Alibaba Cloud
Elastic Compute Service

Security

Issue: 20200618
Legal disclaimer

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

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

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

3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.
5. By law, all the 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 contact Alibaba Cloud directly if you discover any errors in this document.
## Document conventions

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal disclaimer</td>
<td>I</td>
</tr>
<tr>
<td>Document conventions</td>
<td>I</td>
</tr>
<tr>
<td>1 Security groups</td>
<td>1</td>
</tr>
<tr>
<td>1.1 Security group overview</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Advanced security group</td>
<td>6</td>
</tr>
<tr>
<td>1.3 Scenarios for security groups</td>
<td>9</td>
</tr>
<tr>
<td>1.4 Typical applications of commonly used ports</td>
<td>25</td>
</tr>
<tr>
<td>1.5 Create a security group</td>
<td>28</td>
</tr>
<tr>
<td>1.6 Add security group rules</td>
<td>30</td>
</tr>
<tr>
<td>1.7 Add an ECS instances to a security group</td>
<td>37</td>
</tr>
<tr>
<td>1.8 Replace security groups of an ECS instance</td>
<td>38</td>
</tr>
<tr>
<td>1.9 Manage security group rules</td>
<td>40</td>
</tr>
<tr>
<td>1.9.1 Manage security group rules</td>
<td>40</td>
</tr>
<tr>
<td>1.9.2 Modify security group rules</td>
<td>44</td>
</tr>
<tr>
<td>1.9.3 Restore security group rules</td>
<td>44</td>
</tr>
<tr>
<td>1.9.4 Export security group rules</td>
<td>46</td>
</tr>
<tr>
<td>1.9.5 Import security group rules</td>
<td>47</td>
</tr>
<tr>
<td>1.9.6 Delete a security group rule</td>
<td>49</td>
</tr>
<tr>
<td>1.10 Manage security groups</td>
<td>50</td>
</tr>
<tr>
<td>1.10.1 View the security group list</td>
<td>50</td>
</tr>
<tr>
<td>1.10.2 Modify security group attributes</td>
<td>50</td>
</tr>
<tr>
<td>1.10.3 Clone a security group</td>
<td>51</td>
</tr>
<tr>
<td>1.10.4 Remove an instance from a security group</td>
<td>52</td>
</tr>
<tr>
<td>1.10.5 Manage security groups</td>
<td>55</td>
</tr>
<tr>
<td>2 Key pairs</td>
<td>57</td>
</tr>
<tr>
<td>2.1 SSH key pair overview</td>
<td>57</td>
</tr>
<tr>
<td>2.2 Use an SSH key pair</td>
<td>59</td>
</tr>
<tr>
<td>2.2.1 Create an SSH key pair</td>
<td>59</td>
</tr>
<tr>
<td>2.2.2 Import an SSH key pair</td>
<td>60</td>
</tr>
<tr>
<td>2.2.3 View public key information</td>
<td>62</td>
</tr>
<tr>
<td>2.2.4 Bind an SSH key pair to an instance</td>
<td>62</td>
</tr>
<tr>
<td>2.2.5 Add or replace an SSH key pair</td>
<td>64</td>
</tr>
<tr>
<td>2.2.6 Unbind an SSH key pair</td>
<td>64</td>
</tr>
<tr>
<td>2.2.7 Delete an SSH key pair</td>
<td>65</td>
</tr>
<tr>
<td>3 Implement access control by using RAM</td>
<td>67</td>
</tr>
<tr>
<td>4 Instance RAM roles</td>
<td>72</td>
</tr>
<tr>
<td>4.1 Overview</td>
<td>72</td>
</tr>
<tr>
<td>4.2 Bind an instance RAM role</td>
<td>73</td>
</tr>
<tr>
<td>4.3 Manage an instance RAM role</td>
<td>76</td>
</tr>
</tbody>
</table>
4.3.1 Replace an instance RAM role................................................................. 76
4.3.2 Unbind a RAM role..................................................................................77
4.3.3 Obtain a temporary authorization token................................................. 78
4.3.4 Authorize a RAM user to use an instance RAM role................................. 78
4.4 Use an instance RAM role by calling API operations.................................79

5 Basic security services.................................................................................84
6 Anti-DDoS Basic..........................................................................................87
7 Security FAQ...............................................................................................89
# 1 Security groups

## 1.1 Security group overview

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

### Characteristics

A security group can contain instances located in the same region. These instances have the same security requirements and trust each other. Security groups have the following characteristics:

- Each ECS instance must belong to at least one security group and can be added to multiple security groups at the same time.
- A security group can manage multiple ECS instances.
- By default, ECS instances in the same security group can communicate with each other over the internal network.
- By default, instances in different security groups cannot communicate with each other when no security group rule that allows access is configured.
- You can configure security group rules for only basic security groups to authorize mutual access between two security groups.
- Security groups are stateful. The maximum session timeout for a security group is 910 seconds. By default, a security group allows all directions of traffic in the same session. For example, if the request traffic during a session is allowed to flow in, the response traffic is also allowed to flow out.

### Security group types

Security groups are classified into basic security groups and advanced security groups. The following table lists the differences between the two types.
<table>
<thead>
<tr>
<th>Security group type</th>
<th>Security group rule type</th>
<th>Security group rule priority</th>
<th>Inbound rule policy</th>
<th>Outbound rule policy</th>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic security groups</td>
<td>Default rules</td>
<td>Depends on the security group template. *</td>
<td>Depends on the security group template. *</td>
<td>Allows all access requests.</td>
<td>Scenarios that require fine-grained network control, multiple ECS instance types, and moderate network connections</td>
</tr>
<tr>
<td>Custom rules</td>
<td></td>
<td></td>
<td>Supports the allow and deny policies. Allows you to add inbound rules as needed. **</td>
<td>Allows you to add outbound rules as needed. **</td>
<td>Scenarios that require fine-grained network control, multiple ECS instance types, and moderate network connections</td>
</tr>
<tr>
<td>Advanced security groups</td>
<td>Default rules</td>
<td>The value is 1 and cannot be modified.</td>
<td>Depends on the security group template. *</td>
<td>Depends on the security group template. *</td>
<td>Scenarios that have high requirements on O&amp;M efficiency, ECS instance types, and computing nodes</td>
</tr>
<tr>
<td>Custom rules</td>
<td></td>
<td></td>
<td>Supports the allow policy. Allows you to add inbound rules as needed. **</td>
<td>Allows you to add outbound rules as needed. **</td>
<td>Scenarios that have high requirements on O&amp;M efficiency, ECS instance types, and computing nodes</td>
</tr>
</tbody>
</table>

* When you create a security group in the ECS console, you can select Web Server Linux (allows traffic on port 80, 443, 22, and ICMP traffic), Web Server Windows (allows traffic on port 80, 443, 3389, and ICMP traffic), and a custom security group template that denies all access requests in the inbound direction.

** For more information about how to add custom security group rules, see Add security group rules.

This topic describes the concepts in basic security groups and best practices. For information about advanced security groups, see Advanced security group.

**Default security group**

After you create an ECS instance in a region through the ECS console, a default security group is created if no security group has been created under the current account in this
region. The default security group is a basic security group and has the same network type as the instance.

The default security group has the following security group rules:

- **Inbound**: By default, traffic on SSH port 22 and RDP port 3389, and ICMP traffic are allowed. You can also allow traffic on HTTP port 80 and HTTPS port 443. The rule priority is 110.
- **Outbound**: All accesses are allowed.

**Limits**

For information about the limits of security groups, see the Security group limits section in #unique_9.

**Workflow**

The following figure shows the workflow of a basic security group. For information about the workflow of an advanced security group, see Advanced security group.

**Security group rules**

Before a connection for data communication is established, the security group matches all the rules to decide whether to allow the access requests. A security group rule has the following attributes shown in the following table.
Different attributes of security group rules are required for different communication scenarios. For information about examples of rule configuration, see Scenarios for security groups. For example, when you log on to a Linux ECS instance by using an Xshell client, a security group detects an SSH request from the Internet or internal network. The security group then matches each inbound rule to check whether the IP address of the request sender exists, whether the rule priority is the highest, whether the inbound traffic is allowed, and whether port 22 is opened. If only one such rule exists, the connection for data communication is established. The following figure shows how the security group matches its rules to control the access request for a Linux ECS instance.

**Security group rule priority**

For security group rules with the same type, the rule with the highest priority takes effect. When an ECS instance is added to multiple security groups, the rules of those groups are matched in descending order of priority. The priority of a rule has the following values based on how the rule is added. A smaller value indicates a higher priority.

- For manually added rules, the values are between 1 and 100.
- For rules that are added by the system or created by using a template, the value is 110.
Note:
Advanced security groups do not support rule priority configuration.

In one security group or between different security groups, if two security group rules have the same protocol type, port range, authorization type, and authorization object, which rule takes effect depends on the priority and authorization policy settings of each rule.

- If a deny rule and an allow rule have the same priority, the deny rule takes precedence.
- If two rules have different priorities, the rule with a higher priority takes effect.

NIC types

For basic security groups, the NIC type settings of security group rules vary by network types.

- For classic networks, you can select Internal Network or Internet as the NIC type.
- For VPC, only Internal Network is available for the NIC type. However, the configured security group rules apply to both the internal network and the Internet at the same time. Internet network access to and from VPC-type ECS instances is mapped and forwarded by internal NICs. Therefore, the Internet NIC type is not available in VPC-type ECS instances. You can only set security group rules with the Internal NIC type.

Note:
Advanced security groups only support VPCs.

Best practices

When you use security groups, we recommend that you:

- Use security groups as a whitelist when only a few requests are allowed to access ECS instances of security groups. Set the rule policy of all security groups to deny access requests first, and then set the rule policy of these security groups one by one to allow access requests.
- Do not use a security group to manage all applications because isolation requirements are different at different layers.
- Add instances with the same security requirements to the same security group. Do not create a separate security group for each instance.

When you add security group rules, we recommend that you:
- Set simple security group rules. If you add an ECS instance to multiple security groups, hundreds of rules may apply to the instance. Any changes to these rules may cause connection errors.

- Follow the least privilege principle when you configure inbound or outbound rules for applications. For example, you:
  - Select a specific port (instead of a port range) to open, for example, port 80/80.
  - When you add security group rules, do not grant access permission to the 0.0.0.0/0 CIDR block unless necessary.

- Clone an active security group when you want to modify its rules in the production environment. You can modify the rules on the cloned security group to avoid impacts on online applications. For more information about how to clone a security group, see Clone a security group.

### 1.2 Advanced security group

Compared with basic security groups, advanced security groups can contain more ECS instances, elastic network interfaces (ENIs), and private IP addresses. Advanced security groups can be used only in virtual private clouds (VPCs) and are easy to use because of their simplified configuration policies for security group rules. They are suitable for scenarios that require for high O&M efficiency, multiple ECS instance types, and large-scale computing clusters.

#### Feature comparison

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Basic security group</th>
<th>Advanced security group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support all instance types</td>
<td>Yes</td>
<td>Support only IPv6-compatible instance types.</td>
</tr>
<tr>
<td>Support VPCs</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Support classic networks</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Set rule priorities</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Authorize other security groups to access the security group</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Feature</td>
<td>Basic security group</td>
<td>Advanced security group</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>----------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Manually set security group rules that allow access from other security groups</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Manually set Deny security group rules</td>
<td>Yes</td>
<td>No. Advanced security groups deny all access requests by default.</td>
</tr>
<tr>
<td>Bind ENIs to instances of any instance type</td>
<td>Yes. The instance must be VPC-network type.</td>
<td>ENIs can only be bound to instances of IPv6-compatible instance types.</td>
</tr>
<tr>
<td>Number of contained private IP addresses</td>
<td>2,000</td>
<td>65,536</td>
</tr>
<tr>
<td>Allow mutual access between ECS instances in the same security group by default</td>
<td>Yes</td>
<td>No. You need to add security group rules to allow mutual access between ECS instances in the same security group.</td>
</tr>
</tbody>
</table>

**Limits**

For the limits and quotas of advanced security groups, see the "Security group limits" section in #unique_9.

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

- The ECS instances must be created on or after May 30, 2019.
- The ECS instance types must support IPv6. For more information, see #unique_12.
- ECS instances and ENIs have the following requirements for their security group types:
  - An ECS instance cannot belong to both a basic security group and an advanced security group at the same time.
  - An ENI cannot belong to both a basic security group and an advanced security group at the same time.
  - An ENI can be bound to an ECS instance only when they belong to the same security group type.

**Console operations**

In the ECS console, you can perform the following operations to use advanced security groups:
1. Create an advanced security group.

When you create a security group, select **Advanced Security Group** for **Security Group Type**. For more information, see **Create a security group**.

2. Add security group rules.

An advanced security group is equivalent to an access whitelist. Only rules that allow access from other security groups can be added and authorization objects can only be CIDR blocks but not security groups. These rules have no priorities. For more information, see **Add security group rules**.

3. Add your ECS instances or ENIs to the advanced security group as needed.

   • For more information about how to add instances to a security group, see **Add an ECS instances to a security group**.

   ![Note]

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

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

     a. If the ENI is in a basic security group, modify the ENI to add it to the advanced security group,

           For more information, see #unique_15.

     b. Bind the ENI to an ECS instance.

           For more information, see #unique_16.

4. (Optional) Manage the advanced security group. For example, you can add a tag, modify the name and description of the advanced security group, and manage the ECS instances in the advanced security group. For more information, see

   • **View the security group list**
   • **Modify security group attributes**
   • **Clone a security group**
   • **Remove an instance from a security group**
   • **Manage security groups**
API operations

1. Call the #unique_21 operation and set SecurityGroupType to enterprise.

Before you create an advanced security group, make sure that a VPC and a VSwitch have been created.

2. Call the #unique_22 operation to add a rule which allows inbound traffic to the advanced security group. The authorization objects can only be CIDR blocks but not security groups.

An advanced security group is equivalent to a communication whitelist. Policy is set to accept by default. You can leave Priority blank and specify the communication protocol (IpProtocol), communication port range (PortRange), source communication port range (SourcePortRange) (optional), source CIDR block (SourceCidrip), and CIDR block of destination port (DestCidrip) (optional).

3. Call the #unique_23 operation to add an outbound rule to the advanced security group.

4. Call the #unique_24 operation to add a VPC-type ECS instance to the advanced security group.

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

   a. If the ENI is in a basic security group, call the #unique_25 operation to add the ENI to the advanced security group.

   b. Call the #unique_26 operation to attach the ENI that has been added to the advanced security group to an ECS instance.

6. (Optional) Call the #unique_27 operation to query the list of the security groups you have created in the current region.

1.3 Scenarios for security groups

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

Overview

You can configure security group rules for ECS instances in security groups to control instance access to the public network or internal networks. For information about how to create security groups and add security group rules, see Create a security group and Add security group rules. Common scenarios for security group rule configuration are listed as follows:
• **Scenario 1: Allow instances in the same region under the same account to communicate with each other through an internal network**

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

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

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

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

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

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

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

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

For security purposes, you can add security group rules to disallow your instance from accessing specified public IP addresses.

• **Scenario 6: Allow public network access to your instance**

You can connect to your ECS instance from the public network.

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

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

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

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

---

**Note:**

For information about commonly used ports, see *Typical applications of commonly used ports.*
Scenario 1: Allow instances in the same region under the same account to communicate with each other through an internal network

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

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

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

**Note:**

For ECS instances in the same VPC, you can add security group rules to allow them to communicate with each other through an internal network. For ECS instances in different VPCs, you can use Cloud Enterprise Network (CEN) to allow them to communicate with each other, regardless of whether the instances belong to the same account or are located within the same region. For more information, see CEN document #unique_37.

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

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

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

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

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

<table>
<thead>
<tr>
<th>NIC type</th>
<th>Rule direction</th>
<th>Authorization policy</th>
<th>Protocol</th>
<th>Port range</th>
<th>Authorization type</th>
<th>Authorization object</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>Inbound</td>
<td>Allow</td>
<td>Select an applicable protocol.</td>
<td>Specify a port range.</td>
<td>Security group under another account</td>
<td>The ID of the security group Group B. The account ID of User B must be entered in Account ID.</td>
<td>1</td>
</tr>
</tbody>
</table>
• Add the security group rule described in the following table to Group B.

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

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

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

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

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

### Windows instance

<table>
<thead>
<tr>
<th>Network type</th>
<th>NIC type</th>
<th>Rule direction</th>
<th>Authorization policy</th>
<th>Protocol</th>
<th>Port range</th>
<th>Authorization type</th>
<th>Authorization object</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC</td>
<td>Not required</td>
<td>Inbound</td>
<td>Allow</td>
<td>RDP (3389)</td>
<td>3389/3389</td>
<td>CIDR block</td>
<td>The public CIDR block that you allow to connect to your instance. Example: 1.2.3.4/32 or 10.0.0.0/8.</td>
</tr>
<tr>
<td>Classic network</td>
<td>Public</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Scenario 4: Allow your instance to access only specified public IP addresses**

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

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

<table>
<thead>
<tr>
<th>Network type</th>
<th>NIC type</th>
<th>Rule direction</th>
<th>Authorization policy</th>
<th>Protocol</th>
<th>Port range</th>
<th>Authorization type</th>
<th>Authorization object</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC</td>
<td>Not required</td>
<td>Outbound</td>
<td>Deny</td>
<td>All</td>
<td>-1/-1</td>
<td>CIDR block</td>
<td>0.0.0.0/0</td>
<td>2</td>
</tr>
<tr>
<td>Classic network</td>
<td>Public</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Network type</th>
<th>NIC type</th>
<th>Rule direction</th>
<th>Authorization policy</th>
<th>Protocol</th>
<th>Port range</th>
<th>Authorization type</th>
<th>Authorization object</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC</td>
<td>Not required</td>
<td>Outbound</td>
<td>Allow</td>
<td>Select an applicable protocol</td>
<td>Specify a port range.</td>
<td>CIDR block</td>
<td>The public CIDR block that you allow your instance to access. Example: 1.2.3.4/32 or 10.0.0.0/8</td>
<td>1</td>
</tr>
<tr>
<td>Classic network</td>
<td>Public</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
After adding the security group rules, connect to your instance and run the ping or telnet command to check whether the security group rules have taken effect. If your instance can access only the allowed IP addresses, the security group rules have taken effect.

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

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

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

**Scenario 6: Allow public network access to your instance**

To allow public network access to your instance, add the security group rule described in the following table.
<table>
<thead>
<tr>
<th>Network type</th>
<th>NIC type</th>
<th>Rule direction</th>
<th>Authorization policy</th>
<th>Protocol</th>
<th>Port range</th>
<th>Authorization type</th>
<th>Authorization object</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC</td>
<td>Not required</td>
<td>Inbound</td>
<td>Allow</td>
<td>Windows: RDP (3389)</td>
<td>3389/3389.</td>
<td>CIDR block</td>
<td>To allow all public IP addresses to connect to your instance, enter 0.0.0.0/0.0. To allow only specified public IP addresses to connect to your instance, follow the instructions in &quot;Scenario 3: Allow only specified IP addresses access to your instance.&quot;</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Linux: SSH (22)</td>
<td>22/22.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Custom TCP</td>
<td>Specify a port range, such as 8080/8080.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network type</td>
<td>NIC type</td>
<td>Rule direction</td>
<td>Authorization policy</td>
<td>Protocol</td>
<td>Port range</td>
<td>Authorization type</td>
<td>Authorization object</td>
<td>Priority</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------</td>
<td>----------------</td>
<td>----------------------</td>
<td>----------</td>
<td>------------------</td>
<td>--------------------</td>
<td>---------------------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| Classic network     | Public   | Inbound        | Allow                | Windows: RDP (3389) | 3389/3389.       | CIDR block          | To allow all public IP addresses to connect to your instance, enter 0.0.0.0/0.0. To allow only specified public IP addresses to connect to your instance, follow the instructions in "Scenario 3: Allow only specified IP addresses access to your instance."
|                     |          |                |                      | Linux: SSH (22)    | 22/22.           |                    |                     | 1        |
|                     |          |                |                      | Custom TCP         | Specify a port range, such as 8080/8080. |                    |                     |          |

For information about how to customize ports for remote access, see #unique_38.
Scenario 7: Allow an ECS instance that resides in a security group belonging to another account in the same internal network to connect to your ECS instance

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

- To allow an internal IP address of an ECS instance in a security group under another account to connect to your instance, add the security group rule described in the following table. For ECS instances in VPCs, ensure that the instances under the two accounts can communicate with each other through Cloud Enterprise Network (CEN) before you add the security group rule. For more information, see CEN document #unique_37.

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

- To allow all ECS instances in a security group under another account to connect to your instance, add the security group rule described in the following table. For ECS instances in VPCs, ensure that the instances under the two accounts can communicate with each other.
other through Cloud Enterprise Network (CEN) before you add the security group rule. For more information, see CEN document #unique_37.

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

Issue: 20200618
### Scenario 8: Allow public network access to your ECS instance over HTTP or HTTPS

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

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

<table>
<thead>
<tr>
<th>Network type</th>
<th>NIC type</th>
<th>Rule direction</th>
<th>Authorization policy</th>
<th>Protocol</th>
<th>Port range</th>
<th>Authorization type</th>
<th>Authorization object</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC</td>
<td>Not required</td>
<td>Inbound</td>
<td>Allow</td>
<td>HTTP (80)</td>
<td>80/80.</td>
<td>CIDR block</td>
<td>0.0.0.0/0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HTTPS (443)</td>
<td>443/443</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network type</td>
<td>NIC type</td>
<td>Rule direction</td>
<td>Authorization policy</td>
<td>Protocol</td>
<td>Port range</td>
<td>Authorization type</td>
<td>Authorization object</td>
<td>Priority</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>----------------</td>
<td>---------------------</td>
<td>----------</td>
<td>-----------</td>
<td>-------------------</td>
<td>---------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Classic network</td>
<td>Public</td>
<td>Inbound</td>
<td>Allow</td>
<td>HTTP (80)</td>
<td>80/80.</td>
<td>CIDR block</td>
<td>0.0.0.0/0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HTTPS (443)</td>
<td>443/443</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Custom TCP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To allow specified public IP addresses to access your website, add the security group rule described in the following table.

<table>
<thead>
<tr>
<th>Network type</th>
<th>NIC type</th>
<th>Rule direction</th>
<th>Authorization policy</th>
<th>Protocol</th>
<th>Port range</th>
<th>Authorization type</th>
<th>Authorization object</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC</td>
<td>Not required</td>
<td>Inbound</td>
<td>Allow</td>
<td>HTTP (80)</td>
<td>80/80.</td>
<td>CIDR block</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HTTPS (443)</td>
<td>443/443</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Custom TCP</td>
<td></td>
<td>Specify one or more public IP addresses that are allowed to access your website. Example: 1.2.3.4/32 or 10.0.0.0/8.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Security groups

<table>
<thead>
<tr>
<th>Network type</th>
<th>NIC type</th>
<th>Rule direction</th>
<th>Authorization policy</th>
<th>Protocol</th>
<th>Port range</th>
<th>Authorization type</th>
<th>Authorization object</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classic network</td>
<td>Public</td>
<td>Inbound</td>
<td>Allow</td>
<td>HTTP (80)</td>
<td>80/80</td>
<td>CIDR block</td>
<td>Specify one or more public IP addresses that are allowed to access your website. Example: 1.2.3.4/32 or 10.0.0.0/8.</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HTTPS (443)</td>
<td>443/443</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Custom TCP</td>
<td></td>
<td></td>
<td>Specify a port range, such as 8080/8080.</td>
<td></td>
</tr>
</tbody>
</table>

#### Note:
- If you cannot access your instance by using http://public IP address, check whether TCP port 80 is working properly.
- Port 80 is the default HTTP port. To use another port (for example, port 8080) for HTTP, you must modify the listening port settings in the configuration file of the Web server.

### 1.4 Typical applications of commonly used ports

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

**Commonly used ports**

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>FTP</td>
<td>A port opened to the FTP service. The port is used to upload and download files.</td>
</tr>
<tr>
<td>Port</td>
<td>Service</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>22</td>
<td>SSH</td>
<td>SSH port, which is used to connect to a Linux instance by using a password in the command line mode.</td>
</tr>
<tr>
<td>23</td>
<td>Telnet</td>
<td>Telnet port, which is used to telnet to the ECS instance.</td>
</tr>
<tr>
<td>25</td>
<td>SMTP</td>
<td>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.</td>
</tr>
<tr>
<td>80</td>
<td>HTTP</td>
<td>This port provides access to HTTP services, such as IIS, Apache, and Nginx. For more information, see Verify if TCP port 80 works properly.</td>
</tr>
<tr>
<td>110</td>
<td>POP3</td>
<td>This port is used for the POP3 protocol to send and receive emails.</td>
</tr>
<tr>
<td>143</td>
<td>IMAP</td>
<td>This port is used for the IMAP protocol to receive emails.</td>
</tr>
<tr>
<td>443</td>
<td>HTTPS</td>
<td>This port is used to provide access to the HTTPS service. HTTPS is a protocol that provides encryption and transmission through secure ports.</td>
</tr>
<tr>
<td>1433</td>
<td>SQL Server</td>
<td>The TCP port of the SQL Server. This port is used for the SQL Server to provide external services.</td>
</tr>
<tr>
<td>1434</td>
<td>SQL Server</td>
<td>The UDP port of the SQL Server. This port is used to return which TCP/IP port the SQL Server uses.</td>
</tr>
<tr>
<td>1521</td>
<td>Oracle</td>
<td>An Oracle communication port. This port needs to be enabled when Oracle SQL is deployed on the ECS instance.</td>
</tr>
<tr>
<td>3306</td>
<td>MySQL</td>
<td>The port through which the MySQL database provides external services.</td>
</tr>
<tr>
<td>3389</td>
<td>Windows Server Remote Desktop Services</td>
<td>This port is used to connect to a Windows instance.</td>
</tr>
</tbody>
</table>
### Port 8080

**Service**: Proxy port  
**Description**: 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 137, 138, and 139

**Service**: NetBIOS protocol  
**Description**:  
- 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

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Network type</th>
<th>NIC</th>
<th>Rule direction</th>
<th>Authorization policy</th>
<th>Protocol type</th>
<th>Port range</th>
<th>Authorization type</th>
<th>Authorization object</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote access to Linux instances through SSH</td>
<td>VPC</td>
<td>Configuration is not required.</td>
<td>Inbound</td>
<td>Allow</td>
<td>SSH</td>
<td>22/22</td>
<td>Address field access</td>
<td>0.0.0/0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Classic network</td>
<td>Internet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote access to Windows instances through RDP</td>
<td>VPC</td>
<td>Configuration is not required.</td>
<td>Inbound</td>
<td>Allow</td>
<td>RDP</td>
<td>3389/3389</td>
<td>Address field access</td>
<td>0.0.0/0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Classic network</td>
<td>Internet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ping ECS instances through the Internet</td>
<td>VPC</td>
<td>Configuration is not required.</td>
<td>Inbound</td>
<td>Allow</td>
<td>ICMP</td>
<td>-1/-1</td>
<td>Address field access or security group access</td>
<td>Set this parameter according to the authorization type</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Classic network</td>
<td>Internet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 1.5 Create a security group

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

**Background**

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

---

```
<table>
<thead>
<tr>
<th>Scenario</th>
<th>Network type</th>
<th>NIC</th>
<th>Rule</th>
<th>Authorization policy</th>
<th>Protocol</th>
<th>Port range</th>
<th>Authorization type</th>
<th>Authorization object</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use an ECS instance as a Web server.</td>
<td>VPC</td>
<td>Configuration is not required.</td>
<td>Inbound allow</td>
<td>HTTP (80)</td>
<td>80/80</td>
<td>Address field access</td>
<td>0.0.0/0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Upload or download files through FTP.</td>
<td>VPC</td>
<td>Configuration is not required.</td>
<td>Inbound allow</td>
<td>Custom TCP</td>
<td>20/21</td>
<td>Address field access</td>
<td>0.0.0/0</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

**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.
```
Prerequisites

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

Procedure

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

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

     | Template     | Description                                                                 | Scenario                                                                 |
     |--------------|-----------------------------------------------------------------------------|--------------------------------------------------------------------------|
     | Web Server   | Inbound traffic to TCP port 80, TCP port 443, TCP port 22, and for the ICMP  | A Web server must be deployed on the Linux instances in the security group.|
     | Linux        | protocol is allowed by default.                                              |                                                                          |
     | Web Server   | By default, inbound traffic to TCP port 80, TCP port 443, TCP port 3389,    | A Web server must be deployed on the Windows instances in the security group.|
     | Windows      | and for the ICMP protocol is allowed.                                       |                                                                          |
     | Customize    | After creating a security group, you need to **add security group rules**.   | Not for Web server                                                       |

   - **Security Group Name**: specify a valid security group name.
   - **Description**: the description of the security group for later management.
   - **Security Group Type**:
     - Basic Security Group: can be used in scenarios that have higher requirements for refined network control, and prefer multiple ECS instance types and moderate network connections. For more information, see Security group overview.
     - Advanced Security Group: can be used in scenarios that have higher requirements for O&M efficiency, ECS instance specifications, and computing nodes. For more information, see Advanced security group.

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

- **Network Type:**
  - To create a classic network-type security group, select **Classic**.
  - To create a VPC-type security group, select **VPC** and then a specific VPC.

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

3. Click **OK**.

**Results**

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

**Related APIs**

You can call #unique_21 to create a security group.

**Next operations**

- You can add security group rules to allow or deny access to the public or internal networks from ECS instances in security groups.
- An ECS instance must belong to one or more security groups. You can add an instance to one or more security groups based on your business needs.

**1.6 Add security group rules**

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

**Background**

Security groups control access to or from public or internal networks. For security purposes, most security groups use deny policies for inbound traffic. If you use the default security group, or you select a Web Server Linux template or a Web Server Windows template when creating a security group, security group rules are automatically added to some communication ports. For more information, see Security group overview. This topic applies to the following scenarios:
• When your application needs to communicate with the network outside the security group, but the request stays in the wait state, you need to add security group rules first.
• When you discover malicious attacks from some request sources during the application operation, add deny security group rules to implement isolation.

Notes
• Security group rules depend on NIC types.
  - Security group rules for classic networks distinguish between internal and public NICs.
  - Security group rules for VPC networks do not distinguish between internal and public NICs.

  Public network access to and from VPC-type ECS instances is mapped and forwarded by internal NICs. You cannot see public NICs in ECS instances, and can add only internal security group rules. However, security group rules apply to both the internal and public network.
• Before you add any rules to a security group, all outbound traffic is allowed and all inbound traffic is denied.
• The total number of inbound and outbound rules for each security group cannot exceed 100.
• You cannot configure the Priority parameter, set Authorization Type to Security Group, or set Action to Forbid for advanced security group rules. For more information, see Advanced security group.

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

Procedure
1. Log on to the ECS console.
2. In the left-side navigation pane, choose Network & Security > Security Groups.
3. In the top navigation bar, select a region.
4. Locate the security group to which you want to add authorization rules. Click Add Rules in the Actions column.
5. On the **Security Group Rules** page, select one of the following methods to add rules:

- **1. Quick Rule Creation.** It can be used when ICMP and GRE are not required and you can select multiple ports. On the **Quick Rule Creation** page, the following application ports are provided: SSH 22, Telnet 23, HTTP 80, HTTPS 443, MS SQL 1433, Oracle 1521,
MySQL 3306, RDP 3389, PostgreSQL 5432, and Redis 6379. You can select one or more ports, or customize TCP or UDP ports.

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

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

  a. Click Add Security Group Rule.
  b. Select NIC (only for security group rules of the classic network).

    - **Internal Network**: You do not want your ECS instance to access the public network, or public network access is not required.
    - **Internet**: Your ECS instance needs to access the public network, or provide applications to the public network.

  c. Select Rule Direction.

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

  d. Select Action.

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

  e. Select Protocol Type and Port Range.

The port range is based on the protocol type. The following table describes the relationship between **Protocol Type** and **Port Range**. For more information about common ports, see Typical applications of commonly used ports.

<table>
<thead>
<tr>
<th>Protocol type</th>
<th>Port range</th>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>-1/-1</td>
<td>-1/-1 is displayed, indicating all ports. You cannot set a port range for this protocol type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>It is used in all trusted scenarios.</td>
</tr>
</tbody>
</table>

**Note:**

- Internal Network: You do not want your ECS instance to access the public network, or public network access is not required.
- Internet: Your ECS instance needs to access the public network, or provide applications to the public network.
- Outbound: Your ECS instances access other ECS instances in the internal network or resources in the public network.
- Inbound: Other ECS instances in the internal network or resources in the public network access your ECS instances.
- Allow: allows access requests on the port.
- Forbid: Data packets are discarded and no messages are returned. If two security groups have the same rules but different authorization policies, **Forbid** policies are used while **Allow** policies are ignored.
<table>
<thead>
<tr>
<th>Protocol type</th>
<th>Port range</th>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>All ICMP (IPv4)</td>
<td>-1/-1</td>
<td>It is used when you run the ping command to check network connection status between instances.</td>
</tr>
<tr>
<td>All GRE</td>
<td>-1/-1</td>
<td>It is used for VPN.</td>
</tr>
<tr>
<td>Customized TCP</td>
<td></td>
<td>Customize a port range. Valid values: 1 to 65535.</td>
</tr>
<tr>
<td>Customized UDP</td>
<td></td>
<td>It can be used to allow or deny one or several successive ports.</td>
</tr>
<tr>
<td>SSH</td>
<td>22/22</td>
<td>It is used to connect to a Linux instance remotely. After connecting to the ECS instance, you can modify the port number. For more information, see #unique_38.</td>
</tr>
<tr>
<td>Telnet</td>
<td>23/23</td>
<td>It is used to connect to an instance remotely.</td>
</tr>
<tr>
<td>HTTP</td>
<td>80/80</td>
<td>It is used when an instance serves as a website or Web application server.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443/443</td>
<td>It is used when an instance serves as a website or Web application server that supports the HTTPS protocol.</td>
</tr>
<tr>
<td>MS SQL</td>
<td>1433/1433</td>
<td>It is used when an instance serves as an MS SQL server.</td>
</tr>
<tr>
<td>Oracle</td>
<td>1521/1521</td>
<td>It is used when an instance serves as an Oracle SQL server.</td>
</tr>
<tr>
<td>MySQL</td>
<td>3306/3306</td>
<td>It is used when an instance serves as a MySQL server.</td>
</tr>
<tr>
<td>Protocol type</td>
<td>Port range</td>
<td>Scenario</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RDP</td>
<td>3389/3389</td>
<td>It is used to connect to a Windows instance remotely. After connecting to the ECS instance, you can modify the port number. For more information, see #unique_38.</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>5432/5432</td>
<td>It is used when an instance serves as a PostgreSQL server.</td>
</tr>
<tr>
<td>Redis</td>
<td>6379/6379</td>
<td>It is used when an instance serves as a Redis server.</td>
</tr>
</tbody>
</table>

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

f. Select **Authorization Type** and **Authorization Objects**.

The authorized IP address is based on the authorization type.

<table>
<thead>
<tr>
<th>Authorization type</th>
<th>Authorization object</th>
</tr>
</thead>
</table>
| IPv4 CIDR block    | - Enter an IP address or CIDR block, in the format of 12.1.1.1 or 13.1.1.1/25.  
                      - You can enter up to 10 authorization objects at a time. Separate multiple objects with commas (,).  
                      - Specifying 0.0.0.0/0 will allow or deny all IP addresses, based on the authorization policy. Use caution when specifying 0.0.0.0/0. |
### Security groups

<table>
<thead>
<tr>
<th>Authorization type</th>
<th>Authorization object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security group</td>
<td>This authorization type is only valid for the internal network. Authorize the instances in a security group for your account or another account to access the instances in this security group. <strong>CIDR Block</strong> must be selected for public network access.</td>
</tr>
</tbody>
</table>

- Authorize Current Account: Select another security group ID for your account. For a security group of the VPC type, the destination must be a security group in the same VPC.
- Authorize Other Accounts: Enter a security group ID and another account ID. Choose **Account Management > Security Settings** to view your account ID.

**Note:**
For advanced security group rules, you cannot set Authorization Type to Security Group.

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

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

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

**h.** Click **OK**.

### Results

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

### Related APIs

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

Next operations

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

1.7 Add an ECS instances to a security group

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

Background

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

Prerequisites

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

Procedure

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

1. On the Instances page, locate the ECS instance to be added to the security group. Click Manage in the Actions column.
2. Click Security Groups in the left-side navigation pane.
3. Click Add to Security Group.
4. Select the security group. If you want to add the ECS instance to multiple security groups, select a security group and then click Join multiple security groups. A selection box appears that shows the selected security groups.
5. Click OK.
After you add an ECS instance to a security group, the security group rules automatically apply to the ECS instance.

**Related APIs**

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

**Related operations**

- You can query security groups if you want to view all security groups you have created in a region.
- You can remove an instance from a security group if you do not want an ECS instance to belong to one or more security groups. The removed ECS instance will be isolated from other ECS instances in the security group. We recommend that you perform a full test before the remove operation to ensure that the business can run properly after the removal of the ECS instance.
- You can delete one or more security groups if you no longer need them. After you delete a security group, its rules will also be deleted.

### 1.8 Replace security groups of an ECS instance

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

**Prerequisites**

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

**Context**

You can replace security groups in the following scenarios:

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

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

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images > Instances**.
3. In the top navigation bar, select a region.
4. On the **Instances** page, take one of the following steps based on the number of instances that you need to replace security groups for:
   - Replace security groups for a single instance
     Find the target instance and choose **More > Network and Security Group > Replace** in the **Actions** column.
   - Replace security groups for multiple instances
     Select the target instances and choose **More > Network and Security Group > Replace** in the lower part of the instance list.
5. In the **Replace Security Group for Instances** dialog box, select new security groups to replace the original security groups.
   a) **Security Group Type**: Select **Basic Security Group** or **Advanced Security Group**.
   b) **Select Security Groups**: Select a security group from the drop-down list.

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

6. Click **Replace Security Group**.

Result

After the operations are complete, security groups are replaced.

Related topics

#unique_47
1.9 Manage security group rules

1.9.1 Manage security group rules

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

Query security group rules

Prerequisites

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

Procedure

1. Find the target security group, and then click Add Rules in the Actions column.
2. Click a rule direction to query the corresponding security group rules.
   - If you need to query security group rules for a VPC, select Ingress or Outbound.
   - If you need to query security group rules for a classic network, select Internal Network Ingress, Internal Network Egress, Internet Ingress, or Internet Egress.

You can also call DescribeSecurityGroupAttribute to query security group rules.

Modify security group rules

Context

If security group rules do not limit access to certain ports, serious security risks may occur.

You can modify inappropriate rules to ensure the security of your ECS instances.

Prerequisites

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

Procedure

1. On the Security Groups page, find the target security group, and then click Add Rules in the Actions column.
2. Click a rule direction of the security group.
   - If you need to modify security group rules for a VPC, select Ingress or Outbound.
   - If you need to modify the security group rules for a classic network, select Internal Network Ingress, Internal Network Egress, Internet Ingress, or Internet Egress.
3. Find the target security group rule, and click **Modify** in the **Actions** column. For information about how to configure security group rules, see [Add security group rules](#). For information about how to use security group rules, see [Typical applications of security group rules](#).

**Restore security group rules**

**Context**

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

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

- **Partial restoration**: The system adds the rules that are only in the target security group to the source security group and ignores the rules that are only in the source security group.

**Limits**

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

**Prerequisites**

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

**Procedure**

1. Find the security group whose rules you want to restore (this security group serves as the source security group), and then click **Restore Rules** in the **Actions** column.
2. In the **Restore rules** dialog box, perform the following operations as needed:

   a. Select the **Target Security Group**, which must have different rules from the source security group.

   b. Select a **Method**.
      
      - If you want the source security group to have the same rules as the target security group, select **Completely Restore**.
      
      - If you want to add the rules that only exist in the target security group to the source security group, select **Partially Restore**.

   c. Preview the restoration result.
      
      - The rules highlighted in green only exist in the target security group. These rules are added to the source security group regardless of whether you select **Completely Restore** or **Partially Restore**.
      
      - The rules highlighted in red do not exist in the target security group. If you select **Completely Restore**, these rules are deleted from the source security group. If you select **Partially Restore**, these rules are retained in the source security group.

   d. Click **OK**.

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

**Export security group rules**

1. On the **Security Groups** page, find the target security group, and then click **Add Rules** in the **Actions** column.

2. Click **Export Rules** to download and save the security group rules to a local JSON file.

**Note:**

The JSON file name uses the following format:

```
ecs_${region_id}_${groupID}.json
```

If `regionID` is `cn-qingdao` and `groupID` is `sg-123`, then the name of the exported JSON file is `ecs_cn-qingdao_sg-123.json`. 
Import security group rules

1. In the upper-left corner, select the target region.

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

2. On the Security Groups page, find the target security group, and then click Add Rules in the Actions column.

3. Click Import Rules.

4. Select the target JSON file. You can preview the rules in the file.

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

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

5. Click Start.

6. View the import result, and then click Finish and close.

Delete security group rules

1. Find the target security group, and then click the Add Rules in the Actions column.

2. Click a rule direction of the security group.

   • If you need to delete security group rules for a VPC, select Ingress or Outbound.
   • If you need to delete the security group rules for a classic network, select Internal Network Ingress, Internal Network Egress, Internet Ingress, or Internet Egress.

3. Find the target security group rule, and then click Delete in the Actions column.

4. In the Delete Security Group Rule dialog box, click OK.

   You can also call RevokeSecurityGroup to delete an ingress security group rule or call RevokeSecurityGroupEgress to delete an outbound security group rule.
1.9.2 Modify security group rules

Improper settings of security group rules may impose serious security risks. You can modify improper rules in a security group.

Prerequisites

You have created a security group, and added security group rules in that security group.

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose Network & Security > Security Groups.
3. In the top navigation bar, select a region.
4. On the Security Groups page, find the target security group, and then click Add Rules in the Actions column.
5. Click the traffic direction to which a security group rule applies.
   • If you need to modify security group rules for a VPC, select Inbound or Outbound.
   • If you need to modify security group rules for the classic network, select Internal Network Inbound, Internal Network Outbound, Internet Inbound or Internet Outbound.
6. Find the target security group rule, and click Modify in the Actions column. For how to configure security group rules, see Add security group rules. For use cases of security group rules, see Typical applications of security group rules.

API operations

You can call ModifySecurityGroupRule to modify an inbound rule.

What to do next

- If you want to view specific inbound and outbound rules, you can query security group rules.
- If you need to back up security group rules, you can export security group rules.
- If you want to create or restore security group rules quickly, you can import security group rules.
- If you no longer need a security group rule, you can delete security group rules.

1.9.3 Restore security group rules

Restoring security group rules indicates the process of completely or partially restoring the rules in the original security group to those of a target security group. Specifically:
Completely restoring means moving the rules that do not exist in the target security group from the original security group, and adding the rules that only exist in the target security group to the original security group. After restoration, rules in the original security group are identical with those in the target security group.

Partially restoring means adding the rules that only exist in the target security group to the original security group and ignoring the rules that only exist in the original group.

Limits

Restoring security group rules has the following limits:

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

Scenario

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

Prerequisite

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

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, select Networks and Security > Security Groups.
3. Select the target region.
4. Find the security group you want to restore rules for as the original security group and then, in the Actions column, click Restore Rules.
5. In the **Restore Rules** dialog box, follow these steps:

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

   b. Select a restore **Method**:
      - If you want the original security group to have the same rules as the target security group, select **Completely Restore**.
      - If you want to add the rules that only exist in the target security group to the original security group, select **Partially Restore**.

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

   d. Click **OK**.

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

### 1.9.4 Export security group rules

Security group rules can be exported to a JSON file for local backup.

**Procedure**

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

![Image showing Export Rules](image)

**Note:**
The JSON file name takes the following format:

```
ecs_${region_id}_${groupID}.json
```

If regionID is cn-qingdao, and groupID is sg-123, then the exported JSON file name is `ecs_cn-qingdao_sg-123.json`.

### 1.9.5 Import security group rules

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

**Procedure**

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

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

4. On the **Security Groups** list page, find the target security group, and then click **Add Rules** in the **Actions** column.

5. Click **Import Rules**.

![Image showing Import Rules](image)
6. Select the target JSON file. You can preview the rules in the file.

The Preview Rules part displays the following information:

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

**Note:**

Up to 100 security group rules can be imported, so the remaining rules will not be imported. The imported new rules do not overwrite the existing rules.
7. Click **Start** to import the rules.

![Import Security Group Rule](Image)

**Select a file**
Make sure that the number of rules that you need to import is less than 100 because the system uses the duplicate import method to add these rules.

![Select...](Image)

**Preview Rules**
1 out of 1 rules will be imported.

<table>
<thead>
<tr>
<th>Check</th>
<th>Network Type</th>
<th>Direction</th>
<th>Action</th>
<th>Protocol Type</th>
<th>Port Range</th>
<th>Authorization Type</th>
<th>Authorization Objects</th>
<th>Description</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>Internal Network</td>
<td>Ingress</td>
<td>Allow</td>
<td>Customized TCP</td>
<td>3389/3389</td>
<td>CIDR Block</td>
<td>0.0.0.0/0</td>
<td>-</td>
<td>1</td>
</tr>
</tbody>
</table>

- Import All Rules (rule priorities higher than 100 will be set to 100)

![Start](Image) ![Close](Image)

8. View the import results, and then click **Finish and close**.

![Import Security Group Rule](Image)

**Select a file**
Make sure that the number of rules that you need to import is less than 100 because the system uses the duplicate import method to add these rules.

![Select...](Image)

**Rules Imported**
1 rules have been imported.

<table>
<thead>
<tr>
<th>Result</th>
<th>Network Type</th>
<th>Direction</th>
<th>Action</th>
<th>Protocol Type</th>
<th>Port Range</th>
<th>Authorization Type</th>
<th>Authorization Objects</th>
<th>Description</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>Internal Network</td>
<td>Ingress</td>
<td>Allow</td>
<td>Customized TCP</td>
<td>3389/3389</td>
<td>CIDR Block</td>
<td>0.0.0.0/0</td>
<td>-</td>
<td>1</td>
</tr>
</tbody>
</table>

![Finish and Close](Image)

1.9.6 **Delete a security group rule**

You can delete security group rules that you no longer require. To do so, follow these steps:

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

3. Select the target region.

4. Find the security group where you want to delete rules and then, in the **Actions** column, click **Add Rules**.

5. On the security group management page, select the rule direction and find the rule you want to delete.
   - If the security group is for classic network, the rule directions are **Internet Inbound**, **Internet Outbound**, **Intranet Inbound**, and **Intranet Outbound**.
   - If the security group is for VPC, the rule directions are **Inbound** and **Outbound**.

6. In the **Actions** column, click **Delete**.

7. On **Delete Security Group Rule** dialog box, read and confirm the information displayed, and then click **OK**.

### 1.10 Manage security groups

#### 1.10.1 View the security group list

You can view security groups in the ECS console. To do so, follow these steps:

1. Log on to the **ECS console**.
2. In the left-side navigation pane, click **Networks and Security > Security Groups**.
3. Select the target region. A list of all security groups in the specified region is displayed.
4. Select the target VPC name or enter a VPC ID in the search box to search for security groups under a VPC.

#### 1.10.2 Modify security group attributes

You can modify the name and description of a security group at any time. To do so, follow these steps:

1. Log on to the **ECS console**.
2. In the left-side navigation pane, click **Networks and Security > Security Groups**.
3. Select the target region.
4. Modify the attributes of a security group as follows:
   • Modify the name: Hover your mouse over the name of a security group, and then click the pen icon that appears.
   • Modify the name and description: Click Modify on the right of the security group, and then enter a new name and description in the dialog box.

5. Click OK.

1.10.3 Clone a security group

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

Prerequisites

If you want to change the network type of the clone security group to VPC, at least one VPC must exist in the destination region. For more information, see #unique_61.

Context

You can clone a security group in the following scenarios:

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

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose Network & Security > Security Groups.
3. In the top navigation bar, select a region.
4. Find the security group to be cloned on the Security Groups page and click Clone in the Actions column.
5. In the **Clone** dialog box, configure the clone security group.

   - **Destination Region**: Select a region for the clone security group. Note that only some regions are supported. The supported regions are displayed in the console.
   - **Security Group Name**: Enter a name for the clone security group.
   - **Network Type**: Select an applicable network type for the clone security group. If you set Network Type to VPC, select an available VPC in the destination region.

6. Click **OK**.

**Result**

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

### 1.10.4 Remove an instance from a security group

You can remove an ECS instance from one of its security groups as needed. If an instance is removed from a security group, it can no longer communicate with other instances in that group over the intranet. Therefore, we recommend that you conduct sufficient tests before the removal to ensure that your business runs normally after removal.

**Prerequisites**

The ECS instance has been added to two or more security groups.

**Procedure**

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

3. Select a **Region**.

4. On the **Instances** page, find the target instance, and then click **Manage** in the **Actions** column.
5. In the left-side navigation pane, click **Security Groups**.

6. Find the target security group, and then click **Remove** in the **Actions** column.

7. Click **OK**.
1.10.5 Manage security groups

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

Query security groups

1. Log on to the ECS console.
2. In the left-side navigation pane, choose Network & Security > Security Groups.
3. In the top navigation bar, select a region.
4. Optional. Query the security groups as needed.
   - To query a security group by using its name, enter the name in the Security Group Name text box.
   - To query a security group by using its ID, enter the ID in the Security Group ID text box.
   - To query all security groups in a VPC, enter its ID in the VPC ID text box.

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

Modify a security group

1. Log on to the ECS console.
2. In the left-side navigation pane, choose Network & Security > Security Groups.
3. In the top navigation bar, select a region.
4. Find the target security group, and then click Modify in the Actions column.
5. Modify the Security Group Name and Description.
6. Click OK.

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

Clone a security group

1. Log on to the ECS console.
2. In the left-side navigation pane, choose Network & Security > Security Groups.
3. In the top navigation bar, select a region.
4. Find the target security group, and then click Clone in the Actions column.
5. In the **Clone Security Group** dialog box, set the parameters of the new security group.

   - **Target Region**: Select the specific region in which the new security group applies. Not all regions are supported. The supported regions are displayed in the console.
   - **Security Group Name**: Specify a name for the new security group.
   - **Network Type**: Select a network type that applies to the new security group. If you select **VPC**, you must select an available VPC in the target region.

6. Click **OK**.

**Remove an instance from a security group**

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

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

**Delete a security group**

1. Log on to the **ECS console**.
2. In the left-side navigation pane, choose **Network & Security > Security Groups**.
3. In the top navigation bar, select a region.
4. Select one or more security groups, and then click **Delete** in the lower-left corner of the list.
5. In the **Delete Security Group** dialog box, click **OK**.

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


2 Key pairs

2.1 SSH key pair overview

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

Introduction

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

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

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

Benefits

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

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

Limits

SSH key pairs have the following limits:

• If you use an SSH key pair to log on to a Linux instance, the password logon method will
  be disabled for higher security.
• SSH key pairs apply only to Linux instances.
• Currently, only RSA 2048-bit key pairs can be created in the ECS console.
• An Alibaba Cloud account can have a maximum of 500 key pairs in a region.
• A Linux instance can be bound with only one SSH key pair. If your instance has a key pair
  bound, the new key pair will replace the original one.
• Instances of phased-out instance types cannot use SSH key pairs. For more information,
  see #unique_68.
• If you bind an SSH key pair to or unbind an SSH key pair from an instance in the Running
  (Running) state, you must restart the instance for the operation to take effect. This
  enhances data security.

Creation method

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

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

Note:

If you create a key pair in the ECS console, you must download and securely store the
private key for later use. After the key pair is bound to an instance, you cannot log on to
the instance if you do not have the private key.
• Create an SSH key pair by using a key pair generator and import the key pair to the ECS console. The imported key pair must support one of the following encryption methods:
  - rsa
  - dsa
  - ssh-rsa
  - ssh-dss
  - ecdsa
  - ssh-rsa-cert-v00@openssh.com
  - ssh-dss-cert-v00@openssh.com
  - ssh-rsa-cert-v01@openssh.com
  - ssh-dss-cert-v01@openssh.com
  - ecdsa-sha2-nistp256-cert-v01@openssh.com
  - ecdsa-sha2-nistp384-cert-v01@openssh.com
  - ecdsa-sha2-nistp521-cert-v01@openssh.com

2.2 Use an SSH key pair

2.2.1 Create an SSH key pair

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

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose Network & Security > SSH Key Pairs.
3. In the top navigation bar, select a region.
4. Click Create SSH Key Pair.
5. On the **Create SSH Key Pair** page, configure the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH Key Pair Name</td>
<td>The key pair name must be unique. The name must be 2 to 128 characters in length and can contain letters, digits, and the following special characters: periods (.), underscores (_), hyphens (-), and colons (:). It cannot start with a special character or digit.</td>
</tr>
</tbody>
</table>
| Creation Type         | You can select one of the following types of SSH key pairs: We recommend that you select **Auto-create** and save the private key in a timely manner.  

- **Auto-create**: The system automatically creates a key pair for you. Download the private key immediately after its creation. You cannot download the private key at any time afterwards.  
- **Import**: You can import a Base64-encoded public key. |
| Tag                   | You can bind one or more tags to the key pair to facilitate resource search and aggregation. For more information, see #unique_71.                  |

6. Click **OK**.

**What's next**

- [Bind an SSH key pair to an instance](#)

**Related topics**

#unique_73

### 2.2.2 Import an SSH key pair

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

**Prerequisites**

You have obtained the public key information of the key pair to be imported.

**Context**

---

**Note:**
Do not import the private key. Store the private key in a safe location. To log on to an ECS instance that is bound with a key pair, you must have the private key.

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

An imported public key must be Base64 encoded and supports one of the following encryption methods:

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

Procedure

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

![Note:

The 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

#unique_75
2.2.3 View public key information

This topic describes three ways to view public key information.

Windows

To view public key information, follow these steps:

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

Linux or macOS

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

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

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

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAxxxxxxxxxx+GF9q7rh6vYrExwT4WU4f
fsaRcVXGV2Mg9RHEx2hl1au77GkmnIgwKBZjwlfQQT4GDdsy2nBoDjPrCEBiPxxxxxx
xxx/ftcNukjcmMMOA8YUT+sJk3l7rCLkesE+S5880yNdRjBiiUy40kyr7Y+fqGvdsOHGM
XZQPPkBtojcxxxxxxxxxx/htEqGa/Jq4fH7bR6CYQ2XgH/hCap29Mdi/G5Tx1nbUKu
IHdMWOpxjxxxxxxxxx+iHTGiAIRG1riyNRVC47ZEVxxxxxxxx
```

**Note:**

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

View the public key information in the instance

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

2.2.4 Bind an SSH key pair to an instance

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

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

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose Network & Security > SSH Key Pairs.
3. In the top navigation bar, select a region.
4. Find the key pair to be bound and click Bind in the Actions column.
5. Select the target ECS instance in the Select Instance section, and then click the > icon to move the target instance to the Selected section.

   If instance names in the Select Instance section are dimmed, the instances are Windows instances and cannot be bound with SSH key pairs.
6. Click OK.
7. If the selected ECS instance is in the Running (Running) state, complete the following operations to restart the instance to make the binding operation take effect:
   a) In the left-side navigation pane, choose Instances & Images > Instances.
   b) Find the target instance, and choose More > Instance Status > Restart in the Actions column.
   c) In Restart Instance dialog box that appears, click OK.

What's next

- After an SSH key pair is bound to an ECS instance, you can log on to the ECS instance by using the SSH key pair. For more information, see #unique_75.
- If you want to log on to the instance by using the password after you bind a key pair, you can reset the instance password. Then, you can log on to the instance by using the key pair or the new password. For more information, see Reset the logon password of an instance.

Related topics

#unique_79
2.2.5 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 AAAAB3NzaC1yc2EAAAADAQABAAABAQDdlrdZwV3+GF9q7rh6v YrExwT4WU4fsaRcVXGV2Mg9RHex21h1au77GkmnlGuk7jywjwQQT4GDsdjy 2nBoDjPrcEBIPxxxxxw0v/fc7nuJkcmMMAO88YT/2jK3i7rCLkesE+S5880yNdRj BiUy40y7rY7+fgGvdSOGHMXZQppBtojxcsxxxxxw/h7EeqG/2q4fH7bR6CYQ2XgH/ h Concat/29Md7/G5T1XnbUKuIHDMDWOpjfxxxxxxw+lHtGiAIRG1ryNRVC47ZEvCg9iTWW GrWFvxxxxxxxw/9H9mPC01Xt2fxxxxxwBtmR 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+GF9q7rh6v YrExwT4WU4fsaRcVXGV2Mg9RHex21h1au77GkmnlGuk7jywjwQQT4GDsdjy 2nBoDjPrcEBIP6t0MkSxAPkk/fc7nuJkcmMMAO88YT/2jK3i7rCLkesE+S5880yNdRj BiUy40y7rY7+fgGvdSOGHMXZQppBtojxcsxxxxxw/h7EeqG/2q4fH7bR6CYQ2XgH/ h Concat/29Md7/G5T1XnbUKuIHDMDWOpjfxxxxxxw+lHtGiAIRG1ryNRVC47ZEvCg9iTWW GrWFvxxxxxxxw/9H9mPC01Xt2fxxxxxwBtmR imported-openssh-key```

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

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

#unique_82

2.2.7 Delete an SSH key pair

If you no longer require a key pair, you can delete it. Note that deleting a key pair is irreversible. Existing instances that have used the key pair are not affected. However, the deleted key pair name remains associated to the instance. Exercise caution when performing this action.

Note:
• If you delete a key pair that is still attached to an instance, its name cannot be used to create or import a key pair again. Otherwise, the error message "The key pair already exists".
• If you delete a key pair that had never been attached to an instance, its name can be used to create or import a key pair again.

To delete one or more key pairs, follow these steps:

1. Log on to the ECS console.
2. In the left-side navigation pane, click **Networks and Security > SSH Key Pair**.
3. Select one or more key pairs.
4. Click **Delete**.
3 Implement access control by using RAM

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

Context

RAM is a resource access control service provided by Alibaba Cloud. For more information about RAM, see #unique_85. The following section describes how RAM is used to implement access control.

- **RAM users**: If you have purchased one or more ECS instances and multiple RAM users within your organization (such as employees, systems, or applications) need to access the instances, you can create an authorization policy that only grants specific RAM users access to these instances. This eliminates the risk of disclosing your AccessKey pair of your Alibaba Cloud account and helps maintain account security.

- **RAM user groups**: You can create multiple user groups and grant different permissions to each group. In this way, RAM users in each group are assigned the same permissions. Example:

  - You can associate a user group with an authorization policy to deny access to specific ECS resources from IP addresses that are outside your corporate network.
  - You can move a RAM user from one user group to another to change the user’s permissions as needed. For example, you have two user groups: SysAdmins and Developers. The two groups are assigned different permissions.

  - **SysAdmins**: This user group needs permissions to create and manage ECS instances. You can associate the SysAdmins group with an authorization policy that allows its group members to perform all ECS operations to create and manage instances, images, snapshots, and security groups.

  - **Developers**: This user group only needs permissions to use ECS instances. You can associate the Developers group with an authorization policy that allows its group members to call the DescribeInstances, StartInstance, StopInstance, RunInstance, and DeleteInstance operations.

Authorization policies

Authorization policies are categorized into **system policies** and **custom policies**.
• **System policies**: the authorization policies provided by Alibaba Cloud. Some commonly used system policies in ECS are as follows:
  - AliyunECSReadOnlyAccess: grants read-only permissions on ECS instances.
  - AliyunECSFullAccess: grants full administrative permissions on ECS instances.
  - AliyunECSImageImportDefaultRole: grants permissions to import custom images.
  - AliyunECSImageExportDefaultRole: grants permissions to export custom images.
  - AliyunECSNetworkInterfaceManagementAccess: grants permissions to manage ENIs.
• **Custom policies**: the user-defined authorization policies. These policies are suitable for users who are familiar with various Alibaba Cloud APIs and require fine-grained access control. For more information about how to create a custom policy, see *(Optional) Create a custom authorization policy.*

**Prerequisites**

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

**Procedure**

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

1. **Create a RAM user**
2. *(Optional) Create a custom authorization policy*
3. **Authorize the RAM user**

**Create a RAM user**

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

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

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

3. Specify the **Logon Name** and **Display Name** parameters.
4. Under **Access Mode**, select **Console Password Logon** or **Programmatic Access**.

  - **Console Password Logon**: If you select this check box, you must also complete the basic security settings for logon, including deciding whether to automatically generate a password or customize the logon password, whether the user must reset
the password upon the next logon, and whether to enable multi-factor authentication (MFA).

- **Programmatic Access**: If you select this check box, an AccessKey pair is automatically created for the RAM user. The user can access Alibaba Cloud resources by calling an API operation or by using a development tool.

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

5. Click OK.

**(Optional) Create a custom authorization policy**

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

1. In the left-side navigation pane, click **Policies** under **Permissions**.
2. On the page that appears, click **Create Policy**.
3. On the Create Custom Policy page, specify the **Policy Name** and **Note** parameters.
4. Set **Configuration Mode**. You can select **Visualized** or **Script**.
   - If you select **Visualized**, click **Add Statement**. On the page that appears, configure permissions, API operations, and resources.
   - If you select **Script**, edit policy scripts based on #unique_89.

If you select **Script**, you must specify values of the **Action** and **Resource** parameters in **Statement** based on the authentication list section in #unique_90. For more information about values of other parameters, see the following topic in RAM documentation: #unique_89.

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

```json
{
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ecs:DescribeImages",
            "vpc:DescribeVpcs",
            "vpc:DescribeVSwitches",
            "ecs:DescribeSecurityGroups",
            "ecs:RunInstances",
            "ecs:StopInstances",
            "ecs:TerminateInstances",
            "ecs:StartInstances",
            "ecs:CreateTags"
         ],
         "Resource": "*"
      }
   ]
}
```
The following sample policy configured using scripts allows a RAM user to create subscription instances. **bss**-related API operations can be called to view and pay subscription orders and the corresponding system policy is AliyunBSSOrderAccess.

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

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

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

5. Click **OK**.

**Authorize the RAM user**

You can perform the following steps to authorize the RAM user in the RAM console:
1. In the left-side navigation pane, click **Users** under **Identities**.

2. In the **User Logon Name/Display Name** column, find the target RAM user.

3. Click **Add Permissions**. On the page that appears, the principal is automatically filled in.

4. In the **Policy Name** column, select the target policies by clicking the corresponding rows.

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

5. Click **OK**.

6. Click **Finished**.

**What's next**

After authorization is completed, the assigned permissions take effect immediately. The RAM user then can log on to the **RAM console** to operate the target cloud resource.
4 Instance RAM roles

4.1 Overview

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

**Scenarios**

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

Instance RAM roles enable ECS instances to assume roles with certain access permissions. For more information about the roles, see #unique_93.

**Benefits**

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

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

You are not billed for binding an instance RAM role.

Limits

Instance RAM roles have the following limits:

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

References

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

4.2 Bind an instance RAM role

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

Prerequisites

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

Context

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

Procedure

An Alibaba Cloud account is used in the following example to create an instance RAM role and bind the role to an ECS instance in the RAM console:
1. **Step 1: Create an instance RAM role**

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

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

2. **Step 2: Authorize the instance RAM role**

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

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

3. **Step 3: Bind the instance RAM role**

Perform the following operations to bind the instance RAM role to an ECS instance in the ECS console:
1. Log on to the **ECS console**.

2. In the left-side navigation pane, choose **Instances & Images > Instances**.

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

4. Find the target ECS instance and choose **More > Instance Settings > Bind/Unbind RAM Role**.

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

Alternatively, you can select an instance RAM role from the RAM Role drop-down list in the **RAM Role** field on the **System Configurations** page when you create an ECS instance. For more information, see #unique_44.

**Related topics**

#unique_100

#unique_101
4.3 Manage an instance RAM role

4.3.1 Replace an instance RAM role

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

Procedure

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

**Related topics**

#unique_106

### 4.3.2 Unbind a RAM role

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

**Procedure**

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

5. Set **Action** to **Unind**. Click **OK**.
4.3.3 Obtain a temporary authorization token

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

Procedure

1. Connect to the ECS instance remotely. For more information, see #unique_109.
2. Obtain a temporary authorization token for an instance RAM role. The name of the instance RAM role is EcsRamRoleDocumentTesting.

   • For Linux instances, run the `curl http://100.100.100.200/latest/meta-data/Ram/security-credentials/EcsRamRoleDocumentTesting` command.

   An example of the temporary authorization token obtained:

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

4.3.4 Authorize a RAM user to use an instance RAM role

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

Context

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

Procedure
1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click Users under Identities.
3. In the User Logon Name/Display Name column, find the target RAM user.
4. In the Policy Name column, select the desired policies by clicking the corresponding rows.

The authorization policy is as follows. [ECS RAM Action] indicates permissions that can be granted to RAM users. For more information, see #unique_90.

```json
{
  "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": "**"
    }
  ]
}
```

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

5. Click OK.
6. Click Finished.

Related topics
#unique_102

4.4 Use an instance RAM role by calling API operations

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

Prerequisites
The RAM service is activated. For more information, see #unique_97 in the RAM documentation.

Context
Instance RAM roles have the following limits:

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

Procedure

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

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

**Step 1: Create an instance RAM role**

Call the `CreateRole` operation to create an instance RAM role.

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

Set the `AssumeRolePolicyDocument` parameter based on the following policy:

```json
{
    "Statement": [
        {
            "Action": "sts:AssumeRole",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "ecs.aliyuncs.com"
                ]
            }
        }
    ],
    "Version": "1"
}
```
Step 2: Authorize the instance RAM role

Perform the following operations to authorize the instance RAM role:

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

   Configure the following parameters:

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

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

2. Call the AttachPolicyToRole operation to authorize the role policy.

   Configure the following parameters:

   • Set the PolicyType parameter to Custom.
   • Set the PolicyName parameter. For example, set this parameter to EcsRamRoleDocumentTestingPolicy.
   • Set the RoleName parameter. For example, set this parameter to EcsRamRoleDocumentTesting.

Step 3: Bind the instance RAM role

Call the AttachInstanceRamRole operation to bind the instance RAM role.

Configure the following parameters:

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

(Optional) Step 4: Unbind the instance RAM role

Call the DetachInstanceRamRole operation to unbind the instance RAM role.
Configure the following parameters:

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

(Optional) Step 5: Obtain a temporary authorization token

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

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

- Windows instance: For more information, see Metadata.

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

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

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

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

Note:

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

1. Log on to the RAM console.
2. Authorize a RAM user to use the instance RAM role. For more information, see #unique_119.

```json
{
    "Version": "2016-10-17",
    "Statement": [
        
```
Elastic Compute Service

Security / 4 Instance RAM roles

```
"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 #unique_90.

References

Bind an instance RAM role

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

#unique_95
#unique_100
#unique_120
#unique_101
#unique_102
#unique_103
#unique_121
#unique_122
5 Basic security services

Alibaba Cloud Security Center provides ECS with basic security services such as unusual 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.

What are basic security services?

Alibaba Cloud Security Center provides basic security services for ECS, which collect and visualize security logs and fingerprints of ECS assets. Main basic security services security prevention and intrusion detection are available 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 Security Center Documentation.

Billing methods

In Security Center Basic Edition, basic security services for ECS are provided for free.

If you want to upgrade to Security Center Advanced or Enterprise Edition, log on to the Security Center console to try Security Center Advanced or Enterprise Edition for free or purchase it. For the billing methods of Security Center Advanced Edition and Enterprise Edition, see #unique_125 in the Security Center documentation.

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 an ECS instance, the ECS instance is not protected by Security Center. The security data of this instance, such as vulnerabilities, alerts, and baseline vulnerabilities, and asset fingerprints, will not be displayed in the ECS console. For the installation paths of the Security Center agent, see #unique_126.

You can perform the following steps to install or uninstall the Security Center agent:
• Have the Security Center agent automatically installed when you create an ECS instance.

1. Log on to the ECS console.
2. In the left-side navigation pane, choose Instances & Images > Instances.
3. In the top navigation bar, select a region.
4. Create an ECS instance by referring to #unique_44. In the Image section on the Basic Configurations page, select Security Enhancement. The Security Center agent is then automatically installed on the new ECS instance.

Note:
You can also automatically install the Security Center agent by using the following method: Call the #unique_127 operation with SecurityEnhancementStrategy set to Active.

• Manually install the Security Center agent on an existing ECS instance.

1. Log on to the ECS console.
2. On the Overview page, click the shield-like Alibaba Cloud Security icon to log on to the Security Center console.
3. Install the Security Center agent by referring to #unique_128 in the Security Center documentation.

• Uninstall the Security Center agent.

1. Log on to the ECS console.
2. On the Overview page, click the Alibaba Cloud Security icon to log on to the Security Center console.
3. Uninstall the Security Center agent by referring to #unique_129 in the Security Center documentation.

Check the security status of your ECS instance

Perform the following steps to check the security status of your ECS instance:

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

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

Configure alert notifications

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

1. Log on to the ECS console.
2. On the Overview page, click the Alibaba Cloud Security icon to log on to the Security Center console.
3. In the left-side navigation pane, Choose Operation > Settings. On the Settings page, click the Notifications tab.
4. In the Alerts row, select severities and configure the methods and time for sending alert notifications.

Note:
If you have upgraded to Alibaba Cloud Security Advanced or Enterprise Edition, see #unique_130 in the Security Center documentation for more alert notification methods.

Related topics

- Feature comparison among Basic/Advanced/Enterprise Edition
6 Anti-DDoS Basic

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

Anti-DDoS Basic is a free service included in Alibaba Cloud Security. It offers up to 5 GB of mitigation capacity against common DDoS attacks. The ECS instance type determines the free-tier mitigation capacity, and you can log on to the Anti-DDoS Basic console to check the actual mitigation capacity threshold. For more information, see #unique_133.

How Anti-DDoS Basic works

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

Note:

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

Triggering conditions:

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

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

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

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

**Traffic scrubbing thresholds of ECS instances**

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

- **Maximum BPS threshold (Gbit/s):** For more information, see the Bandwidth (Gbit/s) specification in Instance families and #unique_68.
- **Maximum PPS threshold (Kpps):** For more information, see the Packet forwarding rate (Kpps) specification in Instance families and #unique_68.

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

<table>
<thead>
<tr>
<th>Instance type</th>
<th>Maximum BPS threshold (Gbit/s)</th>
<th>Maximum PPS threshold (Kpps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ecs.g5.16xlarge</td>
<td>20</td>
<td>4,000</td>
</tr>
</tbody>
</table>

**What to do next**

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

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

**Warning:**

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

- FAQ on security groups
  - What is a security group?
  - Why do I need to select a security group when I create an ECS instance?
  - What can I do if I create an ECS instance before I create a security group?
  - Why am I being prompted that the maximum number of rules has been reached when I try to add an instance to a security group?
  - If I adjust the maximum number of security groups that a VPC-type ECS instance can belong to, does this adjustment only take effect on security groups created after the limit is adjusted?
  - In what scenarios do security groups use the default security group rules?

- FAQ on security group rules
  - In what scenarios do I need to add a security group rule?
  - Why can't I configure Internet security group rules for my ECS instance in a VPC?
  - Why can't I access TCP port 25?
  - Why can't I access port 80?
  - Why have several internal security group rules been automatically added to my security group?
  - Why is the priority of some security group rules 110?
  - What happens when a security group rule is configured incorrectly?
  - Are the inbound and outbound rules in a security group counted separately?
  - Can I adjust the maximum number of rules that can be added to a security group?

- FAQ on host penalty and unblocking
  - What can I do if I receive a notification that my website has been blocked due to illegal activities and needs to be rectified?
  - What can I do if I receive a notification that my website has been penalized for committing external attacks?

- FAQ on quotas
  - How do I view resource quotas?
What is a security group?

A security group is a virtual firewall that implements access control for one or more ECS instances. Security groups logically isolate security domains in the cloud.

Each ECS instance must belong to at least one security group. When you create an ECS instance, you must specify a security group to add it to the instance. By default, instances within the same security group can communicate with each other but instances in different security groups are isolated from each other. You can configure a security group rule to authorize mutual access between two security groups. For more information, see Security group overview.

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

When you create ECS instances, you must select security groups to divide the security domains within your application environment and configure security group rules for proper network security isolation.

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

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

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

Why am I being prompted that the maximum number of rules has been reached when I try to add an instance to a security group?

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

If you are prompted that Failed to join the security group. The number of security group rules that have acted on the instance has reached the upper limit, we recommend that you select another security group.
If I adjust the maximum number of security groups that a VPC-type ECS instance can belong to, does this adjustment only take effect on security groups created after the limit is adjusted?

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

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

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

• If you have not created a security group when you create an ECS instance in a region in the ECS console for the first time, you can select a default security group automatically created by the system. The default security group is a basic security group. The default security group uses the default security rules. The default security rule has the priority of 110. It specifies that inbound traffic is allowed over ICMP, SSH port 22, and RDP port 3389 and that the authorization object is all CIDR blocks (0.0.0.0/0). You can also choose to allow inbound traffic over HTTP port 80 and HTTPS port 443. All outbound traffic is allowed.

• You have selected a security group template when you created a security group in the ECS console. The security group template applies to both basic security groups and advanced security groups. Alibaba Cloud provides Web Server Linux templates (inbound traffic is allowed over port 80, port 443, port 22, and ICMP), Web Server Windows templates (inbound traffic is allowed over port 80, port 443, port 3389, and ICMP), and custom templates (all inbound access requests are denied).

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

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

• No custom security group rules or default security group rules have been added to the security group to which the ECS instance belongs. When your ECS instance needs to access the Internet or an ECS instance in another security group within the current region, you must add a security rule.

• The created application uses a specified port or port range instead of the default port. In this case, you must allow the specified port or port range before you can check whether the application is connected. For example, assume you have deployed an NGINX service and need to set the listener port to TCP 8000 but only port 80 is allowed in your security group. In this case, you must add a security rule to ensure that the NGINX service is accessible.
Why can't I configure Internet security group rules for my ECS instance in a VPC?

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

Why can't I access TCP port 25?

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

Why can't I access port 80?

See Check whether TCP port 80 is working properly.

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

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

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

Why is the priority of some security group rules 110?

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

What happens when a security group rule is configured incorrectly?

If a security group rule is configured incorrectly, the ECS instances associated with this rule cannot communicate with other devices through the internal network or the Internet. These are examples of the effects:

- You cannot access Linux ECS instances remotely by using SSH or access Windows ECS instances by using the Remote Desktop Protocol (RDP).
- The public IP addresses of ECS instances cannot be pinged.
• The web services provided by the ECS instances cannot be accessed through HTTP or HTTPS.
• The ECS instances associated with this rule cannot communicate with other ECS instances through the internal network.

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

No, the inbound rules and outbound rules of a security group are counted together. The total number of inbound rules and outbound rules for each security group cannot exceed 200. For more information, see #unique_9.

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

No, each security group can contain a maximum of 200 security group rules. Each ENI of an ECS instance can be added to up to five security groups, allowing each ENI of an ECS instance to be associated with up to 1,000 security group rules.

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

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

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

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

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

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

How can I view the resource quota?

For more information about how to view the limits and quotas of resources, see #unique_9.