka-xxx.csv
password	No	If user authentication is enabled, enter the passwords for accessing the Eureka servers. Separate multiple passwords with commas (,) based on the endpoint sequence. If a server does not require a password, enter a space. Example: password1, ,password2
endpoint	Yes	Enter the Eureka server addresses. If Eureka is deployed as a cluster of servers, separate the addresses with commas (,). Example: http://*IP address 1*:*Port 1*,http://*IP address 2*:*Port2* • If user authentication is enabled, add the *Username*@ before *IP address:Port*. Example: http://*Username*@*IP address 1*:*Port 1*,http://*Username*@*IP address 2*:*Port2* • If HTTPS authentication is enabled, change **http://** to **https://**.

4.3.9 Redis Collector (app-discovery-redis)

This collector connects to a Redis node to obtain it IP address, version, and IP addresses of connected clients. For details about the configuration parameters, see **Table 4-9**.

Table 4-9 Parameters for configuring the Redis collector

Parameter	Mandatory	Configuration
output_path	No	Enter the storage path of the collection result file (app-discovery-redis-xxx.csv). If this parameter is left blank, the storage path defaults to <*Collector installation path*>**\output\file**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-redis\output\file\app-discovery-redis-xxx.csv
password	No	If **auth** is set to **1**, set this parameter to the Redis node login password.
mode	Yes	Specify the Redis deployment mode. • **0**: single-node • **1**: cluster
auth	Yes	Specify the Redis authentication method. • **0**: indicates no authentication is required. • **1**: indicates password authentication.
port	Yes	Enter the Redis port.
host	Yes	Enter the IP address of the Redis node.

4.3.10 MongoDB Collector (app-discovery-mongodb)

This collector collects a MongoDB server information and information about connected clients. For details about the configuration parameters, see **Table 4-10**.

Table 4-10 Parameters for configuring the MongoDB collector

Parameter	Mandatory	Configuration
output_path	No	Enter the storage path of the collection result file (app-discovery-mongodb-xxx.csv). If this parameter is left blank, the storage path defaults to <*Collector installation path*>**\output\file**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-mongodb\output\file\app-discovery-mongodb-xxx.csv

Parameter	Mandatory	Configuration
ssl_ca_file	No	If SSL is used for connection, enter the path of the CA certificate file (.pem). You are advised to use a specific set of CA certificates instead of a server certificate issued and signed by a well-known organization.
ssl_client_private_key_password	No	If the private key contained in the certificate file has been encrypted, enter the password or passphrase.
ssl_client_certificate_key_file	No	Enter the path of the .pem file that concatenates the certificate and its private key. If the private key of the certificate is stored in a separate file, it should be concatenated with the certificate file.
auth_source	No	Enter the MongoDB authentication source.
times	Yes	Set the number of collection times. The value ranges from 1 to 1,000.
interval	Yes	Set the collection interval, in seconds. The value ranges from 1 to 60.
password	Yes	Enter the login password.
user	Yes	Enter the name of the user who has the ClusterMonitor and ReadAnyDatabase permissions.
endpoint	Yes	Enter the connection endpoint of the MongoDB server, for example, 127.0.0.1:27017.

4.3.11 MySQL-General Log Collector (app-discovery-mysql-generallog)

This collector collects the host and port information of clients based on the general log of a MySQL database. For details about the configuration parameters, see **Table 4-11**.

Table 4-11 Parameters for configuring the MySQL-General Log collector

Parameter	Mandatory	Configuration
output_path	No	Enter the storage path of the collection result file (app-discovery-mysql-generallog-xxx.csv). If this parameter is left blank, the storage path defaults to <*Collector installation path*>**\output\file**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-mysql-generallog\output\file\app-discovery-mysql-generallog-xxx.csv
exclude_ip	No	Enter the IP addresses of the clients whose data does not need to be collected. Use commas (,) to separate multiple IP addresses. Example: 127.0.0.1,192.168.1.1

import	Yes	Enter the path of the general log, for example, **C:\data\logs**.
		To enable MySQL general log, perform the following steps:
		1. Add the following configuration information to [mysqld] in the **my.ini** file:
		`log-output=FILE`
		`general_log=1`
		`general_log_file="D:\mysqllog\mysql_general.log"`
		general_log_file indicates the log file path. In Linux, the example path is **/data/log/mysql_general.log**.
		2. Run the following command to restart the MySQL service:
		`net stop mysql`
		`net start mysql`

4.3.12 MySQL-JDBC Collector (app-discovery-mysql-jdbc)

This collector collects the host and port information of clients connected to a MySQL database by accessing the process list table of the MySQL database through JDBC. For details about the configuration parameters, see **Table 4-12**.

Table 4-12 Parameters for configuring the MySQL-JDBC collector

Parameter	Mandatory	Configuration
output_path	No	Enter the storage path of the collection result file (app-discovery-mysql-jdbc-xxx.csv). If this parameter is left blank, the storage path defaults to <*Collector installation path*>**\output\file**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-mysql-jdbc\output\file\app-discovery-mysql-jdbc-xxx.csv
ssl	No	If the SSL connection using the CA certificate fails, enter the SSL parameters supported by PyMySQL for login in format of *Parameter name 1*,*Parameter value 1*,*Parameter name 2*,*Parameter value 2*. For details about the parameters, see **Table 4-13**. Example: ca,/data/ca.pem,key,/data/client-key.pem,cert,/data/client-cert.pem,check_hostname,True
ca	No	If the SSL CA authentication is enabled, set this parameter to the path where the CA certificate is stored. In Linux, the default location of MySQL certificates depends on the MySQL installation mode and version. Generally, MySQL certificates are stored in the following directories: • MySQL 5.6 or earlier: /etc/mysql/ • MySQL 5.7 or later: /var/lib/mysql/ For cloud databases, see the database documentation provided by the cloud vendors. • Huawei Cloud **Relational Database Service (RDS)** • Alibaba Cloud **Relational Database Service (RDS)**
exclude_ip	No	Enter the IP addresses of the clients whose data does not need to be collected. Use commas (,) to separate multiple IP addresses. Example: 127.0.0.1,192.168.1.1
password	Yes	Enter the login password.

Parameter	Mandatory	Configuration
user	Yes	Enter the name of the user who has the PROCESS permissions. To check the permissions of your MySQL account, perform the following steps: Run the following command in the database and check whether **PROCESS** is set to **Y**: `SELECT * FROM mysql.user`
port	Yes	Enter the port used to connect to and communicate with the MySQL server, for example, 3306.
endpoint	Yes	Enter the IP address of the MySQL server, for example, 192.168.1.100.

Table 4-13 PyMySQL SSL parameters

Parameter	Mandatory	Description
disabled	No	The default value is **False**. If this parameter is set to **True**, SSL is disabled. If no certificate is specified, this parameter does not take effect.
ca	Yes	Path of the CA certificate file
cert	Yes	Path of the client certificate file
key	Yes	Path of the client private key file
cipher	No	Encryption algorithm to be used
check_hostname	No	If this parameter is set to **True**, the hostname of the database server is verified during SSL connections. If no certificate is specified, this parameter does not take effect.

4.3.13 Nginx Configuration Collector (app-discovery-nginx)

This collector parses the configuration file of Nginx to obtain the Nginx redirection information. For details about the configuration parameters, see **Table 4-14**.

Table 4-14 Parameters for configuring the Nginx configuration collector

Parameter	Mandatory	Configuration
output_path	No	Enter the storage path of the collection result file (app-discovery-nginx-xxx.csv). If this parameter is left blank, the storage path defaults to <*Collector installation path*>**\output\file**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-nginx\output\file\app-discovery-nginx-xxx.csv
max_rewrite	No	Specify the maximum number of rewrites to be queried. The value is an integer ranging from 1 to 20.
filedir	Yes	Enter the path of the folder where the **nginx.conf** file is stored.

4.3.14 Cloud VPC Log Collector (app-discovery-cloud-vpc-log)

This collector collects VPC traffic information from log files. For details about the configuration parameters, see **Table 4-15**.

Table 4-15 Parameters for configuring the cloud VPC log collector

Parameter	Mandatory	Configuration
output_path	No	Enter the storage path of the collection result file (app-discovery-cloud-vpc-log-xxx.csv). If this parameter is left blank, the storage path defaults to <*Collector installation path*>**\output\file**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-cloud-vpc-log\output\file\app-discovery-cloud-vpc-log-xxx.csv
log_path	Yes	Enter the path of the VPC log file, for example, /data/logs/vpc_log.csv.

4.3.15 Nacos Collector (app-discovery-nacos)

This collector collects the service management and configuration management information of the Nacos service, so that it can collect information about source service architectures, discover dynamic services, and parse service associations. For details about the configuration parameters, see **Table 4-16**.

Table 4-16 Parameters for configuring the Nacos collector

Parameter	Mandatory	Configuration
output_path	No	Enter the storage path of the collection result file (app-discovery-nacos-xxx.csv). If this parameter is left blank, the storage path defaults to <*Collector installation path*>**\output\file**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-nacos\output\file\app-discovery-nacos-xxx.csv
rules_path	No	Enter the storage path of the collection rule file (a .properties file). If this parameter is left blank, the path defaults to <*Collector installation path*>**\config\rules.properties**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-nacos\config\rules.properties **NOTICE** You are advised to use the default rule file. If you need to customize collection rules, modify the default rule file.
password	Yes	Enter the login password.
username	Yes	Enter the name of the login user who has the read permissions.
port	Yes	Enter the port for accessing Nacos, for example, 8848.
ip	Yes	Enter the address for accessing Nacos, for example, http://127.0.0.1.

4.3.16 Application Configuration Collector (app-discovery-application-config)

This collector collects application configuration information through application configuration files. For details about the configuration parameters, see **Table 4-17**.

Table 4-17 Parameters for configuring the application configuration collector

Parameter	Mandatory	Configuration
output_path	No	Enter the storage path of the collection result file (app-discovery-application-config-xxx.csv). If this parameter is left blank, the storage path defaults to <*Collector installation path*>**\output\file**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-application-config\output\file\app-discovery-application-config-xxx.csv
rules_path	No	Enter the storage path of the collection rule file (a .properties file). If this parameter is left blank, the path defaults to <*Collector installation path*>**\config\rules.properties**. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-application-config\config\rules.properties **NOTICE** You are advised to use the default rule file. If you need to customize collection rules, modify the default rule file.
path	Yes	Enter the storage path of application configuration files (.yaml).

5 FAQs

5.1 What Are the Requirements on the Server for Installing Edge?

The Windows server for installing Edge must:

- Work on the intranet and can **access the Internet**.
- Use PowerShell **4.0** or later.

5.2 How Do I Run Edge in Compatibility Mode?

Step 1 Right-click the Edge installation program and choose **Properties** from the shortcut menu.

Step 2 Click the **Compatibility** tab. In the **Compatibility mode** area, select **Run this program in compatibility mode**.

Step 3 Click **OK** and restart the Edge installation program.

----End

5.3 What Can I Do If the Edge Device Is Offline?

You can perform the following operations:

- Check whether the server where Edge is installed can access the Internet.
- Check whether the Edge process is running properly.

5.4 How Do I Upgrade Edge to the Latest Version?

Description

If in the Edge device list, **Upgrade available** is displayed in the **Version** column of your device, the installed Edge is not the latest version. To ensure complete functions, you need to upgrade the Edge to the latest version.

Procedure

Step 1 Log in to the **MgC** console from the Windows server where Edge of an earlier version is installed.

Step 2 In the navigation pane on the left, choose **Tools**. In the Edge pane, choose **Download** > **Windows version**.

Step 3 Double-click the downloaded Edge installation package to start the installation and overwrite the Edge of the earlier version. After the installation is complete, go to the MgC console and check that the device version is the latest in the device list.

----End

5.5 How Do I Uninstall Edge?

The uninstallation method depends on the Windows OS version.

CAUTION

You need to uninstall the Edge application and MSI installation program.

Method 1

Step 1 Choose **Start** > **Control Panel**.

Step 2 Click **Programs and Features** or **Uninstall a program**.

Step 3 Enter **Edge** in the search box in the upper right corner of the page to filter the installed Edge software. Right-click the software name and choose **Uninstall/Change** from the shortcut menu to uninstall the software.

----End

Method 2

Step 1 Press Win+I to open Windows Settings, and then click **Applications**.

Step 2 Enter Edge in the search box to filter out the installed Edge software. Click the software name and click **Uninstall** in the lower right corner to uninstall the software.

----End

5.6 How Do I Fix the Error "The collector is not installed" When a Discovery Task Fails?

Symptom

After the Edge device and resource credential are associated, the deeper discovery fails, and the failure cause is "The collector is not installed".

Possible Causes

The required collector on the Edge device became offline.

Solution

The solution described here is true for all collectors. The following table lists the collectors integrated in Edge.

Collector	Collected Resource	Process	Installation Directory
rda-collector-platform	Private cloud: Only VMware is supported.	rda-collector-platform.exe	<Installation path>\Edge\tools\plugins\collectors
rda-collector-server	Server	rda-collector-server.exe	
rda-collector-kubernetes	Container	rda-collector-kubernetes.exe	

Step 1 Go to the **bin** directory in the collector installation directory on the Edge device, for example, C:\Edge\tools\plugins\collectors\rda-collector-server\bin.

Step 2 Double-click **start.bat** to start the server collector.

Step 3 Open the task manager. On the details page, check the running status of the host collector **rda-collector-server.exe**. If the status is **Running**, the collector is started.

Step 4 Return to the MgC console and click **Rediscover** in the **Status** column to collect the resource again.

----End

5.7 What Can I Do If the Port Required by Edge Is Occupied and the Installation Fails?

Symptom

When you tried to install Edge, the following message was displayed: Port used by Edge is occupied. Stop the process that occupies the port and try again.

Possible Causes

The default port 27080 for installing Edge is occupied.

Solution

Stop the application process that occupies port 27080.

WARNING

Before stopping the application process, evaluate the risks by yourself.

Linux

Step 1 Query the ID of the application that occupies the port.

```
netstat -tlnp | grep 27080
```

Assume that the queried application ID is 11083.

```
[root@rda-linux scripts]# netstat -tlnp | grep 7080
tcp6       0      0 :::7080                 :::*                    LISTEN      11083/java
```

Step 2 Query the application process based on the obtained application ID. The application ID is only an example. Replace it with the actual application ID.

```
ps -ef | grep 11083
```

Step 3 Confirm that the application occupying the port can be stopped, and run the following command to stop the application process. Then reinstall Edge.

```
kill -9 11083
```

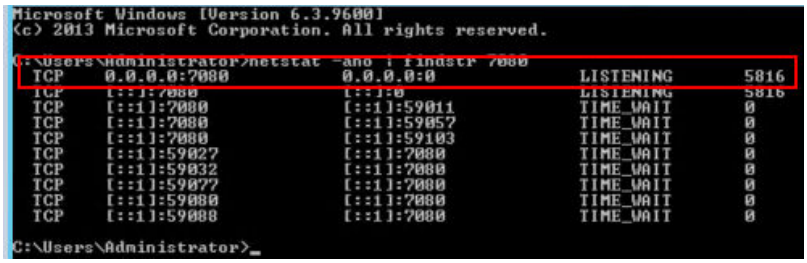
----End

Windows

Step 1 Open the CLI and run the following command to query the ID of the application that occupies the port.

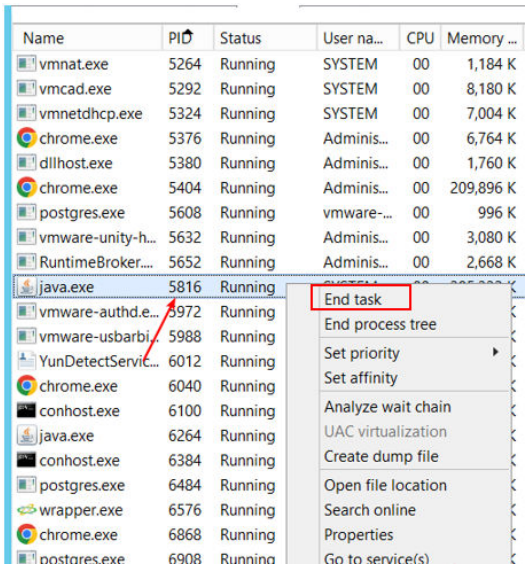
```
netstat -ano | findstr 27080
```

Assume that the queried application ID is 5816. The application ID is only an example. Replace it with the actual query result.



Step 2 Open the **Task Manager**. On the **Details** tab page, find the application process based on the queried application ID.

Step 3 Confirm that the application occupying the port can be stopped, and right-click the application process and choose **End task** from the shortcut menu to stop the application process. Then reinstall Edge.



----End

5.8 What Can I Do If AK/SK Verification Fails?

Symptom

When you tried to register an Edge device to MgC, a message was displayed indicating that the AK/SK authentication failed.

Possible Causes

Possible causes are:

- The entered AK or SK is incorrect.
- The AK/SK pair has been deleted or disabled.
- The programmatic access mode is not enabled for the account that owns the AK/SK pair.

Solutions

- **The entered AK or SK is incorrect.**

  Check whether the entered AK/SK pair of the Huawei Cloud account is correct, especially whether any spaces or characters are missed during the copy. Enter the AK/SK pair for authentication again.

- **The AK/SK pair has been deleted or disabled.**

  Choose **My Credentials** > **Access Keys** to check whether the AK is in the list.

  – If it is not, use an AK/SK pair in the list for authentication or create an AK/SK pair.

  – If it is, check whether it is disabled. If the AK is disabled, enable it.

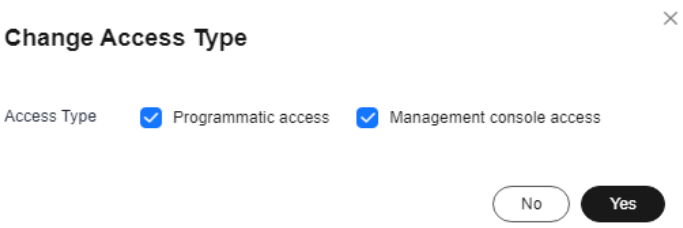
- The programmatic access mode is not enabled for the account that owns the AK/SK pair.

  a. Log in to the management console.

  b. Click the username in the upper right corner and choose **Identity and Access Management**.

  c. In the navigation pane on the left, choose **Users** and click the username you used for migration.

  d. Check whether **Programmatic access** is selected for **Access Type**. If it is nor, click  next to **Access Type**, select **Programmatic Access**, and click **Yes**



5.9 How Do I Configure WinRM on a Windows Source Server and Troubleshoot WinRM Connection Problems?

This section describes how to configure WinRM on a Windows source server and the solutions to connection problems.

Configuring WinRM

Step 1 Log in to the server as an administrator (for example, an administrator account or a local user account in the administrators group).

Step 2 Run PowerShell as administrator.

Step 3 Run the following command on PowerShell to start WinRM:

```
winrm quickconfig
Enable-PSRemoting
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
```


Step 4 Log in to the server where Edge is installed as an administrator and run PowerShell as administrator. Perform steps 5 to 7 on the server with Edge installed.

Step 5 Add the source server to the trusted host list.

Run the following command on PowerShell to add the source server to the trusted host list:

```
winrm set winrm/config/client '@{TrustedHosts="*"}'
```

For security purposes, you are advised to use hostname or IP address of the source server to replace the asterisk (*) in the **TrustedHosts** value. If it is not replaced, any host is trusted.

Step 6 Remotely connect to the source server.

Run the following command to test the connection to the source server. Replace *Login account* and *Source server IP address* with the actual login account and IP address of the source server.

```
Enter-PSSession -Credential Login account -ComputerName Source server IP address
```

Step 7 In the dialog box that is displayed, enter the username and password for logging in to source server and click **OK**.

- If the connection is successful, you can run any command to test the connectivity.
- If the connection fails, rectify the fault by referring to **WinRM Connection Failure Troubleshooting**.

----End

WinRM Connection Failure Troubleshooting

If the remote connection fails, check:

- **Port settings**: Use telnet to check whether port 5985 on the source server can be accessed. If the port cannot be accessed, check the settings of the firewall or security protection software on the source server to ensure that port 5985 is open.

  ```
  telnet ip port
  ```

- **Network settings**: Run the following command to check whether the network mode is set to Classic.

  ```
  reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa" /v forceguest
  ```

  - If the value of **forceguest** is **REG_DWORD 0x0**, the network mode is Classic
  - If the value of **forceguest** is not **REG_DWORD 0x0**, run the following command to change it:

    ```
    reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa"  /v forceguest /t reg_dword /d 0x0
    ```

- **Username and password**: Ensure that the username and password entered in the connection command are correct.

The preceding steps can rectify common connection problems. If the problem persists, contact technical support.

6 Change History

Released On	Description
2024-07-11	This issue is the sixth official release. Added **How Do I Configure WinRM on a Windows Source Server and Troubleshoot WinRM Connection Problems?**
2024-03-21	This issue is the fifth official release. • Added **What Can I Do If the Port Required by Edge Is Occupied and the Installation Fails?** • Added **What Can I Do If AK/SK Verification Fails?**
2024-01-15	This issue is the third official release. • Updated **Adding Resource Credentials**.
2023-12-20	This issue is the second official release. • Added **Tool Discovery**. • Added **How Do I Fix the Error "The collector is not installed" When a Discovery Task Fails?**. • Added **Configuring Collector Parameters**. • Added **How Do I Uninstall Edge?**.
2023-11-30	This issue is the first official release.

