

**数据安全态势感知平台安装部署指南修订记录**

|  |  |  |  |
| --- | --- | --- | --- |
| **日期** | **版本** | **描述** | **作者** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

目录

[第一章 引 言 5](#_Toc468370673)

[1.1目的 5](#_Toc468370674)

[1.2范围 5](#_Toc468370675)

[1.3名词定义 5](#_Toc468370676)

[第二章 运行环境 6](#_Toc468370677)

[2.1 硬件、软件环境 6](#_Toc468370678)

[2.2 SIP部署架构图 6](#_Toc468370679)

[2.3 SIP部署场景举例 7](#_Toc468370680)

[2.3.1 模式一：只有一台服务器 7](#_Toc468370681)

[2.3.2 模式二：有两台或两台以上服务器 7](#_Toc468370682)

[第三章 安装步骤 9](#_Toc468370683)

[3.1 安装RedHat6.3或6.5且为64位系统（略） 9](#_Toc468370684)

[3.2 全新安装 9](#_Toc468370685)

[3.2.1 安装包的结构图 9](#_Toc468370686)

[3.2.2 安装SIP平台 9](#_Toc468370687)

[3.2.3 SIP平台启动、重启 10](#_Toc468370688)

[3.2.4 授权导入 11](#_Toc468370689)

[3.2.5 查看SIP平台版本、机器码 11](#_Toc468370690)

[3.2.6 可选操作 11](#_Toc468370691)

[3.3 单独安装桥接程序 14](#_Toc468370692)

[3.3.1 安装桥接程序 14](#_Toc468370693)

[3.3.2 在SIP平台组件列表里添加此桥接程序 15](#_Toc468370694)

[3.4 事件中附件的下载挂载配置 16](#_Toc468370695)

[第四章 升级安装或卸载 18](#_Toc468370696)

[4.1 升级安装 18](#_Toc468370697)

[4.1.1 Sip平台升级 18](#_Toc468370698)

[4.2 SIP平台卸载 19](#_Toc468370699)

[4.2.1 卸载SIP平台程序 19](#_Toc468370700)

[4.2.2 卸载mysql 19](#_Toc468370701)

[第五章 防火墙例外端口汇总 20](#_Toc468370702)

[第六章 常见问题 21](#_Toc468370703)

[6.1 tomcat启动时报内存溢出异常 21](#_Toc468370704)

[6.2 FTP服务设置 21](#_Toc468370705)

[6.3 默认的数据库root密码是多少？ 22](#_Toc468370706)

[6.4 IP地址或者数据库密码变了，该怎么处理？ 22](#_Toc468370707)

[6.4.1 安装包中提供了修改ip地址和数据库密码的工具包 22](#_Toc468370708)

[6.4.2 修改入库IP配置（一般只有在使用了网络dlp邮件dlp等网络端程序并且是和sip平台分开两台服务器部署才需要操作） 22](#_Toc468370709)

[6.5 服务列表（也称组件列表）变更 24](#_Toc468370710)

# 引 言

## 1.1目的

指导实施人员安装部署数据安全态势感知平台。

## 1.2范围

本安装手册适用于数据安全态势感知平台服务端平台的安装。

## 1.3名词定义

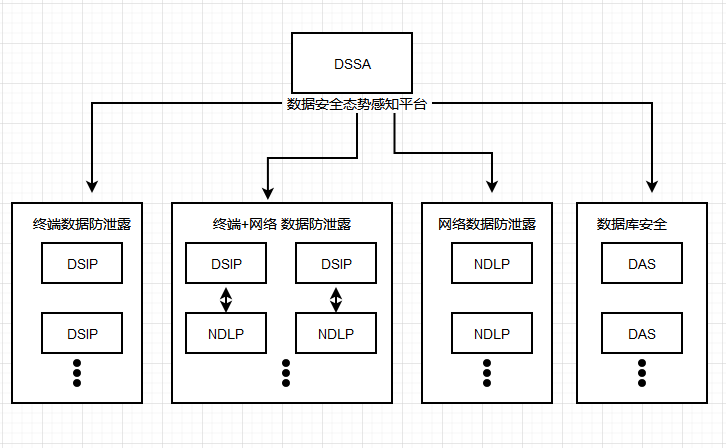
|  |  |
| --- | --- |
| **简称** | **解释** |
|  |  |
| DSSA平台 | 数据安全态势感知平台 |
| 子系统 | DAS |
| NDLP |
| DSIP |

# 运行环境

## 硬件、软件环境

|  |  |
| --- | --- |
| 配置项 | 最低要求 |
| CPU | P4 2.8\*4 |
| 内存 | 16GB |
| 硬盘 | 1TB |
| 软件预留安装空间 | 10GB |
| 支持的操作系统（64bit） | CentOS 7.6 |
| 数据库 | Mysql数据库 |
| JDK | Jdk11 |

## 平台部署架构图



此图展示的是DSSA管理平台部署时的形态，可以包含多个子系统，如网络dlp、Dsip终端防护、DAS数据库防护，管理平台部署在一台服务器上，其他子系统各自安装部署，完成后执行加入平台的脚步（此脚步需要根据实际情况进行修改）。

如果需要DSSA管理平台部署，目前需要根据现场部署方案由研发给出指导。

## 平台部署场景举例

模式一：平台+子系统部署（DSIP、NDLP、DAS）

模式二：平台+多子系统部署（DSIP、NDLP、DAS）

# 安装步骤

## 安装Linux操作系统（略）



### CentOS7.6且为64位系统

如下CentOs，仅按照基础设施服务器接口，无需勾选其他附加选项进行安装，保证环境都使用我们安装包的系统依赖包。



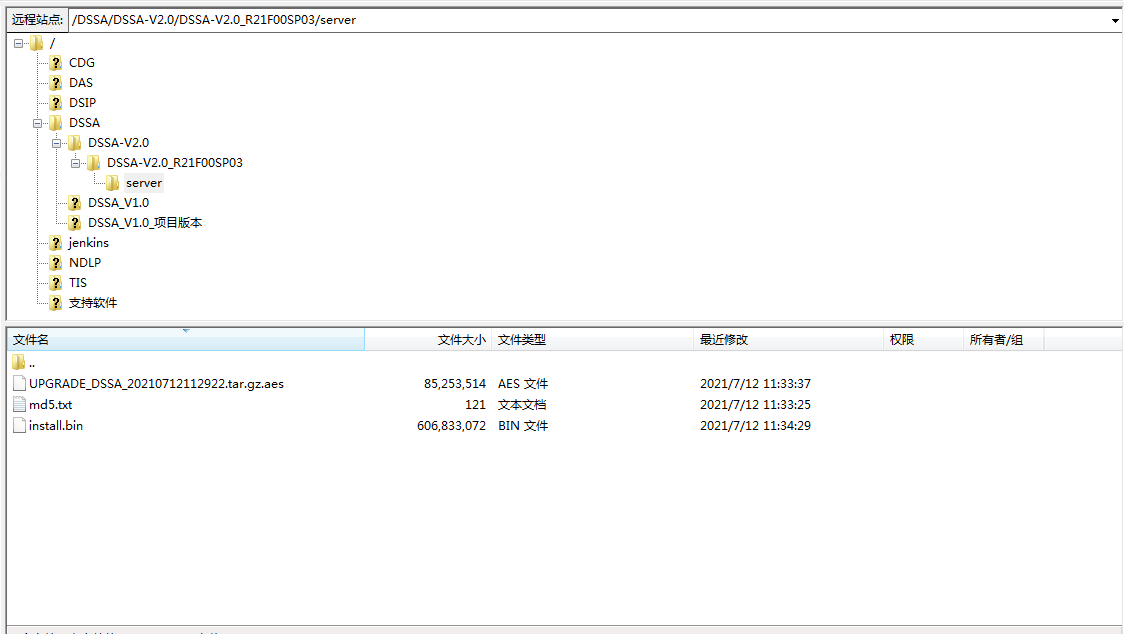


### 安装字体库

系统安装完成后，需要安装字体库，参考命令：yum install fontconfig

## 全新安装

### 安装包的结构图及检查是否损坏



注意：务必在使用安装包前先检查下包是否是损坏的，如果是md5值变了，说明是损坏的，请重新获取安装包。在安装包所在目录操作步骤如下：

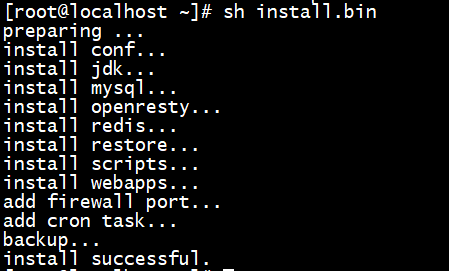
1. 在安装包路径下，执行cat md5s命令，查看各个文件出厂时的正确的md5值。
2. 执行md5sum install.bin命令，将在第二行显示该文件实际md5值。如果和出厂值不一致说明损坏

### 安装DSSA平台

DSSA平台的安装的包是用springboot2开源框架开发的，安装包里面包含可执行jar包，安装包包含有jdk、openresty、redis、msyql等。安装方法如下：

1. 安装文件为install.bin
2. 完全安装，执行的命令如下：

|  |
| --- |
| sh install.bin |



### DSSA平台运维命令

此处所提的启动和重启只限于DSSA平台，不包括其他子系统程序（比如网络dlp、邮件dlp、文件服务器扫描、DSIP、DAS等）。

默认安装完成后等待几分钟服务就会启动。

注意：一般来说重启DSSA服务应该在1~5分钟完成。但是第一次安装后的启动会更慢一些，因为需要执行大量的数据库初始化工作，需要耐心多等待几分钟。注意：安装（包括升级安装）后**第一次启动**的时候，千万不要停服务、重启服务器等，一定要耐心等待服务启动完毕。比如如果在全新安装的时候第一次启动还没完成时，如果手工关服务器可能会造成数据库错误，这时候研发建议直接卸载重装。

#### DSSA服务重启

启动执行命令：/usr/local/dsec/bin/init.d/java\_dssa\_portal start

停止执行命令：/usr/local/dsec/bin/init.d/java\_dssa\_portal stop

重启执行命令：/usr/local/dsec/bin/init.d/java\_dssa\_portal restart

说明：

* DSSA平台有守护机制，服务器启动后会自己启动

#### 附加说明：DSSA平台服务检测（守护机制）介绍

守护机制的配置文件路径: /usr/local/dsec/conf/checkAlive.conf，用vi编辑器打开此配置文件，将

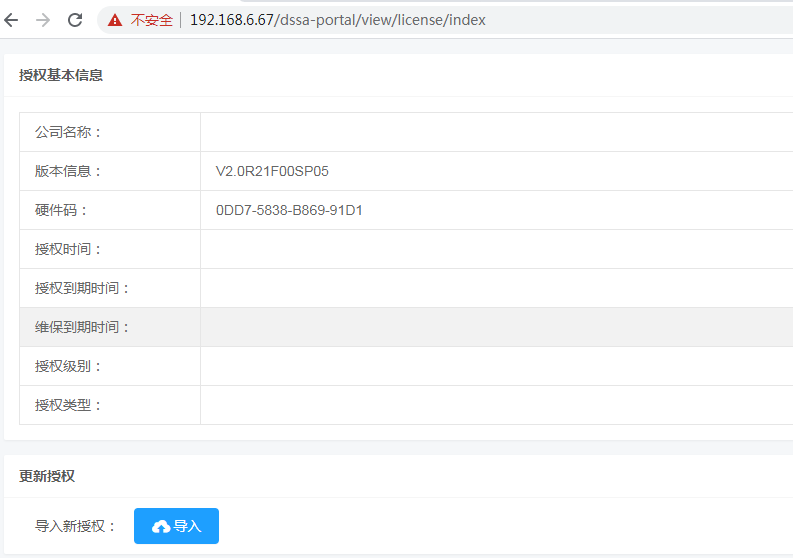
CHECK\_ALIVE=Y改成CHECKALIVE=N即可关闭守护；重新改成Y即可开启守护。

注：CHECK\_ALIVE=Y的时候，会有脚本不停检测，一旦发现DSSA平台服务没启动将自动启动（因此CHECKALIVE=Y的时候，开机后sip平台服务会自动启动）

警告：理论上实施人员至始至终都不需要人工动这个配置文件！随意改这个文件会导致一些严重问题。包括升级安装目前也实现了程序自行智能判断是否自动关闭守护，不再需要人工干预！！！

### 授权导入

1. 通过IE浏览器登陆web（登陆地址：<https://IP>或https://IP/dssa-portal/），输入用户、密码进行登录，登录系统管理员账号：sysAdmin/Dlp@1234；登录成功后,显示导入授权页面,需要导入授权,才可以进行系统进行操作。
2. 导入新授权窗口。

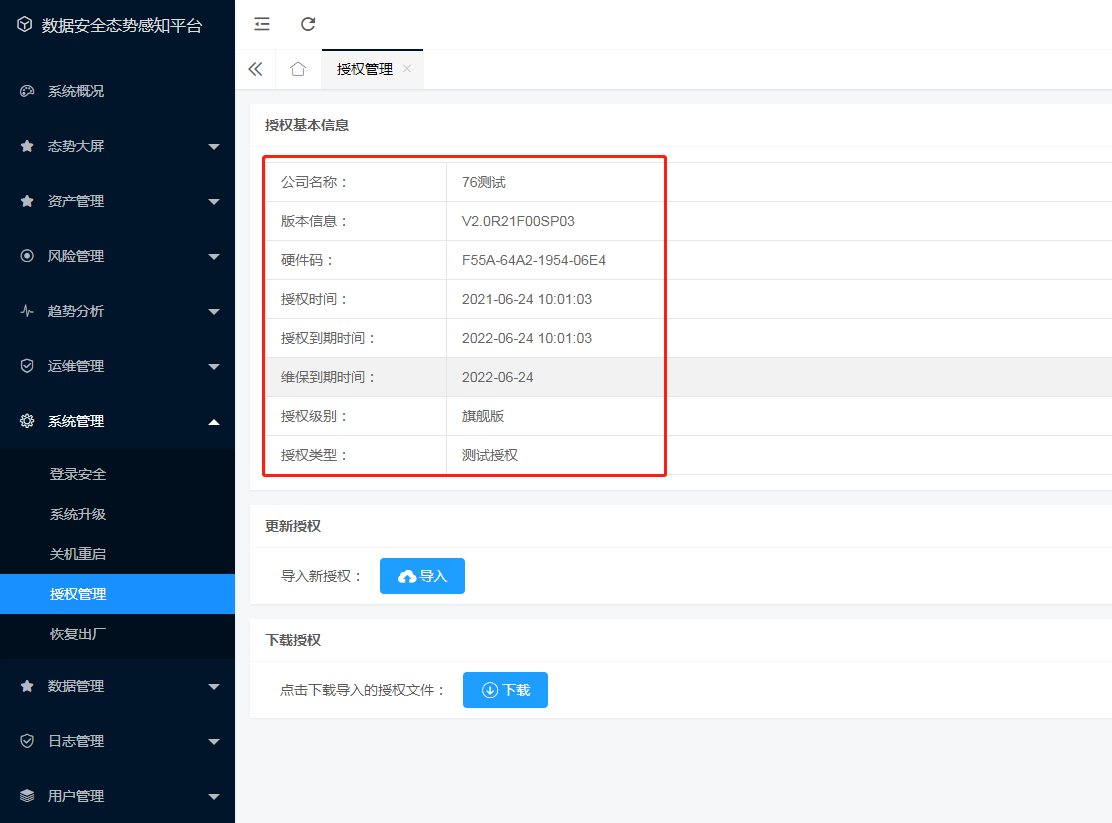


2、发送机器码和版本号信息给亿赛通的相关支持人员（发文本，不要发截图），制作授权。

3、点击“浏览”按钮，选择授权文件，点击“导入”，导入完成后会弹出授权信息（授权信息内容包含：公司名称、公司ID、客户电话、客户端邮箱、产品授权类型、授权时间、授权到期时间、授权终端总数、产品特性）。

### 查看授权信息

登录态势感知平台后，访问系统管理-授权管理，查看授权信息（如下图）。



## 各子系统安装说明

目前支持DSIP、NDLP、DAS服务器作为平台的子系统，不同子系统安装跟单独部署一致，需要参考各系统的安装部署手册。部署完成后，需要进行导入授权。然后可以操作下面操作，将此业务系统作为平台的子系统。业务系统登录，可以通过平台进行单点登录。

### DSIP单独配置说明

#### 执行数据库脚本

-- 当前dsip ip地址

INSERT INTO `est\_property` VALUES ('dssa.instance.ip', '192.168.6.69');

-- 当前dsip端口(tomcat https的端口)

INSERT INTO `est\_property` VALUES ('dssa.instance.port', '8443');

-- 实例取个别名

INSERT INTO `est\_property` VALUES ('dssa.instance.name', 'DSIP-分部名称');

-- 应用id，dsip的id

INSERT INTO `est\_property` VALUES ('dssa.instance.app\_id', '1390219642659794945');

-- 接口访问地址

INSERT INTO `est\_property` VALUES ('dssa.instance.api\_url', 'https://192.168.6.69:8443/ta-server/s/uni/');

-- 实例的类型DSIP-NDLP或DSIP-CLENT

INSERT INTO `est\_property` VALUES ('dssa.instance.type', 'DSIP');

-- 上面部分，需要修改ip、端口、应用名称以及接口路径等；以下配置固定配置

INSERT INTO `est\_property` VALUES ('dssa.instance.proxy.location', '/dsip');

INSERT INTO `est\_property` VALUES ('dssa.instance.redirect\_uri', '/ta-server/user/main.do');

INSERT INTO `est\_property` VALUES ('dssa.open', 'true');

INSERT INTO `est\_property` VALUES ('dssa.portal.proxy.dync', 'true');

INSERT INTO `est\_property` VALUES ('dssa.portal.proxy.location', '/dssa-portal');

INSERT INTO `est\_property` VALUES ('dssa.portal.proxy.open', 'true');

INSERT INTO `est\_property` VALUES ('dssa.portal.url', 'https://dssa.proxy.com/dssa-portal');

#### 修改hosts文件

[root@localhost ~]# cat /etc/hosts

127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4

::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

192.168.6.76 dssa.proxy.com -> dssa.proxy.com

注意：

域名对应的是门户的ip地址，Ip地址为平台服务器的地址。

#### 重启服务器

服务重新启动命令：[root@sip ~]# /esafenet/bin/restartTomcatOpenfire.sh

重启后，子系统会上报平台的应用实例数据。

### DSIP综合配置说明

#### 执行数据库脚本

-- 当前dsip ip地址

INSERT INTO `est\_property` VALUES ('dssa.instance.ip', '192.168.6.69');

-- 当前dsip端口(tomcat https的端口)

INSERT INTO `est\_property` VALUES ('dssa.instance.port', '8443');

-- 实例取个别名

INSERT INTO `est\_property` VALUES ('dssa.instance.name', 'DSIP-分部名称');

-- 应用id，dsip的id

INSERT INTO `est\_property` VALUES ('dssa.instance.app\_id', '1324218212317487254');

-- 接口访问地址

INSERT INTO `est\_property` VALUES ('dssa.instance.api\_url', 'https://192.168.6.69:8443/ta-server/s/uni/');

-- ndlp的ip地址，因为dsip整合ndlp需要配置ndlp的地址

INSERT INTO `est\_property` VALUES ('dssa.instance.ndlp\_ip', '192.168.6.70');

-- ndlp的端口(tomcat https的端口)

INSERT INTO `est\_property` VALUES ('dssa.instance.ndlp\_port', '8443');

-- 实例的类型DSIP-NDLP或DSIP-CLENT

INSERT INTO `est\_property` VALUES ('dssa.instance.type', 'DSIP');

-- 上面部分，需要修改ip、端口、应用名称以及接口路径等；以下配置固定配置

INSERT INTO `est\_property` VALUES ('dssa.instance.proxy.location', '/dsip');

INSERT INTO `est\_property` VALUES ('dssa.instance.redirect\_uri', '/ta-server/user/main.do');

INSERT INTO `est\_property` VALUES ('dssa.open', 'true');

INSERT INTO `est\_property` VALUES ('dssa.portal.proxy.dync', 'true');

INSERT INTO `est\_property` VALUES ('dssa.portal.proxy.location', '/dssa-portal');

INSERT INTO `est\_property` VALUES ('dssa.portal.proxy.open', 'true');

INSERT INTO `est\_property` VALUES ('dssa.portal.url', 'https://dssa.proxy.com/dssa-portal');

#### 修改hosts文件

[root@localhost ~]# cat /etc/hosts

127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4

::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

192.168.6.76 dssa.proxy.com -> dssa.proxy.com

注意：

域名对应的是门户的ip地址，Ip地址为平台服务器的地址。

#### 重启服务器

服务重新启动命令：[root@sip ~]# /esafenet/bin/restartTomcatOpenfire.sh

重启后，子系统会上报平台的应用实例数据。

### NDLP配置说明

#### 执行数据库脚本

INSERT INTO `est\_property` VALUES ('dssa.instance.ip', '192.168.6.70');

INSERT INTO `est\_property` VALUES ('dssa.instance.port', '8443');

INSERT INTO `est\_property` VALUES ('dssa.instance.name', 'NDLP-分部名称');

INSERT INTO `est\_property` VALUES ('dssa.instance.app\_id', '1323121514521851514');

INSERT INTO `est\_property` VALUES ('dssa.instance.api\_url', 'https://192.168.6.70:8443/ta-server/s/uni/');

-- 上面部分，需要修改ip、端口、应用名称以及接口路径等；以下配置固定配置

INSERT INTO `est\_property` VALUES ('dssa.instance.proxy.location', '/dsip');

INSERT INTO `est\_property` VALUES ('dssa.instance.redirect\_uri', '/ta-server/user/main.do');

INSERT INTO `est\_property` VALUES ('dssa.instance.type', 'NDLP');

INSERT INTO `est\_property` VALUES ('dssa.open', 'true');

INSERT INTO `est\_property` VALUES ('dssa.portal.proxy.dync', 'true');

INSERT INTO `est\_property` VALUES ('dssa.portal.proxy.location', '/dssa-portal');

INSERT INTO `est\_property` VALUES ('dssa.portal.proxy.open', 'true');

INSERT INTO `est\_property` VALUES ('dssa.portal.url', 'https://dssa.proxy.com/dssa-portal');

#### 修改hosts文件

[root@localhost ~]# cat /etc/hosts

127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4

::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

192.168.6.76 dssa.proxy.com -> dssa.proxy.com

注意：

域名对应的是门户的ip地址，Ip地址为平台服务器的地址。

#### 重启服务器

服务重新启动命令：[root@sip ~]# /esafenet/bin/restartTomcatOpenfire.sh

重启后，子系统会上报平台的应用实例数据

### DAS配置说明

#### 执行数据库脚本

INSERT INTO `est\_property` VALUES ('dssa.instance.ip', '192.168.6.71');

INSERT INTO `est\_property` VALUES ('dssa.instance.port', '8443');

INSERT INTO `est\_property` VALUES ('dssa.instance.name', 'DAS-数据库审计名称');

INSERT INTO `est\_property` VALUES ('dssa.instance.app\_id', '1407517531658878977');

INSERT INTO `est\_property` VALUES ('dssa.instance.api\_url', 'https://192.168.6.71:8443/ta-server/s/uni/');

-- 上面部分，需要修改ip、端口、应用名称以及接口路径等；以下配置固定配置

INSERT INTO `est\_property` VALUES ('dssa.instance.proxy.location', '/dsip');

INSERT INTO `est\_property` VALUES ('dssa.instance.redirect\_uri', '/ta-server/user/main.do');

INSERT INTO `est\_property` VALUES ('dssa.instance.type', 'DAS');

INSERT INTO `est\_property` VALUES ('dssa.open', 'true');

INSERT INTO `est\_property` VALUES ('dssa.portal.proxy.dync', 'true');

INSERT INTO `est\_property` VALUES ('dssa.portal.proxy.location', '/dssa-portal');

INSERT INTO `est\_property` VALUES ('dssa.portal.proxy.open', 'true');

INSERT INTO `est\_property` VALUES ('dssa.portal.url', 'https://dssa.proxy.com/dssa-portal');

#### 修改hosts文件

[root@localhost ~]# cat /etc/hosts

127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4

::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

192.168.6.76 dssa.proxy.com -> dssa.proxy.com

注意：

域名对应的是门户的ip地址，Ip地址为平台服务器的地址。

#### 重启服务器

服务重新启动命令：[root@sip ~]# /esafenet/bin/restartTomcatOpenfire.sh

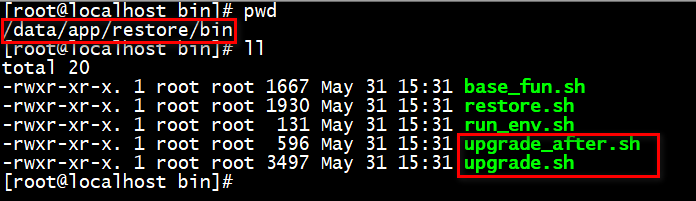
重启后，子系统会上报平台的应用实例数据

# 升级安装或卸载

## 升级安装

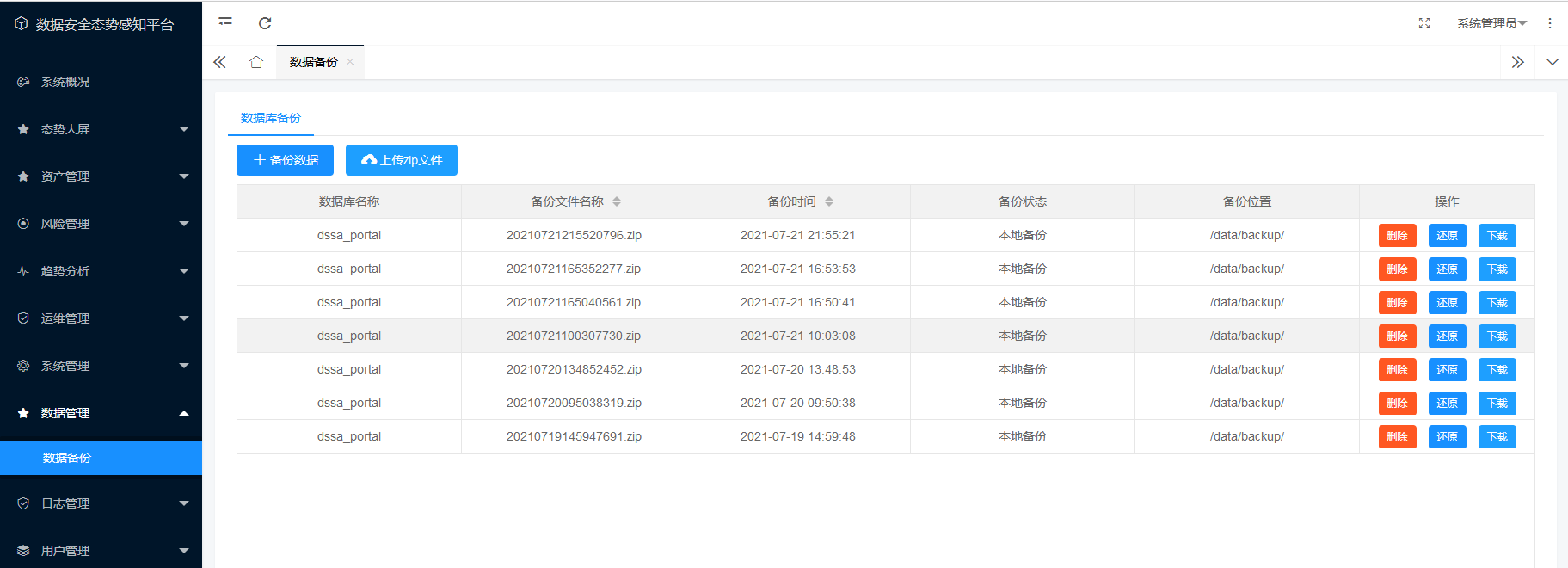
### DSSA平台升级





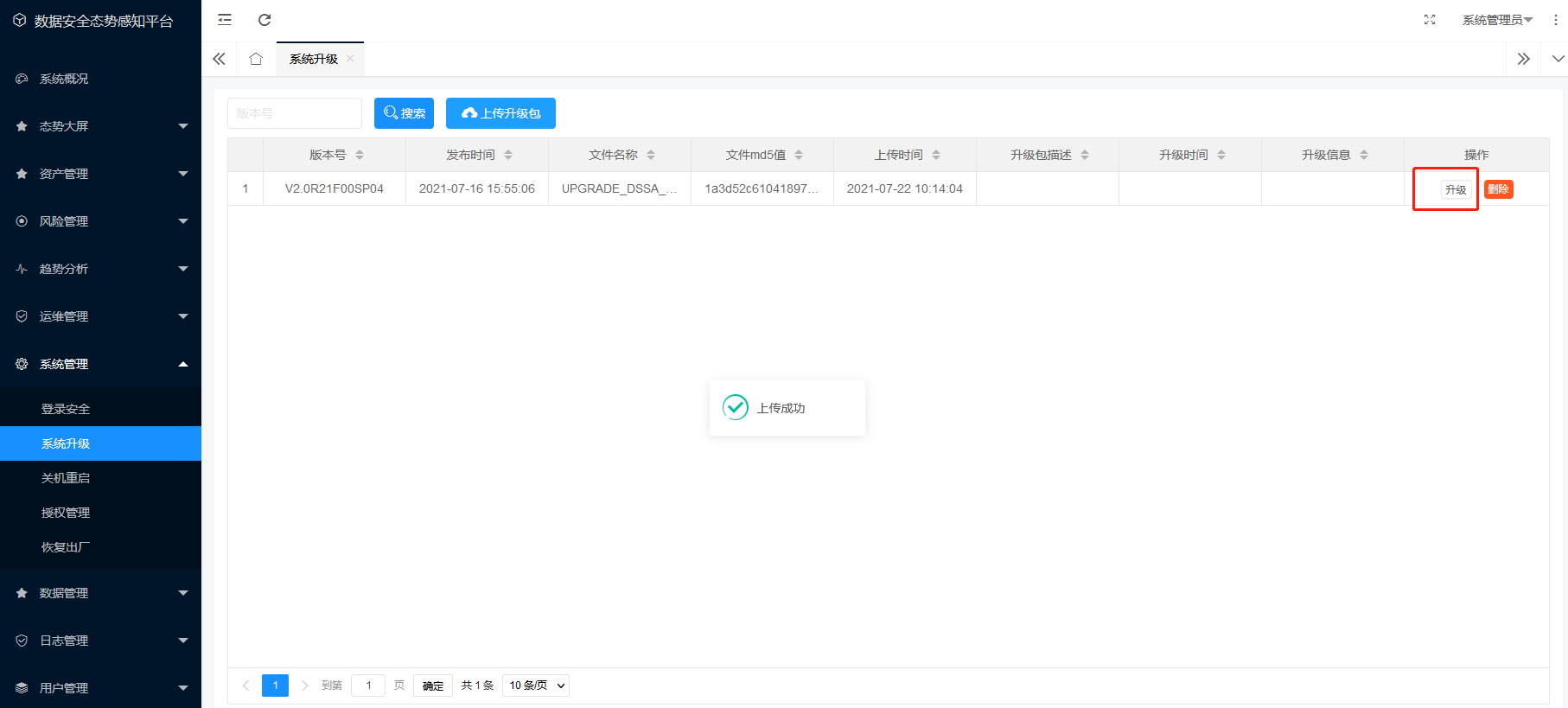
#### 数据库备份

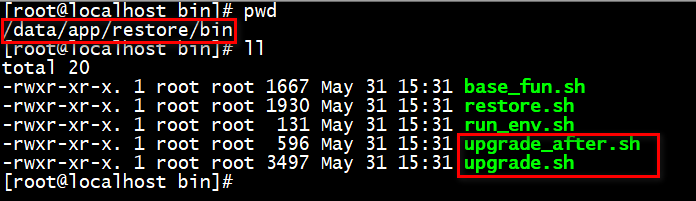
用户sysAdmin登陆平台，点击数据库备份菜单，然后再点击备份按钮完成数据库的备份。各个子系统备份，请参照子系统手册，现平台备份截图如下：



#### 平台升级

将升级包上传到服务器，让后点击【升级】按钮，可以完成升级，没执行升级可以删除，执行升级后不能删除。如下。





#### 启动程序

一般就是执行命令：/usr/local/dsec/bin/init.d/java\_dssa\_portal restart

具体解释请参考： “DSSA平台运维命令”章节（3.2.3）。

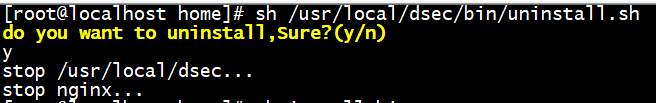
## DSSA平台卸载

### 卸载DSSA平台程序

注意：DSSA平台的所有程序都在/usr/local/dsec目录下，卸载后此文件夹下的所有文件都会被删除，请不要把重要的文件放入到/usr/local/dsec目录里或提前将该目录备份，防止卸载时文件被删除掉。

卸载DSSA平台程序的命令：

|  |
| --- |
| sh /usr/local/dsec/bin/uninstall.sh |



# 防火墙例外端口汇总

平台服务器

|  |  |
| --- | --- |
| **服务名称** | **端口号** |
| 平台WEB服务器默认端口 | 443、56000 |
| 数据库端口 | 3306 |
| Redis缓存服务 | 6379（备注：B090开始默认关闭此端口。仅当双机热备或复杂集群环境才需要开启。单机版系统无需开启） |
| Elasticsearch服务（简称ES） | 9200,9300 |

DSIP服务器

|  |  |
| --- | --- |
| **服务名称** | **端口号** |
| 平台WEB服务器默认端口 | 9090,9091,8080,8443 |
| 数据库端口 | 3306 |
| 终端服务器默认端口 | 5222 |
| FTP默认端口： | 2121 |
| Redis缓存服务 | 6379（备注：B090开始默认关闭此端口。仅当双机热备或复杂集群环境才需要开启。单机版系统无需开启） |
| Elasticsearch服务（简称ES） | 9200,9300 |
| rsync同步软件（平台与网络端同步算法学习结果） | 873 |

DAS服务器

|  |  |
| --- | --- |
| **服务名称** | **端口号** |
| 平台WEB服务器默认端口 | 8443 |
| 数据库端口 | 3306 |
| Redis缓存服务 | 6379（备注：B090开始默认关闭此端口。仅当双机热备或复杂集群环境才需要开启。单机版系统无需开启） |
| Elasticsearch服务（简称ES） | 9200,9300 |

NDLP服务器

|  |  |
| --- | --- |
| **服务名称** | **端口号** |
| 平台WEB服务器默认端口 | 8443 |
| 数据库端口 | 3306 |
| Redis缓存服务 | 6379（备注：B090开始默认关闭此端口。仅当双机热备或复杂集群环境才需要开启。单机版系统无需开启） |
| Elasticsearch服务（简称ES） | 9200,9300 |

照正常步骤安装后这些端口都是加到防火墙例外里的，不需要额外做什么处理。但是如果后期环境发生变化可以对比此表格排查是否防火墙原因。

除此以外，

1. 22端口要打开，这个是ssh远程连接服务使用的端口。这个端口是系统默认打开的，sip平台没有干预。

# 常见问题

## 平台默认的数据库root密码是多少？

可联系产品部支持人员或研发人员获取默认数据库密码。使用默认数据库密码，如更改默认数据库密码，需要对配置文件进行修改。

## 平台IP地址或者数据库密码变了，该怎么处理？

平台IP地址变化，子系统都需要修改/etc/hosts文件里面平台的地址。

## 终端DLP映射到外网需要修改什么吗？

1. 端口需要映射出去：8443、8080、9091、5222、2121、以及端口段如下

|  |  |  |
| --- | --- | --- |
| 端口号 | 协议 | 端口作用 |
| 20010至30020 | tcp | ftp被动模式开放的端口段，用于与客户端文件交互 |

2、修改组件列表的外网ip地址为实际的外网地址。sip平台重启。