**Средства командной строки для управления Active Directory**

Чтобы использовать многочисленные средства командной строки, управляющие Active Directory, нужны базовые знания об Active Directory и ее структурах, В соответствии с замыслом Microsoft эта служба использует в качестве системы именования DNS (Domain Name System). В DNS информация о сетевых ресурсах хранится в виде иерархической структуры, соответствующей схеме управления ресурсами. Эта иерархия доменов, или дерево доменов, лежит в основе среды Active Directory и во многом аналогична структуре каталогов файловой системы. Еще одно название этой иерархии — пространство имен (namespace). В каждой организации, использующей домены Active Directory, существует своя иерархия (или пространство имен) Active Directory.

**Гибкость управления Active Directory из командной строки**

Освоив базовые структуры Active Directory и научившись идентифицировать используемые объекты по DN (Domain Name), вы готовы управлять Active Directory из командной строки. Применение командной строки дает важное преимущество — дополнительную гибкость. Из командной строки легко выполняются многие операции, осуществить которые GUI-средствами гораздо сложнее или просто невозможно. Например, вы можете найти все учетные записи компьютеров, неактивные более недели, и отключить эти записи. Или одной командой изменить свойства нескольких учетных записей пользователей.

Для работы с Windows-доменами Windows Server 2003 и Windows ХР предоставляют набор средств командной строки, управляющих Active Directory. К ним относятся:

DSADD — добавляет объекты в Active Directory;

DSGET — показывает свойства объектов, зарегистрированных в Active Directory;

DSMOD.— изменяет свойства объектов, существующих в Active Directory;

DSMOVE — перемещает один объект в новое место в том же домене или переименовывает объект, не перемещая его;

DSQUERY — ищет объекты Active Directory по определенному критерию;

DSRM — удаляет объекты из Active Directory.

Каждая из утилит командной строки предназначена для работы с определенным набором объектов Active Directory (AD).

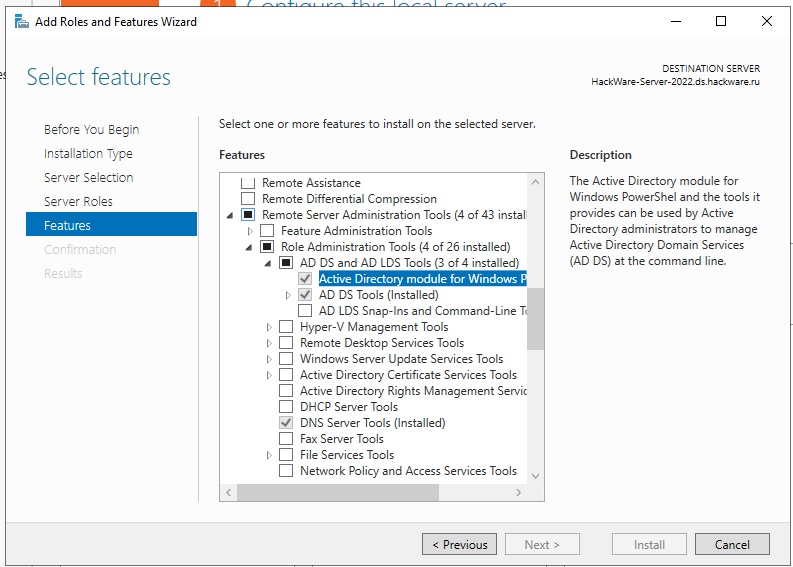
Модуль Active Directory для Windows PowerShell — один из основных инструментов для администрирования домена, управления объектами в Active Directory и получения различной информации о компьютерах AD, пользователях, группах и т. д. Любой администратор Windows должен знать, как использовать как графическую оснастку AD (обычно это ADUC — Active Directory Users & Computers) и командлеты модуля RSAT-AD-PowerShell для выполнения повседневных задач администрирования Active Directory. Мы рассмотрим, как установить модуль PowerShell Active Directory в Windows, познакомимся с его основными функциями и популярными командлетами, которые полезны для управления и взаимодействия с AD.

**Установка модуля Powershell Active Directory на Windows Server**

Active Directory для Windows PowerShell уже встроен в операционные системы Windows Server (начиная с Windows Server 2008 R2), но по умолчанию не включен.

В Windows Server 2016, 2019 и 2022 вы можете установить модуль AD для PowerShell из Диспетчера серверов (Добавить роли и компоненты → Функции → Инструменты удалённого администрирования сервера → Инструменты администрирования ролей → Инструменты AD DS и AD LDS → Модуль Active Directory для Windows PowerShell).

В англоязычной версии сервера это соответственно в Server Manager: Add Roles and Features → Features → Remote Server Administration Tools → Role Administration Tools → AD DS and AD LDS Tools → Active Directory module for Windows PowerShell.



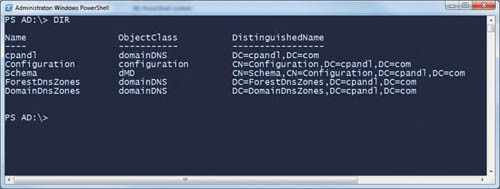
После этого вы должны увидеть ярлык Active Directory Module for Windows PowerShell в разделе Administrative Tools меню Start. Щелкните этот ярлык, чтобы запустить PowerShell с загруженным модулем AD. Если вы уже работаете в PowerShell и хотите просто загрузить модуль, чтобы он стал доступным для использования, можно ввести следующую команду и получить доступ к командам AD и AD Provider:

**-** Import-Module ActiveDirectory

В PowerShell реализована концепция дисков PowerShell, которые я буду называть просто дисками PS. Упрощенно можно назвать диск PS представлением ресурса, такого как пригодная для навигации файловая система, состоящая из папок и конечных элементов. Не каждый ресурс можно представить таким образом, но многие (в том числе AD и реестр) хорошо вписываются в эту модель. Модуль AD содержит провайдера для диска PS AD. Соответственно, можно перемещаться и даже изменять AD, как будто это файловая система.

Как же перемещаться по AD, используя AD Provider? Предполагается, что PowerShell открыт и модуль AD загружен. В этом случае первый шаг — запустить команду Set-Location, которая имеет несколько псевдонимов, в том числе sl и cd:

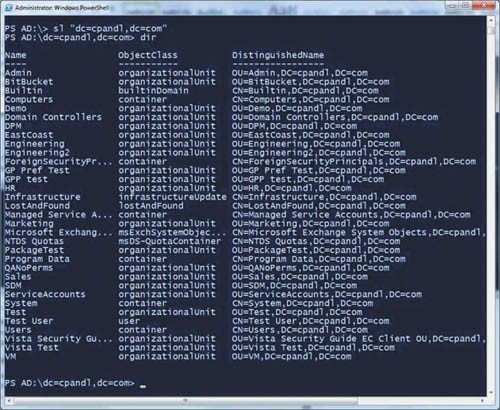
Эта команда изменяет текущее рабочее положение диска PS AD. В результате приглашение PowerShell покажет AD:\ вместо C:\. Затем, чтобы увидеть элементы в диске PS AD, можно применить команду Get-ChildItem с псевдонимом dir:



Как мы видим, команда возвращает список всех доступных разделов домена. Самый интересный, на мой взгляд, — раздел домена с именем cpandl, который содержит имена пользователей и компьютеров. Чтобы изменить этот домен, достаточно ввести команду:

- Set-Location «dc=cpandl,dc=com»

Обратите внимание, что используется команда Set-Location с различающимся именем (DN) моего домена AD. Это требуется для корректной навигации. После перехода в каталог домена (на что указывает приглашение AD:\dc=cpandl,dc=com в PowerShell), можно использовать команду Get-ChildItem, чтобы увидеть структуру AD верхнего уровня (экран 3).



Командная строка PowerShell будет иметь вид AD:\ou=SDM,dc=cpandl,dc=com. На данном этапе можно использовать команду Get-ChildItem, чтобы увидеть все объекты пользователя в этом OU. Если нужно изменить свойство Description на объекте пользователя, представляющем мою учетную запись пользователя Darren Mar-Elia. Для этого есть команда! Команда Set-ItemProperty позволяет изменить свойство в объекте AD. Если нужно изменить описание учетной записи пользователя на Chief Techie, следует выполнить команду:

Set-ItemProperty -Path '.\CN=Darren Mar-Elia' `

-Name «Description» -Value «Chief Techie»

Как мы видим, здесь используется параметр –Path для указания моей учетной записи пользователя в текущем каталоге. Я также использую параметр -Name, дабы указать, что нужно изменить свойство Description, и параметр –Value, для указания описания Chief Techie.

Как видите, работать с AD таким образом довольно просто. Механизм вряд ли подходит для массовых изменений, однако он удобен для работы с AD как с файловой системой. При этом, как я выяснил, большинство администраторов использует команды вместо диска PS AD для управления AD. Посмотрим, как действуют некоторые из этих команд.

Добавление учетных записей пользователя

Команда New-ADUser обеспечивает простой способ добавлять учетные записи пользователя в AD. Если нужно добавить новую учетную запись пользователя с именем Bill Smith в организационную единицу SDM, то в самом простом случае можно создать учетную запись нового пользователя с помощью команды:

New-ADUser -Name «Bill Smith» -SamAccountName «bsmith» `

-GivenName «Bill» -Surname «Smith» `

-DisplayName «Bill Smith» -Path «OU=SDM,DC=cpandl,DC=com»

В этой команде вводится основная информация об учетной записи пользователя. В частности, параметр -SamAccountName служит для предоставления имени учетной записи SAM, необходимой для создания объекта пользователя. Также применяется параметр –Path, чтобы сообщить команде место, куда следует поместить объект — в данном случае в организационную единицу SDM в домене cpandl.com. Кроме того, указано имя пользователя (параметр -GivenName), фамилия (параметр -Surname) и отображаемое имя (параметр -DisplayName).

Выполнение этой команды приведет к созданию учетной записи пользователя, но есть две проблемы. Во-первых, учетная запись будет отключена. Во-вторых, с учетной записью не будет связан пароль, что требуется в большинстве доменов.

Чтобы избежать необходимости активировать учетную запись и назначать пароль отдельно, можно изменить команду New-ADUser. New-ADUser автоматически активирует учетную запись, если указать параметр -Enabled $true в команде. Для активирования требуется пароль, поэтому необходимо также указать его в команде.

Чтобы предоставить пароль, можно использовать параметр –AccountPassword. Однако нельзя ввести пароль простым текстом в командной строке. Этот параметр требует, чтобы пароль был введен в защищенной строке (то есть имел тип данных SecureString). Существует два способа преобразовать пароль в защищенную строку, и в обоих случаях используется переменная.

В первом методе применяется команда ConvertTo-SecureString, которая преобразует строки простого текста в защищенные строки. Например, если нужно преобразовать пароль P@ssw0rd12 в защищенную строку и назначить его переменной $pwd, следует выполнить команду:

$pwd = ConvertTo-SecureString -string «P@ssw0rd12» `

-AsPlainText –force

Это не самый безопасный метод назначения пароля, так как кто-то может заглянуть вам через плечо при вводе команды. Более надежный способ, если команда New-ADUser запросит пароль и будет скрывать вводимые символы. Это можно сделать с помощью команды Read-Hostcmdlet с параметром –AsSecureString:

$pwd = Read-Host -AsSecureString

После выполнения этой команды вы увидите на экране знакомый символ «\*" при вводе пароля. Завершив ввод, нажмите клавишу Enter.

После того, как пароль сохранен в переменной $pwd, можно передать его в команду New-ADUser:

New-ADUser -Name»Bill Smith«-SamAccountName»bsmith«`

-GivenName»Bill«-Surname»Smith«`

-DisplayName»Bill Smith«`

-Path»OU=SDM,DC=cpandl,DC=com«`

-Enabled $true -AccountPassword $pwd

**Командлеты Active Directory PowerShell**

В модуле Active Directory для Windows PowerShell есть множество командлетов для взаимодействия с AD. Каждая новая версия RSAT содержит больше командлетов, чем предыдущая. В Windows Server 2022 доступно 147 командлетов PowerShell для Active Directory.

Перед использованием командлетов модуля Active Directory вам необходимо импортировать его в сеанс PowerShell:

Import-Module ActiveDirectory

Начиная с Windows Server 2012 R2, Windows 8.1 и в последующих версиях модуль импортируется автоматически.

Вы можете отобразить полный список доступных командлетов Active Directory с помощью команды:

Get-Command -module ActiveDirectory

Чтобы посчитать общее количество командлетов в модуле AD выполните команду:

Get-Command -module ActiveDirectory | measure-object | select count

Большинство командлетов RSAT-AD-PowerShell начинаются с префиксов Get-, Set- или New-.

Командлеты Get- класса используются для получения различной информации из Active Directory

Командлеты класса Set- используются для установки (изменения) параметров объекта в Active Directory

Команды, начинающиеся с New- позволяют создавать объекты AD

Командлеты Remove- используются для удаления объектов AD.

Так вы можете получить помощь по любому командлету:

1) Get-Help КОМАНДЛЕТ

2) Get-Help КОМАНДЛЕТ -Full