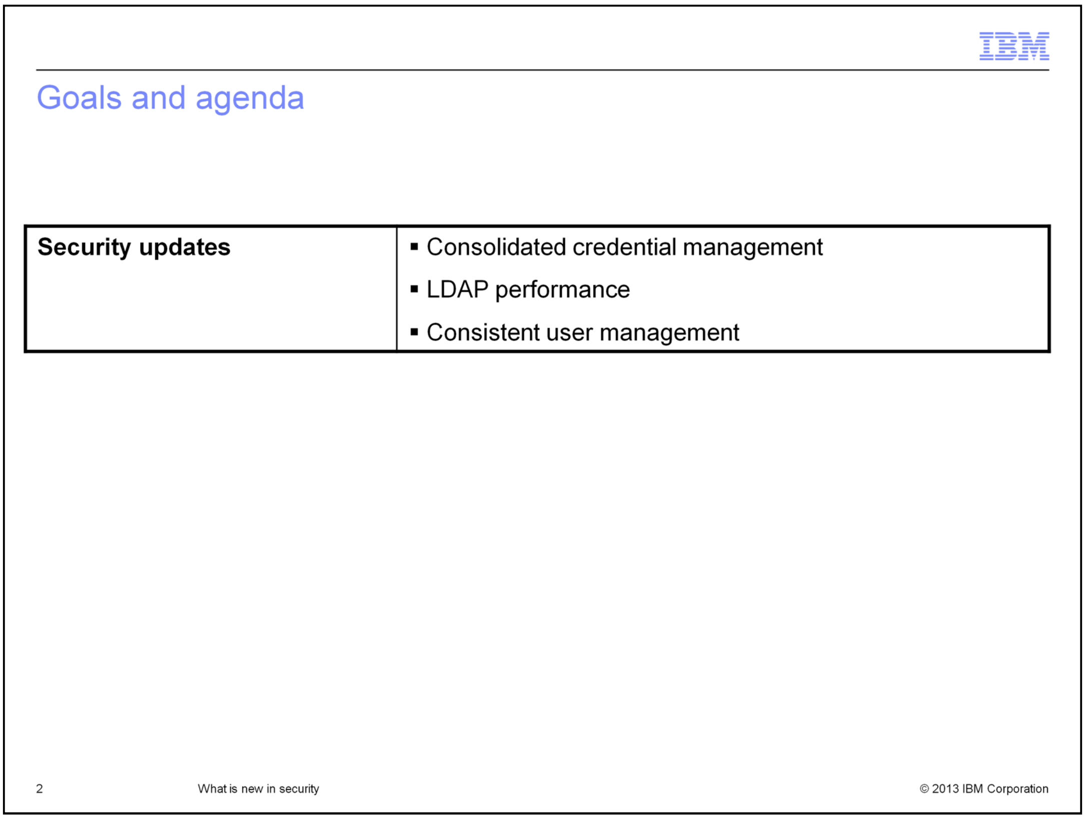
IBM Business Process Manager V8.5

What is new in security

This presentation introduces the new and enhanced security features in IBM Business Process Manager V8.5.

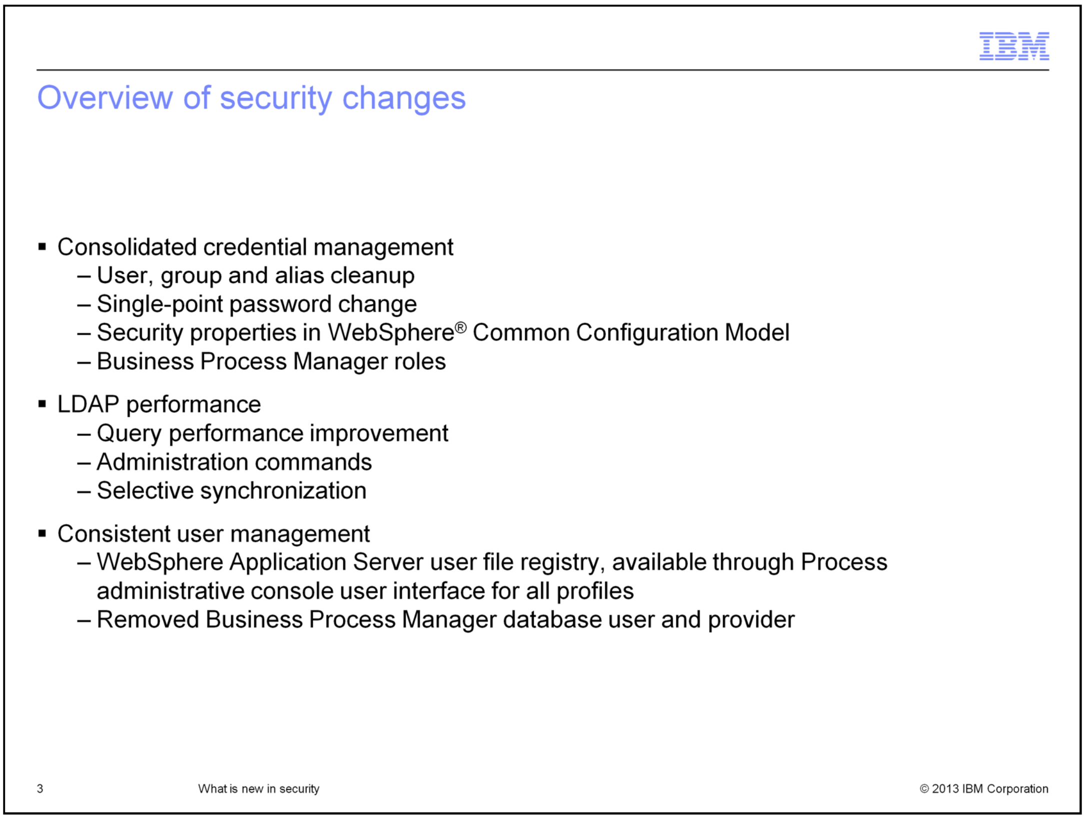


Goals and agenda

Security updates	▪ Consolidated credential management ▪ LDAP performance ▪ Consistent user management

2 What is new in security © 2013 IBM Corporation

This presentation is the second part of the presentation series on what is new in installation, configuration, and migration in IBM Business Process Manager V8.5. It covers the new and enhanced security capabilities in V8.5. These new enhancements allow you to set up and manage more secure user access to applications.



IBM

Overview of security changes

- Consolidated credential management
  - User, group and alias cleanup
  - Single-point password change
  - Security properties in WebSphere® Common Configuration Model
  - Business Process Manager roles
- LDAP performance
  - Query performance improvement
  - Administration commands
  - Selective synchronization
- Consistent user management
  - WebSphere Application Server user file registry, available through Process administrative console user interface for all profiles
  - Removed Business Process Manager database user and provider

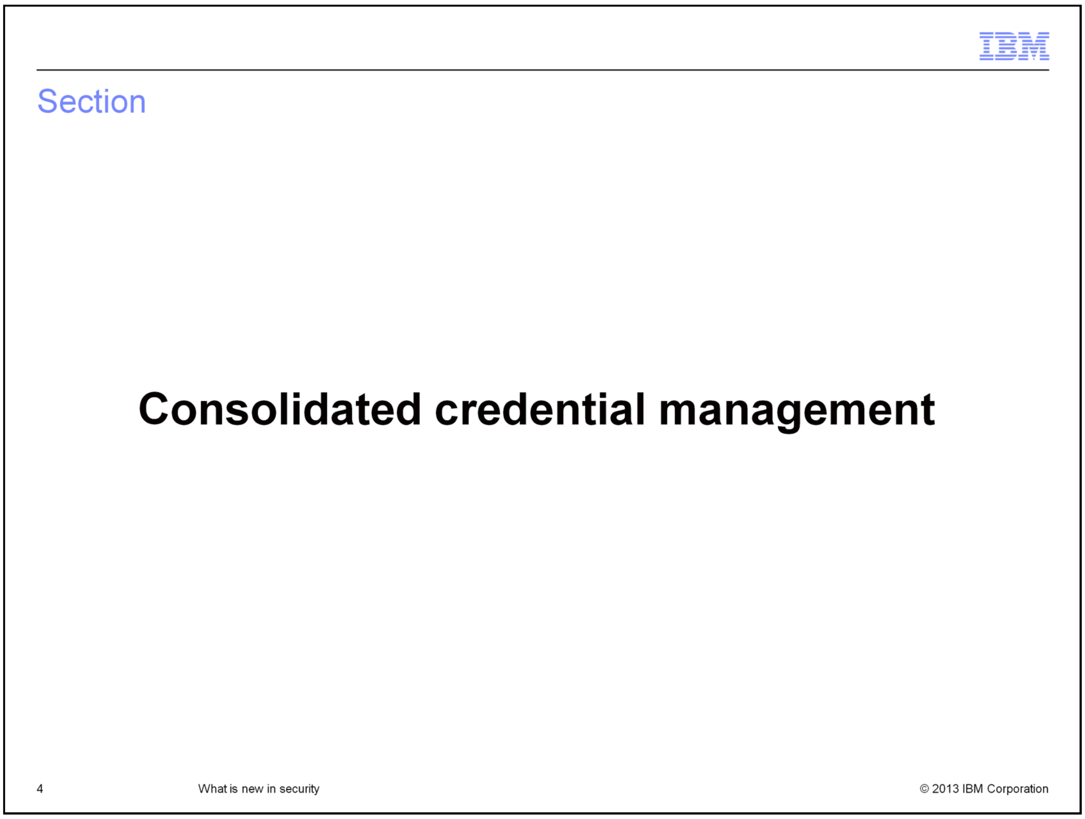
3 What is new in security © 2013 IBM Corporation

The security changes in IBM Business Process Manager V8.5 are focused on simplification of security configuration and improving performance and user-response for customers who use large user repositories, such as LDAP. The improvements are provided by new features in these three areas.

The first improvement is the consolidated credential management. The number of default users has been simplified and reduced, you are now allowed to rename the built-in groups, and the number of aliases has been reduced. There is a new command that enables you to change all user passwords from one place, instead of having to use multiple user interfaces for alias and runAs roles. Security properties have been moved from XML configuration files to WebSphere Common Configuration Model of WebSphere Application Server. And a set of Business Process Manager roles has been introduced to define various capabilities for Business Process Manager users.

As for LDAP performance, the response time for searches in the LDAP directory has been improved by changes in the way that wildcards are used. Administrative commands have been introduced to synchronize users and groups with LDAP. And there is now a way to synchronize only known users, in addition to a synchronizing a specific list or all users.

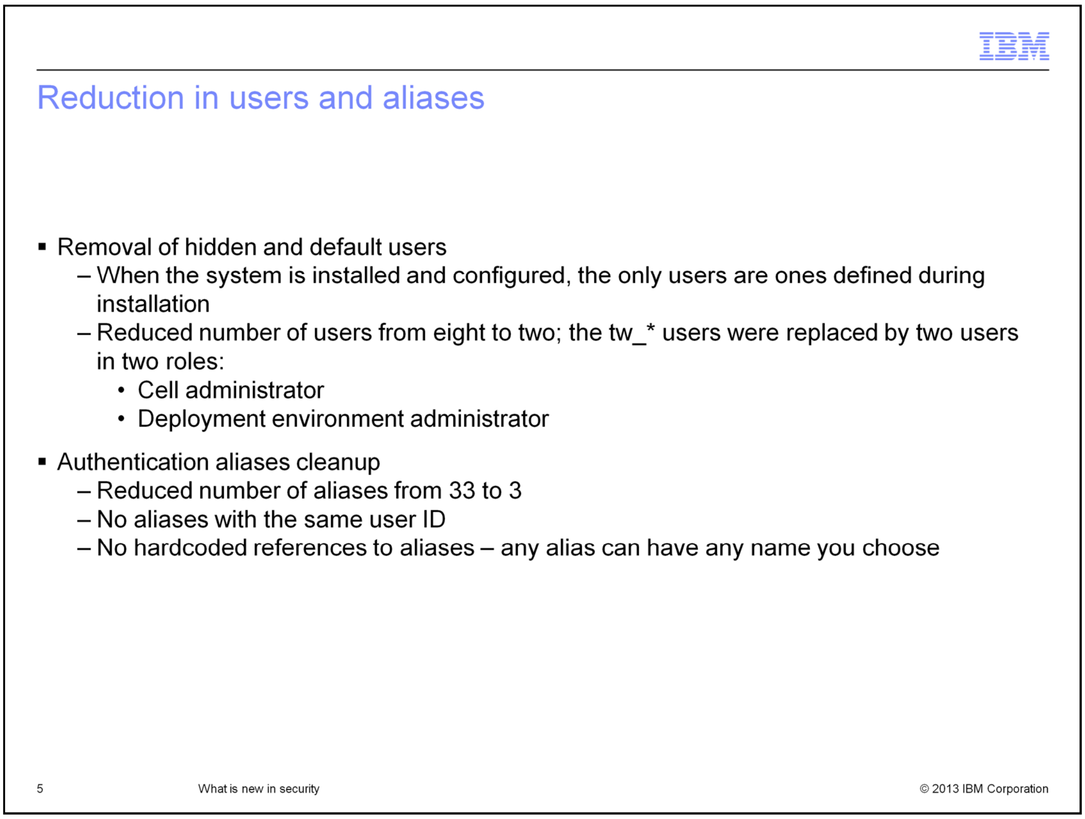
The last improvement area is consistent user management. The internal database-based user registry has been replaced with the built-in WebSphere Application Server file registry. The same user interface is used to manage users in that registry.



Section

Consolidated credential management

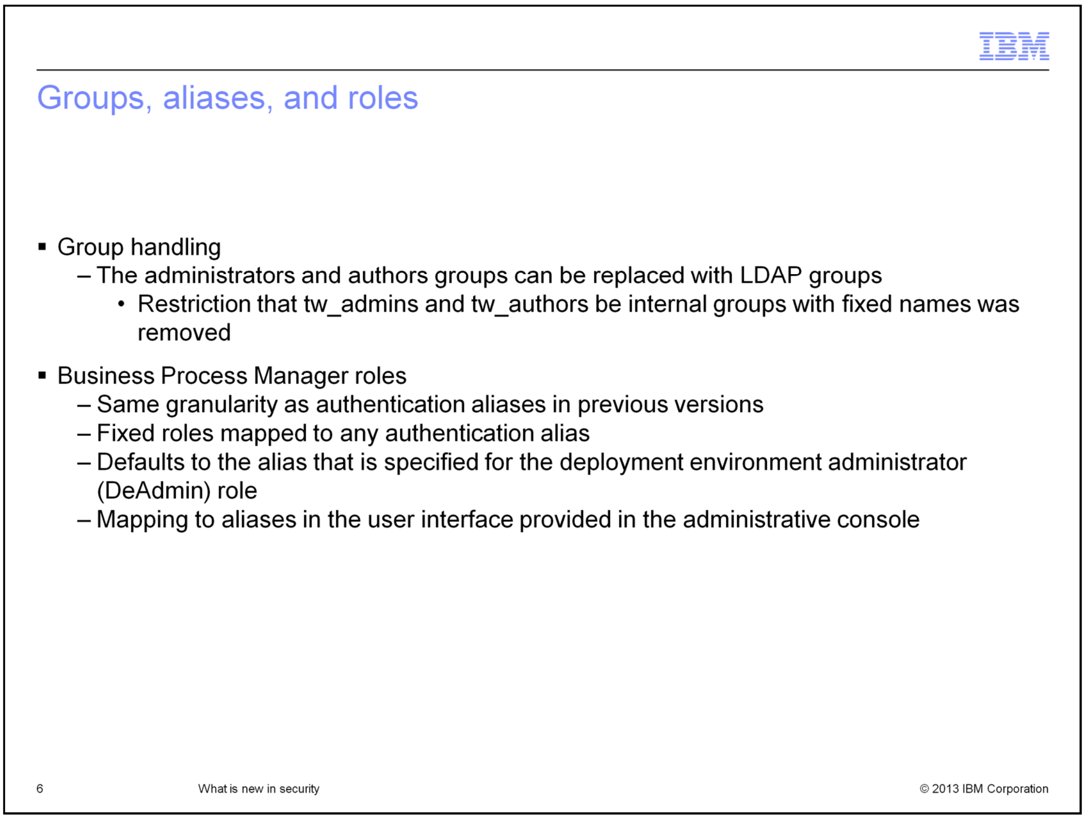
This section describes in more detail consolidated credential management.



Reduction in users and aliases

- Removal of hidden and default users
  - When the system is installed and configured, the only users are ones defined during installation
  - Reduced number of users from eight to two; the tw_* users were replaced by two users in two roles:
    - Cell administrator
    - Deployment environment administrator
- Authentication aliases cleanup
  - Reduced number of aliases from 33 to 3
  - No aliases with the same user ID
  - No hardcoded references to aliases – any alias can have any name you choose

In IBM Business Process Manager V8.5, a reduction in the number of users and aliases and the removal of all default users improves the security of the product.

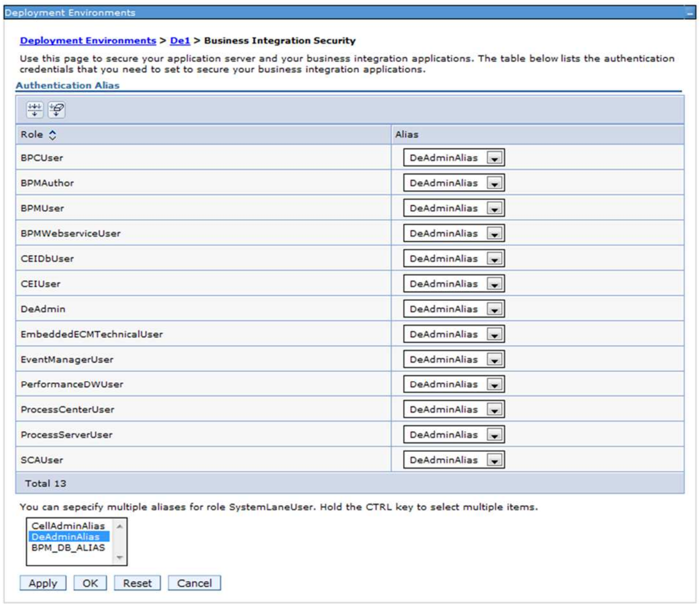


Groups, aliases, and roles

- Group handling
  - The administrators and authors groups can be replaced with LDAP groups
    - Restriction that tw_admins and tw_authors be internal groups with fixed names was removed
- Business Process Manager roles
  - Same granularity as authentication aliases in previous versions
  - Fixed roles mapped to any authentication alias
  - Defaults to the alias that is specified for the deployment environment administrator (DeAdmin) role
  - Mapping to aliases in the user interface provided in the administrative console

The groups in IBM Business Process Manager V8.5 remain the same as in V8.0.1. However, in V8.5, they can be changed to either be different internal groups or groups defined in an external security provider, such as a federated LDAP. The fixed aliases that are used in V8.0.1 have been replaced by Business Process Manager roles, allowing you to modify the alias names to meet your standards. Since there are only three aliases defined initially, all the other roles default to the alias that are specified for the deployment environment administrator role.

Role-to-alias mapping



Deployment Environments > De1 > Business Integration Security

Use this page to secure your application server and your business integration applications. The table below lists the authentication credentials that you need to set to secure your business integration applications.

Authentication Alias

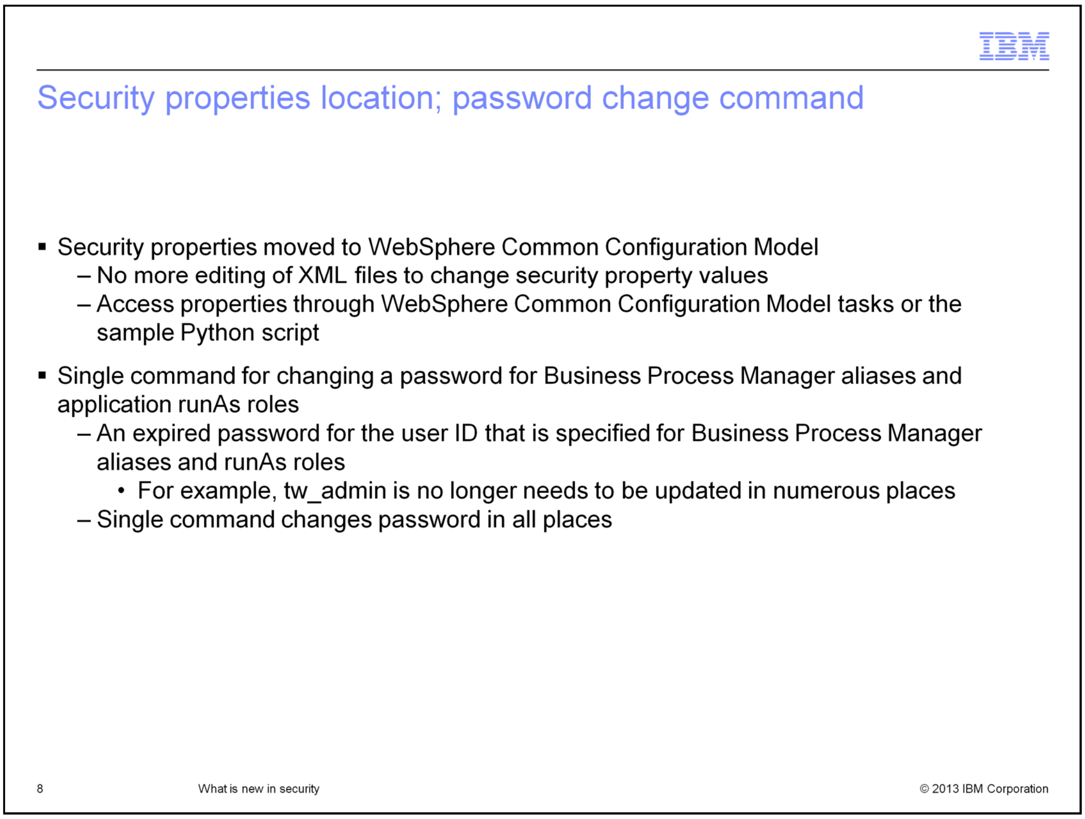
Role	Alias
BPCUser	DeAdminAlias
BPMAuthor	DeAdminAlias
BPMUser	DeAdminAlias
BPMWebserviceUser	DeAdminAlias
CEIDbUser	DeAdminAlias
CEIUser	DeAdminAlias
DeAdmin	DeAdminAlias
EmbeddedECMTechnicalUser	DeAdminAlias
EventManagerUser	DeAdminAlias
PerformanceDWUser	DeAdminAlias
ProcessCenterUser	DeAdminAlias
ProcessServerUser	DeAdminAlias
SCAUser	DeAdminAlias
Total 13	

You can sepecify multiple aliases for role SystemLaneUser. Hold the CTRL key to select multiple items.

- CellAdminAlias
- DeAdminAlias
- BPM_DB_ALIAS

7 What is new in security © 2013 IBM Corporation

This is a screen capture of the WebSphere Application Server administrative console user interface, where you can change the mapping of a Business Process Manager role to an authentication alias. Note that SystemLaneUser is the only role that can be mapped to multiple aliases.

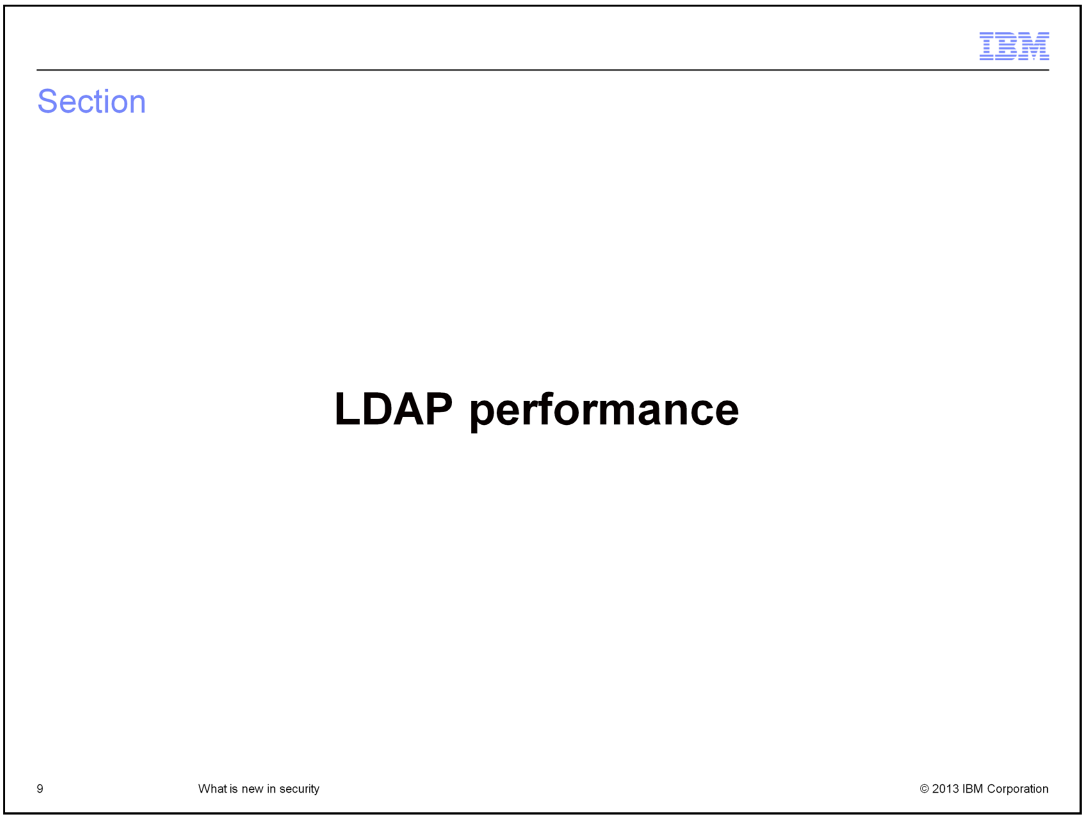


Security properties location; password change command

- Security properties moved to WebSphere Common Configuration Model
  - No more editing of XML files to change security property values
  - Access properties through WebSphere Common Configuration Model tasks or the sample Python script
- Single command for changing a password for Business Process Manager aliases and application runAs roles
  - An expired password for the user ID that is specified for Business Process Manager aliases and runAs roles
    - For example, tw_admin is no longer needs to be updated in numerous places
  - Single command changes password in all places

8 What is new in security © 2013 IBM Corporation

In V8.5, the security properties are no longer located in XML files; they are in WebSphere Common Configuration Model. They can be modified using either WebSphere Application Server commands and tasks or the provided Python script. There is also a new command to change all of the instances of the password for the specified user ID. With this command, the password change is done once and is applied to all instances of that password in the IBM Business Process Manager system applications and known aliases.

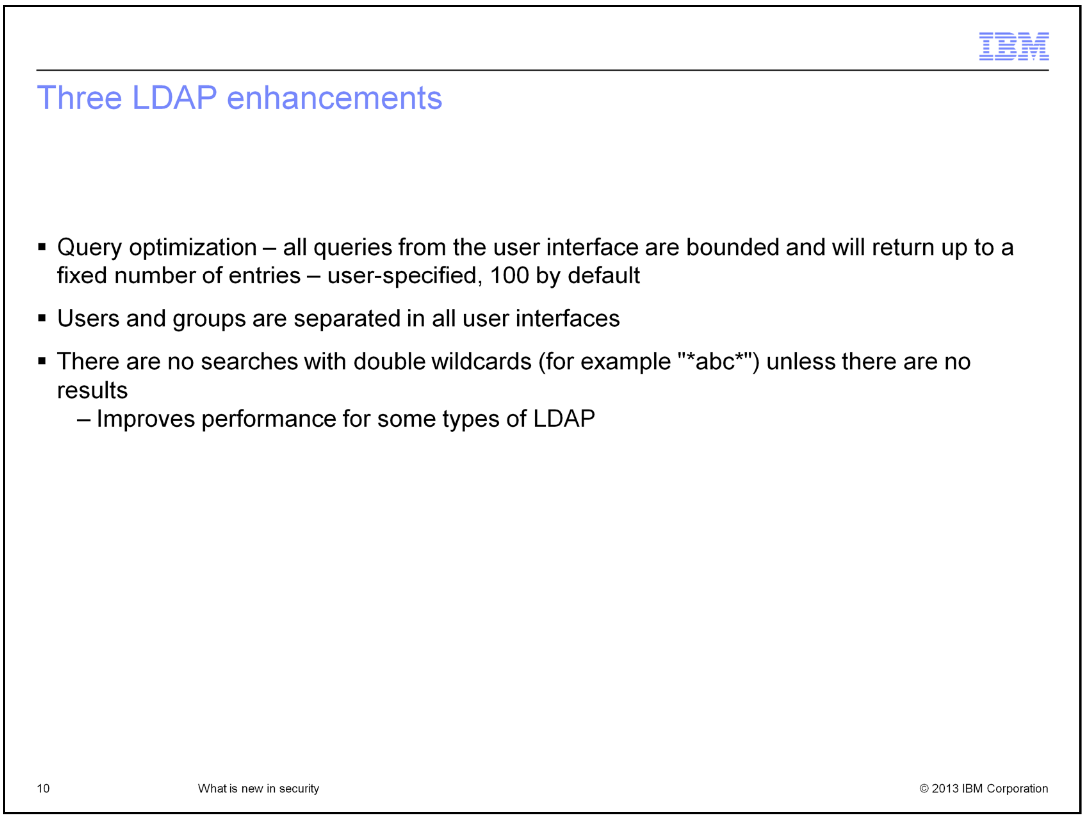


Section

LDAP performance

9 What is new in security © 2013 IBM Corporation

This section describes in detail the changes in LDAP performance.



Three LDAP enhancements

- Query optimization – all queries from the user interface are bounded and will return up to a fixed number of entries – user-specified, 100 by default
- Users and groups are separated in all user interfaces
- There are no searches with double wildcards (for example "*abc*") unless there are no results
  - – Improves performance for some types of LDAP

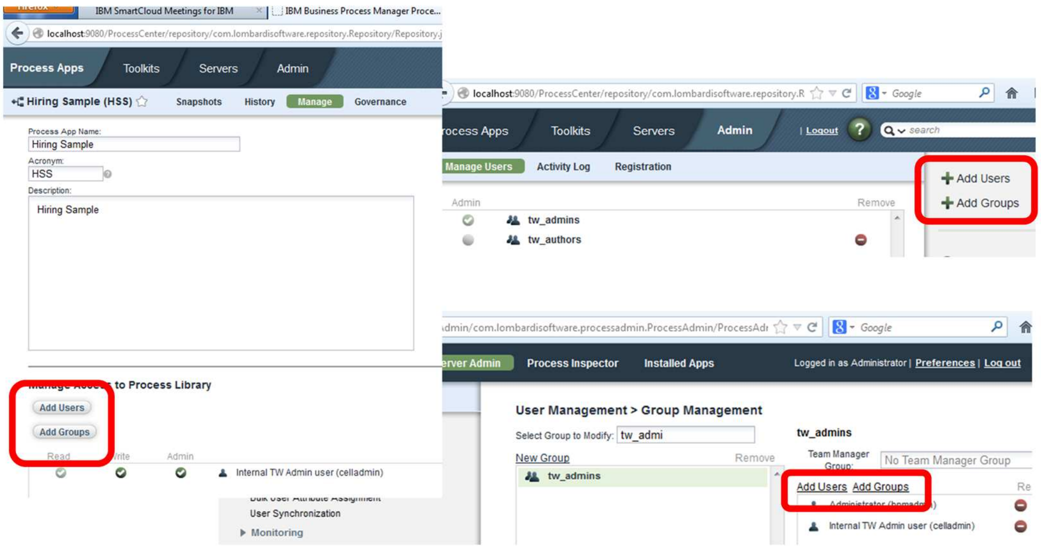
10 What is new in security © 2013 IBM Corporation

In V8.0.1, LDAP queries can run for a very long time and return thousands of results. But in V8.5, the number of results returned by a query is bounded. The default value is one hundred, but you can configure this. You are notified when the available number of results is larger than the bound value.

The user interface now separates users and groups, which avoids randomness in returned results. In some cases in V8.0.1, 'Add Member' returns a mixture of users and groups, depending on the search string.

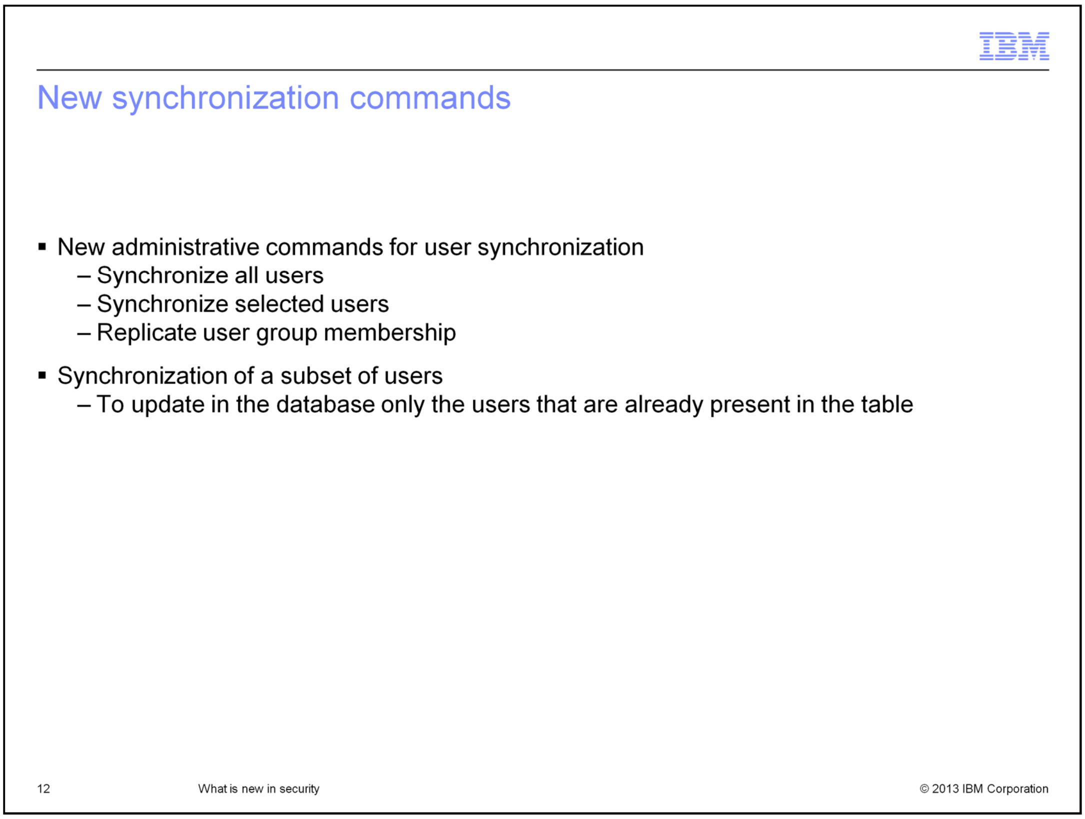
Some types of LDAP queries take a very long time for double wildcard searches. To adjust for that, you can now set the property "optimizeWildcardSearch". With this property set, if you type "abc", the string "abc*" is searched first and, only if that search returns no result, the string "*abc*" is searched second.

Users and groups are separate


IBM SmartCloud Meetings for IBM
IBM Business Process Manager Proce...
localhost:9080/ProcessCenter/repository/com.lombardisoftware.repository.Repository/Repository.j
Process Apps
Toolkits
Servers
Admin
Hiring Sample (HSS)
Snapshots
History
Manage
Governance
Process App Name:
Hiring Sample
Acronym:
HSS
Description:
Hiring Sample
Manage Access to Process Library
Add Users
Add Groups
Read
Write
Admin
Internal TW Admin user (celladmin)
Bulk User Attribute Assignment
User Synchronization
Monitoring
localhost:9080/ProcessCenter/repository/com.lombardisoftware.repository.R
Google
Process Apps
Toolkits
Servers
Admin
Logout
search
Manage Users
Activity Log
Registration
Admin
Remove
tw_admins
tw_authors
Add Users
Add Groups
admin/com.lombardisoftware.processadmin.ProcessAdmin/ProcessAdr
Server Admin
Process Inspector
Installed Apps
Logged in as Administrator | Preferences | Log out
User Management > Group Management
Select Group to Modify: tw_admi
New Group
Remove
tw_admins
tw_admins
Team Manager Group:
No Team Manager Group
Add Users Add Groups
Re
Administrator (bpmadmin)
Internal TW Admin user (celladmin)

11 What is new in security © 2013 IBM Corporation

This slide shows the various user interface screens that now separate users and groups.

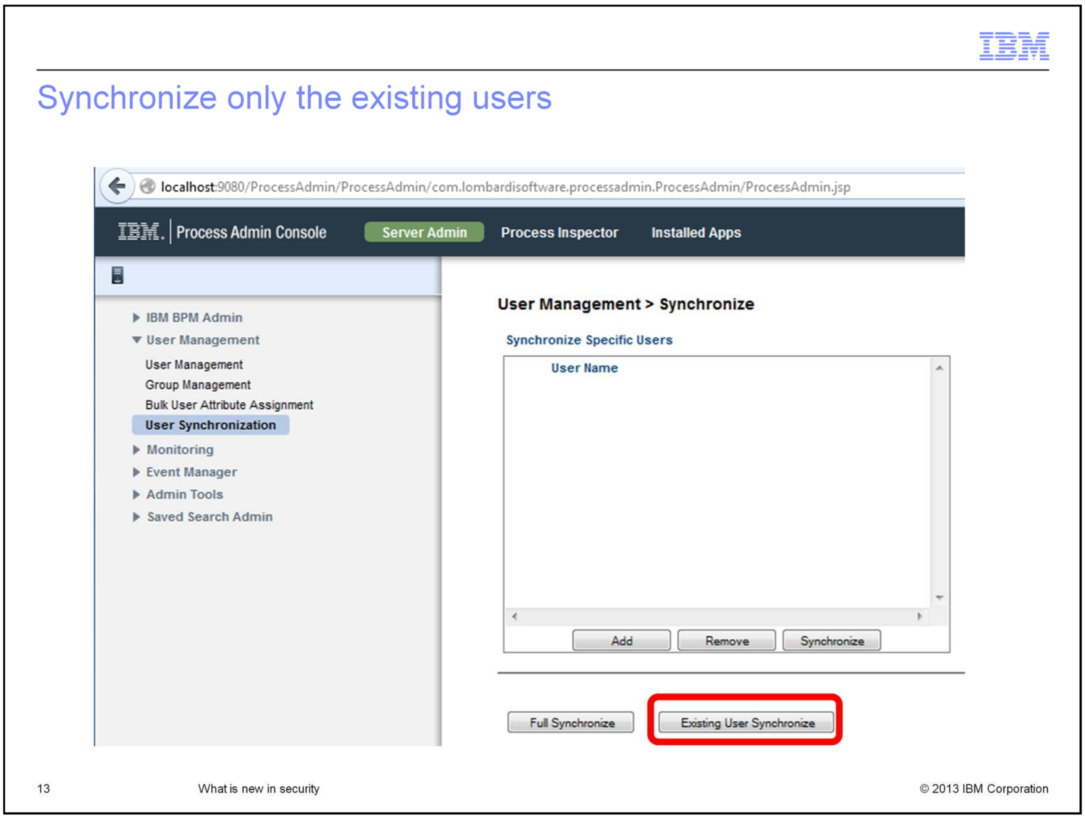


New synchronization commands

- New administrative commands for user synchronization
  - Synchronize all users
  - Synchronize selected users
  - Replicate user group membership
- Synchronization of a subset of users
  - To update in the database only the users that are already present in the table

12 What is new in security © 2013 IBM Corporation

There are new commands for performing some of the synchronization tasks with LDAP from the command line. These commands allow you to perform out-of-bound synchronization. The LDAP notification is outside of IBM Business Process Manager but the commands can now propagate it into IBM Business Process Manager.



Synchronize only the existing users

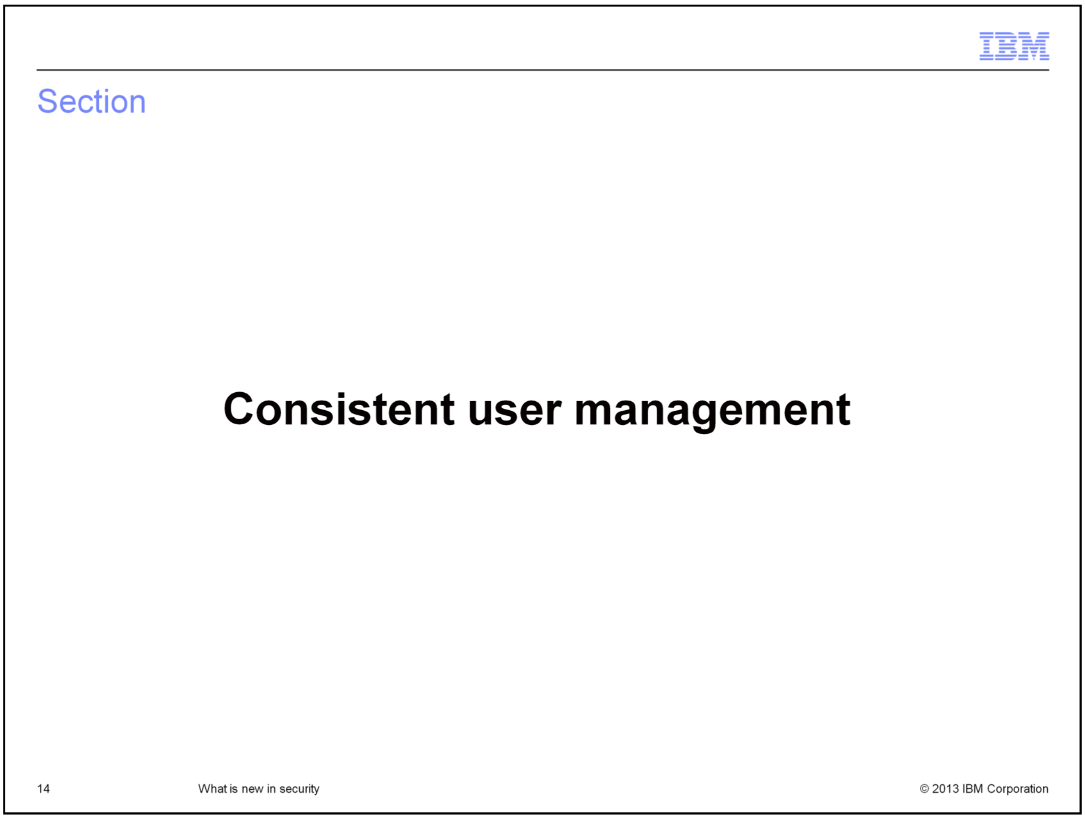
localhost:9080/ProcessAdmin/ProcessAdmin/com.lombardisoftware.processadmin.ProcessAdmin/ProcessAdmin.jsp

User Management > Synchronize

Synchronize Specific Users

13 What is new in security © 2013 IBM Corporation

This slide shows the new button for synchronizing only the known users.

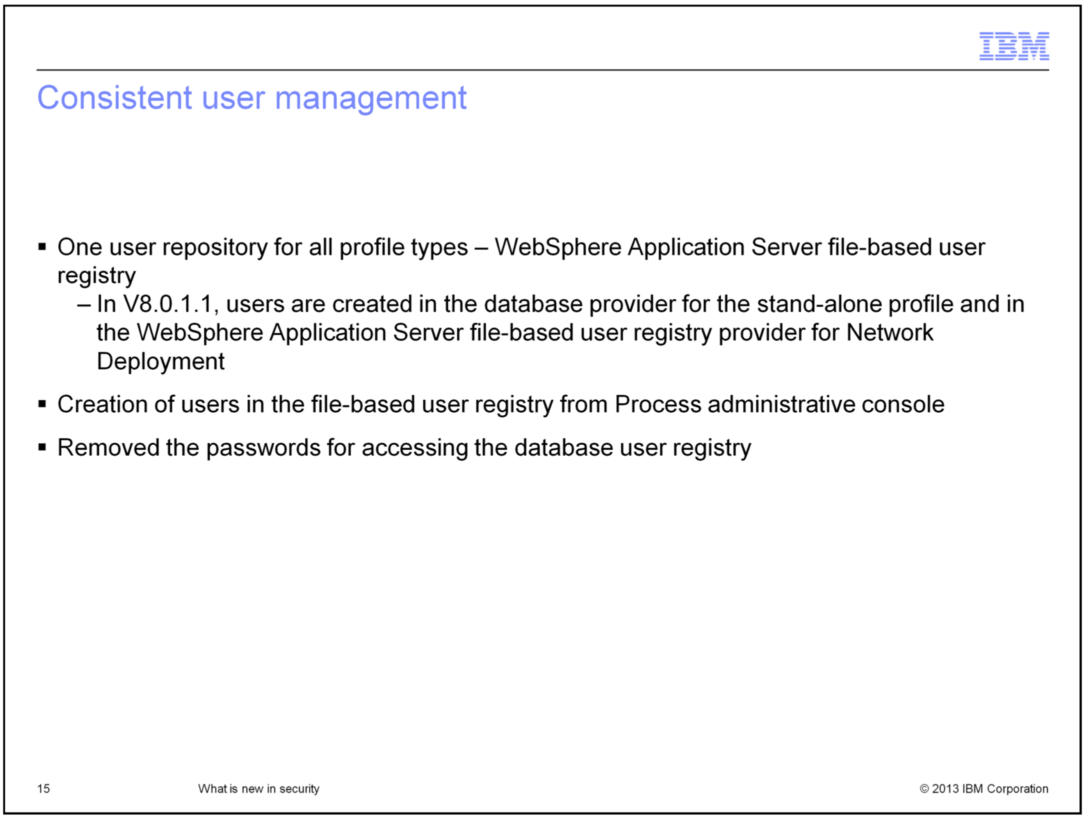


Section

Consistent user management

14 What is new in security © 2013 IBM Corporation

This section discusses the improvements related to consistent user management.

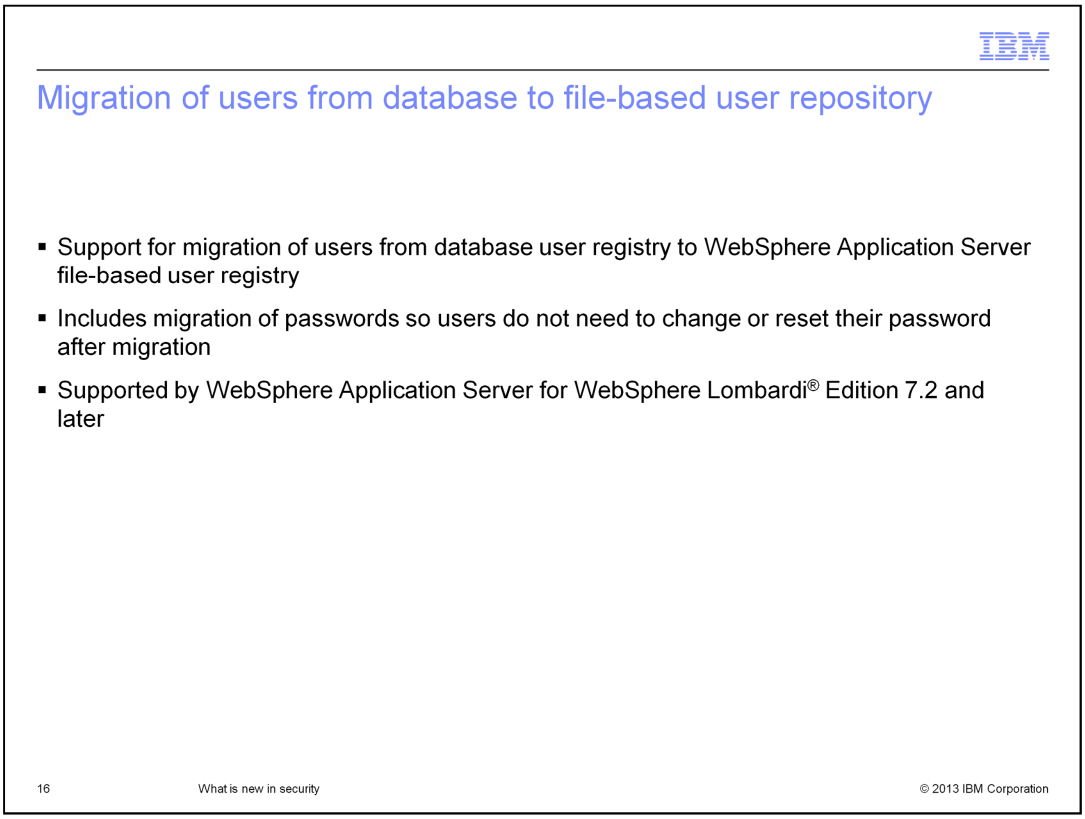


Consistent user management

- One user repository for all profile types – WebSphere Application Server file-based user registry
  - In V8.0.1.1, users are created in the database provider for the stand-alone profile and in the WebSphere Application Server file-based user registry provider for Network Deployment
- Creation of users in the file-based user registry from Process administrative console
- Removed the passwords for accessing the database user registry

15 What is new in security © 2013 IBM Corporation

In IBM Business Process Manager V8.5, the database provider has been eliminated. Instead, there is a WebSphere Application Server file-based user registry provider for use in proof-of-concept scenarios. The user interface is the same as in the stand-alone profile of IBM Business Process Manager V8.0.1 and it also works in Network Deployment. Passwords for accessing the database have been removed from IBM Business Process Manager V8.5, which improves security.

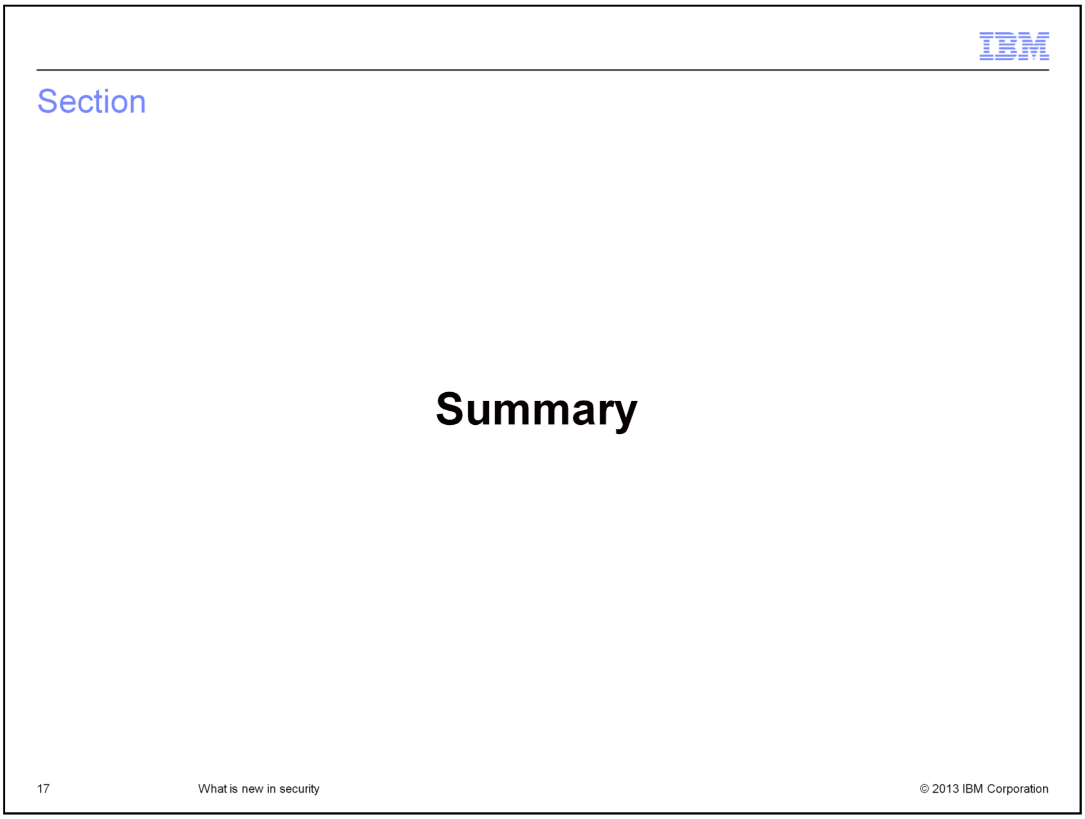


Migration of users from database to file-based user repository

- Support for migration of users from database user registry to WebSphere Application Server file-based user registry
- Includes migration of passwords so users do not need to change or reset their password after migration
- Supported by WebSphere Application Server for WebSphere Lombardi® Edition 7.2 and later

16 What is new in security © 2013 IBM Corporation

The migration of users and their passwords from the database registry to the file-based user registry is fully supported in IBM Business Process Manager V8.5.

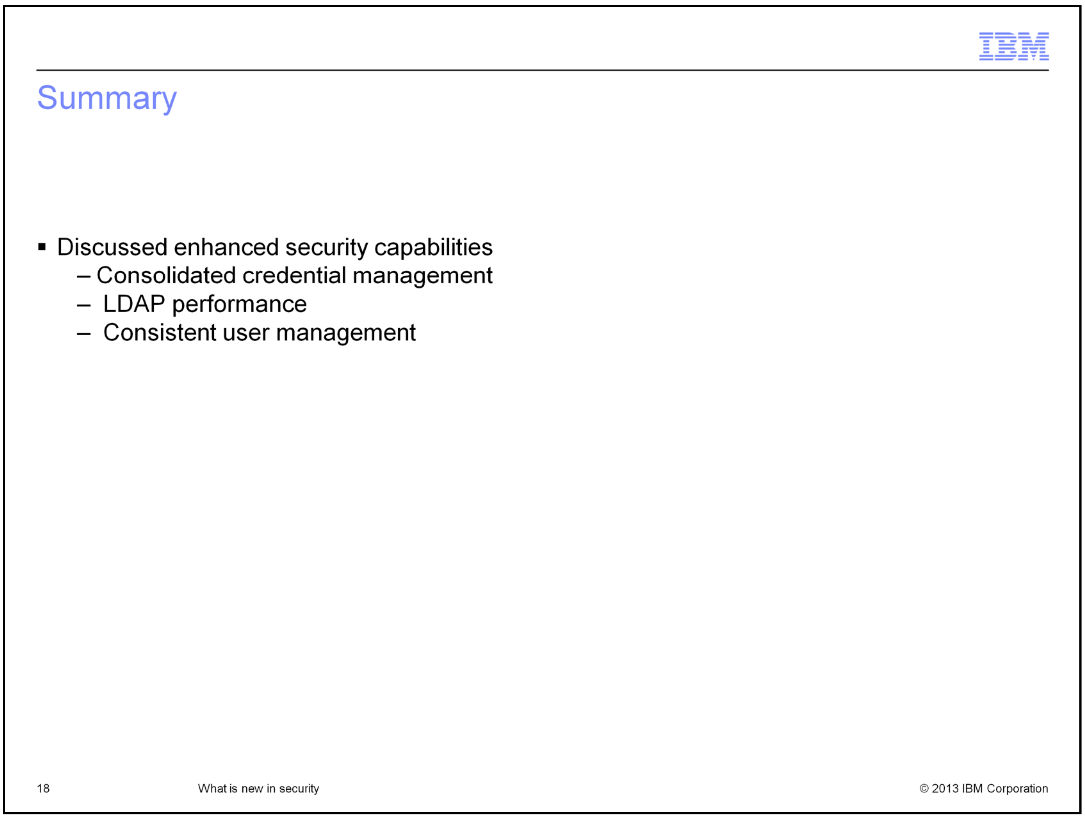


Section

Summary

17 What is new in security © 2013 IBM Corporation

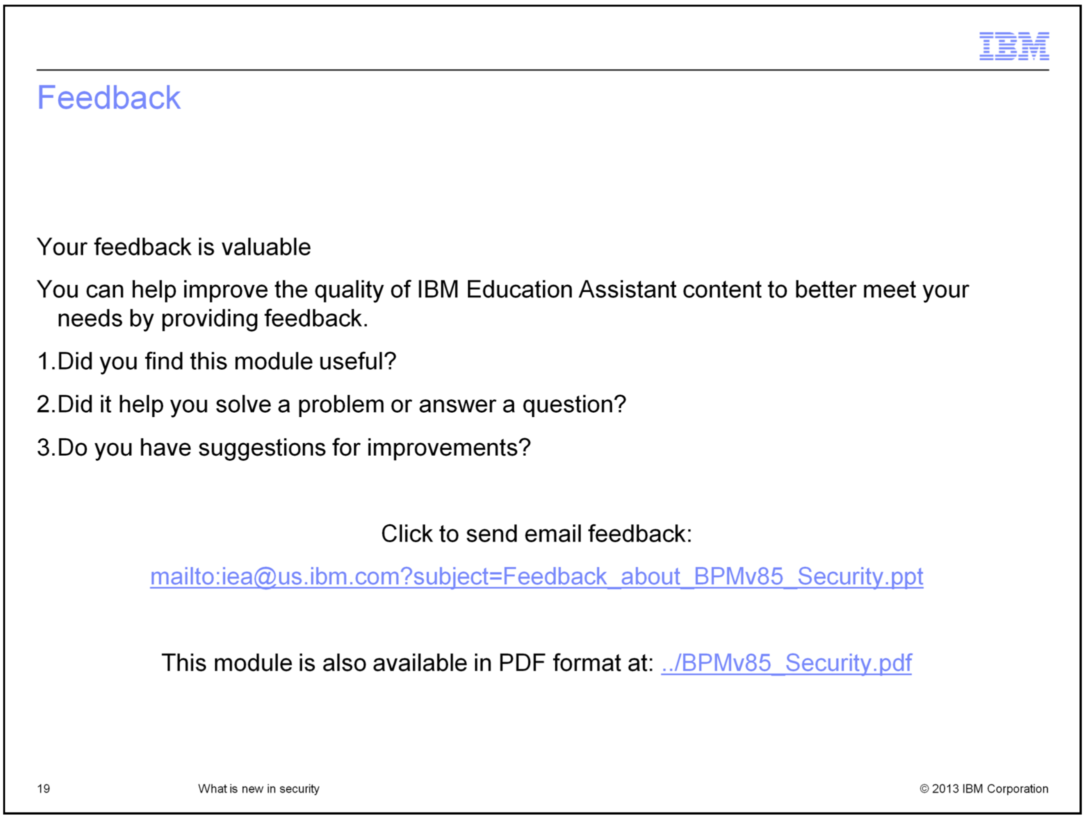
The next slide provides summary of the security enhancements in IBM Business Process Manager V8.5.



Summary

- Discussed enhanced security capabilities
  - Consolidated credential management
  - LDAP performance
  - Consistent user management

In summary, this presentation introduced the new and enhanced security capabilities in the IBM Business Process Manager V8.5 release. The three main improvements are: consolidated credential management, LDAP performance, and consistent user management. You learned about these features and how they differ from the previous release.



Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

1. Did you find this module useful?
2. Did it help you solve a problem or answer a question?
3. Do you have suggestions for improvements?

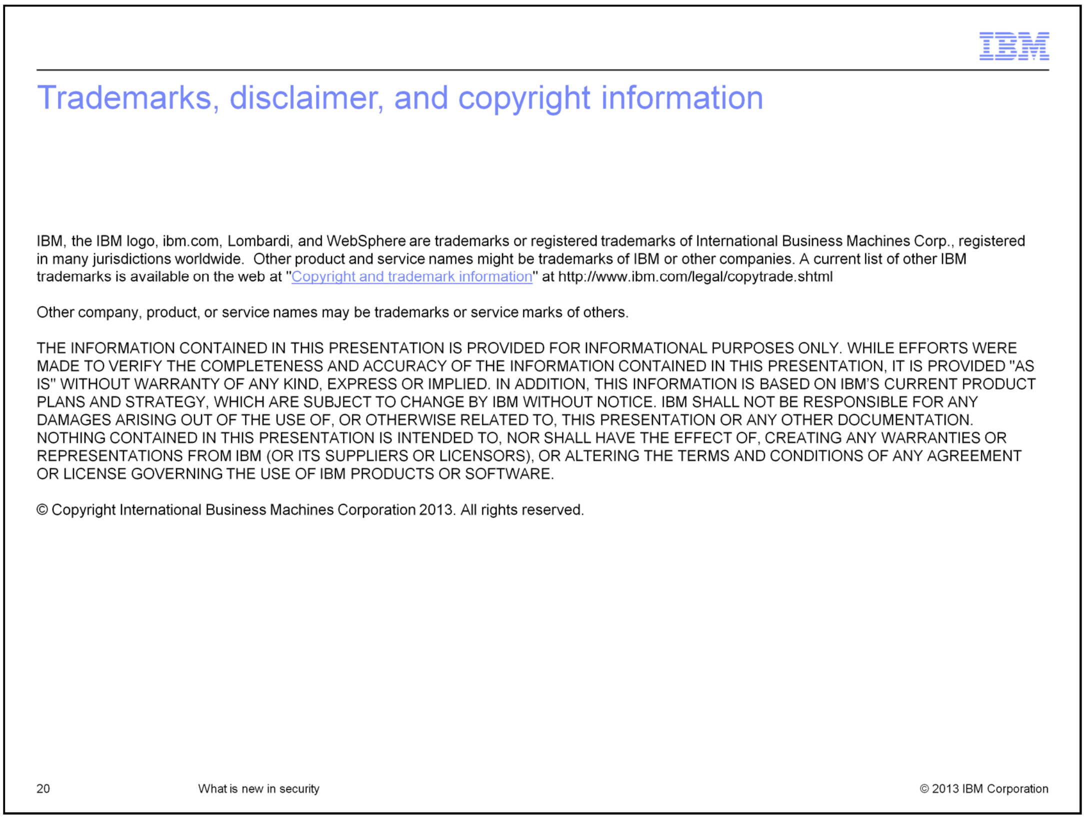
Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_BPMv85_Security.ppt

This module is also available in PDF format at: ../BPMv85_Security.pdf

19 What is new in security

You can help improve the quality of IBM Education Assistant content by providing feedback.



Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, Lombardi, and WebSphere are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

Other company, product, or service names may be trademarks or service marks of others.

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.