ALIBABA CLOUD

Alibaba Cloud

Elastic Compute Service

Security

Document Version: 20201020

Alibaba Cloud

Legal disclaimer

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

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

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

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

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

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

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

Document conventions

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

Table of Contents

1.Security groups

1.1. Overview

Security groups function as virtual firewalls that provide Stateful Packet Inspection (SPI) and packet filtering capabilities to isolate security domains on the cloud. You can configure security group rules to control the inbound and outbound traffic of ECS instances in security groups.

Definition and characteristics

A security group is a logically isolated, mutually accessible group of instances within the same region that all share the same security requirements.

Security groups have the following characteristics:

- Each ECS instance must belong to at least one security group and can belong to multiple security groups at the same time.
- A security group can manage multiple ECS instances within the same region.
- ECS instances in different security groups cannot communicate with each other over the internal network. However, you can configure security group rules to allow access between the security groups.
- Security groups are stateful. The maximum session timeout period for a security group is 910 seconds. By default, a security group allows traffic in all directions within the same session. For example, if request traffic during a session is allowed to flow in, response traffic is also allowed to flow out.

Security group types

Security groups are classified into basic security groups and advanced security groups. The following table compares the features of the two types.

Feature	Basic security group	Advanced security group
Support all instance types	Yes	No. Only VPC-type instances are supported.
Network types	Supports VPCs and the classic network.	Supports VPCs only.
Access policy when no rules are added	• Inbound: denies all access requests. • Outbound: allows all access requests.	• Inbound: denies all access requests. • Outbound: denies all access requests.
Manually add rules	Supports both allow and forbid policies.	Supports only allow policies.
Set rule priorities	The default value is 1 and can be modified.	The value is fixed to 1 and cannot be modified.
Allow access to or from other security groups	Supports access to or from other security groups.	Does not support access to or from other security groups.

Feature	Basic security group	Advanced security group
Bind ENIs to instances of any instance type	No. The instance must be of the VPC type.	No. The instance must be of the VPC type.
Maximum number of private IP addresses	2,000	65,536
Mutual access between instances within the same security group	Allows mutual access between instances over the internal network by default.	By default, instances are isolated from each other over the internal network. You must manually add security group rules to allow access between the instances.
Scenario	Scenarios that require fine-grained network control, multiple ECS instance types, and moderate network connections.	Scenarios that have high requirements on O&M efficiency, ECS instance types, and compute nodes.

Security group rules

Before a connection for data communication is established, the security group matches access requests against all the rules. A security group rule is defined by attributes such as rule direction, action, protocol type, port range, and authorization object. The following table describes these attributes.

Attribute	Description
NIC type	Depending on the network type of the instance: • VPC: not required • Classic network: Internal network and Internet
Rule direction	Both inbound and outbound security group rules are allowed.
Action	Both allow and forbid rules are supported. Note For advanced security groups, you can set only allow rules.
Protocol type	Application layer protocols such as SSH, ICMP, and RDP.
Port range	Ports enabled for applications or protocols. For more information, see Typical applications of commonly used ports.

Attribute	Description
Priority	The value can range from 1 to 100. A smaller value indicates a higher priority. For security group rules of the same type, the rule that has the highest priority takes effect. When an ECS instance is added to multiple security groups, the rules of those groups are matched in descending order of priority. In one security group or between different security groups, if two security group rules have the same protocol type, port range, action, and authorization object, which rule takes effect depends on the priority and action settings of each rule. • If a forbid rule and an allow rule have the same priority, the forbid rule takes precedence. • If two rules have different priorities, the rule that has a higher priority takes effect. Note For advanced security groups, the priority is fixed to 1 and cannot be modified.
Authorization type	CIDR blocks and security groups. Note For advanced security groups, you cannot set this parameter to security group or authorize mutual access between two security groups.
Authorization object	CIDR blocks and security group IDs. Note For advanced security groups, you cannot set security group IDs or authorize mutual access between two security groups.

Different attributes of security group rules are required for different communication scenarios. For example, when you log on to a Linux ECS instance by using an Xshell client, a security group detects an SSH request from the Internet or internal network. The security group then matches the request against each inbound rule to check whether the rule contains the IP address of the request sender, whether the rule has the highest priority among the rules of the same type, whether the rule action is allow, and whether SSH port 22 is enabled. The connection for data communication is not established until an inbound rule that allows the request is matched. The following figure shows how the security group matches its rules to control the access request for a Linux ECS instance.

For information about examples of rule configuration, see Scenarios for security groups.

Default security groups

When you create an ECS instance in a region by using the ECS console, 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 and is of the same network type as the ECS instance.

By default, the default security group has the following security group rules:

- Inbound:
  - ICMP traffic and traffic over SSH port 22 and RDP port 3389 is allowed. The authorization object is 0.0.0.0/0.
  - You can also allow traffic over HTTP port 80 and HTTPS port 443.
  - The rule priority is 100.

    > **Note** The priority of default security group rules created before May 27, 2020 is 110.

- Outbound: All access requests are allowed.

Limits

ECS instances and elastic network interfaces (ENIs) have the following requirements for their security group types:

- An ECS instance cannot belong to both a basic and an advanced security group at the same time.
- An ENI cannot belong to both a basic and an advanced security group at the same time.

For information about the limits and quotas of security groups, see the "Security group limits" section in Limits.

Best practices

For information about the workflow of a security group, see Manage security groups. The following section provides some practical suggestions.

When you use security groups, we recommend that you adhere to the following best practices:

- Use security groups as a whitelist when only a few requests are allowed to access ECS instances in the security groups. Configure deny rules for all security groups and then add allow rules one by one to allow access requests.
- Do not use a security group to manage all applications because isolation requirements are different at different layers.
- Add instances that have the same security requirements to the same security group. Do not create a separate security group for each instance.

When you add security group rules, we recommend that you adhere to the following best practices:

- Configure 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.
- If you want to modify the rules of a security group in the production environment, we recommend that you first test the modification on a cloned security group to avoid potential impacts on online applications. For more information about how to clone a security group, see

Clone a security group.

- Follow the least privilege principle when you configure inbound or outbound rules for applications. For example, we recommend that you adhere to the following best practices:
  - Select a specific port over which to allow traffic, such as 80/80. Do not set a range of ports, such as 1/80.
  - When you add security group rules, do not grant access permissions to the 0.0.0.0/0 CIDR block unless necessary.

1.2. Advanced security groups

Compared with basic security groups, advanced security groups can contain more ECS instances, elastic network interfaces (ENIs), and private IP addresses. Advanced security groups also simplify the configuration policies of security group rules. Advanced security groups can be used in scenarios that have higher requirements for O&M efficiency, ECS instance specifications, and compute nodes.

Comparison of features

The following table compares the features of basic and advanced security groups. For more information about basic security groups, see Overview.

Feature	Basic security group	Advanced security group
Supports all instance types	Yes.	No. The instance must be of the VPC type.
Supports VPCs	Yes.	Yes.
Supports the classic network	Yes.	No.
Allows you to configure rule priorities	Yes.	No.
Allows access from other security groups	Yes.	No.
Allows you to manually set security group rules that allow access from other security groups	Yes.	Yes.
Allows you to manually set Deny security group rules	Yes.	No. Advanced security groups deny all access requests by default.
Access policy when no rules are added	• Inbound: denies all access requests. • Outbound: allows all access requests.	• Inbound: denies all access requests. • Outbound: denies all access requests.
Allows you to bind ENIs to instances of any instance type	No. The instance must be of the VPC type.	No. The instance must be of the VPC type.

Feature	Basic security group	Advanced security group
Maximum allowable number of private IP addresses	2,000.	65,536.
Allows mutual access between ECS instances within the same security group by default	Yes.	No. To allow mutual access between ECS instances in the same security group, you must add security group rules.

Billing

You are not charged extra fees when you use advanced security groups.

Limits

For the limits and quotas of advanced security groups, see the "Security group limits" section in Limits.

In addition to the preceding limits, ECS instances must also meet the following requirements before they can be added to advanced security groups:

- The network type of ECS instances must be VPC.
- ECS instances and ENIs have the following requirements for their security group types:
  - The primary ENI of an instance cannot belong to both a basic and an advanced security group at the same time.
  - A secondary ENI cannot belong to both a basic and an advanced security group at the same time.

Workflow

You can perform the steps in the following workflows to use advanced security groups.

- Use advanced security groups to manage instances

- Use advanced security groups to manage ENIs

Notice When you create an advanced security group by using the ECS console or by calling an API operation, you can configure outbound rules by adhering to the following guidelines:

- When you create the security group by using the ECS console, a security group rule is automatically added to allow all outbound traffic. We recommend that you keep the default setting to avoid network connectivity issues.
- When you create the security group by calling the API operation, no security group rules are added. All outbound traffic is denied by default. We recommend that you manually add security group rules.

Procedure in the console

The following table lists the operations that you can perform in the ECS console to manage advanced security groups.

Operation in the ECS console	Description	Reference
Create an advanced security group	When you create an advanced security group, set **Security Group Type** to **Advanced Security Group**.	Create a security group
Add a security group rule	An advanced security group is equivalent to an access whitelist. Only rules that allow access from other security groups can be added, and authorization objects can only be CIDR blocks. These rules have no priorities.	Add security group rules
Add an ECS instance to an advanced security group	The ECS instance cannot belong to both a basic and an advanced security group at the same time. If the instance belongs to a basic security group, you can replace the basic security group with an advanced security group.	• Add an ECS instances to a security group • Replace security groups of an ECS instance
Add an ENI to an advanced security group	If the ENI belongs to a basic security group, you can modify the ENI to add it to an advanced security group.	Modify an ENI
Bind an ENI to an ECS instance	After the ENI is bound to the instance, the security group rules immediately take effect.	Attach an ENI
Manage advanced security groups	The operations include adding tags, modifying names and descriptions, and managing instances in the advanced security groups.	• Query security groups • Clone a security group • Remove an instance from a security group
Manage rules for advanced security groups	You can modify security group rules during application operation based on your actual needs.	• Modify security group rules • Delete a security group rule • Manage security group rules

API operations

The following table lists the API operations that you can use to manage advanced security groups.

API	Description
CreateSecurityGroup	When you call this operation, set the SecurityGroupType request parameter to *enterprise*. **Note** Before you create an advanced security group, make sure that a VPC and a VSwitch are available.
AuthorizeSecurityGroup	You can call this operation to add a rule that allows inbound traffic to the advanced security group. Authorization objects can only be CIDR blocks. An advanced security group is equivalent to an access whitelist. You can use the following parameters to configure security group rules: • Policy: This parameter is set to *accept* by default. • Priority: This parameter is not required. • IpProtocol: This parameter is required. • PortRange: This parameter specifies the range of ports. • SourcePortRange: Optional. This parameter specifies the range of source ports. • SourceCidrIp: This parameter specifies the range of source IP addresses. • DestCiderIp: Optional. This parameter specifies the range of destination IP addresses.
AuthorizeSecurityGroupEgress	You can call this operation to add an outbound rule to an advanced security group. **Note** We recommend that you add a security group rule to allow all outbound traffic.
JoinSecurityGroup	You can call this operation to add a VPC-type instance to an advanced security group.
ModifyInstanceAttribute	If an instance belongs to a basic security group, you can call the ModifyInstanceAttribute operation to replace the security group with an advanced security group. **Note** When you switch an ECS instance to a security group of a different type, you must understand the differences between the rule configurations of the two security group types to avoid affecting the instance network.
ModifyNetworkInterfaceAttribute	If an ENI belongs to a basic security group, you can call the ModifyNetworkInterfaceAttribute operation to add the ENI to an advanced security group.
AttachNetworkInterface	You can call this operation to bind the ENI that has been added to an advanced security group to an ECS instance.

API	Description
DescribeSecurityGroups	You can call this operation to query the advanced security groups within the current region.

1.3. Scenarios for security groups

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

security group scenario tutorial

Overview

You can configure security group rules to allow or deny ECS instances in security groups to access the Internet or internal network. For information about how to create security groups and add security group rules, see Create a security group and Add security group rules. The following section lists typical scenarios for configuring security group rules:

- Scenario 1: Allow instances within the same region under the same account to communicate with each other through an internal network

  If you need to copy resources between two ECS instances within the same region that are under the same account, you can add security group rules to allow the instances to communicate with each other through an internal network.

- Scenario 2: Allow instances within the same region but under different accounts to communicate with each other through an internal network

  If you need to copy resources between two ECS instances within the same region but under different accounts, you can add security group rules to allow the instances to communicate with each other through an internal network.

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

  For security purposes, you can modify the port number for remote access to allow only specified IP addresses to connect to your ECS instance.

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

  For security purposes, you can add security group rules to allow your instance to access only specified public IP addresses.

- Scenario 5: Deny your instance access to specified public IP addresses

  For security purposes, you can add security group rules to deny your instance access to specified public IP addresses.

- Scenario 6: Allow Internet access to your instance

  You can connect to your instance from the Internet.

- Scenario 7: Allow an ECS instance that resides in a security group that belongs to another account within the same internal network to connect to your instance

  You can connect to your instance from an ECS instance in a security group under another account within the same internal network.

- Scenario 8: Allow Internet access to your ECS instance over HTTP or HTTPS

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

> **Note**
>
> - For information about commonly used ports, see Typical applications of commonly used ports.
> - In this topic, an IP address or a CIDR block is used to describe how to configure security group rules in different scenarios. Example: 12.1.1.1 or 13.1.1.1/25. Multiple IP addresses and CIDR blocks are separated with commas (,).

Scenario 1: Allow instances in the same region under the same account to communicate with each other through an internal network

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

- If the two instances belong to the same security group, they can communicate with each other through an internal network by default.
- If the two instances belong to different security groups, they cannot communicate with each other through an internal network by default. You can add security group rules to both security groups to allow their instances to communicate with each other through an internal network. Security group rule settings vary with network types, as described in the following table.

Network type	NIC type	Rule direction	Authorization policy	Protocol	Port range	Priority	Authorization type	Authorization object
VPC	Not required	Inbound	Allow	Select an applicable protocol.	Specify a port range.	1	Security group under the current account	The ID of the security group to which the allowed instance belongs.
Classic network	Internal							

> **Note**
>
> For ECS instances in the same VPC, you can add security group rules to allow them to communicate with each other through an internal network. For ECS instances in different VPCs, you can use Cloud Enterprise Network (CEN) to allow them to communicate with each other, regardless of whether the instances belong to the same account or are located within the same region. For more information, see *CEN document* Step 1: Network planning.

Scenario 2: Allow instances in the same region but under different accounts to communicate with each other through an internal network

This scenario applies only to ECS instances in classic networks.

For example, User A owns the classic network-type instance Instance A in the China (Hangzhou) region. The instance has the internal IP address A.A.A.A and belongs to the security group Group A.

User B owns the classic network-type instance Instance B in the China (Hangzhou) region. This instance has the internal IP address B.B.B.B and belongs to the security group Group B.

To allow Instance A and Instance B to communicate with each other through the internal network, you must add security group rules in both Group A and Group B.

- Add the security group rule described in the following table in Group A.

NIC type	Rule direction	Authorization policy	Protocol	Port range	Authorization type	Authorization object	Priority
Internal	Inbound	Allow	Select an applicable protocol.	Specify a port range.	Security group under another account	The ID of the security group Group B. The account ID of User B must be entered in **Account ID**.	1

- Add the security group rule described in the following table to Group B.

NIC type	Rule direction	Authorization policy	Protocol	Port range	Authorization type	Authorization object	Priority
Internal	Inbound	Allow	Select an applicable protocol.	Specify a port range.	Security group under another account	The ID of security group Group A. The account ID of User A must be entered in **Account ID**.	1

> **Note** For security purposes, when you add an internal inbound security group rule of the classic network type, we recommend that you set Authorization Type to **Security Group**. If you set Authorization Type to **CIDR Block**, you can enter only a single CIDR block, for example, `a.b.c.d/32`. The CIDR block can be set as needed, but the subnet mask must be /32.

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

To allow only specific IP addresses to connect to your instance, add the security group rule described in one of the following tables to the security group to which your instance belongs.

- Linux instance

Network type	NIC type	Rule direction	Authorization policy	Protocol	Port range	Authorization type	Authorization object	Priority
VPC	Not required	Inbound	Allow	SSH (22)	22/22	CIDR block	The public CIDR block that you allow to connect to your instance. Example: 1.2.3.4/32 or 10.0.0.0/8.	1
Classic network	Public							

- Windows instance

Network type	NIC type	Rule direction	Authorization policy	Protocol	Port range	Authorization type	Authorization object	Priority

Network type	NIC type	Rule direction	Authorization policy	Protocol	Port range	Authorization type	Authorization object	Priority
VPC	Not required	Inbound	Allow	RDP (3389)	3389/3389	CIDR block	The public CIDR block that you allow to connect to your instance. Example: 1.2.3.4/32 or 10.0.0.0/8.	1
Classic network	Public							

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

To allow your instance to access only specific IP addresses, add security group rules to the security group to which your instance belongs as follows:

- Add a security group rule to disallow your instance from accessing all public IP addresses through any protocols, and ensure that the priority of this deny rule is lower than the priority of the security group rule which allows the instance to access public IP addresses. In this example, the priority of the deny rule is set to 2. The deny rule settings are described in the following table.

Network type	NIC type	Rule direction	Authorization policy	Protocol	Port range	Authorization type	Authorization object	Priority
VPC	Not required	Outbound	Deny	All	-1/-1	CIDR block	0.0.0.0/0	2
Classic network	Public							

- Add a security group rule to allow your instance to access specified public IP addresses, and ensure that the priority of this allow rule is higher than the priority of the preceding deny group rule. In this example, the priority of the allow rule is set to 1.

Network type	NIC type	Rule direction	Authorization policy	Protocol	Port range	Authorization type	Authorization object	Priority
VPC	Not required	Outbound	Allow	Select an applicable protocol.	Specify a port range.	CIDR block	The public CIDR block that you allow your instance to access. Example: 1.2.3.4/32 or 10.0.0.0/8.	1
Classic network	Public							

After adding the security group rules, connect to your instance and run the **ping** or **telnet** command to check whether the security group rules have taken effect. If your instance can access only the allowed IP addresses, the security group rules have taken effect.

Scenario 5: Disallow your instance from accessing specified public IP addresses

To disallow your instance from accessing specific public IP addresses, add the security group rule described in the following table to the security group to which your instance belongs.

Network type	NIC type	Rule direction	Authorization policy	Protocol	Port range	Authorization type	Authorization object	Priority
VPC	Not required	Outbound	Deny	All	-1/-1	CIDR block	The public CIDR block that you disallow your instance from accessing. Example: 1.2.3.4/32 or 10.0.0.0/8.	1
Classic network	Public							

Scenario 6: Allow public network access to your instance

To allow public network access to your instance, add the security group rule described in the following table.

Network type	NIC type	Rule direction	Authorization policy	Protocol	Port range	Authorization type	Authorization object	Priority
VPC	Not required	Inbound	Allow	Windows: RDP (3389)	3389/3389.	CIDR block	To allow all public IP addresses to connect to your instance, enter 0.0.0.0/0. To allow only specified public IP addresses to connect to your instance, follow the instructions in "Scenario 3: Allow only specified IP addresses access to your instance."	1
				Linux: SSH (22)	22/22.			
				Custom TCP	Specify a port range, such as 8080/8080.			

Network type	NIC type	Rule direction	Authorization policy	Protocol	Port range	Authorization type	Authorization object	Priority
Classic network	Public	Inbound	Allow	Windows: RDP (3389)	3389/3389.	CIDR block	To allow all public IP addresses to connect to your instance, enter 0.0.0.0/0. To allow only specified public IP addresses to connect to your instance, follow the instructions in "Scenario 3: Allow only specified IP addresses access to your instance."	1
				Linux: SSH (22)	22/22.			
				Custom TCP	Specify a port range, such as 8080/8080.			

For information about how to customize ports for remote access, see Modify the default remote port of an instance.

Scenario 7: Allow an ECS instance that resides in a security group belonging to another account in the same internal network to connect to your ECS instance

If your account is in the same region and internal network as another account and you want to allow an ECS instance in a security group of that account to connect to your ECS instance, perform the following steps:

- To allow an internal IP address of an ECS instance in a security group under another account to connect to your instance, add the security group rule described in the following table. For ECS instances in VPCs, ensure that the instances under the two accounts can communicate with each other through Cloud Enterprise Network (CEN) before you add the security group rule. For more information, see *CEN document* Step 1: Network planning.

Network type	NIC type	Rule direction	Authorization policy	Protocol	Port range	Authorization type	Authorization object	Priority
VPC	Not required	Inbound	Allow	Windows: RDP (3389)	3389/3389.	CIDR block	The private IP address of the peer instance.	1
				Linux: SSH (22)	22/22.			
				Custom TCP	Specify a port range, such as 8080/8080.			
Classic network	Internal	Inbound	Allow	Windows: RDP (3389)	3389/3389.	CIDR block	An internal IP address of the peer instance. For security purposes, only a single CIDR block can be entered, such as a.b.c.d/32.	1
				Linux: SSH (22)	22/22.			
				Custom TCP	Specify a port range, such as 8080/8080.			

- To allow all ECS instances in a security group under another account to connect to your instance, add the security group rule described in the following table. For ECS instances in

VPCs, ensure that the instances under the two accounts can communicate with each other through Cloud Enterprise Network (CEN) before you add the security group rule. For more information, see *CEN document* Step 1: Network planning.

Network type	NIC type	Rule direction	Authorization policy	Protocol	Port range	Authorization type	Authorization object	Priority
VPC	Not required	Inbound	Allow	Windows: RDP (3389)	3389/3389.	Security group under another account	The ID of the security group to which the peer instance belongs. The ID of the peer account must be entered in Account ID.	1
				Linux: SSH (22)	22/22.			
				Custom TCP	Specify a port range, such as 8080/8080.			
Classic network	Internal	Inbound	Allow	Windows: RDP (3389)	3389/3389.	Security group under another account	The ID of the security group to which the peer instance belongs. The ID of the peer account must be entered in Account ID.	1
				Linux: SSH (22)	22/22.			
				Custom TCP	Specify a port range, such as 8080/8080.			

Scenario 8: Allow public network access to your ECS instance over HTTP or HTTPS

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

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

Network type	NIC type	Rule direction	Authorization policy	Protocol	Port range	Authorization type	Authorization object	Priority
VPC	Not required	Inbound	Allow	HTTP (80)	80/80.	CIDR block	0.0.0.0/0	1
				HTTPS (443)	443/443.			
				Custom TCP	Specify a port range, such as 8080/8080.			
Classic network	Public	Inbound	Allow	HTTP (80)	80/80.	CIDR block	0.0.0.0/0	1
				HTTPS (443)	443/443.			
				Custom TCP	Specify a port range, such as 8080/8080.			

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

Network type	NIC type	Rule direction	Authorization policy	Protocol	Port range	Authorization type	Authorization object	Priority

Network type	NIC type	Rule direction	Authorization policy	Protocol	Port range	Authorization type	Authorization object	Priority
VPC	Not required	Inbound	Allow	HTTP (80)	80/80.	CIDR block	Specify one or more public IP addresses that are allowed to access your website. Example: 1.2.3.4/32 or 10.0.0.0/8.	1
				HTTPS (443)	443/443.			
				Custom TCP	Specify a port range, such as 8080/8080.			
Classic network	Public	Inbound	Allow	HTTP (80)	80/80.	CIDR block	Specify one or more public IP addresses that are allowed to access your website. Example: 1.2.3.4/32 or 10.0.0.0/8.	1
				HTTPS (443)	443/443.			
				Custom TCP	Specify a port range, such as 8080/8080.			

Note

- If you cannot access your instance by using `http://public IP address`, check whether TCP port 80 is working properly.
- Port 80 is the default HTTP port. To use another port (for example, port 8080) for HTTP, 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.
1433	SQL Server	The TCP port of the SQL Server. This port is used for the SQL Server to provide external services.

Port	Service	Description
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	Authorization 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							
Remote access to Windows instances through	VPC	Configuration is not required.	Inboun	Allow	RDP (33	3389/3	Address fiel	0.0.0.0	1
	Classic network	Internet							

RDP Scenario	Network type	NIC	d Rule direction	Authorization policy	89) Protocol type	389 Port range	d Authorization type	/0 Authorization object	Priority
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. Manage security groups

This topic describes how to manage security groups. You can manage security groups by using the ECS console or by calling API operations.

Workflow

You can manage security groups by using the ECS console or by calling API operations. The following figure shows the workflow of a security group.

- Manage ECS instances

- Manage ENIs

> **Notice** When you create an advanced security group by using the ECS console or by calling an API operation, you can configure outbound rules by adhering to the following guidelines:
>
> - When you create the security group by using the ECS console, a security group rule is automatically added to allow all outbound traffic. We recommend that you keep the rule unchanged to avoid network connectivity issues.
> - When you create the security group by calling an API operation, no security group rules are added. All outbound traffic is denied by default. We recommend that you manually add security group rules.

Operation in the ECS console

The following table describes the operations that you can perform in the ECS console to manage security groups.

Operation	Description	Reference
Create a security group	You can create a security group.	Create a security group
Add security group rules	After you create a security group, you can add or modify security group rules to control inbound or outbound network access.	Add security group rules
Add an ECS instance to a security group	You can add instances to security groups to control network access in a centralized manner. An ECS instance cannot belong to both a basic and an advanced security group at the same time. If the instance is already added to a basic security group, you can replace the basic security group with an advanced security group.	• Add an ECS instances to a security group • Replace security groups of an ECS instance

Operation	Description	Reference
Add an ENI to a security group	You can add ENIs to security groups to control network access in a centralized manner. If the ENI is already added to a basic security group, you can modify the ENI to add it to an advanced security group.	Modify an ENI
Bind the ENI to an ECS instance	After an ENI is bound to an instance, the security group rules immediately take effect on the ENI.	Attach an ENI
Manage security groups	You can query, modify, clone, and delete security groups as well as remove instances from security groups.	• Query security groups • Modify a security group • Clone a security group • Remove an instance from a security group • Delete security groups
Manage security group rules	You can query, modify, restore, export, import, and delete security group rules.	• Manage security group rules • Modify security group rules • Restore security group rules • Export security group rules • Import security group rules • Delete a security group rule

API operations

The following table lists the API operations that you can use to manage security groups.

Operation	Description
CreateSecurityGroup	Creates a security group. Note Before you create an advanced security group, make sure that a VPC and a VSwitch are available.
AuthorizeSecurityGroup	Creates an inbound security group rule. This operation allows or denies the inbound traffic from other devices to ECS instances in the security group.

Operation	Description
AuthorizeSecurityGroupEgress	Creates an outbound security group rule. This operation allows or denies the outbound traffic from ECS instances in the security group to other devices.
JoinSecurityGroup	Adds an ECS instance to a specified security group.
ModifyInstanceAttribute	Switches an ECS instance to a security group of a different type. If an instance belongs to a basic security group, you can call the ModifyInstanceAttribute operation to replace the security group with an advanced security group. Note Before you switch an ECS instance to a security group of a different type, you must understand the differences between the rule configurations of the two security group types to avoid affecting the instance network.
ModifyNetworkInterfaceAttribute	Modifies the security group of an ENI. If an ENI belongs to a basic security group, you can call the ModifyNetworkInterfaceAttribute operation to add the ENI to an advanced security group.
AttachNetworkInterface	Binds an ENI that is already added to a security group to an ECS instance in a VPC.
DescribeSecurityGroups	Queries security groups that you have created within the current region.

1.6. Create a security group

A security group functions as a virtual firewall that controls network access of ECS instances. This topic describes how to create a security group in the ECS console.

security group virtual firewall network access control

Prerequisites

A VPC and a VSwitch are created if you want to create a VPC-type security group. For more information, see Create a VPC.

Context

An ECS instance must belong to at least one security group. If no security group has been created when you create an ECS instance, a default security group is 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 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.

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. Click **Create Security Group**.
5. In the **Create Security Group** dialog box that appears, configure the parameters listed in the following table.

Parameter	Description
Security Group Name	Specify a valid security group name.
Description	Enter a brief description of the security group for future management.
Network	Set the network type of the security group. ○ To create a classic network-type security group, select **Classic**. ○ To create a VPC-type security group, select an existing VPC.
Security Group Type	Select a security group type. ○ Basic Security Group: applicable to scenarios with small-scale clusters and moderate network connections. For more information, see Overview. ○ Advanced Security Group: applicable to scenarios with large-scale clusters that require high O&M efficiency. For more information, see Advanced security groups.
Access Rule	Specify access rules. The access rules for VPCs and the classic network have the following differences: ○ VPC ■ Inbound: By default, the inbound rules are configured for the ICMP protocol, SSH port 22, RDP port 3389, HTTP port 80, and HTTPS port 443. ■ Outbound: By default, all ports are enabled to allow outbound access of basic security groups, and all ports are disabled to deny outbound access of advanced security groups. ○ Classic network ■ Internet Ingress: By default, the inbound rules are configured for the ICMP protocol, SSH port 22, RDP port 3389, HTTP port 80, and HTTPS port 443. ■ Internet Egress: By default, all ports are disabled. ■ Inbound: By default, all ports are disabled to deny inbound access. ■ Outbound: By default, all ports are enabled to allow outbound access.

6. Click **OK**.

Result

After the security group is created, it is included in the security group list.

What's next

- You can configure security group rules to allow or deny the access of ECS instances in security groups to the Internet or internal network. For more information, see Add security group rules.
- An ECS instance must belong to at least one security group. You can add an instance to one or more security groups. For more information, see Add an ECS instances to a security group.

Related information

- CreateSecurityGroup

1.7. Add security group rules

This topic describes how to add security group rules. You can use security group rules to allow or deny access to or from the Internet or internal network for ECS instances in a security group.

Prerequisites

Before you add security group rules, make sure that the following requirements are met:

- A security group is created. For more information, see Create a security group.
- A list of the Internet or internal networks to which you want to allow or deny access to your instances is obtained. For information about scenarios of adding security group rules, see Scenarios for security groups.

Context

Security groups control access to or from the Internet or internal networks. For security reasons, most security groups use Forbid rules for inbound traffic. If you use the default security group, security group rules are automatically added for some communication ports.

In this topic, security group rules are applied to the following scenarios:

- When an application needs to communicate with a network outside the security group but the access request stays in the wait state, you must add an Allow rule first.
- When you detect attacks from some request sources during the application operation, add Forbid rules to isolate those malicious request sources.

Before you add security group rules, take note of the following points:

- Before you add rules to a basic security group, all outbound traffic is allowed and all inbound traffic is denied.
- Before you add rules to an advanced security group, all outbound and inbound traffic is denied. For advanced security groups, you cannot specify the Priority parameter, set Authorization Type to Security Group, or set Action to Forbid in security group rules.
- The total number of inbound and outbound rules in each security group cannot exceed 200.

For more information, see Overview.

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. Find the security group to which you want to add rules. Click **Add Rules** in the **Actions**

column.

5. On the **Security Group Rules** page, use one of the following methods to add rules:
   - Method 1. Quickly create security group rules

     This method is applicable when ICMP and GRE are not required and you can select multiple ports. In the **Quick Rule Creation** dialog box, 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.

     Click **Quick Rule Creation**. In the **Quick Rule Creation** dialog box, configure parameters such as **NIC Type**, **Rule Direction**, and **Custom Port Range**. For more information about how to configure parameters for a security group rule, see Method 2: **Manually add security group rules**.
   - Method 2. Manually add security group rules
     a. Click **Add Security Group Rule**.
     b. Add a security group rule in the rule list.

Security group rule parameters

Parameter	Description
NIC Type	The **NIC Type** parameter is required only for security group rules of the classic network. ■ **Internal**: sets an internal security group rule of the classic network. ■ **Public**: sets an Internet security group rule of the classic network.
Rule Direction	The direction in which the security group rules are applied. ■ **Outbound**: Select this value if your ECS instances need to access other ECS instances in an internal network or resources in the Internet. ■ **Inbound**: Select this value if other ECS instances in an internal network or resources in the Internet need to access your ECS instances.
Action	■ **Allow**: allows access requests on the specified port. ■ **Forbid**: discards data packets and returns no messages. If two security group rules differ only in their actions, the **Forbid** rule is used while the **Allow** rule is ignored. **Note** Only **Allow** rules can be created for advanced security groups.

Parameter	Description
Protocol Type	The protocol type of the security group rule. For information about the relationship between **Protocol Type** and **Port Range**, see Relationship between protocol types and port ranges. For more information about common ports, see Typical applications of commonly used ports.
Port Range	The port range depends on the protocol type. You can set a custom port range when **Protocol Type** is set to **Custom TCP** or **Customized UDP**. Enter the port range manually. Example: `22/23,443/443`.
Priority	A smaller value indicates a higher priority. Valid values: 1 to 100. **Note** The priority value of each rule in advanced security groups is fixed to 1. You cannot set priority values for rules in advanced security groups.
Authorization Type	Valid values: IPv4 CIDR Block and Security Group. **Note** For advanced security group rules, you cannot set Authorization Type to Security Group.

Parameter	Description
Authorization Object	Supported authorization objects include: ■ IPv4 CIDR block ■ Enter an IPv4 address or an IPv4 CIDR block. Example: 12.1.1.1 or 13.1.1.1/25. For more information about the CIDR format, see Network FAQ. ■ You can enter up to 10 authorization objects at a time. Separate multiple objects with commas (,). ■ If you enter 0.0.0.0/0 as an authorization object, all IPv4 addresses are allowed or denied based on the Action parameter. Evaluate the network risks before you specify 0.0.0.0/0. ■ Security group Note For advanced security group rules, you cannot set Authorization Type to Security Group. This authorization type is valid only for internal networks. Authorize the instances in a security group in your or another account to access the instances in the current security group. For Internet access, you must specify IPv4 or IPv6 CIDR blocks. ■ Authorize current account: Select the ID of another security group in your account. If the current security group is of the VPC type, the security group to be authorized must be in the same VPC as the current security group. ■ Authorize another account: Enter a security group ID and the ID of another account to which the security group belongs. Choose Account Management > Security Settings in the Account Center to view your account ID. Note For security reasons, we recommend that you set Authorization Object to Security Group when you add an internal inbound rule to a security group of the classic network type. If you set Authorization Object to CIDR blocks, you can specify only single IP addresses in CIDR notation in the a.b.c.d/32 format. Only IPv4 is supported, and the subnet mask must be /32.
Description	The description of the security group rule.

Relationship between protocol types and port ranges

Protocol Type	Port Range	Scenario
All	-1/-1 is displayed, indicating all ports. You cannot set a port range for this protocol type.	It can be used in all trusted scenarios.
All ICMP (IPv4)	-1/-1 is displayed, indicating all ports. You cannot set a port range for this protocol type.	It can be used when you run the `ping` command to check the status of network connections between ECS instances.
All GRE	-1/-1 is displayed, indicating all ports. You cannot set a port range for this protocol type.	It can be used for VPN.
Custom TCP Custom UDP	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 traffic on one or more successive ports.
SSH	22/22	It can be used to connect to a Linux instance. After you connect to the instance, you can modify the port number. For more information, see Modify the default remote port of an instance.
TELNET	23/23	It can be used to connect to an instance.
HTTP	80/80	It can be used when an instance serves as a website or web application server.
HTTPS	443/443	It can be used when an instance serves as a website or web application server that supports HTTPS.
MS SQL	1433/1433	It can be used when an instance serves as an MS SQL server.
Oracle	1521/1521	It can be used when an instance serves as an Oracle SQL server.
MySQL	3306/3306	It can be used when an instance serves as a MySQL server.

Protocol Type	Port Range	Scenario
RDP	3389/3389	It can be used to connect to a Windows instance. After you connect to the instance, you can modify the port number. For more information, see Modify the default remote port of an instance.
PostgreSQL	5432/5432	It can be used when an instance serves as a PostgreSQL server.
Redis	6379/6379	It can be used when an instance serves as a Redis server.

Note The default SMTP port for outbound Internet traffic is port 25, which is disabled by default. It cannot be enabled by security group rules. To use SMTP port 25, take preventive measures to minimize security risks and then apply to enable the port. For more information,see Apply to enable TCP port 25.

c. Click OK.

Result

After the security group rule is added, you can view it in the security group rule list. Changes to a security group rule are automatically applied to the ECS instances in the security group. We recommend that you immediately check whether the changes take effect.

What's next

An ECS instance must belong to at least one security group. You can add an instance to one or more security groups. For more information, see Add an ECS instances to a security group.

Related information

- AuthorizeSecurityGroup
- AuthorizeSecurityGroupEgress

1.8. 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.

Add an ECS instance to a security group

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 Overview and Advanced security groups.

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.
2.
3.
4.
5. On the **Instances** page, locate the ECS instance to be added to the security group. Click **Manage** in the **Actions** column.
6. Click **Security Groups** in the left-side navigation pane.
7. Click **Add to Security Group**.
8. 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.
9. 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.

1.9. Replace security groups of an ECS instance

You can replace security groups of an ECS instance based on your business needs.

replace a security group change a security group replace an advanced security group with a basic security group replace a basic security group with an advanced security group

Prerequisites

The instance and the target security groups belong to the same VPC.

Context

You can replace security groups of an instance in the following scenarios:

- Replace one or more basic security groups of an instance with other basic security groups.
- Replace one or more advanced security groups of an instance with other advanced security groups.
- Replace one or more basic security groups of an instance with advanced security groups.
- Replace one or more advanced security groups of an instance with basic security groups.

> **Notice**
> - Security groups can affect the network connections of your instances. We recommend that you debug the target security groups before you replace the security groups to ensure service availability.
> - An instance can only be added to security groups that are of the same type.

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images > Instances**.
3. In the top navigation bar, select a region.
4. On the **Instances** page, take one of the following steps based on the number of instances for which you need to replace security groups:
   - Replace security groups for a single instance

     Find the target instance and choose **More > Network and Security Group > Replace** in the **Actions** column.
   - Replace security groups for multiple instances

     Select the target instances and choose **More > Network and Security Group > Replace** in the lower part of the instance list.
5. In the **Replace Security Group for Instances** dialog box, select new security groups to replace the original security groups.
   i. **Security Group Type**: Select **Basic Security Group** or **Advanced Security Group**.
   ii. **Select Security Groups**: Select a target security group from the drop-down list.

> **Note** If you want to select multiple target security groups, click **Add** to select more security groups. One ECS instance can be added to a maximum of five security groups.

6. Click **Replace Security Group**.

Result

After the operations are complete, security groups are replaced.

Related information

- ModifyInstanceAttribute

1.10. Manage security groups

1.10.1. Query security groups

This topic describes how to query all security groups that you created in a region.

query security groups

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. Use one of the following methods to query security groups:
   - Select **Security Group Name** from the drop-down list, enter a security group name in the search bar, and then click **Search**.
   - Select **Security Group ID** from the drop-down list, enter a security group ID in the search bar, and then click **Search**.
   - Select **VPC ID** from the drop-down list, enter a VPC ID in the search bar, and then click **Search**.

1.10.2. Modify a security group

This topic describes how to modify the name and description of a security group.

modify a security group

Prerequisites

A security group is created. For more information, see Create a security group.

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. On the **Security Groups** page, find the security group to be modified and click **Modify** in the **Actions** column.
5. In the dialog box that appears, modify **Security Group Name** and **Description**.
6. Click **OK**.

Related information

- ModifySecurityGroupAttribute

1.10.3. Clone a security group

You can create identical security groups by cloning a security group. Security groups can be cloned across regions and network types.

clone a security group

Prerequisites

If you want to change the network type of the clone security group to VPC, at least one VPC must exist in the destination region. For more information, see Create a VPC.

Context

You can clone a security group in the following scenarios:

- You have created a security group named SG1 in Region A, and you want to apply the same rules as those of SG1 to instances in Region B. You can clone SG1 to Region B without creating a new security group.
- You have created a security group named SG2 in a classic network, and you want to apply the same rules as those of SG2 to instances located in a VPC. You can clone SG2 and select VPC as the network type for the clone security group in the Clone dialog box.
- If you want to apply new security group rules to an ECS instance that is running an online application, you can clone the original security group to create a backup.

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. Find the security group to be cloned on the **Security Groups** page and click **Clone** in the **Actions** column.
5. In the **Clone** dialog box, configure the clone security group.
   - **Destination Region**: Select a region for the clone security group. Note that only some regions are supported. The supported regions are displayed in the console.
   - **Security Group Name**: Enter a name for the clone security group.
   - **Network Type**: Select an applicable network type for the clone security group. If you set Network Type to VPC, select an available VPC in the destination region.
6. Click **OK**.

Result

The **Clone** dialog box closes after the security group is cloned. You can find the clone security group on the **Security Groups** page.

1.10.4. Remove an instance from a security group

You can remove instances from security groups. When an ECS instance is removed from a security group, the instance is isolated from all other ECS instances in the security group. We recommend that you perform tests in advance to ensure that services can continue to run properly after the instance is removed from the security group.

Prerequisites

The target instance is added to two or more security groups.

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images > Instances**.
3. In the top navigation bar, select a region.
4. On the **Instances** page, find the instance to be removed from a security group, and click **Manage** in the **Actions** column.
5. In the left-side navigation pane, click **Security Groups**.
6. Find the security group from which you want to remove the instance, and click **Remove** in the **Actions** column.
7. Click **OK**.

Related information

- LeaveSecurityGroup

1.10.5. Delete security groups

This topic describes how to delete security groups that are no longer needed. When a security group is deleted, its rules are also deleted.

delete security groups

Prerequisites

- The security group to be deleted does not contain any ECS instances. If the security group to be deleted contains any ECS instances, you must remove the instances from the security group. For more information, see Remove an instance from a security group.
- The security group to be deleted is not authorized by security group rules of other security groups. You can delete a security group directly by following the steps described in this topic. If the security group is authorized by security group rules of other security groups, the error message as shown in the following figure is displayed. You must delete those rules before you can delete the security group.

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. On the **Security Groups** page, select one or more security groups and click **Delete** in the lower part of the security group list.

5. In the **Delete Security Group** message that appears, confirm the information and click **OK**.

Related information

- DeleteSecurityGroup

1.11. Manage security group rules

1.11.1. 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, choose **Network & Security > Security Groups**.
3. In the top navigation bar, select a region.
4. Find 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 **Inbound** or **Outbound**.
   - If you need to query security group rules for a classic network, select **Internal Network Inbound**, **Internal Network Outbound**, **Internet Inbound**, or **Internet Outbound**.

You can also call 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, choose **Network & Security > Security Groups**.
3. In the top navigation bar, select a region.
4. On the **Security Groups** page, find 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 **Inbound** or **Outbound**.
   - If you need to modify the security group rules for a classic network, select **Internal**

Network Inbound, **Internal Network Outbound**, **Internet Inbound**, or **Internet Outbound**.

6. Find 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, choose **Network & Security** > **Security Groups**.
3. In the top navigation bar, select a region.
4. Find 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:
   i. Select the **Target Security Group**, which must have different rules from the source security group.
   ii. 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**.

iii. 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.

iv. Click **OK**.

After restoration, the **Restore Rules** dialog box is closed automatically. On the **Security Groups** page, find 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, choose **Network & Security > Security Groups**.
3. In the top navigation bar, select a region.
4. On the **Security Groups** page, find 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, choose **Network & Security > Security Groups**.
3. In the upper-left corner, select the target region.

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

4. On the **Security Groups** page, find 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, choose **Network & Security > Security Groups**.
3. In the top navigation bar, select a region.
4. Find 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 **Inbound** or **Outbound**.
   - If you need to delete the security group rules for a classic network, select **Internal Network Inbound**, **Internal Network Outbound**, **Internet Inbound**, or **Internet Outbound**.
6. Find 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 RevokeSecurityGroup to delete an ingress security group rule or call RevokeSecurityGroupEgress to delete an outbound security group rule.

1.11.2. Modify security group rules

Improper configuration of security group rules can cause serious security risks. You can modify improper rules in a security group to ensure the network security of instances within the security group.

modify security group rules

Prerequisites

A security group is created and security group rules are added. For more information, see Create a security group and Add security group rules.

Context

Security group rules that do not limit traffic on certain points may be exposed to serious security risks. You can modify security group rules to ensure the network security of instances.

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. On the **Security Groups** page, find the target security group and click **Add Rules** in the **Actions** column.
5. Select a direction of security group rules.

- If the security group is of the VPC type, you can select **Inbound** or **Outbound**.
- If the security group is of the classic network type, you can select **Internal Network Ingress**, **Internal Network Egress**, **Internet Ingress**, or **Internet Egress**.

6. Find the target security group rule and click **Modify** in the **Actions** column.
   - For information about how to configure a security group rule, see Add security group rules.
   - For information about how to use security group rules, see Typical applications of security group rules.

1.11.3. Restore security group rules

Restoring security group rules indicates the process of completely or partially restoring the rules in the original security group to those of a target security group. Specifically:

- **Completely restoring** means moving the rules that do not exist in the target security group from the original security group, and adding the rules that only exist in the target security group to the original security group. After restoration, rules in the original security group are identical with those in the target security group.
- **Partially restoring** means adding the rules that only exist in the target security group to the original security group and ignoring the rules that only exist in the original group.

Limits

Restoring security group rules has the following limits:

- The original security group and the target security group must be in the same region.
- The original security group and the target security group must be of the same network type.
- If any system-level security group rules, of which the priority is 110, exist in the target security group, they are not created during restoration. This means that after restoration, the rules in the original security group may be different. If you need the system-level security group rules, you must manually create the rules and set their priority to 100.

Scenario

If you want to apply new security group rules to an ECS instance that is running an online business application, you can clone the former security group as a backup, and then modify the rules inside. If the new security group rules affect the online business application, you can choose to fully or partially restore the rules.

Prerequisite

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, select **Networks and Security** > **Security Groups**.
3. Select the target region.
4. Find the security group you want to restore rules for as the original security group and then, in the **Actions** column, click **Restore Rules**.
5. In the **Restore Rules** dialog box, follow these steps:

i. Select the **Target Security Group**: Select a security group as the target security group that must have different rules from the original security group.

ii. Select a restore **Method**:

- If you want the original 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 original security group, select **Partially Restore**.

iii. In the **Preview** area, preview the restoration result:

- Rules highlighted in green only exist in the target security group. No matter whether you select **Completely Restore** or **Partially Restore**, these rules are added to the original security group.
- Rules highlighted in red are the rules that do not exist in the target security group. If **Completely Restore** is selected, the system removes these rules from the original security group. If **Partially Restore** is selected, the rules are retained in the original security group.

iv. Click **OK**.

The **Restore Rules** dialog box is closed automatically after successful creation. On the **Security Groups** page, find the original security group you restored the rules for and then, in the **Actions** column, click **Add Rules** to enter the **Security Group Rules** page to view the updated security group rules.

1.11.4. Export security group rules

You can export security group rules to JSON or CSV files for local backup.

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. On the **Security Groups** page, find the security group for which you want to export security group rules and click **Add Rules** in the **Actions** column.
5. Click **Export Rules** and select JSON Format or CSV Format to download and save the rules to a local file.
   - **JSON Format**

     A JSON file must adhere to the following naming conventions: *ecs_${region_id}_${groupID}.json*.

     If regionID is set to *cn-qingdao* and groupID is set to *sg-123*, the name of exported JSON file is *ecs_cn-qingdao_sg-123.json*.
   - **CSV Format**

     A CSV file must adhere to the following naming conventions: *ecs_sgRule_${groupID}_${region_id}_${time}.csv*.

     If regionID is set to *cn-qingdao*, groupID is set to *sg-123*, and time is set to *2020-01-20*, the name of the exported CSV file is *ecs_sgRule_sg-123_cn-qingdao_2020-01-20.csv*.

1.11.5. Import security group rules

Security group rules can be imported to a security group. You can export the rules of a security group to a file, and then import that file into other security groups or the original security group. In this way, you can quickly create or restore security group rules.

Procedure

1. Log on to the ECS console.
2. Click **Security Groups** in the left-side navigation pane.
3. Select a region.

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

4. On the **Security Groups** list page, find 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 Rules part displays the following information:

   - The number of rules to be imported.
   - Import check results. If any rules fail the import check, you can move the cursor over the warning icon for details.
   - Details of the rules to be imported.

   > **Note** Up to 100 security group rules can be imported, so the remaining rules will not be imported. The imported new rules do not overwrite the existing rules.

7. Click **Start** to import the rules.
8. View the import results, and then click **Finish and close**.

1.11.6. Delete a security group rule

This topic describes how to delete a security group rule that are no longer needed.

delete security group rules

Prerequisites

- A security group is created and security group rules are added to the security group. For more information, see Create a security group and Add security group rules.
- Internet or internal network access that will not be allowed or denied by your ECS instance is confirmed.

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. On the **Security Groups** page, find the security group from which you want to delete a security group rule and click **Add Rules** in the **Actions** column.
5. Click the direction of the security group rule.
   - If you want to delete a security group rule in a VPC, select **Inbound** or **Outbound**.
   - If you want to delete a security group rule in the classic network, select **Inbound**, **Outbound**, **Internet Ingress**, or **Internet Egress**.
6. Find the security group rule to be deleted and click **Delete** in the **Actions** column.
7. In the message that appears, click **OK**.

Related information

- RevokeSecurityGroup
- RevokeSecurityGroupEgress

2.Key pairs

2.1. SSH key pair overview

An SSH key pair is a secure authentication method provided by Alibaba Cloud for logon to your instance. An SSH key pair consists of a public key and a private key. You can use SSH key pairs to log on to only Linux instances.

Introduction

An SSH key pair is a pair of public and private keys that are generated based on a cryptographic algorithm. By default, 2048-bit RSA key pairs are used. Before you log on to a Linux instance with an SSH key pair, you must first create the SSH key pair. You can specify an SSH key pair when you create an instance, or bind an SSH key pair to an instance after the instance is created. Then, you can use the private key to connect to the instance.

After you create an SSH key pair, take note of the following items:

- Alibaba Cloud stores the public key of the SSH key pair. After an SSH key pair is bound to a Linux instance, the public key of the key pair is stored in the *~/.ssh/authorized_keys* file.
- You must download and securely store the private key for later use. The private key is in the unencrypted Privacy-Enhanced Mail (PEM)-encoded `PKCS#8` format.

Benefits

Compared with the username and password authentication, SSH key pairs have the following benefits:

- Security: SSH key pair-based authentication is more secure and reliable.
  - SSH key pairs provide higher security than common user passwords and can prevent brute-force attacks.
  - The private key cannot be deduced even if the public key is maliciously acquired.
- Ease of use:
  - If you configure the public key on a Linux instance, you can use the private key to run SSH commands or other tools for logon to the instance. This means you do not need to enter the password every time you log on.
  - You can log on to a large number of Linux instances, which enables easy management. If you need to manage multiple Linux instances, we recommend that you use this method.

Limits

SSH key pairs have the following limits:

- If you use an SSH key pair to log on to a Linux instance, the password logon method will be disabled for higher security.
- SSH key pairs apply only to Linux instances.
- Currently, only RSA 2048-bit key pairs can be created in the ECS console.
- An Alibaba Cloud account can have a maximum of 500 key pairs in a region.
- A Linux instance can be bound with only one SSH key pair. If your instance has a key pair bound, the new key pair will replace the original one.

- Instances of phased-out instance types cannot use SSH key pairs. For more information, see Phased-out instance types.
- If you bind an SSH key pair to or unbind an SSH key pair from an instance in the **Running** (`Running`) state, you must restart the instance for the operation to take effect. This enhances data security.

Creation method

You can use one of the following methods to create an SSH key pair:

- Create an SSH key pair in the ECS console. By default, the key pair is generated in the RSA 2048-bit format. For more information, see Create an SSH key pair.

  > **Note** If you create a key pair in the ECS console, you must download and securely store the private key for later use. After the key pair is bound to an instance, you cannot log on to the instance if you do not have the private key.

- Create an SSH key pair by using a key pair generator and import the key pair to the ECS console. The imported key pair must support one 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

2.2. Use an SSH key pair

2.2.1. Create an SSH key pair

This topic describes how to create an SSH key pair in the ECS console. After a key pair is created, immediately download and save its private key to a safe location. To log on to an ECS instance that is bound with a key pair, you must have the private key. You can have a maximum of 500 key pairs in a region.

secure logon SSH logon SSH logon Linux logon ECS

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Network & Security > SSH Key Pairs**.
3. In the top navigation bar, select a region.

4. Click **Create SSH Key Pair**.
5. On the **Create SSH Key Pair** page, configure the following parameters.

Parameter	Description
SSH Key Pair Name	The key pair name must be unique. The name must be 2 to 128 characters in length and can contain letters, digits, and the following special characters: periods (.), underscores (_), hyphens (-), and colons (:). It cannot start with a special character or digit.
Creation Type	You can select one of the following types of SSH key pairs: We recommend that you select **Auto-create** and save the private key in a timely manner. ○ **Auto-create**: The system automatically creates a key pair for you. Download the private key immediately after its creation. You cannot download the private key at any time afterwards. ○ **Import**: You can import a Base64-encoded public key.
Tag	You can bind one or more tags to the key pair to facilitate resource search and aggregation. For more information, see Overview.

6. Click **OK**.

What's next

Bind an SSH key pair to an instance

Related information

- CreateKeyPair

2.2.2. Import an SSH key pair

You can create an SSH key pair in the ECS console. You can also use a tool to generate a key pair and import its public key to Alibaba Cloud.

upload public key import public key

Prerequisites

The public key information of the key pair to be imported is obtained. For information about how to obtain public key information of key pairs, see View public key information.

Context

> **Note** Do not import the private key. You must keep the private key safe. To log on to an ECS instance that is bound with a key pair, you must have the private key.

An Alibaba Cloud account can have a maximum of 500 key pairs within a region. For more information, see Limits.

An imported public key must be encoded in `Base64` and support one 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

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Network & Security > SSH Key Pairs**.
3. In the top navigation bar, select a region.
4. Click **Create SSH Key Pair**.
5. Enter a key pair name and set Creation Type to **Import**.

   > **Note** The name of the SSH key pair must be unique. Otherwise, you will be prompted that the name is already in use.

6. In the **Public Key** field, enter the public key to be imported.
7. Click **OK**.

What's next

Bind an SSH key pair to an instance

Related information

- ImportKeyPair

2.2.3. Bind an SSH key pair to an instance

You can specify an SSH key pair when you create an instance, or bind an SSH key pair to the instance after the instance is created. This topic describes how to bind an SSH key pair to an ECS instance after the instance is created. If your ECS instance originally adopts password-based authentication, the password-based authentication is automatically disabled after the key pair is bound.

secure logon SSH logon ssh logon Linux logon ecs

Context

Each ECS instance can be bound with only one SSH key pair. If the ECS instance has already been bound with an SSH key pair, the new SSH key pair replaces the original one after the new SSH key pair is bound.

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Network & Security > SSH Key Pairs**.
3. In the top navigation bar, select a region.
4. Find the key pair to be bound and click **Bind** in the **Actions** column.
5. Select the target ECS instance in the **Select Instance** section, and then click the > icon to move the target instance to the **Selected** section. If instance names in the **Select Instance** section are dimmed, the instances are Windows instances and cannot be bound with SSH key pairs.
6. Click **OK**.
7. If the selected ECS instance is in the **Running** (*Running*) state, complete the following operations to restart the instance to make the binding operation take effect:
   i. In the left-side navigation pane, choose **Instances & Images > Instances**.
   ii. Find the target instance, and choose **More > Instance Status > Restart** in the **Actions** column.
   iii. In **Restart Instance** dialog box that appears, click **OK**.

What's next

- After an SSH key pair is bound to an ECS instance, you can log on to the ECS instance by using the SSH key pair. For more information, see Connect to a Linux instance by using an SSH key pair.
- If you want to log on to the instance by using the password after you bind a key pair, you can reset the instance password. Then, you can log on to the instance by using the key pair or the new password. For more information, see Reset the logon password of an instance.

Related information

- AttachKeyPair

2.2.4. Unbind an SSH key pair

This topic describes how to unbind an SSH key pair in the ECS console.

secure logon SSH logon SSH logon Linux logon ECS

Prerequisites

The SSH key pair is bound to an ECS instance. For more information, see Bind an SSH key pair to an instance.

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Network & Security** > **SSH Key Pairs**.
3. In the top navigation bar, select a region.
4. Find the key pair to be unbound and click **Unbind** in the **Actions** column.
5. Select the target ECS instance in the **Select Instance** section and click the > icon to move the target instance to the **Selected** section.
6. Click **OK**.
7. If the ECS instance is in the **Running** state, restart the instance to make the operation take effect.
   i. In the left-side navigation pane, choose **Instances & Images** > **Instances**.
   ii. Find the instance to be restarted, choose **More** > **Instance Status** > **Restart** in the **Actions** column.
   iii. In the **Restart Instance** dialog box, click **OK**.

What's next

After the SSH key pair is unbound, you must reset the password of the instance before you can log on to the instance as the root user. For more information, see Reset the logon password of an instance.

> **Note** If you have reset the password before you unbind the key pair, you can log on by using the password after you unbind the key pair.

Related information

- DetachKeyPair

2.2.5. Delete an SSH key pair

A deleted SSH key pair cannot be restored. However, instances that use the deleted SSH key pair are not affected. The deleted SSH key pair name is still displayed on the instance details page.

Prerequisites

An SSH key pair is created. For more information, see Create an SSH key pair.

Context

Before you delete an SSH key pair, note the following items:

- If you delete a key pair that is bound to an instance, the name of the deleted key pair will no longer be available to create or import key pairs. If you use the name of the deleted key pair to create or import a key pair, the console will report that the key pair already exists.
- If you delete a key pair that is not bound to an instance, the name of the deleted key pair will

still be available to create or import key pairs.

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Network & Security > SSH Key Pairs**.
3. In the top navigation bar, select a region.
4. Select one or more SSH key pairs.
5. Click **Delete**.

Related information

- DeleteKeyPairs

2.2.6. View public key information

This topic describes three ways to view public key information.

Windows

To view public key information, follow these steps:

1. Start PuTTYgen.
2. Click **Load**.
3. Select the *.ppk* or *.pem* file.
   PuTTYgen then displays the public key information.

Linux or macOS

Run the **ssh-keygen** command with the path of the *.pem* file specified.

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

The public key information similar to that of the following content is returned:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAxxxxxxxxxx+GF9q7rhc6vYrExwT4WU4fsaRcVXGV2Mg9RHe
x21hl1au77GkmnIgukBZjywlQOT4GDdsJy2nBOdJPrCEBIPxxxxxxxxxx/fctNuKjcmMMOA8YUT+sJKn3l7rCLkes
E+S5880yNdRjBiiUy40kyr7Y+fqGVdSOHGMXZQPpkBtojcxxxxxxxxxxx/htEqGa/Jq4fH7bR6CYQ2XgH/hCap29
Mdi/G5Tx1nbUKuIHdMWOPvjxxxxxxxxxx+lHtTGiAIRG1riyNRVC47ZEVCxxxxxx
```

> **Note** If the command fails, run the `chmod 400 my-key-pair.pem` command to modify the permissions to ensure that only you can view the file.

View the public key information in the instance

The public key information is in the *~/.ssh/authorized_keys* file. Open the file in the instance to view the public key information.

2.2.7. Add or replace an SSH key pair

You can add multiple key pairs to an instance, allowing these key pairs access to the instance. You can also replace existing key pairs.

Prerequisites

Make sure that you obtain the public key information of new key pairs. For more information, see View public key information.

Procedure

1. Use a current key pair to log on to the ECS instance.
2. Run the **vim .ssh/authorized_keys** command to open the file.
3. Add or replace public key information.
   - Add public key information: You can add and save new public key information under the existing public key information.

     ```
     ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCys3aOkFm1Xh8iN0lijeQF5mz9Iw/FV/bUUduZjaui
     Ja1KQJSF4+czKtqMAv38QEspiWStkSfpTn1g9qeUhfxxxxxxxxxx+XjPsf22fRem+v7MHMa7KnZWiHJxO
     62D4Ihvv2hKfskz8K44xxxxxxxxxx+u17IaL2l2ri8q9YdvVHt0Mw5TpCkERWGoBPE1Y8vxFb97TaE5+zc
     +2+eff6xxxxxxxxxx/feMeCxpx6Lhc2NEpHIPxMpjOv1IytKiDfWcezA2xxxxxxxxxx/YudCmJ8HTCnLId5
     LpirbNE4X08Bk7tXZAxxxxxxxxxx/FKB1Cxw1TbGMTfWxxxxxxxxxx imported-openssh-key
     ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDdlrdZwV3+GF9q7rhc6vYrExwT4WU4fsaRcVXGV2
     Mg9RHex21hl1au77GkmnIgukBZjywlQOT4GDdsJy2nBOdJPrCEBIPxxxxxxxxxxx/fctNuKjcmMMOA8YU
     T+sJKn3l7rCLkesE+S5880yNdRjBiiUy40kyr7Y+fqGVdSOHGMXZQPpkBtojcxxxxxxxxxxx/htEqGa/Jq4fH
     7bR6CYQ2XgH/hCap29Mdi/G5Tx1nbUKuIHdMWOPvjxxxxxxxxxx+lHtTGiAIRG1riyNRVC47ZEVCg9iTW
     WGrWFvxxxxxxxxxx/9H9mPCO1Xt2fxxxxxxxxBtmR imported-openssh-key
     ```

   - Replace public key information: You can delete existing public key information to add and save new public key information.

     ```
     ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDdlrdZwV3+GF9q7rhc6vYrExwT4WU4fsaRcVXGV2
     Mg9RHex21hl1au77GkmnIgukBZjywlQOT4GDdsJy2nBOdJPrCEBIP6t0Mk5aPkK/fctNuKjcmMMOA8YU
     T+sJKn3l7rCLkesE+S5880yNdRjBiiUy40kyr7Y+fqGVdSOHGMXZQPpkBtojcV14uAy0yV6/htEqGa/Jq4f
     H7bR6CYQ2XgH/hCap29Mdi/G5Tx1nbUKuIHdMWOPvjGACGcXclex+lHtTGiAIRG1riyNRVC47ZEVCg9iT
     WWGrWFvVlnI0E3Deb/9H9mPCO1Xt2fxxxxxxxxBtmR imported-openssh-key
     ```

     If you can log on to the instance by using new private keys, the key pairs are added or replaced.

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.

RAM permissions virtual quotient cross-product authentication ecs

Context

RAM is a resource access control service provided by Alibaba Cloud. For more information about RAM, 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 within your organization (such as employees, systems, or applications) need to access the instances, you can create an authorization policy that grants only specific RAM users access to these instances. This eliminates the risk of disclosing your AccessKey pair of your Alibaba Cloud account and helps maintain account security.
- **RAM user groups**: You can create multiple user groups and grant different permissions to each group. This way, RAM users in each group are assigned the same permissions. Example:
  - You can associate a user group with an authorization policy to deny access to specific ECS resources from IP addresses that are outside your corporate network.
  - You can move a RAM user from one user group to another to change the permissions of the users. Assume that you have two user groups: SysAdmins and Developers. The two groups are assigned different permissions.
    - SysAdmins: This user group needs permissions to create and manage ECS instances. You can associate the SysAdmins group with an authorization policy that allows its group members to perform all ECS operations to create and manage instances, images, snapshots, and security groups.
    - Developers: This user group only needs permissions to use ECS instances. 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 policies** and **custom policies**.

- **System policies**: the authorization policies provided by Alibaba Cloud. Some commonly used system policies for ECS instances or default policies included in RAM roles are as follows:
  - AliyunECSReadOnlyAccess: grants read-only permissions on ECS instances.
  - AliyunECSFullAccess: grants full administrative permissions on ECS instances.
  - AliyunECSNetworkInterfaceManagementAccess: grants permissions to manage ENIs.
  - AliyunECSImageImportDefaultRole: This role has permission to allow ECS instances to access OSS when you import custom images.
  - AliyunECSImageExportDefaultRole: This role has permission to allow ECS instances to access OSS when you export custom images.

  - AliyunECSDiskEncryptDefaultRole: This role has permission to access KMS when you encrypt images.

- **Custom policies**: the user-defined authorization policies. These policies are suitable for users who are familiar with various Alibaba Cloud APIs and require fine-grained access control. For more information about how to create a custom policy, see Step 2 (optional). Create a custom authorization policy.

Prerequisites

You have logged on to the RAM console using your Alibaba Cloud account.

Procedure

In the following example, the Alibaba Cloud account creates a RAM user in the RAM console and grants user-defined or system permissions to the RAM user.

- Step 1. Create a RAM user
- Step 2 (optional). Create a custom authorization policy
- Step 3. Authorize the RAM user

Step 1. Create a RAM user

You can perform the following steps to create a RAM user in the RAM console:

1. In the left-side navigation pane, click **Users** under **Identities**.
2. Click **Create User**.

   > **Note** To create multiple RAM users at a time, click **Add User**.

3. Specify the **Logon Name** and **Display Name** parameters.
4. Under **Access Mode**, select **Console Password Logon** or **Programmatic Access**.
   - **Console Password Logon**: If you select this check box, you must also complete the basic security settings for logon, including deciding whether to automatically generate a password or customize the logon password, whether the user must reset the password upon the next logon, and whether to enable multi-factor authentication (MFA).
   - **Programmatic Access**: If you select this check box, an AccessKey pair is automatically created for the RAM user. The user can access Alibaba Cloud resources by calling an API operation or by using a development tool.

     > **Note** We recommend that you select only one access mode for the RAM users to ensure the security of your Alibaba Cloud account. This prevents RAM users who have terminated their employment contracts with the company from accessing Alibaba Cloud resources.

5. Click **OK**.

Step 2 (optional). Create a custom authorization policy

In addition to the system policies provided by Alibaba Cloud, you can create custom policies in the RAM console by performing the following steps:

1. In the left-side navigation pane, click **Policies** under **Permissions**.

2. On the page that appears, click **Create Policy**.
3. On the Create Custom Policy page, specify the **Policy Name** and **Note** parameters.
4. Set **Configuration Mode**. You can select **Visualized** or **Script**.
   - If you select **Visualized**, click **Add Statement**. In the dialog box that appears, configure the permission effect, actions, and resources.
   - If you select **Script**, edit policy scripts based on Policy structure and syntax.

     If you select **Script**, you must specify values of the Action and Resource parameters in Statement based on the authentication list section in Authentication rules. For information about values of other parameters, see the following topic in the *RAM documentation*: Policy structure and syntax.

     - The following sample policy configured using scripts allows a RAM user to create pay-as-you-go instances.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
           "ecs:DescribeImages",
          "vpc:DescribeVpcs",
          "vpc:DescribeVSwitches",
          "ecs:DescribeSecurityGroups",
          "ecs:DescribeKeyPairs",
          "ecs:DescribeTags",
          "ecs:RunInstances"
       ],
       "Resource": "*"
    }
  ],
  "Version": "1"
}
```

     - The following sample policy configured using scripts allows a RAM user to create subscription instances. bss-related API operations can be called to query and pay subscription orders and the corresponding system policy is `AliyunBSSOrderAccess`.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
           "ecs:DescribeImages",
          "vpc:DescribeVpcs",
          "vpc:DescribeVSwitches",
          "ecs:DescribeSecurityGroups",
          "ecs:DescribeKeyPairs",
          "ecs:DescribeTags",
          "ecs:RunInstances",
          "bss:DescribeOrderList",
          "bss:DescribeOrderDetail",
          "bss:PayOrder",
          "bss:CancelOrder"
       ],
      "Resource": "*"
    }
  ],
  "Version": "1"
}
```

- The following sample policy configured using scripts allows a RAM user to query instance and disk information after the RAM user creates an ECS instance.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
           "ecs:DescribeInstances",
           "ecs:DescribeDisks"
       ],
      "Resource": "*"
    }
  ],
  "Version": "1"
}
```

5. Click **OK**.

Step 3. Authorize the RAM user

You can perform the following steps to authorize the RAM user in the RAM console:

1. In the left-side navigation pane, click **Users** under **Identities**.
2. In the **User Logon Name/Display Name** column, find the target RAM user.
3. Click **Add Permissions**. On the page that appears, the principal is automatically filled in.
4. In the **Policy Name** column, select the target policies by clicking the corresponding rows.

   > **Note** You can click **X** in the section on the right side of the page to delete the selected policy.

5. Click **OK**.
6. Click **Finished**.

What's next

After authorization is complete, the assigned permissions take effect immediately. The RAM user then can log on to the RAM console to manage the target cloud resources.

4.Instance RAM roles

4.1. Overview

You can bind an instance RAM role to an ECS instance. Applications deployed on the ECS instance can then access the APIs of other Alibaba Cloud services based on a Security Token Service (STS) temporary credential. This ensures the security of your AccessKey pair and helps you implement fine-grained permission control and management by using RAM.

STS temporary credential session persistence ECS access across cloud services

Scenarios

Applications deployed on ECS instances can access the APIs of other Alibaba Cloud services such as Object Storage Service (OSS), Virtual Private Cloud (VPC), and ApsaraDB for RDS in an Alibaba Cloud account or through an AccessKey pair of a RAM user. The AccessKey pair is configured in an ECS instance, such as writing the AccessKey pair to the configuration file, for easy management and quick calls. However, this method may cause problems such as information leaks and complex maintenance. It may also cause more permissions than necessary to be granted. Instance RAM roles can be used to avoid the preceding problems. For example, you can use an STS temporary credential to access other Alibaba Cloud services.

Instance RAM roles enable ECS instances to assume roles with certain access permissions. For more information about the roles, see RAM role overview.

Benefits

You can use instance RAM roles to perform the following operations:

- Associate a role with an ECS instance.
- Access other Alibaba Cloud services by using an STS temporary credential.
- Grant roles with different authorization policies to different instances so that these instances can have different access permissions on different cloud resources. This allows you to implement fine-grained access control.
- Modify permissions by changing the authorization policy of a role rather than manually changing the AccessKey pair. This allows you to efficiently manage access permissions of an ECS instance.

Billing

You are not billed for binding an instance RAM role.

Limits

Instance RAM roles have the following limits:

- The ECS instance must be a VPC-type instance.
- Only one RAM role can be bound to an ECS instance at a time.

References

- For more information about the cloud services that support STS temporary credentials, see Alibaba Cloud services that support RAM.
- For more information about how to access the APIs of other Alibaba Cloud services, see Access

other Cloud Product APIs by the Instance RAM Role.

4.2. Bind an instance RAM role

This topic describes how to create, authorize, and bind an instance RAM role in the RAM and ECS consoles.

Prerequisites

- The RAM service is activated. For more information, see Activate RAM.
- The network type of the ECS instance to which you want to bind a RAM role is VPC.
- A RAM user is authorized to use the instance RAM role if you use the RAM user to perform operations in this topic. For more information, see Authorize a RAM user to use an instance RAM role.

Context

- Only one RAM role can be bound to an ECS instance at a time.
- If you want to access the APIs of other Alibaba Cloud services from applications within an ECS instance that is bound with an instance RAM role, you must obtain a temporary authorization token for the instance RAM role by using the instance metadata. For more information, see Obtain a temporary authorization token.

Procedure

An Alibaba Cloud account is used in the following example to create an instance RAM role and bind the role to an ECS instance in the RAM console:

1. Step 1: Create an instance RAM role
2. Step 2: Authorize the instance RAM role
3. Step 3: Bind the instance RAM role

Step 1: Create an instance RAM role

Perform the following operations to create an instance RAM role in the RAM console:

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **RAM Roles**.
3. On the **RAM Roles** page, click **Create RAM Role**.
4. In the **Create RAM Role** pane, select **Alibaba Cloud Service** for the **Trusted Entity Type** parameter, and then click **Next**.
5. Select **Normal Service Role** for the **Role Type** parameter.
6. Specify the **RAM Role Name** and **Note** parameters.
7. Select **Elastic Compute Service** as the trusted service.
8. Click **OK**.

Step 2: Authorize the instance RAM role

Perform the following operations to attach a system policy or custom policy to the instance RAM role in the RAM console:

1. Log on to the RAM console by using an Alibaba Cloud account.
2. (Optional) Create a custom policy if you do not want to use a system policy. For more information, see Implement access control by using RAM.
3. In the left-side navigation pane, click **RAM Roles**.
4. In the **RAM Role Name** column, click the name of the target RAM role.
5. On the **Permissions** tab, click **Input and Attach**.
6. Select **System Policy** or **Custom Policy**.
7. Enter the policy name.
8. Click **OK**.
9. Click **Close**.

Step 3: Bind the instance RAM role

Perform the following operations to bind the instance RAM role to an ECS instance in the ECS console:

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images > Instances**.
3. In the top navigation bar, select a region.
4. Find the target ECS instance and choose **More > Instance Settings > Bind/Unbind RAM Role**.

5. In the Bind/Unbind RAM Role dialog box that appears, select an instance RAM role from the RAM Role drop-down list and click **OK**.

Alternatively, you can select an instance RAM role from the RAM Role drop-down list in the **RAM Role** field on the **System Configurations** page when you create an ECS instance. For more information, see Create an instance by using the provided wizard.

Related information

- CreateRole
- CreatePolicy
- AttachPolicyToRole
- AttachInstanceRamRole

4.3. Manage an instance RAM role

4.3.1. Replace an instance RAM role

After binding a RAM role to an ECS instance, you can replace the instance RAM role anytime.

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images > Instances**.
3. In the top navigation bar, select a region.
4. Find an ECS instance to which a RAM role has been bound. Choose **More > Instance Settings > Bind/Unbind RAM Role**.

5. Set **Action** to **Bind**. Select another instance RAM role in the **RAM Role** field and click **OK**.

Related information

- AttachInstanceRamRole

4.3.2. Unbind a RAM role

After binding a RAM role to an ECS instance, you can unbind the role at any time.

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images > Instances**.
3. In the top navigation bar, select a region.
4. Find an ECS instance to which a RAM role has been bound. Choose **More > Instance Settings > Bind/Unbind RAM Role**.

5. Set **Action** to **Unind**. Click**OK**.

Related information

- DetachInstanceRamRole

4.3.3. Obtain a temporary authorization token

You can obtain a temporary authorization token for an instance RAM role. With this periodically updated token, you can use the permissions and resources granted to the RAM role.

Procedure

1. Connect to the ECS instance remotely. For more information, see Overview.
2. Obtain a temporary authorization token for an instance RAM role. The name of the instance RAM role is EcsRamRoleDocumentTesting.
   - For Linux instances, run the `curl http://100.100.100.200/latest/meta-data/Ram/security-credentials/EcsRamRoleDocumentTesting` command.
   - For Windows instances, run the `Invoke-RestMethod http: // 100.100.100.200/latest/meta-data/Ram/security-credentials/EcsRamRoleDocumentTesting` PowerShell command.

     An example of the temporary authorization token obtained:

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

Related information

- Metadata

4.3.4. Authorize a RAM user to use an instance RAM role

If you want to bind, replace, and unbind an instance RAM role of a RAM user, you must use the Alibaba Cloud account to authorize the RAM user to use an instance RAM role. This operation can only be performed by an Alibaba Cloud account.

Context

When you authorize a RAM user to use an instance RAM role, you must grant the RAM user the PassRole permission on the instance RAM role. Without the PassRole permission, the RAM user cannot exercise the permissions specified in role policies.

Procedure

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **Users** under **Identities**.
3. In the **User Logon Name/Display Name** column, find the target RAM user.
4. Click **Add Permissions**. On the page that appears, the principal is automatically filled in.
5. In the **Authorization Policy Name** column, select the desired policies by clicking the corresponding rows.

   The authorization policy is as follows. [ECS RAM Action] indicates permissions that can be granted to the RAM user. For more information, see Authentication rules.

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs: [ECS RAM Action]",
        "ecs: CreateInstance",
        "ecs: AttachInstanceRamRole",
        "ecs: DetachInstanceRAMRole"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ram:PassRole",
      "Resource": "*"
    }
  ]
}
```

Note To remove a policy, select the policy from the right box and then click the × icon.

6. Click OK.
7. Click Finished.

Related information

- CreatePolicy
- AttachPolicyToRole

4.4. Use an instance RAM role by calling API operations

You can call API operations to create, authorize, and bind an instance RAM role.

Prerequisites

The RAM service is activated. For more information, see Billing in the RAM documentation.

Context

Instance RAM roles have the following limits:

- Instance RAM roles are applicable only to VPC-type ECS instances.

- Only one instance RAM role can be bound to an ECS instance at a time.
- If you want to access the APIs of other Alibaba Cloud services from applications within an ECS instance that is bound with an instance RAM role, you must obtain a temporary authorization token of the instance RAM role through the instance metadata. For more information, see Obtain a temporary authorization token.
- If you want to use an instance RAM role of a RAM user, you must use the Alibaba Cloud account to authorize the RAM user to use an instance RAM role. For more information, see Authorize a RAM user to use an instance RAM role.

Procedure

Perform the following operations to use an instance RAM role by calling API operations:

1. Step 1: Create an instance RAM role
2. Step 2: Authorize the instance RAM role
3. Step 3: Bind the instance RAM role
4. (Optional) Step 4: Unbind the instance RAM role
5. (Optional) Step 5: Obtain a temporary authorization token
6. (Optional) Step 6: Authorize a RAM user to use the instance RAM role

Step 1: Create an instance RAM role

Call the CreateRole operation to create an instance RAM role.

Set the RoleName parameter. For example, set this parameter to *EcsRamRoleDocumentTesting*.

Set the AssumeRolePolicyDocument parameter based on the following policy:

```
{
   "Statement": [
   {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
      "Service": [
      "ecs.aliyuncs.com"
      ]
      }
   }
   ],
   "Version": "1"
}
```

Step 2: Authorize the instance RAM role

Perform the following operations to authorize the instance RAM role:

1. Call the CreatePolicy operation to create an authorization policy.Configure the following

parameters:

- Set the RoleName parameter. For example, set this parameter to *EcsRamRoleDocumentTestingPolicy*.
- Set the PolicyDocument parameter based on the following policy:

```
{
   "Statement": [
     {
     "Action": [
       "oss:Get*",
       "oss:List*"
     ],
     "Effect": "Allow",
     "Resource": "*"
     }
   ],
   "Version": "1"
 }
```

2. Call the AttachPolicyToRole operation to authorize the role policy.Configure the following parameters:
   - Set the PolicyType parameter to *Custom*.
   - Set the PolicyName parameter. For example, set this parameter to *EcsRamRoleDocumentTestingPolicy*.
   - Set the RoleName parameter. For example, set this parameter to *EcsRamRoleDocumentTesting*.

Step 3: Bind the instance RAM role

Call the AttachInstanceRamRole operation to bind the instance RAM role.

Configure the following parameters:

- Set the RegionId and InstanceIds parameters to specify the ECS instance.
- Set the RamRoleName parameter. For example, set this parameter to *EcsRamRoleDocumentTesting*.

(Optional) Step 4: Unbind the instance RAM role

Call the DetachInstanceRamRole operation to unbind the instance RAM role.

Configure the following parameters:

- Set the RegionId and InstanceIds parameters to specify the ECS instance.
- Set the RamRoleName parameter. For example, set this parameter to *EcsRamRoleDocumentTesting*.

(Optional) Step 5: Obtain a temporary authorization token

You can obtain a temporary authorization token for an instance RAM role. With this periodically updated token, you can use the permissions and resources granted to the RAM role. Perform the following operations:

Query the temporary authorization token of the instance RAM role named EcsRamRoleDocumentTesting.

- Linux instance: Run the `curl http://100.100.100.200/latest/meta-data/Ram/security-credentials/EcsRamRoleDocumentTesting` command.
- Windows instance: For more information, see Metadata.

Obtain the temporary authorization token. The sample responses are as follow:

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

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

Perform the following operations to authorize a RAM user to use the instance RAM role:

> **Note** When you authorize a RAM user to use an instance RAM role, you must grant the PassRole permission to the RAM user on the instance RAM role. Without the PassRole permission, the RAM user cannot exercise the permissions specified in role policies.

1. Log on to the RAM console.
2. Authorize a RAM user to use the instance RAM role. For more information, see Grant permissions to a RAM user.

```
{
    "Version": "2016-10-17",
    "Statement": [
      {
      "Effect": "Allow",
      "Action": [
        "ecs: [ECS RAM Action]",
        "ecs: CreateInstance",
        "ecs: AttachInstanceRamRole",
        "ecs: DetachInstanceRAMRole"
      ],
      "Resource": "*"
      },
      {
    "Effect": "Allow",
    "Action": "ram:PassRole",
    "Resource": "*"
      }
    ]
}
```

[ECS RAM Action] indicates permissions that can be granted to the RAM user. For more information, see Authentication rules.

Related information

References

- Bind an instance RAM role
- Use RAM roles to access other Alibaba Cloud services
- CreateRole
- ListRoles
- CreatePolicy
- AttachPolicyToRole
- AttachInstanceRamRole
- DetachInstanceRamRole
- DescribeInstanceRamRole

5.Anti-DDoS Basic

Anti-DDoS Basic is a service that protects ECS instances from distributed denial-of-service (DDoS) attacks to ensure system stability. If the inbound traffic to an instance exceeds the maximum traffic allowed by the instance type, Alibaba Cloud Security will limit the inbound traffic.

Anti-DDoS Basic is a free service included in Alibaba Cloud Security. It offers up to 5 GB of mitigation capacity against common DDoS attacks. The ECS instance type determines the free-tier mitigation capacity, and you can log on to the Anti-DDoS Basic console to check the actual mitigation capacity threshold. For more information, see View black hole triggering thresholds in Anit-DDoS Origin Basic.

How Anti-DDoS Basic works

After the Anti-DDoS Basic feature is enabled, Alibaba Cloud Security monitors inbound traffic to ECS instances in real time. When massive traffic or unusual traffic involving DDoS attacks is detected, Alibaba Cloud Security redirects the traffic and removes malicious traffic. After the traffic is cleaned, the traffic is passed back to the target ECS instance. This process is called traffic scrubbing. For more information, see How Anti-DDoS Basic works.

> **Note** If Anti-DDoS Basic is enabled for an ECS instance, Alibaba Cloud Security triggers a black hole when the inbound traffic from the Internet is greater than 5 Gbit/s. All inbound traffic is routed to the black hole and the Internet access is blocked to secure the cluster. For more information, see Alibaba Cloud black hole policies in DDoS Protection.

Triggering conditions:

- Attack types. When specified attacks are identified in the inbound traffic, traffic scrubbing 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, traffic scrubbing is triggered no matter whether the traffic is normal or not.

The methods of traffic scrubbing include filtering attack packets, limiting the bit rate, and limiting the packet forwarding rate.

Therefore, you must configure the following thresholds when you use Anti-DDoS Basic:

- BPS threshold: When the inbound traffic exceeds this value, traffic scrubbing is triggered.
- PPS threshold: When the inbound packet forwarding rate exceeds this value, traffic scrubbing is triggered.

Traffic scrubbing thresholds of ECS instances

The traffic scrubbing threshold of an ECS instance is determined by its instance type.

- **Maximum BPS threshold (Gbit/s)**: For more information, see the **Bandwidth (Gbit/s)** specification in Instance families and Phased-out instance types.
- **Maximum PPS threshold (Kpps)**: For more information, see the **Packet forwarding rate (Kpps)** specification in Instance families and Phased-out instance types.

The following table describes the scrubbing threshold of ecs.g5.16xlarge.

Instance type	Maximum BPS threshold (Gbit/s)	Maximum PPS threshold (Kpps)
ecs.g5.16xlarge	20	4,000

What to do next

By default, Anti-DDoS Basic is enabled for ECS. You can perform the following operations after you create an ECS instance:

- Configure the scrubbing threshold: After an ECS instance is created, the maximum threshold of Anti-DDoS Basic for the instance type is used by default. However, the maximum BPS threshold for some instance types may be too high to be safe. Therefore, you must set a threshold based on your business needs. For more information, see Configure a cleaning threshold in Anti-DDoS Basic User Guide.
- Disable traffic scrubbing (not recommended): When the inbound traffic reaches the configured threshold, the entire traffic (including normal traffic) is cleaned. This may affect or interrupt normal business. Therefore, you can manually disable traffic scrubbing. For more information, see Cancel traffic cleaning in Anti-DDoS Basic User Guide.

> **Warning** After traffic scrubbing is disabled, when the inbound traffic is greater than 5 Gbit/s, all traffic is routed to a black hole. Proceed with caution.

6.Basic security services

Alibaba Cloud Security Center provides ECS with basic security services such as suspicious logon detection, vulnerability scan, and baseline check. You can check the security status of your ECS instances in the ECS console or Security Center console.

Context

Alibaba Cloud Security Center provides basic security services for free, such as vulnerability detection, security alerting, and baseline check, and collects and virtualizes security logs and fingerprints of ECS assets. You can view security information about ECS assets on the **Overview** page of the ECS console or in the Security Center console. For more information, see Security Center documentation.

The billing methods of basic security services are as follows:

- In Security Center Basic Edition, basic security services for ECS are provided for free.
- If you want to upgrade to Security Center Advanced or Enterprise Edition, log on to the Security Center console for a free trial or purchase of Security Center Advanced or Enterprise Edition. For the billing methods of Security Center Advanced Edition and Enterprise Edition, see the Billing methods in *Security Center documentation*.

Use the Security Center Agent

The Security Center agent is a lightweight security control that can be installed on ECS instances. If your ECS instance does not have the Security Center agent installed, your ECS instance will not be protected by Security Center. The security data of this instance, such as vulnerabilities, alerts, baseline vulnerabilities, and asset fingerprints, will not be displayed in the ECS console. For the installation paths of the Security Center agent, see Security Center agent overview.

You can perform the following steps to install or uninstall the Security Center agent:

- Have the Security Center agent automatically installed when you create an ECS instance.
  i. Log on to the ECS console.
  ii. In the left-side navigation pane, choose **Instances & Images** > **Instances**.
  iii. In the top navigation bar, select a region.
  iv. When you create an ECS instance, select **Security Hardening** in the **Image** section. The Security Center agent is then automatically installed on the new ECS instance. For more information, see Create an instance by using the provided wizard.

  > **Note** If you call the RunInstances operation to create an ECS instance, you can also have the Security Center agent automatically installed on the instance by setting `SecurityEnhancementStrategy` to Active.

- Manually install the Security Center agent on an existing ECS instance.
  i. Log on to the ECS console.
  ii. On the **Overview** page, click **Handle** in the **Security Score** section to go to the Security Center console.

iii. Install the agent. For more information, see the Install the Security Center agent in *Security Center documentation*.

- Uninstall the Security Center agent
  i. Log on to the ECS console.
  ii. On the **Overview** page, click **Handle** in the **Security Score** section to go to the Security Center console.
  iii. Uninstall the agent. For more information, see the Uninstall the Security Center agent in *Security Center documentation*.

Check the security status of your ECS instance

You can perform the following steps to check the security status of your ECS instance:

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images > Instances**.
3. In the top navigation bar, select a region.
4. Check the security status of your ECS instance by using one of the following methods:
   - Method 1: On the **Instances** page, view the Alibaba Cloud Security icon in the Monitoring column corresponding to your ECS instance. If the icon is orange, there are vulnerability or security alerts in the instance. You can click the icon to log on to the Security Center console and view the alert details.

     
   - Method 2: Click the instance ID to go to the **Instance Details** page. On the **Instance Details** page, view the Alibaba Cloud Security icon. If the icon is orange, there are vulnerability or security alerts in the instance. You can click the icon to log on to the Security Center console and view the alert details.

     

Set alert notifications

Basic security services allow you to configure alert notifications for security alert items. The alert notifications can be sent by SMS, emails, or internal messages. Perform the following steps to configure alert notifications:

1. Log on to the ECS console.
2. On the **Overview** page, click **Handle** in the **Security Score** section to go to the Security Center console.
3. In the left-side navigation pane, choose **Operation > Settings** and click the **Notifications** tab.
4. In the **Alerts** row, select severities and configure the methods and time for sending alert notifications.

   

   > **Note** If you have upgraded to Security Center Advanced or Enterprise Edition, see the Overview in *Security Center documentation* to learn more alert notification methods.

Related information

Documentation

- Feature comparison among Basic/Advanced/Enterprise Edition
-
-
- RunInstances

7.Security FAQ

What is a security group?

A security group is a virtual firewall that implements access control for one or more ECS instances. 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 to add it to the instance. By default, instances within the same security group can communicate with each other but instances in different security groups are isolated from each other. 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 security groups, the instance will be 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.

Why am I being prompted that the maximum number of rules has been reached when I try to 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 to which the instance can be added × Maximum number of rules in each security group.

If you are prompted that **Failed to join the security group. The number of security group rules that have acted on the instance has reached the upper limit**, we recommend that you select another security group.

If I adjust the maximum number of security groups that a VPC-type ECS instance can belong to, does this adjustment only take effect on security groups created after the limit is adjusted?

No, the adjustment will take effect on all security groups that the VPC-type ECS instance belongs regardless of when these security groups were created.

In what scenarios do security groups use the default security group rules?

The default security group rules are used in the following scenarios:

- If you have not created a security group when you create an ECS instance in a region in the ECS console for the first time, you can select a default security group automatically created by the system. The default security group is a basic security group. The default security group uses the default security rules. The default security rule has the priority of 100. It specifies that inbound traffic is allowed over ICMP, SSH port 22, and RDP port 3389 and that the authorization object is all CIDR blocks (0.0.0.0/0). You can also choose to allow inbound traffic over HTTP port 80 and HTTPS port 443. All outbound traffic is allowed.
- You have selected a security group template when you created a security group in the ECS console. The security group template applies to both basic security groups and advanced security groups. Alibaba Cloud provides Web Server Linux templates (inbound traffic is allowed over port 80, port 443, port 22, and ICMP), Web Server Windows templates (inbound traffic is allowed over port 80, port 443, port 3389, and ICMP), and custom templates (all inbound access requests are denied).

In what scenarios do I need to add a security group rule?

In the following scenarios, you must add a security group rule to ensure that your ECS instances can be accessed:

- No custom security group rules or default security group rules have been added to the

security group to which the ECS instance belongs. When your ECS instance needs to access the Internet or an ECS instance in another security group within the current region, you must add a security rule.

- The created application uses a specified port or port range instead of the default port. In this case, you must allow the specified port or port range before you can check whether the application is connected. For example, assume you have deployed an NGINX service and need to set the listener port to TCP 8000 but only port 80 is allowed in your security group. In this case, you must add a security rule to ensure that the NGINX service is accessible.
- For other scenarios, see Scenarios for security groups.

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

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

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.

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 or the Internet. These are examples of the effects:

- 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 200. For more information, see Limits.

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 200 security group rules. Each ENI of an ECS instance can be added to up to five security groups, allowing each ENI of an ECS instance to be associated with up to 1,000 security group rules.

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.

What can I do if I receive a notification that my website has been blocked due to illegal activities and needs to be rectified?

You can check the records of harmful Internet information to view domain names or URLs with harmful information, penalty actions, reasons, and duration. After you are sure that the harmful information from your domain name or URL has been cleared or does not exist, you can apply to unblock the domain name or URL. For more information, see Harmful Internet information.

What can I do if I receive a notification that my website has been penalized for committing external attacks?

You can check the penalty records to view the details about penalty actions, reasons, and duration. If you do not agree with the penalty measure, provide your feedback and file an appeal. After receiving your feedback on the penalty records, Alibaba Cloud will verify the penalty again, check whether the penalty is correct and effective, and determine whether to maintain or immediately terminate the penalty. For more information, see View the penalty list.

How can I view the resource quota?

For more information about how to view the limits and quotas of resources, see Limits.