ALIBABA CLOUD

Alibaba Cloud

Elastic Compute Service
Deployment & Maintenance

Document Version: 20220707

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
⚠ Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	⚠ **Danger:** Resetting will result in the loss of user configuration data.
🔔 Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	🔔 **Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
📢 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	📢 **Notice:** If the weight is set to 0, the server no longer receives new requests.
ⓘ Note	A note indicates supplemental instructions, best practices, tips, and other content.	ⓘ **Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Instance troubleshooting

1.1. Automatic diagnosis system

If you are experiencing problems when you use cloud resources in the Elastic Compute Service (ECS) console, you can submit information to the automatic diagnosis system for troubleshooting.

Context

The automatic diagnosis system has the following benefits:

- Simplified submission with near instantaneous feedback.
- Intelligent processing that returns diagnostic results within seconds.
- Extended support. The problems that cannot be handled by intelligent processing are immediately forwarded to Alibaba Cloud technical support personnel. This improves the overall efficiency of problem handling.

The following limits apply to the automatic diagnosis system:

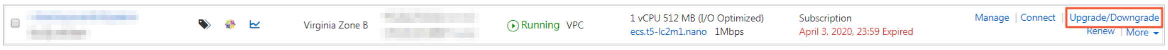
- You can access the automatic diagnosis system only in the ECS console.
- Each account can have up to 20 diagnostic records in the **Pending** state per region. You can submit new diagnostic requests in a region only when less than 20 diagnostic records are in the **Pending** state in that region.
- You can view the diagnostic records of the last 30 days on the Troubleshooting page in the ECS console.

In this topic, an upgrade operation on a subscription instance is used to describe how to use the automatic diagnosis system. The upgrade operation failed because you have unpaid orders. An **Error** message is returned. You can use the automatic diagnosis system to troubleshoot the error. For more information about how to upgrade the instance types of subscription instances, see Upgrade the instance types of subscription instances.

Step 1: Submit an automatic diagnostic request

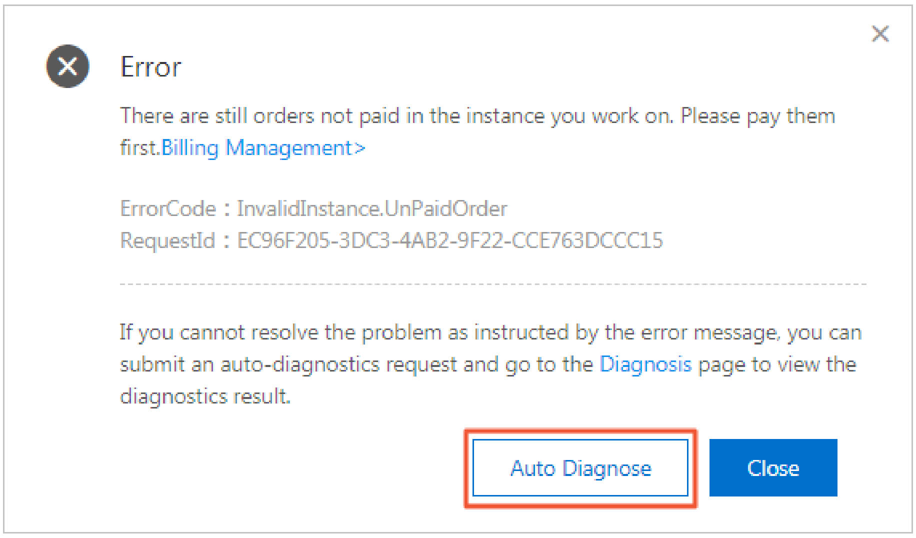
To submit an automatic diagnostic request, perform the following operations:

1.
2.
3.
4. Find the subscription instance whose instance type you want to upgrade and click **Upgrade/Downgrade** in the **Actions** column.



Virginia Zone B | Running VPC | 1 vCPU 512 MB (I/O Optimized) ecs.t5-lc2m1.nano 1Mbps | Subscription April 3, 2020, 23:59 Expired | Manage | Connect | Upgrade/Downgrade Renew | More

5. In the Upgrade/Downgrade Wizard dialog box, select **Upgrade** and click **Continue**.
6. On the Upgrade page, select a new instance type, set the Restart At parameter, and then select *ECS Service Terms*. Then, click **Create Order**.
7. Do not pay for the order. Upgrade the subscription instance again.
8. In the **Note** message, click **Continue Order**.
9. In the **Error** message, click **Auto Diagnose**.


Error

There are still orders not paid in the instance you work on. Please pay them first.Billing Management>

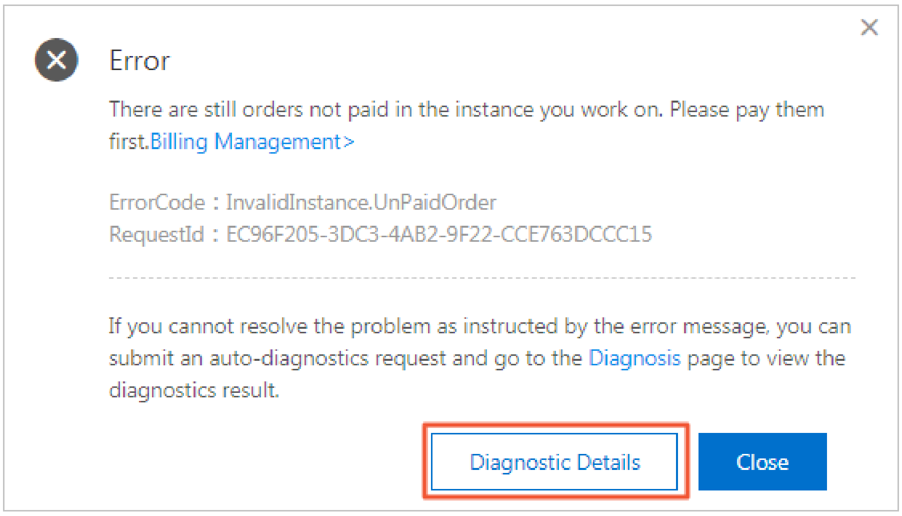
ErrorCode : InvalidInstance.UnPaidOrder
RequestId : EC96F205-3DC3-4AB2-9F22-CCE763DCCC15

If you cannot resolve the problem as instructed by the error message, you can submit an auto-diagnostics request and go to the Diagnosis page to view the diagnostics result.

Step 2: View the solution

To view the recommended solution to the problem, perform the following operations:

1. After your automatic diagnostic request is submitted, click **Diagnostic Details**.

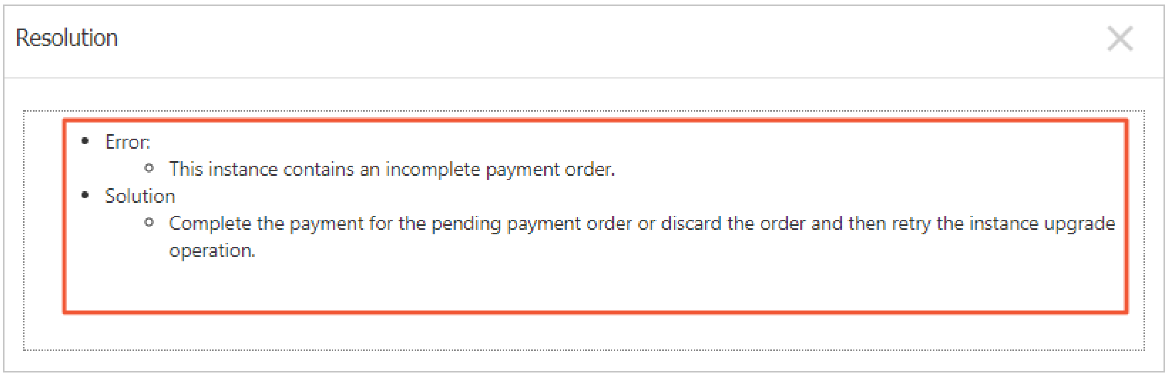

Error

There are still orders not paid in the instance you work on. Please pay them first.Billing Management>

ErrorCode : InvalidInstance.UnPaidOrder
RequestId : EC96F205-3DC3-4AB2-9F22-CCE763DCCC15

If you cannot resolve the problem as instructed by the error message, you can submit an auto-diagnostics request and go to the Diagnosis page to view the diagnostics result.

2. On the **Operation Exception Diagnosis** tab, find your diagnostic record and view its details. **Processed** is displayed in the **Status** column corresponding to the record.
3. Click **View Solutions** in the Actions column to view the error cause and recommended solution.


Resolution

- Error:
  - This instance contains an incomplete payment order.
- Solution
  - Complete the payment for the pending payment order or discard the order and then retry the instance upgrade operation.

Step 3: Submit feedback on the solution

To submit feedback on the recommended solution, perform the following operations:

1. (Optional) In the View Solutions dialog box, enter your feedback about this diagnosis in the text box.
2. If you think the solution is helpful, click **Solved**. If you do not think the solution is helpful, click **Unsolved**.
3. Click **OK**.

1.2. ECS Network Connectivity Diagnostics

1.2.1. Diagnose network connectivity

Elastic Compute Service (ECS) Network Connectivity Diagnostics is a feature that allows you to diagnose the network connectivity between diagnostic objects in the cloud and identify the causes of network connectivity issues. This topic describes the ECS Network Connectivity Diagnostics feature and how to use this feature.

Prerequisites

The following requirements are met:

- If you want to use instances or elastic network interfaces (ENIs) as diagnostic objects, make sure that the instances or ENIs are in the **Running** state.
- If you want to use secondary ENIs as diagnostic objects, make sure that the ENIs are bound to instances. For more information, see Bind an ENI.
- If you diagnose an instance in a scenario where the operating system configurations of the instance are checked, the instance operating system meets the requirements described in the following table.

Operating system architecture	Operating system version	Operating system configuration
x86_64-bit	○ Windows Server 2008 or later ○ Alibaba Cloud Linux 2/3 ○ AlmaLinux 8.x ○ Anolis OS 7.x/8.2 ○ CentOS 7.x/8.x ○ CentOS Stream 8 ○ Debian 8.x/9.x/10.x ○ Fedora 33/34 ○ OpenSUSE 15.x/42.x ○ Rocky Linux 8.x ○ SUSE Linux 12.x/15.x ○ Ubuntu 20.04	○ Python: ■ Python 3.6 to 3.9 ■ Python 2.7 ○ The Cloud Assistant client is installed on the instance. For more information, see Install the Cloud Assistant client.

Context

To use the ECS Network Connectivity Diagnostics feature, perform the following steps:

1. Specify a path.

   Each path includes all information required to execute a diagnostic task, such as a virtual private cloud (VPC) and diagnostic objects (instances, ENIs, or public IP addresses). You can create or clone a path. For more information, see Create a path and Clone a path.

2. Initiate a diagnostic task.

   A diagnostic task is a diagnosis performed to check the real-time network connectivity between the source and destination diagnostic objects configured in a path. After a path is created or cloned, the system immediately initiates a diagnostic task for the path. You can also manually initiate a diagnostic task for an existing path. For more information, see Diagnose a path.

3. View diagnostic results.

   In the diagnostic task list, you can view the results and details of diagnostic tasks. For more information, see Manage diagnostic tasks.

   > **Note** The ECS Network Connectivity Diagnostics feature is used as an auxiliary tool to provide insight into critical network connectivity configurations, but its diagnostic results cannot indicate whether communication over networks is allowed or denied.

When you create a path and initiate a diagnostic task, the system checks whether the AliyunServiceRoleForECSNetworkInsights service-linked role exists. If the role does not exist, the system creates the role. For more information, see Manage the service-linked role for ECS Network Connectivity Diagnostics.

The following table describes the quotas on paths and diagnostic tasks.

Create a path

1.
2.
3.
4. Click the **Network Connectivity Diagnostics** tab.
5. Click **Create Path**.
6. Configure the parameters described in the following table and click **Create**.

Parameter	Description
Path Name	Enter a name for the path. The name must be 2 to 128 characters in length and can contain letters, digits, periods (`.`), underscores (`_`), hyphens (`-`), and colons (`:`). It cannot start with a special character, a digit, `http://` , or `https://` .
VPC	Select a VPC. At least one of the diagnostic objects is an ECS instance or ENI that is located in a VPC.

Parameter	Description
Source and Destination	Select a diagnostic object type and then specify a source diagnostic object and a destination diagnostic object. Valid values for the diagnostic object type: ○ **ECS Instance**: existing ECS instances. The source and the destination diagnostic objects cannot be the same instance. ○ **NIC**: existing ENIs. The source and destination diagnostic objects cannot be the same ENI or the ENIs that are bound to the same instance. ○ **Public IP Address**: public IP addresses. You can manually enter public IP addresses as diagnostic objects. The source and the destination diagnostic objects cannot be public IP addresses at the same time.
Destination Port and Protocol	Specify the destination port and protocol. The supported destination port is determined by the selected protocol. ○ If you set Protocol to **Custom TCP** or **Custom UDP**, select a port from the drop-down list or enter a port number for Destination Port. **SSH (22)**, **Telnet (23)**, **HTTP (80)**, **HTTPS (443)**, **MS SQL (1433)**, **Oracle (1521)**, **MySQL (3306)**, **RDP (3389)**, **PostgreSQL (5432)**, and **Redis (6379)** are displayed on the drop-down list. ○ If you set Protocol to **All ICMP(IPv4)** or **All GRE**, Destination Port is automatically set to **-1**.

After the path is created, the system initiates a diagnostic task to diagnose the network connectivity over the specified protocol from the source diagnostic object to the specified port of the destination diagnostic object.

> **Note** It takes a few minutes for a diagnostic task to be completed. You can view the state and diagnostic result of a diagnostic task in the path list. Alternatively, you can go to the details page of the path to view the state and diagnostic result of the task in the diagnostic task list. For more information, see Manage diagnostic tasks.

Clone a path

You can clone an existing path and modify some settings, such as the source or destination diagnostic object, to quickly create a path.

1.
2.
3.
4. Click the **Network Connectivity Diagnostics** tab.
5. Click **Clone** in the **Actions** column corresponding to a path.
6. Configure the parameters described in the following table and click **Create**.

Parameter	Description
Path Name	Enter a name for the path. The name must be 2 to 128 characters in length and can contain letters, digits, periods (`.`), underscores (`_`), hyphens (`-`), and colons (`:`). It cannot start with a special character, a digit, `http://` , or `https://` .
VPC	Select a VPC. At least one of the diagnostic objects is an ECS instance or ENI that is located in a VPC.
Source and Destination	Select a diagnostic object type and then specify a source diagnostic object and a destination diagnostic object. Valid values for the diagnostic object type: ○ **ECS Instance**: existing ECS instances. The source and the destination diagnostic objects cannot be the same instance. ○ **NIC**: existing ENIs. The source and destination diagnostic objects cannot be the same ENI or the ENIs that are bound to the same instance. ○ **Public IP Address**: public IP addresses. You can manually enter public IP addresses as diagnostic objects. The source and the destination diagnostic objects cannot be public IP addresses at the same time.
Destination Port and Protocol	Specify the destination port and protocol. The supported destination port is determined by the selected protocol. ○ If you set Protocol to **Custom TCP** or **Custom UDP**, select a port from the drop-down list or enter a port number for Destination Port. **SSH (22)**, **Telnet (23)**, **HTTP (80)**, **HTTPS (443)**, **MS SQL (1433)**, **Oracle (1521)**, **MySQL (3306)**, **RDP (3389)**, **PostgreSQL (5432)**, and **Redis (6379)** are displayed on the drop-down list. ○ If you set Protocol to **All ICMP(IPv4)** or **All GRE**, Destination Port is automatically set to **-1**.

After a path is cloned, the system initiates a diagnostic task to diagnose the network connectivity over the specified protocol from the source diagnostic object to the specified port of the destination diagnostic object.

Note It takes a few minutes for a diagnostic task to be completed. You can view the state and diagnostic result of a diagnostic task in the path list. Alternatively, you can go to the details page of the path to view the state and diagnostic result of the task in the diagnostic task list. For more information, see Manage diagnostic tasks.

Diagnose a path

You can manually initiate a diagnostic task for an existing path. However, each path can have only a single diagnostic task ongoing. If a diagnostic task is being executed on a path, no other diagnostic tasks can be initiated for the path.

1.
2.
3.
4. Click the **Network Connectivity Diagnostics** tab.
5. Click **Diagnose** in the **Actions** column corresponding to a path.
6. Click **Continue**.

Manage diagnostic tasks

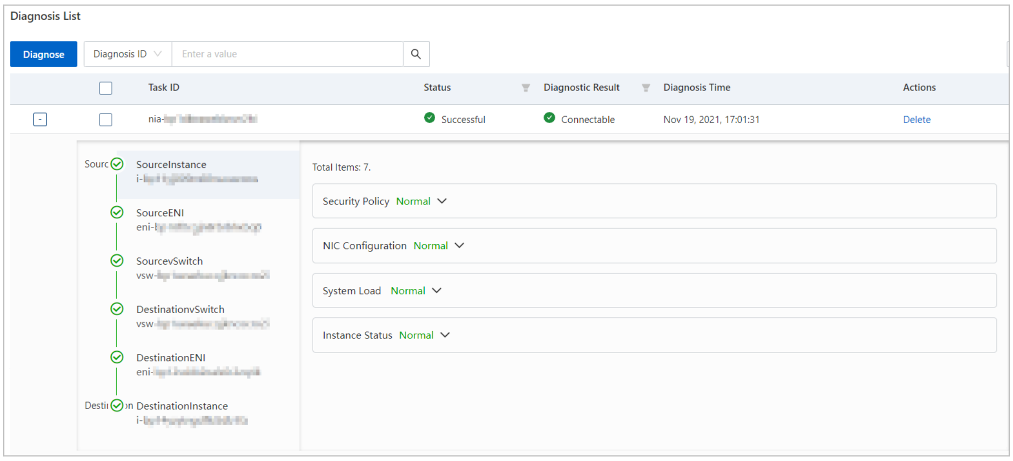
The latest diagnostic results are displayed for paths in the path list. However, you may want to view diagnostic task details or historical diagnostic tasks. For example, when Unconnectable is displayed as the diagnostic result for a path, you may want to look into the details of the diagnostic task for the cause of this issue. This section describes how to manage diagnostic tasks.

> **Note** The records of a limited number of diagnostic tasks can be retained for each path. We recommend that you delete diagnostic tasks that are no longer needed on a regular basis.

1.
2.
3.
4. Click the **Network Connectivity Diagnostics** tab.
5. Click the ID of a path.
6. Perform the following operations based on your business requirements:
   - To initiate a diagnostic task, click **Diagnose** and click **Continue**.
   - To delete a diagnostic task, find the task and click **Delete** in the **Actions** column. Then, click **Continue**.
   - To view details of a specific diagnostic task, click the ⊞ icon in the **Diagnosis List** section on the details page of the task.

     > **Note** For more information about diagnostic items, see Diagnostic items of ECS Network Connectivity Diagnostics.

     Details of a sample diagnostic task whose result is Connectable

     Diagnosis List

     Diagnose | Diagnosis ID | Enter a value

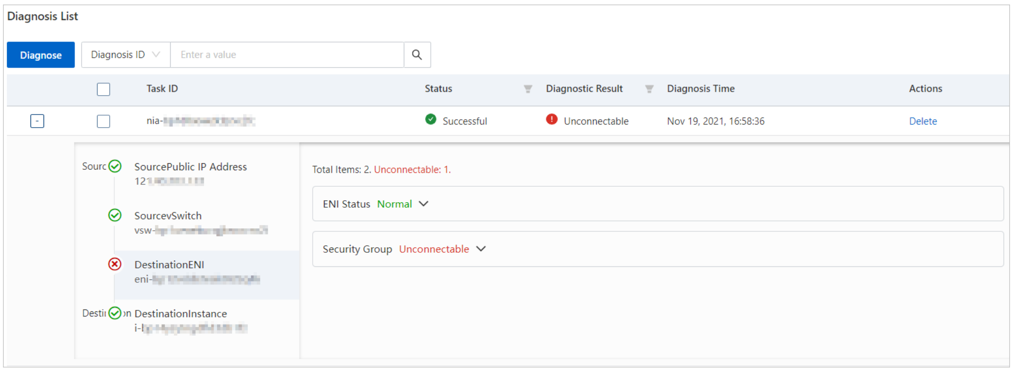
	□	Task ID	Status	Diagnostic Result	Diagnosis Time	Actions
⊟	□	nia-[redacted]	✓ Successful	✓ Connectable	Nov 19, 2021, 17:01:31	Delete

     ✓ SourceInstance i-[redacted]
     ✓ SourceENI eni-[redacted]
     ✓ SourcevSwitch vsw-[redacted]
     ✓ DestinationvSwitch vsw-[redacted]
     ✓ DestinationENI eni-[redacted]
     ✓ DestinationInstance i-[redacted]

     Total Items: 7.

     Security Policy Normal
     NIC Configuration Normal
     System Load Normal
     Instance Status Normal

Details of a sample diagnostic task whose result is Unconnectable



Diagnosis List

	□	Task ID	Status	Diagnostic Result	Diagnosis Time	Actions
-	□	nia-[redacted]	✓ Successful	! Unconnectable	Nov 19, 2021, 16:58:36	Delete

Sourc ✓ SourcePublic IP Address
12[redacted]

✓ SourcevSwitch
vsw-[redacted]

⊗ DestinationENI
eni-[redacted]

Destii ✓ ›n DestinationInstance
i-[redacted]

Total Items: 2. Unconnectable: 1.

ENI Status Normal

Security Group Unconnectable

Delete a path

1.
2.
3.
4. Click the **Network Connectivity Diagnostics** tab.
5. Click **Delete** in the **Actions** column corresponding to a path.
6. Click **Continue**.

1.2.2. Diagnostic items of ECS Network Connectivity Diagnostics

This topic describes the diagnostic items supported by the Elastic Compute Service (ECS) Network Connectivity Diagnostics feature and elaborates the diagnostic scope and results.

Diagnostic items

The ECS Network Connectivity Diagnostics feature supports the following resources:

- ECS instances. The ECS Network Connectivity Diagnostics feature checks the diagnostic items of ECS instances, including security policies, network interface controller (NIC) configurations, system load, and business states.
- Elastic network interfaces (ENIs). The ECS Network Connectivity Diagnostics feature checks the underlying states and security group configurations of ENIs.
- vSwitches. The ECS Network Connectivity Diagnostics feature checks the network access control list (ACL) configurations of vSwitches.

Diagnostic items are assigned the following severity levels:

- Critical: A critical diagnostic item determines network connectivity. If it is diagnosed with exceptions, network connectivity issues have occurred.
- Non-critical: A non-critical diagnostic item may affect network connectivity. If it is diagnosed with exceptions, network connectivity issues may occur.

Diagnostic items of ECS instances

Category	Diagnostic item	Severity	Description	Suggestion
SSH service	Whether the SSH service has started	Critical	Checks whether the SSH service has started and on which port the service is listening on an instance. • If the state of the sshd process is displayed as normal, the SSH service has started and is listening on port 22 on a Linux instance or port 3389 on a Windows instance. • If the sshd process is displayed to be listening on a port other than ports 22 and 3389 (such as port 1234) and port 22 or 3389 is displayed as the destination port to be diagnosed, the SSH service has started and is listening on the port other than ports 22 and 3389. • If the state of the sshd process is displayed as not started, the SSH service has not started.	• If the SSH service is not listening on port 22 on a Linux instance or port 3389 on a Windows instance, select the port on which the SSH service is listening on to connect to the instance, or change the listening port to port 22 or 3389. For more information, see Modify the default port used by an instance to accept connections. • If the SSH service has not started, log on to the instance by using Virtual Network Console (VNC) and start the service.
	Whether critical files or directories required by the SSH service exist	Critical	Checks the integrity of SSH configuration files and directories.	If a message is displayed indicating that an SSH configuration file or directory is missing, recover the file or directory based on the message.
	Check whether SSH allows the root user to log on	Non-critical	Checks whether SSH allows the root user to log on.	If a message is displayed indicating that SSH denies logons by the root user and you want to lift this limit, troubleshoot the issue and modify SSH configurations. For more information, see The error "Permission denied, please try again" is returned when the root user logs on to a Linux instance through SSH.

Category	Diagnostic item	Severity	Description	Suggestion
NIC configurations	Whether the Dynamic Host Configuration Protocol (DHCP) service has started	Critical	If an instance whose image supports DHCP was not correctly assigned a static IP address and the DHCP service has not started on the instance, a message is displayed indicating that DHCP has not started.	Log on to the instance by using VNC and start the DHCP service.
	Whether NIC IP addresses are correct	Critical	For a NIC, if a message similar to " `Invalid IP address` " is displayed, it indicates that the detected IP address is different from the configured one.	Modify the static IP address of the NIC. For more information, see Assign secondary private IP addresses.
	Whether NIC masks are correct	Non-critical	For a NIC, if a message similar to " `No mask is configured for the` *<enild>* `NIC` " is displayed, it indicates that the NIC does not have a mask or has an incorrect mask.	Use the default mask or manually configure a correct mask for the NIC.
Instance security policies	Whether iptables rules are configured to allow or block traffic	Critical	- For an instance, if a message similar to " `The hit iptables rule` *<ruleName>* `blocks traffic` " is displayed, it indicates an iptables rule is configured on the instance to block traffic. - For an instance, if a message similar to " `iptables rules allow traffic` " is displayed, it indicates that an iptables rule is configured on the instance to allow traffic.	- If you do not want to block the traffic, delete the Block iptables rule. - If you do not want to allow the traffic, configure an iptables rule to block the traffic or change the Allow iptables rule into a Block one.

Category	Diagnostic item	Severity	Description	Suggestion
	Whether blackhole filtering is triggered on the public IP address of an instance	Critical	If an instance falls victim to DDoS attacks and the volume of the DDoS attacks exceeds the mitigation capability provided for the instance, blackhole filtering is triggered and all inbound traffic to the public IP address of the instance is blocked. If this occurs, a message similar to "`Blackhole filtering is triggered on <Public IP address>, and the IP address cannot be accessed`" is displayed.	For more information about blackhole filtering policies and how to deactivate blackhole filtering, see Blackhole filtering policy of Alibaba Cloud.
System routing configurations	Whether routing policies are configured	Critical	If no routing policies are configured on an instance, the check fails. If a routing policy is configured on an instance, a message similar to "`The` *policyName* `routing policy forwards traffic`" is displayed.	Check for and delete incorrect routing policies.
Instance system load	CPU load	Non-critical	Checks whether the CPU load of an instance exceeds 80%.	If the CPU load of an instance remains higher than 80%, decide whether to upgrade to an instance type with more vCPUs. For more information, see Change instance types.
	Public bandwidth load	Non-critical	Checks whether the public bandwidth load of an instance exceeds 90%.	If the public bandwidth load of an instance remains higher than 90%, decide whether to increase the public bandwidth. For more information, see Modify public bandwidth.
	Internal bandwidth load	Non-critical	Checks whether the internal bandwidth load of an instance exceeds 90%.	If the internal bandwidth load of an instance remains higher than 90%, decide whether to upgrade to an instance type that provides a higher base bandwidth. For more information, see Change instance types.

Category	Diagnostic item	Severity	Description	Suggestion
User service state	Whether processes are listening on specified destination ports	Critical	Check whether processes are listening on the specified destination ports of an instance. If not, the check fails.	Connect to the instance and start processes to listen on the specified destination ports.
Instance state	Whether an instance has expired	Critical	If an expired instance is detected, a message is displayed.	Renew the instance at your earliest convenience. For more information, see Renewal overview.
	Overdue payments in your Alibaba Cloud account	Critical	If overdue payments are detected in your Alibaba Cloud account, a message is displayed.	Add funds to your account at your earliest convenience.

Diagnostic items of ENIs

Category	Diagnostic item	Severity	Description	Suggestion
ENI state	Underlying state	Critical	If the underlying state of an ENI is abnormal, a message is displayed.	Submit a ticket.
			Security groups control traffic to or from ENIs based on security group types and rules. • Basic security groups: ◦ If the source and destination diagnostic objects in a path belong to the same security group and the security group contains no rules, these diagnostic objects can communicate with each other.	

Category	Diagnostic item	Severity	Description	Suggestion
Security group configurations	Security groups	Critical	○ If the source and destination diagnostic objects in a path belong to different security groups that contain no rules, outbound traffic from the source diagnostic object is allowed and inbound traffic to the destination diagnostic object is denied. - Advanced security groups: If security groups contain no rules, the security groups deny outbound traffic from source diagnostic objects and allow inbound traffic to destination diagnostic objects. - If security groups contain rules, the security groups deny or allow traffic based on their attributes and rules. For more information, see Overview.	Checks whether security groups implement access control as expected. If not, configure them based on your needs.

Diagnostic items of vSwitches

Category	Diagnostic item	Severity	Description	Suggestion

Category	Diagnostic item	Severity	Description	Suggestion
Network ACL	Network ACL configurations	Critical	• If no network ACL is associated with a vSwitch, the vSwitch allows all traffic by default. • If the source and destination diagnostic objects in a path are connected to the same vSwitch, the traffic between these diagnostic objects is exempt from the network ACL rules that are associated with the vSwitch. • If the source and destination diagnostic objects in a path are connected to different vSwitches and network ACLs are associated the vSwitches, the vSwitches determine whether to allow traffic between the diagnostic objects based on the rules in the network ACLs. For more information, see Overview of network ACLs.	Checks whether a vSwitch implements access control as expected. If not, configure a network ACL for the vSwitch based on your needs.

1.2.3. Manage the service-linked role for ECS Network Connectivity Diagnostics

The Elastic Compute Service (ECS) Network Connectivity Diagnostics feature allows you to check the network connectivity between diagnostic objects. Before you can use this feature to create a path and initiate a diagnostic task, you must grant access permissions on required resources to ECS. This topic describes how to use the AliyunServiceRoleForECSNetworkInsights role to grant permissions to ECS. AliyunServiceRoleForECSNetworkInsights is the service-linked role of ECS Network Connectivity Diagnostics.

Prerequisites

If you want to log on to the ECS console as a Resource Access Management (RAM) user to use ECS Network Connectivity Diagnostics, make sure that the RAM user has been granted the permissions to use ECS Network Connectivity Diagnostics by your Alibaba Cloud account so that the RAM user can manage the AliyunServiceRoleForECSNetworkInsights role. For more information, see Grant permissions to a RAM user.

The following policy is attached to grant the RAM user the permissions to use the ECS Network Connectivity Diagnostics feature.

Note Replace *<account ID>* with the ID of your Alibaba Cloud account.

```
{
    "Statement": [
        {
            "Action": [
                "ram:CreateServiceLinkedRole"
            ],
            "Resource": "acs:ram:*:<account ID>:role/*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": [
                        "network-insights.ecs.aliyuncs.com"
                    ]
                }
            }
        }
    ],
    "Version": "1"
}
```

Context

A service-linked role is a role that is linked to a service, and includes the permissions required to call other services. For example, the AliyunServiceRoleForECSNetworkInsights service-linked role includes the access permissions on virtual private cloud (VPC) resources that are required for ECS Network Connectivity Diagnostics to create paths and initiate diagnostic tasks. For more information, see Service-linked roles.

Create the AliyunServiceRoleForECSNetworkInsights service-linked role

When you create a path and initiate a diagnostic task, the system checks whether the AliyunServiceRoleForECSNetworkInsights role exists. If the role does not exist, the system creates the role. The AliyunServiceRolePolicyForECSNetworkInsights policy is attached to the AliyunServiceRoleForECSNetworkInsights role. ECS can assume this role to take on the permissions of the role.

The policy attached to a service-linked role is predefined by the linked service. You cannot add, modify, or delete the policy. You can view policies attached to a role and policy details in the RAM console. For more information, see View the basic information about a RAM role and View the basic information about a policy. The following code shows the content of the AliyunServiceRolePolicyForECSNetworkInsights policy:

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "vpc:DescribeNetworkAcls",
                "vpc:DescribeNetworkAclAttributes",
                "vpc:DescribeNatGateways",
                "vpc:DescribeRouteEntryList",
                "vpc:DescribeRouteTableList",
                "vpc:DescribeRouteTables",
                "vpc:DescribeRouterInterfaceAttribute",
                "vpc:DescribeRouterInterfaces",
                "vpc:DescribeVRouters",
                "antiddos-public:DescribeInstance"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "ram:DeleteServiceLinkedRole",
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": "network-insights.ecs.aliyuncs.com"
                }
            }
        }
    ]
}
```

Delete the AliyunServiceRoleForECSNetworkInsights service-linked role

If the AliyunServiceRoleForECSNetworkInsights service-linked role within your account is no longer needed, you can manually delete the role.

1. Log on to the RAM console.
2. In the left-side navigation pane, choose **Identities > Roles**.
3. In the search box, enter AliyunServiceRoleForECSNetworkInsights.

   The AliyunServiceRoleForECSNetworkInsights role is displayed in the search result.
4. In the **Actions** column, click **Delete**.
5. Click **OK**.

For more information about how to delete a service-linked role, see the "Delete a service-linked role" section in Service-linked roles.

1.3. View system logs and screenshots

ECS is a virtualized cloud-based service. You cannot capture screenshots of Elastic Compute Service (ECS) resources or connect ECS to display devices. However, ECS caches system logs of the most recent start, restart, or shutdown actions of each instance, and you can capture screenshots of the instances on a real-time basis. You can use these features to analyze and troubleshoot instance issues such as operating systems not responding, abnormal restart, or instance connection failures.

Prerequisites

The instance is in the **Running** (*Running*) state. For more information, see Connection methodsGuidelines on instance connection.

Context

System logs are important for O&M diagnostics. If you want to diagnose exceptions, you can query ECS system logs of instance startup and exceptions. The system uses the serial ports to display two types of system logs: startup logs and kernel failure or exception logs.

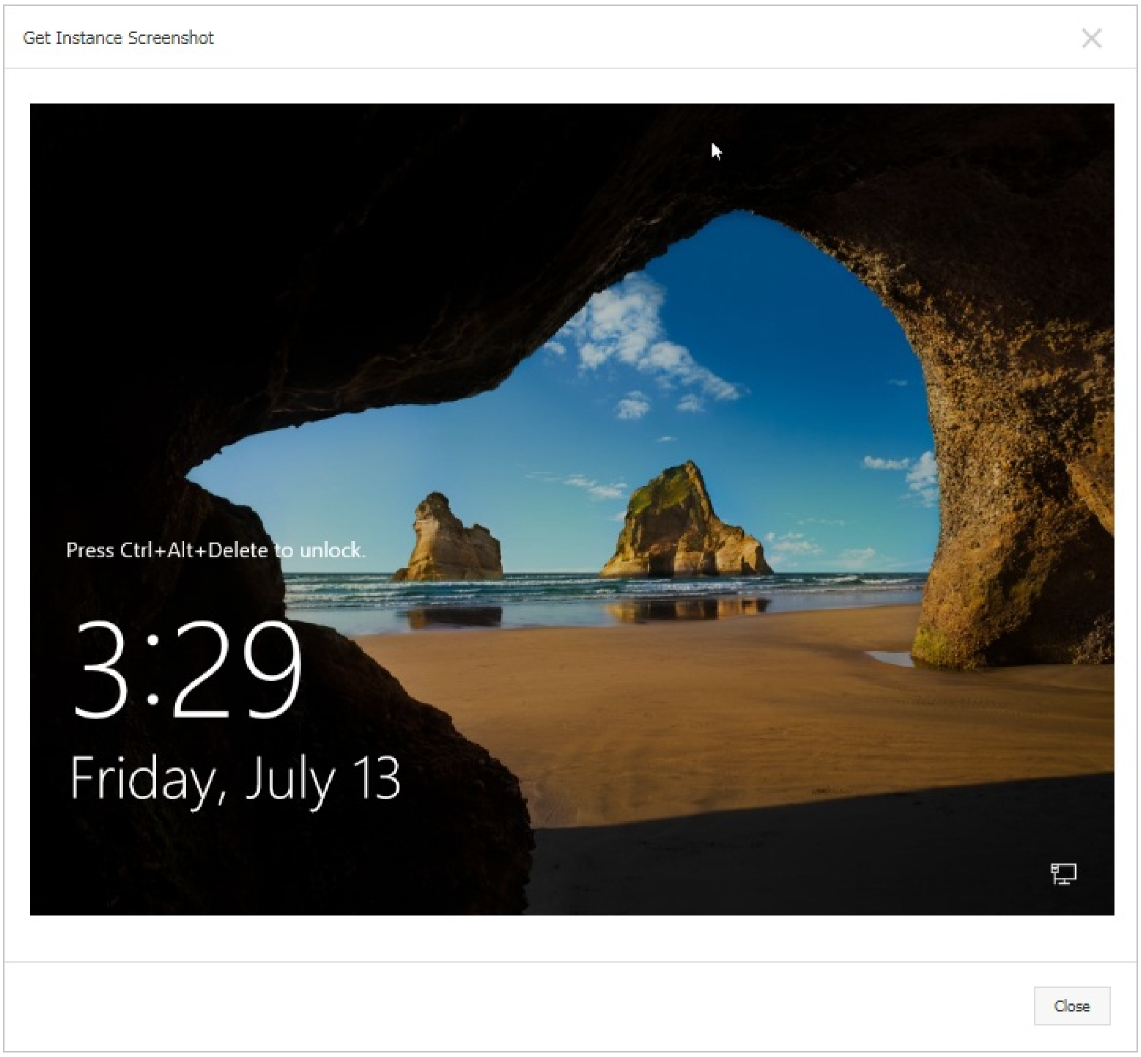
You can view system logs and instance screenshots on the Instance Details or Instances page in the ECS console, or by calling API operations. When you use these features, take note of the following items:

- For Windows instances, you can only view instance screenshots. You cannot obtain system logs of the instances.
- You cannot obtain system logs or screenshots for instances of retired instance types. For more information, see Retired instance types.
- You cannot obtain system logs or screenshots for instances created before January 1, 2018.

Procedure on the Instance Details page

Perform the following steps to view system logs and screenshots of an instance on the Instance Details page:

1.
2.
3.
4. Select the instance that you want to troubleshoot and click the instance ID to go to the **Instance Details** page.
5. In the Basic Information section, choose **More > Get Instance Screenshot** to view instance screenshots, or choose **More > Get Instance System Logs** to view system logs.
6. View screenshots or system logs of the instance.
   - Sample screenshot of a Windows instance

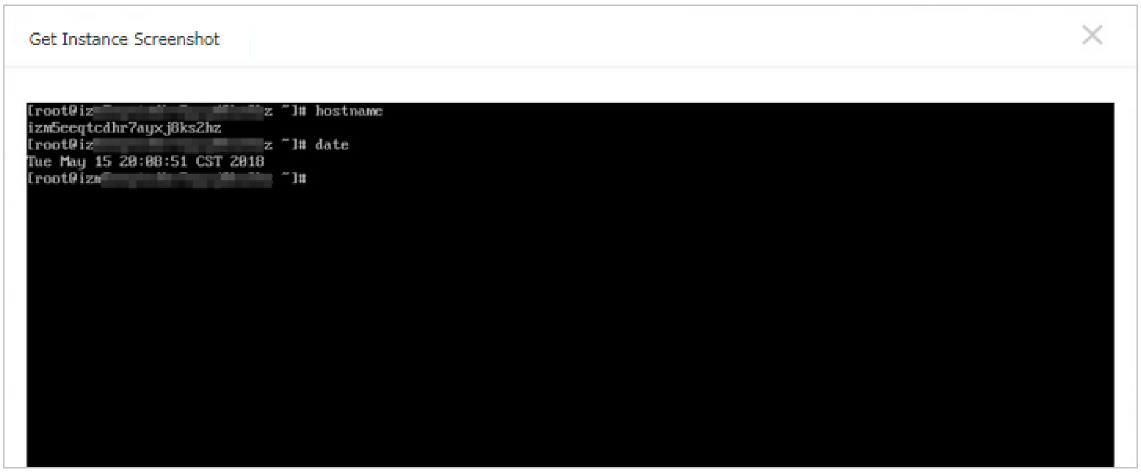


Press Ctrl+Alt+Delete to unlock.

3:29

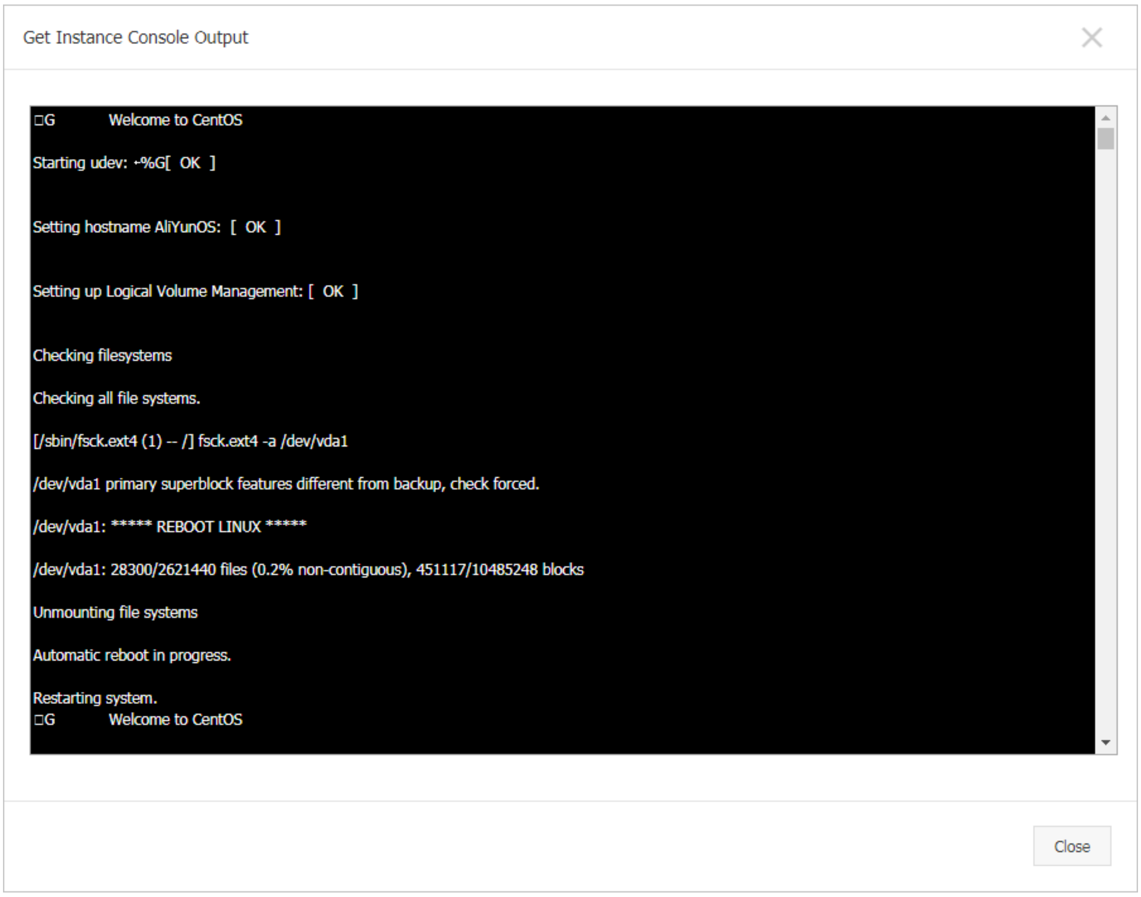
Friday, July 13

- Sample screenshot of a Linux instance



```
[root@iz[redacted]z ~]# hostname
izm5eeqtcdhr7ayxj0ks2hz
[root@iz[redacted]z ~]# date
Tue May 15 20:08:51 CST 2018
[root@izm[redacted] ~]#
```

- Sample system log of a Linux instance



```
□G        Welcome to CentOS

Starting udev: ⁃%G[  OK  ]


Setting hostname AliYunOS:  [  OK  ]


Setting up Logical Volume Management: [  OK  ]


Checking filesystems

Checking all file systems.

[/sbin/fsck.ext4 (1) -- /] fsck.ext4 -a /dev/vda1

/dev/vda1 primary superblock features different from backup, check forced.

/dev/vda1: ***** REBOOT LINUX *****

/dev/vda1: 28300/2621440 files (0.2% non-contiguous), 451117/10485248 blocks

Unmounting file systems

Automatic reboot in progress.

Restarting system.
□G        Welcome to CentOS
```

Procedure on the Instances page

Perform the following steps to view system logs and screenshots of an instance on the Instances page:

1.
2.
3.
4. Find the instance that you want to troubleshoot and the corresponding **Actions** column.
5. Choose **More > Operations and Troubleshooting > Get Instance Screenshot** to view instance screenshots, or choose **More > Operations and Troubleshooting > Get Instance System Logs** to view system logs.
6. View screenshots or system logs of the instance.

What's next

For more information about troubleshooting, see Method for testing links after a packet loss or failure occurs when the ping command is used.

Related information

- GetInstanceScreenshot
- GetInstanceConsoleOutput

2.System events

2.1. Overview

System events are defined by Alibaba Cloud to record and notify resource information, such as the execution states of O&M tasks, resource exceptions, and resource state changes.

> **Note** Many Alibaba Cloud services such as Elastic Compute Service (ECS), ApsaraDB RDS, and Server Load Balancer (SLB) support system events. This topic describes ECS system events. For information about system events of other Alibaba Cloud services, see the corresponding documentation.

System event categories

System events are defined by Alibaba Cloud to record and notify resource information. System events are classified into the categories described in the following table based on their causes:

> **Note** For information about system event categories that ECS supports and how to handle ECS system events, see Summary.

Category	Description	Displayed in the ECS console
Unexpected O&M events	This category of system events is triggered when ECS instances restart or break down due to unexpected issues such as kernel panic, out-of-memory errors, or hardware or software failures in underlying hosts. Alibaba Cloud sends these events when they are detected and restores affected ECS resources as soon as possible. At the same time, Alibaba Cloud notifies you of the execution states of system O&M tasks related to the events.	Yes
Scheduled O&M events	Alibaba Cloud may need to upgrade host software for security reasons or to foresee and take actions against failure risks that lie in underlying host hardware and software. In these cases, if O&M tasks to be executed by Alibaba Cloud may affect the availability or performance of your ECS resources, Alibaba Cloud triggers and sends scheduled O&M events in advance to notify you of task details such as execution times, objects, and impacts. After you receive a scheduled O&M event, you can handle it during an off-peak period within the event execution window to minimize the impact on your business.	Yes
Instance billing events	This category of system events is triggered by upcoming billing changes of instances. For example, instance billing events are triggered when instances expire and are about to be released or when instances are about to be stopped due to overdue payments.	Yes

Category	Description	Displayed in the ECS console
Instance security events	This category of system events is triggered when instances face security threats. For example, instance security events are triggered when instances suffer DDoS attacks or when blackhole filtering is triggered for instances.	Yes
State change events	This category of system events is triggered when operations (such as Start and Stop) on instances cause their lifecycle states to change or when instance attribute changes cause instance lifecycle or other states to change. State change events are classified into the following categories: • Lifecycle state change events: For example, lifecycle state change events are triggered when instances enter a different state, when preemptible instances are interrupted, and when snapshots are created. • Other attribute change events: For example, other attribute change events are triggered when the performance mode of burstable instances is changed or when subscription disks are changed into pay-as-you-go disks.	• Lifecycle state change events are not displayed in the ECS console. • Specific other attribute change events are displayed in the ECS console.

System event severities

System events are assigned the following severities based on their impacts on the normal operation of instances:

- Critical: Critical system events may result in instance unavailability and must be handled as soon as possible. For example, a critical system event is triggered when resources are released due to an overdue payment or when an instance is redeployed due to an instance error.
- Warning: Warning system events have impact on your business. For example, a warning system event is triggered when a burstable instance cannot burst above its performance baseline. You must pay close attention to these events or handle them when appropriate.
- Notification: Notification system events do not affect your business. For example, a notification system event is triggered when a snapshot is created for a disk. You can optionally pay attention to notification system events.

Use scenarios of system events

- Notification of risks and exceptions

  After system events that can be displayed in the ECS console are triggered, Alibaba Cloud pushes the events to the ECS console. These events include those that affect the availability and performance of ECS resources, such as SystemMaintenance.Reboot events among scheduled O&M events and InstanceExpiration.Stop events among instance billing events.For some critical system events, Alibaba Cloud sends additional emails or internal messages. You can handle these events by using the ECS console or by calling API operations. We recommend that you handle the system events as soon as possible to ensure resource availability and performance. For more information, see Query and handle ECS system events.

  For example, when a subscription instance is about to expire, the ECS console prompts you to renew the instance within a specified period of time to ensure service continuity.

- Automated O&M

States are defined for system events displayed in the ECS console to help you understand the execution states of system O&M tasks. Meanwhile, new system events and changes in system event states are reported to CloudMonitor so that you can build an event-driven automated O&M system based on your business requirements. For more information about event states, see the States and windows of system events section in this topic.

> **Note** Each event state corresponds to a CloudMonitor event. For example, the Executing and Executed states that the InstanceFailure.Reboot ECS event type supports correspond to the Instance:InstanceFailure.Reboot:Executing and Instance:InstanceFailure.Reboot:Executed CloudMonitor events.

Some state change events are not displayed in the ECS console and cannot be handled by using the ECS console or by calling API operations. Examples: events that indicate instance state changes or interruptions of preemptible instances. No states are defined for these system events. However, these events are still reported to CloudMonitor when they are triggered so that you can build an event-triggered automated O&M system based on your business requirements.

For example, state change events are triggered when you manually start or stop instances. These events do not indicate risks or exceptions. If you want to log your operations to your system, you can configure event notifications for state change events and use the alert callback feature to write the startup and stop information of instances to operation logs.

Limits

Retired instance families do not support the system event feature. For more information, see Retired instance types.

Operations that can be performed on system events

Operation	Description and references
Understand system events	To learn about system events and understand their categories, severities, use scenarios, limits, states, and name formats, see this topic.
View system events	You can view system events by using the ECS console, CloudMonitor console, or Alibaba Cloud CLI. • For information about how to view system events by using the ECS console or Alibaba Cloud CLI, see Query and handle ECS system events. • For information about how to view system events by using the CloudMonitor console, see View system events.
Handle system events	For some high-risk system events (such as system events that affect the availability and performance of ECS resources), we recommend that you handle the events as suggested by using the ECS console or by calling API operations as soon as possible to ensure service availability. • For information about suggestions on how to handle all system events, see Summary. • For information about how to view and handle pending system events, see Query and handle ECS system events. • For information about how to handle system events related to local disks, see O&M scenarios and system events for instances equipped with local disks.

Operation	Description and references
Monitor system events	To ensure the stability of services that run on ECS instances and automate O&M, we recommend that you configure event notifications to be notified of underlying environment changes. After event notifications are configured, the system uses your specified notification methods to send you notifications. ● For information about how to configure alert rules in the CloudMonitor console to push event notifications, see Configure event notifications. ● For information about how to use a DingTalk chatbot to send event notifications to a DingTalk group, see Send event notifications by using a DingTalk chatbot.
Modify system event-related settings	You can modify system event-related settings based on your business requirements. ● You can modify the maintenance attributes of an instance to configure whether to restart or redeploy the instance after a system event is handled. For more information, see Instance maintenance attributes. ● For scheduled system events, you can set the time when to restart an instance after a scheduled system event is handled. For more information, see Modify the scheduled restart time.

States and windows of system events

The following table describes the states defined for system events that are displayed in the ECS console.

Note For information about the states that different system events support, see the "CloudMonitor event" columns of tables in Summary.

Event state	Attribute	Description
Inquiring	Intermediate	The O&M task related to the system event is pending authorization. After you authorize the task to be executed, the event enters the *Executing* state.
Scheduled	Intermediate	The O&M task related to the system event is scheduled and pending execution. When the O&M task is executed, the event enters the *Executing* state.
Executing	Intermediate	The O&M task related to the system event is being executed.
Executed	Stable	The O&M task related to the system event is completed.
Avoided	Stable	The impacts of the system event are prevented because you have migrated the affected instance within the user operation window.
Failed	Stable	The O&M task related to the system event failed.
Canceled	Stable	The O&M task related to the system event is automatically canceled.

System events have the following windows:

- User operation window

  The user operation window of a system event starts when the event is sent and ends when the O&M task related to the event is executed as scheduled. You can manually handle the event within the user operation window or wait for the system to automatically handle O&M task. Take note of the following items about the lengths of user operation windows:

  - In most cases, the user operation window of a scheduled O&M event ranges from 24 to 48 hours.

    > ? **Note** The lengths of user operation windows are unlimited for system events in the Inquiring state. The O&M tasks related to the events can start only after you authorize the tasks to be executed.

  - Typically, unexpected O&M system events caused by failures or invalid operations do not have a user operation window.
  - For system events indicating that subscription instances are about to expire, the window is three days.
  - For system events indicating that pay-as-you-go instances are to be stopped due to overdue payments, the window is less than 1 hour.

- Event execution window

  The execution window of a system event starts when the O&M task related to the event is executed and ends when the task is completed. Take note of the following items about the lengths of event execution windows:

  - For system events such as failure recovery events, the window is within 10 minutes.
  - Unexpected O&M events caused by failures or invalid operations have a short event execution window.

Formats of ECS event type and CloudMonitor event names

ECS event types and CloudMonitor events follow specific naming conventions for easy understanding.

- ECS event types are named in the `<Event cause>.<Event impact>` format to indicate event causes and impacts on resources.
- CloudMonitor events are named in the `<Resource type>:<Event cause>.<Event impact>:<Event state>` format to indicate resource types, event causes, event impacts on resources, and event states.

> ? **Note** ECS event types and CloudMonitor events may include only some of the preceding information in their names. For example, a CloudMonitor event name of `Disk:ErrorDetected:Executing` indicates that a disk is damaged, and excludes information about impacts on resources.

The following table describes some examples of ECS event types and CloudMonitor events.

> ? **Note** The Undefined event type indicates that ECS events are not displayed in the ECS console and cannot be handled by using the ECS console or by calling API operations. Example: the Instance:StateChange event.

Category	Example ECS event type	Example CloudMonitor event	Description
Scheduled O&M events	SystemMaintenance.Reboot	Instance:SystemMaintenance.Reboot:Inquiring	• Resource type: Instance indicates ECS instance. • Event cause: SystemMaintenance indicates that Alibaba Cloud proactively initiates a system O&M task. • Event impact: Reboot indicates that the instance is to be restarted while the O&M task is being executed. • Event state: Inquiring indicates that the O&M task related to the event is pending authorization and the instance can be restarted only after you authorize the task to be executed.
	SystemMaintenance.Reboot	Instance:SystemMaintenance.Reboot:Executed	• Resource type: Instance indicates ECS instance. • Event cause: SystemMaintenance indicates that Alibaba Cloud proactively initiates a system O&M task. • Event impact: Reboot indicates that the instance is to be restarted while the O&M task is being executed. • Event state: Executed indicates that the instance is stopped.
	ErrorDetected	Disk:ErrorDetected:Executing	• Resource type: Instance indicates ECS instance. • Event cause: ErrorDetected indicates that the local disk is damaged. • Event state: Executing indicates that the damaged local disk has not been repaired.

Category	Example ECS event type	Example CloudMonitor event	Description
Unexpected O&M events	SystemFailure.Redeploy	Instance:SystemFailure.Redeploy:Executed	• Resource type: Instance indicates ECS instance. • Event cause: SystemFailure indicates that the O&M task is caused by a system error. • Event impact: Redeploy indicates that the instance is to be deployed to another host while the O&M task is being executed. • Event state: Executed indicates that the instance is redeployed.
Lifecycle state change events	Undefined	Instance:StateChange	• Resource type: Instance indicates ECS instance. • Event cause: StateChange indicates that the instance state changes.
	Undefined	Snapshot:CreateSnapshotCompleted	• Resource type: Snapshot indicates snapshot. • Event cause: CreateSnapshotCompleted indicates that the snapshot is created.
	InstanceExpiration.Stop	Instance:InstanceExpiration.Stop:Scheduled	• Resource type: Instance indicates ECS instance. • Event cause: InstanceExpiration indicates that the subscription instance has expired. • Event impact: Stop indicates that the instance is to be stopped on expiration. • Event state: Scheduled indicates that the instance is pending a scheduled stop.

Category	Example ECS event type	Example CloudMonitor event	Description
Instance billing events	AccountUnbalanced.Stop	Instance:AccountUnbalanced.Stop:Avoided	• Resource type: Instance indicates ECS instance. • Event cause: AccountUnbalanced indicates that you have overdue payments. • Event impact: Stop indicates that the instance is to be stopped due to an overdue payment. • Event state: Avoided indicates that you have added funds to your account and the scheduled stop operation on the instance is canceled.

2.2. Summary

This topic summarizes the system events supported by Elastic Compute Service (ECS) and provides suggestions on how to handle these events.

Note An event type of Undefined indicates that ECS events are not displayed in the ECS console and cannot be handled by using the ECS console or by calling API operations. Example: the Instance:StateChange event.

Scheduled O&M events

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you
Scheduled instance restart due to system maintenance	SystemMaintenance.Reboot	Critical	• Instance:SystemMaintenance.Reboot:Inquiring • Instance:SystemMaintenance.Reboot:Scheduled • Instance:SystemMaintenance.Reboot:Executing • Instance:SystemMaintenance.Reboot:Executed • Instance:SystemMaintenance.Reboot:Avoided • Instance:SystemMaintenance.Reboot:Failed • Instance:SystemMaintenance.Reboot:Canceled	This system event is triggered 24 or 48 hours before the scheduled time of system maintenance.	We recommend that you take one of the following actions in response to the event: • Modify the scheduled restart time. • Restart the instance. For more information, see Restart an instance. • Wait for the instance to be automatically restarted. ? **Note** You can modify the maintenance attributes of the instance to specify the default action to take when the instance encounters a maintenance event. For more information, see Instance maintenance attributes.

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you
Scheduled instance stop due to system maintenance	SystemMaintenance.Stop	Critical	• Instance:SystemMaintenance.Stop:Scheduled • Instance:SystemMaintenance.Stop:Executing • Instance:SystemMaintenance.Stop:Executed • Instance:SystemMaintenance.Stop:Avoided • Instance:SystemMaintenance.Stop:Failed • Instance:SystemMaintenance.Stop:Canceled	This system event is triggered 24 or 48 hours before the scheduled time of system maintenance.	We recommend that you take one of the following actions in response to the event: • Redeploy the instance. For more information, see Redeploy an instance equipped with local disks. • Wait for the instance to be automatically stopped and then perform instance operations such as redeployment based on your business requirements. Note You can modify the maintenance attributes of the instance to specify the default action to take when the instance encounters a maintenance event. For more information, see Instance maintenance attributes.

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you
Scheduled instance redeployment due to system maintenance	SystemMaintenance.Redeploy	Critical	- Instance:SystemMaintenance.Redeploy:Inquiring - Instance:SystemMaintenance.Redeploy:Scheduled - Instance:SystemMaintenance.Redeploy:Executing - Instance:SystemMaintenance.Redeploy:Executed - Instance:SystemMaintenance.Redeploy:Avoided - Instance:SystemMaintenance.Redeploy:Canceled	This system event is triggered 24 or 48 hours before the scheduled time of system maintenance. **Note** Only instances that depend on host hardware support this type of event, such as instances that use local disks or support Software Guard Extensions (SGX) encrypted computing.	We recommend that you make preparations such as modifying the */etc/fstab* configuration file and backing up data, and then take one of the following actions in response to the event: - Redeploy the instance. For more information, see Redeploy an instance equipped with local disks. - Wait for the instance to be automatically redeployed. **Note** You can modify the maintenance attributes of the instance to specify the default action to take when the instance encounters a maintenance event. For more information, see Instance maintenance attributes.

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you
Isolation of damaged local disks due to system maintenance	SystemMaintenance.IsolateErrorDisk	Critical	● Instance:SystemMaintenance.IsolateErrorDisk:Inquiring ● Instance:SystemMaintenance.IsolateErrorDisk:Executing ● Instance:SystemMaintenance.IsolateErrorDisk:Executed ● Instance:SystemMaintenance.IsolateErrorDisk:Avoided ● Instance:SystemMaintenance.IsolateErrorDisk:Failed ● Instance:SystemMaintenance.IsolateErrorDisk:Canceled	This system event is triggered when a local disk is damaged.	We recommend that you make preparations such as modifying the */etc/fstab* configuration file and backing up data, and then select an appropriate point in time to authorize the damaged disk to be isolated. Then, the local disk is isolated online without the need to restart its associated instance. **Note** For more information, see the "Scenario ③" section in O&M scenarios and system events for instances equipped with local disks.

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you
Re-initialization of damaged local disks due to system maintenance	SystemMaintenance.ReInitErrorDisk	Critical	• Instance:SystemMaintenance.ReInitErrorDisk:Inquiring • Instance:SystemMaintenance.ReInitErrorDisk:Executing • Instance:SystemMaintenance.ReInitErrorDisk:Executed • Instance:SystemMaintenance.ReInitErrorDisk:Avoided • Instance:SystemMaintenance.ReInitErrorDisk:Failed • Instance:SystemMaintenance.ReInitErrorDisk:Canceled	This system event is triggered immediately after Alibaba Cloud replaces a damaged local disk of the host where an instance equipped with local disks resides. Typically, the event is triggered within five business days after you authorize the damaged disk to be isolated.	We recommend that you select an appropriate point in time to authorize the local disk to be restored. Then, the local disk is restored online without the need to restart its associated instance. **Note** For more information, see the "Scenario ③" section in O&M scenarios and system events for instances equipped with local disks.

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you
Isolation of damaged local disks and instance restart due to system maintenance	SystemMaintenance.RebootAndIsolateErrorDisk	Critical	• Instance:SystemMaintenance.RebootAndIsolateErrorDisk:Inquiring • Instance:SystemMaintenance.RebootAndIsolateErrorDisk:Executing • Instance:SystemMaintenance.RebootAndIsolateErrorDisk:Executed • Instance:SystemMaintenance.RebootAndIsolateErrorDisk:Avoided • Instance:SystemMaintenance.RebootAndIsolateErrorDisk:Canceled	This system event is triggered when a damaged local disk cannot be isolated online.	We recommend that you select an appropriate point in time to authorize the damaged disk to be isolated and restart the associated instance after the disk is isolated. In this case, the local disk is isolated offline, so you must restart its associated instance for the isolation operation to take effect. **Note** For more information, see the "Scenario ③" section in O&M scenarios and system events for instances equipped with local disks.

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you
Re-initialization of damaged local disks and instance restart due to system maintenance	SystemMaintenance.RebootAndReInitErrorDisk	Critical	- Instance:SystemMaintenance.RebootAndReInitErrorDisk:Inquiring - Instance:SystemMaintenance.RebootAndReInitErrorDisk:Executing - Instance:SystemMaintenance.RebootAndReInitErrorDisk:Executed - Instance:SystemMaintenance.RebootAndReInitErrorDisk:Avoided - Instance:SystemMaintenance.RebootAndReInitErrorDisk:Canceled	This system event is triggered when a damaged local disk cannot be restored online.	We recommend that you select an appropriate point in time to authorize the local disk to be restored and restart the associated instance after the disk is restored. In this case, the local disk is restored offline, so you must restart its associated instance for the restoration operation to take effect. **Note** For more information, see the "Scenario ③" section in O&M scenarios and system events for instances equipped with local disks.

Unexpected O&M events

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you
Instance restart due to a system error	SystemFailure.Reboot	Critical	- Instance:SystemFailure.Reboot:Executing - Instance:SystemFailure.Reboot:Executed - Instance:SystemFailure.Reboot:Failed	This system event is triggered when an instance is restarted due to a system error.	We recommend that you wait for the instance to be automatically restarted and then check whether the instances and applications continue to work as expected. **Note** You can modify the maintenance attributes of the instance to specify the default action to take when the instance encounters a maintenance event. For more information, see Instance maintenance attributes.
Instance restart due to an instance error	InstanceFailure.Reboot	Critical	- Instance:InstanceFailure.Reboot:Executing - Instance:InstanceFailure.Reboot:Executed	This system event is triggered when an instance is restarted due to an instance error.	We recommend that you wait for the instance to be automatically restarted and then check whether the instances and applications continue to work as expected. You can troubleshoot and prevent the error based on the system logs and screenshots of the instance. For more information, see View system logs and screenshots.

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you
Instance stop due to a system error	SystemFailure.Stop	Critical	• Instance:SystemFailure.Stop:Executing • Instance:SystemFailure.Stop:Executed	This system event is triggered when an instance is stopped due to a system error.	We recommend that you wait for the instance to be automatically stopped. ? **Note** You can modify the maintenance attributes of the instance to specify the default action to take when the instance encounters a maintenance event. For more information, see Instance maintenance attributes.

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you
Instance redeployment due to a system error	SystemFailure.Redeploy	Critical	- Instance:SystemFailure.Redeploy:Inquiring - Instance:SystemFailure.Redeploy:Scheduled - Instance:SystemFailure.Redeploy:Executing - Instance:SystemFailure.Redeploy:Executed - Instance:SystemFailure.Redeploy:Avoided - Instance:SystemFailure.Redeploy:Canceled	This system event is triggered when a system error occurs and makes it necessary to redeploy an instance that is equipped with local disks. **Note** Only instances that depend on host hardware support this type of event, such as instances that are equipped with local disks or support SGX encrypted computing.	We recommend that you make preparations such as modifying the */etc/fstab* configuration file and backing up data, and then take one of the following actions in response to the event: - Redeploy the instance. For more information, see Redeploy an instance equipped with local disks. - Wait for the instance to be automatically redeployed. **Note** You can modify the maintenance attributes of the instance to specify the default action to take when the instance encounters a maintenance event. For more information, see Instance maintenance attributes.

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you
Instance release due to a creation failure	SystemFailure.Delete	Critical	- Instance:SystemFailure.Delete:Executing - Instance:SystemFailure.Delete:Executed	This system event is triggered when an instance cannot be created after the order to create the instance is placed.	We recommend that you wait for the instance to be automatically released. Typically, an instance is automatically released within 5 minutes when the instance cannot be created. **Note** If you have paid for the order, the payment is refunded after the instance is released. To ensure that instances can be created, we recommend that you take the following actions: - Before you create ECS instances in a region and zone, query ECS resource availability and the number of idle private IP addresses in the CIDR block associated with a specified vSwitch in the region and zone. For example, you can call the DescribeAvailableResource operation to query resources in a zone. - Use Auto Provisioning or Auto Scaling to flexibly deliver

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you.
					instances from latter resource pools.
Damage alert generated for local disks	ErrorDetected	Critical	• Disk:ErrorDetected:Executing • Disk:ErrorDetected:Executed	This system event is triggered when a local disk is damaged.	We recommend that you make preparations such as modifying the */etc/fstab* configuration file and backing up data, and then have the damaged local disk isolated and restored when appropriate. **Note** For more information, see the "Scenario ③" section in O&M scenarios and system events for instances equipped with local disks.
Disk performance significantly affected	Stalled	Critical	• Disk:Stalled:Executing • Disk:Stalled:Executed	This system event is triggered when the performance of a disk attached to an ECS instance is significantly affected.	We recommend that you isolate reads and writes on the disk at the application layer or disassociate the ECS instance from the associated Server Load Balancer (SLB) instance.
Trusted Platform Module (TPM) security alert	Security.TpmAlert	Warning	• Instance:Security.TpmAlert:Executing • Instance:Security.TpmAlert:Executed	This system event is triggered when an exception about the trusted system occurs on a security-enhanced instance.	We recommend that you view event details in the ECS console to identify the exception cause and troubleshoot the exception. For more information, see Handle trusted exceptions.

Instance billing events

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you
Subscription instance stop on expiration	Instance Expiration.Stop	Critical	● Instance:InstanceExpiration.Stop:Scheduled ● Instance:InstanceExpiration.Stop:Executing ● Instance:InstanceExpiration.Stop:Executed ● Instance:InstanceExpiration.Stop:Avoided	This system event is triggered 3 days before a subscription instance expires and is stopped	We recommend that you renew the instance at your earliest opportunity. For more information, see Renewal overview.
Subscription instance release after expiration	Instance Expiration.Delete	Critical	● Instance:InstanceExpiration.Delete:Scheduled ● Instance:InstanceExpiration.Delete:Executing ● Instance:InstanceExpiration.Delete:Executed ● Instance:InstanceExpiration.Delete:Avoided	This system event is triggered 3 days before an expired subscription instance is automatically released	We recommend that you renew the instance at your earliest opportunity. For more information, see Renewal overview.
Pay-as-you-go instance stop due to overdue payments	Account Unbalanced.Stop	Critical	● Instance:AccountUnbalanced.Stop:Scheduled ● Instance:AccountUnbalanced.Stop:Executing ● Instance:AccountUnbalanced.Stop:Executed ● Instance:AccountUnbalanced.Stop:Avoided	This system event is triggered 1 hour before a pay-as-you-go instance is stopped due to an overdue payment	We recommend that you maintain a sufficient balance within your payment account to prevent instances from being stopped.

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you
Pay-as-you-go instance release due to overdue payments	AccountUnbalanced.Delete	Critical	- Instance:AccountUnbalanced.Delete:Scheduled - Instance:AccountUnbalanced.Delete:Executing - Instance:AccountUnbalanced.Delete:Executed - Instance:AccountUnbalanced.Delete:Avoided	This system event is triggered 3 days before a pay-as-you-go instance is automatically released due to an overdue payment	We recommend that you maintain a sufficient balance within your payment account to prevent instances from being released.
Disk release due to overdue payments	Undefined	Critical	Disk:OverduePaymentRelease	This system event is triggered when a pay-as-you-go disk is automatically released due to an overdue payment.	We recommend that you maintain a sufficient balance within your payment account to prevent disks from being released.

State change events

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you
Preemptible instance interruption	Undefined	Warning	Instance:PreemptibleInstanceInterruption	This system event is triggered 5 minutes before a preemptible instance is reclaimed.	We recommend that you take one of the following actions: ● Use preemptible instances for stateless applications, such as scalable web services and big data analytics applications. ● Use Auto Provisioning to deliver instances and mitigate the impacts of reclaimed preemptible instances on your business. You can also implement automated O&M based on this event. For example, you can configure notifications about this event in the CloudMonitor console and have preemptible instances automatically purchased when a notification is sent.
					We recommend that you take one of the following actions in response to the event: ● If you want the burstable instance to run at a CPU utilization higher than the baseline for a short period of time, enable the unlimited mode for the

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you
Burstable instance performance limited to the baseline level due to insufficient CPU credits	Undefined	Warning	Instance:BurstablePerformanceRestricted	This system event is triggered when all accrued CPU credits of a burstable instance are consumed.	instance for that period. For more information, see Switch the performance mode of a burstable instance. • If you want the burstable instance to run at a CPU utilization higher than the baseline for a long time, upgrade the instance to a higher-specification instance type or change the instance into a non-burstable instance. For more information, see Change instance types. If you want to specify thresholds for triggering notifications about this event, for example, if you want an event notification to be sent when accrued CPU credits remain less than 10 for consecutive 10 minutes, you can configure event-triggered alert rules for the event in the CloudMonitor console. For more information, see Monitor burstable instances.

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you
Performance mode change of burstable instances	Undefined	Warning	Instance:PerformanceModeChange	This system event is triggered when a burstable instance switches between the unlimited and standard modes.	We recommend that you determine whether to follow the event. If you want to follow the event, you can configure notifications about the event in the CloudMonitor console. For more information, see Configure event notifications.
Instance state change	Undefined	Notification	Instance:StateChange	This system event is triggered when the state of an instance changes, such as from Running to Stopping and from Stopping to Stopped.	We recommend that you determine whether to follow the event. If you want to follow the event, you can configure notifications about the event in the CloudMonitor console. For more information, see Configure event notifications.
Automatic instance reactivation	Undefined	Notification	Instance:AutoReactivateCompleted	This system event is triggered when an instance is automatically reactivated while overdue payments in your account are settled.	We recommend that you determine whether to follow the event. If you want to follow the event, you can configure notifications about the event in the CloudMonitor console. For more information, see Configure event notifications.

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you
Hot migration of instances between dedicated hosts	Undefined	Notification	Instance:LiveMigrationAcrossDDH	This system event is triggered when an instance is hot migrated between dedicated hosts.	We recommend that you determine whether to follow the event. If you want to follow the event, you can configure notifications about the event in the CloudMonitor console. For more information, see Configure event notifications.
Disk operations completed	Undefined	Notification	Disk:DiskOperationCompleted	This system event is triggered when a pay-as-you-go disk is manually attached or detached.	We recommend that you determine whether to follow the event. If you want to follow the event, you can configure notifications about the event in the CloudMonitor console. For more information, see Configure event notifications.
Disk billing method change from subscription to pay-as-you-go	Undefined	Notification	Disk:ConvertToPostpaidCompleted	This system event is triggered when a subscription disk is changed to a pay-as-you-go disk.	We recommend that you determine whether to follow the event. If you want to follow the event, you can configure notifications about the event in the CloudMonitor console. For more information, see Configure event notifications.

Event description	ECS event type	Event severity	CloudMonitor event	Time when a system event is triggered	Handling suggestion for you
Disk snapshot created	Undefined	Notification	Snapshot:CreateSnapshotCompleted	This system event is triggered when a snapshot is created for a disk.	We recommend that you determine whether to follow the event. If you want to follow the event, you can configure notifications about the event in the CloudMonitor console. For more information, see Configure event notifications.

Related information

- Formats of ECS event type and CloudMonitor event names
- Query and handle ECS system events
- View system event history
- Subscribe to system event notifications

2.3. Response process of system events

2.3.1. Query and handle ECS system events

This topic describes how to use the Elastic Compute Service (ECS) console and Alibaba Cloud CLI to query and handle ECS system events.

Context

You can view and handle ECS system events in the ECS console. You can also view systems events of ECS and other Alibaba Cloud services and configure notifications about system events in the CloudMonitor console. For more information, see View system events and Set event notifications.

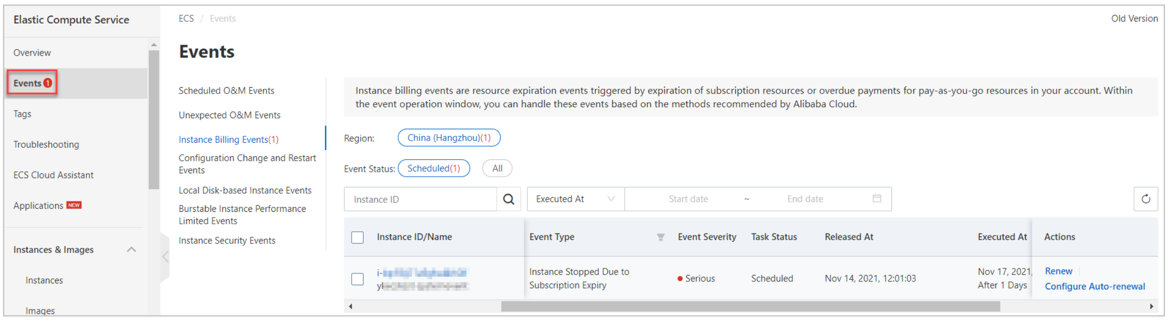
View and handle system events on the Events page in the ECS console

You can view system events of all instances on the Events page in the ECS console.

1.
2.
3.
4.

5. View pending system events.

   If a number appears next to a category of system events, it indicates that some events of that category are pending. Different handling methods are recommended for different system events. For example, we recommend that you renew an instance in response to the event that the instance has expired, and we recommend that you repair a damaged local disk in response to the event that the local disk is damaged. You can manually execute the O&M task related to an event as instructed in the ECS console, or wait for the task to be automatically executed.



Instance billing events are resource expiration events triggered by expiration of subscription resources or overdue payments for pay-as-you-go resources in your account. Within the event operation window, you can handle these events based on the methods recommended by Alibaba Cloud.

Region: China (Hangzhou)(1)

Event Status: Scheduled(1) All

□	Instance ID/Name	Event Type	Event Severity	Task Status	Released At	Executed At	Actions
□	[redacted]	Instance Stopped Due to Subscription Expiry	● Serious	Scheduled	Nov 14, 2021, 12:01:03	Nov 17, 2021, After 1 Days	Renew Configure Auto-renewal

View and handle system events on the Instance Details page in the ECS console

You can view system events of an instance on the Instance Details page in the ECS console.

1.

2.

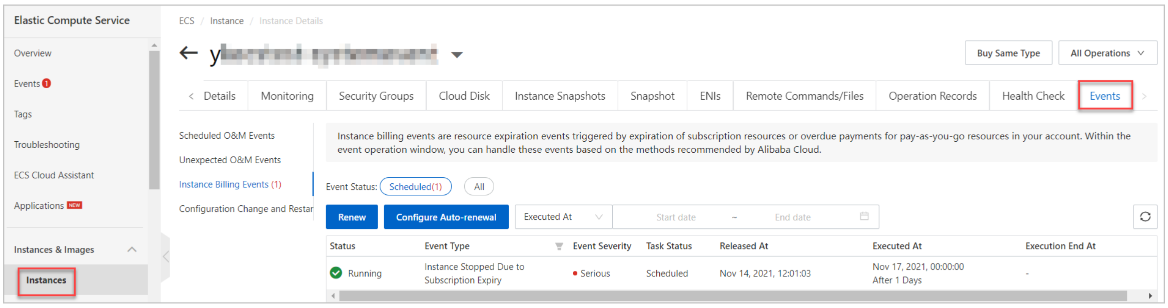
3.

4. Find the instance whose system events that you want to view and click **Manage** in the **Actions** column.

5. Click the **Events** tab.

6. View pending system events.

   If a number appears next to a category of system events, it indicates that some events of that category are pending. Different handling methods are recommended for different system events. For example, we recommend that you renew an instance in response to the event that the instance has expired, and we recommend that you repair a damaged local disk in response to the event that the local disk is damaged. You can manually execute the O&M task related to an event as instructed in the ECS console, or wait for the task to be automatically executed.



[redacted]

Instance billing events are resource expiration events triggered by expiration of subscription resources or overdue payments for pay-as-you-go resources in your account. Within the event operation window, you can handle these events based on the methods recommended by Alibaba Cloud.

Event Status: Scheduled(1) All

Status	Event Type	Event Severity	Task Status	Released At	Executed At	Execution End At
✓ Running	Instance Stopped Due to Subscription Expiry	● Serious	Scheduled	Nov 14, 2021, 12:01:03	Nov 17, 2021, 00:00:00 After 1 Days	-

Query and handle system events by using Alibaba Cloud CLI

You can use Alibaba Cloud CLI to call API operations. For more information, see What is Alibaba Cloud CLI? This section describes a sample procedure to query and handle system events by calling API operations in Alibaba Cloud CLI.

1. Call the DescribeInstances operation to obtain the ID of an instance.

   ```
   aliyun ecs DescribeInstances --RegionId <TheRegionId> --output cols=InstanceId,InstanceName rows=Instances.Instance[]
   ```

2. Call the DescribeInstanceHistoryEvents operation to query the system events of the instance.

   - Query system events in the Scheduled state.

     ```
     aliyun ecs DescribeInstanceHistoryEvents --RegionId <TheRegionId> --InstanceId <YourInstanceId> --InstanceEventCycleStatus.1 Scheduled --output cols=EventId,EventTypeName rows=rows=InstanceSystemEventSet.InstanceSystemEventType[]
     ```

   - Query system events in the Scheduled, Inquiring, Executing, Executed, Avoided, Canceled, and Failed states.

     ```
     aliyun ecs DescribeInstanceHistoryEvents --RegionId <TheRegionId> --InstanceId <YourInstanceId> --InstanceEventCycleStatus.1 Scheduled --InstanceEventCycleStatus.2 Inquiring  --InstanceEventCycleStatus.3 Executing  --InstanceEventCycleStatus.4 Executed  --InstanceEventCycleStatus.5 Canceled  --InstanceEventCycleStatus.6 Avoided --InstanceEventCycleStatus.7 Failed --output cols=EventId,EventTypeName rows=rows=InstanceSystemEventSet.InstanceSystemEventType[]
     ```

   - Query system events in the Executed, Avoided, Canceled, and Failed states.

     ```
     aliyun ecs DescribeInstanceHistoryEvents --RegionId <TheRegionId> --InstanceId <YourInstanceId> --output cols=EventId,EventTypeName rows=rows=InstanceSystemEventSet.InstanceSystemEventType[]
     ```

   - Query system events in the Scheduled, Inquiring, and Executing states.

     ```
     aliyun ecs DescribeInstanceHistoryEvents --RegionId <TheRegionId> --InstanceId <YourInstanceId> --InstanceEventCycleStatus.1 Scheduled --InstanceEventCycleStatus.2 Inquiring --InstanceEventCycleStatus.3 Executing --output cols=EventId,EventTypeName rows=rows=InstanceSystemEventSet.InstanceSystemEventType[]
     ```

3. Select appropriate methods to handle the events and optionally call corresponding API operations.

   Examples:

   - For a system event in the Inquiring state, call the AcceptInquiredSystemEvent operation to authorize Alibaba Cloud to execute the O&M task related to the event, or ignore the event.
   - For a system event that an instance is scheduled to be redeployed, call the RedeployInstance operation to redeploy the instance, or wait for the instance to be automatically redeployed.
   - For a system events that a subscription instance has expired, call the RenewInstance operation to renew the instance, or wait for the instance to be automatically stopped and released.

Allow ECS event notifications to be received

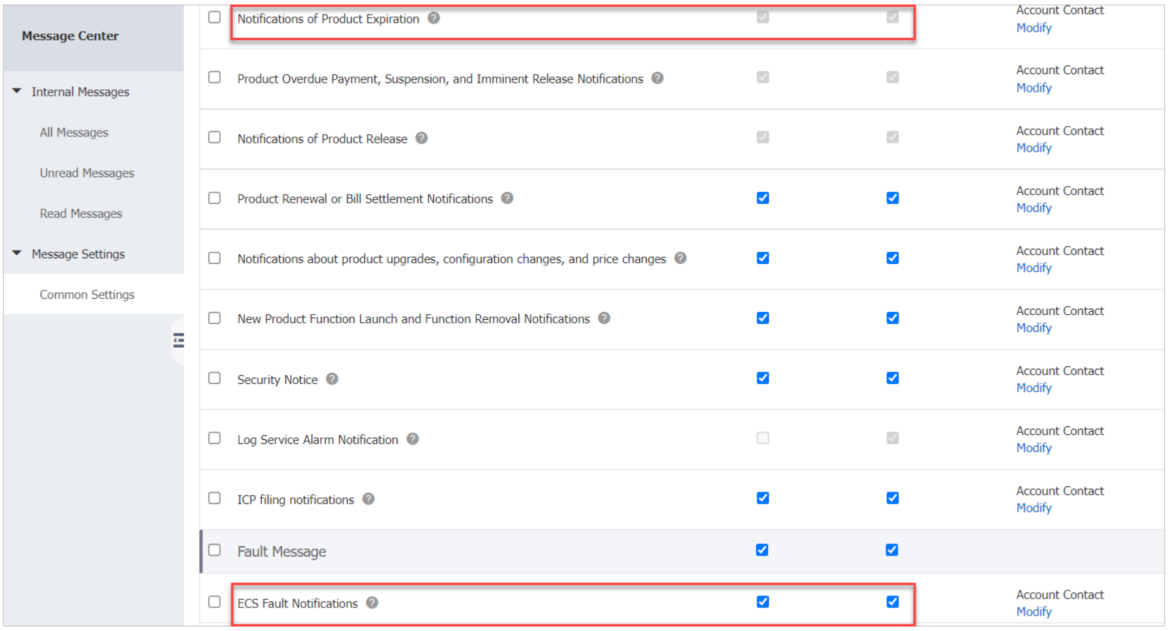
If you want to receive event notifications by internal message or by email, you must allow notifications to be received, such as resource expiration notifications, O&M notifications, and fault notifications, in the Message Center.

1.

2. In the right part of the top navigation bar, move the pointer over the 🔔 icon and click **Message Settings**.

3. In the Message Center, choose **Message Settings > Common Settings** to go the Common Settings page, find the notification types that you want, and then select one or more notification methods that suit your business requirements.

   Example notification types: Product operation notifications, Notifications of Product Expiration, and ECS Fault Notifications.



Message Center
- Internal Messages
  - All Messages
  - Unread Messages
  - Read Messages
- Message Settings
  - Common Settings

□	Notifications of Product Expiration	☑	☑	Account Contact Modify
□	Product Overdue Payment, Suspension, and Imminent Release Notifications	☑	☑	Account Contact Modify
□	Notifications of Product Release	☑	☑	Account Contact Modify
□	Product Renewal or Bill Settlement Notifications	☑	☑	Account Contact Modify
□	Notifications about product upgrades, configuration changes, and price changes	☑	☑	Account Contact Modify
□	New Product Function Launch and Function Removal Notifications	☑	☑	Account Contact Modify
□	Security Notice	☑	☑	Account Contact Modify
□	Log Service Alarm Notification	□	☑	Account Contact Modify
□	ICP filing notifications	☑	☑	Account Contact Modify
□	Fault Message	☑	☑	
□	ECS Fault Notifications	☑	☑	Account Contact Modify

2.4. Perform O&M based on system events

2.4.1. Overview

This topic provides an overview of Elastic Compute Service (ECS) event notifications. Event notifications provide information about resource changes. Notifications can be sent for the following events: system events (including O&M events and exceptions), instance status changes, events that data disks are attached or detached, and events that snapshots are created. Event notifications enable you to configure the message processing middleware for events to implement event-driven automated O&M in place of SDK polling.

Event notification name

After you configure notifications for events, you can receive corresponding notifications when the events occur. The name field of a notification indicates the code name of the event. This field is in the *<resource type>:<event>:<status>* format.

- <resource type>: the type of the corresponding ECS resource. Example values: *Instance* and *Disk*. Instance indicates ECS instances and Disk indicates Elastic Block Storage (EBS) devices.
- <event>: the name of the event. Example values: *SystemMaintenance.Reboot*, *StateChange*, *PreemptibleInstanceInterruption*, *DiskOperationCompleted*, and *CreateSnapshotCompleted*.
- <status>: the status of the event. For information about the valid values of this field, see Overview.

> **Note** The <status> field is available only for system events related to instances and EBS devices.

Event notification format

After event notifications are configured, ECS sends the notifications based on the method that you specified. The following example shows a non-customized event notification in the JSON format. This notification is sent for the event that the state of an ECS instance changes.

> **Note** If the notification method that you set supports format conversion, the notification that you receive may be converted to other formats.

```
{
    "eventTime": "20181226T220114.058+0800",
    "id": "9435EAD6-3CF6-4494-8F7A-3A********77",
    "level": "INFO",
    "name": "Instance:StateChange",
    "product": "ECS",
    "regionId": "cn-hangzhou",
    "resourceId": "acs:ecs:cn-hangzhou:169070********30:instance/i-bp1ecr********5go2go",
    "userId": "169070********30",
    "ver": "1.0",
    "content": {
        "resourceId": "i-bp1ecr********5go2go",
        "resourceType": "ALIYUN::ECS::Instance",
        "state": "Stopping"
    }
}
```

The following table describes fixed top-level fields in a notification.

Field	Description	Example
id	The ID of the event.	*9435EAD6-3CF6-4494-8F7A-3A********77*
eventTime	The time when the event occurred (UTC+8).	*20181226T220114.058+0800*
level	The level of the event. Valid values: - *INFO* - *WARN* - *CRITICAL*	*INFO*
name	The name of the event. For more information, see the Event notification name section.	*Instance:StateChange*
product	The name of the service. Valid value: ECS.	*ECS*

Field	Description	Example
regionId	The ID of the region where the event occurred. For more information about the valid values of this field, see Regions and zones.	*cn-hangzhou*
resourceId	The Alibaba Cloud Resource Name (ARN) of the resource.	*acs:ecs:cn-hangzhou:169070********30:instance/i-bp1ecr********5go2go*
userId	The ID of the Alibaba Cloud account.	*169070********30*
content	The event details. This field can contain one or more subfields. For more information about the subfields, see the following topics: • Instance event notification • EBS event notifications • Snapshot event notifications • ENI operation event notifications	None

Related information

References

- Configure event notifications
- PutEventRule

2.4.2. Configure event notifications

To ensure the stable running of your business in Elastic Compute Service (ECS) and implement automated O&M, we recommend that you configure event notifications to monitor changes in the underlying environments. This topic describes how to create system event-triggered alert rules in the CloudMonitor console to automatically push event notifications. This can help you keep track of events.

Context

CloudMonitor is a service that monitors Internet applications and Alibaba Cloud resources. It allows you to manage, monitor, and query system events that are generated for different Alibaba Cloud services to keep track of service usage and receive alert notifications in a timely manner.

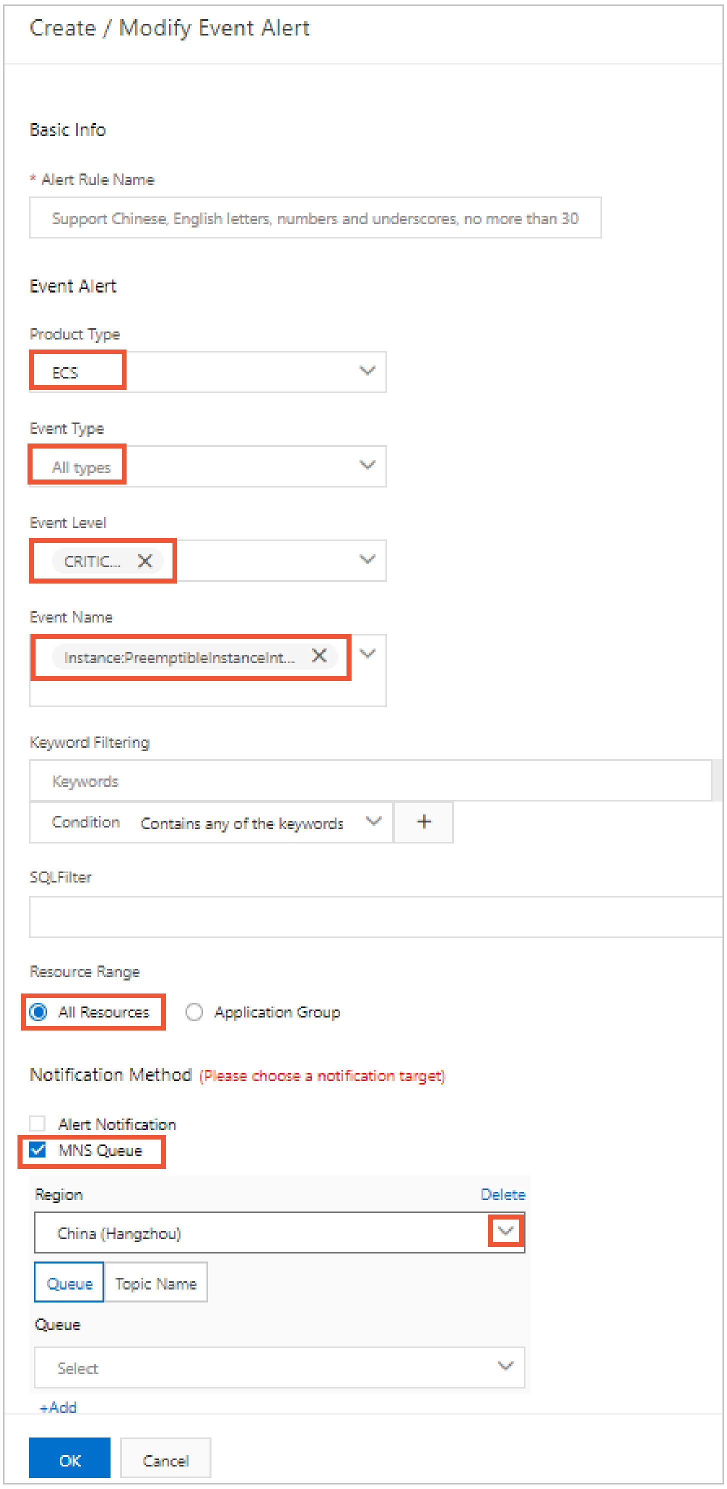
You can use CloudMonitor to configure alert rules so that you are notified when system events occur. CloudMonitor supports different alert notification methods.

- CloudMonitor can send alert notifications by using text messages, emails, or DingTalk chatbots.
- CloudMonitor can push events to Message Service (MNS), Function Compute, Log Service, or the specified callback URL. This allows you to automate the exception handling process based on your business requirements.

Configure event notifications

Notice If you want to apply alert rules to instances in a specified application group, make sure that the application group contains member instances. For more information, see Create an application group and Add resources to the application group.

1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, choose **Event Monitoring** > **System Event**.
3. On the **System Event** page, click the **Event Alert** tab. On the Event Alert tab, click **Create Alert Rule**.
4. In the **Create / Modify Event Alert** panel, set parameters to configure event notifications.



Create / Modify Event Alert

Basic Info

* Alert Rule Name

Support Chinese, English letters, numbers and underscores, no more than 30

Event Alert

Product Type: ECS

Event Type: All types

Event Level: CRITIC...

Event Name: Instance:PreemptibleInstanceInt...

Keyword Filtering: Keywords

Condition: Contains any of the keywords

SQLFilter

Resource Range: ● All Resources ○ Application Group

Notification Method (Please choose a notification target)

□ Alert Notification

☑ MNS Queue

Region: China (Hangzhou)

Queue

Select

The following table describes the parameters. For more information, see Create a system event-triggered alert rule.

Section	Parameter	Description
Basic Info	Alert Rule Name	Enter a name for the alert rule as instructed.
	Product Type	Select **ECS** from the drop-down list.

Section	Parameter	Description
Event Alert	Event Type	Select one or more event types to which you want to subscribe from the drop-down list. Valid values: **Status Notification**, **Exception**, and **Maintenance**.
	Event Level	Select one or more event levels to which you want to subscribe from the drop-down list. Valid values: **CRITICAL** (*CRITICAL*), **WARN** (*WARN*), and **INFO** (*INFO*).
	Event Name	Select one or more event names as needed from the drop-down list. ⓘ **Note** We recommend that you do not select **All Events**. We recommend that you create different event-triggered alert rules based on the impacts of different events on your business.
	Resource Range	If you select **All Resources**, CloudMonitor sends alert notifications for events of all resources based on your configurations.
Notification Method	Notification Method	Set the notification method. When an event occurs, a corresponding event notification is sent by using text messages, emails, or DingTalk chatbots. Select notification methods as needed. ⓘ **Note** Events whose level is **INFO**(*INFO*) occur frequently. We recommend that you do not set Event Level to *INFO* to prevent being disturbed by a large number of notifications.
	Notification message processing middleware	Set the notification message processing middleware. To automate event processing, you can select MNS Queue, Function Compute, URL Callback, and Log Service. If you select URL Callback, you can set Request Method to GET or POST.
	Mute for	Select the interval at which CloudMonitor resends alert notifications. After an alert is triggered, CloudMonitor resends alert notifications at the specified interval before the alert is cleared.

5. Click **OK**.

   After the event notifications are configured, ECS sends notifications based on the specified notification methods. The following example shows a non-customized event notification in the JSON format. The notification is sent when the state of the ECS instance changes.

```
{
    "eventTime": "20181226T220114.058+0800",
    "id": "9435EAD6-3CF6-4494-8F7A-3A********77",
    "level": "INFO",
    "name": "Instance:StateChange",
    "product": "ECS",
    "regionId": "cn-hangzhou",
    "resourceId": "acs:ecs:cn-hangzhou:169070********30:instance/i-bp1ecr********5go2go
",
    "userId": "169070********30",
    "ver": "1.0",
    "content": {
        "resourceId": "i-bp1ecr********5go2go",
        "resourceType": "ALIYUN::ECS::Instance",
        "state": "Stopping"
    }
}
```

For more information about event notifications, see the following topics:

- Instance event notification
- EBS event notifications
- Snapshot event notifications
- ENI operation event notifications

Test the alert rule

After you create a system event-triggered alert rule, you can test the alert rule. You can check whether alert notifications can be received or whether events can be pushed to MNS, Function Compute, Log Service, or the specified callback URL as configured.

References

In CloudMonitor, you can associate subsequent processing methods (such as MNS queues) with alert rules to automatically handle the state change events of ECS instances. For more information, see Automate O&M based on status change events of ECS instances.

2.4.3. Send event notifications by using a DingTalk chatbot

This topic describes how to use a DingTalk chatbot to send event notifications to a DingTalk group. You can understand the system events related to Elastic Compute Service (ECS) instances from the DingTalk group and handle the exceptions that occur when instances are running.

Context

Various system events may be generated when instances are running, such as events about instance state changes and O&M events. Some system events indicate that exceptions occur when instances are running. O&M personnel must be aware of the system events in a timely manner. If O&M personnel have a DingTalk group for communication, a DingTalk chatbot can be used to automatically send event notifications to the DingTalk group so that O&M personnel can handle exceptions that have occurred in a quick manner.

In the following procedure, a DingTalk chatbot and CloudMonitor are used:

1. Create a DingTalk chatbot for a DingTalk group.
2. Use the webhook URL of the DingTalk chatbot as the contact information of the CloudMonitor alert contact.
3. When you configure an CloudMonitor alert rule, select the alert group that includes the corresponding alert contact to receive alert notifications.

After the preceding manual operations are complete, the following procedure is automatically performed to send a notification:

1. When the underlying service of Alibaba Cloud detects a system event on an ECS instance (such as an event about instance state changes or an O&M event), the service pushes the event to the event center of CloudMonitor.
2. CloudMonitor sends a notification to the alert group based on your configured alert rules. The contact information of the alert contact in this group includes the webhook URL of the DingTalk chatbot.
3. When the DingTalk chatbot detects an event, the chatbot sends a notification in the DingTalk group.

Step 1: Create a DingTalk chatbot

A webhook URL is generated after a DingTalk chatbot is created. The webhook URL can be associated with other services such as CloudMonitor to receive notifications.

1. Start DingTalk and go to the DingTalk group in which you want to receive alert notifications.
2. Go to the chatbot settings page.

   i. Click the Group Settings icon (⚙) in the upper-right corner of the DingTalk group.

   ii. In the **Group Settings** panel, click **Group Assistant**.

   iii. In the **Group Assistant** panel, click **Add Robot**.

   iv. In the **Add Robot** section of the **ChatBot** dialog box, click the + icon.

   v. In the **Please choose which robot to add** section, click **Custom**.

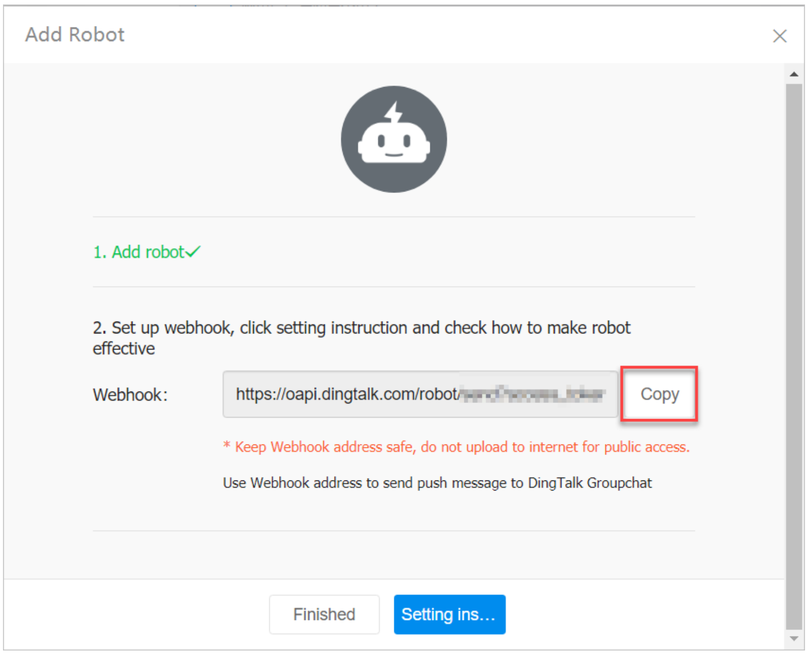
   vi. In the **Robot details** dialog box, click **Add**.

3. Configure the DingTalk chatbot as prompted.

   You must select at least one security setting. In this example, **Custom Keywords** is selected for Security Settings. If you select Custom Keywords, you must enter one or more keywords. When you use the DingTalk chatbot later, the DingTalk chatbot sends alert notifications to the DingTalk group only if the notifications contain at least one of the keywords.

   For example, when CloudMonitor sends an event notification, the notification contains `CloudMonitor`. In this example, `CloudMonitor` is used as a keyword.

4. Copy and save the webhook URL of the DingTalk chatbot.



Add Robot

1. Add robot✓

2. Set up webhook, click setting instruction and check how to make robot effective

Webhook: https://oapi.dingtalk.com/robot/[redacted]

* Keep Webhook address safe, do not upload to internet for public access.

Use Webhook address to send push message to DingTalk Groupchat

Step 2: Associate the DingTalk chatbot with an alert rule

This section focuses on how to associate a DingTalk chatbot with an alert rule. For more information about the detailed operations, see Create an alert contact or alert contact group and Create a system event-triggered alert rule.

1. Log on to the CloudMonitor console.
2. Create an alert contact.
   i. In the left-side navigation pane, choose **Alerts > Alert Contacts**.
   ii. On the Alert Contacts tab, click **Create Alert Contact**.
   iii. In the **Set Alert Contact** panel, configure the alert contact as prompted.

      To associate the DingTalk bot, enter the webhook URL obtained in Step 1: Create a DingTalk chatbot in the **Webhook or DingTalk Robot** section.
3. Create an alert group.
   i. Click the **Alert Contact Group** tab.
   ii. Click **Create Alert Contact Group**.
   iii. In the **Create Alert Contact Group** panel, configure the alert group as prompted.

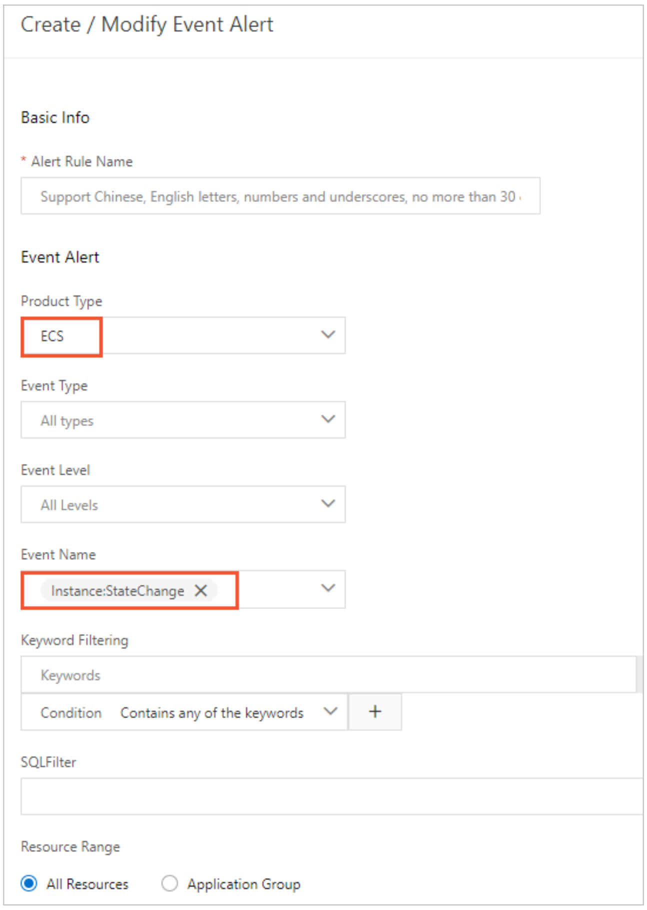
      To associate the DingTalk chatbot, add the alert contact you created to the alert group.
4. Create an alert rule.
   i. In the left-side navigation pane, choose **Event Monitoring > System Event**.
   ii. Click the **Event Alert** tab.
   iii. Click **Create Alert Rule**.

iv. In the **Create/Modify Event Alert** panel, configure the alert rule as prompted.

Take note of the following items:

- In this example, an event about an ECS instance state change is used. The following figure shows how to configure an alert rule for the event.

> **Note** The event level of the instance state change is INFO. A large number of notifications may be sent for this type of event at a high frequency. Select the event that you want to be notified of based on your business requirements.



Create / Modify Event Alert

Basic Info

* Alert Rule Name

Support Chinese, English letters, numbers and underscores, no more than 30 ·

Event Alert

Product Type: ECS

Event Type: All types

Event Level: All Levels

Event Name: Instance:StateChange ✕

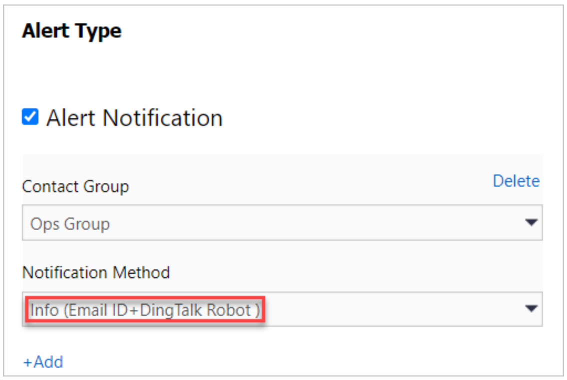
Keyword Filtering: Keywords

Condition: Contains any of the keywords +

SQLFilter

Resource Range: ● All Resources ○ Application Group

- The notification methods must include the DingTalk chatbot, as shown in the following figure.



Alert Type

☑ Alert Notification

Contact Group: Ops Group

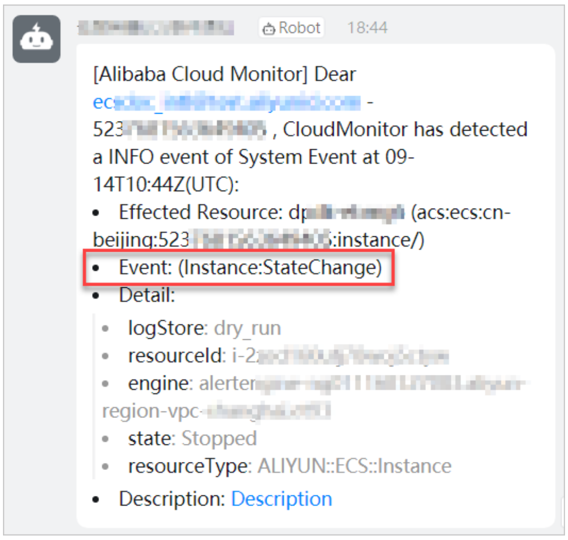
Delete

Notification Method: Info (Email ID+DingTalk Robot)

+Add

Example of an event notification in a DingTalk Group

After the settings are complete, you can change the state of an instance and check whether an event notification is received in your DingTalk group. For example, when you stop an instance, an event notification is received, as shown in the following figure.



[redacted] Robot 18:44

[Alibaba Cloud Monitor] Dear ec[redacted] - 523[redacted] , CloudMonitor has detected a INFO event of System Event at 09-14T10:44Z(UTC):

- Effected Resource: dp[redacted] (acs:ecs:cn-beijing:523[redacted]:instance/)
- Event: (Instance:StateChange)
- Detail:
  - logStore: dry_run
  - resourceId: i-2[redacted]
  - engine: alerten[redacted]-region-vpc-[redacted]
  - state: Stopped
  - resourceType: ALIYUN::ECS::Instance
- Description: Description

2.4.4. Event notification list

2.4.4.1. Instance event notification

Elastic Compute Service (ECS) can send notifications for instance events such as system events, instance state changes, and release of preemptible instances.

Events

ECS can send notifications for the following instance events:

- System events
- Instance state changes
- Release of a preemptible instance
- Hot migration of ECS instances between dedicated hosts
- Changes in the performance mode of burstable instances
- Limited performance of burstable instances

System events

When a system event occurs on an instance, ECS sends an initial notification for the event, and sends subsequent notifications every time the event state changes. For the names of notifications for system events, see Appendix: Notifications for instance-related system events.

The following examples show notifications in the JSON format for an **Instance restart due to system maintenance** (*SystemMaintenance.Reboot*) event.

- The initial notification indicates that the event is in the **Scheduled** (*Scheduled*) state.

```
{
  "ver": "1.0",
  "id": "2256A988-0B26-4E2B-820A-8A********E5",
  "product": "ECS",
  "resourceId": "acs:ecs:cn-hangzhou:169070********30:instance/i-bp1ecr********5go2go",
  "level": "CRITICAL",
  "name": "Instance:SystemMaintenance.Reboot:Scheduled",
  "userId": "169070********30",
  "eventTime": "20190409T121826.922+0800",
  "regionId": "cn-hangzhou",
  "content": {
    "eventId": "e-bp11trd********pqum2",
    "publishTime": "2019-04-09T04:18:26Z",
    "notBefore": "2019-04-12T01:01:01Z",
    "instanceId": "i-bp1ecr********5go2go",
    "eventType": "SystemMaintenance.Reboot",
    "eventStatus": "Scheduled"
  }
}
```

- If you restart the instance before the time specified by the notBefore subparameter, the system event is avoided and ECS sends a notification to indicate that the event state is changed to **Avoided** (*Avoided*).

```
{
  "ver": "1.0",
  "id": "2256A988-0B26-4E2B-820A-8A********E5",
  "product": "ECS",
  "resourceId": "acs:ecs:cn-hangzhou:169070********30:instance/i-bp1ecr********5go2go",
  "level": "CRITICAL",
  "name": "Instance:SystemMaintenance.Reboot:Scheduled",
  "userId": "169070********30",
  "eventTime": "20190410T160101.922+0800",
  "regionId": "cn-hangzhou",
  "content": {
    "eventId": "e-bp11trdr********qum2",
    "publishTime": "2019-04-09T04:18:26Z",
    "notBefore": "2019-04-12T01:01:01Z",
    "instanceId": "i-bp1ecr********5go2go",
    "eventType": "SystemMaintenance.Reboot",
    "eventStatus": "Avoided",
    "executeStartTime": "2019-04-10T08:01:01Z",
    "executeFinishTime": "2019-04-10T08:01:01Z"
  }
}
```

The following table describes the subparameters contained in the content parameter.

Subparameter	Description	Example
eventId	The ID of the system event.	*e-t4navn7********6x5no*
publishTime	The time when the system event is published.	*2019-04-09T04:18:26Z*

Subparameter	Description	Example
notBefore	The scheduled start time of the event. This subparameter is available only for system maintenance events.	*2019-04-12T01:01:01Z*
instanceId	The ID of the affected instance.	*i-bp1ecr********5go2go*
eventType	The type of the system event. For more information about the subparameter values, see Overview.	*SystemMaintenance.Reboot*
eventStatus	The state of the system event. For more information about the subparameter values, see Overview.	*Avoided*
executeStartTime	The start time of the system event. The time is in UTC.	*2019-04-10T08:01:01Z*
executeFinishTime	The end time of the system event. The time is in UTC. **Note** The executeStartTime and and executeFinishTime subparameters are available only for events in the **Executing** (*Executing*), **Executed** (*Executed*), **Canceled** (*Canceled*), or **Avoided** (*Avoided*) state.	*2019-04-10T08:01:01Z*

Instance state changes

When the state of your instance changes, ECS sends you an event notification. For more information about instance state changes, see Instance lifecycle.

The following example shows a notification for the event that the state of an instance changes to **Running** (*Running*):

```
{
  "ver": "1.0",
  "id": "2256A988-0B26-4E2B-820A-8A********E5",
  "product": "ECS",
  "resourceId": "acs:ecs:cn-hangzhou:169070********30:instance/i-bp1ecr********5go2go",
  "level": "INFO",
  "name": "Instance:StateChange",
  "userId": "169070********30",
  "eventTime": "20190409T121826.922+0800",
  "regionId": "cn-hangzhou",
  "content": {
    "resourceId": "i-bp1ecr********5go2go",
    "resourceType": "ALIYUN::ECS::Instance",
    "state": "Running"
  }
}
```

The following table describes the subparameters contained in the content parameter.

Subparameter	Description	Example
resourceId	The ID of the instance.	*i-bp1ecr********5go2go*
resourceType	The type of the resource. Set the value to *ALIYUN::ECS::Instance*.	*ALIYUN::ECS::Instance*
state	The state of the instance. Valid values: ● *Created*: The instance is created. This event notification is sent only once after the instance is created. ● *Starting*: The instance is being started. ● *Running*: The instance is running. ● *Stopping*: The instance is being stopped or restarted. ● *Stopped*: The instance is stopped. ● *Deleted*: The instance is released.	*Running*

Release of a preemptible instance

Preemptible instances may be released due to fluctuations in market prices or insufficient resources. Five minutes before a preemptible instance is released, ECS sends an event notification to warn you about the interruption of the instance. For more information, see Overview.

The following example shows such an event notification in the JSON format:

```
{
  "ver": "1.0",
  "id": "2256A988-0B26-4E2B-820A-8A********E5",
  "product": "ECS",
  "resourceId": "acs:ecs:cn-hangzhou:169070********30:instance/i-bp1ecr********5go2go",
  "level": "INFO",
  "name": "Instance:PreemptibleInstanceInterruption",
  "userId": "169070********30",
  "eventTime": "20190409T121826.922+0800",
  "regionId": "cn-hangzhou",
  "content": {
    "instanceId": "i-bp1ecr********5go2go",
    "action": "delete"
  }
}
```

The following table describes the subparameters contained in the content parameter.

Subparameter	Description	Example
instanceId	The ID of the preemptible instance.	*i-bp1ecr********5go2go*
action	The operation on the preemptible instance. Set the value to *delete*.	*delete*

Hot migration of ECS instances between dedicated hosts

You can call the ModifyInstanceDeployment operation to perform hot migration of ECS instances between dedicated hosts. Hot migration of ECS instances is asynchronous, and the states of the ECS instances do not change during the migration. You can configure notifications for the *Instance:LiveMigrationAcrossDDH* event to receive updates about the migration progress.

The following examples show the event notifications in the JSON format.

- Notification for the event that the hot migration starts:

```
{
  "ver": "1.0",
  "id": "2256A988-0B26-4E2B-820A-8A0580D0B8E5",
  "product": "ECS",
  "resourceId": "acs:ecs:cn-hangzhou:169070********30:instance/i-bp1ecr********5go2go",
  "level": "INFO",
  "instanceName": "instance-event-subscription",
  "name": "Instance:LiveMigrationAcrossDDH",
  "userId": "169070********30",
  "eventTime": "20180608T092537.922+0800",
  "regionId": "cn-hangzhou",
  "content": {
      "instanceId" : "i-bp1ecr********5go2go",
      "sourceDedicatedHostId" : "dh-2ze3lm********t8nr82",
      "destinationDedicatedHostId" : "dh-2ze3lm********t8nr83",
      "startTime" : "2018-06-08T01:25:37Z",
      "status" : "started"
  }
}
```

- Notification for the event that the hot migration is complete:

```
{
  "ver": "1.0",
  "id": "2256A988-0B26-4E2B-820A-8A0580D0B8E5",
  "product": "ECS",
  "resourceId": "acs:ecs:cn-hangzhou:169070********30:instance/i-bp1ecr********5go2go",
  "level": "INFO",
  "instanceName": "instance-event-subscription",
  "name": "Instance:LiveMigrationAcrossDDH",
  "userId": "169070********30",
  "eventTime": "20180608T092545.922+0800",
  "regionId": "cn-hangzhou",
  "content": {
      "instanceId" : "i-bp1ecr********5go2go",
      "sourceDedicatedHostId" : "dh-2ze3lm********t8nr82",
      "destinationDedicatedHostId" : "dh-2ze3lm********t8nr83",
      "startTime" : "2018-06-08T01:25:37Z",
      "endTime" : "2018-06-08T01:25:45Z",
      "status" : "accomplished"
  }
}
```

- Notification for the event that the hot migration fails:

```
{
  "ver": "1.0",
  "id": "2256A988-0B26-4E2B-820A-8A0580D0B8E5",
  "product": "ECS",
  "resourceId": "acs:ecs:cn-hangzhou:169070********30:instance/i-bp1ecr********5go2go",
  "level": "INFO",
  "instanceName": "instance-event-subscription",
  "name": "Instance:LiveMigrationAcrossDDH",
  "userId": "169070********30",
  "eventTime": "20180608T092545.922+0800",
  "regionId": "cn-hangzhou",
  "content": {
      "instanceId" : "i-bp1ecr********5go2go",
      "sourceDedicatedHostId" : "dh-2ze3lm********t8nr82",
      "destinationDedicatedHostId" : "dh-2ze3lm********t8nr83",
      "startTime" : "2018-06-08T01:25:37Z",
      "endTime" : "2018-06-08T01:25:45Z",
      "status" : "failed"
  }
}
```

The following table describes the subparameters contained in the content parameter.

Subparameter	Description	Example
instanceId	The ID of the instance.	*i-bp1ecr********5go2go*
sourceDedicatedHostId	The ID of the source dedicated host.	*dh-2ze3lm********t8nr82*
destinationDedicatedHostId	The ID of the destination dedicated host.	*dh-2ze3lm********t8nr83*
startTime	The start time of the migration. The time is in UTC.	*2018-06-08T01:25:37Z*
endTime	The end time of the migration. The time is in UTC.	*2018-06-08T01:25:45Z*
status	The state of the hot migration. Valid values: • *started*: The migration starts. • *failed*: The migration fails. • *accomplished*: The migration is complete.	*accomplished*

Changes in the performance mode of burstable instances

If the performance mode of a burstable instance changes, ECS sends a notification for the *Instance:PerformanceModeChange* event.

The following example shows such an event notification in the JSON format:

```
{
    "ver": "1.0",
    "id": "2256A988-0B26-4E2B-820A-8A0580D0B8E5",
    "product": "ECS",
    "resourceId": "acs:ecs:cn-hangzhou:169070********30:instance/i-bp1ecr********5go2go",
    "level": "INFO",
    "name": "Instance:PerformanceModeChange",
    "userId": "169070********30",
    "eventTime": "20190409T121826.922+0800",
    "regionId": "cn-hangzhou",
    "content": {
        "instanceId" : "i-bp1ecr********5go2go",
        "creditSpecification" : "Unlimited",
        "operator" : "System"
    }
}
```

The following table describes the subparameters contained in the content parameter.

Subparameter	Description	Example
instanceId	The ID of the instance.	*i-bp1ecr********5go2go*
creditSpecification	The new performance mode of the burstable instance. Valid values: • *Standard*: standard mode • *Unlimited*: unlimited mode	*Standard*
operator	The operator that triggers the event. Valid values: • *User*: The performance mode of the instance is manually changed by the user from the ECS console or by calling API operations. • *System*: The performance mode of the instance is automatically changed by the system. The performance mode of your burstable instance may be automatically changed if the instance depletes its CPU credits, if the economical mode is triggered, or if you have overdue payments in your account. For more information, see Switch the performance mode of a burstable instance.	*User*

Limited performance of burstable instances

When a burstable instance depletes its CPU credits, the instance is limited to its baseline performance and runs in standard mode. An *Instance:BurstablePerformanceRestricted* event is generated.

Note Each Instance:BurstablePerformanceRestricted event spans a period of 1 hour. That means that the interval between the start time and end time of the event is 1 hour. This event indicates only that the instance gets limited to its baseline performance for some duration of the event period but not necessarily the entire event period. If the instance remains limited to its baseline performance for an extended period of time, an Instance:BurstablePerformanceRestricted event is generated every hour.

The following example shows such an event notification in the JSON format:

```
{
    "ver": "1.0",
    "id": "2256A988-0B26-4E2B-820A-8A0580D0B8E5",
    "product": "ECS",
    "resourceId": "acs:ecs:cn-hangzhou:169070********30:instance/i-bp1ecr********5go2go",
    "level": "INFO",
    "name": "Instance:BurstablePerformanceRestricted",
    "userId": "169070********30",
    "eventTime": "20190409T121826.922+0800",
    "regionId": "cn-hangzhou",
    "content": {
        "instanceId" : "i-bp1ecr********5go2go",
        "intervalStart" : "2019-11-11T11:00Z",
        "intervalEnd" : "2019-11-11T12:00Z"
    }
}
```

The following table describes the subparameters contained in the content parameter.

Subparameter	Description	Example
instanceId	The ID of the instance.	*i-bp1ecr********5go2go*
intervalStart	The start time of the event. The time is in UTC.	*2019-11-11T11:00Z*
intervalEnd	The end time of the event. The time is in UTC.	*2019-11-11T12:00Z*

Appendix: Notifications for instance-related system events

Impact	Event type and code	Event notification name and code

Impact	Event type and code	Event notification name and code
The instance is restarted.	Instance restart due to system maintenance: SystemMaintenance.Reboot	• Instance restart scheduled (system maintenance): Instance:SystemMaintenance.Reboot:Scheduled • Scheduled instance restart being executed (system maintenance): Instance:SystemMaintenance.Reboot:Executing • Scheduled instance restart completed (system maintenance): Instance:SystemMaintenance.Reboot:Executed • Scheduled instance restart avoided (system maintenance): Instance:SystemMaintenance.Reboot:Avoided • Scheduled instance restart canceled (system maintenance): Instance:SystemMaintenance.Reboot:Canceled • Scheduled instance restart failed (system maintenance): Instance:SystemMaintenance.Reboot:Failed
The instance is unexpectedly restarted.	Instance restart due to system errors: SystemFailure.Reboot	• Instance restart being executed (system error): Instance:SystemFailure.Reboot:Executing • Instance restart completed (system error): Instance:SystemFailure.Reboot:Executed
The instance is unexpectedly restarted.	Instance restart due to instance errors: InstanceFailure.Reboot	• Instance restart being executed (instance error): Instance:InstanceFailure.Reboot:Executing • Instance restart completed (instance error): Instance:InstanceFailure.Reboot:Executed
The instance is redeployed.	Instance redeployment due to system maintenance: SystemMaintenance.Redeploy	• Instance redeployment scheduled (system maintenance): Instance:SystemMaintenance.Redeploy:Scheduled • Scheduled instance redeployment being executed (system maintenance): Instance:SystemMaintenance.Redeploy:Executing • Scheduled instance redeployment completed (system maintenance): Instance:SystemMaintenance.Redeploy:Executed • Scheduled instance redeployment avoided (system maintenance): Instance:SystemMaintenance.Redeploy:Avoided • Scheduled instance redeployment canceled (system maintenance): Instance:SystemMaintenance.Redeploy:Canceled

Impact	Event type and code	Event notification name and code
The instance is redeployed.	Instance redeployment due to system errors: SystemFailure.Redeploy	• Instance redeployment scheduled (system error): Instance:SystemFailure.Redeploy:Scheduled • Instance redeployment being executed (system error): Instance:SystemFailure.Redeploy:Executing • Instance redeployment completed (system error): Instance:SystemFailure.Redeploy:Executed • Instance redeployment avoided (system error): Instance:SystemFailure.Redeploy:Avoided • Instance redeployment canceled (system error): Instance:SystemFailure.Redeploy:Canceled
The instance is restarted and the damaged local disk is isolated.	Instance restart and local disk replacement due to system maintenance: SystemMaintenance.RebootAndIsolateErrorDisk	• Instance restart and local disk isolation being inquired (system maintenance): Instance:SystemMaintenance.RebootAndIsolateErrorDisk:Inquiring • Instance restart and local disk isolation being executed (system maintenance): Instance:SystemMaintenance.RebootAndIsolateErrorDisk:Executing • Instance restart and local disk isolation completed (system maintenance): Instance:SystemMaintenance.RebootAndIsolateErrorDisk:Executed • Instance restart and local disk isolation avoided (system maintenance): Instance:SystemMaintenance.RebootAndIsolateErrorDisk:Avoided • Instance restart and local disk isolation canceled (system maintenance): Instance:SystemMaintenance.RebootAndIsolateErrorDisk:Canceled

Impact	Event type and code	Event notification name and code
The instance is restarted and the damaged local disk is restored.	Instance restart and local disk re-initialization due to system maintenance: SystemMaintenance.RebootAndReInitErrorDisk	• Instance restart and local disk re-initialization being inquired (system maintenance): Instance:SystemMaintenance.RebootAndReInitErrorDisk:Inquiring • Instance restart and local disk re-initialization being executed (system maintenance): Instance:SystemMaintenance.RebootAndReInitErrorDisk:Executing • Instance restart and local disk re-initialization completed (system maintenance): Instance:SystemMaintenance.RebootAndReInitErrorDisk:Executed • Instance restart and local disk re-initialization avoided (system maintenance): Instance:SystemMaintenance.RebootAndReInitErrorDisk:Avoided • Instance restart and local disk re-initialization canceled (system maintenance): Instance:SystemMaintenance.RebootAndReInitErrorDisk:Canceled
The instance is released.	Automatic instance release due to instance creation failures: SystemFailure.Delete	• Automatic instance release being executed (instance creation failure): Instance:SystemFailure.Delete:Executing • Automatic instance release completed (instance creation failure): Instance:SystemFailure.Delete:Executed • Automatic instance release avoided (instance creation failure): Instance:SystemFailure.Delete:Avoided

2.4.4.2. EBS event notifications

You can subscribe to notifications for the following Elastic Block Storage (EBS) events: system events, data disk attaching or detaching, disk retaining, and disk release due to overdue payments.

Events

You can subscribe to notifications for the following EBS events:

- System events
- Data disk attaching or detaching
- Disk retaining
- Disk release due to overdue payments

System events

EBS system events are caused only by exceptions. Elastic Compute Service (ECS) sends two notifications: one at the start time of the event and the other at the end time of the event. For the event notification names of different system events, see Appendix: event notification names.

The following notifications are example notifications in the JSON format for a *Stalled* event that has a severe impact on disk performance.

- The initial notification that ECS sends you when the event starts contains the executeStartTime parameter.

```
{
  "ver": "1.0",
  "id": "2256A988-0B26-4E2B-820A-8A********E5",
  "product": "ECS",
  "resourceId": "acs:ecs:cn-hangzhou:169070********30:disk/d-t4ndyqve********n4ds",
  "level": "CRITICAL",
  "name": "Disk:Stalled:Executing",
  "userId": "169070********30",
  "eventTime": "20190410T080101.922+0800",
  "regionId": "cn-hangzhou",
  "content": {
    "eventId": "e-t4navn7********6x5no",
    "diskId": "d-t4ndyqve********n4ds",
    "device": "/dev/xvdb",
    "eventType": "Stalled",
    "executeStartTime": "2019-04-10T01:01:01Z",
    "ecsInstanceId": "i-bp1ecr********5go2go",
    "ecsInstanceName": "ecs-instance-name"
  }
}
```

- The notification that ECS sends you when the event ends contains the executeFinishTime parameter.

```
{
  "ver": "1.0",
  "id": "2256A988-0B26-4E2B-820A-8A********E5",
  "product": "ECS",
  "resourceId": "acs:ecs:cn-hangzhou:169070********30:disk/d-t4ndyqve********n4ds",
  "level": "CRITICAL",
  "name": "Disk:Stalled:Executing",
  "userId": "169070********30",
  "eventTime": "20190410T080301.922+0800",
  "regionId": "cn-hangzhou",
  "content": {
    "eventId": "e-t4navn7********6x5no",
    "diskId": "d-t4ndyqve********n4ds",
    "device": "/dev/xvdb",
    "eventType": "Stalled",
    "executeStartTime": "2019-04-10T01:01:01Z",
    "executeFinishTime": "2019-04-10T01:03:01Z",
    "ecsInstanceId": "i-bp1ecr********5go2go",
    "ecsInstanceName": "ecs-instance-name"
  }
}
```

The following table describes parameters in the content field.

Parameter	Description	Example
eventId	The ID of the system event.	*e-t4navn7********6x5no*
diskId	The ID of the EBS device whose performance is affected.	*d-t4ndyqve********n4ds*
device	The mount point of the EBS device.	*/dev/xvdb*
eventType	The type of the system event. Valid values: ● *Degraded*: The performance of the EBS device is degraded. ● *SeverelyDegraded*: The performance of the EBS device is severely degraded. ● *Stalled*: The performance of the EBS device is severely affected.	*Stalled*
executeStartTime	The start time of the system event. The time is in UTC.	*2019-04-10T01:01:01Z*
executeFinishTime	The end time of the system event. The time is in UTC.	*2019-04-10T01:03:01Z*
ecsInstanceId	The ID of the instance to which the EBS device is attached.	*i-bp1ecr********5go2go*
ecsInstanceName	The name of the instance to which the EBS device is attached.	*ecs-instance-name*

Data disk attaching or detaching

After a data disk is attached to or detached from an instance, ECS sends you a notification to indicate whether the attach or detach operation is successful. For more information, see Attach a data disk and Detach a data disk.

The following code shows the event notification in the JSON format:

```
{
  "ver": "1.0",
  "id": "2256A988-0B26-4E2B-820A-8A********E5",
  "product": "ECS",
  "resourceId": "acs:ecs:cn-hangzhou:169070********30:disk/d-t4ndyqve********n4ds",
  "level": "INFO",
  "name": "Disk:DiskOperationCompleted",
  "userId": "169070********30",
  "eventTime": "20190409T121826.922+0800",
  "regionId": "cn-hangzhou",
  "content": {
      "diskId" : "d-t4ndyqve********n4ds",
      "operation" : "AttachDisk",
      "result" : "accomplished"
  }
}
```

The following table describes parameters in the content field.

Parameter	Description	Example
diskId	The ID of the disk.	*d-bp1bwa********9ol4mi*
operation	The type of the operation. Valid values: - *AttachDisk*: attaches a disk. - *DetachDisk*: detaches a disk.	*AttachDisk*
result	The result of the operation. Valid values: - *accomplished*: The operation succeeds. - *failed*: The operation fails. **Note** If the operation succeeds, the *level* value of the event is *INFO*. If the operation fails, the level value of the event is *WARN*.	*accomplished*

Disk retaining

You can disable **Release with Instance** for disks, including system and data disks. The disks are retained and converted to pay-as-you-go data disks when their attached instances are released. For more information, see Release a disk.

The following code shows the event notification in the JSON format:

```
{
    "ver": "1.0",
    "id": "2256A988-0B26-4E2B-820A-8A0580D0B8E5",
    "product": "ECS",
    "resourceId": "acs:ecs:cn-hangzhou:169070********30:disk/d-t4ndyqve********n4ds",
    "level": "INFO",
    "instanceName": "disk-event-subscription",
    "name": "Disk:ConvertToPostpaidCompleted",
    "userId": "169070********30",
    "eventTime": "20190409T121826.922+0800",
    "regionId": "cn-hangzhou",
    "content": {
    "diskId" : "d-t4ndyqve********n4ds",
    "result" : "accomplished"
    }
}
```

The following table describes parameters in the content field.

Parameter	Description	Example
diskId	The ID of the disk.	*d-bp1bwa********9ol4mi*
result	The result of the operation. Valid values: - *accomplished*: The operation succeeds. - *failed*: The operation fails.	*accomplished*

Disk release due to overdue payments

You may receive a disk release notification in the following scenarios:

- Your EBS devices are located in mainland China, but real-name verification is not complete for your account.
- Your pay-as-you-go disk is released because you have an overdue payment in your account.

Note

The following code shows the event notification in the JSON format:

```
{
    "ver": "1.0",
    "id": "2256A988-0B26-4E2B-820A-8A0580D0B8E5",
    "product": "ECS",
    "resourceId": "acs:ecs:cn-hangzhou:169070********30:disk/d-t4ndyqve********n4ds",
    "level": "CRITICAL",
    "instanceName": "disk-event-subscription",
    "name": "Disk:OverduePaymentRelease",
    "userId": "169070********30",
    "eventTime": "20190409T121826.922+0800",
    "regionId": "cn-hangzhou",
    "content": {
    "instanceId" : "i-bp1792********an2ukf",
    "diskId" : "d-t4ndyqve********n4ds"
    }
}
```

The following table describes parameters in the content field.

Parameter	Description	Example
instanceId	The ID of the instance to which the disk is attached.	*i-bp1792********an2ukf*
diskId	The ID of the disk.	*d-bp1bwa********9ol4mi*

Appendix: event notification names

Event	Event type and code	Event notification name and code
Performance impact	Severe impact on disk performance: Stalled	• Start of severe impact on disk performance: Disk:Stalled:Executing • End of severe impact on disk performance: Disk:Stalled:Executed
Local disk damage	Local disks damaged: ErrorDetected	• Start of local disk damage alert: Disk:ErrorDetected:Executing • End of local disk damage alert: Disk:ErrorDetected:Executed

2.4.4.3. Snapshot event notifications

You can subscribe to notifications for snapshot creation events.

Snapshot creation

After a snapshot is created for a disk, ECS sends you a notification to indicate whether the operation succeeded. Example:

```
{
  "ver": "1.0",
  "id": "2256A988-0B26-4E2B-820A-8A********E5",
  "product": "ECS",
  "resourceId": "acs:ecs:cn-hangzhou:169070********30:snapshot/s-bp1fis********b859b3",
  "level": "INFO",
  "name": "Snapshot:CreateSnapshotCompleted",
  "userId": "169070********30",
  "eventTime": "20190409T121826.922+0800",
  "regionId": "cn-hangzhou",
  "content": {
    "result": "accomplished",
    "snapshotId": "s-bp1fis********b859b3",
    "snapshotName": "test-snapshot",
    "snapshotType": "user",
    "diskId": "d-bp1bwa********9ol4mi",
    "startTime": "2019-04-22T08:36:09Z",
    "endTime": "2019-04-22T08:37:11Z"
  }
}
```

The following table describes the subparameters contained in the content parameter.

Subparameter	Description	Example
result	The operation result. Valid values: • *accomplished*: Snapshot creation succeeded. • *failed*: Snapshot creation failed.	*accomplished*
snapshotId	The ID of the snapshot.	*s-bp1fis********b859b3*
snapshotName	The name of the snapshot.	*test-snapshot*
snapshotType	The type of the snapshot. Valid values: • user: manual snapshots • timer: snapshots that are created as scheduled • copied: copied snapshots • imported: imported snapshots	*user*
diskId	The ID of the disk.	*d-bp1bwa********9ol4mi*
startTime	The time when the snapshot starts to be created. The time is in UTC.	*2019-04-22T08:36:09Z*
endTime	The time when the snapshot finishes being created. The time is in UTC.	*2019-04-22T08:37:11Z*

2.4.4.4. ENI operation event notifications

When elastic network interfaces (ENIs) are created, deleted, bound, or unbound, ENI operation events are triggered and event notifications are sent.

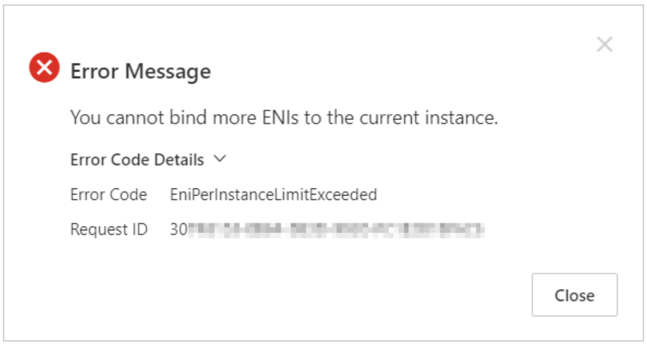
Notifications of ENI operation events

The following conditions must be met to trigger ENI operation events:

- The ENI operation event feature is enabled. The feature is in invitational preview. To use this feature, submit a ticket.
- The operation objects are secondary ENIs.

  ENIs are classified into primary ENIs and secondary ENIs. ENI operation events can be triggered only when the operation objects are secondary ENIs. For more information about the attributes of ENIs, see Attributes.
- ENI operations succeed.

  ENI operation events can be triggered only when ENI operations succeed and no error messages are returned. For example, assume that an Elastic Compute Service (ECS) instance has already reached the maximum number of ENIs to which it can be bound. If you attempt to bind more ENIs to the instance, the attach operation fails and an error message similar to the one shown in the following figure appears. In this case, no ENI operation event is triggered.

  Error Message

  You cannot bind more ENIs to the current instance.

  Error Code Details

  Error Code EniPerInstanceLimitExceeded

  Request ID 30[redacted]

When an ENI operation that meets the preceding conditions is performed, an ENI operation event is triggered and an event notification is sent to the initiator of the operation.

- If the operation object is a managed ENI, the operation is initiated by an Alibaba Cloud service. When the operation is complete, an event notification is sent to the Alibaba Cloud service. For more information about managed ENIs, see Managed ENIs.
- If the operation object is a regular ENI, the operation is initiated by a user to bind, unbind, or delete the ENI. When the operation is complete, an event notification is sent to the user.

You can make configurations in CloudMonitor to receive notifications of ENI operation events and view the ENI operation results by using emails and DingTalk chatbots. You can obtain the information of ENIs and configure ENI operations to be automatically performed in response to the notifications. For more information, see Configure event notifications.

The following JSON code shows an example notification of an ENI operation event.

```
{
    "ver":"1.0",
    "id":"2256A988-0B26-4E2B-820A-8B********A5",
    "product":"ECS",
    "resourceId":"acs:ecs:cn-hangzhou:169070********30:eni/eni-8vb1qo********cdeg2n",
    "level":"INFO",
    "name":"NetworkInterface:NetworkInterfaceOperateCompleted",
    "userId":"169070********30",
    "eventTime":"20190409T121826.922+0800",
    "regionId":"cn-hangzhou",
    "content":{
        "eniId":"eni-8vb1qo********cdeg2n",
        "operation":"AttachNetworkInterface",
        "eniStatus":"InUse",
        "result":"success",
        "requestId":"59701492-A8F2-3375-B0B9-D9********27"
    }
}
```

The following table describes the subparameters contained in the content parameter.

Subparameter	Description	Example
eniId	The ID of the ENI.	eni-8vb1qo********cdeg2n
operation	The type of the operation. Valid values: • CreateNetworkInterface: creates an ENI. • AttachNetworkInterface: binds an ENI. • DetachNetworkInterface: unbinds an ENI. • DeleteNetworkInterface: deletes an ENI.	AttachNetworkInterface

Subparameter	Description	Example
eniStatus	The state of the ENI. Valid values: - Available: The ENI is available and can be bound to an instance. - InUse: The ENI is bound to an instance. - Detaching: The ENI is being unbound from an instance. - Deleting: The ENI is being deleted. - Deleted: The ENI has been deleted. - CreateFailed: The ENI cannot be created.	InUse
result	The operation result. Valid values: - success: The operation succeeds and the event level of the ENI operation event is INFO. - failed: The operation fails and the event level of the ENI operation event is WARN.	success
requestId	The ID of the request that corresponds to the operation.	59701492-A8F2-3375-B0B9-D9********27

Related information

- Create an ENI
- Bind an ENI
- Unbind an ENI
- Delete an ENI

2.5. System events and O&M process of ECS instances equipped with local disks

2.5.1. O&M scenarios and system events for instances equipped with local disks

Local disks do not provide high availability of data. To enhance user experience on local disks, Alibaba Cloud provides various O&M capabilities to help you keep up on and handle exceptions that occur on your local disks. This topic describes common O&M scenarios and system events for Elastic Compute Service (ECS) instances equipped with local disks.

Common O&M scenarios

For ECS bare metal instances, you can install the *xdragon_hardware_detect_plugin* plug-in to check the health status of local disks on the instances on a regular basis. For more information, see Install the monitoring plug-in.

For more information about system events triggered in the scenarios shown in the preceding figure, see the following sections in this topic:

- Scenario ①
- Scenario ②
- Scenario ③
- Scenario ④
- Scenario ⑤

> ? **Note** To ensure that your business is not affected, we recommend that you back up data for affected ECS instances and switch over to other instances before you execute O&M tasks on the instances. For example, you can divert traffic away from the affected ECS instances, disassociate the ECS instances from Server Load Balancer (SLB) instances, and back up disk data of the ECS instances.

Scenario ①

Procedure to handle a SystemMaintenance.Reboot system event:

1. Receive an event notification when an instance is scheduled to be restarted.
2. Use one of following methods to handle the event:
   - If you do not want the instance to be restarted within the scheduled time period, specify a different time at which to automatically restart the instance. For more information, see Modify the scheduled restart time.
   - Restart the instance within the user operation window. For more information, see Restart an instance.

     > ? **Note** You must restart the instance by using the ECS console or by calling the RebootInstance operation. You cannot restart the instance from within the instance.

   - Wait for the instance to be automatically restarted.
3. Check whether the instance and applications continue to work as expected.

For information about the event states supported by SystemMaintenance.Reboot, see Summary. For the figure that shows the typical transitions between event states, see States and windows of system events.

Scenario ②

Procedure to handle a SystemMaintenance.Redeploy system event:

1. Receive an event notification when an instance equipped with local disks is scheduled to be

redeployed.

2. Make preparations such as modifying the */etc/fstab* configuration file and backing up data.

   For more information about preparations that you must make, see the "Prerequisites" section in Redeploy an instance equipped with local disks.

3. Use one of following methods to handle the event:

   - Redeploy the instance within the user operation window. For more information, see Redeploy an instance equipped with local disks.
   - Wait for the instance to be automatically redeployed.

   > ? **Note** When an instance equipped with local disks is redeployed, the instance is migrated to a different physical machine, and the local disks of the instance are re-initialized and lose all their data.

4. Check whether the instance and applications continue to work as expected. If yes, synchronize data based on your business requirements.

For information about the event states supported by SystemMaintenance.Redeploy, see Summary. For the figure that shows the typical transitions between event states, see States and windows of system events.

Scenario ③

Procedure to handle a SystemFailure.Reboot system event:

1. The system restarts an instance due to a system error.
2. Receive an event notification when the instance is being restarted.

   Wait until the instance is restarted without manual intervention.

3. Check whether the instance and applications continue to work as expected.

For information about the event states supported by SystemFailure.Reboot, see Summary. For the figure that shows the typical transitions between event states, see States and windows of system events.

Scenario ④

Procedure to handle a SystemFailure.Redeploy system event:

1. Receive an event notification when an instance equipped with local disks is scheduled to be redeployed.
2. Make preparations such as modifying the */etc/fstab* configuration file and backing up data.

   For more information about preparations that you must make, see the "Prerequisites" section in Redeploy an instance equipped with local disks.

3. Use one of following methods to handle the event:

   - Redeploy the instance within the user operation window. For more information, see Redeploy an instance equipped with local disks.
   - Wait for the instance to be automatically redeployed.

> **Note** When an instance equipped with local disks is redeployed, the instance is migrated to a different physical machine, and the local disks of the instance are re-initialized and lose all their data.

4. Check whether the instance and applications continue to work as expected. If yes, synchronize data based on your business requirements.

For information about the event states supported by SystemFailure.Redeploy, see Summary. For the figure that shows the typical transitions between event states, see States and windows of system events.

Scenario ⑤

For Scenario ⑤ where a local disk is damaged on the host of an instance, you can redeploy the instance to another host or replace the disk.

- When the instance is redeployed, its local disks are restored but lose all their data. For information about how to redeploy an instance equipped with local disks, see Redeploy an instance equipped with local disks.
- When the damaged local disk is replaced, only data of the replaced local disk is lost but data of the other local disks on the instance is retained. Procedure to replace a damaged local disk on an instance:
  1. i. Receive an event notification when a local disk on an instance is damaged and scheduled to be isolated.
  2. ii. Make preparations such as modifying the */etc/fstab* configuration file and backing up data.
  3. iii. Respond to the notification and authorize Alibaba Cloud to isolate the damaged local disk.
  4. iv. If the name of the system event contains Reboot, you must restart the instance.
  5. v. Alibaba Cloud removes the damaged local disk from the host on which your instance resides, inserts a new disk, and then sends you a disk restoration notification.
  6. vi. After you receive the notification, authorize Alibaba Cloud to restore the disk.
  7. vii. If the name of the system event contains Reboot, you must restart the instance.

> **Note** To replace a damaged local disk, you must work together with Alibaba Cloud. For more information, see Isolate damaged local disks in the ECS console and Isolate damaged local disks by using Alibaba Cloud CLI.

2.5.2. Redeploy an instance equipped with local disks

This topic describes how to redeploy an Elastic Compute Service (ECS) instance equipped with local SSDs or HDDs in the ECS console. After an ECS instance is redeployed, the instance is migrated to a different physical machine.

Prerequisites

- Operations described in this topic are applicable only to scenarios where system events occur on ECS instances equipped with local disks.
- Before you redeploy an instance equipped with local disks, the following operations are performed:

i.

ii. (Optional)(Optional) The read/write operations on the local disks are isolated at the application layer.

iii. If the instance runs a Linux operating system, the nofail parameter is added to the */etc/fstab* file of the instance for all data disks.

In this example, the nofail parameter is added for the */dev/vdd* data disk:

```
/dev/vdd /mnt/vdd ext4 defaults,barrier=0,nofail 0 0
```

Parameter	Description
/dev/vdd	The device name of the local disk, which is the Device value returned by the DescribeInstanceHistoryEvents operation.
/mnt/vdd	The mount point of the local disk, which can be queried by using the `mount | grep "/dev/vdd"` command.
ext4	The file system type of the local disk, which can be queried by using the `blkid /dev/vdd1` command.
barrier=0	The mount option used to disable barriers in the file system.
nofail	Indicates that the booting sequence of the ECS instance is not interrupted even if the local disk specified in the file system does not exist.

Context

System events that require local disks to be redeployed include **Instance Redeployment Due to System Maintenance** (`SystemMaintenance.Redeploy`) and **Instance Redeployment Due to System Error** (`SystemFailure.Redeploy`). For more information, see O&M scenarios and system events for instances equipped with local disks.

Notice After an instance is redeployed, the instance is migrated to a different physical machine. The data disks of the instance equipped with local SSDs or HDDs are re-initialized and the data on the local disks is cleared.

Procedure

1.

2.

3. On the **Pending Events** page, click the **System Events** tab. Find the **System O&M** tab. In the event list, find the instance that has an **Instance Redeployment Due to System Maintenance** or **Instance Redeployment Due to System Error** event and click **Redeploy** in the Actions column.

4. In the **Redeploy Instance** dialog box, confirm the impact of redeployment and click **Redeploy**.

What's next

After a Linux instance that has data disks attached is redeployed, you can perform the following operations to re-synchronize data and restore business based on your needs:

- If the instance has cloud data disks attached and is not configured to have the cloud data disks automatically attached on instance startup, you must connect to the instance after it is redeployed and run the following command to re-attach the cloud data disks:

  ```
  mount <Data disk partition> <Mount point>
  ```

- If the instance has local data disks attached, you must partition and format the local data disks. For more information, see Partition and format a data disk on a Linux instance.

Related information

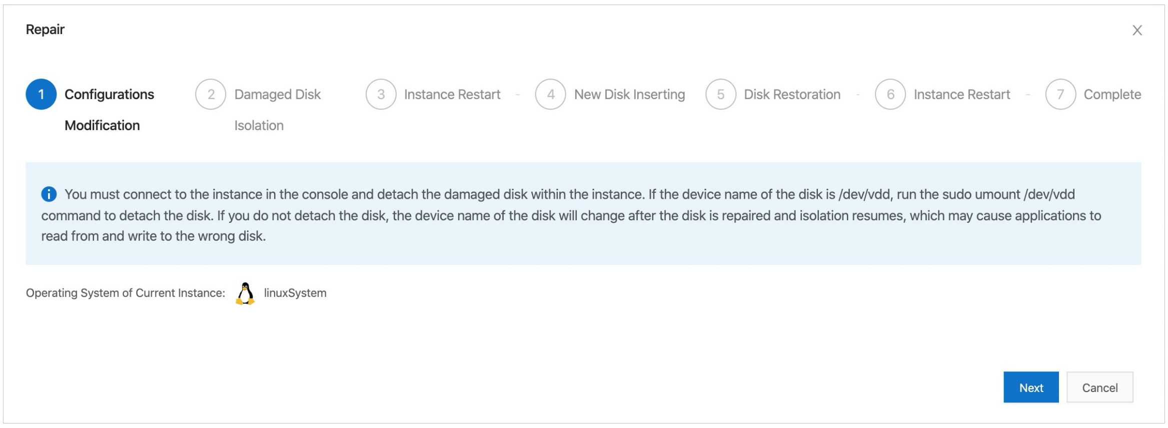
- RedeployInstance

2.5.3. Isolate damaged local disks in the ECS console

This topic describes how to isolate damaged local disks in the ECS console. When a damaged local disk is isolated, the corresponding ECS instance still resides on the same physical machine. The procedure described in this topic is applicable only to resolving system events about damaged local disks on ECS instances.

Procedure

1.
2.
3. On the **Pending Events** page, click the **Local Disk Damaged** tab.
4. Find the target instance, and click **Repair** in the **Actions** column.
5. In the **Configurations Modification** step, modify the configuration file of the instance. Then, click **Next**.



You must connect to the instance in the console and detach the damaged disk within the instance. If the device name of the disk is /dev/vdd, run the sudo umount /dev/vdd command to detach the disk. If you do not detach the disk, the device name of the disk will change after the disk is repaired and isolation resumes, which may cause applications to read from and write to the wrong disk.

Operating System of Current Instance: linuxSystem

   If the **Configurations Modification** step is displayed for some Linux instances, complete the following operations. In this topic, the damaged disk named */dev/vdd* is used as an example.

   i. Connect to the ECS instance. For more information, see Connection methodsGuidelines on instance connection.
   ii. (Optional)Isolate the read and write operations of the local disk at the application layer.

iii. If the instance is a Linux instance, add the nofail parameter to the */etc/fstab* configuration file of the instance for the local disk.

```
/dev/vdd /mnt/vdd ext4 defaults,barrier=0,nofail 0 0
```

Parameter	Description
/dev/vdd	The device name of the local disk, which is the Device value returned by the DescribeInstanceHistoryEvents operation.
/mnt/vdd	The mount point of the local disk, which can be queried by using the `mount | grep "/dev/vdd"` command.
ext4	The file system type of the local disk, which can be queried by using the `blkid /dev/vdd1` command.
barrier=0	The mount option used to disable barriers in the file system.
nofail	Indicates that the booting sequence of the ECS instance is not interrupted even if the local disk specified in the file system does not exist.

iv. Unmount the local disk.

```
umount /dev/vdd
```

> **Notice** If you do not unmount the local disk, the device name of the local disk will change after the local disk is isolated and repaired. In this case, applications may read from or write to another disk.

6. In the **Damaged Disk Isolation** step, click **OK**.

   Refresh the page if the next step is not displayed.

7. (Optional)In the **Instance Restart** step, click **Restart**.

   If the **Instance Restart** step is displayed, you must click Restart to restart the instance.

   > **Note** After the instance is restarted, the isolated damaged local disk is temporarily converted to a 1 MiB dummy hard disk to facilitate subsequent operations. At the application layer, you must continuously isolate read and write operations on the damaged local disk and configure the nofail parameter in the */etc/fstab* file.

8. After the instance is restarted, click **OK** in the **New Disk Inserting** step.

   Wait for Alibaba Cloud to replace the damaged local disk on the physical machine that hosts the instance. Maintenance is typically completed within five weekdays. After maintenance is completed, you will receive a event that requires you to restore the disk.

9. After you receive the event, click **Restore** in the **Disk Restoration** step.

   Refresh the page if the next step is not displayed.

10. (Optional)In the **Instance Restart** step, click **Restart**.

    If the **Instance Restart** step is displayed, you must click Restart to restart the instance.

11. After the instance is restarted, click **Complete** in the **Complete** step.

Result

Within a few minutes after the damaged disk is replaced, the local disk damaged event disappears.

What's next

After the damaged disk is isolated, check the status of the instance and local disk. The replaced local disk is restored to its original capacity, and you can reformat data disks. For more information, see Partition and format a data disk on a Windows instance or Partition and format a data disk on a Linux instance.

Related information

- Isolate damaged local disks by using Alibaba Cloud CLI
- DescribeInstanceHistoryEvents
- AcceptInquiredSystemEvent
- RebootInstance

2.5.4. Isolate damaged local disks by using Alibaba Cloud CLI

When a damaged local disk is isolated, the corresponding ECS instance still resides on the same physical machine. This topic describes how to use Alibaba Cloud CLI to call ECS API operations to isolate damaged local disks. The procedure described in this topic is applicable only to ECS instances on which system events about local disks occur. You can also update the SDKs or call relevant API operations in Alibaba Cloud OpenAPI Explorer to complete the operations.

Prerequisites

Context

The system event codes that correspond to the isolation options of a damaged disk vary with the stage of events. For more information, see O&M scenarios and system events for instances equipped with local disks.

- Before the damaged disk is isolated, the system event code is `SystemMaintenance.IsolateErrorDisk`. If the instance must be restarted, the code is `SystemMaintenance.RebootAndIsolateErrorDisk`.
- After the damaged disk is isolated but before a new disk is re-initialized, the system event code is `SystemMaintenance.ReInitErrorDisk`. If the instance must be restarted, the code is `SystemMaintenance.RebootAndReInitErrorDisk`.

> **Notice** After data disks are re-initialized, data on the isolated local disk is cleared.

Procedure

1. Call the DescribeInstanceHistoryEvents operation to query system events within the specified region that are in the Inquiring state, and record the return values of EventId, DiskId, and Device.

   Run the following command in Alibaba Cloud CLI:

```
aliyun ecs DescribeInstanceHistoryEvents \
--RegionId <TheRegionId> \
--InstanceEventCycleStatus.1 Inquiring
```

Sample response in the JSON format:

```
{
  "InstanceSystemEventSet": {
    "InstanceSystemEventType": [
      {
        "InstanceId": "i-2ze3tphuqvc93ci****3",
        "EventId": "e-2ze9y****wtqcvai68rl",
        "EventType": {
          "Code": 3,
          "Name": "SystemMaintenance.IsolateErrorDisk"
        },
        "EventCycleStatus": {
          "Code": 28,
          "Name": "Inquiring"
        },
        "EventPublishTime": "2017-11-30T06:32:31Z",
        "ExtendedAttribute" : {
          "DiskId": "d-disk1",
          "Device": "/dev/xvda"
        }
      }
    ]
  },
  "PageSize": 10,
  "PageNumber": 1,
  "TotalCount": 1,
  "RequestId": "02EA76D3-5A2A-44EB-****-8901881D8707"
}
```

2. Log on to the ECS instance to make preparations before you isolate the damaged local disk.

   i. Connect to the ECS instance. For more information, see Connection methodsGuidelines on instance connection.

   ii. (Optional)Isolate the read and write operations of the local disk at the application layer.

iii. If the instance is a Linux instance, add the nofail parameter to the */etc/fstab* configuration file of the instance for the local disk.

```
/dev/vdd /mnt/vdd ext4 defaults,barrier=0,nofail 0 0
```

Parameter	Description
/dev/vdd	The device name of the local disk, which is the Device value returned by the DescribeInstanceHistoryEvents operation.
/mnt/vdd	The mount point of the local disk, which can be queried by using the `mount | grep "/dev/vdd"` command.
ext4	The file system type of the local disk, which can be queried by using the `blkid /dev/vdd1` command.
barrier=0	The mount option used to disable barriers in the file system.
nofail	Indicates that the booting sequence of the ECS instance is not interrupted even if the local disk specified in the file system does not exist.

iv. Unmount the local disk.

```
umount /dev/vdd
```

Notice If you do not unmount the local disk, the device name of the local disk will change after the local disk is isolated and repaired. In this case, applications may read from or write to another disk.

3. Call the AcceptInquiredSystemEvent operation to respond to the specified system event.

   Run the following command in Alibaba Cloud CLI:

```
aliyun ecs AcceptInquiredSystemEvent --RegionId <TheRegionId> --EventId <TheEventId>
```

4. Determine whether to restart the instance.

   - When the event code is `SystemMaintenance.IsolateErrorDisk`:
     - If only the RequestId value is returned, you do not need to restart the instance.
     - If the return value of `code` is SwitchToOffline.OnlineIsolateFail, you must restart the instance.
   - When the event code is `SystemMaintenance.RebootAndIsolateErrorDisk`, you must restart the instance after you call the AcceptInquiredSystemEvent operation.

   To restart the instance, run the following command in Alibaba Cloud CLI:

```
aliyun ecs RebootInstance --InstanceId <TheInstanceId>
```

> Note After the instance is restarted, the isolated damaged local disk is temporarily converted to a 1 MiB dummy hard disk to facilitate subsequent operations. At the application layer, you must continuously isolate read and write operations on the damaged local disk and configure the nofail parameter in the */etc/fstab* file.

5. Wait until Alibaba Cloud replaces the damaged local disk on the physical machine and publishes the `SystemMaintenance.ReInitErrorDisk` or `SystemMaintenance.RebootAndReInitErrorDisk` event. This process takes one to five days.
6. Call the AcceptInquiredSystemEvent operation again to respond to the system event. The local disk enters the re-initializing state.

   Run the following command in Alibaba Cloud CLI:

   ```
   aliyun ecs AcceptInquiredSystemEvent --RegionId <TheRegionId> --EventId <TheEventId>
   ```
7. Determine whether to restart the instance.
   - When the event code is `SystemMaintenance.ReinitErrorDisk` :
     - If only the RequestId value is returned, you do not need to restart the instance.
     - If the return value of `code` is SwitchToOffline.OnlineReInitFail, you must restart the instance.
   - When the event code is `SystemMaintenance.RebootAndReinitErrorDisk` , you must restart the instance after you call the AcceptInquiredSystemEvent operation.

   To restart the instance, run the following command in Alibaba Cloud CLI:

   ```
   aliyun ecs RebootInstance --InstanceId <TheInstanceId>
   ```

What's next

After the damaged disk is isolated, check the status of the instance and local disk. The replaced local disk is restored to its original capacity, and you can reformat data disks. For more information, see Partition and format a data disk on a Windows instance or Partition and format a data disk on a Linux instance.

Related information

- Isolate damaged local disks in the ECS console
- DescribeInstanceHistoryEvents
- AcceptInquiredSystemEvent
- RebootInstance

2.6. Manage settings related to system events

2.6.1. Instance maintenance attributes

If a host on which your Elastic Compute Service (ECS) instance resides has potential risks or fails, Alibaba Cloud sends a system event to notify you of the situation. Then, you can handle the event. When you handle the event, the system takes the default maintenance action to restart the instance. If you do not want the instance to be automatically restarted, you can change the maintenance action for the instance by modifying its maintenance attribute.

Context

Instance maintenance attributes specify the default actions to take on ECS instances after unexpected or scheduled O&M events occur for the instances. You can define the default maintenance action for an instance by modifying its maintenance attribute. For example, you can configure whether to automatically restart or stop an instance in case of an unexpected O&M event. The following table describes the maintenance attributes supported by instances.

> ? **Note** You can modify instance maintenance attributes but the new maintenance attributes do not affect ongoing operations. For example, if you modify the maintenance attribute of an instance that is being automatically restarted, the new maintenance attribute cannot stop the restart operation or change it into a different operation.

Instance maintenance attribute	System event	Supported instance	Description
Automatically Restart (Default)	• SystemMaintenance.Reboot • SystemFailure.Reboot	All instances that support system events.	Restores the instance to the state that it was in before the O&M task related to a system event is executed. • If the instance was in the **Running** state before the O&M task is executed, the instance is automatically restarted to continue providing services. • If the instance was in the **Stopped** state before the O&M task is executed, the instance remains in the **Stopped** state.
Stop	• SystemMaintenance.Stop • SystemFailure.Stop	All instances that support system events.	Puts the instance into the **Stopped** state. This maintenance attribute is applicable to scenarios in which failovers or switchovers are performed at the application layer for disaster recovery purposes to prevent conflicts between multiple nodes in service.

Instance maintenance attribute	System event	Supported instance	Description
Automatically Re-deploy	• SystemMaintenance.Redeploy • SystemFailure.Redeploy	Instances that depend on host hardware, such as instances that have local disks attached or that support Software Guard Extensions (SGX) encrypted computing. For information about the instance families of such instances, see Instance family. ⓘ **Note** After an instance is redeployed, the data on its local disks is deleted and SGX is reset.	Redeploys the instance to another host to continue providing services.

To make better use of instance maintenance attributes, we recommend that you use multiple methods to improve fault tolerance for your business and reduce the impacts of O&M. Examples:

- Configure core applications such as SAP HANA to automatically start on system startup. This helps prevent business interruptions.
- Enable the automatic reconnection feature for your applications. For example, allow applications to automatically connect to MySQL, SQL Server, or Apache Tomcat.
- Deploy multiple ECS instances in a cluster if you use Server Load Balancer (SLB). When an ECS instance is being automatically restarted, other ECS instances can continue to provide access to your services.
- Back up data on local disks on a regular basis to ensure that redundant data copies are available for you to redeploy instances.

Procedure

1.
2.
3.
4.
5. Find the instance and use one of the following methods to modify its maintenance attribute:
   - Method 1: Choose **More > Operations and Troubleshooting > Modify Instance Maintenance Attribute** in the **Actions** column corresponding to the instance.
   - Method 2: Click the ID of the instance to go to the Instance Details page. In the upper-right corner of the tab, choose **All Operations > Operations and Troubleshooting > Modify Instance Maintenance Attribute**.
6. In the **Modify Instance Maintenance Attribute** dialog box, set the Maintenance Action parameter and click **OK**.
   - If the instance has only cloud disks attached, you can select one of the following options for

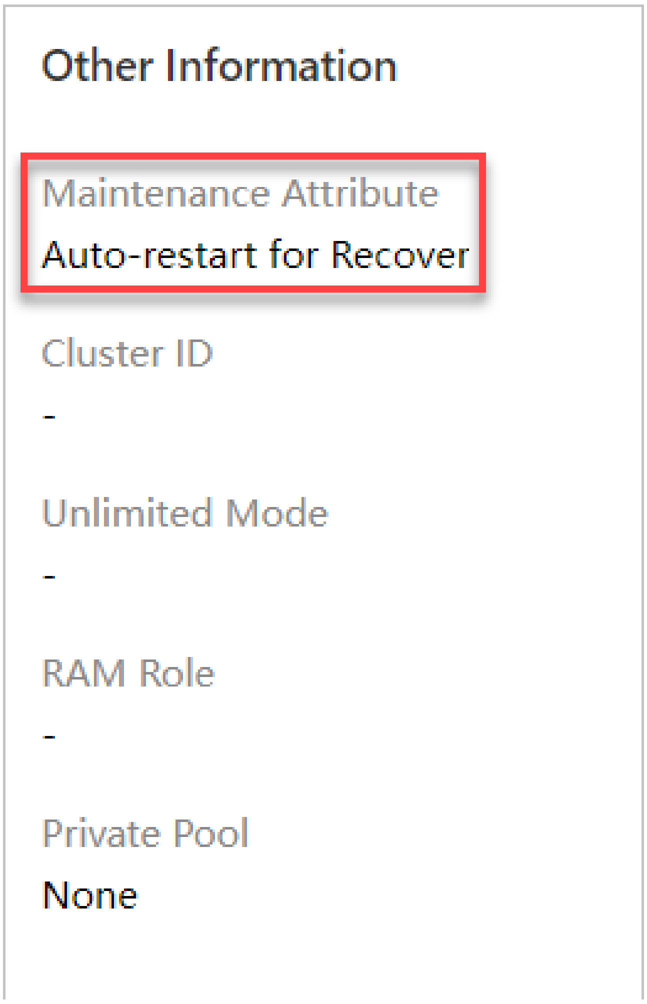
Maintenance Action:

  - Automatically Restart
  - Stop

- If the instance has local disks attached, you can select one of the following options for Maintenance Action:

  - Automatically Restart
  - Stop
  - Automatically Re-deploy

7. In the **Other Information** section of the **Instance Details** tab, confirm the new **Maintenance Attribute** settings.



Other Information

Maintenance Attribute
Auto-restart for Recover

Cluster ID
-

Unlimited Mode
-

RAM Role
-

Private Pool
None

Related information

- DescribeInstanceMaintenanceAttributes
- ModifyInstanceMaintenanceAttributes
- RedeployInstance
- DescribeInstanceHistoryEvents

2.6.2. Modify the scheduled restart time

This topic describes how to modify the scheduled restart time in the ECS console.

Prerequisites

You have a system event that has a restart plan.

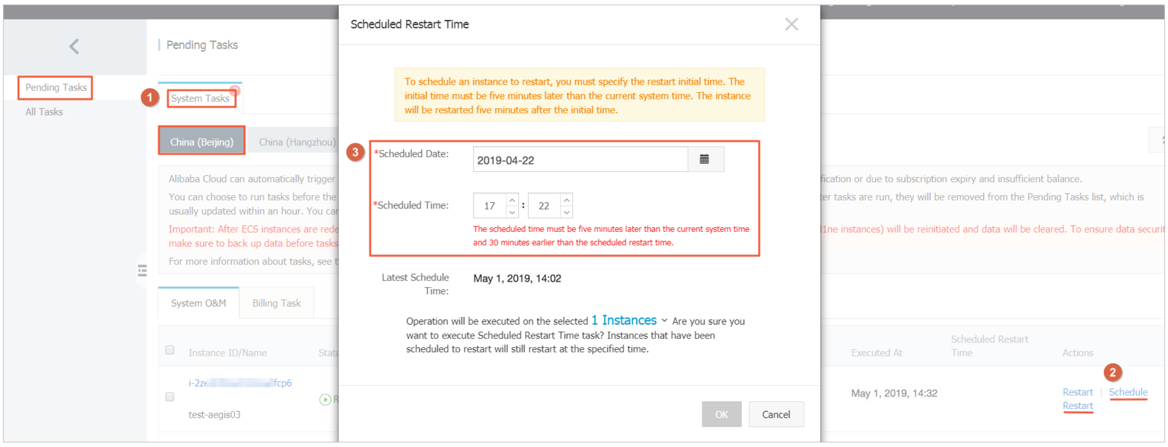
Context

You can modify the execution time of a system event in the ECS console or manually restart an instance before the scheduled restart time. This operation is applicable only to system events that have restart plans, such as instance restart due to system maintenance.

Procedure

1.
2.
3. On the **System Events** tab, select a region.
4. Find the instance to be restarted and click **Schedule Restart** in the **Actions** column.
5. In the **Scheduled Restart Time** dialog box, specify **Scheduled Date** and **Scheduled Time**.

> ? **Note** The scheduled restart time cannot be later than the **Latest Schedule Time**. The **Latest Schedule Time** is 30 minutes earlier than the **planned execution time**.



Alibaba Cloud can automatically trigger … fication or due to subscription expiry and insufficient balance.
You can choose to run tasks before the … er tasks are run, they will be removed from the Pending Tasks list, which is usually updated within an hour. You ca
Important: After ECS instances are rede … 1ne instances) will be reinitiated and data will be cleared. To ensure data securi … make sure to back up data before tasks
For more information about tasks, see t

Scheduled Restart Time

To schedule an instance to restart, you must specify the restart initial time. The initial time must be five minutes later than the current system time. The instance will be restarted five minutes after the initial time.

*Scheduled Date: 2019-04-22

*Scheduled Time: 17 : 22

The scheduled time must be five minutes later than the current system time and 30 minutes earlier than the scheduled restart time.

Latest Schedule Time: May 1, 2019, 14:02

Operation will be executed on the selected 1 Instances Are you sure you want to execute Scheduled Restart Time task? Instances that have been scheduled to restart will still restart at the specified time.

6. Click **OK**.

3.Instance issue identification and troubleshooting

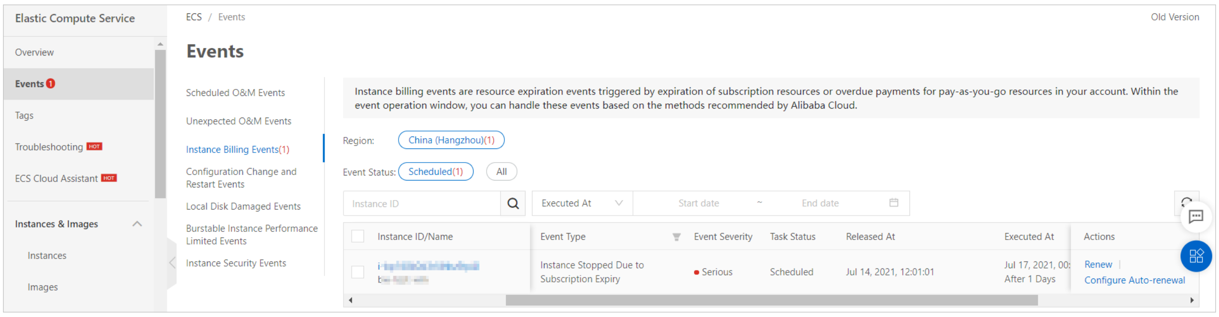
3.1. Identify and troubleshoot instance issues

You can use Elastic Compute Service (ECS) monitoring features to identify and troubleshoot instance issues and address potential risks before they affect your business.

Handle system events in a timely manner

When the system performs O&M and identifies issues that affect the running of ECS instances, system event notifications are sent. System event notifications provide information such as solutions and event cycles. We recommend that you handle system events in a timely manner to prevent consequences of system events such as instance restart and stop from affecting your business deployed on the instances. For more information, see Overview.

When a subscription instance expires, a system event is displayed in the ECS console, as shown in the following figure.



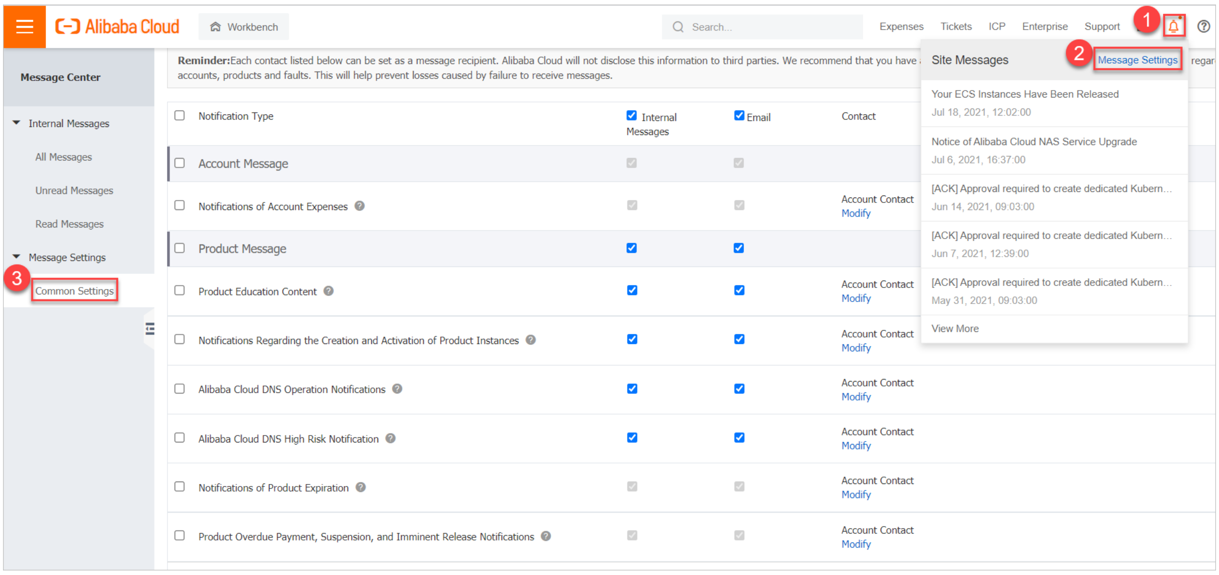
Instance billing events are resource expiration events triggered by expiration of subscription resources or overdue payments for pay-as-you-go resources in your account. Within the event operation window, you can handle these events based on the methods recommended by Alibaba Cloud.

Region: China (Hangzhou)(1)

Event Status: Scheduled(1) All

□	Instance ID/Name	Event Type	Event Severity	Task Status	Released At	Executed At	Actions
□	[redacted]	Instance Stopped Due to Subscription Expiry	● Serious	Scheduled	Jul 14, 2021, 12:01:01	Jul 17, 2021, 00: After 1 Days	Renew | Configure Auto-renewal

Make sure that internal messages for instance expiration, service O&M, and instance issues are enabled on the Common Settings page in the Message Center console, as shown in the following figure. Otherwise, you cannot receive system event notifications in the ECS console.



Reminder: Each contact listed below can be set as a message recipient. Alibaba Cloud will not disclose this information to third parties. We recommend that you have a accounts, products and faults. This will help prevent losses caused by failure to receive messages.

□ Notification Type	☑ Internal Messages	☑ Email	Contact
□ Account Message	☑	☑	
□ Notifications of Account Expenses	☑	☑	Account Contact Modify
□ Product Message	☑	☑	
□ Product Education Content	☑	☑	Account Contact Modify
□ Notifications Regarding the Creation and Activation of Product Instances	☑	☑	Account Contact Modify
□ Alibaba Cloud DNS Operation Notifications	☑	☑	Account Contact Modify
□ Alibaba Cloud DNS High Risk Notification	☑	☑	Account Contact Modify
□ Notifications of Product Expiration	☑	☑	Account Contact Modify
□ Product Overdue Payment, Suspension, and Imminent Release Notifications	☑	☑	Account Contact Modify

Site Messages

Your ECS Instances Have Been Released
Jul 18, 2021, 12:02:00

Notice of Alibaba Cloud NAS Service Upgrade
Jul 6, 2021, 16:37:00

[ACK] Approval required to create dedicated Kubern...
Jun 14, 2021, 09:03:00

[ACK] Approval required to create dedicated Kubern...
Jun 7, 2021, 12:39:00

[ACK] Approval required to create dedicated Kubern...
May 31, 2021, 09:03:00

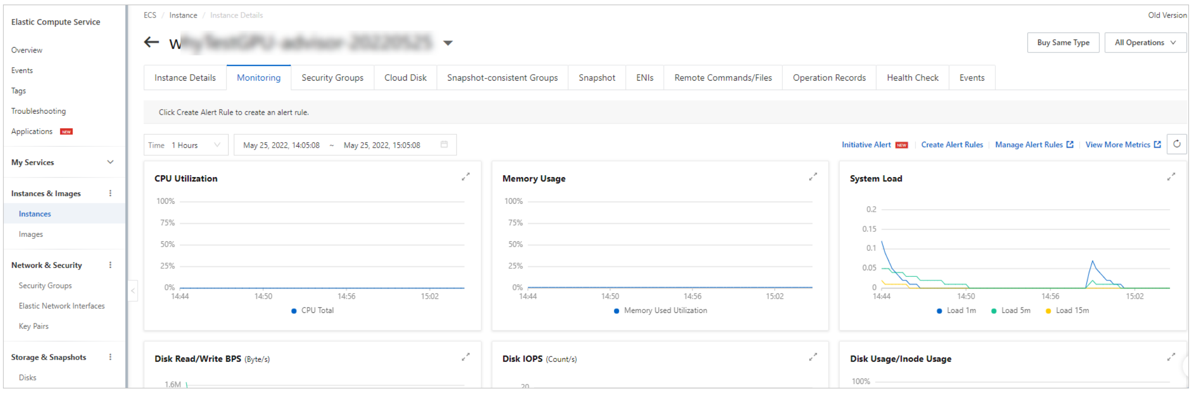
View More

Monitor the running metrics of instances

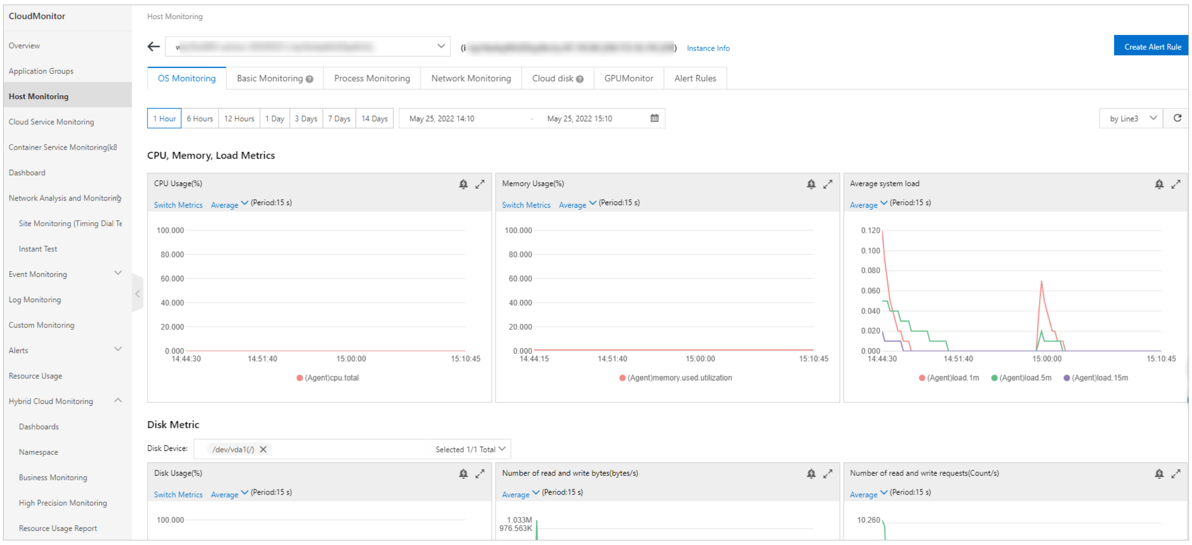
Alibaba Cloud collects and shows the running metrics of your instances to help you understand their real-time and historical running status. You can check whether instances are running normally based on their running metrics. If the CPU utilization of an instance is consistently high, you can check whether processes on the instance are abnormal or whether the configurations of the instance cannot meet your requirements.

You can view the running metrics of an instance on the Instance Details page in the ECS console or on the Host Monitoring page in the CloudMonitor console. For more information, see View the monitoring information of an instance and Overview

- The following running metrics of an instance are displayed on the Instance Details page in the ECS console:
    - The usage of computing, storage, and network resources such as the CPU utilization, disk read/write performance, and packet forwarding rate
    - The CPU credit usage of a burstable instance



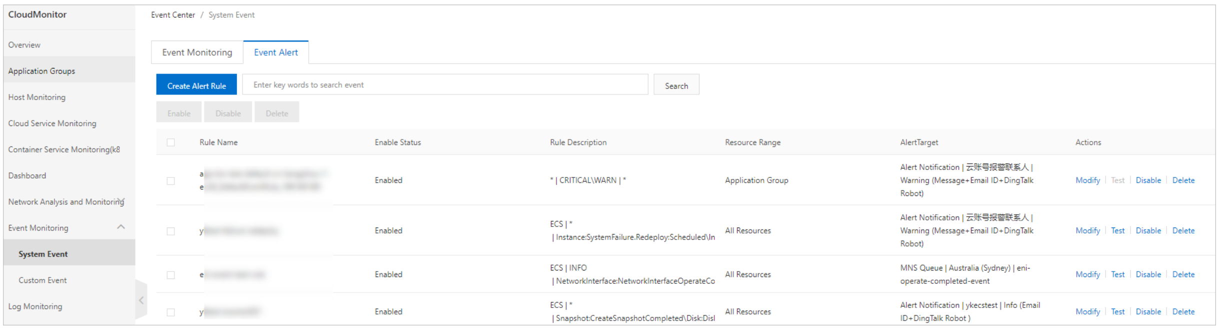
- The following running metrics of an instance are displayed on the Host Monitoring page in the CloudMonitor console:
    - The usage of computing, storage, and network resources such as the CPU utilization, disk read/write performance, and packet forwarding rate
    - The active processes on an instance
    - The GPU memory usage of a GPU-accelerated instance



Use the alerting feature to trigger notifications

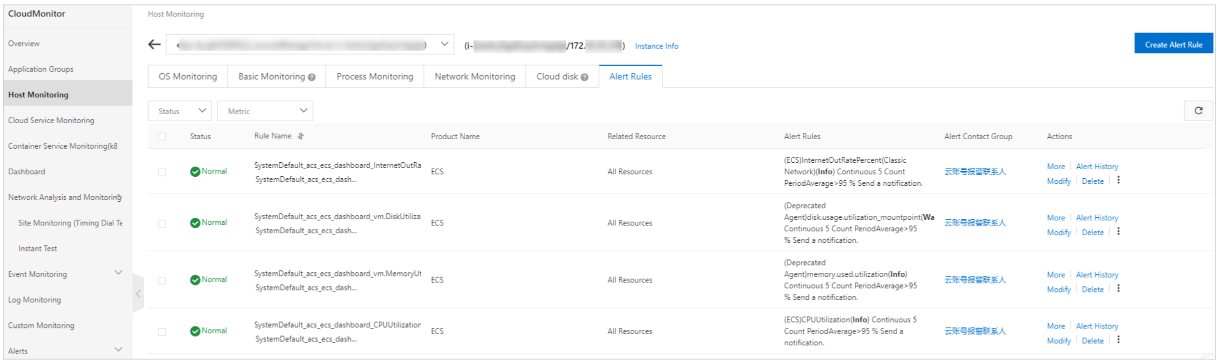
You can use the alerting feature of CloudMonitor to set alert rules for specified events and instance running metrics. When specified events occur or when instance running metrics are abnormal, notifications are sent to the contacts by email. This reduces manual O&M workloads. For more information, see Configure event notifications and Configure alerts for an ECS instance.

You can set an alert rule for a specified event, as shown in the following figure.



Rule Name	Enable Status	Rule Description	Resource Range	AlertTarget	Actions
a[redacted] e[redacted]	Enabled	* | CRITICAL\WARN | *	Application Group	Alert Notification | 云账号报警联系人 | Warning (Message+Email ID+DingTalk Robot)	Modify | Test | Disable | Delete
y[redacted]	Enabled	ECS | * | Instance:SystemFailure.Redeploy:Scheduled\In	All Resources	Alert Notification | 云账号报警联系人 | Warning (Message+Email ID+DingTalk Robot)	Modify | Test | Disable | Delete
e[redacted]	Enabled	ECS | INFO | NetworkInterface:NetworkInterfaceOperateCo	All Resources	MNS Queue | Australia (Sydney) | eni-operate-completed-event	Modify | Test | Disable | Delete
y[redacted]	Enabled	ECS | * | Snapshot:CreateSnapshotCompleted\Disk:Disl	All Resources	Alert Notification | ykecstest | Info (Email ID+DingTalk Robot)	Modify | Test | Disable | Delete

You can set alert rules for instance running metrics, as shown in the following figure.



Status	Rule Name	Product Name	Related Resource	Alert Rules	Alert Contact Group	Actions
Normal	SystemDefault_acs_ecs_dashboard_InternetOutRa SystemDefault_acs_ecs_dash...	ECS	All Resources	(ECS)InternetOutRatePercent(Classic Network)(**Info**) Continuous 5 Count PeriodAverage>95 % Send a notification.	云账号报警联系人	More | Alert History Modify | Delete | ⋮
Normal	SystemDefault_acs_ecs_dashboard_vm.DiskUtiliza SystemDefault_acs_ecs_dash...	ECS	All Resources	(Deprecated Agent)disk.usage.utilization_mountpoint(**Wa** Continuous 5 Count PeriodAverage>95 % Send a notification.	云账号报警联系人	More | Alert History Modify | Delete | ⋮
Normal	SystemDefault_acs_ecs_dashboard_vm.MemoryUt SystemDefault_acs_ecs_dash...	ECS	All Resources	(Deprecated Agent)memory.used.utilization(**Info**) Continuous 5 Count PeriodAverage>95 % Send a notification.	云账号报警联系人	More | Alert History Modify | Delete | ⋮
Normal	SystemDefault_acs_ecs_dashboard_CPUUtilization SystemDefault_acs_ecs_dash...	ECS	All Resources	(ECS)CPUUtilization(**Info**) Continuous 5 Count PeriodAverage>95 % Send a notification.	云账号报警联系人	More | Alert History Modify | Delete | ⋮

3.2. View the monitoring information of an instance

You can monitor the health of your Elastic Compute Service (ECS) instances to ensure that your users can always access your websites and applications, process data, or render videos. Alibaba Cloud provides data monitoring, visualization of monitoring data, and real-time alerts to help ensure that your ECS instances are running normally.

Context

You can monitor your ECS instances by using the ECS monitoring service or CloudMonitor. ECS provides monitoring of vCPU utilization, network traffic, and disk I/O for instances. CloudMonitor provides finer-grained monitoring of resources. The following section describes some of the monitoring metrics for ECS instances:

- vCPU utilization: the percentage of allocated compute units that are currently in use on an ECS instance. A higher percentage indicates a higher vCPU load on the instance. You can view the monitoring data of an ECS instance by using the ECS or CloudMonitor console or by calling ECS API operations. You can also connect to an ECS instance to view its monitoring data. You can use one of the following methods to view the vCPU utilization of an ECS instance after you connect to the instance:

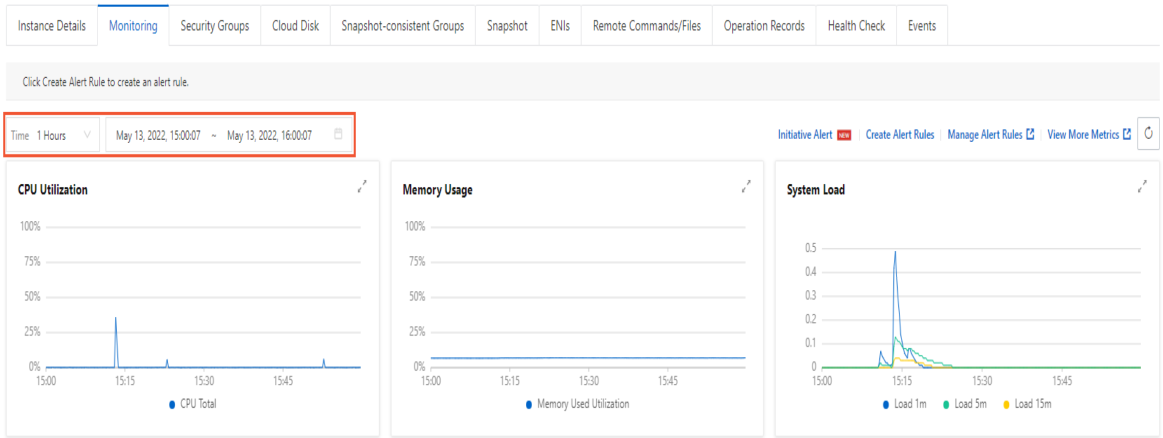
- Windows instance: View the vCPU utilization in **Task Manager**. You can sort processes by vCPU utilization to identify processes that are consuming the vCPUs of the specified ECS instance.
- Linux instance: Run the **top** command on an ECS instance to view its vCPU utilization. Press **Shift+P** to sort processes by vCPU utilization and identify processes that are consuming the vCPUs of the ECS instance.

- Network traffic-related metrics: the inbound and outbound bandwidth usages of the ECS instance in Kbit/s. ECS monitors public bandwidth usage, whereas CloudMonitor monitors both public and internal bandwidth usages. If an outbound public bandwidth of 1,024 Kbit/s is allocated to an ECS instance and the outbound public bandwidth usage by the instance reaches 1 Mbit/s, the allocated outbound public bandwidth is fully utilized.

ECS monitoring service

To view monitoring data in the ECS console, perform the following steps.

1.
2.
3.
4. On the Instances page, find the instance that you want to monitor and click its ID.
5. On the **Instance Details** page, click the **Monitoring** tab.
6. Specify the time period to query and view monitoring data such as vCPU utilization.



Click Create Alert Rule to create an alert rule.

Time 1 Hours

May 13, 2022, 15:00:07 ~ May 13, 2022, 16:00:07

> **Note** The length of the specified time period affects the granularity of the data displayed. The longer the time period, the finer granularity of the data displayed. For example, the average values for monitoring data within 1 hour and within 6 hours are different.

You can also call ECS API operations such as DescribeInstanceMonitorData, DescribeDiskMonitorData, and DescribeEniMonitorData to query monitoring data.

The following table describes the monitoring metrics in ECS. The sampling interval for each metric is 1 minute.

Metric	Description	Unit
CPUUtilization	The CPU utilization.	%

Metric	Description	Unit
InternetInRate(Classic Network)	The average rate of inbound traffic over the Internet.	bit/s
IntranetInRate	The average rate of inbound traffic over the internal network.	bit/s
InternetOutRate(Classic Network)	The average rate of outbound traffic over the Internet.	bit/s
IntranetOutRate	The average rate of outbound traffic over the internal network.	bit/s
DiskReadBPS	The number of bytes that are read from the system disk per second.	Byte/s
DiskWriteBPS	The number of bytes that are written to the system disk per second.	Byte/s
DiskReadIOPS	The number of read operations that are performed on the system disks per second.	Read IOPS
DiskWriteIOPS	The number of write operations that are performed on the system disks per second.	Write IOPS
InternetInRate_IP	The inbound public bandwidth.	bit/s
InternetOutRate_IP	The outbound public bandwidth.	bit/s
InternetOutRatePercent_IP	The outbound public bandwidth usage.	bit/s
InternetIn(Classic Network)	The amount of inbound traffic over the Internet.	Bytes
InternetOut(Classic Network)	The amount of outbound traffic over the Internet.	Bytes
IntranetInRate	The amount of inbound traffic over the internal network.	Bytes

CloudMonitor

CloudMonitor provides end-to-end and out-of-box monitoring solutions for enterprises in the cloud. CloudMonitor provides the host monitoring service to monitor ECS instances.

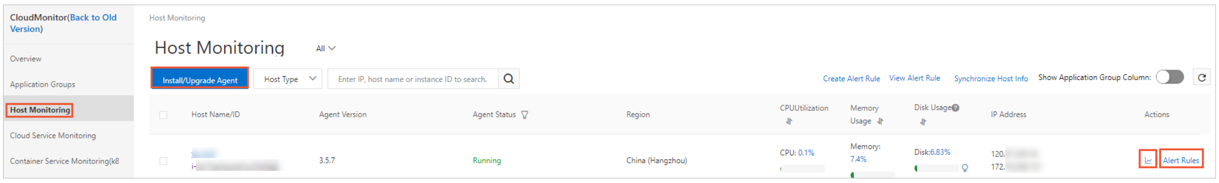
- For more information about the host monitoring service, see Overview.
- For information about the items and metrics related to the host monitoring service, see Metrics.

To obtain monitoring data of an ECS instance in the CloudMonitor console, perform the following steps.

1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, click **Host Monitoring**.
3. Find the ECS instance that you want to monitor.
4. (Optional)If the CloudMonitor agent is not installed on the ECS instance, click **Install/Upgrade Agent**.
5. To obtain monitoring data, click the 📈 icon in the Actions column.

> **Note** Monitoring data can be retained for up to 30 days.

6. To configure alert rules, click **Alert Rules** in the Actions column.



	Host Name/ID	Agent Version	Agent Status	Region	CPUUtilization	Memory Usage	Disk Usage	IP Address	Actions
□	[redacted]	3.5.7	Running	China (Hangzhou)	CPU: 0.1%	Memory: 7.4%	Disk:6.83%	120.[redacted] 172.[redacted]	📈 Alert Rules

Related information

- DescribeInstanceMonitorData
- DescribeDiskMonitorData
- DescribeEniMonitorData

3.3. View the health status of an instance

You can perform regular checks on an instance to monitor its health status. This topic describes how to view the health status of an instance by using the ECS console or calling API operations.

Context

The health status of an instance is centered around network configuration exceptions, software failure, and hardware usage. The system can record network, software, or hardware problems of an instance in a timely manner by monitoring the health status of the instance,.

This feature can be used together with the metric monitoring feature of Cloud Monitor to dynamically customize the standard health level of computing resource maintenance. For more information, see What is Cloud Monitor?

The following table describes the texts in the console and API parameter values that indicate the health status of instances.

Text in the console	API parameter value	Description	Alert color in the console
Passed	*Ok*	The instance has passed the health check.	Green

Text in the console	API parameter value	Description	Alert color in the console
Impaired	*Impaired*	The instance performance is deteriorated.	Red
Warning	*Warning*	The instance performance is at risk and may decline due to maintenance or technical problems.	
Maintaining System	*Maintaining*	The instance is under maintenance.	
Initializing	*Initializing*	The instance is being initialized.	
Insufficient Data	*InsufficientData*	The health status cannot be determined due to insufficient data.	
No Status	*NotApplicable*	The instance health status is not applicable.	

View the health status of an instance by using the ECS console

1.
2.
3.
4. Find the instance for which you want to view the health status and click the instance ID.
5. In the upper-right corner of the **Instance Details** page, view the health status of the instance.

View the health status of an instance by using Alibaba Cloud CLI

- Run the following command to call the DescribeInstances and DescribeInstancesFullStatus operations to view the health status of a specific instance:

```
aliyun ecs DescribeInstances --RegionId TheRegionId --output cols=InstanceId,InstanceName
rows=Instances.Instance[]
aliyun ecs DescribeInstancesFullStatus --RegionId TheRegionId --InstanceId.1 i-bp1afnc98r
8k69****** --output cols=HealthStatus rows=InstanceFullStatusSet.InstanceFullStatusType[]
```

- Run the following command to call the DescribeInstancesFullStatus operation to view the health status of all instances in a specific region. For more information about region IDs, see Regions and zones.

```
aliyun ecs DescribeInstancesFullStatus --RegionId TheRegionId --output cols=HealthStatus
rows=InstanceFullStatusSet.InstanceFullStatusType[]
```

After you submit a health check request, Alibaba Cloud returns the health check result for each instance included in the request.

- If the health check succeeds, *Ok* is returned.
- If the health check fails, other metrics are returned.

Related information

- DescribeInstances
- DescribeInstancesFullStatus

3.4. Configure alerts for an ECS instance

You can enable initiative alert on the details page of an ECS instance or configure custom alert rules to detect exceptions of an ECS instance in a timely manner.

Context

You can enable the initiative alert and custom alert rule features on the Monitoring tab of the instance details page.

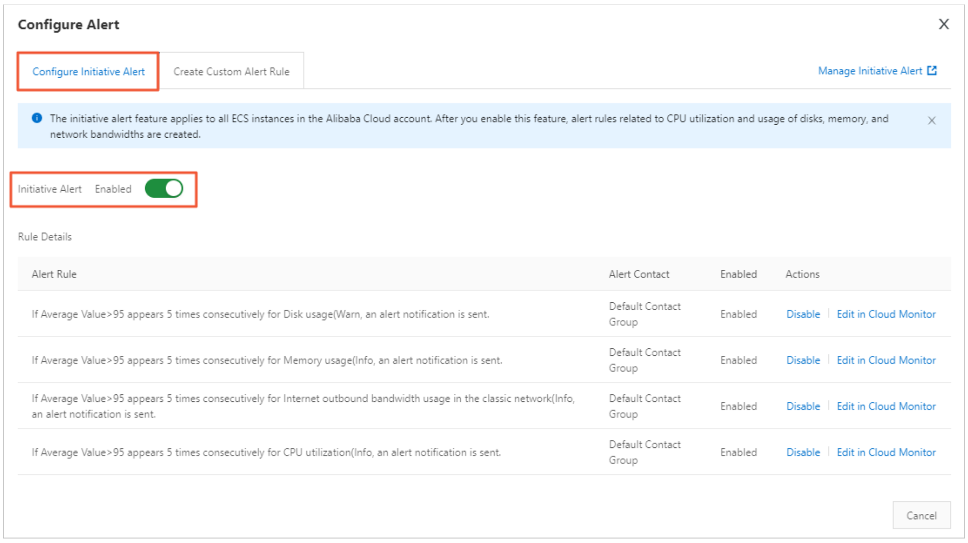
- After initiative alert is enabled, alert rules related to the CPU utilization, disk usage, memory usage, and network bandwidth usage are created for all ECS instances within your Alibaba Cloud account. For more information, see Enable initiative alert.
- You can configure custom alert rules for an ECS instance. These custom alert rules take effect only for the current ECS instance. For more information, see Configure custom alert rules.

If you want to manage alert rules or require more monitoring and alert features, you can go to the Cloud Monitor console. For more information, see What is CloudMonitor?

Enable initiative alert

You can enable initiative alert for key metrics of ECS to quickly establish an alert system and obtain the exception information of key metrics in a timely manner. After initiative alert is enabled, the related alert rules apply to all ECS instances within your Alibaba cloud account.

1.
2.
3.
4. Find the instance and click its ID.
5. On the **Instance Details** page, click the **Monitoring** tab.
6. Click **Initiative Alert**.
7. On the **Configure Initiative Alert** tab, turn on **Initiative Alert**.



The initiative alert feature applies to all ECS instances in the Alibaba Cloud account. After you enable this feature, alert rules related to CPU utilization and usage of disks, memory, and network bandwidths are created.

Initiative Alert Enabled

Rule Details

Alert Rule	Alert Contact	Enabled	Actions
If Average Value>95 appears 5 times consecutively for Disk usage(Warn, an alert notification is sent.	Default Contact Group	Enabled	Disable | Edit in Cloud Monitor
If Average Value>95 appears 5 times consecutively for Memory usage(Info, an alert notification is sent.	Default Contact Group	Enabled	Disable | Edit in Cloud Monitor
If Average Value>95 appears 5 times consecutively for Internet outbound bandwidth usage in the classic network(Info, an alert notification is sent.	Default Contact Group	Enabled	Disable | Edit in Cloud Monitor
If Average Value>95 appears 5 times consecutively for CPU utilization(Info, an alert notification is sent.	Default Contact Group	Enabled	Disable | Edit in Cloud Monitor

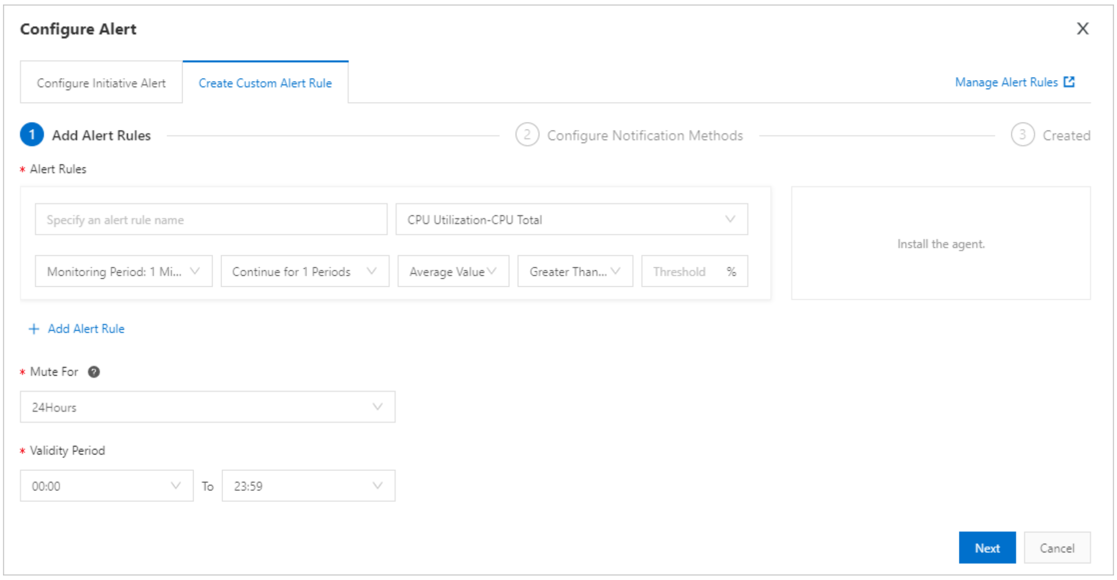
After initiative alert is enabled, you can view the details of an alert rule. You can also perform the following operations:

- Disable an alert rule: If you no longer need an alert rule, you can disable the rule.
- Modify an alert rule: If you find that an alert rule is not suitable for your business, you can go to the Cloud Monitor console to modify the rule.

Configure custom alert rules

In addition to initiative alert, you can also configure custom alert rules for your instance based on your business requirements. The created custom alert rules automatically take effect for the current instance, which allows you to learn about the exceptions of the instance in a timely manner.

1.
2.
3. Find the instance and click its ID.
4. On the **Instance Details** page, click the **Monitoring** tab.
5. Click **Create Alert Rules**.
6. On the **Create Custom Alert Rule** tab, create custom alert rules.
    i. Configure parameters for the alert rule and click **Next**.



Parameter	Description
Alert Rules	Specifies parameters for the alert rule, including the name and content of the alert rule. This parameter specifies the condition that triggers an alert. For example, if the condition specifies that the average CPU utilization every 5 minutes is greater than or equal to 90% for three consecutive cycles, Cloud Monitor checks whether the condition is met every 5 minutes only three times. Note ■ For information about the ECS metrics of alert rules, see Metrics. ■ You can click **Add Alert Rule** to create multiple alert rules.
Mute For	Specifies the mute period. If the alert is not cleared within the mute period, a new alert notification is sent when the mute period ends.
Validity Period	Specifies the period during which the alert rule is in effect. The system monitors the metrics and generates alerts only when the alert rule is in effect.

ii. Configure the parameters in the Configure Notification Methods step and click **Create**.

Parameter	Description
Alert Contact	The contacts or contact groups to which an alert notification is sent. For more information, see Create an alert contact or alert contact group.
Notification Methods	The method to receive alert notifications and the supplementary information of alert emails. The value is set to Email and Webhook URL. You can specify custom remarks that you want to include in the alert notification email.
Callback URL	The callback URL that can be accessed over the Internet. Cloud Monitor sends a POST request to push alert messages to the specified callback URL. Only HTTP requests are supported.

The created custom alert rule takes effect only for the current instance.

7. (Optional)You can click **Manage Alert Rules** on the **Monitoring** tab to go to the Cloud Monitor console to view or modify the custom alert rule.

References

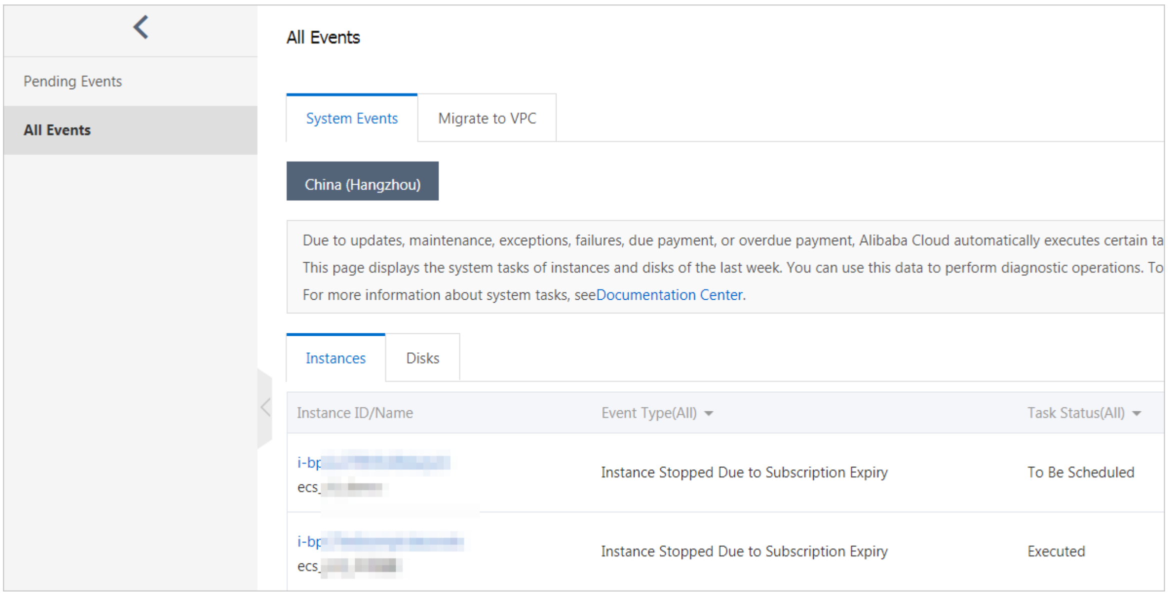
- What is CloudMonitor?
- Enable the initiative alert feature
- Manage alert rules

3.5. View system event history

This topic describes how to view system events. You can query system events that were handled within the last week in the ECS console and obtain data for troubleshooting and analysis.

View system event history in the ECS console

1.
2.
3. In the left-side navigation pane, click **All Events**.
4. On the **All Events** page, click the **System Events** tab to view system events in different regions, instance IDs, event types, and event states.



All Events

Due to updates, maintenance, exceptions, failures, due payment, or overdue payment, Alibaba Cloud automatically executes certain ta
This page displays the system tasks of instances and disks of the last week. You can use this data to perform diagnostic operations. To
For more information about system tasks, seeDocumentation Center.

Instance ID/Name	Event Type(All)	Task Status(All)
i-bp[redacted] ecs_[redacted]	Instance Stopped Due to Subscription Expiry	To Be Scheduled
i-bp[redacted] ecs_[redacted]	Instance Stopped Due to Subscription Expiry	Executed

View system event history by using Alibaba Cloud CLI

1. Obtain the instance ID.

```
aliyun ecs DescribeInstances --RegionId <TheRegionId> --output cols=InstanceId,Instance
Name rows=Instances.Instance[]
```

2. Call the DescribeInstanceHistoryEvents operation to query the system event history of the instance.

```
aliyun ecs DescribeInstanceHistoryEvents --RegionId <TheRegionId> --InstanceId i-bp13kp
qetxnp2a****** --output cols=EventId,EventTypeName rows=InstanceSystemEventSet.Instance
SystemEventType[]
```

Related information

- DescribeInstanceHistoryEvents

4.Cloud assistant

4.1. Overview

Cloud Assistant is a native automated operations and maintenance (O&M) tool developed for Elastic Compute Service (ECS). It allows you to batch maintain ECS instances and batch execute scripts on and send files to ECS instances in a password-free, logon-free manner without the use of jumper servers. Typically, you can use Cloud Assistant to install and uninstall software, start and stop services, distribute configuration files, and execute commonly used commands or scripts.

Features

After ECS instances that are installed with the Cloud Assistant client enter the **Running** (`Running`) state, you can use Cloud Assistant to perform the following operations on the instances by using the ECS console or by calling API operations:

- Run batch and PowerShell scripts on Windows instances, or run shell scripts on Linux instances.
- Upload files to the instances.
- Run the same command on multiple instances. The execution state and results of one instance do not affect the other instances.
- Configure custom parameters in Cloud Assistant commands to adapt to different scenarios.

> **Note** Cloud Assistant does not proactively initiate operations. You have full control over all Cloud Assistant operations.

Use scenarios

Cloud Assistant can help you perform deployment and O&M tasks on ECS instances. The following list provides some examples:

- Uploading and running automated O&M scripts
- Running the scripts that are already installed on instances
- Managing software lifecycle
- Deploying code or applications
- Polling processes
- Installing patches or security updates
- Obtaining updates from Object Storage Service (OSS) or YUM repositories
- Changing hostnames or user logon passwords

Billing

Cloud Assistant is provided free of charge.

However, you may be charged for the ECS resources used by Cloud Assistant to execute deployment and O&M tasks. For more information about the billing of ECS resources, see Overview.

Limits

- Only API operations can be used to configure the recurring executions of a Cloud Assistant command. The interval at which the command is run cannot be less than 10 seconds.

- For each command, the total size of the Base64-encoded batch, PowerShell, or shell scripts together with the Base64-encoded custom parameters cannot exceed 16 KB.
- The size of a Base64-encoded file to send cannot exceed 32 KB.
- Each command can contain a maximum of 20 custom parameters.
- Cloud Assistant commands can be run only on instances that use the following operating systems:
  - Alibaba Cloud Linux
  - CentOS 6, CentOS 7, and CentOS 8 and later
  - CoreOS
  - Debian 8, Debian 9, and Debian 10 and later
  - OpenSUSE
  - RedHat 5, RedHat 6, and RedHat 7 and later

    For Red Hat instances, you must download the RPM package to install the Cloud Assistant client. For more information, see Install the Cloud Assistant client.
  - SUSE Linux Enterprise Server (SLES) 11, SLES 12, and SLES 15 and later
  - Ubuntu 12, Ubuntu 14, Ubuntu 16, and Ubuntu 18 and later
  - Windows Server 2012, Windows Server 2016, and Windows Server 2019 and later

For more information about the limits and service quotas of Cloud Assistant, see the "Cloud Assistant limits" section of Limits.

Terms

The following table describes relevant terms in Cloud Assistant.

Term	Description
Cloud Assistant	A tool provided by Alibaba Cloud that can help you perform routine maintenance tasks on multiple ECS instances and ECS bare metal instances at a time. Cloud Assistant is available in all Alibaba Cloud regions.
Cloud Assistant client	A lightweight plug-in that can be installed on ECS instances to run Cloud Assistant commands. • On Windows instances, the process of the client program is AliyunService. • On Linux instances, the process of the client program is aliyun.service.
Cloud Assistant daemon process	A daemon process that is used to monitor the resource consumption of the Cloud Assistant client, report the running state of the client, and restart the client when the client fails. • Service name: `AssistDaemon` • Path: */usr/local/share/assist-daemon/assist_daemon* **Note** The Cloud Assistant daemon process is available only for Linux instances.

Term	Description
task execution path	A path in which Cloud Assistant saves your command as a file on an ECS instance and executes the file. The path varies based on the operating system. - Linux: */tmp* - Windows: *<Installation path of Cloud Assistant>/work/script*
command	A specific command such as a shell script or a PowerShell script that can be run on ECS instances.
custom parameter	A variable that is configured in the {{key}} format in a command. You can specify a custom parameter and its value in the {{"<key>":"<value>"}} format when you create a task to run the command. The number of Cloud Assistant commands that you can have within each Alibaba Cloud region is limited. To adapt Cloud Assistant commands to multiple scenarios, we recommend that you configure custom parameters.
one-time execution	An execution (`Invocation`) that runs a command only once on one or more instances.
recurring execution	An execution that periodically runs a command on one or more instances based on your specified schedule.
execution state	The relationships among different types of execution states. For more information, see Execution states.

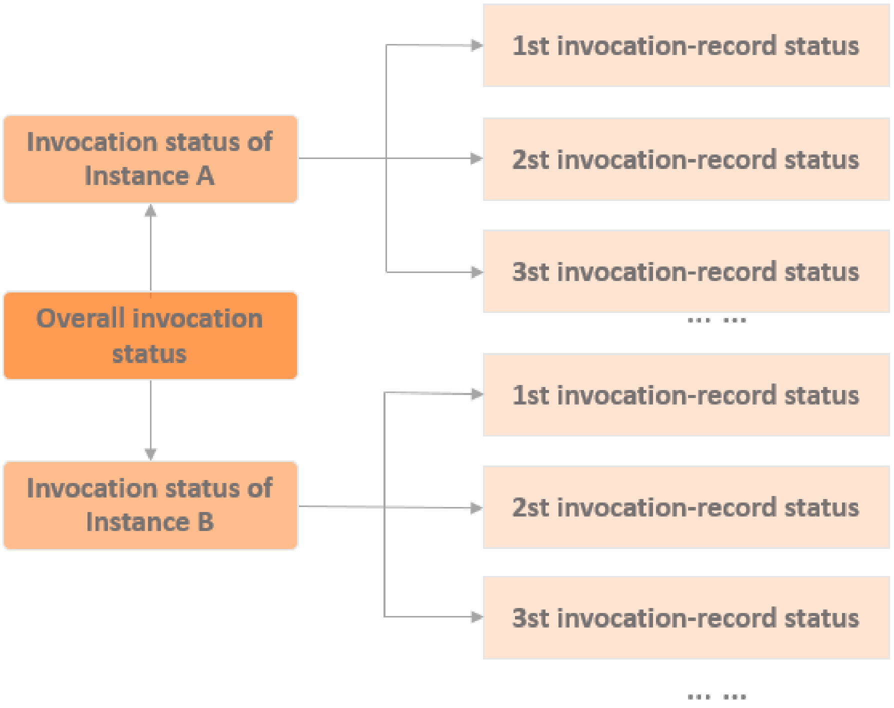
Execution states

The following table describes the instance-level execution state of a command that is run on a single instance. The InvocationStatus parameter in API indicates the execution state of a command.

Execution state in an API operation	Execution state in the ECS console	Description
`Running`	Task Running	The command is being run.
`Stopping`	Task Stopping	The command is being stopped.
`Stopped`	Manually Stopped	The command is stopped.
`Finished`	Task Completed	The command is run to completion. This does not indicate that the command succeeds. You can check whether the command succeeds based on the output (`Output`) and the exit code (`ExitCode`).
`Failed`	Task Failed	The command cannot be run or the command process cannot run to completion before the timeout period specified by `Timeout` expires.

States of batch executions and recurring executions

A batch execution is a one-time execution that runs a command on multiple instances. To better manage batch executions and recurring executions, you can manage the lifecycles of the executions based on the overall execution status, the instance-level execution status, and the record-level execution status. The InvokeStatus parameter in API indicates the execution status of a command. The following figure shows the relationships among the three types of execution states.

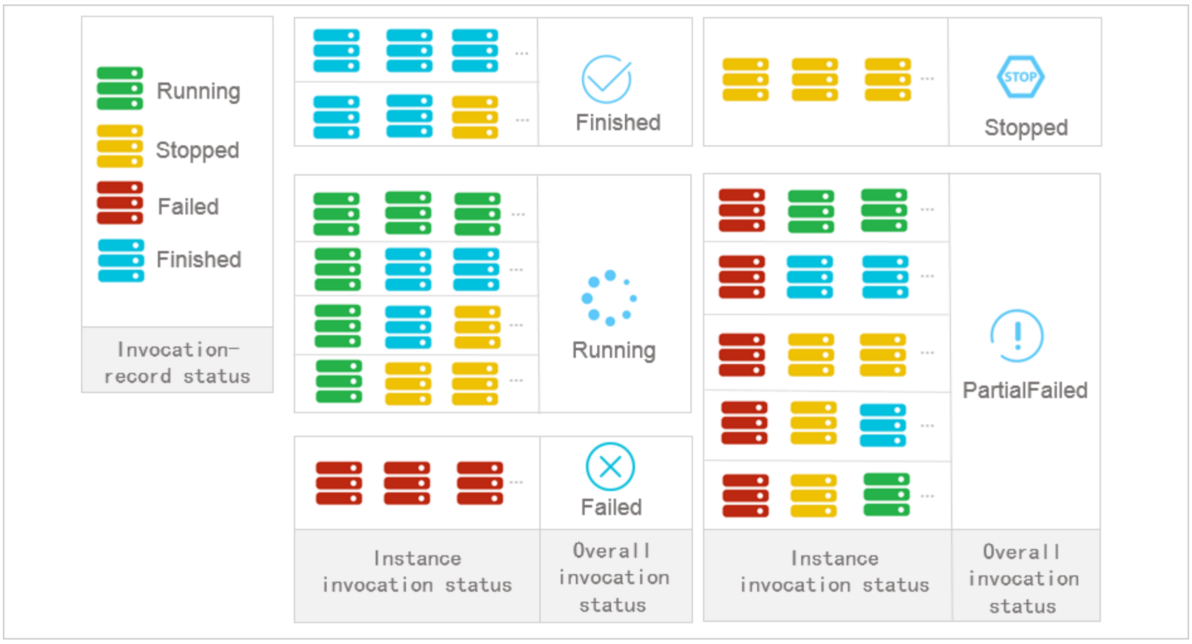

Invocation status of Instance A
Overall invocation status
Invocation status of Instance B
1st invocation-record status
2st invocation-record status
3st invocation-record status
... ...
1st invocation-record status
2st invocation-record status
3st invocation-record status
... ...

- The following table describes the overall execution states of a command that is run on multiple instances at the same time.

Execution state in an API operation	Execution state in the ECS console	Description	Priority
`Running`	Task Running	The instance-level execution state is Running on some or all instances.	1
`Stopping`	Task Stopping	The instance-level execution state is Stopping on some or all instances.	2
`Stopped`	Manually Stopped	The instance-level execution state is Stopped on all instances.	3
`Failed`	Task Failed	The instance-level execution state is Failed on all instances, or is Failed on some instances and is Stopped on the other instances.	4
`Finished`	Task Completed	The instance-level execution state is Finished on all instances, or is Finished on some instances and is Stopped on the other instances.	5

Execution state in an API operation	Execution state in the ECS console	Description	Priority
`PartialFailed`	Partially Failed	The instance-level execution state is Failed on some instances and is Finished on the other instances.	6

The following figure shows the relationship between the overall execution states and the instance-level execution states of a one-time execution that runs a command on three instances at the same time.


Running
Stopped
Failed
Finished
Invocation-record status
Finished
Stopped
Running
PartialFailed
Failed
Instance invocation status
Overall invocation status
Instance invocation status
Overall invocation status

- The following table describes the states of recurring executions of a command.

State	Description
Overall execution state	The overall execution state is always **Running** (`Running`) unless you stop the command on all the instances.
Instance-level execution state	For each instance, the instance-level execution state is always **Running** (`Running`) unless you stop the command on the instance.
Record-level execution state	For more information, see Execution states.

Related operations

You can use Cloud Assistant by using the ECS console or by calling an API operation.

Business requirement	References	API operation
The Cloud Assistant client must be installed on an ECS instance before Cloud Assistant can be used on the instance. By default, ECS instances that were created after December 01, 2017 from public images have the Cloud Assistant client pre-installed. You must manually install the Cloud Assistant client on some ECS instances.	Install the Cloud Assistant client	• InstallCloudAssistant • DescribeCloudAssistantStatus
You are familiar with using OpenAPI Explorer and this is the first time that you use Cloud Assistant.	• Use Java to manage ECS instances without logging on to the instances • Use Python to manage ECS instances without logging on to the instances	N/A
Create a Cloud Assistant command.	Create a command	• RunCommand • CreateCommand
Run a created command on ECS instances.	Run a command	• RunCommand • InvokeCommand
View the execution states and results of commands. Execution results are the actual outputs generated on the specified instances.	Query execution results and fix common problems	• DescribeInvocations • DescribeInvocationResults
Modify a created command. You can modify the name and description of the command.	Modify a command	N/A
Create a new version of a Cloud Assistant command or modify the properties of the command such as the name, description, type, content, execution path, or timeout period.	Clone a command	N/A
Stop a running command.	Stop a command	StopInvocation
Delete Cloud Assistant commands that are no longer needed to free up quotas for new commands.	Delete a command	DeleteCommand

4.2. Manage servers that are not provided by Alibaba Cloud

Register managed instances

This topic describes how to register a non-Alibaba Cloud server as an instance that can be managed by Alibaba Cloud. After a server is registered as a managed instance, the server can use a variety of online services provided by Alibaba Cloud such as Cloud Assistant, Operation Orchestration Service (OOS), and Alibaba Cloud DevOps.

Prerequisites

- The server runs an operating system of one of the following versions:
  - Alibaba Cloud Linux 2 and Alibaba Cloud Linux 3 and later
  - CentOS 6, CentOS 7, and CentOS 8 and later
  - CoreOS
  - Debian 8, Debian 9, and Debian 10 and later
  - OpenSUSE
  - RedHat 5, RedHat 6, and RedHat 7 and later
  - SUSE Linux Enterprise Server (SLES) 11, SLES 12, and SLES 15 and later
  - Ubuntu 12, Ubuntu 14, Ubuntu 16, and Ubuntu 18 and later
  - Windows Server 2012, Windows Server 2016, and Windows Server 2019 and later
- The server can access the Internet.

Preparations

Non-Alibaba Cloud servers can be registered as managed instances in the following regions: China (Qingdao), China (Beijing), China (Zhangjiakou), China (Hohhot), China (Ulanqab), China (Hangzhou), China (Shanghai), China (Shenzhen), China (Heyuan), China (Hong Kong), Singapore (Singapore), and Japan (Tokyo). You can choose the region that best suits your server.

For example, you can run the Ping command to test the connection speed and choose the region where your server is connected at the fastest speed.

- Run the following command to test the connection to the server in the China (Beijing) region:

  ```
  ping -c 4 cn-beijing.axt.aliyuncs.com
  ```

- Run the following command to test the connection to the server in the China (Hangzhou) region:

  ```
  ping -c 4 cn-hangzhou.axt.aliyuncs.com
  ```

- Run the following command to test the connection to the server in the China (Shanghai) region:

  ```
  ping -c 4 cn-shanghai.axt.aliyuncs.com
  ```

Procedure

Perform the following steps to register your servers as managed instances based on whether the servers can directly access the Internet.

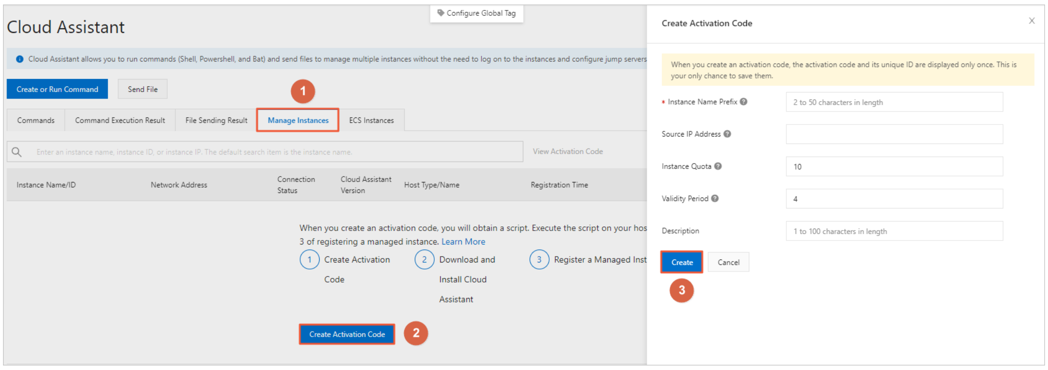
- Perform the following steps if your server can directly access the Internet:
  i. Step 1: Create an activation code for managed instances
  ii. Step 2: Install the Cloud Assistant client on a server and register the server as a managed instance (common method)
  iii. Step 3: View the managed instance in the ECS console

- Perform the following steps if you must configure a proxy server for your server to access the Internet:
    i. Step 1: Create an activation code for managed instances
    ii. Step 2: Install the Cloud Assistant client on a server and register the server as a managed instance (proxy method)
    iii. Step 3: View the managed instance in the ECS console

Step 1: Create an activation code for managed instances

This section describes how to create an activation code for managed instances in the Elastic Compute Service (ECS) console and generate an installation script.

1.
2.
3.
4. On the Cloud Assistant page, click the **Manage Instances** tab.



Cloud Assistant allows you to run commands (Shell, Powershell, and Bat) and send files to manage multiple instances without the need to log on to the instances and configure jump servers

When you create an activation code, you will obtain a script. Execute the script on your hos
3 of registering a managed instance. Learn More

When you create an activation code, the activation code and its unique ID are displayed only once. This is your only chance to save them.

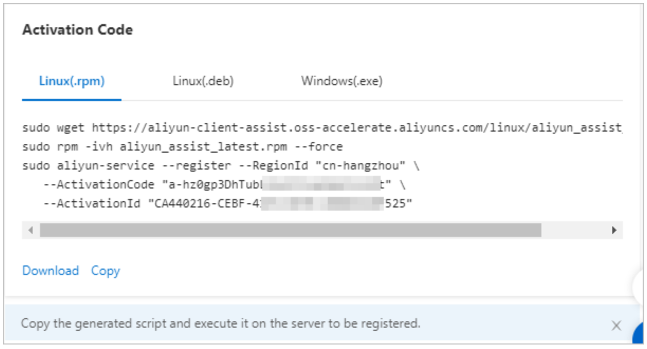
* Instance Name Prefix	2 to 50 characters in length
Source IP Address	
Instance Quota	10
Validity Period	4
Description	1 to 100 characters in length

5. Click **Create Activation Code**.
6. In the **Create Activation Code** panel, configure the parameters described in the following table.

Parameter	Description
Instance Name Prefix	Specifies the prefix of the names of instances to be managed for subsequent management.
Source IP Address	Specifies the IP addresses or CIDR blocks of managed instances. ○ If you enter the public IP addresses or CIDR blocks of servers, only the servers whose IP addresses are within the specified range can be managed. ○ If you do not specify this parameter, all servers can be managed.
Instance Quota	Specifies the number of managed instances. Valid values: 1 to 1000. Default value: 10.
Validity Period	Specifies the validity period of the activation code. If the activation code is not used until the validity period ends, the activation code cannot be used and you must create another one. Valid values: 1 to 24. Default value: 4. Unit: hours.

Parameter	Description
Description	Specifies the description of the activation code. You can enter information such as the purpose of the code for subsequent management.

7. Click **Create**.
   After the activation code is generated, installation scripts are generated.



Activation Code

```
sudo wget https://aliyun-client-assist.oss-accelerate.aliyuncs.com/linux/aliyun_assist
sudo rpm -ivh aliyun_assist_latest.rpm --force
sudo aliyun-service --register --RegionId "cn-hangzhou" \
   --ActivationCode "a-hz0gp3DhTubl[redacted]t" \
   --ActivationId "CA440216-CEBF-4[redacted]525"
```

Copy the generated script and execute it on the server to be registered.

8. Select an installation script suitable for the operating system type of your server and click **Download** or **Copy** to save the script to your computer.

> Notice
>
> - After the activation code is generated, the installation scripts are displayed only once. You must save the suitable installation scripts to your computer.
> - If your servers runs different operating systems, you must download the corresponding installation scripts.

Step 2: Install the Cloud Assistant client on a server and register the server as a managed instance (common method)

After you obtain the installation script, you must install the Cloud Assistant client on your server and register the server as a managed instance. If your server can access the Internet, perform the following steps. If your server must use a proxy server to access the Internet, see the Step 2: Install the Cloud Assistant client on a server and register the server as a managed instance (proxy method) section.

Install the Cloud Assistant client on a Linux server and register the server as a managed instance

1. Log on to the server by using SSH.
2. Create an installation script in the server.
   i. Run the following command to create a script by using the VIM editor:

      ```
      vim installAssistant.sh
      ```

   ii. Press the `I` key to enter the edit mode.
   iii. Paste the content of the script generated in the ECS console. For more information, see the Step 1: Create an activation code for managed instances section.
   iv. Press the `Esc` key to exit the edit mode.

v. Enter `:wq` and press the `Enter` key to save and exit the script.

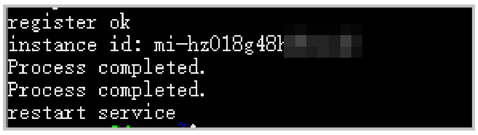
3. Run the following command to grant execution permissions on the installation script:

```
sudo chmod 755 installAssistant.sh
```

4. Run the following command to install the Cloud Assistant client on the server:

```
sudo ./installAssistant.sh
```

If the Cloud Assistant client is installed, a command output similar to the following one is returned.



```
register ok
instance id: mi-hz018g48[redacted]
Process completed.
Process completed.
restart service
```

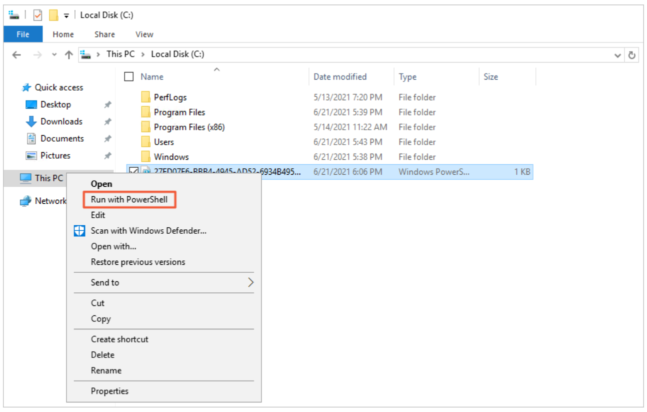
Install the Cloud Assistant client on a Windows server and register the server as a managed instance

1. Log on to the server by using **Remote Desktop Connection**.
2. Upload the installation script to the server.

   For information about how to obtain the installation script, see the Step 1: Create an activation code for manage instances section in this topic.

   > **Note** **Remote Desktop Connection** allows you to directly copy and paste the script file to the server. If the script file cannot be directly copied due to network environment limits, you can upload scripts by using FTP or other software.

3. Right-click the installation script and select **Run with PowerShell** to install the Cloud Assistant client.



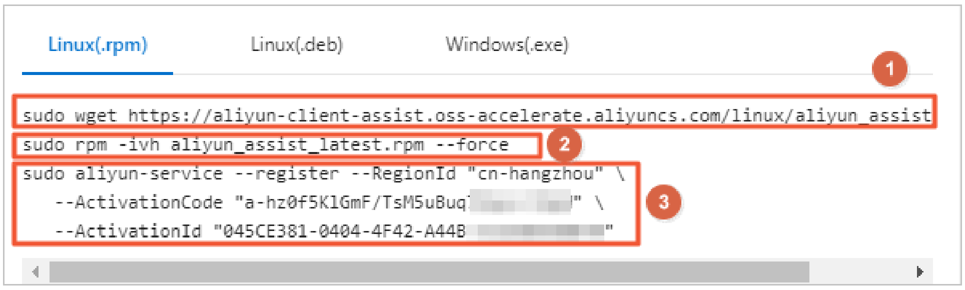
Name	Date modified	Type	Size
PerfLogs	5/13/2021 7:20 PM	File folder	
Program Files	6/21/2021 5:39 PM	File folder	
Program Files (x86)	5/14/2021 11:22 AM	File folder	
Users	6/21/2021 5:43 PM	File folder	
Windows	6/21/2021 5:38 PM	File folder	
27ED07E6-BBB4-4945-AD52-6934B495...	6/21/2021 6:06 PM	Windows PowerS...	1 KB

Step 2: Install the Cloud Assistant client on a server and register the server as a managed instance (proxy method)

After you obtain the installation script, you must install the Cloud Assistant client on your server and register the server as a managed instance. If your server can access the Internet, perform the following steps. If your server must use a proxy server to access the Internet, see the Step 2: Install the Cloud Assistant client on a server and register the server as a managed instance (common method) section.

Install the Cloud Assistant client on a Linux server and register the server as a managed instance

This section describes how to configure a proxy server. In this example, a server that runs CentOS 7.8 is used. If your server runs an operating system such as Debian, you must modify the commands shown in the following figure based on the installation script generated in the ECS console.



```
sudo wget https://aliyun-client-assist.oss-accelerate.aliyuncs.com/linux/aliyun_assist
sudo rpm -ivh aliyun_assist_latest.rpm --force
sudo aliyun-service --register --RegionId "cn-hangzhou" \
   --ActivationCode "a-hz0f5K1GmF/TsM5uBuq[redacted]" \
   --ActivationId "045CE381-0404-4F42-A44B[redacted]"
```

- ①: Download the installation package of the Cloud Assistant client
- ②: Install the Cloud Assistant client
- ③: Register the server as an instance managed by Cloud Assistant

If your server must use a proxy server to access the Internet, you must add the proxy server information to the commands.

1. Log on to the server by SSH.
2. Run the following command to download the Cloud Assistant client by using the proxy server:

   ```
   sudo https_proxy=<http://your_proxy_address> && wget https://aliyun-client-assist.oss-a
   ccelerate.aliyuncs.com/linux/aliyun_assist_latest.rpm
   ```

   Note You must replace `<http://your_proxy_address>` with the IP address of your proxy server.

3. Run the following command to install the Cloud Assistant client:

   ```
   sudo rpm -ivh aliyun_assist_latest.rpm --force
   ```

4. Configure a proxy server for Cloud Assistant.

   i. Modify the Cloud Assistant service configuration file.

      Modify the Cloud Assistant service configuration file and configure the ALIYUN_ASSIST_PROXY environment variable. Perform the following steps:

      a. Create the *vim /etc/sysconfig/aliyun* file by using the VIM editor.

         ```
         sudo vim /etc/sysconfig/aliyun
         ```

      b. Enter the following content. Then, save and exit the file.

         ```
         ALIYUN_ASSIST_PROXY=<http://your_proxy_address>
         ```

         Note You must replace `<http://your_proxy_address>` with the IP address of your proxy server.

   ii. Run the following command to reload the systemd configuration:

      ```
      sudo systemctl daemon-reload
      ```

iii. Run the following command to restart the Cloud Assistant client:

```
sudo systemctl restart aliyun.service
```

After the Cloud Assistant client is started, if a proxy server is created for Cloud Assistant, `Detected environment variable ALIYUN_ASSIST_PROXY for proxy setting` exists in the logs of Cloud Assistant. The default log path is */usr/local/share/aliyun-assist/{version}/log/aliyun_assist_main.log*.

5. Run the following commands to register the server as an instance managed by Cloud Assistant by using the proxy server.

   i. Run the following command to configure the proxy server:

   ```
   sudo export ALIYUN_ASSIST_PROXY=<http://your_proxy_address>
   ```

   > **Note** You must replace `<http://your_proxy_address>` with the IP address of your proxy server.

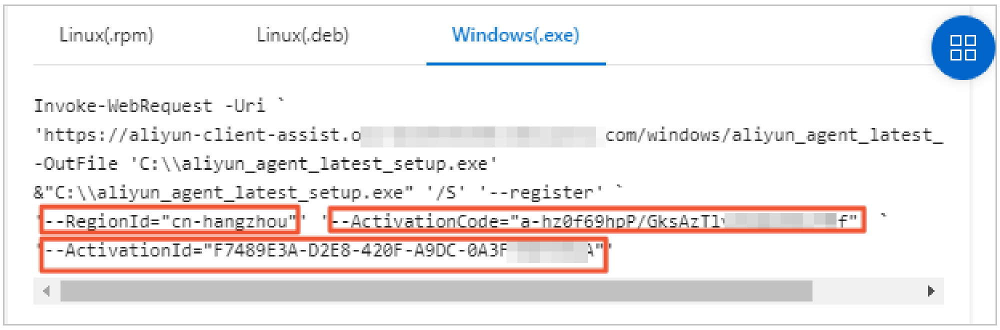
   ii. Run the following commands to register the server as an instance managed by Cloud Assistant:

   ```
   sudo aliyun-service --register --RegionId "cn-hangzhou" \
      --ActivationCode "a-hz0f5KlGmF/TsM5uBuq7Eqor+****" \
      --ActivationId "045CE381-0404-4F42-A44B-CC232B3E****"
   ```

   > **Note** The preceding commands are for reference only. You must copy and paste the script generated in the ECS console. For more information, see the Step 1: Create an activation code for managed instances section.

Install the Cloud Assistant client on a Windows server and register the server as a managed instance

This section describes how to configure a proxy server. In this example, a server that runs Windows Server 2016 Datacenter is used. The installation script of the Cloud Assistant client for a Windows server is shown in the following figure. When you configure a proxy server, the `RegionId`, `ActivationCode`, and `ActivationId` parameter values are required.

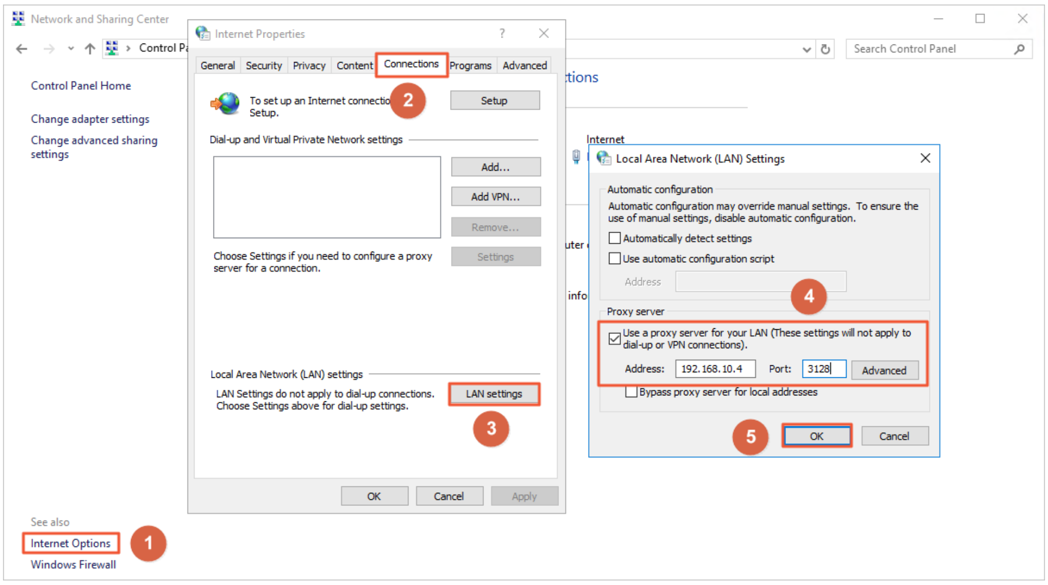


```
Invoke-WebRequest -Uri `
'https://aliyun-client-assist.o[redacted]com/windows/aliyun_agent_latest_
-OutFile 'C:\\aliyun_agent_latest_setup.exe'
&"C:\\aliyun_agent_latest_setup.exe" '/S' '--register' `
'--RegionId="cn-hangzhou"' '--ActivationCode="a-hz0f69hpP/GksAzTl[redacted]f"' `
'--ActivationId="F7489E3A-D2E8-420F-A9DC-0A3F[redacted]A"'
```

1. Log on to the server by using **Remote Desktop Connection**.
2. Configure a proxy server for the browser.
   i. Choose **Start > Control Panel**.
   ii. Click **Network and Internet**.

iii. Click **Network and Sharing Center**.

iv. In the lower-left corner, click **Internet Options**.



Network and Sharing Center
Control Pa
Control Panel Home
Change adapter settings
Change advanced sharing settings
See also
Internet Options
Windows Firewall
1
Internet Properties
General
Security
Privacy
Content
Connections
Programs
Advanced
2
To set up an Internet connection, click Setup.
Setup
Dial-up and Virtual Private Network settings
Add...
Add VPN...
Remove...
Choose Settings if you need to configure a proxy server for a connection.
Settings
Local Area Network (LAN) settings
LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.
LAN settings
3
OK
Cancel
Apply
Search Control Panel
Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Address
4
Proxy server
Advanced
5
OK
Cancel

□ Automatically detect settings

□ Use automatic configuration script

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 192.168.10.4 Port: 3128

□ Bypass proxy server for local addresses

v. Click the **Connections** tab and click **LAN settings**.

vi. In the **Proxy server** section, configure the address and port of the proxy server and click **OK**.

3. Download the installation package of the Cloud Assistant client.

   i. Click Start and choose **Windows PowerShell > Windows PowerShell**.

   ii. Right-click **Windows PowerShell** and select **Run as administrator**.

   iii. In the **Windows PowerShell** dialog box, run the following command to download the installation package of the Cloud Assistant client:

```
Invoke-WebRequest -Uri 'https://aliyun-client-assist.oss-accelerate.aliyuncs.com/windows/aliyun_agent_latest_setup.exe' -OutFile 'C:\\aliyun_agent_latest_setup.exe'
```

4. After you download the installation package, install the Cloud Assistant client.

   i. Open the *C:\* drive.

   ii. Double-click *aliyun_agent_latest_setup.exe* and follow the installation wizard to install the Cloud Assistant client.

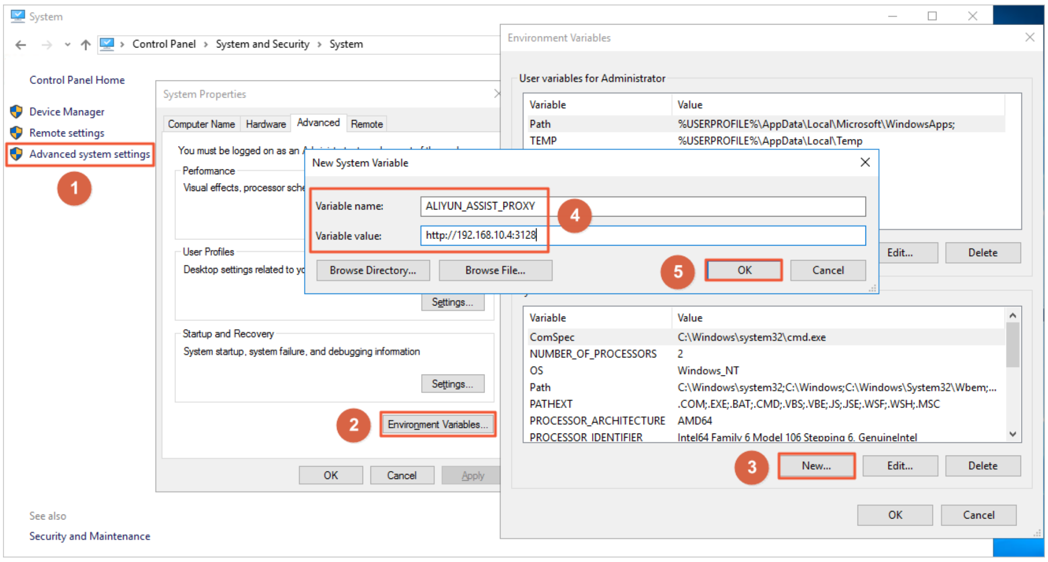
5. Configure a proxy server for Cloud Assistant.

   i. Choose **Start > Control Panel**.

   ii. Click **System and Security**.

   iii. Click **System**.

iv. In the left-side navigation pane, click **Advanced system settings**.



Variable name: ALIYUN_ASSIST_PROXY

Variable value: http://192.168.10.4:3128

User variables for Administrator:

Variable	Value
Path	%USERPROFILE%\AppData\Local\Microsoft\WindowsApps;
TEMP	%USERPROFILE%\AppData\Local\Temp

System variables:

Variable	Value
ComSpec	C:\Windows\system32\cmd.exe
NUMBER_OF_PROCESSORS	2
OS	Windows_NT
Path	C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;...
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE	AMD64
PROCESSOR_IDENTIFIER	Intel64 Family 6 Model 106 Stepping 6, GenuineIntel

v. Click the **Advanced** tab and click **Environment Variables**.

vi. In the **System variables** section, click **New**.

vii. Configure **Variable name** and **Variable value** and click **OK**.

- **Variable name**: Set this parameter to ALIYUN_ASSIST_PROXY.
- **Variable value**: Set this parameter to the IP address of your proxy server.

viii. Run the following commands in **Windows PowerShell** to restart the Cloud Assistant client.

Run the following command to disable the Cloud Assistant client:

```
net stop AliyunService
```

Run the following command to restart the Cloud Assistant client:

```
net start AliyunService
```

6. Use the proxy server to register the Windows server as an instance managed by Cloud Assistant in **Windows PowerShell**.

Run the following command to go to the directory where the Cloud Assistant client is installed:

```
cd C:\ProgramData\aliyun\assist\{version}
```

> **Note** `{version}` specifies the version of the Cloud Assistant client. You must set this value to a specific version number.

Run the following command to register the Windows server as an instance managed by Cloud Assistant:

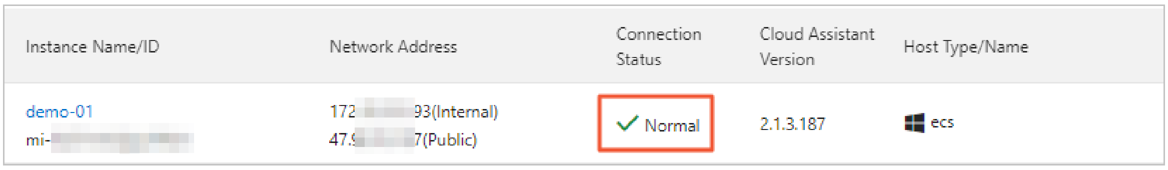
```
 .\aliyun_assist_service.exe  --register  --RegionId="cn-hangzhou" --ActivationCode="a-hz0f6dB8Fg6hhtK0A5n9xqqdH****" --ActivationId="0A2E5ECE-5C71-4FA3-807B-05962C25****"
```

> Note The preceding command is used for reference only. You must change the values of `RegionId` , `ActivationCode` , and `ActivationCode` to those in the script generated in the ECS console. For more information, see the Step 1: Create an activation code for managed instances section.

Step 3: View the managed instance in the ECS console

After the Cloud Assistant client is installed, you must go back to the ECS console to check whether the managed instance is connected.

1.
2.
3. On the Cloud Assistant page, click the **Manage Instances** tab to view the list of managed instances.



Instance Name/ID	Network Address	Connection Status	Cloud Assistant Version	Host Type/Name
demo-01 mi-[redacted]	172[redacted]93(Internal) 47.[redacted]7(Public)	✓ Normal	2.1.3.187	ecs

   If the server is registered as a managed instance, **Normal** is displayed in the **Connection Status** column corresponding to the managed instance, as shown in the preceding figure.

You can then use Cloud Assistant to manage the server without logging on to the server. For information about how to use Cloud Assistant, see Use the immediate execution feature and Upload files to ECS instances.

(Optional) Unregister managed instances and uninstall the Cloud Assistant client

If Cloud Assistant is no longer needed, you can unregister managed instances and disable and uninstall the Cloud Assistant client.

If your server runs a Linux operating system, perform the following steps:

1. Log on to the server by using SSH.
2. Run the following command to unregister the managed instance:

```
sudo aliyun-service --deregister
```

3. Disable and uninstall the Cloud Assistant daemon process.

   Run the following command to disable the Cloud Assistant daemon process:

```
sudo /usr/local/share/assist-daemon/assist_daemon --stop
```

> Note In the preceding command, */usr/local/share/assist-daemon/assist_daemon* specifies the default path of the Cloud Assistant daemon process.

   Run the following command to uninstall the Cloud Assistant daemon process:

```
sudo /usr/local/share/assist-daemon/assist_daemon --delete
```

4. Run the following command to disable the Cloud Assistant client:

   > **Note** Linux has different kernel versions and uses different initialization process services. Linux that uses a later kernel version such as Ubuntu 18.04 generally uses the systemd initialization process service. In this example, the systemd initialization process is used. For more information about how to use other initialization process services, see Uninstall the Cloud Assistant daemon process from a Linux instance.

   ```
   sudo systemctl stop aliyun.service
   ```

5. Run the following command to uninstall the Cloud Assistant client.

   - RPM package:

     ```
     sudo rpm -qa | grep aliyun_assist | xargs sudo rpm -e
     ```

   - DEB package:

     ```
     sudo dpkg -r aliyun_assist_latest.deb
     ```

6. Delete the Cloud Assistant daemon process and the Cloud Assistant client.

   Run the following command to delete the directory where the Cloud Assistant daemon process is stored:

   ```
   sudo rm -rf /usr/local/share/assist-daemon
   ```

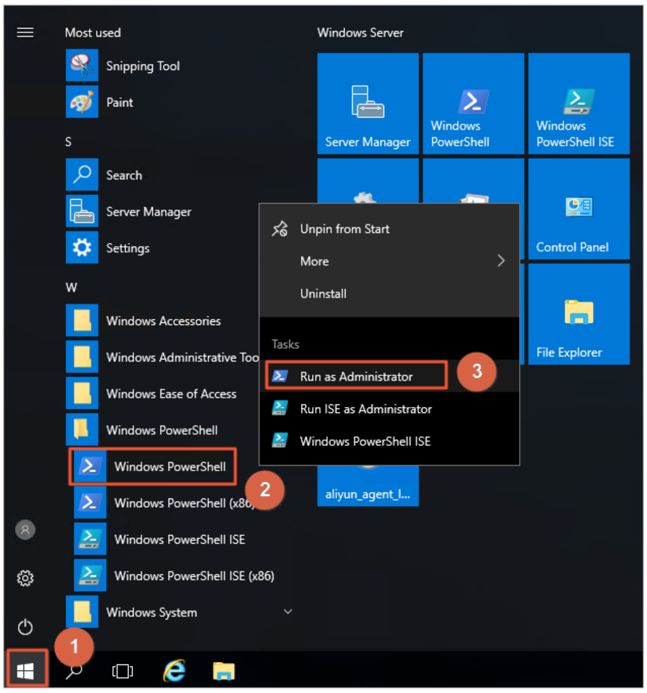
   Run the following command to delete the directory where the Cloud Assistant client is stored:

   ```
   sudo rm -rf /usr/local/share/aliyun-assist
   ```

If your server runs a Windows operating system, perform the following steps:

> **Note** In this example, a server that runs Windows Service 2019 is used. The paths for Windows PowerShell and services in other Windows versions may be different.

1. Log on to the server by using the administrator account.
2. Start Windows PowerShell as an administrator.



i. Click Start.

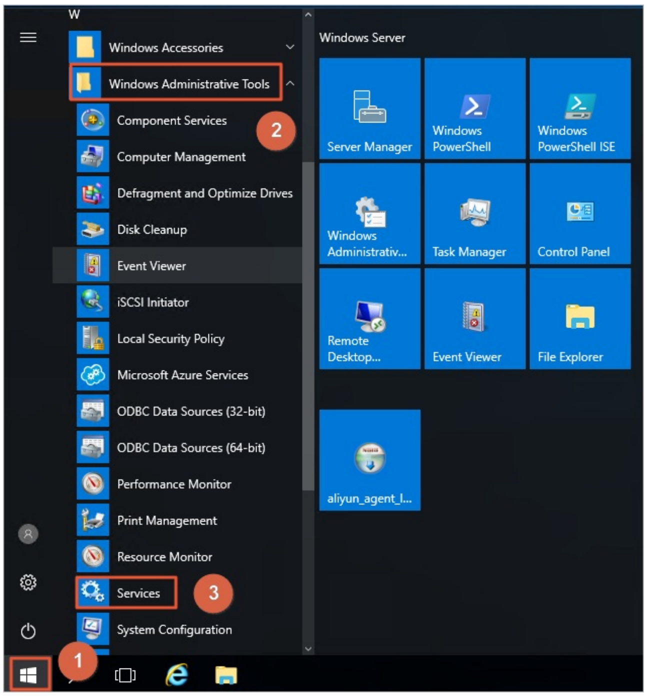
ii. Choose **Windows PowerShell > Windows PowerShell**.

iii. Right-click **Windows PowerShell** and select **Run as administrator**.

3. Run the following command in **Windows PowerShell** to unregister the managed instance:

```
aliyun-service --deregister
```

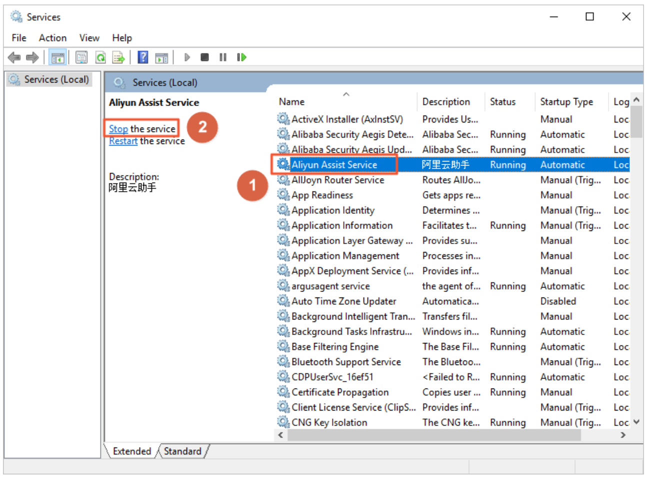
4. Open the service management window.



i. Click Start.

ii. Choose **Administrative Tools > Service**.

5. Find **Aliyun Assist Service** and click **Stop the service**.



Aliyun Assist Service

Stop the service
Restart the service

Description:
阿里云助手

Name	Description	Status	Startup Type	Log
ActiveX Installer (AxInstSV)	Provides Us...		Manual	Loc
Alibaba Security Aegis Dete...	Alibaba Sec...	Running	Automatic	Loc
Alibaba Security Aegis Upd...	Alibaba Sec...	Running	Automatic	Loc
Aliyun Assist Service	阿里云助手	Running	Automatic	Loc
AllJoyn Router Service	Routes AllJo...		Manual (Trig...	Loc
App Readiness	Gets apps re...		Manual	Loc
Application Identity	Determines ...		Manual (Trig...	Loc
Application Information	Facilitates t...	Running	Manual (Trig...	Loc
Application Layer Gateway ...	Provides su...		Manual	Loc
Application Management	Processes in...		Manual	Loc
AppX Deployment Service (...	Provides inf...		Manual	Loc
argusagent service	the agent of...	Running	Automatic	Loc
Auto Time Zone Updater	Automatica...		Disabled	Loc
Background Intelligent Tran...	Transfers fil...		Manual	Loc
Background Tasks Infrastru...	Windows in...	Running	Automatic	Loc
Base Filtering Engine	The Base Fil...	Running	Automatic	Loc
Bluetooth Support Service	The Bluetoo...		Manual (Trig...	Loc
CDPUserSvc_16ef51	<Failed to R...	Running	Automatic	Loc
Certificate Propagation	Copies user ...	Running	Manual	Loc
Client License Service (ClipS...	Provides inf...		Manual (Trig...	Loc
CNG Key Isolation	The CNG ke...	Running	Manual (Trig...	Loc

References

- CreateActivation
- DisableActivation
- DeregisterManagedInstance
- DescribeActivations
- DescribeManagedInstances
- DeleteActivation

4.3. Configure the Cloud Assistant client

4.3.1. Install the Cloud Assistant client

The Cloud Assistant client is used to run Cloud Assistant commands on Elastic Compute Service (ECS) instances. This topic describes how to install the Cloud Assistant client.

Prerequisites

- An administrator account is used to install and use the Cloud Assistant client. The administrator username is root for Linux instances, and system for Windows instances.
- Before you install the Cloud Assistant client, make sure that your instance type and operating system support Cloud Assistant. For more information, see the "Limits" section in Overview.

Context

By default, ECS instances created from public images after December 1, 2017 are pre-installed with the Cloud Assistant client. For ECS instances created before December 1, 2017, you must manually install the Cloud Assistant client.

The following table describes the installation methods of the Cloud Assistant client on different operating systems.

Operating system	Installation method
Windows	- Install the client on Windows instances - Install the client on Windows or Linux instances by using Alibaba Cloud CLI
Linux operating systems such as Alibaba Cloud Linux, CentOS, Red Hat Enterprise Linux (RHEL), and SUSE Linux	- Install the client on Linux instances by using the RPM package - Install the client on Linux instances by using the binary package - Install the client on Linux instances by using source code - Install the client on Windows or Linux instances by using Alibaba Cloud CLI **Note** You cannot use Alibaba Cloud Command Line Interface (CLI) to install the Cloud Assistant client on instances that run RHEL.
Linux operating systems such as Debian and Ubuntu	- Install the client on Linux instances by using the Debian package - Install the client on Linux instances by using the binary package - Install the client on Linux instances by using source code - Install the client on Windows or Linux instances by using Alibaba Cloud CLI
Other Linux operating systems	- Install the client on Linux instances by using the binary package - Install the client on Linux instances by using source code - Install the client on Windows or Linux instances by using Alibaba Cloud CLI

Install the client on Windows instances

1. Connect to an ECS instance as the root user. For more information, see Connection methodsGuidelines on instance connection.
2. Download the Cloud Assistant client installation file.

   You can download the installation file for a specific version of the Cloud Assistant client from one of the following URLs:

   - Public URL for the latest version: latest version of the Cloud Assistant client
   - Public URL for a specific version:

```
https://aliyun-client-assist.oss-accelerate.aliyuncs.com/windows/aliyun_agent_{version}_setup.exe
```

- Internal URL for the latest version:

```
https://aliyun-client-assist-{regionId}.oss-{regionId}-internal.aliyuncs.com/windows/aliyun_agent_latest_setup.exe
```

- Internal URL for a specific version:

```
https://aliyun-client-assist-{regionId}.oss-{regionId}-internal.aliyuncs.com/windows/aliyun_agent_{version}_setup.exe
```

> Note
>
> - *{version}* indicates the version number of the Cloud Assistant client.
> - *{regionId}* indicates the **region ID** of your instance.

For example, you can download the installation file for the 1.0.0.128 version of the Cloud Assistant client from the following internal URL in the China (Hangzhou) region:

```
https://aliyun-client-assist-cn-hangzhou.oss-cn-hangzhou-internal.aliyuncs.com/windows/aliyun_agent_1.0.0.128_setup.exe
```

3. Double-click the installation file and install the client as instructed.
   The default installation path is *C:\ProgramData\aliyun\assist\* for Windows instances.
4. If the instance is in the classic network, perform the following steps:
   i. In the directory where the Cloud Assistant client is installed, create a file named *region-id* and do not add extensions such as *.txt* or *.conf* to the file.
   ii. In the *region-id* file, enter the region ID of the instance. Example: *cn-hangzhou*.

> Note In Windows, you must clear the Hide extensions for known file types option to check whether the *region-id* file has an extension.

Install the client on Linux instances by using the RPM package

This method is applicable to operating systems such as Alibaba Cloud Linux, CentOS, RHEL, and SUSE Linux.

1.
2. Download the RPM package for a specific version of the Cloud Assistant client from one of the following URLs:
   - Public URL for the latest version:
     - Download URL for Linux x86:

```
wget "https://aliyun-client-assist.oss-accelerate.aliyuncs.com/linux/aliyun_assist_latest.rpm"
```

    - Download URL for Linux ARM:

      ```
      wget "https://aliyun-client-assist.oss-accelerate.aliyuncs.com/arm/aliyun-assist-latest-1.aarch64.rpm"
      ```

  - Public URL for a specific version:
    - Download URL for Linux x86:

      ```
      wget "https://aliyun-client-assist.oss-accelerate.aliyuncs.com/linux/aliyun_assist_{version}.rpm"
      ```

    - Download URL for Linux ARM:

      ```
      wget "https://aliyun-client-assist.oss-accelerate.aliyuncs.com/arm/aliyun-assist-{version}-1.aarch64.rpm"
      ```

  - Internal URL for the latest version:
    - Download URL for Linux x86:

      ```
      wget "https://aliyun-client-assist-{regionId}.oss-{regionId}-internal.aliyuncs.com/linux/aliyun_assist_latest.rpm"
      ```

    - Download URL for Linux ARM:

      ```
      wget "https://aliyun-client-assist-{regionId}.oss-{regionId}-internal.aliyuncs.com/arm/aliyun-assist-latest-1.aarch64.rpm"
      ```

  - Internal URL for a specific version:
    - Download URL for Linux x86:

      ```
      wget "https://aliyun-client-assist-{regionId}.oss-{regionId}-internal.aliyuncs.com/linux/aliyun_assist_{version}.rpm"
      ```

    - Download URL for Linux ARM:

      ```
      wget "https://aliyun-client-assist-{regionId}.oss-{regionId}-internal.aliyuncs.com/arm/aliyun-assist-{version}-1.aarch64.rpm"
      ```

> **Note**
>
> - *{version}* indicates the version number of the Cloud Assistant client.
> - *{regionId}* indicates the **region ID** of your instance.

For example, you can download the RPM package for the 1.0.2.458 x86 version of the Cloud Assistant client from the following internal URL in the China (Hangzhou) region:

```
wget "https://aliyun-client-assist-cn-hangzhou.oss-cn-hangzhou-internal.aliyuncs.com/linux/aliyun_assist_1.0.2.458.rpm"
```

3. Install the Cloud Assistant client.

   If you select the default installation directories, the Cloud Assistant client is installed in one of the following directories on Linux instances:

- CoreOS: */opt/local/share/aliyun-assist/*.
- Other operating systems: */usr/local/share/aliyun-assist/*. Other operating systems include Alibaba Cloud Linux, Ubuntu, Debian, Red Hat, SUSE Linux Enterprise Server, and openSUSE.

In this example, the latest version of the Cloud Assistant client is installed.

- Download URL for Linux x86:

```
rpm -ivh --force aliyun_assist_latest.rpm
```

- Download URL for Linux ARM:

```
rpm -ivh --force aliyun-assist-latest-1.aarch64.rpm
```

4. Perform the following operations based on the operating system and network type of the ECS instance:
   - If the instance runs a Red Hat operating system, perform the following steps:
     a. Stop the qemu-ga service.

     ```
     systemctl stop qemu-guest-agent
     systemctl disable qemu-guest-agent
     ```

     b. Restart Cloud Assistant.

     ```
     systemctl restart aliyun.service
     ```

   - If the instance is in the classic network, perform the following steps:
     a. In the directory where the Cloud Assistant client is installed, create a file named *region-id* and do not add extensions such as *.txt* or *.conf* to the file.
     b. In the *region-id* file, enter the region ID of the instance. Example: *cn-hangzhou*.

Install the client on Linux instances by using the Debian package

This method is applicable to operating systems such as Debian and Ubuntu.

1.
2. Download the Debian package for a specific version of the Cloud Assistant client from one of the following URLs:
   - Public URL for the latest version:
     - Download URL for Linux x86:

     ```
     wget "https://aliyun-client-assist.oss-accelerate.aliyuncs.com/linux/aliyun_assist_latest.deb"
     ```

     - Download URL for Linux ARM:

     ```
     wget "https://aliyun-client-assist.oss-accelerate.aliyuncs.com/arm/aliyun-assist_latest-1_arm64.deb"
     ```

   - Public URL for a specific version:
     - Download URL for Linux x86:

```
wget "https://aliyun-client-assist.oss-accelerate.aliyuncs.com/linux/aliyun_assist_{version}.deb"
```

    - Download URL for Linux ARM:

        ```
        wget "https://aliyun-client-assist.oss-accelerate.aliyuncs.com/arm/aliyun-assist_{version}-1_arm64.deb"
        ```

- Internal URL for the latest version:
    - Download URL for Linux x86:

        ```
        wget "https://aliyun-client-assist-{regionId}.oss-{regionId}-internal.aliyuncs.com/linux/aliyun_assist_latest.deb"
        ```

    - Download URL for Linux ARM:

        ```
        wget "https://aliyun-client-assist-{regionId}.oss-{regionId}-internal.aliyuncs.com/arm/aliyun-assist_latest-1_arm64.deb"
        ```

- Internal URL for a specific version:
    - Download URL for Linux x86:

        ```
        wget "https://aliyun-client-assist-{regionId}.oss-{regionId}-internal.aliyuncs.com/linux/aliyun_assist_{version}.deb"
        ```

    - Download URL for Linux ARM:

        ```
        wget "https://aliyun-client-assist-{regionId}.oss-{regionId}-internal.aliyuncs.com/arm/aliyun-assist_{version}-1_arm64.deb"
        ```

> Note
>
> - *{version}* indicates the version number of the Cloud Assistant client.
> - *{regionId}* indicates the **region ID** of your instance.

For example, you can download the Debian package for the 1.0.2.458 x86 version of the Cloud Assistant client from the following internal URL in the China (Hangzhou) region:

```
wget "https://aliyun-client-assist-cn-hangzhou.oss-cn-hangzhou-internal.aliyuncs.com/linux/aliyun_assist_1.0.2.458.deb"
```

3. If an earlier version of the Cloud Assistant client is installed on the instance, uninstall the earlier version.

    ```
    dpkg -r aliyun-assist
    ```

4. Install the Cloud Assistant client.

    If you select the default installation directories, the Cloud Assistant client is installed in one of the following directories on Linux instances:

    - CoreOS: */opt/local/share/aliyun-assist/*.
    - Other operating systems: */usr/local/share/aliyun-assist/*. Other operating systems include Alibaba Cloud Linux, Ubuntu, Debian, Red Hat, SUSE Linux Enterprise Server, and openSUSE.

In this example, the latest version of the Cloud Assistant client is installed.

- Download URL for Linux x86:

  ```
  dpkg -i aliyun_assist_latest.deb
  ```

- Download URL for Linux ARM:

  ```
  dpkg -i aliyun-assist_latest-1_arm64.deb
  ```

5. If the instance is in the classic network, perform the following steps:

   i. In the directory where the Cloud Assistant client is installed, create a file named *region-id* and do not add extensions such as *.txt* or *.conf* to the file.

   ii. In the *region-id* file, enter the region ID of the instance. Example: *cn-hangzhou*.

Install the client on Linux instances by using the binary package

This method is applicable to mainstream Linux operating systems.

1. Connect to an ECS instance as the root user. For more information, see Connection methodsGuidelines on instance connection.
2. Download the binary package for a specific version of the Cloud Assistant client from one of the following URLs:
   - Public URL for the latest version:
     - Download URL for Linux x86:

       ```
       wget "https://aliyun-client-assist.oss-accelerate.aliyuncs.com/linux/aliyun_assist_
       latest_update.zip"
       ```

     - Download URL for Linux ARM:

       ```
       wget "https://aliyun-client-assist.oss-accelerate.aliyuncs.com/arm/aliyun_assist_la
       test_update_arm.zip"
       ```

   - Public URL for a specific version:
     - Download URL for Linux x86:

       ```
       wget "https://aliyun-client-assist.oss-accelerate.aliyuncs.com/linux/aliyun_assist_
       {version}_update.zip"
       ```

     - Download URL for Linux ARM:

       ```
       wget "https://aliyun-client-assist.oss-accelerate.aliyuncs.com/arm/aliyun_assist_{v
       ersion}_update_arm.zip"
       ```

   - Internal URL for the latest version:
     - Download URL for Linux x86:

       ```
       wget "https://aliyun-client-assist-{regionId}.oss-{regionId}-internal.aliyuncs.com/
       linux/aliyun_assist_latest_update.zip"
       ```

    - Download URL for Linux ARM:

      ```
      wget "https://aliyun-client-assist-{regionId}.oss-{regionId}-internal.aliyuncs.com/
      arm/aliyun_assist_latest_update_arm.zip"
      ```

  - Internal URL for a specific version:
    - Download URL for Linux x86:

      ```
      wget "https://aliyun-client-assist-{regionId}.oss-{regionId}-internal.aliyuncs.com/
      linux/aliyun_assist_{version}_update.zip"
      ```

    - Download URL for Linux ARM:

      ```
      wget "https://aliyun-client-assist-{regionId}.oss-{regionId}-internal.aliyuncs.com/
      arm/aliyun_assist_{version}_update_arm.zip"
      ```

  > **Note**
  >
  > - *{version}* indicates the version number of the Cloud Assistant client.
  > - *{regionId}* indicates the **region ID** of your instance.

  For example, you can download the binary package for the 2.2.3.282 x86 version of the Cloud Assistant client from the following internal URL in the China (Hangzhou) region:

  ```
  wget "https://aliyun-client-assist-cn-hangzhou.oss-cn-hangzhou-internal.aliyuncs.com/li
  nux/aliyun_assist_2.2.3.282_update.zip"
  ```

3. Install the Cloud Assistant client.

   If you select the default installation directories, the Cloud Assistant client is installed in one of the following directories on Linux instances:

   - CoreOS: */opt/local/share/aliyun-assist/*.
   - Other operating systems: */usr/local/share/aliyun-assist/*. Other operating systems include Alibaba Cloud Linux, Ubuntu, Debian, Red Hat, SUSE Linux Enterprise Server, and openSUSE.

   Decompress the binary package to the corresponding installation directory and install the client. In this example, the 2.2.3.282 x86 version of the Cloud Assistant client is installed.

   ```
   unzip  -o aliyun_assist_2.2.3.282_update.zip -d /usr/local/share/aliyun-assist/
   chmod a+x /usr/local/share/aliyun-assist/2.2.3.282/update_install
   bash /usr/local/share/aliyun-assist/2.2.3.282/update_install
   ```

4. Perform the following operations based on the operating system and network type of the ECS instance:

   - If the instance runs a Red Hat operating system, perform the following steps:

     a. Stop the qemu-ga service.

     ```
     systemctl stop qemu-guest-agent
     systemctl disable qemu-guest-agent
     ```

   b. Restart Cloud Assistant.

   ```
   systemctl restart aliyun.service
   ```

- If the instance is in the classic network, perform the following steps:

   a. In the directory where the Cloud Assistant client is installed, create a file named *region-id* and do not add extensions such as *.txt* or *.conf* to the file.

   b. In the *region-id* file, enter the region ID of the instance. Example: *cn-hangzhou*.

Install the client on Linux instances by using source code

1.
2. Install necessary software such as Git and Go.

   In this example, YUM is used to install Git and Go. If you use other versions of Linux, use the corresponding package manager.

   - Install Git.

     ```
     yum install git -y
     ```

   - Install Go.

     ```
     yum install go -y
     ```

3. Download the source code of the Cloud Assistant client.

   ```
   git clone https://github.com/aliyun/aliyun_assist_client
   ```

4. Access the source code directory.

   ```
   cd ./aliyun_assist_client
   ```

5. Compile the source code.

   ```
   go build
   ```

   If no error message is returned, the client is installed.

6. If the instance is in the classic network, perform the following steps:

   i. In the directory where the Cloud Assistant client is installed, create a file named *region-id* and do not add extensions such as *.txt* or *.conf* to the file.

   ii. In the *region-id* file, enter the region ID of the instance. Example: *cn-hangzhou*.

7. Run the Cloud Assistant client.

   ```
   aliyun-service -d
   ```

Install the client on Windows or Linux instances by using Alibaba Cloud CLI

To use this method, you do not need to connect to the instance but you must install Alibaba Cloud Command Line Interface (CLI) first. For more information about how to install Alibaba Cloud CLI in different operating systems, see the following topics:

- Windows
- Linux

- macOS

> Note You cannot use Alibaba Cloud CLI to install the Cloud Assistant client on instances that run RHEL.

1. Call the DescribeCloudAssistantStatus operation to check whether the Cloud Assistant client is installed on your ECS instance.

   ```
   aliyun ecs DescribeCloudAssistantStatus --RegionId TheRegionId --InstanceId.1 i-bp1g6zv0ce8og******p --output cols=CloudAssistantStatus rows=InstanceCloudAssistantStatusSet.InstanceCloudAssistantStatus[]
   ```

   If the value of `CloudAssistantStatus` is true in the response, the Cloud Assistant client is installed on the instance. Otherwise, proceed to the next step.

2. Call the InstallCloudAssistant operation to install the Cloud Assistant client.

   ```
   aliyun ecs InstallCloudAssistant --RegionId TheRegionId --InstanceId.1 i-bp1g6zv0ce8og******p
   ```

3. Call the RebootInstance operation to restart the ECS instance.

   ```
   aliyun ecs RebootInstance --InstanceId i-bp1g6zv0ce8og******p
   ```

4. If the instance is in the classic network, add a region declaration within the instance.

   i. Connect to the ECS instance as the administrator. For more information, see Connection methodsGuidelines on instance connection.

   ii. Check the version of Cloud Assistant.

   - For Linux instances, run the following command:

     ```
     aliyun-service -v
     ```

   - For Windows instances, see Upgrades or disable upgrades for the Cloud Assistant client.

   If the version of the Cloud Assistant client is later than 1.0.1.400, the Cloud Assistant client is installed. Otherwise, proceed to the next step.

   iii. In the directory where the Cloud Assistant client is installed, create a file named *region-id* and do not add extensions such as *.txt* or *.conf* to the file.

   iv. In the *region-id* file, enter the region ID of the instance. Example: *cn-hangzhou*.

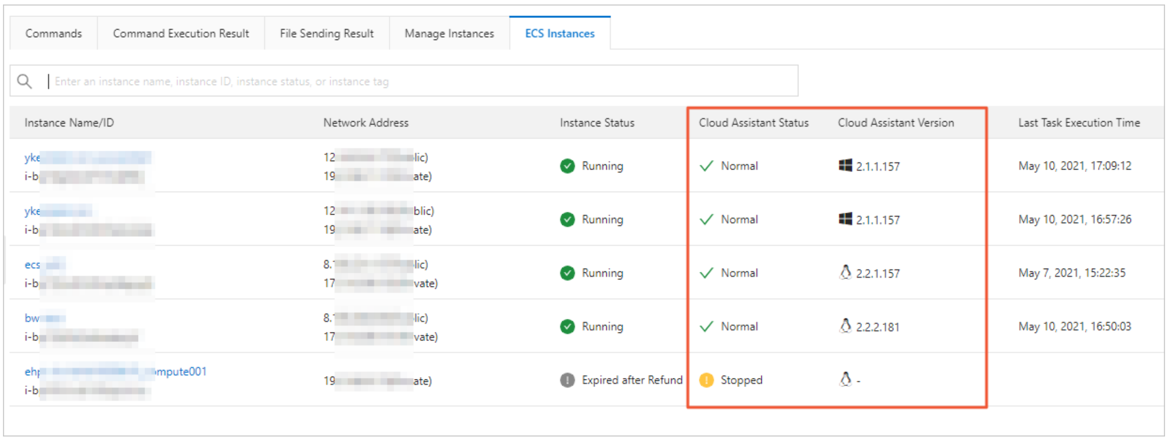
   > Note In Windows, you must clear the Hide extensions for known file types option to check whether the *region-id* file has an extension.

View information of the Cloud Assistant client on an ECS instance

After you install the Cloud Assistant client on an instance, you can perform the following steps to query the version number and state of the client on the instance.

1.
2.
3.
4. Click the **ECS Instances** tab to view the information about the Cloud Assistant client on the ECS

instances within the current region.



Instance Name/ID	Network Address	Instance Status	Cloud Assistant Status	Cloud Assistant Version	Last Task Execution Time
yke[redacted] i-b[redacted]	12[redacted]lic) 19[redacted]ate)	Running	✓ Normal	2.1.1.157	May 10, 2021, 17:09:12
yke[redacted] i-b[redacted]	12[redacted]blic) 19[redacted]ate)	Running	✓ Normal	2.1.1.157	May 10, 2021, 16:57:26
ecs[redacted] i-b[redacted]	8.[redacted]lic) 17[redacted]vate)	Running	✓ Normal	2.2.1.157	May 7, 2021, 15:22:35
bw[redacted] i-b[redacted]	8.[redacted]lic) 17[redacted]vate)	Running	✓ Normal	2.2.2.181	May 10, 2021, 16:50:03
ehp[redacted]mpute001 i-b[redacted]	19[redacted]ate)	Expired after Refund	Stopped	-	

Related information

Reference

- InvokeCommand
- DescribeCloudAssistantStatus
- InstallCloudAssistant
- RebootInstance
- Regions and zones
- Alibaba Cloud GitHub repository

4.3.2. Upgrades or disable upgrades for the Cloud Assistant client

The Cloud Assistant client is an agent that runs Cloud Assistant commands on Elastic Compute Service (ECS) instances. This topic describes how to upgrade and disable upgrades for the Cloud Assistant client.

Prerequisites

The Cloud Assistant client is installed. For more information, see Install the Cloud Assistant client.

Automatic upgrade

The Cloud Assistant client automatically runs the *aliyun_assist_update* upgrade process every hour, which is located in the following path:

- Windows instances: *C:\ProgramData\aliyun\assist\${version}/aliyun_assist_update*
- Linux instances: */usr/local/share/aliyun-assist/${version}/aliyun_assist_update*

Manual upgrade

If the automatic upgrade fails, you can create an upgrade command and run the command on a regular basis. For more information, see Create a command.

If you are using an RPM installation package, you can run the following Cloud Assistant command to upgrade the Cloud Assistant client. For information about the upgrade commands for other installation packages, see Install the Cloud Assistant client.

```
wget "https://aliyun-client-assist.oss-accelerate.aliyuncs.com/linux/aliyun_assist_latest.r
pm" && rpm -ivh --force aliyun_assist_latest.rpm
```

Manually disable upgrades

You can disable upgrades for the Cloud Assistant client by disabling the *aliyun_assist_update* automatic upgrade process.

- Run the following command in PowerShell if the instance on which the Cloud Assistant client is installed runs a Windows Server operating system:

  ```
  Rename-Item -Path 'C:\ProgramData\aliyun\assist\${version}\aliyun_assist_update.exe' -New
  Name 'C:\ProgramData\aliyun\assist\${version}\aliyun_assist_update.exe.bk'
  ```

- Run the following command if the instance on which the Cloud Assistant client is installed runs a Linux operating system:

  ```
  chmod a-x aliyun_assist_update
  ```

Related information

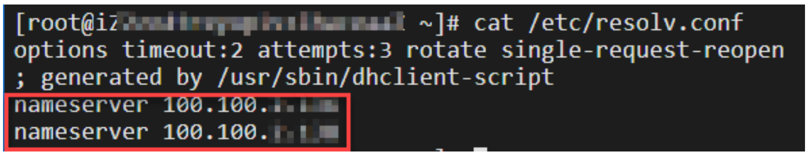
- CreateCommand

4.3.3. Configure DNS resolution for Cloud Assistant

This topic describes how to configure Domain Name System (DNS) resolution for Cloud Assistant. During the configuration procedure, you must obtain the IP addresses that correspond to the Cloud Assistant endpoints and then modify the hosts file.

Context

When you use features such as Cloud Assistant on an Elastic Compute Service (ECS) instance, the instance must have access to the endpoints required to perform the actions that you specify, such as running a Cloud Assistant command. The default DNS Nameserver is installed on each ECS instance to resolve domain names. You can run the **cat /etc/resolv.conf** command to view the DNS Nameserver settings. Example command output:



```
[root@iz[redacted] ~]# cat /etc/resolv.conf
options timeout:2 attempts:3 rotate single-request-reopen
; generated by /usr/sbin/dhclient-script
nameserver 100.100.[redacted]
nameserver 100.100.[redacted]
```

If you modify the configuration file to override the default DNS Nameserver settings, domain names may fail to resolve or resolve slowly when you use features such as Cloud Assistant. This may cause the features to be unavailable. For example, Cloud Assistant commands cannot be run. In this case, you can perform the following procedure to configure DNS resolution for Cloud Assistant.

Procedure

1. Connect to an ECS instance. For more information, see Overview.
2. Obtain the IP addresses that correspond to the Cloud Assistant endpoints.

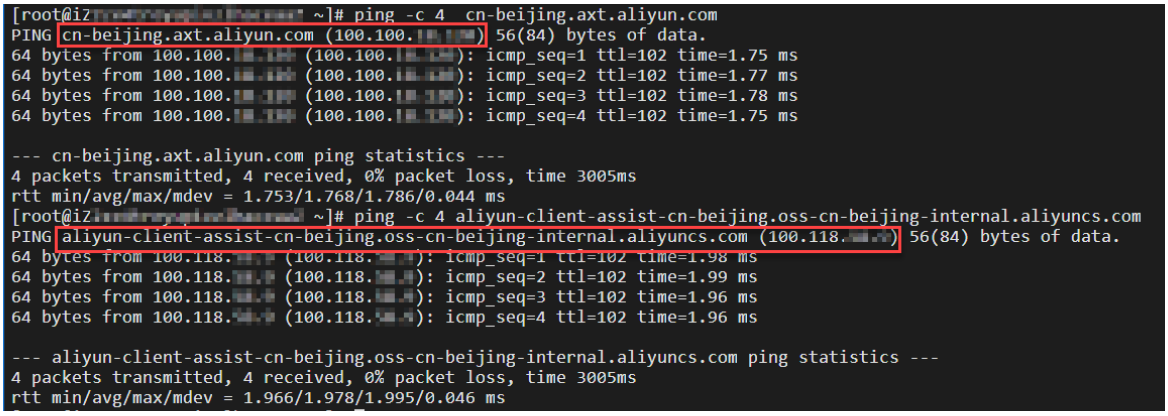
   The following Cloud Assistant endpoints are available:

   - Endpoint used to run Cloud Assistant commands, in the format of `<region-id>.axt.aliyun.com`
   - Endpoint used to obtain the Cloud Assistant plug-in and update packages, in the format of `aliyun-client-assist-<region-id>.oss-<region-id>-internal.aliyuncs.com`

   > Note Replace *<region-id>* with a region ID.

   In this example, the China (Beijing) region is used. Run the following commands to obtain the IP addresses that correspond to the Cloud Assistant endpoints:

   ```
   ping -c 4 cn-beijing.axt.aliyun.com
   ping -c 4 aliyun-client-assist-cn-beijing.oss-cn-beijing-internal.aliyuncs.com
   ```

   ```
   [root@iZ[redacted] ~]# ping -c 4  cn-beijing.axt.aliyun.com
   PING cn-beijing.axt.aliyun.com (100.100.[redacted]) 56(84) bytes of data.
   64 bytes from 100.100.[redacted] (100.100.[redacted]): icmp_seq=1 ttl=102 time=1.75 ms
   64 bytes from 100.100.[redacted] (100.100.[redacted]): icmp_seq=2 ttl=102 time=1.77 ms
   64 bytes from 100.100.[redacted] (100.100.[redacted]): icmp_seq=3 ttl=102 time=1.78 ms
   64 bytes from 100.100.[redacted] (100.100.[redacted]): icmp_seq=4 ttl=102 time=1.75 ms

   --- cn-beijing.axt.aliyun.com ping statistics ---
   4 packets transmitted, 4 received, 0% packet loss, time 3005ms
   rtt min/avg/max/mdev = 1.753/1.768/1.786/0.044 ms
   [root@iZ[redacted] ~]# ping -c 4 aliyun-client-assist-cn-beijing.oss-cn-beijing-internal.aliyuncs.com
   PING aliyun-client-assist-cn-beijing.oss-cn-beijing-internal.aliyuncs.com (100.118.[redacted]) 56(84) bytes of data.
   64 bytes from 100.118.[redacted] (100.118.[redacted]): icmp_seq=1 ttl=102 time=1.98 ms
   64 bytes from 100.118.[redacted] (100.118.[redacted]): icmp_seq=2 ttl=102 time=1.99 ms
   64 bytes from 100.118.[redacted] (100.118.[redacted]): icmp_seq=3 ttl=102 time=1.96 ms
   64 bytes from 100.118.[redacted] (100.118.[redacted]): icmp_seq=4 ttl=102 time=1.96 ms

   --- aliyun-client-assist-cn-beijing.oss-cn-beijing-internal.aliyuncs.com ping statistics ---
   4 packets transmitted, 4 received, 0% packet loss, time 3005ms
   rtt min/avg/max/mdev = 1.966/1.978/1.995/0.046 ms
   ```

3. Modify the hosts file.

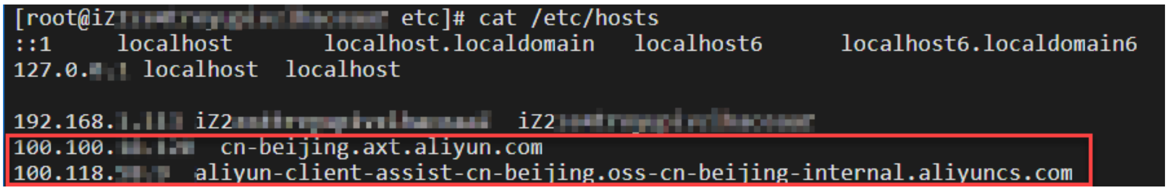
   ```
   echo "100.100.XX.XX cn-beijing.axt.aliyun.com" >> /etc/hosts && \
   echo "100.118.XX.XX aliyun-client-assist-cn-beijing.oss-cn-beijing-internal.aliyuncs.co
   m" >> /etc/hosts
   ```

   > Note Replace `100.100.XX.XX` and `100.118.XX.XX` with the IP addresses that you obtained in the previous step.

4. Check whether the hosts file is modified.

   ```
   cat /etc/hosts
   ```

   If the hosts file is modified, the command output includes the Cloud Assistant endpoints and their corresponding IP addresses. Example command output:

   ```
   [root@iZ[redacted] etc]# cat /etc/hosts
   ::1     localhost       localhost.localdomain   localhost6      localhost6.localdomain6
   127.0.[redacted] localhost  localhost

   192.168.[redacted] iZ2[redacted]  iZ2[redacted]
   100.100.[redacted]  cn-beijing.axt.aliyun.com
   100.118.[redacted]  aliyun-client-assist-cn-beijing.oss-cn-beijing-internal.aliyuncs.com
   ```

   After the hosts file is modified, the ECS instance can automatically obtain IP addresses from the hosts file to resolve the Cloud Assistant endpoints.

4.3.4. Configure network permissions for the Cloud Assistant client

This topic describes how to configure security group rules for Elastic Compute Service (ECS) instances that have the Cloud Assistant client installed and manage network permissions of the Cloud Assistant client with ease.

Context

To ensure that you can use Cloud Assistant on an ECS instance, the instance must have access to the endpoints or IP addresses required to perform specified operations such as running a Cloud Assistant command. You must configure security group rules to allow outbound access to the endpoints or IP addresses described in the following table.

Endpoint/IP address	Description
https://*{region-id}*.axt.aliyun.com:443/	This endpoint is used to access the Cloud Assistant server.
http://100.100.100.200:80/	This IP address is used to access MetaServer.
https://aliyun-client-assist-*{region-id}*.oss-*{region-id}*-internal.aliyuncs.com:443/	This endpoint is used to access the server where the Cloud Assistant client installation package resides to install or update your Cloud Assistant client.

Note *{region-id}* specifies the region ID of the instance. For example, if the instance resides in the China (Hangzhou) region, set this parameter to `cn-hangzhou` .

You can use one of the following methods to configure security group rules for an instance on which the Cloud Assistant client is installed:

- General configurations: In most cases, you can use this method to configure security group rules to allow access from the CIDR blocks and ports of the Cloud Assistant server and the server where the Cloud Assistant client installation package resides.
- Fine-grained configurations: If you want to manage network permissions in a fine-grained manner, you can use this method to allow access from the specified ports and IP addresses based on the region of the instance on which the Cloud Assistance client is installed.

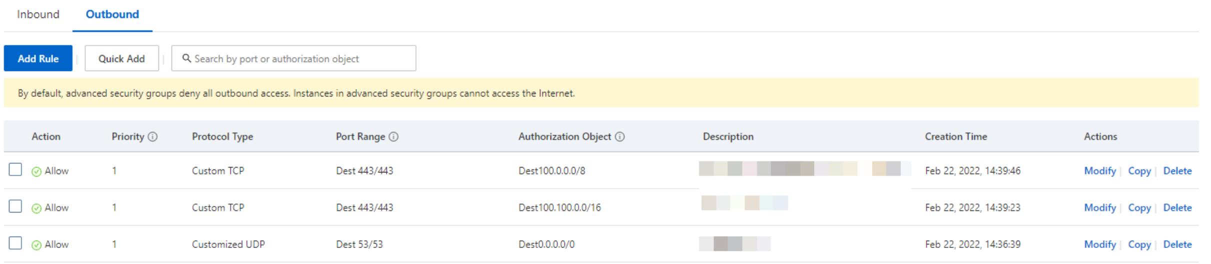
General configurations

To simplify the configurations and the management of network permissions, you can configure security group rules to allow access form the CIDR blocks and ports of the Cloud Assistant server and the server where the Cloud Assistant client installation package resides.

Note The CIDR block of the Cloud Assistant server is 100.100.0.0/16. The CIDR block of the server where the Cloud Assistant client installation package resides is 100.0.0.0/8.

By default, basic security groups allow all outbound access. ECS instances in a basic security group allow outbound traffic. By default, advanced security groups deny all outbound access. ECS instances in an advanced security group deny outbound traffic. For advanced security groups, you must configure security group rules to allow outbound access to the endpoints, CIDR blocks, or ports described in the following table. For more information, see Add a security group rule.

Endpoint/CIDR block/Port	Description
DNS/UDP port 53	This port is used to resolve domain names.
https://<100.100.0.0/16>:443/	This CIDR block is used to access the Cloud Assistant server.
https://<100.0.0.0/8>:443/	This CIDR block is used to access the server where the Cloud Assistant client installation package resides to install or update your Cloud Assistant client.



By default, advanced security groups deny all outbound access. Instances in advanced security groups cannot access the Internet.

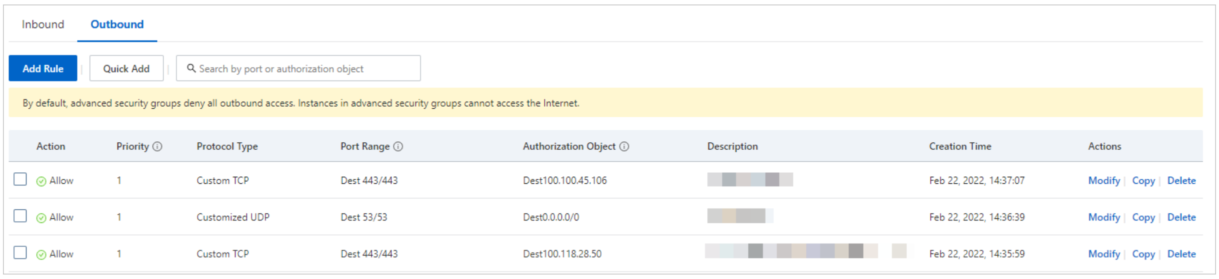
	Action	Priority	Protocol Type	Port Range	Authorization Object	Description	Creation Time	Actions
□	Allow	1	Custom TCP	Dest 443/443	Dest100.0.0.0/8	[redacted]	Feb 22, 2022, 14:39:46	Modify | Copy | Delete
□	Allow	1	Custom TCP	Dest 443/443	Dest100.100.0.0/16	[redacted]	Feb 22, 2022, 14:39:23	Modify | Copy | Delete
□	Allow	1	Customized UDP	Dest 53/53	Dest0.0.0.0/0	[redacted]	Feb 22, 2022, 14:36:39	Modify | Copy | Delete

Fine-grained configurations

If you want to manage network permissions in a fine-grained manner, you can allow access from the IP addresses of the Cloud Assistant server and the server where the Cloud Assistant client installation package resides in the specified region.

For example, if your instance resides in the China (Hangzhou) region, you must configure rules for advanced security groups to allow outbound access to the endpoints, IP addresses, or ports described in the following table. For more information, see Add a security group rule.

Endpoint /IP Address/Port	Description
DNS/UDP port 53	This port is used to resolve domain names.
https://100.100.45.106:443/	This IP address is used to access the Cloud Assistant server in the China (Hangzhou) region.
https://100.118.28.50:443/	This IP address is used to access the server where the Cloud Assistant client installation package resides in the China (Hangzhou) region to install or update your Cloud Assistant client.



By default, advanced security groups deny all outbound access. Instances in advanced security groups cannot access the Internet.

	Action	Priority ⓘ	Protocol Type	Port Range ⓘ	Authorization Object ⓘ	Description	Creation Time	Actions
□	✓ Allow	1	Custom TCP	Dest 443/443	Dest100.100.45.106	[redacted]	Feb 22, 2022, 14:37:07	Modify | Copy | Delete
□	✓ Allow	1	Customized UDP	Dest 53/53	Dest0.0.0.0/0	[redacted]	Feb 22, 2022, 14:36:39	Modify | Copy | Delete
□	✓ Allow	1	Custom TCP	Dest 443/443	Dest100.118.28.50	[redacted]	Feb 22, 2022, 14:35:59	Modify | Copy | Delete

The following table lists the endpoints and IP addresses that the Cloud Assistant must be able to access in each region.

The first row in the Endpoint column of each region indicates the endpoint and IP address of the Cloud Assistant server, and the second row indicates the endpoint and IP address of the server where the Cloud Assistant client installation package resides.

Region	Region ID	Endpoint	IP Address
China (Qingdao)	cn-qingdao	cn-qingdao.axt.aliyun.com	100.100.15.4
		aliyun-client-assist-cn-qingdao.oss-cn-qingdao-internal.aliyuncs.com	100.115.173.9
China (Beijing)	cn-beijing	cn-beijing.axt.aliyun.com	100.100.18.120
		aliyun-client-assist-cn-beijing.oss-cn-beijing-internal.aliyuncs.com	100.118.58.9
China (Zhangjiakou)	cn-zhangjiakou	cn-zhangjiakou.axt.aliyun.com	100.100.99.23
		aliyun-client-assist-cn-zhangjiakou.oss-cn-zhangjiakou-internal.aliyuncs.com	100.118.90.245
China (Hohhot)	cn-huhehaote	cn-huhehaote.axt.aliyun.com	100.100.126.8
		aliyun-client-assist-cn-huhehaote.oss-cn-huhehaote-internal.aliyuncs.com	100.118.195.21
China (Ulanqab)	cn-wulanchabu	cn-wulanchabu.axt.aliyun.com	100.100.0.3
		aliyun-client-assist-cn-wulanchabu.oss-cn-wulanchabu-internal.aliyuncs.com	100.118.214.0
China (Hangzhou)	cn-hangzhou	cn-hangzhou.axt.aliyun.com	100.100.45.106
		aliyun-client-assist-cn-hangzhou.oss-cn-hangzhou-internal.aliyuncs.com	100.118.28.50
China (Shanghai)	cn-shanghai	cn-shanghai.axt.aliyun.com	100.100.36.108
		aliyun-client-assist-cn-shanghai.oss-cn-shanghai-internal.aliyuncs.com	100.118.102.35

Region	Region ID	Endpoint	IP Address
China (Nanjing - Local Region)	cn-nanjing	cn-nanjing.axt.aliyun.com	100.100.0.1
		aliyun-client-assist-cn-nanjing.oss-cn-nanjing-internal.aliyuncs.com	100.114.142.7
China (Shenzhen)	cn-shenzhen	cn-shenzhen.axt.aliyun.com	100.100.0.70
		aliyun-client-assist-cn-shenzhen.oss-cn-shenzhen-internal.aliyuncs.com	100.118.78.4
China (Heyuan)	cn-heyuan	cn-heyuan.axt.aliyun.com	100.100.0.5
		aliyun-client-assist-cn-heyuan.oss-cn-heyuan-internal.aliyuncs.com	100.98.83.0
China (Guangzhou)	cn-guangzhou	cn-guangzhou.axt.aliyun.com	100.100.0.4
		aliyun-client-assist-cn-guangzhou.oss-cn-guangzhou-internal.aliyuncs.com	100.115.33.49
China (Chengdu)	cn-chengdu	cn-chengdu.axt.aliyun.com	100.100.0.42
		aliyun-client-assist-cn-chengdu.oss-cn-chengdu-internal.aliyuncs.com	100.115.155.18
China (Hong Kong)	cn-hongkong	cn-hongkong.axt.aliyun.com	100.100.35.30
		aliyun-client-assist-cn-hongkong.oss-cn-hongkong-internal.aliyuncs.com	100.115.61.10
Singapore (Singapore)	ap-southeast-1	ap-southeast-1.axt.aliyun.com	100.100.30.60
		aliyun-client-assist-ap-southeast-1.oss-ap-southeast-1-internal.aliyuncs.com	100.118.219.18
Australia (Sydney)	ap-southeast-2	ap-southeast-2.axt.aliyun.com	100.100.44.12
		aliyun-client-assist-ap-southeast-2.oss-ap-southeast-2-internal.aliyuncs.com	100.100.44.1
Malaysia (Kuala Lumpur)	ap-southeast-3	ap-southeast-3.axt.aliyun.com	100.100.127.16
		aliyun-client-assist-ap-southeast-3.oss-ap-southeast-3-internal.aliyuncs.com	100.118.165.0
Indonesia (Jakarta)	ap-southeast-5	ap-southeast-5.axt.aliyun.com	100.100.80.165
		aliyun-client-assist-ap-southeast-5.oss-ap-southeast-5-internal.aliyuncs.com	100.100.16.5

Region	Region ID	Endpoint	IP Address
Philippines (Manila)	ap-southeast-6	ap-southeast-6.axt.aliyun.com	100.100.0.15
		aliyun-client-assist-ap-southeast-6.oss-ap-southeast-6-internal.aliyuncs.com	100.115.16.209
India (Mumbai)	ap-south-1	ap-south-1.axt.aliyun.com	100.100.80.108
		aliyun-client-assist-ap-south-1.oss-ap-south-1-internal.aliyuncs.com	100.118.211.136
Japan (Tokyo)	ap-northeast-1	ap-northeast-1.axt.aliyun.com	100.100.0.76
		aliyun-client-assist-ap-northeast-1.oss-ap-northeast-1-internal.aliyuncs.com	100.100.40.129
US (Silicon Valley)	us-west-1	us-west-1.axt.aliyun.com	100.100.29.34
		aliyun-client-assist-us-west-1.oss-us-west-1-internal.aliyuncs.com	100.100.29.86
US (Virginia)	us-east-1	us-east-1.axt.aliyun.com	100.100.152.140
		aliyun-client-assist-us-east-1.oss-us-east-1-internal.aliyuncs.com	100.115.60.17
Germany (Frankfurt)	eu-central-1	eu-central-1.axt.aliyun.com	100.100.46.12
		aliyun-client-assist-eu-central-1.oss-eu-central-1-internal.aliyuncs.com	100.115.154.14
UK (London)	eu-west-1	eu-west-1.axt.aliyun.com	100.100.0.20
		aliyun-client-assist-eu-west-1.oss-eu-west-1-internal.aliyuncs.com	100.100.41.198
UAE (Dubai)	me-east-1	me-east-1.axt.aliyun.com	100.100.43.7
		aliyun-client-assist-me-east-1.oss-me-east-1-internal.aliyuncs.com	100.100.43.1
Russia (Moscow)	rus-west-1	rus-west-1.axt.aliyun.com	100.100.0.4
		aliyun-client-assist-rus-west-1.oss-rus-west-1-internal.aliyuncs.com	100.118.214.129
China East 2 Finance	cn-shanghai-finance-1	cn-shanghai-finance-1.axt.aliyun.com	100.100.0.46
		aliyun-client-assist-cn-shanghai-finance-1.oss-cn-shanghai-finance-1-internal.aliyuncs.com	100.100.36.8

Region	Region ID	Endpoint	IP Address
China South 1 Finance	cn-shenzhen-finance-1	cn-shenzhen-finance-1.axt.aliyun.com	100.103.0.140
		aliyun-client-assist-cn-shenzhen-finance-1.oss-cn-shenzhen-finance-1-internal.aliyuncs.com	100.112.15.71
China North 2 Ali Gov 1	cn-north-2-gov-1	cn-north-2-gov-1.axt.aliyun.com	100.100.0.67
		aliyun-client-assist-cn-north-2-gov-1.oss-cn-north-2-gov-1-internal.aliyuncs.com	100.100.49.4

4.3.5. Start or stop the Cloud Assistant client

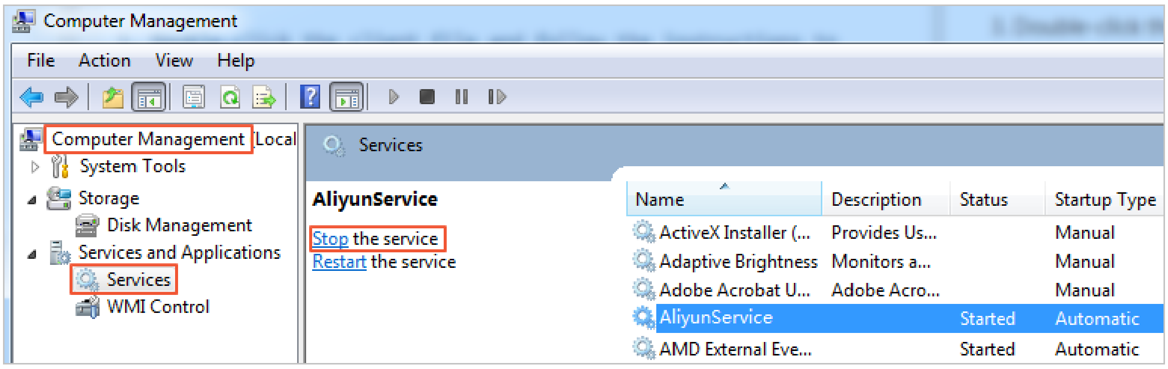
The Cloud Assistant client is an agent that runs Cloud Assistant commands on Elastic Compute Service (ECS) instances. This topic describes how to start or stop the Cloud Assistant client.

Start or stop the Cloud Assistant client on a Windows instance

To start or stop the Cloud Assistant client on a Windows instance, perform the following steps.

> **Warning** **Aliyun Assist Service** is the process of the Cloud Assistant client. If you stop **Aliyun Assist Service**, the Cloud Assistant client also stops. This may cause an exception on the instance, and the instance cannot be stopped in the ECS console. Proceed with caution when you stop Aliyun Assist Service.

1. Connect to the Windows instance. For more information, see Connect to a Windows instance by using a username and password.
2. Click Start and choose **Windows Administrative Tools > Computer Management**.
3. Choose **Computer Management (Local) > Services and Applications > Services**.
4. Find **Aliyun Assist Service** and click **Stop the service** or **Restart the service**.



Name	Description	Status	Startup Type
ActiveX Installer (...	Provides Us...		Manual
Adaptive Brightness	Monitors a...		Manual
Adobe Acrobat U...	Adobe Acro...		Manual
AliyunService		Started	Automatic
AMD External Eve...		Started	Automatic

Uninstall the Cloud Assistant daemon process from a Linux instance

The Cloud Assistant daemon process is used to monitor the resource consumption of the Cloud Assistant client, report the running status of the client, and restart the client when the client fails. Before you stop the Cloud Assistant client, you must first uninstall the Cloud Assistant daemon process.

> **Note** The Cloud Assistant daemon process is available only for Linux instances.

1. Connect to the Linux instance. For more information, see Connect to a Linux instance by using a password.
2. Stop the Cloud Assistant daemon process.

   ```
   /usr/local/share/assist-daemon/assist_daemon --stop
   ```

   > Note In the preceding command, */usr/local/share/assist-daemon/assist_daemon* specifies the default path of the Cloud Assistant daemon process.

3. Uninstall the Cloud Assistant daemon process.

   ```
   /usr/local/share/assist-daemon/assist_daemon --delete
   ```

4. Delete the directory of the Cloud Assistant daemon process.

   ```
   rm -rf /usr/local/share/assist-daemon
   ```

Start or stop the Cloud Assistant client on a Linux instance

> Note Before you stop the Cloud Assistant client, you must first uninstall the Cloud Assistant daemon process. For more information, see Uninstall the Cloud Assistant daemon process from a Linux instance.

To start or stop the Cloud Assistant client on a Linux instance, perform the following steps:

1. Connect to the Linux instance. For more information, see Connect to a Linux instance by using a password.
2. Run the following commands based on the initialization process of the Linux instance.
   - Linux operating systems that are based on new versions of the Linux kernel typically use the **systemd** initialization process. Perform the following steps:
     - Check whether the instance uses the systemd initialization process. If the instance uses systemd, a command output is displayed.

       ```
       strings /sbin/init | grep "/lib/system"
       ```

     - Stop the Cloud Assistant client.

       ```
       systemctl stop aliyun.service
       ```

     - Start the Cloud Assistant client.

       ```
       systemctl start aliyun.service
       ```

     - Restart the Cloud Assistant client.

       ```
       systemctl restart aliyun.service
       ```

   - Ubuntu 14 and earlier operating systems typically use the **UpStart** initialization process. Perform the following steps:

    - Check whether the instance uses the UpStart initialization process. If the instance uses UpStart, a command output is displayed.

      ```
      strings /sbin/init | grep "upstart"
      ```

    - Stop the Cloud Assistant client.

      ```
      /sbin/initctl stop aliyun-service
      ```

    - Start the Cloud Assistant client.

      ```
      /sbin/initctl start aliyun-service
      ```

    - Restart the Cloud Assistant client.

      ```
      /sbin/initctl restart aliyun-service
      ```

  - Linux operating systems that are based on earlier versions of the Linux kernel typically use the **sysvinit** initialization process. Perform the following steps:

    - Check whether the instance uses the sysvinit initialization process. If the instance uses sysvinit, a command output is displayed.

      ```
      strings /sbin/init | grep "sysvinit"
      ```

    - Stop the Cloud Assistant client.

      ```
      /etc/init.d/aliyun-service stop
      ```

    - Start the Cloud Assistant client.

      ```
      /etc/init.d/aliyun-service start
      ```

    - Restart the Cloud Assistant client.

      ```
      /etc/init.d/aliyun-service restart
      ```

4.4. Use the cloud assistant

4.4.1. Use the immediate execution feature

You can create and run a new command simultaneously by using the immediate execution feature.

Prerequisites

- The instances on which to run a command are in the **Running** (Running) state.
- You can retain up to 100 Cloud Assistant commands within an Alibaba Cloud region. This quota may increase based on your ECS usage. For more information about how to view the quota, see Step 1: View resource quotas. If you click Run when you create a command in the Create Command panel, the command does not count against your command quota.

  > **Note** You can also call the DescribeAccountAttributes operation with AttributeName.N set to *max-axt-command-count* to query the maximum number of Cloud Assistant commands that you can retain within a region.

- You can run Cloud Assistant commands up to 5,000 times within a region per day. This quota may increase based on your ECS usage. For more information about how to view the quota, see Step 1: View resource quotas.

  > **Note** You can also call the DescribeAccountAttributes operation with the AttributeName.N parameter set to *max-axt-invocation-daily* to query the maximum number of times that you can run Cloud Assistant commands within in a region per day.

- The Cloud Assistant client is installed on the instance. For more information, see Install the Cloud Assistant client.

  If you are concerned about recurring tasks, make sure that the version of the Cloud Assistant client is not earlier than the following ones. A recurring task is a task that is scheduled to run a command at a specified interval, only once at a specified time, or on a schedule defined by a cron expression with a specified year or time zone.

  - Linux: 2.2.3.282
  - Windows: 2.1.3.282

  If the `ClientNeedUpgrade` error code is returned after a recurring task is executed, update the Cloud Assistant client to the latest version. For more information, see Upgrades or disable upgrades for the Cloud Assistant client.

Context

When you use the immediate execution feature, take note of the following items:

- A command cannot exceed 16 KB in size after it is encoded in Base64.
- Up to 20 custom parameters can be specified in a single Cloud Assistant command.
- You can call an API operation to run a command on up to 50 instances.
- When you create a command, you must check whether the syntax, logic, and algorithm of the command are correct.

  For example, assume that you have created the */backup* directory (`mkdir /backup`) on an instance. You can run the following shell commands to archive a file in this directory:

  ```
  #!/bin/bash
  OF=/backup/my-backup-$(date +%Y%m%d).tgz
  tar -cf $OF {{file}}
  ```

  > **Note** In the preceding example, `{{file}}` is a custom parameter. When you run the commands, you can set this custom parameter to the name of the file to be archived. Example: */app/usrcredential*. Custom parameters can be used in scenarios that require dynamic values and multi-purpose values. We recommend that you specify custom parameters for security-sensitive data or data that changes with the environment. This data includes AccessKey pairs, instance IDs, authorization codes, time parameters, and critical system files.

Procedure in the ECS console

1.
2.
3.

4. In the upper-right corner, click **Create or Run Command**.

5. In the **Command Information** section, configure the parameters described in the following table.

Parameter	Description
Command Source	Select the command source. ○ **Enter Command Content**: creates a command. ○ **Select Saved Command**: selects an existing command.
Command Name	Enter a name for the command.
Implementation plan	Select a plan on how to run the command. ○ **Immediate execution**: The command is run immediately after you click **Run** or **Execute and Save**. ○ **After the next startup of the system**: The command is run the next time the selected instances are started after you click **Run** or **Execute and Save**. ○ **After each system startup**: The command is run each time the selected instances are started after you click **Run** or **Execute and Save**. ○ **Run on Schedule**: The command is run at a specified interval, at a specified time, or on a schedule after you click **Run** or **Execute and Save**. If you set Implementation plan to Run on Schedule, the following options are available: ■ **Run at Fixed Interval**: Use a rate expression to specify an interval at which to run the command. You can specify the interval in seconds, minutes, hours, or days. This option is applicable when tasks need to be executed at a fixed interval. **Note** When you set an interval, take note of the following limits: ■ The specified interval can only be anywhere from 60 seconds to 7 days and must be longer than the timeout period of the recurring task. ■ The specified interval is the amount of time elapsed between two consecutive times that the command is run on the selected instances. This interval does not relate to the amount of time required to run the command each time. For example, assume that you set the interval to 5 minutes and that it takes 2 minutes to run the command each time. Each time the command is run, the system waits 3 minutes before it runs the command again. ■ A task is not executed immediately after the task is created. For example, assume that you set the interval to 5 minutes for a task. The task begins to be executed 5 minutes after it is created.

Parameter	Description
	■ **Run Only Once at Specified Time**: Specify a point in time and a time zone to run the command only once. For example, if you set **Execution Time** to **2022-05-17 17:30:50** and **Time Zone** to **(GMT+8:00) Asia/Shanghai**, the command was run only once at 17:30:50 on May 17, 2022 (UTC+8). ■ **Run on Clock-based Schedule**: Use a cron expression to specify a schedule on which to run the command. Set Execution Frequency to a cron expression that defines a schedule accurate to the second, minute, hour, day of the month, month, day of the week, or year, and select a time zone from the Time Zone drop-down list. The system calculates the execution times of the command based on this cron expression and time zone and runs the command as scheduled. This option provides flexibility and is applicable when tasks need to executed on a regular basis. For more information about cron expressions, see Cron expression. **Note** The minimum interval must be 10 seconds or more and cannot be shorter than the timeout period of the recurring task. For example, if you set **Execution Frequency** to **0 0 12 ? * WED 2022** and set **Time Zone** to **(GMT+8:00) Asia/Shanghai**, the system runs the command at 12:00 every Wednesday in 2022 (UTC+8).
Command type	Select a command type. ○ For Linux instances, select **Shell**, **Python**, or **Perl**. ○ For Windows instances, select **Bat** or **PowerShell**.
Command	Enter or paste the content of the command. For information about sample shell commands, see View instance configurations.
Use Parameters	Specifies whether to use parameters. If you turn on **Use Parameters**, you can specify custom parameters in the `{{key}}` format in the **Command** field.
Command Description	Enter a description for the command. We recommend that you enter identifiable command information (such as the purpose of the command) for easy management and maintenance.

Parameter	Description
Username	Specify the username that is used to run the command on ECS instances. The best practice is to run commands based on the least privilege principle. We recommend that you run Cloud Assistant commands as a regular user. For more information, see Run Cloud Assistant commands as a regular user. By default, Cloud Assistant commands are run by the root user on Linux instances and by the system user on Windows instances.
Execution Path	Specify an execution path for the command. Default execution paths for instances that use different types of operating system: ○ For Linux instances, the default execution path is the */home* directory of the root user. ○ For Windows instances, the default execution path is *C:\Windows\system32*.
Timeout Period	Specify a timeout period for the command to be run on instances. If a task that runs a command times out, Cloud Assistant forcefully stops the task process. Unit: seconds. Default value: 60. Minimum value: 10. If you set **Timeout Period** to a value of less than 10, the system changes the value to 10 to ensure that the command can be run.

6. In the **Select Instances** and **Select Managed Instances** sections, select the instances on which you want to run the command.

   > ? **Note** A managed instance is an instance that is managed by Cloud Assistant but not provided by Alibaba Cloud. For more information, see Manage servers that are not provided by Alibaba Cloud.

7. Click **Execute and Save** or **Run** to immediately run the command task.

Procedure by using the CLI

Example on how to run a command only once

- Sample request:

  Call the RunCommand operation to create and run a Cloud Assistant command named update to update the operating system on instances.

```
aliyun ecs RunCommand --RegionId 'cn-hangzhou' \
--Name 'update' --Username 'root' --Type 'RunShellScript' \
--CommandContent 'eXVtIC15IHVwZGF0ZQ==' \
--Timeout '60' --RepeatMode 'Once' --ContentEncoding 'Base64' \
--InstanceId.1 'i-bp12e0ib2ztibede****'
```

> **Note** Values enclosed in single quotation marks ('') are example values of the parameters and must be changed based on actual conditions.

Parameter	Example	Description
RegionId	cn-hangzhou	The ID of region in which to create the command.
Name	update	The name of the command.
Username	root	The username used to run the command on ECS instances.
Type	RunShellScript	The command type. ○ For Linux instances, set the value to RunShellScript. ○ For Windows instances, set the value to RunBatScript or RunPowershellScript.
CommandContent	eXVtIHVwZGF0ZSAteQ==	The Base64-encoded content of the command.
Timeout	60	The timeout period.
RepeatMode	Once	The execution plan.
ContentEncoding	Base64	The encoding format.
InstanceId.1	i-bp12e0ib2ztibede****	The ID of ECS instance N on which to run the command. In this example, the N value is 1.

For more information, see RunCommand.

- Sample success response:

```
{
        "CommandId": "c-hz018qlm868****",
        "InvokeId": "t-hz018qlm86d****",
        "RequestId": "1D24FA80-64DB-4842-AB20-25207994418F"
}
```

Example on how to run a command on a regular basis

- Sample request:

  Call the RunCommand operation to create and run a Cloud Assistant command named update to update the operating system on instances at 12:00 every day in 2022 (UTC+8).

```
aliyun ecs RunCommand --RegionId 'cn-hangzhou' \
--Name 'update' --Description 'update' --Username 'root' --Type 'RunShellScript' \
--CommandContent 'eXVtIC15IHVwZGF0ZQ==' \
--Timeout '60' --RepeatMode 'Period' --ContentEncoding 'Base64' \
--Frequency '0 0 12 * * ? 2022 Asia/Shanghai' \
--InstanceId.1 'i-bp12e0ib2ztibede****'
```

> **Note** Values enclosed in single quotation marks ('') are example values of the parameters and must be changed based on actual conditions.

Parameter	Example	Description
RegionId	cn-hangzhou	The ID of region in which to create the command.
Name	update	The name of the command.
Description	update	The description of the command.
Username	root	The username used to run the command on ECS instances.
Type	RunShellScript	The command type. ◦ For Linux instances, set the value to RunShellScript. ◦ For Windows instances, set the value to RunBatScript or RunPowershellScript.
CommandContent	eXVtIC15IHVwZGF0ZQ==	The Base64-encoded content of the command.
Timeout	60	The timeout period.
RepeatMode	Period	The execution plan.
ContentEncoding	Base64	The encoding format.
Frequency	0 0 12 * * ? 2022 Asia/Shanghai'	The schedule on which to run the command.
InstanceId.1	i-bp12e0ib2ztibede****	The ID of ECS instance N on which to run the command. In this example, the N value is 1.

For more information, see RunCommand.

- Sample success response:

```
{
        "CommandId": "c-hz018qlm868****",
        "InvokeId": "t-hz018qlm86d****",
        "RequestId": "1D24FA80-64DB-4842-AB20-25207994418F"
}
```

Related information

- Query execution results and fix common problems
- RunCommand
- DescribeAccountAttributes

4.4.2. Create a command

You can use Cloud Assistant commands to perform routine tasks on ECS instances. These tasks include running automated O&M scripts, polling processes, resetting user passwords, installing or uninstalling software, updating applications, and installing patches. Command types can be batch or PowerShell for Windows instances, and shell for Linux instances. You can specify custom parameters as variables in Cloud Assistant commands.

Context

-
-
-
-

Procedure in the console

1.
2.
3.
4.
5.
6.
7. Click **Save**.

Procedure by using the CLI

- Sample request:

  Call the CreateCommand operation to create a Cloud Assistant command named *update* to update the system on instances.

```
aliyun ecs CreateCommand --RegionId 'cn-hangzhou' \
--CommandContent 'eXVtIHVwZGF0ZSAteQ==' \
--Type 'RunShellScript' \
--Name 'update' \
--Description 'update' \
--output cols=CommandId
```

> **Note** Values enclosed within single quotation marks ('') are example values of the parameters and must be changed based on actual conditions.

Parameter	Example	Description
RegionId	cn-hangzhou	The region ID.
Name	update	The name of the command.

Parameter	Example	Description
Type	RunShellScript	The type of the command. ○ For Linux instances, set the value to RunShellScript. ○ For Windows instances, the valid values are RunBatScript and RunPowershellScript.
CommandContent	eXVtIHVwZGF0ZSAteQ== =	The Base64-encoded content of the command.
Description	update	The description of the command.

For more information, see CreateCommand.

- Sample success response:

```
CommandId
---------
c-hz018qng4on****
```

What's next

After the command is created, you can view its detailed information on the **Commands** tab. For information about how to run this command on a specific instance, see Run a command.

Note If you turn on Use Parameters when you create a command, you must enter parameter values in the **Command Parameters** fields when you run the command.

Related information

- CreateCommand
- DescribeAccountAttributes

4.4.3. Run a command

After you create a Cloud Assistant command, you can run it on one or more Elastic Compute Service (ECS) instances. The execution status and results of the command on multiple instances do not affect each other.

Prerequisites

Before you run a Cloud Assistant command on ECS instances, make sure that the instances meet the following requirements:

- The instances are in the **Running** (`Running`) state.
-

Context

-
- If you select more than 50 instances to run a command in the ECS console, the system runs the

command on the instances in batches.

-

Procedure in the ECS console

1.
2.
3.
4. On the **Commands** tab of the Cloud Assistant page, find the command that you want to run and click **Create Task** in the **Actions** column.
5. In the **Create Task** panel, configure parameters.
   i. In the **Command Information** section, check the command content and configure command parameters and Username.

Parameter	Description
Command	Click **View** to check the command.
Implementation Plan	Select a command execution plan.
Username	The username that is used to run the command on the ECS instance. The best practice in permission management is to run commands based on the least privilege principle. We recommend that you run Cloud Assistant commands as a regular user. For more information, see Run Cloud Assistant commands as a regular user. By default, Cloud Assistant commands are run by the root user on Linux instances and by the system user on Windows instances.

   ii. In the **Select Instances** and **Select Managed Instances** sections, select one or more instances.

   If you have multiple instances, you can search for instances by ID, name, or tag, and filter results by client status.

   Note

6. Click **Create Task**.

Procedure by using the CLI

1. (Optional)Check the state of the instances on which you want to run a command. If the instances are not in the **Running** (`Running`) state, call the StartInstance operation to start the instances.

```
aliyun ecs StartInstance --InstanceId 'i-bp1f4f6o8lv0wqof****'
```

Note In this example, the values enclosed within single quotation marks ('') are example values of the parameters. You must change these values based on your actual conditions.

For more information, see StartInstance.

2. (Optional)Call the DescribeCloudAssistantStatus operation to check whether the Cloud Assistant client is installed on the instances.

```
aliyun ecs DescribeCloudAssistantStatus --RegionId 'cn-hangzhou' \
--InstanceId.1 'i-bp1f4f6o8lv0wqof****'
```

If the value of `CloudAssistantStatus` is true in the response, the Cloud Assistant client is installed on the instances. Otherwise, call the InstallCloudAssistant operation to install the Cloud Assistant client on the instances. For more information, see DescribeCloudAssistantStatus and InstallCloudAssistant.

3. Call the InvokeCommand operation to run a created Cloud Assistant command on one or more instances.

```
aliyun ecs InvokeCommand --RegionId 'cn-hangzhou' \
--InstanceId.1 'i-bp1f4f6o8lv0wqof****' \
--InstanceId.2 'i-bp137qu6142s3mhm****' \
--CommandId 'c-hz018qp243j****' \
--Timed 'false'
```

Parameter	Example	Description
RegionId	cn-hangzhou	The region ID of the command.
InstanceId.1	i-bp1f4f6o8lv0wqof****	The ID of the first instance on which to run the command.
InstanceId.2	i-bp137qu6142s3mhm****	The ID of the second instance on which to run the command.
CommandId	c-hz018qp243j****	The ID of the command.
Timed	false	Specifies whether to periodically run the command. If you want to run a command on a periodic basis, set **Timed** to true and set **Frequency** to specify a schedule on which to run the command. You can configure a command to run at a fixed interval based on a rate expression, run only once at a specified time, or run at scheduled times based on a cron expression. For example, if you specify a cron expression of 0 */20 * * * ?, the command is run every 20 minutes. For more information, see Cron expression

For more information, see InvokeCommand.

Related information

- Query execution results and fix common problems
- DescribeAccountAttributes
- InvokeCommand

4.4.4. Upload files to ECS instances

This topic describes how to use the Cloud Assistant client to upload files such as configuration files and scripts to Elastic Compute Service (ECS) instances.

Prerequisites

- The ECS instances to which you want to upload a file are in the **Running** (Running) state.
- The Cloud Assistant client is installed on the instances. For more information, see Install the Cloud Assistant client.
- You can call an API operation to send a file to up to 50 instances at a time.
- The file that you want to upload cannot exceed 32 KB in size after it is encoded in Base64.

Background information

You can use the Cloud Assistant client to upload files that cannot exceed 32 KB in size. If you want to upload files that are larger than 32 KB in size or if you want to download files from ECS instances, we recommend that you use the FileZilla tool over the SSH File Transfer Protocol (SFTP) and port 22.

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Maintenance & Monitoring** > **Cloud Assistant**.
3. In the top navigation bar, select a region.
4. In the upper-right corner of the Cloud Assistant page, click **Send File**.
5. In the **Command Information** section, configure the parameters described in the following table.

Parameter	Description
Destination System	Select the operating system of the ECS instances. Valid values: ○ **Linux** ○ **Windows**

Parameter	Description
Upload File	Select a method to use to upload the file. Valid values: ○ **Upload File**: You can click Upload File to select a file or drag a file to the Upload File section. ○ **Paste File Content**: You can paste the file content to the field. Note The file that you want to upload cannot exceed 32 KB in size after it is encoded in Base64.
File Name	Specify a name for the file. Note If you turn off **Overwrite**, make sure that the file name is unique across the destination path of the ECS instances.
Destination Path	Specify the destination path to save the file. ○ Default value when Destination System is set to Linux: `/root` ○ Default value when Destination System is set to Windows: `C:/Users/Administrator/Documents`
File Description	Specify a description for the file.
User	Specify the user to which the file belongs. This parameter is required only for Linux instances.
User Group	Specify the user group to which the file belongs. This parameter is required only for Linux instances.

Parameter	Description
Permission	Configure permissions on the file. Default value: `0644` . This value indicates that the file owner has read and write permissions on the file, and that other users in the same user group as the file owner and public users have read permissions on the file. This parameter is required only for Linux instances.
Overwrite	Specify whether to overwrite the file that has the same name as the uploaded file in the destination path.
Timeout Period	Set the timeout period for the file sending task. When the file sending task times out, Cloud Assistant forcibly stops the task process. Unit: seconds. Valid values: 10 to 86400. Default value: 60.

6. In the **Select Instances** and **Select Managed Instances** sections, select one or more instances.

   > ⓘ **Note**
   >
   > A managed instance is an instance that is not provided by Alibaba Cloud but managed by Cloud Assistant. For more information, see Manage servers that are not provided by Alibaba Cloud.

7. Click **Create Task**.
8. In the panel that appears, view the execution results of the file sending task.

View the execution results of the file sending task

1. In the left-side navigation pane, choose **Maintenance & Monitoring** > **Cloud Assistant**.
2. On the Cloud Assistant page, click the **File Sending Result** tab.
3. In the task list, view the execution states, execution IDs, and destination paths of file sending tasks.

   You can perform the following operations in the Actions column corresponding to a file sending task:

   - Click **View** to view the execution results of the task on each instance.
   - Click **Export** to export the task execution results.
   - Click **Send Again** to execute the task again.

References

- SendFile
- DescribeSendFileResults

4.4.5. Query execution results and fix common problems

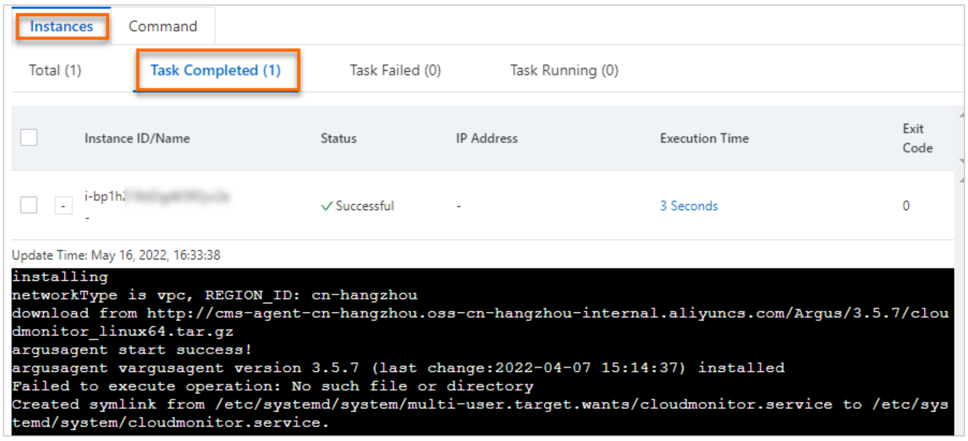
You can run a Cloud Assistant command only when all requirements are met, regardless of whether you run the command in the Elastic Compute Service (ECS) console or after you log on to an instance. To ensure that the intended operation is complete, we recommend that you view the command execution result and status after you run a command. If the execution fails, you can identify and fix the problems based on common error messages.

Context

When exceptions occur, different execution results and status are displayed for the command. These exceptions include the lack of dependencies, network disruptions, command semantic errors, command debugging errors, and abnormal instance status. You can use the ECS console or call an API operation to view the error messages in the execution results, and diagnose and fix the problems.

View execution results in the ECS console

1.
2.
3.
4. Click the **Command Execution Result** tab to view the execution results.
    - If the command execution succeeds, you can view the output in the execution results.
        a. Find a command execution result for which **Successful** is displayed in the **Status** column.
        b. In the **Actions** column, click **View**.
        c. In the Execution Details panel, view the execution result on the **Task Completed** tab of the **Instances** tab.



□	Instance ID/Name	Status	IP Address	Execution Time	Exit Code
□ -	i-bp1h[redacted] -	✓ Successful	-	3 Seconds	0

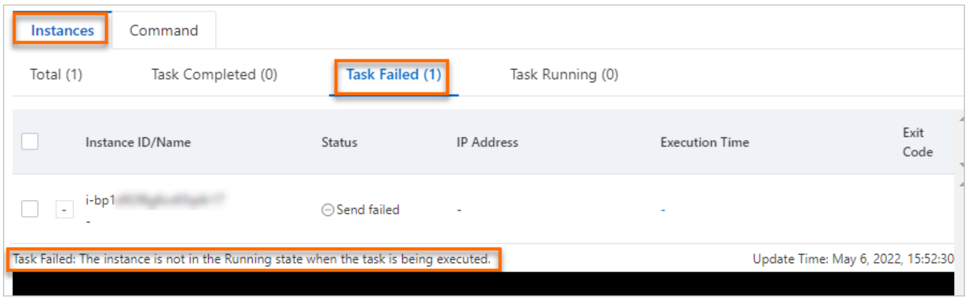
Update Time: May 16, 2022, 16:33:38

```
installing
networkType is vpc, REGION_ID: cn-hangzhou
download from http://cms-agent-cn-hangzhou.oss-cn-hangzhou-internal.aliyuncs.com/Argus/3.5.7/clou
dmonitor_linux64.tar.gz
argusagent start success!
argusagent vargusagent version 3.5.7 (last change:2022-04-07 15:14:37) installed
Failed to execute operation: No such file or directory
Created symlink from /etc/systemd/system/multi-user.target.wants/cloudmonitor.service to /etc/sys
temd/system/cloudmonitor.service.
```

    - If the command execution fails, view the error messages in the execution results, and diagnose and fix the problems based on the error messages.
        a. Find a command execution result for which **Task Failed** is displayed in the **Status** column.
        b. In the **Actions** column, click **View**.

c. In the Execution Details panel, view the execution result on the **Task Failed** tab of the **Instances** tab.

For information about common error messages and the solutions to the errors, see the Command errors and solutions section.



Instances | Command

Total (1) | Task Completed (0) | Task Failed (1) | Task Running (0)

□	Instance ID/Name	Status	IP Address	Execution Time	Exit Code
□ -	i-bp1[redacted] -	⊖ Send failed	-	-	

Task Failed: The instance is not in the Running state when the task is being executed.

Update Time: May 6, 2022, 15:52:30

[redacted]

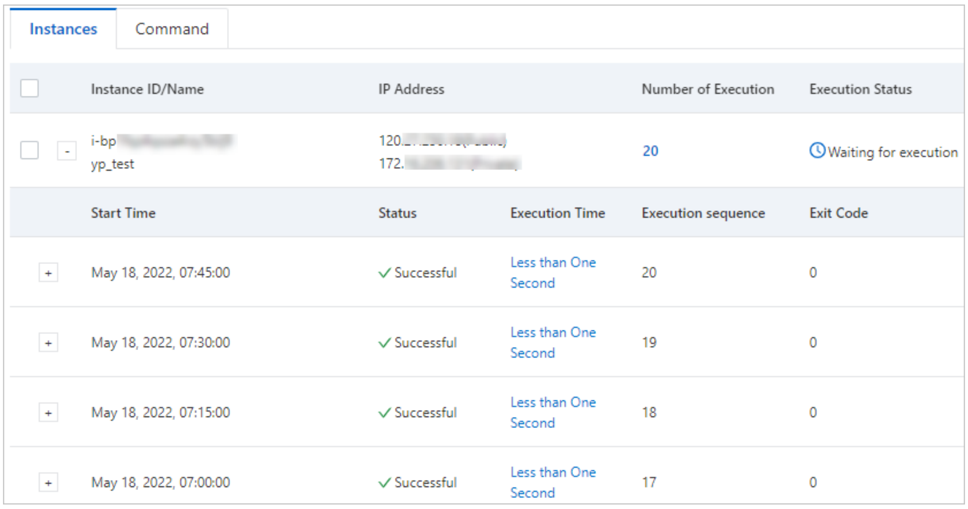
- View the results of a scheduled execution task.

a. Find a command execution result for which **Waiting for execution** is displayed in the **Status** column.

b. In the **Actions** column, click **View**.

c. In the Execution Details panel, view the execution result on the **Instances** tab.

The following figure shows the execution results of a command that is executed every 15 minutes.



Instances | Command

□	Instance ID/Name	IP Address	Number of Execution	Execution Status
□ -	i-bp[redacted] yp_test	120.[redacted] 172.[redacted]	20	Waiting for execution

	Start Time	Status	Execution Time	Execution sequence	Exit Code
+	May 18, 2022, 07:45:00	✓ Successful	Less than One Second	20	0
+	May 18, 2022, 07:30:00	✓ Successful	Less than One Second	19	0
+	May 18, 2022, 07:15:00	✓ Successful	Less than One Second	18	0
+	May 18, 2022, 07:00:00	✓ Successful	Less than One Second	17	0

View execution results by using Alibaba Cloud CLI

If you use Cloud Assistant by means of Alibaba Cloud CLI or OpenAPI Explorer, you can call the DescribeInvocations or DescribeInvocationResults operation to query the execution results of Cloud Assistant commands. If the execution fails, you can refer to the ErrorCode and ErrorInfo fields for error details.

In the following examples, the DescribeInvocations and DescribeInvocationResults operations are used to describe how to use Alibaba Cloud CLI to query execution results.

- Call the DescribeInvocations operation to query the execution status of a command.

```
aliyun ecs DescribeInvocations --RegionId TheRegionId --InvokeId your-invoke-id
```

- Call the DescribeInvocationResults operation to query the execution result of a command on a specific instance.

```
aliyun ecs DescribeInvocationResults --RegionId TheRegionId --InstanceId i-bp1g6zv0ce8og*
*****p --InvokeId your-invoke-id
```

Command errors and solutions

Error code	Error message	Solution
InstanceNotRunning	The error message returned because the instance is not in the Running state while the task is being created.	Check whether the instance is running normally.
InstanceRestarted	The error message returned because the instance is restarted while the task is being executed.	Do not restart the instance while the task is being executed.

ClientNotRunning	The error message returned because the Cloud Assistant client is not running.	The Cloud Assistant client is stopped or not installed. Perform the following operations to install or start the Cloud Assistant client:
		1. Check whether the process of the Cloud Assistant client runs normally.
		○ For Linux instances, run the following command:
		`ps -ef |grep aliyun-service`
		○ For Windows instances, check whether the aliyun_assist_service process exists in the Task Manager.
		2. If the process does not exist, start the Cloud Assistant client.
		○ For Linux instances, run the following command:
		`#If the Linux instances support systemctl, run the following command:`
		`systemctl start aliyun.service`
		`#If the Linux instances do not support systemctl, run the following command:`
		`/etc/init.d/aliyun-service start`
		○ For Windows instances, start AliyunService by using the Server Manager.
		Note If the Cloud Assistant client still cannot be started after the preceding operations are performed, re-install the Cloud Assistant client. For more information, see Install the Cloud Assistant client.

Error code	Error message	Solution
ClientNetworkBlocked	The error message returned because the instance network environment is abnormal.	1. Run the following command to check the network connectivity. If the network is normal, the instance ID is returned. `curl https://{region-id}.axt.aliyun.com/luban/api/instance/instance-id` 2. If the instance ID is not returned, check the instance security groups, firewall, DNS configurations, and route table to troubleshoot the problem. You must enable TCP port 443, TCP port 80, and UDP port 53 in the outbound direction to ensure that Cloud Assistant can access the following URLs: ○ https://*{region-id}*.axt.aliyun.com:443/ ○ http://100.100.100.200:80/ ○ http://aliyun-client-assist-*{region-id}*.oss-*{region-id}*-internal.aliyuncs.com **Note** *{region-id}* specifies the region ID of the instance. For example, if the instance resides in the China (Hangzhou) region, set this parameter to `cn-hangzhou`.

Error code	Error message	Solution

ClientNotResponse	The error message returned because the Cloud Assistant client does not respond.	Troubleshoot the problem based on logs of the Cloud Assistant client.
		1. Open the log file of the Cloud Assistant client. The following section describes the default paths of the log file:
		○ Linux instances: */usr/local/share/aliyun-assist/<Version number of Cloud Assistant>/log/aliyun_assist_main.log*
		○ Windows instances: *C:\ProgramData\aliyun\assist\<Version number of Cloud Assistant>\log\aliyun_assist_main.log*
		2. Query whether the task ID exists in the log file.
		○ If the task ID exists, check whether exceptions exist in the context. For example, you can check whether the command execution is complete and reported.
		○ If the task ID does not exist, run the Cloud Assistant command again. If the execution fails again, we recommend that you restart the Cloud Assistant client.
		■ For Linux instances, run one of the following commands:
		`#If the Linux instances support systemctl, run the following command:`
		`systemctl restart aliyun.service`
		`#If the Linux instances do not support systemctl, run the following command:`
		`/etc/init.d/aliyun-service restart`
		■ For Windows instances, start AliyunService by using the Server Manager.

ClientNeedUpgrade	The error message returned because the Cloud Assistant client is not upgraded.	Enable auto upgrade for the Cloud Assistant client or manually upgrade the Cloud Assistant client. For more information, see Upgrades or disable upgrades for the Cloud Assistant client.
ClientNotOnline	The error message returned because the Cloud Assistant client is not connected to the Cloud Assistant server.	Restart the Cloud Assistant client. For more information, see Start or stop the Cloud Assistant client. If the Cloud Assistant client still cannot connect to the Cloud Assistant server after it is restarted, submit a ticket.

Error code	Error message	Solution
DeliveryTimeout	The error message returned because the Cloud Assistant server failed to send the command to the Cloud Assistant client.	If the Cloud Assistant command is not sent to the instance, we recommend that you run the command again. If the problem persists, submit a ticket.
ExecutionTimeout	The error message returned because the command execution has timed out.	Extend the command execution timeout period. ● If you create and run a command in the ECS console, the **Timeout Period** parameter is set to 60 seconds by default. Specify an appropriate value. ● If you run a command by calling the RunCommand operation, the Timeout parameter is set to *60* seconds by default. Specify an appropriate value. ● If you create a command by calling the CreateCommand operation and run the command by calling the InvokeCommand operation, the Timeout parameter is set to *60* seconds by default when you create the command. Specify an appropriate value when you create the command, or call the ModifyCommand operation to change the value to an appropriate value after the command is created.
ExecutionException	The error message returned because an exception has occurred in command execution.	Check the error message in the ErrorInfo field. If you cannot identify the problem based on the error message, submit a ticket.
ExitCodeNonzero	The error message returned because the exit code of the execution is not 0 when the command is executed.	Check the command script and the command output.

Related information

- DescribeInvocationResults
- DescribeInvocations

4.4.6. View and run common Cloud Assistant commands

Common commands are Cloud Assistant commands that Alibaba Cloud provides to all users. These commands are applicable to a variety of scenarios such as software installation or uninstallation, instance status diagnostics, and key rotation. This topic describes how to view and run common Cloud Assistant commands.

Context

Common commands are Cloud Assistant commands that Alibaba Cloud provides to all Alibaba Cloud users. These commands contain scripts or executable programs that are used to install Cloud Assistant plug-ins and complex scripts that are used to configure servers, conduct health or security checks, install applications and system patches, handle files, modify system configurations, and manage services or applications.

Compared with custom commands, common commands are provided, published, and updated by Alibaba Cloud. After a common command is published, you can view the detailed content of the command and run the command on Elastic Compute Service (ECS) instances to perform specific operations. For example, you can run common commands to upgrade the Cloud Assistant client on Linux instances, determine whether to resize disks attached to Linux instances, or install Java on instances. After a common command is run on instances, you can view its execution progresses and results. You can run common commands to complete complex configurations in an easy and quick manner, which improves the efficiency of O&M.

In this topic, the `ACS-ECS-DiskResize-Diagnostic-for-linux.sh` common command is used. The command is used to check whether to resize disks attached to a Linux instance.

Methods

Method	Description
Run common commands in the ECS console	Run common commands by using the ECS console.
Run common commands by using the OpenAPI Explorer	Call the DescribeCommands operation to view common commands and call the InvokeCommand operation to run common commands by using the OpenAPI Explorer.
Run common commands by using Alibaba Cloud CLI	Call the DescribeCommands operation to view common commands and call the InvokeCommand operation to run common commands by using Alibaba Cloud CLI.

Run common commands in the ECS console

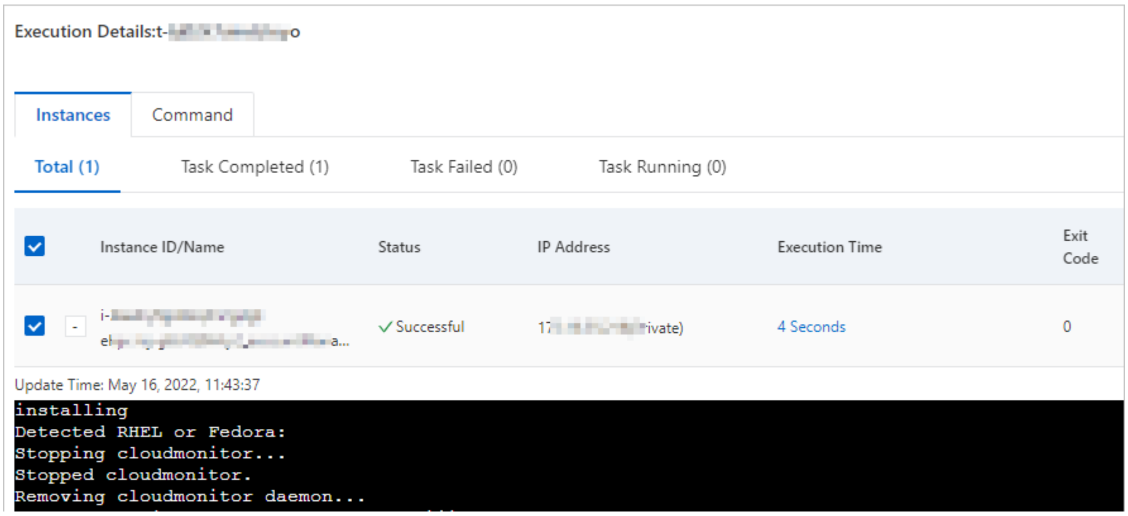
1.
2.
3.
4.
5. On the **Cloud Assistant** page, click the **Common Commands** tab.
6. Find the common command that you want to run and click **Create Task** in the **Actions** column.
7. In the **Create Task** panel, configure parameters and click **Create Task**.

   The following table describes the main parameters.

Note For information about parameters required to run common commands, see Procedure in the ECS console.

Section	Parameter	Description
Command Information	Command	Click **View** to view the command content.
	Implementation plan	Select an execution plan for the command. Valid values: ○ **Immediate execution** ○ **After the next startup of the system** ○ **After each system startup** ○ **Run on Schedule** For more information about execution plans, see Use the immediate execution feature.
	Username	Enter a username used to run the command on the ECS instance. Example: **root**. By default, Cloud Assistant commands are run by the root user on Linux instances and by the system user on Windows instances.
	Command Parameters	If Command Parameters is displayed in the panel, enter a custom valid value for each required parameter.
Select Instances	-	Select one or more instances on which you want to run the command. The selected instances must be in the Running state and have the Cloud Assistant client installed.
Select Managed Instances	-	Select one or more managed instances on which you want to run the command. The selected managed instances must be in the Normal state and have the Cloud Assistant client installed. Note Managed instances are servers that are not deployed on Alibaba Cloud but are managed by Cloud Assistant. For more information, see Manage servers that are not provided by Alibaba Cloud.

8. On the **Command Execution Result** tab, find the common command that is run and click **View** in the **Actions** column.
   On the execution details page, if **Successful** is displayed in the Status column, you can view the execution results of the common command.



Execution Details:t-[redacted]o

☑	Instance ID/Name	Status	IP Address	Execution Time	Exit Code
☑ -	i-[redacted] el[redacted]a...	✓ Successful	17[redacted]rivate)	4 Seconds	0

Update Time: May 16, 2022, 11:43:37

```
installing
Detected RHEL or Fedora:
Stopping cloudmonitor...
Stopped cloudmonitor.
Removing cloudmonitor daemon...
```

> Note If the common command execution fails, check the error message and troubleshoot the error. For more information, see Command errors and solutions.

Run common commands by using the OpenAPI Explorer

1. Query common commands by using the OpenAPI Explorer.

   You can call the DescribeCommands operation to query common commands or query a specified common command by using its name.

   In this example, the operation is called to query `ACS-ECS-DiskResize-Diagnostic-for-linux.sh` common command in the China (Hangzhou) region. Sample request:

```
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
import com.aliyuncs.profile.DefaultProfile;
import com.google.gson.Gson;
import java.util.*;
import com.aliyuncs.ecs.model.v20140526.*;
public class DescribeCommands {
    public static void main(String[] args) {
        DefaultProfile profile = DefaultProfile.getProfile("cn-hangzhou", "<accessKeyId
>", "<accessSecret>");
        IAcsClient client = new DefaultAcsClient(profile);
        DescribeCommandsRequest request = new DescribeCommandsRequest();
        request.setRegionId("cn-hangzhou");
        request.setName("ACS-ECS-DiskResize-Diagnostic-for-linux.sh");
        try {
            DescribeCommandsResponse response = client.getAcsResponse(request);
            System.out.println(new Gson().toJson(response));
        } catch (ServerException e) {
            e.printStackTrace();
        } catch (ClientException e) {
            System.out.println("ErrCode:" + e.getErrCode());
            System.out.println("ErrMsg:" + e.getErrMsg());
            System.out.println("RequestId:" + e.getRequestId());
        }
    }
}
```

In this example, the information of the `ACS-ECS-DiskResize-Diagnostic-for-linux.sh` common command is displayed. Sample response:

```
{
  "TotalCount": 1,
  "PageSize": 10,
  "RequestId": "2C23A5BA-66CF-5B70-BB1C-524AD75D****",
  "PageNumber": 1,
  "Commands": {
    "Command": [
      {
        "Description": "Check whether the disks attached to a Linux instance need to be
resized.",
        "Category": "Alibaba Cloud-ECS-Control and Diagnostics System\t",
        "ParameterNames": {
          "ParameterName": []
        },
        "Timeout": 60,
        "Provider": "AlibabaCloud.ECS.Diagnosis",
        "Name": "ACS-ECS-DiskResize-Diagnostic-for-linux.sh",
        "WorkingDir": "",
        "CommandContent": "IyEvYmluL2Jhc2gKIyBQcm92aWRlZCBieSBBbGliYWJhIENsb3VkIEVDUyBE
aWFnbm9zdGljIFNlcnZpY2UKIyBSZXR1cm46IHRydWU6IFlvdSBuZWVkIHRvIGV4ZWN1dGUgc29tZSBjb21tYW5
kIHRvIHJlc2l6ZSB5b3VyIGRpc2ssIHBsZWFzZSByZWZlciBodHRwczovL2hlbHAuYWxpeXVuLmNvbS9kb2N1bW
VudF9kZXRhaWwvMTEzMzE2Lmh0bWwuCiMgZmFsc2U6IE5vdGluZyB5b3UgbmVlZCB0byBkby4KIyBWZXJzaW9uO
iAxLjAKCnJlYWxEaXNrU2l6ZT1gZmRpc2sgLWx1IHwgZ3JlcCAnRGlzayAvZGV2JyB8IGF3ayAne3ByaW50ICQz
fScgfCBhd2sgJ3t4Kz0kMX1FTkR7cHJpbnQgeH0nYAoKZWZmZWN0aXZlRGlza1NpemU9YGRmIC1oIHwgYXdrICd
7TkY9Mn0xJyB8IGdyZXAgJy9kZXYvJyB8IGF3ayAne3ByaW50ICQyfScgfCBncmVwIC1vICdbWzpkaWdpdDpdXV
wrJyB8IGF3ayAne3grPSQxfUVORHtwcmludCB4fSdgCgpzdWJzdHJhY3Rpb249YGVjaG8gIiRyZWFsRGlza1Npe
mUgLSAkZWZmZWN0aXZlRGlza1NpemUiIHwgYmNgCgpzdWJzdHJhY3Rpb25QZXJjZW50PWBlY2hvICJzY2FsZT00
OyAkc3Vic3RyYWN0aW9uIC8gJHJlYWxEaXNrU2l6ZSIgfCBiY2AKCmlmIFsgYGVjaG8gIiRzdWJzdHJhY3Rpb25
QZXJjZW50PjAuMiIgfCBiY2AgLWVxIDEgXQp0aGVuCgllY2hvICJ0cnVlIgplbHNlCgllY2hvICJmYWxzZSIKZm
k=",
        "Type": "RunShellScript",
        "Version": 1,
        "InvokeTimes": 265,
        "CreationTime": "2022-04-22T02:34Z",
        "Latest": true,
        "EnableParameter": false,
        "CommandId": "c-hz02hthgomejtvk"
      }
    ]
  }
}
```

2. Run common commands by using the OpenAPI Explorer.

   You can call the InvokeCommand operation to run common commands or run a specified common command by using its name or by using the return value of `CommandId` in Step 1. The name of each common command remains the same in different regions.

   This section describes how to run a common command by calling the InvokeCommand operation. In this example, the operation is called to run the `ACS-ECS-DiskResize-Diagnostic-for-linux.sh` common command in the China (Hangzhou) region. Sample request:

```
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
import com.aliyuncs.profile.DefaultProfile;
import com.google.gson.Gson;
import java.util.*;
import com.aliyuncs.ecs.model.v20140526.*;
public class InvokeCommand {
    public static void main(String[] args) {
        DefaultProfile profile = DefaultProfile.getProfile("cn-hangzhou", "<accessKeyId
>", "<accessSecret>");
        IAcsClient client = new DefaultAcsClient(profile);
        InvokeCommandRequest request = new InvokeCommandRequest();
        request.setCommandId("ACS-ECS-DiskResize-Diagnostic-for-linux.sh"); //Enter the
name of the common command.
        request.setRegionId("cn-hangzhou");                                //Enter a r
egion ID. Example: cn-hangzhou.
        List<String> instanceIdList = new ArrayList<String>();
        instanceIdList.add("i-bp1czdx85x4yivyq****");
        request.setInstanceIds(instanceIdList);
        try {
            InvokeCommandResponse response = client.getAcsResponse(request);
            System.out.println(new Gson().toJson(response));
        } catch (ServerException e) {
            e.printStackTrace();
        } catch (ClientException e) {
            System.out.println("ErrCode:" + e.getErrCode());
            System.out.println("ErrMsg:" + e.getErrMsg());
            System.out.println("RequestId:" + e.getRequestId());
        }
    }
}
```

After the operation is called, you can obtain the value of `InvokeId` in the response, which is the execution ID of the common command. Sample response:

```
{
  "RequestId": "D0630B5E5-CF9D-5B9F-9AE8-8C3566D1****",
  "InvokeId": "t-hz02kwqc9pg****"
}
```

Then, on the Command Execution Result tab in the ECS console, you can view the command execution results to determine whether to resize the disks attached to the Linux instance.

Run common commands by using Alibaba Cloud CLI

1. Query common commands by using Alibaba Cloud CLI.

   You can call the DescribeCommands operation to query common commands.

   You can set the `Provider` parameter to `AlibabaCloud` to query all common commands that Alibaba Cloud provides. In this example, the operation is called to query the `ACS-ECS-DiskResize-Diagnostic-for-linux.sh` common command in the China (Hangzhou) region. The command is used to check whether to resize disks attached to a Linux instance. Sample request:

```
aliyun ecs DescribeCommands --region cn-hangzhou --RegionId cn-hangzhou --CommandId ACS
-ECS-DiskResize-Diagnostic-for-linux.sh
```

2. *Optional.* Check the state of the instance.
   - If the instance is in the **Running** state, skip this step.
   - If the instance is not in the **Running** state, call the StartInstances operation to start the instance.

     In this example, the operation is called to start the instance whose ID is `i-bp1f4f6o8lv0wqof****`. Sample request:

     ```
     aliyun ecs StartInstance --InstanceId 'i-bp1f4f6o8lv0wqof****'
     ```

3. Check whether the Cloud Assistant client is installed on the instance.

   Call the DescribeCloudAssistantStatus operation to check whether the Cloud Assistant client is installed on the instance. For more information, see DescribeCloudAssistantStatus.

   In this example, the operation is called to check whether the Cloud Assistant client is installed on the instance whose ID is `i-bp1f4f6o8lv0wqof****`. Sample request:

   ```
   aliyun ecs DescribeCloudAssistantStatus --RegionId 'cn-hangzhou' \
   --InstanceId.1 'i-bp1f4f6o8lv0wqof****'
   ```

   - If the value of `CloudAssistantStatus` is `true` in the response, the Cloud Assistant client is installed on the instance.
   - If the value of `CloudAssistantStatus` is `false` in the response, the Cloud Assistant client is not installed on the instance. This way, call the InstallCloudAssistant operation to install the Cloud Assistant client on the instance. For more information, see InstallCloudAssistant.

4. Run common commands by using Alibaba Cloud CLI.

   You can call the InvokeCommand operation to run a Cloud Assistant common command on one or more instances. For more information, see InvokeCommand.

   In this example, the operation is called to run the `ACS-ECS-DiskResize-Diagnostic-for-linux.sh` common command. The command is used to check whether to resize disks attached to a Linux instance. Sample request:

   ```
   aliyun ecs InvokeCommand --RegionId 'cn-hangzhou' \
   --InstanceId.1 'i-bp1f4f6o8lv0wqof****' \
   --InstanceId.2 'i-bp137qu6142s3mhm****' \
   --CommandId 'ACS-ECS-DiskResize-Diagnostic-for-linux.sh' \
   --Timed 'false'
   ```

   After the operation is called, you can obtain the value of `InvokeId` in the response, which is the execution ID of the common command. Example: `t-7d2a745b412b4601b2d47f6a768d****`. You can call the DescribeInvocations or DescribeInvocationResults operation to query command execution results. For more information, see DescribeInvocations or DescribeInvocationResults.

   Then, on the Command Execution Result tab in the ECS console, you can view the command execution results to determine whether to resize the disks attached to the Linux instance.

Related information

- DescribeCommands

- InvokeCommand
- StartInstance
- DescribeCloudAssistantStatus
- InstallCloudAssistant
- DescribeInvocations
- DescribeInvocationResults
- Query execution results and fix common problems

4.4.7. Modify a command

This topic describes how to modify the name and description of a Cloud Assistant command. We recommend that you properly manage created Cloud Assistant commands.

Procedure

1.
2.
3.
4. Move the pointer over the name of the command that you want to modify, click the ✎ icon, and configure the following parameters in the Modify Command dialog box:
    - **Name**: Enter a new command name.
    - **Description**: Enter a new command description.
5. Click **OK**.

4.4.8. Clone a command

A command clone operation creates a new version of an existing Cloud Assistant command. You can retain all the information of the original command (cloned command), or you can modify information such as the name, description, type, content, execution path, or timeout period in the new command (command clone).

Procedure

1.
2.
3.
4. On the **Commands** tab, find the Cloud Assistant command that you want to clone and click **Clone** in the **Actions** column.
5. In the **Clone Command** panel, configure the parameters described in the following table.

Parameter	Description
Command Name	Specify a name for the new command.
Implementation plan	Select a command execution plan.

Parameter	Description
Command Type	Select a command type.
Command	Enter or paste the command content. For more information about shell commands, see View instance configurations.
Command Description	Specify a description for the new command. We recommend that you set a description with information such as the command purpose that makes the command easy to identify, manage, and maintain.
Execution Path	Specify an execution path for the new command. Different default execution paths are provided based on the operating system of instances on which the command is run.
Timeout Period	Set the **timeout period** for the new command to run on instances. If a task that runs a command times out, Cloud Assistant forcefully stops the task process. Unit: seconds. Default value: 60. Minimum value: 10. If you set **Timeout Period** to a value of less than 10, the system changes the value to 10 to ensure that the execution succeeds.

6. After you confirm the configured parameters, click **Clone**.

4.4.9. Stop a command

This topic describes how to stop a running Cloud Assistant command in the Elastic Compute Service (ECS) console.

Prerequisites

The command to be stopped is in the **Running** (`Running`) or **Waiting for execution** (`Waiting for execution`) state.

Procedure

1.
2.
3.
4. Click the **Command Execution Result** tab, find the command task that you want to stop and click **Stop Task** in the **Actions** column.
5. In the **Stop Task** dialog box, select one or more ECS instances on which you want to stop the command and click **Stop**.

Related information

- StopInvocation

4.4.10. Delete a command

You are granted a quota for the number of Cloud Assistant commands per Alibaba Cloud region. To ensure a sufficient command quota, we recommend that you regularly delete commands that are no longer needed.

Context

You can also use the immediate execution feature to create and execute commands without consuming the command quota. For more information, see Use the immediate execution feature.

Procedure

1.
2.
3.
4. Find the commands that you want to delete and use one of the following methods to delete them:
    - To delete a single command, click **Delete** in the **Actions** column.
    - To delete multiple commands at a time, select the commands and click **Delete Command** in the lower part of the Cloud Assistant page.
5. In the **Delete Command** message, click **OK**.

Related information

- DeleteCommand

4.4.11. Use Cloud Assistant plug-ins

Cloud Assistant can remotely run commands and upload files and provide plug-ins. You can use Cloud Assistant plug-ins to make complex configurations by running simple commands. This improves O&M efficiency.

Context

Cloud Assistant plug-in	Description
Running method	• Log on to an Elastic Compute Service (ECS) instance by using SSH and run commands on the instance. This method is applicable only to Linux instances. For information about how to log on to an instance, see Connection methodsGuidelines on instance connection. • Go to the Cloud Assistant page in the ECS console.
Usage	• To query plug-ins, run the `acs-plugin-manager --list` command. • To run a specific plug-in, run the `acs-plugin-manager --exec --plugin <Plug-in name>` command.

Cloud Assistant plug-in	Description
Usage example	• Configure kdump • Automatically configure an ENI • Configure IPv6 addresses • Configure NIC multi-queue • Manage Intel Hyper-Threading • Manage security patches

Configure kdump

Kdump is a feature of the Linux kernel to create core dumps when kernel errors occur. The `ecs_dump_config` plug-in can be used to enable and disable the kdump feature, and query the status of the feature.

- Enable kdump.

  ```
  acs-plugin-manager --exec --plugin=ecs_dump_config --params --enable
  ```

- Disable kdump.

  ```
  acs-plugin-manager --exec --plugin=ecs_dump_config --params --disable
  ```

- Query the status of kdump.

  ```
  acs-plugin-manager --exec --plugin=ecs_dump_config --params --status
  ```

Automatically configure an ENI

Typically, you must manually make network configurations for an elastic network interface (ENI) after you add the ENI. The `multi-nic-util` plug-in can be used to automatically make network configurations for your ENI.

```
acs-plugin-manager --exec --plugin=multi-nic-util
```

Configure IPv6 addresses

The `ecs-util-ipv6` plug-in can be used to configure IPv6 addresses for ECS instances that have been assigned IPv6 addresses, or clear IPv6 configurations for ECS instances that have not been assigned IPv6 addresses. The `ecs-util-ipv6` plug-in can be used to enable IPv6, disable IPv6, and automatically or manually configure IPv6 addresses for instances. By default, the plug-in automatically configures IPv6 addresses. For more information about the integrated ecs-util-ipv6 tool of the `ecs-util-ipv6` plug-in, see Automatically configure IPv6 addresses.

- Enable IPv6.

  ```
  acs-plugin-manager --exec --plugin=ecs-utils-ipv6 --params --enable
  ```

- Disable IPv6.

  ```
  acs-plugin-manager --exec --plugin=ecs-utils-ipv6 --params --disable
  ```

- Automatically configure IPv6 addresses.

```
acs-plugin-manager --exec --plugin=ecs-utils-ipv6
```

- Manually configure IPv6 addresses.

  ```
  acs-plugin-manager --exec --plugin=ecs-utils-ipv6 --params --static,<dev>,<ip6s>,<prefix_
  len>,<gw6>
  ```

  Sample command:

  ```
  acs-plugin-manager --exec --plugin=ecs-utils-ipv6 --params --static,eth0,fe80::216:3eff:*
  ***:****,64,2408:400a:108:8300:ffff:ffff:****:****
  ```

Configure NIC multi-queue

Network interface controller (NIC) multi-queue enables an ECS instance to use multiple NIC queues to improve network performance. Performance bottlenecks may occur when a single vCPU of an instance is used to process NIC interrupts. To solve this issue, you can use NIC multi-queue to distribute NIC interrupts across different vCPUs. You can run the `ethtool -l ehtname` command to query the current number of NIC queues and the supported number of NIC queues.

The `ecs_tools_multiqueue` plug-in can be used to set the number of queues to the supported maximum number of queues on all NICs.

```
acs-plugin-manager --exec --plugin=ecs_tools_multiqueue
```

Manage Intel Hyper-Threading

ECS bare metal instances require Intel Hyper-Threading (HT) to be disabled for specific business scenarios. The `ecs_disable_intel_hyper-threading` plug-in can implement this feature.

To use this plug-in, you must add the `nr_cpus` kernel parameter to the *grub* file and set the parameter to half of the number of vCPUs of the instance type. Then, the **nr_cpus** parameter limits the maximum number of vCPUs supported by the kernel and disables HT.

After the kernel parameter is configured, you must restart the instance for the parameter to take effect. After the plug-in is run, the output prompts you to restart the instance.

> **Note** This plug-in cannot be used to disable HT on ECS instances that are not ECS bare metal instances. If you run the plug-in on an instance that is not an ECS bare metal instance, the system prompts you that the instance is not an ECS bare metal instance and then exits the plug-in.

```
acs-plugin-manager --exec --plugin=ecs_disable_intel_hyper-threading
```

Manage security patches

Security vulnerabilities on ECS instances must be fixed in a timely manner. Otherwise, serious security risks may arise. The `patch_manager` plug-in can be used to scan for and install security patches on ECS instances.

- Scan for security patches.

  ```
  acs-plugin-manager --exec --plugin=patch_manager --params --operation,scan
  ```

- Install the security patches and have the instance restarted if required.

```
acs-plugin-manager --exec --plugin=patch_manager --params --operation,install,--reboot,if
need
```

- Install the security patches without restarting the instance.

```
acs-plugin-manager --exec --plugin=patch_manager --params --operation,install,--reboot,no
```

4.4.12. Manage the service-linked role for Operation Content and Result Delivery

The Operation Content and Result Delivery feature provided by Cloud Assistant allows you to deliver O&M task execution records to specified Object Storage Service (OSS) buckets or Log Service Logstores for persistent storage. AliyunServiceRoleForECSArchiving is the Resource Access Management (RAM) service-linked role provided by Cloud Assistant for this feature to obtain access permissions on resources of other Alibaba Cloud services.

Context

A service-linked role is a role that is linked to a service and includes the permissions required to call other services. For example, the AliyunServiceRoleForECSArchiving service-linked role includes the access permissions on Log Service and OSS resources that are required for the Operation Content and Result Delivery feature to deliver Cloud Assistant task execution records. For more information about service-linked roles, see Service-linked roles.

Create the AliyunServiceRoleForECSArchiving role

When you use the Operation Content and Result Delivery feature, the system checks whether the AliyunServiceRoleForECSArchiving role exists. If the role does not exist, the system creates the role. The AliyunServiceRolePolicyForECSArchiving policy is attached to the AliyunServiceRoleForECSArchiving role. Cloud Assistant can assume the role to take on the permissions of the role.

The policy attached to a service-linked role is predefined by the linked service. You cannot add, modify, or delete the policy. You can view policies attached to a role and policy details in the RAM console. For more information, see View the basic information about a RAM role and View the basic information about a policy. The following code shows the content of the AliyunServiceRoleForECSArchiving policy:

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "oss:PutObject",
        "oss:GetBucketInfo",
        "log:GetProject",
        "log:GetLogStore",
        "log:CreateLogStore",
        "log:PostLogStoreLogs",
        "log:GetIndex",
        "log:CreateIndex"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "archiving.ecs.aliyuncs.com"
        }
      }
    }
  ]
}
```

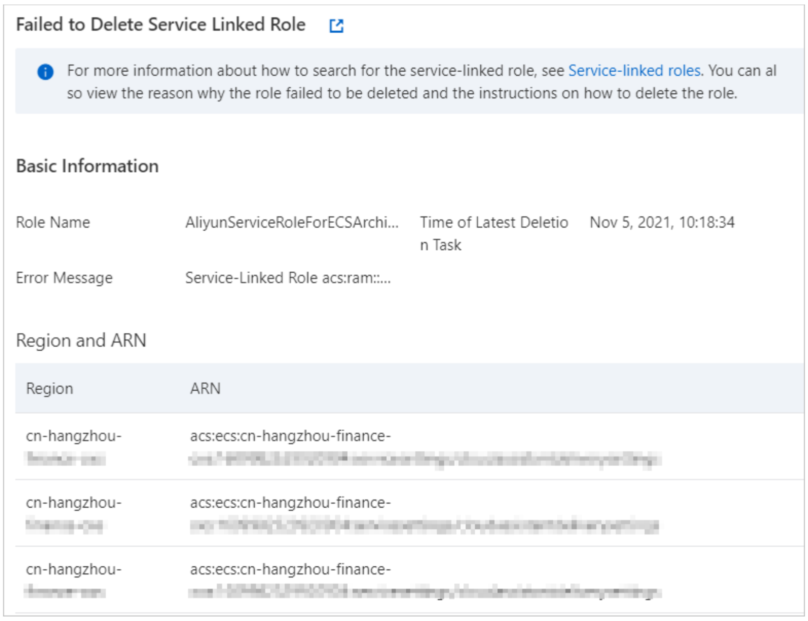
Delete the AliyunServiceRoleForECSArchiving role

If the AliyunServiceRoleForECSArchiving role within your account is no longer needed, you can manually delete the role.

1. Log on to the RAM console.
2. In the left-side navigation pane, choose **Identities > Roles**.
3. In the search box, enter AliyunServiceRoleForECSArchiving.

   The AliyunServiceRoleForECSArchiving role is displayed in the search result.
4. In the **Actions** column, click **Delete**.
5. Click **OK**.

   When the Operation Content and Result Delivery feature is enabled in one or more regions, the AliyunServiceRoleForECSArchiving role cannot be deleted and an error is reported if you attempt to delete the role. This prevents this role from being deleted by accident to ensure the availability of the Operation Content and Result Delivery feature. You can look into the error message for the regions in which the Operation Content and Result Delivery feature is enabled, as shown in the following figure. Then, you can disable the feature in the regions and try to delete the role again.



Failed to Delete Service Linked Role

For more information about how to search for the service-linked role, see Service-linked roles. You can also view the reason why the role failed to be deleted and the instructions on how to delete the role.

Basic Information

Role Name	AliyunServiceRoleForECSArchi...	Time of Latest Deletion Task	Nov 5, 2021, 10:18:34
Error Message	Service-Linked Role acs:ram::...		

Region and ARN

Region	ARN
cn-hangzhou-[redacted]	acs:ecs:cn-hangzhou-finance-[redacted]
cn-hangzhou-[redacted]	acs:ecs:cn-hangzhou-finance-[redacted]
cn-hangzhou-[redacted]	acs:ecs:cn-hangzhou-finance-[redacted]

For more information about how to delete service-linked roles, see Delete a service-linked role.

FAQ

Why cannot the AliyunServiceRoleForECSArchiving role be automatically created when I use a RAM user?

If you want to log on to the ECS console as a RAM user to use the Operation Content and Result Delivery feature, you must first use your Alibaba Cloud account to create and attach a policy to grant the RAM user the required permissions. Then, the AliyunServiceRoleForECSArchiving role can be automatically created. For more information, see Grant permissions to a RAM user. The following code indicates the policy that you must create and attach to the RAM user:

Note Replace *<account ID>* with the ID of your Alibaba Cloud account.

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "ram:CreateServiceLinkedRole"
            ],
            "Resource": "acs:ram:*:<account ID>:role/*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": [
                        "archiving.ecs.aliyuncs.com"
                    ]
                }
            }
        }
    ]
}
```

4.5. DevOps practice

4.5.1. Use Java to manage ECS instances without logging on to the instances

You can use Cloud Assistant to simultaneously run a command on multiple Elastic Compute Service (ECS) instances. The command can be a shell, batch, or PowerShell command. This topic describes how to use SDK for Java to check the state of the Cloud Assistant client, run a Cloud Assistant command, and query the execution results of the Cloud Assistant command.

Prerequisites

- The Cloud Assistant client is installed on the ECS instances that you want to manage. For more information, see Install the Cloud Assistant client.
- The ECS instances are in the **running** state. For information about how to use SDK for Java to check the state of ECS instances, see Query an ECS instance.
- The aliyun-java-sdk-ecs SDK dependency in Java is updated to V4.18.3 or later. For more information about the latest versions, visit MavenRepository.
- The shell, batch, or PowerShell command is compiled based on the instance configurations and the operations that you want to perform.

Context

The Cloud Assistant client can remotely run commands only when it is in the running state. We recommend that you check the state of the Cloud Assistant client before you use it.

Procedure

1. Obtain the AccessKey pair (AccessKey ID and AccessKey secret) of your account and query the region ID.

   For more information, see Regions and zones and Obtain an AccessKey pair.

2. Create a RunCommandBestPractice class to run a Cloud Assistant command on one or more ECS instances.

   The RunCommandBestPractice class performs the following operations:

   i. Check the state of the Cloud Assistant client on ECS instances.

      The Cloud Assistant client can remotely run commands only when it is in the **running** state. In this step, the class checks whether the Cloud Assistant client is in the **running** state, and performs operations based on the check result:

      - If the client is not in the **running** state, try again later.
      - If the client is in the **running** state, go to the next step.

   ii. Run a Cloud Assistant command on ECS instances.

   Sample code:

```
import com.aliyuncs.AcsResponse;
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.RpcAcsRequest;
import com.aliyuncs.ecs.model.v20140526.DescribeCloudAssistantStatusRequest;
import com.aliyuncs.ecs.model.v20140526.DescribeCloudAssistantStatusResponse;
import com.aliyuncs.ecs.model.v20140526.RunCommandRequest;
import com.aliyuncs.ecs.model.v20140526.RunCommandResponse;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
import com.aliyuncs.profile.DefaultProfile;
import com.google.gson.Gson;
import java.util.Arrays;
import java.util.List;
public class RunCommandBestPractice {
    private static final int MAX_RETRIES = 2;
    private static final long MAX_WAIT_INTERVAL = 20000L;
    private static final long TIME_OUT = 60L;
    public static void main(String[] args) throws InterruptedException {
        //The IDs of one or more ECS instances.
        List<String> instanceIds = Arrays.asList("<yourInstanceId01>", "<yourInstanceId02>");
        if (!checkCloudAssistantStatus(instanceIds)) {
            //After a timeout occurs, the Cloud Assistant client is still not in the running state.
            //Handle the exception or proceed to call the RunCommand operation.
        }
        RunCommandResponse runCommandResponse = runCommand(instanceIds);
        System.out.println(new Gson().toJson(runCommandResponse));
        //Call the DescribeInvocations operation to check the execution results of the Cloud Assistant command.
    }
    /**
     * Check the state of the Cloud Assistant client on the instances.
     * If a value of false is returned, try again later.
     * @param instanceIds
     * @return
     * @throws InterruptedException
     */
    private static boolean checkCloudAssistantStatus(List<String> instanceIds) throws InterruptedException {
        int retryTimes = 0;
        boolean retry = false;
        do {
            long waitTime = Math.min(getWaitInternal(retryTimes), MAX_WAIT_INTERVAL);
            Thread.sleep(waitTime);
            DescribeCloudAssistantStatusResponse describeCloudAssistantStatusResponse = describeCloudAssistantStatus(instanceIds);
            if (describeCloudAssistantStatusResponse == null) {
                //Handle exceptions such as the exception thrown when specified instances do not exist or are in the stopped state.
                retry = false;
            } else {
                for (DescribeCloudAssistantStatusResponse.InstanceCloudAssistantStatus instanceCloudAssistantStatus :
                        describeCloudAssistantStatusResponse.getInstanceCloudAssistantStatusSet()) {
                    if ("false".equals(instanceCloudAssistantStatus.getCloudAssistantSt
atus())) {
                        retry = true;
                        break;
                    }
                }
            }
        } while (retry && (retryTimes++ < MAX_RETRIES));
        return retryTimes <= MAX_RETRIES;
    }
    /**
     * Call the DescribeCloudAssistantStatus operation to check whether the Cloud Assis
tant client is installed on the instances.
     * @param instanceIds
     * @return
     */
    private static DescribeCloudAssistantStatusResponse describeCloudAssistantStatus(Li
st<String> instanceIds) {
        DescribeCloudAssistantStatusRequest describeCloudAssistantStatusRequest = new D
escribeCloudAssistantStatusRequest();
        describeCloudAssistantStatusRequest.setInstanceIds(instanceIds);
        return sendRequest(describeCloudAssistantStatusRequest);
    }
    /**
     * Call the RunCommand operation to run the Cloud Assistant command.
     * @param instanceIds
     * @return
     */
    private static RunCommandResponse runCommand(List<String> instanceIds) {
        RunCommandRequest runCommandRequest = new RunCommandRequest();
        //Edit the Cloud Assistant command.
        runCommandRequest.setCommandContent("<yourScript>");
        runCommandRequest.setInstanceIds(instanceIds);
        runCommandRequest.setType("RunShellScript");
        runCommandRequest.setTimeout(TIME_OUT);
        return sendRequest(runCommandRequest);
    }
    /**
     * Use the exponential backoff algorithm to obtain the retry interval.
     * @param retryTime
     * @return
     */
    private static long getWaitInternal(int retryTime) {
        return (long)(Math.pow(2, retryTime) * 1000L);
    }
    private static <T extends AcsResponse> T sendRequest(RpcAcsRequest<T> request) {
        //Initialize the profile object and configure the region ID (Example: cn-hangzh
ou) and the AccessKey pair.
        DefaultProfile profile = DefaultProfile.getProfile("<yourRegionId>", "<yourAcce
ssKeyId>", "<yourAccessKeySecret>");
        IAcsClient client = new DefaultAcsClient(profile);
        try {
            T response = client.getAcsResponse(request);
            return response;
        } catch (ServerException e) {
            //Handle 5XX errors.
            e.printStackTrace();
        } catch (ClientException e) {
            //Handle 4XX errors.
            System.out.println("ErrCode:" + e.getErrCode());
            System.out.println("ErrMsg:" + e.getErrMsg());
            System.out.println("RequestId:" + e.getRequestId());
        }
        return null;
    }
}
```

Note If the Cloud Assistant client is always in the **not running** state, we recommend that you troubleshoot the problem by performing the following operations:

- Check whether the Cloud Assistant client is installed. By default, ECS instances created from public images after December 1, 2017 are pre-installed with the Cloud Assistant client. If the Cloud Assistant client is not installed on your instances, install the client. For more information, see Install the Cloud Assistant client.
- Check the network configurations. Make sure that you can perform domain name resolution or make network requests on the instances and that you can access the endpoint of the Cloud Assistant in the format of `https://{regionId}.axt.aliyun.com`. Replace *{regionId}* with the region ID of your instances.

A result similar to the following one is returned. Record InvokeId.

```
{
    "RequestId": "473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E",
    "InvokeId": "t-hz0b22o6******",
    "CommandId": "c-b224dc5072f3460fbb10fc2912******"
}
```

3. Create a DescribeInvocationsSample class to check whether the command is executed.

```
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.ecs.model.v20140526.DescribeInvocationsRequest;
import com.aliyuncs.ecs.model.v20140526.DescribeInvocationsResponse;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
import com.aliyuncs.profile.DefaultProfile;
import com.google.gson.Gson;
public class DescribeInvocationsSample {
    public static void main(String[] args) {
        DefaultProfile profile = DefaultProfile.getProfile("<yourRegionId>", "<yourAcce
ssKeyId>", "<yourAccessKeySecret>");
        IAcsClient client = new DefaultAcsClient(profile);
        DescribeInvocationsRequest request = new DescribeInvocationsRequest();
        //Enter the execution ID of the Cloud Assistant command.
        request.setInvokeId("t-hz0b22o6******");
        try {
            DescribeInvocationsResponse response = client.getAcsResponse(request);
            System.out.println(new Gson().toJson(response));
        } catch (ServerException e) {
            e.printStackTrace();
        } catch (ClientException e) {
            System.out.println("ErrCode:" + e.getErrCode());
            System.out.println("ErrMsg:" + e.getErrMsg());
            System.out.println("RequestId:" + e.getRequestId());
        }
    }
}
```

Result

A result similar to the following one is returned. You can call the InvokeInstances operation to view the execution states and results of the command. For more information, see DescribeInvocations.

```
{
    "requestId": "42837BE9-1230-4E66-A21C-EC11C24221A3",
    "totalCount": 1,
    "pageNumber": 1,
    "pageSize": 10,
    "invocations": [{
        "invokeId": "t-hz0b22o6******",
        "creationTime": "2021-01-07T10:11:03Z",
        "commandId": "c-hz0179jxlag****",
        "commandType": "RunShellScript",
        "commandName": "cmd-2021-01-07",
        "commandContent": "******",
        "frequency": "",
        "timed": false,
        "invokeStatus": "PartialFailed",
        "invocationStatus": "PartialFailed",
        "parameters": "{}",
        "username": "",
        "invokeInstances": [{
            "instanceId": "i-bp11entzst4xwyb******",
            "repeats": 1,
            "instanceInvokeStatus": "Finished",
            "invocationStatus": "Success",
            "output": "******",
            "exitCode": 0,
            "dropped": 0,
            "errorCode": "",
            "errorInfo": "",
            "creationTime": "2021-01-07T10:11:03Z",
            "startTime": "2021-01-07T10:11:04Z",
            "stopTime": "",
            "finishTime": "2021-01-07T10:11:05Z",
            "updateTime": "2021-01-07T10:11:05Z"
        }, {
            "instanceId": "i-bp1ida94x2133l******",
            "repeats": 1,
            "instanceInvokeStatus": "Failed",
            "invocationStatus": "Timeout",
            "output": "******",
            "dropped": 49259,
            "errorCode": "ExecutionTimeout",
            "errorInfo": "the command execution has been timeout.",
            "creationTime": "2021-01-07T10:11:03Z",
            "startTime": "2021-01-07T10:11:04Z",
            "stopTime": "",
            "finishTime": "2021-01-07T10:12:04Z",
            "updateTime": "2021-01-07T10:12:04Z"
        }]
    }]
}
```

Related information

- RunCommand
- DescribeInstances
- DescribeInvocations

4.5.2. Use Python to manage ECS instances without logging on to the instances

You can use Cloud Assistant to simultaneously run a command on multiple Elastic Compute Service (ECS) instances. The command can be a shell, batch, or PowerShell command. You can use SSH or Remote Desktop Protocol (RDP) to log on to ECS instances and perform O&M. Cloud Assistant allows you to perform O&M on ECS instances without logging on to the instances. This topic describes how to use Cloud Assistant to manage ECS instances in a Python development environment.

Prerequisites

- The Cloud Assistant client is installed on the ECS instances that you want to manage. For more information, see Install the Cloud Assistant client.
- The aliyun-python-sdk-ecs SDK dependency in Python is updated to V2.1.2 or later. For more information about the latest versions, visit GitHub Repo Alibaba Cloud.

Procedure

1. Compile the shell, batch, or PowerShell command based on the instance configurations and the operations that you want to perform.

   For more information about sample commands, see View instance configurations and Modify instance configurations and install applications.

2. Find the instances that meet the specified requirements.

   The instances must be in the **running** state. For more information about how to use ECS SDK for Python to query instances, see Query an ECS instance.

3. Obtain the AccessKey pair of your account and query the region ID.

   For more information, see Regions and zones and Obtain an AccessKey pair.

4. Run a Cloud Assistant command on one or more ECS instances.

   Sample code:

```
# coding=utf-8
# If the Python sdk is not installed, run 'sudo pip install aliyun-python-sdk-ecs'.
# Make sure you're using the latest sdk version.
# Run 'sudo pip install --upgrade aliyun-python-sdk-ecs' to upgrade.
from aliyunsdkcore.client import AcsClient
from aliyunsdkcore.acs_exception.exceptions import ClientException
from aliyunsdkcore.acs_exception.exceptions import ServerException
from aliyunsdkecs.request.v20140526.RunCommandRequest import RunCommandRequest
from aliyunsdkecs.request.v20140526.DescribeInvocationResultsRequest import DescribeInvocationResultsRequest
import json
import sys
import base64
import time
import logging
```

```
# Configure the log output formatter
logging.basicConfig(level=logging.INFO,
                    format="%(asctime)s %(name)s [%(levelname)s]: %(message)s",
                    datefmt='%m-%d %H:%M')
logger = logging.getLogger()
access_key = '<yourAccessKey ID>'             # Enter your AccessKey ID.
access_key_secret = '<yourAccessKey Secret>'  # Enter your AccessKey secret.
region_id = '<yourRegionId>'                  # Enter your region ID.
client = AcsClient(access_key, access_key_secret, region_id)
def base64_decode(content, code='utf-8'):
    if sys.version_info.major == 2:
        return base64.b64decode(content)
    else:
        return base64.b64decode(content).decode(code)
def get_invoke_result(invoke_id):
    request = DescribeInvocationResultsRequest()
    request.set_accept_format('json')
    request.set_InvokeId(invoke_id)
    response = client.do_action_with_exception(request)
    response_detail = json.loads(response)["Invocation"]["InvocationResults"]["InvocationResult"][0]
    status = response_detail.get("InvocationStatus","")
    output = base64_decode(response_detail.get("Output",""))
    return status,output
def run_command(cmdtype,cmdcontent,instance_id,timeout=60):
    """
    cmdtype: The command type. Valid values: RunBatScript, RunPowerShellScript, or RunShellScript.
    cmdcontent: The command content.
    instance_id: The instance ID.
    """
    try:
        request = RunCommandRequest()
        request.set_accept_format('json')
        request.set_Type(cmdtype)
        request.set_CommandContent(cmdcontent)
        request.set_InstanceIds([instance_id])
        # Specify the timeout period for running the command. Unit: seconds. The default value is 60. Specify this parameter based on the actual command.
        request.set_Timeout(timeout)
        response = client.do_action_with_exception(request)
        invoke_id = json.loads(response).get("InvokeId")
        return invoke_id
    except Exception as e:
        logger.error("run command failed")
def wait_invoke_finished_get_out(invoke_id,wait_count,wait_interval):
    for i in range(wait_count):
        status,output = get_invoke_result(invoke_id)
        if status not in ["Running","Pending","Stopping"]:
            return status,output
        time.sleep(wait_interval)
    logger.error("after wait %d times, still can not wait invoke-id %s finished")
    return "",""
def run_task():
    # Specify the type of the Cloud Assistant command.
    cmdtype = "RunShellScript"
    # Specify the content of the Cloud Assistant command.
    cmdcontent = """
    #!/bin/bash
    yum check-update
    """
    # Specify the timeout period.
    timeout = 60
    # Specify the ID of your instance.
    ins_id = "i-wz9bsqk9pa0d2oge****"
    # Run the command.
    invoke_id = run_command(cmdtype,cmdcontent,ins_id,timeout)
    logger.info("run command,invoke-id:%s" % invoke_id)
    # Wait for the command to be run. Query the command running state 10 times at an interval of 5 seconds. Specify the query times and the interval based on your actual requirements.
    status,output = wait_invoke_finished_get_out(invoke_id,10,5)
    if status:
        logger.info("invoke-id execute finished,status: %s,output:%s" %(status,output))
if __name__ == '__main__':
    run_task()
```

Related information

References

- CreateCommand
- InvokeCommand
- DescribeInvocationResults
- DescribeCommands

4.5.3. Change the logon password of an instance

If you do not specify a password when you create an ECS instance or forget the password of an instance, you can use Cloud Assistant to change the password of the instance. You can also reset the password in the console. However, the password changed by using Cloud Assistant takes effect without the need to restart the instance.

Procedure

1.
2.
3.
4. Click the ID of the instance for which you want to run the Cloud Assistant command to go to the **Instance Details** page.
5. Click the **Remote Commands/Files** tab and click **Send Command**.
6. Configure parameters to change the instance password. The following table describes the parameters.

Parameter	Description
Command Type	The type of the command. ◦ For Linux instances, **Shell** is selected by default. ◦ For Windows instances, select **Bat** or **PowerShell**.
Retain Command	Specifies whether to save the command. After you save the command, you can use Cloud Assistant to view, modify, and run the command again.

Command Content	The content of the command used to change the instance password. Run one of the following commands based on the operating system of your instance:
	◦ Linux:
	`echo "root:<yourPassword>"|chpasswd`
	◦ Windows:
	`net user "Administrator" "<yourPassword>"`
	Note
	◦ Replace *<yourPassword>* with your new password.
	◦ The password must be 8 to 30 characters in length. It must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters. The password of a Windows instance cannot start with a forward slash (/).

7. Click **Run**.

Result

If **Success** is displayed in the **Command Output** section, the password is changed. Then, you can check whether the new password can be used to log on to the instance. For more information about how to log on to the instance, see Guidelines on instance connection.

4.5.4. View instance configurations

You can use Cloud Assistant to compile scripts for viewing instance configurations and run the scripts on multiple ECS instances simultaneously. Then, you can determine what action to take next based on the responses, such as continuing downloading or updating the software. This topic uses shell scripts for Linux as an example to describe how to view instance configurations.

Make sure that you fully understand how to use Cloud Assistant. For more information, see *Use the cloud assistant* .

- Create a command
- Run a command

- Use the immediate execution feature
- Query execution results and fix common problems

Overview

Whether the scripts in this topic can be run on an ECS instance depends on the operating system and configurations of the instance. We recommend that you modify the scripts as needed. You can include the custom parameter {{key}} in the script to increase its applicability.

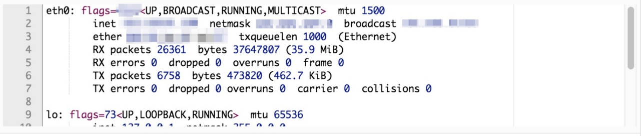
- View basic configurations of an instance
- View system processes or file details
- View information of Java projects

View basic configurations of an instance

- Scenario: You can use Cloud Assistant to query multiple instances simultaneously.
- Example: You can run the following scripts to view some configurations of an instance.

```
# View information of activated network interface controllers (NICs). ifconfig
# View information of all NICs. ifconfig -a
# View brief information of NICs. ifconfig -s
# View memory information. free -g
# View memory information. cat /proc/meminfo
# View operation system information, such as the kernel version. uname -a
# View hard disk usage. df -h
# View information of all hardware. dmidecode | more
```

- Result: If you run the ifconfig script, the following output is displayed in the ECS console.



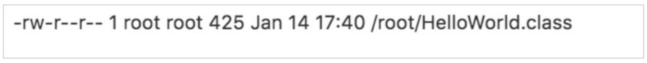
```
eth0: flags=[redacted]<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        ether [redacted]  txqueuelen 1000  (Ethernet)
        RX packets 26361  bytes 37647807 (35.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6758  bytes 473820 (462.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
```

View system processes or file details

- Scenario: You can use Cloud Assistant to view system processes or file details within an instance.
- Example: You can run the following scripts to query information of files and system processes.

```
# View information of all system processes. ps -ef
# View information of a specific system process. {{processName}} is the key of a custom p
arameter and you need to set the corresponding value before you run the script. ps -ef |
grep {{processName}}
# View details of the file. ls -la {{fileName}}
# Query the file path. find {{path}} | grep {{fileName}}
```

- Result: If you run the `ls -la /root/HelloWorld.class` script, the following output is displayed in the ECS console.



```
-rw-r--r-- 1 root root 425 Jan 14 17:40 /root/HelloWorld.class
```

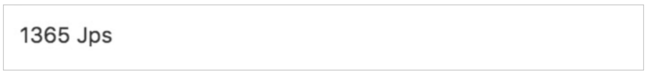
View information of Java projects

- Scenario: You can use Cloud Assistant to view the details of a specific process in the instance, such as memory or usage frequency of the process.

- Example: You can run the following scripts to view information of processes or memory in a Java project.

  ```
  # View real-time monitoring statistics on the resources and performance of applications,
  such as the heap size and garbage collection. jstat
  jstat -compiler pid: shows information about the number of Just in Time (JIT) compilers o
  n the Java Virtual Machine (JVM). jstat -class pid: shows information about the number an
  d space usage of loaded class files. jstat -gcnew pid: shows information about new object
  s. jstat -gcnewcapacity pid: shows information and usage of new objects. jps
   # Obtain memory matching details from core files or processes, such as the heap size and
  perm size of the JMV heap. jmap
  jmap -histo pid
  ```

- Result: The following output is displayed in the ECS console.

  ```
  1365 Jps
  ```

Related information

- RunCommand
- CreateCommand
- InvokeCommand
- DescribeInvocations

4.5.5. Modify instance configurations and install applications

You can use Cloud Assistant to compile scripts for modifying configurations or installing applications and run the scripts on multiple ECS instances simultaneously. This eliminates the need to log on to instances one by one, saving your time. This topic uses shell scripts for Linux as an example to describe how to modify instance configurations.

Make sure that you fully understand how to use Cloud Assistant. For more information, see *Use the cloud assistant* .

- Create a command
- Run a command
- Use the immediate execution feature
- Query execution results and fix common problems

Overview

Whether the scripts in this topic can be run on an ECS instance depends on the operating system and configurations of the instance. We recommend that you modify the scripts as needed. You can include the custom parameter {{key}} in the script to increase its applicability.

- Modify instance configurations
- Install applications
- Upgrade applications

Modify instance configurations

- Scenario: Modify configurations of an ECS instance by using Cloud Assistant.
- Example: Run the following scripts to add, delete, and modify user information in an instance.

```
# Add a user and set a password. {{password}} is the key of a custom parameter and you need to set the corresponding value before you run the script. useradd -m -p {{password}} {{newUser}}
# Change the password. passwd {{password}}
# Delete the user. userdel {{newUser}}
# Modify the username. usermod -l {{newUser}} -d /home/{{newUser}} -m {{previousUser}}
```

- Result: If you run the `useradd -m -p test** student` script, the following output is generated:

```
[root@EcsHost ~]# su - student -c pwd
/home/student
```

Install applications

- Scenario: You can simultaneously install applications on multiple instances by using Cloud Assistant. This reduces repeated installation and deployment operations.
- Example: Run the following scripts to install Python 3, which is suitable for systems that use yum, such as CentOS.

```
yum install zlib zlib-devel readline-devel sqlite-devel bzip2-devel openssl-devel gdbm-devel libdbi-devel ncurses-libs kernel-devel libxslt-devel libffi-devel python-devel zlib-devel openldap-devel sshpass gcc git -y
wget -c https://www.python.org/ftp/python/3.6.6/Python-3.6.6.tgz
tar -xzvf Python-3.6.6.tgz
cd Python-3.6.6
./configure --prefix=/usr/local/python3
make all
make install
make clean
make distclean
ln -s /usr/local/python3/bin/python3 /usr/bin/python3
ln -s /usr/local/python3/bin/pip3 /usr/bin/pip3
```

- Result: If you run the python3 script after Python 3 is installed, the following output is generated. If Python 3 is not installed, the error message `command not found` is returned.

```
[root@EcsHost ~]# python3
Python 3.6.6 (default, Jan 10 20**, 14:09:05)
[GCC 4.8.5 20150623 (Red Hat 4.8.5-39)] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

Upgrade applications

- Scenario: You can upgrade applications within multiple ECS instances by using Cloud Assistant.
- Example: You can run the following scripts to upgrade Python from 3.6.0 to 3.7.0.

```
wget https://www.python.org/ftp/python/3.7.0/Python-3.7.0.tgz && rm -rf /usr/bin/python3
tar -xzvf Python-3.7.0.tgz
cd Python-3.7.0
./configure && make && make install
ln -s /usr/local/bin/python3.7 /usr/bin/python3
ln -s /usr/local/bin/python3.7-config /usr/bin/python-config
python3 -V
```

- Result: The application is upgraded.

```
[root@EcsHost ~]# python3 -V
Python 3.7.0
```

Related information

- RunCommand
- CreateCommand
- InvokeCommand
- DescribeInvocations

4.5.6. Use RAM to implement permission control

Resource Access Management (RAM) users are virtual accounts to which RAM policies can be attached to grant different levels of permissions. This ensures more secure and controllable access and reduces the risk of disclosing the AccessKey pair of your Alibaba Cloud account. This topic describes how to grant permissions to a RAM user and provides some sample policies on Cloud Assistant.

Context

RAM policies can be custom policies created by yourself and system policies provided by Alibaba Cloud. You can use an Alibaba Cloud account to create custom policies to define region-specific permissions and permissions on Elastic Compute Service (ECS) instances, Cloud Assistant commands, or managed-instance activation codes, and attach the policies to RAM users.

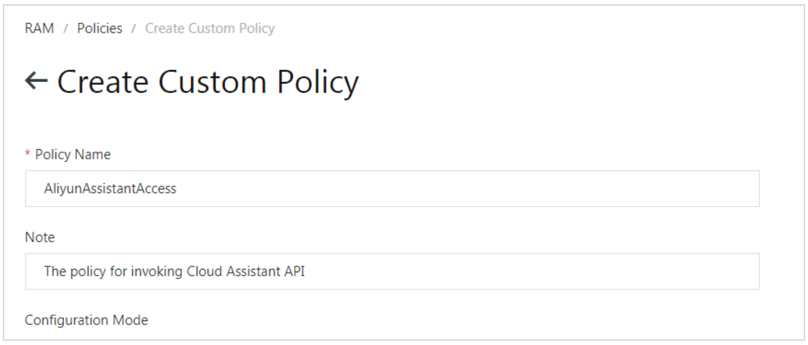
Procedure

1. Use your Alibaba Cloud account to create a RAM user.

   For more information, see Create a RAM user.

2. Use your Alibaba Cloud account to create a custom policy.

   For more information, see Create a custom policy.

   * Policy Name

   AliyunAssistantAccess

   Note

   The policy for invoking Cloud Assistant API

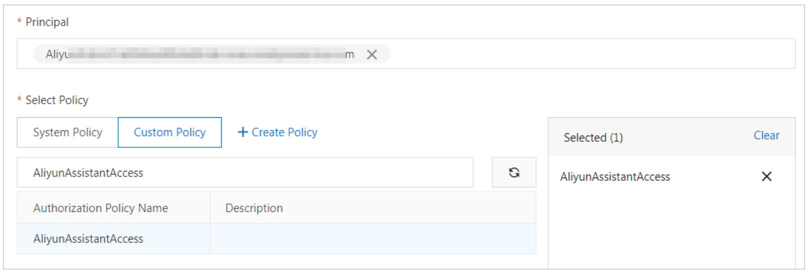
   Examples of custom policies on Cloud Assistant:

- Policies that grant the following permissions on Cloud Assistant:
  - Administrator (read and write) permissions on Cloud Assistant
  - Read-only permissions on Cloud Assistant
  - Region-specific permissions on Cloud Assistant
- Policies that grant the following permissions on the Cloud Assistant client:
  - Permissions to query the installation status of the Cloud Assistant client
  - Permissions to install the Cloud Assistant client
- Policies that grant the following permissions on Cloud Assistant commands:
  - Permissions to query Cloud Assistant commands
  - Permissions to delete Cloud Assistant commands
  - Permissions to create Cloud Assistant commands
  - Permissions to modify Cloud Assistant commands
  - Permissions to run Cloud Assistant commands
  - Permissions to create and run Cloud Assistant commands simultaneously
  - Permissions to query command execution results
  - Permissions to stop running commands
- Policies that grant the following permissions on file sending:
  - Permissions to upload local files
  - Permissions to query the results of file upload operations
- Policies that grant the following permissions on Operation Content and Result Delivery:
  - Permissions to query and modify the Operation Content and Result Delivery settings
  - Permissions to query the Operation Content and Result Delivery settings
  - Region-specific permissions on Operation Content and Result Delivery
  - Permissions to query Object Storage Service (OSS) buckets
  - Permissions to query Log Service projects and Logstores
- Policies that grant the following permissions on managed instances:
  - Permissions to deregister managed instances
  - Permissions to query managed instances
  - Permissions to create activation codes
  - Permissions to disable activation codes
  - Permissions to query activation codes
  - Permissions to delete activation codes

3. Use your Alibaba Cloud account to attach policies to the created RAM user.

   For more information, see Grant permissions to a RAM user.

   - Attach a created custom policy.



* Principal

Aliyu[redacted]m ×

* Select Policy

AliyunAssistantAccess

Authorization Policy Name	Description
AliyunAssistantAccess	

Selected (1) Clear

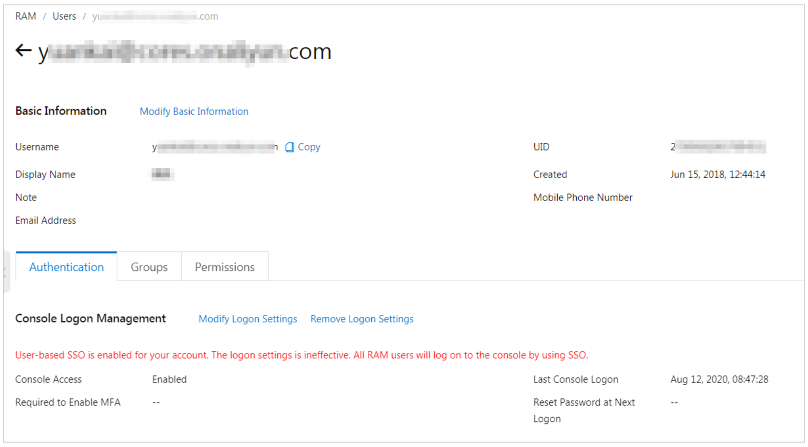
AliyunAssistantAccess ×

- Attach the following system policies provided by Alibaba Cloud:
    - AliyunECSAssistantFullAccess: grants RAM users the permissions to manage Cloud Assistant.
    - AliyunECSAssistantReadonlyAccess: grants RAM users read-only permissions on Cloud Assistant.

  You can log on to the RAM console to view the system policies and their details. For more information, see View the basic information about a policy.

4. Check whether the RAM user is authorized to log on to the Alibaba Cloud Management Console.

   If a RAM user does not have the **Console Access** permission, the RAM user can use Cloud Assistant only by calling API operations. For more information, see View the permissions of a RAM user.



RAM / Users / y[redacted].com

← y[redacted].com

Basic Information Modify Basic Information

Username	y[redacted]n Copy	UID	2[redacted]
Display Name	[redacted]	Created	Jun 15, 2018, 12:44:14
Note		Mobile Phone Number	
Email Address			

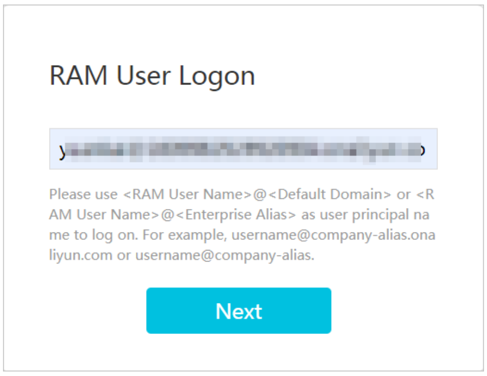
Console Logon Management Modify Logon Settings Remove Logon Settings

User-based SSO is enabled for your account. The logon settings is ineffective. All RAM users will log on to the console by using SSO.

Console Access	Enabled	Last Console Logon	Aug 12, 2020, 08:47:28
Required to Enable MFA	--	Reset Password at Next Logon	--

5. Log on to the Alibaba Cloud Management Console as the RAM user.

   For more information, see Log on to the Alibaba Cloud Management Console as a RAM user.



RAM User Logon

y[redacted]

Please use <RAM User Name>@<Default Domain> or <RAM User Name>@<Enterprise Alias> as user principal name to log on. For example, username@company-alias.onaliyun.com or username@company-alias.

6. Log on to the ECS console as the RAM user, go to the Cloud Assistant page, and use Cloud Assistant.

Administrator (read and write) permissions on Cloud Assistant

The following sample policy grants RAM users all the query and management permissions on Cloud Assistant API operations.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeInstances",
                "ecs:DescribeTag*",
                "ecs:*Command",
                "ecs:DescribeCommand*",
                "ecs:DescribeInvocation*",
                "ecs:StopInvocation",
                "ecs:*CloudAssistant*",
                "ecs:SendFile",
                "ecs:DescribeSendFileResults",
                "ecs:*ManagedInstance",
                "ecs:DescribeManagedInstances",
                "ecs:*Activation",
                "ecs:DescribeActivations"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/*",
                "acs:ecs:*:*:command/*",
                "acs:ecs:*:*:activation/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ram:CreateServiceLinkedRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": [
                        "archiving.ecs.aliyuncs.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecs:ListServiceSettings",
                "ecs:UpdateServiceSettings"
            ],
            "Resource": [
                "acs:ecs:*:*:servicesettings/cloudassistantdeliverysettings"
            ]
        }
    ]
}
```

Read-only permissions on Cloud Assistant

The following sample policy grants RAM users all the query permissions on Cloud Assistant API operations.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeInstances",
                "ecs:DescribeTag*",
                "ecs:DescribeCommand*",
                "ecs:DescribeInvocation*",
                "ecs:DescribeCloudAssistant*",
                "ecs:DescribeSendFileResults",
                "ecs:DescribeManagedInstances",
                "ecs:DescribeActivations"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/*",
                "acs:ecs:*:*:command/*",
                "acs:ecs:*:*:activation/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecs:ListServiceSettings"
            ],
            "Resource": [
                "acs:ecs:*:*:servicesettings/cloudassistantdeliverysettings"
            ]
        }
    ]
}
```

Region-specific permissions on Cloud Assistant

You can specify region fields in the Resource list to limit the permissions of RAM users to a specific region. The following sample policy grants RAM users permissions to use Cloud Assistant within the China (Hangzhou) region.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeInstances",
                "ecs:DescribeTag*",
                "ecs:*Command",
                "ecs:DescribeCommand*",
                "ecs:DescribeInvocation*",
                "ecs:StopInvocation",
                "ecs:*CloudAssistant*",
                "ecs:SendFile",
                "ecs:DescribeSendFileResults",
                "ecs:*ManagedInstance",
                "ecs:DescribeManagedInstances",
                "ecs:*Activation",
                "ecs:DescribeActivations"
            ],
            "Resource": [
                "acs:ecs:cn-hangzhou:*:instance/*",
                "acs:ecs:cn-hangzhou:*:command/*",
                "acs:ecs:cn-hangzhou:*:activation/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ram:CreateServiceLinkedRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": [
                        "archiving.ecs.aliyuncs.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecs:ListServiceSettings",
                "ecs:UpdateServiceSettings"
            ],
            "Resource": [
                "acs:ecs:cn-hangzhou:*:servicesettings/cloudassistantdeliverysettings"
            ]
        }
    ]
}
```

Permissions to query the installation status of the Cloud Assistant client

API operation: DescribeCloudAssistantStatus

- The following sample policy grants RAM users the permissions to query the installation status of the Cloud Assistant client on all ECS instances.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeInstances",
                "ecs:DescribeCloudAssistantStatus"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/*"
            ]
        }
    ]
}
```

- You can specify instance IDs in the Resource list to limit the permissions to specific instances. The following sample policy grants RAM users the permissions to query the installation status of the Cloud Assistant client on the specified instances.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeInstances",
                "ecs:DescribeCloudAssistantStatus"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/i-instancexxx000a",
                "acs:ecs:*:*:instance/i-instancexxx000b"
            ]
        }
    ]
}
```

Permissions to install the Cloud Assistant client

API operation: InstallCloudAssistant

- The following sample policy grants RAM users the permissions to install the Cloud Assistant client on any ECS instance.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:InstallCloudAssistant"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/*"
            ]
        }
    ]
}
```

- You can specify instance IDs in the Resource list to limit the permissions to specific instances. The following sample policy grants RAM users the permissions to install the Cloud Assistant client on the specified instances.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:InstallCloudAssistant"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/i-instancexxx00a",
                  "acs:ecs:*:*:instance/i-instancexxx00b"
            ]
        }
    ]
}
```

Permissions to query Cloud Assistant commands

API operation: DescribeCommands

- The following sample policy grants RAM users the permissions to query all Cloud Assistant commands.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeCommands"
            ],
            "Resource": [
                "acs:ecs:*:*:command/*"
            ]
        }
    ]
}
```

- You can specify command IDs in the Resource list to limit the permissions to specific commands. The following sample policy grants RAM users the permissions to query the specified commands.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeCommands"
            ],
            "Resource": [
                "acs:ecs:*:*:command/c-commandxxx000a",
                "acs:ecs:*:*:command/c-commandxxx000b"
            ]
        }
    ]
}
```

Permissions to delete Cloud Assistant commands

API operation: DeleteCommand

- The following sample policy grants RAM users the permissions to delete all Cloud Assistant commands.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DeleteCommand"
            ],
            "Resource": [
                "acs:ecs:*:*:command/*"
            ]
        }
    ]
}
```

- You can specify command IDs in the Resource list to limit the permissions to specific commands. The following sample policy grants RAM users the permissions to delete the specified commands.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DeleteCommand"
            ],
            "Resource": [
                "acs:ecs:*:*:command/c-commandxxx000a",
                "acs:ecs:*:*:command/c-commandxxx000b"
            ]
        }
    ]
}
```

Permissions to create Cloud Assistant commands

API operation: CreateCommand

The following sample policy grants RAM users the permissions to create Cloud Assistant commands.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:CreateCommand"
            ],
            "Resource": [
                "acs:ecs:*:*:command/*"
            ]
        }
    ]
}
```

Permissions to modify Cloud Assistant commands

API operation: ModifyCommand

- The following sample policy grants RAM users the permissions to modify all Cloud Assistant commands.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:ModifyCommand"
            ],
            "Resource": [
                "acs:ecs:*:*:command/*"
            ]
        }
    ]
}
```

- You can specify command IDs in the Resource list to limit the permissions to specific commands. The following sample policy grants RAM users the permissions to modify the specified commands.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:ModifyCommand"
            ],
            "Resource": [
                "acs:ecs:*:*:command/c-commandxxx000a",
                "acs:ecs:*:*:command/c-commandxxx000b"
            ]
        }
    ]
}
```

Permissions to run Cloud Assistant commands

API operation: InvokeCommand

- The following sample policy grants RAM users the permissions to run commands on any instance.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:InvokeCommand"
            ],
            "Resource": [
                "acs:ecs:*:*:command/*",
                "acs:ecs:*:*:instance/*"
            ]
        }
    ]
}
```

- You can specify instance IDs in the Resource list to limit the permissions to specific instances. The following sample policy grants RAM users the permissions to run commands on the specified instances.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:InvokeCommand"
            ],
            "Resource": [
                "acs:ecs:*:*:command/*",
                "acs:ecs:*:*:instance/i-instancexxx00a",
                "acs:ecs:*:*:instance/i-instancexxx00b"
            ]
        }
    ]
}
```

- You can specify command IDs in the Resource list to limit the permissions to specific commands. The following sample policy grants RAM users the permissions to run the specified commands on instances.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:InvokeCommand"
            ],
            "Resource": [
                "acs:ecs:*:*:command/c-commandxxx00a",
                "acs:ecs:*:*:command/c-commandxxx00b",
                "acs:ecs:*:*:instance/*"
            ]
        }
    ]
}
```

- You can specify both command IDs and instance IDs in the Resource list to limit the permissions to specific commands and instances. The following sample policy grants RAM users the permissions to run the specified commands on the specified instances.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:InvokeCommand"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/i-instancexxx00a",
                "acs:ecs:*:*:instance/i-instancexxx00b",
                "acs:ecs:*:*:command/c-commandxxx00a",
                "acs:ecs:*:*:command/c-commandxxx00b"
            ]
        }
    ]
}
```

Permissions to create and run Cloud Assistant commands simultaneously

API operation: RunCommand

Note If you set the `KeepCommand` parameter to true when you call the RunCommand operation, you must add the `"acs::ecs:*:*:command/*"` line to the Resource list.

- The following sample policy grants RAM users the permissions to create and run commands simultaneously on any instance.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs: RunCommand"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/*"
            ]
        }
    ]
}
```

- You can specify instance IDs in the Resource list to limit the permissions to specific instances. The following sample policy grants RAM users the permissions to create and run commands simultaneously on the specified instances.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs: RunCommand"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/i-instancexxx00a",
                "acs:ecs:*:*:instance/i-instancexxx00b"
            ]
        }
    ]
}
```

Permissions to query command execution results

API operation: DescribeInvocations

- The following sample policy grants RAM users the permissions to query command execution results on any instance.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs: DescribeInvocations"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/*",
                "acs:ecs:*:*:command/*"
            ]
        }
    ]
}
```

- You can specify instance IDs in the Resource list to limit the permissions to specific instances. The following sample policy grants RAM users the permissions to query command execution results on the specified instances.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs: DescribeInvocations"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/i-instancexxx00a",
                "acs:ecs:*:*:instance/i-instancexxx00b",
                "acs:ecs:*:*:command/*"
            ]
        }
    ]
}
```

- You can specify command IDs in the Resource list to limit the permissions to specific commands. The following sample policy grants RAM users the permissions to query the execution results of the specified commands on instances.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs: DescribeInvocations"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/*",
                "acs:ecs:*:*:command/c-commandxxx00a",
                "acs:ecs:*:*:command/c-commandxxx00b"
            ]
        }
    ]
}
```

- You can specify both command IDs and instance IDs in the Resource list to limit the permissions to specific commands and instances. The following sample policy grants RAM users the permissions to query the execution results of only specified commands on the specified instances.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs: DescribeInvocations"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/i-instancexxx00a",
                "acs:ecs:*:*:instance/i-instancexxx00b",
                "acs:ecs:*:*:command/c-commandxxx00a",
                "acs:ecs:*:*:command/c-commandxxx00b"
            ]
        }
    ]
}
```

Permissions to stop running commands

API operation: StopInvocation

- The following sample policy grants RAM users the permissions to stop running commands on any instance.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:StopInvocation"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/*"
            ]
        }
    ]
}
```

- You can specify instance IDs in the Resource list to limit the permissions to specific instances. The following sample policy grants RAM users the permissions to stop running commands on the specified instances.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:StopInvocation"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/i-instancexxx00a",
                "acs:ecs:*:*:instance/i-instancexxx00b"
            ]
        }
    ]
}
```

Permissions to upload local files

API operation: SendFile

- The following sample policy grants RAM users the permissions to upload local files to any instance.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:SendFile"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/*"
            ]
        }
    ]
}
```

- You can specify instance IDs in the Resource list to limit the permissions to specific instances. The following sample policy grants RAM users the permissions to upload local files to the specified instances.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:SendFile"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/i-instancexxx00a",
                  "acs:ecs:*:*:instance/i-instancexxx00b"
            ]
        }
    ]
}
```

Permissions to query the results of file upload operations

API operation: DescribeSendFileResults

- The following sample policy grants RAM users the permissions to query the results of file upload operations to any instance.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeSendFileResults"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/*"
            ]
        }
    ]
}
```

- You can specify instance IDs in the Resource list to limit the permissions to specific instances. The following sample policy grants RAM users the permissions to query the results of file upload operations to the specified instances.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeSendFileResults"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/i-instancexxx00a",
                  "acs:ecs:*:*:instance/i-instancexxx00b"
            ]
        }
    ]
}
```

Permissions to query and modify the Operation Content and Result Delivery settings

The following sample policy grants RAM users the permissions to query and modify the Operation Content and Result Delivery settings.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:ListServiceSettings",
                "ecs:UpdateServiceSettings"
            ],
            "Resource": [
                "acs:ecs:*:*:servicesettings/cloudassistantdeliverysettings"
            ]
        }
    ]
}
```

Permissions to query the Operation Content and Result Delivery settings

The following sample policy grants RAM users the permissions to query the Operation Content and Result Delivery settings

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:ListServiceSettings"
            ],
            "Resource": [
                "acs:ecs:*:*:servicesettings/cloudassistantdeliverysettings"
            ]
        }
    ]
}
```

Region-specific permissions on Operation Content and Result Delivery

You can specify region fields in the Resource list to limit the permissions of RAM users to a specific region.

- The following sample policy grants RAM users the permissions to query and modify the Operation Content and Result Delivery settings within the China (Hangzhou) region.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:ListServiceSettings",
                "ecs:UpdateServiceSettings"
            ],
            "Resource": [
                "acs:ecs:cn-hangzhou:*:servicesettings/cloudassistantdeliverysettings"
            ]
        }
    ]
}
```

- The following sample policy grants RAM users the permissions to query the Operation Content and Result Delivery settings within the China (Hangzhou) region.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:ListServiceSettings"
            ],
            "Resource": [
                "acs:ecs:cn-hangzhou:*:servicesettings/cloudassistantdeliverysettings"
            ]
        }
    ]
}
```

Permissions to query Object Storage Service (OSS) buckets

When you deliver O&M task execution records to OSS as a RAM user, you must grant the RAM user the permissions to query OSS buckets.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "oss:ListBuckets"
            ],
            "Resource": "*"
        }
    ]
}
```

You must also learn about RAM policies on OSS so that you can query and analyze the execution records delivered to OSS. For more information, see OSS RAM policy overview and Common examples of OSS RAM policies.

Permissions to query Log Service projects and Logstores

When you deliver O&M task execution records to Log Service as a RAM user, you must grant the RAM user the permissions to query Log Service projects and Logstores.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "log:ListProject",
                "log:ListLogStores"
            ],
            "Resource": "*"
        }
    ]
}
```

You must also learn about RAM policies on Log Service so that you can query and analyze the execution records delivered to Log Service. For more information, see RAM authentication rule overview.

Permissions to deregister managed instances

API operation: DeregisterManagedInstance

- The following sample policy grants RAM users the permissions to deregister managed instances.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DeregisterManagedInstance"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/*"
            ]
        }
    ]
}
```

- You can specify instance IDs in the Resource list to limit the permissions to specific instances. The following sample policy grants RAM users the permissions to deregister the specified managed instances.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DeregisterManagedInstance"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/i-instancexxx00a",
                  "acs:ecs:*:*:instance/i-instancexxx00b"
            ]
        }
    ]
}
```

Permissions to query managed instances

API operation: DescribeManagedInstances

- The following sample policy grants RAM users the permissions to query managed instances.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeManagedInstances"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/*"
            ]
        }
    ]
}
```

- You can specify instance IDs in the Resource list to limit the permissions to specific managed instances. The following sample policy grants RAM users the permissions to query the specified managed instances.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeManagedInstances"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/i-instancexxx00a",
                  "acs:ecs:*:*:instance/i-instancexxx00b"
            ]
        }
    ]
}
```

Permissions to create activation codes

API operation: CreateActivation

The following sample policy grants RAM users the permissions to create activation codes and use them to register servers that are not provided by Alibaba Cloud as Alibaba Cloud managed instances.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:CreateActivation"
            ],
            "Resource": [
                "acs:ecs:*:*:activation/*"
            ]
        }
    ]
}
```

Permissions to disable activation codes

API operation: DisableActivation

- The following sample policy grants RAM users the permissions to disable any activation code that is used to register an Alibaba Cloud managed instance.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DisableActivation"
            ],
            "Resource": [
                "acs:ecs:*:*:activation/*"
            ]
        }
    ]
}
```

- You can specify instance IDs in the Resource list to limit the permissions to specific instances. The following sample policy grants RAM users the permissions to disable the activation codes of the specified managed instances.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DisableActivation"
            ],
            "Resource": [
                "acs:ecs:*:*:activation/*****-*****A",
                  "acs:ecs:*:*:activation/*****-*****B"
            ]
        }
    ]
}
```

Permissions to query activation codes

API operation: DescribeActivations

- The following sample policy grants RAM users the permissions to query the created activation codes and their usage.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeActivations"
            ],
            "Resource": [
                "acs:ecs:*:*:activation/*"
            ]
        }
    ]
}
```

- You can specify instance IDs in the Resource list to limit the permissions to specific instances. The following sample policy grants RAM users the permissions to query activation codes of the specified managed instances and their usage.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeActivations"
            ],
            "Resource": [
                "acs:ecs:*:*:activation/*****-*****A",
                  "acs:ecs:*:*:activation/*****-*****B"
            ]
        }
    ]
}
```

Permissions to delete activation codes

API operation: DeleteActivation

- The following sample policy grants RAM users the permissions to delete the activation codes that are not used.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DeleteActivation"
            ],
            "Resource": [
                "acs:ecs:*:*:activation/*"
            ]
        }
    ]
}
```

- You can specify instance IDs in the Resource list to limit the permissions to specific instances. The following sample policy grants RAM users the permissions to delete the activation codes that are not used of the specified managed instances.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DeleteActivation"
            ],
            "Resource": [
                "acs:ecs:*:*:activation/*****-*****A",
                  "acs:ecs:*:*:activation/*****-*****B"
            ]
        }
    ]
}
```

4.5.7. Run Cloud Assistant commands as a regular user

The best practice in permission management is to run commands based on the least privilege principle. We recommend that you run Cloud Assistant commands as a regular user. This topic describes how to configure access control for RAM users to run Cloud Assistant commands as regular users.

Prerequisites

Regular users are created for the ECS instance. In this topic, regular users user01 and user02 are used.

Context

When you run a Cloud Assistant command, the command is run based on the highest level of permissions on the ECS instance if you do not configure the specified permission. For example, Cloud Assistant commands are run by the root user on Linux instances and by the system user on Windows instances.

For information security, you may need to forbid the use of the root or system user in ECS instances. In this case, you can use a RAM user and configure a permission policy to forbid the root or system user to run Cloud Assistant commands on ECS instances, and allow a specific user (such as user01 and user02) to run the Cloud Assistant commands on the ECS instances.

Run Cloud Assistant commands on Linux instances as a regular user

To run Cloud Assistant commands only on Linux instances, you can perform the following operations to limit a RAM user from running Cloud Assistant commands as the root user.

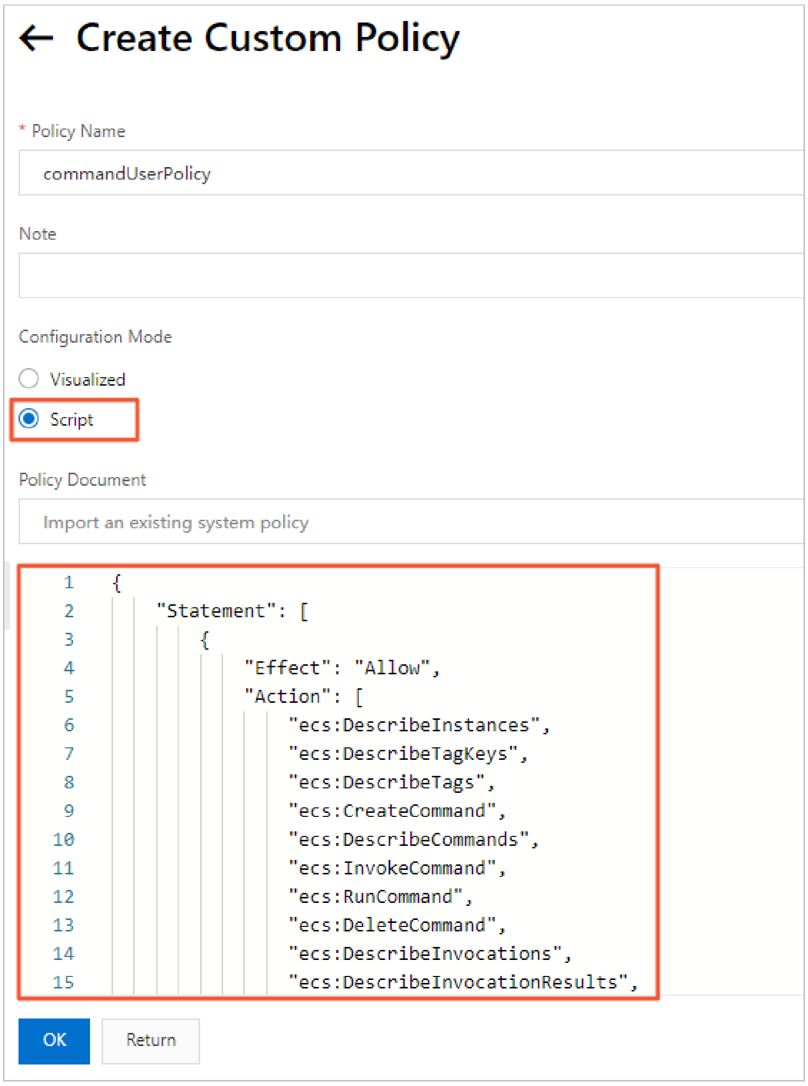
1. Log on to the RAM console by using your Alibaba Cloud account.
2. Create a RAM user. For more information, see Create a RAM user.

   The following table shows a configuration example.

Parameter	Example
Logon Name	commandUser
Display Name	commandUser
Access Mode	You can use Cloud Assistant by using the Alibaba Cloud Management Console or by calling API operations. In this example, select **Console Access** and **Programmatic Access**. **Note** You can select an access mode based on your actual usage to implement least privilege-based management.
Console Password	Select **Automatically Generate Default Password**.
Password Reset	Select **Required at Next Logon**.
Multi-factor Authentication	Select **Not Required**.

   After you have created the RAM user, you must keep the username, password, and AccessKey pair of the RAM user.

3. Create a Cloud Assistant permission policy. For more information, see Create a custom policy.



```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeInstances",
                "ecs:DescribeTagKeys",
                "ecs:DescribeTags",
                "ecs:CreateCommand",
                "ecs:DescribeCommands",
                "ecs:InvokeCommand",
                "ecs:RunCommand",
                "ecs:DeleteCommand",
                "ecs:DescribeInvocations",
                "ecs:DescribeInvocationResults",
```

Create a commandUserPolicy policy to limit users from running Cloud Assistant commands on the ECS instance. The following section shows the example policies. You can modify them based on your needs.

- RAM permission policy that allows some regular users (such as user01 and user02) to run Cloud Assistant commands on the ECS instance:

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeInstances",
                "ecs:DescribeTagKeys",
                "ecs:DescribeTags",
                "ecs:CreateCommand",
                "ecs:DescribeCommands",
                "ecs:InvokeCommand",
                "ecs:RunCommand",
                "ecs:DeleteCommand",
                "ecs:DescribeInvocations",
                "ecs:DescribeInvocationResults",
                "ecs:StopInvocation",
                "ecs:DescribeCloudAssistantStatus",
                "ecs:InstallCloudAssistant"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/*",
                "acs:ecs:*:*:command/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ecs:CommandRunAs": [
                        "user01",
                        "user02"
                    ]
                }
            }
        }
    ],
    "Version": "1"
}
```

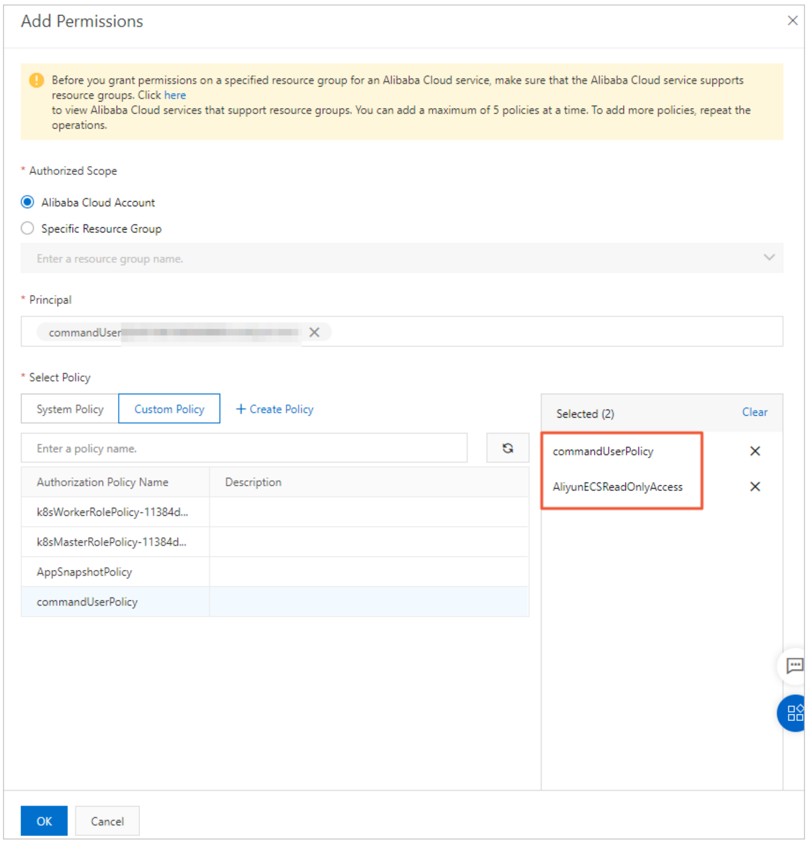
> **Note** If you want to allow other users, you can modify the username or add usernames in the Condition parameter.

- RAM permission policy that forbids some users (such as the root or system user) to run Cloud Assistant commands on the ECS instance:

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeInstances",
                "ecs:DescribeTagKeys",
                "ecs:DescribeTags",
                "ecs:CreateCommand",
                "ecs:DescribeCommands",
                "ecs:InvokeCommand",
                "ecs:RunCommand",
                "ecs:DeleteCommand",
                "ecs:DescribeInvocations",
                "ecs:DescribeInvocationResults",
                "ecs:StopInvocation",
                "ecs:DescribeCloudAssistantStatus",
                "ecs:InstallCloudAssistant"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/*",
                "acs:ecs:*:*:command/*"
            ],
            "Condition": {
                "StringNotEqualsIgnoreCase": {
                    "ecs:CommandRunAs": [
                        "system",
                        "root"
                    ]
                }
            }
        }
    ],
    "Version": "1"
}
```

Note If you want to forbid other users, you can modify the username or add usernames in the Condition parameter.

4. Grant the ECS read-only and Cloud Assistant permissions to the RAM user. For more information, see Grant permissions to a RAM user.



Add Permissions

Before you grant permissions on a specified resource group for an Alibaba Cloud service, make sure that the Alibaba Cloud service supports resource groups. Click here to view Alibaba Cloud services that support resource groups. You can add a maximum of 5 policies at a time. To add more policies, repeat the operations.

* Authorized Scope

● Alibaba Cloud Account

○ Specific Resource Group

Enter a resource group name.

* Principal

commandUser[redacted] ×

* Select Policy

Authorization Policy Name	Description
k8sWorkerRolePolicy-11384d...	
k8sMasterRolePolicy-11384d...	
AppSnapshotPolicy	
commandUserPolicy	

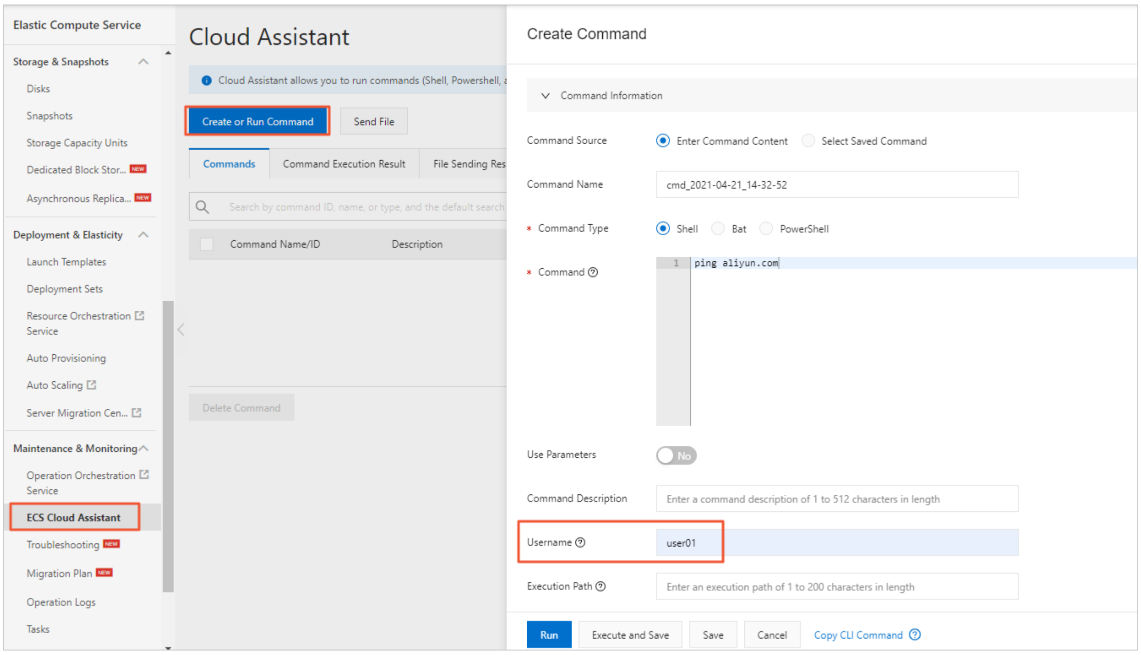
Selected (2) Clear

commandUserPolicy ×

AliyunECSReadOnlyAccess ×

- Grant the ECS read-only permission: On the **System Policy** tab, select **AliyunECSReadOnlyAccess**.
- Grant the Cloud Assistant permission: On the **Custom Policy** tab, select **commandUserPolicy** that you created in the previous step.

5. Log on to the Alibaba Cloud Management Console as the RAM user.
6. Run a Cloud Assistant command and verify the result. For more information, see Use the immediate execution feature.
   - The following figure shows the procedure by using the ECS console. You must set the Execution user parameter.



Create Command

Command Information

Command Source: ● Enter Command Content ○ Select Saved Command

Command Name: cmd_2021-04-21_14-32-52

* Command Type: ● Shell ○ Bat ○ PowerShell

* Command:

```
ping aliyun.com
```

Use Parameters: No

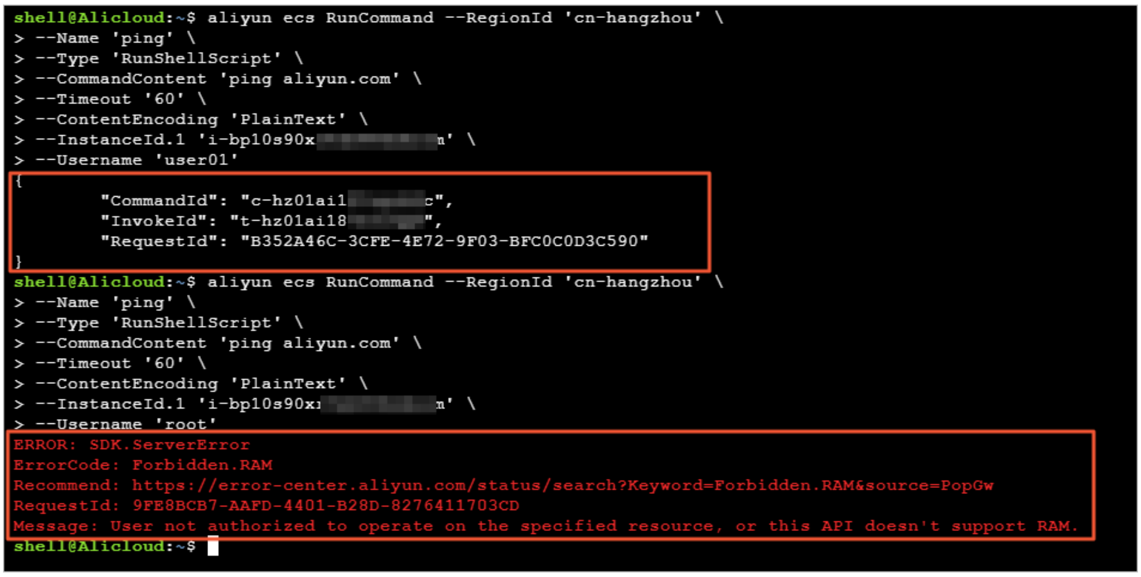
Command Description: Enter a command description of 1 to 512 characters in length

Username: user01

Execution Path: Enter an execution path of 1 to 200 characters in length

user01 is able to run the Cloud Assistant command, but an error is reported when the root user runs the command.

- The following figure shows the procedure by using the CLI. user01 is able to run the Cloud Assistant command, but an error is reported when the root user runs the command.



```
shell@Alicloud:~$ aliyun ecs RunCommand --RegionId 'cn-hangzhou' \
> --Name 'ping' \
> --Type 'RunShellScript' \
> --CommandContent 'ping aliyun.com' \
> --Timeout '60' \
> --ContentEncoding 'PlainText' \
> --InstanceId.1 'i-bp10s90x[redacted]m' \
> --Username 'user01'
{
        "CommandId": "c-hz01ai1[redacted]c",
        "InvokeId": "t-hz01ai18[redacted]",
        "RequestId": "B352A46C-3CFE-4E72-9F03-BFC0C0D3C590"
}
shell@Alicloud:~$ aliyun ecs RunCommand --RegionId 'cn-hangzhou' \
> --Name 'ping' \
> --Type 'RunShellScript' \
> --CommandContent 'ping aliyun.com' \
> --Timeout '60' \
> --ContentEncoding 'PlainText' \
> --InstanceId.1 'i-bp10s90x[redacted]m' \
> --Username 'root'
ERROR: SDK.ServerError
ErrorCode: Forbidden.RAM
Recommend: https://error-center.aliyun.com/status/search?Keyword=Forbidden.RAM&source=PopGw
RequestId: 9FE8BCB7-AAFD-4401-B28D-8276411703CD
Message: User not authorized to operate on the specified resource, or this API doesn't support RAM.
shell@Alicloud:~$
```

Run Cloud Assistant commands on Windows instances as a regular user

To run Cloud Assistant commands on Windows instances, you must provide the username and password. For data security, you must host your logon password in Operation Orchestration Service (OOS) and perform encryption by using Key Management Service (KMS). For more information, see Introduction to OOS and What is Key Management Service?

You can perform the following operations to limit a RAM user from running Cloud Assistant commands as the root or system user.

1. Log on to the RAM console by using your Alibaba Cloud account.

2. Create a RAM user. For more information, see Create a RAM user.

   The following table shows a configuration example.

Parameter	Example
Logon Name	commandUser
Display Name	commandUser
Access Mode	You can use Cloud Assistant by using the Alibaba Cloud Management Console or by calling API operations. In this example, select **Console Access** and **Programmatic Access**. ⓘ **Note** You can select an access mode based on your actual usage to implement least privilege-based management.
Console Password	Select **Automatically Generate Default Password**.
Password Reset	Select **Required at Next Logon**.
Multi-factor Authentication	Select **Not Required**.

   After you have created the RAM user, you must keep the username, password, and AccessKey pair of the RAM user.

3. Create Cloud Assistant and KMS permission policies. For more information, see Create a custom policy.

   - Cloud Assistant permission policy:

     Create a commandUserPolicy policy to limit users from running Cloud Assistant commands on the ECS instance. The following section shows the example policies. You can modify them based on your needs.

     - RAM permission policy that allows some regular users (such as user01 and user02) to run Cloud Assistant commands on the ECS instance:

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeInstances",
                "ecs:DescribeTagKeys",
                "ecs:DescribeTags",
                "ecs:CreateCommand",
                "ecs:DescribeCommands",
                "ecs:InvokeCommand",
                "ecs:RunCommand",
                "ecs:DeleteCommand",
                "ecs:DescribeInvocations",
                "ecs:DescribeInvocationResults",
                "ecs:StopInvocation",
                "ecs:DescribeCloudAssistantStatus",
                "ecs:InstallCloudAssistant"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/*",
                "acs:ecs:*:*:command/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ecs:CommandRunAs": [
                        "user01",
                        "user02"
                    ]
                }
            }
        }
    ],
    "Version": "1"
}
```

Note If you want to allow other users, you can modify the username or add usernames in the Condition parameter.

        - RAM permission policy that forbids some users (such as the root or system user) to run Cloud Assistant commands on the ECS instance:

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeInstances",
                "ecs:DescribeTagKeys",
                "ecs:DescribeTags",
                "ecs:CreateCommand",
                "ecs:DescribeCommands",
                "ecs:InvokeCommand",
                "ecs:RunCommand",
                "ecs:DeleteCommand",
                "ecs:DescribeInvocations",
                "ecs:DescribeInvocationResults",
                "ecs:StopInvocation",
                "ecs:DescribeCloudAssistantStatus",
                "ecs:InstallCloudAssistant"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/*",
                "acs:ecs:*:*:command/*"
            ],
            "Condition": {
                "StringNotEqualsIgnoreCase": {
                    "ecs:CommandRunAs": [
                        "system",
                        "root"
                    ]
                }
            }
        }
    ],
    "Version": "1"
}
```

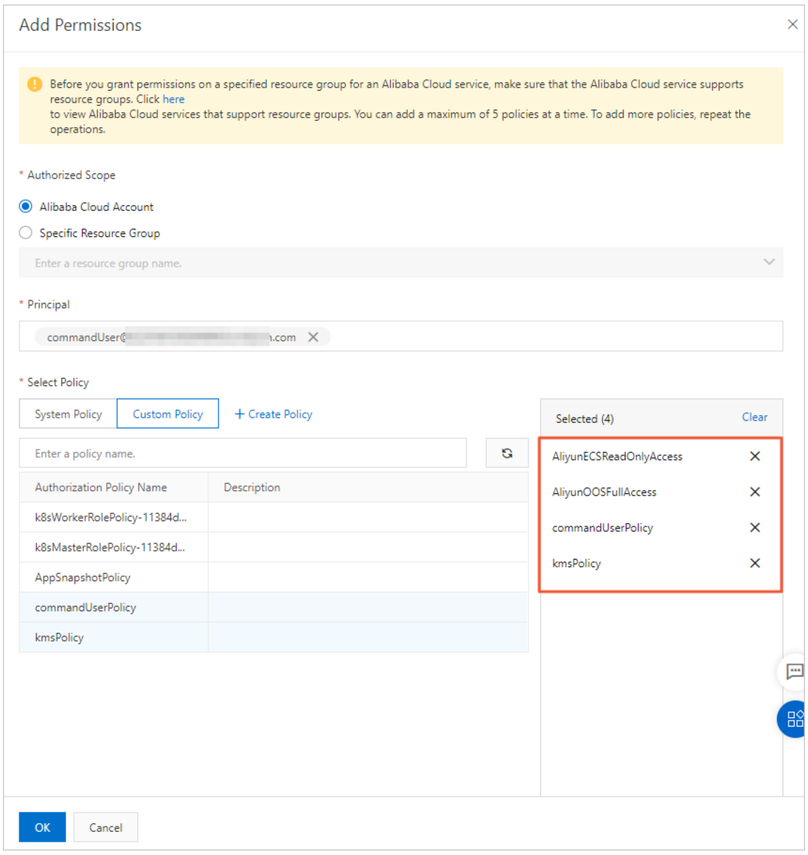
> **Note** If you want to forbid other users, you can modify the username or add usernames in the Condition parameter.

    - KMS permission policy:

      Create a kmsPolicy policy, as shown in the following example. For more information, see Examples of RAM policies.

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:List*", "kms:Describe*",
        "kms:Encrypt", "kms:Decrypt", "kms:GenerateDataKey"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

4. Grant ECS, OOS, Cloud Assistant, and KMS permissions to the RAM user. For more information, see Grant permissions to a RAM user.



Add Permissions

Before you grant permissions on a specified resource group for an Alibaba Cloud service, make sure that the Alibaba Cloud service supports resource groups. Click here
to view Alibaba Cloud services that support resource groups. You can add a maximum of 5 policies at a time. To add more policies, repeat the operations.

* Authorized Scope

● Alibaba Cloud Account

○ Specific Resource Group

Enter a resource group name.

* Principal

commandUser@[redacted].com

* Select Policy

System Policy | Custom Policy | + Create Policy

Enter a policy name.

Authorization Policy Name	Description
k8sWorkerRolePolicy-11384d...	
k8sMasterRolePolicy-11384d...	
AppSnapshotPolicy	
commandUserPolicy	
kmsPolicy	

Selected (4) Clear

- AliyunECSReadOnlyAccess
- AliyunOOSFullAccess
- commandUserPolicy
- kmsPolicy

- Grant the ECS read-only permission: On the **System Policy** tab, select **AliyunECSReadOnlyAccess**.
- Grant the OOS read-only permission: On the **System Policy** tab, select **AliyunOOSReadOnlyAccess**.
- Grant the Cloud Assistant permission: On the **Custom Policy** tab, select **commandUserPolicy** that you created in the previous step.
- Grant the KMS permission: On the **Custom Policy** tab, select **kmsPolicy** that you created in the previous step.

5. Configure a RAM role for the Windows instance.
   i. Create a RAM policy. For more information, see Create a custom policy.

      Example:

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "kms:GetSecretValue"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "oos:GetSecretParameter"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

   ii. Create a RAM role. For more information, see Create a RAM role for a trusted Alibaba Cloud service.

      The following table shows a configuration example.

Parameter	Example
Trusted entity type	Select **Alibaba Cloud Service**.
Role Type	Select **Normal Service Role**.
RAM Role Name	AxtSecretRamRole
Select Trusted Service	Select **Elastic Compute Service** from the drop-down list.

   iii. Grant permissions to the RAM role. For more information, see Grant permissions to a RAM role.

   iv. Configure the RAM role for the ECS instance. For more information, see Attach an instance RAM role to an ECS instance.

6. Create encryption parameters in OOS to manage the logon passwords for Windows instances.

   > **Note** The encryption parameters must be located within the same region as the ECS instance. Otherwise, the logon password of the ECS instance cannot be hosted in OOS.

   The following table shows an example of configuring the password of user01.

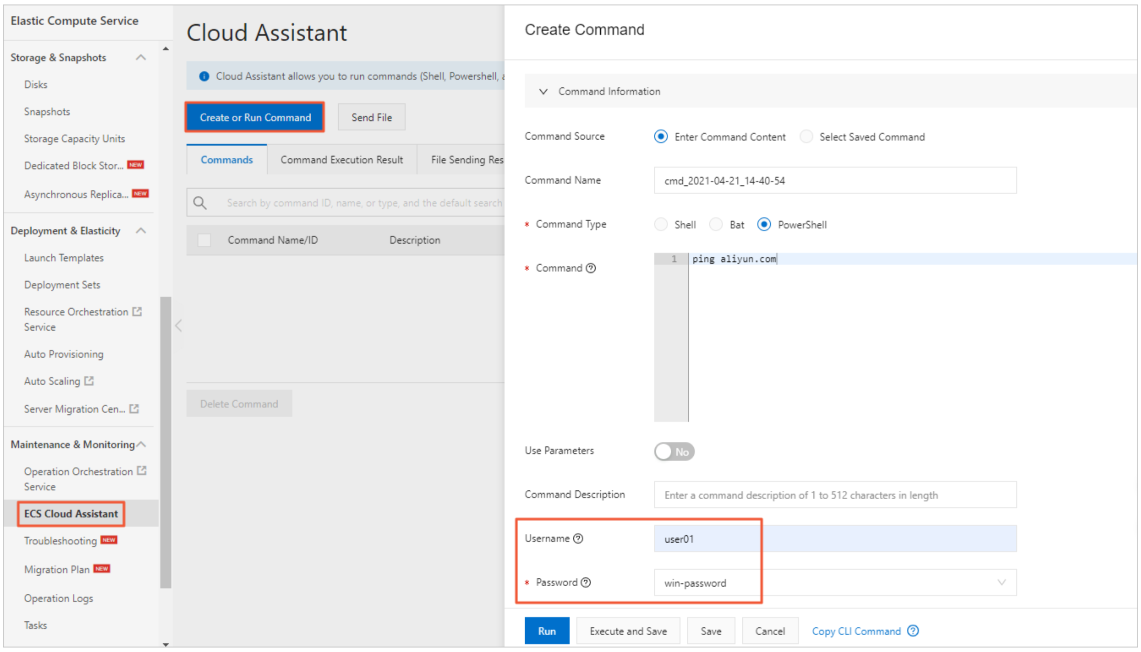
Parameter	Example
Parameter Name	axtSecretPassword

Parameter	Example
KMS Key ID	Select **Default Service CMK**.
Value	The logon password of the Windows instance. In this example, enter the logon password of user01.

7. Log on to the Alibaba Cloud Management Console as the RAM user.
8. Run a Cloud Assistant command and verify the result. For more information, see Use the immediate execution feature.

   Run the Cloud Assistant command on the Windows instance and verify whether the permission settings have taken effect.

   - The following figure shows the procedure by using the ECS console. You must set the Execution user and Password name parameters.

     Create Command

     Command Information

     Command Source: ● Enter Command Content ○ Select Saved Command

     Command Name: cmd_2021-04-21_14-40-54

     * Command Type: ○ Shell ○ Bat ● PowerShell

     * Command:

     ```
     ping aliyun.com
     ```

     Use Parameters: No

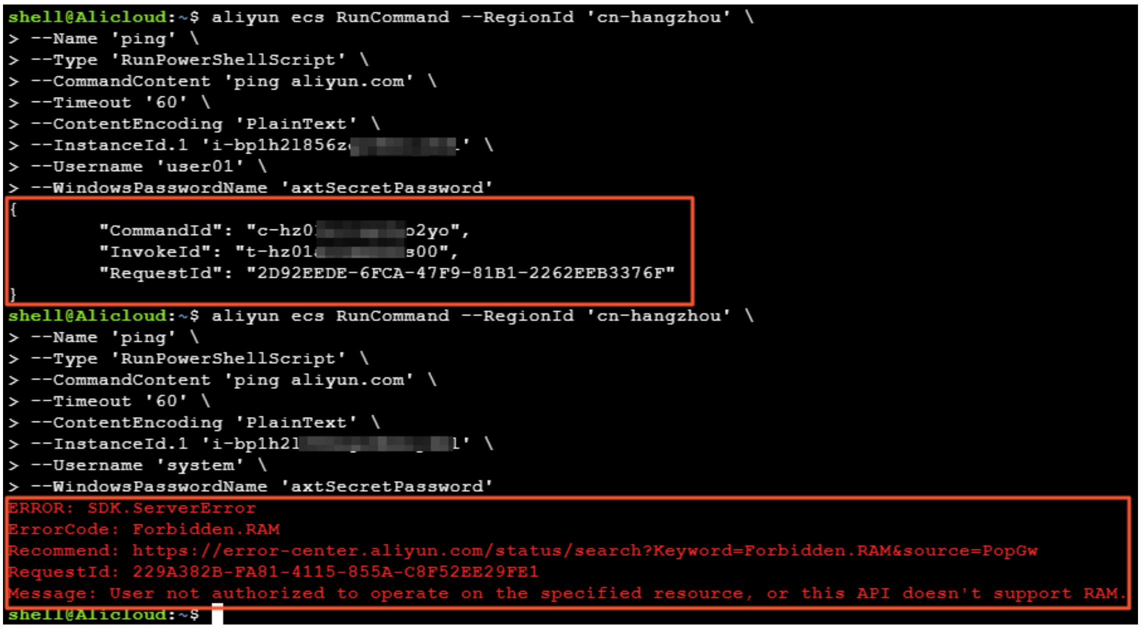
     Command Description: Enter a command description of 1 to 512 characters in length

     Username: user01

     * Password: win-password

     user01 is able to run the Cloud Assistant command, but an error is reported when the system user runs the command.

   - The following figure shows the procedure by using the CLI. user01 is able to run the Cloud Assistant command, but an error is reported when the system user runs the command.



```
shell@Alicloud:~$ aliyun ecs RunCommand --RegionId 'cn-hangzhou' \
> --Name 'ping' \
> --Type 'RunPowerShellScript' \
> --CommandContent 'ping aliyun.com' \
> --Timeout '60' \
> --ContentEncoding 'PlainText' \
> --InstanceId.1 'i-bp1h21856z[redacted]' \
> --Username 'user01' \
> --WindowsPasswordName 'axtSecretPassword'
{
        "CommandId": "c-hz0[redacted]o2yo",
        "InvokeId": "t-hz01[redacted]s00",
        "RequestId": "2D92EEDE-6FCA-47F9-81B1-2262EEB3376F"
}
shell@Alicloud:~$ aliyun ecs RunCommand --RegionId 'cn-hangzhou' \
> --Name 'ping' \
> --Type 'RunPowerShellScript' \
> --CommandContent 'ping aliyun.com' \
> --Timeout '60' \
> --ContentEncoding 'PlainText' \
> --InstanceId.1 'i-bp1h21[redacted]1' \
> --Username 'system' \
> --WindowsPasswordName 'axtSecretPassword'
ERROR: SDK.ServerError
ErrorCode: Forbidden.RAM
Recommend: https://error-center.aliyun.com/status/search?Keyword=Forbidden.RAM&source=PopGw
RequestId: 229A382B-FA81-4115-855A-C8F52EE29FE1
Message: User not authorized to operate on the specified resource, or this API doesn't support RAM.
shell@Alicloud:~$
```

4.5.8. Use OOS Parameter Store in Cloud Assistant commands

You can use custom parameters in Cloud Assistant commands to write scripts and improve the reusability of commands. Operation Orchestration Service (OOS) provides the Parameter Store feature that allows you to configure common parameters and encryption parameters. You can use the Parameter Store feature of OOS in Cloud Assistant commands to manage custom parameters.

Prerequisites

- The Elastic Compute Service (ECS) instance on which you want to run Cloud Assistant commands meets the following requirements:
  - The instance is in the **Running** (`Running`) state.
  - The instance has the Cloud Assistant client installed. For more information, see Install the Cloud Assistant client.
- OOS is activated. For more information, see Introduction to OOS.
- Key Management Service (KMS) is activated if you want to use encryption parameters. For more information, see What is Key Management Service?

Context

You can use `{{`*parameterName*`}}` to indicate a custom parameter in Cloud Assistant commands. For example, you can run the `adduser {{username}}` command to add a username for a Linux instance. In this command, *username* indicates a custom parameter. You can specify its value in the Parameters parameter of RunCommand or InvokeCommand.

You can reference parameters in OOS Parameter Store to use them for a variety of purposes. Parameters in Parameter Store are classified into common parameters and encryption parameters. Cloud Assistant uses `{{oos:}}` to define common parameters and uses `{{oos-secret:}}` to define encryption parameters.

- We recommend that you use common parameters to store non-sensitive data. For more information, see Use common parameters in Cloud Assistant commands.

- We recommend that you use encryption parameters to store sensitive data such as passwords. For more information, see Use encryption parameters in Cloud Assistant commands.

Use common parameters in Cloud Assistant commands

If you run a Cloud Assistant command as a RAM user, you must attach a policy to the RAM user. For more information, see Create a custom policy and Grant permissions to a RAM user. RAM users must have the API permissions from Cloud Assistant and OOS Parameter Store to run Cloud Assistant commands by using common parameters. The following code provides an example on the policy to attach to the RAM user.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeInstances",
                "ecs:DescribeTagKeys",
                "ecs:DescribeTags",
                "ecs:CreateCommand",
                "ecs:DescribeCommands",
                "ecs:InvokeCommand",
                "ecs:RunCommand",
                "ecs:DeleteCommand",
                "ecs:DescribeInvocations",
                "ecs:DescribeInvocationResults",
                "ecs:StopInvocation",
                "ecs:DescribeCloudAssistantStatus",
                "ecs:InstallCloudAssistant",
                "oos:GetParameters",
                "oos:GetParameter"
            ],
            "Resource": "*"
        }
    ],
    "Version": "1"
}
```

If your command does not involve sensitive data, you can use common parameters. This section describes how to use common parameters of OOS Parameter Store in a Cloud Assistant command. In the example, a user is added to a Linux instance.

1. Create common parameters by using OOS Parameter Store.

   The following table provides an example of adding a username parameter to the common parameters. The value of the parameter is set to user01. You can change the value to suit your needs.

Parameter	Example
Parameter Name	username
Parameter Type	String

Parameter	Example
Value	user01

2. Use ECS SDK for Java to call the RunCommand operation to run a Cloud Assistant command.

   The following code provides an example on how to create a user for a Linux instance by running a Cloud Assistant command. The command content is `adduser {{oos:username}}`. In this command, `{{oos:username}}` indicates that the username is specified by the username parameter.

```
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.ecs.model.v20140526.RunCommandRequest;
import com.aliyuncs.ecs.model.v20140526.RunCommandResponse;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
import com.aliyuncs.profile.DefaultProfile;
import com.google.gson.Gson;
import java.util.ArrayList;
import java.util.List;
public class addUserName {
    public static void main(String[] args) {
        # Set the region ID and the AccessKey pair.
        DefaultProfile profile = DefaultProfile.getProfile("cn-hangzhou", "<accessKeyId
>", "<accessSecret>");
        IAcsClient client = new DefaultAcsClient(profile);
        RunCommandRequest request = new RunCommandRequest();
        # Set the region ID of the instance.
        request.setRegionId("cn-hangzhou");
        # Set the language of the Cloud Assistant command. In this example, shell is us
ed.
        request.setType("RunShellScript");
        # Set the command content. In this example, a user is added to a Linux instance
. The username parameter specifies the username of the user.
        request.setCommandContent("adduser {{oos:username}}");
        List<String> instanceIdList = new ArrayList<String>();
        # Set the ID of the instance on which to run the Cloud Assistant command.
        instanceIdList.add("i-bp1dktddjsg7oh11****");
        request.setInstanceIds(instanceIdList);
        # Set the Cloud Assistant command to support custom parameters.
        request.setEnableParameter(true);
        try {
            RunCommandResponse response = client.getAcsResponse(request);
            System.out.println(new Gson().toJson(response));
        } catch (ServerException e) {
            e.printStackTrace();
        } catch (ClientException e) {
            System.out.println("ErrCode:" + e.getErrCode());
            System.out.println("ErrMsg:" + e.getErrMsg());
            System.out.println("RequestId:" + e.getRequestId());
        }
    }
}
```

The following command output is returned:

```
{
    "requestId": "67D1BD1A-0D08-42C3-AFD9-A3397CD67CD1",
    "commandId": "c-hz01hkgs19i****",
    "invokeId": "t-hz01hkgs19s****"
}
```

3. (Optional)Check the output of the Cloud Assistant command.

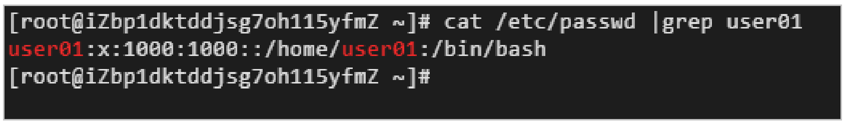
   You can log on to the ECS instance to check whether the Cloud Assistant command has taken effect. Perform the following steps to check whether user01 is added to the Linux instance:

i. Log on to the ECS instance. For more information, see Connect to a Linux instance by using a password.

ii. Run the following command to check whether user01 is added:

```
cat /etc/passwd |grep user01
```

If the following command output is returned, user01 is added.



```
[root@iZbp1dktddjsg7oh115yfmZ ~]# cat /etc/passwd |grep user01
user01:x:1000:1000::/home/user01:/bin/bash
[root@iZbp1dktddjsg7oh115yfmZ ~]#
```

Use encryption parameters in Cloud Assistant commands

If you run a Cloud Assistant command as a RAM user, you must attach a policy to the RAM user. For more information, see Create a custom policy and Grant permissions to a RAM user. RAM users must have the API permissions from Cloud Assistant, OOS Parameter Store, and KMS to run Cloud Assistant commands by using encryption parameters. The following code provides an example on the policy to attach to the RAM user.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeInstances",
                "ecs:DescribeTagKeys",
                "ecs:DescribeTags",
                "ecs:CreateCommand",
                "ecs:DescribeCommands",
                "ecs:InvokeCommand",
                "ecs:RunCommand",
                "ecs:DeleteCommand",
                "ecs:DescribeInvocations",
                "ecs:DescribeInvocationResults",
                "ecs:StopInvocation",
                "ecs:DescribeCloudAssistantStatus",
                "ecs:InstallCloudAssistant",
                "oos:GetParameters",
                "oos:GetSecretParameters",
                "oos:GetParameter",
                "oos:GetSecretParameter",
                "kms:GetSecretValue"
            ],
            "Resource": "*"
        }
    ],
    "Version": "1"
}
```

If your command involves sensitive data such as passwords used to log on to your server or database, we recommend that you use encryption parameters to improve the security of your command. This section describes how to use encryption parameters of OOS Parameter Store in a Cloud Assistant command. In the example, the password of a Linux instance user is modified.

ⓘ **Note** Before you perform the following operations, you must have created a user for the instance. For information about how to add users to Linux instances, see Use common parameters in Cloud Assistant commands.

1. Create encryption parameters and common parameters by using OSS Parameter Store.

   The following tables provide examples of creating a username parameter and a password parameter in OOS Parameter Store.

   - Add a username parameter to the common parameters. The value of the parameter is set to user01. You can change the value to suit your needs.

Parameter	Example
Parameter Name	username
Parameter Type	String
Value	user01

   - Add a password parameter to the encryption parameters. The value of the parameter is set to MyPassword01. You can change the value to suit your needs.

Parameter	Example
Parameter Name	password
KMS Key ID	Default Service CMK
Value	MyPassword01 ⓘ **Note** The password used in this example is for reference only. Do not use it in the online environment.

2. Bind a RAM role to the ECS instance.

i. Create a RAM role. For more information, see Create a RAM role for a trusted Alibaba Cloud service.

   The following table provides a configuration example.

Parameter	Example
Trusted entity type	Select **Alibaba Cloud Service**.
Role Type	Select **Normal Service Role**.
RAM Role Name	AxtParametersRamRole
Select Trusted Service	Select **Elastic Compute Service** from the drop-down list.

ii. Create a policy for the RAM role. For more information, see Create a custom policy.

   The policy name is AxtParametersRamPolicy. The following code shows the policy content. The policy allows calls to the following KMS and OOS API operations: GetSecretValue, GetParameters, GetSecretParameters, GetParameter, and GetSecretParameter.

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "kms:GetSecretValue"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "oos:GetParameters",
                "oos:GetSecretParameters",
                "oos:GetParameter",
                "oos:GetSecretParameter"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

iii. Attach the AxtParametersRamPolicy policy to the AxtParametersRamRole role. For more information, see Grant permissions to a RAM role.

iv. Bind the AxtParametersRamRole role to the ECS instance. For more information, see Attach an instance RAM role to an ECS instance.

3. Use ECS SDK for Java to call the RunCommand operation to run a Cloud Assistant command.

   The following example describes how to modify the password for a Linux instance user by running a Cloud Assistant command. The following code shows the command content:

```
echo '{{oos-secret:password}}' | passwd '{{oos:username}}' --stdin"
```

   In this command, `{{oos-secret:password}}` indicates that the new password is specified by the password parameter. `{{oos:username}}` indicates that the username is specified by the username parameter.

```
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.ecs.model.v20140526.RunCommandRequest;
import com.aliyuncs.ecs.model.v20140526.RunCommandResponse;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
import com.aliyuncs.profile.DefaultProfile;
import com.google.gson.Gson;
import java.util.ArrayList;
import java.util.List;
public class changePassword {
    public static void main(String[] args) {
        # Set the region ID and the AccessKey pair.
        DefaultProfile profile = DefaultProfile.getProfile("cn-hangzhou", "<accessKeyId
>", "<accessSecret>");
        IAcsClient client = new DefaultAcsClient(profile);
        RunCommandRequest request = new RunCommandRequest();
        # Set the region ID of the instance.
        request.setRegionId("cn-hangzhou");
        # Set the language of the Cloud Assistant command. In this example, shell is us
ed.
        request.setType("RunShellScript");
        # In this example, the password of the Linux instance user is modified. The use
rname is specified by the username parameter and the password is specified by the passw
ord parameter.
        request.setCommandContent(
                "echo '{{oos-secret:password}}' | passwd '{{oos:username}}' --stdin");
        List<String> instanceIdList = new ArrayList<String>();
        instanceIdList.add("i-bp1dktddjsg7oh11****");
        request.setInstanceIds(instanceIdList);
        request.setEnableParameter(true);
        try {
            RunCommandResponse response = client.getAcsResponse(request);
            System.out.println(new Gson().toJson(response));
        } catch (ServerException e) {
            e.printStackTrace();
        } catch (ClientException e) {
            System.out.println("ErrCode:" + e.getErrCode());
            System.out.println("ErrMsg:" + e.getErrMsg());
            System.out.println("RequestId:" + e.getRequestId());
        }
    }
}
```

The following command output is returned:

```
{
    "requestId": "C73D7B90-6503-4DB4-844C-9412AC55ECC5",
    "commandId": "c-hz01hnyd4e8****",
    "invokeId": "t-hz01hnyd4ed****"
}
```

4. (Optional)Check the output of the Cloud Assistant command.

   You can log on to the ECS instance by using the new password to check whether the Cloud Assistant command has taken effect. For more information, see Connect to a Linux instance by using a password.

4.5.9. Run Cloud Assistant commands and restart ECS instances

If you want to restart an Elastic Compute Service (ECS) instance after you run a Cloud Assistant command on the instance, we recommend that you do not add the **reboot** or **shutdown** operation to the Cloud Assistant command. Otherwise, Cloud Assistant cannot report the command execution results and the command is in an abnormal state. This topic describes how to call API operations and use Operation Orchestration Service (OOS) to batch run Cloud Assistant commands and restart ECS instances. You can choose an appropriate method based on your needs.

Call API operations to batch run Cloud Assistant commands and restart instances

Alibaba Cloud provides a variety of API operations for you to manage your cloud resources. This section describes how to run Python code to call API operations in an on-premises Linux environment to batch run Cloud Assistant commands and restart instances.

1. Prepare information required to run Cloud Assistant commands.

   i. Obtain an AccessKey pair.

      We recommend that you obtain the AccessKey pair of a RAM user. For more information, see Obtain an AccessKey pair.

   ii. Obtain the region ID of the instances on which you want to run the commands.

      You can call the DescribeRegions operation to query the most recent region list. For information about parameters in DescribeRegions, see DescribeRegions.

   iii. Obtain the IDs of the instances on which you want to run the commands.

      You can call the DescribeInstances operation to query the list of instances that meet specific filter conditions. For example, you can query the list of instances that are in the Running state or have specific tags added. For information about parameters in DescribeInstances, see DescribeInstances.

2. Configure the on-premises environment and run the sample code.

   i. Install Alibaba Cloud ECS SDK for Python.

      ```
      sudo pip install aliyun-python-sdk-ecs
      ```

   ii. Upgrade ECS SDK for Python to the latest version.

      ```
      sudo pip install --upgrade aliyun-python-sdk-ecs
      ```

   iii. Create a *.py* file and write the following sample code to the file.

      - Replace <yourAccessKey ID> in `access_key = '<yourAccessKey ID>'` with the AccessKey ID obtained in the preceding step.
      - Replace <yourAccessKey Secret> in `access_key_secret = '<yourAccessKey Secret>'` with the AccessKey secret obtained in the preceding step.

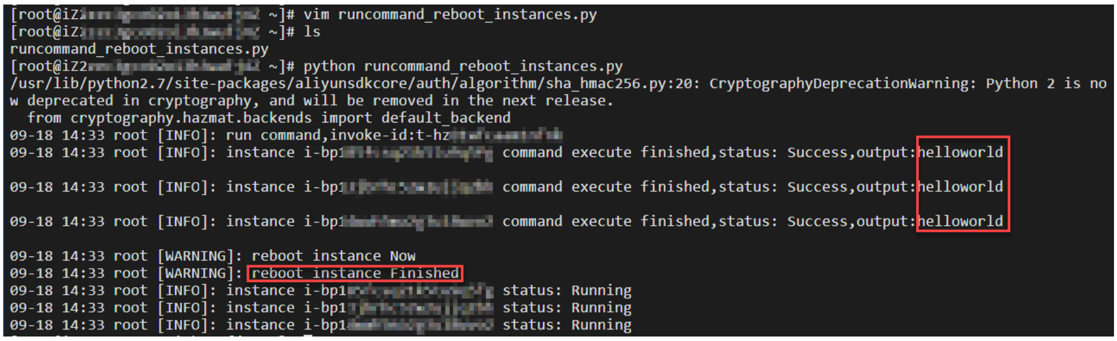
- Replace <yourRegionId> in `region_id = '<yourRegionId>'` with the region ID obtained in the preceding step.
- Specify the instance IDs obtained in the preceding step in the specified format. Example: `ins_ids= ["i-bp185fcs****","i-bp14wwh****","i-bp13jbr****"]` .

Sample code:

```
# coding=utf-8
# If the Python sdk is not installed, run 'sudo pip install aliyun-python-sdk-ecs'.
# Make sure you're using the latest sdk version.
# Run 'sudo pip install --upgrade aliyun-python-sdk-ecs' to upgrade.
import json
import sys
import base64
import time
import logging
from aliyunsdkcore.client import AcsClient
from aliyunsdkcore.acs_exception.exceptions import ClientException
from aliyunsdkcore.acs_exception.exceptions import ServerException
from aliyunsdkecs.request.v20140526.RunCommandRequest import RunCommandRequest
from aliyunsdkecs.request.v20140526.DescribeInvocationResultsRequest import DescribeInvocationResultsRequest
from aliyunsdkecs.request.v20140526.RebootInstancesRequest import RebootInstancesRequest
from aliyunsdkecs.request.v20140526.DescribeInstancesRequest import DescribeInstancesRequest
# Configure the log output formatter
logging.basicConfig(level=logging.INFO,
                    format="%(asctime)s %(name)s [%(levelname)s]: %(message)s",
                    datefmt='%m-%d %H:%M')
logger = logging.getLogger()
access_key = '<yourAccessKey ID>'  # The AccessKey ID you obtained.
access_key_secret = '<yourAccessKey Secret>'  # The AccessKey secret you obtained.
region_id = '<yourRegionId>'  # The region ID you obtained.
client = AcsClient(access_key, access_key_secret, region_id)
def base64_decode(content, code='utf-8'):
    if sys.version_info.major == 2:
        return base64.b64decode(content)
    else:
        return base64.b64decode(content).decode(code)
def get_invoke_result(invoke_id):
    request = DescribeInvocationResultsRequest()
    request.set_accept_format('json')
    request.set_InvokeId(invoke_id)
    response = client.do_action_with_exception(request)
    response_details = json.loads(response)["Invocation"]["InvocationResults"]["InvocationResult"]
    dict_res = { detail.get("InstanceId",""):{"status": detail.get("InvocationStatus",""),"output":base64_decode(detail.get("Output",""))}  for detail in response_details }
    return dict_res
def get_instances_status(instance_ids):
    request = DescribeInstancesRequest()
    request.set_accept_format('json')
    request.set_InstanceIds(instance_ids)
    response = client.do_action_with_exception(request)
    response_details = json.loads(response)["Instances"]["Instance"]
    dict_res = { detail.get("InstanceId",""):{"status":detail.get("Status","")} for
detail in response_details }
    return dict_res
def run_command(cmdtype,cmdcontent,instance_ids,timeout=60):
    """
    cmdtype: the command type, which can be RunBatScript, RunPowerShellScript, or R
unShellScript.
    cmdcontent: the command content.
    instance_ids: the IDs of the instances on which you want to run the command.
    """
    try:
        request = RunCommandRequest()
        request.set_accept_format('json')
        request.set_Type(cmdtype)
        request.set_CommandContent(cmdcontent)
        request.set_InstanceIds(instance_ids)
        # The timeout period for running the command. Unit: seconds. Default value:
60. Specify this parameter based on the command that you want to run.
        request.set_Timeout(timeout)
        response = client.do_action_with_exception(request)
        invoke_id = json.loads(response).get("InvokeId")
        return invoke_id
    except Exception as e:
        logger.error("run command failed")
def reboot_instances(instance_ids,Force=False):
    """
    instance_ids: the IDs of the instances that you want to restart.
    Force: specifies whether to forcibly restart the instances. Default value: Fals
e.
    """
    request = RebootInstancesRequest()
    request.set_accept_format('json')
    request.set_InstanceIds(instance_ids)
    request.set_ForceReboot(Force)
    response = client.do_action_with_exception(request)
def wait_invoke_finished_get_out(invoke_id,wait_count,wait_interval):
    for i in range(wait_count):
        result = get_invoke_result(invoke_id)
        if set([res["status"] for _,res in result.items()]) & set(["Running","Pendi
ng","Stopping"]):
            time.sleep(wait_interval)
        else:
            return result
    return result
def wait_instance_reboot_ready(ins_ids,wait_count,wait_interval):
    for i in range(wait_count):
        result = get_instances_status(ins_ids)
        if set([res["status"] for _,res in result.items()]) != set(["Running"]):
            time.sleep(wait_interval)
        else:
            return result
    return result
def run_task():
    # Specify the type of the command.
    cmdtype = "RunShellScript"
    # Specify the content of the command.
    cmdcontent = """
    #!/bin/bash
    echo helloworld
    """
    # Specify the timeout period.
    timeout = 60
    # Specify the IDs of the instances on which you want to run the command. After
the command is run on these instances, these instances are restarted.
    ins_ids= ["i-bp185fcs****","i-bp14wwh****","i-bp13jbr****"]
    # Run the command.
    invoke_id = run_command(cmdtype,cmdcontent,ins_ids,timeout)
    logger.info("run command,invoke-id:%s" % invoke_id)
    # Wait for the command to finishing running. Query the command running state 10
times at an interval of 5 seconds. Specify the number of queries and the query inte
rval based on the actual requirements.
    invoke_result = wait_invoke_finished_get_out(invoke_id,10,5)
    for ins_id,res in invoke_result.items():
        logger.info("instance %s command execute finished,status: %s,output:%s" %(i
ns_id,res["status"],res["output"]))
    # Restart the instances.
    logger.warn("reboot instance Now")
    reboot_instances(ins_ids)
    time.sleep(5)
    # Wait for the instances to enter the Running state. Query the instance states
30 times at an interval of 10 seconds.
    reboot_result = wait_instance_reboot_ready(ins_ids,30,10)
    logger.warn("reboot instance Finished")
    for ins_id,res in reboot_result.items():
        logger.info("instance %s status: %s" %(ins_id,res["status"]))
if __name__ == '__main__':
    run_task()
```

iv. Run the *.py* file.

The following figure shows a sample result of running the .py file. In this example, a command is run on three instances to obtain `helloworld` and the three instances are then restarted.



```
[root@iZ[redacted] ~]# vim runcommand_reboot_instances.py
[root@iZ[redacted] ~]# ls
runcommand_reboot_instances.py
[root@iZ2[redacted] ~]# python runcommand_reboot_instances.py
/usr/lib/python2.7/site-packages/aliyunsdkcore/auth/algorithm/sha_hmac256.py:20: CryptographyDeprecationWarning: Python 2 is no
w deprecated in cryptography, and will be removed in the next release.
  from cryptography.hazmat.backends import default_backend
09-18 14:33 root [INFO]: run command,invoke-id:t-hz[redacted]
09-18 14:33 root [INFO]: instance i-bp1[redacted] command execute finished,status: Success,output:helloworld

09-18 14:33 root [INFO]: instance i-bp1[redacted] command execute finished,status: Success,output:helloworld

09-18 14:33 root [INFO]: instance i-bp1[redacted] command execute finished,status: Success,output:helloworld

09-18 14:33 root [WARNING]: reboot instance Now
09-18 14:33 root [WARNING]: reboot instance Finished
09-18 14:33 root [INFO]: instance i-bp1[redacted] status: Running
09-18 14:33 root [INFO]: instance i-bp1[redacted] status: Running
09-18 14:33 root [INFO]: instance i-bp1[redacted] status: Running
```

Use OOS to batch run Cloud Assistant commands and restart instances

OOS is an automated O&M service provided by Alibaba Cloud. You can use OOS templates to customize and execute O&M tasks.

1. Go to the Create Template page.
   i. Log on to the OOS console.
   ii. In the left-side navigation pane, click **My Templates**.
   iii. On the My Templates page, click **Create Template**.
2. Configure parameters on the Create Template page.
   i. Enter a template name in the Template Name field. Example: `runcommand_reboot_instances` .
   ii. Click the **YAML** tab and enter the following code:

```
FormatVersion: OOS-2019-06-01
Description:
  en: Bulky run command on ECS instances and reboot instance.
  name-en: ACS-ECS-BulkyRunCommandRboot
  categories:
    - run_command
Parameters:
  regionId:
    Type: String
    Description:
      en: The id of region
    Label:
      en: Region
    AssociationProperty: RegionId
    Default: '{{ ACS::RegionId }}'
  targets:
    Type: Json
    Label:
      en: TargetInstance
    AssociationProperty: Targets
    AssociationPropertyMetadata:
      ResourceType: ALIYUN::ECS::Instance
      RegionId: regionId
  commandType:
    Description:
      en: The type of command
    Label:
      en: CommandType
    Type: String
    AllowedValues:
      - RunBatScript
      - RunPowerShellScript
      - RunShellScript
    Default: RunShellScript
  commandContent:
    Description:
      en: Command content to run in ECS instance
    Label:
      en: CommandContent
    Type: String
    MaxLength: 16384
    AssociationProperty: Code
    Default: echo hello
  workingDir:
    Description:
      en: 'The directory where the created command runs on the ECS instances.Linux
instances: under the home directory of the administrator (root user): /root.Windows
instances: under the directory where the process of the Cloud Assistant client is l
ocated, such asC:\Windows\System32.'
    Label:
      en: WorkingDir
    Type: String
    Default: ''
  timeout:
    Description:
      en: The value of the invocation timeout period of a command on ECS instances
    Label:
      en: Timeout
    Type: Number
    Default: 600
  enableParameter:
    Description:
      en: Whether to include secret parameters or custom parameters in the command
    Label:
      en: EnableParameter
    Type: Boolean
    Default: false
  username:
    Description:
      en: The username that is used to run the command on the ECS instance
    Label:
      en: Username
    Type: String
    Default: ''
  windowsPasswordName:
    Description:
      en: The name of the password used to run the command on a Windows instance
    Label:
      en: WindowsPasswordName
    Type: String
    Default: ''
    AssociationProperty: SecretParameterName
  rateControl:
    Description:
      en: Concurrency ratio of task execution
    Label:
      en: RateControl
    Type: Json
    AssociationProperty: RateControl
    Default:
      Mode: Concurrency
      MaxErrors: 0
      Concurrency: 10
  OOSAssumeRole:
    Description:
      en: The RAM role to be assumed by OOS
    Label:
      en: OOSAssumeRole
    Type: String
    Default: OOSServiceRole
RamRole: '{{ OOSAssumeRole }}'
Tasks:
  - Name: getInstance
    Description:
      en: Views the ECS instances.
    Action: ACS::SelectTargets
    Properties:
      ResourceType: ALIYUN::ECS::Instance
      RegionId: '{{ regionId }}'
      Filters:
        - '{{ targets }}'
    Outputs:
      instanceIds:
        Type: List
        ValueSelector: Instances.Instance[].InstanceId
  - Name: runCommand
    Action: ACS::ECS::RunCommand
    Description:
      en: Execute cloud assistant command.
    Properties:
      regionId: '{{ regionId }}'
      commandContent: '{{ commandContent }}'
      instanceId: '{{ ACS::TaskLoopItem }}'
      commandType: '{{ commandType }}'
      workingDir: '{{ workingDir }}'
      timeout: '{{ timeout }}'
      enableParameter: '{{ enableParameter }}'
      username: '{{ username }}'
      windowsPasswordName: '{{ windowsPasswordName }}'
    Loop:
      RateControl: '{{ rateControl }}'
      Items: '{{ getInstance.instanceIds }}'
      Outputs:
        commandOutputs:
          AggregateType: Fn::ListJoin
          AggregateField: commandOutput
    Outputs:
      commandOutput:
        Type: String
        ValueSelector: invocationOutput
  - Name: rebootInstance
    Action: ACS::ECS::RebootInstance
    Description:
      en: Restarts the ECS instances.
    Properties:
      regionId: '{{ regionId }}'
      instanceId: '{{ ACS::TaskLoopItem }}'
    Loop:
      RateControl: '{{ rateControl }}'
      RateControl: '{{ rateControl }}'
      Items: '{{ getInstance.instanceIds }}'
Outputs:
  instanceIds:
    Type: List
    Value: '{{ getInstance.instanceIds }}'
```

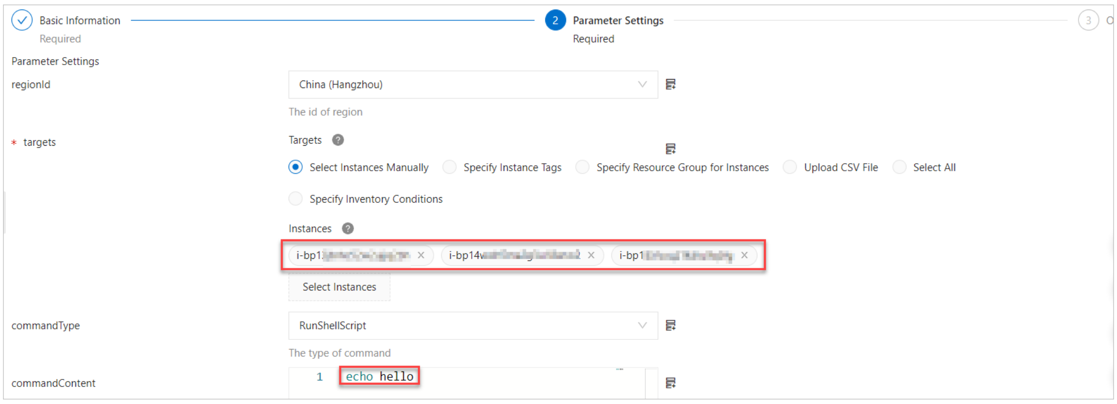
iii. Click **Create Template**.

3. Execute the template.

   i. Find the created template and click **Create Execution** in the **Actions** column.

   ii. Configure the execution.

   Complete the execution configurations step by step as instructed. In the **Parameter Settings** step, select multiple instances and use the default values for other parameters.



Parameter Settings

regionId: China (Hangzhou)
The id of region

* targets
Targets
● Select Instances Manually ○ Specify Instance Tags ○ Specify Resource Group for Instances ○ Upload CSV File ○ Select All
○ Specify Inventory Conditions
Instances
i-bp1[redacted] × i-bp14[redacted] × i-bp1[redacted] ×
Select Instances

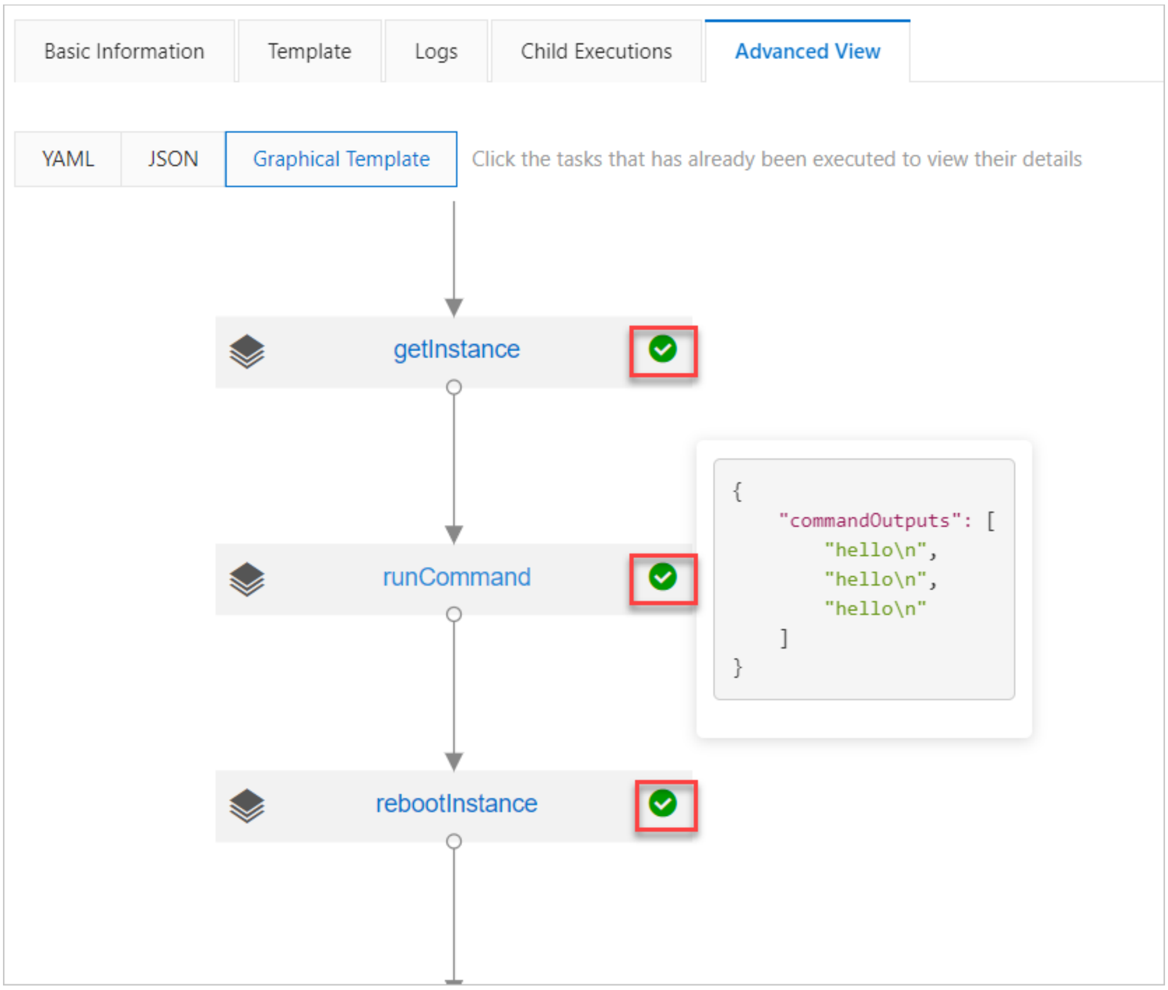
commandType: RunShellScript
The type of command

commandContent:
```
echo hello
```

   iii. In the **OK** step, click **Create**.
   After the execution is created, you are automatically directed to the **Basic Information** tab on the execution details page. If the template is executed, Success is displayed in the Execution Status section.

4. View the execution result.

   You can click the **Advanced View** tab to view the execution process and result. The following figure shows that the operations specified in the template are performed.



```
{
    "commandOutputs": [
        "hello\n",
        "hello\n",
        "hello\n"
    ]
}
```

4.6. Use the Operation Content and Result Delivery feature

The Operation Content and Result Delivery feature provided by Cloud Assistant allows you to deliver O&M task execution records to Object Storage Service (OSS) or Log Service for persistent storage. This topic describes how to configure delivery settings to deliver O&M task execution records to specified OSS buckets or Log Service Logstores and how to query delivered execution records.

Context

Cloud Assistant allows O&M task execution records to be retained but puts limits on the maximum number of execution records retained and their retention periods. For more information, see the "Cloud Assistant limits" section in Limits. If you want to retain a large number of execution records or retain execution records for an extended period of time, we recommend that you use the Operation Content and Result Delivery feature. It allows you to deliver and query O&M task execution records and perform operations on them, such as behavioral or security analysis, resource change tracking, and behavioral compliance auditing.

You can perform the following steps to use the Operation Content and Result Delivery feature:

1. Configure delivery settings. Specify a destination Log Service project and Logstore or a destination OSS bucket.

For more information, see the Configure delivery settings in the Elastic Compute Service (ECS) console section in this topic.

2. Run commands or send files. Then, the corresponding task execution records are automatically delivered to your specified Logstore or OSS bucket.

   For more information, see Use the immediate execution feature, Run a command, and Upload files to ECS instances.

3. Go to the Log Service console or OSS console to query the delivered execution records.

   For more information, see the Query O&M task execution records in the Log Service console and Query O&M task execution records in the OSS console sections in this topic.

Configure delivery settings in the Elastic Compute Service (ECS) console

1.

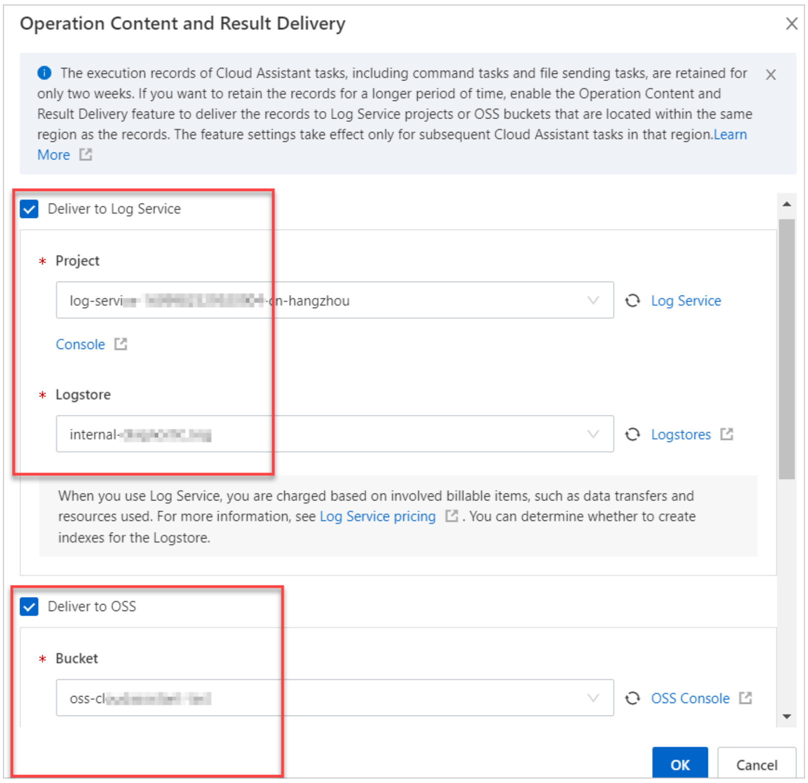
2.

3. In the upper-left corner of the top navigation bar, select a region.

   > **Note** O&M task execution records cannot be delivered across regions. To deliver O&M task execution records in multiple regions, configure delivery settings for each of these regions.

4. In the upper-right corner of the **Cloud Assistant** page, click **Operation Content and Result Delivery**.

5. In the **Operation Content and Result Delivery** dialog box, configure delivery settings.



Operation Content and Result Delivery

The execution records of Cloud Assistant tasks, including command tasks and file sending tasks, are retained for only two weeks. If you want to retain the records for a longer period of time, enable the Operation Content and Result Delivery feature to deliver the records to Log Service projects or OSS buckets that are located within the same region as the records. The feature settings take effect only for subsequent Cloud Assistant tasks in that region.Learn More

☑ Deliver to Log Service

* Project: log-servi[redacted]-cn-hangzhou

* Logstore: internal-[redacted]

When you use Log Service, you are charged based on involved billable items, such as data transfers and resources used. For more information, see Log Service pricing . You can determine whether to create indexes for the Logstore.

☑ Deliver to OSS

* Bucket: oss-cl[redacted]

> **Note** The first time you configure delivery settings, the system grants Cloud Assistant the permissions to access Log Service and OSS resources so that O&M task execution records can be delivered to your specified Logstore or OSS bucket. You can also manually manage the permissions. For more information, see Manage the service-linked role for Operation Content and Result Delivery.

i. Select **Deliver to Log Service**. Then, select a created Log Service project from the Project drop-down list and a created Logstore from the Logstore drop-down list.

   If you have not created Log Service projects or Logstores in the selected region, click **Log Service Console** or **Logstores** to create projects or Logstores in the Log Service console. After you create projects or Logstores in the selected region, go back to the Operation Content and Result Delivery dialog box and click the ⟳ icon to obtain the most recent list of projects or Logstores. For more information, see Manage a project and Manage a Logstore.

   Before you can query or analyze logs in Log Service, you must enable indexing. For more information, see Configure indexes.

   > **Notice** The Operation Content and Result Delivery dialog box feature is free to use. However, you are charged for traffic generated when you use Log Service features such as indexing. For more information, see Overview.

ii. Select **Deliver to OSS**. Then, select a created OSS bucket and specify the root directory in which to store execution records.

   If you have not created OSS buckets in the selected region, click **OSS console** to create buckets in the OSS console. After you create buckets in the selected region, go back to the Operation Content and Result Delivery dialog box and click the ⟳ icon to obtain the most recent list of buckets. For more information, see Create buckets.

   > **Notice** The Operation Content and Result Delivery dialog box feature is free to use. However, you are charged for traffic generated when you use OSS features such as object management. For more information, see Billing overview.

iii. Click **OK**.

Query O&M task execution records in the Log Service console

This section describes how to access a specified Logstore from the ECS console to query logs about delivered O&M task execution records. Alternatively, you can log on to the Log Service console and access the specified Logstore.

1.

2.

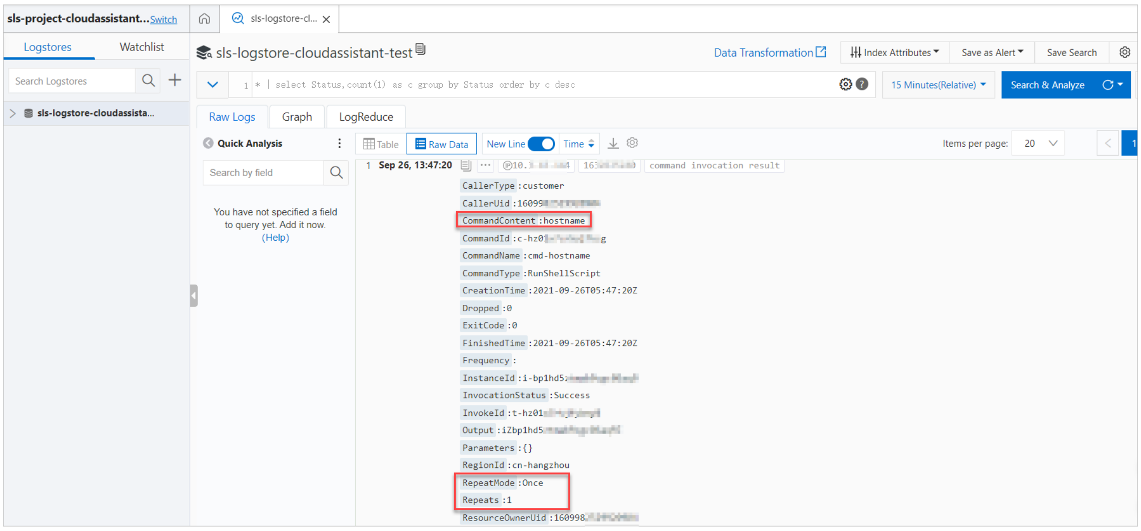
3.

4. In the upper-right corner of the **Cloud Assistant** page, click **Operation Content and Result Delivery**.
5. In the **Operation Content and Result Delivery** dialog box, click **Logstores** on the right of the **Logstore** field.

For more information about how to query logs, see Query and analyze logs.

The following figures show example logs about O&M task execution records. For information about parameters contained in the execution records, see the Parameters contained in O&M task execution records section in this topic.

- Example log about one-time execution records (execution records of a command task that runs a command only once)

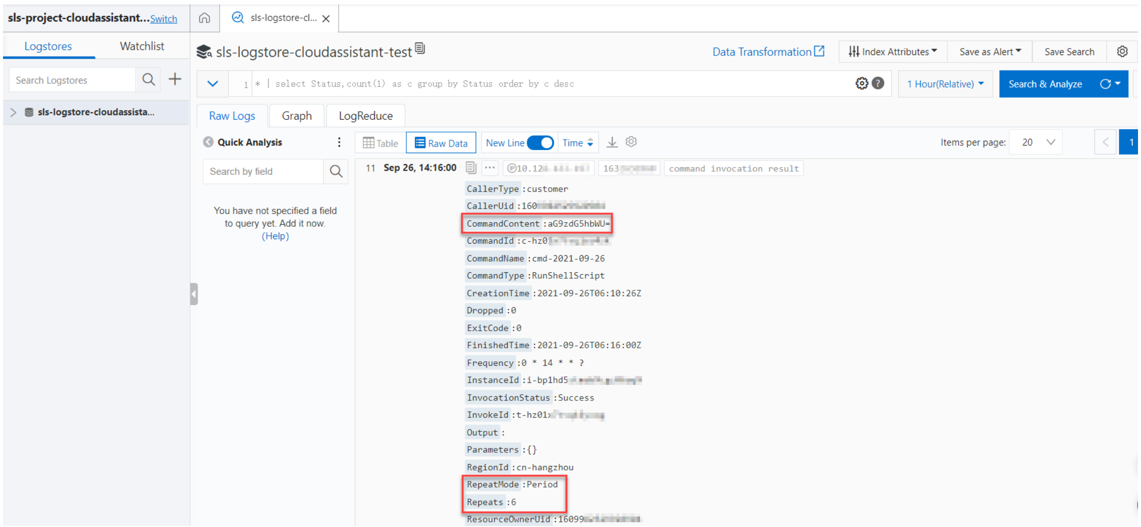


```
* | select Status, count(1) as c group by Status order by c desc
```

```
1  Sep 26, 13:47:20   @10.[redacted]  163[redacted]  command invocation result
   CallerType :customer
   CallerUid :16099[redacted]
   CommandContent :hostname
   CommandId :c-hz01[redacted]g
   CommandName :cmd-hostname
   CommandType :RunShellScript
   CreationTime :2021-09-26T05:47:20Z
   Dropped :0
   ExitCode :0
   FinishedTime :2021-09-26T05:47:20Z
   Frequency :
   InstanceId :i-bp1hd5[redacted]
   InvocationStatus :Success
   InvokeId :t-hz01[redacted]
   Output :iZbp1hd5[redacted]
   Parameters :{}
   RegionId :cn-hangzhou
   RepeatMode :Once
   Repeats :1
   ResourceOwnerUid :160998[redacted]
```

- Example log about recurring execution records (execution records of a command task that runs a command on a recurring schedule)

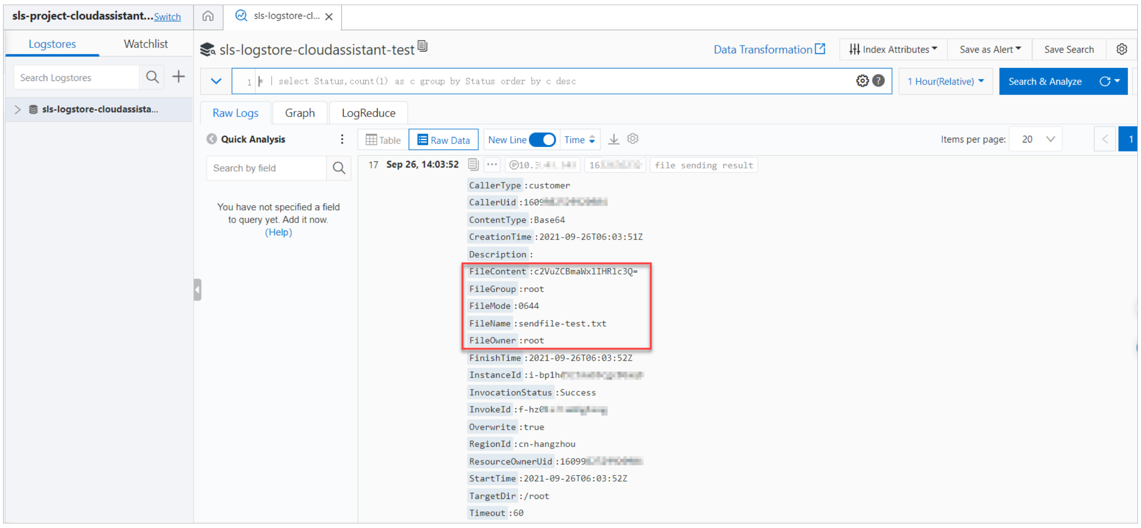
  The Repeats value indicates the number of times that the command was run.



```
* | select Status, count(1) as c group by Status order by c desc
```

```
11  Sep 26, 14:16:00   @10.12[redacted]  163[redacted]  command invocation result
    CallerType :customer
    CallerUid :160[redacted]
    CommandContent :aG9zdG5hbWU=
    CommandId :c-hz0[redacted]
    CommandName :cmd-2021-09-26
    CommandType :RunShellScript
    CreationTime :2021-09-26T06:10:26Z
    Dropped :0
    ExitCode :0
    FinishedTime :2021-09-26T06:16:00Z
    Frequency :0 * 14 * * ?
    InstanceId :i-bp1hd5[redacted]
    InvocationStatus :Success
    InvokeId :t-hz01[redacted]
    Output :
    Parameters :{}
    RegionId :cn-hangzhou
    RepeatMode :Period
    Repeats :6
    ResourceOwnerUid :16099[redacted]
```

- Example log about file-sending task execution records



```
* | select Status, count(1) as c group by Status order by c desc
```

```
17  Sep 26, 14:03:52   10.3[redacted]   16[redacted]   file sending result
CallerType :customer
CallerUid :1609[redacted]
ContentType :Base64
CreationTime :2021-09-26T06:03:51Z
Description :
FileContent :c2VuZCBmaWxlIHRlc3Q=
FileGroup :root
FileMode :0644
FileName :sendfile-test.txt
FileOwner :root
FinishTime :2021-09-26T06:03:52Z
InstanceId :i-bp1h[redacted]
InvocationStatus :Success
InvokeId :f-hz0[redacted]
Overwrite :true
RegionId :cn-hangzhou
ResourceOwnerUid :16099[redacted]
StartTime :2021-09-26T06:03:52Z
TargetDir :/root
Timeout :60
```

Query O&M task execution records in the OSS console

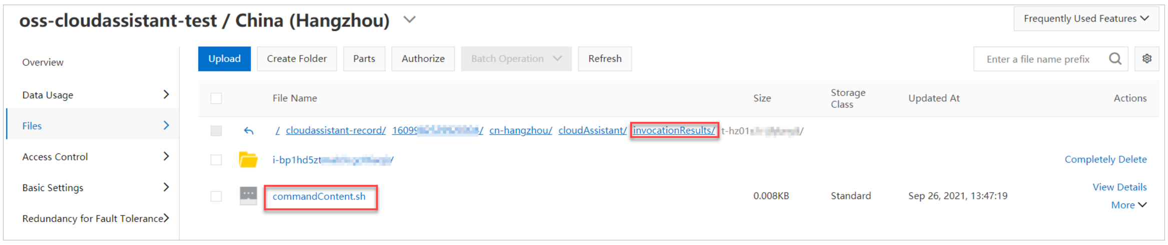
This section describes how to access a specified OSS bucket from the ECS console to query objects that contain delivered O&M task execution records. Alternatively, you can log on to the OSS console and access the specified bucket.

1.
2.
3.
4. In the upper-right corner of the **Cloud Assistant** page, click **Operation Content and Result Delivery**.
5. In the **Operation Content and Result Delivery** dialog box, click **OSS Console** on the right side of the **Bucket** field.
6. Go to the directory in which the object that contains the execution records of an O&M task is stored.

   After you log on to the OSS console, the system directs you to the root directory that you specified when you configured delivery settings in the Operation Content and Result Delivery dialog box. You can go to automatically generated subdirectories based on O&M task types.

   - For a command task, go to the *invocationResults/<Execution ID>* subdirectory. In this subdirectory, directories that are named after ECS instance IDs and the script of the command are displayed. The script may have one of the following names*:*
     - *commandContent.bat*: A batch command is run on specified Windows ECS instances.
     - *commandContent.ps1*: A PowerShell command is run on specified Windows ECS instances.
     - *commandContent.sh*: A shell command is run on specified Linux ECS instances.
   - For a file-sending task, go to the *sendFileResults/<Execution ID>* subdirectory. In this subdirectory, directories that are named after ECS instance IDs and the *fileContent.txt* file are displayed. The fileContent.txt file contains the sent content.

The following figure shows an example subdirectory generated for a command task that runs a shell command on a Linux ECS instance.



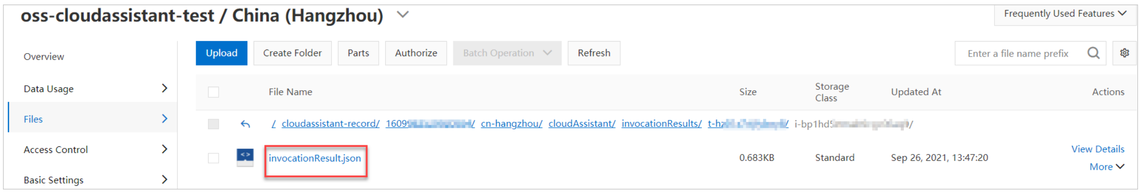
/ cloudassistant-record/ 16099[redacted]/ cn-hangzhou/ cloudAssistant/ invocationResults/ t-hz01[redacted]/

File Name	Size	Storage Class	Updated At	Actions
i-bp1hd5zt[redacted]/				Completely Delete
commandContent.sh	0.008KB	Standard	Sep 26, 2021, 13:47:19	View Details More

7. Go to the directory that is named after the ID of an ECS instance to query the object that contains the execution records of tasks run on the instance.

   The following figures show example JSON-formatted objects that contain O&M task execution records.

   - Example object that contains one-time execution records

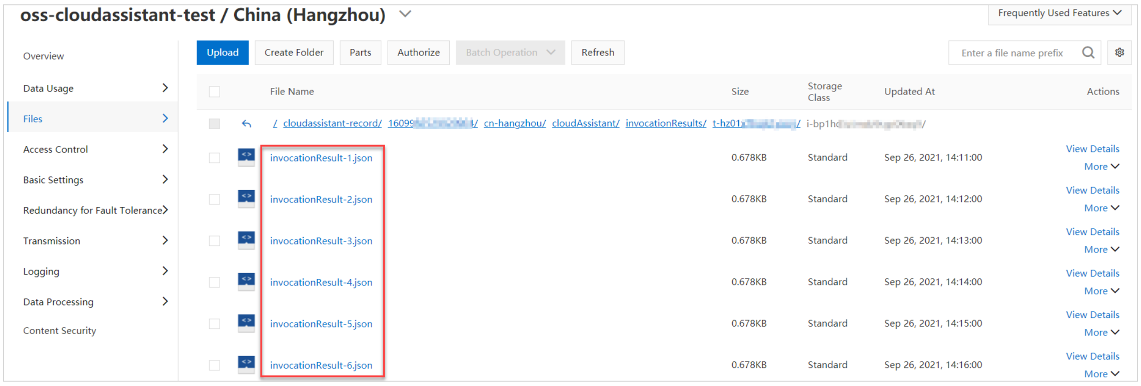


/ cloudassistant-record/ 16099[redacted]/ cn-hangzhou/ cloudAssistant/ invocationResults/ t-hz[redacted]/ i-bp1hd5[redacted]/

File Name	Size	Storage Class	Updated At	Actions
invocationResult.json	0.683KB	Standard	Sep 26, 2021, 13:47:20	View Details More

   - Example object that contains recurring execution records

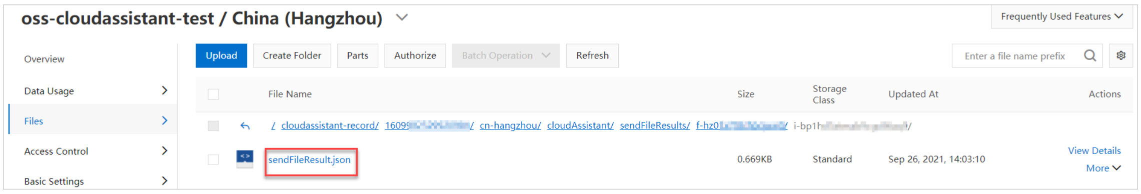
     The digits in each object name indicate the number of times that the command was run on the specified instance.



/ cloudassistant-record/ 16099[redacted]/ cn-hangzhou/ cloudAssistant/ invocationResults/ t-hz01[redacted]/ i-bp1hd[redacted]/

File Name	Size	Storage Class	Updated At	Actions
invocationResult-1.json	0.678KB	Standard	Sep 26, 2021, 14:11:00	View Details More
invocationResult-2.json	0.678KB	Standard	Sep 26, 2021, 14:12:00	View Details More
invocationResult-3.json	0.678KB	Standard	Sep 26, 2021, 14:13:00	View Details More
invocationResult-4.json	0.678KB	Standard	Sep 26, 2021, 14:14:00	View Details More
invocationResult-5.json	0.678KB	Standard	Sep 26, 2021, 14:15:00	View Details More
invocationResult-6.json	0.678KB	Standard	Sep 26, 2021, 14:16:00	View Details More

   - Example object that contains file-sending task execution records



/ cloudassistant-record/ 16099[redacted]/ cn-hangzhou/ cloudAssistant/ sendFileResults/ f-hz01[redacted]/ i-bp1h[redacted]/

File Name	Size	Storage Class	Updated At	Actions
sendFileResult.json	0.669KB	Standard	Sep 26, 2021, 14:03:10	View Details More

8. Click **View Details** in the **Actions** column corresponding to an object that contains execution records. Then, download the object or copy the object URL and view the object content.

   The following code shows an example object that contains the one-time execution records of a shell command. For information about parameters contained in the execution records, see the Parameters contained in O&M task execution records section in this topic.

```
{
    "RegionId":"cn-hangzhou",
    "InstanceId":"i-bp1hd5ztmab9cgc0****",
    "InvokeId":"t-hz01x7rtjfy****",
    "CommandId":"c-hz01x7cn5aj****",
    "CommandName":"cmd-hostname",
    "CommandType":"RunShellScript",
    "CommandContent":"hostname",
    "ResourceOwnerUid":160998252992****,
    "CallerUid":160998252992****,
    "CallerType":"customer",
    "Timeout":60,
    "Frequency":"",
    "Parameters":"{}",
    "Username":"",
    "RepeatMode":"Once",
    "Repeats":1,
    "InvocationStatus":"Success",
    "Dropped":0,
    "Output":"iZbp1hd5ztmab9cgc0****\n",
    "ExitCode":0,
    "CreationTime":"2021-09-26T05:47:20Z",
    "StartTime":"2021-09-26T05:47:20Z",
    "UpdateTime":"2021-09-26T05:47:20Z",
    "FinishedTime":"2021-09-26T05:47:20Z",
    "StopTime":""
}
```

Parameters contained in O&M task execution records

The following table describes the parameters contained in the execution records of command tasks. For more information about the parameters such as their valid values, see DescribeCommands and DescribeInvocationResults.

Parameter	Example	Description
RegionId	cn-hangzhou	The region ID of the ECS instance on which the command was run.
InstanceId	i-bp1hd5ztmab9cgc0****	The ID of the ECS instance.
InvokeId	t-hz01x7rtjfy****	The ID of the execution.
CommandId	c-hz01x7cn5aj****	The ID of the command.
CommandName	cmd-hostname	The name of the command.
CommandType	RunShellScript	The type of the command.
CommandContent	hostname	The plaintext content of the command.

Parameter	Example	Description
ResourceOwnerUid	160998252992****	The Alibaba Cloud account ID of the command caller.
CallerUid	160998252992****	The account ID of the command caller.
CallerType	customer	The call mode of the command caller.
Timeout	60	The timeout period for the command to run on the ECS instance. Unit: seconds.
Frequency	0 * 14 * * ?	The schedule on which the recurring executions of the command take place. The value of this parameter is a cron expression. For more information, see Cron expression.
Parameters	{}	The key-value pairs of custom parameters to be passed in when the command can include custom parameters.
Username	root	The username that is used to run the command on the ECS instance.
RepeatMode	Period	The execution mode of the command.
Repeats	2	The number of times that the command was run on the ECS instance.
InvocationStatus	Success	The command state on a single ECS instance.
ErrorCode	InstanceNotExists	The error code returned when the command cannot be sent or run.
ErrorInfo	the specified instance does not exists	The error message returned when the command cannot be sent or run.
Dropped	0	The size of truncated and discarded text when the size of text in the Output response parameter is larger than 24 KB.
Output	iZbp1hd5ztmab9cgc0****\n	The command output.
ExitCode	0	The exit code of the command.
CreationTime	2021-09-26T05:47:20Z	The creation time of the execution.
StartTime	2021-09-26T05:47:20Z	The time when the command started to run on the ECS instance.
UpdateTime	2021-09-26T06:53:00Z	The time when the execution state was updated.
FinishedTime	2021-09-26T06:53:00Z	The completion time of the execution.

Parameter	Example	Description
StopTime	2021-09-26T06:53:00Z	The time when the command stopped being run on the ECS instance. If you called the StopInvocation operation to manually stop the execution, the value is the time when the operation was called.

The following table describes the parameters contained in the execution records of file-sending tasks. For more information about the parameters such as their valid values, see DescribeSendFileResults.

Parameter	Example	Description
RegionId	cn-hangzhou	The region ID of the ECS instance to which the file was sent.
InstanceId	i-bp1hd5ztmab9cgc0****	The ID of the ECS instance.
InvokeId	f-hz01xeva44****	The ID of the execution.
FileName	sendfile-test.txt	The name of the file.
ContentType	Base64	The content type of the file.
Description	Used for test	The description of the file.
FileContent	c2VuZCBmaWxlIHRlc3Q=	The content of the file.
FileGroup	root	The group of the file.
FileMode	0644	The permissions on the file.
FileOwner	root	The owner of the file.
ResourceOwnerUid	16099825299****	The Alibaba Cloud account ID of the file sender.
CallerUid	16099825299****	The account ID of the file sender.
CallerType	customer	The call mode of the file sender.
Overwrite	true	Specifies whether to overwrite a file in the destination directory if the file has the same name as the sent file.
TargetDir	/root	The destination directory to which the file is sent.
Timeout	60	The timeout period for sending the file. Unit: seconds.
InvocationStatus	Success	The state of the file-sending task.
ErrorCode	FileAlreadyExists	The error code returned when the file cannot be sent to the ECS instance.

Parameter	Example	Description
ErrorInfo	File already exists: sendfile-test.txt	The error message returned when the file cannot be sent to the ECS instance or when the file-sending task cannot be executed on the ECS instance.
CreationTime	2021-09-28T05:31:04Z	The creation time of the file-sending task.
StartTime	2021-09-28T05:31:04Z	The time when the file-sending task started to be executed on the ECS instance.
UpdateTime	2021-09-28T05:31:04Z	The time when the state of the file-sending task was updated.
FinishTime	2021-09-28T05:31:04Z	The time when the file-sending task finished being executed.

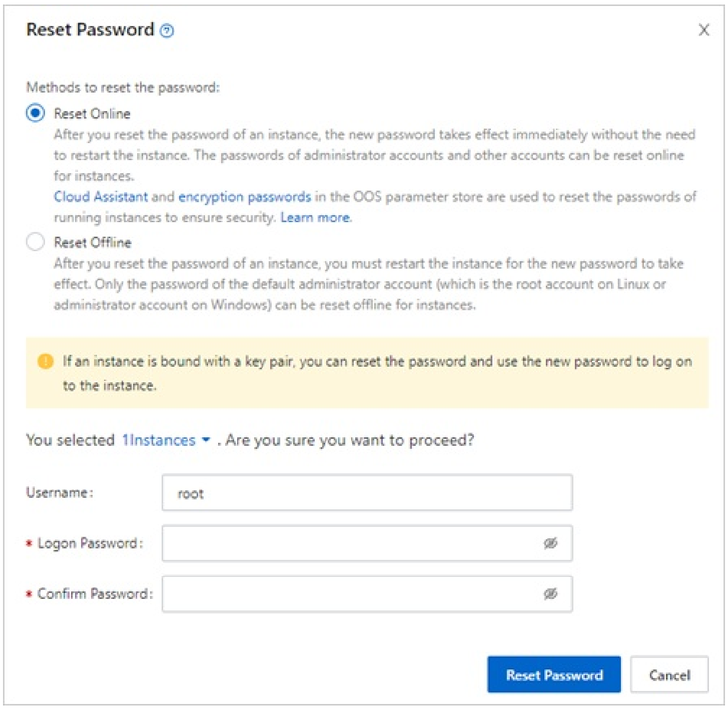
4.7. Change the password of an instance online

Change the password of an instance online

Alibaba Cloud Elastic Compute Service (ECS) allows you to change the logon password of an ECS instance online. After you change the password, the new password immediately takes effect without the need to restart the instance in the ECS console. This topic describes how the encryption parameters and templates of Operation Orchestration Service (OOS) work during the process of changing the password of an instance online.

Description

In the **Reset Password** dialog box, select **Reset Online** to change the password of an instance online. After you change the password, the new password immediately takes effect without the need to restart the instance in the ECS console.



Reset Password ⓘ

Methods to reset the password:

● Reset Online
After you reset the password of an instance, the new password takes effect immediately without the need to restart the instance. The passwords of administrator accounts and other accounts can be reset online for instances.
Cloud Assistant and encryption passwords in the OOS parameter store are used to reset the passwords of running instances to ensure security. Learn more.

○ Reset Offline
After you reset the password of an instance, you must restart the instance for the new password to take effect. Only the password of the default administrator account (which is the root account on Linux or administrator account on Windows) can be reset offline for instances.

If an instance is bound with a key pair, you can reset the password and use the new password to log on to the instance.

You selected 1Instances . Are you sure you want to proceed?

Username: root

* Logon Password:

* Confirm Password:

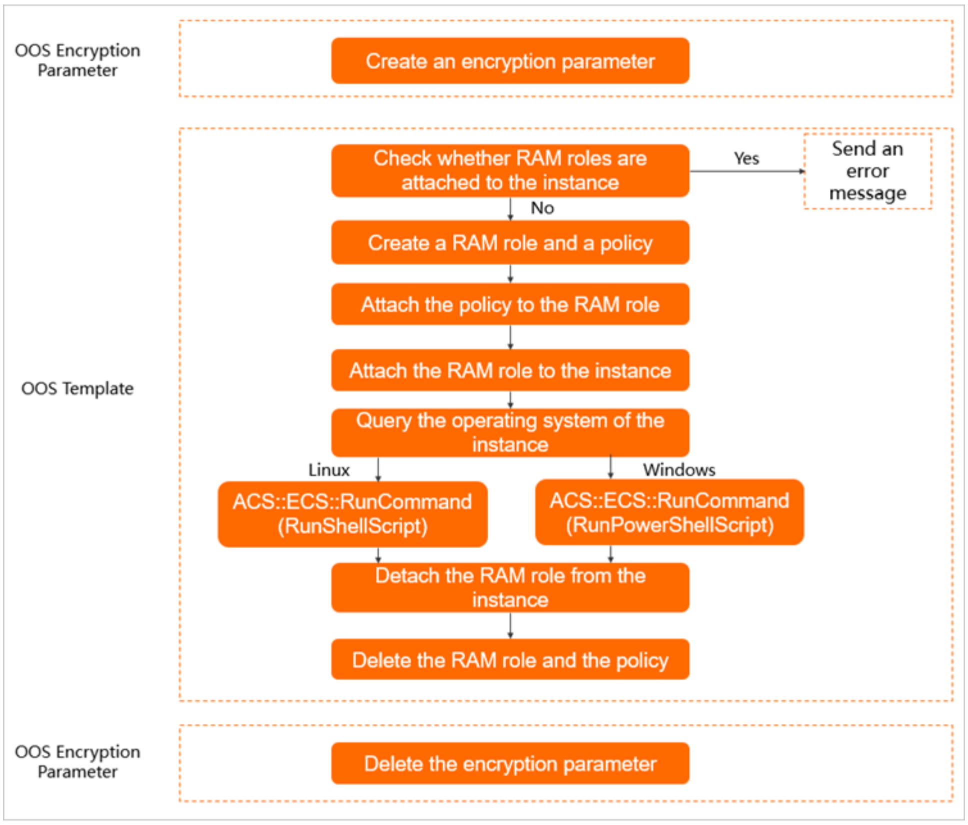
In addition to the templates and encryption parameters of OOS, Resource Orchestration Service (ROS), Key Management Service (KMS), and ECS are also involved in the procedure to change the passwords of instances online. For more information, see Procedure.

Before the password of an instance can be changed online, the following conditions must be met:

- An Alibaba Cloud account instead of a RAM user is used.
- The instance resides in a virtual private cloud (VPC). Only the password of an instance in a VPC can be changed online. The password of an instance in the classic network cannot be changed online.
- KMS is activated. For more information, see Activate KMS.
- The instance is in the **Running** (Running) state.
- No RAM roles are attached to the instance.

Procedure

The following figure shows the procedure of changing the password of an ECS instance online.


OOS Encryption Parameter
Create an encryption parameter
OOS Template
Check whether RAM roles are attached to the instance
Yes
Send an error message
No
Create a RAM role and a policy
Attach the policy to the RAM role
Attach the RAM role to the instance
Query the operating system of the instance
Linux
Windows
ACS::ECS::RunCommand (RunShellScript)
ACS::ECS::RunCommand (RunPowerShellScript)
Detach the RAM role from the instance
Delete the RAM role and the policy
OOS Encryption Parameter
Delete the encryption parameter

Encryption parameters are used to encrypt passwords and OSS templates are used to implement O&M. For more information, see Manage encryption parameters. The following table describes the steps in the password change procedure.

No.	Step	Description
①	Create an encryption parameter.	The system creates an encryption parameter in OOS Parameter Store based on the specified plaintext password.
②	Check whether RAM roles are attached to the instance.	The system checks whether RAM roles are attached to the instance. ● If RAM roles are attached to the instance, the system sends an error message. ● If no RAM roles are attached to the instance, the system goes to the next step.

<table>
<tr><th>No.</th><th>Step</th><th>Description</th></tr>
<tr><td>③</td><td>Create a RAM role and a policy.</td><td>

The system uses ROS stacks to create a RAM role and a policy for the instance.

The following code shows the content of the policy:

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "kms:*",
                "oos:*"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

</td></tr>
</table>

No.	Step	Description

④	Attach the policy to the RAM role.	The system uses an ROS stack to attach the policy to the RAM role.
		The following code shows the trust policy of the RAM role:
		`{`
		`  "Statement": [`
		`    {`
		`      "Action": "sts:AssumeRole",`
		`      "Effect": "Allow",`
		`      "Principal": {`
		`        "Service": [`
		`          "oos.aliyuncs.com",`
		`          "ecs.aliyuncs.com"`
		`        ]`
		`      }`
		`    }`
		`  ],`
		`  "Version": "1"`
		`}`

⑤	Attach the RAM role to the instance.	The system attaches the created RAM role to the instance.
⑥	Query the operating system of the instance.	The system queries the operating system of the instance.

<table>
<tr><th>No.</th><th>Step</th><th>Description</th></tr>
<tr><td>⑦</td><td>ACS::ECS::RunCommand</td><td>

The system runs one of the following commands to change the password of the instance based on the operating system of the instance.

- If the instance is a Linux instance, the system runs the following command:

```
echo '{{username}}:
{{passwordParameter}}'|chpasswd
if [ $? -eq 0 ]; then
    if grep -q "PasswordAuthentication no"
/etc/ssh/sshd_config;then
        sed -i "s/PasswordAuthentication
no/PasswordAuthentication yes/g"
/etc/ssh/sshd_config
        systemctl restart sshd
    fi
else
    exit 1;
fi
```

- If the instance is a Windows instance, the system runs the following command:

```
net user {{username}} "{{passwordParameter}}"
```

</td></tr>
<tr><td>⑧</td><td>Detach the RAM role from the instance.</td><td>The system detaches the RAM role from the instance.</td></tr>
<tr><td>⑨</td><td>Delete the RAM role and the policy.</td><td>The system deletes the RAM role and the policy.</td></tr>
<tr><td>⑩</td><td>Delete the encryption parameter.</td><td>The system deletes the created encryption parameter.</td></tr>
</table>

4.8. Cron expression

When you run a Cloud Assistant command, you can call an API operation and use the Timed and Frequency parameters to set when to run the Cloud Assistant command. The value of the Frequency parameter is a cron expression. This parameter specifies the frequency of scheduled tasks, frequency of routine maintenance, and the point in time at which to complete a one-time task.

Introduction

A cron expression is a string that represents time. The string consists of five or six spaces and six or seven fields, which is in the `x x x x x x x` format. `x` is a placeholder of a field. The last filed that indicates the year is not required and can be left empty. If a field contains multiple values, the values are separated by commas (`,`). Each field can be a specific value or special characters that have logical representations. Each field supports a maximum of one leading zero.

Note If you specify to execute a task at 8:15 every day in 2022, the cron expression can be specified to `0 15 8 ? * * 2022` or `0 15 08 ? * * 2022` but cannot be specified to `0 15 008 ? * * 2022` .

Field values

The following table describes valid values and supported special characters for each field in cron expressions.

Field	Required	Valid value range	Special character
Second	Yes	[0, 59]	* , - /
Minute	Yes	[0, 59]	* , - /
Hour	Yes	[0, 23]	* , - /
Day	Yes	[1, 31]	* , - / ? L W
Month	Yes	[1, 12] or [JAN, DEC]	* , - /
Week	Yes	[1, 7] or [MON, SUN]. If you use the [1, 7] format, `1` indicates Monday and `7` indicates Sunday.	* , - / ? L #
Year	No	[Current year ,2099]	* , - /

Special characters

Each field in a cron expression can contain a specific number of special characters. Each special character represents a logical argument.

Special character	Description	Example
`*`	Indicates all valid values.	In the Month field, an asterisk (`*`) indicates every month. In the Week field, an asterisk (`*`) indicates every day of the week.
`,`	Lists enumerated values.	In the Minute field, `5,20` indicates that the task is triggered once at both the 5th and 20th minutes.
`-`	Indicates a range.	In the Minute field, `5-20` indicates that the task is triggered once every minute from the 5th to 20th minute.

Special character	Description	Example
`/`	Indicates increments.	In the Minute field, `0/15` indicates that the task is triggered once every 15 minutes from the beginning of an hour. In the Minute field, `3/20` indicates that the task is triggered once every 20 minutes from the 3rd minute of an hour.
`?`	Indicates an unspecified value. Only the Day and Week fields support this character.	If the Day or Week field is specified, the other field must be set to a question mark (`?`) to prevent conflicts.
`L`	Indicates the last day of a specific period. Only the Day and Week fields support this character. **Note** To prevent logic errors, do not specify a list or range when you use the `L` character.	- In the Day field, `L` indicates the last day of a month. In the Day of a week field, `L` indicates the last day of a week, which is Sunday (`SUN`). - `L` can be preceded by a value. For example, `6L` in the Week field indicates the last Saturday of a month.
`W`	The weekday that is nearest to the specified day of the month. The weekday that the `W` character indicates is in the same month as the specified day of the month. `LW` indicates the last weekday of the specified month.	If `5W` is specified in the Day field and the 5th day of the month falls on Saturday, the task is triggered on Friday, which is the 4th day of the month. If the 5th day of the month falls on Sunday, the scheduled task is triggered on Monday, which is the 6th day of the month. If the 5th day of the month falls on a weekday, the scheduled task is triggered on the 5th day of the month.
`#`	A specific day of a specific week in every month. Only the Day of a week field supports this character.	In the Week field, `4#2` indicates the second Thursday of a month.

Examples

The following table describes some example values of cron expressions.

Example	Description
`0 15 10 ? * *`	Executes the task at 10:15 every day.
`0 15 10 * * ?`	Executes the task at 10:15 every day.
`0 0 12 * * ?`	Executes the task at 12:00 every day.
`0 0 10,14,16 * * ?`	Executes the task at 10:00, 14:00, and 16:00 every day.
`0 0/30 9-17 * * ?`	Executes the task every half an hour between 09:00 and 17:00 every day.

Example	Description
`0 * 14 * * ?`	Executes the task every minute between 14:00 and 14:59 every day.
`0 0-5 14 * * ?`	Executes the task every minute between 14:00 and 14:05 every day.
`0 0/5 14 * * ?`	Executes the task every 5 minutes between 14:00 and 14:55 every day.
`0 0/5 14,18 * * ?`	Executes the task every 5 minutes between 14:00 and 14:55 and between 18:00 and 18:55 every day.
`0 0 12 ? * WED`	Executes the task at 12:00 every Wednesday.
`0 15 10 15 * ?`	Executes the task at 10:15 on the 15th day of every month.
`0 15 10 L * ?`	Executes the task at 10:15 on the last day of every month.
`0 15 10 ? * 6L`	Executes the task at 10:15 on the last Saturday of every month.
`0 15 10 ? * 6#3`	Executes the task at 10:15 on the third Saturday of every month.
`0 10,44 14 ? 3 WED`	Executes the task at 14:10 and 14:44 every Wednesday in March every year.
`0 15 10 ? * * 2022`	Executes the task at 10:15 every day in 2022.
`0 15 10 ? * * *`	Executes the task at 10:15 every day every year.
`0 0/5 14,18 * * ? 2022`	Executes the task every 5 minutes between 14:00 and 14:55 and between 18:00 and 18:55 every day in 2022.
`0 15 10 ? * 6#3 2022,2023`	Executes the task at 10:15 on the third Saturday of every month from 2022 to 2023.
`0 0/30 9-17 * * ? 2022-2025`	Executes the task every half an hour between 9:00 and 17:30 every day from 2022 to 2025.
`0 10,44 14 ? 3 WED 2022/2`	Executes the task at 14:10 and 14:44 every Wednesday in March every 2 years starting from 2022.

Related information

- InvokeCommand
- RunCommand

5.Operation Orchestration Service

5.1. Overview

Operation Orchestration Service (OOS) automatically manages and executes O&M tasks. In a template, you can define items such as O&M tasks, execution processes, and input and output of the execution. Then, you only need to execute the template to implement automated O&M.

Scenarios

OOS is applicable to the following scenarios:

- Scheduled and batch O&M tasks. For example, you can check the remaining storage space of cloud disks in multiple ECS instances. You can select the ECS instances that you want to check by items such as name, tag group, and resource group. Then, you can run Cloud Assistant commands to perform disk checks and view the results in a unified manner.
- Event-driven O&M tasks. For example, when the vCPU utilization of an ECS instance reaches 85%, OOS can automatically restart the ECS instance to prevent service interruption.
- Cross-region O&M tasks. For example, you can copy multiple ECS instances from one region to another by using the image copy feature.
- O&M tasks subject to approval. For example, you can add an approval process for purchasing or releasing ECS instances.

OOS provides best practices of operations as code. OOS is a centralized O&M platform that allows you to create templates from manuals such as Operations and Maintenance Guides, User Guide, and Operation Guides.

Benefits

OOS improves the efficiency and security of O&M tasks by offering the following benefits:

- Visualized execution processes and results
- Free and managed service
- Efficiency in managing multiple O&M tasks at a time
- Superior authentication and verification systems
- Easy-to-use templates
- Cross-region O&M
- Operations as code
- Delegated authorization

References

- Start multiple ECS instances by using OOS
- Overview

5.2. Start multiple ECS instances by using OOS

This topic describes how to start multiple ECS instances in the ECS console by using the ACS-ECS-BulkyStartInstances public template of Operation Orchestration Service (OOS).

Prerequisites

Before you create an O&M task on OOS, ensure that the following requirements are met:

- OOS is activated.
- A RAM role is created and the *AliyunECSFullAccess* policy is granted to the OOS service role.

  The OOSServiceRole-EcsDocGuideTest RAM role is created in this example.
- A specified tag is bound to the target instance. For more information, see Create or bind a tag.

  The `ECS: Documentation` tag is created in this example.

Context

OOS defines the O&M tasks that you want to perform in a template. Both YAML and JSON formats are supported for templates, which are divided into public and custom templates. Public templates are provided for your reference and can be used directly, such as the **ACS-ECS-BulkyStartInstances** public template in this topic. Before executing a template, you must check the O&M tasks defined in the template and set up a test environment to check the execution results of the template.

You can also customize a template to perform your O&M tasks.

Procedure

1. Log on to the OOS console.
2. In the left-side navigation pane, click **Public Templates**.
3.
4. On the **Public Templates** page, select **ACS-ECS-BulkyStartInstances** and click **Create Execution**.
5. On the **Create** page, perform the following operations:
   i. In the **Basic Information** step, keep the default settings and click **Next: Parameter Settings**.

      Execution Mode: **Automatic** is selected in this example, indicating that all tasks in the template are to be executed automatically.

ii. Configure parameters in the **Parameter Settings** step.

The following table describes some parameters. You can keep the default settings of the other parameters.

Parameter	Description	Example
targets	The method to specify the instance. An error is returned if the instance is not in the **Stopped** state. You can specify the instance by using one of the following methods: ▪ **Select Instances Manually** ▪ **Specify Instance Tags** ▪ **Specify the resource group for instances**	Specify Instance Tags
Select Instances	If you select **Select Instances Manually**, you must select one or more instances that are in the **Stopped** state.	i-bp1e9mxelweamh5g****
Instance Tags	If you select **Specify Instance Tags**, you must select one or more available tags. The tag keys are required. OOS calls the StartInstance operation to start multiple ECS instances at a time.	ECS:Documentation
Resource Group	If you select **Specify the resource group for instances**, you must select a resource group.	*Test*
Permissions	OOS allows you to use RAM to configure O&M permissions. You can use the permissions of your own account or use the permissions of the created **oosAssumeRole** RAM role to implement fine-grained control.	**Specify RAM Role and Use Permissions Granted to This Role**

iii. Click **Next: OK**.

iv. In the **OK** step, preview and confirm the values defined in the **Basic Information** and **Parameter Settings** steps and then click **Create**.

Result

You can view the execution results of O&M tasks on the **Executions** page after you create O&M tasks.

- If **Success** is displayed in the **Execution Status** column corresponding to an O&M task, the O&M task is successful.
- If **Failed** is displayed in the **Execution Status** column corresponding to an O&M task, you can click **Details** in the **Actions** column and then click **Execution Logs**. Then, you can analyze and adjust the execution content based on the log information.

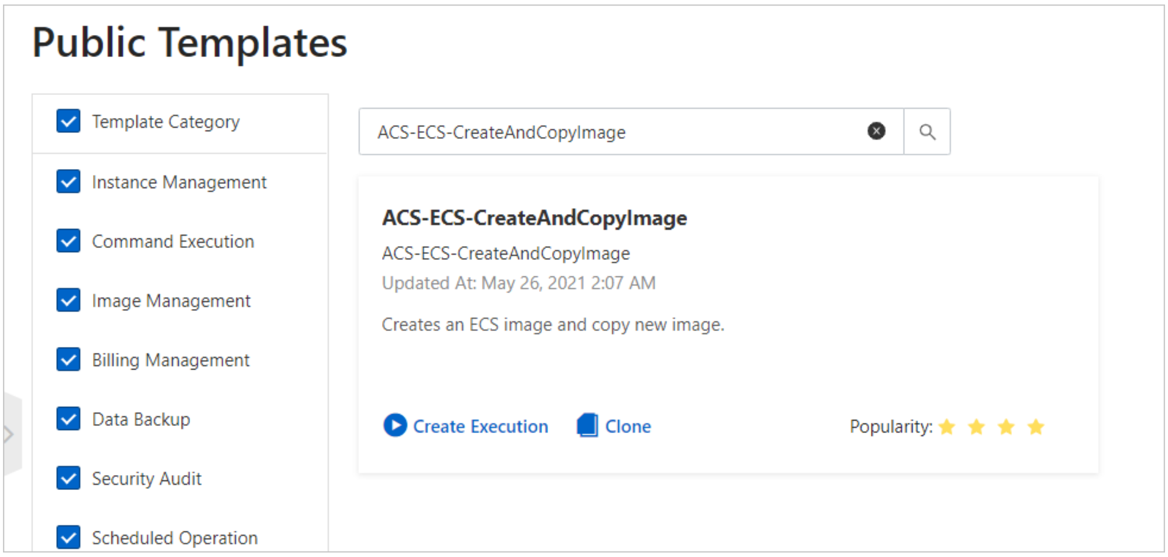
5.3. View the information of a public template

Operation Orchestration Service (OOS) provides public templates for common O&M tasks to meet your O&M requirements and reduce your time costs in developing templates. This topic describes how to view the information of a public template to understand its execution process and impact.

Procedure

1. Log on to the OOS console.
2. In the left-side navigation pane, click **Public Templates**.
3. On the **Public Templates** page, find the template that you want to view and click its name.

   You can filter templates by category or enter a template name to search for the template. For example, enter ACS-ECS-CreateAndCopyImage to search for the public template that is used to create custom images and copy them to other regions.



Public Templates

☑ Template Category

☑ Instance Management

☑ Command Execution

☑ Image Management

☑ Billing Management

☑ Data Backup

☑ Security Audit

☑ Scheduled Operation

ACS-ECS-CreateAndCopyImage

ACS-ECS-CreateAndCopyImage

ACS-ECS-CreateAndCopyImage

Updated At: May 26, 2021 2:07 AM

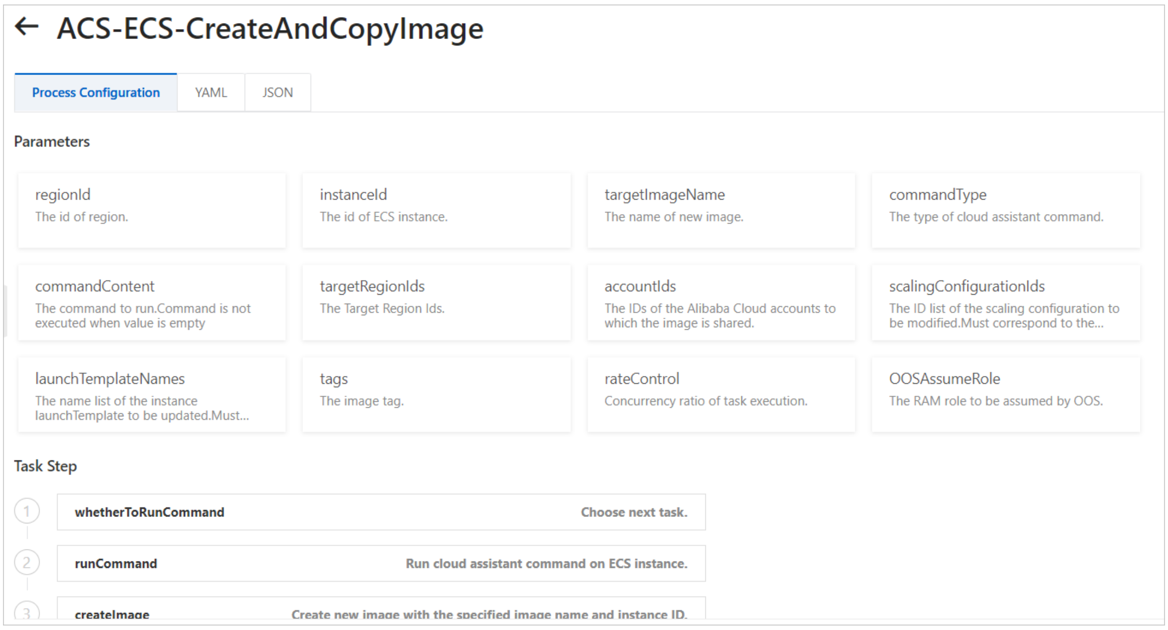
Creates an ECS image and copy new image.

Create Execution Clone Popularity: ★ ★ ★ ★

4. On the **Process Configuration** tab, view the parameters, task steps, and output of the template.

   Parameters are the information that you can specify to create an execution for the template. Output is the information returned after an execution of the template is complete. The task steps define the O&M operations that make up the template execution process. During an execution of this template, task steps are completed or skipped based on the parameter settings. For example, if you did not specify the Copy to Other Region parameter when you created an execution for the ACS-ECS-CreateAndCopyImage template, the step to copy the created image to other regions is skipped during the execution.

You can click the **YAML** or **JSON** tab to view the detailed code of the template.



ACS-ECS-CreateAndCopyImage

Parameters

regionId
The id of region.

instanceId
The id of ECS instance.

targetImageName
The name of new image.

commandType
The type of cloud assistant command.

commandContent
The command to run.Command is not executed when value is empty

targetRegionIds
The Target Region Ids.

accountIds
The IDs of the Alibaba Cloud accounts to which the image is shared.

scalingConfigurationIds
The ID list of the scaling configuration to be modified.Must correspond to the...

launchTemplateNames
The name list of the instance launchTemplate to be updated.Must...

tags
The image tag.

rateControl
Concurrency ratio of task execution.

OOSAssumeRole
The RAM role to be assumed by OOS.

Task Step

1 whetherToRunCommand — Choose next task.

2 runCommand — Run cloud assistant command on ECS instance.

3 createImage — Create new image with the specified image name and instance ID.

6.Manage licenses

6.1. Create a license management task

License Manager automates the discovery and statistics collection of cloud resources associated with licenses. This can help you monitor and manage your license usage in real time, mitigate non-compliance risks, and reduce management costs. This topic describes how to create license management tasks and the limits on license management tasks.

Context

An increasing number of enterprise users migrate their business to the cloud, and the demand for using and managing licenses also increases. Previously, you had to manually track resource creation and license usage. Problems such as lack of monitoring of the number of licenses used, frequent creation and release of instances, and failure to update usage records in real time were common. To solve these problems, Alibaba Cloud provides License Manager to help you monitor license usage in real time.

License Manager provides simplified management and usage monitoring for your software such as Windows Server and SQL Server. This mitigates non-compliance risks that arise from overuse of licenses and reduces your management costs.

Limits

- License Manager is now available only in the US (Silicon Valley), US (Virginia), and China (Hangzhou) regions, and will be gradually supported in other regions.
- You can create up to 25 license management tasks within a single region.

Procedure

1.
2. In the left-side navigation pane, choose **Maintenance & Monitoring > License Manager**.
3. On the **License Manager** page, click **Create License Management Task**.
4. When you use License Manager for the first time, you must follow the instructions to complete authorization.

   If the `Cloud resource access authorization successful` message appears and you are directed to the ECS console, you are authorized to use License Manager.

   > **Note** For more information about RAM roles, see RAM role overview.

5. In the Create License Management Task dialog box, configure the parameters for the license management task.

Parameter	Description

Parameter	Description
License Management Task Name	The name of the license management task. Example: Windows server1234567. The name must be 2 to 128 characters in length and can contain letters, digits, `periods (.),underscores (_), hyphens (-), and colons (:)`. It cannot start with a digit, a special character, http://, or https://.
Description	The description of the license management task. The description must be 2 to 256 characters in length.
License Type	The type of the managed license. ○ **Instance**: The license is associated with instances. You must set **License Limit of Instance** to specify the number of instances that can be associated with the license as the counting model used for the licenses. The value must be a positive integer. Valid values: 1 to 100000. ○ **vCPU**: The license is associated with vCPUs. You must set **License Limit of vCPU** to specify the number of vCPUs that can be associated with the license as the counting model used for the licenses. The value must be a positive integer. Valid values: 1 to 100000.
Automated Discovery Rule	The product and product version that correspond to the license. This can help you discover and manage licenses in a more precise manner.

6. After you configure the parameters, click **Create**.

   After the license management task is created, **Activated** is displayed in the Status column.

What's next

After the license management task is created, the system automatically discovers and collects statistics on cloud resources associated with the license management task based on the information that you configured. You can view and manage the resources and your license management tasks. For more information, see View the resources associated with a license and Manage license management tasks.

6.2. View the resources associated with a license

After you create a license management task, the system automatically discovers and collects statistics on resources associated with the licenses managed by the license management task, automated discovery rules, and resources that fail to be associated with the licenses based on the parameters such as License Type, Automated discovery rules, and Instance Quantity Limit Setting.

View the resources associated with a license

1.
2. In the left-side navigation pane, choose **Maintenance & Monitoring > License Manager**.

3. On the **Managed license** page, click the license ID to go to the Basic Information page.
4. Click the **Tracked resources** tab to view the associated resources that meet the configured conditions and rules of the license management task.

> ⓘ **Note** License Manager automatically tracks the cloud resources that match your configured rules every 24 hours and updates the displayed information.

View the resources that fail to be associated with a license

Some cloud resources may fail to be associated with your license because these cloud resources exceed the usage limits of your license or do not match your configured rules, or because system errors occur. You can perform the following operations to view these resources:

1.
2. In the left-side navigation pane, choose **Maintenance & Monitoring > License Manager**.
3. On the **Managed license** page, click the license ID to go to the Basic Information page.
4. Click the **Associated wrong resource** tab to view the resources that fail to be associated with the licenses managed by the license management task.

View automated discovery rules

> ⓘ **Note** You cannot modify or remove automated discovery rules. If you want to modify or remove an automated discovery rule, you must delete the license management task and create another one.

1.
2. In the left-side navigation pane, choose **Maintenance & Monitoring > License Manager**.
3. On the **Managed license** page, click the license ID to go to the Basic Information page.
4. Click the **Automatic Identification License Rules** tab to view the discovery rules of your license management task.

6.3. Manage license management tasks

You can modify the status, instance or vCPU quantity limits, and automated discovery rules of your created license management tasks. If you do not want to manage or monitor your license usage, you can delete your license management tasks. This topic describes how to manage license management tasks.

Deactivate a license management task

If you temporarily do not want to associate your cloud resources with a license management task, you can deactivate the license management task. Your created license configurations are still retained. You can reactivate the license management task at any time.

1.
2. In the left-side navigation pane, choose **Maintenance & Monitoring > License Manager**.
3. On the **License Manager** page, find the license management task that you want to deactivate

and click **Deactivate** in the Actions column.

4. In the **Deactivate License Configuration** message, check the displayed information of the license management task and click **OK**.

   When the license management task enters the **Deactivated** state, the license management task is deactivated.

Activate a license management task

If you want to associate your cloud resources with a license management task again, you can perform the following operations to activate the license management task:

1.
2. In the left-side navigation pane, choose **Maintenance & Monitoring > License Manager**.
3. On the **License Manager** page, find the license management task that you want to activate and click **Activate** in the Actions column.
4. In the **Activate** message, check the displayed information of the license management task and click **OK**.

   When the license management task enters the **Activated**, the license management task is activated.

Set an instance or vCPU quantity limit

If you want to change the instance or vCPU quantity limit for a license management task, you can perform the following operations to set the quantity limit:

1.
2. In the left-side navigation pane, choose **Maintenance & Monitoring > License Manager**.
3. On the **License Manager** page, find the license management task for which you want to change the quantity limit and click **Set License Limit** in the Actions column.
4. In the **Set License Limit** dialog box, enter a value in the Instance Quantity Limit Setting or vCPU Quantity Limit Setting field and click **OK**.

   When the new value appears in the Number of Licenses Consumed column, the quantity limit is changed.

Add an automated discovery rule

If you want to add an automated discovery rule, you can perform the following operations.

> **Note** You cannot modify or remove automated discovery rules. If you want to modify or remove an automated discovery rule, you must delete the associated license management task and then create another one.

1.
2. In the left-side navigation pane, choose **Maintenance & Monitoring > License Manager**.
3. On the **License Manager** page, click the license ID to go to the Basic Information page.
4. Click the **Automated Discovery Rules** tab and then click **Add License Rule**.
5. In the **Add License Rule** dialog box, select the automated discovery rule that you want to add.

> **Note** Automated discovery rules can be configured for a service of multiple versions. If you have an existing rule for a service, you can add rules only for other versions of the service.

6. Click **OK**.

   The added automated discovery rule is displayed on the **Automated Discovery Rules** tab.

Delete a license management task

If you no longer want to associate your cloud resources with a license management task, you can delete the license management task. If you confirm the delete operation, the license management task is permanently deleted. Proceed with caution.

1.
2. In the left-side navigation pane, choose **Maintenance & Monitoring > License Manager**.
3. On the **License Manager** page, find the license management task that you want to delete and click **Delete** in the Actions column.
4. In the **Delete License** message, confirm the information of the license delete and click **OK**.