Alibaba Cloud
Elastic Compute Service

Security

Issue: 20190614

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 due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information 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.
	This warning information 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 restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd /d C:/windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

1 Security groups

1.1 Overview

A security group is a virtual firewall that provides Stateful Packet Inspection (SPI), also known as dynamic packet filtering. Security groups are used to allow or deny one or more ECS instances to access the Internet or intranet. Specifically, security groups logically isolate security domains in the cloud.

Background information

A security group is a logically isolated group of instances within the same region that share the same security requirements and are mutually accessible. Considerations to note about using security groups are as follows:

- Each instance must belong to at least one security group. You need to specify the security group when you create an instance.
- Only instances in the same security group can communicate with each other through an intranet. Instances in different security groups are isolated by default. However, you can set security group rules to authorize mutual access between two security groups.
- Security groups are stateful, and states can be kept through sessions. If you send a request from your instance, the security group accepts the responses in the same session. Note that the maximum session timeout is 910s.

Security group types

Security groups can be divided into default and custom security groups. The following table provides information about these two security group types.

Security group type	Security group rule type	Security group rule priority	Inbound rule	Outbound rule	Scenario
Default security group	Default rules of the default security group	110	Enable ICMP, port SSH 22, and port RDP 3389. Disable other access. You can select Allow port HTTP 80 and port HTTPS 443.	Allow all access.	No custom security group exists in the same VPC.
Custom security group	Default rules of the custom security group	110	Deny all access.	Allow all access.	Custom security groups have been created in the same VPC, but no security group rules have been added to these security groups.
	Custom rules of the custom security group	Custom. Value range: 1 to 100	Add security group rules as needed. For more information, see *Add security group rules* and *Scenarios*.	Add security group rules as needed. For more information, see *Add security group rules* and *Scenarios*.	Custom security groups have been created in the same VPC, and rules have been added to these security groups.

Security group rules vary depending on network types.

Security group rules for classic networks apply to either Internet access or intranet access, whereas security group rules for VPCs apply to both. VPC instances can

access the Internet through intranet NIC mapping. Therefore, an Internet NIC will be invisible in your instance. You can only set intranet rules in the security group. The security group rules apply to the intranet and the Internet.

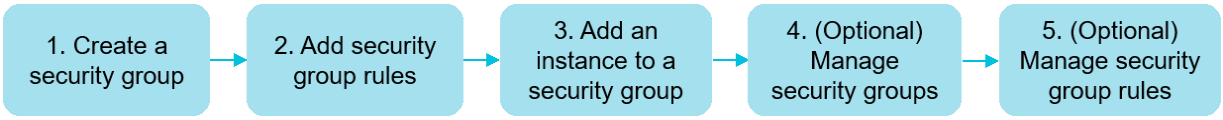
Security group priority

A smaller priority value of a security group rule indicates a higher priority.

One ECS instance can belong to different security groups. As a result, instances may have multiple security group rules that apply to them and that have the same protocol type, port range, authorization type, and authorization object. The rule that takes effect depends on the priority and authorization policy settings of each rule.

- If the priority among the rules is the same, then the corresponding 'deny' authorization rule takes effect and the 'allow' authorization rule does not take effect.
- If the priority among the rules is different, the rule with a higher priority takes effect, regardless of the authorization policy settings of each of the rules.

Procedure



Security group precautions

- Use a security group as a whitelist.
- Observe the 'minimum authorization' principle when you configure inbound or outbound rules for applications. For example, you can allow a specific port (such as port 80).
- Do not use one security group to manage all applications because requirements must be different at different layers.
- Add instances with the same security requirements to the same security group. Do not set a separate security group for each instance.
- Set simple security group rules. If you add an ECS instance to multiple security groups, hundreds of rules may apply to the instance. This may cause connection errors when you access the instance.
- The ECS console allows you to clone a security group and security group rules. If you want to modify an active security group and its rules, we recommend that you

clone the security group and modify the cloned security group to avoid impact on online applications.

1.2 Limits

This topic describes the limits of security groups and security group rules.

Security group limits

- By default, each account can create up to 100 security groups in a region. You can create more if your membership level increases. To raise the limit, open a ticket.
- By default, each Elastic Network Interface (ENI) of an instance can join up to five security groups. To raise the limit, open a ticket. If you do so, Alibaba Cloud assesses your service traffic to see if you need to add your ENI to more security groups. If you pass the assessment, you can add your ENI to 10 or 16 security groups.
- Security groups are divided into two network types: classic networks and Virtual Private Clouds (VPCs).
  - Classic network instances can join security groups of the classic network type in the same region.

    A single security group of the classic network type cannot contain more than 1,000 instances. If mutual access is required among more than 1,000 instances over the intranet, you can assign them to different security groups and allow mutual access through mutual authorization.
  - VPC instances can join security groups in the same VPC.

    A single VPC security group can contain up to 2,000 private IP addresses (shared by the primary and secondary ENIs). If mutual access is required among more than 2,000 private IP addresses over the intranet, you can assign the relevant instances to different security groups and authorize mutual access.
- If an outbound packet is permitted, inbound packets corresponding to this connection is also permitted.

For more information, see *Security group FAQ*.

Security group rule limits

Maximum number of security group rules of each ENI of an instance = number of security groups that the instance can join × maximum number of rules of each

security group. Each ENI of an instance can have up to 500 security group rules.

- By default, an ENI can join up to five security groups. Each security group can have 100 rules, that is, the total number of inbound and outbound rules of each security group cannot exceed 100.
- The number of rules in each security group varies according to the number of security groups that an ENI can join. However, the total number cannot exceed 100 (that is, inbound and outbound rules are not counted separately).
  - If each ENI is allowed to join 10 security groups, each security group can have up to 50 rules.
  - If each ENI is allowed to join 16 security groups, each security group can have up to 30 rules.

The following table shows how the number of rules varies according to the number of security groups.

Number of security groups	Maximum number of security group rules (inbound and outbound rules)
5 (default value)	100
10 (you need to open a ticket)	50
16 (you need to open a ticket)	30

1.3 Scenarios

This topic describes several typical scenarios in which VPC security groups and classic network security groups are used.

 Note:

- For information about how to create security groups and add security group rules, see *#unique_10* and *Add security group rules*.
- For information about commonly used ports, see *Typical applications of commonly used ports*.

- *Scenario 1: Establish intranet communication between two instances in the same region and under the same account*

  If you need to copy resources between two ECS instances in the same region and under the same account, you can configure security group settings to establish intranet communication between the two ECS instances.
- *Scenario 2: Establish intranet communication between two instances in the same region and under different accounts*

  If you need to copy resources between two ECS instances in the same region and different accounts, you can configure security group settings to establish intranet communication between the two ECS instances.
- *Scenario 3: Allow remote access to your instance from only specified IP addresses*

  You can remotely modify the logon port number and only allow specified IP addresses to log on to your ECS instance.
- *Scenario 4: Allow your instance to access specified external IP addresses only*

  You can configure security group rules to allow your instance to access specified external IP addresses only.
- *Scenario 5: Deny your instance to access specified external IP addresses*

  You can configure security group settings to deny your instance to access specified external IP addresses.
- *Scenario 6: Allow remote access to your instance through the Internet*

  You can remotely connect to your ECS instance through the Internet.
- *Scenario 7: Allow an ECS instance in a security group under another account in the same intranet to remotely connect to your instance*

  You can remotely connect to your instance by using an ECS instance in a security group under another account in the same intranet.
- *Scenario 8: Allow access to your instance through HTTP and HTTPS*

  If you host a website on your instance, you can add security group rules to allow your users to access the website through HTTP or HTTPS.

Scenario 1: Establish intranet communication between two instances in the same region and under the same account

For two instances in the same region and under the same account:

- If the two instances are in the same security group, they can communicate with each other. Configuration is not required.
- If the two instances are in different security groups, they cannot communicate with each other. You can add a rule to the security groups respectively to authorize the instances in the security groups to access each other through the intranet. Security rule settings vary among different network types, as shown in the following table.

Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Priority	Authorization type	Authorization object
VPC	Configuration is not required.	Inbound	Allow	Set the applicable protocol.	Set the port range.	1	Security group access (authorize this account).	Select the ID of the security group in which the allowed instance is located.
Classic network	Intranet							

Note:

For ECS instances that belong to a VPC, if they are in the same VPC, you can configure their security group rules to establish intranet communication. If they are in different VPCs (regardless of whether they belong to the same account or in the same region), you can use Express Connect to establish VPC communication. For more information, see *Connect two VPCs under different accounts*.

Scenario 2: Establish intranet communication between two instances in the same region and under different accounts

This scenario applies only to ECS instances in a classic network.

For example, User A owns an ECS instance in a classic network in China East 1, named Instance A (The intranet IP address is A.A.A.A), which belongs to a security group named Group A.

User B owns an ECS instance in a classic network in China East 1, named Instance B (The intranet IP address is B.B.B.B), which belongs to a security group named Group B.

You must add security group rules in Group A and Group B to authorize intranet communication between Instance A and Instance B.

- Add a rule to Group A to authorize Instance B to access Instance A. The rule settings are described in the following table.

NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
Intranet	Inbound	Allow	Select the applicable protocol type.	Set the port range.	Security group access (authorize other accounts).	The ID of Group B. Enter the User B's ID specified in Account ID.	1

- Add a rule to Group B to authorize Instance A to access Instance B. The rule settings are described in the following table.

NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
Intranet	Inbound	Allow	Select the applicable protocol type.	Set the port range.	Security group access (authorize other accounts).	The ID of Group A. Enter the User A's ID specified in Account ID.	1

Note:

To guarantee instance security, when you set an intranet inbound rule for the classic network, Security Group Access is preferred for the authorization type. If you select CIDR block Access, only a single IP address can be authorized, and the authorization object must be in the format of `a . b . c . d / 32`. The IP address can be set as needed, but the subnet mask must be /32.

Scenario 3: Allow remote access to your instance from only specified IP addresses

If you only want a specified IP address to remotely log on to your instance, add a rule to the security group to which your instance belongs by using the settings described in the following examples.

- Linux instance

Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
VPC	Configuration is not required.	Inbound	Allow	SSH (22)	22/22	CIDR block access	The IP address that allows remote access (for example, 1.2.3.4/32 or 10.0.0.0/8)	1
Classic network	Internet							

- Windows instance

Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
VPC	Configuration is not required.	Inbound	Allow	RDP (3389)	3389/3389	CIDR block access	The IP address that allows remote access (for example, 1.2.3.4/32 or 10.0.0.0/8)	1
Classic network	Internet							

Scenario 4: Allow your instance to access specified external IP addresses only

If you only want your instance to access only a specified IP address, add a rule to the security group to which your instance belongs by using the settings described in the following examples.

- To deny your instance to access all Internet IP addresses through any protocol, set a priority lower than the priority of the security group rule that allows access to Internet IP addresses. In this example, set the priority to 2. The security group rule settings are described in the following table.

Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
VPC	Configuration is not required.	Outbound	Deny	All	-1/-1	CIDR block access	0.0.0.0/0	2
Classic network	Internet							

- To allow your instance to access specified Internet IP addresses, set a priority higher than the priority of the security group rule used to deny access to Internet IP addresses. In this example, set the priority to 1.

Network Type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
VPC	Configuration is not required.	Outbound	Allow	Select the applicable protocol type.	Set the port range.	CIDR block access	The specified Internet IP address that you allow to be accessed by your instance (for example, 1.2.3.4/32 or 10.0.0.0/8)	1
Classic network	Internet							

After adding a security group rule, connect to the instance, and then conduct a `ping` or `telnet` test. If the instance can access only the allowed IP address, it means that the security group rule takes effect.

Scenario 5: Deny your instance to access specified external IP addresses

If you do not want your instance to access a specified external IP address, add a rule to the security group to which your instance belongs by using the settings described in the following tables.

Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
VPC	Configuration is not required.	Outbound	Deny	All	-1/-1	CIDR block access	The specified Internet IP address that you deny to be accessed by your instance (for example, 1.2.3.4/32 or 10.0.0.0/8)	1
Classic network	Internet							

Scenario 6: Allow remote access to your instance through the Internet

To allow remote access to your instance through the Internet, add the security group rule described in the following table.

Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
VPC	Configuration is not required.	Inbound	Allow	Windows: RDP (3389)	3389/3389	CIDR block access	If you allow all Internet IP addresses to connect to your instance, enter 0.0.0.0/0. If you only allow specified IP addresses to remotely connect to your instance, see *Scenario 3: Allow remote access to your instance from specified IP addresses only*.	1
				Linux: SSH (22)	22/22			
				Custom TCP	Custom (for example, 8080/8080)			

Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
Classic network	Internet	Inbound	Allow	Windows: RDP (3389)	3389/3389	CIDR block access	If you allow all Internet IP addresses to connect to your instance, enter 0.0.0.0/0. If you only allow specified IP addresses to remotely connect to your instance, see *Scenario 3: Allow remote access to your instance from only specified IP addresses*.	1
				Linux: SSH (22)	22/22			
				Custom TCP	Custom (for example, 8080/8080)			

For information about how to customize remote access ports, see *Modify the default remote access port*.

Scenario 7: Allow an ECS instance in a security group under another account in the same intranet to remotely connect to your instance

If your account is in the same intranet as another account in the same region, and you want to allow remote access to an ECS instance in a security group of that account, add a security group rule by using the settings described in the following examples.

- To allow an intranet IP address of an instance under another account to connect to your instance, add the security group rule described in the following table. For VPC instances, ensure that the instances under the two accounts can communicate with each other through Express Connect before you add a security group rule. For more information, see *Interconnect two VPCs under the same account*.

Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
VPC	Configuration is not required.	Inbound	Allow	Windows: RDP (3389)	3389/3389	CIDR block access	The private IP address of the peer instance	1
				Linux: SSH (22)	22/22			
				Custom TCP	Custom, for example, 8080/8080			

Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
Classic network	Intranet	Inbound	Allow	Windows: RDP (3389)	3389/3389	CIDR block access	The intranet IP address of the peer instance. For security purposes, only single IP address authorization is supported (for example, a.b.c.d/32).	1
				Linux: SSH (22)	22/22			
				Custom TCP	Custom, for example, 8080/8080			

- To allow all ECS instances in a security group under another intranet account to connect to your instance, add the security group rule described in the following table. For VPC instances, ensure that the instances under the two accounts can

communicate with each other through Express Connect before you add a security group rule. For more information, see *Connect two VPCs under the same account*.

Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
VPC	Configuration is not required.	Inbound	Allow	Windows: RDP (3389)	3389/3389	Security group access (authorize other accounts)	The ID of the security group to which the peer instance belongs. Enter the ID of the peer account.	1
				Linux: SSH (22)	22/22			
				Custom TCP	Custom, for example, 8080/8080			
Classic network	Intranet	Inbound	Allow	Windows: RDP (3389)	3389/3389	Security group access (authorize other accounts).	The ID of the security group to which the peer instance belongs. Enter the ID of the peer account.	1
				Linux: SSH (22)	22/22			
				Custom TCP	Custom (for example, 8080/8080)			

Scenario 8: Allow access to your instance through HTTP and HTTPS

If you host a website on your instance, you can add a security group rule to allow your users to access the website through HTTP or HTTPS.

- To allow all Internet IP addresses to access your website, add the security rule described in the following table.

Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
VPC	Configuration is not required.	Inbound	Allow	HTTP (80)	80/80	CIDR block access	0.0.0.0/0	1
				HTTPS (443)	443/443			
				Custom TCP	Custom (for example, 8080/8080)			
Classic network	Internet	Inbound	Allow	HTTP (80)	80/80	CIDR block access	0.0.0.0/0	1
				HTTPS (443)	443/443			
				Custom TCP	Custom, for example, 8080/8080			

- To allow specified Internet IP addresses to access your website, add the security group rule described in the following table.

Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
VPC	Configuration is not required.	Inbound	Allow	HTTP (80)	80/80	CIDR block access	One or more Internet IP addresses of the hosts that you allow to access your website	1
				HTTPS (443)	443/443			
				Custom TCP	Custom (for example, 8080/8080)			
Classic network	Internet	Inbound	Allow	HTTP (80)	80/80	CIDR block access	One or more Internet IP addresses of the hosts that you allow to access your website	1
				HTTPS (443)	443/443			
				Custom TCP	Custom (for example, 8080/8080)			

Note:

- If your users cannot access your instance by using the `http :// Internet IP address`, *verify if TCP port 80 works properly*.

- Port 80 is the default port for the HTTP service. If you want to use another port (for example, port 8080), you must modify the listening port settings in the configuration file of the Web server.

1.4 Typical applications of commonly used ports

This topic describes commonly used ports of ECS instances and the typical applications of these ports.

Commonly used ports

Port	Service	Description
21	FTP	A port opened to the FTP service. The port is used to upload and download files.
22	SSH	SSH port, which is used to *connect to a Linux instance by using a password* in the command line mode.
23	Telnet	Telnet port, which is used to telnet to the ECS instance.
25	SMTP	A port opened to the SMTP service. The port is used to send emails. For security purposes, ECS instances are disabled to access port 25. If you want to enable ECS instances to access this port, see *Apply to enable TCP port 25*.
80	HTTP	This port provides access to HTTP services, such as IIS, Apache, and Nginx. For more information, see *Verify if TCP port 80 works properly*.
110	POP3	This port is used for the POP3 protocol to send and receive emails.
143	IMAP	This port is used for the IMAP protocol to receive emails.
443	HTTPS	This port is used to provide access to the HTTPS service. HTTPS is a protocol that provides encryption and transmission through secure ports.

Port	Service	Description
1433	SQL Server	The TCP port of the SQL Server. This port is used for the SQL Server to provide external services.
1434	SQL Server	The UDP port of the SQL Server. This port is used to return which TCP/IP port the SQL Server uses.
1521	Oracle	An Oracle communication port. This port needs to be enabled when Oracle SQL is deployed on the ECS instance.
3306	MySQL	The port through which the MySQL database provides external services.
3389	Windows Server Remote Desktop Services	This port is used to *connect to a Windows instance*.
8080	Proxy port	Similar to port 80, port 8080 is used by WWW agents to browse webpages. If you use port 8080 to access a website or use a proxy server, you must add `: 8080` after the IP address. If you install the Apache Tomcat service, the default service port is 8080.
137, 138, and 139	NetBIOS protocol	· Ports 137 and 138 are UDP ports used to transfer files through the network neighbor. · Port 139 provides access to the NetBIOS/SMB service. The NetBIOS protocol is often used for Windows files, printer sharing, and Samba.

Typical applications of commonly used ports

Scenario	Network type	NIC	Rule direct	Autho policy	Proto type	Port range	Autho ion type	Autho ion objec	Priority
Remote access to Linux instances through SSH	VPC	Configuration is not required.	Inbound	Allow	SSH (22)	22/22	Address field access	0.0.0.0/0	1
	Classic network	Internet							

Scenario	Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
Remote access to Windows instances through RDP	VPC	Configuration is not required.	Inbound	Allow	RDP (3389)	3389/3389	Address field access	0.0.0.0/0	1
	Classic network	Internet							
Ping ECS instances through the Internet	VPC	Configuration is not required.	Inbound	Allow	ICMP	-1/-1	Address field access or security group access	Set this parameter according to the authorization type.	1
	Classic network	Internet							
Use an ECS instance as a Web server.	VPC	Configuration is not required.	Inbound	Allow	HTTP (80)	80/80	Address field access	0.0.0.0/0	1
	Classic network	Internet							
Upload or download files through FTP.	VPC	Configuration is not required.	Inbound	Allow	Custom TCP	20/21	Address field access	0.0.0.0/0	1
	Classic network	Internet							

Note:

- Some operators consider ports 135, 139, 444, 445, 5800, and 5900 as high-risk ports and block these ports by default. Therefore, even if the ports are enabled for ECS instances, the ports cannot be accessed in some regions. We recommend that you use non-high-risk ports to meet your specific service needs.
- For more information about Windows instance service ports, see *Service overview and network port requirements for Windows*.

1.5 Create a security group

In the default security group, the default rules only apply to the incoming ICMP traffic and the incoming access to SSH port 22, RDP port 3389, HTTP port 80, and HTTPS port 443. Moreover, the default rules vary according to the network type of the security group. If you do not want to add your instance to the default security group, you can create a custom security group.

Context

Each ECS instance must join at least one security group. For more information, see *Security groups*.

If you did not create a security group before creating an instance, you can use the default security group. For more information, see *Default security group rules*.

Prerequisites

If you want to create a security group for a VPC, you must first *create a VPC and a vSwitch*.

> Note:
> If you create a security group in a VPC, you can use that security group together with different vSwitches in that VPC. However, you cannot use that security group in other VPCs.

Procedure

1. Log on to the *ECS console*.
2. In the left-side navigation pane, choose Network and Security > Security Groups.
3. Select a region.
4. Click Create Security Group.
5. In the displayed Create Security Group dialog box, complete the following configurations:
   - Template: Select a template according to the services deployed in the instances inside the security group. Templates are designed to simplify the configuration of security group rules. The following table describes how templates can be applied to various scenarios.

Scenario	Template	Description

Web services need to be deployed in Linux instances in the security group.	Web Server Linux	By default, incoming access to TCP ports 80 /443/22 and incoming ICMP traffic are allowed.
Web services need to be deployed in Windows instances in the security group.	Web Server Windows	By default, incoming access to TCP ports 80/ 443/3389 and incoming ICMP traffic are allowed.
No special requirements	Custom	After the security group is created, you can add security group rules according to your business needs. #unique_11

- Security Group Name: Enter a name for the security group.
- Description: Enter a description of the security group.
- Network Type:
  - To create a security group for a VPC, select VPC, and then select the target VPC.
  - To create a security group for the classic network, select Classic.

6. Click OK.

If you create a new security group without adding any rules, the default rules for both the Internet and intranet apply. Specifically, outbound access is allowed while inbound access is denied.

API operations

You can call #unique_29 to create a security group.

What to do next

- You can *add security group rules* to control the Internet- or intranet-based access of your ECS instances. For information about the ports commonly involved in security group rules, see *Introduction to common ECS instance ports*. For details about typical use cases, see *Typical applications of security group rules*.

1.6 Add security group rules

You can add security group rules to enable or disable access to and from the Internet or intranet for ECS instances in the security group.

- VPC: You only need to set inbound and outbound rules, and you do not need to create different rules for the Internet and intranet. The Internet access for VPC instance is realized through private NIC mapping. Therefore, you cannot see the Internet NIC inside the instance, and you can only set intranet rules in the security group. The rules apply to Internet and intranet access.
- Classic network: You must set outbound and inbound rules for the Internet and intranet respectively.

For a new security group without any rules, outbound traffic is allowed and inbound traffic is refused by default, over either the Internet or intranet. Therefore, we recommend that you only set rules to refuse outbound traffic or allow inbound traffic.

Changes to the security group rules automatically apply to ECS instances in the security group.

Prerequisites

You have created a security group. For more information, see *create a security group*.

You know which Internet or intranet requests need to be allowed or refused for your instance.

Procedure

1. Log on to the *ECS console*.
2. In the left-side navigation pane, select Networks and Security > Security Groups.
3. Select the target region.
4. Find the security group to add authorization rules and then, in the Actions column, click Add Rules.
5. On the Security Group Rules page, click Add Security Group Rule.

Note:
If you do not need to enable or disable all ports for all protocols, ICMP, or GRE, you can select Quick Rule Creation.

Protocol	SSH	telnet	HTTP	HTTPS	MS SQL

Port	22	23	80.	443	1433
Protocol	Oracle	MySQL	RDP	PostgreSQL	Redis
Port	1521	3306	3389	5432	6379

Note:
See step 6 for descriptions on each parameter configuration.

6. In the dialog box, set the following parameters:
   - NIC:
     - For a VPC-Cconnected security group, you do not need to select the NIC.

       Note:
       ■ If your instances can access the Internet, the rules work for both the Internet and intranet.
       ■ If your instances cannot access the Internet, the rules work for intranet only.
     - For a Classic network-connected security group, you must select Internet or Intranet.
   - Rule Direction:
     - Outbound: ECS instances access other ECS instances over intranet networks, or through Internet resources.
     - Inbound: Other ECS instances in the intranet and Internet resources access the ECS instance.
   - Action: Select Allow or Forbid.

     Note:
     Forbid policies discard the data packet without returning a response. If two security group rules overlap except the authorization policy, the Forbid rule takes priority over the Allow rule.
   - Protocol Type and Port Range: The port range setting is affected by the selected protocol type. The following table shows the relationship between protocol types and port ranges.

Protocol Type	Port Range	Scenarios

All	Shown as -1/-1, indicating all ports. You cannot modify it.	Used in scenarios where both applications are fully and mutually trusted.
All ICMP	Shown as -1/-1, indicating no port restriction. You cannot modify it.	Used to detect the instance network connection status by using `ping`.
All GRE	Shown as -1/-1, indicating no port restriction. You cannot modify it.	Used for VPN service.
Custom TCP Custom UDP	For custom port ranges, the valid port value is 1–65535, and the valid port range format is Start Port/End Port. A valid port range format must be used for one port. For example, use 80/80 to indicate port 80.	It can be used to allow or forbid one or several successive ports.
SSH	Shown as 22/22. After connecting to the ECS instance, you can modify the port number. For more information, see *default remote access port modifications*.	Used for SSH to connect to a Linux instance remotely.
TELNET	Shown as 23/23.	Used to remotely log on to instances by using Telnet.
HTTP	Shown as 80/80.	The instance is used as a server for a website or a web application.
HTTPS	Shown as 443/443.	The instance is used as a server for a website or a web application that supports HTTPS.

MS SQL	Shown as 1433/1433.	The instance is used as an MS SQL server.
Oracle	Shown as 1521/1521.	The instance is used as an Oracle SQL server.
MySQL	Shown as 3306/3306.	The instance is used as a MySQL server.
RDP	Shown as 3389/3389. After connecting to the ECS instance, you can modify the port number. For more information, see *default remote access port modifications*.	Used to remotely connect to Windows instances.
PostgreSQL	Shown as 5432/5432.	The instance is used as a PostgreSQL server.
Redis	Shown as 6379/6379.	The instance is used as a Redis server.

Note:
Port 25 is restricted by default and cannot be opened through security group rules. However, you can submit a ticket to *apply to open TCP port 25*. For more information, see *introduction to common ECS instance ports*.

- Authorization Type and Authorization Object: The authorization object affects the setting of authorization type. The following table shows the relationship between them.

Authorization Type	Authorization Object
Address field access	Use the IP or CIDR block format such as 10.0.0.0 or 192.168.0.0/24. Only IPv4 addresses are supported. 0.0.0.0/0 indicates all IP addresses.

Security group access	Only for intranet access. Authorize the instances in a security group under your account or another account to access the instances in this security group. - Authorize this account: Select a security group under your account. Both security groups must be in the same VPC. - Authorize another account: Enter the target security group ID and the account ID. On the Account Management > Security Settings, you can obtain the account ID. For VPC-Connected network instances, security group access works for private IP addresses only. If you want to authorize Internet IP address access, use address field access.

Note:
To guarantee the security of your instance, when you are configuring an intranet inbound rule for a classic network-connected security group, Security Group Access is the top priority for Authorization Type. If you select Address Field Access, and you want to type an IP address in the CIDR format, type an IP address in the format of a.b.c.d/32. Only 32 is the valid CIDR prefix.

- Priority: The value range is 1-100. The smaller the value, the higher the priority. For more information, see *#unique_11/unique_11_Connect_42_priority*.

7. Click OK.

Security group rules generally take effect immediately.

Verify security group rules

If you have installed a web service on the instance and added a security group rule in a security group, you can allow all IP addresses to have inbound access to TCP port 80 of the instance. Follow these steps according to your instance OS to verify the security group rule.

Linux instances:

For a Linux instance in the security group, follow these steps to verify the security group rule:

1. *#unique_23*.
2. Run the following command to check whether TCP 80 is being listened.

```
netstat -an | grep 80
```

If the following result returns, web service for TCP port 80 is enabled.

```
tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN
```

3. Enter `http://public IP address of the instance` into your browser. If access is successful, the rules have been activated.

Windows instances:

For a Windows instance in the security group, follow these steps to verify the security group rule:

1. *#unique_24*.
2. Run the CMD, and run the following command to check whether TCP port 80 is being listened.

```
netstat -aon | findstr :80
```

If the following result returns, web service for TCP port 80 is enabled.

```
TCP 0.5.0.0:80 0.5.0.0:0 listening 1172
```

3. Enter `http://instance public IP address` into your browser. If access is successful, the rules have been activated.

ECS security group rule priority explanation

The Priority value of a security group rule ranges from 1 to 100. A smaller number indicates a higher priority.

ECS instances can belong to different security groups. As a result, instances may have multiple security group rules that have the same protocol types, port ranges, authorization types, and authorization objects. The rule that takes effect depends on the setting of Priority and Authorization Policy:

- If the rules have the same Priority, the Forbid rule takes effect over the Allow rule.

- If the rules have different Priority, the rule with the higher priority takes effect first, regardless of the setting of Authorization Policy .

Related topics

- *Security group FAQ*
- *Security groups*
- *#unique_27*
- *Implication and matching sequence of the ECS security group rule priority*

1.7 Add an instance to a security group

You can add an ECS instance to one or more security groups according to your business needs. By default, an ECS instance can join up to five security groups.

Context

Security groups are an important means for network security isolation. They are used to set network access control for one or more ECS instances. Each instance must belong to at least one security group.

Prerequisites

- You have *created an ECS instance*.
- Classic network instances must join a security group of the classic network in the same region.
- VPC instances must join a security group in the same VPC.

Procedure

1. Log on to the *ECS console*.
2. In the left-side navigation pane, click Instances.
3. Select a region.
4. Select the target instance on the Instances page. Click Manage in the Actions column.
5. Click Security Groups.
6. Click Add to Security Group.

7. Select the security group to which the instance will be added. If you need to add the instance to multiple security groups, select a security group and then click Join multiple security groups. A selection box appears that shows the selected security groups.

8. Click OK.

After the instance is added to a security group, the rules of that security group apply to the instance automatically.

API operations

You can use the *JoinSecurityGroup* interface to add an instance to a specified security group.

What to do next

- If you want to view all the security groups that you have created under a region, you can *view the security group list*.
- If you want to modify the name and description of a security group, you can *modify security group attributes*.
- If you want to remove an instance from one or more security groups, you can *remove an instance from a security group*. If an instance is removed from a security group, it can no longer communicate with other instances in that group through the intranet. Therefore, we recommend that you test your running environment before removing the instance to ensure that your services can continue to run normally.
- If you no longer need one or more security groups, you can *delete security groups*. Deleting a security group will delete all its rules.

1.8 Manage security groups

This topic describes how to manage security groups. After you create security groups, you can query, modify, clone, remove, and delete them.

Query security groups

1. Log on to the *ECS console*.
2. In the left-side navigation pane, click Security Groups.

3. Select the target region. A list of all security groups in the region is displayed.
4. Optional. Query the security groups as needed.
   - To query a security group by using its ID, enter the ID in the Security Group ID text box.
   - To query all security groups in a VPC, enter its ID in the VPC ID text box.
   - To query a security group by using its name, enter the name in the Security Group Name text box.

   You can also call the API *DescribeSecurityGroups* to query the basic information of security groups.

Modify a security group

1. Log on to the *ECS console*.
2. In the left-side navigation pane, click Security Groups.
3. Select the target region.
4. Locate the target security group, and then click Modify in the Actions column.
5. Modify the Security Group Nameand Description.
6. Click OK.

   You can also call the API *ModifySecurityGroupAttribute* to modify the name and description of a security group.

Clone a security group

1. Log on to the *ECS console*.
2. In the left-side navigation pane, click Security Groups.
3. Select the target region.
4. Locate the target security group, and then click Clone Security Group in the Actions column.

5. In the Clone Security Group dialog box, set the parameters of the new security group.
   - Target Region: Select the specific region in which the new security group applies. Not all regions are supported. The supported regions are displayed in the console.
   - Security Group Name: Specify a name for the new security group.
   - Network Type: Select a network type that applies to the new security group. If you select VPC, you must select an available VPC in the target region.
6. Click OK.

Remove an instance from a security group

1. Log on to the *ECS console*.
2. In the left-side navigation pane, click Instances.
3. Select the target region.
4. On the Instances page, locate the target instance, and then click Manage in the Actions column.
5. Click Security Groups.
6. Locate the target security group, and then click Remove in the Actions column.
7. Click OK.

You can also call the API *LeaveSecurityGroup* to remove an instance from a specified security group.

Delete a security group

1. Log on to the *ECS console*.
2. In the left-side navigation pane, choose Networks and Security > Security Groups.
3. Select the target region.
4. Select one or more security groups, and then click the Delete button in the bottom left corner of the list.
5. In the Delete Security Group dialog box, click OK.

You can also call the API *#unique_44* to delete a security group.

1.9 Manage security group rules

This topic describes how to manage security group rules. After you add security group rules, you can query, modify, restore, export, import, and delete them.

Query security group rules

Prerequisites

You have added rules to your security groups. For more information, see *Add security group rules*.

Procedure

1. Log on to the *ECS console*.
2. In the left-side navigation pane, click Security Groups.
3. Select the target region.
4. Locate the target security group, and then click Add Rules in the Actions column.
5. Click a rule direction to query the corresponding security group rules.
   - If you need to query security group rules for a VPC, select Ingress or Outbound.
   - If you need to query security group rules for a classic network, select Internal Network Ingress, Internal Network Egress, Internet Ingress, or Internet Egress.

You can also call the API *DescribeSecurityGroupAttribute* to query security group rules.

Modify security group rules

Context

If security group rules do not limit access to certain ports, serious security risks may occur. You can modify inappropriate rules to ensure the security of your ECS instances.

Prerequisites

You have created a security group and added security group rules to the security group. For more information, see *Create a security group* and *add security group rules*.

Procedure

1. Log on to the *ECS console*.
2. In the left-side navigation pane, click Security Groups.
3. Select the target region.

4. On the Security Groups page, locate the target security group, and then click Add Rules in the Actions column.
5. Click a rule direction of the security group.
   - If you need to modify security group rules for a VPC, select Ingress or Outbound.
   - If you need to modify the security group rules for a classic network, select Internal Network Ingress, Internal Network Egress, Internet Ingress, or Internet Egress.
6. Locate the target security group rule, and click Modify in the Actions column. For information about how to configure security group rules, see *Add security group rules*. For information about how to use security group rules, see *Typical applications of security group rules*.

Restore security group rules

Context

Restoring security group rules means to restore all or some of the rules in a security group to those rules in the target security group.

- Complete restoration: The system deletes the rules that are not in the target security group from the source security group and adds the rules that are only in the target security group to the source security group. After restoration is finished, the rules in the source security group are identical to those in the target security group.
- Partial restoration: The system adds the rules that are only in the target security group to the source security group and ignores the rules that are only in the source security group.

Limits

- The source security group and the target security group must be in the same region .
- The source security group and the target security group must be of the same network type.
- If there are system-level security group rules (with a priority level of 110) in the target security group, these rules cannot be restored. After restoration, the rules in the source security group may be different from expected. If you need the system-level security group rules, you can create similar rules with a priority level of 100.

Prerequisites

You must have at least one security group of the same network type in the same region.

Procedure

1. Log on to the *ECS console*.
2. In the left-side navigation pane, click Security Groups.
3. Select the target region.
4. Locate the security group whose rules you want to restore (this security group serves as the source security group), and then click Restore Rules in the Actions column.
5. In the Restore rules dialog box, perform the following operations as needed:
   a. Select the Target Security Group, which must have different rules from the source security group.
   b. Select a Method.
      - If you want the source security group to have the same rules as the target security group, select Completely Restore.
      - If you want to add the rules that only exist in the target security group to the source security group, select Partially Restore.
   c. Preview the restoration result.
      - The rules highlighted in green only exist in the target security group. These rules are added to the source security group regardless of whether you select Completely Restore or Partially Restore.
      - The rules highlighted in red do not exist in the target security group. If you select Completely Restore, these rules are deleted from the source security group. If you select Partially Restore, these rules are retained in the source security group.
   d. Click OK.

   After restoration, the Restore Rules dialog box is closed automatically. On the Security Groups page, locate the source security group, and then click Add Rules in the Actions column to open the Security Group Rules page and view the updated security group rules.

Export security group rules

1. Log on to the *ECS console*.
2. In the left-side navigation pane, click Security Groups.
3. Select the target region.
4. On the Security Groups page, locate the target security group, and then click Add Rules in the Actions column.
5. Click Export Rules to download and save the security group rules to a local JSON file.

> **Note:**
> The JSON file name uses the following format:
>
> `ecs_ ${ region_id } _ ${ groupID }. json`
>
> If `regionID` is `cn - qingdao` and `groupID` is `sg - 123` , then the name of the exported JSON file is `ecs_cn - qingdao_sg - 123 . json` .

Import security group rules

1. Log on to the *ECS console*.
2. In the left-side navigation pane, click Security Groups.
3. Select the target region.

> **Note:**
> You can import security group rules from different regions.

4. On the Security Groups page, locate the target security group, and then click Add Rules in the Actions column.
5. Click Import Rules.
6. Select the target JSON file. You can preview the rules in the file.

   The preview displays the following information:

   - The number of rules to be imported.
   - File check results. If any rule that may cause import failure exists in the JSON file, you can move the point over the warning icon for details.
   - Details of the rules to be imported.

> **Note:**

> Up to 100 security group rules can be imported. The excessive rules cannot be imported. The newly imported rules do not overwrite the existing rules.

7. Click Start.
8. View the import result, and then click Finish and close.

Delete security group rules

1. Log on to the *ECS console*.
2. In the left-side navigation pane, click Security Groups.
3. Select the target region.
4. Locate the target security group, and then click the Add Rules in the Actions column.
5. Click a rule direction of the security group.
   - If you need to delete security group rules for a VPC, select Ingress or Outbound.
   - If you need to delete the security group rules for a classic network, select Internal Network Ingress, Internal Network Egress, Internet Ingress, or Internet Egress.
6. Locate the target security group rule, and then click Delete in the Actions column.
7. In the Delete Security Group Rule dialog box, click OK.

You can also call the API *RevokeSecurityGroup* to delete an ingress security group rule or call the API *RevokeSecurityGroupEgress* to delete an outbound security group rule.

1.10 Security group FAQ

- *What is a security group?*
- *Why do I need to select a security group when I create an ECS instance?*
- *Why am I unable to set Internet security group rules for a VPC instance?*
- *Why am I unable to access TCP port 25?*
- *Why am I unable to access port 80?*
- *Why have several rules been added to a security group automatically?*
- *Why is the priority of some security group rules 110?*
- *Why am I prompted that the number of rules has exceeded the limit when I add an instance to a security group?*
- *What should I do if I create an ECS instance before I create a security group?*

What is a security group?

A security group is a virtual firewall that is used to set the network access control for one or more ECS instances. More specifically, security groups logically isolate security domains in the cloud.

Each instance must belong to at least one security group, which is specified when you create an instance. Instances in the same security group can communicate through the intranet. In contrast, instances in different security groups are isolated from each other. However, you can set security group rules to authorize mutual access between two security groups. For more information, see *Security group overview*.

Why do I need to select a security group when I create an ECS instance?

When you purchase an ECS instance, you must select a security group to divide the security domains of the application environment and set security group rules for proper network security isolation.

If you do not select a security group, all the ECS instances that you have created are assigned to the default security group. As a result, you will need to remove instances from the default security group and add them to a new security group.

Why am I unable to set Internet security group rules for a VPC instance?

You are unable to set Internet security group rules for a instance in a VPC because VPC instances can only access the Internet through intranet NIC mapping, which makes the Internet NIC invisible to your instance. As a result, you can only set intranet rules in the security group. The security group rules apply to the intranet and the Internet.

Why am I unable to access TCP port 25?

TCP port 25 is the default email service port. For security purposes, port 25 of ECS is disabled by default. We recommend that you use port 465 instead to send emails. For more information, see *Scenarios*.

Why am I unable to access port 80?

See *Verify if TCP port 80 works properly*.

Why have several rules been added to my security group automatically?

Several rules were added to your security group automatically likely due to one of the following two scenarios:

- If you have accessed DMS, the relevant rules are automatically added to the security group. .
- If you have migrated data by using Alibaba Cloud Data Transmission Service (DTS), the security group will automatically add the rules relating to the IP address of the DTS service.

Why is the priority of some security group rules 110?

The security group rules whose priority is 110 are the default rules created by the system. The priority of such default rules is always lower than that of any manually added security group rules. When you manually add security group rules, you can only set the priority to a value ranging from 1 to 100.

Why am I prompted that the number of rules has exceeded the limit when I add an instance to a security group?

Maximum number of security group rules of an instance (primary ENI) = number of security groups that the instance can join × maximum number of rules of each security group.

If you are prompted that the number of rules has exceeded the limit, it means that the number of security group rules applied to the instance has exceeded the upper limit.

What should I do if I create an ECS instance before I create a security group?

If you have not created a security group before you create an ECS instance, you can select the default security group. The default security group allows commonly used ports, such as TCP port 22 and port 3389. For more information, see *Default security group rules*.

What happens when a security group is configured incorrectly?

If a security group is configured incorrectly, mutual access between the ECS instance and other devices through the private network or the Internet will fail. For example:

- Linux instances cannot be accessed remotely through SSH, or Windows instances cannot be accessed through the remote desktop.
- The Internet IP address of the ECS instance cannot be pinged.
- The Web service provided by the ECS instance cannot be accessed through HTTP or HTTPS.
- Other ECS instances cannot be accessed through the intranet.

Are the inbound and outbound rules of a security group counted separately?

No, inbound rules and outbound rules of a security group are counted together. The total number of inbound rules and outbound rules for each security group cannot exceed 100.

Am I able to adjust the maximum number of security group rules allowed?

No, the maximum number of security group rules cannot be changed. Each security group can contain only a maximum of 100 security group rules. If the maximum number of instances cannot meet your needs, follow these steps:

1. Check whether redundant rules exist. You can also *open a ticket* for Alibaba Cloud technical support.
2. If any redundant rules exist, clear the redundant rules. If no redundant rules exist, you can create multiple security groups.

 Note:
By default, each ENI of an instance can be added to up to five security groups. Therefore, each ENI of an instance can contain up to 500 security group rules. This is sufficient for most scenarios.

If I adjust the maximum number of security groups for a VPC instance, does the adjustment apply only to the security groups that I add after the adjustment date?

No, the adjustment applies to the security groups of all VPC instances created before and after the adjustment date.

2 Key pairs

2.1 SSH key pair overview

What is an SSH key pair?

An SSH key pair, or key pair for short, is a secure authentication method provided by Alibaba Cloud for remote logon to your Linux instance. It is an alternative to authentication using a username and password.

The key pair is composed of a public key and a private key. The asymmetric cryptography feature uses the public key to encrypt data, and the local client uses the private key to decrypt the data.

The Linux ECS instance stores the public key. You use the private key to connect to your instance by entering SSH commands or using other tools. Username and password authentication is disabled by ECS once the SSH key pair is enabled to guarantee security.

Benefits

Compared with typical username and password authentication, SSH key pair has the following benefits:

High security

Using an SSH key pair to log on to a Linux instance is more secure and reliable.

- A key pair prevents brute force attacks targeted at password cracking.
- Due to the complexity of RSA encryption, the private key cannot be deduced even if the public key is maliciously acquired.

Ease of use

- You can log on remotely to an instance by configuring the key pair in the ECS console and on the local client, meaning you do not need to enter a password every time you log on.
- We recommend this method if you maintain multiple ECS instances.

Limits

Using an SSH key pair has the following restrictions:

- Applies only to Linux instances.
- Alibaba Cloud only supports the creation of 2048-bit RSA key pairs.
  - Alibaba Cloud holds the public key of the key pair.
  - After the key pair is created, you must download and securely store the private key.
  - The private key is in the unencrypted PEM-encoded `PKCS # 8` format.
- Each Alibaba Cloud account can have a maximum of 500 key pairs per region.
- Only one SSH key pair can be added to a Linux instance at a time. If a key pair has already been added to your instance, the new key pair replaces the old one.
- During the lifecycle of a Linux instance, you can add or remove an SSH key pair at any time. After you add or remove a key pair, you must *restart the instance* for the change to take effect.
- All instances of any *instance type family*, except for the I/O optimized-instances of Generation I, support SSH key pairs.

Create an SSH key pair

To create an SSH key pair, you can use either of the following methods:

- *Create an SSH key pair* in the ECS console.

Note:

Once you create a key pair in the ECS console, you must immediately download and securely store the private key for later use. If SSH key pair authentication is enabled for an ECS instance, you cannot log on to the ECS instance without the private key of the key pair.

- Create an SSH key pair by using other key pair builders and *import it* to ECS.

  The following key types are supported:

  - rsa
  - dsa
  - ssh-rsa
  - ssh-dss
  - ecdsa
  - ssh-rsa-cert-v00@openssh.com
  - ssh-dss-cert-v00@openssh.com
  - ssh-rsa-cert-v01@openssh.com
  - ssh-dss-cert-v01@openssh.com
  - ecdsa-sha2-nistp256-cert-v01@openssh.com
  - ecdsa-sha2-nistp384-cert-v01@openssh.com
  - ecdsa-sha2-nistp521-cert-v01@openssh.com

2.2 How do I use an SSH key pair?

This topic describes how to use an SSH key pair in the ECS console. Note that only Linux instances support an SSH key pair.

Create an SSH key pair

1. Log on to the ECS console.
2. In the left-side navigation pane, choose Networks and Security > SSH Key Pair.
3. Select the target region.
4. Click Create SSH Key Pair.
5. Enter a name for the SSH key pair, and then select Auto-Create SSH Key Pair.

   Note:
   Do not enter an SSH key pair name that already exists. Otherwise, the ECS console prompts you that the key already exists.
6. Click OK to create the SSH key pair.

   Note:

- After an SSH key pair is created, we recommend that you immediately download and securely save the private key.
- Each Alibaba account can have up to 500 SSH key pairs in each region.

Related API: *CreateKeyPair*

View public key information

For Windows:

1. Start PuTTYgen.
2. Click Load.
3. Select the *.ppk* or *.pem* file.

PuTTYgen shows the public key information.

For Linux or Mac:

Run the `ssh-keygen` command and specify the path of the *.pem* file.

```
ssh-keygen -y -f /path_to_key_pair/my-key-pair.pem
```

The returned public key information is as follows:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDdlrdZwV3+
GF9q7rhc6v YrExwT4WU4 fsaRcVXGV2 Mg9RHex21h l1au77Gkmn
IgukBZjywl QOT4GDdsJy 2nBOdJPrCE BIP6t0Mk5a PkK/fctNuKjcmM
MOA8YUT+sJKn3l7rCL kesE+S5880yNdRj BiiUy40kyr 7Y+fqGVdSOHGM
XZQPpkBtoj cV14uAy0yV 6/htEqGa/Jq4fH7bR6C YQ2XgH/hCap29Mdi
/G5Tx1nbUKu IHdMWOPvjG ACGcXclex+lHtTGiAIRG 1riyNRVC47
ZEVCxxxxxx
```

Note:
If the execution of this command fails, run the `chmod 400 my-key-pair.pem` command to change the ownership to you only.

View public key information within an instance

A public key is stored in the `~/.ssh/authorized_keys` file. Opening that file in an instance returns public key information.

Import an SSH key pair

In addition to creating an SSH key pair in the ECS console, you can also use a tool to generate an SSH key pair and import the public key to Alibaba Cloud.

 Note:
You must securely save the private key. Do not import the private key to Alibaba Cloud. Otherwise, your account security may be compromised.

An imported public key must be `Base64` encoded and must support any of the following encryption methods:

- rsa
- dsa
- ssh-rsa
- ssh-dss
- ecdsa
- ssh-rsa-cert-v00@openssh.com
- ssh-dss-cert-v00@openssh.com
- ssh-rsa-cert-v01@openssh.com
- ssh-dss-cert-v01@openssh.com
- ecdsa-sha2-nistp256-cert-v01@openssh.com
- ecdsa-sha2-nistp384-cert-v01@openssh.com
- ecdsa-sha2-nistp521-cert-v01@openssh.com

1. Obtain public key information. For more information, see ######.
2. Log on to the ECS console.
3. In the left-side navigation pane, choose Networks and Security > SSH Key Pair.
4. Select the target region.
5. Click Create SSH Key Pair.
6. Enter a name for the SSH key pair, select Import SSH Key Pair, and then enter public key information in the Public Key box.

    Note:
   Do not specify a name that is the same as an existing one or as one that is deleted while remains attached to an instance. Otherwise, the ECS console prompts you that the key already exists.
7. Click OK.

Related API: *ImportKeyPair*.

Attach an SSH key pair

You can attach an SSH key pair to an instance during or after instance creation.

> Note:
>
> - Each ECS instance can only be associated with one SSH key pair. If an ECS instance is already associated with an SSH key pair, the old key is automatically replaced with the new key.
> - If an ECS instance uses password authentication, the password authentication mode is automatically disabled after a key pair is associated with the instance. However, if you ###### after attaching a key pair to an instance, you can use both the password and the key pair to log on to the instance.

1. Log on to the ECS console.
2. In the left-side navigation pane, choose Networks and Security > SSH Key Pair.
3. Select the target region.
4. Find the target key pair, and click Bind in the Actions column.
5. In the Select Instance box, select the target ECS instance, and click > to move it to the Selected box.

   > Note:
   > If an ECS instance in the Select Instance box appears grey, it means that the instance is running Windows, which does not support usage of SSH key pairs.
6. Click OK.

   > Note:
   > If an ECS instance is in the Running state, you must restart it in the ECS console or by using the API to activate the key pair after attaching it to the instance.

After you attach an SSH key pair to an ECS instance, you can log on to that ECS instance by using the SSH key pair.

Related API: *AttachKeyPair*.

Detach an SSH key pair

1. Log on to the ECS console.
2. In the left-side navigation pane, choose Networks and Security > SSH Key Pair.
3. Select the target region.

4. Find the target key pair, and click Unbind in the Actions column.
5. In the Select Instance box, select the target ECS instance, and click > to move it to the Selected box.

   Note:
   If an ECS instance in the Select Instance box appears grey, it means that the instance is running Windows, which does not support usage of SSH key pairs.
6. Click OK.

   Note:

   - If an ECS instance is in the Running state, you must restart it in the ECS console or by using the API to complete the operation after detaching it from the instance.
   - If an instance password is reset before the detach operation, you can use the password to log on to the instance after the detach operation. Otherwise, after the detach operation, you must ###### before you can use a password to log on to the instance.

Related API: *DetachKeyPair*.

Add or replace a key pair in an instance

You can add multiple key pairs in an instance and use them to access that instance. You can also replace an existing key pair.

1. Retrieve the public key of a new key pair. For more information, see ######.
2. Use the existing key pair to log on to the ECS instance.
3. Run `vim . ssh / authorized _keys` to open the file.
4. Add or replace the public key.

   - Add a public key: Add a new public key below the existing public key, and save the file.

```
ssh - rsa  AAAAB3NzaC  1yc2EAAAAD  AQABAAABAQ  Cys3aOkFm1
Xh8iN0lije  QF5mz9Iw / FV / bUUduZjaui  Ja1KQJSF4 + czKtqMAv38
QEspiWStkS  fpTn1g9qeU  hfKd4uWlmx  eQ + XjPsf22fRe  m +
v7MHMa7KnZ  WiHJxO62D4  Ihvv2hKfsk  z8K44mVMeI  nMjGO +
u17IaL2l2r  i8q9YdvVHt  0Mw5TpCkER  WGoBPE1Y8v  xFb97TaE5 + zc
+ 2 + eff6PDCMkV  TP + c / feMeCxpx6L  hc2NEpHIPx  MpjOv1IytK
iDfWcezA2a  CmKre0Q2t / YudCmJ8HTC  nLId5Lpirb  NE4X08Bk7t
XZAU8UaoeD  dUr / FKB1Cxw1Tb  GMTfWBcdWk  dp2lv  imported -
openssh - key
```

```
ssh - rsa   AAAAB3NzaC  1yc2EAAAAD  AQABAAABAQ  DdlrdZwV3 +
GF9q7rhc6v  YrExwT4WU4  fsaRcVXGV2  Mg9RHex21h  l1au77Gkmn
IgukBZjywl  QOT4GDdsJy  2nBOdJPrCE  BIP6t0Mk5a  PkK / fctNuKjcmM
MOA8YUT + sJKn3l7rCL  kesE + S5880yNdRj  BiiUy40kyr  7Y +
fqGVdSOHGM  XZQPpkBtoj  cV14uAy0yV  6 / htEqGa / Jq4fH7bR6C
YQ2XgH / hCap29Mdi / G5Tx1nbUKu  IHdMWOPvjG  ACGcXclex +
lHtTGiAIRG  1riyNRVC47  ZEVCg9iTWW  GrWFvVlnI0  E3Deb /
9H9mPCO1Xt  2fxxxxxxxx  BtmR   imported - openssh - key
```

- Replace a public key: Delete the existing public key, add a new public key, and save the file.

```
ssh - rsa   AAAAB3NzaC  1yc2EAAAAD  AQABAAABAQ  DdlrdZwV3 +
GF9q7rhc6v  YrExwT4WU4  fsaRcVXGV2  Mg9RHex21h  l1au77Gkmn
IgukBZjywl  QOT4GDdsJy  2nBOdJPrCE  BIP6t0Mk5a  PkK / fctNuKjcmM
MOA8YUT + sJKn3l7rCL  kesE + S5880yNdRj  BiiUy40kyr  7Y +
fqGVdSOHGM  XZQPpkBtoj  cV14uAy0yV  6 / htEqGa / Jq4fH7bR6C
YQ2XgH / hCap29Mdi / G5Tx1nbUKu  IHdMWOPvjG  ACGcXclex +
lHtTGiAIRG  1riyNRVC47  ZEVCg9iTWW  GrWFvVlnI0  E3Deb /
9H9mPCO1Xt  2fxxxxxxxx  BtmR   imported - openssh - key
```

If you can use the new private key to log on to the ECS instance, the add or replace operation is completed successfully.

Delete an SSH key pair

An SSH key pair cannot be restored once it is deleted. However, the delete operation does not impact the instance that is using that key pair, and the instance details still show the name of the deleted key pair.

Note:

- If your key pair has been attached to an instance, and it is not detached from that instance before the deletion, you cannot create a key pair of the same name after the deletion. Otherwise, if you create or import such a key pair, the ECS console prompts you that the key pair already exists when you enter this key pair name.
- If your key pair is not attached to an instance, or is detached from an instance before the deletion, you can create a key pair of the same name after the deletion.

1. Log on to the ECS console.
2. In the left-side navigation pane, choose Networks and Security > SSH Key Pair.
3. Select the target region.
4. Select one or more key pairs to be deleted.
5. Click Delete.

Related API: *DeleteKeyPairs*.

3 Anti-DDoS Basic

Anti-DDoS Basic is a free Distributed Denial of Service (DDoS) protection service that safeguards data and applications on your ECS instance.

As a global service from Alibaba Cloud Security, Anti-DDoS Basic offers a mitigation capacity of 5 Gbit/s against common DDoS attacks. When the inbound traffic of an ECS instance exceeds its limits, which is determined by the ECS instance type, Alibaba Cloud Security enables throttling to maintain stable performance. For more information, see *Anti-DDoS Basic black hole threshold*.

How Anti-DDoS Basic works

When the Anti-DDoS Basic is enabled, Alibaba Cloud Security monitors the inbound traffic in real time. When massive traffic or abnormal traffic involving DDoS attacks is monitored, Alibaba Cloud Security redirects the traffic, removes malicious traffic, and passes clean traffic back to the target ECS instance. This process is called flow cleaning. For more information, see *Anti-DDoS Basic service - product architecture*.

 Note:
If Anti-DDoS Basic is enabled for an ECS instance, when the inbound traffic from Internet is higher than 5 Gbit/s, to secure the global cluster, Alibaba Cloud Security triggers a black hole to receive such traffic. For more information, see *Alibaba Cloud black hole policies*.

Factors that can trigger flow cleaning include:

- Attack types. When specified attacks are identified in the inbound traffic, flow cleaning is triggered.
- Traffic size. Generally, traffic involving DDoS attacks is measured in Gbit/s. When the inbound traffic into an ECS instance exceeds the specified threshold, flow cleaning is triggered no matter whether the traffic is normal or not.

Methods to clean traffic include filtering ICMP packets, limiting the bit rate, and limiting the packet forwarding rate.

Therefore, when using Anti-DDoS Basic, you must set the following thresholds:

- BPS threshold: When the inbound traffic exceeds the BPS threshold, flow cleaning is triggered.

- PPS threshold: When the inbound packet forwarding rate exceeds the PPS threshold, flow cleaning is triggered.

Cleaning thresholds of each instance type

The configuration of each instance type determines its maximum flow cleaning threshold. The following table lists the cleaning thresholds of some *available* and *phased-out* instance types.

Instance type	Maximum BPS threshold (Mbit/s)	Maximum PPS threshold (PPS)
ecs.g5.16xlarge	20,000	4,000,000
ecs.g5.22xlarge	30,000	4,500,000
ecs.g5.2xlarge	2,500	800,000
ecs.g5.4xlarge	5,000	1,000,000
ecs.g5.6xlarge	7,500	1,500,000
ecs.g5.8xlarge	10,000	2,000,000
ecs.g5.large	1,000	300,000
ecs.g5.xlarge	1,500	500,000
ecs.sn2ne. 14xlarge	10,000	4,500,000
ecs.sn2ne. 2xlarge	2,000	1,000,000
ecs.sn2ne. 4xlarge	3,000	1,600,000
ecs.sn2ne 8xlarge	6,000	2,500,000
ecs.sn2ne.large	1,000	300,000
ecs.sn2ne.xlarge	1,500	500,000
ecs.c5.16xlarge	20,000	4,000,000
ecs.c5.2xlarge	2,500	800,000
ecs.c5.4xlarge	5,000	1,000,000
ecs.c5.6xlarge	7,500	1,500,000
ecs.c5.8xlarge	10,000	2,000,000
ecs.c5.large	1,000	300,000
ecs.c5.xlarge	1,500	500,000
ecs.sn1ne. 2xlarge	2,000	1,000,000
ecs.sn1ne. 4xlarge	3,000	1,600,000

Instance type	Maximum BPS threshold (Mbit/s)	Maximum PPS threshold (PPS)
ecs.sn1ne. 8xlarge	6,000	2,500,000
ecs.sn1ne.large	1,000	300,000
ecs.sn1ne.xlarge	1,500	500,000
ecs.r5.16xlarge	20,000	4,000,000
ecs.r5.22xlarge	30,000	4,500,000
ecs.r5.2xlarge	2,500	800,000
ecs.r5.4xlarge	5,000	1,000,000
ecs.r5.6xlarge	7,500	1,500,000
ecs.r5.8xlarge	10,000	2,000,000
ecs.r5.large	1,000	300,000
ecs.r5.xlarge	1,500	500,000
ecs.re4.20xlarge	15,000	2,000,000
ecs.re4.40xlarge	30,000	4,000,000
ecs.se1ne. 14xlarge	10,000	4,500,000
ecs.se1ne. 2xlarge	2,000	1,000,000
ecs.se1ne. 4xlarge	3,000	1,600,000
ecs.se1ne. 8xlarge	6,000	2,500,000
ecs.se1ne.large	1,000	300,000
ecs.se1ne.xlarge	1,500	500,000
ecs.se1.14xlarge	10,000	1,200,000
ecs.se1.2xlarge	1,500	400,000
ecs.se1.4xlarge	3,000	500,000
ecs.se1.8xlarge	6,000	800,000
ecs.se1.large	500	100,000
ecs.d1ne. 2xlarge	6,000	1,000,000
ecs.d1ne. 4xlarge	12,000	1,600,000
ecs.d1ne. 6xlarge	16,000	2,000,000
ecs.d1ne. 8xlarge	20,000	2,500,000
ecs.d1ne. 14xlarge	35,000	4,500,000

Instance type	Maximum BPS threshold (Mbit/s)	Maximum PPS threshold (PPS)
ecs.d1.2xlarge	3,000	300,000
ecs.d1.4xlarge	6,000	600,000
ecs.d1.6xlarge	8,000	800,000
ecs.d1.8xlarge	10,000	1,000,000
ecs.d1-c8d3.8xlarge	10,000	1,000,000
ecs.d1.14xlarge	17,000	1,800,000
ecs.d1-c14d3.14xlarge	17,000	1,400,000
ecs.i2.xlarge	1,000	500,000
ecs.i2.2xlarge	2,000	1,000,000
ecs.i2.4xlarge	3,000	1,500,000
ecs.i2.8xlarge	6,000	2,000,000
ecs.i2.16xlarge	10,000	4,000,000
ecs.i1.xlarge	800	200,000
ecs.i1.2xlarge	1,500	400,000
ecs.i1.4xlarge	3,000	500,000
ecs.i1-c10d1.8xlarge	6,000	800,000
ecs.i1-c5d1.4xlarge	3,000	400,000
ecs.i1.14xlarge	10,000	1,200,000
ecs.hfc5.large	1,000	300,000
ecs.hfc5.xlarge	1,500	500,000
ecs.hfc5.2xlarge	2,000	1,000,000
ecs.hfc5.4xlarge	3,000	1,600,000
ecs.hfc5.6xlarge	4,500	2,000,000
ecs.hfc5.8xlarge	6,000	2,500,000
ecs.hfg5.large	1,000	300,000
ecs.hfg5.xlarge	1,500	500,000
ecs.hfg5.2xlarge	2,000	1,000,000
ecs.hfg5.4xlarge	3,000	1,600,000
ecs.hfg5.6xlarge	4,500	2,000,000

Instance type	Maximum BPS threshold (Mbit/s)	Maximum PPS threshold (PPS)
ecs.hfg5.8xlarge	6,000	2,500,000
ecs.hfg5.14xlarge	10,000	4,000,000
ecs.c4.2xlarge	3,000	400,000
ecs.c4.4xlarge	6,000	800,000
ecs.c4.xlarge	1,500	200,000
ecs.ce4.xlarge	1,500	200,000
ecs.cm4.4xlarge	6,000	800,000
ecs.cm4.6xlarge	10,000	1,200,000
ecs.cm4.xlarge	1,500	200,000
ecs.gn5-c28g1.14xlarge	10,000	4,500,000
ecs.gn5-c4g1.xlarge	3,000	300,000
ecs.gn5-c4g1.2xlarge	5,000	1,000,000
ecs.gn5-c8g1.2xlarge	3,000	400,000
ecs.gn5-c8g1.4xlarge	5,000	1,000,000
ecs.gn5-c28g1.7xlarge	5,000	2,250,000
ecs.gn5-c8g1.8xlarge	10,000	2,000,000
ecs.gn5-c8g1.14xlarge	25,000	4,000,000
ecs.gn5i-c2g1.large	1,000	100,000
ecs.gn5i-c4g1.xlarge	1,500	200,000
ecs.gn5i-c8g1.2xlarge	2,000	400,000
ecs.gn5i-c16g1.4xlarge	3,000	800,000
ecs.gn5i-c28g1.14xlarge	10,000	2,000,000
ecs.gn4-c4g1.xlarge	3,000	300,000
ecs.gn4-c8g1.2xlarge	3,000	400,000
ecs.gn4-c4g1.2xlarge	5,000	500,000
ecs.gn4-c8g1.4xlarge	5,000	500,000
ecs.gn4.8xlarge	6,000	800,000
ecs.gn4.14xlarge	10,000	1,200,000
ecs.ga1.xlarge	1,000	200,000

Instance type	Maximum BPS threshold (Mbit/s)	Maximum PPS threshold (PPS)
ecs.ga1.2xlarge	1,500	300,000
ecs.ga1.4xlarge	3,000	500,000
ecs.ga1.8xlarge	6,000	800,000
ecs.ga1.14xlarge	10,000	1,200,000
ecs.f1-c28f1.7xlarge	5,000	2,000,000
ecs.f1-c8f1.2xlarge	2,000	800,000
ecs.f2-c28f1.14xlarge	10,000	2,000,000
ecs.f2-c28f1.7xlarge	5,000	1,000,000
ecs.f2-c8f1.2xlarge	2,000	400,000
ecs.f2-c8f1.4xlarge	5,000	1,000,000
ecs.t5-c1m1.2xlarge	1,200	400,000
ecs.t5-c1m1.large	500	100,000
ecs.t5-c1m1.xlarge	800	200,000
ecs.t5-c1m1.4xlarge	1,200	600,000
ecs.t5-c1m2.2xlarge	1,200	400,000
ecs.t5-c1m2.large	500	100,000
ecs.t5-c1m2.xlarge	800	200,000
ecs.t5-c1m2.4xlarge	1,200	600,000
ecs.t5-c1m4.2xlarge	1,200	400,000
ecs.t5-c1m4.large	500	100,000
ecs.t5-c1m4.xlarge	800	200,000
ecs.t5-lc1m1.small	200	60,000
ecs.t5-lc1m2.large	400	100,000
ecs.t5-lc1m2.small	200	60,000
ecs.t5-lc1m4.large	400	100,000
ecs.t5-lc2m1.nano	1,000	40,000
ecs.ebmg4.8xlarge	10,000	4,500,000
ecs.ebmg5.24xlarge	10,000	4,500,000
ecs.sccg5.24xlarge	10,000	4,500,000

Instance type	Maximum BPS threshold (Mbit/s)	Maximum PPS threshold (PPS)
ecs.xn4.small	500	50,000
ecs.mn4.small	500	50,000
ecs.mn4.large	500	100,000
ecs.mn4.xlarge	800	150,000
ecs.mn4.2xlarge	1,200	300,000
ecs.mn4.4xlarge	2,500	400,000
ecs.n4.small	500	50,000
ecs.n4.large	500	100,000
ecs.n4.xlarge	800	150,000
ecs.n4.2xlarge	1,200	300,000
ecs.n4.4xlarge	2,500	400,000
ecs.n4.8xlarge	5,000	500,000
ecs.e4.small	500	50,000
ecs.sn1.medium	500	100,000
ecs.sn1.large	800	200,000
ecs.sn1.xlarge	1,500	400,000
ecs.sn1.3xlarge	3,000	500,000
ecs.sn1.7xlarge	6,000	800,000
ecs.sn2.medium	500	100,000
ecs.sn2.large	800	200,000
ecs.sn2.xlarge	1,500	400,000
ecs.sn2.3xlarge	3,000	500,000
ecs.sn2.7xlarge	6,000	800,000
ecs.sn2.13xlarge	10,000	120,000

Related operations

By default, Anti-DDoS Basic is enabled for an ECS instance after it is created. You can do the following:

- Set a threshold for flow cleaning. After an ECS instance is created, the maximum threshold for the instance type is used for Anti-DDoS Basic by default. However,

the maximum BPS threshold for some instance types may be too big to be safe. Therefore, you must set a threshold according to your business needs. For more information, see *Set the cleaning trigger value* in the Anti-DDoS Basic documentation.

- (Not recommended) Cancel flow cleaning. When the inbound traffic to an ECS instance reaches the cleaning threshold, the entire traffic (including normal traffic) is cleaned. This may interrupt the normal business. To avoid business interruptions, you can cancel flow cleaning. For more information, see *Cancel flow cleaning*.

   Warning:
  If you cancel flow cleaning, when the inbound traffic to an ECS instance exceeds 5 Gbit/s, all traffic is routed to a black hole. Proceed with caution.

4 Implement access control by using RAM

This topic describes how to control access to ECS instances at the account level by using Resource Access Management (RAM). Specifically, this topic describes how to create a RAM user and how to create policies to grant specific permissions to one or more RAM users and RAM user groups.

Background information

RAM is a resource access control service provided by Alibaba Cloud. For more information, see *What is RAM?*. The following describes how RAM is applied to RAM users and RAM user groups to achieve access control:

- RAM users: If you have purchased one or more ECS instances, and multiple RAM users in your organization (such as employees, systems, or applications) need to access the instances, you can create a policy that only grants specific RAM users access to those instances. This application of RAM for access control means you do not need to disclose the AccessKey of your Alibaba Cloud account, which helps maintain account security.
- RAM user groups: You can create multiple user groups and grant different permissions to these user groups so that all RAM users in each user group are applied with the same permissions at the same time. For example:
  - You can associate a user group with a policy that denies access to the target ECS resources if IP addresses from that user group are not from within your corporate network.
  - You can add and remove RAM users to and from different user groups when the access control requirements of a RAM user changes. For example, you have two user groups, SysAdmins and Developers, that are applied with specific permissions for system administrators and developers, respectively. If a RAM user who is a developer becomes a system administrator, you can move the target RAM user from the Developers group to the SysAdmins group. Details of the two user groups are as follows:
    - SysAdmins: This user group requires permissions to create and manage ECS instances. Therefore, you can associate the SysAdmins group with a policy that allows its group members to perform all ECS operations, including the

creation and management of ECS instances, images, snapshots, and security groups.

- Developers: This user group requires permissions to operate on ECS instances, but not create instances. Therefore, you can associate the Developers group with a policy that allows its group members to call DescribeInstances, StartInstance, StopInstance, RunInstance, and DeleteInstance.

Authorization policy

Authorization policies are categorized as either a System Policy or Custom Policy.

- System Policy: Alibaba Cloud provides a variety of default authorization policies. Some commonly-used system policies for ECS instances are as follows:
  - AliyunECSReadOnlyAccess: Grants read-only access.
  - AliyunECSFullAccess: Grants full administrative access.
  - AliyunECSImageImportDefaultRole: Grants permission to *import a custom image*.
  - AliyunECSImageExportDefaultRole: Grants permission to *export a custom image*.
  - AliyunECSNetworkInterfaceManagementAccess: Grants permission to manage *Elastic Network Interfaces (ENIs)*.
- Custom Policy: A user-generated policy. This policy type is suitable to users who are familiar with various Alibaba Cloud APIs and require fine-grained access control. For more information, see *Step 2*.

Step 1: Create a RAM user

1. Log on to the *RAM console*.
2. In the left-side navigation pane, click Users.
3. Click Create User.

> Note:
> For detailed information about how to create a RAM user, see *RAM users*.

(Optional) Step 2: Create a custom policy

1. Log on to the *RAM console*.
2. In the left-side navigation pane, click Policies.
3. Create Create Authorization Policy.
4. Enter an Authorization Policy Name and Description.

5. Enter the parameters for the Policy Content according to the JSON template.

> **Note:**
> For information about the values of the `Action` and `Resource` parameters, see *Authentication rules*. For information about the values of other parameters, see *Policy elements*.

- Example policy 1: Allow a RAM user to create Pay-As-You-Go instances.

```
{
    " Statement ": [
        {
            " Effect ": " Allow ",
            " Action ": [
                    " ecs : DescribeIm  ages ",
                " vpc : DescribeVp  cs ",
                " vpc : DescribeVS  witches ",
                " ecs : DescribeSe  curityGrou  ps ",
                " ecs : DescribeKe  yPairs ",
                " ecs : DescribeTa  gs ",
                " ecs : RunInstanc  es "
          ],
            " Resource ": ""
        }
    ],
    " Version ": " 1 "
}
```

- Example policy 2: Allow a RAM user to create Subscription instances. Note that `bss` related APIs are mainly used to view and pay Subscription orders, and the corresponding system policy is `AliyunBSSO rderAccess`.

```
{
    " Statement ": [
        {
            " Effect ": " Allow ",
            " Action ": [
                    " ecs : DescribeIm  ages ",
                " vpc : DescribeVp  cs ",
                " vpc : DescribeVS  witches ",
                " ecs : DescribeSe  curityGrou  ps ",
                " ecs : DescribeKe  yPairs ",
                " ecs : DescribeTa  gs ",
                " ecs : RunInstanc  es ",
                        " bss : DescribeOr  derList ",
                 " bss : DescribeOr  derDetail ",
                 " bss : PayOrder ",
                " bss : CancelOrde  r "
          ],
            " Resource ": ""
        }
    ],
    " Version ": " 1 "
```

```
}
```

- **Example policy 3: Allow a RAM user to query instance and disk information after creating an ECS instance.**

```
{
    " Statement ": [
        {
            " Effect ": " Allow ",
            " Action ": [
                    " ecs : DescribeIn  stances ",
                " ecs : DescribeDi  sks "
          ],
            " Resource ": ""
        }
    ],
    " Version ": " 1 "
}
```

6. **Click Create Authorization Policy.**

Step 3: Authorize a RAM user

1. **Log on to the *RAM console*.**
2. **In the left-side navigation pane, click Users.**
3. **Find the RAM user created in step 1 and then, in the Actions column, select Authorize.**
4. **In Available Authorization Policy Names area, select one or more system or custom policies.**
5. **Click OK.**

5 Instance RAM roles

5.1 What is the RAM role of an instance

Instance RAM (Resource Access Management) roles allow you to authorize role-based permissions to ECS instances.

You can assign a *role* to an ECS instance to allow applications hosted on that instance to access other cloud services by using a temporary STS (Security Token Service) credential. This helps guarantee the security of your AccessKey and allows you to apply fine-grained access control of your instances.

Background

Generally, applications within an ECS instance need to use the AccessKey of the primary account or *RAM user account*, which includes an AccessKeyId and AccessKeySecret, to access various cloud services on the Alibaba Cloud platform.

This means that, to make a call, you must apply the AccessKey directly in the instance , such as in the configuration file. However, if Alibaba Cloud writes the AccessKey into the instance for calling purposes, the AccessKey may be mistakenly exposed. To ensure the security of your account and resources, Alibaba Cloud provides instance RAM roles to support .

Benefits

Instance RAM roles enable you to:

- Associate a *role* to an ECS instance.
- Access other cloud services securely (such as OSS, SLB, and ApsaraDB for RDS) by using the STS credential from the applications within the ECS instance.
- Assign roles that have different policies for different ECS instances, and allow those instances have restrictive access level to other cloud services to obtain fine-grained access control.
- Maintain the access permission of ECS instances by modifying only the policy of the RAM role, meaning no changes to the AccessKey are required.

Pricing

Instance RAM roles are free to use.

Limits

Instance RAM roles have the following limits:

- Instance RAM roles are only applicable to VPC instances.
- An ECS instance can only be authorized to one instance RAM role.

How to use an instance RAM role

The instance RAM role can be used by any of the following methods:

- *Use the instance RAM role in the console*.
- *#unique_96*.

References

- For a list of cloud services that support STS, see *cloud services supporting RAM*.
- See *access other Cloud Product APIs by the Instance RAM Role* for instruction on how to access other cloud services.

5.2 Use the instance RAM role in the console

Limits

Instance RAM roles have the following limits:

- Instance RAM roles are only applicable to VPC-Connected instances.
- An ECS instance can only be authorized to one instance RAM role at a time.
- After an instance RAM role is bound to an ECS instance, if you want to access other cloud services (such as OSS, SLB, or ApsaraDB for RDS) from applications within the ECS instance, you must obtain the authorization credential of the instance RAM role by using *metadata*. For more information, see *obtain authorization credentials*.
- If you are using an instance RAM role through a RAM user account, you must use a primary account to *authorize a RAM user to use the instance RAM role*.

Prerequisites

You must have activated the RAM service. See *activation method* to activate the RAM service.

1. Create an instance RAM role

1. Log on to the *RAM console*.
2. In the left-side navigation pane, click Roles.

3. Click Create Role.
4. In the dialog box:
   a. Select Service Role for Role Type.
   b. Select ECS Elastic Compute Service for Type.
   c. Enter a role name and description, for example, EcsRamRoleDocumentTesting.
   d. Click Create.

2. Authorize the instance RAM role

1. Log on to the *RAM console*.
2. In the left-side navigation pane, click Policies.
3. Click Create Authorization Policy.
4. In the dialog box:
   a. Select Blank Template for authorization policy template.
   b. Enter a Authorization Policy Name and Policy Content. In this example, they are EcsRamRoleDocumentTestingPolicy.

      Note:
      For information about how to write the authorization policy in JSON format, see *policy syntax structure*.

   c. Click Create Authorization Policy.
5. In the left-side navigation pane, click Roles.
6. Select a role, for example, EcsRamRoleDocumentTesting, and click Authorize.
7. Enter the Authorization Policy Name and select it from the drop-down menu. In this example, EcsRamRoleDocumentTestingPolicy is selected.
8. Click the icon > to select the policy name, and then click OK.

3. Bind an instance RAM role

1. Log on to the *ECS console*.
2. In the left-side navigation pane, click Instances.
3. Select the target region.

4. Find the target ECS instance and select More > Instance Settings > Bind/Unbind RAM Role.
5. Select Bind for Action, select a role (for example, EcsRamRoleDocumentTesting), and then click OK.

4. (Optional). Unbind an instance RAM role

1. Log on to the *ECS console*.
2. In the left-side navigation pane, click Instances.
3. Select the target region.
4. Find the target ECS instance and select More > Instance Settings > Bind/Unbind RAM Role.
5. Select Unbind for Action, and click OK.

5. (Optional). Replace an instance RAM role

1. Log on to the *ECS console*.
2. In the left-side navigation pane, click Instances.
3. Select the target region.
4. Find the target ECS instance and select More > Instance Settings > Bind/Unbind RAM Role.
5. Select Bind for Action, select another instance RAM role in the list of RAM Role, and then click OK.

6. (Optional). Obtain authorization credentials

To access an internal application of an ECS instance, you can obtain STS credentials of the instance RAM role (which is part of the metadata of an instance) to access the role-authorized permissions and resources. The credential is updated periodically. To access an instance by STS, follow these steps:

1. Connect to the target ECS instance.

2. Obtain the STS credential of the instance RAM role. In this example, it is EcsRamRoleDocumentTesting:
   - For a Linux instance: run `curl http :// 100 . 100 . 100 . 200 / latest / meta - data / Ram / security - credential s / EcsRamRole DocumentTe sting .`
   - For a Windows instance: see *Instance metadata*.
3. Get the credential. An example return is as follows:

```
{
" AccessKeyI d " : " XXXXXXXXX ",
" AccessKeyS ecret " : " XXXXXXXXX ",
" Expiration " : " 2017 - 11 - 01T05 : 20 : 01Z ",
" SecurityTo ken " : " XXXXXXXXX ",
" LastUpdate d " : " 2017 - 10 - 31T23 : 20 : 01Z ",
" Code " : " Success "
}
```

7. (Optional). Authorize a RAM user to use the instance RAM role

> **Note:**
> You must grant the RAM user with the PassRole permission to use the instance RAM role feature. Without the PassRole permission, a RAM user cannot carry out the permission of the authorization policy that is attached to the RAM user.

Log on to the RAM console and authorize the target RAM user by means of *authorizing RAM users* to complete the authorization. The following is an authorization policy example:

```
{
        " Version ": " 2016 - 10 - 17 ",
        " Statement ": [
            {
            " Effect ": " Allow ",
            " Action ": [
                " ecs : [ ECS RAM Action ]",
                " ecs : CreateInst ance ",
                " ecs : AttachInst anceRamRol e ",
                " ecs : DetachInst anceRAMRol e "
            ],
            " Resource ": "*"
            },
            {
        " Effect ": " Allow ",
        " Action ": " ram : PassRole ",
        " Resource ": "*"
            }
        ]
```

```
}
```

The parameter `[ ECS RAM Action ]` indicates that a RAM user can be authorized for certain actions. For more information, see *authorization rules*.

References

- Click the following link to learn how to *use the instance RAM role by calling APIs*.
- Click the following link to see how to *access other cloud products by using the instance RAM role*.

5.3 Use the instance RAM role by calling APIs

Limits

Instance RAM roles have the following limits:

- Instance RAM rolesare only applicable to VPC-Connected instances.
- An ECS instance can only be authorized to one RAM role at a time.
- After an instance RAM role is attached to an ECS instance, if you want to access other cloud services (such as OSS, SLB, or ApsaraDB for RDS) from applications within the ECS instance, you must obtain the authorization credential of the instance RAM role by using *#unique_100*. For more information, see*obtain the on-demand authorization credential*.
- If you are using an instance RAM role through a RAM user account, you must use a primary account to *authorize a RAM user to use the instance RAM role*.

Prerequisite

If you are using a RAM user account, it must be authorized to use the instance RAM role. See *activation method* to activate the RAM service.

1. Create an instance RAM role

1. Call the CreateRole *CreateRole* to create an instance RAM role.
2. Set a parameter RoleName, for example, EcsRamRoleDocumentTesting.
3. Set the `AssumeRole PolicyDocu ment` as follows:

```
" Statement ": [

" Action ": " sts : AssumeRole ",
" Effect ": " Allow ",
" Principal ": {
" Service ": [
```

```
" ecs . aliyuncs . com "

}


" Version ": " 1 "
```

2. Authorize the instance RAM role

1. Call the CreatePolicy to *CreatePolicy* create an authorization policy.
2. Set a parameter RoleName, for example, set it to EcsRamRoleDocumentTe stingPolicy.
3. Set the `PolicyDocu ment` as follows.

```
" Statement ": [

" Action ": [
" oss : Get *",
" oss : List *"

" Effect ": " Allow ",
" Resource ": "*"


" Version ": " 1 "
```

4. Call the *AttachPolicyToRole* to authorize the role policy.
5. Set `PolicyType` to Custom.
6. Set a parameter `PolicyName` , for example, EcsRamRoleDocumentTestingPolicy.
7. Set a parameter `RoleName` , for example, EcsRamRoleDocumentTesting.

Attach the instance RAM role

1. Call the *AttachInstanceRamRole* to attach an instance RAM role to an ECS instance.
2. Set the parameters `RegionId` and `InstanceId s` to specify an ECS instance.
3. Set a parameter `RamRoleNam e` , for example, EcsRamRoleDocumentTesting.

4. (Optional). Detach an instance RAM role

1. Call the *DetachInstanceRamRole* to detach an instance RAM role.
2. Set the parameters `RegionId` and `InstanceId s` to specify an ECS instance.
3. Set a parameter `RamRoleNam e` , for example, EcsRamRoleDocumentTesting.

5. (Optional). Obtain the on-demand authorization credential

For the internal application of an ECS instance, you can obtain the STS credential of the instance RAM role, which is a metadata of an instance, to access the role

-authorized permissions and resources. The credential is updated periodically. Example:

1. Obtain the STS credential of the instance RAM role, for example, EcsRamRoleDocumentTesting:
   - Linux instance: run `curl http://100.100.100.200/latest/meta-data/Ram/security-credentials/EcsRamRoleDocumentTesting`.
   - Windows instance: see *#unique_100*.
2. Get the credential Token. Return example:

```
"AccessKeyId" : "XXXXXXXXX",
"AccessKeySecret" : "XXXXXXXXX",
"Expiration" : "2017-11-01T05:20:01Z",
"SecurityToken" : "XXXXXXXXX",
"LastUpdated" : "2017-10-31T23:20:01Z",
"Code" : "Success"
```

6. (Optional). Authorize a RAM user to use the instance RAM role

> **Note:**
> You must grant the RAM user with the `PassRole` permission to use the instance RAM role feature.

Log on to the RAM console and follow the steps to*authorize RAM users*. Then, authorize the RAM user to complete the authorization, see the following code snippet as an authorization policy example:

```
"Version": "2016-10-17",
"Statement": [

"Effect": "Allow",
"Action": [
"ecs:[ECS RAM Action]",
"ecs:CreateInstance",
"ecs:AttachInstanceRamRole",
"ecs:DetachInstanceRAMRole"

"Resource": "*"


"Effect": "Allow",
"Action": "ram:PassRole",
"Resource": "*"
```

```
```

The parameter `[ ECS RAM Action ]` indicates that a RAM user is authorized for certain actions. See *authorization rules*.

References

- Click the following link to see how to *use the instance RAM role in the console*.
- For instruction on how to access other cloud services, see *access other Cloud Product APIs by the Instance RAM Role*.
- APIs related to the instance RAM role include:
  - *CreateRole*: Create an instance RAM role
  - *ListRoles*: Query the list of instance RAM roles
  - *CreatePolicy*: Create an instance RAM role policy
  - *AttachPolicyToRole*: Authorize an instance RAM role policy
  - *AttachInstanceRamRole*: Attach an instance RAM role
  - *DetachInstanceRamRole*: Detach an instance RAM role
  - *DescribeInstanceRamRole*: Query an instance RAM role