权限中心人员同步 AD同步部分

技术手册

远洋地产有限公司

版本.1草稿

沈峥

顾问

shenzheng@microsoft.com

版本历史

变更记录

|  |  |  |  |
| --- | --- | --- | --- |
| 日期 | 作者 | 版本 | 变更内容 |
| 2013-9-27 | 危仁飞 | .1 | 建立文档 |
|  |  |  |  |
|  |  |  |  |

审阅记录

|  |  |  |  |
| --- | --- | --- | --- |
| 姓名 | 审阅版本 | 职位 | 日期 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

适用用户

用户说明

|  |  |
| --- | --- |
| 用户 | 说明 |
| 开发用户 | 指对项目源代码进行开发的人员，包括对项目进行二次开发的人员，对项目进行bug修复的人员以及修改源代码的其他人员。 |
| 维护用户 | 对项目进行配置维护，数据维护的人员，不改变项目源代码 |
| 使用用户 | 指使用该项目的项目人员，不改变项目源代码 |

适用参考

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 章节 | 开发用户 | 维护用户 | 使用用户 | 页码范围 |
| 项目介绍 | √ | √ | √ | 7 |
| 开发说明 | √ |  |  | 12 |
| 使用说明 | √ | √ | √ | 23 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

内容大纲

[1. 总体介绍 5](#_Toc369341997)

[1.1. 目标 5](#_Toc369341998)

[1.2. 范围 5](#_Toc369341999)

[1.3. 内容 5](#_Toc369342000)

[1.4. 术语 5](#_Toc369342001)

[2. 项目介绍 7](#_Toc369342002)

[2.1. 概要介绍 7](#_Toc369342003)

[2.2. 同步逻辑介绍 8](#_Toc369342004)

[2.3. 正向同步过程 10](#_Toc369342005)

[2.4. 反向同步过程 11](#_Toc369342006)

[3. 开发说明 12](#_Toc369342007)

[3.1. 程序集说明 12](#_Toc369342008)

[3.2. 配置说明 12](#_Toc369342009)

[3.3. 开发说明 15](#_Toc369342010)

[3.3.1. 数据库说明： 15](#_Toc369342011)

[3.3.2. MCS.Library.SOA.Security.ADSyncUtilities程序集 15](#_Toc369342012)

[4. 使用说明 19](#_Toc369342013)

[4.1. 权限中心AD同步的WebService 19](#_Toc369342014)

[4.2. 通过程序发起同步 19](#_Toc369342015)

[4.3. 通过权限中心手动发起 19](#_Toc369342016)

[4.4. 查看同步操作日志 19](#_Toc369342017)

1. 总体介绍
   1. 目标

介绍远洋地产权限中心AD同步服务, 包括权限中心AD介绍, 设计理念, 使用, 开发, 部署及与其他系统的结合. 保证代码规范性和一致性，提高代码质量，降低代码维护难度。

## 范围

本文档主要适用于远洋地产权限中心项目使用, 开发, 部署阶段。适用人员包括项目负责人、架构人员、开发人员、测试人员。

## 内容

第２节项目介绍, 包括术语说明, 功能说明, 设计理念

第3节开发说明, 包括配置，类型介绍，数据库说明

第4节使用说明,

## 术语

* 平台服务： 远洋地产项目应用架构的一种服务(还包括业务服务和专业服务), 对业务服务和专业服务提供服务, 是服务的服务. 与具体流程无关, 独立的.
* 自定义控件: 已编译的服务器端控件, 它将用户界面和其他功能封装到可用的包内. 开发者可以和使用.Net自带的控件一样使用.
* AD(Active Directory):在微软Windows Server上运行的目录服务。
* DC（Domain Controller）:域控制器，是一个在Windows服务器域中的接受安全认证请求（登录，检查权限，等）的服务器。
* 权限中心：管理机构人员，应用授权的一整套的解决方案和服务。
* 人员(用户)：在AD中，为用户（User），在权限中心，对应的是人员。权限中心，人员可以位于多个组织中，也可以没有组织单独存在，而AD中，人员只允许且必须出现在一个组织中。
* DN（Distinguished Names）：可辨识名称。活动目录中的每一个对象都有一个可辨识名称，可辨识名称包含对象在名字空间中的完整路径名，该名称由多个顺序排列的由逗号分隔的相对可辨识名称（RDN）组成，从基本的名字空间包容器开始，通过层层包容器对象，一直到达对象节点。不同的名字空间有不同的标识名命名规则，ADSI提供了一个命名框架，通过名字即可识别相应的目录服务和名字空间。
* RDN(Ralative distinguished names):是一个属性和关联的值，格式为 属性=值，值由UTF-8编码的字符表示。每个属性表示不同的含义，见下：

|  |  |
| --- | --- |
| **属性** | **属性类型** |
| **DC** | domainComponent |
| **CN** | commonName |
| **OU** | organizationalUnitName |
| **O** | organizationName |
| **STREET** | streetAddress |
| **L** | localityName |
| **ST** | stateOrProvinceName |
| **C** | countryName |
| **UID** | userid |

* 群组（组）：在AD中，为组（Group），在权限中心，对应的是群组。群组是人员的容器。
* 组织：在AD中，为组织（Organization），在权限中心，对应的是组织。组织对人员和群组进行分层管理。在AD中，组织中亦包含其他对象。

# 项目介绍

* 1. 概要介绍

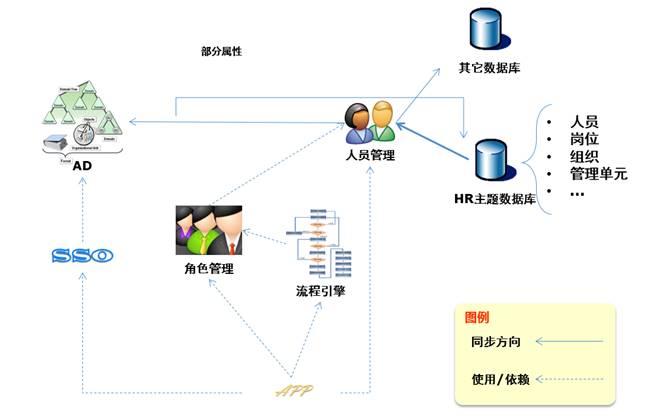
AD同步是新版权限中心业务功能的一个重要部分。虽然在旧版权限中心中也存在AD同步的功能，但是同步源和同步方向是不同的。在新版权限中心，机构人员管理工作主要在权限中心中完成。除了邮件地址，Lync地址等属性，人员数据由权限中心同步至AD，而不是反过来。同时，HR数据也将直接进入权限中心而不是AD（规划中）。

AD中的组织结构与权限中心类似，但是仍有如下不同点：

1、AD中人员只能属于一个组织，权限中心中人员可以属于不同的组织甚至无组织。

2、AD中组织中可以包含其他类型的对象。

3、AD中的数据一旦删除则无法恢复。考虑到权限中心的设计特点，因此在AD中保留一个特殊的组织，用来存放删除的对象（如果对象在权限中心中被移动到同步范围外，则在AD中也意味着删除），在必要时，还可以进行恢复。



* 1. 同步逻辑介绍

**权限中心同步逻辑**

新版权限中心与AD进行人员，群组和组织机构同步。数据以权限中心为准[[1]](#footnote-1)，向AD同步。同步时，有如下规则：

人员：只同步选定分支的组织树中担任主职的现有用户。如果该人员在此分支中无主职，将随机挑选其中的一个兼职作为主职同步至AD中。人员优先以ID为标识符，其次是登录名。如果人员在权限中心存在而AD中不存在，则人员在AD中被创建。如果人员已存在，但位置不同，则将人员从AD移动到对应的位置。如果人员在权限中心不存在，而在AD中存在，则人员被移动到回收站。

组织：同步选定分支的组织树中的组织。组织优先以ID作为唯一标识符，其次是路径名称。如果组织在AD中不存在，则在AD中创建对应的组织。如果组织在AD中不存在，则将组织包括其下级对象移动到回收站。

群组：同步选定分支组织树中的群组。优先以ID为标识符，其次是登录名。如果群组在权限中心中存在而AD中不存在，则群组在AD中被创建，如果群组已存在，但位置不同，则群组将从AD中的当前位置移动到对应的位置。如果群组在权限中心不存在，而在AD中存在，那么取决于此群组是否是由同步程序创建，会分别移动到回收站，或者不进行任何操作。

群组中的人员：如果此群组为权限中心中的群组，那么在AD中必有对应的群组，群组中的人员为AD同步的分支中存在的人员，同步后，多余的人员会被剔除。如果此群组为AD中创建的但并非在权限中心有对应的群组，那么次群组会被忽略不进行任何修改。

**同步策略**

同步时，仅进行增量同步。同步前进行数据对比，仅对差异的部分进行同步。

**属性同步逻辑**

1、简单属性：简单属性为权限中心和AD中均为字符串的属性，这种属性可以直接对应。

2、路径（可分辨名称）：在权限中心中为对象的一个固有属性，在AD中表现为一个只读的属性，但是格式不同。例如权限中心中路径为：机构人员\远洋地产\集团总部\流程管理部\曹会超，而AD中使用DN来表示: CN=A-曹会超,OU=流程管理部,OU=集团总部,OU=远洋地产,DC=sinooceanland,DC=com。

3、布尔值和枚举属性：在权限中心中为布尔值，在AD中为枚举值，并且对应枚举值的部分位。例如DontExpirePassword属性。

4、日期值：权限中心中为日期，在AD中也为日期，但日期在AD中表示为一个大整数。

5、多值属性：权限中心中为以分号分隔的字符串值，在AD中为一个多值属性。例如OtherMP属性。

6、特殊类型：在权限中心和AD中属性不直接对应。典型的是照片属性，在权限中心，它是一个序列化的图片描述字符串，在AD中，是一个二进制数组。这让比较和同步都与其他属性不同。在权限中心，提供的是照片的描述字符串，其中包含这个照片的最后更新时间。在AD，使用pager属性来保存最后更新日期，使用thumbnailPhoto属性来保存照片数据。比较的时候，只比较更新日期。

下表列出各个对象的属性同步规则，其中同步方式“→”表示正向同步，“←”表示反向同步。其中userAccountControl为枚举值属性，otherMobile为多值属性，照片含有2部分，一部分是标记属性，一部分是二进制值属性。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 对象 | 属性 | 权限中心接口属性 | AD属性 | 同步方式 |
| 通用 | 名称 | OBJ\_NAME | name | → |
| 通用 | 显示名称 | DISPLAY\_NAME | displayName | → |
| 通用 | 排序号 | INNER\_SORT | adminDisplayName | → |
| 通用 | 全局序号 | GLOBAL\_SORT | extensionName | → |
| 通用 | 全路径 | ALL\_PATH\_NAME | distinguishedName | →移动 |
| 用户 | 代码名称 | LOGON\_NAME | samAccountName | → |
| 用户 | 名 | FIRST\_NAME | givenName | → |
| 用户 | 姓 | LAST\_NAME | sn | → |
| 用户 | 移动电话 | MP | mobile | → |
| 用户 | 工作电话 | WP | telephoneNumber | → |
| 用户 | 账户禁用 | AccountDisabled | userAccountControl | →（枚举值） |
| 用户 | 账户不需要密码 | PasswordNotRequired | userAccountControl | →（枚举值） |
| 用户 | 密码不过期 | DontExpirePassword | userAccountControl | →（枚举值） |
| 用户 | 账户过期 | AccountExpires | accountExpires | → |
| 用户 | 其他电话 | OtherMP | otherMobile | →（多值） |
| 用户 | 公司 | CompanyName | company | → |
| 用户 | 部门 | DepartmentName | department | → |
| 用户 | 级别名 | RANK\_NAME | title | → |
| 用户 | 照片时间 | PhotoTimestamp | pager，thumbnailPhoto | →（照片标记和照片数据） |
| 用户 | 邮件地址 | Mail | mail | ← |
| 用户 | Lync地址 | Sip | msRTCSIP-PrimaryUserAddress | ← |
| 群组 | 代码名称 | LOGON\_NAME | samAccountName | → |
| 组织 | 代码名称 | CODE\_NAME | adminDescription | → |

对于群组成员，权限中心接口提供的是一个对象属性Members，而AD中表现为一个普通属性member，这个属性是个多值属性，每个属性值为一个人员的DN。

为了区别AD中用户创建的群组和由权限中心在AD中建立的群组，我们借用Group的属性displayNamePrintable，当这个属性存在并且值为“{\_\_pc\_involved\_\_}”时，表示此群组为权限中心控制的。这个属性在进行群组创建和配对后会自动被加上。，

* 1. 正向同步过程

**同步策略**

1、初始化同步上下文。

2、对同步 上下文使用锁。避免多个用户同时发起同步。在同步的各个阶段都需要不停的对锁进行延续操作，避免锁过期。如果同步时，已经被其他同步锁定无法加锁，则退出。

3、保存同步上下文。这将在权限中心中记录本次同步。

3、准备同步分支。这包括确保同步分支节点和AD目标节点均存在，创建回收站等。

4、比对和配对数据，并将差异登记到同步上下文中。这个过程会比较权限中心的对象和AD中对象的差异，并自动将已存在的对象进行配对和保存到同步上下文。

5、应用修改。对上下文中登记的差异，逐条将改动应用到AD中。更新权限中心与AD中对应对象的ID映射表。对于发生的任何错误，都将登记到权限中心AD同步日志中。

6、同步结束，更新日志状态。

7、解除同步上下文的锁。这将允许下一次同步。

其中比对数据和应用修改都是一个复杂的过程。

**冲突策略**

1、名称冲突，要添加或移动的目的位置已经存在同名的对象，造成添加或移动失败，但目标位置的同名对象应该被删除或改名或移动到其他位置。这种情况下，先将被移动的对象改名为一个临时名称，然后进行创建或移动，并登记延迟改名操作，在同步的最后阶段，将目标改名为实际的名称。

2、群组成员的策略。群组成员的修改，必须是所有人员修改完成之后来进行比对和修改。因为群组成员根据人员的DN路径来比对和保存，因此要等待人员位置确定之后才可以进行。

**属性修改的规则**

1、对象创建时，需要使用RDN来创建。

2、密码使用其他方式修改。

3、对象名称使用专用的Rename方式来修改。

4、移动对象用MoveTo方法。

5、部分属性在修改后必须进行Commit后才可以修改其他属性。

* 1. 反向同步过程

反向同步逻辑相对简单。

1、初始化同步上下文。

2、对上下文使用锁。

3、将同步日志写入数据库。

4、从数据库中载入ID映射。

5、分批查询AD中的用户和权限中心的用户，找到对应的属性，跟权限中心的数据属性进行比对。如果存在差异，将差异合并到权限中心。

6、更新同步日志，包括同步的最终结果。

7、释放同步上下文锁。

# 开发说明

* 1. 程序集说明

1、MCS.Library.SOA.Security.ADSyncUtilities：AD同步的程序集

2、PermissionCenterServices：权限中心服务的Web应用。

3、MCS.Library.SOA.DataObjects.Security：权限中心

4、MCS.Library.ADHelper：访问目录服务的类库。

5、MCS.Library.OGUPermission：权限中心接口类库。

* 1. 配置说明

参照：全局配置serverInfoConfigSettings.config，serverInfoConfigSettings.config，PermissionCenterServices项目的web.config，全局配置

1、配置AD服务器，配置节类型

MCS.Library.Configuration.ServerInfoConfigSettings, MCS.Library

<serverInfoConfigSettings>

<serverInfos>

<add name="dc" serverName=" AD服务器IP地址" identityName="domainUser" port="0" authenticateType="NTLM"/>

<add name="smtp" serverName="exmbsrv.sinooceanland.com" identityName="smtpSender" port="25" authenticateType="Basic"/>

</serverInfos>

</serverInfoConfigSettings>

2、配置AD服务器账号，配置节类型

MCS.Library.Configuration.IdentityConfigSettings, MCS.Library

<identityConfigSettings>

    <identities>

<add name="documentServer" userId="登录 DC的用户名" domain="域名" password="登录口令" />

</identities>

</identityConfigSettings>

3、配置属性比较器，配置节类型

MCS.Library.SOA.DataObjects.Security.Transfer.PropertyComparersSettings, MCS.Library.SOA.DataObjects.Security

包含2个集合属性objectComparers和propertyComparers，分别注册对象和属性的比较器。

4、属性设置器，配置节类型

MCS.Library.SOA.DataObjects.Security.Transfer.PropertySettersSettings, MCS.Library.SOA.DataObjects.Security

包含2个集合属性objectSetters和propertySetters，分别注册对象和属性的设置器。

5、AD属性映射配置，配置节类型

MCS.Library.SOA.Security.ADSyncUtilities.PermissionCenterToADSynchronizeSettings, MCS.Library.SOA.Security.ADSyncUtilities

对属性进行介绍

defaultStartPath：缺省开始路径。指定一个权限中心的组织路径，表示从哪个组织开始同步。当未指定同步路径时，从此路径开始同步。

sourceRoot：源根路径。指定一个权限中心组织路径，表示此路径映射到AD的根路径。

recycleBinOU：指定一个DN，表示AD中回收站的可辨识名称。

targetRootOU：指定一个DN，表示在AD中对应权限中心源根组织的一个组织的DN。

defaultPassword：指定一个字符串，表示创建用户时，为用户指定的缺省的口令。

objectMappings元素：包含一个或多个配置，每个配置表示权限中心的组织跟AD中组织的名称映射。注意此名称应该分别在源根组织和目标根组织中存在，并且是直接的子级。配置的范例如下：

<add name="adTest" scObjectName="AD测试" adObjectName="OU=AD测试" />

schemaMappings：包含一个或多个配置，定义类型和类型的属性映射。类型可以继承。配置项范例如下

<add name="Users" inherited="Base" comparerName="UserObjectComparer" prefix="CN">

</add>

|  |  |  |
| --- | --- | --- |
| 属性 | 类型 | 说明 |
| name | 字符串 | 权限中心对象类型的名称 |
| inherited | 字符串 | 如果此类型为派生类型，则为基类型的名称 |
| comparerName | 字符串 | 指定关联的对象比较器配置项名 |
| prefix | 字符串 | 用于构造对象末端RDN的属性名 |

每个配置项包含modifyOperations，comparedProperties 和modifiedProperties三个集合。

除了作为基类型，modifyOperations必须包含名为Add，Delete和PropertyModified的三种操作的配置，每个操作对应一个对象设置器。范例如下：

<add name="Add" opName="addADUserObjectSetter" />

其中opName属性对应一个对象设置器的配置名称

ComparedProperties集合的每一项对应对每个属性应用的比较器类型，范例如下：

<add name="LOGON\_NAME" targetPropertyName="samAccountName" enabled="true" opName="simplePropertyComparer" />

|  |  |  |
| --- | --- | --- |
| 属性 | 类型 | 说明 |
| name | 字符串 | 权限中心对象属性的名称 |
| targetPropertyName | 字符串 | 对象AD中对象属性的名称 |
| enabled | 布尔值 | 如果为true，表示此属性将用于比较，否则忽略此属性 |
| opName | 字符串 | 指定关联的属性比较器的配置名 |
| context | 字符串 | 属性比较器所需的上下文数据，对于枚举属性，为枚举的标帜名称 |

ModifiedProperties集合的每一项对应对每个属性应用的修改器的类型，范例如下：

<add name="DepartmentName" targetPropertyName="department" enabled="true" opName="simplePropertySetter" />

|  |  |  |
| --- | --- | --- |
| 属性 | 类型 | 说明 |
| name | 字符串 | 权限中心对象属性的名称 |
| targetPropertyName | 字符串 | 对象AD中对象属性的名称 |
| enabled | 布尔值 | 如果为true，表示此属性将用于修改，否则忽略此属性 |
| opName | 字符串 | 指定关联的属性修改器的配置名 |
| context | 字符串 | 属性修改器所需的上下文数据，对于枚举属性，为枚举的标帜名称 |

* 1. 开发说明
     1. 数据库说明：

AD同步使用MCS\_PERMISSION\_CENTER库，数据库详细说明请参考权限中心关于数据库的说明，参考地址：$/Seagull2Projects/03.数据库设计/19.权限中心

日志信息：



ID映射表：



* + 1. 时序说明：

正向同步整体时序如图：







* + 1. MCS.Library.SOA.Security.ADSyncUtilities程序集

**MCS.Library.SOA.Security.ADSyncUtilities命名空间**

**基本类**

ADObjectFinder：从AD中查找对应权限中心的对象

ADObjectModifier：用于执行添加修改操作

ADObjectWrapper：包装AD对象的属性，以便在脱离AD的情况下来访问。

ADObjectWrapperCollection：AD包装对象的集合。

ADToPermissionCenterSynchronizer：提供从AD同步部分属性回权限中心的功能

IDMapper：权限中心和AD对象的ID映射。如果AD对象ID为null时表示新建。

KeyedOguObjectCollection：根据键来访问的权限中心对象的集合

LogHelper：用于记录日志

ObjectSetterHelper：执行相应修改操作的帮助类

OguObjectFinder：从权限中心查找AD对象的子对象

PathPartEnumerator：将路径拆分为可枚举的字符串

PermissionCenterSynchronizer：提供从权限中心同步到AD的主要功能

PermissionCenterToADSynchronizeSettings：表示同步的配置节

SynchronizeHelper：同步帮助类

**对象比较器**

OguAndADObjectComparerBase：比较器的基类

UserObjectComparer：用户比较器

OrganizationObjectComparer：组织对象比较器

GroupObjectComparer：群组对象比较器

**对象修改器**

OguAndADObjectSetterBase:对象修改器的基类

AddADObjectSetter：添加一般对象的修改器

AddADGroupObjectSetter:添加群组的修改器

AddADUserObjectSetter：添加用户的修改器

DeleteADObjectSetter：删除一般AD对象的修改器

DeleteADOrganizationObjectSetter：删除组织的修改器

DeleteADUserObjectSetter：删除用户的修改器

ModifyADObjectPropertiesSetter：修改属性的修改器

**属性比较器**

OguAndADObjectPropertyComparerBase：属性比较器的基类

DNPropertyComparer：DN属性的比较器

LargeIntAndDateTimePropertyComparer：大整数和时间属性的比较器

NamePropertyComparer：名称属性的比较器

PhotoKeyComparer：照片属性的比较器

SimplePropertyComparer：简单属性（字符串）的比较器

StringCollectionPropertyComparer：字符串集合属性的比较器

UACPropertyComparer：UAC属性的比较器

**属性修改器**

OguAndADObjectPropertySetterBase：属性修改器的基类

SimplePropertySetter：简单属性的属性修改器

CodeNamePropertySetter：代码名称属性的修改器

LargeIntAndDateTimePropertySetter：整数和时间属性的修改器

ObjNamePropertySetter：修改对象名称属性的修改器

PhotoPropertySetter：照片属性的修改器

StringCollectionPropertySetter：字符串集合的属性修改器

UACPropertySetter：UAC（枚举）属性的修改器

UserCodeNamePropertySetter：用户的代码名称（登录名）属性的修改器

**MCS.Library.SOA.Security.ADSyncUtilities.Adapters命名空间**

ADReverseSynchronizeLogAdapter:AD反向同步的日志适配器，用于查询反向同步日志

ADReverseSynchronizeLogDetailAdapter：AD反向同步的日志详情适配器，用于查询反向同步日志详情

ADSynchronizeLogAdapter：AD同步日志适配器，用于查询正向同步日志

ADSynchronizeLogDetailAdapter：AD同步日志详情适配器，用于查询正向同步详情

SimpleUserAdapter：ID映射的适配器

SimpleUserAdapter：简单用户适配器，检索用于反向同步用的用户

**MCS.Library.SOA.Security.ADSyncUtilities.Entity命名空间**

IDMapping：表示ID映射，即AD对象和权限中心对象ID的关联

IDMappingCollection：ID映射的集合

ADIDMappingCollection:以字符串为键的ID映射的集合

SCIDMappingCollection：以权限中心ID为键的ID映射的集合

ADReverseSynchronizeLog：表示反向同步日志

ADReverseSynchronizeLogCollection：反向同步日志的集合

ADReverseSynchronizeLogDetail：表示反向同步详情

ADReverseSynchronizeLogDetailCollection：反向同步日志详情的集合

ADSynchronizeLog：表示AD同步日志

ADSynchronizeLogCollection：AD同步日志的集合

ADSynchronizeLogDetail：表示AD同步日志详情

ADSynchronizeLogDetailCollection：表示AD同步日志的详情

ADSynchronizeResult：取值表示同步的结果值

IDelayAction：定义延迟操作的接口

DelayActionCollection：延迟操作的集合

DelayRenameAction：表示延迟改名操作

DelayRenameCodeNameAction：延迟修改代码名称（已废）

EntityMappingCollection：用于反向同步，表示人员和代码名称的映射

ModifiedItem：修改的项目，包含应更新到AD中的权限中心对象和一个AD对象的包装

ModifiedItemgCollection：修改的项目的集合

SimpleUser：保存用户的简单属性，用于反向同步。

SynchronizeContext：保存同步上下文的状态。

1. 使用说明
   1. 权限中心AD同步的WebService

服务名称 为：/MCSWebApp/PermissionCenterServices/services/PermissionCenterToADService.asmx

AD同步的入口点为：StartSynchronize。含有2个参数：startPath表示同步的起始路径，如果未指定此参数，则使用缺省路径；taskID，如果通过计划任务启动，则将taskID通过此参数传入。

AD反向同步的入口点为：StartADReverseSynchronize。含有1个参数，taskID。如果通过计划任务启动服务，则将taskID通过此参数传入。

* 1. 通过程序发起同步

AD同步：初始化PermissionCenterSynchronizer的新实例，并调用实例的Start方法。

AD反向同步：调用ADToPermissionCenterSynchronizer的Start方法。

* 1. 通过权限中心手动发起

管理员进入权限中心管理功能，通过点击AD同步中的“立即同步”按钮来手动发起AD同步，或者点击AD反向同步中的“立即同步”按钮来发起反向同步。



* 1. 查看同步操作日志

转到权限中心“操作日志”，点击左边分类中的“活动目录同步”来查看AD同步日志，或者点击“活动目录反向同步”来查看AD反向同步日志。

1. 暂时，有部分数据仍来自AD。例如，联系人的Lync地址。 [↑](#footnote-ref-1)