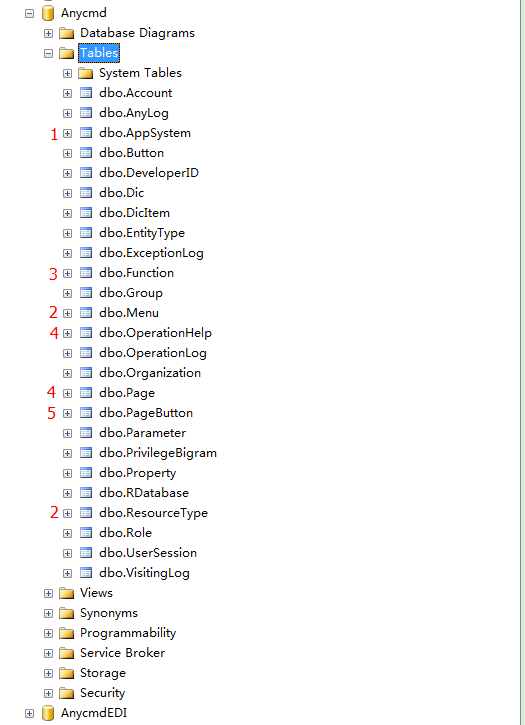
# Anycmd开源通用权限数据库设计说明

开发的时候不一定是dbFirst的，但文档从关系数据库的设计开始可能是一个良好的入口点。因为关系数据库领域是大家熟悉的，而且关系数据库领域的概念不像其它领域那样缺少标准。

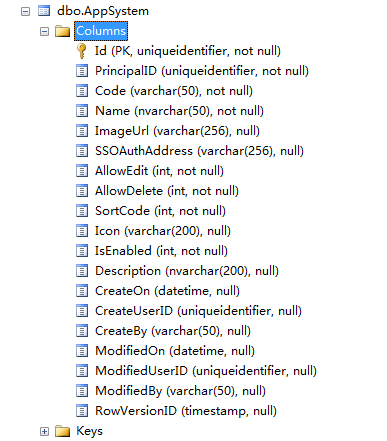
本文会详细介绍anycmd数据库，从一些重要关系洞察整个系统。本文按照anycmd数据库中表的依赖关系安排段落的先后顺序。所有的表如下：



图上未标数字的表也会介绍。

## 1 AppSystem表：

AppSystem是应用系统，在Anycmd中就是权限应用系统。比如OA系统、CRM系统等，如果这些系统接入Anycmd中心系统来统一管理安全策略的话每一个系统就会在Anycmd中心系统的AppSystem数据库表中对应一条记录。这条记录登记的是应用系统的基本信息：



值得说明的是Id字段和Code字段。Id和Code的功用都是唯一地标识和识别一个应用系统的，为什么要提供两种标识呢？这是因为Id往往是数字或Guid等人类难以从中读出信息的值，Id值往往是由计算机程序填入的，而Code可以留给人填入。人类自己填入的值当然更加具有可读性。整个anycmd系统内部不涉及与人类交互的地方都应该使用Id来识别对象而不应使用Code，但可以在与人类交互地方比如与程序员交互的入口可以使用Code来索引应用系统集（AppSystemSet）中的对象，一旦索引得到appSystem对象后Code字段就无用了因为系统内部是使用Id而非Code的。

## 2 ResourceType表：

ResourceType是资源类型。资源是什么呢？资源是需要进行访问控制的系统资源，例如文件、打印机、终端、数据库记录等。而资源类型的本质是对资源的分类。这里需要首次引入分类法。

人类发明的分类法其原理是比较抽象和复杂的。Anycmd用到了分类法所以需要试图表述清除它。

分类就是按照[事物](http://baike.baidu.com/view/93825.htm" \t "_blank)的性质、特点、用途等作为区分的标准，将符合同一标准的事物聚类，不同的则分开的一种认识事物的方法。

分类法是指将类或组按照相互间的关系，组成系统化的结构，并体现为许多类目按照一定的原则和关系组织起来的体系表，作为分类工作的依据和工具。分类法有交叉分类法，树状分类法等等。摘自[百度百科](http://baike.baidu.com/view/555149.htm?fr=aladdin)

我不理解百度百科上所说的交差分类法是什么？我认为如果我们按照人类的性别对人类类型对象集分类的话应该会是“男人”、“女人”、“未知”、“未说明”这么几类，人类的分类法绝不会把一个人既归类到“男人”又归类到“女人”。那么百度百科上所说的“交差分类法”是个什么东西呢？我觉得这可能是“泛型”导致的。当我们研究一个对象集合的时候我们可以从多种角度观察和分类它，每一个研究角度可以看作分类法的一个型。用非形式化的文字表述和理解概念是很困难的，下面我们建立一个Category模型，如下：

public class Category {

public Guid Id { get;set; }

public string Code { get; set; }

public string Name { get; set; }

}

public class CategoryType {

public Guid Id { get; set; }

public string Code { get; set; }

public string Name { get; set; }

public IReadOnlyCollection<Category> Items { get; set; }

}

上面两个模型一个是分类，一个是分类类型。伪代码用来说明模型的组织结构不考虑设计模式。

那么对人类对象集按照性别分类就是

var humanCategoryBySex = new Category {

Id = new Guid(“EC47866B-7E69-4092-A378-A0AB00BD43B0”),

Code = “humanSex”,

Name = “按照性别对人类对象集进行分类”,

Items = new List<Category> {

new Category {

Id = “08CAC9DE-C332-4C3C-A3F3-18F763F8D78D”,

Code = “01”,

Name = “男”

},

new Category {

Id = “08CAC9DE-C332-4C3C-A3F3-18F763F8D78D”,

Code = “02”,

Name = “女”

},

new Category {

Id = “08CAC9DE-C332-4C3C-A3F3-18F763F8D78D”,

Code = “03”,

Name = “未知”

},

new Category {

Id = “08CAC9DE-C332-4C3C-A3F3-18F763F8D78D”,

Code = “09”,

Name = “未说明”

}

}

}

对人类按照国籍进行分类就是：

var humanCategoryBySex = new Category {

Id = new Guid(“EC47866B-7E69-4092-A378-A0AB00BD43B0”),

Code = “humanNationality”,

Name = “按照国籍对人类对象集进行分类”,

Items = new List<Category> {

new Category {

Id = “08CAC9DE-C332-4C3C-A3F3-18F763F8D78D”,

Code = “cn”,

Name = “中国”

},

new Category {

Id = “08CAC9DE-C332-4C3C-A3F3-18F763F8D78D”,

Code = “us”,

Name = “美国”

}

}

}

一个对象至多关联一种分类方式的一个分类节点，不可能关联多个节点，关联多个节点的那种不叫分类。

停下！如果有人既拥有中国国籍又拥有美国国籍怎么办？这是个问题。对于分类法来说解决这个问题的方式是添加新的分类项：cn&us。将既有中国国籍又有美国国籍的人归类到新的编码为“cn&us”（随便什么编码，唯一即可）类别下。这就是分类法，它不分层级，它覆盖整个被分类的对象集，不存在归类不到某个分类项的子集（您可能见到过“男人”、“女人”、“其它”，为什么有其它？因为要覆盖整个人类集）。

**系统字典——忘掉分类法。**分类模型跟字典模型是完全一样的。通常，您的系统中有个“系统字典”模型，这个系统字典模型跟分类法模型是完全一样的，也就是说在实现分类模型的时候可以借助系统字典模型而无需添加新的模型。听到字典一词我们可能会跟离散扯上关系，跟分类一样字典项是离散的，但字典所建立起来的字典项取值可以涵盖整个对象集。比如金额看似不是字典类型的，但如果需要你也可以建立<小于1万，大于等于1万小于100万，大于100万>这样的字典项，这样的字典项覆盖了整个对象集。

如果您从书上看到过层次化的分类模型的话，请忘掉它，那是不正确的。分类法是没有层次的。有层次的是分类法的子类：组织结构。

**什么是组织结构？**

组织结构是对对象集的单元划分。这种划分单元的方式与普通的分类有一个明显的不同是——组织结构具有层级关系。组织结构是一种添加了偏移量的分类方式，组织结构也是分类法，当然一个对象至多属于一种组织结构的一个节点，不可能属于多个节点，属于多个节点的那种不叫分类更不叫组织结构。

下面是从anycmd的源码上复制来的关于组织结构的注释：组织结构是对资源的单元划分。组织结构属于一种分类法，它与普通的分类法的唯一差别是组织结构具有偏移量。

给定一个0到100的实数集合Set{0…100}。普通的分类法所做的分类类似这样：

{

[0…10},

[10…20},

[20…50},

[50…100]

}

而组织结构是这样：

{

{

[0…10},

[10…20}

},

[20…30},

{

[30…35},

[35…40},

[40…50},

{

[50…60},

[60…70},

[70…75},

[75…80},

}

},

[80…100],

}

**组织结构不是资源的固有属性，但应该作为资源的扩展字段直接和资源存储在一起。**

Anycmd对组织结构的使用几乎遍布所有资源，组织结构是资源的附加属性，而资源的固有属性只是没有偏移的分类。Anycmd希望在需要的时候能够被允许侵入应用系统的数据库设计以保存资源管理员添加的组织属性（这个组织属性可能不止一种，但不管资源管理员在管理资源集的时候添加了多少组织属性Anycmd都只会使用你对应的数据库表的一个字段存储）。之所以要侵入应用数据库表是为了根据组织结构对资源集的筛选能够在数据库进程完成而不必加载进应用系统的内存再筛选。框架使用那一个字段比如varchar(100)，框架把它的长度再做单元划分，如果一个单元定长为10就可以存储资源管理员添加的10种组织结构。根据组织结构查询的时候应用系统发出的sql中会截取这个字段的正确的单元。

Anycmd.AC是个权限框架，也支持实体级的控制。管理资源的时候尽量不推荐使用实体级的控制，首先评估实体属性（在实体属性上可以对资源集进行分类划分），如果在实体上的那些固有属性上难以制定出满足安全需求的策略的话再考虑是不是需要组织结构，尽量使用附加的组织属性去对资源划分单元，按照单元进行控制。尽量不使用实体级的控制（因为实体太多了，但如果目标实体是主体的话，比如User实体是主体，这个可以实体级控制，由各个主体自主控制自己而不用管理员工作）。实体级的控制的开启也需要侵入应用系统的数据库，侵入目标资源表建立“一个”安全字段，这个字段中存储的是这条记录的安全策略，安全策略是跟实体记录一同加载进应用系统的内存的，之所以要侵入你的数据库也是因为不应该多一次专门查询ACL策略的查询。

**什么是标签？**

标签不分层级。一个对象可以有多个标签，一个标签可以关联多个对象，对象和标签是多对多关系。

标签也不是资源的固有属性，但它没有组织结构那么高的地位，通常不应将标签作为资源的扩展字段而和资源存储在一起。

举例：

淘宝的商品“类目”是个什么东西？这可能是淘宝自创的概念，如果你进一步了解会发现淘

宝的类目还分“前台类目”和“后台类目”，淘宝的前台类目就是“标签”，后台类目就是“类

别”。前台类目多对多，后台类目多对一。

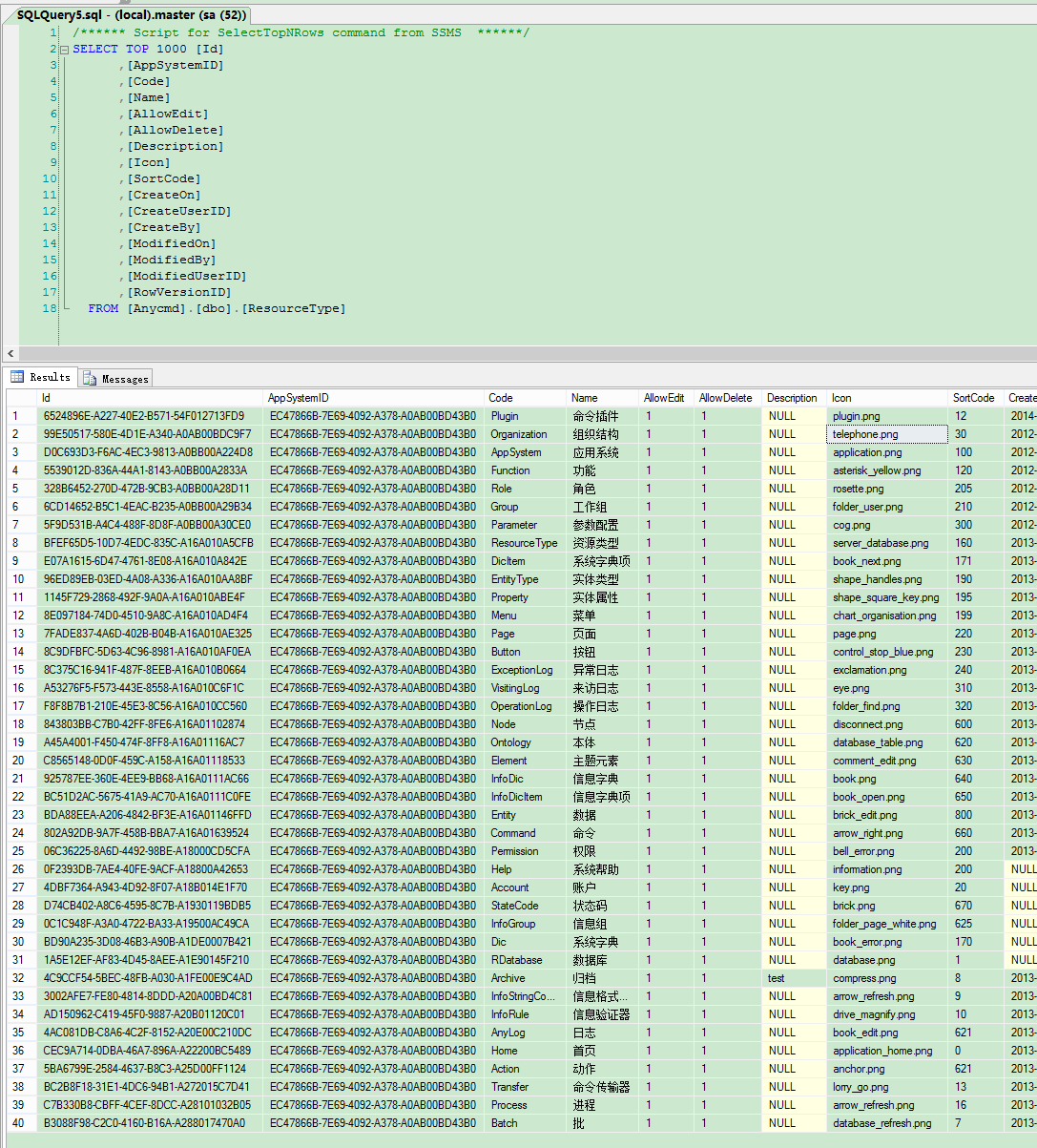
教师的组织结构是个什么东西？政府作为一个大的行政单位，它有很多很多资源，为了对这

些资源进行良好的管理政府划分了很多“行政单位”。同样，教育部也对教育单位做了单元

划分，区县、学校、电教馆、教科所等这些就是教育组织结构。一个老师必定是属于且只属

于一个组织结构的，系统可以直接使用区县、学校、电教馆等这些自然的组织结构来组织师生记录资源。在工作的开展上，一个老师有可能效力不只一个学校，但从资源记录的角度一个老师至多属于一个组织结构。

**到这里已经严重跑题了。**回到ResourceType表。ResourceTye是什么？ResourceType是对系统中的所有资源建立的第一次第0级分类。



**今天到这里，一次性写不完。排版不好，多多见谅，汇总时改正。**