LAB: System i Access for Web Configuration

Linda Hirsch (LLHIRSCH@us.ibm.com), IBM Rochester

http://www.ibm.com/systems/i/software/access/web

Table of Contents

Preface

Lab Objective

The first objective of this lab is to familiarize the student with the process of setting up the ASF Tomcat and WebSphere Application Server V6.1 for i5/OS web serving environments on i5/OS and configure System i Access for Web.

The second objective of this lab is to provide enough detailed information and generic examples so that the student can perform this lab at home.

The steps necessary to configure the web serving environment for System i Access for Web include:

- Verify hardware requirements
- Verify software requirements
- Install System i Access for Web
- Verify PTFs are loaded and applied
- Setup an HTTP server
- Setup the web application server (i.e. ASF Tomcat, WebSphere Application Server)
- Configure System i Access for Web

Because this is a shared lab environment, only a portion of the steps listed above will be performed by the student. For the purpose of the lab, some assumptions have to be made (listed in the Assumptions section below) in order for the lab to work for all students.

This lab does not have the objective of addressing topics such as:

- Advanced networking issues in the web environment.
- Advanced TCP/IP communications configuration.
- Tuning of HTTP or WebSphere Application servers.
- The usage of the servlets provided within the System i Access for Web product.

Assumptions

In this lab, there are many students that will be connecting to and using only a few i5/OS systems. Because there are only a few systems, we are going to assume the following setup steps have been performed by the lab setup team:

- Verify hardware requirements
- Verify software requirements
- Install System i Access for Web
- Verify PTFs are loaded and applied

For your reference, detail for each of these steps has been included below so that you can perform these steps at home.

Verify hardware requirements

Refer to the web application server documentation to determine what System i5 models, processor features, server disk space, and the memory requirements are for the web application server that is to be used:

- WebSphere http://www.ibm.com/servers/eserver/iseries/software/websphere/wsappserver/
- ASF Tomcat http://www.ibm.com/servers/eserver/iseries/software/http/

In general, your i5/OS system should have the following minimums

- 1000 CPW (when using WebSphere)
- 1GB memory
- 470MB available server disk space for System i Access for Web

When referencing the web server documentation it should be noted that System i Access for Web consists of servlets. This makes a difference how much resource the web application server requires from the server.

The System i Access for Web product also has a solution for the WebSphere Portal environment on the i5/OS system. This lab does not cover any WebSphere Portal related setup information. If you are interested in the WebSphere Portal environment, additional information is available in the IBM InfoCenter documentation and from the System i Access for Web website: http://www.ibm.com/servers/eserver/iseries/access/web. You should refer to the WebSphere Portal documentation for specific hardware requirements.

Verify software requirements

Run the i5/OS command **`GO LICPGM`** to display the list of currently installed software, compare that displayed list to the table below. You should also refer to the web application server documentation to determine if there are additional software requirements not listed in the table below.

Product Number	Product Name	Option
5722-SS1	V5R3 System i Access for Web supports OS/400 V5R2 or i5/OS V5R3 V5R4 System i Access for Web support i5/OS V5R3 and V5R4	Base
5722-SS1	i5/OS - Extended Base Directory Support	3
5722-SS1	I5/OS - AFP Compatibility Fonts	8
5722-SS1	I5/OS - Host Servers	12
5722-SS1	i5/OS QShell Interpreter	30
5722-SS1 5722-AC3	If you plan to use Secure Sockets Layer (SSL): i5/OS Digital Certificate Manager Cryptographic Access Provider (128-bit)	34

5722-IP1	IBM Info Print Server (**optional**) (provides best PDF documents)	Base
5722-DG1	IBM HTTP Server for System i	Base
5722-JV1	Developer Kit for Java Developer Kit for Java Version 1.3 Developer Kit for Java Version 1.4	Base 5 6
5722-JC1	Toolbox for Java	Base
5722-TC1	TCP/IP Connectivity Utilities for System i	Base
5722-XW1 5722-XH2	System i Access Family System i Access for Web	Base, 1 Base
  5733-W61 5733-W60 5722-E51 5733-W51 5722-IWE 5733-WS5 5722-DG1	One, or more, of the following web servers WebSphere Application Server v6.1 for i5/OS WebSphere Application Server - Express v6.1 for i5/OS WebSphere Application Server Network Deployment v6.1 for i5/OS WebSphere Application Server v6.0 for OS/400 WebSphere Application Server - Express v6.0 for OS/400 WebSphere Application Server Network Deployment v6.0 for OS/400 WebSphere Application Server v5.1 - Express for iSeries WebSphere Application Server v5.1 (Base and Network Deployment editions) WebSphere Application Server v5.0 - Express for iSeries WebSphere Application Server v5.0 (Base and Network Deployment editions) Apache Software Foundation Tomcat (part of 5722-DG1 product)	See documentation

Install System i Access for Web

System i Access for Web is a licensed program product (LPP). Like other LPPs, System i Access for Web is installed to i5/OS using the server command: **`RSTLICPGM`**

The product ID for System i Access for Web is 5722-XH2 in V5R4 and earlier, and 5761-XH2 in V6R1. Below is an example of running the server command:

RSTLICPGM LICPGM(5722XH2) DEV(OPT01) OPTION(*BASE)

Restoring System i Access for Web to i5/OS will:
- Create library QIWA2 and objects in QIWA2
- Create IFS directories
  - /QIBM/ProdData/Access/Web2/...
  - /QIBM/UserData/Access/Web2/...
- Set basic authorities to IFS objects.

The restore process will not...
- Make any changes to HTTP server configurations.
- Make any changes to web application server configurations.
- Make System i Access for Web ready for use, it still has to be configured.

Verify PTFs are loaded and applied

After all the i5/OS software has been installed, program temporary fixes (PTFs) need to be loaded and applied if they are not already on i5/OS.

The information below tells you how to determine what level of fixes are on your i5/OS.

Latest server Cumulative PTF package
The WebSphere group PTFs identify what level of OS/400 cumulative PTF package is required. Refer to the WebSphere group PTF information to determine what level was used to test the group PTFs.

WebSphere Application Server
Each WebSphere group PTF has a level. You can use the commands listed below to display the current level of the group PTF and compare that to what the WebSphere web site says is the latest available group PTF.

To determine the current available group PTF level:
- Open a browser to http://www.ibm.com/servers/eserver/iseries/software/websphere/wsappserver/
- Click the PTFs link
- Click the link for your release/WAS version
- The displayed information should state the currently available group PTF level.

Use these server commands to determine what level is installed on your server:

V5R3 i5/OS

WRKPTFGRP SF99322	v6.1 for i5/OS (Base, Express, ND)
WRKPTFGRP SF99301	v6.0 for OS/400 (Base, Express, ND)
WRKPTFGRP SF99275	v5.1 Express for iSeries
WRKPTFGRP SF99285	v5.1 Base Edition
WRKPTFGRP SF99286	v5.1 Network Deployment Edition
WRKPTFGRP SF99272	v5.0 Express for iSeries
WRKPTFGRP SF99287	v5.0 Base Edition
WRKPTFGRP SF99288	v5.0 Network Deployment Edition

V5R4 i5/OS

WRKPTFGRP SF99323	v6.1 for i5/OS (Base, Express, ND)
WRKPTFGRP SF99312	v6.0 for OS/400 (Base, Express, ND)
WRKPTFGRP SF99311	v5.1 Express for iSeries
WRKPTFGRP SF99308	v5.1 Base Edition
WRKPTFGRP SF99309	v5.1 Network Deployment Edition

HTTP Server/ASF Tomcat server
The HTTP server and the ASF Tomcat web application server are both delivered in the software product 5722-DG1 (or 5761-DG1 for V6R1), “IBM HTTP Server”. PTFs for each server are delivered as 57xx-DG1 PTFs.

Each HTTP/Tomcat server group PTF has a level. You can use the commands listed below to display the current level of the group PTF and compare that to what the HTTP/Tomcat web site says is the latest available group PTF.

To determine the current available group PTF level:

- Open a browser to
  http://www.ibm.com/servers/eserver/iseries/software/http
- Click the PTFs link
- Click the link for your release of operating system.
- The displayed information should state the currently available group PTF level

Use these server commands to determine what level is installed on your server:

V5R3 i5/OS
WRKPTFGRP SF99099

V5R4 i5/OS
WRKPTFGRP SF99114

System i Access for Web

The web site http://www.ibm.com/systems/i/software/access/web contains information on the latest available PTF/Service Pack.

TCP/IP Ports

Port usage within this lab

Port usage is always a concern of system administrators.

Within this lab, port usage will start in the range of 2xx00 where xx is the team number of each workstation within the lab environment. Below is more detail on port usage for each lab exercise

ASF Tomcat exercise

For this exercise a single port will be used for the HTTP server, and a single port will be used between the HTTP server and the Tomcat server.

The HTTP server port will be of the form 2xx16, where xx is the team number of each workstation. Teams 1-9 should prepend their number with a 0 so that two digits are used.

The port used between the HTTP and Tomcat servers will be of the form 2xx17, where xx is the team number of each workstation. Teams 1-9 should prepend their number with a 0 so that two digits are used.

WebSphere Application Server exercise

For this exercise a single port will be used for the HTTP server, and a range of ports will be used by the WebSphere Application Server.

The HTTP server port will be of the form 2xx30, where xx is the team number of each workstation. Teams 1-9 should prepend their number with a 0 so that two digits are used.

The WebSphere Application Server will use a range of ports (approximately 10 ports) starting at 2xx31, where xx is the team number of each workstation. Teams 1-9 should prepend their number with a 0 so that two digits are used.

Items to note:

- The ports listed above have to be unique, meaning they are not already in use or are going to be used by another application.
- Use the i5/OS command NETSTAT *CNN to display ports that are already in use on the server.
- Use the i5/OS command CFGTCP --> option 21 to Configure related tables --> option 1 to Work with Service Table Entries. This will display a list of configured services/applications and what ports they will use.

Lab Exercises

Note to Students

The lab exercises below include examples for both the ASF Tomcat and WebSphere Application Server environments.

This lab will be using V5R4 System i Access for Web.

If your interest is only in ASF Tomcat, you can just run the ASF Tomat exercises.

If your interest is only in WebSphere Application Server, you can just run the WebSphere Application Server exercises.

Regardless of whether you run the exercises for both environments, we do ask that you please run the cleanup exercises at the end. These cleanup exercises will show you how to cleanup the web environment and also prepare the environment for the next student that uses your lab workstation.

If you have any question or problems, please raise your hand or grab one of the lab team members.

Thank You, enjoy the lab.
System i Access for Web development team

ASF Tomcat exercise

This exercise is designed to show the student how to setup an ASF Tomcat web serving environment for System i Access for Web to be deployed into. The student will perform the tasks listed below and verify System i Access for Web can be accessed using a web browser.

Introduction

This exercise will walk the student through the following tasks:

1. Starting and using the IBM Web Administration for i5/OS interface to setup the web environment.
2. Creating and configuring an HTTP web server.
3. Creating and configuring an ASF Tomcat server.
4. Configuring System i Access for Web.
5. Starting the environment.
6. Using a browser to access System i Access for Web.

Tasks

1. The student will use the IBM Web Administration for i5/OS interface to create the HTTP and ASF Tomcat server. To start this web interface:
   i. The screen at the front of the room should be displaying server name information. Ask the lab instructor for assistance if needed.

   ii. Start a 5250 session to the server.

   iii. Signon as user: WAxxADM password: WAxxPWD
   Note:
   - This WAxxADM user profile has, at a minimum, the following special authorities: *ALLOBJ, *IOSYSCFG, *JOBCTL, *SECADM.
   - xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

   iii Run i5/OS command to start the web administration interface job:
   `STRTCPSVR *HTTP HTTPSVR(*ADMIN)`

   iv Minimize the 5250 session.

2. The student will use the web administration interface to create the HTTP web server:
   i. Open a browser to:
   `http://<system_name>:2001`

   ii. Login as user: WAxxADM password: WAxxPWD
   Note: xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

   iii. Click the link:
   IBM Web Administration for i5/OS

iv. At the top of the web page, click the tab:
Setup

v. On the left side of the web page, under Common Tasks and Wizards, click the link:
Create HTTP Server

vi. The "Create HTTP Server" page is displayed.

In the Server name field, type **HTTPIWAxx**, where xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

vii. Click Next.

viii. Click Next on the page where the Server root field is displayed.

ix. Click Next on the page where the Document root field is displayed.

x. Type **2xx16** in the Port field, where xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

This is the port that users will specify in the URL of their web browser when accessing System i Access for Web servlets.

xi. Click Next.

xii. Click Next on the page asking about the access log.

xiii. Click Next on the page where you specify the time to keep the log files.

xiv. Click Finish.

xv. The web page is refreshed to have the Manage/HTTP Servers tab active for the HTTPIWAxx - Apache web server. On the left side, under Server Properties, click the link:
ASF Tomcat Settings

xvi. The ASF Tomcat Settings page is displayed.

xvii. Click the checkbox:
Enable servlets for this HTTP server.

xviii. The page is refreshed with additional configuration options.

xix. Uncheck the checkbox:
Enable an "in-process" servlet engine

xx. The page is refreshed again.

xxi. Click the checkbox:
Enable "out-of-process" servlet engine connections

xxii. The page is refreshed with additional configuration options.

Click the Add button for the Out-of-process workers box.

xxiii. In the Hostname:Port column/field, edit the 8009 number and change it to **2xx17** where xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

When done editing, the value in the column should be similar to:
localhost:2xx17

This port will be used for communication between the HTTP server and the ASF Tomcat server that will be created in later steps.

xxiv. In the URLs (Mount points) column/field, type:
/webaccess/*

xxv. Click the Continue button.

xxvi. The worker is added to the table of Out-of-process workers. Ignore any error that may be displayed in the table in red text. The displayed error will be resolved as the rest of the configuration is performed in the steps below.

xxvii. Click the OK button.

xxviii. The steps above created the HTTPIWAxx web server and set it's configuration values for connecting with an ASF Tomcat server. The ASF Tomcat server will be created in the following steps.

3. <u>The student will use the web administration interface to create the ASF Tomcat server.</u>
   i. The previous step left the browser open to the Manage/HTTP Servers tab of the HTTP server. Return to that browser session.

   ii. At the top, click the ASF Tomcat Servers tab.

   iii. On the left side of the page, under Tomcat Tasks and Wizards, click:
   Create ASF Tomcat Server

   iv. The Out-of-Process Engine Creation page is displayed. In the ASF Tomcat server name field type (exactly as shown below):

tciwaxx

where xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

v. Click Next.

vi. The Out-of-Process Engine Configuration page is displayed. From the displayed information, write down the values for the following fields here exactly as they appear (i.e. case sensitivity):
Server userid: _____
ASF Tomcat home: _____

vii. Click Next.

viii. The Out-of-Process Communication Settings page is displayed. In the Port field, change the 8009 number to:
2xx17

where xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

This is the same port number that was specified in the ASF Tomcat settings of the HTTPIWAxx server created earlier.

This port will be used for communication between the HTTP server and the ASF Tomcat server.

ix. Click Next.

x. The Out-of-Process Application Context Definition page is displayed. Click the Add button for the Application contexts table.

xi. In the URL path column/field, type:
/webaccess

xii. In the Application base directory column/field, type:
webapps/webaccess

xiii. Click the Continue button. Ignore any error that may be displayed in the table in red text. The displayed error will be resolved as the rest of the configuration is performed in the steps below.

xiv. Click Next.

xv. Click Finish. The page will be refreshed.

xvi. In the upper left of the page, click the All servers tab.

xvii. The displayed page contains tabs which you can select to view the various configured servers.

xviii. Minimize the browser.

4. The student will now configure System i Access for Web.
   i. Restore the 5250 session window.

   ii. To configure System i Access for Web, type the following server command and press **F4** to prompt for the parameters:
   QIWA2/CFGACCWEB2

   iii. The cursor should be positioned in the "Web application server type" field, press **F4** to display allowed values.

   iv. The options available are:
      a. *WAS50 WebSphere V5.0 base edition
      b. *WAS50EXP WebSphere V5.0 - Express for iSeries
      c. *WAS51 WebSphere V5.1 base edition
      d. *WAS51EXP WebSphere V5.1 - Express for iSeries
      e. *WAS60 WebSphere V6.0 for OS/400
      f. *WAS60ND WebSphere Network Deployment V6.0 for OS/400
      g. *WP50 WebSphere Portal V5.0.2
      h. *WP51 WebSphere Portal for Multiplatforms V5.1.0.1
      i. *WSE Workplace Services Express V2.5
      j. *ASFTOMCAT Apache Software Foundation Tomcat

   v. In the Web application server type field, type:
   ***ASFTOMCAT**

   vi. Press the Enter key to display the conditional parameters.

   vii. In the Tomcat server name field, type (exactly as shown):
   tciwaxx

   where xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

   viii. In the Tomcat home directory field, type the value that you recorded while creating the ASF Tomcat server. It is probably something similar to:
   /ASFTomcat/tciwaxx

where xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

You recorded this value in an earlier step.

ix. In the Tomcat user profile field, type the value that you recorded while creating the ASF Tomcat server. It is probably something similar to:
QTMHHTTP

You recorded this value in an earlier step.

x. Press Enter to run the command.

xi. Several messages similar to the following will be displayed:
Configuring System i Access for Web

Preparing to perform the configuration changes.

Configuring System i Access for Web for the ASF Tomcat server.

System i Access for Web command has completed.

The ASF Tomcat server must be stopped and then started to enable the configuration changes.

The command has completed, press Enter to exit the Java Shell Display session.

xii. Press **Enter** when the command completes to exit the Java Shell Display session.

If the command were to fail, or indicate an error, you could refer to the log files:

/QIBM/UserData/Access/Web2/logs/cmds.log	High level, Cause/Recovery information, translated
/QIBM/UserData/Access/Web2/logs/cmdstrace.log	Detailed command flow, For Service and development, English only

xiii. After successfully configuring System i Access for Web, the ASF Tomcat server must be started. This will be done in later steps.

xiv. Signoff the 5250 session window.

xv. Close the 5250 session window.

5. Start the web environment.

i. Return to the browser window that is open to the IBM Web Administration for i5/OS interface. The Manage/All Servers tab should be the active page.

ii. Click the All HTTP Servers tab.

iii. Click the radio button for the HTTPIWAxx server and click the Start button, where xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

iv. Click the All ASF Tomcat Servers tab.

v. Click the radio button for the TCIWAxx server and click the Start button, where xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

System i Access for Web will load and start as the Tomcat server starts.

vi. Wait a minute or two to allow the Tomcat server to start and load the java classes.

vii. Close the browser window.

6. Use a browser to verify and access System i Access for Web.
   i. Open a browser to:
   `http://<system_name>:2xx16/webaccess/iWAHome`
   `http://<system_name>:2xx16/webaccess/iWAMain`

   ii. Login as user: WAxxADM password: WAxxPWD
   Note: xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

   iii. The initial load of System i Access for Web can take a few seconds. Tomcat is loading java classes, etc. Subsequent loads of System i Access for Web will be quicker.

   iv. The System i Access for Web Home Page and Main Page should be displayed.

   v. Please be sure to run the cleanup exercise at the end of this lab so you can see how System i Access for Web can be removed from the web application server, and allow the next student in the lab to use this workstation to perform the exercise you just completed.

   vi. Close the browser session.

Summary of tasks completed

- An HTTP server named HTTPIWAxx was created.
- A Tomcat application server named tciwaxx was created.

- System i Access for Web was configured for the Tomcat application server.

- The HTTP server and Tomcat application server were started.
  - System i Access for Web started when the Tomcat server started.

- Verification that System i Access for Web can be accessed from a browser.

End of ASF Tomcat exercise

WebSphere Application Server V6.1 for i5/OS exercise

This exercise is designed to show the student how to setup a WebSphere Application Server web serving environment for System i Access for Web to be deployed into. The student will perform the tasks listed below and verify System i Access for Web can be accessed using a web browser.

Introduction

This exercise will walk the student through the following tasks:

1. Starting and using the IBM Web Administration for i5/OS interface to setup the web environment.
2. Creating an HTTP web server and a WebSphere Application Server V6.1 for i5/OS web application server.
3. Configuring System i Access for Web.
4. Starting the environment.
5. Using a browser to access System i Access for Web.

Tasks

1. The student will use the IBM Web Administration for i5/OS interface to create the HTTP and WebSphere servers. To start this web interface:
   i. The screen at the front of the room should be displaying server name information. Ask the lab instructor for assistance if needed.

   ii. Start a 5250 session to the server.

   iii. Signon as user: WAxxADM password: WAxxPWD
   Note:
   - This WAxxADM user profile has, at a minimum, the following special authorities: *ALLOBJ, *IOSYSCFG, *JOBCTL, *SECADM.
   - xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used..

   iii Run server command to start the web administration interface job (only one student needs to run this on each server being used):
   `STRTCPSVR *HTTP HTTPSVR(*ADMIN)`

   iv Minimize the 5250 session.

2. The student will use the web administration interface to create the HTTP/WebSphere servers:
   i. Open a browser to:
   `http://<system_name>:2001`

   ii. Login as user: WAxxADM password: WAxxPWD

Note: xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

iii. Click the link:
IBM Web Administration for i5/OS

iv. At the top of the web page, click the tab:
Setup

v. On the left side of the page, under Common Tasks and Wizards, click the link:
Create Application Server

vi. The web page is refreshed displaying some text welcoming you to the Create Application Sever wizard.

vii. Click Next.

viii. You may be prompted to select the WebSphere version that you want to configure. This wizard web page is conditionally displayed if more than one version of WebSphere is installed on your i5/OS system.

If only one version of WebSphere is installed on your i5/OS system, this wizard web page is not displayed. Skip to the next step in this exercise.

If the wizard web page is displayed, click the radio button for:
V6.1 Express

Click Next.

ix. The "Specify Application Server Name" page is displayed.

Type **`iwawasxx`** in the "Application server name" field, where xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

This will be the name of the WebSphere web application server.

x. Click Next.

xi. The "Select HTTP Server Type" page is displayed.

Click the radio button for the "Create a new HTTP server (powered by Apache)" option.

xii. Click Next.

xiii. The "Create a new HTTP server (powered by Apache)" page is displayed.

Type **IWAHTTPxx** in the "HTTP server name" field.

Type **2xx30** in the "Port" field where xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

xiv. Click Next.

xv. The "Specify Internal Ports Used by the Server" page is displayed.

Change the default value to **2xx31** in the "First port in range" field, teams 1-9 prepend the number with 0 so that two digits are used.

xvi. Click Next.

xvii. Click Next until the "Summary" page is displayed..

xviii. Click Finish.

xix. The web page is redisplayed. The Manage/Application Servers tab is now the active page.

The Server pulldown field in the upper left lists "iwawasxx/iwawasxx - V6.1 Express" with a status of "Creating". From this web page, you can manage the WebSphere application server.

Use the refresh icon next to the "Creating" status to refresh the page (if the page does not periodically refresh).

xx. When the status is updated to "Stopped", click the green icon next to "Stopped" to start the WebSphere application server.

The status will be updated to "Starting", use the refresh icon next to the "Starting" status to refresh the page if the page does not periodically refresh.

System i Access for Web requires the WebSphere application server is running before it can be configured.

Wait for the status to be updated to "Running" before moving to the next step.

xxi. The steps above created the HTTP server IWAHTTPxx, and created and started the WebSphere application server iwawasxx.

Minimize the browser window.

3. <u>The student will now configure System i Access for Web.</u>

i. Restore the 5250 session window.

ii. To see the WebSphere application server running, run server command:
WRKACTJOB SBS(QWAS61)

iii. Verify IWAWASxx is listed as a job under the QWAS61 subsystem. System i Access for Web requires the WebSphere application server is running before it can be configured.

iv. To verify the application server is really ready
   a. Enter option #**5** on your IWAWASxx job.
   b. Enter option #**10** to display the job log.
   c. Press **F10** to display detailed messages.
   d. Verify the message "Websphere application server iwawasxx ready" is listed. This message indicates the application server as fully started and is ready for web serving.
   e. Press **F3** until you return to a command line.

v. System i Access for Web can be configured using either CL commands provided in the QIWA2 library or QShell script commands provided in directory /QIBM/ProdData/Access/Web2/install.

   The Tomcat configuration exercise found earlier in this lab used a CL command to configure System i Access for Web. For this exercise, the QShell script command will be used to configure System i Access for Web.

   The script commands run within the QShell environment. Run server command:
   QSH

vi. Change the current directory to where the commands reside. Run server command:
   cd /QIBM/ProdData/Access/Web2/install

vii. Display the contents of the directory. Run server command:
   ls

viii. One of the listed files should be cfgaccweb2.

ix. To configure System i Access for Web for the iwawasxx WebSphere application server created/started above, run server script command:
   cfgaccweb2 -appsvrtype *WAS61EXP -wasprf iwawasxx

   where xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

   The *WAS61EXP must be typed exactly as shown.

x. Several messages similar to the following will be displayed:
Configuring System i Access for Web

Preparing to perform the configuration changes.

Calling WebSphere to perform the configuration changes.

System i Access for Web command has completed.

The WebSphere application server must be stopped and then started to enable the configuration changes.

xi. Press F3 when the command completes to exit the Java Shell Display session.

If the command were to fail, or indicate an error, you could refer to the log files:

/QIBM/UserData/Access/Web2/logs/cmds.log	High level, Cause/Recovery information, translated
/QIBM/UserData/Access/Web2/logs/cmdstrace.log	Detailed command flow, For Service and development, English only

xii. After successfully configuring System i Access for Web, the WebSphere application server must be restarted to load the changes to it's configuration. This will be done in later steps.

xiii. Signoff the 5250 session window.

xiv. Close the 5250 session window.

4. Start (Restart) the web environment.
   i. Return to the browser window that is open to the Web Administration for i5/OS server management page.

   The Manage/Application Servers tab should be the active page, the Server pulldown field in the upper left lists "iwawasxx/iwawasxx - V6.1 Express" with a status of "Running".

   Click the red icon to stop the WebSphere application server.

   Use the refresh icon next to the "Stopping" status to refresh the page if the page does not periodically refresh.

   ii. When the status is updated to "Stopped", click the green icon next to "Stopped" to start the WebSphere application server.

The status will be updated to "Starting", use the refresh icon next to the "Starting" status to refresh the page if the page does not periodically refresh.

Wait for the status to be updated to "Running" before moving to the next step.

System i Access for Web will load and start as the WebSphere application server starts.

iii. Click the tab labeled HTTP Servers.

iv. In the Server pulldown field in the upper left, select "IWAHTTPxx - Apache".

v. The current status of this Apache HTTP server should be stopped. Click the green icon next to the status to start the HTTP server. The status should be updated to Running.

vi. Close the browser window.

5. Use a browser to verify and access System i Access for Web.
   i. Open a browser to:
   http://<system_name>:2xx30/webaccess/iWAHome
   http://<system_name>:2xx30/webaccess/iWAMain

   ii. Login as user: WAxxADM password: WAxxPWD
   Note: xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

   iii. The initial load of System i Access for Web can take a few seconds. WebSphere is loading java classes. Subsequent loads of System i Access for Web will be quicker.

   iv. The System i Access for Web Home Page and Main page should be displayed.

   v. Please be sure to run the cleanup exercise at the end of this lab so you can see how System i Access for Web can be removed from the web application server, and allow the next student in the lab to use this workstation to perform the exercise you just completed.

   vi. Close the browser window.

Summary of tasks completed

- A WebSphere application server named iwawasxx was created.
- An HTTP server named IWAHTTPxx was created.
- System i Access for Web was configured for the WebSphere application server.

- The HTTP server and WebSphere application server were started/restarted.
  - System i Access for Web started when the WebSphere application server started.

- Verification that System i Access for Web can be accessed from a browser.

End of WebSphere Application Server exercise

Setting up access to multiple servers exercise

Note: This exercise is optional

Introduction
Many administrators would like to contain their web serving environment to a i5/OS system. This is defined to mean keeping the HTTP server and WebSphere/Tomcat on a single i5/OS system.

Containing the web serving environment can really help with the administration and licensing requirements that can be necessary when web serving is propagated to many servers.

System i Access for Web has the ability to be installed and configured on a single i5/OS system, and then configured to connect to other i5/OS systems in the network.

The tasks below walk the student through the updates necessary to have System i Access for Web connect to other servers in the network.

Configuring System i Access for Web to connect to other servers
The System i Access for Web CFGACCWEB2/cfgaccweb2 commands support a parameter called "Target server" (TGTSVR).

When a fully qualified i5/OS system name is specified for this TGTSVR parameter this instance of System i Access for Web will be set to connect to the i5/OS name specified.

1. Perform at least one of the tasks earlier in this document that configures System i Access for Web and starts the environment.

2. Invoke the configuration command specifying the "Target server" parameter. To run the command for one of the environments configured earlier in this document:

   For ASF Tomcat
   QIWA2/CFGACCWEB2 APPSVRTYPE(*ASFTOMCAT)
   TCSVRNAME(tciwaxx)
   TCHOMEDIR('/ASFTomcat/tciwaxx')
   TCUSRPRF(QTMHHTTP)
   TGTSVR(<ask lab instructor>)

   For WebSphere Application Server V6.0 for OS/400
   QSH
   cd /QIBM/ProdData/Access/Web2/install

cfgaccweb2 -appsvrtype *WAS61EXP
-wasprf iwawasxx
-tgtsvr <ask lab instructor>

3 The Websphere application server and/or ASF Tomcat server must be stopped and restarted to load this configuration change. The HTTP server does not have to be restarted.

Open your browser to the following address to stop/restart WebSphere/ASF Tomcat:
`http://<system_name>:2001`

4 After restarting the web application server, open a browser to one of the following URLs which is based on the tasks earlier in this document that had the student setup System i Access for Web:

For ASF Tomcat
`http://<system_name>:2xx16/webaccess/iWAHome`

For WebSphere Application Server
`http://<system_name>:2xx30/webaccess/iWAHome`

where xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

Note that the same HTTP port is still used.

5 The user ID/password prompt should indicate you are connecting to the server specified in the CFGACCWEB2/cfgaccweb2 command's TGTSVR/tgtsvr parameter in the previous step.

6 Login using a valid user ID/password for the server that is being connected.

7 The webpage should connect to the server specified in the CFGACCWEB2/cfgaccweb2 command's TGTSVR/tgtsvr parameter in the previous step.

8 If there are additional backend i5/OS systems in your environment, you can:
i. Repeat the setup steps and create additional instances of WebSphere/ASF Tomcat, one for each additional server you wish to have System i Access for Web connect to.
ii. Configure System i Access for Web to those instances.

This will give your users access to multiple i5/OS systems but you only need to manage the web environment on a single i5/OS system.

Note: If additional setups are performed, the ports called for in the exercise instructions must be different from those already specified or already in use.

End of Setting up access to multiple servers

Cleanup Exercise

This exercise will cleanup the configurations that were created in the previous exercises. These steps are designed to teach the student how to cleanup the web environment, and also prepare this workstation for the next student to run this lab.

This exercise will walk the student through the following tasks.

1. Start a 5250 session and the web administration interface.
2. Remove the System i Access for Web configuration from the web application server.
3. Stop and delete the HTTP server and ASF Tomcat/WebSphere web application servers.

ASF Tomcat environment cleanup

1. The student will use a 5250 session and the web administration interface to perform cleanup:
   i. Start a 5250 session to the server.

   ii. Signon as user: WAxxADM password: WAxxPWD
   Note:
   - This WAxxADM user profile has, at a minimum, the following special authorities: *ALLOBJ, *IOSYSCFG, *JOBCTL, *SECADM.
   - xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used..

   iii Run server command to start the web administration interface job (only one student needs to run this on each server being used):
   `STRTCPSVR *HTTP HTTPSVR(*ADMIN)`

2. The student will remove the System i Access for Web configuration:
   i. To remove the System i Access for Web configuration, type the following server command in the 5250 session and press **F4** to prompt the fields:
   `QIWA2/RMVACCWEB2`

   ii. The cursor should be positioned in the "Web application server type" field, press **F4** to display allowed values.

   iii. The only options available are:
   a. *WAS50 WebSphere V5.0 base edition
   b. *WAS50EXP WebSphere V5.0 - Express for iSeries
   c. *WAS51 WebSphere V5.1 base edition
   d. *WAS51EXP WebSphere V5.1 - Express for iSeries
   e. *WAS60 WebSphere V6.0 for OS/400
   f. *WAS60ND WebSphere Network Deployment V6.0 for OS/400
   g. *WP50 WebSphere Portal V5.0.2
   h. *WP51 WebSphere Portal for Multiplatforms V5.1.0.1
   i. *WSE Workplace Services Express V2.5
   j. *ASFTOMCAT Apache Software Foundation Tomcat

k. *WAS40ADV WebSphere Advanced Edition 4.0
l. *WAS40SNG WebSphere Single Server Edition 4.0

iv. In the Web application server type field, type:
`*ASFTOMCAT`

v. Press the Enter key to display the parameters.

vi. In the Tomcat server name field, type:
`tciwaxx`

where xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

vii. Press Enter to run the command.

viii. Several messages similar to the following will be displayed:
Removing System i Access for Web

Preparing to perform the configuration changes.

Removing System i Access for Web from the ASF Tomcat server.

System i Access for Web command has completed.

The ASF Tomcat server must be stopped and then started to enable the configuration changes.

The command has completed, press Enter to exit the Java Shell Display session.

ix. Press **`Enter`** when the command completes to exit the Java Shell Display session.

If the command were to fail, or indicate an error, you could refer to the log files:

/QIBM/UserData/Access/Web2/logs/cmds.log	High level, Cause/Recovery information, translated
/QIBM/UserData/Access/Web2/logs/cmdstrace.log	Detailed command flow, For Service and development, English only

x. Minimize the 5250 session window.

3. The student will use the web administration interface to stop and delete the HTTP server and ASF Tomcat server:
i. Open a browser to:

http://<system_name>:2001

ii. Login as user: WAxxADM password: WAxxPWD
Note: xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

iii. Click the link named below on the i5/OS Tasks web page:
IBM Web Administration for i5/OS

iv. At the top of the web page, click the tab:
Manage

v. Click the tab labeled HTTP Servers.

vi. Click the tab labeled All HTTP Servers.

vii. Locate the HTTP server named HTTPIWAxx. Select the radio button for it and click the Stop button if the HTTPIWAxx server is not already in a Stopped status.

viii. Select the Delete button at the bottom of the page to delete your HTTPIWAxx server.

ix. Click the tab labeled All ASF Tomcat Servers.

x. Locate the Tomcat server named TCIWAxx. Select the radio button for it and click the Stop button if the TCIWAxx server is not already in a Stopped status.

xi. Select the Delete button at the bottom of the page to delete your TCIWAxx server.

xii. Close your browser window.

xiii. Restore your 5250 window.

xiv. The IFS directory structure set up to contain the HTTPIWAxx server's files needs to be deleted. Run the server command:
wrklnk '/www'

xv. An object link named "www" of type "DIR" should be displayed. Enter option **2** to Edit the "www"object. Press the Enter key.

xvi. A list of objects will be displayed. These objects are the directories that were created when HTTP servers were created on this server.

Page through the list and locate the "httpiwaxx" directory for the team you are signed on (where xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used)

xvii. Enter option **9** for your "httpiwaxx" directory to perform a recursive delete of the directory and all its contents. Press the Enter key twice to delete the directory.

xviii. Press F3 to return to a command entry line.

xix. The IFS directory structure set up to contain the tciwaxx Tomcat server's files needs to be deleted. Run the server command:
wrklnk '/ASFTomcat'

xx. An object link named "ASFTomcat" of type "DIR" should be displayed. Enter option **2** to Edit the "ASFTomcat"object. Press the Enter key.

xxi. Page through the list and locate the "tciwaxx" directory for the team you are signed on (where xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used)

xxii. Enter option **9** for your "tciwaxx" directory to perform a recursive delete of the directory and all its contents. Press the Enter key twice to delete the directory.

xxiii. Press F3 to return to a command entry line.

xxiv. Signoff the 5250 session window.

xxv. Close the 5250 session window.

Summary of tasks completed

- The System i Access for Web configuration was removed from the ASF Tomcat server using the RMVACCWEB2 CL command.
- The HTTP server named HTTPIWAxx was stopped and deleted.
- The ASF Tomcat server named tciwaxx was stopped and deleted.

WebSphere Application Server environment cleanup

1. The student will use a 5250 session and the web administration interface to perform cleanup:
   i. Start a 5250 session to the server.

   ii. Signon as user: WAxxADM password: WAxxPWD
   Note:
   - This WAxxADM user profile has, at a minimum, the following special authorities: *ALLOBJ, *IOSYSCFG, *JOBCTL , *SECADM.
   - xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used..

   iii Run server command to start the web administration interface job (only one student needs to run this on each server being used):
   `STRTCPSVR *HTTP HTTPSVR(*ADMIN)`

2. The student will remove the System i Access for Web configuration:
   i. Restore the 5250 session window.

   ii. To see the WebSphere application server running, run server command:
   `WRKACTJOB SBS(QWAS61)`

   iii. Verify iwawasxx is listed as a job under the QWAS61 subsystem. System i Access for Web requires the WebSphere application server is running before it can be removed from the configuration.

   iv. To verify the application server is really ready
   a. Enter option #**`5`** on your IWAWASxx job.
   b. Enter option #**`10`** to display the job log.
   c. Press **`F10`** to display detailed messages.
   d. Verify the message "Websphere Application Server iwawasxx Ready" is listed. This message indicates the application server as fully started and is ready for web serving.
   e. Press **`F3`** until you return to a command line.

   v. The System i Access for Web configuration can be removed using either CL commands provided in the QIWA2 library or QShell script commands provided in directory /QIBM/ProdData/Access/Web2/install.

   The Tomcat configuration exercise found earlier in this lab used a CL command to remove the System i Access for Web configuration. For this exercise, the QShell script command will be used to remove the System i Access for Web configuration.

   The script commands run within the QShell environment. Run server command:
   `QSH`

vi. Change the current directory to where the commands reside. Run server command:
`cd /QIBM/ProdData/Access/Web2/install`

vii. Display the contents of the directory. Run server command:
`ls`

viii. One of the listed files should be rmvaccweb2.

ix. To remove the System i Access for Web configuration for the iwawasxx WebSphere application server, run server command:
`rmvaccweb2 -appsvrtype *WAS61EXP -wasprf iwawasxx`

x. Several messages similar to the following will be displayed:
Removing System i Access for Web

Preparing to perform the configuration changes.

Calling WebSphere to perform the configuration changes.

System i Access for Web command has completed.

The WebSphere application server must be stopped and then started to enable the configuration changes.

xi. Press F3 to return to the command line.

If the command were to fail, or indicate an error, you could refer to the log files:

/QIBM/UserData/Access/Web2/logs/cmds.log	High level, Cause/Recovery information, translated
/QIBM/UserData/Access/Web2/logs/cmdstrace.log	Detailed command flow, For Service and development, English only

xii. Minimize the 5250 session window.

3. <u>The student will use the web administration interface to stop and delete the HTTP server and the WebSphere application server:</u>
   i. Open a browser to:
   `http://<system_name>:2001`

   ii. Login as user: WAxxADM password: WAxxPWD
   Note: xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

iii. Click the link named below on the i5/OS Tasks web page:
IBM Web Administration for i5/OS

iv. At the top of the web page, click the tab:
Manage

v. Click the tab labeled All Servers.

vi. Click the tab labeled All HTTP Servers.

vii. Locate the HTTP server named IWAHTTPxx. Select the radio button for it and click the Stop button if the IWAHTTPxx server is not already in a Stopped status.

viii. Select the Delete button at the bottom of the page to delete your IWAHTTPxx server..

ix. Select the tab All Application Servers.

x. Page through the list of servers and locate your iwawasxx server, where xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used.

xi. Select the radio button for your iwawasxx server. Click the Stop button at the bottom of the web page if your iwawasxx server is not already in a Stopped status.

xii. Select the Delete button at the bottom of the page to delete your iwawasxx server.

xiii. Close your browser window.

xiv. Restore your 5250 window.

xv. The IFS directory structure set up to contain the IWAHTTPxx server's files needs to be deleted. Run the server command:
wrklnk '/www'

xvi. An object link named "www" of type "DIR" should be displayed. Enter option **2** to Edit the "www"object. Press the Enter key.

xvii. A list of objects will be displayed. These objects are the directories that were created when HTTP servers were created on the server.

Page through the list and locate the "iwahttpxx" directory for the team you are signed on (where xx is your team number, teams 1-9 prepend the number with 0 so that two digits are used)

xviii. Enter option **9** for your "iwahttpxx" directory to perform a recursive delete of the directory and all its contents. Press the Enter key twice to delete the directory.

xix.Press F3 to return to a command entry line.

xx. Signoff the 5250 session window.

xxi.Close the 5250 session window.

Summary of tasks completed

- The System i Access for Web configuration was removed from WebSphere Application Server using the rmvaccweb2 script command.
- The HTTP server named IWAHTTPxx was stopped and deleted.
- The WebSphere application server named iwawasxx was stopped and deleted

End of cleanup exercises.

.

Reference Information on Security

SSL/HTTPS

The Internet was designed to be an open system and it allows any computer on the network to see the messages passing through. To consider an information transaction secure, it has to have the following characteristics:

Confidentiality

Use encryption if you want to ensure that the contents of the message remain private as they pass through the network.

Integrity

Use encryption and digital signatures if you want to ensure integrity. Messages are not altered while being transmitted.

Accountability

Use digital signatures when both the sender and the receiver agree that the exchange took place to ensure accountability.

Authenticity

OS/400 SSL provides server authentication so you can authenticate with whom you are talking.

You can configure the i5/OS system to use a security protocol, called Secure Sockets Layer (SSL), for data encryption and client/server authentication. A client establishes an SSL session by sending an HTTPS request to the server on the SSL port. If SSL client authentication is enabled on the server, a client certificate is requested for any HTTPS request. SSL uses a handshake protocol where the server authenticates and the client authenticates if enabled. When authenticated, they agree on the security keys to use for the session, and the algorithms to be used for encryption and message digests or hashes. When a session has been established, all data exchanged on that session is encrypted.

Below is a high level list of steps involved with enabling HTTPS. The steps may not address all issues relative to your environment. It is recommended that the i5/OS information center and HTTP server documentation be referenced to enable HTTPS.

1. If you are new to SSL, HTTPS, or digital certificates, review the following information before configuring SSL.

    i. Security concepts information in the i5/OS Information Center (http://www.ibm.com/eserver/iseries/infocenter). Look for information under the topics **Networking-->Networking Security**.

ii. Security and SSL information in the HTTP server documentation at http://www.ibm.com/servers/eserver/iseries/software/http

2. Configure your HTTP server instance to allow SSL connections. You must already have created an HTTP server that you want to enable to run SSL.

3. Configure digital certificates through the Digital Certificate Manager on the System i server.

4. Configure the web application server to use the SSL port. The SSL port must be listed within the WebSphere virtual host alias table.

5. Open a browser to one of the following URLs:

   - If using the default SSL port of 443

     ```
     https://<system_name>/webaccess/iWAHome
     ```

   - If using any other port number, replace the `<port> with the port number configured with the HTTP server.`

     ```
     https://<system_name>:<port>/webaccess/iWAHome
     ```

Firewalls

A firewall is a blockade between a secure internal network and an untrusted network such as the Internet. Most companies use a firewall to connect an internal network safely to the Internet, although you can use a firewall to secure one internal network from another also.

A firewall provides a controlled single point of contact (called a chokepoint) between your secure internal network and the untrusted network. The firewall:

- Lets users in your internal network use authorized resources that are located on the outside network.
- Prevents unauthorized users on the outside network from using resources on your internal network.

When you use a firewall as your gateway to the Internet (or other network), you reduce the risk to your internal network considerably. Using a firewall also makes administering network security easier because firewall functions carry out many of your security policy directives.

How a firewall works

To understand how a firewall works, imagine that your network is a building to which you want to control access. Your building has a lobby as the only entry point. In this lobby, you

have receptionists to welcome visitors, security guards to watch visitors, video cameras to record visitor actions, and badge readers to authenticate visitors who enter the building.

These measures may work well to control access to your building. But, if an unauthorized person succeeds in entering your building, you have no way to protect the building against this intruder's actions. If you monitor the intruder's movements, however, you have a chance to detect any suspicious activity from the intruder.

Firewall components

A firewall is a collection of hardware and software that, when used together, prevent unauthorized access to a portion of a network. A firewall consists of the following components:

- Hardware. Firewall hardware usually consists of a separate computer or device dedicated to running the firewall software functions.
- Software. Firewall software provides a variety of applications. In terms of network security, a firewall provides these security controls through a variety of technologies:
  - Internet Protocol (IP) packet filtering
  - Network address translation (NAT) services
  - SOCKS server
  - Proxy servers for a variety of services such as HTTP, Telnet, FTP, and so forth
  - Mail relay services
  - Split Domain name services (DNS)
  - Logging
  - Real-time monitoring

  Note: Some firewalls provide virtual private networking (VPN) services so that you can set up encrypted sessions between your firewall and other compatible firewalls.

Using firewall technologies

You can use the firewall proxy servers, SOCKS server, or NAT rules to provide internal users with safe access to services on the Internet. The proxy and SOCKS servers break TCP/IP connections at the firewall to hide internal network information from the untrusted network. The servers also provide additional logging capabilities.

You can use NAT to provide Internet users with easy access to a public server behind the firewall. The firewall still protects your network because NAT hides your internal IP addresses.

A firewall also can protect internal information by providing a DNS server for use by the firewall. In effect, you have two DNS servers: one that you use for data about the internal network, and one on the firewall for data about external networks and the firewall itself. This allows you to control outside access to information about your internal systems

When you define your firewall strategy, you may think it is sufficient to prohibit everything that presents a risk for the organization and allow everything else. However, because computer criminals constantly create new attack methods, you must anticipate ways to prevent these attacks. As in the example of the building, you also need to monitor for signs that, somehow, someone has breached your defenses. Generally, it is much more damaging and costly to recover from a break-in than to prevent one.

In the case of a firewall, your best strategy is to permit only those applications that you have tested and have confidence in. If you follow this strategy, you must exhaustively define the list of services you must run on your firewall. You can characterize each service by the direction of the connection (from inside to outside, or outside to inside). You should also list users who you will authorize to use each service and the machines that can issue a connection for it.

What a firewall can do to protect your network

You install a firewall between your network and your connection point to the Internet (or other untrusted network). The firewall then allows you to limit the points of entry into your network. A firewall provides a single point of contact (called a chokepoint) between your network and the Internet (see the figure below). Because you have a single point of contact, you have more control over which traffic to allow into and out of your network.

A firewall appears as a single address to the public. The firewall provides access to the untrusted network through proxy or SOCKS servers or network address translation (NAT) while hiding your internal network addresses. Consequently, the firewall maintains the privacy of your internal network. Keeping information about your network private is one way in which the firewall makes an impersonation attack (spoofing) less likely.

A firewall allows you to control traffic into and out of your network to minimize the risk of attack to your network. A firewall securely filters all traffic that enters your network so that only specific types of traffic for specific destinations can enter. This minimizes the risk that someone could use TELNET or file transfer protocol (FTP) to gain access to your internal systems.

What a firewall cannot do to protect your network

While a firewall provides a tremendous amount of protection from certain kinds of attack, a firewall is only part of your total security solution. For instance, a firewall cannot necessarily protect data that you send over the Internet through applications such as SMTP mail, FTP,

and TELNET. Unless you choose to encrypt this data, anyone on the Internet can access it as it travels to its destination.

Additional information

HTTP Server redbook

http://www.redbooks.ibm.com/redpieces/pdfs/sg246716.pdf

Section 6.3 Encrypting your data with SSL and TLS

Section 6.4 Proxy server: Protecting direct access

Information Center

Setting up a reverse proxy for HTTP server

http://publib.boulder.ibm.com/iseries/v5r2/ic2924/index.htm?info/rzaie/rzaiereverseproxy.htm

Tradmarks and Disclaimers

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Trademarks of International Business Machines Corporation in the United States, other countries, or both can be found on the World Wide Web at http://www.ibm.com/legal/copytrade.shtml.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce. ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others.

Information is provided "AS IS" without warranty of any kind.

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product

announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. 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.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.