

**360终端安全管理系统**

**部署及配置手册**

**适用版本：10.0.0.05100**

版权声明

©2021-2022 360公司 保留所有权利

本文档所有内容均为360公司独立完成，未经360公司作出明确书面许可，不得为任何目的、以任何形式或手段（包括电子、机械、复印、录音或其他形状）对本文档的任何部分进行复制、修改、存储、引入检索系统或者传播。

前言

本文档为360终端安全管理系统部署及配置手册，请在部署前详细阅读手册内容，并按照文档内容进行部署前准备和安装操作。

文档概述

本文档主要内容包含：

* 文档主要由产品概述、部署规划、安装前准备、可用性检查、安装部署、安装后检测以及FAQ等组成。
* 文档主要讲述如何部署360终端安全管理系统部署的环境要求、操作步骤、注意事项等内容。
* 通过阅读该文档可以完成360终端安全管理系统的部署和配置。

读者对象

本文档的主要阅读对象包括：

* 项目交付工程师
* 研发工程师
* 测试工程师
* 技术支持

通用约定

在本文中可能会出现下列文字，它们所代表的含义如下：

|  |  |
| --- | --- |
| 符号 | 说明 |
|  | 表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的后果。 |
|  | 表示是正文的附加信息，是对正文的强调和补充。 |

参考文档

无

术语解释

|  |  |
| --- | --- |
| 术语 | 说明 |
|  |  |
|  |  |
|  |  |

修订记录

| 版本 | 修订时间 | 编制者 | 审核者 | 修订内容 |
| --- | --- | --- | --- | --- |
| V2.0 | 2021-12-04 |  |  | 更新5100版本内容 |
| V2.1 | 2021-12-09 |  |  | 增加CDN部署内容 |
| V2.2 | 2021-12-10 |  |  | 增加db分离部署内容 |

目 录

[1. 产品概述 1](#_Toc92285881)

[2. 部署规划 2](#_Toc92285882)

[2.1. 安装部署总流程 2](#_Toc92285883)

[2.2. 测试环境部署规划 2](#_Toc92285884)

[2.2.1. 服务器配置 2](#_Toc92285885)

[2.3. 生产环境部署规划 3](#_Toc92285886)

[2.3.1. 服务器配置 3](#_Toc92285887)

[3. 安装前准备 4](#_Toc92285888)

[3.1. 硬件准备 4](#_Toc92285889)

[3.2. 软件准备 4](#_Toc92285890)

[3.3. 环境准备 4](#_Toc92285891)

[4. 可用性检查 5](#_Toc92285892)

[4.1. 硬件检查 5](#_Toc92285893)

[4.2. 软件检查 5](#_Toc92285894)

[4.3. 环境检查 5](#_Toc92285895)

[4.3.1. 硬件环境检查 5](#_Toc92285896)

[4.3.2. 网络环境检查 5](#_Toc92285897)

[5. 安装部署 6](#_Toc92285898)

[5.1. 管控中心部署-单级 6](#_Toc92285899)

[5.1.1. 安装须知 6](#_Toc92285900)

[5.1.2. 操作步骤 6](#_Toc92285901)

[5.1.3. 服务检查 7](#_Toc92285902)

[5.1.4. 检查与配置 8](#_Toc92285903)

[5.1.5. 支持https访问 9](#_Toc92285904)

[5.1.6. 服务端整体升级 9](#_Toc92285905)

[5.2. 管控中心部署-db/应用服务分离 9](#_Toc92285906)

[5.2.1. 安装须知 9](#_Toc92285907)

[5.2.2. 操作步骤 9](#_Toc92285908)

[5.2.3. 服务检查 12](#_Toc92285909)

[5.2.4. 检查与配置 12](#_Toc92285910)

[5.2.5. 支持https访问 12](#_Toc92285911)

[5.2.6. 服务端升级 13](#_Toc92285912)

[5.3. 管控中心部署-多级 14](#_Toc92285913)

[5.3.1. 安装须知 14](#_Toc92285914)

[5.3.2. 操作步骤 14](#_Toc92285915)

[5.3.3. 服务检查 16](#_Toc92285916)

[5.3.4. 检查与配置 17](#_Toc92285917)

[5.3.5. 支持https访问 17](#_Toc92285918)

[5.3.6. 级联关系建立 17](#_Toc92285919)

[5.4. 私有云安装 20](#_Toc92285920)

[5.4.1. 操作步骤 20](#_Toc92285921)

[5.5. 安装软件管家 23](#_Toc92285922)

[5.5.1. 操作步骤 23](#_Toc92285923)

[5.6. 部署CDN服务 24](#_Toc92285924)

[5.6.1. 操作步骤 24](#_Toc92285925)

[6. 安装后检查 26](#_Toc92285926)

[6.1. 检查Docker服务 26](#_Toc92285927)

[6.2. 检查数据库 26](#_Toc92285928)

[6.3. 服务与配置检查 27](#_Toc92285929)

[6.4. 授权证书配置 27](#_Toc92285930)

[6.4.1. 管控中心首页，更新授权证书 28](#_Toc92285931)

[6.4.2. 授权证书获取-申请序列号 29](#_Toc92285932)

[6.4.3. 生成授权证书 29](#_Toc92285933)

[6.4.4. 管控中心导入证书 29](#_Toc92285934)

[7. FAQ 30](#_Toc92285935)

[7.1. 客户端安装 30](#_Toc92285936)

[7.1.1. 手动安装客户端 30](#_Toc92285937)

[7.2. 客户端服务端通讯 30](#_Toc92285938)

[7.2.1. 客户端与管理后台 30](#_Toc92285939)

[7.3. 服务端下发杀毒命令 33](#_Toc92285940)

[7.4. 客户端数据上报 33](#_Toc92285941)

[7.4.1. 客户端杀毒上报数据 33](#_Toc92285942)

[7.4.2. 客户端隔离区上报数据 34](#_Toc92285943)

[7.4.3. 客户端信任区上报数据 34](#_Toc92285944)

[7.4.4. 客户端中心地址迁移 34](#_Toc92285945)

[7.5. 漏洞 34](#_Toc92285946)

[7.6. 网络环境 35](#_Toc92285947)

[7.6.1. 外网环境 35](#_Toc92285948)

[7.6.2. 内网环境 35](#_Toc92285949)

[7.6.3. 内网外网网段ip隔离环境 36](#_Toc92285950)

[7.6.4. 管理后台命令下发 36](#_Toc92285951)

[7.7. 授权文件 37](#_Toc92285952)

[7.8. 软件更新 37](#_Toc92285953)

[7.8.1. 管理后台更新 37](#_Toc92285954)

[7.8.2. 客户端更新 37](#_Toc92285955)

[7.8.3. 病毒库漏洞库更新 37](#_Toc92285956)

[7.8.4. 代理服务器 38](#_Toc92285957)

[7.8.5. 安全设置 38](#_Toc92285958)

[7.9. 软件管家 38](#_Toc92285959)

[7.10. 部署相关 38](#_Toc92285960)

[7.10.1. 软硬件环境 38](#_Toc92285961)

[7.10.2. 网络相关 39](#_Toc92285962)

[7.10.3. 客户端相关 40](#_Toc92285963)

[7.10.4. 服务端 41](#_Toc92285964)

[7.10.5. 私云部署 42](#_Toc92285965)

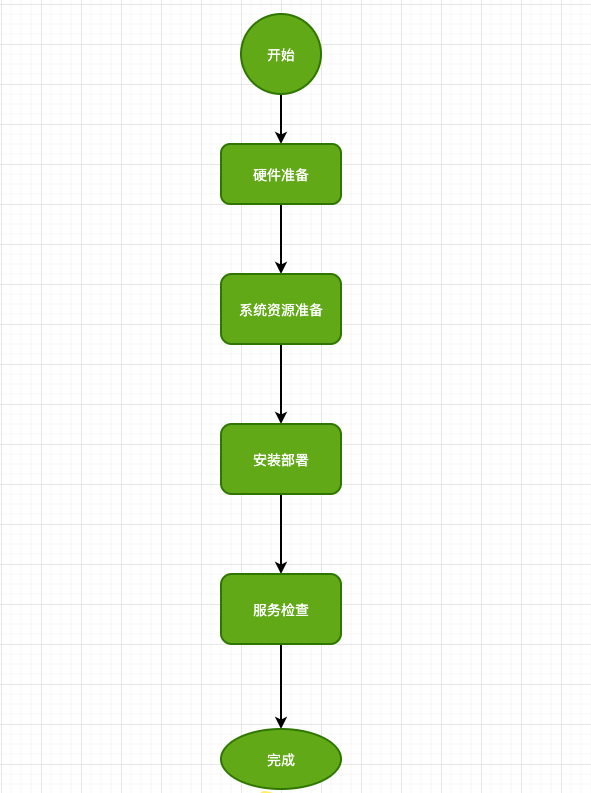
# 产品概述

360终端安全管理系统是360集团面向政府、军队、金融、制造业、医疗、教育等大型企事业单位推出的以安全防御为核心、以安全策略管控为重点、以自动化运维管理为支撑、以可靠服务为保障的终端安全解决方案。

360终端安全管理系统分为管理控制台和客户端程序两大部分，客户端部分是一个独立的本地可执行程序，执行管理员下发的任务和策略。管理控制台部分采用B/S架构，完成管理员的管理需求。

# 部署规划

## 安装部署总流程



## 测试环境部署规划

### 服务器配置

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务器 | 准备项 | 需求 |
| 1 | 管理中心 | 硬件配置 | 5000点以下终端规模，管控中心服务器配置建议：  CPU：8C；内存：16G；硬盘：1T；网卡：千兆网卡；/data目录需要大于500G，部署docker服务。  *5000点以上终端规模，管控中心服务器的配置请联系产品经理* |
| 2 | 操作系统 | 系统版本：Centos7.6；硬盘分区：/data 500G |
| 3 | IP地址 | 固定IP地址 |
| 4 | 开放端口 | 80、81、8080、8081、8082，36093,36094,36444 |

## 生产环境部署规划

### 服务器配置

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务器 | 准备项 | 需求 |
| 1 | 管理中心 | 硬件配置 | 5000点以下终端规模，管控中心服务器配置建议：  CPU：8C；内存：16G；硬盘：1T；网卡：千兆网卡；/data目录需要大于500G，部署docker服务。  *5000点以上终端规模，管控中心服务器的配置请联系产品经理* |
| 2 | 操作系统 | 系统版本：Centos7.6；硬盘分区：/data 500G |
| 3 | IP地址 | 固定IP地址 |
| 4 | 开放端口 | 80、81、8080、8081、8082，36093,36094,36444 |

# 安装前准备

## 硬件准备

|  |  |
| --- | --- |
| 序号 | 组件 |
| 1 | 机柜 |
| 2 | 硬件服务器 |

## 软件准备

|  |  |
| --- | --- |
| 序号 | 软件包 |
| 1 | 360终端安全管理系统安装包 |

## 环境准备

* 系统版本要求：限定操作系统为Centos 7.6，以及以上版本操作系统
* 网络环境：确保安装管控中心服务器和终端之间的网络畅通

# 可用性检查

## 硬件检查

|  |  |  |
| --- | --- | --- |
| 检查项 | 检查步骤 | 检查结果 |
| 机柜 | 检查机柜外观与布线 | 外观无异常，布线规范 |
| 服务器 | 服务器通电开机 | 可正常开机 |

## 软件检查

|  |  |  |
| --- | --- | --- |
| 检查项 | 检查步骤 | 检查结果 |
| 360终端安全管理系统安装包 | 检查安装包 | 版本信息与文件格式与预期一致 |

## 环境检查

### 硬件环境检查

|  |  |  |
| --- | --- | --- |
| 检查项 | 检查步骤 | 检查结果 |
| 操作系统 | 查看操作系统版本 | Centos 7.6，以及以上版本操作系统 |
| CPU | 检查CPU | 8C及以上 |
| 内存 | 检查内存 | 16G及以上 |
| 硬盘 | 检查硬盘 | 1T及以上 |
| 网卡 | 检查网卡 | 千兆网卡 |
| /data目录 | 检查/data目录 | 大于500G |
| IP地址 | 检查IP | 固定IP地址 |

### 网络环境检查

|  |  |  |
| --- | --- | --- |
| 检查项 | 检查步骤 | 检查结果 |
| 目的IP：服务器IP  端口：80、81、8080、8081、8082，36093,36094,36444 | 执行命令：telnet 服务器IP 端口号 | 端口开放，网络畅通 |

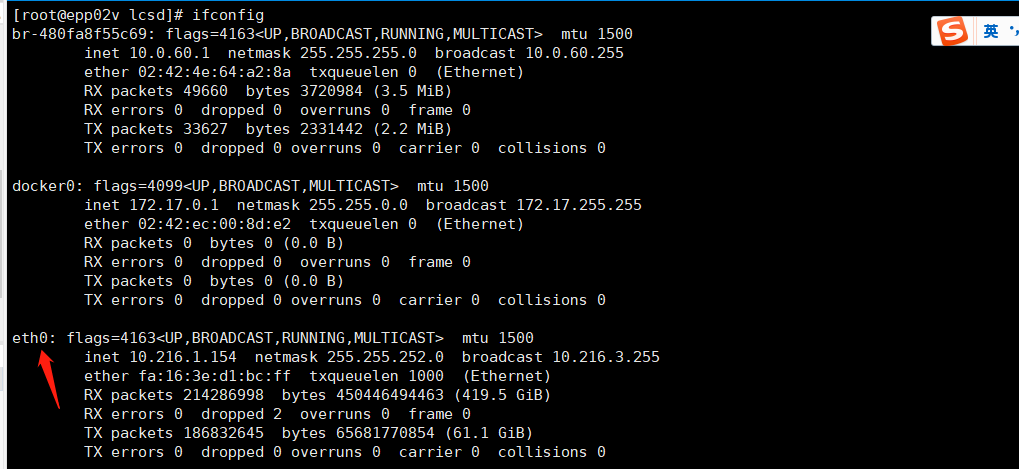
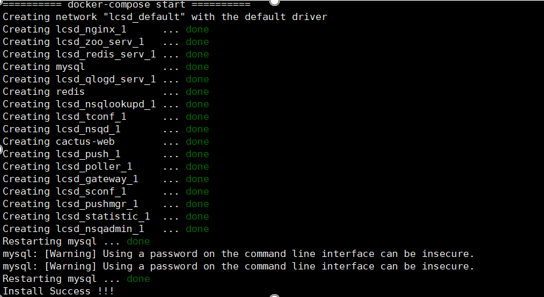
# 安装部署

## 管控中心部署-单级

### 安装须知

管控中心部署为一键式部署，执行部署过程中，如果发现出现异常，则会停止安装并给出提示信息，请根据提示信息解决或参考本文档FAQ章节内容进行处理。

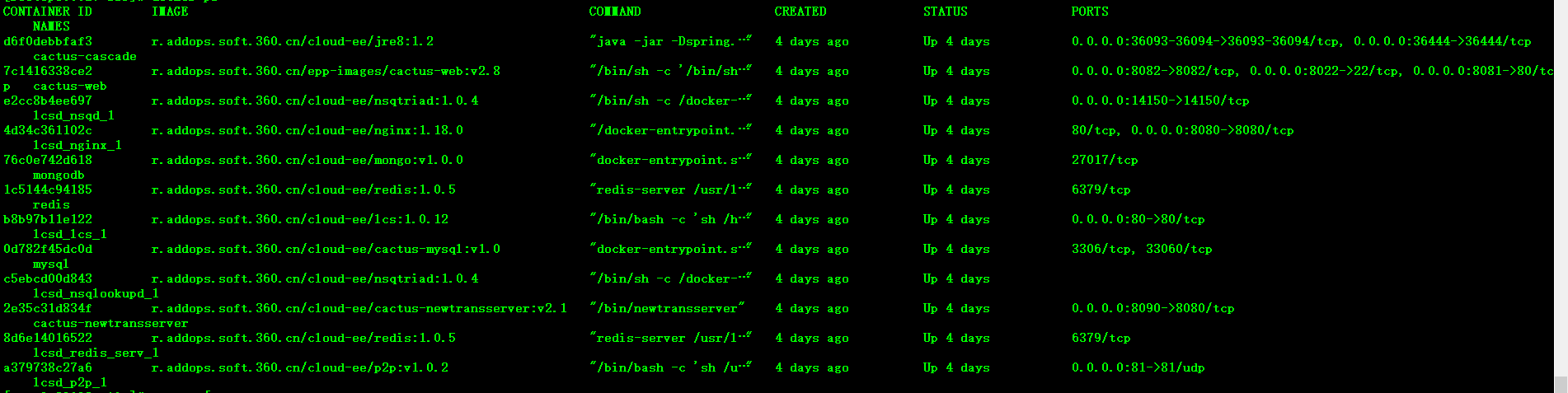
### 操作步骤

1. 获取到360EPP\_v10.0.0.05100.tar.gz压缩包
2. 解压缩360EPP\_v10.0.0.05100.tar.gz并进入目录
3. 以root权限执行安装 sh install.sh 网卡名， #注：查看网卡名称用ifconfig命令查看，此参数是将对外提供网络服务的网卡名称，如eth0  
   
4. 安装成功时，可见“Install Success !!!”提示，如果失败，则会有相应提示  
   
5. 多场景部署方式均可支持
6. Sh install.sh –n eth0
7. Sh install.sh –I 192.168.0.2(现场实际ip)
8. Sh install.sh –n eth0 –t 10080 -h 18080 –w 18081
9. 参数说明：-n 网卡名 ；-t tcp端口 -h http端口 –w web端口
10. 如不指定端口 则默认tcp为80端口 http为8080端口 web端口为8081

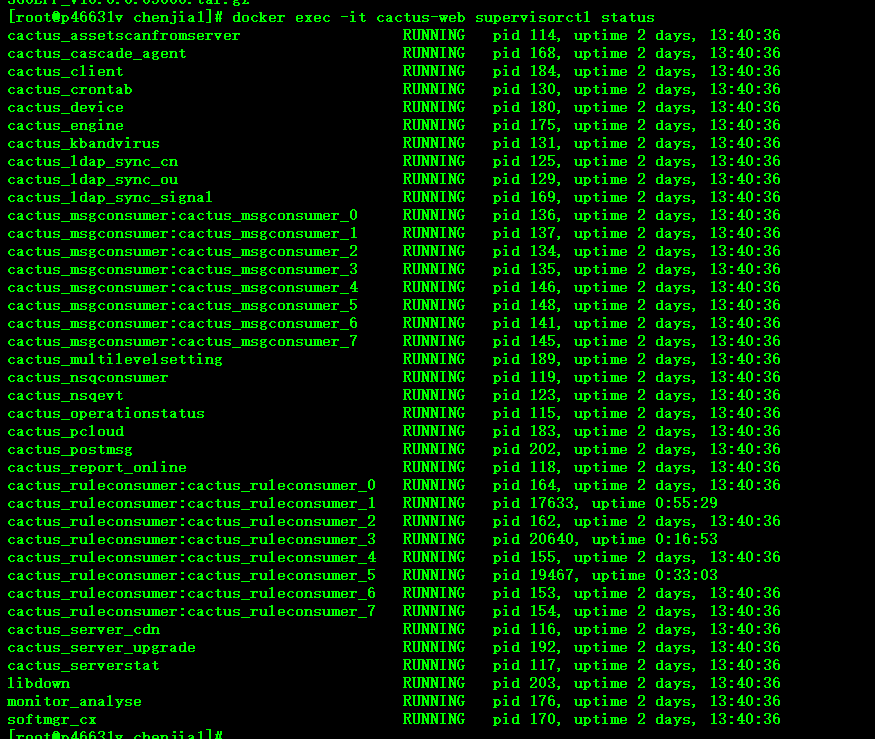
### 服务检查

提供一些方法以确认服务各项流程正常

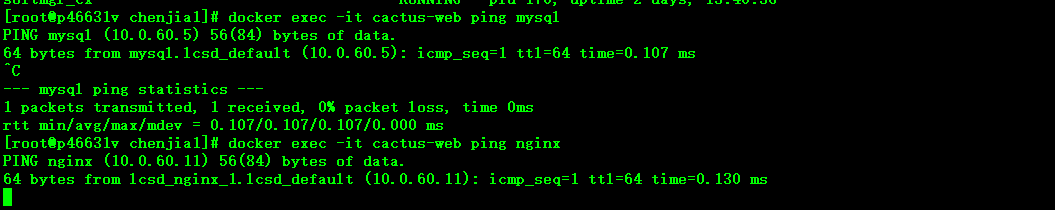
Docker ps docker容器情况 都up即可。



docker exec -it cactus-web supervisorctl status 进程启动情况 均running即可。



容器内检查：主要看mysql 以及nginx 跟web是否互通。



### 检查与配置

通过浏览器（要求Chrome76版本及以上）访问 http://{IP}:8081/dist/，应该出现登录界面（用户名: eppadmin, 密码: pass-abcd-1234）。登录成功后，左侧有功能菜单，点击菜单 【终端管理】->【安全设置】，选择 【基本设置】，在 "升级服务器" 对应的输入框中输入 "服务器IP:80"，然后点击对应的设置按钮，完成基本配置。

### 支持https访问

通过浏览器（要求Chrome76版本及以上）访问 https://{IP}:443/dist/，应该出现登录界面（用户名: eppadmin, 密码: pass-abcd-1234）。登录成功后，左侧有功能菜单，点击菜单 【终端管理】->【安全设置】，选择 【基本设置】，在 "升级服务器" 对应的输入框中输入 "服务器IP:80"，然后点击对应的设置按钮，完成基本配置。

### 服务端整体升级

直接执行发布的升级sh脚本即可完成升级。

## 管控中心部署-db/应用服务分离

### 安装须知

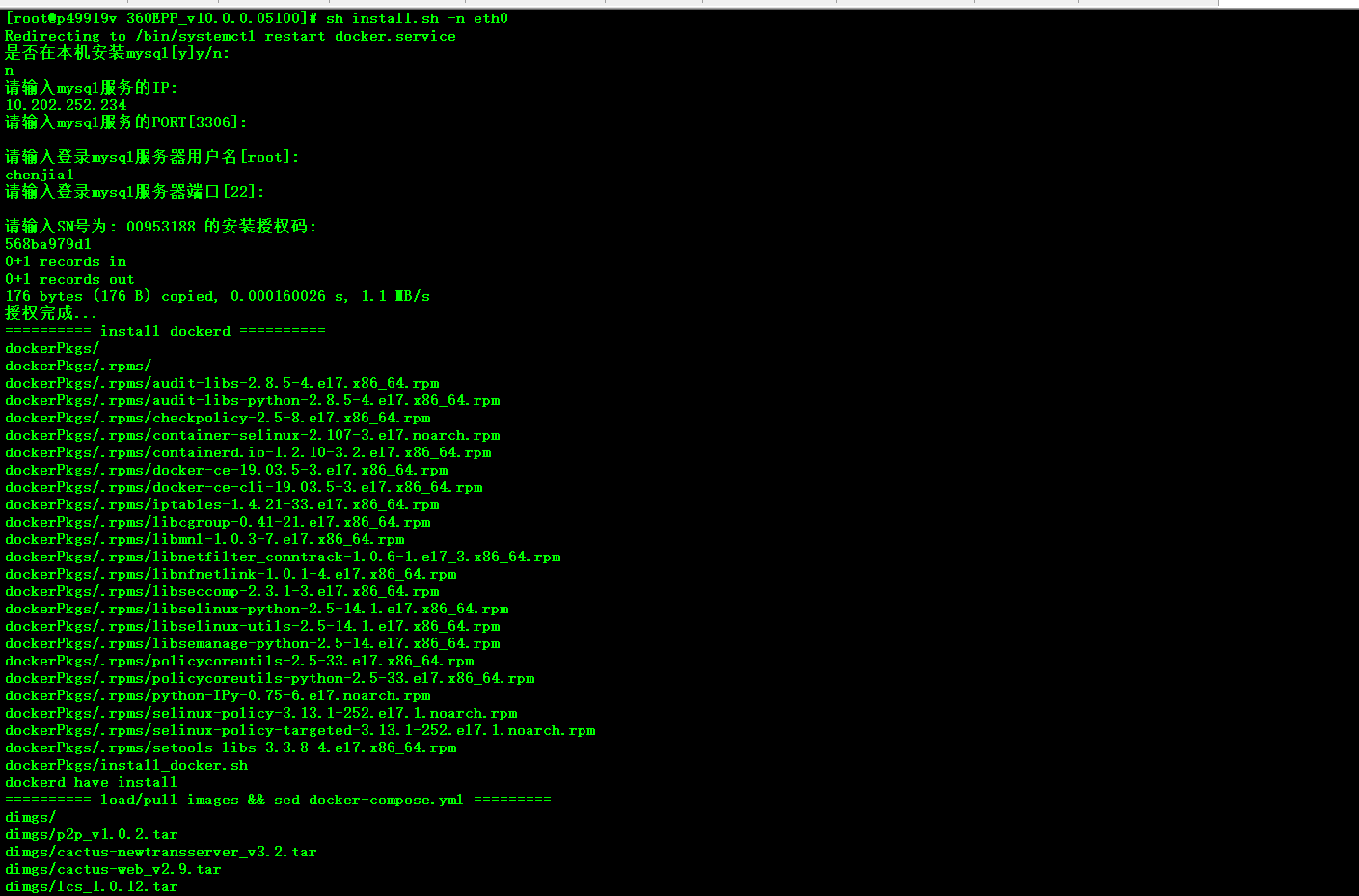
管控中心部署为一键式部署，执行部署过程中，如果发现出现异常，则会停止安装并给出提示信息，请根据提示信息解决或参考本文档第七章FAQ进行处理。

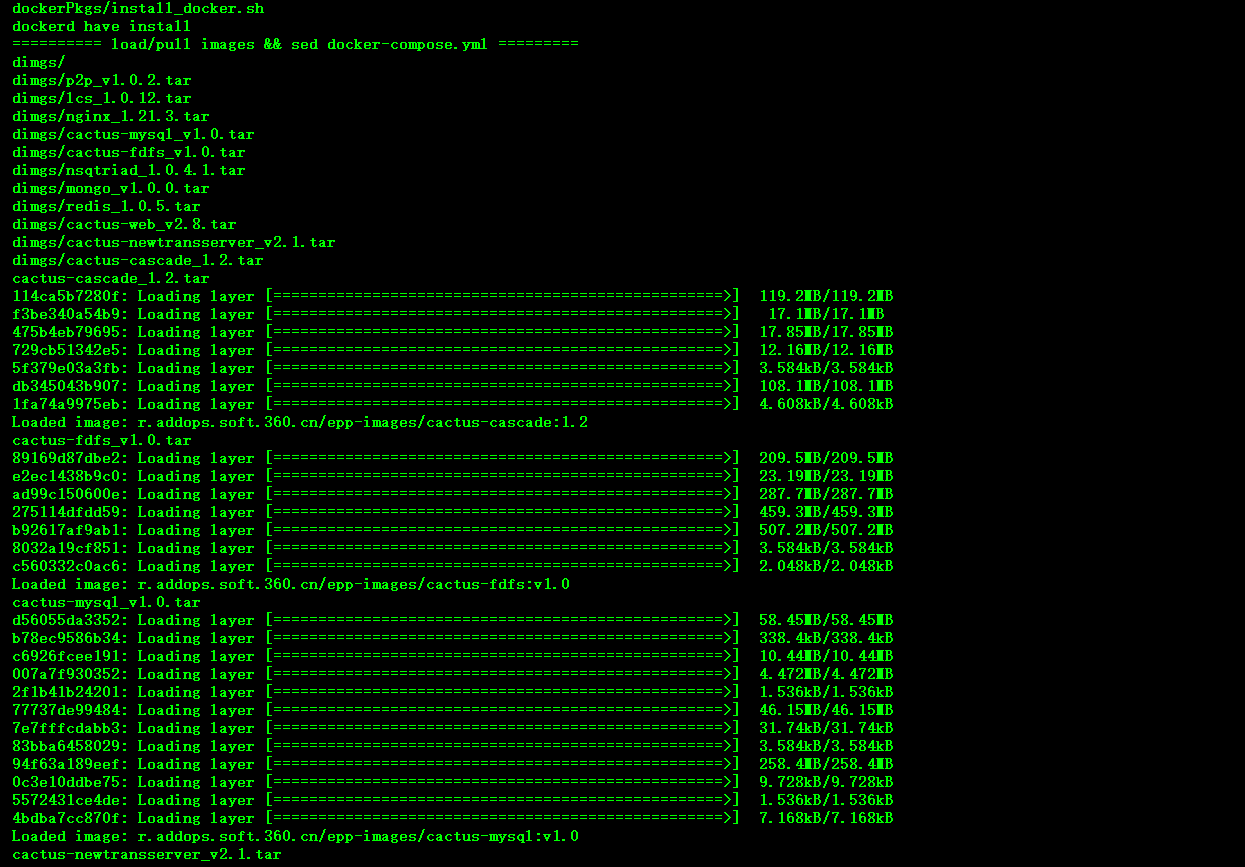
### 操作步骤

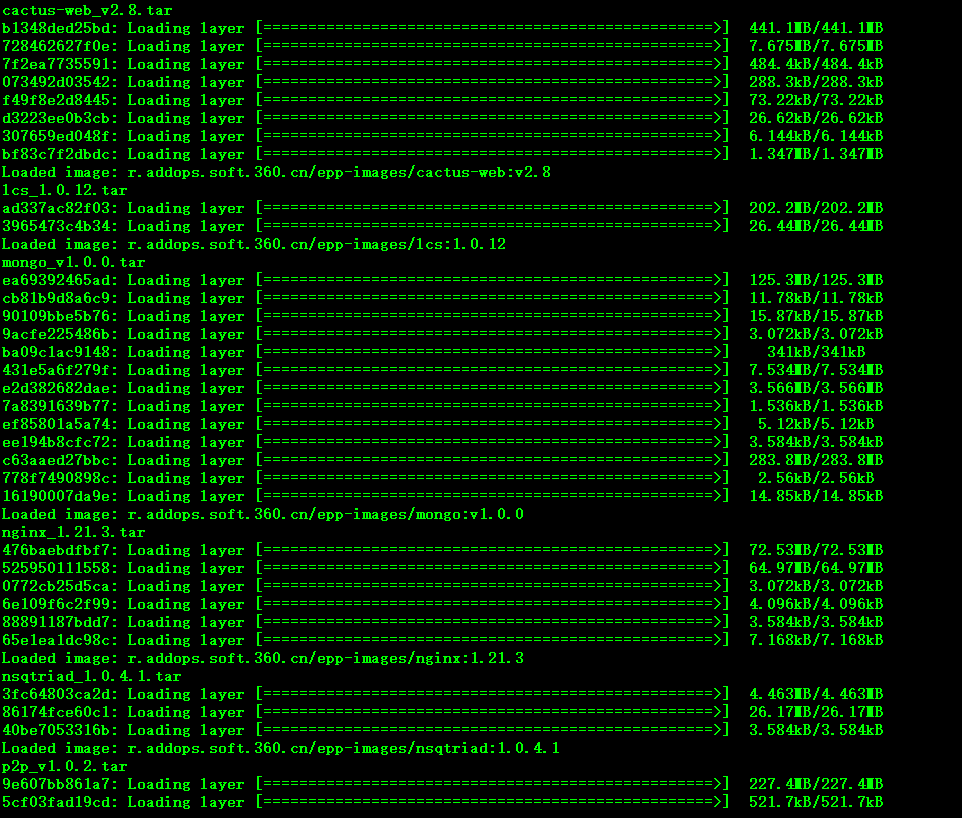
1. 获取到360EPP\_v10.0.0.05100.tar.gz压缩包
2. 解压缩360EPP\_v10.0.0.05100.tar.gz并进入目录
3. Db服务器与应用服务器互通
4. 获取db服务器ip
5. 执行部署

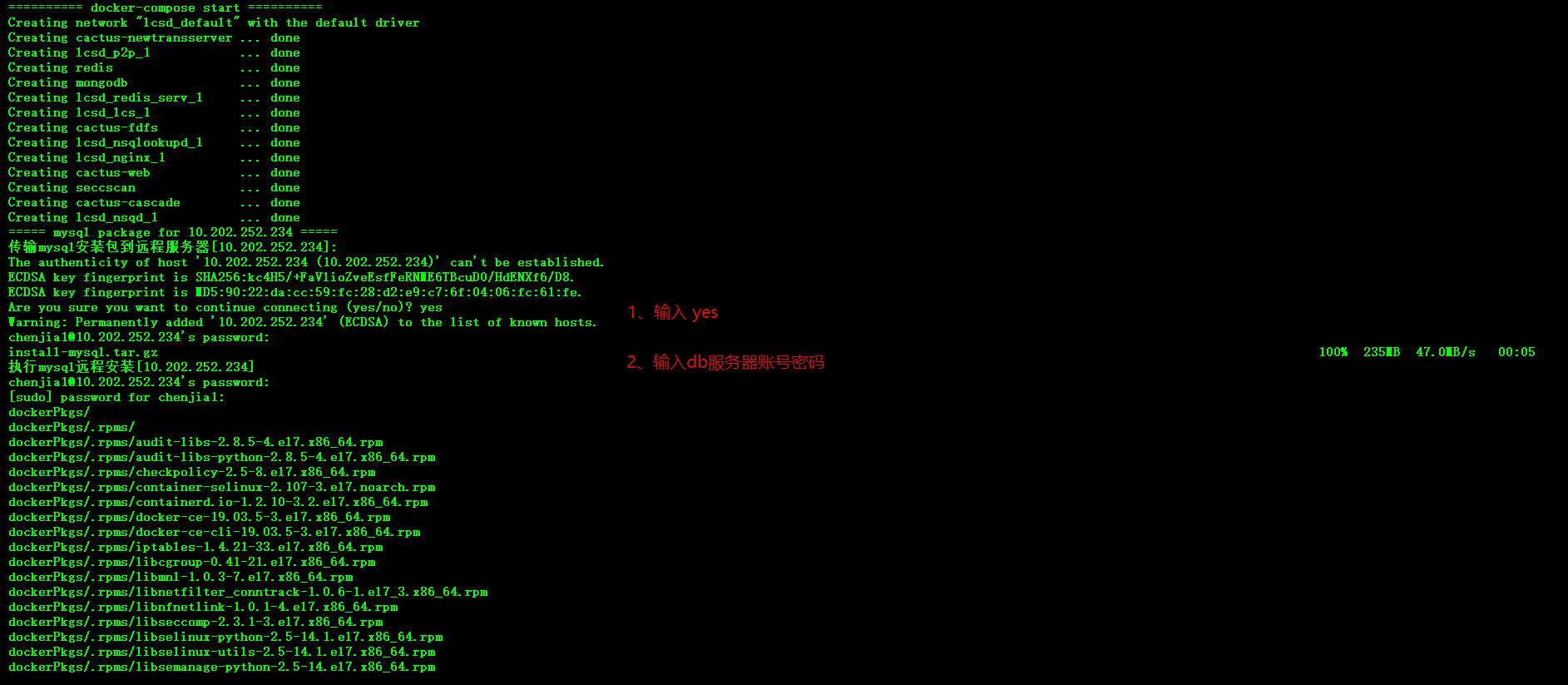
以root权限执行安装 sh install.sh 网卡名， #注：查看网卡名称用ifconfig命令查看，此参数是将对外提供网络服务的网卡名称，如eth0

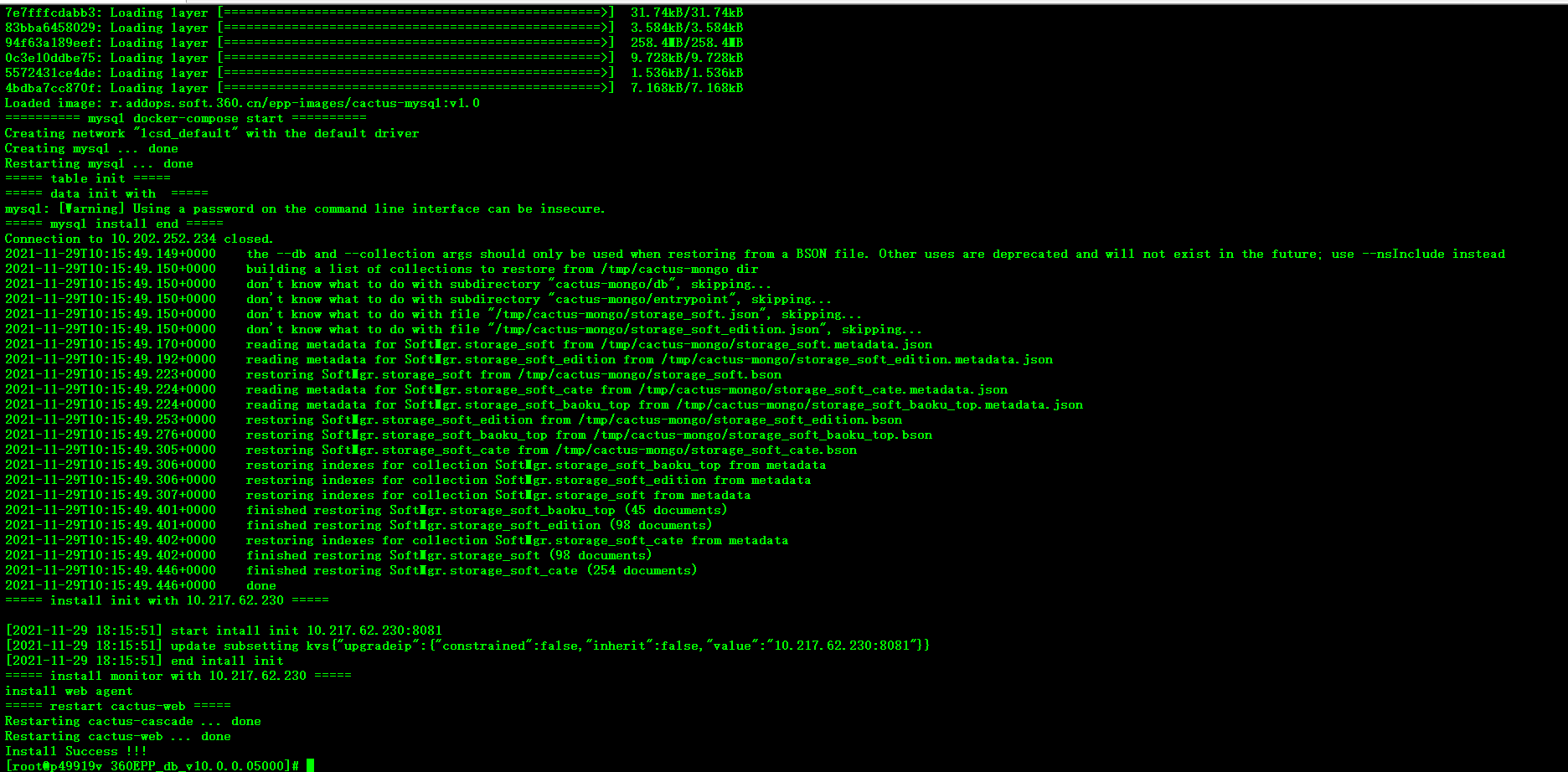
1. 执行部署









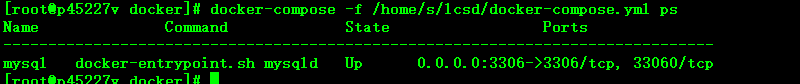


安装结束。

### 服务检查

要用服务检查，参考【安装部署-服务检查】章节内容。

增加db服务检查：





状态“Up”即为成功。

### 检查与配置

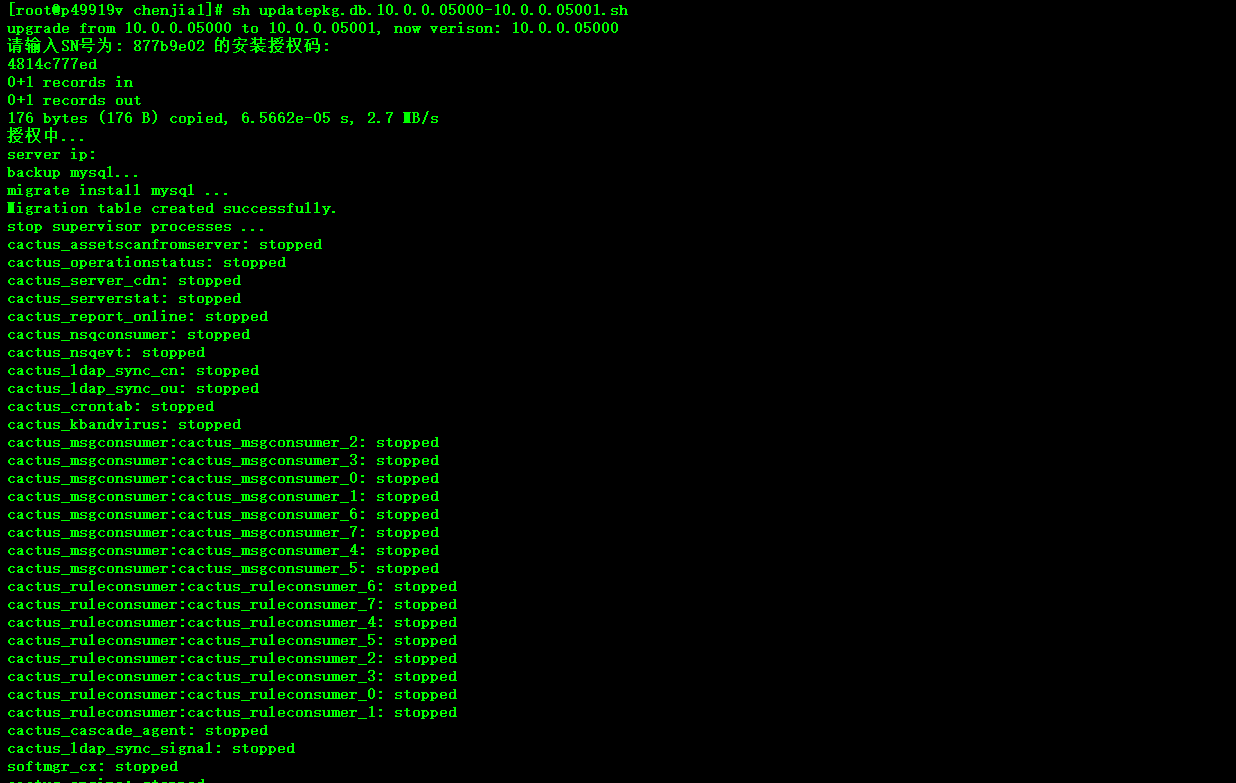
通过浏览器（要求Chrome76版本及以上）访问 http://{IP}:8081/dist/，应该出现登录界面（用户名: eppadmin, 密码: pass-abcd-1234）。登录成功后，左侧有功能菜单，点击菜单 【终端管理】->【安全设置】，选择 【基本设置】，在 "升级服务器" 对应的输入框中输入 "服务器IP:80"，然后点击对应的设置按钮，完成基本配置。

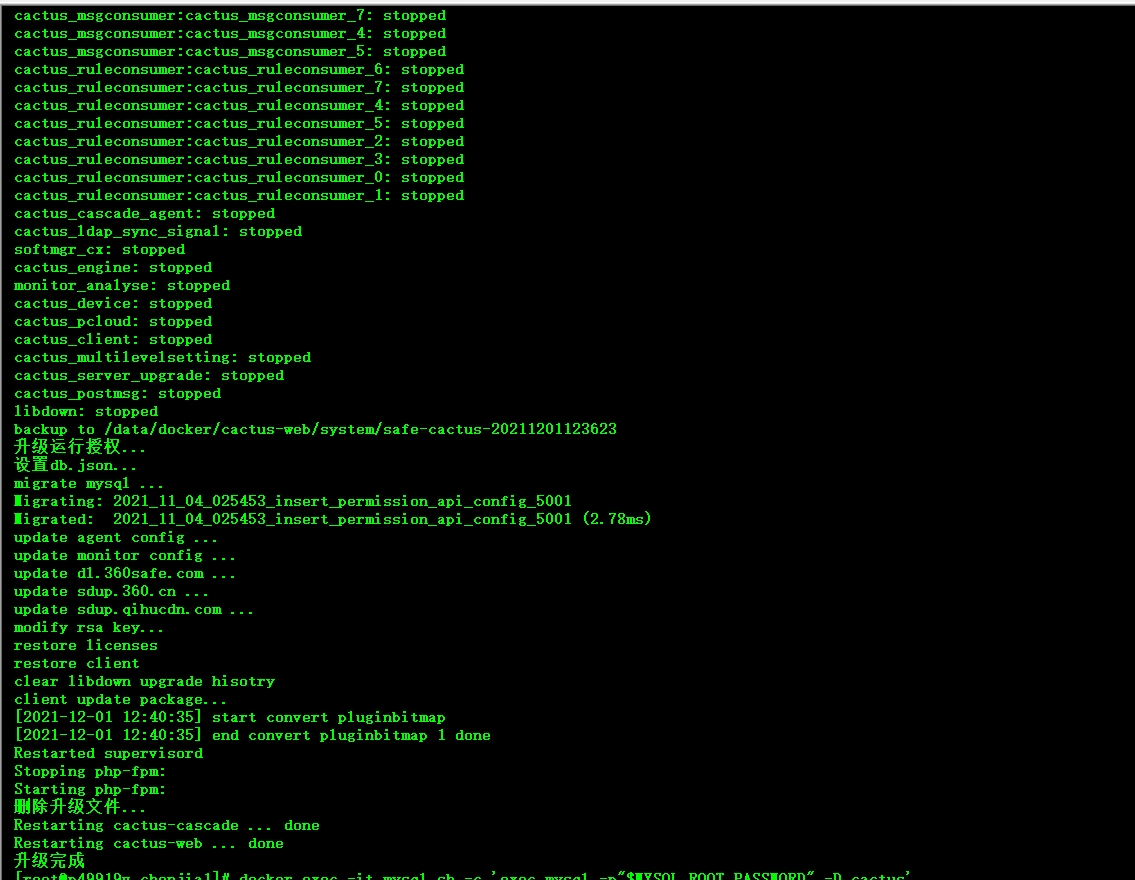
### 支持https访问

通过浏览器（要求Chrome76版本及以上）访问 https://{IP}:443/dist/，应该出现登录界面（用户名: eppadmin, 密码: pass-abcd-1234）。登录成功后，左侧有功能菜单，点击菜单 【终端管理】->【安全设置】，选择 【基本设置】，在 "升级服务器" 对应的输入框中输入 "服务器IP:80"，然后点击对应的设置按钮，完成基本配置。

### 服务端升级

在应用服务所在的机器执行升级脚本完成升级即可。例：应用部署在A服务器，mysql部署在B服务器，则在A服务器执行升级脚本即可：





## 管控中心部署-多级

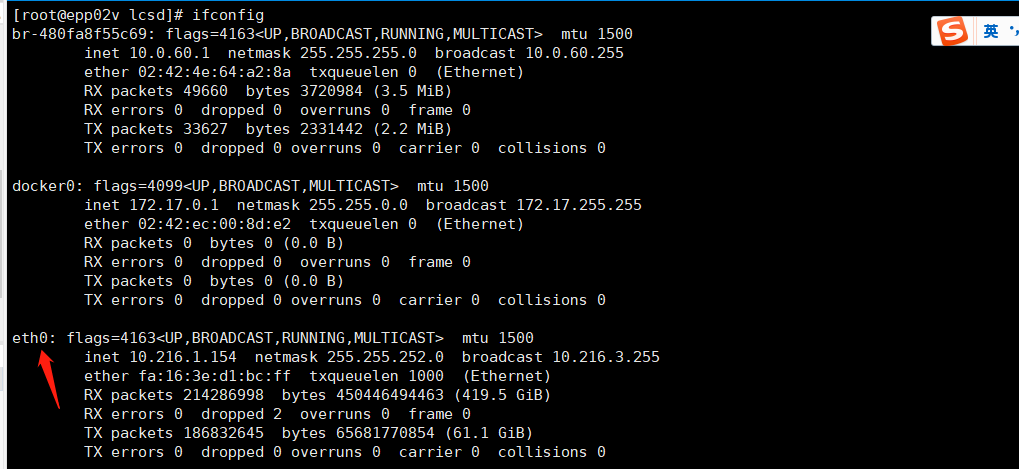
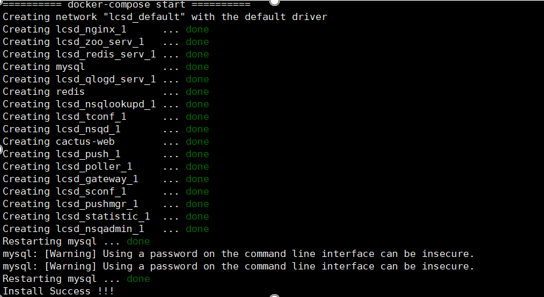
### 安装须知

管控中心部署为一键式部署，执行部署过程中，如果发现出现异常，则会停止安装并给出提示信息，请根据提示信息解决或参考本文档第七章FAQ进行处理。

多级环境部署参考单机部署，部署完成之后各单机服务器建立上下级级联关系。

多级环境需要确保各级中心服务端版本保持一致，另外机器配置参考单机配置即可。

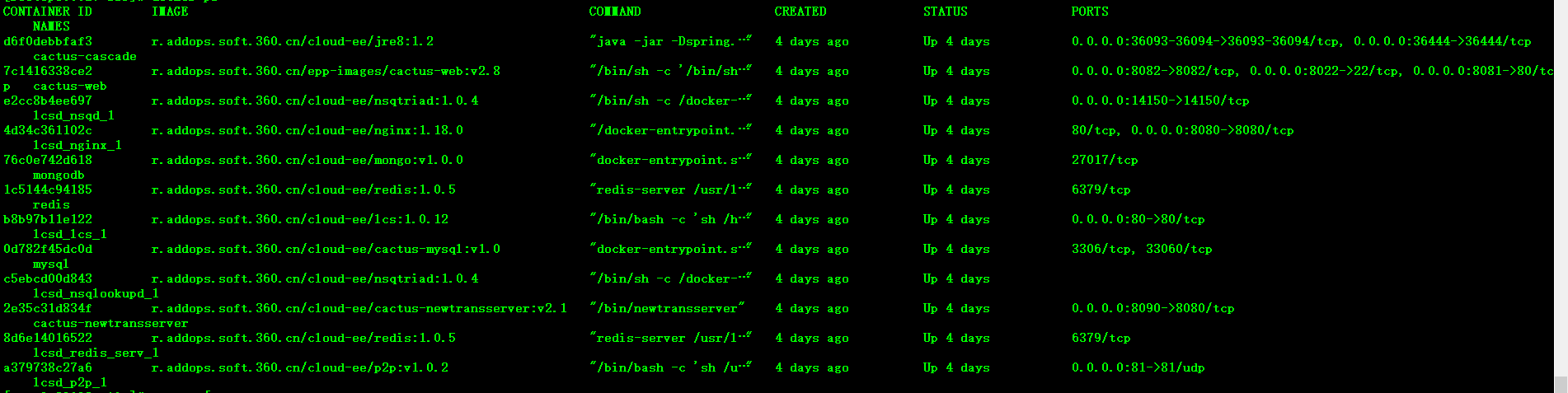
### 操作步骤

1. 获取到360EPP\_v10.0.0.05100.tar.gz压缩包
2. 解压缩360EPP\_v10.0.0.05100.tar.gz并进入目录
3. 以root权限执行安装 sh install.sh 网卡名， #注：查看网卡名称用ifconfig命令查看，此参数是将对外提供网络服务的网卡名称，如eth0  
   
4. 安装成功时，可见“Install Success !!!”提示，如果失败，则会有相应提示  
   
5. 多场景部署方式均可支持
6. Sh install.sh –n eth0
7. Sh install.sh –I 192.168.0.2(现场实际ip)
8. Sh install.sh –n eth0 –t 10080 -h 18080 –w 18081
9. 参数说明：-n 网卡名 ；-t tcp端口 -h http端口 –w web端口
10. 如不指定端口 则默认tcp为80端口 http为8080端口 web端口为8081

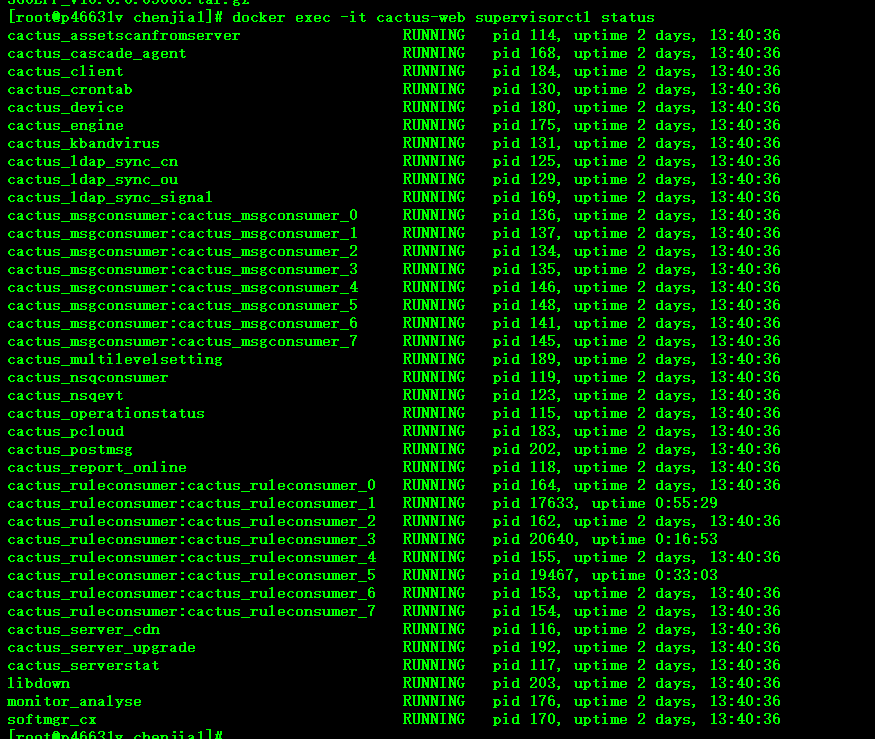
### 服务检查

提供一些方法以确认服务各项流程正常。

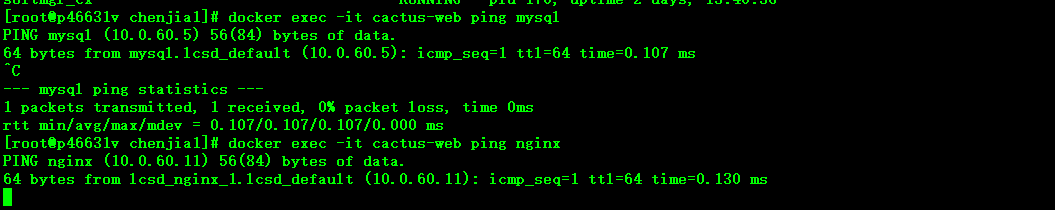
Docker ps docker容器情况 都up即可：



docker exec -it cactus-web supervisorctl status 进程启动情况 均running即可：



容器内检查：主要看mysql 以及nginx 跟web是否互通：



### 检查与配置

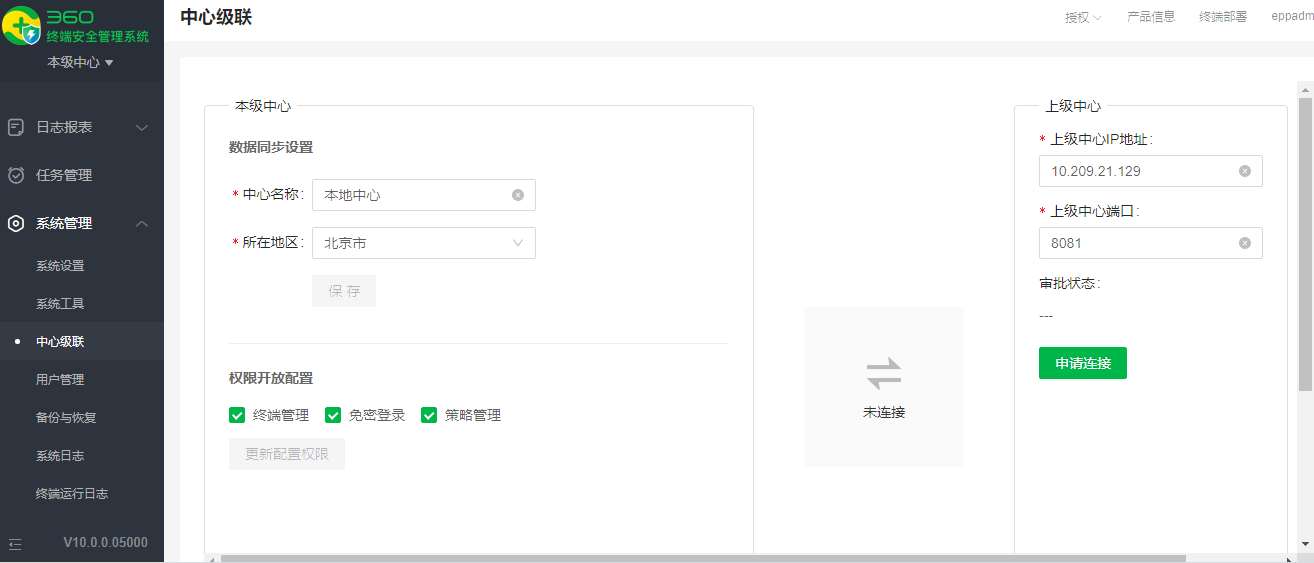
通过浏览器（要求Chrome76版本及以上）访问 http://{IP}:8081/dist/，应该出现登录界面（用户名: eppadmin, 密码: pass-abcd-1234）。登录成功后，左侧有功能菜单，点击菜单 【终端管理】->【安全设置】，选择 【基本设置】，在 "升级服务器" 对应的输入框中输入 "服务器IP:80"，然后点击对应的设置按钮，完成基本配置。

### 支持https访问

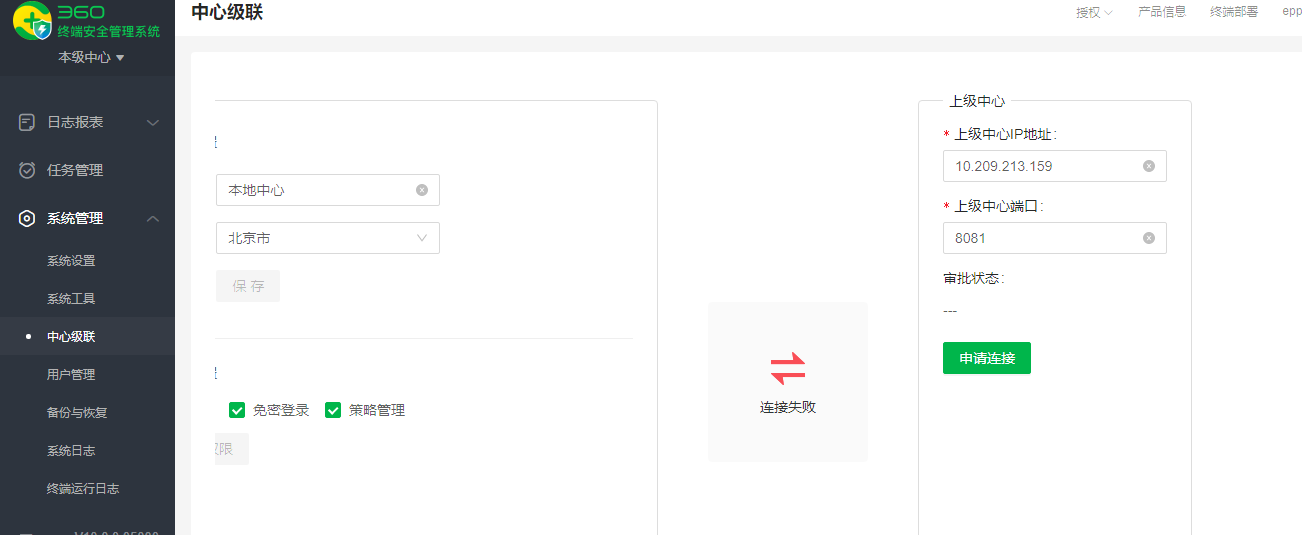
通过浏览器（要求Chrome76版本及以上）访问 https://{IP}:443/dist/，应该出现登录界面（用户名: eppadmin, 密码: pass-abcd-1234）。登录成功后，左侧有功能菜单，点击菜单 【终端管理】->【安全设置】，选择 【基本设置】，在 "升级服务器" 对应的输入框中输入 "服务器IP:80"，然后点击对应的设置按钮，完成基本配置。

### 级联关系建立

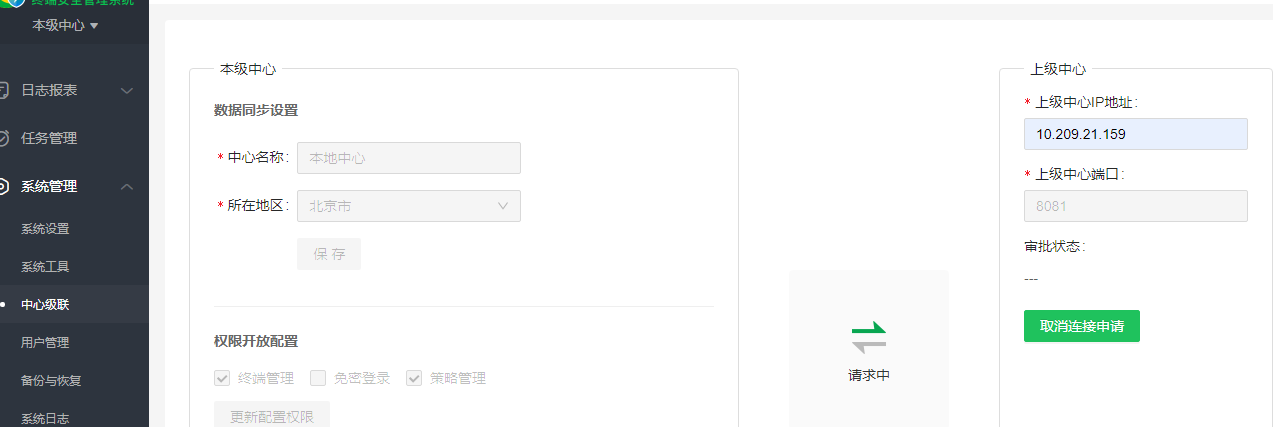
访问web管控中心，选择左侧菜单栏 系统管理-》中心级联，输入上级中心ip以及上级中心代理端口，点击申请连接：

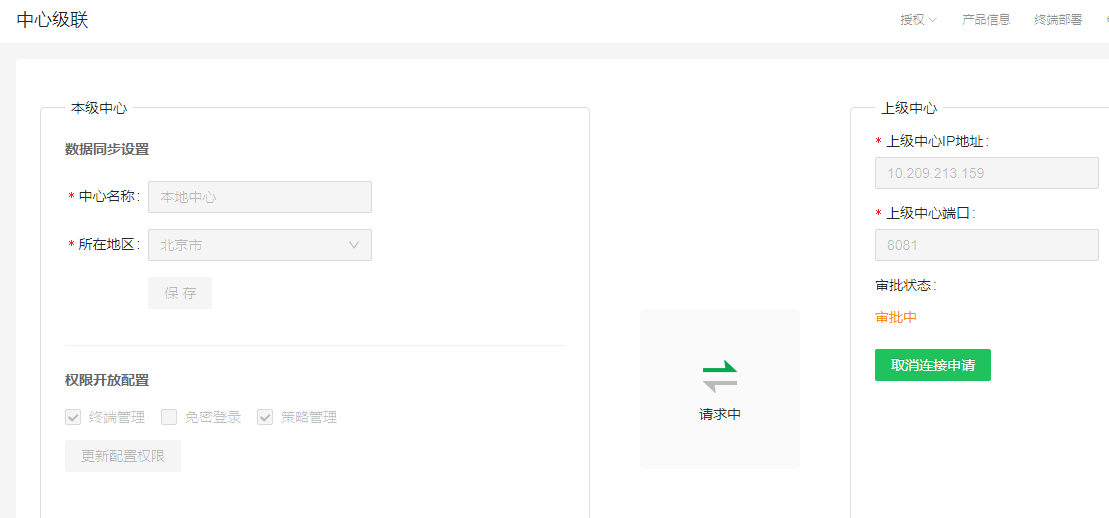


中心之间通讯不通会返回连接状态为失败：

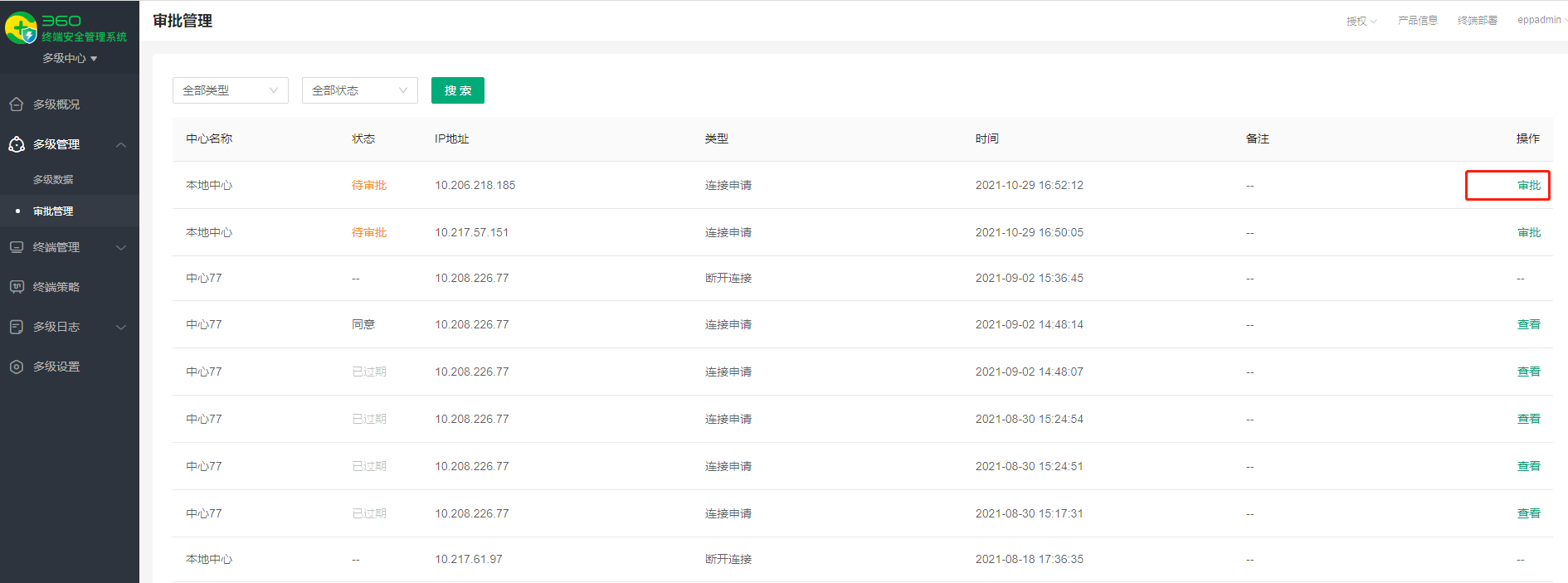


中心链接成功，则提示请求中：



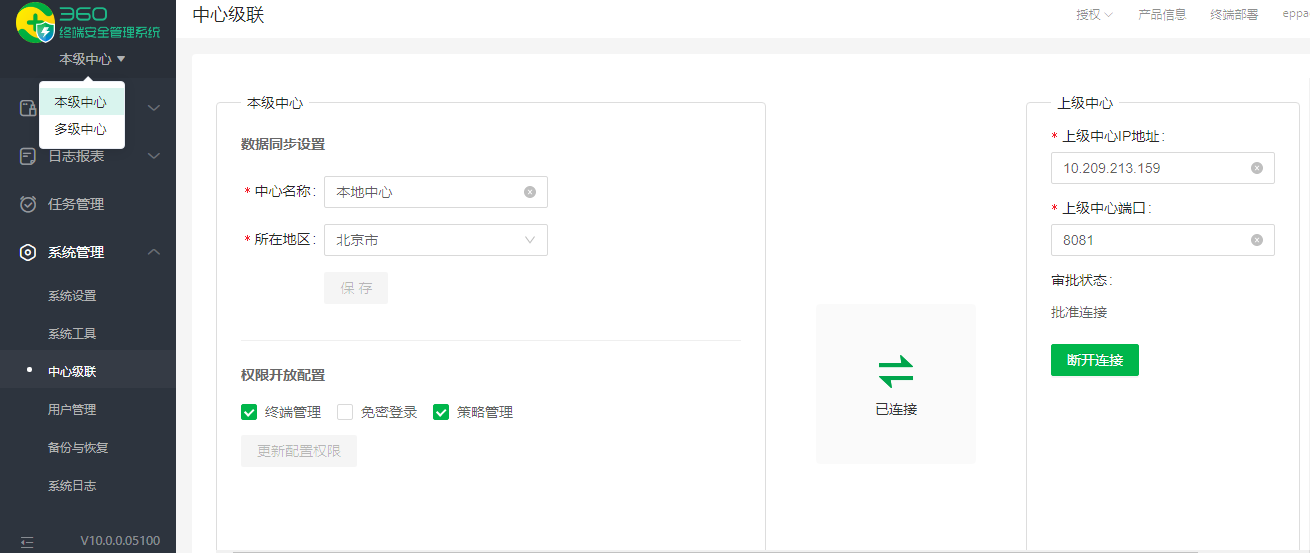


登录上一级管控中心进行级联审批 多级中心-多级管理-》审批管理：





审批拒绝则不建立上下级，审批通过则完成上下级关系建立：

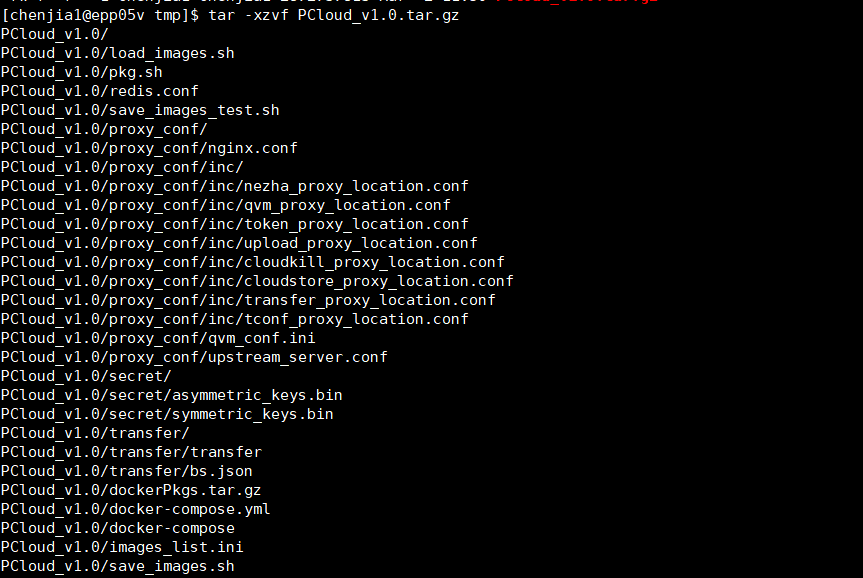
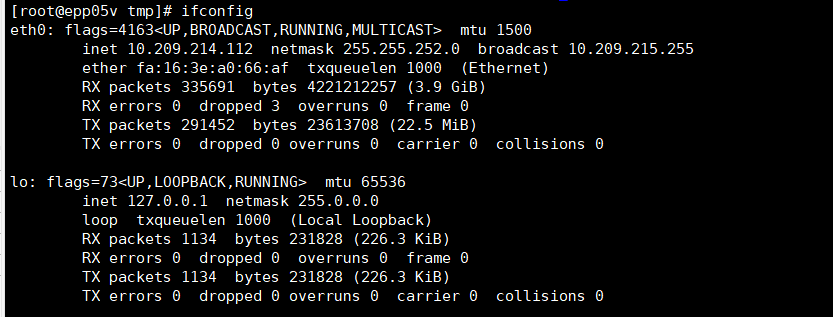
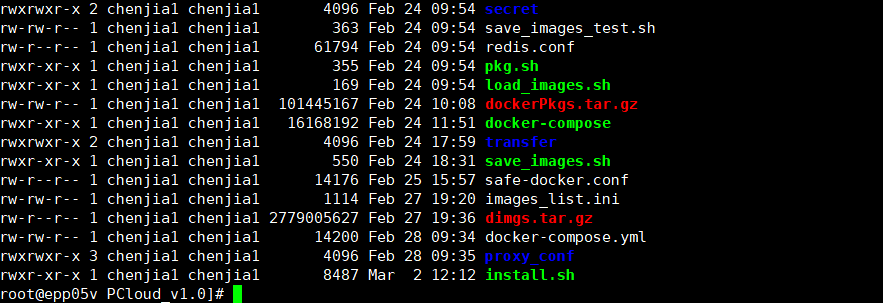
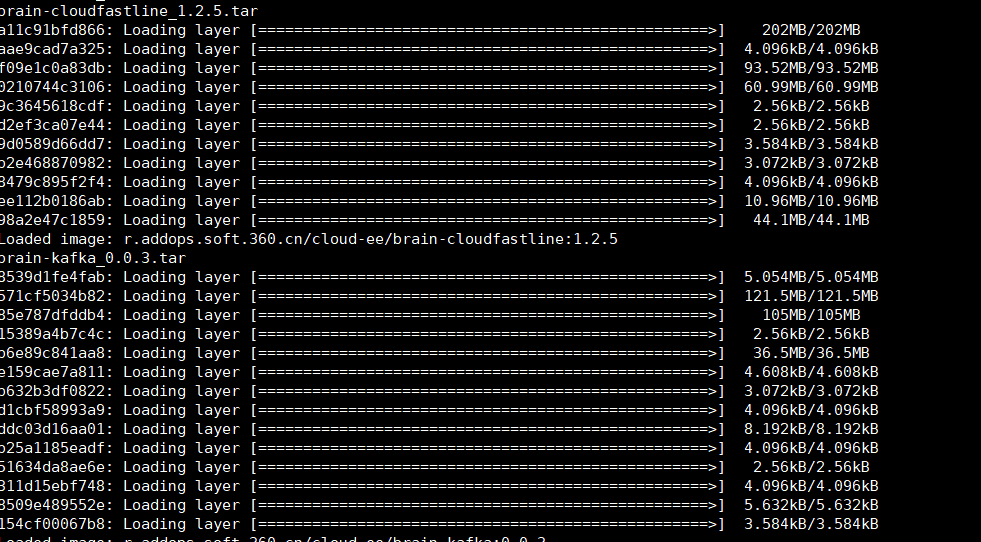
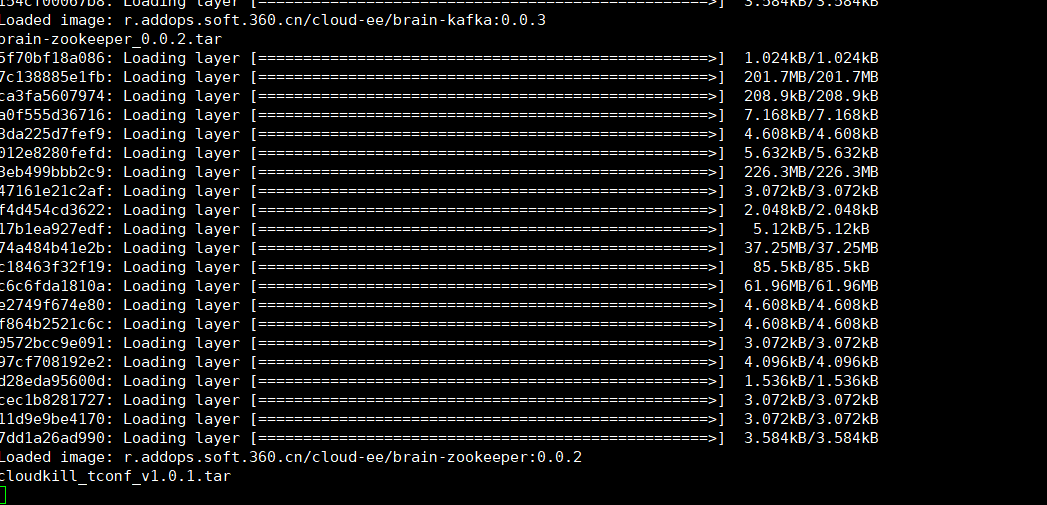
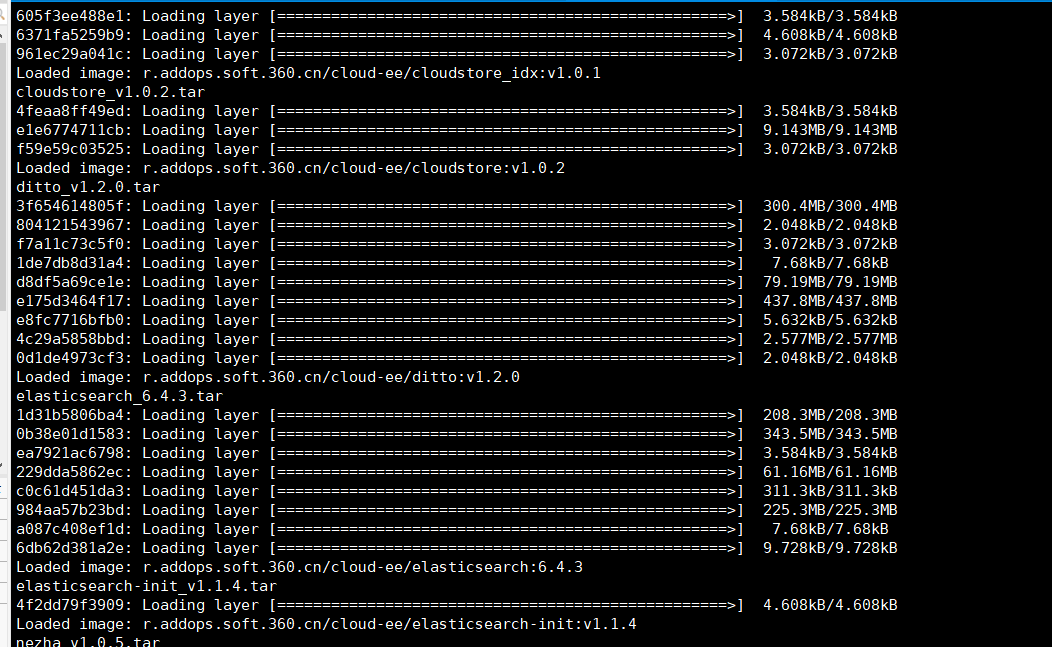
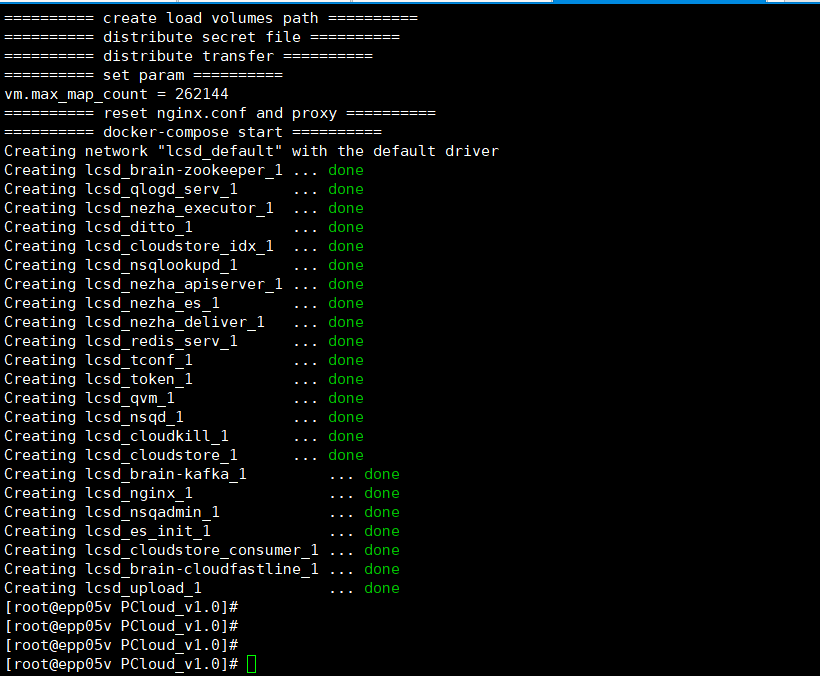




建立多级后可完成上下级授权分配，数据汇总，上下级策略约束，上下级升级等相关操作；具体多级使用请参考产品操作手册文档。

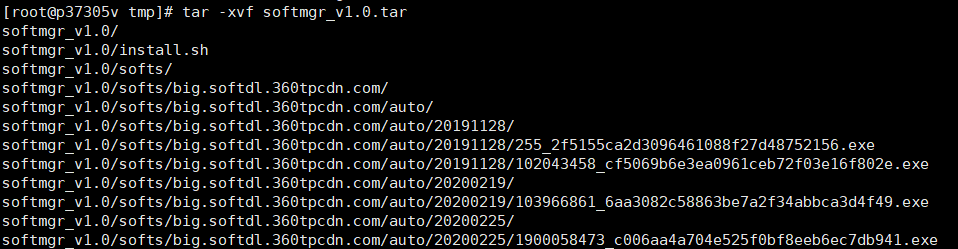
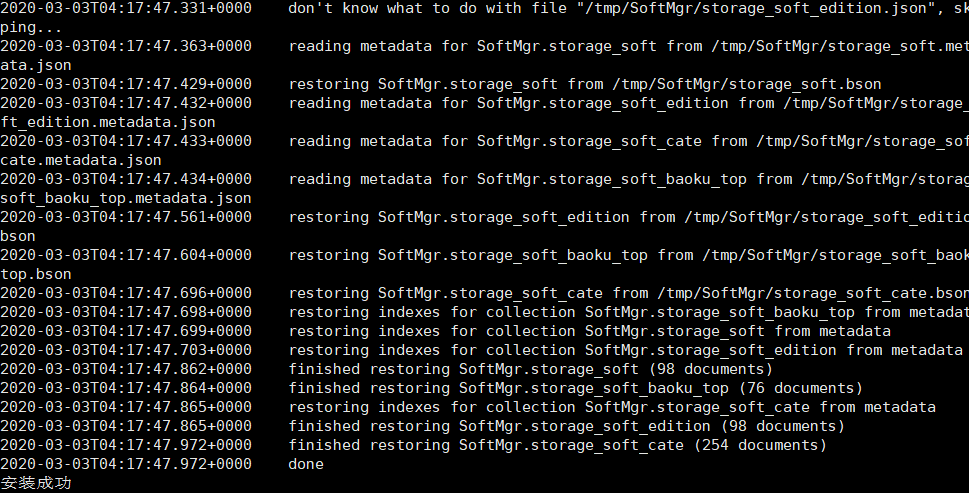
## 私有云安装

### 操作步骤

1. 解压缩安装包  
   
2. 检查网卡  
   
3. 进入到解压缩目录：PCloud\_v1.0  
   
4. 执行脚本：sh install.sh  
     
     
     
   

## 安装软件管家

### 操作步骤

1. 解压缩安装
2. 执行安装脚本：sh install.sh  
   

## 部署CDN服务

### 操作步骤

1. v10.0.0.03000以上版本支持，部署fastdfs，secccdn两套服务，具体软件包联系360获取
2. 安装部署请参考《360终端安全管理系统CDN服务部署以及使用手册》。
3. 使用场景说明：  
   1、nginx限流  
   2、具备多节点进行流控  
   3、控制管控中心以及客户端文件上传下载流量
4. 系统部署图  
   

secccdn支持单机，也支持集群，部署实施时需要根据项目实际情况决定集群规模的大小。

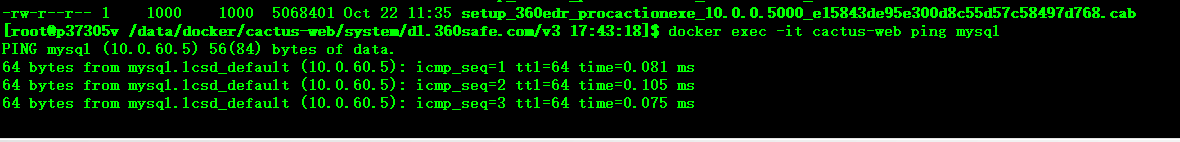
# 安装后检查

## 检查Docker服务

|  |  |  |
| --- | --- | --- |
| 检查项 | 检查步骤 | 检查结果 |
| 查看服务运行状态 | docker-compose ps 查看 | 全部为Up状态 |
| docker exec -it cactus-web supervisorctl status 查看 | 全部为RUNNING状态 |
|  |  |  |


## 检查数据库



容器内互通即可。

## 服务与配置检查

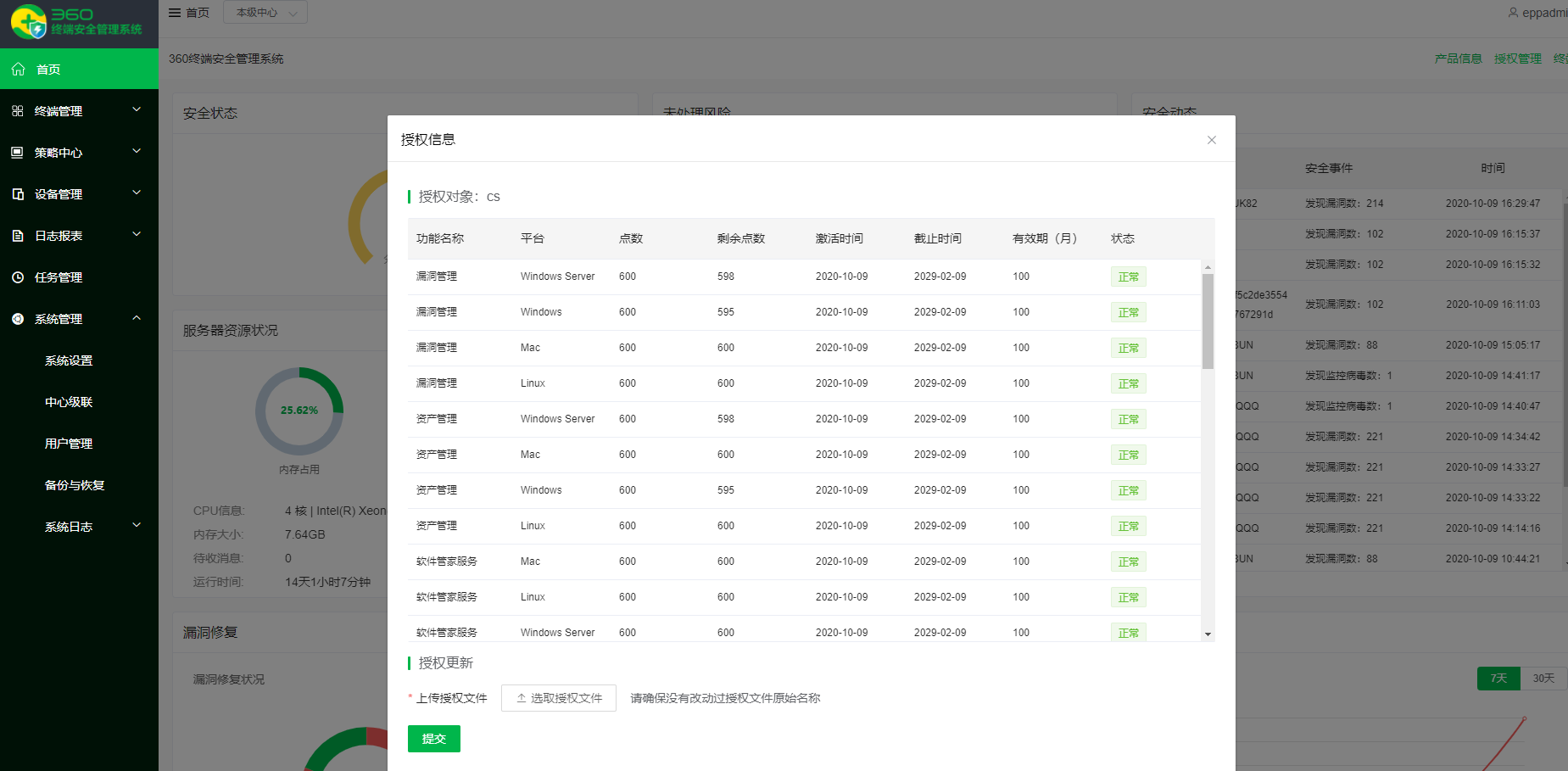
|  |  |  |  |
| --- | --- | --- | --- |
| 检查项 | 检查步骤 | 检查结果 | 备注 |
| 健康状态 | 执行cd /home/s/lcsd/ 执行命令 docker-compose ps，查看“State” | 如果存在“unhealthy”，则该项服务有异常 | 如果安装后出现异常，可cd /home/s/lcsd/到该目录下执行命令docker-compose restart做出简单的处理后再行测试。 |
| 配置检查 | 1、通过浏览器（要求Chrome76版本及以上）访问 http://{IP}:8081/dist/，应该出现登录界面（用户名: eppadmin, 密码: pass-abcd-1234）。 2、登录成功后，点击左侧菜单 【终端管理】->【安全设置】，选择 【基本设置】，在 "升级服务器" 对应的输入框中输入 "服务器IP:80"，然后点击对应的设置按钮。 | 完成功能设置 |  |

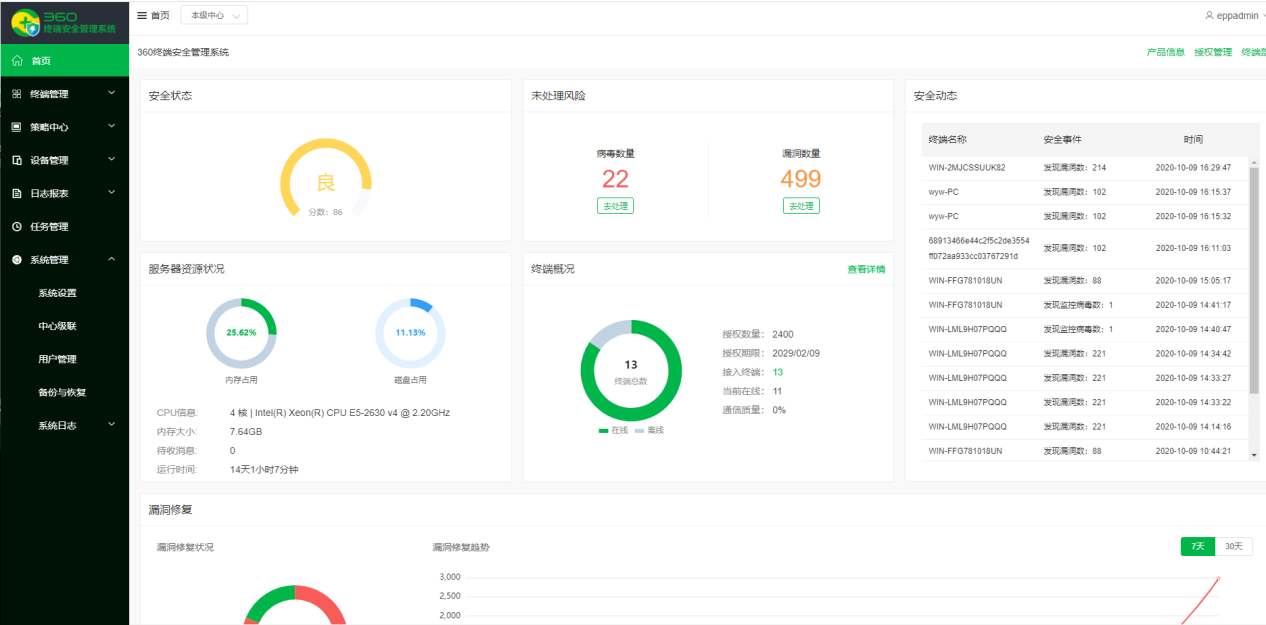
## 授权证书配置

|  |  |  |  |
| --- | --- | --- | --- |
| 检查项 | 检查步骤 | 检查结果 | 备注 |
| 序列号申请 | 联系授权管理平台生成对应序列号 | 获取到序列号 |  |
| 生成授权证书 | 联系授权服务平台注册，对应序列号生成证书，并下载证书 | 获取到证书 |  |
| 管控中心管理员导入证书 | 管控中心右上角-授权-授权管理进行证书导入 | 证书导入成功 |  |

### 管控中心首页，更新授权证书







### 授权证书获取-申请序列号

请联系授权管理平台生成对应序列号。

### 生成授权证书

请联系授权服务平台注册，对应序列号生成证书，并下载证书。

### 管控中心导入证书

管控中心管理员导入证书。

# FAQ

## 客户端安装

### 手动安装客户端

**问题现象1**：首页无法下载企业版杀毒客户端

解决办法：

1. 检查对应的安装程序是否被迅雷之类下载软件接管了下载；
2. 检查管控后台是否配置了对应的下载地址。

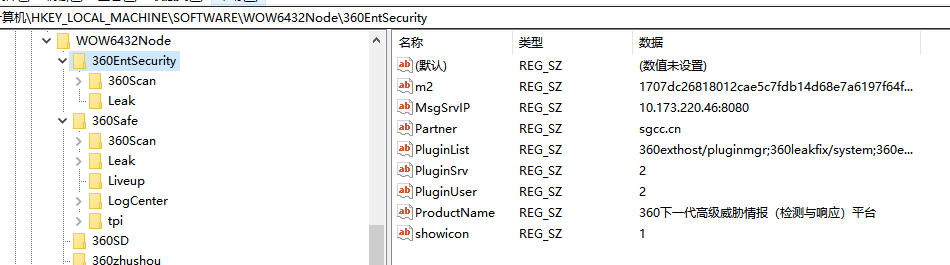
## 客户端服务端通讯

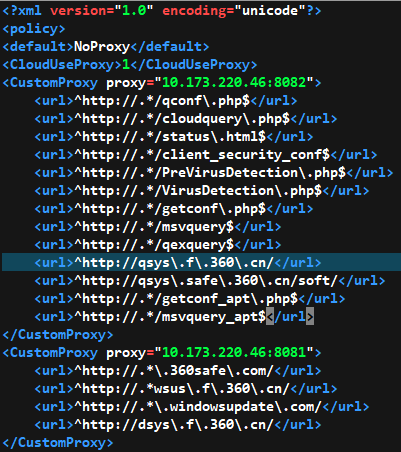
### 客户端与管理后台

**问题现象1**：客户端连接不到管理后台，托盘显示未连接服务。

解决办法：

1. 查看客户端C:\Program Files (x86)\360\360EntSecurity\ProxyConfig.xml，是否有类似内容：如果没有则表示管理后台没有下发配置给客户端，需要检查管理后台对应的cactus-web的服务是否正常，如服务端服务不正常，则需要检查后台服务是否正常工作；确认其他客户端是否能正常连接到管理后台。
2. 检查客户端注册表相关信息，确认客户端是否有注册上，如下图：





**问题现象2**：EPP客户端连接到管理后台，托盘显服务已连接，但是管理后台看不到该客户端。

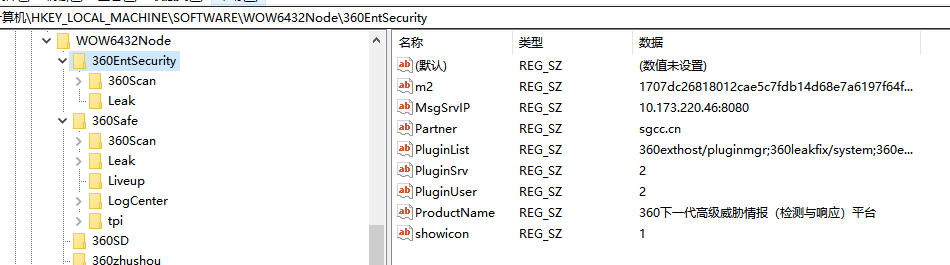
解决办法：检查[后台服务器docker exec -it cactus-web curl http://lcs:8080/m2list](file:///C:\\Users\\chenjia1\\AppData\\Roaming\\CCwork\\7652669648801607\\FileRecv\\后台服务器docker%20exec%20-it%20cactus-web%20curl%20http:\\lcs:8080\\m2list)，查看返回的的list地址是否有该M2客户端，一般情况下都会有该客户端，那么就说明长连接服务跟客户端是连接正常的，这种情况就转到长连接跟管理后台服务端不通；一般都是长连接服务跟管理后台服务之间的端口不通。

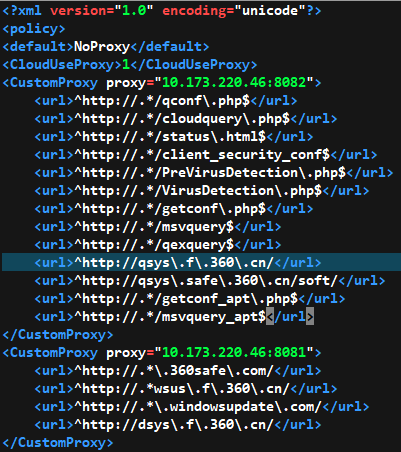
**问题现象3**：服务部署完成客户端无法在管控中心展示。

解决办法：

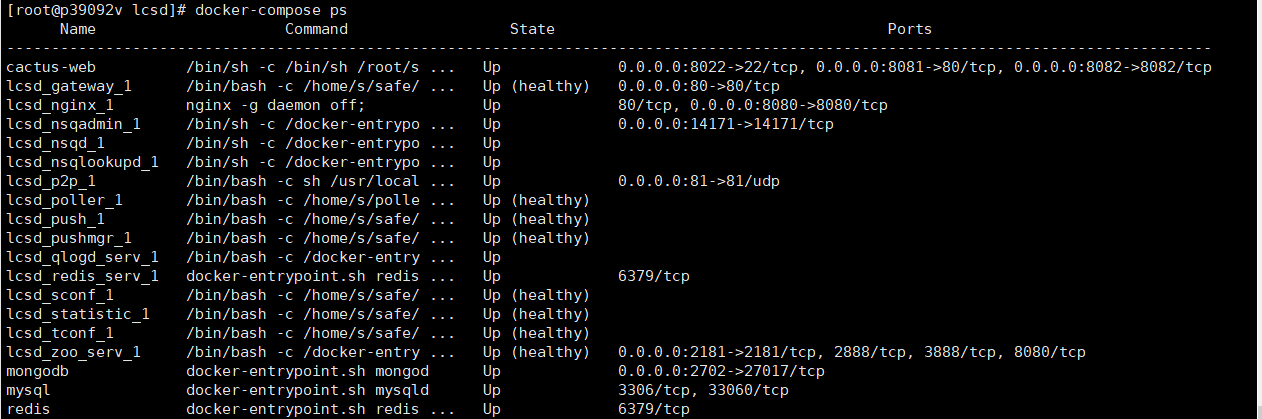
1、查看客户端C:\Program Files (x86)\360\360EntSecurity\ProxyConfig.xml，是否有类似内容：如果没有则表示管理后台没有下发配置给客户端，需要检查管理后台对应的cactus-web的服务是否正常，如服务端服务不正常，则需要检查后台服务是否正常工作；确认其他客户端是否能正常连接到管理后台。

2、检查客户端注册表相关信息，确认客户端是否有注册上，如下图：





3、如果以上还不能解决问题：则需要到管控中心服务器看下docker服务部署情况：



## 服务端下发杀毒命令

**问题现象1**：客户端没有执行杀毒指令（快扫&全盘扫）。

解决办法：

1、检查确认客户端是否在线，在管理后台是否显示在线；

2、检查命令是否下发到了客户端：[http://IP:8081/dist/#/operation/actions](http://10.173.220.46:8081/dist/" \l "/operation/actions),检查进度



1. 这种情况一般都是要么客户端不在线，要么就是客户端还没有收到杀毒命令，批量下发指令可能没那么快下达到客户端（终端数过多情况下）一般很快 不到1分钟客户端收到命令后肯定会执行杀毒指令（暂没有遇到在线的客户端收到指令后不执行杀毒的情况）

## 客户端数据上报

### 客户端杀毒上报数据

**问题现象1：**客户端杀毒完成后服务端上展示的病毒数与客户端病毒数不一致。

解决办法：检查确认客户端杀毒完成后是否有点确认，如果没有确认，是不会上报数据到服务端管理后台的，上报后数据即同步；逻辑要求触发确认后完成上报。

### 客户端隔离区上报数据

**问题现象1：**客户端杀毒完成并隔离完成；但是隔离区数据与管理后台隔离区数据不一致。

解决办法：检查确认在管理后台是否完成了隔离区数据的上报，需要管理员手动触发该客户端的隔离区数据上报，完成上报后服务端即同步了客户端的隔离区数据并入库到管理后台。

### 客户端信任区上报数据

**问题现象1：**客户端杀毒完成并隔离完成，恢复并信任相关数据；但是信任区数据与管理后台信任区数据不一致。

解决办法：一般情况下 客户端的信任区变更之后，服务端会实时同步，管理后台会立即更新个人信任区；管理后台更新了个人信任区之后 客户端的个人信任区刷新后也会同步更新。

### 客户端中心地址迁移

**问题现象1：**客户端连接的管控中心ip变更之后，客户端无法连接新的中心。

解决办法：一般情况下将变更前的中心下发策略到客户端，通讯ip与端口都变更成新的管控中心ip+端口，客户端收到策略完成重启之后即可连接新的管控中心。

## 漏洞

**问题现象1：**管理后台下发漏洞扫描，扫描不到客户端漏洞信息。

解决办法：检查确认管理后台能否上外网，如果不能上外网则不能拉取更新到漏洞库，也就是exthost安装目录下检查是否有以下文件：



如果没有，确认也不能上外网，则需要将以上文件打包cab，并更新exthost.ini文件，给客户端更新（内网部署可以参考该方案）-外网无需考虑 会自动从外网拉取到漏洞库信息；

**问题现象2：**管理后台下发漏洞修复，无法完成修复。

解决办法：检查确认管理后台能否上外网，如果不能上外网则即使具备了5.6.1中的有了漏洞库，现阶段也不支持离线修复补丁的，需要等新版本来解决；



**问题现象3：**管理后台下发漏洞修复，完成修复后，管理后台还显示未修复

解决办法：有些漏洞需要修复后重启客户端电脑（漏洞属性），重启后会再次自动上报漏洞状态，管理后台查看这个已经修复了该漏洞的终端，这个漏洞就会状态更新为已修复；

## 网络环境

### 外网环境

**问题现象1：**服务均正常部署，但是外网访问不通，访问不了外网云查等服务。

解决办法：检查确认管理后台部署的服务器是否有做外网访问端口的限制，如果有则需要打开相应限制，确保可以正常联通conf.f.qh-lb.com、bp.qh-lb.com、sconf.f.360.cn，有NAT则需要跟对应网络管理员确认是否有地址转换相关限制，一般情况下 提供的部署服务器没有做这些限制，正常外网连接，正常访问云查。

### 内网环境

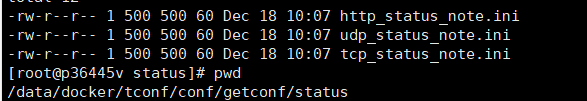
**问题现象1：**服务均正常部署，功能有限，无法修复漏洞，病毒查杀效率低下。

解决办法：暂无本地云查功能，也无本地漏洞修复功能，可以等后续版本；漏洞扫描可以提前打包对应漏洞库提供给客户来支持漏洞本地扫描。

**问题现象2：**服务均正常部署，但是管理后台看不到客户端。

解决办法：

1、检查部署配置：/data/docker/tconf/conf/getconf/status



2、修改以上三个ini文件

[docker]

business=cloudkill,hips,scan,poll

10.173.220.46=10

3、修改完成后，重启docker服务，以上ip为管理后台部署服务的ip

/home/s/lcsd路径下执行docker-compose down 停服务，执行：docker-compose up –d启服务。

### 内网外网网段ip隔离环境

**问题现象1：**服务均正常部署，服务器有内网&外网ip，客户端均在内网,但是管理后台看不到客户端信息。

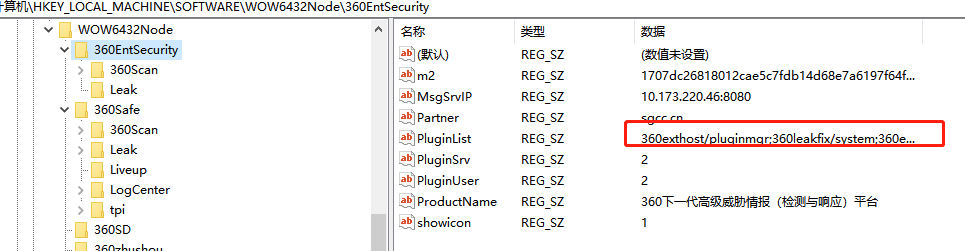
解决办法：部署环境有NAT防火墙，且同时存在内外网ip的情况下，查看上文提到的m2list接口，确认是否返还了客户端信息，如果返还了，说明长连接本身是跟客户端是连接状态，只是长连接服务端口跟管理后台端口不通；现有部署都是长连接服务跟管理后台应用服务部署在同一个主机上，这种现有解决办法是通过虚拟网卡方式来解决，给长连接服务指定虚拟网卡端口。

### 管理后台命令下发

**问题现象1：**管理后台给客户端下发命令，提示客户端缺少相关插件。

解决办法：

1、查看注册表信息，检查pulginlist是否有正确加载相关插件：

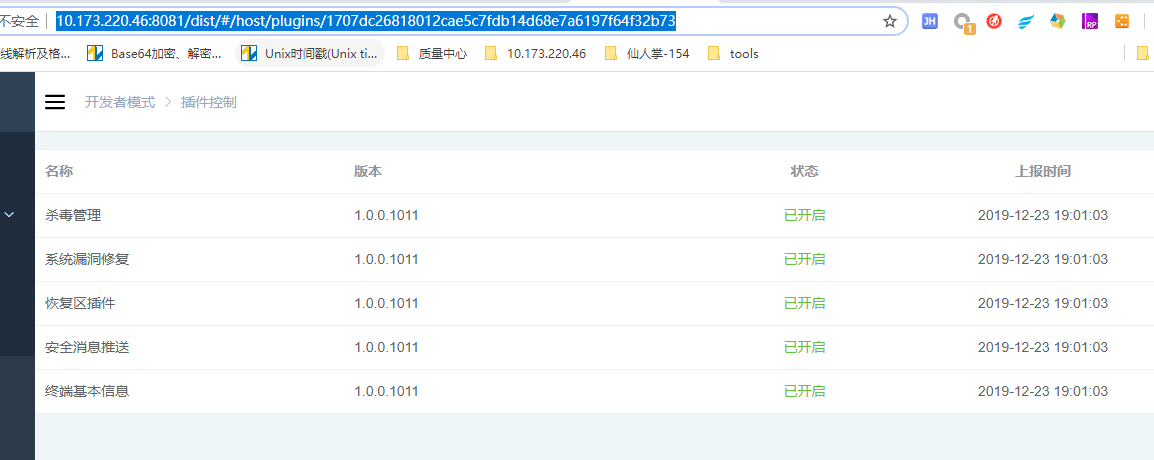


360exthost/pluginmgr;360leakfix/system;360exthost/leakfix;360exthost/pcinfo;360exthost/messagepush;360exthost/360sdmgr;360exthost/quarant

2、检查客户端是否有打开这5个插件：

[http://IP:8081/dist/#/host/plugins/1707dc26818012cae5c7fdb14d68e7a6197f64f32b73](http://10.173.220.46:8081/dist/#/host/plugins/1707dc26818012cae5c7fdb14d68e7a6197f64f32b73)

其中1707dc26818012cae5c7fdb14d68e7a6197f64f32b73为对应客户端的m2



## 授权文件

**问题现象1：**授权文件是否可以管理员自己生成。

解决办法：

1、授权文件由软件提供方统一下发给客户，客户导入授权文件完成授权确认；

2、客户联系销售去授权服务平台注册，生成授权证书，导入到管控中心完成授权认证。

## 软件更新

### 管理后台更新

**问题现象1：**管理后台更新客户通过什么方式更新。

解决办法：现在只支持离线方式，提供更新包的方式更新（一键更新）。

### 客户端更新

**问题现象1：**杀毒客户端是否支持离线和在线方式更新。

解决办法：现阶段只支持离线更新，通过v3的方式提供更新包给客户，客户通过sftp更新到管理后台v3，自动下发更新任务到各个客户端主机自动更新客户端。

### 病毒库漏洞库更新

**问题现象1：**漏洞库病毒库是否支持在线更新，是否支持离线更新。

解决办法：具备连接外网的管理后台支持自动更新病毒库以及漏洞库，自动下载漏洞补丁程序，非外网的暂时只具备离线更新漏洞库、病毒库。

### 代理服务器

**问题现象1：**管理后台是否可以使用其他代理服务器来代理转发请求云查。

解决办法：管理后台可以设置代理云查的服务器IP&端口。

### 安全设置

**问题现象1：**升级服务器、长连接、sftp账号、云查、p2p代理 是否可以随意设置ip跟端口。

解决办法：现阶段以上这些服务均打包到了安装包一起，相对应的docker服务也部署在管理后台同一个主机上，不建议将各个服务配置到不同服务器上，避免低效率的网络请求与交互；升级服务器配置为管理后台IP:端口8081，长连接管理后台IP:端口8080，数据更新sftp账号管理后台IP:端口8022，云查配置为管理后台IP:端口8082，P2P配置为管理后台IP:端口81。

## 软件管家

**问题现象1：**客户端软件管家列表数据为空。

解决办法：软件管家ip:8081/softmgr/software；重新发布即可。

**问题现象2：**软件管家不知道怎么新增软件到客户端。

解决办法：管控中心，新增软件，编辑版本，并上传到管控平台，拿到代理连接url，更新到管控中心平台。

## 部署相关

### 软硬件环境

**问题现象1：**新挂硬盘到data数据盘的情况。

解决办法：

1、查看硬盘情况:fdisk -l ；查看挂载情况:df -lh ；fdisk操作:fdisk /dev/sda（如果是新挂硬盘到data则需要上述操作）

2、格式化：mke2fs -t ext4 /dev/sdb1

3、挂载：mount /dev/sda1 /var/xxx 即可挂载分区到/var/xxx这个路径上

4、查看data挂载后的磁盘大小：

df -T | grep sdb

mount /dev/sdb1 /data

cat /etc/mtab | grep /data >> /etc/fstab 挂载后 加到启动项，reboot

还可以通过软连接方式快速处理扩展data磁盘空间

一般创建/home/data

ln -sf /home/data /data--建立软连接

### 网络相关

**问题现象1：**存在内外网NAT。

解决办法：

iptables –t nat –A POSTROUTING –s 192.168.10.10 –o eth1 –j SNAT --to-source 111.196.221.212

解压安装大包后执行 sh reset\_service\_ip.sh -i nat映射后的IP地址：

sh reset\_service\_ip.sh -i 192.222.22.21

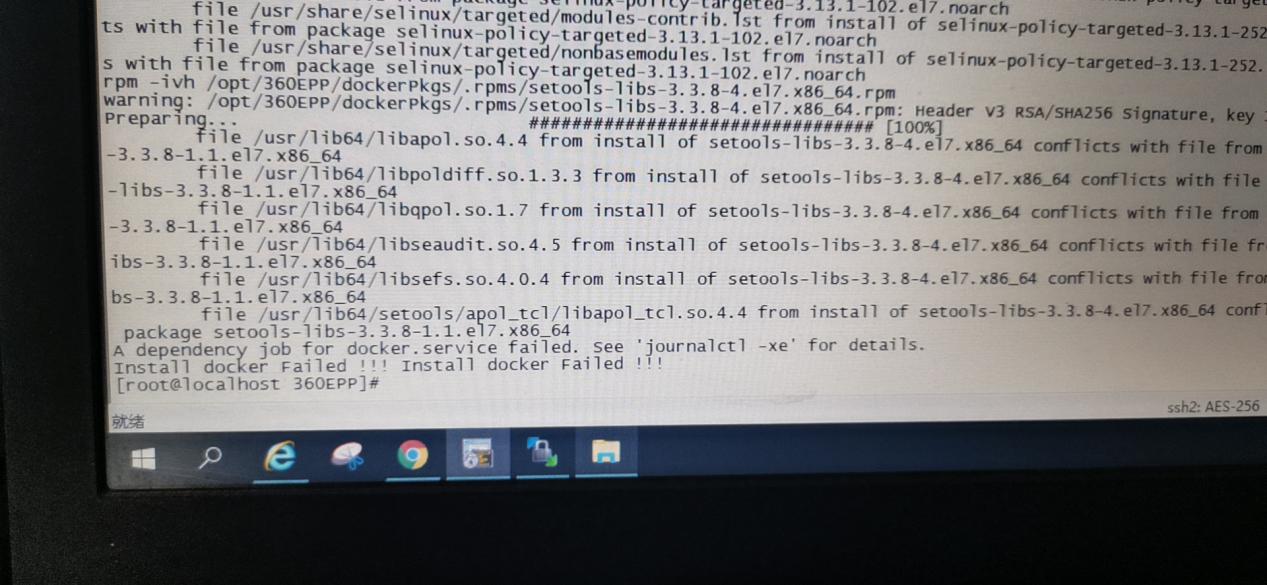
查看长连接用到哪个ip：

cat /data/docker/tconf/conf/getconf/status/tcp\_status\_note.ini

如果有私云：

curl http://10.216.7.95:8080/cloudstore/eppadmin/status?type=usage 中心上curl，返回200则成功；

curl -I 10.216.7.95:8080/cloudbuilder 中心curl 返回数据则标识私云内部docker服务是通的；



Docker安装不上，检查防火墙是否关闭

cat /etc/selinux/config

**问题现象2：**办公网和机房网互通，但是客户不想让服务器的80 8080开放给办公网，两个端口全不让开放或者其中一个不让开放。

解决办法：

sh install.sh -n 网卡名 或者 -i 网卡名对应的实际ip -p 客户允许的tcp端口 -h 客户端允许的http端口

-p和-h，用到哪个就给哪个参数，比如80不让开，可以开放81，就-p 81，此时tcp端口就是81，http还是8080

**问题现象3：**办公网和机房网不通，得用NAT。

解决办法：

安装:sh install.sh -i NAT映射的ip

这样安装，也就是机房还是默认用80 和8080

假设映射为：80->80, 8080->8080，也就是映射前后端口完全一致，就什么都不用做了

假设映射为：80->10080, 8080->18080，安装完后

第一步：sh reset\_service\_ip.sh -i 127.0.0.10 -p 10080

第二步：到管控平台上，修改长连接通信服务器地址 映射ip:18080

### 客户端相关

**问题现象1：**客户端问题无法定位。

解决办法：

客户端日志：

%appdata%下的360safe目录下手工建立LiveUpdateLog目录 看下360sdUpd.log日志。

C:\Users\chenjia1\AppData\Roaming\360Safe

P2SP\_360sdupd.log

C:\Users\chenjia1\AppData\Roaming\360safe\LiveUpdateLog--新建这个目录生成log

--客户端log

c盘

根目录的log.ini文件

[app]

log = 1

C盘生成360entcom\_log.txt

客户端路由信息：

C:\Users\chenjia1\AppData\Roaming\360Safe

日志抓取：

Dbgview.exe,procexp.exe,Procmon.exe,procdump.exe 加上entcom的日志版&msgrouter日志版抓取日志确认问题

### 服务端

**问题现象1：**客户端在中心显示不在线。

解决办法：cat /data/docker/cactus-web/logs/cactus.safe.360.cn/app/nsq.data |grep "PCI" 看下是否有上报打点，如果没有则是长连接问题，排查长连接服务。

**问题现象2：**web服务登录不了。

解决办法：

docker exec -it cactus-web supervisorctl status 查看web服务是否里面有进程没起来。

docker exec -it cactus-web supervisorctl reload

docker exec -it cactus-web supervisorctl start cactus\_nsqconsumer cactus\_postmsg cactus\_nsqevt

Web服务端：

update user\_info set password='149cb8511cf1e4666545e3dbed44dbf9' where username='eppeppadmin';

或者执行

docker exec -it cactus-web php /home/q/system/safe-cactus/application/script/ResetPassword.php 初始化密码

**问题现象3：**Web的nginx配置。

解决办法：

/data/docker/cactus-web/nginx/cactus/vhost.conf 涉及到端口修改；

下载地址调整，通过nginx配置实现

/data/docker/cactus-web/nginx/cactus/vhost.conf

删除download的重定向 然后重启web里面的nginx配置

docker exec -it cactus-web /usr/local/nginx/sbin/nginx -s reload 重新加载nginx

服务端程序升级--dockerweb里面配置host：

10.173.220.54 entup.safe.360.cn

### 私云部署

检查服务器CPU、内存、磁盘, 建议CPU16C，内存32G，SSD磁盘128G，挂载data1下，机械盘500G，挂在data下；

执行安装，安装时指定db文件db.tar.gz, db文件路径为绝对路径：

sudo sh install\_single.sh -d /tmp/PCloud\_Cluster\_v1.0/db.tar.gz

安装完成进入pcloud查看服务是否都up:

cd /home/s/pcloud

私云端口：

安装包下，etc/docker-compose.yml.tianqing

14171:14171 改成24171：4171 8080：080 改成18080：8080

中心配置私云ip为18080

关闭防火墙：

systemctl stop firewalld 单机部署私云跟中心需要关闭防火墙。