Steve's Exercise Notes and Errata

Version: 2022-02-07

Summary

This is a set of notes, errata, sample command lines and **important points** that students of the WE761 may find useful. This should be referenced as progress is made through the exercises. Sections in italics below are from the exercise booklet.

Exercises description

If you are unable to complete an exercise, you can copy the model solution application from the lab files directory /home/student/labfiles/dp/Solutions.
WRONG: no user folder 'student' The course lab files can be found in the following directory:
`/home/localuser/labfiles/dp`
The supplied course image is Ubuntu 14.04 LTS

Exercise 1. Upgrading image firmware

Estimated time - 00:30
Objectives
After completing this exercise, you should be able to:
• Identify the current firmware level on the gateway
• Upgrade the firmware level on the gateway
• Switch the installation image between the current and the previous version of the firmware.

An Ubuntu user ID was created for you. You use this ID to log on to the image.
*• User ID: **localuser***
*• Password: **passw0rd** (replace the o with a zero 0)*

1.1. Terminology

The version that is running on the gateway should be an older version of the 7.6.0 firmware.
*This level is referred to as the current-1 level (**IRLP 7.6.0.3**).*

The version in /home/localuser/firmware/ should be the most current level of 7.6.0 firmware.
*This level of firmware is referred to as the current level (**IRLP 7.6.0.5**).*

1.2. Determine the current firmware level

Login Blueprint Console (?) icon has menu item ***About***.

1.3. Where you download the firmware

No need to download firmware from FixCentral, provided in course folder in *image* (Ubuntu).

1.4. Upload and upgrade the firmware

System Control / Boot Image / Upload Button Boot Image `/home/localuser/firmware/idg7605.scrypt4`

1.5. Switch the installation image

Provides an option to return to the earlier level of the firmware (and subsequently return to latest installed).
CLI command: `boot switch`

Exercise 2. Using the CLI and the XML Management Interface to manage DataPower appliances

Estimated time - 01:30
CLI, SOMA, and AMP
Objectives
After completing this exercise, you should be able to:
- *Create DataPower resources by using the CLI*
- *Create DataPower resources by using SOMA requests*
- *Send appliance management requests by using AMP*

2.1. Create a student administrative user account by using CLI

CLI command: **`ssh 192.168.100.201`**

```
idg# show rbm
admin-state: enabled
apply-cli:   on
```

<lab_files>/mgmtInterface/createAdminUserGroup.txt
CLI commands:

```
usergroup student01_admin_group
summary "student01 administrative user group"
access-policy "*/*/*?Access=rwadx"
access-policy "*/*/file/store?Access=r"
access-policy "*/*/network/interface?Access=r"
exit

user student01_admin
access-level group-defined
group student01_admin_group
password
student01
student01
```

CLI logout sysadmin.
CLI login student01_admin.

2.2. Review the XML Management Interface WSDL (optional)

Files in Ubuntu `<lab_files>/mgmtInterface/DP` are copies of what is in DataPower `store:///` folder.
DO NOT SPEND TOO MUCH TIME ON THIS.

2.3. Create developer resources by using XML Management Interface

```
cd /home/localuser/labfiles/dp/mgmtInterface
```

Note: last folder name above should have capital '**I**'.

Note: curl commands below are on a single line.

```
curl -H "Content-Type: text/xml" --data-binary @createDeveloperResources.xml
https://192.168.100.201:5550/service/mgmt/current -u sysadmin:sysadminpassw0rd -k

curl -H "Content-Type: text/xml" --data-binary @saveConfig.xml
https://192.168.100.201:5550/service/mgmt/current -u sysadmin:sysadminpassw0rd -k
```

2.4. Import a domain configuration from an HTTP server

Log in to the CLI as a student developer.
Id: `student01`
Domain to log in to: `student01_domain`
CLI commands:

```
ping 192.168.100.1
test tcp-connection 192.168.100.1 80

co
copy http://192.168.100.1/dp/DPCert.cer cert:///DPCert.cer (*** NOT USED)
copy http://192.168.100.1/dp/Alice-sscert.pem cert:///Alice-sscert.pem
copy http://192.168.100.1/dp/Alice-privkey.pem cert:///Alice-privkey.pem
```

DPCert.cer expires 2013-06-06, but not a problem, since not used.
Alice-sscert.pem expires 2028-01-13, so that's not a problem.

CLI commands:

```
import-package DPAdminPackage
source-url http://192.168.100.1/dp/DPAdmin.zip
import-format ZIP
exit

import-execute DPAdminPackage
```

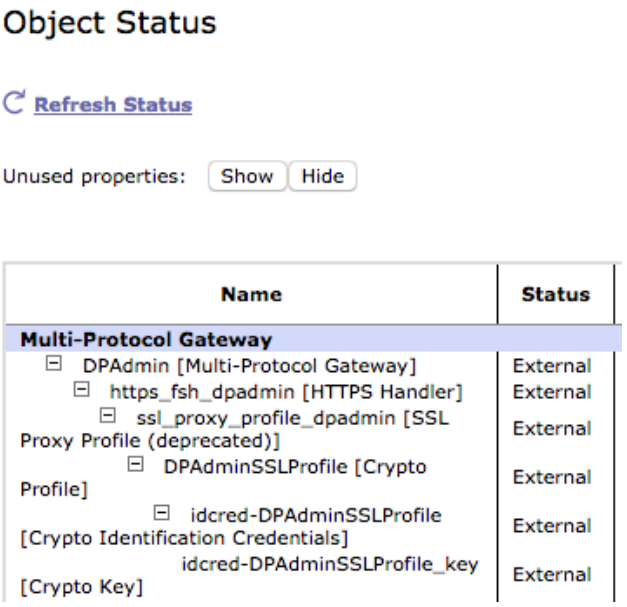
Crypto Certificate
idcred-DPAdminSSLProfile_cert references Alice-sscert.pem

Configuration of MPGW and subobjects not stored locally, see the following code section in the config file of the domain `config:///student01_domain.cfg`:

```
%if% available "import-package"

import-package "DPAdminPackage"
  source-url "http://192.168.100.1/dp/DPAdmin.zip"
  import-format ZIP
  overwrite-files
  overwrite-objects
  local-ip-rewrite
  auto-execute
```

```
exit

%endif%

import-execute "DPAdminPackage"
```

So when the domain is restarted, the configuration of the services and objects defined in that remote ZIP file will be read in again, and overwrite any changes that might have been made since initially imported (e.g using any of WebGUI, CLI, XMI, RMI). If you look at the status of the service and its related object (by clicking *View Status*), you will notice that the are ***external***:



So, when changes are made and *Applied*, the running objects are modified, but when Saving Changes, no objects that are external may be seen in the domain's config file. Therefore, a restart of the domain will not have any of the changes made since the `import-execute` was run.

CLI commands:

```
show source-https https_fsh_dpadmin

source-https https_fsh_dpadmin
port 10011
exit
```

The <mpgw_dpadmin> port is 10**01**1.

After this change, the status of the HTTPS Handler goes from external to modified.
However, this is no record of this in the domain CFG file.

If, however, the DPAdmin.zip file had been imported (e.g. *Control Panel* / *Import Configuration*), as is often done during development, all of the service objects will then be defined in the domain CFG file, once the *Save Configuration* action has occurred.

2.5. Test the DPAdmin multi-protocol gateway service

Authentication sysadmin / sysadminpassw0rd

2.6. Create more developer domains by using XML Management Interface requests

Edit **`set-config.xml`**, changing **nn** to **01**

```
curl -H "Content-Type: text/xml" --data-binary @set-config.xml
https://192.168.100.201:5550/service/mgmt/current -u sysadmin:sysadminpassw0rd -k

curl -H "Content-Type: text/xml" --data-binary @saveConfig.xml
https://192.168.100.201:5550/service/mgmt/current -u sysadmin:sysadminpassw0rd -k
```

2.7. Modify the developer user group by using an XML Management Interface request

Edit **`modify-config.xml`**, changing **nn** to **01**

```
curl -H "Content-Type: text/xml" --data-binary @modify-config.xml
https://192.168.100.201:5550/service/mgmt/current -u sysadmin:sysadminpassw0rd -k

curl -H "Content-Type: text/xml" --data-binary @saveConfig.xml
https://192.168.100.201:5550/service/mgmt/current -u sysadmin:sysadminpassw0rd -k

curl -H "Content-Type: text/xml" --data-binary @backup-domain.xml
https://192.168.100.201:5550/service/mgmt/current -u sysadmin:sysadminpassw0rd -k
```

2.8. Use AMP to interrogate the gateway

```
curl -H "Content-Type: text/xml" --data-binary @getdeviceinfo.xml
https://192.168.100.201:5550/service/mgmt/amp/3.0 -u sysadmin:sysadminpassw0rd -k
```

Edit **`getdomainstatus.xml`**, changing **nn** to **01**

```
curl -H "Content-Type: text/xml" --data-binary @getdomainstatus.xml
https://192.168.100.201:5550/service/mgmt/amp/3.0 -u sysadmin:sysadminpassw0rd -k
```

2.9. REST management

(See alternative to *RESTClient* Firefox add-on: *POSTMAN*)

```
GET https://192.168.100.201:5554/mgmt/status/default/ActiveUsers

GET https://192.168.100.201:5554/mgmt/domains/config/
```

Note: reduced JSON structure, as some of the settings are default:

```
POST https://192.168.100.201:5554/mgmt/config/default/Domain
       {
         "Domain" : {
           "name" : "student01_REST_domain",
           "mAdminState" : "enabled",
           "UserSummary" : "REST-added domain for student account 01.",
           "NeighborDomain" : {"value": "default"}
         }
       }
```

```
PUT https://192.168.100.201:5554/mgmt/config/default/Domain/student01_REST_domain/UserSummary
       { "UserSummary" : "Modified summary for student account 01."}

GET https://192.168.100.201:5554/mgmt/config/default/Domain/student01_REST_domain

POST https://192.168.100.201:5554/mgmt/actionqueue/default
       {"SaveConfig" : ""}

GET https://192.168.100.201:5554/mgmt/status/default/DomainStatus

DELETE https://192.168.100.201:5554/mgmt/config/default/Domain/student01_REST_domain
```

Exercise 3. Using the troubleshooting tools to debug errors

Estimated time 01:00
Objectives
After completing this exercise, you should be able to:
- *Set up and analyze the default system logs*
- *Configure a multi-step probe to conduct message-level process debugging*

3.1. Import the correct configuration

<studentnn_domain> domain
<lab_files>/Troubleshooting, and select MyBasicMPG.zip
MyBasicMPG / HTTP_FSH_MyBasicMPG
192.168.100.202:10016

3.2. Use the default system logs for problem determination

Change the system log level to debug.

cd /home/localuser/labfiles/dp/Troubleshooting

ERROR should be <dp_public_ip>:
Section 2: Test case 1: Execution and analysis
curl -H "Content-Type: text/xml" --data-binary @AddressReq.xml http://<dp_internal_ip>:<mpgw_basic_port>

curl -H "Content-Type: text/xml" --data-binary @AddressReq.xml http://192.168.100.202:10016

Section 3: Test case 2: Execution and analysis
Fail case.
<title1>
System log
<title>

3.3. Use the multi-step probe to debug message flows in DataPower

curl -H "Content-Type: text/xml" --data-binary @AddressReq.xml http://192.168.100.202:10016

Section 3: Challenge test cases: Execution and analysis
Fail case.
<title1>
curl -H "Content-Type: text/xml" --data-binary @AddressReq.xml http://192.168.100.202:10016

3.4. Use Wireshark to view a packet capture file for debugging purposes

sysadmin
Domain default
Section 2: Load the pcap file in the Wireshark tool
Use prepared PCAP file.

*** NEED TO DRAG DOWN DIVIDER TO SEE UPPER WINDOW

Frames 54 / 59 - OK (200)
Frames 196 / 200 (not 199 ***) - Fault (500)

Exercise 4. Securing connections with SSL

Objectives
After completing this exercise, you should be able to:
- *Use the DataPower cryptographic tools to generate cryptographic keys*
- *Use a cryptographic key and certificate object to create a cryptographic identification credential*
- *Use a validation credential object to validate certificates*
- *Create an SSL proxy profile to accept SSL connections from a client*

4.1. Generate a certificate-key pair on the DataPower appliance

BPC student01 / domain student01_domain

Information
Both files (*** NOT objects) are in the cert: directory.

Crypto Identification Credential: StudentIdCred
Crypto Validation Credential: StudentValCred
Crypto Profile: StudentServerCP
- set up to allow mutual auth
You build the Crypto Profile: StudentServerCP, but it is never used.
So you can miss out the section:
__ *3. Create a server crypto profile to use in an SSL communication.*
on page 4-10.

4.3. Configure server-side SSL

Change the crypto profile DPAdminSSLProfile to use the new identification credential: **StudentIdCred**

This profile is the one used in the DPAdmin multi-protocol gateway.

*** Exercise uses SSL Proxy Profile, should NOT be used.
Use SSL Server Profile instead.

EXTRA change Front Side Protocol https_fsh_dpadmin to use Server Profile instead of Proxy Profile instead.
Use Identifcation Credentials 'StudentIdCred'

The following section is misleading:

4.3. Configure server-side SSL

_2. Examine the DPAdmin MPGW
_d. From the User Agent settings section, find the DPAdmin proxy profile.
Because it is the HTTPS FSH that we are changing!

Exercise 5. Logging to an external system

Estimated time 01:00
Objectives
After completing this exercise, you should be able to:
- *Use the Generate Log Event action to test the log target configuration*
- *Create a log target that subscribes to specific log categories*
- *Create a log target that sends log messages to an external logging system*

Log Category: orderEntry01

Log target: orderEntrynnLocalLog

5.3. Use an event trigger

Add to create a specific event trigger.
Message ID: 0x88776655.
Regular Expression: orderError
matches Log messsage
CLI Command:
mkdir local:///capturedLog; copy logtemp:///default-log local:///capturedLog/retained-default-log

Generate Log Event
Log Category: orderEntry01
Log Level: error
Log Message: orderError - name is missing
Event Code: 0x88776655
WORKS!

5.4. Create a syslog-tcp log target

5.5. Import and modify the LogTransformMPG service

curl -H "Content-Type: text/xml" --data-binary @AddressReq.xml http://192.168.100.201:10015

Published on:
https://docs.google.com/document/d/e/2PACX-1vRcV7Rqh0NmXnPf9XZmW4kZQTY8a80-LhESSVonywK8csnDCr5Xmtz3O5bIcjqiijG0cbPM5sXL9xNm/pub