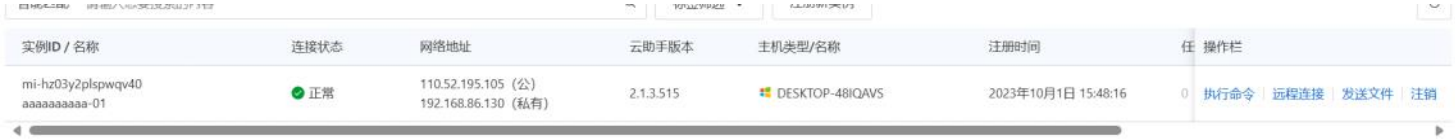
H.3 阿里云ECS云助手[适合权限维持]

2023年10月1日 16:05

By:弱鸡
笔者微信：vivo50KFCKFC
项目地址：https://github.com/RuoJi6/Deskbypass
博客：https://vlog.taoyuan.cool/
工具链接：
链接：https://pan.baidu.com/s/1XdVkAJU_Q9rD0PMiSDZFKQ?pwd=zdpm
提取码：zdpm
--来自百度网盘超级会员V4的分享

ECS云助手　执行命令　远程连接　文件操作



ECS云助手安装

云助手是专为云服务器ECS打造的原生自动化运维工具，免密码、免登录、无需使用跳板机，即可批量执行命令（Shell、PowerShell、Bat等），实现自动化运维脚本、轮询进程、安装卸载软件、启动或停止服务、安装补丁或安装安全更新等任务。

阿里云设计云助手主要用来操作阿里云服务器使用，但同时，也对非阿里云服务器提供了混合云方案，即使我们的目标不是阿里云服务器，也可以让它上线到云安全中心进行远控。

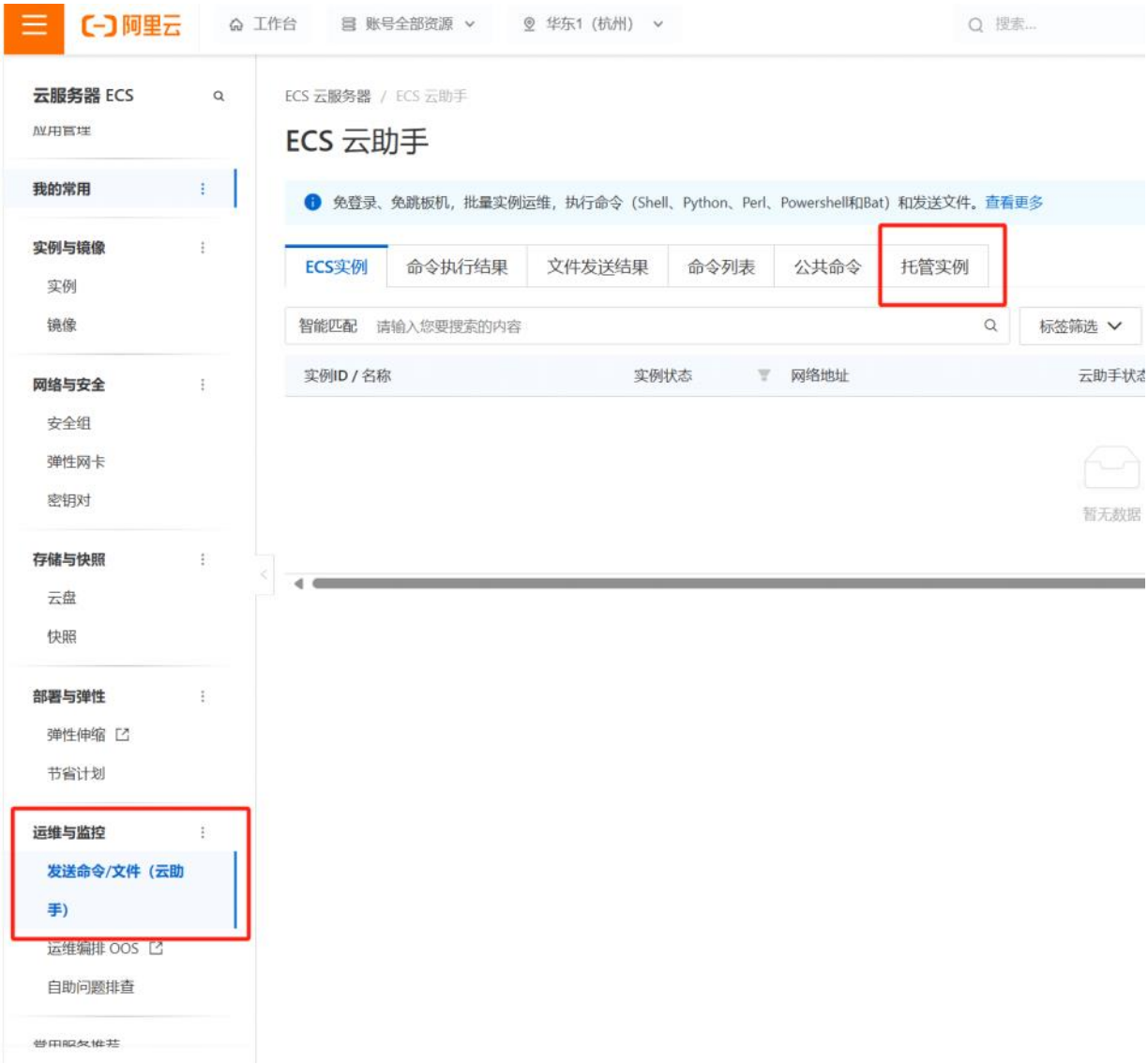
版本要求：

- Alibaba Cloud Linux 2/3及更高版本
- CentOS 6/7/8及更高版本
- CoreOS
- Debian 8/9/10及更高版本
- OpenSUSE
- RedHat 5/6/7及更高版本
- SUSE Linux Enterprise Server 11/12/15及更高版本
- Ubuntu 12/14/16/18及更高版本
- Window Server 2012/2016/2019及更高版本

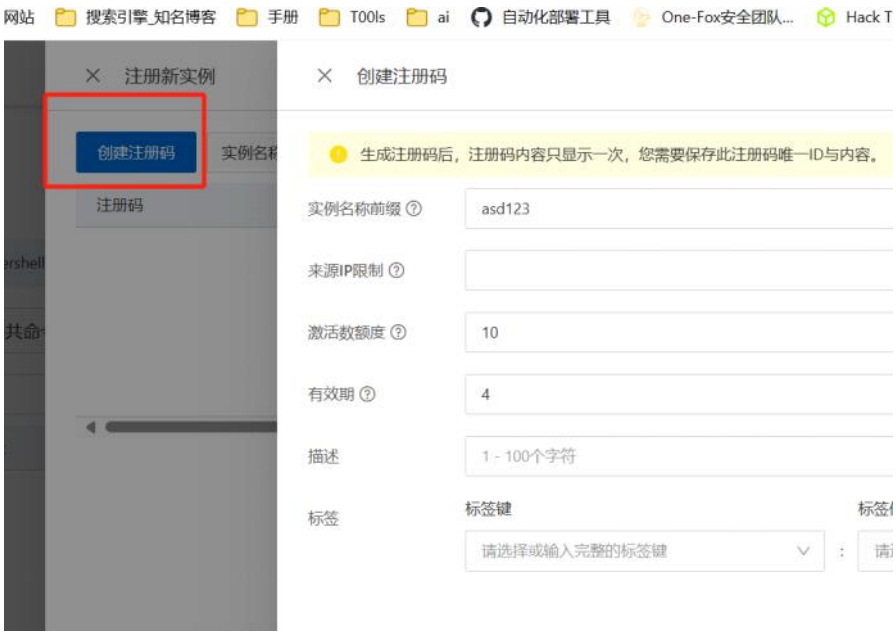
安装云助手Agent

1、创建托管实例注册码

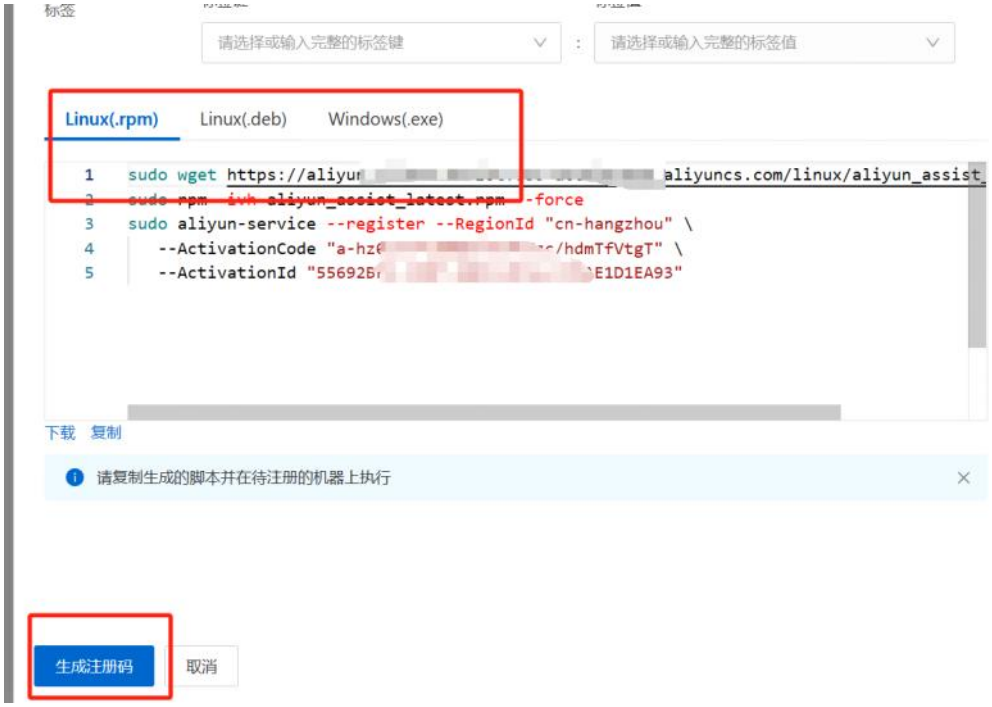
云服务器ECS-运维与监控-发送命令/文件（云助手），选择托管实例


阿里云
工作台
账号全部资源
华东1（杭州）
搜索...
云服务器 ECS
我的常用
实例与镜像
实例
镜像
网络与安全
安全组
弹性网卡
密钥对
存储与快照
云盘
快照
部署与弹性
弹性伸缩
节省计划
运维与监控
发送命令/文件（云助手）
运维编排 OOS
自助问题排查
ECS 云服务器 / ECS 云助手
ECS 云助手
免登录、免跳板机，批量实例运维，执行命令（Shell、Python、Perl、Powershell和Bat）和发送文件。查看更多
ECS实例
命令执行结果
文件发送结果
命令列表
公共命令
托管实例
智能匹配
请输入您要搜索的内容
标签筛选
实例ID / 名称
实例状态
网络地址
暂无数据

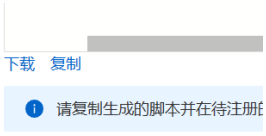

免登录、免跳板机，批量实例运维，执行命令（Shell、Python、Perl、Powershell和Bat）和发送文件。查看更多
ECS实例
命令执行结果
文件发送结果
命令列表
公共命令
托管实例
智能匹配
请输入您要搜索的内容
标签筛选
注册新实例
实例ID / 名称
连接状态
网络地址
云助手版本
主机类型/名称
暂无数据



点击生成注册码后，会出现注册命令，如下图

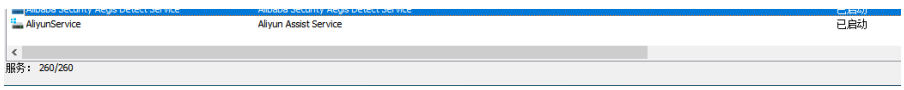


复制命令或者下载执行

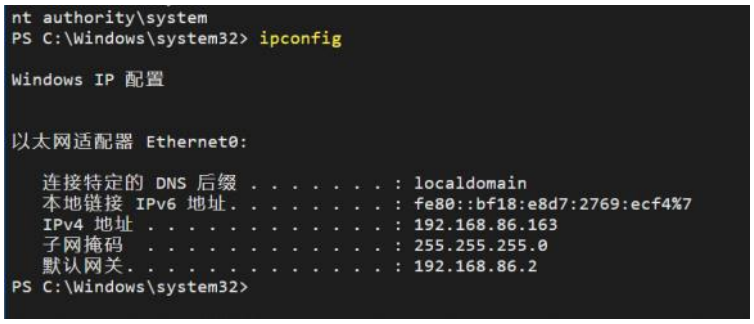


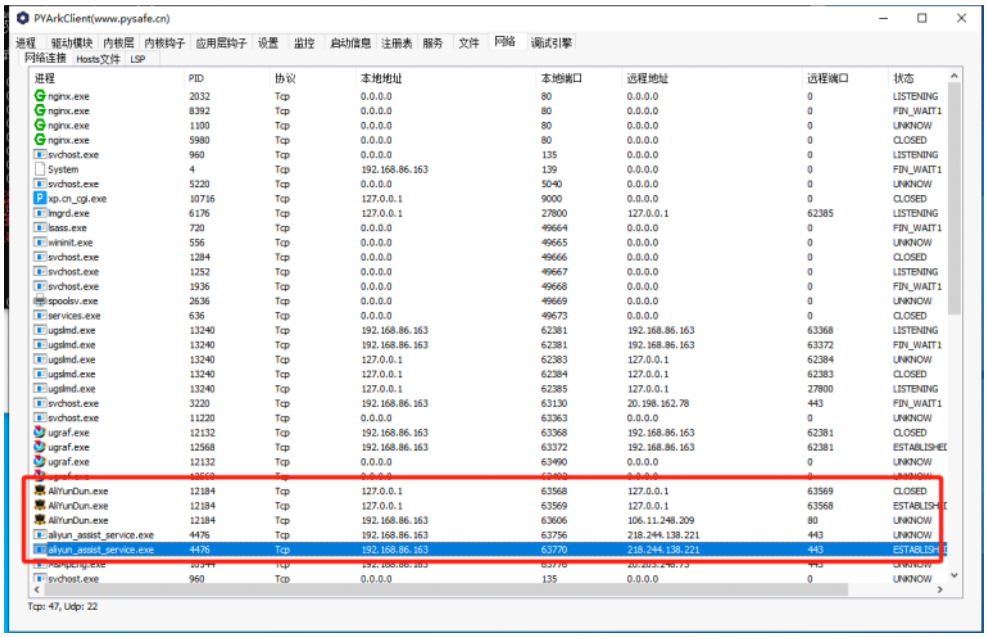
2、复制执行

需要管理员权限[需要等待一段时间]




免登录、免跳板机，批量实例运维，执行命令（Shell、Python、Perl、Powershell和Bat）和发送文件。查看更多
ECS实例
命令执行结果
文件发送结果
命令列表
公共命令
托管实例
智能匹配
请输入您要搜索的内容
标签筛选
注册新实例
实例ID / 名称
连接状态
网络地址
云助手版本
主机类型/名称
注册时间
操作栏
mi-hz03y2o72q7diww
ccccccccc-01
正常
110.52.195.105（公）
192.168.86.163（私有）
2.1.3.515
DESKTOP-48IQAVS
2023年10月1日 15:32:29
执行命令
远程连接
发送文件
注销
共1条，每页显示20条
1
20 条/页


nt authority\system
PS C:\Windows\system32> ipconfig
Windows IP 配置
以太网适配器 Ethernet0:
连接特定的 DNS 后缀 . . . . . : localdomain
本地链接 IPv6 地址. . . . . : fe80::bf18:e8d7:2769:ecf4%7
IPv4 地址 . . . . . : 192.168.86.163
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 192.168.86.2
PS C:\Windows\system32>


PYArkClient(www.pysafe.cn)
进程
驱动模块
内核层
内核钩子
应用层钩子
设置
监控
启动信息
注册表
服务
文件
网络
调试引擎
网络连接
Hosts文件
LSP
进程
PID
协议
本地地址
本地端口
远程地址
远程端口
状态
Tcp: 47, Udp: 22