Harmonia Install Guide (using the installer)

Nicole Keller

Table of Contents

1. Pre-Install System Requirements
   1. Hardware Requirements
      1. Hardware Requirements for the Harmonia Server
         * At least 1 GHz Pentium CPU (at least 2GHz recommended).
         * Minimum 256 MB of RAM (512 MB recommended).
         * A hard disk partition with enough space to accommodate the Harmonia Server code - approx. 150 KB.
         * Adequate space in the Active Directory for Harmonia data.
         * VGA or higher-resolution monitor.
         * Keyboard.
         * Mouse.
         * Network adapter.
      2. Hardware Requirements for the Target Systems
         * At least 400 MHz CPU.
         * Minimum 128 MB of RAM.
         * A hard disk partition with enough space to accommodate the User Environment Simulator code – approx. 100KB.
         * VGA or higher-resolution monitor.
         * Keyboard.
         * Mouse.
         * Network adapter.
   2. Software Requirements
      1. Software Requirements for the Harmonia Server
         * Windows 2003 Server or higher.
         * DNS and Active Directory Installed.
         * MS Certificate Services installed.
         * Java Standard Edition Runtime Environment (JRE) 1.4.1 or newer.
         * JAVA\_HOME needs to be set up.
      2. Software Requirements for the Target Systems
         * Windows 2000 or XP.
         * Java Standard Edition Runtime Environment (JRE) 1.4.1 or newer.
         * JAVA\_HOME needs to be set up.
      3. Software Requirements for the Harmonia Applications
         * JavaMail.
         * OpenOffice both the SDK and the EXE.
         * Apache Ant
2. First the user has to install the Harmonia Application ( This gives the user all the files that will have to be added.
3. Before Running the Harmonia Application after the install.
   1. Active Directory Setup
      1. Setting Up Active Directory and DNS Server

Step 1: Open the Server Manager

Step 2: Select action in the tool bar and then click add roles

Step 3: Add Active Directory Domain Services and DNS server there will be instructions on how to start the active directory wizard

At the end of the wizard you should have set up the users domain name to look like this : firstInitialLastNameLab.company.com, org, gov, etc.The forest functional level should be Server 2008 R2. The NETBIOS Name is usually the first part of your user domain name.

* + 1. .LDF File Modifications

The user will need to edit the .ldf files that are found in PM/doc/ADSchema folder. For every [domain name] the user will have to replace it with their own domain name ( this can be found in the server manager). The way this should be formatted is for example if my domain name is jdoe.computer.net, the way I would put it in my .ldf files is DC= jdoe, DC = computer, DC = net.

* + 1. Extending the Active Directory Schema

The Active Directory Schema must be extended with a set of PM-specific AD attributes and classes. Appendix A contains a description of them.

You may extend the AD schema by following the steps:

Step 1. Log on as administrator on the Windows 2000 or 2003 server that will host the PM server.

Step 2. Add the following key to the registry:

HKEY\_LOCAL\_MACHINE/System/CurrentControlSet/Services/NTDS/Parameters/Schema Update Allowed

with the value (REG\_DWORD)1 (i.e., true).

Step 3. Update the two files PMAttributes.ldf and PMClasses.ldf, which were contained in the distribution file, to reflect your domain name. Specifically, replace all occurrences of the string “DC=pm1, DC=local” by your domain name, for example “DC=fabrikam, DC=com” in both files.

Step 4. Open a MS-DOS command window, cd to the directory that contains the two edited files PMAttributes.ldf, PMClasses.ldf, and PMContainers.ldf and run the commands:

ldifde -i -f PMAttributes.ldf

ldifde -i -f PMClasses.ldf

ldifde –i –f PMContainers.ldf

Afterwards, you may use the ADSI editor to examine your changes. Look for attributes and classes with the prefix “pm”.

Note that once a class is created, it cannot be modified or deleted (the only exception is adding or deleting *optional* attributes to/from the class).

* 1. Certificate Generation
     1. Harmonia Server Certificate

Clients like PM Administrative Tool communicate with the PM Engine (server) using SSL, hence the need for the server (and the client) to identify itself to the other party through public key certificates. This section explains how to obtain a server certificate from a MS Stand-alone Certification Authority (CA).

Step 1. Log as Administrator on the computer that will host the PM engine (server). Make sure that a stand-alone certification authority is installed, and that it automatically issues the requested certificates (in order to simplify the procedure). Install the CA root certificate in the Trusted Root Certification Authorities.

Step 2. Create a folder named Keystores. This folder will contain the PM server key store and trust store. The key store is a repository for the PM server’s private key and certificate. The trust store is a repository for public key certificates that the PM server trusts. For simplicity, we assume that the same CA is used to issue all certificates. Then the trust store needs only contain the CA’s root certificate.

Step 3. Open a MS-DOS command window, cd to the Keystores folder, and run the following commands:

>keytool -genkey -keyalg RSA -alias pmserver -keystore serverKeystore

Enter keystore password: aaaaaa

What is your first and last name?

[Unknown]: pmserver

What is the name of your organizational unit?

[Unknown]: CSD

What is the name of your organization?

[Unknown]: NIST

What is the name of your City or Locality?

[Unknown]: Gaithersburg

What is the name of your State or Province?

[Unknown]: Maryland

What is the two-letter country code for this unit?

[Unknown]: US

Is CN=pmserver, OU=CSD, O=NIST, L=Gaithersburg, ST=Maryland, C=US correct?

[no]: yes

Enter key password for <pmserver>

(RETURN if same as keystore password):

>keytool -certreq -alias pmserver -file pmserver.csr -keystore serverKeystore

Enter keystore password: aaaaaa

The file pmserver.csr contains a standard certificate request.

Step 4. Use the MS Internet Explorer to submit the certificate request to the CA installed on the MS Windows Server 2000 or 2003. Namely, open the URL

<http://mymachine/certsrv>

where “mymachine” must be replaced by the server’s host name. From the web page displayed, select the radio button “Request a certificate” and click the “Next” button. From the next page, select the radio button “Advanced request” and click the “Next” button. From the next page, select the radio button “Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file” and click the “Next” button. Copy the contents of the pmserver.csr file and paste it in the text area titled “Saved Request”. Click the “Submit” button.

In the next page, select the radio button “Base 64 encoded” and select the link “Download CA certificate”. When asked, save the downloaded certificate under the name “pmserver.cer” to the Keystores folder.

Step 5. In the Windows Explorer window, double-click on the certificate pmserver.cer. In the certificate manager, select the tab “Details” and click the “Copy to File…” button. This launches the Certificate Export Wizard. Click the “Next” button, select the radio button “Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)”, check the checkbox “Include all certificates in the certification path if possible”, and click the “Next” button. Export the certificates under the name pmserver.p7b to folder Keystores. Click “Next”, then “Finish”.

Step 6. In the MS-DOS command window, run the following command:

>keytool -import -alias pmserver -file pmserver.p7b -keystore serverKeystore

Enter keystore password: aaaaaa

Top-level certificate in reply:

Owner: CN=PMCA, OU=CSD, O=NIST, L=Gaithersburg, ST=Maryland, C=US, EMAILADDRESS=

serban.gavrila@nist.gov

Issuer: CN=PMCA, OU=CSD, O=NIST, L=Gaithersburg, ST=Maryland, C=US, EMAILADDRESS

=serban.gavrila@nist.gov

Serial number: 186ae6f14015eb86435db3746312cab9

Valid from: Fri Aug 26 12:26:08 EDT 2005 until: Mon Aug 25 12:34:37 EDT 2008

Certificate fingerprints:

MD5: 68:F5:23:C4:7F:11:AF:D5:B1:1D:EB:0A:7B:22:6E:96

SHA1: D6:E0:29:DF:3E:D4:A7:44:F2:86:3E:F9:09:1C:E4:E6:11:93:CE:59

... is not trusted. Install reply anyway? [no]: yes

Certificate reply was installed in keystore

Step 7. Using the same certificate manager, save the CA root certificate base 64-encoded as root.cer, then run the command:

>keytool -import -alias root -file root.cer -keystore serverTruststore

Enter keystore password: aaaaaa

Owner: CN=PMCA, OU=CSD, O=NIST, L=Gaithersburg, ST=Maryland, C=US, EMAILADDRESS=

serban.gavrila@nist.gov

Issuer: CN=PMCA, OU=CSD, O=NIST, L=Gaithersburg, ST=Maryland, C=US, EMAILADDRESS

=serban.gavrila@nist.gov

Serial number: 186ae6f14015eb86435db3746312cab9

Valid from: Fri Aug 26 12:26:08 EDT 2005 until: Mon Aug 25 12:34:37 EDT 2008

Certificate fingerprints:

MD5: 68:F5:23:C4:7F:11:AF:D5:B1:1D:EB:0A:7B:22:6E:96

SHA1: D6:E0:29:DF:3E:D4:A7:44:F2:86:3E:F9:09:1C:E4:E6:11:93:CE:59

Trust this certificate? [no]: yes

Certificate was added to keystore

* + 1. Harmonia User Certificate

Obtaining a user’s certificate is very similar to obtaining the server’s certificate. Here we detail the procedure for the user “super”. For other users, simply replace “super” with the user’s name everywhere.

Step 1. Log as Administrator on the computer whose CA was used to issue the PM server’s certificate.

Step 2. Create a folder named Keystores. This folder will contain the PM user key store and trust store. The key store is a repository for the user’s private key and certificate. The trust store is a repository for public key certificates that the user trusts. For simplicity, we assume that the same CA issues all certificates. Hence, the trust store needs only contain the CA’s root certificate.

Step 3. Open a MS-DOS command window, cd to the Keystores folder, and run the following commands:

>keytool -genkey -keyalg RSA -alias super -keystore superKeystore

Enter keystore password: aaaaaa

What is your first and last name?

[Unknown]: super

What is the name of your organizational unit?

[Unknown]: CSD

What is the name of your organization?

[Unknown]: NIST

What is the name of your City or Locality?

[Unknown]: Gaithersburg

What is the name of your State or Province?

[Unknown]: Maryland

What is the two-letter country code for this unit?

[Unknown]: US

Is CN=super, OU=CSD, O=NIST, L=Gaithersburg, ST=Maryland, C=US correct?

[no]: yes

Enter key password for <super>

(RETURN if same as keystore password):

>keytool -certreq -alias super -file super.csr -keystore superKeystore

Enter keystore password: aaaaaa

The file super.csr contains a standard certificate request.

Step 4. Use the MS Internet Explorer to submit the certificate request to the CA installed on the MS Windows Server 2000 or 2003. Namely, open the URL

<http://mymachine/certsrv>

where “mymachine” must be replaced by the server’s host name. From the web page displayed, select the radio button “Request a certificate” and click the “Next” button. From the next page, select the radio button “Advanced request” and click the “Next” button. From the next page, select the radio button “Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file” and click the “Next” button. Copy the contents of the super.csr file and paste it in the text area titled “Saved Request”. Click the “Submit” button.

In the next page, select the radio button “Base 64 encoded” and select the link “Download CA certificate”. When asked, save the downloaded certificate under the name “super.cer” to the Keystores folder.

Step 5. In the Windows Explorer window, double-click on the certificate super.cer. In the certificate manager, select the tab “Details” and click the “Copy to File…” button. This launches the Certificate Export Wizard. Click the “Next” button, select the radio button “Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)”, check the checkbox “Include all certificates in the certification path if possible”, and click the “Next” button. Export the certificates under the name super.p7b to folder Keystores. Click “Next”, then “Finish”.

Step 6. In the MS-DOS command window, run the following command:

>keytool -import -alias super -file super.p7b -keystore superKeystore

Enter keystore password: aaaaaa

Top-level certificate in reply:

Owner: CN=PMCA, OU=CSD, O=NIST, L=Gaithersburg, ST=Maryland, C=US, EMAILADDRESS=serban.gavrila@nist.gov

Issuer: CN=PMCA, OU=CSD, O=NIST, L=Gaithersburg, ST=Maryland, C=US, EMAILADDRESS

=serban.gavrila@nist.gov

Serial number: ...

... is not trusted. Install reply anyway? [no]: yes

Certificate reply was installed in keystore

Step 7. Using the same certificate manager, save the CA root certificate base 64-encoded as root.cer, then run the command:

>keytool -import -alias root -file root.cer -keystore superTruststore

Enter keystore password: aaaaaa

Owner: CN=PMCA, OU=CSD, O=NIST, L=Gaithersburg, ST=Maryland, C=US, EMAILADDRESS=

serban.gavrila@nist.gov

Issuer: CN=PMCA, OU=CSD, O=NIST, L=Gaithersburg, ST=Maryland, C=US, EMAILADDRESS

=serban.gavrila@nist.gov

Serial number: 186ae6f14015eb86435db3746312cab9

Valid from: Fri Aug 26 12:26:08 EDT 2005 until: Mon Aug 25 12:34:37 EDT 2008

Certificate fingerprints:

MD5: 68:F5:23:C4:7F:11:AF:D5:B1:1D:EB:0A:7B:22:6E:96

SHA1: D6:E0:29:DF:3E:D4:A7:44:F2:86:3E:F9:09:1C:E4:E6:11:93:CE:59

Trust this certificate? [no]: yes

Certificate was added to keystore

* + 1. Where the certificate and keystore needs to be located

The user’s certificate and keystore needs to be put in the keystores folder. The proper naming format for the keystore is: *computername***Keystore.**

* 1. Configuration File Modifications
     1. PMServerConfiguration.pm

The user will have to go to the PM/conf folder and edit the PMServerConfiguration.pm file using a text editor. The modifications that need to be made are the replacement of [Client\_Computer\_Name] with the client’s computer name. In addition the [Server\_Computer\_Name] also need to be replaced by the server’s computer name.

* + 1. PMClientConfiguration.pm

The user will have to go to the PM/conf folder and edit the PMClientConfiguration.pm file using a text editor. The modifications that need to be made are the replacement of [Client\_Computer\_Name] with the client’s computer name.

* 1. Folders that Need to be Added
     1. PMWorkArea

The user will need to create a folder called pmworkArea in the C:\ drive. This is where all the data that is generated by the Harmonia(Policy Machine).

1. Running Harmonia
   1. Server

To run the server, double click on the server.bat file this should have been added on the Desktop after installing Harmonia. The user will then be promted to enter your password as well as the keystore password. **Note:** The default keystore password is: aaaaaa.

* 1. Administrator Tool

To run the administrator tool, first start the server and then double click on the super.bat file found on the Desktop. The user will be prompted to enter the keystore password. After that a windows explorer will pop up, this is where the user will need to choose the server’s keystore which is superKeystore and after choosing that the user will need to select the truststore which is: clientTruststore. Finally the user will need to input super’s password which is: super.

* 1. Client Tool

To run the client tool, first start the simulator by double clicking the simulator.bat file found on the Desktop. After that is running double click on the sesmgr.bat file found on the Desktop, a prompt will pop up that instructs the user to input the username and the user’s password. By default we have 5 users: Dave, Bob, Katie, Alice and Charlie. Their passwords are their names, everything is in lowercase when putting it in the prompt.

1. Important Notes
   1. Data that Needs to be Changed ONLY if you changed it.
      1. Keystore Passwords

Keystore passwords only need to be changed if the user ends up changing the password. The default keystore password is: aaaaaa. If the user does change the password they will have to go into each batch file and update the passwords.