基于上节所述的 RBAC 基本思想，这里将详细介绍模型中的具体概念，其中主要有四

个实体：用户（User） 、角色（Role）、权限（Permission）、会话（ Session ）。

（1）用户（User）：对资源进行访问的访问者。一般而言，用户就是人，但是随着

计算机的发展，它也可以是一些智能程序。

（2）角色（Role）：可以执行特定任务或被指定拥有一定工作职能的工作头衔。它

代表一种权利和责任。它根据具体的业务场景来进行划分。

（3）权限 （Permission）：表示用户对资源的操作许可，与具体的系统应用有关。

通常权限限定相关联的资源。

（4）会话（Session）：用户和角色之间的映射，通常该映射为一对多关联。用户想

要得到相应的访问权限，必须激活相对应的角色，而角色的激活就要在某个会话中完成。

每个会话和单个用户关联，并且每个用户可以关联到一个或多个会话。

基于给定的四个基本实体，还需要定义一下概念：

（5）权限分配（Permission Assignment，PA）：权限与角色之间的多对多映射，即

有 PA ⊆ P×R。 ( r ,p)∈PA表示角色 r 拥有权限 p。

（6）用户分配角色（User Assignment，UA）：用户与角色之间的多对多映射，即有

UA ⊆ U×R。 ( u ,r)∈UA表示用户 u 拥有角色 r。

（7）角色层次（Role Hierarchy，RH）：角色要素关系或者角色等级的一种偏序关

系。（8）约束条件（Constraints）：约束关系，用来决定模型中各种部件的操作是否被

允许。













