

产品部署之中台服务对接数据初始化相关接口的说明

产品部署之中台服务对接数据初始化相关接口的说明

说明

数据初始化接口说明

CAS认证

用户服务

授权服务

云平台菜单、操作

说明

本文档，为中台产品在部署时，提供对接数据初始化的相关接口

主要涉及：

- 1. CAS认证，创建 Service
- 2. 授权服务，创建 应用，应用角色
- 3. 云平台菜单，创建 应用，菜单，角色权限的关联

数据初始化接口说明

CAS认证

采用业务管理接口进行部署

版本要求：1.2.0

- 部署接口

- 1. 创建 Service

```
curl -i -s -X POST \
-H 'Content-Type: application/json' \
-d '{
  "id": "0",
  "companyId": 1,
  "name": "示例",
  "description": "示例",
  "informationUrl": "https://example.com",
  "logoutUrl": "https://example.com/slo",
  "responseType": "REDIRECT",
  "logoutType": "FRONT_CHANNEL",
  "evaluationOrder": 0,
  "friendlyName": "示例",
  "registeredServiceId": 0,
```

```
"serviceId": "https://example.com/(.*)",
"enabled": true,
"ssoEnabled": true,
"requireAllAttributes": true,
"idTokenEnabled": false,
"jwtAsServiceTicket": false,
"adaptV4Product": false,
"applicationId": "0",
"applicationDomain": "example.com",
"externalId": "0"
}' \
'http://authx-service-user-data-service-goa.authx-
service.svc.cluster.local:8080/v1/admin/services'
```

2. 更新 Service

```
curl -i -s -X PUT \
-H 'Content-Type: application/json' \
-d '{
  "id": "0",
  "companyId": 1,
  "name": "示例",
  "description": "示例",
  "informationUrl": "https://example.com",
  "logoutUrl": "https://example.com/slo",
  "responseType": "REDIRECT",
  "logoutType": "FRONT_CHANNEL",
  "evaluationOrder": 0,
  "friendlyName": "示例",
  "registeredServiceId": 0,
  "serviceId": "https://example.com/(.*)",
  "enabled": true,
  "ssoEnabled": true,
  "requireAllAttributes": true,
  "idTokenEnabled": false,
  "jwtAsServiceTicket": false,
  "adaptV4Product": false,
  "applicationId": "0",
  "applicationDomain": "example.com",
  "externalId": "0"
}' \
'http://authx-service-user-data-service-goa.authx-
service.svc.cluster.local:8080/v1/admin/services'
```

说明

修改 id、registeredServiceId、applicationId、externalId，应用的ID、标识等

修改 evaluationOrder

修改 name、description、friendlyName，应用的名称

修改 idTokenEnabled、jwtAsServiceTicket、adaptV4Product，true 启用，false 禁用

修改 informationUrl、logoutUrl、serviceld、applicationDomain，相关地址、域名修改

● 接口属性说明

应用（Service）的属性说明

属性名	说明
id	确保唯一性
name	应用名称
description	描述
informationUrl	应用的访问地址
logoutUrl	应用的前端注销地址
responseType	登录成功后的响应方式，固定为 REDIRECT
logoutType	单点注销方式，固定为 FRONT_CHANNEL
evaluationOrder	优先级
friendlyName	同 应用名称
registeredServiceld	唯一ID，整型
serviceld	应用匹配规则，确保前缀与对接时的 service 相匹配
enabled	是否启用
ssoEnabled	是否支持单点登录
requireAllAttributes	固定为 true
idTokenEnabled	是否返回 ID Token，方便公司内产品的前端，调用后端接口
jwtAsServiceTicket	是否返回 JWT 格式的票据，便于纯前端项目对接
adaptV4Product	是否适配认证V4，用于兼容公司历史版本的认证
applicationId	应用标识，可与 id 保持一致
applicationDomain	应用域，使用访问地址中的 域名
externalId	外部ID（预留），与 id 保持一致

用户服务

可以添加 用户、账号，部门，用户组，

服务地址: `http://authx-service-user-data-service-go.aauthx-service.svc.cluster.local:8080`

- 用户创建接口

版本要求: 1.2.7、1.3.2、1.4.1、1.5.0

仅创建用户的基本信息，不会创建账号

POST /api/v1/trans/user?transOrigin=init

Content-Type: application/json

```
{
  "uid": "string",
  "passWord": "string",
  "name": "string",
  "nameSpelling": "string",
  "fullNameSpelling": "string",
  "certificateTypeCode": "string",
  "certificateNumber": "string",
  "phoneNumber": "string",
  "email": "string",
  "imageUrl": "string",
  "genderCode": "string",
  "nationCode": "string",
  "countryCode": "string",
  "addressCode": "string",
  "activation": true,
  "dataCenter": true,
  "externalId": "string"
}
```

用户的属性说明

属性名	说明	是否必填
uid	用户标识	否，为空时，随机生成
passWord	密码	否，为空时，默认123456，且激活状态为 未激活
name	姓名	是
nameSpelling	姓名简拼	否
fullNameSpelling	姓名全拼	否
certificateTypeCode	证件类型代码（参考字典表 证件类型，如 1 居民身份证）	是
certificateNumber	证件号码	是
phoneNumber	联系电话（预留手机）	否
email	电子邮箱（预留邮箱）	否
imageUrl	头像地址	否
genderCode	性别代码（参考字典表 性别，如 1 男，2 女）	否
nationCode	民族代码（参考字典表 民族，如 01 汉族）	否
countryCode	国家代码（参考字典表 国家，如 156 中国）	否
addressCode	地区代码（参考字典表 地区，如 110000 北京市，120000 天津市，310000 上海市）	否
activation	是否激活（true 是，false 否）	是
dataCenter	是否来源数据中心（true 是，false 否）	是
externalId	外部Id	否

- 账号（包含用户信息）创建接口

版本要求：1.0+

POST /api/v1/trans/account?transOrigin=init

Content-Type: application/json

```
{
  "uid": "string",
  "passWord": "string",
  "name": "string",
  "nameSpelling": "string",
  "fullNameSpelling": "string",
```

```
"certificateTypeCode": "string",
"certificateNumber": "string",
"phoneNumber": "string",
"email": "string",
"imageUrl": "string",
"genderCode": "string",
"nationCode": "string",
"countryCode": "string",
"addressCode": "string",
"accountName": "string",
"organizationCode": "string",
"identityTypeCode": "string",
"accountExpiryDateMillis": 0,
"state": "string",
"activation": true,
"dataCenter": true,
"externalId": "string"
}
```

账号的属性说明

属性名	说明	是否必填
uid	用户标识	否，为空时，随机生成
passWord	密码	否，为空时，默认123456，且激活状态为 未激活
name	姓名	是
nameSpelling	姓名简拼	否
fullNameSpelling	姓名全拼	否
certificateTypeCode	证件类型代码（参考字典表 证件类型，如 1 居民身份证）	是
certificateNumber	证件号码	是
phoneNumber	联系电话（预留手机）	否
email	电子邮箱（预留邮箱）	否
imageUrl	头像地址	否
genderCode	性别代码（参考字典表 性别，如 1 男，2 女）	否
nationCode	民族代码（参考字典表 民族，如 01 汉族）	否
countryCode	国家代码（参考字典表 国家，如 156 中国）	否
addressCode	地区代码（参考字典表 地区，如 110000 北京市，120000 天津市，310000 上海市）	否
accountName	账号名	是
organizationCode	组织机构代码（对应组织机构代码）	是
identityTypeCode	身份代码（对应身份的代码）	是
accountExpiryDateMillis	过期时间（时间戳，毫秒）	否
state	状态（NORMAL: 正常, FREEZE: 冻结, WRITTENOFF: 注销）	是
activation	是否激活（true 是，false 否）	是
dataCenter	是否来源数据中心（true 是，false 否）	是
externalId	外部Id	否

- 部门创建接口

版本要求：1.0+

POST /api/v1/trans/organization?transOrigin=init
Content-Type: application/json

```
{
  "parentOrganizationCode": "string",
  "code": "string",
  "name": "string",
  "description": "string",
  "typeCode": "string",
  "state": 0,
  "isDataCenter": true,
  "externalId": "string"
}
```

组织机构的属性说明

属性名	说明	是否必填
parentOrganizationCode	上级部门的代码（对应组织机构的代码）	是
code	代码	是
name	名称	是
description	描述	否
typeCode	组织机构类型代码（参考字典表 组织机构类型）	是
state	状态（0: 正常, 1: 冻结, 2: 注销）	是
isDataCenter	是否来源数据中心（true 是，false 否）	否，为空时，默认为 true
externalId	外部Id	否

- 用户组创建接口

版本要求：1.2.9、1.3.5、1.4.3、1.5.0

POST /api/v1/trans/group?transOrigin=init
Content-Type: application/json


```
{
  "code": "string",
  "name": "string",
  "description": "string",
  "type": "string",
  "state": 0,
  "categoryCode": "string",
  "common": true,
  "applicationId": "string",
  "isDataCenter": true,
  "externalId": "string"
}
```

用户组的属性说明

属性名	说明	是否必填
parentOrganizationCode	上级部门的代码（对应组织机构的代码）	是
code	代码	是
name	名称	是
description	描述	否
type	类型（1: 普通用户组, 2: 岗位用户组）	是
state	状态（1: 启用, 0: 禁用）	是
common	是否公共用户组（true 是，false 否）	否，为空时，默认为 true
applicationId	所属应用标识（common 为 false 时，须设置）	否
isDataCenter	是否来源数据中心（true 是，false 否）	否，为空时，默认为 true
externalId	外部Id	否

授权服务

采用 sql 文件执行接口进行部署

版本要求：1.2.3

- 部署接口

```
curl -i -s -X POST \  
  -H 'Content-Type: text/plain' \  
  --data-binary @user_authz_integrate.sql \  
  'http://authx-service-user-authz-service-sa.authx-  
service.svc.cluster.local:8080/deploy/execSql'
```

- SQL脚本示例

user_authz_integrate.sql

-- 应用的创建脚本

```
INSERT INTO TB_R_SYSTEM (ID, COMPANY_ID, DELETED, ADD_ACCOUNT, ADD_TIME,  
  BUSINESS_DOMAIN_ID,  
  CODE, NAME, ENABLED)  
VALUES ('0', '1', 0, 'init', null,  
  '1',  
  '0', '示例系统', 1);  
  
INSERT INTO TB_APPLICATION (ID, COMPANY_ID, DELETED, ADD_ACCOUNT, ADD_TIME,  
  BUSINESS_DOMAIN_ID, SYSTEM_ID,  
  NAME, APPLICATION_ID, SYNC_URL, ENABLED)  
VALUES ('0', '1', 0, 'init', null,  
  '1', '0',  
  '示例应用', '0', '', 1);  
  
commit;
```

如须自动同步角色，请修改 `SYNC_URL`

系统信息表 TB_R_SYSTEM

字段名	字段说明
ID	确保唯一性
COMPANY_ID	固定为 1
DELETED	是否删除，固定为 0
ADD_ACCOUNT	创建帐号
ADD_TIME	创建时间，建议为 null；如必要，可填入时间
-	-
BUSINESS_DOMAIN_ID	所属业务域，暂时固定为 1
CODE	系统代码
NAME	系统名称
ENABLED	是否启用（1 启用，0 禁用）

应用信息表 TB_APPLICATION

字段名	字段说明
ID	确保唯一性
COMPANY_ID	固定为 1
DELETED	是否删除，固定为 0
ADD_ACCOUNT	创建帐号
ADD_TIME	创建时间，建议为 null；如必要，可填入时间
-	-
BUSINESS_DOMAIN_ID	所属业务域，暂时固定为 1
SYSTEM_ID	所属系统，同 TB_R_SYSTEM 的 ID
NAME	应用名称
APPLICATION_ID	应用标识，可以与 ID 保持一致
SYNC_URL	角色数据的同步接口。若不需要，可以为空
ENABLED	是否启用（1 启用，0 禁用）

** 采用业务管理接口进行部署 **

创建角色

```
curl -i -s -X POST \
  -H 'Content-Type: application/json' \
  -d '{
    "id": "0",
    "code": "example-admin",
    "name": "示例管理员",
    "description": "示例管理员",
    "enabled": true,
    "applicationId": "0",
    "externalId": "0"
  }' \
  'http://authx-service-user-authz-service-sa.authx-
service.svc.cluster.local:8080/v1/admin/roles'
```

角色表 TB_ROLE

属性名	说明
id	确保唯一性
applicationId	所属应用，同 TB_APPLICATION 的 ID
code	角色代码
name	角色名称
description	角色描述
enabled	是否启用（1 启用，0 禁用）
externalId	对应所在应用内的数据的ID

云平台菜单、操作

采用业务管理接口进行部署

版本要求：1.2.0

- 部署接口

创建应用

```
curl -i -s -X POST \
  -H 'Content-Type: application/json' \
  -d '{"id": "0", "code": "0", "name": "示例", "memo": "示例", "status": "1", "url": ""}' \
  'http://admin-platform-admin-center-sa.admin-
platform.svc.cluster.local:8080/v1/admin/applications'
```

导入菜单

```
curl -i -s -X POST \
  -H 'Content-Type: application/json' \
  -d '{
    "applicationId": "0",
    "menuList":
      [
        {
          "id": "0-10000", "parentIdOrCode": "1", "code": "example-10000", "name": "示例一
级", "memo": "", "status": "1",
          "icon": "", "origin": "http://admin-platform.paas.xxx.edu.cn", "url": "/",
"target": "",
          "order": 10000, "resourceIdOrCodes": []
        },
        {
          "id": "0-10100", "parentIdOrCode": "0-10000", "code": "example-10100", "name":
"示例二级", "memo": "", "status": "1",
          "icon": "su-icon-denglupiezhi", "origin": "http://admin-
platform.paas.xxx.edu.cn", "url": "/example/example-10100", "target": "",
          "order": 10100, "resourceIdOrCodes": []
        },
        .....
      ]
    }' \
  'http://admin-platform-admin-center-sa.admin-
platform.svc.cluster.local:8080/v1/admin/menus/importMenu'
```

导入操作（按钮权限）

```
curl -i -s -X POST \
  -H 'Content-Type: application/json' \
  -d '{
    "applicationId": "0",
    "operationList":
      [
        {
          "id": "0-10000-10001", "parentIdOrCode": "0-10000", "code": "example-10000-
10001", "name": "示例一级-操作", "memo": "", "status": "1",
          "order": 10001, "resourceIdOrCodes": []
        },
        {
          "id": "0-10100-10101", "parentIdOrCode": "0-10100", "code": "example-10100-
10101", "name": "示例二级-操作", "memo": "", "status": "1",
          "order": 10101, "resourceIdOrCodes": []
        },
        .....
      ]
    }' \
```

```
'http://admin-platform-admin-center-sa.admin-  
platform.svc.cluster.local:8080/v1/admin/operations/importOperation'
```

导入资源

```
curl -i -s -X POST \  
-H 'Content-Type: application/json' \  
-d '{  
  "applicationId": "0",  
  "resourceList":  
    [  
      {  
        "id": "0-10001", "code": "example-10001", "name": "示例资源一", "memo": "",  
"status": "1",  
        "origin": "http://admin-platform.paas.xxx.edu.cn", "method": "GET", "path":  
"/api/v1/example/10001", "access": "authenticate",  
        "order": 10001, "resourceIdOrCodes": []  
      },  
      {  
        "id": "0-10002", "code": "example-10002", "name": "示例资源二", "memo": "",  
"status": "1",  
        "origin": "http://admin-platform.paas.xxx.edu.cn", "method": "GET", "path":  
"/api/v1/example/10001", "access": "authenticate",  
        "order": 10002, "resourceIdOrCodes": []  
      },  
      .....  
    ]  
}' \  
'http://admin-platform-admin-center-sa.admin-  
platform.svc.cluster.local:8080/v1/admin/resources/importResource'
```

角色权限（关联菜单、操作）

```
curl -i -s -X POST \  
-H 'Content-Type: application/json' \  
-d '{  
  "rolePermissionList":  
    [  
      {  
        "roleCode": "example-admin",  
        "permissionIdOrCodes": ["0-10000", "0-10100", "0-10000-10001", "0-10100-10101"]  
      },  
      .....  
    ]  
}' \  
'http://admin-platform-admin-center-sa.admin-  
platform.svc.cluster.local:8080/v1/admin/rolePermissions/importRolePermission'
```

- 接口 属性说明

应用的属性说明

属性名	说明
id	确保唯一性
code	应用标识，与 id 保持一致
name	应用名称
memo	描述
status	状态（1 启用，0 停用）

菜单的属性说明

属性名	说明
id	确保唯一性
parentIdOrCode	上级菜单的ID 或 代码
code	菜单代码
name	菜单名称
memo	描述
status	状态（1 启用，0 停用）
icon	图标 CSS 名
origin	归属域名，一般为 admin-platform 的域名
url	菜单地址、路由
target	打开方式，空 表示当前窗口直接打开；iframe 表示在iframe中打开
order	排序
resourceIdOrCodes	关联的资源（后端接口）的ID 或 代码。数组，可以为空

操作的属性说明

属性名	说明
id	确保唯一性
parentIdOrCode	上级菜单的ID 或 代码
code	操作代码
name	操作名称
memo	描述
status	状态（1 启用，0 停用）
order	排序
resourceIdOrCodes	关联的资源（后端接口）的ID 或 代码。数组，可以为空

资源的属性说明

属性名	说明
id	确保唯一性
parentIdOrCode	上级菜单的ID 或 代码
code	资源代码
name	资源名称
memo	描述
status	状态（1 启用，0 停用）
origin	归属域名，一般为 admin-platform 的域名
method	GET, POST, PUT, DELETE 四选一
path	资源的请求路径
access	访问规则。anonymous, 匿名访问（未登录时，可访问）；authenticate, 认证访问（登录后，可访问）；authorize, 授权访问（须授权后，可访问）；permitAll, 允许所有（都可访问）；denyAll, 拒绝所有（都不可访问）。

角色权限的属性说明

属性名	说明
roleId	角色ID
roleCode	角色代码
permissionIdOrCodes	关联的菜单的ID 或 代码。数组

