边缘计算机器

操作指南

产品文档

腾讯云

文档目录

EIP直通

操作指南
登录 Linux 实例

最近更新时间：2023-12-26 09:37:39

操作场景

边缘计算机器提供如下两种登录方式：
通过 VNC 方式登录
通过 SSH 方式登录
您可在创建边缘实例成功后，按照本文指引进行登录实例。

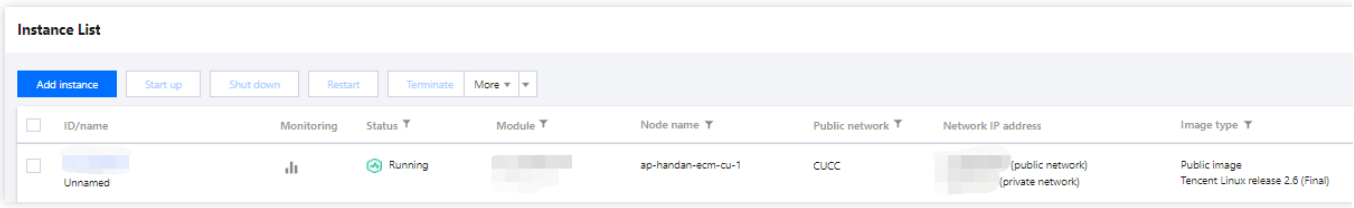
前提条件

已创建边缘计算实例，及获取公网 IP。
已获取登录实例的管理员账号及密码。
如果您忘记密码，请 重置密码。
如选择通过 SSH 方式登录 Linux 实例，本地计算机中需已安装 Xshell 软件。

操作步骤

通过 VNC 方式登录

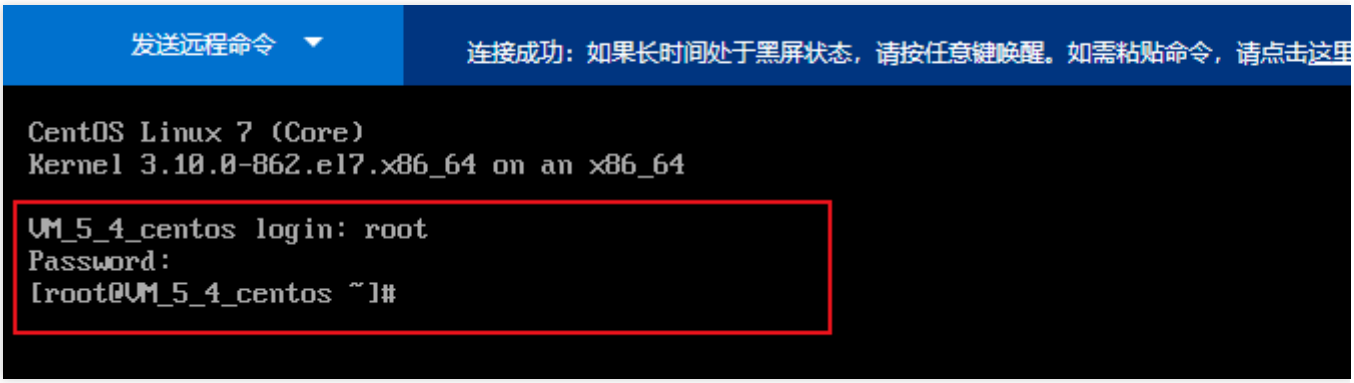
1. 登录 边缘计算机器控制台，在左侧导航栏中选择**实例列表**。
2. 在**实例列表**，选择需要登录的 Linux 实例，单击**登录**。如下图所示：



3. 在弹出的**登录 Linux 实例**窗口中，选择**VNC 登录**，单击**立即登录**。如下图所示：

4. 在弹出的对话框中，在 “login” 后输入用户名，按 **Enter**。
5. 在 **Password** 后输入密码，按 **Enter**。

输入的密码默认不显示，如下图所示：

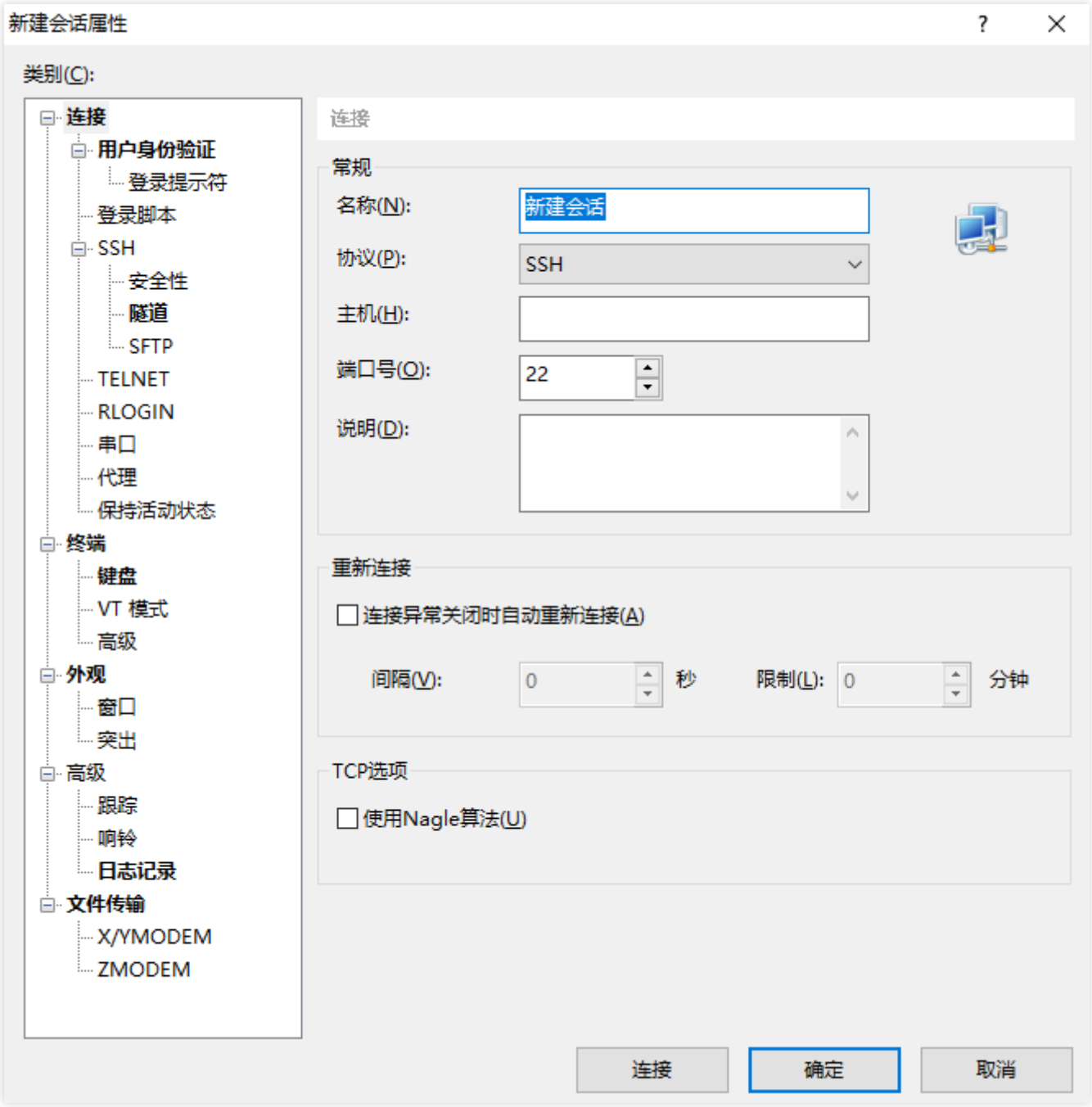


通过 SSH 方式登录

说明：

登录 Linux 实例的远程登录软件有很多种，例如 PuTTY、Xshell 等软件。本操作以 Xshell 6 软件为例，介绍如何在 Windows 系统的本地计算机中使用远程登录软件登录 Linux 实例。

1. 打开 Xshell 客户端，单击**新建**。
2. 在打开的新建会话属性窗口中，输入以下内容。如下图所示：



名称：填写会话名称，例如 test。

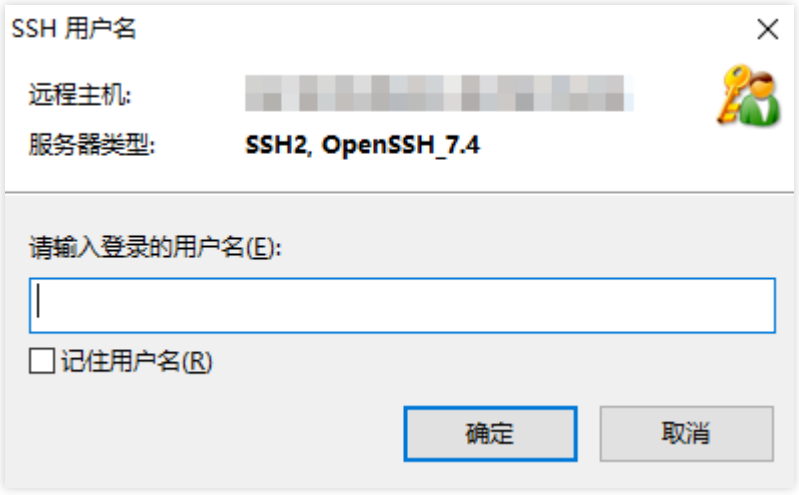
主机：边缘计算机器实例的公网 IP（登录 边缘计算机器控制台，可在实例列表页中获取公网 IP）。

协议：选择 **SSH**。

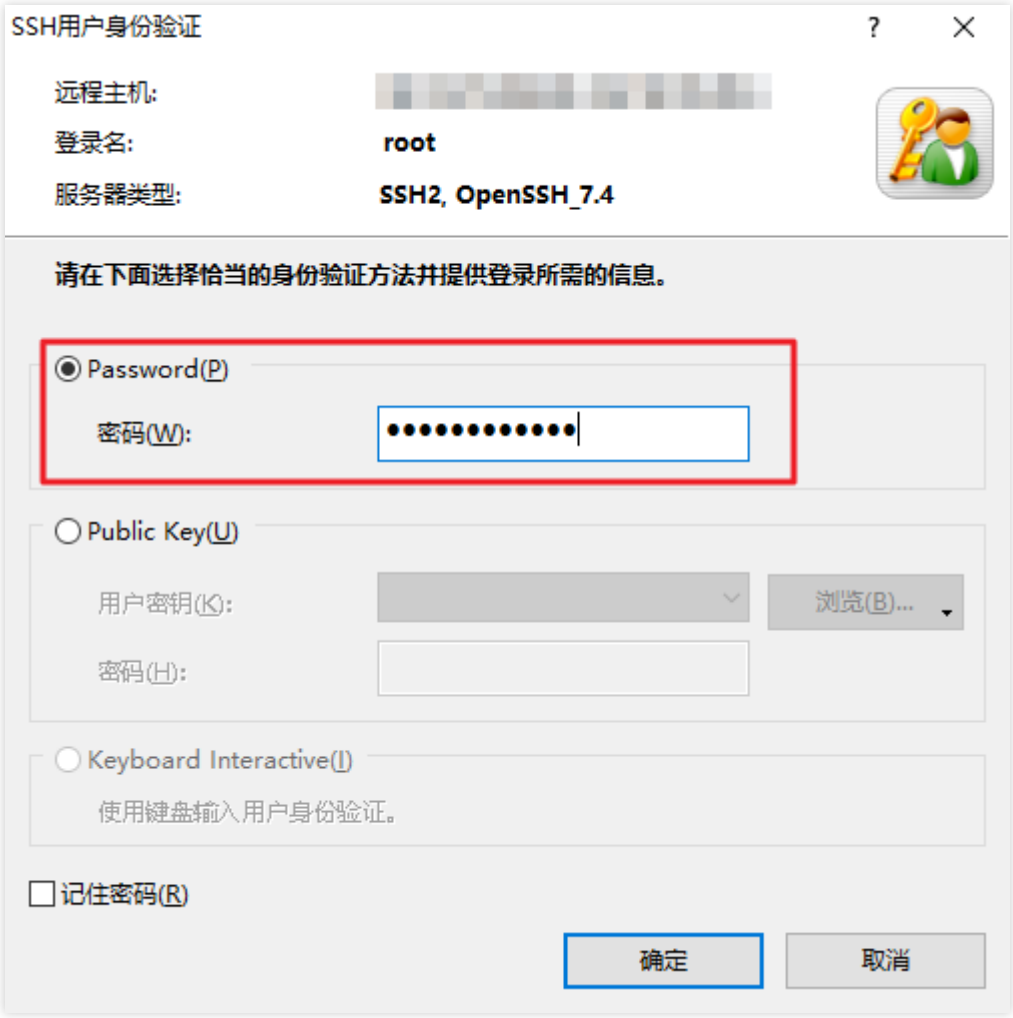
端口号：边缘计算机器实例的端口，必须设置为22。

3. 单击**连接**。

4. 输入登录的用户名（如 root），单击**确定**。如下图所示：



5. 输入登录的密码，单击**确定**。如下图所示：



登录完成后，命令提示符左侧将显示当前登录边缘计算机器实例的信息。

登录 Windows 实例

最近更新时间：2023-12-26 09:44:49

操作场景

本文介绍如何在 Windows 系统的本地计算机中通过远程桌面登录 Windows 实例。

前提条件

已创建边缘计算实例，及获取公网 IP。
已获取远程登录 Windows 实例需要使用实例的管理员账号和对应的密码。
如果您忘记密码，请 重置密码。

操作步骤

说明：
以下操作步骤以 Windows 10 操作系统为例。
1. 在本地 Windows 计算机上，右键单击

，选择**运行**。
2. 在打开的运行窗口中，输入 **mstsc**，按 **Enter**，打开远程桌面连接对话框。
3. 在**计算机**后面，输入 Windows 实例的公网 IP，单击**连接**。
4. 在弹出的 **Windows 安全**窗口中，输入实例的管理员账号和密码。
说明：
若弹出**是否信任此远程连接？**对话框，可勾选**不再询问我是否连接到此计算机**，单击**连接**。
5. 单击**确定**，即可登录到 Windows 实例。

管理边缘模块
创建边缘模块

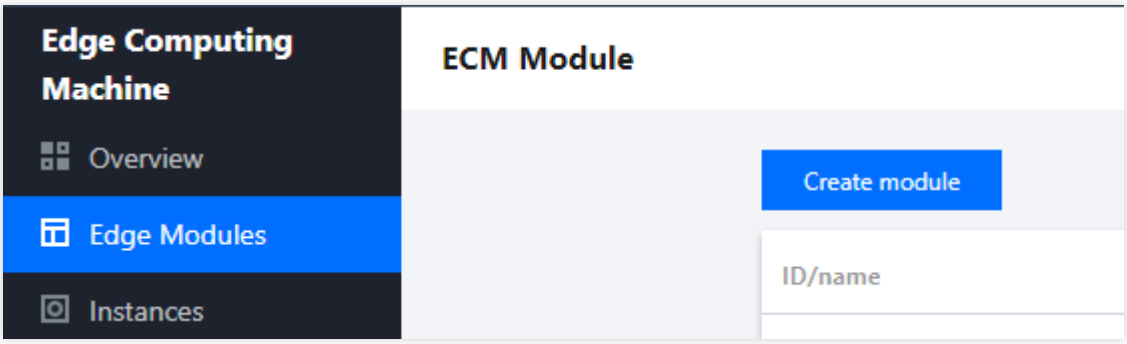
最近更新时间：2023-12-26 09:46:29

操作场景

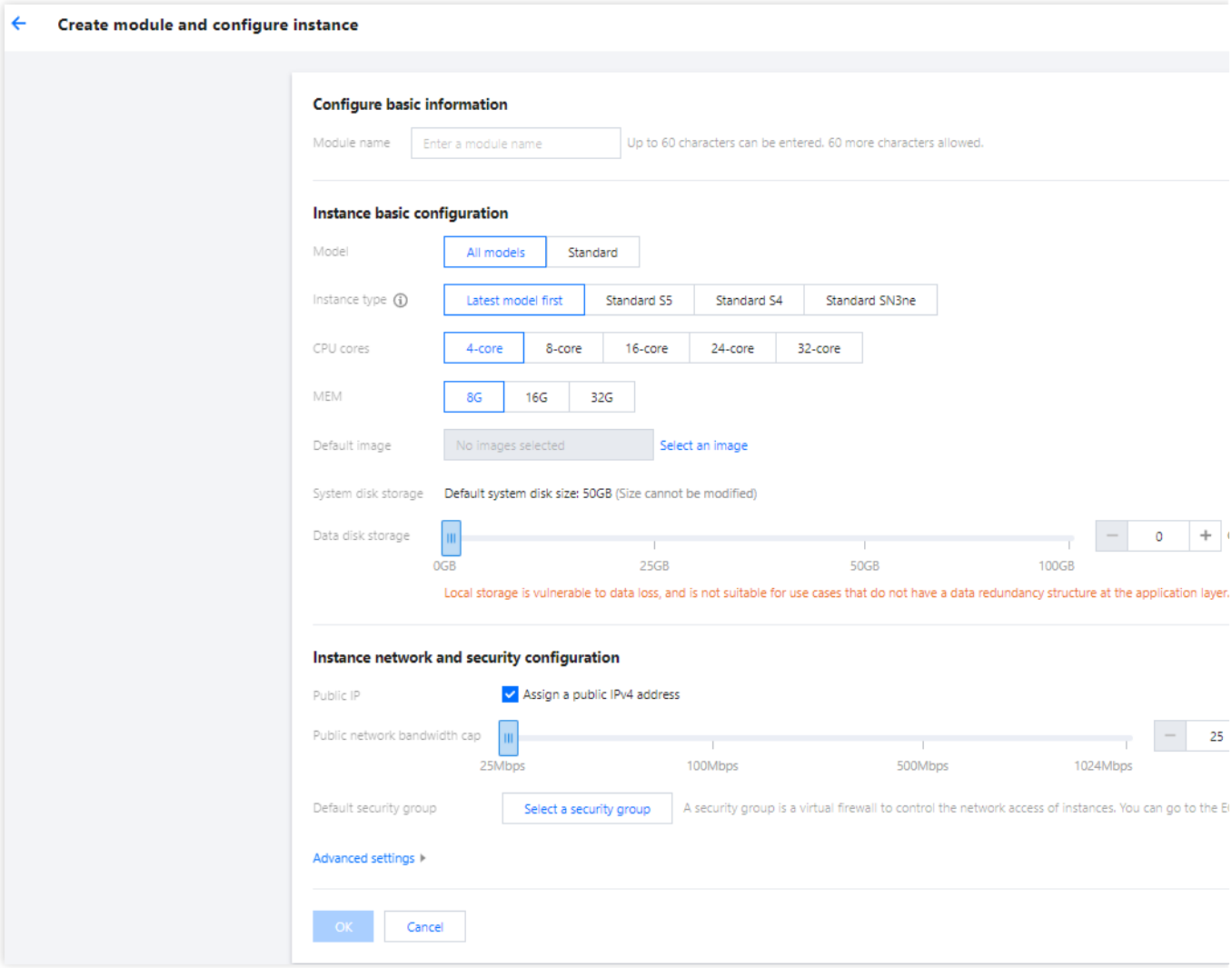
边缘模块是管理边缘服务的基础模块，包括边缘实例，模块下所有实例使用基本一致的计算、网络和镜像等配置，对外可以提供相同的服务。通过管理边缘模块，可以简化扩缩容操作，易于后续灵活调整业务的区域部署。本文指导您如何通过控制台创建边缘模块。

操作步骤

1. 登录 边缘计算机器控制台，在左侧导航栏中选择**边缘模块**。
2. 在边缘模块页面，单击**新建模块**。



3. 在创建模块及实例配置页面，根据提示，配置以下信息：



模块名称：表示需要创建的边缘模块名称，用户自定义。

实例类型：目前支持**高 IO 型 IT5**、**标准型S4**、**高内网带宽型S4**和**标准型 SN3ne**。在某些特殊场景下，不同的机型性能会有略微差异。如需了解具体差异，则请查阅 实例规格。

为简化实例创建的机型选择，建议您选择**新机型优先**。在此策略下，系统会在您选择的边缘节点按可用的最新机型创建实例。若某个选定的节点无可用的最新机型，则系统会按其他可用机型创建实例。

CPU核数：请根据实际需求进行选择。

内存：请根据实际需求进行选择。

默认镜像：腾讯云提供公共镜像和自定义镜像。对于刚开始使用腾讯云的用户，推荐选择公共镜像。

系统盘存储：默认为50GB，不支持调整大小。

数据盘存储：用于扩展边缘模块的存储容量，提供高效可靠的存储设备。默认为0GB，上限为100GB。

默认网络带宽上限：对带宽上限进行限制，若超出此上限，则默认丢包。默认为25Mbps，上限为1024Mbps。

默认安全组：安全组是一种虚拟防火墙，用于实例的网络访问控制。您可前往边缘计算机器控制台的 安全组，新建边缘安全组。

高级设置：可修改默认 IP 直通和默认标签的设置，请根据实际需求进行选择：

默认IP直通：IP 直通功能适用于边缘云服务器内需要查看公网 IP 的场景，例如，将内网流量和外网流量分别转发到不同的 IP 地址。

注意：

创建 Linux 操作系统的边缘实例时，系统默认按 IP 直通方式创建（您也可以在高级设置中，修改为非直通方式创建），创建后不支持修改 IP 直通方式。若创建 Windows 操作系统的边缘实例，系统会按非直通方式创建（Windows 操作系统暂时不支持IP直通方式）。

默认标签：通过设置默认标签，您可以对边缘模块进行分类管理。边缘模块已设置的默认标签会在创建新实例时作为新实例的标签建议键值，您也可以在创建实例时修改为您需要的标签键值。

注意：

该设置项仅修改边缘模块的标签键值，不会自动同步修改已经创建成功的实例标签键值。

4. 单击**确定**。

说明：

如控制台提供的边缘模块配置未能满足您的要求，请通过 提交工单 反馈，会有专门的商务人员与您对接。

删除边缘模块

最近更新时间：2023-12-26 09:49:02

操作场景

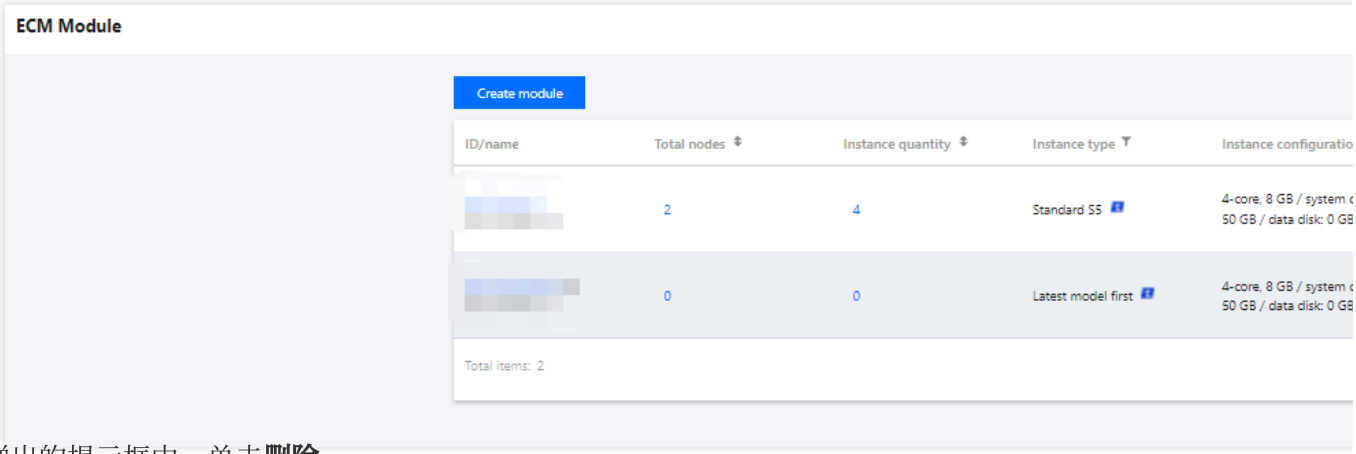
当您不需要某个边缘模块时，可以对该模块进行删除。本文指导您如何通过控制台删除边缘模块。

操作步骤

1. 登录 边缘计算机器控制台，在左侧导航栏中选择**边缘模块**。
2. 在边缘模块页面，选择待删除的边缘模块，单击操作栏的**删除**。

说明：

执行此操作前，请确认该模块下是否有创建实例，如果有，该模块将无法删除。



3. 在弹出的提示框中，单击**删除**。

配置模块默认安全组

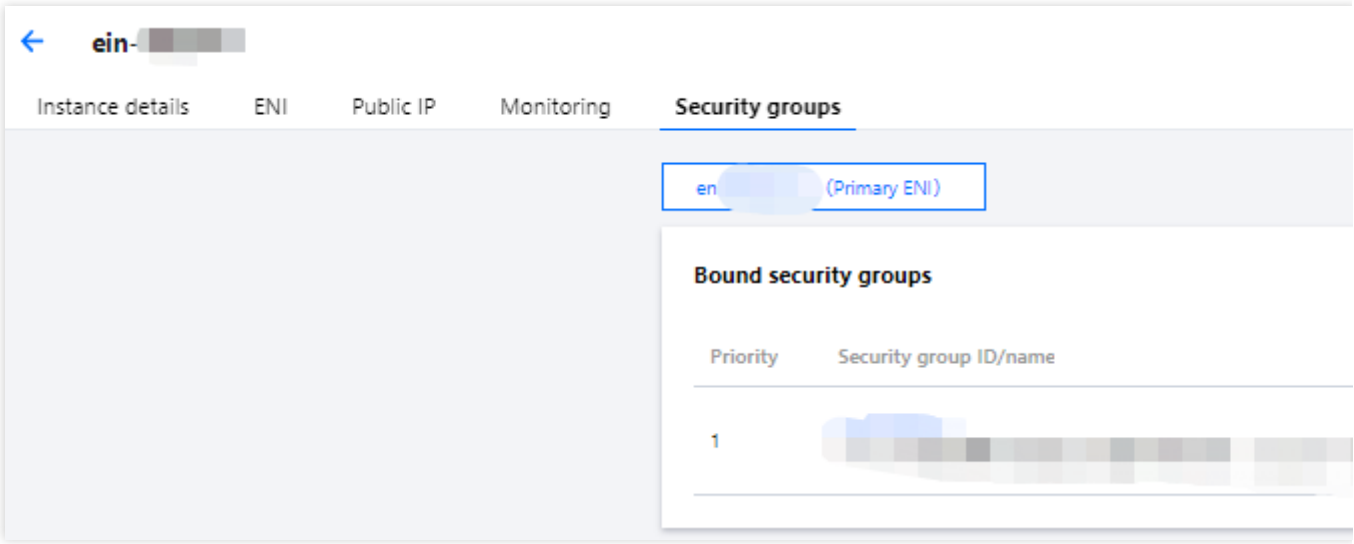
最近更新时间：2023-12-26 09:52:17

操作场景

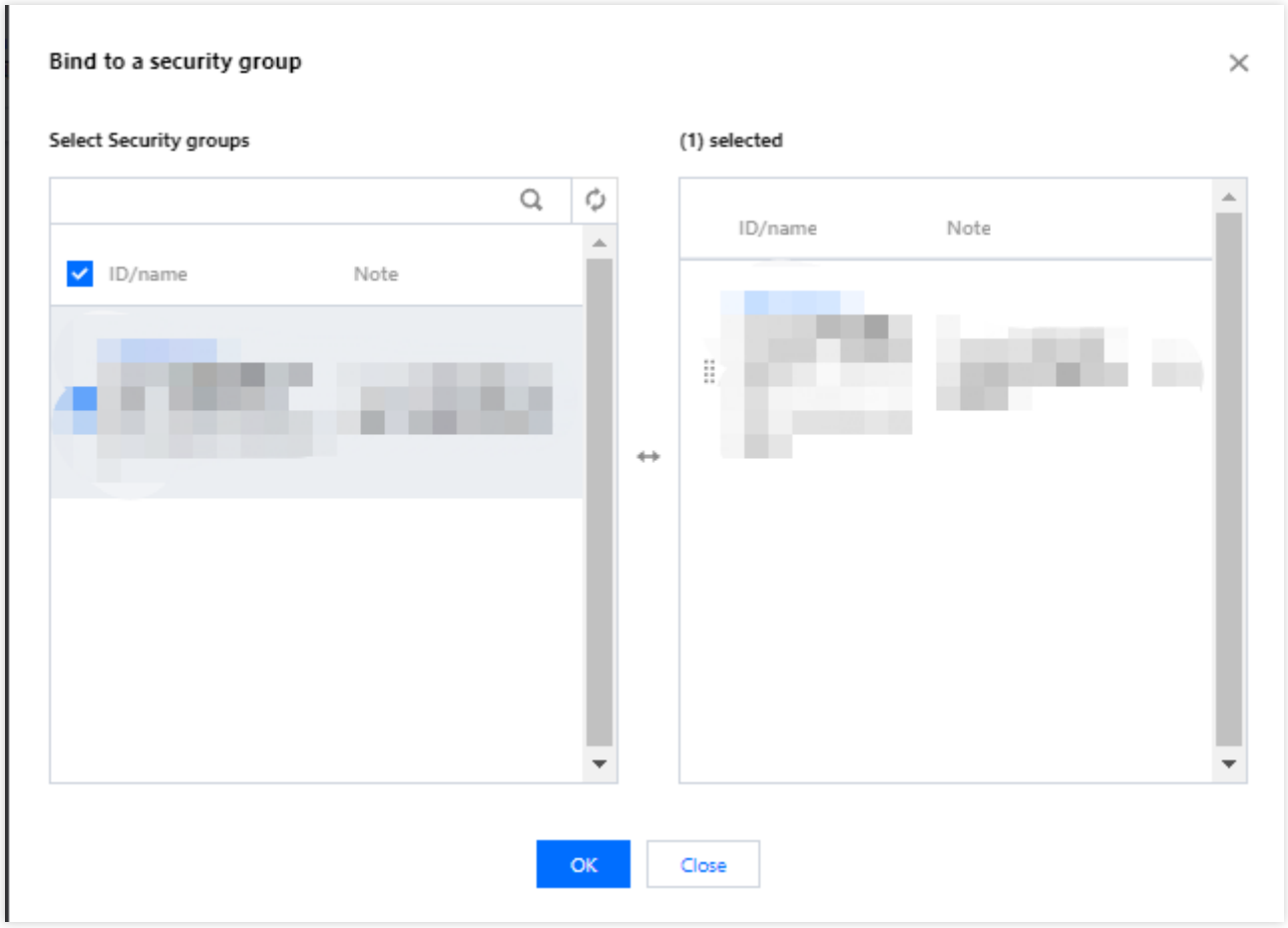
安全组是一种虚拟防火墙，具备有状态的数据包过滤功能，用于设置单台或多台边缘实例的网络访问控制，是腾讯云提供的重要的网络安全隔离手段。
创建边缘模块时必须要为模块配置默认安全组，作为创建边缘实例的默认安全组配置项，您可参考本文修改对应默认安全组。同时，腾讯云支持用户在创建边缘实例后更换实例所属的安全组，详情请参见 配置实例安全组。

操作步骤

1. 登录边缘计算机器控制台，选择左侧导航栏中的 边缘模块，进入**边缘模块**页面。
2. 在**边缘模块**页面中，单击需配置安全组的边缘模块 ID，进入模块详情页面。
3. 在模块详情页面，选择**安全组**页签，并在**已绑定安全组**栏中，单击**绑定**。如下图所示：



4. 在弹出的**配置安全组**窗口中，根据实际需求勾选需要绑定的安全组，单击**确定**即可完成绑定。如下图所示：


Bind to a security group
Select Security groups
(1) selected
ID/name
Note
ID/name
Note
OK
Close

管理实例
创建实例

最近更新时间：2023-12-26 09:56:04

操作场景

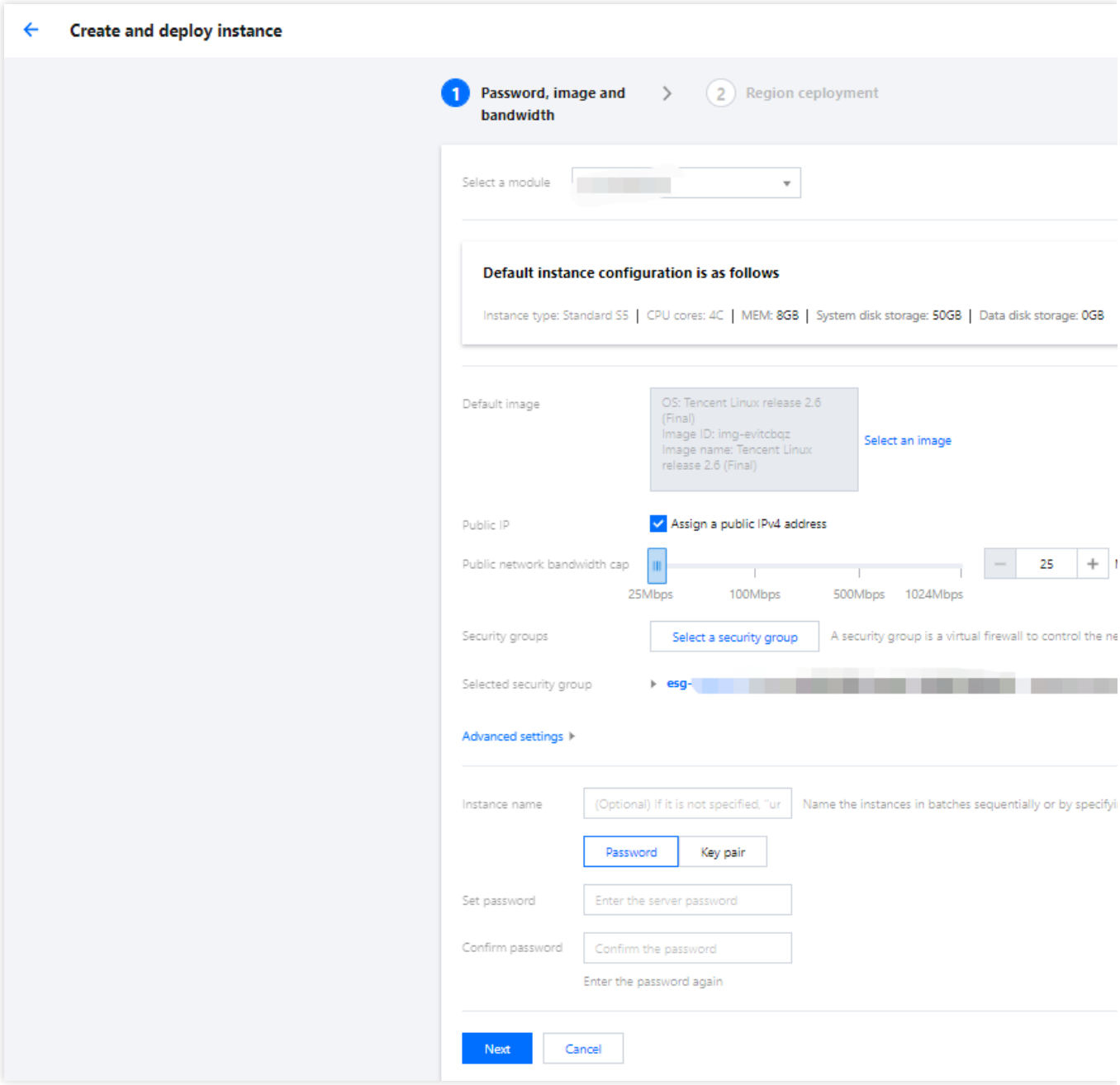
本文档指导您如何创建腾讯云边缘计算机器（Edge Computing Machine，ECM）实例。

前提条件

在创建边缘计算机器实例前，您需要完成以下工作：
注册腾讯云账号，并完成 实名认证。
已 创建边缘模块。
如需使用 Windows 镜像，则请通过 提交工单 申请或联系您的专属商务经理。

操作步骤

1. 登录 边缘计算机器控制台，在左侧导航栏中选择**实例列表**。
2. 在实例列表页面，单击**新增实例**，进入创建实例进行部署页面。
3. 根据页面提示，配置以下信息：



选择所属模块：请根据实际需求进行选择。

默认镜像：腾讯云提供公共镜像和自定义镜像。默认为与所属模块相同的镜像，请根据实际需求进行选择。

默认网络带宽上限：对带宽上限进行限制，若超出此上限，则默认丢包。默认为25Mbps，上限为1024Mbps。

安全组：安全组是一种虚拟防火墙，用于实例的网络访问控制。默认已选安全组为所属模块的安全组，用户可自行更改安全组设置。

高级设置：可修改默认 IP 直通和默认标签的设置，请根据实际需求进行选择：

IP直通：IP 直通功能适用于边缘云服务器内需要查看公网 IP 的场景。例如，将内网流量和外网流量分别转发到不同的 IP 地址。

注意：

创建 Linux 操作系统的边缘实例时，系统默认按 IP 直通方式创建（您也可以在高级设置中，修改为非直通方式创建），创建后不支持修改 IP 直通方式。若创建 Windows 操作系统的边缘实例，系统会按非直通方式创建（Windows 操作系统暂时不支持 IP 直通方式）。

标签：通过设置默认标签，您可以对边缘模块进行分类管理。边缘模块已设置的默认标签会在创建新实例时作为新实例的标签建议键值，您也可以在创建实例时修改为您需要的标签键值。

注意：

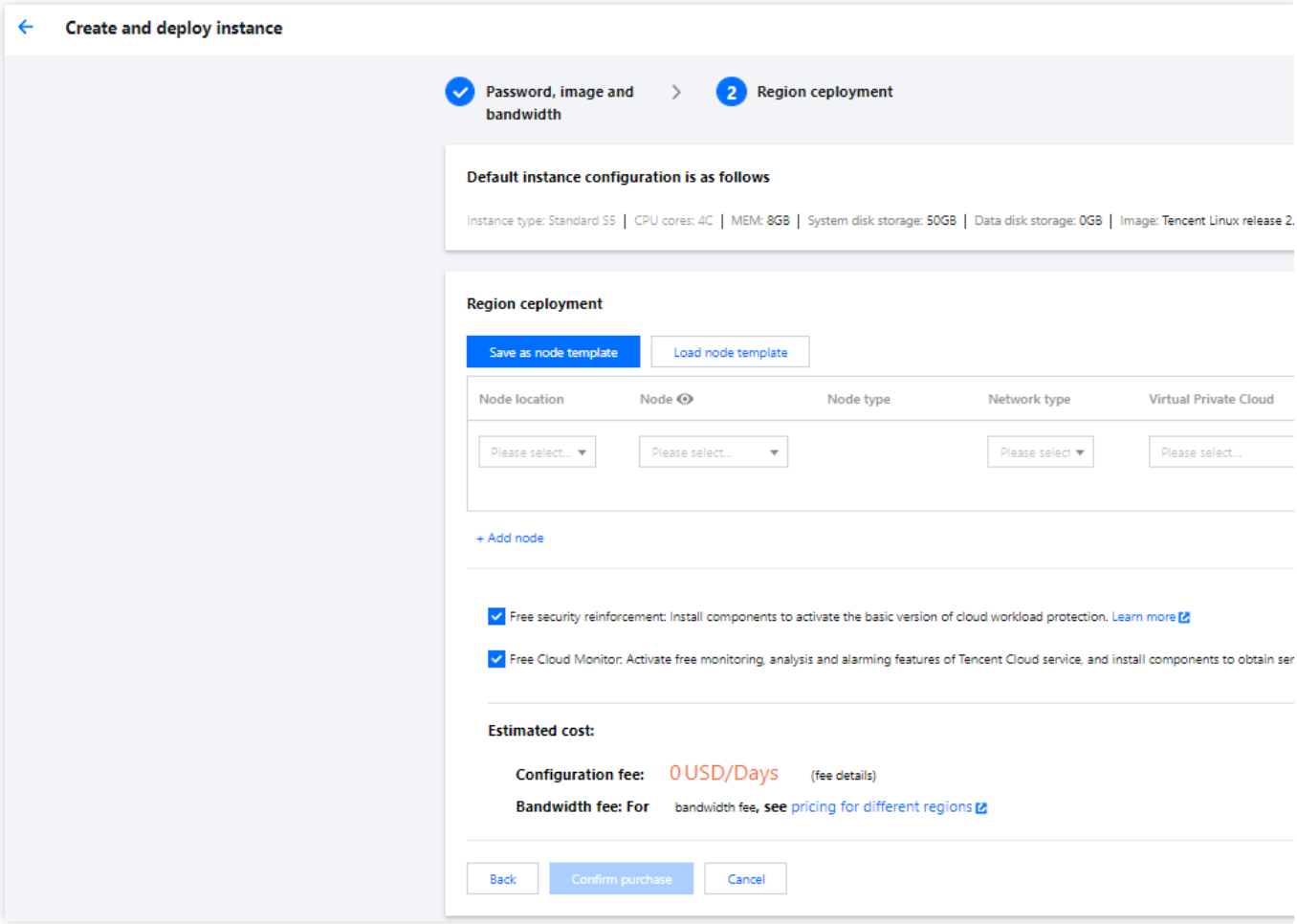
该设置项仅修改边缘模块的标签键值，不会自动同步修改已创建成功的实例标签键值。

实例名称：表示需要创建的实例名称，用户自定义。

设置密码和确认密码：自定义设置登录实例的密码。

4. 单击**下一步**。

5. 在创建实例进行部署的**区域部署**页面，根据提示，配置以下信息：



节点省份：建议选择与您的客户最近的省份，可降低访问时延、提高访问速度。

节点地区：请根据实际需求进行选择。

网络类型：请根据实际需求选择公网运营商。

实例数量：表示需购买云服务器的数量。

免费开通主机安全加固：默认勾选，帮助用户构建服务器安全防护体系，防止数据泄露。

免费开通腾讯云可观测平台：默认勾选，免费开通云产品监控，安装组件获取主机监控指标并以监控图标形式展示，且支持设置自定义告警阈值等。

6. 单击**确定购买**。

实例创建成功后，相关信息将通过您订阅的通知消息通道发送给您。您也可以在 实例列表 中查看新创建的资源。

查看实例详情

最近更新时间：2023-12-26 09:58:06

操作场景

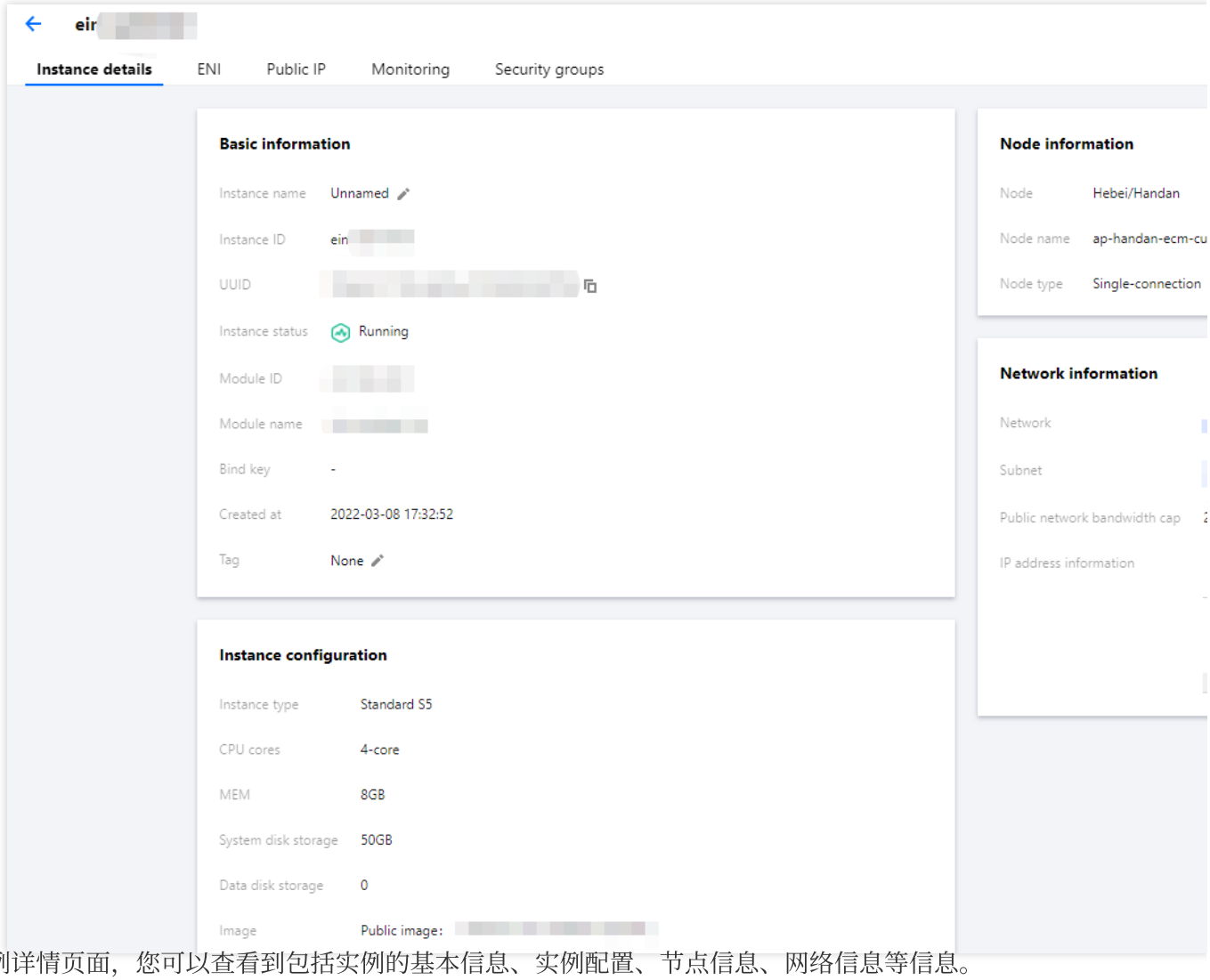
在完成边缘计算机器的实例创建之后，您可以在控制台中查看实例详情。

操作步骤

1. 登录 边缘计算机器控制台。
2. 在左侧导航栏中，选择**实例列表**。
3. 在实例列表页面，找到需要查看详情的实例，单击 ID/实例名，进入实例详情页面。

说明：

您也可以在需要查看详情的实例行中，单击**更多操作 > 详情**，进入实例详情页面。



在实例详情页面，您可以查看到包括实例的基本信息、实例配置、节点信息、网络信息等信息。

调整网络

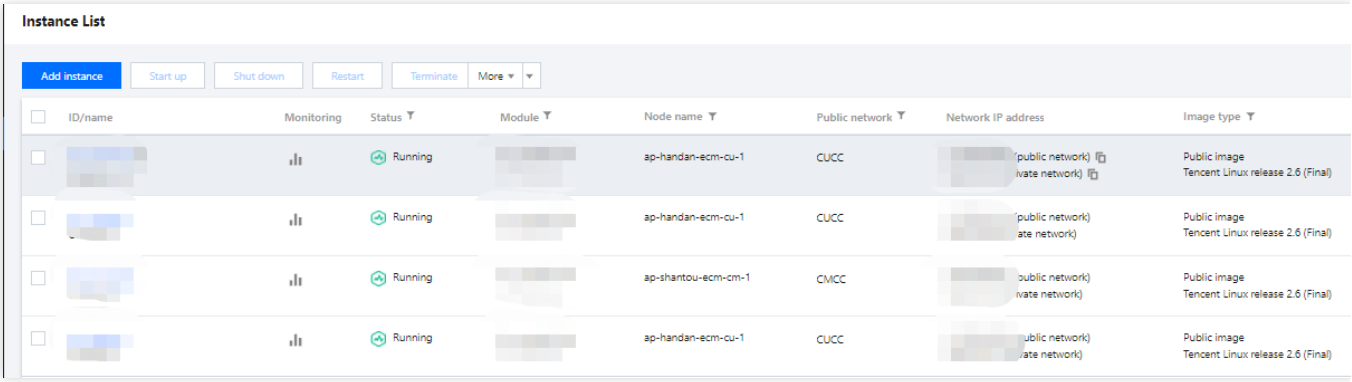
最近更新时间：2023-12-26 09:59:09

操作场景

本文指导您如何修改实例的带宽上限。

操作步骤

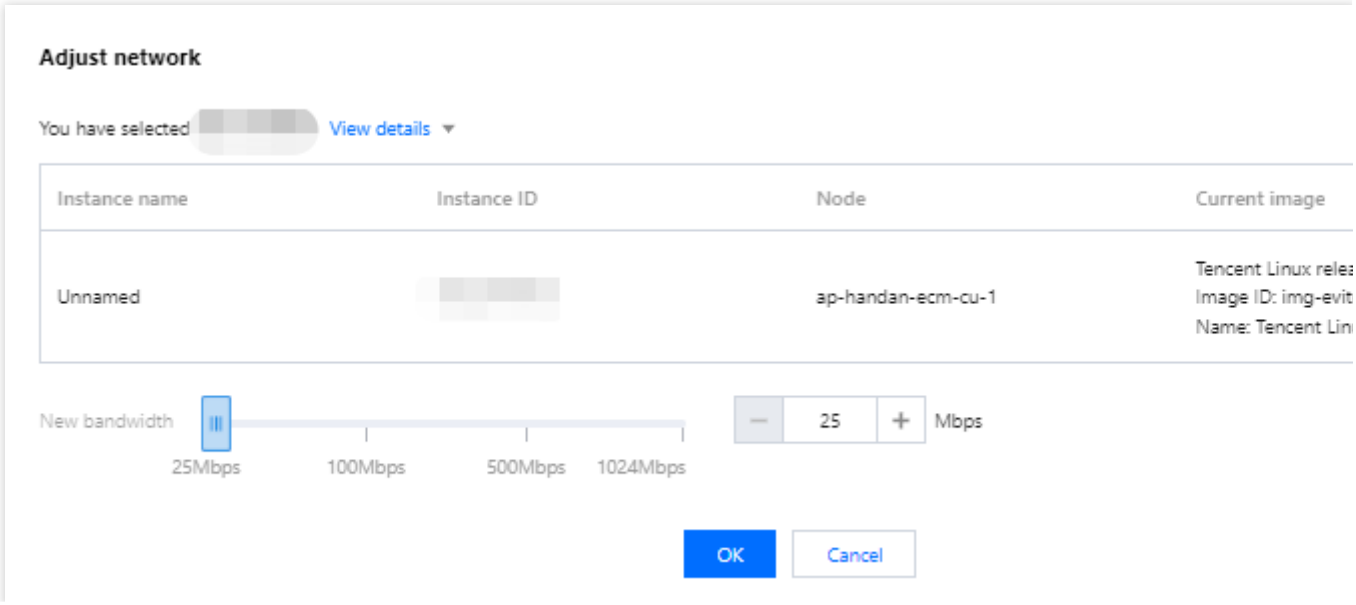
1. 登录 边缘计算机器控制台。
2. 在左侧导航栏中，选择**实例列表**。
3. 在实例列表页面，选择待调整网络的实例，单击**更多操作** > **调整网络**。



4. 在弹出的窗口中，设置目标带宽，单击**确定**。

说明：

实例的带宽上限默认为1Gbps。如果带宽的默认上限无法满足您的需求，请通过 提交工单 申请。


Adjust network
You have selected
View details
Instance name
Instance ID
Node
Current image
Unnamed
ap-handan-ecm-cu-1
Tencent Linux relea
Image ID: img-evit
Name: Tencent Lin
New bandwidth
25
Mbps
25Mbps
100Mbps
500Mbps
1024Mbps
OK
Cancel

销毁实例

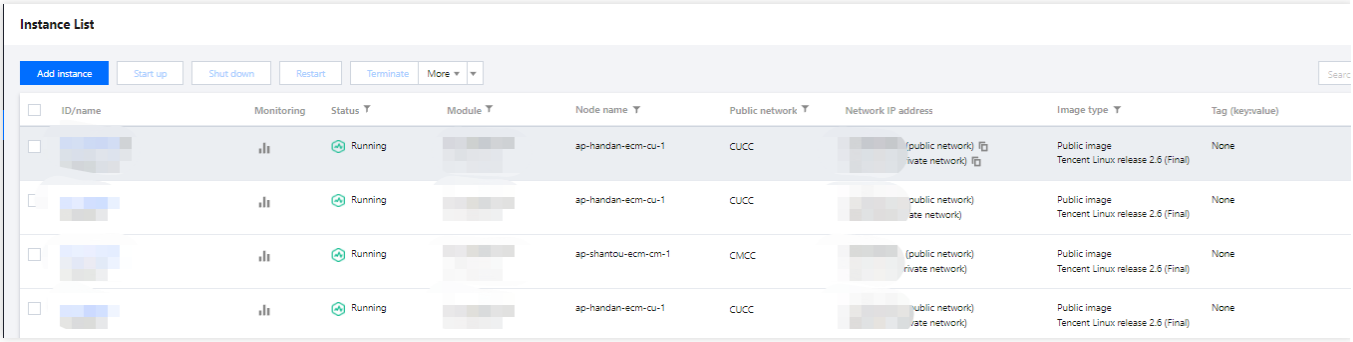
最近更新时间：2023-12-25 14:43:58

操作场景

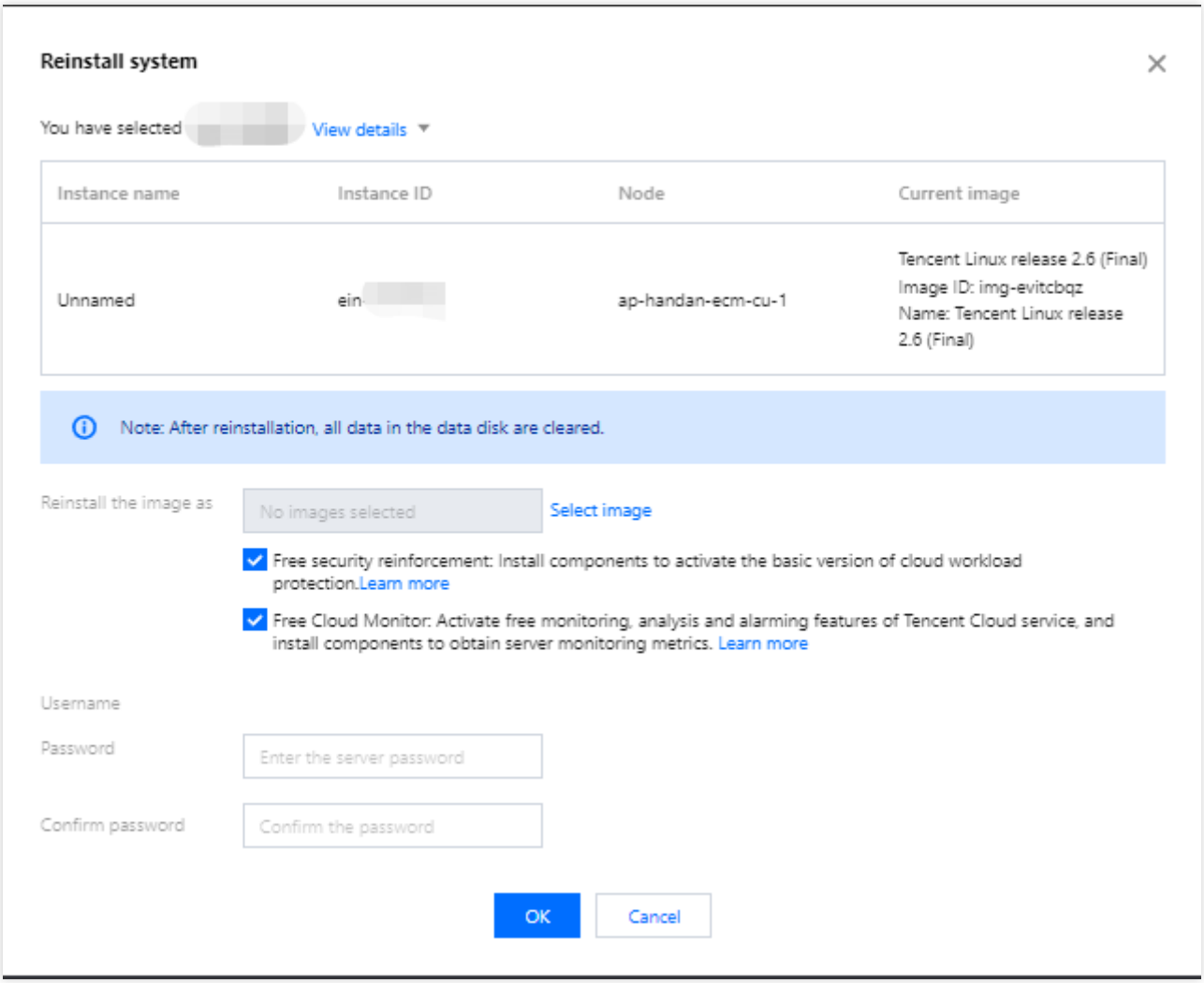
当您不再需要边缘计算机器实例时，可以对边缘计算机器实例进行销毁。本文指导您如何销毁边缘计算机器实例。

操作步骤

1. 登录 边缘计算机器控制台。
2. 在左侧导航栏中，选择**实例列表**。
3. 在实例列表页面，选择待销毁的实例，单击**更多操作** > **销毁**。如下图所示：



4. 在弹出的窗口中，根据实际需求，选择**立即销毁**或者**定时销毁**，单击**下一步**。如下图所示：



立即销毁：如果选择立即销毁，该实例相关数据会被清除且不可恢复。

定时销毁：如果选择定时销毁，您需要设置一个定时销毁的时间，到期后实例会被定时销毁，且数据不可恢复。

5. 确认销毁的实际及相关资源，单击**开始销毁**。

重置密码

最近更新时间：2023-12-25 14:44:10

操作场景

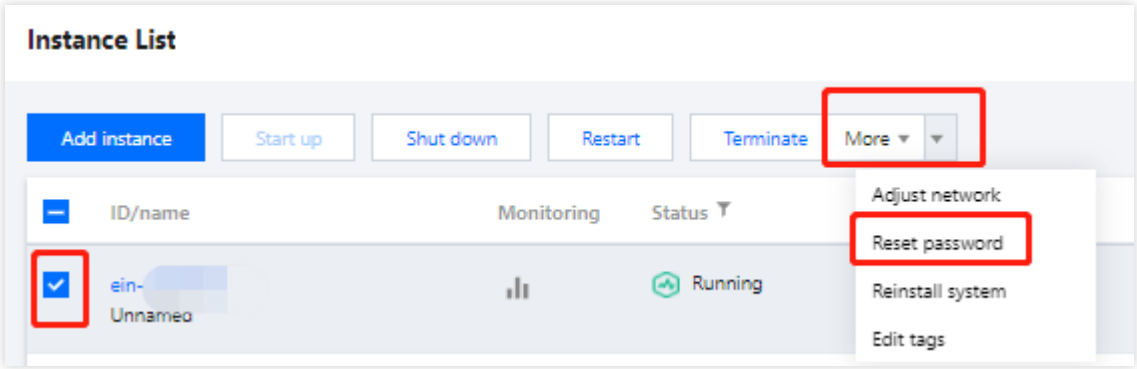
如果您遗忘了密码，您可以在控制台上重新设置实例的登录密码。本文指导您如何在控制台上修改实例的登录密码。

注意事项

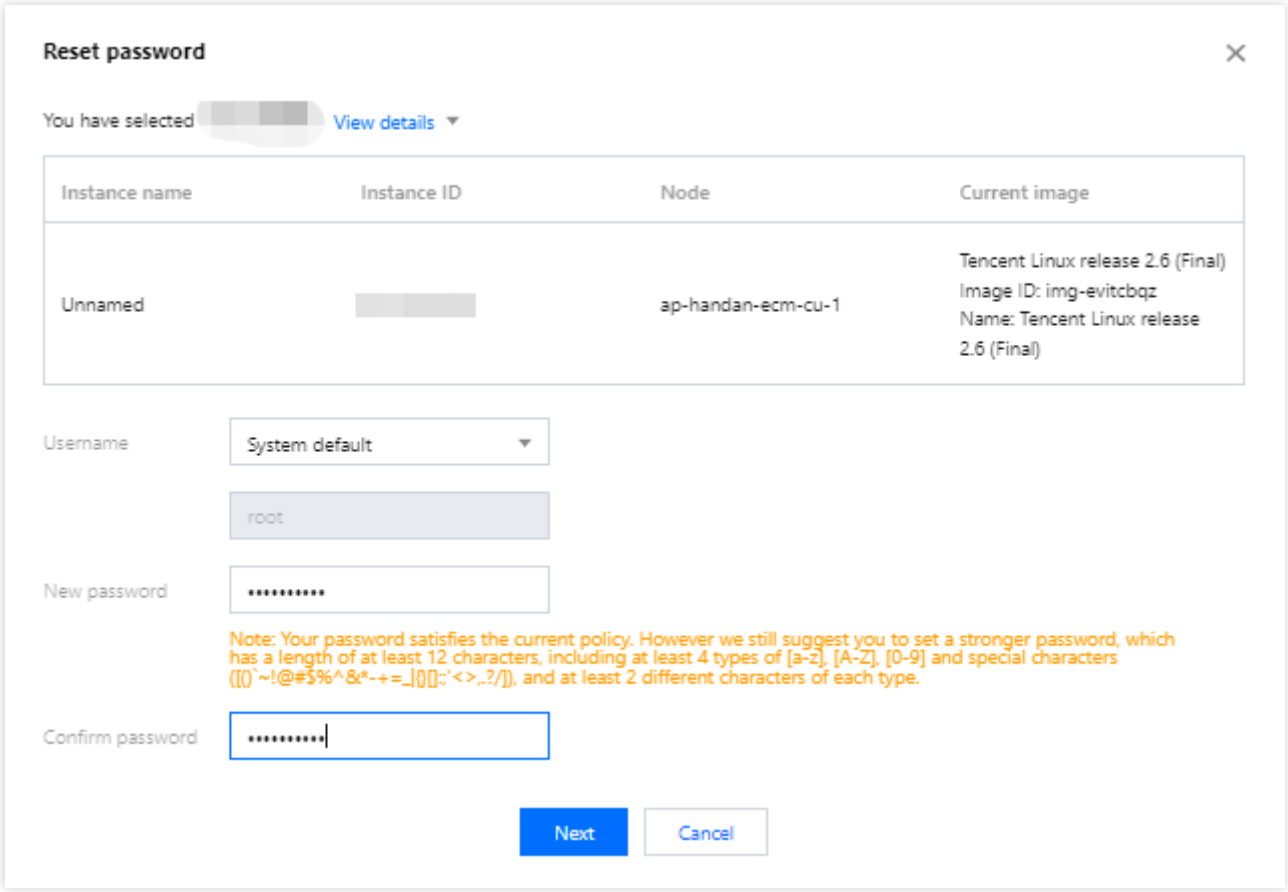
在重置密码过程中会关闭服务器。为了避免数据丢失，请提前规划好操作时间，建议在业务低谷时进行此操作，将影响降到最低。
重置 Linux 实例的密码要求：长度8-30位，不能以“/”开头且需包含大写字母、小写字母、数字0-9、符号任意三项。
重置 Windows 实例的密码要求：长度12-30位，不能以“/”开头且需包含大写字母、小写字母、数字0-9、符号任意三项，不能包含用户名。

操作步骤

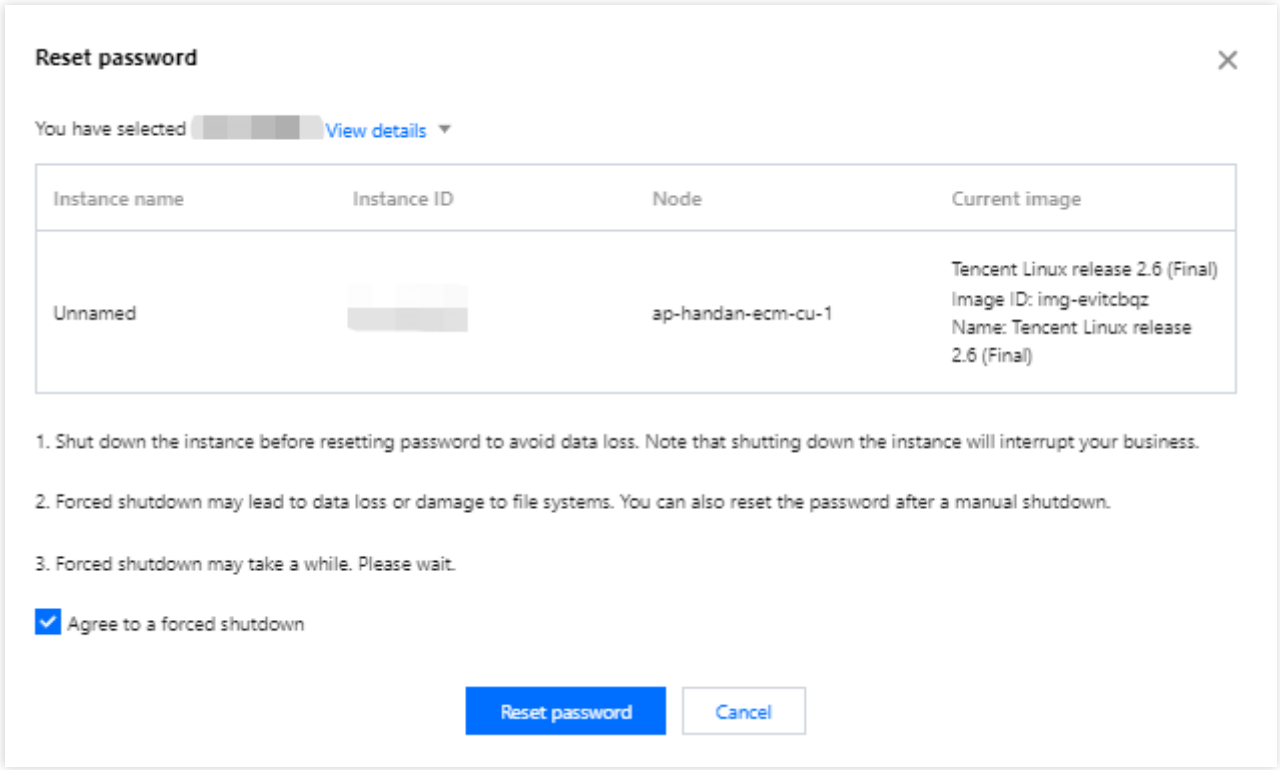
1. 登录 边缘计算机器控制台。
2. 在左侧导航栏中，选择**实例列表**。
3. 在实例列表页面，勾选待重置密码的实例，单击**更多操作** > **重置密码**。



4. 在弹出的窗口中，确认需要重置密码的用户名（如 Linux 实例的用户名为 `root` 、Windows 实例的用户名为 `Administrator` ），输入对应的**新密码**和 **确认密码**，单击**下一步**。如下图所示：



5. 勾选**同意强制关机**，单击**重置密码**，完成重置。如下图所示：



查看实例监控数据

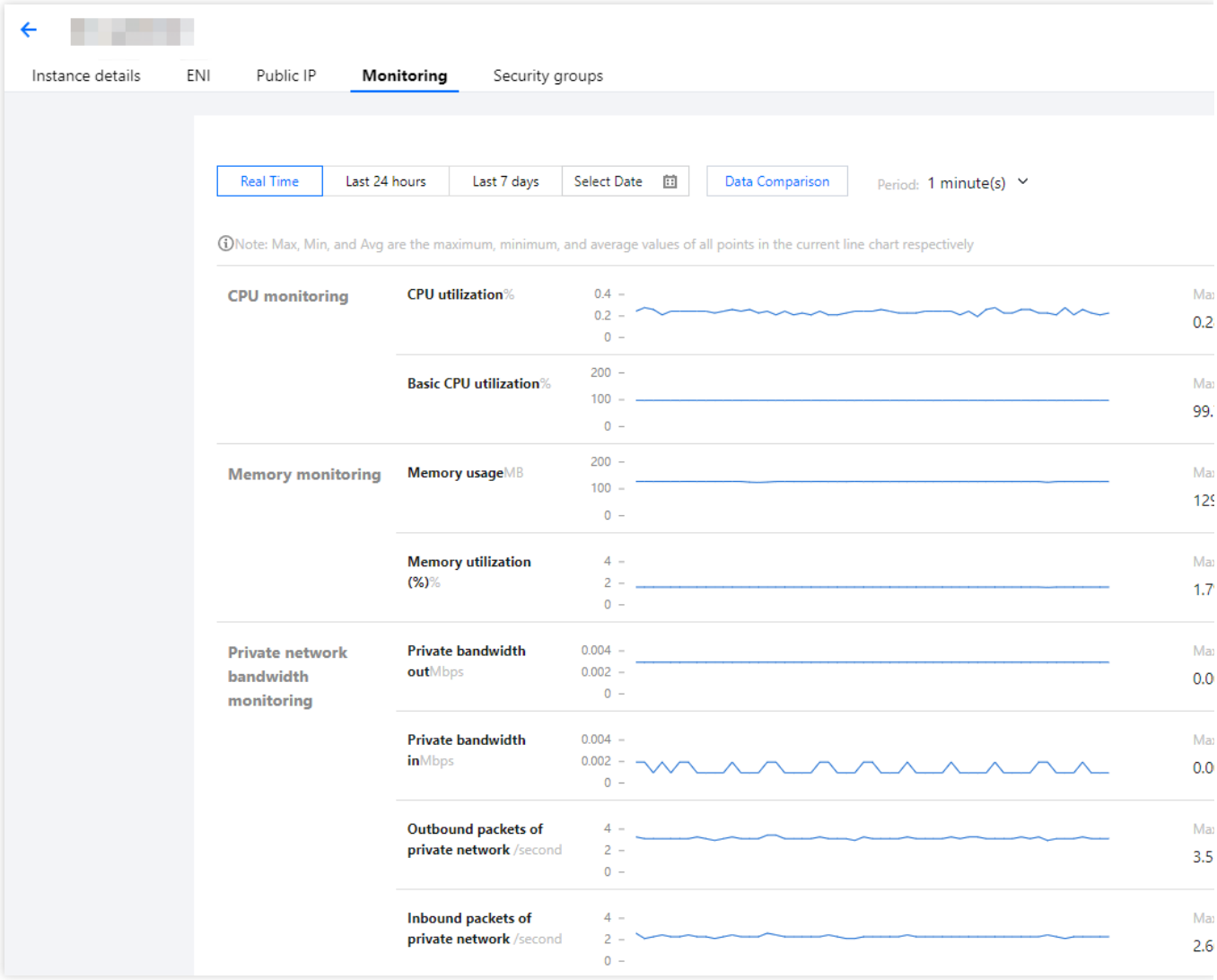
最近更新时间：2023-12-25 14:44:22

操作场景

本文指导您如何在控制台上查看当前实例的监控数据。

操作步骤

1. 登录 边缘计算机器控制台。
2. 在左侧导航栏中，选择**实例列表**。
3. 在实例列表页面，找到需要查看监控数据的实例，单击 ID/实例名，进入实例详情页面。
4. 选择**监控**页签，进入监控页面，即可查看边缘计算机器实例的 CPU、内存、内网带宽、外网带宽以及硬盘使用情况的监控信息。如下图所示：



在监控页面，您还可以选择时间维度筛选数据和导出数据，方便您更轻松的管理边缘计算机器实例。

配置实例安全组

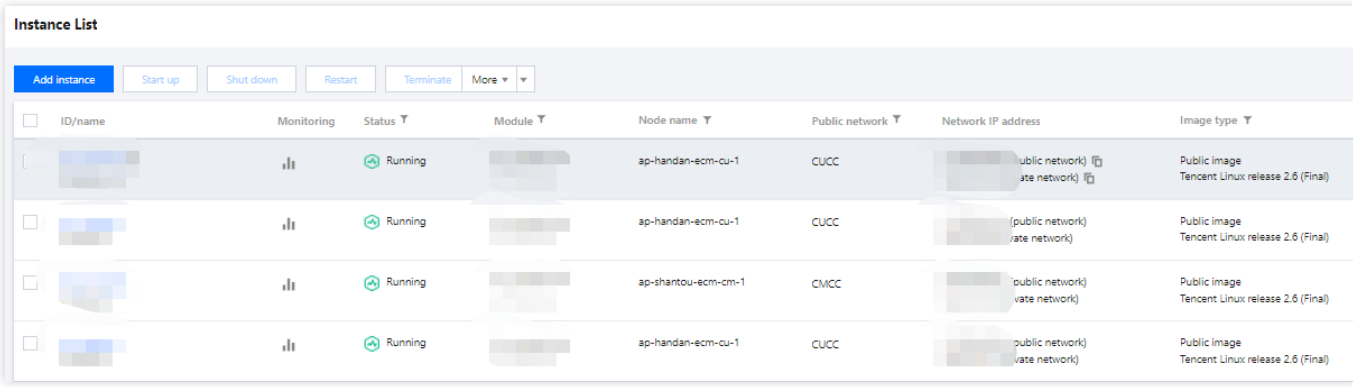
最近更新时间：2023-12-26 09:33:01

操作场景

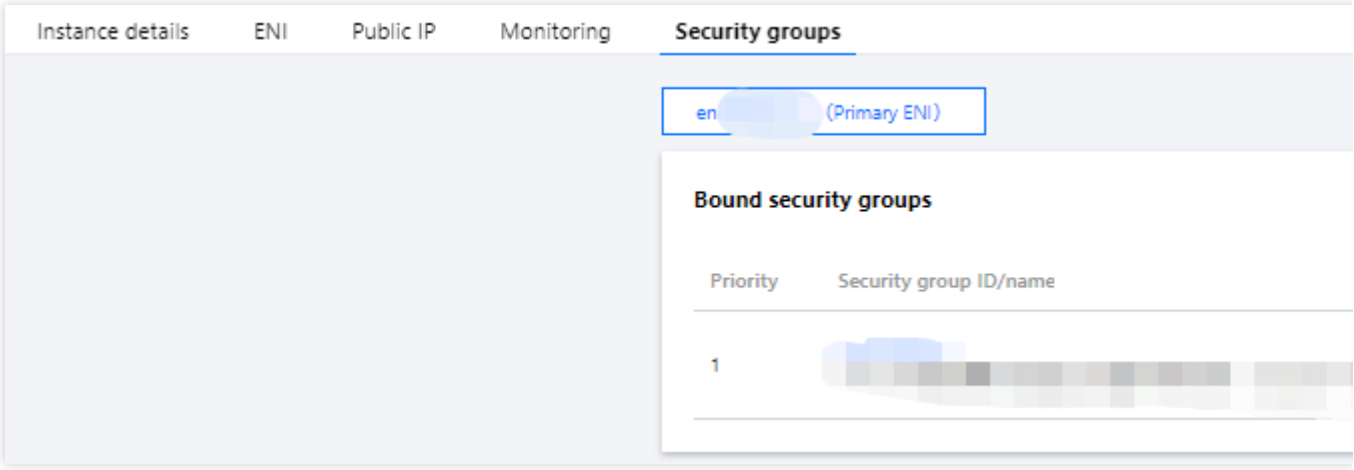
安全组是一种虚拟防火墙，具备有状态的数据包过滤功能，用于设置单台或多台边缘实例的网络访问控制，是腾讯云提供的重要的网络安全隔离手段。
创建边缘实例时必须要为实例配置安全组，如果您已创建的实例默认使用的模块安全组或自定义配置的安全组无法满足您的业务场景时，可参考本文更换实例所属的安全组。

操作步骤

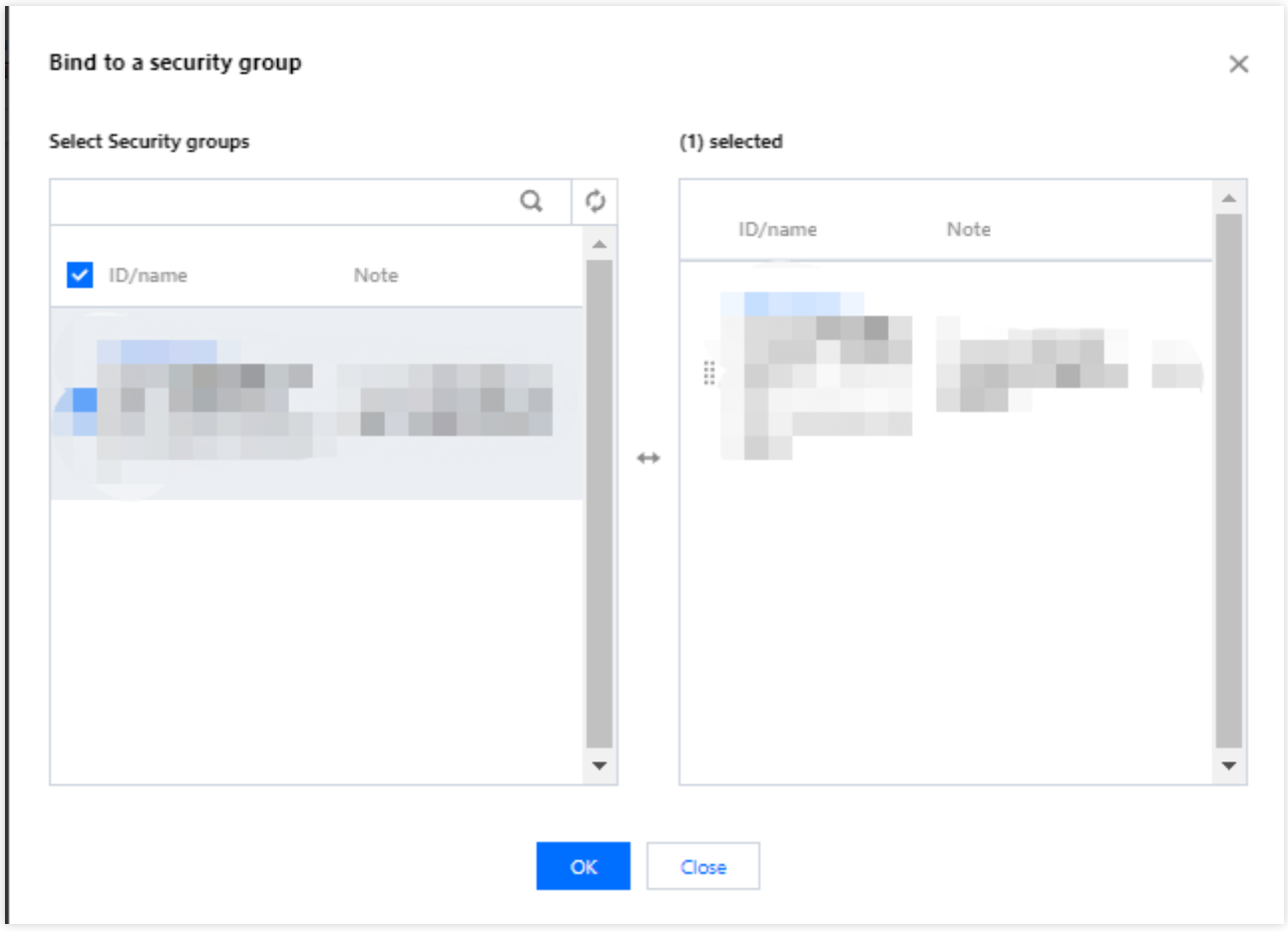
1. 登录 边缘计算机器控制台。
2. 选择左侧导航栏中的 实例列表，进入**实例列表**页面。
3. 在**实例列表**页面中，选择需重新配置安全组边缘实例所在行右侧的**更多** > **配置安全组**。如下图所示：



即可跳转至实例管理页**安全组**页签，进行安全组绑定。
4. 在**安全组**页签的**已绑定安全组**，单击**绑定**。如下图所示：



5. 在弹出的**配置安全组**窗口中，根据实际需求勾选需要绑定的安全组，单击【**确定**即可完成绑定。如下图所示：



管理安全组

安全组概述

最近更新时间：2023-12-25 14:45:52

安全组是一种虚拟防火墙，具备有状态的数据包过滤功能，用于设置边缘计算机器（Edge Computing Machine, ECM）实例、边缘负载均衡 ELB、弹性网卡等资源的网络访问控制，控制实例级别的出入流量，是重要的网络安全隔离手段。

您可以通过配置安全组规则，允许或禁止安全组内的实例的出流量和入流量。

边缘计算机器的安全组功能与中心云的公共安全组功能逻辑上隔离，云服务器等中心云产品无法关联边缘计算机器产品下的安全组，边缘计算机器下的产品（例如边缘模块、ECM 实例及 ELB）等资源亦无法直接关联中心云的公共安全组。如果您在公共安全组中有已创建的安全组策略，可通过 导入安全组 进行对应的数据导入，导入后会重新生成面向边缘产品的安全组数据。

说明：

中心云泛指腾讯云在地域与可用区下的各类产品，详情请参见 云服务器概述、地域和可用区 及 安全组。

安全组特点

安全组是一个逻辑上的分组，您可以将具有相同网络安全隔离需求的 ECM 实例、ELB、弹性网卡等资源加到同一个安全组内。

关联了同一安全组的实例间默认不会互通，您需要添加相应的允许规则。

安全组是有状态的，创建后无规则时默认拒绝所有流量，对于您已允许的入站/出站流量，都将自动允许其流出，反之亦然。

您可以随时修改安全组的规则，新规则立即生效。

使用限制

ECM 安全组的使用限制及配额如下表所示：

功能描述	数量
用户创建安全组上限	200
安全组出（入）站规则数	100
每个安全组关联的 ECM 实例数	2000
每个安全组关联的 ECM 模块数	100

每个 ECM 资源（实例，弹性网卡等）关联的安全组个数	5
每个 ECM 模块关联的安全组个数	5
每个安全组可以引用的安全组 ID 的个数	10

安全组规则

组成部分

安全组规则包括如下组成部分：
来源：源数据（入站）或目标数据（出站）的 IP。
协议类型和协议端口：协议类型如 TCP、UDP、HTTP 等。
策略：允许或拒绝。

规则优先级

安全组内规则具有优先级。规则优先级通过规则在列表中的位置来表示，列表顶端规则优先级最高，最先应用；列表底端规则优先级最低。
若有规则冲突，则默认应用位置更前的规则。
当有流量入/出绑定某安全组的实例时，将从安全组规则列表顶端的规则开始逐条匹配至最后一条。如果成功匹配某条规则，则对应该规则的流量不会继续往下匹配。

多个安全组

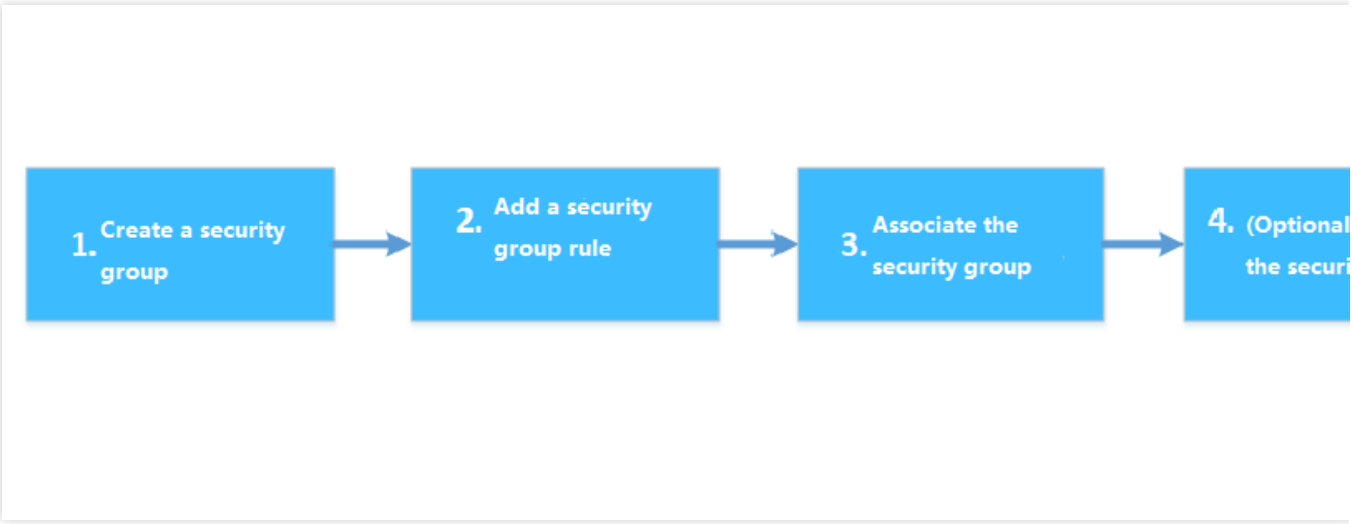
一个实例可以绑定一个或多个安全组，当实例绑定多个安全组时，多个安全组将按照从上到下依次匹配执行，您可以随时调整安全组的优先级。

安全组模板

新建安全组时，您可以选择腾讯云为您提供的两种安全组模版：
放通全部端口模板：将会放通所有出入站流量。
放通常用端口模板：将会放通 TCP 22端口（Linux SSH 登录），80、443端口（Web 服务），3389端口（Windows 远程登录）、 ICMP 协议（Ping）、放通内网。

使用流程

安全组的使用流程如下图所示：


1. Create a security group
2. Add a security group rule
3. Associate the security group
4. (Optional

创建安全组

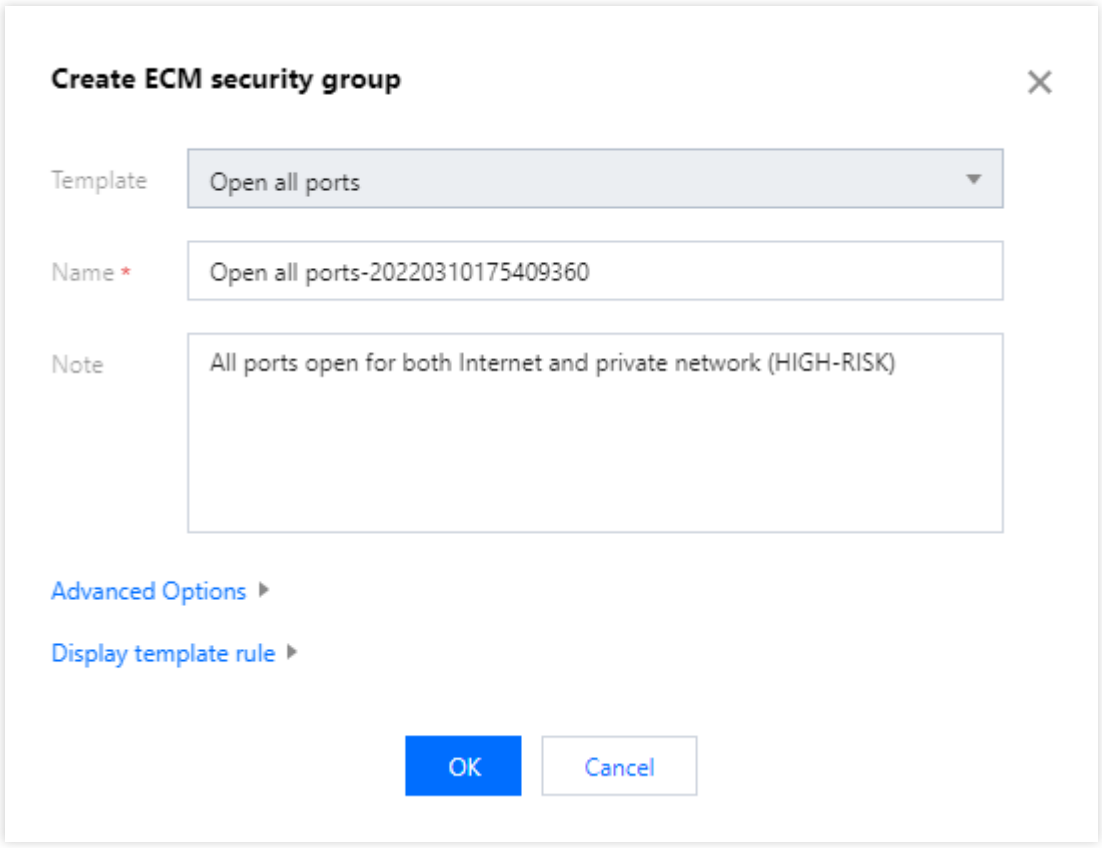
最近更新时间：2023-12-25 14:46:04

操作场景

安全组是边缘实例的虚拟防火墙，每台边缘实例必须至少关联一个安全组。在您创建边缘实例时，如果您还未创建过安全组，腾讯云提供了“**放通全部端口**”和“**放通22，80，443，3389端口和ICMP协议**”两种模版为您创建一个安全组。详情请参见 安全组概述。
您也可以根据本文描述，自行创建安全组。本文介绍通过控制台创建一个边缘计算机器下的安全组。

操作步骤

1. 登录边缘计算机器控制台，选择左侧导航中的**边缘网络** > **安全组**。
2. 在**安全组**管理页面中，单击**新建**。
3. 在弹出的**新建边缘安全组**窗口中，参考以下信息进行配置。如下图所示：



模板：根据安全组中的边缘实例需要部署的服务，选择合适的模板，简化安全组规则配置。如下表所示：

模板	说明	场景
放通全部端口	默认放通全部端口到公网和内网，具有一定安全风险。	-
放通22，80，443，3389端口和ICMP协议	默认放通22，80，443，3389端口和 ICMP 协议，内网全放通。	安全组中的实例需要部署 Web 服务。
自定义	安全组创建成功后，按需自行添加安全组规则。具体操作请参见 添加安全组规则。	-

名称：自定义设置安全组名称。

备注：自定义，简短地描述安全组，便于后期管理。

高级选项：展开后可为安全组添加标签。

显示模板规则：展开后可查看当前安全组已具有规则。

4. 单击**确定**，完成安全组的创建。

导入安全组

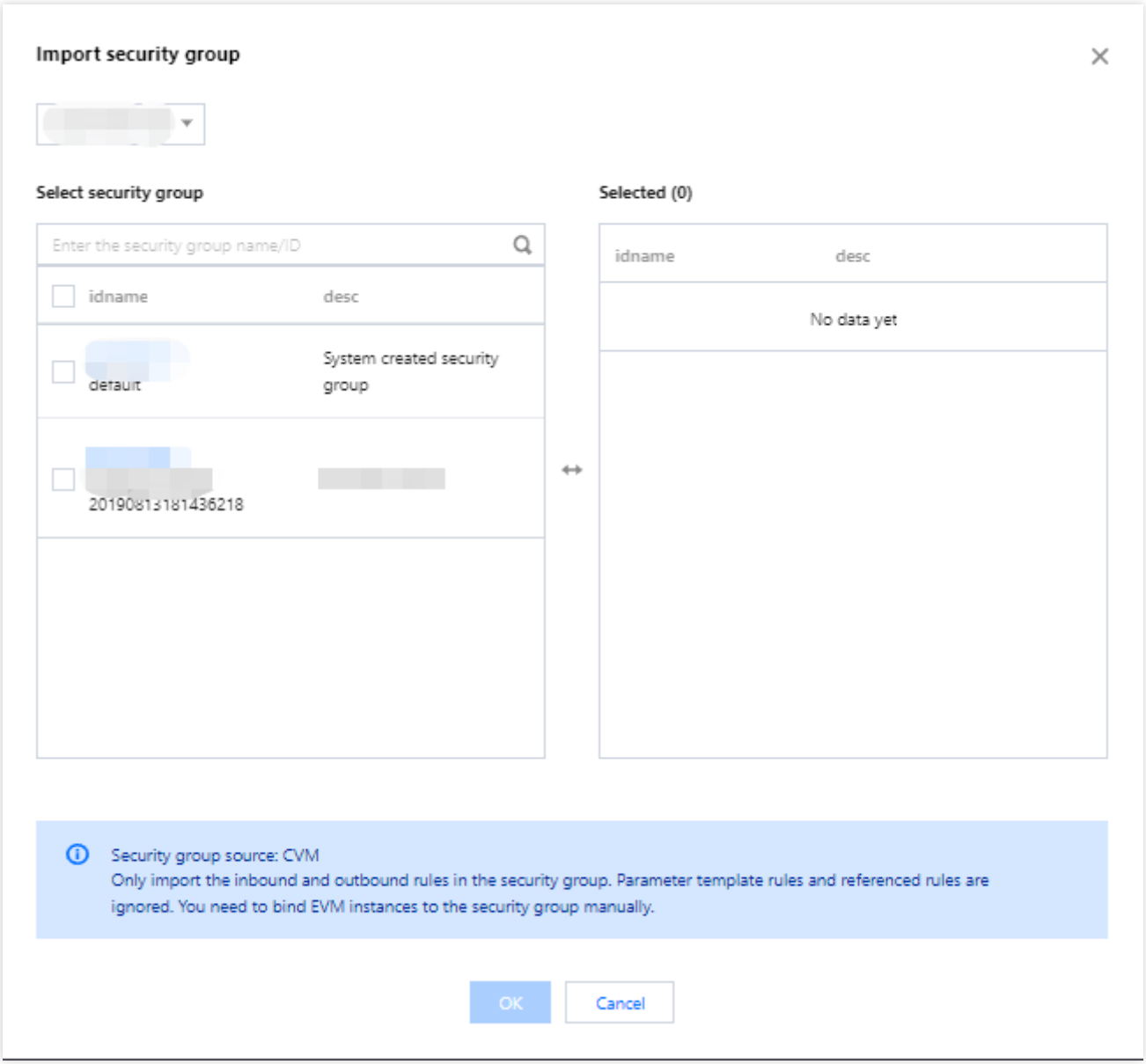
最近更新时间：2023-12-25 14:46:15

操作场景

边缘计算机器（Edge Computing Machine，ECM）的安全组功能与中心云的公共安全组功能逻辑上隔离，云服务器等中心云产品无法关联边缘计算机器产品下的安全组，边缘计算机器下的产品（如边缘模块、ECM 实例及边缘负载均衡 ELB）等资源亦无法直接关联中心云的公共安全组。如果您在公共安全组中有已创建的安全组策略，可通过本功能进行对应的数据导入，导入后会重新生成一条面向边缘产品的安全组数据。
您还可以自行创建安全组，详情请参见 创建安全组。

操作步骤

1. 登录边缘计算机器控制台，选择左侧导航中的**边缘网络** > **安全组**。
2. 在“安全组”管理页面，单击**导入**。
3. 在弹出的**导入安全组**窗口中，进行以下操作。如下图所示：



1. 选择对应的中心云地域（Region），界面会展示该地域下的所有安全组。
2. 选择需要导入的安全组数据。

注意：

当前无法导入金融地区及海外地区的安全组数据。

仅导入安全组出入站规则，规则内包含的参数模板规则及安全组嵌套规则将进行过滤处理。

3. 单击**确定**即可对中心云的公共安全组进行导入，安全组管理列表产生新的数据。

关联实例至安全组

最近更新时间：2023-12-25 14:46:56

说明：

安全组支持关联边缘计算机器实例、边缘负载均衡 ELB、弹性网卡等资源，本文以关联边缘计算机器为例。

操作场景

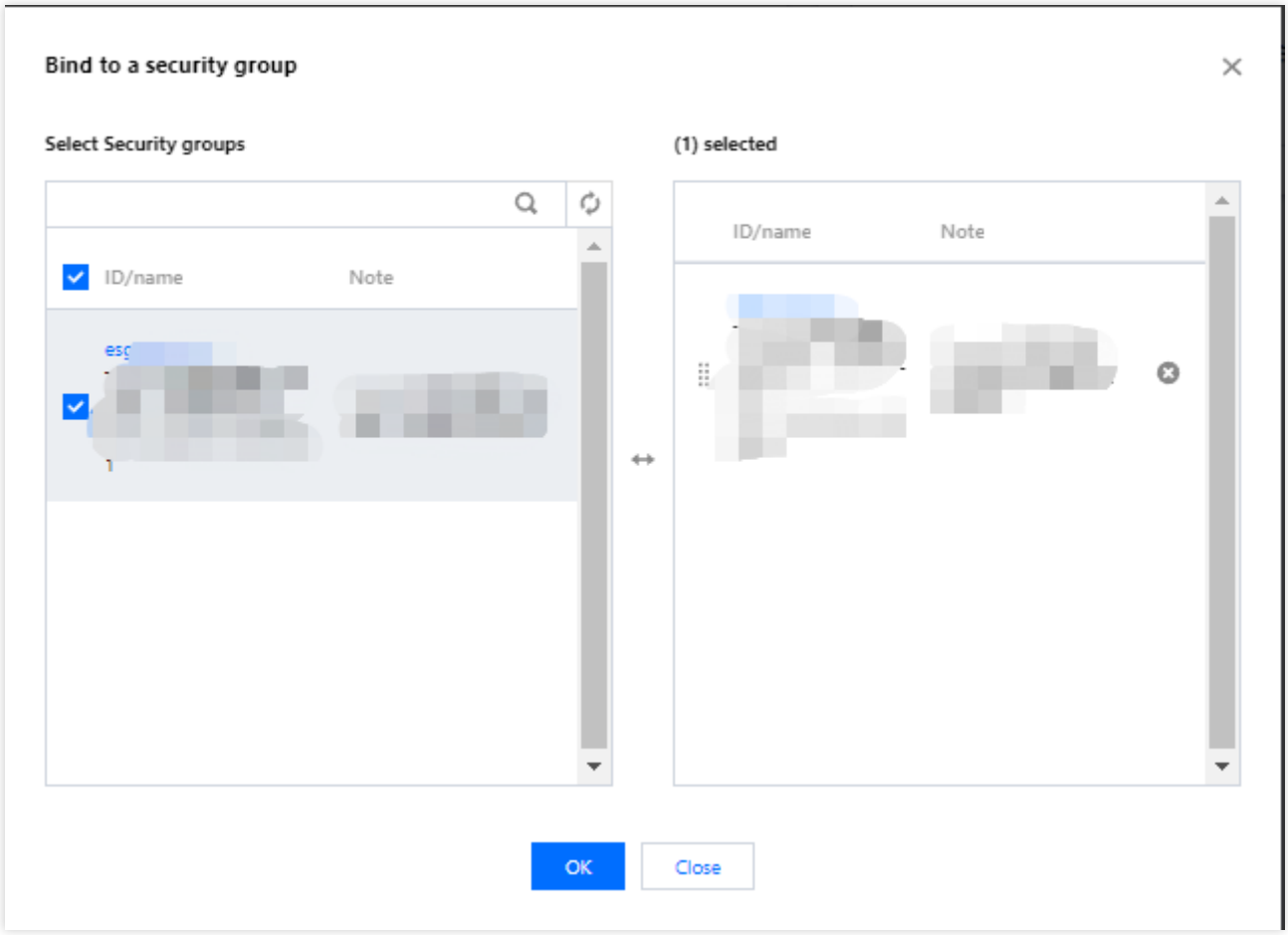
安全组用于设置单台或多台边缘实例的网络访问控制，是重要的网络安全隔离手段。您可以根据业务需要，将边缘实例关联一个或多个安全组。下面将指导您如何在控制台上将边缘实例关联至安全组。

前提条件

已创建边缘计算机器实例。

操作步骤

1. 登录边缘计算机器控制台，选择左侧导航中的**边缘网络** > **安全组**。
2. 在**安全组**管理页面，选择需关联实例安全组所在行右侧的**更多** > **管理实例**。
3. 在**关联实例**页面中，单击**新增关联**。
4. 在弹出的**关联实例**窗口中，完成以下操作。如下图所示：



5. 筛选对应的节点地区，界面会展示该地域下的所有边缘实例，默认展示全部地区的实例数据。
6. 筛选对应的所属模块，界面会展示该模块下的所有边缘实例，默认展示全部模块的实例数据。
7. 通过实例 ID、实例名称，选择需要关联的边缘实例。
8. 单击**确定**即可进行关联操作。

后续操作

如果您想查看您已创建的所有安全组，您可以查询安全组列表，并根据资源属性进行过滤。
具体操作请参见 查看安全组。
如果您不希望您的边缘实例属于某个或某几个安全组，您可以将边缘实例移出安全组。
具体操作请参见 移出安全组。
如果您的业务不再需要一个或多个安全组，您可以删除安全组。安全组删除后，该安全组内的所有安全组规则将同时被删除。
具体操作请参见 删除安全组。

查看安全组

最近更新时间：2023-12-25 14:47:10

操作场景

如果您想查看您创建的所有安全组，您可以通过以下操作查看安全组列表。

操作步骤

查看所有安全组

1. 登录边缘计算机器控制台，选择左侧导航中的**边缘网络** > **安全组**。
2. 在**安全组**管理页面，即可查看创建的所有安全组。

查看指定安全组

您还可以通过安全组管理页面的搜索功能，筛选您需要查看的安全组。

1. 登录边缘计算机器控制台，选择左侧导航中的**边缘网络** > **安全组**。
2. 在“安全组”管理页面的列表的右上方，单击搜索文本框，选择以下任一方式查询您需要查看的安全组。

选择**安全组名称**，输入安全组名称，按

，即可筛选出该安全组名称对应的安全组。

选择**安全组ID**，输入安全组 ID，按

，即可筛选出该安全组 ID 对应的安全组。

选择**安全组标签**，输入标签名称，按

，即可筛选出该标签下所有的安全组。

其他操作

如需了解更多查看指定安全组的语法，可在搜索文本框中单击

查看相关语法。

移出安全组

最近更新时间：2023-12-25 14:47:24

操作场景

如果您不希望您的边缘实例属于某个或某几个安全组，您可以根据业务需要，将边缘实例移出安全组。

前提条件

边缘计算机器实例已加入两个或两个以上安全组。

操作步骤

1. 登录边缘计算机器控制台，选择左侧导航中的**边缘网络** > **安全组**。
2. 在**安全组**管理页面，选择需移出安全组所在行右侧的**更多** > **管理实例**。
3. 在**关联实例**页面，选择需要移出的实例，单击**移出安全组**。
4. 在弹出的提示框中，单击**确定**即可移出安全组。

删除安全组

最近更新时间：2023-12-25 14:47:38

操作场景

如果您的业务已经不再需要一个或多个安全组，您可以删除安全组。安全组删除后，该安全组内所有安全组规则同时被删除。

前提条件

请确认待删除的安全组不存在关联的实例。若存在关联的实例，请先将关联实例移出安全组，否则删除安全组操作不可执行。具体操作请参见 移出安全组。

操作步骤

1. 登录边缘计算机器控制台，选择左侧导航中的**边缘网络** > **安全组**。
2. 在**安全组**管理页面，选择需删除安全组所在行右侧的**更多** > **删除**。
3. 在弹出的提示框中，单击**确定**即可删除该安全组。

调整安全组优先级

最近更新时间：2023-12-26 09:30:34

操作场景

一个边缘计算机器实例可以绑定一个或多个安全组，当边缘计算机器实例绑定多个安全组时，多个安全组将按照优先级顺序（如1、2）依次匹配执行，您可以根据以下操作调整安全组的优先级。

前提条件

边缘计算机器实例已加入两个或两个以上安全组。

操作步骤

1. 登录边缘计算机器控制台，选择左侧导航栏中的实例列表，进入**实例列表**页面。
2. 在**实例列表**页面，单击边缘计算机器实例 ID，进入详情页面。
3. 选择**安全组**页签，进入安全组管理页面。
4. 在右侧**已绑定安全组**模块中，单击**排序**，选中安全组右侧的

并上下拖动，调整安全组的优先级，位置越靠上，安全组的优先级越高。
5. 完成调整后，单击**保存**即可。

管理安全组规则
添加安全组规则

最近更新时间：2023-12-25 14:57:30

操作场景

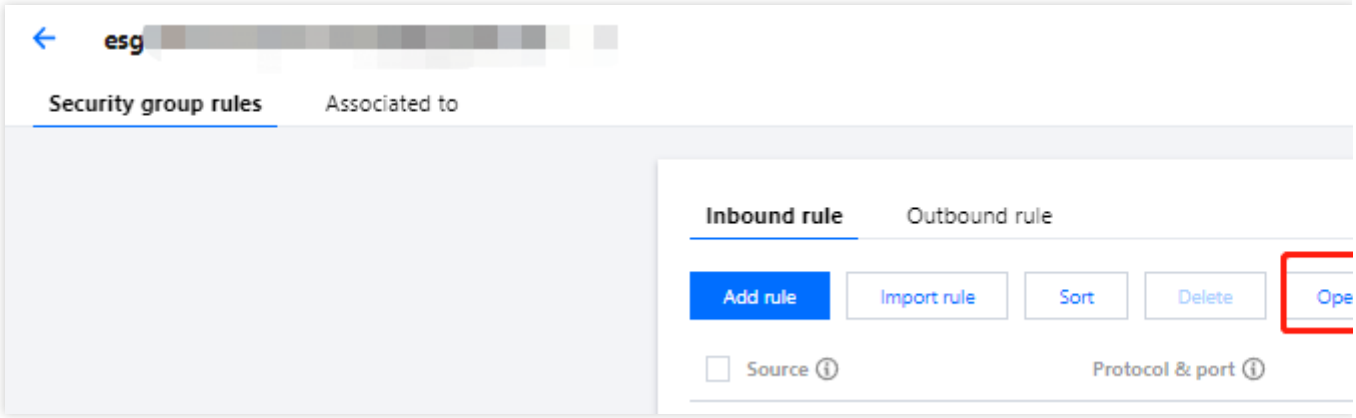
安全组用于管理是否放行来自公网或者内网的访问请求。为安全起见，安全组入方向大多采取拒绝访问策略。如果您在创建安全组时选择了“放通全部端口”模板或者“放通22，80，443，3389端口和ICMP协议”模板，系统将会根据选择的模板类型给部分通信端口自动添加安全组规则。详情请参见 安全组概述。
本文指导您通过添加安全组规则，允许或禁止安全组内的边缘实例及资源对公网或私网的访问。

前提条件

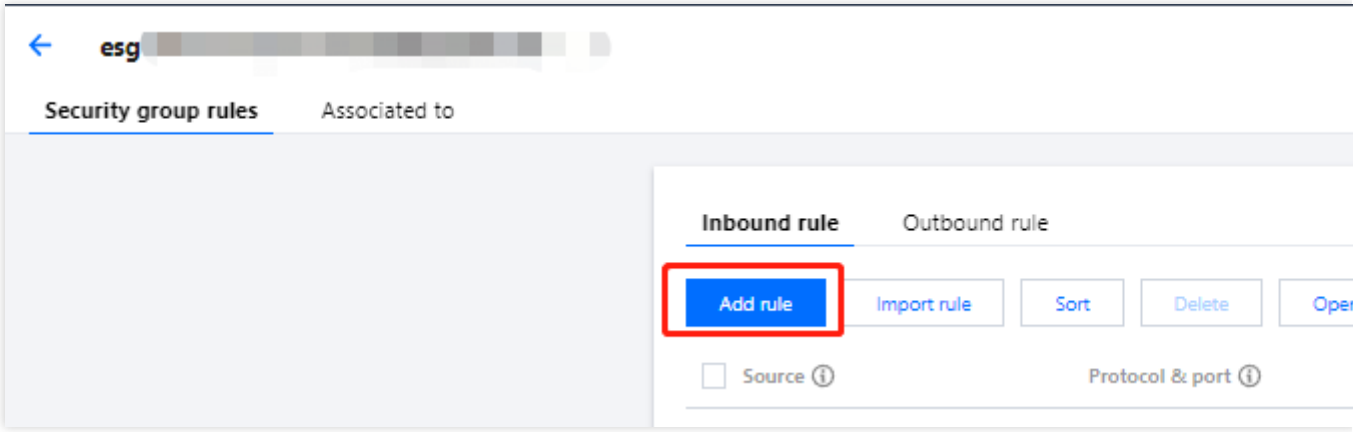
您已经创建一个安全组。具体操作请参见 创建安全组。
您已经知道边缘实例需要允许或禁止哪些公网或内网的访问。更多安全组规则设置的相关应用案例，请参见 安全组应用案例。

操作步骤

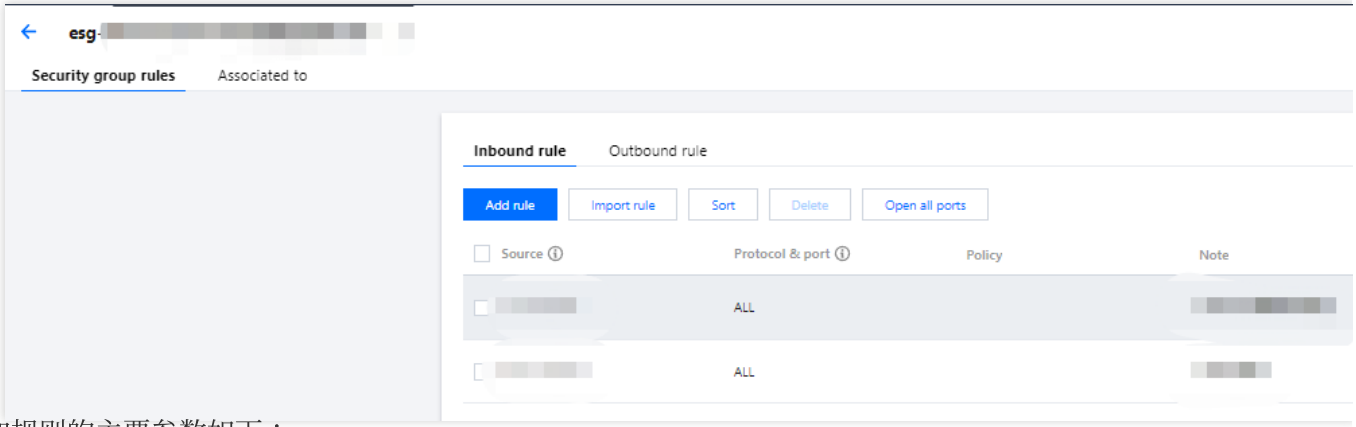
1. 登录边缘计算机器控制台，选择左侧导航中的**边缘网络** > **安全组**。
2. 在**安全组**管理页面，选择需设置规则的安全组所在行右侧的**修改规则**。
3. 在**安全组规则**页签中，单击**入站/出站规则**，并根据实际需求选择以下任意一种方式完成操作。
方式一：单击**一键放通**，并在弹出窗口中进行确认。此方式适用于无需设置 ICMP 协议规则，并通过22，3389，ICMP，80，443，20，21端口便能完成操作的场景。如下图所示：



方式二：单击**添加规则**，并在弹出窗口中进行配置，详情请参见 步骤5。此方式适用于需要设置多种通信协议的场景，例如 ICMP 协议。如下图所示：



方式三：在安全组规则页面，可按需修改入站/出站规则。选择**入站/出站规则**页签，根据期望添加规则的位置，单击已有规则所在行右侧的**插入 > 向上/向下插入一行**，并参考 步骤5 快速配置规则。如下图所示：



4. 添加规则的主要参数如下：

类型：默认选择“自定义”，您也可以选择其他系统规则模板，例如 “Windows 登录”模板、“Linux 登录”模板、“Ping”模板、**HTTP(80)**模板和 **HTTPS(443)**模板等。

来源：流量的源（入站规则） 或目标（出站规则），请指定以下选项：

指定的源/目标	说明
单个 IPv4 地址或 IPv4 地址范围	用 CIDR 表示法（如203.0.113.0、203.0.113.0/24或者0.0.0.0/0，其中0.0.0.0/0代表匹配所有 IPv4 地址）。

协议端口：填写协议类型和端口范围。例如，UDP:53、TCP:80,443。

策略：默认选择“允许”。

允许：放行该端口相应的访问请求。

拒绝：直接丢弃数据包，不返回任何回应信息。

备注：自定义，简短地描述规则，便于后期管理。

5. 单击**完成**，完成安全组入站规则的添加。

6. 在安全组规则页面，单击“出站规则”，并参考 步骤4 - 步骤5，完成所需安全组出站规则的添加。

查看安全组规则

最近更新时间：2023-12-25 14:58:05

操作场景

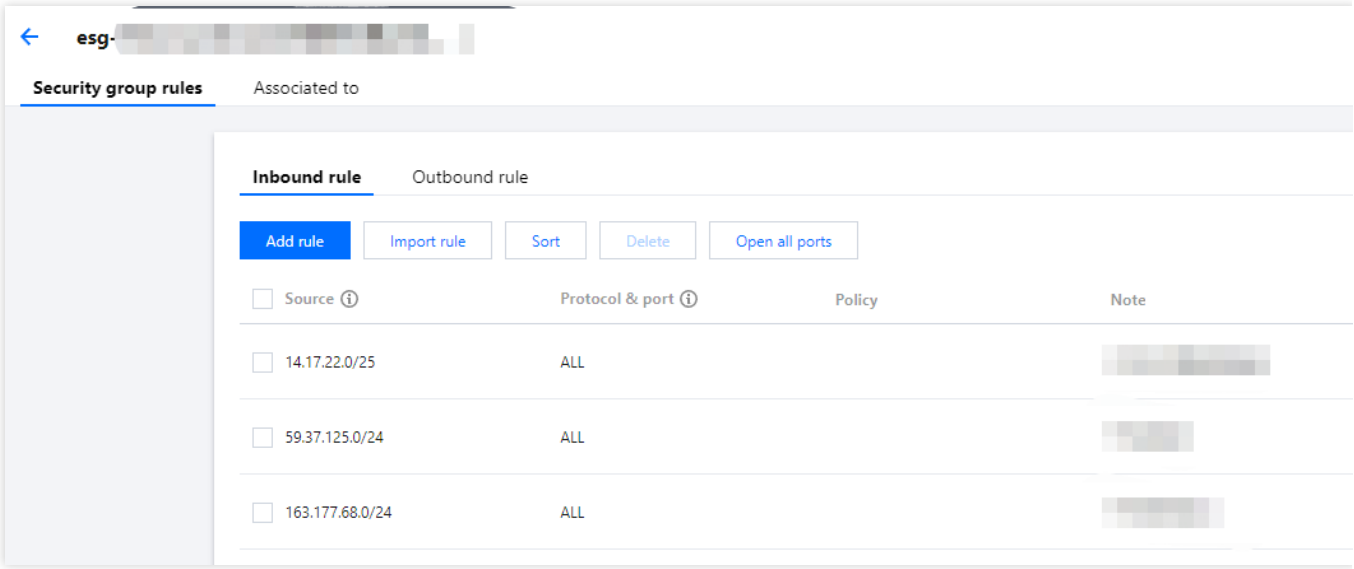
添加安全组规则后，您可以通过控制台查看安全组规则的详细信息。

前提条件

已创建安全组，并已在该安全组中添加了安全组规则。
如何创建安全组和添加安全组规则，请参见 创建安全组 和 添加安全组规则。

操作步骤

1. 登录边缘计算机器控制台，选择左侧导航中的**边缘网络** > **安全组**。
2. 进入**安全组**管理页面，单击需要查看规则的安全组 ID/名称，或该安全组所在行右侧的**修改规则**，进入安全组规则页面。
3. 在安全组规则页面，单击**入站/出站规则**页签，可以查看到入站/出站的安全组规则。如下图所示：



修改安全组规则

最近更新时间：2023-12-25 14:59:37

操作场景

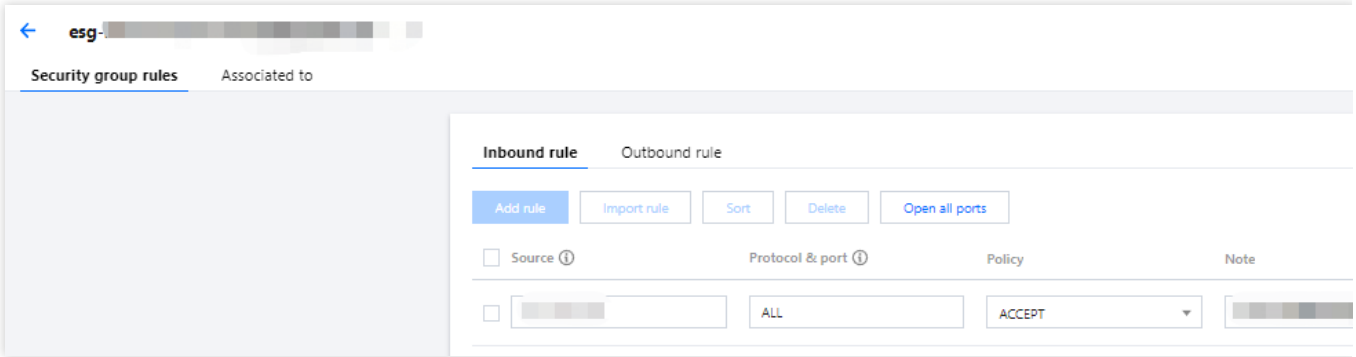
安全组规则设置不当会造成严重的安全隐患，例如安全组规则对特定端口的访问不做限制。您可以通过修改安全组中不合理的安全组规则，保证边缘计算机器实例的网络安全。本文指导您如何修改安全组规则。

前提条件

已创建安全组，并已在该安全组中添加了安全组规则。
如何创建安全组和添加安全组规则，请参见 创建安全组 和 添加安全组规则。

操作步骤

1. 登录边缘计算机器控制台，选择左侧导航中的**边缘网络** > **安全组**。
2. 进入“**安全组**管理页面，单击需要查看规则的安全组 ID/名称，或该安全组所在行右侧的**修改规则**，进入安全组规则页面。
3. 在安全组规则页面，根据需要修改安全组规则所属的方向（入站/出站），单击**入站/出站规则**页签。
4. 找到需要修改的安全组规则，单击该规则所在行右侧的**编辑**。
5. 可参考 规则参数说明 对已有规则进行修改，修改完成后单击**保存**即可。如下图所示：



删除安全组规则

最近更新时间：2023-12-25 14:59:51

操作场景

如果您不再需要某个安全组规则，可以参考本文进行安全组规则删除操作。

前提条件

已创建安全组，并已在该安全组中添加了安全组规则。
如何创建安全组和添加安全组规则，请参见 创建安全组 和 添加安全组规则。
已确认边缘计算机器实例不需要允许/禁止哪些公网访问或内网访问。

操作步骤

1. 登录边缘计算机器控制台，选择左侧导航中的**边缘网络** > **安全组**。
2. 在**安全组**管理页面中，单击需删除规则安全组所在行右侧的**修改规则**，进入安全组规则页面。
3. 在安全组规则页面，根据需要删除安全组规则所属的方向（入站/出站），单击**入站/出站规则**页签。
4. 找到需要删除的安全组规则，单击该规则所在行右侧的**删除**。
也可勾选规则左侧的多选框，单击顶部的**删除**进行批量删除操作。
5. 在弹出的提示框中，单击**确定**即可完成删除操作。

导出安全组规则

最近更新时间：2023-12-25 15:00:05

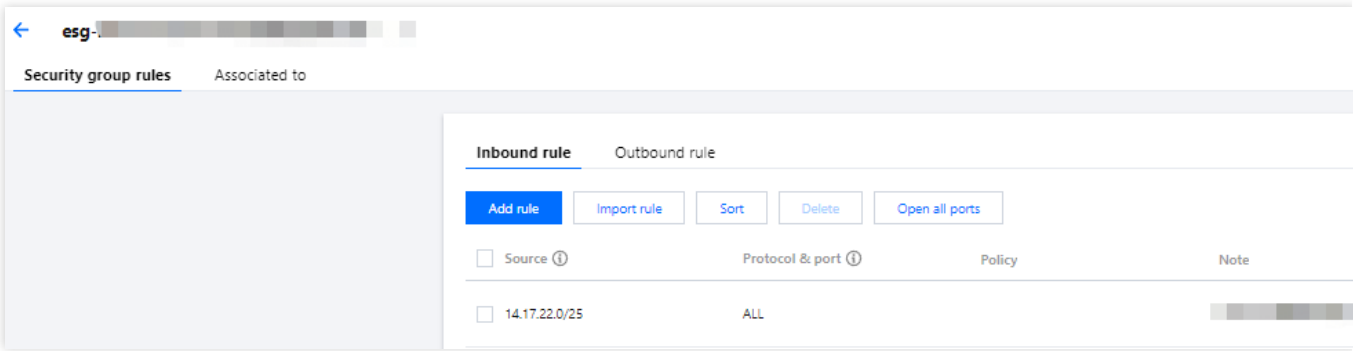
操作场景

安全组规则支持导出功能，您可以将安全组下的安全组规则导出，用于本地备份。

操作步骤

1. 登录边缘计算机器控制台，选择左侧导航中的**边缘网络** > **安全组**。
2. 在**安全组**管理页面，单击需要导出规则的安全组 ID/名称，进入安全组规则页面。
3. 在安全组规则页面，根据需要导出安全组规则所属的方向（入站/出站），单击**入站/出站规则**页签。
4. 在入站/出站规则页签下，单击右上方的

，下载并保存安全组规则文件至本地。如下图所示：



导入安全组规则

最近更新时间：2023-12-25 15:00:17

操作场景

安全组规则支持导入功能。您可以将导出的安全组规则文件导入到安全组中，快速创建或恢复安全组规则。

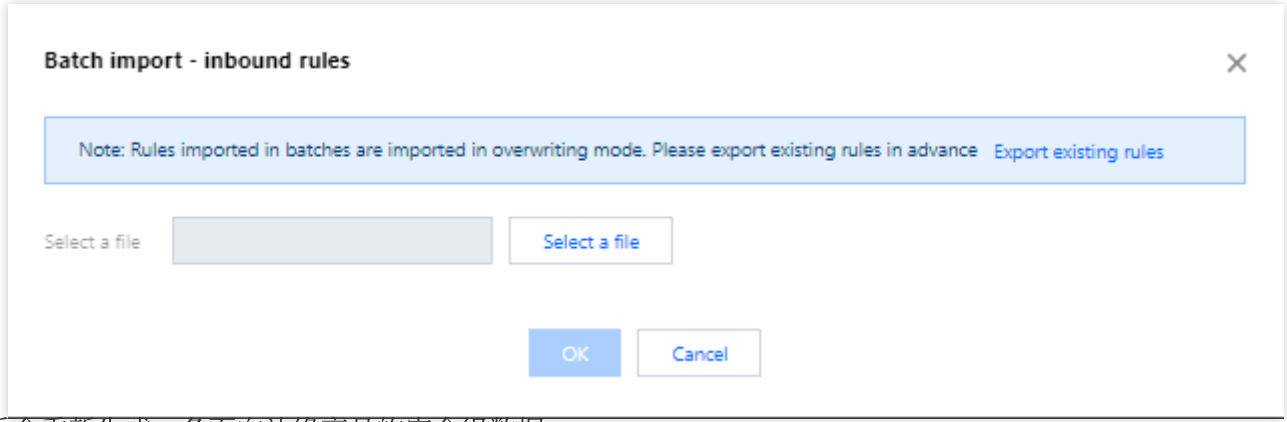
操作步骤

1. 登录边缘计算机器控制台，选择左侧导航中的**边缘网络** > **安全组**。
2. 在**安全组**管理页面，单击需导入规则的安全组 ID/名称，或该安全组所在行右侧的**修改规则**，进入安全组规则页面。
3. 在安全组规则页面，根据需要导入安全组规则所属的方向（入站/出站），单击**入站/出站规则**页签。
4. 在**入站/出站规则**页签中，单击**导入规则**。
5. 在弹出的**批量导入-入站/出站规则**窗口中，选择已编辑好的入站/出站规则模板文件，单击**确定**即可。如下图所示：

说明：

如果需要导入规则的安全组下已存在安全组规则，建议您先导出现有规则，否则导入新规则时，将覆盖原有规则。

如果需要导入规则的安全组下没有安全组规则，建议您先下载模板，待编辑好模板文件后，再将文件导入。



导入后会重新生成一条面向边缘产品的安全组数据。

安全组应用案例

最近更新时间：2023-12-26 10:08:01

安全组的设置用来管理边缘实例是否可以被访问，您可以通过配置安全组的入站和出站规则，设置您的边缘实例是否可以被访问以及访问其他网络资源。
默认情况下，安全组的入站规则和出站规则如下：
为了数据安全，安全组的入站规则为拒绝策略，禁止外部网络的远程访问。如果您需要您的边缘实例被外部访问，则需要放通相应端口的入站规则。
安全组的出站规则用于设置您的边缘实例是否可以访问外部网络资源。如果您选择 “放通全部端口” 或 “放通22，80，443，3389端口和 ICMP 协议”，安全组出站规则为全部放通。如果您选择自定义安全组规则，出站规则默认为全部拒绝，您需要放通相应端口的出站规则来访问外部网络资源。

常见应用场景

本文介绍了几个常见的安全组应用场景，如果以下场景可以满足您的需求，可直接按照场景中的推荐配置进行安全组的设置。

场景一：允许 SSH 远程连接 Linux 边缘实例

案例：您创建了一台 Linux 边缘实例，并希望可以通过 SSH 远程连接到边缘实例。
解决方法：添加安全组规则 时，在 “类型” 中选择 **Linux 登录**，开通22号协议端口，放通 Linux SSH 登录。
您还可以根据实际需求，放通全部 IP 或指定 IP（IP 段），配置可通过 SSH 远程连接到边缘实例的 IP 来源。

方向	类型	来源	协议端口	策略
入方向	Linux 登录	全部 IP：0.0.0.0/0 指定 IP：输入您指定的 IP 或 IP 段	TCP:22	允许

场景二：允许 RDP 远程连接 Windows 边缘实例

案例：您创建了一台 Windows 边缘实例，并希望可以通过 RDP 远程连接到边缘实例。
解决方法：添加安全组规则 时，在 “类型” 中选择 “Windows 登录”，开通3389号协议端口，放通 Windows 远程登录。
您还可以根据实际需求，放通全部 IP 或指定 IP（IP 段），配置可通过 RDP 远程连接到边缘实例的 IP 来源。

方向	类型	来源	协议端口	策略
入方向	Windows 登录	全部 IP：0.0.0.0/0 指定 IP：输入您指定的 IP 或 IP 段	TCP:3389	允许

场景三：允许公网 Ping 服务器

案例：您创建了一台边缘实例，希望可以测试这台边缘实例和其他边缘实例之间的通信状态是否正常。

解决方法：使用 ping 程序进行测试。即在 添加安全组规则 时，将 “类型” 选择为 “Ping”，开通 ICMP 协议端口，允许其他边缘实例通过 ICMP 协议访问该边缘实例。

您还可以根据实际需求，放通全部 IP 或指定 IP（IP 段），配置允许通过 ICMP 协议访问该边缘实例的 IP 来源。

方向	类型	来源	协议端口	策略
入方向	Ping	全部 IP：0.0.0.0/0 指定 IP：输入您指定的 IP 或 IP 地址段	ICMP	允许

场景四：Telnet 远程登录

案例：您希望可以通过 Telnet 远程登录边缘实例。

解决方法：如需通过 Telnet 远程登录边缘实例，则需在 添加安全组规则 时，配置以下安全组规则：

方向	类型	来源	协议端口	策略
入方向	自定义	全部 IP：0.0.0.0/0 指定 IP：输入您指定的 IP 或 IP 地址段	TCP:23	允许

场景五：放通 Web 服务 HTTP 或 HTTPS 访问

案例：您搭建了一个网站，希望用户可以通过 HTTP 或者 HTTPS 的方式访问您搭建的网站。

解决方法：如需通过 HTTP 或者 HTTPS 的方式访问网站，则需在 添加安全组规则 时，根据实际需求配置以下安全组规则：

允许公网上的所有 IP 访问该网站

方向	类型	来源	协议端口	策略
入方向	HTTP（80）	0.0.0.0/0	TCP:80	允许
入方向	HTTPS（443）	0.0.0.0/0	TCP:443	允许

允许公网上的部分 IP 访问该网站

方向	类型	来源	协议端口	策略
入方向	HTTP（80）	允许访问您网站的 IP 或 IP 地址段	TCP:80	允许
入方向	HTTPS（443）	允许访问您网站的 IP 或 IP 地址段	TCP:443	允许

场景六：允许外部 IP 访问指定端口

案例：您部署业务后，希望指定的业务端口（例如：1101）可以被外部访问。

解决方法：添加安全组规则 时，在 “类型” 中选择 “自定义”，开通1101号协议端口，允许外部访问指定的业务端口。您还可以根据实际需求，放通全部 IP 或指定 IP（IP 段），允许访问指定的业务端口的 IP 来源。

方向	类型	来源	协议端口	策略
入方向	自定义	全部 IP：0.0.0.0/0 指定 IP：输入您指定的 IP 或 IP 地址段	TCP:1101	允许

场景七：拒绝外部 IP 访问指定端口

案例：您部署业务后，希望指定的业务端口（例如：1102）不被外部访问。

解决方法：添加安全组规则 时，在 “类型” 中选择 “自定义”，配置1102号协议端口，将 “策略” 设置为 “拒绝”，拒绝外部访问指定的业务端口。

方向	类型	来源	协议端口	策略
入方向	自定义	全部 IP：0.0.0.0/0 指定 IP：输入您指定的 IP 或 IP 地址段	TCP:1102	拒绝

场景八：只允许边缘实例访问特定外部 IP

案例：您希望您的边缘实例只能访问外部特定的 IP 地址。

解决方法：参考如下配置，增加如下两条出方向的安全组规则。

允许实例访问特定公网 IP 地址

禁止实例以任何协议访问所有公网 IP 地址

注意：

允许访问的规则优先级应高于拒绝访问的规则优先级。

方向	类型	来源	协议端口	策略
出方向	自定义	允许边缘实例访问的特定公网 IP 地址	需使用的协议类型和端口	允许
出方向	自定义	0.0.0.0/0	ALL	拒绝

场景九：拒绝边缘实例访问特定外部 IP

案例：您不希望您的边缘实例可以访问外部特定的 IP 地址。

解决方法：参考如下配置，添加安全组规则。

方向	类型	来源	协议端口	策略
出方向	自定义	拒绝实例访问的特定公网 IP 地址	ALL	拒绝

场景十：使用 FTP 上传或下载文件

案例：您需要使用 FTP 软件向边缘实例上传或下载文件。

解决方法：参考如下配置，添加安全组规则。

方向	类型	来源	协议端口	策略
入方向	自定义	0.0.0.0/0	TCP:20-21	允许

多场景组合

在实际的场景中，可能需要根据业务需求配置多个安全组规则。例如，同时配置入站或者出站规则。一台边缘实例可以绑定一个或多个安全组，当边缘实例绑定多个安全组时，多个安全组将按照从上到下依次匹配执行。您可以随时调整安全组的优先级，安全组规则的优先级说明请参考 规则优先级说明。

服务器常用端口

最近更新时间：2023-12-25 15:00:46

如下是服务器常用端口介绍，关于 Windows 下更多的服务应用端口说明，请参考微软官方文档（Windows 的服务概述和网络端口要求）。

端口	服务	说明
21	FTP	FTP 服务器所开放的端口，用于上传、下载。
22	SSH	22端口就是 SSH 端口，用于通过命令行模式远程连接 Linux 系统服务器。
25	SMTP	SMTP 服务器所开放的端口，用于发送邮件。
80	HTTP	用于网站服务例如 IIS、Apache、Nginx 等提供对外访问。
110	POP3	110端口是为 POP3（邮件协议 3）服务开放的。
137、138、139	NETBIOS 协议	其中137、138是 UDP 端口，当通过网上邻居传输文件时用这个端口。而139端口：通过这个端口进入的连接试图获得 NetBIOS/SMB 服务。这个协议被用于 Windows 文件和打印机共享和 SAMBA。
143	IMAP	143端口主要是用于“Internet Message Access Protocol”v2（Internet 消息访问协议，简称 IMAP），和 POP3 一样，是用于电子邮件的接收的协议。
443	HTTPS	网页浏览端口，能提供加密和通过安全端口传输的另一种 HTTP。
1433	SQL Server	1433端口，是 SQL Server 默认的端口，SQL Server 服务使用两个端口：TCP-1433、UDP-1434。其中1433用于供 SQL Server 对外提供服务，1434用于向请求者返回 SQL Server 使用了哪个 TCP/IP 端口。
3306	MySQL	3306端口，是 MySQL 数据库的默认端口，用于 MySQL 对外提供服务。
3389	Windows Server Remote Desktop Services（远程桌面服务）	3389端口是 Windows Server 远程桌面的服务端口，可以通过这个端口，用“远程桌面”连接工具来连接到远程的服务器。
8080	代理端口	8080端口同80端口，是被用于 WWW 代理服务的，可以实现网页浏览，经常在访问某个网站或使用代理服务器的时候，会加上“:8080”端口号。另外 Apache Tomcat web server 安装后，默认的服务端口就是8080。

管理镜像

最近更新时间：2023-12-26 10:09:11

操作场景

边缘计算机器提供了公有镜像，包含基础操作系统和腾讯云提供的初始化组件，所有用户均可使用。当您需要快速创建更多包含相同配置和应用的实例时，可通过镜像制作功能制作自定义镜像，并在创建实例时使用该镜像。边缘计算机器支持通过导入镜像的操作，从中心云可用区将自定义镜像导入到边缘计算机器实例。本文指导您如何在控制台中导入镜像，以及管理镜像。

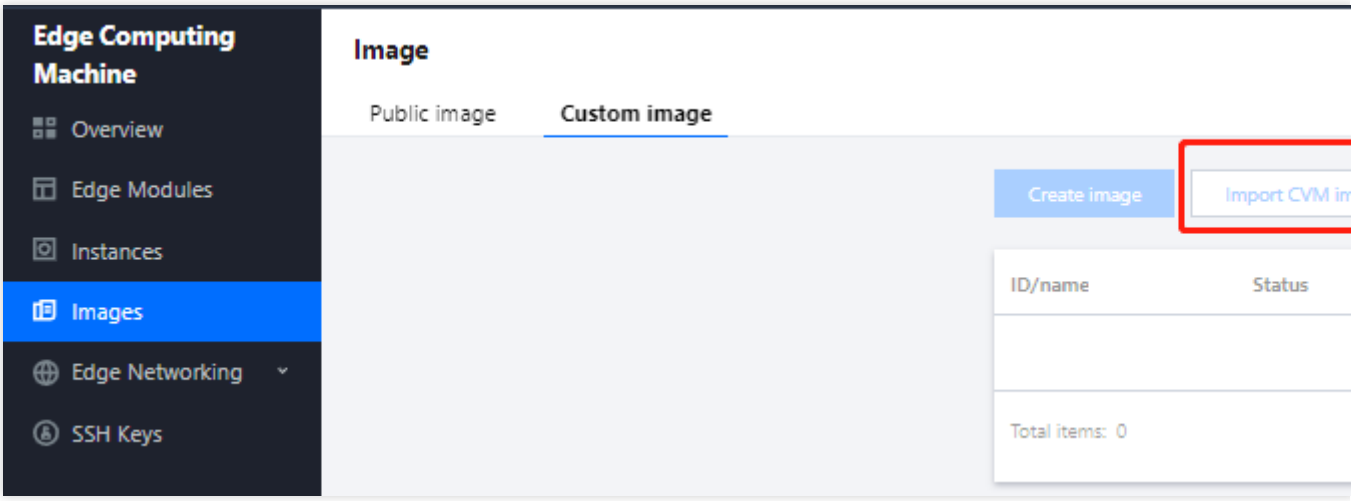
前提条件

已在中心云（即云服务器）的可用区中创建自定义镜像。

操作步骤

导入镜像

1. 登录 边缘计算机器控制台。
2. 在左侧导航栏中，选择**镜像**。
3. 在镜像页面，单击**导入镜像**。 如下图所示：



4. 在弹出的窗口中，选择待导入镜像的所在区域、操作系统、系统架构和镜像ID/名称，单击**确定**。

说明：

边缘计算机器目前支持同时保留最多10个自定义镜像。

成功导入后，即表示您已将云服务器的数据同步至边缘计算机器中。

删除镜像

1. 登录 边缘计算机器控制台。
2. 在左侧导航栏中，选择**镜像**。
3. 在镜像页面，选择待删除的镜像，单击操作栏的**删除**。

说明：

执行此操作前，请确认是否存在边缘模块使用该镜像。如果存在，该镜像将无法删除。

4. 在弹出的提示框中，单击**确定**。

编辑标签

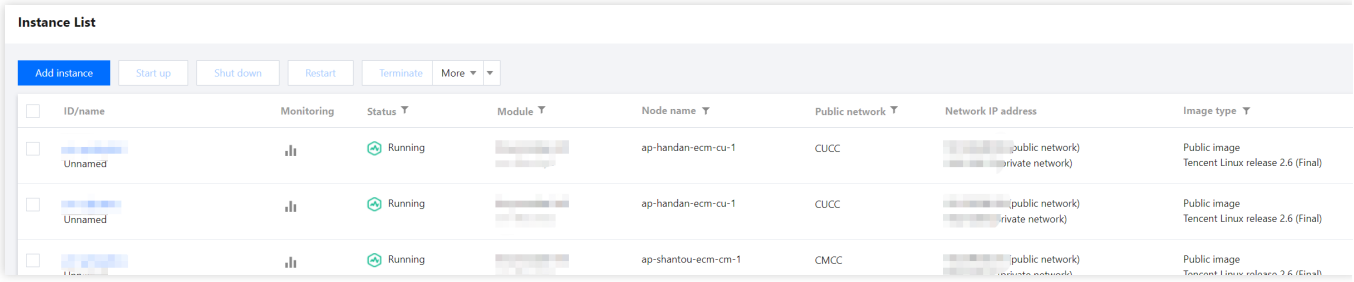
最近更新时间：2023-12-26 09:28:25

操作场景

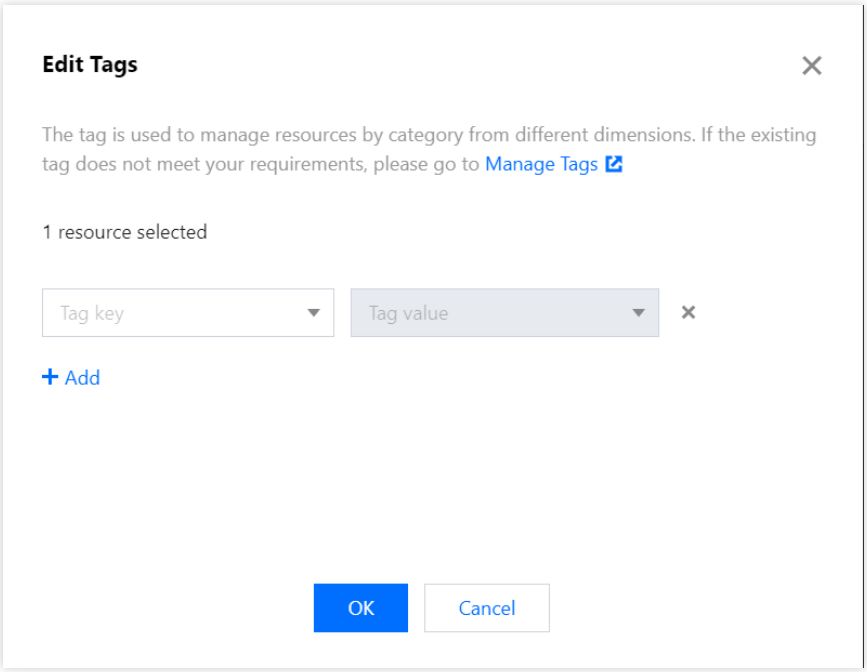
标签可以帮助您从各种维度（例如业务，用途，负责人等）方便的对边缘计算机器资源进行分类管理。本文介绍如何在控制台中为边缘计算机器实例添加标签。

操作步骤

1. 登录 边缘计算机器控制台。
2. 在左侧导航栏中，选择**实例列表**。
3. 在实例列表页面，选择待调整网络的实例，单击**更多操作** > **编辑标签**。



4. 在弹出的窗口中，根据实际需求，输入标签键和标签值，单击**确定**。


Edit Tags
The tag is used to manage resources by category from different dimensions. If the existing tag does not meet your requirements, please go to Manage Tags
1 resource selected
Tag key
Tag value
Add
OK
Cancel

EIP直通

最近更新时间：2023-12-26 09:27:32

操作场景

创建边缘计算机器实例时，默认已配置 EIP 直通。如您的边缘计算机器实例未配置 EIP 直通，可通过执行 EIP 直通脚本进行配置。本文指导您如何在边缘计算机器实例上配置 EIP 直通脚本，并指导您在误操作删除脚本时，该如何恢复 EIP 直通脚本。

注意事项

目前仅支持在 Linux 实例上配置 EIP 直通。
EIP 直通脚本需在 CentOS 6 及以上版本和 Ubuntu 系统上运行。

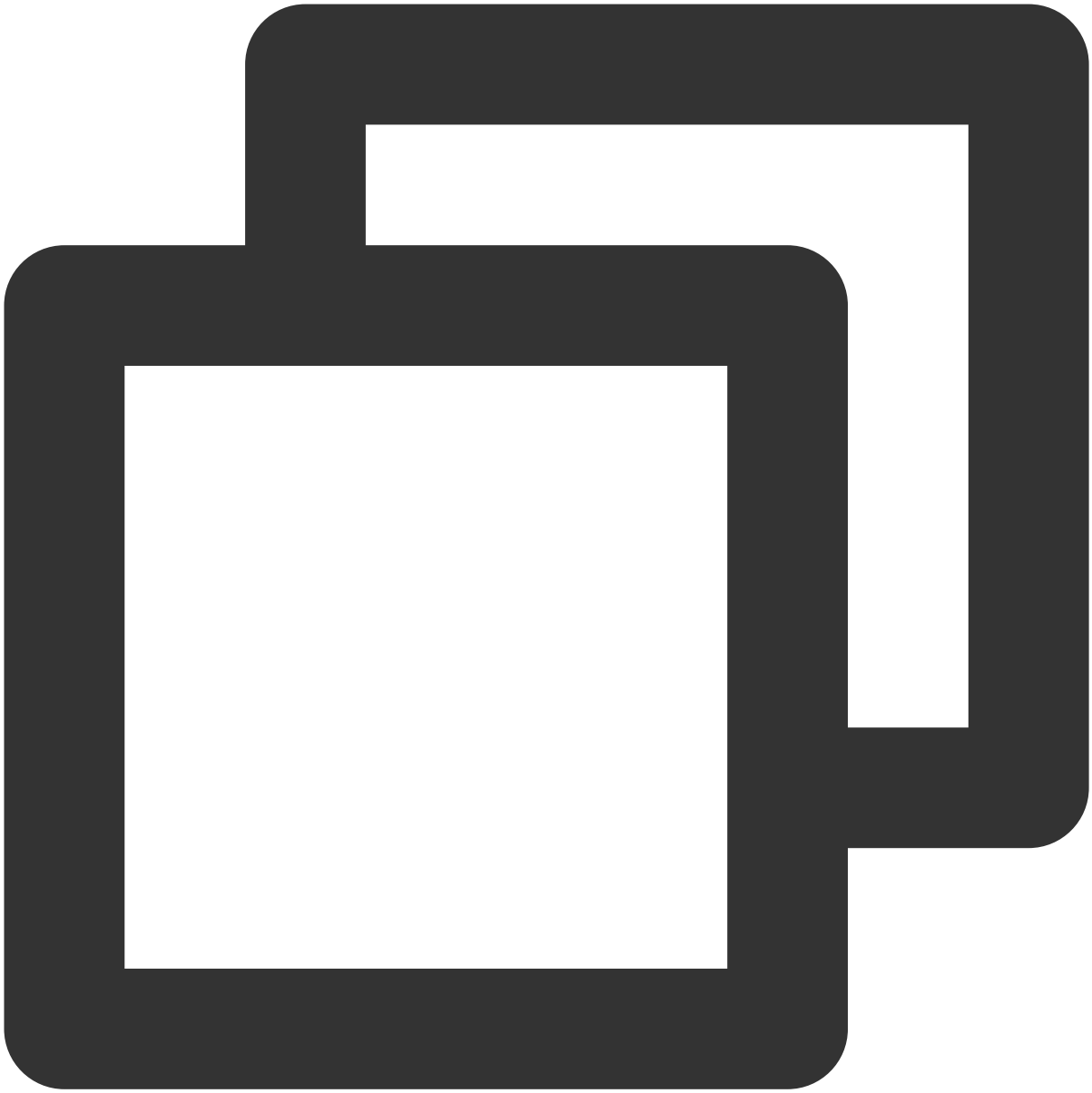
前提条件

已创建边缘计算实例，及获取公网 IP。
已获取实例的管理员号和对应的密码。
Linux 实例的内网 IP 和弹性公网 IP 需均在主网卡（eth0）上。
如果主网卡绑定的公网 IP 不是弹性 IP，则需要先转换为弹性 IP。

操作步骤

下载 EIP 直通脚本

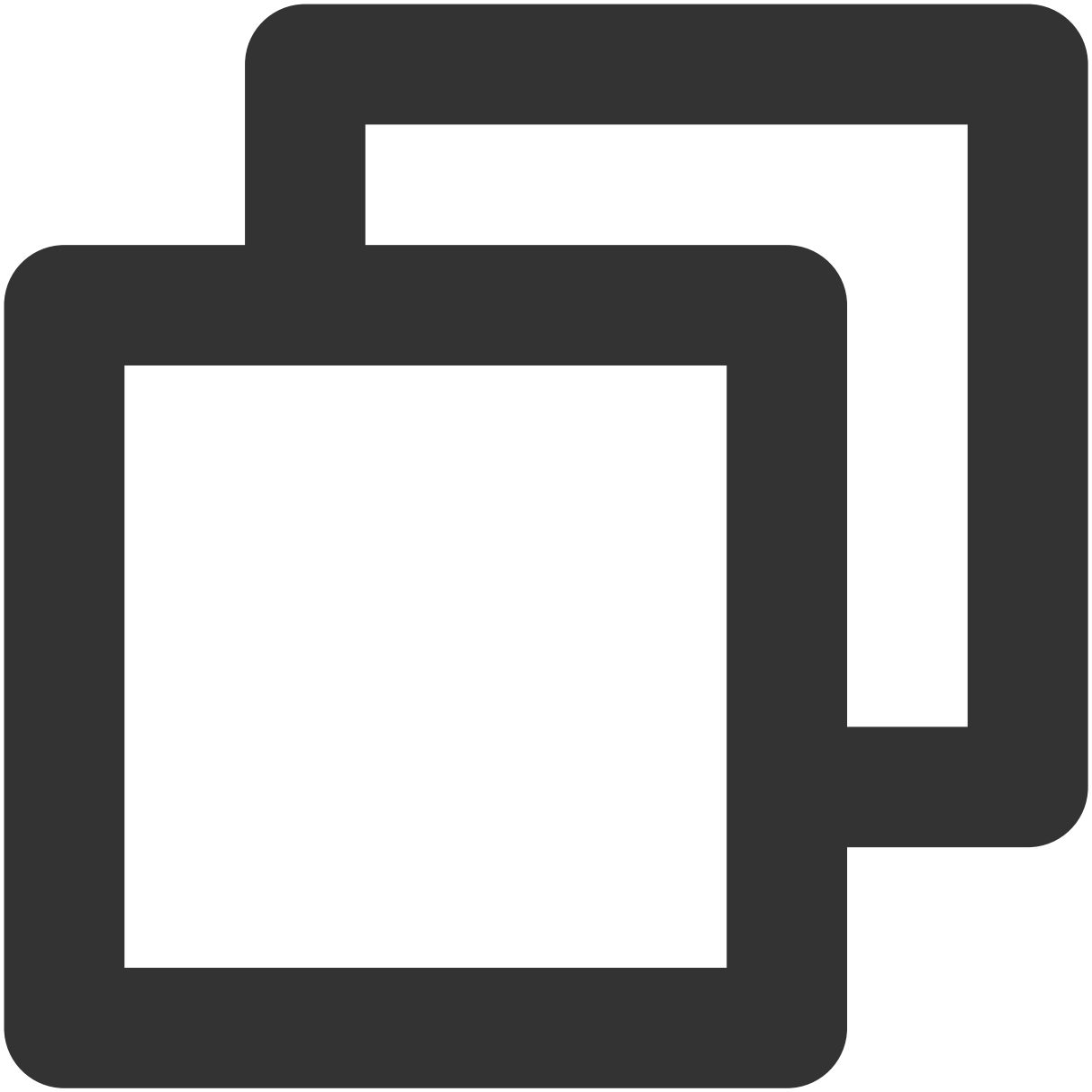
由于 EIP 直通过程会导致网络中断，请先选择如下任意一种方式将 EIP 直通脚本保存至边缘云服务器中。
方式一：上传 EIP 直通脚本
1.1 在本地计算机中，下载 EIP 直通脚本。
1.2 将已下载的 EIP 直通脚本上传至需要进行 EIP 直通的边缘计算机器实例中。
方式二：直接使用命令
登录边缘计算机器实例，并在实例中执行如下命令，下载 EIP 直通脚本。



```
wget https://eip-direct-1254277469.cos.ap-guangzhou.myqcloud.com/eip_direct.sh
```

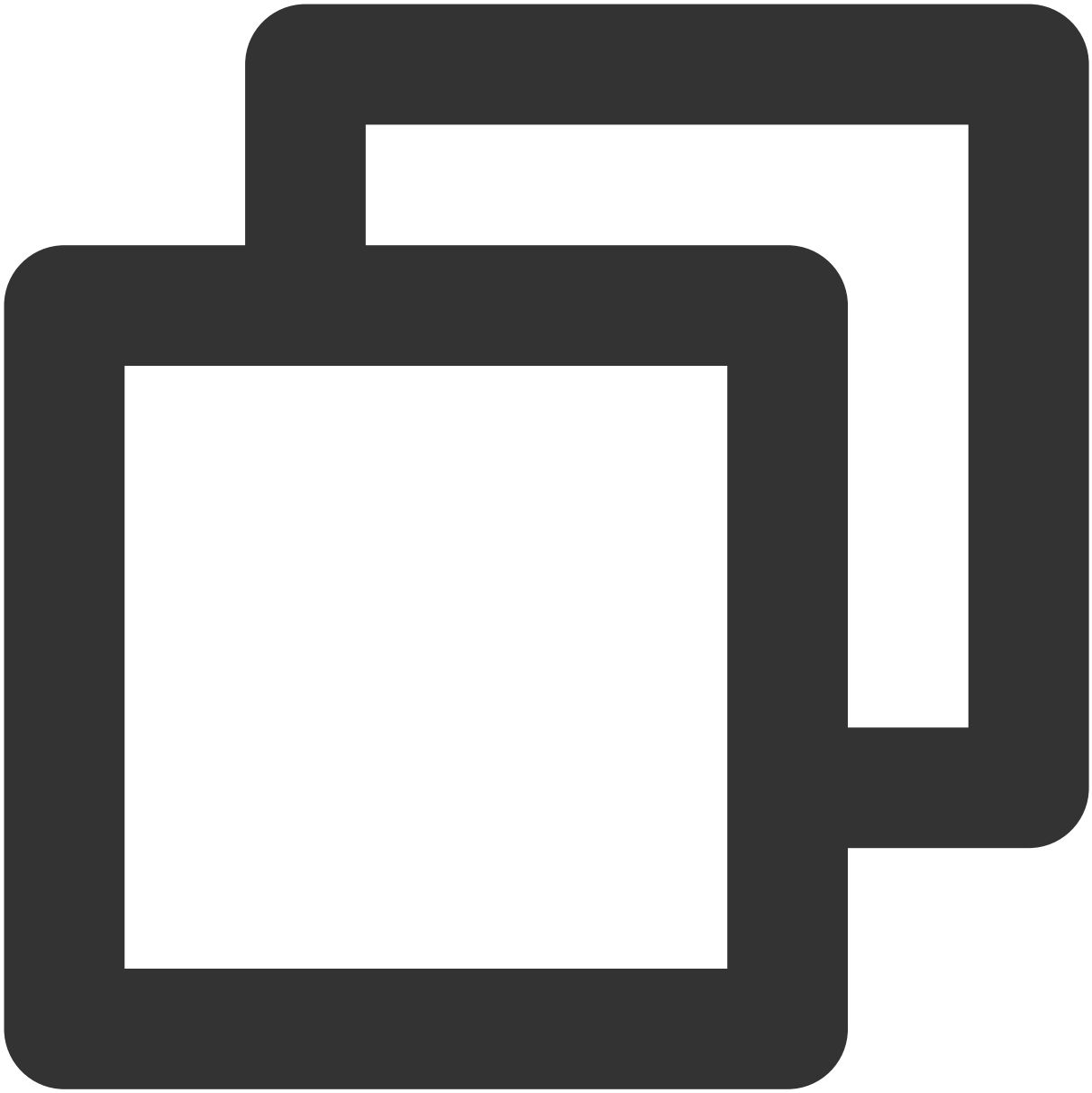
运行 EIP 直通脚本

1. 登录 Linux 实例。
2. 执行如下命令，添加执行权限。



```
chmod +x eip_direct.sh
```

3. 执行如下命令，执行脚本。



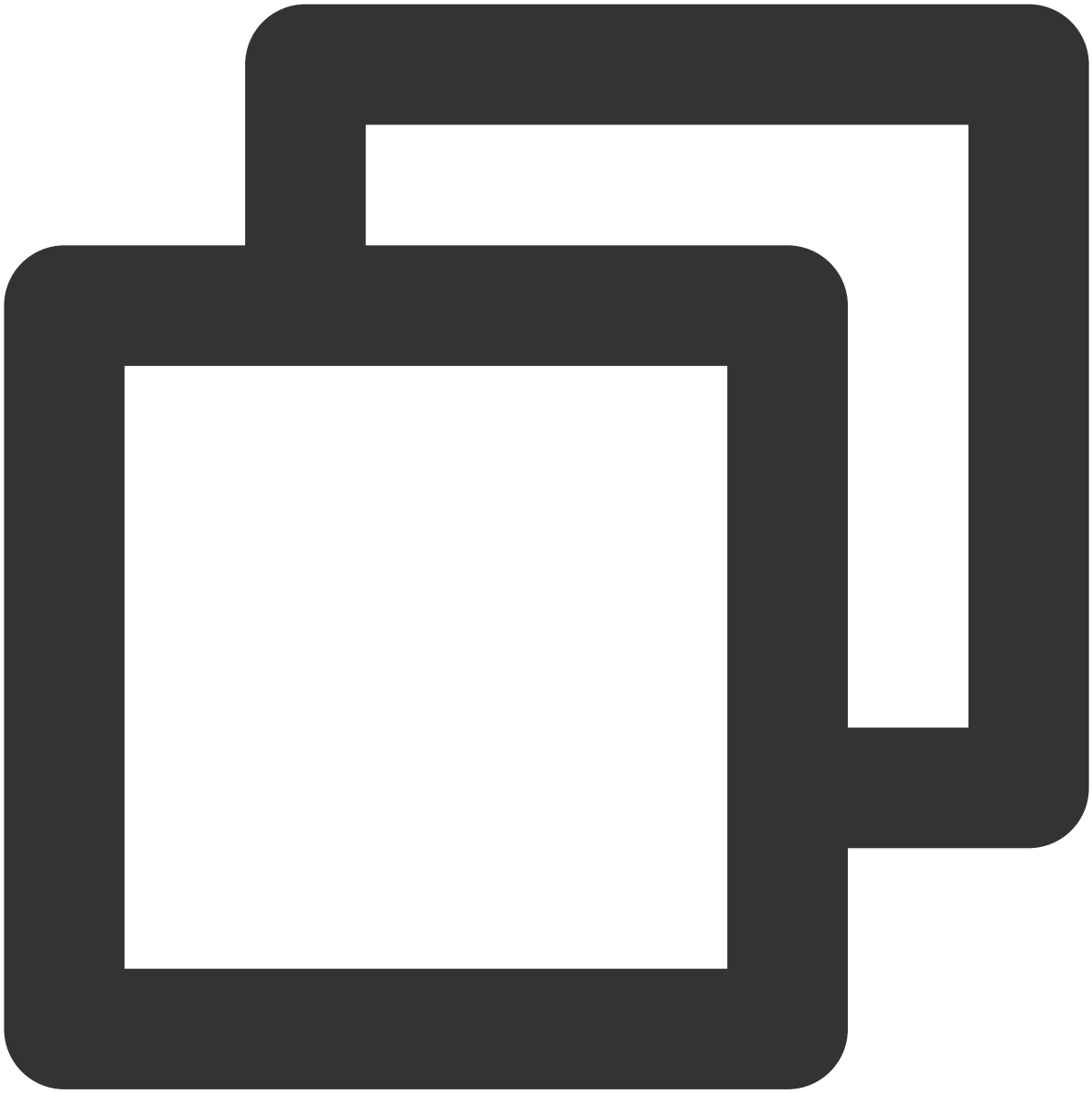
```
./eip_direct.sh install XX.XX.XX.XX
```

其中，`XX.XX.XX.XX` 为 EIP 地址，可选填。如不填写，直接执行 `./eip_direct.sh install` 即可。

附录

如果您误操作删除了 EIP 直通脚本，可通过如下操作进行恢复。

1. 将 EIP 直通脚本上传/下载到边缘计算机器实例中。
详情请参考 下载 EIP 直通脚本。
2. 登录实例，并在该实例中执行如下命令，重启实例。



```
reboot
```