This presentation will cover CloudBurst's security features.

Agenda

- Creating users and groups
- Understanding permissions and entity access
- User authentication
- WebSphere® cloud secure communications
- CloudBurst appliance security

This presentation will cover aspects of CloudBurst security. You will cover users and user groups, permissions, entity access, LDAP integration and appliance security.

Section

Creating users and groups

This section will walk through setting up users and groups.

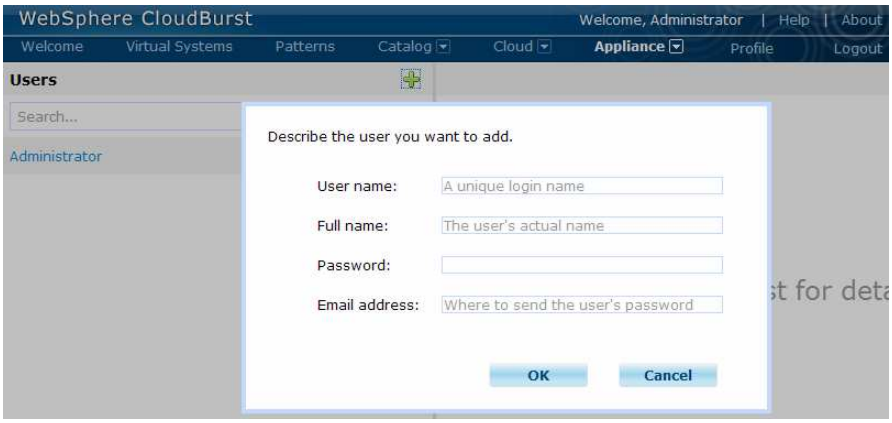
Create users

- Create individual users
- Create logical groups of users

There are two ways to create users and groups. You can access the feature through the main welcome page or you can click the “Appliance” button located on the feature ribbon.

Administrator creates user ID

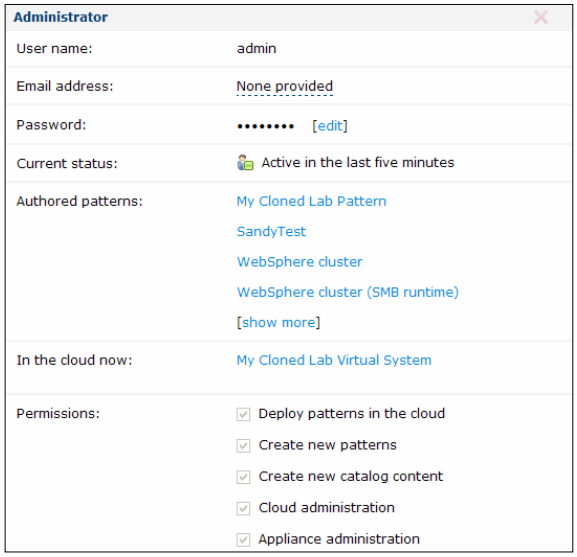
- Administrator creates a user ID and an initial password for a new user
- New user will receive user ID and password by way of e-mail
- New user can then change his password



Creating a user is a two step process. You first need to supply basic information such as user name, full name, password and an e-mail address. The e-mail address is used to send you your initial password and for other CloudBurst notifications such as when the user's virtual system starts up. The second part of user creation is to assign the user permissions.

User attributes

- User attributes view
  - Patterns authored
  - Deployed virtual systems
  - Permissions



The user's attributes page allows the administrator to view which patterns and virtual systems the user is authorized to view and modify. This view also allows the administrator to edit the password and assign permissions to the user. Permissions grant users the ability to use specific CloudBurst features. All users are granted the "Deploy patterns in the cloud" permission. Permissions are further discussed in a follow-up slide.

User register their own account

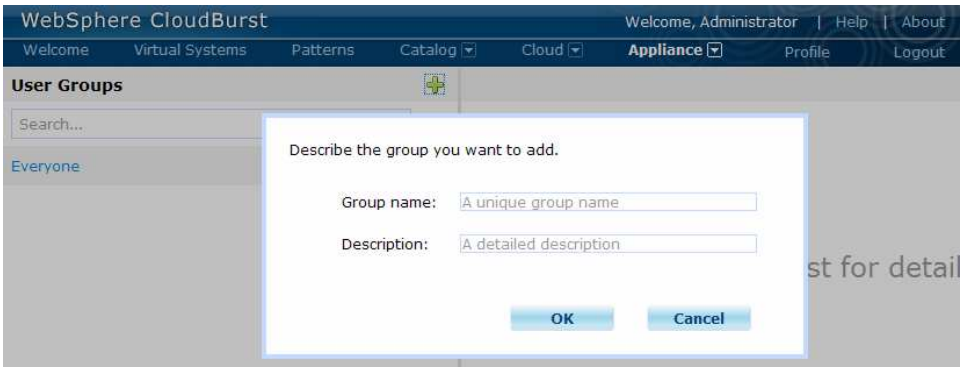
- Enable users to register for their own accounts

There are two ways to create a new user account. Either the administrator can create the account which you have seen in the prior slides or the user can create their own account. In order to allow the users to create their own account you need to activate this feature. To activate this feature navigate to the “Settings” by way of the “Appliance” tab. Enable the “Allow new users to create their own accounts” settings. This will have the side effect of adding a “Register” button to the initial login screen.

Any user is able to create an account and they will be assigned the default “Deploy patterns in the cloud” permission. If the user requires additional permissions the administrator will need to assign those permissions.

Create groups

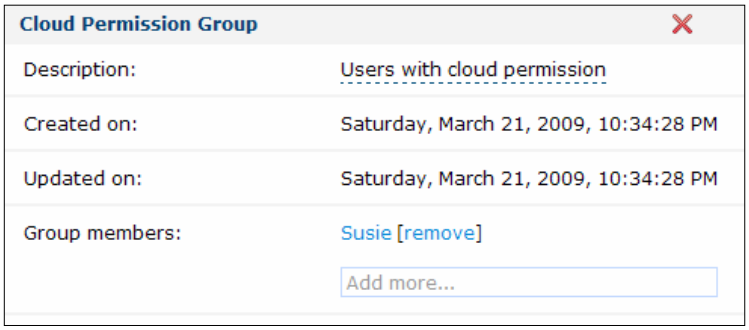
- Groups allow you to group users according to some criteria that you define



Groups allow you to group users according to some criteria that you define. For example you can group administrators together or group by department. Once you create the group you will need to add users to the group.

User group attributes

- User group attributes view
  - View group members
  - Add group members
  - Remove group members

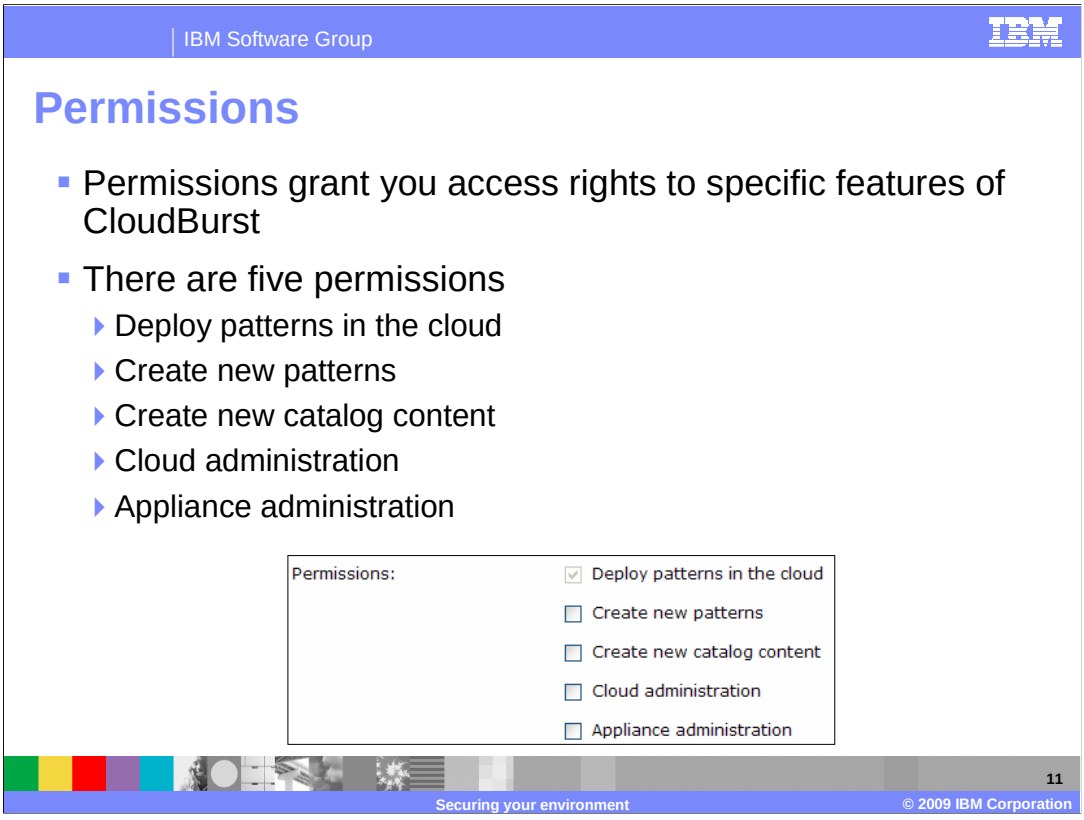


In the user group attributes view, you can view current group members, remove group members and add additional group members.

Section

Understanding permissions and entity access

Understanding permissions and entity access is key to managing user security within CloudBurst.



Separating the roles is crucial to managing security within CloudBurst. Just as you wouldn't want everyone signing on to the operating system as root you wouldn't want everyone signing on to CloudBurst with root type authorities. This separation of roles can be accomplished by the use of permissions in CloudBurst.

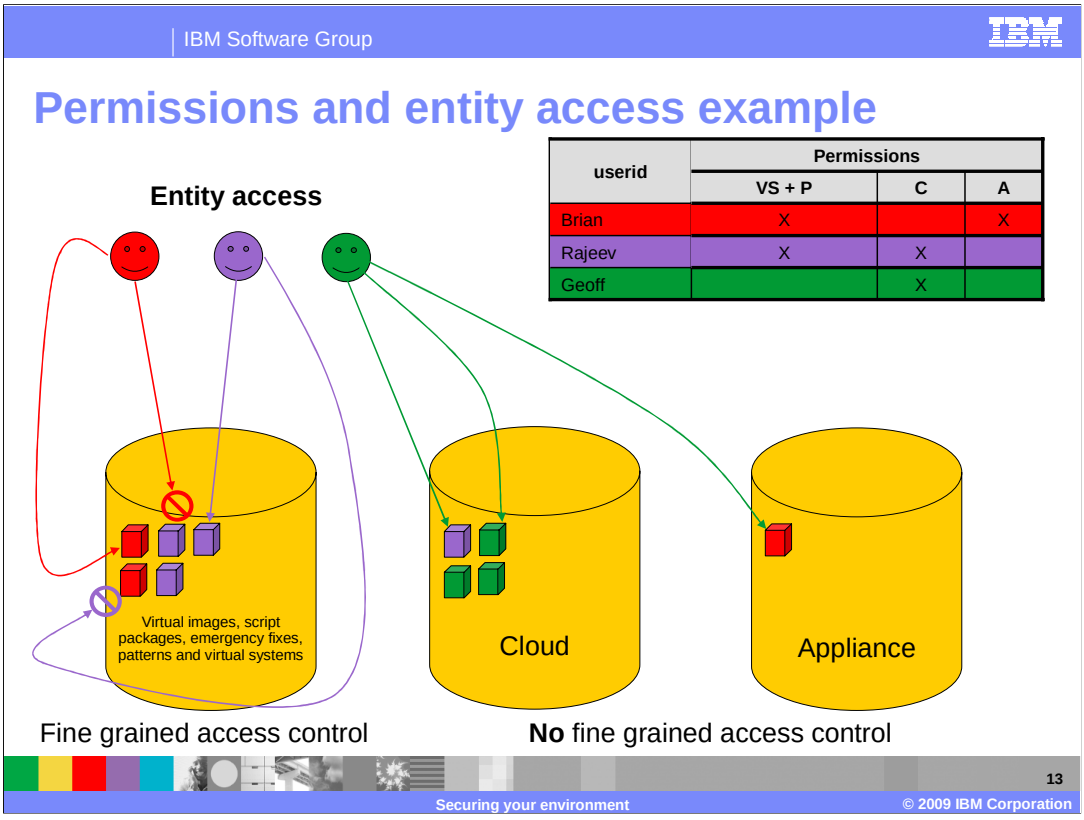
Each feature in CloudBurst is governed by a permission. What this means is that if you don't have the permission you are not allowed to use that particular feature. Taking this one step further if you don't have a permission then the specific features associated with the permission will not be present in the CloudBurst administrative console. Every user is granted "Deploy patterns in the cloud" permission by default. You cannot remove this permission.

There are a total of five permissions. The "Deploy patterns in the cloud" permission is the default permission and allows you to deploy existing patterns into the WebSphere cloud. The "Create new patterns" permission allows you to create and work with patterns. 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.

Fine grained access control

- Permissions are high level constructs and entities are the parts contained within these constructs
- Fine grained access control is available for
  - Virtual images
  - Script packages
  - Emergency fixes
  - Patterns
  - Virtual systems

Permissions give you access to specific features, but this does not mean you have access to all data specific to that feature. This security feature is what is called fine grained access control. Fine grained access control is available for virtual images, script packages, emergency fixes, patterns and virtual systems.



The difference between permissions and fine grained access control can be confusing so to clarify the difference an example is provided. The table above shows the specific permissions for each of the three users in this example.

In this example it shows that Brian created two virtual systems and patterns as defined by the red blocks. The graphic also shows that Rajeev created three virtual systems and patterns defined by the purple blocks. Both Rajeev and Brian 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 fined grained access control comes into the picture. Even though both Rajeev and Brian 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 Rajeev cannot view Brian’s data and Brian cannot view Rajeev’s data. If Rajeev for example needed to view or modify Brian’s patterns or virtual systems then Brian would need to specifically grant access to Rajeev.

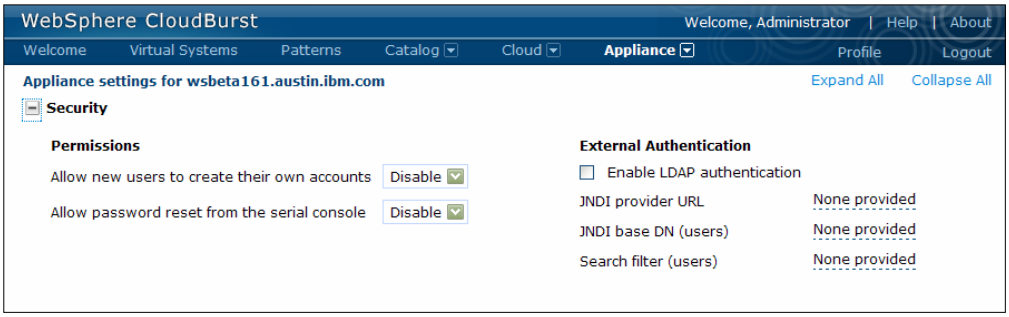
Section

User authentication

This section will cover user authentication.

Setting up LDAP

- From this panel you can connect to an existing LDAP server
- Authentication only



CloudBurst can work in conjunction with an LDAP server. LDAP is only used for authentication purposes. Authorization is performed by the CloudBurst appliance. What this means is that the users are defined locally in CloudBurst and backed up by the LDAP server. Groups are only defined locally in CloudBurst. All security data is stored on the flash drive found within the tamper proof case of the CloudBurst appliance and any attempt to breach the case will result in the appliance not being able to boot. The flash drive is encrypted and the key is tied to the box, so you are unable to move the flash drive to another device.

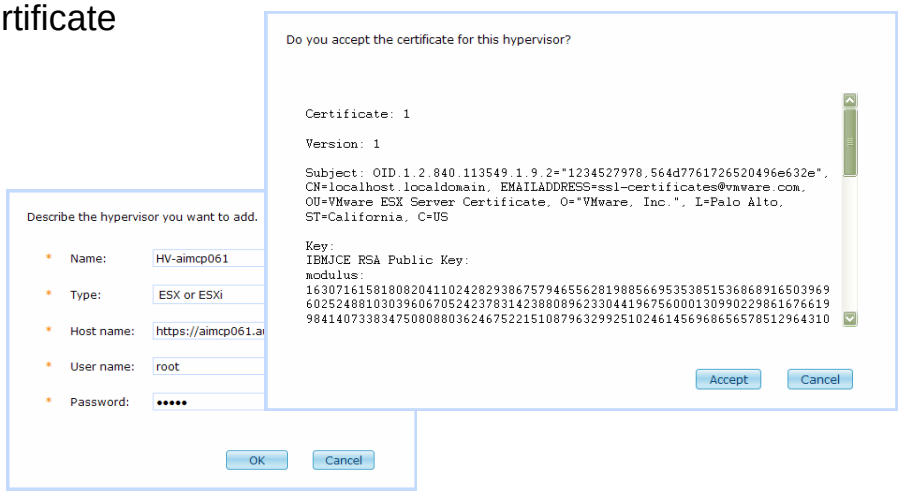
Section

WebSphere cloud secure communications

This section covers WebSphere cloud secure communications.

WebSphere cloud secure communications

- Adding a hypervisor requires acceptance of hypervisor's certificate



When you add a hypervisor to CloudBurst you are required to accept the hypervisor's public certificate. By accepting this certificate you are guaranteeing any further communication between CloudBurst and the hypervisor will be encrypted.

Section

CloudBurst appliance security

This section covers CloudBurst appliance security.

Appliance security

- Contents of flash drive and hard disks are encrypted using key unique to the appliance
- Sensitive data such as passwords and encryption keys stored on internal flash drive inside tamper proof case
- Appliance provides no way for user to upload executable scripts or code outside of the script package mechanism
- System backup is encrypted
- Appliance contains no command shell
- Appliance follows Just enough OS (JeOS) concepts

This slide is intended to show some but not all of the security features built into the CloudBurst appliance to protect your sensitive data.

Contents of the flash drive and the hard disks are encrypted using a key unique to the appliance. Each appliance has its own unique key and this key is not viewable. The outcome of this is that any data encrypted on a specific appliance can only be decrypted on that same appliance. If someone were to steal your external hard drive they can not decrypt it. The flash drive contains sensitive information such as passwords and private keys. The flash drive is housed inside the tamper proof case and any attempt to open the case will cause the appliance to not boot. The system will need to be brought to IBM for a factory reset. In both cases, worst outcome is that you have a loss of data and no security breach.

Appliance provides no way for anyone to upload executable scripts or code outside of the script package mechanism. The only mechanism by which to upload software to the appliance is by way of the firmware upgrade feature. And even in this case the firmware must be signed by a trusted authority before it is accepted by the appliance. System backup is encrypted using a user supplied key or a key generated by the appliance. The appliance contains no command shell and follows the Just enough OS concepts.

Section

Summary

The next slide provides a summary of this presentation.

Summary

- As you can seen CloudBurst offers an extensive list of security features
  - Users and groups
  - Permissions and fine grained access control
  - Authentication by way of LDAP
  - Secure communications between CloudBurst and the WebSphere cloud
  - CloudBurst appliance security measures

CloudBurst offers an extensive list of security features. This presentation went through many but not all of the security features offered by CloudBurst. You went through setting up users and groups, working with LDAP for the added authentication benefits, secure communications between CloudBurst and the WebSphere cloud and security measures of the CloudBurst appliance. All areas that make up the CloudBurst environment have been given security considerations.

Feedback

Your feedback is valuable

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

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

Click to send e-mail feedback:

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

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

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

Trademarks, copyrights, and disclaimers

IBM, the IBM logo, ibm.com, and the following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

WebSphere

If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. 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.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements or changes in the products or programs described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (for example, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.