奇安信
新一代网络安全领军者

奇安信天擎终端安全管理系统单机安装部署手册 V10.7

创建时间：2023 年 10 月 25 日

修改时间：2025 年 08 月 21 日

网络安全服务热线：95015

公司网址：https://www.qianxin.com/

联系地址：北京市西城区西直门外南路 26 号院 1 号楼

邮编：10004

● 版权声明

目录

第1章 前言

1.1 文档范围

本文档主要介绍奇安信天擎终端安全管理系统 V10.0 的安装和初始化配置，主要包括系统介绍、部署介绍和环境准备、管理系统单机部署、客户端的安装与卸载、系统基本配置。

1.2 文档对象

本文档适合希望了解奇安信天擎终端安全管理系统安装和部署的用户、系统管理员、工程师进行阅读。

1.3 技术支持

用户支持邮箱：kefu@qianxin.com

用户支持热线：95015

奇安信官网：https://www.qianxin.com/

第2章 系统介绍

2.1 产品概述

奇安信天擎终端安全管理系统是面向政府、企业、金融、军队、医疗、教育、制造业等大型企事业单位推出的集病毒防护与终端安全管控于一体的解决方案。奇安信天擎终端安全管理系统，以大数据技术为支撑、以可靠服务为保障，它能够为用户精确检测已知病毒木马、未知恶意代码，有效防御 APT 攻击，并提供终端资产管理、漏洞补丁管理、系统安全加固、安全运维管控、终端准入管理、基线核查、数据防泄漏等诸多功能。

第3章 安装部署和更新

3.1 部署介绍

奇安信天擎终端安全管理系统（以下简称奇安信天擎，管理中心为奇安信天擎管理服务端的 WEB 端，客户端为奇安信天擎客户端）是集终端防病毒和安全管控于一体的管理系统，软件形态交付并部署在企业内部，内网中的办公终端安装奇安信天擎客户端，奇安信天擎客户端通过管理中心进行升级、更新等，管理中心具有缓存功能，同样的数

据文件只会下载一次，可以大幅节省企业总出口宽带。奇安信天擎客户端根据管理中心制定的安全策略，进行体检、杀毒和修复漏洞等安全操作，在互联网模式下终端可以直接连接的云查杀系统，进行云查杀，在隔离网模式下使用离线工具，定期从相关的服务器下载病毒库、木马库、漏洞补丁文件等，更新到管理中心并提供终端更新。

部署过程：

1) 安装奇安信天擎。

2) 部署奇安信天擎客户端。

3) 设置统一杀毒、修复漏洞、终端管控等安全策略，确保终端安全。

4) 终端集中管理。

5) 对于隔离网环境，定期使用离线工具下载数据，并更新到管理中心。

3.2 部署准备

3.2.1 管理中心安装环境要求

3.2.1.1 环境鉴别

Linux x86_64 机型类似下图，Intel、海光、兆芯处理器为 Linux x86_64 机型

鉴别指令：cat /proc/cpuinfo | fgrep 'model name'

```
[root@devops001v ~]# cat /proc/cpuinfo | fgrep 'model name'
model name      : Intel(R) Xeon(R) Gold 5318Y CPU @ 2.10GHz
model name      : Intel(R) Xeon(R) Gold 5318Y CPU @ 2.10GHz
model name      : Intel(R) Xeon(R) Gold 5318Y CPU @ 2.10GHz
model name      : Intel(R) Xeon(R) Gold 5318Y CPU @ 2.10GHz
model name      : Intel(R) Xeon(R) Gold 5318Y CPU @ 2.10GHz
model name      : Intel(R) Xeon(R) Gold 5318Y CPU @ 2.10GHz
model name      : Intel(R) Xeon(R) Gold 5318Y CPU @ 2.10GHz
model name      : Intel(R) Xeon(R) Gold 5318Y CPU @ 2.10GHz
```

Linux ARM_64 机型类似下图，ARM 处理器为 Linux ARM_64 机型

鉴别指令：cat /proc/cpuinfo | fgrep 'model name'

```
[es-ops@jrd01v ~]$ cat /proc/cpuinfo | fgrep 'model name'
model name      : ARMv8 CPU
model name      : ARMv8 CPU
model name      : ARMv8 CPU
model name      : ARMv8 CPU
model name      : ARMv8 CPU
model name      : ARMv8 CPU
model name      : ARMv8 CPU
model name      : ARMv8 CPU
```

Windows x86_64 机型如下图，Intel、海光、兆芯处理器为 Windows x86_64 机型

鉴别方法：我的电脑->右键属性查看

3.2.1.2 系统要求

系统类型	系统型号	特殊说明
Windows x86_64	Windows Server 2012 R2 64 位 Windows Server 2016 64 位 Windows Server 2019 64 位 Windows Server 2022 64 位	适合 Windows 单机部署场景 CPU 支持：intel,海光，兆芯

Linux x86_64	RedHat 7.6-7.9 CentOS 7.5-7.9 银河麒麟高级服务器操作系统 V10sp1(Tercel) 银河麒麟高级服务器操作系统 V10sp2(Sword) 银河麒麟高级服务器操作系统 V10sp3 2303(Lance) AnolisOS(龙蜥)7.9 BC-Linux el7.8 OpenEuler20.03(LTS-SP3) OpenEuler22.03(LTS-SP4) OpenEuler 24.03 LTS（10.7.0.2700） RockyLinux 8.8 AnolisOS(龙蜥)8.9（10.7.0.2800） RedFlag Asianux Server Linux V8（10.7.0.2800）	适合 linux 单机部署场景 CPU 支持：intel，海光，兆芯
Linux ARM64	银河麒麟高级服务器操作系统 V10sp1(Tercel) 银河麒麟高级服务器操作系统 V10sp2(Sword) 银河麒麟高级服务器操作系统 V10sp3 2303(Lance) 统信服务器操作系统 V20(1020e) 统信服务器操作系统 V20(1021e) 统信服务器操作系统 V20(1050e) 统信服务器操作系统 V20(1050u2e) 统信服务器操作系统 V20(1070e)（10.7.0.2800）	适合 ARM 单机部署场景 CPU 支持：飞腾，鲲鹏 ARM 架构服务器同等配置终端负载点数,CPU、内存需要按上调 2 倍资源评估处理

	银河麒麟高级服务器操作系统 V10sp3 2403(Halberd)（10.7.0.2800）	

其他说明：

1) **Windows 单机部署，需要设置 4G 虚拟内存。**详细资源要求详见 KB47609。

2) 支持在物理环境或者虚拟化环境部署。

3) 不同的硬件资源、业务模块所支撑的点数会有差异，磁盘读写速度会影响安装和业务访问的速度以及挂载点数，可下载 CrystalDiskMark、Diskspd 等工具检测。

4) **磁盘性能过低可能会导致安装失败**，请参考第 5.1 章节中低 IOPS 配置，调整系统参数后再尝试重新安装。

5) 对于 Windows Serer 2012 R2 操作系统，在安装奇安信天擎前请确认是否开启了 Windows Update 并进行了更新，或者在控制面板安装程序中检查是否安装了补丁 KB2999226，如果没有请下载并安装，如果安装失败请依次尝试安装 KB2919355、KB2919442 后再次尝试。安装补丁后请重启操作系统。

3.2.1.3硬件配置要求

最大支持终端点数及资源	最低资源 要求	
1000 以下	CPU	4 核 2.4Ghz
	内存	8G
	硬盘	300G，推荐 SSD,磁盘 IOPS 不低于 5000
	网卡	千兆单网卡
1000-5000	CPU	8 核 2.4Ghz
	内存	16G
	硬盘	300G，推荐 SSD，磁盘 IOPS 不低于 5000
	网卡	千兆单网卡

5000-10000	CPU	16 核 2.4Ghz
	内存	32G
	硬盘	1T，推荐 SSD，磁盘 IOPS 不低于 5000
	网卡	千兆单网卡
10000-20000	CPU	32 核 2.4Ghz
	内存	64G
	硬盘	2T，推荐 SSD，磁盘 IOPS 不低于 5000
	网卡	千兆单网卡

特殊说明：

1、**ARM 架构服务器同等配置终端负载点数，CPU、内存需要按上调 2 倍资源评估处理。**

2、**4c8g 部署低资源部署将不支持 edr、天机、云查等业务，后续资源扩充也不支持业务动态扩充，需要铲掉重装。**

3、上述最低磁盘存储按照所有数据持续存储 180 天推算。

4、4 核 8G 硬件环境承载终端点数接近最大支持上限数量时，服务器可能出现性能存在压力的风险。4 核 8G 硬件环境低于 10.6 升级到此版本时，需要先升级到 10.6.0.2600 批次大版本再升级到此版本，不支持从低于 10.6 批次的版本跨批次跳升到此版本。

5、低于 8C16G 不会安装威胁检查与响应（EDR）、移动安全、病毒防护云查杀。

3.2.1.4特殊业务说明

业务	系统配置
使用终端审计功能	每千终端每天需**额外准备**约 1GB 存储
涉及补丁文件存储	需根据覆盖的操作系统**额外准备** 500GB 到 1TB 存储（仅 WinPC 系统含 Win10 时需 700GB，如果包含 WinServer 系统及其他软件建议使用 1T）

安全空间模块	最低 8C16G
使用 EDR 基础版功能	每千终端每天需**额外准备**约 1GB 存储
EDR 高级版	需要配置终端大数据分析平台，仅全新安装时支持，不支持动态扩容增加业务 a) 天擎管理中心服务器 4C8G 配置不支持 EDR（含 EDR 高级版、EDR 基础版）。 b) 天擎管理中心服务器 8C16G 配置可支持 100 点的 EDR 高级版。 c) 天擎管理中心服务器 16C32G 配置可支持 3000 点的 EDR 高级版。 d) 如有更多的终端需要采用集群部署。 注意：最新配置参考《奇安信天擎终端安全管理系统 V10.0R7R8-EDR 资源评估手册.xlsx》
天机	天机业务不支持 windows 部署。

3.2.2互联网资源

注：若服务器网络访问受限，需确保如下资源可访问。

域名	IP 段	端口	IP 示例	备注
darwin.b.qianxin.com	无固定 IP 信息	443 80		S3（解析到 CDN 供应商，IP 列表无法固定，建议做 DNS 白名单）
darwin.qianxin.com	101.227.27.128/27	443 6781	101.227.27.154	云升级服务
oss-zz-zzt.yun.qianxin.com	36.99.137.0/24	443	36.99.137.45	云查服务

styxcl.b.qianxin.com	无固定 IP 信息	443		云查服务
styxps.b.qianxin.com	无固定 IP 信息	443		云查服务
styxapsl.b.qianxin.com	无固定 IP 信息	443		云查服务
styxqde.b.qianxin.com	无固定 IP 信息	443		云查服务
styxcl.b.qianxin.com	无固定 IP 信息	8443		终端漫游直连云查服务
cstyx.b.qianxin.com	无固定 IP 信息	6781		终端直连云查服务，仅适用于管理中心低配置（x86:4C8G /arm64:8C16G）
api.license.qianxin.com	103.114.156.64/26	6781	103.114.156.68	许可证
dlleak.qianxin.com	无固定 IP 信息	80 443		补丁下载
file.soft.qianxin.com	无固定 IP 信息	80 443		软管下载
dl.qianxin.com	无固定 IP 信息	80 443		库文件下载服务
errorreport.b.qianxin.com	无固定 IP 信息	10443	103.114.156.68	日志服务

3.2.3服务器时间

1. 请确保服务器的系统日期、时间和时区与当地时间相同，若不相同请调整正确服务器的系统日期、时间和时区；
2. 若拥有 NTP 服务器可提前在服务器中设置好。

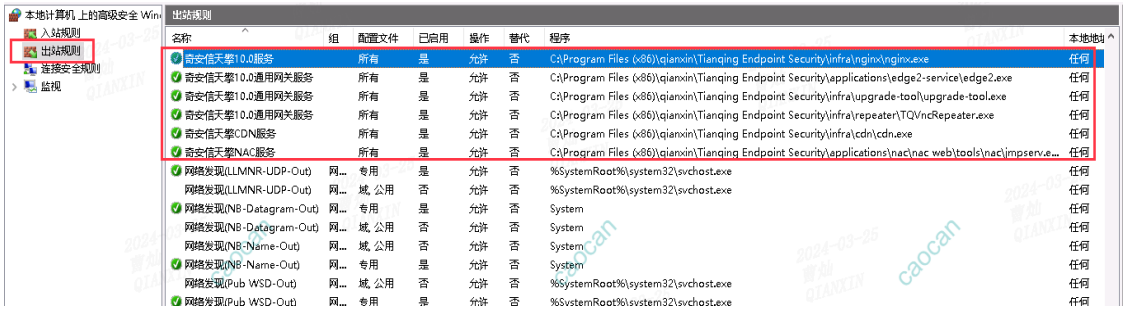
3.2.4域名及 NAT 模式访问

参见控制中心管理员手册-管理中心通信地址

3.3 管理中心部署

3.3.1Windows 单机部署网络连通性要求

奇安信天擎管理中心对外暴露如下端口，为了确保网络连通性，请检查防火墙的放行策略已做了例外（正常安装完毕后会自动添加）并在外部对服务器进行测试；



端口支持自定义配置，在管理中心所在服务器上打开奇安信天擎配置工具可以查看和修改端口，其他端口如终端远程协助可按需在管理中心确认和修改。

注意：如果部署客户端后再修改端口会导致已经部署好的客户端失联。

3.3.1.1Windows 单机部署默认开启端口

端口信息	端口说明	访问源	业务说明
6785	终端通信服务端口，TCP 协议	客户端	常规服务如任务、策略、级联通信等

19345	终端文件传输 HTTPS 服务端口，TCP 协议	客户端	在线部署页面及文件上传下载
19346	终端文件传输服务 HTTP 端口，TCP 协议，随着 HTTPS 端口变化而变化	客户端	在线部署页面及在线安装时文件下载
36781	服务接入端口，TCP 协议	客户端、WEB 端	微服务接入
28443	管理中心访问端口，TCP 协议	WEB 端	
80/443	下载在线部署客户端的页面的简化端口，默认不启用。 通过“服务端配置工具”开启“客户端在线部署地址切换”则启用 80 或者 443 端口。	WEB 端	在线部署页面及在线安装时文件下载

3.3.1.2Windows 单机部署特殊业务端口

端口信息	端口说明	访问源	业务说明
5500	被控端口	客户端	远程协助默认端口
5901	主控端口	客户端	远程协助默认端口
19092	级联数据端口	下级服务端	下级上传数据的端口

3.3.2 Windows 服务器单机部署（包含升级）

升级部署可升级路线：参考 KB35578。

3.3.2.1安装包说明

奇安信天擎终端安全管理系统的安装文件名称为：QI-ANXINTianqing-server-[版本信息]_[系统平台 Win/Linux]_[文件 MD5]，示例：QI-ANXINTianqing-Server-Windows_10.6.0.2600_A5E091A9B4922364861BBE5BF245B445.iso，其中：

1）10.6.0.2600 是版本号。

2）Windows 是系统平台，表示当前安装包是 Windows 服务器版本。

3）A5E091A9B4922364861BBE5BF245B445 是安装文件的 MD5，可用 MD5 工具验证是否正确。

3.3.2.2安装包获取方式

在奇安信官网（地址见 1.3 章节）申请产品试用，获得许可证 ID 后在奇安信官网激活绑定时根据提示获取下载链接下载，或者拨打 95015。

需要升级时获取安装包：

1）在管理中心>系统管理>更新管理>主程序更新 Tab 页的“管理中心主程序更新设置”可以设置或手动点击“检查更新”，然后根据提示找到下载的最新安装包安装更新；

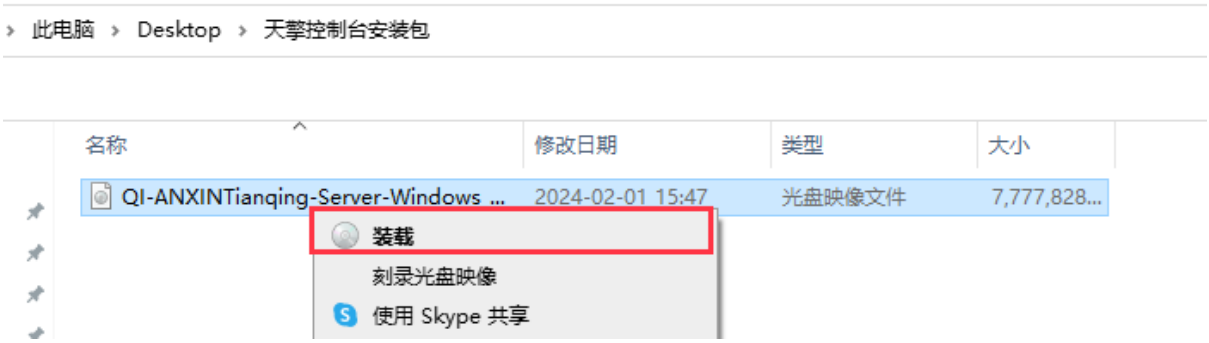
2）通过许可证 ID 从奇安信官网获取安装包然后拷贝至服务器安装更新。

3.3.2.3全新部署及升级部署

获取 ISO 包后打开然后双击运行目录下的 Setup.exe 安装程序即可开始奇安信天擎的安装；安装时请确认好网络连通性，且部署后随意更改发布的通信地址会导致管理中心和客户端无法访问。

1）**开始部署**

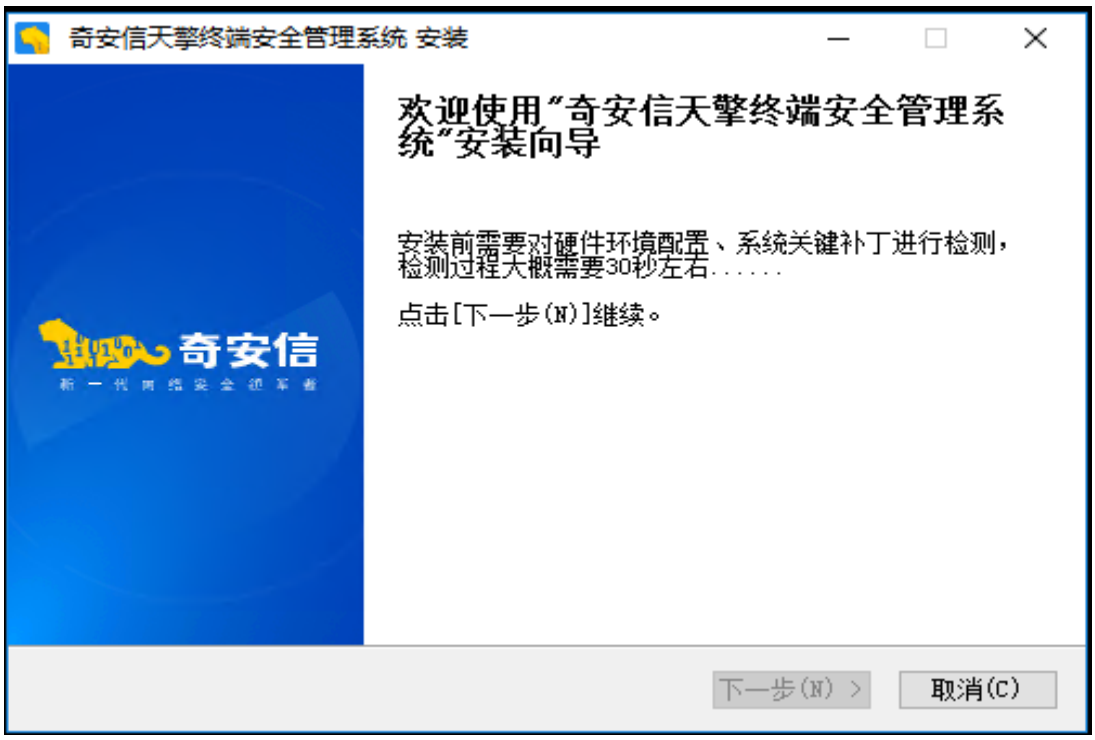
装载：右键点击安装包并选择装载菜单，完成装载安装包操作。



开始部署：双击 setup.exe 进行部署

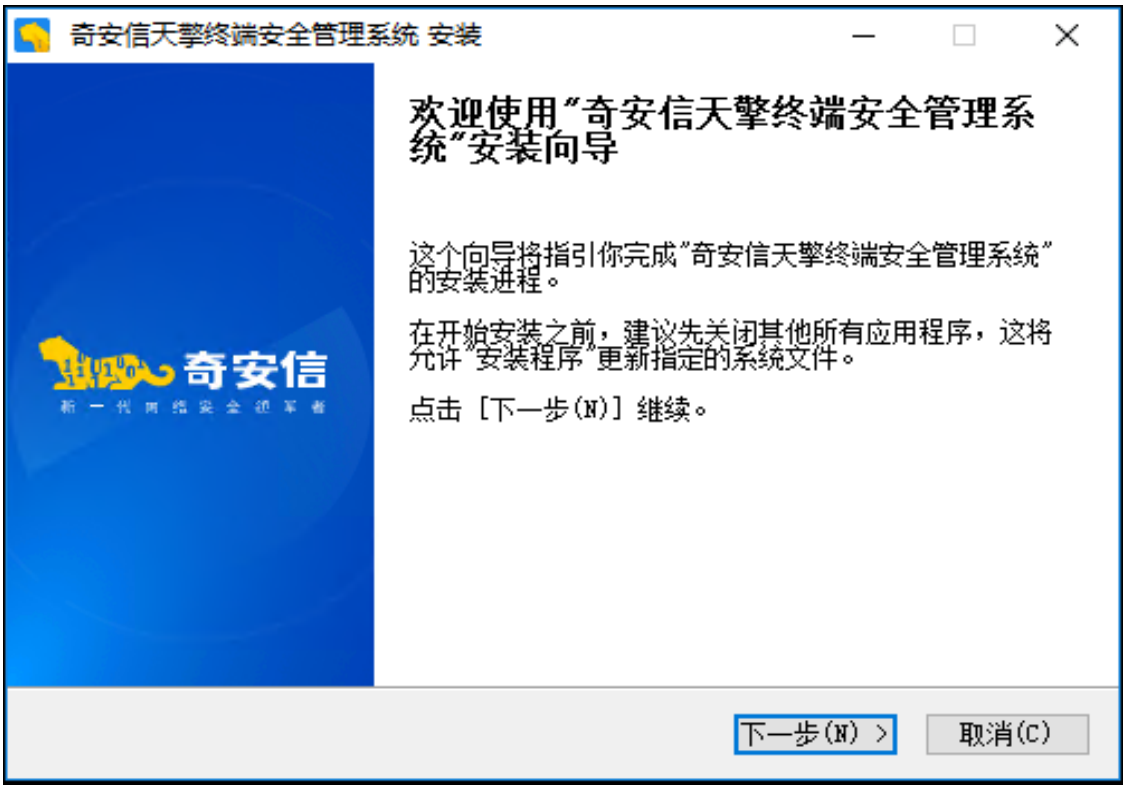
2）**环境检查**

安装程序启动后，会检查用户环境，包括系统版本、必备补丁、服务器账号等问题。



3）**安装向导及许可条款确认**

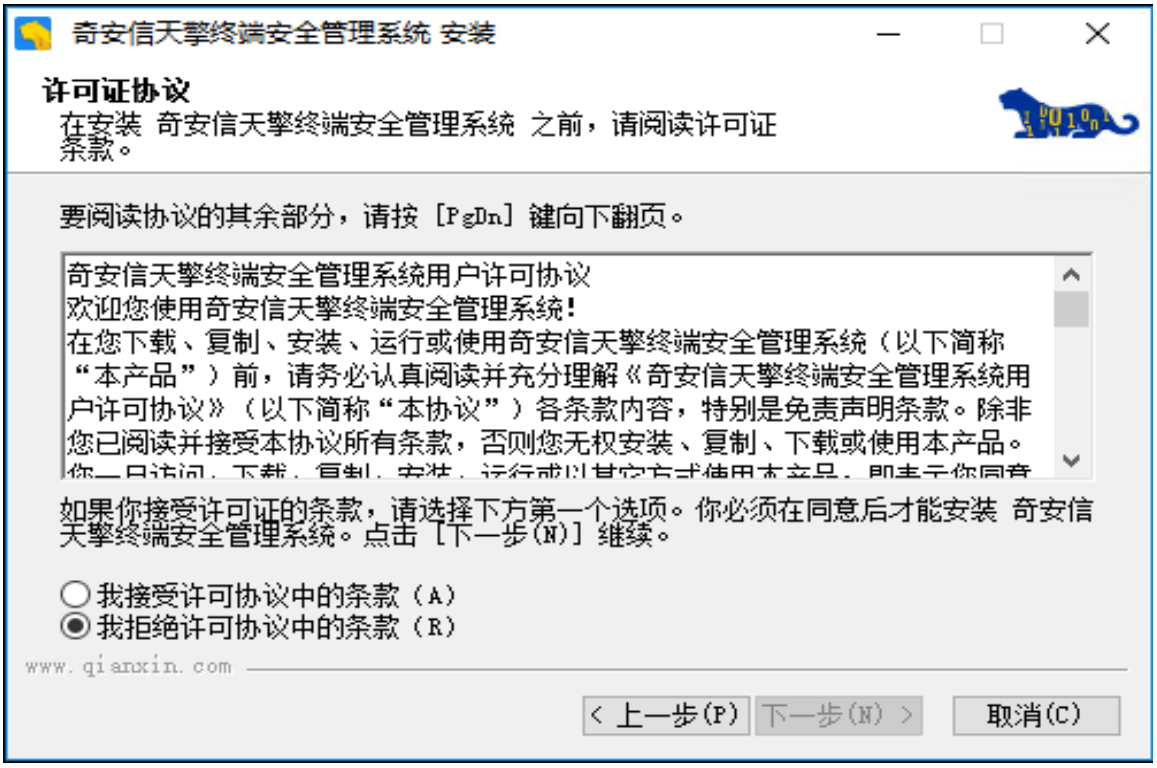
安装向导：环境检测完成后，会进入“奇安信天擎”安装向导初始化界面。



许可确认：单击[下一步]按钮进入“许可证协议”界面，如果此时单击[取消]按钮，则退出安装。

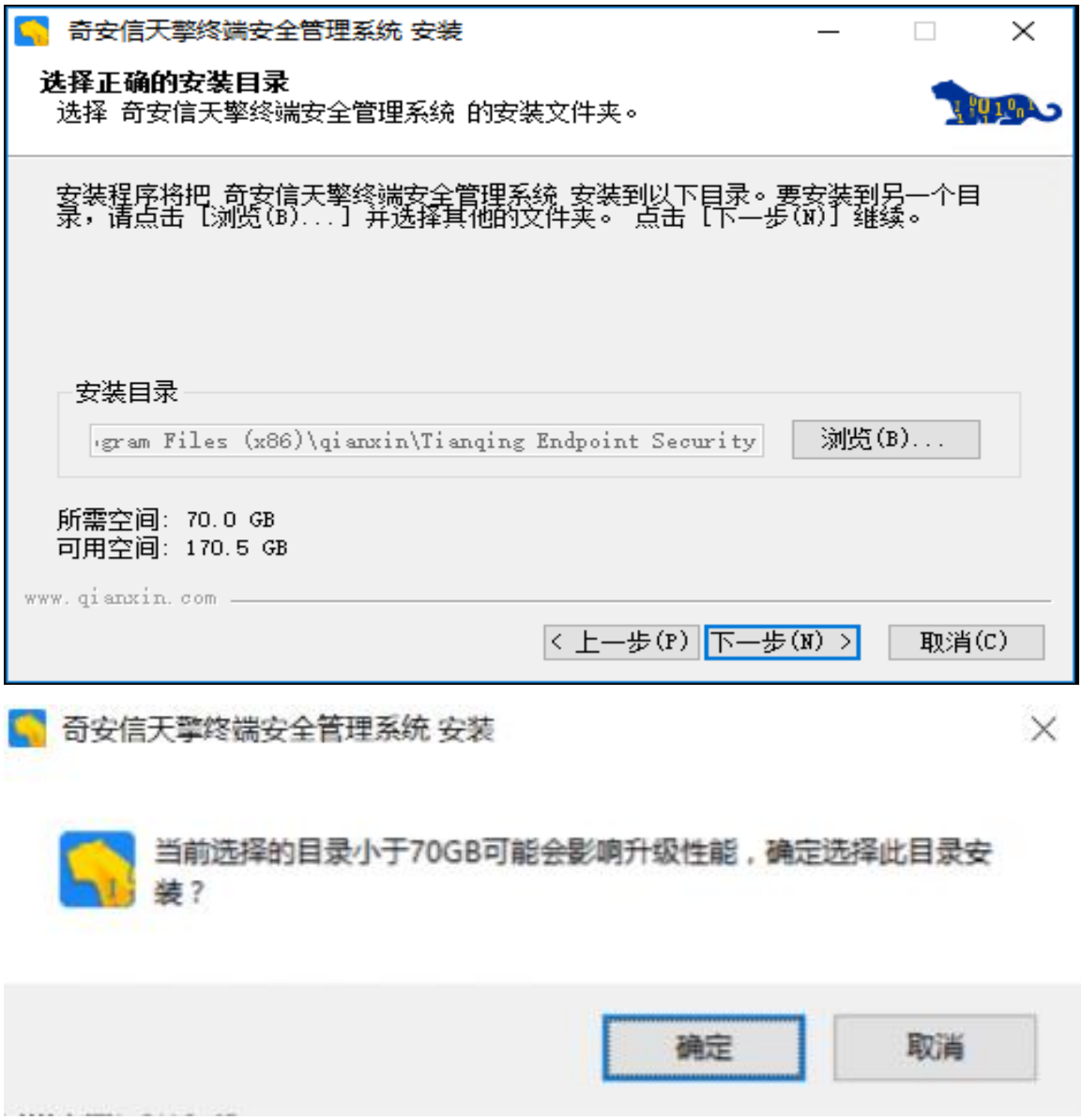
建议您认真对奇安信天擎许可证协议进行阅读和理解，在您阅读完后，选择“我接受许可证协议中的条款”后可以点击[下一步]按钮进行继续安装，如果您对许可协议存在疑议，

您可以选择“我拒绝许可证协议中的条款”并点击[取消]按钮终止本次安装。



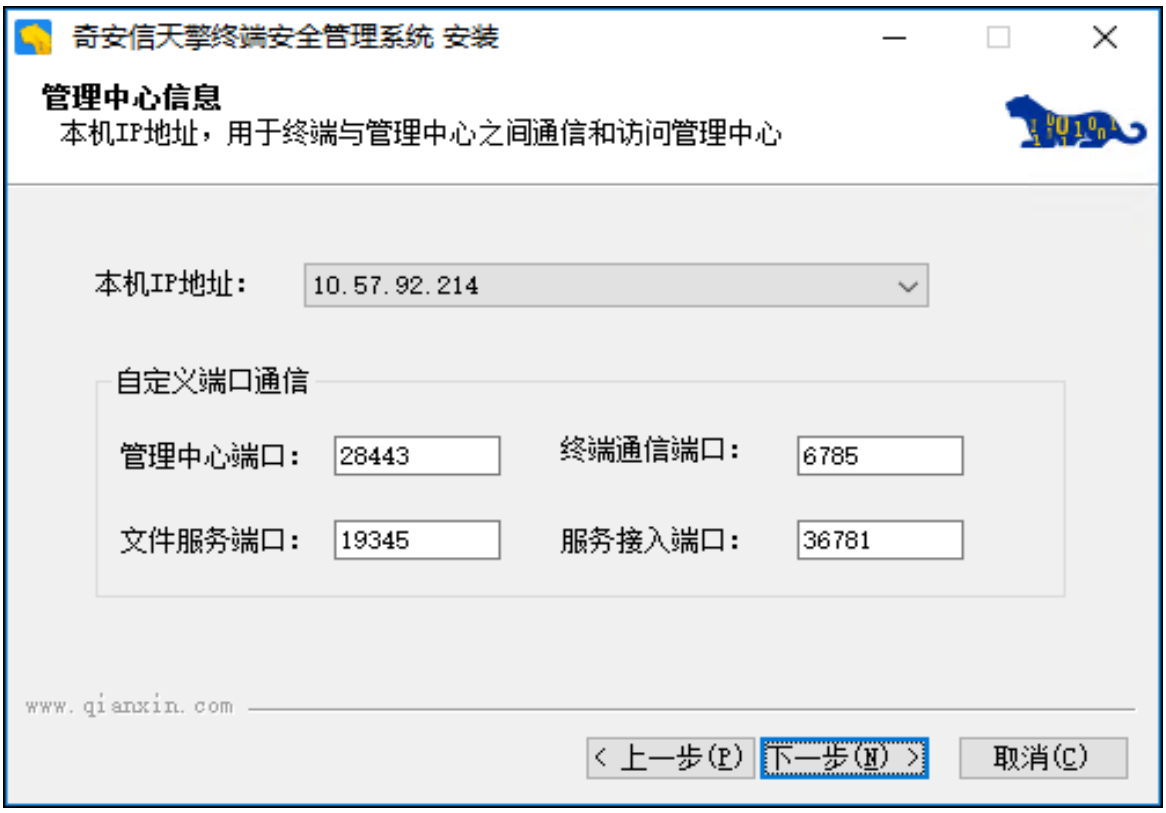
4）安装目录选择（仅全新部署可选择目录）

点击[浏览]按钮，选择奇安信天擎的安装路径，系统默认安装路径为 C:\Program Files (x86)\qianxin\Tianqing Endpoint Security，您可以根据实际情况修改对应的安装路径（建议安装路径设置为非系统盘，且所在盘符剩余空间大于 70GB）。



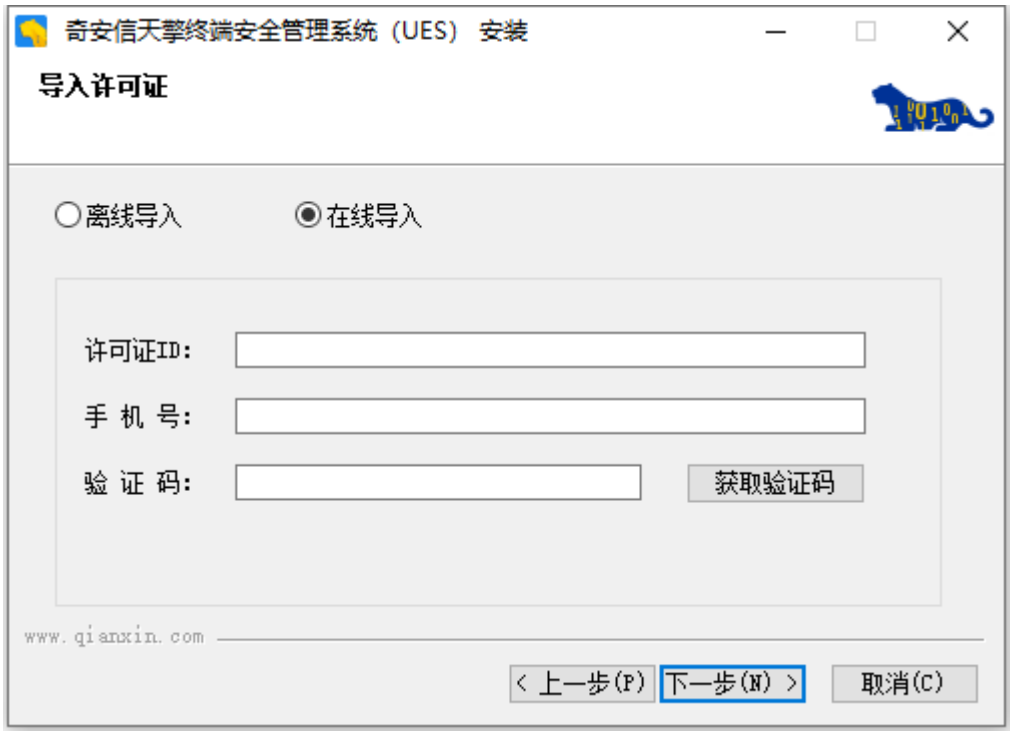
5）管理中心信息配置（仅全新部署会有）

管理系统的通信地址是管理中心的地址和管理终端的默认地址，只有通过访问管理系统通信地址才可以访问管理中心。确认要发布的通信地址并保证各端口可联通。

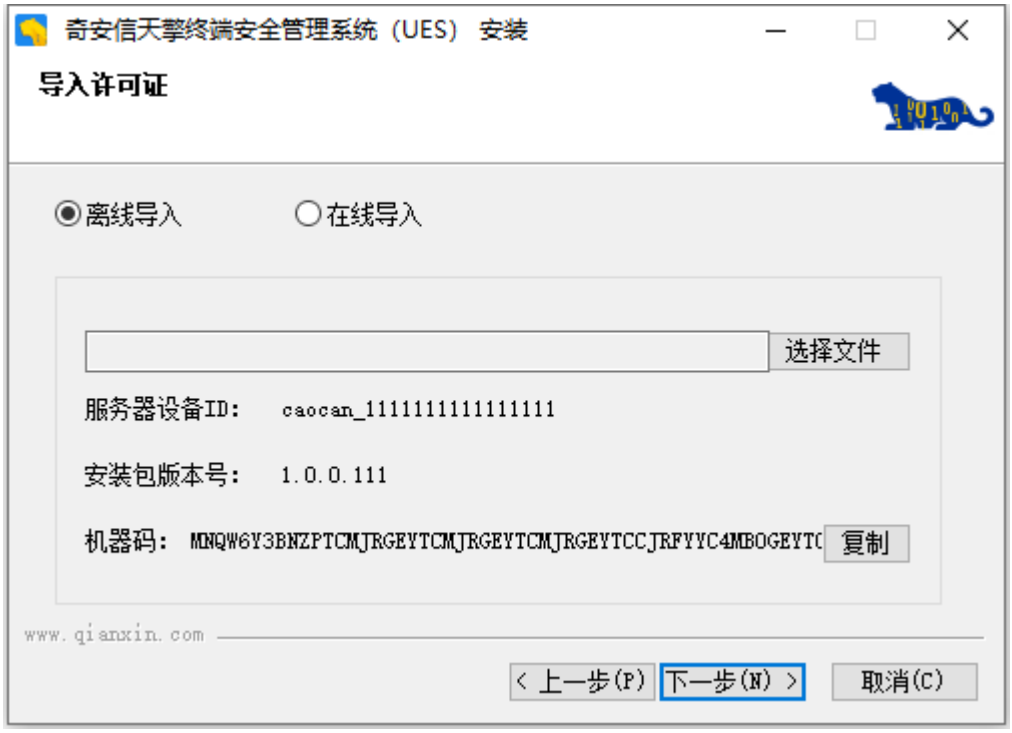


6) **导入许可证（仅全新部署会有）**

在线导入：联网情况下，输入许可证 ID、手机信息，点击下一步后许可证将可自动导入。

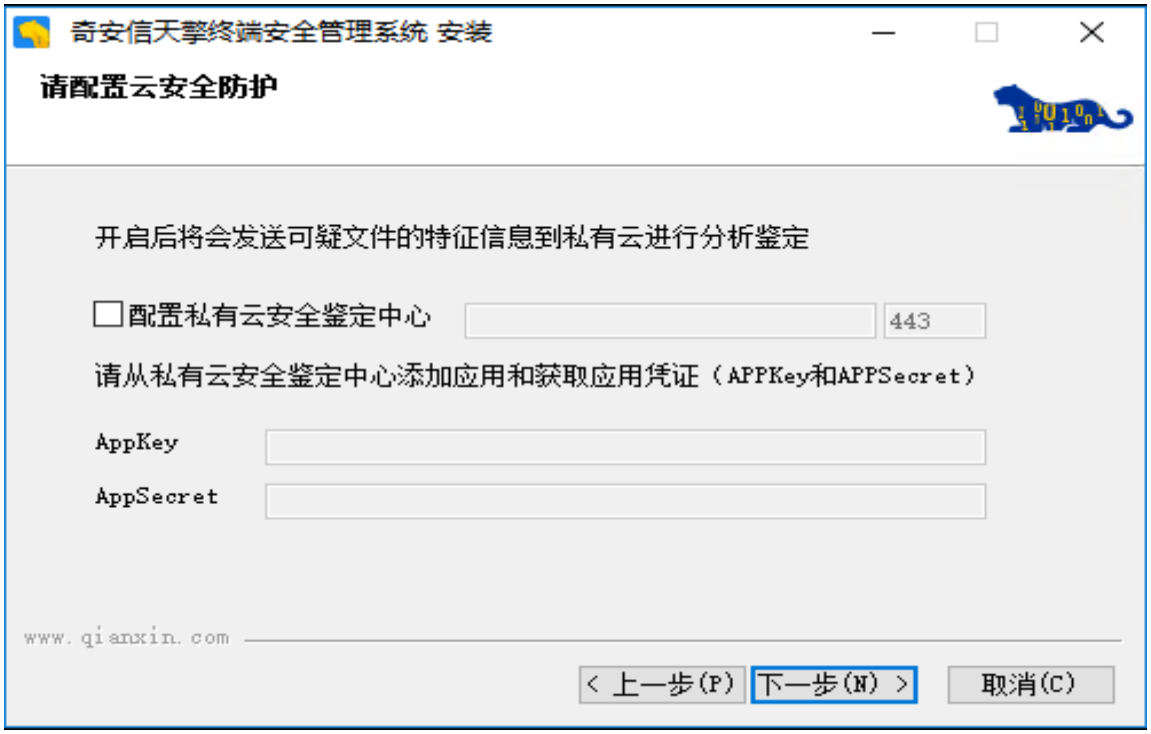


离线导入：隔离网环境中，可点击离线导入，将机器码复制后在奇安信官网与许可证进行绑定激活后，下载许可证文件进行导入。



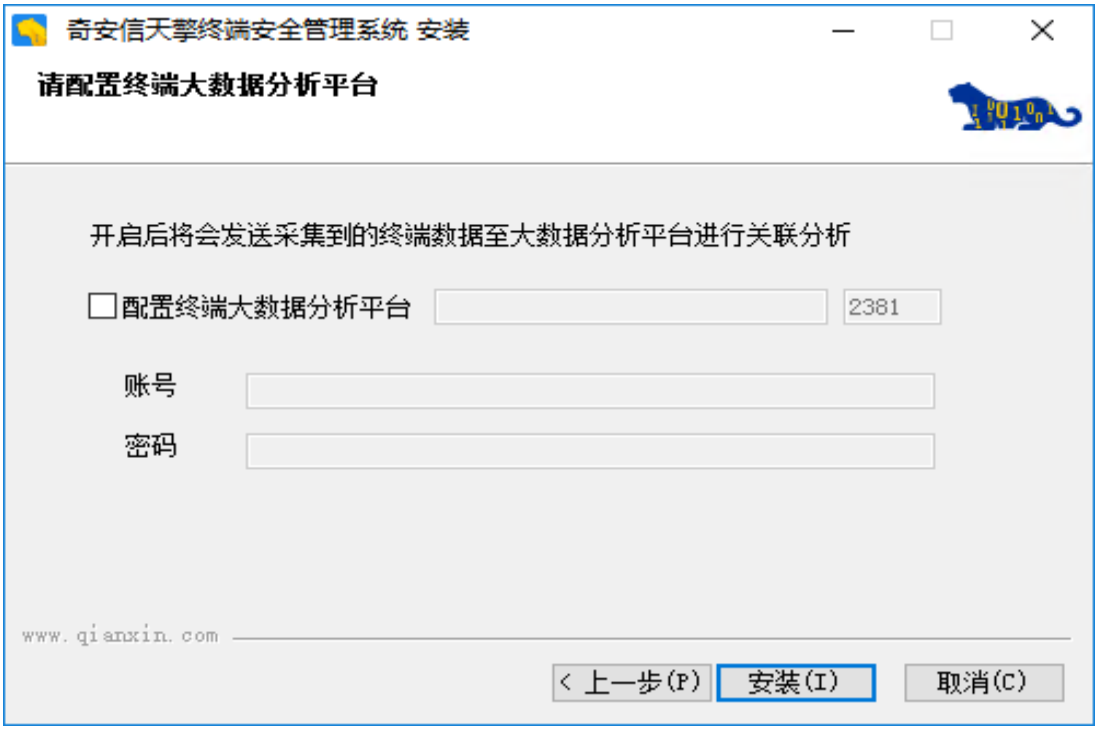
7）配置云安全防护（可选，仅全新部署会有）

如果购买并部署了私有云安全鉴定中心，则可选择开启并配置，然后点击[下一步]则继续安装，点击[上一步]按钮回到上一步操作界面，如果点击[取消]按钮，则会终止本次安装。



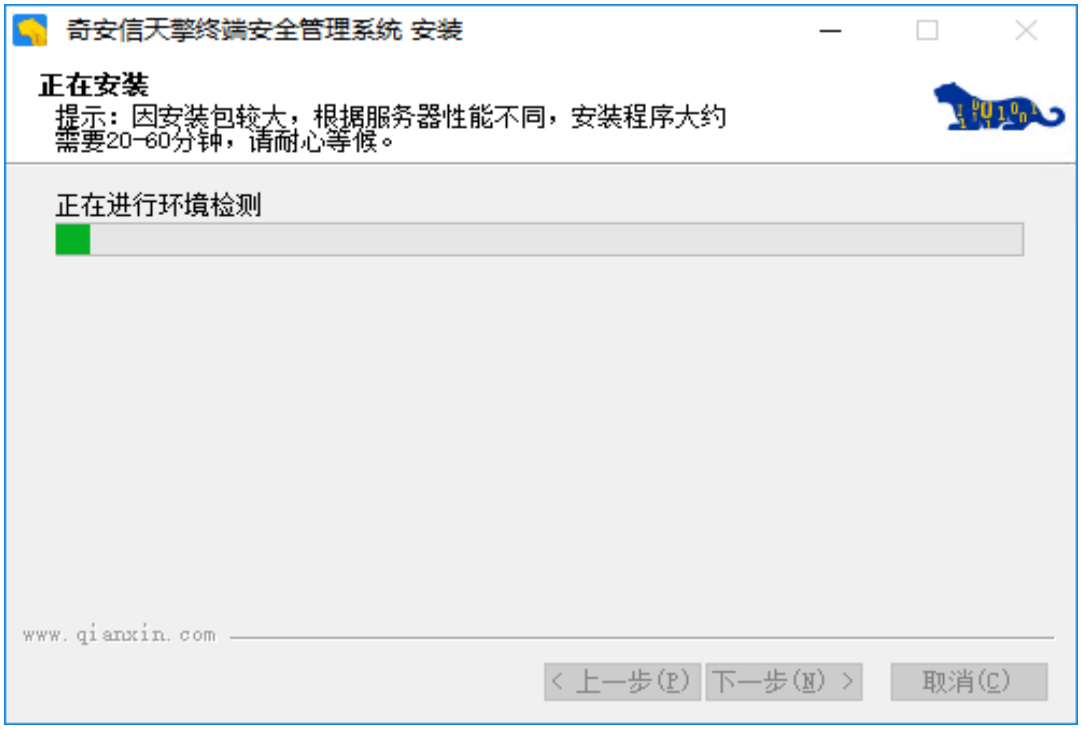
8）**配置终端大数据分析平台（可选，仅全新部署会有）**

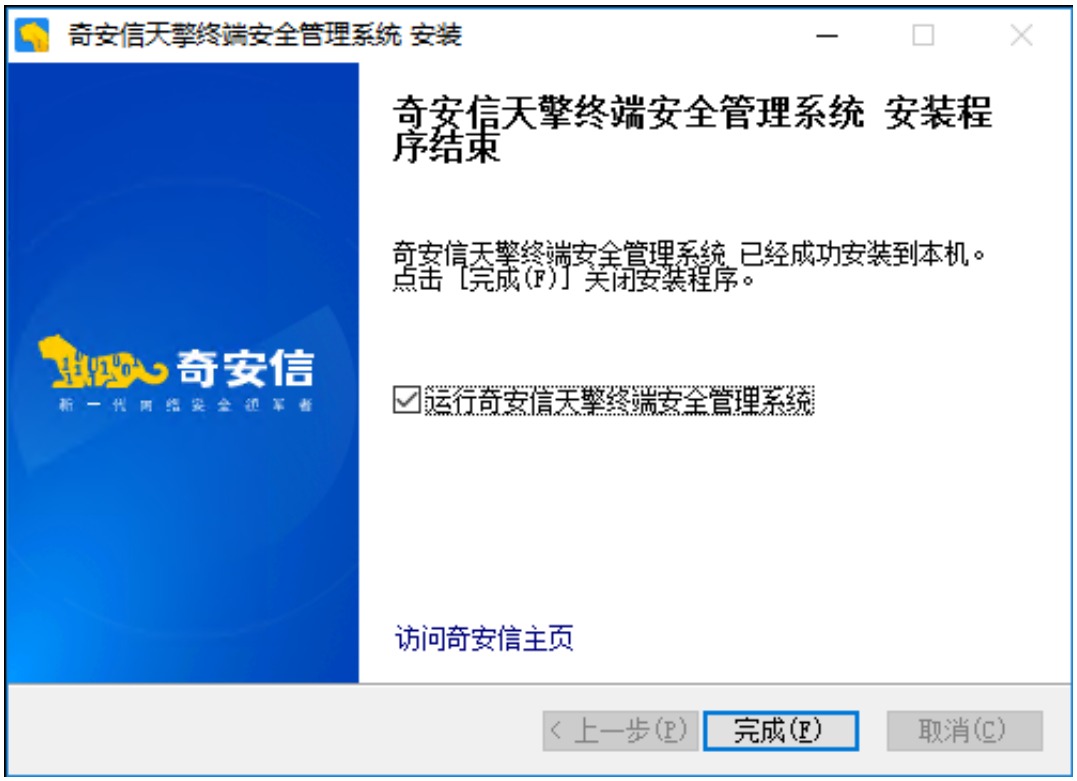
如果购买并部署了终端大数据分析平台，可选择开启并配置，输入“终端大数据分析平台地址”和端口“2381”，账号和密码可留空。然后点击[安装]则开始进行安装，点击[上一步]按钮回到上一步操作界面，如果点击[取消]按钮，则会终止本次安装。



9）**安装**

上述配置完成后即开始释放文件安装，由于文件较多，根据不同服务器性能安装时间大约在 20~60 分钟，请耐心等待安装完成。（磁盘 IOPS 越低，安装时间越长，低于 240 时，失败率很高）

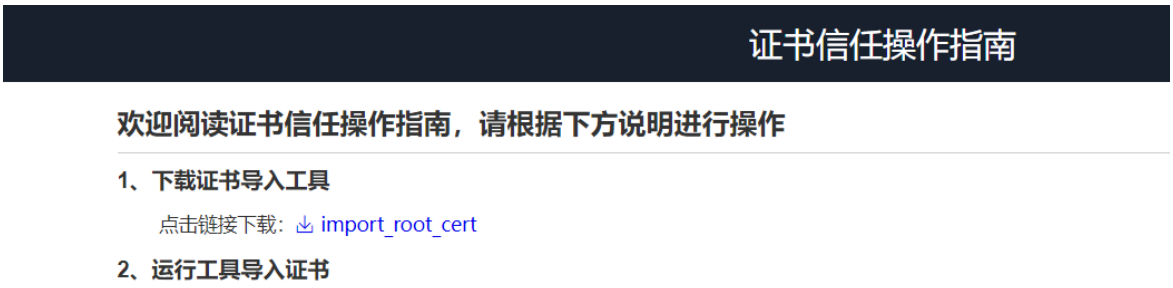




此时您已经成功完成了奇安信天擎的安装。当勾选“运行奇安信天擎终端安全管理系统” 并点击[完成]按钮时，会自动打开浏览器跳转到管理中心登录页。

3.3.2.4首次登录

Windows 操作系统首次访问如果遇到如下提示需要先点击[**查看帮助文档**]根据提示安装 CRT 证书后重新打开浏览器。



其他操作系统首次访问管理系统如果遇到如下提示需要先点击[查看帮助文档] 根据提示安装 CRT 证书后重新打开浏览器。

说明：

1、证书信任操作指南链接为：“https://管理中心地址:28443/cert-manual”。

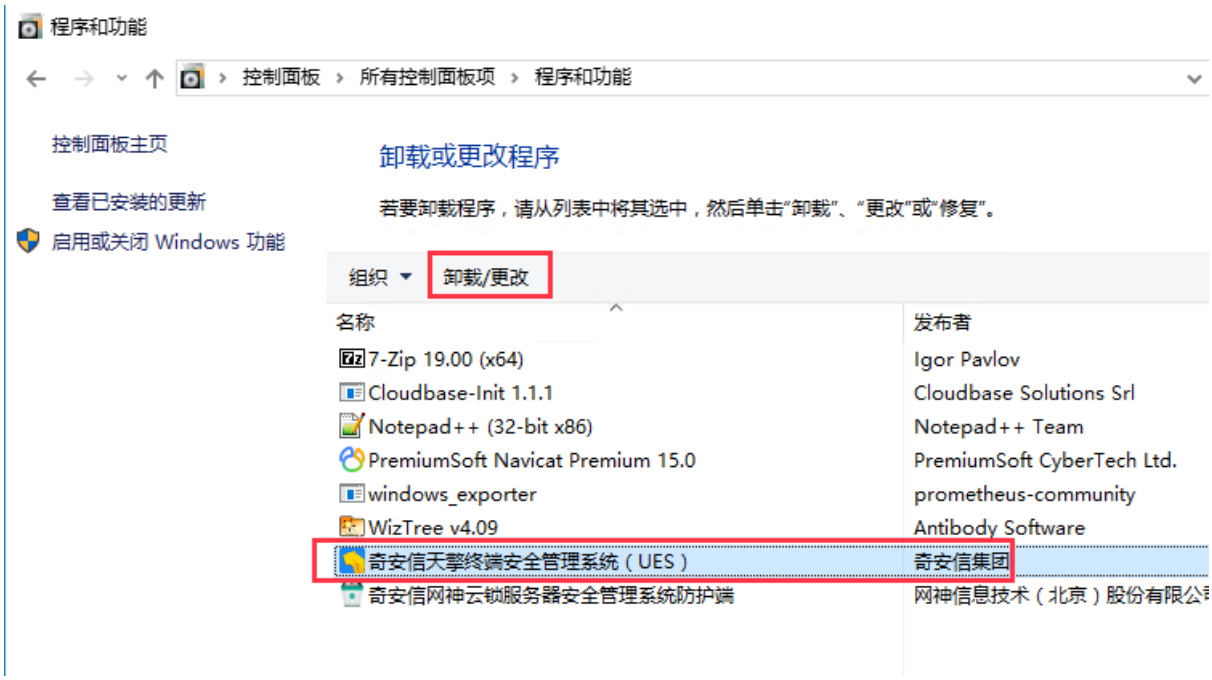
2、访问管理中心，请使用 Chrome 84 以上版本，Edge 84 以上版本的浏览器或奇安信浏览器访问。

再次访问管理中心，进入管理中心登录界面，如下为系统初始用户名和密码

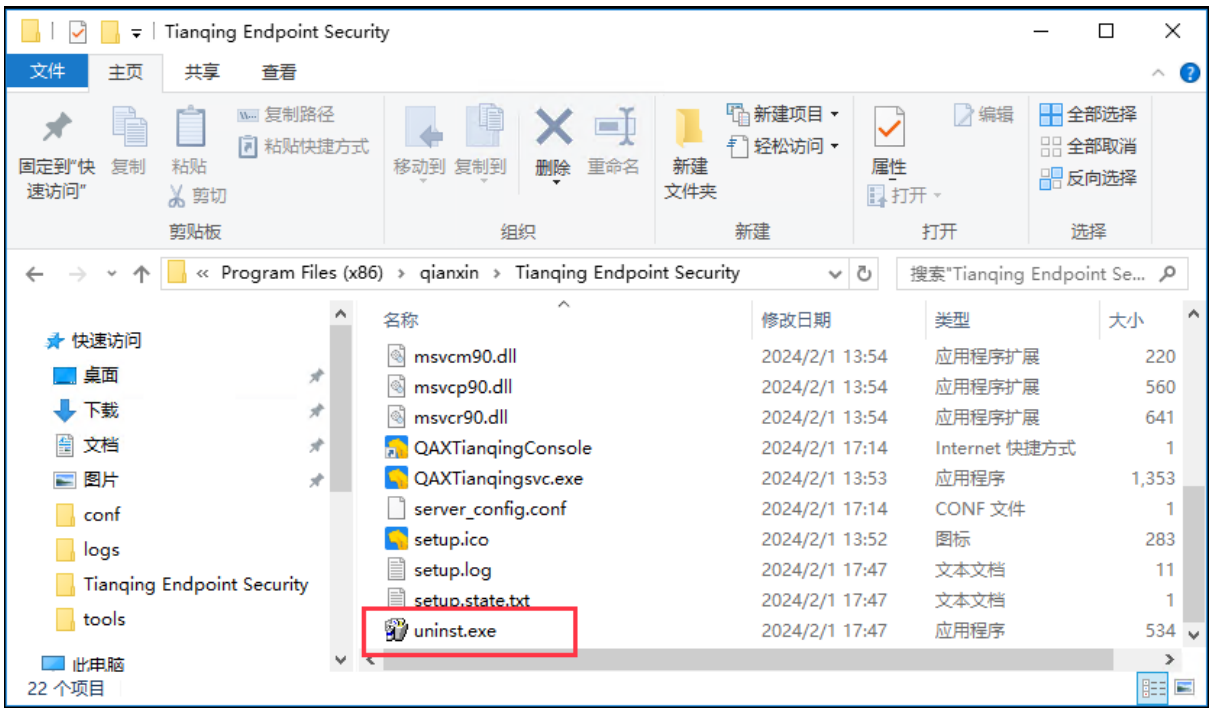
初始用户名	初始密码	备注
system	Admin123@	创建新的管理员账号后，初始用户将不可用，请保存好新帐号的密码

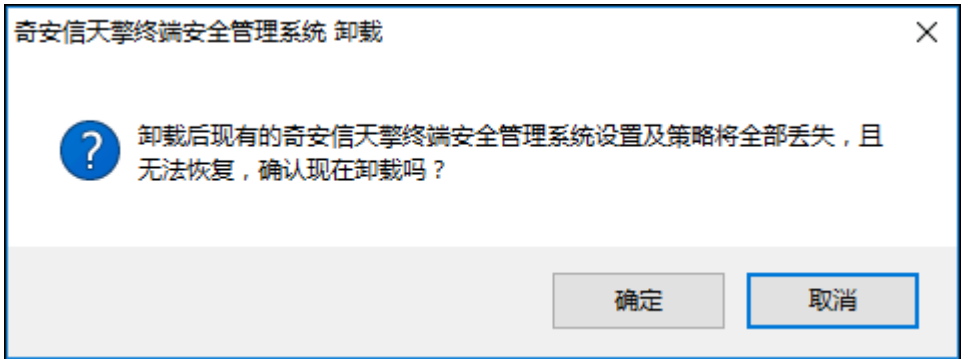
3.3.2.5 卸载

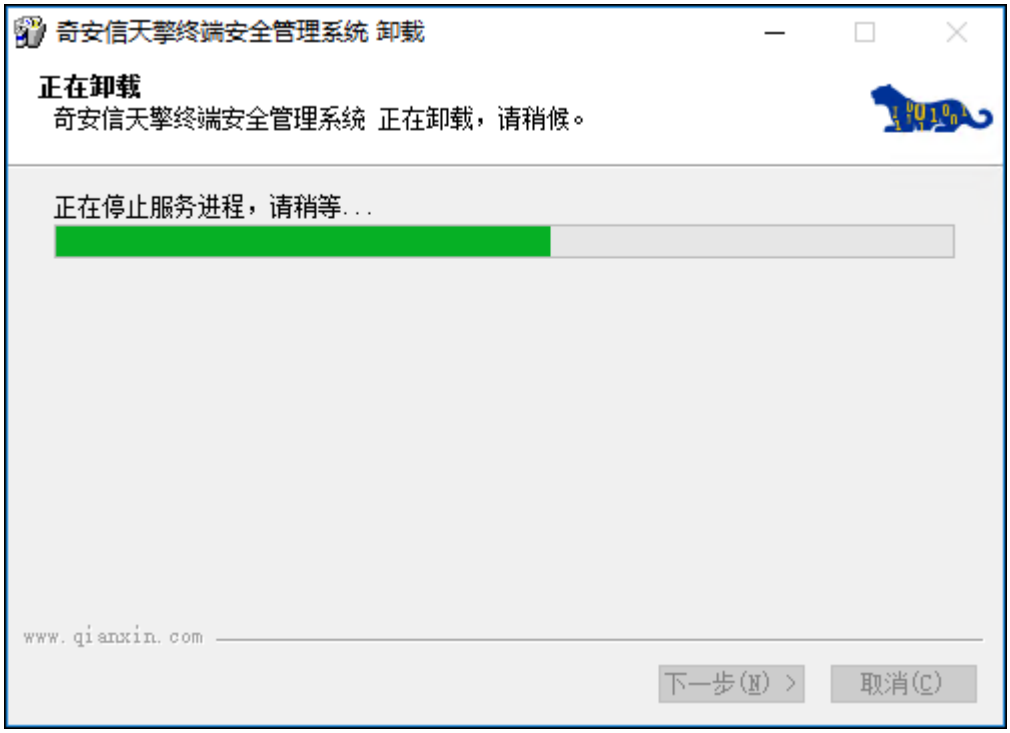
卸载 1：进入控制面板选中奇安信终端管理系统，并点击卸载按钮。



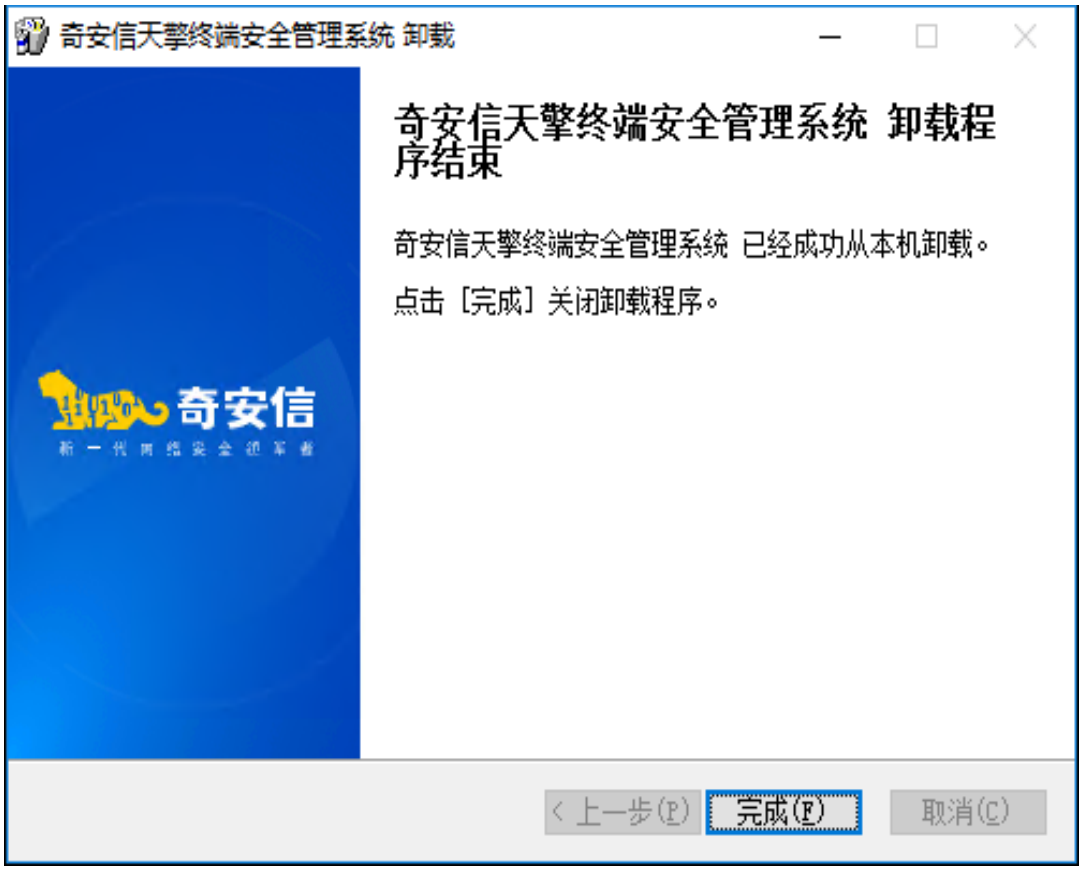
卸载 2：打开安装目录，双击执行 uninst.exe 进行卸载。







卸载完成后，会提示对应的完成向导。



点击[完成]，卸载完毕，退出卸载向导。

注意事项：

许可证重新绑定新设备 ID 后会重新生成新资产 ID，之前挂载的客户端因资产 ID 不匹配而无法与管理中心通信，需卸载后重新安装。

3.3.2.6Windows 版本配置工具

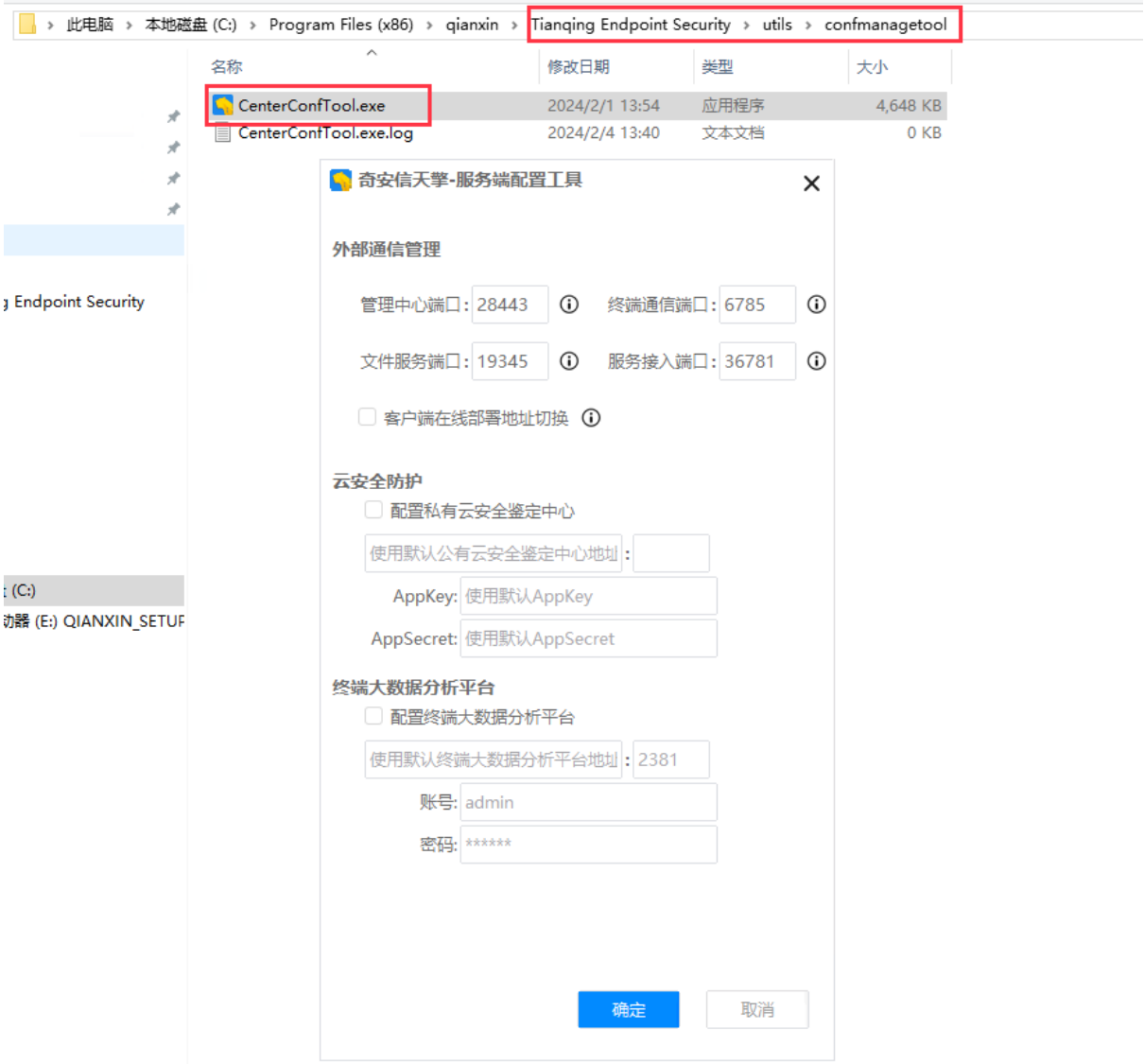
部署完成后，如果需要修改对外通信端口、配置私有云安全鉴定中心和终端大数据分析平台，可在开始菜单找到或搜到到“服务端配置工具”，在使用此工具前确保管理中心已经导入许可证。

1、外部通信管理。各端口的说明参见 3.2.2 章节，可在此调整默认端口，**调整后之前部署的客户端将失联，需重新部署**；如果勾选“客户端在线部署地址切换”功能，在线下载客户端的地址将展示为：“https://管理中心地址”。

2、云安全防护。如果客户购买并部署了私有云安全鉴定中心，确认其地址、端口，以及在鉴定中心创建的应用凭证（AppKey、AppSecret）后，则可运行此工具配置。

3、终端大数据分析平台。如果客户购买并部署了终端大数据分析平台，配置时可参考 3.4.2 章节。

工具所在位置，及界面如下图：



3.3.3信创与 Linux 服务器单机部署网络连通性要求

奇安信天擎管理中心对外暴露如下端口，为了确保网络连通性，请检查防火墙的放行策略已做了例外（正常安装完毕后会自动添加）并在外部对服务器进行测试；

端口支持自定义配置，在管理中心所在服务器上打开奇安信天擎配置工具可以查看和修改端口，其他端口如终端远程协助可按需在管理中心确认和修改。

注意：如果部署客户端后再修改端口会导致已经部署好的客户端失联。

3.3.3.1信创与 Linux 单机部署默认开放的端口

端口信息	端口说明	访问源	业务说明

30080	终端通信服务端口，TCP 协议	客户端	常规服务如任务、策略、级联通信等
32185	终端文件传输 HTTPS 服务端口，TCP 协议	客户端/移动终端	在线部署页面及文件上传下载
32186	终端文件传输服务 HTTP 端口，TCP 协议，随着 HTTPS 端口变化而变化	客户端/移动终端	在线部署页面及在线安装时文件下载
30081	服务接入端口，TCP 协议	客户端、WEB 端	微服务接入
30082	管理中心访问端口，TCP 协议	WEB 端	
5223	Apple APNs 网关服务器 ，TCP 协议	iOS 移动终端	iOS 移动终端链接 Apple APNs 网关服务器,例如：IOS 消息推送功能。
53	DNS 服务器 ，TCP 协议	管理中心	DNS 服务器，进行域名解析
22	系统调试，TCP 协议	WEB 端	管理员登录后台系统进行系统调试
9080	可视化部署临时端口，部署完可关闭，TCP 协议	WEB 端	可视化部署
31001/31002/31003/31004(UDP，双向)/31006/31007	自建的流媒体引擎,远程控制服务,TCP、UDP 协议	移动终端	远程控制服务

3.3.3.2 信创与 Linux 单机部署特殊业务端口

端口信息	端口说明	访问源	业务说明
30090	主控端口	客户端	远程协助默认端口
30091	被控端口	客户端	远程协助默认端口

9092	级联数据端口	下级服务端	下级上传数据的端口

3.3.4信创与 Linux 服务器单机部署（包含升级）

升级部署可升级路线：参考 KB35578。

3.3.4.1安装包说明

奇安信天擎终端安全管理系统的安装文件名称为：QI-ANXINTianqing-Server-[系统平台 Win/Linux]_[版本信息]_[文件 MD5]，示例：QI-ANXINTianqing-Server-Linux_Allinone_10.7.0.1010_99963E43448E95CDC55781141F0A07C5.tar，其中：

1、10.7.0.1010 是版本号。

2、Linux 是系统平台，表示当前安装包是 Linux 服务器版本。

3、99963E43448E95CDC55781141F0A07C5 是安装文件的 MD5，可用 MD5 工具验证是否正确。

安装包获取方式：在奇安信官网（地址见 1.3 章节）申请产品试用，获得许可证 ID 后在奇安信官网激活绑定时根据提示获取下载链接下载，或者拨打 95015。

3.3.4.2全新安装

3.3.4.2.1 安装前检查

安装前请拔掉 U 盘，移动硬盘等移动设备，防止设备 ID 生成异常。

安装时有如下预检查，需要在安装前确认：

检查项	操作命令
检查 cpu 核心数	检查 cpu 核心数，如果包含准入，至少需要 16 核；否则，至少需要 4 核。 操作命令： cat /proc/cpuinfo | grep "processor" |wc -l
检查内存大小	检查内存大小，如果包含准入，至少需要 32G；否则至少需要 8G。 操作命令：free -h
检测操作系统是否合法	目前支持的操作系统： FusionOS，统信，欧拉，麒麟, Anolis, Centos7.5-7.9； 查看操作系统类型，可以使用命令： cat /etc/os-release | grep -E ^NAME
检测 umask 的值是否合法	执行 umask 命令查看 如果值不是 0022，需要修改/etc/bashrc 最后一行为:umask 0022，保存退出， 执行命令 source /etc/bashrc ， 执行命令 umask，返回为 0022 代表修改成功
检测 PATH 环境变量是否合规	PATH 环境变量必须包含 /usr/local/bin， 查看 PATH 环境变量的命令： echo $PATH
检测 selinux 是否关闭	查看命令： getenforce； 如果命令输出不是 Disabled， 就 vi /etc/selinux/config，将配置文件中的 SELINUX=enforcing 修改为 SELINUX=disabled，使用:wq 保存，最后重启服务器生效
检测 ulimit 的值是否合法	查看命令： ulimit -n ； 如果命令输出小于 655360 就不合法，需要 vi /etc/security/limits.conf 在末尾加上两行（注意：每行分隔使用 tab 键） * hard nofile 1020000 * soft nofile 1020000 完成后使用 :wq 保存，需要重启服务器生效
安装包 md5 检测	安装前，需要检测安装包的 MD5 值是否正确； 操作命令： md5sum 包路径
检测时区应该为东八区	执行 date -R 命令，命令输出应该包含 +0800
需要 root 用户或者有 sudo 权限的用户	看看 sudo su - 命令是否能够成功
关闭 firewalld	systemctl stop firewalld
关闭 swap	先执行 swapoff -a，再执行 vi /etc/fstab，将 swap 相关的注释掉
安装路径所在分区至少有 70G 的空闲空间	执行 df -lhT 命令查看
之前没有安装过 docker 且不能存在 docker 残余文件	执行命令 systemctl list-units | grep docker 查看是否安装过 docker 执行命令 systemctl list-units | grep containerd 查看是否安装过 containerd
检测服务器是否配置默认路由	ip route | grep default 应该有标准输出 (与客户沟通，检查服务器环境，添加默认路由信息)
检查当前系统时间是否正确	常看当前系统时间的命令： date -R

3.3.4.2.2 图形化安装

1) 创建目录，下载安装包，解压文件。解压命令为：

```
Shell>  tar -xvf QI-ANXINTianqing-Server-*.tar
```

```
[root@whlinux01v qaxdata]# mkdir -p /qaxdata/10.7.0.1010
[root@whlinux01v qaxdata]# cd /qaxdata/10.7.0.1010/
[root@whlinux01v 10.7.0.1010]# wget http://dl.qianxin.com/tianqing/QI-ANXINTianqing-Server-Linux_Allinone_10.7.0.1010_99963E4344
[root@whlinux01v 10.7.0.1010]# tar -xvf QI-ANXINTianqing-Server-Linux_Allinone_10.7.0.1010_99963E43448E95CDC55781141F0A07C5.tar
plan_client/
plan_client/plan_client
plan_client/third_party/
plan_client/third_party/linux_allinone/
plan_client/third_party/linux_allinone/README
plan_client/third_party/linux_allinone/tqv10.tar.gz
```

2) 解压完毕后执行

```
Shell> sudo sh install.sh
```

```
[success] 操作系统: centos, 检查通过
[success] cpu核数: 8, 检查通过
[success] 内存: 16430552, 检查通过
[success] umask: 0022, 检查通过
[success] PATH: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/root/bin, 检查通过
[success] SELINUX=disabled, 检查通过
[success] ulimit: 102400, 检测通过
[success] fs.file-max: 1024000, 检测通过
[success] Hostname 检测通过
[success] 时区为: +0800, 检测通过
[warning] 服务器时间: 2023-05-18 14:34:04, 是否正确? [Y/n]
y
[success] 服务器检查通过, 安装服务启动中...
```

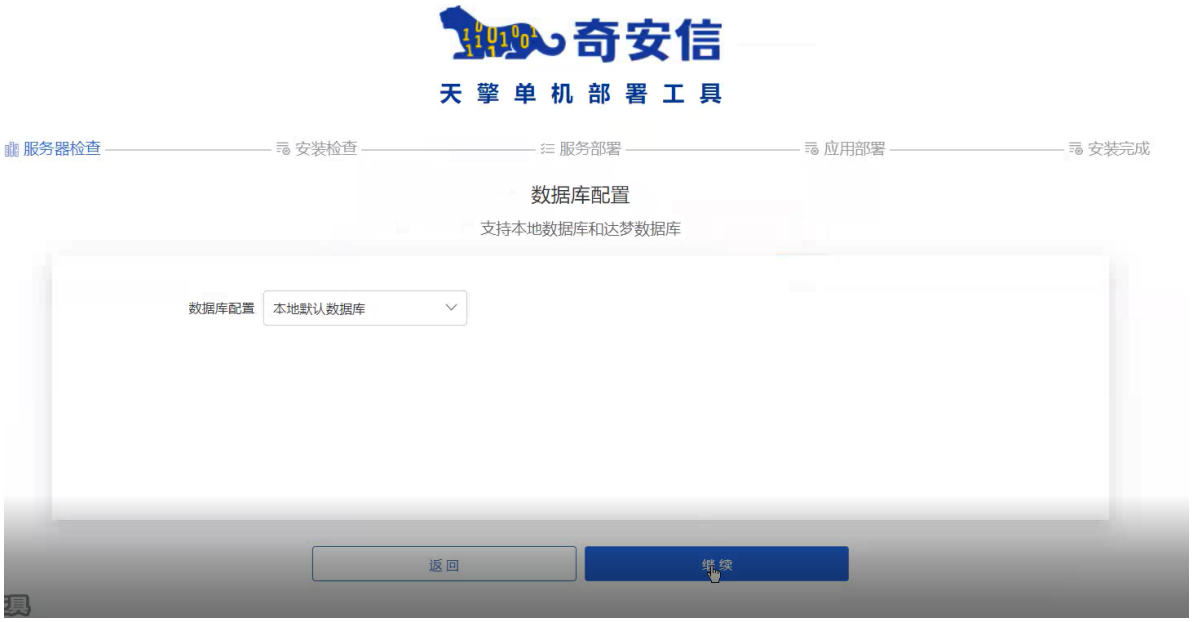
程序进行安装前检测,请根据提示进行相关问题处理或确认

3）**浏览器访问安装部署配置页面。**浏览器输入 http://IP:9080 访问安装部署页面，点击开始部署。

4) 许可证导入。复制机器码到奇安信官网进行绑定，下载许可证文件后导入。

5) 数据库配置。支持本地数据库和达梦数据库，默认为本地数据库

- 选择本地默认数据库，无需任何设置，直接点击继续：



➢ 选择达梦数据库：

需填写数据库地址、账号及密码。

- 数据库地址由“IP:端口”组成。若达梦采用单机部署，则只需配置一个地址；若达梦采用主备集群方式部署，需配置多个地址，多个地址之间用逗号分隔，参考下面示例截图。
- 可通过测试连接测试与数据库的连接是否成功。

注意：

- **使用达梦数据库，管理中心无法使用备份/还原能力进行灾备**
- **使用达梦数据库，管理中心在升级前需要手动备份数据库，否则升级失败后，无法自动回滚，会导致数据、功能异常，最严重后果会导致管理中心需要彻底铲掉后重新安装。**
- 支持达梦数据库版本是：8.1.2.174，10.7.0.2800 版本支持 8.1.3.162，查看版本方法：select build_version from v$instance;
- 达梦数据库安装时的初始配置要满足如下：

参数名	参数值	说明
loginMode	1	通过加密验证和 IP 白名单提升数据库安全性
COMPATIBLE_MODE	0	使用达梦数据库自身的 SQL 语法和特性，不兼容其他数据库
CASE_SENSITIVE	1	大小写敏感
PAGE_SIZE	32K	数据分页大小，务必设置为 32K

CHARSET	GB18030	字符集
MAX_SESSIONS	3000/10000	单机部署设置为 3000；集群部署设置为 10000；
VM_STACK_SIZE	1024	数据库的配置超过了栈
UNDO_RETENTION	86400	建议事务撤销时间控制在 1 天
ENABLE_IGNORE_PURGE_REC	0	关闭空间快速释放
用户密码要求		支持“英文大小写” + “数字" + "_!()” 其它特殊字符不支持

未特殊说明，都采用数据库部署时的默认值。

- 如果达梦采用守护集群方式部署（HA），填写数据库地址时，务必按照主备顺序填写，即“ip1:端口 1,ip2,端口 2”，其中 ip1 是主库，ip2 是备库。
- 选择达梦数据库安装时将不会安装准入服务。
- 权限要求：在达梦数据库中，需要赋予用户 SYSDBA 权限，或赋予用户以下权限

```
-- 创建用户
CREATE USER "QAX_TIANQING" IDENTIFIED BY "Test123456" PASSWORD_POLICY 6;
-- 授予角色
GRANT "PUBLIC", "RESOURCE" TO "QAX_TIANQING";
-- 授予系统权限
GRANT SELECT ANY TABLE, SELECT ANY VIEW, CREATE MATERIALIZED VIEW, SELECT ANY MATERIALIZED VIEW TO "QAX_TIANQING";
```

权限解释：

PUBLIC 角色：在达梦数据库中，PUBLIC 是一个特殊的角色，所有用户默认都会拥有这个角色。它包含了一些基础的、通用的权限，例如连接数据库的权限等。

RESOURCE 角色：RESOURCE 角色一般包含了创建数据库对象的权限，像创建表、索引、视图、存储过程等。拥有这个角色的用户能够在自己的模式下创建和管理这些数据库对象。

SELECT ANY TABLE：该权限允许用户查询数据库里的任意表，由于部分能力需要查询系统表获取数

据，故需要该权限。

SELECT ANY VIEW：这个权限允许用户查询数据库中的任意视图。由于部分能力需要查询相关视图，故需要该权限。

CREATE MATERIALIZED VIEW：此权限允许用户创建物化视图。物化视图是一种预先计算并存储查询结果的特殊视图，它可以提高复杂查询的性能，BI 报表需要这个权限。

SELECT ANY MATERIALIZED VIEW：该权限允许用户查询数据库中的任意物化视图，BI 报表需要这个权限。

注意：

1. **当引入第三方的系统时，务必准备额外的单独服务器部署，不要部署在天擎的服务器上。**
2. **使用第三方数据库时，第三方数据库服务器的资源配置，建议按天擎数据库服务器上调 2 倍资源评估处理。**
3. **使用第三方数据库时，天擎数据库服务器中仅 Postgresql 数据存储在第三方数据库；Redis，etcd，S3 存储数据，并不会存储在第三方数据库服务器。**
4. **准入业务不支持第三方系统：达梦数据库。**

6) **配置终端大数据分析平台（可选）。**如果购买并部署了终端大数据分析平台，可选择开启并配置，输入“终端大数据分析平台地址”和端口“2381”，账号和密码可留空。然后点击[继续]则继续进行安装，点击[返回]按钮回到上一步操作界面。

7） **输入通信地址信息。**可自动获取当前机器 IP，多个 IP 时请选择正确的通信 IP 进行填充。

8） **安装检查。**进行安装检查，状态全部显示成功后可点击继续进行下一步安装；状态显示失败的服务，可点击查看失败详情，并点击重试进行重新检查。

9) **服务部署。**进行服务部署，状态全部显示成功后可点击继续进行下一步安装；状态显示失败的服务，可点击查看失败详情，并点击重试进行重新检查。该过程时间较久，请耐心等待。

10) **应用部署。**进行应用部署，全部执行成功后可点击继续进行安装；显示失败的可点击查看失败信息，并点击重试进行重新部署。 该过程时间较久，请耐心等待。

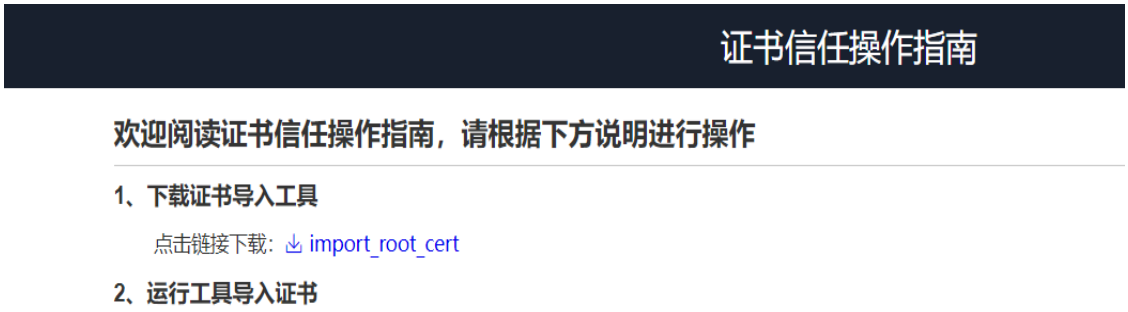
11) 安装完成。点击前往管理中心，可访问天擎管理中心。

3.3.4.2.3 首次登录

Linux 服务器部署后，访问管理中心地址为“https://管理中心地址:30082/”

Linux 等操作系统首次访问管理系统如果遇到如下提示需要先点击[查看帮助文档] 根据提示安装 CRT 证书后重新打开浏览器。

Windows 操作系统首次访问如果遇到如下提示需要先点击[查看帮助文档] 根据提示安装 CRT 证书后重新打开浏览器。



说明：

1、证书信任操作指南链接为：“https://管理中心地址:30082/cert-manual”。

2、访问管理中心，请使用 Chrome 84 以上版本，Edge 84 以上版本的浏览器或奇安信浏览器访问。

10.6.0.2000 及以下版本或安装过程中许可证导入未成功时，再次访问管理中心时会 弹出导入许可证弹窗，导入许可证即可继续操作，具体请参考第 4 章节许可证申请和 激活。

导入许可证后会进入登录界面，如下为系统初始用户名和密码。

初始用户名	初始密码	备注
system	Admin123@	创建新的管理员账号后，初始用户将不可用，请保存好新帐号的密码。

3.3.4.3升级部署

当有版本更新时，可以下载最新的安装包，然后执行如下命令进行更新：

```
Shell> nohup ./tianqing-client upgrade -f 2>&1 &
```

注意，如果解压完包后，没有发现 tianqing-client，请先 cd 到 plan_client/third_party/ linux_allinone/ 目录下。

```
Shell> cd plan_client/third_party/linux_allinone/
Shell> nohup ./tianqing-client upgrade -f 2>&1 &
```

查看升级进程，可以使用命令：

```
Shell> tail -f nohup.out
```

升级失败的回滚操作(如果环境使用的是达梦数据库，不支持使用此命令回滚)：

```
Shell> ./tianqing-client rollback
```

如果回滚时报了 Unable to parse output from tqv10redis.service 的错误，就添加 --install-path 参数，指定安装目录，默认安装目录是 /qaxdata

```
Shell> ./tianqing-client rollback --install-path /qaxdata
```

如果升级时，报了这个错： [ERROR TQV10Version]: couldn’t parse tianqing version “”， 那就很有可能升级前的版本是手扶起来的，需要执行如下命令提交版本号之后，再升级：

```
Shell> ./tianqing-client install phase darwin commintversion
```

可覆盖更新的范围参考同版本的《奇安信天擎终端安全管理系统 xxxx 版本发布说明书》。

使用安装包更新时会将当前安装目录的数据进行备份，需确保当前磁盘空间充足（按照大于管理中心安装目录的大小预留），以保证更新过程能够顺利进行。获取更新包的方式：

1、 在管理中心的系统管理>更新管理>主程序更新页的“管理中心主程序更新设置”可以设置或手动点击[检查更新]，然后根据提示找到下载的最新安装包安装更新；

2、 通过许可证 ID 从奇安信官网 https://www.qianxin.com/applyfortrial）获取，安装包然后拷贝至服务器安装更新。对于客户端主程序、病毒库等更新支持互联网模式的在线更新，也支持使用离线工具进行更新。

3.3.4.4卸载

1、需要 root 用户或者有 sudo 权限的用户

2、卸载脚本 uninstall.sh 在安装包解压目录（跟 install.sh 同级目录）

卸载命令：

```
Shell> sh uninstall.sh
```

卸载失败：会有相应失败原因提示，可根据失败提示自行查找资料解决，或提交 TAC 申请产线支持。

卸载成功：会有相应的“成功卸载天擎 V10”提示

3.4 终端大数据分析平台部署（可选）

3.4.1终端大数据分析平台部署

注意：该文档只提供单机部署管理中心时的终端大数据分析平台配置方法，其他情况下的配置方法见《奇安信天擎终端安全管理系统 V10.0R7-集群部署手册》

3.4.1.1安装前的工具检测

每次在部署前都需要邮件或【天擎 V10 集群部署环境检测工具】蓝信群中申请环境检查工具进行检测，环境检查工具验证通过才能进行部署，如果不进行检测直接部署，出现问题，产品线将不予支持处理。具体申请方式奇安信技术工程师可参考如下 KB24277。

3.4.1.2安装环境要求

系统类型	操作系统	资源配置（单机部署）	
Linux x86_64	CentOS 7.6 x86_64 CentOS 7.7 x86_64 CentOS 7.8 x86_64 CentOS 7.9 x86_64 银河麒麟高级服务器操作系统 V10SP1(Tercel) 银河麒麟高级服务器操作系统 V10SP2(Sword)	CPU：最低 32 核 内存容量：最低 64GB 硬盘(系统盘)：1TB SATA 硬盘 硬盘（数据盘）：2 块 * 4TB SATA 硬盘，格式 ext4 网卡：千兆单网卡	
Linux ARM64	银河麒麟高级服务器操作系统 V10 sp2(Sword)		
注意事项：			g)

1) 每次在部署前都需要邮件或【天擎 V10 集群部署环境检测工具】蓝信群中申请环境检查工具进行检测，环境检查工具验证通过才能进行部署，如果不进行检测直接部署，出现问题，产品线将不予支持处理。具体申请方式奇安信技术工程师可参考如下 KB24277。

2) 【天擎 V10 集群部署环境检测工具】产线选择 skylar，是否有高级版 EDR 选项选择时，若为 POC 测试可以选择 n，非 POC 测试需要选择 y。

3) 单机版大数据分析平台支持最大终端数量为 1000 个。

4) 分区：只分/根目录和/boot 即可，不要把/var 单独分区！

5) 使用 EDR 高级版，必须配置终端大数据分析平台。

a) 天擎管理中心服务器 4C8G 配置不支持 EDR（含 EDR 高级版、EDR 基础版）。

b) 天擎管理中心服务器 8C16G 配置可支持 100 点的 EDR 高级版。

c) 天擎管理中心服务器 16C32G 配置可支持 3000 点的 EDR 高级版。

d) 如有更多的终端需要采用集群部署。

e) 终端大数据分析平台需与部署的管理中心相匹配，部署文件是同一批次发布。不支持交叉部署。

f) 如果采用信创管理中心服务器，以上数据仅供参考。

注意：最新配置参考《奇安信天擎终端安全管理系统 V10.0R7R8-EDR 资源评估手册.xlsx》

3.4.1.3端口开放要求

终端大数据分析平台服务器默认开启了主机防火墙，应开放访问天擎管理中心机器端口，其余机器全部禁止，如需添加运维机器访问终端大数据分析平台服务器，需要再主机防火墙添加 ACL 放行规则。

源 IP	目的 IP	端口	协议	用途	服务名称
终端大数据分析平台	Windows 天擎管理中心	36781	grpc（tcp）	天擎管理中心代理服务	edge2-service

源 IP	目的 IP	端口	协议	用途	服务名称
终端大数据分析平台	Linux 天擎管理中心	30081	grpc（tcp）	天擎管理中心代理服务	edge2-service
天擎管理中心	终端大数据分析平台	2381	tcp	etcd 服务	etcd
天擎管理中心	终端大数据分析平台	25432	tcp	pg 服务	postgres
天擎管理中心	终端大数据分析平台	2181	tcp	zk 服务	zookeeper
天擎管理中心	终端大数据分析平台	9092	tcp	kafka 服务	kafka
天擎管理中心	终端大数据分析平台	9345	tcp	S3 服务	minio
天擎管理中心	终端大数据分析平台	9103	tcp	schema 服务	schema-registry
天擎管理中心	终端大数据分析平台	9200	tcp	es 服务	elasticsearch
天擎管理中心	终端大数据分析平台	30043	https	noah 服务	Noah
天擎管理中心	终端大数据分析平台	31191	http	sabre-server 服务	sabre-server
天擎管理中心	终端大数据分析平台	31181	http	noah-flink 服务	noah-flink
天擎管理中心	终端大数据分析平台	8088	http	星海服务	bm
天擎管理中心	终端大数据分析平台	32181	http	sabre-server 服务	sabre-server
天擎管理中心	终端大数据分析平台	29010	tcp	clickhouse 服务	clickhouse-server

源 IP	目的 IP	端口	协议	用途	服务名称
天擎管理中心	终端大数据分析平台	29011	tcp	clickhouse 服务	clickhouse-server

3.4.1.4安装包说明

终端大数据分析平台（EDR）的安装文件名称为：QI-ANXINTianqing-EDR-[系统平台 Win/Linux/ARM64] _[版本信息] _[文件 MD5]，示例：QI-ANXINTianqing-EDR-Linux_10.3.0.3000_48354EEEEA940B30CFF4C99959C264AB.tar，其中：

1）10.3.0.3000 是版本号。

2）Linux 是系统平台，表示当前安装包是 Linux 服务器版本。

3）48354EEEEA940B30CFF4C99959C264AB 是安装文件的 MD5，可用 MD5 工具验证是否正确。

4）天擎管理中心和大数据分析平台版本对应关系

架构	天擎版本	大数据版本	大数据包名
X86	10.3.0.3000	10.3.0.3000	QI-ANXINTianqing-EDR-Linux_10.3.0.3000_1de0b98bbb12e641453f631a8f9f9445.tar
X86	10.3.0.5000	10.3.0.5000	QI-ANXINTianqing-EDR-Linux_10.3.0.5000_f9bb56cf5e69803ee4e296e0cecccf49.tar
X86	10.6.0.1000	10.6.0.1000	QI-ANXINTianqing-EDR-Linux_10.6.0.1000_0171289923b42450903fb2aae2374416.tar
X86	10.7.0.1000	10.7.0.1000	QI-ANXINTianqing-EDR-Linux_10.7.0.1000_f8b1d74820c481b5853e426b85b7e2eb.tar
ARM64	10.7.0.1000	10.7.0.1000	QI-ANXINTianqing-EDR-ARM64_10.7.0.1000_87e140f18b1e848e855fcfddd230034e.tar
X86	10.7.0.1000 以上 10.8.0.1000 以下	10.7.0.1600	QI-ANXINTianqing-EDR-Linux_10.7.0.1600_f3cfa8c256805fd0eb41b4e98afc6542.ta
ARM64	10.7.0.1000 以上 10.8.0.1000 以下	10.7.0.1600	QI-ANXINTianqing-EDR-ARM64_10.7.0.1600_c379c7b27f3fce49e34185562a48dc85.tar

说明：

1. 天擎 Windows 10.3.0.3000 以下单机版版本不支持 EDR 功能

2. 天擎 Linux 10.6.0.1000 以下单机版版本不支持 EDR 功能

3. 天擎信创 10.7.0.1000 以下单机版版本不支持 EDR 功能

4. 天擎管理中心和大数据分析平台未做跨版本兼容性支持，需选择对应的版本进行安装，天擎管理中心版本未在列表中的，请选择所在区间的低版本大数据分析平台进行部署，如：天擎管理中心版本为 10.5.0.1000，选择大数据版本 10.3.0.5000 即可

3.4.1.5上传安装包

安装终端大数据分析平台（EDR）需准备安装包，提前上传至服务器并解压安装包，请将安装包放置到有存储空间的目录下，可使用命令查看目录剩余存储空间，如：df -h /var。

```
[root@edr plan_client]# df -h /root/
Filesystem              Size  Used Avail Use% Mounted on
/dev/mapper/centos-root  589G   59G  531G  10% /
[root@edr plan_client]# df -h /var
Filesystem              Size  Used Avail Use% Mounted on
/dev/mapper/centos-root  589G   59G  531G  10% /
[root@edr plan_client]#
```

执行解压命令：

tar xvf QI-ANXINTianqing-EDR-Linux_10.3.0.3000_48354EEEEA940B30CFF4C99959C264AB.tar

```
total 5984124
-rw-r--r--. 1 root root 6127741993 May 27 11:05 QI-ANXINTianqing-EDR-linux_10.3.0.3000_4e372c67a7bf76635890383e9515edbc.tar
[root@localhost ~]# tar xvf QI-ANXINTianqing-EDR-linux_10.3.0.3000_4e372c67a7bf76635890383e9515edbc.tar
plan_client/
plan_client/plan.test.yaml
plan_client/third_party/
plan_client/third_party/ansible-playbooks/
plan_client/third_party/ansible-playbooks/deploy/
plan_client/third_party/ansible-playbooks/deploy/playbooks/
plan_client/third_party/ansible-playbooks/deploy/playbooks/install_k8s.yaml
plan_client/third_party/ansible-playbooks/deploy/playbooks/filter_plugins/
plan_client/third_party/ansible-playbooks/deploy/playbooks/filter_plugins/services.pyc
plan_client/third_party/ansible-playbooks/deploy/playbooks/filter_plugins/address.py
plan_client/third_party/ansible-playbooks/deploy/playbooks/filter_plugins/address.pyc
plan_client/third_party/ansible-playbooks/deploy/playbooks/filter_plugins/__pycache__/
plan_client/third_party/ansible-playbooks/deploy/playbooks/filter_plugins/__pycache__/address.cpython-36.pyc
plan_client/third_party/ansible-playbooks/deploy/playbooks/filter_plugins/__pycache__/services.cpython-36.pyc
plan_client/third_party/ansible-playbooks/deploy/playbooks/filter_plugins/services.py
plan_client/third_party/ansible-playbooks/deploy/playbooks/ansible.cfg
plan_client/third_party/ansible-playbooks/deploy/playbooks/deploy-ceph-mons.yml
plan_client/third_party/ansible-playbooks/deploy/playbooks/install_sabre.yaml
plan_client/third_party/ansible-playbooks/deploy/playbooks/uninstall_bi.yaml
plan_client/third_party/ansible-playbooks/deploy/playbooks/install_kernel.yaml
plan_client/third_party/ansible-playbooks/deploy/playbooks/install_logger.yaml
plan_client/third_party/ansible-playbooks/deploy/playbooks/uninstall_noah.yaml
plan_client/third_party/ansible-playbooks/deploy/playbooks/templates/
plan_client/third_party/ansible-playbooks/deploy/playbooks/templates/exporter/
plan_client/third_party/ansible-playbooks/deploy/playbooks/templates/exporter/node_exporter_sd.json.j2
plan_client/third_party/ansible-playbooks/deploy/playbooks/templates/exporter/exporter_sd.yaml.j2
plan_client/third_party/ansible-playbooks/deploy/playbooks/templates/exporter/exporter_sd.json.j2
plan_client/third_party/ansible-playbooks/deploy/playbooks/templates/secrets.j2
plan_client/third_party/ansible-playbooks/deploy/playbooks/uninstall_schema_registry.yaml
plan_client/third_party/ansible-playbooks/deploy/playbooks/uninstall_logger.yaml
plan_client/third_party/ansible-playbooks/deploy/playbooks/install_search.yaml
plan_client/third_party/ansible-playbooks/deploy/playbooks/uninstall_sabre.yaml
plan_client/third_party/ansible-playbooks/deploy/playbooks/deploy-ceph-mds.yml
plan_client/third_party/ansible-playbooks/deploy/playbooks/install_election.yaml
plan_client/third_party/ansible-playbooks/deploy/playbooks/install_init_system.yaml
plan_client/third_party/ansible-playbooks/deploy/playbooks/install_grafana.yaml
plan_client/third_party/ansible-playbooks/deploy/playbooks/gather-facts.yml
plan_client/third_party/ansible-playbooks/deploy/playbooks/install_cdn.yaml
plan_client/third_party/ansible-playbooks/deploy/playbooks/install_db.yaml
plan_client/third_party/ansible-playbooks/deploy/playbooks/install_node_exporter.yaml
plan_client/third_party/ansible-playbooks/deploy/playbooks/install_wormhole.yaml
plan_client/third_party/ansible-playbooks/deploy/playbooks/inventory.example.yaml
plan_client/third_party/ansible-playbooks/deploy/playbooks/install_bm.yaml
plan_client/third_party/ansible-playbooks/deploy/playbooks/install_preflight.yaml
plan_client/third_party/ansible-playbooks/deploy/playbooks/install_repeater.yaml
plan_client/third_party/ansible-playbooks/deploy/playbooks/files/
plan_client/third_party/ansible-playbooks/deploy/playbooks/files/x86_64/
plan_client/third_party/ansible-playbooks/deploy/playbooks/files/x86_64/init-edr/
plan_client/third_party/ansible-playbooks/deploy/playbooks/files/x86_64/init-edr/migration_noah
plan_client/third_party/ansible-playbooks/deploy/playbooks/files/x86_64/init-edr/etcdctl
plan_client/third_party/ansible-playbooks/deploy/playbooks/files/x86_64/oasis/
plan_client/third_party/ansible-playbooks/deploy/playbooks/files/x86_64/oasis/oasis-linux-amd64-v1.1.11.tar.gz
```

3.4.1.6 安装操作步骤

注意事项：

操作系统 IP 地址配置需要填写上网关地址，否则会因为缺失默认路由数据导致安装失败。

操作系统 IP 地址配置如果是 192.168.x.x，此 IP 段与默认的 docker 网段冲突导致安装失败，请按下面步骤 6 进行配置修改。

1）检查本机主机名

服务器主机名如果为 localhost.localdomain，则需要修改主机名。

执行命令：hostnamectl set-hostname

输入自定义主机名，注意主机名不能包含**中划线** -

例如：hostnamectl set-hostname edr.qianxin.com

2）增加主机名解析

执行命令：vi /etc/hosts

输入服务器 iP 地址和服务器主机名

例如：10.41.5.232 edr.qianxin.com

参考图如下：

```
[root@edr plan_client]# vi /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
10.41.5.232 edr.qianxin.com
~
```

3）修改 resolv.conf 文件

执行命令：vi /etc/resolv.conf

修改/etc/resolv.conf，删除 search 开头的字符串

例如：删除“search qianxin.com”

参考图如下：

```
[root@localhost ~]# hostnamectl set-hostname edr.qianxin.com
[root@localhost ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search qianxin.com
```

4）配置 selinux

执行命令：getenforce

查看 selinux 状态是否为 disabled（disabled 则已禁止），如果为 disabled，可以跳过修改。如果不是 disabled，需要修改/etc/selinux/config

执行命令：vi /etc/selinux/config

修改 SELINUX=disabled

修改后需要重启服务器，配置才可生效，重启服务器后，可使用 getenforce 命令查看

参考图如下：

```
[root@localhost ~]# vi /etc/selinux/config

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

5）修改 plan.test.yaml

文件路径：plan_client/plan.test.yaml，修改文件中的以下选项

##连接本机得用户名和密码，需要有 sudo 权限得用户或者 root 用户

```
##权限验证，当前用户登录后，输入 sudo su，无需输入密码则正确
user: "root"
passwd: "1234567"
##机器网卡名称，可以通过 ip addr 命令查看
network_interface: "eth0"
##需要安装得服务器 IP 地址
hosts:
  #计算型
  service_host_list:
    - "10.41.5.232"
  #数据库型
  database_host_list:
    - "10.41.5.232"
  #大数据型
  bigdata_host_list:
- "10.41.5.232"
```

6) 检查服务器 IP 是否为“192.168.x.x”开头，若不是的话请跳过该步骤继续向下执行，如果服务器 IP 是以“192.168.x.x”开头，请修改配置文件为“193.168.x.x”，命令：vi plan_client/third_party/ansible-playbooks/deploy/playbooks/roles/docker/templates/daemon.json.j2

```
[root@edr ~]# vi plan_client/third_party/ansible-playbooks/deploy/playbooks/roles/docker/templates/daemon.json.j2
{
  "bip": "193.168.0.1/20",
  "exec-opts": ["native.cgroupdriver=cgroupfs"],
  "log-driver": "json-file",
    "log-opts": {
        "max-size": "100m",
        "max-file": "3"
    },
  "storage-driver": "overlay2",
  "storage-opts": [
    "overlay2.override_kernel_check=true"
  ]
}
```

7）挂载数据盘

准备两块硬盘作为数据盘，分别挂载到/qaxdata/data01 和/qaxdata/data02。

查看未挂载盘 lsblk

```
[root@whinstxh01v zhengchaoping]# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0  600G  0 disk
└─sda1   8:1    0  600G  0 part /
sdb      8:16   0  600G  0 disk
sdc      8:32   0  600G  0 disk
```

mkfs.ext4 /dev/sdb ,挂载分区

a） mkdir -p /qaxdata/data01

b） mount /dev/sdb /qaxdata/data01/

c） echo "/dev/sdb /qaxdata/data01 ext4 defaults 0 0" >> /etc/fstab

```
[root@whinstxh01v zhengchaoping]# mkfs.ext4 /dev/sdb
mke2fs 1.42.9 (28-Dec-2013)
/dev/sdb is entire device, not just one partition!
Proceed anyway? (y,n) y
Discarding device blocks: done
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
39321600 inodes, 157286400 blocks
7864320 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2304770048
4800 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624, 11239424, 20480000, 23887872, 71663616, 78675968,
        102400000

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

[root@whinstxh01v zhengchaoping]# a)mkdir -p /qaxdata/data01
bash: syntax error near unexpected token `)'
[root@whinstxh01v zhengchaoping]# mkdir -p /qaxdata/data01
[root@whinstxh01v zhengchaoping]# mount /dev/sdb /qaxdata/data01/
[root@whinstxh01v zhengchaoping]# echo "/dev/sdb /qaxdata/data01 ext4 defaults 0 0" >> /etc/fstab
[root@whinstxh01v zhengchaoping]# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0  600G  0 disk
└─sda1   8:1    0  600G  0 part /
sdb      8:16   0  600G  0 disk /qaxdata/data01
sdc      8:32   0  600G  0 disk
```

同样的方式挂载其他数据盘。应用部署机上修改对应 bm.conf.j2

vim plan_client/third_party/ansible-playbooks/deploy/playbooks/roles/xh_cluster/templates/bm.conf.j2

```
[root@whinstk8s01v zhengchaoping]# vim /opt/cli/tq_paas/skylar/skylar_linuxserver_client/plan_client/third_party/ansible-playbooks/deploy/playbooks/roles/xh_cluster/templates/bm.conf.j2

[bm]
mode = {{xh_install_mode}}
security_level = 0
install_path = {{install_root_path}}
database_type = postgresql
disk_num_min = 2
cluster_name = {{ bm_cluster_name }}
admin_user = admin
admin_password = U2FsdGVkX1/Xzea0Ca4eliXOCMGxSFgz+Z31+/p/PGQ=
product_line = {{ bm_product_line_name }}
mem_size = {{xh_host_mem}}
node_number = 003
deploy_from_excel = true
template = {{ xh_install_template }}
data_volume_name_equal_width = true
cpu_structure= x86_64
check_root_partition = false
auto_disk_format = false
custom_formatted_disk = /qaxdata/data01,/qaxdata/data02
iptables_or_firewalld = firewalld
;security_virtual_ip = 127.0.0.1
```

当有 n 块数据盘时，custom_formatted_disk= /qaxdata/data01, /qaxdata/data02,…,/qaxdata/data0n

8）执行安装脚本

执行命令：bash install.sh，填写 Windows 或 Linux 单机版管理中心 IPV4 地址，如：10.41.5.231。

```
[root@edr plan_client]# ./install.sh
Please enter the Windows IPv4 address:10.41.5.231
```

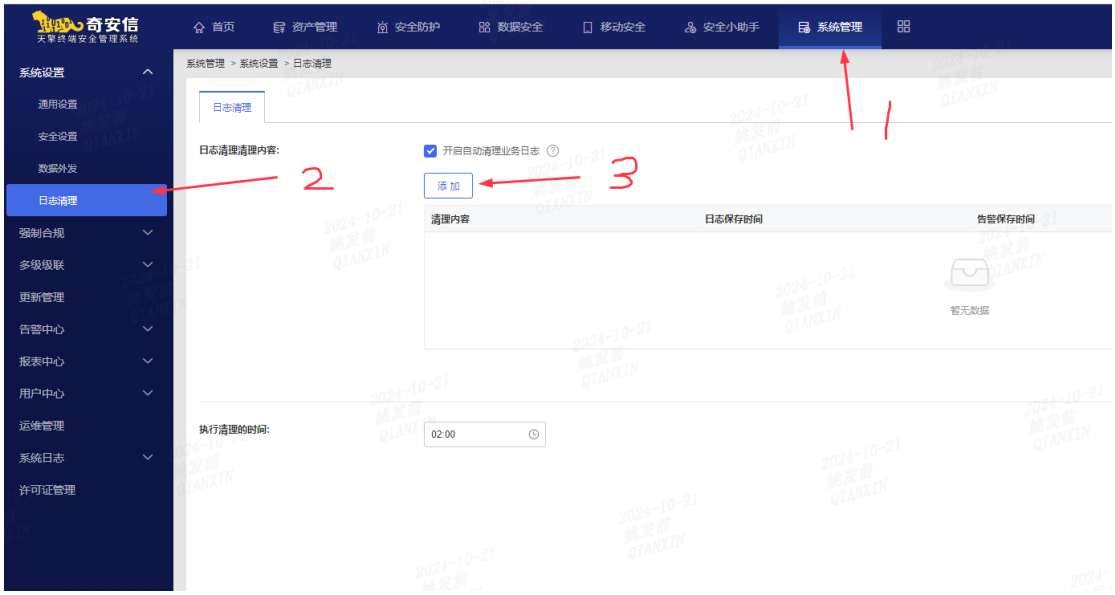
数据分析平台部署成功参考图如下：

```
Complete!
/root/plan_client/ark-ansible
 pass层开始安装
 安装需要一段时间，需要查看实施日志可以在打开一个终端查看install.log
 pass层安装完成
 安装完成
[root@test plan_client]#
```

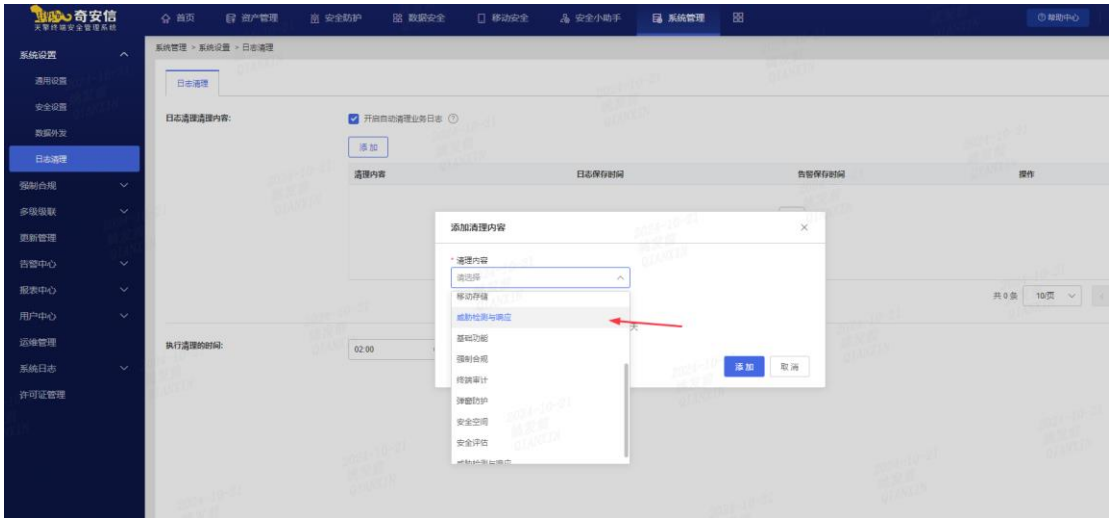
注意：新增或者更新 EDR 授权后，需要手动重启 EDR 相关服务，请参考 KB119952 。

3.4.1.7开启日志清理（必须开启）

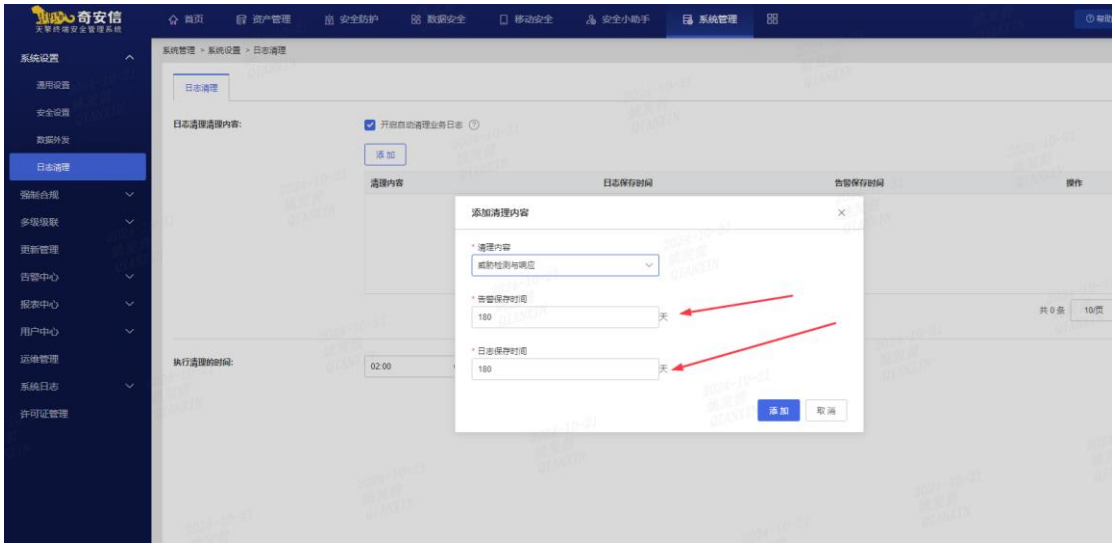
参考下图步骤开启 EDR 日志清理，防止不开启清理导致时间长了 EDR 日志占满磁盘空间导致天擎故障。



选择业务



修改保存天数这里一定要按照资源评估的天数走 只能小于等于资源评估的天数。比如当初评估的是保存 180 天日志的磁盘空间大小 只能填小于或者等于 180 天。



点击添加即可 执行清理时间可以根据客户需求走，建议最好是后半夜。

3.4.1.8卸载

请提 TAC 工单支持

3.4.2管理中心联动配置

注意：联动配置完成后，需要更新/手动导入一次 IOA、IOC 库才可以正常工作。

3.4.2.1全新部署配置方法

Windows 服务器单机部署配置：

- 登录大数据分析平台后台，检查天擎管理中心 IP 是否在防火墙白名单中，命令行： iptables -nvL -t mangle

```
[root@edr ~]# iptables -nvL -t mangle
Chain PREROUTING (policy ACCEPT 6075 packets, 953K bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  ens160 *       10.58.192.14         0.0.0.0/0
  182 36507 ACCEPT     all  --  ens160 *       10.58.192.22         0.0.0.0/0
    0     0 ACCEPT     all  --  ens160 *       172.17.0.0/16        0.0.0.0/0
    0     0 ACCEPT     all  --  ens160 *       172.16.0.0/16        0.0.0.0/0
    0     0 ACCEPT     all  --  ens160 *       127.0.0.1            0.0.0.0/0
    0     0 DROP       tcp  --  ens160 *       0.0.0.0/0            0.0.0.0/0           multiport dports 8443,2381,25432,5432,31181,2181,8088,9092,9345,9103,9200,31191,32181

Chain INPUT (policy ACCEPT 6149 packets, 907K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 98 packets, 81357 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 6287 packets, 951K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 6385 packets, 1032K bytes)
 pkts bytes target     prot opt in     out     source               destination
4727K  246M TCPMSS     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x06/0x02 TCPMSS clamp to PMTU

Chain KUBE-KUBELET-CANARY (0 references)
 pkts bytes target     prot opt in     out     source               destination

Chain KUBE-PROXY-CANARY (0 references)
 pkts bytes target     prot opt in     out     source               destination
[root@edr ~]#
```

若天擎管理中心 IP 已在白名单中，请继续执行下一步操作，若不在白名单中请执行以下操作：

1.执行命令进行添加，命令：iptables -t mangle -I PREROUTING -i "eth0" -s 10.41.5.231 -j ACCEPT;

注意：命令中的“eth0”和管理中心 IP“10.41.5.231”按实际环境进行调整

```
~
[root@edr ~]# iptables -t mangle -I PREROUTING -i "eth0" -s  10.41.5.231  -j ACCEPT;
[root@edr ~]#
```

2.将命令行写入文件“/qaxdata/s/services/tmp/iptables.sh”，命令：vi /qaxdata/s/services/tmp/iptables.sh

```
~
[root@edr ~]# vi /qaxdata/s/services/tmp/iptables.sh
#!/bin/bash

iptables -t mangle -L -n |grep "DROP" |grep 8443 > /dev/null 2>&1

if [ "$?" == "0" ]; then
        echo "iptables 已添加"
        exit
fi


DROP_PORT_LIST="8443,2381,25432,5432,31181,2181,8088,9092,9345,9103,9200,31191,32181"


##accept ip all
iptables -t mangle -I PREROUTING -i "eth0" -s  127.0.0.1  -j ACCEPT;
iptables -t mangle -I PREROUTING -i "eth0" -s  172.16.0.0/16  -j ACCEPT;
iptables -t mangle -I PREROUTING -i "eth0" -s  172.17.0.0/16  -j ACCEPT;
iptables -t mangle -I PREROUTING -i "eth0" -s  10.58.192.22  -j ACCEPT;
iptables -t mangle -I PREROUTING -i "eth0" -s  10.58.192.14  -j ACCEPT;
iptables -t mangle -I PREROUTING -i "eth0" -s  10.41.5.231  -j ACCEPT;


##drop port all
iptables -t mangle -A PREROUTING -i "ens160" -m multiport -p tcp --dport $DROP_PORT_LIST -j DROP


crontab -l |grep iptables
if [ "$?" != "0" ]; then
        (crontab -l;echo "*/1 * * * *  sudo  bash "/qaxdata/s/services/tmp/iptables.sh";   >/dev/null 2>&1") | crontab
fi
~
```

- 部署天擎管理中心，具体配置路径可参见 3.3.2.3 章节中配置终端大数据分析平台部分， 输入“终端大数据分析平台地址”和端口“2381”，账号和密码可留空。
- 等待天擎管理中心安装成功后，修改天擎管理中心操作系统的 hosts 文件

修改 Windows 管理中心 hosts 文件，确保 Windows 服务器可以解析 Linux 服务器主机名

修改前先对 hosts 文件进行备份，路径：

C:\Windows\System32\drivers\etc\hosts

Hosts 文件中添加 Linux 服务器 IP 地址和服务器主机名，例如：

10.41.5.232 edr.qianxin.com

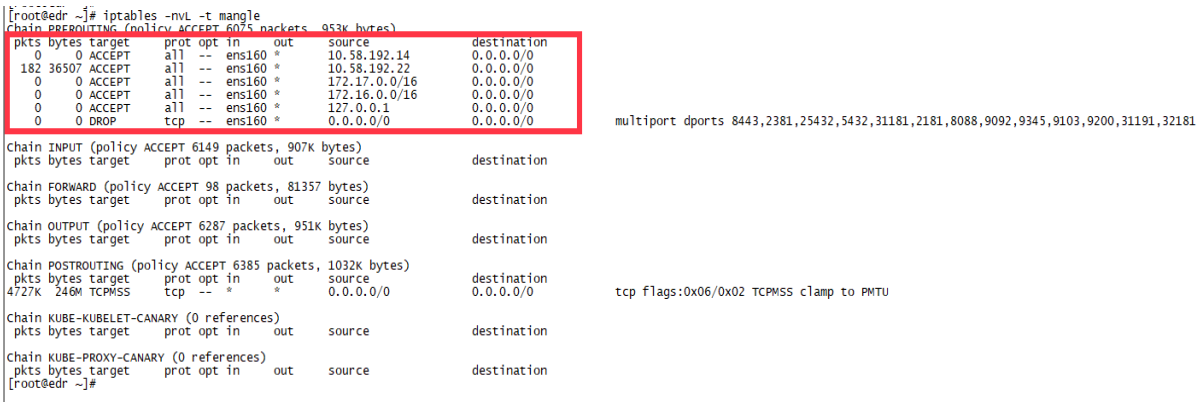
注：添加完成后需进行测试，在 Windows 服务器上运行 cmd 命令

ping Linux 服务器主机名

例如：ping edr.qianxin.com

Linux 服务器单机部署配置：

- 登录大数据分析平台后台，检查天擎管理中心 IP 是否在防火墙白名单中，命令行： iptables -nvL -t mangle



若天擎管理中心 IP 已在白名单中，请继续执行下一步操作，若不在白名单中请执行以下操作：

1. 执行命令进行添加，命令：iptables -t mangle -I PREROUTING -i "eth0" -s 10.41.5.231 -j ACCEPT;

注意：命令中的“eth0”和管理中心 IP“10.41.5.231”按实际环境进行调整

```
~
[root@edr ~]# iptables -t mangle -I PREROUTING -i "eth0" -s  10.41.5.231  -j ACCEPT;
[root@edr ~]#
```

2.将命令行写入文件“/qaxdata/s/services/tmp/iptables.sh”，命令：vi /qaxdata/s/services/tmp/iptables.sh

```
~
[root@edr ~]# vi /qaxdata/s/services/tmp/iptables.sh
#!/bin/bash

iptables -t mangle -L -n |grep "DROP" |grep 8443 > /dev/null 2>&1

if [ "$?" == "0" ]; then
        echo "iptables 已添加"
        exit
fi


DROP_PORT_LIST="8443,2381,25432,5432,31181,2181,8088,9092,9345,9103,9200,31191,32181"


##accept ip all
iptables -t mangle -I PREROUTING -i "eth0" -s  127.0.0.1  -j ACCEPT;
iptables -t mangle -I PREROUTING -i "eth0" -s  172.16.0.0/16  -j ACCEPT;
iptables -t mangle -I PREROUTING -i "eth0" -s  172.17.0.0/16  -j ACCEPT;
iptables -t mangle -I PREROUTING -i "eth0" -s  10.58.192.22  -j ACCEPT;
iptables -t mangle -I PREROUTING -i "eth0" -s  10.58.192.14  -j ACCEPT;
iptables -t mangle -I PREROUTING -i "eth0" -s  10.41.5.231  -j ACCEPT;


##drop port all
iptables -t mangle -A PREROUTING -i "ens160" -m multiport -p tcp --dport $DROP_PORT_LIST -j DROP


crontab -l |grep iptables
if [ "$?" != "0" ]; then
        (crontab -l;echo "*/1 * * * *  sudo  bash "/qaxdata/s/services/tmp/iptables.sh";   >/dev/null 2>&1") | crontab
fi
~
```

- 部署天擎管理中心，具体配置路径可参见 3.3.4.2.2 章节中配置终端大数据分析平台部分， 输入“终端大数据分析平台地址”和端口“2381”，账号和密码可留空。
  - 等待天擎管理中心安装成功后，若大数据平台域名无法被内网 DNS 解析，则需要进行本地 hosts 解析，修改文件“/qaxdata/TianqingEndpointSecurity/conf/template.yaml”，向节点“extends:”下添加子节点“k8s_hosts”并填写大数据平台域名和 IP 地址，修改完成后，切换到安装包所在目录，执行命令：“/qaxdata/TianqingEndpointSecurity/utils/darwin/darwin-client install --data.source=local --execute.type=docker-compose --up_for_component=true --assign.tag --template.file=/qaxdata/TianqingEndpointSecurity/conf/template.yaml --actions=deploy --full.deploy --services_filter=heka-service,edr-service-league,edr-flow-league,argo-service”，等待命令执行完成即可。域名数据配置如下：

```
extends:
  k8s_hosts:
    edr.qianxin.com: 10.41.5.232
  mount:
    darwin-cdn: src=/qaxdata/TianqingEndpointSecurity/data/cdn/files,dest=/home/s/darwin-cdn/data/files,is_dir=true,host_path=true
    trantor-league-v2: src=/qaxdata/TianqingEndpointSecurity/data/trantor-league-v2/data,dest=/home/s/data,is_dir=true,host_path=true
  mod_depends:
    integrated_bi: integrated_noah
  k8s_service:
    darwin-cdn: nodeport,Cluster:https,TCP,32185,32185;http,TCP,32186,32186
    edge2-service: nodeport,local:tcp,TCP,6781,30080;grpc-web,TCP,26781,30081
    gossip-hub: nodeport,Cluster:tcp,TCP,9120
    trantor-fe: nodeport,Cluster:https,TCP,8443,30082
    remote-assistance-repeater: nodeport,Cluster:https,TCP,5901,30090;http,TCP,5500,30091
```

3.4.2.2配置工具配置方法

Windows 服务器单机部署配置：

- 登录大数据分析平台后台，检查天擎管理中心 IP 是否在防火墙白名单中，命令行： iptables -nvL -t mangle

```
[root@edr ~]# iptables -nvL -t mangle
Chain PREROUTING (policy ACCEPT 6075 packets, 953K bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  ens160 *       10.58.192.14         0.0.0.0/0
  182 36507 ACCEPT     all  --  ens160 *       10.58.192.22         0.0.0.0/0
    0     0 ACCEPT     all  --  ens160 *       172.17.0.0/16        0.0.0.0/0
    0     0 ACCEPT     all  --  ens160 *       172.16.0.0/16        0.0.0.0/0
    0     0 ACCEPT     all  --  ens160 *       127.0.0.1            0.0.0.0/0
    0     0 DROP       tcp  --  ens160 *       0.0.0.0/0            0.0.0.0/0           multiport dports 8443,2381,25432,5432,31181,2181,8088,9092,9345,9103,9200,31191,32181

Chain INPUT (policy ACCEPT 6149 packets, 907K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 98 packets, 81357 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 6287 packets, 951K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 6385 packets, 1032K bytes)
 pkts bytes target     prot opt in     out     source               destination
4727K  246M TCPMSS     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x06/0x02 TCPMSS clamp to PMTU

Chain KUBE-KUBELET-CANARY (0 references)
 pkts bytes target     prot opt in     out     source               destination

Chain KUBE-PROXY-CANARY (0 references)
 pkts bytes target     prot opt in     out     source               destination
[root@edr ~]#
```

若天擎管理中心 IP 已在白名单中，请继续执行下一步操作，若不在白名单中请执行以下操作：

1. 执行命令进行添加，命令：iptables -t mangle -I PREROUTING -i "eth0" -s 10.41.5.231 -j ACCEPT;

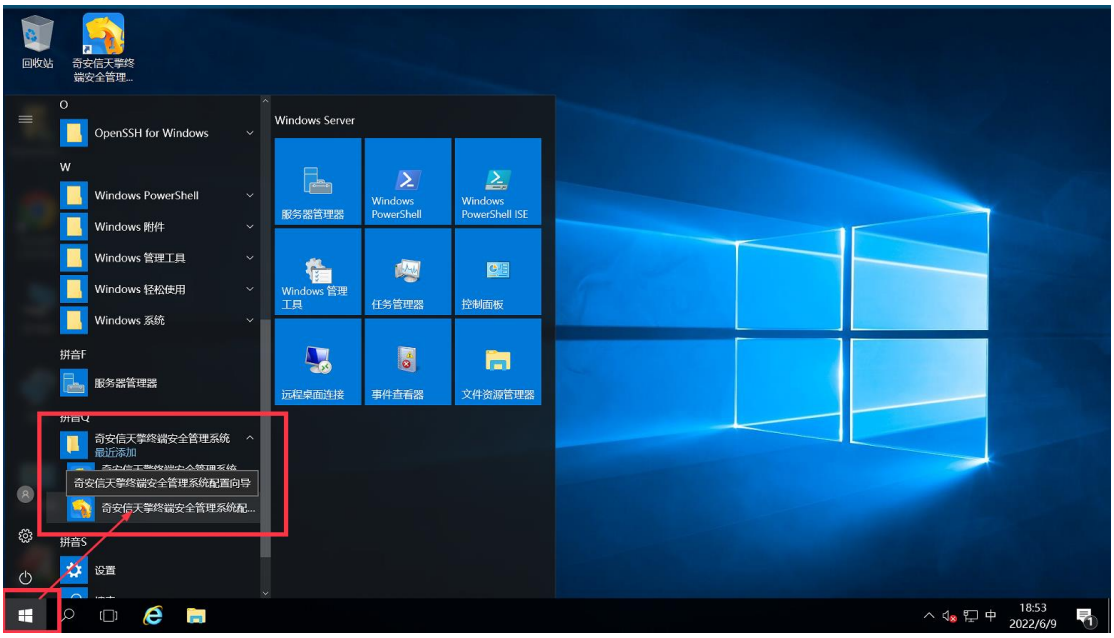
注意：命令中的“eth0”和管理中心 IP“10.41.5.231”按实际环境进行调整

```
~
[root@edr ~]# iptables -t mangle -I PREROUTING -i "eth0" -s  10.41.5.231  -j ACCEPT;
[root@edr ~]#
```

2. 将命令行写入文件“/qaxdata/s/services/tmp/iptables.sh”，命令：vi /qaxdata/s/services/tmp/iptables.sh

```
~
[root@edr ~]# vi /qaxdata/s/services/tmp/iptables.sh
#!/bin/bash

iptables -t mangle -L -n |grep "DROP" |grep 8443 > /dev/null 2>&1

if [ "$?" == "0" ]; then
        echo "iptables 已添加"
        exit
fi


DROP_PORT_LIST="8443,2381,25432,5432,31181,2181,8088,9092,9345,9103,9200,31191,32181"


##accept ip all
iptables -t mangle -I PREROUTING -i "eth0" -s  127.0.0.1  -j ACCEPT;
iptables -t mangle -I PREROUTING -i "eth0" -s  172.16.0.0/16  -j ACCEPT;
iptables -t mangle -I PREROUTING -i "eth0" -s  172.17.0.0/16  -j ACCEPT;
iptables -t mangle -I PREROUTING -i "eth0" -s  10.58.192.22  -j ACCEPT;
iptables -t mangle -I PREROUTING -i "eth0" -s  10.58.192.14  -j ACCEPT;
iptables -t mangle -I PREROUTING -i "eth0" -s  10.41.5.231  -j ACCEPT;


##drop port all
iptables -t mangle -A PREROUTING -i "ens160" -m multiport -p tcp --dport $DROP_PORT_LIST -j DROP


crontab -l |grep iptables
if [ "$?" != "0" ]; then
        (crontab -l;echo "*/1 * * * *  sudo  bash "/qaxdata/s/services/tmp/iptables.sh";   >/dev/null 2>&1") | crontab
fi
~
```

- 打开奇安信天擎安全管理系统配置工具。



- 启用终端大数据分析平台配置，输入“终端大数据分析平台”IP 地址和端口“2381”，账号和密码可留空。

➢ 修改天擎管理中心操作系统的 hosts 文件

修改 Windows 管理中心 hosts 文件，确保 Windows 服务器可以解析 Linux 服务器主机名

修改前先对 hosts 文件进行备份，路径：C:\Windows\System32\drivers\etc\hosts

Hosts 文件中添加 Linux 服务器 IP 地址和服务器主机名，例如：10.41.5.232 edr.qianxin.com

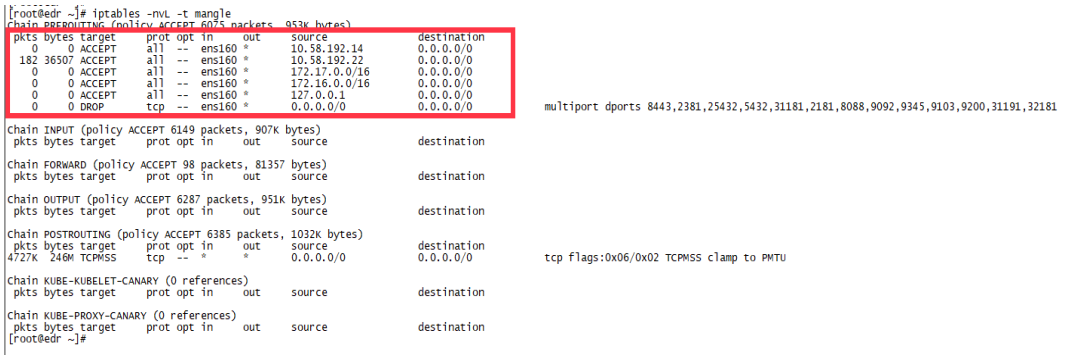
注：添加完成后需进行测试，在 Windows 服务器上运行 cmd 命令

ping Linux 服务器主机名

例如：ping edr.qianxin.com

Linux 服务器单机部署配置：

- 登录大数据分析平台后台，检查天擎管理中心 IP 是否在防火墙白名单中，命令行： iptables -nvL -t mangle



若天擎管理中心 IP 已在白名单中，请继续执行下一步操作，若不在白名单中请执行以下操作：

1. 执行命令进行添加，命令：iptables -t mangle -I PREROUTING -i "eth0" -s 10.41.5.231 -j ACCEPT;

注意：命令中的“eth0”和管理中心 IP“10.41.5.231”按实际环境进行调整

```
[root@edr ~]# iptables -t mangle -I PREROUTING -i "eth0" -s  10.41.5.231  -j ACCEPT;
[root@edr ~]#
```

2. 将命令行写入文件“/qaxdata/s/services/tmp/iptables.sh”，命令：vi /qaxdata/s/services/tmp/iptables.sh

```
[root@edr ~]# vi /qaxdata/s/services/tmp/iptables.sh
#!/bin/bash

iptables -t mangle -L -n |grep "DROP" |grep 8443 > /dev/null 2>&1

if [ "$?" == "0" ]; then
        echo "iptables 已添加"
        exit
fi


DROP_PORT_LIST="8443,2381,25432,5432,31181,2181,8088,9092,9345,9103,9200,31191,32181"


##accept ip all
iptables -t mangle -I PREROUTING -i "eth0" -s  127.0.0.1  -j ACCEPT;
iptables -t mangle -I PREROUTING -i "eth0" -s  172.16.0.0/16  -j ACCEPT;
iptables -t mangle -I PREROUTING -i "eth0" -s  172.17.0.0/16  -j ACCEPT;
iptables -t mangle -I PREROUTING -i "eth0" -s  10.58.192.22  -j ACCEPT;
iptables -t mangle -I PREROUTING -i "eth0" -s  10.58.192.14  -j ACCEPT;
iptables -t mangle -I PREROUTING -i "eth0" -s  10.41.5.231  -j ACCEPT;


##drop port all
iptables -t mangle -A PREROUTING -i "ens160" -m multiport -p tcp --dport $DROP_PORT_LIST -j DROP


crontab -l |grep iptables
if [ "$?" != "0" ]; then
        (crontab -l;echo "*/1 * * * *  sudo  bash "/qaxdata/s/services/tmp/iptables.sh";   >/dev/null 2>&1") | crontab
fi
~
```

- 通过管理中心配置工具，配置大数据平台，执行命令：“/qaxdata/TianqingEndpointSecurity/utils/tianqing-client confmanagetool edrswitcher --etcdaddr 10.41.5.232:2381”，如果终端大数据平台的 etcd 开启认证需要增加--etcduser 和--etcdpassword 参数,默认账号密码可通过命令行 /qaxdata/TianqingEndpointSecurity/utils/tianqing-client confmanagetool edrswitcher --help 查询。其中“10.41.5.232”为大数据平台的 IP 地址，如下：

```
[root@qax ~]# /qaxdata/TianqingEndpointSecurity/utils/tianqing-client confmanagetool edrswitcher --etcdaddr 10.41.5.232:2381
/usr/bin/edr-switcher-x86 is not exist, err: exit status 1
2023-02-17 19:18:52.814457 [INFO] <main.go:52> msg:
edr-switcher is a tool for switch infra services from Windows to Linux.

Usage:
        edr-switcher.exe -addr="***.***.***.***" -port="****" -user="****" -password="******"

Use "edr-switcher.exe --help" for help.

2023-02-17 19:18:52.814561 [INFO] <main.go:53> msg:edr-switcher version: 2022.05.11
2023-02-17 19:18:52.814575 [INFO] <main.go:108> msg:the parameters entered, addr: 10.41.5.232, port: 2381, user: root, checkMode: false, skipNoah: false
2023-02-17 19:18:52.814590 [INFO] <main.go:124> msg:enter switch mode
2023-02-17 19:18:52.815011 [INFO] <net.go:70> msg:DialTimeout success, host: 10.41.5.232, port: 2381
2023-02-17 19:18:52.815069 [INFO] <net.go:47> msg:test etcd port successfully
2023-02-17 19:18:52.815081 [INFO] <switcher.go:73> msg:edr.0) dialEtcd success
2023-02-17 19:18:52.930659 [INFO] <switcher.go:85> msg:edr.1) getConfFromLinux success
2023-02-17 19:18:52.930953 [INFO] <net.go:70> msg:DialTimeout success, host: 10.41.5.232, port: 9092
2023-02-17 19:18:52.931254 [INFO] <net.go:70> msg:DialTimeout success, host: 10.41.5.232, port: 25432
2023-02-17 19:18:52.931553 [INFO] <net.go:70> msg:DialTimeout success, host: 10.41.5.232, port: 9200
2023-02-17 19:18:52.931824 [INFO] <net.go:70> msg:DialTimeout success, host: 10.41.5.232, port: 30043
2023-02-17 19:18:52.932051 [INFO] <net.go:70> msg:DialTimeout success, host: 10.41.5.232, port: 2181
2023-02-17 19:18:52.932263 [INFO] <net.go:70> msg:DialTimeout success, host: 10.41.5.232, port: 9103
2023-02-17 19:18:52.932582 [INFO] <net.go:70> msg:DialTimeout success, host: 10.41.5.232, port: 31191
2023-02-17 19:18:52.932833 [INFO] <net.go:70> msg:DialTimeout success, host: 10.41.5.232, port: 31181
2023-02-17 19:18:52.933065 [INFO] <net.go:70> msg:DialTimeout success, host: 10.41.5.232, port: 9345
2023-02-17 19:18:52.933089 [INFO] <net.go:29> msg:test infra service port successfully
2023-02-17 19:18:52.933103 [INFO] <switcher.go:94> msg:edr.2) dialInfraServices success
```

- 等待天擎管理中心配置成功后，若大数据平台域名无法被内网 DNS 解析，则需要进行本地 hosts 解析，修改文件“/qaxdata/TianqingEndpointSecurity/conf/template.yaml”，向节点“extends:”下添加子节点“k8s_hosts”并填写大数据平台域名和 IP 地址，修改完成后，切换到安装包所在目录，执行命令：“/qaxdata/TianqingEndpointSecurity/utils/darwin/darwin-client install --data.source=local --execute.type=docker-compose --assign.tag --template.file=/qaxdata/TianqingEndpointSecurity/conf/template.yaml --actions=deploy --local.full_install --services_filter=heka-service,edr-service-league,edr-flow-league,argo-service”，等待命令执行完成即可。域名数据配置如下：

```
extends:
  k8s_hosts:
    edr.qianxin.com: 10.41.5.232
  mount:
    darwin-cdn: src=/qaxdata/TianqingEndpointSecurity/data/cdn/files,dest=/home/s/darwin-cdn/data/files,is_dir=true,host_path=true
    trantor-league-v2: src=/qaxdata/TianqingEndpointSecurity/data/trantor-league-v2/data,dest=/home/s/data,is_dir=true,host_path=true
  mod_depends:
    integrated_bi: integrated_noah
  k8s_service:
    darwin-cdn: nodeport,Cluster:https,TCP,32185,32185;http,TCP,32186,32186
    edge2-service: nodeport,local:tcp,TCP,6781,30080;grpc-web,TCP,26781,30081
    gossip-hub: nodeport,Cluster:tcp,TCP,9120
    trantor-fe: nodeport,Cluster:https,TCP,8443,30082
    remote-assistance-repeater: nodeport,Cluster:https,TCP,5901,30090;http,TCP,5500,30091
```

3.5 接入点安装部署（可选）

接入点的安装是在天擎管理中心部署完后进行，需要在天擎管理中心导入许可证后安装。

接入点的作用主要是为了网络代理和分担终端接入量。

服务器操作系统要求：

操作系统	指令集	部署模式	磁盘
CentOS 7.5-7.9 银河麒麟高级服务器操作系统 V10SP3 2303(Lance) AnolisOS(龙蜥)7.9 Alma Linux 9.3 RedFlag-Asianux-7.6	x86_64	虚拟机	根据实际需要缓存的大小
银河麒麟高级服务器操作系统 V10SP2(Sword)	ARM		

注意：10.7.0.2600 及以上版本支持银河麒麟高级服务器操作系统 V10SP3 2303(Lance)和 AnolisOS(龙蜥)7.9，10.7.0.2800 及以上版本支持 Alma Linux 9.3，RedFlag-Asianux-7.6

接入点配置：默认安装路径是:/qaxdata， 要求空间不小于 300G， 接入点有下载缓存的能力，建议将缓存空间设置为 2T（qaxdata 目录大小），以减少接入从管理中心的下载量。配置推荐表如下：

终端数	配置推荐
1000-5000	4C8G
5000-10000	8C16G
10000-20000	16C32G

终端数	配置推荐
备注	**接入点的默认存储方案与缓存正向相关，当缓存占满存储空间时，接入点将会对原有缓存删除，拉取目标缓存对象存储到本地空间；** 故如若对接入点带宽无要求与天擎主机管理中心服务器相同的话，按照实际使用需求的最小容量来部署即可；若与之相反，推荐和与天擎主机服务器的容量一致。 **具体部署时使用的镜像版本请根据部署文档/测试压报告推荐机型。**

3.5.1 检查条件

1) 接入点部署帐号的密码只能为数字、字母、！、@的组合；
2) 接入点部署帐号 sudo 权限；（sudo su 命令进行提权）
3) 根目录分区是否小于 100G；
4) selinux 关闭；
5) swap 分区是永久关闭；
6) sysctl.conf 文件权限是为 644；
7) tmp 分区是否小于 10G；
8) umask 值为 0022；
9) 服务器的时间必须同步；
10) Hostname 设置正确，hostname -f 对应 hostname -i；
11) 时区为 Asia/Shanghai；

3.5.2 网络访问要求

3.5.2.2 windows 管理中心

访问源	目标地址	目标端口	端口说明	业务说明

客户端	接入点	30080	终端通信服务端口，TCP 协议	常规服务如任务、策略、级联通信等
		32185	终端文件传输 HTTPS 服务端口，TCP 协议	在线部署页面及文件上传下载
		32186	终端文件传输服务 HTTP 端口，TCP 协议，随着 HTTPS 端口变化而变化	在线部署页面及在线安装时文件下载
		30081	服务接入端口，TCP 协议	GRPC web 请求
		5500	远程桌面被控端口	远程协助
		5901	远程桌面主控端口	远程协助
接入点	管理中心	6785	终端通信服务端口，TCP 协议	常规服务如任务、策略、级联通信等
		19345	终端文件传输 HTTPS 服务端口，TCP 协议	在线部署页面及文件上传下载
		19346	终端文件传输服务 HTTP 端口，TCP 协议，随着 HTTPS 端口变化而变化	在线部署页面及在线安装时文件下载
		36781	服务接入端口，TCP 协议	GRPC web 请求
管理中心	接入点	32185	管理中心下载接入点文件	天擎 10.7 及以后版本，DLP 文件存储在接入点功能
		32186	管理中心下载接入点文件	天擎 10.7 及以后版本，DLP 文件存储在接入点功能

3.5.2.2 linux 单机管理中心

访问源	目标地址	目标端口	端口说明	业务说明

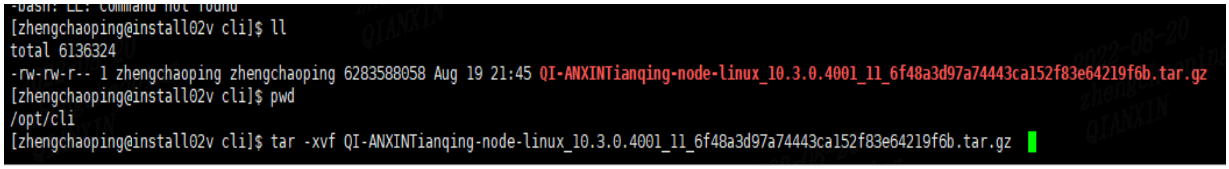
客户端	接入点	30080	终端通信服务端口，TCP 协议	常规服务如任务、策略、级联通信等
		32185	终端文件传输 HTTPS 服务端口，TCP 协议	在线部署页面及文件上传下载
		32186	终端文件传输服务 HTTP 端口，TCP 协议，随着 HTTPS 端口变化而变化	在线部署页面及在线安装时文件下载
		30081	服务接入端口，TCP 协议	GRPC web 请求
		30090	远程桌面主控	远程协助
		30091	远程桌面主控	远程协助
接入点	管理中心	30080	终端通信服务端口，TCP 协议	常规服务如任务、策略、级联通信等
		32185	终端文件传输 HTTPS 服务端口，TCP 协议	在线部署页面及文件上传下载
		32186	终端文件传输服务 HTTP 端口，TCP 协议，随着 HTTPS 端口变化而变化	在线部署页面及在线安装时文件下载
		30081	服务接入端口，TCP 协议	GRPC web 请求
管理中心	接入点	32185	管理中心下载接入点文件	天擎 10.7 及以后版本，DLP 文件存储在接入点功能
		32186	管理中心下载接入点文件	天擎 10.7 及以后版本，DLP 文件存储在接入点功能

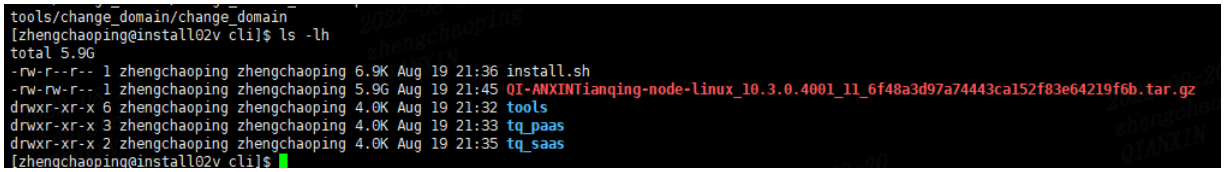
3.5.3 获取文件

访问奇安信官网下载中心页面（https://download.qianxin.com），下载天擎相同版本的接入点，将文件放在/opt/cli 下

3.5.4 解压文件

在接入点上解压安装文件 tar -xvf QI-ANXINTianqing-node-linux_10.3.0.4001_11_6f48a3d97a74443ca152f83e64219f6b.tar.gz 【示例文件】





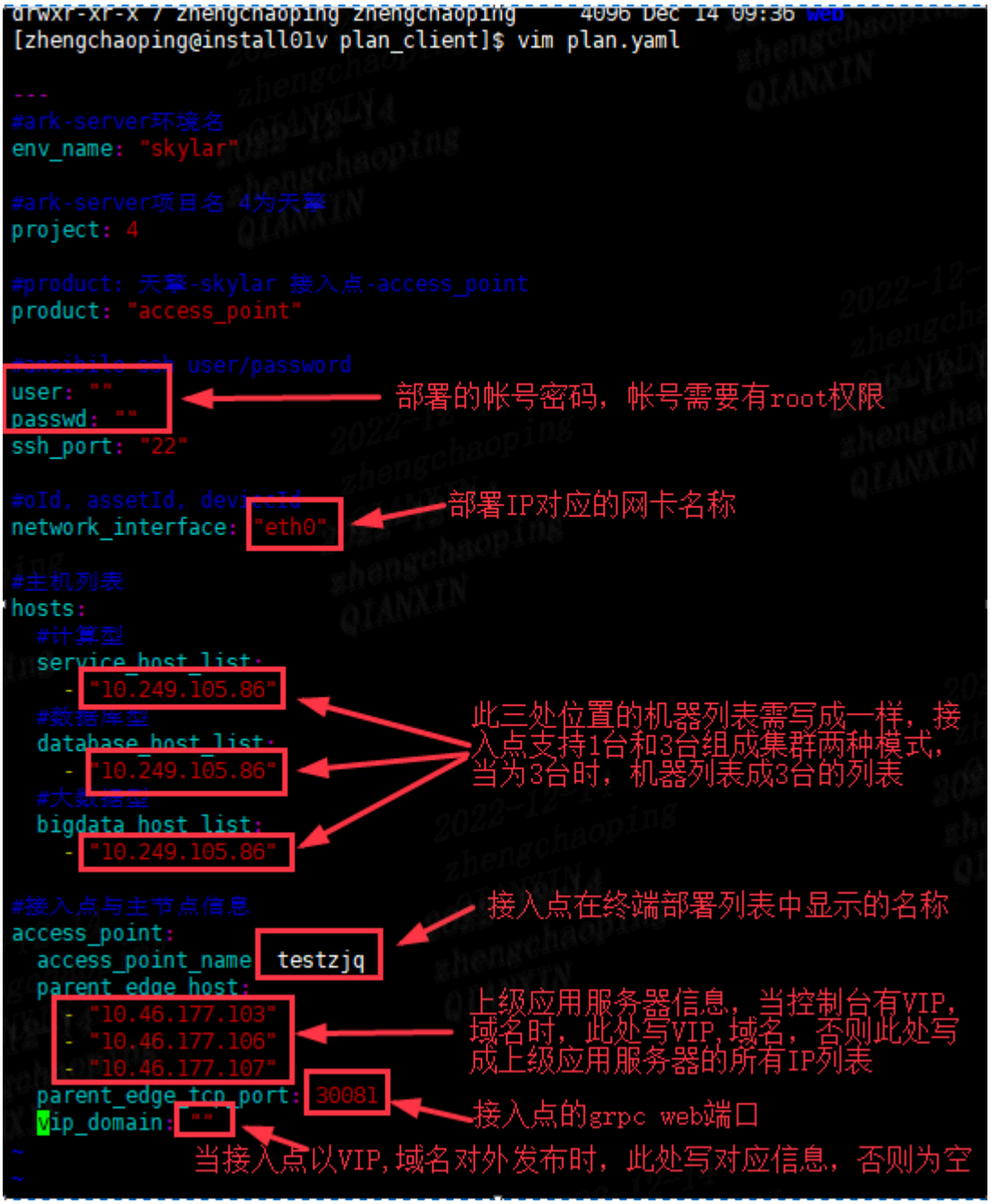
3.5.5 命令行安装（10.6.0.1001 版本支持）

1) 进入安装目录 cd

tq_paas/skylar/skylar_linuxserver_client/plan_client/

2) cp plan.yaml.template plan.yaml

3) vim plan.yaml 配置信息



4) 第 3）步中 parent_edge_tcp_port 可以在上级管理中心>终端管理>终端部署

5) cd /opt/cli

6) nohup sudo sh install.sh > log.install 2>&1 &

3.5.6 图形化安装（10.7.0.1001 以上支持）

1) 解压完成后，先执行 chmod +x install.sh，再执行 sudo sh install.sh，最后浏览器访问 http://ip:9080 地址进行图形化安装。

2) 输入服务器账号、密码等信息后点击继续。该页面信息全部为必填项。

注意：接入点域名跟上级域名相同时，上级不要填域名避免 DNS 解析异常。

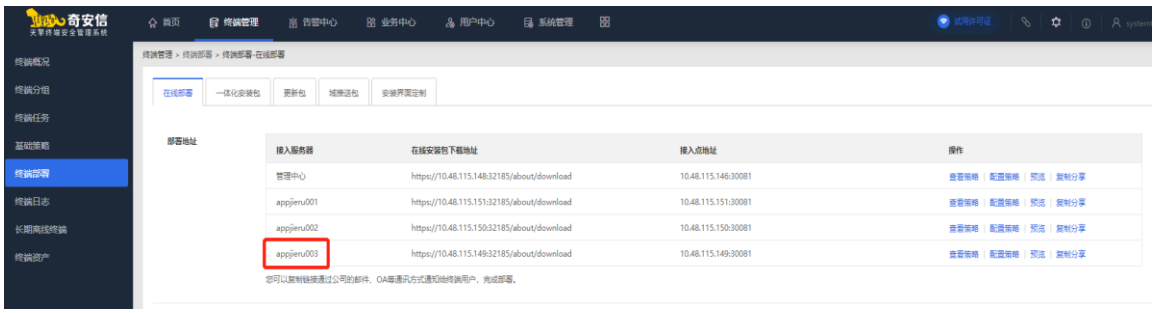
3) 输入接入点地址、VIP 地址（全部为可选项），点击继续。

4) 服务器和服务分布映射关系展示页面，可直接点击继续。

5) 安装检查时间较长，请耐心等待；状态报错时可点击重试失败服务进行重试。多次重试未成功时，需致电 95015 由二线专家进行原因分析。请将失败日志一并上传便于二线专家分析。

3.5.7 安装检查

程序完成，登录天擎管理中心，终端管理>终端部署>在线部署中的部署地址是否出现新安装的新入点。出现为接入点部署成功。



3.6 Windows 客户端部署

3.6.1 安装准备

终端安装后可能占用磁盘 2GB~6GB 左右磁盘空间，默认安装在系统盘 C 盘，您可以在安装的时候手动选择安装的位置，如 D 盘等。终端安装程序支持静默安装、指定路径安装等命令行参数，详见 KB46502。

终端安装后，默认 C:\ProgramData\QI-ANXIN Tianqing 目录会存储一些日志，可能占用 C 盘空间 1~2GB，此占用空间不可更改。如果有补丁模块则定期会进行下载补丁文件至安装目录，进行补丁修复工作，补丁文件默认存放 7 天，如果 C 盘空间不足的情况建议安装在其他磁盘空间充足的路径。

仅防病毒模块时 Windows 客户端版本内存不小于 2GB，CPU 不小于 1GHz 单核；Windows 服务器版内存不小于 4GB，CPU 不小于 1GHz 双核。根据定制模块的数量，硬件配置需适当提高。全部模块时 Windows 客户端版本内存不小于 4GB、建议 8GB，CPU 不小于双核、建议 4 核；Windows 服务器版内存不小于 8GB，CPU 不小于 4 核。

3.6.2 客户端兼容说明

客户端类型	操作系统
Windows 个人版	Windows XP Service Pack 3(x86) Windows 7 Service Pack0(x86/x86_64) Windows 7 Service Pack1(x86/x86_64) Windows 7 Embedded Standard(x86/x86_64) Windows 8.1(x86/x86_64) Windows 10 Version 1507(x86/x86_64) Windows 10 Version 1511(x86/x86_64) Windows 10 Version 1607(x86/x86_64) Windows 10 Version 1703(x86/x86_64) Windows 10 Version 1709(x86/x86_64) Windows 10 Version 1803(x86/x86_64) Windows 10 Version 1809(x86/x86_64)

	Windows 10 Version 1903(x86/x86_64) Windows 10 Version 1909(x86/x86_64) Windows 10 Version 2004(x86/x86_64) Windows 10 Version 20H2(x86/x86_64) Windows 10 Version 21H1(x86/x86_64) Windows 10 Version 21H2(x86_64) Windows 10 Version 22H2(x86_64) Windows 10 神州网信政府版 V0-H/V2020-L/V2022-L Windows 11 Version 21H2(x86_64) Windows 11 Version 22H2(x86_64) Windows 11 Version 23H2(x86_64)（10.7.0.2500 及以上）
Windows 服务器版	Windows Server 2003(x86) Windows Server 2003 R2(x86) Windows Server 2008 Service Pack 2(x86/x86_64)（需更新补丁 KB4474419、KB4493730，确保引入 SHA-2 代码签名支持） Windows Server 2008 R2 Service Pack1(x86_64) Windows Server 2012 R2(x86_64) Windows Server 2016(x86_64) Windows Server 2019(x86_64) Windows Server 2022(x86_64)

3.6.3 客户端功能定制

主要用于不同分组的终端能够定制不同的功能模块，同时能够定义不同的管理员，不同的 logo、界面、语言和托盘右键菜单。满足不同组织不同架构下能够有不同的定制策略需求。

在推送终端安装前为了避免服务器瞬时访问下载的压力，可以适当对全网策略的定制模块进行调整，减小安装包大小，待终端通过自动分组或者其他方式分到对应分组后会自动获取对应的分组策略。

功能模块列表如下：进程管理、远程协助、网络防护、能耗管理、外设管理、违规外联、病毒防护、Win7 加固、XP 加固、BitDefender 引擎、截屏水印、屏显水印、打印

水印、文件分发、移动存储、防火墙、软件统计、软件管理、补丁管理、威胁追踪、威胁处置、数据防泄漏、准入认证客户端、安检合规、基线核查、弹窗防护等。

3.6.4 客户端在线部署

使用在线部署前，管理员可以在终端管理>基础策略页面配置安全策略，并在终端管理>终端部署页面自定义部署通知和安装界面，并通过内部邮件或 OA 系统等多种渠道通知终端用户。终端用户访问部署地址、下载对应操作系统的终端并双击安装即可。安装过程的速度与安装模块多少及网络带宽有关。

入口：终端管理>终端部署页面，切换至“在线部署”，即可配置安装说明等信息，并预览实际效果。

说明：

1、如果在服务端配置工具中勾选“客户端在线部署地址切换”功能，在线下载客户端的地址将展示为：“https://管理中心地址”。配置方法详见 3.3.2.6 章节。

2、终端部署页面支持使用 Chrome69 以上版本、Edge84 以上版本、IE10 以上版本、Firefox52.2.0 以上版本的浏览器或者奇安信浏览器访问。

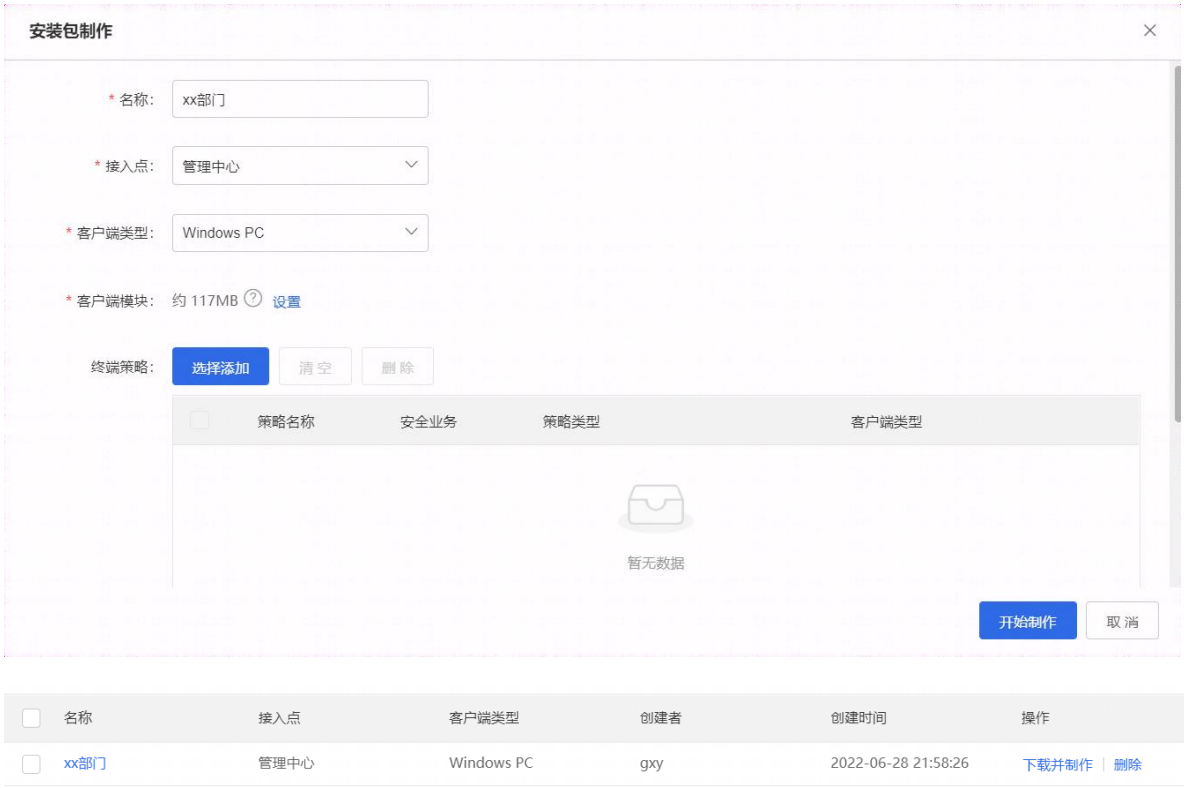
3.6.5 客户端离线部署

使用一体化安装包进行离线部署，一部分是为了节约服务器带宽，避免企业内部瞬时带宽或服务器瞬时压力不足时带来的影响，另一方面是保证安装成功率。

如果用于完全不连接网络的孤岛终端，也可以使用制作出的一体化安装包，给这些终端安装。

入口：终端管理>终端部署页面并切换至“一体化安装包”

操作：选择[添加]然后完成客户端类型、模块等相关信息的设置然后保存，之后下载制作工具制作即可。



解压后使用下载的 exe 工具双击运行，则程序按照指定的信息制作一体化安装包。制作完成后会在一个临时文件夹中生成安装程序，类似：C:\ProgramData\QAXSafe\Update\{1aa13c66-b310-4437-afb9-12a58bbb517b}.tmp\download，安装程序分发给对应终端用户安装即可。

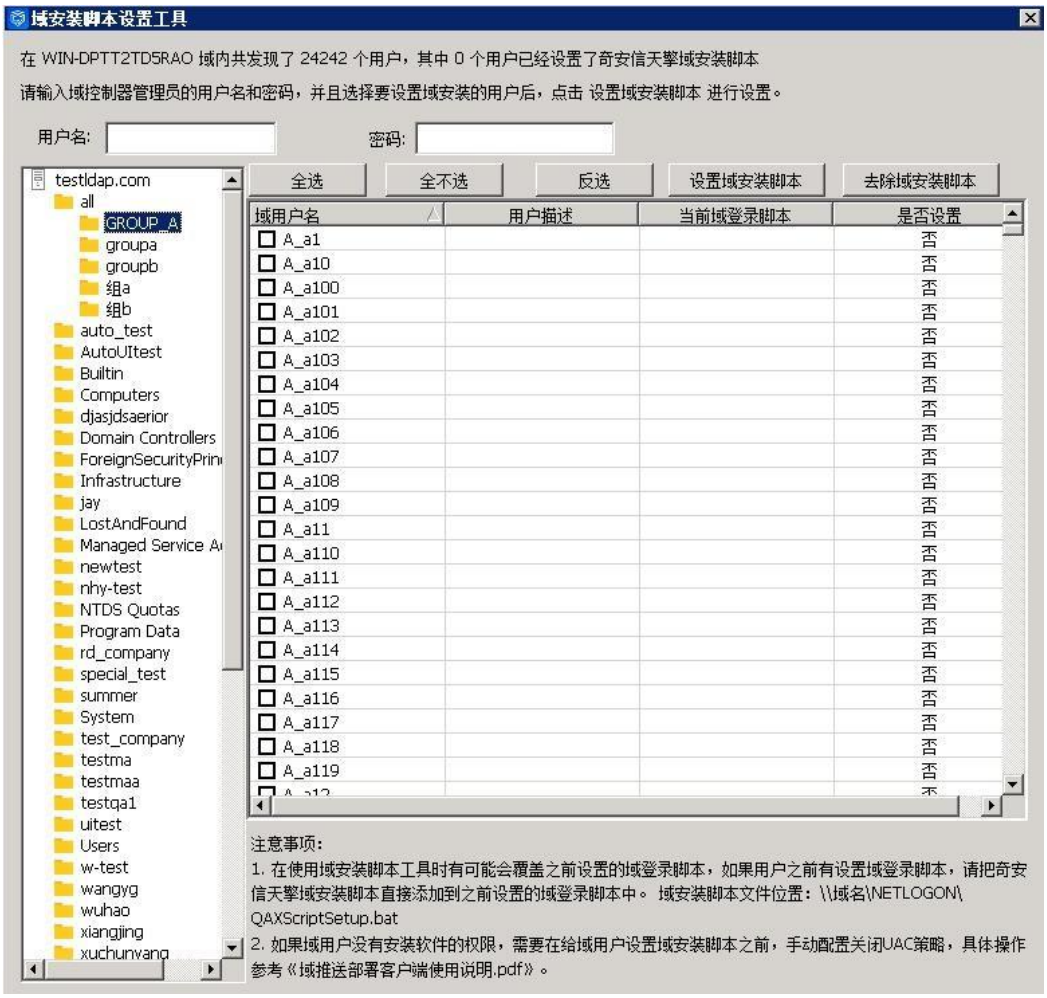
3.6.6 终端域推送部署

企业有域服务器时可以使用域推送的方式把奇安信天擎终端安装在域内设备上，对应的域用户下次登录系统后会自动静默安装。

在管理中心的“终端管理-终端部署”页面的“域推送包”Tab 页，下载域推送工具。具体操作步骤如下：

从奇安信天擎管理中心下载域推送工具压缩包后解压，然后把 QAXScriptSetup.exe 文件放到企业的域控制器上，并将 config.ini 和

runinstall.exe 放在 QAXScriptSetup.exe 同级目录下，然后运行 QAXScriptSetup.exe，如下图：



在使用域推送工具之前，需要确认域环境中的域用户是否具有安装软件的权限，如果域用户不具备安装软件的权限，需要在使用域推送工具之前，手动配置关闭 UAC 策略，否则域推送工具的域安装脚本无法进行提权并安装奇安信天擎客户端。配置关闭 UAC 策略的操作步骤如下：

（1）打开组策略管理编辑器，选择一个 OU，右键点击【在这个域中创建 GPO 并在此处链接】

（2）在新建 GPO 的弹窗中，输入名称，点击【确定】

（3）选择该 GPO，右键点击【编辑】，会打开“组策略管理编辑器”，在“组策略管理编辑器”中依次展开“计算机配置-策略-Windows 设置-安全设置-本地策略-

安全选项”，在安全选项中，双击“用户账户控制：以管理员批准模式运行所有管理员”，勾选“定义此策略设置”，选择“已禁用”，并【应用】，点击【确定】

（4）完成关闭 UAC 策略的配置后，该策略会推送并应用到所选 OU 下域用户的计算机上。

注意：OU 下的组策略需要有计算机才生效，如果只有域用户则不生效，因为组策略是配置“计算机配置”、非“用户配置”。

如果需要全局生效（无需移动计算机到 OU），则在组策略管理中，右键编辑“Default Domain Policy”，在“组策略管理编辑器”中依次展开“计算机配置-策略-Windows 设置-安全设置-本地策略-安全选项”，在安全选项中，双击“用户账户控制：以管理员批准模式运行所有管理员”，勾选“定义此策略设置”，选择“已禁用”，并【应用】，点击【确定】。

该策略在被应用到计算机上后，需要计算机重启策略才会实际生效，建议在使用域推送工具之前，至少提前一天配置关闭 UAC 策略。

如果域用户具有安装软件的权限，或者域用户没有安装软件的权限，但已配置关闭 UAC 策略且策略已生效，则打开域推送工具，待当前域控服务器的用户分组、用户列表获取完毕，选择用户分组以及用户分组下需要部署奇安信天擎客户端的域用户之后，输入域控服务器管理员的用户名和密码，然后点击右上方的【设置域安装脚本】按钮，这样在该用户的当前域登录脚本就会显示 QAXScriptSetup.bat。

给域用户设置域登录脚本后，会自动推送到域用户的计算机上，在域用户注销或者重启机器后再次登录操作系统，域登录脚本才会自动运行进行静默安装，安装成功之后当前用户即可使用奇安信天擎客户端。

注意事项：在使用域安装脚本工具时有可能会覆盖之前设置的域登录脚本，如果用户之前有设置域登录脚本，请把奇安信天擎域安装脚本直接添加到之前设置的域登录脚本中。

域安装脚本文件位置：\\域名\NETLOGON\QAXScriptSetup.bat

3.6.7 客户端跃迁

当企业内网中已经存在 V6 版本的终端时，仍可使用上述终端安装方法安装 V10 版本客户端。在安装 V10 版本客户端前也可以利用分发工具或者天擎软件分发功能批量分发 V10 安装包进行安装，存在 V6 客户端的终端仅会安装 V10 的基础模块并上报到 V10 管理中心，且托盘会隐藏。

管理员可在 V10 管理中心下发跃迁任务完成 V6 客户端的卸载以及 V10 客户端的安装，安装状态可在终端管理-终端概况查看，过程和结果可在管理中心-终端管理-终端日志查看。

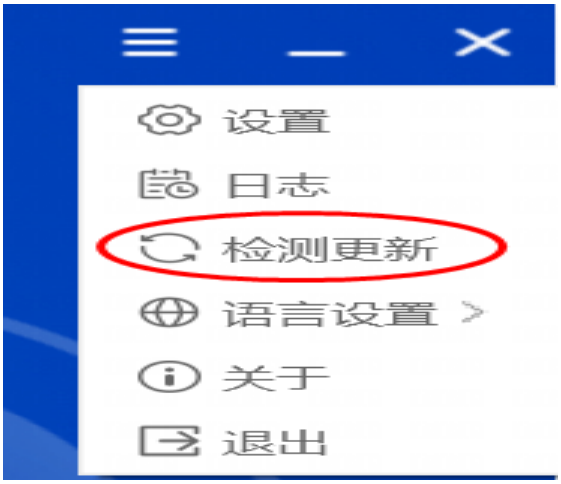
具体操作参考《奇安信天擎终端安全管理系统 V10.0 终端跃迁手册》，可在文档中心下载，或联系交付咨询获取。

3.6.8 客户端更新

如果已存在 V10 版本客户端，可以打开主界面点击左上角箭头（图一）或者右上角托盘菜单下“检测更新”（图二）进行更新检查和更新。

另外，客户端也会按照管理员配置的更新设置自动定时从服务端检查更新。

图一



图二

3.6.9 客户端卸载

Windows 版本请直接打开系统卸载程序，找到奇安信天擎终端安全管理系统，双击卸载即可，管理员可能配置有密码，输入卸载密码即可完成一键卸载。

3.7 macOS 客户端部署

3.7.1 客户端兼容说明

操作系统	CPU 架构	
	x86/x86_64	ARM(M 系列芯片)
macOS X 10.15	✓	
macOS 11	✓	
macOS 12.0.1	✓	
macOS 12.1	✓	✓
macOS 12.2	✓	✓
macOS 12.3	✓	✓
macOS 12.4	✓	✓
macOS 12.5	✓	✓
macOS 12.6	✓	✓
macOS 12.7	✓	✓
macOS 13	✓	✓
macOS 14	✓	✓

3.7.2 客户端功能定制

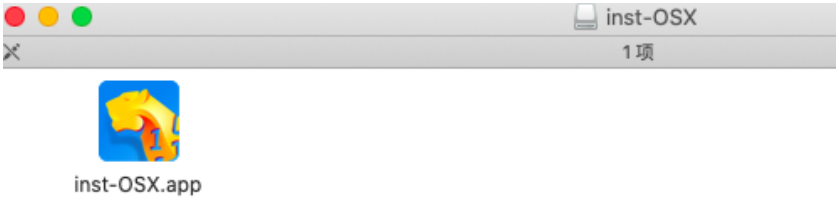
主要用于不同分组的终端能够定制不同的功能模块，同时能够定义不同的管理员，不同的 Logo、界面、语言和托盘右键菜单。满足不同组织不同架构下，有不同定制策略的需求。

3.7.3 客户端在线部署

登录管理中心，进入终端管理>终端部署，配置所需安全策略后通过邮件、OA 等方式通知终端用户访问并下载安装。参考如下步骤：

1、终端用户获取在线部署地址访问并下载对应平台在线安装包

2、运行 inst-OSX-(10.48.56.172_30001-CNbHgOCIy4nqJBCHjwY=).dmg（示例）

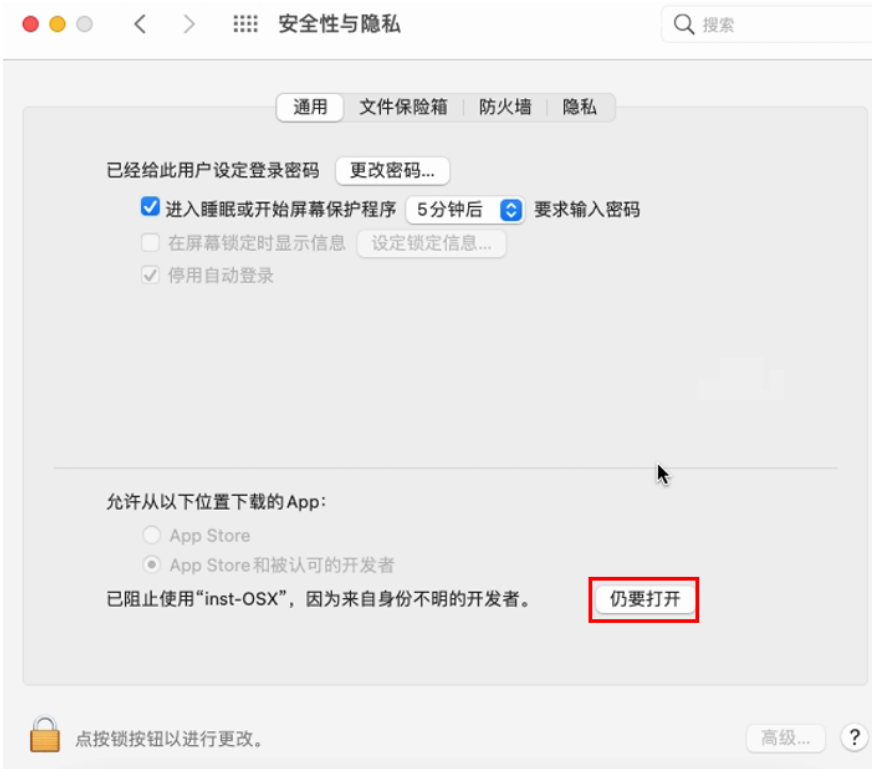


3、点击运行 inst-OSX.app，点击立即安装

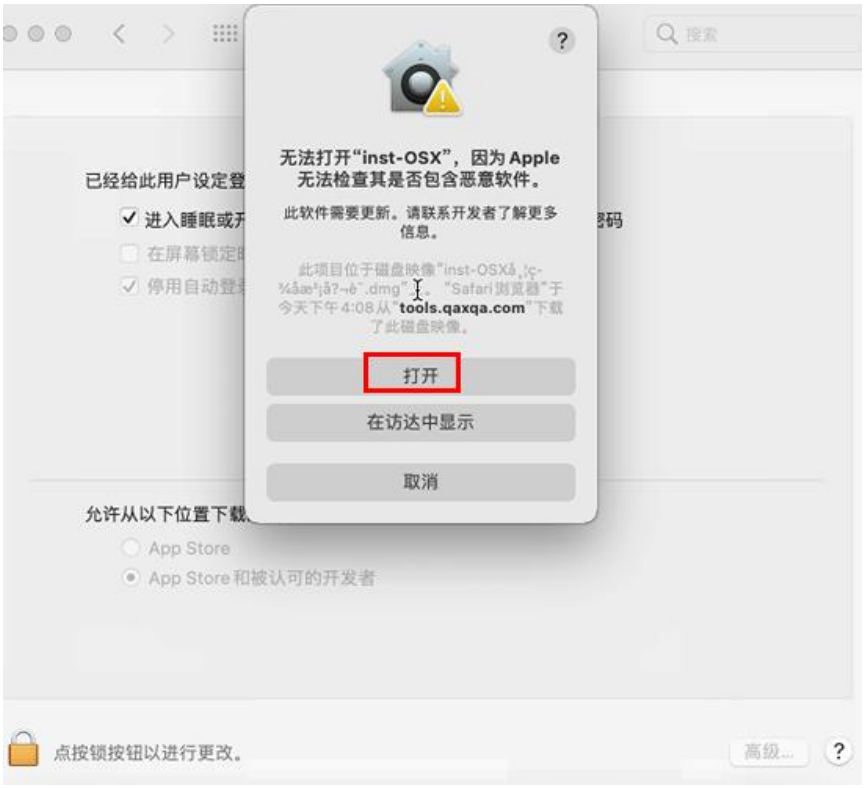
在这个步骤，可能会遇到下面的弹窗。

这是正常弹窗。原因是触发了苹果的 GateKeeper 检查，解决方法：

1）系统偏好设置>安全性与隐私>通用，点击仍要打开



2）再次点击运行 inst-OSX.app，在弹窗中点击打开。



说明：终端部署页面支持使用 Chrome69 以上版本、Edge84 以上版本、IE10 以上版本、Firefox52.2.0 以上版本的浏览器或者奇安信浏览器访问。

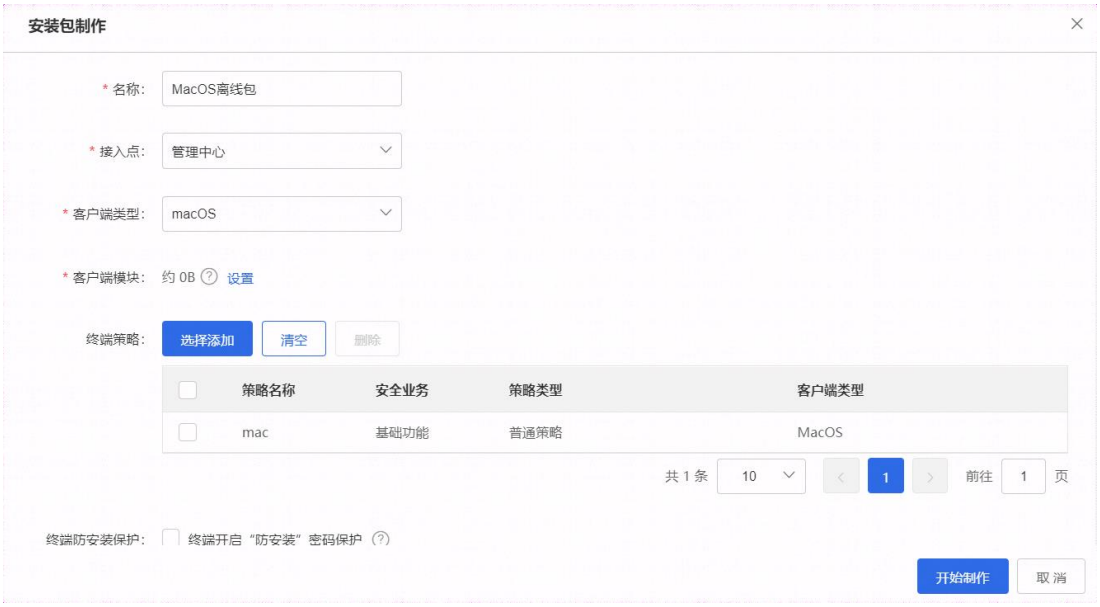
3.7.4 客户端离线部署

使用一体化安装包进行离线部署，一部分是为了节约服务器带宽，避免企业内部瞬时带宽或服务器瞬时压力不足时带来的影响，另一方面是保证安装成功率。

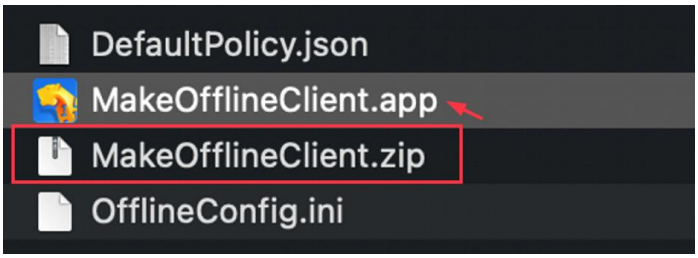
如果用于完全不连接网络的孤岛终端，也可以使用制作出的一体化安装包，给这些终端安装。

入口：终端管理>终端部署并切换至“一体化安装包”

操作：选择[添加]然后完成客户端类型、模块等相关信息的设置然后保存，之后下载制作工具在对应平台双击运行制作即可，制作完成后即可分发给终端用户直接安装。

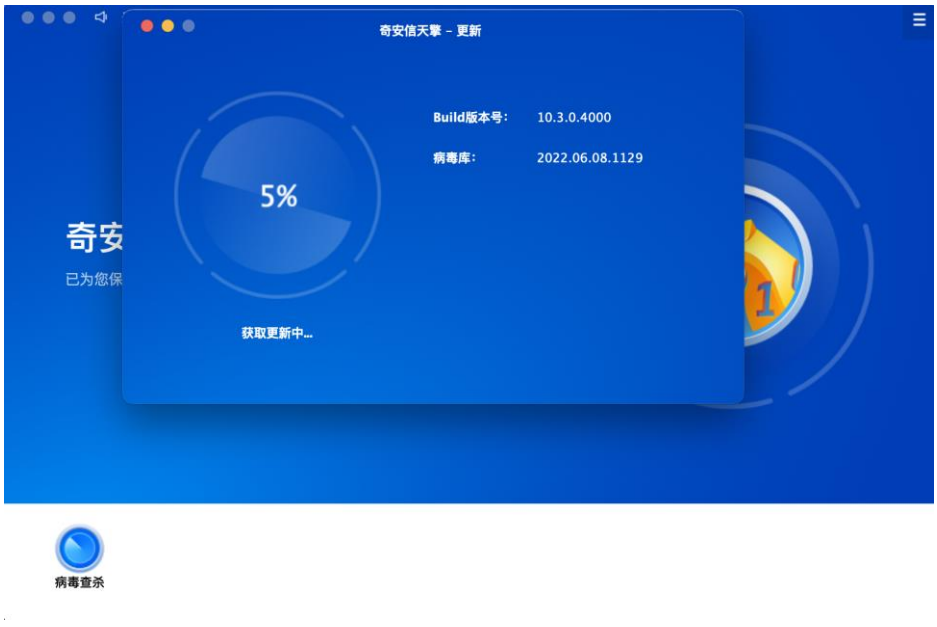


在 macOS 系统解压 zip 包，然后再将 MakeOfflineClient.zip 解压，然后双击或者右击“打开”即开始制作并生成 dmg 安装包；双击或右击“打开”dmg 文件即可开始安装。



3.7.5 客户端更新

打开客户端，点击主界面右上角菜单项-检测更新，客户端会自动更新主程序、病毒库等。



3.7.6 客户端卸载

在终端上找到应用程序，直接将程序右击选择放进废纸篓即可。

3.8 信创与 Linux 服务器客户端部署

3.8.1 客户端兼容说明

操作系统	CPU 架构			
	ARM	MIPS	x86_64	LoongArch
中标麒麟 v5	✓	✓	✓	
中标麒麟 v6	✓	✓	✓	
中标麒麟 v7	✓	✓	✓	
银河麒麟 v3	✓	✓	✓	
银河麒麟 v4	✓	✓	✓	
麒麟 V10	✓	✓	✓	✓
深度操作系统 v15			✓	
统信 UOS v20	✓	✓	✓	✓
CentOS 5			✓	
CentOS 6			✓	
CentOS 7			✓	
CentOS 8			✓	
Red Hat Enterprise Linux 5			✓	
Red Hat Enterprise Linux 6			✓	
Red Hat Enterprise Linux 7			✓	
Red Hat Enterprise Linux 8			✓	

Ubuntu			✓	
SLES11SP3			✓	

以上仅作为系统类别的简述，截止目前已经适配了 510 多个不同版本的信创系统和 Linux 系统，具体版本支持情况请参考 KB28560、KB45759 或联系奇安信技术人员。

3.8.2 客户端在线部署

使用在线部署前，管理员可以在终端管理>基础策略页面配置安全策略，并在终端管理>终端部署页面自定义部署通知和安装界面，并通过 OA 或者内部邮件等渠道通知终端用户，终端用户获取部署地址后访问并下载对应操作系统的客户端下载，然后安装即可；安装过程与安装模块多少以及网速相关。

前提：在线部署客户端前需先更新 Linux 服务器或信创终端等需使用的版本，“更新管理”检查更新，或者使用离线更新工具更新。

部署入口：终端管理-终端部署页面并切换至“在线部署”。使用浏览器访问部署地址，查看下方“不同的终端/系统下载”

点击“***下载”，获取安装脚本，不要修改文件名称，在目标终端的命令行窗口，使用 sudo bash 执行脚本，例如：sudo bash installer-linuxc.sh

然后根据提示操作安装；

该脚本自动到管理中心下载相应版本的安装文件，直至完成安装。

```
root@test-pc:/home/test/桌面# sudo bash '/home/test/下载/installer-linuxc .sh'
用法：您可以通过执行如下命令进入定制模式
bash /home/test/下载/installer-linuxc .sh diy
---------------------------------
## 当前系统信息：
## 系统位数:64位系统
## 芯片架构:x86
## 安装包管理器:deb
## 终端类别:信创终端
```

说明：

1、因统信 UOS 系统，默认没有启用 root 用户权限，无法支持在线安装部署，需要用离线部署方式，见下节 3.8.3 客户端离线部署。

2、终端部署页面支持使用 Chrome69 以上版本、Edge84 以上版本、IE10 以上版本、Firefox52.2.0 以上版本的浏览器或者奇安信浏览器访问。

注意：Linux Server 没有 UI 界面。

3.8.3 客户端离线部署

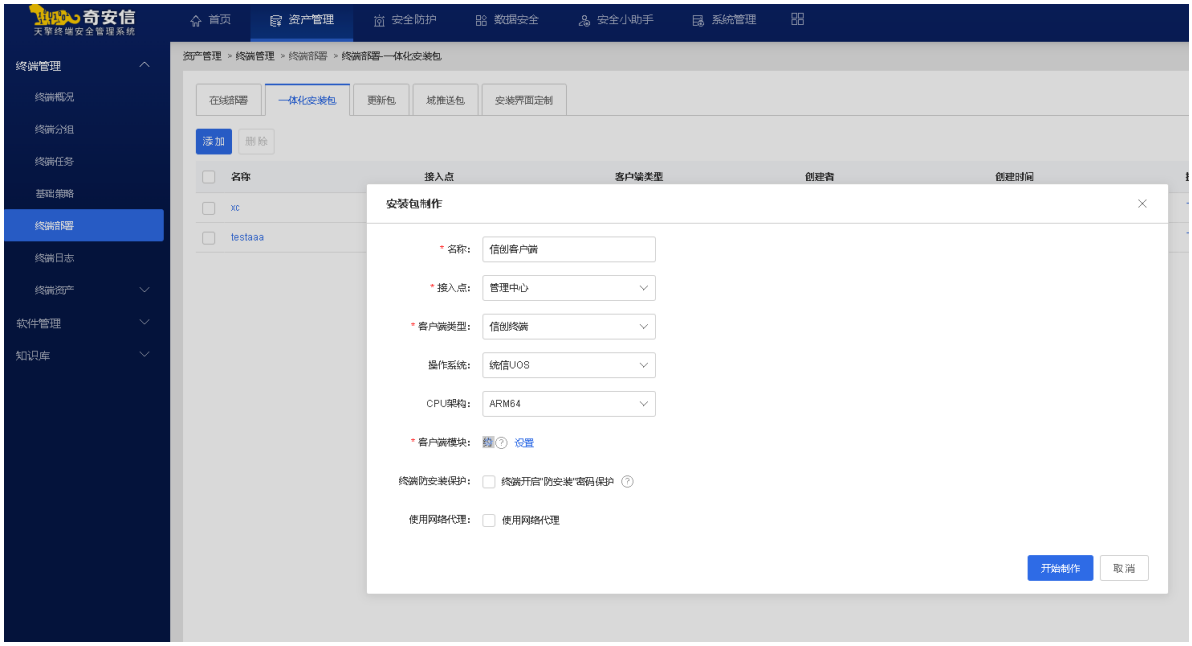
使用一体化安装包进行离线部署，一部分是为了节约服务器带宽，避免企业内部瞬时带宽或服务器瞬时压力不足时带来的影响，另一方面是保证安装成功率。

如果用于完全不连接网络的孤岛终端，也可以使用制作出的一体化安装包，给这些终端安装。

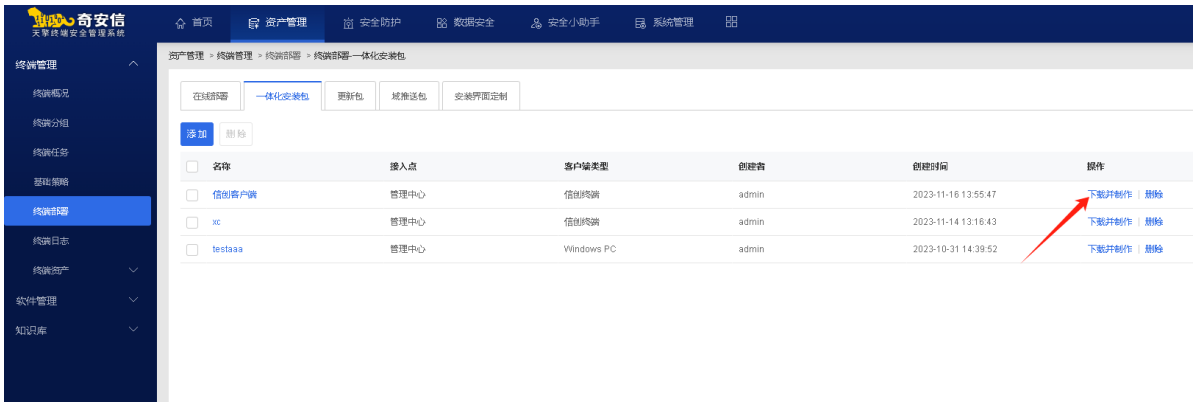
入口：终端管理>终端部署页面并切换至“一体化安装包”

操作：

1. 选择[添加]，输入名称、接入点、客户端类型、操作系统、CPU 架构、客户端模块等相关信息的设置然后点击[开始制作]，之后下载制作工具制作即可。



2. 点击【下载并制作】，如图下载到本地为 “信创客户端_安装包制作工具.zip” 的压缩包

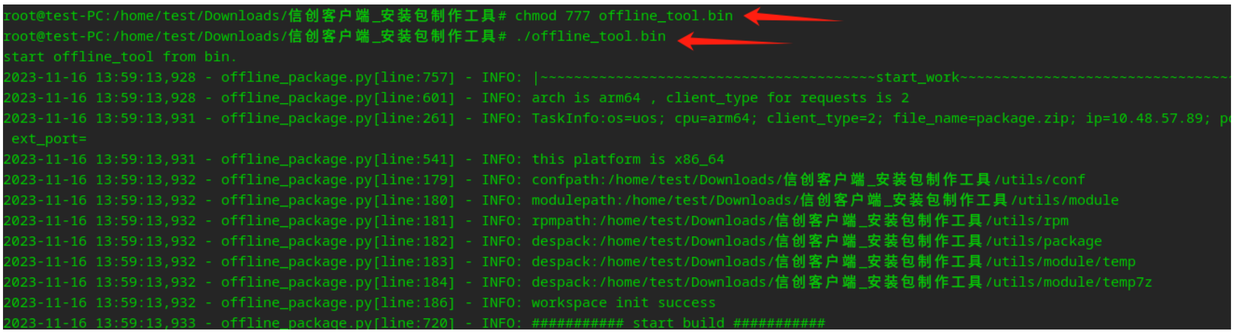


3. 解压“信创客户端_安装包制作工具.zip”

4. 在终端命令行进入解压目录后，要使用 root 用户，先给 offline_tool.bin 文件可执行权限：

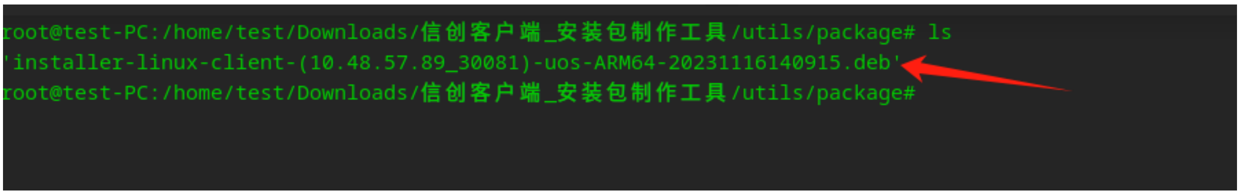
```
chmod 777 offline_tool.bin
```

注意：如果终端是 UOS 系统，需要开启 UOS 系统的开发者模式，才能用 root 用户。



5. 终端命令行执行 ./offline_tool.bin，然后开始下载响应模块文件，制作完成后，提示如下：

6. 生成的安装包存在 utils/package　目录下，如图：



一体化安装包使用时注意：

1） 安装前确认信息：

- ➢ 确认当前环境的硬件平台以及操作系统（包含内核等信息）
- ➢ 非麒麟 V10 或统信 UOS 的系统确认软件管理机制是 rpm 还是 dpkg

2） 进行安装

- ➢ 如果系统软件管理机制为 rpm 安装命令为 【rpm -ivh 安装包.rpm】
- ➢ 如果系统软件管理机制为 dpkg 安装命令为【dpkg -i 安装包.deb】
- ➢ 如果系统为麒麟 V10 或统信 UOS，在桌面直接双击安装离线安装包即可

说明：

当发现产品安装异常、或部分功能不生效时，请查看 KB28560，返回系统内核版本等信息，根据 wiki 中指引提交系统适配的工作。

3.8.4 客户端跃迁

当企业内网中已经存在信创 V8 版本的终端时，可以使 V8 客户端无感知升级到 V10 版本。

功能说明：支持 V8.0.5.5144 及以上（小于 8.0.5.5200）、V8.0.5.5260 及以上版本的信创终端和 Linux 服务器终端跃迁到 V10 版本。

操作说明：

1) V8 版本的终端需要先升级到支持跃迁的版本（升级操作见《奇安信网神终端安全管理系统-部署实施方案》）。
2) 管理员通过 V8 控制中心，通过“系统管理-系统工具-迁移工具”下发终端迁移任务，把 V8 版本的终端迁移到 V10 的控制中心（V8 版本的终端迁移操作见《奇安信网神终端安全管理系统-管理员操作手册》）。
3) 终端迁移到 V10 控制中心后，自动下载 V10 版本的终端文件，下载完成后，在 V10 的控制中心的终端概况中，可查看终端的版本为 V10 的版本，完成客户端跃迁。

3.8.5 客户端更新

如果已存在 V10 版本客户端，可以打开主界面点击左上角箭头（保证服务端已有可更新的版本）。另外，客户端也会按照管理员配置的更新设置自动定时从服务端检查更新。

3.8.6 客户端卸载

1) 卸载前确认信息：

- 系统的软件管理机制是 rpm 还是 dpkg
- 如果系统是 UOS，我们的程序名为：com.qianxin.qaxsafe
- 如果系统不是 UOS，我们的程序名为：qaxsafe

2) 进行卸载

- 如果系统软件管理机制为 rpm 卸载命令为 【rpm -e 程序名】
- 如果系统软件管理机制为 dpkg 卸载命令为【dpkg -P 程序名】
- 如果系统为麒麟 V10 或统信 UOS，也可使用系统程序管理来进行卸载

第4章 许可证申请和激活

4.1 许可证激活及下载

快捷激活平台（奇安信官网）：https://www.qianxin.com/applyfortrial

1) **申请试用**：可直接在奇安信官网填写信息后申请一个月的试用许可证，申请通过后会将许可证码通过短信或者邮件方式通知用户；或者联系销售人员和当地经销商。

2) **许可证激活**：访问奇安信奇安信**官网**输入**许可证 ID** 后点击“下一步”并按照提示输入**设备 ID** 和手机号进行激活和下载。

3) **导入许可证**：首次登陆管理中心，会提示需要导入许可证，此时选择许可证文件导入或者联网模式下使用许可证 ID 直接激活导入即可。

4) **许可证更换**：登陆管理中心，在页面右上角有许可证信息 

，点击许可证即可跳转至许可证信息页面，点击“更新”然后选择许可证导入即可完成更换，具有相同组织和资产 ID 的许可证才可以导入更换；管理中心在互联网模式下可以自动更新

特别说明：不同机构/组织不可混用许可证，在激活、导入和更换过程中遇到任何问题，请联系 95015 或对应项目支持团队项目经理协助解决，或参考许可证使用手册 KB38547。

4.2 许可证更换场景 FAQ

4.2.1 许可证到期或者测试许可转正式许可该如何操作？

场景说明：如果您网内仅有 1 台服务器，测试完成后希望换成正式许可证使用，或者当旧许可证到期需要更换新许可证（不续期旧许可）。

操作方法：

1) 如果都是新旧许可都是测试许可，则直接通过奇安信官网或者蓝信平台即可完成新许可与旧设备 ID 绑定；

2) 如果是测试转正式，或者正式过期换新的正式许可，则需要在奇安信官网先对旧许可证进行解绑，再用设备 ID 绑定新许可证即可。

4.2.2 天擎管理中心铲了重装，许可证如何处理？

场景说明：如果您网内安装服务器后，无论是否挂载了客户端，此时因各种原因需要卸载重装。

操作方法：

1) 10.3.0.4200 以下版本，卸载天擎管理中心再重装后需要使用“更换设备”功能将新设备 ID 进行更换。详见许可证使用手册。

2) 如果 10.4.0.4200 及以上版本，卸载天擎管理中心后再重装，设备 ID 不变，无需操作可直接导入原许可证使用。

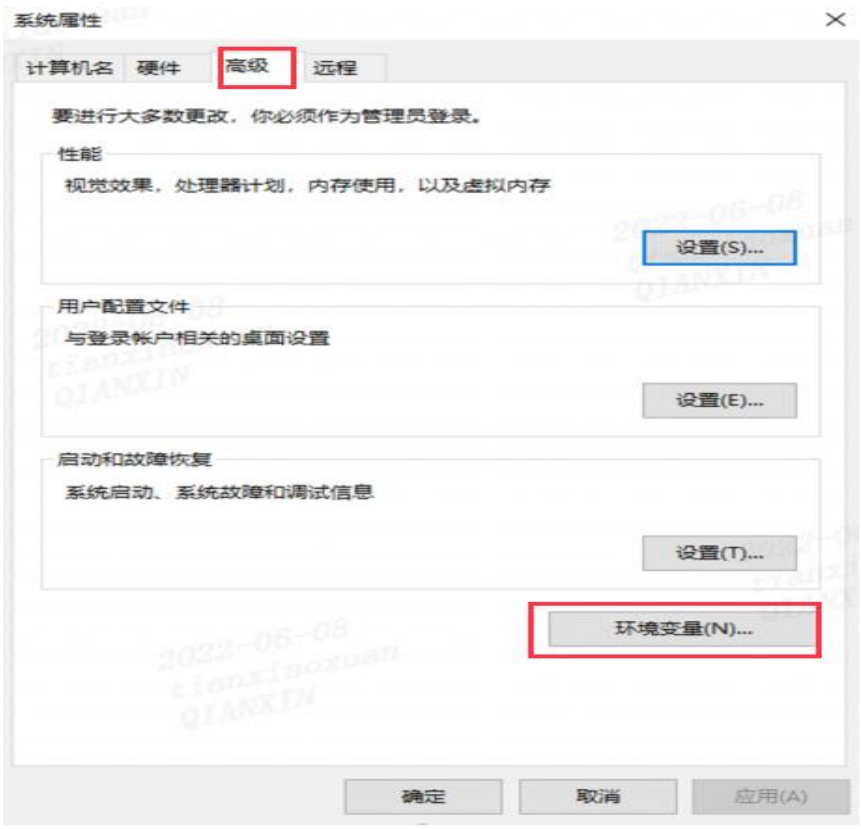
3) 任何版本的天擎管理中心，服务器操作系统重装后再安装天擎，需要使用“更换设备”功能将新设备 ID 进行更换。详见许可证使用手册。

第5章 附录

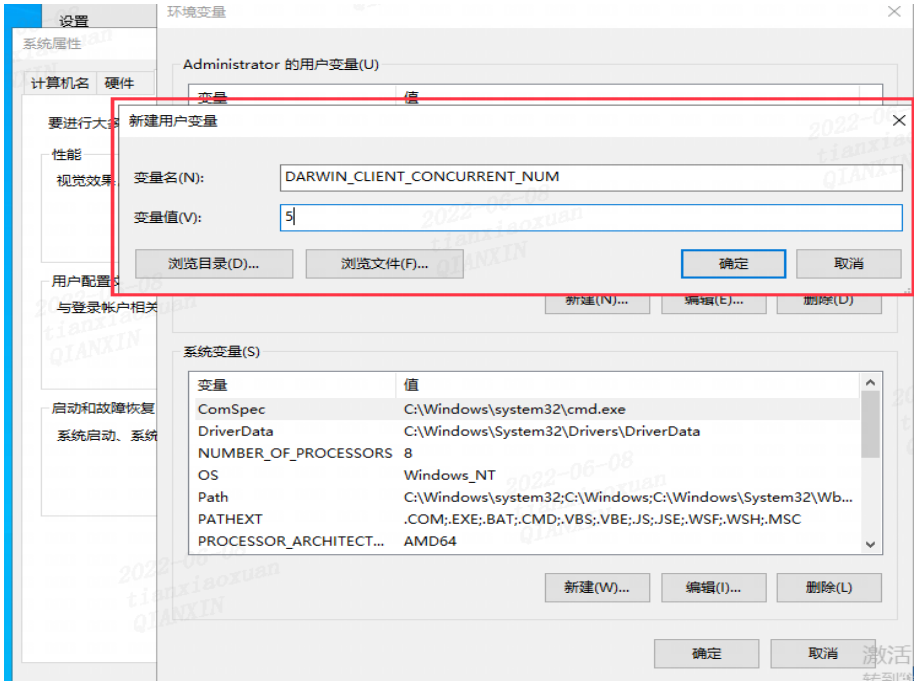
5.1 低 IOPS 配置下系统参数调整

IOPS 在 200 左右的硬盘（例如比较老旧的传统机械硬盘），安装时可能因磁盘性能不足导致安装失败，按照如下操作可提高安装成功率：

1) 进入控制面板，找到“系统-高级系统设置”，在系统属性界面中点击“高级”中的环境变量。



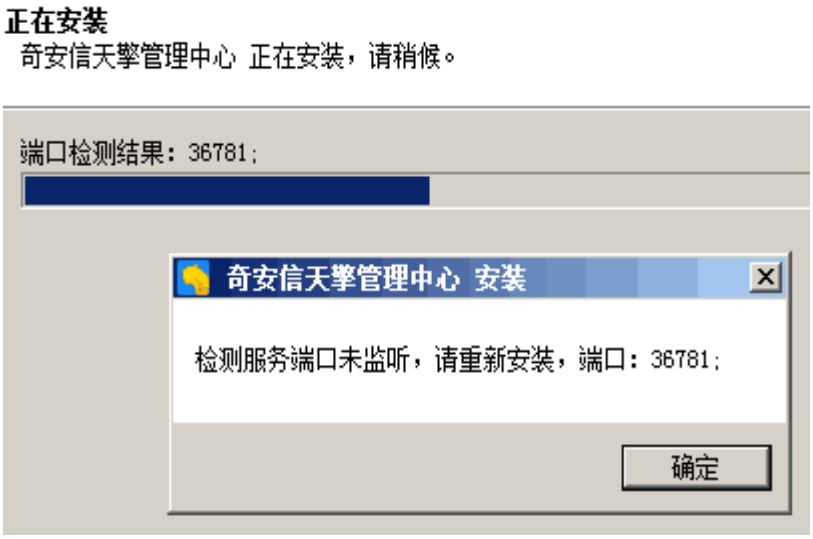
2）在用户变量中选择新建， 添加变量名：DARWIN_CLIENT_CONCURRENT_NUM，变量值：5。



3）点[确定]后，重新运行安装包即可。

5.2 单机部署常见问题

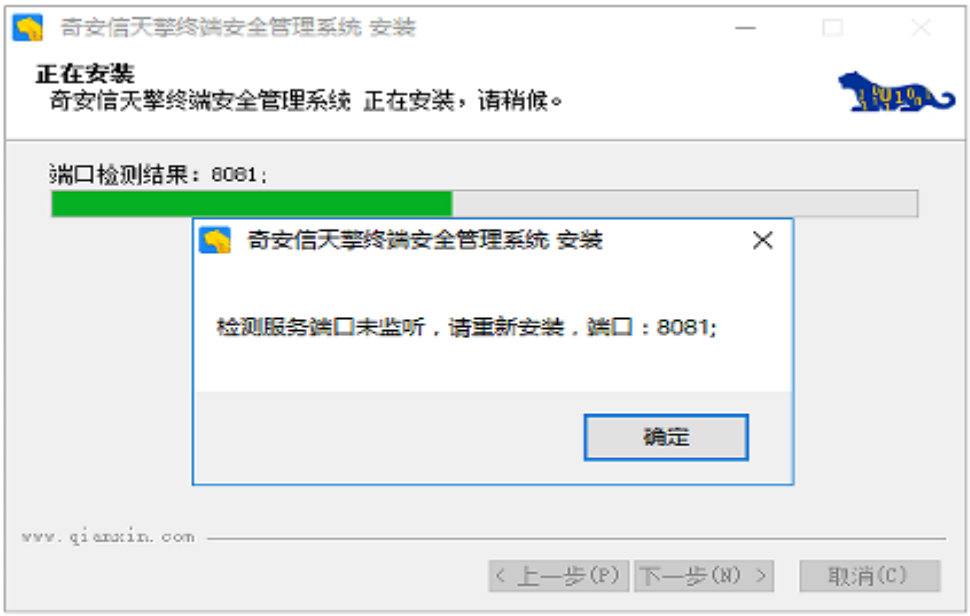
5.2.1 天擎管理系统安装，弹窗提示“检测服务端口未监听，请重新安装，端口：36781”。



解答：

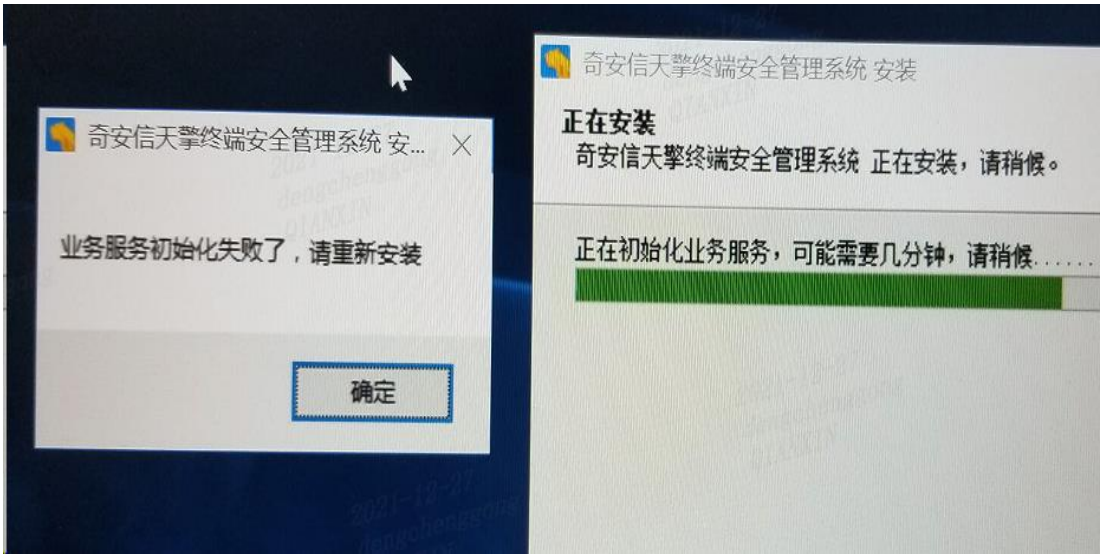
端口对应服务未启动，需要检查服务器的软硬件要求要求是否满足（参考 3.2.1 章节），亦可查看安装目录的 Setup 日志。

5.2.2 天擎管理系统在 Server 2012 R2 系统安装，弹窗提示“检测服务端口未监听，请重新安装，端口号：2379；5432；6379；8081；9345；36781”。



解答：目前新天擎管理系统服务器使用 Windows Serer 2012 R2 操作系统进行部署需要安装补丁，在控制面板安装程序中检查是否安装了补丁 KB2999226，如果没有请下载并安装，如果安装失败请依次尝试安装 KB2919355、KB2919442 后再次尝试。安装补丁后请重启操作系统。如果已安装补丁或其他操作系统版本可联系技术支持。

5.2.3 安装 V10 控制中心，进度显示“正在初始化业务服务，可能需要几分钟，请稍后”，然后一会弹窗出现“业务服务初始化失败了，请重新安装”报错。



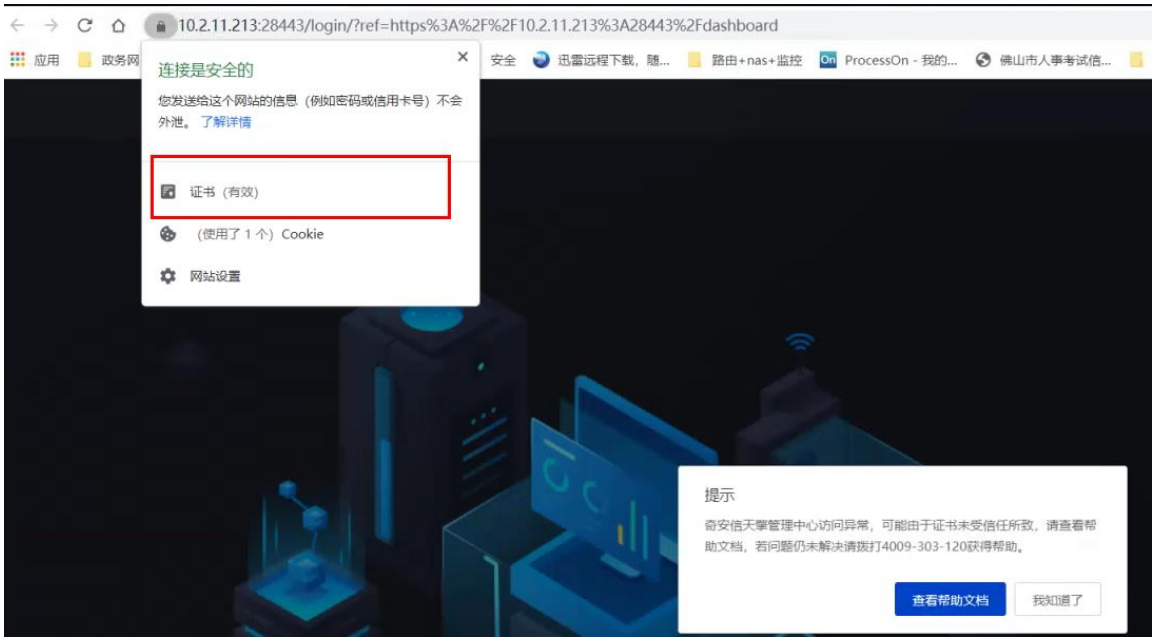
解答：

a) 检查管理系统服务器时间是否正确。

b) 查看服务器是否是公网云服务器，并参考端口放行矩阵，确认是否放通相关端口。

c) 检查服务器 IP 是否是公网 IP，如果是，则在本地网卡增加一个私网地址进行安装。

5.2.4 非服务器本地访问管理系统，一直提示导入证书，但是证书显示有效。

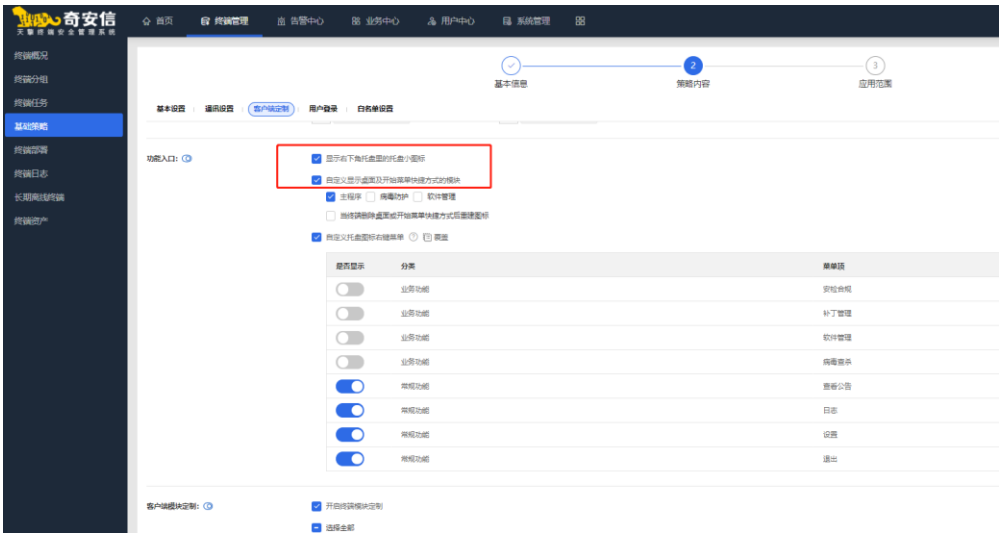


解答：查看访问管理系统的环境是否放行了如下 28443 和 36781 端口（参见 3.2.2 章节），没有放通需要及时放通。

5.2.5V10 客户端刚安装完成，桌面无快捷方式且客户端无模块、无托盘图标怎么办？

解答：

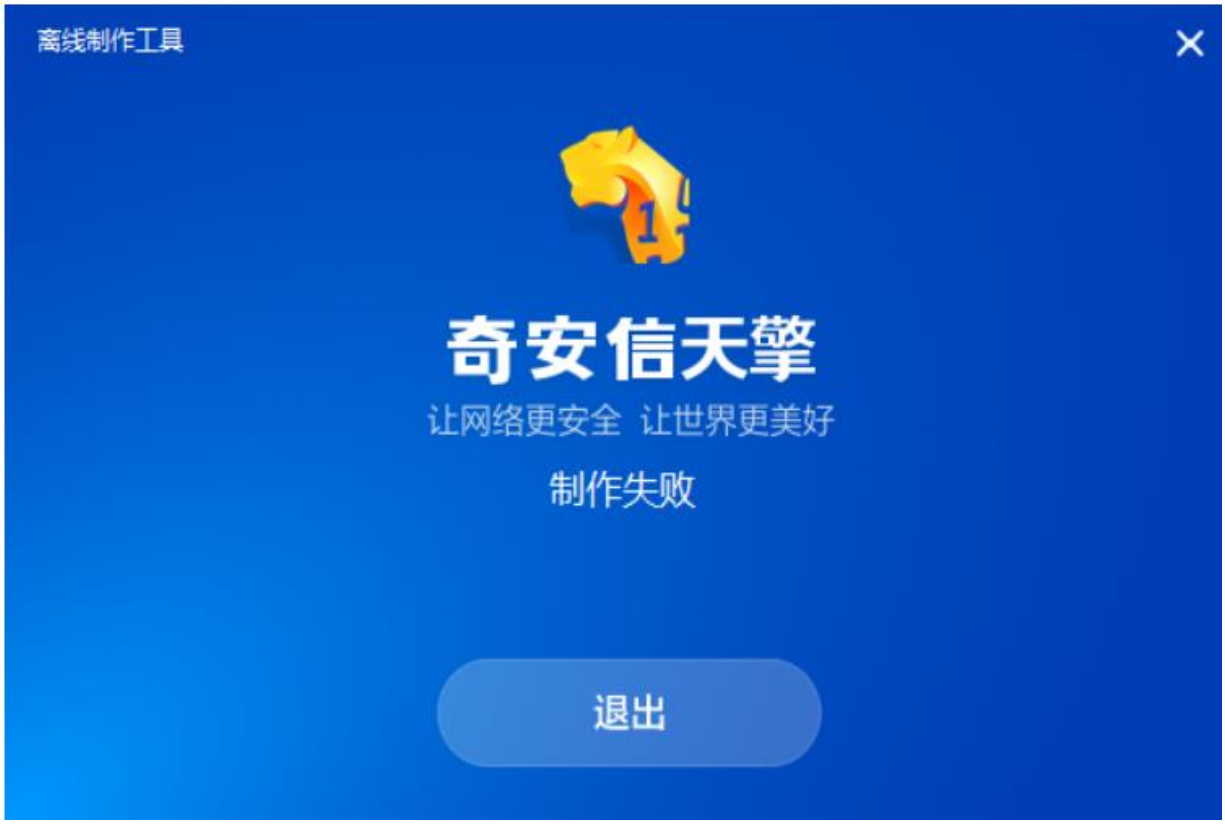
终端进行跃迁操作，安装了 V10 客户端基础模块后，还需要在【终端管理】>【基础策略】下为终端配置基础策略，勾选图标显示策略。



针对需要跃迁的终端下发跃迁任务，然后终端右下角才会显示托盘图标。

如果终端已安装其他安全卫士产品，需要进行卸载。如有残留右下角也不显示运行的图标，而服务端显示在线状态。

5.2.6 客户端在线安装提示“安装失败”，离线制作也提示“制作失败”。



解答：

a) 网络正常情况下更新服务端后，不可突然断开服务端网络。因为服务端升级时，并不会把真正的更新文件下载到管理系统，而仅仅是更新升级文件的索引。管理系统更新完毕，终端去执行升级时，根据服务端返回的索引，直接去公网下载对应的文件。

b) 管理中心不能继续连接公网，则需要使用离线工具进行同步数据，参考《管理员操作手册》。

c) 管理中心能继续连接公网，则放开管理中心到公网的网络即可。

5.2.7 服务器 IP 不变的情况下，将数据迁移到新的服务器怎么办？

解答：

IP 不变情况下使用如下方式进行服务器迁移：

1、直接将 Tianqing Endpoint Security 复制到另一台机器上， 保持目录不变。

2、老服务器上备份注册表路径

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\QAXTianqing

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\QAXTianqingsvc.exe

注册表编辑器，找到路径右键导出 reg 文件备份，将 reg 文件备份传到新服务器备用。

3、然后使用管理员权限打开 cmd， cd 到 Tianqing Endpoint Security 目录下，执行命令 QAXTianqingsvc.exe -i

4、新服务器恢复注册表 reg 文件备份 ，双击 reg 文件导入。

5、最后，启动天擎服务。

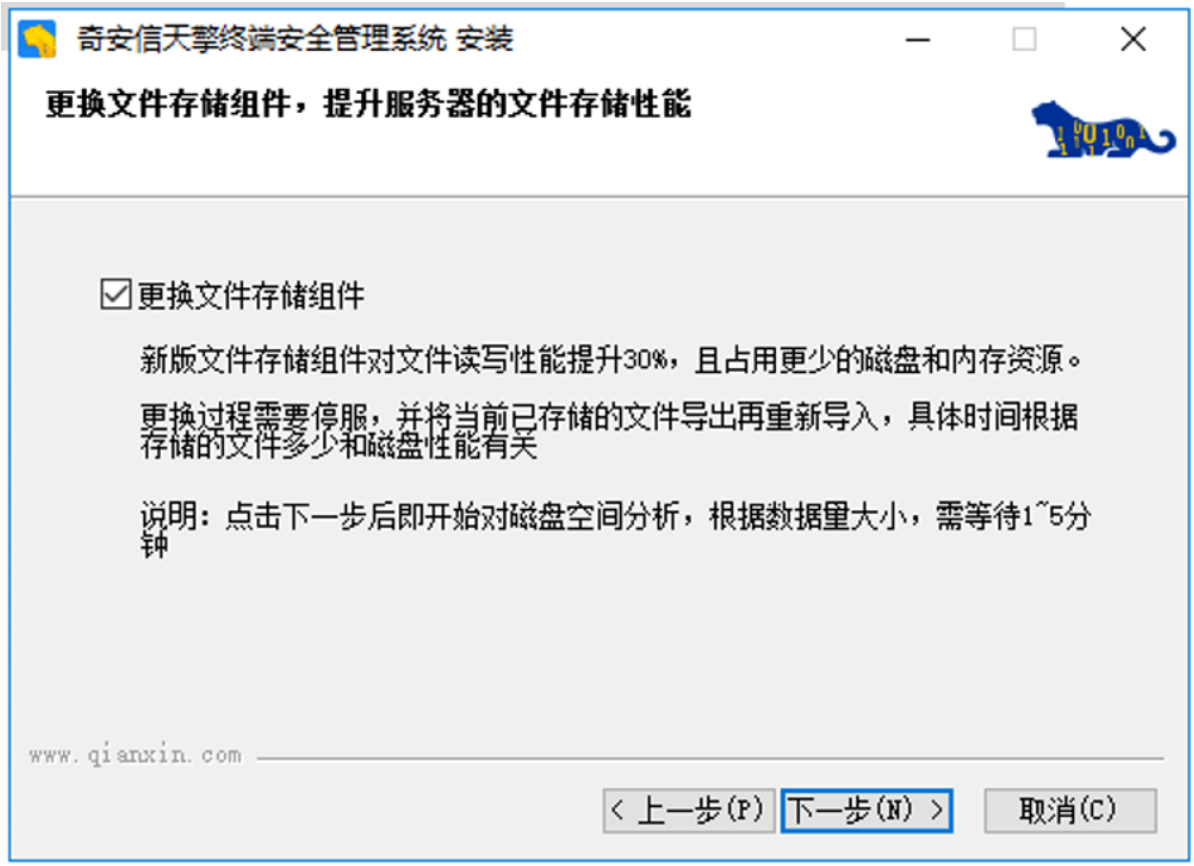
5.2.8 安装天擎以后使用 sysprep 封装镜像启动失败

参考 KB35249 解决

5.2.9 安装部署过程中，出现更换文件存储组件页面

解答：

覆盖安装 10.3.0.2000 以下的版本过程中，出现“更换文件存储组件”页面，是由于新版本的文件存储系统做了大幅优化调整，需要导出导入当前存储的数据，不会影响功能的使用。



5.2.9 服务器配置扩容到 8C16G 及以上后，需要手动处理

解答：

服务器配置从 4C8G 扩容到 8C16G 以上后，不会自动开启 noah web，需要手动开启，避免分区表创建失败导致无日志问题。

5.3 管理中心升级时，推荐的数据备份方案

1) 如果采用虚拟机部署，并且支持虚拟机镜像，推荐在升级前，停止天擎系统，对虚拟机进行镜像备份，备份完成后再升级天擎；

2) 使用天擎的备份恢复功能，在升级前先通过备份功能将全部数据备份到安全的存储空间中，备份完成后再升级天擎。如果升级出现异常，重新安装原版本的天擎，通过备份的数据进行恢复，目前备份恢复功能仅支持 10.3.0.4200 及以上版本，仅支持 Windows 单机部署的环境。

5.4 天擎服务运维中界面展示

1) 此特性当前仅支持 windows 单机部署；

2) 部署完成后，登陆管理中心时，若天擎各服务未全部启动，将进入“运维中”页面。所有进程全部启动后，将自动进入管理中心登录页面；

3) 在服务器重启、天擎重启等场景中，天擎各服务启动时，也会展示此“运维中”页面；

4) 部署完成后，天擎各服务启动需占用较长时间，请耐心等待。若“运维中”状态超过 10 分钟，可能部分服务无法自行启动，可通过下方的“跳过服务运维检测，直接登录”文字按钮进入管理中心，也可尝试重启服务器或联系客服。

5.5 级联部署常见问题

1)级联环境部署时，上级管理中心与下级管理中心之间不支持有 NAT 等转发设备。

2)级联部署环境升级时，需要先升级上级管理中心，再升级下级管理中心。否则容易出现日志数据丢失的情况。

3)Windows 单机部署作为级联上级的时候，需要将 kafka 端口暴露给下级管理中心，用于日志数据的同步，具体请参考 KB36974。

4)级联情况上下级服务器之间的心跳时间是 1 分钟（服务器时间相差不能超过 1 分钟）。

5.6 产品中心停止更新通知

产品中心即日起停止更新功能，只维护旧有功能。如需要进行设备绑定、许可证激活下载、解绑设备、更换设备请访问奇安信官网

（https://www.qianxin.com/applyfortrial），并按照操作指引进行操作。