

User Interface - Bug #2928

non-localhost testing and fixes

12/12/2015 07:23 AM - Greg Shah

Status:	Closed	Start date:	
Priority:	Normal	Due date:	
Assignee:	Sergey Ivanovskiy	% Done:	100%
Category:		Estimated time:	0.00 hour
Target version:	GUI Support for a Complex ADM2 App	case_num:	
billable:	No	version:	
vendor_id:	GCD		
Description			

History

#1 - 12/12/2015 07:24 AM - Greg Shah

Please test the web client from a browser on a separate physical system than where the Java client process launches. Report any found issues here. Resolve those issues. Anything risky can be posted here as a diff. If the changes are not risky, they can be directly checked into 1811t.

#2 - 12/12/2015 07:26 AM - Greg Shah

For testing, please run through the standalone GUI testcases list (the same ones we use for regression testing GUI). All testing should be done on branch 1811t.

#3 - 12/14/2015 11:32 AM - Sergey Ivanovskiy

Let the simple server be located on 192.168.1.35 and accessed by <https://192.168.1.35:7443/gui>. Trying to login the simple server from the different computer throws the following exception on the web java side:

```
Dec 14, 2015 7:14:59 PM WebPageHandler
INFO: {main} target=/ page=/com/goldencode/p2j/ui/client/driver/web/index.html
Dec 14, 2015 7:14:59 PM WebPageHandler
INFO: {main} target=/index.html page=/com/goldencode/p2j/ui/client/driver/web/index.html
Dec 14, 2015 7:14:59 PM org.eclipse.jetty.server.Server doStart
INFO: jetty-9.1.2.v20140210
Dec 14, 2015 7:14:59 PM org.eclipse.jetty.server.handler.ContextHandler doStart
INFO: Started o.e.j.s.h.ContextHandler@1018bde2{/,null,AVAILABLE}
Dec 14, 2015 7:14:59 PM org.eclipse.jetty.server.handler.ContextHandler doStart
INFO: Started o.e.j.s.h.ContextHandler@65b3f4a4{/,null,AVAILABLE}
Dec 14, 2015 7:14:59 PM org.eclipse.jetty.server.handler.ContextHandler doStart
INFO: Started o.e.j.s.h.ContextHandler@f2ff811{/client, jar:file:/home/sbi/projects/1811t/build/lib/p2j.jar!/co
m/goldencode/p2j/ui/client/gui/driver/web/res,AVAILABLE}
Dec 14, 2015 7:14:59 PM org.eclipse.jetty.server.handler.ContextHandler doStart
INFO: Started o.e.j.s.h.ContextHandler@568ff82{/common, jar:file:/home/sbi/projects/1811t/build/lib/p2j.jar!/co
m/goldencode/p2j/ui/client/driver/web/res,AVAILABLE}
Dec 14, 2015 7:14:59 PM org.eclipse.jetty.server.AbstractConnector doStart
INFO: Started ServerConnector@34f7cfd9{SSL-HTTP/1.1}{localhost:7449}
Dec 14, 2015 7:14:59 PM GenericWebServer.startup
INFO: {main} Server URL: https://localhost:7449/
java.lang.NullPointerException
    at com.goldencode.p2j.ui.client.gui.driver.web.WebFontMetricsHelper.charWidth(WebFontMetricsHelper.java:67
)
    at com.goldencode.p2j.ui.client.gui.driver.AbstractGuiDriver.scaleFont(AbstractGuiDriver.java:1384)
    at com.goldencode.p2j.ui.client.FontManager$WorkArea.createFont(FontManager.java:935)
    at com.goldencode.p2j.ui.client.FontManager$WorkArea.initialize(FontManager.java:895)
    at com.goldencode.p2j.ui.client.FontManager.init(FontManager.java:639)
    at com.goldencode.p2j.ui.chui.ThinClient.initializePost(ThinClient.java:2808)
    at com.goldencode.p2j.main.ClientCore.start(ClientCore.java:218)
    at com.goldencode.p2j.main.ClientCore.start(ClientCore.java:102)
    at com.goldencode.p2j.main.ClientDriver.start(ClientDriver.java:201)
    at com.goldencode.p2j.main.CommonDriver.process(CommonDriver.java:398)
```

```
at com.goldencode.p2j.main.ClientDriver.process(ClientDriver.java:95)
at com.goldencode.p2j.main.ClientDriver.main(ClientDriver.java:267)
```

Thus the redirect url is not correct. The JS client gets <https://localhost:7449/?token=65530ae10df22750310955211b944410b0b4c129> instead of <https://192.168.1.35:7449/?token=65530ae10df22750310955211b944410b0b4c129>. It can be resolved by setting the direct IP address of localhost for the webClient container

```
<node class="string" name="host">
  <node-attribute name="value" value="192.168.1.35"/>
</node>
```

but I am not sure that this solution is correct.

#4 - 12/14/2015 12:49 PM - Sergey Ivanovskiy

1811t has the known missed space character issue in text fields for the swing and web clients. Thus it hasn't been resolved yet.

#5 - 12/14/2015 01:15 PM - Sergey Ivanovskiy

- File *calc.p.png* added

For the web client the plus sign becomes damaged if do clicking on its neighbor row buttons. It can be reproduced for the current trunc version.

#6 - 12/14/2015 01:46 PM - Sergey Ivanovskiy

- File *calc-static-chars.p.png* added

For the swing and web clients the plus sign button looks like it doesn't fit the required bounds. It can be reproduced for the current trunc version.

#7 - 12/14/2015 02:25 PM - Sergey Ivanovskiy

- File *image.png* added

./image/image0.p displays a faded *app-icon.ico*. The same issue happens with local launches. It can be reproduced for the current trunc version.

#8 - 12/14/2015 02:43 PM - Sergey Ivanovskiy

/button/gui_btn_test5.p has a known issue with a damaged image if do clicking on the "enable on/off" button two times and then press the "quit" button. Also it is present for the current trunc version.

#9 - 12/14/2015 02:58 PM - Sergey Ivanovskiy

./window_sizing/test_runner.p, *./window_sizing/default_empty_window.p* and *./window_sizing/create_empty_window.p* are failed with out of pop errors and critical *NS_ERROR*. Also it is present for the current trunc version.

#10 - 12/14/2015 03:28 PM - Sergey Ivanovskiy

- File *browse.png* added

./browse/gui/browse-gui-stat1.p has faded columns headers in the case if the js client is on the different computer, but I am not sure that this issue is related to the remote launch, it can be related to the specific configuration. Thus it seems that there are no new bugs related to the remote launches with Firefox 38.0.5 on Fedore 20.

#11 - 12/15/2015 03:06 AM - Sergey Ivanovskiy

The bug from [#2928-5](#) (./demo/calc.p) can be reproduced for the current trunc version.

#12 - 12/15/2015 07:43 AM - Greg Shah

This has been reported by a customer:

----- Forwarded Message -----

Subject: Re: GUI distribution
Date: Tue, 15 Dec 2015 11:37:29 +0000
From: Paul E
To: Constantin Asofiei
CC: Greg Shah ...

Hi again,

As I said in my previous email. It works for me.

This is when I'm running on Linux, using Firefox and I'm either running the browser locally to the P2J server or tunnelling to the P2J server (with webClient/host set to "localhost").

We'd like to demo this ... tomorrow.

This demo will be on a Windows PC (or Firefox will be).

I just tried modifying webClient/host from "localhost" to the hostname of the Linux VM that the P2J server is running on and connecting to that and I see an exception I haven't seen before (see bottom of this email).

Obviously in testing it in this fashion we're introducing two things:

- 1) setting webClient/host to something other than localhost
- 2) using Firefox on Windows

I'm suggesting a workaround to 1) by using a windows SSH client (bitwise tunnelier) and setting up a local port forwarding rule in it and maybe it'll work then (once I revert the hostname to "localhost").

As I said, logs attached. The interesting bit is probably this:

```
[12/15/2015 11:10:12 GMT] (com.goldencode.p2j.ui.FontTable:SEVERE) Could not load the legacy text metrics from file text-metrics.xml
java.lang.NullPointerException
at com.goldencode.p2j.ui.client.gui.driver.web.WebFontMetricsHelper.charWidth(WebFontMetricsHelper.java:67)
at com.goldencode.p2j.ui.client.gui.driver.AbstractGuiDriver.scaleFont(AbstractGuiDriver.java:1384)
at com.goldencode.p2j.ui.client.FontManager$WorkArea.createFont(FontManager.java:935)
at com.goldencode.p2j.ui.client.FontManager$WorkArea.initialize(FontManager.java:895)
at com.goldencode.p2j.ui.client.FontManager.init(FontManager.java:639)
at com.goldencode.p2j.ui.chui.ThinClient.initializePost(ThinClient.java:2810)
at com.goldencode.p2j.main.ClientCore.start(ClientCore.java:218)
at com.goldencode.p2j.main.ClientCore.start(ClientCore.java:102)
at com.goldencode.p2j.main.ClientDriver.start(ClientDriver.java:201)
at com.goldencode.p2j.main.CommonDriver.process(CommonDriver.java:398)
at com.goldencode.p2j.main.ClientDriver.process(ClientDriver.java:95)
at com.goldencode.p2j.main.ClientDriver.main(ClientDriver.java:267)
```

Cheers,
Paul.

#13 - 12/15/2015 07:44 AM - Greg Shah

Sergey/Constantin: please work with Paul to find a solution to his issue. This has high priority since he is trying to do a demo tomorrow.

Sergey: please report which of the problems noted above (if any) are:

1. Caused by the non-localhost configuration.
2. Not present in the P2J trunk.

#14 - 12/15/2015 08:28 AM - Paul E

Ah good, I see you get the same behaviour that I do - that's encouraging.

In that case we should be able to get this working with the port forwarding approach I've suggested (adding forwarding rules for 7443 and 7449).

I'm relying on someone else to do this, following my instructions, since I don't have access to a Windows machine at the moment. If this doesn't work then I'll follow-up with another comment on this issue.

#15 - 12/15/2015 08:58 AM - Sergey Ivanovskiy

Hi Paul,

Could you please report here the redirect url the JS client gets if you set the hostname of the Linux VM that the P2J server is running on?

In my test all nodes are connected directly like in the star topology with the one router node. Thus if I set webClient/host to its IP address (192.168.1.35), then the JS client (Firefox browser) will be redirected to <https://192.168.1.35:7449/>. And if we provide the domain host name, then the host name must be resolved somehow by the browser to get the target IP address. But what is a redirect url in your case?

#16 - 12/15/2015 09:59 AM - Constantin Asofiei

Paul Eames wrote:

Ah good, I see you get the same behaviour that I do - that's encouraging.

This NPE is generated when a call from the spawned client to the browser (via Web Sockets) did not return a result in 10 seconds (WebClientProtocol.waitForResult timeouts). Can you check the latency between the machine from where the Web client is started and the VM where the P2J server/spawned client is ran? In any case, we need to make this timeout configurable and also raise a more explanatory exception.

In that case we should be able to get this working with the port forwarding approach I've suggested (adding forwarding rules for 7443 and 7449).

This is needed only if the VM and the client machine are on different networks. Also, the VM where the P2J server and spawned P2J client are ran must accept traffic on the 7443 and 7449 ports. I've tested this on a my network and:

1. I had to add rules to iptables to allow incoming traffic to 7443 and 7449 ports
2. I had to change the webClient/host to the IP of the machine where the P2J server was running
3. from the Windows machine, the web client connected and started OK, using Firefox and the server's IP

#17 - 12/15/2015 10:36 AM - Paul E

Sergey,

In my case the server name is "gui-conv".

I see a redirect address of:

<https://gui-conv:7449/?token=...>

Constantin,

Thanks - I'll try using the IP address then.

#18 - 12/15/2015 11:09 AM - Sergey Ivanovskiy

In that case this issue is related to how host names can be resolved in your network and to accepted routes. I haven't tried hosts configuration file yet but it should work to resolve host names to IPs.

#19 - 12/15/2015 11:11 AM - Paul E

It's working now.

Thank you for your help.

I changed to use IP addresses. TBH I'm not sure if that was the important change.

I was about to gather all of the logs to send to you and noticed that the logs in run/client hadn't been written to recently, I changed permissions on the directory so all users can write to it. I suspect it's more likely that that is the change that made it work?

#20 - 12/15/2015 11:21 AM - Constantin Asofiei

Paul Eames wrote:

I changed to use IP addresses. TBH I'm not sure if that was the important change.

I was about to gather all of the logs to send to you and noticed that the logs in run/client hadn't been written to recently, I changed permissions on the directory so all users can write to it. I suspect it's more likely that that is the change that made it work?

What matters is the user specified in the login window has access to the directory specified in webClient/workingDir, as the spawned client will be executed using the permissions for the user specified at login. Also, the spawner will not start the client if it can't access this folder and there will be a message displayed in the login window.

#21 - 12/15/2015 11:31 AM - Paul E

Constantin,

When you say "has access to", what do you mean?

Permissions on the working directory were 0775 and owned by me.

I can't remember but I probably tested this as me this morning, but didn't want to share my system password so used a different user when testing from Windows. This other user would have had read and execute permissions on the working directory. Perhaps write permissions are also required (so that the client log can be created and written to?).

#22 - 12/15/2015 11:40 AM - Constantin Asofiei

Paul Eames wrote:

Constantin,

When you say "has access to", what do you mean?

Full read/write access.

Permissions on the working directory were 0775 and owned by me.

I can't remember but I probably tested this as me this morning, but didn't want to share my system password so used a different user when testing from Windows. This other user would have had read and execute permissions on the working directory. Perhaps write permissions are also required (so that the client log can be created and written to?).

Yes, the user needs read/write access to the working directory.

#23 - 12/16/2015 04:41 AM - Sergey Ivanovskiy

Greg Shah wrote:

Sergey: please report which of the problems noted above (if any) are:

1. Caused by the non-localhost configuration.
2. Not present in the P2J trunk.

All reported bugs are present in the P2j trunc. And one bug [#2928-10](#) is related to the screen resolution and fonts for the tested notebook.

#24 - 12/16/2015 08:24 AM - Greg Shah

Sergey:

1. Are any of these bugs caused by non-localhost browser usage?
2. Please create new sub-tasks of [#2677](#) for any of these bugs which were not already known.

#25 - 12/17/2015 10:10 AM - Sergey Ivanovskiy

1. Are any of these bugs caused by non-localhost browser usage?

I couldn't find bugs caused by non-localhost browser usage. All found bugs can be reproduced for P2j trunc:

[#2928-4](#) old

[#2928-5](#) new

[#2928-6](#) new

[#2928-7](#) new

[#2928-8](#) current

[#2928-9](#) old

2. Please create new sub-tasks of [#2677](#) for any of these bugs which were not already known.

Planning to add new issues for new bugs.

#26 - 12/17/2015 10:18 AM - Greg Shah

Sergey Ivanovskiy wrote:

Let the simple server be located on 192.168.1.35 and accessed by <https://192.168.1.35:7443/gui>. Trying to login the simple server from the different computer throws the following exception on the web java side:

[...]

Thus the redirect url is not correct. The JS client gets <https://localhost:7449/?token=65530ae10df22750310955211b944410b0b4c129> instead of <https://192.168.1.35:7449/?token=65530ae10df22750310955211b944410b0b4c129> It can be resolved by setting the direct IP address of localhost for the webClient container

[...]

but I am not sure that this solution is correct.

It is one option.

I think we need to consider 2 things:

1. Have you tested with a DNS name (other than localhost) to confirm that we don't have any unexpected issues there? This would be the more common way to solve the problem. And in a scenario where all the clients are spawned on the same system, this seems to be a perfectly good solution.
2. We should consider providing support (by default, if host is not specified) where the client reports the FQDN of the URL. I'm not sure why this isn't already present. This would cleanly handle all cases (all clients spawned on the same system, clients spawned on multiple systems as well as both remote and local spawning).

#27 - 12/17/2015 10:21 AM - Greg Shah

And one bug [#2928-10](#) is related to the screen resolution and fonts for the tested notebook.

Is this a bug in P2J? Or do we have a core requirement for a minimum resolution and font support?

#28 - 12/17/2015 12:29 PM - Sergey Ivanovskiy

Greg Shah wrote:

I think we need to consider 2 things:

1. Have you tested with a DNS name (other than localhost) to confirm that we don't have any unexpected issues there? This would be the more common way to solve the problem. And in a scenario where all the clients are spawned on the same system, this seems to be a perfectly good solution.

In my test environment that consists of two nodes and one router the simple name doesn't work for remote launches and works for local launches in the case my test environment is properly set.

Suppose that the p2j server with its web server is running on the machine A (192.168.1.35) and the clients machine is B (192.168.1.34). The /etc/hosts file of the machine B is listed below

```
127.0.0.1 localhost
192.168.1.35 A
```

The /etc/hosts file of the machine A is the same listed below

```
127.0.0.1 localhost
192.168.1.35 A
```

The client requests this url <https://A:7443/gui> and the web server on the machine A responds with the login page. Then the client posts the login form to the web server and the client is redirected to this page <https://A:7449> but Firefox couldn't resolve this url and the spawned java web client is failed after timeout. I don't understand that the first request GET <https://A:7443/gui> is resolved but the second GET <https://A:7449> is not. But the first request is GET <https://192.168.1.35:7443/gui> but the second is GET <https://A:7449/?.....> Thus we can see that the Firefox doesn't want to resolve the redirect url! I guess that the redirect host should be resolved by the router but my router doesn't run the domain names service.

2. We should consider providing support (by default, if host is not specified) where the client reports the FQDN of the URL. I'm not sure why this

isn't already present. This would clearly handle all cases (all clients spawned on the same system, clients spawned on multiple systems as well as both remote and local spawning).

GenericWebServer.getHost() returns the first ip address of the host's active interface from 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 if the host is not provided by the configuration file.

#29 - 12/18/2015 02:59 AM - Sergey Ivanovskiy

Greg, please clarify your vision of this issue. My test environment only proves that Firefox doesn't cache a host name to its IP address, because the first two requests: GET and POST have a resolved host name address in the requests body but the third request GET (redirect url) has not.

#30 - 12/18/2015 05:22 AM - Greg Shah

As of now, spawning web clients using a hostname that is not localhost does not work with Firefox. That is unacceptable and must be resolved. Customers would have a reasonable expectation that such a configuration would work. Some customer use cases like load balancing may even require such a configuration.

Please determine where the problem exists (our redirect approach, Firefox. ..). Then we can discuss solutions.

#31 - 12/18/2015 12:07 PM - Sergey Ivanovskiy

I have installed the local DNS service on the server machine A(192.168.1.35) - dnsmasq the lightweight DNS server which is useful for local customer's network.

```
sudo /etc/init.d/dnsmasq restart
```

/etc/hosts for machine A (192.168.1.35) is listed below (this file is exported by the installed DNS server)

```
localhost 127.0.0.1
A 192.168.1.35
```

Then test it on the machine A by

```
nslookup A
```

```
Server:      127.0.0.1
Address:    127.0.0.1#53
```

```
Name:      A
Address: 192.168.1.35
```

Then permit this DNS service for clients hosts

```
sudo iptables -t filter -I INPUT 3 -i eth0 -p udp -m udp --dport 53 -j ACCEPT
```

This command has a session life time and insert the udp 53 accept rule after the third rule in the FILTER table in the server host A (192.168.1.35).

Then setup DHCP service for the router (192.168.1.1) in order to export this DNS server to clients (it depends on the router software).

Restart network interface on the client machine B (192.168.1.34) and test the local DNS service

```
nslookup A
```

Server: 192.168.1.35
Address: 192.168.1.35#53

Name: A
Address: 192.168.1.35

The local DNS service is good.

Start p2j server on the machine A (192.168.1.35) with the web client host name to be A.

Open Firefox on the client machine B (192.168.1.34) and print this url : <https://A:7443/gui>

The P2J server responds with the login page, fill correct login and password and submit to the server.

The P2J server responds with <https://A:7449/?>.... and loads our application successfully.

This experiment proves that the local DNS server is required!

#32 - 12/21/2015 03:20 PM - Greg Shah

This experiment proves that the local DNS server is required!

Can you please clarify this statement? I assume that you mean that the customer must use a DNS that provides lookup support for all the names which are being referenced and that all of the systems being used (A and B in this example) must be configured to resolve names through that DNS.

When you say "local DNS server", I am assuming that you do NOT mean that the DNS server must run on the same system as the P2J server.

In addition, you are implying that the issue here is that the use of the hosts file is inadequate for name resolution, even when all systems (A and B here) have the needed names mapped in their local version of hosts.

Am I understanding correctly?

If so, why do you estimate the hosts file is failing? This is pretty unexpected.

#33 - 12/21/2015 03:33 PM - Greg Shah

When you investigate the details of the item in note 10/note 27, please post them here. If it is a real issue, I want to make sure a new sub-task of [#2677](#) is created for it.

#34 - 12/22/2015 12:35 AM - Sergey Ivanovskiy

Greg Shah wrote:

This experiment proves that the local DNS server is required!

Can you please clarify this statement? I assume that you mean that the customer must use a DNS that provides lookup support for all the names which are being referenced and that all of the systems being used (A and B in this example) must be configured to resolve names through that DNS.

When you say "local DNS server", I am assuming that you do NOT mean that the DNS server must run on the same system as the P2J server.

In addition, you are implying that the issue here is that the use of the hosts file is inadequate for name resolution, even when all systems (A and B here) have the needed names mapped in their local version of hosts.

Am I understanding correctly?

Yes, correctly. I mean the local DNS server is a non ISP DNS server or a private network DNS server.

If so, why do you estimate the hosts file is failing? This is pretty unexpected.

Agree. In my first test case without DNS it supposed that the browser could cache the resolved name and use it later without lookups.

I think my test's environment with the installed DNS service becomes close to the real customer's environment and it follows that the hosts names can be used without problems.

#35 - 12/22/2015 12:40 AM - Sergey Ivanovskiy

Greg Shah wrote:

When you investigate the details of the item in note 10/note 27, please post them here. If it is a real issue, I want to make sure a new sub-task of [#2677](#) is created for it.

I created this Bug [#2944](#): The browse header and body fonts are not usable for display resolution 1366x768, but didn't succeeded with understanding root causes.

#36 - 12/22/2015 12:52 AM - Constantin Asofiei

Sergey Ivanovskiy wrote:

Greg Shah wrote:

When you investigate the details of the item in note 10/note 27, please post them here. If it is a real issue, I want to make sure a new sub-task of [#2677](#) is created for it.

I created this Bug [#2944](#): The browse header and body fonts are not usable for display resolution 1366x768, but didn't succeeded with understanding root causes.

Sergey, related to [#2944](#) and in general: in Firefox, we haven't found a way to disable anti-aliasing "on the page", via CSS or something else - only on the full browser can be disabled.

[#2944](#) might have something to do with anti-aliasing (beside some positioning issues, I think)- please check if you can disable anti-aliasing in other browsers.

#37 - 12/22/2015 05:09 AM - Sergey Ivanovskiy

Constantin Asofiei wrote:

Sergey Ivanovskiy wrote:

Greg Shah wrote:

When you investigate the details of the item in note 10/note 27, please post them here. If it is a real issue, I want to make sure a new sub-task of [#2677](#) is created for it.

I created this Bug [#2944](#): The browse header and body fonts are not usable for display resolution 1366x768, but didn't succeeded with understanding root causes.

Sergey, related to [#2944](#) and in general: in Firefox, we haven't found a way to disable anti-aliasing "on the page", via CSS or something else - only on the full browser can be disabled.

[#2944](#) might have something to do with anti-aliasing (beside some positioning issues, I think)- please check if you can disable anti-aliasing in other browsers.

I have checked on Window 7 Enterprise Service Pack 1 virtual image that if we turn off Clear Type option, then Firefox displays the header and body fonts correctly. I have problems to check IE11 due to Invalid Certificate and strange redirect url behavior. Let me explain. The session Network

activities log displays that the redirect url has been cut to remove the protocol, host name, port and to leave `/?token=...` only in the GET redirect request, but some times I have forced to display the page `hostname:7449/index.html` successfully, but now I haven't understand the issue. At the current moment only 1811t can work with IE11. Constantin, do you try IE11 remote launch? The web server sends the 302 HTTP code and the correct redirect url in the response to the authorized post request. It doesn't provide REFERER header, but it is not required. If I copy the redirect url from IE Network activities and force it to load by pasting into the IE address field, the application is loaded successfully. To reproduce this experiment it needs to increase web server timeout manually `WebClientProtocol`

```
public Object waitForResult(int msgId)
{ ... }
```

#38 - 12/22/2015 01:27 PM - Sergey Ivanovskiy

The only difference has been found that IE11 tries to use POST method forcing redirect to new resource by the 302 HTTP server response with LOCATION <https://hostname:7449/?token=...>, but Firefox and Google Chrome use GET method. Now I have stopped experiments with IE11 for a while.

#39 - 12/23/2015 06:01 AM - Sergey Ivanovskiy

The only difference has been found that IE11 tries to use POST method forcing redirect to new resource by the 302 HTTP server response with LOCATION <https://hostname:7449/?token=...>, but Firefox and Google Chrome use GET method. Now I have stopped experiments with IE11 for a while.

I have tried to change the response HTTP code to 303. It forces IE11 to use GET method but the IE redirect behavior is strange even the address field is not changed to the target redirect url given by Location HTTP response header's field

```
+         if (response instanceof Response)
+         {
+             ((Response) response).sendRedirect(HttpServletResponse.SC_SEE_OTHER, remoteUri);
+         }
-         response.sendRedirect(remoteUri);
```

Thus I need a help to check the certificate IE11 issue and IE11 remote launch for the current 1811t branch using different environments.

#40 - 12/30/2015 10:08 PM - Greg Shah

Thus I need a help to check the certificate IE11 issue and IE11 remote launch for the current 1811t branch using different environments.

Can you be more specific about what you need help with? It is not clear from the above details.

In addition, is the certificate issue a real problem? Or is it just the common issue of all browsers when dealing with self-signed certificates? Please explain how it is different for IE than for Firefox.

#41 - 01/02/2016 10:02 AM - Sergey Ivanovskiy

Greg Shah wrote:

Thus I need a help to check the certificate IE11 issue and IE11 remote launch for the current 1811t branch using different environments.

Can you be more specific about what you need help with? It is not clear from the above details.

In addition, is the certificate issue a real problem? Or is it just the common issue of all browsers when dealing with self-signed certificates? Please explain how it is different for IE than for Firefox.

Firefox only warns "This site makes use of a SHA-1 Certificate; it's recommended you use certificates with signature algorithms that use hash functions stronger than SHA-1.", probably IE11 doesn't permit certificates with SHA-1 hash function. And I need to do some strange manipulations: copy the redirect url and paste it to the browser's URL address field in order to force IE to load the application page.

#42 - 01/05/2016 03:14 PM - Greg Shah

Firefox only warns "This site makes use of a SHA-1 Certificate; it's recommended you use certificates with signature algorithms that use hash functions stronger than SHA-1.",

Did this start happening on January 1st? On January 1, 2016 most browsers were planning to start warning about SHA-1 certs.

probably IE11 doesn't permit certificates with SHA-1 hash function.

Yes, could be.

We need to move away from SHA-1 certs to SHA-2. We should also consider a larger default key strength (more than 1024). I think the self-signed certs were created using our own wrappers that in turn use the BouncyCastle library. I suspect that the SHA-1 usage comes from the BCCertFactory constructor:

```
digCalc = new BcDigestCalculatorProvider()  
.get(new AlgorithmIdentifier(OIWObjectIdentifiers.idSHA1));
```

Constantin: Are there any other dependencies on SHA-1? What do you think about the key strength issue? Are there any other changes we should be considering at this point?

#43 - 01/05/2016 04:03 PM - Constantin Asofiei

Greg Shah wrote:

Constantin: Are there any other dependencies on SHA-1? What do you think about the key strength issue? Are there any other changes we should be considering at this point?

This is a little surprising, as the certificate is signed with SHA256WithRSA in BCCertFactory.generateCertificate (and is reported as such in the browser). The SHA-1 you mention is used to create a "thumbprint"/checksum of the certificate, and store it in a separate field (see here for more details: <https://morgansimonsenblog.azurewebsites.net/2013/04/16/understanding-x-509-digital-certificate-thumbprints/>). I'm not sure what this can be changed to: in the list found here <http://www.alvestrand.no/objectid/1.3.14.3.2.html> there is no SHA-2 mention, only relevant entry I can see is 1.3.14.3.2.29 - SHA1 with RSA signature.

Sergey: please post a screenshot to show how the certificate is reported/read by your browser (or the output from a keytool -list -v -keystore <store-name> call). I don't get any SHA-1 warnings or errors in IE11, in the login page or in the application page. Also, when you tested this, were the server and client on the same machine?

#44 - 01/05/2016 04:16 PM - Constantin Asofiei

Greg Shah wrote:

Constantin: What do you think about the key strength issue?

The key strength can be specified manually to something else (i.e. 2048), and this value will also be saved in the directory (and all subsequent calls will default to it). But I think is best to force a minimum 2048 key length (and also show a warning at server startup?).

#45 - 01/06/2016 04:22 AM - Sergey Ivanovskiy

Constantin Asofiei wrote:

Greg Shah wrote:

Constantin: Are there any other dependencies on SHA-1? What do you think about the key strength issue? Are there any other changes we should be considering at this point?

This is a little surprising, as the certificate is signed with SHA256WithRSA in `BCCertFactory.generateCertificate` (and is reported as such in the browser). The SHA-1 you mention is used to create a "thumbprint"/checksum of the certificate, and store it in a separate field (see here for more details: <https://morgansimonsenblog.azurewebsites.net/2013/04/16/understanding-x-509-digital-certificate-thumbprints/>). I'm not sure what this can be changed to: in the list found here <http://www.alvestrand.no/objectid/1.3.14.3.2.html> there is no SHA-2 mention, only relevant entry I can see is 1.3.14.3.2.29 - SHA1 with RSA signature.

Sergey: please post a screenshot to show how the certificate is reported/read by your browser (or the output from a `keytool -list -v -keystore <store-name>` call). I don't get any SHA-1 warnings or errors in IE11, in the login page or in the application page. Also, when you tested this, were the server and client on the same machine?

Certainly, the reported server certificate uses this signature algorithm, SHA1withRSA. Constantin, have you built the server certificate manually? From this document `built_in_cryptography.odt` it follows that

```
java -classpath build/lib/p2j.jar com.goldencode.p2j.security.SSLCertGenUtil <directory-file>
```

there are few cryptography options to set up this wizard. I have found only RSA key length

```
<node class="container" name="certificates">
  <node class="container" name="company">
    <node class="integer" name="rsa keystrength">
      <node-attribute name="value" value="2048"/>
    </node>
    <node class="string" name="rsa public exponent">
      <node-attribute name="value" value="65337"/>
    </node>
  </node>
</node>
```

#46 - 01/06/2016 04:45 AM - Constantin Asofiei

Sergey Ivanovskiy wrote:

Certainly, the reported server certificate uses this signature algorithm, SHA1withRSA. Constantin, have you built the server certificate manually? From this document `built_in_cryptography.odt` it follows that
[...]
there are few cryptography options to set up this wizard. I have found only RSA key length
[...]

All the certificates I'm using for testing are generated via `SSLCertGenUtil`; same for GUI project.

I think the certificate in the `testcases/uast/simple/server/p2j-server-key.store` is not generated via `SSLCertGenUtil` - please re-generate them and try again.

#47 - 01/06/2016 08:13 AM - Greg Shah

But I think is best to force a minimum 2048 key length (and also show a warning at server startup?).

Agreed. Constantin: please go ahead with this change.

#48 - 01/06/2016 11:42 AM - Constantin Asofiei

Greg Shah wrote:

But I think is best to force a minimum 2048 key length (and also show a warning at server startup?).

Agreed. Constantin: please go ahead with this change.

Changes are in 1811t rev 10972. Note that if the source `directory.xml` already has a `/security/certificates/company/rsaKeyStrength` node with a value less than 2048, remove this node before running `SSLCertGenUtil`.

#49 - 01/07/2016 04:21 AM - Sergey Ivanovskiy

- File `directory.xml` added
- File `p2j-root-keys.store` added
- File `p2j-servers-keys.store` added
- File `shared-private-key.store` added
- File `wizard_logs.txt` added

I rebuilt certificates using this command `java -classpath build/lib/p2j.jar com.goldencode.p2j.security.SSLCertGenUtil <directory-file>`.

Yes, SHA256WithRSA is used for all generated certificates. For my configuration `directory.xml` the wizard didn't store in a separate file the private key for the "standard" peer and only `TrustedCertEntry` keys saved in the created java keys store, but for the "shared" peer the private key was saved in a separate file. Finally I decided to use this created "shared" private keys store with the "standard" server using this bootstrap configuration file

```
<?xml version="1.0"?>
<!-- Server side bootstrap configuration
-->
<node type="server">
  <net>
    <router threads="2"/>
  </net>

  <security>
    <server id="standard"/>
    <keystore filename="shared-private-key.store"/>
    <keystore alias="shared"/>
  </security>

  <directory>
    <backend type="xml"/>
    <xml filename="directory.xml"/>
  </directory>

  <access>
    confidential data redacted
  </access>
</node>
```

in order to start the standard server.

I followed the "P2J Cryptography Tool" document and tried to use different options in order to create the standard server private key in a separate file without success. What is incorrect?

LE: GES redacted confidential data.

#50 - 01/07/2016 04:32 AM - Constantin Asofiei

Sergey Ivanovskiy wrote:

I rebuilt certificates using this command `java -classpath build/lib/p2j.jar com.goldencode.p2j.security.SSLCertGenUtil <directory-file>`. Yes, SHA256WithRSA is used for all generated certificates. For my configuration `directory.xml` the wizard didn't store in a separate file the private key for the "standard" peer and only `TrustedCertEntry` keys saved in the created java keys store, but for the "shared" peer the private key was saved in a separate file. Finally I decided to use this created "shared" private keys store with the "standard" server using this bootstrap configuration file
[...] in order to start the standard server.

I followed the "P2J Cryptography Tool" document and tried to use different options in order to create the standard server private key in a separate file without success. What is incorrect?

I think the following are missing:

1. Include the root CA certificate, to use this store as a trust store (yes/no)? no - you should have chosen yes
2. in the `server.xml`, you need to specify the `p2j-servers-keys.store` store with its password (as this is where the certificates were saved); also, `<keystore alias="shared"/>` should have been `<keystore alias="standard"/>`, as this is the alias used by the server. The minimal `server.xml` can look like this, as the certificate private-keys are saved in the directory:

```
<?xml version="1.0"?>
<!-- Server side bootstrap configuration -->
<node type="server">
  <net>
    <router threads="2"/>
  </net>

  <security>
    <server id="standard"/>
  </security>

  <directory>
    <backend type="xml"/>
    <xml filename="directory.xml"/>
  </directory>
</node>
```

You need to regenerate so the external store where the certificates are saved is a trust-store; please use these options:

```
Save servers' certificates in an external key store (yes/no): yes
Include the root CA certificate, to use this store as a trust store (yes/no)? yes
Enter key store file name: srv-certs.store
```

After that, please try the minimal `server.xml` above and let me know if it works.

I'll also re-build the certificates and change the `uast/simple/server` setup, and commit them.

#51 - 01/07/2016 05:01 AM - Sergey Ivanovskiy

Yes, rebuilt certificates with all options selected and proved that the minimal server.xml works properly.

The debugging showed that if we provide

```
<security>
  <server id="standard"/>
  <keystore filename="srv-certs.store"/>
  <keystore alias="standard"/>
</security>
```

then srv-certs.store should contain the private key entry with this "standard" alias, because it is used by TransportSecurity and the "standard" alias should be validated as a private key entry. It forced me to change the keystore file and the alias name.

#52 - 01/07/2016 05:22 AM - Sergey Ivanovskiy

I understand that NativeSecureConnection is used by spawn.c and srv-certs.store is a trusted certificates store.

#53 - 01/07/2016 05:24 AM - Constantin Asofiei

Sergey Ivanovskiy wrote:

Yes, rebuilt certificates with all options selected and proved that the minimal server.xml works properly.

The debugging showed that if we provide

[...]

then srv-certs.store should contain the private key entry with this "standard" alias, because it is used by TransportSecurity and the "standard" alias should be validated as a private key entry. It forced me to change the keystore file and the alias name.

Sorry, I've confused that, server.xml contains specs for private keys, not certificates.

Sergey Ivanovskiy wrote:

I understand that NativeSecureConnection is used by spawn.c and srv-certs.store is a trusted certificates store.

Correct, it needs a trusted cert store, so that it can connect only to trusted/known servers.

#54 - 01/07/2016 06:12 AM - Constantin Asofiei

rev 1447 of the testcases project adds new certificates, with SHA-2 and 2048-bit key length (generated via SSLCertGenUtil).

Also, 1811t rev 10973 has a change in SSLCertGenUtil to allow private-keys for the server's certificate(s) to be saved in external key-stores. Using configuration via server.xml, it allows multiple directories to worry only about the certificates, and not duplicate the private-key(s) in each one (as there are H2/linux/windows versions of the directory in testcases/simple/server).

#55 - 01/25/2016 04:08 PM - Greg Shah

Are there any issues still open in this task?

If not, is there any further testing needed or is this ready to close?

#56 - 01/25/2016 04:19 PM - Sergey Ivanovskiy

It seems that there are no new issues. #note-43 Constantin didn't reproduce the IE connection issue, but this issue could be reproduced with new generated self-signed certificate with SHA-2 and 2048-bit key length in my virtual environment Windows 7 Service Pack 1. #note-39 Thus it can be closed.

#57 - 01/25/2016 05:26 PM - Greg Shah

but this issue could be reproduced with new generated self-signed certificate with SHA-2 and 2048-bit key length in my virtual environment Windows 7 Service Pack 1.

Do you mean that once you generated a new certificate that the problem **could not** be recreated?

#58 - 01/26/2016 01:46 AM - Sergey Ivanovskiy

No, I mean that it is still reproduced in my environment: Window 7 Service Pack 1 with the limited evaluation period.

#59 - 01/26/2016 08:03 AM - Greg Shah

I don't understand. It seems like there is a real problem that still needs to be resolved.

#60 - 01/26/2016 08:14 AM - Sergey Ivanovskiy

I don't understand. It seems like there is a real problem that still needs to be resolved.

I would like if it is possible that this IE scenario with demo_widgets.p has been checked in the different environment. My environment is based on Window 7, 32-bit OS image that was downloaded from Microsoft with the limited evaluation period. The issue is described in these notes: #note-37, #note-38, #note-39, #note-41.

#61 - 01/26/2016 09:32 AM - Greg Shah

Please do check it on a different VM and report the results here. Try the VM with IE11 on Windows 8.1.

#62 - 01/26/2016 02:25 PM - Sergey Ivanovskiy

Planning to check it today.

#63 - 01/26/2016 07:21 PM - Sergey Ivanovskiy

Tested with Windows 8.1, 32-bit. The result is the same.

- 1) Print <https://192.168.1.35:7443/gui> in the IE address field
- 2) Get the "There is a problem with this website's security certificate" page.
- 3) Select this option "Continue to this website (not recommended)"
- 4) The login page is loaded.
- 5) Post user/password
- 6) Get the "There is a problem with this website's security certificate" page.
- 7) Do 3) Select this option "Continue to this website (not recommended)"
- 8) The redirect doesn't happen and the server encounters the following error

```
OpenJDK 64-Bit Server VM warning: ignoring option MaxPermSize=64m; support was removed in 8.0
ERROR: transport error 202: bind failed: Address already in use
ERROR: JDWP Transport dt_socket failed to initialize, TRANSPORT_INIT(510)
JDWP exit error AGENT_ERROR_TRANSPORT_INIT(197): No transports initialized [debugInit.c:750]
[01/27/2016 02:54:29 MSK] (LogicalTerminal:WARNING) No client parameters are set: calling the client-side to d
etermine the driver type is expensive!
[01/27/2016 02:54:29 MSK] (com.goldencode.p2j.net.Protocol:WARNING) stopQueue
```

the address in use due to the web server gets <https://192.168.1.35:7443/gui> request from the JS client.

The problem is that for IE the response with 302 http error must invoke the redirect using the POST method, but the response with 303 http error must force IE to use the GET method. And the second issue is the redirect from one site to another that actually doesn't occur.

I don't understand why the server is tried to create new spawn process and doesn't use the existing process, because it is not possible to create two spawn process with the same opened port 7449. If my understanding that spawn process is created one per a user is correct, then it is not possible to use one server <https://192.168.1.35:7443/gui> by two different users because the port 7449 can't be shared.

#64 - 01/27/2016 12:42 AM - Sergey Ivanovskiy

The reason of IE failures can be a bug while processing the "There is a problem with this website's security certificate" page. It explains why on the step 7, the web server gets the old request. My #note-39 describes the experiment with changing the response code to 303 to force IE using GET redirect. This experiment also proves that this connection issue looks like an IE bug, because at the step 7 the browser url page is not changed and points to the web server address <https://192.168.1.35:7443/gui>.

#65 - 01/27/2016 07:40 AM - Greg Shah

I don't understand why the server is tried to create new spawn process and doesn't use the existing process,

Please check if the original login form is POSTed a second time (after the redirect fails). This would cause the 2nd spawning.

We probably should protect against this by clearing the password field on the original submit.

If my understanding that spawn process is created one per a user is correct, then it is not possible to use one server <https://192.168.1.35:7443/gui> by two different users because the port 7449 can't be shared.

Yes, you are correct. This configuration is useful for testing, but it cannot be used for production systems that require more than 1 simultaneous user. In other words, this won't be used for production.

This experiment also proves that this connection issue looks like an IE bug

I agree it seems like a browser bug, but we definitely must make changes to resolve it in our code. We are required to support IE by the customer. Without the redirect, our system does not work (it is not reasonable to force the end user to copy/paste the URL).

Please try to find a solution.

#66 - 01/27/2016 11:14 AM - Sergey Ivanovskiy

Planning to use JS object XMLHttpRequest in web_client.html to post the login/password and to get the redirect url with the authorization token, and then to set window.location = (redirect url).

#67 - 01/27/2016 08:43 PM - Sergey Ivanovskiy

Sergey Ivanovskiy wrote:

Planning to use JS object XMLHttpRequest in web_client.html to post the login/password and to get the redirect url with the authorization token, and then to set window.location = (redirect url).

Checked that XMLHttpRequest object automatically executes the redirect response with IE, Chrome and Firefox if the server allows the cross domain requests. The spec can be found here <https://dvcs.w3.org/hg/xhr/raw-file/tip/Overview.html#infrastructure-for-the-send%28%29-method>. Now the issue is reduced to how to replace the current document with the target redirected document.

#68 - 01/28/2016 04:38 AM - Sergey Ivanovskiy

Planning to use JS object XMLHttpRequest in web_client.html to post the login/password and to get the redirect url with the authorization token, and then to set window.location = (redirect url).

Checked that XMLHttpRequest object automatically executes the redirect response with IE, Chrome and Firefox if the server allows the cross domain requests. The spec can be found here <https://dvcs.w3.org/hg/xhr/raw-file/tip/Overview.html#infrastructure-for-the-send%28%29-method>. Now the issue is reduced to how to replace the current document with the target redirected document.

The question is not easy, because the current document location is set to "https://192.168.1.35:7443/gui", but the received redirected document is from "https://192.168.1.35:7449".

The IE redirection works properly using XMLHttpRequest, but breaks in the case of using the browser's agent. The log proves that IE gets the correct redirect url from the server, may be the server should specify additional headers. For example, the server must send Access-Control-Allow-Origin: "" in the response header in order the browser's engine permits XMLHttpRequest to execute the redirect.

#69 - 01/28/2016 06:03 AM - Sergey Ivanovskiy

Decided to change the redirect response(302/303) to the simple text response(200) with the encoded redirect path in order to be processed by the simple ajax handler. The issue is successfully solved using XMLHttpRequest ajax handler. Planning to prepare for the review.

#70 - 01/28/2016 07:45 AM - Sergey Ivanovskiy

- File *ajax_changes_1.txt* added

The committed revision 10988 fixes the IE connection issue. Passes tests with IE, Chrome and Firefox.

#71 - 01/28/2016 08:22 AM - Greg Shah

Code Review Task Branch 1811t Revisions 10987 and 10988

This is really good work! And it highlights again why IE is nasty. I have the following small things to mention:

1. In web_client.html, wouldn't it be more clear (and safer from future editing mistakes) to call requestHelper.initialize() in an onload event?
2. In web_client.html, please remove the extra space in stateChanged () and add a line break before the curly brace in if (httpRequest.readyState === 4) {. Also, the first inline script section should be indented 6 spaces.

#72 - 01/28/2016 09:27 AM - Sergey Ivanovskiy

Committed revision 10990 has fixes according to the review.

#73 - 01/28/2016 10:57 AM - Greg Shah

- % Done changed from 0 to 100

- Status changed from New to Closed

The code looks good. I'm closing this now.

#74 - 02/05/2016 04:40 AM - Constantin Asofiei

Sergey, an issue about using XMLHttpRequest - if the web client startup fails, then the message is not displayed as a html page, but included in the URL.

#75 - 02/05/2016 04:54 AM - Sergey Ivanovskiy

Constantin Asofiei wrote:

Sergey, an issue about using XMLHttpRequest - if the web client startup fails, then the message is not displayed as a html page, but included in the URL.

Ok, planning to fix it.

#76 - 02/05/2016 05:35 AM - Sergey Ivanovskiy

- File *notify_about_errors_1.txt* added

Committed revision 11013 should fix the incorrect processing error's page.

#77 - 02/05/2016 05:52 AM - Sergey Ivanovskiy

- File *ajax_changes_2.txt* added

Constantin Asofiei wrote:

Sergey, an issue about using XMLHttpRequest - if the web client startup fails, then the message is not displayed as a html page, but included in the URL.

Committed revision 11014 should fix it.

#78 - 02/05/2016 05:54 AM - Sergey Ivanovskiy

- File *deleted (ajax_changes_2.txt)*

#79 - 02/05/2016 05:54 AM - Sergey Ivanovskiy

- File *notify_about_errors_2.txt* added

#80 - 11/16/2016 12:12 PM - Greg Shah

- Target version changed from Milestone 12 to GUI Support for a Complex ADM2 App

#81 - 11/28/2016 04:17 PM - Greg Shah

- File deleted (*p2j-root-keys.store*)

#82 - 11/28/2016 04:17 PM - Greg Shah

- File deleted (*directory.xml*)

#83 - 11/28/2016 04:17 PM - Greg Shah

- File deleted (*p2j-servers-keys.store*)

#84 - 11/28/2016 04:17 PM - Greg Shah

- File deleted (*shared-private-key.store*)

#85 - 11/28/2016 04:18 PM - Greg Shah

- File deleted (*wizard_logs.txt*)

Files

calc.p.png	9.89 KB	12/14/2015	Sergey Ivanovskiy
calc-static-chars.p.png	4.15 KB	12/14/2015	Sergey Ivanovskiy
image.png	14.1 KB	12/14/2015	Sergey Ivanovskiy
browse.png	10.1 KB	12/14/2015	Sergey Ivanovskiy
ajax_changes_1.txt	5.74 KB	01/28/2016	Sergey Ivanovskiy
notify_about_errors_1.txt	3.57 KB	02/05/2016	Sergey Ivanovskiy
notify_about_errors_2.txt	3.58 KB	02/05/2016	Sergey Ivanovskiy