

IBM WebSphere CloudBurst Appliance

Appliance settings



This presentation will discuss the settings for IBM WebSphere® CloudBurst™ appliance.

Table of contents

- Customize settings
 - Application identification
 - Security
 - Ethernet interfaces
 - Domain name servers
 - Date and time
 - Mail delivery
 - Backup and restore
 - Firmware
 - Power
- Create users

When you are setting up your WebSphere CloudBurst Appliance, you will want to modify some of the appliance settings and create new user accounts to perform different operations on the appliance. This presentation will discuss the **Customize settings** and **Create users** functions of the WebSphere Cloudburst appliance. The settings include **application identification, security, Ethernet interfaces, domain name servers, date and time, mail delivery, backup and restore, firmware, and power**. You will see how to create users, review user information, and see what permissions you can set from the user definition screen.

WebSphere CloudBurst Appliance settings

This section will discuss a general overview of the WebSphere Cloudburst Appliance settings.

Settings

The screenshot shows the WebSphere CloudBurst administrator interface. At the top, the navigation bar includes 'Welcome, Administrator', 'Help', and 'About'. Below this, a secondary navigation bar contains 'Welcome', 'Virtual Systems', 'Patterns', 'Catalog', 'Cloud', 'Appliance', 'Profile', and 'Logout'. The 'Appliance' menu is open, showing options for 'Settings', 'Users', 'User Groups', 'Task Queue', and 'Troubleshooting'. The 'Settings' option is highlighted with a red box and a hand cursor. A yellow callout box with the text 'One way to access settings' points to the 'Customize settings' link under 'Step 1: Set up the appliance'. Another yellow callout box with the text 'Another way to access settings' points to the 'Settings' option in the 'Appliance' dropdown menu. The main content area is titled 'Welcome to WebSphere CloudBurst!' and provides a brief overview of the appliance's function. It is divided into 'Deployment made easier' (with four steps) and 'Additional tasks'.

WebSphere CloudBurst

Welcome, Administrator | Help | About

Welcome Virtual Systems Patterns Catalog Cloud Appliance Profile Logout

Welcome to WebSphere CloudBurst!

WebSphere CloudBurst is a hardware appliance that automates and optimizes the deployment of WebSphere Application Server environments.

Deployment made easier

Step 1: Set up the appliance
Customize the appliance settings. Create user accounts. You can also create user groups.
[Customize settings](#) [Create users](#)

Step 2: Set up the cloud
Create the cloud by identifying IP groups and collections of hypervisors called cloud groups.
[Add IP groups](#) | [Add cloud groups](#)

Step 3: Create a virtual system
Create a virtual system by deploying a reusable pattern.
[Select a pattern to deploy](#)

Step 4: View virtual systems
View the current status, metrics, and details of virtual systems in the cloud.
[View virtual systems](#)

Additional tasks

Appliance ▾

- [Settings](#)
- [Users](#)
- [User Groups](#)
- [Task Queue](#)
- [Troubleshooting](#)

4 Appliance settings © 2010 IBM Corporation

After you have logged on to the WebSphere CloudBurst appliance, you will see the welcome screen. To set up the appliance, you click **Customize settings** under the topic “Step 1: Set up the appliance” topic. Alternatively you can click **Appliance** within the title bar, and within the pull down that opens, click **Settings**.

Appliance settings

WebSphere CloudBurst

Welcome Virtual Systems Patterns Catalog Cloud **Appliance**

Appliance settings for 9.3.75.157

- + Appliance Identification
- + Security
- + Ethernet Interfaces
- + Domain Name Servers
- + Date and Time
- + Mail Delivery
- + Backup and Restore
- + Firmware
- + Power

Appliance settings will allow you to customize appliance identification, security, Ethernet interfaces, domain name servers, date and time, mail delivery, backup and restore, review and update firmware, and administer power.

Appliance Identification

The screenshot shows the 'Appliance Identification' settings for a WebSphere CloudBurst appliance. The page title is 'WebSphere CloudBurst' and the breadcrumb trail includes 'Welcome', 'Virtual Systems', 'Patterns', 'Catalog', 'Cloud', and 'Appliance'. The main heading is 'Appliance settings for 9.3.75.157'. Under the 'Appliance Identification' section, the following fields are visible:

Appliance name	None provided
Appliance group	None provided
Appliance unique identifier	6804133

Below this section, there are several expandable categories: Security, Ethernet Interfaces, Domain Name Servers, Date and Time, Mail Delivery, Backup and Restore, Firmware, and Power. Three yellow callout boxes are present on the left side of the page:

- 'Add or modify appliance name' points to the 'Appliance name' field.
- 'Add or modify appliance group' points to the 'Appliance group' field.
- 'View appliance unique identifier' points to the 'Appliance unique identifier' field.

At the bottom left of the page, the number '6' is displayed. At the bottom center, the text 'Appliance settings' is shown. At the bottom right, the copyright notice '© 2010 IBM Corporation' is present.

WebSphere CloudBurst appliances can be named and assigned to appliance groups for easy identification on the network

Security

WebSphere CloudBurst Welcome, Administrator

[Welcome](#)
[Virtual Systems](#)
[Patterns](#)
[Catalog](#)
[Cloud](#)
[Appliance](#)
Pr...

Appliance settings for 9.3.75.157 Expand All

[Appliance Identification](#)
[Security](#)

Permissions

Allow new users to create their own accounts

Allow password reset from the serial console

Sessions

Logout inactive users after 24 hours. [\[edit\]](#)

External Authentication

Enable LDAP authentication

Name	None provided
JNDI provider URL	None provided
JNDI base DN (users)	None provided
JNDI base DN (groups)	None provided
Search filter (users)	(&(uid={0})(objectclass=inetOrgPerson))
JNDI security authentication	None provided
Password [edit]

[Test LDAP authentication settings](#)

To test whether LDAP authentication settings are setup correctly.

LDAP user name

LDAP group name

7 Appliance settings © 2010 IBM Corporation

Within the security settings, you can customize some of the settings for permissions and external authentication. Within permissions, you can allow or disallow new users to create their own accounts within the appliance. Also, you can allow or disallow a password reset from within the serial console. External authentication allows you to enable LDAP authentication and provides the capability to test the LDAP settings.

Ethernet interfaces

WebSphere CloudBurst Welcome, Administrator

Welcome Virtual Systems Patterns Catalog Cloud **Appliance**

Appliance settings for 9.3.75.158

Security

Ethernet Interfaces Add, delete, modify Ethernet interfaces

Interface	IP address/mask	Default gateway	MTU	Mode
<input checked="" type="checkbox"/> eth0	172.16.0.217/21	None provided	1500	Auto
<input checked="" type="checkbox"/> eth1	None provided	None provided	1500	Auto
<input checked="" type="checkbox"/> eth2	172.16.15.194/21	None provided	1500	Auto
<input checked="" type="checkbox"/> mgmt	9.3.75.158/24	9.3.75.1	1500	Auto

Ethernet interfaces status

Interface	MAC address	Link status	Mode status	Collisions	Received				Transmitted				
					kilobytes	packets	errors	drops	kilobytes	packets	errors	drops	
eth0	00:1a:64:88:93:d9	no-link	10baseT-HD	0	0	0	0	0	0	0	0	0	0
eth1	00:14:5e:f1:d4:26	no-link	10baseT-HD	0	0	0	0	0	0	0	0	0	0
eth2	00:14:5e:f1:d4:28	no-link	10baseT-HD	0	0	0	0	0	0	0	0	0	0
mgmt	00:1a:64:88:93:d8	ok	100baseT	0	8371	94995	0	0	2327	2816	0	0	0

Link status

Check for collisions

Received errors or drops?

Transmitted errors or drops?

8 Appliance settings © 2010 IBM Corporation

The Ethernet interfaces settings allow you to review Ethernet definitions and to add, change, or delete these definitions. The status portion of the screen allows you to review the individual Ethernet interfaces. This includes MAC address, link status, mode status, number of collisions, the number of kilobytes sent and received, the number of packets sent and received, and the number of errors and dropped packets.

Domain name servers

The screenshot displays the 'Appliance settings for 9.3.3.3' page in the WebSphere CloudBurst console. The navigation bar includes 'Welcome', 'Virtual Systems', 'Patterns', 'Catalog', and 'Cloud'. The 'Domain Name Servers' section is expanded, showing a list of servers with IP addresses 9.3.3.11 and 9.3.3.1, each with a red 'x' icon. A 'Click to add' link is present. A yellow callout bubble points to the 'Add, delete or review DNS' text. Below this, a 'Lookup host name or IP address' section features a text input field containing 'server3.mycompany.com' and a 'Lookup' button. A second yellow callout bubble points to the 'Lookup' button with the text 'Validity check host names or IP addresses'. The results below the input show 'Host name: server3.mycompany.com' and 'IP address: 9.3.3.3'. The footer contains the page number '9', 'Appliance settings', and '© 2010 IBM Corporation'.

The domain name server settings allow you to review, delete, and add domain name servers. It also provides a lookup function to allow you to verify host names or IP addresses, which assists you with validation of the environment.

Date and time

WebSphere CloudBurst

Welcome Virtual Systems Patterns Catalog Cloud

Appliance settings for 9.3.3.3

- + Security
- + Ethernet Interfaces
- + Domain Name Servers
- **Date and Time**

The current time is Dec 9, 2009 1:02:48 PM

The current time zone is

NTP server addresses

someNTPserver.com ↑ ↓ ✕

someOtherNTPserver.com ↑ ↓ ✕

[Click to add](#)

Set time zone

Review, add, delete NTP servers

The date and time setting allows you to set the time zone for the appliance and to add, review, and delete network time protocol servers.

Mail delivery

The screenshot shows the WebSphere CloudBurst management console. The main heading is "WebSphere CloudBurst" with a navigation bar containing "Welcome", "Virtual Systems", "Patterns", and "Catalog". Below this, the page is titled "Appliance settings for 9.3.3.3". A list of settings categories is shown with expand/collapse icons: Security, Ethernet Interfaces, Domain Name Servers, Date and Time, and Mail Delivery. The "Mail Delivery" section is expanded, showing two settings: "SMTP server" with the value "someSMPT.server.com" and "Reply-to address" with the value "purple-box@Lab.com". Two yellow callout boxes with black text point to these values: "SMTP server" points to the first value, and "Reply-to address" points to the second value.

The mail delivery settings allow you to add, delete, or change the SMTP server setting and reply-to address for the appliance. These settings are used by the appliance when it delivers notification messages to users defined within the appliance.

Backup and restore

Backup and Restore

Step 1: Find a place to store your backups

Step 2: Secure your backups

Step 3: Schedule a new backup

Step 4: Restore from a backup

Click each
step to see
settings

Using the backup and restore settings, you can ensure that the appliance can be restored when required. Click each step to see the settings. The four steps involved in setting up the backup and restore environment are: Step 1: Find a place to store your backups, Step 2: Secure your backups, Step 3: Schedule a new backup, and Step 4: Restore from a backup.

Backup and restore – store your backups

Backup and Restore

Step 1: Find a place to store your backups

This step is required. You must specify where backups will be stored.

Host: aimcp063.austin.ibm.com

Specify host for
your backups

Path: /drouter

Specify path to
store backup

User name: root

Password: [edit]

Specify
credentials

Test connection

When you click “Step 1: Find a place to store your backups”, the screen expands to allow you to specify the host system, directory path and host credentials where backups are stored.

Backup and restore – secure your backups

Backup and Restore

Step 1: Find a place to store your backups

Step 2: Secure your backups

This step is required. You must generate a keypair or provide your own certificate.

Generate your own keypair

Upload your own certificate

Generate your own keypair by providing a password...

...or upload your own certificate

When you click “Step 2: Secure your backups”, you must then generate your own keypair or upload your own certificate to secure the backup images.

Backup and restore - schedule a new backup

[-] Backup and Restore

Step 1: Find a place to store your backups

Step 2: Secure your backups

Step 3: Schedule a new backup

Select a date and time to create the backup (the default is right now).

Specify the date and
time to create your
backup

Once you click “Step 3: Schedule a new backup”, you can then specify the date and time when the backup is to occur. The default date and time is “right now”. You will review a message confirming that the backup is scheduled, with a link to the Tasks list so you can review the progress of the backup.

Backup and restore - restore from backup

Backup and Restore

Step 1: Find a place to store your backups

Step 2: Secure your backups

Step 3: Schedule a new backup

Step 4: Restore from a backup

Archive file date	Firmware version	Certificate issuer	Certificate subject	Serial Number	
00:27 Fri, May 7, 2010	2.0.0.0-22581	O=IBM WebSphere CloudBurst CN=Backup and Restore	O=IBM WebSphere CloudBurst CN=Backup and Restore	14117762760831341719	Restore

Private key...

Passphrase

1. Select the backup you want

2. Type backup private key and password

3. Upload the backup

4. When uploaded, start the restore

When you click “Step 4: Restore from a backup” you will see a list of backup images on the host server. Once you select the backup you want, you will see an input field for the backup private key and password. After providing that information, you click **Upload** to begin the upload of the image. Once you see a confirmation message that the image is uploaded, you can then click **Restore** to begin the restore of the image.

Firmware

+ Backup and Restore**- Firmware**

The current firmware version is WebSphere CloudBurst 1.1.0.0-17266

cloudburst.firmware.1100.172

Browse...

... 0 MB

Upgrade



1. Navigate to
new firmware
file

2. Click Upgrade and this
spinning icon is displayed

3. Upload progress
indicator is displayed
until installation begins

The firmware settings allow you to see the current firmware level that is installed on the appliance and to optionally upgrade the firmware. To upgrade the firmware level, click the **Browse** button to navigate to the firmware upgrade file on your client computer. Then click the **Upgrade** button to begin the upgrade. You will see a spinning activity icon to indicate that the upload of the upgrade image has begun, and you will see an upload progress indicator. Once the upload is completed, you will see a message indicating the upgrade of the appliance has begun.

Power administration

The screenshot shows the 'Power' section of the 'Appliance settings' interface. It contains two main options: 'Restart the appliance' and 'Shut down the appliance'. Below these are two dialog boxes. The first dialog, titled 'When do you want to restart?', has two radio button options: 'Wait until active tasks have completed' and 'Immediately'. The second dialog, titled 'When do you want to shut down?', also has two radio button options: 'Wait until active tasks have completed' and 'Immediately'. Both dialog boxes include 'OK' and 'Cancel' buttons. Yellow callout boxes point to each of these elements with the following text: 'Restart?', 'Shutdown?', 'Do it now!', 'Cancel my request', and 'Wait until active tasks complete?'.

18

Appliance settings

© 2010 IBM Corporation

The power portion of the settings allow you to restart or shutdown the appliance. For both options, you will see a popup that allows you to restart or shutdown only when all active tasks have completed or perform the function immediately, or you can cancel the function.

Create users

The screenshot shows the WebSphere CloudBurst administrator interface. The top navigation bar includes 'Welcome, Administrator', 'Help', and 'About'. Below the navigation bar, the 'Appliance' menu is highlighted with a red dashed box. A dropdown menu is open, showing options: 'Settings', 'Users', 'User Groups', 'Task Queue', and 'Troubleshooting'. The 'Users' option is highlighted with a red box and a mouse cursor. A yellow callout box points to the 'Users' option in the dropdown, stating 'Another way to user definition'. Another yellow callout box points to the 'Create users' link in the 'Step 1: Set up the appliance' section, stating 'One way to user definition'. The 'Create users' link is also highlighted with a red box. The page number '19' is visible in the bottom left corner, and the copyright notice '© 2010 IBM Corporation' is in the bottom right corner.

As an administrator, you can define the users that access the appliance. To access the user definition screen, click **Create users** under the topic “Step 1: Set up the appliance”. Alternatively you can click **Appliance** within the title bar, and within the pull-down that opens, click **Users**.

Create user detail

Users

Search...

Administrator

Click the "+" sign to create a new user



Provide the information for the new user

Password fields do not appear if you have LDAP security

Describe the user you want to add.

* User name: ✓

* Full name: ✓

Password: ✓

Verify password: ✓

* Email address: ✓

Once the **Users** list opens, click the plus sign to define a new user. Then in the right pane supply user name, full name, password, and password verification, and finally the email address for the new user. The **Password** and **Verify password** fields do not display if you are using LDAP security.

Create user detail

Users

Search...

- Administrator
- John Smith**
- user1
- user2

John Smith

User name: jsmith

Email address: jsmith@mycompany.com

Password: [edit]

Current status: User has not logged in yet

User groups: 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 catalog content
- Cloud administration
- Appliance administration
- License tracking

Callouts:

- What patterns and cloud groups has he created?
- What virtual systems has he deployed?
- What additional permissions should he have?
- Has new user logged in yet?
- What user groups is he in?

After the new user is initially defined, you can then set specific permissions for the new user, including create new patterns, create new catalog content, cloud administration, appliance administration, and license tracking. The user detail panel also displays the group membership for the user, and allows you to add the user to other groups. It shows you the patterns and cloud groups that the user has created, and the virtual systems that the user has deployed.

Section

Summary

This section will summarize the settings presentation.

Summary

- Customize settings
 - Application identification
 - Security
 - Ethernet interfaces
 - Domain name servers
 - Date and time
 - Mail delivery
 - Backup and restore
 - Firmware
 - Power
- Create users

This presentation discussed the WebSphere CloudBurst appliance settings and creating new users. In the security settings, you can allow or disallow new users to create their own accounts, and set up and test LDAP security. In Ethernet interfaces, you can review, add, change, or delete Ethernet connection definitions and review statistics, including error and drop counts, for the Ethernet connections you have defined. Within the domain name servers setting, you can review, add, or delete domain name servers, and test IP and host names. You use the date and time setting to specify the time zone and to review, add, or delete network time protocol servers. Under mail delivery, you can specify the SMTP server and reply-to address for the appliance to use when sending notification email to registered users. Within the backup and restore settings, you can provide the information needed for taking a backup image of your appliance and for restoring from a backup image. Under firmware settings, you can review the current firmware level settings and upgrade the firmware level. Finally, under power administration, you can restart or shutdown the appliance.

You saw how to create a new user account, how to review user information, and how to specify user permissions.



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 email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_CB20_ApplianceSettings.ppt

This module is also available in PDF format at: [../CB20_ApplianceSettings.pdf](..../CB20_ApplianceSettings.pdf)

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, CloudBurst, Current, 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>

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 2010. All rights reserved.