

Migration Center

Tools Guide

Issue 16
Date 2025-02-14



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. 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 Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Contents

1 MgC Agent Overview	1
2 Downloading and Installing the MgC Agent (Formerly Edge)	23
2.1 Installing the MgC Agent on Windows	23
2.2 Installing the MgC Agent on Linux	26
3 Local Discovery and Collection	29
4 Connecting the MgC Agent to MgC	34
4.1 Connecting the MgC Agent to MgC	34
4.2 Managing Huawei Cloud Credentials	36
5 Agent-based Discovery	37
5.1 Adding Resource Credentials	37
5.2 Configuring an OBS Bucket	42
5.3 Managing MgC Agents	44
5.4 Event Recording	45
6 Collector-based Discovery	46
6.1 Creating a Collection Task	46
6.2 Managing Collectors	47
6.3 Configuring Collector Parameters	48
6.3.1 Kubernetes Static Collector (app-discovery-k8s)	48
6.3.2 Kubernetes Contrack Collector (app-discovery-k8s-contrack)	49
6.3.3 Kubernetes Pod Network Collector (app-discovery-k8s-pod-net)	51
6.3.4 Process and Network Collector (app-discovery-process-netstat)	52
6.3.5 Windows Process and Network Collector (app-discovery-process-netstat-win)	54
6.3.6 RabbitMQ Collector (app-discovery-rabbitmq)	56
6.3.7 Kafka Collector (app-discovery-kafka)	57
6.3.8 Eureka Collector (app-discovery-eureka)	57
6.3.9 Redis Collector (app-discovery-redis)	58
6.3.10 MongoDB Collector (app-discovery-mongodb)	59
6.3.11 MySQL-General Log Collector (app-discovery-mysql-generallog)	60
6.3.12 MySQL-JDBC Collector (app-discovery-mysql-jdbc)	61
6.3.13 Nginx Configuration Collector (app-discovery-nginx)	63
6.3.14 Cloud VPC Log Collector (app-discovery-cloud-vpc-log)	64

6.3.15 Nacos Collector (app-discovery-nacos).....	64
6.3.16 Application Configuration Collector (app-discovery-application-config).....	65
7 Best Practices.....	67
7.1 Setting JVM Parameters for the MgC Agent (Formerly Edge).....	67
7.1.1 Setting JVM Parameters for the MgC Agent's Tomcat Server.....	67
7.1.2 Setting JVM Parameters for Collectors.....	71
8 FAQs.....	74
8.1 What Are the Requirements for the Server for Installing the MgC Agent (Formerly Edge)?.....	74
8.2 How Do I Run the MgC Agent in Compatibility Mode?.....	75
8.3 What Can I Do If the MgC Agent (Formerly Edge) Is Offline?.....	75
8.4 Why Can't the MgC Agent (Formerly Edge) Start After Being Installed?.....	76
8.4.1 MgC Agent for Windows.....	76
8.4.2 MgC Agent for Linux.....	76
8.5 How Do I Upgrade the MgC Agent (Formerly Edge) to the Latest Version?.....	77
8.5.1 Upgrading the MgC Agent for Windows.....	77
8.5.2 Upgrading the MgC Agent for Linux.....	77
8.6 How Do I Uninstall the MgC Agent (Formerly Edge)?.....	78
8.6.1 Uninstalling the MgC Agent for Windows.....	78
8.6.2 Uninstalling the MgC Agent for Linux.....	78
8.7 How Do I Restart the MgC Agent (Formerly Edge)?.....	79
8.8 How Do I Check the Current MgC Agent Version (Formerly Edge)?.....	80
8.9 How Do I Obtain Run Logs of the MgC Agent (Formerly Edge) on Linux?.....	80
8.10 How Do I Fix the Error "The collector is not installed" When a Discovery Task Fails?.....	82
8.11 How Do I Obtain the Hive Metastore Credential Files?.....	84
8.12 What Can I Do If the Port Required by the MgC Agent Is Occupied and the Installation Fails?.....	84
8.13 What Can I Do If AK/SK Verification Fails?.....	86
8.14 How Do I Configure WinRM and Troubleshoot WinRM Connection Problems?.....	87
8.15 What Do I Do If the Credential List Is Empty When I Create a Data Connection for Big Data Verification?.....	89

1 MgC Agent Overview

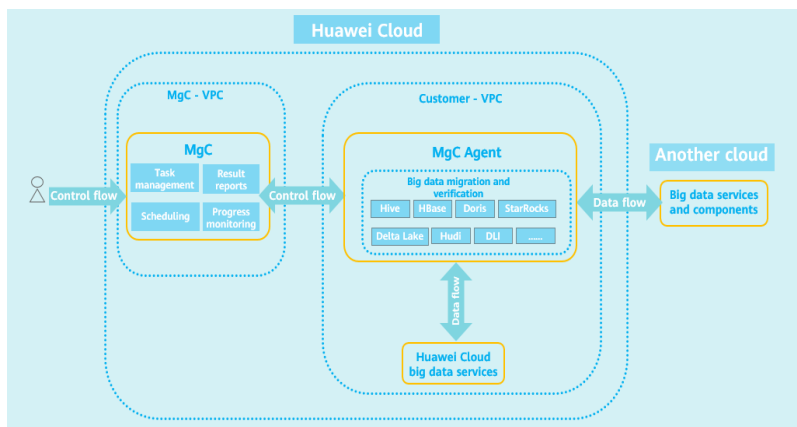
The MgC Agent (formerly Edge) is a tool that collects information about your source resources and executes migration commands from MgC.

Architecture

The MgC Agent can be deployed at the network edge of your cloud environment and is used to collect and migrate data. It frees you from these complex tasks. As a bridge between the MgC and your network, the MgC Agent ensures smooth, secure data migration.

Figure 1-1 shows the logical architecture of MgC Agent in big data migration and verification scenarios.

Figure 1-1 Logical architecture in big data scenarios



Feature Switches

The following table lists the MgC Agent 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 the MgC Agent.	<ul style="list-style-type: none"> • NoopHostnam eVerifier: The verification is disabled. • MustHostnam eVerifier: The verification is enabled. 	<installation-path>\Edge\tools\SecAs-1.2.29\webmanagementapps\the MgC Agent-server-0.0.1\WEB-INF\classes\application.yml
edge.plugin-ssl-mode	Indicates whether to use the SSL channel for tunneling Remote Procedure Call (RPC) connections.	<ul style="list-style-type: none"> • true: The SSL channel is used to tunnel RPC connections. • false: The SSL channel is not used to tunnel RPC connections. 	<installation-path>\Edge\tools\SecAs-1.2.29\webmanagementapps\the MgC Agent-server-0.0.1\WEB-INF\classes\application.yml

Domain Names

The following table lists the domain names that the MgC Agent must be able to access.

Parameter	Description	Value	Location
edge.iot-host	The IoTDA service address	<ul style="list-style-type: none"> AP-Singapore: ssl:// 31f50f5a99.st1.iotda-device.ap-southeast-3.myhuaweicloud.com:8883 LA-Santiago: ssl:// eee2b036e2.st1.iotda-device.la-south-2.myhuaweicloud.com:8883 LA-Sao Paulo: ssl:// eee2b036e2.st1.iotda-device.sa-brazil-1.myhuaweicloud.com:8883 TR-Istanbul: ssl:// aa6d529566.st1.iotda-device.tr-west-1.myhuaweicloud.com:8883 	<i><installation-path></i> \Edge\tools\SecAs-1.2.29\we bmanagementaps\the MgC Agent-server-0.0.1\WEB-INF\classes\application.yml
edge.mgc-host	The MgC service address	<ul style="list-style-type: none"> AP-Singapore: https://mgc.ap-southeast-3.myhuaweicloud.com LA-Santiago: https://mgc.la-south-2.myhuaweicloud.com LA-Sao Paulo: https://mgc.sa-brazil-1.myhuaweicloud.com TR-Istanbul: https://mgc.tr-west-1.myhuaweicloud.com 	
edge.vars.sms-agent-url	The SMS bucket address	https://sms-resource-intl-ap-southeast-3.obs.ap-southeast-3.myhuaweicloud.com	

Parameter	Description	Value	Location
edge.vars.sms-domain	The SMS domain name	sms.ap-southeast-3.myhuaweicloud.com	

Source servers must be able to access the domain names of cloud services listed in the following table.

Cloud Service	Domain Name
SMS	SMS domain name for all regions except LA-Sao Paulo: https://sms.ap-southeast-3.myhuaweicloud.com:443 SMS domain name for LA-Sao Paulo: https://sms.sa-brazil-1.myhuaweicloud.com:443
OBS	https://sms-resource-intl-ap-southeast-3.obs.ap-southeast-3.myhuaweicloud.com:443 , which is the address for downloading SMS-Agent.
IAM	iam.myhuaweicloud.com and the IAM domain name for the target region. For details about the IAM domain name for each region, see Endpoints . For example: <ul style="list-style-type: none">• If the target region is AP-Singapore, source servers must be able to access https://iam.myhuaweicloud.com and https://iam.ap-southeast-3.myhuaweicloud.com:443.• If the target region is LA-Sao Paulo, source servers must be able to access https://iam.myhuaweicloud.com and https://iam.sa-brazil-1.myhuaweicloud.com:443.• If the target region is TR-Istanbul, source servers must be able to access https://iam.myhuaweicloud.com and https://iam.tr-west-1.myhuaweicloud.com:443.
ECS	The ECS domain name for the target region. For details about the ECS domain name for each region, see Endpoints . For example: <ul style="list-style-type: none">• If the target region is AP-Singapore, its domain name is https://ecs.ap-southeast-3.myhuaweicloud.com:443.• If the target region is LA-Sao Paulo, the ECS domain name is https://ecs.sa-brazil-1.myhuaweicloud.com:443.• If the target region TR-Istanbul, its domain name is https://ecs.tr-west-1.myhuaweicloud.com:443.

Cloud Service	Domain Name
IMS	<p>The IMS domain name for the target region. For details about the IMS domain name for each region, see Endpoints.</p> <p>For example:</p> <ul style="list-style-type: none">• If the target region is AP-Singapore, its domain name is https://ims.ap-southeast-3.myhuaweicloud.com:443.• If the target region is LA-Sao Paulo, its domain name is https://ims.sa-brazil-1.myhuaweicloud.com:443.• If the target region TR-Istanbul, its domain name is https://ims.tr-west-1.myhuaweicloud.com:443.
EVS	<p>The EVS domain name for the target region. For details about the EVS domain name for each region, see Endpoints.</p> <p>For example:</p> <ul style="list-style-type: none">• If the target region is AP-Singapore, its domain name is https://evs.ap-southeast-3.myhuaweicloud.com:443.• If the target region is LA-Sao Paulo, the EVS domain name is https://evs.sa-brazil-1.myhuaweicloud.com:443.• If the target region TR-Istanbul, its domain name is https://evs.tr-west-1.myhuaweicloud.com:443.
VPC	<p>The VPC domain name for the target region. For details about the VPC domain name for each region, see Endpoints.</p> <p>For example:</p> <ul style="list-style-type: none">• If the target region is AP-Singapore, its domain name is https://vpc.ap-southeast-3.myhuaweicloud.com:443.• If the target region is LA-Sao Paulo, its domain name is https://vpc.sa-brazil-1.myhuaweicloud.com:443.• If the target region TR-Istanbul, its domain name is https://vpc.tr-west-1.myhuaweicloud.com:443.

Credentials Required for Data Collection

The MgC Agent can gather details of various resources, such as servers, databases, containers, VMware environments, and cloud platforms. You must provide the MgC Agent with the credentials for accessing your servers, databases, containers, VMware platforms, and cloud platforms (AK/SK pairs).

Communication Matrix

The communication matrix lists the ports used by the MgC Agent for different purposes, along with the transport layer protocols, authentication types, and encryption modes.

Table 1-1 MgC Agent communication matrix

Source Device	Source IP Address	Source Port	Destination Device	Destination IP Address	Destination Port (for Listening)	Protocol	Port Description	Listening Port Configurable	Authentication Type	Encryption Mode
-	-	-	MgC Agent server	IP address of the MgC Agent server	27080	HTTPS	The MgC Agent listening port, which is used for man-machine interaction.	No	Password	HTPS
MgC Agent server	IP address of the MgC Agent server	-	MgC Agent server	IP address of the MgC Agent server	5678	TCP	The MgC Agent listening port, which is used for internal interaction between collectors and the MgC Agent.	No	None	None

Source Device	Source IP Address	Source Port	Destination Device	Destination IP Address	Destination Port (for Listening)	Protocol	Port Description	Listening Port Configurable	Authentication Type	Encryption Mode
		-	Server	IP address of the destination server	User input	TCP	SSH port, which is used for file transfer (over SCP and SFTP) and execution of collection scripts.	Yes	Password	SSL
		-	Server	IP address of the destination server	5985	TCP	WinRM port, which is used to remotely execute collection scripts.	No	Password	HT TPS

Source Device	Source IP Address	Source Port	Destination Device	Destination IP Address	Destination Port (for Listening)	Protocol	Port Description	Listening Port Configurable	Authentication Type	Encryption Mode
		8080	Platform	IP address of the destination server	443	TCP	Listening port used for collecting VMware platform information. The source port is the default port that is inherited from the Wus han framework and is not used by services.	No	Password	HT TPS

Source Device	Source IP Address	Source Port	Destination Device	Destination IP Address	Destination Port (for Listening)	Protocol	Port Description	Listening Port Configurable	Authentication Type	Encryption Mode
		8000	Database	IP address of the destination server	User input	TCP	Listening port of the database service. The source port is the default port that is inherited from the Wus han framework and is not used by services.	Yes	Password	SSL

Source Device	Source IP Address	Source Port	Destination Device	Destination IP Address	Destination Port (for Listening)	Protocol	Port Description	Listening Port Configurable	Authentication Type	Encryption Mode
		7050	Container	IP address of the destination server	User input	TCP	Listening port of the container service. The source port is the default port that is inherited from the Wus han framework and is not used by services.	Yes	Key file	HT TPS

Source Device	Source IP Address	Source Port	Destination Device	Destination IP Address	Destination Port (for Listening)	Protocol	Port Description	Listening Port Configurable	Authentication Type	Encryption Mode
		9977	Storage	IP address of the destination server	User input	TCP	Listening port of the object storage service. The source port is the default port that is inherited from the Wus han framework and is not used by services.	Yes	Password	SSL

Command Matrix

The command matrix lists the commands contained in the MgC Agent as well as the absolute paths, functions, and usage of the commands.

Table 1-2 MgC Agent command matrix

Node	Command	Absolute Path	Whether Can Be Invoked Independently	Function	Usage	Risk	Category
Edge	accountPermission.ps1	/Edge/tools/plugins/collectors/rda-collector-server/powershell	Yes	Queries the roles assigned to the administrator user group.	.\accountPermission.ps1	None	Function
	basicInfo.ps1	/Edge/tools/plugins/collectors/rda-collector-server/powershell	Yes	Queries the basic information.	.\basicInfo.ps1	None	Function
	checkBasicObjects.ps1	/Edge/tools/plugins/collectors/rda-collector-server/powershell	Yes	Checks basic system components.	.\checkBasicObjects.ps1	None	Function
	checkPerformanceObjects.ps1	/Edge/tools/plugins/collectors/rda-collector-server/powershell	Yes	Checks basic system performance components.	.\checkPerformanceObjects.ps1	None	Function

Node	Command	Absolute Path	Whether Can Be Invoked Independently	Function	Usage	Risk	Category
	diskInfo.ps1	/Edge/tools/plugins/collectors/rda-collector-server/powershell	Yes	Queries basic disk information.	.\diskInfo.ps1	None	Function
	eachDiskPerformance.ps1	/Edge/tools/plugins/collectors/rda-collector-server/powershell	Yes	Queries disk performance information.	.\eachDiskPerformance.ps1	None	Function
	fileSharingInfo.ps1	/Edge/tools/plugins/collectors/rda-collector-server/powershell	Yes	Queries file system information.	.\fileSharingInfo.ps1	None	Function
	fireware.ps1	/Edge/tools/plugins/collectors/rda-collector-server/powershell	Yes	Queries firmware information.	.\fireware.ps1	None	Function

Node	Command	Absolute Path	Whether Can Be Invoked Independently	Function	Usage	Risk	Category
	memorySize.ps1	/Edge/tools/plugins/collectors/rda-collector-server/powershell	Yes	Queries memory information.	.\memorySize.ps1	None	Function
	netcardInfo.ps1	/Edge/tools/plugins/collectors/rda-collector-server/powershell	Yes	Queries NIC information.	.\netcardInfo.ps1	None	Function
	netcardPerform.ps1	/Edge/tools/plugins/collectors/rda-collector-server/powershell	Yes	Queries NIC bandwidth and PPS information.	.\netcardPerform.ps1	None	Function
	oemSystem.ps1	/Edge/tools/plugins/collectors/rda-collector-server/powershell	Yes	Checks the OEM system.	.\oemSystem.ps1	None	Function

Node	Command	Absolute Path	Whether Can Be Invoked Independently	Function	Usage	Risk	Category
	osInfo.ps1	/Edge/tools/plugins/collectors/rda-collector-server/powershell	Yes	Queries OS information.	.\osInfo.ps1	None	Function
	processInfo.ps1	/Edge/tools/plugins/collectors/rda-collector-server/powershell	Yes	Queries process information.	.\processInfo.ps1	None	Function
	scheduledTasks.ps1	/Edge/tools/plugins/collectors/rda-collector-server/powershell	Yes	Queries scheduled task information.	.\scheduledTasks.ps1	None	Function
	specialHardware.ps1	/Edge/tools/plugins/collectors/rda-collector-server/powershell	Yes	Queries hardware information.	.\specialHardware.ps1	None	Function

Node	Command	Absolute Path	Whether Can Be Invoked Independently	Function	Usage	Risk	Category
	systemRoot.ps1	/Edge/tools/plugins/collectors/rda-collector-server/powershell	Yes	Queries system directories.	.\systemRoot.ps1	None	Function
	systemService.ps1	/Edge/tools/plugins/collectors/rda-collector-server/powershell	Yes	Checks the VSS service.	.\systemService.ps1	None	Function
	tcpNum.ps1	/Edge/tools/plugins/collectors/rda-collector-server/powershell	Yes	Queries the number of connections.	.\tcpNum.ps1	None	Function
	utilInfo.ps1	/Edge/tools/plugins/collectors/rda-collector-server/powershell	Yes	Queries performance information.	.\utilInfo.ps1	None	Function

Node	Command	Absolute Path	Whether Can Be Invoked Independently	Function	Usage	Risk	Category
	virtioDriver.ps1	/Edge/tools/plugins/collectors/rda-collector-server/powershell	Yes	Checks VirtIO drivers.	.\virtioDriver.ps1	None	Function
	getArchitecture.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries OS architecture.	sh getArchitecture.sh	None	Function
	getBootLoader.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries the system boot type.	sh getBootLoader.sh	None	Function
	getCPUCores.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries the number of CPUs.	sh getCPUCores.sh	None	Function

Node	Command	Absolute Path	Whether Can Be Invoked Independently	Function	Usage	Risk	Category
	getCpuFrequency.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries the CPU dominant frequency.	sh getCpuFrequency.sh	None	Function
	getCPURate.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries the CPU usage.	sh getCPURate.sh	None	Function
	getCPUtype.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries the CPU type.	sh getCPUtype.sh	None	Function
	getDisk_each_read_write_info.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries the disk throughput.	sh getDisk_each_read_write_info.sh	None	Function
	getDiskInfo.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries the basic disk information.	sh getDiskInfo.sh	None	Function

Node	Command	Absolute Path	Whether Can Be Invoked Independently	Function	Usage	Risk	Category
	getDiskUtil.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries the disk usage.	sh getDiskUtil.sh	None	Function
	getFileSharingInfo.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries file system information.	sh getFileSharingInfo.sh	None	Function
	getFirmwareType.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries the firmware type.	sh getFirmwareType.sh	None	Function
	getGPUDevices.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries GPU devices.	sh getGPUDevices.sh	None	Function
	getHostname.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries the hostname.	sh getHostname.sh	None	Function

Node	Command	Absolute Path	Whether Can Be Invoked Independently	Function	Usage	Risk	Category
	getMem.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries memory information.	sh getMem.sh	None	Function
	getMemRate.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries the memory usage.	sh getMemRate.sh	None	Function
	getKernel.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries the kernel information.	sh getKernel.sh	None	Function
	getNetCards.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries NIC information.	sh getNetCards.sh	None	Function
	getNetcardInfo.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries NIC bandwidth and PPS information.	sh getNetcardInfo.sh	None	Function

Node	Command	Absolute Path	Whether Can Be Invoked Independently	Function	Usage	Risk	Category
	getOsDisk.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries system disk information.	sh getOsDisk.sh	None	Function
	getOsInfo.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries OS information.	sh getOsInfo.sh	None	Function
	getRawDevices.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries raw device information.	sh getRawDevices.sh	None	Function
	getRsync.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Checks rsync.	sh getRsync.sh	None	Function
	getProcessInfo.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries process information.	sh getProcessInfo.sh	None	Function

Node	Command	Absolute Path	Whether Can Be Invoked Independently	Function	Usage	Risk	Category
	getScheduledTasks.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries scheduled task information.	sh getScheduledTasks.sh	None	Function
	getUSBDevices.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries GPU devices.	sh getUSBDevices.sh	None	Function
	getTcpTotal.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries the number of connections.	sh getTcpTotal.sh	None	Function
	getVirtioDriver.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Checks VirtIO drivers.	sh getVirtioDriver.sh	None	Function
	getVirtualType.sh	/Edge/tools/plugins/collectors/rda-collector-server/shell	Yes	Queries the virtualization type.	sh getVirtualType.sh	None	Function

2 Downloading and Installing the MgC Agent (Formerly Edge)

2.1 Installing the MgC Agent on Windows

The MgC Agent for Windows is used to collect details of resources such as servers, storage systems, containers, and big data clusters. In addition, it works with migration workflows to migrate applications and data to the cloud.

Preparations

- Prepare a Windows server for installing the MgC Agent (formerly Edge) in the source intranet environment. The Windows server must:
 - Be able to access the Internet and the domain names of MgC, IoTDA, and other cloud services. For details about the domain names to be accessed, see [Domain Names](#).
 - Allow the ports required by the MgC Agent (formerly Edge). For details about the required ports, see [Communication Matrix](#).
 - Use PowerShell **3.0** 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.
 - Not have any antivirus or protection software enabled. This type of software may stop the MgC Agent from executing migration commands, resulting in migration failures.

CAUTION

Do not install the MgC Agent on a source server to be migrated.

- **High resource consumption:** The MgC Agent consumes CPU and memory resources during collection and migration. If a large number of migration tasks are performed by the MgC Agent, services on the source server may be affected.
 - **Port occupation:** The MgC Agent occupies some ports on the server, which may affect services running on it.
-

- [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.

Notes and Constraints

- If there are Windows source servers to be migrated, these servers must:
 - Allow access from the server where the MgC Agent is installed over port 5985.
 - Have WinRM enabled and have connected to the server where the MgC Agent is installed. For more information, see [How Do I Configure WinRM on a Windows Source Server and Troubleshoot WinRM Connection Problems?](#)
 - Allow the execution of shell scripts. Open PowerShell on the source servers as an administrator and run the following command to view the current execution policy:

```
Get-ExecutionPolicy
```

If **Restricted** is returned, no script can be executed. Run the following command and enter **Y** to change the policy to **RemoteSigned**:

```
Set-ExecutionPolicy RemoteSigned
```

- If there are Linux source servers to be migrated, these servers must:
 - Allow access from the server where the MgC Agent is installed over port 22.
 - Allow direct root access. That means remote connections using root with SSH or other tools must be allowed on these Linux source servers.
 - Have SFTP and SSH enabled.
 - Support the following SSH connection security algorithms:
ssh-ed25519, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, rsa-sha2-512, and rsa-sha2-256

If a server does not support the preceding security algorithms, you are advised to upgrade OpenSSH to 8.0 or later. Otherwise, deep collection cannot be performed for that server.

- Have their iptables configured to allow all communications with the server where the MgC Agent is installed. Run the following command on the source servers. If the **source** field in the command output contains the IP address and port of the server where the MgC Agent is installed, it means that the MgC Agent is not allowed to access these source servers. In this case, ensure that access from the MgC Agent is permitted

```
iptables -L INPUT -v -n
```

```
[root@rda-linux ~]# iptables -L INPUT -v -n
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
0 0 DROP all -- * * 123.....3 0
```

- You are advised to change your MgC Agent access password every three to six months.

Procedure

Step 1 Sign in to the [MgC console](#) from the Windows server you prepared.

Step 2 In the navigation pane, choose **MgC Agents**.

- Step 3** In the **Windows** area, click **Download Installation Package** to download the MgC Agent installation package to the Windows server you prepared.
- Step 4** Decompress the downloaded the MgC Agent installation package, double-click the 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 the MgC Agent 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

The MgC Agent can only be installed in drive C. If you select another disk for installation, the MgC Agent may fail to start.

- Step 7** After the installation is complete, click **Finish** to open the MgC Agent console and go to the [User Registration](#) page.

----End

Registering an Account

When you log in to the MgC Agent 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**.

CAUTION

You are advised to change your password for accessing the MgC Agent every three to six months.

----End

2.2 Installing the MgC Agent on Linux

The MgC Agent for Linux is mainly used for big data verification, big data migration, and big data lineage collection.

Preparations

- Prepare a Linux server for installing the MgC Agent in the source intranet environment. The Linux server must:
 - Be able to access the Internet and the domain names of MgC, IoTDA, and other cloud services. For details about the domain names to be accessed, see [Domain Names](#).
 - Allow the ports required by the MgC Agent (formerly Edge). For details about the required ports, see [Communication Matrix](#).
 - Allow outbound traffic on 8883 if the server is in a security group.
 - Run CentOS 8.X.
 - Have at least 4 CPUs and 8 GB of memory. If you want to use big data verification, the server must have at least 8 CPUs and 16 GB of memory.

CAUTION

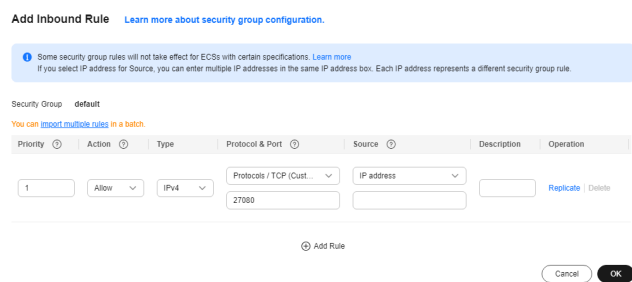
Do not install the MgC Agent on a source server to be migrated.

- **High resource consumption:** The MgC Agent consumes CPU and memory resources during collection and migration. If a large number of migration tasks are performed by the MgC Agent, services on the source server may be affected.
 - **Port occupation:** The MgC Agent occupies some ports on the server, which may affect services running on it.
-
- Run the following command to check whether rng-tools is installed on the Linux server where the MgC Agent is installed:

```
rpm -qa | grep rng-tools
```

If no rng-tools-related information is displayed, rng-tools is not installed on the server. Run the following command to install rng-tools:

```
yum -y install rng-tools
```
 - Disable any antivirus and protection software on the Linux server where the MgC Agent is installed. This type of software may stop the MgC Agent from executing migration commands, resulting in migration failures.
 - Add an inbound rule to the security group of the Linux server to allow TCP traffic on port 27080. Set the source address to the IP address of the Windows server you use to log in to the MgC Agent console.



- [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.

Downloading and Installing the MgC Agent

Step 1 Sign in to the [MgC console](#) from the Linux server you prepared.

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

Step 3 In the Linux area, click **Download Installation Package** or **Copy Download Command** to download the MgC Agent installation program to the Linux server.

Step 4 Decompress the MgC Agent installation package.

```
tar zxvf Edge.tar.gz
```

Step 5 Go to the **scripts** directory in the decompressed MgC Agent directory.

```
cd Edge/scripts/
```

Step 6 Run the MgC Agent installation script.

```
./install.sh
```

Step 7 Enter the EIP bound to the NIC of the Linux server. The IP address will be used for accessing the MgC Agent console. If the entered IP address is not used by the Linux server, the system will prompt you whether to use any public IP address of the Linux server as the MgC Agent access address.

```
Please enter the access address of the local server:1.1.1.1
The entered IP address is not in the local IP address list.
Do you want to allow access from all IP addresses?(y/n)
```

Step 8 Check if the message shown in the following figure is displayed. If it is, the MgC Agent for Linux has been installed. The port in the following figure is for reference only. Note the actual port returned. Generally, the port is 27080.

```
There are some variables appended into /etc/profile, if you want to make these available in current terminal, please run command 'source /etc/profile'

Open the Edge management console by accessing https://'Available IP of local host':27080/ from the browser.
```

Update environment variables.

```
source /etc/profile
```

Step 9 On the Windows server for which an inbound rule is added to the security group of the server where the MgC Agent is installed, open a browser and enter **https://<IP-address-entered-in-step-7>:<port-obtained-in-step-8>** in the address box to access the user registration page of the MgC Agent. For example, if the IP address

entered in step 7 is **192.168.x.x** and the port returned in step 8 is **27080**, the MgC Agent access address is **https://192.168.x.x:27080**.

NOTICE

If there are access problems, check the IP address entered in the address box and the inbound rule settings of the security group of the Linux server with the MgC Agent installed.

----End

Registering an Account

When you log in to the MgC Agent 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**.

CAUTION

You are advised to change your password for accessing the MgC Agent every three to six months.

----End

3 Local Discovery and Collection

The MgC Agent (formerly Edge) allows you to discover local servers and collect their details without the need of a connection to MgC.

Notes

- If local collection is required, do not connect the MgC Agent to MgC, or local collection will be unavailable. After being connected to MgC, the MgC Agent can only execute tasks issued from MgC and can no longer execute local collection .
- You are advised to connect the MgC Agent to MgC after all necessary local collection tasks are complete.

Methods for Discovering Servers

There are three methods for using the MgC Agent to discover servers locally.

- **VMware collection:** You provide the IP addresses and credentials of vCenter Servers to discover all VMs they manage.
- **RVTools data import:** You can import the report generated by RVTools to the MgC Agent. Then the MgC Agent can extract information about servers.
- **CIDR block scanning:** You can use the MgC Agent to scan for servers on a specific network range over the intranet.

Prerequisites

You have [installed the MgC Agent](#) and registered an account.

VMware Collection

Only VMware vSphere 5.0 to 7.0 are supported.

Step 1 Use the registered account to log in to the MgC Agent console.

Step 2 In the navigation pane, choose **Agent-based Discovery > Credentials**.

Step 3 Click **Discover Servers** above the list.

Step 4 Set **Discovery Mode** to **VMware collection** and set **Connection Address** to the IP address of your vCenter Server.

- Step 5** Select **Create** for **Credential** and enter the username and password for logging in to the vCenter Server.
- Step 6** Click **OK**. The MgC Agent starts to discover your server resources.
- Step 7** Click **View Task** in the upper right corner of the page. On the **Task List** page, view the task status. When the task is complete, you can view the discovered servers in the list.

If these servers need to be migrated, [perform a deep collection](#) for them.

NOTICE

To perform a deep collection for your source servers to collect as much as details, provide server credentials that meet the following requirements:

- Linux: **root** and its password
- Windows: **administrator** and its password

----End

RVTools Data Import

You need to [export resources details from RVTools](#).

Then import the RVTools data to the MgC Agent by following the requirements below:

- The supported RVTools versions include 4.4.1, 4.4.2, 4.4.3, 4.4.4, 4.4.5, 4.5.0, 4.5.1, and 4.6.1.
- The file to be imported must be in XLSX format.
- The file to be imported cannot be larger than 100 MB, and the compression ratio cannot be lower than 5%.

- Step 1** Use the registered account to log in to the MgC Agent console.
- Step 2** In the navigation pane, choose **Agent-based Discovery > Credentials**.
- Step 3** Click **Discover Servers** above the list.
- Step 4** Set **Discovery Mode** to **RVTools import**, click **Select File**, and select the file exported from RVTools.
- Step 5** Click **OK** to upload the file to the MgC Agent.
- Step 6** Click **View Task** in the upper right corner of the page. On the **Task List** page, view the task status. When the task is complete, you can view the imported servers in the list.

If these servers need to be migrated, [perform a deep collection](#) for them.

NOTICE

To perform a deep collection for your source servers to collect as much as details, provide server credentials that meet the following requirements:

- Linux: **root** and its password
- Windows: **administrator** and its password

----End

Network Range Scan

- Step 1** Use the registered account to log in to the MgC Agent console.
- Step 2** In the navigation pane, choose **Agent-based Discovery > Credentials**.
- Step 3** Click **Discover Servers** above the list.
- Step 4** Set **Discovery Mode** to **Network Range Scan** and set parameters based on [Table 3-1](#).

Table 3-1 Parameters for scanning a network range

Parameter	Description
Protocol	Only TCP is available.
Network Range	Enter an IP address range which must fall within: <ul style="list-style-type: none">• 10.0.0.0 – 10.255.255.255• 172.16.0.0 – 172.31.255.255• 192.168.0.0 – 192.168.255.255
Linux	Enter the port used to scanning for Linux servers. If you do not need to scan for Linux servers, set the port number to 0 .
Windows	Enter the port used to scanning for Windows servers. If you do not need to scan for Windows servers, set the port number to 0 .

- Step 5** Click **OK**. The MgC Agent starts to discover your server resources.
- Step 6** Click **View Task** in the upper right corner of the page. On the **Task List** page, view the task status. When the task is complete, you can view the discovered servers in the list.

If these servers need to be migrated, [perform a deep collection](#) for them.

NOTICE

To perform a deep collection for your source servers to collect as much as details, provide server credentials that meet the following requirements:

- Linux: **root** and its password
- Windows: **administrator** and its password

----End

Performing a Deep Collection for Servers

After server resources are discovered, perform the following steps to perform a deep collection for them:

- Step 1** In the server list, click **Configure Credential** in the **Operation** column.
- Step 2** Configure the parameters listed in [Table 3-2](#).

Table 3-2 Parameters for configuring a deep collection

Parameter	Configuration
Type	Set this parameter based on the source server OS type.
IP Address	Select the IP address for accessing the source server. It can be a public or private IP address.
Port	Enter the port on the source server that allows access from the MgC Agent. <ul style="list-style-type: none">• By default, port 5985 on Windows source servers must be opened to the MgC Agent. The port cannot be changed.• By default, port 22 on Linux source servers must be opened to the MgC Agent. You can specify a different port if needed.
Credential	Select the server credential. <ul style="list-style-type: none">• If the server credential has been added to the MgC Agent, select it from the drop-down list.• If the server credential has not been added to the MgC Agent, click Create Credential and add the server credential. Then select it from the drop-down list. <p>NOTICE</p> <p>The account provided in the credential must have sufficient permissions, so the MgC Agent can collect necessary server details. The credential you provided must meet the following requirements:</p> <ul style="list-style-type: none">• Linux: root account and its password• Windows: administrator account and its password

- Step 3** After the credential is configured, click **Deep Collection** in the **Operation** column. When **Collected** shows up in the **Deep Collection** column, the collection is complete.

----End

Exporting Server Information

On the server list page, click **Export** in the upper right corner to export all server information to a CSV file and download the file to the local PC.

4 Connecting the MgC Agent to MgC

4.1 Connecting the MgC Agent to MgC

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

After the connection is set up, you can perform the following operations on the MgC console:

- **Create resource discovery tasks** to discover multiple types of source resources over the Internet. You can also perform deep collection for the discovered resources, such as servers, containers, object storage, and databases.
- **Create server migration workflows** using the template provided by MgC. Before that, you can get target server recommendations based on the collected performance data of the source servers.
- **Create big data migration tasks.** Currently, migrating data from Alibaba Cloud MaxCompute to Huawei Cloud DLI is supported.
- **Create big data verification tasks** to verify data consistency.

Notes and Constraints

- A maximum of 100 MgC Agents can be online in an account.
- In a single MgC project, a maximum of five MgC Agents (regardless of the status) can be registered.

Prerequisites

You have [installed the MgC Agent](#) and registered an account.

Procedure

Step 1 Use the registered account to log in to the MgC Agent console.

Step 2 On the **Overview** page, click **Connect** in the upper right corner. The **Connect to MgC** page is displayed on the right.

Figure 4-1 Connecting the MgC Agent to MgC

The screenshot shows a 'Connect to MgC' dialog box with three steps:

- Step 1: Enter Credential**
 - Information: A credential is required to connect the MgC Agent to MgC. To obtain the credential, choose [My Credentials > Access Keys](#) Learn how.
 - Region: A dropdown menu with '--Select--'.
 - Huawei Cloud Account AK: A text input field.
 - Huawei Cloud Account SK: A text input field with a 'List Migration Projects' link.
 - Save as Target Credential: A checked checkbox. Below it, a note states: 'This credential will be deleted by default after the connection is complete. If you choose to save the credentials, they will be encrypted and saved locally and will be used for migrating source servers and uploading logs. guide right at _3p.3'.
- Step 2: Select MgC Migration Project**
 - Information: If no project is found, you can create one on the Settings page of the MgC console.
 - Migration Project: A dropdown menu with '--Select--'.
- Step 3: Preset MgC Agent Name**
 - Information: This name uniquely identifies the MgC Agent on the MgC console. It cannot be modified after the MgC Agent is connected to MgC.

A 'Connect' button is located at the bottom right of the dialog.

Step 3 In **Step 1: Enter Cloud Credential**, select the region where your MgC migration project is located, enter the AK/SK of your Huawei Cloud account, and click **Query Project**. After the MgC Agent is authenticated using the entered AK/SK pair, you can go to the next step. If the system displays a message indicating that the AK/SK pair is incorrect, try to rectify the fault by following the instructions in [What Can I Do If the AK/SK Verification Fails?](#)

NOTICE

If your source servers need to be migrated, the entered AK/SK pair must have permissions to use SMS. For details, see [SMS Custom Policies](#).

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 MgC Agent 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 established. When you migrate workloads to Huawei Cloud, the AK/SK pair will be delivered to SMS-Agent on the source servers for executing the migration.

Step 4 In **Step 2: Select MgC Migration Project**, select a [migration project](#) from the project drop-down list. The MgC Agent will report the collected information about your source resources to this project.

Step 5 In **Step 3: Preset MgC Agent Name**, specify a name for the MgC Agent, which will be displayed on the MgC console, and click **Next**. Confirm the connection to MgC, and click **OK**.

 **CAUTION**

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

Step 6 If **Connected** shows up on the overview page, the connection to MgC is successful.

----End

4.2 Managing Huawei Cloud Credentials

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

Prerequisites

[The MgC Agent has been connected to MgC.](#)

Adding Huawei Cloud Credentials

If you did not save the Huawei Cloud credentials used to [connect the MgC Agent to MgC](#) as the migration credentials, you can add those or other credentials by following the instructions below.

Step 1 On the **Overview** page of the MgC Agent (formerly Edge) console, click **View Configuration** in the upper right corner

Step 2 In the Huawei Cloud account box, click **Configure**.

Step 3 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

5 Agent-based Discovery

5.1 Adding Resource Credentials

You need to provide the MgC Agent (formerly Edge) with the credentials for accessing your source resources, so it can collect information about them and migrate them to Huawei Cloud. After you connect the MgC Agent to MgC, only the attributes of source resources' credentials will be synchronized to MgC. The credentials themselves are encrypted and stored locally, and will not be synced to MgC.

 CAUTION

Credentials you add to the MgC Agent are valid for 60 days. After the validity period expires, you need to add the credentials to the MgC Agent again if you still want to discover or migrate the resources.

Prerequisites

You have [installed the MgC Agent](#) in your source environment and [connected the MgC Agent to MgC](#).

Authentication Methods

You can add credentials of the following types of resources to the MgC Agent: private clouds, servers, big data clusters, and containers. For details about the authentication methods supported for each resource type, see [Table 5-1](#).

Table 5-1 Authentication methods

Resource Type	Authentication Method	Description
Public cloud	<ul style="list-style-type: none"> AK/SK Configuration file ID/Secret 	<ul style="list-style-type: none"> AK/SK pairs of cloud platforms, such as Huawei Cloud, Alibaba Cloud, AWS, Tencent Cloud, Qiniu Cloud, and Kingsoft Cloud 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. IDs and secrets are Azure credentials. To learn how to obtain Azure credentials, see How Do I Obtain Azure Credentials?
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.
Big data - Executor	Username/Password	<p>Enter the username and password for logging in to the server deployed as an executor. Then specify Network Range, which can be a single IP address or an IP address range.</p> <p>The value can be:</p> <ul style="list-style-type: none"> 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.
Big data - Hive Metastore	Username/Key	Upload the core-site.xml , hivemetastore-site.xml , hive-site.xml , krb5.conf , and user.keytab files. For details about how to obtain the certificate files, see How Do I Obtain the Hive Metastore Credential Files?
Big data - Data Lake Search (DLI)	AK/SK	Enter the AK/SK pair of the Huawei Cloud account. For details about how to obtain an AK/SK pair, see How Do I Obtain the AK/SK and Project ID?
Big Data - MaxCompute	AK/SK	Enter the AK/SK pair of the source Alibaba Cloud account. For details about how to obtain the key pair, see Viewing the Information About AccessKey Pairs of a RAM User .

Resource Type	Authentication Method	Description
Big data - Doris	Username/Password	Enter the username and password of the Doris database.
Big data - HBase	Username/Key	<ul style="list-style-type: none"> For an unsecured cluster, upload the core-site.xml, hdfs-site.xml, yarn-site.xml, mapred-site.xml, and hbase-site.xml files. For a secured cluster, upload seven files, including core-site.xml, hdfs-site.xml, yarn-site.xml, krb5.conf, user.keytab, mapred-site.xml, and hbase-site.xml. <p>The preceding configuration files are usually stored in the conf subdirectory of the Hadoop and HBase installation directories.</p>
Big data - ClickHouse	Username/Password	Enter the username and password of the ClickHouse database.
Windows server	Username/Password	<p>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.</p> <p>The value can be:</p> <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Username/Password Username/Key 	<ul style="list-style-type: none"> 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. <p>NOTICE If the key file is not encrypted, you do not need to enter the password.</p> <p>Then specify Network Range, which can be a single IP address or an IP address range. The value can be:</p> <ul style="list-style-type: none"> 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 .yaml file.

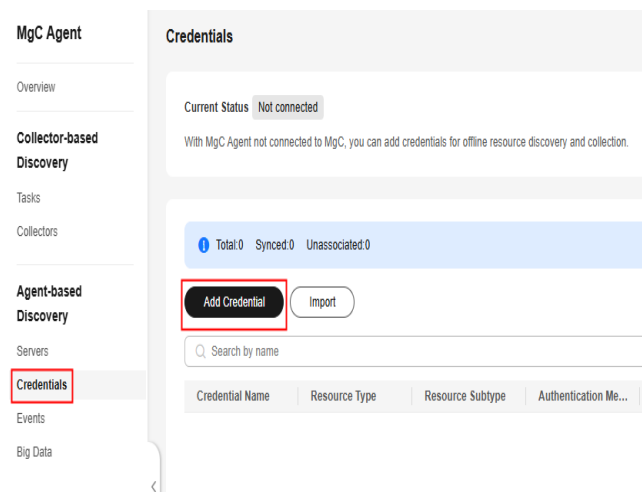
Adding Credentials

Step 1 Use the registered username and password to log in to the MgC Agent console.

Step 2 In the navigation pane, choose **Agent-based Discovery > Credentials**.

Step 3 Click **Create Certificate** above the list.

Figure 5-1 Adding a credential

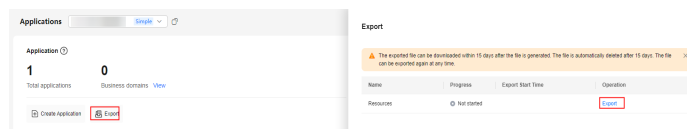


- Step 4** Select a resource type and authentication method as prompted. Specify a credential name, enter your credentials, and click **Confirm**.
- If the MgC Agent is not connected to MgC, the added resource credentials can be used for deep collection.
 - If the MgC Agent is connected to MgC, the added resource credentials will be automatically synchronized to MgC.
- End

Importing Credentials

- Step 1** On the MgC console, switch to the **Applications** page and export the discovered source servers and databases to a CSV file.

Figure 5-2 Exporting resource information



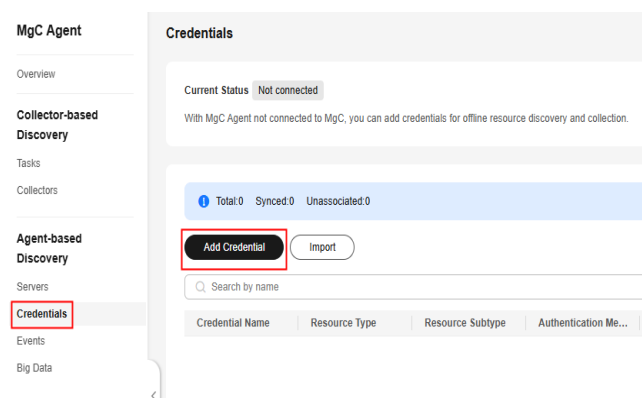
- Step 2** Open the exported CSV file, add columns **user_name** and **password** to the end, and enter the username and password for each resource. Save the file.



Ensure that the saved CSV file is correct and has no incorrect configuration or garbled characters.

- Step 3** On the **Credentials** page of the MgC Agent console, click **Import Credential** above the list.

Figure 5-3 Importing credentials



- Step 4** Click **Select File** to upload the saved CSV file.

NOTICE

- A maximum of 1,000 complete credential records can be imported at a time. If there are any blanks or incomplete credentials, they will be ignored.
- Credential names are automatically generated based on the resource name and access address.
- Credentials can be imported repeatedly, but they will be named differently.

Step 5 Click **OK** to complete the import. After the import is successful, the system automatically synchronizes the credentials to MgC and associate them with corresponding resources.

----End

Synchronizing Credentials

If the MgC Agent 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**.

5.2 Configuring an OBS Bucket

You can upload big data verification logs and content verification results to OBS for saving local storage and effectively managing and analyzing logs and results. After an OBS bucket is configured, the task logs and content verification results will be automatically uploaded to the specified OBS bucket.

Required Permissions

Ensure that the Huawei Cloud account that owns the added **credentials** have the following permissions for the log bucket:

- **obs:object:PutObject** (Uploading objects with PUT or POST, copying objects, appending content to objects, initiating a multipart upload, as well as uploading, copying, and assembling parts)
- **obs:bucket:ListAllMyBuckets** (Listing buckets)
- **obs:bucket:ListBucket** (Listing objects in a bucket)

For details about more permissions, see [Permissions Management](#).

Prerequisites

- You have [installed the MgC Agent](#) and registered an account.
- You have connected the MgC Agent to MgC. For details, see [Connecting the MgC Agent to MgC](#).

Procedure

Step 1 Use the registered username and password to log in to the MgC Agent console.

Step 2 In the navigation pane, choose **Agent-based Discovery > Big Data**.

Step 3 In the **Bucket Configuration** area, click **Configure**.

Step 4 Configure a log bucket by referring to [Table 5-2](#).

Table 5-2 Parameters for configuring a log bucket

Parameter	Configuration
Bucket Type	Two types are supported: Parallel File System and Bucket.
OBS Endpoint	Enter the endpoint of the region where the log bucket is located. For details, see Regions and Endpoints . Click Verify to obtain the bucket list.
Bucket	Select the desired bucket from the drop-down list.
(Optional) Folder	<p>Specify the folder for storing log files and content verification results in the bucket. The folder path must start with a slash (/). For example, if the bucket name is mgc01 and the folder name is /test, the log file path is obs://mgc01/test/bigdata/task/Date/Task execution ID/Log file. The content verification result path is obs://mgc01/test/bigdata/task/Task execution ID/Database name/Table name/Content verification result file.</p> <ul style="list-style-type: none"> • If you do not specify a folder, the system automatically creates a folder named bigdata in the bucket. <ul style="list-style-type: none"> – Log files are stored in obs://Bucket name/bigdata/task/Date/Task execution ID/Log file. – The path for storing the content verification result is obs://Bucket name/bigdata/task/Task execution ID/Database name/Table name/Content verification result file. • If the specified folder is not found, the system automatically creates the folder before uploading log files.

Step 5 Click **OK**.

NOTICE

Deleting the bucket configuration does not delete the bucket itself or the files stored in it, but you cannot use the log upload function of MgC.

----End

5.3 Managing MgC Agents

You can monitor and manage the MgC agents you connected to MgC on the MgC console.

Prerequisites

You have [installed the MgC Agent](#) in your source environment and [connected the MgC Agent to MgC](#).

View the MgC Agent List

- Step 1** Sign in to the [MgC console](#). In the navigation pane, under **Project**, choose your [project](#) from the drop-down list.
- Step 2** In the navigation pane, choose **MgC Agents** to view all MgC agents and their statuses in the current project.

For details about the MgC Agent statuses, see [Table 5-3](#).

Table 5-3 MgC Agent statuses

Status	Description
Online	The MgC Agent stays connected with the MgC console.
Offline	The MgC Agent is disconnected from the MgC console for at least one minute.
Error	The MgC Agent 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 MgC Agent

- Step 1** Click **Delete** in the **Operation** column.
- Step 2** Enter **DELETE** and click **OK** to confirm the deletion.

 **CAUTION**

MgC Agents that are executing data collection cannot be deleted.

----End

5.4 Event Recording

The MgC Agent (formerly Edge) offers comprehensive logging and event auditing. You can review operations, troubleshoot faults, and locate involved resources through the console and log files.

Overview

- **Logging:** Operations are logged in `<MgC-Agent-installation-directory>/logs/audit/audit.log`.
- **Event recording:** On the MgC Agent console, you can view event records, which include event details such as the event source, involved resources, key behaviors, operation time, and operation result.
- **Filtering and search:** You can filter event records by key behavior or search for event records by keyword.
- **Troubleshooting:** If an operation fails, you can review the logs to learn what the cause is.
- **Key operation and resource display::**
 - For key actions such as changing passwords or credentials, the resource field displays the involved account name or credential ID.
 - For key actions such as MgC delivering instructions to the MgC Agent or the MgC Agent reporting data to MgC, the resource field displays the path of the file that stores the instructions or data. You can find the file using the following path:
 - Instructions received from MgC: `<MgC-Agent-installation-directory>/logs/audit/downlink_command.txt`
 - Data reported to MgC: `<MgC-Agent-installation-directory>/logs/audit/uplink_data.txt`
- **Periodic log archiving:** The system automatically compresses the `audit.log` file into a .zip package at the beginning of each month and saves the package to the `<MgC-Agent-installation-directory>/logs/audit/` directory. The package name is in the format of year-month.zip, for example, **2024-xx.zip**.

6 Collector-based Discovery

6.1 Creating a Collection Task

The MgC Agent (formerly Edge) provides multiple types of collectors for 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 the MgC Agent](#) and registered an account.
- The required [collectors](#) have been installed.

Procedure

- Step 1** Use the registered username and password to log in to the MgC Agent console. In the navigation pane, 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

6.2 Managing Collectors

The MgC Agent (formerly Edge) installation package contains some collector installation packages. When the MgC Agent 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 the MgC Agent](#) and registered an account.

Offline Upgrade

Step 1 Use your username and password to log in to the MgC Agent console. In the navigation pane, choose **Collectors**.

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

Step 2 Sign in to the [MgC console](#), download the latest MgC Agent installation package and save it to the root directory of the MgC Agent 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, 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 MgC Agent 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 MgC Agent installation package on the **MgC Agents** 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, 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

6.3 Configuring Collector Parameters

6.3.1 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 6-1](#).

Table 6-1 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 <i><collector-installation-path>\output\file</i> . Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-k8s\output\file\app-discovery-k8s-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 <i><collector-installation-path>\config\rules.properties</i> . 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.

Parameter	Mandatory	Configuration
config_path	Yes	<p>Enter the absolute path of the folder that stores the configuration files (in YAML format) of clusters to be collected.</p> <p>CAUTION This storage path stores only YAML configuration files of clusters to be collected. Irrelevant YAML files should not be stored here.</p> <p>To obtain the content of a cluster's configuration file, perform the following steps:</p> <p>On a cluster node, run the following command, and copy the returned information to a YAML file.</p> <pre>cat ~/.kube/config</pre> <p>NOTICE Only one configuration file can be stored for a Kubernetes cluster.</p>

6.3.2 Kubernetes Contrack Collector (app-discovery-k8s-contrack)

The contrack utility is used to collect the application association topology of a Kubernetes cluster. For details about the configuration parameters, see [Table 6-2](#).

Table 6-2 Parameters for configuring the Kubernetes contrack collector

Parameter	Mandatory	Configuration
output_path	No	<p>Enter the storage path of the collection result file (app-discovery-k8s-contrack-xxx.csv). If this parameter is left blank, the storage path defaults to <i><collector-installation-path>\output\file</i>.</p> <p>Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-k8s-contrack\output\file\app-discovery-k8s-contrack-xxx.csv</p>
rules_path	No	<p>Enter the storage path of the collection rule file (a .properties file). If this parameter is left blank, the path defaults to <i><collector-installation-path>\config\rules.properties</i>.</p> <p>Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-k8s-contrack\config\rules.properties</p> <p>NOTICE You are advised to use the default rule file. If you need to customize collection rules, modify the default rule file.</p>

Parameter	Mandatory	Configuration
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	<p>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 <i><collector-installation-path>\config\nodes.csv</i>.</p> <p>Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-k8s-contrack\config\nodes.csv</p> <p>NOTICE You are advised to use the default access configuration file. If you need to customize access information, modify the default file.</p>

Parameter	Mandatory	Configuration
config_path	No	<p>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 <i><collector-installation-path>\config\kube-config\xxx.yaml</i>.</p> <p>Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-k8s-contrack\config\kube-config\xxx.yaml</p> <p>To obtain the content of a cluster's configuration file, perform the following steps:</p> <p>On a cluster node, run the following command, and copy the returned information to a YAML file.</p> <pre>cat ~/.kube/config</pre> <p>NOTICE Only one configuration file can be stored for a Kubernetes cluster.</p>

6.3.3 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 6-3](#).

Table 6-3 Parameters for configuring the Kubernetes pod network collector

Parameter	Mandatory	Configuration
output_path	No	<p>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 <i><collector-installation-path>\output\file</i>.</p> <p>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</p>

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

6.3.4 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 6-4](#).

Table 6-4 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 <i><collector-installation-path>\output\file</i> . 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 <i><collector-installation-path>\config\rules.properties</i> . 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	<ul style="list-style-type: none">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 <i><collector-installation-path>\config\nodes.csv</i>. Example: C:\Edge\tools\plugins\collectors\app-discovery-collectors\python\mgc-app-discovery-collectors\app-discovery-process-netstat\config\rules.propertiesIf 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. <p>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.</p>

6.3.5 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 6-5 Parameters for configuring the Windows process and network collector

Parameter	Mandatory	Configuration
host_path	Yes	<p>Enter the path to the CSV file that contains Windows server authorization information, for example, D:\nodes.csv.</p> <p>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.</p> <ul style="list-style-type: none"> • IP(REQUIRED) • PORT(REQUIRED) • USER(REQUIRED) • PASSWORD(SENSITIVE) • PRI_KEY_PATH(SENS_PATH) • CLUSTER • APPLICATION • BUSINESS_DOMAIN • PASSWORD(ENCRYPTED) • PRI_KEY_PATH(ENCRYPTED) <p>CAUTION The provided accounts (username and password) must have the permission to run the netstat command on the server.</p>
app_only	No	<p>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.</p> <p>CAUTION If this parameter is set to false, the time parameter is mandatory.</p>
time	No This parameter is mandatory when app_only is set to false .	<p>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.</p>

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 <i><collector-installation-path>\output\file</i> . 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

6.3.6 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 6-6](#).

Table 6-6 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 <i><collector-installation-path>\output\file</i> . 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 .

6.3.7 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 6-7](#).

Table 6-7 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 <i><collector-installation-path>\output\file</i> . 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. <ul style="list-style-type: none">• 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.

6.3.8 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 6-8](#).

Table 6-8 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 <i><collector-installation-path>\output\file</i> . 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: <i>http://IP address 1:Port 1,http://IP address 2:Port2</i> <ul style="list-style-type: none">• If user authentication is enabled, add the <i>Username@</i> before <i>IP address:Port</i>. Example: <i>http://Username@IP address 1:Port 1,http://Username@IP address 2:Port2</i>• If HTTPS authentication is enabled, change http:// to https://.

6.3.9 Redis Collector (app-discovery-redis)

This collector connects to a Redis node to obtain its IP address, version, and IP addresses of connected clients. For details about the configuration parameters, see [Table 6-9](#).

Table 6-9 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 <i><collector-installation-path>\output\file</i> . 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. <ul style="list-style-type: none"> • 0: single-node • 1: cluster
auth	Yes	Specify the Redis authentication method. <ul style="list-style-type: none"> • 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.

6.3.10 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 6-10](#).

Table 6-10 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 <i><collector-installation-path>\output\file</i> . 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	Man dator y	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.

6.3.11 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 6-11](#).

Table 6-11 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 <i><collector-installation-path>\output\file</i> . 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: <ol style="list-style-type: none">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.Run the following command to restart the MySQL service: net stop mysql net start mysql

6.3.12 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 6-12](#).

Table 6-12 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 <i><collector-installation-path>\output\file</i> . 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 <i>Parameter name 1,Parameter value 1,Parameter name 2,Parameter value 2</i> . For details about the parameters, see Table 6-13 . 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: <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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 : <code>SELECT * FROM mysql.user</code>
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 6-13 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.

6.3.13 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 6-14](#).

Table 6-14 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 <i><collector-installation-path>\output\file</i> . 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.

6.3.14 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 6-15](#).

Table 6-15 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 <i><collector-installation-path>\output\file</i> . 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.

6.3.15 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 6-16](#).

Table 6-16 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 <i><collector-installation-path>\output\file</i> . 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 <i><collector-installation-path>\config\rules.properties</i> . 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.

6.3.16 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 6-17](#).

Table 6-17 Parameters for configuring the application configuration collector

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

7 Best Practices

7.1 Setting JVM Parameters for the MgC Agent (Formerly Edge)

7.1.1 Setting JVM Parameters for the MgC Agent's Tomcat Server

Windows

The following procedure uses Windows 11 as an example.

Step 1 Navigate to the location of the startup script.

Go to the MgC Agent installation directory (**C:\Edge** by default) and find **.\tools\SecAs-1.2.29\bin\startup.bat**.

Step 2 Set the JVM parameters.

1. In the MgC Agent installation directory (**C:\Edge** by default), edit **.\tools\SecAs-1.2.29\bin\catalina.bat**.

2. Add the following information below **@echo off** in the file:
set "JAVA_OPTS=-Xms512M -Xmx1024M"

In the preceding information, **-Xms512M -Xmx1024M** are the JVM parameters to be configured. **-Xms512M** indicates that the initial heap memory allocated to the JVM is 512 MB. **-Xmx1024M** indicates that the maximum heap memory that can be allocated to the JVM is 1,024 MB. You can add other JVM parameters as required.

```

1  @echo on
2  set "JAVA_OPTS=-Xms512M -Xmx1024M"
3  rem Licensed to the Apache Software Foundation (ASF) under one or more
4  rem contributor license agreements. See the NOTICE file distributed with
5  rem this work for additional information regarding copyright ownership.
6  rem The ASF licenses this file to You under the Apache License, Version 2.0
7  rem (the "License"); you may not use this file except in compliance with
8  rem the License. You may obtain a copy of the License at
9  rem
10 rem http://www.apache.org/licenses/LICENSE-2.0
11 rem
12 rem Unless required by applicable law or agreed to in writing, software
13 rem distributed under the License is distributed on an "AS IS" BASIS,
14 rem WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
15 rem See the License for the specific language governing permissions and

```

3. Save and exit **catalina.bat**. The JVM parameters are configured for the Edge Tomcat server.

⚠ CAUTION

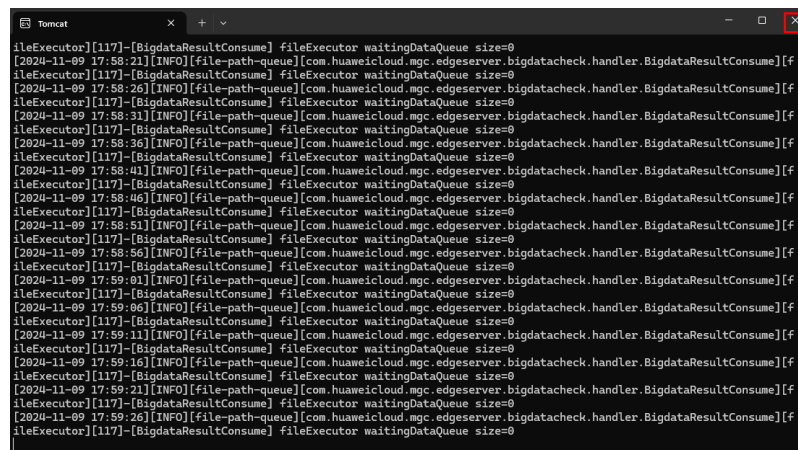
This configuration will be applied if the MgC Agent is started using the startup script. It will not be applied if the MgC Agent is automatically started upon system or service startup.

Step 3 Restart the Edge Tomcat server.

If the MgC Agent is running, stop Tomcat and the pre-installed collectors. After that, restart the MgC Agent.

- Stop the MgC Agent's Tomcat server.
 1. If the MgC Agent is automatically started upon system startup or service startup, perform the following steps:
 - a. Press **Ctrl, Alt,** and **Delete** and select **Task Manager** on the displayed page to open it. In the **Task Manager** dialog box, choose the **Details** tab.
 - b. Select **tomcat9.exe** and click **End Task**.
 2. If the MgC Agent is started using the startup script, close the **command prompt** window that appears during the script execution.

Figure 7-1 Command prompt



- Stop the collectors.

1. Stop the collectors using the task manager.
 - a. Press **Ctrl, Alt,** and **Delete** and select **Task Manager** on the displayed page to open it. In the **Task Manager** dialog box, choose the **Details** tab.
 - b. Select **rda-storage-collector.exe, rda-collector-server.exe, rda-collector-platform.exe, rda-collector-kubernetes.exe,** and **rda-collector-database.exe** individually and click **End Task**.
 2. Run a script to stop a single collector. **rda-storage-collector** is used as an example.
 - a. Go to the MgC Agent installation directory, find the collector's directory (**C:\Edge\tools\plugins\collectors\rda-storage-collector\bin\stop.bat** by default), and run **stop.bat**.
 - b. Find and stop the other collectors in the **.\tools\plugins\collectors** directory.
- Restart the MgC Agent.

Go to the MgC Agent installation directory (**C:\Edge** by default) and run **.\tools\SecAs-1.2.29\bin\startup.bat**. the MgC Agent's Tomcat server and the pre-installed collectors are restarted.

Step 4 Query the JVM parameters of the MgC Agent's Tomcat server.

⚠ CAUTION

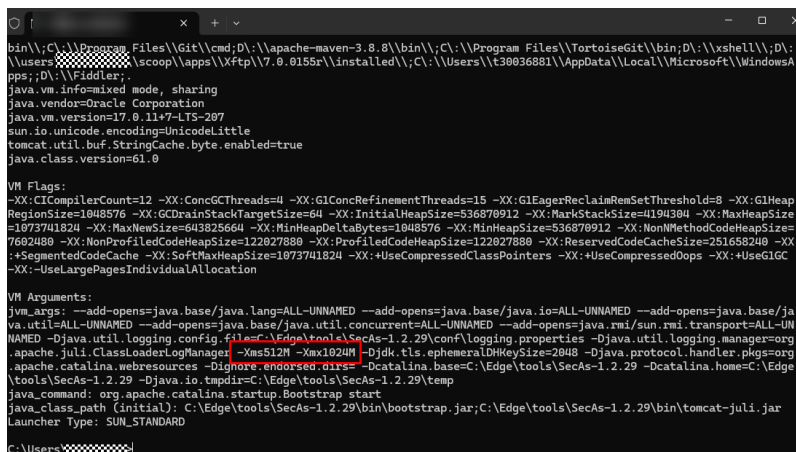
This step requires that the Java development environment be installed on Windows.

1. Press **Ctrl, Alt,** and **Delete** and select **Task Manager** on the displayed page to open it. In the **Task Manager** dialog box, choose the **Details** tab.
2. The following steps depend on how the MgC Agent is started.
 - a. If the MgC Agent is automatically started upon system startup or service startup, find **tomcat9.exe** in **Task Manager** and check the corresponding PID.
 - b. If the MgC Agent is started using the startup script, search for the **java.exe** program and check the corresponding PID. If there are multiple **java.exe** programs, do as follows:
 - i. After querying the JVM settings of a Java program, you can determine whether the program is the MgC Agent program based on the value of **java_class_path** in the command output. If the **MgC Agent** and **tomcat** fields are contained, it is the MgC Agent program.
 - ii. After obtaining the PID, open **Command Prompt** as the administrator, enter the following command, and press **Enter**:

```
jinfo <PID>
```

In the preceding command, **PID** indicates the PID of the MgC Agent program. You can view the effective JVM parameters in the command output.

Figure 7-2 Command prompt



```
bin\;C:\Program Files\Git\cmd;D:\apache-maven-3.8.8\bin\;C:\Program Files\TortoiseGit\bin;D:\xshell\;D:\
\Users\XXXXXX\scoop\apps\Xftp\17.0.0155r\installed\;C:\Users\{t30936881\AppData\Local\Microsoft\WindowsA
pps;D:\Viddler;
java.vendor=Oracle Corporation
java.vm.version=17.0.11+7-LTS-207
sun.io.unicode.encoding=UnicodeLittle
tomcat.util.buf.StringCache.byte.enabled=true
java.class.version=61.0

VM Flags:
-XX:CICompilerCount=12 -XX:ConcGCThreads=4 -XX:G1ConcRefinementThreads=15 -XX:G1EagerReclaimRemSetThreshold=8 -XX:G1Heap
RegionSize=1048576 -XX:GCDrainStackTargetSize=64 -XX:InitialHeapSize=536870912 -XX:MarkStackSize=4194384 -XX:MaxHeapSize
=1073741824 -XX:MaxNewSize=643825664 -XX:MinHeapDeltaBytes=1048576 -XX:MinHeapSize=536870912 -XX:NonMethodCodeHeapSize=
7602480 -XX:NonProfiledCodeHeapSize=122027880 -XX:ProfiledCodeHeapSize=122027880 -XX:ReservedCodeCacheSize=251658240 -XX
:+SegmentedCodeCache -XX:SoftMaxHeapSize=1073741824 -XX:+UseCompressedClassPointers -XX:+UseCompressedOops -XX:+UseG1GC
-XX:-UseLargePagesIndividualAllocation

VM Arguments:
jvm_args: --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/java.io=ALL-UNNAMED --add-opens=java.base/ja
va.util=ALL-UNNAMED --add-opens=java.base/java.util.concurrent=ALL-UNNAMED --add-opens=java.rmi/sun.rmi.transport=ALL-UN
NAMED -Djava.util.logging.config.file=C:\Edge\tools\SecAs-1.2.29\conf\logging.properties -Djava.util.logging.manager=org
.apache.juli.ClassLoaderLogManager -Xms512M -Xmx1024M -Djdk.tls.ephemeralDHKeySize=2048 -Djava.protocol.handler.pkgs=org
.apache.catalina.webresources -Dignore.endorsed.dirs=-Dcatalina.base=C:\Edge\tools\SecAs-1.2.29 -Dcatalina.home=C:\Edge
\tools\SecAs-1.2.29 -Djava.io.tmpdir=C:\Edge\tools\SecAs-1.2.29\temp
java_command: org.apache.catalina.startup.Bootstrap start
java_class_path (initial): C:\Edge\tools\SecAs-1.2.29\bin\bootstrap.jar;C:\Edge\tools\SecAs-1.2.29\bin\tomcat-juli.jar
Launcher Type: SUN_STANDARD

C:\Users\XXXXXX\
```

----End

Linux

The following uses CentOS 8 as an example.

Step 1 Navigate to the location of the startup script.

Go to the MgC Agent installation directory (`/opt/cloud/Edge` by default) and find `./scripts/start.sh`.

Step 2 Set the JVM parameters.

1. In the MgC Agent installation directory (`/opt/cloud/Edge` by default), edit `/tools/SecAs-1.2.29/bin/catalina.sh`.
2. Add the following information at the beginning of the file:
JAVA_OPTS="-Xms512M -Xmx1024M"

In the preceding information, `-Xms512M -Xmx1024M` are the JVM parameters to be configured. `-Xms512M` indicates that the initial heap memory allocated to the JVM is 512 MB. `-Xmx1024M` indicates that the maximum heap memory that can be allocated to the JVM is 1,024 MB. You can add other JVM parameters as required.

```
1 JAVA_OPTS="-Xms512M -Xmx1024M"
2 #!/bin/sh
3
4 # Licensed to the Apache Software Foundation (ASF) under one or more
5 # contributor license agreements. See the NOTICE file distributed with
6 # this work for additional information regarding copyright ownership.
7 # The ASF licenses this file to You under the Apache License, Version 2.0
8 # (the "License"); you may not use this file except in compliance with
9 # the License. You may obtain a copy of the License at
10 #
11 # http://www.apache.org/licenses/LICENSE-2.0
12 #
13 # Unless required by applicable law or agreed to in writing, software
14 # distributed under the License is distributed on an "AS IS" BASIS,
15 # WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
16 # See the License for the specific language governing permissions and
17 # limitations under the License.
18
19 # -----
20 # Control Script for the CATALINA Server
21 #
22 # For supported commands call "catalina.sh help" or see the usage section at
23 # the end of this file.
24 #
25 # Environment Variable Prerequisites
26 #
27 # Do not set the variables in this script. Instead put them into a script
```

3. Save and exit `catalina.bat`. The JVM parameters are configured for the Edge Tomcat server.

Step 3 Restart the Edge Tomcat server.

If the MgC Agent is running, stop Tomcat and the pre-installed collectors.

1. Go to the `.\script` directory in the MgC Agent installation directory (`/opt/cloud/Edge` by default).
2. Run the following command to stop the MgC Agent:
sh stop.sh
3. Run the following command to start the MgC Agent:
sh start.sh

Step 4 Query the JVM parameters of the MgC Agent's Tomcat server.

Run the `ps -ef|grep java` command to check the JVM parameters when the MgC Agent is running.

```
ps -ef|grep java
jre  68952   1  0 11:08          0:00 java -Djava.util.logging.config.file=/opt/cloud/Edge/tools/sec6e-1.2.20/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djdk.reflect.useDirectMethodAccess -Djava.awt.headless=true -Djdk.random=data -Dcom.huawei.log.file=/opt/cloud/Edge/tools/sec6e-1.2.20/log/manager.log java -jar /opt/cloud/Edge/tools/sec6e-1.2.20/bin/tomcat-juli.jar Catalina.base=/opt/cloud/Edge/tools/sec6e-1.2.20 Catalina.home=/opt/cloud/Edge/tools/sec6e-1.2.20 -Djava.io.tmpdir=/opt/cloud/Edge/tools/sec6e-1.2.20/tem

jre  68790   1  0 11:08          0:00 java -jar rda-collector-platform-1.1.17.jar

jre  68790   1  0 11:08          0:00 java -jar rda-collector-kubernetes.jar

jre  68790   1  0 11:08          0:00 java -jar rda-collector-jdbc.jar

jre  68790   1  0 11:08          0:00 java -Djava.util.logging.config.file=/opt/cloud/Edge/tools/sec6e-1.2.20/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djdk.reflect.useDirectMethodAccess -Djava.awt.headless=true -Djdk.random=data -Dcom.huawei.log.file=/opt/cloud/Edge/tools/sec6e-1.2.20/log/manager.log java -jar /opt/cloud/Edge/tools/sec6e-1.2.20/bin/tomcat-juli.jar Catalina.base=/opt/cloud/Edge/tools/sec6e-1.2.20 Catalina.home=/opt/cloud/Edge/tools/sec6e-1.2.20 -Djava.io.tmpdir=/opt/cloud/Edge/tools/sec6e-1.2.20/tem

root 68228 68100  31 11:49  0:00 java -jar /usr/share/migrate/migrate-agent.jar --log-dir /opt/cloud/Edge/tools/sec6e-1.2.20/conf --log-file /opt/cloud/Edge/tools/sec6e-1.2.20/log/manager.log

root 68228 68100  31 11:48  0:00 java -jar /usr/share/migrate/migrate-agent.jar --log-dir /opt/cloud/Edge/tools/sec6e-1.2.20/conf --log-file /opt/cloud/Edge/tools/sec6e-1.2.20/log/manager.log
```

----End

7.1.2 Setting JVM Parameters for Collectors

Windows

The following procedure uses Windows 11 and `rda-collector-server` as an example.

Step 1 Navigate to the location of the startup script.

Go to the MgC Agent installation directory (`C:\Edge` by default) and find `.\tools\plugins\collectors\rda-collector-server\bin\start.bat`. `rda-collector-server` can be replaced with the collector you want to configure. The supported collectors include:

- Database collector `rda-collector-database`
- Container collector `rda-collector-kubernetes`
- Platform collector `rda-collector-platform`
- Server collector `rda-collector-server`
- Storage collector `rda-storage-collector`

Step 2 Set the JVM parameters.

1. In the MgC Agent installation directory (`C:\Edge` by default), edit `.\tools\plugins\collectors\rda-collector-server\bin\start.bat`.
2. Add the following JVM parameters after `-jar` in the second statement.
-Xms512M -Xmx1024M

In the preceding information, `-Xms512M -Xmx1024M` are the JVM parameters to be configured. `-Xms512M` indicates that the initial heap memory allocated to the JVM is 512 MB. `-Xmx1024M` indicates that the maximum heap memory that can be allocated to the JVM is 1,024 MB. You can add other JVM parameters as required.

```
1 @echo off
2 copy "%RDA_JRE_HOME%\bin\javaw.exe" "%RDA_JRE_HOME%\bin\rda-collector-database.exe" /y
3 start %RDA_JRE_HOME%\bin\rda-collector-database -jar: "-Xms512M -Xmx1024M" ../rda-collector-database.jar
```

3. Save and exit **start.bat**. The JVM parameters are configured for the server collector.

Step 3 Restart the collector.

The JVM parameters will be applied after the collector is restarted.

1. Go to the MgC Agent installation directory (**C:\Edge** by default) and run **.\tools\plugins\collectors\rda-collector-server\bin\stop.bat** as the administrator.
2. Run the collector startup script **start.bat** in the same directory.

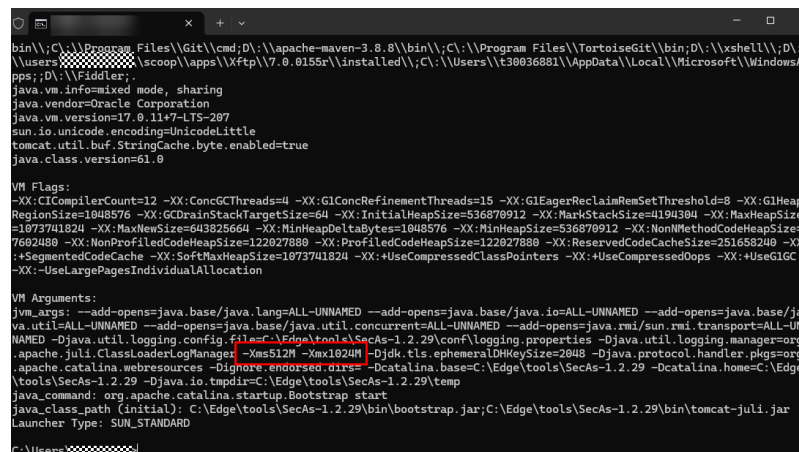
Step 4 Query the JVM parameters of the collector.

1. Press **Ctrl, Alt,** and **Delete** and select **Task Manager** on the displayed page to open it. In the **Task Manager** dialog box, choose the **Details** tab.
2. Find **rda-collector-server.exe** and check its PID.
3. Open **Command Prompt** as the administrator, enter the following command, and press **Enter**:

```
jinfo PID
```

In the preceding command, **PID** indicates the PID of the MgC Agent program. You can view the effective JVM parameters in the command output.

Figure 7-3 Command prompt



```
bin\;C:\Program Files\Git\cmd;D:\apache-maven-3.8.8\bin\;C:\Program Files\TortoiseGit\bin;D:\xshell\;D:\Users\y\OneDrive\apps\Xftp\7.0.0155r\installed\;C:\Users\t30036801\AppData\Local\Microsoft\WindowsApps;D:\Fiddler;
java.vm.info=mixed mode, sharing
java.vendor=Oracle Corporation
java.vm.version=17.0.11+7-LTS-207
sun.io.unicode.encoding=UnicodeLittle
tomcat.util.buf.StringCache.byte.enabled=true
java.class.version=61.0

VM Flags:
-XX:CICompilerCount=12 -XX:ConcGCThreads=4 -XX:G1ConcRefinementThreads=15 -XX:G1EagerReclaimRemSetThreshold=8 -XX:G1HeapRegionSize=1048576 -XX:GCDrainStackTargetSize=64 -XX:InitialHeapSize=536870912 -XX:MarkStackSize=4194304 -XX:MaxHeapSize=1073741824 -XX:MaxNewSize=643825664 -XX:MinHeapDeltaBytes=1048576 -XX:MinHeapSize=536870912 -XX:NonMethodCodeHeapSize=7602480 -XX:NonProfiledCodeHeapSize=122027880 -XX:ProfiledCodeHeapSize=122027880 -XX:ReservedCodeCacheSize=251658240 -XX:+SegmentedCodeCache -XX:SoftMaxHeapSize=1073741824 -XX:+UseCompressedClassPointers -XX:+UseCompressedOops -XX:+UseG1C -XX:-UseLargePagesIndividualAllocation

VM Arguments:
jvm_args: --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/java.io=ALL-UNNAMED --add-opens=java.base/java.util=ALL-UNNAMED --add-opens=java.base/java.util.concurrent=ALL-UNNAMED --add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED -Djava.util.logging.config.file=C:\Edge\tools\SecAs-1.2.29\conf\logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Xms512M -Xmx1024M -Djdk.tls.ephemeralDHKeySize=2048 -Djava.protocol.handler.pkgs=org.apache.catalina.webresources -Dignore.endorsed.dirs=-Dcatalina.base=C:\Edge\tools\SecAs-1.2.29 -Dcatalina.home=C:\Edge\tools\SecAs-1.2.29 -Djava.io.tmpdir=C:\Edge\tools\SecAs-1.2.29\temp
java_command: org.apache.catalina.startup.Bootstrap start
java_class_path (initial): C:\Edge\tools\SecAs-1.2.29\bin\bootstrap.jar;C:\Edge\tools\SecAs-1.2.29\bin\tomcat-juli.jar
Launcher Type: SUN_STANDARD
C:\Users\y\OneDrive\apps\Xftp\7.0.0155r\installed\;C:\Users\t30036801\AppData\Local\Microsoft\WindowsApps;D:\Fiddler;
```

----End

Linux

The following procedure uses CentOS 8 and **rda-collector-server** as an example.

Step 1 Navigate to the location of the startup script.

Go to the MgC Agent installation directory. The default directory is **/opt/cloud/Edge**. Find **/tools/plugins/collectors/rda-collector-server**. **rda-collector-server** can be replaced with the collector you want to configure. The supported collectors include:

Database collector **rda-collector-database**

Container collector **rda-collector-kubernetes**

8 FAQs

8.1 What Are the Requirements for the Server for Installing the MgC Agent (Formerly Edge)?

Windows Installation Requirements

The Windows server for installing the MgC Agent must:

- Be able to access the Internet and the domain names of MgC, IoTDA, and other cloud services. For details about the domain names to be accessed, see [Domain Names](#).
- Allow the ports required by the MgC Agent (formerly Edge). For details about the required ports, see [Communication Matrix](#).
- Use PowerShell **3.0** 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.
- Not have any antivirus or protection software enabled. This type of software may stop the MgC Agent from executing migration commands, resulting in migration failures.

 **CAUTION**

Do not install the MgC Agent on a source server to be migrated.

- **High resource consumption:** The MgC Agent consumes CPU and memory resources during collection and migration. If a large number of migration tasks are performed by the MgC Agent, services on the source server may be affected.
 - **Port occupation:** The MgC Agent occupies some ports on the server, which may affect services running on it.
-

Linux Installation Requirements

The Linux server for installing the MgC Agent must:

- Be able to access the Internet and the domain names of MgC, IoTDA, and other cloud services. For details about the domain names to be accessed, see [Domain Names](#).
- Allow the ports required by the MgC Agent (formerly Edge). For details about the required ports, see [Communication Matrix](#).
- Allow outbound traffic on 8883 if the server is in a security group.
- Run CentOS 8.X.
- Have at least 4 CPUs and 8 GB of memory. If you want to use big data verification, the server must have at least 8 CPUs and 16 GB of memory.

 **CAUTION**

Do not install the MgC Agent on a source server to be migrated.

- **High resource consumption:** The MgC Agent consumes CPU and memory resources during collection and migration. If a large number of migration tasks are performed by the MgC Agent, services on the source server may be affected.
 - **Port occupation:** The MgC Agent occupies some ports on the server, which may affect services running on it.
-

8.2 How Do I Run the MgC Agent in Compatibility Mode?

Step 1 Right-click the MgC Agent (formerly 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 MgC Agent installation program.

----End

8.3 What Can I Do If the MgC Agent (Formerly Edge) Is Offline?

You can perform the following operations:

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

8.4 Why Can't the MgC Agent (Formerly Edge) Start After Being Installed?

8.4.1 MgC Agent for Windows

Symptom

After the MgC Agent for Windows was installed, the registration page could not show up.

Possible Causes

On the server where the MgC Agent was installed, there were too many background processes or the available CPUs were too small to run the MgC Agent.

Solution

Perform the following steps to manually start the MgC Agent:

1. Open the task manager of the server where the MgC Agent was installed.
2. Click the **Services** tab, right-click **Edge_Tomcat**, and choose **Start** from the shortcut menu.
3. After the MgC Agent is started, go to the registration page.

8.4.2 MgC Agent for Linux

Symptom

After the MgC Agent for Linux was installed, it could not start.

Possible Causes

On the server where the MgC Agent was installed, there were too many background processes or the available CPUs were too small to run the MgC Agent.

Solution

Perform the following steps to manually start the MgC Agent:

- Step 1** Go to the **scripts** directory in the MgC Agent installation directory.

```
cd /opt/cloud/Edge/scripts/
```

- Step 2** Run the following commands to start the MgC Agent:

```
./start.sh
```

If the following information is displayed, the MgC Agent is started.

```
server not started yet.
Using CATALINA_BASE:   /opt/cloud/Edge/tools/SecAs-1.2.29
Using CATALINA_HOME:   /opt/cloud/Edge/tools/SecAs-1.2.29
Using CATALINA_TMPDIR: /opt/cloud/Edge/tools/SecAs-1.2.29/temp
Using JRE_HOME:        /opt/cloud/Edge/tools/jre
Using CLASSPATH:       /opt/cloud/Edge/tools/SecAs-1.2.29/bin/bootstrap.jar:/opt/cloud/Edge/tools/SecAs-1.2.29/bin/tomcat-juli.jar
Tomcat started.
```


- Step 2** In the navigation pane, choose **MgC Agents**.
- Step 3** In the Linux area, click **Download Installation Package** or **Copy Download Command** to download the MgC Agent installation program to the Linux server.
- Step 4** Install the latest version of the MgC Agent. For details, see [Installing the MgC Agent for Linux](#).
- End

8.6 How Do I Uninstall the MgC Agent (Formerly Edge)?

8.6.1 Uninstalling the MgC Agent for Windows

The uninstallation method depends on the Windows OS version.



You need to uninstall the MgC Agent application and MSI installer.

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 find the installed the MgC Agent 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** and **I** to open **Windows Settings**, and then click **Applications**.
- Step 2** Enter **Edge** in the search box to find the installed the MgC Agent software. Click the software name and click **Uninstall** in the lower right corner to uninstall the software.
- End

8.6.2 Uninstalling the MgC Agent for Linux

The following describes how to uninstall the MgC Agent for Linux.

Procedure

Step 1 Go to the **scripts** directory in the MgC Agent installation directory.

```
cd /opt/cloud/Edge/scripts/
```

Step 2 Run the MgC Agent uninstallation script.

```
./uninstall.sh
```

If the information shown in the following figure is displayed, the environment variables of the MgC Agent for Linux need to be updated.

```
variables not available yet, please run command `source /etc/profile` first
```

Step 3 Update environment variables.

```
source /etc/profile
```

Step 4 Run the MgC Agent uninstallation script.

```
./uninstall.sh
```

Check if the message shown in the following figure is displayed. If it is, the MgC Agent for Linux has been uninstalled.

```
try to stop all collectors
please wait for collectors stopping...
Removed /etc/systemd/system/multi-user.target.wants/Edge-start.service.
clear profiles
groupdel: group 'edge' does not exist
```

----End

8.7 How Do I Restart the MgC Agent (Formerly Edge)?

MgC Agent for Windows

1. Open the task manager of the server where the MgC Agent was installed.
2. Click the **Services** tab, right-click **Edge_Tomcat**, and choose **Start** from the shortcut menu.

MgC Agent for Linux

Step 1 Go to the **scripts** directory in the MgC Agent installation directory.

```
cd /opt/cloud/Edge/scripts/
```

Step 2 Run the following commands to start the MgC Agent:

```
./start.sh
```

If the following information is displayed, the MgC Agent is started.

```
server not started yet.
Using CATALINA_BASE: /opt/cloud/Edge/tools/SecAs-1.2.29
Using CATALINA_HOME: /opt/cloud/Edge/tools/SecAs-1.2.29
Using CATALINA_TMPDIR: /opt/cloud/Edge/tools/SecAs-1.2.29/temp
Using JRE_HOME: /opt/cloud/Edge/tools/jre
Using CLASSPATH: /opt/cloud/Edge/tools/SecAs-1.2.29/bootstrap.jar:/opt/cloud/Edge/tools/SecAs-1.2.29/bin/tomcat-juli.jar
Using CATALINA_OPTS:
Tomcat started.
```

Step 3 Run the following command to view the MgC Agent process:

```
ps -ef |grep edge
```

If the following information is displayed, the MgC Agent process is started.

Log File	Description
debug.log	Debug logs recording the running of the MgC Agent.
error.log	Error logs generated when the MgC Agent is running.
operation.log	Operation logs recording interactions between users and the interface.
plugins.log	IoTDA logs, which record the messages exchanged between the MgC Agent and MgC through IoTDA.
run.log	All logs generated during the running of the MgC Agent.
warn.log	Alarm logs generated during the running of the MgC Agent.
user.log	User audit logs.

Step 3 If the log file has been archived, perform the following steps to view the archived log file:

1. Run the **cd** command to access the archived log directory. Replace `<xxx/>` with the actual archived log directory.

```
cd <xxx/>
```
2. Run the **gunzip** command to decompress the archived log file. For example, if the name of an archived log file is **archived_log.gz**, you can run **gunzip archived_log.gz** to decompress the file.

----End

Viewing Logs of the Big Data Plug-in

Step 1 Go to the log directory in the MgC Agent installation directory. This directory contains various log files generated during the running of the big data plug-in.

```
cd /opt/cloud/Edge/tools/plugins/collectors/bigdata-migration/logs
```

Step 2 Run the **vi** command to view a specific log file.

```
vi <xxx.log>
```

Replace `<xxx.log>` with the log file you want to view. The following table lists the names and descriptions of different types of log files.

Log File	Description
debug.log	Debug logs generated during the running of the big data plug-in.
error.log	Error logs generated during the running of the big data plug-in.
run.log	All logs generated during the running of the big data plug-in.

Log File	Description
warn.log	Alarm logs generated during the running of the big data plug-in.
rda_run.log	Recording the plug-in startup command.
api.log/user.log	Deprecated. No content is recorded.

Step 3 If the log file has been archived, perform the following steps to view the archived log file:

1. Run the **cd** command to access the archived log directory. Replace `<xxx/>` with the actual archived log directory.

```
cd <xxx/>
```
2. Run the **gunzip** command to decompress the archived log file. For example, if the name of an archived log file is **archived_log.gz**, you can run **gunzip archived_log.gz** to decompress the file.

----End

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

Symptom

After the MgC Agent and resource credential were associated, the deep collection failed, and the failure cause was "The collector is not installed."

Possible Causes

Possible causes are:

- The MgC Agent server's capacity is too small to run the collector. The recommended specifications are 4 vCPUs and 8 GB of memory.
- The collector was offline even though the MgC Agent server's capacity was sufficient.


Solutions

- **The MgC Agent server's capacity is too small.**
Upgrade the MgC Agent server's specifications or install the MgC Agent on a server with a larger capacity. Then perform a deep collection again.
- **The collector was offline.**
The following table lists the collectors integrated in the MgC Agent. The server collector is used as an example to explain the method, which applies to other collectors as well.

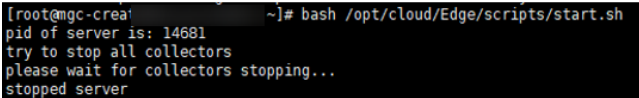
Collector	Collected Resource	Process	Installation Directory
rda-collector-platform	VMware-based private cloud platforms	rda-collector-platform.exe	<installation-path> \Edge\tools\plugins\collectors
rda-collector-server	Server	rda-collector-server.exe	
rda-collector-kubernetes	Container	rda-collector-kubernetes.exe	

- **Restarting the Windows collector**
 - i. Go to the **bin** directory in the collector installation directory on the MgC Agent server, for example, **C:\Edge\tools\plugins\collectors\rda-collector-server\bin**.
 - ii. Double-click **start.bat** to start the server collector.
 - iii. Open Task Manager. On the details page, check the status of **rda-collector-server.exe**. If the status is **Running**, the collector is started.
 - iv. Return to the MgC console, locate the source resource, and click **Collect Again** in the **Deep Collection** column to collect the resource information again.
- **Restarting the Linux collector**
 - i. Log in to the MgC console and check if the MgC Agent is executing any deep collection, intranet scanning, or VMware VM discovery tasks. If it is, perform subsequent operations after the tasks are complete.
 - ii. Log in to the Linux server where the MgC Agent is installed.
 - iii. Apply environment variables.

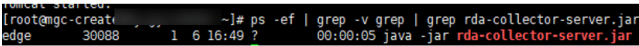
```
source /etc/profile
```


 - iv. Restart the MgC Agent.

```
bash /opt/cloud/Edge/scripts/start.sh
```


 - v. Check whether the collector process runs properly.

```
ps -ef | grep -v grep | grep rda-collector-server
```


 - vi. Return to the MgC console, locate the source resource, and click **Collect Again** in the **Deep Collection** column to collect the resource information again.

8.11 How Do I Obtain the Hive Metastore Credential Files?

- Step 1** Log in to FusionInsight Manager by referring to [Accessing FusionInsight Manager](#) and go to the **System** page.
- Step 2** In the navigation pane on the left, choose **Permission > User**.
- Step 3** In the user list, locate the user whose credential needs to be added to the MgC Agent (formerly Edge) and choose **More > Download Authentication Credential** in the **Operation** column. You can obtain the **krb5.conf** and **user.keytab** files in the credential file.

 **CAUTION**

When adding a credential on the MgC Agent, ensure that the entered username is paired with the credentials downloaded here.

- Step 4** On the menu bar, choose **Cluster > Hive**. On the **Hive** overview page that is displayed, choose **More > Download Client** in the upper right corner.
 - Step 5** Set **Select Client Type** to **Configuration Files Only** and click **OK**.
 - Step 6** Decompress the downloaded package to obtain the **core-site.xml**, **hivemetastore-site.xml**, and **hive-site.xml** credential files in the **/Hive/config** folder.
- End

8.12 What Can I Do If the Port Required by the MgC Agent Is Occupied and the Installation Fails?

Symptom

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

Possible Causes

The default port 27080 for installing the MgC Agent 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 the MgC Agent.

```
kill -9 11083
```

----End

Windows

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

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

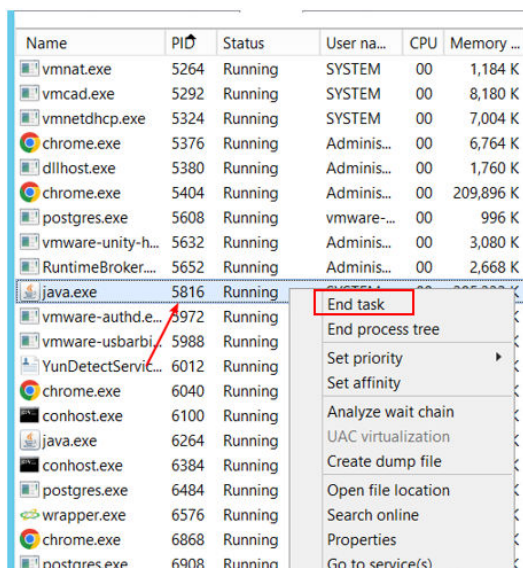
Assume that the queried application ID is 5816. The application ID is only an example. Replace it with the actual query result.

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>netstat -ano | findstr 7080
TCP        0.0.0.0:7080          0.0.0.0:0          LISTENING      5816
TCP        [::]:7080          [::]:0             LISTENING      5816
TCP        [::1]:7080          [::1]:59011        TIME_WAIT      0
TCP        [::1]:7080          [::1]:59057        TIME_WAIT      0
TCP        [::1]:7080          [::1]:59103        TIME_WAIT      0
TCP        [::1]:59027        [::1]:7080         TIME_WAIT      0
TCP        [::1]:59032        [::1]:7080         TIME_WAIT      0
TCP        [::1]:59077        [::1]:7080         TIME_WAIT      0
TCP        [::1]:59080        [::1]:7080         TIME_WAIT      0
TCP        [::1]:59088        [::1]:7080         TIME_WAIT      0
C:\Users\Administrator>
```

Step 2 Open the **Task Manager**. On the **Details** tab, 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 the MgC Agent.



Name	PID	Status	User na...	CPU	Memory ...
vmnat.exe	5264	Running	SYSTEM	00	1,184 K
vmcad.exe	5292	Running	SYSTEM	00	8,180 K
vmnetdhcp.exe	5324	Running	SYSTEM	00	7,004 K
chrome.exe	5376	Running	Adminis...	00	6,764 K
dllhost.exe	5380	Running	Adminis...	00	1,760 K
chrome.exe	5404	Running	Adminis...	00	209,896 K
postgres.exe	5608	Running	vmware-...	00	996 K
vmware-unity-h...	5632	Running	Adminis...	00	3,080 K
RuntimeBroker...	5652	Running	Adminis...	00	2,668 K
java.exe	5816	Running			
vmware-authd.e...	5972	Running			
vmware-usbarbi...	5988	Running			
YunDetectServic...	6012	Running			
chrome.exe	6040	Running			
conhost.exe	6100	Running			
java.exe	6264	Running			
conhost.exe	6384	Running			
postgres.exe	6484	Running			
wrapper.exe	6576	Running			
chrome.exe	6868	Running			
postgres.exe	6908	Running			

----End

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

Symptom

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


Possible Causes

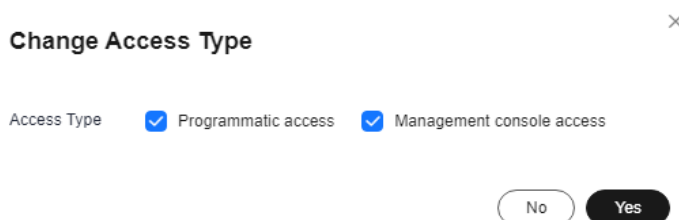
Possible causes are:

- 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.
- The time on the server where the MgC Agent was installed is inconsistent with the local standard time.

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. Sign 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 not, click  next to **Access Type**, select **Programmatic Access**, and click **Yes**



- The time on the server where the MgC Agent was installed is inconsistent with the local standard time.
 - a. On the Windows server where the MgC Agent was installed, open **Date and Time**.
 - b. On the **Date and Time** page, enable **Set time automatically** and click **Sync now** to trigger time synchronization.
 - c. Ensure that the time zone and time are the same as the local standard time, return to the MgC Agent console, and query MgC migration projects again.

8.14 How Do I Configure WinRM 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 the MgC Agent (formerly Edge) is installed as an administrator and run PowerShell as administrator. Perform steps 5 to 7 on the server with the MgC Agent 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-PSession -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.

8.15 What Do I Do If the Credential List Is Empty When I Create a Data Connection for Big Data Verification?

Symptom

When you tried to create a data connection for big data verification, the credential drop-down list was empty or your credential was not found in the list.

Possible Causes

The possible causes are:

- Your credential was incorrect. Specifically, the credential you added to the MgC Agent (formerly Edge) did not match the required type for the new connection.
- The credential you added to the MgC Agent was not synchronized to MgC.

Solutions

- If the credential is incorrect, go to the MgC Agent console and check whether the credential type is that required by the new connection. If the credential has not been added, add it by referring to [Adding Resource Credentials](#). After the credential is added, it will be automatically synchronized to MgC.
- If the credential fails to be synchronized, go to the MgC console and choose **Settings** > **Credentials** in the navigation pane, click the MgC Agent name, and check whether the credential added to the MgC Agent can be found in the list. If the credential cannot be found, go to the MgC Agent console to synchronize the credential again. Ensure that the credential is displayed on the **Credentials** page of the MgC console.

