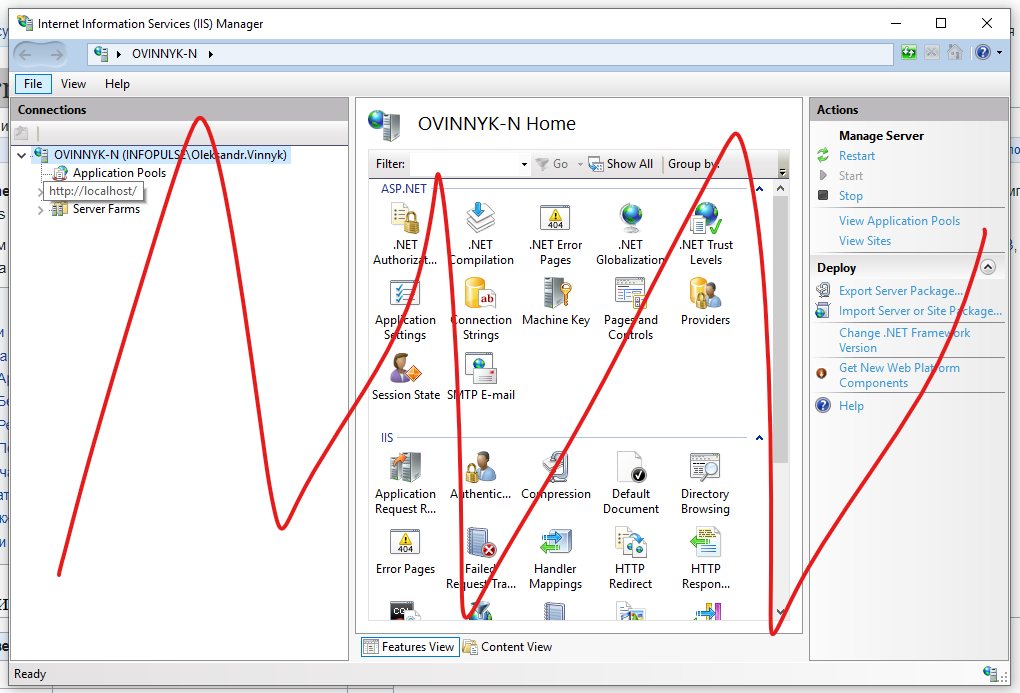
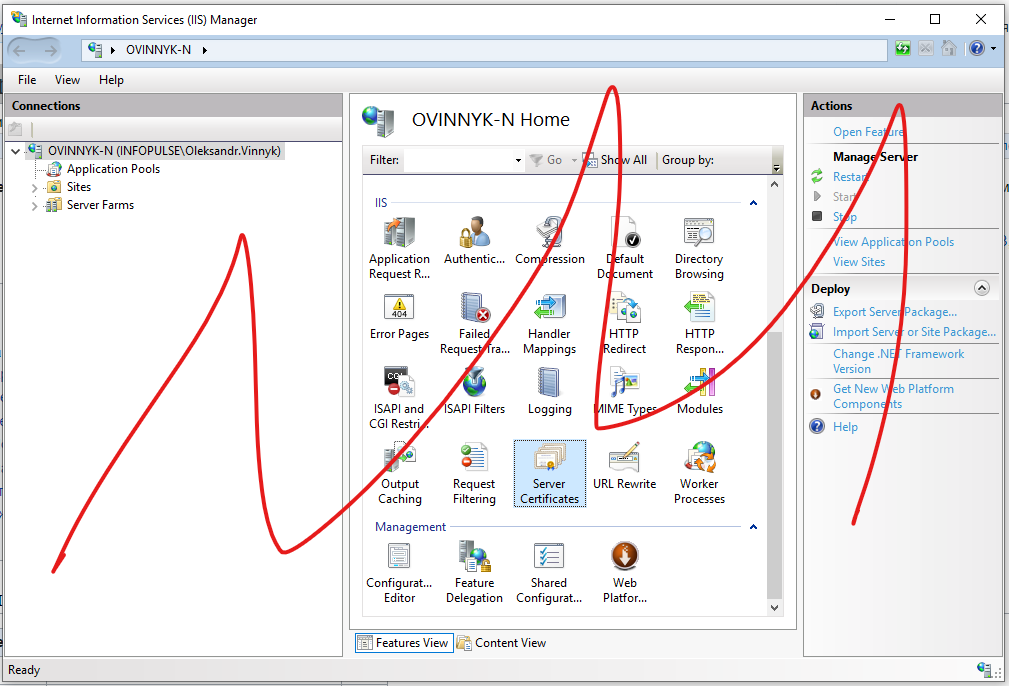
# Процедура розгортки застосунку

Даний розділ описує процедуру розгортання застосунку для його подальшого застосування.

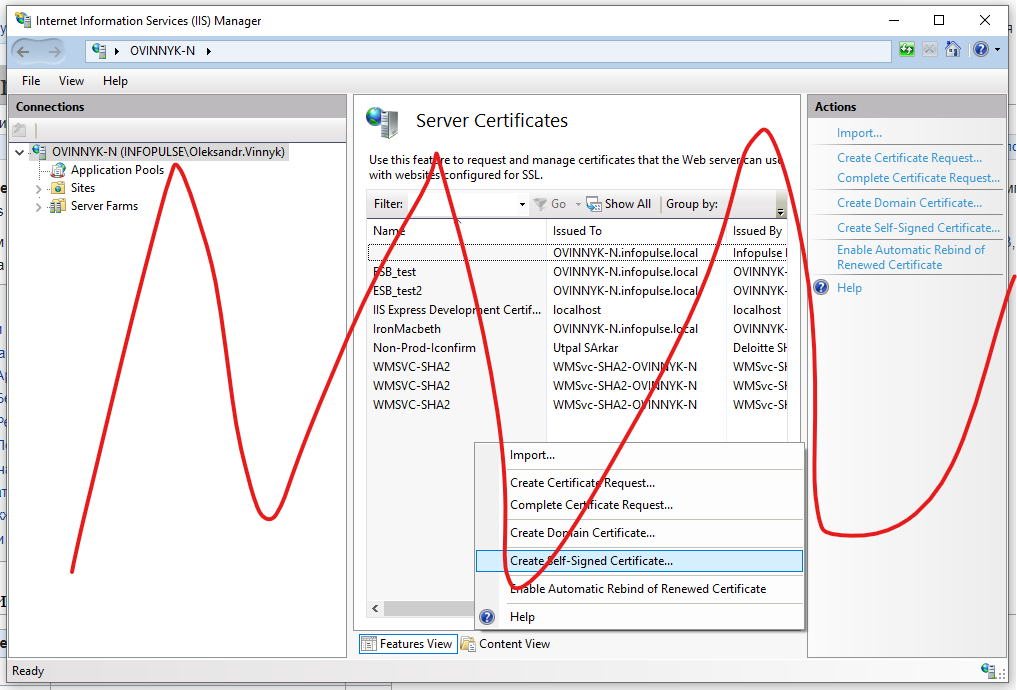
1. Як описано у розділі «» застосунку для безпечної роботи необхідно мати сертифікат стандарту X.509. Якщо застосунок планується розгортати для використання кінцевими користувачами (Production/Live environment), необхідно придбати дійсний сертифікат у дійсному центрі сертифікації (англ. Certification authority, CA). У разі розгортання з іншою метою допустимим є використання самозавіреного сертифікату (англ. Self-signed certificate). Подальші підпункти описують створення самозавіреного сертифікату (За необхідності можна використовувати сертифікат за шляхом «SolutionFiles\Cert.pfx», пароль «123»):
   1. Створення самозавіреного сертифікату використовуючи утіліту IIS:
      1. Відкрити утіліту Internet Information Services (IIS)



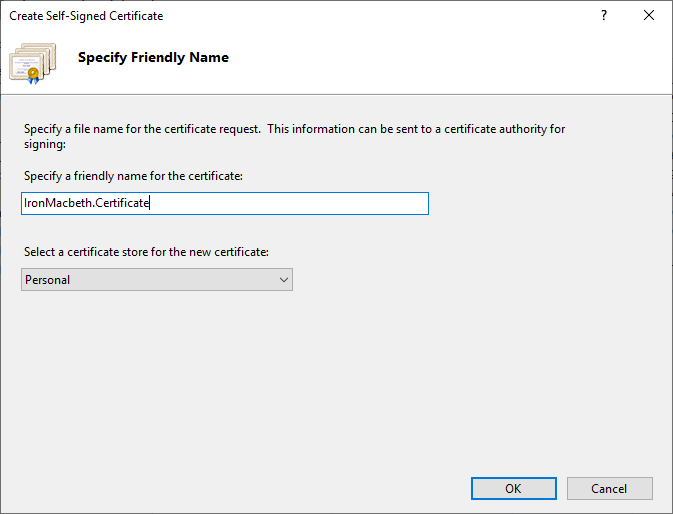
* + 1. Обрати розділ «Server Certificates»



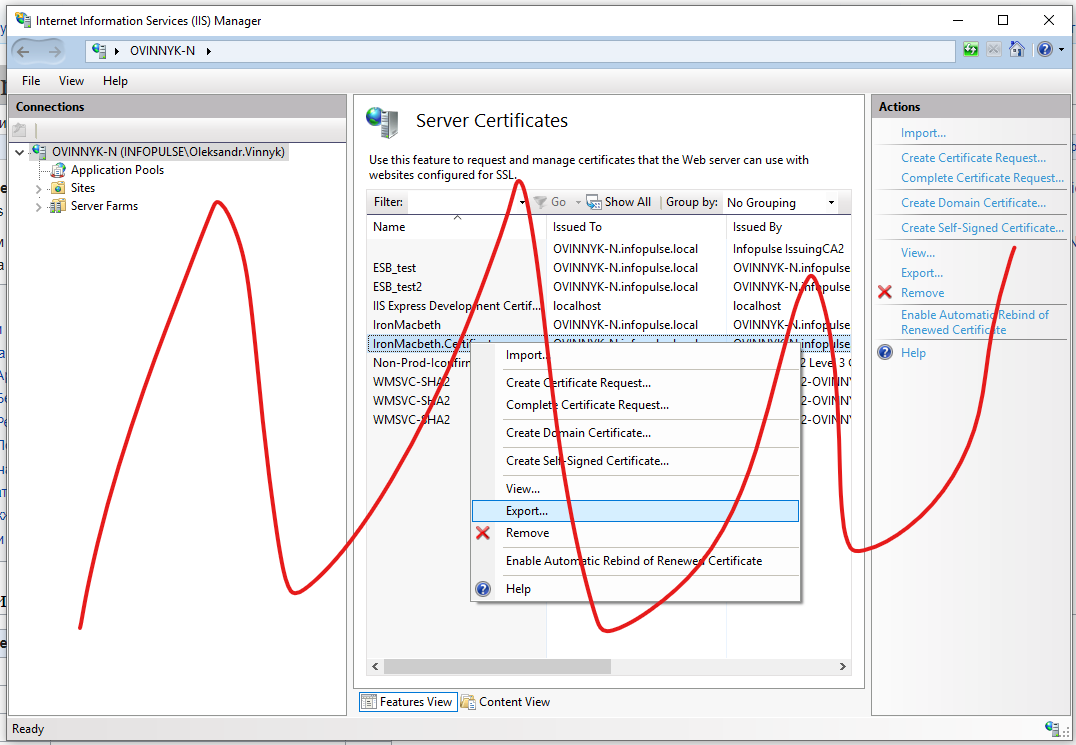
* + 1. Натиснути ПКМ та обрати опцію «Create Self-Signed Certificate…»



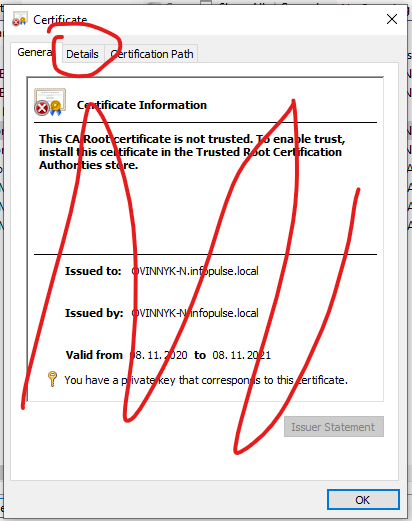
* + 1. У вікні що відкрилось, вказати довільне ім’я сертифікату (наприклад, «IronMacbeth.Certificate»)



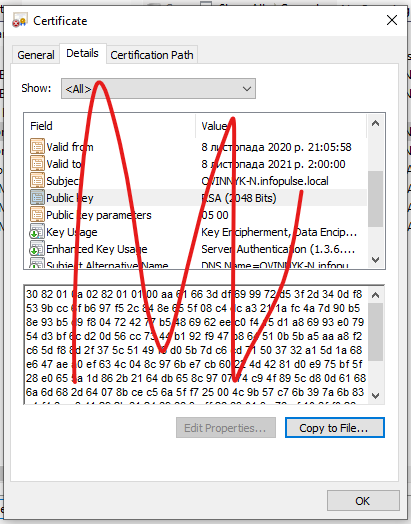
* + 1. Натиснути кнопку «ОК». Сертифікат має з’явитись у списку.
    2. Експортувати сертифікат для його подальшого застосування на необхідній обчислювальній машині. Обрати у списку необхідний сертифікат і натиснути ПКМ. Обрати опцію «Export…»



* + 1. У вікні що відкрилось, обрати зручне місце на носії інформації куди буде експортовано сертифікат, а також захистити сертифікат паролем, який буде необхідний для імпорту сертифіката на необхідній обчислювальній машині.
    2. Експортувати публічний ключ та серійний номер сертифікату
       1. Двічі натиснути ЛКМ на необхідному сертифікаті

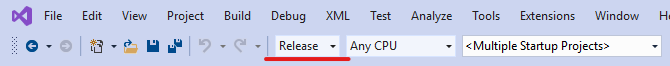


* + - 1. Перейти у вкладку «Details» та знайти у списку полів «Public key» та натиснути кнопку «Copy to File…»



* + - 1. У вікні що відкрилось, натиснути «Next», впевнитись що обрана опція «No, do not export the private key», натиснути «Next», обрати опцію «Base-64 encoded X.509 (.CER)», натиснути «Next», обрати зручне місце на носії інформації куди буде експортовано публічний ключ, натиснути «Finish».
      2. знайти у списку полів «Serial number», скопіювати значення та зберегти у зручному та безпечному місці для подальшого застосування.

1. Створення виконуваних файлів на основі сирцевого коду (хе-хе)
   1. Відкрити Solution «IronMacbeth» використовуючи Visual Studio 2019 або новіше
   2. Обрати «Release» Build configuration



* 1. Виконати компіляцію. Build -> Build Solution.
  2. Після успішного завершення компіляції, скопіювати вміст папок «IronMacbeth\IronMacbeth.BFF\bin\Release», «IronMacbeth.FileStorage\IronMacbeth.FileStorage\bin\Release» та «IronMacbeth\IronMacbeth.UserManagement\IronMacbeth.UserManagement\bin\Release»
  3. У Visual Studio перейти до Solution Explorer, обрати проект «IronMacbeth.Client», натиснути ПКМ та обрати опцію «Publish…».
  4. У вікні що відкрилось, обрати зручний шлях на носії інформації та натиснути «Next», обрати бажану опцію (наприклад From a CD-ROM or DVD-ROM) та натиснути «Next» двічі, а потім «Finish».
  5. Перейти до обраної папки та замінити у конфігураційному файлі «publish\Application Files\IronMacbeth.Client\_1\_0\_0\_0\ IronMacbeth.Client.exe.config.deploy»:
     1. Адреси «IronMacbeth.BFF» сервісу за шляхом «configuration\system.serviceModel\client\endpoint» атрибут «address» у першому і другому елементі «endpoint» відповідно до адрес які будуть відповідати обчислювальній машині на якій розгорнуто «IronMacbeth.BFF» сервіс.
     2. Публічний ключ сертифікату якому має довіряти клієнтський застосунок за шляхом «configuration\system.serviceModel\client\endpoint\identity\certificate» атрибут «encodedValue».
  6. По завершенню розгортання, решти системи розповсюдити отримані файли між користувачами.

1. Розгортання баз даних
   1. Створити 3 бази даних на SQL Server, який буде доступний по комп’ютерній мережі обчислювальним машинам на яких планується розгортати сервіси «IronMacbeth.BFF», «IronMacbeth.FileStorage» та «IronMacbeth.UserManagement».
      1. Запустити Microsoft SQL Server Management Studio та підєднатись до СУБД, яка планується до використання.
      2. У Object Explorer обрати «Databases», натиснути ПКМ та обрати опцію «New Database…».
      3. Вказати ім’я (наприклад «IronMacbeth.BFF.Database», «IronMacbeth.FileStorage.Database» або «IronMacbeth.UserManagement.Database») та натиснути «ОК».
      4. Виконати пункти тричі.
   2. Виконати Publish баз даних
      1. У Visual Studio відкрити Solution Explorer, обрати проект Database\ IronMacbeth.BFF.Database.
      2. Натиснути ПКМ та обрати опцію «Publish».
      3. У вікні що відкрилось, натиснути «Edit», у вікні що відкрилось, обрати підключення для необхідної бази даних та натиснути «ОК».
      4. Натиснути кнопку «Publish».
      5. Дочекатись завершення операції.
      6. Повторити пункти для Database\IronMacbeth.FileStorage.Database та Database\IronMacbeth.UserManagement.Database.
2. Розгортання сервісів
   1. Розмістити файли, отримані у пункті 2.d., на відповідних обчислювальних машинах між якими можливий зв'язок по комп’ютерній мережі.
   2. Сконфігурувати «IronMacbeth.FileStorage» сервіс.
      1. Відкрити файл «IronMacbeth.UserManagement.exe.config» за замінити наступні налаштування:
         1. Connection String до бази даних за шляхом «configuration\connectionStrings\add» атрибут «connectionString». Замінити значення на Connection String до бази даних, у яку був виконаний publish з проекту Database\IronMacbeth.FileStorage.Database.
         2. Trusted certificate за шляхом «configuration\trustedCertificates\add» атрибут «value». Замінити значення на серійний номер сертифікату, який буде використовувати «IronMacbeth.BFF» сервіс при підключенні до даного сервісу.
         3. Service Certificate за шляхом «configuration\system.serviceModel\behaviors\serviceBehaviors\behavior\serviceCredentials\serviceCertificate» атрибут «findValue». Замінити значення на серійний номер сертифікату, що буде використовуватись як серверний сертифікат для сервісу.
         4. Base Address за шляхом «configuration\system.serviceModel\services\service\host\baseAddresses\ add» атрибут «baseAddress». Замінити значення на адресу, за якою інші обчислювальні машини зможуть звернутись до сервісу.
   3. Сконфігурувати «IronMacbeth.FileStorage» сервіс за аналогією до попереднього пункту «4.b.».
   4. Сконфігурувати «IronMacbeth.BFF»
      1. Відкрити файл «IronMacbeth.BFF.exe.config» за замінити наступні налаштування:
         1. Connection String до бази даних за шляхом «configuration\connectionStrings\add» атрибут «connectionString». Замінити значення на Connection String до бази даних, у яку був виконаний publish з проекту Database\IronMacbeth.BFF.Database.
         2. Service Certificate за шляхом «configuration\system.serviceModel\behaviors\serviceBehaviors\behavior\serviceCredentials\serviceCertificate» атрибут «findValue». Замінити значення на серійний номер сертифікату, що буде використовуватись як серверний сертифікат для сервісу.
         3. Сертифікат для авторизації з’єднання з «IronMacbeth.FileStorage» сервісом за шляхом «configuration\system.serviceModel\behaviors\endpointBehaviors\behavior (name="ServiceToServiceBehavior.FileStorage")\clientCredentials\clientCertificate» атрибут «findValue». Замінити значення на серійний номер сертифікату, який буде використаний для авторизації з’єднання з «IronMacbeth.FileStorage» сервісом (має співпадати зі значенням пункту «4.b.i.2» при налаштуванні «IronMacbeth.FileStorage» сервісу).
         4. Сертифікат для авторизації з’єднання з «IronMacbeth.FileStorage» сервісом за шляхом «configuration\system.serviceModel\behaviors\endpointBehaviors\behavior (name="ServiceToServiceBehavior.UserManagement")\clientCredentials\clientCertificate» атрибут «findValue». Замінити значення на серійний номер сертифікату, який буде використаний для авторизації з’єднання з «IronMacbeth.FileStorage» сервісом (має співпадати зі значенням пункту «4.b.i.2» при налаштуванні «IronMacbeth.UserManagement» сервісу).
         5. Address за шляхом «configuration\system.serviceModel\services\service (name="IronMacbeth.BFF.Service")\ endpoint» атрибут «address». Замінити значення на адресу, за якою інші обчислювальні машини зможуть звернутись до сервісу.
         6. Address за шляхом «configuration\system.serviceModel\services\service (name="IronMacbeth.BFF.AnonymousService")\ endpoint» атрибут «address». Замінити значення на адресу, за якою інші обчислювальні машини зможуть звернутись до сервісу.
         7. Base Address за шляхом «configuration\system.serviceModel\services\ service (name="IronMacbeth.BFF.Service")\host\baseAddresses\ add» атрибут «baseAddress». Замінити значення на адресу, за якою інші обчислювальні машини зможуть звернутись до сервісу.
         8. Base Address за шляхом «configuration\system.serviceModel\services\ service (name="IronMacbeth.BFF.AnonymousService")\host\baseAddresses\ add» атрибут «baseAddress». Замінити значення на адресу, за якою інші обчислювальні машини зможуть звернутись до сервісу.
         9. Адреса сервісу «IronMacbeth.UserManagement» за шляхом «configuration\system.serviceModel\client\endpoint (name="IronMacbeth.UserManagementEndpoint")» атрибут «address». Замінити на адресу, за якою можна буде звернутись до сервісу «IronMacbeth.UserManagement».
         10. Адреса сервісу «IronMacbeth.FileStorage» за шляхом «configuration\system.serviceModel\client\endpoint (name="IronMacbeth.FileStorage")» атрибут «address». Замінити на адресу, за якою можна буде звернутись до сервісу «IronMacbeth.FileStorage».
         11. Публічний ключ сертифікату якому має довіряти сервіс при з’єднанні з сервісом «IronMacbeth.UserManagement» за шляхом «configuration\system.serviceModel\client\endpoint (name="IronMacbeth.UserManagementEndpoint")\identity\certificate» атрибут «encodedValue».
         12. Публічний ключ сертифікату якому має довіряти сервіс при з’єднанні з сервісом «IronMacbeth.FileStorage» за шляхом «configuration\system.serviceModel\client\endpoint (name="IronMacbeth.FileStorage")\identity\certificate» атрибут «encodedValue».
3. Встановлення сертифікатів
   1. На всіх обчислювальних машинах, на яких було розгорнуто сервіси встановити необхідні сертифікати (при розгортанні **не** для використання кінцевими користувачами (Production/Live environment) зручніше використовувати лише один сертифікат для всіх сервісів):
      1. Файл з сертифікатом, що був зекспортований у пункті «1.a.vii» розмістити на необхідних обчислювальних машинах.
      2. Обрати файл та двічі натиснути ЛКМ.
      3. У вікні що відкрилось, обрати опцію «Local Machine» та натиснути «Next», впевнившись що обрано правильний файл, натиснути «Next», ввести пароль та натиснути «Next», ще раз «Next» і «Finish».
4. Запуск сервісів
   1. Запустити виконувані файли «IronMacbeth.UserManagement.exe», «IronMacbeth.FileStorage.exe» та «IronMacbeth.BFF.exe» на відповідних обчислювальних машинах від імені адміністратора.

Якщо всі вище перечисленні пункти було успішно виконано, розподілена система готова до використання.