
第 17 章 — 安全性

“安全性”菜单选项位于“数据模型管理器”下方。它包含下列菜单选项。

- 用户控制台
- 角色控制台
- 公司属性
- 访问控制组
- 访问权
- 活动日志

角色和用户

在 WebSphere Product Center 中，对用户的管理是通过一组角色控制的，这些角色是通过“安全性”模块的“管理角色”组件创建的。

规则：将特权授予用户被指定到的角色，而不是授予用户个人。如果给用户指定了多个角色，则他们从每个角色继承特权。

可以创建对特定 WebSphere Product Center 功能和 / 或对象具有许可权的定制角色（例如，内容复查员、内容核准员和目录管理员）。因此，要应用定制角色的特权，请给用户指定该角色。

使用 WebSphere Product Center 的访问控制组（ACG）来根据哪些用户可以查看 / 编辑特定的目录来设置许可权。根据用户的职责，给该用户指定了一个或多个 ACG。如果有需要的话，将各种角色分组到单个对象中。

可以通过“目录访问权控制台”来对目录访问权进行其它控制。可以设置一组特权来指定哪些角色可以查看 / 编辑目录中的特定列。

角色和特权

创建角色的目的是控制用户的目录管理特权。将特权授予用户被指定到的角色，而不是授予用户个人。虽然创建 ACG 的目标有助于控制用户的特权，但是，创建 ACG 的目的是将一组用户分组到单个对象中。

注意：对象不能映射至多个 ACG。

访问控制权是按如下方式使用的：

- 每个角色都可以包含多个用户
- 用户可以属于多个角色
- 每个访问控制组都包含许多对象（在此实例中，包含目录）

- 目录只能属于一个访问控制组
-

用户管理方案

John 已经花费了时间来创建一组用户和目录。现在，他希望通过使用角色和 ACG 来指定每个用户可以访问哪些目录以及定义他们的特权。

假定已经创建了用户和目录，并且尚未将目录指定给 ACG，下列各节将逐个步骤地完成下列任务：

- 创建新角色
- 创建新的访问控制组
- 将 ACG 指定给对象（目录）
- 给用户指定角色

创建新角色

1. 使用菜单路径：**数据模型管理器 > 安全性 > 角色控制台**。将显示“角色控制台”表。
2. 单击**新建**并输入“角色名”和“角色描述”（这两个是必需字段）。
3. 对于“访问控制组”，选择“缺省值”。
4. 为此角色选择一组特权。（注意：角色对特定访问控制组可以拥有的特权是在以后定义的；那些特权将是这里给出的特权的子集。）
5. 单击**保存**（位于屏幕顶部）。

总结

在保存新角色之后，该角色将显示在“角色控制台”表中，请参阅下图。注意，“已指定”列包含已指定了该角色的用户的数目。

注意：在管理用户时，必须给每个用户指定他们的用户概要文件中的至少一个角色。

创建新的访问控制组

1. 使用菜单路径：**数据模型管理器 > 安全性 > 访问控制组 > 访问控制组控制台**并单击**新建**。
2. 输入新的 ACG 的名称和描述。
3. 从下拉菜单中选择角色。
4. 为所选角色选择特权集合。（注意：这些特权用来控制用户可以执

行的操作。)

5. 单击**保存**。

将 ACG 指定给对象

下列操作将把 ACG 应用于目录。

1. 使用菜单路径：**数据模型管理器 > 安全性 > 访问控制组 > 对象到访问控制组映射**。将显示向导驱动的 GUI。
2. 选择对象类型“目录”。从“选择对象”下拉列表中选择目录。
3. 选择 ACG。这将把该目录指定给该控制组。

总结

现在，已创建了角色并将它们分组为不同的 ACG，并且已将 ACG 映射至目录。既然已经创建了所有特权，就可以给用户指定任何角色了，并且所选角色的所有特权都适用。

给用户指定角色

1. 使用菜单路径：**数据模型管理器 > 安全性 > 用户控制台**。将显示“当前用户”表。
2. 单击用户超链接以查看该用户的概要文件。从“当前用户的角色”表中，选择已给该用户指定的所有角色。
3. 单击**修改角色信息**。

总结

授予用户的特权是由用户被指定到的角色以及该角色所属的访问控制组确定的。

创建用户

在创建用户之前，在应用程序中必须存在至少一个角色。

1. 从左窗格中，选择“组织层次结构”。右键单击组织的名称并从菜单中选择“添加用户”。将显示“新建用户”屏幕。
2. 在“用户概要文件”界面中输入必需的详细信息。
3. 输入用户的密码。
4. 给该用户指定一个角色。可以根据职责选择多个角色。
5. 在输入了所需的所有信息之后，单击“保存”以存储该信息。
6. 最后一个步骤的目的是在系统中启用该用户。新用户的缺省状态始

终是“已禁用”。

启用用户

新用户在被删除后，他们处于禁用状态。要允许新用户访问应用程序，必须启用他们。

从菜单**数据模型管理器 > 安全性 > 用户控制台**中，单击**已禁用**按钮。该按钮更改为“已启用”。

访问控制组

访问控制组 — 使用 WebSphere Product Center 的访问控制组（ACG）来根据哪些用户可以查看 / 编辑特定的目录来设置许可权。创建访问组并将访问权指定给 ACG 中的每个角色。将 ACG 映射至对象。然后，根据用户的职责，给该用户指定了一个或多个角色。

可以将 ACG 应用于：

- 目录
- 协作区
- 层次结构
- 选择
- 工作流

可以通过创建用于限制对一组角色的访问权的规则来对各种对象设置特权。将对所有指定了那些角色的用户强制实施这些规则。

将 ACG 映射至对象

用来创建目录和层次结构的向导需要与 ACG 的关联。对于在 WebSphere Product Center 中创建的其它对象，情况亦如此。下表中列出的下列对象需要与 ACG 的关联。右列描述了如何将 ACG 映射至该对象。

对象	如何与 ACG 相关联
目录	“数据模型管理器” > “安全性” > “访问权” > “目录访问权控制台” 或者 “数据模型管理器” > “安全性” > “访问控制组” > “对象到访问控制组映射”
协作区	在创建协作区期间关联 ACG

层次结构	“数据模型管理器” > “安全性” > “访问权” > “层次结构访问权控制台” 或者 “数据模型管理器” > “安全性” > “访问控制组” > “对象到访问控制组映射”
选择	在创建选择时关联 ACG
工作流	在创建工作流期间关联 ACG

示例：使 ACG 与目录相关联

为了对目录实施访问控制，必须将该目录映射至 ACG，此操作是在创建目录期间完成的。

1. 使用菜单路径**产品管理器** > **目录** > **目录控制台**来显示“目录控制台”。
2. 单击**新建**以创建新目录。
3. 对于“选择访问控制组”步骤，创建 ACG 或选择现有的 ACG。

示例 — 应用用于选择的访问控制

可以根据指定给用户的角色的访问权定义来限制用户的访问权（查看选择、编辑选择规则和删除选择）。为了限制对选择的访问权，使用受限访问权定义的角色必须与“项选择”正在使用的 ACG 相关联。

因此，可以使单个选择可供特定 ACG 使用，作为该 ACG 一部分的所有角色都将能够访问该“项选择”。一旦给用户指定了该角色，就允许他们访问该“项选择”。

故障诊断

如果用户无法查看由 ACG 定义的项选择，则检查下列各项：

- 确保已启用该用户
- 进行检查，确保已给该用户指定了适当的角色
- 检查是否已按照步骤“创建新角色”中描述的那样正确定义了角色的访问权。
- 进行检查，了解该用户是否属于允许访问特定目录的 ACG。如果将用户设置为能够访问项选择，但不能访问目录，则该用户将看不到任何信息。

创建新角色并指定给 ACG

对于每个角色，可以实现三个领域的安全性：

- 组访问权 — 限制对每个相关联的 ACG 的角色的访问权
- 系统范围访问权 — 限制对各种应用程序功能部件的访问权
- 语言环境访问权 — 限制对一个或多个可用语言环境的访问权

在为角色设置特定于组的访问权时，建议您为 ACG “缺省” 选择访问权。ACG “缺省” 是在缺省情况下创建的，并且，当没有为对象选择定制 ACG 时，该对象将使用 ACG “缺省”。所有可以与 ACG 相关联的对象都要求有一个 ACG 与该对象相关联。因此，为该角色创建一组组访问权十分重要。

1. 使用菜单路径**数据模型管理器 > 安全性 > 角色控制台**，将显示“角色控制台”对话框。
2. 单击**新建**并为该角色输入名称和描述。对于本练习，使用名称“Basic View”。
3. 从“角色的特定于组的访问权”表中，为每个访问控制组选择组访问权。

注意在“ACG 控制台”中也会更新这些更改。

4. 单击**保存**以提交设置。将显示一条消息，指示角色创建成功。
5. 向下滚动到“角色的系统范围访问权”表；单击“编辑屏幕”超链接以访问“编辑屏幕访问权”页面。
6. 选择将允许该角色使用的屏幕。作为最低要求，必须选择下列屏幕：
 - 查看“WebSphere Product Center 主要”屏幕
 - 查看“WebSphere Product Center”屏幕
 - 查看“目录导航窗格”屏幕
 - 查看“我的主页”屏幕
 - 查看“协作控制台”屏幕
7. 单击**修改**以提交设置。

创建访问控制组

ACG 映射至各种对象，于是，那些对象强制实施该组的角色中定义的一组安全性规则。这些对象要求选择 ACG，如果不希望使用定制的 ACG，则选择 ACG “缺省”。

1. 使用菜单路径**数据模型管理器 > 安全性 > 访问控制组 > 访问控制组控制台**，将显示 ACG 控制台。
2. 单击**新建**并为 ACG 输入名称和描述。对于本练习，ACG 名为“E”。
3. 从下拉列表中选择任何角色。在下一节中，将创建一个新角色，并且将把该角色添加至 ACG。

4. 在“访问控制组”表中，选择下列复选框：

- 目录 — 列示
- 目录 — 查看
- 目录 — 搜索
- 选择 — 列示

5. 单击**保存**以创建新的 ACG。

对用户强制实施访问控制

要强制实施已经为 ACG 设置的访问控制规则，必须将该用户指定给该 ACG 的角色成员。

将角色指定给用户

在创建用户和角色之后，使用“用户控制台”来给用户指定角色。

1. 使用菜单路径**数据模型管理器 > 安全性 > 用户控制台**；将显示“当前用户”表。
2. 单击用户名。
3. 向下滚动到“当前用户的角色”表并选择先前创建的角色“Basic View”。
4. 单击“修改角色信息”以提交新的用户概要文件。

注意：任何指定了 Basic View 角色的用户对下一节中创建的项选择都将具有仅查看访问权。

访问权

设置访问权是对为 ACG 定义的安全性规则的扩展。通过使用 WebSphere Product Center 的“目录访问权控制台”，用户能够将目录的相关属性集合限制到一个或多个角色成员。

例如，当定义目录的访问权时，可以强制实施目录的属性集合的查看和 / 或编辑特权，从而提供对角色可以查看或编辑哪些目录属性的全面控制。如果已引入语言环境，则可以根据可用的语言环境来限制属性。

设置目录访问权

可以根据在“目录访问权控制台”中配置的一组已定义的特权来将角色限制到任何目录。被指定到该角色的用户将被限制为仅具有该目录的访问权。

创建规则以允许角色强制实施对任何目录的可查看和 / 或可编辑特

权。将需要为每个需要访问该目录的角色定义特权。

1. 从菜单路径**数据模型管理器 > 安全性 > 访问权 > 目录访问权控制台**，单击将要从中创建访问权的目录的名称旁边的**新建**按钮。将显示“目录访问权”向导。

2. 从下拉字段中选择角色。将只显示作为与所选目录相关的 ACG 的成员的角色。

3. 从“目录访问权编辑器”中，将属性集合设置为可查看或可编辑。

注意：属性旁边出现的“V”表示查看特权。“V+E”表示查看和编辑特权。

4. 要除去规则，从“已选择”框中单击属性集合并单击“除去”。

5. 在定义了所有特权之后，单击**保存**。将有一条消息指示已成功地保存了特权。

6. 如果您愿意的话，为所有相关联的角色创建特权。每个已定义了特权的角色都会显示在“目录访问权控制台”中。

7. 要编辑角色的特权，请从“目录访问权控制台”中单击“编辑”图标，在编辑器中进行更改，然后单击“保存”。

除去目录访问权

要除去一个角色的所有目录访问权，请执行下列操作：

1. 从“目录访问权控制台”中，单击“编辑”按钮以编辑该角色。

2. 突出显示“已选择的属性”框中的所有属性并单击**除去**。

3. 单击**保存**。返回至“目录访问权控制台”，该属性集合已被除去。

编辑角色访问权

限制角色的访问权，这将应用于任何指定了该特定角色的用户。在“编辑角色访问权”屏幕中所作的更改将在相关联的“访问控制组详细信息”和“系统范围访问权”页面中反映出来。

编辑角色访问权

1. 要编辑角色访问权，使用菜单路径**数据模型管理器 > 安全性 > 角色控制台**。将显示“角色控制台”表，该表包含已创建的角色列表。

2. 选择要编辑的角色，将显示“编辑角色访问权”页面。每个与该角色相关联的访问控制组都将显示在单独的列中。

3. 为每个访问控制组选择特定的访问权。在“角色的系统范围访问权”表中，单击“编辑屏幕”链接以限制对特定应用程序屏幕的访问权。

注意： 请参阅下表以获取角色访问权描述。

角色的特定于组的访问权	
目录	
列示	<p>允许在“目录控制台”中以及在整个 WebSphere Product Center 中的列表中显示目录</p> <p>如果未选择此项，则“目录控制台”指示“找不到目录”</p>
编辑目录视图	允许创建、删除和编辑目录视图
查看项	允许对目录项的仅查看访问权
添加项	允许创建新项。如果未选择此项，则所有用来添加项的按钮和短菜单都处于禁用状态
修改项	<p>允许修改项</p> <p>* 注意：如果未选择此项，则必须取消选择“添加项”和“将项重新分类”</p>
删除项	允许删除项。如果未选择此项，则“项编辑屏幕”中的“删除”按钮处于禁用状态
将项重新分类	<p>允许对目录中的项进行重新分类</p> <p>如果未选择此项，则“项编辑屏幕”中的“分类”按钮处于禁用状态</p>
总结项	不起作用。在将来的发行版中将除去此访问权
导出	允许从目录中导出目录项或项一类别属性值
属性	允许通过“目录控制台”中的“属性”按钮来访问属性页面
差别	允许显示两个目录之间的差别
回滚	允许回滚目录
搜索	允许对目录执行基本搜索或丰富搜索

删除	允许从“目录控制台”中删除目录
运行预览脚本	允许对项运行预览脚本（例如，“项 HTML 预览”和“项制表符定界预览”）
层次结构	
列示	<p>允许在“层次结构控制台”中以及在整个 WebSphere Product Center 中的列表中显示层次结构</p> <p>如果未选择此项，则“层次结构控制台”指示“找不到层次结构”</p>
编辑层次结构视图	允许创建、删除和编辑类别视图
查看层次结构节点	<p>允许对层次结构的仅查看访问权</p> <p>* 注意：如果未选择此项，则还必须取消选择“添加类别”、“修改类别名”和“修改类别属性”。</p>
添加层次结构节点	允许创建新类别
修改层次结构节点属性	<p>允许修改层次结构节点属性</p> <p>* 注意：如果未选择此项，则还必须取消选择“添加类别”</p>
删除层次结构节点	允许删除类别
将层次结构节点重新分类	允许对类别进行重新分类
总结层次结构节点	不起作用。在将来的发行版中将除去此访问权
规范映射层次结构节点	允许查看规范映射层次结构节点
属性	允许查看层次结构属性
回滚	允许回滚层次结构
删除	允许删除层次结构
选择	
列示	允许在“选择控制台”中显示选择
编辑规则	允许创建应用于选择的规则
删除	允许删除选择

导入	
列示	允许在“导入控制台”中显示导入
执行导入	允许启动导入以将目录项或项一类别属性值导入目录中
删除	允许删除导入
选择成员	
查看项	查看项选择
添加项	将项添加至选择
修改项	修改选择中的项
删除项	删除选择中的项
将项重新分类	对选择中的项进行重新分类
查看层次结构节点	查看选择中的层次结构节点
添加层次结构节点	在选择中添加层次结构节点
修改层次结构节点属性	更改选择中的层次结构节点属性
删除层次结构节点	删除选择中的层次结构节点
将层次结构节点重新分类	对选择中的层次结构节点进行重新分类
规范映射层次结构节点	在选择中创建规范映射层次结构节点
文档库	
查看文件	查看文档库中的文件
删除文件	删除文档库中的文件
采购订单导出	
列示	允许在“PO 导出控制台”中显示采购订单导出
导出	允许启动采购订单导出
删除	允许删除采购订单导出
工作流	
列示	允许在“工作流控制台”中显示工作流

编辑	允许编辑工作流
删除	允许删除工作流
协作区	
列示	
检出条目	允许在“协作控制台”中检出条目

角色的系统范围访问权	
规范	
修改规范	允许修改任何规范
修改规范映射	允许修改任何规范映射
屏幕	编辑屏幕 (单击此项以编辑屏幕访问权)
查看	允许访问在以上“编辑屏幕”中选择的屏幕。如果未选择此框，则该角色不可使用所选屏幕的列表。
脚本	
创建修改脚本	允许创建脚本。未选择此项时，“脚本控制台”中的“新建”按钮不会出现
调度程序	
查看公司作业	允许在“作业控制台”中显示作业
安全性	
修改用户	允许创建、删除和编辑用户
修改角色访问权	允许创建、删除和编辑角色

“角色的语言环境访问权”用来从角色的可用语言环境列表中进行选择。

角色的语言环境访问权	
可用的语言环境	在“管理公司属性”中已设置的可用语言环境的列表。
选择的语言环境	已提供给角色使用的所选语言环境的列表

编辑屏幕设置

可以将角色限制到特定的 WebSphere Product Center 屏幕。在“系统范围访问权”表中，单击“编辑屏幕”超链接，将显示“角色信息”表，该表包含屏幕的分层列表。

通过将屏幕名旁边的复选框保留为空白，可以限制角色不得访问每一个列示的屏幕。因此，选取的复选框允许访问该屏幕。在完成对屏幕的所有限制之后，单击“修改”以更新更改。

最低需求设置

尽管“编辑屏幕”的行为是相当直接的，但也有几个需要注意的特殊情况，下列各节对那些情况作了描述。

用户的主页由各种屏幕组成；因此，必须提供对每个屏幕的访问权。对于用户登录并查看主页而言，下列设置是最低要求。

- 查看“WebSphere Product Center 主要”屏幕
- 查看 WebSphere Product Center 屏幕
- 查看“目录导航窗格”屏幕
- 查看“我的主页”屏幕
- 查看“协作控制台”屏幕

如果具有对上述屏幕的访问权，用户主页就将显示“WebSphere Product Center 主要”、“导航窗格”和“协作控制台”。

如果取消选择了上述其中一个屏幕许可权，则您将接收到错误消息“您不具有查看此页面的特权”而不是看到“协作控制台”。

下列各节定义了“角色信息”表中的每个屏幕设置。

活动日志

可以通过 WebSphere Product Center 的“活动日志”来监视用户执行的活动。监视用户已访问了哪些页面、监视用户已编辑了哪些目录并

且通过电子邮件将活动实例通知另一个用户。创建新用户时，将把他们自动添加至“活动日志”中的用户列表。

配置活动日志

1. 使用菜单路径：**数据模型管理器 > 安全性 > 活动日志 > 活动日志**。
2. 通过单击适当的框选项，监视用户的活动、提供活动通知或者跟踪删除活动。
3. 要通过电子邮件接收更新，请单击“更新通知电子邮件”复选框并输入电子邮件地址。
4. 在配置了所有活动之后，单击“更新”。

查看用户活动

从“监视的用户”表中，选择“会话”、“日志”或“总结”以查看用户的当前活动。

- “会话”链接提供用户已访问过的页面的列表。
- “日志”链接显示用户已访问过的页面的日志。
- “总结”链接显示用户对一个页面的访问次数的总结。

通知用户

从“活动日志”屏幕中，可以创建消息并将其发送至所有用户或仅仅发送至当前已登录到应用程序的那些用户。“监视的用户”表显示了所有当前用户。该消息将被发送至用户的概要文件中定义的电子邮件地址或者“监视的用户”表中定义的通知电子邮件地址。此电子邮件地址可以与用户的概要文件中定义的电子邮件地址不同。

将消息发送至用户

1. 滚动到“活动日志”屏幕的末尾。在“通知用户”表中输入消息。
2. 进行选择以将消息发送至“活动日志”框中列示的所有用户或者仅仅发送至当前已登录的用户。
3. 单击**发送**，将把该消息发送至每个用户的电子邮件地址。