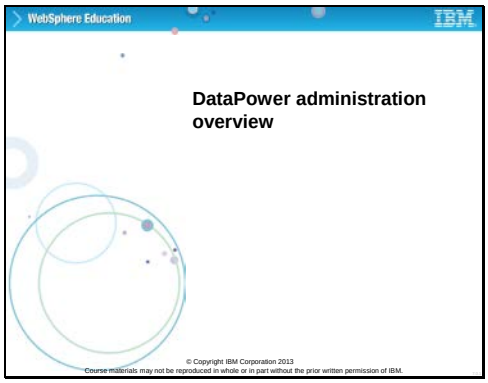
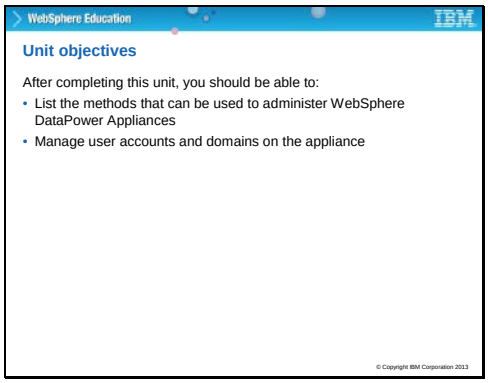
Slide 1



Unit 1

Unit 1, DataPower administration overview.

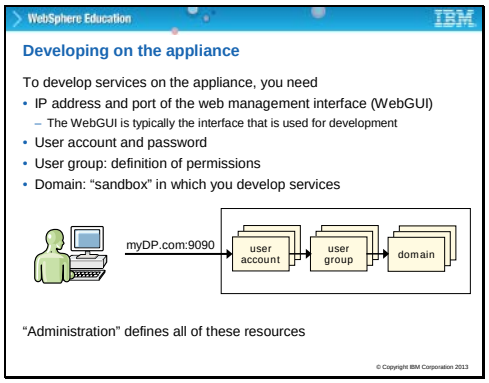
Slide 2



Unit overview

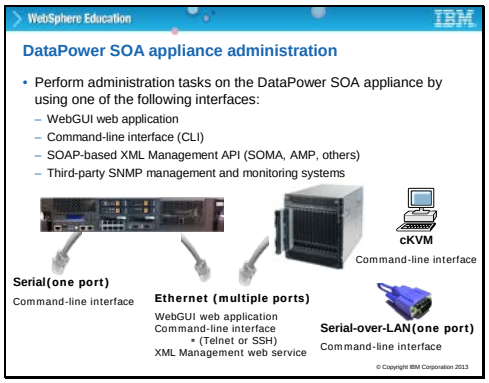
In this unit, you learn about the administration of the DataPower appliances.

Slide 3



This unit is a basic introduction to administration on the DataPower appliance. For a developer, it is helpful to know these basics, as they might request assistance from administrators. To begin working with the appliance, a developer accesses the WebGUI on an IP address and a port. Before they can do anything, they log in to a user account. Most user accounts are assigned to a user group. A particular user group defines a set of access permissions, to both functions and to resources. All work is done in a domain, which is usually one of the resources that are defined in the user group.

Slide 4

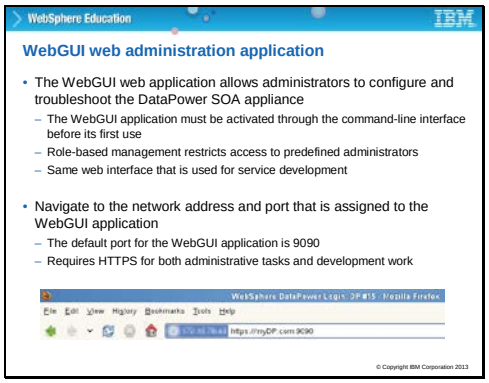


DataPower SOA appliance administration

Probably the simplest way to do development work on the appliance is through the web-based interface, or WebGUI. When you work in pre-production environments, or production environments, you are more likely use the command-line interface, and if you are working remotely you might use the XML management API, which is SOAP-based. Actually, the command-line interface is the only one available to you as delivered, through the serial port. You use the command-line interface to enable the four Ethernet ports. You can also work with the command-line interface through the Ethernet ports, but the ports that are listed give you the additional capabilities of working with the WebGUI and the XML management API.

The ports are all on the front of the appliance. On the back of the appliance is the on-off switch, the power supply, and two fan trays, so that if one fan dies the second keeps cooling the appliance while you replace the dead fan. The mentioned configuration is the limit of your options to mess around with the hardware of the appliance! As noted in the previous presentation, you cannot open the case and poke around inside. Remember also that there are no USB ports, no parallel ports, and no CD drive.

Slide 5

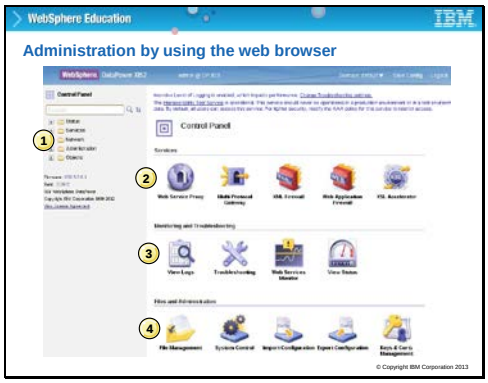


WebGUI web administration application

You access the WebGUI interface by opening a browser and going to the URL. The protocol is secure HTTP! One of the first mistakes you made is forgetting that the DataPower appliance is on a secure protocol. You give the URL of the appliance, and indicate the port as 9090 by default. Remember also that you are not able to access this WebGUI out of the Shipping box; it is locked down. You go in first through the serial port and activate the Ethernet ports.

As for browsers and browser levels, the WebGUI supports Internet Explorer 6 and 7 (but not Internet Explorer 8), Mozilla Firefox (officially at level 2, but many people use level 3 with no problem). Symptoms of browser level support problems are drop-down boxes that are not displayed, or items in a box not being displayed.

Slide 6



Administration by using the web browser

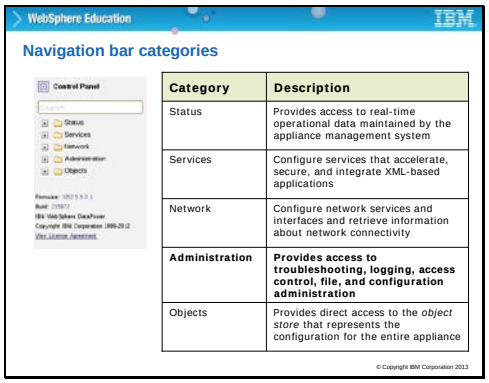
When the WebGUI opens, you first see the control panel. The WebGUI gives shortcuts to many of the things you are using: the services (indicated as number 2 on the slide), different monitoring options, file management, including importing and exporting configuration files, and management of keys and certificates. There is a link back to the control panel in the upper left corner (number 1 on the slide). If you are in another view and you get back to this display of shortcuts, you can click the link.

Just under the control panel link there are five categories in what is called the navigation bar. Clicking one of the links makes it open up and display many options for configuring DataPower or the services you create.

Underneath these categories, there is a little information about the firmware level the box is running at. On this slide, you can see that it is at level 3.8.0.0, and also that this control panel is being displayed for an XI50 appliance.

At the top of the GUI, in the blue bar, you can see the name of the person who logged in (here it says student01). Also displayed is an indication of which appliance is logged on to (in this case, an appliance that is identified as DP #10). On the right, you can see which domain the user is currently logged in to (a domain that is called ‘student01-domain’ in the present case). Domains are covered a little further on.

Slide 7



Navigation bar categories

Take a closer look at the categories on the navigation bar.

The first is Status. Status provides access to information about the different objects, such as services, that are held on the appliance.

The next category is Services. You can drop this category down and have access to all the different service options. The five principal ones also have icons on the control panel.

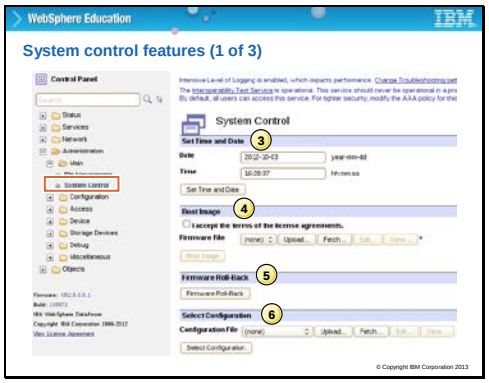
Network gives access to things such as user agent, load balancer group.

Administration is where you can get access to files, or system control (where you would go to change your password, for example). You have some of the same options in the ‘Files and Administration’ section of the control panel view.

And finally objects, where you have access to each object that is used to create services on the appliance. DataPower is based on the concept of objects. The objects are not objects in a programming sense. Think of them rather as containers of configuration information that can be assembled to configure services.

The next few slides examine the highlighted category, Administration.

Slide 8



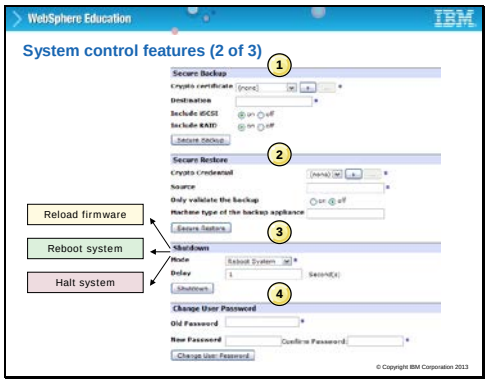
System control features (1 of 3)

Administration has five subcategories: main, configuration, device, debug, and miscellaneous. Here you can see the first of these subcategories, 'Main', which includes file management and system control. This slide looks at system control. You can get to the same point by clicking the icon on the control panel view.

Here then you can set the time and date for the appliance. The setting is important for things such as certificate validity. You can set the appliance to point to a Network Time Protocol server, or NTP server. Boot image allows you to upgrade to a new level of firmware. If the new level introduces problems in the configuration, you can roll it back (number 5 on the slide). You can roll back one level, to whatever was installed before the new firmware upload. Number 6, select configuration, allows you to select different configurations, and to upload a configuration to the appliance. By the way, to the left, in the navigation bar, under configuration, you see that you can import and export configurations. This topic is covered in more detail further on.

The options that you can see here are only available in the default domain. If you are logged in to a different domain, the only thing you are able to do is to change your password.

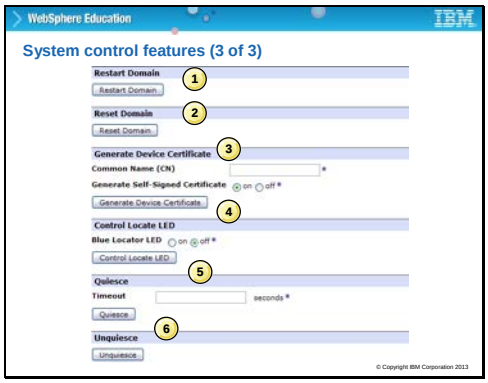
Slide 9



System control features (2 of 3)
You can use secure backup and restore to complete a full backup of a DataPower device configuration, and then restore the image to a compatible device. The benefits include disaster recovery, and also copying a configuration from one device to other devices in the same environment. For security, the backup files are encrypted.

There are three types of shutdown you can complete. Reload firmware keeps the appliance up and running but reloads the operating system. Reboot system switches off the system and then brings it back up again. Halt system switches it off. This action does not physically switch off the appliance; it is still powered on. It is the operating system that is off.
Changing the password can be done in any domain, not just the default.

Slide 10



System control features (3 of 3)

Restarting and resetting the domain is different from rebooting or halting the system. These two options (numbers 1 and 2 on the slide) react only on the domain into which you are logged. Other users are not affected. A domain is like a sandbox for the configuration for a particular user. It is an application domain where you configure your services. You can have as many domains as you need; it just depends on how you want to structure your services. Restart domain deletes any unsaved changes. Reset domain deletes any configured objects.

You can generate a self-signed certificate for this device by giving a name, or ‘common name’. There is a control for a blue LED that is on the front of the DataPower box. Imagine that you have a rack of a dozen DataPower boxes, and you recable Ethernet ports on a few of them. First, you would come to this system control and turn on the blue LED of the devices that require maintenance. Then, you can go to the rack of DataPower boxes and immediately locate the ones that you deal with.

Quiesce and unquiesce are complementary actions. Quiesce stops the appliance from accepting new requests by a service. It allows the service to complete processing on any request that is already accepted. It can be applied to a domain or to an appliance.

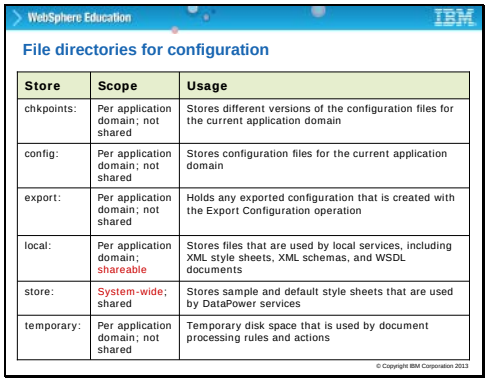
Slide 11

File management

You can access the file management area either from the navigation bar administration category, or from the icon on the control panel view. The top-level directories are pre-defined, but you can add subdirectories to some of them (the local directory, for example). The second column, ‘Actions’, is where you can create or delete directories, or upload files. The available actions depend on what object you chose. You can upload a file to the cert directory, or edit your configuration file. For the logs, you can view them (you click directly on the name of the log).

As you learned, there are several top level pre-defined directories. The directories fall into three categories: configuration object directories, security object directories, and logging directories. The next few slides examine them in more detail.

Slide 12



File directories for configuration

There are five configuration directories. Config: holds the domain configuration for the domain you are logged on to. There is one for each domain, and they cannot be shared between domains.

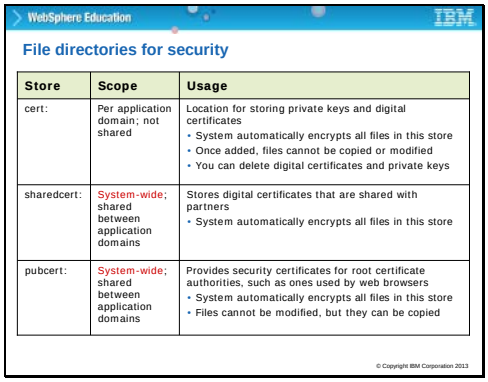
Export: holds the exported configuration that you created by using the export operation. You saw this briefly a few slides back. A closer look at this option is provided later in this presentation.

Local: holds any files that the current domain is using for services. Other domains can share these files (that is to say, copy them over into the other domain) by making this current domain visible. The setting for the configuration is called ‘Visible domains’, and can be found under Administration-configuration in the default domain. More information about visible domains is provided in a few more slides.

The store: directory holds template style sheets that are shared by all domains. You should therefore copy whatever you want to use into your own domain before editing.

Finally, there is the temporary: directory, which is (as the name implies) used for temporary storage. When the appliance is shut down, everything in this directory is automatically deleted.

Slide 13

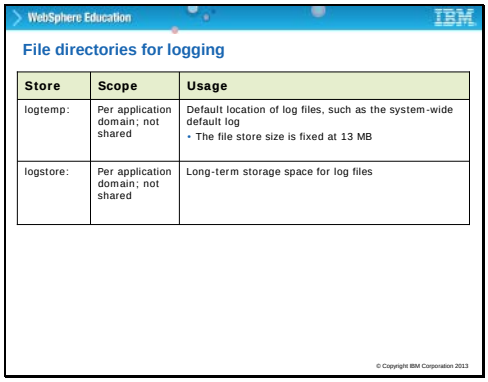


File directories for security

Security has three directories. The first on this slide is the `cert:` directory. Each domain has its own directory of certificates and keys and all are encrypted. Notice that you cannot copy or modify a file that is added to this directory. The only modification that you can do is to delete it!

The `sharedcert:` directory is visible to all domains. The directory is where there are intermediary CA certificates, or certificates of partners you work with all the time. Likewise, all domains share `pubcert`. The `pubcert` is where the root certificate authority certificates are stored.

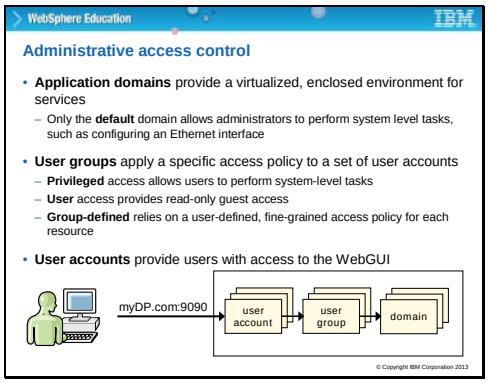
Slide 14



File directories for logging

Logging has two directories. The difference is one of durability. The one has temporary life; the other is long term. Logs are created for each domain and are not shared.

Slide 15



Administrative access control

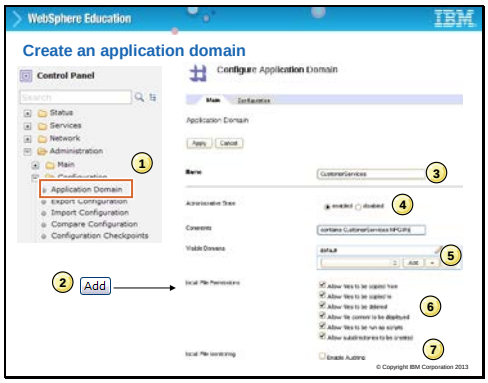
A domain is a separate environment for a service or services. It encapsulates these services and the objects that the services require, and are defined by a configuration file. By default there is a domain that is called ‘Default’, and you can create as many other domains as necessary.

As you see in the slides that discuss directories, some objects might be shared between domains, but the services themselves are only visible and usable in the domain where they where created.

Domains are accessed by users who have a user account. Users can be grouped to apply a policy that limits the authority of those users. The ‘privileged’ group is restricted to administrators. The group that is simply called ‘User’ has read-only access. The third type, “group-defined’, allows for a more fine-grained definition of access policies. There can be any number of group-defined user groups.

An appliance might have several domains. A domain might have several user groups that are defined, and the user groups might have several accounts that are associated.

Slide 16



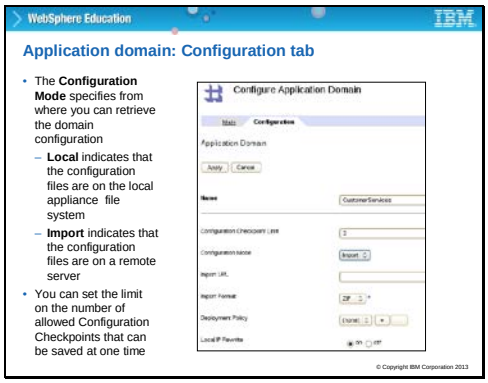
Create an application domain

To create an application domain, you are in the default domain. Clicking 'Application Domain' brings up a list of all existing domains (domains are covered on the next three slides) and an 'Add' button to create a domain. The slide shows the main tab of the configure application domain dialog. Here you can see something that were briefly mentioned a few slides back – domain visibility. The default domain is automatically visible to this new domain. You drop down the list of existing domains, select one; then click the 'Add' button to add it to the list of visible domains.

You can also choose the file permissions that you want. For example, do you want to allow other domains to copy files from this domain?

In summary, if you want to be able to see the files on another domain you add them as visible domains, and those domains allow files to be copied from them.

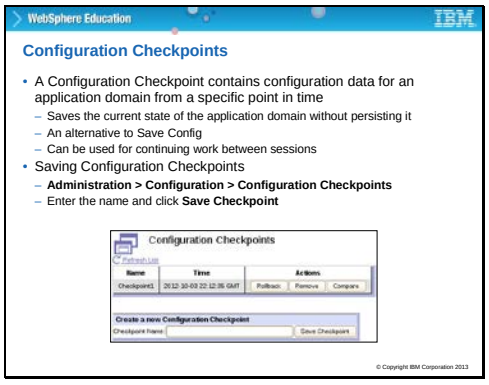
Slide 17



Application domain: Configuration tab

You are still in the dialog for configuring an application domain, but now you can see the configuration tab. You can see that the maximum number of configuration checkpoints is set to 3 (more on checkpoints on the next slide) and the configuration mode is set to local, which is the default. Local says that the configuration file is on the appliance. The second option is remote, when the file is not on the appliance.

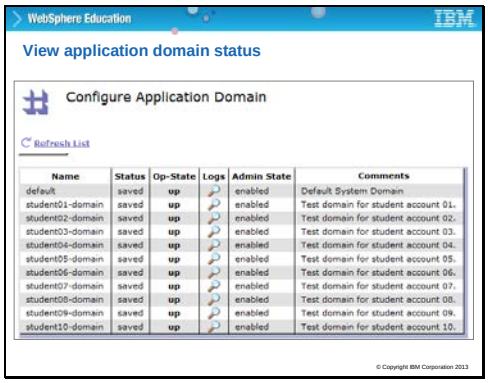
Slide 18



Configuration Checkpoints

A configuration checkpoint is like an undo capability. You saw on the previous slide that is set to 3. The setting means that as you reconfigure your domain, instead of persisting the changes that you can apply a checkpoint, and you can store three such checkpoint markers. Now, if you decide that your latest configuration is not what you want. You can easily revert to a previous state without having to remember all the changes you made and then undo them one by one.

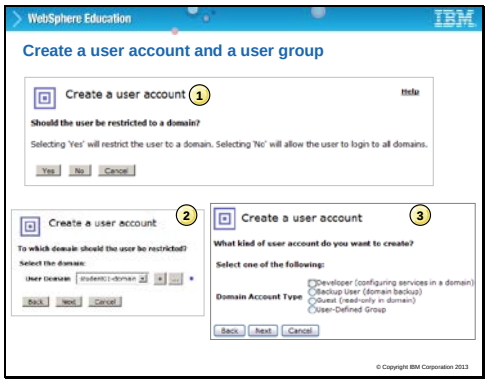
Slide 19



View application domain status

When you first click the Application Domain link in the configuration subcategory of the navigation bar, you get a list of all domains. The list of domains is together with their status and their operational state (which will by up or down). You can read the system log for a domain, and check the admin state. For example, if you click a domain name and change its admin state to disabled. When you return to this page you see the domain status as ‘modified’, the op-state as ‘down’, and the admin state as ‘disabled'. Looking at the log, you see that the operational state is logged as down.

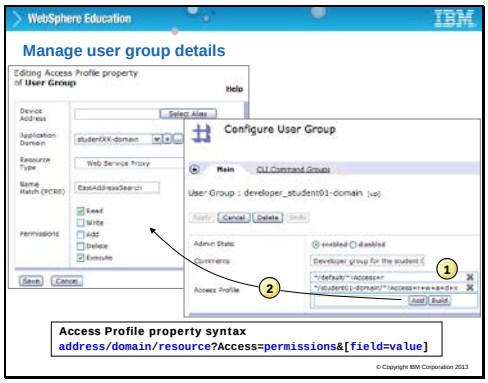
Slide 20



Create a user account and a user group

Creating a user account can be done from the navigation bar. The first decision is whether to restrict the user to a specific domain or whether to give them access to all domains. Typically you might want to restrict the user. For example, a developer needs access, so you provide a restricted access to a developer domain. In the example, number 2 shows that the user is restricted to ‘student01-domain’. Finally, you specify what type of developer they are. Is read-only access ok? Does this developer be able to configure services?

Slide 21

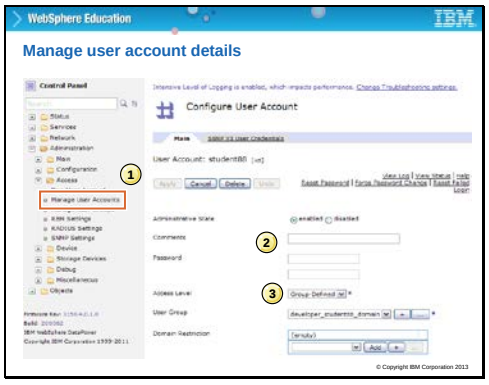


Manage user group details

Here is the configuration of a user group. Look at the right side of the diagram first (number 1). You can see that there is a user group called developer_student01-domain. You build access profiles: one or more. Here there are two defined. If you are unsure how to implement, you can click Build and use the wizard. The Build opens up the dialog you can see to the left of the slide. You can restrict access to a specific device, or a particular domain, or more fine-grained, a resource type or a name match. You then check off the permissions that should be granted to this profile: read, write, add, delete, or execute.

When you click Save, the definition shows up in the field next to Add, which you can see to the right. If you now click Add, this access profile is added to the list for this group. How should you interpret the access profiles that are listed there? The first says that, for the default domain, for all objects (the character is the asterisk), access is restricted to read. The second says that for student01-domain, for all objects, access permissions are r, w, a, d, and x, or read, write, add, delete, and execute.

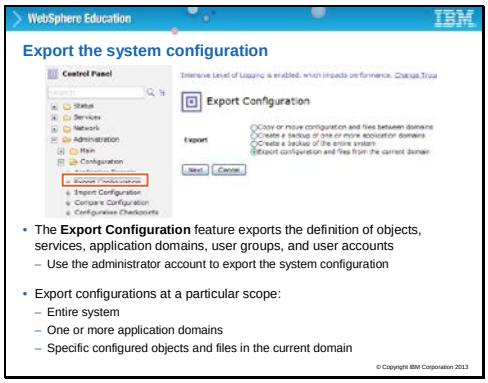
Slide 22



Manage user account details

Now you can associate a user account with a user group through the Configure User Account dialog.

Slide 23

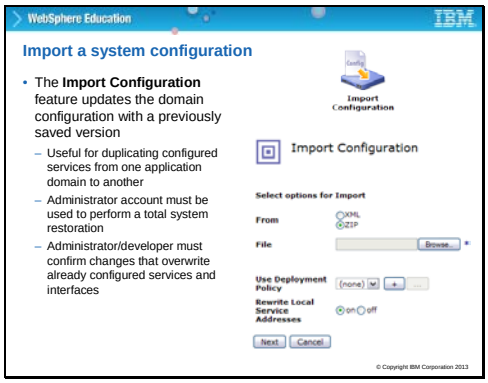


Export the system configuration

You can export a configuration by choosing the navigation tab subcategory and clicking the radio button according to what scope you want to export. The configuration can be restricted to the configuration and files of the domain you are currently logged in to, or it might be an export of the whole system. 'Export' does not include everything in the domain. For example, certificates and keys are not exported.

When you click **Next** (the button you can see in the screen capture to the right), you get to a dialog where you can define what export you want (XML or `.zip` are the options). Select the objects to include in the export.

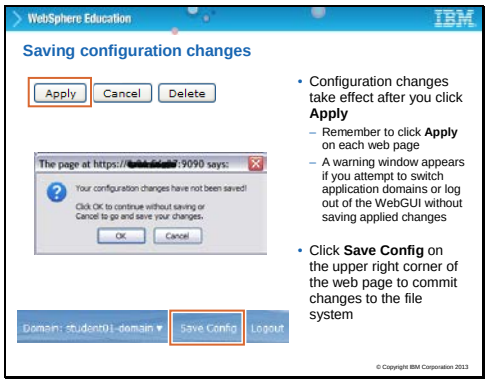
Slide 24



Import a system configuration

Since export is possible, it follows the import is possible! Remember from the previous slide that the file type options for the export were XML and `.zip`. Therefore, the file types for the import are also XML and `.zip`. When you click **Next**, you can select which files you want to import, and as a convenience you are given a list of files that are identical to existing files.

Slide 25



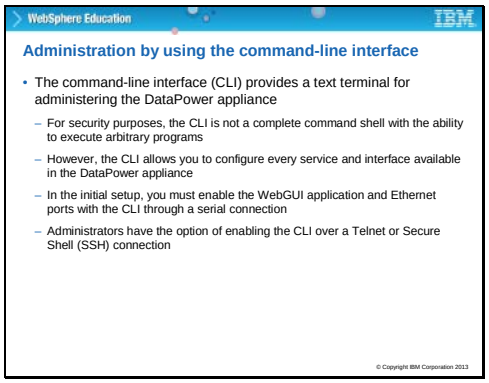
Saving configuration changes

Saving configuration changes is a two-step process. The immediate and essential thing is to click **Apply**. Clicking apply temporarily adds any changes that you made to the configuration. If you try to leave a page without applying, a warning dialog pops up.

To add your changes to the configuration, you must click **Save Config**. You can test your changes without doing the process (the running configuration includes any changes that you made). However, if you switch domains or log out while there are unsaved changes, you might lose them.

If you try to switch domains while there are unsaved changes, you get a warning dialog.

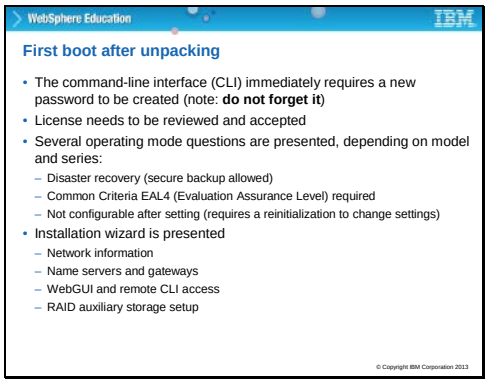
Slide 26



Administration by using the command-line interface

When you first get the appliance, everything is dead except for the serial port. Initially, you connect the serial port to your computer (probably through a USB-to-serial connector). After that, you might still want or use the serial connection to do administration through the command-line interface. You can enable the CLI over Telnet or over SSH, but here is a word of advice: enable it over SSH, not Telnet!

Slide 27

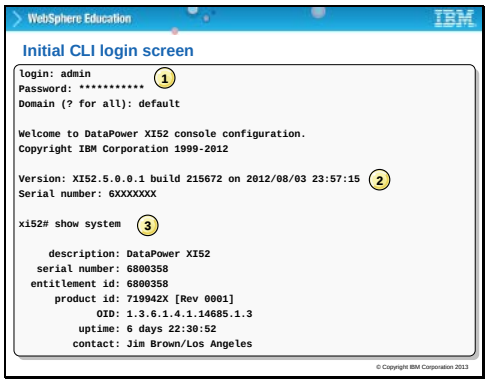


First boot after unpacking

The first to do with your new DataPower appliance is to create a password. Note it carefully somewhere! If you forget it, you must return the appliance to IBM to be reset.

There is an installation wizard to help you with the initial configuration of the appliance, but you can also set up this initial configuration through a command-line interface.

Slide 28

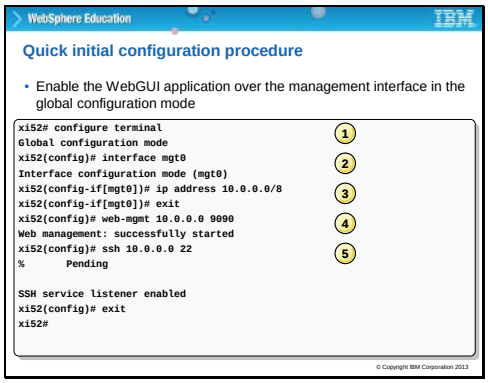


Initial CLI login screen

The first screen gives you some basic information about what you are connecting to. In this screen capture, you can see that it is an XI50, with a certain version and build level, and with a specific serial number.

The prompt is now XI50 with a hash sign. The first thing that you might want to do is get a little more information about the system. To obtain more information, you type the command ‘show system’. The content shows you how long since the appliance started running, what its name is, where it is, how many services it has, and so on.

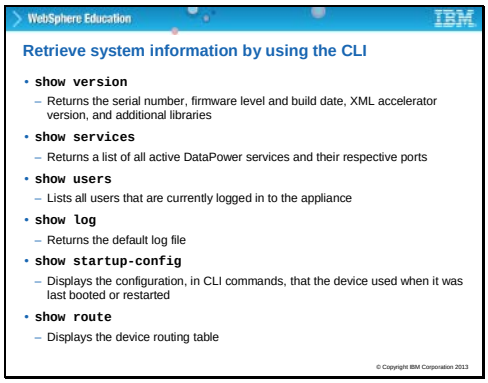
Slide 29



Quick initial configuration procedure

The first necessity is going to be to enable the Ethernet interfaces. At the command prompt you type ‘configure terminal’, which puts you into the configuration mode. Now you want to work on the interface ‘mgt 0’, which is the Ethernet terminal 4. The appliance responds by telling you that you are in interface configuration mode for ‘mgt 0’, and the prompt changes to reflect such. It actually says ‘xi52(config-if[eth4])’, indicating that indeed you are connected to the Ethernet terminal 4. You define an IP address for the port (this action is one that you see often through the next presentations). Typing `exit` does a save. Next, you configure the web management interface. The port is 9090. You want to open a CLI session over SSH, so you enable the session by defining the port on a specific interface. After a moment, the response tells you that the SSH service listener is enabled. Again, by typing ‘exit’ you save the changes.

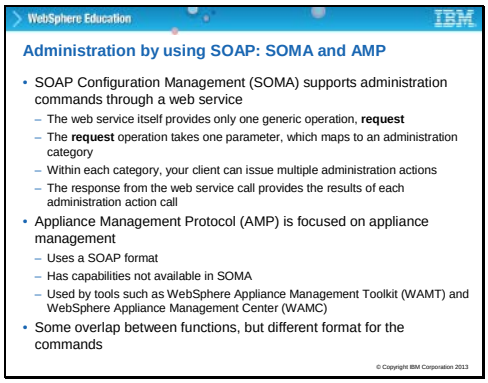
Slide 30



Retrieve system information by using the CLI

Here are some of the more common commands that are used over CLI. You can get some general information about the appliance, or a list of active services together with the port numbers on which they are defined. You can see who is logged in, and read the default log file. You can call up a display of the configuration that was used at start, or see the routing table of the appliance.

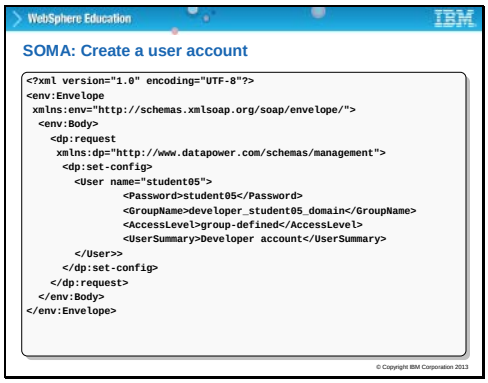
Slide 31



Administration by using web service

Here is another way to interact with the appliance: through a web service. The DataPower web service interface has one operation, request, with a single parameter that defines what action to take.

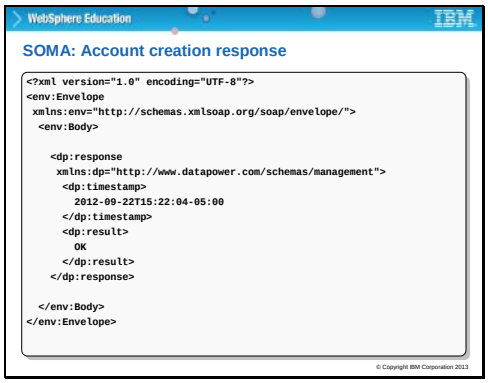
Slide 32



XML Management: Create an application domain

Here is an example of what you might do. This SOAP message includes the request ccommand that you saw in the previous slide. The parameter ‘set-config’ indicates that the request is to modify the configuration. The details within the set-config tag indicate that the request is to create a domain. Domain visibility is set to default; in other words, only the default domain is visible to this new domain.

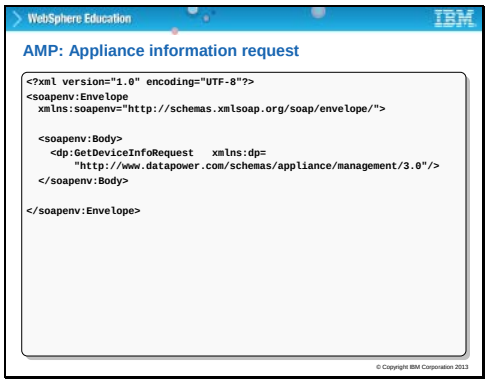
Slide 33



XML Management: Domain creation response

The response is the response to the request sent on the previous slide. There is always a timestamp, and if everything goes well, the single result message is ‘ok’.

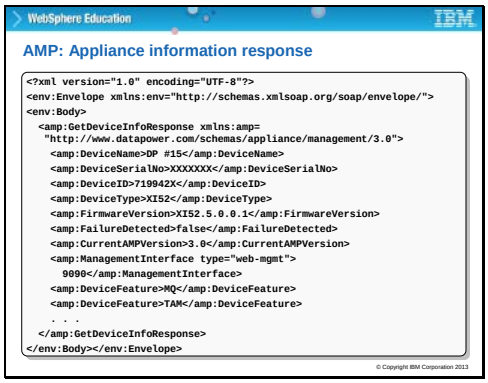
Slide 34



Notes:

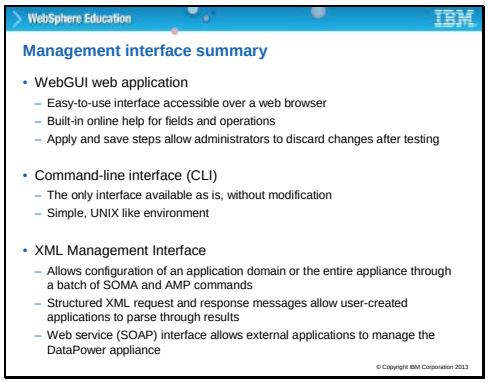
Administration by using the Appliance Management Protocol (AMP).
Here is another way to interact with the appliance – using AMP. The DataPower AMP interface has one operation, request, with a single parameter that defines what action to take. However, The AMP WSDL defines multiple operations, unlike the Web Service

Slide 35



The complete list of device features is returned by the command but is not listed because of space restrictions.

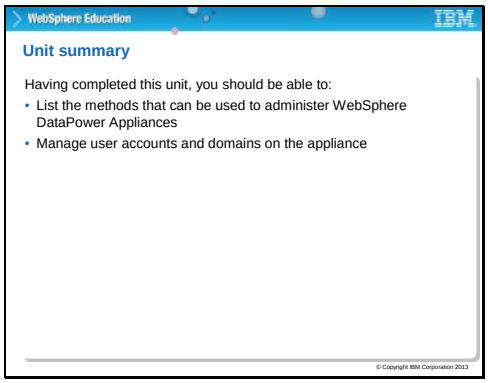
Slide 36



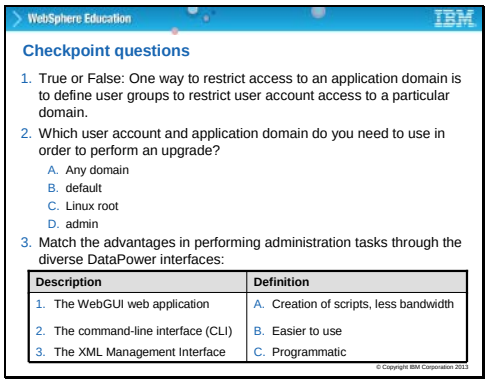
Management interface summary

To sum up, there are three primary ways to manage the appliance. There is the WebGUI, which gives easy visual access over a web browser. The WebGUI is the one you use in the exercises that are associated with this course. There is the command-line interface, which is the only one available upon initial appliance configuration, and is the preferred interface for general management of the appliance. And finally there is the web service interface, which allows XML management through SOAP messages.

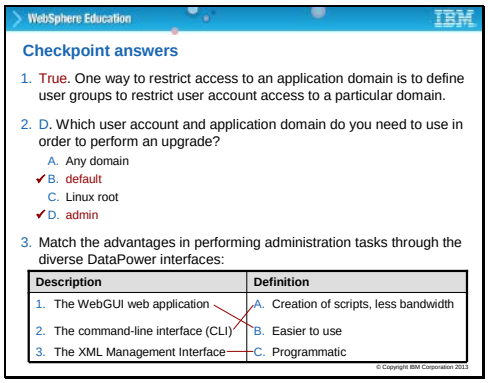
Slide 37


WebSphere Education
IBM
Unit summary
Having completed this unit, you should be able to:
• List the methods that can be used to administer WebSphere DataPower Appliances
• Manage user accounts and domains on the appliance
© Copyright IBM Corporation 2013

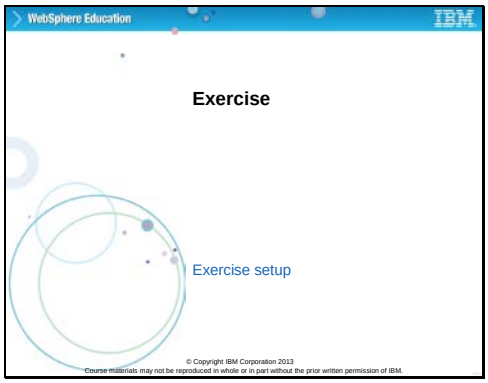
Slide 38


WebSphere Education
IBM
Checkpoint questions
1. True or False: One way to restrict access to an application domain is to define user groups to restrict user account access to a particular domain.
2. Which user account and application domain do you need to use in order to perform an upgrade?
A. Any domain
B. default
C. Linux root
D. admin
3. Match the advantages in performing administration tasks through the diverse DataPower interfaces:
Description
Definition
1. The WebGUI web application
A. Creation of scripts, less bandwidth
2. The command-line interface (CLI)
B. Easier to use
3. The XML Management Interface
C. Programmatic
© Copyright IBM Corporation 2013

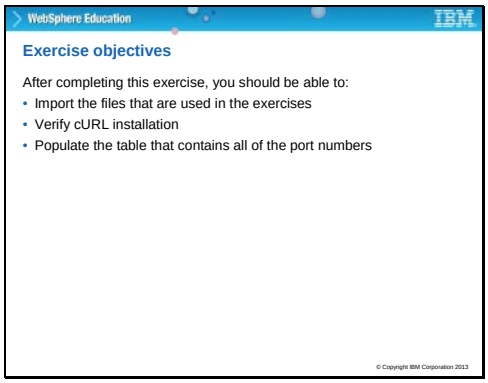
Slide 39


WebSphere Education
IBM
Checkpoint answers
1. True. One way to restrict access to an application domain is to define user groups to restrict user account access to a particular domain.
2. D. Which user account and application domain do you need to use in order to perform an upgrade?
A. Any domain
✓B. default
C. Linux root
✓D. admin
3. Match the advantages in performing administration tasks through the diverse DataPower interfaces:
Description
Definition
1. The WebGUI web application
2. The command-line interface (CLI)
3. The XML Management Interface
A. Creation of scripts, less bandwidth
B. Easier to use
C. Programmatic
© Copyright IBM Corporation 2013

Slide 40


WebSphere Education
IBM
Exercise
Exercise setup
© Copyright IBM Corporation 2013
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Slide 41


WebSphere Education
IBM
Exercise objectives
After completing this exercise, you should be able to:
• Import the files that are used in the exercises
• Verify cURL installation
• Populate the table that contains all of the port numbers
© Copyright IBM Corporation 2013