

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 компании, находящейся в городе Казань. В главном офисе вы управляете доменом skill39.wsr. Вам необходимо настроить сервисы в локальной сети головного офиса.

Компания, в которой вы работаете, хочет выйти на рынки северной Европы. Для этого она устанавливает партнерские отношения с одной из компаний, находящейся в Санкт-Петербурге. Вам нужно помочь администратору партнерской компании с настройкой своего домена (skill39.wsr), а потом настроить между доменами доверие.

Также Вам предстоит настроить канал связи между офисами с помощью статических маршрутов.

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, а также рекомендации по выделению ресурсов для виртуальных машин.

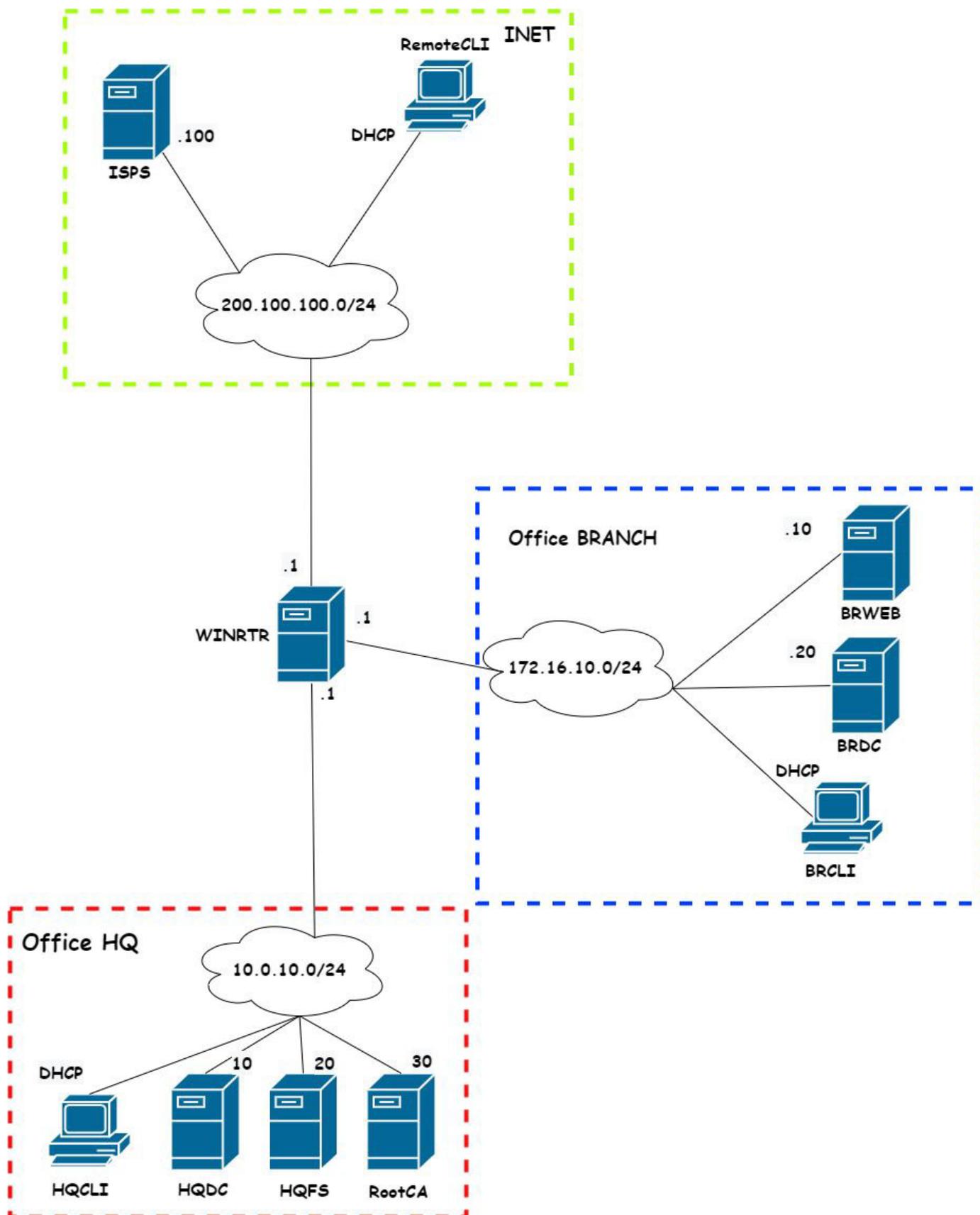
2. Программное обеспечение:

- Windows10.ADMX.

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.



Базовая настройка

- 1) Адреса и хостнеймы сконфигурированы заранее. Удостоверьтесь, что конфигурация является корректной
- 2) Обеспечьте возможность работы протокола icmp, windows firewall при этом должен быть включен
- 3) Обеспечьте ввод машин в домен
 - a) В домене skill39.wsr должны присутствовать машины BRDC, BRWEB, BRCLI, HQDC, HQCLI, HQFS, RemoteCLI
 - b) Остальные машины должны быть сконфигурированы для участия в рабочей группе NONDOMAIN
- 4) На всех машинах обоих доменов отключите режим сна
- 5) Проверьте работоспособность отключенного режима сна. **Без отключения режима сна проверка некоторых частей задания будет НЕВОЗМОЖНА.**

Конфигурация систем централизованного управления пользователями и компьютерами

- 1) На машине HQDC разверните домен skill39.wsr
 - a) Импортируйте пользователей из файла C:\Users.csv при помощи скрипта C:\import_users.ps1. В скрипте могут быть допущены ошибки. Устраните ошибки в скрипте и сохраните его с названием C:\import_users_v2.ps1. Создайте организационные единицы и группы внутри. В качестве названия используйте поле Job Title пользователя. Пользователи должны располагаться в корректных организационных подразделениях и должны быть добавлены в корректные группы
 - b) Для пользователей ИТ сконфигурируйте парольную политику со следующими параметрами:
 - i) Длина пароля не менее 10 символов
 - ii) Срок действия пароля 15 дней
 - iii) Пароль должен быть комплексным
 - iv) Парольная политика применяется только к группе ИТ без использования GPO
 - v) Сконфигурируйте название политики ITPassPolicy
 - c) Так же создайте в домене пользователя Secret с паролем P@ssw0rd. В качестве Job Title данного пользователя укажите Secret User. Пользователь должен располагаться в OU Users и не должен быть включен ни в какие группы, кроме групп по умолчанию. Так же сконфигурируйте параметр City для данного пользователя. Укажите значение Secret City
 - d) Синхронизируйте время с сервером ISPS. Все остальные машины должны синхронизировать время с HQDC
 - e) Поместите все клиентские машины в OU Clients, Все сервера в OU Servers. При необходимости создайте данные организационные подразделения
- 2) На машине BRDC разверните контроллер домена skill39.wsr только для чтения;
 - a) Разрешите репликацию паролей для группы competitors
 - b) Запретите репликацию паролей для группы ИТ и администраторов домена

- 3) Сконфигурируйте групповые политики в домене skill39.wsr
 - a) запретите анимацию при первом входе пользователей в систему на всех клиентских компьютерах домена;
 - b) члены группы IT должны быть членами группы локальных администраторов на всех клиентских компьютерах домена;
 - c) Сконфигурируйте стартовую страницу www.skill39.wsr для всех клиентских машин, в браузерах Internet Explorer и Microsoft edge.
 - d) для каждого пользователя, члена группы IT, создайте автоматически подключаемую в качестве диска U:\ домашнюю папку внутри папки по адресу SRV1→d:\shares\IT. Папки должны создаваться динамически, при первом входе пользователя в систему
 - e) На всех клиентских компьютерах домена все пользователи должны видеть ярлык приложения калькулятор
 - f) Сконфигурируйте заставку рабочего стола. Заставка должна обозначать принадлежность машины к офису, например в офисе HQ заставка должна содержать слово HQ, в офисе Branch, слово Branch.

- 4) Введите машину RemoteCLI в домен при помощи функции оффлайн присоединения к домену. Файл для присоединения сохраните в корне диска C:\

Конфигурация сетевой инфраструктуры

- 1) На сервере HQDC сконфигурируйте DHCP сервер для подсети офисов HQ и Branch
 - a) в качестве диапазона выдаваемых адресов используйте все незанятые серверами адреса в подсети
 - b) Обеспечьте отказоустойчивость DHCP между серверами HQDC и HQFS
 - i) При выходе из строя DHCP сервера на HQDC в работу должен вступать сервер на HQFS. Все остальное время DHCP сервер на HQFS должен находиться в режиме простоя
 - ii) Обеспечьте автоматическое переключение между серверами не более чем за одну минуту
 - c) Сконфигурируйте дополнительные опции (адреса DNS серверов и шлюз по умолчанию)

- 2) На машине WINRTR сконфигурируйте DHCP Relay

- 3) Сконфигурируйте DNS для домена skill39.wsr
 - a) Обеспечьте возможность разрешения обратных имен
 - b) Запретите использование нелатинских символов

- c) Добавьте запись www.skill39.wsr таким образом, чтобы машины из офиса Branch обращались к BRWEB, а машины из офиса HQ к HQFS.

- 4) На сервере ISP сконфигурируйте эмуляцию соединения с интернетом. При проверке наличия соединения с интернетом любой сервер и любой клиент любого офиса должны давать положительный ответ. Все машины всех офисов должны считать, что они находятся в интернете

Конфигурация служб хранения данных

- 1) Из дополнительных жестких дисков создайте массив RAID1 и присвойте ему букву D:
- 2) создайте общие папки для подразделений по адресу SRV1→d:\shares\departments.
 - a) Просматривать и редактировать файлы в папках могут только члены соответствующей группы.
- 3) обеспечьте привязку общей папки подразделения к соответствующей группе пользователей в качестве диска G:\.
- 4) пользователи домена при обращении к общим папкам, на доступ которым у них нет разрешений, должны получать вместо стандартного уведомления следующего вида: «You do not have permissions to use this path - [путь к папке]! Do not try it again!».
- 5) установите максимальный размер в 2 Gb для каждой домашней папки пользователя (U:\);
- 6) запретите хранение в домашних папках пользователей файлов с расширениями .mp3 и .wav; учтите, что файлы остальных типов пользователи вправе хранить в домашних папках.
- 7) для хранения профилей пользователей в домене skill39.wsr используйте общую папку по адресу HQFS→D:\Shares\profiles;
- 8) 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.
- 9) Создайте каталог D:\Shares\Secret. Обеспечьте возможность доступа к данному каталогу только пользователям, Job Title которых установлен как Secret User, и параметр City -- Secret City

Конфигурация веб- и почтовых служб

- 1) На HQFS создайте сайт www.skill39.wsr
 - a) При переходе на сайт должна быть видна надпись Welcome to Head-Quater!
 - b) Сайт должен быть доступен по https
 - i) Используйте сертификат, выданный HQDC
 - ii) При переходе на сайт не должно возникать ошибок, связанных с сертификатами
 - iii) Настройте автоматическое перенаправление http -> https

- c) Обеспечьте возможность доступа на сайт по имени www.skill39.wsr с клиентских машин обоих офисов
- 2) На BRWEB создайте сайт www.skill39.wsr
- a) При переходе на сайт должна быть видна надпись Welcome to Branch!!
 - b) Сайт должен быть доступен по https
 - i) Используйте сертификат, выданный HQDC
 - ii) При переходе на сайт не должно возникать ошибок, связанных с сертификатами
 - iii) Настройте автоматическое перенаправление http -> https
 - c) Обеспечьте возможность доступа на сайт по имени www.skill39.wsr с клиентских машин обоих офисов

Конфигурация параметров безопасности и служб аутентификации

- 1) Сконфигурируйте корневой недоменный центр сертификации на машине RootCA
 - a) имя центра сертификации – HQRootCA
 - b) срок действия сертификата – 8 лет;
 - c) Сконфигурируйте корректные CRL и AIA
 - d) Подпишите сертификат для подчиненного центра сертификации и отключите сетевой адаптер средствами операционной системы
- 2) Сконфигурируйте подчиненный доменный центр сертификации на машине HQDC
 - a) Имя центра сертификации -- HQ Sub
 - b) Срок действия 5 лет
 - c) Сконфигурируйте корректные CRL и AIA
 - d) Создайте шаблон для группы IT. В качестве названия шаблон укажите ITUsers, Subject Name = Common Name, обеспечьте автоматическую выдачу данного сертификата только группе IT
 - e) Создайте шаблон Clients для всех клиентских компьютеров домена. В качестве названия шаблона укажите Clients, Subject Name = Common Name, обеспечьте автоматическую выдачу данного сертификата только для клиентских ПК.
- 3) Все машины офисов HQ и Branch должны доверять сертификатам обоих центров сертификации

Настройка маршрутизации

- 1) Сконфигурируйте WINRTR для достижения полной связанности между всеми офисами и интернетом.
- 2) Средствами Windows Firewall запретите icmp трафик из сети интернет до сети любого из офисов. Весь остальной трафик должен быть разрешен.

Конфигурация служб мониторинга, резервного копирования, журналирования

В данном модуле настройка не предусмотрена

Конфигурация служб удаленного доступа

В данном модуле настройка не предусмотрена

Настройка подключений к глобальным сетям

В данном модуле настройка не предусмотрена

Конфигурация подсистемы телефонной связи

В данном модуле настройка не предусмотрена

Виртуализация

В данном модуле настройка не предусмотрена

СУБД

В данном модуле настройка не предусмотрена

Автоматизация администрирования

В данном модуле настройка не предусмотрена

Конфигурация и установка системы

В данном модуле настройка не предусмотрена

ПРИЛОЖЕНИЕ

ВВЕДЕНИЕ. Настоящие дополнения содержат описание вида предустановок, описание используемых операционных систем, рекомендации по выделению ресурсов для виртуальных машин.

ОПИСАНИЕ ПРЕДУСТАНОВОК

1. На SRV1 должно быть установлено четыре (или пять) жестких диска: один не менее – 25 Gb, три (четыре) – 5 Gb .
2. Все остальные жесткие диски всех виртуальных машин должны иметь объем не менее 25 Gb.
3. После установки на всех виртуальных машинах необходимо выполнить сценарий *Sysprep* с опцией *generalize*.
4. После выполнения работ перезагрузка стендов остается на усмотрение экспертов.

ОПИСАНИЕ ПРИМЕНЯЕМЫХ ОПЕРАЦИОННЫХ СИСТЕМ

Имя компьютера	Операционная система
HQDC	Windows Server 2019 GUI
HQCLI	Windows 10 Enterprise
HQFS	Windows Server 2019 Core
BRDC	Windows 2019 GUI
ISPS	Windows 2019 GUI
RootCA	Windows Server 2019 Core
BRWEB	Windows Server 2019 Core
BRCLI	Windows 10 Enterprise
WINRTR	Windows Server 2019 GUI
RemoteCLI	Windows 10 Enterprise

Задание протестировано на 100% следующих сборках ОС:

- Server 2019 – 17763.379.190312-0539;
- Win 10 Ent – 18362.30.190401-1528.

***РЕКОМЕНДАЦИИ ПО ВЫДЕЛЕНИЮ ОПЕРАТИВНОЙ ПАМЯТИ ВИРТУАЛЬНЫХ
МАШИН***

- Windows Server 2019 Core: минимум – 1 Gb, рекомендовано – 1,5 Gb;
- Windows Server 2019 GUI: минимум – 1,5 Gb, рекомендовано – 2 Gb;
- Windows 10 Enterprise: минимум – 1,5 Gb, рекомендовано – 2 Gb.