IBM WEBSPHERE BUSINESS MONITOR V6.1- End-to-end security

## WebSphere Business Monitor V6.1

# End-to-end security with a federated repository (LDAP)

What this exercise is about
Lab requirements2
What you should be able to do2
Introduction2
LDAP information (reference)
User names used to complete the end-to-end security configuration3
Part 1: Installing and configuring Tivoli Directory Server V6.04
→ Creating a new Tivoli Directory Server Instance
→ Configuring IBM Tivoli Directory Server
Part 2: Securing the Portal Server with Tivoli Directory Server V6.0
→ Disable WebSphere Application Server and Portal security:
→ Enable WebSphere Portal Security with LDAP:
Part 3: Enable security for Monitor Server profile (WebSphere Application Server V6.1)
→Update J2C authentication data entries for messaging buses
Part 4: Enable security for WebSphere Process Server V6.161
→Update security role mappings for BPE container and task container76
→Update J2C authentication data entries for messaging buses80
Part 5: Configure Remote CEI server to use WebSphere Business Monitor in a secured environment
Part 6: Security configuration - After model deployment93
Troubleshooting:

## What this exercise is about

The objective of this lab is to show you how to setup end to end security for Monitor Server, Portal Server, and Process Server using a federated repository.

## Lab requirements

List of system and software required for the student to complete the lab.

- WebSphere Business Monitor V6.1 installed
- Tivoli Directory Server V6.0
- WebSphere Portal Server installed
- WebSphere Process Server installed

## What you should be able to do

At the end of this lab you should be able to:

- Install and configure Tivoli Directory Server
- Setup security for Portal Server, Monitor Server and Process Server

## Introduction

When you enable security, you are enabling administrative and application security settings. WebSphere Business Monitor uses many of the security mechanisms provided by the prerequisite products, including WebSphere® Application Server and WebSphere Portal.

For WebSphere Application Server, you must enable administrative and application security. For WebSphere Portal, you can enable security using the configuration wizard.

You can configure access to the monitor model resources using Monitor Data Security in the administrative console. For WebSphere Application Server instances that run the Business Monitor server including Web-based dashboards, you must configure them to use the federated repository, and not a local operating system, stand-alone LDAP registry, or stand-alone custom registry.

Note: If you are not using WebSphere Portal, you can use a file-based repository.

WebSphere Portal must be able to share a user registry with the Business Monitor server, meaning that only LDAP Server registry or custom user registry is supported.

Note: The WebSphere Portal database user registry cannot be used by and is not compatible with the Business Monitor server.

For this lab, you will create an LDAP registry using Tivoli Directory Server

## LDAP information (reference)

For reference, these are the LDAP values that were used for this lab. Use appropriate values for your environment.

Property	Parameter
LDAPHostName	IdlsIdap.austin.ibm.com
LDAPPort	389
LDAPAdminUId	cn=root
LDAPAdminPwd	Idapadmin
LDAPServerType	IBM Tivoli Directory Server V6.0
LDAPBindID	uid=wpsbind,cn=users,dc=ibm,dc=com
LDAPBindPassword	wpsbind
LDAPSuffix	dc=ibm,dc=com

## User names used to complete the end-to-end security configuration

To make it simple, very few users are used to complete the monitor end-to-end security configuration. The following table refers to the users used on different servers in the monitor domain.

Server	User Name	Password
Portal Server (Dashboard)	wpsadmin	wpsadmin
WebSphere Application Server V6.1 (Monitor Server)	was61admin	was61admin
Process Server (BPEL)	wpsrvadmin	wpsrvadmin

#### Reference: 1

dn: uid=wpsadmin,cn=users,dc=ibm,dc=com
objectclass: organizationalPerson
objectclass: top
objectclass: inetOrgPerson
uid: wpsadmin
userpassword: wpsadmin
sn: admin
givenName: wps
cn: wps admin
Reference: 2
dn: cn=wpsadmins,cn=groups,dc=ibm,dc=com
objectclass: groupOfUniqueNames
objectclass: top
uniquemember: uid=wpsadmin,cn=users,dc=ibm,dc=com
cn: wpsadmins

## Part 1: Installing and configuring Tivoli Directory Server V6.0

This part of the lab provides instructions on how to install and configure the Tivoli Directory Server V6.0.

\_\_\_\_\_1. Run the Tivoli Directory Server Launchpad by double clicking on setup.exe



\_\_\_2. Select **English** as the language to be used for this wizard

🔁 IBM Tivoli Directory Server 💶 🔲 🗙
Select a language to be used for this wizard.
English
<u>OK</u> <u>C</u> ancel

- \_\_\_\_\_ 3. Click **OK**
- 4. Read the instructions on the Tivoli Directory Server V6.0 Welcome panel

200	Welcome to the InstallShield Wizard for IBM Tivoli
	The InstallShield Wizard will install IBM Tivoli Directory Server 6.0 on your computer. To continue, choose Next. IBM Tivoli Directory Server 6.0
InstallShield	

#### \_\_\_\_5. Click Next

6. Read the License agreement and accept it

🛃 IBM Tivoli Directory S	erver 6.0 📃 🗌 🗙
115 18	Software License Agreement
1000	Please read the following license agreement carefully.
	International Program License Agreement 📃 🔺
	BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING THE PROGRAM YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,
14. 1.	- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, OR USE THE PROGRAM; AND
Rollin	- PROMPTLY RETURN THE PROGRAM AND PROOF OF ENTITLEMENT TO THE PARTY FROM WHOM YOU ACQUIRED IT TO OBTAIN A REFUND OF THE AMOUNT YOU PAID. IF YOU DOWNLOADED THE PROGRAM, CONTACT THE PARTY FROM
	I accept the terms in the license agreement
	C I do not accept the terms in the license agreement
InstallShield	
	< <u>B</u> ack <u>N</u> ext > <u>C</u> ancel

\_\_\_\_7. Click Next

8. In the following panel, accept the default **Directory Name** for the target install directory

😼 IBM Tivoli Directory S	ierver 6.0	_ 🗆 ×
	Click Next to install "IBM Tivoli Directory Server 6.0" to this directory, or cli install to a different directory. Directory:	ck Browse to
	C:\Program Files\IBM\LDAP\V6.0	Browse
InstallShield	< <u>B</u> ack Next >	<u>C</u> ancel

#### \_\_\_\_9. Click Next

\_\_\_\_\_ 10. In the following "Select the features to install" panel, accept the defaults (all features)

🕢 IBM Tivoli Directory Serv	ver 6.0	_ 🗆 X
200 00	Select the features to install:	
	Client SDK 6.0	
	🔽 Java Client 6.0	
	🔽 Web Administration Tool 6.0	
- 12 E	Proxy Server 6.0	
	🔽 Server 6.0 (Full Server Package)	
	🔽 embedded version of WebSphere Application Server - Express	
Carlos Carlos	☑ DB2 V8.2	
Le The	GSKit	
	Space required for C:\; 709 MB_Available: 71389 MB	
InstallOhiold		
	< <u>B</u> ack <u>N</u> ext > <u>C</u> a	ancel

## \_\_\_\_ 11. Click Next

- \_\_\_\_\_12. Enter the DB2 User ID and Password
  - \_\_\_\_a. User ID : db2admin
  - \_\_\_\_b. Password : db2admin
  - \_\_\_\_ c. Confirm Password : db2admin

🚱 IBM Tivoli Directory Se	erver 6.0	_ 🗆 🗙
	Enter the userid and password for the DB2 system id. If you are using an existing userid be sure your password is correct. User ID	1
	Password	
	Enter the password again to confirm	
	*****	
matanoment ,	< <u>B</u> ack <u>N</u> ext > <u>C</u> an	cel

### \_\_\_\_ 13. Click Next

## \_\_\_\_\_14. Review the installation **Summary**

😼 IBM Tivoli Directory Serv	/er 6.0	
	Installation has enough information to start copying files. Please review the settings below and if you wish to change any setting, click Back. If you are satisfied with the settings, click Next to begin copying files.	,
	IBM Tivoli Directory Server 6.0 will be installed to the following directory: C:\Program Files\IBM\LDAP\V6.0 The following features will be installed: Client SDK Java Client Web Administration Tool Proxy Server Server	•
InstallShield		
	< <u>B</u> ack <u>Next &gt;</u> <u>C</u> ar	ncel

#### \_\_\_\_\_ 15. Click Next

\_\_\_\_\_ 16. The installation progresses starting with DB2 as shown below:

😼 IBM Tivoli Directory S	erver 6.0
InstallShield -	Installing DB2. This background install may take up to 20 minutes, please wait.
	< <u>B</u> ack <u>N</u> ext > <u>C</u> ancel
BM Tivoli Directory S	Installing GSKit, please wait.
InstallShield	< <u>B</u> ack <u>N</u> ext ≻ <u>C</u> ancel
🛃 IBM Tivoli Directory S	erver 6.0
BM Tivoli Directory S	erver 6.0

🛃 IBM Tivoli Directory So	erver 6.0
	Installing embedded version of WebSphere Application Server - Express, please wait.
- m	
InstallShield	
	< <u>B</u> ack <u>N</u> ext > <u>C</u> ancel

\_\_\_\_ 17. Once the Installation is complete, the IBM Tivoli Directory Server instance Administration Tool is launched. You can close it at this point and launch it later.

8	BM Tivoli Directory Se	rver 6.	D				ĺ	- 🗆 ×
	2 6	Installation is now complete.						
		A confi	guration tool h	as been laui	nched. To use IB	M Tivoli Dire	ectory Server, you r	nust
	🚰 IBM Tivoli Director	y Serve	er Instance Ad	ministratior	n Tool		_ [	l ×
	Li <u>s</u> t of directory server in	stances	installed on the r	machine				
	Instance	Туре	Version	Description			Create	
							Edit TCP/IP settings	
							Delete	
1104							⊻iew	
W								
1	4					F		
	<u> </u>							
							se <u>He</u> lp	?
		1						
Ins	stalishield							
					< <u>B</u> ack	Next	≻ <u>F</u> inis	h

- 18. Click the Close button to quit the IBM Tivoli Directory Server Instance Administration Tool. Click the Yes button to confirm
- \_\_\_\_\_ 19. Click the **Finish** button to exit the Tivoli Directory Server V6.0 installation wizard

## → Creating a new Tivoli Directory Server Instance

In the part of the lab, you will create a Tivoli Directory Server instance and then configure it.

1. Launch the IBM Tivoli Directory Server Instance Administration Tool, from Start → Programs → IBM Tivoli Directory Server 6.0 → Instance Administration tool ( $\checkmark$  Instance Administration Tool)

🤣 IBM Tivoli Directory Server Instance Administration Tool 📃 📃 🗙								
List of directory server instances installed on the machine								
Instance	Туре	Version	Description	Create				
				Edit TCP/IP settings				
				Delete				
				⊻iew				
•				F				
				Close Help ?				

- \_\_\_\_ 2. Click the Create button
- \_\_\_\_3. The Create new directory server instance wizard is launched. Select the radio button next to Create a new directory server instance

🗲 Create new director	y server instance	
Create or migrate		
Create a new direct	tory server instance:	
◯ <u>M</u> igrate from a pre-	6.0 version of directory server	
Enter path of the bac	ed up files	
	Br <u>o</u> wse	
Help ?	< Back Next > Finish	Cancel

- \_\_\_\_\_4. Click Next
- 5. In the following **instance details** panel, enter the following information:
  - \_\_\_\_a. User name : idsldap
  - \_\_\_\_b. Install location : C (default)
  - \_\_\_\_ c. Encryption seed string : monitorserversecurity (Note : 13 chars or more)
  - \_\_\_\_d. Instance Description : Directory Server Instance for WebSphere Portal Server

💋 Create new directory	y server instance	
Instance details The directory server inst User name idsIdap	ance will be created in an existing system user account.	
Install location (at least 3	30 MB free)	
Encryption seed string		
Directory Server Instan	ce for WebSphere Portal Server	
J		
Help ?	< Back Next > Finish	<u>C</u> ancel
	Contractors with values in the range of 33 to 126 inclusive. It must be a minimum of 12 and a maximum of 1016 characters in length.	

#### \_\_\_\_6. Click Next

7. In the following DB2 instance details panel, select idsIdap as the DB2 instance name from the drop down list

🚰 Create new directory serve	r instance			
DB2 instance details				
Enter the details of the DB2 insta server instance. You may select instance name.	nce to be as: : an existing E	sociated with the n B2 instance or ent	ew directory er a new DB2	
DB2 instance name idsldap				
Note:				
<ol> <li>You cannot select a D</li> </ol>	B2 instance v	which is already as	sociated	
with another directory 2. The new DB2 instance system user account.	e name shoul	nce. d be same as an e>	kisting	
Help ?	< <u>B</u> ack	Next >	Finish	Cancel

- \_\_\_\_ 8. Click Next
- 9. Accept the defaults in the following **TCP/IP settings for multihomed** hosts panel

🗲 Create new director	y server instance			
TCP / IP settings for mult	ihomed hosts			
🔽 Listen on all configu	red IP addresses			
Select the specific IP ac	dresses to listen on			
9.3.75.95				
Help ?	< <u>B</u> ack	<u>N</u> ext >	Finish	Cancel

- \_\_\_\_ 10. Click Next
- \_\_\_\_\_ 11. In the following **TCP/IP ports settings** panel, accept the default port numbers

🗲 Create new directory server instance	_ 🗆 ×
TCP / IP port settings	
Enter port details	
Server port number	
389	
Server secure port number	
636	
Admin daemon port number	
3538	
Admin daemon secure port number	
3539	
Help ? < Back Next > Finish	Cancel

- \_\_\_\_ 12. Click Next
- \_\_\_\_\_13. In the following **Optional steps** panel, ensure the two check boxes are selected

🚰 Create new directory ser	ver instance			_ 🗆 🗡
Optional steps				
You can choose to configure or configure them later using t do not wish to carry out now.	admin DN / pass he idsxcfg tool.	word and databa Uncheck the step:	se now, s you	
Steps	password			
Configure <u>d</u> atabase				
Help ?	< <u>B</u> ack	<u>N</u> ext >	Finish	<u>C</u> ancel

- \_\_\_\_\_14. Click Next
- \_\_\_\_\_ 15. In the following **Configure administrator DN and password** panel, enter the following information:
  - \_\_\_\_a. Administrator DN : cn=root
  - \_\_\_\_b. Administrator password : Idapadmin
  - \_\_\_\_ c. Confirm password : Idapadmin

🗲 Create new directory server instance	
Configure administrator DN and password	
Administrator DN	
cn=root	
Administrator password	
*****	
Confirm password	
****	
Help ? < Back Next > Finish	Cancel

#### \_\_\_\_\_16. Click Next

- \_\_\_\_\_ 17. In the following **Configure database** panel, enter the following information:
  - \_\_\_\_a. Database user name : db2admin
  - \_\_\_\_b. Password : **db2admin**
  - \_\_\_ c. Database name : LDAPDB

🚰 Create new directory server instance			_ 🗆 🗙
Configure database			
Database user name			
db2admin			
Password			
*****			
Database name			
LDAPDB			
Help ? Sack	Next >	Finish	Cancel

- \_\_\_\_\_18. Click Next
- \_\_\_\_\_ 19. In the following **Database options** panel, complete the following instructions:
  - \_\_\_\_a. Select C drive as the Database install location
  - \_\_\_\_b. Select the radio button next to Create a universal DB2 database for the Character-set option

👉 Create new directory server instance	_ 🗆 🗙
Database options	
Database install location (at least 80 MB free)	
c 🔽	
Character-set option	
Create a universal DB2 database (UTF-8 / UCS-2)	
C Create a local codepage DB2 database	
<b>Note :</b> Create a universal DB2 database if you anticipate storing data from multiple character sets (recommended).	
Help ? < Back Next > Finish	Cancel

- \_\_\_\_ 20. Click Next
- \_\_\_\_\_ 21. Verify the settings in the following panel

🎽 Create new directory sei	ver instance			
Verify settings Verify that the settings below Click Finish to begin the instar	/ are correct. nce creation.			
The directory server instance The description will be set to The directory server instance The directory server instance The directory server instance The directory server instance Database instance 'idsIdap' v The directory server instance Database instance 'idsIdap' v The directory server instance Database instance 'idsIdap' v The directory server instance The database 'LDAPD ' will k The database will be created Database will be UTF-8.	e will be created : 'Directory Serve e will be configur e's port will be se e's secure port w e's Admin Daemo e's Admin Daemo vill be configured e admin DN will b be configured. Hat: 'C'.	at: 'C'. er Instance for W ed for IP 'All'. to '389'. vill be set to '636' n port will be set n secure port wi l. e set to 'cn=root'	'ebSphere Portal : to '3538'. Il be set to '3539'	Server'.
Help ?	< <u>B</u> ack	<u>N</u> ext >	Finish	Cancel

- \_\_\_\_\_ 22. Click the **Finish** button
- 23. Ensure the Directory Server Instance is successfully created

💋 Create new directo	ry server instance - Results		×
Start time	Elapsed time		
6/22/07 5:26 PM	0:1:33		
Task messages			
GLPCTL027I Created data	abase: 'LDAPDB'.		<b>A</b>
GLPCTL034I Updating the	e database: 'LDAPDB'		
GLPCTL035I Updated the	database: 'LDAPDB'		
GLPCTL020I Updating the	e database manager: 'idsldap'.		
GLPCTL021I Updated the	database manager: 'idsldap'.		
GLPCTL023I Enabling mul	ti-page file allocation: 'LDAPDB'		
GLPCTL024I Enabled mult	ti-page file allocation: 'LDAPDB'		
GLPCDB005I Configuring	database 'LDAPDB' for directory server instance: 'idsldap'.		
GLPCDB006I Configured	database 'LDAPDB' for directory server instance: 'idsldap'.		
GLPCDB003I Added data	base 'LDAPDB' to directory server instance: 'idsldap'.		-
•			▶
		Close	H <u>e</u> lp ?

\_\_\_\_\_24. Click the Close button

ſ	👉 IBM Tivoli Director	y Serv	er Instance	Administration Tool		
I	Li <u>s</u> t of directory server in	stances	installed on t	he machine		
	Instance	Туре	Version	Description		Create
	idsldap		6.0	asdasdas		
						Edit TCP/IP settings
						Delete
						<u>⊻</u> iew
	•					
					Cle	ose Help ?

25. Close the IBM Tivoli Directory Server instance Administration Tool

## → Configuring IBM Tivoli Directory Server

- \_\_\_\_\_1. To configure the directory server with Portal users, you will import the LDIF file.
  - \_\_\_\_a. Open a command line window and change the directory to C:\Program Files\IBM\LDAP\V6.0\bin
  - \_\_\_\_b. Run the idsxcfg command to open the IBM Tivoli Directory Server Configuration Tool

📾 C:\WINDOWS\system32\cmd.exe - idsxcfg	<u>- 0 ×</u>
Microsoft Windows [Version 5.2.3790] (C) Copyright 1985-2003 Microsoft Corp.	
C:\Documents and Settings\Administrator>cd C:\Program Files\IBM\LDAP\V6.0\bi	.n
C:\Program Files\IBM\LDAP\V6.0\bin>idsxcfg (-> SHOW_TOOLBAR (-> TEXT_BOTTOM (+> NO_TEXT (-> TASKPAD -	

- \_\_\_\_ c. In the configuration Tool, click **Manage suffixes** in the task list on the left pane. The **Manage suffixes** window opens in the Right pane
- \_\_\_\_d. In the Manage Suffixes window, type dc=ibm,dc=com in the Suffix DN field and click the Add button

🚰 IBM Tivoli Directory Server Configuration Tool	
<u>F</u> ile <u>H</u> elp	<u>@</u>
Choose a task: Introduction Administrator DN/password Configure database Configure database Configure.unconfigure changelog Manage suffixes Manage schema files Manage schema files Current suffix DNs Current suffix DNs Current suffix DNs Current suffix database Packup database	Add <u>R</u> emove

**Note:** When you click the **Add** button, the suffix is added to the list in the **Current suffix DNs** text box; however, the suffix is not actually added to the directory until you click **OK** 

🗲 IBM Tivoli Directory Server Configu	iration Tool	
<u>File H</u> elp		@
Choose a task: Introduction Administrator DN/password Configure database Unconfigure database Configure/unconfigure changelog Manage suffixes Manage schema files Import LDIF data Export LDIF data Backup database Restore database Optimize database	Manage suffixes Suffixes Suffix DN Current suffix DNs cn=localhost cn=pwdpolicy cn=ibmpolicies o=root organization dC=ibm, dc=com Note: Removing a suffix eliminates access to all direct that suffix; however, the data is not removed from the	Add <u>R</u> emove

- \_\_\_\_e. Click the **OK** button
- 2. To import the Portal users, complete the following instructions:
  - \_\_\_\_a. In the Configuration Tool, click **Import LDIF data** in the task list on the left pane. The **Import LDIF data** window opens in the Right pane
  - \_\_\_\_b. In the **Import LDIF data** window on the right, click the **Browse** button to locate the LDIF file that consists of the portal users
  - \_\_\_\_ c. Ensure the radio button next to Standard Import is selected

💋 IBM Tivoli Directory Server Confi	juration Tool		
<u>F</u> ile <u>H</u> elp			e
Choose a task: Overview Manage administrator DN Manage administrator password Configure database Unconfigure database Manage changelog Manage suffixes Manage schema files Manage schema files Export LDIF data Export LDIF data Backup database Optimize database	Import LDIF data Enter the path and name of the LD Note: Before importing an LDIF file Path and LDIF file name C: 'PortalUsers_final.ldif Remove trailing spaces in Sta Standard import Standard import C Data ver Schema ch but the data Warning: T Bulkload do of the data. the LDIF file	IF file (on the LDAP server) you must add the correspond a you must add the correspond add the correspond add the correspond add to the directory. For improve performance les not check the correctness . Run Data validation only on a before attempting bulkload.	from which you want to import directory data. ling suffixes in the Manage suffixes task. Browse Browse Bulkload Use bulkload for very large LDIF files. Bulkload options Enable schema checking Enable ACL checking Enable gassword policy
	Start time Elapse	ed time	<u>Cl</u> ear results Stop <u>Close</u> <u>Help</u> ?

- \_\_\_\_ d. Click the Import button
- \_\_\_\_e. Ensure that all the entries in the LDIF file are imported successfully as shown in the **Task Messages** text area and click the **Clear results** button

Task messages	
GLPCOM022I The database plugin is successfully loaded from C:/Program Files/IBM/LDAP/V6.	0/lib/libback-conf
GLPRDB002W ldif2db: 17 entries have been successfully added out of 17 attempted.	
<u> 1 </u>	
	Clear results

- \_\_\_\_f. Close the IBM Tivoli Directory Server Configuration Tool by selecting **File → Close** from the main menu. Click the **Yes** button to confirm
- 3. Start the Tivoli Directory Server. To start the IBM Tivoli Directory Server from the Windows Services by right clicking on "IBM Tivoli Directory Server"
- 4. The Configuration is complete

## Part 2: Securing the Portal Server with Tivoli Directory Server V6.0

If WebSphere Application Server global security is enabled, you must disable it before modifying your security configuration. By default the WebSphere Application Server Global Security and Portal Server security is enabled internally during the installation for security reasons. So before trying to enable LDAP security for Portal Server, the WebSphere Application Server global security and the Portal Security turned off.

The following are the steps to turn off WebSphere Application Server Global Security and disable WebSphere Portal security.

## → Disable WebSphere Application Server and Portal security:

The following steps must be completed on the machine designated for Portal Server:

- 1. Start the WebSphere Application Server (server1) and the WebSphere Portal Server (WebSphere\_Portal)
  - \_\_\_\_a. On the Portal Server machine, locate the **config/wizard** directory (C:\IBM\WebSphere\PortalServer\config\wizard)

🗁 C:\IBM\WebSphere\PortalServer\config\wizard				
Address 🛅 C:\IBM\WebS	phere\PortalServer\config\wizard	💌 🄁 Go		
<ul> <li>cfgwiz.jar</li> <li>configwizard400.bat</li> <li>configwizard.bat</li> <li>configwizard.sh</li> <li>dpicfg.nsf</li> <li>dpiwiz.bat</li> </ul>	dpiwiz.sh ⊉ DPIWizard.jar g parent_ascii.properties			

- \_\_\_\_b. Double click the configwizard.bat to launch the Portal Server Configuration Wizard
- \_\_\_\_ c. Select **English** as language

🕀 InstallShield Wizard	_ 🗆 🗙
Select a language to be use	d for this wizard.
English	-
<u>OK</u>	Cancel

\_\_\_\_ d. Click **OK**. The Configuration Wizard is launched

WebSphere Portal Configuration V WebSphere Portal	Vizard			IBM.
Welcome to the conf This wizard will run advanced We To access information about this	iguration wizard for We bSphere Portal configuration tasks of product, choose Launch Information	<b>bSphere Portal</b> n your computer. Center.	6.0.1	****
Choose Next to continue.				A
Help		< <u>B</u> ack	Next >	<u>C</u> ancel

\_\_\_\_e. Click Next over the Welcome Screen

\_\_\_\_f. In the following panel, select the radio button next to Disable Security

bSphere Portal Configuration Wizard		
WebSphere Portal		Į.
Select the task that you want to perform.		
💿 Disable security <		
C Enable LDAP security		
C Transfer data to another database		
C Connect additional node to database		
IlShield		
elp	< Back Next > Ca	ncel

## \_\_\_g. Click Next

\_\_\_h. In the following panel, enter the WebSphere Application Server User ID and Password

- User ID : was602admin
- Password : was602admin

ebSphere Portal Configuration Wizard	
WebSphere Portal	TEM
Specify the administrator ID and password for the WebSphere Application Server. Username:	
was602admin Password:	
*****	

\_\_\_ i. Click Next

# \_\_\_\_ j. On a successful validation of the WebSphere Application Server, User and password, provide the disable\_security helper file. This file is located at ORTAL\_HOMEORTAL\_HOMEORTAL\_HOMEORTAL\_HOME

By default <PORTAL\_HOME> is C:\IBM\WebSphere\PortalServer

Please enter you wish to u button on the	an appropriate proper se for this session. Fo lower left corner of this	ties file location for th or additional informatio s panel.	e properties file on click the 'Help'	-
C:\IBMWebS	per me location. phere\PortalServer\cor	nfig\helpers\security_	disable.properties	
			Browse	

## \_\_\_ k. Click Next

- \_\_\_ I. In the following panel, enter the following values
  - WebSphere Portal Administrator ID : wpsadmin

- Password : wpsadmin
- Confirm Password : wpsadmin
- WebSphere Portal administrator group : <Accept the default >
- Member Manager password : <Accept the default>

WebSphere Portal administrator ID:	
wpsadmin	
Password:	
*****	
Confirm password:	
*****	
WebSphere Portal administrator group:	
<portaladmingroupid></portaladmingroupid>	
Member Manager password:	
+++++++++++++++++++++++++++++++++++++++	

\_\_ m. Click Next

\_\_\_\_n. Review the Summary

WebSphere Portal Configuration Wizard		
WebSphere Portal		IBM.
The wizard is ready to run the following task:		
Disable security		
Click Next to continue.		
tallShield		
Help	< <u>B</u> ack	<u>Next&gt;</u>

- \_\_\_o. Click Next
- \_\_\_\_p. The **Disable Security** task progresses. Monitor the configuration log file for any failure messages. The configuration log file is located at **<WPS\_HOME>\logs\ConfigTrace.log**

VebSphere Portal	inguration wizaru		IEN
Punning task: Dis:	able security		 R
Logging to C:\IBM\\ Open	WebSphere\PortalServer	1log\configwizard.log	
	39%		-
allShield		1	

The task completed succes	efully	
Disable security	Sidily.	T
For additional information, r C:\IBM\WVEBSPH~1\PORTAL	efer to the log file _~1\log\disable-security.log.	
View Log F	file	
To perform additional tasks	for WebSphere Portal, choose Run Wizard Again.	
Run Wizard /	Again	
To exit the wizard, choose F	inish.	

- \_\_\_\_\_ 2. Click Finish
- 3. You have now disabled the WebSphere Application Server security and Portal Server security

## → Enable WebSphere Portal Security with LDAP:

- 4. Start the WebSphere Application Server (server1) and the WebSphere Portal Server (WebSphere\_Portal)
- 5. On the Portal Server machine, locate the **config/wizard** directory (C:\IBM\WebSphere\PortalServer\config\wizard)

🚞 C:\IBM\WebSphere\F	PortalServer\config\wizard	
Address 🛅 C:\IBM\WebS	ohere\PortalServer\config\wizard	💌 🄁 Go
🔋 cfgwiz.jar	🖬 dpiwiz.sh	
👅 configwizard400.bat	🔋 DPIWizard.jar	
configwizard.bat	🖪 parent_ascii.properties	
🔟 configwizard.sh		
🚾 dpicfg.nsf		
👅 dpiwiz. bat		

- 6. Double click the **configwizard.bat** to launch the Portal Server Configuration Wizard
- \_\_\_\_\_7. Select English as language and click OK
- 8. Click **Next** over the Welcome Screen
- 9. In the following panel, select the option, **Enable LDAP Security**

Select the	task that you want to p	perform.		
C Disat	ole security			
📀 Enab	le LDAP security <			
O Trans	sfer data to another da	itabase		
C Conn	ect additional node to	database	100	F

#### \_\_\_\_\_ 10. Click Next

#### \_\_\_\_\_ 11. Select the LDAP type as IBM Directory Server

	ne) (
T	:::
in the second second	

#### \_\_\_\_12. Click Next

\_\_\_\_\_ 13. In the following panel, specify the LDAP settings to connect WebSphere Portal to LDAP server:

\_\_\_\_a. Host name : <fully qualified LDAP sever host name>

Example: idsldap.austin.ibm.com

\_\_\_\_b. Port : **389** 

- \_\_\_\_ c. User name : cn=root
- \_\_\_\_d. Password : Idapadmin
- \_\_\_\_e. LDAP suffix : dc=ibm,dc=com

pecify the LDAP settings to co he LDAP server.	onnect WebSphere Porta	al to	1	
Host name:			1	
idsIdap.austin.ibm.com				
Port:				
389				
User name:				
cn=root				
Password:				
******			-	E
LDAP suffix:				100
dc=ibm,dc=com				

- \_\_\_\_\_ 14. Click Next
- 15. In the following panel, specify the LDAP user settings for authenticating with the WebSphere Application Server and Portal Server:
  - \_\_\_a. WebSphere Portal administrator ID : uid=wpsadmin,cn=users,dc=ibm,dc=com
  - \_\_\_\_b. Password : wpsadmin
  - \_\_\_\_c. WebSphere Application Server administrator ID: uid=was602admin,cn=users,dc=ibm,dc=com
  - \_\_\_\_d. Password : was602admin
  - \_\_\_\_e. Bind Distinguished name : uid=wpsbind,cn=users,dc=ibm,dc=com
  - \_\_\_f. Password : wpsbind
  - \_\_\_\_g. User search filter : < Depends on your environment >

pecify the LDAP user settings for authenticating with t	he servers.		1
WebSphere Portal administrator ID:			
uid=wpsadmin,cn=users,dc=ibm,dc=com			
Password:			
*****			
WebSphere Application Server administrator ID:			00
uid=was602admin,cn=users,dc=ibm,dc=com			A COLUMN T
Password:		19	
*******			
Bind dinstinguished name:			
uid=wpsbind,cn=users,dc=ibm,dc=com			
Password:		100	1 den
******			
User search filter:			-
User search filter:			

#### \_\_\_\_ 16. Click Next

\_\_\_\_\_ 17. In the following panel, specify the LDAP group settings for authenticating with the server:

\_\_\_\_a. WebSphere Portal administrator group : cn=wpsadmins,cn=groups,dc=ibm,dc=com

\_\_\_\_b. Web Content Management administrators group : cn=wpsadmins,cn=groups,dc=ibm,dc=com

- \_\_\_\_ c. Portal Server content administrators group : cn=wpsadmins,cn=groups,dc=ibm,dc=com
- \_\_\_\_d. Portal Server document reviewer group : cn=wpsadmins,cn=groups,dc=ibm,dc=com
- \_\_\_\_e. Group search filter : <Depends on your environment>

Note: To make it simple only one group, wpsadmins, is being used for all the Portal groups.

pecify the LDAP group settings for authenticating with the servers.	1	
WebSphere Portal administrator group:		
cn=wpsadmins,cn=groups,dc=ibm,dc=com		
Web Content Management administrators group:		
cn=wpsadmins,cn=groups,dc=ibm,dc=com		
WebSphere Portal Server content administrators group:		
cn=wpsadmins,cn=groups,dc=ibm,dc=com		
WebSphere Portal Server document reviewer group:		
cn=wpsadmins,cn=groups,dc=ibm,dc=com		
Group search filter:	100	10
(&(cn=%v)(objectclass=groupOfUniqueNames))		free -

## \_\_\_\_ 18. Click Next

\_\_\_\_\_ 19. In the following panel, specify the short names for the groups used in Web Content Management:

\_\_\_\_a. Web Content Management administrators group : wpsadmins

\_\_\_b. WebSphere Portal Server content administrators group : wpsadmins

\_\_\_ c. Portal Server document reviewer group : wpsadmins

ebSphere Portal Configuration Wizard		
WebSphere Portal		IBW
Specify the short names for these groups used in Web Content M	anagement	+
Web Content Management administrators group:		
wpsadmins		
WebSphere Portal Server content administrators group:		
wpsadmins		
WebSphere Portal server document reviewer group:		le l
wpsadmins		10
		THE OTHER DESIGN
telp	< Back	Next > Cance

#### 20. Click Next

\_\_\_\_\_ 21. In the following panel, specify the LDAP prefixes and suffixes:

- \_\_\_a. User prefix : uid
- \_\_\_b. User suffix : cn=users
- \_\_\_\_ c. Group prefix : cn
- \_\_\_\_d. Group suffix : cn=groups

Poltai			
pecify the LDAP prefixes and suffixes.		~	
User prefix:			
uid			
User suffix:			
cn=users			
Group prefix:			
cn			
Group suffix:			
cn=groups			

- 22. Click Next
- \_\_\_\_\_ 23. In the following panel, specify the single sign-on settings:
  - \_\_\_\_a. The domain name for all the single sign-on hosts : ibm.com
  - \_\_\_\_b. Does single sign-on require an SSL connection? : No
  - \_\_\_\_ c. Enter a password that will be used to encrypt LTPA keys : password
  - \_\_\_\_d. Confirm password : password
  - \_\_\_\_e. LTPA token expiration time in minutes : 120

pecify the following single sign-on settings.		20
The domain name for all allowed single sign-on h	osts:	
ibm.com		
Does single sign-on require an SSL connection?		
C Yes		
© No		
Enter a password that will be used to encrypt LTP	A keys:	
********		
Confirm password:		
******		
LTPA token expiration time in minutes:		
120		

## \_\_\_\_\_ 24. Click Next

\_\_\_\_\_ 25. In the following panel, accept the default parameters or specify the parameters as per your environment:

pecify the LDAP nodes settings for users and groups in this configuration.	
User object class:	TAN
inetOrgPerson	
Group object class:	
groupOfUniqueNames	
Group membership attribute:	
uniqueMember	
User base attributes:	
givenName,sn,preferredLanguage	
Minimum user attributes:	
	100
Minimum group attributes:	

### \_\_\_\_ 26. Click Next

\_\_\_\_\_ 27. In the following 'Additional LDAP settings' panel, accept the defaults:

dditional LDAP settings.		
Allow only qualified user nar	nes within the security domain?	
C Yes		1
No		
Issue a warning if an applic: policy file? • Yes	ation is installed with a permissior that is disallowed by the	
C No		
Security cache timeout in se	conds:	
600		
Authentication protocol for R	MI/IIOP requests:	
вотн	•	1 days

- \_\_\_\_\_ 28. Click Next
  - \_\_\_\_29. In the following panel, accept the defaults:

WebSphere Portal			IEN
dditional LDAP settings continued			
Host name of the web server handling HTTP requests:			
LDAP server response timeout in seconds:			
120			
Reuse LDAP connections?			
€ Yes			
C No			
Ignore case when checking user names and passwords?			
Yes			
C. No			
Enable Lookaside?		1	
O Yes			
No     No			
allShield		8	
elp	< <u>B</u> ack	Next >	<u>C</u> ance

### \_\_\_\_\_ 30. Click Next

\_\_\_\_\_ 31. In the following panel, review the summary:

Enable LDAP security with these configuration settings:		-	
LDAP Type:	IBM Directory Server		
Host name: Port:	portaldash.austin.ibm.com 389		
User name: LDAP suffix:	cn=root dc≕ibm,dc=com		
WebSphere Portal administrator ID:	uid=wpsadmin,cn=users,dc=ibm,dc=com	-	A

#### \_\_\_\_\_ 32. Click Next

33. The **Enable LDAP** task progresses. Monitor the logs for any failure messages. The configuration log is located at **<PORTAL\_HOME>\log\ConfigTrace.log** 

ebSphere Portal Configuration Wizard	
WebSphere Portal	IBM
The task completed successfully.	-
Enable LDAP security	
For additional information, refer to the log file C:\IBMWVEBSPH~1\PORTAL~1\log \enable-Idap-security.log.	
View Log File	
To perform additional tasks for WebSphere Portal, choose Run Wizard Again.	
Run Wizard Again	
To exit the wizard, choose Finish.	
allShield	
elp < Ba	ck Next > Einish

- \_\_\_\_ 34. Once the Security configuration is complete, click **Finish**
- 35. Restart the Portal Server and review the System Out log file and ensure the server is started successfully
- \_\_\_\_ 36. The Enable Security Task for Portal sever with Tivoli Directory Server is complete
  - \_\_ 37. Export LTPA key file. You will be importing the exported key file across all the servers in the monitor domain
    - \_\_\_\_a. Launch the WebSphere Application Server admin console for the wp\_profile: https://hostname:10039/ibm/console
    - b. Login to the administrative console using the user name and password (was602admin and was602admin)
    - \_\_\_ c. In the left navigation pane of the administrative console, expand 'Security' and click the 'Global security' link

B	Security
	Global security <del>«Cont</del>
	SSL

\_\_\_\_\_d. In the following panel, expand 'Authentication mechanisms' under the 'Authentication' category and click the 'LTPA' link



\_\_\_\_e. In the following 'LTPA' panel, enter the 'Key file name' (Example: C:\securePortal.key)

eneral Properties	
	Additional Properties
Password	Single signon (SSO)
Confirm password	Trust association
•••••	
Timeout	
120	

\_\_\_\_f. Click the 'Export Keys' button. This action exports a key file to the specified location

\_\_\_\_g. Click the Save link, to save the configuration



- \_\_\_h. Click the Save button
- 38. Close the administrative console
# Part 3: Enable security for Monitor Server profile (WebSphere Application Server V6.1)

In this part of the lab, you will enable the LDAP security for Monitor Server which includes Web-based Dashboard and REST Server. In this process, you will configure WebSphere Application Server V6.1 to use LDAP in a federated repository.

#### Prerequisite:-

Copy the **securePortal.key** file that you have exported to a temporary location on to the Monitor Server machine

Complete the following instructions to enable LDAP security for the WebSphere Application Server, which is the Monitor Server profile

- 1. Start the monitor server profile and launch the administrative console
- 2. Login to the administrative console using the user name and password if the default security is enabled
- 3. In the administrative console's left navigation pane, expand 'Security' and click the 'Secure administration, applications and infrastructure' link

View: All tasks					
Welcome					
🗄 Guided Activities					
🖂 Security					
Secure administration, applications, j and infrastructure					
SSL certificate and key management					
Bus Security					
Monitor Data Security					

\_\_\_ 4. In the following 'Secure administration, applications and infrastructure' panel to the left, click the 'Security Configuration Wizard' button

Security Configuration Wizard Security Conf	iguration Report
Administrative security <ul> <li>Administrative User Roles</li> <li>Administrative Group Roles</li> </ul>	Authentication □ Use domain-qualified user name Web security
Application security Enable application security	<ul> <li>■ RMI/IIOP security</li> <li>■ Java Authentication and Authoriza</li> </ul>
Java 2 security           Java 2 security           Use Java 2 security to restrict application access to local resources	Authentication mechanisms and expir
<ul><li>Warn if applications are granted custom permissions</li><li>Restrict access to resource authentication data</li></ul>	<ul> <li><u>External authorization providers</u></li> <li><u>Custom properties</u></li> </ul>
User account repository Current realm definition	
Federated repositories Available realm definitions	

5. In the following 'Step1: Specify extent of protection' panel, ensure the check box for 'Enable application security' is selected



- \_\_\_\_6. Click Next
- \_\_\_\_7. In the following 'Step2: Select user repository' panel, ensure the radio button for 'Federated repositories' is selected



8. Click Next

- 9. In the following 'Step 3: Configure user repository' panel, enter the primary administrative user name and password
  - \_\_\_\_a. Primary administrative user name : was61admin
  - \_\_\_\_b. Password : was61admin
  - \_\_\_\_ c. Confirm password : was61admin

Co	onfigure security ? -						
	Sec	ure the application ser	ving environment				
	Step 1: Specify extent of protection		Configure user repository				
	→	Step 2: Select user repository Step 3: Configure user repository Step 4: Summary	A secure, file-based user repository is built into the system for storing administrative users or environments with a small number of users. The file-based user repository can be federated with one or more external LDAP repositories. If this is the first time security has been enabled using this repository, provide a new user name and password to act as an administrator. If security was previously enabled using this repository, provide the name of a user with administrator privileges that is in the built-in repository.				
			Note: Use this panel to configure a federated repository with a built-in, file-based repository in the realm. To configure a federated repository with a non file-based repository in the realm, you must use the User accounts repository section on the Secure administration, applications, and infrastructure panel. * Primary administrative user name was61admin Password ••••••••••••••••••••••••••••••••••••				
	Previous Next Cancel						

- \_\_\_\_\_ 10. Click Next
- \_\_\_\_\_ 11. In the following 'Step 4: Summary' panel, review the summary information



- 12. Click Finish. You will see the following 'Secure administration, applications and infrastructure' panel
  - \_\_\_\_a. Select 'Federated repositories' from the drop down list for the 'Available realm definitions'

onfiguration	
Security Configuration Wizard Security Confi	guration Report
Administrative security       Administrative User Roles         Image: Security Security       Administrative Group Roles	Authentication Use domain-qualified user names Web security
Application security	<ul> <li>RMI/IIOP security</li> <li>Java Authentication and Authorization</li> </ul>
Java 2 security ☐ Use Java 2 security to restrict application access to local resources ₩ Warn if applications are granted custom permissions ■ Restrict access to resource authentication data	<ul> <li><u>External authorization providers</u></li> <li><u>Custom properties</u></li> </ul>
User account repository Current realm definition Federated repositories Available realm definitions Federated repositories	

\_\_\_\_ 13. Click the **Configure** button

- 14. In the following '**Configuration**' panel for '**Federated repositories**', enter the following under the '**General Properties**' category
  - \_\_\_\_a. Realm name : <fully qualified LDAP server host name>: <LDAP Port>
    - : Example: idsldap.austin.ibm.com:389

**Note:** The realm name for Portal is typically the fully qualified LDAP hostname:portNumber (example: "idsldap.austin.ibm.com:389") to verify this, you can open C:\ WebSphere\profiles\wp\_profile\config\cells\<your-cell-name>\security.xml and look for <userRegistries xmi:type="security:LDAPUserRegistry" .... – there is a "realm=" entry on that line

### \_\_\_\_b. Primary administrative user name : was61admin

General Properties						
* Realm name						
idsIdap.austin.ibm.com: 389						
* Primary administrative user name						
was61a	was61admin 🧲					
Server u	ser identity					
• Aut	omatically generated server ider	ntity				
O Ser	ver identity that is stored in the	repo	sitory			
Se	rver user ID or administrative us	er o	n a Version 6.0.x node			
Pa	ssword					
V Ion	ore case for authorization					
Reposit	tories in the realm:					
	Add Base entry to Realm	٦	Use built-in renosi	tory	Remove	
					i	
Select	Base entry	Rep	oository identifier	Reposito	ry type	
	o=defaultWIMFileBasedRealm	Inte	ernalFileRepository	File		
Additional Properties Related Items						
= <u>P</u>	roperty extension repository		= <u>Mana</u>	<u>le reposito</u>	ories	
= <u>E</u>	Entry mapping repository					
= <u>s</u>	Supported entity types					

15. Scroll down and click the 'Add Base entry to Realm' button. This action opens the 'Repository reference' panel as shown below:

Secure administration, applications, and infrastructure ? =					
<u>Secure administration, applications, and infrastructure</u> > <u>Federated repositories</u> > Repository reference					
Specifies a set of identity entries in a repository that are referenced by a base entry into the directory information tree. If multiple repositories are included in the same realm, it might be necessary to define an additional distinguished name that uniquely identifies this set of entries within the realm.					
Configuration					
General Properties					
* Repository none defined - Add Repository					
* Distinguished name of a base entry that uniquely identifies this set of entries in the realm					
Distinguished name of a base entry in this repository					
Apply OK Reset Cancel					

\_\_\_\_\_ 16. Click the 'Add Repository' button

\_\_\_\_\_ 17. In the following new repository reference panel, enter the following:

\_\_\_\_a. Repository identifier : LDAP-idsIdap (Any meaningful identifier)

\_\_\_\_b. LDAP Server

• Directory Type : IBM Tivoli Directory Server V6.0

• Primary host name : idsldap.austin.ibm.com

• Port : 389

\_\_\_ c. Security

- Bind distinguished name : uid=wpsbind,cn=users,dc=ibm,dc=com
- Bind password : wpsbind
- Login properties : uid
- Certificate mapping : Select 'EXACT\_DN' from the drop down list

#### **General Properties**

I DAR-idaldan		
EDAP-Idsidap		
LDAP server	Security	
* Directory type	Bind distinguished name	
IBM Tivoli Directory Server Version 6	uid=wpsbind,cn=users,dc=ibr	
* Primary bost pame Port	Bind password	
idsldap.austin.ibm.com 389	•••••	
	Login properties	
Failover server used when primary is not available:	uid	
Delete	Certificate mapping	
Select Failover host name Port	EXACT_DN 💽	
None	Certificate filter	
Add		
	Require SSL communications	
Support referrals to other LDAP servers		
ignore 👻	Centrally managed	
	Manage endpoint security configurations	
	Use specific SSL alias	
	NodeDefaultSSI Settings	

- \_\_\_\_\_18. Click OK. You will be back to the 'Repository reference' panel again
- \_\_\_\_\_ 19. In the 'Repository Reference' panel, enter the following:
  - \_\_\_\_a. Repository : Select 'LDAP-idsIdap' from the drop down list
  - \_\_\_\_b. Distinguished names of a base entry that uniquely identifies this set of entries in the realm : dc=ibm,dc=com
  - \_\_\_\_ c. Distinguished name of a base entry in this repository : dc=ibm,dc=com

LDAP-idsldap 🗸	Add Repository
<ul> <li>Distinguished name entries in the realm</li> </ul>	of a base entry that uniquely identifies this set
dc=ibm,dc=com	
dc=ibm,dc=com Distinguished name dc=ibm,dc=com	of a base entry in this repository

- \_\_\_\_ 20. Click **OK**
- 21. The '**Federated repositories**' panel should look like the picture shown below:

G	General Properties					
*	Realm	name				
	idsldap	austin.ibm.com:389				
*	Primary was61a	administrative user name dmin				
	Server us	er identity				
	🛈 Auto	matically generated server ide	ntity			
	O Serv	er identity that is stored in the	repo	sitory		
	Ser	ver user ID or administrative u	ser o	n a Version 6.0.x node		
	Pas	sword				
	<b>V</b>					
	I⊻I Igno	ore case for authorization				
	Repositories in the realm:					
		Add Base entry to Realm		Use built-in reposi	itory	Remove
	Select	Base entry	Rep	oository identifier	Reposito	ry type
		dc=ibm,dc=com	LDAP	-idsldap	LDAP:IDS	6
		o=defaultWIMFileBasedRealm	Int	ernalFileRepository	File	

22. Select the check box for 'o=defaultWIMFIleBasedRealm' if it is existing (it exists if the default security is enabled) and click the **Remove** button.

Seneral Properties  * Realm name idsIdap.austin.ibm.com:389					
* Primary administrative user name was61admin					
Server user identity					
• Automatically generated server	r identity	,			
O Server identity that is stored in the repository Server user ID or administrative user on a Version 6.0.x node Password					
Ignore case for authorization Repositories in the realm:					
Add Base entry to Realm Use built-in repository Remove					
Select Base entry Repository identifier Repository type					
dc=ibm,dc=com	LDAP	-idsldap	LDAP:IDS	6	

- 23. Configuring supported entity types in a federated repository configuration
  - \_\_\_a. In the Federated Repositories panel, click the 'Supported entity types' under the 'Additional Properties' section

Repositories in the realm:							
	Add Base entry to Realm	Use built-in repo	sitory Remove				
Select	Base entry	Repository identifier	Repository type				
	<u>dc=ibm,dc=com</u>	LDAP-idsldap	LDAP:IDS6				
Additio	nal Properties	Related It	tems				
= <u>P</u>	roperty extension repository	= <u>Man</u>	age repositories				
= <u>E</u>	ntry mapping repository						

\_\_\_\_b. In the 'Supported entity types' panel, update the 'Base entry for default parent' values for Group, OrgContainer and PersonAccount with 'dc=ibm,dc=com' and accept the defaults for the 'Relative Distinguished Name properties'. The 'Supported entity types' panel should look like the picture below:

Supported entity types

ecure administration, applications, and infrastructure ? =							
<u>Secure administration, applications, and infrastructure</u> > <u>Federated repositories</u> > Supported entity types							
Use this page to configure entity types that are supported by the member repositories.							
	Preferences						
***							
Entity type 🛟	Base entry for the default parent $\diamondsuit$	Relative Distinguished Name properties $\diamondsuit$					
Group	dc=ibm,dc=com	cn					
OrgContainer dc=ibm,dc=com o;ou;dc;cn							
PersonAccount dc=ibm,dc=com uid							
Total 3							

- \_\_\_\_ c. Save to the master configuration
- 24. Configure the LDAP entity types
  - \_\_\_\_a. While you are in the 'Federated repositories' panel (Secure administration, applications and infrastructure → Federated repositories), click the 'Repository identifier' link, (Example:-LDAP-idsIdap)

Repositories in the realm:

	Add Base entry to Realm		Use built-in repo	sitory Remove
Select	Base entry	Repo	sitory identifier	Repository type
	<u>dc=ibm,dc=com</u>	LDAP-	idsIdap	LDAP:IDS6

b. In the following panel, scroll to the bottom and click the 'LDAP entity types' link under the 'Additional Properties' section

Addi	tional Properties
	Performance
	LDAP entity types

- Group attribute definition
- \_\_\_\_ c. In the following 'LDAP entity types' panel, update the following for the Group, OrgContainer and PersonAccount entity types:

#### 1) Group

- Object classes : groupOfUniqueNames
- Search bases : dc=ibm,dc=com
- Search filter : (objectclass=groupOfUniqueNames)

#### 2) OrgContainer

- <Accept the defaults>
- 3) PersonAccount

- Object classes : person
- Search bases : dc=ibm,dc=com
- Search filter : (objectclass=person)

2) The 'LDAP entity' panel will look like the picture below:

Secure administration, applications, and	infrastructure ? =
<u>Secure administration, applications, a LDAP-idsldap</u> > LDAP entity types	and infrastructure > <u>Federated repositories</u> >
Use this page to list entity types that select an entity type to view or chang	are supported by the member repositories or to e its configuration properties.
Entity type 🗢	Object classes 🗘
Group	groupOfUniqueNames
<u>OrgContainer</u>	organization;organizationalUnit;domain;container
PersonAccount	person
Total 3	

- \_\_\_\_b. Save to the master configuration
- 25. Configure group attribute definition
  - \_\_\_\_a. While you are in the 'Federated repositories' panel (Secure administration, applications and infrastructure → Federated repositories), click the 'Repository identifier' link, (Example:-LDAP-idsIdap)

Repositories in the realm:

	Add Base entry to Realm		Use built-in repo	sitory	Remove
Select	Base entry	Repo	sitory identifier	Repository	/ type
	<u>dc=ibm,dc=com</u>	LDAP	-idsldap	LDAP:IDS6	5

\_ b. In the following panel, scroll to the bottom and click the '**Group attribute definition**' link under the '**Additional Properties**' section

Additional Properties	
Performance	
LDAP entity types	
🗉 Group attribute definition 🗲	

- \_\_\_\_ c. In the following 'Group attribute definition' panel, enter the following information:
  - Name of group membership attribute : LDAP-AllGroups
  - For the scope, select the check box for 'All- Contains all direct, nested and dynamic members'

Configuration	
General Properties          Name of group membership attribute         LDAP-AllGroups	Additional Properties
Scope of group membership attribute O Direct - Contains only immediate members of the group without members of subgroups O Nested - Contains direct members and members nested within subgroups of this group O All - Contains all direct, nested, and dynamic members	attributes
Apply OK Reset Cancel	

• Click Apply

\_\_\_\_d. While you are in the 'Group attribute definition' panel, click the 'Member attributes' link under 'Additional properties' section

Secu	ure ad	ministration, applications, and	infrastructure	? -
5	ecure <u>Grou</u>	<u>administration, applications, a pattribute definition</u> > Membe	and infrastructure > <u>Federated</u> er attributes	repositories > <u>LDAP-idsldap</u>
ι	Jse thi	s page to manage Lightweight	Directory Access Protocol (LDAP	) member attributes.
Œ	] Pref	erences		
	New	Delete		
		ð # \$		
s	Select	Name 🛟	Scope 🗘	Object class 🗘
		member	all	groupOfNames
	Total	2		

\_\_\_\_e. In the following panel, click the **New** button to create a new member attribute

- \_\_\_\_f. In the following panel, enter the following information:
  - Name of member attribute : uniqueMember
  - Object class : groupOfUniqueNames
  - For the scope, select the check box for 'All- Contains all direct, nested and dynamic members'

inquententeer	
bject class	
groupOfUniqueName	25
<b>Cope</b> O Direct - Contains	only immediate members of the group without members of subgroups
🗘 Nested - Contains	s direct members and members nested within subgroups of this group

- Click OK
- \_\_\_\_g. Save to the master configuration
- \_\_\_\_\_ 26. Configure 'Single Sign-on'
  - \_\_\_\_a. Navigate to the 'Secure administration, applications and infrastructure' panel, expand 'Web Security' under the 'Authentication' category

	all searcheses
A	utientication
	Use domain-qualified user names
Ð	Web security
	General settings
	🗉 <u>single sign-on (SSO)</u> 🛛 🗲 🛶 🛶
	Trust association
Ŧ	RMI/IIOP security
Ŧ	Java Authentication and Authorization Ser
-	Authentication mechanisms and expiration

- \_\_\_\_b. Click the 'single sign-on (SSO)' link
- \_\_\_\_ c. In the following 'single sign-on (SSO)' panel, do the following:
  - Select the check box for 'Enabled'
  - Ensure the check box for 'Required SSL' is not selected
  - Domain name : ibm.com
  - Select the check box for 'Interoperability Mode'
  - Unselect the check box for 'Web bound security attribute propagation'

General Properties
🗹 Enabled
Requires SSL
Domain name
ibm.com
🗹 Interoperability Mode <
Web inbound security attribute propagation
Apply OK Reset Cancel

- 27. Click OK. You will be directed to the 'Secure administration, applications and infrastructure' panel again
- 28. While you are in the 'Secure administration, applications and infrastructure' panel, click the 'Authentication mechanisms and expiration' link

- A	uthentication
Γ	Use domain-qualified user names
Ð	Web security
Ŧ	RMI/IIOP security
Ŧ	Java Authentication and Authorization Service
-(	Authentication mechanisms and expiration

29. In the following 'Authentication mechanisms and expiration' panel, enter the following under the 'Cross-cell single sign-on' category to import the key file that you had exported on the portal (dashboard) server machine

**Note:** Enter the LTPA password that you specified when you Enabled LDAP Security for Portal, and enter the LTPA key file name that you specified near the end of the "LDAP Security for Portal" configuration.

- \_\_\_\_a. Password : password
- \_\_\_\_b. Confirm password : password
- \_\_\_\_ c. Fully Qualified Key file name : Example:- C:\KeyFile\securePortal.key

L GLOOD
Generate keys
set groups
ication expiration
ication information persists in the system for a limited amount of fore it expires and must be refreshed.
tication cache timeout
minutes 0 seconds
Il single sign-on ign-on across cells can be provided by sharing keys and rds. To share the keys and password, log on to one cell, specify a , and click Export keys. Then, log on to the other cell, specify the , and click Import keys.
ord
•••
m password
m password
m password •••• ualified key file name ufile) securePortal key

- \_\_\_\_\_ 30. Click the 'Import Keys' button
- \_\_\_\_\_ 31. Click the **Save** link, to save the configuration

Messages
The keys were successfully imported from the file C:\Keyfile\securePortal.key.
⚠ Changes have been made to your local configuration. You can:
<ul> <li><u>Save</u> directly to the master configuration.</li> <li><u>Review</u> changes before saving or discarding.</li> </ul>
$\Delta$ The server may need to be restarted for these changes to take effect.

\_\_\_\_\_ 32. Restart the server, launch the administrative console and log in using the user name and password

**Note:** To restart the server at this time, you should enter the old user name and password configured during the WebSphere Business Monitor server installation.

\_\_\_\_ 33. In the left navigation pane of the administrative console, expand 'Applications' and click the 'Enterprise Applications' link.

Integrate	ed Solutions Console	Welcome wasadmin
View:	All tasks	*
Welco	me	
🗄 Guide	d Activities	
E Serve	ers	
🖯 Appli	cations	
Er Er	iterprise Applications	
In In	stall New Application	
= M	onitor Models	
= Da	ata Movement Service	
🗄 Mo	nitor Action Manager	

\_\_\_\_ 34. In the following 'Enterprise Applications' panel, click the 'AlphabloxPlatform' link

Star	t Stop Install Uninstall Update Rollout Update	Remove File Export Export DDL Export File
D		
Select	Name 🛟	Application Status ሷ
	AlphabloxPlatform	<b>\$</b>
	ApplicationStudio e	÷
	DefaultApplication	÷
	IBM WBM ABX WEB DASHBOARD	÷
	IBM WBM ACTIONSERVICES	÷
	IBM WBM DMS SERVICE	÷
	IBM WBM REST SERVICES	÷
	IBM WBM WEB DASHBOARD	÷
	ivtApp	÷
	<u>query</u>	÷
Total	10	

\_\_\_\_\_ 35. In the following panel, click the 'security role to user/group mapping' link

General Properties	Modules
* Name AlphabloxPlatform	Manage Modules
Application reference validation	Web Module Properties
Issue warnings 🔍	Session management
Detail Properties	Context Root For Web Modules
Target specific application status	Initialize parameters for servlets
Charter behavior	JSP reload options for web modules
<ul> <li><u>Startup benavior</u></li> <li>Application binaries</li> </ul>	Virtual hosts
Class loading and update detection	
Remote request dispatcher properties	
Security role to user/group mapping	
View Deployment Descriptor	
Last participant support extension	

- Shared library references
- 36. In the following panel, select the check box for 'AlphabloxAdministrator' role and click the 'Look up users' button

	Look up users Look up groups							
Ø								
Select	ct Role Everyone? All authenticated? Mapped users Mapped groups							
	AlphabloxAdministrator							
	AlphabloxUser							
	AlphabloxDeveloper							

\_\_\_\_ 37. In the following panel, enter a wild character (\*) as the search string and click the Search button. Select was61admin from the available users listed, and then click the right directional arrow button, to move the user ID to the selected text area

To search for users or groups, enter a limit (number) and a search pattern (such as a*) and click Search: imit (number of items) 20
Search String
Available: perkpiadmin dashuser4 wpsrvadmin wpsbind dashuser2 wpsadmin was61 admin pubkpiadmin
OK Cancel

\_\_\_\_\_ 38. Click OK

39. Ensure that the check boxes for 'All authenticated?' are selected for the 'AlphabloxUser' and 'AlphabloxDeveloper' roles

40. The **security role to user/group mapping** panel for the **AlphabloxPlatform** application will look like the picture below:

Look up users Look up groups						
Select	Role	Everyone?	All authenticated?	Mapped users	Mapped groups	
	AlphabloxAdministrator			was61admin		
	AlphabloxUser					
	AlphabloxDeveloper					

- \_\_\_\_\_ 41. Click **OK** and save to the master configuration
- \_\_\_\_\_ 42. Back to the 'Enterprise Applications' panel, click the 'ApplicationStudio' link
- \_\_\_\_\_ 43. In the following panel, click the 'security role to user/group mapping' link
- 44. In the following panel, map the was61admin user for 'AlphabloxAdministrator' role and ensure the check box for 'All authenticated?' is selected for 'AlphabloxUser' role. Click OK and save to the master configuration
- 45. The **security role to user/group mapping** panel for the **ApplicationStudio** application will look like the picture below:

Lo	Look up users Look up groups						
Select	Role	Everyone?	All authenticated?	Mapped users	Mapped groups		
	AlphabloxAdministrator			was61admin			
	Alphablo×User						

- \_\_\_\_\_ 46. Back to the 'Enterprise Applications' panel, click the 'IBM\_WBM\_REST\_SERVICES' link
- 47. In the following panel, click the 'security role to user/group mapping' link

General Properties	Modules
* Name IBM_WBM_REST_SERVICES	Manage Modules
Application reference validation	Web Module Properties
Issue warnings 📃 👻	Session management
Detail Properties	Context Root For Web Modules
Target specific application status	JSP reload options for web
Startup behavior	modules
Application binaries	Virtual hosts
<ul> <li><u>Class loading and update</u> <u>detection</u></li> </ul>	
<ul> <li><u>Remote request dispatcher</u></li> <li><u>properties</u></li> </ul>	
Security role to user/group mapping	
View Deployment Descriptor	
Last participant support extension	
References	
Shared library references	

48. In the following panel, ensure the check box for 'All authenticated?' for the 'monitorusers' role is selected

terprise	Applications				
<u>Enterprise Applications</u> > <u>IBM_WBM_REST_SERVICES</u> > Security role to user/group mapping					
Security	role to user/gro	oup mapping	9		
Each ro from th	le that is define le domain user	ed in the ap registry.	plication or module	must map to a (	user or group
Lo	ok up users	Look u	up groups		
Select	Role	Everyone?	All authenticated?	Mapped users	Mapped groups
	monitorusers		☑ ←		
ок с	ancel				

49. Click **OK** and save the changes to the master configuration

\_\_\_\_\_ 50. Back to the 'Enterprise Applications' panel, click the 'IBM\_WBM\_WEB\_DASHBOARD' link

- \_\_\_\_\_ 51. In the following panel, click the 'security role to user/group mapping' link
- \_\_\_\_\_52. In the following panel, select the check box for 'All authenticated?' for the 'Administrator' role

terprise	Applications				
Enterpris mapping	<u>Enterprise Applications</u> > <u>IBM_WBM_WEB_DASHBOARD</u> > Security role to user/group mapping				
Security	role to user/gro	oup mapping	9		
Each ro from th	le that is define le domain user	ed in the app registry.	plication or module	must map to a (	user or group
Lo	ok up users	Look u	ip groups		
Select	Role	Everyone?	All authenticated?	Mapped users	Mapped groups
	Administrator		☑ ←		
OK Cancel					

\_\_\_\_\_ 53. Click **OK** and save to the master configuration

## $\rightarrow$ Update J2C authentication data entries for messaging buses

This part of the lab updates the J2C authentication data entries for the messaging buses on the Monitor Server. There are two messaging buses, a Common Event Infrastructure (CEI) messaging bus and a Monitor messaging bus and you will be updating them with the user.

1. In the left navigation pane of the administrative console, expand 'Security' and then click 'Bus Security' link

Ξse	🖂 Security			
	Secure administration, applications, and infrastructure			
	SSL certificate and key management			
	Bus Security <			
	Monitor Data Security			

2. In the following 'Buses' panel, click the 'Enabled' link for 'CommonEventInfrastructure\_Bus'

ises			7		
Buses					
A service integration bus supports applications using message-based and service-oriented architectures. A bus is a group of interconnected servers and clusters that have been added as members of the bus. Applications connect to a bus at one of the messaging engines associated with its bus members.					
New Delete					
Select	Name 🛟	Description 🗘	Security 🗘		
	CommonEventInfrastructure Bus	CommonEventInfrastructure Bus	Enabled		
	MONITOR.aimcp094Node01Cell.Bus	Bus for Monitor	Enabled		
Total	2				

\_\_ 3. In the following panel, click the 'J2C-authentication data' under the 'Related Items' section

Related Items				
-	JAAS - J2C authentication data			
	<u>Secure</u> <u>Administration</u> <u>and Applications</u>			

- 4. In the following panel, click the 'CommonEventInfrastructureJMSAuthAlias' link
- 5. In the following panel, update the User ID and Password
  - \_\_\_a. User ID : was61admin

#### \_\_\_\_b. Password : was61admin

General Properties
* Alias CommonEventInfrastructureJMSAuthAlias
* User ID
was61admin 🧲
* Password
Description Authentication alias for the C
Apply OK Reset Cancel

- \_\_\_\_\_6. Click **OK** and save to the master configuration
- 7. Navigate to the 'Security → Bus Security → CommonEventInfrastructure\_Bus → Enabled' again and click the 'Users and groups in the bus connector role' link under the 'Additional Properties' section to the right

eneral Properties	Additional Properties
Security Enable bus security	Users and groups in the bus connector role
Inter-engine authentication alias MonitorBusAuth	Permitted transports
Permitted transports	Related Items
<ul> <li>Restrict the use of defined transport channel chains to those protected by SSL</li> <li>Restrict the use of defined transport channel chains to the list of permitted transports</li> </ul>	<ul> <li>JAAS - J2C authentication data</li> </ul>
Mediations authentication alias	<ul> <li>Secure Administration and Applications</li> </ul>
Apply OK Reset Cancel	

\_\_\_ 8. In the following panel, add the group and user as shown below:

New Delete				
Select	Name 🛟	Туре 🗘		
	Server	Group		
	was61admin	User		
Total 2				

- \_\_\_\_\_9. Save to the master configuration
- 10. Repeat the above instructions to update the J2C authentication alias data for the monitor bus named 'Monitor.<CELL\_NAME>.Bus'. The J2C authentication named you should update is MonitorBusAuth
- \_\_\_\_\_11. Now update the Alphablox 'Server.properties' file wit the new user name and password

\_\_\_\_a. Navigate to the following location:

#### <WBM\_PROFILE\_HOME>\Alphablox\_server1\repository\servers\AlphabloxAnalytics

Example: - **WBM\_PROFILE\_HOME>** - C:\IBM\WebSphere\Monitor\profiles\WBMon01\

🗁 C:\IBM\WebSphere\MonServer\profiles\WBMon01\Alphablox_server1\repository\servers\Alphabloæaly 💶 🗖	×			
Eile Edit View Favorites Tools Help	7			
🔇 Back 🝷 🕥 🖌 🦻 🔎 Search 🌔 Folders 🛛 😰 🎯 🗙 🌍 🧮 🐨				
Address C:\IBM\WebSphere\MonServer\profiles\WBMon01\Alphablox_server1\repository\servers\AlphabloxAnalytics 💌 🎅 G	5			
🛅 logs				
cubemgr.properties				
server.copy				
Server.properties				

- \_\_\_\_b. Edit the 'Server.properties' file and scroll to the very end of this file
- \_\_\_\_ c. Add the following lines at the end of the properties file
  - ws.admin.username = <USERNAME> (was61admin)
  - ws.admin.password = <PASSWORD> (was61admin)
- \_\_\_\_ d. Save the changes and close the properties file

#### **Restart the Monitor Server profile**

- stopServer.bat server1 –username was61admin –password was61admin
- startServer.bat server1
- Ensure the server is started successfully. Review the 'SystemOut.log' file for any security related errors

## Part 4: Enable security for WebSphere Process Server V6.1

In this part of the lab, you will enable the LDAP security for WebSphere Process Server V6.1. This is not the Monitor Server, but the server where you are running your BPEL processes.

#### Prerequisite:-

Copy the **securePortal.key** file that you have exported to a temporary location on to the Process Server machine

Complete the following instructions to enable LDAP security for the WebSphere Application Server, which is the Process Server profile

- \_\_\_\_\_1. Start the process server profile and launch the administrative console
- \_\_\_\_\_2. Login to the administrative console using the user name and password if the default security is enabled at this time
- 3. In the administrative console's left navigation pane, expand 'Security' and click the 'Secure administration, applications and infrastructure' link



\_\_\_ 4. In the following 'Secure administration, applications and infrastructure' panel to the left, click the 'Security Configuration Wizard' button

Security Configuration Wizard Security Conf	iguration Report
Administrative security <ul> <li>Administrative User Roles</li> <li>Administrative Group Roles</li> </ul>	Authentication □ Use domain-qualified user name Web security
Application security Enable application security	<ul> <li>■ RMI/IIOP security</li> <li>■ Java Authentication and Authoriza</li> </ul>
Java 2 security           Java 2 security           Use Java 2 security to restrict application access to local resources	Authentication mechanisms and expir
<ul><li>Warn if applications are granted custom permissions</li><li>Restrict access to resource authentication data</li></ul>	<ul> <li><u>External authorization providers</u></li> <li><u>Custom properties</u></li> </ul>
User account repository Current realm definition	
Federated repositories Available realm definitions	

5. In the following 'Step1: Specify extent of protection' panel, ensure the check box for 'Enable application security' is selected



- \_\_\_\_6. Click Next
- \_\_\_\_7. In the following 'Step2: Select user repository' panel, ensure the radio button for 'Federated repositories' is selected



8. Click Next

- 9. In the following '**Step 3: Configure user repository**' panel, enter the primary administrative user name and password
  - \_\_\_\_a. Primary administrative user name : wpsrvadmin
  - \_\_\_\_b. Password : wpsrvadmin
  - \_\_\_\_ c. Conform password : wpsrvadmin

Note: The primary administrative user you enter here must exist in the LDAP user repository.

	Step 1: Specify	Configure user repository		
→	Step 2: Select user repository Step 3: Configure user repository Step 4: Summary	A secure, file-based user repository is built into the system for storing administrative users or environments with a small number of users. The file-based user repository can be federated with one or more external LDAP repositories. If this is the first time security has been enabled using this repository, provide a new user name and password to act as an administrator. If security was previously enabled using this repository, provide the name of a user with administrator privileges that is in the built-in repository.		
		Note: Use this panel to configure a federated repository with a built-in, file-based repository in the realm. To configure a federated repository with a non file-based repository in the realm, you must use the User accounts repository section on the Secure administration, applications, and infrastructure panel.		
		* Primary administrative user name wpsrvadmin		
		Password		
		•••••		
		Confirm password		
		••••••		
F	Previous Next (	Cancel		

\_\_\_\_\_ 10. In the following 'Step 4: Summary' panel, review the summary information

	Step 1: Specify	Summary			
	Step 2: Select user repository	Displays the list of values that are selected during the wizard and are used to enable security.			
	Step 3: Configure user repository	Options	Values		
		Enable administrative security	true		
→	Step 4: Summary	Enable application security	true		
		Use Java 2 security to restrict application access to local resources	false		
		User repository	Federated repositories		
		Primary administrative user name	wpsrvadmin		
Previous Finish Cancel					

- 11. Click **Finish.** You should see the following '**Secure administration, applications and infrastructure**' panel
  - \_\_\_a. Select 'Federated repositories' from the drop down list for the 'Available realm definitions'

Configuration       Security Configuration Report         Administrative security       Administrative User Roles         Image: Configuration security       Administrative Group Roles         Application security       Administrative Group Roles         Image: Configuration security       Multiplication security         Image: Configuration security       Restrict access to resource authentication access to local resources         Image: Configuration security       Image: Configuration mechanisms and explication mechanisms and explication providers         Image: Configuration repository       External authorization providers         Image: Configuration repository       Current realm definition         Image: Configuration repository       Current realm definition	ecure administration, applications, and infrastructure	
Security Configuration Wizard       Security Configuration Report         Administrative security       Administrative User Roles         Image: Control Contecontrol Control Control Control Control Con		
Security Configuration Report         Administrative security       Administrative User Roles         Image: Control of the security       Administrative Group Roles         Application security       Administrative Group Roles         Image: Control of the security       Administrative Group Roles         Application security       RMI/IIOP security         Image: Control of the security       RMI/IIOP security         Image: Control of the security       Image: Control of the security         Image: Control of the security       Image: Control of the security         Image: Control of the security       Image: Control of the security         Image: Control of the security       Image: Control of the security         Image: Control of the security       Image: Control of the security         Image: Control of the security       Image: Control of the security         Image: Control of the security       Image: Control of the security         Image: Control of the security       Image: Control of the security         Image: Control of the security       Image: Control of the security         Image: Control of the security       Image: Control of the security         Image: Control of the security       Image: Control of the security         Image: Control of the security       Image: Control of the security       Image: Control of the security </th <th></th> <th></th>		
Administrative security       ■ Administrative User Roles         ■ Enable administrative security       ■ Administrative Group Roles         Application security       ■ Muthentication         ■ Enable application security       ■ RMI/IIOP security         ■ Java 2 security       ■ Java 4 uthentication and Author         ■ Use Java 2 security       ■ Authentication mechanisms and extensions         ■ Restrict access to resource authentication data       ■ External authorization providers         User account repository       © Current realm definition         Erederated renositories       ■ Security	Security Configuration Wizard Security Conf	figuration Report
<ul> <li>✓ Enable administrative security ■ Administrative User Roles Administrative Group Roles</li> <li>✓ Use domain-qualified user nate Administrative Group Roles</li> <li>✓ Web security</li> <li>✓ RMI/IIOP security</li> <li>✓ Java 2 security</li> <li>✓ Java 2 security</li> <li>✓ Use Java 2 security to restrict application access to local resources</li> <li>✓ Warn if applications are granted custom permissions</li> <li>✓ Restrict access to resource authentication data</li> <li>✓ External authorization providers</li> <li>✓ Current realm definition</li> <li>✓ Enable definition</li> </ul>	Administrative security	Authentication
<ul> <li>Administrative Group Roles</li> <li>Application security</li> <li>Image: Enable application security</li> <li>Image: Enable application security</li> <li>Image: Enable application security</li> <li>Image: Enable application security</li> <li>Image: Image: Image: Enable application security</li> <li>Image: Image: Ima</li></ul>	Enable administrative security Administrative User Roles	Use domain-qualified user name
Application security         Image: Enable application security         Java 2 security         Image: Use Java 2 security to restrict application access to local resources         Image: Warn if applications are granted custom permissions         Image: Restrict access to resource authentication data         User account repository         Current realm definition         Endersted repositories	Administrative Group Roles	₩eb security
Image: Provide security       Image: Provide security         Java 2 security       Image: Provide security         Image: Provide security       Image: Provide security	Application security	■ RMI/IIOP security
<ul> <li>Enable application security</li> <li>Java 2 security</li> <li>Use Java 2 security to restrict application access to local resources</li> <li>Warn if applications are granted custom permissions</li> <li>Restrict access to resource authentication data</li> <li>User account repository</li> <li>Current realm definition</li> <li>Eadersted repositories</li> </ul>		
Java 2 security       ■ Authentication mechanisms and ex         □ Use Java 2 security to restrict application access to local resources       ■ Authentication mechanisms and ex         □ Use Java 2 security to restrict application access to local resources       ■ External authorization providers         □ Restrict access to resource authentication data       ■ External authorization providers         □ User account repository       ■ Current realm definition         □ External authorization       ■ Custom properties	Enable application security	
<ul> <li>Use Java 2 security to restrict application access to local resources</li> <li>Warn if applications are granted custom permissions</li> <li>Restrict access to resource authentication data</li> <li>External authorization providers</li> <li>Custom properties</li> </ul>	Java 2 security	Authentication mechanisms and expiration
<ul> <li>Warn if applications are granted custom permissions</li> <li>Restrict access to resource authentication data</li> <li>User account repository</li> <li>Current realm definition</li> <li>Endersted repositories</li> </ul>	$\square$ Use Java 2 security to restrict application access to local resources	
Restrict access to resource authentication data      User account repository      Current realm definition      Federated repositories	🔽 Warn if applications are granted custom permissions	External authorization providers
User account repository Current realm definition	Restrict access to resource authentication data	Custom properties
Current realm definition Federated repositories	User account repository	
Federated repositories	Current realm definition	
rederated repositories	Federated repositories	
Available realm definitions	Available realm definitions	
Federated repositories 💽 Configure Set as current	Federated repositories 💽 Configure Set as current	
Apply Reset	Apply Recet	

- \_\_\_\_ 12. Click the **Configure** button
- 13. In the following '**Configuration**' panel for '**Federated repositories**', enter the following under the '**General Properties**' category

\_\_\_\_a. Realm name : <fully qualified LDAP server host name>: <LDAP Port>

: Example: idsIdap.austin.ibm.com:389

Note: The realm name for Portal is typically the fully qualified LDAP hostname:portNumber (example: "idsldap.austin.ibm.com:389") to verify this, you can open C:\ WebSphere\profiles\wp\_profile\config\cells\<your-cell-name>\security.xml and look for <userRegistries xmi:type="security:LDAPUserRegistry" .... – there is a "realm=" entry on that line"

\_\_\_\_b. Primary administrative user name : wpsrvadmin

General Properties
* Realm name idsldap.austin.ibm.com:389
* Primary administrative user name wpsrvadmin
Server user identity
$oldsymbol{eta}$ Automatically generated server identity
O Server identity that is stored in the repository
Server user ID or administrative user on a Version 6.0.x node
Password
Ignore case for authorization

Repositories in the realm:

	Add Base entry to Realm		Use built-in reposi	tory	Remove
Select	Base entry	Re	pository identifier	Repository type	
	o=defaultWIMFileBasedRealm	Int	ternalFileRepository	File	

\_\_\_\_14. Scroll down and click the 'Add Base entry to Realm' button. This action opens the 'Repository reference' panel as shown below:

Secure administration, applications, and infrastructure				
<u>Secure administration, applications, and infrastructure</u> > <u>Federated repositories</u> > Repository reference				
Specifies a set of identity entries in a repository that are referenced by a base entry into the directory information tree. If multiple repositories are included in the same realm, it might be necessary to define an additional distinguished name that uniquely identifies this set of entries within the realm.				
Configuration				
General Properties				
* Repository       none defined     Add Repository				
* Distinguished name of a base entry that uniquely identifies this set of entries in the realm				
Distinguished name of a base entry in this repository				
Apply OK Reset Cancel				

\_\_\_\_\_ 15. Click the 'Add Repository' button

\_\_\_\_\_ 16. In the following new repository reference panel, enter the following:

\_\_\_\_a. Repository identifier : LDAP-idsIdap (Any meaningful identifier)

\_\_\_\_b. LDAP Server

- Directory Type : IBM Tivoli Directory Server V6.0
- Primary host name : idsldap.austin.ibm.com
- Port : 389
- \_\_\_ c. Security
  - Bind distinguished name : uid=wpsbind,cn=users,dc=ibm,dc=com
  - Bind password : wpsbind
  - Login properties : uid
  - Certificate mapping : Select 'EXACT\_DN' from the drop down list

General	Properties
---------	------------

* Repository identifier	
LDAP-idsldap	
LDAP server	Security
* Directory type	Bind distinguished name
* Primary host name Port	Bind password
idsIdap.austin.ibm.com 389	Login properties
Failover server used when primary is not available:	uid
Delete	Certificate mapping
Select Failover host name Port	EXACT_DN
None	Certificate filter
Add	
	Require SSL communications
Support referrals to other LDAP servers ignore 💌	Centrally managed
	Manage endpoint security configurations
	Use specific SSL alias
	NodeDefaultSSLSettings 🔽 SSL configurations

- \_\_\_\_\_17. Click **OK**. You will be back to the 'Repository reference' panel again
- \_\_\_\_\_ 18. In the 'Repository Reference' panel, enter the following:
  - \_\_\_\_a. Repository : Select 'LDAP-idsIdap' from the drop down list

- \_\_\_\_b. Distinguished names of a base entry that uniquely identifies this set of entries in the realm : dc=ibm,dc=com
- \_\_\_\_ c. Distinguished name of a base entry in this repository : dc=ibm,dc=com

	General Properties
	* Repository LDAP-idsIdap 🔽 Add Repository
	<ul> <li>Distinguished name of a base entry that uniquely identifies this set of entries in the realm</li> </ul>
	Distinguished name of a base entry in this repository dc=ibm,dc=com
	Apply OK Reset Cancel
_	
9.	Click OK
).	Click <b>OK</b> The ' <b>Federated repositories</b> ' panel will look like the picture shown below:
9. ).	Click <b>OK</b> The ' <b>Federated repositories</b> ' panel will look like the picture shown below:
9. ). <u>G</u>	Click <b>OK</b> The ' <b>Federated repositories</b> ' panel will look like the picture shown below:
9. ). <u>G</u>	Click <b>OK</b> The ' <b>Federated repositories</b> ' panel will look like the picture shown below:
9. ). <u>G</u>	Click <b>OK</b> The ' <b>Federated repositories</b> ' panel will look like the picture shown below:  eneral Properties  Realm name  idsIdap.austin.ibm.com:389  Primary administrative user name  wpsrvadmin  Server user identity
9. ). <u>G</u> * *	Click <b>OK</b> The ' <b>Federated repositories</b> ' panel will look like the picture shown below:  eneral Properties  Realm name idsIdap.austin.ibm.com:389  Primary administrative user name wpsrvadmin  Server user identity    Automatically generated server identity
9. 0. * *	Click OK The 'Federated repositories' panel will look like the picture shown below:  aneral Properties Realm name idsldap.austin.ibm.com:389 Primary administrative user name wpsrvadmin Server user identity  Automatically generated server identity  Server identity that is stored in the repository
9. 0. * *	Click OK The 'Federated repositories' panel will look like the picture shown below: eneral Properties Realm name idsIdap.austin.ibm.com:389 Primary administrative user name wpsrvadmin Server user identity  Automatically generated server identity Server identity that is stored in the repository Server user ID or administrative user on a Version 6.0.x node
9. ). * *	Click OK The 'Federated repositories' panel will look like the picture shown below: eneral Properties Realm name idsldap.austin.ibm.com:389 Primary administrative user name wpsrvadmin Server user identity  Automatically generated server identity  Server identity that is stored in the repository Server user ID or administrative user on a Version 6.0.x node Password

☑ Ignore case for authorization

Repositories in the realm:

	Add Base entry to Realm	Use built-in reposi	tory Remove
Select	Base entry	Repository identifier	Repository type
	<u>dc=ibm,dc=com</u>	LDAP-idsldap	LDAP:IDS6
	o=defaultWIMFileBasedRealm	InternalFileRepository	File

\_21. Select the check box for 'o=defaultWIMFIleBasedRealm' if it is existing (it exists if the default security is enabled) and click the Remove button.

Gei	neral P	roperties				
* F [	Realm <mark>idsldap</mark>	name <mark>. austin. ibm. com: 389</mark>				
* [	Primary	administrative user name				
1	wpsrva	dmin				
s	erver u	ser identity				
	🖸 Auto	omatically generated server i	dentity			
	O Serv	ver identity that is stored in t	he repo	ository		
	Sei	ver user ID or administrative	user c	on a Version 6.0.x node	2	
	Pas	ssword				
ſ	🗸 Ign	ore case for authorization				
F	Reposit	ories in the realm:				
		Add Base entry to Realm		Use built-in repo	sitory	Remove
	Select	Base entry	Repos	sitory identifier	Repository	type
		dc=ibm,dc=com	LDAP-	idsIdap	LDAP:IDS6	

- 22. Click OK.
- 23. Configuring supported entity types in a federated repository configuration
  - \_\_\_\_a. In the Federated Repositories panel, click the 'Supported entity types' under the 'Additional Properties' section

Repositories in the realm:					
Add Base entry to Realm Use built-in repository Remove					
Selec	t Base entry	Repository identifier	Repository type		
	dc=ibm,dc=com	LDAP-idsldap	LDAP:IDS6		
Additional Properties Related Items					
	Property extension repository	= <u>Man</u>	age repositories		
	Entry mapping repository				
	Supported entity types 🛛 🔫 🗕				

\_\_\_\_ b. In the 'Supported entity types' panel, update the 'Base entry for default parent' values for Group, OrgContainer and PersonAccount with 'dc=ibm,dc=com' and accept the defaults for the 'Relative Distinguished Name properties'. The 'Supported entity types' panel will look like the picture below:

Secure administration, applications, and infrastructure ? =					
<u>Secure administration, applications, and infrastructure</u> > <u>Federated repositories</u> > Supported entity types					
Use this page to co	onfigure entity types that are supporte	d by the member repositories.			
***					
Entity type 🛟	Base entry for the default parent $\diamondsuit$	Relative Distinguished Name properties $\diamondsuit$			
Group	dc=ibm,dc=com	cn			
OrgContainer	dc=ibm,dc=com	o)ou)dc)cn			
PersonAccount	dc=ibm,dc=com	uid			
Total 3					

- \_\_\_\_ c. Save to the master configuration
- 24. Configure the LDAP entity types
  - \_\_\_\_a. While you are in the 'Federated repositories' panel (Secure administration, applications and infrastructure → Federated repositories), click the 'Repository identifier' link, (Example:-LDAP-idsIdap)

Repositories in the realm:

Add Base entry to Realm			Use built-in repo	sitory Remove
Select	Base entry	Repo	sitory identifier	Repository type
	<u>dc=ibm,dc=com</u>	LDAP-	idsIdap	LDAP:IDS6

\_\_\_\_ b. In the following panel, scroll to the bottom and click the 'LDAP entity types' link under the 'Additional Properties' section

Addit	tional Properties	
	Performance	

- 🗉 LDAP entity types <
- Group attribute definition
- \_\_\_\_ c. In the following 'LDAP entity types' panel, update the following for the Group, OrgContainer and PersonAccount entity types:

#### 1) Group

- Object classes : groupOfUniqueNames
- Search bases : dc=ibm,dc=com
- Search filter : (objectclass=groupOfUniqueNames)
- 2) OrgContainer
  - <Accept the defaults>
- 3) PersonAccount

- Object classes : person
- Search bases : dc=ibm,dc=com
- Search filter : (objectclass=person)

4) The 'LDAP entity' panel will look like the picture below:

Secure administration, applications, and infrastructure				
<u>Secure administration, applications, and infrastructure</u> > <u>Federated repositories</u> > <u>LDAP-idsldap</u> > LDAP entity types				
Use this page to list entity types that are supported by the member repositories or to select an entity type to view or change its configuration properties.				
Preferences     ■				
*** **				
Entity type 💲	Object classes 🗘			
Group	groupOfUniqueNames			
OrgContainer organization; organizationalUnit; domain; container				
PersonAccount person				
Total 3				

- \_\_\_\_ d. Save to the master configuration
- 25. Configure group attribute definition
  - \_\_\_\_a. While you are in the 'Federated repositories' panel (Secure administration, applications and infrastructure → Federated repositories), click the 'Repository identifier' link, (Example:-LDAP-idsIdap)

Repositories in the realm:

	Add Base entry to Realm	Use built-in rep	ository Remove
Select	Base entry	Repository identifier	Repository type
	<u>dc=ibm,dc=com</u>	LDAP-idsldap	LDAP:IDS6

\_ b. In the following panel, scroll to the bottom and click the '**Group attribute definition**' link under the '**Additional Properties**' section

Additional Properties				
	Performance			
	LDAP entity types			
	Group attribute definition <			

- \_\_\_\_ c. In the following 'Group attribute definition' panel, enter the following information:
  - Name of group membership attribute : LDAP-AllGroups
  - For the scope, select the check box for 'All- Contains all direct, nested and dynamic members'

Configuration	
General Properties          Name of group membership attribute         LDAP-AllGroups	Additional Properties  Member attributes Dynamic member attributes
Scope of group membership attribute O Direct - Contains only immediate members of the group without members of subgroups O Nested - Contains direct members and members nested within subgroups of this group O All - Contains all direct, nested, and dynamic members	
Apply OK Reset Cancel	

• Click Apply

\_\_\_\_d. While you are in the 'Group attribute definition' panel, click the 'Member attributes' link under 'Additional properties' sections

Secure administration, applications, and infrastructure ? =							
	<u>Secure administration, applications, and infrastructure</u> > <u>Federated repositories</u> > <u>LDAP-idsldap</u> > <u>Group attribute definition</u> > Member attributes						
	Use thi	nis page to manage Lightweight Directory Access Protocol (LDAP) member attributes.					
	🕀 Pref	eferences					
New Delete							
	D						
	Select	Name 🛟	Scope 🗘	Object class 🗘			
		member	all	groupOfNames			
	Total	Total 2					

\_\_\_\_e. In the following panel, click the **New** button to create a new member attribute

- \_\_\_\_f. In the following panel, enter the following information:
  - Name of member attribute : uniqueMember
  - Object class : groupOfUniqueNames
  - For the scope, select the check box for 'All- Contains all direct, nested and dynamic members'
| uniqueMember   |   |
|--|---|
| bject class  |   |
| groupOfUniqueNames   |   |
| Cope<br>C Direct - Contains only ir<br>C Nested - Contains direc | nmediate members of the group without members of subgroups<br>t members and members nested within subgroups of this group |

- Click OK
- \_\_\_\_g. Save to the master configuration
- \_\_\_\_\_ 26. Configure 'Cross Cell Single Sign-on'
  - \_\_\_\_a. While you are in the 'Secure administration, applications and infrastructure' panel, expand 'Web Security' under the 'Authentication' category

	and a second second
A	uthentication
	Use domain-qualified user names
Ð	Web security
	General settings
	🗉 single sign-on (SSO) 🛛 🗲 🗕 🛶
	Trust association
Ŧ	RMI/IIOP security
Đ	Java Authentication and Authorization Ser
-	Authentication mechanisms and expiration

- \_\_\_\_b. Click the 'single sign-on (SSO)' link
- \_\_\_\_ c. In the following 'single sign-on (SSO)' panel, do the following:
  - Select the check box for 'Enabled'
  - Ensure the check box for 'Required SSL' is not selected
  - Domain name : ibm.com
  - Select the check box for 'Interoperability Mode'
  - Unselect the check box for 'Web bound security attribute propagation'

General Properties
🗹 Enabled
Requires SSL
Domain name
ibm.com
🗹 Interoperability Mode <
└── Web inbound security attribute propagation ↑
Apply OK Reset Cancel

- 27. Click OK. You will be directed to the 'Secure administration, applications and infrastructure' panel again
- 28. While you are in the 'Secure administration, applications and infrastructure' panel, click the 'Authentication mechanisms and expiration' link

- A	uthentication
	Use domain-qualified user names
Ð	Web security
Ŧ	RMI/IIOP security
Ŧ	Java Authentication and Authorization Service
-(	Authentication mechanisms and expiration

29. In the following 'Authentication mechanisms and expiration' panel, enter the following under the 'Cross-cell single sign-on' category to import the key file that you had exported on the portal (dashboard) server machine

**Note:** Enter the LTPA password that you specified when you Enabled LDAP Security for Portal, and enter the LTPA key file name that you specified near the end of the "LDAP Security for Portal" configuration.

- \_\_\_\_a. Password : password
- \_\_\_\_b. Confirm password : password
- \_\_\_\_ c. Fully Qualified Key file name : Example:- C:\KeyFile\securePortal.key

kep	t in one or more key stores.
Ke N	y set group odeLTPAKeySetGroup 💌 🛛 Generate keys
-	Key set groups
Aut	hentication expiration
Aut tim	hentication information persists in the system for a limited amount of a before it expires and must be refreshed.
Au	thentication cache timeout
	10 minutes 0 seconds
Cros Sino pas key	gle sign-on < gle sign-on across cells can be provided by sharing keys and swords. To share the keys and password, log on to one cell, specify a file, and click Export keys. Then, log on to the other cell, specify the file, and click Import keys.
Cro Sin pas key key	gle sign-on <b>&lt;</b> gle sign-on across cells can be provided by sharing keys and swords. To share the keys and password, log on to one cell, specify a file, and click Export keys. Then, log on to the other cell, specify the file, and click Import keys.
Cro Sin pas key key	gle sign-on constant of the provided by sharing keys and swords. To share the keys and password, log on to one cell, specify a file, and click Export keys. Then, log on to the other cell, specify the file, and click Import keys.
Cro Sin pas key key * P •	gle sign-on cross cells can be provided by sharing keys and swords. To share the keys and password, log on to one cell, specify a file, and click Export keys. Then, log on to the other cell, specify the file, and click Import keys.
Cros Sing pas key key • •	gle sign-on across cells can be provided by sharing keys and swords. To share the keys and password, log on to one cell, specify a file, and click Export keys. Then, log on to the other cell, specify the file, and click Import keys. assword assword
Cro: Sin; pass key key * P * C • •	ses-cell single sign-on < gle sign-on across cells can be provided by sharing keys and swords. To share the keys and password, log on to one cell, specify a file, and click Export keys. Then, log on to the other cell, specify the file, and click Import keys. assword onfirm password onfirm password onfirm password
Cros Siny pass key key * Pa * Ci * Ci	ss-cell single sign-on < gle sign-on across cells can be provided by sharing keys and swords. To share the keys and password, log on to one cell, specify a file, and click Export keys. Then, log on to the other cell, specify the file, and click Import keys. assword assw
Cros Sing pas key key * P * • • •	ss-cell single sign-on < gle sign-on across cells can be provided by sharing keys and swords. To share the keys and password, log on to one cell, specify a file, and click Export keys. Then, log on to the other cell, specify the file, and click Import keys. assword a

\_\_\_\_\_ 30. Click the 'Import Keys' button

\_\_\_\_\_ 31. Click the **Save** link, to save the configuration

**Note:** To restart the server at this time, you should enter the old user name and password configured during the WebSphere Process Server profile creation.

# →Update security role mappings for BPE container and task container

1. In the left navigation pane of the administrative console, expand '**Applications**' and click the '**Enterprise Applications**' link



\_\_ 2. In the following 'Enterprise Applications' panel, click the 'BPEContainer\_<NODE\_NAME>\_server1' link



3. In the following panel, click the 'Security role to user/group mapping' link under the 'Detail Properties' section

nterprise Applications	? -
Enterprise Applications > BPEContainer_aimcpC	)95Node05_server1
Use this page to configure an enterprise applicat	tion. Click the links to access pages for
further configuring of the application or its modu	les.
Configuration	
General Properties	Modules
* Name BPEContainer_aimcp095Node05_server1	Manage Modules
	Web Module Properties
Application reference validation Issue warnings	Session management
Detail Properties	<ul> <li><u>Context Root For Web</u></li> <li><u>Modules</u></li> </ul>
Target specific application status	<ul> <li>JSP reload options for web modules</li> </ul>
Startup behavior	Virtual hosts
<ul> <li>Application binaries</li> <li>Class loading and update</li> </ul>	Enterprise Java Bean Properties
detection	Application profiles
Remote request dispatcher properties	Message Driven Bean listener bindings
Security role to user/group mapping	EJB JNDI names
User RunAs roles	Web Services Properties
View Deployment Descriptor	Provide JMS and EJB
Last participant support extension	endpoint URL information
References	<u>Publish WSDL files</u> Describe UTTP and existent UP1
Resource references	Provide HTTP endpoint UKL information

4. In the flowing panel, select the check boxes for 'BPESystemAdministrator' and 'BPESystemMonitor' roles, click the 'Look up users' button and map the user ID (Example: wpsrvadmin). Also select the check boxes in the 'All Authenticated' column for 'BPEAPIUser', 'WebClientUser' and 'JMSAPIUser' roles

Look up users Look up groups					
Select	Role	Everyone?	All authenticated?	Mapped users	Mapped groups
	BPEAPIUser		☑ ←		
	BPESystemAdministrator			wpsrvadmin	
	BPESystemMonitor			wpsrvadmin	
	WebClientUser		☑ 🔶		
	JMSAPIUser		☑ 🛶 —		

- \_\_\_\_\_5. Click **OK** and save to the master configuration
- 6. Back to the 'BPEContainer\_<NODE\_NAME>\_server1' configuration panel, click the 'User RunAs roles' link under the 'Detail Properties' section

Detail Properties		
	Target specific application status	
	Startup behavior	
	Application binaries	
	Class loading and update detection	
	<u>Remote request dispatcher</u> properties	
	Security role to user/group	
	<u>User RunAs roles</u> 🛛 👞	
	View Deployment Descriptor	
	Last participant support extension	

- \_\_\_\_\_7. In the following panel, update the 'JMSAPIUser' role. Do the following:
  - \_\_\_a. Username : **wpsrvadmin**
  - \_\_\_\_b. Password : wpsrvadmin
  - \_\_\_\_ c. Select the check box for 'JMSAPIUser' role
  - \_\_\_\_ d. Click the Apply button. You should specify the JMSAPIUser

Enterprise Applications	2 -				
Enterprise Applications > BPEContainer_aimcp	<u>095Node05_server1</u> > User RunAs roles				
User RunAs roles					
The enterprise beans or servlet that you are in Some enterprise beans or servlet use RunAs ro recognized when interacting with another enter	istalling contain predefined RunAs roles. oles to run as a particular role that is prise bean.				
username					
wpsrvadmin 🗲 🛶					
password					
••••••					
Remove the RunAsUser user name and passw	ord from the selected roles.				
Remove					
Select Role User name					
→ 🔽 JMSAPIUser	wpsrvadmin <				
OK Cancel					

- 8. Click **OK** and save to the master configuration
- 9. Follow the above instructions and update the security role mappings for the 'Task Container' named 'TaskContainer\_<NODE\_NAME>\_server1'. The security configuration is as show below:

nterprise Applications ?						
<u>Enterprise Applications</u> > <u>TaskContainer_aimcp095Node05_server1</u> > Security role to user/group mapping						
Security role to user/group mapping						
Each role that is defined in the application or module must map to a user or group from the domain user registry.						
	Look up users Look up groups					
Select	Role	Everyone?	All authenticated?	Mapped users	Mapped groups	
	TaskAPIUser		V			
	TaskSystemAdministrator			wpsrvadmin	<del>~</del>	
	TaskSystemMonitor			wpsrvadmin	-	
	EscalationUser					
OK Cancel						

- \_\_\_\_\_10. Click **OK** and save to the master configuration
  - \_\_\_\_ 11. Update security role mappings for BPC Explorer

\_\_\_\_a. On the Enterprise Application page, click on BPCExplorer\_<NODE\_NAME>\_server1



\_\_\_\_\_12. Click **OK** and save to the master configuration

## →Update J2C authentication data entries for messaging buses

This part of the lab updates the J2C authentication data entries for the messaging buses on the WebSphere Process Server.

1. In the left navigation pane of the administrative console, expand 'Security' and then click 'Bus Security' link

Ξ	∃ Security			
	e,	Business Integration Security		
	1	Secure administration, applications, and infrastructure		
		SSL certificate and key management		
	1	Bus Security		

2. In the following 'Buses' panel, click the 'Enabled' link for 'CommonEventInfrastructure\_Bus'

Buses			
A servi bus is Applica	ce integration bus supports applications using a group of interconnected servers and clusters itions connect to a bus at one of the messagir	message-based and service-orient that have been added as member: ng engines associated with its bus m	ed architectures s of the bus. nembers.
🕀 Pret	ferences		
New	Delete		
	∎ ₩ ₽		
Select	Name 🛟	Description 🗘	Security 🗘
	BPC.aimcp095Node03Cell.Bus	Messaging bus for Process Choreographer	Enabled
•	CommonEventInfrastructure Bus	CommonEventInfrastructure Bus	Enabled
	SCA.APPLICATION.aimcp095Node03Cell.Bus	Messaging bus for Service	Enabled
	SCA.SYSTEM.aimcp095Node03Cell.Bus	Messaging bus for Service	Enabled

\_\_ 3. In the following panel, click the 'J2C-authentication data' under the 'Relation Items' section



- 4. In the following panel, click the 'CommonEventInfrastructureJMSAuthAlias' link
- \_\_\_\_ 5. In the following panel, update the User ID and Password

#### \_\_\_a. User ID : wpsrvadmin

\_\_\_\_b. Password : wpsrvadmin

General Properties
* Alias CommonEventInfrastructureJMSAuthAlias
* User ID wpsrvadmin
* Password
Description Authentication alias for the C
Apply OK Reset Cancel

- \_\_\_\_\_6. Click **OK** and save to the master configuration
- \_\_\_\_7. Navigate to the 'Security → Bus Security → CommonEventInfrastructure\_Bus → Enabled' again and click the 'Users and groups in the bus connector role' link under the 'Additional Properties' section to the right

eneral Properties	Additional Properties
Security          Inter-engine authentication alias         MonitorBusAuth	<ul> <li>Users and groups in the bus connector role</li> <li>Permitted transports</li> </ul>
Permitted transports         O Allow the use of all defined transport channel chains         • Restrict the use of defined transport channel chains to those protected by SSL         • Restrict the use of defined transport channel chains to the list of permitted transports         Mediations authentication alias         (none)	Related Items           JAAS - J2C           authentication           data           Secure           Administration           and Applications
Apply OK Reset Cancel	

\_\_\_\_\_ 8. In the following panel, add the group and user as shown below:

Buses ? -			
<u>Buses</u> > <u>Security for bus CommonEventInfrastructure</u> Bus > Users and groups in the bus connector role			
Users in the bus connector role are able to connect to the bus to perform messaging operations. Users can have this role either by specifically having that role, or because they are in a group with that role.			
🕀 Pre	ferences		
New Delete			
Select	Name 🛟	Type 🗘	
	Server	Group	
	wpsrvadmin	User	
Total 2			

- \_\_\_\_\_9. Save to the master configuration
- 10. Repeat the above instructions to update the J2C authentication alias data for the monitor bus named 'BPC.<CELL\_NAME>.Bus', 'SCA.APPLICATION.<CELL\_NAME>.Bus' and 'SCA.SYSTEM.<CELL\_NAME>.Bus'

#### **Restart the Process Server profile**

- stopServer.bat server1 –username was61admin –password was61admin
- startServer.bat server1
- Ensure the server is started successfully

## Part 5: Configure Remote CEI server to use WebSphere Business Monitor in a secured environment

In this part of the lab, you will use the cross cell files and run the cross cell script to create the remote service integration bus and create the link between the local and remote buses. This enables WebSphere Business Monitor server to receive Common Event Infrastructure (CEI) events from a remote CEI server. The instructions in this lab are good for the remote CEI server on either WebSphere Process Server V6.1 or WebSphere Process Server V6.0.2 with or with out WebSphere Business Monitor installed.

#### **Prerequisites:-**

→ The service integration bus for the local Business Monitor server has been created. By default the WebSphere Business Monitor installation wizard creates it for you. To see if the monitor service integration bus has been created, launch the WebSphere Business Monitor profile administrative console and login using the user name and password.

- In the left navigation pane, expand 'Service Integration' and then click the 'Bus' link
- You should see the monitor service integration bus named as 'Monitor.<CELL\_NAME>Bus>' with security 'Enabled'

New Delete			
Select	Name 🛟	Description 🗘	Security 🗘
	CommonEventInfrastructure Bus	CommonEventInfrastructure Bus	Enabled
	MONITOR.aimcp094Node01Cell.Bus	Bus for the Business Monitor server	<u>Enabled</u>
Total 2			

- If the monitor service integration bus does not exist on your local Monitor server installation, follow the instructions below to create one:
  - Open a command line window and change directories to WebSphere Business Monitor server profile. Example: <WBM\_PROFILE\_HOME>\bin (C:\IBMWebSphere\Monitor\profiles\WBMon01\bin)
  - Run the 'monitorSIBConfig.py' script interactively as shown below:

#### wsadmin –f <WBM\_HOME>\scripts.wbm\sib\monitorSIBConfig.py

Where <WBM\_HOME> is C:\IBM\WebSphere\Monitor

o Follow the instructions and enter the required parameters when prompted

→ Ensure security is enabled on both the local WebSphere Business Monitor server and the remote WebSphere Process Server cells. Note that they both should use the one federated repository, for example LDAP.

→ Ensure that LTPA authentication is configured across the WebSphere Business Monitor and WebSphere Process Server cells. For example export the LTPA key from the WebSphere Business Monitor cell and import it to WebSphere Process Server cell

 $\rightarrow$  Enable the server-to-server trust (SSL) between the servers hosting each side of the service integration bus. Follow the instructions below, to enable the server-to-server trust among the servers:

#### Local WebSphere Business Monitor Server:

• Login to the WebSphere Business Monitor server administrative console. In the left navigation pane, expand 'Security' and then click the 'SSL certificate and key management' link



• In the following 'SSL certificate and key management' to the right, click the 'Key stores and certificates' link under the 'Related Items' section

Related Items
SSL configurations
<ul> <li><u>Dynamic outbound</u> endpoint <u>SSL</u> configurations</li> </ul>
Key stores and certificates
Key sets
Key set groups
Key managers
Trust managers

• In the following 'Key stores and certificates' panel, click the 'NodeDefaultTrustStore' link

New Delete Exchange signers			
Select	Name 🛟	Path 🗘	
	NodeDefaultKeyStore	\${CONFIG_ROOT}/cells/aimcp094Node01Cell/nodes/aimcp094Node01/key.p12	
	NodeDefaultTrustStore	\${CONFIG_ROOT}/cells/aimcp094Node01Cell/nodes/aimcp094Node01/trust.p12	
	NodeLTPAKeys	\${CONFIG_ROOT}/cells/aimcp094Node01Cell/nodes/aimcp094Node01/ltpa.jceks	
Total	3		

• In the following 'NodeDefaultTrustStore' panel, click the 'Signer Certificates' link under the 'Additional Properties' section



• In the following 'Signer Certificates' panel, click the 'Retrieve from port' button

Add Delete Extract Retrieve from port				
Select	Alias 🗘	Issued to 🗘	Fingerprint (SHA digest) 💲	Expiration 🗘
	<u>default</u>	CN= <b>EXE</b> .austin.ibm.com, O=IBM, C=US	5F:7D:2C:48:EF:D8:E1:49:A6:C0	Valid from February 25,
	<u>dummyclientsigner</u>	CN=jclient, OU=SWG, O=IBM, C=US	0B:3F:C9:E0:70:54:58:F7:FD:81	Valid from July 30, 2003
	<u>dummyserversigner</u>	CN=jserver, OU=SWG, O=IBM, C=US	FB:38:FE:E6:CF:89:BA:01:67:8F:	Valid from July 30, 2003

- In the following 'Retrieve from port' panel, enter the following information:
  - Host : <fully qualified host name of the remote CEI Server> (Example: remotecei.austin.ibm.com)
  - o Port : 7286 (SSL port)

**Note:** To determine the correct SSL port number, log in to the WebSphere Business Monitor server administrative console; expand '**Servers**' in the left navigation pane and then click the '**Application Servers**' link. In the following application server panel to the right, click the '**server1**' link. In the following panel expand '**Ports**' under the '**Communications**' section and note down the port number corresponding to '**SIB\_ENDPOINT\_SECURE\_ADDRESS**' port name.

o Alias : Example: remoteCEI

General Properties
* Host
remotecei.austin.ibm.com 🛛 🗧 💳
* Port
7286 🔶
SSL configuration for outbound connection NodeDefaultSSLSettings 🔽 * Alias remoteCEI
Retrieve signer information
Apply OK Reset Cancel

- o Click the 'Retrieve signer information' button
- You should see the following signer information that is retrieved from the remote CEI server

General Properties
* Host
remotecei, austin, ibm, com
* Port
7286
SSL configuration for outbound connection
NodeDefaultSSLSettings 💌
* Alias
remoteCEI
Retrieve signer information
Retrieved signer information
Serial number
1203967108
Issued to
CN= <b>remoțtecei.austin.ibm.com</b> O=IBM, C=US
Issued by
CN= remotecei. austin. ibm. com O=IBM, C=US
Fingerprint (SHA digest)
85:4A:47:CE:32:2E:CB:1F:7E:44:38:EA:42:7E:B3:CB:6F:4E:69:F2
Validity period
February 21, 2023
Apply OK Reset Cancel

• Click **OK** and save to the master configuration

#### Remote CEI Server (WebSphere Process Server V6.1):

 Now you need to setup trust on the remote CEI server. So follow the above instructions but this time you will be logged on the remote CEI server in order to retrieve the signer information from the WebSphere Business Monitor Server cell

 $\rightarrow$  Create a user that is valid in both the WebSphere Business Monitor server and WebSphere Process Server for the Monitor Bus link authentication. The monitor bus link requires a user ID where the user name is valid in both the cells. However the password can be unique to each cell, but the user name must be the same.

Complete the following instructions to configure the cross cell communication between the WebSphere Business Monitor server and WebSphere Process Server cells:

1. Navigate to the WebSphere Business Monitor, scripts (scripts.wbm) directory located at <br/>
WBM\_HOME> (Example: C:\IBM\WebSphere\Monitor\scripts.wbm\crossCell)

🗁 C:\IBM\WebSphere\MonServer\scripts.wbm\crossCell 📃 🗖 🗙
Address C:\IBM\WebSphere\MonServer\scripts.wbm\crossCell
🛋 com.ibm.wbimonitor.observationmgr.crosscell_6.1.0.0.jar
💽 configRemoteMonitorBus.bat
configRemoteMonitorBus.props
🚾 configRemoteMonitorBus.sh
🖳 mon61to61CrossCell.zip 🛛 <table-cell-columns> 🗧</table-cell-columns>
🛋 mon61to602CrossCell.jar
💭 mon61to602CrossCell.zip < —

- 2. Depending on the type of remote CEI server, take the appropriate action.
  - \_\_\_\_a. Remote CEI server on WebSphere Process Server V6.1
    - 1) If WebSphere Business Monitor 6.1 is installed locally, but **not** on the remote CEI server:

From the **<WBM\_HOME>/scripts.wbm/crossCell** directory of the local Business Monitor server installation, copy the mon61to61CrossCell.zip file to the **<WPS61\_HOME>\plugins** directory of the remote CEI server, that is WebSphere Process

Server V6.1 and extract the contents

Address C:\IBM\WebSphere\ProcServer\plugins	💌 🄁 Go
😰 org.eclipse.jdt.core_3.2.0.v_671.jar	com.ibm.wbimonitor.observationmgr.crosscell_6.1.0.0.jar
🛐 org.eclipse.osgi_3.2.1.R32x_v20060919.jar	🔊 com.ibm.wbimonitor.observationmgr.spi.impl_6.1.0.0.jar
🛐 org.eclipse.text_3.2.0.v20060605-1400.jar	com.ibm.wbimonitor.observationmgr.spi_6.1.0.0.jar
🛐 org.eclipse.update.configurator_3.2.1.v20092006.jar	🔊 com.ibm.wbimonitor.util_6.1.0.0.jar
🖳 mon61to61CrossCell.zip 🔫 —	
com.ibm.wbimonitor.monresources_6.1.0.jar	Delete
com.ibm.wbimonitor.observationmgr.configutil_6.1.0.0.jar	Delete

2) If WebSphere Business Monitor 6.1 is installed both locally and on the remote CEI server:

From the **<WBM\_HOME>/scripts.wbm/crossCell** directory of the local Business Monitor server installation, copy the

com.ibm.wbimonitor.observationmgr.crosscell\_6.1.0.0.jar file to the
<WPS61\_HOME>\plugins of the remote CEI server, that is the WebSphere Process Server
V6.1

3) From the remote CEI server's **<WPS61\_HOME>/bin** directory, run the appropriate command to configure the application server to recognize the .jar files: **osgiCfgInit.bat** or **osgiCfgInit.sh** 

\_\_\_\_b. Remote CEI Server on WebSphere Process Server V6.0.2

 From the <WBM\_HOME>/scripts.wbm/crossCell directory of the local Business Monitor server installation, copy the mon61to602CrossCell.zip file to the <WPS602\_HOME>/lib folder of the remote CEI server, that is WebSphere Process Server V6.0.2 and extract the contents

Address C:\IBM\WebSphere\ProcServer\lib		💌 🄁 Go
🚺 org.eclipse.jdt.core_3.2.0.v_671.jar	🔊 monSPIImpl.jar	
🛐 org.eclipse.osgi_3.2.1.R32x_v20060919.jar	🔊 monSPI.jar	
🛐 org.eclipse.text_3.2.0.v20060605-1400.jar		
org.eclipse.update.configurator_3.2.1.v20092006.jar		
🖳 mon61to602CrossCell.zip 🛛 👡 🚬		
mon61to602CrossCell.jar		
monCrossCellMBean.jar		

2) Restart the WebSphere Process Server

3. Run the 'configRemoteMonitorBus.bat' script on the local WebSphere Business Monitor server

**Note:** Ensure both the WebSphere Business Monitor server and the WebSphere Process server are started at this time.

\_\_\_\_a. Open a command line window and change directories to <WBM\_HOME>\scripts.wbm\crossCell and run the 'configRemoteMonitorBus.bat' script

C:\WINDOWS\system32\cmd.exe

C:\IBM\WebSphere\MonServer\scripts.wbm\crossCell>configRemoteMonitorBus.bat 🛓 👘

\_\_\_\_b. Type 'yes' when prompted to answer the question 'Is security enabled for this configuration?'

🙉 C:\WINDOWS\system32\cmd.exe - configRemoteMonitorBus.bat	_ 🗆 🗡
This utility will create a foreign bus link between the Monitor bus and a r cell	emote
Is security enabled for this configuration? yes or no yes 🚄	

\_\_\_\_ c. Hit the 'Enter' key

\_\_\_\_d. Enter the fully qualified host name of the host machine hosting the WebSphere Business Monitor Server (Example: monitor61.austin.ibm.com)

🔤 C:\WINDOWS\system32\cmd.exe - configRemoteMonitorBus.bat

Enter the fully qualified hostname of the server or deployment manager hosting B	
usiness Monitor	
Hit enter to accept the default (localhost) :	
monitor61.austin.ibm.com < 🗕 🚽 🚽 🛶 🛶 🛶 🛶 🛶 🛶 🛶 🛶 🛶 🛶 🛶 🛶 🛶	

\_\_\_\_e. Hit the 'Enter' key

\_\_\_\_f. Enter the SOAP port of the WebSphere Business Monitor Server. (Example: 8880)

\_ | 🗆 🗙

**Note:** To determine the correct SOAP port number, log in to the WebSphere Business Monitor server administrative console; expand '**Servers**' in the left navigation pane and then click the '**Application Servers**' link. In the following application server panel to the right, click the '**server1**' link. In the following panel expand '**Ports**' under the '**Communications**' section and note down the port number corresponding to '**SOAP CONNECTOR ADDRESS**' port name.



\_\_\_\_g. Hit the 'Enter' key

\_\_\_ h. Enter the administrative user ID for the WebSphere Business Monitor Server (Example: was61admin)

C:\WINDOWS\system32\cmd.exe - configRemoteMonitorBus.bat

Enter an administrator userid for the server or deployment manager hosting Busin ess Monitor : was61admin ————

\_\_\_\_ i. Hit the 'Enter' key

- \_\_\_\_j. Enter the password for the above user ID when prompted. (Example: was61admin). Hit the 'Enter' key
- \_\_\_\_k. Enter the fully qualified host name of the host machine hosting the remote CEI server, that is the WebSphere Process Server (Example: remotecei.austin.ibm.com)

```
      C:\WINDOWS\system32\cmd.exe - configRemoteMonitorBus.bat
      Image: C:\WINDOWS\system32\cmd.exe - configRemoteMonitorBus.bat

      Enter the hostname of the remote server or deployment manager hosting CEI

      Hit enter to accept the default (localhost) :

      remotecei.austin.ibm.com
```

\_\_\_I. Hit the 'Enter' key

\_\_\_\_m. Enter the SOAP port of the remote CEI server (Example: 8880)

```
C:\WINDOWS\system32\cmd.exe - configRemoteMonitorBus.bat
```

\_\_\_ n. Hit the 'Enter' key

\_\_\_\_\_o. Enter the administrative user ID for the remote CEI server (Example: wpsrvadmin)

\_ 🗆 ×

🔤 C:\WINDOW5\system32\cmd.exe - configRemoteMonitorBus.bat
Enter an administrator userid for the remote server or deployment manager hostin g CEI : wpsrvadmin
p. Hit the ' <b>Enter</b> ' key
q. Enter the password for the above user ID when prompted. (Example: wpsrvadmin). Hit the ' <b>Enter</b> ' key
r. If prompted for a SSL Signer Certificate exchange, say ' <b>y</b> ' for yes
📾 C:\WINDOWS\system32\cmd.exe - configRemoteMonitorBus.bat
*** SSL SIGNER EXCHANGE PROMPT *** SSL signer from target host is not found in trust store C:/IBM/WebSphe re/MonServer/profiles/WBMon01/etc/trust.p12.
Here is the signer information (verify the digest value matches what is displaye d at the server):
Subject DN: CN=austin.ibm.com, O=IBM, C=US Issuer DN: CN=OFaustin.ibm.com, O=IBM, C=US Serial number: 1203967108 Expires: Tue Feb 21 13:18:28 CST 2023 SHA-1 Digest: 85:4A:47:CE:32:2E:CB:1F:7E:44:38:EA:42:7E:B3:CB:6F:4E:69:F2 MD5 Digest: AE:59:BE:02:86:F2:CE:68:CA:9E:CD:4A:51:EA:0B:AE
Add signer to the trust store now? (y/n) y 🚄 🔤 🔤 🔤

\_\_\_\_s. Hit the 'Enter' key

\_\_\_\_t. Say 'yes' to use the defaults when configuring the messaging engine.

Note: Additional configuration is needed if you choose not to use the defaults when configuring the messaging engine. To make it simple, this lab covers only the default configuration.

📾 C:\WINDOWS\system32\cmd.exe - configRemoteMonitorBus.bat	
Do you want to use the defaults when configuring the messaging engine	? yes or no
Hit enter to accept the default (yes) : yes 🛫 —	

\_\_\_\_ u. Hit the 'Enter' key

\_\_\_\_v. Enter the user ID for authentication with the Monitor bus in the remote cell (Example: wpsrvadmin)



\_\_\_\_w. Hit the 'Enter' key

\_\_\_\_x. Enter the password for the above user ID when prompted. (Example: wpsrvadmin). Hit the 'Enter' key

\_\_\_\_y. Enter the user ID where the user name is valid in both the WebSphere Business Monitor and WebSphere Process Server cells

**Note:** The monitor bus link requires a user ID where the user name is valid in both the cells. However the password can be unique to each cell, but the user name must be the same.

📾 C:\WINDOWS\system32\cmd.exe - configRemoteMonitorBus.bat	_ 🗆 🗵
The Monitor bus link requires a userid where the user name is valid in both s. The password can be unique to each cell, but the name must be the same Enter a user name that is valid in both cells : buslinkuser	cell

- \_\_\_\_ z. Hit the 'Enter' key
- \_\_\_\_aa. Enter the password for the above user ID for the local cell, which is WebSphere Business Monitor cell when prompted. (Example: wpsrvadmin). Hit the 'Enter' key
- \_\_\_\_ bb. Enter the password for the above user ID for the remote cell, which is WebSphere Process Server cell when prompted. (Example: wpsrvadmin). Hit the 'Enter' key
- \_\_ cc. The remote CEI configuration progresses with the creation of remote bus named 'Monitor.<REMOTE\_CELL\_NAME.Bus>' creates the foreign buses, foreign bus links and eventually saves the configuration.
- \_\_\_\_dd. Restart both the WebSphere Business Monitor server and the WebSphere Process Server

**Troubleshooting:** If you see the following message on both the cells, it means that the server-to-server trust (SSL) across the WebSphere Business Monitor and the remote CEI server cells is not configured.

#### Local WebSphere Business Monitor cell:

CWPKI0022E: SSL HANDSHAKE FAILURE: A signer with SubjectDN "CN=remotecei.austin.ibm.com, O=IBM, C=US" was sent from target host:port "remotecei.austin.ibm.com:7286". The signer may need to be added to local trust store "<WBM\_PROFILE\_HOME>/config/cells/Node01Cell/nodes/Node01/trust.p12" located in SSL configuration alias "NodeDefaultSSLSettings" loaded from SSL configuration file "security.xml". The extended error message from the SSL handshake exception is: "No trusted certificate found".

#### Remote CEI Server (WebSphere Process Server) cell:

CWPKI0022E: SSL HANDSHAKE FAILURE: A signer with SubjectDN "CN=monitor61.austin.ibm.com, O=IBM, C=US" was sent from target host:port "monitor61.austin.ibm.com:7286". The signer may need to be added to local trust store "<WPS\_PROFILE\_HOME>/config/cells/Node01Cell/nodes/Node01/trust.p12" located in SSL configuration alias "NodeDefaultSSLSettings" loaded from SSL configuration file "security.xml". The extended error message from the SSL handshake exception is: "No trusted certificate found".

Follow the instructions from the prerequisite section of this document to configure the server-to-server trust (SSL) across the cells and then restart both the servers.

\_\_\_\_ ee. You should see the following message in 'SystemOut.log' of both the WebSphere Business Monitor and the remote WebSphere Process Server indicating that the monitor cross cell bus is consistent

#### Local WebSphere Business Monitor and Remote CEI Server cells:

SibMessage I [MONITOR.<CELL\_NAME>.Bus:<NODE\_NAME>.server1-MONITOR. <CELL\_NAME>.Bus] CWSIP0382I: Messaging engine BE14D3AA1B50DA1B responded to subscription request, **Publish Subscribe topology now consistent**.

### Part 6: Security configuration - After model deployment

After you deploy a model into a cross-cell configuration, it is necessary to perform additional security configuration for each model. The following instructions should be implemented on the remote CEI server:

#### → Grant user or group Sender role access to the foreign bus:

Open a command window and change directories to the WebSphere Process Server profile's **bin**directory

#### cd <WPS\_PROFILE\_HOME>\bin

Example: C:\IBM\WebSphere\ProcServer\profiles\ProcSrv01\bin

• Run the 'wsadmin' script as shown below:

```
> wsadmin – username wpsrvadmin – password wpsrvadmin
```

wsadmin>

• Run the following wsadmin commands:

```
$AdminTask addUserToForeignBusRole {
-bus <BUS_NAME>
-foreignBus <FOREIGN_BUS_NAME>
-role Sender
-user <USER_NAME>
}
$AdminTask addGroupToForeignBusRole {
-bus <BUS_NAME>
-foreignBus <FOREIGN_BUS_NAME>
```

```
-role Sender
-group <GROUP_NAME>
}
```

#### **\$AdminConfig save**

- $\rightarrow$  Grant user or group Sender role access to the foreign destination:
  - Run the following wsadmin commands:

```
$AdminTask addUserToDestinationRole {
-type foreignDestination
-bus <BUS_NAME>
-foreignBus <FOREIGN_BUS_NAME>
-destination <DESTINATION_NAME>
-role Sender
-user <USER_NAME>
}
$AdminTask addGroupToDestinationRole {
-type foreignDestination
-bus <BUS_NAME>
```

```
2008 February, 28 IBM WebSphere Business Monitor V6.1 – End-to-end security
```

#### -foreignBus <FOREIGN\_BUS\_NAME> -destination <DESTINATION\_NAME> -role Sender -group <GROUP\_NAME> }

#### \$AdminConfig save

#### Example:

**wsadmin>** \$AdminTask addUserToForeignBusRole { -bus Monitor.<REMOTECEI\_CELL\_NAME>.Bus – foreignBus Monitor.<WBM\_CELL\_NAME>.Bus -role Sender -user wpsrvadmin }

.....

.....

wsadmin> \$AdminTask addUserToDestinationRole { -type foreignDestination -bus Monitor.<REMOTECEI\_CELL\_NAME>.Bus –foreignBus Monitor.<WBM\_CELL\_NAME>.Bus –destination wbm\_clipsbpm\_20071120175457\_Q\_Destination -role Sender –user wpsrvadmin }

.....

.....

wsadmin> \$AdminConfig save

# Troubleshooting:

#### → Problem if the LTPA security configuration across the cells is missing

If you see the following exception during the monitor model deployment, which happens while retrieving the event group profile list name during the CEI configuration:

javax.naming.NoPermissionException: NO\_PERMISSION exception caught [Root exception is org.omg.CORBA.NO\_PERMISSION: JSAS0202E: [{0}] Credential token expired. {1} vmcid: 0x49424000 minor code: 306 completed: No]

**Solution**: Ensure the LTPA authentication is configured across the WebSphere Business Monitor and WebSphere Process Server cells. For example export the LTPA key from the WebSphere Business Monitor cell and import it to WebSphere Process Server cell

# $\rightarrow$ Send access to destination denied for user (CWSIA0069E: The user does not have authorization to carry out this operation). This error occurs on the remote CEI server.

The following error occurs if the user or group sender roles are not granted to the foreign bus and the foreign destination:

SibMessage W [:] CWSII0213W: The bus MONITOR.CELL\_NAME.Bus denied the user <USER\_NAME> access to send messages to the destination wbm\_clipsbpm\_20071120175457\_Q\_Destination.

EventDistribu E com.ibm.events.distribution.impl.EventDistribution publishEventNotifications CEIES0011E The event server failed to distribute an event notification.

Exception message: CEIES0004E No event notifications were sent because the event server could not connect to the JMS destination.

Event group name: wbm\_clipsbpm\_20071120175457\_Group

JMS connection factory JNDI name: jms/wbm/clipsbpm/20071120175457/QF

JMS destination JNDI name: jms/wbm/clipsbpm/20071120175457/Q: CWSIA0069E: The user does not have authorization to carry out this operation. See the linked exception for details.

**Solution:** Grant user or group sender roles access to the foreign bus and the destination. Follow the instruction in the model deployment security configuration section of this lab.

#### → SSL HANDSHAKE FAILURE

If you see the following message on both the cells, it means that the server-to-server trust (SSL) across the WebSphere Business Monitor and the remote CEI server cells is not configured.

#### Local WebSphere Business Monitor cell:

CWPKI0022E: SSL HANDSHAKE FAILURE: A signer with SubjectDN "CN=remotecei.austin.ibm.com, O=IBM, C=US" was sent from target host:port "remotecei.austin.ibm.com:7286". The signer may need to be added to local trust store "<WBM\_PROFILE\_HOME>/config/cells/Node01Cell/nodes/Node01/trust.p12" located in SSL configuration alias "NodeDefaultSSLSettings" loaded from SSL configuration file "security.xml". The extended error message from the SSL handshake exception is: "No trusted certificate found".

#### Remote CEI Server (WebSphere Process Server) cell:

CWPKI0022E: SSL HANDSHAKE FAILURE: A signer with SubjectDN "CN=monitor61.austin.ibm.com, O=IBM, C=US" was sent from target host:port "monitor61.austin.ibm.com:7286". The signer may need to be added to local trust store "<WPS\_PROFILE\_HOME>/config/cells/Node01Cell/nodes/Node01/trust.p12" located in SSL configuration alias "NodeDefaultSSLSettings" loaded from SSL configuration file "security.xml". The extended error message from the SSL handshake exception is: "No trusted certificate found".

**Solution:** Configure server-to-server trust (SSL) across the cells. Follow the instructions from the cross cell bus prerequisite section of this document to configure the server-to-server trust (SSL) across the cells and then restart both the servers.