ВВЕДЕНИЕ

Умение работать с операционными системами семейства Microsoft Windows является важным навыком для тех, кто желает построить успешную карьеру в ИТ. Данное задание содержит множество задач, основанных на опыте реальной эксплуатации информационных систем, в основном интеграции и аутсорсинге. Если вы можете выполнить задание с высоким результатом, то вы точно сможете обслуживать информационную инфраструктуру большого предприятия.

ОПИСАНИЕ ЗАДАНИЯ

В рамках легенды задания Вы – системный администратор вновь создаваемой московской компании. Вам необходимо настроить сервисы в локальной сети головного офиса.
Также учтите, что компания приобрела одно из малых предприятий в Ижевске и им тоже нужна Ваша помощь.
Также Вам предстоит настроить защищенный канал связи между офисами, доверие между доменами и удаленное подключение клиентов, предварительно смоделировав наличие провайдера Интернета. Брандмауэры на всех доступных устройствах должны быть активны!

ЗАДАНИЕ

Настройка DC-M

Базовая настройка

- переименуйте компьютер в DC-M;
- задайте настройки сети в соответствии с таблицей 1;
- обеспечьте работоспособность протокола ICMP (для использования команды ping).

Active Directory

- сделайте сервер основным контроллером домена Moscow.ru;
- настройте одностороннее нетранзитивное доверие с доменом Izhevsk.ru – пользователи домена Moscow.ru должны иметь доступ к ресурсам домена Izhevsk.ru, но не наоборот.

DHCP

- настройте протокол DHCP для автоконфигурации клиентов;
- настройте failover: mode – Load balancer, partner server – FILES-M, state swithover – 10 min;
- диапазон выдаваемых адресов: 172.16.0.100-200/24;
- настройте дополнительные свойства области (адреса обоих DNS-серверов и основного шлюза).

DNS

- настройте необходимые зоны прямого и обратного просмотра, обеспечьте их согласованную работу со службой DNS на FILES-M;
- создайте вручную все необходимые записи типа A и PTR для серверов домена и необходимых web-сервисов;
- сделайте необходимые настройки для работоспособности доверия с доменом Izhevsk.ru (при появлении в сети новых DNS серверов они должны автоматически получать необходимые для работоспособности доверия настройки).

GPO

- запретите анимацию при первом входе пользователей в систему на всех клиентских компьютерах домена;
- члены группы IT должны быть членами группы локальных администраторов на всех клиентских компьютерах домена;

- в браузерах IE Explorer и Microsoft Edge (установите и используйте windows10.admx) должна быть настроена стартовая страница – www.moscow.ru;
- запретите изменение экранной заставки и *Корзину* на рабочем столе для всех пользователей домена, кроме членов группы локальных администраторов клиентских компьютеров;
- для членов группы Experts настройте перенаправление папок *my Documents* и *Desktop* по адресу FILES-M→d:\shared\redirected.

Элементы доменной инфраструктуры

- создайте подразделения: Experts, Competitors, Managers, Visitors, IT и Project;
- в соответствующих подразделениях создайте доменные группы: Experts, Competitors, Managers, Visitors, IT, Project_Budget-R, Project_Budget-W, Project_Intranet-R, Project_Intranet-W, Project_Logistics-R, Project_Logistics-W;

Внимание! Указанные выше подразделения и группы должны быть созданы в домене обязательно. Если Вы считаете, что для выполнения задания необходимы дополнительные элементы доменной инфраструктуры, Вы можете создать их.

- создайте 3-4 пользователя используя данные из файла **users.htm** (вся имеющаяся информация о пользователях должна быть внесена в Active Directory); поместите пользователей в соответствующие подразделения и группы; все созданные учетные записи должны быть включены и доступны;
- для каждого пользователя создайте автоматически подключаемую в качестве диска U:\ домашнюю папку по адресу FILES-M→d:\shares\users.

Настройка FILES-M

Базовая настройка

- переименуйте компьютер в FILES-M;
- задайте настройки сети в соответствии с таблицей 1;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к домену Moscow.ru;
- из трех имеющихся жестких дисков создайте RAID-5 массив; назначьте ему букву D:\.

Active Directory

- сделайте сервер дополнительным контроллером домена Moscow.ru;
- контроллер не должен выполнять функцию глобального каталога.

DHCP

- настройте протокол DHCP для автоконфигурации клиентов;
- настройте failover: mode – Load balancer, partner server – DC-M, state swithover – 10 min;

DNS

- сделайте сервер дополнительным DNS-сервером в домене Moscow.ru;
- загрузите с DC-M все зоны прямого и обратного просмотра.

Общие папки

- создайте общие папки для подразделений (Competitors, Experts and Managers) по адресу FILES-M→d:\shares\departments;
- обеспечьте привязку общей папки подразделения к соответствующей группе в качестве диска G:\;
- создайте общую папку проектов по адресу FILES-M→d:\shares\projects;
- в папке d:\shares\projects создайте следующие папки: Budget, Intranet, Logistics; настройте разрешения этих папок в соответствии с таблицей 2;
- создайте привязку общей папки проектов для всех пользователей, кроме членов группы Visitors, в качестве диска P:\; пользователи должны видеть только те папки внутри диска P:\, к которым им разрешен доступ.

Квоты/Файловые экраны

- установите максимальный размер в 5Gb для каждой домашней папки пользователя (U:\);
- запретите хранение в домашних папках пользователей файлов с расширениями .cmd и .exe; учтите, что файлы остальных типов пользователи вправе хранить в домашних папках.

IIS

- создайте сайт для менеджеров компании (используйте предоставленный html-файл в качестве документа по умолчанию);
- сайт должен быть доступен по имени managers.moscow.ru только по протоколу https исключительно для членов группы Managers по их пользовательским сертификатам.

Настройка ROOTCA-M

Базовая настройка

- переименуйте компьютер в ROOTCA-M;
- задайте настройки сети в соответствии с таблицей 1;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- не присоединяйте компьютер к какому-либо домену.

Службы сертификации

- установите службы сертификации;
- настройте одиночный корневой сервер сертификации (длина ключа и алгоритмы шифрования значения не имеют);
- имя центра сертификации – Moscow Root CA;
- срок действия сертификата – 10 лет;
- CRL location: http://RU-SUBCA.russia.net/certenroll/<caname><crlnamesuffix><deltacrlallowed>.crl
- AIA location: http://RU-SUBCA.russia.net/certenroll/<serverdnsname>_<caname><certificatename>.crt
- создайте список отзыва сертификатов и сертификат корневого центра сертификации для SUBCA-M;
- выпустите сертификат подчиненного центра сертификации для SUBCA-M, одобрив соответствующий запрос;
- после всех настроек отключите сетевой интерфейс.

Настройка SUBCA-M

Базовая настройка

- переименуйте компьютер в SUBCA-M;
- задайте настройки сети в соответствии с таблицей 1;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к домену Moscow.ru.

Службы сертификации

- установите службы сертификации;
- настройте подчиненный доменный центр сертификации;
- имя центра сертификации – Moscow Sub CA;
- срок действия сертификата – 5 лет;
- импортируйте и опубликуйте список отзыва сертификатов с ROOTCA-M;
- настройте шаблон выдаваемого сертификата для клиентских компьютеров *MoscowClients*: *subject name=common name*, автозапрос для всех клиентских компьютеров домена;
- настройте шаблон выдаваемого сертификата для группы Managers *MoscowUsers*: *subject name=common name*, автозапрос только для пользователей – членов группы Managers.

Настройка CLIENT-M

Базовая настройка

- переименуйте компьютер в CLIENT-M;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к домену Moscow.ru;
- установите набор компонентов удаленного администрирования RSAT;
- запретите использование «спящего режима»;
- используйте компьютер для тестирования настроек в домене Moscow.ru: пользователей, общих папок, групповых политик, в том числе – тестирования удаленных подключений через Direct Access (временно переключаю компьютер в сеть Internet).

Работа с DC-IZ

Active Directory

- сделайте сервер основным контроллером домена Izhevsk.ru;
- создайте 3-4 пользователя используя данные из файла **users.htm,** учетные записи должны быть отключены.

DNS

- сделайте необходимые настройки для работоспособности доверия с доменом Moscow.ru (при появлении в сети новых DNS серверов они должны автоматически получать необходимые для работоспособности доверия настройки);
- обеспечьте разрешение имен сайтов www.moscow.ru и www.izhevsk.ru.

Службы удаленных рабочих столов

- разверните терминальный сервер, не устанавливайте и не настраивайте компоненты лицензирования;
- сконфигурируйте web-доступ RemoteApp к службам терминалов сервера;
- опубликуйте программу *Wordpad* на web-портале RemoteApp для членов группы Moscow\IT;
- опубликуйте программу *Notepad* на web-портале RemoteApp для членов группы Moscow\Managers;
- web-интерфейс сервера должен быть настроен таким образом, чтобы пользователи могли автоматически получать доступ к форме входа на web-интерфейс удаленных рабочих столов при указании адресов http://rds.izhevsk.ru и https://rds.izhevsk.ru;
- с помощью доменного центра сертификации на сервере SUBCA-M сгенерируйте и используйте для терминальных служб соответствующий SSL-сертификат. Сертификат должен быть использован для всех установленных компонентов терминальных служб. При обращении с любого компьютера в домене Moscow.ru или Izhevsk.ru к сайту по имени https://rds.izhevsk.ru сертификат должен распознаваться как доверенный и действительный.

Работа с IIS-IZ

IIS

- создайте сайт www.moscow.ru (используйте предоставленный htm-файл в качестве документа по умолчанию);
- создайте сайт www.izhevsk.ru (используйте предоставленный htm-файл в качестве документа по умолчанию);
- оба сайта должны быть доступны по протоколу https с использованием сертификатов, выданных SUBCA-M.

Работа с CLIENT-IZ

Базовая настройка

- переименуйте компьютер в CLIENT-IZ;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);

- присоедините компьютер к домену Izhevsk.ru;
- запретите использование «спящего режима»;
- используйте компьютер для тестирования настроек в домене Izhevsk.ru.

Настройка EDGE-IZ

Базовая настройка

- переименуйте компьютер в EDGE-IZ;
- задайте настройки сети в соответствии с таблицей 1;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к домену Izhevsk.ru.

Настройка RRAS

- установите USERGATE;
- настройте шлюз для доступа к сети «интернет» пользователям сети Izhevsk

Настройка EDGE-M

Базовая настройка

- переименуйте компьютер в EDGE-M;
- задайте настройки сети в соответствии с таблицей 1;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к домену Moscow.ru.

Настройка RRAS

- установите USERGATE;
- настройте шлюз для доступа к сети «интернет» пользователям сети Moscow

Имя компьютера	Имя домена	IP-адреса
DC-IZ	Izhevsk.ru	172.19.0.1/24
CLIENT-IZ		DHCP
IIS-IZ		172.19.0.3/24
EDGE-IZ		172.19.0.250/24 200.100.50.101/24
DC-M	Moscow.ru	172.16.0.1/24
FILES-M		172.16.0.2/24
SUBCA-M		172.16.0.4/24
EDGE-M		172.16.0.250/24 200.100.50.100/24
CLIENT-M		DHCP
ROOTCA-M	None	172.16.0.3/24

Таблица 2.

Имя общего ресурса	Расположение	Доступ только для чтения	Доступ для чтения и записи
Budget	FILES-M→D:\shares\projects	RU-Budget-R	RU-Budget-W
Intranet		RU-Intranet-R	RU-Intranet-W
Logistics		RU-Logistics-R	RU-Logistics-W

Диаграмма виртуальной сети