Hosting Management Server Installation Guide

The JDA ESO Application requires a Hosting Management Server to enable the deployment of new code and code updates to the ESO operational Servers (Both Web & Application). This document describes the prerequires and steps required to install and instance of the HM Server. The HM Server contains two main components, an SQL Server instance, and a Web Server instance. This document assumes that the instances are on separate servers to provide separation of functions.

Steps

This document is intended to be followed in sequence.

* HM SQL Server

1. Prerequisites
2. SQL Server Installation
3. SQL Server Configuration
4. HM Tools Installation

* HM Web Server
  1. Prerequisites
  2. IIS Installation
  3. IIS Configuration
  4. HM Tools Installation
  5. Tools Basic Setup

HM SQL Server

Prerequisites

* Windows Server 2012R2 or 2016.
* SQL Server 2014 or 2016.
* Domain or SQL account credentials with admin access to the DB Server, must have modify access to the root drive where the SQL databases are going to be placed.
* Trusted (Integrated) authentication credentials.
* A pre-built set of installation files containing:

1. SQL Server 2005 Backward Compatibility Components.
2. Visual C++ redistributable
3. MSCOMCTRL file for VB UI components
4. SQL Client Tools
5. Empty Hosting Management Tools SQL backup (.bak) file.
6. HM Extracted code files
7. Empty Object Repository (OR) SQL backup (.bak) file.
8. OR Extracted code files
9. Example GlobalSettings.xml
10. Example Logconfig.xml
11. Object Repository views SQL Script
12. Registry key file to configure location of global settings and log config files.
13. ESO one-time deployment files
14. Tools patch files

Assumptions

* The HM SQL Server is stand alone and not part of a cluster
* Trusted authentication will be used wherever possible.

SQL Server Installation

1. The following components should be selected during the installation process from with the SQL Server Installation Center:

* SQL Server Database Services: Required.
* Client Tools Connectivity.
* Client Tools Backwards Compatibility.
* Management Tools – Basic.
* Management Tools – Complete.
* Shared feature directory: modify as needed.

1. Instance Configuration

* The installation path for SQL files should point to a non-system drive.
* The instance root directory should point to a non-system drive.
* Avoid using named instances. The SQL Server should only provide services to the HM Server.
* Verify disk space usage.

1. Server configuration panel

* SQL Agent – enter domain account credentials and change the agent startup type to “Automatic”. Use a user account, do not use a group account.
* On the collation tab, check that the default collation is selected (SQL\_Latin1\_General\_CP1\_CI\_AS).

1. Database Engine configuration

* In the account provision tab, ensure that Mixed Mode authentication is selected.
* Set the System Administrator password.
* Configure the data directories. It is recommended to use different drives for the user databases, database logs and temp DB logs, the temp DB, and backup files.

1. Click install to complete the initial installation

SQL Server Configuration

Start the SQL Server Management Studio to complete the configuration

1. Right click on the server instance name and select Facets. In Surface Area Configuration, set the following properties to true and click OK.
   * Ad-Hoc Remote Queries
   * CLR Integration
   * Database Mail
   * SQL Mail
2. Right click on the server instance name and select Facets. In Server Configuration, set the max degree of parallelism to 4 if the server has 4 or more CPU cores, otherwise set the value to 0. Click OK.
3. If not already installed run the SQLServer2005\_BC\_x64.msi to install backwards compatibility.
   * Click Next and accept the terms of the license agreement.
   * Enter Name and Company, click Next.
   * Do not change the feature installation list, click Next.
   * Click Finish.
4. Configure Distributed Transaction Coordinator (DTC)
   * In windows search, select Administrative tools.
   * Double Click Component Services.
   * In the Component Services panel expand Computers, My Computer, Distributed Transactions.
   * Right Click on Local DTC, select Properties and select the Security tab. Enable the following:
   1. Network DTC Access
   2. Allow Remote Administration
   3. Allow Inbound
   4. Allow Outbound
   5. No Authentication Required
   6. Enable XA Transactions
   * Click OK, if prompted to restart DTC select Yes.
   * Exit Component Services and Administrative Tools.

HM Tools Installation

1. SQL Login

* Open SQL Management Studio and connect to the HM DB Server.
* Expand the server, and Right Click on security at add a new login, enter the following:

1. Login Name
2. SQL Authentication
3. Password
4. Unselect: Enforce password policy, enforce password expiration, and user must change password at next login.
5. Click OK
6. Create an Empty OR Database

* Right Click on databases and select Restore Database.
* Select to restore from a device and browse to the file containing and empty object repository database bak file. This is located in the installation package under \JDA\ESO Installation\Application\EmptyORDB\.
* Select the Restore check box for the backup set.
* In the to-database field enter the name of the HM object repository, for example hm\_or. This database should not already exist.
* Adjust the paths to the recommended non-system data and log paths.
* Click OK.

1. Import the ESO Application into the Tools database

* The ESO code .dat files are located in the folder \JDA\ESO Installation\Application\Current Version\Extracted Files.
* Navigate to the Extracted Files folder.
* Open a command prompt an execute the following:

Importbuild *DestinationServerName ORDBName DBUserName DBUserPassword*

1. DestinationSeverName = The HM SQL Server
2. ORDBName = The database that was restored from the empty object repository DB (hm\_or)
3. DBUserName = The SQL User created in step #1.
4. DBUserPassword = The password associated to the user.

* Close the command prompt.

1. Create an Empty Tools Database

* Right Click on databases and select Restore Database.
* Select to restore from a device and browse to the file containing and empty hm tools database bak file. This is located in \JDA\ESO Installation\Tools\EmptyToolsDB\
* Select the Restore check box for the backup set.
* In the to-database field enter the name of the HM object repository, for example hm\_tools. This database should not already exist.
* Adjust the paths to the recommended non-system data and log paths.
* Click OK.

1. Permissions for HM DB User

* Select Security, Logins and Right Click on the HM DB User, and perform the following:
* In user mappings, Select the Map check box for the HM tools database and select the db\_owner in the role membership section at the bottom of the page.
* Select the Map check box for the HM object repository database and select the db\_datareader in the role membership section at the bottom of the page.
* Click Ok.

1. Import the HM Tools Application into the Tools database

* The tools code .dat files are located in the folder \JDA\ESO Installation\Tools\Current Version\Extracted Files.
* Navigate to the Extracted Files folder.
* Open a command prompt an executed the following:

Importbuild *DestinationServerName ToolsDBName DBUserName DBUserPassword*

1. DestinationSeverName = The HM SQL Server
2. ToolsDBName = The database that was restores from the empty tools DB (hm\_tools)
3. DBUserName = The SQL User created in step #1.
4. DBUserPassword = The password associated to the user.
5. Object Repository Views

* Open SQL Server Management Studio, login using he SQL User created in step 1 and Select the HM Server.
* Select File Open and open the file orbviews.sql located in \JDA\ESO Installation\Tools\SQL Scripts.
* Replace all occurrences of the string %orb% with the name of the hm tools database (hm\_tools).
* Ensure the database is set to the tools database and execute the script.

1. One Time Server Deploy

* From the \JDA\ESO Installation\OneTimeDeploy\ExtractedFiles, run ScriptRunnerV2x.exe
* In the Target Database area of the page, enter the server name, HW DB User and Password.
* Click Connect.
* Click the Wave Database drop-down list and select the hm tools database.
* Click Run. A confirmation message is displayed.
* Click Yes. A confirmation message is displayed.
* Click OK. The Output files from window is displayed.
* Review the output files for errors.

1. Run tools patch if present
2. Verify SQL Server Agent Startup

* Navigate to Windows Services, and verify that the SQL Server Agent is running and is set to Automatic startup.

1. Create APE Scheduler Job

* Click SQL Server Agent.
* Right-click Jobs and select New Job…The New Job window is displayed.
* In the Name field, enter APE Scheduler.
* Select Steps in the left pane and perform the following:
* Click New

1. In the Step Name field, enter APE Scheduler.
2. In the Database field, enter HM.
3. In the Command field, enter the following:

declare @current\_timestamp datetime

select @current\_timestamp = current\_timestamp exec ape\_scheduler\_clock @current\_timestamp

* Click OK.
* Select Schedules in the left pane and perform the following:
* Click New

1. In the Name field, enter Every 5 minutes.
2. Click the Occurs drop-down list and select Daily.
3. Select the Occurs every option and enter 5 minutes.

* Click OK twice.

HM Web Server

Prerequisites

* Windows Server 2012R2 or 2016.
* MSXML 4.0 SP 2
* .NET Framework 3.5 SP 1
* MS Report Viewer Redistributable 2008, Service Pack 1
* Visual C++ 2005 Redistributable Package, Service Pack 1
* Visual C++ 2005 Redistributable Package SP 1 ATL Hotfix
* SQL Client Tools
* SQL Server 2005 Backward Compatibility Components
* HM Server should be a member of the Active Directory domain. If the HM Server is in a workgroup, only local deploys using the Enterprise Deploy Tool can be performed
* HM Server should be "enabled for delegation" in Active Directory Users and Computers
* HM Server must be able to access Target Web/APP Servers
* Local HM Server -> requires an Active Directory account with administrative rights on the Web/App servers you are deploying and an HM user account with the Host Management role.
* The local deploy server address needs to be added to the Local Intranet Security Zone in Internet Explorer on the target server.
* Internet Explorer must be configured as per the description provided in the Retail Classic Web Client Requirements document.

IIS Installation

1. IIS Installation

* On the target server, open Server Manager and select Manage, then Add Roles and Features.
* Select Role-based installation, click Next.
* Choose to Select a Server, then highlight the local server and click Next.
* In Server Roles list, expand Web Server IIS and enable the set the following:

1. Common HTTP features
   1. Default Document
   2. Directory Browsing
   3. HTTP Errors
   4. Static Content
2. Health and Diagnostics
   1. HTTP Logging
   2. ODBC Logging
   3. Request Monitor
3. Performance
   1. Static Content Compression
   2. Dynamic Content Compression
4. Security
   1. Request Filtering
   2. Basic Authentication
   3. Windows Authentication
5. Application Development
   1. .Net Extensibility 3.5
   2. .Net Extensibility 4.5
   3. ASP
   4. ASP.NET 3.5
   5. ASP.NET 4.5
   6. ISAPI Extensions
   7. ISAPI Filters
6. Management Tools
   1. Management Console
   2. IIS 6 Management Compatibility
   3. Management Scripts and Tools
   4. Management Services

* Click Next, then Install.
* Click Next and Review the installation, click Install. Restart the IIS Service.
* Exit Server Manager.

IIS Configuration

1. IIS Administrative Configuration

* Navigate to Administrative Tools, Internet Information Services Manager.

1. Highlight the Server name, Double Click Logging and set the following:
   1. Click Select Fields and Select all check boxes.
   2. In the directory field, enter a non-system drive in place of %SystemDrive%.
   3. Select Use Local Time.
   4. Click Apply, then Click back on the server name.
2. Double Click on ASP, and set the following:
3. Enabled Parent Paths = True
4. Response Buffering Limit = 41943040
5. Script Time-Out = 00:05:00
6. Click Apply, then Click back on the server name.
7. Double Click on Authentication and perform one of the following actions for the IIS Anonymous Account:
   1. If you have single server environments, leave the default setting.
   2. If you have multiple server environments, select Right Click to Edit. use the same account on all servers. A domain account is recommended. If you are using local accounts, verify the account name and password is the same on all servers. Note: Add this user to the IIS\_USRS group in Local Users and Groups.

* Navigate to Administrative Tools, Component Services, expand My Computer, Distributed Transactions. Right Click on Local DTC, select the Properties Security and select the following:
  1. Network DTC Access
  2. Allow Remote Administration
  3. Allow Inbound
  4. Allow Outbound
  5. No Authentication Required
  6. Enabled XA Transactions
  7. Close component Services
  8. Restart DTC

HM Tools Installation

1. Create directories and settings files

* Create a directly structure for the application and log files. If possible use a non-system drive. The following 3 subdirectories need to be created:
  1. \JDA\HM Server
  2. \JDA\LogFiles\Log4Rads
  3. \JDA\LogFiles\IIS
* Grant modify access for the HM Server and Logfiles directories to the IIS anonymous user account.
* From the folder \JDA\ESO Installation\Tools there will be an example GlobaSetings.xml file. Copy this file to the root of the JDA directory.
* Open the file in a text editor and modify the following settings:

1. HM DB Server Name
2. HM Server Name (This will be the name of the new web site)
3. HM Object Repository DB name
4. HM Object Repository DB User
5. HM Object Repostitory DB User Password
6. Fully qualified domain name of hm server
7. HM Tools DB Name
8. HM Tools DBUser Name
9. HM Tools DB User Password

* From the folder \JDA\ESO Installation\Tools there will be an example Logconfig.xml file. Copy this file to the root of the JDA directory.
* Open the file in a text editor and rules for the correct directory paths:

<?xml version="1.0" encoding="utf-8"?>

<log4rad>

<appenders>

<file\_appender id="AllErrors" base\_file\_name="E:\JDA\logs\log4rad\EMCWT1403\_allerrors" roll\_size="10000000" roll\_count="10" />

</appenders>

<event\_source\_rules>

<event\_source prefix="">

<rule level="ERROR" appender="AllErrors" />

</event\_source>

<event\_source prefix="Platform.WaveServiceProduction.MemoryContext.get\_aspBased">

<rule appender="AllErrors" level="IGNORE"/>

</event\_source>

</event\_source\_rules>

</log4rad>Create the web site

* Open Internet Information Services (IIS) Manager
* Expand the server node, and Right Click on Sites, then Click Add Web Site.
* Complete the following:

1. Enter the name of the new web site that was configured in the global settings file.
2. Enter the Physical path web site. The should be the directory created in step 1, for example \JDA\HM Server
3. If the site will use SSL and the certificate has been loaded on the server, click the Type drop-down list and select https and enter 443 in the Port field.
4. Normally web servers are dedicated to the application and the IP address field can be left to contain All Unassigned.
5. In the Host Name field, enter the URL for this Web Site. If this is left blank, the server responds to any URL that resolves to the server.
6. Deselect the Start Web site immediately check box.

* Click OK.

1. Deploy the HM tools application

* From the folder where deploy.exe is located and Double Click on the file deploy.exe.
* In the login and password fields enter the HM tools user id and password
* Click Login
* In the Hosting Management Server filed enter the name of the web site that was created.
* Select the Release Mode option
* In the Target Directory, select the Physical path for the Web Site
* The release field should contain the current version of the tools (3.5.4.6)
* From the Web Site drop down list select the name of the Web Site that was created.
* The namespace field must match the namespace entered in the global settings file.
* Select the options to restart services and install APE.
* Click Deploy, when finished check for errors.

1. Set Anonymous user at the web site level.

* Open Internet Information Services (IIS) Manager, Expand Server Node and Sites.
* Click the HM Web site.
* Double-click Authentication. The Authentication window is displayed.
* Disable Anonymous Authentication for the web site.
  1. Click Anonymous Authentication.
  2. In the Actions pane on the right, click Disable.
  3. Click Windows Authentication.
  4. In the Actions pane on the right, click Enable.
* Access the Tools virtual directory authentication settings.
* Expand the HM web site and Services, Click Tools.

1. Double-click Authentication. The Authentication window is displayed.
2. Enable Anonymous Authentication.
3. Click Anonymous Authentication.
4. In the Actions pane on the right, click Enable.
5. Click Windows Authentication.
6. In the Actions pane on the right, click Disable.

* Restart IIS.

1. IIS, by default, does not allow paths to include files in the bin directory (where ORF.dll is located). If a HTTP Error 404.8 is displayed while attempting to access the application Welcome page, perform the following to modify applicationHost.config:

* Navigate to %win%\System32\inetsrv\config.
* Backup applicationHost.config.
* Open the file with a text editor such as Notepad.
* Search for hiddenSegments.
* Comment out the line <add segment="bin" />
* Save and Close the file.
* Restart IIS.
* Open the browser and try the page again.

Tools Basic Setup

1. User and Client configuration

* From the HM Web Server load the default web site <http://localhost>
* Login to the Hosting Management

1. Username: Waveadmin
2. Password: admin
3. It is good practice to change this password

* In the Search box at the top of the screen, Enter Client Setup, the Client Setup window is displayed.
* Click Add Client, and complete the following fields:
* Client Code
* Name
* Click the User tab and complete the following fields, the add the Client Admin User:

1. First Name
2. Last Name
3. Language
4. Password

* Click the Address tab and complete the following:

1. Address Line 1
2. City
3. State
4. Postal Code
5. Country

* Click Continue, and note the user name assigned on the message, then Click OK.
* Click the Language tab and select a default language.
* Click the Services tab and select Default and the Hosting Management Explicit check boxes.
* Save & Close
* Logout, but keep the browser Open.
* and close the browser.

1. Employee and HM User

* Login use the Client Admin login created in the previous step.
* Using the search at the top of the screen find Employee Setup.
* Click Add Employee, to create the user that will be used to deploy to the Web and App Servers.
  1. Enter an Appropriate Name, in the name fields.
* Click the Login tab, and complete the following:
  1. Login: This must match the name of the domain login with access to the servers.
  2. Password: This must match the \_\_WaveLoginPassword entered in the Global Settings file.
  3. De-Select the Force password on next login.
* Click on the role tab and Select the Hosting Management user role.
* Save and Close
* If the login name does not match the user’s domain account, you can select the user again and select the Login tab and change the Employee Member ID
* Logout and close the browser
* Open the site again, if logged into the domain as the HM user, the site should not prompt for a login.
* If not logged in as the domain HM User, Login with HM User id and password.
* Navigate to Hosting Management, Server Setup, the Servers window is displayed.
* Click Add Server
* Complete the following:
  1. In the Server Name field, enter the name of the HM server.
  2. In the Description field, enter a server description.
  3. Click the Location drop-down list and select the location for the server. If no locations exist for the server, select Add New, enter a name and description for the new location. Note: A new location is needed for an environment that has a firewall between it and the HM server.
  4. Click Save & Close.
* Click the IP Address Tab and perform the following:

1. Click Ping for IP Address. A confirmation message is displayed.
2. Click OK.
3. Click Save & Close.

* From the command prompt, run the following command replacing the FQDN or hostheader of the HM server and server name:
  1. Setspn - A http/servername.domain.com servername
  2. A registering ServicePrincipalNames will respond with the following:

Registering ServicePrincipalNames for CN=servername,CN=Computers,DC=domain,DC=domain,DC=com

http/servername.domain.com

Updated object