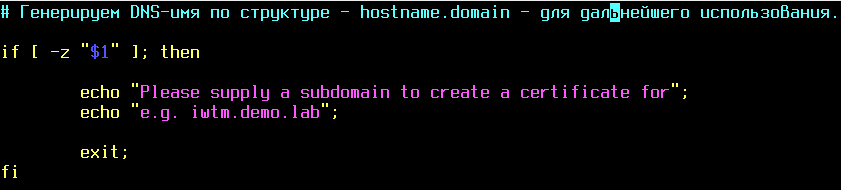
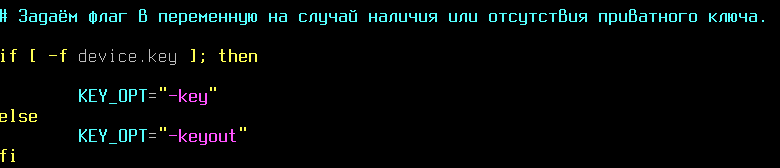
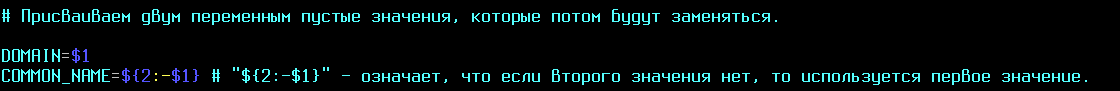
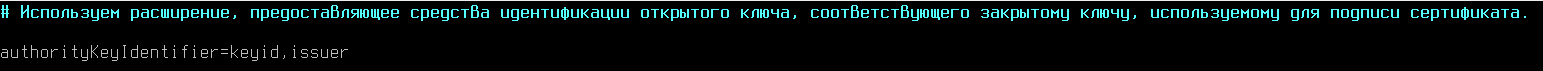
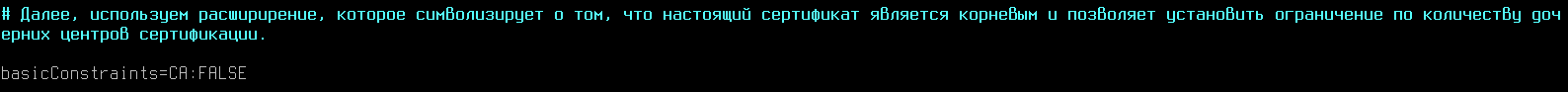
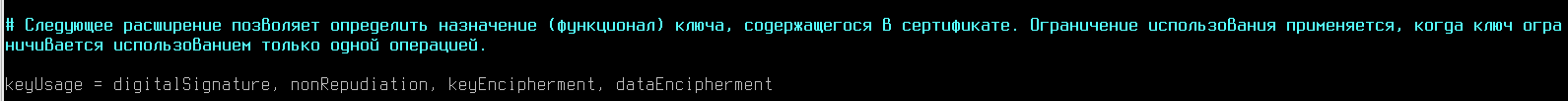
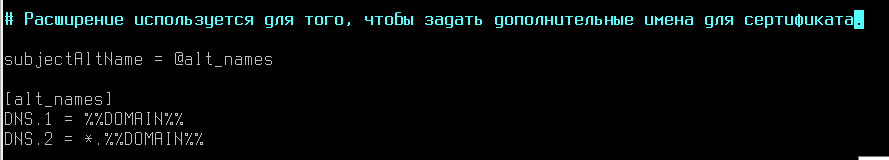
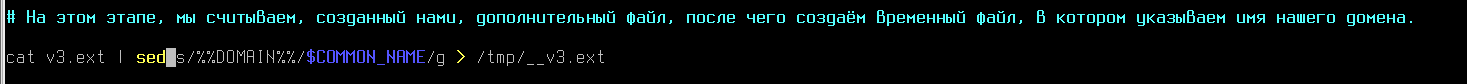
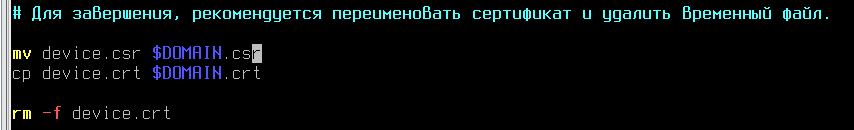
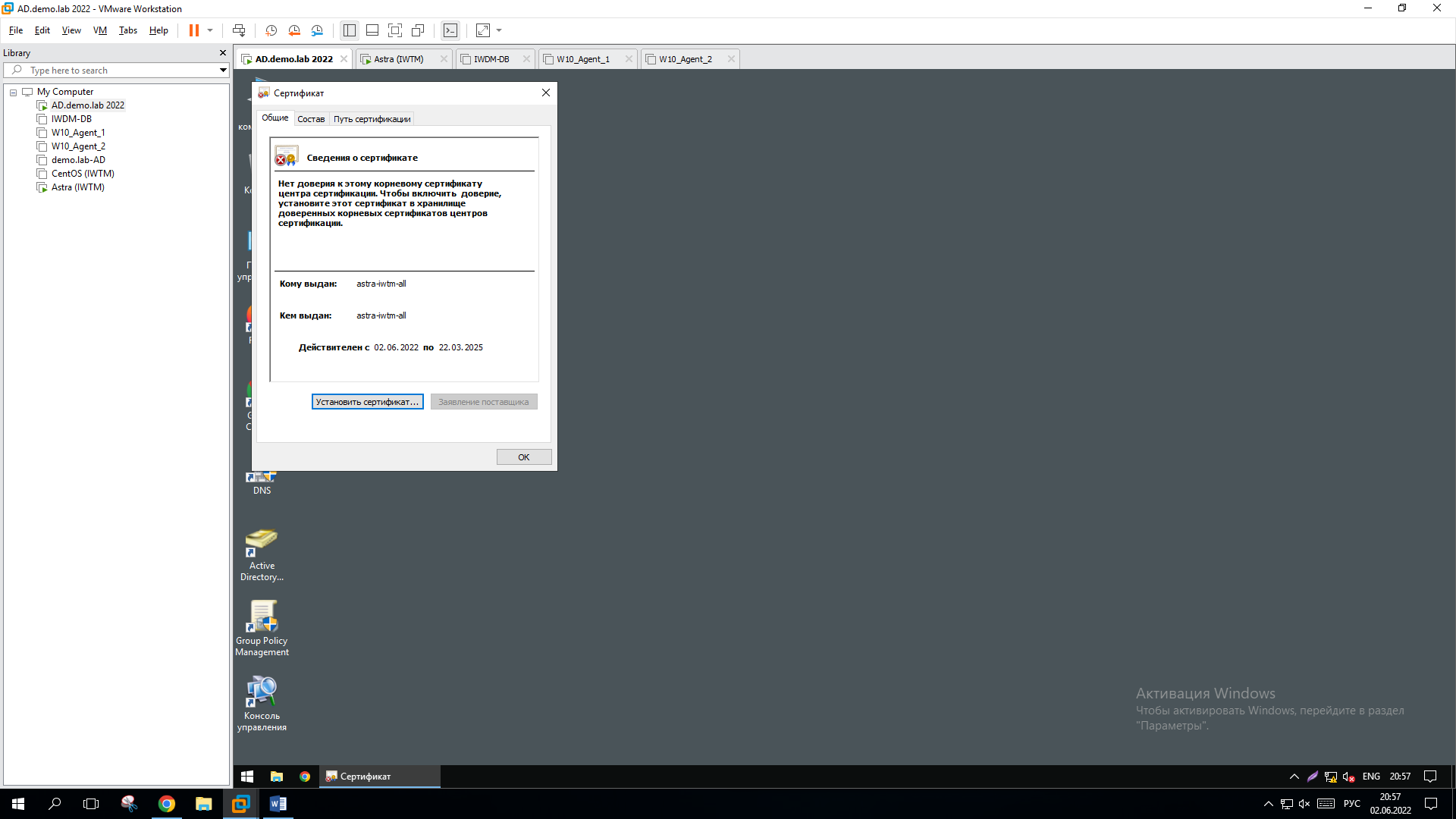
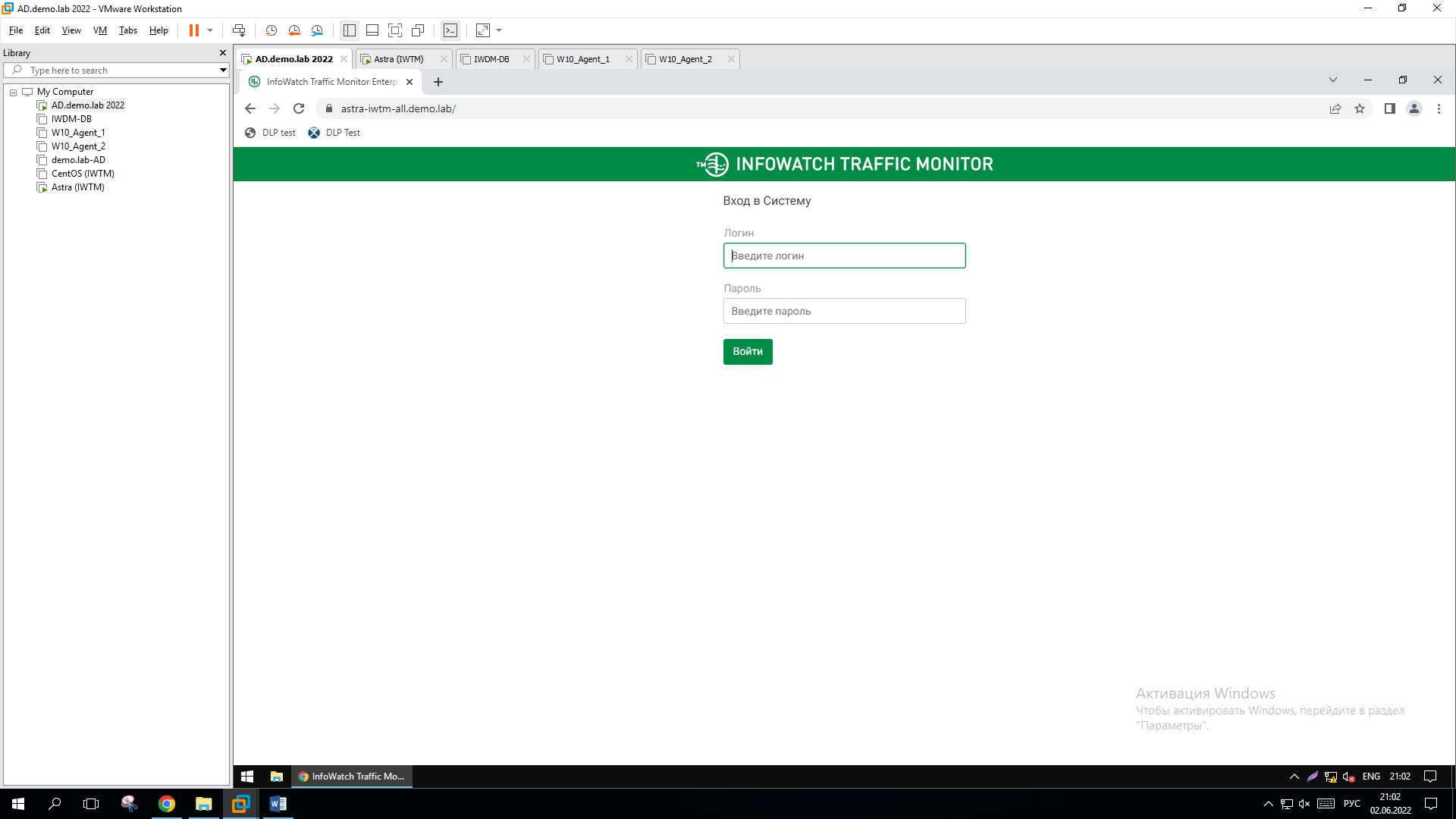
**Алгоритм создания сертификата**

1. Генерируем закрытый (2048 битный) ключ для корневого сертификата; − **(openssl genrsa -out rootCA.key 2048);**
2. Генерируем запрос и на корневой сертификат и подписываем его – **(openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem);**
3. Создаём файл, в котором будем создавать сертификат сервера − **(touch file\_name.sh);**
4. Заходим в него и следуем инструкции из скриншотов;
5. 
6. 
7. 
8. 
9. После проделанных шагов, сохраняем и выходим из файла и создаём новый файл, который будет задавать основные параметры серверного сертификата, для обеспечения его валидности – **(touch file\_name.ext);**
10. Заходим в него и следуем инструкции по аналогии;
11. 
12. 
13. 
14. 
15. На этом этапе, сохраняем и закрываем этот файл, после чего, возвращаемся в предыдущий файл;
16. 
17. 
18. 
19. После, мы выходим и сохраняем файл, и запускаем его – **(./file\_name.sh «DNS-имя»);**
20. По завершению работы, заходим в конфигурационный файл – **(nano /etc/nginx/conf.d/iwtm.conf;**
21. Далее находим ниже указанные строки− 
22. Меняем 2 значения на – ssl\_certificate **/(полный путь до сертификатов)/сертификаты.**

Вид у меня – 

1. После проделанной работы, выходим из файла и проверяем на наличие ошибок сервис **nginx,** с помощью команды – **nginx –t;**
2. Если всё в порядке, перезапускаем сервис с помощью команды – **service nginx restart;**
3. По окончанию этих задач, мы должны перейти на доменную машину и через утилиту - **WinSCP,** подключиться к IWTM, а потом, забрать, **ВНИМАНИЕ, КОРНЕВОЙ СЕРТИФИКАТ,** не серверный.
4. Выгружаем его на рабочий стол доменной машины и устанавливаем его. 
5. **ВАЖНО,** установить нужно сертификат на Доверенные корневые центры сертификации. (ПУНКТ – Хранилище сертификатов)
6. Наконец, после установки, заходим в браузер и вводим в url – полный DNS−адрес Вашего веб−сервера.



**Всё, начальные настройки сертификатов завершены, далее можно будет установить сертификаты клиентов и создавать древо сертификатов.**

*Очень полезные сайты – (*[*https://www.opennet.ru/base/sec/openssl.txt.html*](https://www.opennet.ru/base/sec/openssl.txt.html)*,* [*https://www.opennet.ru/docs/RUS/ldap\_apacheds/tech/ssl.html#single-root*](https://www.opennet.ru/docs/RUS/ldap_apacheds/tech/ssl.html#single-root) *и* [*https://pki-tutorial.readthedocs.io/en/latest/expert/component-ca.conf.html*](https://pki-tutorial.readthedocs.io/en/latest/expert/component-ca.conf.html)*)*