权限中心II期

管理单元设计

# Schema类型

1、管理单元的数据类型仍然坚持权限中心的Schema体系。管理单元使用如下几种主要Schema：

|  |  |  |
| --- | --- | --- |
| Schema名称 | 类型名 | 说明 |
| AUSchemas | AUSchema | 表示管理架构 |
| AUSchemaRoles | AUSchemaRole | 表示管理单元架构定义的角色 |
| AdminUnits | AdminUnit | 表示管理单元 |
| AURoles | AURole | 表示管理单元角色 |
| AUScopes | AUScope | 表示管理单元的一个类型的管理范围 |
| AUSItemXXXs | AUScopeItem的派生类 | 表示自定义的管理范围类型 |
|  |  |  |

2、各个Schema所包含的基本属性（不包括ID，VS，VE，Status）。

|  |  |  |  |
| --- | --- | --- | --- |
| Schema类型 | 属性 | 属性类型 | 说明 |
| AUSchemas | Name | String | 管理架构的名称，规定同一级分类下，不可重名。 |
| AUSchemas | CodeName | String | 管理架构的代码名称，规定通过代码名称可直接查找管理架构，因此各个管理架构其代码名称必须唯一。 |
| AUSchemas | DisplayName | String | 管理架构的显示名称 |
| AUSchemas | Comment | String | 管理架构的描述信息 |
| AUSchemas | Scopes | String | 以逗号分隔的管理范围类别列表（保存管理范围类别的SchemaType） |
| AUSchemas | CategoryID | String | 管理架构的分类的ID |
| AUSchemas | MasterRole | String | 负责管理架构管理的角色（APPCodeName:RoleCodeName） |
| AUSchemaRoles | Name | String | 角色名称，规定同一管理架构，下角色名称不可重复 |
| AUSchemaRoles | CodeName | String | 角色的代码名称，规定同一管理架构，角色代码名称不可重复 |
| AUSchemaRoles | DisplayName | String | 角色的显示名称 |
| AUSchemaRoles | Comment | String | 对角色的描述 |
| AdminUnits | Name | String | 管理单元的名称，规定同一级管理架构和管理单元中，其名称互不相同。 |
| AdminUnits | CodeName | String | 管理单元的代码名称，各个管理单元其代码名称必须唯一，无论是否属于不同管理架构。 |
| AdminUnits | DisplayName | String | 管理单元的显示名称 |
| AdminUnits | Comment | String | 对此管理单元的描述 |
| AdminUnits | AUSchemaID | String | 此管理单元所属的架构的ID |
| AdminUnits | AllowAclInheritance | Boolean | 是否从上级继承ACL |
| AdminUnitRole | SchemaRoleID | String | 对应管理架构中定义的角色的ID |
| AUScopes | ScopeSchemaType | String | 管理单元的管理范围类类型 |
| AdminScopeXXX | RefID | String | 表示引用在其他业务系统的管理范围对象的ID此ID通常与对象ID一样 |
| ~~AdminScopeXXX~~ | ~~CodeName~~ | ~~String~~ | ~~表示标示此管理范围的代码名（权限中心不使用此信息）~~ |
| ~~AdminScopeXXX~~ | ~~Name~~ | ~~String~~ | ~~管理范围对象的名称~~ |
| AdminScopeXXX | Description | String | 对于此管理范围对象的文字描述信息 |
| AdminScopeXXX | SearchTags | String | 用空格分隔的标签或关键词，用于全文检索用 |

2、关联类型（SchemaRelation）：

|  |  |  |
| --- | --- | --- |
| ChildSchemaType | ParentSchemaType | 说明 |
| AdminUnit | AUSchemas | 表示一个管理单元属于一个管理单元架构（仅顶级管理单元） |
| AdminUnit | AdminUnit | 表示一个管理单元是另一个管理单元的下级管理单元 |

3、成员类型：

|  |  |  |
| --- | --- | --- |
| MemberSchemaType | ContainerSchemaType | 说明 |
| AUSchemaRoles | AUSchema | 管理架构定义的角色 |
| AUScopes | AdminUnit | 表示管理单元的一个管理范围 |
| AdminScopeXXX | AUScopes | 表示管理范围的固定成员 |
| AURoles | AdminUnit | 表示管理单元的一个角色，此角色对应一个架构定义的角色 |
| Users | AURoles | 表示管理单元角色中的一个用户 |

4、管理范围的条件表达式（Type=“ADM”）

与其他场合下的条件表达式不同的是，此条件表达式仅一条。

5、授权控制（ACL）（等需求准确之后）

|  |  |  |  |
| --- | --- | --- | --- |
| MemberSchemaType | ContainerSchemaType | ContainerPermission | 说明 |
| AdminUnit | AdminUnit | EditRoleMembers | 修改本单元角色配置人员 |
| AdminUnit | AdminUnit | EditAdminScope | 修改本单元管理范围 |
| AdminUnit | AdminUnit | EditProperty | 修改本单元基本属性 |
| AdminUnit | AdminUnit | AddSubUnit | 添加子管理单元 |
| AdminUnit | AdminUnit | DeleteSubUnit | 删除子管理单元 |
| AdminUnit | AdminUnit | EditSubUnitAcl | 修改子单元授权 |

# 管理架构类别

为了简单起见，管理架构类别简化为以下模式：

1、管理架构类别的ID:。每个管理架构有一个标识：ID

2、管理架构类别名称（Name）：管理架构的可见名称

3、上层管理架构的ID（ParentID）：如果没有上层管理架构，则为空。

4、版本开始时间(VersionStartTime):缺省为当前时间

5、版本结束时间(VersionEndTime): 99990909 00:00:00

6、状态(Status)：缺省值1，表示正常。

7、层级（Level）：缺省值0，表示顶级。

# 管理单元角色

管理单元角色使用Excel的角色矩阵编辑。角色矩阵的维度由管理架构进行定义。管理架构应包含一个维度：AdminUnit（内定的名称），也可以缺省此维度，定义其他维度时不应使用此名称。管理单元维度的值应该是管理单元的代码名称。

# 管理范围

管理范围对象来自各个应用系统，权限中心无法了解其全部以及相互关系，也无法将其结构完全在权限中心实现。为了能够进行有效的计算和查询任务，需要将管理范围对象按权限中心可以识别的模式同步至权限中心（没有逆同步）。这包括权限中心向各个注册的应用系统查询数据，以及其他业务系统向权限中心提取数据2部分。

# 管理范围类型

管理范围的类型由管理架构的管理范围类型字符串来指定。当对管理架构进行修改时，如果管理范围类型发生变化，则会联动的更改所有管理单元。对于修改，会出现如下情况：

1. 为管理架构添加一个新的管理范围类型。这种情况下，会自动为所有管理单元创建一个管理范围对象，并通过成员关系进行关联。
2. 从管理架构删除一个管理范围类型。这种情况下，仅删除管理单元与管理范围对象的关联，管理范围对象仍然保留，并在下次重新添加此管理范围类型时，重新建立关联。
3. 删除一个管理范围，然后重新添加该管理范围，参考第二条的处理。