**Министерство образования и науки Самарской области**

**ГБПОУ «ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ КОЛЛЕДЖ»**

**Типовое задание**

для оценки освоения итоговых образовательных результатов

профессионального модуля

**ПМ 02 Организация сетевого администрирования**

программы подготовки специалистов среднего звена по специальности

**09.02.06Сетевое и системное администрирование**

**Инструкция**

Внимательно прочитайте задание полностью. Обратите внимание на то, что задание составлено не в хронологическом порядке. Некоторые секции могут потребовать действий из других секций, которые изложены ниже. На вас возлагается ответственность за распределение своего рабочего времени. Не тратьте время, если у вас возникли проблемы с некоторыми заданиями. Вы можете использовать временные решения (если у вас есть зависимости в технологическом стеке) и продолжить выполнение других задач. Рекомендуется тщательно проверять результаты своей работы..

**Задание**:

**Настройка DC1**

**Базовая настройка**

* переименуйте компьютер в DC1;
* в качестве адреса DC1 используйте первый возможный адрес из подсети 172.16.19.64/26;
* обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом WindowsFirewall должен быть включен для всех сетевых профилей.

**Active Directory**

* сделайте сервер контроллером домена Kazan.wsr.

**DHCP**

* настройте протокол DHCP для автоконфигурации клиентов – в качестве диапазона выдаваемых адресов используйте все незанятые серверами адреса в подсети;
* настройте failover: mode – Load balancer, partner server – SRV1, state switchover – 5 min;
* настройте дополнительные свойства области (адреса DNS-серверов и основного шлюза).

**DNS**

* настройте необходимые зоны прямого и обратного просмотра;
* создайте все необходимые записи типа A и PTR для серверов домена и необходимых web-сервисов;
* обеспечьте разрешение имен сайтов обеих компаний.

**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;
* Для пользователей группы Sales в браузерах IE Explorer и MicrosoftEdge должна быть настроена стартовая страница – www.kazan.wsr;
* Для пользователей группы IT должна быть настроена стартовая страница SPB.wse
* пользователи домена при обращении к общим папкам, на доступ которым у них нет разрешений, должны получать вместо стандартного уведомление следующего вида: «Youdonothavepermissionstousethispath - [путь к папке]! Donottryitagain!».

**Элементы доменной инфраструктуры**

* создайте подразделения: IT и Sales;
* в соответствующих подразделениях создайте одноименные доменные группы.
* в каждой группе создайте с помощью скрипта по 30 пользователей. Все учетные записи должны иметь возможность входа в домен с логином, созданным по следующему шаблону *НазваниеГруппы\_ПорядковыйНомерПользователя@kazan.wsr.* В качестве пароля используйте P@ssw0rdX, где X – номер пользователя Все учетные записи пользователей должны быть включены. Вход в систему должен быть обеспечен для всех пользователей со всех клиентских компьютеров домена и рядовых серверов.
* для каждого пользователя, члена группы IT, создайте автоматически подключаемую в качестве диска U:\ домашнюю папку внутри папки по адресу SRV1→d:\shares\IT;
* все пользователи при первом входе в домен с компьютера CLI1 должны видеть на рабочем столе ярлык программы *MicrosoftManagementConsole*.

**Настройка SRV1**

**Базовая настройка**

* переименуйте компьютер в SRV1;
* в качестве адреса SRV1 используйте второй возможный адрес из подсети 172.16.19.64/26;
* обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей.
* с помощью дополнительных жестких дисков создайте RAID-5 массив; назначьте ему букву D:\.

**Active Directory**

* сделайте сервер дополнительным контроллером домена Kazan.wsr;
* сервер должен быть контроллером домена только для чтения.

**DHCP**

* настройте протокол DHCP для автоконфигурации клиентов;
* настройте failover: mode – Load balancer, partner server – DC1, state switchover – 5 min.

**DNS**

* сделайте сервер дополнительным DNS-сервером в домене Kazan.wsr;
* загрузите c DC1 все зоны прямого и обратного просмотра;

**Общие папки**

* создайте общие папки для подразделений (IT, Sales) по адресу SRV1→d:\shares\departments. Просматривать и редактировать файлы в папках могут только члены соответствующей группы.
* обеспечьте привязку общей папки подразделения к соответствующей группе пользователей в качестве диска G:\.
* Настройте перенаправление каталогов Documents и Desktop в директорию SRV1: D:\Shares\Redirected для всех пользователей группы IT

**Квоты/Файловые экраны**

* установите максимальный размер в 10 MB для каждой домашней папки пользователя (U:\);
* запретите хранение в домашних папках пользователей файлов с использованием встроенного шаблона для блокировки мультимедиа.

**IIS**

* создайте сайт компании со стартовой страницей следующего содержания:

<html>

Welcome to Kazan!

</html>;

* сайт должен быть доступен по имени www.kazan.wsr по протоколам http и https в обоих сетевых сегментах с использованием сертификатов, выданных DCA.

**Настройка DCA**

**Базовая настройка**

* переименуйте компьютер в DCA;
* в качестве адреса DCA используйте третий возможный адрес из подсети 172.16.19.64/26;
* обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом WindowsFirewall должен быть включен для всех сетевых профилей;
* присоедините компьютер к домену Kazan.wsr.

**Службы сертификации**

* установите службы сертификации;
* настройте основной доменный центр сертификации;
* имя центра сертификации – RootKazanCA;
* срок действия сертификата – 8 лет;
* настройте шаблон выдаваемого сертификата для клиентских компьютеров ClientComps: subjectname=commonname, автозапрос только для компьютера R1;
* настройте шаблон выдаваемого сертификата *ITUsers*: *subjectname=commonname*, автозапрос только для пользователей – членов группы IT.

**Настройка CLI1**

**Базовая настройка**

* переименуйте компьютер в CLI1;
* обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом WindowsFirewall должен быть включен для всех сетевых профилей;
* присоедините компьютер к домену *Kazan.wsr;*
* запретите использование «спящего режима» таким образом, чтобы пользователи домена не могли изменить эту настройку без участия администратора домена;
* используйте компьютер для тестирования настроек в домене *Kazan.wsr:* пользователей, общих папок, групповых политик.

**Настройка DC2**

**Базовая настройка**

* переименуйте компьютер в DC2;
* в качестве адреса DC2 используйте первый возможный адрес из подсети 172.16.20.96/27;
* обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом WindowsFirewall должен быть включен для всех сетевых профилей.

**ActiveDirectory**

* сделайте сервер контроллером домена *SPB.wse;*
* настройте двустороннее доверие доменом *Kazan.wsr.*

**DHCP**

* настройте протокол DHCP для автоконфигурации клиентов – в качестве диапазона выдаваемых адресов используйте все незанятые серверами адреса в подсети.

**DNS**

* настройте необходимые зоны прямого и обратного просмотра;
* создайте вручную все необходимые записи типа A и PTR для серверов домена и необходимых web-сервисов;
* обеспечьте разрешение имен сайтов обеих компаний.

**Элементы доменной инфраструктуры**

* создайте учетную запись пользователя домена *User1\P@ssw0rd*, используйте группу по умолчанию – *DomainUsers*.
* для всех *пользовательских учетных записей в домене используйте перемещаемые профили;*
* *для хранения профилей пользователей используйте общую папку по адресу SRV2→c:\profiles;*
* *каждый пользователь должен иметь доступ к файлам только* своего профиля; при обращении к указанной общей папке средствами программы *Проводник* пользователь должен видеть в списке только папку со своим профилем.

**GPO**

* настройте необходимые политики, обеспечивающие использование сервера DCA.kazan.wsr в качестве доверенного центра сертификации.

**RDS**

* На сервере DC2 разверните RDS
* Опубликуйте приложение Notepad для группы IT
* У пользователей группы IT на рабочем столе должен присутствовать ярлык RDS приложения Notepad

**Настройка SRV2**

**Базовая настройка**

* переименуйте компьютер в SRV2;
* в качестве адреса SRV1 используйте второй возможный адрес из подсети 172.16.20.96/27;
* обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом WindowsFirewall должен быть включен для всех сетевых профилей;
* присоедините компьютер к домену *SPB.wse.*

**IIS**

* создайте сайт компании со стартовой страницей следующего содержания:
* *<html>*
* *Welcome to Saint-Petersburg!*
* *</html>;*
* сайт должен быть доступен по имени [*www.spb.wse*](http://www.spb.wse), по протоколам httphttps в обоих сетевых сегментах с использованием сертификатов, выданных DCA.

**Настройка CLI2**

**Базовая настройка**

* переименуйте компьютер в CLI2;
* обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом WindowsFirewall должен быть включен для всех сетевых профилей;
* присоедините компьютер к домену *SPB.wse.*
* запретите использование «спящего режима» таким образом, чтобы пользователи домена не могли изменить эту настройку без участия администратора домена;
* используйте компьютер для тестирования настроек в домене*SPB.wse.*

**Настройка R2**

**Базовая настройка**

* переименуйте компьютер в R2;
* задайте настройки сети следующим образом: для сетевого интерфейса, подключенного к коммутатору ISP, используйте адрес 200.100.100.1/30; для сетевого адреса в подсети *SPB.wse* используйте последний возможный адрес из используемого адресного пространства;
* обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом WindowsFirewall должен быть включен для всех сетевых профилей;
* присоедините компьютер к домену *SPB.wse.*

**Настройка RRAS**

* установите службу RRAS;
* настройте статические маршруты для связи с сетевым сегментом в Казани.

**Настройка R1**

**Базовая настройка**

* переименуйте компьютер в R1;
* задайте настройки сети следующим образом: для сетевого интерфейса, подключенного к подключенного к коммутатору ISP, используйте адрес 200.100.100.2/30; для сетевого адреса в подсети Kazan.wsr используйте последний возможный адрес из используемого адресного пространства;
* обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом WindowsFirewall должен быть включен для всех сетевых профилей;
* присоедините компьютер к домену Kazan.wsr.

**Настройка RRAS**

* установите службу RRAS;
* настройте статические маршруты для связи с сетевым сегментом в Санкт-Петербурге.