Alibaba Cloud
Elastic Compute Service

Security

MORE THAN JUST CLOUD | Alibaba Cloud

Legal disclaimer

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

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

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

3. The content of this document may be changed 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 group overview

This topic provides an overview of security groups.

What is a security group?

Security groups are logically isolated groups of instances that are located within the same region and share the same security requirements while also being mutually accessible. They act as virtual firewalls that provide Stateful Packet Inspection (SPI), also known as dynamic packet filtering. In a security group, security group rules can be used to grant or limit the access of ECS instances to the Internet or local private networks.

Limits

Security groups have the following limits:

· Each instance must belong to at least one security group. When you create an instance, you must specify the security group to which the instance will belong.

· By default, instances in different security groups cannot communicate with each other. However, you can set security group rules to authorize mutual access between two security groups.

· The maximum session timeout for a security group is 910s.

> **Note:**
> Security groups are stateful, and states can be kept through sessions. If outbound data packets are allowed for a connection, inbound data packets are also allowed for this connection. When you send a request from your instance, the security group accepts the response in the same session.

Security group types

Security groups can be divided into basic security group and advanced security group. The following table provides information about these two security group types. For more information, see Overview of advanced security group.

> **Note:**

The advanced security group type is in the beta testing phase in China North 5 (Hohhot) and US West 1 (Silicon Valley). You can open a ticket to apply for a free trial.

Security group type	Security group rule type	Security group rule priority	Inbound rule	Outbound rule	Scenario
Basic security group	Default rules of the basic security group	Depends on the security group template*	Depends on the security group template*	Allow all access requests.	Scenarios with high network control requirements, multiple ECS instance types, and moderate network connections
	Custom rules of the basic security group	Custom. Value range: 1 to 100	Supports the allow and deny policies. Add inbound rules as needed.**	Add outbound rules as needed.**	
Advanced security group	Default rules of the advanced security group	1. This value cannot be modified.	Depends on the security group template*	Allow all access requests.	Scenarios with high requirements on O&M efficiency, ECS instance types, and computing nodes
	Custom rules of the advanced security group		Supports the allow policy. Add inbound rules as needed.**	Allow all access requests.	

*When you create a security group in the ECS console, you can select Web Server Linux, Web Server Windows, and a custom security group template.

**For more information, see #unique_8 and #unique_9.

Default security group

After you create an ECS instance in a region, a default security group is created if no security group has been created under the current account in this region. The default security group is a basic security group.

The default rules of the default security group are as follows:

- Inbound: ICMP, SSH port 22, and RDP port 3389 are opened. You can also open HTTP port 80 and HTTPS port 443. The rule priority is 110.
- Outbound: Allow all access requests.

Security group rule priority

When you add a security group rule, you can set its priority to a value ranging from 1 to 100. A smaller value indicates a higher priority. The priority of a default security group rule is 110, lower than that of any manually created security group.

In a security group or between different security groups, if two security group rules 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 both security group rules have the same priority, the deny policy takes effect, but the allow policy does not take effect.
- If both security group rules have different priorities, the rule with a higher priority takes effect, regardless of the policy settings of both rules.

> **Note:**
> Advanced security groups do not support rule priority settings.

Network types

For basic security groups, the ENI settings of security group rules vary depending on network types.

- In a classic network, you must select a private ENI or public ENI before you can set security group rules.
- In a VPC, you do not need to select a private ENI or public ENI before you set security group rules.

> **Note:**
> ECS instances in a VPC access the Internet through private ENI mapping. Therefore, you cannot find public ENIs in these ECS instances. You can only set private security group rules, but these rules apply to the Internet and the intranet at the same time.
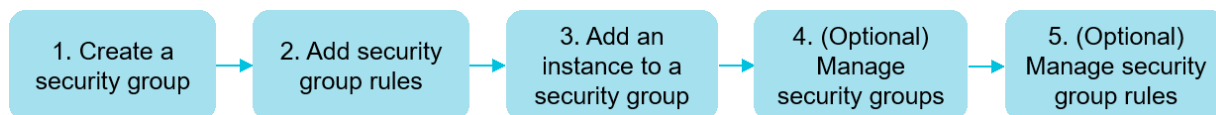
> **Note:**

> Advanced security groups only support VPCs.

Workflow

The following figure shows the workflow of basic security groups. For information about the workflow of advanced security groups, see Overview of advanced security group.

Usage notes

When you use security groups, we recommend that you:

- Use them as a whitelist.
- Set the rule policy of all security groups to deny access requests first, and then set the rule policy of these security groups one by one to allow access requests.
- Observe the principle of least privilege when you configure inbound or outbound rules for applications.
- Set a specific port (instead of a port range) to be opened, for example, port 80/80.
- Do not grant the access permission to objects whose CIDR block is 0.0.0.0/0 unless necessary when you add security group rules.
- Do not use one security group to manage all applications because isolation requirements are 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. Any changes to these rules may cause connection errors.
- Clone an active security group and modify the cloned copy. Modifying the cloned copy allows you to avoid interruptions to your application. After you modify the copy, you can delete the original security group and activate the new copy. For more information, see #unique_10.

1.2 Advanced security group overview

Compared with basic security groups, advanced security groups can contain more ECS instances and ENIs, and can manage unlimited private IP addresses. Advanced

security groups are applicable to VPC networks, and have a simplified rule adding mechanism. Advanced security groups can be used in scenarios that have higher requirements for O&M efficiency, ECS instance specifications, and computing nodes.

Feature comparison

Because you cannot add ECS instances or ENIs to both basic and advanced security groups, we recommend that you learn about the functional differences between the two security group types before planning your network environment. For more information about basic security groups, see #unique_12.

Item	Basic security group	Advanced security group
Supports all instance types ?	Yes	No. Only supports instances that support IPv6.
Supports VPCs?	Yes	Yes
Supports classic networks?	Yes	No
Rule priority available?	Yes	No
Access permissions granted to other security groups?	Yes	No
Manual setting of allow security group rules?	Yes	Yes
Manual setting of deny security group rules?	Yes	No. All access requests are denied for advanced security groups by default.
Number of ENIs supported	Limited by the number of ECS instances in the security group	50,000
ENIs bound to any instance type?	Yes. The instance network type must be VPC.	No. ENIs can only be bound to instance types that support IPv6.
Number of private IP addresses	2,000	No limit

Limits

· You cannot add ECS instances created before May 30, 2019 to advanced security groups.

- You can add only instance types that support IPv6 to advanced security groups. For more information, see #unique_13.
- ECS instances and ENIs have the following requirements on security group types:

    - An ECS instance cannot be added to both a basic security group and an advanced security group.
    - An ENI cannot be added to both a basic security group and an advanced security group.
    - When an ENI is bound to an ECS instance, they must belong to the same security group type.

Console operations

In the ECS console, you can use advanced security groups as follows:

1. Create an advanced security group. Set Security Group Type to Advanced Security Group.

2. Add an allow rule to the advanced security group.

    An advanced security group is equivalent to a communication whitelist. Only allow rules can be created and no priority values can be set for rules. Authorization objects must be CIDR blocks instead of security groups.

3. Add an ECS instance that supports IPv6 to an advanced security group. An ECS instance cannot be added to both a basic security group and an advanced security group.

4. Perform the following steps to use an ENI in an advanced security group:

    a. If an ENI is already in a basic security group, you can #unique_16 to add the ENI to an advanced security group.

    b. Bind the ENI to an ECS instance.

5. (Optional) Manage an advanced security group. For example, you can add a tag, modify the name and description, and manage ECS instances in the advanced security group.

API operations

1. Call CreateSecurityGroup and set `SecurityGr  oupType` to `enterprise` .

    Before creating a security group, confirm that a VPC and a VSwitch have been created.

2. Call AuthorizeSecurityGroup to add a rule which allows inbound traffic to the advanced security group. Authorization objects must be CIDR blocks instead of security groups.

   An advanced security group is equivalent to a communication whitelist. Policy is set to `accept` by default. You can leave `Priority` blank, but you must specify `IpProtocol` , `PortRange` , `SourcePort Range` (**optional**), `SourceCidr Ip` , and `DestCiderI p` .

3. Call AuthorizeSecurityGroupEgress to add an outbound rule to the advanced security group.

4. Call JoinSecurityGroup to add a VPC-type ECS instance to the advanced security group.

5. Perform the following steps to use an ENI in an advanced security group:

   a. Call ModifyNetworkInterfaceAttribute to add an ENI to an advanced security group, if the ENI is already in a basic security group.

   b. Call #unique_23 to attach an ENI that has been added to an advanced security group to an ECS instance.

6. (Optional) Call DescribeSecurityGroups to view the list of security groups you have created in the current region.

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_14 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	Authoriz ion policy	Protocol type	Port range	Authoriz ion type	Authoriz ion object	Priority
VPC	Configurat ion 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	Authoriz ion policy	Protocol type	Port range	Authoriz ion type	Authoriz ion 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 authorizat ion 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	Authoriz ion policy	Protocol type	Port range	Authoriz ion type	Authoriz ion object	Priority
VPC	Configurat ion 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 direction	Action policy	Protocol type	Port range	Authorization type	Authorization object	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	Authorion policy	Protocol type	Port range	Authorion type	Authorion 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

A security group is a virtual firewall for an ECS instance. This topic describes how to create a security group in the ECS console.

Background

An ECS instance must belong to one or more security groups. If no security group is created when you create an ECS instance, a default security group will be created. The default security group only has inbound rules configured for the ICMP protocol, SSH port 22, RDP port 3389, HTTP port 80, and HTTPS port 443. For more information, see Security group overview. If you do not want the ECS instance to be added to the default security group, you can create a security group as described in this topic.

Prerequisites

If you want to create a VPC-type security group, confirm that a VPC and a VSwitch have been created. For more information, see Create a VPC and a VSwitch.

Procedure

1. Click Create Security Group.
2. In the Create Security Group dialog box, configure the following parameters:

   · Template: If the instances in the security group are for Web server deployment, select a suitable template to simplify security group rule configuration.

Template	Description	Scenario
Web Server Linux	Inbound traffic to TCP port 80 , TCP port 443, TCP port 22, and for the ICMP protocol is allowed by default.	A Web server must be deployed on the Linux instances in the security group .
Web Server Windows	By default, inbound traffic to TCP port 80, TCP port 443, TCP port 3389, and for the ICMP protocol is allowed.	A Web server must be deployed on the Windows instances in the security group .

Template	Description	Scenario
Customize	After creating a security group, you need to add security group rules.	Not for Web server

· Security Group Name: specify a valid security group name.

· Description: the description of the security group for later management.

· Security Group Type:

  - Basic Security Group: can be used in scenarios that have higher requirements for refined network control, and prefer multiple ECS instance types and moderate network connections. For more information, see #unique_12.

  - Advanced Security Group: can be used in scenarios that have higher requirements for O&M efficiency, ECS instance specifications, and computing nodes. For more information, see #unique_5.

  > **Note:**
  > An ECS instance cannot be added to both a basic security group and an advanced security group.

· Network Type:

  - To create a classic network-type security group, select Classic.

  - To create a VPC-type security group, select VPC and then a specific VPC.

  > **Note:**
  > You must select VPC for an advanced security group.

3. Click OK.

Results

After the security group is created, a new security group is added to the security group list. If you select a custom template, we recommend that you configure security group rules as prompted on the page.

Related APIs

You can call #unique_18 to create a security group.

Next operations

· You can add security group rules to allow or deny access to the public or internal networks from ECS instances in security groups.

· An ECS instance must belong to one or more security groups. You can add an instance to one or more security groups based on your business needs.

1.6 Add security group rules

You can use security group rules to control the access to public or internal networks of the ECS instances in a security group.

Background

Security groups control access to or from public or internal networks. For security purposes, most security groups use deny policies for inbound traffic. If you use the default security group, or you select a Web Server Linux template or a Web Server Windows template when creating a security group, security group rules are automatically added to some communication ports. For more information, see #unique_12. This topic applies to the following scenarios:

· When your application needs to communicate with the network outside the security group, but the request stays in the wait state, you need to add security group rules first.

· When you discover malicious attacks from some request sources during the application operation, add deny security group rules to implement isolation.

Notes

· Security group rules depend on NIC types.

- Security group rules for classic networks distinguish between internal and public NICs.

- Security group rules for VPC networks do not distinguish between internal and public NICs.

Public network access to and from VPC-type ECS instances is mapped and forwarded by internal NICs. You cannot see public NICs in ECS instances, and can add only internal security group rules. However, security group rules apply to both the internal and public network.

· Before you add any rules to a security group, all outbound traffic is allowed and all inbound traffic is denied.

· The total number of inbound and outbound rules for each security group cannot exceed 100.

· You cannot configure the Priority parameter, set Authorization Type to Security Group, or set Action to Forbid for advanced security group rules. For more information, see #unique_5.

Prerequisites

· You have created a security group. For more information, see #unique_14.

· You know which internal or public network requests need to be allowed or denied for your instance. For more information about security group rule configuration cases, see Security group scenarios.

Procedure

1. Log on to the ECS console.

2. In the left-side navigation pane, choose Network & Security > Security Groups.

3. In the top navigation bar, select a region.

4. Locate the security group to which you want to add authorization rules. Click Add Rules in the Actions column.

5. On the Security Group Rules page, select one of the following methods to add rules:

· 1. Quick Rule Creation. It can be used when ICMP and GRE are not required and you can select multiple ports. On the Quick Rule Creation page, the following application ports are provided: SSH 22, Telnet 23, HTTP 80, HTTPS 443, MS SQL

1433, Oracle 1521, MySQL 3306, RDP 3389, PostgreSQL 5432, and Redis 6379. You can select one or more ports, or customize TCP or UDP ports.

For more information about the parameters such as NIC, Rule Direction, and Port Range on the Quick Rule Creation page, see Add Security Group Rule.

· 2. Add Security Group Rule. It can be used when multiple communication protocols such as ICMP and GRE are required.

a. Click Add Security Group Rule.

b. Select NIC (only for security group rules of the classic network).

- Internal Network: You do not want your ECS instance to access the public network, or public network access is not required.

- Internet: Your ECS instance needs to access the public network, or provide applications to the public network.

c. Select Rule Direction.

- Outbound: Your ECS instances access other ECS instances in the internal network or resources in the public network.

- Inbound: Other ECS instances in the internal network or resources in the public network access your ECS instances.

d. Select Action.

- Allow: allows access requests on the port.

- Forbid: Data packets are discarded and no messages are returned. If two security groups have the same rules but different authorization policies, Forbid policies are used while Allow policies are ignored.

e. Select Protocol Type and Port Range.

The port range is based on the protocol type. The following table describes the relationship between Protocol Type and Port Range. For more information about common ports, see #unique_44.

Protocol type	Port range	Scenario
All	-1/-1 is displayed, indicating all ports. You cannot set a port range for this protocol type.	It is used in all trusted scenarios.

Protocol type	Port range	Scenario
All ICMP (IPv4)	-1/-1 is displayed, indicating all ports. You cannot set a port range for this protocol type.	It is used when you run the `ping` command to check network connection status between instances.
All GRE	-1/-1 is displayed, indicating all ports. You cannot set a port range for this protocol type.	It is used for VPN.
Customized TCP	Customize a port range. Valid values: 1 to 65535. You must use the `< start port >/< end port >` format. For example, 80/80 indicates port 80, and 1/22 indicates port 1 to port 22.	It can be used to allow or deny one or several successive ports.
Customized UDP		
SSH	22/22	It is used to connect to a Linux instance remotely. After connecting to the ECS instance, you can modify the port number. For more information, see #unique_45.
Telnet	23/23	It is used to connect to an instance remotely.
HTTP	80/80	It is used when an instance serves as a website or Web application server.
HTTPS	443/443	It is used when an instance serves as a website or Web application server that supports the HTTPS protocol.
MS SQL	1433/1433	It is used when an instance serves as an MS SQL server.
Oracle	1521/1521	It is used when an instance serves as an Oracle SQL server.
MySQL	3306/3306	It is used when an instance serves as a MySQL server.

Protocol type	Port range	Scenario
RDP	3389/3389	It is used to connect to a Windows instance remotely. After connecting to the ECS instance, you can modify the port number. For more information, see #unique_45.
PostgreSQL	5432/5432	It is used when an instance serves as a PostgreSQL server .
Redis	6379/6379	It is used when an instance serves as a Redis server.

📋 **Note:**

The default STMP port for outbound Internet traffic is port 25, which is disabled by default. It cannot be enabled by security group rules. If you need to use STMP port 25, take proper measures to avoid security risks and then apply for enabling STMP port 25.

f. Select Authorization Type and Authorization Objects.

The authorized IP address is based on the authorization type.

Authorization type	Authorization object
IPv4 CIDR block	- Enter an IP address or CIDR block, in the format of 12.1.1. 1 or 13.1.1.1/25. - You can enter up to 10 authorization objects at a time. Separate multiple objects with commas (,). - Specifying 0.0.0.0/0 will allow or deny all IP addresses , based on the authorization policy. Use caution when specifying 0.0.0.0/0.

Authorization type	Authorization object
Security group	This authorization type is only valid for the internal network. Authorize the instances in a security group for your account or another account to access the instances in this security group. CIDR Block must be selected for public network access. - Authorize Current Account: Select another security group ID for your account. For a security group of the VPC type, the destination must be a security group in the same VPC. - Authorize Other Accounts: Enter a security group ID and another account ID. Choose Account Management > Security Settings to view your account ID. 📋 Note: For advanced security group rules, you cannot set Authorization Type to Security Group.

📋 Note:

When you add an inbound internal network rule for a security group of the classic network type, set Authorization Type to Security Group to improve security. If CIDR Block is selected, only one entry can be authorized. The entry must be in the a.b.c.d/32 format. Only IPv4 is supported and the subnet mask must be /32.

g. Specify a value for Priority. Valid values: 1 to 100.

📋 Note:

The smaller the number, the higher the priority. You can set priority values only for basic security groups, but not for advanced security groups. For more information, see Security group overview.

h. Click OK.

Results

Click the refresh icon to confirm that the security group rule is added. Changes to security group rules are automatically applied to ECS instances in the security group. We recommend that you immediately test whether the changes take effect.

Related APIs

- Call AuthorizeSecurityGroup to add an inbound security group rule.
- Call AuthorizeSecurityGroupEgress to add an outbound security group rule.

Next operations

An ECS instance must belong to one or more security groups. You can add an instance to one or more security groups based on your business needs.

1.7 Add an ECS instances to a security group

You can add an ECS instance to one or more security groups based on your business needs. An ECS instance can be added to up to five security groups.

Background

A security group controls access to ECS instances. An ECS instance must belong to one or more (up to five) security groups.

Prerequisites

- You have created an ECS instance.
- An ECS instance of the classic network type must be added to a security group of the classic network type in the same region.
- An ECS instance of the VPC type must be added to a security group in the same VPC .
- If an ECS instance has been added to a security group, the new security group to which the ECS instance is to be added must be of the same type as the other security group. For more information, see #unique_12 and #unique_5.

Procedure

In the ECS console, you can add an ECS instance to a security group on the Instance page. You can also do it on the Network & Security > Security Groups page.

1. On the Instances page, locate the ECS instance to be added to the security group. Click Manage in the Actions column.
2. Click Security Groups in the left-side navigation pane.
3. Click Add to Security Group.

4. Select the security group. If you want to add the ECS 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.

5. Click OK.

After you add an ECS instance to a security group, the security group rules automatically apply to the ECS instance.

Related APIs

You can call JoinSecurityGroup to add an ECS instance to a specified security group.

Related operations

· You can query security groups if you want to view all security groups you have created in a region.

· You can remove an instance from a security group if you do not want an ECS instance to belong to one or more security groups. The removed ECS instance will be isolated from other ECS instances in the security group. We recommend that you perform a full test before the remove operation to ensure that the business can run properly after the removal of the ECS instance.

· You can delete one or more security groups if you no longer need them. After you delete a security group, its rules will also be deleted.

1.8 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.

1.9 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, choose Network & Security > Security Groups.

3. In the top navigation bar, select a region.

4. Optional. Query the security groups as needed.

   · To query a security group by using its name, enter the name in the Security
     Group Name text box.

   · 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.

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, choose Network & Security > Security Groups.

3. In the top navigation bar, select a region.

4. Find the target security group, and then click Modify in the Actions column.

5. Modify the Security Group Name and 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, choose Network & Security > Security Groups.

3. In the top navigation bar, select a region.

4. Find the target security group, and then click Clone 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, choose Network & Security > Security Groups.

3. In the top navigation bar, select a region.

4. On the Instances page, find the target instance, and then click Manage in the Actions column.

5. Click Security Groups.

6. Find 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 Network & Security > Security Groups.

3. In the top navigation bar, select a region.

4. Select one or more security groups, and then click Delete in the lower-left corner of the list.

5. In the Delete Security Group dialog box, click OK.

You can also call the API DeleteSecurityGroup to delete a security group.

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 Use an SSH key pair

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

Create an SSH key pair

1. Click Create SSH Key Pair.

2. 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.

3. 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_ke  y_pair / my - key - pair . pem
```

The returned public key information is as follows:

```
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
ZEVCxxxxxx
```

Note:

If 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 View public key information.

2. Click Create SSH Key Pair.

3. 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.

4. 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 reset the instance logon password 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. Find the target key pair, and click Bind in the Actions column.

2. 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.

3. 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. Find the target key pair, and click Unbind in the Actions column.

2. 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.

3. 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 reset the instance logon password 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 View public key information.

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. Select one or more key pairs to be deleted.
2. Click Delete.

Related API: DeleteKeyPairs.

3 Implement access control by using RAM

This topic describes how to use Resource Access Management (RAM) to control access to ECS resources at the account level.

Scenarios

RAM is a resource access control service provided by Alibaba Cloud. For more information, see What is RAM?. The following section describes how RAM is used to implement 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 an authorization policy that only grants specific RAM users access to these instances. This eliminates the risk of disclosing 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 assigned the same permissions at the same time. For example:

  - You can associate a user group with an authorization policy which denies access to specific ECS resources from IP addresses that are outside your corporate network.

  - You can add and remove a RAM user to and from different user groups when the access control requirements of this RAM user change. For example, you have two user groups, SysAdmins and Developers, which grant different permissions for system administrators and developers.

    ■ SysAdmins: This user group needs permissions to create and manage ECS instances. Therefore, you can associate the SysAdmins group with an authorization 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 only needs permissions to use ECS instances. Therefore, you can associate the Developers group with an authorization policy that allows its group members to call the DescribeInstances, StartInstance, StopInstance, RunInstance, and DeleteInstance operations.

Authorization policies

Authorization policies are categorized into System Policy and Custom Policy.

- System Policy: the default authorization policies provided by Alibaba Cloud. Some commonly used system policies for ECS instances are as follows:

  - AliyunECSReadOnlyAccess: grants read-only access to ECS instances.
  - AliyunECSFullAccess: grants full administrative access to ECS instances.
  - AliyunECSImageImportDefaultRole: grants the permission to import custom images.
  - AliyunECSImageExportDefaultRole: grants the permission to export custom images.
  - AliyunECSNetworkInterfaceManagementAccess: grants the permission to manage ENIs.

- Custom Policy: the user-defined authorization policies. This policy type is suitable for 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

Follow this procedure to create a RAM user:

1. Log on to the RAM console.
2. In the left-side navigation pane, choose Identities > Users.
3. On the Users page, click Create User. *For more information about how to create a RAM user, see* Create a RAM user in the RAM documentation.

(Optional) Step 2: Create a custom authorization policy

Follow this procedure to create a custom authorization policy:

1. In the left-side navigation pane, choose Permissions > Policies.
2. On the Policies page, click Create Policy.
3. On the Create Custom Policy page, set Policy Name and Note. For example, set Policy Name to createEcs and Note to Permission to create ECS resources.
4. Select Script for Configuration Mode.

> **Note:**
> You can also select Visualized for Configuration Mode to complete the policy settings without referring to Authentication rules.

5. **Set the parameters in the Policy Document section based on the JSON template.**

   For the values of the `Action` **and** `Resource` **parameters, see** Authentication rules**.** *For the values of other parameters, see* Policy elements **in the RAM documentation.**

   · **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 operations are 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 the RAM user creates an ECS instance.

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

6. **Click OK.**

Step 3: Authorize the RAM user

Follow this procedure to authorize the RAM user:

1. **In the left-side navigation pane, choose Identities > Users.**

2. **On the Users page, find the RAM user created in step 1. Then in the Actions**
    column, click Add Permissions.

3. **In the Select Policy section of the Add Permissions pane, select one or more system**
    policies or custom policies to associate with the RAM user.

4. **Click OK.**

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_89.
- #unique_90.

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 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.

4.3 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_94. For more information, seeobtain 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 #unique_103 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 #unique_104 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 - credential  s / EcsRamRole  DocumentTe  sting .`

   · Windows instance: see #unique_94.

2. Get the credential Token. Return example:

```
" AccessKeyI  d " : " XXXXXXXXX ",
" AccessKeyS  ecret " : " XXXXXXXXX ",
" Expiration " : " 2017 - 11 - 01T05 : 20 : 01Z ",
" SecurityTo  ken " : " XXXXXXXXX ",
" LastUpdate  d " : " 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 :  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 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

5 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.

6 Security FAQ

- Security groups

    - What is a security group?

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

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

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

    - If I adjust the maximum number of ECS instances that each security group in VPCs can contain, does this adjustment take effect only on the security groups that I create after the time of adjustment?

- Security group rules

    - Why can't I configure public security group rules for my ECS instance in a VPC?

    - Why can't I access TCP port 25?

    - Why can't I access port 80?

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

    - Why is the priority of some security group rules 110?

    - What happens when a security group rule is configured incorrectly?

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

    - Can I adjust the maximum number of rules that can be added to a security group?

What is a security group?

A security group is a virtual firewall that implements access control for one or more ECS instances. As an important means of security isolation, security groups logically isolate security domains in the cloud.

Each ECS instance must belong to at least one security group. When you create an ECS instance, you must specify a security group for it. Instances in the same security group can communicate with each other, but instances in different security groups are isolated from each other by default. You can configure a security group rule 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 create ECS instances, you must select security groups to divide the security domains within your application environment and configure security group rules for proper network security isolation.

If you create an ECS instance in the ECS console in a region where you have not created any security groups, the instance is automatically assigned to the default security group. We recommend that you remove the instance from the default security group and add it to a new security group.

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

If you have not created any security groups before you create an ECS instance, you can use the default security group. The default security group allows access to common ports such as TCP port 22 and port 3389. For more information, see the Default security group section in Security group overview.

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 that can be associated with an ECS instance (primary ENI) = Maximum number of security groups that the instance can be added to $\times$ Maximum number of rules in each security group

If you are prompted that the number of rules has exceeded the limit, the number of security group rules that are associated with the instance has exceeded the upper limit. We recommend that you select another security group.

If I adjust the maximum number of ECS instances that each security group in VPCs can contain, does this adjustment take effect only on the security groups that I create after the time of adjustment?

No, the adjustment takes effect on all the security groups that you create in VPCs before and after the time of adjustment.

Why can't I configure public security group rules for my ECS instance in a VPC?

It is because instances in VPCs can access the public network only through internal NIC mapping, which makes public NICs invisible in the instances. As a result, you can configure only internal rules in the security groups that your instance belongs to. The security group rules you configure apply to both the internal network and public network.

Why can't I access TCP port 25?

TCP port 25 is the default email service port. For security reasons, port 25 of ECS instances is disabled by default. We recommend that you use port 465 to send emails. For more application scenarios, see Scenarios.

Why can't I access port 80?

See Check whether TCP port 80 is working properly.

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

Rules may be automatically added to your security group in either of the following situations:

· You have accessed Data Management Service (DMS). .

· You have migrated data by using Alibaba Cloud Data Transmission Service (DTS). The rules associated with the DTS IP address are automatically added to your security group.

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 the default rules is always lower than that of manually added security group rules. When you manually add security group rules, you can set the priority to a value ranging from 1 to 100.

What happens when a security group rule is configured incorrectly?

If a security group rule is configured incorrectly, the ECS instances associated with this rule cannot communicate with other devices through the internal network. For example:

· You cannot access Linux ECS instances remotely by using SSH or access Windows ECS instances by using the Remote Desktop Protocol (RDP).

· The public IP addresses of ECS instances cannot be `pinged` .

· The Web services provided by the ECS instances cannot be accessed through HTTP or HTTPS.

· The ECS instances associated with this rule cannot communicate with other ECS instances through the internal network.

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

No, the 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. For more information, see #unique_127.

Can I adjust the maximum number of rules that can be added to a security group?

No, each security group can contain a maximum of 100 security group rules. Each ENI of an ECS instance can be added to a maximum of five security groups by default . Therefore, each ENI of an ECS instance can be associated with a maximum of 500 security group rules, which meets the needs of most scenarios.

If the maximum number of rules in each security group has been reached but you need to add more security group rules, perform the following steps:

1. Check whether redundant rules exist. You can also submit a ticket to ask Alibaba Cloud technical support personnel to check for you.
2. If any redundant rules exist, delete them and then add new security group rules. If no redundant rules exist, create more security groups and add new security group rules.