Notes on Installing Cognos 11.1.x in a Windows Environment

I know there are dozens of documents, blog posts, YouTube videos, white papers, documentation, webinars, and slide decks on this topic, but my personal experience continues to prove that there really isn't any single "authoritative" resource that covers *everything*. This is mostly due to the fact that every environment is unique, and rightfully there is no one-size-fits-all recipe for success.

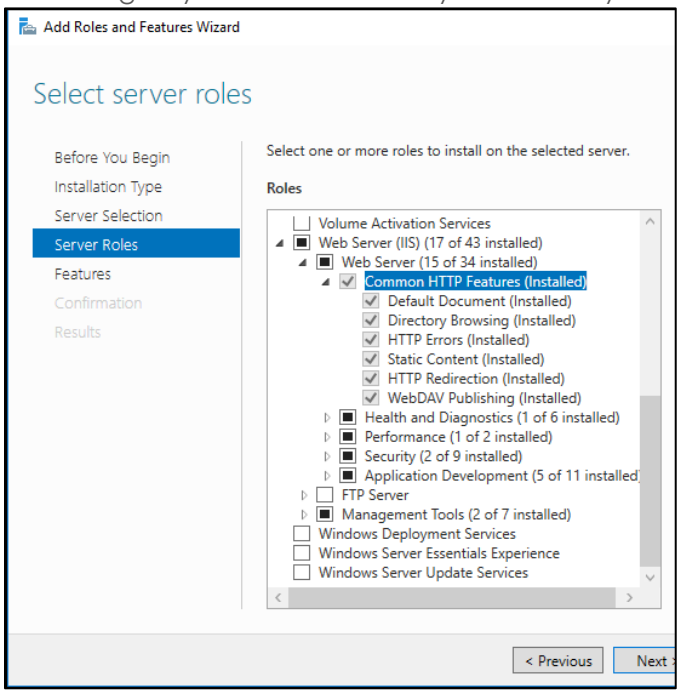
However, the vast majority of "clean" installs – meaning a virgin, dedicated Windows server – do tend to have a pretty consistent profile. If you plan to leverage IIS as your web server, Active Directory for single sign-on, and SQL Server for your content store, then you should have it pretty easy, right? Well, for the most part, yes. My goal here is to highlight the key steps that can cause great frustration if not followed precisely, and that aren't all nicely captured in a single document (including IBM's own installation guides). Hopefully this document can be a useful resource for those of you installing in a pure Windows environment, but as always, keep current and continue to leverage all available sources of information.

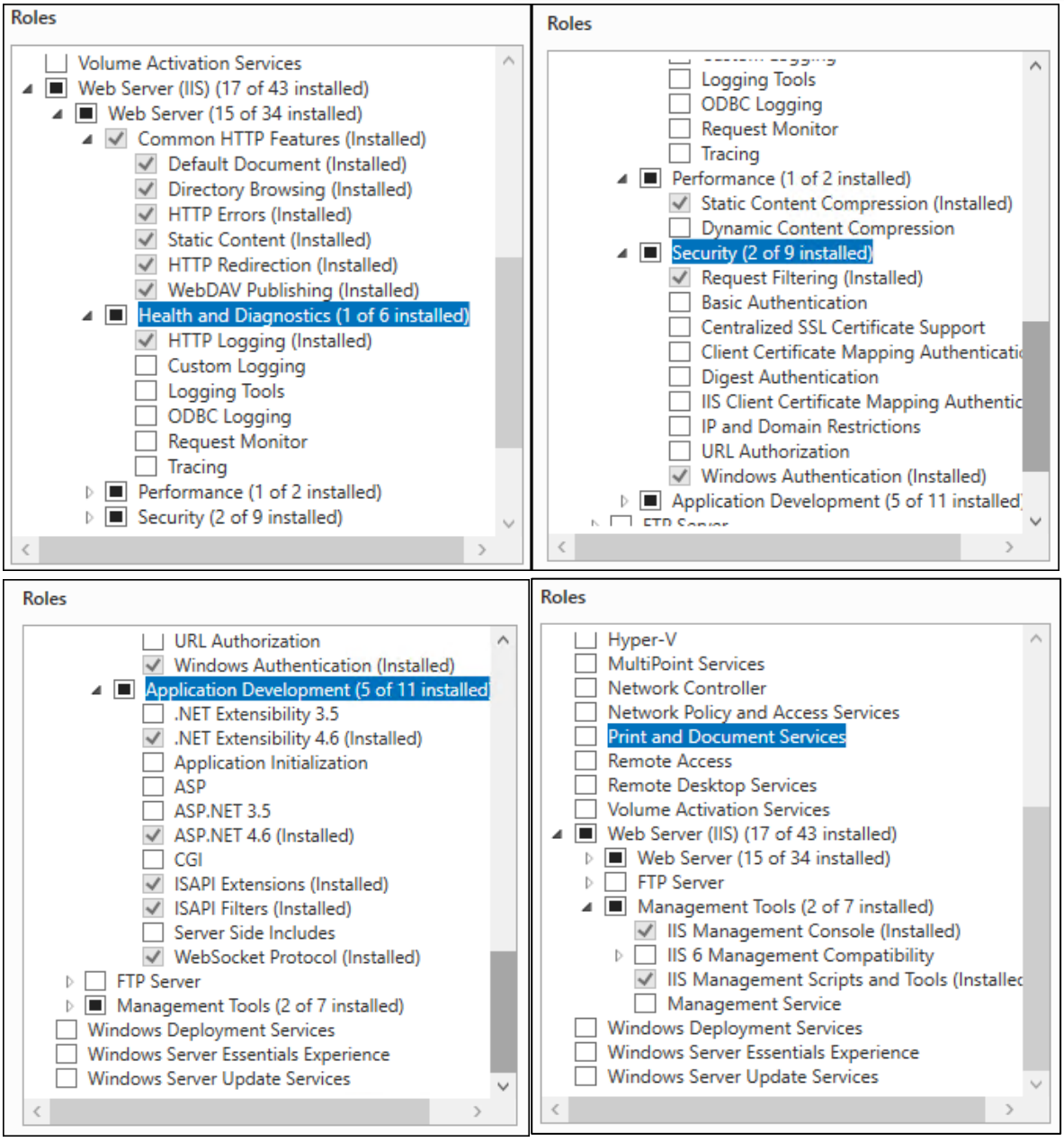
First, we have to be careful about software compatibility. Since this is a constantly moving target, you should always start here to spec out your environment:
https://www.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html

Ok, let's get started. We assume that you have already downloaded the necessary installation media and run the installer program for each component on the appropriate machine. Again, this is 100% focused on a pure Windows environment.

Once you have your compatible OS and other prerequisites selected, installed, updated, and patched (you shouldn't need to patch a current Windows release), make sure you set IE Enhanced Security Configuration to OFF in the Windows Server Manager homepage. Also set Data Execution Protection (DEP) to essential Windows programs and services ONLY.

Next, configure the necessary features and roles for IIS – this is for the machine where the Cognos web gateway will reside. Again, this is crucial on a virgin server, but if you are adding the Cognos gateway to an existing IIS environment, most of these features would likely already be available. Either way, it doesn't hurt to make sure. From the Windows Server Manager, use the Add Roles and Features wizard, which you can find on the home page. The following screen shots will give you all the necessary functionality for the Cognos Analytics 11.1.7 environment:





The next step for your web server is to download and install Application Request Routing: https://www.iis.net/downloads/microsoft/application-request-routing

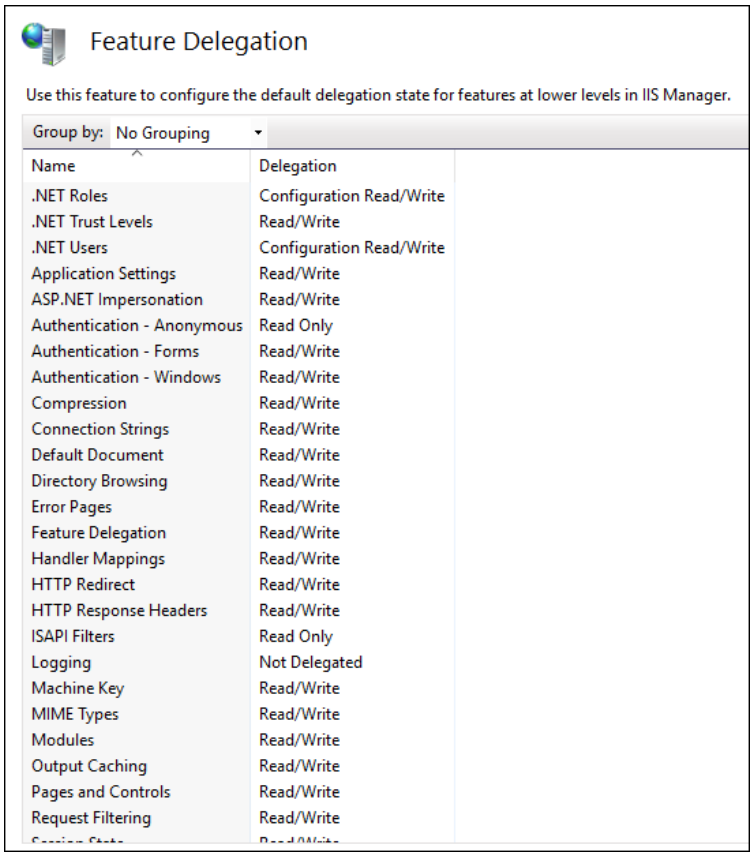
Run the program: **ARRv3_0.exe**, accept all the defaults, and exit.

Next, browse to <Install Location>\cognos\analytics\cgi-bin\templates\IIS and rename the **CA_IIS_Config.bat** file to CA_IIS_Config_old.bat. Edit the CA_IIS_Config_old.bat file in a text editor, and make the following changes to reflect your environment:

1. "set ca_path=C:\Program Files\ibm\cognos\analytics" changes to:
    a. "set ca_path=<your install path>"
2. "set disp[1].name=localhost" changes to:
    a. "set disp[1].name=<your fully qualified dispatcher host name>"
    b. And add any others here, as necessary
3. "set enable_SSO=False" changes to:
    a. "set enable_SSO=True" *IF USING IIS FOR SSO*
4. "set cam_namespace=" changes to:
    a. "set cam_namespace=<your default namespace>" (you may be able to leave this blank if not setting a default namespace, but this is rare in a secured environment and might cause issues with SSO)

Save the file as **CA_IIS_Config.bat**. Right-click and run the .bat file as Administrator

You may also need to update Feature Delegation on the **root server node** in IIS. Feature Delegation can be found in the Management section in IIS manager. The following two settings should be set to **Read/Write**: **Authentication – Windows** and **Modules**.



At this point, IIS should be ready to go. The next step should be your Cognos Configuration. If you are installing multiple components on the same server, make sure you are accessing Cognos Configuration from the **Start Menu > IBM Cognos Analytics** path. Start with the **Environment** node. The default settings can throw you off. The first one to modify is the **Gateway URI**. It should look like this: http://<gatewayhost>:80/ibmcognos/bi/v1/disp where <gatewayhost> is the fully qualified host name of your IIS/Cognos gateway. The key here is to include the Cognos alias that you defined in the CA_IIS_Config.bat file (we kept the default "ibmcognos" in this example).

The **Dispatcher URI** should be in this format: http://<primarydispatcherhost>:9300/bi/v1/disp where <primarydispatcherhost> is the fully qualified host name of your main application tier, or report server.

Configure the Controller URI for gateway if necessary as per instructions from your Controller administrator.

If you are also installing application tier components (Report server or content manager) on the same server, you will be configuring the **Dispatcher Settings** as well. If not, these settings will need to be configured on those separate instances.

In almost all cases the External and Internal dispatcher URI's will be the same. They will point to the local host machine and will be in the format: http://<localhost>:9300/p2pd/servlet/dispatch where <localhost> is the fully qualified host name of the local machine.

The Other URI Settings are used as follows:

Dispatcher URI for external applications is used by client tools such as Framework Manager and Transformer and should point to the primary content manager. It will be in the format: http://<contentmanagerhost>:9300/bi/v1/disp where <contentmanagerhost> is the fully qualified host name of your primary content manager (theoretically, any available dispatcher value will work here). The **Content Manager URIs** setting can have multiple values. It requires just the one, primary, content manager and is formatted as: http://<contentmanagerhost>:9300/p2pd/servlet/dispatch where <contentmanagerhost> is the fully qualified host name of your primary content manager. Click in the ellipsis on this setting to add additional, backup, content managers as desired.

To make sure single sign-on works, the IBM documentation assumes no other configuration is necessary as you can take advantage of the native Windows support of Kerberos pass-through authentication. I found it still necessary to configure the Advanced properties at the **Authentication** node under the Security group on all of your content manager servers. At this node, click the **Advanced properties**, click the edit tool, and click Add in the dialog box to add an advanced property named **SingleSignOnOption** with the value **IdentityMapping**. Both name and value are case-sensitive. Disable the anonymous access at the Cognos node, and add your Active Directory server. These settings are all pretty self-explanatory, but you will also want to add the following Advanced properties (this setting is found on the Active Directory namespace under the Multitenancy area). Click the **Advanced properties**, click the edit tool, and click Add in the dialog box to add three advanced properties:

SingleSignOnOption with the value **IdentityMapping**

chaseReferrals with the value **True**

multiDomainTrees with the value **True** Again, both name and value are case-sensitive. The last two settings can certainly be environment-specific, and may not be 100% necessary, but I've found that most AD environments require these settings for a true SSO experience.

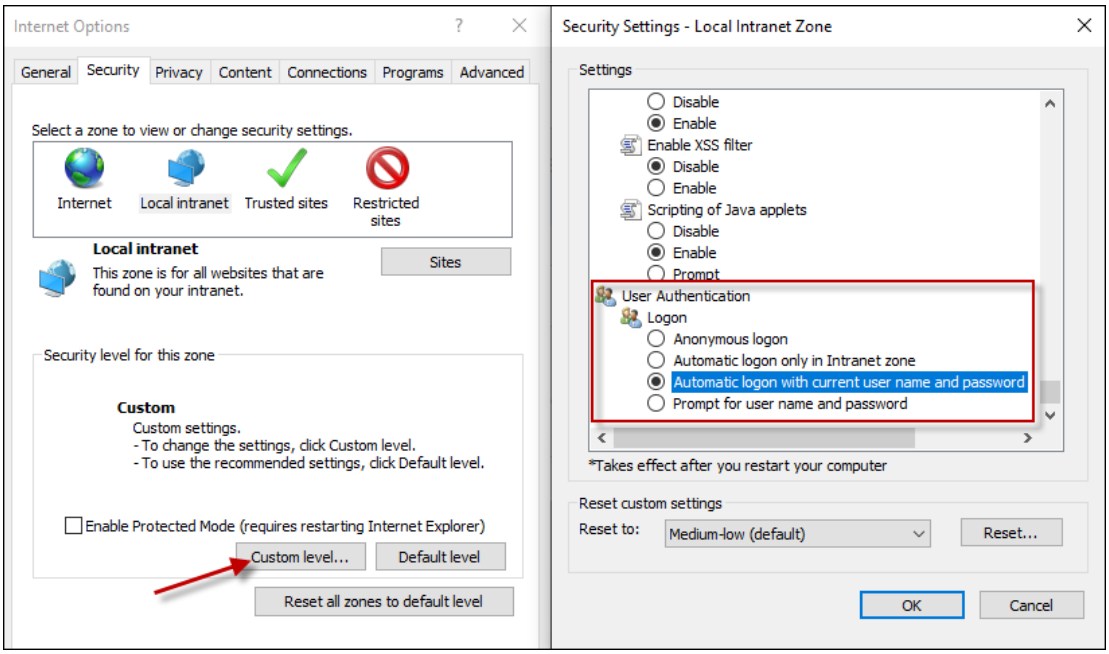
At this point, you should be able to successfully save your Cognos Configuration. In a distributed environment, you need to configure and save your primary content manager FIRST. This means you will need to have your content store and audit databases setup, because the next step will be to start the Cognos service on this server. Save and start services on the backup content managers next. Then do the same for each report server, then your gateway/web server(s), and finally all FM and Transformer clients (you don't need to, nor can you, start any services on standalone client machines). Failure to follow this order and any inability to connect to gateway and content manager dispatcher will cause the configuration to fail, and can result in cryptography keys being mismatched and having to be regenerated.

Make sure your Cognos Configuration on the client machines are using the below configuration for **Gateway URI**: http://<gatewayhost>:80/ibmcognos/bi/v1/disp where <gatewayhost> is the fully qualified host name of your IIS/Cognos gateway. The key here is to include the Cognos alias that you defined in the CA_IIS_Config.bat file (we kept the default "ibmcognos" in this example).

The configuration under the path Start > IBM Cognos 11 is the one for Transformer. Use the above **Gateway URI** setting, and the **Dispatcher URI for external applications** should be in the format: http://<contentmanagerhost>:9300/p2pd/servlet/dispatch where <contentmanagerhost> is the fully qualified host name of your primary content manager.

The configuration under the path Start > IBM Cognos Framework Manager is the one for FM. Use the above **Gateway URI** setting, and the **Dispatcher URI for external applications** should be in the format: http://<contentmanagerhost>:9300/bi/v1/disp where <contentmanagerhost> is the fully qualified host name of your primary content manager.

The last pieces are browser-related. On any Windows machine that will host Framework Manager and/or Transformer, keep in mind that these applications user Internet Explorer capabilities for authentication. You will need a compatible install of IE on these machines. If your environment is on the local intranet, you should be able to just modify the following setting from Tools > Internet Options. Click the Security tab, click on Local intranet, and click Custom level. Make the following change:



One final note on browsers: the latest update to Chrome is no longer supported for Cognos Analytics 11.1.7. This is another reminder to review the latest compatibility reports at: https://www.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html. Browser updates come fast and frequent and you may have become accustomed to a more open standard as previous versions of Cognos have worked fine with most browsers popular with the user community. However, remember that any browser-based application is only tested against versions of browsers that are available at the time of development.

Enjoy – and please reach out if you need anything!