



天融信产品部署使用指南 (阿里云)



北京市海淀区西北旺东路 10 号院西区 11 号楼 1 层 101 天融信科技集团 100193

电话: 010-82776666

传真: 010-82776677

服务热线: 4007770777

<http://www.topsec.com.cn>

TOP SECRET

版权声明

本文档中的所有内容及格式的版权属于北京天融信公司（以下简称天融信）所有，未经天融信许可，任何人不得仿制、拷贝、转译或任意引用。

版权所有 不得翻印 © 2025 天融信公司

商标声明

本文档中所谈及的产品名称仅做识别之用。文档中涉及的其他公司的注册商标或是版权属各商标注册人所有，恕不逐一列明。

TOPSEC® 天融信公司

信息反馈

<http://www.topsec.com.cn>

变更记录

版本	修订日期	修订人	修订类型	修订章节	修订内容
V1.0.1	2025/5/8	孙钰峰	A	建立基础版本	建立基础版本
V1.0.2	2025/11/18	张志宇	M	阿里云版修订	通用使用指南

*修订类型分为 A- ADDED M- MODIFIED D -DELETED

注：对该文件内容增加、删除或修改均需填写此记录，详细记载变更信息，以保证其可追溯性

目录

1	指南简介	1
2	部署实施	1
2.1	阿里云	1
2.1.1	登录阿里云	1
2.1.2	上传镜像至 oss	2
2.1.2.1	创建 Bucket	2
2.1.2.2	上传镜像	3
2.1.2.3	获取镜像 URL	5
2.1.3	创建自定义镜像	6
2.1.4	部署云防火墙	9
2.1.4.1	购买云服务器	9
2.1.4.2	确认部署成功	12
2.1.5	配置网络和安全组	14
2.1.6	设备登录	15
3	设备授权	16
3.1	云安全管理平台授权	17
3.1.1	平台部署	17
3.1.2	授权申请	17
3.1.3	授权导入	18
3.1.4	下发授权	18
3.2	LICENSE-CONTROLLER 授权	20
4	常见问题	20
4.1	无法正常配置 IP 问题	20
4.2	授权是提示“无可授权”	20
5	注意事项	21

1 指南简介

天融信云安全解决方案针对公有云环境下用户面临的运维负担加重、数据主权保障不足及原生安全能力薄弱等痛点，依托安全虚拟化技术构建了全栈防护体系，其核心能力覆盖多架构兼容（信创 ARM/Hygon 与非信创 x86）、弹性云化部署及无公网环境下的自授权管理，通过深度适配云原生特性（如动态流量调度、微隔离策略），实现从基础设施到应用层的纵深防御，有效解决传统安全架构在云环境中的适配性不足问题，帮助客户在保障数据合规性的同时提升安全运维效率。

2 部署实施

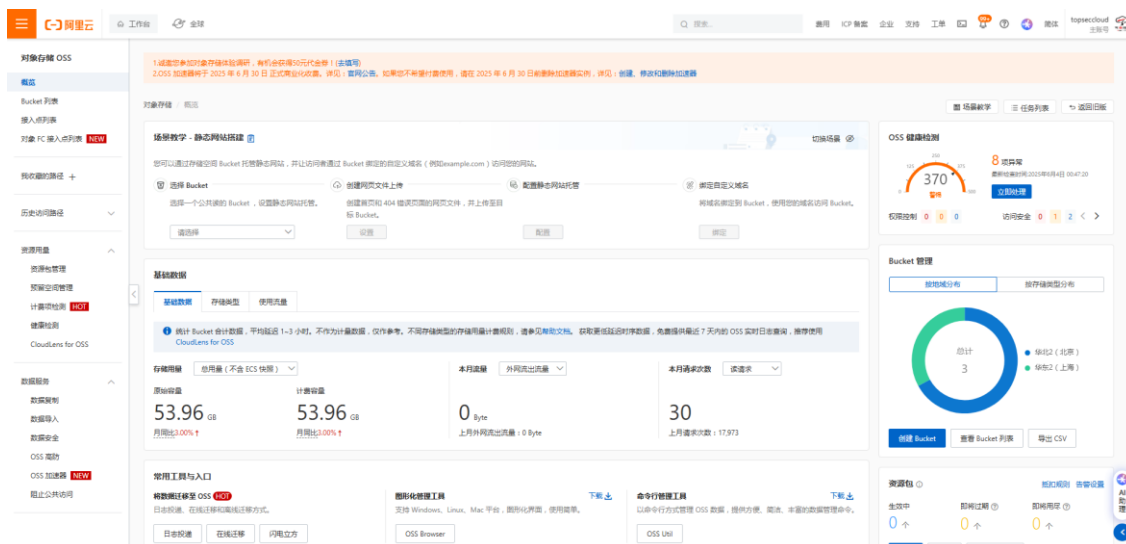
2.1 阿里云

2.1.1 登录阿里云

第一步：登陆阿里云中国站 www.aliyun.com，搜索对象存储 oss 控制台，点击进入。



第二步：进入到 OSS 管理控制台。

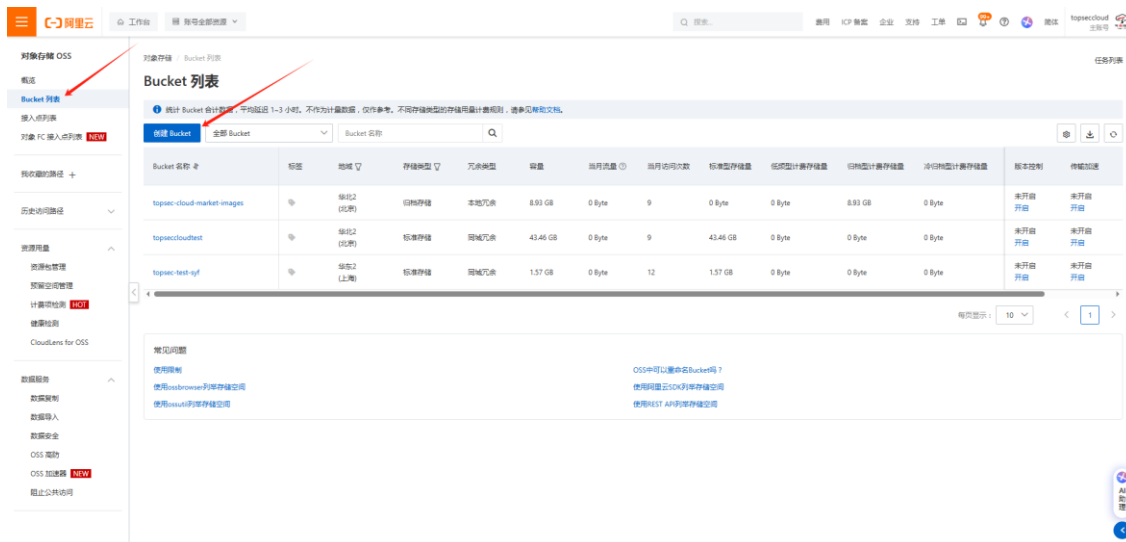


2.1.2 上传镜像至 oss

2.1.2.1 创建 Bucket

由于镜像需要上传至阿里云 oss 对象存储服务中的 bucket 中，若客户环境已具备 Bucket 可直接使用，若不具备则需要新建。

第一步：点击 Bucket 列表，然后点击添加 Bucket。



第二步：填写 Bucket 名称，选择地域，其余可按默认配置，然后点击“完成创建”。

此处需注意：“bucket 的地域”需要与“创建安全网元的 ECS 服务器地域”相同。

创建 Bucket

×

模式选择

☒ 自定义创建

☐ 快速创建

基础信息

* Bucket 名称

bushuzhidao

11/63

✓

注意

创建成功后名称将无法更改。

* 地域

有地域属性

华东2（上海）

▼

注意

创建成功后地域将无法更改，相同区域内的产品内网可以互通。

Endpoint

oss-cn-shanghai.aliyuncs.com

* 存储类型 ①

标准存储

低频访问

归档存储

冷归档存储

深度冷归档存储 NEW

描述

高可靠、高可用、高性能，数据会经常被访问到。

注意

存储类型，创建成功后不支持修改。

* 存储冗余类型

同城冗余存储（推荐）

本地冗余存储

描述

OSS 同城冗余采用多可用区（AZ）冗余机制，将用户的数据分散存放在同一地域的多个可用区。当某个可用区不可用时，仍然能够保障数据的正常访问。[了解更多](#)

计费

同城冗余存储将采用较高的计费标准，产生的存储费用仅可被同城冗余存储包抵扣。[计费文档](#)

注意

选择同城冗余类型后，将不支持转换为本地冗余类型。

阻止公共访问

已开通

☒

描述

阻止公共访问能够方便企业对 OSS 资源进行集中化的权限管理，有效降低数据被盗刷的风险，同时降低数据泄漏风险。了解更多功能介绍，请查看 [阻止公共访问介绍](#)

注意

已开启阻止公共访问，该存储桶将不再允许匿名访问且不允许创建含有公共访问语义的权限策略。发生鉴权时，已设置的公共读 ACL、公共读写 ACL 和含有公共访问语义的权限策略将被忽略，创建新的公共读 ACL、公共读写 ACL 和含有公共访问语义的权限策略时将被禁止。

完成创建

取消

2.1.2.2 上传镜像

第一步：进入到创建好的 Bucket 中，点击上传文件。

对象存储

Bucket 列表

bushuzhidao

文件列表

← bushuzhidao / 华东2（上海）

▼

文件列表

☆

上传文件

新建目录

图片管理

授权

请输入文件名前缀匹配

Q

更多搜索 ①

数据索引

文件名称

文件大小

存储类型

更新时间

操作

□

设置文件元数据

导出 URL 列表

下载 ②

解冻

批量删除

常见问题 更多

最佳实践 更多

如何分片上传？

如何分片上传？

如何上传下载目录？

如何上传下载？

如何鉴权？

如何鉴权？

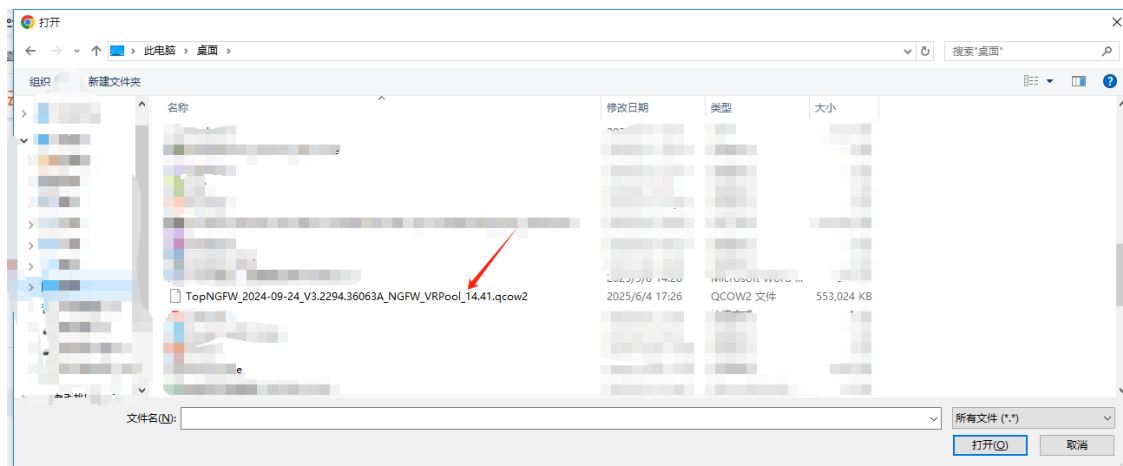
如何鉴权？

如何鉴权？

第二步：进入到上传文件页面后，点击“扫描文件”。



第三步：选择要上传的云防火墙镜像文件。



第四步：点击“上传文件”，完成上传。



第五步：等待上传完成。

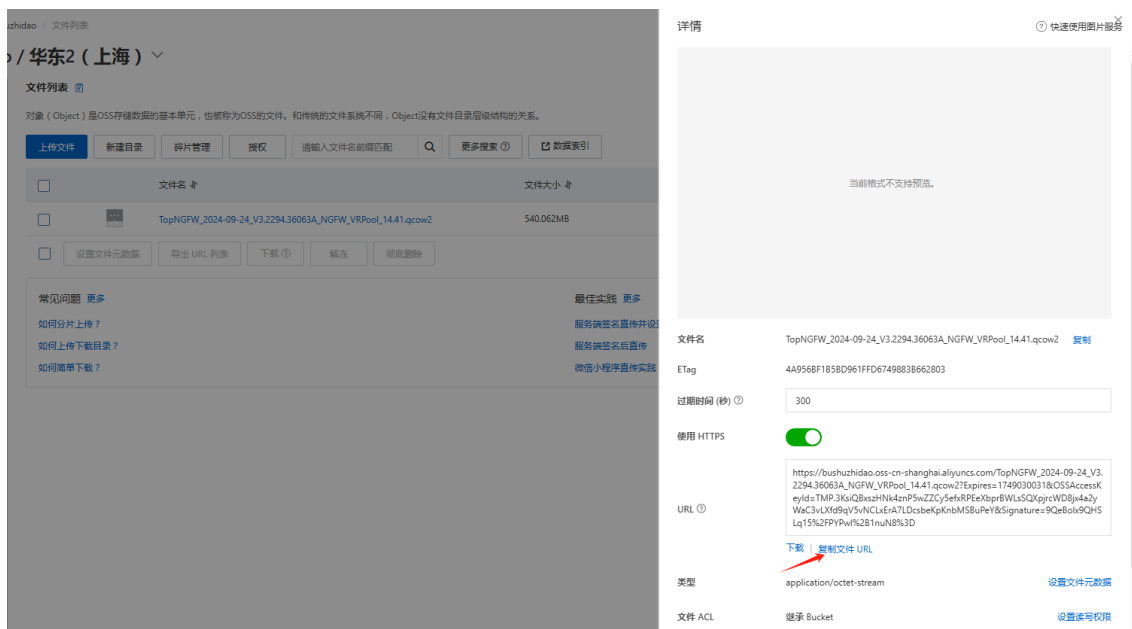


2.1.2.3 获取镜像 URL

第一步：点击已上传至 oss 存储服务的文件“详情”

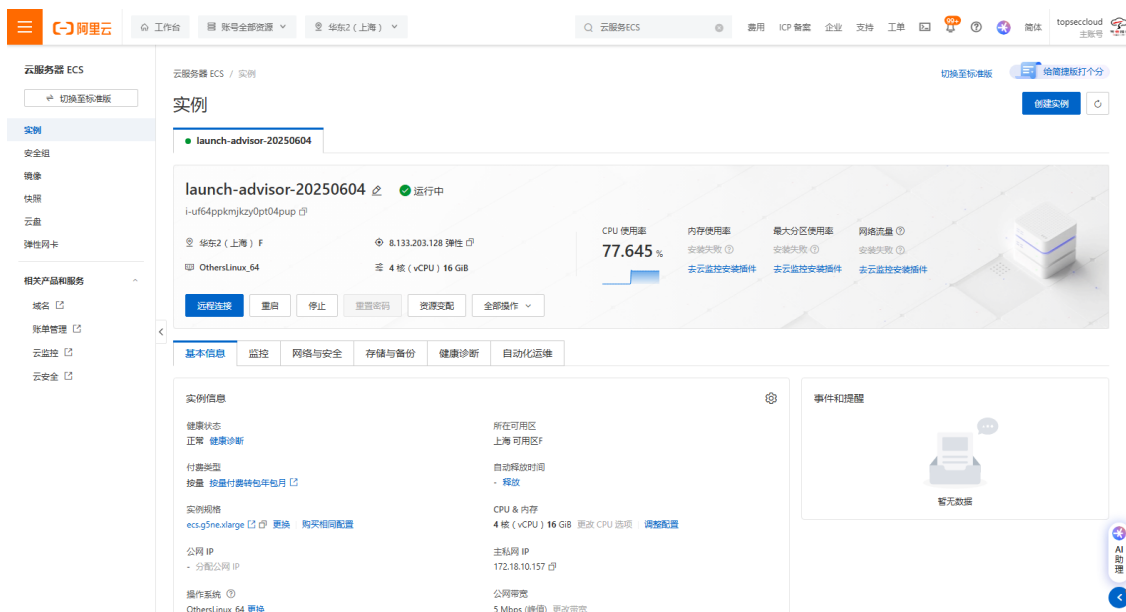


第二步：此处获取文件的 URL 地址，点击“复制文件 URL”。

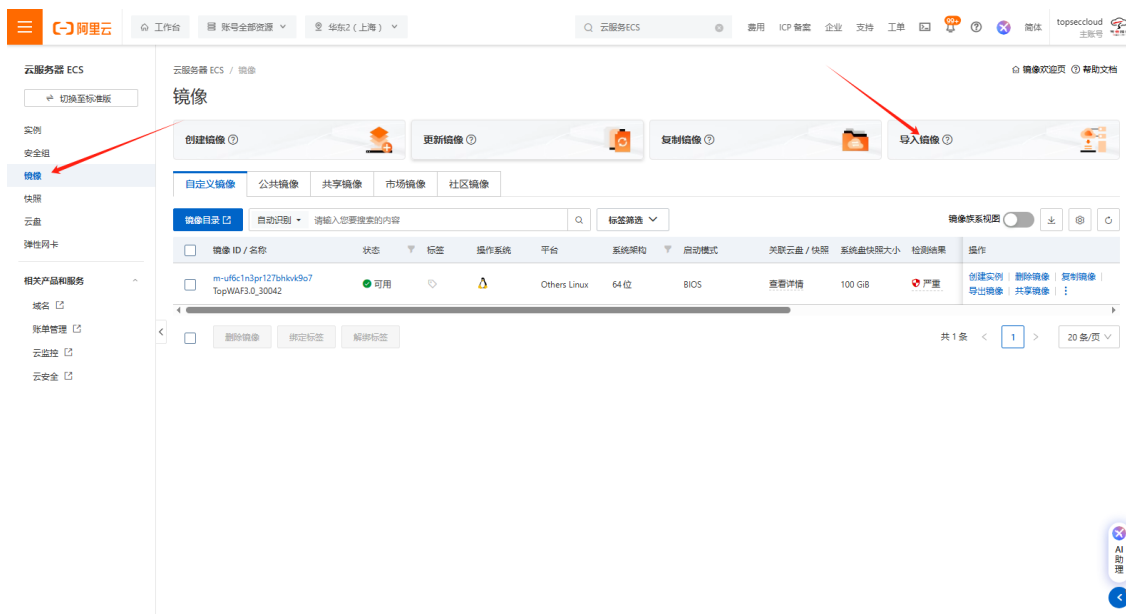


2.1.3 创建自定义镜像

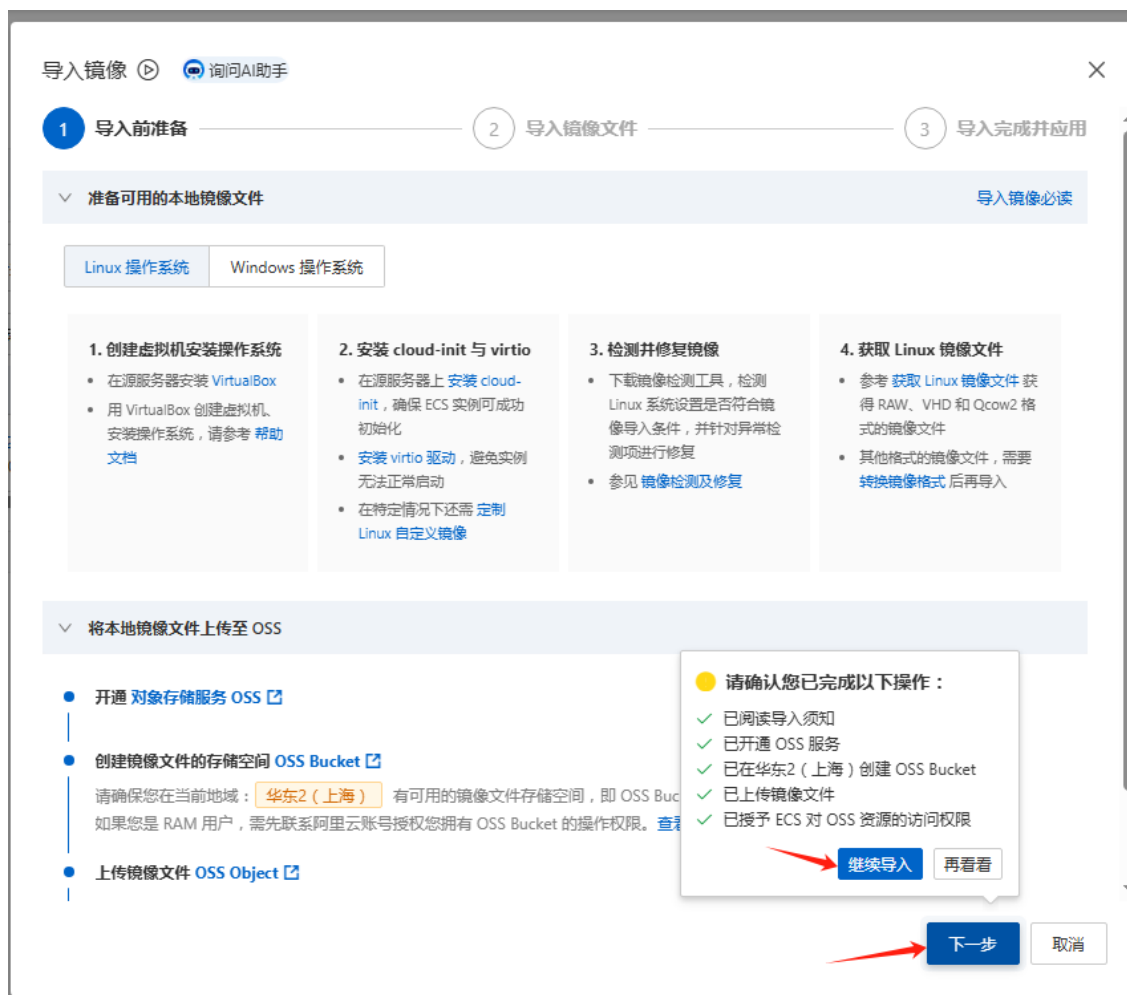
第一步：进入云服务 ECS 控制台。



第二步：点击“镜像”，进入镜像页面。然后点击“导入镜像”。



第三步：点击“下一步”，然后点击“继续导入”。



第四步：使用 3.1.2.3 章节获取的 URL 地址，按下方实例填写信息即可。然后点击“确定导入”，后续等待镜像创建完成即可。

导入镜像

询问AI助手

×

1 导入前准备

2 导入镜像文件

3 导入完成并应用

1. 计费提示 导入镜像时，系统默认会创建相关快照。阿里云快照已实行商业化，关联的快照将产生费用，请参见 [快照计费](#)。

2. 请您确保在当前地域：华东2（上海）有可用的镜像文件存储空间，即 OSS Bucket。

* 镜像文件 URL

填写镜像URL地址

[如何在 OSS 控制台获取镜像文件的 URL >>](#)

* 镜像名称

* 操作系统类型

linux 选择Linux

* 操作系统版本

Others Linux 选择Others Linux

* 系统架构

64 位操作系统 按镜像架构选择

镜像检测

☒ 导入后执行检测

镜像检测服务能帮您快速发现镜像中存在的潜在问题，并提供修复方案，使导入的镜像符合阿里云标准，提升启动成功率。检测服务目前免费，部分系统不会触发检测。具体请参考：《[镜像检测项说明](#)》、《[镜像检测系统限制](#)》

启动模式

BIOS x86架构选择BIOS，ARM架构选择UEFI

镜像格式

自动检测

许可证类型

自动检测 Auto

上一步

确定导入

取消

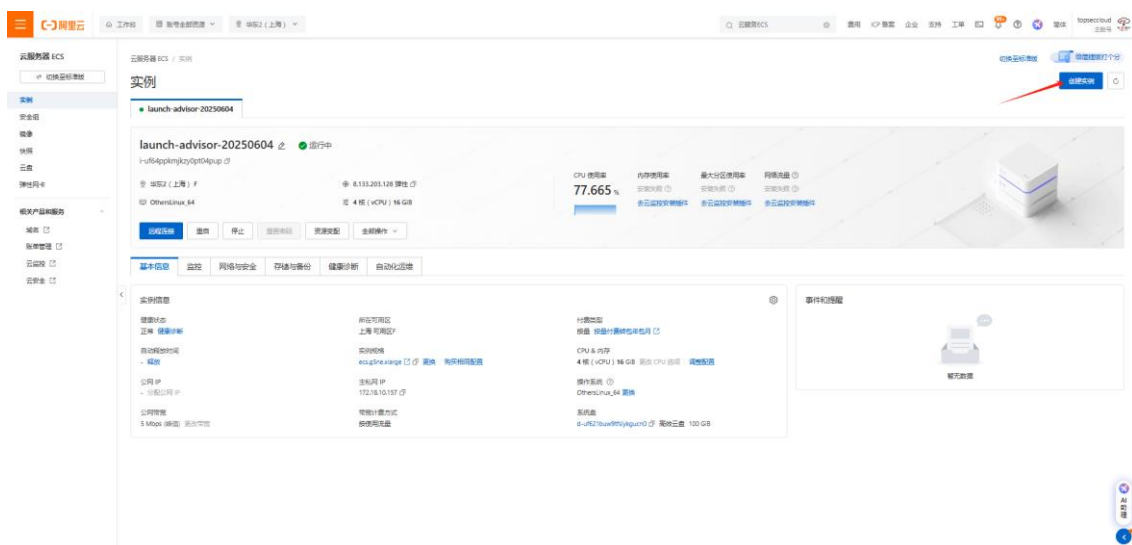
2.1.4 部署云防火墙

2.1.4.1 购买云服务器

第一步：进入云服务 ECS 控制台。

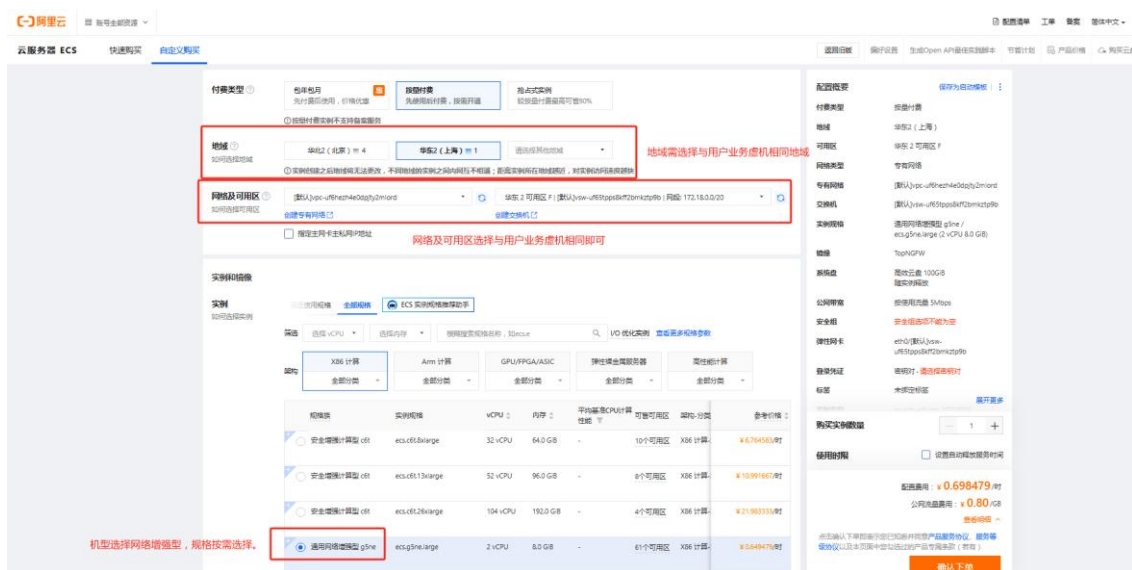


第二步：点击“创建实例”。



第三步：配置 ECS 实例

- 1、地域：按用户需求选择，此处需要与自定义镜像地域一致，并且与用户业务 ECS 相同地域。
- 2、网络与可用区：按用户需求选择，尽量与用户业务 ECS 相同。
- 3、机型：当前云防火墙产品，仅推荐使用“通用网络增强型 G5”机型。



第四步：配置 ECS 实例

- 1、镜像：选择“自定义镜像”中 3.1.3 章节创建好的云防火墙镜像。
- 2、磁盘：系统盘按默认 100G 即可，云防火墙无需数据盘。



第五步：配置完成后点击“确定下单”，完成部署。

- 1、公网 IP：此处可按需选择。
- 2、安全组：此处按默认即可，后续 3.1.5 章节进行详细配置。
- 3、网卡：网卡按需选择，默认一张网卡即可。若有 ipv6 需求需要勾选“免费分配 IPV6 地址”。

带安全和安全组

公网 IP

☐ 分配公网 IPv4 地址

不为实例分配公网 IP 地址，如需访问公网，请配置并绑定弹性公网 IP 地址，或者购买实例后升级实例的带宽，系统会自动为实例分配公网 IP

公网ip按需选择

安全组

已有安全组 [新建安全组](#)

如何配置安全组

安全组名称

安全组类型 普通安全组 企业级安全组 [普通安全组和企业级安全组的对比差异>](#)

此处安全组可按默认，后续进行详细配置

开通IPv4端口/协议

☒ SSH (TCP : 22)
☐ HTTPS (TCP : 443)
☐ MySQL (TCP : 3306)
☐ Redis (TCP : 6379)

☐ Telnet (TCP : 23)
☐ MS SQL (TCP : 1433)
☒ RDP (TCP : 3389)
☒ ICMP (IPv4)

☐ HTTP (TCP : 80)
☐ Oracle (TCP : 1521)
☐ PostgreSQL (TCP : 5432)

① 选择 SSH (TCP : 22) 将设置 0.0.0.0/0 作为源规则的，即允许所有 IP 地址通过22端口访问您的实例。我们建议您创建实例后将安全组规则设置为仅允许从已知的IP地址进行访问

弹性网卡

主网卡

[新建网卡](#) 已有网卡

交换机 ☒ 自动分配 IP 地址 ☒ 随实例释放 ☐ 源/目的检查

辅助网卡

[新建网卡](#) 已有网卡

+ 添加辅助弹性网卡 (0 / 1) 创建实例时只能附加 1 块弹性网卡，了解更多>

IPv6

☒ 免费分配 IPv6 地址

网卡按需选择，默认一张网卡。
若客户有ipv6需求，需勾选“免费分配IPv6地址”

管理设置

登录凭证

☐ 密码对 ☒ 使用镜像预设密码 ☐ 创建后设置

保留所选镜像的预设密码。为了保证您的正常使用，请保证所选镜像中已经设置了密码

密码使用镜像默认

付费类型

按量付费

地域

华东2 (上海)

可用区

华东 2 可用区 F

网络类型

专有网络

专有子网

[默认]vpc-uf6hcz4e0dtpjy2mlord

交换机

[默认]vsw-uf65tpps8kft2bmktzp9b

实例规格

通用网络增强型 g5ne / ecs.g5ne.large (2 vCPU 8.0 GiB)

镜像

TopNGFW

系统盘

高效云盘 100GiB
随实例释放

公网带宽

您没有为实例分配公网IP地址

安全组

新建

弹性网卡

eth0/[默认]vsw-uf65tpps8kft2bmktzp9b

IPv6

免费分配 IPv6 地址

登录凭证

使用镜像预设密码

标签

未绑定标签

实例名称

launch-advisor-20250604

实例释放保护

否

元数据访问模式

普通模式和加盐模式 [展开更多](#)

购买实例数量

使用期限

☐ 设置自动释放服务时间

配置费用: ¥ 0.698479 /时

查看明细

完成上述配置后，点击下方完成部署

点击确认下单将表示您已知悉并同意产品服务协议、服务协议以及本页面下方勾选过的产品专项条款（若有）

[确认下单](#)

2.1.4.2 确认部署成功

第一步：进入到 ECS 控制台，点击“远程登录”

云服务器 ECS

实例

launch-advisor-20250604

launch-advisor-20250604

运行中

操作系统启动中

实例名称

launch-advisor-20250604

实例规格

通用网络增强型 g5ne

实例配置

2 核 (vCPU) 8 GiB

操作系统

CentOS Linux 6.4

公网 IP

172.18.10.158

公网带宽

100 GiB

实例状态

运行中

实例规格

通用网络增强型 g5ne

实例配置

2 核 (vCPU) 8 GiB

操作系统

CentOS Linux 6.4

公网 IP

172.18.10.158

公网带宽

100 GiB

基本设置

网络与安全

存储与备份

健康诊断

自动化运维

实例信息

实例名称

launch-advisor-20250604

实例规格

通用网络增强型 g5ne

实例配置

2 核 (vCPU) 8 GiB

操作系统

CentOS Linux 6.4

公网 IP

172.18.10.158

公网带宽

100 GiB

实例状态

运行中

实例规格

通用网络增强型 g5ne

实例配置

2 核 (vCPU) 8 GiB

操作系统

CentOS Linux 6.4

公网 IP

172.18.10.158

公网带宽

100 GiB

第二步：选择通过 VNC 远程连接。



第三步：使用默认账号密码登录到云防火墙，执行“network interface show”命令，查看是否成功获取到 ip。如下图，则代表部署成功。

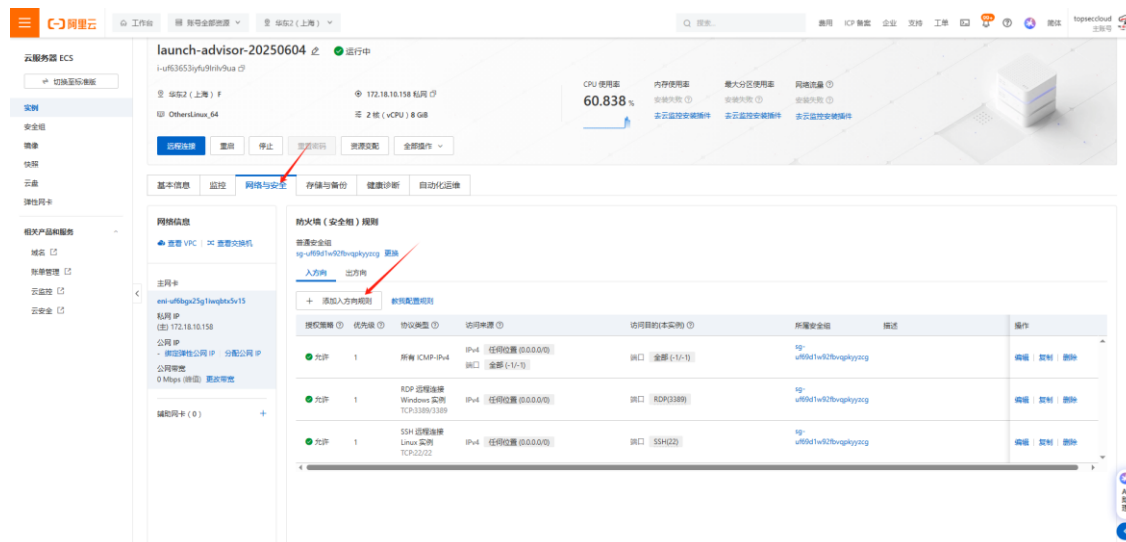
```
login: superman
Password:
TopsecOS# network interface show
eth0      Link encap:Ethernet  HWaddr 00:16:3e:1e:a5:fe
          Link status: established, Autoneg enable
          Full duplex, 10Gbps
          inet addr:172.18.10.158  Bcast:172.18.15.255  Mask:255.255.240.0  DHCP
          inet6 addr:fe80::216:3eff:fe1e:a5fe/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500
          Rx packets:26 Tx packets:44 Dropped:3
          RX bytes:2544 (2.4 kb)  TX bytes:3674 (3.5 kb)
          Usys:root_vsys  If index:6
          Commttype:routing

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:65536
          Rx packets:9411 Tx packets:9411 Dropped:0
          RX bytes:1848452 (1.7 Mb)  TX bytes:1848452 (1.7 Mb)
          Usys:root_vsys  If index:1
          Commttype:routing

TopsecOS#
```

2.1.5 配置网络和安全组

第一步：进入 ECS 控制台，点击“网络与安全”打开安全组页面，再次点击“添加入方向规则”。



第二步：配置放行“443”、“7443”端口。其中 443 为云防火墙的管理端口，7443 为授权端口，其余业务端口可按需放行。

添加加入方向规则 ×

安全组

自定义安全组-20250604 ▼

* 授权策略 ?

允许 拒绝

* 优先级 ?

1

* 协议类型 ?

自定义 TCP ▼

* 访问来源 ?

IPv4 ▼ 0.0.0.0/0 (任何位置) ×

* 访问目的(本实例) ?

端口 HTTPS(443) × 7443 × 放行443与7443端口

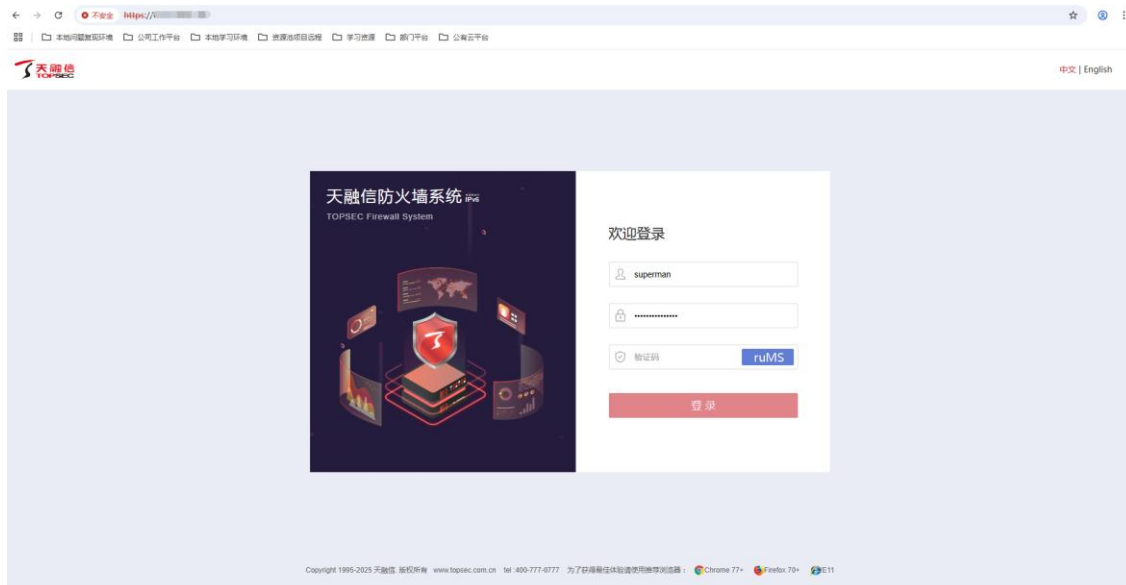
描述

0 / 256

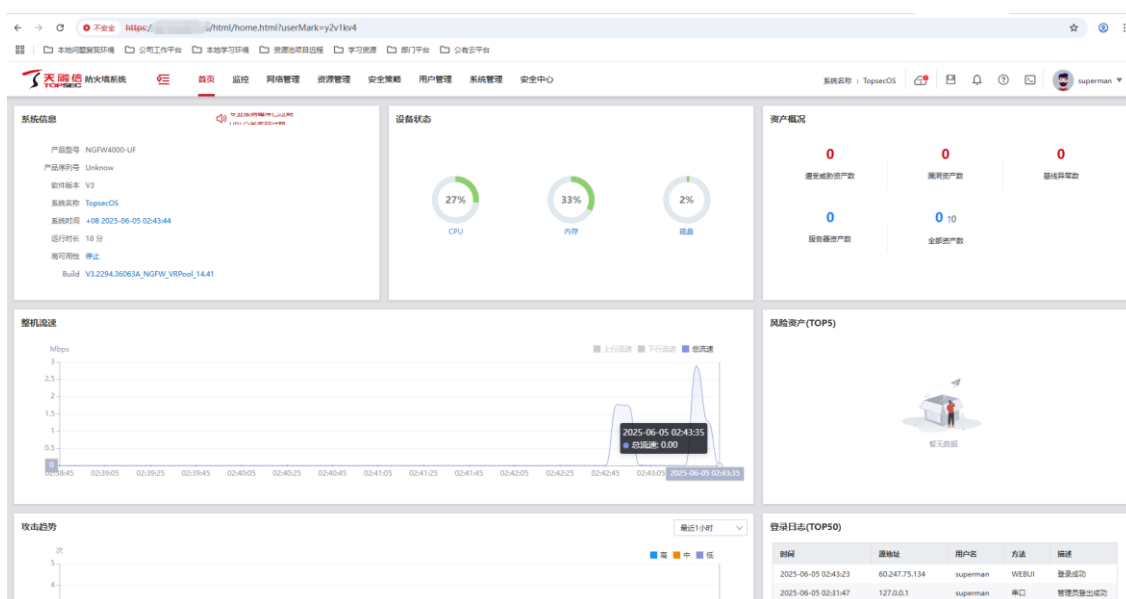
确定 关闭

2.1.6 设备登录

第一步：使用公网地址登录云防火墙，登陆方式：<https://x.x.x.x>。



第二步：使用默认账号密码“superman/Cloud@talent123”进行登录。



3 设备授权

3.1 云安全管理平台授权

授权前请务必确保：云安全管理平台与安全网元 7443 端口双向互通。

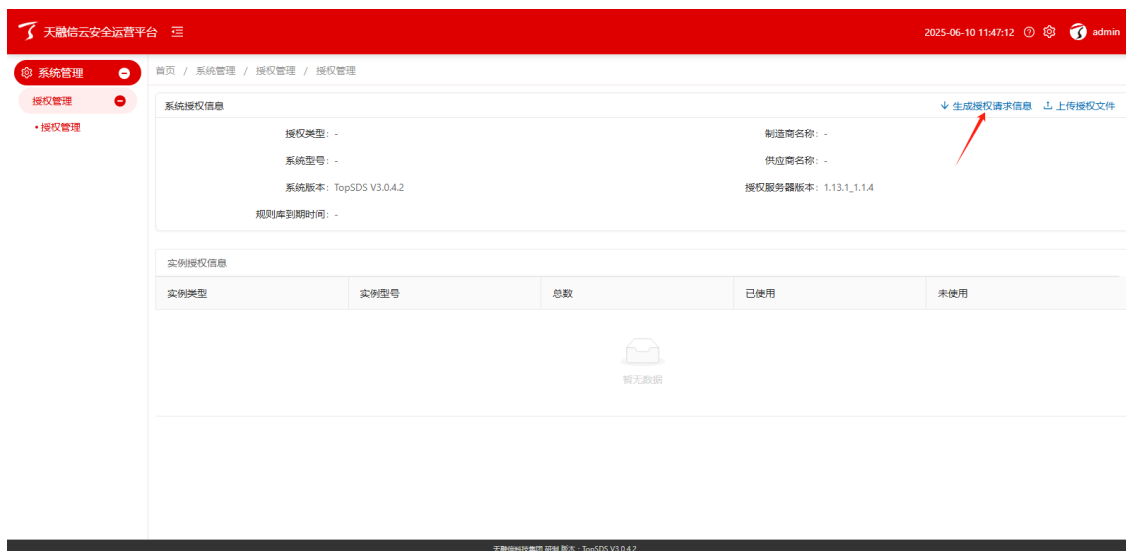
3.1.1 平台部署

请参照第 2 章节云平台部署流程，将云安全管理平台镜像按相同方式部署。

3.1.2 授权申请

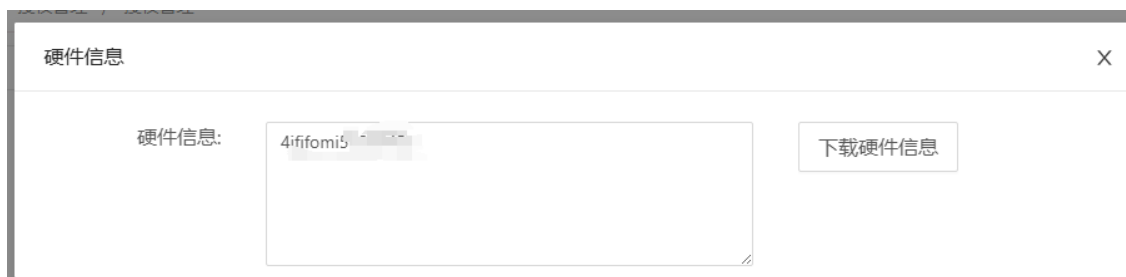
申请步骤以防火墙为例，其他产品参考此步骤，激活时选择对应的产品类型。

第一步：登录云安全管理平台，选择【授权管理】，点击【生成授权请求信息】。



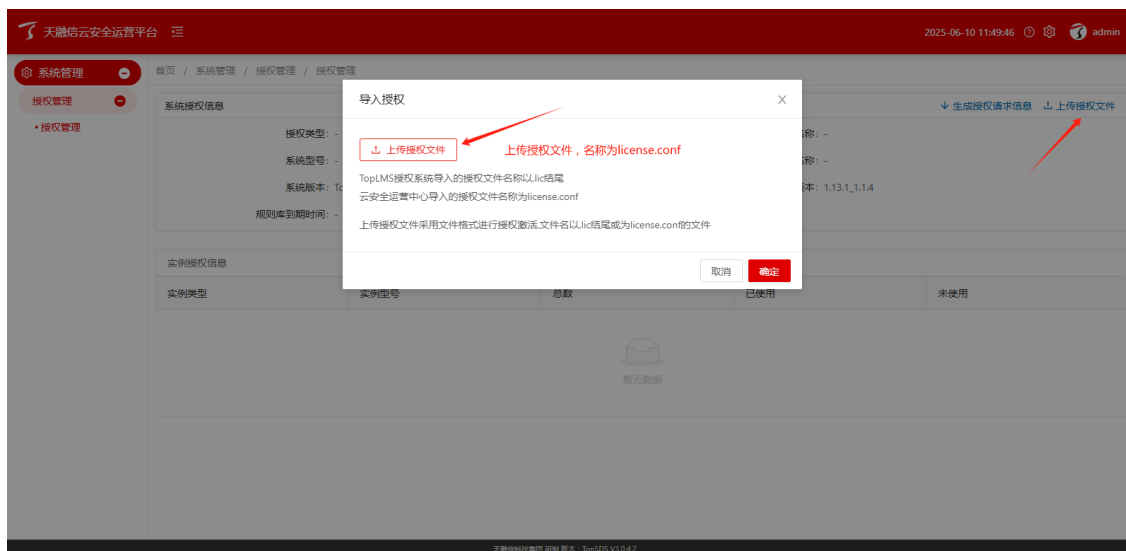
第二步：获取硬件信息码，用于后续授权申请。

请按照天融信公司流程申请所需授权，授权申请流程与问题请联系天融信阿里云客服。



3.1.3 授权导入

第一步：登录云安全管理平台，选择【系统管理】→【授权管理】→【上传授权文件】，导入即可。



3.1.4 下发授权

第一步：创建租户，在【租户管理】页面添加租户，按照提示信息完成名称、密码、邮箱等填写。

添加

* 租户名称 ?

部署指导

* 密码 :

.....

* 确认密码 :

.....

* 手机号 :

13.....

* 邮箱 :

topsec_.....

姓名 :

单位名称 :

取消

确定

第二步：实例激活，在【租户管理】-【租户服务】页面，点击实例激活，填写云防火墙的地址、实例名称(可以自定义)、租户名称、实例类型、版本等信息，最后点击确定完成激活。

实例激活

* IP : 192.1

* 实例名称 : 云防火墙

* 租户名称 : 部署指导

* 实例类型 : 下一代防火墙

* 版本 : 高级版 → 此处注意按需选择

平台 : topsec 1.0.0

区域 :

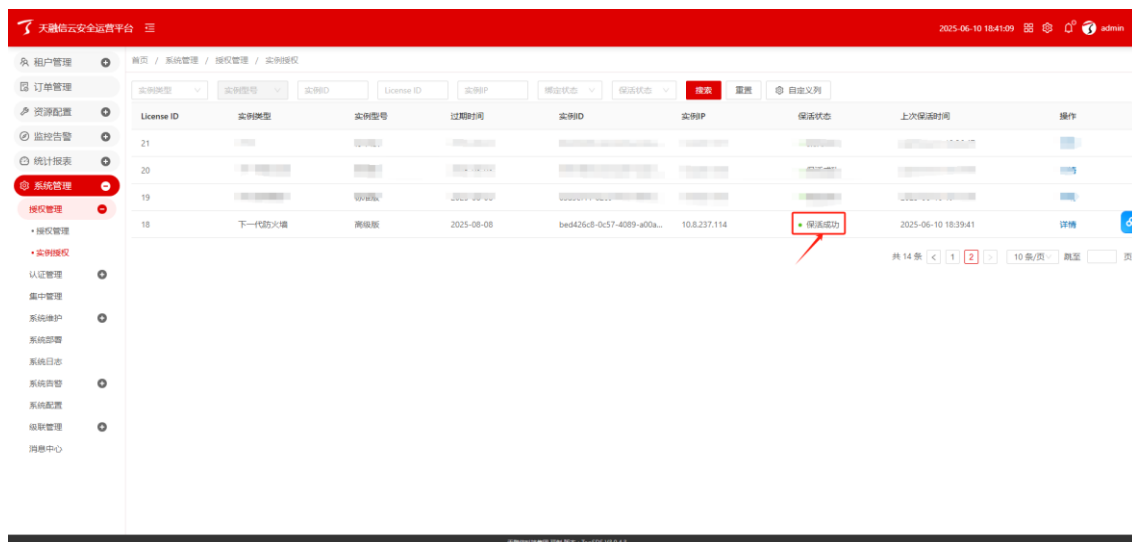
实例激活所需时间较长, 请耐心等待

取消

确定

第三步：检查状态，激活后云防火墙会自动重启，重启后登录云防火墙的 web 页面，在【首页】【系统信息】可以看到租约信息。同时在云安全管理平台【系统管理】-【授权管理】-【实例授权】可以看到此云防火墙的保活状态，如果为保活成功，则说明授权激活成功。





3.2 License-Controller 授权

License-Controller 使用场景，具体咨询阿里云天融信客服。

4 常见问题

4.1 无法正常配置 ip 问题

阿里云推荐使用“通用网络增强型”ECS，使用其他机型可能会出现“IP 无法自动获取”、“镜像启动异常”等问题。如遇到相关问题尝试解决失败，请联系客服及相关接口人沟通。

4.2 授权是提示“无可用授权”

云安全管理平台授权成功导入后，需要退出重新登录后才可正常授权。

5 注意事项

- 不能选择低于最低配置建议的 ECS 规格，避免异常流量带来的性能压力。
- 注意购买云服务器的地域一定要选择和用户云业务服务器在同一地域。
- 授权完成后，需要等待一段时间，所需时间不等，但一般不超过半小时。

声明

1. 本文档所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信不另行通知。
2. 本文档中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异，此种情况产生的差异为正常现象，产品功能或性能请以产品用户手册等资料为准。
3. 本文档中提到的信息为正常公开的信息，若因本文档或其所提到的任何信息造成或可能造成他人直接或间接的资料流失、利益损失，天融信及其员工不承担任何责任。