Hardening Novell GroupWise 2012 Security Lab

GW04

Novell Training Services

www.novell.com

ATT LIVE 2012 LAS VEGAS

Novell®

Legal Notices

Novell, Inc.

404 Wyman Street, Suite 500

Waltham, MA 02451

U.S.A.

www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

Third-Party Materials

Contents

SECTION 1 Hardening GroupWise 2012 Security

In this lab you will enhance your GroupWise systems Security by completing the following:

Exercise 1-1 Configure GroupWise Agents on Linux to run as a Non-root User

In this lab you will configure the GroupWise Agents running on Linux to run as a Non-root account.

1. Login to the GW2012-Linux VM as **root** with a password of **n0v3ll**
2. Open a terminal by right-mousing and selecting **Open in Terminal**
3. Type **ls -l /mail**
4. Type **chmod -R 777 /mail**

NOTE: This will change the permissions of the /mail folder and sub folders to rwx.rwx.rwx This will allow any user we configure to run as non-root have adequate rights to the files.

---

5. Type **ls -l /mail**
6. Type **cd /etc/opt/novell/groupwise**
7. type **mkdir agents**
8. Type **cd agents**
9. Type **vi uid.conf**
10. Hit the **Insert key** to enter insert mode
11. Type **attuser**
12. Hit **ESC** and then type **:wq** to save and exit
13. Stop all Groupwise Agents by typing **rcgrpwise stop**
14. We need to delete the existing uid.run files in the agent directories type the following:
    - **rm /mail/slcdom/uid.run**
    - **rm /mail/slcdom/wpgate/gwia/uid.run**
    - **rm /mail/slcpo/uid.run**
15. Restart the Groupwise Agents by typing **rcgrpwise start**
16. Type **rcgrpwise status** to verify all agents are running
17. Once the agents are restarted type **ps -eaf | grep gw**, then scroll up, this will show all GroupWise processes running and what user they are running as.

NOTE: Notice the Domain, Post Office and Internet agent are running as attuser. The instances of the DVA are still running as root.

---

18. Type **Exit** to close the terminal window.

You have successfully configured the Linux GroupWise Agents to run as a non-root user.

(End of Exercise)

Exercise 1-2 Enabling LDAP Authentication

In this Exercise you will configure LDAP authentication and LDAP Pooling

- Enable the POA for LDAP Authentication
- Enabling LDAP Authentication Pooling

Prerequisites

The following steps must be completed prior to starting the lab.

1. GW8-NetWare VM is loaded.
2. GW2012-Linux VM is loaded with GW 2012 Agents
3. The WinXP VM is logged into the DA-TREE Tree

Task I: Enable LDAP Authentication

In the classroom we have been using GroupWise passwords of n0v3ll up to now. All of the users in the system also have an eDirectory password set to n0v3ll (all lowercase). We will change a few users GroupWise passwords before configuring for LDAP Authentication. If you are going to be running NLDAP and GWIA on the same server (like in the Lab) you would need to disable LDAP on the GWIA.

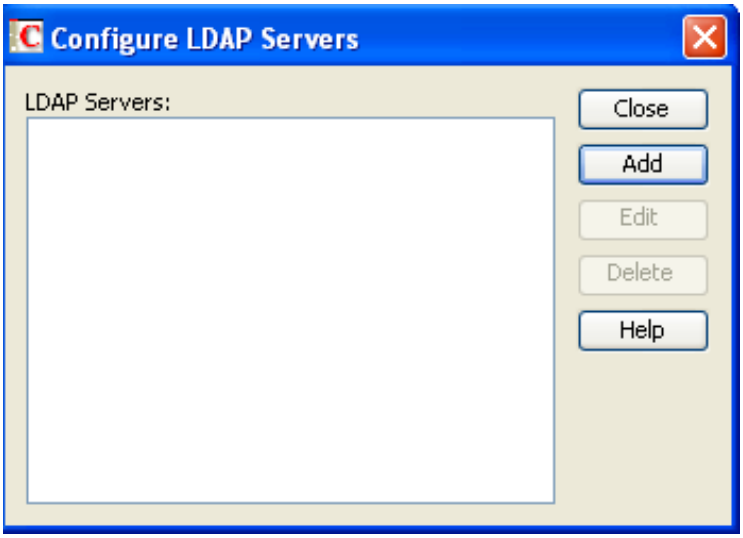
1. Switch to the GW2012-Linux VM
2. Launch ConsoleOne, authenticate at **Admin** password **n0v3ll**
3. Click the **GroupWise System**
4. Select **Tools | GroupWise System Operations | Select Domain**
5. Accept the Domain Path of **/mail/lgadom** by selecting **Ok**
6. Change the pull-down menu to display the **Users**
7. Highlight user **SHussey**, right-mouse select **Properties**
8. Navigate to **GroupWise > Account**, then select **Change GroupWise Password** Enter the new password of groupwise (all lower case), Select **Ok**

   Wait 30 seconds for the password to change before proceeding
9. Switch to the WinXP VM
10. Launch the GroupWise client. Login is as **SHussey**, password **groupwise**
11. Close the GroupWise Client
12. Repeat Steps 7 to 10 but with the user **KWilde**

    Once both users have different GroupWise and eDirectory password we can continue on configuring LDAP Authentication
13. Change the pull-down menu to display the **Gateways**
14. Right-click on **GWIA** and choose **Properties**

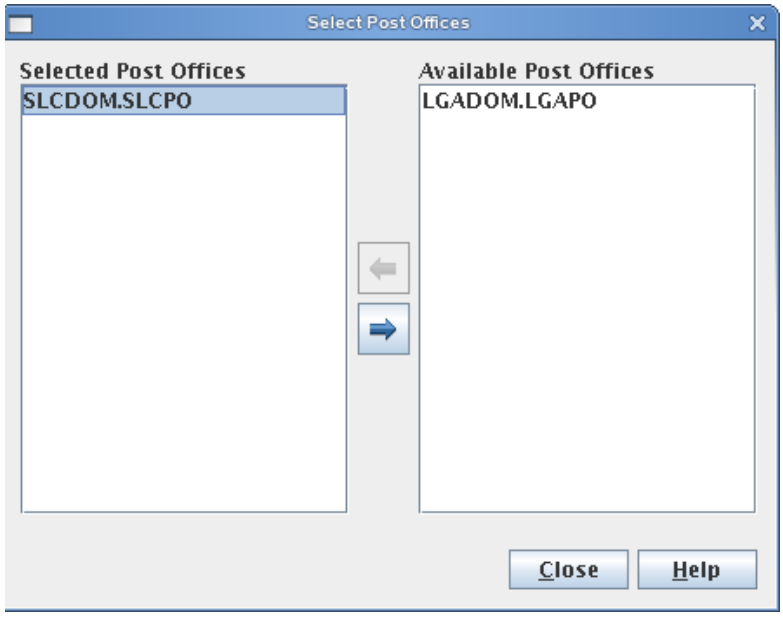
15. Click the **LDAP** Tab
16. Verify that Enable LDAP service is unchecked
17. Select **Ok** or Cancel
18. Switch to the GW2012-W2K8 VM
19. Launch ConsoleOne
20. Click the **GroupWise System**
21. Change the pull-down menu to display the **Gateways**
22. Right-click on **GWIAW2K8** and choose **Properties**
23. Click on the **LDAP** Tab
24. Verify that Enable LDAP service is unchecked
25. Select **Ok** or Cancel

    Now that we have disabled LDAP on both the GWIA's we can configure LDAP Authentication
26. Switch to the GW2012-Linux VM
27. Launch ConsoleOne
28. Highlight the GroupWise system
29. From the TOOLS menu choose GroupWise System Operations | LDAP Servers
30. You should see an empty list of LDAP Servers similar to the graphic:

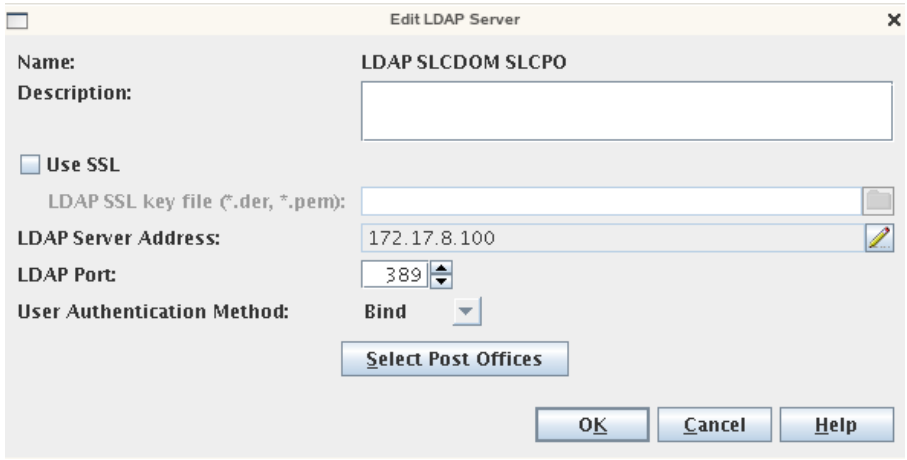


31. Select **Add**
32. Enter **LDAP SLCDOM SLCPO** for the name
33. Click on the Pencil Icon to the right of the LDAP server Address
34. Enter **172.17.8.225** as the IP Address and choose **OK**

35. Click on Select Post Offices
36. Verify the SLCDOM.SLCPO is on the selected list. If not add it.

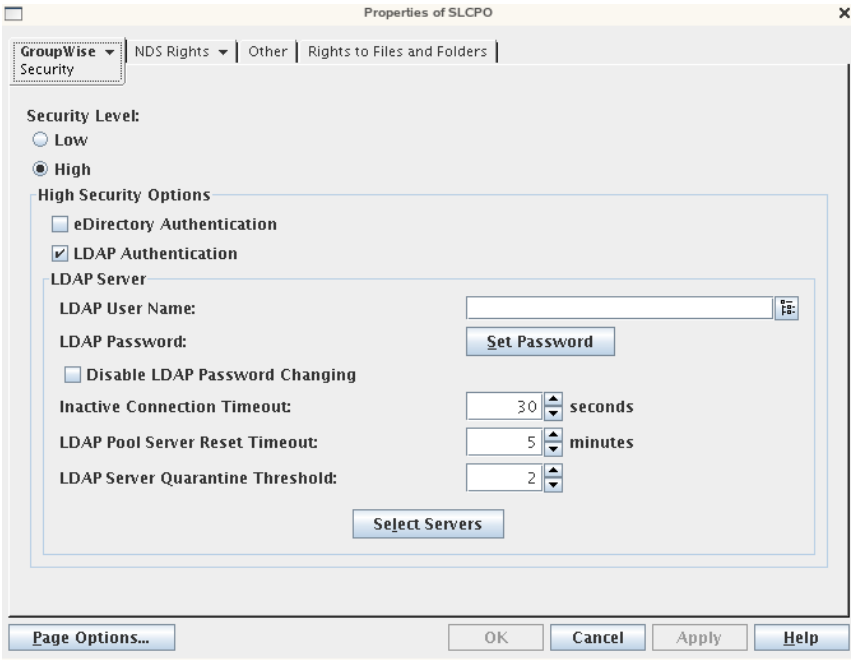


37. Select **Close**
38. Your LDAP configuration should look like the following:



39. Select **OK**
40. Select **Add**
41. Enter **LDAP LGADOM LGAPO** for the name
42. Click on the Pencil Icon to the right of the LDAP server Address
43. Set the LDAP Server Address to **172.17.8.200**
44. Select Post Offices and verify that **LGADOM.LGAPO** is on the Selected List

45. Click Close
46. Choose **OK**
47. Select Close to Close Configure LDAP Servers
48. Expand the GroupWise system to display the Domains and Post Offices
49. Right-Click on the SLCPO and choose Properties
50. From the GroupWise tab choose Security



51. Enable LDAP Authentication by checking the box
52. Click on the Select Servers box
53. Verify that the LDAP SLCDOM SLCPO Server is on the select list and then choose Close
54. Click OK
55. Repeat for the LGAPO - Except assign it to the LDAP LGADOM LGAPO Server
56. Login to GroupWise as **KWilde** from the GW2012-W2K8 VM, password **groupwise**
57. Login in a second time use **groupwise** as the password again

TIP: You will now see a warning about LDAP authentication being activated and to use a directory services password

58. Use **n0v3ll** as the password

59. If you to log at the POA log files you should see it login and verify the credentials against the LDAP server Example:

```
07:45:32 0F0C C/S Login Windows  Net Id=admin.SLC.DA ::GW Id=kwilde :: 172.17.8.245
07:45:32 0F0C Initializing LDAP session with 172.17.8.200 at port 389 (kwilde)
07:45:35 0F0C LDAP Error: 49  (kwilde)
07:45:35 0F0C LDAP Error: Invalid credentials  (kwilde)
07:45:38 0F0C LDAP Error: 49  (kwilde)
07:45:38 0F0C LDAP Error: Invalid credentials  (kwilde)
07:45:38 0F0C Error: Invalid password [D019] User:kwilde  (kwilde)
07:45:44 0F0C LDAP Error: 49  (kwilde)
07:45:44 0F0C LDAP Error: Invalid credentials  (kwilde)
07:45:44 0F0C Error: Invalid password [D019] User:kwilde  (kwilde)
07:45:49 0F0C Processing update: environment settings record (kwilde)
07:45:49 0F0C Processing update: environment settings record (kwilde)
07:45:50 054C Processing update: environment settings record (kwilde)
07:45:50 0F0C Processing update: environment settings record (kwilde)
07:45:51 0F0C *** NEW APP CONNECTION, Tbl Entry=1, Check ID=1333994822
07:45:51 0F0C C/S Login Windows  Net Id=admin.SLC.DA ::GW Id=kwilde :: 172.17.8.245
```

60. Exit the GroupWise client for KWilde
61. Launch ConsoleOne
62. From ConsoleOne click on LGAPO
63. Change the Pull-down menu to display users
64. Right-Click on KWilde and choose properties
65. From the Restrictions tab choose Password Restrictions
66. Click Change Password
67. Change **KWilde's** password to **ldaprules** (all lowercase)
68. Choose OK to close properties on KWilde

IMPORTANT: We changed the eDirectory password, not the GroupWise password. With LDAP Authentication we use the eDirectory password

---

69. Login to GroupWise as KWilde, when prompted for a password enter **n0v3lll**
70. What Happens?
71. Enter **ldaprules** as the password and choose **Ok**
72. From the GroupWise Client select **Tools > Options** then select **Security**
73. Change the password back to **n0v3ll** from ldaprules (use all lowercase), select **Ok**

NOTE: Just to keep the passwords consistent for the rest of class

---

IMPORTANT: Once you enable LDAP Authentication if a user changes their password in GroupWise they are changing their eDirectory password. If you do not want them to change their eDirectory password from GroupWise, make sure you Disable LDAP Password Changing option

---

74. Select **Close** to close the options dialog

75. Exit GroupWise for KWilde
76. From ConsoleOne right-click on the SLCPO post office and choose **properties**
77. From the GroupWise tab choose **Security**
78. Check the box next to **Disable LDAP Password Changing**
79. Choose OK

    Wait for the change to replicate about 15-30 seconds
80. Launch the GroupWise client and log in as **KWilde**, password **n0v3ll**
81. From the GroupWise Tools menu choose Options | Security try to change the password

---

NOTE: You can enter the current password, but the New Password fields should be greyed out and you can not change the password

---

WARNING: If the option is not greyed out the update has not yet made it to the POA. Exit the GroupWise client and give it a moment then try again

---

82. Close the GroupWise client
83. From ConsoleOne go back to Security for the SLCPO and uncheck the box next to Disable LDAP Password Changing
84. Launch a Web Browser from the WinXP VM
85. Browse to Web Console for the LGAPO POA

TIP: Browse to http://da-w2k8.digitalairlines.com:7181 or http://172.17.8.245:7181

---

86. Login as **webagent** password **n0v3ll**
87. Click on the **Configuration** link at the top of the page
88. Scroll down to the LDAP Authentication on the POA configuration settings section

---

NOTE: It is now showing as Enabled

---

89. Click on the **LDAP Authentication** link
90. Notice the LDAP Server Status of **Good**
91. Close the Web Browser
92. Close ConsoleOne

Task II: Test LDAP Authentication from the Linux POA

We now know that users on the DA-W2K8 POA can authenticate. We need to verify that users on the Linux POA can also authenticate to NLDAP Running on Linux.

1. Switch to the GW2012-Linux VM
2. Launch the GroupWise Client login as **SHussey**. Use **groupwise** (lowercase) as the password
3. Enter the password of **groupwise** a second time
4. You should receive an LDAP failure detected
5. Open a Web Browser from the WinXP VM and browse to **http://da-linux.digitalairlines.com:7181**

   NOTE: This is web console for the Linux PO

6. Enter **webagent** for the username and **n0v3ll** for the password
7. Select **Configuration**
8. Click on the **LDAP Authentication** Link
9. Check the LDAP server Status. It should say **Good** in green letters.
10. Select **Log Files**
11. Select **Cycle Log**
12. Select the Log just above the current log. The current log is marked with an asterix
13. Select **View Events**
14. Scroll through the Log looking for LDAP Errors. You should see LDAP Error 13

    If you were to search the Knowledge base on Http://support.novell.com for LDAP Error: 13 you would find `TID10067376 Common LDAP Errors reported by the POA`

    TID 10100740 Lists LDAP Error 13:

    09:58:37 1C5 LDAP Error: 13

    09:58:37 1C5 LDAP Error: Confidentiality required

    09:58:37 1C5 Error: LDAP failure detected [D06B] User:User1

    Error 13 Cause/Fix: This error will occur when SSL is NOT being used AND the LDAP Group Object is not configured to use Clear Text Passwords. This can be resolved by either enabling SSL or by editing the LDAP Group Object and Disable the checkbox Require TLS For Simple Bind with password
15. Switch to GW2012-Linux Virtual machine
16. Launch ConsoleOne if not already open

17. Authenticate to the DA-TREE Tree as **Admin**, password of **n0v3ll**
18. Browse to the **SLCA.DA** container
19. Select the **LDAP Group - DA-Linux** object in the SLC.DA container then **right-mouse** and choose **Properties**
20. Uncheck **Requires TLS for Simple Binds with Passwords**
21. Choose OK
22. From a Terminal Prompt on DA2L switched to the root user, enter **rcndsd restart**
23. Once NDSD is restarted, enter **rcndsd status** to verify
24. Launch GroupWise login as **SHussey** with **n0v3ll** (lowercase) as the password

    NOTE: This time you should be able to logon as SHussey. If you receive an error check your steps

25. Exit the GroupWise Client

Task III: Enabling LDAP Authentication Pooling

1. From a Terminal Prompt on GW2012-Linux, enter **rcndsd stop**

   NOTE: This will stop eDirectory on the Linux box

2. Attempt to Logon to GroupWise as **SHussey** with **n0v3ll** (lowercase) as the password twice.

   NOTE: Logon will fail with an LDAP failure since the LDAP server was stopped in Step 1

3. Open a Web Browser on the WinXP VM and browse to **http://da-linux.igitalairlines.com:7181**

   NOTE: This is Web Console for the Linux PO

4. Enter **webagent** as the username and **n0v3ll** for the password
5. Select **Configuration**
6. Select **LDAP Authentication**
7. Under the Section Load Balance Pool Configuration notice the following:
   - There is only 1 server listed LDAP LGADOM LGAPO
   - The LDAP Server Status is **Bad**
8. Minimize the Web Browser

9. Switch to a GW2102-Linux Terminal Window and enter **rcndsd start**, to restart eDirectory
10. From ConsoleOne on the GW2012-Linux VM Right-click on the **SLCPO** and choose **properties**
11. From the GroupWise Tab choose **Security**
12. Choose Select Servers
13. Select the LDAP LGADOM LGAPO and add it to the List of selected servers
14. Choose close
15. Choose OK
16. Repeat for the LGAPO, add the LDAP SLCDOM.SLCPO to the list of selected servers
17. Open FireFox on GW2012-Linux
18. Maximize the Web Browser and refresh the browser to **http://da-linux.digitalairlines.com:7181**

    NOTE: This is Web Console for the Linux PO

19. Select Configuration
20. Select LDAP Authentication
21. Under the Section Load Balance Pool Configuration notice the following:
    - There are now 2 servers listed LDAP LGADOM LGAPO and SLCDOM.SLCPO
    - LDAP LGADOM.LGAPO shows as Starting and LDAP SLCDom.SLCPO shows as Starting
22. Switch to the Terminal window and enter **rcndsd stop**, to stop eDirectory
23. Launch GroupWise on the WinXP VM as **SHussey** with **n0v3ll** (lowercase) as the password

    TIP: If you get an LDAP error wait a minute until the configuration changes replicate and try again

24. Once you are logged in to GW, from the Web Browser Choose Refresh to reload the Web page
25. Notice the LGADPM LGAPO Server Status shows Good and the SLCDOM.SLCPO shows Bad.

Load Balance Pool Configuration: **	
Server Pool: LDAP LGADOM LGAPO	
LDAP Authentication Server IP Address	172.17.8.200
LDAP Server Port	389
LDAP SSL Enabled	No
LDAP User Authentication Method	Bind
LDAP Server Status	Good
Total Hits on an Established Bind:	2
Total Number of New Binds:	2
Total LDAP Requests to this Server:	4
Total Number of Failed Bind:	0
Server Pool: LDAP SLCDOM SLCPO	
LDAP Authentication Server IP Address	172.17.8.225
LDAP Server Port	389
LDAP SSL Enabled	No
LDAP User Authentication Method	Bind
LDAP Server Status	Bad
Time left before Server resets	293
Last Quarantine Error code	81
Last Down Time	04-10-12 10:30:37
Total Hits on an Established Bind:	0
Total Number of New Binds:	1
Total LDAP Requests to this Server:	1
Total Number of Failed Bind:	1

26. Exit Groupwise
27. Close the Web Browser
28. Exit ConsoleOne
29. From a Terminal Prompt on GFW2012-Linux switched to the root user, enter **rcndsd start**

NOTE: This will re-start eDirectory on the Linux box

(End of Exercise)

Exercise 1-3 Enable SSL

SSL helps to provide additional security in your GroupWise system. Communication in GroupWise is already encrypted; MTA - POA, POA - Client, however SSL can provide additional security, especially if you are connecting over the internet.

Task I Enable SSL for LDAP Authentication

If you enable LDAP Authentication, but do not SSL-ize it, passwords will be passed as clear text. This is generally not acceptable, even inside the firewall. If you plan on using LDAP Authentication, please SSL enable the POA.

1. From the WinXP VM open windows explorer and browse to **F:\Public**
2. Copy **F:\Public\RootCert.der** to **S:** to place file on the DA-Linux server
3. Copy **F:\Public\RootCert.der** to **W:** to place file on the DA-W2K8 server
4. Switch to the GW2012-Linux VM
5. Open a Terminal
6. Enter **cp /mail/RootCert.der /opt/novell/groupwise/agents/lib/nldap**
7. Enter **cp /mail/RootCert.der /opt/novell/groupwise/agents/bin**
8. Launch ConsoleOne, authenticate as **Admin**, password **n0v3ll**
9. Select the GroupWise system
10. From the Tools menu Choose GroupWise System Operations | Select Domain
11. Select Ok
12. Expand the GroupWise System highlight the SLCDOM object
13. From the Tools menu choose GroupWise System Operations | LDAP Servers
14. Edit the LDAP SLCDOM SLCPO Server
15. Click on Use SSL
16. For the SSL Key File enter **RootCert.der**

> IMPORTANT: Do not specify a path. If no path is specified then the POA will look into the directory it was started from for RootCert.der. Also for Linux compatibility maintain the proper case.

17. Verify the LDAP port is **636** and choose OK
18. Choose **Close** to close the LDAP servers window
19. Switch to the Terminal
20. Restart GroupWise by entering rcgrpwise restart
21. Login to the GroupWise client as **SHussey** use **n0v3ll** (lowercase) as the password
22. You should notice the Secure Login on the POA - Example:

```
12:55:10 F087 *** NEW APP CONNECTION, Tbl Entry=0, Check ID=1334062283
12:55:10 F087 C/S Login Windows  Net Id=admin.SLC.DA ::GW Id=shussey :: 172.17.8.101
12:55:10 F087 Initializing Secured LDAP session with 172.17.8.225 at port 636 using SSL Key file /o
12:55:10 F087 Processing update: environment settings record (shussey)
12:55:10 F087 Processing update: environment settings record (shussey)
12:55:11 F087 Processing update: environment settings record (shussey)
12:55:11 F087 Processing update: environment settings record (shussey)
```

NOTE: You may need to close and login several times before the Secure LDAP connection starts.

23. Launch a Web Browser and Browse to **http://da-1inux.digitalairlines.com:7181**

TIP: This is Web Console for the SLC POA

24. Enter **webagent** and **n0v3ll** for the password
25. Click the **Configuration** at the top of the window and then Click the LDAP Authentication link
26. Notice that now it is showing SSL as Enabled.

Load Balance Pool Configuration: **	
Server Pool: LDAP LGADOM LGAPO	
LDAP Authentication Server IP Address	172.17.8.200
LDAP Server Port	389
LDAP SSL Enabled	No
LDAP User Authentication Method	Bind
LDAP Server Status	Starting
Total Hits on an Established Bind:	0
Total Number of New Binds:	0
Total LDAP Requests to this Server:	0
Total Number of Failed Bind:	0
Server Pool: LDAP SLCDOM SLCPO	
LDAP Authentication Server IP Address	172.17.8.225
LDAP Server Port	636
LDAP SSL Enabled	Yes
LDAP SSL Key File Name	/opt/novell/groupwise/agents/bin/RootCert.der
LDAP User Authentication Method	Bind
LDAP Server Status	Starting
Total Hits on an Established Bind:	0
Total Number of New Binds:	0
Total LDAP Requests to this Server:	0
Total Number of Failed Bind:	0

27. Switch to the GW2012-W2K8 VM
28. Open a Explorer and navigate to c:\grpwise
29. Copy **RootCert.der to c:\Program Files(x86)\Novell\GroupWise Server\Agents**
30. From ConsoleOne on the GW2012-Linux VM go back to **Tools | GroupWise System Operations | LDAP Servers**
31. Edit the **LDAP LGADOM LGAPO** server
32. Select **Use SSL**
33. Type in **RootCert.der** for the SSL Key file (do not browse for it and maintain the proper case)

34. Verify the port for the LDAP Server Address to **636**
35. Choose **OK**
36. Choose **Close** to close the LDAP servers window
37. Give the admin task a few moments to process on the LGAPO POA
38. Switch to the GW2012-W2K8 Server
39. Restart the LGAPO Post Office, by selecting **Start > Administrative Tools > Services**, click on the Description field to get the GroupWise components listed at the top
40. Highlight the LGAPO POA and right-mouse select **Restart**
41. Launch GroupWise from the WinXP VM login as **KWilde** - password **n0v3ll** (lowercase)
42. Launch a web Browser and browse to **http://da-linux.digitalairlines.com:7181**
43. Enter **webagent** as the username and **n0v3ll** for the password
44. Select **Configuration**
45. Select **LDAP Authentication**

Load Balance Pool Configuration: **	
Server Pool: LDAP LGADOM LGAPO	
LDAP Authentication Server IP Address	172.17.8.200
LDAP Server Port	636
LDAP SSL Enabled	Yes
LDAP SSL Key File Name	C:\Program Files (x86)\Novell\GroupWise Server\Agents\RootCert.der
LDAP User Authentication Method	Bind
LDAP Server Status	Good
Total Hits on an Established Bind:	1
Total Number of New Binds:	1
Total LDAP Requests to this Server:	2
Total Number of Failed Bind:	0
Server Pool: LDAP SLCDOM SLCPO	
LDAP Authentication Server IP Address	172.17.8.225
LDAP Server Port	636
LDAP SSL Enabled	Yes
LDAP SSL Key File Name	C:\Program Files (x86)\Novell\GroupWise Server\Agents\RootCert.der
LDAP User Authentication Method	Bind
LDAP Server Status	Good
Total Hits on an Established Bind:	0
Total Number of New Binds:	0
Total LDAP Requests to this Server:	0
Total Number of Failed Bind:	0

You will now see both LDAP server configured for SSL

46. You will need to review the log files for the POA in Web a console for that Post office if you want to see the secure LDAP connection at Port 636. You can Cycle the Log and then View Events to see the login text.
47. Exit the client when done
48. Close all Browser Windows

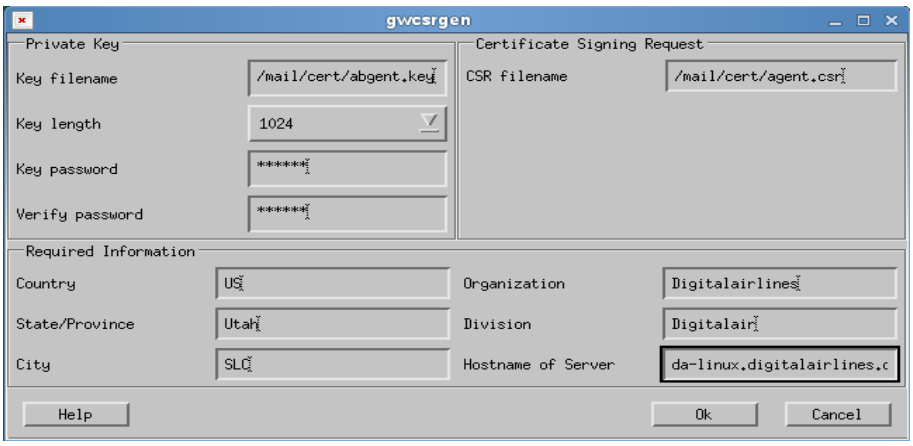
Task II SSL Enable the MTA and POA

Information passed between the GroupWise agents is already encrypted. In some situations you may want to add additional encryption. For example if you have an MTA and a POA that communicate over an Internet Connection, or MTA to MTA communication with internet connectivity.

IMPORTANT: This lab shows enabling SSL if you are using Novell Certificate server. If you are not, you will need to use a 3rd party source to mint or issue the certificate.

---

1. Open a Terminal on the GW2012-Linux VM and browse to /opt/novell/groupwise/agents/bin
2. Create a directory to place the certificate and key files enter **mkdir /mail/cert**
3. Launch the CSR Generator by entering ./gwscrgen &From Windows Explorer browse to **H:\software\admin\utility\gwcsrgen**
4. Double click **gwcsrgen.exe** to run
5. Select **Run**
6. Fill in the CSR with the following:
   - Key Filename **/mail/cert/agent.key**
   - Key Length = **1024**
   - Password = **n0v3ll** (lowercase)
   - CSR Filename **/mail/cert/agent.csr**
   - Country = **US**
   - State = **Utah**
   - City = **SLC**
   - Organization = **DigitalAirlines**
   - Division = **DigitalAir**
   - Hostname = **da-linux.digitalairlines.com**

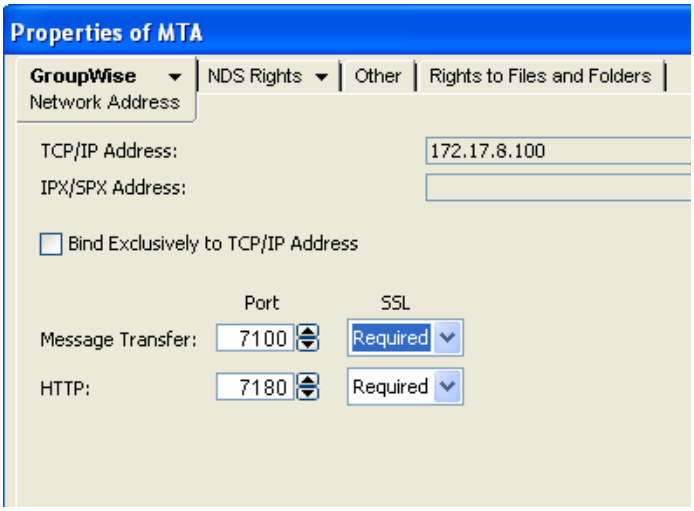


7. Choose **Create** to generate the key file and csr file
8. Enter **ls -l /mail/cert** to verify that the files were created successfully
9. Launch ConsoleOne
10. Click on the **DA** organizational unit
11. From the Tools menu choose **Issue Certificate**
12. For the filename enter **/mail/cert/agent.csr**
13. Choose **Next**
14. Choose **Nex**t
15. Select **Custom** as the type
16. Under KEY Usage - Check all three boxes
    - Data Encipherment
    - Key Encipherment
    - Digital Signature
17. Check the box: **Set the key usage extension to critical**
18. Choose **Next**
19. Notice you can change the validity period of the certificate - leave it at the default 1 year and choose **Next**
20. Select **Finish**
21. Select File in **Base 64** format
22. Change the filename to **h:\cert\agent.b64** and choose **Save**
23. Click on the SLCDOM Domain object in GroupWise system view
24. Change the pull-down to display **Message Transfer Agents**
25. Right-click the MTA and choose **properties**
26. From the GroupWise tab choose **SSL Settings**
27. For the certificate file enter **/mail/cert/agent.b64**
28. For the SSL key file enter **/mail/cert/agent.key**
29. Set the password to **n0v3ll** (lowercase)
30. From the GroupWise tab choose **Network Address**
31. For Message Transfer change SSL to **Required**

    As you have seen the Web Console is an extremely convenient and powerful feature for GroupWise administrators to leverage. However if you are going to access Web Console over the internet it is a good idea to use SSL. This protects your information, especially your authentication information, from being passed clear text across the web.

NOTE: Most of the work to SSL-ize Web Console had already been done, since a certificate for the Server has already been minted. You just need to enable it for the HTTP Protocol

32. For the HTTP change SSL to **Required**



33. Choose **OK**
34. Change the Pull-down menu to Display Post Office Agents
35. Right-Click on the POA and choose **properties**
36. From the GroupWise tab choose **SSL Settings**
37. Since the MTA and POA are on the same server you can use the same Certificate and Key files. Remember to set the password to **novell** (lowercase)
38. Once you have set the Certificate and Key files for the POA choose Network Address from the GroupWise Tab
39. For Message Transfer change SSL to **Required**
40. For HTTP change SSL to **Required**
41. Choose **Ok**
42. Switch to the Terminal, then restart GroupWise by entering **rcgrpwise restart**
43. Switch to the WinXP VM
44. Open Explorer and navigate to **s:**
45. Copy the **cert** folder and paste to **w:**
46. Switch to the GW2012-W2K8 VM
47. Launch ConsoleOne select the **LGADOM** Domain object in the GroupWise system view
48. Right click on the POA for the LGAPO and choose **properties**
49. From the GroupWise tab select **SSL Settings**

50. Enter **c:\grpwise\cert\agent.b64** for the Certificate File
51. Enter **c:\grpwise\cert\agent.b64** for the SSL Key file
52. Set the password to **n0v3ll** (lowercase)

IMPORTANT: You can mint separate certificates for each server if you choose. However GroupWise does not require that to enable SSL. For class we will keep it simple and re-use the already minted certificates.

---

53. From the GroupWise tab choose **Network Address**
54. For Message Transfer change SSL to **Required**
55. For HTTP change SSL to **Required**
56. Choose **OK**
57. Change the Pull-down menu in ConsoleOne to display **Message Transfer Agents**
58. Repeat for the LGADOM Domain MTA. Set Message Transfer SSL and HTTP SSL to **Required**

IMPORTANT: Make sure you use the c:**\grpwise\cert\agent.b64** and **c:\grpwise\cert\agent.key** when configuring the MTA just like you did with the POA

WARNING: Don't forget to set the password

---

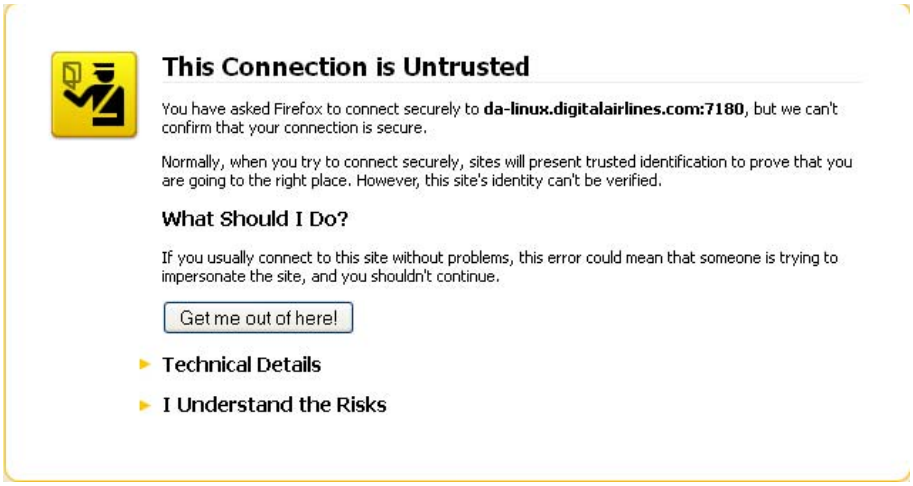
59. On GW2012-W2K8 open the Services and restart the **LGADOM**
60. Login to GroupWise as SHussey from the WinXP VM. Send and Mail message to KWilde
61. Exit the GroupWise client
62. Launch FireFox from the WinXP VM and login to the SLCDOM Domain MTA's WebConsole

---

TIP: Browse to http://da1.digitalairlines.com:7180

---

63. You should receive the following security alert



64. Since we are not using a public certificate FireFox doesn't know if it can trust it. Choose the **I Understand the Risks** link then the **Add Exception**, button
65. Make sure the Permanently store this exception box is selected and click **Confirm Security Exception** button
66. Login to the WebConsole as **webagent** and **n0v3ll** for the password
67. Notice the URL is now **https://da-1inux.digitalairlines.com:7180**

IMPORTANT: The POA recognizes the change on the fly, in order to SSL-ize your Web Console connection to the MTA you may need to restart the MTA's. The Linux agents may also require a restart.

---

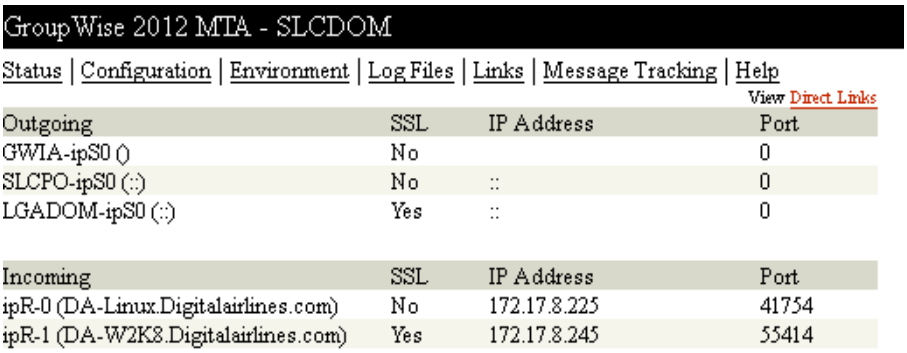
68. Click on the **Links** tab and then click on the view **TCP/IP Connections** link

---

IMPORTANT: You may need to send a few messages from MGillen to BToney and hit refresh on the following screen to see the SSL connection. The TCP/IP Connections link only shows the current Active connections. So you have to catch it in progress.

---

69. Notice which links show SSL as Yes



IMPORTANT: If you are not seeing any SSL links, send some Mail between the two domains (IE From MGillen to BToney) and then refresh your browser. The links that are showing here are only the Active links

70. Exit FireFox

You have just SSL-ized your MTA and POA

Task III: SSL Enable POA - Client connections

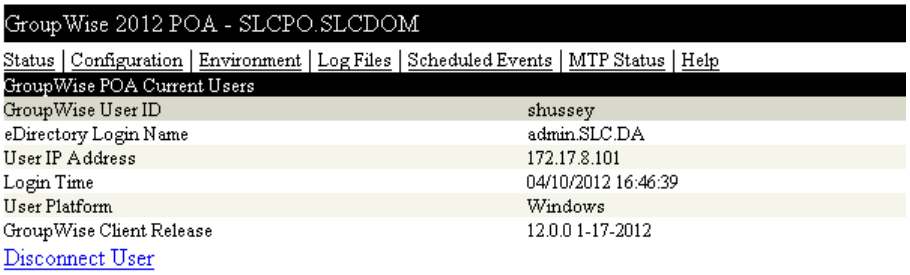
When enabling SSL for connections between the 32 bit client and POA you have a couple of scenarios. You can choose to enable SSL for clients on your local intranet, or for clients connecting from the Internet (through a proxy server) or both. You can also either enable SSL for the connection or require it. If you choose to require SSL only 6.5 clients or later can connect to the POA. If you enable SSL then older clients will still be able to connect to the POA, but 6.5 clients and later will connect using SSL.

Since we have already enabled SSL for the POA, all that needs to be done is to turn it on for the Client connection.

1. Login to the GroupWise client as SHussey
2. Launch FireFox and browse to the Web Console for the SLCPO POA

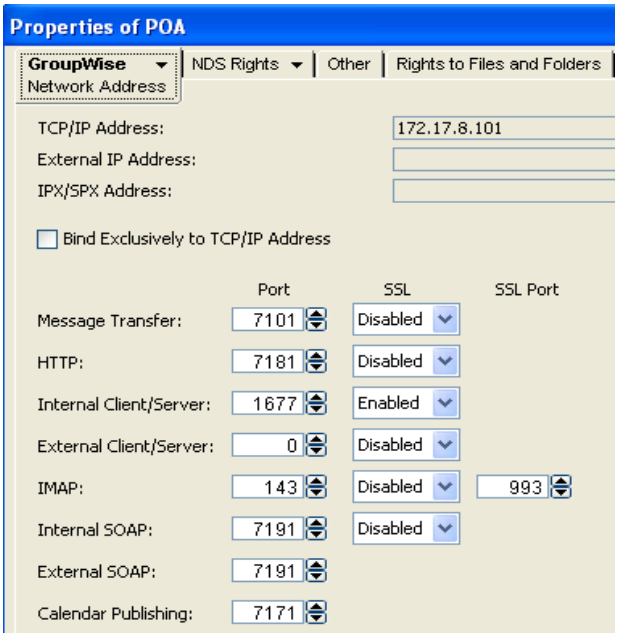
NOTE: **http://da-1inux.digitalairlines.com:7181**

3. You will receive a security alert, use same procedure in previous task to add the web site as an exception
4. Login in as **webagent** password of **n0v3ll**
5. Click on the **C/S Users** Link
6. Notice the Login Information for user SHussey and the IP Address



7. Exit the GroupWise client
8. Minimize the Web Browser
9. Switch to the GW2012-Linux VM
10. Launch ConsoleOne

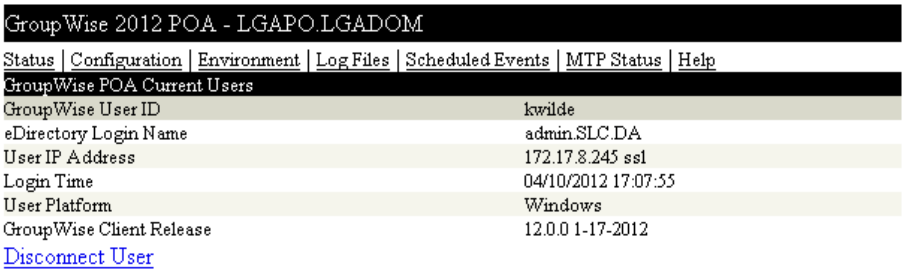
11. Edit the Properties for the SLCPO POA
12. Choose **Network Address** from the GroupWise Tab
13. Set SSL to be **Enabled** for the local Intranet Client/Server



14. Choose **OK**
15. Choose **OK**
16. Repeat for the LGAPO POA
17. Switch to the GW2012-W2K8 VM
18. Login to GroupWise as KWilde
19. If you receive the following GroupWise Security Warning dialog

Click on the Accept button to Accept and Trust the certificate and continue the GroupWise login.

20. Notice the PADLOCK icon in the lower right hand corner of the GroupWise client. This icon represents that the connection is SSL Secured
21. Maximize the Web Browser and refresh the C/S Users section of WebConsole for the LGAPO POA
22. Notice the IP address for user KWilde



23. Close the GroupWise Client
24. Close all browser windows.

As you can see SSL-izing communications is fairly easy to do. It is suggested that if you are going to enable LDAP Authentication, you should SSL-ize it. You should also SSL-ize Web Console. SSL-izing your Agent to Agent communications and POA to Client connection is really up to your security needs. Remember that it is already encrypted. Anytime the Agents or the client connect over the internet would be a great place to SSL-ize communication.

(End of Exercise)

Exercise 1-4 SSL-ize Apache on Linux for WebAccess

In this lab you will generate a CSR and key file to be used win SSL-izing Apache on Linux. You will then also redirect all HTTP traffic to HTTPS to secure GroupWise WebAccess

Task I: Configure Apache on Linux to use SSL

1. Switch to the GW2012-Linux VM and open a Terminal
2. Type **cd /mail/cert**
3. Type **openssl req -new -newkey rsa:1024 -keyout ssl.key -nodes -out ssl.csr**

   This will generate a key file and a customer signing Request that can be used to issue a SSL certificate by your own Certificate Authority or sent to a third Party to have a certificate minted
4. Enter **US** for the Country Name, and press **Enter**
5. Enter **Utah** for the State Name, then press **Enter**
6. Enter **Provo** for the Locality Name, then press **Enter**
7. Enter **Digital Airlines** for the Organization Name, then press **Enter**
8. Enter **DigitalAir** for the Organizational Unit Name, then press **Enter**
9. Enter **da-linux.digitalairlines.com** for the Common Name, then press **Enter**
10. Enter **shussey@digitalairlines.com** for the E-mail Address, then press **Enter**
11. Enter **novell** for the Challenge Password, then press **Enter**
12. On the Option company name, leave it blank and press **Enter**
13. Type **ls**, notice the 2 new SSL files
14. Launch ConsoleOne
15. Authenticate to the DA-TREE Tree as **Admin** and a password of **n0v3ll**
16. Expand the DA-CORP object and Select the **DA** organization object
17. From the menu select **Tools | Issue Certificate**
18. Browse to **/mail/cert/ssl.csr**, select **Open**
19. Select **Next**
20. On the Specify the certificate authority screen select **Next**
21. On the Select how the key is to be used screen, select the **SSL or TLS**, then select **Next**
22. On the Specify the certificate parameters use the drop down to select **Maximum** for the Validity period, then select **Next**
23. Select **Finish**
24. On the Save Certificate screen, change the path to **/mail/cert/ssl.der**, then Select **Save**

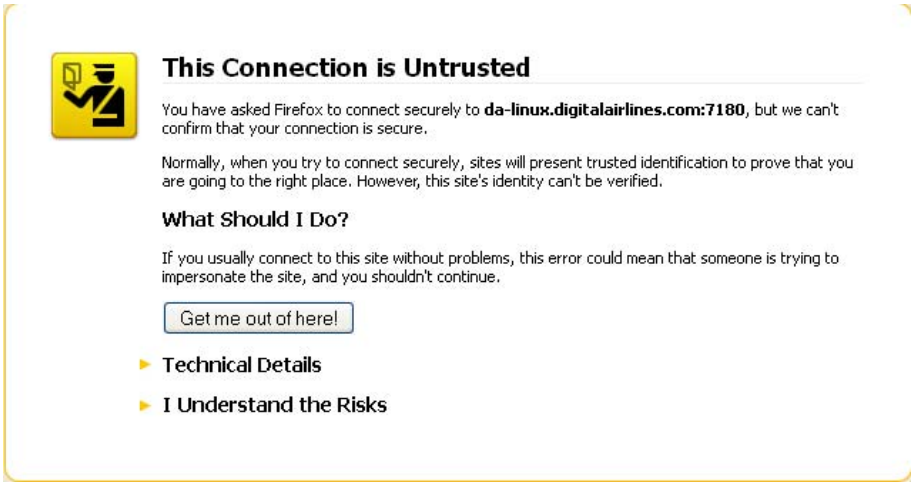
25. From the Terminal prompt type **ls**, verify that the **ssl.der** file has been created
26. Type **cd /etc/apache2/vhosts.d**
27. Type **cp vhost-ssl.template vhost-ssl.conf**
28. Type **ls,** verify vhost-ssl.conf has been created
29. Type **gedit vhost-ssl.conf**
30. Scroll down until you see a SSLCertificateFile line, change the line to point to the path of the ssl.der file The Line should look as follows:

    SSLCertificateFile /mail/cert/ssl.der
31. Scroll down until you see a SSLCertificateKeyFile line, change the line to point to the path of the ssl.key file The Line should look as follows:

    SSLCertificateKeyFile /mail/cert/ssl.key
32. **Save** and **Exit** the gedit application
33. Type **gedit /etc/sysconfig/apache2**
34. Scroll down to the APACHE_SERVER_FLAGS line. Change the line to be as follows:

    APACHE_SERVER_FLAGS=”SSL”
35. Scroll down to the APACHE_START_TIMEOUT line. Change the line to be as follows:

    APACHE_START_TIMEOUT=”10”
36. **Save** and **Exit** the gedit application
37. Type **rcapache2 restart** to restart the Apache Web Server
38. Open FireFox and browse to **https://da-linux.digitalairlines.com/gw/webacc**
39. Since we used our own Certificate Authority to mint the certificate, we will need to accept the certificate into FireFox. Click the **I Understand the Risks**, link



40. Click on the **Add Exception** button
41. Click on the **Confirm Security Exception** button
42. Notice we now are using a HTTPS secure Web Connection. This can be verified by the padlock in the lower right corner of the browser.
43. Login to WebAccess as **SHussey**, password **n0v3ll**

    Verify the contents of the Mailbox
44. Logout of WebAccess
45. Close the Browser

    In this task you will force any user attempting to access the Novell GroupWise WebAccess page using HTTP to use HTTPS

Task II: Force Novell GroupWise WebAccess to Use SSL

1. Type **gedit /etc/sysconfig/apache2**
2. Scroll down to line 103 the **APACHE_MODULES**= Line, insert after the word negotiation, the word rewrite. Make sure to leave a space before and after the word rewrite.

```
APACHE_MODULES="actions alias auth_basic authn_file authz_host authz_grou
cgi dir env expires include log_config mime negotiation rewrite setenvif
```

3. Save and Exit
4. Enter **rcapache2 restart,** if no error appear continue
5. Type cd **/etc/opt/novell/groupwise/webaccess**
6. Type **gedit gw.conf**
7. Scroll to just below the **Alias /gw "/opt/novell/groupwise/webaccess/gw/"** line
8. Enter the following

   <IfModule !mod_rewrite.c>

   LoadModule rewrite_module /usr/lib/apache2/mod_rewrite.so

   </IfModule>

   <IfModule mod_rewrite.c>

   RewriteEngine on

   Rewritecond %{SERVER_PORT} ^80$

   RewriteRule ^/gw/(.*) https://%{HTTP_HOST}/gw/$1 [NC,R,L]

   </IfModule>

   This will cause access to the GroupWise WebAccess page to use SSL
9. Save the file and Exit gedit

10. Type **rcapache2 restart**
11. Open FireFox and type http://da-linux.digitalairlines.com/gw/webacc

    You should now be redirected to a secure https web page for WebAccess

Task III: Force the default web page to Novell GroupWise WebAccess

In this task you will create an Index.html file that will redirect the default HTTP request to a HTTPS request for WebAccess

1. From the Terminal window type **cd /srv/www/htdocs**
2. Type **gedit index.html**
3. Enter the Following:

   <html>

   <head>

   <meta http-equiv="refresh" content="0;url=https://da-linux.digitalairlines.com/gw/webacc" />

   <title>Redirecting to Secure GroupWise Webaccess</title>

   </head>

   <body>

   This page is used to redirect to the Secure GroupWise Webaccess server. If your browser does not automatically redirect you in a few seconds, click here to go to the secure page.

   </body>

   </html>
4. **Save** and **Exit** the gedit application
5. Open FireFox and browse to **http://da-linux.digitalairlines.com**. You should see a web page flash and then get re-directed to the WebAccess Login Page.

   Notice it is now using a secure connection.

(End of Exercise)