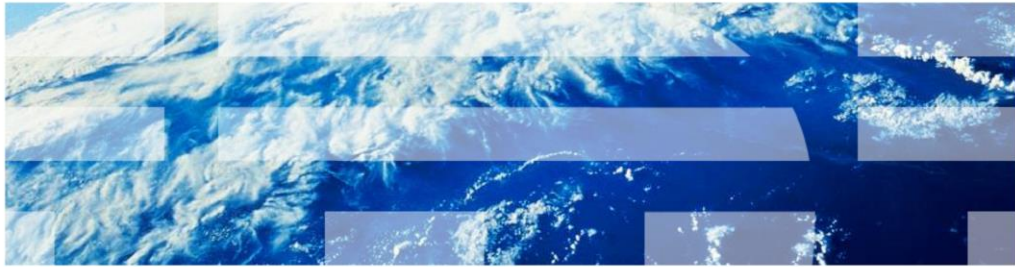


IBM PureApplication System

System security



This presentation covers security in managing IBM PureApplication™ System.

Table of contents

- Overview
- Security - LDAP settings
- Users
- Permissions - Details
- User groups
- Adding users to groups
- Fine-grained access control
- Special access for IBM service personnel
- Summary

The presentation begins with an overview of security settings for LDAP and how that affects user and user group management. The next sections focus on users, permission details, and user groups, followed by a discussion of how to add users to groups. You then learn how to grant access at the data level through fine-grained access control. Finally, you learn how to enable the service panels provided for on-site IBM service personnel.

Overview

This section of the presentation provides an overview of the security features of PureApplication System.

Security overview

IBM PureApplication System Workload Console **System Console**

Welcome Cloud Hardware Reports **System**

- **System Console > System > Users**
 - Define and manage user accounts
- **System Console > System > User Groups**
 - Define and manage user groups
- **System Console > System > Security**
 - Local or LDAP authentication supported
- Important notes
 - User actions are audited (discussed in a separate presentation)
 - Security within the deployed software and operating systems:
 - Normal security provided by that software or operating system

Auditing
Settings
Users
User Groups
Security
Customer Network Configuration
Job Queue
Events
Troubleshooting
Problems
Product Licenses

Set of functions related to security configuration

4 System security © 2012 IBM Corporation

The snapshot on this slide shows you the three important security-related items in the System pull-down menu on the System Console: **Users**, **User Groups**, and **Security**.

A user account is required to access PureApplication System. The **Users** and **User groups** features of PureApplication System allows you to create individual user accounts and put them together into logical groups. These features allow you to manage the level of access for each individual. The **Security** feature allows you to set up an optional LDAP server, so that each user can be registered with “local” authentication or LDAP authentication.

There are two important notes about security in this environment. First, PureApplication System user activity is tracked for audit purposes. Auditing is covered in a separate presentation.

Secondly, the workload security for the middleware running in the virtual machines is the normal deployed middleware and operating system security. For example, WebSphere® security manages the WebSphere Application Server security through the configuration of the middleware and not through PureApplication System.

Security – LDAP settings

This section of the presentation provides an overview of the LDAP settings within PureApplication System.

Security settings

- **System Console → System → Security**
 - Selection of external LDAP authentication
 - Testing the LDAP setting

System

- Auditing
- Settings
- Users
- User Groups
- Security**
- Customer Network Configuration
- Job Queue
- Events
- Troubleshooting
- Problems
- Product Licenses

LDAP Settings

LDAP provider URL	ldaps://172.16.248.9:636
Security certificate	Accepted
LDAP base DN (users)	ou=WebSphere,o=ibm,c=us
LDAP base DN (groups)	ou=groups,o=ibm,c=us
Search filter (users)	(&(uid={0})(objectclass=inetOrgPerson))
Search filter (groups)	(&(member={0})(objectclass=groupOfNames))
LDAP security authentication	cn=root
Password [Edit]

Test LDAP authentication settings

To test whether LDAP authentication settings are setup correctly.

LDAP user name

user1 ✓

LDAP group name

group1 ✗

6

System security

© 2012 IBM Corporation

Local authentication is a great way to get started with PureApplication System. However, if PureApplication System is going to be shared by a large organization, you can use an external authenticator, like a Lightweight Directory Access Protocol, or LDAP directory.

External authentication option, as shown in the slide, allows you to configure LDAP authentication and provides the capability to test the LDAP settings. When you define a user, you select if the user is Local – which means the user is defined only within the PureApplication System - or if the user is registered in LDAP.

You must perform the LDAP authentication before defining any users that must use LDAP security.

PureApplication System has provided a validation function to test the connection to the LDAP server by submitting a query to find a particular LDAP user name or LDAP group name. When successful, you will see a green check box. If there is an error with the query, or with the LDAP parameters or if a connection to the LDAP server cannot be established, an exception is displayed.

Integration with LDAP – users and groups

- When a new user is created in PureApplication System, the administrator can specify if the authentication is Local or LDAP
 - If LDAP is selected, user authentication is performed within LDAP
 - If Local is selected, PureApplication System authenticates the user
 - LDAP plays no role in local authentication
- When creating groups in PureApplication System, the administrator specifies if the authentication is Local or LDAP
 - Membership of the LDAP group is defined in LDAP and not in PureApplication System
- LDAP administrator must add the user or group in LDAP, if LDAP authentication is selected for the user or the group
 - PureApplication System does not modify LDAP – it merely authenticates the user in LDAP, or checks the user membership in a LDAP group

When a new user is created, the security administrator can choose either local or LDAP authentication for that user. If LDAP authentication is selected, PureApplication System will use LDAP to authenticate the user. If local authentication is set, PureApplication System will use its own registry to authenticate the user.

Similarly, when creating new groups, the security administrator can choose either local or LDAP authentication. If LDAP is used, membership of the LDAP group is defined in LDAP and not in PureApplication System. When LDAP is used to authenticate a user, that user needs to be added to PureApplication System and to the LDAP registry. PureApplication System does not modify LDAP. It merely authenticates the user in LDAP, or checks the user membership in a LDAP group. More details about users and groups is presented in subsequent slides.

Section

Users

This section of the presentation provides an overview of defining and managing users in PureApplication System.

Creating new user

- Security administrator creates new user
 - **System Console** → **System** → **Users** and click the **[+]** sign
- User security account type can be 'Local' or 'LDAP'
 - Based on **Account type** when the user is defined
 - 2a • If local, then need to provide password
 - 2b • If LDAP, then Security settings for LDAP must already be defined

A user account can be created by a security administrator by navigating to the **System Console** panel, then the **System** menu, selecting **Users**, and clicking the “+” icon.

Creating the user account is a two step process. You first need to supply basic information such as user name, full name, password, and an email address. The email address is used to send the user the initial password and other notifications, such as notification of a deployment.

PureApplication System supports local and LDAP user management integration. You can define users that belong in either the LDAP server or local to PureApplication System. PureApplication System first checks to ensure the user name has not already been defined within PureApplication System, as either a local or an LDAP user. Then if you select LDAP, PureApplication System ensure that LDAP security has been defined and that the user is defined within LDAP. If you select LDAP, then LDAP type users do not require a password because the password is stored in the LDAP server.

The second part of user creation is to assign the roles to the users to authorize them to certain functions. This is discussed in detail later.

An email address is always required, even if SMTP is not yet enabled within PureApplication System.

User attributes (entire screen)

System Console → System → Users

The screenshot displays two panels from the IBM System Console. The left panel, titled 'User attributes (entire screen)', shows the configuration for a user named 'deployer'. Fields include: Full name (Some Deployer), Email address (deployer@some_addr), Password (masked with asterisks and an 'edit' button), Type (Internal), and User groups (Everyone with a 'remove' button and an 'Add more...' dropdown). Below these are sections for Authorized IP groups, virtual appliances, virtual machines, and cloud groups, each showing 0 in total. The Permissions section is set to 'Workload Management' and includes options for creating patterns, environment profiles, catalog content, and using the ILMT tool. A 'Delete' button is visible in the top right of this panel. The right panel, titled 'Administrators', shows the role configuration for 'Administrators'. It includes a checkbox for 'Allow delegation when full permission is selected' and lists several administrative roles: Workload resources administration, Cloud group administration, Hardware administration, Auditing, and Security Administration. Each role has radio buttons for 'View all' (Read-only) and 'Manage' (Full permission) options. A red dashed line connects the 'Add more...' dropdown in the left panel to the 'Administrators' panel on the right. The bottom left of the slide shows the number '10' and the text 'System security'. The bottom right shows the copyright notice '© 2012 IBM Corporation'.

To manage users in PureApplication System, from the **System Console** navigate to **System** and then click **Users**. From here you can create users or modify user attributes. If you then click a user name, the user's attributes are displayed, depicted by the screen capture shown here.

More information about these settings is provided in subsequent slides.

User attributes - overview

The screenshot displays the user attributes for a user named "deployer". The interface is organized into four main sections, each highlighted with a yellow box and a red bracket:

- User specific information:** Includes fields for Full name (Some Deployer), Email address (deployer@some_addr), Password (masked with dots and an [edit] button), and Type (Internal).
- User groups:** Shows the user is in the "Everyone" group with a [remove] button. Below this is an "Add more..." dropdown menu.
- "Authorized" information:** Lists four categories, each with a count of 0 in total:
 - Authorized IP groups: 0 in total
 - Authorized virtual appliance: 0 in total
 - Authorized virtual machine: 0 in total
 - Authorized cloud groups: 0 in total
- Permissions:** Shows "Workload Management" as the selected subrole. Below this is a prompt: "Select the specific subrole(s) for this user".

Additional details from the screenshot include a "Delete" icon in the top right corner, a "11" in the bottom left corner, and "System security" and "© 2012 IBM Corporation" in the bottom center.

This slide gives you an idea of the kinds of information provided within the user properties display. There are four major areas – user specific information, user groups, authored information, and the permissions section. More about each section is shown in subsequent slides. Notice the **Delete** icon at the upper right, this allows security administrator to delete the user from the system.

User attributes – user specific information and user groups

- User specific information
 - User name
 - Email address
 - Required to send notification emails
 - Password
 - If user authentication is local
 - Type
 - Internal (local)
 - LDAP

deployer	
Full name:	Some Deployer
Email address:	deployer@some.addr
Password:	***** [edit]
Type:	Internal
User groups:	Everyone [remove]
	<input type="text" value="Add more..."/>

- User groups
 - Security administrator can add user to or remove user from groups

Continued on next slide

The user-specific information includes the user name, the required email ID, the password for local users, and type indicating whether the user is “local” denoted as “internal” or LDAP.

The user groups section show you the groups in which the user is enrolled and provides an input area so the security administrator can register the user into additional groups. All user names are automatically enrolled in the “Everyone” group, and if the user name is in additional groups, they are listed here as well. Group permissions are inherited by the user. This is explained in details later in this presentation.

Users – Authorized section and permissions

Continued from previous slide

- Authorized section – shows resources owned by this user
 - IP groups
 - Cloud groups
 - Virtual appliances
 - Virtual machines



+	Authorized IP groups:	1 in total
+	Authorized virtual appliance:	1 in total
+	Authorized virtual machine:	500 in total
+	Authorized cloud groups:	1 in total

- Security permissions
 - Separation of duties for different user activities
 - Two major categories defined
 - Workload Management
 - Administrators



Permissions:	Workload Management
	Select the specific subrole(s) for this user
	<input checked="" type="checkbox"/> Create new patterns

Continued on next slide

The “Authorized” section provides information about the resources that this user has created. They include the IP groups, cloud groups, virtual appliances and virtual machines.

In the “Permissions” section, you can modify the permissions for this user to control the level of access that is assigned to the user. These permissions determine the tasks the user can or cannot perform.

PureApplication System security allows separation of duties for different user activities. Two major permission categories exist, namely, Workload Management and Administrators. Within Administrators there are several sub categories to provide further separation of duties.

Permissions – Workload management

- Workload management for managing and deploying workloads
 - Virtual applications
 - Virtual systems
- Permissions can be given for
 - Create new patterns
 - Create new environment profiles
 - Create new catalog content
 - Manage licensing thru' ILMT
- Default: all users have “Deploy pattern to cloud”
 - Patterns they authored
 - Patterns to which they have been granted permission

Continued from previous slide

Workload Management

Select the specific subrole(s) for this user

- Create new patterns
- Create new environment profiles
- Create new catalog content
- IBM License Metric Tool (ILMT)

Continued on next slide

Workload Management allows the security administrator to manage functions available to users by setting specific permissions. Workload Management permissions give the user the ability to create new patterns, create new environmental profiles, create new catalog content and work with the IBM License Metric Tool.

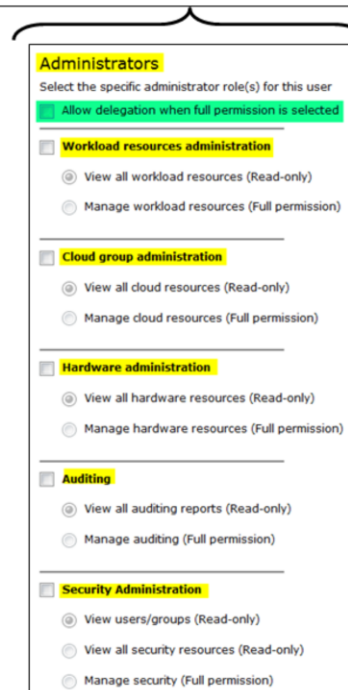
A user with a workload administrative permission for creating new patterns, new environment profiles, or new catalog content can also modify or delete resources authored by other users, if they have been given write access to that resource.

By default, everyone has permission to “deploy patterns in the cloud” for patterns they authored, or for patterns to which they have been given permission.

Permissions – Administrators

- Distinct administrative areas
 - Ability to give administrative permissions to users or user groups on distinct administrative functions of the system
 - Prevents giving user full authority on the entire system
- Major security administration permissions categories:
 - Workload resources, Cloud group, Hardware, Auditing, and Security
- Administration permission levels
 - **Manage (full permission)**
 - **View (read-only permission)**
- Users with **delegate permission** can give to or revoke permissions from other users

[More details provided later](#)



Administrators
Select the specific administrator role(s) for this user

Allow delegation when full permission is selected

Workload resources administration

- View all workload resources (Read-only)
- Manage workload resources (Full permission)

Cloud group administration

- View all cloud resources (Read-only)
- Manage cloud resources (Full permission)

Hardware administration

- View all hardware resources (Read-only)
- Manage hardware resources (Full permission)

Auditing

- View all auditing reports (Read-only)
- Manage auditing (Full permission)

Security Administration

- View users/groups (Read-only)
- View all security resources (Read-only)
- Manage security (Full permission)

15

System security

© 2012 IBM Corporation

PureApplication Server provides distinct administrative permissions to allow you to define user roles that allow separation of duties. You do not have to have an administrator with full access to the entire system. The permissions that you see here for the various administrators provide either “view” access or “manage” access to the resources.

Workload resources administration gives permission related to viewing or managing workloads, such as catalog resources, patterns, and deployed instances.

Cloud Administration gives permission related to viewing or managing cloud groups, IP pools, shared services, and environment profiles.

Hardware Administration gives permission related to viewing or managing the individual hardware components within PureApplication Server.

Auditing gives permission related to viewing audit records or for managing the configuration for the automatic external storage of auditing records.

Security Administration gives permission related to viewing or managing users or user groups, security resources in general, and setting up external security services. Security administration has two “view” permissions so that a user can have “view” access of only users and groups, or can have “view” access of all security resources including LDAP settings.

The “Allow delegation” security setting, seen at the top of the list of permissions further enhances the permissions functionality. An administrator with this permission can give to or revoke from another user any permission that they themselves possess.

PureApplication System ensures there is at least one user will full administration authority in each of the five categories.

More details on all these permissions and the delegation are provided later.

Permissions - Details

This section of the presentation provides an details of permissions available in PureApplication System.

Workload management permissions - Details

Workload Management

Select the specific subrole(s) for this user

- Create new patterns
- Create new environment profiles
- Create new catalog content
- IBM License Metric Tool (ILMT)

Workload management permissions	Actions that can be performed
Deploy patterns in Cloud ▪ Not explicitly shown in the panel	Default permission for all users Permission to deploy permissible patterns to the cloud – must have permission to access the pattern (given by the pattern owner) or use their patterns or one of the available patterns (that everyone has access)
Create new patterns	Permission to create new patterns and then optionally give permission (read-only or edit) to other users
Create new environment profiles	Permission to create new environment profiles and then optionally give permission (read-only or edit) to other users
Create new catalog content	Permission to create/add new content in catalog (virtual images, configuration scripts, plug-ins, pattern types, add-ons)
IBM License Metric Tool (ILMT)	Permission to configure ILMT

The table covers all the workload management permissions. You can set separate permissions to create new patterns, create new environment profiles, create new catalog content, or configure the IBM License Metric tool.

By default, all users have permissions to deploy patterns that they own or to which they are granted permission.

Workload administration permissions - Details

Workload resources administration

- View all workload resources (Read-only)
- Manage workload resources (Full permission)

Workload administration permissions	Actions that can be performed
Manage workload resources (Full permission)	All of workload management permissions – Deploy, create patterns, create new environment profiles, catalog content and IBM License Metric Tool
View workload resources	View all Workload Management resources

Workload resource administration permissions allow either read only or full permission to all workload resources mentioned in the previous slide. This includes deploy, create patterns, create new environment profiles, create catalog content and configure IBM License Metric Tool or view its configuration.

Cloud group administration permissions - Details

Cloud group administration

- View all cloud resources (Read-only)
- Manage cloud resources (Full permission)

Cloud group administration permissions	Actions that can be performed
Manage cloud resources (Full permission)	Manage or configure: <ul style="list-style-type: none"> ▪ Cloud groups, IP groups, storage volumes, virtual appliances, virtual machine groups, virtual machines ▪ Shared services ▪ Manage monitoring for all deployments (Monitor administrator for deployments)
View all cloud resources (Read-only)	View: <ul style="list-style-type: none"> ▪ Cloud groups, IP groups, storage volumes, virtual appliances, virtual machine groups, virtual machines ▪ Shared services ▪ View monitoring for all deployments (Monitor operator for deployments)

The table shows Cloud group administration permissions. These permissions allow the authorized user or group permissions to manage or view cloud resources.

Cloud resources include cloud groups, IP groups, storage volumes, virtual appliances, virtual machine groups, virtual machines, shared services and monitoring for all deployments.

Hardware administration permissions - Details

Hardware administration

- View all hardware resources (Read-only)
- Manage hardware resources (Full permission)

Hardware administration permissions	Actions that can be performed
Manage hardware resources (Full permission)	Manage or configure: <ul style="list-style-type: none"> ▪ All H/W resources - (Compute nodes, management nodes, storage devices), network devices, external access network, system settings, ▪ Apply system maintenance ▪ Manage all H/W monitoring ▪ View machine reports ▪ Enable on-site IBM service personnel special access to troubleshoot, apply maintenance and upgrade the system.
View all hardware resources (Read-only)	View: <ul style="list-style-type: none"> ▪ All H/W resources - (Compute nodes, management nodes, storage devices), network Devices, external access network, system settings, ▪ View system maintenance ▪ View all H/W monitoring ▪ View machine reports

The table shows the Hardware administration permissions. They allow the authorized user or group permissions to manage or view hardware resources.

Hardware resources includes the compute nodes, management nodes, storage devices, network devices, external access network, system settings, apply or view system maintenance, manage or view all hardware monitoring, and view machine reports.

The hardware full administrator also has the ability to enable on-site IBM support personnel to log into the service console. The service console provides special access for troubleshooting, applying maintenance and upgrading the system.

Audit administration permissions - Details

Auditing

- View all auditing reports (Read-only)
- Manage auditing (Full permission)

Audit administration permissions	Actions that can be performed
Managing auditing (Full permission)	<ul style="list-style-type: none"> Can configure external storage server settings so that audit file packages can be pushed to an external system Can read and download audit file packages
View all auditing reports (Read-only)	<ul style="list-style-type: none"> Can review external storage server settings Can read and download all audit file packages

The table shows all the auditing administration permissions.

With auditing (Read-only) permission, the user or group can view and download all audit file packages, and can review a subset of the external storage server settings. With auditing (Full permission), the user or group can additionally configure the external storage server settings so that audit file packages can be pushed to an external system using SCP.

Security administration permissions - Details

Security Administration

- View users/groups (Read-only)
- View all security resources (Read-only)
- Manage security (Full permission)

Security administration permissions	Actions that can be performed
View users/groups (Read-only)	Can view the users and groups and their permissions but cannot change any of those settings
View all security resources (Read-only)	Can view all security resources and security settings but cannot change any of the settings or permissions
Manage security (Full permission)	Can view, set and change all security resources and security settings. Can add, change or delete user accounts or user groups. (LDAP group membership is controlled by LDAP security administrator.)

The table shows all the security administration permissions.

Users or groups with view users and groups permission can view all the users and groups and their permissions but cannot change them.

Users or groups with view all security resources permission can view all the security resources like LDAP settings, but cannot change them.

Users or groups with manage security full permission can view, change all security resource settings and user/group attributes. They can add/delete new users and groups.

Delegate permissions

Allow delegation when full permission is selected

- **Users can provide or revoke permissions for other users if:**
 - They have “full permission” for at least one of the five administrative roles, and
 - They have “Allow delegation...” permission
 - Includes giving or revoking “delegate permission”

Example 1

- John has following permissions
 - “Allow delegation...” permission
 - Workload administration (Full permission)
 - Hardware administration (Read-only) permission
 - Security administration (Full permission)
- John **CAN** give or revoke any or all of his permissions for other users or groups
 - Reason: He has at least 1 administration full permission and “Allow delegation..”

Example 2

- Jane has following permissions:
 - “Allow delegation...” permission
 - Workload administration (Read-only) permission
 - Hardware administration (Read-only) permission
- Jane **CANNOT** give any of the her permissions to other users or groups
 - Reason: She does not have any one of five full permissions

23

System security

© 2012 IBM Corporation

The “Allow delegation...” permission setting can extend a user’s authority level in respect to controlling permissions for other users. Users that have “Allow delegation...” permission can delegate their permissions to others, or remove the permissions they have from others, provided they have “full” permission set for at least one of the five administrative categories. They can only give or revoke the permissions they have.

PureApplication System ensures that there is at least one user with full administration authority in each of the five categories.

The delegation permission is shown by two examples. In example one, John has “Allow delegation...” permission, Workload administration (full permission), Hardware administration (Read-only) and Security administration (Full permission). Since John has “Allow delegation...” and two of the five full permissions, namely Workload administration and Security administration, he can give the permissions that he has to other users and groups, or revoke the permissions he has from other users and groups.

In example two, Jane has “Allow delegation...” permission, but only Read-only permission for Workload administration and Hardware administration. Since Jane does not have a single full permission role, she cannot set or revoke any permissions for other users or groups.

User groups

This section discusses setting up and managing PureApplication System user groups.

Creating user group

- **System Console → System → User Groups**
- Groups allow you to group users according to some criteria that you define
- Group account type can be Local or LDAP
- If LDAP is selected, group membership is dictated by LDAP

The screenshot illustrates the steps to create a user group in the IBM System Console. On the left, the 'System' menu is expanded, and 'User Groups' is highlighted. The main area shows the 'User Groups' page with a search bar and an add icon. A dialog box titled 'Describe the group you want to add.' is open, showing the following fields:

- Group name: Workload Group
- Description: Users with Workload permissions
- Account type: Local (selected from a dropdown menu)

Buttons for 'OK' and 'Cancel' are visible at the bottom of the dialog box.

25

System security

© 2012 IBM Corporation

Groups allow you to group users by some criteria that you define. For example, you can group administrators together or group users by department. A group can be created by an administrator by navigating to the System Console, clicking **System**, and selecting **User group**. To add a new group, click the add icon, provide the required information, and click OK. When defining a group with account type of LDAP, the group must have already been defined within the LDAP server. The group membership itself is determined by the membership defined for the group within the LDAP server.

User group attribute panel

Workload Group Delete

Group name: Workload Group

Description: Users with workload permission

Type: Internal

Created on: 6/4/12 10:27 AM

Updated on: 6/4/12 10:27 AM

Group members: (none)
Add more...

Permissions:

Workload Management
Select the specific subrole(s) for this user

- Create new patterns
- Create new environment profiles
- Create new catalog content
- IBM License Metric Tool (ILMT)

Administrators
Select the specific administrator role(s) for

26

System security

© 2012 IBM Corporation

After creating or modifying a user account, you can add the user to a user group by opening the System Console and navigating the System and clicking User Groups. You then click the specific user group you want to change. You must manually add users to the group in the “Group members” section. By default, all users are automatically part of the “Everyone” group.

User group attributes are similar to the user attributes except there are no authored resources, and in groups, there are group members.

The permission attributes are the same as in user attributes.

When you set permissions for a group from the “Permissions” section of this panel, you grant permissions for all members of the group at the same time.

Adding user to groups

This section of the presentation discusses adding users to the groups and the effective permission.

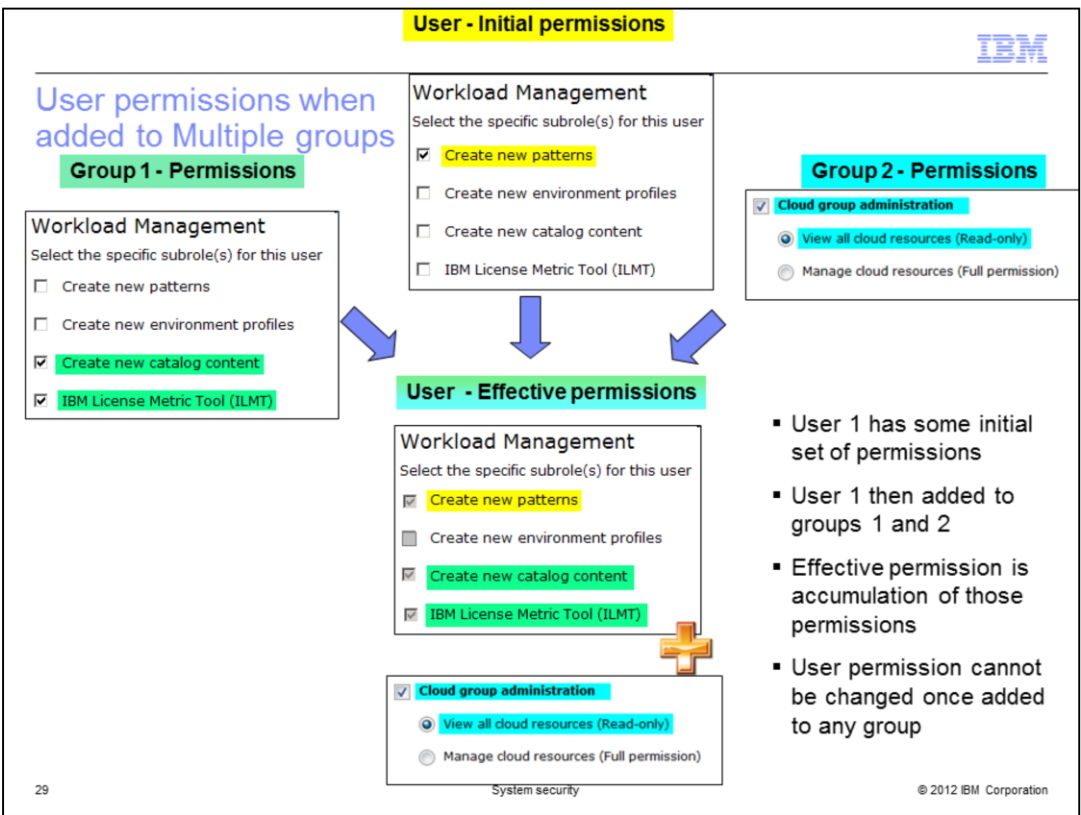
Group-level permissions

- When a user is added to a group:
 - Group permissions are added to the user's permissions
 - User permissions assigned before adding the user to the group are preserved
 - Modifications to group-level permissions apply to all members
- After being added to a group:
 - Permissions can no longer be changed at the user level
 - Does not include the **Everyone** group
- If included in multiple groups:
 - User account has combined permissions for all assigned groups, **plus**
 - Previously assigned user permissions (before the user was added to any group)
- When user is removed from the group:
 - Group permissions that were applied are removed
 - Previously assigned permissions (before user was added to group) still present

When a user is added to a group, the user inherits the permissions of the group. Any permission that the user had before becoming a group member are retained. When a user is included in multiple groups, the inherited permissions reflect the combined permissions for all assigned groups plus the permissions the user had before joining any group.

Once a user is a member of a group, except for the group called Everyone, user permissions can no longer be set from the user panel. They have to be set at the group level.

When the user is removed from the group, the group permissions are also removed. When a user is removed from all the groups, the original user permissions are still present.



This slide shows an example of effective permissions of a user that is a member in multiple groups.

When a user is included in multiple groups, the inherited permissions reflect the combined permissions for all assigned groups plus the permissions the user had before joining any group.

In the example, the user had “Create new patterns permission” before the user was added to a group.

When added to group1 and group2, the user inherited the permissions of both the groups and retained his own permission.

If there is a conflict in the permission, for example, one group has view only and another one has full permissions on a set of permissions, the full permission will prevail.

Fine-grained access control

This section of the presentation focuses on fine-grained access control.

Fine-grained access control

- Permissions provide administrative access to resources
 - “Fine-grained access” provides mechanism to allow individuals to grant access to specific data artifacts
 - Example: permission to “Create Content”
 - Allows user to create new content
 - Does not provide permission to view or use other user’s content, unless explicitly given by the owner
 - Exception: administrators with “full permissions” can access, modify, or delete all the related artifacts, and can change permissions
- Explicit access must be granted to work with the resources, unless you are owner or Full permission administrator for those objects
- Users given access must have the necessary permission for those resource types

Access granted to:	<div style="border: 1px solid red; padding: 2px;"> deploy18 [owner] <input type="text" value="Add more..."/> </div>
--------------------	--

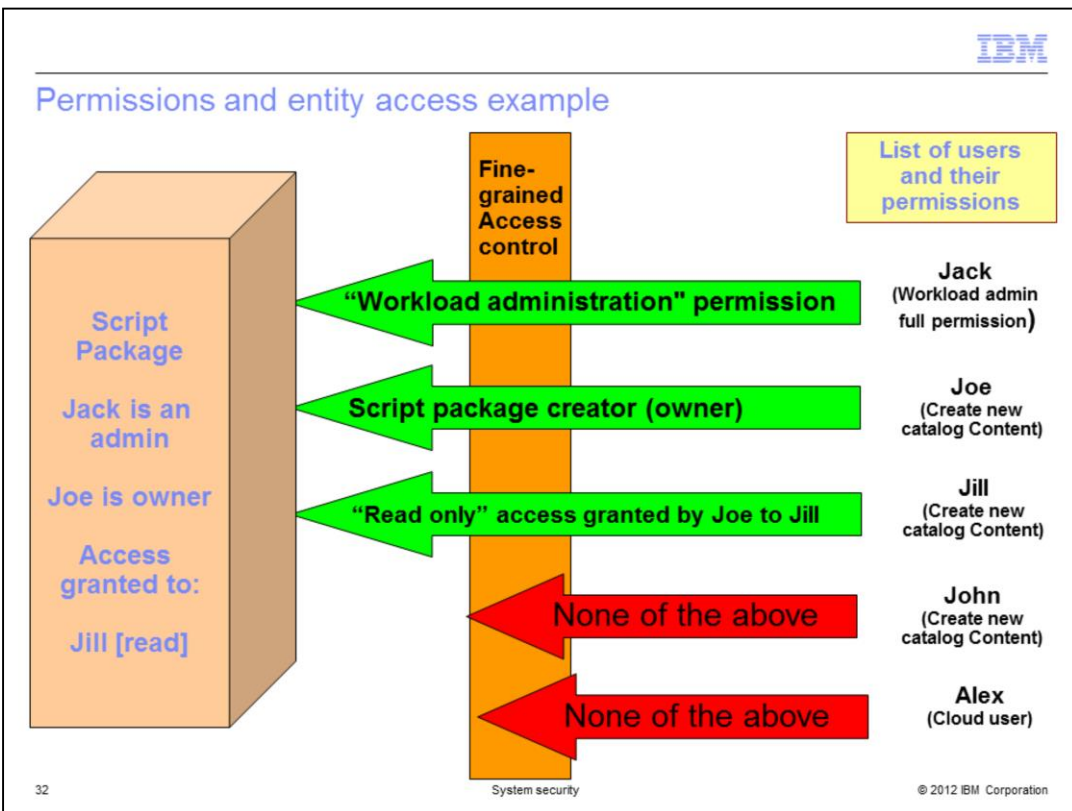
While permissions give you administrative access to certain features, you might not have access to all the data artifacts associated with that feature. The additional security mechanism implemented for low-level data artifact access is called fine-grained access control. You must explicitly be granted access to work with most of the objects that make up the PureApplication System environment, unless you are the owner or have administration authority on those objects.

Permissions provide general administrative access to resources. Fine-grained access further provides mechanism to allow owner and administrators of a given resource grant access to other users or groups. The access can be read, write, or “all” permission. This allows resource owners to protect their resources so that others cannot see, or modify, or delete resources, unless explicitly granted permission.

Users who are given access must have the general permission for those resource types.

An administrator with “Full permission” for a given resource type, by default, already have those permissions for all the resources of that type. For example Cloud administrators have access to all cloud resources. No fine grained permission is required for administrators with “Full permission.”

Permissions and entity access example



32

System security

© 2012 IBM Corporation

This example clarifies the difference between permissions and fine-grained access control. The orange vertical wall in the center of the slide represents fine-grained access control. At the right are four users that have the necessary permissions to create the script package in the catalog, shown on the left and an additional user who has “cloud user” access. Jack with “workload administration full permission” automatically has the fine-grained access to view all objects of that type. Joe with “Create new catalog content” permission is the script package creator and therefore has full access rights to the object he created. Jill has been granted “read” access to Joe’s script package, so she can see and use the object but cannot modify or delete it. Although John can create objects of the same type, he is not a workload administrator, he is not the object creator, and he has not been granted access to the script package. Hence, John cannot see or work with this script package object. Alex cannot be given any rights to the script package since he does not have “Create new catalog content” permission and does not have workload permission to view Catalog resources.

Resources for fine-grained access

- **Workload Console → Cloud**
 - Shared services
 - Environment profile
 - **Workload Console → Catalog**
 - Virtual images
 - Script packages
 - Add-ons
 - Emergency fixes
 - Reusable components
 - Virtual application templates
 - **Workload Console → Patterns**
 - Virtual applications
 - Virtual systems
 - Database patterns
 - **Workload Console → Instances**
 - Virtual applications
 - Virtual system
 - Database
 - Shared services
 - **System Console → Cloud**
 - Virtual machines
-
- Deployers can only deploy if they have read permission to both the environment profile and the pattern

Shown in the slides are resources where fine grained access control can be given by the administrators or owners of those resources. These are for all resources in the workload console and system console.

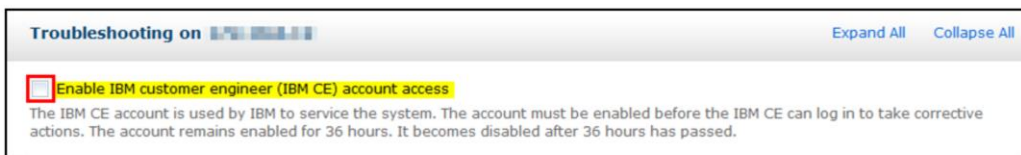
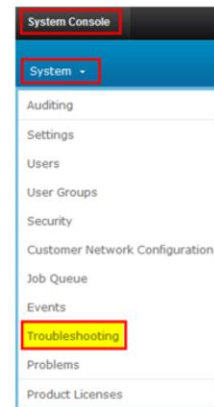
For deployment of a pattern, the deployer must have at least read permissions on the pattern itself, and permission for the environment profile that is used to target the pattern deployment.

Special access to on-site IBM service personnel

This section of the presentation focuses on the special access that a hardware administrator can provide to an on-site IBM representative for troubleshooting, maintenance and upgrades..

Special permission to service panels for IBM service personnel

- Special service panels for IBM on-site service personnel
 - Available for access to deep system level information
 - Troubleshooting
 - Maintenance
 - Upgrade the system
 - No remote access to service panels
 - Service laptop used to connect to the **internal** system network
- Service personnel use special user ID “**ibmeng**” for access
 - ID is hidden and not displayed in the user panel
 - Password:
 - Acquired from IBM Support
 - Allows access to service panels
 - Tied to a specific rack
- Client hardware administrator **MUST** enable access for service
 - **System Console** → **System** → **Troubleshooting** panel
 - Automatically disabled after 36 hours



PureApplication System provides special service panels for IBM service personnel. These service panels provide capabilities for troubleshooting, system maintenance and upgrades to the system. The service panels cannot be accessed remotely; the service personnel must be on-site in order to access them. Access is achieved by using the service laptop supplied with PureApplication Server. Only the internal system network within PureApplication System itself is accessed by the service laptop.

A special user ID called “ibmeng” is provided for access to the service laptop. This ID is hidden and does not display in any user panel. The service personnel acquire the password for this special ID from IBM support. The password is specific to only one PureApplication System.

By default, the on-site IBM service personnel cannot log into PureApplication System service console unless the client Hardware administrator gives IBM access to the login panel. To allow access, the Hardware administrator navigates to System Console > System > Troubleshooting, and then selects the check box entitled “Enable IBM customer engineer (IBM CE) account access”. This access setting automatically disables itself after 36 hours.

Summary

The next section is the summary of this presentation.

Summary

- Overview
- Security – LDAP settings
- Users
- Permissions - Details
- User groups
- Adding users to groups
- Fine-grained access control
- Special access for IBM service personnel

This presentation discussed security settings in the PureApplication Server environment. You first saw how you can optionally define an LDAP server for your system and how that impacts user and group management. You saw how users and groups were defined, how groups were modified, and how permissions were set for them. You saw information about “fine-grained access,” which provides low-level control over access to data artifacts within the system. You also saw how to enable access for IBM service personnel.

Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, PureApplication, 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](http://www.ibm.com/legal/copytrade.shtml)" 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.

© Copyright International Business Machines Corporation 2012. All rights reserved.