Министерство науки и высшего образования Российской Федерации

Санкт-Петербургский Политехнический Университет Петра Великого

—

Институт компьютерных наук и кибербезопасности

ЛАБОРАТОРНАЯ РАБОТА № 2

«Установка и настройка службы каталога Active Directory»

1. по дисциплине «Безопасность современных информационных технологий»
2. Выполнил
3. студент гр. 5151004/10101 Веремейчук Я.Ю.

<подпись>

1. Преподаватель Соловей Р.С.

<подпись>

1. Санкт-Петербург
2. 2024
3. Цель работы

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

1. Задача

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.

6. Создать тестовых пользователей в каждой из групп.

7. Выполнить проверку правильности настройки полномочий путем попыток исполнения соответствующих действий от имен пользователей различных групп.

8. 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.

9. 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.

1. Теоретические исследования

Active Directory – службы каталогов корпорации Microsoft для операционных систем семейства Windows Server. Первоначально создавалась, как LDAP-совместимая реализация службы каталогов, однако, начиная с Windows Server 2008, включает возможности интеграции с другими службами авторизации, выполняя для них интегрирующую и объединяющую роль. Позволяет администраторам использовать групповые политики для обеспечения единообразия настройки пользовательской рабочей среды, разворачивать программное обеспечение на множестве компьютеров через групповые политики или посредством System Center Configuration Manager (ранее — Microsoft Systems Management Server), устанавливать обновления операционной системы, прикладного и серверного программного обеспечения на всех компьютерах в сети, используя Службу обновления Windows Server. Хранит данные и настройки среды в централизованной базе данных. Сети Active Directory могут быть различного размера: от нескольких десятков до нескольких миллионов объектов.

1. Ход работы

Были установлены две виртуальные машины: Windows Server 2019 Datacenter Evaluation (Desktop Ex.) и Windows 10 Pro. На Windows Server 2019 выставлены настройки сети «Сетевой мост», а также выделено 50 Гб виртуальной памяти, 4 Гб под оперативную память и 4 процессора (при более жестких настройках виртуальная машина зависала).

При запуске Windows Server можно увидеть панель мониторинга.

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок 1 – Панель мониторинга

Эта панель – основное (графическое) средство администрирования Windows Server. Здесь можно управлять компонентами и сервисами на сервере (проще говоря, настраивать то, что умеет делать сервер). Эту же панель можно использовать и для базовых сетевых настроек Windows Server, для чего есть вкладка "Local Server".

Первое, что нужно сделать — это поменять сетевое имя сервера (если при установке виртуальной машины оно не было установлено).

Сетевое имя (hostname) — это удобный способ идентификации узла в сети. Сетевое имя используется как альтернатива IP-адресу и позволяет не запоминать IP-адрес компьютера (при том, что этот адрес может меняться время от времени), а связываться с этим компьютером по его логическому названию.

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок 2 – Сетевое имя сервера

Для текущего стенда необходимо включить следующие сервисы (роли) на Windows Server: Доменные службы Active Directory, DNS-сервер.

Доменные службы Active Directory – эта роль фактически "включает" технологию Active Directory на сервере и делает его контроллером домена (под доменом в технологии AD понимается группа логически связанных объектов в сети). Благодаря этой роли администратор получает возможность управлять объектами в сети, а также хранить информацию о них в специальной распределенной базе данных.

Эта база данных содержит всю информацию об объектах в сети (например, именно в неё заносится информация об учётных записях пользователей). Когда человек подходит к рабочей станции и пытается выполнить вход в свою доменную учётную запись, эта рабочая станция связывается с контроллером домена с запросом на аутентификацию, и в случае успеха загружает пользовательский рабочий стол.

DNS-сервер. Обычно протокол DNS (Domain Name System) используется для обращения к узлам в сети не по их IP-адресу, а по доменному имени (строковый идентификатор), что, конечно, гораздо удобнее. Другими словами, DNS чаще всего используется для разрешения доменных имен.

Но область применения протокола DNS не ограничивается только сопоставлением хостового имени и IP-адреса, что как раз подтверждает технология Active Directory. Дело в том, что Microsoft решила построить технологию Active Directory не с нуля, а на основе протокола DNS. В частности, протокол DNS используется при определении местонахождения всех ключевых сервисов Active Directory в сети. Другими словами, рабочая станция при подключении к контроллеру домена понимает, "куда" ей надо обращаться, именно с помощью протокола DNS.

Все DNS-записи (в том числе с информацией о сервисах Active Directory) хранятся на DNS-сервере, а это значит, что необходимо поднять собственный DNS-сервер.

Итак, для настройки ролей необходимо выбрать «Manage» > «Add roles…». Приветственный экран можно пропустить. Далее нужно выбрать значение по умолчанию «Установка ролей или компонентов».

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок 3 – Установка ролей

Далее необходимо выбрать единственный текущий сервер.

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок 4 – Выбор текущего сервера

Далее необходимо выбрать две вышеописанные роли.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок 5 – Выбор ролей

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок 6 – Выбор компонентов

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок 7 – Установка необходимых пакетов

После установки пакетов на данном этапе сервер пока не обладает ролью контроллера домена. Необходимо продолжить настройку, нажав на кнопку «Promote this server to a domain controller».

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок 8 – Продолжение настройки AD

Далее приветствует мастер настройки доменных служб Active Directory с предложением выбрать конфигурацию развёртывания.

Технология Active Directory (как и DNS) подразумевает иерархическое построение имён на основе доменов. Домены могут выстраиваться в доменные деревья по принципу "родительско-дочерних" отношений. В основе дерева лежит так называемый корневой домен. При этом домен может иметь сколько угодно потомков. Домен-потомок располагается в пространстве имён родителя и является его "поддоменом" (subdomain). У доменного имени домена-потомка есть дополнительный префикс относительно доменного имени родителя (rus.abc.com, eng.abc.com). Один корневой домен основывает только одно доменное дерево со своим независимым пространством имён.

Если таких независимых деревьев много, то в этом случае эти деревья образуют структуру, которая называется "лес".

Изображение выглядит как текст, диаграмма, линия, шаблон

Автоматически созданное описание

Рисунок 9 – Пример леса

При этом в Active Directory доменные деревья не могут быть "сами по себе" – они обязательно должны находиться в лесу (даже если лес будет состоять всего из одного-единственного домена). Первый домен, который добавляется в лес, называется корневым доменом леса. Корневой домен леса используется для идентификации всего леса.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок 10 – Создание нового леса

Далее предлагается выбрать возможные параметры:

1. Режим работы леса и домена. Домены в одном лесу могут работать в разных режимах в зависимости от версии Windows Server на борту. Лес должен иметь режим не выше, чем самый "старый" домен в его составе. Т.к. планируется использовать только Windows Server 2019, то можно оставить этот режим и для леса и для домена;
2. DNS-сервер. Если ранее не была активирована роль DNS-сервера в мастере добавления ролей, то можно сделать это сейчас;
3. Должен ли контроллер домена выступать в роли Global Catalog-сервера. Глобальный каталог – это распределенное хранилище данных, которое хранит частичное представление обо всех AD-объектах в лесу. Это хранилище располагается на котроллерах домена, которые имеют дополнительную роль "Global Catalog Server" (Сервер глобального каталога). От обычного контроллера домена GC-сервер отличается в первую очередь тем, что помимо полной копии всех объектов в своем домене, хранит также частичную информацию обо всех объектах в других доменах леса.;
4. Включить ли режим базы данных Active Directory "только на чтение". Основная задача, которую преследует технология RODC — возможность безопасной установки собственного контролера домена в удаленных филиалах и офисах, в которых сложно обеспечить физическую защиту сервера с ролью DC. Контроллер домена RODC содержит копию базы Active Directory, доступную только на чтение. Это означает, что никто, даже при получении физического доступа к такому контроллеру домена, не сможет изменить данные в AD (в том числе сбросить пароль администратора домена).

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Автоматически созданное описание

Рисунок 11 – Создание пароля для восстановления служб каталогов DSRM

Далее, делегирование DNS – это передача ответственности за некоторую DNS-зону отдельному DNS-серверу. Это распространенная практика в больших сетях, в которых требуется разграничить зоны ответственности за доменные зоны между различными серверами. При делегировании DNS в "главный" DNS-сервер вносится запись о том, что "вот за эту DNS-зону несёт ответственность вон тот DNS-сервер, обращайся туда". Но в данной лабораторной работе одна зона DNS и DNS-сервер тоже один.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок 12 – Пропуск пункта о делегировании DNS

NetBIOS (Network Basic Input/Output) – это ещё один способ разрешения имён узлов в сети (более древний и более примитивный, чем DNS). NetBIOS-имена не предполагают никакой иерархии, их длина ограничивается всего лишь 16 символами, и они применяются только для разрешения имён компьютеров в локальной сети.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок 13 – Установка NetBIOS-имени

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Автоматически созданное описание

Рисунок 14 – Расположение базы данных

Все настройки должны проходить предварительную проверку.

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок 15 – Все проверки пройдены

Далее необходимо нажать «Install» и подождать. Стенд перезагрузится.

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок 16 – Просмотр компонентов домена

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Автоматически созданное описание

Рисунок 17 – Просмотр компонентов домена

Далее необходимо отключить фаервол.

Изображение выглядит как текст, снимок экрана, число, Шрифт

Автоматически созданное описание

Рисунок 18 – Отключение Firewall

Также необходимо включить видимость в сети (которая отключается при каждой перезагрузке системы).

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Рисунок 19 – Включение видимости в сети

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

Рисунок 20 – Включение видимости в сети

Далее необходимо установить политики выполнения PowerShell (для запуска скриптов). Область действия Set-ExecutionPolicy командлета по умолчанию – LocalMachine, которая затрагивает всех, кто использует компьютер.

Изображение выглядит как текст, Шрифт, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок 21 – Установка разрешений

Можно не забыть сделать снапшот машины.

Далее будет настроена политика паролей.

Парольная политика в домене Active Directory задает базовые требования безопасности к паролям учетных записей пользователей такие как сложность, длину пароля, частоту смены пароля и т.д. Надежная политика паролей AD позволяет снизить возможность подбора или перехвата паролей пользователей.

Настройки политики паролей пользователей в домене AD по умолчанию задаются через групповую политику Default Domain Policy.

Необходимо отредактировать Default Domain Policy с помощью кнопки «Edit». Если она недоступна, необходимо изменить права, добавив пользователя в группу Group Policy Creator Owners (и на всякий случай в другие админские группы). Затем перезагрузить стенд.

Изображение выглядит как текст, электроника, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 22 – Настройка парольной политики

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

Рисунок 23 – Edit

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок 24 – Поиск политик

Далее были установлены настройки, блокирующие на 5 минут после 3-кратного ввода неправильного пароля.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рисунок 25 – Новые настройки

По требованиям к лабораторной работе была создана простейшая структура компании.

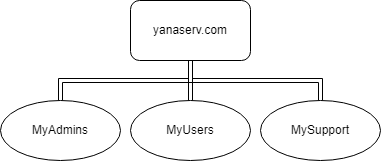


Рисунок 26 – Структура компании

Далее необходимо создать юниты для подразделений компании.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рисунок 27 – Создание юнитов

Изображение выглядит как текст, снимок экрана, число, Шрифт

Автоматически созданное описание

Рисунок 28 – Создание юнита

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рисунок 29 – Созданные юниты

Далее будут настроены сетевые папки.

Необходимо запустить mmc (Win + R).

Изображение выглядит как текст, снимок экрана, дисплей, Шрифт

Автоматически созданное описание

Рисунок 30 – Поиск редактора управления групповыми политиками

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Автоматически созданное описание

Рисунок 31 – Поиск редактора управления групповыми политиками

Изображение выглядит как текст, программное обеспечение, Значок на компьютере, веб-страница

Автоматически созданное описание

Рисунок 32 – Создание политики для группы MyUsers

Изображение выглядит как текст, программное обеспечение, снимок экрана, число

Автоматически созданное описание

Рисунок 33 – Создание политики для группы MyUsers

Далее необходимо создать две папки на диске C: для сопоставления дисков. Необходимо в настройках задать полный доступ и разрешение на редактирование.

Изображение выглядит как текст, диаграмма, программное обеспечение, число

Автоматически созданное описание

Рисунок 34 – Настройка папок

Изображение выглядит как текст, снимок экрана, число, программное обеспечение

Автоматически созданное описание

Рисунок 35 – Установка разрешений

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

Рисунок 36 – Установка разрешений

После этого нужно создать две Общие папки.

Изображение выглядит как текст, программное обеспечение, Значок на компьютере, число

Автоматически созданное описание

Рисунок 37 – Создание общей папки

Далее необходимо создать два диска в ранее открытом интерфейсе mmc во вкладке Drive Maps.

Изображение выглядит как текст, снимок экрана, число, дисплей

Автоматически созданное описание

Рисунок 38 – Создание диска

Изображение выглядит как текст, программное обеспечение, Значок на компьютере, веб-страница

Автоматически созданное описание

Рисунок 39 – Создание дисков

Далее для PCFolder необходимо создать папку.

Изображение выглядит как текст, программное обеспечение, снимок экрана, Значок на компьютере

Автоматически созданное описание

Рисунок 40 – Создание папки

После перезапуска системы был создан пользователь.

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок 41 – Добавление нового пользователя

Теперь нужно подключить второй стенд (Windows 10 Pro) к домену.

Но возникает ошибка.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок 42 – Ошибка при попытке назначить домен

Для решения проблемы необходимо:

1. Посмотреть с помощью команды ipconfig IP-адрес сервера
2. Открыть настройки сети на клиенте
3. Если в настройках виртуальной машины было настроено два адаптера (NAT и сетевой мост), нужно понять, какой именно адаптер является мостом. Для этого можно попортить настройки сети и попробовать открыть браузер. Если открылся, значит, настройки принадлежали адаптеру с мостом. Нужно выставить IP-адрес сервера.

Изображение выглядит как текст, программное обеспечение, снимок экрана, Значок на компьютере

Автоматически созданное описание

Рисунок 43 – Выставленные правильные настройки адаптера и появление сети домена yanaserv.com

Изображение выглядит как текст, программное обеспечение, Значок на компьютере, веб-страница

Автоматически созданное описание

Рисунок 44 – Успешное подключение к домену

Далее можно зайти от лица созданного ранее пользователя домена user1. При первом входе это происходит при нажатии на Other user, а при повторном входе пользователь появляется в списке.

Изображение выглядит как снимок экрана, текст, вода, небо

Автоматически созданное описание

Рисунок 45 – Вход под user1

При первом входе отображается только одна общая папка, а при повторном входе – обе.

Изображение выглядит как текст, программное обеспечение, Значок на компьютере, веб-страница

Автоматически созданное описание

Рисунок 46 – Появление папок для user1

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рисунок 47 – Автоматически созданная на сервере папка user1

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок 48 – Разрешение подключения к ПК на клиенте

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок 49 – Разрешение подключения к ПК

Изображение выглядит как текст, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок 50 – Запуск команд на клиенте

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок 51 – Создание групп администраторов

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рисунок 52 – Создание пользователей-администраторов

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок 53 – Процесс выдачи прав

Изображение выглядит как текст, снимок экрана, программное обеспечение, Операционная система

Автоматически созданное описание

Рисунок 54 – Вход в UserAccManager

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 55 – Создание нового пользователя

Изображение выглядит как текст, снимок экрана, программное обеспечение, Шрифт

Автоматически созданное описание

Рисунок 56 – Вход под новым созданным с помощью UserAccManager пользователем

Изображение выглядит как небо, снимок экрана, облако, вода

Автоматически созданное описание

Рисунок 57 – Неправильные пароли

Изображение выглядит как вода, текст, снимок экрана, гора

Автоматически созданное описание

Рисунок 58 – Отказ на вход

1. Выводы

В ходе выполнения данной лабораторной работы были получены навыки работы с Active Directoty, настройки контроллера домена, добавления компьютера пользователя в домен, создания файлового сервера, редактирования групповых политик. Также были получены навыки написания скриптов для PowerShell.

Источники

1. Настраиваем и автоматизируем развёртывание Active Directory // Хабр URL: <https://habr.com/ru/companies/testo_lang/articles/525326/#vklyuchaem-nuzhnye-komponenty>
2. Настройка политики паролей в домене Active Directory // WinITPro URL: <https://winitpro.ru/index.php/2018/10/26/politika-parolej-uchetnyx-zapisej-v-active-directory/>
3. Can't edit default domain policy // Microsoft Learn URL: <https://learn.microsoft.com/en-us/archive/msdn-technet-forums/d3eea9a4-3e74-4f7d-9c0c-1fb70badece9>
4. Сопоставление дисков на сервере. logonuser, username. Общие папки [Windows Server 2012] #6 // YouTube URL: <https://www.youtube.com/watch?v=h46zIleS0lY>

Приложение А

Листинг скрипта для создания пользователя.

Import-Module ActiveDirectory

$OU = Get-ADOrganizationalUnit -SearchBase "DC=yanaserv,DC=com" -SearchScope Subtree -Filter \*

ForEach($ou in $OU)

{

if($ou.Name -eq $args[0])

{

$Users = Search-ADAccount -SearchBase $ou -UsersOnly -LockedOut

foreach ($user in $Users)

{

Unlock-ADAccount -Identity $($user.Name)

Write-Host $user.Name " unlocked"

}

}

}

Приложение Б

Листинг скрипта для создания групп

Import-Module ActiveDirectory

$domainL1="com"

$domainL2="yanaserv"

$domainL3="MyAdmins"

$groupGeneralAdmins="GeneralAdmins"

$groupResourceAdmins="ResourceAdmins"

$groupAccountManagers="AccountManagers"

$groupHelpDesk="HelpDesk"

New-ADGroup -Name $groupGeneralAdmins -GroupCategory Security -GroupScope Global -Path "OU=$domainL3, DC=$domainL2, DC=$domainL1"

New-ADGroup -Name $groupResourceAdmins -GroupCategory Security -GroupScope Global -ManagedBy $groupGeneralAdmins -Path "OU=$domainL3, DC=$domainL2, DC=$domainL1"

New-ADGroup -Name $groupAccountManagers -GroupCategory Security -GroupScope Global -ManagedBy $groupGeneralAdmins -Path "OU=$domainL3, DC=$domainL2, DC=$domainL1"

New-ADGroup -Name $groupHelpDesk -GroupCategory Security -GroupScope Global -ManagedBy $groupGeneralAdmins -Path "OU=$domainL3, DC=$domainL2, DC=$domainL1"

Приложение В

Листинг скрипта для создания пользователей-администраторов

Import-Module ActiveDirectory

New-ADUser -Name "UserAccManager" -SamAccountName "UserAccManager" -Path "OU=MyAdmins, DC=yanaserv, DC=com" -AccountPassword(ConvertTo-SecureString "BSIT2am" -AsPlainText -Force) -Enable $true

New-ADUser -Name "UserHelpDesk" -SamAccountName "UserHelpDesk" -Path "OU=MyAdmins, DC=yanaserv, DC=com" -AccountPassword(ConvertTo-SecureString "BSIT2hd" -AsPlainText -Force) -Enable $true

New-ADUser -Name "UserGenAdmin" -SamAccountName "UserGenAdmin" -Path "OU=MyAdmins, DC=yanaserv, DC=com" -AccountPassword(ConvertTo-SecureString "BSIT2ga" -AsPlainText -Force) -Enable $true

New-ADUser -Name "UserResAdmin" -SamAccountName "UserResAdmin" -Path "OU=MyAdmins, DC=yanaserv, DC=com" -AccountPassword(ConvertTo-SecureString "BSIT2ra" -AsPlainText -Force) -Enable $true

Add-ADGroupMember "AccountManagers" UserAccManager

Add-ADGroupMember "HelpDesk" UserHelpDesk

Add-ADGroupMember "GeneralAdmins" UserGenAdmin

Add-ADGroupMember "ResourceAdmins" UserResAdmin

Приложение Г

Листинг скрипта для создания папки OU

Import-Module ActiveDirectory

$domenL1="com"

$domenL2="yanaserv"

$domenL3="MyUsers"

New-ADOrganizationalUnit -Name Customers -Path "DC=$domenL2, DC=$domenL1"

New-ADOrganizationalUnit -Name Admins -Path "DC=$domenL2, DC=$domenL1"

New-ADOrganizationalUnit -Name Categories -Path "DC=$domenL2, DC=$domenL1"

New-ADOrganizationalUnit -Name Hits -Path "OU=$domenL3, DC=$domenL2, DC=$domenL1"

New-ADOrganizationalUnit -Name Sales -Path "OU=$domenL3, DC=$domenL2, DC=$domenL1"

Приложение Д

Листинг скрипта для поиска пользователей, у которых скоро истекает срок действия пароля

Import-module ActiveDirectory

$daysLim = [int]($args[0])

$UserList=Search-ADAccount -AccountExpiring -TimeSpan (New-TimeSpan -Days $daysLim)

if($UserList)

{

foreach($User in $UserList)

{

$expireDate=$User.AccountExpirationDate

$currentDate=get-Date

$daysLeft = $expireDate - $currentDate

write-host "[Searcher] " $User.Name ": time left until password expires " $daysLeft.Days " days!"

}

}

else

{

write-host "[Searcher] There is no user whose password is about to expire!"

}

Приложение Е

Листинг скрипта для установления прав для групп

dsacls.exe "OU=MyAdmins DC=yanaserv, DC=com" /I:T /G "yanaserv\AccountManagers:CCDC;user"

dsacls.exe "OU=MyAdmins DC=yanaserv, DC=com" /I:S /G "yanaserv\AccountManagers:RCWDWO;;user"

dsacls.exe "OU=MyAdmins DC=yanaserv, DC=com" /I:S /G "yanaserv\AccountManagers:CALO;;user"

dsacls.exe "OU=MyAdmins DC=yanaserv, DC=com" /I:S /G "yanaserv\AccountManagers:RPWP;userAccountControl;user"

dsacls.exe "OU=MyAdmins DC=yanaserv, DC=com" /I:S /G "yanaserv\AccountManagers:RPWP;pwdLastSet;user"

dsacls.exe "OU=MyAdmins DC=yanaserv, DC=com" /I:S /G "yanaserv\HelpDesk:RPWP;lockoutTime;user"

dsmod group "cn=Administrators, cn=Builtin, DC=yanaserv, DC=com" -addmbr "cn=GeneralAdmins, OU=MyAdmins, DC=yanaserv, DC=com"

dsmod group "cn=IIS\_IUSRS, cn=Builtin, DC=yanaserv, DC=com" -addmbr "cn=ResourceAdmins, OU=MyAdmins, DC=yanaserv, DC=com"

Приложение Ж

Листинг скрипта для разблокировки пользователей

Import-Module ActiveDirectory

$OU = Get-ADOrganizationalUnit -SearchBase "DC=yanaserv,DC=com" -SearchScope Subtree -Filter \*

ForEach($ou in $OU)

{

if($ou.Name -eq $args[0])

{

$Users = Search-ADAccount -SearchBase $ou -UsersOnly -LockedOut

foreach ($user in $Users)

{

Unlock-ADAccount -Identity $($user.Name)

Write-Host $user.Name " unlocked"

}

}

}