

Introduction

Out of the box, WebSphere Lombardi Edition installation comes configured with a single federated internal repository that provides default groups and users for Lombardi environment. You can create new users and groups in the internal repository and use the users and roles as part of the business process definition. Alternately, many organizations uses LDAP for users and group management and you would want to source the users and groups from LDAP and use it as part of your business process. You can use the internal Lombardi repository in conjunction with an external security provider (like LDAP). This tutorial describes how to configure LDAP with WLE and use it as part of Business processes.

Objectives

In this tutorial, you will learn how to:

- Setup users and groups in LDAP
- Configure LDAP with WebSphere Lombardi Edition.
- Associate LDAP Roles with WLE Process

Prerequisites

You need to be familiar with WebSphere Lombardi Edition V7.1 and Tivoli LDAP 6.3.

System requirements

You need WebSphere Lombardi Edition V7.1 and Tivoli LDAP 6.3 installed and running on any supported environment. For this tutorial, we have used Windows XP system.

Duration

2 hours

Create sample users and groups in Tivoli LDAP

In this tutorial, we will start off by creating sample users and groups in LDAP, which would be used later as part of the Business processes in WebSphere Lombardi Edition.

Follow the steps below to create sample uses and groups in LDAP

- Start the LDAP instance
 - `<LDAP_Install>/sbin/ibmslapd`

- Create a base entry for our LDAP

```
<LDAP_Install>/sbin/idsctgsuf -s dc=ibm,dc=com
```

- Load sample data (users and groups) by running the following command. Replace "cn=root" and password by your LDAP bind username and password.

ldap-sample-user-group.txt

```
<LDAP_Install/bin/ldapadd -h ldap://localhost -D "cn=root" -w  
password -f ldap-nao.ldif
```

The above command would setup Organization called Sample Org with 3 roles (BankManagerLDAP, BankOfficerLDAP and CustomerLDAP) and set of sample users in each of the group.

Configure LDAP with WebSphere Lombardi Edition

To configure LDAP with WebSphere Lombardi Edition, start the default administration server if its not already started by carrying out the following

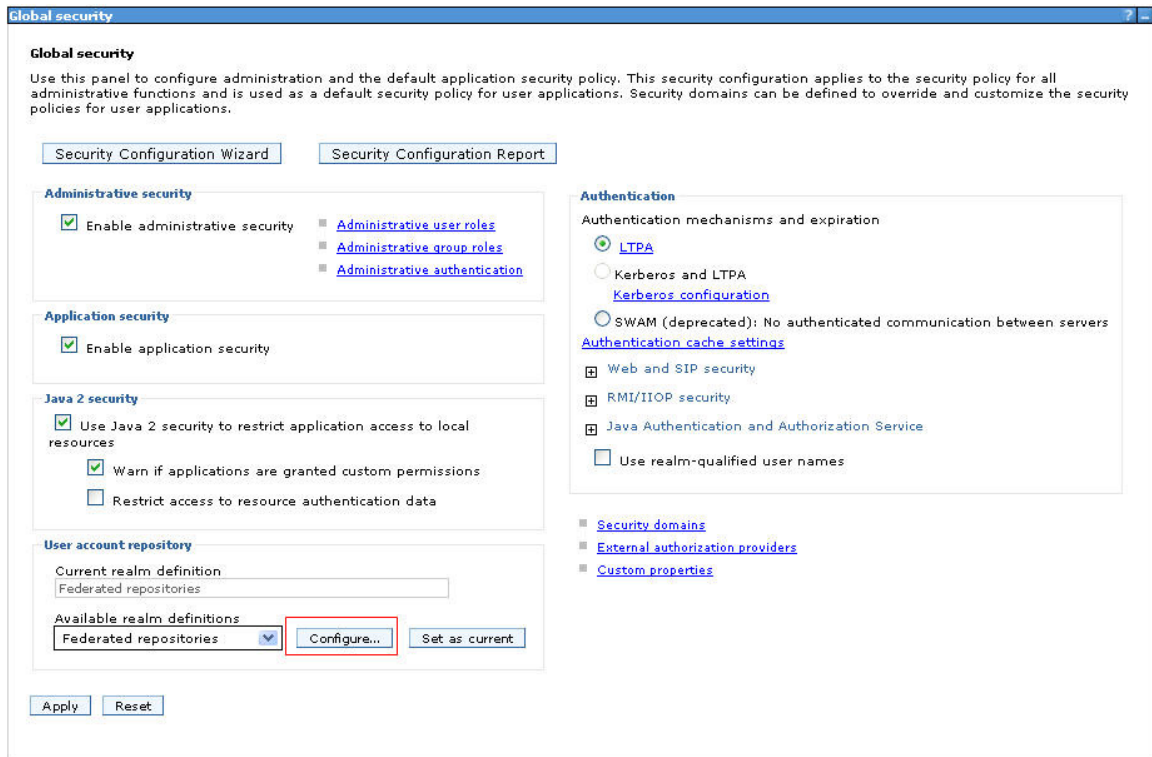
- Open up the command prompt and change directory <WLE install directory>\AppServer\profiles\Lombardi\bin.
- Next execute the command, *startserver server1*

This would start the default server which hosts the administration console. Logon to Administration console as tw_user/tw_user (Get the port number from <WLE install directory>\AppServer\profiles\Lombardi\properties\portdef.props, by looking at the property value associated with WC_adminhost property).

In the administration console, carryout out the following tasks

1. Login to WAS Administration console.
2. Go to Security > Global Security.
3. Click "Configure" for Federated Repositories in the "User account repository" section as shown in figure 1.

Figure 1.



4. Click "Manage Repositories" as shown in Figure 2.

Figure 2.



5. On the Manage repositories page, click Add as shown in figure 3 below.

Figure 3.



6. Enter the following the details as shown in figure 4.
 1. Repository Identifier: TLLDAP
 2. Directory Type: Specifies the type of LDAP server to which you connect. Select IBM Tivoli Directory Server
 3. Primary Host name: Specifies the host ID (IP address or domain name service (DNS) name) of the LDAP server
 4. Port: Specifies the host port of the LDAP server (default port is 389).
 5. Bind Distinguished Name: Specifies the DN to be used, when binding to the directory service. (Ex: cn=root)
 6. Bind password: Specifies the password to be used, when binding to the directory service (ex: password)
 7. Click Apply button at bottom of the page.

Figure 4.

[Global security](#) > [Federated repositories](#) > [Manage repositories](#) > **TLDAP**

Specifies the configuration for secure access to a Lightweight Directory Access Protocol (LDAP) repository with optional failover servers.

General Properties

* Repository identifier

TLDAP

LDAP server

* Directory type
IBM Tivoli Directory Server

* Primary host name Port
9.121.187.71 389

Failover server used when primary is not available:

Delete		
Select	Failover Host Name	Port
None		

Add

Support referrals to other LDAP servers

ignore

Security

Bind distinguished name
cn=root

Bind password

Login properties
uid

LDAP attribute for Kerberos principal name

Certificate mapping
EXACT_DN

Certificate filter

Require SSL communications

Centrally managed

▪ [Manage endpoint security configurations](#)

Use specific SSL alias

NodeDefaultSSLSettings

▪ [SSL configurations](#)

7. Click "Group attribute definition" under additional properties as shown in figure 5.

Figure 5.

General Properties

* Repository identifier

TLDAP

LDAP server

* Directory type

IBM Tivoli Directory Server

* Primary host name

9.121.187.71

Port

389

Failover server used when primary is not available:

Select	Failover Host Name	Port
<input type="checkbox"/>	None	

Add

Support referrals to other LDAP servers

ignore

Security

Bind distinguished name

cn=root

Bind password

Login properties

uid

LDAP attribute for Kerberos principal name

Certificate mapping

EXACT_DN

Certificate filter

Require SSL communications

Centrally managed

[Manage endpoint security configurations](#)

Use specific SSL alias

NodeDefaultSSLSettings

[SSL configurations](#)

Additional Properties

- [Performance](#)
- [LDAP entity types](#)
- [Group attribute definition](#)

8. On group attribute definition, click on Member attributes.

[Global security](#) > [Federated repositories](#) > [Manage repositories](#) > [TLDAP](#) > [Group attribute definition](#)

Use this page to specify the name of the group membership attribute. Every Lightweight Directory Access Protocol (LDAP) entry includes this attribute to indicate the groups to which this entry belongs.

General Properties

Name of group membership attribute

Scope of group membership attribute

- Direct - Contains only immediate members of the group without members of subgroups
- Nested - Contains direct members and members nested within subgroups of this group
- All - Contains all direct, nested, and dynamic members

Apply OK Reset Cancel

Additional Properties

- [Member attributes](#)
- [Dynamic member attributes](#)

9. On the Member attributes page. Click New.
10. Enter the following information as shown in Figure 6. This entry provides details on how to retrieve user information associated with the Group. This is based on data that we had populated in Section 2 .
 - In Name of member attribute enter: uniquemember
 - In object class enter: groupOfUniqueNames
 - Click OK.

Figure 6.

[Global security](#) > [Federated repositories](#) > [TLDAP](#) > [Group attribute definition](#) > [Member attributes](#) > [uniquemember](#)

Use this page to manage Lightweight Directory Access Protocol (LDAP) member attributes.

General Properties

* Name of member attribute
uniquemember

Object class
groupOfUniqueNames

Scope

Direct - Contains only immediate members of the group without members of subgroups

Nested - Contains direct members and members nested within subgroups of this group

All - Contains all direct, nested, and dynamic members

Note – Following is the sample LDAP entry that we had populated, that matches the above screen.

```
dn: cn=CustomerLDAP,ou=groups,DC=IBM,DC=COM  
  
objectClass: groupOfUniqueNames  
  
objectClass: top  
  
cn: CustomerLDAP  
  
uniquemember: uid=SamLDAP,ou=people,DC=IBM,DC=COM
```

11. Click LDAP entity types under additional properties as shown in figure 7

Figure 7.

Additional Properties

- [Performance](#)
- [LDAP entity types](#)
- [Group attribute definition](#)

12. Click Group on the LDAP entity type page. We need to change the objectClass to map it with our entity type in LDAP.

13. On the Group page, replace the Object Class with following values as shown in Figure 8. i.e groupOfNames;groupOfUniqueNames

Figure 8

The screenshot shows a web browser window titled "Global security". The breadcrumb navigation is "Global security > Federated repositories > TLDAP > LDAP entity types > Group". Below the breadcrumb is a description: "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." The "General Properties" section contains several fields: "Entity type" (Group), "Object classes" (groupOfNames;groupOfUniqueNames), "Search bases", and "Search filter". At the bottom are buttons for "Apply", "OK", "Reset", and "Cancel".

14. Click OK button

15. On the Group page, click "Federated Repositories" on the top navigation link

16. Click Add Base entry to Realm... button as shown in figure 9

Figure 9.

Ignore case for authorization

Repositories in the realm:

<input type="button" value="Add Base entry to Realm..."/>		<input type="button" value="Use built-in repository"/>	<input type="button" value="Remove"/>
Select	Base entry	Repository identifier	Repository type
<input type="checkbox"/>	o=defaultWIMFileBasedRealm	InternalFileRepository	File

17. Enter the following the details as shown in figure 10.
 1. Repository: TLDAP
 2. Distinguished name of a base entry that uniquely identifies this set of entries in the realm: dc=IBM,dc=COM (The entry was populated in LDAP in Section 2)
 3. Click OK

Figure 10.

Global security

Global security > Federated repositories > 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.

General Properties

* Repository
TLDAP

* Distinguished name of a base entry that uniquely identifies this set of entries in the realm
dc=ibm,dc=com

Distinguished name of a base entry in this repository

18. Save the changes to Master configuration.
19. Stop and Start the server.

Associate LDAP Roles in WLE Process

As part of your business process you would have defined activity that needs to be completed by a human. The human activity is assigned to a group and/or users. The groups and users can come from the internal Lombardi repository or an external provider like LDAP.

There are 2 ways by which you can associate users and groups from LDAP to WLE process, one is via the Lombardi Authoring environment and other is via the Process Administration console. The Process Administration console would be typically used when you have deployed the process and it's up and running and want to declaratively associate Roles with the processes.

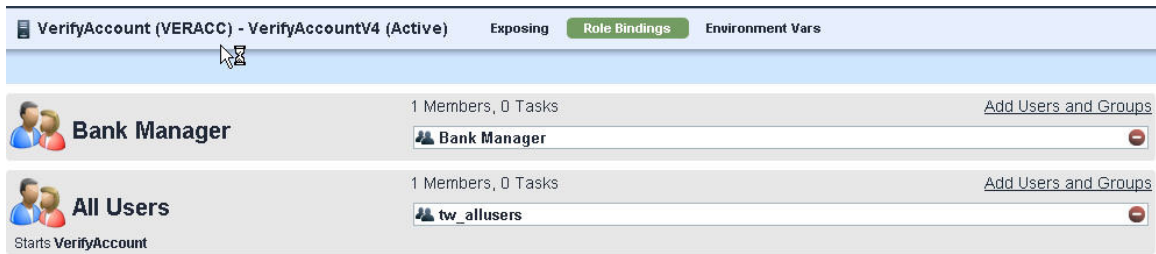
For associating LDAP roles with processes in Lombardi Authoring environment carryout the following tasks

1. Logon to WLE Authoring environment
2. Select the required process application and Business process definition
3. Select the participant group in your process that you want to associate an LDAP group. For instance, in the example shown below we show how to add the BankMangerLDAP to Bank Manager Participant group.
4. On the Participant Group page, click on Add Group.
 - In the pop up window, type BankManager as shown in the figure below and click on it to add it to Member list.
 - Save the work.



For associating LDAP roles with processes in Process Administration console carryout the following tasks

- Logon to Lombardi Process Administration console using tw_admin/tw_admin
- Click on InstalledApps
- Click on Selected Process. For instance, in the example we select an existing VerifyAccount process.
- Click on Role Binding



- Click on Add Users and Groups next to Bank Manager. On the Add People to Bank Manager Role screen, type in bank in the retrieve text box and select BankManagerLDAP option and click Add.
- Save the process.

Conclusion

This tutorial discussed how to configure LDAP with WLE and use it part of the Business process. As part of the tutorial we created sample users and groups in LDAP and used the groups as part of WLE processes.