Update TestProject_AS21.md
Денис Дюгуров authored 1 day ago

TestProject_AS21.md 63.2 KB

Конкурсное задание

Компетенция «Сетевое и системное администрирование» Версия 1.1 от 21.07.2021

Общее время на выполнение конкурсного задания: **15** часов

ВВЕДЕНИЕ

209a81cf

Данное конкурсное задание содержит множество задач, основанных на опыте реальной эксплуатации информационных систем в сфере интеграции и аутсорсинга корпоративных вычислительных сетей.

ОПИСАНИЕ КОНКУРСНОГО ЗАДАНИЯ

Данное конкурсное задание разработано с использованием различных технологий, входящих в сертификационные программы LPIC, Red Hat, CCNA, CCNP, MCSA.

Совместное использование этих технологий представляет собой достаточно сложную инфраструктуру. Требования в задании представлены в общем виде, конкретный метод выполнения и технологии, необходимые для его реализации, вы вправе выбрать самостоятельно с учётом указанных в задании требований.

Можно заметить, что многие технологии должны работать в связке или поверх других. 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 вам не удалось настроить IPsec, но вы смогли настроить GRE, то вы все еще получите баллы за организацию удаленного доступа.

Главной задачей является получение работоспособной системы в том или ином виде, а также её ежедневная доработка и улучшение. **СХЕМА ОЦЕНКИ**

Оцениваемые аспекты имеют разный вес в зависимости от их сложности. Схема оценки построена так, чтобы каждый аспект оценивался только один раз. Например, в задании предписывается настроить корректные имена для всех устройств, данный аспект будет оценен только один раз и повторная оценка данного аспекта проводится не будет. 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.

Следует также учесть, что для данного задания возможна автоматическая оценка результатов.

Проверка будет производиться с использованием доменных имен. Проверка по IP-адресам выполняться не будет. НЕОБХОДИМОЕ ОБОРУДОВАНИЕ, ПРИБОРЫ, ПО И МАТЕРИАЛЫ

Конкурсное задание выполнимо в полном объеме с привлечением оборудования и материалов, указанных в Инфраструктурном листе. **ИНСТРУКЦИИ ДЛЯ УЧАСТНИКА**

В первую очередь рекомендуется прочитать задание полностью. Следует обратить внимание, что задание составлено не в строгом хронологическом порядке. Для выполнения некоторых пунктов задания может потребоваться выполнение действий из других пунктов, которые изложены в задании ниже. Таким образом, порядок выполнения задания и распределение временных затрат определяется участниками самостоятельно.

Конкурсное задание имеет сквозную структуру, и предполагается, что вы продолжаете его выполнение на следующий день с того момента, на котором остановились в предыдущий. Вам доступно полное задание на все конкурсные дни.

Рекомендуется тщательно проверять результаты своей работы. В частности, рекомендуется убедиться в полной работоспособности служб DNS для клиентских устройств.

Также учтите, что в конце третьего дня все виртуальные машины должны быть выключены, а затем участник сможет их включить в желаемом порядке. Сетевое оборудование будет перезагружено по питанию. Также рабочее место может быть выключено в ночное время.

IP адресация в топологии выбирается на ваше усмотрение, за исключением адресов, предоставляемых провайдерами. Например, для сервера DC в сети WINA вы может использовать адреса 172.16.10.156 или 192.168.0.12. Сохранение существующей адресации не требуется и не оценивается. Однако, вы должны самостоятельно убедиться, что разработанные вами схемы адресации соответствуют

требованиям задания.

Виртуальные машины могут иметь предустановленное программное обеспечение, которое будет применяться при проверке и оценке, его не рекомендуется удалять.

Для доступа к виртуальным Linux-машинам используйте логин **root** с паролем **toor** и логин **skill39** с паролем

P@ssw0rd. Для доступа к ESXi используйте логин **root** с паролем***P@ssw0rd***.

При первом доступе к Windows-машинам следуйте инструкциям мастера. В любом случае на всех машинах обеспечьте работоспособность учетной записи: ***Administrator***/***P@ssw0rd*** с правами как локального, так и доменного администратора.

Если Вам требуется установить пароль, не указанный в задании, а также в инструкциях и файлах дополнений, используйте: **P@ssw0rd**

У вас есть консольный доступ к сетевому оборудованию. Доступ к маршрутизатору ISP не предусмотрен. На части устройств уже настроен пользователь **atom** с паролем **skills** и пароль на enable **as**. На остальных устройствах логины и пароли отсутствуют, устройства имеют "нулевую" конфигурацию.

На клиентских виртуальных машинах можно сменить дистрибутив ОС Linux.

Для смены образа виртуальной машины используйте меню **Settings -> Change VM type**. Кнопка **Re-Create** в меню виртуальной машины вернёт преднастроенный образ по умолчанию. **Обратите внимание**: используя функцию **Re-Create**, вы сбрасываете устройство на первоначальное состояние (на начало первого дня) и безвозвратно теряете все сделанные изменения.

ПРЕДНАСТРОЙКИ РАБОЧЕГО МЕСТА

1. На всех узлах под управлением ОС Linux установлены пакеты программного обеспечения **tcpdump**, **net-tools**, **dnsutils**, **sshpass**, **curl**, **open-vm-tools**, **snmp**, браузер **lynx**, клиенты **ftp** и **lftp**.
2. На всех предустановленных Windows-машинах установлены утилита **curl** и гостевые дополнения для гипервизора. 3. На DC, WINCLI1 и WINCLI2 в оптических приводах находится диск с дистрибутивом соответствующей операционной системы. 4. На всех Windows-машинах выполнена команда sysprep.
5. Ряд дополнительных пакетов и приложений, а также комплекты документации доступны на сервере moogle.ru, имитирующем реальную работу сети Интернет.
6. Все сетевые устройства сконфигурированы для удалённого администрирования из соответствующих локальных сетей по протоколу Telnet. На межсетевой экран скопирован дистрибутив ASDM.
7. Параметры интернет-провайдеров, предоставляющих услуги организации или клиентам.

Провайдер	**Адрес IPv4/Маска**	**Шлюз IPv4**	**AS**
MOONET	172.217.35.80/24	172.217.35.1	15169
LVL80	138.12.12.5/24	138.12.12.1	3356
GIGAFON CR2	178.207.179.4/29	178.207.179.1	31133
GIGAFON HQ1	178.207.179.29/29	178.207.179.25	31133
GOSTELECOM	77.34.141.141/22	77.34.140.1	12332
TTL	62.33.111.111/25	62.33.111.1	20485
PURPLE	2.2.1.101/24	2.2.1.1	3215
WATERFONE	84.64.44.24/28	84.64.44.17	1273
ROAMING1	DHCP (12.12.12.0/24)	DHCP (12.12.12.1)	7018
ROAMING2	DHCP (13.13.13.0/24)	DHCP (13.13.13.1)	7018

11. Провайдеронезависимые (PI) адреса и ASN в ЦОДе

Адрес IPv4/Маска	Сеть	AS
203.0.113.0/24	DMZ1	64500
203.0.117.0/24	LINDMZ	64500

12. Адреса Moogle

	Префиксы	DNS	AS

	Префиксы	DNS	AS
MOOGLE	172.110.32.0/21 172.217.0.0/16 8.8.8.0/24	8.8.8.8	15169

13. В сетях MOONET, LVL80 и GIGAFON CR2 сделаны настройки BGP.
    1. Соседство устанавливается по IPv4 с адреса шлюза на выделяемый провайдером адрес через физический интерфейс и указанные выше номера автономных систем.
    2. Все провайдеры анонсируют делегируемые префиксы в "интернет".
    3. Провайдеронезависимый префикс не анонсируется.
14. На HQ1, D1, A1 и A2 сделаны базовые настройки, обеспечивающие работу локальной сети и выход в Интернет для клиентов центрального офиса.
15. На CR1 и CSW1 сделаны базовые настройки, обеспечивающие работу локальной сети и выход в Интернет для устройств в ЦОД.
16. Между CR1 и HQ1 установлен GRE-туннель и настроена маршрутизация для обеспечения связи между сетью центрального офиса и ЦОДа.

Настройка сети центрального офиса

1. Настройте административный доступ ко всем сетевым устройствам в центральном офисе.
    1. Для обеспечения административного доступа создайте интерфейс Loopback1 на HQ1, HQ2, D1, D2. На коммутаторах A1 и A2 используйте интерфейс Vlan 13.
    2. Используйте SSH версии 2 и ключ длиной 4096 бит.
    3. Используйте для аутентификации по SSH NPS-сервер, но предусмотрите локальный вход в случае недоступности сервера. 4. Используйте локальную аутентификацию для консоли.
    5. Создайте локальную учётную запись **tech** с паролем **easy** на маршрутизаторах HQ1 и HQ2 с возможностью просматривать настройки IP на интерфейсах и таблицу маршрутизации, но исключите возможность вводить другие команды. 6. Создайте учётную запись **atom** с защищённым паролем **skills** и максимальными привилегиями на тех устройствах, где её ещё нет.
    7. При входе в систему по SSH или через консоль с учётной записью **atom** пользователю должны автоматически передаваться максимальные полномочия.
    8. Настройте хешированный пароль **as** на режим enable.
    9. Все пароли должны храниться в защищённом виде с использованием алгоритма scrypt.
    10. В случае попытки подбора пароля на маршрутизаторах HQ1 и HQ2 (не менее 3 раз за 15 секунд) они должны временно блокировать доступ по SSH со стороны интернета на 2 минуты. Доступ со стороны локальной сети должен сохраняться.

    HQ1(config)#login block-for 120 attempts 3 within 15

    HQ1(config)#ip access-list standard LOGIN

    HQ1(config-std-acl)# permit 192.168.11.0 0.0.0.255 - ну и дальше все что хочешь разреши

    HQ1(config)# login quiet-mode access-class LOGIN

    Для проверки пиши команду - sh login

    2. Настройте маршрутизатор HQ2 и коммутатор D2 согласно топологии L3.

    1. Создайте необходимые SVI на D2.
    2. Настройте IP-адреса на внутреннем интерфейсе маршрутизатора HQ2 и интерфейсах коммутатора D2 на ваше усмотрение. 3. Настройте IP-адрес на маршрутизаторе HQ2, выдаваемый провайдером.
3. Настройте L2-Etherchannel между коммутаторами D1, D2, A1 и A2.
    1. Используйте протокол LACP.
    2. Коммутаторы D1 и D2 должны инициировать согласование канала.

3. Используйте балансировку по MAC-адресам источника и назначения. **Примечание**: для корректной настройки LACP возможно потребуется предварительно выключить физические порты с двух сторон Etherchannel, произвести настройку и затем включить физические порты.

4. Настройте L3-Etherchannel между коммутаторами D1 и D2.
   1. Используйте протокол PAgP. Коммутатор D1 должен инициировать создание канала.
5. Настройте транки между коммутаторами D1, D2, A1 и A2 поверх Etherchannel.
   1. Транки должны устанавливаться принудительным образом. В явном виде отключите протокол DTP.
   2. Вручную ограничьте список VLAN, разрешённых на этих транках таким образом, чтобы в него входили только фактически используемые сети VLAN.
6. Настройте VRRP на коммутаторах D1 и D2 для сетей WINA, WINB и LINA.
   1. Используйте версию 2.
   2. Используйте номер группы, совпадающий с номером VLAN.
   3. Все устройства из соответствующих сетей должны использовать адрес виртуального маршрутизатора в качестве шлюза. 4. В сетях WINA и WINB должен по умолчанию предпочитаться шлюз D1, а в сети LINA - шлюз D2.

D1(config)# fhrp version vrrp v2

D1(config)#int vlan 11

D1(config-vlan)# vrrp 11 ip 192.168.11.254 - указываем уже общий адрес

D1(config-vlan)# vrrp 11 priority 100 - приоритет

D1(config-vlan)# vrrp 11 preempt - для перехвата мастера VRRP

7. Настройте службу DHCP в центральном офисе.
   1. Сделайте необходимые настройки, чтобы устройства в сети WINA могли получить адрес по DHCP от сервера DC. 2. Настройте DHCP Snooping на коммутаторах A1 и A2.
8. Настройте протокол STP на коммутаторах D1, D2, A1, A2.
   1. Коммутатор D1 должен быть корнем в VLAN 11 и 12. Коммутатор D2 должен быть корнем в VLAN 13.
   2. Используйте протокол 802.1w.
9. Настройте порты доступа на коммутаторах A1 и A2.

1. Порты в сторону клиентских устройств и серверов должны сразу переходить в состояние Forwarding, но блокироваться, если на них приходит BPDU.
2. Принудительно переведите их в режим доступа и отключите в явном виде протокол DTP. 10. Включите протокол LLDP на всех сетевых устройствах центрального офиса.
   1. Отключите отправку LLDP-сообщений в сторону клиентов и серверов, а также провайдера, но ~~оставьте их получение.~~

11. Настройте динамическую маршрутизацию с помощью протокола OSPF.
    1. Используйте область 0.
    2. Коммутаторы D1 и D2 должны использовать маршрут по умолчанию типа 1, полученный по OSPF.
    3. Все сети центрального офиса должны быть объявлены в OSPF.
    4. Все интерфейсы, через которые не предусмотрено соседство, должны находиться в пассивном режиме.

12. Настройте второй интернет-канал в центральном офисе через маршрутизатор HQ2.
   1. Второй канал должен использоваться в качестве резервного.

13. Настройте на маршрутизаторах HQ1 и HQ2 проверку связи со шлюзом провайдера по ICMP. В случае недоступности шлюза провайдера с маршрутизатора HQ1 должно автоматически происходить переключение на резервный канал связи.

OSPF на HQ2

default-information originate {MAX_METRIC} metric-type 1

OSPF на HQ1

default-information originate metric-type 1

SLA на HQ1

HQ1(config)# ip sla 1

HQ1(config-ip-sla)# icmp-echo 77.34.140.1 - указали какой адрес проверяем

HQ1(config-ip-sla-echo)# threshold 1000

HQ1(config-ip-sla-echo)# timeout 3000

HQ1(config-ip-sla-echo)# frequency 4

HQ1(config)# ip sla schedule 1 forever start-time now

HQ1(config)# track 1 ip sla 1 reach

HQ1(config-track)# exit

HQ1(config)# event manager applet INET_DOWN

HQ1(config-applet)# event track 1 state down

HQ1(config-applet)# action 001 syslog msg “INET SLOMALSYA!”

HQ1(config-applet)# action 002 cli command enable

HQ1(config-applet)# action 003 cli command “clear ip bgp *”

HQ1(config-applet)# action 004 cli command “end”

14. Настройте синхронизацию времени между сетевыми устройствами по протоколу NTP.
    1. В качестве сервера должен выступать маршрутизатор HQ1 со стратум 5
    2. Используйте на маршрутизаторе HQ1 интерфейс Loopback1 в качестве источника.
    3. Все остальные сетевые устройства должны синхронизировать своё время с маршрутизатором HQ1.
    4. Используйте на всех устройствах московский часовой пояс.
15. Настройте мониторинг, журналирование и архивирование конфигураций на сетевых устройствах HQ1, HQ2, D1, D2, A1,
    A2. 1. Используйте SNMPv2c и строку сообщества **atomskills2021**
    2. Опрос по SNMP нужно разрешить для сервера SRV.
    3. Архив конфигурации необходимо при каждом сохранении отправлять на TFTP-сервер на SRV.
    4. Имя архива должно содержать имя устройства, дату и время.
    5. Syslog уровня важности 5 и более важные необходимо отправлять на сервер SRV.
    6. В сообщениях журнала необходимо указывать дату, время и часовой пояс.
    7. В качестве источника трафика на сетевых устройствах D1, D2, HQ, HQ2 используйте интерфейс Loopback1. На устройствах A1 и A2 используйте интерфейс VLAN13
16. Настройте DMVPN между центральным офисом и ЦОД.
    1. Используйте CR1 и CR2 в качестве хабов.
    2. Используйте номер интерфейса 101 на CR1, 102 на CR2, номера 101 и 102 на HQ1 и HQ2 в сторону CR1 и CR2 соответственно. 3. На CR1 используйте интерфейс в сторону провайдера LVL80.
    4. Используйте следующие параметры для защиты туннеля:
        1. IKEv1 с параметрами AES128, SHA, DH14
        2. IPsec с помощью протокола ESP с шифрованием AES128 и хешем SHA.

DMVPN

CR1(config)#int tun 101
CR1(config-int)# ip address 10.5.5.1 255.255.255.0
CR1(config-int)# ip nhrp map multicast dynamic
CR1(config-int)# ip nhrp network-id 101
CR1(config-int)# tunnel source e0/2
CR1(config-int)# tunnel mode gre multipoint
CR1(config-int)# tunnel key 101

_____

CR2(config-int)# int tun 102
CR2(config-int) # ip address 10.5.5.2 255.255.255.0
CR2(config-int)# ip nhrp map multicast dynamic
CR2(config-int)# ip nhrp network-id 102
CR2(config-int)# tunnel source e0/0
CR2(config-int)# tunnel mode gre multipoint
CR2(config-int)# tunnel key 102

_____

HQ1(config)# int tun 101
HQ1(config-int)# ip address 10.5.5.3 255.255.255.0
HQ1(config-int)# ip nhrp map multicast 138.12.12.5 - пишешь внешний адрес
HQ1(config-int)# ip nhrp map 10.5.5.1 138.12.12.5
HQ1(config-int)# ip nhrp network-id 101
HQ1(config-int)# tunnel key 101
HQ1(config-int)#tunnel mode gre multipoint
HQ1(config-int)# ip nhrp nhs 10.5.5.1

_____

HQ2(config)# int tun 102
HQ2(config-int)# ip address 10.5.5.4 255.255.255.0
HQ2(config-int)# ip nhrp map multicast 172.207.65.1 - пишешь внешний адрес
HQ2(config-int)# ip nhrp map 10.5.5.2 172.207.65.1
HQ2(config-int)# ip nhrp network-id 102
HQ2(config-int)#tunnel key 102
HQ2(config-int)# tunnel mode gre multipoint
HQ2(config-int)#ip nhrp nhs 10.5.5.2
IPSEC
CR1(config)# crypto isakmp policy 1
CR1(config-isakmp)# encr aes128
CR1(config-isakmp)# auth pre-share
CR1(config-isakmp)# hash sha
CR1(config-isakmp)# group 14
CR1(config)# crypto isakmp key cisco address 0.0.0.0
CR1(config)# crypto ipsec trasnform-set IPSEC esp-aes128 esp-sha-hmac
CR1(config-crypto-trans)# mode tunnel
CR1(config)# crypto ipsec profile IPSEC
CR1(config-profile)# set transform-set IPSEC
CR1(config)# int tun1
CR1(config-int)# tunnel protection IPSEC

17. Настройте маршрутизацию EIGRP поверх DMVPN
    1. Используйте номер автономной системы 65000.
    2. Для связи между ЦОД и центральным офисом должен предпочитаться маршрут через CR2 и HQ2.
    3. Настройте BFD для быстрого определения состояния каналов.

    bfd all-interfaces - в конфиге EIGRP

Настройка сервисов ОС Linux в сети центрального офиса

1. Настройте административный доступ к серверу SRV.

    1. Настройте службу SSH.

        Запретите вход пользователю root по протоколу SSH, в том числе с использованием аутентификации на основе открытых ключей. - **PermitRootLogin no**

        Служба SSH должна работать на порту 1022. - **Port 1022**

        Доступ к SRV по SSH должен быть разрешён только пользователю **linadmin**.

        Запретите аутентификацию с использованием паролей при подключении по SSH. - **PasswordAuthentication no**

    2. Виртуальная машина ASTERISK должна выступать клиентом удаленного доступа по протоколу SSH.

        Для пользователя **linadmin** доступ к SRV должен происходить автоматически по правильному порту, без его явного указания номера порта в команде подключения.

        Для других серверов по умолчанию должен использоваться порт 22.

2. Настройте аутентификацию на SRV и ASTERISK.

    1. Создайте пользователя **linadmin** на SRV и ASTERISK с паролем **P@ssw0rd**
    2. Разрешите пользователю **linadmin** на ASTERISK повышать привилегии с использованием команды sudo. 3. При использовании команды sudo на ASTERISK для пользователя linadmin не должен запрашиваться пароль при вводе команд, начинающихся с **systemctl** и **journalctl**.

    visudo

    linadmin ALL=NOPASSWD: ALL

    4. У других пользователей не должно быть прав на повышение привилегий с использованием команды sudo. 3. Настройте службу TFTP на SRV для хранения резервных копий конфигурационных файлов.

    1. Используйте каталог **/opt/tftp** для хранения файлов.

    apt install tftpd-hpa

    mkdir /opt/tftp

    chmod 777 /opt/tftp -R

    vim /etc/default/tftpd-hpa

```
TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/opt/tftp"
TFTP_ADDRESS="0.0.0.0:69"
TFTP_OPTIONS="-c -p -s"
```

4. На сервере SRV должна быть настроена служба централизованного сбора журналов.

    1. Журналы должны храниться в директории **/opt/logs/**
    2. Журналирование должно производиться в соответствии с **Таблицей 2**.

    vim /etc/rsyslog.conf

```
#### GLOBAL DIRECTIVES ####
############################
if $hostname contains 'ASTERISK' or $fromhost-ip contains '10.10.12.20' then {
        auth,authpriv.* /opt/logs/auth/ASTERISK.log;
}
if $hostname contains 'SRV' then {
        *.err,*.warn /opt/logs/local/errors.log;
}
if $fromhost-ip contains '10.10.12.1' then {
        *.* /opt/logs/net/10.10.12.1.log;
}

if  $fromhost-ip contains '192.168.30.30' then {
        *.* /opt/logs/net/192.168.30.30.log;
}
```

5. На SRV настройте веб-сервер с базовой аутентификацией для быстрого доступа к файлам резервных копий конфигурационных файлов.

    1. Веб-сервер должен отображать файлы в каталоге **/opt/tftp**.
    2. Настройте базовую аутентификацию (Basic Auth) для доступа к файлам для пользователя **web** с паролем **P@ssw0rd**
    3. Сайт должен быть доступен по доменному имени configs.AS21.local для клиентов локальной сети организации.
        1. Веб-сайт должен работать по протоколу HTTPS.

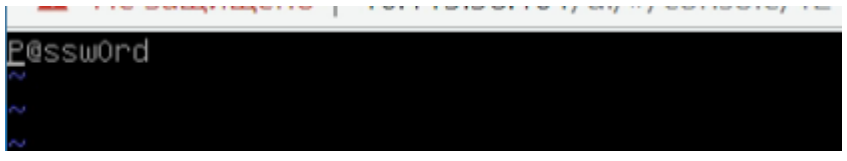
        2. Настройте автоматическую переадресацию протокола HTTP на HTTPS.

4. Сайт должен быть доступен только по доменным именам, при запросе по IP адресу должна отображаться страница ошибки с кодом 404.

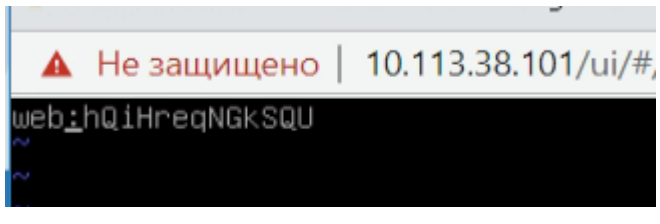
vim /etc/nginx/conf.d/site.conf

```
server {
        listen 10.10.12.10:443 ssl;
        ssl_certificate /etc/nginx/configs1.crt;
        ssl_certificate_key /etc/nginx/configs1.key;
        ssl_password_file /etc/nginx/configs1.pass;
        root /opt/tftp;
        server_name configs.as21.local;
        autoindex on;
        auth_basic "Enter your login";
        auth_basic_user_file /etc/nginx/users;
        location / {
                root /opt/tftp;
}
}
server {
        listen 10.10.12.10;
        return 404;
}

server {
        listen 10.10.12.10:80;
        server_name configs.as21.local;
        return 301 https://configs.as21.local/$request_uri;
}
```

Содержимое файла configs1.pass



Содержимое файла /etc/nginx/users



openssl passwd >> /etc/nginx/users - создаст тебе пароль в зашифрованном виде как на скрине сверху

5. Установите сертификат для сайта configs.AS21.local

1. Сертификат должен быть подписан **DEM-CA**.

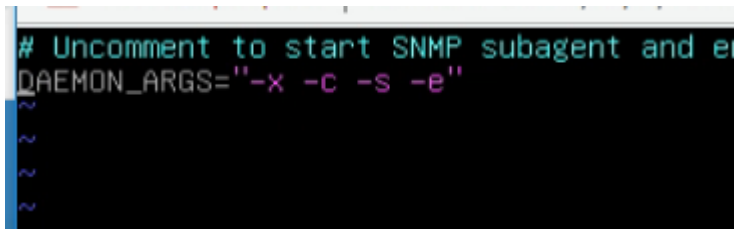
```
openssl pkcs12 -in [yourfilename.pfx] -nocerts -out [keyfilename-encrypted.key] - так вытащить ключ
openssl pkcs12 -in [yourfilename.pfx] -clcerts -nokeys -out [certificatename.crt] -  так сертификат
```

2. Клиентские операционные системы должны доверять сертификатам сайтов и не выдавать никаких предупреждений.

6. Включите протокол CDP на сервере SRV для работы в оба направления.

apt install lldpd

vim /etc/default/lldpd



7. Настройте АТС на ASTERISK. Используйте пакет Asterisk.

1. Используйте номера согласно **L3 диаграмме**.
2. SIP-клиенты должны быть зарегистрированы под учётными записями пользователей.

   Используйте учетную запись linadmin для ASTERISK.

   Используйте учетную запись User_001 для WINCLI2.

3. Разместите ярлык запуска программного телефона на рабочем столе соответствующего пользователя. 4. Добавьте в контакты программного телефона номер второго абонента. Например: 2001@sip.AS21.local 5. Бинарные пакеты программного телефона linphone 4.2 доступны на сервере moogle.ru.

apt install asterisk

vim /etc/asterisk/module.conf

noload => chan_pjsip.so

vim /etc/asterisk/users.conf

[2001]

secret = 2001

host = dynamic

context = as21

[2002]

secret = 2002

host = dynamic

context = as21

Пишем это все чуть выше примера описания юзера 6000

```
[2001]
secret = 2001
host = dynamic
context = as21

[2002]
secret = 2002
host = dynamic
context = as21
```

vim /etc/asterisk/extensions.conf

[as21]

exten => _200X!,1,Dial(SIP/${EXTEN})

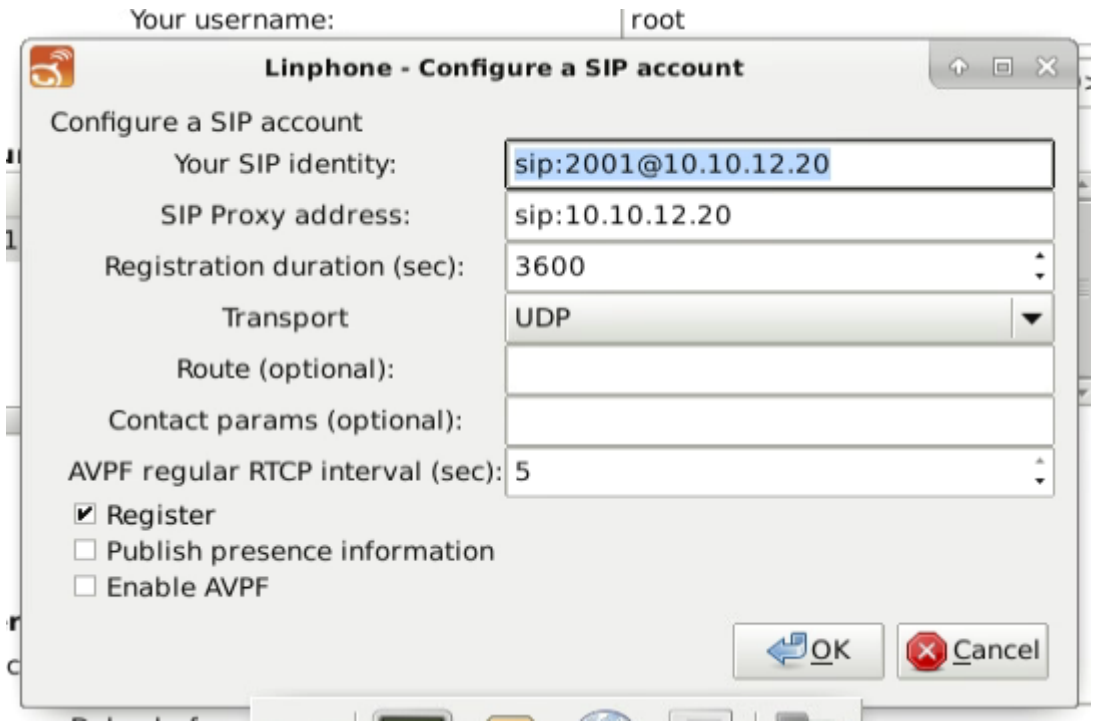
```
;
[as21]
exten => _200X!,1,Dial(SIP/${EXTEN})

;[context]
```

[context] - чуть выше данного поля пишем свой профиль

Далее на клиенте ASTERISK - ставим linphone

apt install linphone

Далее открываем его через GUI → Options → заполняй его как на скрине внизу



На винде поставим PhonerLite - там все интуитивно понятно

8. Настройте на SRV сервис удаленного доступа на основе технологии OpenVPN, используя следующие параметры:

    1. TUN адаптер.
    2. Протокол UDP.
    3. Порт сервера 8081.
    4. Включите дополнительную TLS аутентификацию.

Конвертация - openssl x509 -inform DER -in certificate.cer -out certificate.crt из Cer для Crt

Если будут проблемы с паролем

```
# (see "pkcs12" directive in man page).
ca /etc/openvpn/RootCA.crt
cert /etc/openvpn/OpenVPN.crt
key /etc/openvpn/OpenVPN.key  # This file should be kept secret
askpass '/etc/openvpn/pass'
# Diffie hellman parameters.
```

Итак, для сервера достаточно выпустить обычный сертификат из шаблона Web Server. В common-name укажешь свой адрес для работы OpenVPN

Windows выпустит шаблон в формате pfx, надо будет его разобрать для работы в Linux среде

```
52  openssl pkcs12 -in ClientOpenVPN.pfx -cacerts -nokeys  -out CA.crt
53  openssl pkcs12 -in ClientOpenVPN.pfx -nokeys -clcerts -out Client.crt
54  openssl pkcs12 -in ClientOpenVPN.pfx -nocerts -nodes -out Client.key
```

- данная команда актуальна для распаковки любого pfx, который тебе может понадобится.

Далее самый обычный OpenVPN-server, без особых сложностей, добавь только tls-auth ta.key одинаковый и для сервера и для клиента, также в конфиге добавь строчку duplicate-cn, чтобы клиенты могли аутентифицироваться под одним CN в сертификате

Для клиента нужно будет сделать сертификат из шаблона Workstation Authentication - в CN напиши просто client.

Далее распаковка сертификата, как по примеру сверху. Прокинь сертификаты на клиенты и все.

Настройка сервисов ОС Microsoft Windows в сети центрального офиса

1. Сделайте сервер DC контроллером домена AS21.local.
    1. Учетная запись доменного администратора должна иметь логин **Administrator** и пароль **P@ssw0rd**; других доменных администраторов быть не должно;
    2. На контроллере домена перед окном ввода пользовательских реквизитов должен находиться баннер с надписью "Warning! Property of RosAtom!".
2. Сделайте компьютеры WINCLI1 и WINCLI2 членами домена AS21.local.
    1. Учетная запись локального администратора на WINCLI1 и WINCLI2 должна иметь логин **Administrator** и пароль **P@ssw0rd**; других локальных администраторов быть не должно.
    2. Приветственная анимация при входе новых пользователей должна быть отключена.
    3. При первом локальном входе любого пользователя на компьютер WINCLI1 на рабочем столе должен находиться файл **Test.txt** со следующим содержанием "It is a first login".

    1) Создаем файлик на Раб Столе с нужным текстом

    2) Идем на клиенте в папку - C:\Users\default\Desktop и располагаем файл там ***(если по GPO - mo user config - Windows Setup - Files и там все понятно)***

4. На клиентах домена включите возможность подключения к ним с использованием утилиты Remote Desktop Connection с защитой подключения с помощью сертификатов, выданных сервером SubCA (данная настройка должна автоматически применяться для любых новых клиентов домена). При подключении должна быть возможность использовать канонические и короткие имена компьютеров, а также их ip-адреса (при этом не должно возникать никаких ошибок и предупреждений). 3. Обеспечьте работоспособность службы DNS на DC.
    1. Должна быть настроена переадресация запросов для имен, не связанных с внутренним доменом, на сервер Moogle. 2. Для имеющихся в основной доменной зоне записей с одинаковыми именами, но разными адресами должна работать балансировка по алгоритму round-robin, при этом не должно быть повышения нагрузки на DNS-сервер из-за слишком частого обновления зон.

    В Advanced-режиме DNS Manager нужно создать запись с TTL - 0, потом в свойствах DNS-сервера в Advanced убрать галку с параметра DNS network order.

    4. Обеспечьте работоспособность службы DHCP на DC.
    1. Все клиенты в сети центрального офиса должны иметь возможность получать корректные адреса в своих подсетях с DC. 5. Проверьте работоспособность файловых служб на DC.
    1. Члены группы Engineers должны иметь полный доступ к общей папке Work.
    2. Члены группы Projects должны иметь доступ к общей папке Work только для чтения.
    3. Создайте в домене при необходимости указанные выше группы, в каждой группе создайте по одному пользователю Engineer1/P@ssw0rd и Projects1/P@ssw0rd соответственно.
    4. Переместите в общую папку Work исполняемый файл notepad.exe; обеспечьте возможность запуска notepad.exe из общей папки Work, но учтите, что никакие другие исполняемые файлы не должны запускаться из этой папки.

    Делаем GPO -> Comp.Config -> Windows Setup -> Security Options -> Software Restriction Policies -> Additional Levels -> создаем два правила - Hash Rule and Path Rule.

6. Проверьте работоспособность служб времени на DC и в домене в целом.

1. Контроллер домена должен быть настроен для синхронизации системного времени с сервером Moogle. 2. Все компьютеры в домене должны синхронизировать время с контроллером домена DC.
3. На всех компьютерах домена должна быть установлена зона "Ekaterinburg Standard Time"; эта настройка должна действовать всегда, в том числе, после перезагрузки.

7. Создайте подразделения, группы безопасности и пользователей на контроллере домена DC
   1. Создайте подразделение Office.
   2. В подразделении Office создайте три группы Group1, Group2, Group3.
   3. В подразделении Office создайте 150 пользователей **User1** - **User150**. Имя входа в домен, например, **User1@AS21.local** (для остальных пользователей аналогично). Пароль для входа в домен ***P@ssw0rd*** (для всех создаваемых пользователей). Первые 50 пользователей должны быть членами группы Group1, следующие 50 пользователей - членами группы Group2, оставшиеся 50 пользователей - членами группы Group3. Все созданные аккаунты должны быть включены. 4. Разрешите членам группы Group3 локальный вход на контроллер домена DC.

Policies -> Windows Settings -> Security Settings -> Заходим в Default Policy -> Computer Configuration ->

   5. Для членов группы Group3 настройте использование перемещаемых профилей (место хранения профилей выберите самостоятельно); каждый пользователь должен иметь доступ только к папке своего профиля, в том числе при обращении к папке по сети через файловый менеджер.

8. Настройте корневой центр сертификации на контроллере домена DC
   1. Имя настраиваемого центра сертификации - RootCA.
   2. Срок действия сертификата - 4 года.
   3. Обеспечьте доверие данному центру сертификации на всех компьютерах и устройствах в соответствии с настоящим конкурсным заданием.
9. На всех компьютерах под управлением ОС Microsoft Windows обеспечьте функционирование Defender Firewall. При этом работоспособность настроенных ранее сервисов не должна нарушиться.

Настройка ЦОД

1. Настройте административный доступ ко всем устройствам в центре обработки данных.
   1. Создайте для этого интерфейс Loopback1 на CR1, CR2, CSW1, CSW2.
   2. Используйте SSH версии 2 и ключ длиной 4096 бит.
   3. Используйте для аутентификации локальные базы учётных записей.
   4. Используйте локальную аутентификацию для консоли.
   5. Создайте учётную запись **atom** с защищённым паролем **skills** и максимальными привилегиями на тех устройствах, где её ещё нет.
   6. При входе в систему по SSH или через консоль с учётной записью **atom** пользователю должны автоматически передаваться максимальные полномочия.
   7. Настройте хешированный пароль **as** на режим enable.
   8. Все пароли должны храниться в защищённом виде с использованием алгоритма scrypt.
2. Настройте все сети VLAN согласно топологии.
   1. Создайте недостающие VLAN и укажите их имена согласно топологии.
   2. На всех транках должны быть разрешены только используемые в топологии VLAN.
3. Настройте IP-адресацию на CR1, CR2, CSW1, CSW2.
4. Настройте выход в интернет в ЦОД
   1. Настройте подключение через LVL80 на CR1.
   2. Настройте подключение через GIGAFON на CR2.
5. Настройте BGP на CR1, CR2, CSW1, CSW2, LINDMZ.
   1. Настройте соседство с провайдерами на CR1 и CR2.
   2. Настройте iBGP между всеми сетевыми устройствами ЦОД.
   3. Используйте CSW1 и CSW2 в качестве Route Reflector.
   4. Сделайте необходимые настройки, чтобы для выхода в Интернет и входящего трафика предпочитался канал LVL80, однако сети MOOGLE и GIGAFON были доступны напрямую через соответствующие автономные системы.
6. Настройте EIGRP на CR1, CR2, CSW1 и CSW2.
   1. Используйте номер автономной системы 65000.
   2. Все интерфейсы, через которые не предусмотрено соседство, должны быть в режиме Passive. Соседство между CSW1 и CSW2 должно быть только через VLAN 50.
   3. Настройте редистрибуцию сетей из EIGRP в OSPF и обратно. Не используйте статические маршруты для обеспечения маршрутизации между центральным офисом и ЦОД.
7. Сервер LINDMZ должен получать только маршрут по умолчанию по протоколу BGP от CSW1 и CSW2. Все остальные префиксы должны быть отфильтрованы.
   1. Входящий трафик из интернета до сервера LINDMZ должен приходить через CSW1 и переключаться на CSW2 только в случае проблем со связью на CSW1, CR1 или у провайдера.

Настройка виртуальной инфраструктуры

1. Включите протокол CDP на ESXi1 для работы в оба направления.
2. Выполните миграцию виртуальной машины CLOUDWEB с сервера ESXi1 на KVM1.
   1. Настройки и программное обеспечение на CLOUDWEB должны быть сохранены, включая IP адрес.
3. Увеличьте объем диска для хранения веб-сайта на CLOUDWEB.

1. Добавьте новый виртуальный тонкий диск объёмом 2 ГБ к CLOUDWEB.
2. Сайт располагается на LVM разделе, смонтированном в каталог **/var/www/html**.
3. Объедините объем существующего раздела с вновь созданным диском.

4. Виртуальная машина должна стартовать автоматически при загрузке KVM1.
   1. Задержка включения после загрузки KVM1 не должна превышать 10 сек.

apt install qemu* -y

qemu-img convert -O qcow2 *.vmdk *.qcow2

Так как я дурак и не умею работать с KVM по гконсоли, мы настроим проброс X по ссш

на сервере KVm -

```
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
X11DisplayOffset 10
#X11UseLocalhost yes
```

Подключаться к машине - ssh -X root@kvm_address

А потом запускай virt-manager и там все легко

для расширения LVM раздела -

Команды для помощи - pvs - покажет тебе список всех дисков подключенных к LVM

lvs - покажет объем текущей LVM раздела

vgextend WWW /dev/sdd1 - добавили его в VG группу

для расширения LVM раздела - lvextend /dev/WWW/LVM /dev/sdd1

все команды доступны вот тут

```
root@CLOUDWEB1:~# vgextend WWW /dev/sdd1
  Physical volume "/dev/sdd1" successfully created.
  Volume group "WWW" successfully extended
root@CLOUDWEB1:~# pvs
  PV         VG  Fmt  Attr PSize    PFree
  /dev/sda1  WWW lvm2 a--  1020.00m       0
  /dev/sdb1  WWW lvm2 a--  1020.00m       0
  /dev/sdc1  WWW lvm2 a--  1020.00m       0
  /dev/sdd1  WWW lvm2 a--  1020.00m 1020.00m
  Insufficient free space: 256 extents needed, but only 255 available
root@CLOUDWEB1:~# pvs
  PV         VG  Fmt  Attr PSize    PFree
  /dev/sda1  WWW lvm2 a--  1020.00m       0
  /dev/sdb1  WWW lvm2 a--  1020.00m       0
  /dev/sdc1  WWW lvm2 a--  1020.00m       0
  /dev/sdd1  WWW lvm2 a--  1020.00m 1020.00m
root@CLOUDWEB1:~# lvs
  LV   VG  Attr       LSize  Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
  LVM  WWW -wi-a----- <2.99g
root@CLOUDWEB1:~# lvextend /dev/WWW/LVM /dev/sdd1
  Size of logical volume WWW/LVM changed from <2.99 GiB (765 extents) to 3.98 GiB (1020 extents).
  Logical volume WWW/LVM successfully resized.
root@CLOUDWEB1:~# lvs
  LV   VG  Attr       LSize Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
  LVM  WWW -wi-a----- 3.98g
root@CLOUDWEB1:~# pvs
  PV         VG  Fmt  Attr PSize    PFree
  /dev/sda1  WWW lvm2 a--  1020.00m    0
  /dev/sdb1  WWW lvm2 a--  1020.00m    0
  /dev/sdc1  WWW lvm2 a--  1020.00m    0
  /dev/sdd1  WWW lvm2 a--  1020.00m    0
root@CLOUDWEB1:~#
```

Для добавления в автозагрузку - virsh start CLOUDWEB

Потом ребут и проверяем

Настройка сервисов ОС Linux в ЦОД

1. Настройте делегирование зоны skill39.ru для обеспечения работы доменных имён согласно **Таблице 1**. Для делегирования зоны skill39.ru укажите IPv4 адреса DNS серверов, обслуживающих зону, на сайте nic.moogle.ru.
2. На виртуальной машине CLOUDWEB настроен веб-сервер.
   1. Веб-сервер работает по протоколу HTTP.
   2. Обеспечьте доступность сайта на CLOUDWEB по доменному имени cloud.AS21.local для клиентов локальной сети организации по протоколу HTTPS.
   3. Для обеспечения доступа к сайту настройте обратный прокси (reverse proxy) на LINDMZ.
   4. Доменное имя cloud.AS21.local должно быть CNAME записью для имени web.AS21.local, согласно **Таблице 1**.
   5. Сертификат должен быть подписан **DEM-CA**.
   6. Клиентские операционные системы должны доверять сертификатам сайтов и не выдавать никаких предупреждений.

vim /etc/nginx/conf.d/proxy.conf

```
upstream cloud {
        server 192.168.30.40:80;
}

server {
        listen 192.168.30.30:443 ssl;
        ssl_certificate /var/www/cloud.crt;
        ssl_certificate_key /var/www/cloud.key;
        ssl_password_file /var/www/cloud.pass;
        location / {
                proxy_pass http://cloud;
                }
}
```

Это надо продублировать дважды для сайта web, серты делай под *

3. В случае сбоя одного из провайдеров сайты на LINDMZ должны быть доступны из интернета.
    1. Сайт должен быть доступен по доменному имени web.skill39.ru для клиентов в сети Интернет.

```
ip link add dev lo1 type dummy
ip addr add 1.1.1.1/32 dev lo1
ip link set lo1 up_
~
~
~
```

Вот так создать ЛУПБАК!!!

Кароч пока идея такая, что мы просто сделаем лупбэк и анонсируем его в BGP, дело сделано. Повторить на стенде особо не удалось

4. Установите Ansible на CLOUDCLI.
    1. Создайте пользователя control с паролем P@ssw0rd
    2. Запуск Ansible будет производиться от имени пользователя control.
    3. Для хранения файлов и скриптов Ansible используйте каталог /home/control/playbook
    4. Отключите строгую проверку ключей для SSH на CLOUDCLI.

    vim /etc/ssh/ssh_config

```
Host *
#   ForwardAgent no
#   ForwardX11 no
#   ForwardX11Trusted yes
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
    StrictHostKeyChecking no
```

5. Модифицируйте имеющийся шаблон виртуальной машины (template-vm) на KVM1 для работы с Ansible. 1. Ansible, установленный на CLOUDCLI, должен подключаться по ssh к вновь развёрнутым виртуальным машинам без указания логина и пароля.

Для работы с темплейтами было бы удобно поставить пакет - apt install libguestfs-tools -y

    2. Настройте пользователя control для подключения Ansible.
    3. Обеспечьте возможность повышения привилегий пользователем control без ввода пароля.
6. Разработайте playbook для Ansible, который должен автоматизировать следующие задачи:
    1. Создание виртуальной машины на KVM1.

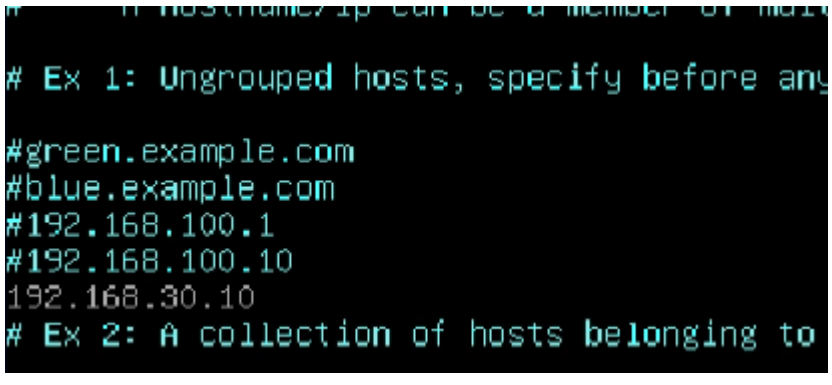
    Может понадобится выдать юзеру control добавить в группу libvirt - да понадобится

    2. Настройку имени виртуальной машины.
        1. Используйте информацию об имени хоста из конфигурационного файла Ansible.
    3. Настройку записи в файле /etc/hosts сопоставляющей имя виртуальной машины с адресом 127.0.1.1.
    4. Создание административного пользователя для подключения к виртуальной машине с использованием логина и пароля. 5. Включение пользователя в одну из существующих групп.
    6. Настройку прав владельца с доступом на чтение и запись для административного пользователя на каталог {{ admin_path }}. Другие пользователи должны иметь права только на чтение (755).
7. Создайте файл с переменными Ansible в каталоге ~/playbook с именем vars.yml
8. Файл vars.yml должен содержать следующие переменные:
    1. {{ vm_name }} - имя виртуальной машины для создания
    2. {{ admin_name }} - имя административного пользователя
    3. {{ admin_group }} - группа, в которую необходимо добавить созданного пользователя.
    4. {{ admin_path }} - каталог, к которому созданный пользователь должен иметь права, помимо домашней директории.
9. Создайте файл сейфа Ansible в каталоге ~/playbook с именем vault.yml
10. Файл vault.yml должен содержать следующие переменные:

11. {{ admin_password }} - пароль для административного пользователя в открытом виде.

Первым делом ставим ansible - apt install anisble -y

Далее идем в /etc/ansible/hosts и указываем там адрес нашего KVM-сервера



Настрой подключение к KVM по ключам для пользователя control

После этого проверь что все ок простой командой - ansible all -m ping - если вернется норм ответ, значит все правильно

Далее все готово к созданию плейбука.

Первым делом создаем файл vars.yml - файл для хранения переменных

- инициализируем все переменные, которые нам надо (только без матюков - дисквал)

Далее нужно создать файл vault.yml - для хранения там пароля админа в закрытом виде

```
control@CLOUDCLI:~$ ansible-vault encrypt_string --vault-password-file pass.yxy  'P@sswOrd' --name '
admin_password' > vault.yml
control@CLOUDCLI:~$ cat vault.yml
admin_password: !vault |
          $ANSIBLE_VAULT;1.1;AES256
          643563343166363164396465613262623632356635353263353935666637333537643135313438333
          643863636561316362316238323837373134613763343736 0a623637633332666334366162356436
          646534306365653837663666656465325338386664316235313333386333623637393265386663343
          666136353837613239 0a653133623230333662363566383533666666539643431363865316138636 1
          3465
```

Содержимое pass.txt

```
          3465
control@CLOUDCLI:~$ cat pass.yxy
P@sswOrd
```

Далее создаем task.yaml

```
---
- name: Task AS2021
  hosts: all
  vars_files:
          - /home/control/playbook/vars.yml
          - /home/control/playbook/vault.yml
  tasks:
          - name: Create VM on KVM1 server
            command: "sudo virt-clone --original template-vm --name {{ vm_name }} --file /mnt/{{ vm_
name }}"
          - name: Set Hostname
            command: "sudo virt-customize -d {{ vm_name }} --hostname {{ vm_name }}"
          - name: Create Admin user
            command: "sudo virt-customize -d {{ vm_name }} --run-command 'useradd {{ admin_name }}'"
          - name: Create Password for Admin
            command: "sudo virt-customize -d {{ vm_name }} --run-command 'echo {{ admin_name }}:{{ a
dmin_password }} | chpasswd' "
          - name: Configure ssh for new admin user
            command: "sudo virt-customize -d {{ vm_name }} --run-command 'echo AllowUsers {{ admin_n
ame }} root control >> /etc/ssh/sshd_config'"
          - name: Configure ssh for control-user
            command: "sudo virt-customize -d {{ vm_name }} --ssh-inject control:file:/home/control/.
ssh/id_rsa.pub"
          - name: Create Admin group
            command: "sudo virt-customize -d {{ vm_name }} --run-command 'groupadd {{ admin_group }}
'"
          - name: Add Admin group
            command: "sudo virt-customize -d {{ vm_name }} --run-command 'usermod {{ admin_name }} -
a -G {{ admin_group }}'"
          - name: Create Admin folder
            command: "sudo virt-customize -d {{ vm_name }} --run-command 'mkdir -p {{ admin_path }}'
"
          - name: Fix permissions
            command: "sudo virt-customize -d {{ vm_name }} --run-command 'chmod 755 {{ admin_path }}
'"
          - name: Launch net VM
                                                                    1,3           Top
```

```
"
          - name: Fix permissions
            command: "sudo virt-customize -d {{ vm_name }} --run-command 'chmod 755 {{ admin_path }}
'"
          - name: Launch net VM
            command: "sudo virsh start {{ vm_name }}"
          - name: Configuring /etc/hosts
            shell: |
                    echo '{{ vm_name }}' 127.0.1.1 >> /etc/hosts
                                                                   32,11         Bot
```

Комментарий для плейбука:

--- тремя символами - ты начинаешь свой плейбук

- name: Task AS2021 - глобальное имя твоего плейбука

hosts: all - все перечисленные в /etc/anisble/hosts устройства, в нашем случае там только KVM сервер

vars_files:

- **/home/control/playbook/vars.yml - указывашь, откуда брать переменные**
- **/home/control/playbook/vault.yml - указываешь, откуда брать скрытые переменные, то есть из сейфа**

tasks:

-name: Create VM on KVM1 server - пишем описание, какой процесс сейчас будем делать

command: “sudo virt-clone --original template-vm --name {{ vm_name }} --file /mnt/{{ vm_name }}” - данной командой выполняем копирование ВМки из шаблона template-vm в ВМку с именем {{ vm_name }}, которое берется из описанного ранее файла vars.yml

Далее все в целом понятно, кроме момента с пробросом ключа.

У тебя на машине CLOUDCLI уже есть ключи юзера control, передай их на KVM в локальную папку юзера ссш, а потом с помощью команды --ssh-inject добавь его в твой клон

Для правильного запуска плейбука пиши -так нужно для подключения ключа от vault.yml файла

```
"vars.yml" 6L, 81C written
control@CLOUDCLI:~/playbook$ ansible-playbook  --vault-password-file pass.txt task.yaml
```

Настройка компонентов ОС Microsoft Windows в ЦОД

1. На WINSRV1 настройте дополнительный контроллер домена AS21.local.
    1. Данный дополнительный контроллер домена должен быть контроллером только для чтения.
    2. Сайты основного и дополнительного контроллеров домена AS21.local должны быть разными.
    3. В случае появления доменных Windows-клиентов в ЦОД, они должны в первую очередь обращаться к дополнительному контроллеру, и только если он не доступен - к основному.
2. Настройка сервиса DNS на WINSRV1
    1. Передайте на WINSRV1 все зоны прямого просмотра с сервера DC.
    2. На WINSRV1 не должно быть ни одной основной зоны.
3. Настройка сервера терминалов на WINSRV1
    1. Разверните терминальный сервер, не устанавливайте и не настраивайте компоненты лицензирования. 2. Сконфигурируйте web-доступ к службам терминалов сервера.
    3. Web-интерфейс сервера должен быть доступен только по протоколу https по имени rds.AS21.local/RDweb. 4. Опубликуйте программу WordPad на web-портале RemoteApp для всех членов группы Group2, при запуске этой программы у пользователей не должны появляться никакие ошибки и предупреждения системы безопасности.
4. Настройка центра сертификации на WINSRV2
    1. Сделайте сервер членом домена AS21.local.
    2. Настройте на сервере подчиненный доменный центр сертификации с именем SubCA.
    3. В браузере IE Explorer должна быть настроена стартовая страница с актуальным списком выданных и отозванных сертификатов SubCA, доступным для скачивания;
    4. Сертификаты для членов группы Group3, для защиты подключений RDS, для сайтов и всех прочих целей должны быть выпущены этим центром сертификации.
5. Настройка web-сервера на WINDMZ
    1. Установите на сервер компоненты IIS.
    2. Настройте сайт со следующей страницей по умолчанию:

```
<html>
<body>
<center>  <h1>
Test site  </h1>
</center>  </body>
</html>
```


    3. Сайт должен быть доступен по имени www.AS21.local только по протоколу https для членов группы Group1 при предъявлении пользовательского сертификата.
    4. Внутри сайта создайте виртуальный каталог Docs. Поместите в него текстовый файл Test.txt. Включите возможность обзора содержимого каталога при подключении к нему пользователей через браузер.
6. На серверах WINSRV1 и WINSRV2 установите соответствующие роли для организации распределенной файловой системы.
7. Создайте папку C:\Share на сервере WINSRV1 и папку C:\Share на сервере WINSRV2. Внутри созданных папок создайте папки Man_share и Work_share.
8. Создайте корень DFS с именем FS. Данный корень должен поддерживаться обоими серверами. Создайте под этим корнем папку с именем Share, ссылающуюся на сетевые директории с тем же именем (Share) созданные вами ранее на каждом сервере. Обеспечьте членам группы Group1 доступ к этой папке на запись. Настройте репликацию между папками средствами DFS. Установите жесткое ограничение 1 Гб на размер папки FS\Share.
9. Запретите хранение аудио- и видео-файлов в папках C:\Share на серверах WINSRV1 и WINSRV2.
10. На всех компьютерах под управлением ОС Microsoft Windows обеспечьте функционирование Defender Firewall. При этом работоспособность настроенных ранее сервисов не должна нарушиться.

Настройка сети филиала 1

1. Настройте межсетевой экран ASA для обеспечения доступа в интернет для клиентов локальной сети. 1. Используйте в качестве имени внешнего интерфейса название провайдера.
    2. Настройте IP-адреса на внешнем и внутреннем интерфейсах.
    3. Настройте службу DHCP для локальной сети. Используйте MOOGLE в качестве DNS-сервера.
    4. Настройте NAT для адресов в локальной сети.
2. Настройте административный доступ к межсетевому экрану ASA.
    1. Используйте SSH версии 2 и ключ длиной 4096 бит.
    2. Используйте локальную аутентификацию для консольного доступа.
    3. Создайте учётную запись **atom** с паролем **skills** и максимальными привилегиями на тех устройствах, где её ещё нет. 4. При

входе в систему по SSH или через консоль с учётной записью **atom** пользователю должны автоматически передаваться максимальные полномочия.

5. Настройте пароль **asa** на режим enable.

3. Настройте технологию SSL VPN с помощью Cisco AnyConnect.
    1. Используйте пакет openconnect на LINNET для проверки соединения.
    2. Настройте автоматическое подключение с проверкой пользователя по сертификатам.
    3. Весь трафик от клиента должен передаваться через это соединение.
4. Настройте соединение IPsec с помощью IKEv1 между ASA и HQ1
    1. Используйте следующие параметры защиты IKEv1: аутентификация по общему ключу, AES128, SHA, DH5 2. Используйте IPsec с помощью протокола ESP с шифрованием AES128 и хешем SHA.
    3. Необходимо защитить трафик между локальной сетью филиала и сетью LINA в центральном офисе, а также трафик от клиентов AnyConnect.

Настройка сети филиала 2

1. Настройте маршрутизатор LINRTR для обеспечения доступа в интернет для клиентов локальной сети. 1. Настройте сервис DHCP для локальной сети.
    2. Используете адрес LINRTR в качестве адреса DNS сервера для клиентов сети.
    3. Настройте NAT для адресов в локальной сети.
2. Настройте службу DNS на маршрутизаторе LINRTR.
    1. LINRTR должен выполнять трансляцию DNS запросов (DNS Forwarding) от локальных клиентов.
3. Настройте GRE-туннель между маршрутизатором LINRTR и маршрутизатором HQ2 в центральном офисе. 1. На маршрутизаторе HQ2 используйте туннельный интерфейс с номером 2. 2. GRE-туннель на маршрутизаторе LINRTR должен устанавливаться при загрузке операционной системы. 3. Используйте статическую маршрутизацию для обеспечения связи между сетью филиала и сетью LINA в центральном офисе.

Настройка сети филиала 3

1. Настройте на межсетевом экране USG IP-адреса для связи с провайдером и для локальной сети филиала. 2. Настройте на межсетевом экране USG DHCP-сервер. Клиент WINCLI3 должен автоматически получать адрес по DHCP. 1. Используете адрес MOOGLE в качестве адреса DNS сервера для клиентов сети.
3. Настройте NAT и обеспечьте доступ в интернет для клиентов локальной сети.
4. Настройте GRE-туннель между межсетевым экраном USG и маршрутизатором HQ2 в центральном офисе. 1. На маршрутизаторе HQ2 используйте туннельный интерфейс с номером 3.
5. Настройте защиту GRE-туннеля с помощью IPsec.
    1. Используйте IKEv2 с общим ключом.
    2. Используйте шифрование AES256, хеширование SHA256, группу DH15.
6. Настройте протокол динамической маршрутизации OSPF для обмена маршрутами между филиалом и центральным офисом.
    1. Используйте область 3. 2. Объявите сеть филиала в OSPF.

7. На WINCLI3 обеспечьте функционирование Defender Firewall.
8. Введите WINCLI3 в домен AS21.local

Настройка мобильных клиентов

1. На LINNET установите пакет openconnect и настройте его для проверки подключения к VPN на межестевом экране ASA 1. Получите пользовательский сертификат и используйте его для подключения.
    2. VPN соединение должно устанавливаться автоматически после перезагрузки компьютера.
    3. После установления VPN соединения LINNET должен иметь возможность доступа к локальным ресурсам сети по доменным именам зоны AS21.local.
2. На виртуальной машине WINNET:
    1. Сформируйте конфигурационный файл для автоматизации установления VPN соединения.
    2. При подключении к VPN серверу не должен запрашиваться ввод дополнительных параметров.
    3. После установления VPN соединения WINNET должен иметь возможность доступа к локальным ресурсам сети по доменным именам зоны AS21.local.
    4. VPN соединение должно устанавливаться автоматически после перезагрузки компьютера.
    5. В качестве сервера OpenVPN используйте SRV.
    https://strongvpn.com/autoconnect-windows-10-openvpn/ - лучше всего тут расскажут как это делать, там быстрО!

По завершению третьего дня

В конце рабочего дня будет необходимо выключить ВСЕ виртуальные машины.
Включать виртуальные машины можно только по указанию от экспертов.
После завершения выполнения задания будет проведена проверка результатов.
Проверка будет выполняться исключительно по доменным именам.
В случае, если устройство или виртуальная машина недоступны по какой-либо причине (не подходят учётные записи, оговоренные

в задании, нет сетевой связности), дальнейшая проверка этого устройства не проводится.

Таблица 1. Настройки служб DNS.

Устройство	Доменное имя	Тип записи
DC	dc.AS21.local	A, PTR
WINSRV1	winsrv1.AS21.local	A, PTR
WINCLI1	wincli1.AS21.local	A, PTR
WINCLI2	wincli2.AS21.local	A, PTR
WINDMZ	www.AS21.local	A
LINDMZ	web.AS21.local	A
LINDMZ	web.skill39.ru	A
LINDMZ	cloud.AS21.local	CNAME
LINRTR (внутренний адрес)	rtr.AS21.local	A
SRV	srv.AS21.local	A
ASTERISK	sip.AS21.local	A
D1	d1.AS21.local	A, PTR
D2	d2.AS21.local	A, PTR
HQ1	hq1.AS21.local	A, PTR
HQ2	hq2.AS21.local	A, PTR
A1	a1.AS21.local	A, PTR
A2	a2.AS21.local	A, PTR
CR1	cr1.AS21.local	A, PTR
CR2	cr2.AS21.local	A, PTR

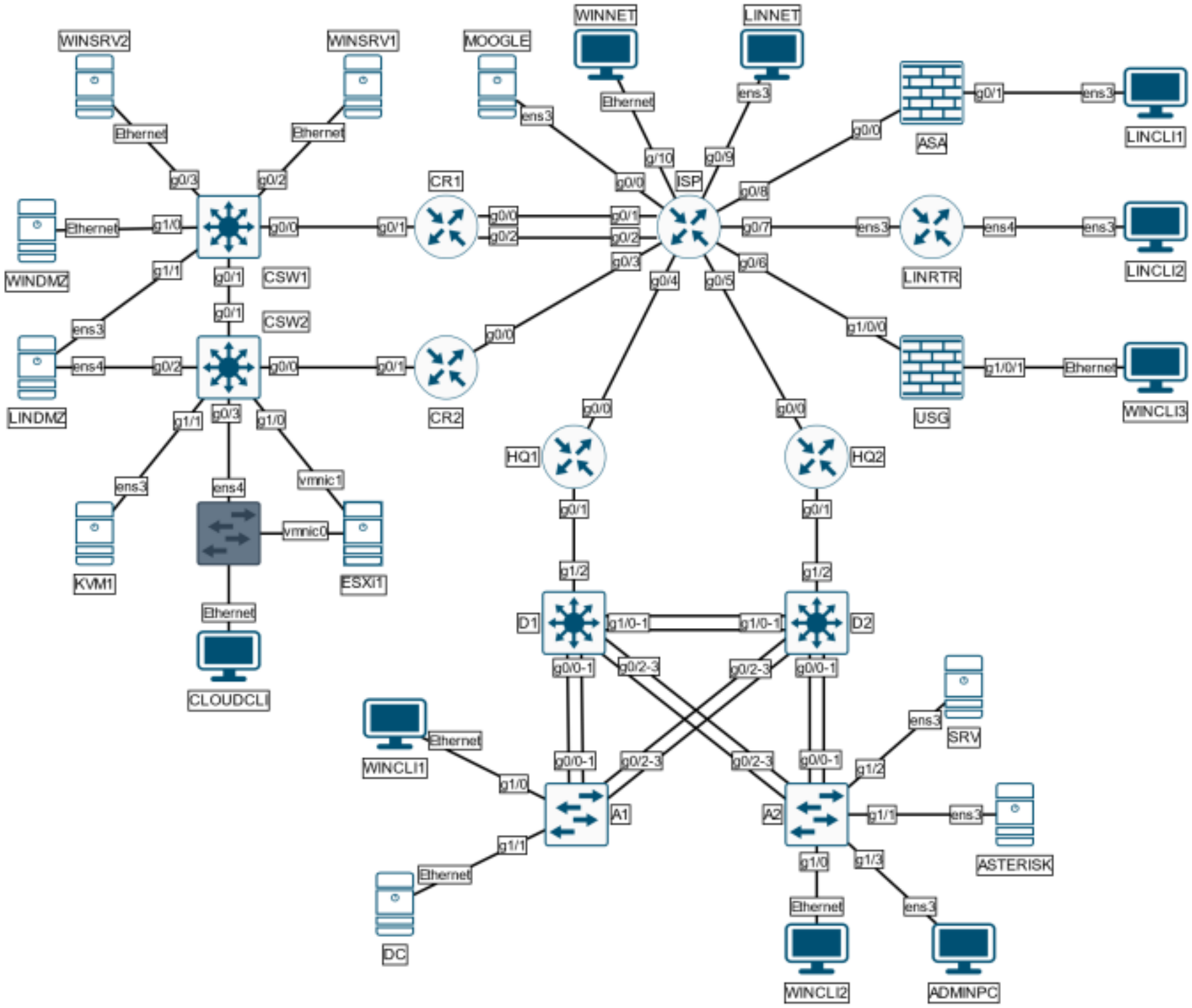
Устройство	Доменное имя	Тип записи
CSW1	csw1.AS21.local	A, PTR
CSW2	csw2.AS21.local	A, PTR
HQ1	test.AS21.local	A, PTR
D1	test.AS21.local	A, PTR

Таблица 2. Правила журналирования.

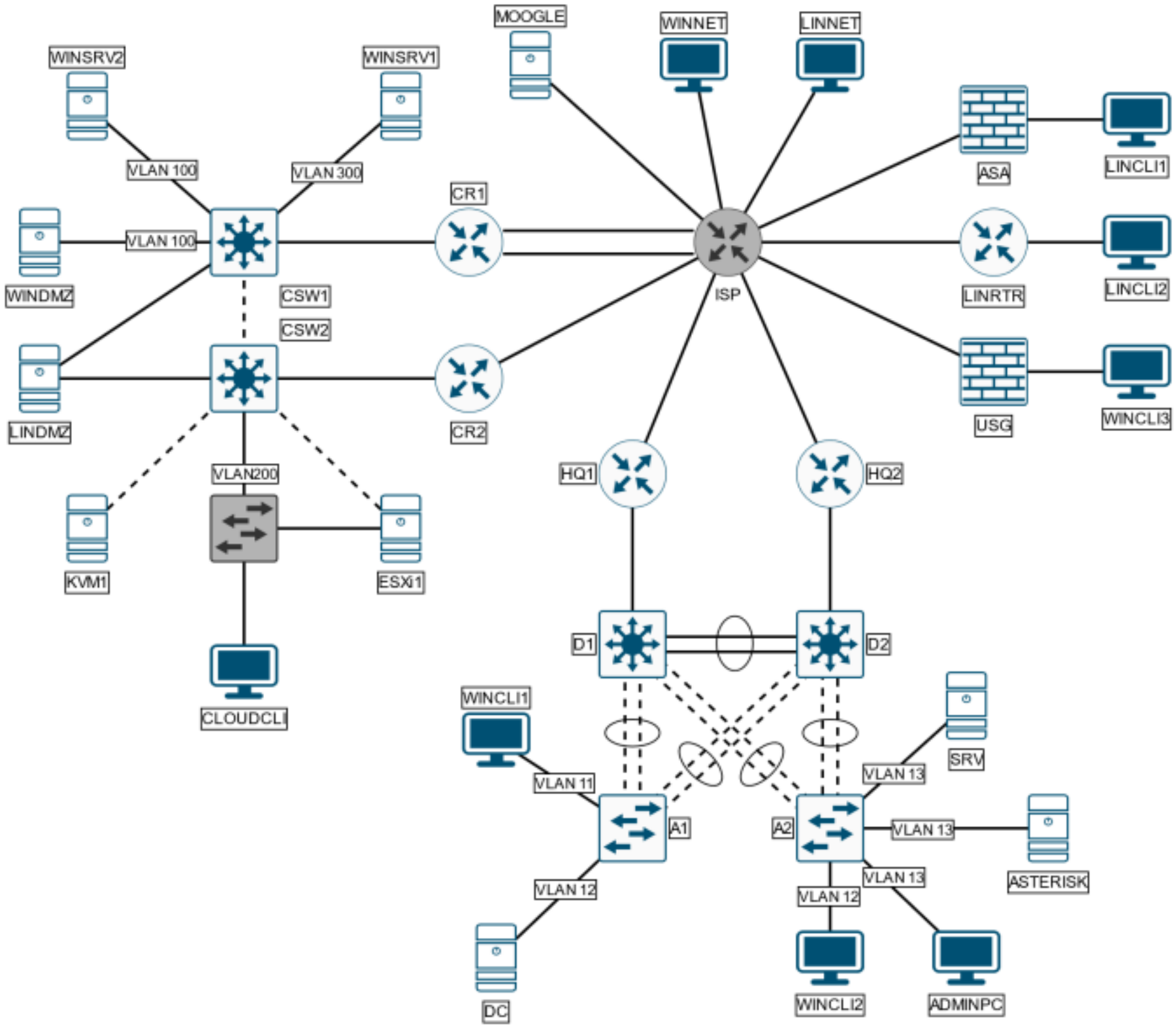
Устройство	Тип сообщений	Файл
ASTERISK	auth, authpriv	/opt/logs/auth/<hostname>.log
Сетевые устройства	Все notification и более важные	/opt/logs/net/<ip>.log
SRV	Error и более важные	/opt/logs/local/errors.log

* где **<hostname>** должен быть заменён на имя устройства и **<ip>** должен быть заменён на IP адрес устройства.

Топология L1



Топология L2



Топология L3