



访问控制权限(ACRs)

王元
AVEVA中国
2004.10.14



ACR的作用



- ▼ 访问控制权限Access Control Rights(ACR)
- ▼ ACR的作用
 - 限制用户操作命名的元素或者某一个类型的元素
 - 限制用户的操作，如生成，修改和删除
 - 限制用户能操作具体的属性

郑重提醒

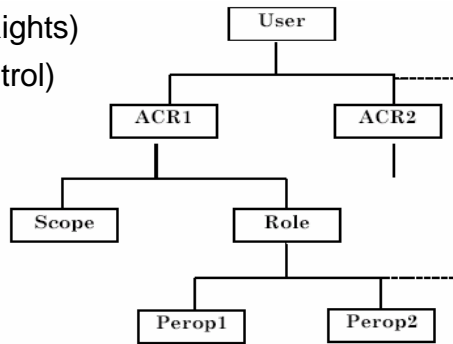


- ▼ 一旦决定使用DAC，所有普通用户(General users)都必须设置相应的ACR，否则用户对任何元素都没有写的权限
- ▼ ACR的顺序很重要
- ▼ 超级用户(Free users)始终具有所有权限

基本概念



- ▼ Permissible Operations (Perops)
- ▼ Role
- ▼ Scope
- ▼ ACR(Access Control Rights)
- ▼ DAC(Data Access Control)



VANTAGE Plant Design

ACRs, Roles and Scopes



- ▼ 每一个用户可以赋给一个或者多个访问控制权限 (ACRs), 每个ACR 包含两部分:
 - 角色Role, 定义用户对元素的操作, 如生成, 修改和删除所以类型的管道元素
 - 范围Scope, 定义角色的作用范围, 如具体的Zone或者一个范围内的模型
- ▼ 角色(Roles)和范围(Scopes)必须在ACR之前建立

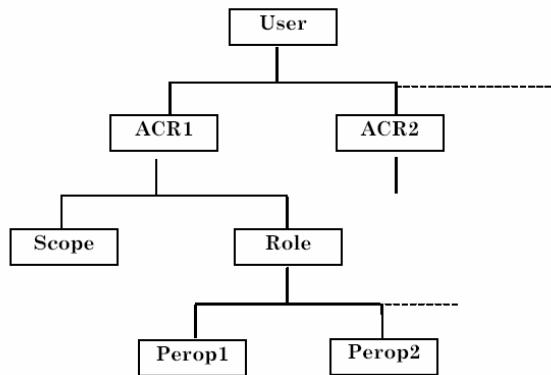
VANTAGE Plant Design

Permissible Operations (Perops)



▼ 可允许的操作 Permissible Operations (Perops)

- 角色包括很多的可允许的操作，每一个定义一种操作状态



VANTAGE Plant Design

权限不能有冲突



▼ 可允许的操作的应用规则

- 可允许的操作中必须让用户可以操作
- 可允许的操作中不能拒绝用户操作,一旦定义了不允许的操作,将覆盖已有的允许的操作

VANTAGE Plant Design

可允许的操作定义内容



- ▼ 对于每一个可允许的操作，定义如下内容
 - 元素类型
 - 在上述元素类型上的操作方式
 - 不允许的操作

操作控制(Perops)的选项说明



- ▼ 操作控制的选项说明
 - 忽略Ignore,没有定义用户允许操作,可能在其它的Perops中定义了允许的操作
 - 不允许操作Disallow,即使其它的Perops有允许的操作
 - 允许操作Allow,但是要保证其它的Perops没有不允许的操作



分区权限控制实例



分区权限控制示例约定

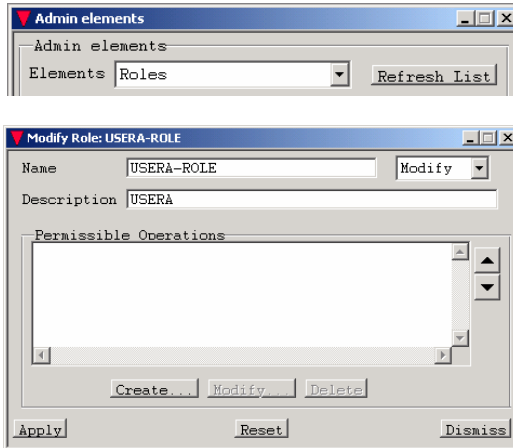


- ▼ 在SAM项目测试
- ▼ 管道设计数据库PIPE/DESI为多写数据库，由两人完成
 - USERA
 - USERB
- ▼ Zone的Area属性记录小分区的顺序号
 - USERA对应的Area = 1
 - USERB对应的Area = 2
- ▼ 每个设计人员只能修改属于自己的Zone及Zone以下层次

生成USERA的Roles



▼ 生成USERA的Roles



VANTAGE Plant Design

USERA可允许的操作



▼ 3项操作，操作顺序非常重要

- 生成Zone及以下层次，用户首先生成Zone
- 只能修改删除Area of Zone=0的Zone及以下层次，对其他的Zone没有权限，用户修改Zone的Area=1
- 只能修改删除Area of Zone=1的Zone及以下层次

VANTAGE Plant Design

USERA用户可允许的操作1



- ▼ **Perop1**:生成Zone及以下层次，第一个操作只用于生成，修改和删除随后定义

Perop	Elements	Operations	Attributes
USERACREATE	Zone Hierarchy	Create Allow Modify Ignore Delete Ignore Claim Ignore Issue Ignore Drop Ignore	All

Condition:true

VANTAGE Plant Design

Perop1: USERACREATE



- ▼ 生成**Perop1**:
USERACREATE

VANTAGE Plant Design

USERA用户可允许的操作2



- ▼ **Perop2**:只能修改删除Area of Zone=0的Zone及以下层次，对其他的Zone没有权限

Perop	Elements	Operations	Attributes
USERAMODIFY	Zone Hierarchy	Create	Ignore All
		Modify	Allow
		Delete	Allow
		Claim	Allow
		Issue	Ignore
		Drop	Ignore

Condition: Area OF ZONE Eq 0

VANTAGE Plant Design

Perop2: USERAMODIFY



- ▼ 生成**Perop2**:
USERAMODIFY

VANTAGE Plant Design

USERA用户可允许的操作3



▼ Perop3:只能修改删除Area of Zone=1的Zone及以下层次

Perop	Elements	Operations	Attributes
USERADELETE	Zone Hierarchy	Create Ignore Modify Allow Delete Allow Claim Allow Issue Ignore Drop Ignore	All

Condition:Area OF ZONE EQ 1

VANTAGE Plant Design

Perop3: USERADELETE



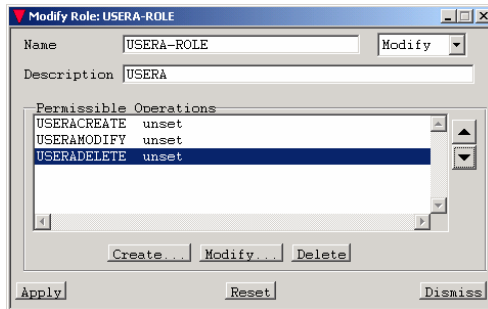
▼ 生成Perop3:
USERADELETE

VANTAGE Plant Design

完成USERA用户可允许的操作设置



▼ 完成后的效果

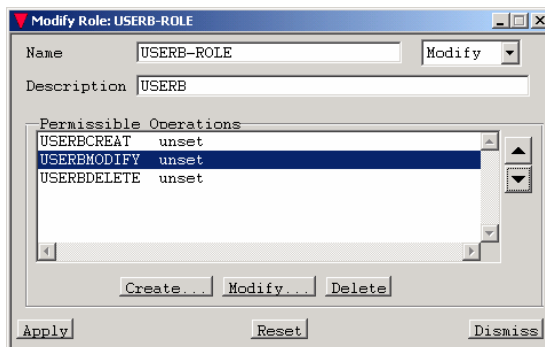


VANTAGE Plant Design

USERB用户可允许的操作



▼ USERB用户可允许的操作设置与USERA方法一样

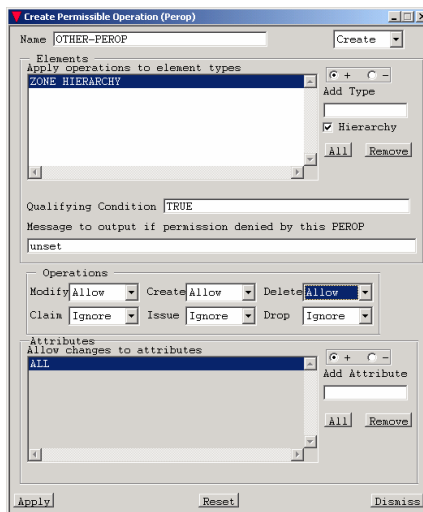


VANTAGE Plant Design

其它用户可允许的操作



- ▼ 其它用户可允许的操作必须设置,只允许操作Zone

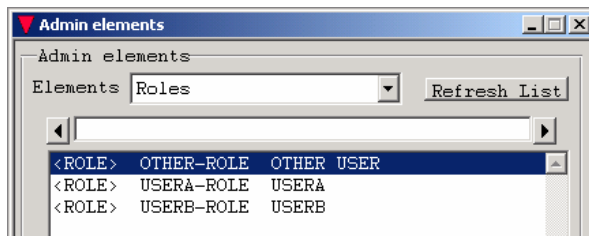


VANTAGE Plant Design

完成Role的定义



- ▼ 完成后的效果

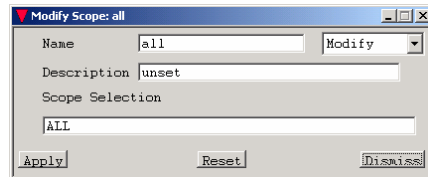
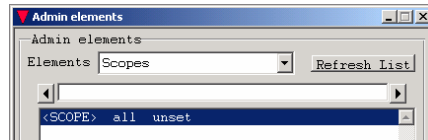


VANTAGE Plant Design

生成Scopes



▼ 没有特殊限制

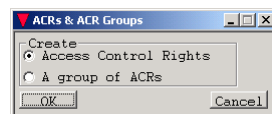
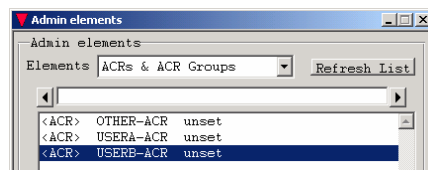


VANTAGE Plant Design

生成ACR



▼ 生成ACR

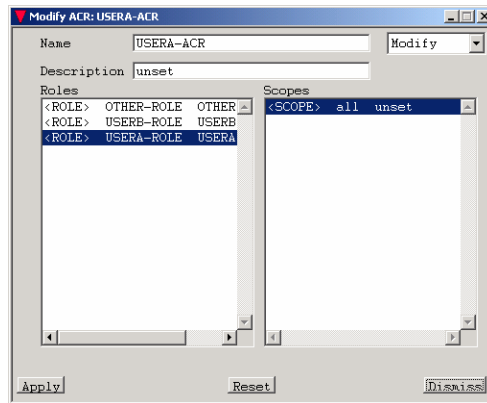


VANTAGE Plant Design

USERA-ACR



▼ USERA-ACR关联Role与Scope

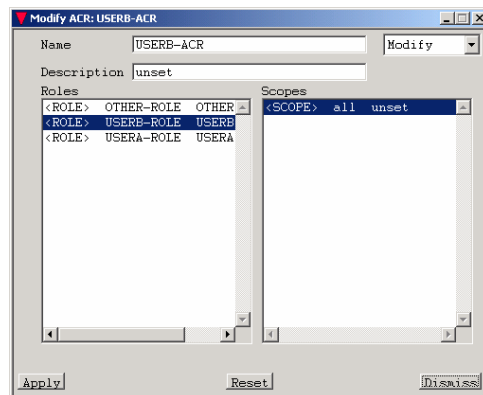


VANTAGE Plant Design

USERB-ACR



▼ USERB-ACR关联Role与Scope

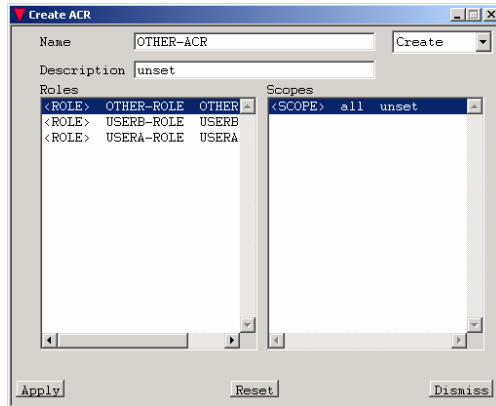


VANTAGE Plant Design

OTHER-ACR



▼ OTHER-ACR关联Role与Scope

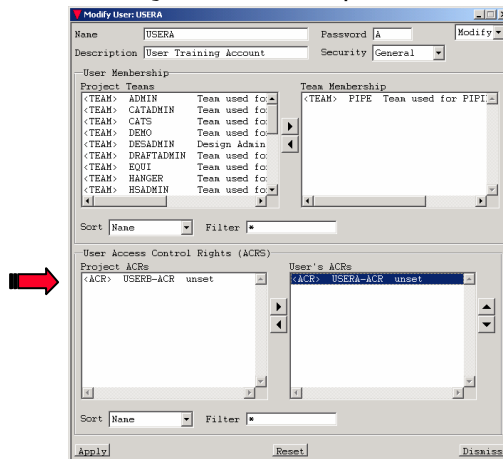


VANTAGE Plant Design

给用户USERA添加访问控制权限



▼ 进入USERA的用户定义窗口,将Project ACR中的USERA-ACR加入到用户USERA的User's ACR中

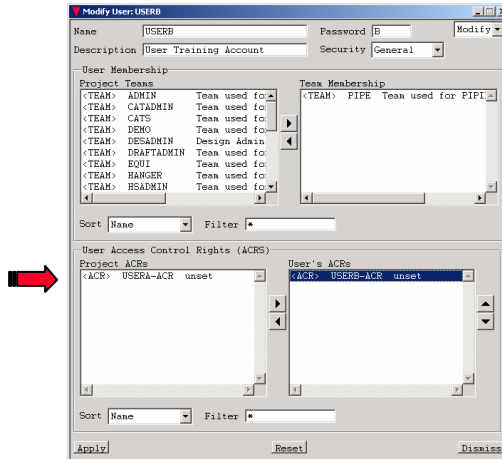


VANTAGE Plant Design

给用户USERB添加访问控制权限



- ▼ 进入USERB的用户定义窗口,将Project ACR中的USERB-ACR加入到用户USERB的User's ACR中



VANTAGE Plant Design

给其它用户添加访问控制权限



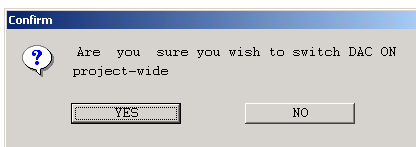
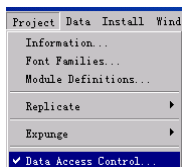
- ▼ 为项目中的每一个用户添加访问控制权限OTHER-ACR

VANTAGE Plant Design

打开DAC



▼ 打开DAC(Data Access Control)



▼ 开始使用

VANTAGE Plant Design



支吊架设计权限控制实例



支吊架设计程序约定



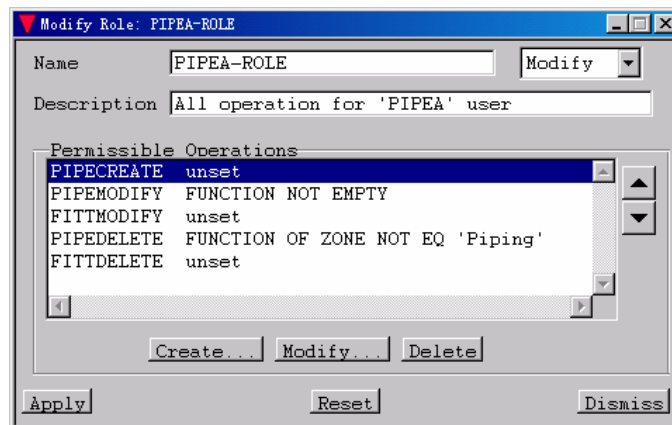
- ▼ 结构数据库为多写数据库，支吊架设计人员具有写权限
- ▼ 埋件Fitting中的Function属性记录用户的名字
- ▼ 每个支吊架设计人员只能修改自己提出的埋件
- ▼ 结构设计人员只能修改自己添加的埋件

VANTAGE Plant Design

生成管道用户的Roles



- ▼ ‘PIPEA’ 是一个用户的Name



VANTAGE Plant Design

管道用户可允许的操作



▼ 5项操作，其中3项针对管道操作

- 生成Zone及以下层次，不能修改删除
- 只能修改删除Func of Zone=unset的Zone及以下层次，对其他的Zone没有权限
- 只能修改删除Func of Zone='Piping'的Zone及以下层次

▼ 2项针对埋件操作

- 只能修改删除Func of CE=unset的Fitt,Pfit
- 只能修改删除Func of CE='PIPEA'的Fitt,Pfit

PIPEA用户可允许的操作1



▼ Perop1:生成Zone及以下层次，不能修改删除

Perop	Elements	Operations		Attributes
PIPEACREATE	Zone Hierarchy	Creat	Allow	All
		Modify	Ignore	
		Delete	Ignore	
		Claim	Ignore	
		Issue	Ignore	
		Drop	Ignore	

Condition:true

PIPEA用户可允许的操作2



- ▼ Perop2:只能修改删除Func of Zone=unset的Zone及以下层次，对其他的Zone没有权限

Perop	Elements	Operations		Attributes
PIPEAMODIFY	Zone Hierarchy	Creat	Ignore	All
		Modify	Allow	
		Delete	Allow	
		Claim	Allow	
		Issue	Ignore	
		Drop	Ignore	

Condition:EMPTY (FUNC OF ZONE)

VANTAGE Plant Design

PIPEA用户可允许的操作3



- ▼ Perop3:只能修改删除Func of Zone='Piping'的Zone及以下层次

Perop	Elements	Operations		Attributes
PIPEADELETE	Zone Hierarchy	Creat	Ignore	All
		Modify	Allow	
		Delete	Allow	
		Claim	Allow	
		Issue	Ignore	
		Drop	Ignore	

Condition:FUNC OF ZONE EQ 'Piping'

- ▼ 埋件Fitt在结构的Zone层次中，不会被删除

VANTAGE Plant Design

PIPEA用户可允许的操作4



▼ Perop4:只能修改删除Func of CE=unset的Fitt,Pfit

Perop	Elements	Operations	Attributes
PIPEAFITTMOD	FITT	Creat	Ignore All
	PFIT	Modify	Allow
		Delete	Allow
		Claim	Allow
		Issue	Ignore
		Drop	Ignore

Condition:EMPTY (ATTRIB FUNC OF CE)

▼ Func属性中需要写入User的Name，用于区分不同用户创建的埋件，如Func='PIPEA'

VANTAGE Plant Design

PIPEA用户可允许的操作5



▼ Perop5:只能修改删除Func of CE='PIPEA'的Fitt,Pfit

Perop	Elements	Operations	Attributes
PIPEAFITTDEL	FITT	Creat	Ignore All
	PFIT	Modify	Allow
		Delete	Allow
		Claim	Allow
		Issue	Ignore
		Drop	Ignore

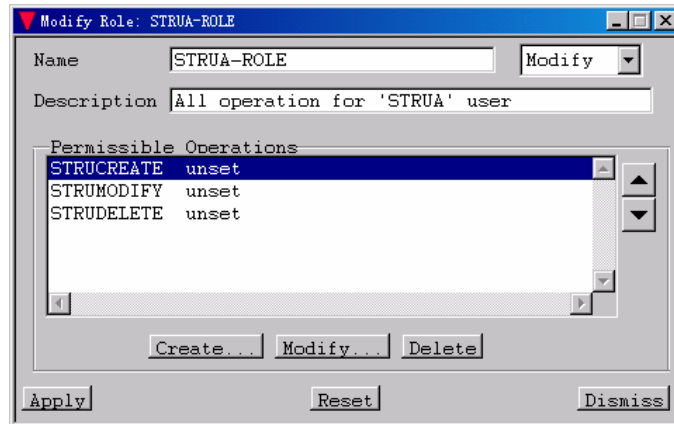
Condition:FUNC OF CE EQ 'PIPEA'

VANTAGE Plant Design

生成结构用户的Roles



▼ ‘STRUA’ 是一个用户的Name



VANTAGE Plant Design

结构用户可允许的操作



▼ 5项操作，其中3项针对结构操作

- 生成Zone及以下层次，不能修改删除
- 只能修改删除Func of Zone=unset的Zone及以下层次，对其他的Zone没有权限
- 只能修改删除Func of Zone='Steelwork'的Zone及以下层次，不能修改删除埋件Fitt

▼ 2项针对埋件操作

- 只能修改删除Func of CE=unset的Fitt,Pfit
- 只能修改删除Func of CE='STRUA'的Fitt,Pfit

VANTAGE Plant Design

STRUA用户可允许的操作1



▼ Perop1:生成Zone及以下层次，不能修改删除

Perop	Elements	Operations		Attributes
STRUACREATE	Zone Hierarchy	Creat	Allow	All
		Modify	Ignore	
		Delete	Ignore	
		Claim	Ignore	
		Issue	Ignore	
		Drop	Ignore	

Condition:true

VANTAGE Plant Design

STRUA用户可允许的操作2



▼ Perop2:只能修改删除Func of Zone=unset的Zone及以下层次，对其他的Zone没有权限

Perop	Elements	Operations		Attributes
STRUAMODIFY	Zone Hierarchy	Creat	Ignore	All
		Modify	Allow	
		Delete	Allow	
		Claim	Allow	
		Issue	Ignore	
		Drop	Ignore	

Condition:EMPTY (FUNC OF ZONE)

VANTAGE Plant Design

STRUA用户可允许的操作3



- ▼ Perop3:只能修改删除Func of Zone='Steelwork'的Zone及以下的层次

Perop	Elements	Operations		Attributes
STRUADELETE	Zone Hierarchy	Creat	Ignore	All
		Modify	Allow	
		Delete	Allow	
		Claim	Allow	
		Issue	Ignore	
		Drop	Ignore	

Condition:FUNC OF ZONE EQ 'Steelwork' AND FUNC OF CE EQ "

- ▼ 因为支吊架埋件的Func都记录了User name,不允许删除

VANTAGE Plant Design

STRUA用户可允许的操作4



- ▼ Perop4:只能修改删除Func of CE=unset的Fitt,Pfit

Perop	Elements	Operations		Attributes
STRUAFITTMOD	FITT	Creat	Ignore	All
	PFIT	Modify	Allow	
		Delete	Allow	
		Claim	Allow	
		Issue	Ignore	
		Drop	Ignore	

Condition:EMPTY (ATTRIB FUNC OF CE)

- ▼ Func属性中需要写入User的Name，用于区分不同用户创建的埋件，如Func='STRUA'

VANTAGE Plant Design

STRUA用户可允许的操作5



▼ Perop5:只能修改删除Func of CE='STRUA'的Fitt,Pfit

Perop	Elements	Operations	Attributes
STRUAFITTDDEL	FITT	Creat Ignore All	
	PFIT	Modify Allow	
		Delete Allow	
		Claim Allow	
		Issue Ignore	
		Drop Ignore	

Condition: FUNC OF CE EQ 'STRUA'

VANTAGE Plant Design

其它用户可允许的操作



▼ 其它用户可允许的操作必须设置,只允许操作Zone

The screenshot shows the 'Create Permissible Operation (Perop)' dialog box. The 'Name' field is 'OTHER-PEROP'. The 'Elements' list contains 'ZONE HIERARCHY'. The 'Qualifying Condition' is set to 'TRUE'. The 'Message to output if permission denied by this PEROP' is 'unset'. The 'Operations' section shows 'Modify' set to 'Allow', 'Create' set to 'Allow', 'Delete' set to 'Allow', 'Claim' set to 'Ignore', 'Issue' set to 'Ignore', and 'Drop' set to 'Ignore'. The 'Attributes' list contains 'All'. The 'Apply' button is highlighted.

VANTAGE Plant Design

生成Scopes



▼ 没有特殊限制

Modify Scope: ALL

Name: ALL Modify

Description: unset

Scope Selection: ALL

Apply Reset Dismiss

VANTAGE Plant Design

生成ACR



▼ 生成PIPEA-ACR,关联Role与Scope

Modify ACR: PIPEACR

Name: PIPEA-ACR Modify

Description: unset

Roles

<ROLE>	STRUA	All operat
<ROLE>	PIPEA	All operat

Scopes

<SCOPE>	ALL	unset
---------	-----	-------

Apply Reset Dismiss

VANTAGE Plant Design

生成STRUA-ACR



▼ 生成STRUA-ACR，关联Role与Scope

Modify ACR: STRUA-ACR

Name: STRUA-ACR Modify

Description: unset

Roles:

<ROLE>	STRUA	All operat
<ROLE>	PIPEA	All operat

Scopes:

<SCOPE>	ALL	unset
---------	-----	-------

Apply Reset Dismiss

VANTAGE Plant Design

OTHER-ACR



▼ OTHER-ACR关联Role与Scope

Create ACR

Name: OTHER-ACR Create

Description: unset

Roles:

<ROLE>	OTHER-ROLE	OTHER
<ROLE>	USERB-ROLE	USERB
<ROLE>	USERA-ROLE	USERA

Scopes:

<SCOPE>	all	unset
---------	-----	-------

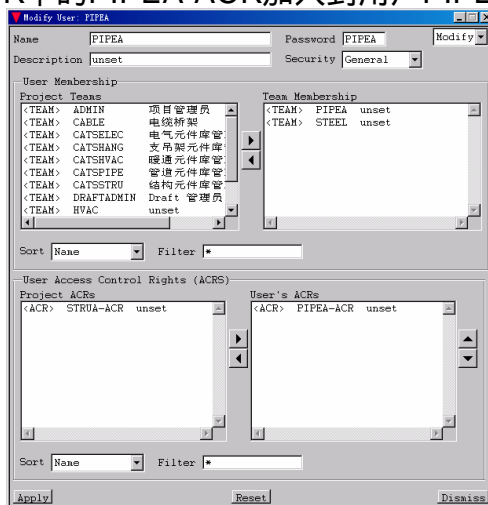
Apply Reset Dismiss

VANTAGE Plant Design

给用户添加权限控制



- ▼ 将Project ACR中的PIPEA-ACR加入到用户PIPEA的ACR中

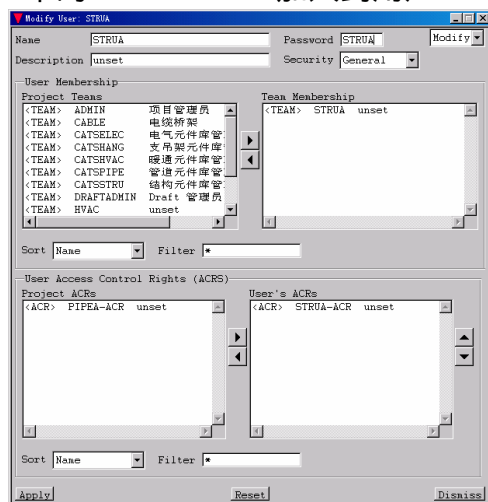


VANTAGE Plant Design

给用户添加权限控制



- ▼ 将Project ACR中的STRUA-ACR加入到用户STRUA的ACR中



VANTAGE Plant Design

给其它用户添加访问控制权限



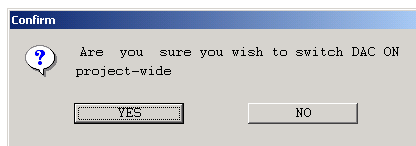
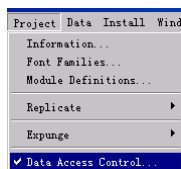
- ▼ 为项目中的每一个用户添加访问控制权限OTHER-ACR

VANTAGE Plant Design

打开DAC



- ▼ 打开DAC(Data Access Control)



- ▼ 开始使用

VANTAGE Plant Design

AVEVA™