H.2、阿里云安全中心平台

2023年10月1日 14:22

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

1、前言

云安全中心是一个实时识别、分析、预警安全威胁的服务器主机安全管理系统，通过防勒索、漏洞扫描修复、防病毒、防篡改、合规检查等安全能力，帮助用户实现威胁检测、响应、溯源的自动化安全运营闭环，保护云上主机、本地服务器和容器安全，并满足监管合规要求。[在笔者看来很适合权限维持]

aliyun安全中心提供终端控制平台和agent，用于监听和控制资产内的主机
agent安装后，会实时向云安全中心服务端上报客户端信息，包括：终端是否在线、终端采集所需数据等
agent运行条件，**Linux使用root账号运行、Windows使用system账号权限运行**。（这个条件在攻防当中利用妥当，直接不用提权）

文件下载时间：安装Agent插件后，aegis_client文件会下载到服务器中。

文件所在路径：

Windows 32位系统：C:\Program Files\Alibaba\aegis

Windows 64位系统：C:\Program Files (x86)\Alibaba\aegis

Linux系统：/usr/local/aegis

aegis_update功能：该目录下核心进程为AliYunDunUpdate，用于定期检测云安全中心Agent是否需要升级。

文件下载时间：安装Agent插件后，aegis_update文件会下载到服务器中。

文件所在路径：
Windows 32位系统：C:\Program Files\Alibaba\aegis
Windows 64位系统：C:\Program Files (x86)\Alibaba\aegis

Linux系统：/usr/local/aegis

以上两个文件安装Agent时会自动下载，同时还有很多可选文件，需要打开相应功能才能下载，具体见：https://help.aliyun.com/zh/security-center/user-guide/overview-of-the-security-center-agent?spm=a2c4g.11186623.0.0.45e94e8421q0r9

兼容性
Window(32/64)：

Windows Server 2022
Windows Server 2019
Windows Server 2016
Windows Server 2012
Windows Server 2008
Linux (64)：

Alibaba Cloud Linux
AlmaLinux
Anolis OS
CentOS 6、7、8
CentOS Stream
Debian 8及以上版本
Gentoo

OpenSUSE
Red Hat 6及以上版本
RHEL 6、7、8
Rocky Linux
SUSE
Ubuntu 14.04及以上版本
同时该Agent还支持众多不同内核版本的系统，
详见：
https://help.aliyun.com/zh/security-center/user-guide/overview-of-the-security-center-agent?spm=a2c4g.11186623.0.0.45e94e842lq0r9

从兼容性上看，直接降低了agent安装利用的难度。

2、Agent安装

一键自动安装Agent

前提条件：

- 服务器为阿里云服务器
- 服务器在运行，且网络无故障
- 服务器使用专有网络
- 服务器不能使用其他第三方安全软件
- 服务器所在地域支持一键安装功能
- 服务器已安装云助手

操作步骤：

i. 登录云安全中心控制台。在控制台左上角，选择需防护资产所在的区域：中国或全球（不含中国）。
ii. 在左侧导航栏，选择系统配置 > 功能设置。
iii. 在客户端 > 未安装客户端页签，在要安装Agent的服务器的操作列单击安装客户端，为该服务器安装Agent。

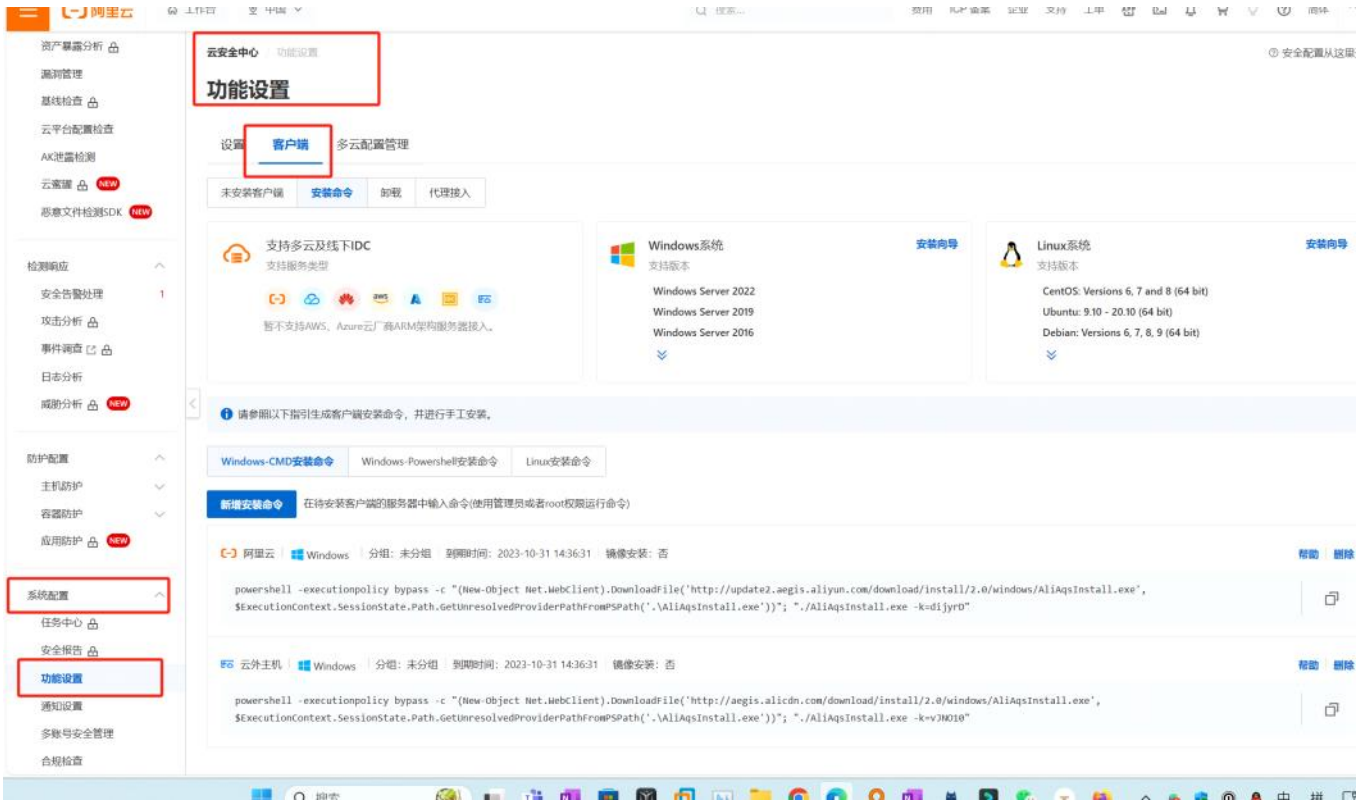
您也可以选中多台服务器后单击一键安装，批量安装Agent。
Agent插件安装完成约5分钟后，可在资产中心 > 主机资产 > 服务器页签，查看服务器的客户端在线情况。
这种方式只仅限于目标服务器是阿里云服务器，日常攻防工作当中，非云服务器目标资产还是占大多数的。这种方式不再赘述。

手动安装Agent

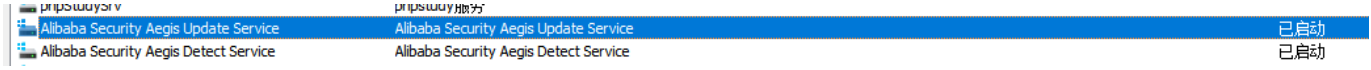
该方式为非云服务器上云统一管控提供了解决方案，可以将非云或其他云服务器托管到云安全中心进行统一管理。

1、登录云安全中心，区域选择全国

2、系统配置-功能设置-客户端-安装命令**[需要管理员权限运行]**



注意：安装后，服务器会启动三个进程：AliYunDunUpdate、AliYunDun和AliYunDunMonitor。其中AliYunDunMonitor进程会在其他两个进程启动后的**大概10分钟左右启动**。没启动前，云安全中心显示离线状态。



此时客户端主机已经上线，不过还无法进行远控，还需要安装云助手（如果服务器是云服务器，可以一键安装，安装后可进行远控）。通过云助手远控客户端。下面了解下云助手的作用和部署方式。

这里执行命令有两种方式

安装[执行远程运维bug，不是阿里云机器就会失效]

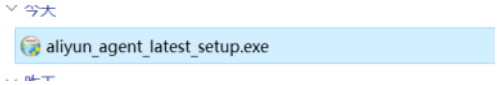
版本限制

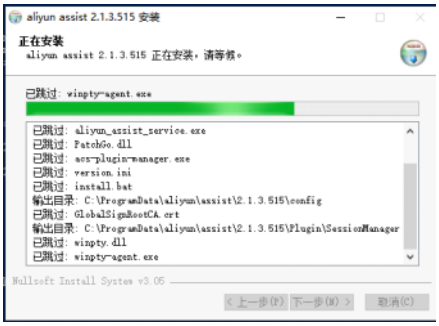
使用限制

- 只能通过控制台方式调用Python或Perl脚本。

  > **说明** 请确保目标实例具备正确的运行环境，例如执行Python命令时，需确保ECS实例已安装Pyth

- 创建的Bat、PowerShell或者Shell脚本和自定义参数在Base64编码后，使用场景与文件大小说明如下：
  - 创建命令：综合大小不能超过18 KB。
  - 立即执行并保存命令：综合大小不能超过18 KB。
  - 立即执行但不保存命令：综合大小不能超过24 KB。
  - 上传文件：文件大小不能超过32 KB。
- 一条命令中，自定义参数的个数不能超过20个。
- 您只能在以下操作系统中运行云助手命令：
  - Alibaba Cloud Linux
  - CentOS 6/7/8及更高版本
  - CoreOS
  - Debian 8/9/10及更高版本
  - OpenSUSE
  - Rocky Linux
  - RedHat 5/6/7及更高版本
    RedHat中需要您自行下载rpm包安装云助手Agent，具体操作，请参见安装云助手Agent。
  - 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





安装完成之后，我这个还是没有上线，建议使用ECS云助手

第二个是使用ECS云助手[下一篇文章讲解]