Министерство образования и науки Российской Федерации

Санкт-Петербургский политехнический университет Петра Великого

—

Институт прикладной математики и механики

**Кафедра «Информационная безопасность компьютерных систем»**

**ЛАБОРАТОРНАЯ РАБОТА №2**

**«Установка и настройка службы каталога Active Directory»**

по дисциплине «Безопасность современных информационных технологий»

Выполнил

студент гр. 33609/3 Югай П.Э.

<*подпись*>

Руководитель Иванов Д.В.

<*подпись*>

Санкт-Петербург

2018

**Цель работы:**

Изучить способы и механизмы установки и настройки службы каталога Active Directory.

**Задачи:**

1. Придумать и описать структуру некоторой компании (без привязки к компьютерному обеспечению).
2. Разработать логическую структуру Active Directory, удовлетворяющую структуре компании.
3. Выполнить установку и настройку Active Directory в соответствии с разработанной структурой.
4. Создать следующие административные группы пользователей в Active Directory: Account Managers, Help Desk, Resource Admins, Genereal Admins.
5. Настроить полномочия для созданных групп пользователей:

Account Managers могут только создавать учетные записи для новых сотрудников и удалять их при необходимости.

Help desk могут только разблокировать пользовательские учетные записи в случае их блокировки при неудачном вводе пароля.

Resource Admins должны управлять доступом к информационным ресурсам организации.

General Admins должны обладать полным доступом и контролировать работу администраторов нижних уровней.

1. Создать тестовых пользователей в каждой из групп.
2. Выполнить проверку правильности настройки полномочий путем попыток исполнения соответствующих действий от имен пользователей различных групп.
3. Создать файловый сервер. На файловом сервере должны быть папки для каждого компьютера и каждого пользователя в организации. При входе пользователя на некоторый компьютер, ему должны монтироваться два разделяемых ресурса, соответствующие папке компьютера и папке пользователя на файловом сервере.

Создать инструментарий, помогающий в работе администраторам: скрипт для поиска пользователей, у которых скоро истекает срок действия пароля, и скрипт для разблокирования всех учетных записей пользователей в заданном организационном подразделении.

**Требования:**

* У каждого студента должна быть своя структура организации, повторов быть не может.
* Создание групп пользователей, настройка их полномочий, создание тестовых пользователей и другие настройки должны выполняться автоматизированно с помощью скриптов.
* Логическая структуру Active Directory должна включать в себя, как мимнимум, домены и организационные подразделения (минимум два).
* Демонстрационный стенд должен состоять минимум из трех компьютеров (возможно использование виртуальных машин).
* В состав стенда должны входить сервера на базе Windows 2008 или выше и рабочие станции на базе Windows 7 или выше.
* Количество дней до истечения срока действия пароля для скрипта поиска пользователей, должно являться входным параметром скрипта.

Название организационного подразделения для скрипта разблокирования учетных записей пользователей должно являться входным параметром скрипта.

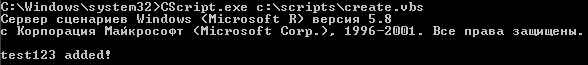
**Ход работы:**

Создана логическая структура Active Directory вымышленной компании myforest, имеющий домен corp.myforest.com с собственным DNS, DHCP и файловым серверами. Компания имеет 4 подразделения: forest1, forest2, forest3, forest4, имеющие группы: Account Managers, General Admins, Help Desk, Resource Admins соответственно каждому подразделению.

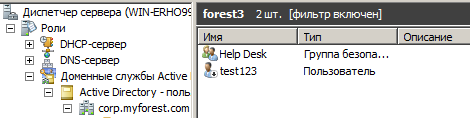
Для упрощенного управления над созданной структурой Active Directory были созданы скрипты, написанные на языке программирования Visual Basic, которые создают пользователей, удаляют их, разблокировывают их, так как при создании по умолчанию пользователи находятся в заблокированном режиме, осуществляют поиск пользователей, у которых скоро истекает срок действия пароля. Данные скрипты имеют расширения vbs.

**Результаты лабораторной работы:**

Для тестирования установленного сервера Active Directory с помощью разработанного скрипта (приложение 1) был создан пользователь test123, включенный в группу Help Desk, находящееся в подразделении forest3.

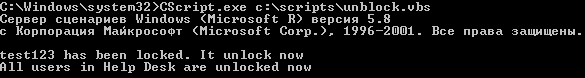


Изображение 1 – Запуск скрипта создания пользователей

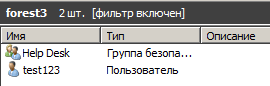


Изображение 2 – Подразделение forest3

После этого пользователь test123 был разблокирован через скрипт (приложение 3).

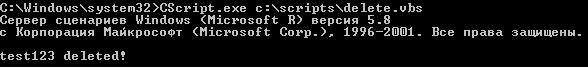


Изображение 3 – Разблокировка пользователя

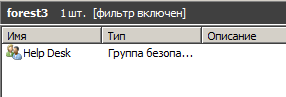


Изображение 4 – Разблокированный пользователь в Active Directory

Далее был протестирован скрипт удаления пользователей (приложение 2) из домена Active Directory. Был удален пользователь test123. Результаты представлены ниже на скриншотах.

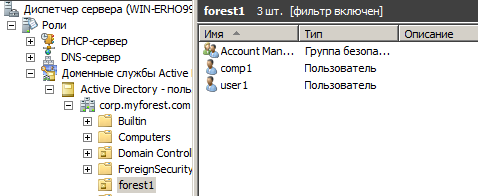


Изображение 5 – Удаление пользователя



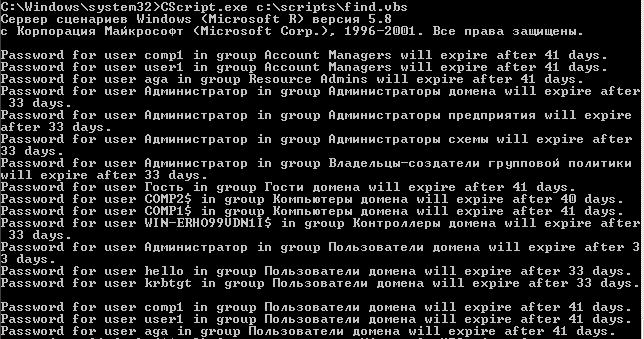
Изображение 6 – Подразделение forest3 без пользователя test123

Для дальнейшего тестирования были созданы два пользователя comp1 и user1 в подразделении forest1 в группе Account Managers. Через учетную запись comp1 пользователь должен присоединять свой компьютер к домену corp.myforest.com, а через user1 он может зайти в данный домен сервера в качестве пользователя. После их создания они были разблокированы с помощью разработанного скрипта.



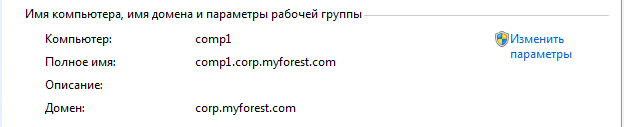
Изображение 7 – Пользователи user1 и comp1

С помощью скрипта (приложение 4) был выведен список пользователей и их групп, в которых они состоят, у которых истекает срок действия их пароля менее, чем через 100 дней.

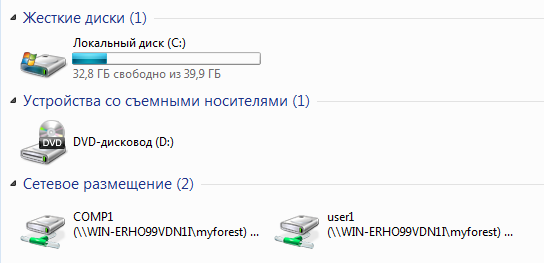


Изображение 8 – Список пользователей, у которых истекает срок действия пароля менее, чем через 100 дней

Чтобы убедиться в том, что к данному домену можно подключиться с другого компьютера, была установлена виртуальная машина с операционной системой Windows 7 Ultimate Edition. С помощью настроек свойств компьютера и изменения настроек сетевого адаптера, а именно указание в качестве адреса DNS сервера адрес нашего сервера (192.168.1.13), было произведено соединение с доменом corp.myforest.com под учетной записью comp1. В качестве пользователя использовалась учетная запись user1. После входа пользователя в домен corp.myforest.com ему монтируются два сетевых диска, которые соответствуют учетной записи компьютера и пользователя, от имени которого был осуществлен вход в этот домен.



Изображение 9 – Учетная запись компьютера пользователя



Изображение 10 – Сетевые диски компьютера и пользователя

**Вывод:**

В ходе выполнения данной лабораторной работы были изучены способы и механизмы установки и настройки службы каталога Active Directory. Была создана логическая структура вымышленной компании myforest, имеющая домен corp.myforest.com, которая была разбита на подразделении, каждая из которых имеет определенную собственную группу пользователей. Для упрощенного управления разработанной логической структурой были созданы скрипты, написанные на языке программирования Visual Basic.

**Приложения:**

Приложение 1. Скрипт создания пользователей (create.vbs).

Uname = CStr(InputBox("Enter name:","",""))

Password = CStr(InputBox("Enter password:","",""))

Subunit = CStr(InputBox("Enter subunit:","",""))

Gname = CStr(InputBox("Enter group's name:","",""))

strpath = "work.bat"

Set Domain = GetObject("LDAP://" & "ou=" &Subunit & ",dc=corp,dc=myforest,dc=com")

Set User = Domain.Create("User", "cn=" & Uname)

User.Put "sAMAccountName", Uname

User.Put "scriptPath", strpath

User.SetInfo

User.SetPassword Password

User.SetInfo

Set Group = GetObject("LDAP://" & "cn= " & Gname & ",ou=" & Subunit & ",dc=corp,dc=myforest,dc=com")

Group.Add("LDAP://" & User.distinguishedName)

set fso = createobject ("scripting.filesystemobject")

fso.createfolder "C:\myforest\" & Uname

WScript.Echo(Uname & " added!")

Приложение 2. Скрипт удаления пользователей (delete.vbs).

Set Domain = GetObject("WinNT://corp.myforest.com")

Uname = CStr(InputBox("Enter name:","Delete account",""))

Domain.Delete "User", Uname

strFolder = "C:\myforest\" & Uname

SET objFSO = CREATEOBJECT("Scripting.FileSystemObject")

objFSO.DeleteFolder strFolder

WScript.Echo(Uname & " deleted!")

Приложение 3. Скрипт разблокировки пользователей (unblock.vbs).

GroupName = InputBox("Enter group:","Unblock account","")

DomainController = "corp.myforest.com"

Set objGroup = GetObject("WinNT://" & DomainController & "/" & GroupName)

For Each Member in objGroup.Members

If Member.Class = "User" Then

If Member.IsAccountLocked = TRUE Or Member.AccountDisabled = TRUE Then

Wscript.Echo(Member.Name & " has been locked. It unlock now")

Member.IsAccountLocked = FALSE

Member.AccountDisabled = FALSE

Member.SetInfo

End If

End If

Next

Wscript.Echo("All users in " & GroupName & " are unlocked now")

Приложение 4. Скрипт поиска для поиска пользователей, у которых скоро истекает срок действия пароля (find.vbs).

ExpDaysMax = CInt(InputBox("Enter amount of days:","",""))

Set colGroups = GetObject("WinNT://corp.myforest.com" & "")

colGroups.Filter = Array("group")

For Each objGroup In colGroups

Set group = GetObject("WinNT://corp.myforest.com/" & objGroup.Name)

'Wscript.Echo objGroup.Name

For Each user in group.Members

'Wscript.Echo user.Name

ExpDays = CInt(user.PasswordExpirationDate - Now() - 1)

If ExpDays < ExpDaysMax Then

Wscript.Echo("Password for user " & user.Name & " in group " & objGroup.Name &" will expire after " & ExpDays & " days.")

End If

Next

Next

Приложение 5. Скрипт создания сетевого диска для компьютера (work.bat).

@echo off

mkdir \\WIN-ERHO99VDN1I\myforest\%ComputerName%

net use L: \\WIN-ERHO99VDN1I\myforest\%ComputerName%