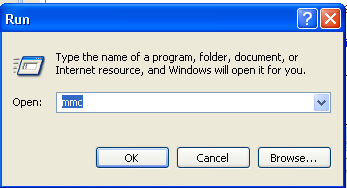
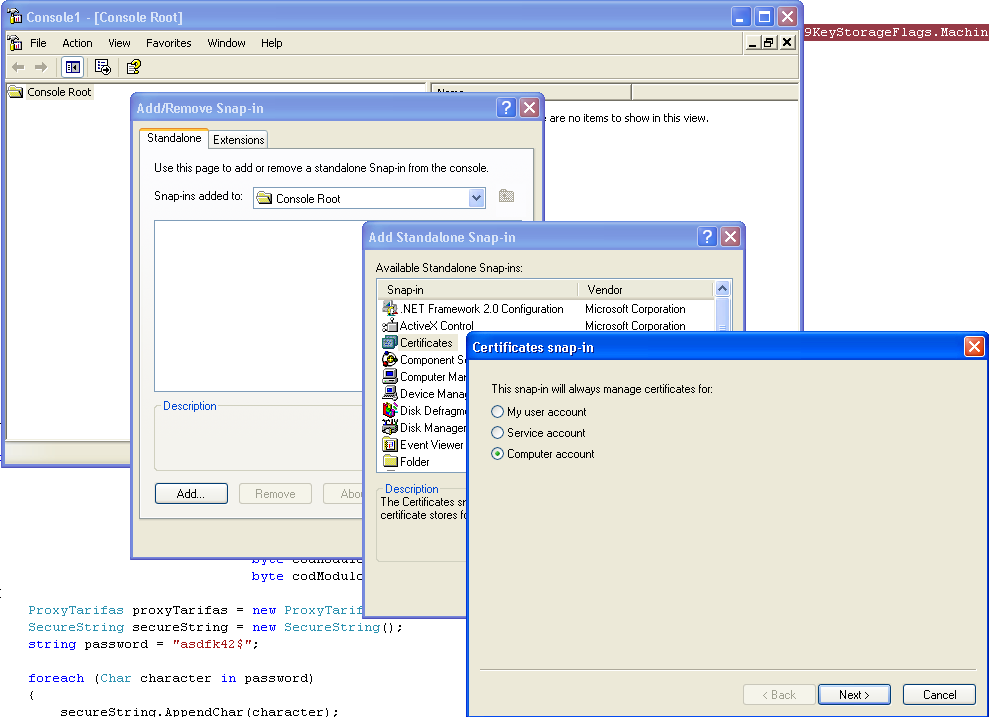
# INSTALACION DE LOS CERTIFICADOS DE SANCOR

# Crear Snap-In de certificados en la consola

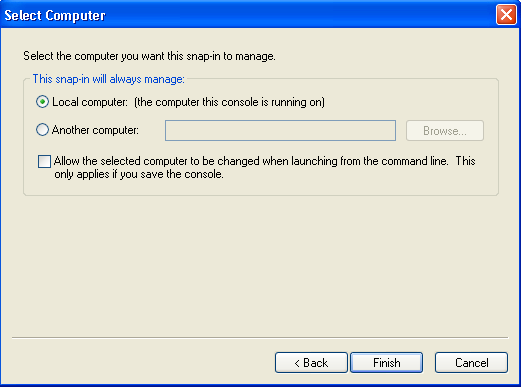
Abrir la consola mmc desde el command (cmd) de windows.



Se abrirá la consola vaciía, ir a File -> Add/Remove Snap In luego el botón add, a continuación seleccionar Certificates y luego Computer Account como se muestra en la imagen siguiente.



Presionar el botón Next y luego seleccionar Local computer…



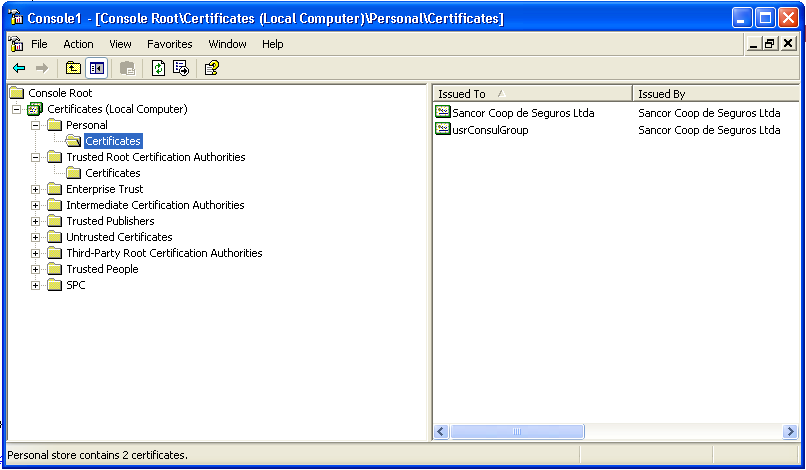
Importar los archivos root.cer y usrConsulGroupCtaCte.pfx (botón contextual del mouse sobre la carpeta Personal), seleccionar la segunda opción como lo detalla la imagen siguiente.

Para certificado CtaCte -> Password="con43$su2"



A continuación se muestra como quedan instalados los certificados.

El certificado root.cer también se almacena en el área de certificados de Trusted Root Certification Authorities.



En este punto ya se puede acceder al web service de forma autenticada desde este servidor. En el paso siguiente se instalará la aplicación (dll .NET) que accederá al web service de Sancor desde SQL Server.

# INSTALACION DE COMPONENTE EN SQL PARA WEB SERVICE DE TARIFACION

En el servidor de SQL se crearán 2 assemblies, el que contiene la dll WSSancor.dll y el de serialización WSSancor.XmlSerializers.dll, finalmente se creará la función que será utilizada por el usuario para consumir el web service.

# Prerequisitos

Habilitar el CLR en el servidor SQL. Ejecutar el siguiente script.

EXEC sp\_configure 'show advanced options' , '1';

go

reconfigure;

go

EXEC sp\_configure 'clr enabled' , '1'

go

reconfigure;

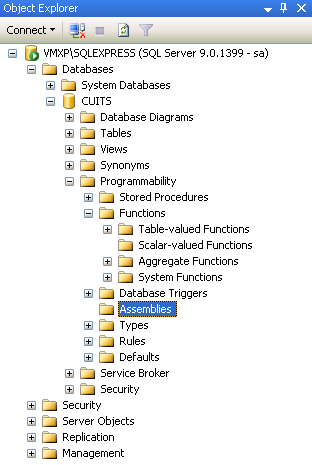
-- Turn advanced options back off

EXEC sp\_configure 'show advanced options' , '0';

Go

Dar permiso de TRUSTWORTHY a la base de datos

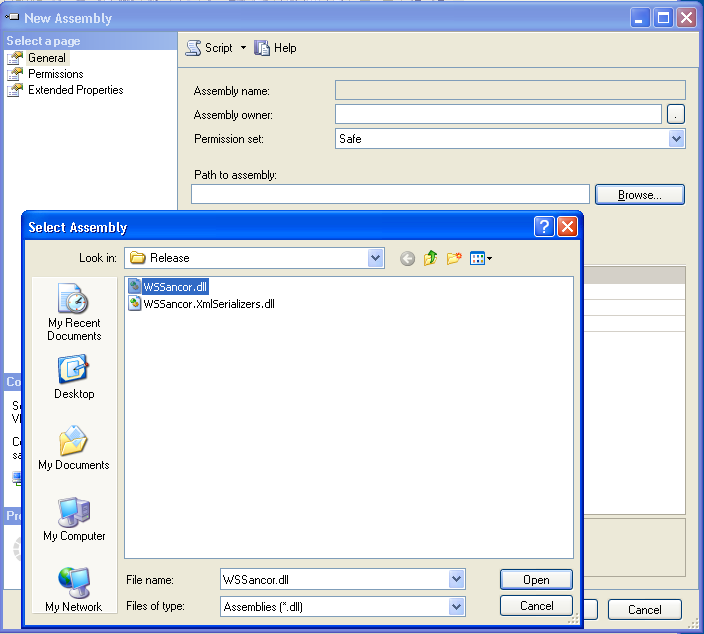
ALTER DATABASE CUITS SET TRUSTWORTHY ON

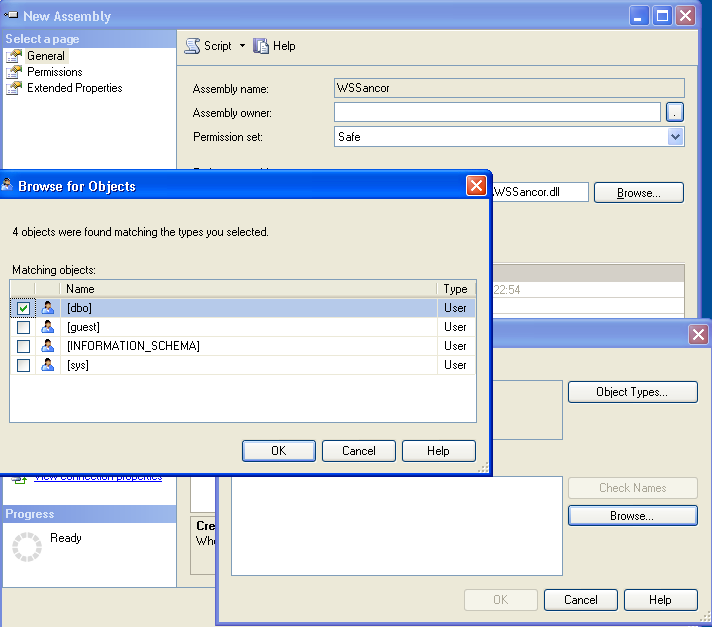


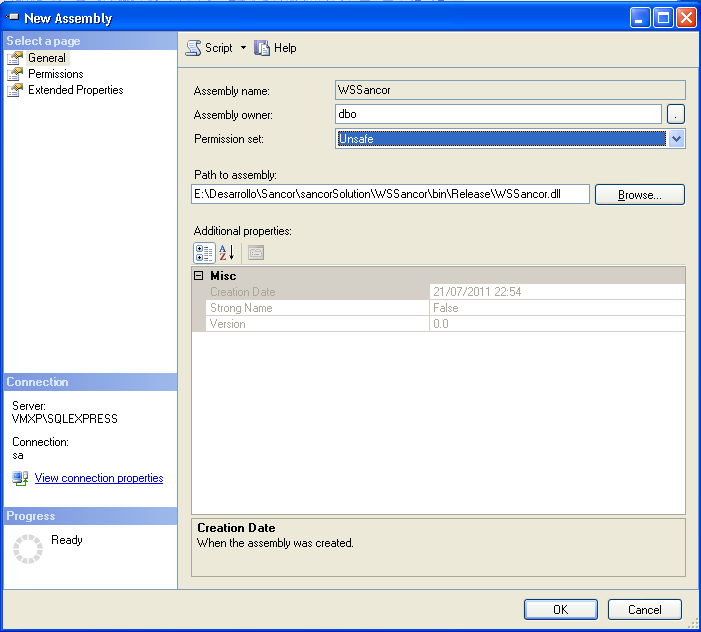
Estado del servidor antes de la instalación

# Instalación de los assemblies

Ir a la carpeta Programability\Assemblies de SQL Server, seleccionar “New Assembly”. Click en Browse y seleccionar el archivo WSSancor.dll, a continuación establecer el Persmission Set como “Unsafe”, y por último establecer el valor Assembly owner como [dbo], como muestan las siguientes imágenes.







Pasos para la instalación de los assemblies en SQL Server

Repetir los mismos pasos para el asembly WSSancor.XmlSerializers.dll.

En este punto ya están los assemblies instalados, solo resta crear la función.

# Creación de la función SQL

Correr el siguiente script en la base de datos seleccionada:

set ANSI\_NULLS ON

set QUOTED\_IDENTIFIER ON

go

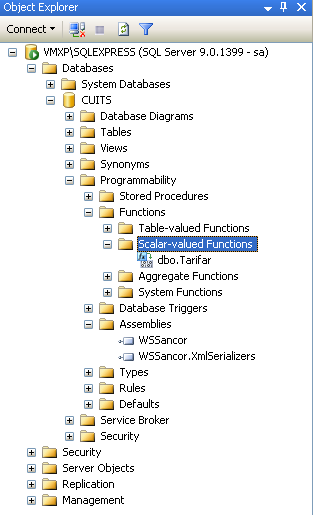
CREATE FUNCTION [dbo].[FN\_Cotizar\_ART](@CuitEmpresa [bigint], @CodActividad [int], @CantTrabajadores [int], @MasaSalarial [decimal](18, 0), @CodPostal [smallint])

RETURNS [nvarchar](4000) WITH EXECUTE AS CALLER

AS EXTERNAL NAME [WSSancor].[WSSancor.Tarifas].[CotizarART]

Ejemplo de utilización:

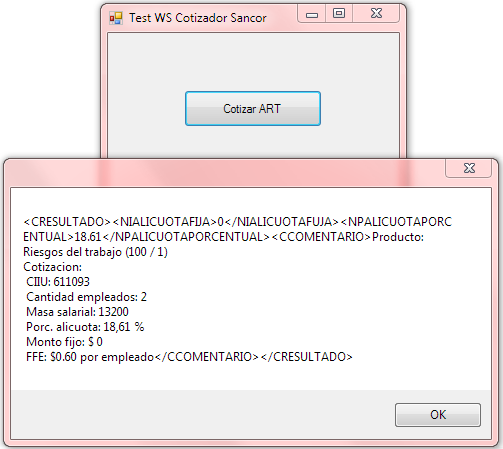
select dbo.FN\_Cotizar\_ART(30599791716, 611093, 2, 13200, 1425)



Servidor con los assemblies y la función instalada

# Aplicación ejemplo para testear Cotizador

Este es un ejecutable WSSancor.exe que, como ya se comentó esta aplicación sirve para testear la conectividad con el web service sin necesidad de utilizar SQL, los datos están fijos y son los mismos que los usados en la descripción de la función SQL mencionada anteriormente.



Ejemplo de ejecución del test

# INSTALACION DE SERVICIO DE WINDOWS PARA USO DEL WEB SERVICE DE CUENTA CORRIENTE

Pasos de instalación:

-. Correr el script “dbo.WSSancorCtaCteRequest.Table.sql” que genera la tabla WSSancorCtaCteRequest provisto en la solución, mantener esta tabla SIN registros o con registros en estado “1” (finalizado), para que se pueda subir el servicio sin inconvenientes.

-. Cambiar el valor del connection string en el archivo “WSSancorService.exe.config”. En este mismo archivo se puede cambiar la configuración del web service de Sancor como la url donde apunta y el lugar donde se ha almacenado el certificado a utilizar para conectar con el mismo.

<system.serviceModel>

<bindings>

<basicHttpBinding>

<binding name="requestReplyRoutingEndpoint">

<security mode="Transport">

<transport clientCredentialType="Certificate" />

</security>

</binding>

<binding name="BasicHttpBinding\_IARTServices" />

</basicHttpBinding>

</bindings>

<client>

<endpoint address="https://200.41.127.78/CurrentAccountARTPublicServices/ARTAccountingServices.svc"

behaviorConfiguration="httpbehaviorARTServices" binding="basicHttpBinding"

bindingConfiguration="requestReplyRoutingEndpoint" contract="ARTServices.IARTServices"

name="BasicHttpBinding\_IARTServices" />

</client>

<behaviors>

<endpointBehaviors>

<behavior name="httpbehaviorARTServices">

<clientCredentials>

<clientCertificate findValue="usrConsulGroup"

storeLocation="LocalMachine"

storeName="My"

x509FindType="FindBySubjectName"/>

</clientCredentials>

</behavior>

</endpointBehaviors>

</behaviors>

</system.serviceModel>

-. Ejecutar el snippet de SQL “service-broker-snippet.sql” provisto con la solución que configurará SQL para que “escuche” cuando se ingresen registros a la tabla WSSancorCtaCteRequest, para luego enviar la peticiona al Windows Service que ejecuta el Web Service de consulta de cuenta corriente. Reemplazar los valores de dominio\usuario y nombre de base de datos.

-. Instalar el servicio abriendo la consola de Windows desde command prompt como “ADMINISTRADOR”, luego registrar el servicio de la siguiente manera:

C:\Windows\system32>installutil /i c:\PATH\WSSancorService.exe

A continuación abrir la consola de Windows Services escribiendo en la barra de búsqueda de Windows “services.msc”, buscar el servicio WSSancorService e iniciarlo presionando “PLAY”.

En este punto ya está funcionando el servicio, solo resta agregar o modificar registros en la tabla WSSancorCtaCteRequest pasándolos al estado “0” (pendiente).