

Управляем объектами в Active Directory

Часть 3

Иван Коробко

Прочитав статью, вы узнаете, что происходит в каталоге Active Directory в тот момент, когда изменяется значение какого-либо параметра объекта. Это поможет вам понять объектную модель Active Directory; принципы, заложенные при ее создании.

Существует два способа чтения/изменения свойств объектов в каталоге Active Directory: программным способом и с помощью мастера MMC-консоли. Первый способ (программное создание объектов) был описан в предыдущей статье (см. №6 за 2008 г.). О втором способе мы поговорим в этой статье: попробуем разобраться в том, как связаны поля в Active Directory с параметрами, отображаемыми в мастере MMC-консоли Active Directory Users and Computers.

В Active Directory чаще всего используются три типа объектов: учетная запись пользователя, учетная запись группы и контейнер. Причем большим количеством атрибутов по сравнению с другими объектами обладает учетная запись пользователя. Да и все операции, связанные с программным управлением, на 80% затрагивают учетную запись пользователя.

Для управления учетной записью пользователя необходимо не только знать поддерживаемые свойства и методы, но и его объектную модель,

т.е. названия параметров, соответствующие им поля в Active Directory и их типы данных.

Объектная модель учетной записи пользователя

В классическом понимании описание объектной модели представляет множество таблиц, в которых подробно рассказано о содержащихся в ней параметрах, соответствующих им типам данных и т. д. Отойдём от традиционного подхода и рассмотрим объектную модель с другого ракурса.

Давайте запустим мастер изменения учетной записи пользователя. Для этого запустим MMC-оснастку Active Directory Users and Computers и дважды кликнем левой кнопкой мыши по ранее созданной учетной записи пользователя. В результате выполнения манипуляций на экране появится диалоговое окно с множеством вкладок (см. **рис. 1**). Каждая из них содержит в среднем 2-3 группы параметров. Назначение каждой группы параметров приведено в **таблице 1**.

По умолчанию отображается вкладка General.

Существуют два режима работы MMC-оснастки Active Directory Users and Computers: обычный и расширенный режим. При включении расширенного режима в свойствах всех объектов появляются еще три вкладки: Published Certificates, Object, Security. На **рис. 1** приведены вкладки расширенного режима, в **таблице 1** соответственно – краткое описание всех вкладок.

Поскольку вкладок очень много и их доскональное описание выходит за рамки статьи, уделим внимание только часто используемым вкладкам: General, Account, Profile.

Вкладка General

Во вкладке General (см. **рис. 2**) задаются личные данные сотрудника и его контактная информация: телефоны, размещение, адрес электронной почты и др. Вкладка General отображается по умолчанию при вызове свойств учетной записи любого объекта из Active Directory: группы или поль-

зователя. В качестве значений параметров указаны названия соответствующих им полей в Active Directory. В **таблице 2** эта информация дополнена описанием соответствующих им типов данных.

Рассмотрим подробно каждый из задаваемых параметров.

Имя пользователя

Имя пользователя отображается около значка с человечком.

Во вкладке General его невозможно изменить. В Active Directory этому параметру соответствуют два параметра, значение которых совпадает: name и cn. В поле name, необходимое для совместимости с доменами Windows NT, дублируется значение параметра cn (canonical name).

Display Name

Значение параметра – отображаемое имя пользователя, которое видит администратор, войдя в Active Directory, оно также отображается в адресной книге почтового клиента, например Microsoft Outlook. Значение этого параметра фиксируется в параметре displayName в Active Directory.

Значение этого обязательного параметра складывается из суммы значений трех параметров: First Name, Initials и Last Name по шаблону: «a b. c», где a – имя пользователя, b – инициал (6 символов), c – фамилия. Один из этих трех параметров должен быть задан, однако по отдельности каждый из них является необязательным.

First Name

Необязательный параметр. Его значение – имя сотрудника, которому соответствует настоящая учетная запись. В Active Directory этому параметру соответствует поле givenName.

Initials

Необязательный параметр длиной не более 6 символов. Значению этого параметра соответствует инициал пользователя. Чаще всего этот параметр не заполняют.

Last name

Значение параметра – фамилия сотрудника, для которого создана учетная запись. В Active Directory ему соответствует параметр sn. Как прави-

Таблица 1. Назначение вкладок учетной записи пользователя

Вкладка	Описание	Расширенный режим
General	Основная вкладка, содержащая информацию, идентифицирующую личность человека, которой соответствует данная учетная запись	–
Address	Физический адрес местонахождения человека	–
Account	Характеристики учетной записи пользователя, настройка правил регистрации в сети	–
Profile	Настройка профиля учетной записи пользователя	–
Telephones	Настройка телефонии	–
Organization	Данные о сотруднике согласно штатному расписанию	–
Environment	Настройка сценария регистрации и правил поведения сетевых ресурсов в терминальной сессии	–
Sessions	Настройка правил функционирования терминальной сессии	–
Remote Control	Настройка удаленного доступа	–
Terminal Services Profile	Настройка профиля для терминального сервера	–
COM +	Выбор из списка объектов COM+	–
Published Certificates	Настройка списка сертификатов	+
Member Of	Управление членством в группах безопасности	–
Dial-In	Настройка регистрации учетной записи пользователя с помощью соединения Dial-Up	–
Object	Информация об объекте	+
Security	Права доступа к объекту	+

ло, из трех параметров задают только два: имя и фамилию.

Description

Это поле обычно заполняют каким-либо комментарием. Например, если имя и фамилия пользователя в домене задаются латинской транслитерацией, то это поле вполне подойдет для ФИО на русском языке. В Active Directory данные хранятся в одноименном поле.

Office

Указывается физическое месторасположение пользователя: комната, офис и т. д. Параметру Office в Active

Directory соответствует параметр physicalDeliveryOfficeName.

Telephone number

В этом поле обычно хранится номер телефона сотрудника. В Active Directory ему соответствует поле telephoneNumber.

Other

Если у сотрудника несколько телефонных номеров, то их можно занести в список, нажав кнопку Other, относящуюся к полю Telephone Number вкладки General. В появившемся диалоговом окне (см. **рис. 3**) с помощью мастера добавляют номера телефо-

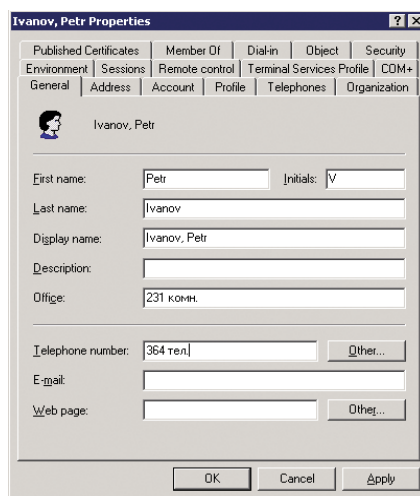


Рисунок 1. Свойства учетной записи пользователя

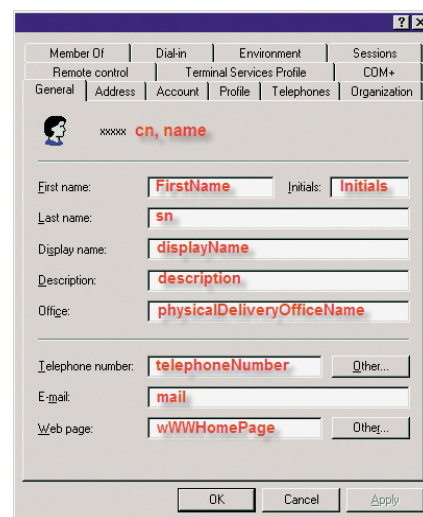



Рисунок 2. Вкладка General

Таблица 2. Соответствие параметров во вкладке General полям в Active Directory

Поле на вкладке General	Тип	Поле в Active Directory	Тип
	InputBox	cn name	String
First name	InputBox	givenName	String
Initials	InputBox	Initials	String
Last name	InputBox	sn	String
Display Name	InputBox	displayName	String
Description	InputBox	description	String
Office	InputBox	physicalDeliveryOfficeName	String
Telephone number	InputBox	telephoneNumber	String
Other	Button	otherTelephone	Array
E-mail	InputBox	mail	String
Web page	InputBox	wwwHomePage	String
Other	Button	url	Array

нов в список. В Active Directory списку соответствует массив otherTelephone, элементы которого – строки.

E-mail

Автоматически заполняемое поле (поле mail в Active Directory) в соответствии с форматом UPN (см. RFC 822) при создании почтового ящика для учетной записи пользователя. По умолчанию оно пустое.

Web page

В этом поле указывают ссылку на веб-страницу сотрудника. В Active Directory ему соответствует поле wwwHomePage.

Other

Если у сотрудника несколько ссылок на веб-сайты, то их можно занести в список, нажав кнопку Other, относящуюся к полю wwwHomePage вкладки General. В появившемся диалоговом окне (см. **рис. 4**) с помощью мастера добавляю ссылки на сайты.

Вкладка Account

Во вкладке Account сосредоточены настройки, характеризующие правила доступа пользователя к сети, включая имя входа в сеть. В **таблице 3** приведены описания полей вкладки Account и поля, соответствующие им в Active Directory.

User login name

Для совместимости с доменами pre-Windows 2000 (Windows NT) в Active Directory задается два имени пользователя, значения которых имеют разный формат. Первое имя, используемое в доменах Window 2k, – UPN-имя, которому в Active Directory соответствует поле userPrincipalName, имеющее формат user@domain, где domain – DNS-имя домена, например MSK.RU; user – имя пользователя в сети. Для удобства назначения имен UPN-имя разделено на две части (см. **рис. 5**).

Второе задаваемое имя пользова-

теля – SAM-имя, которое используется для совместимости в доменах Windows NT. Структура SAM-имени следующая: domain\user, где domain – сокращенное имя домена, например MSK, user – имя пользователя. Для удобства назначения имени поле также разбито на две части. В Active Directory хранится только имя пользователя в поле samAccountName. Первая часть SAM-имени однозначно вычисляется из DNS-имени домена.

User must change password at next logon

Этот параметр и дата окончания действия учетной записи – единственные два параметра, которые заданы в явном виде во вкладке Account. Остальные значения заданы одним параметром, которые в зависимости от выбранных опций изменяют значение (см. **таблица 4**).

Параметр User must change password at next logon по умолчанию включен. В Active Directory ему соответствует параметр pwdLastSet, который равен 0 или 0x7FFFFFFFFFFFFFFF (9223372036854775807), если галка стоит, то в качестве значения указывается время с точностью 100 наносекунд, прошедшее с 1 января 1601 года.

Account expires

За состояние переключения параметров в группе Account expires отвечает параметр userAccountControl = 8388608, возможные значения которого будут рассмотрены в разделе Account options. При установленном значении userAccountControl необходимо установить дату выключения пользователя. По умолчанию назначается значение равное месяцу, которое фиксируется в Active Directory в поле AccountExpires. Так же, как и значение параметра pwdLastSet, значением является период времени с точностью 100 наносекунд, прошедшее с 1 января 1601 года.

Account options

Все параметры данной группы, за исключением первого (см. **рис. 5**), составляют значение параметра userAccountControl, которое образуется путем суммирования всех установленных значений. Однако в **таблице 3** приведены только те значения, которые можно изменить явным образом с помощью вкладки Account. В **таблице 5** приведены значения параметра userAccountControl, не вошедшие в **таблицу 3**.

В **таблице 5** красным шрифтом выделены параметры, которые можно задать явным способом во вкладке Account.

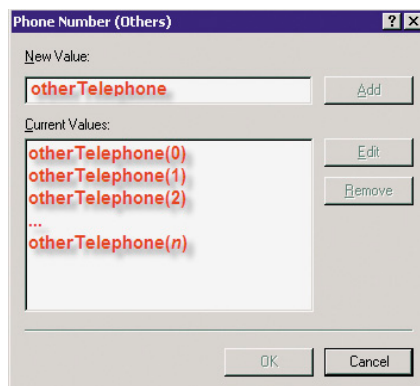


Рисунок 3. Создание списка телефонов

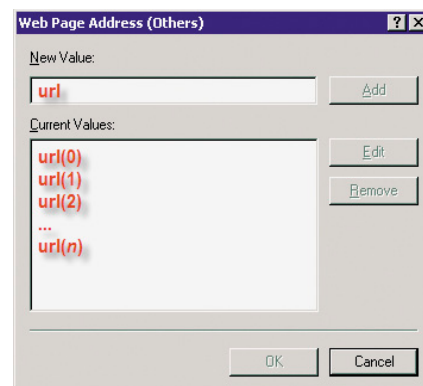


Рисунок 4. Создание списка веб-сайтов

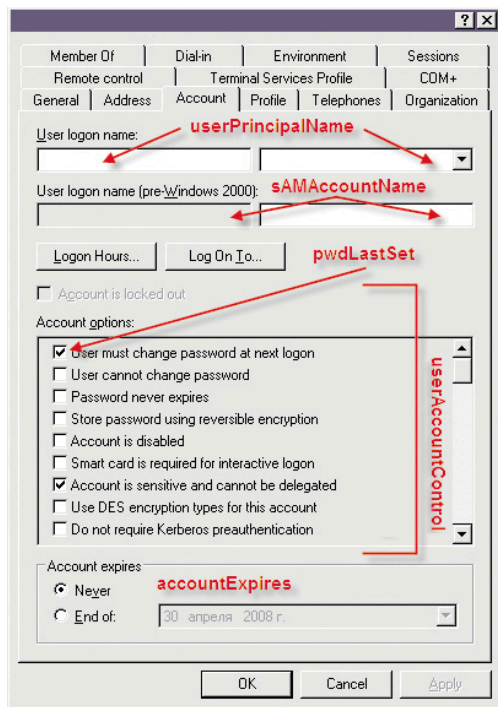


Рисунок 5. Вкладка Account

В **листинге** приведен шаблон сценария, с помощью которого можно определить установки параметра userAccountControl.

Листинг. Определение опций, установленных параметров userAccountControl

```
Set objHash = CreateObject("Scripting.Dictionary")

objHash.Add "SCRIPT", 1
objHash.Add "ACCOUNTDISABLED", 2
objHash.Add "UNKNOWN", 4
objHash.Add "HOMEDIR_REQUIRED", 8
objHash.Add "LOCKOUT", 16
objHash.Add "PASSWD_NOTREQD", 32
objHash.Add "PASSWD_CANT_CHANGE", 64
objHash.Add "ENCRYPTED_TEXT_PWD_ALLOWED", 128
objHash.Add "TEMP_DUPLICATE_ACCOUNT", 256
objHash.Add "NORMAL_ACCOUNT", 512
objHash.Add "UNKNOWN", 1024
objHash.Add "INTERDOMAIN_TRUST_ACCOUNT", 2048
objHash.Add "WORKSTATION_TRUST_ACCOUNT", 4096
objHash.Add "SERVER_TRUST_ACCOUNT", 8192
objHash.Add "UNKNOWN", 16384
objHash.Add "UNKNOWN", 32768
objHash.Add "DON'T_EXPIRE_PASSWORD", 65536
objHash.Add "MNS_LOGON_ACCOUNT", 131072
objHash.Add "SMARTCARD_REQUIRED", 262144
objHash.Add "TRUSTED_FOR_DELEGATION", 524288
objHash.Add "NOT_DELEGATED", 1048576
objHash.Add "USER_DES_KEY_ONLY", 2097152
objHash.Add "DON'T_REQ_PREAUTH", 4194304
objHash.Add "PASSWORD_EXPIRED", 8388608
objHash.Add "TRUSTED_TO_AUTH_FOR_DELEGATION", 16777216

Set objUser = GetObject("LDAP://" & Path)
intUAC = objUser.Get("userAccountControl")
t = " "
For Each Key In objHash.Keys
    If objHash(Key) And intUAC Then
        t = t & Key & vbTab & "ВЫКЛ" & vbNewLine
    Else
        t = t & Key & vbTab & "ВКЛ" & vbNewLine
    End If
Next
Wscript.Echo t
```

Шаблон работает по следующему сценарию: сначала создается словарь сопоставлений псевдонимов с помо-

Таблица 3. Соответствие параметров во вкладке Account полям в Active Directory

Поле на вкладке Account	Тип	Поле в Active Directory	Тип
User logon name	InputBox ListBox	userPrincipalName	String
User logon name (pre-Windows 2000)	InputBox (Read) InputBox	sAMAccountName	String
Logon Hours	Button	logonHours	Binary
Log On To	Button	userWorkstations	Array
Account is locked out	CheckBox	userAccountControl = 16	String
User must change password at next logon	CheckBox	pwdLastSet	String
User cannot change password	CheckBox	userAccountControl = 64	String
Password never expires	CheckBox	userAccountControl = 65536	String
Store password using reversible encryption	CheckBox	userAccountControl = 128	String
Account is disabled	CheckBox	userAccountControl = 2	String
Smart card is required for interactive logon	CheckBox	userAccountControl = 262144	String
Account is sensitive and cannot be delegated	CheckBox	userAccountControl = 1048576	String
Use DES encryption types for this account	CheckBox	userAccountControl = 2097152	String
Do not require Kerberos preauthentication	CheckBox	userAccountControl = 4194304	String
Account expires	Radio ListBox	userAccountControl = 8388608 AccountExpires	String String

щью объекта Scripting.Dictionary. Затем с помощью функции GetObject() осуществляется подключение к пространству имен учетной записи пользователя и чтение значения параметра userAccountControl. Далее осуществляется расшифровка полученных данных и подстановка соответствующих текстовых значений в соответствии с созданным словарем (см. **рис. 6**).

Вкладка Profile

Во вкладке Address (см. **рис. 7**) сосредоточены параметры, касающиеся местоположения человека, которому соответствует учетная запись пользователя: его почтовый адрес, включая регион, индекс, город, код города. Все перечисленные параметры необязательны, в мастере создания учетной записи они недоступны. В **таблице 4** приведены соответствия описанных параметров полям в Active Directory.

Полю Profile Path соответствует строковый параметр profilePath в Active Directory. В качестве значения указывают путь к перемещаемому профилю в виде UCN-пути: \\Server\ShareName\UserNameFolder. Необходимо отметить, что папка ShareName – имя опубликованной папки в сети на сервере Server.

В качестве значения UserNameFolder, как правило, используют переменную %username% (см. **таблицу 4**), которая автоматически расшифровывается в сокращенное имя пользователя в сети. В Active Directory значению перемен-

Таблица 4. Соответствие параметров во вкладке Profile полям в Active Directory

Поле на вкладке Profile	Тип	Поле в Active Directory	Тип
Profile Path	InputBox	profilePath	String
Logon Script	InputBox	scriptPath	String
Local Path	InputBox	HomeDirectory	String
Connect	CheckBox InputBox	HomeDriver HomeDirectory	String String

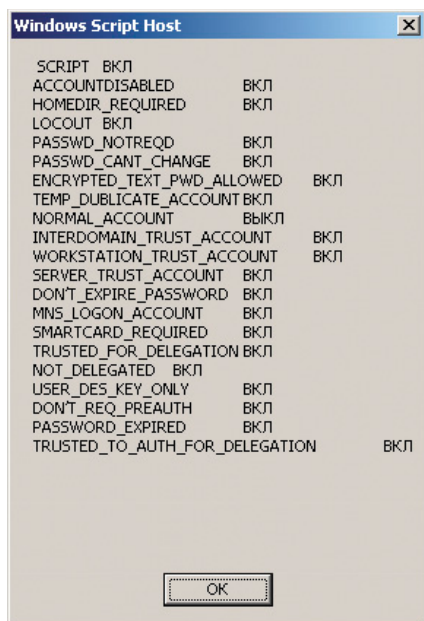


Рисунок 6. Расшифровка параметров userAccountControl

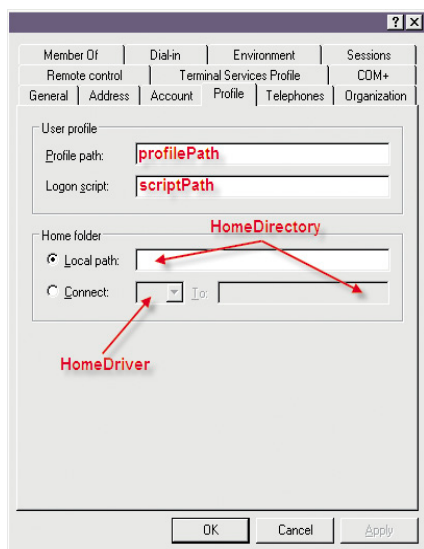


Рисунок 7. Вкладка Profile

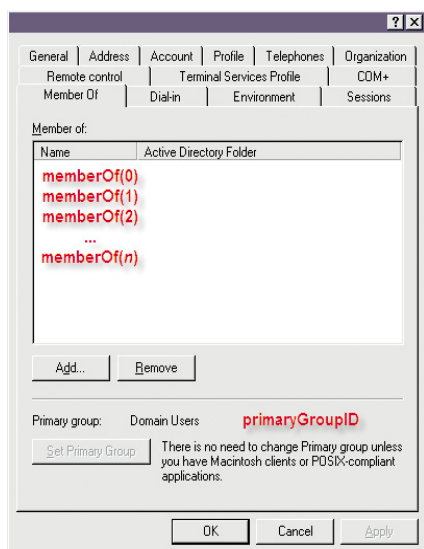


Рисунок 8. Вкладка MemberOf

Таблица 5. Флаговые значения параметра userAccountControl

Флаг	Значение	Описание
SCRIPT	1	Запуск сценария входа
ACCOUNTDISABLED	2	Отключение учетной записи пользователя
UNKNOWN	4	—
HOMEDIR_REQUIRED	8	Требуется домашняя папка
LOGOUT	16	Учетная запись пользователя заблокирована
PASSWD_NOTREQD	32	Пароль не требуется
PASSWD_CANT_CHANGE	64	Пользователь не может изменить пароль самостоятельно
ENCRYPTED_TEXT_PWD_ALLOWED	128	Пользователь может отправить зашифрованный пароль
TEMP_DUPLICATE_ACCOUNT	256	Учетная запись для пользователя, чьи основные данные хранятся в другом домене
NORMAL_ACCOUNT	512	Тип учетной записи, используемой по умолчанию, соответствующей обычному пользователю
UNKNOWN	1024	—
INTERDOMAIN_TRUST_ACCOUNT	2048	Разрешение доверять учетную запись домена другому домену
WORKSTATION_TRUST_ACCOUNT	4068	Учетная запись для компьютера с ядром Windows 2k
SERVER_TRUST_ACCOUNT	8192	Учетная запись для контроллера домена, являющегося членом домена
UNKNOWN	16384	—
UNKNOWN	32768	—
DON'T_EXPIRE_PASSWORD	65536	Срок действия установленного пароля не истекает
MNS_LOGON_ACCOUNT	131072	Учетная запись входа MSN
SMARTCARD_REQUIRED	262144	Для регистрации в сети требуется смарт-карта
TRUSTED_FOR_DELEGATION	524288	Учетная запись пользователя или компьютера, из-под имени которой выполняется служба, которой доверяется делегирование Kerberos
NOT_DELEGATED	1048576	Делегирование каких-либо полномочий службе Kerberos отключено
USER_DES_KEY_ONLY	2097152	Для шифрования ключей используется DES-шифрование
DON'T_REQ_PREAUTH	4194304	Для входа в сеть не требуется предварительная проверка Kerberos
PASSWORD_EXPIRED	8388608	Срок действия пароля истек
TRUSTED_TO_AUTH_FOR_DELEGATION	16777216	Учетной записи разрешено безопасное делегирование. Данный параметр разрешает службе использовать учетные данные и проходить проверку подлинности от имени пользователя для других удаленных серверов сети

ной %username% соответствует параметру samAccountName.

Logon Script

В Active Directory полю Logon Script соответствует значение строкового параметра scriptPath.

Сценарий входа, или как его еще называют сценарий регистрации пользователей в сети, можно присвоить по профилю или с помощью групповых политик (Group Policy). Windows 2k всегда ищет сценарий на контроллере домена в папке %SystemRoot%\SYSVOL\systvol\DomainName\Scripts, где DomainName – DNS-имя домена, например msk.ru. В сети доступ в этой папке осуществляется через UNC-путь \\DomainName\Netlogon. В качестве сценария может быть использован файл с расширением BAT (сценарий на

базе командной строки), VBS (Microsoft Visual Basic Script) или JS (Microsoft Java Script). При создании сценариев могут быть использованы различные переменные среды (см. таблицу 6).

Home Folder

Домашний каталог может быть задан двумя способами:

- как локальный путь, например, C:\Storage\Profiles\APetrov;
- как сетевой диск, который будет монтироваться каждому сотруднику после регистрации в сети.

Local Path

Если домашний каталог должен храниться локально на рабочей станции, то необходимо указать локальный путь, которому в Active Directory соответствует поле HomeDirectory, при этом значе-

ние поля HomeDriver="". Формат пути: C:\FolderName. После регистрации пользователя в сети указанная папка будет создана локально на компьютере пользователя.

Connect

Для того чтобы пользователю после регистрации компьютера в сети монтировалась папка с домашним каталогом на сетевой диск с указанным именем, необходимо перейти в режим Connect. В отличие от предыдущего режима необходимо указать два параметра – имя диска и списка, которому в Active Directory соответствует текстовое поле HomeDriver и UNC-путь к подключаемой папке. Этому пути соответствует строковый параметр HomeDirectory. После того как задан UNC-путь, осуществляется его проверка как на соответствие формата (\\Server\ShareName\FolderName), так и на существовании папки, к которой предоставлен сетевой доступ.

Вкладка MemberOf

Во вкладке MemberOf (см. **рис. 8**) формируется список групп, членом которых является текущий пользователь; назначить Primary Group (основная группа).

MemberOf

Для управления членством пользователя в группах безопасности Active Directory используются две кнопки, находящиеся под списком групп, членами которой является пользователь: Add (Добавить) и Remove (Удалить). По умолчанию пользователь входит в группу Domain Users. Эта группа не отображается в списке.

Механизм управления следующий. Для добавления пользователя в какую-либо группу необходимо нажать кнопку Add... В появившемся диалоговом окне (см. **рис. 9**), осуществляется поиск объектов по заданным критериям. В поле Enter the object names to select указывается одно из имен пользователя (cn или samAccountName), при этом в списке фиксируется значение поля distinguishedName, в то время как отображается cn этого объекта.

Primary Group

Единственная группа, членом которой является пользователь после создания его учетной записи, – Domain Users.

Таблица 6. Переменные, используемые в сценариях регистрации пользователей в сети

Переменная	Описание
%homedrive%	Буква, на которую будет монтироваться сетевой диск, содержащий домашний каталог пользователя
%homepath%	Полный путь к домашней папке пользователя
%os%	Версия операционной системы рабочей станции, на которой выполняется сценарий загрузки
%processor_architecture%	Тип процессора рабочей станции, на которой выполняется сценарий
%processor_level%	Уровень процессора рабочей станции, на которой выполняется сценарий
%userdomain%	Сокращенное имя домена, в пространстве которого выполняется сценарий
%username%	Сокращенное имя пользователя (поле samAccountName в Active Directory)

Таблица 7. Соответствия параметров во вкладке MemberOf полям в Active Directory

Поле на вкладке MemberOf	Тип	Поле в Active Directory	Тип
Member of	ListBox, Button	MemberOf	Array
PrimaryGroup	Button	primaryGroupID	String

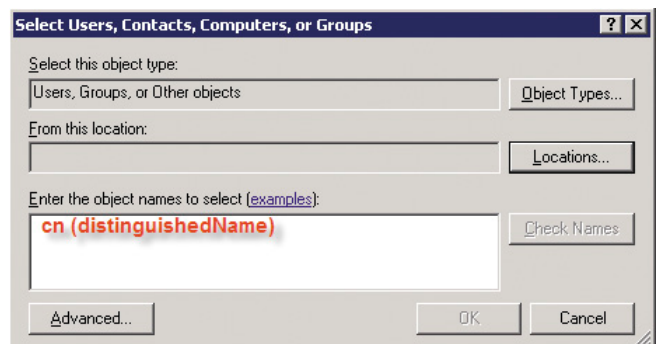


Рисунок 9. Поиск объектов в Active Directory по заданному критерию

Значение параметра – идентификационный номер группы. По умолчанию назначена группа Domain Users, имеющая идентификатор 513.

Рассмотрим пример. Пусть пользователь Test_User входит в группу Test_Group. SID группы – S-1-5-21-42226584364-21557989-1436132917-12213. Необходимо определить значение параметра PrimaryGroupID, если primary group – группа Test_Group.

Последний раздел SID является идентификатором основной группы, поэтому параметр PrimaryGroupID = 12213 (см. **рис. 10**).

Заключение

В этой статье вы получили представление об основных параметрах учетной записи пользователя. В следующей статье поговорим подробнее о программном управлении членством пользователей (вкладка Member Of), затем рассмотрим объектные модели контейнера и учетной записи группы.

Удачи!

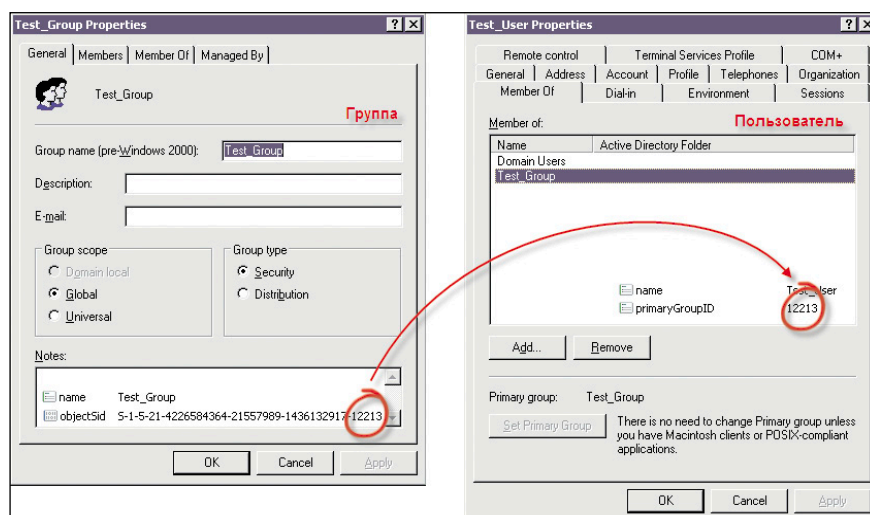


Рисунок 10. Определение значения параметра primaryGroupID