Business Process Manager - Security

Sridhar Edam (sedam@us.ibm.com)
Dhamu Veluswamy (dveluswa@us.ibm.com)

11/20/2012

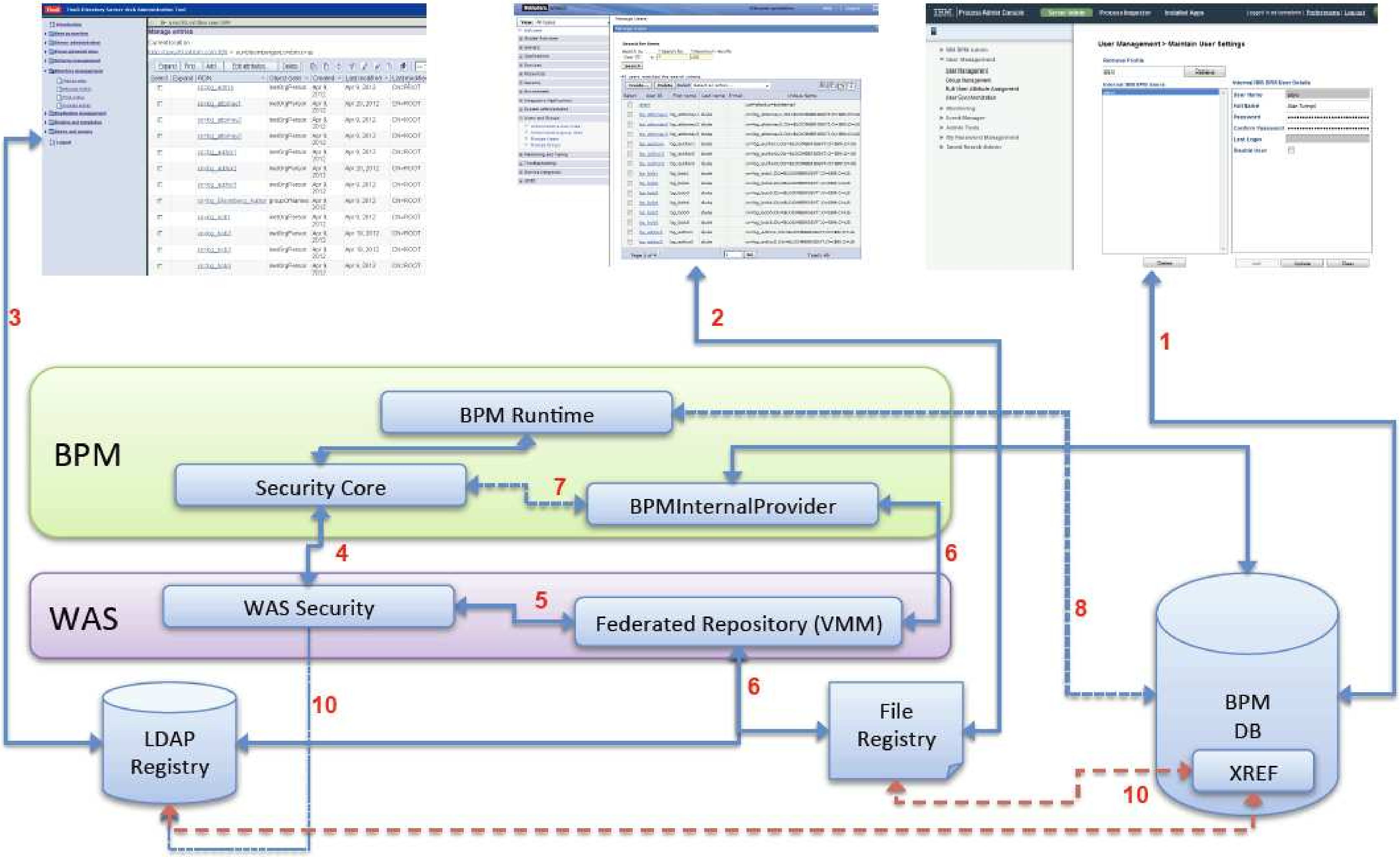
Agenda

- Overview
- Authentication - Who has access
  - Supported Configurations
  - Tivoli LDAP , HTTP Server
- Authorization - Access to what
  - Users and Groups
- Common security considerations
- Troubleshooting
- Q&A

Panel of Experts

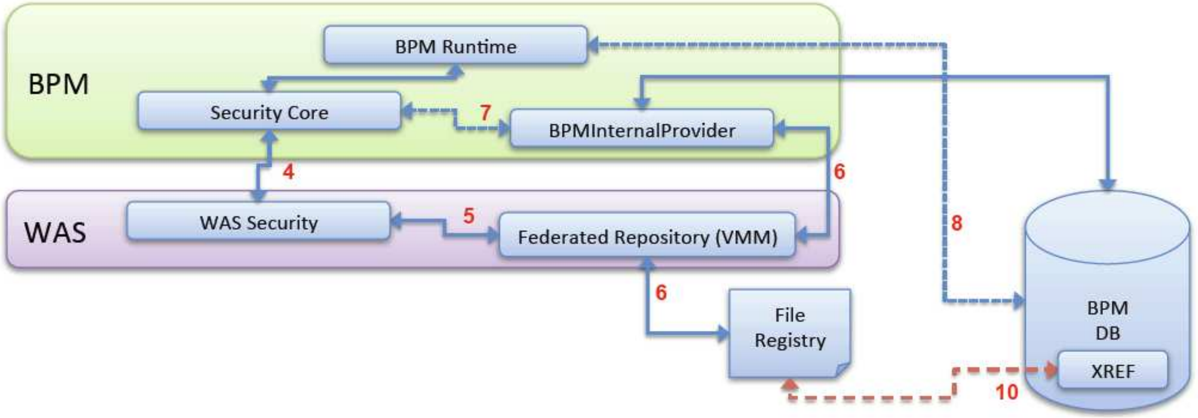
Sridhar Edam	Sridhar Edam has been a long time support engineer for IBM BPM Products and has very good understanding of the architecture , design and operational aspects of the BPM Products.
Dhamu Veluswamy	Dhamu Veluswamy has been working in WebSphere Support team for several year. In this role, he is responsible for customer support for WebSphere Adapters and Business Process Manager. He has good understating of Business Process Manager and its design.

Overview - Complexity



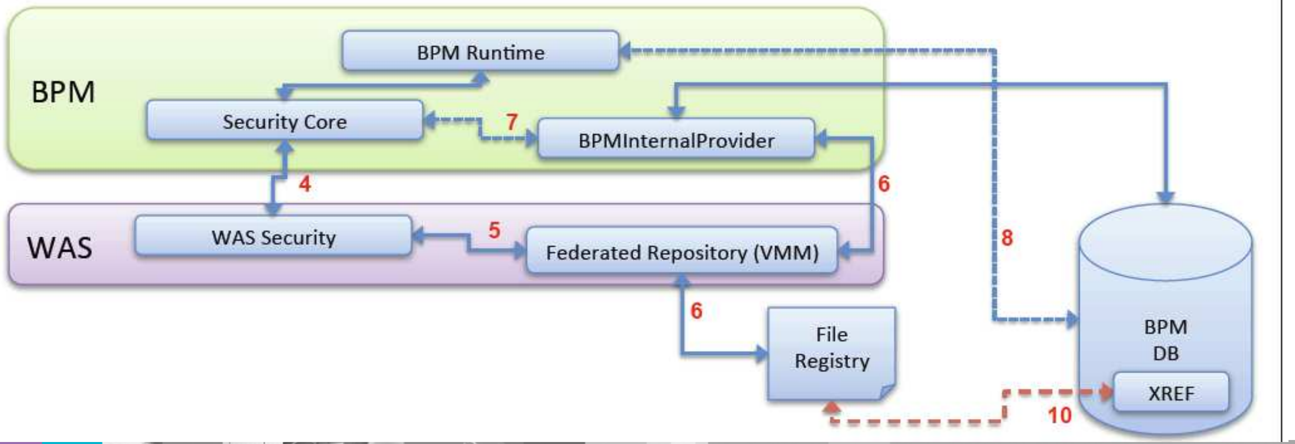
Default Configuration

- By default, BPM is configured with Federated repositories (VMM)
    - This is the RECOMMENDED CONFIGURATION
- Standalone servers have two repositories in the federation
- Network Deployment environments by default only have one
- Internal Security Provider: Code which allows login to WAS for users that have been created in the BPM database



Typical Configuration

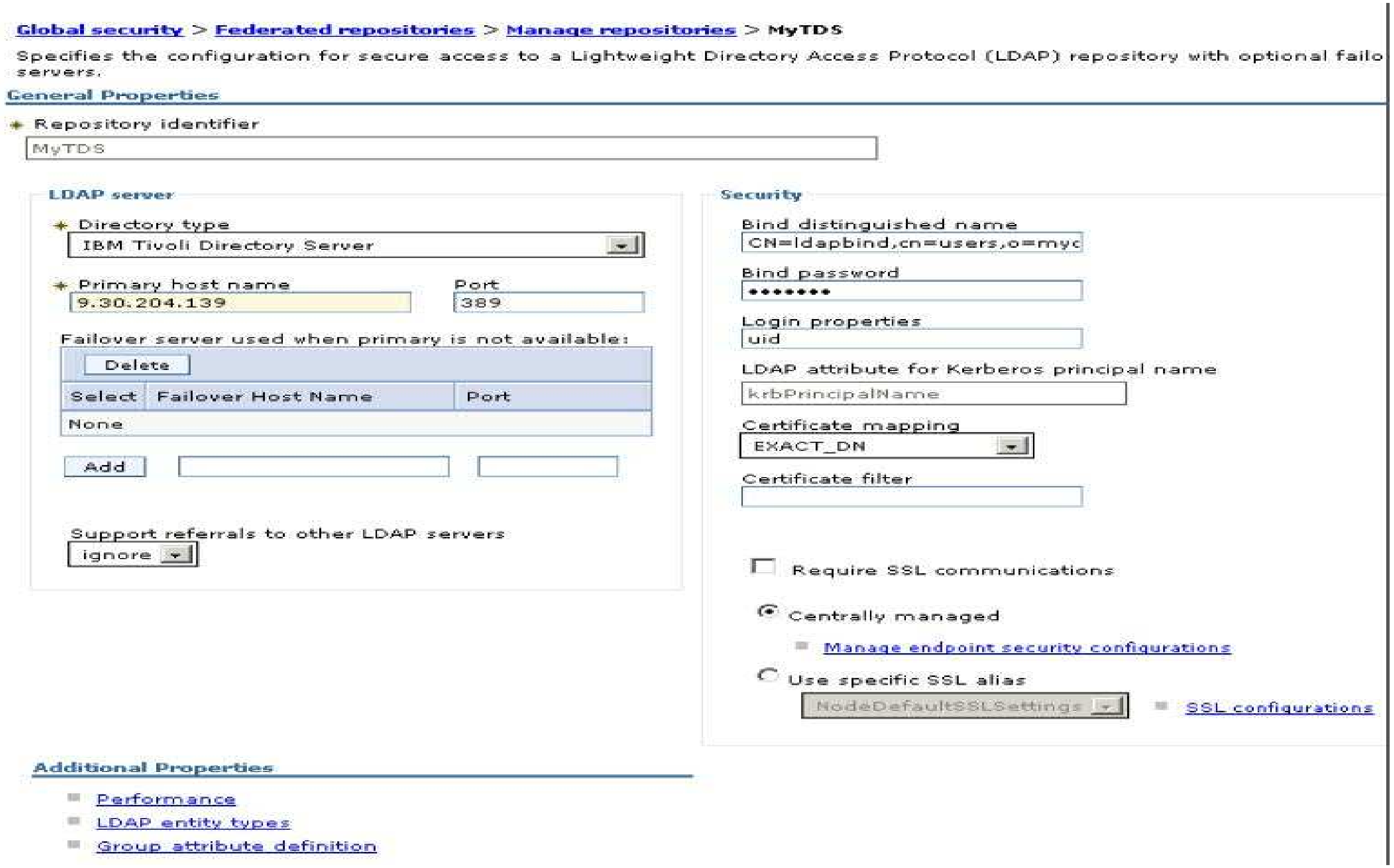
- Most customers have an LDAP repository
  - No need for internal user management: the internal security provider can be removed
- Business users are maintained in LDAP
- A number of default users are “BPM Specific”
  - Some customers don’t want them in LDAP
  - The file-based repository can be used instead
- This allows admins to login, when LDAP is down



Supported Configuration

- There are many additional options, such as
  - Standalone LDAP configuration
  - (Discouraged: there is no reason to do that)
  - Federated Repositories with one or more LDAPs federated, no file-based repository
  - Custom User Registry
  - Others
- Note that some features in BPM require Federated Repositories
  - Substitution in Human Task Manager (Advanced Edition only)
  - User Chooser in Business Space (e.g. searching by last name)

Tivoli LDAP



Global security > Federated repositories > Manage repositories > MyTDS

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

General Properties

* Repository identifier: MyTDS

LDAP server

* Directory type: IBM Tivoli Directory Server

* Primary host name: 9.30.204.139

Port: 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=ldapbind,cn=users,o=myc

Bind password: •••••••

Login properties: uid

LDAP attribute for Kerberos principal name: krbPrincipalName

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

Tivoli LDAP

- log into admin console
  - **Security->Global Security-> Federated Repository -> Configure->Manage Repositories -**

    >Add

    Bind distinguished name : CN=ldapbind,cn=users,o=mycompany.org

    Bind password: ldapbind

    Save the setting.

    Go back to this repository and click on LDAP entity types

    Make sure you have the same value:
- **Go to Security->Global Security-> Federated Repository -> Configure->Add Base Entry to Realm**
  - Choose the repository which was created in previous step. In this case "MyTDS"

    apply and ok. Restart server.

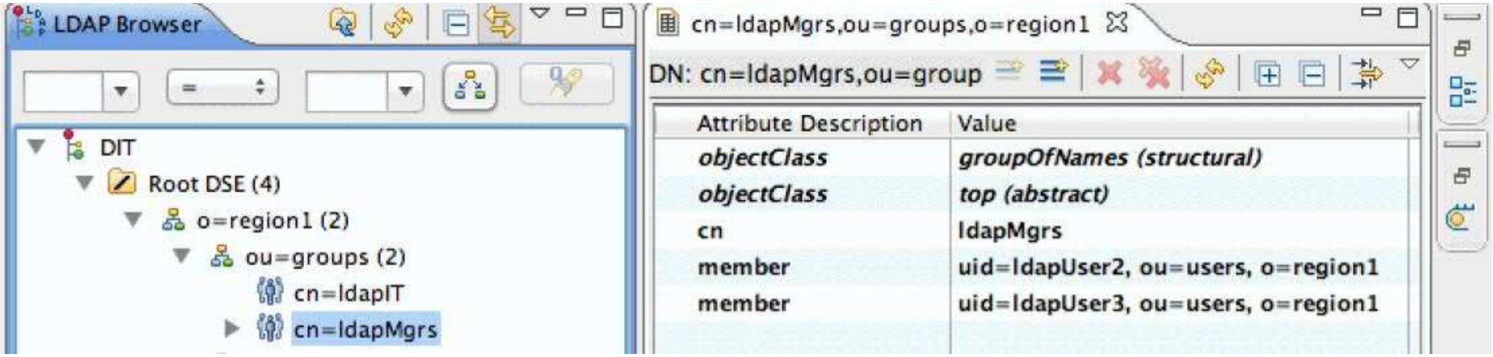
IBM HTTP Server

- Add HTTP server to the WAS configuration.
- Generate the web server plug-in
- Map application modules to route through HTTP server.
- Customize the 100Custom.xml to point to the web server

```
authoring-environment merge="mergeChildren">
    <!--
       Prefix for serving images in the Authoring Environment
    -->
    <images-prefix merge="replace">http://My2008.usca.ibm.com/teamworks</images-prefix>

    <!-- Prefix for urls that refer to the portal -->
    <portal-prefix merge="replace">http://My2008.usca.ibm.com/portal</portal-prefix>

    <!-- Prefix for urls that refer to the repository view -->
    <repository-prefix merge="replace">http://My2008.usca.ibm.com/ProcessCenter</repository-prefix>

    <servlet-prefix merge="replace">http://My2008.usca.ibm.com/teamworks</servlet-prefix>

    <!-- Prefix for urls that refer to the webapi -->
    <webapi-prefix merge="replace">http://My2008.usca.ibm.com/webapi</webapi-prefix>

    <process-help-wiki-url-view
    merge="replace">http://My2008.usca.ibm.com/processhelp/en/%TITLE%?teamworksTitle=%TEAMWORKS_TITLE%</process-help-wiki-url-view>
    <process-help-wiki-url-edit
    merge="replace">http://My2008.usca.ibm.com/processhelp/en/Special:Edit?topic=%TITLE%&amp;teamworksTitle=%TEAMWORKS_TITLE%</process-help-wiki-url-edit>

  </authoring-environment>
```

Authorization: Groups

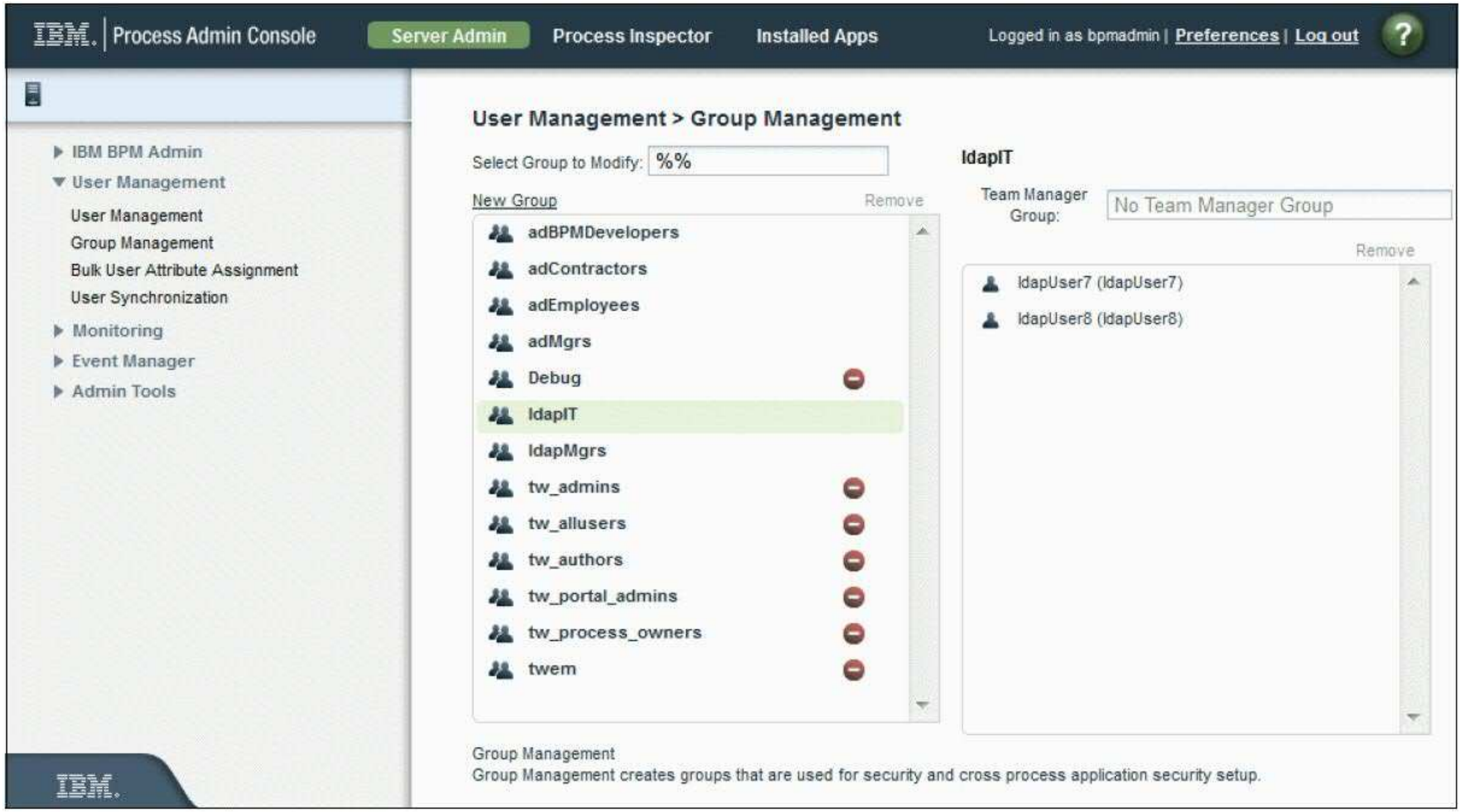
- Groups versus roles
- Grouping mechanisms
  - LDAP groups
  - VMM security groups



DN: cn=ldapMgrs,ou=group

Attribute Description	Value
objectClass	*groupOfNames (structural)*
objectClass	*top (abstract)*
cn	ldapMgrs
member	uid=ldapUser2, ou=users, o=region1
member	uid=ldapUser3, ou=users, o=region1

Authorization: Process Admin groups



User Management > Group Management

Select Group to Modify: %%

New Group

Remove

- adBPMDevelopers
- adContractors
- adEmployees
- adMgrs
- Debug
- ldapIT
- ldapMgrs
- tw_admins
- tw_allusers
- tw_authors
- tw_portal_admins
- tw_process_owners
- twem

ldapIT

Team Manager Group: No Team Manager Group

Remove

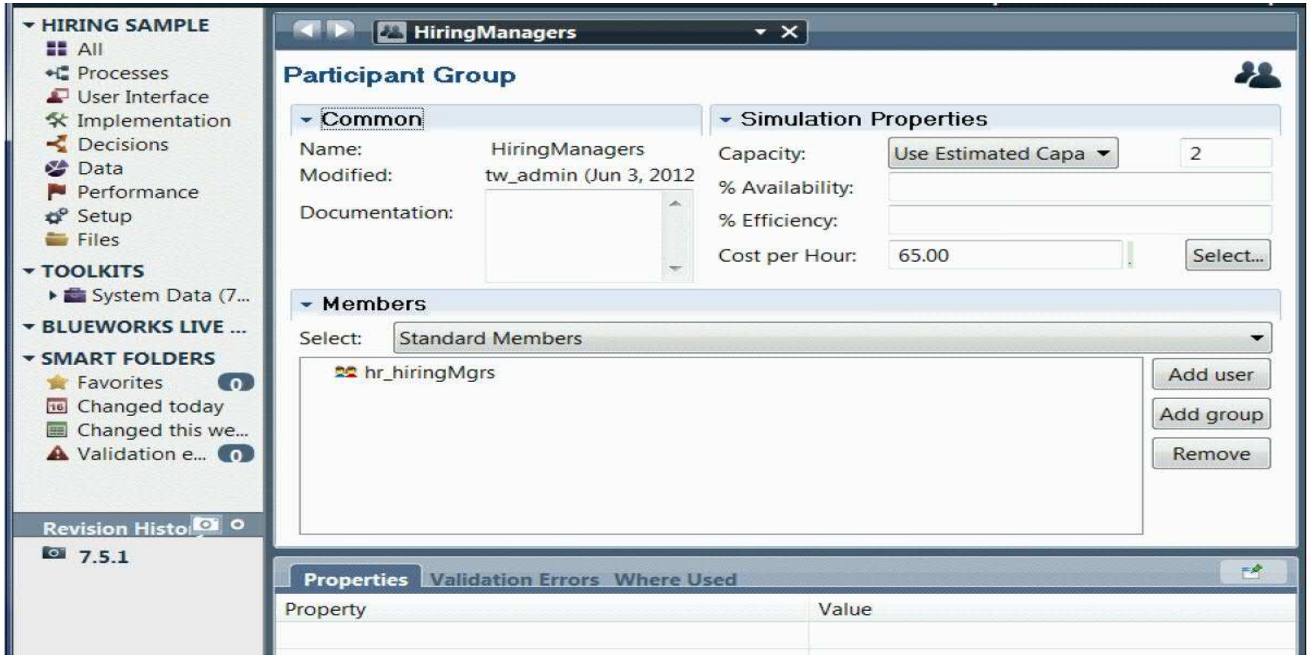
- ldapUser7 (ldapUser7)
- ldapUser8 (ldapUser8)

Group Management

Group Management creates groups that are used for security and cross process application security setup.

Authorization: Participant Groups

- Process Designer Swimlanes are authorized for a participant group
- Participant group users receive work items of their swimlane activities
- Role binding for a participant group is associated with process admin groups.



Participant Group

Common

Name: HiringManagers
Modified: tw_admin (Jun 3, 2012
Documentation:

Simulation Properties

Capacity: Use Estimated Capa 2
% Availability:
% Efficiency:
Cost per Hour: 65.00

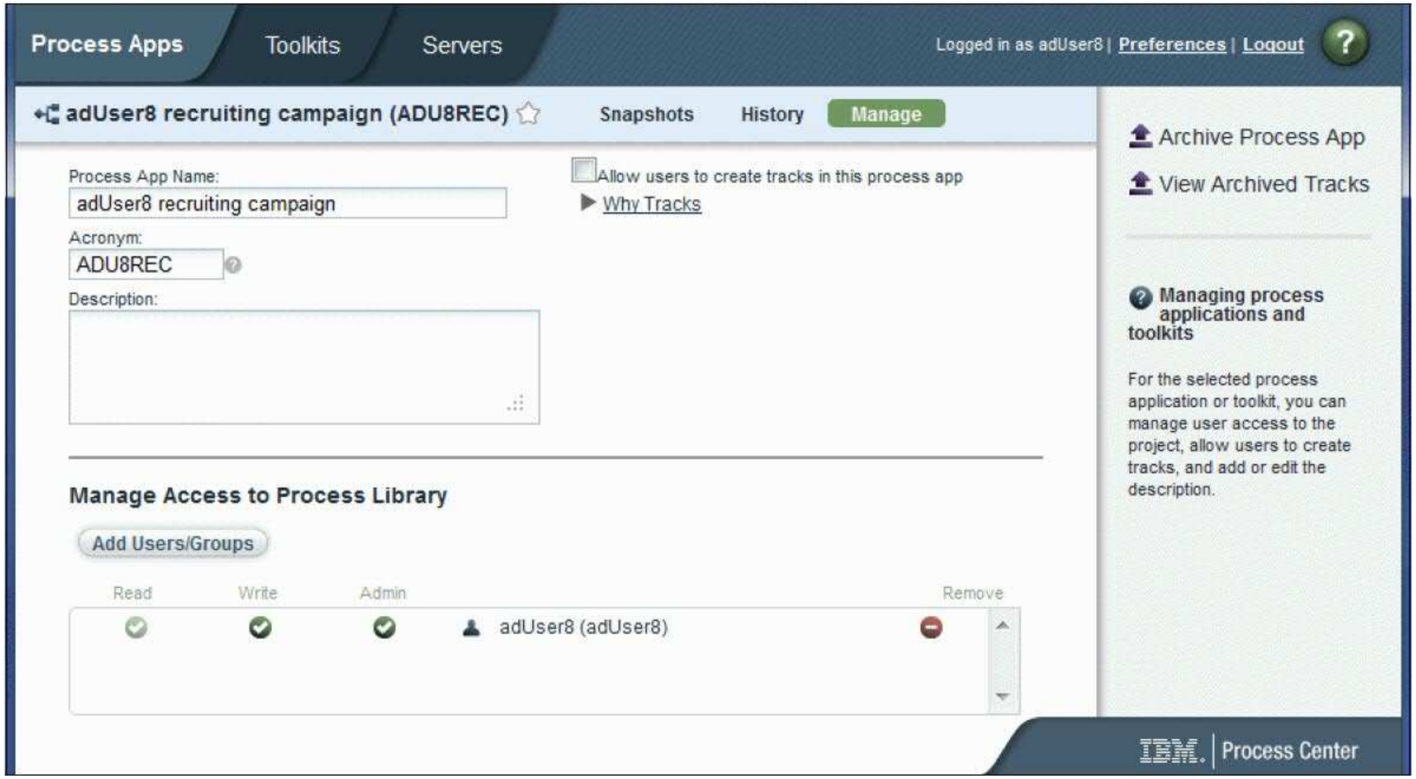
Members

Select: Standard Members

hr_hiringMgrs

Property	Value

Authorization: Process App Access



adUser8 recruiting campaign (ADU8REC)

Process App Name: adUser8 recruiting campaign

Acronym: ADU8REC

Description:

□ Allow users to create tracks in this process app

▶ Why Tracks

Manage Access to Process Library

Add Users/Groups

Read	Write	Admin		Remove
✓	✓	✓	adUser8 (adUser8)	⊖

Archive Process App

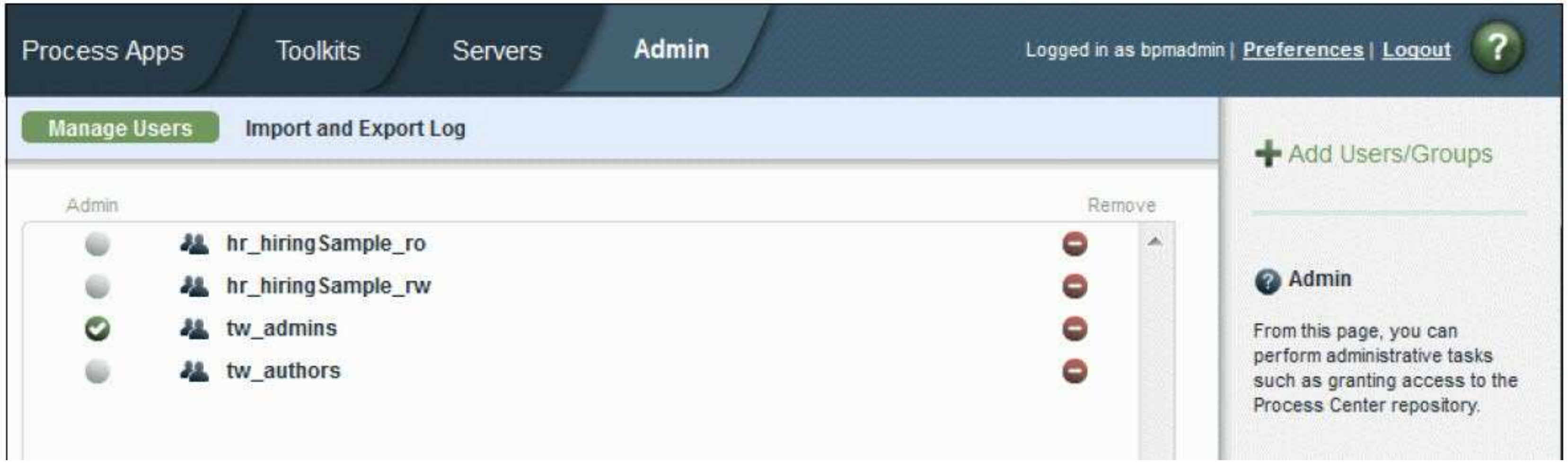
View Archived Tracks

Managing process applications and toolkits

For the selected process application or toolkit, you can manage user access to the project, allow users to create tracks, and add or edit the description.

Authorization: Process Designer

- A user with full administrative rights to the /ProcessCenter can grant Process Designer access
- This can be done on /ProcessCenter Admin tab , by adding the appropriate group / user.



Admin		Remove
○	hr_hiringSample_ro	⊖
○	hr_hiringSample_rw	⊖
✓	tw_admins	⊖
○	tw_authors	⊖

Admin

From this page, you can perform administrative tasks such as granting access to the Process Center repository.

Common security holes with authorization

- Overuse of administrator privileges
- Failure to map participant groups
- Overpopulation of groups
- Overuse of tw_authors, tw_admins
- Faith in firewalls

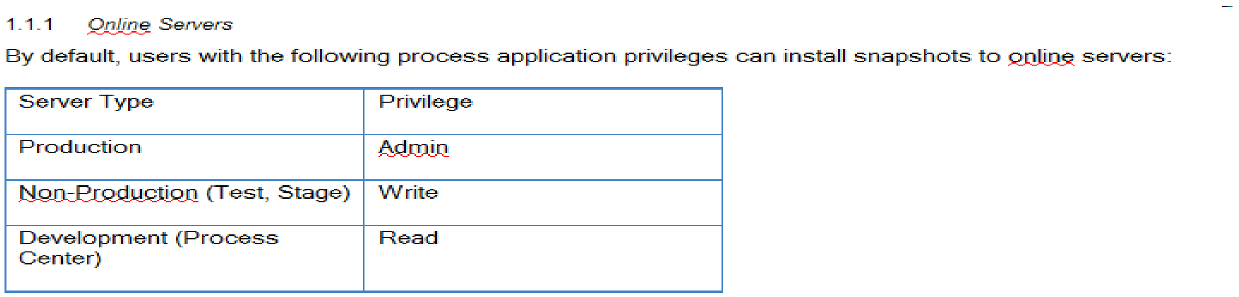
Common security holes with authentication

- Weak password policies
- Failure to change default passwords
- Faith in firewalls
- Insecure LDAP connections
- Insecure SSO solutions

Common security considerations

- Firewalls
- SSL between BPM and database server
- SSL between Process Center and Process Server
- Encrypt data at rest
- Change - default BPM accounts
- Change - trust in certificate authorities

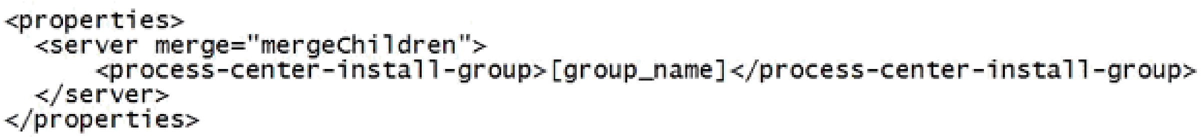
Q&A - Who can install to process server



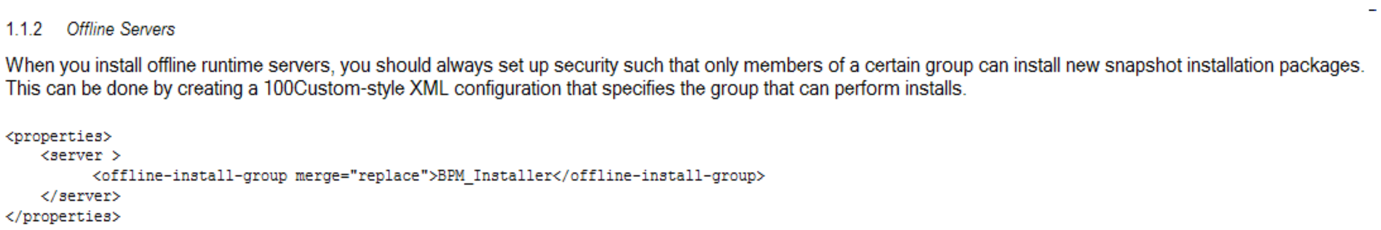
1.1.1 *Online Servers*

By default, users with the following process application privileges can install snapshots to online servers:

Server Type	Privilege
Production	Admin
Non-Production (Test, Stage)	Write
Development (Process Center)	Read



```
<properties>
  <server merge="mergeChildren">
      <process-center-install-group>[group_name]</process-center-install-group>
  </server>
</properties>
```



1.1.2 *Offline Servers*

When you install offline runtime servers, you should always set up security such that only members of a certain group can install new snapshot installation packages. This can be done by creating a 100Custom-style XML configuration that specifies the group that can perform installs.

```
<properties>
    <server >
          <offline-install-group merge="replace">BPM_Installer</offline-install-group>
    </server>
</properties>
```

Q&A – How to secure portal functions to a set of users

- Done through changes in 100Custom.xml
- Eg: <portal> <default-action-policy> <action type="ACTION_REASSIGN_TASK_USER_ROLE" merge="replace"> <role>project_managers</role> </action> </default-action-policy> </portal>
- http://publib.boulder.ibm.com/infocenter/dmndhelp/v7r5m1/index.jsp?topic=%2Fcom.ibm.wbpm.admin.doc%2Ftopics%2Frestricting_access_to_portal_functions.html

Q&A – Password change and issues

- http://publib.boulder.ibm.com/infocenter/dmndhelp/v7r5m1/index.jsp?topic=%2Fcom.ibm.wbpm.imuc.ebpm.doc%2Ftopics%2Ftchanging_admin_password.html

- Check for the db2admin password expiry and change the J2C Authentication aliases accordingly

- Copy the old password from the db to the password field of LSW_USERS tables

Summary

References and Useful Links (Optional)

- Reference 1:
  http://www.ibm.com/developerworks/websphere/community/

- Reference 2:
  http://www.ibm.com/software/websphere/events_1.html

- Reference 3:
  http://www.websphere.org

- Reference 4:
  http://www.ibm.com/software/info/education/assistant

- Reference 5:
  http://www.ibm.com/software/websphere/support/d2w.html

- Reference 6:
  http://www.redbooks.ibm.com/redbooks/pdfs/sg248027.pdf

Additional WebSphere Product Resources

- Learn about upcoming WebSphere Support Technical Exchange webcasts, and access previously recorded presentations at: http://www.ibm.com/software/websphere/support/supp_tech.html
- Discover the latest trends in WebSphere Technology and implementation, participate in technically-focused briefings, webcasts and podcasts at: http://www.ibm.com/developerworks/websphere/community/
- Join the Global WebSphere Community: http://www.websphereusergroup.org
- Access key product show-me demos and tutorials by visiting IBM® Education Assistant: http://www.ibm.com/software/info/education/assistant
- View a webcast replay with step-by-step instructions for using the Service Request (SR) tool for submitting problems electronically: http://www.ibm.com/software/websphere/support/d2w.html
- Sign up to receive weekly technical My Notifications emails: http://www.ibm.com/software/support/einfo.html

Connect with us!

1. **Get notified on upcoming webcasts**
   Send an e-mail to wsehelp@us.ibm.com with subject line “wste subscribe” to get a list of mailing lists and to subscribe
2. **Tell us what you want to learn**
   Send us suggestions for future topics or improvements about our webcasts to wsehelp@us.ibm.com
3. **Be connected!**
   Connect with us on Facebook
   Connect with us on Twitter

Questions and Answers