



worldskills

КОМПЕТЕНЦИЯ «СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

КОНКУРСНОЕ ЗАДАНИЕ

МОДУЛЬ В: ПУСКО-НАЛАДКА ИНФРАСТРУКТУРЫ НА ОСНОВЕ ОС СЕМЕЙСТВА MICROSOFTWINDOWS

Разработано
сертифицированным экспертом WSR:
Дюгуровым Д.В.

Дата 09.04.18
Версия: 1



Введение. На выполнение задания отводится ограниченное время – подумайте, как использовать его максимально эффективно. Составьте план выполнения работ. Вполне возможно, что для полной работоспособности системы в итоге действия нужно выполнять не строго в той последовательности, в которой они описаны в данном конкурсном задании.

В рамках легенды конкурсного 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. В ижевском офисе сеть уже функционировала, но системный администратор (из-за скандала при увольнении) не предоставил доступа к действующему там контроллеру домена. Вам придется восстановить доступ к ижевскому домену.

Также Вам предстоит настроить защищенный канал связи между офисами, доверие между доменами и удаленное подключение клиентов, предварительно смоделировав наличие провайдера Интернета.

Внимательно прочтите задание от начала до конца – оно представляет собой целостную систему. При первом доступе к операционным системам либо следуйте указаниям мастера, либо используйте следующие реквизиты: *Administrator/P@ssw0rd*.

Если предоставленные виртуальные машины начнут самопроизвольно отключаться в процессе работы, попробуйте выполнить на них команду *slmgr /rearm* или обратитесь к техническому эксперту.

Комплектация конкурсного задания

1. Текстовые файлы:
 - данный файл с конкурсным заданием;
 - файл дополнений к конкурсному заданию, содержащий: описание вида предустановок, описание используемых операционных систем, рекомендации по выделению ресурсов для виртуальных машин, рекомендации возможных изменений к заданию в рамках 30%.
2. Предоставляемые конкурсантам компоненты проекта:
 - файл для импорта пользователей в домен Moscow (.xlsx);
 - стартовая страница сайта managers.moscow.ru (.htm);
 - стартовая страница сайта www.moscow.ru (.htm);
 - стартовая страница сайта www.izhevsk.ru (.htm).
3. Программное обеспечение:
 - Windows server 2016;
 - Microsoft Office;
 - RSAT tools for Windows 10;
 - Windows10.ADMX.

Внимание! Все указанные компоненты предоставляются участникам в виде ISO-файлов на локальном или удаленном хранилище.

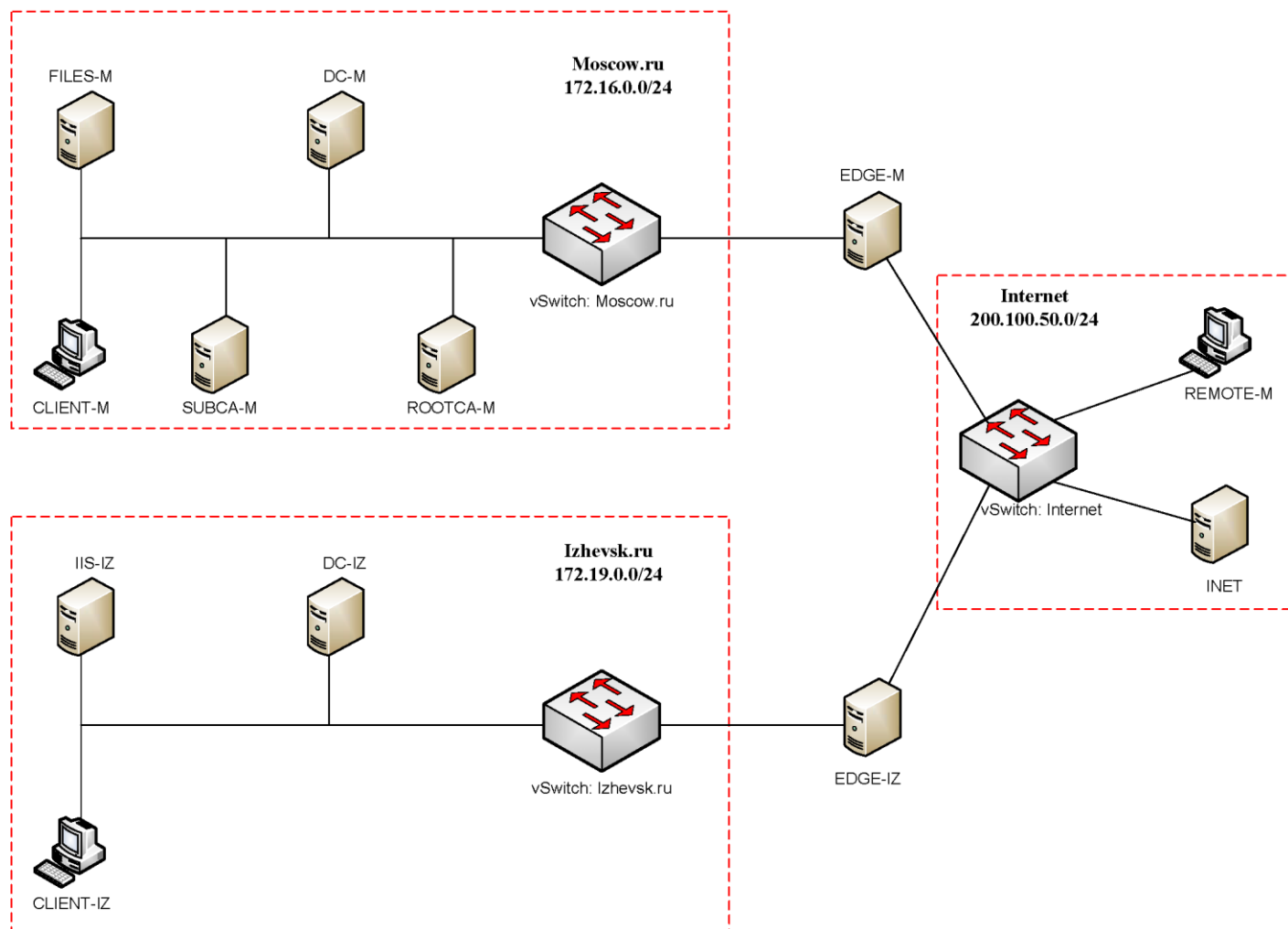
Участники не имеют права пользоваться любыми устройствами, за исключением находящихся на рабочих местах устройств, предоставленных организаторами.

Участники не имеют права приносить с собой на рабочее место заранее подготовленные текстовые материалы.

В итоге участники должны обеспечить наличие и функционирование в соответствии с заданием служб и ролей на указанных виртуальных машинах. При этом участники могут самостоятельно выбирать способ настройки того или иного компонента, используя предоставленные им ресурсы по своему усмотрению.



Network diagram





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;
- также создайте доменную группу DAClients;



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 пользователей, используя прилагаемый excel-файл (вся имеющаяся в файле 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 switchover – 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.



ИИС

- создайте сайт для менеджеров компании (используйте предоставленный htm-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://SUBCA-M.Moscow.ru/certenroll/<caname><crlnamesuffix><deltacrlallowed>.crl`
- AIA location: `http://SUBCA-M.Moscow.ru/certenroll/<serverdnsname>_<caname><certificatename>.crl`
- 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 переключая компьютер в сеть Internet).

Работа с DC-IZ

Восстановление доступа

- получите (восстановите) доступ к контроллеру домена и реплике Active Directory; помните – на сервере хранится важная информация, поэтому просто переустановить операционную систему нельзя!

Поиск пользователей и ресурсов

- найдите всех пользователей домена Izhevsk.ru, у которых в графе *Job Title* проставлено значение *Expert*;
- переместите всех найденных пользователей в специальное подразделение Migration (при необходимости создайте его) и отключите учетные записи в домене Izhevsk.ru;
- найдите в домене Izhevsk.ru и скопируйте на FILES-M→d:\shares\migrated все домашние папки ранее найденных пользователей;
- в домене Moscow.ru в подразделении Migrated (при необходимости создайте это подразделение) создайте новые учетные записи, соответствующие найденным ранее и отключенным учетным записям; задайте для них пароль *NewP@ssw0rd*;
- для вновь созданных учетных записей обеспечьте привязку домашних папок в качестве диска S:\; проследите, что вновь созданные в домене Moscow.ru пользователи имеют доступ к скопированным из домена Izhevsk.ru файлам, находящимся в их домашних папках.

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 Domain Admins;



- опубликуйте программу *Notepad* на web-портале RemoteApp для членов группы Domain Users;
- 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 INET

Базовая настройка

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

DNS/IIS

- настройте эмуляцию подключения к Интернету, принимая во внимание версии используемых операционных систем;
- создайте в DNS соответствующие записи для удаленного подключения клиентов к серверу Direct Access в домене Moscow.ru, а также записи для доступа внешних клиентов к сайтам www.moscow.ru и www.izhevsk.ru.



ДНСР

- настройте протокол DHCP для клиентов в сети Internet;
- диапазон выдаваемых адресов: .170-190/24;
- остальные необходимые параметры области сконфигурируйте по вашему выбору.

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 службу RRAS;
- настройте защищенное VPN-соединение с доменом Moscow.ru с использованием аутентификации по сертификатам компьютеров; сертификаты должны быть выданы SUBCA-M; весь трафик между доменами должен передаваться через это соединение;
- настройте проброс портов для доступа удаленных клиентов (проверяется из сети Internet) к сайтам www.moscow.ru и www.izhevsk.ru, развернутым на IIS-IZ.

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 службу RRAS;
- настройте защищенное VPN-соединение с доменом Izhevsk.ru с использованием аутентификации по сертификатам компьютеров; сертификаты должны быть выданы SUBCA-M; весь трафик между доменами должен передаваться через это соединение.

Настройка Direct Access

- сделайте учетные записи компьютеров CLIENT-M и REMOTE-M членам группы DAClients;
- только члены группы DAClients могут подключаться к сети с использованием Direct Access;
- название соединения – *DA-Moscow*;
- в качестве NCA используйте FILES-M;
- для подключения внешних клиентов используйте имя *connect.moscow.ru*;
- для настройки используйте соответствующий сертификат, выданный SUBCA-M (использование самозаверенных сертификатов не допускается);
- клиенты Direct Access должны иметь полный доступ к общим ресурсам в обоих офисах.



Настройка REMOTE-M

Базовая настройка

- переименуйте компьютер в REMOTE-M;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- запретите использование «спящего режима»;
- не меняя сетевых настроек (сетевой интерфейс должен быть соединен с сетью Internet) присоедините компьютер к домену Moscow.ru в режиме OFFLINE;
- сохраните созданный на DC-M файл ответов для offline-присоединения к домену по адресу C:\Remote.txt.

Таблица 1 – Реквизиты

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
REMOTE-M		DHCP
ROOTCA-M	None	172.16.0.3/24
INET		200.100.50.200/24

Таблица 2 – Файловый доступ

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