

安装部署手册

业务中台之认证授权服务

- 修订历史

版本	作者	日期	备注
v1	刘洪青	2020-06-10	初稿
v1.4	刘洪青	2021-09-21	V1.4部署更新

安装部署手册

- 安装准备
 - MySQL 初始配置及相关基础命令
 - Harbor 准备及相关说明
 - Rancher 准备及相关说明
 - 域名准备
 - 应用配置项说明
 - 公共配置项
 - 服务配置项
- 开始安装
 - 数据库创建
 - rancher 容器部署
 - 数据配置

安装准备

MySQL 初始配置及相关基础命令

数据文件目录：/var/lib/mysql

- 安装完成后，调整 mysql 服务的配置参数
 - 查看当前配置：show variables;
 - 最大连接数 max_connections 操作日志的保留时长 binlog_expire_logs_seconds
 - 参考命令：

```
set global max_connections = 1000;
set persist max_connections = 1000;

// 7天 86400 * 7
// 1天 86400
set global binlog_expire_logs_seconds = 86400 * 7;
set persist binlog_expire_logs_seconds = 86400 * 7;
```

- 时区设置
 - 确保MySQL 的时区设置为 GMT+8
- 创建数据库帐号
 - 参考命令：

```
create user 'user'@'%' identified with mysql_native_password by 'your_password';
```

- 创建 database
 - 参考命令：

```
create database `user` DEFAULT CHARSET utf8 COLLATE utf8_general_ci;
```

- 授予权限

将 database 的权限授予对应的帐号

参考命令：

```
grant all privileges on `user`.* to 'user'@'%' with grant option;
```

- 授予 SUPER 权限 由于 部分帐号 需要创建 触发器，故，需要 SUPER 权限 涉及帐号有 user、user_authz、cas_server

参考命令：

```
grant SUPER on *.* to 'user'@'%';  
grant SUPER on *.* to 'user_authz'@'%';  
grant SUPER on *.* to 'cas_server'@'%';  
  
grant SUPER on *.* to 'tmp_data'@'%';
```

- 备份与还原

参考命令： 备份：

```
mysqldump -u root -p cas_server > cas_server.sql  
mysqldump -u root -p token_server > token_server.sql  
mysqldump -u root -p user > user.sql  
mysqldump -u root -p user_authz > user_authz.sql  
mysqldump -u root -p authx_log > authx_log.sql  
  
mysqldump -u root -p agent_service > agent_service.sql
```

还原：

```
mysql -u root -p cas_server < cas_server.sql  
mysql -u root -p token_server < token_server.sql  
mysql -u root -p user < user.sql  
mysql -u root -p user_authz < user_authz.sql  
mysql -u root -p authx_log < authx_log.sql  
  
mysql -u root -p agent_service < agent_service.sql
```

Harbor 准备及相关说明

- 创建 devops 帐号

用于 rancher 部署时拉取镜像

用户管理 下 创建用户 如 devops

- 镜像同步

从 <https://harbor.supwisdom.com> 中同步镜像（须申请 harbor 帐号）

仓库管理 下 新建目标

```
supwisdom      https://harbor.supwisdom.com      rancher.devops / PWMgP85qiLFC
```

同步管理 下 新建规则

admin-portal	admin-portal/*
authx-service	authx-service/*
authx-log	authx-log/*

thirdparty-agent-service	thirdparty-agent-service/*
user-data-service	goa/*
user-authorization-service	user-authorization-service/*
cas-server	cas-server/*
token-server	token-server/*
attest-server	attest-server/*
jobs-server	jobs-server/*
personal-security-center	personal-security-center/*

同步规则，创建完成后，进行镜像同步

选择某个同步规则，点击 同步，等待任务完成

- 授予 devops 帐号 对各个项目的 访客 权限

项目 下，点击 项目名称，进入到 成员，添加用户，查找用户 devops，选择角色 访客，确定，添加即可

Rancher 准备及相关说明

- 创建项目

进入 全局 - 集群（具体名称视项目安装而定） - 项目/命名空间，添加项目

输入 项目名称，保存

- 创建命名空间

进入 全局 - 集群（具体名称视项目安装而定） - 项目/命名空间

在新建的项目中，添加命名空间

输入 名称，保存

- 导入YAML

进入 全局 - 集群（具体名称视项目安装而定） - 项目（某个项目）

进入 资源 - 工作负载

域名准备

- 确定域名

首先明确是否使用泛域名，如： `*.paas.xxx.edu.cn`，或 直接使用学校域名 `xxx.edu.cn`

本产品安装需要的域名如下：

cas.paas.xxx.edu.cn	认证（视具体情况，可调整；包括，CAS 认证、Token 认证、身份验证服务）
token.paas.xxx.edu.cn	（废弃，合并至 cas）认证（APP适用）
personal-security-center.paas.xxx.edu.cn	（废弃，合并至 authx-service）个人安全中心后端API
security-center.paas.xxx.edu.cn	（废弃，合并至 authx-service）安全中心前端UI（帐号激活、忘记密码）
authx-service.paas.xxx.edu.cn	用户授权服务（包括，用户认证授权管理前端UI、安全中心前端UI、安全中心后端API）
authx-minio.paas.xxx.edu.cn	文件服务

如果使用 学校域名，则去除 .paas 即可，同时申请开通相关域名

应用配置项说明

公共配置项

- JVM 相关
ConfigMap, jvm-env

key	说明	配置示例
MAX_RAM_PERCENTAGE	JAVA 应用, JVM内存 占 POD内存的比例	75.0

- 数据库连接配置相关
Secret, datasource-env-secret

key	说明	配置示例
JDBC_URL	数据源连接配置 (base64加密)	amRiYzpteXNxbDovL215c3FsLXNlcnZlci5hdXRoeC1zZXJ2aWNlLnN2Yy5jbHVzdGVyLmxvY2FsOjMzMdYvdXNlcj9zZXJ2ZXJlUaW1lem9uZT1Bc2lhL1NoYW5naGFp
JDBC_USERNAME	数据库用户 (base64加密)	dXNlcg==
JDBC_PASSWORD	数据库密码 (base64加密)	a2luZ3N0YXl=

- redis 连接配置相关
Secret, redis-env-secret

key	说明	配置示例
SPRING_REDIS_HOST	redis 服务 (base64加密), 默认为 redis-server	cmVkaXMtc2VydmVy
SPRING_REDIS_PORT	redis 服务端口 (base64加密), 默认为 6379	NjM3OQ==
SPRING_REDIS_PASSWORD	redis 服务密码 (base64加密)	

- rabbit mq 连接配置相关
Secret, rabbitmq-env-secret

key	说明	配置示例
SPRING_RABBITMQ_HOST	rabbit mq 服务 (base64加密), 默认为 rabbitmq-server	cmFiYml0bXEtc2VydmVy
SPRING_RABBITMQ_PORT	rabbit mq 服务端口 (base64加密), 默认为 5672	NTYzMg==
SPRING_RABBITMQ_USERNAME	rabbit mq 服务用户 (base64加密)	
SPRING_RABBITMQ_PASSWORD	rabbit mq 服务密码 (base64加密)	

服务配置项

注: 外部访问地址, 一般为域名地址, 需要根据学校域名进行修改 k8s集群内部地址, 为集群内部, 跨namespace访问的域名地址, 一般无须修改

- auth-service 下的 authx-service-minio
Secret, minio-env-secret

key	说明	配置示例
MINIO_ACCESS_KEY	minio帐号 (base64加密), 默认为 1y8N@8R@a_2u	MXk4TkA4UkBhXzJ1
MINIO_SECRET_KEY	minio密钥 (base64加密), 默认为 8pxlle9#IN7Q	OHB4bEIIOsNsTjdR

- auth-service 下的 authx-service-bff
ConfigMap, authx-service-bff-env

key	说明	配置示例
UNIAUTH_BASIC_AUTH_USERNAME	uniauth sa basic 认证的 用户名	saadmin
UNIAUTH_BASIC_AUTH_PASSWORD	uniauth sa basic 认证的 密码	saadminfoobar
-	-	-
CASSERVER_SA_API_SERVER_URL	CAS认证服务管理接口地址（k8s集群内部地址）	http://cas-server-sa-api-svc.cas-server.svc.cluster.local:8080
USER_DATA_SERVICE_SERVER_URL	用户服务管理接口地址（k8s集群内部地址）	http://user-data-service-go-svc.user-data-service.svc.cluster.local:8080
USER_AUTHZ_SERVICE_SERVER_URL	授权服务管理接口地址（k8s集群内部地址）	http://user-authorization-sa-svc.user-authorization-service.svc.cluster.local:8080
UNIAUTH_SERVER_SA_API_SERVER_URL	Uniauth 管理接口地址（k8s集群内部地址）	http://uniauth-prod-backend.uniauth.svc.cluster.local:9090
TPAS_FILE_API_URL	文件服务接口地址（k8s集群内部地址） 默认：minio文件服务	http://agent-service-svc.thirdparty-agent-service.svc.cluster.local:8080/api/v1/tpas/file/minio
-	-	-
AUTHX_LOG_ENABLED	是否开启日志推送	true
AUTHX_LOG_RABBITMQ_HOST	rabbit mq 服务地址（k8s集群内部地址）	rabbitmq-server.authx-service.svc.cluster.local
AUTHX_LOG_RABBITMQ_PORT	rabbit mq 服务端口	5672
AUTHX_LOG_RABBITMQ_USERNAME	rabbit mq 服务用户	
AUTHX_LOG_RABBITMQ_PASSWORD	rabbit mq 服务密码	

- thirdparty-agent-service 下的 thirdparty-agent-service

ConfigMap, agent-service-env

key	说明	配置示例
FILE_MINIO_AUTOCONFIGURE_ENABLED	minio 服务开启开关	true、false
FILE_MINIO_ENDPOINT	minio 服务地址（k8s集群内部地址）	http://minio-svc.authx-service.svc.cluster.local:9000
-	-	-
MAIL_SMTP_AUTOCONFIGURE_ENABLED	smtp 服务开启开关	true、false
MAIL_SMTP_HOST	smtp 服务地址	smtp.mxhichina.com
MAIL_SMTP_PORT	smtp 服务端口	25
MAIL_SMTP_SECURE_MODE	smtp 服务的安全模式（NONE，无；SSL，安全）	NONE
MAIL_SMTP_USERNAME	smtp 服务帐号	security.institute@supwisdom.com
MAIL_SMTP_PASSWORD	smtp 服务密码	Security2019
MAIL_SMTP_FROM	发件人邮箱	security.institute@supwisdom.com
MAIL_SMTP_FROM_PERSONAL	发件人名称	智慧校园
-	-	-
SMS_ALIYUN_AUTOCONFIGURE_ENABLED	阿里云短信服务开启开关	true、false
SMS_ALIYUN_REGION_ID	区域	cn-hangzhou
SMS_ALIYUN_ACCESS_KEY_ID	阿里云短信服务的帐号	
SMS_ALIYUN_ACCESS_SECRET	阿里云短信服务的密钥	
-	-	-
FACE_AIFACE_AUTOCONFIGURE_ENABLED	新开普人脸开启开关	true、false
FACE_AIFACE_URL	新开普人脸地址	
FACE_AIFACE_APPKEY	app key	
FACE_AIFACE_APPSECRET	app secret	
FACE_AIFACE_SECRETKEY	secret key	
FACE_AIFACE_TERM_CODE	term code	
-	-	-
FACE_AIPFACE_AUTOCONFIGURE_ENABLED	百度人脸开启开关	true、false
FACE_AIPFACE_APPID	app id	
FACE_AIPFACE_APIKEY	app key	
FACE_AIPFACE_SECRETKEY	secret key	
FACE_AIPFACE_GROUPIDLIST	组ID，多个用逗号分隔，最多20个	

Secret, agent-service-env-secret

key	说明	配置示例
FILE_MINIO_ACCESSKEY	minio 服务帐号（base64加密），默认为 1y8N@8R@a_2u	MXk4TkA4UkBhXzJ1
FILE_MINIO_SECRETKEY	minio 服务密钥（base64加密），默认为 8pxlle9#IN7Q	OHB4bEIIOsNsTjdR

- user-data-service 下的 user-data-service-poa
ConfigMap, user-data-service-poa-env

key	说明	配置示例
CASSERVER_SA_API_SERVER_URL	CAS认证服务管理接口地址（k8s集群内部地址）	http://cas-server-sa-api-svc.cas-server.svc.cluster.local:8080
-	-	-
TPAS_FILE_API_URL	文件服务接口地址（k8s集群内部地址） 默认：minio文件服务	http://agent-service-svc.thirdparty-agent-service.svc.cluster.local:8080/api/v1/tpas/file/minio
-	-	-
FILE_SERVER_TYPE	文件服务类型	minio
FILE_SERVER_URL	文件服务地址（外网地址）	https://authx-minio.paas.xxx.edu.cn
-	-	-
AUTHX_LOG_ENABLED	是否开启日志推送	true
AUTHX_LOG_RABBITMQ_HOST	rabbit mq 服务地址（k8s集群内部地址）	rabbitmq-server.authx-service.svc.cluster.local
AUTHX_LOG_RABBITMQ_PORT	rabbit mq 服务端口	5672
AUTHX_LOG_RABBITMQ_USERNAME	rabbit mq 服务用户	
AUTHX_LOG_RABBITMQ_PASSWORD	rabbit mq 服务密码	

- user-data-service 下的 user-data-service-go

ConfigMap, user-data-service-go-env

key	说明	配置示例
PASSWORD_ENCODER_IMPL	密码加密算法的实现 default: 支持 bcrypt 等加密算法，默认； SHA-256: 支持 SHA-256 加密算法	default、SHA-256
-	-	-
JOBS_RABBITMQ_ENABLED	是否推送数据到 jobs-server 的 rabbit mq	true、false
JOBS_RABBITMQ_HOST	rabbit mq 服务地址（k8s集群内部地址）	rabbitmq-server.jobs-server.svc.cluster.local
JOBS_RABBITMQ_PORT	rabbit mq 服务端口	5672
JOBS_RABBITMQ_USERNAME	rabbit mq 服务用户	
JOBS_RABBITMQ_PASSWORD	rabbit mq 服务密码	
JOBS_RABBITMQ_ACCOUNTUSERSVC2JOBSRABBITSENDER_ENABLED	是否同步帐号数据至 jobs 的 MQ	true、false
JOBS_RABBITMQ_ACCOUNTUSERSVC2JOBSYNCPASSWORDRABBITSENDER_ENABLED	是否同步密码（明文密码）到 jobs 的 MQ	true、false
JOBS_RABBITMQ_ORGANIZATIONUSERSVC2JOBSRABBITSENDER_ENABLED	是否同步组织机构数据至 jobs 的 MQ	true、false
JOBS_RABBITMQ_GROUPUSERSVC2JOBSRABBITSENDER_ENABLED	是否同步用户组数据至 jobs 的 MQ	true、false
-	-	-
AUTHX_LOG_ENABLED	是否开启日志推送	true
AUTHX_LOG_RABBITMQ_HOST	rabbit mq 服务地址（k8s集群内部地址）	rabbitmq-server.authx-service.svc.cluster.local
AUTHX_LOG_RABBITMQ_PORT	rabbit mq 服务端口	5672
AUTHX_LOG_RABBITMQ_USERNAME	rabbit mq 服务用户	
AUTHX_LOG_RABBITMQ_PASSWORD	rabbit mq 服务密码	

- user-data-service 下的 user-data-service-biz

ConfigMap, user-data-service-biz-env

key	说明	配置示例
CASSERVER_SA_API_SERVER_URL	CAS认证服务管理接口地址（k8s集群内部地址）	http://cas-server-sa-api-svc.cas-server.svc.cluster.local:8080
-	-	-
USER_AUTHZ_SERVICE_SERVER_URL	授权服务管理接口地址（k8s集群内部地址）	http://user-authorization-sa-svc.user-authorization-service.svc.cluster.local:8080
-	-	-
TPAS_FILE_API_URL	文件服务接口地址（k8s集群内部地址） 默认：minio文件服务	http://agent-service-svc.thirdparty-agent-service.svc.cluster.local:8080/api/v1/tpas/file/minio
-	-	-
AUTHX_LOG_ENABLED	是否开启日志推送	true
AUTHX_LOG_RABBITMQ_HOST	rabbit mq 服务地址（k8s集群内部地址）	rabbitmq-server.authx-service.svc.cluster.local
AUTHX_LOG_RABBITMQ_PORT	rabbit mq 服务端口	5672
AUTHX_LOG_RABBITMQ_USERNAME	rabbit mq 服务用户	
AUTHX_LOG_RABBITMQ_PASSWORD	rabbit mq 服务密码	

- user-authorization-service 下的 user-authorization-service-poa
ConfigMap, user-authorization-service-poa-env

key	说明	配置示例
USER_DATA_SERVICE_SERVER_URL	用户服务管理接口地址（k8s集群内部地址）	http://user-data-service-goa-svc.user-data-service.svc.cluster.local:8080
-	-	-
AUTHX_LOG_ENABLED	是否开启日志推送	true
AUTHX_LOG_RABBITMQ_HOST	rabbit mq 服务地址（k8s集群内部地址）	rabbitmq-server.authx-service.svc.cluster.local
AUTHX_LOG_RABBITMQ_PORT	rabbit mq 服务端口	5672
AUTHX_LOG_RABBITMQ_USERNAME	rabbit mq 服务用户	
AUTHX_LOG_RABBITMQ_PASSWORD	rabbit mq 服务密码	

- user-authorization-service 下的 user-authorization-service-sa
ConfigMap, user-authorization-service-sa-env

key	说明	配置示例
USER_AUTHORIZATION_SA_USER_RABBITMQ_CONSUMER_ENABLED	是否开启用户数据订阅	true
USER_AUTHORIZATION_SA_USER_RABBITMQ_HOST	rabbit mq 服务地址（k8s集群内部地址）	rabbitmq-server.authx-service.svc.cluster.local
USER_AUTHORIZATION_SA_USER_RABBITMQ_PORT	rabbit mq 服务端口	5672
USER_AUTHORIZATION_SA_USER_RABBITMQ_USERNAME	rabbit mq 服务用户	
USER_AUTHORIZATION_SA_USER_RABBITMQ_PASSWORD	rabbit mq 服务密码	
-	-	-
AUTHX_LOG_ENABLED	是否开启日志推送	true
AUTHX_LOG_RABBITMQ_HOST	rabbit mq 服务地址（k8s集群内部地址）	rabbitmq-server.authx-service.svc.cluster.local
AUTHX_LOG_RABBITMQ_PORT	rabbit mq 服务端口	5672
AUTHX_LOG_RABBITMQ_USERNAME	rabbit mq 服务用户	
AUTHX_LOG_RABBITMQ_PASSWORD	rabbit mq 服务密码	

- cas-server 下的 cas-server-sa-api
ConfigMap, cas-server-sa-api-env

key	说明	配置示例
SERVICE_REFRESH_REDIS_TIMER_ENABLED	是否定时刷新应用对接数据 默认: true	true、false
ACCOUNT_REFRESH_REDIS_TIMER_ENABLED	是否定时刷新帐号数据 默认: false	true、false
FEDERATION_REFRESH_REDIS_TIMER_ENABLED	是否定时刷新联合登录帐号绑定数据 默认: true	true、false
-	-	-
USER_DATA_SERVICE_SA_API_SERVER_URL	用户服务管理接口地址 (k8s集群内部地址)	http://user-data-service-go-a-svc.user-data-service.svc.cluster.local:8080
-	-	-
AUTHX_LOG_ENABLED	是否开启日志推送	true
AUTHX_LOG_RABBITMQ_HOST	rabbit mq 服务地址 (k8s集群内部地址)	rabbitmq-server.authx-service.svc.cluster.local
AUTHX_LOG_RABBITMQ_PORT	rabbit mq 服务端口	5672
AUTHX_LOG_RABBITMQ_USERNAME	rabbit mq 服务用户	
AUTHX_LOG_RABBITMQ_PASSWORD	rabbit mq 服务密码	

- cas-server 下的 cas-server-security-engine
ConfigMap, cas-server-security-engine-env

key	说明	配置示例
CASSERVER_SA_API_SERVER_URL	CAS认证服务开放接口地址 (k8s集群内部地址)	http://cas-server-sa-api-svc.cas-server.svc.cluster.local:8080

- cas-server 下的 cas-server-site-webapp
ConfigMap, cas-server-site-webapp-env

key	说明	配置示例
LOGGING_CONFIG	日志配置文件路径	file:/etc/cas/log4j2-file.xml
-	-	-
CAS_SERVER_NAME	CAS认证地址 (外部访问地址)	https://cas.paas.xxx.edu.cn
CAS_TGC_SECURE	TGC cookie 安全设置 true: https安全 false:	true、false
CAS_TICKET_TGT_MAX_TIME_TO_LIVE_IN_SECONDS	TGT的最大生命周期 默认: 14天	1209600
CAS_TICKET_TGT_TIME_TO_KILL_IN_SECONDS	TGT的失效时长 默认: 2天	172800
CAS_AUTHN_TOKEN_CRYPTO_SIGNING_KEY	jwt格式的ticket的签名密钥	(@<rhnpaUYKC_k770*DuWwYQ_#Zc#8c(2rB?kae)rN)>K7qy)awCjxp\$L653Mf\$2
SPRING_THYMELEAF_PREFIX	登录页面UI的代码目录	classpath:/templates/themes/classic/
-	-	-
CASSERVER_JWT_ISS	idToken 签发者标识	cas.paas.xxx.edu.cn
CASSERVER_JWT_PRIVATE_KEY_PEM_PKCS8	idToken 签名私钥 (pkcs8), 参考 certs/jwt/readme.md 生成公私钥pem	
CASSERVER_JWT_PUBLIC_KEY_PEM	idToken 签名公钥, 参考 certs/jwt/readme.md 生成公私钥pem	
-	-	-
CASSERVERSITE_CAPTCHA_ENABLED	是否启用登录验证码	true、false
CASSERVERSITE_ACCOUNT_SERVICE_IMPL	帐号服务的实现 redis: 帐号数据存放在redis中 user-sa: 帐号数据从用户服务获取	user-sa
CASSERVERSITE_ROLE_SERVICE_IMPL	角色服务的实现 redis: 角色数据存放在redis中 user-authz-sa: 角色数据从授权服务获取	user-authz-sa
CASSERVERSITE_SMS_SENDER_IMPL	动态密码的短信发送实现 default: 控制台输出 agent-service: 代理服务	agent-service
CASSERVERSITE_PASSWORDLESS_TOKEN_EXPIRATION_IN_SECONDS	动态密码失效时长 默认: 5分钟	300
CASSERVERSITE_PASSWORDLESS_SMS_FROM	动态密码的短信发送者	认证中心
CASSERVERSITE_PASSWORDLESS_SMS_TEXT_TEMPLATE	动态密码的短信模板	【认证中心】您正在登录统一身份认证, 本次登录的动态密码为

		{token}, 有效期5分钟, 请尽快完成登录。
-	-	-
SUPERAPP_TOKEN_SIGNING_KEY_URL	TOKEN认证验证签公钥地址 (k8s集群内部地址)	http://token-server-svc.token-server.svc.cluster.local:8080/token/jwt/publicKey
-	-	-
TPAS_AGENT_SERVICE_SERVER_URL	代理服务接口地址 (k8s集群内部地址)	http://agent-service-svc.thirdparty-agent-service.svc.cluster.local:8080
TPAS_AGENT_SERVICE_SMS_SENDER_PATH	短信发送服务地址 console: 控制台输出, 默认 aliyun: 阿里云短信服务 其他, 支持学校定制接口	/api/v1/tpas/sms/console/send
TPAS_AGENT_SERVICE_FILE_PATH	文件服务地址 默认: minio文件服务	/api/v1/tpas/file/minio
-	-	-
CASSERVER_SA_API_SERVER_URL	CAS认证服务管理接口地址 (k8s集群内部地址)	http://cas-server-sa-api-svc.cas-server.svc.cluster.local:8080
-	-	-
USER_DATA_SERVICE_SA_API_SERVER_URL	用户服务管理接口地址 (k8s集群内部地址)	http://user-data-service-go-a-svc.user-data-service.svc.cluster.local:8080
-	-	-
USER_AUTHZ_SERVICE_SA_API_SERVER_URL	授权服务管理接口地址 (k8s集群内部地址)	http://user-authorization-sa-svc.user-authorization-service.svc.cluster.local:8080
-	-	-
ATTEST_SERVER_URL	身份验证服务地址 (k8s集群内部地址)	http://attest-server-svc.attest-server.svc.cluster.local:8080/attest
-	-	-
IPADDR_SERVER_URL	IP地址服务	http://ipaddr.ipaddr.svc.cluster.local:9090
-	-	-
AUTHX_LOG_ENABLED	是否开启日志推送	true
AUTHX_LOG_RABBITMQ_HOST	rabbit mq 服务地址 (k8s集群内部地址)	rabbitmq-server.authx-service.svc.cluster.local
AUTHX_LOG_RABBITMQ_PORT	rabbit mq 服务端口	5672
AUTHX_LOG_RABBITMQ_USERNAME	rabbit mq 服务用户	
AUTHX_LOG_RABBITMQ_PASSWORD	rabbit mq 服务密码	

- cas-server 下的 cas-server-site-scheme

ConfigMap, cas-server-site-scheme-config

key	说明	配置示例
SCHEME_COLOR	UI 主题色	409EFF
-	-	-
CASSERVER_SA_API_SERVER_URL	CAS认证服务开放接口地址 (k8s集群内部地址)	http://cas-server-sa-api-svc.cas-server.svc.cluster.local:8080

注: 若配置了 CASSERVER_SA_API_SERVER_URL, 则使用配置表中的配置; 否则, 使用 SCHEME_COLOR 指定的设置。

- token-server 下的 token-server

ConfigMap, token-server-env

key	说明	配置示例
TOKEN_SERVER_PREFIX	TOKEN认证地址 (外部访问地址)	https://token.paas.xxx.edu.cn/token
-	-	-
TOKEN_SERVER_SECURITY_JWT_ISS	idToken签发者标识	token.paas.xxx.edu.cn
TOKEN_SERVER_SECURITY_JWT_EXPIRATION	idToken 失效时长 默认: 30天	2592000
TOKEN_SERVER_SECURITY_JWT_PRIVATE_KEY_PEM_PKCS8	idToken 签名私钥 (pkcs8), 参考 certs/jwt/readme.md 生成公私钥pem 可以与CAS认证一致	
TOKEN_SERVER_SECURITY_JWT_PUBLIC_KEY_PEM	idToken 签名公钥, 参考 certs/jwt/readme.md 生成公私钥pem 可以与CAS认证一致	
-	-	-
TOKEN_SERVER_FACE_SOURCE_TYPE	人脸服务 aiface: 新开普人脸	aiface

	aipface：百度人脸	
若须对接新开普人脸，须由新开普人脸系统提供相关配置		
TOKEN_SERVER_FACE_AIFACE_URL		
TOKEN_SERVER_FACE_AIFACE_APPKEY		
TOKEN_SERVER_FACE_AIFACE_APPSECRET		
TOKEN_SERVER_FACE_AIFACE_SECRETKEY		
TOKEN_SERVER_FACE_AIFACE_TERM_CODE		
若须对接百度人脸，须在百度开放平台注册应用		
TOKEN_SERVER_FACE_AIPFACE_APPID		
TOKEN_SERVER_FACE_AIPFACE_APIKEY		
TOKEN_SERVER_FACE_AIPFACE_SECRETKEY		
-	-	-
TOKEN_SERVER_PASSWORDLESS_TOKEN_EXPIRATION_IN_SECONDS	动态密码失效时长 默认：5分钟	300
TOKEN_SERVER_PASSWORDLESS_SMS_TEXT_TEMPLATE	动态密码的短信模板	【认证中心】您正在登录统一身份认证，本次登录的动态密码为{token}，有效期5分钟，请尽快完成登录。
TOKEN_SERVER_PASSWORDLESS_SMS_FROM	动态密码的短信发送者	认证中心
-	-	-
GETUI_SERVER_URL	个推服务地址	https://openapi-gy.getui.com
GETUI_GEGAN_APP_ID	个推，个验 app id	
GETUI_GEGAN_APP_KEY	个推，个验 app key	
GETUI_GEGAN_APP_SECRET	个推，个验 app secret	
GETUI_GEGAN_MASTER_SECRET	个推，个验 master secret	
-	-	-
MESSAGECENTER_ENABLED	是否对接消息平台 默认：false	true、false
MESSAGECENTER_APP_ID	应用ID（由消息平台生成）	
MESSAGECENTER_MESSAGE_TYPE_CODE_APP_LOGIN	消息类型代码，APP 登录	APP_LOGIN
MESSAGECENTER_MESSAGE_TYPE_CODE_PASSWORD	消息类型代码，密码修改登出	PASSWORD
MESSAGECENTER_MESSAGE_TYPE_CODE_APPPUSH	消息类型代码，消息推送	APPPUSH
-	-	-
POA_SERVER_URL	POA网关地址（外部访问地址）	https://poa.paas.xxx.edu.cn
POA_CLIENT_ID	client id	
POA_CLIENT_SECRET	client secret	
POA_SCOPES	api 接口的 scope	messagecenter:v1:sendMessage
-	-	-
TPAS_AGENT_SERVICE_SERVER_URL	代理服务接口地址（k8s集群内部地址）	http://agent-service-svc.thirdparty-agent-service.svc.cluster.local:8080
TPAS_AGENT_SERVICE_SMS_SENDER_PATH	短信发送服务地址 console：控制台输出，默认 aliyun：阿里云短信服务 其他，支持学校定制接口	/api/v1/tpas/sms/console/send
-	-	-
CASSERVER_SA_API_SERVER_URL	CAS认证服务管理接口地址（k8s集群内部地址）	http://cas-server-sa-api-svc.cas-server.svc.cluster.local:8080
-	-	-
USER_DATA_SERVICE_SA_API_SERVER_URL	用户服务管理接口地址（k8s集群内部地址）	http://user-data-service-go-a-svc.user-data-service.svc.cluster.local:8080
-	-	-
ATTEST_SERVER_URL	身份验证服务地址（k8s集群内部地址）	http://attest-server-svc.attest-server.svc.cluster.local:8080/attest
-	-	-
IPADDR_SERVER_URL	IP地址服务	http://ipaddr.ipaddr.svc.cluster.local:9090
-	-	-
AUTHX_LOG_ENABLED	是否开启日志推送	true
AUTHX_LOG_RABBITMQ_HOST	rabbit mq 服务地址（k8s集群内部地址）	rabbitmq-server.authx-service.svc.cluster.local
AUTHX_LOG_RABBITMQ_PORT	rabbit mq 服务端口	5672
AUTHX_LOG_RABBITMQ_USERNAME	rabbit mq 服务用户	
AUTHX_LOG_RABBITMQ_PASSWORD	rabbit mq 服务密码	
-	-	-
USER_RABBITMQ_ENABLED	是否开启用户数据的消息接收	true
USER_RABBITMQ_HOST	rabbit mq 服务地址（k8s集群内部地址）	rabbitmq-server.authx-service.svc.cluster.local

USER_RABBITMQ_PORT	rabbit mq 服务端口	5672
USER_RABBITMQ_USERNAME	rabbit mq 服务用户	
USER_RABBITMQ_PASSWORD	rabbit mq 服务密码	
USER_RABBITMQ_CONSUMER_ENABLED	是否开启用户数据订阅	true

- personal-security-center 下的 personal-security-center-bff

ConfigMap, personal-security-center-bff-env

key	说明	配置示例
PERSONAL_SECURITY_CENTER_SERVER_PREFIX	个人安全中心访问地址（外部访问地址）	https://authx-service.paas.xxx.edu.cn/personal
CAS_SERVER_PREFIX	CAS认证地址（外部访问地址）	https://cas.paas.xxx.edu.cn/cas
-	-	-
CASSERVER_SITE_SERVER_URL	CAS认证接口地址（k8s集群内部地址）	http://cas-server-site-webapp-svc.cas-server.svc.cluster.local:8080/cas
-	-	-
CASSERVER_SA_API_SERVER_URL	CAS认证服务管理接口地址（k8s集群内部地址）	http://cas-server-sa-api-svc.cas-server.svc.cluster.local:8080
-	-	-
USER_DATA_SERVICE_SA_API_SERVER_URL	用户服务开放接口地址（k8s集群内部地址）	http://user-data-service-goa-svc.user-data-service.svc.cluster.local:8080
-	-	-
TPAS_FILE_API_URL	文件服务接口地址（k8s集群内部地址） 默认：minio文件服务	http://agent-service-svc.thirdparty-agent-service.svc.cluster.local:8080/api/v1/tpas/file/minio
TPAS_MAIL_API_URL	邮件发送服务地址（k8s集群内部地址） console：控制台输出，默认 smtp：SMTP服务 其他，支持学校定制接口	http://agent-service-svc.thirdparty-agent-service.svc.cluster.local:8080/api/v1/tpas/mail/smtp
TPAS_SMS_API_URL	短信发送服务地址（k8s集群内部地址） console：控制台输出，默认 aliyun：阿里云短信服务 其他，支持学校定制接口	http://agent-service-svc.thirdparty-agent-service.svc.cluster.local:8080/api/v1/tpas/sms/console
-	-	-
AUTHX_LOG_ENABLED	是否开启日志推送	true
AUTHX_LOG_RABBITMQ_HOST	rabbit mq 服务地址（k8s集群内部地址）	rabbitmq-server.authx-service.svc.cluster.local
AUTHX_LOG_RABBITMQ_PORT	rabbit mq 服务端口	5672
AUTHX_LOG_RABBITMQ_USERNAME	rabbit mq 服务用户	
AUTHX_LOG_RABBITMQ_PASSWORD	rabbit mq 服务密码	

ConfigMap, personal-security-center-bff-template-env 邮件内容模板、短信内容模板

key	说明	配置示例
EMAIL_TEMPLATE_ACTIVE_USER_SEND_CODE_BY_EMAIL_ADDRESS	邮件内容模板-激活帐号	{name}：您正在激活帐号，须验证邮箱有效，验证码{code}，有效期5分钟，请尽快完成验证。
EMAIL_TEMPLATE_FORGOT_PASSWORD_SEND_CODE	邮件内容模板-找回密码	{name}：您正在找回密码，须验证身份，验证码{code}，有效期5分钟，请尽快完成验证。
-	-	-
EMAIL_TEMPLATE_USER_SECURITY_PASSWORD_SEND_CODE	邮件内容模板-修改密码	{name}：您正在修改密码，须验证身份，验证码{code}，有效期5分钟，请尽快完成验证。
EMAIL_TEMPLATE_USER_SECURITY_EMAIL_ADDRESS_SEND_CODE	邮件内容模板-修改安全邮箱	{name}：您正在修改安全邮箱，须验证身份，验证码{code}，有效期5分钟，请尽快完成验证。
EMAIL_TEMPLATE_USER_SECURITY_EMAIL_ADDRESS_SEND_CODE_BY_EMAIL_ADDRESS	邮件内容模板-修改安全邮箱-验证邮箱	{name}：您正在修改安全邮箱，须验证邮箱有效，验证码{code}，有效期5分钟，请尽快完成验证。
EMAIL_TEMPLATE_USER_SECURITY_MOBILE_SEND_CODE	邮件内容模板-修改安全手机	{name}：您正在修改安全手机，须验证身份，验证码{code}，有效期5分钟，请尽快完成验证。
-	-	-
EMAIL_TEMPLATE_USER_FEDERATION_QQ_SEND_CODE	邮件内容模板-绑定QQ	{name}：您正在绑定QQ，须验证身份，验证码{code}，有效期5分钟，请尽快完成验证。
EMAIL_TEMPLATE_USER_FEDERATION_QQ_SEND_CODE_UNBIND_QQ	邮件内容模板-解绑QQ	{name}：您正在解绑QQ，须验证身份，验证码{code}，有效期5分钟，请尽快完成验证。
EMAIL_TEMPLATE_USER_FEDERATION_OPENWEIXIN_SEND_CODE	邮件内容模板-绑定微信	{name}：您正在绑定微信，须验证身份，验证码{code}，有效期5分钟，请尽快完成验证。
EMAIL_TEMPLATE_USER_FEDERATION_OPENWEIXIN_SEND_CODE_UNBIND_OPENWEIXIN	邮件内容模板-解绑微信	{name}：您正在解绑微信，须验证身份，验证码{code}，有效期5分钟，请尽快完成验证。

EMAIL_TEMPLATE_USER_FEDERATION_WORKWEIXIN_SEND_CODE	邮件内容模板-绑定企业微信	{name}: 您正在绑定企业微信, 须验证身份, 验证码{code}, 有效期5分钟, 请尽快完成验证。
EMAIL_TEMPLATE_USER_FEDERATION_WORKWEIXIN_SEND_CODE_UNBIND_WORKWEIXIN	邮件内容模板-解绑企业微信	{name}: 您正在解绑企业微信, 须验证身份, 验证码{code}, 有效期5分钟, 请尽快完成验证。
EMAIL_TEMPLATE_USER_FEDERATION_ALIPAY_SEND_CODE	邮件内容模板-绑定支付宝	{name}: 您正在绑定支付宝, 须验证身份, 验证码{code}, 有效期5分钟, 请尽快完成验证。
EMAIL_TEMPLATE_USER_FEDERATION_ALIPAY_SEND_CODE_UNBIND_ALIPAY	邮件内容模板-解绑支付宝	{name}: 您正在解绑支付宝, 须验证身份, 验证码{code}, 有效期5分钟, 请尽快完成验证。
-	-	-
SMS_TEMPLATE_ACTIVE_USER_SEND_CODE_BY_PRE_MOBILE	短信内容模板-激活帐号-预留手机身份验证	{prefix}您正在激活帐号, 须验证身份, 验证码{code}, 有效期5分钟, 请尽快完成验证。
SMS_TEMPLATE_ACTIVE_USER_SEND_CODE_BY_MOBILE	短信内容模板-激活帐号	{prefix}您正在激活帐号, 须验证手机有效, 验证码{code}, 有效期5分钟, 请尽快完成验证。
SMS_TEMPLATE_FORGOT_PASSWORD_SEND_CODE	短信内容模板-找回密码	{prefix}您正在找回密码, 须验证身份, 验证码{code}, 有效期5分钟, 请尽快完成验证。
-	-	-
SMS_TEMPLATE_USER_SECURITY_PASSWORD_SEND_CODE	短信内容模板-修改密码	{prefix}您正在修改密码, 须验证身份, 验证码{code}, 有效期5分钟, 请尽快完成验证。
SMS_TEMPLATE_USER_SECURITY_EMAIL_ADDRESS_SEND_CODE	短信内容模板-修改安全邮箱	{prefix}您正在修改安全邮箱, 须验证身份, 验证码{code}, 有效期5分钟, 请尽快完成验证。
SMS_TEMPLATE_USER_SECURITY_MOBILE_SEND_CODE	短信内容模板-修改安全手机	{prefix}您正在修改安全手机, 须验证身份, 验证码{code}, 有效期5分钟, 请尽快完成验证。
SMS_TEMPLATE_USER_SECURITY_MOBILE_SEND_CODE_BY_MOBILE	短信内容模板-修改安全手机-验证手机	{prefix}您正在修改安全手机, 须验证手机有效, 验证码{code}, 有效期5分钟, 请尽快完成验证。
-	-	-
SMS_TEMPLATE_USER_FEDERATION_QQ_SEND_CODE	邮件内容模板-绑定QQ	{prefix}您正在绑定QQ, 须验证身份, 验证码{code}, 有效期5分钟, 请尽快完成验证。
SMS_TEMPLATE_USER_FEDERATION_QQ_SEND_CODE_UNBIND_QQ	邮件内容模板-解绑QQ	{prefix}您正在解绑QQ, 须验证身份, 验证码{code}, 有效期5分钟, 请尽快完成验证。
SMS_TEMPLATE_USER_FEDERATION_OPENWEIXIN_SEND_CODE	邮件内容模板-绑定微信	{prefix}您正在绑定微信, 须验证身份, 验证码{code}, 有效期5分钟, 请尽快完成验证。
SMS_TEMPLATE_USER_FEDERATION_OPENWEIXIN_SEND_CODE_UNBIND_OPENWEIXIN	邮件内容模板-解绑微信	{prefix}您正在解绑微信, 须验证身份, 验证码{code}, 有效期5分钟, 请尽快完成验证。
SMS_TEMPLATE_USER_FEDERATION_WORKWEIXIN_SEND_CODE	邮件内容模板-绑定企业微信	{prefix}您正在绑定企业微信, 须验证身份, 验证码{code}, 有效期5分钟, 请尽快完成验证。
SMS_TEMPLATE_USER_FEDERATION_WORKWEIXIN_SEND_CODE_UNBIND_WORKWEIXIN	邮件内容模板-解绑企业微信	{prefix}您正在解绑企业微信, 须验证身份, 验证码{code}, 有效期5分钟, 请尽快完成验证。
SMS_TEMPLATE_USER_FEDERATION_ALIPAY_SEND_CODE	邮件内容模板-绑定支付宝	{prefix}您正在绑定支付宝, 须验证身份, 验证码{code}, 有效期5分钟, 请尽快完成验证。
SMS_TEMPLATE_USER_FEDERATION_ALIPAY_SEND_CODE_UNBIND_ALIPAY	邮件内容模板-解绑支付宝	{prefix}您正在解绑支付宝, 须验证身份, 验证码{code}, 有效期5分钟, 请尽快完成验证。
-	-	-
SMS_TEMPLATE_ACCOUNT_INFO_SEND_CODE_BY_MOBILE	帐号查询-验证手机	{prefix}您当前正在查询账号, 须验证手机有效, 验证码{code}, 有效期5分钟, 请尽快完成验证。'
SMS_TEMPLATE_ACCOUNT_INFO_SEND_ACCOUNT_NAME	帐号查询-发送帐号名	{prefix}您当前正在查询账号, 查询结果为: {accountName}, 账号是您在学校中的重要信息, 请妥善保管。'
-	-	-
SMS_TEMPLATE_PREFIX	短信签名、前缀	

- personal-security-center 下的 personal-security-center-zuul ConfigMap, personal-security-center-zuul-env

key	说明	配置示例
APP_SERVER_HOST_URL	个人安全中心访问地址（外部访问地址）	https://authx-service.paas.xxx.edu.cn/personal
CAS_SERVER_HOST_URL	CAS认证地址（外部访问地址）	https://cas.paas.xxx.edu.cn/cas
-	-	-
APPLICATION_INDEX_REDIRECT_URI	网关服务的默认首页，安全中心访问地址（外部访问地址）	https://authx-service.paas.xxx.edu.cn
-	-	-
USER_DATA_SERVICE_SERVER_URL	用户服务开放接口地址（k8s集群内部地址）	http://user-data-service-go-svc.user-data-service.svc.cluster.local:8080
-	-	-
USER_AUTHZ_SERVICE_SERVER_URL	授权服务管理接口地址（k8s集群内部地址）	http://user-authorization-sa-svc.user-authorization-service.svc.cluster.local:8080

- personal-security-center 下的 security-center-ui

ConfigMap, security-center-ui-env

key	说明	配置示例
RESOURCE_PREFIX	LOGO、FAVICON 等资源地址	https://authx-minio.paas.xxx.edu.cn/security-center-ui
MAIN_SERVER	安全中心访问地址（外部访问地址）	https://authx-service.paas.xxx.edu.cn
-	-	-
PERSONAL_CENTER_API	后端API，个人安全中心访问地址（外部访问地址）	https://authx-service.paas.xxx.edu.cn/personal
-	-	-
AUTH_TYPE	认证对接方式，可选 cas, uniauth	cas
-	-	-
AUTH_CAS	CAS认证地址（外部访问地址）	http://cas.paas.xxx.edu.cn/cas
JWT_ISS	JWT Token 签名方标识	http://cas.paas.xxx.edu.cn/cas
JWT_SECRET	JWT Token 签名密钥	固定值，(@<rhnpaUYKC_k770*DulwYQ_#Zc#8c(2rB?kae)rN)>K7qy)awCjxp\$L653Mf\$2
-	-	-
UNIAUTH_IDTOKEN	uniauth认证地址（外部访问地址）	https://uniauth.paas.xxx.edu.cn/identitytoken
UNIAUTH_IDTOKEN_ISS	Id Token 签名方标识	uniauth
UNIAUTH_CLIENT_ID	client id	22

注：AUTH_TYPE 为 cas 时，配置 AUTH_CAS、JWT_ISS、JWT_SECRET AUTH_TYPE 为 uniauth 时，配置 UNIAUTH_IDTOKEN、UNIAUTH_IDTOKEN_ISS、UNIAUTH_CLIENT_ID

- attest-server 下的 attest-server

ConfigMap, attest-server-env

key	说明	配置示例
POA_SERVER_URL	POA网关地址（外部访问地址）	https://poa.paas.xxx.edu.cn
POA_CLIENT_ID	client id	
POA_CLIENT_SECRET	client secret	
POA_SCOPES	api 接口的 scope	appPush:v1:apppushByMessageType
-	-	-
ATTEST_SERVER_PREFIX	身份验证服务地址（外部访问地址）	https://attest.paas.xxx.edu.cn/attest
-	-	-
ATTEST_SERVER_SECUREPHONE_SMS_TEXT_TEMPLATE	短信内容模板	【认证服务】{name}: 您正在进行验证身份, 验证码为{code}, 有效期5分钟, 请尽快完成验证。
ATTEST_SERVER_SECUREPHONE_SMS_FROM	短信内容标题	认证服务
-	-	-
ATTEST_SERVER_SECUREEMAIL_MAIL_TEXT_TEMPLATE	邮件内容模板	【认证服务】{name}: 您正在进行验证身份, 验证码为{code}, 有效期5分钟, 请尽快完成验证。
ATTEST_SERVER_SECUREEMAIL_MAIL_FROM	邮件内容标题	认证服务
-	-	-
ATTEST_SERVER_FACEVERIFY_SUPERAPP_URL_SCHEME	在超级APP 中唤起人脸识别的 URL Scheme	superapp
-	-	-
TOKEN_SERVER_TOKEN_SIGNING_KEY_URL	TOKEN认证验签公钥地址（k8s集群内部地址）	http://token-server-svc.token-server.svc.cluster.local:8080/token/jwt/publicKey
-	-	-
TPAS_AGENT_SERVICE_SERVER_URL	代理服务接口地址（k8s集群内部地址）	http://agent-service-svc.thirdparty-agent-service.svc.cluster.local:8080
TPAS_AGENT_SERVICE_SMS_SENDER_PATH	短信发送服务地址 console: 控制台输出, 默认 aliyun: 阿里云短信服务 其他, 支持学校定制接口	/api/v1/tpas/sms/console/send
TPAS_AGENT_SERVICE_MAIL_SENDER_PATH	邮件发送服务地址 console: 控制台输出, 默认 smtp: SMTP服务 其他, 支持学校定制接口	/api/v1/tpas/mail/console/send
-	-	-
USER_DATA_SERVICE_SA_API_SERVER_URL	用户服务管理接口地址（k8s集群内部地址）	http://user-data-service-go-a-svc.user-data-service.svc.cluster.local:8080
-	-	-
TOKEN_SERVER_SERVER_URL	Token认证服务接口地址（k8s集群内部地址）	http://token-server-svc.token-server.svc.cluster.local:8080/token

- authx-log 下的 authx-log-sa
ConfigMap, authx-log-sa-env

key	说明	配置示例
USER_DATA_SERVICE_SERVER_URL	用户服务管理接口地址（k8s集群内部地址）	http://user-data-service-go-a-svc.user-data-service.svc.cluster.local:8080
-	-	-
IPADDR_SERVER_URL	IP地址服务	http://ipaddr.ipaddr.svc.cluster.local:9090
-	-	-
AUTHX_LOG_ENABLED	是否开启日志推送	true
AUTHX_LOG_RABBITMQ_HOST	rabbit mq 服务地址（k8s集群内部地址）	rabbitmq-server.authx-service.svc.cluster.local
AUTHX_LOG_RABBITMQ_PORT	rabbit mq 服务端口	5672
AUTHX_LOG_RABBITMQ_USERNAME	rabbit mq 服务用户	
AUTHX_LOG_RABBITMQ_PASSWORD	rabbit mq 服务密码	

开始安装

数据库创建

- 数据库帐号

以下是 各服务对应的数据库帐号

服务	数据库帐号
用户服务 user-data-service	user
授权服务 user-authorization-service	user_authz
-	-
日志服务 authx-log	authx_log
-	-
认证服务 cas-server	cas_server
认证服务（APP适用） token-server	token_server
-	-
（可选）第三方代理服务 thridparty-agent-service	agent_service
-	-
v4认证迁移数据	tmp_data

命令： 请修改命令中的 `your_password` 为实际的数据库帐号的密码

```
create user 'user'@'%' identified with mysql_native_password by 'your_password';
create user 'user_authz'@'%' identified with mysql_native_password by 'your_password';

create user 'authx_log'@'%' identified with mysql_native_password by 'your_password';

create user 'cas_server'@'%' identified with mysql_native_password by 'your_password';
create user 'token_server'@'%' identified with mysql_native_password by 'your_password';

create user 'agent_service'@'%' identified with mysql_native_password by 'your_password';

create user 'tmp_data'@'%' identified with mysql_native_password by 'your_password';
```

- 数据库

以下是 各服务对应的数据库

服务	数据库
用户服务 user-data-service	user
授权服务 user-authorization-service	user_authz
-	-
日志服务 authx-log	authx_log
-	-
认证服务 cas-server	cas_server
认证服务（APP适用） token-server	token_server
-	-
（可选）第三方代理服务 thridparty-agent-service	agent_service
-	-
v4认证迁移数据	tmp_data

命令：

```
create database `user` DEFAULT CHARSET utf8 COLLATE utf8_general_ci;
create database `user_authz` DEFAULT CHARSET utf8 COLLATE utf8_general_ci;

create database `authx_log` DEFAULT CHARSET utf8 COLLATE utf8_general_ci;

create database `cas_server` DEFAULT CHARSET utf8 COLLATE utf8_general_ci;
create database `token_server` DEFAULT CHARSET utf8 COLLATE utf8_general_ci;

create database `agent_service` DEFAULT CHARSET utf8 COLLATE utf8_general_ci;

create database `tmp_data` DEFAULT CHARSET utf8 COLLATE utf8_general_ci;
```

- 数据库权限授予

将 database 的权限授予对应的帐号

命令：

```
grant all privileges on `user`.* to 'user'@'%' with grant option;
grant all privileges on `user_authz`.* to 'user_authz'@'%' with grant option;

grant all privileges on `authx_log`.* to 'authx_log'@'%' with grant option;

grant all privileges on `cas_server`.* to 'cas_server'@'%' with grant option;
grant all privileges on `token_server`.* to 'token_server'@'%' with grant option;

grant all privileges on `agent_service`.* to 'agent_service'@'%' with grant option;

grant all privileges on `tmp_data`.* to 'tmp_data'@'%' with grant option;
```

- SUPER 权限授予

由于 部分帐号 需要创建 触发器，故，需要 SUPER 权限 涉及帐号有 user、user_authz、cas_server

命令：

```
grant SUPER on *.* to 'user'@'%';
grant SUPER on *.* to 'user_authz'@'%';
grant SUPER on *.* to 'cas_server'@'%';

grant SUPER on *.* to 'tmp_data'@'%';
```

- 用户数据的交换帐号

待部署完成后操作

如果，存在数据交换 须将组织机构数据、帐号数据 同步到用户服务的数据库的 则，需要创建一个 交换用的数据库帐号（user_trans），并为该帐号授予 表 user.TMP_ORGANIZATION_ORIGIN、user.TMP_ACCOUNT_ORIGIN 的读写操作的权限

命令：

```
create user 'user_trans'@'%' identified with mysql_native_password by 'your_password';

grant select on `user`.`TMP_ORGANIZATION_ORIGIN` to 'user_trans'@'%';
grant insert on `user`.`TMP_ORGANIZATION_ORIGIN` to 'user_trans'@'%';
grant update on `user`.`TMP_ORGANIZATION_ORIGIN` to 'user_trans'@'%';
grant delete on `user`.`TMP_ORGANIZATION_ORIGIN` to 'user_trans'@'%';

grant select on `user`.`TMP_ACCOUNT_ORIGIN` to 'user_trans'@'%';
grant insert on `user`.`TMP_ACCOUNT_ORIGIN` to 'user_trans'@'%';
grant update on `user`.`TMP_ACCOUNT_ORIGIN` to 'user_trans'@'%';
grant delete on `user`.`TMP_ACCOUNT_ORIGIN` to 'user_trans'@'%';

grant select on `user`.`TMP_ORGANIZATION_TRANS` to 'user_trans'@'%';
grant insert on `user`.`TMP_ORGANIZATION_TRANS` to 'user_trans'@'%';
grant update on `user`.`TMP_ORGANIZATION_TRANS` to 'user_trans'@'%';
grant delete on `user`.`TMP_ORGANIZATION_TRANS` to 'user_trans'@'%';

grant select on `user`.`TMP_ACCOUNT_TRANS` to 'user_trans'@'%';
grant insert on `user`.`TMP_ACCOUNT_TRANS` to 'user_trans'@'%';
grant update on `user`.`TMP_ACCOUNT_TRANS` to 'user_trans'@'%';
grant delete on `user`.`TMP_ACCOUNT_TRANS` to 'user_trans'@'%';
```

rancher 容器部署

- 修改 yaml 中的相关配置

具体参考 yaml 文件中的说明

0.infras

基础设施，目前包含 MySQL数据库的Web管理端、SpringBoot服务的管理端

0.0.0.infras-base.yaml	请修改 harbor-registry 的帐号密码
0.0.1.infras-mysql.yaml	请修改 MySQL数据库 的地址、IP, mysql-adminer 访问域名
0.0.2.infras-sba.yaml	请修改 docker 镜像地址

1.authx-service

业务中台 之 认证授权服务

参考 yaml 中的说明，修改相关配置

在各个服务的安装脚本目录下，修改以下文件（若存在）中的配置	
0.*-base.yaml	请修改 harbor-registry 的帐号密码
4.x.*.yaml, 5.*-datax-job.yaml	请修改 docker 镜像地址

1.*-env.yaml, 5.*-datax-job.yaml 请修改 数据库密码

2.*-ingresses.yaml 请修改 访问域名

0.0.trans-service-v4

此为 认证v4 的数据迁移服务（可选）

将 认证v4 的数据导入到 tmp_data 下

数据迁移后，还需要手动编写脚本，将数据迁移至 用户服务、授权服务 的数据库中

0.authx-service

此为 公共基础服务

如：MySQL 服务地址（Endpoints）、文件存储服务

1.authx-service-mysql.yaml

请修改 mysql 的服务地址 IP

2.authx-service-minio.yaml

请修改 minio 的 `MINIO_ACCESS_KEY`、`MINIO_SECRET_KEY`

根据情况修改 pvc 的 storageClassName

9.poa-api-docs_install.yaml

用于将 认证授权服务的 poa 接口文档，导入到 poa-sa 中，**请在 poa 安装完成后处理**

请修改 poa 的服务地址 `POA_SERVER_URL`

1.thirdparty-agent-service

此为 第三方服务的代理服务

file-minio

修改 minio 的 `FILE_MINIO_ACCESSKEY`、`FILE_MINIO_SECRETKEY`

mail-smtp

获取 学校的 smtp 服务地址，邮箱帐号，用于发送邮件

sms-aliyun

如果 学校使用 阿里云的短信服务，提供 `ACCESS_KEY_ID`、`ACCESS_SECRET`；
否则，提供相关的短信平台，进行定制开发

2.user-data-service

此为 用户服务

user-data-service-go

如果 须将用户数据的变更下发到 Openldap 等第三方业务中，则须配置 `JOBS_RABBITMQ_*` 为开启（ENABLED=true）

3.user-authorization-service

此为 授权服务

4.cas-server

此为 认证服务

cas-server-site-webapp

生成公私钥证书, 参考 certs/jwt/readme.md 生成公私钥pem, 修改相关配置 `CASSERVER_JWT_PRIVATE_KEY_PEM_PKCS8`、`CASSERVER_JWT_PUBLIC_KEY_PEM`

修改 认证服务的外网访问地址 `CAS_SERVER_NAME`

修改 CAT TGC 的安全, 若 使用 https, 则须修改 `CAS_TGC_SECURE: "true"``

修改 安全中心(帐号激活、找回密码)的链接地址 `CASSERVERSITE_FORGOT_PASSWORD_URL`、`CASSERVERSITE_ACTIVE_ACCOUNT_URL`

联合登录(QQ、微信、企业微信、支付宝等)配置 `CASSERVER_FEDERATION_*`

动态密码认证 相关配置

1. 短信模板(动态密码) `CASSERVERSITE_PASSWORDLESS_SMS_TEXT_TEMPLATE`
2. 短信接口地址 `TPAS_AGENT_SERVICE_SMS_SENDER_PATH`

如果 须与 超级APP 对接, 须修改 Token 验签公钥地址 `SUPERAPP_TOKEN_SIGNING_KEY_URL`

如果 须开启图片验证码, 修改 `CASSERVERSITE_CAPTCHA_ENABLED: "true"``

5.token-server

此为 认证服务(适用于APP, 可选)

token-server

生成公私钥证书(与cas-server保持一致), 参考 certs/jwt/readme.md 生成公私钥pem, 修改相关配置 `TOKEN_SERVER_SECURITY_JWT_PRIVATE_KEY_PEM_PKCS8`、`TOKEN_SERVER_SECURITY_JWT_PUBLIC_KEY_PEM`

修改 认证服务的外网访问地址 `TOKEN_SERVER_PREFIX`

修改 认证服务 Id-Token 的签发者标识 `TOKEN_SERVER_SECURITY_JWT_ISS`

动态密码认证 相关配置(与cas-server保持一致)

1. 短信模板(动态密码) `TOKEN_SERVER_PASSWORDLESS_SMS_TEXT_TEMPLATE`
2. 短信接口地址 `TPAS_AGENT_SERVICE_SMS_SENDER_PATH`

人脸认证, 须配置人脸服务, 目前支持 新开普人脸服务、百度人脸服务, 根据情况获取相关配置参数

APP 登录信息 个推, 使用了消息服务的接口, 该接口由 POA 提供, 故须

1. 注册 POA client, 获取 `clientId`、`clientSecret`, 申请 Scope `messagecenter:v1:sendMessage`
2. 获取 消息服务的 `appId`

6.personal-security-center

此为 个人安全中心 后端API, 安全中心 前端UI

提供个人帐号相关的操作的接口, 以及 帐号激活、密码找回 等功能

TODO: 修改 bff、zuul 配置

TODO: 修改 security-center-ui 配置

7.attest-server

此为 身份验证服务

提供双因子、二次认证时，进行用户的身份验证，包括 APP推送验证、安全手机验证、安全邮箱验证、人脸识别验证 等能力

8.authx-log

此为 日志服务

收集 用户、认证、授权 的管理、使用过程中产生的 操作日志、登录日志；同时，提供日志查询、基于日志的统计功能

9.jobs-server

此为 任务调度服务

基于 定时任务、触发任务 等，完成 用户数据的同步

如：

- * 源头数据进入到临时表后，写入用户的正式表
- * 用户数据更新后，通过消息队列，增量更新 Openldap 数据

● 添加项目、命名空间

项目

infras	# 基础设施（可选，方便实施工作）
authx-service	# 认证授权服务
admin-platform	# 管理平台

命名空间

在项目 infras 下创建 命名空间：

base

在项目 authx-service 下创建 命名空间：

trans-service（认证v4的数据迁移服务，可选）

authx-service

thirdparty-agent-service

user-data-service

user-authorization-service

cas-server

token-server

personal-security-center

attest-server

authx-log

jobs-server

- 导入YAML

在项目 infras 中，将 0.infras 下的 yaml 按编号依次导入

```
0.0.0.infras-base.yaml

0.0.1.infras-mysql.yaml          mysql web管理

0.0.2.infras-sba.yaml
```

在项目 authx-service 中，将 1.authx-service 下的 yaml 按编号依次导入

务必确保 **4.0.*-installer.yaml** 执行成功

数据配置

数据脚本初始化

先修改 脚本中的域名（如果存在）

- 必须，1.authx0service/10.0.init.sql
包括，安全中心的认证对接配置 云平台，管理接口的路由配置 云平台，管理功能的菜单配置
- 可选，1.authx-service/10.0.tmp.sql
若通过交换同步组织机构、帐号数据的，须执行该数据库脚本