ALIBABA CLOUD

Alibaba Cloud

Elastic Compute Service

Security

Document Version: 20220620

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.Best practices for security

This topic describes how to improve the security of instances when you create and use them.

Context

Security covers a variety of aspects. Alibaba Cloud guarantees the security of the Alibaba Cloud infrastructure and services such as data centers and virtualization platforms. However, when you use Alibaba Cloud services, you must also follow the best practices for security such as controlling traffic, keeping confidential information, and controlling permissions.

Use the account security features

Alibaba Cloud provides the following account-related security features to help you avoid risks at the account level:

- Enable multi-factor authentication (MFA) for Alibaba Cloud accounts.

  When MFA is enabled, a dynamic authentication code generated by an MFA device is required in addition to your username and password when you attempt to log on to the Alibaba Cloud Management Console. This way, unauthorized access can be blocked to ensure security of your account in the event of password leaks.

- Use Resource Access Management (RAM) users and user groups to control access to resources at the account level.

  If multiple users want to use the same resources, we recommend that you do not share your Alibaba Cloud account with these users. If you share the AccessKey pair of your Alibaba Cloud account with other users, confidential information may be leaked, and the security of all resources within your account may be threatened. We recommend that you create RAM users and user groups and grant them the minimum permissions to reduce security risks.

  RAM users can be used to represent employees, systems, and applications within an enterprise. You can grant the minimum access permissions to the RAM users based on your needs. If RAM users have clear responsibilities, you can classify RAM users that have the same responsibilities to the same RAM user group to improve management efficiency. For example, you can perform the following operations:

  i. Create a SysAdmins user group for RAM users who create and use resources and attach policies to grant them permissions to perform all operations.
  ii. Create a Developers user group for RAM users who use resources and attach policies to grant them permissions to call the StartInstance, StopInstance, and DescribeInstances operations.
  iii. Create RAM users for employees and add them to different groups based on their positions.
  iv. Attach policies to deny group users access to the enterprise resources if their IP addresses are from outside the enterprise. This can enhance network security.
  v. If employees change positions from developers to system administrators, move their associated RAM users from the Developers user group to the SysAdmins user group.
  vi. If RAM users in the Developers user group require more permissions, modify the policies of the user group to grant more permissions to all RAM users in the group.

  For more information, see Control access to resources by using RAM users.

- Use an instance RAM role to ensure the confidentiality of AccessKey pairs.

To allow applications deployed on an Elastic Compute Service (ECS) instance to call API operations of other Alibaba Cloud services such as Object Storage Service (OSS), Virtual Private Cloud (VPC), and ApsaraDB RDS, do not store AccessKey pairs on the instance, such as by writing an AccessKey pair to configuration files, which increases the risk of leaks.

We recommend that you assign a RAM role to the instance, and the ECS instance can assume the RAM role. Then, you can use temporary tokens issued by Security Token Service (STS) to call API operations of other Alibaba Cloud services. This ensures the security of your AccessKey pair and helps you implement fine-grained permission control and management by using RAM. For more information, see Overview.

Enable security compliance when you create instances

Alibaba Cloud provides features that meet the requirements of security compliance for instances, such as instance types and disk encryption. You can use them based on your needs.

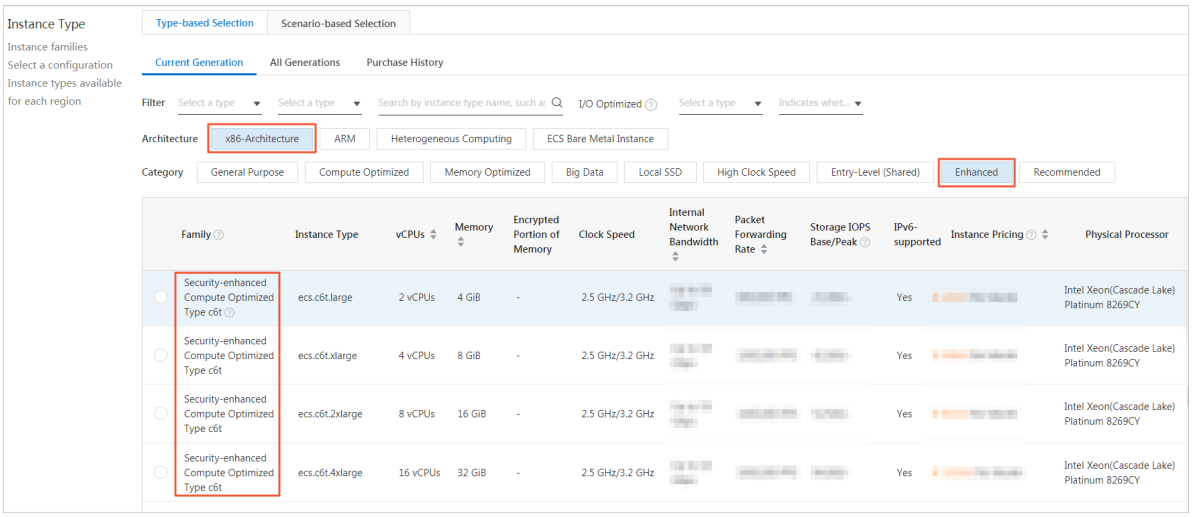
- Activate Key Management Service (KMS).

  If you want to encrypt data related to cloud services, we recommend that you activate KMS in advance. You can enable data encryption in cloud services without the need to develop and maintain the cryptographic infrastructure on your own. For example, you can enable disk encryption and trusted boot on ECS instances. For more information, see Activate KMS.

- Create security-enhanced instances for business scenarios that require high security and enhanced trust.

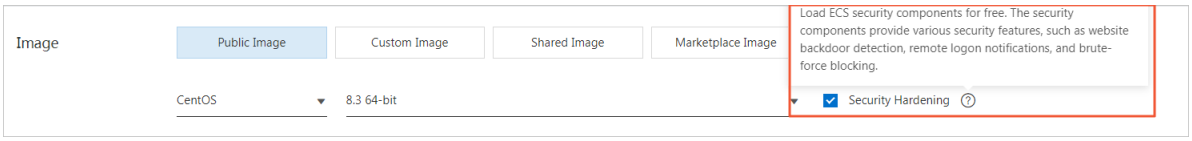
  Security-enhanced instances provide the trusted computing capability based on Trusted Cryptography Module (TCM) or Trusted Platform Module (TPM) chips. This ensures trusted boot of instances and the security of private data on instances. For more information, see Overview.

  Example: Select c6t, the security-enhanced compute-optimized instance family.



- Enable security hardening for instances that use public images.

Instances that have security hardening enabled load basic security components when they start. These components can be used to check the security configurations of cloud services for exceptional logons, DDoS attacks, and common vulnerabilities. In addition, assets of the instances can be managed in Security Center in a centralized manner. For more information, see Introduction to Security Center Basic.

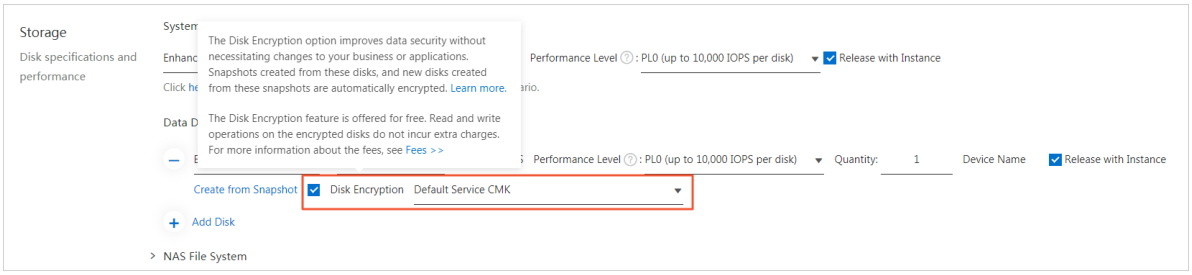


- Enable disk encryption.

  Disks are encrypted by using the AES-256 algorithm. You can use the keys managed in KMS to ensure the security of data stored on disks without the need to build or maintain your key management infrastructure. For more information, see Encrypt a system disk and Encrypt a data disk. The following section describes the effect of disk encryption:

  - System disk: Data in the operating system is automatically encrypted. The data is decrypted when it is read.
  - Data disk: After an encrypted data disk is attached to an instance, data stored on the disk, data transmitted between the disk and the instance (excluding data in the operating system), and data transmitted from the instance to a backend storage cluster are automatically encrypted. The data is decrypted when it is read. In addition, snapshots created from encrypted disks and disks created from encrypted snapshots are automatically encrypted.

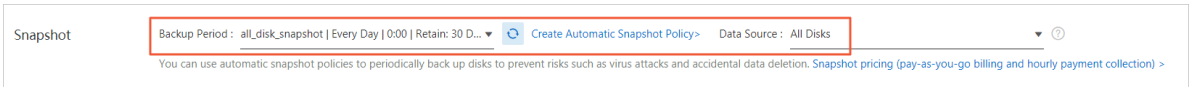
  For example, you can encrypt the data disk created along with an instance, as shown in the following figure.



- Use snapshots to back up data for disaster recovery.

  Snapshots are a convenient and efficient method for data disaster recovery. You can create snapshots for a disk to back up data stored on the disk on a regular basis. If the data is exceptional or lost due to system failures or accidental operations, you can use the most recently created snapshot to restore the data to reduce loss. Before you perform high-risk operations, we recommend that you create snapshots to avoid unexpected outcomes.

  For example, you can enable the snapshot service for an instance when you create the instance, as shown in the following figure. This way, snapshots are automatically created for all disks of the instance on a daily basis.



Build a secure network environment for instances

When you build a network environment for an instance, you can perform operations such as network isolation and network throttling on the instance to reduce the chances of being exposed to attacks.

- Use security groups to decrease the attack range.

  A security group is a virtual firewall that is used to control the inbound and outbound traffic of instances in the security group. We recommend that you perform the following operations when you use a security group:

  - Use a security group as a whitelist that denies all access by default. You can add rules to allow access to or from specific destinations or sources on specific ports. Security group rules can be configured based on 5-tuples. You can implement fine-grained control of source IP addresses, destination IP addresses, source ports, destination ports, and transport layer protocols. For more information, see Security group quintuple rules.
  - Follow the principle of least privilege when you configure security group rules. For example, to allow connections to port 22 on a Linux instance, we recommend that you add a rule to allow access from specific IP addresses instead of all IP addresses (`0.0.0.0/0`).

    Alibaba Cloud provides the feature of detecting potential high-risk security groups to help you identify security group rules that do not restrict access.

    If security group rules that do not restrict access are identified, check whether you need to allow traffic on the corresponding port and modify the excessive permissions in a timely manner. For example, if MySQL is installed on your instance, access to the Internet cannot be allowed over port 3306 by default. Modify the current security group rules to deny access from all IP addresses, set priority to the smallest value, and then follow the principle of least privilege to add security group rules that allow access.
  - Make sure that the rules in each security group are simple and clear. A single instance can be added to multiple security groups. A single security group can contain multiple rules. If an excessive number of rules are applied to an instance, management complexity is increased, and risks are introduced.
  - Add instances that serve different purposes to different security groups and separately maintain the security group rules applied to the instances. For example, if you add instances that need to be accessible from the Internet to a single security group, you must add rules to the security group to enable only ports that are used to provide external services, such as ports 80 and 443 because the security group that contains no rules denies all access by default. To ensure that instances accessible from the Internet do not provide other services such as MySQL and Redis, we recommend that you deploy internal services on the instances inaccessible from the Internet and then add these instances to another security group.
  - Make proper use of mutual access between basic security groups. By default, instances in basic security groups can access each other. In some cases, the default mutual access can decrease management complexity. For example, if multiple security groups exist and you want to add complex rules for instances that require access to each other over the internal network, you can create a security group for these instances. However, if the number of instances is large, we recommend that you do not use a security group to manage all instances, which makes it complex to manage the outbound rules of the group.

    Basic security groups can also be configured with internal isolation rules. For more information, see Network isolation within a basic security group.

- Make proper use of mutual access authorization between basic security groups. For example, in distributed applications, the SG_Web security group is created for the Web service and the SG_Database security group is created for the MySQL database service. You can add a rule to SG_Database to allow all instances in SG_Web to access port 3306 of instances in SG_Database.

  The private IP addresses of instances of the classic network type frequently change. We recommend that you authorize mutual access between security groups and do not enable authorization based on CIDR blocks or private IP addresses.
- Do not modify the security groups that are used in the production environment. All changes to a security group are automatically applied to the instances in the security group. Before you change a security group, you can clone, change, and debug it in the test environment to ensure that the change does not interrupt the communication between the associated instances.
- Specify identifiable names and tags for security groups for easy search and management. For more information about tags, see Create or bind a tag.

For more information about the scenarios and practical suggestions of security group configurations, see the following topics:

- Security groups for different use casesConfiguration guide for ECS security groups
- Best practices of the security group (part 1)
- Best practices for ECS security groups (part 2)
- Best practices for ECS security groups (part 3)

- Use VPC to isolate services of different security levels within an enterprise.

  VPCs are logically isolated from each other based on tunneling technology. You can implement network isolation by using VPC. We recommend that you perform the following operations when you use VPC:

  - Deploy business systems that require strict isolation in different VPCs, such as the production and test environments.
  - You can use vSwitches to divide a VPC into multiple subnets and manage services that have different access policies. For example, you can deploy web services in subnets that can access the Internet and deploy database services in subnets that are completely isolated from the outside.

  For more information about network planning based on business scenarios, see Plan networks.
- Make proper use of jump servers or bastion hosts to defend against internal and external intrusions.

  In a VPC, we recommend that you create dedicated vSwitches for instances used as jump servers. You can access the Internet by assigning elastic IP addresses (EIPs) or configuring port forwarding tables of NAT gateways and control access by using security groups. For example, you can perform the following operations:

  i. Create the SG_Bridge security group for the jump server. You can authorize access to only required ports (such as port 22 on a Linux instance and port 3389 on a Windows instance) and restrict the authorized object to specific IP addresses or CIDR blocks to reduce unauthorized logons to the jump server.
  ii. Add the jump server to the SG_Bridge security group.
  iii. Configure access rules for the security group to allow the jump server to access instances in other security groups.

For example, you can add rules to the SG_Current security group and specify the SG_Bridge security group as the authorization object to control access to specific ports by using specific protocols.

> **Note** When you use the jump server to log on to another instance, we recommend that you preferentially use SSH key pairs. For more information, see Overview.

Jump servers can enhance security. However, excessive permissions are offered to the jump servers, which makes operation auditing difficult. You can use bastion hosts that are more secure to meet the O&M requirements of access controlling, operation auditing, and security compliance. Alibaba Cloud also provides Bastionhost. For more information, see What is Bastionhost?

- Allow only required instances to access the Internet.

  Access management can be simplified, and the risks of external attacks can be reduced by allowing required instances to access the Internet in a proper manner. We recommend that you perform the following operations:

  - Most distributed applications contain different layers and groups. Do not assign public IP addresses to instances that cannot access the Internet. If multiple instances can access the Internet, we recommend that you use Server Load Balancer (SLB) to distribute the Internet traffic to improve security and availability. This avoids exposing excessive instances to the Internet and affecting access due to single points of failure of instances. For more information, see What is CLB?
  - If instances that are not assigned public IP addresses in VPCs need to access the Internet, use the SNAT feature of NAT gateways to enable instances without public IP addresses in VPCs to access the Internet. This avoids exposing instances that require only access the Internet to the Internet. For more information about how to specify instances or vSwitches to access the Internet when you create an SNAT entry, see Create and manage SNAT entries.

Use security services to build a security defense system

Alibaba Cloud provides a comprehensive range of security services to improve the security of your cloud assets in various scenarios.

- Use Alibaba Cloud Anti-DDoS services to defend against traffic flood attacks.

  In a DDoS attack, multiple computers launch coordinated attacks against one or more intended servers by using malicious programs. The attack undermines the performance or consumes network bandwidth and causes the intended servers to be unable to provide services.

  Alibaba Cloud provides the Anti-DDoS Origin and Anti-DDoS Premium services. Anti-DDoS Origin enhances the DDoS attack defense capability for instances such as ECS instances, SLB instances, Web Application Firewall (WAF) instances, and EIPs that have public IP addresses assigned and is applicable to the business whose resources are deployed on the cloud. When the traffic exceeds the default scrubbing threshold that is predefined in Anti-DDoS Origin, traffic scrubbing is automatically triggered to mitigate DDoS attacks. For more information about how to customize the traffic scrubbing threshold, see Configure a traffic scrubbing threshold.

  Anti-DDoS Origin provides a basic defense capacity of up to 5 Gbit/s against DDoS attacks for free. By default, Anti-DDoS Origin is enabled. If you need advanced defense capacity, purchase other paid editions of Anti-DDoS services. For more information, see Overview.

- Connect instances to Security Center to defend against system security vulnerabilities.

Security Center Basic provides free basic features to harden the security of your instances. You can use these features to detect risks on your instances, such as exceptional logons, DDoS attacks, common vulnerabilities, and configuration risks of Alibaba Cloud services. For more information, see Introduction to Security Center Basic.

Security Center Basic detects risks, but cannot handle these risks. If you need features such as vulnerability fixing and proactive defense, go to the Security Center console to purchase a paid edition of Security Center.

Paid editions of Security Center provide the following features in addition to basic security hardening capabilities:

- Vulnerability fixing: fixes Linux software vulnerabilities and Windows system vulnerabilities. Vulnerabilities can lead to long-standing security risks. Security Center can detect vulnerabilities in a timely manner and improve vulnerability fixing efficiency.
- Virus defense: provides the antivirus feature to scan for persistent viruses and generates alerts when persistent viruses are detected. This feature also supports virus deep cleaning and data backup to prevent viruses from intruding your instances.
- Security alerting: generates alerts when Security Center detects web tampering proofing, web shells, exceptional logons, suspicious processes, and malicious processes. You can identify the security threats to your assets based on these alerts.

For more information about the features of Security Center, see Features.

- Purchase Alibaba Cloud WAF to defend against application security vulnerabilities.

  WAF identifies malicious traffic, scrubs and filters the traffic, and then forwards normal traffic to your web server. WAF protects your web server against attacks and ensures the security of your data and business.

  When you use WAF, your instance can defend against common web application attacks and mitigate HTTP attacks without the need to install hardware or software or adjust route configurations. This improves the security of websites. For more information about how to enable WAF, see Quick start.

  When WAF is used with Anti-DDoS services and Security Center, the protection capability can be enhanced, and business security can be improved in a comprehensive manner.

Complete security configurations in the instance operating system

Proper security configurations in the operating system of an instance can reduce the risk of being intruded.

- Improve the security of logon configurations.
  - Linux instances:
    - Use only SSH key pairs to log on to Linux instances. An SSH key pair is a pair of public and private keys that are generated based on an encryption algorithm. By default, 2048-bit RSA key pairs are used. SSH key pairs are more secure and convenient than passwords. For more information about how to use SSH key pairs and their features, see Overview and Connect to a Linux instance by using an SSH key pair.
    - Do not log on to a Linux instance by using a root user. Use another user as the administrator. If the user wants to perform operations that require the administrator permissions, run the sudo command to grant the administrator permissions to the user.

  - Windows instances: Use a strong password. The password must be 8 to 30 in length and must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters (( ) ` ~ ! @ # $ % ^ & * _ - + = | { } [ ] : ; ' < > , . ? /). We recommend that you include special characters in the password. When you use a password to log on to an instance, we recommend that you change the password on a regular basis.

- Protect service ports.

  When an instance is used to provide services, the service ports of the instance are enabled. The more service ports are enabled, the higher the potential risk. We recommend that you enable only required service ports, modify the default port numbers of the service ports to port numbers that are greater than 30000, and use firewalls and security groups to control access to the ports. For more information about how to modify the default remote port of an instance, see Modify the default port used by an instance to accept connections.

  For example, you can access the database services only over the internal network to avoid exposing the database services to the Internet. If you want to access the database services over the Internet, you can modify the default port number (such as port 3306 for MySQL databases) to a higher port number and authorize specific IP addresses to access the database services.

- Do not use weak passwords.

  If you use weak passwords that are easy to guess and crack, your instances may be prone to unauthorized access or be destroyed, and your data may be stolen. We recommend that you set a complex password and change it on a regular basis.

Follow the best practices for security when you use services

In addition to using security services and making security configurations, you must also follow the best practices for security to avoid leaks of confidential information such as AccessKey pairs and logon passwords and use the audit features to track the use of the confidential information when you complete the security configurations and use security services.

- Properly keep and use confidential information.
  - AccessKey pairs of Alibaba Cloud accounts are equivalent to the logon passwords used to call API operations of cloud services. AccessKey pairs are also important identity credentials to access cloud resources. We recommend that you perform the following operations:
    - Use the AccessKey pairs of RAM users instead of those of Alibaba Cloud accounts and follow the principle of least privilege to grant permissions to RAM users. This avoids threats to the security of all resources within the account due to the leaks of the AccessKey pair of the account.
    - Do not write AccessKey pairs into code to avoid accidental leaks along with the code.
    - Change AccessKey pairs on a regular basis to ensure that online business is not affected if the previous AccessKey pairs are leaked.
    - Delete AccessKey pairs that are no longer needed.
    - Enable ActionTrail and store operation logs in OSS buckets and Log Service Logstores.
    - Take note of the AccessKey pair leak notifications from Security Center. By default, the AccessKey pair leakage check feature of Security Center is enabled. If AccessKey pairs leaked on GitHub are detected, Security Center sends you a notification so that you can respond in a quick manner and minimize the negative impacts.

  - To ensure the security of key pairs and passwords, we recommend that you perform the following operations:
    - Use different keys and passwords on different platforms to avoid threats to the security of all resources on the platforms due to the leaks of the keys and passwords.
    - Do not share keys and passwords between different users on instances.
    - Keep the purpose of a key simple. For example, do not use the keys used to log on to instances for other scenarios.
  - Use KMS to manage confidential information and do not store passwords and keys in plaintext.

  For more information, see Best practices to prevent AccessKey pair leaks.

- Encrypt data in transit.

  Use encryption protocols such as Transport Layer Security (TLS) 1.2 or later to encrypt sensitive data transmitted between instances and clients, and configure security groups and firewalls in the operating system to ensure that only encrypted communications are allowed between instances and sensitive remote network services.

- Enable ActionTrail.

  After you enable ActionTrail, the events of all accounts can be recorded and stored in an OSS bucket or a Log Service Logstore. You can implement security analytics, resource change tracking, and compliance auditing based on these records. For more information, see Create a single-account trail. The following examples show the applications of ActionTrail:

  - Analyze information such as the logon time, logon IP addresses, and whether MFA is enabled to determine whether the account has security risks such as exceptional logons.
  - Use RAM to manage the identities of multiple members in an organization and obtain the detailed operation records to meet the compliance auditing requirements of the organization.
  - In the event of exceptional changes to the state of resources, such as an exceptional shutdown of an instance, use the operation logs to search for information such as the operator, operation time, and operation IP addresses to identify and troubleshoot the exception.

2.Security groups

2.1. Overview

A security group acts as a virtual firewall to control the inbound and outbound traffic of Elastic Compute Service (ECS) instances to improve security. Security groups provide Stateful Packet Inspection (SPI) and packet filtering capabilities. You can use security groups and security group rules to define security domains in the cloud.

Security groups and security group rules

Security groups are classified into basic security groups and advanced security groups. Advanced security groups are suitable for enterprise-level scenarios and can contain more instances, elastic network interfaces (ENIs), and private IP addresses and implement more rigorous levels of access control than basic security groups.

- The following rules apply when you add instances to security groups:
  - Each instance must belong to one or more security groups.
  - The secondary ENIs that are attached to an instance can be assigned to security groups different from those of the instance.
  - An instance cannot belong to a basic security group and an advanced security group at the same time.
- Security groups can control inbound and outbound traffic even before you manually add rules to the security groups. You can manually add and modify the rules of security groups to implement finer-grained traffic control. After rules are added to a security group or after rules in the security group are modified, the rules are automatically applied to instances in the security group. Security group rules can be used to control access to or from specific IP addresses, CIDR blocks, security groups, or prefix lists. For more information, see Add a security group rule.
- When you create security groups in the ECS console, default rules are automatically added to the security groups. You can maintain the rules based on your needs.

> **Note**
>
> - When you create security groups by calling API operations, no default rules are added to the security groups.
> - Security groups are stateful. The maximum session timeout period for a security group is 910 seconds. After instances in a security group can be accessed and sessions are established between the instances, the security group allows traffic in both directions during the same session. For example, if a request traffic during a session is allowed to flow in, the corresponding response traffic is also allowed to flow out.

The following table describes the differences between basic and advanced security groups.

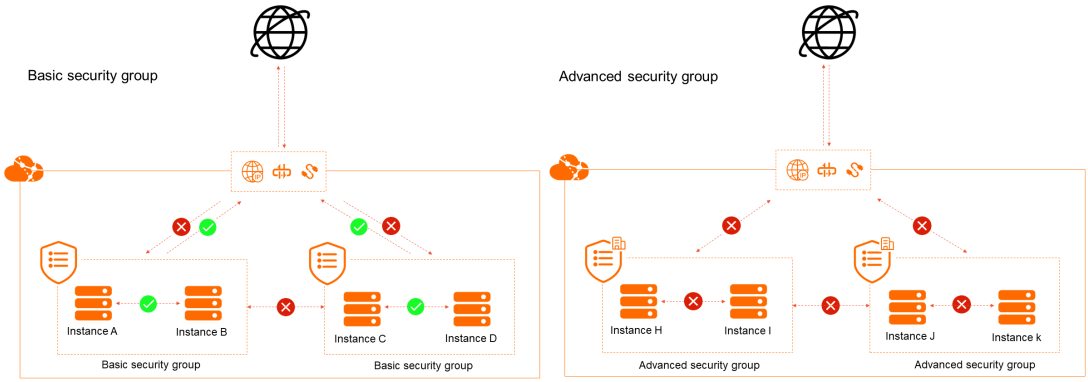
Comparison item	Basic security group	Advanced security group
Supported network type	Virtual Private Cloud (VPC) and classic network	VPC

Comparison item	Basic security group	Advanced security group
Support for all instance types	Yes	No, only instance types that use VPC are supported.
Number of private IP addresses supported in the classic network	1,000①	The classic network is not supported.
Number of private IP addresses supported in VPCs	2,000②	65,536③
Support for adding security group rules that allow or deny access	Yes	Yes
Support for specifying policy priority	Yes	Yes
As the authorization objects of security group rules for other security groups	Supported	Not supported
Network communication policy for instances within the same security group when no security group rules are added	• Instances and ENIs in the same basic security group can communicate with each other over the internal network. The internal communication has a higher priority than other communications controlled by using custom rules. • Instances and ENIs in a basic security group are isolated from instances and ENIs in a different basic security group over the internal network. • By default, all inbound access requests are denied. The following Access request control of security groups that have no rules shows how access is controlled by a basic security group that has no rules.	• Instances and ENIs in the same advanced security group are isolated from each other over the internal network. • Instances and ENIs in an advanced security group are isolated from instances and ENIs in a different advanced security group over the internal network. • By default, all access requests are denied. The following Access request control of security groups that have no rules shows how access is controlled by an advanced security group that has no rules.

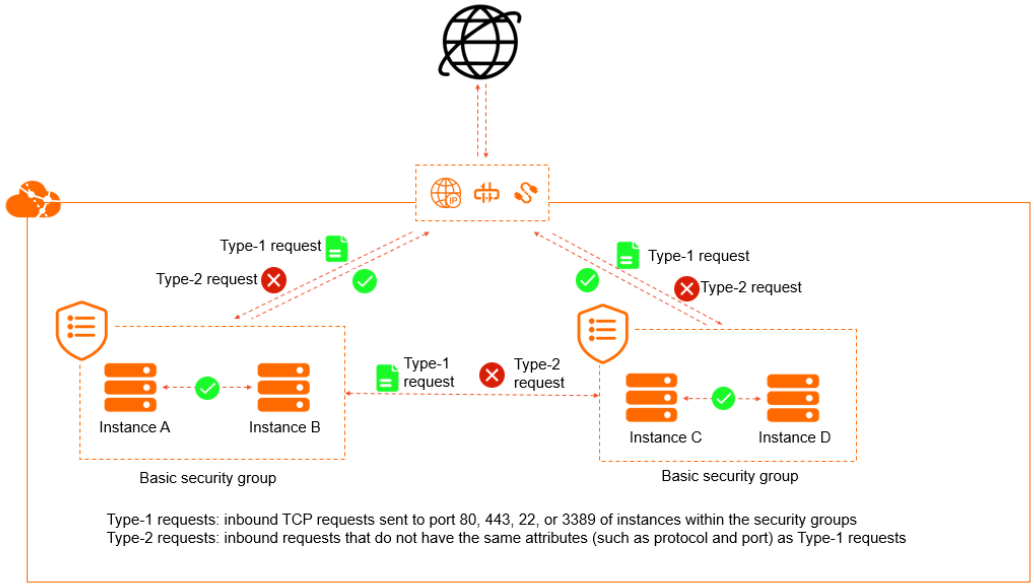
Comparison item	Basic security group	Advanced security group
Default rules when a security group is created in the ECS console	• Inbound: four inbound rules that allow TCP access from all IP addresses to ports 80 (HTTP), 443 (HTTPS), 22 (SSH), and 3389 (RDP) and one inbound rule that allows Internet Control Message Protocol version 4 (ICMPv4) access from all IP addresses to all ports. • Outbound: none. The following Access request control of basic security groups that have default rules shows how access is controlled by a basic security group that has default rules.	• Inbound: four inbound rules that allow TCP access from all IP addresses to ports 80 (HTTP), 443 (HTTPS), 22 (SSH), and 3389 (RDP) and one inbound rule that allows Internet Control Message Protocol version 4 (ICMPv4) access from all IP addresses to all ports. • Outbound: one outbound rule that allows access from all IP addresses to all ports corresponding to all protocols to prevent network connectivity issues. The following Access request control of advanced security groups that have default rules shows how access is controlled by an advanced security group that has default rules.

For information about the limits marked with ①, ②, and ③, see Security group limits.

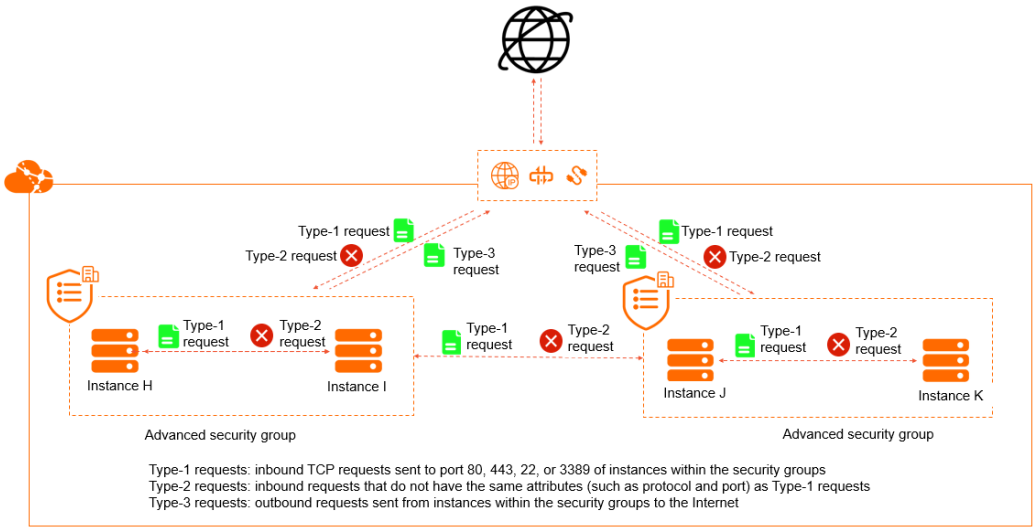
Access request control of security groups that have no rules



Access request control of basic security groups that have default rules



Access request control of advanced security groups that have default rules



If an instance is assigned to multiple security groups, the rules of all the security groups are applied to the instance. When an access request destined for the instance is detected, the request is matched against applied security group rules one by one based on the rule attributes such as protocol, port range, and priority. No sessions are established until an Allow rule matches the request. For more information about the attributes and examples of security group rules, see Overview.

Work with security groups

You can perform the following operations to use security groups to control traffic for instances:

1. Create security groups.
2. Add rules to the security groups.
3. Add instances to the security groups.
4. Manage existing security groups and security group rules based on your needs.

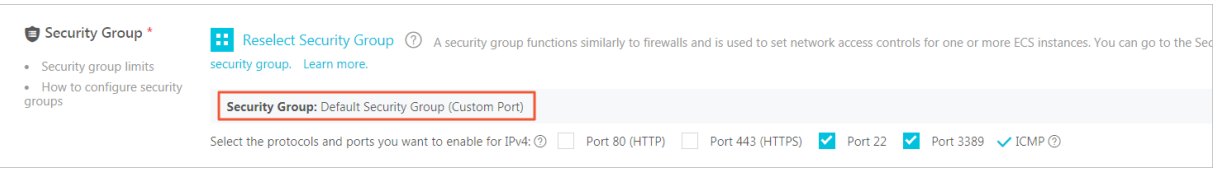
You can perform the following operations to use security groups to control traffic for secondary ENIs:

1. Create security groups.
2. Add rules to the security groups.
3. Add secondary ENIs to the security groups.
4. Bind the secondary ENIs to instances.
5. Manage existing security groups and security group rules based on your needs.

For information about how to perform operations on security groups and use cases of security groups, see Manage security groups and Security groups for different use casesConfiguration guide for ECS security groups.

Default security groups

Each instance must belong to one or more security groups. When you use the ECS console to create instances within a region in which you have not created security groups, you can use the default security group. The system creates a default security group when it creates the instances that you request. The network type of the security group is the same as that of the instances. The default security group is a basic security group that has default rules, as shown in the following figure.



Description of default rules:

- The rules have a priority of 100.

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

- The rules allow TCP access from all IP addresses to ports 22 (SSH) and 3389 (RDP).
- The rules allow ICMPv4 access from all IP addresses to all ports.
- If you select **Port 80 (HTTP)** and **Port 443 (HTTPS)**, rules are automatically added to allow TCP access from all IP addresses to ports 80 (HTTP) and 443 (HTTPS).

Managed security groups

Other Alibaba Cloud services such as Cloud Firewall and NAT Gateway also use security group capabilities. The Alibaba Cloud services create and use managed security groups to ensure service availability and prevent accidental operations on resources. Managed security groups are managed by the Alibaba Cloud services that create them. You can view managed security groups but cannot perform operations on them. For more information, see Managed security groups.

Practical suggestions

- Use a security group that has no rules as a whitelist to deny all inbound access. You can add rules to allow access to or from specific destinations or sources on specific ports.
- Follow the principle of least privilege when you add security group rules. For example, to allow connections to port 22 on a Linux instance, we recommend that you add a rule to allow access from only specific IP addresses instead of all IP addresses (`0.0.0.0/0`).
- Make sure that each security group has simple and clear rules. A single instance can be added to multiple security groups. A single security group can have multiple rules. If a large number of rules are

applied to an instance, management is complex and unforeseen risks can be introduced.

- Add instances that serve different purposes to different security groups and separately maintain the security group rules applied to the instances. For example, you can add instances that need the Internet access to a security group. Then, in the security group, add rules to deny all access and allow inbound access to only the ports used to provide external services, such as ports 80 and 443. Meanwhile, to ensure that the instances accessible from the Internet do not provide other services (such as MySQL and Redis), we recommend that you deploy internal services on the instances inaccessible from the Internet and then add these instances to another security group.
- Do not modify security groups that are in use within the production environment. All changes to a security group are automatically applied to the instances within the security group. Before you change the configurations of a security group, you can clone, change, and debug it within the test environment to ensure that the change does not interrupt the communication between the associated instances.
- Specify identifiable names and tags for security groups for easy search and management.

Properly use security groups and make combined use of security groups and other means as required to improve the security of instances. For more information, see Best practices for security.

2.2. Managed security groups

Managed security groups are security groups that are created in managed mode. These security groups are used to ensure the availability of cloud services and prevent unexpected operations on resources. When you use cloud services that require security groups, security groups are created in managed mode for the cloud services. This topic describes managed security groups and their related permissions.

Background information

A security group in managed mode is a managed security group. The managed mode is used to control the operation permissions on security groups for some cloud services such as Cloud Firewall and NAT Gateway. Managed security groups are managed by cloud service systems. You can view managed security groups but cannot perform operations on these security groups. The following descriptions are applicable to managed security groups.

> **Note** Alibaba Cloud services use Security Token Service (STS) to grant permissions to RAM roles of your account to create managed security groups. For more information, see What is STS?.

- In a cloud service console, you cannot perform operations on managed security groups but can view their information.
- When you use OpenAPI to access managed security groups, you can call only query operations. If you call an operation that is used to manage security groups for a managed security group, an error message that contains the `InvalidOperation.ResourceManagedByCloudProduct` error code is returned. The error message indicates that the security group is managed by a cloud service system and you cannot perform operations on this security group. For more information, see Permissions on API operations related to managed security groups.

You can call the DescribeSecurityGroups operation and view the `ServiceManaged` and `ServiceID` parameters in the response to check whether a security group is a managed security group.

Permissions on API operations related to managed security groups

API	API operation	Can be performed by your Alibaba Cloud account	Can be performed by the cloud service system for which the managed security group is created
AuthorizeSecurityGroup	• Adds an inbound rule to a security group. • Controls inbound access to a managed security group.	No	Yes
AuthorizeSecurityGroupEgress	• Adds an outbound rule to a security group. • Controls outbound access from a managed security group.	No	Yes
RevokeSecurityGroup	Deletes an inbound rule from a security group.	No	Yes
RevokeSecurityGroupEgress	Deletes an outbound rule from a security group.	No	Yes
JoinSecurityGroup	Adds a resource to a security group.	No	Yes
LeaveSecurityGroup	Removes a resource from a security group.	No	Yes
DeleteSecurityGroup	Deletes a security group.	No	Yes
ModifySecurityGroupAttribute	Modifies a security group.	No	Yes
ModifySecurityGroupRule	Modifies the description of an inbound security group rule.	No	Yes
ModifySecurityGroupEgressRule	Modifies the description of an outbound security group rule.	No	Yes
ModifySecurityGroupPolicy	Modifies a security group policy.	No	Yes
DescribeSecurityGroupAttribute	Queries security group rules.	Yes	Yes
DescribeSecurityGroups	Queries security groups.	Yes	Yes
DescribeSecurityGroupReferences	Queries whether a security group is referenced by other security groups.	Yes	Yes

API	API operation	Can be performed by your Alibaba Cloud account	Can be performed by the cloud service system for which the managed security group is created
CreateNetworkInterface	Creates an elastic network interface (ENI).	No	Yes
ModifyNetworkInterfaceAttribute	Modifies an ENI.	No	Yes
RunInstances	Creates one or more instances.	No	Yes
CreateInstance	Creates an instance.	No	Yes
ModifyInstanceAttribute	Modifies the security group to which an instance belongs.	No	Yes

2.3. Security groups for different use cases

This topic describes how to configure security group rules for common scenarios (such as scenarios where a website deployed on your instance needs to provide external web services or where you want to connect to your instance from an on-premises server) based on security group characteristics in Elastic Compute Service (ECS).

Background information

Take note of the following items about security group rules:

- In security groups of the Virtual Private Cloud (VPC) type, each rule controls access to or from both the Internet and the internal network. In security groups of the classic network type, public rules (Internet ingress and Internet egress rules) control access to or from the Internet, whereas internal rules (inbound and outbound rules) control access to or from the internal network.
- All example rules described in this topic are configured for the default ports used by typical applications. Applications deployed on instances use ports of the instances to provide external services. For more information, see Typical applications of commonly used ports.

Security group rules for websites to provide web services

Security groups that contain no rules deny all inbound access. If a website deployed on your instance needs to provide external web services, you must add the security group rules described in the following table to allow inbound access to the required ports such as ports 80 (HTTP) and 443 (HTTPS).

Direction	Action	Priority	Protocol type	Port range	Authorization object

Direction	Action	Priority	Protocol type	Port range	Authorization object
Inbound	Allow	1	Custom TCP	Destination: 80/80	Source: 0.0.0.0/0
Inbound	Allow	1	Custom TCP	Destination: 443/443	Source: 0.0.0.0/0

Note If the website still cannot be accessed after the preceding rules are added, troubleshoot the problem. For more information, see Check whether TCP port 80 is available.

Security group rules for connecting to an instance from an on-premises server

Security groups that contain no rules deny all inbound access. Before you can connect to an instance from an on-premises server, you must add security group rules to allow inbound access to the required ports based on your connection method. For example, to connect to a Linux instance by using Secure Shell (SSH), you must add a rule that allows inbound SSH access to port 22. To connect to a Windows instance by using the Remote Desktop Protocol (RDP), you must add a rule that allows inbound RDP access to port 3389. The following table describes the example rules.

Direction	Action	Priority	Protocol type	Port range	Authorization object
Inbound	Allow	1	Custom TCP	Destination: 22/22	Source: 0.0.0.0/0
Inbound	Allow	1	Custom TCP	Destination: 3389/3389	Source: 0.0.0.0/0

Note `0.0.0.0/0` indicates all IP addresses. For security purposes, we recommend that you specify specific IP addresses as authorization objects based on the principle of least privilege.

When you use Alibaba Cloud Workbench to connect to an instance, you must add security group rules to allow access to specified servers. The following table describes the example rules.

Direction	Action	Priority	Protocol type	Port range	Authorization object
Inbound	Allow	1	Custom TCP	Destination: 22/22	Source: 161.117.90.22/32
Inbound	Allow	1	Custom TCP	Destination: 3389/3389	Source: 161.117.90.22/32

> **Note** For more information about the security group rules used to allow Workbench access to instances in the classic network, see the "Add security group rules to allow Workbench access to a Linux instance" section in Connect to a Linux instance by using a password or key and the "Add security group rules to allow Workbench access to a Windows instance" section in Connect to a Windows instance by using a password or key.

Security group rules for instances within different security groups to communicate with each other

Instances within different security groups that contain no rules are isolated from each other over the internal network. If you want to share data between instances from different security groups within the same VPC (for example, if you want instances within Security Group A to access shared files on instances within Security Group B over FTP), you can add rules to allow mutual access between the security groups over the internal network. This is more convenient than adding rules to allow access to or from individual IP addresses or CIDR blocks.

> **Note** This method does not work for instances that reside within different VPCs. You can use Cloud Enterprise Network (CEN) to connect instances within a VPC to those within another VPC. For more information, see Overview.

If Security Group A and Security Group B belong to the same Alibaba Cloud account, you must specify the ID of Security Group A as the authorization object when you add a rule to Security Group B to allow inbound access from Security Group A. The following table describes an example rule.

Direction	Action	Priority	Protocol type	Port range	Authorization object
Inbound	Allow	1	Custom TCP	Destination: 21/21	Source: sg-bp1hv6wvmegs036****

> **Note** The security group ID provided in the preceding table is for reference only. Replace it with the actual security group ID.

If Security Group A and Security Group B do not belong to the same Alibaba Cloud account, you must specify the ID of Security Group A and the ID of its associated Alibaba Cloud account as the authorization object when you add a rule to Security Group B to allow inbound access from Security Group A. The following table describes an example rule.

Direction	Action	Priority	Protocol type	Port range	Authorization object
Inbound	Allow	1	Custom TCP	Destination: 21/21	Source: 160998252992****/sg-bp174yoe2ib1sqj5****

Note The Alibaba Cloud account ID and the security group ID provided in the preceding table are for reference only. Replace them with the actual IDs.

Security group rules for access to databases

If you have deployed databases on your instance and want other instances to obtain data from the databases over the internal network, you must add rules to allow inbound access to the required ports based on the database types, such as port 3306 (MySQL), port 1521 (Oracle), port 1433 (MS SQL), port 5432 (PostgreSQL), and port 6379 (Redis). The following table describes the example rules.

Direction	Action	Priority	Protocol type	Port range	Authorization object
Inbound	Allow	1	Custom TCP	Destination: 3306/3306	Source: 172.16.XX.XX. XX
Inbound	Allow	1	Custom TCP	Destination: 1521/1521	Source: 192.168.XX.XX
Inbound	Allow	1	Custom TCP	Destination: 1433/1433	Source: 192.168.XX.XX /16
Inbound	Allow	1	Custom TCP	Destination: 5432/5432	Source: sg-bp1hv6wvmeg s036****
Inbound	Allow	1	Custom TCP	Destination: 6379/6379	Source: 160998252992 ****/sg-bp174yoe2ib1 sqj5****

Note The IP addresses, CIDR block, Alibaba Cloud account ID, and security group IDs provided in the preceding table are for reference only. Replace them with actual information.

Security group rules for pinging instances

The Internet Control Message Protocol (ICMP) is used to transmit control messages. You must add rules to allow inbound ICMP access before you can perform specific test operations, such as running the ping command on a client to ping your instance. The following table describes the example rules.

Direction	Action	Priority	Protocol type	Port range	Authorization object
Inbound	Allow	1	All ICMP (IPv4)	Destination: -1/-1	Source: 0.0.0.0/0
Inbound	Allow	1	All ICMP (IPv6)	Destination: -1/-1	Source: ::/0

Security group rules for restricting access from instances to external websites

By default, basic security groups allow all outbound access. To allow instances within a basic security group access only to specific websites, you can use the security group as a whitelist and add a Forbid rule that denies all outbound access and then Allow rules that allow outbound access to the IP addresses of the websites. Take note of the following items:

- After multiple rules match the request based on their protocols, port ranges, and authorization objects, the request is further matched against the priorities and actions of these rules to determine a single rule to apply. No session is established until an Allow rule is matched and applied.
- A smaller value of the priority of the security group rule indicates a higher priority. If two security group rules have the same priority and are different only in the action, the Forbid rule takes effect. Therefore, the priority of the Forbid rule must be lower than that of the Allow rule. This way, the Allow rule takes effect to allow outbound access to the IP addresses of the specified websites.

The following table describes the example rules.

Direction	Action	Priority	Protocol type	Port range	Authorization object
Outbound	Forbid	2	All	Destination: -1/-1	Destination: 0.0.0.0/0
Outbound	Allow	1	Custom TCP	Destination: 80/80	Destination: 47.96.XX.XX
Outbound	Allow	1	Custom TCP	Destination: 443/443	Destination: 121.199.XX.XX

Note The IP addresses of the websites provided in the preceding table are for reference only. Replace them with the actual IP addresses of your websites.

After the rules are added, you can log on to your instance to perform tests, such as running the ping command. If your instance can access only the specified IP addresses, the security group rules have taken effect.

2.4. 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.

Port	Service	Description
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.
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.

Port	Service	Description
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 RDP	VPC	Configuration is not required.	Inbound	Allow	RDP (3389)	3389/3389	Address field access	0.0.0.0/0	1
	Classic network	Internet							
Ping ECS instances through the Internet	VPC	Configuration is not required.	Inbound	Allow	ICMP	-1/-1	Address field access or security group access	Set this parameter according to the authorization typ	1
	Classic network	Internet							

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

2.5. 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 a security group rule
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 instance to a security group • Replace the security groups of ECS instances
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.	Bind 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 a security group

Operation	Description	Reference
Manage security group rules	You can query, modify, restore, export, import, and delete security group rules.	• Query 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.
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.

Operation	Description
DescribeSecurityGroups	Queries security groups that you have created within the current region.

2.6. Create a security group

A security group acts as a virtual firewall that is used to control access to and from Elastic Compute Service (ECS) instances. Each instance must belong to at least one security group. This topic describes how to create a security group and configure security group rules in the ECS console.

Prerequisites

A virtual private cloud (VPC) and a vSwitch are already created if you want to create a security group of the VPC type. For more information, see 创建和管理专有网络.

Context

If you do not create a security group when you create an ECS instance, a default security group is created. The default security group contain the following default rules:

- An inbound rule that allows Internet Control Message Protocol (ICMP) traffic to support operations such as pinging the ECS instance.
- An inbound rule that allows traffic on SSH port 22 and Remote Desktop Protocol (RDP) port 3389 to access the ECS instance.
- An optional inbound rule that allows traffic on HTTP port 80 and HTTPS port 443. If you want to build websites by using the ECS instance, you must select HTTP port 80 and HTTPS port 443 to create the rule in the default security group.

If you want to add an ECS instance to a user-created security group, you can perform the following operations to create a security group. For more information, see Overview.

Procedure

1. Go to the Security Groups page.
   i.
   ii.
   iii.
2. Click **Create Security Group**.
3. In the **Basic Information** section, configure the parameters described in the following table.

Parameter	Description
Security Group Name	Specify a name for the security group.
Description	Enter a brief description of the security group for future management.

Parameter	Description
Network	Set the network type of the security group. ○ To create a security group of the VPC type, select an existing VPC. ○ To create a security group of the classic network type, select **Classic Network**.
Security Group Type	Select a security group type. ○ Basic Security Group: applicable to scenarios that involve small clusters and require moderate network connections. ○ Advanced Security Group: applicable to scenarios that involves large-scale clusters and require highly efficient O&M. For information about other functional differences between basic and advanced security groups, see Overview.
Resource group	Select a resource group to which to assign the security group to facilitate subsequent O&M.
Tags	Configure tags for the security group to facilitate subsequent O&M.

4. (Optional)In the **Access Rule** section, configure security group rules.

   The system adds default security group rules that have the basic configurations. To add user-created security group rules, perform the following operations. For more information, see Add a security group rule.

i. Click the **Inbound** or **Outbound** tab to select the security group rule direction.

Network type	Rule direction
VPC	■ Inbound: controls inbound traffic from both the Internet and internal networks. By default, inbound rules are added to allow ICMP traffic and traffic on SSH port 22, RDP port 3389, HTTP port 80, and HTTPS port 443. ■ Outbound: controls outbound traffic to both the Internet and internal networks. By default, basic security groups allow all outbound access, and advanced security groups deny all outbound access.
Classic network	■ Internet Ingress: For security reasons, we recommend that you select a security group for Authorization Object when you add a public inbound rule to a security group of the classic network type. If you want to control access from IP addresses, enter individual IP addresses instead of CIDR blocks. ■ Internet Egress: By default, all outbound access to the Internet is allowed. ■ Inbound: By default, the internal inbound rules are added to allow ICMP traffic and traffic on SSH port 22, RDP port 3389, HTTP port 80, and HTTPS port 443. ■ Outbound: By default, all inbound access from the internal network is allowed

ii. Click **Add Rule**.

iii. Add user-created security group rules.

Parameter	Description
Action	■ **Allow**: allows access requests on a specific port. ■ **Forbid** :denies access requests and drops data packets without returning a response. If two security group rules differ only in their actions, the **Forbid** rule is used but the **Allow** rule is ignored.
Priority	A smaller value indicates a higher priority. Valid values: 1 to 100.

Parameter	Description
Protocol Type	The protocol type of the security group rule. Valid values: ■ **All** ■ **Custom TCP** ■ **Customized UDP** ■ **All ICMP (IPv4)** ■ **All ICMP (IPv6)** ■ **All GRE**
Port Range	You can specify a port range when **Protocol Type** is set to **Custom TCP** or **Customized UDP**. Enter one or more port ranges. Separate the port ranges with commas (,). Example: `22/23,443/443`. For more information about the **Protocol Type** and **Port Range** parameters, see Typical applications of commonly used ports and What is the relationship between protocol types and port ranges in security group rules?.
	You can specify an authorization object of the following types: ■ IP Address You can enter individual IP addresses. Example: 192.168.0.100 or 2408:4321:180:1701:94c7:bc38:3bfa:. ■ CIDR blocks You can enter a CIDR block. Example: 192.168.0.0/24 or 2408:4321:180:1701:94c7:bc38:3bfa:***/128. For more information about IP addresses and CIDR blocks, see the "What is the relationship between the IP addresses and CIDR blocks specified as authorization objects of a security group rule?" issue in What is the relationship between the IP addresses and CIDR blocks specified as authorization objects of a security group rule?.

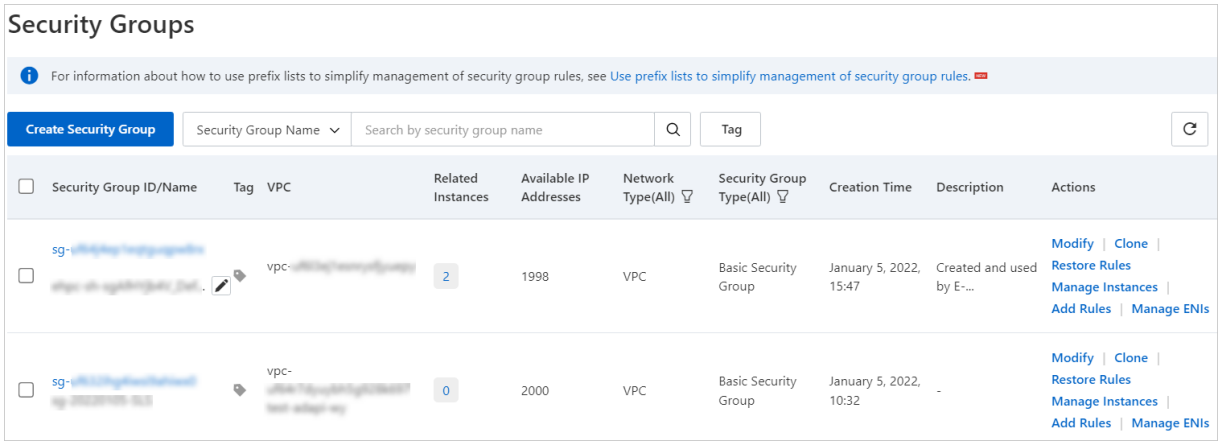
Parameter	Description
Authorization Object	■ Security groups This authorization type is valid only for the internal network. You can specify a security group in the current account or a different account as the authorization object to allow mutual access between instances or elastic network interfaces (ENIs) in that security group and instances in the current security group over the internal network. **Note** ■ For advanced security groups, security groups are not supported as authorization objects. ■ For each basic security group, a maximum of 20 security groups are supported as authorization objects. ■ Authorize the current account: Enter the ID of the security group that you want to specify as the authorization object within the current account. If the current security group is of the VPC type, the security group that you want to specify as the authorization object must reside within the same VPC as the current security group. ■ Authorize another account: Enter the ID of the different Alibaba Cloud account and the ID of the security group to which you want to grant permissions in the `ID of the Alibaba Cloud account/ID of the security group` format. You can choose **Account Management > Basic Information** to view your account ID. ■ Prefix lists A prefix list is a set of network prefixes (CIDR blocks). The prefix list feature is supported only on security groups of the VPC type. After you reference a prefix list in a security group rule, the rule applies to all CIDR blocks in the prefix list. For more information, see Overview and Create a prefix list. If a prefix list is referenced in a security group rule, the maximum number of entries in the prefix list counts against the rule quota for the security group. For example, assume that a prefix list can contain a maximum of 100 entries. If the prefix list is referenced in a security group rule, the prefix list counts as 100 rules for the security group regardless of the number of existing entries in the prefix list. Take note of the following items: ■ You can enter up to 10 authorization objects at a time. Separate the objects with commas (,). Each authorization object corresponds to a rule. For example, if you add 10 authorization objects at a time, 10 rules are generated. ■ If you enter `0.0.0.0/0` or `::/0` as an authorization object, all IP addresses are allowed. Evaluate the network risks before you specify 0.0.0.0/0 or ::/0. ■ For security reasons, we recommend that you select a security group for Authorization Object when you add a public inbound rule to a security group of the classic network type. If you want to specify IP addresses as authorization objects in security group rules, enter individual IP addresses instead of CIDR blocks.

Parameter	Description
Description	The description of the security group rule.

5. Click **Create Security Group**.

Result

After the security group is created, the security group is displayed on the Security Groups page.



What's next

- You can configure security group rules to allow or deny access to or from the Internet or internal network for ECS instances within a security group. For more information, see Add a security group rule.
- Each 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 instance to a security group.
- For information about why services on instances cannot be accessed after a security group is configured, see the "Why am I unable to access services after I configure a security group?" issue in Why am I unable to access services after I configure a security group?

Related information

- CreateSecurityGroup

2.7. Add a security group rule

This topic describes how to add security group rules. You can configure security group rules to allow or deny access to or from the Internet or internal network for Elastic Compute Service (ECS) instances within a security group.

Prerequisites

The public or internal IP addresses for which you want to control access for your instances are obtained. For information about the scenarios of adding security group rules, see Security groups for different use casesConfiguration guide for ECS security groups.

Context

Security groups control access to or from the Internet or internal network. For security purposes, most security groups use deny rules (Forbid rules) for inbound traffic. If you use the default security group, the system adds security group rules for some communication ports.

This topic is suitable for the following scenarios:

- When an application deployed on your instance initiates a request to communicate with a network outside of the security groups to which the instance belongs but the request remains in the waiting state, you must add a security group rule to allow this request.
- When attacks on running applications are detected from some of the request sources, you can add security group rules to block the malicious requests.

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

- If no rules are added to a basic security group, all inbound traffic to the security group is denied and all outbound traffic from the security group is allowed.
- If no rules are added to an advanced security group, all inbound and outbound traffic of the security group is denied. For advanced security groups, you cannot specify security groups as the authorization objects of security group rules.
- Both IPv4 and IPv6 addresses can be used as the authorization objects of security group rules.
- The total number of inbound and outbound rules within each security group cannot exceed 200.
- For a basic security group, if you specify security groups as the authorization objects of security group rules, a maximum of 20 security group rules can be specified in the basic security group.

For more information, see Overview.

Procedure

1. Go to the Security Groups page.
   i.
   ii.
   iii.
2. Find the security group to which you want to add a rule and click **Add Rules** in the **Actions** column.
3. On the **Security Group Rules** page, choose a rule direction in the **Access Rule** section based on the network type of the security group.

Network type	Rule direction
Virtual Private Cloud (VPC)	○ Inbound: The rule controls inbound traffic from both the Internet and internal network. ○ Outbound: The rule controls outbound traffic to both the Internet and internal network.
Classic network	○ Internet ingress: The rule controls inbound traffic from the Internet. ○ Internet egress: The rule controls outbound traffic to the Internet. ○ Inbound: The rule controls inbound traffic from the internal network. ○ Outbound: The rule controls outbound traffic to the internal network.

4. On the Security Group Rules page, add a security group rule.

- Method 1: Quickly add a security group rule

  This method is ideal for configuring commonly used TCP rules. Click **Quick Add**. In the Quick Add dialog box, set **Action** and **Authorization Object** and select one or more ports.

- Method 2: Manually add a security group rule

  You can specify the Action, Priority, and Protocol Type parameters. Perform the following steps to manually add a security group rule:

  i. Click **Add Rule**.

  ii. Configure the new security group rule by specifying the parameters described in the following table.

Parameter	Description
Action	■ **Allow**: allows access requests on a specific port. ■ **Forbid** :denies access requests and drops data packets without returning a response. If two security group rules differ only in their actions, the **Forbid** rule is used but the **Allow** rule is ignored.
Priority	A smaller value indicates a higher priority. Valid values: 1 to 100.
Protocol Type	The protocol type of the security group rule. Valid values: ■ **All** ■ **Custom TCP** ■ **Customized UDP** ■ **All ICMP (IPv4)** ■ **All ICMP (IPv6)** ■ **All GRE**
Port Range	You can specify a port range when **Protocol Type** is set to **Custom TCP** or **Customized UDP**. Enter one or more port ranges. Separate the port ranges with commas (,). Example: `22/23,443/443`. For more information about the **Protocol Type** and **Port Range** parameters, see Typical applications of commonly used ports and What is the relationship between protocol types and port ranges in security group rules?.
	You can specify an authorization object of the following types: ■ IP Address You can enter individual IP addresses. Example: 192.168.0.100 or 2408:4321:180:1701:94c7:bc38:3bfa:.

Parameter	Description
Authorization Object	■ CIDR blocks You can enter a CIDR block. Example: 192.168.0.0/24 or 2408:4321:180:1701:94c7:bc38:3bfa:***/128. For more information about IP addresses and CIDR blocks, see the "What is the relationship between the IP addresses and CIDR blocks specified as authorization objects of a security group rule?" issue in What is the relationship between the IP addresses and CIDR blocks specified as authorization objects of a security group rule?. ■ Security groups This authorization type is valid only for the internal network. You can specify a security group in the current account or a different account as the authorization object to allow mutual access between instances or elastic network interfaces (ENIs) in that security group and instances in the current security group over the internal network. **Note** ■ For advanced security groups, security groups are not supported as authorization objects. ■ For each basic security group, a maximum of 20 security groups are supported as authorization objects. ■ Authorize the current account: Enter the ID of the security group that you want to specify as the authorization object within the current account. If the current security group is of the VPC type, the security group that you want to specify as the authorization object must reside within the same VPC as the current security group. ■ Authorize another account: Enter the ID of the different Alibaba Cloud account and the ID of the security group to which you want to grant permissions in the `ID of the Alibaba Cloud account/ID of the security group` format. You can choose **Account Management > Basic Information** to view your account ID. ■ Prefix lists A prefix list is a set of network prefixes (CIDR blocks). The prefix list feature is supported only on security groups of the VPC type. After you reference a prefix list in a security group rule, the rule applies to all CIDR blocks in the prefix list. For more information, see Overview and Create a prefix list. If a prefix list is referenced in a security group rule, the maximum number of entries in the prefix list counts against the rule quota for the security group. For example, assume that a prefix list can contain a maximum of 100 entries. If the prefix list is referenced in a security group rule, the prefix list counts as 100 rules for the security group regardless of the number of existing entries in the prefix list. Take note of the following items: ■ You can enter up to 10 authorization objects at a time. Separate the objects with commas (,). Each authorization object corresponds to a rule. For example, if you add 10 authorization objects at a time, 10 rules are generated.

Parameter	Description
	■ If you enter `0.0.0.0/0` or `::/0` as an authorization object, all IP addresses are allowed. Evaluate the network risks before you specify 0.0.0.0/0 or ::/0. ■ For security reasons, we recommend that you select a security group for Authorization Object when you add a public inbound rule to a security group of the classic network type. If you want to specify IP addresses as authorization objects in security group rules, enter individual IP addresses instead of CIDR blocks.
Description	The description of the security group rule.

Parameter	Description
Action	■ **Allow**: allows access requests on a specific port. ■ **Forbid** :denies access requests and drops data packets without returning a response. If two security group rules differ only in their actions, the **Forbid** rule is used but the **Allow** rule is ignored.
Priority	A smaller value indicates a higher priority. Valid values: 1 to 100.
Protocol Type	The protocol type of the security group rule. Valid values: ■ **All** ■ **Custom TCP** ■ **Customized UDP** ■ **All ICMP (IPv4)** ■ **All ICMP (IPv6)** ■ **All GRE**
Port Range	You can specify a port range when **Protocol Type** is set to **Custom TCP** or **Customized UDP**. Enter one or more port ranges. Separate the port ranges with commas (,). Example: `22/23,443/443`. For more information about the **Protocol Type** and **Port Range** parameters, see Typical applications of commonly used ports and What is the relationship between protocol types and port ranges in security group rules?.
	You can specify an authorization object of the following types: ■ IP Address You can enter individual IP addresses. Example: 192.168.0.100 or 2408:4321:180:1701:94c7:bc38:3bfa:. ■ CIDR blocks You can enter a CIDR block. Example: 192.168.0.0/24 or 2408:4321:180:1701:94c7:bc38:3bfa:***/128. For more information about IP addresses and CIDR blocks, see the "What is the relationship between the IP addresses and CIDR blocks specified as authorization objects of a security group rule?" issue in What is the relationship between the IP addresses and CIDR blocks specified as authorization objects of a security group rule?.

Parameter	Description
Authorization Object	■ Security groups This authorization type is valid only for the internal network. You can specify a security group in the current account or a different account as the authorization object to allow mutual access between instances or elastic network interfaces (ENIs) in that security group and instances in the current security group over the internal network. **Note** ■ For advanced security groups, security groups are not supported as authorization objects. ■ For each basic security group, a maximum of 20 security groups are supported as authorization objects. ■ Authorize the current account: Enter the ID of the security group that you want to specify as the authorization object within the current account. If the current security group is of the VPC type, the security group that you want to specify as the authorization object must reside within the same VPC as the current security group. ■ Authorize another account: Enter the ID of the different Alibaba Cloud account and the ID of the security group to which you want to grant permissions in the `ID of the Alibaba Cloud account/ID of the security group` format. You can choose **Account Management > Basic Information** to view your account ID. ■ Prefix lists A prefix list is a set of network prefixes (CIDR blocks). The prefix list feature is supported only on security groups of the VPC type. After you reference a prefix list in a security group rule, the rule applies to all CIDR blocks in the prefix list. For more information, see Overview and Create a prefix list. If a prefix list is referenced in a security group rule, the maximum number of entries in the prefix list counts against the rule quota for the security group. For example, assume that a prefix list can contain a maximum of 100 entries. If the prefix list is referenced in a security group rule, the prefix list counts as 100 rules for the security group regardless of the number of existing entries in the prefix list. Take note of the following items: ■ You can enter up to 10 authorization objects at a time. Separate the objects with commas (,). Each authorization object corresponds to a rule. For example, if you add 10 authorization objects at a time, 10 rules are generated. ■ If you enter `0.0.0.0/0` or `::/0` as an authorization object, all IP addresses are allowed. Evaluate the network risks before you specify 0.0.0.0/0 or ::/0. ■ For security reasons, we recommend that you select a security group for Authorization Object when you add a public inbound rule to a security group of the classic network type. If you want to specify IP addresses as authorization objects in security group rules, enter individual IP addresses instead of CIDR blocks.

Parameter	Description
Description	The description of the security group rule.

iii. Click **Save** in the **Actions** column.

Result

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

FAQ

- For information about the **Protocol Type** and **Port Range** parameters, see Typical applications of commonly used ports and What is the relationship between protocol types and port ranges in security group rules?
- For information about why services on instances cannot be accessed after the instances are added to security groups, see Why am I unable to access services after I configure a security group?
- For information about why TCP port 80 and 25 cannot be accessed, see Why am I unable to access TCP port 80? and Why am I unable to access TCP port 25?
- For more information about security group rules, see Security FAQ.

Related information

- AuthorizeSecurityGroup
- AuthorizeSecurityGroupEgress

2.8. Add an ECS instance to a security group

Security groups are an important means for security isolation. Security groups are used to control access to and from Elastic Compute Service (ECS) instances. You can add an ECS instance to one or more security groups based on your business needs. Each ECS instance must belong to at least one security group. By default, each instance can belong to up to five security groups.

Prerequisites

Before you add an ECS instance to a security group, make sure that the following requirements are met:

- An instance is created. For more information, see Create an instance by using the wizard.
- The ECS instance and the security group to which you want to add the instance are of the same network type. If the network type is Virtual Private Cloud (VPC), the security group and the ECS instance must reside in the same VPC.
- If the ECS instance already belongs to a security group, this new security group must be of the same type as the security group to which the ECS instance already belongs. For more information, see

Overview.

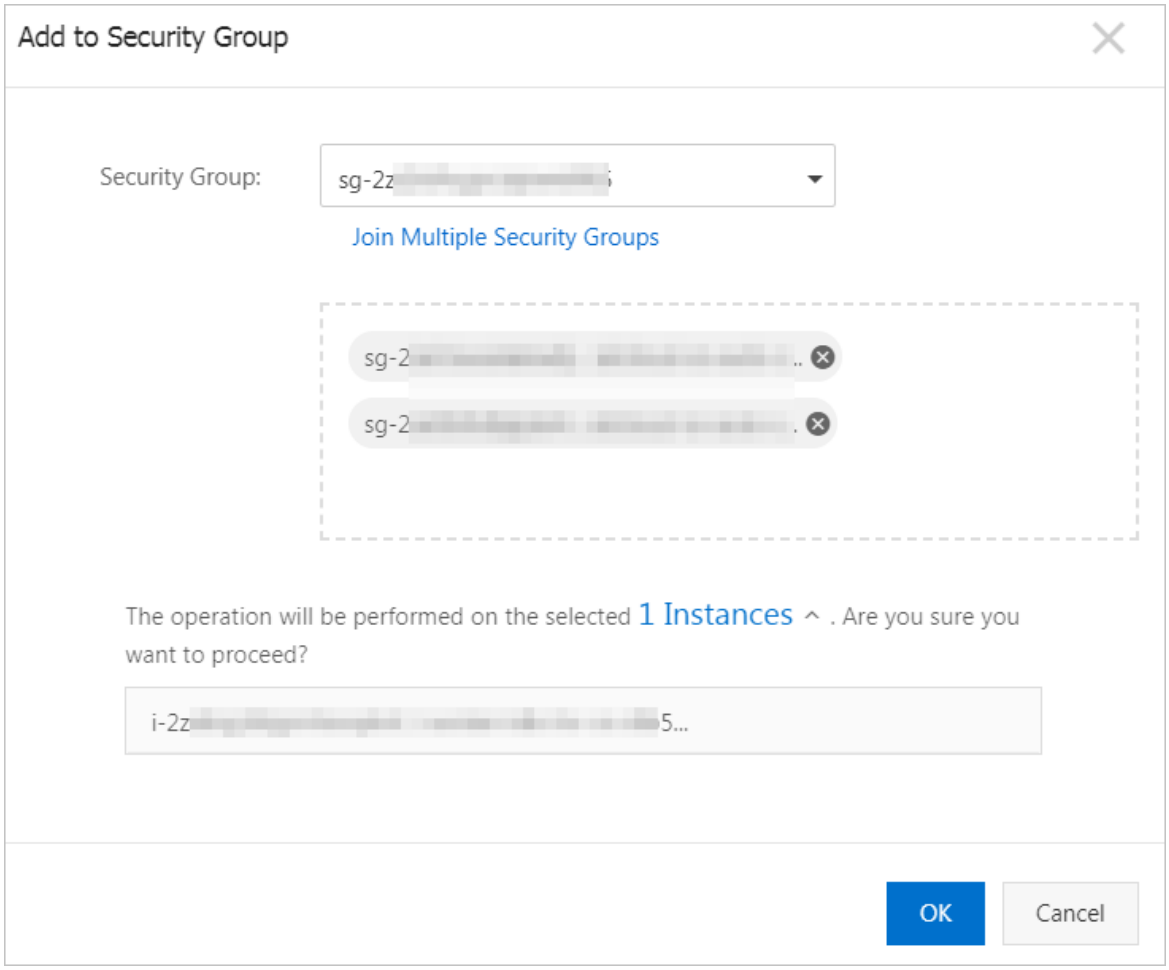
Add an instance to one or more security groups

Perform the following steps to add an instance to one or more security groups on the Instances page.

1.
2.
3.
4. On the **Instances** page, find the ECS instance that you want to add to security groups. You can use one of the following methods to add the instance to security groups:
   - Add the instance to security groups on the **Security Groups** tab of the Instance Details page.
     a. On the Instances page, click **Manage** in the **Actions** column.
     b. On the **Instance Details** page, click the **Security Groups** tab.
     c. Click **Add to Security Group**.
   - Add the instance to security groups on the Instances page.

     Choose **More > Network and Security Group > Add to Security Group** in the Actions column.
5. In the **Add to Security Group** dialog box, select a security group from the Security Group drop-down list.

   To add the ECS instance to multiple security groups, select a security group and click **Join Multiple Security Groups**. The selected security group is automatically added to the selection box that appears. Repeat this operation to add more security groups to the selection box.



6. Click **OK**.

   After the ECS instance is added to the selected security groups, the security groups rules in the security groups automatically apply to the instance.

Add one or more instances to the same security group

Perform the following steps to add one or more instances to the same security group on the Security Groups page.

1.
2.
3.
4. Find the security group to which you want to add instances and click **Manage Instances** in the **Actions** column.
5. In the upper-right corner of the **Instances in Security Group** page, click **Add Instance**.
6. In the **Add Instance** dialog box, select an instance ID and click **OK**.

   To add multiple ECS instances to the security group, click **Add Instance** to add more ECS instances.

   After the ECS instances are added to the security group, the security group rules in the security group automatically apply to these ECS instances.

What to do next

- You can view all security groups that you create within a region. For more information, see Query security groups.
- You can remove an instance from one or more security groups. After an ECS instance is removed from a security group, the instance is isolated from the other ECS instances in the security group. To ensure that services can run properly after an ECS instance is removed, we recommend that you perform sufficient tests before you remove the ECS instance. For more information, see Remove an instance from a security group.
- You can delete one or more security groups that are no longer needed. When a security group is deleted, its rules are also deleted. For more information, see Delete a security group.

Related information

- ModifyInstanceAttribute
- ModifyNetworkInterfaceAttribute

2.9. Replace the security groups of ECS instances

You can replace the security groups of Elastic Compute Service (ECS) instances as your business needs change. This topic describes how to replace the original security groups of instances with the destination security groups.

Prerequisites

- The instances and the destination security groups belong to the same virtual private cloud (VPC).
- If you want to replace the security groups of multiple instances at a time, the instances reside within the same VPC.

Context

You can replace the security groups of instances in the following scenarios:

- The original basic security groups of the instances need to be replaced with other basic security groups or advanced security groups.
- The original advanced security groups of the instances need to be replaced with other advanced security groups or basic security groups.

> **Notice**
>
> - Security groups can affect the network connectivity of instances. Before you replace the security groups of instances, make sure that the destination security groups suit your network connectivity requirements and do not affect service availability.
> - An ECS instance cannot belong to both basic and advanced security groups at the same time.

Procedure

1.
2.
3.

4. On the **Instances** page, use one of the following methods to replace the security groups of one or more instances:
   - Replace the security groups of a specific instance on the **Security Groups** tab of the Instance Details page.
     a. Find the instance whose security groups you want to replace and click **Manage** in the **Actions** column.
     b. On the **Instance Details** page, click the **Security Groups** tab.
     c. Click **Replace**.
   - Replace the security groups of one or more instances on the Instances page.
     - Replace the security groups of a single instance

       Find the instance whose security groups you want to replace and choose **More > Network and Security Group > Replace** in the **Actions** column.
     - Replace the security groups of multiple instances

       Select the instances whose security groups you want to replace 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 security groups to replace the original security groups.
   i. In the **Security Group Type** section, select **Basic Security Group** or **Advanced Security Group**.
   ii. In the **Select Security Groups** section, select a security group from the drop-down list.

   > **Note**
   > - If you want to select more security groups, click **Add**. By default, an ECS instance can be added to a maximum of five security groups.
   > - If you select some security groups that do not match your expectations, click **Delete** in the **Actions** column corresponding to the security groups. After the security groups are deleted, you can select security groups that you expect.
6. Click **Replace Security Group**.

Result

After you perform the preceding operations, the original security groups of the instances are replaced with the destination security groups. The destination security group rules automatically take effect on the instances. For more information about security groups, see Overview.

Related information

- ModifyInstanceAttribute

2.10. Manage security groups

2.10.1. Query security groups

This topic describes how to query security groups within a region in different methods and view the details of the security groups.

Procedure

1.
2.
3.
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 the icon.
   - Select **Security Group ID** from the drop-down list, enter a security group ID in the search bar, and then click the icon.
   - Select **VPC ID** from the drop-down list, enter the ID of a virtual private cloud (VPC) in the search bar, and then click the icon.

2.10.2. Modify a security group

This topic describes how to modify the attributes of a security group. These attributes include the name, description, and internal access control policy of the security group.

Prerequisites

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

Modifies the name and description of a security group

1.
2.
3.
4. On the **Security Groups** page, find the security group that you want to modify and click **Modify** in the **Actions** column.
5. In the Modify Security Group dialog box, modify **Security Group Name** and **Description**.
6. Click **OK**.

Modify the Internal access control policy of a security group

By default, Elastic Compute Service (ECS) instances within the same basic security group can communicate with each other over all protocols and ports. You can modify the Internal access control policy of the security group.

> **Note** The internal access control policies of advanced security groups and managed security groups cannot be modified.

1.
2.
3.
4. On the **Security Groups** page, find the security group whose internal access control policy you

want to modify and click the security group ID.

5. In the **Basic Information** section, set **Internal Access Control Policy** as needed.
   - If **Internal Access Control Policy** is set to **Allow**, all instances within the security group can communicate with each other over the internal network by default. To isolate instances within this security group from each other, you can click **Set to Deny** to change the Internal Access Control Policy value to Deny. When Internal Access Control Policy is set to Deny and no other security group rules are added to the security group, all instances within this security group are isolated from each other over the internal network by default.
   - If **Internal Access Control Policy** is set to **Deny**, all instances within the security group cannot communicate with each other over the internal network by default. To allow mutual access between instances within this security group over the internal network, you can click **Set to Allow** change the Internal Access Control Policy value to Allow. When Internal Access Control Policy is set to Allow, instances within the security group can communicate with each other over the internal network by default regardless of custom security group rules.
6. In the Modify Internal Access Control Policy message, click **OK**.

Related information

- ModifySecurityGroupAttribute

2.10.3. Clone a security group

This topic describes how to create identical security groups by means of cloning. Security groups can be cloned across regions and network types.

Prerequisites

If you want to clone a security group from the classic network to a virtual private cloud (VPC), at least one VPC is created in the destination region. For more information, see 创建和管理专有网络.

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 the need to create a new security group.
- You have created a security group named SG2 in the classic network and you want to apply the same rules as those of SG2 to instances in a VPC. You can clone SG2 and select VPC as the network type for the clone security group in the Clone dialog box.
- 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 for backup.

Procedure

1.
2.
3.
4. On the **Security Groups** page, find the security group that you want to clone 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. Only specific regions are supported, which are displayed in the console.
- **Security Group Name**: Specify a name for the clone security group.
- **Network Type**: Select a network type for the clone security group. If you set Network Type to VPC, select an usable VPC in the destination region.
- **Import All Rules**: Specify whether to import all rules whose priorities are higher than 100 from the original security group to the clone security group.
  - If you do not select **Import All Rules**, only the rules whose priorities are 1 to 100 are imported to the clone security group.
  - If you select **Import All Rules**, all rules whose priorities are 1 to 100 and higher than 100 are imported to the clone security group. After the rules are imported to the clone security group, rules whose priorities are greater than 100 have their priorities changed to 100.

6. Click **OK**.

Result

After the security group is cloned, the **Clone** dialog box closes. You can view the clone security group on the **Security Groups** page of the destination region.

2.10.4. 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 the 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 instance is added to two or more security groups.

Context

You can use one of the following methods to remove instances from a security group:

- For information about how to remove a single instance from a security group, see Remove a single instance.
- For information about how to remove multiple instances from a security group, see Remove multiple instances.

Remove a single instance

1.
2.
3.
4. On the **Instances** page, find the instance to be removed from a security group, and click **Manage** in the **Actions** column.
5. The **Instance Details** tab appears. Click the **Security Groups** tab.
6. Find the security group from which you want to remove the instance, and click **Remove** in the **Actions** column.

7. Click **OK**.

Remove multiple instances

1.
2.
3.
4. On the **Security Groups** page, find the security group from which you want to remove instances, and click the security group ID.
5. In the left-side navigation pane, click **Instances in Security Group**.
6. Select one or more instances, and click **Remove from Security Group**.
7. Click **OK**.

Related information

- ModifyInstanceAttribute
- ModifyNetworkInterfaceAttribute

2.10.5. Edit the tags of a security group

Tags can be used to identify resources with the same characteristics (such as security groups that belong to the same organization or that serve the same purpose) for easy search and management. This topic describes how to edit the tags of an existing security group.

Context

For information about how to use tags, the resources that support tags, and the limits on tags, see Overview and the "Tag limits" section of the Limits topic.

Procedure

1.
2.
3.
4. Find the security group whose tags you want to edit, move the pointer over the  icon in the **Tag** column, and then click **Edit Tags**.
5. In the **Edit Tags** dialog box, click Available Tags to select existing tags or click Create to create tags. Then, click **OK**.

What's next

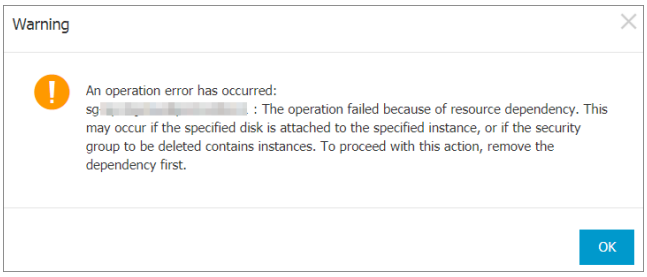
After tags are added to your security groups, you can filter the security groups by tag to perform different operations. For example, you can add Elastic Compute Service (ECS) instances to security groups that have a set of tags and add rules to security groups that have a different set of tags.

2.10.6. Delete a security group

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

Prerequisites

- The security group that you want to delete does not contain Elastic Compute Service (ECS) instances. If the security group that you want to delete contains 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 is not referenced by rules of other security groups. If the security group is referenced by rules of other security groups, you must delete those rules as prompted. For more information, see Delete a security group rule.



Procedure

1.
2.
3.
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, confirm the information and click **OK**.

Related information

- DeleteSecurityGroup

2.11. Manage security group rules

2.11.1. Overview

The rules of a security group control the inbound or outbound traffic to or from the instances in the security group.

Attributes of security group rules

To add or modify a security group rule, you must configure the attributes described in the following table.

Attribute	Description

Attribute	Description
Direction	The direction of the rule. The network types of security groups affect rule directions. • In a security group of the Virtual Private Cloud (VPC) type, rules are classified as inbound or outbound and each rule controls access to or from both the Internet and internal network. • In a security group of the classic network type, rules are classified as public inbound (Internet ingress), public outbound (Internet egress), internal inbound (inbound), or internal outbound (outbound). Public inbound and outbound rules control access to and from the Internet. Internal inbound and outbound rules control access to and from the internal network. Access requests are matched against inbound and outbound rules based on different attributes. • Inbound access requests are matched against inbound rules based on their transport layer protocols, destination port numbers, and source IP addresses. An inbound rule matches an inbound access request when they have the same transport layer protocol, destination port number, and source IP address. • Outbound access requests are matched against outbound rules based on their transport layer protocols, destination port numbers, and destination IP addresses. An outbound rule matches an outbound access request when they have the same transport layer protocol, destination port number, and destination IP address. **Note** By default, security group rules are created in the Elastic Compute Service (ECS) console based on 3-tuples. To implement finer-grained access control, you can call API operations to create rules to allow or deny access based on 5-tuples: source IP address, source port number, destination IP address, destination port number, and transport layer protocol. For more information, see Security group quintuple rules.
Action	The action of the rule. You can set the action to Allow or Forbid. If two security group rules are different only in the action, the Forbid rule takes effect.
Priority	The priority of the rule. The priority ranges from 1 to 100. A smaller value indicates a higher priority.
Protocol type	The transport layer protocol. TCP, User Datagram Protocol (UDP), Internet Control Messages Protocol version 4 (ICMPv4), ICMP version 6 (ICMPv6), and Generic Routing Encapsulation (GRE) are supported.
Port range	The range of destination ports for inbound or outbound traffic. You can specify single port numbers or a range of port numbers. For information about the default ports used by typical applications, see Typical applications of commonly used ports.

Attribute	Description
Authorization object	The source for inbound traffic or the destination for outbound traffic. You can specify the following items as authorization objects: • Single IP addresses. Example: `192.168.0.100` or `2408:4321:180:1701:94c7:bc38:3bfa:` . • Classless Inter-domain Routing (CIDR) blocks. Example: `192.168.0.0/24` or `2408:4321:180:1701:94c7:bc38:3bfa:***/128` . • Other security groups. A rule that includes another security group as the authorization object controls mutual access between the instances in that security group and the instances in the current security group over the internal network. When you configure a rule in a security group, you can specify a different security group within the same or another Alibaba Cloud account as the authorization object. **Note** Security groups can be specified as authorization objects only in rules of basic security groups. • Prefix lists. A prefix list is a set of one or more CIDR blocks. If a prefix list is specified as the authorization object in a security group rule, the rule is applied to all CIDR blocks included in the prefix list. Example: `192.168.0.0/24,172.16.0.0/16` .

Procedure to filter access requests based on security group rules

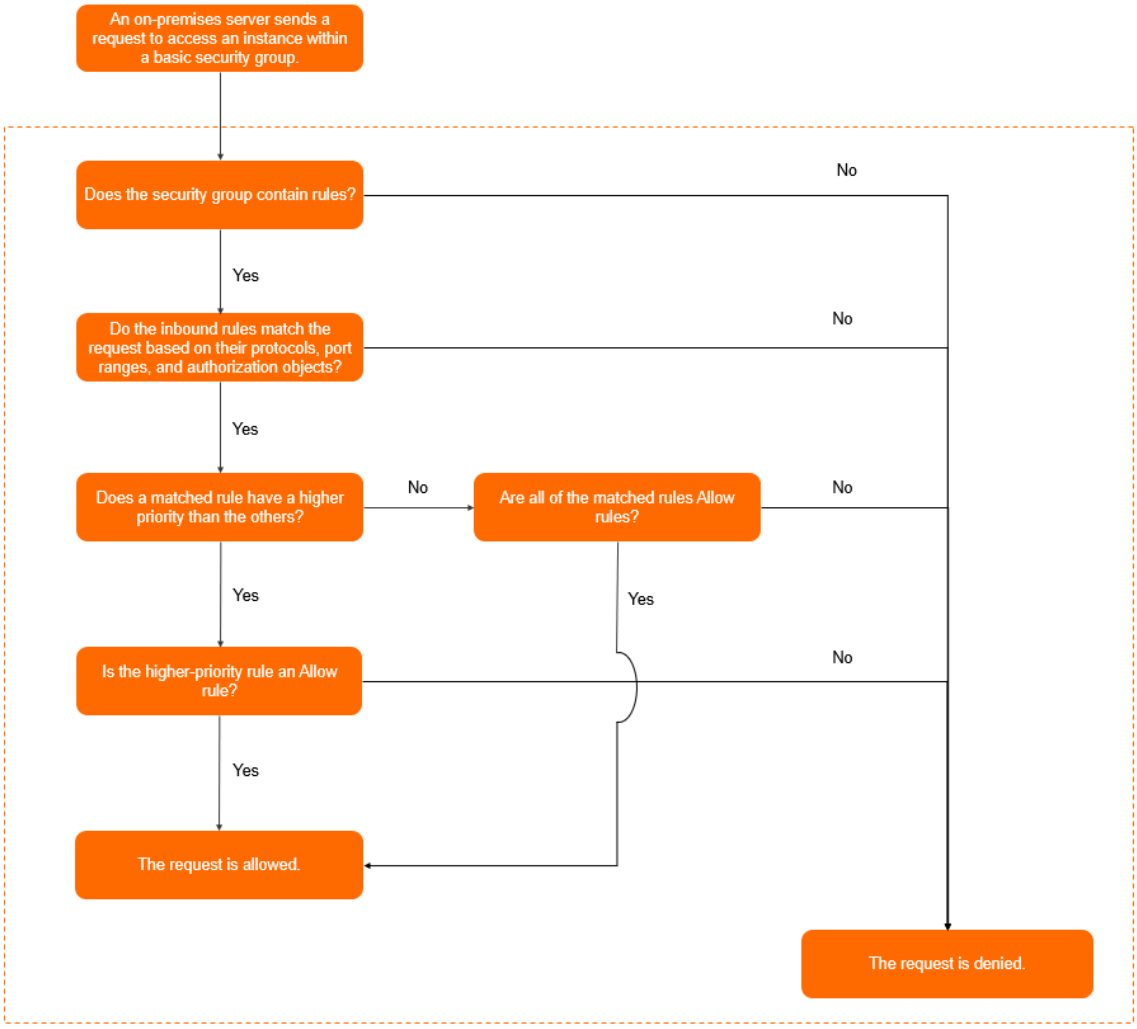
If an instance is assigned to multiple security groups, the rules of all the security groups are applied to the instance. When an access request destined for the instance is detected, the request is matched against each rule one by one. If multiple rules match the request based on their protocols, port ranges, and authorization objects, the request is further matched against the priorities and actions of these rules to determine a single rule to apply. No session is established until an Allow rule is matched and applied.

You can add or modify rules of a security group. The new or modified rules are automatically applied to the instances in the security group.

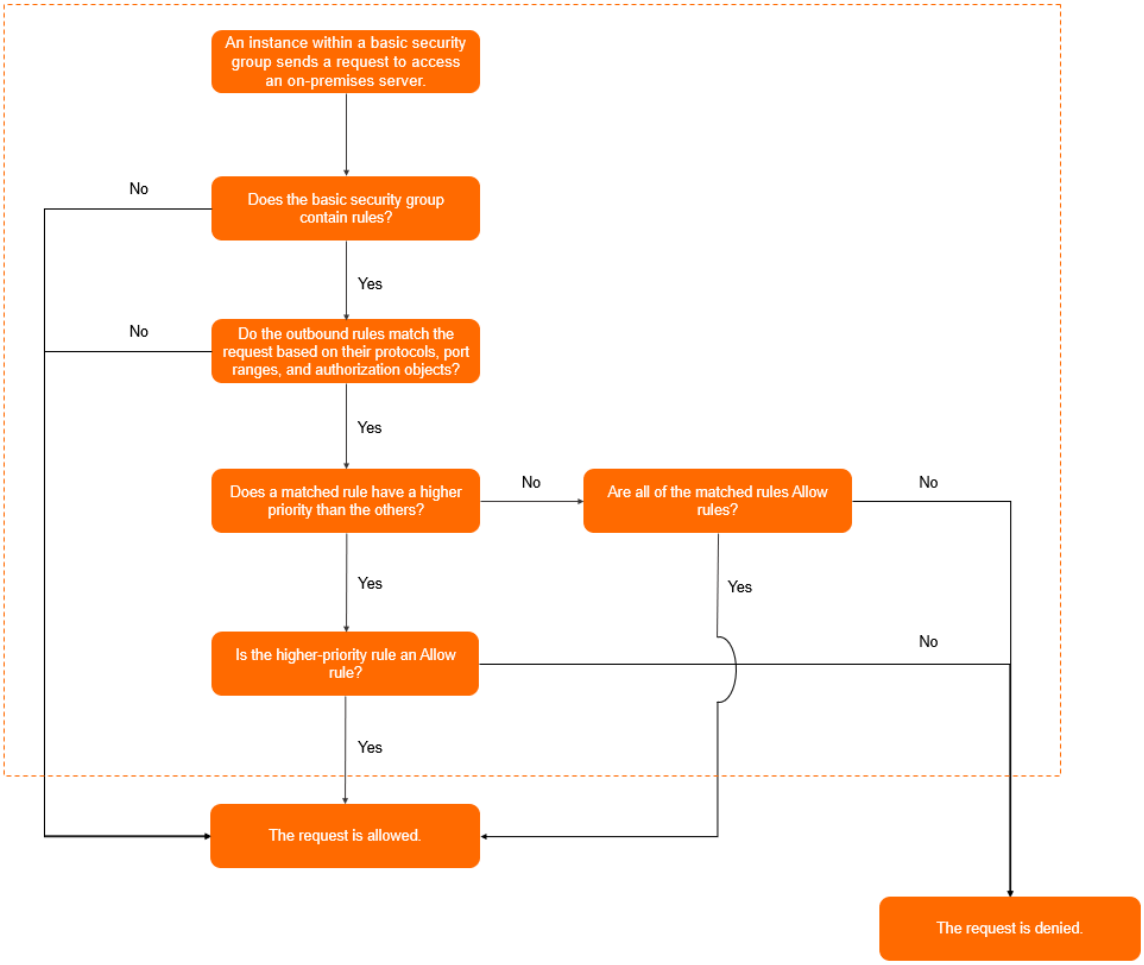
An on-premises server and instances in a basic security group are used in the following flowcharts to show how to filter access requests based on security group rules. In the flowcharts, if a security group contains no rules, it indicates that all user-created and default rules have been deleted from the security group.

Note When a security group is created in the ECS console, default rules are automatically added to the security group. For information about default rules, see Default security groups and Security groups and security group rules.

- The following flowchart shows how the rules of a basic security group control access from an on-premises server to an instance in the security group.



- The following flowchart shows how the rules of a basic security group control access from an instance in the security group to an on-premises server.



Example security group rules

To use an SSH key pair to connect to a Linux instance, make sure that the security group of the instance contains a rule to allow inbound SSH access to the required port. The following table describes an example rule that allows inbound SSH access to port 22 in a security group of the VPC type.

Direction	Action	Priority	Protocol type	Port range	Authorization object
Inbound	Allow	1	Custom TCP	Destination: 22/22	Source: 0.0.0.0/0

> **Note** `0.0.0.0/0` indicates all IP addresses. For security purposes, we recommend that you specify specific IP addresses as authorization objects based on the principle of least privilege.

Basic security groups to which no user-created rules are added allow all outbound access. If you want to use a basic security group as a whitelist, you can add a rule to deny all outbound access. The following table describes an example rule that is added to a security group of the VPC type to deny all outbound access.

Direction	Action	Priority	Protocol type	Port range	Authorization object
Outbound	Forbid	100	All	Destination: -1/-1	Destination: 0.0.0.0/0

For information about more example security group rules, see Security groups for different use casesConfiguration guide for ECS security groups.

2.11.2. Query security group rules

This topic describes how to query security group rules. After you add security group rules, you can query their details in the console.

Prerequisites

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

Procedure

1.
2.
3.
4. Find the security group whose rules you want to query, and then click **Add Rules** in the **Actions** column.
5. Click a rule direction to query the corresponding security group rules.
   - If the security group is of the VPC type, select **Inbound** or **Outbound**.
   - If the security group is of the classic network type, select **Internal Network Ingress**, **Internal Network Egress**, **Internet Ingress**, or **Internet Egress**.

Related information

- DescribeSecurityGroupAttribute

2.11.3. Modify security group rules

This topic describes how to modify security group rules. Improper configurations of security group rules may cause serious security risks. You can modify improper rules in a security group to ensure the network security of instances within the security group.

Prerequisites

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

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.
2.
3.
4. Find the security group whose rules you want to modify, and then click **Add Rules** in the **Actions** column.
5. Select a direction of security group rules.
   - If the security group is of the VPC type, select **Inbound** or **Outbound**.
   - If the security group is of the classic network type, select **Internal Network Ingress**, **Internal Network Egress**, **Internet Ingress**, or **Internet Egress**.
6. Find the security group rules that you want to modify 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.
7. After you modify security group rules, click **OK**.

2.11.4. Restore security group rules

This topic describes how to restore rules from one security group to another. For example, if you want to apply new security group rules to an ECS instance that is running an online application, you can clone the security group to make a backup, and then modify the rules. If the new security group rules affect the online application, you can perform a complete or partial restoration of the security group rules.

Prerequisites

- The security group whose rules are to be restored (source security group) and the security group based on which rules in the source security group are to be restored (destination security group) must be in the same region.
- The source security group and the destination security group must be of the same network type.

Context

When you restore security group rules, you fully or partially restore the rules from the destination security group to the source security group.

- **Completely Restore**: deletes the rules that do not exist in the destination security group from the source security group, and adds the rules that exist only in the destination security group to the source security group. After the restoration is complete, the source security group has the same rules as the destination security group.
- **Partially Restore**: adds the rules that exist only in the destination security group to the source security group, and ignores the rules that exist only in the source security group.

> **Note**
>
> Restoring security group rules has the following limits: If system-level security group rules with a priority of 110 exist in the destination security group, these rules cannot be created during restoration. Rules in the source security group after restoration may not be as expected. If you need the system-level security group rules, you must manually create them and set their priority to 100.

Procedure

1.
2.
3.
4. On the **Security Groups** page, find the security group whose rules you want to restore and click **Restore Rules** in the **Actions** column.
5. In the **Restore Rules** dialog box, perform the following operations:
   i. Set **Destination Security Group**. The specified destination security group must have rules different from those in the source security group.
   ii. Set **Restoration Type**.
   - If you want the source security group to have the same rules as the destination security group, select **Completely Restore**.
   - If you want to add the rules that exist only in the destination security group to the source security group, select **Partially Restore**.

   iii. Preview the restoration result.
   - The rules highlighted in green exist only in the destination 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 destination security group.
     - If you select **Completely Restore**, these rules are removed from the source security group.
     - If you select **Partially Restore**, these rules are retained in the source security group.

   iv. Click **OK**.
   After the rules are restored, the **Restore Rules** dialog box is closed.

Result

On the **Security Groups** page, find the source security group, and then click **Add Rules** in the **Actions** column. On the **Security Group Rules** page, you can view the updated security group rules.

2.11.5. Export security group rules

You can export security group rules to JSON or CSV files for on-premises backup.

Procedure

1.

2.
3.
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. In the **Access Rule** section, click **Export**, select a file format, and then save the file to your computer.
   - **JSON Format**

     A JSON file must follow the following naming convention: *ecs_${regionID}_${groupID}.json*.

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

     A CSV file must follow the following naming convention: *ecs_sgRule_${groupID}_${regionID}_${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*.

2.11.6. Import security group rules

Security group rules can be imported to security groups. You can export the rules of a security group to a file, and then import the file to other security groups or the original security group to create or restore security group rules in a quick and easy manner.

Context

You can import security group rules from different regions.

You can choose **Export** > **JSON Format** or **Export** > **CSV Format** on the Security Group Rules page of a security group to download and save the security group rules to a local JSON or CSV file. You can modify the JSON or CSV file and add custom security group rules in the required format.

Procedure

1.
2.
3.
4. On the **Security Groups** page, find the security group to which you want to import rules and click **Add Rules** in the **Actions** column.
5. In the **Access Rule** section of the Security Group Rules page, click **Import Security Group Rule**.
6. In the **Import Security Group Rule** dialog box, click **Select a file** and then select the local JSON or CSV file that you want to import.

   The dialog box provides a preview of the rules in the file. The following information about the rules is displayed:
   - The result of the import check. If a rule fails the import check, you can move the pointer over the warning icon for details.
   - Details of the rules.

> **Note** You can import a maximum of 200 security group rules to a security group. Newly imported rules do not overwrite existing rules. When the maximum number of rules in the security group is reached, excess rules are not imported to the security group.

7. Click **Start**.

2.11.7. Delete a security group rule

This topic describes how to delete a security group rule that is no longer needed to allow or deny access to instances in a security group.

Procedure

1.
2.
3.
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 a tab based on the network type of the security group.
   - If the network type of the security group is Virtual Private Cloud (VPC), click the **Inbound** or **Outbound** tab.
   - If the network type of the security group is classic network, click the **Inbound**, **Outbound**, **Internet Ingress**, or **Internet Outbound** tab.
6. Find the security group rule that you want to delete and click **Delete** in the **Actions** column.
7. In the Delete Security Group Rule message, click **OK**.

Related information

- RevokeSecurityGroup
- RevokeSecurityGroupEgress

3.Key pairs

3.1. Overview

An SSH key pair is a secure and convenient authentication method provided by Alibaba Cloud for instance logon. 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 an encryption algorithm. By default, 2048-bit RSA key pairs are used. Before you log on to a Linux instance by using 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 lock away the private key. The private key is unencrypted. It is in the `PKCS#8` format and Privacy-Enhanced Mail (PEM) encoded.

Benefits

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

- Security: SSH key pairs provide higher security and reliability for logons.
  - SSH key pairs are more secure than general user passwords against brute-force attacks.
  - Private keys cannot be deduced even if the public keys are maliciously acquired.
- Ease of use:
  - If you configure a public key on a Linux instance, you can use the corresponding private key to run SSH commands or other tools for passwordless logons to the instance.
  - You can log on to a large number of Linux instances at the same time. If you want 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 is 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 SSH key pairs in a region.
- When you bind SSH key pairs to Linux instances in the ECS console, you can bind a single SSH key pair to a Linux instance. If the instance already has a key pair bound, the new key pair replaces the original one. If you want to use multiple key pairs to log on to a Linux instance, you can manually modify the *~/.ssh/authorized_keys* file from within the instance to add multiple key pairs.

- Instances of retired instance types do not support logons based on SSH key pairs. For more information, see Retired 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 methods

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.

  > **Notice** If you create a key pair in the ECS console, you must download and securely lock away the private key. 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 then 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

3.2. Manage SSH key pairs

3.2.1. Create an SSH key pair

This topic describes how to create an SSH key pair in the Elastic Compute Service (ECS) console. After an SSH key pair is created, its private key is automatically downloaded. You must securely store the private key and ensure its confidentiality. To log on to an ECS instance to which an SSH key pair is bound, you must provide the private key. You can have a maximum of 500 key pairs within a region.

Procedure

1.
2.
3.
4. Click **Create SSH Key Pair**.
5. On the **Create SSH Key Pair** page, configure the parameters described in the following table.

Parameter	Description
SSH Key Pair Name	Enter a name for the key pair. The key pair name must be unique. The name must be 2 to 128 characters in length and can contain letters, digits, periods (.), underscores (_), hyphens (-), and colons (:). It cannot start with a digit or special character.
Creation Type	Select a method of creating the key pair. We recommend that you select **Auto-create**. Then, you must securely store the private key in a timely manner and ensure its confidentiality. ○ **Auto-create**: The system creates a key pair for you. The private key is automatically downloaded after the key pair is created. The private key can be downloaded only once. You must securely store the private key file and ensure its confidentiality. ○ **Import**: You can import a Base64-encoded public key.
Resource Group	You can assign the key pair to a resource group for easy management. For more information, see Resource groups.
Tag	Select one or more tags to add to the key pair. You can add one or more tags to a key pair to facilitate resource search and aggregation. For more information, see Overview.

6. Click **OK**.

Result

After the key pair is created, your browser downloads the private key file (*<Key pair name>.pem*) to your computer.

> **Notice** Private key files are downloaded to your computer only when Auto-create is selected. Private key files are not saved in the ECS console and cannot be recovered if they are lost. Make sure that you securely store your private key files and ensure their confidentiality.

What's next

Before you can use a created key pair to log on to an instance, you must bind the key pair to the instance.

- For information about how to bind a key pair to an instance, see Bind an SSH key pair to an instance.
- For information about how to log on to an instance by using a key pair, see Connect to a Linux instance by using an SSH key pair.

Related information

- CreateKeyPair

3.2.2. Import an SSH key pair

You can create an SSH key pair in the Elastic Compute Service (ECS) console. You can also use a third-party tool to generate an SSH key pair and import its public key to Alibaba Cloud.

Prerequisites

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

Context

> **Note**
> - Do not import the private key. You must keep the private key secure. To log on to an ECS instance bound with an SSH key pair, you must have the private key.
> - Only one public key can be imported into an ECS instance.

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

Imported public keys 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.
2.
3.
4. Click **Create SSH Key Pair**.
5. Enter an SSH key pair name and set Creation Type to **Import**.

   > **Note** The SSH key pair name must be unique. Otherwise, you are 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

3.2.3. Bind an SSH key pair to an instance

You can specify an SSH key pair when you create an ECS 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 instance after the instance is created. If your ECS instance originally uses password-based authentication, the password-based authentication is automatically disabled after the key pair is bound.

Context

Each ECS instance can be bound with only one SSH key pair in the console. If an 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.

> **Note** 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 can modify this file to add multiple key pairs or replace existing key pairs. For more information, see Add or replace an SSH key pair.

Procedure

1.
2.
3.
4. Find the key pair to be bound and click **Bind** in the **Actions** column.
5. Select the ECS instance to which to bind the SSH key pair 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, perform 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 instance to be restarted and choose **More > Instance Status > Restart** in the **Actions** column.
   iii. In the **Restart Instance** dialog box, 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 an instance by using the password after you bind a key pair to the instance, 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

3.2.4. Unbind an SSH key pair

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

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.
2.
3.
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

3.2.5. 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.
2.
3.
4. Select one or more SSH key pairs.
5. Click **Delete**.

Related information

- DeleteKeyPairs

3.2.6. View public key information

This topic describes three ways to view public key information. If you want to configure the same public key file for a group of ECS instances but the public key file has no backups in your PC, you can view public key information by using the following methods.

Windows

To view public key information, perform the following operations:

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 following example shows the returned public key information:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABA****+GF9q7rhc6vYrExwT4WU4fsaRcVXGV2Mg9RHex21hl1au77Gkm
nIgukBZjywlQOT4GDdsJy2nBOdJPrCEBIPxxxxxxxxx/fctNuKjcmMMOA8YUT+sJKn3l7rCLkesE+S5880yNdRjBii
Uy40kyr7Y+fqGVdSOHGMXZQPpkBtojcxxxxxxxxxx/htEqGa/Jq4fH7bR6CYQ2XgH/hCap29Mdi/G5Tx1nbUKuIHdM
WOPvjxxxxxxxxx+lHtTGiAIRG1riyNRVC47ZEVCxxxxx
```

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.

3.2.7. 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/bUUduZjauiJa1KQ
     JSF4+czKtqMAv38QEspiWStkSfpTn1g9qeUhfxxxxxxxxxx+XjPsf22fRem+v7MHMa7KnZWiHJxO62D4Ihvv2
     hKfskz8K44xxxxxxxxx+u17IaL2l2ri8q9YdvVHt0Mw5TpCkERWGoBPE1Y8vxFb97TaE5+zc+2+eff6xxxxx
     xxxxx/feMeCxpx6Lhc2NEpHIPxMpjOv1IytKiDfWcezA2xxxxxxxxx/YudCmJ8HTCnLId5LpirbNE4X08Bk7
     tXZAxxxxxxxxx/FKB1Cxw1TbGMTfWxxxxxxxxx imported-openssh-key
     ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDdlrdZwV3+GF9q7rhc6vYrExwT4WU4fsaRcVXGV2Mg9RHex
     21hl1au77GkmnIgukBZjywlQOT4GDdsJy2nBOdJPrCEBIPxxxxxxxxxxx/fctNuKjcmMMOA8YUT+sJKn3l7rC
     LkesE+S5880yNdRjBiiUy40kyr7Y+fqGVdSOHGMXZQPpkBtojcxxxxxxxxxx/htEqGa/Jq4fH7bR6CYQ2XgH/
     hCap29Mdi/G5Tx1nbUKuIHdMWOPvjxxxxxxxxxx+lHtTGiAIRG1riyNRVC47ZEVCg9iTWWGrWFvxxxxxxxxxx
     /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+GF9q7rhc6vYrExwT4WU4fsaRcVXGV2Mg9RHex
     21hl1au77GkmnIgukBZjywlQOT4GDdsJy2nBOdJPrCEBIP6t0Mk5aPkK/fctNuKjcmMMOA8YUT+sJKn3l7rCL
     kesE+S5880yNdRjBiiUy40kyr7Y+fqGVdSOHGMXZQPpkBtojcV14uAy0yV6/htEqGa/Jq4fH7bR6CYQ2XgH/h
     Cap29Mdi/G5Tx1nbUKuIHdMWOPvjGACGcXclex+lHtTGiAIRG1riyNRVC47ZEVCg9iTWWGrWFvVlnI0E3Deb/
     9H9mPCO1Xt2fxxxxxxxxBtmR imported-openssh-key
     ```

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

4.Manage identities and permissions

4.1. RAM overview

Resource Access Management (RAM) allows you to manage the identities and permissions of Alibaba Cloud services and users to implement access control over resources.

Identities

Identities in RAM include physical identities (RAM users and user groups) and virtual identities (RAM roles).

- A RAM user is an entity that has a logon password and an AccessKey pair. A RAM user group is a collection of RAM users who share the same responsibilities. You can attach a set of policies to a RAM user or user group. A RAM user can represent a person or an application to interact with Alibaba Cloud, which eliminates the need to share confidential account information such as your password when you need to share your resources with other users. You must follow the principle of least privilege when you grant permissions to RAM users or user groups. This way, leaks of confidential information do not jeopardize the security of all resources within your account.
- A RAM role is an identity that has policies attached to determine what the identity can and cannot do. A RAM role does not have a logon password or an AccessKey pair. A RAM role must be assumed by a trusted entity that wants to obtain the permissions of the role. During the communication between Alibaba Cloud services, after a trusted entity such as an Elastic Compute Service (ECS) instance assumes a RAM role, the entity can use the temporary credentials issued by Security Token Service (STS) to the role to access the APIs of other Alibaba Cloud services. This eliminates the need for high-risk operations such as writing AccessKey pairs to configuration files and ensures the security of AccessKey pairs.

Permissions

A policy is an object that defines permissions in RAM. Each policy consists of a few basic elements. For more information, see Policy elements. You can attach policies to an identity (a RAM user, user group, or role) to control what actions the identity can perform, on which resources, and under what conditions.

Policies are categorized into system policies and custom policies.

- System policies are the common policies predefined by Alibaba Cloud. These system policies cannot be modified. The following system policies are related to ECS:
  - AliyunECSFullAccess: grants the permissions to perform all operations on all ECS resources, including the permissions to create, view, and delete ECS resources.
  - AliyunECSReadOnlyAccess: grants the read-only permissions on ECS resources.
  - AliyunECSNetworkInterfaceManagementAccess: grants the permissions to manage elastic network interfaces (ENIs), including the permissions to create, view, and delete ENIs.
  - AliyunECSAssistantFullAccess: grants the permissions to manage Cloud Assistant commands, including the permissions to create, run, view, and delete Cloud Assistant commands.
  - AliyunECSAssistantReadonlyAccess: grants the read-only permissions on Cloud Assistant commands.

- AliyunECSImageExportRolePolicy: grants the permissions required to export images, including the read permissions on Object Storage Service (OSS) buckets and the read and write permissions on OSS objects.
- AliyunECSImageImportRolePolicy: grants the permissions required to import images, including the write permissions on OSS buckets and the read and write permissions on OSS objects.
- AliyunECSInstanceForYundunSysTrustRolePolicy: grants the permissions required for security-enhanced ECS instances to use the Alibaba Cloud trusted system.
- AliyunECSDiskEncryptRolePolicy: grants the permissions required to encrypt disks.

For more information about system policies, see Example system policies.

- Custom policies are the policies that you create and manage within your Alibaba Cloud account. For information about and examples on how to work with custom policies, see Create a custom policy and Overview of sample policies.

Usage examples

Perform the following operations to control access to resources for employees inside an enterprise:

1. Create a SysAdmins user group for employees who need to create and manage resources and attach policies that grant the permissions to perform all operations on all resources to the user group.
2. Create a Developers user group for employees who need to use resources and attach policies that grant the permissions to call the StartInstance, StopInstance, and DescribeInstances operations to the user group.
3. Create RAM users for employees and add the users to different user groups based on the needs of the employees.
4. To enhance network security, attach policies to deny the RAM users access to resources if they are using an IP address from outside the enterprise.
5. If employees change positions from a developer to an administrator, move their corresponding RAM users from the Developers user group to the SysAdmins user group.
6. If RAM users in the Developers user group require more permissions, modify the policies of the user group to grant required permissions to all RAM users in the group.

Attach one of the following RAM roles to an ECS instance so that the instance can use the temporary credentials provided by the role to access other Alibaba Cloud services:

- AliyunECSImageExportDefaultRole: The AliyunECSImageExportRolePolicy system policy is attached to this role. After this role is attached to an ECS instance, the instance has the permissions required to export images.
- AliyunECSImageImportDefaultRole: The AliyunECSImageImportRolePolicy system policy is attached to this role. After this role is attached to an ECS instance, the instance has the permissions required to import images.
- AliyunECSInstanceForYundunSysTrustRole: The AliyunECSInstanceForYundunSysTrustRolePolicy system policy is attached to this role. After this role is attached to an ECS instance, the instance has the permissions required to use the Alibaba Cloud trusted system.
- AliyunECSDiskEncryptDefaultRole: The AliyunECSDiskEncryptRolePolicy system policy is attached to this role. After this role is attached to an ECS instance, the instance has the permissions required to encrypt disks.

Related information

- What is RAM?

4.2. Control access to resources by using RAM users

In scenarios where multiple users simultaneously access resources, you can create multiple RAM users and grant the RAM users permissions based on their roles so that different RAM users can access and manage different resources. This can improve management efficiency and reduce the risk of information leaks. This topic describes how to create a RAM user and attach a policy to the RAM user to control access to Elastic Compute Service (ECS) resources.

Procedure

1. Create a RAM user.

   For more information, see Create a RAM user.

2. (Optional)Create a custom policy.

   Alibaba Cloud provides system policies that allow RAM users to access ECS resources. For more information, see Example system policies. If system policies cannot meet your requirements, you can create custom policies. For more information, see Create a custom policy.

   If you set Configuration Mode to **Script** when you create a custom policy on the Create Custom Policy page in the Resource Access Management (RAM) console, you must specify the Action and Resource parameters in Statement. For information about the values of these parameters, see Authentication rules. For information about the values of other parameters, see Policy structure and syntax.

   - The following sample policy created by using the code editor allows a RAM user to create pay-as-you-go ECS 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 created by using the code editor allows a RAM user to create subscription ECS instances. bss-related API operations can be called to query and pay for 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 created by using the code editor allows a RAM user to query instance and disk information after the user creates an ECS instance:

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

3. Attach the policy to the RAM user to grant the user permissions to access ECS resources.

   For more information, see Grant permissions to a RAM user.

What's next

After permissions are granted to the RAM user, the permissions immediately take effect. The RAM user can log on to the RAM console to manage the applicable resources. For more information, see Log on to the Alibaba Cloud Management Console as a RAM user.

4.3. Use RAM roles to control resource access

4.3.1. 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.

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 RDS by using an AccessKey pair of an Alibaba Cloud account or 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:

- Bind a role to 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 Use RAM roles to access other Alibaba Cloud services.
- For more information about how to obtain a temporary authorization token, see Obtain a temporary authorization token.

4.3.2. Attach an instance RAM role to an ECS instance

This topic describes how to create an instance RAM role, attach a policy to the RAM role, and then attach the RAM role to an Elastic Compute Service (ECS) instance by using the Resource Access Management (RAM) and ECS consoles.

Prerequisites

- The RAM service is activated. For more information, see Activate RAM.
- The ECS instance to which you want to attach a RAM role is located in a virtual private cloud (VPC).
- A RAM user is already authorized to use the instance RAM role if you use the RAM user to perform the procedure described in this topic. For more information, see Authorize a RAM user to manage an instance RAM role.

Context

- An instance RAM role can be attached to a single instance at a time.
- If you have attached an instance RAM role to an ECS instance and want to access the APIs of other Alibaba Cloud services from applications deployed on the instance, 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 attach the role to an ECS instance in the RAM console:

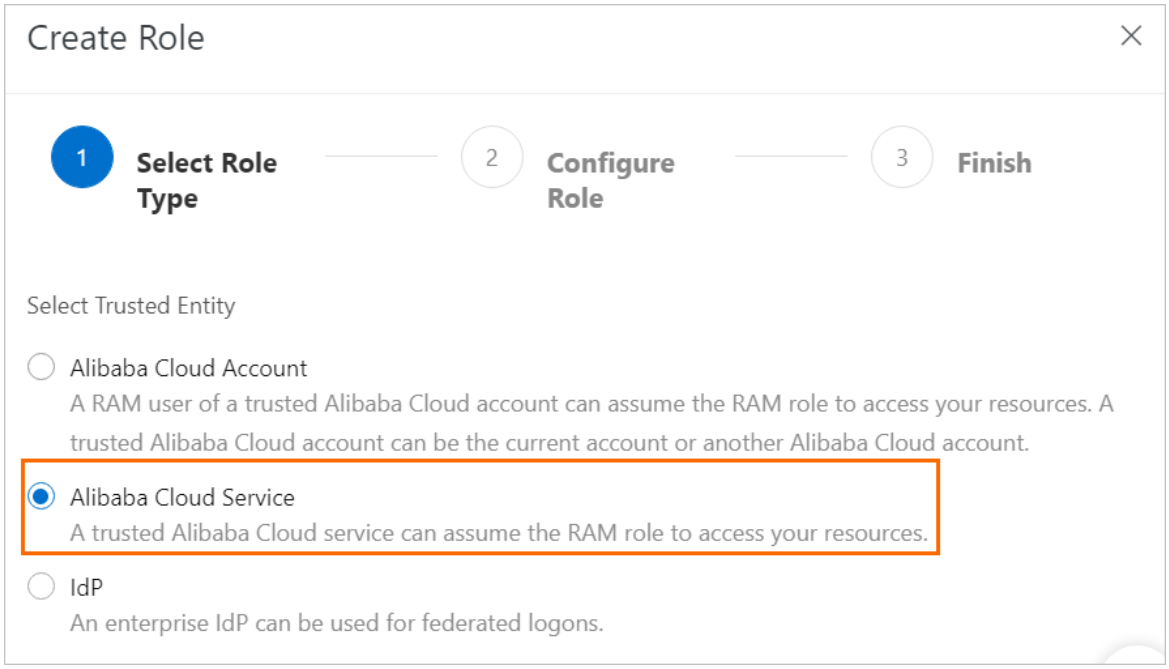
1. Step 1: Create an instance RAM role
2. Step 2: Attach a policy to the RAM role
3. Step 3: Attach the RAM role to an ECS instance

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 your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Roles**.
3. On the **Roles** page, click **Create Role**.
4. In the **Create Role** panel, select **Alibaba Cloud Service** as the trusted entity and click **Next**.

   Select **Alibaba Cloud Service** to authorize ECS instances to access or manage your cloud resources. After you select **Alibaba Cloud Service** for the RAM role, you can attach the RAM role to ECS instances.



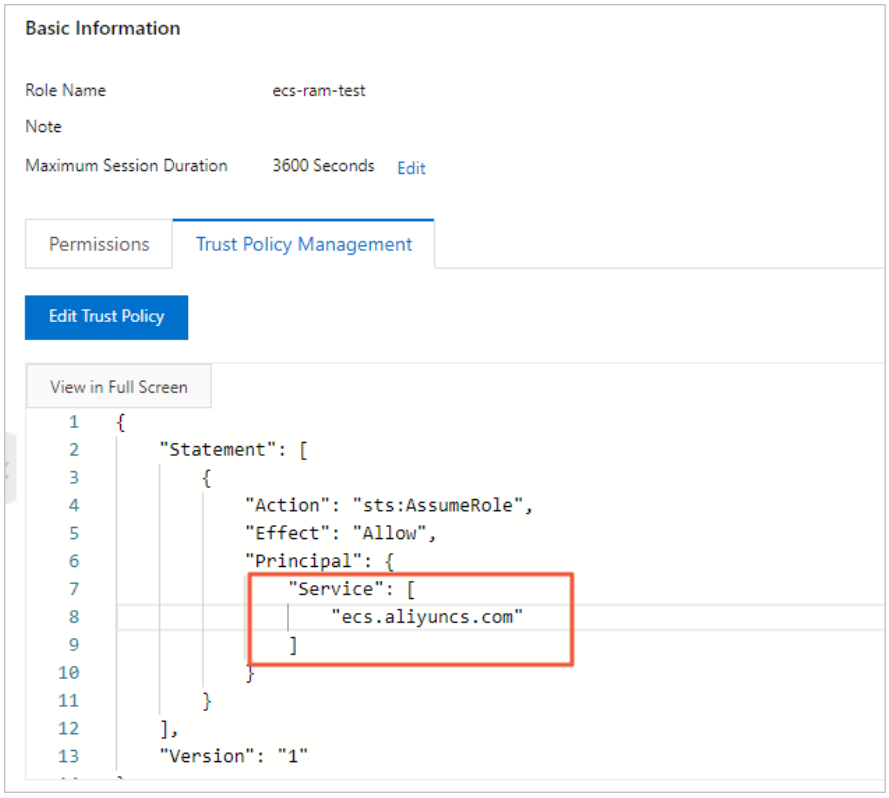
Note

If you select **Alibaba Cloud Account** for a RAM role, you must click **Edit Trust Policy** on the **Trust Policy Management** tab to manually add the following permission policy for ECS after the RAM role is created:

```
"Service": [
    "ecs.aliyuncs.com"
]
```

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**.
9. Click **Close**.

After the RAM role is created, check whether the RAM role include the following permission policy for ECS on the **Trust Policy Management** tab.



Step 2: Attach a policy to the RAM role

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

1.
2. (Optional) Create a custom policy if you do not want to use a system policy. For more information, see the "Create a custom policy" section in Control access to resources by using RAM users.
3.
4.
5.
6.
7.

Step 3: Attach the RAM role to an ECS instance

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

1.
2.
3.
4. Find the ECS instance to which you want to attach the RAM role and choose **More > Instance Settings > Bind/Unbind RAM Role** in the Actions column.

5. In the Bind/Unbind RAM Role dialog box, select the RAM role in the RAM Role drop-down list and click **OK**.

Alternatively, you can select the created instance RAM role from the **RAM Role** drop-down list in the **System Configurations (Optional)** step when you create an ECS instance. For more information, see Create an instance by using the wizard.

Related information

- CreateRole
- CreatePolicy
- AttachPolicyToRole
- AttachInstanceRamRole

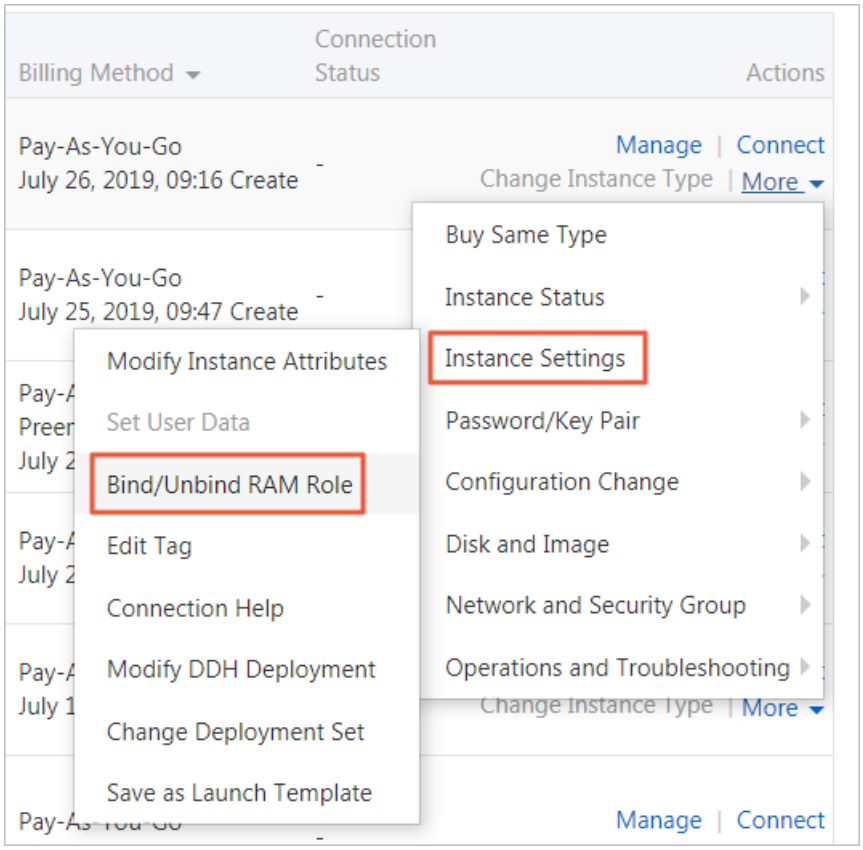
4.3.3. Manage an instance RAM role

4.3.3.1. Replace an instance RAM role

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

Procedure

1.
2.
3.
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

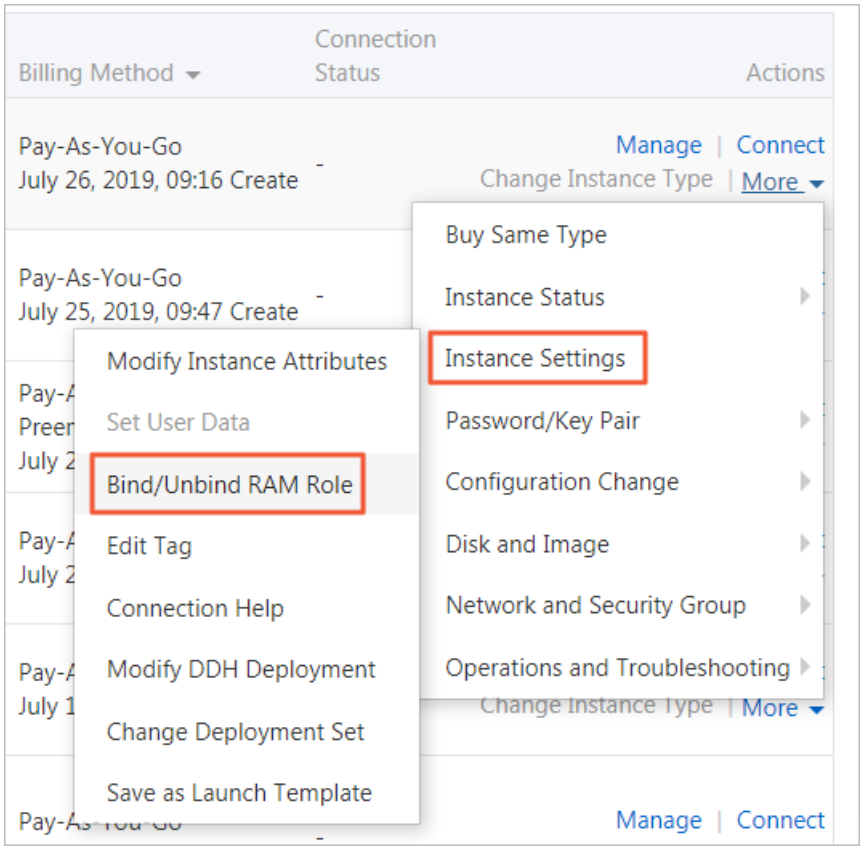
- AttachInstanceRamRole

4.3.3.2. Unbind a RAM role

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

Procedure

1.
2.
3.
4. Find an ECS instance to which a RAM role has been bound. Choose **More > Instance Settings > Bind/Unbind RAM Role** in the Actions column.



5. Select **Unbind** as **Action**, and then click **OK**.

Related information

- DetachInstanceRamRole

4.3.3.3. Obtain a temporary authorization token

You can obtain a temporary authorization token for an instance RAM role. The token is updated on a regular basis and allows you to use the permissions and resources granted to the RAM role.

Procedure

1. Connect to an ECS instance from a remote client. For more information, see Connection methodsGuidelines on instance connection.
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 following command:

     ```
     curl http://100.100.100.200/latest/meta-data/ram/security-credentials/EcsRamRoleDocumentTesting
     ```

   - For Linux instances, run the following PowerShell command:

     ```
     Invoke-RestMethod http://100.100.100.200/latest/meta-data/ram/security-credentials/EcsRamRoleDocumentTesting
     ```

     Example of a temporary authorization token obtained:

```
{
   "AccessKeyId" : "<yourAccessKeyId>",
   "AccessKeySecret" : "<yourAccessKeySecret>",
   "Expiration" : "2017-11-01T05:20:01Z",
   "SecurityToken" : "<yourSecurityToken>",
   "LastUpdated" : "2017-10-31T23:20:01Z",
   "Code" : "Success"
}
```

Related information

- Overview of ECS instance metadata

4.3.3.4. Authorize a RAM user to manage an instance RAM role

If you want to attach, replace, or detach an instance RAM role by using a RAM user, you must use the Alibaba Cloud account to authorize the RAM user to manage the instance RAM role. The procedure described in this topic can be used only when you use 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. If the RAM user does not have the PassRole permission, the RAM user cannot exercise the permissions specified in role policies.

Procedure

1.
2.
3.
4. In the **Add Permissions** panel, grant permissions to the RAM user.
   i.
   ii.
   iii. In the **Select Policy** section, click **Create Policy**.

iv. On the Create Policy page, click the JSON tab to create a custom policy.

The following code describes the custom policy. [ECS RAM Action] indicates the 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": "*"
        }
    ]
}
```

5. Go back to the **Add Permissions** panel and click **Custom Policy** in the **Select Policy** section.
6. In the **Authorization Policy Name** column, click the names of policies to be attached to the RAM user.

> **Note** In the Selected section on the right, you can click the cross sign (×) next to a RAM policy to remove the RAM policy.

7. Click **OK**.
8. Click **Complete**.

Related information

- CreatePolicy
- AttachPolicyToRole

4.3.4. Use an instance RAM role by calling API operations

This topic describes how to create an instance RAM role, attach a policy to the RAM role, and then attach the RAM role to an Elastic Compute Service (ECS) instance by calling API operations.

Prerequisites

The Resource Access Management (RAM) service is activated. For more information, see Activate RAM.

Context

The following limits apply:

- Instance RAM roles can be attached only to ECS instances in virtual private clouds (VPCs).
- Only one instance RAM role can be attached to a single ECS instance at a time.
- If you have attached an instance RAM role to an ECS instance and want to access the APIs of other Alibaba Cloud services from applications deployed on the instance, 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.
- If you want to use an instance RAM role as a RAM user, you must use the Alibaba Cloud account to authorize the RAM user to use the instance RAM role. For more information, see Authorize a RAM user to use an instance RAM role.

Procedure

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

1. Step 1: Create an instance RAM role
2. Step 2: Attach a policy to the instance RAM role
3. Step 3: Attach the instance RAM role to an instance
4. Step 4: (Optional) Detach the instance RAM role from the instance
5. Step 5: (Optional) Obtain a temporary authorization token
6. Step 6: (Optional) 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. In this 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: Attach a policy to the instance RAM role

1. Call the CreatePolicy operation to create an authorization policy.
   - Set the RoleName parameter. In this 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 attach the policy to the role.
   - Set the PolicyType parameter to *Custom*.
   - Set the PolicyName parameter. In this example, set this parameter to *EcsRamRoleDocumentTestingPolicy*.
   - Set the RoleName parameter. In this example, set this parameter to *EcsRamRoleDocumentTesting*.

Step 3: Attach the instance RAM role to an instance

Call the AttachInstanceRamRole operation to attach the instance RAM role to an instance.

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

Step 4: (Optional) Detach the instance RAM role from the instance

Call the DettachInstanceRamRole operation to detach the instance RAM role from the instance.

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

Step 5: (Optional) Obtain a temporary authorization token

You can obtain a temporary access token from the instance RAM role. The token is automatically updated on a regular basis and allows you to exercise the permissions and use the resources of the instance RAM role. You can perform the following operations:

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

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

Obtain the temporary authorization token. A command output similar to the following one is returned.

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

Step 6: (Optional) 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 RAM user the PassRole permission on the instance RAM role. If the RAM user does not have 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

- Attach an instance RAM role to an ECS instance
- Use RAM roles to access other Alibaba Cloud services
- CreateRole
- ListRoles

- CreatePolicy
- AttachPolicyToRole
- AttachInstanceRamRole
- DetachInstanceRamRole
- DescribeInstanceRamRole

4.4. Example system policies

This topic describes example system policies to help you understand the details and operations of common system policies used for Elastic Compute Service (ECS) and create custom policies based on your needs.

AliyunECSFullAccess

System policy that grants the permissions to manage ECS resources

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

AliyunECSReadOnlyAccess

System policy that grants the permissions to view ECS resources

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": "ecs:Describe*",
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "ecs:List*",
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "vpc:DescribeVpcs",
                "vpc:DescribeVSwitches"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

AliyunECSNetworkInterfaceManagementAccess

System policy that grants the permissions to manage elastic network interfaces (ENIs)

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "vpc:DescribeVSwitchAttributes"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "ecs:CreateNetworkInterface",
                "ecs:DeleteNetworkInterface",
                "ecs:DescribeNetworkInterfaces",
                "ecs:CreateNetworkInterfacePermission",
                "ecs:DescribeNetworkInterfacePermissions",
                "ecs:DeleteNetworkInterfacePermission"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

AliyunECSAssistantFullAccess

System policy that grants the permissions to manage Cloud Assistant commands

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeInstances",
                "ecs:DescribeTag*",
                "ecs:*Command",
                "ecs:DescribeCommand*",
                "ecs:DescribeInvocation*",
                "ecs:StopInvocation",
                "ecs:*CloudAssistant*"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/*",
                "acs:ecs:*:*:command/*"
            ]
        }
    ]
}
```

AliyunECSAssistantReadonlyAccess

System policy that grants the permissions to view Cloud Assistant commands

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeInstances",
                "ecs:DescribeTag*",
                "ecs:DescribeCommand*",
                "ecs:DescribeInvocation*",
                "ecs:DescribeCloudAssistant*"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/*",
                "acs:ecs:*:*:command/*"
            ]
        }
    ]
}
```

AliyunECSImageExportRolePolicy

System policy that grants the permissions required to export images

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "oss:GetObject",
                "oss:PutObject",
                "oss:DeleteObject",
                "oss:GetBucketLocation",
                "oss:AbortMultipartUpload",
                "oss:ListMultipartUploads",
                "oss:ListParts",
                "oss:GetBucketInfo",
                "oss:GetBucketUserQos"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

AliyunECSImageImportRolePolicy

System policy that grants the permissions required to import images

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "oss:GetObject",
                "oss:GetBucketLocation",
                "oss:GetBucketInfo"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

AliyunECSInstanceForYundunSysTrustRolePolicy

System policy that grants the permissions required for security-enhanced instances to use the Alibaba Cloud trusted system

```
{
    "Statement": [
        {
            "Action": [
                "yundun-systrust:GenerateNonce",
                "yundun-systrust:GenerateAikcert",
                "yundun-systrust:RegisterMessage",
                "yundun-systrust:PutMessage"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ],
    "Version": "1"
}
```

AliyunECSDiskEncryptRolePolicy

System policy that grants the permissions required to encrypt disks

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "kms:List*",
                "kms:DescribeKey",
                "kms:TagResource",
                "kms:UntagResource"
            ],
            "Resource": [
                "acs:kms:*:*:*",
                "acs:kms:*:*:*/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "acs:kms:*:*:*/*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

AliyunServiceRolePolicyForECSAutoProvisioning

System policy that grants the permissions on Auto Provisioning

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "ecs:CreateInstance",
                "ecs:RunInstances",
                "ecs:StartInstance",
                "ecs:AllocatePublicIpAddress",
                "ecs:StopInstance",
                "ecs:DeleteInstance",
                "ecs:DescribeInstances",
                "ecs:DescribeInstanceAttribute",
                "ecs:ModifyInstanceAttribute",
                "ecs:DescribeSecurityGroupAttribute",
                "ecs:DescribeImages",
                "ecs:DescribeSnapshots",
                "ecs:DescribeKeyPairs",
                "ecs:CreateLaunchTemplate",
                "ecs:DescribeLaunchTemplates",
                "ecs:DescribeLaunchTemplateVersions",
                "ecs:DescribeSecurityGroups",
                "ecs:DescribeHpcClusters",
                "ecs:DescribeImageFromFamily",
                "slb:DescribeLoadBalancerAttribute",
                "slb:RemoveBackendServers",
                "slb:DescribeHealthStatus",
                "slb:AddBackendServers",
                "slb:SetBackendServers",
                "slb:DescribeLoadBalancers",
                "slb:DescribeVServerGroups",
                "slb:DescribeVServerGroupAttribute",
                "slb:AddVServerGroupBackendServers",
                "slb:RemoveVServerGroupBackendServers",
                "slb:DescribeMasterSlaveServerGroupAttribute",
                "slb:DescribeMasterSlaveServerGroups",
                "slb:SetVServerGroupAttribute",
                "slb:DescribeLoadBalancerUDPListenerAttribute",
                "slb:DescribeLoadBalancerHTTPListenerAttribute",
                "slb:DescribeLoadBalancerHTTPSListenerAttribute",
                "slb:DescribeLoadBalancerTCPListenerAttribute",
                "rds:ModifySecurityIps",
                "rds:DescribeDBInstanceAttribute",
                "rds:DescribeTaskInfo",
                "rds:DescribeDBInstanceIPArrayList",
                "oos:GetTemplate",
                "oos:StartExecution",
                "ecs:DescribeUserData",
                "ecs:DescribeInstanceRamRole",
                "ecs:DescribeDisks",
                "ecs:DescribeAutoSnapshotPolicyEx",
                "ecs:DescribeDedicatedHosts",
                "ecs:DescribeDedicatedHostTypes"
            ],
```

```
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "vpc:DescribeVpcs",
                "vpc:DescribeVSwitches"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "mns:ListTopic",
                "mns:ListQueue",
                "mns:SendMessage",
                "mns:PublishMessage"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "cms:NodeInstall",
                "cms:NodeStatusList",
                "cms:QueryCustomMetricList",
                "cms:ProfileSet",
                "cms:CreateAlert",
                "cms:DeleteAlert",
                "cms:QueryAlert",
                "cms:UpdateAlert",
                "cms:DisableAlert",
                "cms:EnableAlert",
                "cms:CreateAction",
                "cms:GetAction",
                "cms:CreateDimensions",
                "cms:QueryDimensions",
                "cms:UpdateDimensions",
                "cms:QueryMetricList",
                "cms:ListAlarmHistory"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "ram:PassRole",
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "acs:Service": [
                        "ecs.aliyuncs.com",
                        "oos.aliyuncs.com"
                    ]
```

```
                }
            }
        },
        {
            "Action": "ram:DeleteServiceLinkedRole",
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": "autoprovisioning.ecs.aliyuncs.com"
                }
            }
        }
    ]
}
```

AliyunServiceRolePolicyForECSImageBuilder

System policy that grants the permissions on Image Builder

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "oos:CreateTemplate",
                "oos:StartExecution",
                "oos:CancelExecution",
                "oos:ListExecutions",
                "oos:ListTaskExecutions",
                "oos:ListExecutionLogs",
                "oos:DeleteTemplate"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ecs:DescribeAvailableResource",
                "ecs:DescribeInstances",
                "ecs:DescribeCloudAssistantStatus",
                "ecs:DescribeImages",
                "ecs:DescribeInvocations",
                "ecs:DescribeInvocationResults",
                "ecs:CreateSecurityGroup",
                "ecs:DescribeSecurityGroups",
                "ecs:CancelCopyImage",
                "ecs:RunInstances",
                "ecs:CopyImage",
                "ecs:DeleteSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
```

```
        {
            "Action": [
                "ecs:RebootInstance",
                "ecs:DeleteInstance",
                "ecs:DeleteImage",
                "ecs:DescribeImageSharePermission",
                "ecs:DeleteSecurityGroup",
                "ecs:ModifyImageSharePermission",
                "ecs:InstallCloudAssistant",
                "ecs:RunCommand",
                "ecs:StopInstance",
                "ecs:CreateImage"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ecs:tag/imagepipelineid": "*"
                }
            }
        },
        {
            "Action": [
                "vpc:DescribeVSwitches",
                "vpc:DescribeVpcs",
                "vpc:CreateVpc",
                "vpc:CreateVSwitch",
                "vpc:DeleteVSwitch",
                "vpc:DeleteVpc"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "ram:DeleteServiceLinkedRole",
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": "imagebuilder.ecs.aliyuncs.com"
                }
            }
        }
    ]
}
```

5.Anti-DDoS Basic

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

Anti-DDoS Basic is a free service included in Alibaba Cloud Security. It offers up to 5 Git/s of mitigation capacity against common DDoS attacks for free. The instance type of an ECS instance determines the mitigation capacity that is provided in the free tier. You can log on to the Traffic Security (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 Anti-DDoS Basic is enabled, Alibaba Cloud Security monitors inbound traffic to ECS instances in real time. When large amounts of traffic or suspicious traffic such as DDoS attack traffic is detected, Alibaba Cloud Security redirects the traffic from the destination network to a scrubbing device. The scrubbing device identifies and removes malicious traffic and then returns legitimate traffic to the destination network to be forwarded to the ECS instances. This process is called traffic scrubbing. For more information, see What is Anti-DDoS Origin?.

> **Note** If Anti-DDoS Basic is enabled for an ECS instance, Alibaba Cloud Security triggers a blackhole when inbound traffic from the Internet exceeds 5 Gbit/s. All traffic to the instance is routed to the blackhole and all accesses from the Internet to the instance are blocked to ensure cluster-wide security. For more information, see Blackhole filtering policy of Alibaba Cloud.

Trigger conditions:

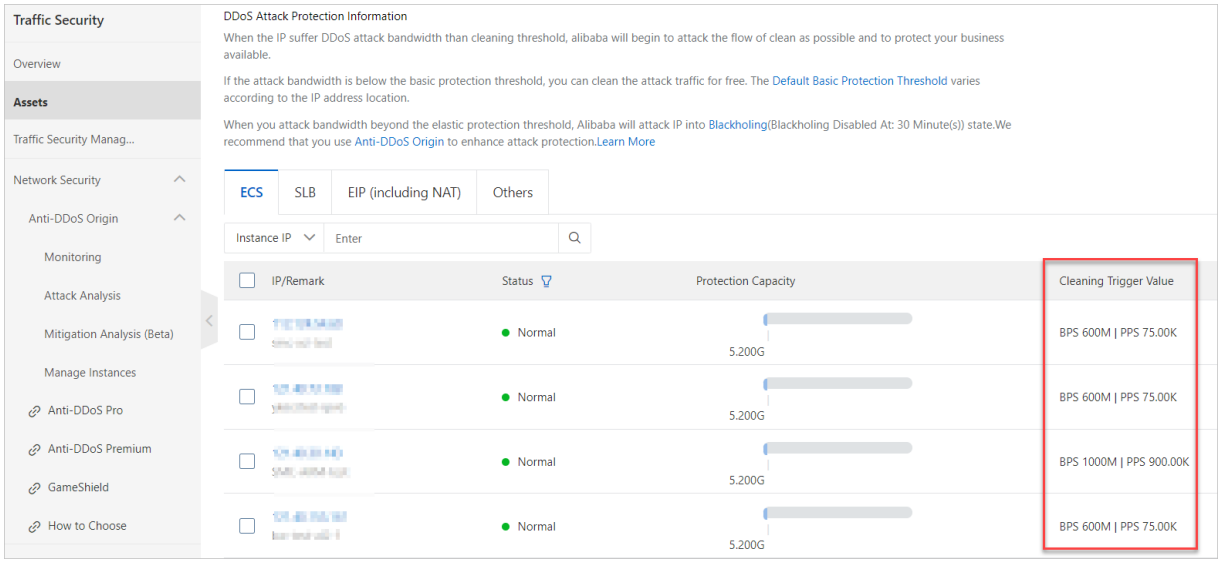
- Traffic pattern. When inbound traffic matches an attack traffic pattern, traffic scrubbing is triggered.
- Traffic amounts. Typically, DDoS attacks generate flood traffic on a magnitude of Gbit/s. When inbound traffic to an ECS instance reaches a specific threshold, traffic scrubbing is triggered regardless of whether the traffic is normal.

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

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

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

The actual scrubbing thresholds are displayed in the Traffic Security console, as shown in the following figure. For information about how to view the thresholds, see Assets.



Operations

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

- Configure scrubbing thresholds. After an ECS instance is created, the maximum thresholds of Anti-DDoS Basic for the instance type are used. However, the maximum BPS threshold for some instance types may be high and not safe. You must set the threshold based on your business needs. For more information, see Configure a traffic scrubbing threshold in Anti-DDoS Basic User Guide.
- (Not recommended) Disable traffic scrubbing. When traffic scrubbing is enabled and inbound traffic to an ECS instance reaches a specific threshold, traffic scrubbing is triggered regardless of whether the traffic is normal. This may affect or interrupt normal business. You can manually disable traffic scrubbing for ECS instances. For more information, see Cancel traffic cleaning in Anti-DDoS Basic User Guide.

> **Warning** After traffic scrubbing is disabled for an ECS instance, when inbound traffic to the instance exceeds 5 Gbit/s, all traffic to the instance is routed to a blackhole. Proceed with caution.

6.Basic security services

Alibaba Cloud Security Center provides Elastic Compute Service (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 collects and virtualizes security logs and fingerprints of ECS assets. Basic security services such as vulnerability detection, security alerts, and baseline check are provided free of charge. 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 What is Security Center?

Basic security services support the following billing methods:

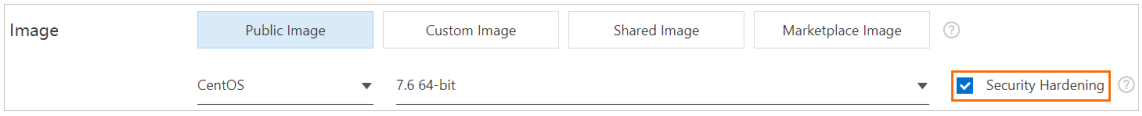
- In Security Center Basic Edition, basic security services for ECS are free of charge.
- If you want to upgrade to Security Center Advanced or Enterprise Edition, log on to the Security Center console for a free trial or purchase of Security Center Advanced or Enterprise Edition. For more information about the billing methods of Security Center Advanced Edition and Enterprise Edition, see Billing 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 the Security Center agent is not installed on your ECS instance, your ECS instance is not protected. The security data of the instance, such as vulnerabilities, alerts, baseline vulnerabilities, and asset fingerprints, is not displayed in the ECS console. For more information about the installation paths of the Security Center agent, see Overview of the Security Center agent.

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

- Have the Security Center agent automatically installed when you create an ECS instance.
  i.
  ii.
  iii.
  iv. When you create an ECS instance, select **Security Hardening** in the **Image** section. The system installs the Security Center agent on the ECS instance. For more information, see Create an instance by using the 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.
  ii. On the **Overview** page, click **Handle** in the **Security Score** section to go to the Security Center console.

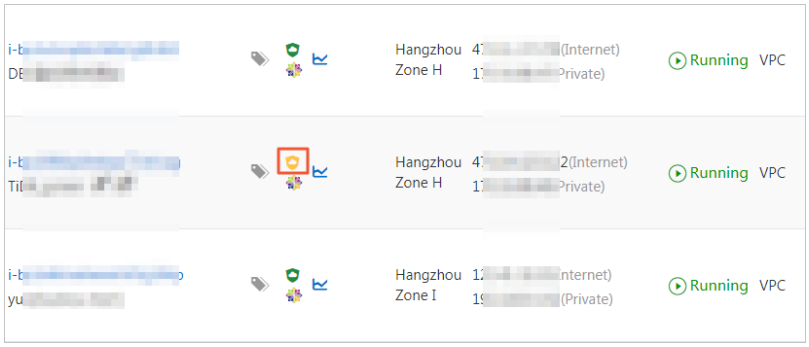
iii. Install the Security Center agent. For more information, see Install the Security Center agent in *Security Center documentation*.

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

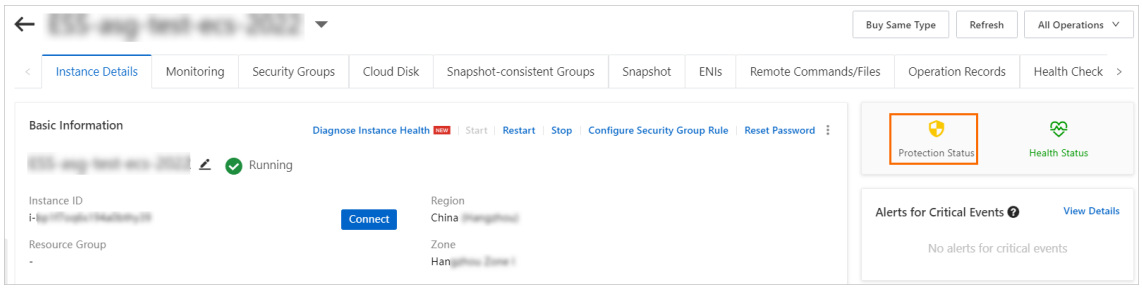
Check the security status of your ECS instance

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

1.
2.
3.
4. Use one of the following methods to check the security status of your ECS instance:
   - 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, vulnerability or security alerts in the instance are reported. You can click the icon to log on to the Security Center console and view the alert details.



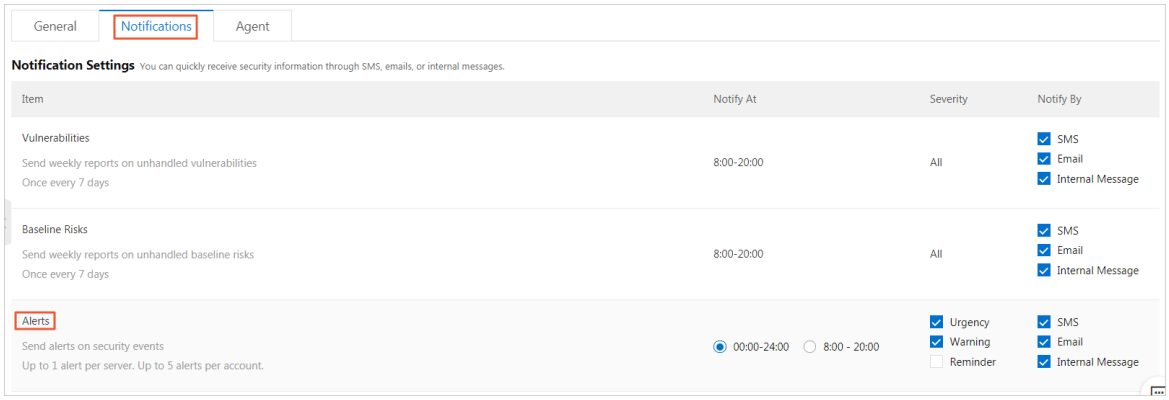
   - Method 2: Click the instance ID to go to the **Instance Details** page. On the **Instance Details** page, view the Alibaba Cloud Security icon. You can click the icon to log on to the Security Center console and view the alert details.



Set alert notifications

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

1.
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, click **Settings**. On the **Settings** page, click the **Notifications** tab.
4. In the **Alerts** section, specify a severity for alerts and configure the methods and time for sending alert notifications.



Note If you have upgraded Security Center to Security Center Advanced or Enterprise Edition, see Overview in *Security Center documentation*.

Related information

References

- Feature comparison among Basic, Advanced, and Enterprise editions
-
- RunInstances

7.Security FAQ

This topic provides answers to frequently asked questions about security of Elastic Compute Service (ECS) instances.

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 for the instance. Security groups are classified into basic and advanced security groups. For more information, see Overview.

Why must I select a security group when I create an ECS instance?

When you create an ECS instance, you must select a security group to divide your application environment into security domains and configure security group rules to properly isolate networks.

If you do not select security groups when you create an ECS instance, the instance is automatically asssigned to the default security group. We recommend that you move the instance from the default security group to a security group that you created.

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

If you have not created security groups before you create an ECS instance, you can select the default security group. The default security group allows traffic on common ports such as TCP port 22 and port 3389.

When I attempt to add an ECS instance to a security group, I am prompted that the maximum number of rules has been reached. Why?

You can use the following formula to calculate the maximum number of security group rules that can be associated with the primary elastic network interface (ENI) of an ECS instance: Maximum number of security groups to which the instance can belong × Maximum number of rules in each security group.

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

If I adjust the maximum number of security groups to which an ECS instance of the virtual private cloud (VPC) type can belong, does this adjustment take effect only on the security groups created after the number is adjusted?

No, the adjustment takes effect on all security groups to which ECS instances of the VPC type belong, regardless of when the security groups are created.

In what scenarios are the default security group rules used?

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 for the first time in the ECS console, you can select the default security group 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 rules are inbound rules that have a priority of 100 and grant access to all CIDR blocks (0.0.0.0/0). These rules allow inbound Internet Control Message Protocol (ICMP) traffic on all ports and inbound TCP traffic on SSH port 22 and Remote Desktop Protocol (RDP) port 3389. You can

also choose to allow inbound traffic over HTTP port 80 and HTTPS port 443. All outbound traffic is allowed.

- When you create a security group in the ECS console, the system creates default security group rules in the security group. These rules are inbound rules that grant access to all CIDR blocks (0.0.0.0/0). These rules allow inbound ICMP traffic on all ports, and inbound TCP traffic on SSH port 22, RDP port 3389, HTTP port 80, and HTTPS port 443.

How do ECS instances in different security groups communicate with each other over the internal network?

By default, instances in different security groups within the same account or different accounts are isolated from each other over the internal network. For more information about the use cases in which instances within different security groups can communicate with each other over the internal network, see Security group rules for instances within different security groups to communicate with each other and Configure interconnection of instances in the classic network.

How are ECS instances in the same security group isolated from each other over the internal network?

By default, ECS instances in the same basic security group can communicate with each other over all protocols and ports. You can modify the access control policies of basic security groups to isolate instances in the basic security groups. For more information, see Network isolation within a basic security group.

Why am I unable to access services after I configure a security group?

When traffic on a port is allowed by a security group rule in the ECS console, access to and from the port is not restricted but this does not indicate that this port is enabled. To allow Internet access to a port of an ECS instance, make sure that the following requirements are met:

- Traffic on the port is allowed by a security group rule.
- The software that listens to the port is in the running state and configured with a listening address of 0.0.0.0. You can run the **netstat -ano |findstr <Port number>** command to check whether the port is in the listening state.
- The internal firewall of the instance is disabled, or traffic on the port is allowed by the firewall.

How do I add an ENI to a security group?

You can change the security group of a primary ENI by changing the security group to which its bound ECS instance belongs. You can also change the security group to which an ENI belongs by modifing the attributes of a secondary ENI. For more information, see Modify an ENI.

In what scenarios must I add security group rules?

In the following scenarios, you must add security group rules to ensure that your ECS instance can be accessed:

- The security group to which your ECS instance belongs does not contain custom or default security group rules. Your ECS instance needs to access the Internet or another ECS instance in a different security group within the same region.
- The application deployed on your ECS instance 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, you have deployed the NGINX service and want to set TCP port 8000 as the listening port 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 information about other scenarios, see Security groups for different use casesConfiguration guide for ECS security groups.

What is the relationship between protocol types and port ranges in security group rules?

You must specify the communication port or port range when you add security group rules for a security group. The security group can determine whether to allow data to be forwarded to ECS instances based on the Allow or Forbid policy in the specified rule.

The following table describes the relationship between protocol types and port ranges in security group rules. For more information about commonly used ports, see Typical applications of commonly used ports.

Protocol type	Port range	Use scenario
All	-1/-1 is displayed, which indicates all ports. You cannot configure a port range for this protocol type.	It can be used in all trusted scenarios.
All ICMP (IPv4)	-1/-1 is displayed, which indicates all ports. You cannot configure a port range for this protocol type.	It can be used when you run the `ping` command to check the state of network connections between ECS instances.
All GRE	-1/-1 is displayed, which indicates all ports. You cannot configure a port range for this protocol type.	It can be used for VPN.
Custom TCP	A custom port range. Valid values of port numbers: 1 to 65535. You must use the *<start port>/<end port>* format to specify a port range or a single port. For example, 80/80 indicates port 80, and 1/22 indicates ports 1 to 22.	It can be used to allow or deny traffic on one or more successive ports.
Custom UDP	A custom port range. Valid values of port numbers: 1 to 65535. You must use the *<start port>/<end port>* format to specify a port range or a single port. For example, 80/80 indicates port 80, and 1/22 indicates ports 1 to 22.	It can be used to allow or deny traffic on one or more successive ports.

The following table describes the common scenarios in which TCP ports are used.

Use scenario	Protocol type	Port range	Description
Connection to a server	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 port used by an instance to accept connections.
	TELNET	23/23	It can be used to connect to an instance.
	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 port used by an instance to accept connections.
Website service	HTTP	80/80	It can be used when an instance serves as a website server or web application server.
	HTTPS	443/443	It can be used when an instance serves as a website server or web application server that supports HTTPS.
Database	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.
	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.

What is the relationship between the IP addresses and CIDR blocks specified as authorization objects of a security group rule?

IP addresses are individual IP addresses. Example: 192.168.0.100 or 2408:4321:180:1701:94c7:bc38:3bfa:. CIDR blocks are IP address ranges. Example: 192.168.0.0/24 or 2408:4321:180:1701:94c7:bc38:3bfa:***/128.

CIDR is an addressing scheme for the Internet that allows for IP addresses to be assigned in a more efficient manner than the traditional scheme based on classes A, B, and C. CIDR notation is used to denote IP addresses and IP ranges. It consists of an IP address and a forward slash followed by a decimal number that denotes how many bits are in the network prefix.

- Example 1: Convert a CIDR block into an IP address range

  For example, you can convert the 10.0.0.0/8 CIDR block into a 32-bit binary IP address of 00001010.00000000.00000000.00000000. In this CIDR block, /8 represents an 8-bit network ID. The first 8 bits of the 32-bit binary IP address are fixed, and the corresponding IP addresses are from 00001010.00000000.00000000.00000000 to 00001010.11111111.11111111.11111111. After you convert the preceding IP addresses into IP addresses in the decimal format, the 10.0.0.0/8 CIDR block indicates the IP addresses from 10.0.0.0 to 10.255.255.255 with a subnet mask of 255.0.0.0.

- Example 2: Convert an IP address range into a CIDR block

For example, you have a range of IP addresses from 192.168.0.0 to 192.168.31.255. You can convert the last two parts of the first and last IP addresses to binary numbers from 00000000.00000000 to 00011111.11111111. The first 19 (8 × 2 + 3) bits are fixed. After you convert the IP addresses to IP addresses in the CIDR format, the corresponding CIDR block is 192.168.0.0/19.

Why am I unable to access TCP port 25?

TCP port 25 is the default email service port. For security reasons, TCP port 25 is disabled for ECS instances by default. We recommend that you use port 465 to send emails. For information about more use cases of security groups, see Security groups for different use cases.

Why am I unable to access TCP port 80?

For more information about how to troubleshoot problems related to port 80, see Check whether TCP port 80 is available.

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

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

- You have accessed Data Management (DMS).
- You have migrated data by using Alibaba Cloud Data Transmission Service (DTS). The rules associated with the IP addresses of DTS servers are automatically added to your security group.

What happens if a security group rule is incorrectly configured?

If a security group rule is incorrectly configured, the ECS instances associated with this rule are unable to communicate with other devices over the internal network or the Internet.

- Linux ECS instances cannot be connected to by using SSH, and Windows ECS instances cannot be connected to 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 over HTTP or HTTPS.
- ECS instances associated with this rule cannot communicate with other ECS instances over the internal network.

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

No, the inbound and outbound rules in a security group are counted together. The total number of inbound and outbound rules in 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, you cannot adjust the maximum number of rules that can be added to a security group. 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. This allows each ENI of an ECS instance to be associated with up to 1,000 security group rules. This can meet the requirements in most scenarios.

If the maximum number of rules in each security group has been reached but you want 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 redundant rules exist, delete them. If no redundant rules exist, create more security groups.

If you have activated Cloud Firewall, you can configure access control policies on VPC firewalls to control traffic between VPCs. This way, fewer ECS security group rules are required. For more information about how to configure access control policies on VPC firewalls, see Create an access control policy for a VPC firewall.

How are my created security group rules prioritized?

The priority ranges 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 is applied. If an ECS instance belongs to multiple security groups, the security group rules of these security groups are applied to the instance in descending order of priority. Security group rules are applied based on the following principles:

- If two security group rules are different only in the authorization policy, the Forbid policy is applied and the Allow policy is not.
- If two security group rules are different only in priorities, the rule with a higher priority is applied.

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

You can check the records of harmful Internet information to view domain names or URLs that contain harmful information, penalty actions, reasons, and duration. When 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 View 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, provide your feedback and file an appeal. After Alibaba Cloud receives your feedback on the penalty, Alibaba Cloud checks the penalty and determines whether the penalty is appropriate and whether to uphold or rescind 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.