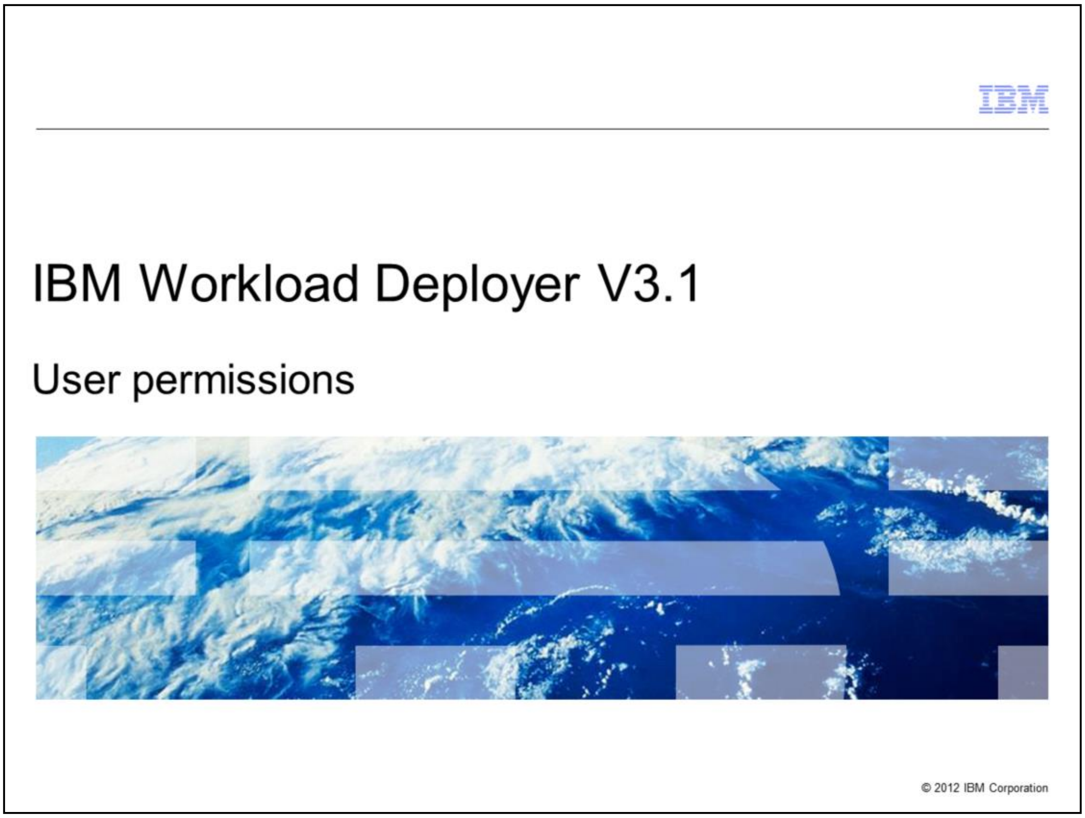


IBM Workload Deployer V3.1

User permissions

This presentation provides an overview of the permissions that can be assigned to an user or group for the IBM Workload Deployer.

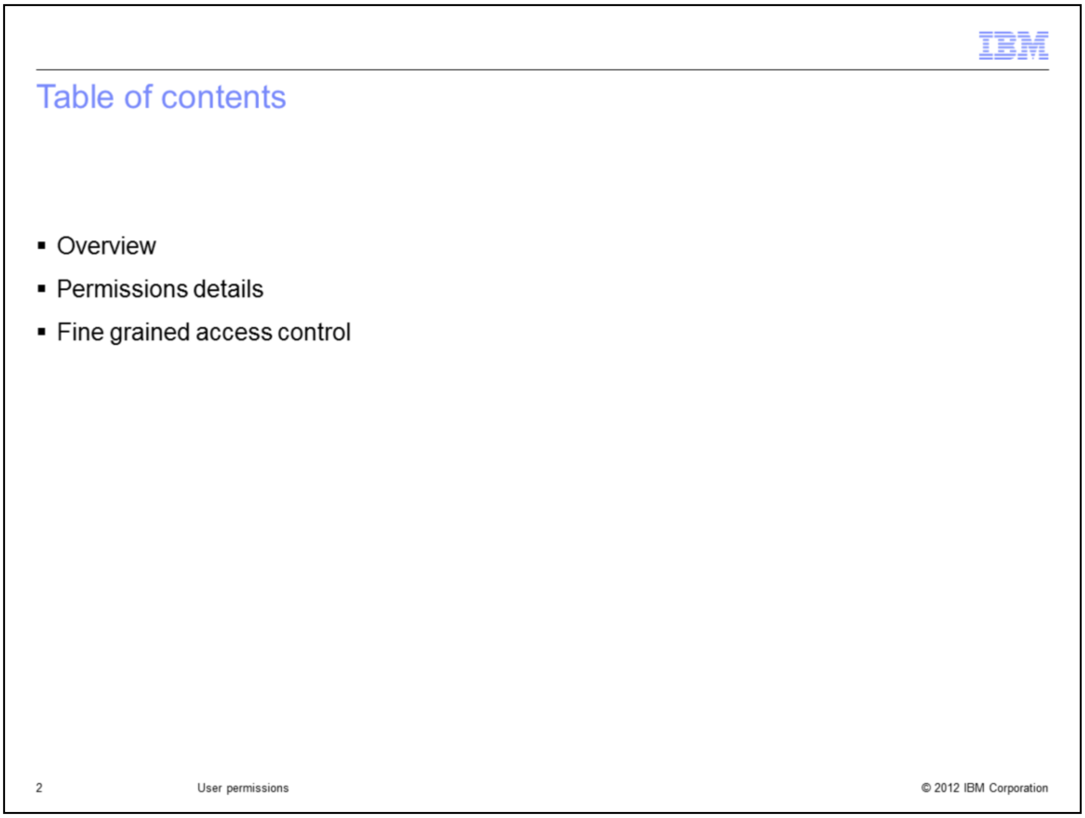


Table of contents

- Overview
- Permissions details
- Fine grained access control

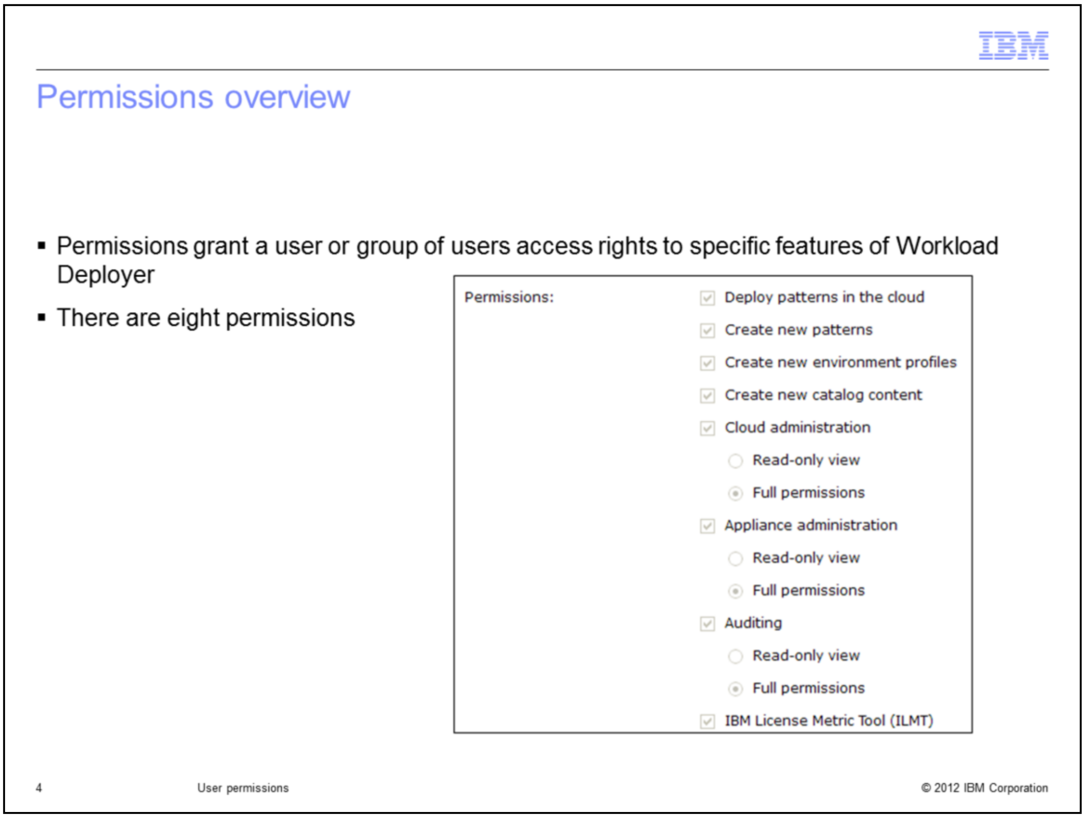
Understanding permissions and object access is critical to understanding user security in Workload Deployer. This presentation starts with an overview of user permissions. The next section will focus on detailed permissions information and permission management for users and groups. Finally, how to grant access at the data level through fine grained access control is covered.

Section

Overview

3 User permissions © 2012 IBM Corporation

This section of the presentation provides an overview of the user permissions available in the Workload Deployer Appliance.



Permissions overview

- Permissions grant a user or group of users access rights to specific features of Workload Deployer
- There are eight permissions

Permissions:

☑ Deploy patterns in the cloud
☑ Create new patterns
☑ Create new environment profiles
☑ Create new catalog content
☑ Cloud administration
○ Read-only view
● Full permissions
☑ Appliance administration
○ Read-only view
● Full permissions
☑ Auditing
○ Read-only view
● Full permissions
☑ IBM License Metric Tool (ILMT)

4 User permissions © 2012 IBM Corporation

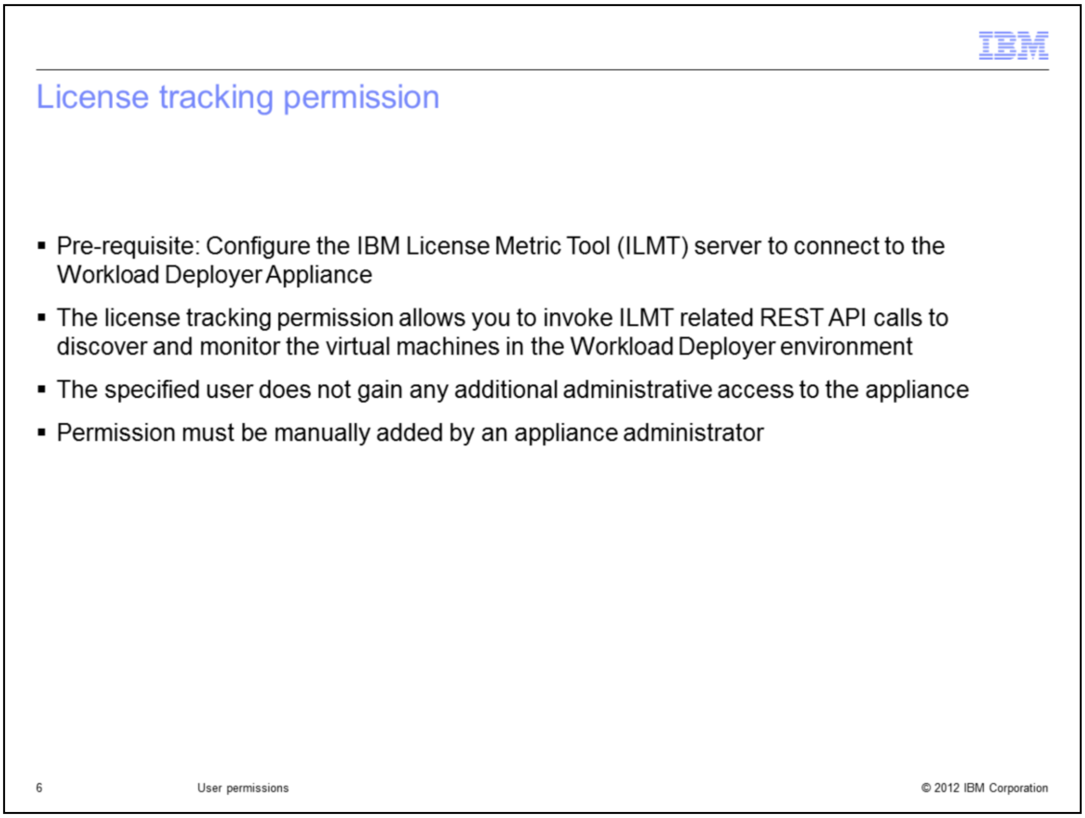
Just as you do not want everyone to be able to sign on to the operating system as the root user, you do not want everyone to be able to sign on to Workload Deployer with super user type authorities. You can separate roles by using the permissions to control the level of access for Workload Deployer users. Permissions govern each category of administrative tasks. What this means is that if you don’t have the particular permission required, you are not allowed to perform the administrative tasks associated with that permission. Additionally, the content or viewable panels that are related to that permission are not present in the Workload Deployer web console.

There are a total of seven permissions. Every user is granted “**Deploy patterns in the cloud**” permission by default. You cannot remove this permission. It allows you to deploy existing patterns into the WebSphere® cloud, but you cannot add, remove or modify any items. All other permissions must be explicitly granted by an administrator. The “**Create new patterns**” permission allows you to create and work with patterns. The “**Create new environment profiles**” permission allows you to create environment profiles. The “**Create new catalog content**” permission allows you to create and work with existing catalog content, such as virtual images, script packages, and emergency fixes. The “**Cloud administration**” permission allows you to configure cloud resources, such as IP Groups and hypervisors. The “**Appliance administration**” permission allows you to configure the appliance. Both “**Cloud Administration**” and “**Appliance administration**” is further specified with either full or read-only permission. Read-only permissions allow you to see but not modify the associated content. Full permissions are required to make modifications. When you select the “**Full permissions**” under “**Appliance administration**”**,** all of the other permissions check boxes are selected automatically. The “**Auditing”** read-only permission allows you to view auditing settings and download audit data. **“Full permissions”** under “**Auditing”** allows you to change auditing settings that are editable (such as the option to delete audit data from the Workload Deployer appliance after download) and download audit data. The “**IBM License Metric Tool (ILMT)**” permission allows the user to run licensing specific scripts or agents to gather data. By setting this permission, the specified user does not gain any additional access in the user interface.

Section

Permissions

This section of the presentation focuses on the “License Tracking” permission and the administration of user and group permissions.



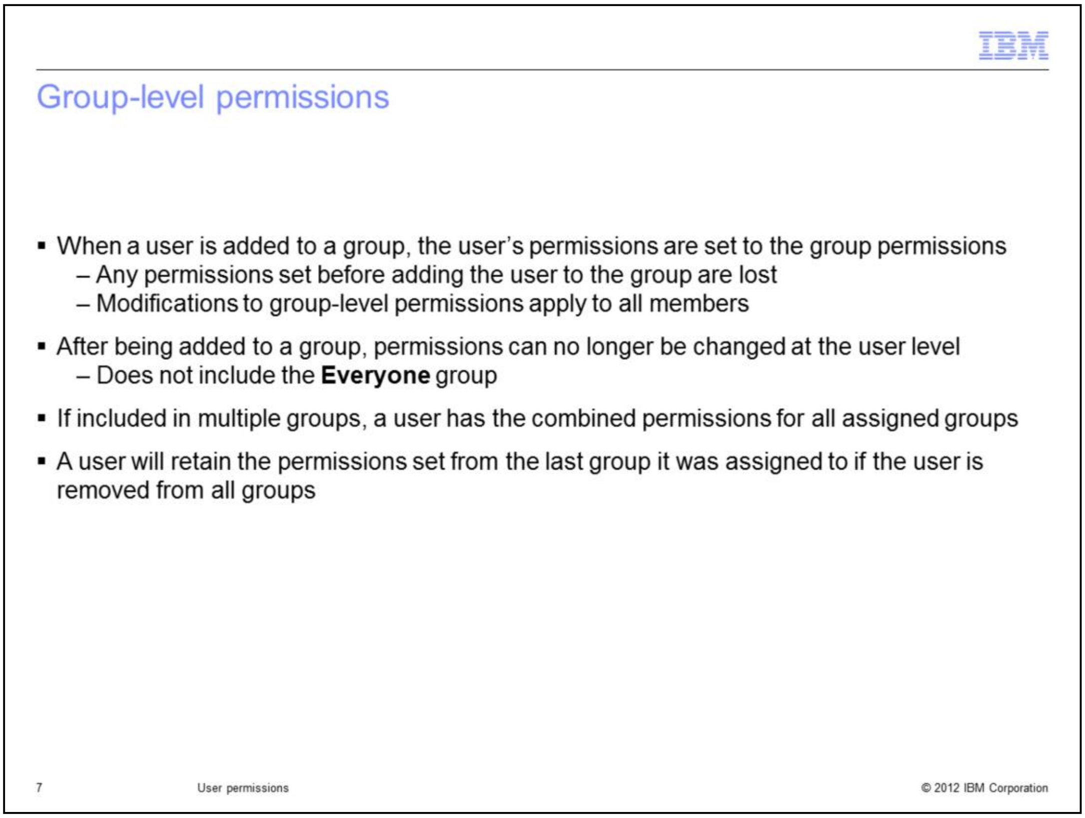
License tracking permission

- Pre-requisite: Configure the IBM License Metric Tool (ILMT) server to connect to the Workload Deployer Appliance
- The license tracking permission allows you to invoke ILMT related REST API calls to discover and monitor the virtual machines in the Workload Deployer environment
- The specified user does not gain any additional administrative access to the appliance
- Permission must be manually added by an appliance administrator

6 User permissions

To use the license tracking features of Workload Deployer, you must first configure the IBM License Metric Tool to connect to your Workload Deployer Appliance. Assigning the license tracking permission to a user will then allow you to invoke IBM License Metric Tool related REST API calls. The license tracking permission is designed to give you the ability to run specified licensing specific scripts or agents to discover and monitor virtual machines in the Workload Deployer environment, while limiting the ability to perform other administrative tasks on the appliance. This permission is not assigned by default and must be manually added by an appliance administrator after the user is created or registered.

You should not assign the license tracking permission to normal users because they might be able to use APIs to discover information about virtual machines that they are not entitled to. You should create a user with only license tracking permissions and then configure the ILMT with that user ID and password. Then only the ILMT server or anyone with access to the ILMT configuration is able to retrieve the licensing information about the Workload Deployer environment without gaining administrative access to Workload Deployer Appliance.

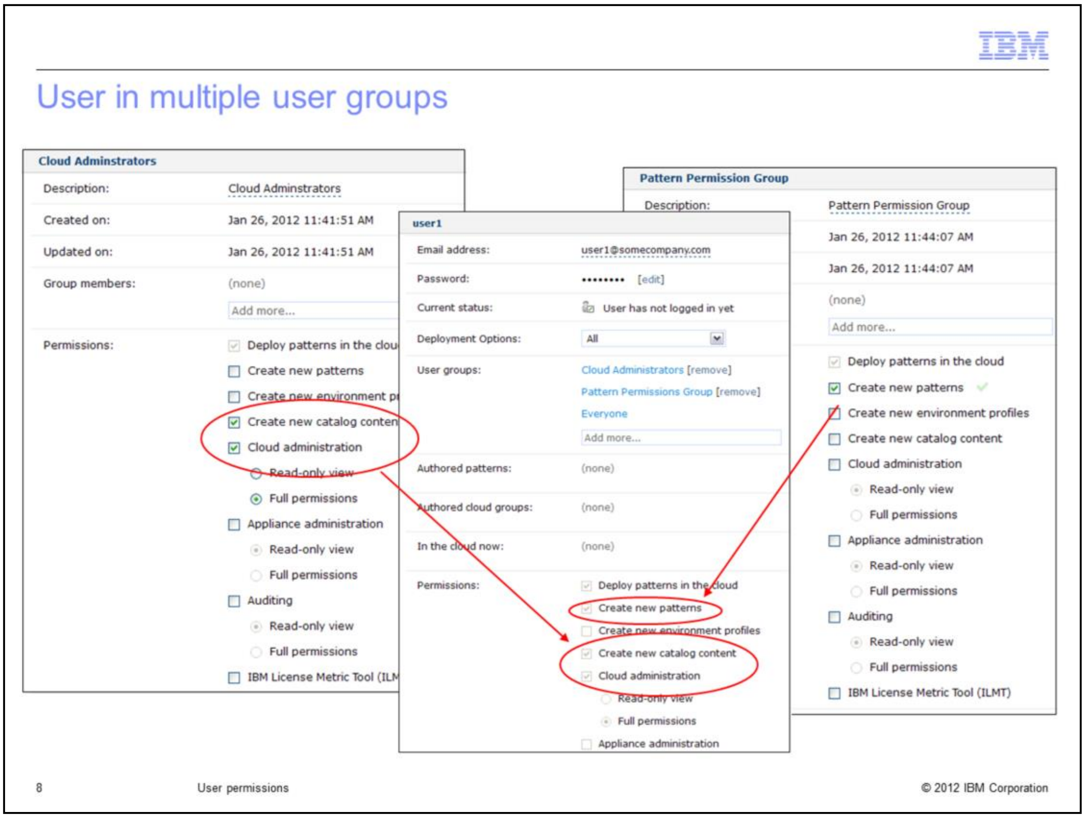


Group-level permissions

- When a user is added to a group, the user’s permissions are set to the group permissions
  - Any permissions set before adding the user to the group are lost
  - 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, a user has the combined permissions for all assigned groups
- A user will retain the permissions set from the last group it was assigned to if the user is removed from all groups

7 User permissions © 2012 IBM Corporation

When a user is added to a group, the users’ permissions are set at the group level. If any permissions were set before adding a user to a group, they are reset to the group permissions. Workload Deployer does not allow you to modify the user permissions from the User Panel if the user belongs to a group. The **Everyone** group does not count. When a user is included in multiple groups, his permissions set will reflect the combined permissions for all assigned groups.



User in multiple user groups

Cloud Adminstrators

Description: Cloud Adminstrators
Created on: Jan 26, 2012 11:41:51 AM
Updated on: Jan 26, 2012 11:41:51 AM
Group members: (none)
Add more...
Permissions:
☑ Deploy patterns in the clou
□ Create new patterns
□ Create new environment pr
☑ Create new catalog conten
☑ Cloud administration
○ Read-only view
● Full permissions
□ Appliance administration
● Read-only view
○ Full permissions
□ Auditing
● Read-only view
○ Full permissions
□ IBM License Metric Tool (ILM

user1

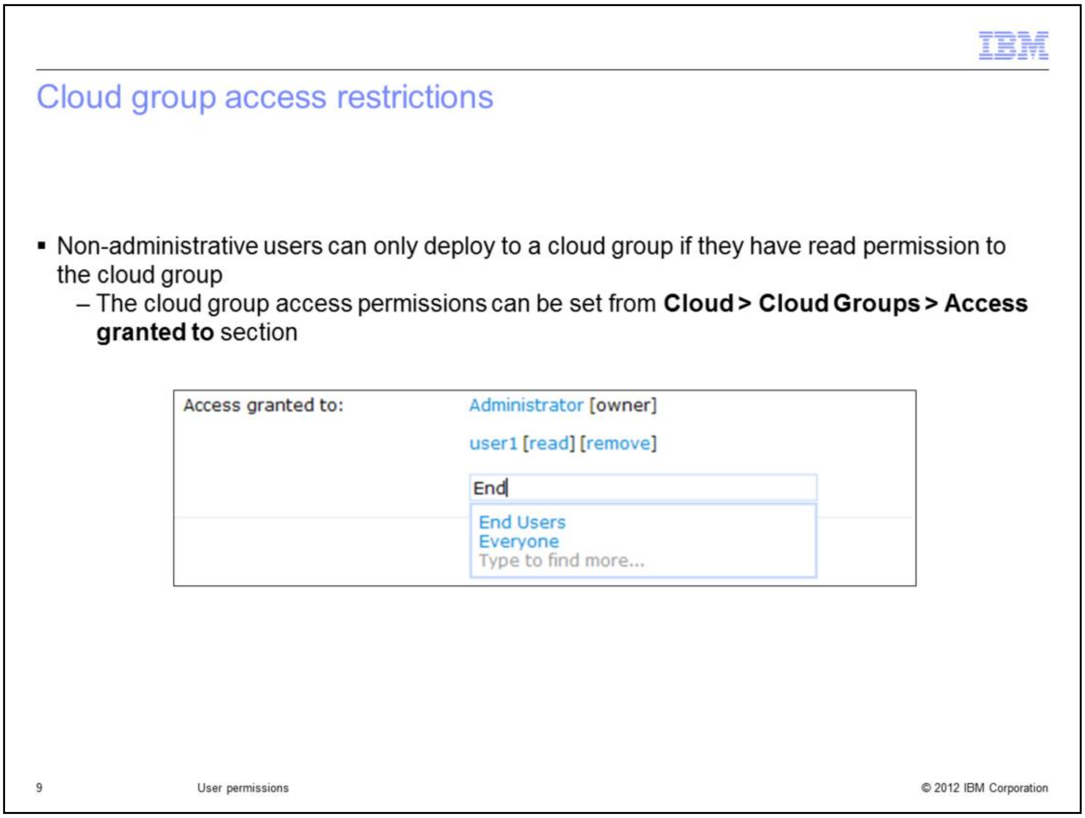
Email address: user1@somecompany.com
Password: •••••••• [edit]
Current status: User has not logged in yet
Deployment Options: All
User groups: Cloud Administrators [remove]
Pattern Permissions Group [remove]
Everyone
Add more...
Authored patterns: (none)
Authored cloud groups: (none)
In the cloud now: (none)
Permissions:
☑ Deploy patterns in the cloud
☑ Create new patterns
□ Create new environment profiles
☑ Create new catalog content
☑ Cloud administration
○ Read-only view
● Full permissions
□ Appliance administration

Pattern Permission Group

Description: Pattern Permission Group
Jan 26, 2012 11:44:07 AM
Jan 26, 2012 11:44:07 AM
(none)
Add more...
☑ Deploy patterns in the cloud
☑ Create new patterns ✓
□ Create new environment profiles
□ Create new catalog content
□ Cloud administration
● Read-only view
○ Full permissions
□ Appliance administration
● Read-only view
○ Full permissions
□ Auditing
● Read-only view
○ Full permissions
□ IBM License Metric Tool (ILMT)

8 User permissions

When a user is included in multiple groups, his or her permissions set will reflect the combined permissions for all assigned groups. For example, if user1 were assigned to a group that set the “**Cloud administration**” permission and to another group that set the “**Create new patterns**” permission, then user1 is a cloud administrator and is able to create new patterns.



Cloud group access restrictions

- Non-administrative users can only deploy to a cloud group if they have read permission to the cloud group
  - The cloud group access permissions can be set from **Cloud > Cloud Groups > Access granted to** section

Access granted to: Administrator [owner]

user1 [read] [remove]

End

End Users
Everyone
Type to find more...

9 User permissions © 2012 IBM Corporation

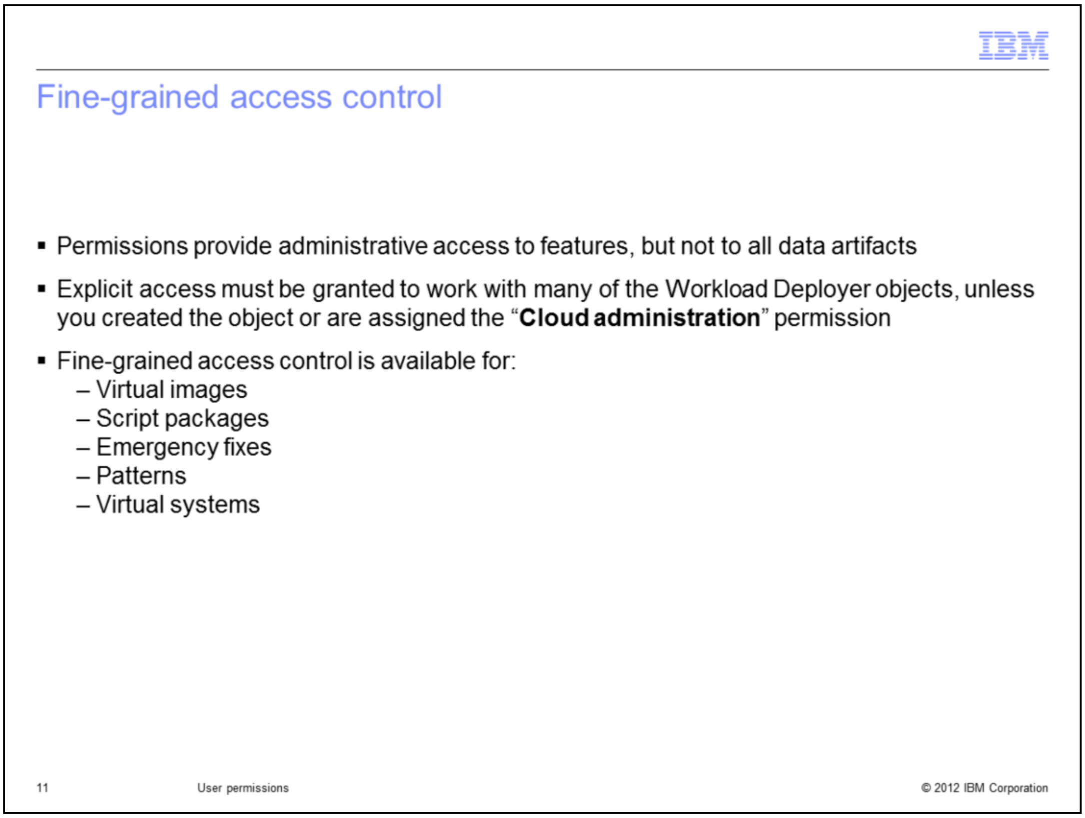
You might not want all of the users on your appliance to be able to deploy to all virtual systems in your environment. For example, you can restrict access to certain virtual systems by department, so each group within your organization has access to a unique pool of resources. Or you may want to restrict access to your production virtual systems. Regardless of your motive, you can restrict which non-administrative users have access to a particular set of virtual systems by granting users or user groups access to different cloud groups in your environment. For example, you can have one cloud group that represents your production systems and another cloud group that represents your development and test environment with a different set of users permitted to access each.

When talking about cloud group permissions, only cloud or appliance administrators can add, edit or delete hypervisors from the cloud group. However, you can set cloud group access permissions to permit some non-administrative users access to deploy patterns to cloud groups. To set the cloud group access permissions, navigate to the “**Cloud**” menu from the top menu bar, select “**Cloud Groups**” and then permissions can be set from the “**Access granted to:**” section of the “**Cloud Groups**” panel. The users you add to this section are able to deploy patterns to a Cloud Group, even if they are non-administrative users.

Section

Fine-grained access control

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

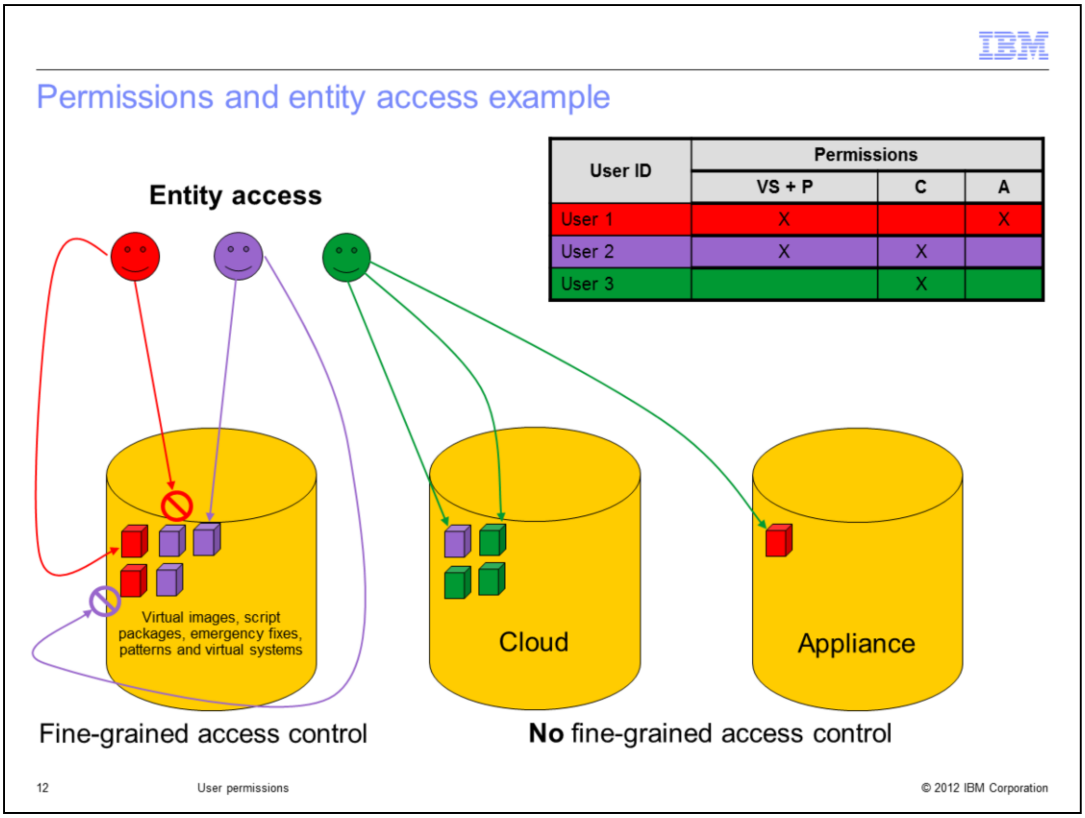


Fine-grained access control

- Permissions provide administrative access to features, but not to all data artifacts
- Explicit access must be granted to work with many of the Workload Deployer objects, unless you created the object or are assigned the "**Cloud administration**" permission
- Fine-grained access control is available for:
  - Virtual images
  - Script packages
  - Emergency fixes
  - Patterns
  - Virtual systems

11 User permissions © 2012 IBM Corporation

While permissions give you administrative access to certain features, you will not likely have access to all the data associated with that feature. The additional security mechanism required is called fine-grained access control. You must explicitly be granted access to work with many of the objects that make up your Workload Deployer environment, unless you created that object or have Cloud administration permission. The following objects are restricted by fine-grained access control: virtual images, script packages, emergency fixes, patterns and virtual systems.



Permissions and entity access example

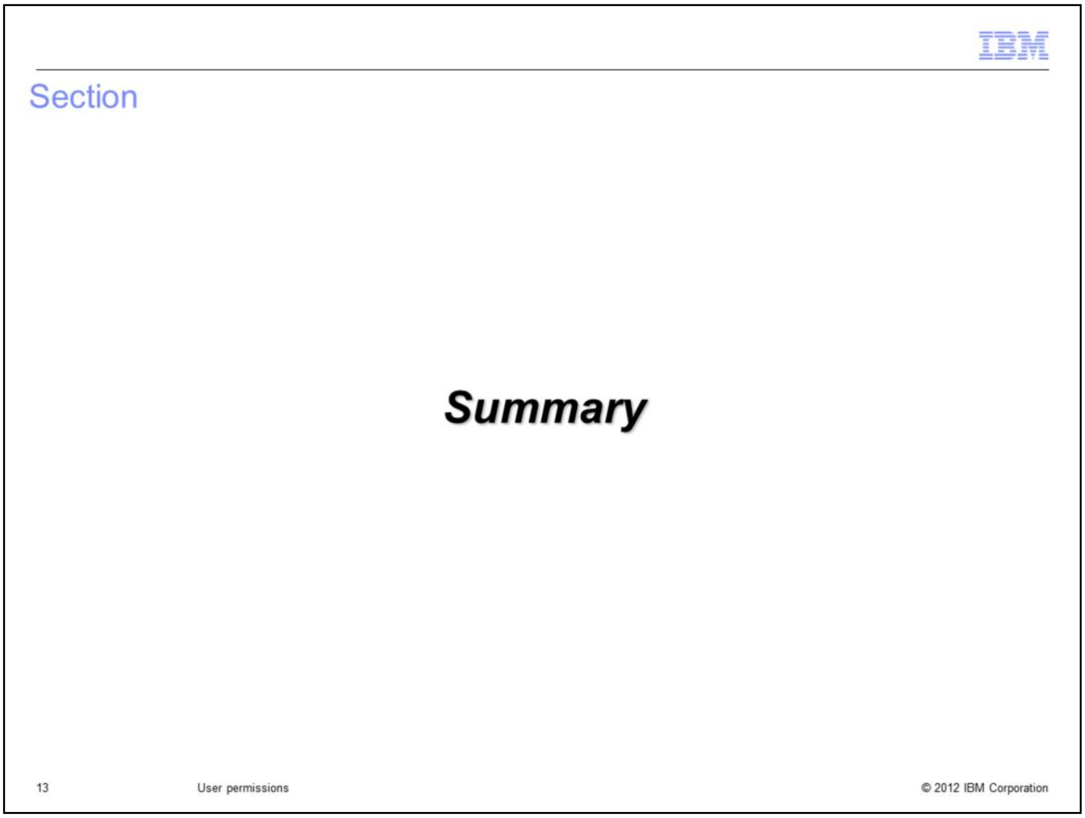
User ID	Permissions		
	VS + P	C	A
User 1	X		X
User 2	X	X	
User 3		X	

Entity access
Virtual images, script packages, emergency fixes, patterns and virtual systems
Cloud
Appliance
Fine-grained access control
No fine-grained access control

12 User permissions © 2012 IBM Corporation

This example is provided to help clarify the difference between permissions and fine grained access control. The table here shows the specific permissions for the three users in this example. It shows that User 1 created two virtual systems and patterns as defined by the red blocks. The graphic also shows that User 2 created three virtual systems and patterns defined by the purple blocks. Both User 2 and User 1 can create patterns and virtual systems because they both are assigned the “**Deploy patterns in the cloud**” and “**Create new patterns**” permissions.

Now here is where fine-grained access control comes into the picture. Even though both User 2 and User 1 have the “**Deploy patterns in the cloud**” and “**Create new patterns**” permissions, this does not imply that they can view patterns and virtual systems created by someone else. So User 2 cannot view User 1’s data and User 1 cannot view User 2’s data. If User 2, for example, needed to view or modify User 1’s patterns or virtual systems then User 1 needs to specifically grant access to User 2.

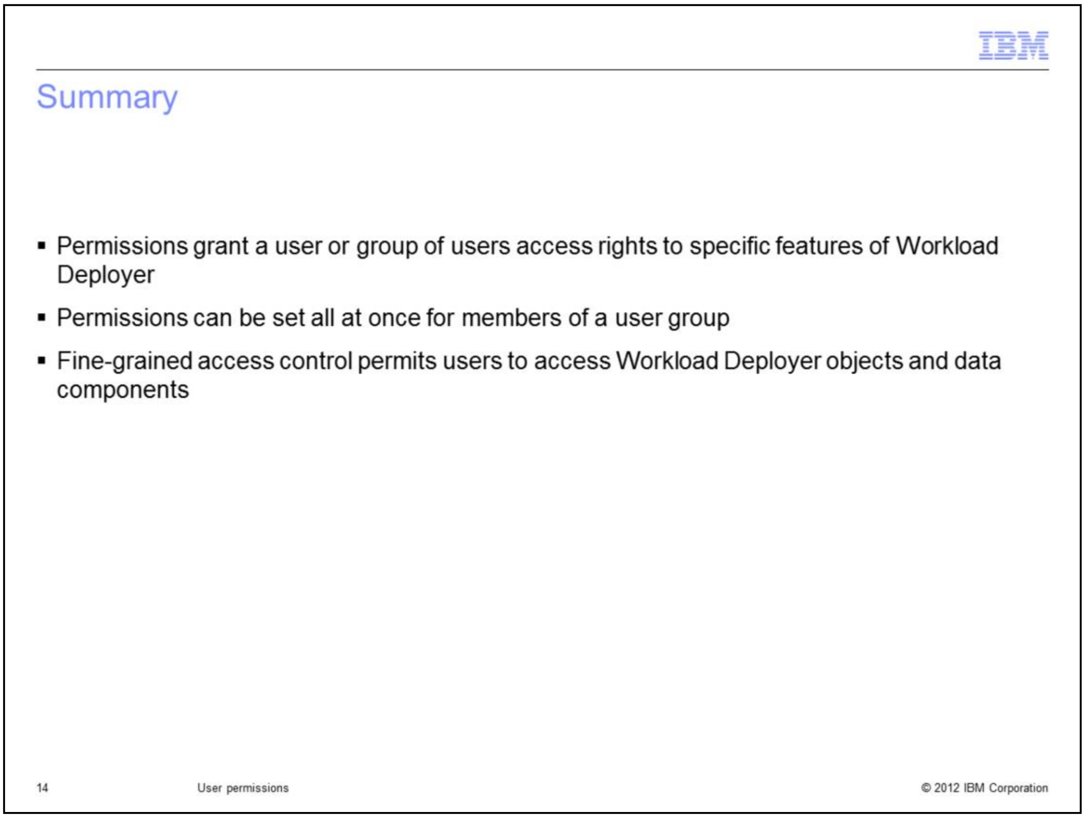


Section

Summary

13 User permissions

This section is the summary.

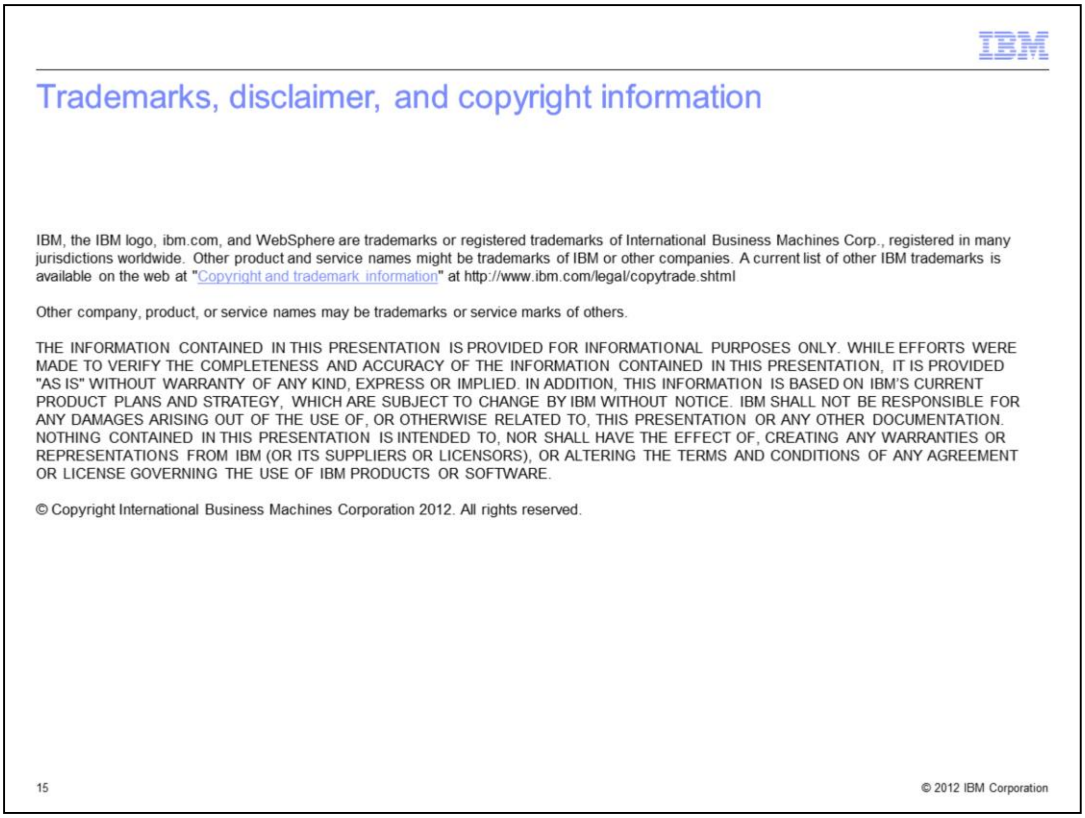


Summary

- Permissions grant a user or group of users access rights to specific features of Workload Deployer
- Permissions can be set all at once for members of a user group
- Fine-grained access control permits users to access Workload Deployer objects and data components

14 User permissions © 2012 IBM Corporation

User permissions are defined to control the level of access to the Workload Deployer Appliance and to determine which web console panels are viewable and modifiable. Permissions can be set for multiple users at once at the group level. To manage the data components of a particular feature, fine-grained access control is used. Understanding permissions and object access is critical to understanding user security in Workload Deployer.



Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, 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.