RHEV 2.2:
REST API INSTALLATION

BY JAMES RANKIN
12/22/10

TABLE OF CONTENTS

OVERVIEW

This whitepaper will outline how a RHEV administrator may add the REST API developer preview onto an existing RHEV 2.2 installation. Please ensure the RHEV 2.2 environment is installed and operational before installing this REST API.

Note also that the REST API will be installed automatically once RHEV-M reaches version 2.3. This document applies only to RHEV-M 2.2.

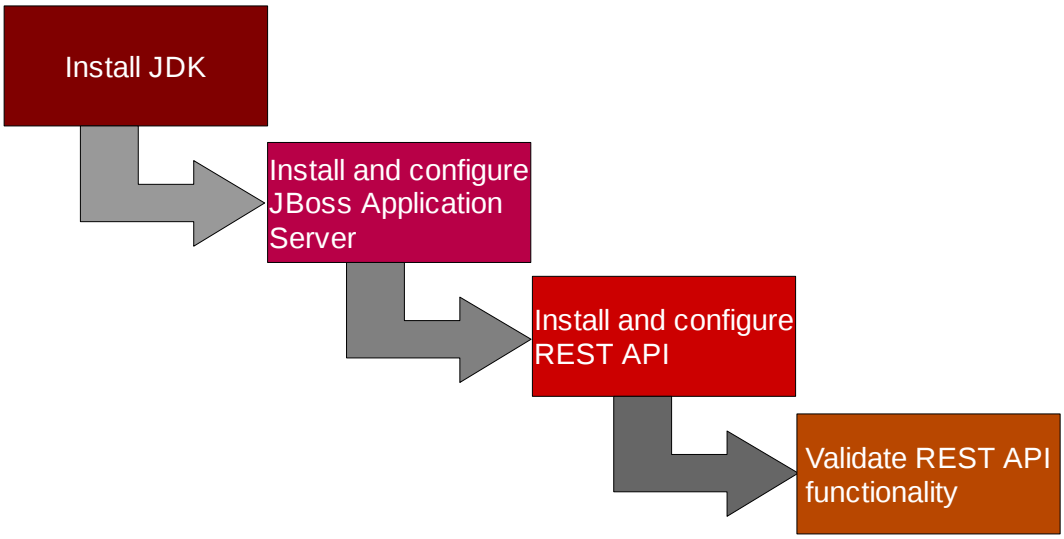
The REST API developer preview homepage is:

https://fedorahosted.org/rhevm-api/

The developer documentation for the API is available at:

http://markmc.fedorapeople.org/rhevm-api/en-US/html/index.html

The workflow of this install will be as follows:



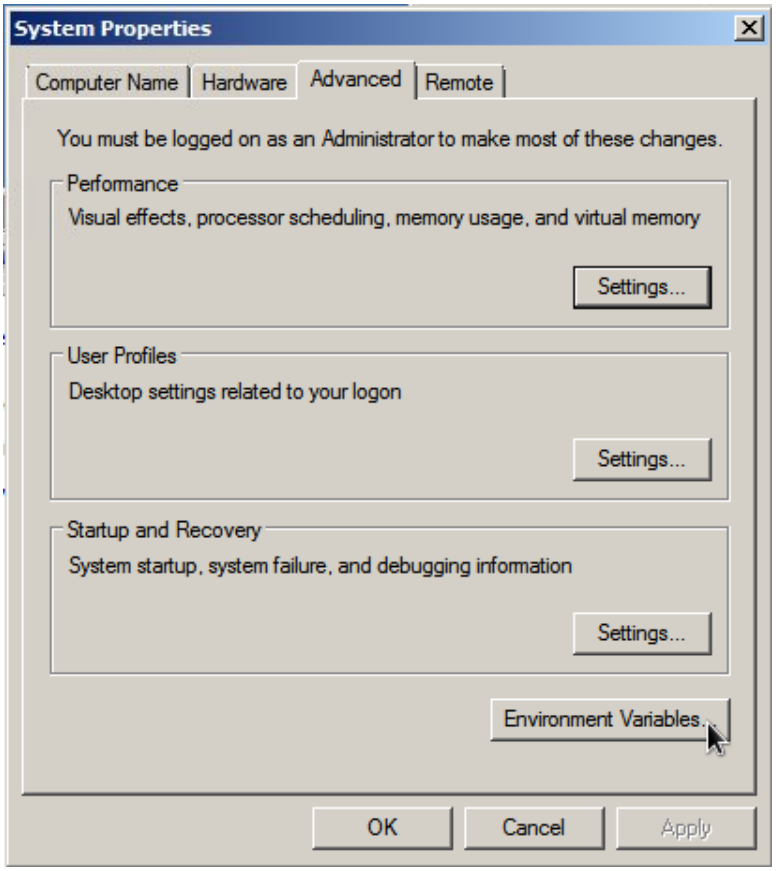
JAVA AND ENVIRONMENT VARIABLES

Because the REST API runs on an embedded JBoss Application Server, the Oracle JDK must be installed onto the Windows Server 2008 R2 machine that runs the RHEV Manager service.

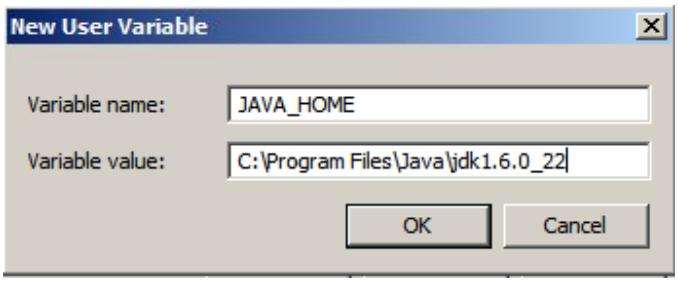
First, download the current 64 bit JDK and install it onto the RHEV-M server. At the time of the writing of this whitepaper, the current JDK is “Java 6 Update 22.” The JDK download is available at the Java SE landing page: http://www.oracle.com/technetwork/java/javase/downloads/index.html

After installation of the JDK, the %JAVA_HOME% environment variable must be set to the JDK path; the JBoss Application Server will not start unless this variable is correctly defined.

To set the %JAVA_HOME% variable in Windows Server, click “Start”, then right-click “Computer” and choose “Properties”. Toward the upper left of the System properties window, click the “Advanced system settings” link. Next, click the “Environment Variables...” box, as shown below.



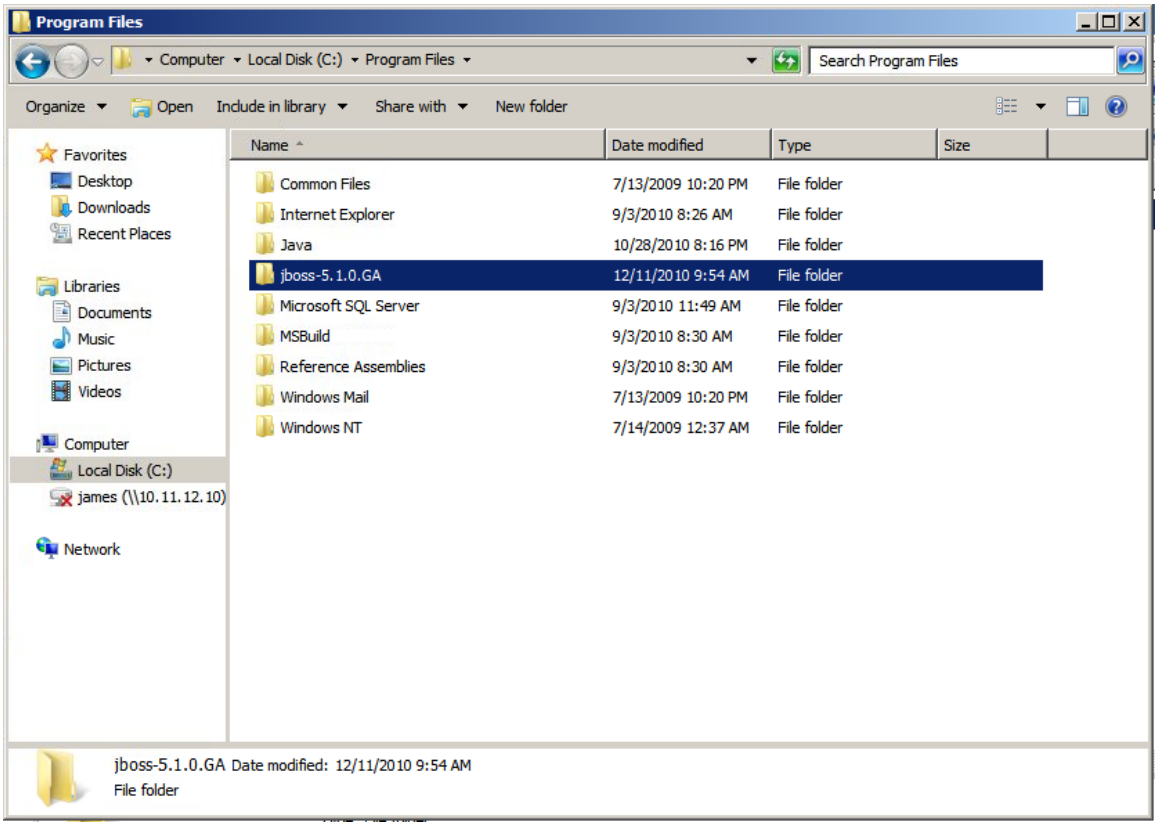
In the Environment Variables window, click the “New” button, and set the JAVA_HOME variable to the path to your newly installed JDK. In the example below, the variable is set to the default path for the 64 bit JDK 6u22 install.



JBOSS INSTALLATION

With the JDK installed, download version 5.1.0 of the JBoss Application Server:
http://sourceforge.net/projects/jboss/files/JBoss/JBoss-5.1.0.GA/jboss-5.1.0.GA.zip/download

Install JBoss by simply unzipping it into a directory of your choice. In the example below, JBoss was placed in “Program Files.”



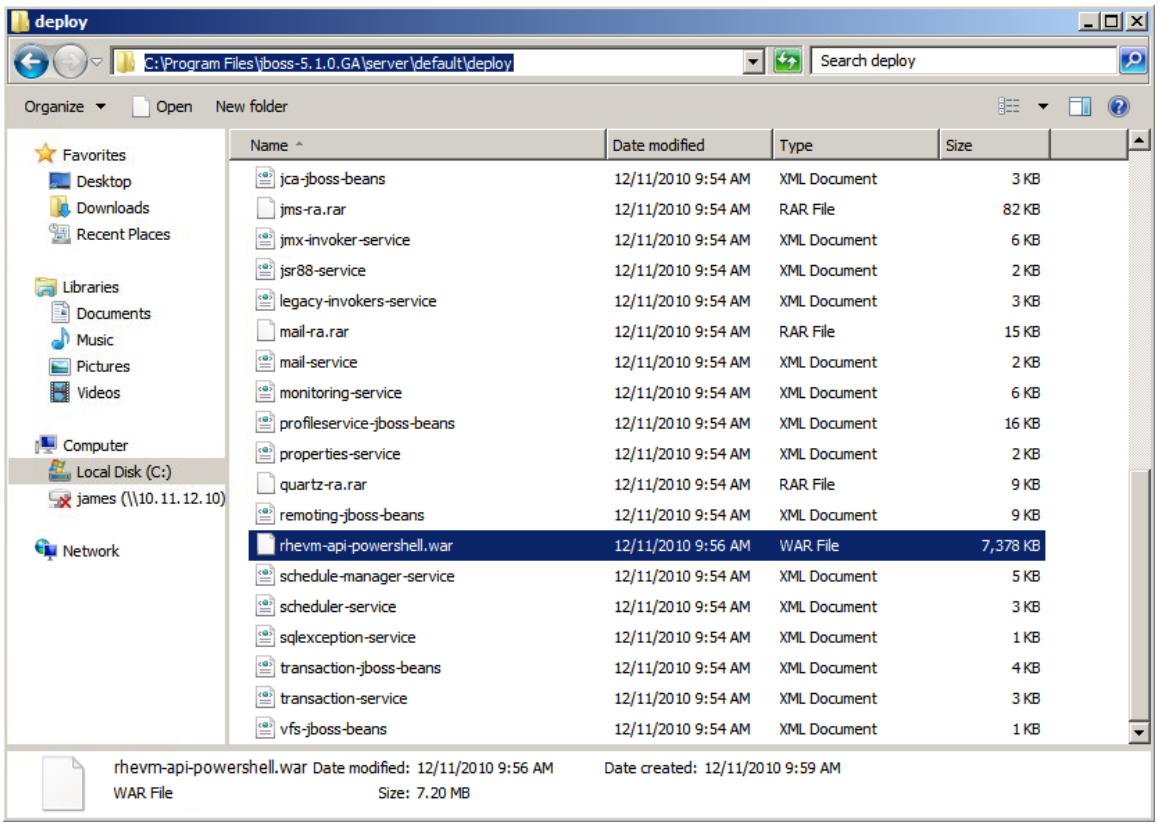
REST API SETUP

Download the current “milestone” release of the REST API from the REST API homepage on fedorahosted.org. At the time of writing, the current milestone is 5:

https://fedorahosted.org/releases/r/h/rhevm-api/rhevm-api-distro-0.9-milestone5.zip

Like the JBoss install, simply unzip the API zip file into Program Files, or any other location.

Navigate into the “webapp” folder of the REST API. Copy the **`rhevm-api-powershell.war`** file and then paste it into the **`\server\default\deploy`** directory inside the JBoss install, as shown below.



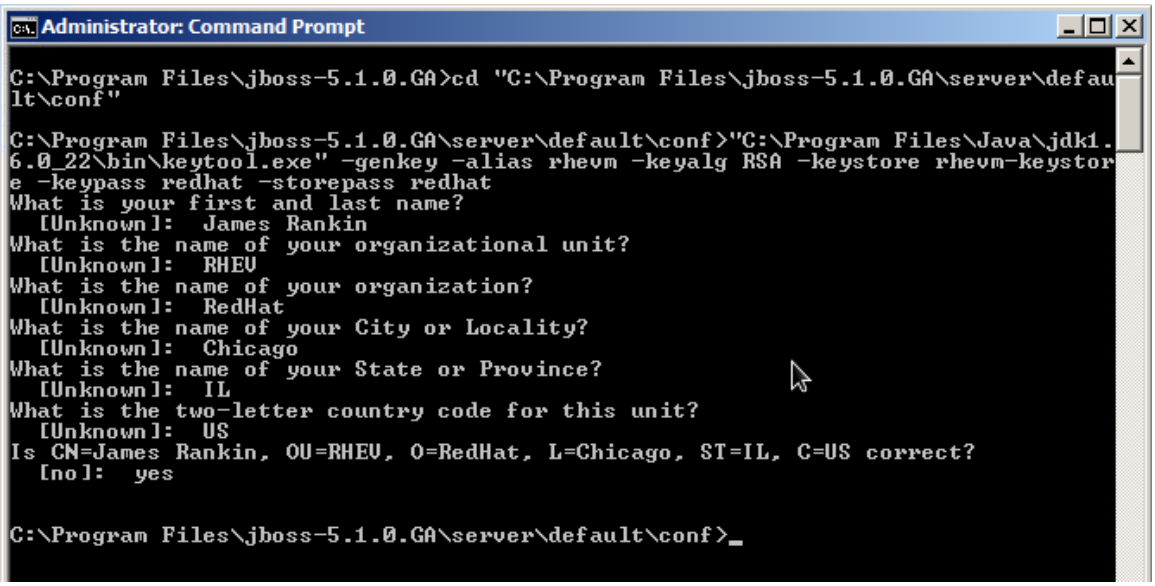
Next, create a certificate for https communication (which is also described in the README_HTTPS file). To do this, open a command prompt in Windows *as an Administrator*. Simply navigate to the “Command Prompt” icon in the Start menu, right-click it, and choose “Run as Administrator.” If the command prompt is not opened as an administrator, then you will not have write access into Program Files.

With the command prompt open, navigate to your **`JBoss\server\default\conf`** directory, and run the following Java keytool command to generate a certificate:

```
“C:\Program Files\Java\jdk1.6.0_22\bin\keytool.exe” -genkey -alias rhevm
-keyalg RSA -keystore rhevm-keystore -keypass redhat -storepass redhat
```

In this example, note that the path to keytool.exe is fully qualified and in quotes. If using a JDK other than 6U22, this path would be different, so using tab completion is advised. Also, note that the “redhat” values in this command are certificate passwords; please change these to any value you prefer.

After running the keytool.exe command, answer the certificate creation questions when prompted. An example is below.



With the certificate creates, the next step is to modify the **`server.xml`** file in the JBoss install. *Start WordPad as an Administrator* and navigate to **`$JBOSS_HOME\server\default\deploy\jbossweb.sar\`** and open **`server.xml`**

With the server.xml file open, find the following section:

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore
<Connector protocol="HTTP/1.1" SSLEnabled="true"
     port="8443" address="${jboss.bind.address}"
     scheme="https" secure="true" clientAuth="false"
     keystoreFile="${jboss.server.home.dir}/conf/chap8.keystore"
     keystorePass="rmi+ssl" sslProtocol = "TLS" />
-->
```

First, ensure that the “SSL/TLS Connector...” stanza is no longer commented out; these lines are commented out by default. Next, modify the keystoreFile and keystorePass values to correspond to the filename and passwords chosen when creating the certificate. Since the example here uses rhevm-keystore as the keystore file and “redhat” as the password, the server.xml should be edited as shown below:

```
<!-- SSL/TLS Connector configuration using our new keystore -->
<Connector protocol="HTTP/1.1" SSLEnabled="true"
     port="8443" address="${jboss.bind.address}"
     scheme="https" secure="true" clientAuth="false"
     keystoreFile="${jboss.server.home.dir}/conf/rhevm-keystore"
     keystorePass="redhat" sslProtocol = "TLS" />
```

The three changes necessary are highlighted above in yellow. Notice again how the comment at the beginning of the stanza is now closed at the end of the first line. After making these changes, save the file in WordPad.

Next, the JBoss run.conf.bat file will need one edit to ensure that the REST API does not produce a port conflict. Again run *WordPad as an Administrator*, and open the **`$JBOSS_HOME\bin\run.conf.bat`** file.

Find a JAVA_OPTS line and add “**`-Djboss.service.binding.set=ports-01`**” to the end. For example, find the following existing section:

```
rem # Reduce the RMI GCs to once per hour for Sun JVMs.
set "JAVA_OPTS=%JAVA_OPTS% -Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000"
```

And edit this as shown below (with the change highlighted in yellow):

```
rem # Reduce the RMI GCs to once per hour for Sun JVMs.
set "JAVA_OPTS=%JAVA_OPTS% -Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000 -Djboss.service.binding.set=ports-01"
```

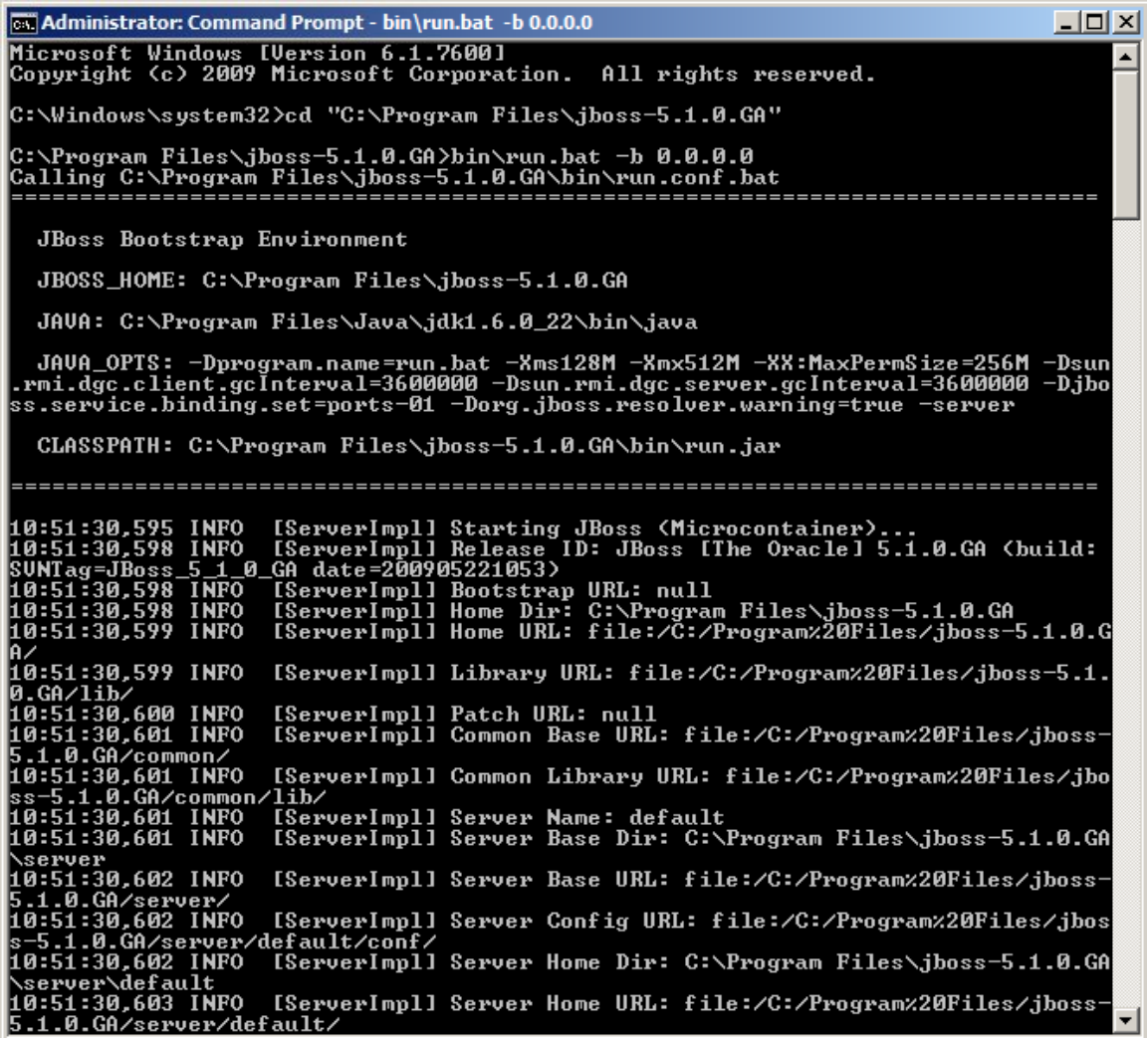
Finally, save the file and exit WordPad.

RUN JBOSS

Open a command prompt *as an Administrator* and navigate to the JBoss directory. Run the following command in the JBoss directory to start the JBoss Application Server:

```
bin\run.bat -b 0.0.0.0
```

Once JBoss starts, you'll see output similar to the example below. Starting JBoss and the REST API may take a minute.



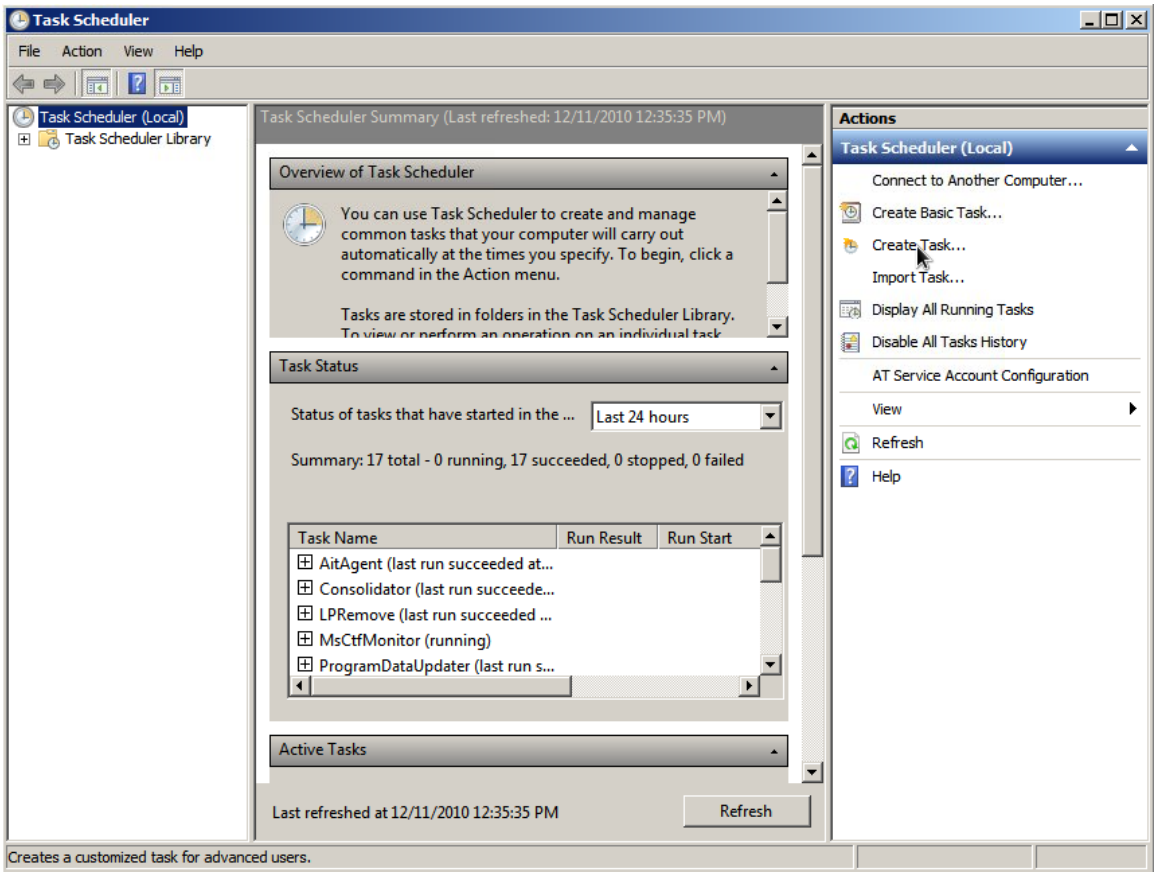
START JBOSS ON BOOT

Once the JBoss Application Server starts correctly on the command prompt, one way to automatically start this service on Windows Server's boot is with a Scheduled Task.

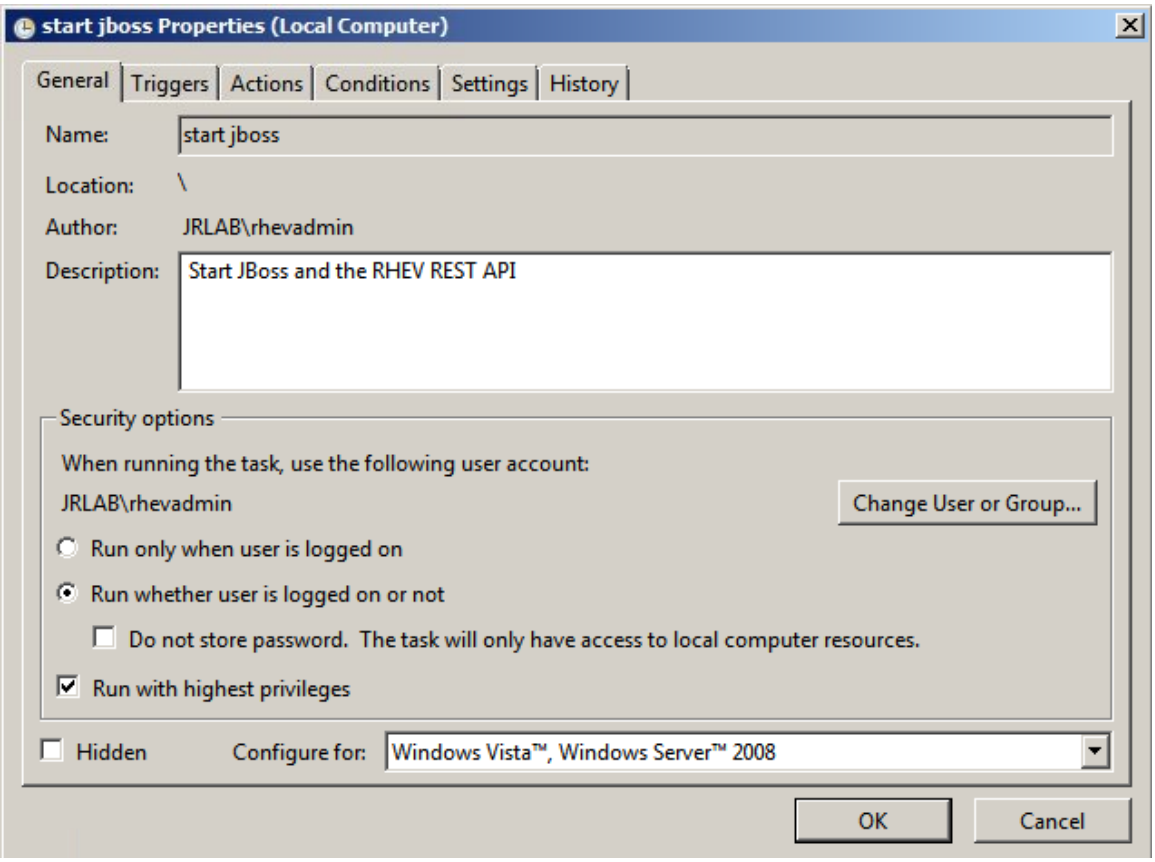
Another means to start JBoss on boot is by using JBossNative, which will configure JBoss to start as a Windows Service. This document lists the steps for creating a Task.

To setup a scheduled task, click on the Start menu and choose “Administrative Tools” > “Task Scheduler.”

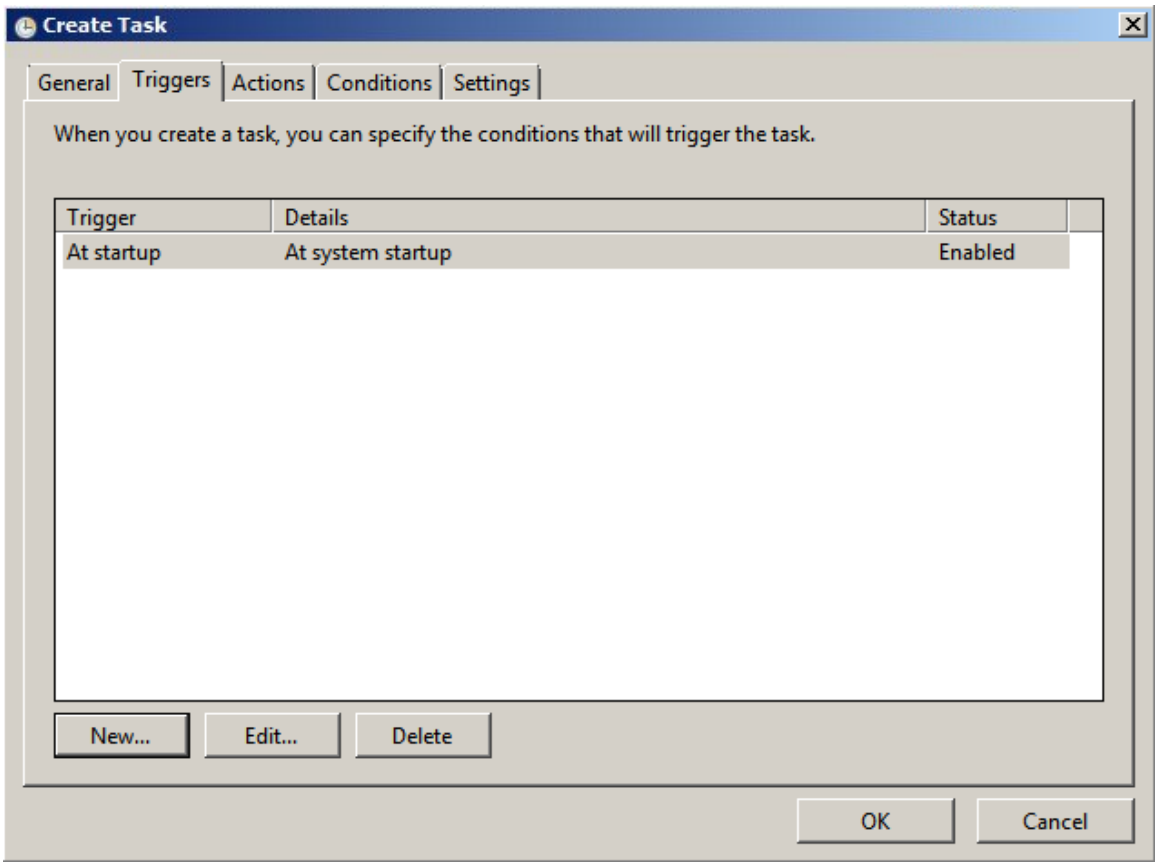
In the Task Scheduler window, click on the “Create Task” link, as shown below:



In the Create Task wizard, name the task (in this example, “start jboss”). Also, choose the “Run whether user is logged on or not” radio button and check the box next to “Run with highest privileges,” as shown in the example below.



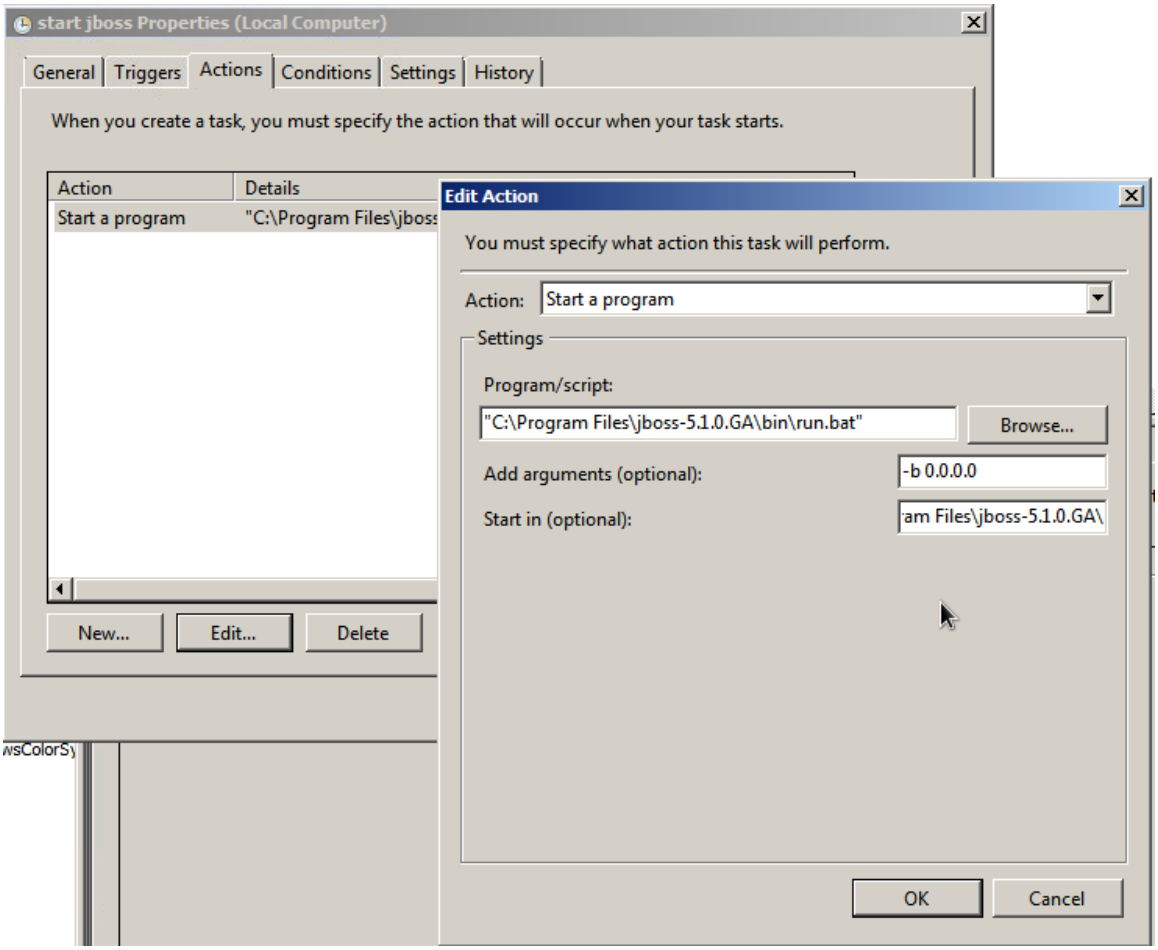
Next, click on the “Triggers” tab and create a trigger to start the task “At system startup,” as depicted below:



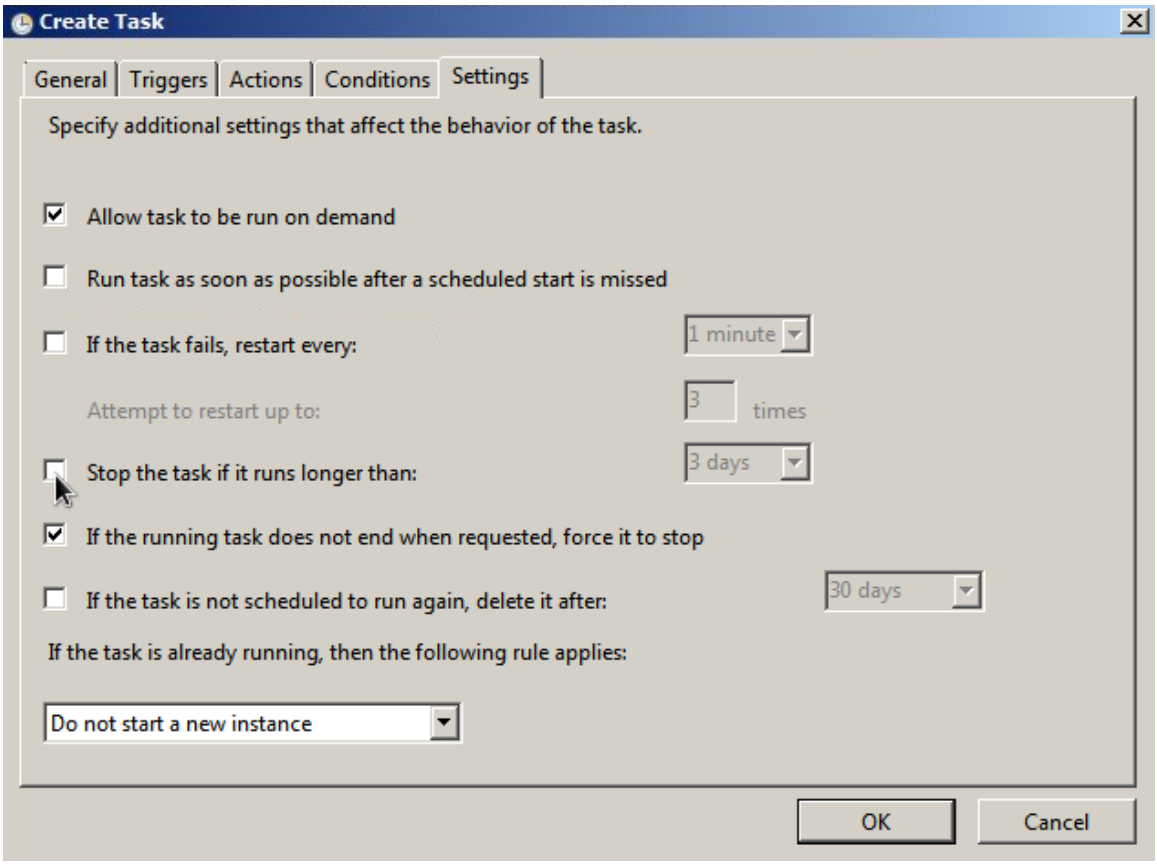
Now, click on the “Actions” tab and create a new action. The action should contain the following values (if you chose to not install JBoss in Program Files, then adjust these accordingly):

Action:	Start a Program
Program/script:	“C:\Program Files\jboss-5.1.0.GA\bin\run.bat”
Add arguments:	-b 0.0.0.0
Start in:	C:\Program Files\jboss-5.1.0.GA\

Note that the “Program” value includes quotes and the “Start in” value does not. *This is required*. If the “Start in” value contains quotes, Windows will produce an error and will fail to start the task.



Lastly, click on the “Settings” tab and *deselect* the box next to “Stop the task if it runs longer...”



Click OK and the task will be created. Verify that the Task works correctly by rebooting the Windows Server and observe that JBoss and the REST API start automatically on boot.

VALIDATE INSTALL VIA WEB BROWSER

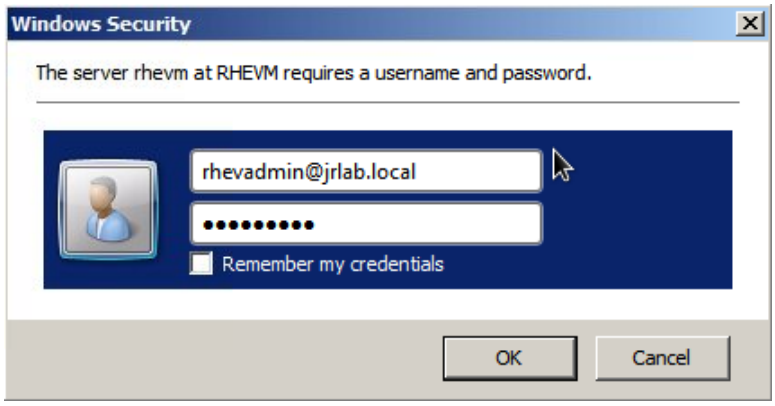
REST API functionality can be easily verified using any web browser. Start Internet Explorer or Firefox and navigate to:

`https://<rhevm-IP-address-or-FQDN>:8543/rhevm-api-powershell/`

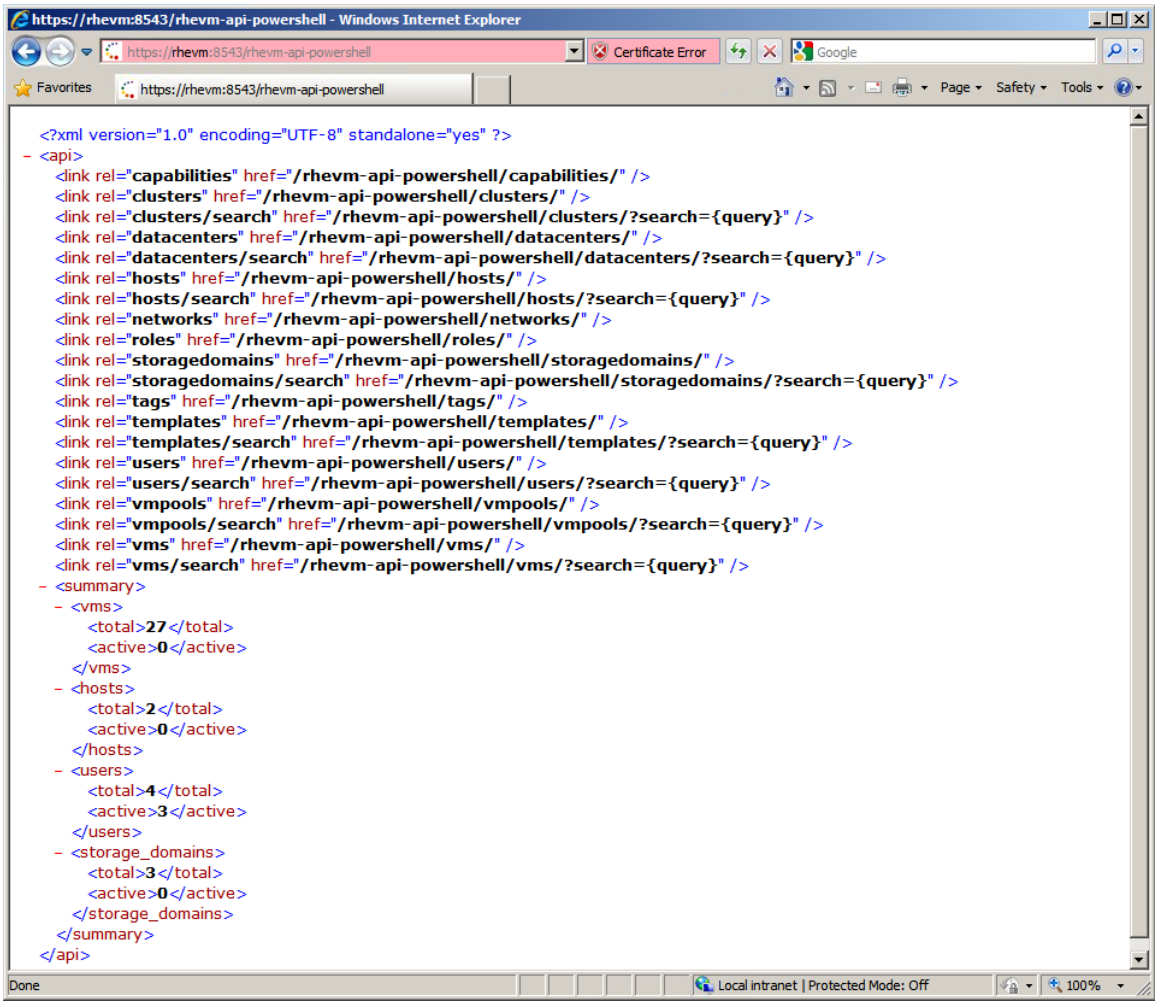
Note that connections to the API will be on port 8543. If the Windows Firewall is enabled, ensure that this port is open.

Since the SSL certificate is self-signed, accept the IE or Firefox security warning. To prevent this warning from occurring again, import the certificate.

Next, you will be prompted to provide RHEV Administrator credentials. Note that the username syntax is required to be **`<username>@<domain-name>`**. In the example below, the username is “rhevadmin” and the domain is “jrlab.local.”



Once RHEV Administrator credentials are provided, the API will output XML similar to the example below.



Also browse to the “/rhevm-api-powershell/vms” and other URLs to see more information on your RHEV environment. Please consult the API documentation for additional options and details.

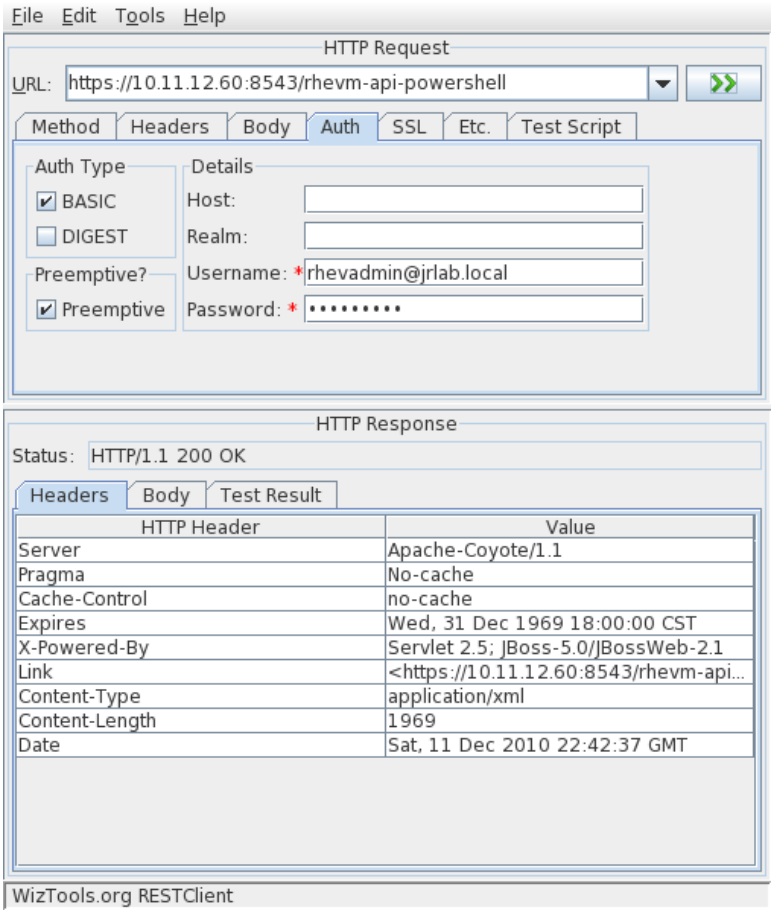
VALIDATE INSTALL VIA REST CLIENT

Another easy way to test the REST API is with the java rest-client available on Google Code:

http://code.google.com/p/rest-client/

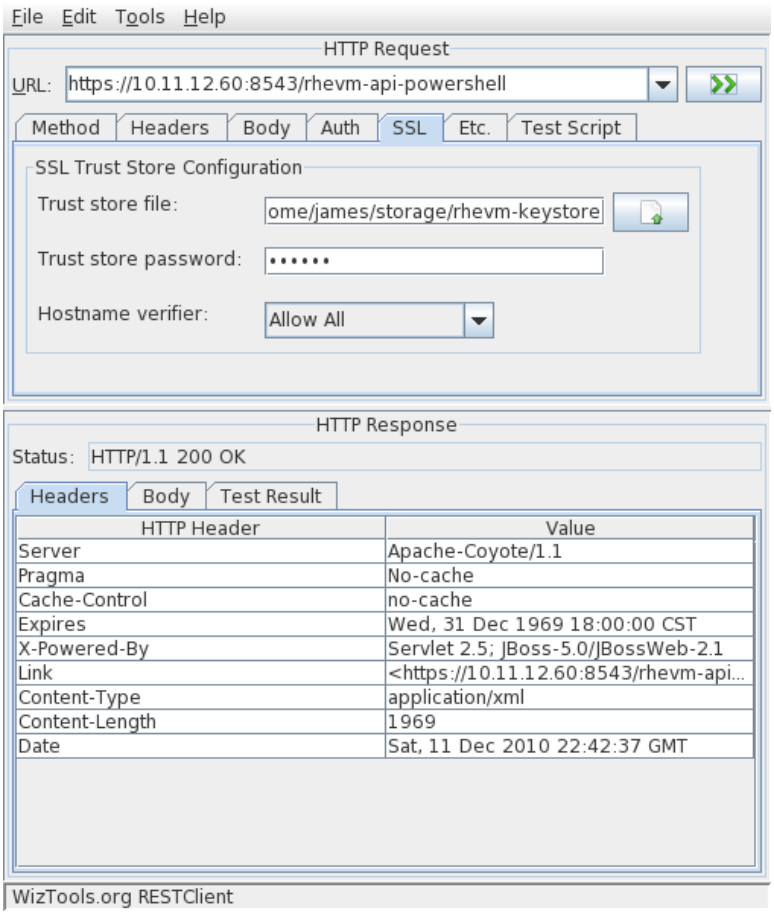
Download the jar file for the rest-client from the project homepage. On Windows, simply double click the jar file to run the client. On Linux, issue the command “java -jar <jar-file-name>”.

To configure the rest-client, provide a URL to the client, just as when testing the API via a web browser. Under the “Auth” tab, choose “BASIC” authentication and furnish RHEV Administrator credentials, as shown below:

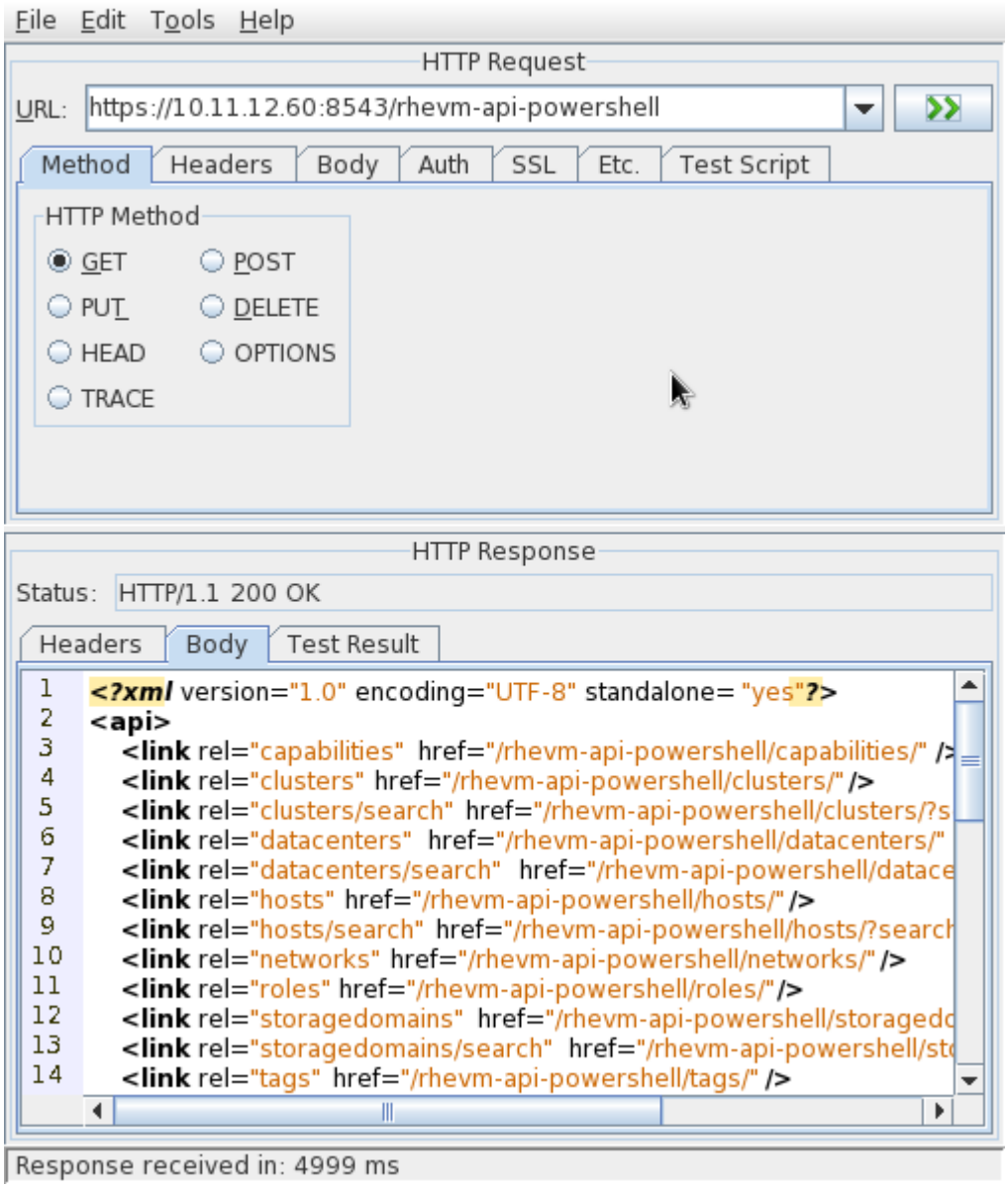


Next, click on the “SSL” tab and provide the client with a copy of the rhevm-keystore file that was created during the earlier setup process. Also provide the trust store password; in the example in this whitepaper, the trust store password was “redhat”.

Last, change the “hostname verifier” to “allow all,” as shown below:



To run the GET query, click the green button to the right of the URL field. After processing the query, click on the “Body” tab under “HTTP Response” to view the XML response:



The rest-client may also be used to issue POSTs and PUTs into the API. Please consult the API documentation or the rhev-api mailing list for more detail.