IBM WebSphere CloudBurst Appliance

Appliance settings

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

IBM

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

2　　　　Appliance settings　　　　　　　　　　　　　　　　© 2010 IBM Corporation

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.

Section

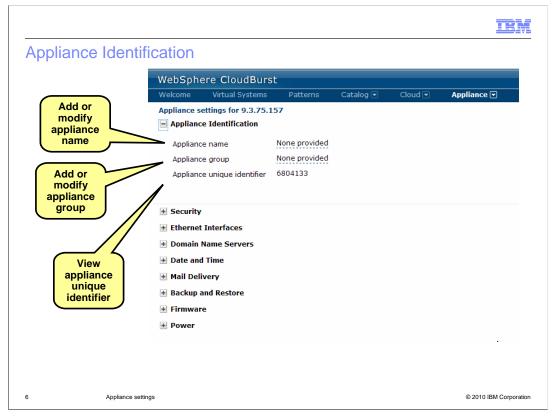# *WebSphere CloudBurst Appliance settings*

Appliance settings

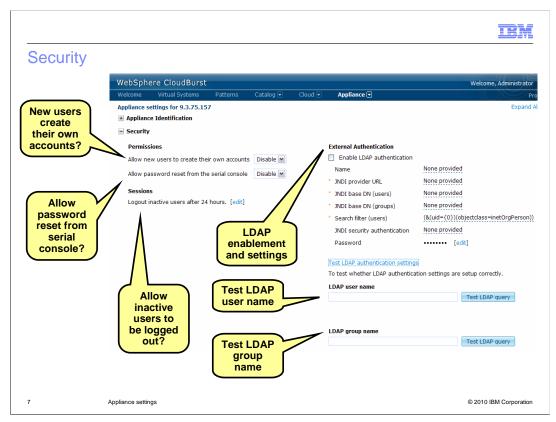This section will discuss a general overview of the WebSphere Cloudburst Appliance settings.

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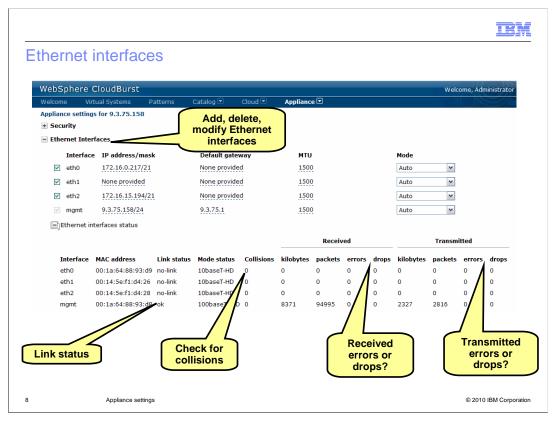
Appliance settings will allow you to customize appliance identification, security, Ethernet interfaces, domain name servers, date and time, mail delivery, backup and restore, review and update firmware, and administer power.

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

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
☑	eth0	172.16.0.217/21	None provided	1500	Auto
☑	eth1	None provided	None provided	1500	Auto
☑	eth2	172.16.15.194/21	None provided	1500	Auto
☑	mgmt	9.3.75.158/24	9.3.75.1	1500	Auto

➖ Ethernet interfaces status

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

Link status   *Check for collisions*   *Received errors or drops?*   *Transmitted errors or drops?*

8   Appliance settings   © 2010 IBM Corporation
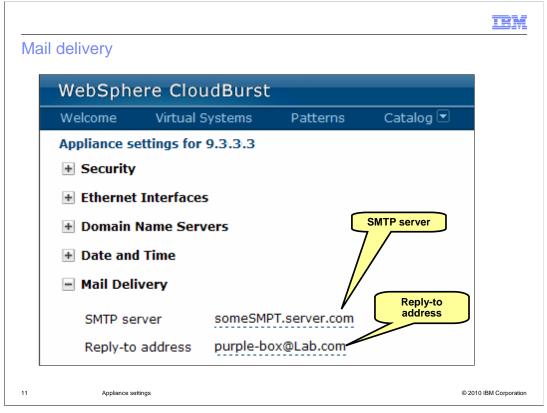
The Ethernet interfaces settings allow you to review Ethernet definitions and to add, change, or delete these definitions. The status portion of the screen allows you to review the individual Ethernet interfaces. This includes MAC address, link status, mode status, number of collisions, the number of kilobytes sent and received, the number of packets sent and received, and the number of errors and dropped packets.
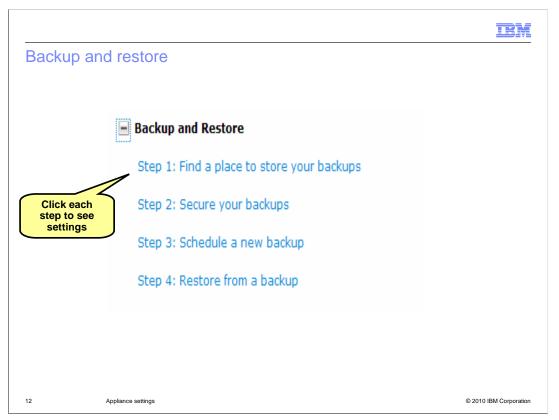
Domain name servers

WebSphere CloudBurst

Welcome   Virtual Systems   Patterns   Catalog ▾   Cloud ▾

Appliance settings for 9.3.3.3

⊞ Security
⊞ Ethernet Interfaces
⊟ Domain Name Servers

Add, delete or review DNS

9.3.3.11 ✖   9.3.3.3
9.3.3.1 ✖
Click to add

Validity check host names or IP addresses

Lookup host name or IP address

server3.mycompany.com   Lookup

Host name: server3.mycompany.com

IP address: 9.3.3.3

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

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.
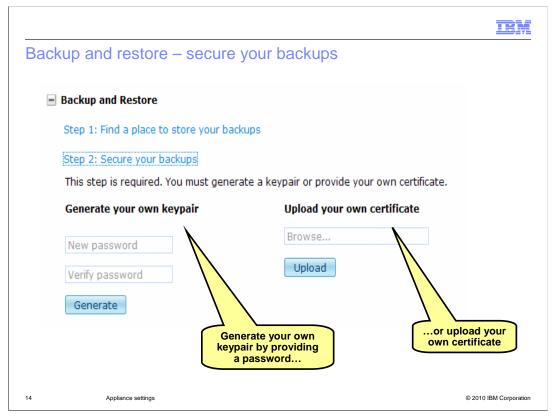
The mail delivery settings allow you to add, delete, or change the SMTP server setting and reply-to address for the appliance. These settings are used by the appliance when it delivers notification messages to users defined within the appliance.
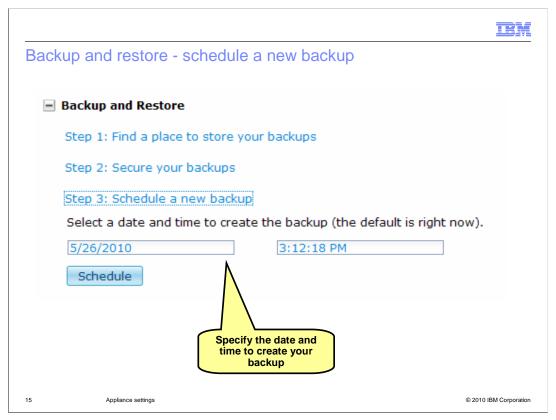
Using the backup and restore settings, you can ensure that the appliance can be restored when required. Click each step to see the settings. The four steps involved in setting up the backup and restore environment are: Step 1: Find a place to store your backups, Step 2: Secure your backups, Step 3: Schedule 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**
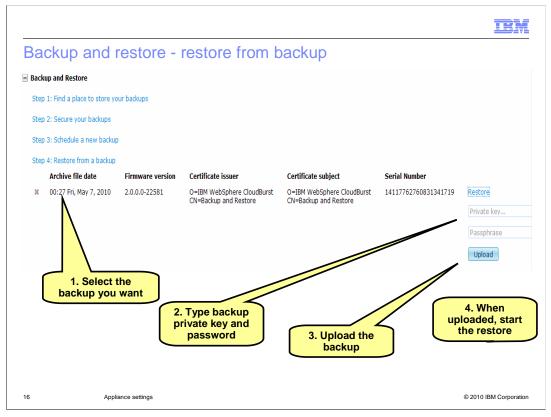
Test connection

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.
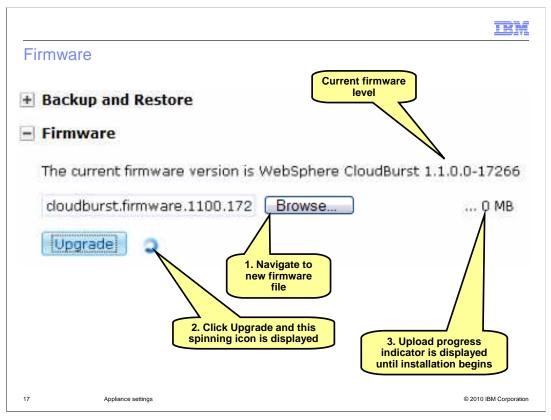
When you click "Step 2: Secure your backups", you must then generate your own keypair or upload your own certificate to secure the backup images.
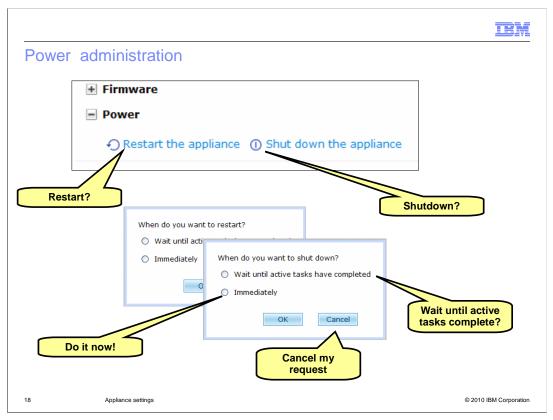
Once you click "Step 3: Schedule a new backup", you can then specify the date and time when the backup is to occur. The default date and time is "right now". You will review a message confirming that the backup is scheduled, with a link to the Tasks list so you can review the progress of the backup.

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

Upload

1. Select the backup you want

2. Type backup private key and password

3. Upload the backup

4. When uploaded, start the restore

16   Appliance settings   © 2010 IBM Corporation

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.

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.

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

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

Describe the user you want to add.

* User name: jsmith ✔

* Full name: John Smith ✔

Password: •••••••• ✔

Verify password: •••••••• ✔

* Email address: jsmith@mycompany.com ✔

✔

OK   Cancel

Provide the information for the new user

Password fields do not appear if you have LDAP security

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

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.
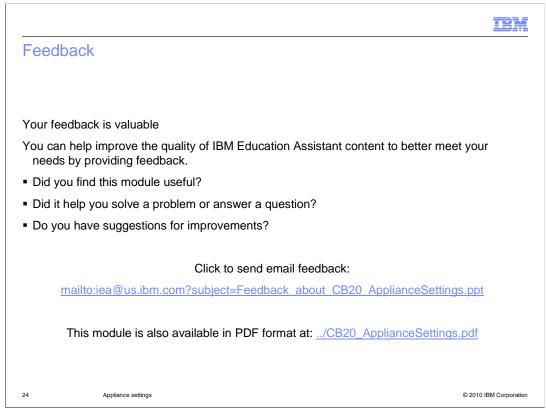
Summary

Appliance settings

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

　　　　Appliance settings　　　　

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

Trademarks, disclaimer, and copyright information

IBM