КОМПЕТЕНЦИЯ «СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

КОНКУРСНОЕ ЗАДАНИЕ

МОДУЛЬ А: ПУСКО-НАЛАДКА ИНФРАСТРУКТУРЫ НА ОСНОВЕ ОС СЕМЕЙСТВА LINUX

Разработано экспертами WSR:
Фучко М.М.
Мухаметовым Р.А.

Дата: 06.09.17
Версия: 1

СОДЕРЖАНИЕ

Данное конкурсное задание состоит из следующих документов\файлов:
1. RC1718_TP39_Module-A_RU.docx
2. RC1718_TP39_Module-A-Topology_RU.vsd

ВВЕДЕНИЕ

Умение работать с системами на основе открытого исходного кода становится все более важным навыком для тех, кто желает построить успешную карьеру в ИТ. Данное конкурсное 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 КОНКУРСНОГО ЗАДАНИЯ

Данное конкурсное задание разработано с использованием различных открытых технологий, с которыми вы должны быть знакомы по сертификационным курсам LPIC и Red Hat. Задания поделены на следующие секции:

- Базовая конфигурация
- Конфигурация сетевой инфраструктуры
- Службы централизованного управления и журналирования
- Конфигурация служб удаленного доступа
- Конфигурация служб хранения данных
- Конфигурация параметров безопасности и служб аутентификации

Секции независимы друг от друга, но вместе они образуют достаточно сложную инфраструктуру. Некоторые задания достаточно просты и понятны, некоторые могут быть неочевидными. Можно заметить, что некоторые технологии должны работать в связке или поверх других технологий. Например, динамическая маршрутизация должна выполнять поверх настроенного между организациями туннеля. Важно понимать, что если вам не удалось настроить полностью технологический стек, то это не означает что работа не будет оценена. Например, для удаленного доступа необходимо сконфигурировать IPsec-туннель, внутри которого организовать GRE-туннель. Если, например, вам не удалось настроить IPsec, но вы смогли настроить GRE то вы все еще получите баллы за организацию удаленного доступа.

ИНСТРУКЦИИ ДЛЯ УЧАСТНИКА

В первую очередь необходимо прочитать задание полностью. Следует обратить внимание, что задание составлено не в хронологическом порядке. Некоторые секции могут потребовать действий из других секций, которые изложены ниже. Например, задание 6 в секции «Базовая конфигурация» предписывает автоматизировать удаленный доступ, который, разумеется, не будет работать без предварительной конфигурации, изложенной в секции «Маршрутизация и удаленный доступ». 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.

Доступ ко всем виртуальным машинам настроен по аккаунту root:toor.

Виртуальная машина ISP преднастроена. Управляющий доступ участника к данной виртуальной машине для выполнения задания не предусмотрен.

НЕОБХОДИМОЕ ОБОРУДОВАНИЕ, ПРИБОРЫ, ПО И МАТЕРИАЛЫ

Ожидается, что конкурсное задание выполнимо Участником с привлечением оборудования и материалов, указанных в Инфраструктурном Листе.

СХЕМА ОЦЕНКИ

Каждый субкритерий имеет приблизительно одинаковый вес. Пункты внутри каждого критерия имеют разный вес, в зависимости от сложности пункта и количества пунктов в субкритерии.

Схема оценка построена таким образом, чтобы каждый пункт оценивался только один раз. Например, в секции «Базовая конфигурация» предписывается настроить имена для всех устройств, однако этот пункт будет проверен только на одном устройстве и оценен только 1 раз. Одинаковые пункты могут быть проверены и оценены больше чем 1 раз, если для их выполнения применяются разные настройки или они выполняются на разных классах устройств.

Подробное описание методики проверки должно быть разработано экспертами, принимающими участие в оценке конкурсного задания чемпионата, и вынесено в отдельный документ. Данный документ, как и схема оценки, является объектом внесения 30% изменений.

Конфигурация хостов

1) Настройте имена хостов в соответствии с **Таблицей 1.**
2) Установите следующее ПО на **ВСЕ** хосты:
    a. Пакет tcpdump
    b. Клиент ftp
    c. Клиент lftp
    d. Пакет net-tools
    e. Редактор vim
    f. lynx
    g. dhclient
    h. bind-utils
    i. nfs-utils
3) На хостах RTR, CLI-P, SRV, CLI-N, CLI-C сформируйте файл **/etc/hosts** в соответствии с **Таблицей 1** (кроме адреса хоста CLI-P). Данный файл будет применяться во время проверки в случае недоступности DNS-сервисов. Проверка по IP-адресам выполняться не будет. В случае корректной работы DNS-сервисов ответы DNS должны иметь более высокий приоритет.

Конфигурация сетевой инфраструктуры

1) Настройте IP-адресацию на ВСЕХ хостах в соответствии с **Таблицей 1.**
2) Настройте сервер протокола динамической конфигурации хостов для машин CLI-C и CLI-P
    a. В качестве DHCP-сервера используйте машину SRV
    b. Используйте пул адресов 172.16.100.60 — 172.16.100.75
    c. Используете адрес машины SRV в качестве адреса DNS-сервера
    d. Настройте DHCP-сервер таким образом, чтобы машина CLI-C всегда получала фиксированный IP-адрес в соответствии с **Таблицей 1**
    e. В качестве шлюза по умолчанию используйте адрес интерфейса RTR в локальной сети
    f. Используйте DNS-суффикс **house.mad**
    g. DNS-записи типа A соответствующего хоста должны обновляться при получении им адреса от DHCP-сервера.
3) На машине SRV настройте службу разрешения доменных имен
    a. Сервер должен обслуживать зону **house.mad**
    b. Сопоставление имен организовать в соответствии с **Таблицей 2**
    c. Запросы, которые выходят за рамки зоны **house.mad** должны пересылаться DNS-серверу ISP
    d. Реализуйте поддержку разрешения обратной зоны.
    e. Файлы зон располагать в **/opt/dns/**
4) На RTR настройте интернет-шлюз для организации коллективного доступа в интернет. Настройте трансляцию сетевых адресов из внутренней сети в адрес внешнего интерфейса.

Службы централизованного управления и журналирования

1) На SRV разверните RADIUS-сервер с использованием пакета freeradius для организации централизованного управления учетными записями

a. Создайте учетные записи user01 … user50
b. Учетные записи должны храниться в локальном файле **/etc/passwd**
c. Настройте RTR, CLI-C и CLI-P в качестве клиентов RADIUS-сервера.

2) На SRV организуйте централизованный сбор журналов с хостов CLI-C, CLI-P, RTR и SRV
   a. Журналы должны храниться в директории **/opt/logs/**
   b. Журналирование должно производится в соответствии с **Таблицей 3.**

Конфигурация служб удаленного доступа

1) На RTR настройте сервер удаленного доступа на основе технологии OpenVPN:
   a. В качестве сервера выступает RTR
   b. Параметры туннеля
      i. Устройство TUN
      ii. Протокол UDP
      iii. Применяется сжатие
      iv. Порт сервера 1122
   c. Ключевая информация должна быть сгенерирована на RTR
   d. В качестве адресного пространства подключаемых клиентов использовать сеть 5.5.5.0/24
      i. Обеспечить присвоение закрепленных адресов в соотвествии с **Таблицей 1.**
   e. Хранение всей необходимой (кроме конфигурационных файлов) информации организовать в **/opt/vpn**
2) На CLI-N настройте клиент удаленного доступа на основе технологии OpenVPN:
   a. Запуск удаленного подключения должен выполняться скриптом **start_vpn**
      i. Автоматизация отключения VPN-туннеля не требуется
      ii. Скрипт должен располагаться в **/opt/vpn.**
      iii. Скрипт должен вызываться из любого каталога без указания пути
      iv. Используйте следующий путь для расположения файла скрипта **/opt/vpn/start_vpn.sh**
3) На RTR настройте удаленный доступ по протоколу SSH:
   a. Доступ ограничен пользователями **ssh_p** и **ssh_c**
      i. В качестве пароля использовать **ssh_pass**
   b. SSH-сервер должен работать на порту **1022**
4) На CLI-N настройте клиент удаленного доступа SSH:
   a. Доступ к серверу RTR должен происходить автоматически по правильному порту, без его явного указания номера порта в команде подключения
   b. Для других серверов по умолчанию должен использоваться порт **22**
   c. Доступ к RTR под учетной записью **ssh_p** должен происходить с помощью аутентификации на основе открытых ключей.

Конфигурация служб хранения данных

1) На SRV настройте сервер файлового хранилища на основе технологии NFS:
   a. В качестве хранилища используется каталог **/opt/nfs**
   b. Доступ организуется для чтения и записи

2) Настройте автоматическое монтирование NFS-хранилища для клиентов CLI-C, CLI-P и CLI-N:
   a. Используйте DNS-имя NFS-сервера
   b. Используйте **/opt/nfs** в качестве пути для монтирования
   c. Клиенты CLI-C и CLI-P монтируют NFS-каталог при запуске ОС
   d. Клиент CLI-N монтирует NFS-каталог после установления VPN-туннеля с RTR
3) На SRV настройте FTP-сервер для доступа к файловому хранилищу
   a. Обеспечьте доступ для клиента CLI-N с использованием стандартных портов протокола FTP через внешний интерфейс маршрутизатора RTR
   b. Корень FTP-сервера должен располагаться в **/opt/nfs**
   c. Доступ должен быть ограничен пользователем ftpuser:ftppass с правами на чтение и запись

Конфигурация параметров безопасности и служб аутентификации

1) Настройте межсетевой экран на RTR
   a. Запретите прямое попадание трафика из сети **First Mile** в **Internal**
   b. Разрешите удаленные подключения с использованием OpenVPN на внешний интерфейс маршрутизатора RTR
   c. Разрешите SSH подключения на соответствующий порт
   d. Разрешите подключения по FTP в соответствии с заданием
   e. Для VPN-клиентов должен быть предоставлен полный доступ к сети **Internal**
   f. Остальные сервисы следует запретить.

Таблица 1. Адресация

Сеть	**Хосты**	**Адреса (/24)**
Internal	CLI-P CLI-C RTR SRV	DHCP 172.16.100.50 (DHCP) 172.16.100.1 172.16.100.100
Last Mile	ISP RTR	10.10.10.1 10.10.10.10
First Mile	ISP CLI-N	20.20.20.1 20.20.20.10
VPN	RTR CLI-N	5.5.5.1 5.5.5.50

Таблица 2. DNS-имена

Хост	**DNS-имя**
CLI-P	A:cli-p.house.mad CNAME: mom.house.mad CNAME: dad.house.mad
CLI-C	A:cli-c.house.mad CNAME: son.house.mad
SRV	A:srv.house.mad

	CNAME: server.house.mad CNAME: center.house.mad
RTR	A:rtr.house.mad CNAME: fw.house.mad

Таблица 3. Правила журналирования

Источник	**Уровень журнала**	**Файл**
Все хосты	critical и выше	/opt/logs/<HOSTNAME>/crit.log
SRV	auth.*	/opt/logs/<HOSTNAME>/auth.log
RTR	*.err	/opt/logs/<HOSTNAME>/error.log
Все кроме RTR	*.err	/opt/logs/err.log

*<HOSTNAME> - название директории для журналируемого хоста

**В директории /opt/logs/ не должно быть файлов, кроме тех, которые указаны в таблице

ДИАГРАММА ВИРТУАЛЬНОЙ СЕТИ