Про корневой сертификат УКЦ – администрирование – коневые каталоги - нажать создать каталог.

Устанавливаем 6 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

Сделать 0 снапшоты.

Поставить IP адреса.

На машине Open подключаем фреймворк для этого установить WIN10 ОТКРЫТЬ ЧЕРЕЗ АДМИНИСРАТОРА (лежит в дистрибутивах/випнетсофт). Устанавливаем SQL. Зайти в программу подключить необходимые настройки.

Устанавливаем ЦУС и УКЦ на админ сервер и клиент. На других машинах Устанавливаем клиент, кроме опена. Перед установкой лицензии сделать снапшот.

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!.

Создать и отправить справочники.

Зайти в УКЦ . 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. При выдачи дистрибутива пишем другой пароль у пользователей.

Сетевые узлы – создать и передать В ЦУС. Пользователи – снять галочку – нажать передать в ЦУС.

Еще раз отправить справочники. Разнести ключи по пользователям.

Настройка Кордов. После изменить шлюз у админа и опена.

Псоле перейти в УКЦ. Перейти в пользователи и поставить галочку, и нажать создать и передать в цус.

Зайти на опен и установить цус, пока не настраивать.

Перейти 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.

Зайти в ЦУС внизу (слева маленький сертификат). Нажать создать учетную запить. Создать admindb.

Перейти в опен вбить admindb и поменять пароль далее.

Перейти в админ, зайти в интернет 10.0.0.1:8080. Сверху зайти как администратор. Межсетевой экран - локальные фильтры открытой сети – добавить – Имя HTTP8080, Фильтр включен, пропускать трафик. источники 10.0.0.3. назначение мой узел. Протоколы 8080. Применить все/

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 УКЦ вкладка Администрирование – Корневые сертификаты – кнопка Создать – данные по заданию имя demo.lab почта [админ@demo.lab](mailto:админ@demo.lab) в должности администратор

4)При выдаче сертификатов необходимо заполнить следующие поля:

Имя: <Имя пользователя или узла>

Электронная почта: <Имя пользователя>@demo.lab

Город: Казань

Область: Республика Татарстан

Страна: RU

Организация: ФИРПО

Подразделение: Отдел информационной безопасности

Почтовый индекс: 123123

Вкладка Ключевой центр – Пользователи – Пользователь 2, Oper-CA, Admin – Ключи пользователя – Создать и передать ключи в ЦУС. Вбить данные (казань и тд)

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

Сетевые узлы - Оператор УЦ – создать и передать в ЦУС.

Создать / передать справочники.

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.

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

У меня он никогда не выходил 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 на машине опер

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 (не рабочая версия из видео \\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.

(Установить filezilla, добавить пользователя администратор или попробовать User1. Изменить папку , нужно создать Pub. Попробовать зайти в ftp server ftp://10.0.0.4 /

Перейти в публикейшен – публикации – сертификаты издателей – ftp сервер 10.0.0.4. в конце проверить подключение.)

Зайти в свойства ПАБ (ОПЕР) открыть безопасность добавить юсер 1(но это не получилось). Потом почемуто меняет имя на админ на файл зилла.

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. Перейти в УЦК на админе- удостоверяющий центр – пользователи моей сети -выделить все и опубликовать. В Сервис публикации должно появится 2 сертификата, но почему-то у меня они не появились, а это значит, что где-то ошибка. Потом как то они должны появится на ftp сервере. Но они так же там не появились.

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.

Создать в регистрейшен поинт пользователя ЛКМ, в завершении поставить галочку на создать запрос на дистрибутив ключей. Заходим в Registration Point-Пользователи-правой кнопкой мыши зарегистрировать пользователя- User 2. User 2- правой кнопкой мыши- сертификаты-создать запрос-далее далее.

Нажать на пользователя создать сертификат. Перейти в УКЦ в Уд должен появится сертификат, нажать удовлетворить. Перейти в сертификат и приостановить сертификат. В УЦК удовлетворить. Затем аннулировать и удовлетворить в УКЦ.

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.

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

Подразделение: IT

Город: Казань

Область: Республика Татарстан

Страна: RU

TSP ничего не понятно

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.

(Зайти в CSP добавить контейнер указать файл TSP. Затем необходимо сертификат перенести с флешкой на админ зайфти в УКЦ Удостоверяющий центр – внешние пользователи загрузить сертификат – и издать. Перенести на флешке на Опер и установить на лок ком , личное.)

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.