ReportPlus™
POWERED BY INFRAGISTICS

ReportPlus Web 5

Kerberos Sign-on Configuration

ReportPlus™ Web 5.0 –Kerberos Sign-on Configuration 1.0.

Table of Contents

Requirements

To successfully configure a Kerberos based single sign-on, you need **Windows Identity Foundation** installed on the Web server.

Validation

If you want to validate that WIF is installed on the server, you can search for this key in the registry:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsIdentityFoundation\setup\v3.5

Installation

In case you don't have it installed then you can download an installer from here:

http://www.microsoft.com/en-us/download/details.aspx?id=17331

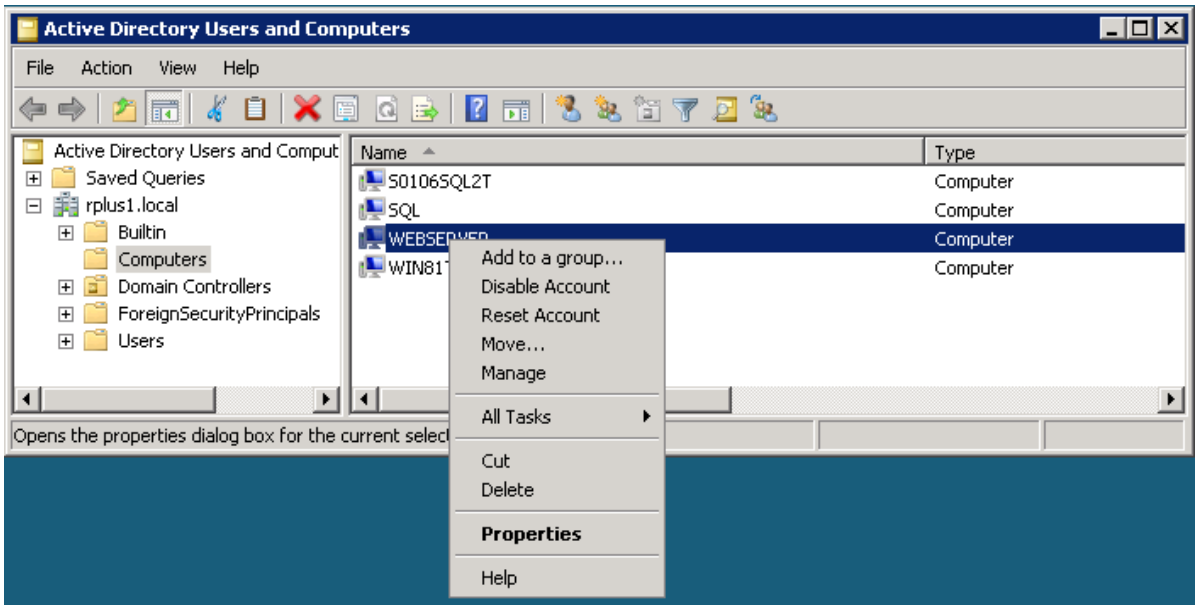
Configuration Steps

1. Server delegation

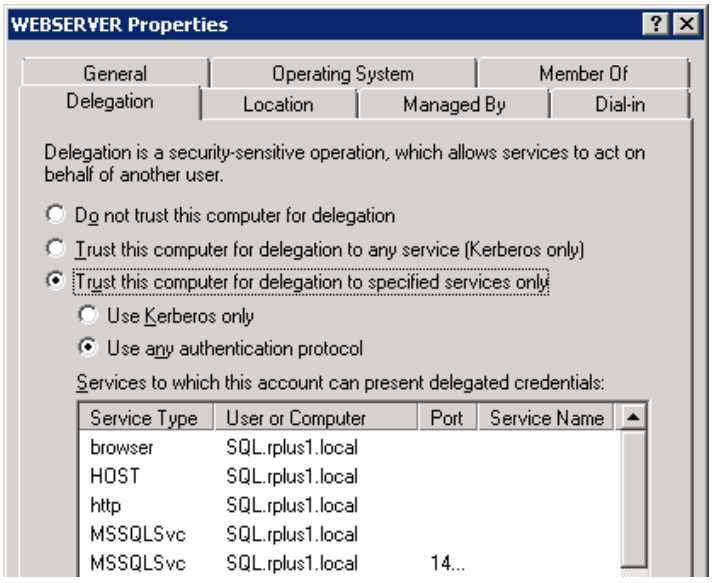
The first step is to grant delegation rights from the Web server to the SQL Server Analysis Services (SSAS). In order to do this you should use the Server Principal Name (SPN) of the SSAS machine and set it up in the Active Directory (AD) server.

i) Go to **Active Directory Server**.

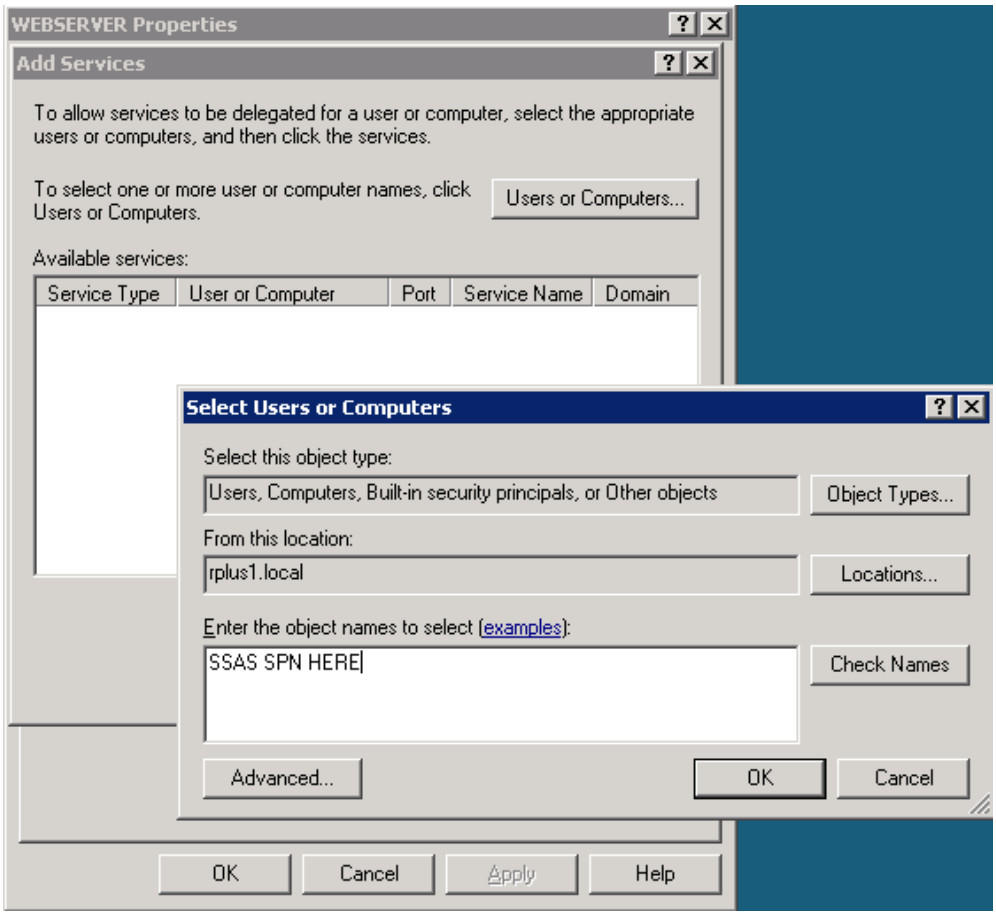
ii) Open the **Active Directory Users and Computers** console, find *WEBSERVER* computer, right-click on it and select *Properties*.



iii) Navigate to the *Delegation* tab and select the *Trust this computer for delegation to specified services only* option.



iv) Use the *Add* button to specify which back-end servers can be accessed by the accounts.



v) (Only SSAS Server) Enable a specific service.
In case you want to configure a SSAS Server, you should ensure that the **MSOLAPSvc.3** service is selected.
If you can't find that service listed, that's because a Service Principal Name (SPN) must be created in the Active Directory (AD) for the Analysis service.
You can make that with the following command:

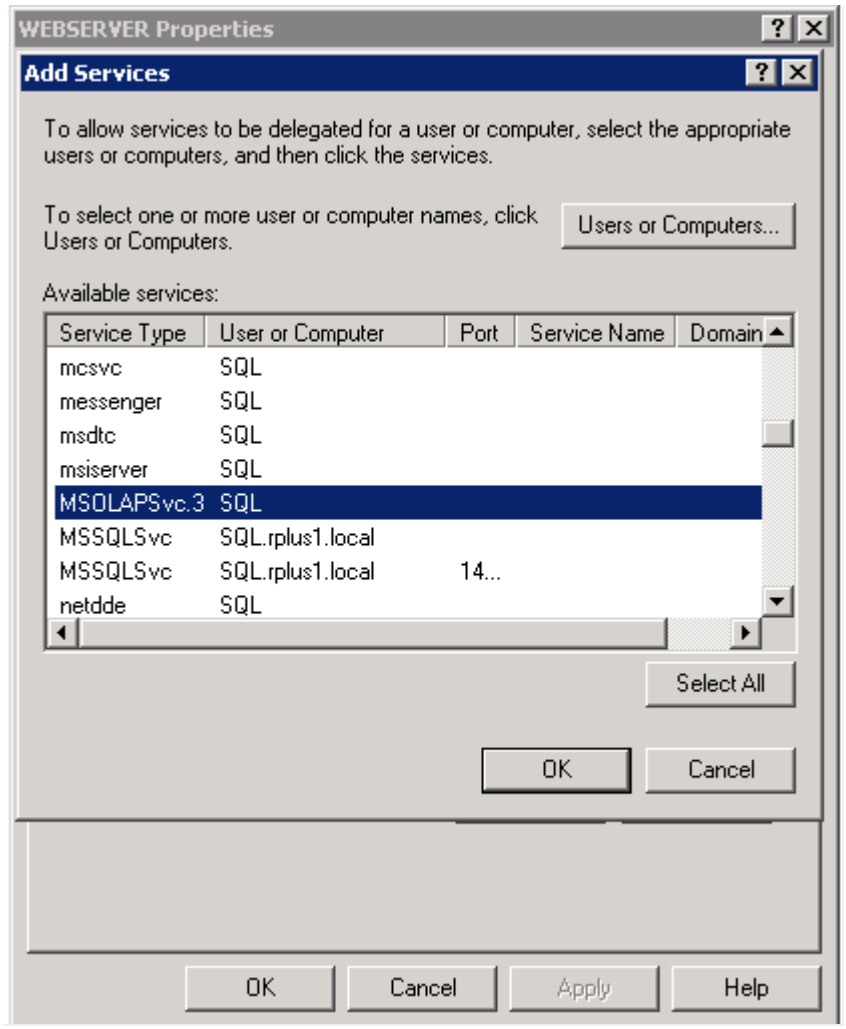
```
setspn -s MSOLAPSvc.3/<serverFQDN> <server>
```

A real use case should be similar to the following example:

```
setspn -s MSOLAPSvc.3/SQL.rplus1.local SQL
```

If you prefer to do it manually, you can do it by launching *ADSIEdit* on the DC, locating the SQL computer object, going to its properties and editing the *ServicePrincipalName* attribute. **MSOLAPSvc.3/SQL.rplus1.local** was the value we added in the example above.

After that you should be able to grant trust for delegation to the service, in a screen similar to the following one:



2. **Claims to Windows Token Service**

   i) Open a cmd prompt on the server as System Administrator.

   ii) Execute the following command:

   ```
   sc config "c2wts" depend= CryptSvc
   ```

   iii) Navigate to *C:\Program Files\Windows Identity Foundation\v3.5* and open the **c2wtshost.exe.config** file with a text editor.

   iv) Add **NT AUTHORITY\Network Service, NT AUTHORITY\Local Service**

   v) Find the Claims to Windows Token Service in the Services console (run services.msc to open the console).

   vi) Double-click on it. Then, on the *General tab*, change the *startup type* to **Automatic**, then navigate to the *Log On* tab and select *LocalSystem*.

   vii) Right-click on the service and select **Start**.

3. **Application configuration.**

   After configuring server's delegation you need to modify ReportPlus Web application configuration in order to support Single Sign-on.

   i) Go to ReportPlus Web application physical path and open the **Web.config** file. Normally, the path is: *C:\inetpub\wwwroot\RPlusServer*

   ii) Find the tag *security* and add the following two properties in that line:

```
useRoleBasedModel="false"
useClaims2WindowsTokenService="true"
```

   iii) Add the mappings for SSAS SPN under the *ServerNameMapping* tag, inside *security*.

   The complete security section configuration in the **Web.config** file should be similar to this:

```
<security requiresSSL="false" useRoleBasedModel="false" useClaims2WindowsTokenService="true"
secureStorageConnectionString="..connectionstring..">
    <serverNameMapping>
        <map originalName="10.20.37.248" targetName="SQL.rplus1.local"/>
    </serverNameMapping>
</security>
```