5 виртуальных машин:

V-1-Adm (ЦУС, УКЦ, ПО Client)

V-1-Coord

V-1-Open (БД SQL)

V-1-Oper-CA (клиент ЦУС, ПО Client, Registration Point, Publication Service)

V-2-Client (ПО Client)

V-2-Coord

Нулевые снапшоты координаторов

Первичная настройка сети:

На V-1-Adm ip 10.0.0.2, маска 255.255.255.0, основной шлюз 10.0.0.3;

На V-1-Open ip 10.0.0.3, маска 255.255.255.0, основной шлюз 10.0.0.2;

На V-1-Oper-CA 10.0.0.4, маска 255.255.255.0, основной шлюз 10.0.0.1, предпочитаемый DNS-сервер 10.0.0.1;

На V-2-Client ip 192.168.100.2, маска 255.255.255.192, основной шлюз 192.168.100.1, предпочитаемый DNS-сервер 192.168.100.1.

Адаптеры в настройках виртуальных машин: Hardware – Network Adapter - Custom

Admin - VMnet1

Open - VMnet1

OperCA - VMnet1

V-1-Coord - VMnet2, VMnet1, VMnet0, VMnet0

V-2-Coord - VMnet2, VMnet3, VMnet0, VMnet0

V-2-Client - VMnet3

СНАПШОТ!

На V-1-Open нужно установить .NET Framework 3.5 либо через Интернет, либо установив какую-то штуку (Win10-2004-20H1-DotNet3.5, запустить с правами админа): Программы – Включение или отключение компонентов Windows.

Распаковать SQL на диск С, установить:

* Новая установка изолированного экземпляра SQL Server
* Условия лицензии: Я принимаю
* Центр обновления Майкрософт – далее, обновление продукта – далее,
* Правила установки хз
* Выбор компонентов: компоненты – далее
* Настройки экземпляра: Именованный экземпляр WINNCCSQL
* Конфигурация сервера: Ядро СУБД Авто, Обозреватель Авто
* Настройка компонента: Конфигурация сервера - Смешанный режим, FILESTREAM – три галочки

Далее в диспетчере конфигурации SQL: Сетевая конфигурация SQL Server – Протоколы для WINNCCSQL включить протоколы TCP/IP, Именованные к…

Зайти в службы SQL Server и перезагрузить сервер. Настройка клиента – Клиентские протоколы: 1 Общая память, 2 TCP/IP, 3 Именованные к…

На V-1-Adm установить ЦУС Сервер подключившись к базе данных: Имя сервера 10.0.0.3/WINNCCSQL, Проверка подлинности SQL Server, имя пользователя sa и пароль. Установить ЦУС Клиент. Установить УКЦ. Установить ViPNet Client.

На V-1-Oper-CA, V-2-Client установить ViPNet Client.

Первый вход в ЦУС на V-1-Adm, имя/пароль Administrator. ДО ЛИЦЕНЗИИ СДЕЛАТЬ СНАПШОТ! Настроить структуру защищенной сети самостоятельно. В соответствии с заданием.

Координаторы:

Coord Office, роли удалить, добавить Coordinator HW-VA;

Coord Sub, роли удалить, добавить Coordinator HW-VA, адреса во внешних сетях 192.168.100.1;

Межсерверные каналы

Клиенты:

Admin на Coord Office, роли Business Mail, VPN-клиент, Обмен сообщениями и файлами (ну и изначально стоит Network Control Center).

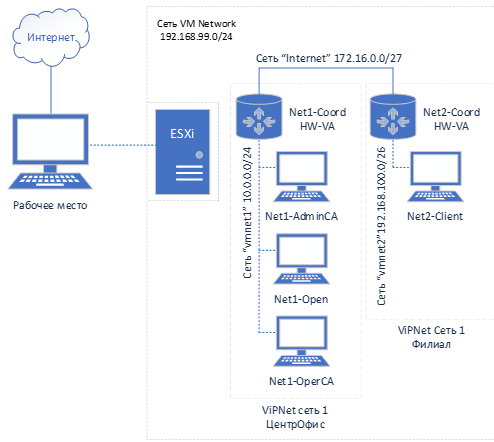
Пользователь 2 на Coord Sub, роли Business Mail, VPN-клиент, Обмен сообщениями и файлами.

Оператор УЦ на Coord Office, роли Business Mail, VPN-клиент, Обмен сообщениями и файлами и плюс !Registration Point!

СНАПШОТ! Настроить связи с пользователями по заданию.

Вход в УКЦ. Настройка новой базы данных. SQL-сервер 10.0.0.3\winnccsql далее, собственный пароль. Ключевой центр – группы узлов – вся сеть, поменять пароль. Сетевые узлы – у каждого поменять пароль. Выделить все сетевые узлы – Выдать новый дистрибутив ключей. Скопировать папку с дистрибутивами. Сетевые узлы – Создать и передать ключи в ЦУС. Пользователи – Ключи пользователей – Создавать ключи электронной подписи (В итоге создание ключей – не будут создаваться). Пользователи – Ключи пользователей – Создать и передать ключи в ЦУС (В итоге статус ключей – переданы в ЦУС).

Далее в ЦУС Справочники и ключи – Создать справочники – Создать для всего списка. На каждого пользователя устанавливаем ключи из скопированной папки дистрибутивов (V-1-Adm, V-1-Oper-CA, V-2-Client) СНАПШОТ!



Переходим к настройке координаторов.

Coord Office user/user 2, Europe - Russia - Urals, время, cd

Eth0 UP, StaticIP, 172.16.0.1/255.255.255.224, UP

Eth1 StaticIP, 10.0.0.1/255.255.255.0,

Eth2 DOWN

Eth3 DOWN

IP-address 172.16.0.2

DNS OFF

Enter hostname coordoffice, next, VPN no, yes

Coord Sub user/user 2, Europe - Russia - Urals, время, cd

Eth0 UP, StaticIP, 172.16.0.2/255.255.255.224, UP

Eth1 StaticIP, 192.168.100.1/255.255.255.192,

Eth2 DOWN

Eth3 DOWN

IP-address 172.16.0.1

DNS OFF

Enter hostname coordsub, next, VPN no, yes

После настройки координаторов меняем IP:

На V-1-Adm ip 10.0.0.2, маска 255.255.255.0, основной шлюз 10.0.0.1;

На V-1-Open ip 10.0.0.3, маска 255.255.255.0, основной шлюз 10.0.0.1;

В ЦУС в координаторах статус справочников и ключей – готовы к отправке. Отправить справочники и ключи. В УКЦ Пользователи – Ключи пользователей – Создать ключи электронной подписи. Пользователи – Ключи пользователей – Создать и передать ключи в ЦУС. Отправить справочники и ключи (Статус отправлены). Зайти в ViPNet Client везде и проверить сеть. СНАПШОТ!

На V-1-Open установить ЦУС Клиент.

На V-1-Adm заходим в ViPNet Client Фильтры открытой сети – Создать – КлиентЦУС, пропускать трафик; Источники – Добавить – IP-адрес или диапазон адресов – 10.0.0.3; Назначения – Мой узел; Протоколы – Добавить – Протокол TCP/UDP – Порт назначения от 9000 до 9900.

В ЦУС добавить учетную запись admindb. Войти под этой учетной записью в V-1-Open.

На V-1-Adm в строке браузера написать 10.0.0.1:8080, войти как администратор. Локальные фильтры открытой сети – Добавить – HTTP8080, Фильтр включен, пропускать трафик; Источники – Добавить – IP-адрес или диапазон адресов – 10.0.0.3; Назначения – Мой узел; Протоколы – Протокол TCP/IP – Номер порта 8080; В V-1-Open в браузере написать 10.0.0.1:8080.

На V-1-Adm в УКЦ – Сервис – Настройки – Программные средства – Функционировать в режиме аккредитованного удостоверяющего центра поставить галочку; Автоматический режим – переходить в автоматический режим работы через 15 мин;

Данные из задания

Средства удостоверяющего центра - Программные средства: Средство электронной подписи издателя – ViPNet CSP; Средство удостоверяющего центра – ПК ViPNet УЦ 4;

Сертификаты соответствия: Сертификат на средство эп издателя – Demo.lab.crt, Сертификат на средство удостоверяющего центра - Demo.lab.p7b.

На V-1-Adm вкладка Администрирование – Корневые сертификаты – кнопка Создать – данные по заданию. Вкладка Ключевой центр – Пользователи – Пользователь 2, Oper-CA, Admin – Ключи пользователя – Создать и передать ключи в ЦУС.

Пользователь 2 – Ключи пользователя – Создать ключи электронной подписи и сохранить в файл на рабочий стол. Потом проверить чтобы все ключи были созданы и переданы в ЦУС в Сетевые узлы. В ЦУС отправить справочники и ключи. 56мин

На V-1-Adm Client Сервис-Настройка параметров безопасности-Электронная подпись (Статус -действ, кем выдан- администратор сети). Сервис-Настройка-Публикация данных: скопировать путь -папка с сертификатами, предназначенными для публикации. Перейти по этому пути и сделать папку Publication с общим доступом: Свойства-Доступ-Общий доступ-Поделиться-скопировать Сетевой путь.

В УКЦ-Действия-Обновлять списки аннулированных сертификатов: каждый 1 день, Передавать все CRL в Центр управления сетью: каждый 24 часа, по заданию!

На V-1-Oper-CA Текущий сертификат ЭП не найден-Настройка параметров безопасности-ЭП-Выбрать-Установить сертификат-Далее, далее. Установка корневого сертификата – ОК

Установить Registration Point, Publication Service.

Заходим в Registration Point – Настройка-Папка ключей сетевого узла-ProgramData-InfoTeCS-Цифры. Войти и закрыть пока.

Сеть-Правой кнопкой мыши-подключение сетевого диска- [\\10.0.0.2\Publication](file:///\\10.0.0.2\Publication) (не рабочая версия из видео [\\V-1-ADM\Publication](file:///\\V-1-ADM\Publication)). Ввод сетевых учетных данных User-xxXX1234. Потом происходит волшебное подключение.

Потом запускаем Publication Service, выбираем запустить Publication Service. Настройки-Папка приема файлов из УКЦ Z:\Out, Папка отправки файлов в УКЦ Z:\In

Далее веселье с FTP-сервером. Устанавливаем Filezilla. I agree, Next…

Connect to Server. Server-Configure-Rights management: Users. Add – User 1. Локальный диск - Создать папку Pub-pubsvr-data. В свойствах папки Pub – Безопасность – все разрешения. Справа Add Virtual path /, Natrive path C:\Pub – Apply. Далее в проводнике прописать <ftp://10.0.0.4/> Пользователь User1 Проверить можно ли подключиться к ftp серверу. В Publication Service зайти с правами администратора Публикации-Добавить-Сертификаты издателей- Тип хранилища FTP-сервер-10.0.0.4 порт 21, абсолютный путь до каталога -/ , Проверить указанные параметры-Готово.

На V-1-Adm зайти в УКЦ, выделить все сертификаты и опубликовать.

На V-1-Oper-CA зайти на ftp-сервер <ftp://10.0.0.4/> Если нету опубликованных, то зайти в журнал и обновить. Появятся папки с опубликованными сертификатами. СНАПШОТ

Заходим в Registration Point-Пользователи-правой кнопкой мыши зарегистрировать пользователя- User 2. User 2- правой кнопкой мыши- сертификаты-создать запрос-далее далее.

На V-1-Adm зайти в УКЦ-Внешние пользователи. Если не приходит опросить транспортный модуль. Ключевой центр-Пользователи-Запросы на дистрибутивы ключей-Удовлетворить-далее далее. Удостоверяющий центр-Запросы на сертификаты-Необработанные запросы-Запросы центров регистрации-Удовлетворить.

На V-1-Oper-CA заходим в Registration Point – Запросы-Запросы на сертификаты-Отправленные-посмотреть чтобы статус был Удовлетворен.

Далее заходим в сертификаты и все приостанавливаем. Транспортный модуль на опере и админе чтобы быстрее пришло. На V-1-Adm в УКЦ-Удостоверяющий центр-Запросы на аннулирование сертификатов-выделяем все и удовлетворить. В Registration Point на V-1-Oper-CA Сертификаты-Статус Приостановлен. Далее аннулируем сертификаты.

На V-1-Adm зайти в УКЦ - Удостоверяющий центр-Необработанные запросы-Удовлетворить. В Registration Point на V-1-Oper-CA Сертификаты-Статус Аннулирован.

СНАПШОТ

На V-1-Adm установить CA Informing, запустить Настройки Способ выдачи уведомлений– сохранять в папку – создать папку на рабочем столе CA, Свойства сообщений с уведомлениями: Отображаемый адрес OperCA@demo.lab, Отображаемое имя OperCA, OperCA@demo.lab , База данных удостоверяющего центра: Тип базы данных – SQL Server УКЦ 4x , Строка подключения к базе данных

Data Source=10.0.0.3\winnccsql;Initial Catalog=ViPNetAdministrator;User:Id=KcaUser;Password=Number1;

Кросс сертификаты можно не настраивать, если в задании нет.

Путь сохранения отчетов – созданная папка CA. Проверить настройки!

Отчеты-Добавить-Сохранить файл с сертификатами, Путь для сохранения – СА, Фильтрация сертификатов E-MAIL, город, имя (по заданию) – ОК. Выполнить. Проверяем отчет в папке СА. СНАПШОТ

На V-1-Oper-CA TSP-OCSP Service скачать. В поиске найти Создание запроса на сертификат. Шаблон сертификата: Для TSP-сервера

Адрес электронной почты: [TSP@demo.lab](mailto:TSP@demo.lab)

Подразделение: IT

Город: Казань

Область: Республика Татарстан

Страна: RU

Сохранение запроса в файл: создать папку на рабочий стол TSP. Сформировать запрос в созданную папку. Затем скинуть файл в общую сетевую папку Publication или можно этот файл с запросом через флешку перенести на V-1-Adm. Далее в УКЦ - Удостоверяющий центр – Внешние пользователи – Загрузить и обработать запрос – на флешке выбрать файл с запросом TSP – Издать сертификат. Файл с изданным сертификатом перекинуть на V-1-Oper-CA. На V-1-Oper-CA открыть ViPNet CSP – Добавить контейнер - Инициализация контейнера ключей – Папка на диске – Созданная папка TSP – ок. Установить сертификат – Сертификат изданный на админе – далее, далее – ок. Настройка параметров – Запустить TCP – Действия – Настроить сервер – Серийный номер 01 00 00 00 00 00 00 00. Создать – Идентификатор объекта политики – 1.2.643.100.1.2.3 Закрыть и заново открыть. Установить сертификат: кликнуть по нему – локальный компьютер – поместить все сертификаты в следующее хранилище – Личное- Готово. Службы УЦ – Службы TCP – Выбрать сертификат – Должен появиться сертификат, выбрать его.

На V-1-Adm в УКЦ – Пользователи - Пользователь 2 – Считать ключи скомпрометированными - Да. Пароль – Сменить. Сетевые узлы – Выбрать Admin, CoordSub, Пользователь 2 (те, у кого статус ключей требуется создать) – Создать и передать в ЦУС. Затем заходим в ЦУС – отправить справочники и ключи – ТОЛЬКО НА ПОЛЬЗОВАТЕЛЯ 2. На V-1-Adm в УКЦ – Пользователи – Пользователь 2 – Ключи пользователя – Создать и сохранить РНПК в файл – на рабочем столе создать папку РНПК – ОК. Пользователь 2 – Создать и передать ключи в ЦУС. Потом переходим в ЦУС – Отправить справочники и ключи - ТОЛЬКО НА ПОЛЬЗОВАТЕЛЯ 2.

На Client 2 подергать транспортный модуль. ViPNet Client должен вылететь и потухнуть все узлы.

На V-1-Adm в УКЦ – Сетевые узлы – Oper CA, CoordOffice (статус CRL неактуальные) – Создать и передать ключи в ЦУС.

На Client 2 должно выйти предупреждение – срок действия текущего пароля пользователя истек сменить пароль – пароль сохранить в файл. Далее предупреждение – текущий сертификат электронной подписи недействителен – выбрать другой demo.lab. Далее установка корневого сертификата – ОК.

На V-1-Adm в ЦУС – Отправить справочники и ключи – Отправить на весь список. На V-1-Adm в ViPNet Client должен потухнуть Пользователь 2. Далее на Client 2 должно все восстановиться, все узлы должны гореть. На админе тоже. Вуаля.