Alibaba Cloud
Elastic Compute Service

Security

Issue: 20190228

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 Security groups

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

Specifically, a security group is a logically isolated group of instances within the same region that have the same security requirements and are mutually accessible. Each instance must belong to at least one security group, which is specified during instance creation. Although instances in the same security group can communicate through the intranet, instances in different security groups are isolated from each other by default. However, mutual access between two security groups can be authorized.

Security group restrictions

- By default, each account can create a maximum of 100 security groups per region. This restriction can increase according to your membership level. To raise the upper limit, you can *open a ticket*.
- Each Elastic Network Interface (ENI) of an instance can join up to five security groups by default. You can *open a ticket* to raise the upper limit to a maximum of 10 or 16, depending on your membership level.
- You can choose either classic network or Virtual Private Cloud (VPC) as the network type of a security group.
  - Classic network instances can join security groups of classic networks in the same region.

    A security group within a classic network can contain a maximum of 1,000 instances. If more than 1,000 instances need to access each other over the

intranet, allocate them to different security groups and authorize mutual access among the security groups.

- VPC instances can join security groups on the same VPC.

  A security group within a VPC can contain a maximum of 2,000 private IP addresses (shared by the primary and secondary ENIs). If more than 2,000 private IP addresses need to access each other over the intranet, allocate the relevant instances to different security groups and authorize mutual access among the security groups.

- Modifying the configurations of a security group does not affect the continuity of your services.
- If an outbound packet is permitted, inbound packets over this connection are also permitted.

For more information, see *FAQ about security group limits*.

Overview of security group rules

For ECS instances in a security group, you can set security group rules to permit or forbid inbound and outbound access over the Internet or intranet.

You can create or delete security group rules at any time. Once changes are made, the updated security group rules are automatically applied to ECS instances in the security group.

When setting security group rules, we recommend that you make sure they are concise. For example, if you add an ECS instance to multiple security groups, hundreds of rules may immediately apply to the instance, which may cause connection errors when you access the instance.

Restrictions on security group rules

The maximum number of security group rules per ENI = number of security groups that the subject instance can join × maximum number of rules per security group.

Each ENI of an instance can have a maximum of 500 security group rules. Where:

- Each instance can join up to five security groups by default.

  You can open a ticket to raise the limit to 10 or 16, depending on your membership level. However, raising the number of security groups lowers the number of rules permitted in one security group.

- Each security group can have a maximum of 100 security group rules, including both inbound and outbound rules.

  The number of rules per security group can be 30, 50, or 100, depending on the quota of security groups.

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

Number of security groups	Max. number of rules
5 (default value)	100
10 (you need to open a ticket)	50
16 (you need to open a ticket)	30

Example

By default, an ENI can join up to five security groups, each of which has a maximum of 100 rules.

However, if your membership level allows each ENI to join up to 10 security groups , each security group can have a maximum of 50 rules. This is because for each instance, the total number of security group rules cannot be greater than 500.

If you want more security groups and less rules per group for one instance, you can *open a ticket* to adjust the upper limit.

1.2 Scenarios

This topic describes several scenarios that use security groups. The scenarios include instances of both VPC and Classic network types.

 Note:

- For information about how to create security groups and add security group rules, see *Create a security group* and *Add a security group rule*.
- For information about relevant ports, see *Introduction to common ECS instance ports*.
- For security group rule configurations of relevant ports, see *Typical applications of security group rules*.

- *Scenario 1: Enable intranet communication*

  If you want to copy files between two Classic network-connected ECS instances owned by different accounts or located in different security groups, you can configure security group rules to enable communication between the instances through the intranet.

- *Scenario 2: Allow remote connection to your ECS instance from specified IP addresses only*

  You can modify the remote connection port and then configure security group rules to only allow access specified IP address access to your ECS instance.

- *Scenario 3: Allow your ECS instance to access specified IP addresses only*

  You can configure security group rules to allow your instance to access only specified IP addresses or ports.

- *Scenario 4: Allow remote connection to your ECS instance*

  You can configure security group rules to allow remote access to your ECS instance through the Internet or intranet.

- *Scenario 5: Allow access to your ECS instance by using HTTP or HTTPS*

  If you have built a website on your ECS instance, you can configure security group rules to allow users to access the website.

- *Scenario 6: Deny your ECS instance to access specified external IP addresses*

  If you do not want your ECS instance to access specified external IP addresses, you can configure security group rules accordingly.

Scenario 1: Enable intranet communication

You can create security group rules to allow communication between instances through the intranet in the following cases:

- Case 1: The ECS instances belong to the same region and account.
- Case 2: The ECS instances belong to the same region but to different accounts.

Note:

- For VPC-Connected ECS instances, if they are in the same VPC, you can configure their security group rules to implement intranet communication. If they are in different VPCs (regardless of whether they are owned by the same account or located in the same region), you can use Express Connect to implement intranet

communication. For more information, see *Interconnect two VPCs under different accounts*.

Case 1: The ECS instances belong to the same region and account

By default, two instances located in the same region and owned by the same account can communicate with each other through the intranet. If the instances are in different security groups, you can configure security group rules to enable intranet communication according to the network type.

- VPC

  If the instances are in the same VPC, add a rule to each security group to authorize mutual access between the security groups. The rule settings are described as follows.

NIC	Rule direction	Authorization policy	Protocol type	Port range	Priority	Authorization type	Authorization object
Not required	Inbound	Allow	Select the required protocol.	Set the required port range.	1	Security group access (authorize this account)	Select the ID of the security group to which the instance to be accessed belongs.

- Classic network

  Add a rule to each security group to authorize mutual access between the security groups. The rule settings are described as follows.

NIC	Rule Direction	Authorization Policy	Protocol Type	Port Range	Priority	Authorization Type	Authorization Object
Intranet	Inbound	Allow	Select the required protocol.	Set the required port range.	1	Security group access (authorize this account)	Select the ID of the security group to which the instance to be accessed belongs.

Case 2: The ECS instances belong to the same region but to different accounts

The information in this case is for Classic network-connected ECS instances only.

Add a rule to each security group to authorize mutual access between the security groups. For example:

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

1. Add a rule to Group A to authorize Instance B to access Instance A. The rule settings are described as follows.

NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
Intranet	Inbound	Allow	Select the required protocol.	Set the required port range.	Security group access (authorize other accounts)	Enter the account ID of User B and the security group ID of Group B.	1

2. Add a rule to Group B to authorize Instance A to access Instance B. The rule settings are described as follows.

NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
Intranet	Inbound	Allow	Select the required protocol.	Set the required port range.	Security group access (authorize other accounts)	Enter the account ID of User A and the security group ID of Group A	1

Note:

To guarantee instance security, when you set an intranet inbound rule for the Classic network, Security Group Access is the top priority for Authorization Type. If you select Address Field Access, only a single IP address can be authorized and the authorized object must be in the format of a.b.c.d/32. The IP address can be set as needed, but only IPv4 is supported. The subnet mask must be `/ 32 `.

Scenario 2: Allow remote connection to your ECS instance from specified IP addresses only

If you want to allow remote connection to your instance from specified IP addresses only, add the following rule. In this example, remote connection to an instance on TCP port 22 from a specified IP address is allowed.

Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
VPC	Not required	Inbound	Allow	SSH(22)	22/22	Address field access	IP addresses that allow remote access, such as 1.2.3.4	1
Classic network	Internet							

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

If you want your ECS instance to access specified IP addresses, add the following rules to its security group.

1. Add the following rule to deny your instance to access any public IP addresses. The priority (for example, 2) must be lower than the rule in step 2.

Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
VPC	Not required	Outbound	Drop	All	-1/-1	Address field access	0.0.0.0/0	2
Classic network	Internet							

2. Add the following rule to allow your instance to access the specified IP address, with a higher priority than that in step 1.

Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
VPC	Not required	Outbound	Allow	Select the required protocol.	Set the required port range.	Address field access	Enter the specified IP address, for example, 1.2.3.4	1
Classic network	Internet							

After you add the rules, connect to the instance and try to `ping` it or `telnet` to the instance from the specified IP address. If the instance can be accessed, the rule is successfully applied.

Scenario 4: Allow remote connection to your ECS instance

You can allow remote connection to your instance in the following cases:

- Case 1: Allow remote connection to your instance from the Internet.
- Case 2: Allow remote connection to your instance from the intranet.

Case 1: Allow remote connection to your instance from the Internet

To allow remote connection to your instance from the Internet, add the following rule based on the network type and the operating system of your instance:

- VPC

NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
Not required	Inbound	Allow	Windows: RDP(3389)	3389/3389	Address field access	To allow Internet access from any public IP address, enter 0.0.0.0/0. To allow Internet access from a specified public IP address, see *Scenario 2*.	1
			Linux: SSH (22)	22/22			
			Custom TCP	Custom			

- Classic network

NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
Internet	Inbound	Allow	Windows: RDP(3389)	3389/3389	Address field access	To allow Internet access from any public IP address, enter 0.0.0.0/0. To allow Internet access from a specified public IP address, see *Scenario 2*.	1
			Linux: SSH(22)	22/22			
			Custom TCP	Custom			

To customize the port for remote connection, see *Modify the default remote access port*.

Case 2: Allow remote connection to your instance from the intranet

If you have enabled intranet communication between instances that belong to the same region but to different accounts, and you want to allow the instances in a security group under a different account to connect to your instance, add the following rules as needed.

- To allow an intranet IP address to connect to your instance:
  - VPC

    Make sure that you have established intranet communication between both accounts by using *Express Connect*, and then add the following rule.

NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
Not required	Inbound	Allow	Windows: RDP(3389)	3389/3389	Address field access	Specify the private IP address of the peer instance.	1
			Linux: SSH (22)	22/22			
			Custom TCP	Custom			

  - Classic network

    Add the following rule.

NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
Intranet	Inbound	Allow	Windows: RDP (3389)	3389/3389	Address field access	Specify the private IP address of the peer instance. To guarantee instance security, only an IP address with the CIDR prefix `/32` in the format of a.b.c.d/32 is allowed.	1
			Linux: SSH (22)	22/22			
			Custom TCP	Custom			

- To allow all instances in a security group under a different account to connect to your instance:
  - VPC

    Make sure that you have established intranet communication between both accounts by using *Express Connect*, and then add the following rule.

NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
Not required	Inbound	Allow	Windows: RDP (3389)	3389/3389	Security group access (authorize other accounts)	Enter the account ID and the security group ID of the peer instance.	1
			Linux: SSH(22)	22/22			
			Custom TCP	Custom			

  - Classic network

    Add the following rule.

NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
Intranet	Inbound	Allow	Windows: RDP (3389)	3389/3389	Security group access (authorize other accounts)	Enter the account ID and the security group ID of the peer instance.	1
			Linux: SSH(22)	22/22			
			Custom TCP	Custom			

Scenario 5: Allow access to your ECS instance by using HTTP or HTTPS

If you have built a website on your instance and want to allow users to visit the website through HTTP or HTTPS, add the following rules as needed.

- To allow all IP addresses to access your website:
  - VPC: Add the following rule.

NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
Not required	Inbound	Allow	HTTP(80)	80/80	Address field access	0.0.0.0/0	1
			HTTPS(443)	443/443			
			Custom TCP	Custom, for example, 8080/8080			

  - Classic network: Add the following rule.

NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
Internet	Inbound	Allow	HTTP(80)	80/80	Address field access	0.0.0.0/0	1
			HTTPS (443)	443/443			
			Custom TCP	Custom, for example, 8080/8080			

- To allow some public IP addresses to access your website:
  - VPC: Add the following rule.

NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
Not required	Inbound	Allow	HTTP(80)	80/80	Address field access	Specify one or more public IP addresses that you allow to access your website.	1
			HTTPS(443)	443/443			
			Custom TCP	Custom, for example, 8080/8080			

  - Classic network: Add the following rule.

NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
Internet	Inbound	Allow	HTTP(80)	80/80	Address field access	Specify one or more public IP addresses that you allow to access your website.	1
			HTTPS (443)	443/443			
			Custom TCP	Custom, for example, 8080/8080			

Note:

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

- TCP port 80 is the default port for HTTP services. If you want to use other ports, such as port 8080, you must modify the listening port settings in the configuration file of the Web server.

Scenario 6: Deny your ECS instance to access specified external IP addresses

If you do not want your ECS instance to access an external IP address, add the following rule to the security group to which your instance belongs:

Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
VPC	Not required	Outbound	Drop	All	-1/-1	Address field access	Specify the public IP address that you deny your instance to access, for example, 1.2.3.4.	1
Classic network	Internet							

1.3 Introduction to common ECS instance ports

The following table lists commonly used ECS instance ports.

Port	Service	Description
21	FTP	A port opened by the FTP service is used for uploading and downloading files.
22	SSH	An SSH port is used to *connect to a Linux instance by using a password* in command-line mode.

23	Telnet	The Telnet port is used for Telnet to log on to the ECS instance.
25	SMTP	The port that is open to the SMTP service is used for sending mails. Based on security concerns, ECS instance Port 25 is restricted by default. See *apply to open TCP port 25*to remove the limit.
80	HTTP	Provides access to HTTP services, such as IIS, Apache, and Nginx. We recommend that you *verify if TCP port 80 works properly* .
110	POP3	A port used for the POP3 protocol, which is a protocol for sending and receiving emails.
143	IMAP	A port used for IMAP (Internet Message Access Protocol), which is a protocol for receiving emails.
443	HTTPS	A port used to provide access to the HTTPS service. HTTPS is a protocol that provides encryption and transmissi on through secure ports.
1433	SQL Server	The TCP port of the SQL Server that is used for external service by SQL Server.
1434	SQL Server	The SQL Server UDP port that is used to return which TCP/IP port SQL Server uses.

1521	Oracle	An Oracle communications port. The port that needs to be released by Oracle SQL is deployed on the ECS instance.
3306	MySQL	The port through which the MySQL database provides external service.
3389	Windows Server Remote Desktop Services	The Windows Server Remote Desktop Services port can be used to *connect to a Windows instance*.
8080	Proxy port	Similar to 80 port, port 8080 is used by WWW agents to enable web browsing. If you are using port 8080, when you visit a Web site or use a proxy server, you must add `: 8080` after the IP Address: 8080. If you install the Apache Tomcat service, the default service port is 8080.
137, 138, 139	NetBIOS protocol	· Ports 137 and 138 are UDP ports that are used to transfer files through the network neighbor. · The connection entering through the port 139 attempts to obtain the NetBIOS/smb service. NetBIOS protocols are often used for Windows files, printer sharing, and samba.

Some ports cannot be accessed

Issue: An ECS instance attempts to listen for the corresponding port, but the port is not accessible, while other ports can be accessed normally.

Cause: Some operators determine that port numbers 135, 139, 444, 445, 5800, 5900, and related ports, are high-risk ports, which are then blocked by default.

Resolution: We recommend that you change the port to another port number

Related topic

For more information on how to release a service port through a security group, see *add security group rules*.

1.4 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_7*

   - 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 *CreateSecurityGroup* 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*.

1.5 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	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.
Custom UDP		
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_7/unique_7_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_17*.
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_18*.
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_21*
- *Implication and matching sequence of the ECS security group rule priority*

1.6 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.

1.7 Delete a security group

You can delete security groups that you no longer require. Deleting a security group also deletes all its corresponding rules.

 **Note:**

Before you delete a security group, note the following:

- Make sure there are no ECS instances in the security group. For more information on how to move an ECS instance to another security group, see *add to or remove from a security group*.
- Make sure the security groupis not referenced in the rules of another security group. You can delete a security group directly by following the steps described in this document. If the security group is authorized by another security group, error message shown in the following figure appears. If this occurs, you must delete the corresponding authorization rule.

Procedure

To delete a security group, follow these steps:

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

Related APIs

- Delete a security group: *DeleteSecurityGroup*
- Query authorization relationships between a security group and another security group: *DescribeSecurityGroupReferences*
- Move an ECS instance out of a security group: *LeaveSecurityGroup*

1.8 View the security group rules

You can view the security group rules at any time. To do so, follow these steps:

1. Log on to the *ECS console*.
2. In the left-side navigation pane, click Networks and Security > Security Groups.
3. Select the target region.
4. Select a security group, and click Add Rules.

5. Depending on the network type, the following information is displayed for security groups s:
   - For VPC, Inbound and Outbound is displayed.
   - For classic network, Internet Inbound, Internet Outbound, Intranet Inbound, and Intranet Outbound is displayed.
6. Click a tab to view the security group rules for that type.

2 Key pairs

2.1 SSH key pairs

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 log-on to your Linux instance. It is an alternative to authentication using a user name and password.

The key pair is composed of a public key and a private key. The asymmetric cryptography feature uses thepublic 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. User name and password authentication is disabled by ECS once the SSH key pair is enabled to guarantee security.

Benefits

Compared with typical user name 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 a 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

Related operations

- If you do not have an SSH key pair, you can *create an SSH key pair*.
- If you have created an SSH key pair by using another tool, you can *import an SSH key pair*.
- If you do not need a key pair, you can *delete an SSH key pair*.
- If you want to enable or disable SSH key pair authentication for logging on to a Linux ECS instance, you can *add or remove an SSH key pair*.
- You can allocate an SSH key pair when *creating an ECS instance*.
- You can *log on to an instance by using an SSH key pair*.

2.2 Create an SSH key pair

Limits

- The *SSH key pair*, known as as key pair, applies to Linux instances only.

- Currently, only 2048-bit RSA key pairs are supported.
  - Of the key pair components, Alibaba Cloud holds the public key.
  - After creating the key pair, you must download and securely store the private key of the key pair for future use.
  - The private key is in the unencrypted PEM-encoded `PKCS # 8` format.
- An Alibaba Cloud account can have a maximum of 500 key pairs per region.

Create an SSH key pair

1. Log on to the *ECS console*.
2. In the left-side navigation pane, select Networks and Security > SSH Key Pair.
3. Select the target region.
4. On the SSH Key Pairs page, select the target region and click Create SSH Key Pair.
5. On the Create SSH Key Pair page, enter a name for the key pair, and select Auto-Create SSH Key Pair.

   Note:
   The specified key pair name must be unique under the Alibaba Cloud account. That is, the name cannot be the same as that of an existing key pair or of a key pair that has been attached to an instance but has since been deleted. Otherwise, the error message "The key pair already exists" appears.

6. Click OK.

   Note:
   After a key pair is created, you must download and securely store the private key for future use. If you do not have the private key, you cannot log on to the ECS instance.

   After creating the key pair, you can view the information, including key pair Name and Fingerprint in the key pair list.

What to do next

After creating an SSH key pair, you can *attach or remove it* to or from an ECS instance.

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 Instance RAM roles

4.1 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:

- *#unique_60*.
- *#unique_61*.

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.

4.2 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 *#unique_65*. 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 *#unique_65*.
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*.

4.3 Use the instance RAM role by calling APIs

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 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_65*. 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_65*.
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