**Модуль А: «Пусконаладка инфраструктуры на основе OC семейства**

**Linux»** (или аналог)

**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 Экзаменационное 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 ЭКЗАМЕНАЦИОННОГО ЗАДАНИЯ**

Данное Экзаменационное 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 веб-служб
* 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 выполняться 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 настроить 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.

**ИНСТРУКЦИИДЛЯ 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. 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**.

**Если Вам требуется установить пароль, (и он не указан в задании) используйте: “P@ssw0rd”**.

**Виртуальная машина ISP преднастроена. Управляющий доступ участника к данной виртуальной машине для выполнения задания не предусмотрен. При попытке его сброса возникнут проблемы.**

Организация LEFT включает виртуальные машины: L-SRV, L-FW, L-RTR-A, L-RTR-B, L-CLI-A, L-CLI-B.

Организация RIGHT включает виртуальные машины: R-SRV, R-FW, R-RTR, R-CLI.

**НЕОБХОДИМОЕ ОБОРУДОВАНИЕ, ПРИБОРЫ, ПО И МАТЕРИАЛЫ**

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

В качестве системной ОС в организации **LEFT** используется **Debian**

В качестве системной ОС в организации **RIGHT** используется **CentOS**

Вамдоступендиск CentOS-7-x86\_64-Everything-1810.iso

Вам доступен диск debian-10.0.0-amd64-BD-1.iso

Вам доступен диск debian-10.0.0-amd64-BD-2.iso

Вам доступен диск debian-10.0.0-amd64-BD-3.iso

Вам доступен диск debian-10.0.0-amd64-BD-4.iso

Вам доступен диск Additional.iso, на котором располагаются недостающие RPM пакеты

**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.**

**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, принимавшими участие в оценке экзаменационного задания, 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**Диаграммой.**
2. Установите следующее ПО на**ВСЕ**виртуальные машины:
	1. **Tcpdump**
	2. **Net-tools**
	3. **Curl**
	4. **Vim**
	5. **Lynx**
	6. **Dhclient**
	7. **Bind-utils**
	8. **Nfs-utils**
	9. **Cifs-utils**
	10. **Sshpass**
3. На хостах сформируйте файл **/etc/hosts** в соответствии с

**Диаграммой** (кроме адреса хоста L-CLI-A). Данный файл будет применяться

во время проверки в случае недоступности DNS-сервисов. Проверка по IPадресам выполняться не будет.

1. В случае корректной работы DNS-сервисов ответы DNS должны иметь более высокий приоритет.
2. ***Все хосты должны быть доступны аккаунту root по SSH на стандартном (22) порту***

**Конфигурация сетевой инфраструктуры**

1. Настройте IP-адресацию на ВСЕХ хостах в соответствии с Диаграммой.
2. Настройте сервер протокола динамической конфигурации хостов для L-CLI-A и L-CLI-B
3. В качестве DHCP-сервера организации LEFT используйте L-RTR-A.
	1. Используйте пул адресов 172.16.100.65 — 172.16.100.75 для сети L-

RTR-A

* 1. Используйте пул адресов 172.16.200.65 — 172.16.200.75 для сети L-

RTR-B

1. Используете адрес L-SRV в качестве адреса DNS-сервера.
2. Настройте DHCP-сервер таким образом, чтобы L-CLI-B всегда получал фиксированный IP-адрес в соответствии с Диаграммой.
	1. В качестве шлюза по умолчанию используйте адрес интерфейса

соответствующего маршрутизатора в локальной сети.

1. Используйте DNS-суффикс skill39.wsr.
	1. DNS-записи типа A и PTR соответствующего хоста должны

обновляться при получении им адреса от DHCP-сервера.

1. На L-SRV настройте службу разрешения доменных имен
	1. Сервер должен обслуживать зону skill39.wsr.
	2. Сопоставление имен организовать в соответствии с Таблицей 1.
	3. Запросы, которые выходят за рамки зоны skill39.wsr должны

пересылаться DNS-серверу ISP. Для проверки используйте доменное имя ya.ru.

* 1. Реализуйте поддержку разрешения обратной зоны.
	2. Файлы зон располагать в /opt/dns/
	3. Запретите клиентам из сети 31.33.7.0/24 обращаться к этой зоне
1. На L-FW и R-FW настройте интернет-шлюзы для организации коллективного доступа в Интернет.
	* 1. Настройте трансляцию сетевых адресов из внутренней сети в адрес

внешнего интерфейса.

* + 1. Организуйте доступность сервиса DNS на L-SRV по внешнему

адресу L-FW.

* + 1. Сервер L-FW должен перенаправлять внешние DNS запросы от OUT-CLI на L-SRV. www.skill39.wsr должен преобразовываться во внешний адрес R-FW.
1. На L-FW реализуйте синхронизацию времени по протоколу NTP на основе сервера Chrony.
2. Часовой пояс всех хостов: MSK.
3. Разрешается синхронизация только для клиентов сети LEFT и RIGHT.
4. В случае, если отклонение от сервера составляет более двух тысяч секунд - машина выполняет жесткуюсинхронизацию времени.

**Службы централизованного управления и журналирования**

1. Разверните LDAP-сервер для организации централизованного управления учетными записями
	1. В качестве сервера выступает L-SRV.
	2. Учетные записи создать в соответствии с Таблицей 2.
	3. Группы(LDAP) и пользователей создать в соответствии с Таблицей

2.

* 1. L-CLI-A, L-SRV и L-CLI-B должны аутентифицироваться через LDAP.
1. На L-SRV организуйте централизованный сбор журналов с хостов L-FW, L-SRV.
	1. Журналы должны храниться в директории /opt/logs/.
	2. Журналирование должно производится в соответствии с Таблицей 3

**Конфигурация служб удаленного доступа**

1. На L-FW настройте сервер удаленного доступа на основе технологии OpenVPN:
	1. В качестве сервера выступает L-FW
	2. Параметры туннеля.
		1. Устройство TUN. ii) Протокол UDP.
		2. Применяется сжатие.
		3. Порт сервера 1122.
	3. Ключевая информация должна быть сгенерирована на R-FW.
	4. В качестве адресного пространства подключаемых клиентов использовать сеть 5.5.5.0/27.
	5. Хранение всей необходимой (кроме конфигурационных файлов)

информации организовать в /opt/vpn.

* 1. Подключившийся клиент должен быть автоматически сконфигурирован на использование DNS-инфраструктуры предприятия.
1. На OUT-CLI настройте клиент удаленного доступа на основе технологии OpenVPN:
	1. Запуск удаленного подключения должен выполняться скриптом start\_vpn.sh
		1. Отключение VPN-туннеля должно выполняться скриптом stop\_vpn.sh.
		2. Скрипты должны располагаться в /opt/vpn.
		3. Скрипты должны вызываться из любого каталога без указания

пути.

* + 1. Используйте следующий каталог для расположения файлов скриптов /opt/vpn/.
1. Настройте защищенный канал передачи данных между L-FW и RFW с помощью технологии IPSEC:
	1. Параметры политики первой фазы IPSec:
		1. Проверка целостности SHA-1
		2. Шифрование 3DES iii) ГруппаДиффи-Хеллмана — 14 (2048) iv) Аутентификация по общему ключу WSR-2019
	2. Параметры преобразования трафика для второй фазы IPSec:
		1. Протокол ESP ii) Шифрование AES iii) Проверка целостности SHA-2
	3. В качестве трафика, разрешенного к передаче через IPsec-туннель,

должен быть указан только GRE-трафик между L-FW и R-FW 4) Настройте GRE-туннель между L-FW и R-FW:

a) Используйте следующую адресацию внутри GRE-туннеля:

* + 1. L-FW: 10.5.5.1/30 ii) R-FW: 10.5.5.2/30
1. Настройте динамическую маршрутизацию по протоколу OSPF с использованием пакета FRR:
	1. Анонсируйте все сети, необходимые для достижения полной

связности.

* 1. Применение статических маршрутов не допускается.
	2. В обмене маршрутной информацией участвуют L-RTR-A, L-RTR-B, R-RTR, L-FW и R-FW.
	3. Соседство и обмен маршрутной информацией между L-FW и R-FW

должно осуществляться исключительно через настроенный GRE-туннель.

* 1. Анонсируйте сети локальных интерфейсов L-RTR-A и L-RTR-B.
1. На R-SRV настройте удаленный доступ по протоколу SSH:
	1. Доступ ограничен пользователями ssh\_p, root и sshuser

i) В качестве пароля пользователь (кроме root) использовать ssh\_pass. ii) root использует стандартный пароль

* 1. SSH-сервер должен работать на порту 22
1. На CLI-2L сконфигурируйте SSH клиент.
	* 1. Автоматическое подключение к порту 2222 сервера R-FW
		2. Сервер R-FW выполнять перенаправление на 22 порт сервера

R-SRV iii) Сконфигурируйте аутентификацию при помощи ключей для пользователя sshuser.

 iv) Обеспечьте возможность входа на сервер с использованием

алиасов R-SRV.skill39.wsr.

**Конфигурация веб-служб**

1. На R-SRV установите инастройте веб-сервер NGINX:
	1. Настройте веб-сайт для внешнего пользования [www.skill39.wsr.](http://www.skill39.wsr/)
		1. Используйте директорию /var/www/html/out.
		2. Используйте порт 80.
		3. Сайт предоставляет доступ к двум файлам.
2. Документ index.html должен содержать:
	1. “Hello, www.skill39.wsr is here!”

**Конфигурация служб хранения данных**

1. Реализуйте синхронизацию каталогов на основе демона rsyncd.
	1. В качестве сервера синхронизации используется L-SRV.
		1. Для работы синхронизации создайте специального пользователя mrsync
2. В качестве пароля используйте toor.
	1. Домашний каталог данного пользователя должен быть расположен в

/opt/sync/. Данный каталог используйте как каталог синхронизации

* 1. Домашний каталог не должен содержать никакой посторонней

информации.

* 1. Для выполнения синхронизации создайте rsync-пользователя sync c

паролем parol666.

* 1. Подключение к rsyncd должны быть разрешены исключительно от

клиентов L-CLI-A и L-CLI-B

1. В качестве клиентов используются L-CLI-A и L-CLI-B
	1. Синхронизируемый каталог располагается по адресу /root/sync/
	2. Каталоги должны быть зеркально идентичны по содержимому.
	3. Реализуйте синхронизацию в виде скрипта:
		1. Скрипт находится по адресу /root/sync.sh
		2. Автоматизация скрипта реализована средствами cron пользователя root.
		3. Выполнение производится каждую минуту.

**Конфигурация параметров безопасности и служб аутентификации** 1) Настройте CA на R-FW, используя OpenSSL.

* 1. Используйте /etc/ca в качествекорневой директории CA
	2. Атрибуты CA должны быть следующими:
		1. Страна RU
		2. Организация WorldSkills Russia iii) CN должен быть установлен как WSR CA
	3. Создайте корневой сертификат CA
	4. Все клиентские операционные системы должны доверять CA

 2) Настройте межсетевой экран iptables на L-FW и firewalld на R-FW

1. Запретите прямое попадание трафика из сетей в Internal
2. Разрешите удаленные подключения с использованием OpenVPN на

внешний интерфейс маршрутизатора L-FW

1. Разрешите необходимый трафик для создания IPSec и GRE туннелей

между организациями

1. Разрешите SSH подключения на соответствующий порт
2. Для VPN-клиентов должен быть предоставлен полный доступ к сети

Internal

1. Разрешите необходимый трафик к серверам L-SRV и R-SRV для

работы настроенных сервисов.

1. Остальные сервисы следует запретить.
2. В отношении входящих (из внешней сети) ICMP запросов поступать

по своему усмотрению

**Таблица 1** – DNS-имена







\*<HOSTNAME> - название директории для журналируемого хоста

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



**ДИАГРАММА ВИРТУАЛЬНОЙ СЕТИ**



|  |  |  |
| --- | --- | --- |
| Sub CriteriaName or Description | Aspect - Description | MaxMark |
| Basic configuration and Network Services |   |   |
|   | Hostnames | 0,1 |
|   | IPv4 connectivity | 0,2 |
|   | Software installation | 0,2 |
|   | Local hostname table | 0,2 |
|   | Name lookup order | 0,2 |
|   | DHCP-A: Basic Operation | 0,3 |
|   | DHCP-A: Additional Parameters | 0,3 |
|   | DHCP-B: Basic Operation | 0,3 |
|  | DHCP-B: Additional Parameters | 0,3 |
|   | DNS: Forward zone | 0,3 |
|   | DNS: Reverse zone | 0,3 |
|   | DNS: ISP Forwarders | 0,3 |
|   | DNS: Secondary DNS | 0,3 |
|   | DNS: Dynamic DNS | 0,5 |
|   | Internet Gateway (Dynamic NAT)-LEFT | 0,3 |
|   | Internet Gateway (Dynamic NAT)-RIGHT | 0,3 |
|   | DNS-Proxy | 0,1 |
| Centralized Management |   |   |
|   | LDAP: Users, Groups and OU | 0,5 |
|   | LDAP: Clients authentication | 0,5 |
|   | LDAP: Logon restriction | 0,5 |
|   | Syslog: L-SRV | 0,4 |
|   | Syslog: L-FW | 0,4 |
| Routing & Remote Access |   |   |
|   | RA: OpenVPN basic | 0,5 |
|   | RA: VPN Clients have full access to LEFT and RIGHT LANs | 0,2 |
|   | IPSEC + GRE | 0,4 |
|   | GRE Tunnel Cinnectivity | 0,3 |
|   | FRR: Neigbours  | 0,3 |
|   | FRR: Local interfaces | 0,3 |
|   | FRR: Passive interfaces | 0,3 |
|   | SSH: Users | 0,2 |
|   | SSH: Client’s Default Port | 0,2 |
|   | SSH: Key authentication | 0,2 |
| Web services, Storage and File sharing |   |   |
|   | Apache: Port, PHP | 0,4 |
|   | NGINX: Access | 0,2 |
|   | NGINX: Reverse SSL proxy | 0,3 |
|   | NGINX: Redirection | 0,3 |
|   | NGINX: Passive check | 0,3 |
|   | NGINX: Caching | 0,3 |
|   | rsync: L-SRV configuration | 0,3 |
|   | rsync: Client sync  | 0,4 |
| Security |   |   |
|   | OpenSSL: CA | 0,5 |
|   | Certificate Attributes | 0,5 |
|   | IPTables: Block traffic | 0,3 |
|   | IPTables: Port forwarding | 0,3 |
|   | IPTables: Allow only nessesary traffic | 0,3 |
|   | Firewalld: Block traffic | 0,3 |
|   | Firewalld: Port forwarding | 0,3 |
|   | Firewalld: Allow only nessesary traffic | 0,3 |

Перевод баллов в оценку

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Оценка  | «2» | «3» | «4» | «5» |
| Количество баллов  | < 1,19 | 1,2 – 2,39 | 2,4 – 4,19 | ≥ 4,2 |