WebSphere® Application Server EAL4
AGD - Guidance

IBM WebSphere
Security Development Team
Austin, TX

Date: 27 April 2006
Issue: 9.2
Reference: WAS/EAL4/AGD/92

This Page Intentionally Left Blank.

Table of Contents

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States and other countries, or both:

AIX®
DB2®
IBM®
Power PC®
Tivoli®
WebSphere®
z/OS®

The following terms are trademarks of other companies:

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. 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.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

References

[CC] Common Criteria for Information Technology Security Evaluation, CCIMB-2004-01, Version 2.2, January 2004.

Document Control Information

Identification	Author	Summary of Changes
Version 9.2 Dated 27 April 2006 Reference: WAS/EAL4/AGD/92	Kristen Clarke Donna Skibbie WebSphere Application Server Development	Registered trademarks and a statement regarding z/OS installations

Identification	Author	Summary of Changes
Version 9.1 Dated 16 March 2006 Reference: WAS/EAL4/AGD/91	Kristen Clarke Elton Faggett Darrin Giesy Cheryl King Dan Murphy Donna Skibbie WebSphere Application Server Development	Countermeasures for vulnerabilities added
Version 9.0 Dated 13 March 2006 Reference: WAS/EAL4/AGD/90	Kristen Clarke Elton Faggett Darrin Giesy Cheryl King Dan Murphy Donna Skibbie WebSphere Application Server Development	Command syntax clarification.
Version 8.0 Dated 10 March 2006 Reference: WAS/EAL4/AGD/80	Kristen Clarke Elton Faggett Darrin Giesy Cheryl King Dan Murphy Donna Skibbie WebSphere Application Server Development	Made updates related to Vulnerability Analysis.
Version 7.0 Dated 10 March 2006 Reference: WAS/EAL4/AGD/70	Kristen Clarke Elton Faggett Darrin Giesy Cheryl King Dan Murphy Donna Skibbie WebSphere Application Server Development	Responded to Misuse Analysis ETRs. Updated Notices section. Command syntax clarification and editing.
Version 6.0 Dated 07 March 2006 Reference: WAS/EAL4/AGD/60	Kristen Clarke Elton Faggett Cheryl King Dan Murphy Donna Skibbie	Responded to comments from evaluators.

Identification	Author	Summary of Changes
	WebSphere Application Server Development	
Version 5.0 Dated 27 February 2006 Reference: WAS/EAL4/AGD/50	Kristen Clarke Elton Faggett Cheryl King Dan Murphy Donna Skibbie WebSphere Application Server Development	
Version 4.0 Dated 17 February 2006 Reference: WAS/EAL4/AGD/40	Kristen Clarke Elton Faggett Cheryl King Dan Murphy Donna Skibbie WebSphere Application Server Development Team, Austin, TX	Addressed ETRs for Ease of Misuse Analysis
Version 3.0 Dated 10 February 2006 Reference: WAS/EAL4/AGD/30	Kristen Clarke Elton Faggett Cheryl King Dan Murphy Donna Skibbie WebSphere Application Server Development Team, Austin, TX	
Version 2.0 Dated 01 December 2005 Reference: WAS/EAL4/AGD/20	Kristen Clarke Elton Faggett Cheryl King Dan Murphy Donna Skibbie WebSphere Application Server Development Team, Austin, TX	
Version 1.0 Dated 14 October 2005 Reference: WAS/EAL4/AGD/10	Kristen Clarke Elton Faggett Cheryl King Dan Murphy Donna Skibbie	Initial version

Identification	Author	Summary of Changes
	WebSphere Application Server Development Team, Austin, TX	

1 Introduction to the Certified System

This document describes how to set up and use the WebSphere Application Server system environment that is certified to operate at a Common Criteria EAL4 level of assurance. The following information is covered:

- Overview of the certified system
- An installation and configuration guide for the certified system
- An administrator guide for the certified system
- A developer's guide for the certified system

1.1 Glossary

This document uses the following terms:

API	Application Programming Interface
Certified application, certified resource adapter, certified providers	An enterprise application, resource adapter, or resource provider is certified at a Common Criteria EAL4 level of assurance to run inside the certified system.
Certified system	The WebSphere Application Server system environment that is certified to operate at a Common Criteria EAL4 level of assurance.
Channel chain	Channel chain refers to the channel transport chain such as that used by DCS. For details on the DCS channel transport chain options, reference the WebSphere Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/urun_chain_typedcs.html
CSIv2	Common Secure Interoperability Version 2 is an authentication protocol developed by the Object Management Group (OMG) that supports interoperability, authentication delegation and privileges. For details on authentication protocols for EJB security on the Application server see http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/csec_corba.html

DCS	The Distribution and Consistency Services is a component of the WebSphere high availability network which uses the Channel Framework as the default network protocol and allows configuration of a transport channel. For details on configuring the DCS transport channel reference the WebSphere Application Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/urun_chain_typedcs.html
HA Manager	The High Availability (HA) Manager component of the WebSphere Application Server. For details, reference the WebSphere Application Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/crun_ha_hamanager.html
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol (HTTP) an internet protocol that is used to transfer and display hypertext and XML documents on the Web.
IBM HTTP Server	IBM HTTP Server. For details, see the IBM HTTP Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/welcome_ihs.html
IIOP	Internet Inter-ORB Protocol (IIOP) is a protocol used for communication between Common Object Request Broker Architecture (CORBA) Object Request Brokers.
JAAS	Java Authentication and Authorization Service (JAAS) is the package through which services can authenticate and authorized users while enabling the applications to remain independent from underlying technologies. For details see the WebSphere Application Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/csec_jaas.html
JACC	Java Authorization Contract for Containers (JACC) is a J2EE specification that enables third party security providers to manage authorization in the application

	server. For details, see the WebSphere Application Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/csec_jaccauthorization.html
JDBC	Java Database Connectivity (JDBC) is an industry standard for database-independent connectivity between Java code and a wide range of databases. The JDBC provides a call-level application programming interface (API) for SQL-based database access. For information on creating and configuring a JDBC provider for WebSphere Application Server, see the Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/tdat_tccrtprovds.html
JDK	Java Development Kit
JMS	Java Message Service (JMS) is a Java API that supports the creation and communication of various messaging implementations. For more on messaging and WebSphere Application Server see the Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/tm_learn.html
JVM	Java Virtual Machine (JVM) is a software implementation of a central processing unit that runs compiled Java code (applets and applications).
LDAP	Lightweight Directory Access Protocol (LDAP) is an open protocol that uses TCP/IP to provide access to information directories that support an X.500 model and it does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory. For information on configuring LDAP as the user registry with WebSphere Application Server, see http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/tsec_ldap.html
LTPA	Lightweight Third Party Authentication (LTPA) is a

	protocol that uses cryptography to support security in a distributed environment. For details see the WebSphere Application Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/csec_ltpa.html
ORB	Object Request Broker (ORB) in object-oriented programming, software that serves as an intermediary by transparently enabling objects to exchange requests and responses. For details, see the WebSphere Application Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/welc6tech_orb.html
RMI	Remote Method Invocation (RMI) is a protocol that is used to communicate method invocations over a network. Java Remote Method Invocation is a distributed object model in which the methods of remote objects written in Java programming language can be invoked from other Java virtual machines, possibly on different hosts.
SSL	Secure Sockets Layer (SSL) is a security protocol that provides transport layer security: authenticity, integrity, and confidentiality, for a secure connection between a client and a server. The protocol runs above TCP/IP and below application protocols.
SWAM	Simple WebSphere Application Server Authentication Protocol (SWAM) is an authentication mechanism for simple, non-distributed, single application server run-time environments. For details, see the WebSphere Application Server Information Center at: http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/rsec_swam.html
TCP/IP	Transmission Control Protocol/Internet Protocol (TCP/IP) is an industry-standard nonproprietary set of communication protocols that provide reliable end-to-end connections between applications over interconnected networks of different types.
TOE	Target Of Evaluation. An IT product or system and its associated administrator and user guidance documentation that is the subject of the evaluation.

Trusted application, trusted resource adapter, trusted providers	An enterprise application, resource adapter, or resource provider that was written by a developer who is trusted to comply with all the guidelines identified in section 5.
UDDI	Universal Description, Discovery, and Integration (UDDI) defines a way to publish and discover information about Web Services. Refer to the WebSphere Application Server Information Center for more details on the UDDI registry for WebSphere Application Server http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/cwsu_over.html
URL	Uniform Resource Locator (URL) is the unique address of a file that is accessible in a network such as the Internet. The URL includes the abbreviated name of the protocol used to access the information resource and the information used by the protocol to locate the information resource

2 Overview of the Certified System

Common Criteria is an internationally recognized International ISO standard (ISO/IEC 15408) for the assurance evaluation of IT products. The following versions and editions of WebSphere® Application Server Version provide a system environment that has been evaluated according to Common Criteria and, as a result of this evaluation, has been certified to operate at an EAL4 level of assurance:

- WebSphere Application Server v6.0.2.3 (32-bit)
- WebSphere Application Server Express v6.0.2.3
- WebSphere Application Server Network Deployment v6.0.2.3 (32-bit)
- WebSphere Application Server for z/OS v6.0.1, service level 6.0.2.3

Note: WebSphere Application Server V6.0.2.3, WebSphere Application Server Express V6.0.2.3, and WebSphere Application Server Network Deployment V6.0.2.3 requires interim fixes for APARs PK15487, PK16977, PK13494, PK13653, PK15059, PK18574, PK18576, and PK18991. WebSphere Application Server for z/OS 6.01, service level 6.0.2.3 requires the fix to APAR AK17408.

These versions and editions have been evaluated and certified on the following operating system platforms:

- AIX® 5.2 (64-bit);
- HP-UX 11i (64-bit PA-RISC);
- Linux® Redhat 4 on Power PC® (64-bit) /Intel™ / z/OS®
- Linux SuSE Enterprise Edition 9 (SLES 9) on Power PC (64-bit) / z/OS;
- Sun Solaris 9 (64-bit);
- Microsoft® Windows® 2003; and
- z/OS 1.6.

The evaluated and certified system environment consists of the following:

- Target of Evaluation (TOE)
- Evaluated configuration
- Evaluated security functions
- Organization policies

2.1 Target of Evaluation (TOE)

The TOE is the set of WebSphere Application Server components that have been evaluated and certified. These components are:

- Application Server
- Admin Scripting Client (the wsadmin tool and the administrative client code)
- IBM HTTP Server
- Node Agent Server
- Deployment Manager Server

Note: The Node Agent Server and Deployment Manager Server are provided only with the WebSphere Application Server Network Deployment Manager and WebSphere Application Server for z/OS products. Therefore, these two servers were evaluated and certified only with these two products.

2.2 Evaluated Configuration

The evaluated configuration is the configuration in which the TOE was evaluated and certified. The following describes the evaluated configuration of the TOE.

2.2.1 Application Server (required)

This section applies to all the editions of the WebSphere Application Server.

The Application Server is provided by WebSphere Application Server and is required. It must be installed on one of the operating system platforms listed in Section 2. The following table lists the configuration parameters of the Application Server that must be set in a certain way in order for the Application Server to be in the evaluated configuration:

Parameter	Setting	Comment
Security->Global Security	Enabled	
Security->Global Security->Active Protocol	CSI	Selecting CSI results in use of the Common Security Interoperability Version 2 (CSIv2) protocol. Note: It is strongly recommended that you configure CSIv2 to use the SSL with encryption.

Parameter	Setting	Comment
Security->Global Security->Enforce Java2 Security	Enabled	
Security->Global Security-> User Registry	LDAP (for WebSphere Application Server, WebSphere Application Server, Express and WebSphere Application Server, Network Deployment) Local OS (for WebSphere Application Server for z/OS)	The Custom user registry must not be configured.
Security-> Global Security-> User Registry-> Local OS Ignore case for authorization	Enabled	This step applies to z/OS Local OS user registry only
Security-> Global Security-> User Registry Custom Properties com.ibm.security.SAF.authorization	False	This step applies to z/OS Local OS user registry only.
Security-> Global Security-> User Registry Custom Properties com.ibm.security.SAF.delegation	False	This step applies to z/OS Local OS user registry only.
Security-> Authentication Mechanism	LTPA (Lightweight Third Party Authentication)	SWAM must not be configured.
Security -> Authentication Mechanism-> LTPA -> SSO (single signon)	Enabled	
Security-> Authentication Protocol ->CSI Inbound Authentication-> Security Attribute Propagation	Enabled	

Parameter	Setting	Comment
Administrative connection	RMIConnector	
System Administration-> Deployment Manager-> Additional Properties-> Ports	Only the following ports may be configured. Any other ports must be deleted: • CELL_DISCOVERY_ADDRESS • BOOTSTRAP_ADDRESS • ORB_LISTENER_ADDRESS • DCS_UNICAST_ADDRESS • WC_adminhost_secure For WebSphere Application Server, Network Deployment, the following ports may be present: • CSIV2_SSL_MUTUALAUTH_LISTENER • CSIV2_SSL_SERVERAUTH_LISTENER For WebSphere Application Server for z/OS, the following port may be present: • ORB_SSL_LISTENER_ADDRESS	This parameter is only applicable for the Network Deployment and z/OS product. For those additions, ports other than those listed must be removed.
System Administration-> Node Agents -> node agent name-> Additional Properties-> Ports	Only the following ports may be configured. Any other ports must be deleted: • BOOTSTRAP_ADDRESS • ORB_LISTENER_ADDRESS • DCS_UNICAST_ADDRESS • NODE_DISCOVERY_ADDRESS • NODE_IPV6_MULTICAST_DISCOVERY • NODE_MULTICAST_DISCOVE	This parameter is only applicable for the Network Deployment and z/OS product. For those additions, ports other than those listed must be removed.

Parameter	Setting	Comment
	RY_ADDRESS For WebSphere Application Server, Network Deployment, the following ports may be present: - CSIV2_SSL_MUTUALAUTH_LISTENER - CSIV2_SSL_SERVERAUTH_LISTENER For WebSphere Application Server for z/OS, the following port may be present: - ORB_SSL_LISTENER_ADDRESS	
System Administration-> Servers-> Application Servers -> Application Server name -> Communications-> Ports	- BOOTSTRAP_ADDRESS - ORB_LISTENER_ADDRESS - DCS_UNICAST_ADDRESS - WC_defaulthost - WC_defaulthost_secure - SIB_ENDPOINT_SECURE_ADDRESS - SIB_MQ_ENDPOINT_ADDRESS (Note: applicable only if WebSphere MQ is configured) - SIB_MQ_ENDPOINT_SECURE_ADDRESS (Note: applicable only if WebSphere MQ is configured) For WebSphere Application Server, WebSphere Application Server, Express and WebSphere Application Server, Network Deployment, the following ports may be present: - CSIV2_SSL_MUTUALAUTH_LISTENER - CSIV2_SSL_SERVERAUTH_LI	

Parameter	Setting	Comment
	STENER For WebSphere Application Server for z/OS, the following port may be present: - ORB_SSL_LISTENER_ADDRESS	
Servers-> Core Groups-> Core Group Settings-> DefaultCoreGroup->Transport types	Channel Framework	This parameter is applicable only for the Network Deployment and z/OS product. For those products, this parameter is required for High Availability Manager.
Servers-> Core Groups->Core Group Settings-> DefaultCoreGroup-> Channel Chain Name	DCS or DCS_SECURE	This parameter is applicable only for the Network Deployment and z/OS products. For those products, this parameter is required for High Availability Manager. Note: It is strongly recommended that you configure DCS_SECURE rather than DCS, since DCS_SECURE provides an SSL encrypted transport.
Applications	Only the following applications can be installed: - The UDDI application provided by WebSphere Application Server (if multiple Application Servers are configured, only one of these	This applies to the applications that are provided with WebSphere Application Server as well as any user applications.

Parameter	**Setting**	**Comment**
	servers can contain the UDDI application) - Trusted applications - Certified applications	
Applications->UDDI->Role mappings	Must be the mappings configured in the shipped configuration, which are as follows: GUI_Publish_User role—No IDs mapped to this role (see Note 1) GUI_Inquiry_User role – No IDs mapped to this role. (see Note 1) SOAP_Publish_User – AllAuthenticated is mapped to this role. SOAP_Inquiry_User – Everyone is mapped to this role. (See Note 1) EJB_Inquiry_Role - No IDs mapped to this role. (see Note 1) EJB_Publish_Role – No IDs mapped to this role. V3SOAP_Inquiry_User – Everyone is mapped to this role. (see Note 1) V3SOAP_Security_User_Role – No IDs are mapped to this role. V3SOAP_Publish_User_Role – AllAuthenticated is mapped to this role. V3SOAP_Custody_Transfer_User_Role – AllAuthenticated is mapped to this role. (Note 1: this role is not relevant to the evaluated security functions.)	These mappings applicable and required only if the UDDI application is configured. These mappings should not be changed.
Applications->UDDI->Properties->Use authinfo credentials if provided	Disabled	This parameter is applicable and required only if the UDDI application is configured.

Parameter	**Setting**	**Comment**
Applications->UDDI->Properties->Automatically register UDDI publishers	Disabled	This parameter is applicable and required only if the UDDI application is configured.
Applications->UDDI->properties -> Key space request require digital signature	Disabled	This parameter is applicable and required only if the UDDI application is configured.
System applications	No system applications should be installed on the application server. For WebSphere Application Server, ND and WebSphere Application Server for z/OS, only the Secured File Transfer system application may be installed on the deployment manager system.	System applications are not visible using the administrative interfaces. See the validation script in the appendices for information on how to view the system applications and see the example configuration scripts in the appendices for information on how to delete the system applications.
Resource Providers-> JMS providers	Only the following types of resource providers can be configured: • WebSphere JMS Provider (used with Default messaging in WebSphere Application Server) • WebSphere MQ JMS Provider (used by IBM WebSphere MQ 5.3.0.2 csd 6 (non-z/OS platforms) or by WebSphere MQ 5.3.1 for z/OS (z/OS platform). This provider is part of the environment. • A trusted JMS provider • A certified JMS provider	This parameter is applicable and required only when a messaging application is used -- such as Default messaging in the WebSphere Application server or WebSphere MQ in the environment.

Parameter	Setting	Comment
Servers-> Application Servers-> serverX-> Messaging Engine Inbound Transports-> Inbound Basic Messaging	Disabled	This parameter is applicable and required only when the Default Messaging is configured.
Servers-> Application Servers-> ServerX-> Messaging Engine Inbound Transports-> Inbound Secure Messaging	Enabled	This parameter is applicable and required only when the Default Messaging is configured.
Service Integration-> Buses -> BusX-> Secure	Enabled	This parameter is applicable and required only when the Default Messaging is configured.
Service Integration-> Buses-> BusX->Inter-engine Transport Chain	Enter a name for the Transport Chain	This parameter is applicable and required only when the Default Messaging is configured.
Service Integration-> Buses-> BusX->Inter-engine Authentication Alias	Specify the Inter-engine Authentication Alias	This parameter is applicable and required only when the Default Messaging is configured.
Default Messaging -> Role mappings	Bus Connector role – remove AllAuthenticated from this role. Sender role – remove AllAuthenticated from this role Receiver role – remove AllAuthenticated from this role Browser role – remove AllAuthenticated from this role.	This parameter is applicable and required only when the Default Messaging is configured.
Resources-> JDBC Providers	Only the following types of JDBC providers can be configured:	This parameter is applicable and required only when a JDBC

Parameter	Setting	Comment
	• Cloudscape JDBC Provider • DB2 JDBC provider • A trusted JDBC provider • A certified JDBC provider	resource is being used
Resources->URL Provider	Only the following types of URL providers can be configured: • Default URL Provider • A trusted URL provider • A certified URL provider	
Resources-> Resource Adapters	Only the following types of Resource Adapters can be configured: • SIB JMS Resource Adapter (for use by Default Messaging) • WebSphere Relational Resource Adapter • A trusted Resource adapter • A certified Resource adapter	
Resources-> Mail Providers	Only the following types of Mail Providers can be configured: • Built-in Mail Provider • A trusted Mail Provider • A certified Mail Provider	
Security->Global security-> Authentication-> LTPA-> Trust Association	Only the following types of Trust Association Interceptors can be configured: • A trusted Trust Association Interceptor • A certified Trust Association Interceptor	
Security-> Global security-> Authorization Providers	No JACC providers must be configured.	

Parameter	**Setting**	**Comment**
Security-> Global Security-> JAAS Configuration	Only the following types of JAAS login modules can be configured: • Application Logins o Client container o DefaultPrincipalMapping o WSLogin o A trusted JAAS provider o A certified JAAS provider • System Logins o Default o LTPA o LTPA_WEB o RMI_INBOUND o RMI_OUTBOUND o SWAM o WEB_INBOUND o wssecurity.IDAssertion o wssecurity.IDAssertionUsernameToken o wssecurity.PKCS7 o wssecurity.PkiPath o wssecurity.signature o wssecurity.UsernameToken o wssecurity.X509BST For WebSphere Application Server for z/OS the following additional System Logins can be configured: o SWAM_ZOSMAPPING o ICSF	This parameter is applicable and required for the use by applications and system resources .The login modules should not be removed.

Parameter	Setting	Comment
Security-> Global Security-> Custom Properties	For the com.ibm.wsspi.security.ltpa.tokenFactory property, the value configured to specify the token factories should be: • com.ibm.ws.security.ltpa.LTPATokenFactory|com.ibm.ws.security.ltpa.LTPAToken2Factory|com.ibm.ws.security.ltpa.AuthzPropTokenFactory	

2.2.2 Admin Scripting Client (required)

This section applies to all the editions of the WebSphere Application Server.

The Admin Scripting Client (wsadmin and admin client) is provided by WebSphere Application Server and is required. It must be installed on one of the operating system platforms listed in the beginning of Section 2.

In order for the Admin Scripting Client to be in the evaluated configuration, it must be configured to communicate with the Application Server, Node Agent, or Deployment Manager through the remote RMI JMX connector port.

2.2.3 IBM HTTP Server (optional)

This section applies to all the editions of the WebSphere Application Server.

The IBM HTTP Server is provided by WebSphere Application Server on all platforms except for z/OS and is optional. If IBM HTTP Server is configured, it must be installed on one of the platforms listed in the beginning of Section 2 with the exception of the z/OS platform. In addition, the httpd.conf configuration file must be updated as follows in order to be in the evaluated configuration.

- The SSLFIPSEnable directive must be included
- No SSLCipher directives must be present
- The following Load Module directives, but no others, are included
    - LoadModule log_config_module modules/mod_log_config.so
    - LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
    - LoadModule was_ap20_module "modules/mod_was_ap20_http.so"

2.2.4 Deployment Manager (optional)

This section applies only to the WebSphere Application Server Network Deployment and WebSphere Application Server for z/OS editions.

The Deployment Manager is provided by WebSphere Application Server Network Deployment and WebSphere Application Server for z/OS. The Deployment Manager is optional. If configured, it must be installed on one of the operating system platforms listed in the beginning of Section 2 and only one Deployment Manager can be configured. (The evaluated configuration does not support multiple cells and for a z/OS cell, all the systems must be on the z/OS platform.)

The same restrictions apply to the configuration parameters of the Deployment Manager as those that apply to the configuration parameters of the Application Server with the following exceptions:

- No applications can be installed on the Deployment Manager in the evaluated configuration, except for the Secured File Transfer system application.
- One system application must be installed on the Deployment Manager in the evaluated configuration and this application must be the Secured File Transfer application (fileTransferSecured.ear). System applications are not visible using the administrative interfaces. See the verification script in the appendices for information on how to view the system applications and see the example configuration scripts in the appendices for information on how to delete the system applications.

2.2.5 Node Agent (optional)

This section applies only to the WebSphere Application Server Network Deployment and WebSphere Application Server for z/OS editions.

The Node Agent is provided by WebSphere Application Server Network Deployment and WebSphere Application Server for z/OS. The Node Agent is optional, but must be configured if the Deployment Manager is configured. If configured, the Node Agent must be installed on one of the operating system platforms listed in the beginning of Section 2 and one Node Agent must be configured on each node containing an Application Server.

The same restrictions apply to the configuration parameters of the Node Agent as those that apply to the configuration parameters of the Application Server with the following exception: No applications can be installed on the Node Agent in the evaluated configuration.

2.3 Evaluated Security Functions

The evaluated security functions are the TOE security functions that have been evaluated and certified. They consist of the following:

- Evaluated Identification Functions
- Evaluated Access Control Functions
- Evaluated Security Management Functions
- Evaluated Invocation of SSL Function

Most of the evaluated security functions are designed to protect a set of resources from access by un-authorized remote callers. The following describes the protected resources and then describes the evaluated security functions.

2.3.1 Protected Resources

Most of the evaluated security functions are designed to protect the following resources:

- Protected resources of the administration service
- Protected resources of the naming service
- Protected resources and HTML pages in deployed web server applications
- Protected resources in deployed enterprise beans
- Protected resources of the UDDI Registry service
- Protected resources of the Transactions and Activities Services
- Protected resources of the Default Messaging Provider
- Protected file resources

2.3.1.1 Protected Resources of the Administration Service

The administration service is implemented by the Application Server, Node Agent, and Deployment Manager. It consists of a set of management beans, called MBeans. The protected resources of the administration service are the methods that can be accessed remotely, by means of remote interfaces, and that can be used to request an MBean to perform any of the following operations:

- Operations that get or set configuration attributes of the Application Server, Node Agent, or Deployment Manager.
- Operations that affect the runtime state of the Application Server, Node Agent, or Deployment Manager)

2.3.1.2 Protected Resources of the Naming Service

The naming service is implemented by the Application Server, Node Agent, and Deployment Manager. The protected resources of the naming service are the methods that can be accessed remotely, by means of remote interfaces, and that can be used to request a read, write, create, or delete operation in the naming directory.

2.3.1.3 Protected Resources of Deployed Web Server Applications

One or more web server applications optionally can be deployed in an Application Server. These applications contain methods or HTML pages that implement HTTP interfaces and the HTTP interfaces are configured with a URL address. A remote caller can access a method or HTML page in a web server application by issuing an HTTP request to the Application Server and, in the request, specifying the URL address and HTTP interface of the desired method or HTML page.

The protected resources of a deployed web server application are methods or HTML pages that the developer has configured as follows:

- The URL for the method or HTML page is configured with a login constraint.
- The method or HTML page is configured with a security constraint clause, which lists each application-defined role that has permission to invoke the method or HTML page.

2.3.1.4 Protected Resources of Deployed Enterprise Beans

One or more enterprise beans optionally can be deployed in an Application Server. The enterprise beans could contain remote RMI interfaces or web services interfaces that correspond to the methods in the enterprise bean.

If an enterprise bean contains a remote RMI interface, a remote caller can access the method that corresponds to this interface by issuing an IIOP request to the Application Server and, in the IIOP request, specifying the remote RMI interface that corresponds to the method. If an enterprise bean contains a web service interface, a remote caller can access the method that corresponds to this interface by issuing an HTTP request to the Application Server and, in the HTTP request, specifying the web service interface.

The protected resources in a deployed enterprise bean consist of each method in the enterprise bean in which the developer has defined a corresponding remote RMI interface or web service interface for the method and also has configured this interface with a permission clause, which lists each application-defined role that has permission to invoke the associated method.

2.3.1.5 Protected Transaction and Activities Resources

Web server applications, enterprise beans, or both that are deployed on different Application Servers could be coded to share a single transaction or activity. If so, the Application Servers must exchange information about the transaction or activity. The remote interfaces that the Application Servers use to exchange information about a transaction are not documented in the user documentation and are protected interfaces.

2.3.1.6 Protected Resources of the UDDI Registry Service

The UDDI registry service is an application that optionally can be installed on an Application Server. The protected resources of the UDDI registry service are the methods that can be accessed remotely, by means of remote interfaces, and that can be used to publish information in the UDDI registry.

2.3.1.7 Protected Resources of the Default Messaging Provider

An Application Server optionally can be configured to use the Default Messaging Provider. The protected resources of the Default Messaging Provider are the methods that can be accessed remotely, by means of remote interfaces, and that can be used to access any of the following destinations: bus, queues, temporary destinations, topic space root, topic spaces, and topics.

2.3.1.8 Protected File Resources

When using the WebSphere Application Server Network Deployment or WebSphere Application Server for z/OS edition, the Application Server, Node Agent, and Deployment Manager use remote interfaces to exchange files with each other. The remote interfaces are not documented in the user documentation and are all protected.

2.3.2 Evaluated Identification Functions

The evaluated identification can be grouped into the following categories:

- Identification
- Re-identification
- Run-as

The identification functions intercept requests to the remote interfaces of the Application Server, Node Agent, and Deployment Manager and attempts to identify the remote caller using the configured identification protocol. If the caller cannot be identified, the request is denied. Otherwise, the function gets the user and group IDs of the remote caller from the user registry and associates these IDs with the request.

The following table lists the remote interfaces that can be configured for the Application Server, Node Agent, and Deployment Manager in the evaluated configuration and that process an identification function:

Remote Interface	Application Server	Node Agent	Deployment Manager
HTTP/S	X		X
ORB	X	X	X
Secure Messaging (InboundSecureMessaging)	X (optional)		
HA Manager (DCS or DCS_SECURE)	X	X	X

The re-identification function applies only to a web services interface of a web service enterprise bean, which is supported in the evaluated configuration only on an Application Server, and only if this interface (also called an endpoint) is configured to require an identification token, trust token, or both. If so, the re-identification function attempts to re-identify the caller of the request to the web services endpoint using information of the web services caller that was passed in the identification token or in the combination of identification token and trust token. (The HTTP or HTTPS caller already has been identified using the information passed with the HTTP request. This function attempts to identify the caller of the web services request, which is embedded in the HTTP or HTTPS request, using the information passed with the identification token, the trust token, or both.) If the caller of the web services request cannot be identified, the request is denied. Otherwise, the re-identification function gets the user and group IDs of the web services caller and associates these IDs with the request as a replacement to the IDs from the HTTP or HTTPS caller.

The run-as function applies only to a method in a deployed web server application or enterprise bean. It sets the identity of the method to either the caller, which is the default, or to the configured run-as attribute which can be any of the following:

- Client (caller)
- Specified identity (a run-as role that has been mapped to a user ID and password)
- System (applicable only for a method in an enterprise bean)

2.3.3 Evaluated Access Control Functions

The evaluated access control functions control access to the protected resource. The following describes the evaluated access control functions

2.3.3.1 Protection of Methods and HTML Pages in Deployed Web Server Applications

When a remote caller issues a request to an HTTP interface that corresponds to a method or HTML page in a deployed web server application that is configured as described, this function invokes the method or HTML page only if one of the following conditions is true:

- A user or group ID of the user is mapped to a role that has permission to access the method or HTML page.
- The special group ID of “Everyone” is mapped to a role that has permission to access the method or HTML page.
- The special group ID of “AllAuthenticatedUsers” is mapped to a role that has permission to access the method or HTML page and the remote caller has been successfully identified.
- The method is not configured with a permission (security constraint).

2.3.3.2 Protection of Methods in Deployed Enterprise Beans

When a remote caller issues a request to the remote RMI interface that corresponds to a method in an enterprise bean, this function invokes the method only if one of the following conditions is true:

- A user or group ID of the user is mapped to a role that has permission to access the method.
- The special group ID of “Everyone” is mapped to a role that has permission to access the method
- The special group ID of “AllAuthenticatedUsers” is mapped to a role that has permission to access the method and the remote caller has been successfully identified.
- The method is not configured with a permission clause.

2.3.3.3 Protection of Resources of the Naming Service

When a remote caller issues a request to the remote interface that corresponds to a protected method of the naming service, the request is denied unless one of the following conditions is true:

- A user or group ID of the user is mapped to a role that has permission to perform the operation.
- The special group ID of “Everyone” is mapped to a role that has permission to perform the operation.

- The special group ID of “AllAuthenticatedUsers” is mapped to a role that has permission to perform the operation and the remote caller has been successfully identified.

The following table lists the naming roles and permissions that are granted to each role:

Naming Role	Permission
CosNamingRead	Permission to read from the naming directory
CosNamingWrite	CosNamingRead permission plus permission to write to the naming directory
CosNamingCreate	CosNamingWrite permission plus permission to insert entries in the naming directory
CosNamingDelete	CosNamingCreate permission plus permission to delete entries in the naming directory

2.3.3.4 Protection of Resources of the Administration Service

When a remote caller issues a request to the remote interface of the administration service that can be used to access configuration data or runtime state, the request is denied unless one of the following conditions is true:

- A user or group ID of the user is mapped to a role that has permission to perform the operation.
- The special group ID of “Everyone” is mapped to a role that has permission to perform the operation.
- The special group ID of “AllAuthenticatedUsers” is mapped to a role that has permission to perform the operation and the remote caller has been successfully identified.

The following table lists the administration roles and, in general, the permissions that are granted for each role.

Administration Role	Permission
Monitor	Permission to read configuration attributes and runtime state
Operator	Monitor permission plus permission to affect runtime state
Configurator	Monitor permission plus permission to write configuration attributes with the exception of the highly sensitive configuration attributes

Administrator	Operator and Configurator permission plus permission to write highly sensitive configuration attributes

However, in some cases, the permissions for a specific MBean are somewhat different from those indicated in the table. See the MBean Javadoc in the WebSphere Application Server Information Center at the following link for complete information on the permissions for each MBean: http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.javadoc.doc/public_html/mbeandocs/html/index.html

2.3.3.5 Protection of Transactions and Activity Resources

When a remote caller issues a request to a remote interface of the transaction or activity service, the request is denied unless a user or group ID of the caller is mapped to the administrator role.

2.3.3.6 Protection of Messaging Resources

When a remote caller issues a request to a remote interface of the Default Messaging Provider for the purpose of performing a protected messaging operation (connect, send, receive, browse, create, or identity adopter) against a protected messaging resource (local bus, queue destination, temporary destination, topic space, topic space root, and topics), the request is denied unless one of the following conditions are true:

- The special group ID of “Everyone” is mapped to a role that has permission to perform the operation.
- The user ID is mapped to a role that has permission to perform the operation.
- The special group ID of “AllAuthenticated” is mapped to a role that has permission to perform the operation and the remote caller has been successfully identified.
- A user or group ID is mapped to a role that has permission to perform the operation. (See section 4.6 for information on the roles that have permission to perform the protected messaging operations.)

2.3.3.7 Protection of UDDI Registry Resources

The UDDI application has two groups of remote interfaces: remote RMI interfaces and remote HTTP interfaces. When a remote caller issues a request to a remote RMI interface of the UDDI registry, the request is always denied. When a remote caller issues a request to a remote HTTP interface of the UDDI registry, the request is denied unless both of the following conditions are true:

- The TOE has identified the user and validated this identity

- The user is registered as a UDDI publisher

The following are the UDDI protected operations:

- update UDDI data
- return the set of UDDI entities owned by the user
- return information about UDDI publisher assertions
- transfer UDDI entities
- request and discard UDDI security tokens

2.3.3.8 Protection of Internal File Resources

When a remote caller issues a request a remote interface of the Application Server, Node Agent, and Deployment Manager for the purpose of exchanging files, the request is denied unless a user or group ID of the caller is mapped to one of the administration roles (Administrator, Configurator, Operator, and Monitor.)

2.3.4 Evaluated Security Management Functions

The evaluated security management functions are the functions that an administrator can use, during runtime of the certified system, to configure attributes that control the security of protected resources. These attributes are:

- Administration mapping attributes
- Naming mapping attributes
- Application mapping attributes
- Messaging mapping attributes
- Messaging flag attributes
- Register UDDI publisher attributes
- Application run-as mapping attributes

2.3.4.1 Administration Mapping Attributes

The administration mapping attributes are attributes that map user and group IDs to the administration roles. The administration roles are the roles used by the access control function of the administration service and are as follows:

- Administrator
- Configurator
- Operator
- Monitor

When the certified system is first installed and configured, no IDs are mapped to any of the administration roles. The user who installed and configured the system must use the evaluated scripting interfaces under the identity of the Application Server to configure a user ID to the Administrator role.

After the system is installed and configured, a user who is running under an ID that is mapped to the administration role of Administrator can use the evaluated scripting interfaces to change the configuration of the administration mapping attributes.

2.3.4.2 Naming Mapping Attributes

Naming mapping attributes are attributes that map user and group IDs to the roles used by the naming service. The following are the roles used by the naming service:

- CosNamingRead
- CosNamingWrite
- CosNamingCreate
- CosNamingDelete

When the certified system is first installed and configured, the special group ID of Everyone is mapped to the CosNamingRead role and the special group ID of AllAuthenticated is mapped to the CosNamingWrite, CosNamingCreate, and CosNamingDelete roles.

After the system is installed and configured, a user running under an ID that is mapped to the Administrator or Configurator administration role can use can use evaluated scripting interfaces to change the configuration of the naming mapping attributes.

2.3.4.3 Application Mapping Attributes

Application mapping attributes are attributes that map user and group IDs to the roles used by deployed applications (web server applications, enterprise beans, or both). When a developer creates an application to be deployed, the developer must define application roles for the application and configure these roles in the security constraint clauses or permission clauses for the application. The developer might also configure application mapping attributes for the application.

When an administrator deploys the application, the administrator has the option of specifying application mapping attributes for the application. If the administrator specifies the application mapping attributes, they override any attributes configured by the developer. Otherwise, the attributes that were configured by the developer are used or, if the developer did not configure these attributes, no application mapping attributes are used.

After an application is deployed, a user running under an ID that is mapped to the Administrator or Configurator administration role can use the evaluated scripting interfaces to configure or change the configuration of the application-mapping attributes.

2.3.4.4 Messaging Mapping Attributes

Messaging attributes are attributes that map user and group IDs to the roles used by messaging destinations. The roles used by messaging destinations are described in section 4.6 of this document.

The default is that no IDs are mapped to any of the roles used by messaging destinations. After the system is installed and configured, a user running under an ID that is mapped to the Administrator or Configurator administration role can use evaluated scripting interfaces to change the configuration of the messaging mapping attributes.

2.3.4.5 Messaging Flag Attributes

The following are the Messaging flag attributes:

- Inherit defaults flag for each new Messaging queue, topic space, or topic
- Topic space access check flag for each new Messaging topic space
- Inherit sender flag for new topics
- Inherit receiver flag for new topics

The default for each of these flag attributes is true.

A user running under an ID that is mapped to the Administrator or Configurator role optionally can change the value of any of these flag attributes.

2.3.4.6 Register UDDI Publishers Attributes

The UDDI publisher attributes are for registering users as UDDI publishers. The default is that no users are registered as UDDI publishers. A user running under an ID that is mapped to the Administrator or Operator role can use these attributes to register users as UDDI publishers.

2.3.4.7 Application Run-As Mapping Attributes

The developer of a web server application or enterprise bean optionally can configure a method in an application to run under a specified identity. If so, the developer of the application specifies a run-as role for the method. The developer optionally can also define a user ID and password that maps to the run-as role.

When an administrator deploys the application, the administrator has the option of specifying a user ID and password application that map to a run-as role. If the administrator specifies this, it overrides the mapping (if any) that was configured by the developer.

After an application is deployed, a user running under an ID that is mapped to the Administrator or Configurator administration role can use the evaluated scripting interfaces to configure or change the configuration of the user ID and password that map to a run-as role.

2.3.5 Evaluated Invocation of SSL Function

This function is applicable only the IBM HTTP Server provided with WebSphere Application Server, WebSphere Application Server, Express and WebSphere Application Server, Network Deployment. It ensures that the IBM HTTP Server will invoke SSL using the configured ciphers.

2.4 Organization Policies

An organization that implements the certified system is responsible for enforcing the following policies:

- Administrator policy
- Developer policy

2.4.1 Administrator Policy

The organization must enforce the following policy about the administrators who manage the system:

- Administrators must be trustworthy, diligent, and able to work according to the guidance provided by the system documentation.
- Administrators must adhere to the guidelines described in section 4 in this document titled "Administrator Guide for the Certified System".

2.4.2 Developer Policy

The organization must enforce the following policy about the developers who create applications that are deployed into the system:

- Developers must be trustworthy, diligent, and able to work according to the guidance provided by the system documentation.
- Developers must adhere to the guidelines and restrictions described in section 5 in this document titled "Developer’s Guide for the Certified System."

3 Installation and Configuration Guide for the Certified System

This section describes the procedure to use for installing and configuring the WebSphere Application Server components that are used in the certified system. The procedure described in this section replaces the procedure described elsewhere in the information center. Do not perform both procedures. Follow this procedure to set up a CC-compliant environment.

Attention: If you use any other procedure to install WebSphere Application Server, you change the compliant configuration that was evaluated. It is likely that by following another installation procedure, the system you install does not meet the evaluated configuration.

3.1 Modes of Operation

The purpose of the installation and configuration instructions in the following sections is to aid an authorized administrator to properly install and configure the WebSphere Application Server. As such, the TOE is always in a known mode.

3.2 Preparing for Installation and Configuration

Before doing the installation and configuration, note the following:

- Verify that you are using clean systems that do not have previous versions of WebSphere Application Server installed. You are not allowed to migrate a Version 3.5.x system, Version 4.x system or a Version 5.x system to version 6.0.2.3 as a basis for an evaluated configuration.
- It is recommended that you use easy installation programs, if supported for your particular platform. If easy installation is not supported, ensure that you follow native installation instructions and refer to the fix pack readme file for any last-minute updates.
- Refer to the following link for supported hardware:

  http://www-306.ibm.com/software/webservers/appserv/doc/v60/prereqs/hardware602.htm
- Refer to the following link for supported software:

  http://www-306.ibm.com/software/webservers/appserv/doc/v60/prereqs/prereq602.html

3.3 Installing the WebSphere Application Server Components

Use the following procedure to install WebSphere Application Server, Version 6.0.2.3 on a specific platform using the English language. Note that internet access and web browsers are required in order to download the product fix pack and product 6.0.2.3 update. You must install the product from the Administrator user ID or from a user ID that belongs to the Administrator user group and has the following advanced user rights:

- Acts as part of the operating system
- Logs on as a service

Note that instructions for UNIX® and Linux platforms include the following platforms unless otherwise specified:

- AIX 5.2 (64-bit);
- HP-UX 11i (64-bit PA-RISC);
- Linux Redhat 4 on PPC (64-bit) / Intel / z/OS
- Linux SuSE Enterprise Edition 9 (SLES 9) on PPC (64-bit) / z/OS;
- Sun Solaris 9 (64-bit)

3.3.1 Install WebSphere Application Server for z/OS

Use the documentation provided with ServerPac to install WebSphere Application Server for z/OS version 6.0.1 with service level 6.0.2.3. Then install the fix to APAR number AK17408.

Refer to the instructions in the WebSphere Application Server Information Center for "Installing your Application Server Environment" at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.zseries.doc/info/zseries/ae/welc6topinstalling.html

To verify that the installed version of WebSphere Application Server for z/OS is the evaluated version, take the following steps.

1. Change to the bin directory in the path where WebSphere Application Server is installed:

   cd <WAS_INSTALL_ROOT>\bin

2. Use the versionInfo.sh command to check the version:

   ./versionInfo.sh -maintenancePackageDetail

You should see the Installed product listed as "WebSphere Application Server for z/OS and version displayed as 6.0.2.3.

3. Verify that the fix to APAR number AK17408 is installed by taking the following steps:

- From a z/OS telnet session, start the deployment manager, for example:

```
/WebSphere/V6R0M0/DeploymentManager/profiles/default/bin/startManager.sh
```

- From a z/OS TSO session, go to the SDSF panel (option 13.14 on z/OS 1.6), type **da** to display the active jobs and type an **s** to the left of the job name for the deployment manager (can be control region or server region).
- On the option command line, type:

```
f BBOM0007I
```

- Verify that you see the following message:

```
BBOM0007I CURRENT CB SERVICE LEVEL IS build level AK17408 release
WAS602.ZNATV date 03/01/06 15:50:18.
```

3.3.2 Install WebSphere Application Server 6.0 (non-z/OS product)

To obtain the WebSphere Application Server 6.0 installation image, please refer to the Appendix A: How to Acquire WebSphere Application Server. Follow the instructions in sections 3.3.2 through 3.3.11 to install WebSphere Application Server 6.0 and its upgrades, and optional components.

Windows platform:

1. From a command window, do the following:

   mkdir C:\was_install

2. Extract the WebSphere Application Server 6.0 install image to C:\was_install.
3. **cd C:\was_install\WAS**
4. Using the default supplied response file (responsefile.<edition>.txt), create a new file called ccresponse.<edition>.txt in the current directory as shown below:

   For WebSphere Application Server Express:

   copy responsefile.express.txt ccresponse.express.txt

   For WebSphere Application Server:

   copy responsefile.base.txt ccresponse.base.txt

   For WebSphere Application Server Network Deployment:

copy responsefile.nd.txt ccresponse.nd.txt

The ccresponse.<edition>.txt is used to ensure that the WebSphere Application Server is installed in the evaluated configuration.

5. Modify the following values in the newly created ccresponse.<edition>.txt file. Make sure the lines modified are uncommented. Save the file after making all changes.

For WebSphere Application Server and WebSphere Application Express, change the following values:

a) –P wasProductBean.installLocation=<WAS_INSTALL_ROOT>
b) –P samplesProductFeatureBean.active=”false”
c) –W nodehostandcellnamepanelInstallWizardBean.nodeName=”YOUR_NODE_NAME”
d) –W setcellnameinglobalconstantsInstallWizardBean.value=”YOUR_CELL_NAME”
e) –W nodehostandcellnamepanelInstallWizardBean.hostName=”YOUR_HOST_NAME”
f) –W winservicepanelInstallWizardBean.winServiceQuery=”false”
g) –W winservicepanelInstallWizardBean.userName=”YOUR_USER_NAME”
h) –W winservicepanelInstallWizardBean.password=”YOUR_PASSWORD”

For WebSphere Application Server Network Deployment, change the following values:

a) –P wasProductBean.installLocation=<WAS_INSTALL_ROOT>
b) –P samplesProductFeatureBean.active=”false”
c) –W ndsummarypanelInstallWizardBean.launchPCT="false"

Substitute the path where WebSphere Application Server should be installed for <WAS_INSTALL_ROOT>. The location <WAS_INSTALL_ROOT> will be used in the subsequent instructions for installation and configuration. In the examples in this section and the sections which follow, C:\WebSphere\AppServer is used as the value for <WAS_INSTALL_ROOT>.

Substitute the name of your node for “*YOUR_NODE_NAME*” and the name of your cell for “*YOUR_CELL_NAME*”. These are unique names you choose.

Substitute the name of your computer for “*YOUR_HOST_NAME*”.

Substitute the name of the logged in Windows Administrative user for “*YOUR_USER_NAME*” and the Windows Administrative user’s password for “*YOUR_PASSWORD*”.

Example (WebSphere Application Server and WebSphere Application Server Express):

```
–P wasProductBean.installLocation=”C:\WebSphere\AppServer”
–P samplesProductFeatureBean.active=”false”
–W nodehostandcellnamepanelInstallWizardBean.nodeName=”mynode”
–W nodehostandcellnamepanelInstallWizardBean.hostName=”myhost”
–W setcellnameinglobalconstantsInstallWizardBean.value="mycell"
–W winservicepanelInstallWizardBean.winServiceQuery=”false”
–W winservicepanelInstallWizardBean.userName=”adminuser”
–W winservicepanelInstallWizardBean.password=”adminuserpwd”
```

Example (WebSphere Application Server Network Deployment):

```
–P wasProductBean.installLocation=”C:\WebSphere\AppServer”
–P samplesProductFeatureBean.active=”false”
–W ndsummarypanelInstallWizardBean.launchPCT="false"
```

6. Accept the License by setting the following value to true in the response file and remove the # from the beginning of the line if present. Save the file after making the modification:

   ```
   -W silentInstallLicenseAcceptance.value=”true”
   ```

7. Type the following commands to install Version 6.0.0.1:

   install -silent -options “C:/was_install/WAS/ccresponse.<edition>.txt”

   (The command will return immediately, but the installation will take about 5 to 30 minutes depending upon the speed of your machine. Verify that the installation has succeeded by entering the following command:

   cd <WAS_INSTALL_ROOT>\bin

   versionInfo.bat

   You should see the installed product version displayed as Version 6.0.0.1)

UNIX and Linux platforms:

1. From a command window, do the following:

   mkdir   /was_install

2. Extract the WebSphere Application Server installation image to /was_install.
3. Change to the image installation directory:

AIX:	**cd /was_install/WAS**
Linux:	**cd /was_install/WAS**
Solaris:	**cd /was_install/WAS**
HPUX:	**cd /was_install/WAS**

4. Using the default supplied response file (responsefile.<edition>.txt), create a new file called ccresponse.<edition>.txt in the current directory, as shown below:

   For WebSphere Application Server Express:

   cp responsefile.express.txt ccresponse.express.txt

   For WebSphere Application Server:

   cp responsefile.base.txt ccresponse.base.txt

   For WebSphere Application Server Network Deployment:

cp responsefile.nd.txt ccresponse.nd.txt

The ccresponse.<edition>.txt is used to ensure that the WebSphere Application Server is installed in the evaluated configuration.

5. Modify the following values in the newly created ccresponse.<edition>.txt file. Make sure the lines modified are uncommented. Save the file after making all changes:

For WebSphere Application Server and WebSphere Application Server Express, change the following values:

a) –P wasProductBean.installLocation=”<WAS_INSTALL_ROOT>”

b) –P samplesProductFeatureBean.active=”false”

c) –W nodehostandcellnamepanelInstallWizardBean.nodeName=”YOUR_NODE_NNAME”

d) –W setcellnameinglobalconstantsInstallWizardBean.value=”YOUR_CELL_NAME”
e) –W nodehostandcellnamepanelInstallWizardBean.hostName=”YOUR_HOST_NAME”

For WebSphere Application Server Network Deployment, change the following values:

a) –P wasProductBean.installLocation=<WAS_INSTALL_ROOT>
b) –P samplesProductFeatureBean.active=”false”
c) –W ndsummarypanelInstallWizardBean.launchPCT="false"

Substitute the path where WebSphere Application Server should be installed for <WAS_INSTALL_ROOT>. The location <WAS_INSTALL_ROOT> will be used in the subsequent instructions for installation and configuration. In the examples in this section and the sections which follow, /opt/WebSphere/AppServer is used as the value for <WAS_INSTALL_ROOT>.

Substitute the name of your node for “*YOUR_NODE_NAME*” and the name of your cell for “*YOUR_CELL_NAME*”. These are unique names you choose.

Substitute the name of your computer for “*YOUR_HOST_NAME*”.

Example (WebSphere Application Server and WebSphere Application Server Express):

```
–P wasProductBean.installLocation=”/opt/WebSphere/AppServer”

–P samplesProductFeatureBean.active=”false”

–W nodehostandcellnamepanelInstallWizardBean.nodeName=”mynode”

 –W setcellnameinglobalconstantsInstallWizardBean.value="mycell"
–W nodehostandcellnamepanelInstallWizardBean.hostName=”myhost”
```

Example (WebSphere Application Server Network Deployment):

```
–P wasProductBean.installLocation=”/opt/WebSphere/AppServer”
–P samplesProductFeatureBean.active=”false”
–W ndsummarypanelInstallWizardBean.launchPCT="false"
```

6. Accept the License by setting the following value to true in the response file and remove the # from the beginning of the line if present. Save the file after making the modification:

   -W silentInstallLicenseAcceptance.value="true"

7. Type the following commands to install Version 6.0.0.1:

   ./install -options "/was_install/WAS/ccresponse.<edition>.txt"

   -silent

   The command will return immediately, but the installation will take about 5 to 30 minutes depending upon the speed of your machine. Verify that the installation has succeeded by entering the following commands:

   cd <WAS_INSTALL_ROOT>/bin

   ./versionInfo.sh

   You should see the installed product version displayed as Version 6.0.0.1.

3.3.3 Install WebSphere Application Server Refresh Pack 2 (Required)

Windows platform:

1. Open a web browser and download WebSphere Application Server Refresh Pack 2 to upgrade to version 6.0.2:

- Open a web browser, and go to:
- http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24009813.
- Scroll down to the "Download Package" section
- Click on the "DD" link next to "Intel Application Server" to download the server fix pack. Note the file size.
- Click on the "I agree" button in the popup window to accept Download Terms and Conditions.
- Click on "Yes" to accept the IBM security certificate.
- For the download location, specify C:\temp
- If asked to create the directory click "Ok"
- If asked to configure proxy click "No" unless a proxy must be configured.
- Wait for the download to complete.
- After the download completes, press Details to display the file name and size. Verify the file size to ensure the correct file has been successfully downloaded.

2. Extract the Refresh Pack zip, 6.0-WS-WAS-Winx32-RP0000002.zip, to <WAS_INSTALL_ROOT>.

The package will automatically create an “updateinstaller” directory.

So if your <WAS_INSTALL_ROOT> was C:\WebSphere\Appserver, the extract will create C:\WebSphere\AppServer\updateinstaller.

3. Install Refresh Pack 2:

   cd C:\<WAS_INSTALL_ROOT>\bin

   setupCmdLine.bat

   cd C:\<WAS_INSTALL_ROOT>\updateinstaller\

   Issue the following commands to start the install. Each of these commands should be typed all on one line. Replace <WAS_INSTALL_ROOT> with the path you used for <WAS_INSTALL_ROOT> when installing WebSphere Application Server 6.0 (for example C:\WebSphere\AppServer). You may issue the update commands one after another.

   update.exe -silent -W relaunch.active=false -W maintenance.package=”<WAS_INSTALL_ROOT>\updateinstaller\maintenance\6.0-WS-WAS-WinX32-RP0000002.pak” -W update.type=”install” -W product.location=”<WAS_INSTALL_ROOT>”

   update.exe -silent -W maintenance.package=”<WAS_INSTALL_ROOT>\updateinstaller\maintenance\6.0-WS-WAS-WinX32-RP0000002.pak” -W update.type=”install” -W product.location=”<WAS_INSTALL_ROOT>”

   Example:

   update.exe -silent -W relaunch.active=false -W maintenance.package=”C:\WebSphere\AppServer\updateinstaller\maintenance\6.0-WS-WAS-WinX32-RP0000002.pak” -W update.type=”install” -W product.location=”C:\WebSphere\AppServer”

   update.exe -silent -W maintenance.package=”C:\WebSphere\AppServer\updateinstaller\maintenance\6.0-WS-WAS-WinX32-RP0000002.pak” -W update.type=”install” -W product.location=”C:\WebSphere\AppServer”

The command will return immediately, but the installation will take about 5 to 30 minutes depending upon the speed of your machine. After the installation has been verified, change to the root installation directory:

cd <WAS_INSTALL_ROOT>/bin

Enter the following command to display the version:

versionInfo

You should see the installed product version displayed as Version 6.0.2.0.

UNIX and Linux platforms:

1. Open a command prompt set WAS_HOME to <WAS_INSTALL_ROOT>:

   export WAS_HOME=<WAS_INSTALL_ROOT>
2. **cd $WAS_HOME**
3. Open a web browser, download and extract Refresh Pack 2 to $WAS_HOME:
   - For AIX, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010066
   - For HP-UX, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010067
   - For Linux, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010068
   - For Solaris, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010069

   - Scroll down to the "Download Package" section
   - Click on the "DD" link next to Application Server to download the server fix pack. Note the file size.
   - Click on the "I agree" button in the popup window to accept Download Terms and Conditions.
   - Click on "Yes" to accept the IBM security certificate.
   - For the download location, specify $WAS_HOME like the following:

     a) /usr/WebSphere/AppServer (AIX)

     b) /opt/WebSphere/AppServer (Linux, Solaris, HPUX)

   - If asked to create the directory, click "Ok".
   - If asked to configure proxy click "No" unless a proxy must be configured.
   - After the download completes, press Details to display the file name and size. Verify the file size to ensure the correct file has been successfully downloaded.
   - Extract the Refresh pack:

     cd $WAS_HOME
     tar -xvf 6.0-WS-WAS-<*platform*>-RP0000002.tar

4. Set JAVA_HOME to the location of the WebSphere Application Server Java™ installation by typing:

   ```
   export JAVA_HOME=$WAS_HOME/java
   ```

5. Install Refresh Pack 2 by following the instructions below. The update commands may be issued one after another.

   ```
   cd $WAS_HOME/bin
   ```

   ```
   . ./setupCmdLine.sh
   ```

   ```
   cd $WAS_HOME/updateinstaller
   ```

   ```
   ./update -silent -W relaunch.active=false -W
   maintenance.package=”$WAS_HOME/updateinstaller/maintenance/6.0-
   WS-WAS-<platform>-RP0000002.pak” -W update.type=”install” -W
   product.location=”$WAS_HOME”
   ```

   ```
   ./update -silent -W
   maintenance.package=”$WAS_HOME/updateinstaller/maintenance/6.0-
   WS-WAS-<platform>-RP0000002.pak” -W update.type=”install” -W
   product.location=”$WAS_HOME”
   ```

   Example:

   ```
   ./update -silent -W relaunch.active=false -W
   maintenance.package=”/opt/WebSphere/AppServer/updateinstaller/maintenanc
   e/6.0-WS-WAS-LinuxX32-RP0000002.pak” -W update.type=”install” -W
   product.location=”/opt/WebSphere/AppServer”
   ```

   ```
   ./update -silent -W
   maintenance.package=”/opt/WebSphere/AppServer/updateinstaller/maintenanc
   e/6.0-WS-WAS-LinuxX32-RP0000002.pak” -W update.type=”install” -W
   product.location=”/opt/WebSphere/AppServer”
   ```

   For AIX, specify /usr, not /opt, for the locations above. Additionally, the filename of the fix pack is also specific to platform (e.g. LinuxX32).

   When the fix pack installation is complete, you will be returned to the command prompt.

   The command will return immediately, but the installation will take about 5 to 30 minutes depending upon the speed of your machine. After the command returns to the command prompt,

cd $WAS_HOME/bin

Type the following command to display the version:

./versionInfo.sh.

You should see the installed product version displayed as Version 6.0.2.0.

6. Delete the $WAS_HOME/updateinstaller directory

   cd $WAS_HOME

   rm -r -f updateinstaller

3.3.4 Install WebSphere Application Server 6.0.2 Fix Pack 3 (Required)

Windows platform:

1. Open a web browser, download the WebSphere Application Server Fix Pack 3 update package to update to version 6.0.2.3:
   - Open a web browser, and go to: http://www-1.ibm.com/support/docview.wss?uid=swg24010724
   - Scroll down to the "Download Package" section , and click on the "DD" link for the "Intel Application Server" to begin downloading the update package, saving it to the C:\temp directory. Note the file size.
   - Click on the "I agree" button in the popup window to accept Download Terms and Conditions.
   - Click "Yes" to accept the IBM security certificate.
   - For the download location, specify C:\temp
   - If asked to create the directory click "Ok"
   - If asked to configure proxy click "No" unless a proxy must be configured.
   - After the download completes, press Details to display the file name and size. Verify the file size to ensure the correct file has been successfully downloaded.

2. Extract the Fix Pack 3 zip file, 6.0.2-WS-WAS-WinX32-FP0000003.zip, to your <WAS_INSTALL_ROOT> directory.

   The package will automatically update the "updateinstaller" directory. If you are prompted that a file already exists and asked if you want to replace it, answer "Yes to all".

   If your <WAS_INSTALL_ROOT> was C:\WebSphere\Appserver, the extract will update C:\WebSphere\AppServer\updateinstaller

3. Install Fix Pack 3:

   cd C:\<WAS_INSTALL_ROOT>\bin

   setupCmdline.bat

   cd C:\<WAS_INSTALL_ROOT>\updateinstaller\

   Issue the following command to start the install. Replace <WAS_INSTALL_ROOT> with the path where you installed WebSphere Application Server, such as "C:\WebSphere\AppServer".

   update.exe -silent -W maintenance.package="<WAS_INSTALL_ROOT\updateinstaller\maintenance\6.0.2-WS-WAS-WinX32-FP0000003.pak" -W update.type="install" -W product.location="<WAS_INSTALL_ROOT>"

   Example:

   update.exe -silent -W maintenance.package="C:\WebSphere\AppServer\updateinstaller\maintenance\6.0.2-WS-WAS-WinX32-FP0000003.pak" -W update.type="install" -W product.location="C:/WebSphere/AppServer"

   The command will return immediately, but the installation will take about 5 to 30 minutes depending upon the speed of your machine. After the installation has completed, change to the bin directory:

   cd <WAS_INSTALL_ROOT>\bin

   Enter the following command to display the version:

   versionInfo

   You should see the installed product version displayed as Version 6.0.2.3.

UNIX and Linux platforms:

1. Open a command window and set WAS_HOME to <WAS_INSTALL_ROOT>.

   export $WAS_HOME=<WAS_INSTALL_ROOT>

2. **cd $WAS_HOME**

3. Open a web browser, download and unzip the 6.0.2.3 update package:

   - For AIX, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010719
   - For HP-UX, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010721

- For Linux, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010722
- For Solaris, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010723
- . The file may be downloaded using a Windows Internet Explorer browser and then transferred to the Unix machine.
- Scroll down to the “Download Package” section , and click on the “DD” link for the Application Server to begin downloading the update package, saving it to the $WAS_HOME directory. Note the file size.
- Click on the “I agree” button in the popup window to accept Download Terms and Conditions.
- Click on “Yes” to accept the IBM security certificate.
- For the download location, specify $WAS_HOME like the following:
  a. /usr/WebSphere/AppServer (AIX)
  b. /opt/WebSphere/AppServer (Linux, Solaris, HPUX)
- If asked to create the directory, click “Ok”.
- If asked to configure proxy click “No” unless a proxy must be configured.
- After the download completes, press Details to display the file name and size. Verify the file size to ensure the correct file has been successfully downloaded.

4. Transfer the file (if required) then extract the file into the $WAS_HOME directory. This will automatically create a $WAS_HOME/updateinstaller directory.

   cd $WAS_HOME

   tar -xvf 6.0.2-WS-WAS-<*platform*>-FP0000003.tar

4. Install Fix Pack 3:

   cd $WAS_HOME/updateinstaller

   ./update -silent -W maintenance.package=”$WAS_HOME/updateinstaller/maintenance/6.0.2-WS-WAS-<platform>-FP0000003.pak” -W update.type=”install” -W product.location=”$WAS_HOME”

   Example:

   ./update -silent -W maintenance.package=”/opt/WebSphere/AppServer/updateinstaller/maintenance/6.0.2-WS-WAS-LinuxX32-FP0000003.pak” -W update.type=”install” -W product.location=”/opt/WebSphere/AppServer”

   For AIX, specify /usr, not /opt for the locations above. Additionally, the filename of the service pack is also specific to platform (e.g. LinuxX32).

When the service pack installation is complete, you will be returned to the command prompt.

The command will return immediately, but the installation will take about 5 to 30 minutes depending upon the speed of your machine. After the command returns to the command prompt:

cd $WAS_HOME/bin

Type the following command to display the product version.

./versionInfo.sh.

You should see the installed product version displayed as Version 6.0.2.3.

5. Delete the $WAS_HOME/updateinstaller directory

   cd $WAS_HOME

   rm -r -f updateinstaller

3.3.5 Install IBM HTTP Server 6.0 (Optional)

Windows platform:

1. Change to the directory where the WebSphere Application Server 6.0 IBM HTTP Server install image is located:

   cd C:\was_install\IHS

2. Copy the supplied default response file, responsefile.txt, to a new file "ccihsresponsefile.txt".
3. Modify the following values in the response file, "ccihsresponsefile.txt" as shown below. Make sure the lines modified are uncommented.

   Substitute the name of the logged in Windows Administrative user for "YOUR_USER_NAME" and the administrative password for "YOUR_PASSWORD". For "-P ihs.installLocation", substitute the path where you want to install the IBM HTTP Server, such as "C:\IBMHTTPServer". (We recommend that you not include spaces in the path name.) In subsequent install instructions, we will refer to this location as <IHS_INSTALL_ROOT>.

   a) -W silentInstallLicenseAcceptance.value="true"
   b) -P ihs.installLocation="C:\IBMHTTPServer"
   c) -W WinServicePanel.user="YOUR_USER_NAME"
   d) -W WinServicePanel.password="YOUR_PASSWORD"

4. Save changes to the "ccihsresponsefile.txt".

5. Type the following command to install IBM HTTP Server Version 6.0.0:

```
Install.exe -silent -options ccihsresponsefile.txt
```

The command will return immediately, but the installation will take about 5 to 30 minutes depending upon the speed of your machine.

When the installation has completed, change to the directory you specified as the IBM HTTP Server installation location <IHS_INSTALL_ROOT> (e.g. C:\IBMHTTPServer). Then change to the bin directory and issue the following command to verify the version.

```
cd <IHS_INSTALL_ROOT>\bin
apache.exe -V
```

The version of the IBM HTTP Server should display as:

Server version: IBM_HTTP_SERVER/6.0 Apache/2.0.47.

UNIX and Linux platforms:

1. Change to the installation directory:

```
cd   /was_install/IHS
```

2. Copy the supplied default response file, responsefile.txt, to a new file “ccihsresponsefile.txt”.
3. Modify the following values in the response file, “ccihsresponsefile.txt” as shown below. Make sure the lines modified are uncommented.

   For “-P ihs.installLocation”, substitute the path where you want to install the IBM HTTP Server, such as “/opt/IBMHTTPServer”. (We recommend that you not include spaces in the path name.) In subsequent install instructions, we will refer to this location as <IHS_INSTALL_ROOT>.

   a) -W silentInstallLicenseAcceptance.value="true"
   b) -P ihs.installLocation="/opt/IBMHTTPServer”

4. Save changes to the “ccihsresponsefile.txt”.
5. Type the following command to install IBM HTTP Server Version 6.0.0:

```
./install -silent -options ccihsresponsefile.txt
```

The command will return immediately, but the installation will take about 5 to 30 minutes depending upon the speed of your machine.

When the installation has completed, change to the directory you specified as the IBM HTTP Server installation location <IHS_INSTALL_ROOT> (e.g. /opt/IBMHTTPServer). Then change to the bin directory and issue the following command to verify the version.

```
cd <IHS_INSTALL_ROOT>/bin
./apachectl -V 4
```

The version of the IBM HTTP Server should display as:

Server version: IBM_HTTP_SERVER/6.0 Apache/2.0.47.

3.3.6 Install IBM HTTP Server Plug-in 6.0 (Optional)

Windows platform:

1. For WebSphere Application Server and WebSphere Application Server Express, create a plug-in configuration file. Do not perform this step for WebSphere Application Server Network Deployment.
   - Change to <WAS_INSTALL_ROOT>\bin and create a plugin configuration file.

     cd <WAS_INSTALL_ROOT>\bin
   - Type the following command to create a plug-in configuration file:

     GenPluginCfg.bat

     You will see a message that a plug-in configuration file is being generated followed by, “PLGC0005I: Plug-in configuration file=<WAS_INSTALL_ROOT>/profiles/default/config/cells/plugin-cfg.xml”
2. Change to the directory where the WebSphere Application Server 6.0 install image is located:

   cd C:\was_install
3. Change to the directory where the IBM HTTP Server Plug-in install image is located:

   cd plugin
4. Copy the supplied default response file, responsefile.txt, to a new file, “ccpluginresponse.txt”. Modify the values as shown below. Make sure the lines modified are uncommented.

   For the “pluginProductBeaninstallLocation”, you should substitute the location where you want the plugin installed. In subsequent install instructions, this will be referenced as <PLUGIN_INSTALL_ROOT>. For the “websphereLocationWizardBean.wasExistingLocation, substitute your

<WAS_INSTALL_ROOT>. For “pluginSettings.webServerConfigFile1”, substitute the location of the IBM HTTP Server config file, httpd.conf.

a) -W silentInstallLicenseAcceptance.value="true"
b) -P pluginProductBean.installLocation=”<PLUGIN_INSTALL_ROOT>”
c) -W websphereLocationWizardBean.wasExistingLocation="<WAS_INSTALL_ROOT>”
d) -P pluginSettings.webServerSelected="ihs"
e) -P pluginSettings.webServerConfigFile1="<IHS_INSTALL_ROOT>\conf\httpd.conf"
f) -P pluginSettings.webServerDefinition="null"

Example:

```
-W silentInstallLicenseAcceptance.value="true"
-P pluginProductBean.installLocation="C:\WebSphere\plugin”
-W websphereLocationWizardBean.wasExistingLocation="C:\WebSphere\AppServer”
-P pluginSettings.webServerSelected="ihs"
-P pluginSettings.webServerConfigFile1="C:\IBMHTTPServer\conf\httpd.conf"
-P pluginSettings.webServerDefinition="null"
```

5. Save changes to “ccpluginresponse.txt”.
6. Type the following command to install IBM HTTP Server plugins Version 6.0.0:

   install -silent -options ccpluginresponse.txt

When the installation has completed, change to the directory you specified as the “pluginProductBean.installLocation” (from the example install command above, this is C:\WebSphere\plugin) and then change to the bin directory and issue the following command to verify the version.

versionInfo.bat

The version of the IBM HTTP Server should display as:

Name: Web server plug-ins for IBM WebSphere Application Server

Version: 6.0.0.1

UNIX and Linux platforms:

1. For WebSphere Application Server and WebSphere Application Server Express, create a plug-in configuration file. Do not perform this step for WebSphere Application Server Network Deployment.
   - Change to $WAS_HOME/bin and create a plugin configuration file.

     cd $WAS_HOME/bin
   - Type the following command to create a plug-in configuration file.

./GenPluginCfg.sh

You will see a message that a plug-in configuration file is being generated followed by, “PLGC0005I: Plug-in configuration file=<WAS_INSTALL_ROOT>/profiles/default/config/cells/plugin-cfg.xml”

2. Change to the installation directory:

   cd /was_install/plugin

3. Copy the supplied default response file, responsefile.txt, to a new file, “ccpluginresponse.txt”. Modify the values as shown below. Make sure the lines modified are uncommented.

   For the “pluginProductBeaninstallLocation”, you should substitute the location where you want the plugin installed. In subsequent install instructions, this will be referenced as <PLUGIN_INSTALL_ROOT>. For the “websphereLocationWizardBean.wasExistingLocation, substitute your <WAS_INSTALL_ROOT>. For “pluginSettings.webServerConfigFile1”, substitute the location of the IBM HTTP Server config file, httpd.conf.

   a) -W silentInstallLicenseAcceptance.value="true"
   b) -P pluginProductBean.installLocation=”<PLUGIN_INSTALL_ROOT>”
   c) -W websphereLocationWizardBean.wasExistingLocation="<WAS_INSTALL_ROOT>”

   d) -P pluginSettings.webServerSelected="ihs"
   e) -P pluginSettings.webServerConfigFile1="<IHS_INSTALL_ROOT>\conf\httpd.conf"
   f) -P pluginSettings.webServerDefinition="null"

Example:

```
-W silentInstallLicenseAcceptance.value="true"
-P pluginProductBean.installLocation="/opt/WebSphere/plugin”
-W websphereLocationWizardBean.wasExistingLocation="/opt/WebSphere/AppServer”
-P pluginSettings.webServerSelected="ihs"
-P pluginSettings.webServerConfigFile1="/opt/IBMHTTPServer/conf/httpd.conf"
-P pluginSettings.webServerDefinition="null"
```

7. Save changes to “ccpluginresponse.txt”.

8. Type the following command to install IBM HTTP Server plugins Version 6.0.0:

   ./install -silent -options ccpluginresponse.txt

When the installation has completed, change to the directory you specified as the “pluginProductBean.installLocation” (from the example install command above, this is /opt/WebSphere/plugin) and then change to the bin directory and issue the following command to verify the version.

./versionInfo.sh

The version of the IBM HTTP Server should display as:

Name: Web server plug-ins for IBM WebSphere Application Server

Version: 6.0.0.1

3.3.7 Install IBM HTTP Server Refresh Pack 2 (Required if IBM HTTP Server is installed)

Windows platform:

1. Open a web browser, download the IBM HTTP Server Refresh Pack 2 to upgrade to version 6.0.2:
   - Open a web browser, and go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24009813
   - Scroll down to the “Download Package” section
   - Click on the “DD” link next to ”Intel IBM HTTP Server” to download the server refresh pack.   Note the file size.
   - Click on the “I agree” button in the popup window to accept Download Terms and Conditions.
   - Click on “Yes” to accept the IBM security certificate.
   - For the download location, specify C:\temp
   - If asked to create the directory, click “Ok”.
   - If asked to configure proxy click “No” unless a proxy must be configured.
   - Wait for the download to complete.
   - After the download completes, press Details to display the file name and size. Verify the file size to ensure the correct file has been successfully downloaded.
2. Extract the IBM HTTP Server Refresh Pack, 6.0-WS-WASIHS-WinX32-RP0000002.zip, to the location where you installed the IBM HTTP Server - <IHS_INSTALL_ROOT>. If you are prompted that a file already exists and asked if you want to replace it, answer "Yes to all". The extract will automatically create an “updateinstaller” directory.
3. Install the IBM HTTP Server Refresh Pack 2:

   Change directory to “updateinstaller” directory for the IBM HTTP Server update.

   cd C:\<IHS_INSTALL_ROOT>\updateinstaller

   Use the update command to install the refresh pack as shown below. For <IHS_INSTALL_ROOT>, substitute the location where you installed the IBM

HTTP Server. For “maintenance.package”, substitute the location of the IBM HTTP Server Refresh Pack 2 which you extracted.

update.exe -silent -W product.location=”<IHS_INSTALL_ROOT>” -W maintenance.package=”<IHS_INSTALL_ROOT>/updateinstaller/maintenance/6.0-WS-WASIHS-WinX32-RP0000002.pak” -W update.type=”install”

Example:

update.exe -silent -W product.location=”C:/IBMHTTPServer” -W maintenance.package=”C:/IBMHTTPServer/updateinstaller/maintenance/6.0-WS-WASIHS-WinX32-RP0000002.pak” -W update.type=”install”

This installation will take about 5 minutes. To verify the version of the HTTP Server installed, change to the bin directory under the directory where you installed the IBM HTTP Server:

cd <IHS_INSTALL_ROOT>\bin

Type the following command to display the version:

apache.exe -V

The version should display as:

Server version: IBM_HTTP_SERVER/6.0.2 Apache/2.0.47

UNIX and Linux platforms:

1. Open a command prompt and set $IHS_HOME to the root directory where the IBM HTTP Server was installed (IHS_INSTALL_ROOT).
2. **cd $IHS_HOME**
3. Open a web browser, download and extract Refresh Pack 2:
   - For AIX, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010066
   - For HP-UX, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010067
   - For Linux, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010068
   - For Solaris, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010069.

- Scroll down to the “Download Package” section
- Click on the “DD” link next to ”IBM HTTP Server” to download the server fix pack. Note the file size.

- Click on the “I agree” button in the popup window to accept Download Terms and Conditions.
- Click on “Yes” to accept the IBM security certificate.
- For the download location, specify $IHS_HOME like the following:
  a) /usr/IBMHTTPServer (AIX)
  b) /opt/IBMHTTPServer (Linux, Solaris, HPUX)
- If asked to create the directory, click “Ok”.
- If asked to configure proxy click “No” unless a proxy must be configured.
- Wait for the download to complete.
- After the download completes, press Details to display the file name and size. Verify the file size to ensure the correct file has been successfully downloaded.

4. Extract the IBM HTTP Server Refresh Pack to the location where you installed the IBM HTTP Server -<IHS_INSTALL_ROOT>. The extract will automatically create an “updateinstaller” directory.

   cd $IHS_HOME
   tar -xvf 6.0-WS-WASIHS-<*platform*>-RP0000002.tar

   This automatically creates the $IHS_HOME/updateinstaller directory.

5. Install the IBM HTTP Server Refresh Pack 2

cd $IHS_HOME/updateinstaller

./update -silent -W product.location=”<IHS_INSTALL_ROOT>” -W maintenance.package=”<IHS_INSTALL_ROOT>/updateinstaller/maintenance/6.0-WS-WASIHS-<platform>-RP0000002.pak” -W update.type=”install”

Example:

./update -silent -W product.location=”/opt/IBMHTTPServer” -W maintenance.package=”/opt/IBMHTTPServer/updateinstaller/maintenance/6.0-WS-WASIHS-LinuxX32-RP0000002.pak” -W update.type=”install”

For AIX, specify /usr, not /opt for the locations above. Additionally, the filename of the fix pack is also specific to platform (e.g. LinuxX32).

The command will return immediately, but the installation will take about 5 to 30 minutes depending upon the speed of your machine. After the command returns to the command prompt, perform the following procedures to verify the version.

To verify the version of the HTTP Server installed, change to the bin directory under the directory where you installed the IBM HTTP Server:

cd <IHS_INSTALL_ROOT/bin

Type the following command to display the version:

```
./apachectl -V 4
```

The version should display as:

Server version: IBM_HTTP_SERVER/6.0.2 Apache/2.0.47

5. Once the execution of the fix pack has been determined to be successful, delete the $IHS_HOME/updateinstaller directory

```
cd $IHS_HOME
rm -r -f updateinstaller
```

3.3.8 Install IBM HTTP Server Plug-ins Refresh Pack 2 (Required if you installed the IBM HTTP Server Plug-in)

Windows platform:

1. Open a web browser, download and extract the IBM HTTP Server Plug-ins Refresh Pack 2 to upgrade to version 6.0.2:
   - Open a web browser, and go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24009813
   - Scroll down to the “Download Package” section
   - Click on the “DD” link next “Intel Plug-ins” to download the server fix pack. Note the file size.
   - Click on “Yes” to accept the IBM security certificate.
   - For the download location, specify C:\temp.
   - If asked to create the directory, click “Ok”.
   - If asked to configure proxy click “No” unless a proxy must be configured.
   - Wait until the download is complete.
   - After the download completes, press Details to display the file name and size. Verify the file size to ensure the correct file has been successfully downloaded.

2. Extract the Refresh Pack 2 zip file, 6.0-WS-WASPlugIn-WinX32-RP0000002.zip”, to the directory where you installed the IBM HTTP Server Plug-in (<PLUGIN_INSTALL_ROOT>).

   The extract will automatically create an “updateinstaller” directory in this location.

3. Install IBM HTTP Server Plug-ins Refresh Pack 2.

Change to the updateinstaller directory for the plugin:

```
cd <PLUGIN_INSTALL_ROOT>\updateinstaller
```

Example: cd C:\WebSphere\plugin\updateinstaller

Use the update commands to install the refresh pack as shown below. For <PLUGIN_INSTALL_ROOT>, substitute the location where you installed the IBM HTTP Server Plug-in. For “maintenance.package”, substitute the location of the IBM HTTP Server Plug-in Refresh Pack 2 which you extracted. You may issue the update commands one after the other.

```
update.exe -silent -W relaunch.active=false -W product.location=”<PLUGIN_INSTALL_ROOT>” -W maintenance.package=”<PLUGIN_INSTALL_ROOT>/updateinstaller/maintenance/6.0-WS-WASPlugIn-WinX32-RP0000002.pak” -W update.type=”install”
```

```
update.exe -silent -W product.location=”<PLUGIN_INSTALL_ROOT>” -W maintenance.package=”<PLUGIN_INSTALL_ROOT>/updateinstaller/maintenance/6.0-WS-WASPlugIn-WinX32-RP0000002.pak” -W update.type=”install”
```

Example:

```
update.exe -silent -W relaunch.active=false -W product.location=”C:/WebSphere/plugin” -W maintenance.package=”C:/WebSphere/plugin/updateinstaller/maintenance/6.0-WS-WASPlugIn-WinX32-RP0000002.pak” -W update.type=”install”
```

```
update.exe -silent -W product.location=”C:/WebSphere/plugin” -W maintenance.package=”C:/WebSphere/plugin/updateinstaller/maintenance/6.0-WS-WASPlugIn-WinX32-RP0000002.pak” -W update.type=”install
```

The command will return immediately, but the installation will take about 5 to 30 minutes depending upon the speed of your machine. To verify the version of the HTTP Server Plug-in installed, change to the bin directory under the directory where you installed the IBM HTTP Server Plug-in.

```
cd <PLUGIN_INSTALL_ROOT>\bin
```

Type the following command to display the version:

```
versionInfo.bat
```

The version should display as:

```
Name: Web server plug-ins for IBM WebSphere Application Server
Version: 6.0.2.0
```

UNIX and Linux platforms:

1. Set $PLUGIN_HOME to the value of <PLUGIN_INSTALL_ROOT>.
2. Open a web browser, download and extract the IBM HTTP Server Plug-ins Refresh Pack 2:

- For AIX, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010066
- For HP-UX, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010067
- For Linux, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010068
- For Solaris, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010069
- Scroll down to the “Download Package” section
- Click on the “DD” link next “Plug-ins” to download the server fix pack. Note the file size.
- Click on the “I agree” button in the popup window to accept Download Terms and Conditions.
- Click on “Yes” to accept the IBM security certificate.
- For the download location, specify $PLUGIN_HOME like the following:
  a) /usr/WebSphere/plugin (AIX)
  b) /opt/WebSphere/plugin (Linux, Solaris, HPUX)

- If asked to create the directory, click “Ok”.
- If asked to configure proxy click “No” unless a proxy must be configured.
- Wait until the download is complete.
- After the download completes, press Details to display the file name and size. Verify the file size to ensure the correct file has been successfully downloaded.

- After download is complete:
  cd $PLUGIN_HOME
  tar -xvf 6.0-WS-WASPlugIn-<*platform*>-RP0000002.tar

3. Install Refresh Pack 2 by following the instructions below. You may issue the update commands one after another.

cd $PLUGIN_HOME/updateinstaller

./update -silent -W relaunch.active=false -W product.location=”$PLUGIN_HOME” -W maintenance.package=”$PLUGIN_HOME/updateinstaller/maintenance/6.0-WS-WASPlugIn-<platform>-RP0000002.pak” -W update.type=”install”

./update –silent –W product.location=”$PLUGIN_HOME” -W maintenance.package=”$PLUGIN_HOME/updateinstaller/maintenance/6.0-WS-WASPlugIn-<platform>-RP0000002.pak” -W update.type=”install”

Example:

```
./update -silent -W relaunch.active=false -W
product.location=”/opt/WebSphere/plugin” -W
maintenance.package=”/opt/WebSphere/plugin/updateinstaller/maintenance/6.
0-WS-WASPlugIn-LinuxX32-RP0000002.pak” -W update.type=”install”
```

```
./update -silent -W product.location=”/opt/WebSphere/plugin” -W
maintenance.package=”/opt/WebSphere/plugin/updateinstaller/maintenance/6.
0-WS-WASPlugIn-LinuxX32-RP0000002.pak” -W update.type=”install”
```

For AIX, specify /usr, not /opt for the locations above. Additionally, the filename of the fix pack is also specific to platform (e.g. LinuxX32).

The command will return immediately, but the installation will take about 5 to 30 minutes depending upon the speed of your machine. After the command returns to the command prompt, perform the following procedures:

To verify the version of the HTTP Server Plug-in installed, change to the bin directory under the directory where you installed the IBM HTTP Server Plug-in.

cd $PLUGIN_HOME/bin

Type the following command to display the version:

./versionInfo.sh

The version should display as:

Name: Web server plug-ins for IBM WebSphere Application Server

Version: 6.0.2.0

4. Once the execution of the fix pack has been determined to be successful, delete the $PLUGIN_HOME/updateinstaller directory.

    cd $PLUGIN_HOME

    rm -r -f updateinstaller

3.3.9 Install IBM HTTP Server 6.0.2 Fix Pack 3 (Required if IBM HTTP Server is installed)

Windows platform:

1. Open a web browser and download IBM HTTP Server, Fix Pack 3 to upgrade to version 6.0.2.3.

   - Open a web browser and go to: http://www-1.ibm.com/support/docview.wss?uid=swg24010724
   - Scroll down to the "Download Package" section
   - Click on the "DD" link next to "Intel IBM HTTP Server" to download the server fix pack. Note the file size.
   - Click on the "I agree" button in the popup window to accept Download Terms and Conditions.
   - Click on "Yes" to accept the IBM security certificate.
   - For the download location, specify C:\temp:
   - If asked to create the directory, click "Ok".
   - If asked to configure proxy click "No" unless a proxy must be configured.
   - After the download completes, press Details to display the file name and size. Verify the file size to ensure the correct file has been successfully downloaded.

2. Extract the Fix Pack 3 zip file, 6.0.2-WS-WASIHS-WinX32-FP0000003.zip, to the location where you installed the IBM HTTP Server (<IHS_INSTALL_ROOT>). If you are prompted that a file already exists and asked if you want to replace it, answer "Yes to all".

   The extract will update the "updateinstaller" directory for the IBM HTTP Server. If IBM HTTP Server is installed in C:\IBMHTTPServer, the C:\IBMHTTPServer\updateinstaller directory will be updated with the new fix pack to be installed.

3. Install the IBM HTTP Server Fix Pack 3.

Change to the IBM HTTP Server "updateinstaller" directory.

cd <IHS_INSTALL_ROOT>\updateinstaller

Use the update command to install the fix pack as shown below. For <IHS_INSTALL_ROOT>", substitute the location where you installed the IBM HTTP Server. For "maintenance.package", substitute the location of the IBM HTTP Server Refresh Pack 2 which you extracted.

update.exe -silent -W product.location="<IHS_INSTALL_ROOT>" -W maintenance.package="<IHS_INSTALL_ROOT>/updateinstaller/maintenance/6.0.2-WS-WASIHS-WinX32-FP0000003.pak" -W update.type="install"

Example:

update.exe -silent -W product.location=”C:/IBMHTTPServer” -W maintenance.package=”C:/IBMHTTPServer/updateinstaller/maintenance/6.0.2-WS-WASIHS-WinX32-FP0000003.pak” -W update.type=”install”

The command will return immediately, but the installation will take about 5 to 30 minutes depending upon the speed of your machine. To verify the version of the HTTP Server installed, change to the bin directory under the directory where you installed the IBM HTTP Server :

cd <IHS_INSTALL_ROOT>\bin

Type the following command to display the version:

apache.exe -V

The version should display as:

Server version: IBM_HTTP_SERVER/6.0.2.3 Apache/2.0.47

UNIX and Linux platforms:

1. Open a command prompt and set $IHS_HOME to <IHS_INSTALL_ROOT>.
2. **cd $IHS_HOME**
3. Open a web browser, download and extract Fix Pack 3:
   - For AIX, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010719
   - For HP-UX, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010721
   - For Linux, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010722

- For Solaris, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010723.
- Scroll down to the “Download Package” section
- Click on the “DD” link next to ”IBM HTTP Server” to download the server fix pack. Note the file size.
- Click on the “I agree” button in the popup window to accept Download Terms and Conditions.
- Click on “Yes” to accept the IBM security certificate.
- For the download location, specify $IHS_HOME like the following:

a)	/usr/IBMHTTPServer	(AIX)
b)	/opt/IBMHTTPServer	(Linux, Solaris, HPUX)

  - If asked to create the directory, click “Ok”.
  - If asked to configure proxy click “No” unless a proxy must be configured.

- After the download completes, press Details to display the file name and size. Verify the file size to ensure the correct file has been successfully downloaded.
- Extract the fix pack:

cd $IHS_HOME
tar -xvf 6.0.2-WS-WASIHS-<*platform*>-FP0000003.tar

4. Install Fix Pack 3

cd $IHS_HOME/updateinstaller

./update -silent -W product.location="$IHS_HOME" -W maintenance.package="$IHS_HOME/updateinstaller/maintenance/6.0.2-WS-WASIHS-<platform>-FP0000003.pak" -W update.type="install"

Example:

./update -silent -W product.location="/opt/IBMHTTPServer" -W maintenance.package="/opt/IBMHTTPServer/updateinstaller/maintenance/6.0.2-WS-WASIHS-LinuxX32-FP0000003.pak" -W update.type="install"

For AIX, specify /usr, not /opt for the locations above. Additionally, the filename of the fix pack is also specific to platform (e.g. LinuxX32).

.

The command will return immediately, but the installation will take about 5 to 30 minutes depending upon the speed of your machine. After the command returns to the command prompt, perform the following procedures.

To verify the version of the HTTP Server installed, change to the bin directory under the directory where you installed the IBM HTTP Server :

cd $IHS_HOME/bin

Type the following command to display the version:

./apachectl -V 4

The version should display as:

Server version: IBM_HTTP_SERVER/6.0.2.3 Apache/2.0.47

5. Once the execution of the fix pack has been determined to be successful, delete the $IHS_HOME/updateinstaller directory

cd $IHS_HOME

rm -r -f updateinstaller

3.3.10 Install IBM HTTP Server Plug-in 6.0.2 Fix Pack 3 (Required if the IBM HTTP Server Plug-in is installed)

Windows platform:

1. Open a web browser and download the IBM HTTP Server Plug-in Fix Pack 3 to upgrade to version 6.0.2.3.
   - Open a web browser, and go to:

     http://www-1.ibm.com/support/docview.wss?uid=swg24010724
   - Scroll down to the "Download Package" section
   - Click on the "DD" link next "Intel Plug-ins" to download the server fix pack. Note the file size.
   - Click on the "I agree" button in the popup window to accept Download Terms and Conditions.
   - Click on "Yes" to accept the IBM security certificate.
   - For the download location, specify C:\temp.
   - If asked to create the directory, click "Ok".
   - If asked to configure proxy click "No" unless a proxy must be configured.
   - After the download completes, press Details to display the file name and size. Verify the file size to ensure the correct file has been successfully downloaded.
2. Extract the IBM HTTP Server Plug-ins Fix Pack 3 zip file, 6.0.2-WS-WASPlugIn-WinX32-FP0000003.zip", to the directory where you installed the IBM HTTP Server Plug-in (<PLUGIN_INSTALL_ROOT>). If you are prompted that a file already exists and asked if you want to replace it, answer "Yes to all".

   This will replace the IBM HTTP Server Plug-in "updateinstaller" directory with the latest update.
3. Install Fix Pack 3:

Change to the updateinstaller directory for the plugin:

cd <PLUGIN_INSTALL_ROOT>\updateinstaller

Use the update command to install the refresh pack as shown below. For <PLUGIN_INSTALL_ROOT>, substitute the location where you installed the

IBM HTTP Server Plug-in. For “maintenance.package”, substitute the location of the IBM HTTP Server Plug-in Fix Pack 3 which you extracted.

update.exe -silent -W product.location=”<PLUGIN_INSTALL_ROOT>” -W maintenance.package=”<PLUGIN_INSTALL_ROOT>/updateinstaller/maintenance/6.0.2-WS-WASPlugIn-WinX32-FP0000003.pak” -W update.type=”install”

Example:

update.exe -silent -W product.location=”C:/WebSphere/plugin” -W maintenance.package=”C:/WebSphere/plugin/updateinstaller/maintenance/6.0.2-WS-WASPlugIn-WinX32-FP0000003.pak” -W update.type=”install”

The command will return immediately, but the installation will take about 5 to 30 minutes depending upon the speed of your machine. To verify the version of the HTTP Server Plug-in installed, change to the bin directory under the directory where you installed the IBM HTTP Server Plug-in:

cd <PLUGIN_INSTALL_ROOT>\bin

Type the following command to display the version:

versionInfo.bat

The version should display as:

Name: Web server plug-ins for IBM WebSphere Application Server

Version: 6.0.2.3

UNIX and Linux platforms:

1. Open a command prompt and set $PLUGIN_HOME to <PLUGIN_INSTALL_ROOT>.
2. **cd $PLUGIN_HOME**
3. Open a web browser, download and extract Fix Pack 3:
   - For AIX, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010719
   - For HP-UX, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010721
   - For Linux, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010722
   - For Solaris, go to: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24010723.
   - Scroll down to the “Download Package” section

- Click on the “DD” link next to ”Plugins” to download the fix pack. Note the file size.
- Click on the “I agree” button in the popup window to accept Download Terms and Conditions.
- Click on “Yes” to accept the IBM security certificate.
- For the download location, specify $PLUGIN_HOME like the following:
  a) /usr/WebSphere/plugin (AIX)
  b) /opt/WebSphere/plugin (Linux, Solaris, HPUX)
- If asked to create the directory, click “Ok”.
- If asked to configure proxy click “No” unless a proxy must be configured.
- After the download completes, press Details to display the file name and size. Verify the file size to ensure the correct file has been successfully downloaded.
- Extract the fix pack
  cd $PLUGIN_HOME
  tar -xvf 6.0.2-WS-WASPlugIn-<*platform*>-FP0000003.tar

4. Install Fix Pack 3

   cd $PLUGIN_HOME/updateinstaller

   ./update -silent -W product.location=”$PLUGIN_HOME” -W maintenance.package=”$PLUGIN_HOME/updateinstaller/maintenance/6.0.2-WS-WASPlugIn-<platform>-FP0000003.pak” -W update.type=”install”

   Example:

   ./update -silent -W product.location=”/opt/WebSphere/plugin” -W maintenance.package=”/opt/WebSphere/plugin/updateinstaller/maintenance/6.0.2-WS-WASPlugIn-LinuxX32-FP0000003.pak” -W update.type=”install”

   For AIX, specify /usr, not /opt for the locations above. Additionally, the filename of the fix pack is also specific to platform (e.g. LinuxX32).

   The command will return immediately, but the installation will take about 5 to 30 minutes depending upon the speed of your machine. After the command returns to the command prompt, perform the following procedures.

   To verify the version of the HTTP Server Plug-in installed, change to the bin directory under the directory where you installed the IBM HTTP Server Plug-in:

   cd $PLUGIN_HOME/bin

   Type the following command to display the version:

   ./versionInfo.sh

   The version should display as:

Name: Web server plug-ins for IBM WebSphere Application Server

Version: 6.0.2.3

5. Once the execution of the fix pack has been determined to be successful, delete the $PLUGIN_HOME/updateinstaller directory

```
cd $PLUGIN_HOME
rm -r -f  updateinstaller
```

3.3.11 Install Interim Fixes for WebSphere Application Server (Required)

For WebSphere Application Server, WebSphere Application Server Express and WebSphere Application Server Network Deployment, you must install interim fixes (Ifixes) so that your WebSphere Application Server installation conforms to the evaluated configuration.

The following Interim Fixes (Ifixes) must be installed from the WebSphere Application Server support site at:

http://www-306.ibm.com/software/webservers/appserv/was/support/

Required Ifixes:

APAR Number:	**Ifix Package name:**
PK15487	6.0.2.0-WS-WAS-MultiOS-IFPK15487
PK16977	PK16977.6.0.2-WS-WAS-IF0000001
PK13494	PK13494.6.0.2-WS-WAS-IF0000001
PK13653	6.0.2.3-WS-WAS-MultiOS-IFPK13653
PK15059	PK15059.6.0.2-WS-WAS-F0000001
PK18574	6.0.2.3-WS-WAS-MultiOS-IFPK18574
PK18576	6.0.2.3-WS-WAS-MultiOS-IFPK18576
PK18991	PK18991.6.0.2-WS-WAS-IF0000001

Under, "Search Support (this product)", enter the name of each of the APAR numbers and check "Download". Press "Search". From the search results select the item showing the APAR number for 6.0.2.3. For APAR PK15487, select the item showing the APAR number for 6.0.2. You should see a page with the Abstract and Description for the APAR you selected. Scroll down to the "Download Package" section and verify the package name is the same as that in the table above. Select to download using the "DD" option for the APAR package name. Note the file size in bytes.

Follow the instructions on the WebSphere Application Server Support Site to obtain the updateinstaller and to install each of the Interim fixes. (Note: the updateinstaller may be downloaded once and the same updateinstaller may be used to install each of the Ifixes).

http://www-1.ibm.com/support/docview.wss?rs=180&context=SSEQTP&q1=updateinstaller&uid=swg21205400&loc=en_US&cs=utf-8&lang=en

Windows platform:

Example (Installing an Ifix):

- Extract the fix pack to <WAS_INSTALL_ROOT>\updateinstaller\maintenance
- cd <WAS_INSTALL_ROOT>\updateinstaller
- update -silent -W maintenance.package="<WAS_INSTALL_ROOT>\updateinstaller\maintenance\<Ifix Package Name>.pak"

To verify that each of the Interim Fixes has been installed correctly take the following steps:

- cd <WAS_INSTALL_ROOT>\logs\update\<fix_pack_name>.install\updatelog.txt
- Edit the log and search for the string “INSTCONFSUCCESS” to verify that the Interim Fix Pack was installed successfully.
- Repeat this procedure for each of the interim fix packs.

UNIX and Linux platforms:

Example (Installing an Ifix):

- Extract the fix pack to <WAS_INSTALL_ROOT>/updateinstaller/maintenance
- cd <WAS_INSTALL_ROOT>/updateinstaller
- ./update -silent -W maintenance.package="<WAS_INSTALL_ROOT>/updateinstaller/maintenance/<Ifix Package Name>.pak"

To verify that each of the Interim Fixes has been installed correctly take the following steps:

- cd <WAS_INSTALL_ROOT>/logs/update/<fix_pack_name>.install/updatelog.txt

- Edit the log and search for the string “INSTCONFSUCCESS” to verify that the Interim Fix Pack was installed successfully.
- Repeat this procedure for each of the interim fix packs.

3.4 Configuring the WebSphere Application Server Components

WebSphere Application Server must be configured in the evaluated configuration. The evaluated configuration is described in Section 2.2 of this document. This section provides steps for configuring the components of WebSphere Application Server in the evaluated configuration. It also provides examples of some possible combinations of components in the evaluated configuration for each of the WebSphere Application Server editions and the procedures that can be used to configure these example configurations in sections 3.4.10 through 3.4.13.

3.4.1 Download Common Criteria Sample Scripts

Sample scripts for the setup and validation of the WebSphere Application Server EAL4 evaluated configuration can be found on the WebSphere Application Server Common Criteria page at the following link:

http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24011697

From this WebSphere Application Server Common Criteria page, under the “Download Package” section, select the platform (Windows, UNIX platforms, or z/OS) for the scripts you want to download. Select “DD” under “Download Options” to download using Download Director. Follow the directions below for the WebSphere Application Server product you have installed.

WebSphere Application Server and WebSphere Application Server, Express

On Windows systems, download the zip file and place it in the C:\cc_scripts directory on the machine where your WebSphere Application Server is installed. Extract the contents to the C:\cc_scripts directory.

On UNIX systems, download the tar file and place it in the /cc_scripts directory on the machine where your WebSphere Application Server is installed. Unpack the file into the /cc_scripts directory. Change to the /cc_scripts directory and issue the following commands to set the permissions for the files:

- “chmod 644” on files that you want to read and edit such as properties files
- “chmod 544” on files you execute such as .sh files
- “chmod 744” on files you execute that require editing

WebSphere Application Server , Network Deployment

On Windows systems, download the zip file and place it in a C:\cc_scripts directory on the machine where your deployment manager is installed. Extract the contents to the C:\cc_scripts directory.

On UNIX systems, download the tar file and place it in /cc_scripts on the machine where your deployment manager is installed. Unpack the file into the /cc_scripts directory. Change to the /cc_scripts directory and issue the following commands to set the permissions for the files:

- “chmod 644” on files that you want to read and edit such as properties files
- “chmod 544” on files you execute such as .sh files
- “chmod 744” on files you execute that require editing.

WebSphere Application Server for z/OS

Transfer the tar file package to your z/OS system, and unpack the tar file into the /cc_scripts directory on the machine where your deployment manager is installed. Change to the /cc_scripts directory and issue the following commands to set the permissions for the files:

- “chmod 644” on files that you want to read and edit such as properties files
- “chmod 544” on files you execute such as .sh files
- “chmod 744” on files you execute that require editing
- Convert executable files (createUDDI30.sh and setupUDDI.sh) from ASCII to EBCDIC.

3.4.2 Create Application Server Profiles

The WebSphere Application Server profile defines the runtime environment. The sections below provide information on profile creation for the WebSphere Application Server products.

WebSphere Application Server and WebSphere Application Server, Express

WebSphere Application Server and WebSphere Application Server Express installation creates an application server profile with an application server called server1. In the description of the steps to set up the evaluated configuration which follow, we are assuming use of this “default” profile and the default application server, “server1”. Optionally, you may create your own application server profile.

For more information on creating customized profiles, refer the WebSphere Application Server Information Center at:

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/tpro_instancessaappserv.html

WebSphere Application Server , Network Deployment

After installation, you must create profiles for your deployment manager, node agents and application servers for WebSphere Application Server, Network Deployment according to the instructions in the WebSphere Application Server Information Center at:

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/tpro_instancessaappserv.html

Also refer to information on using the wasprofile command:

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/rxml_wasprofile.html

In the description of the steps to set up the evaluated configuration which follow, we are assuming use of the <Dmgr_profile> which is the name of the profile you create for your deployment manager. And we are assuming <appServer*name> are the names of the application servers in the cell, where * is a number. You may substitute your profile name for the <Dmgr_profile> profile and your application server names for <appServer*name>.

The examples below show the commands to set up a two machine configuration with a deployment manager, node agent, and two application servers on the first machine (machine1) and a node agent and two application servers on the second machine (machine2) as described in the example configuration in section 3.4.12.

Refer to Appendix B: Sample Ports Files for Configuring Profiles for the example file contents used for the -portsfile parameter when configuring the deployment manager and node profiles. These files should be placed on machines 1 and 2 in the /usr/ccTmp/portsFiles directory for AIX, the /opt/ccTmp/portsFiles directory for Linux, HP, or Solaris, and the C:\ccTmp\portsFiles directory for Windows.

In the steps below, the following values are used when configuring the example configuration for WebSphere Application Server Network Deployment as described in section 3.4.12.

<Dmgr_profile>	cc_DMGR
<DM_RMI_PORT>	9809
<dmShortHostname>	short host name for the machine
<dmHost>	fully qualified host name for the machine
<Node1_profile>	cc_MANAGED
<Node1_nodeName>	ccNode01

<node1ShortHostname>	short host name of machine 1
<node1_Host>	fully qualified host name of machine 1
<Node2_profile>	cc_MANAGED
<Node2_nodeName>	ccNode02
<node2ShortHostname>	short host name of machine 2
<node2_Host>	fully qualified host name of machine 2
<appServer1name>	na1server1
<appServer2name>	na1server2
<appServer3name>	na2server1
<appServer4name>	na2server2

Windows platform:

1. On machine 1, type the following instructions to configure the deployment manager and node profiles.

-
  ```
  cd <WAS_INSTALL_ROOT>\bin
  ```

-
  ```
  wasprofile.bat -create -profileName <Dmgr_profile> \
  -profilePath <WAS_INSTALL_ROOT>/profiles/<Dmgr_profile> \
  -templatePath <WAS_INSTALL_ROOT>/profileTemplates/dmgr \
  -nodeName <dmShortHostname>Manager -cellName cceal4Cell \
  -hostName <dmHost> \
  -portsFile c:/ccTmp/portsFiles/dmPorts.props –isDefault
  ```

-
  ```
  cd <WAS_INSTALL_ROOT>\bin
  ```

-
  ```
  wasprofile.bat -create -profileName <Node1_profile> \
  -profilePath <WAS_INSTALL_ROOT>/profiles/<Node1_profile> \
  -templatePath <WAS_INSTALL_ROOT>/profileTemplates/managed \
  -nodeName <Node1_nodeName> -cellName <node1ShortHostname>Cell \
  -hostName <node1_Host> \
  -portsFile c:/ccTmp/portsFiles/na1Ports.props
  ```

2. On machine 2, type the following instructions to create the node profile.

-
  ```
  cd <WAS_INSTALL_ROOT>\bin
  ```

-
  ```
  wasprofile.bat -create -profileName <Node2_profile> \
  -profilePath <WAS_INSTALL_ROOT>/profiles/<Node2_profile> \
  ```

**-templatePath <WAS_INSTALL_ROOT>/profileTemplates/managed **

**-nodeName <Node2_nodeName> -cellName <node2ShortHostname>Cell **

**-hostName <node2_Host> **

-portsFile c:/ccTmp/portsFiles/na2Ports.props

3. On machine 1, type the following instructions to start the deployment manager and add the node to the cell.
   - **cd <WAS_INSTALL_ROOT>\profiles\<Dmgr_profile>\bin**
   - **startManager.bat**
   - **cd <WAS_INSTALL_ROOT>\bin**
   - **addNode.bat <dmHost> <DM_RMI_Port> -username srvrid -password srvrpwd -conntype RMI -profileName <Node1_profile>**
4. On machine 2, type the following instructions to add the node to the cell.

   Note: The system clock of the new node system must be synchronized with the Deployment manager system within 5 minutes and must be in the same time zone.

- **cd <WAS_INSTALL_ROOT>\bin**
- **addNode.bat <dmHost> <DM_RMI_Port> -username srvrid -password srvrpwd -conntype RMI -profileName <Node2_profile>**

5. On the machine indicated below, type the following command to synchronize nodes.

   For machine 1, type:

- cd <WAS_INSTALL_ROOT>\profiles\<Node1_profile>\bin
- **syncNode.bat <dmHost> <DM_RMI_Port> -conntype RMI -stopservers -profileName <Node1_profile>**

For machine 2, type:

- cd <WAS_INSTALL_ROOT>\profiles\<Node2_profile>\bin
- **syncNode.bat <dmHost> <DM_RMI_Port> -conntype RMI -stopservers -profileName <Node2_profile>**

6. On the machine indicated below, type the following command start the node.

   For machine 1, type:

- **<WAS_INSTALL_ROOT>\profiles\<Node1_profile>\bin\startNode.bat**

  For machine 2, type:

- **<WAS_INSTALL_ROOT>\profiles\<Node2_profile>\bin\startNode.bat**

7. On machine 1, type the following commands to create the application servers.

- **cd <WAS_INSTALL_ROOT>\profiles\<Dmgr_profile>\bin**
- **wsadmin.bat -conntype RMI -port 9809 -c "$AdminTask createApplicationServer <Node1_nodeName> {-name <appServer1name> -templateName default -genUniquePorts}"**
- **wsadmin.bat -conntype RMI -port 9809 -c "$AdminTask createApplicationServer <Node1_nodeName> {-name <appServer2name> -templateName default -genUniquePorts}"**
- **wsadmin.bat -conntype RMI -port 9809 -c "$AdminTask createApplicationServer <Node2_nodeName> {-name <appServer3name> -templateName default -genUniquePorts}"**
- **wsadmin.bat -conntype RMI -port 9809 -c "$AdminTask createApplicationServer <Node2_nodeName> {-name <appServer4name> -templateName default -genUniquePorts}"**

8. On the machine indicated below, type the following command to synchronize nodes.

   For machine 1, type:

- cd <WAS_INSTALL_ROOT>\profiles\<Node1_profile>\bin
- **syncNode.bat <dmHost> <DM_RMI_Port> -conntype RMI -stopservers -profileName <Node1_profile>**

For machine 2, type:

- cd <WAS_INSTALL_ROOT>\profiles\<Node2_profile>\bin
- **syncNode.bat <dmHost> <DM_RMI_Port> -conntype RMI -stopservers -profileName <Node2_profile>**

9. On the machine indicated below, type the following command start the node.

   For machine 1, type:

- **<WAS_INSTALL_ROOT>\profiles\<Node1_profile>\bin\startNode.bat**

   For machine 2, type:

- **<WAS_INSTALL_ROOT>\profiles\<Node2_profile>\bin\startNode.bat**

10. On machine 1, start the application servers.

- **<WAS_INSTALL_ROOT>\profiles\<Node1_profile>\bin\startServer.bat <appServer1name>**

-
  ```
  <WAS_INSTALL_ROOT>\profiles\<Node1_profile>\bin\startServer.bat
  <appServer2name>
  ```

11. On machine 2, start the application servers.

-
  ```
  <WAS_INSTALL_ROOT>\profiles\<Node2_profile>\bin\startServer.bat
  <appServer3name>
  ```

-
  ```
  <WAS_INSTALL_ROOT>\profiles\<Node2_profile>\bin\startServer.bat
  <appServer4name>
  ```

UNIX and Linux platforms:

1. On machine 1, type the following instructions to configure the deployment manager and node profiles.

-
  ```
  cd <WAS_INSTALL_ROOT>/bin
  ```

-
  ```
  ./wasprofile.sh -create -profileName <Dmgr_profile> \
  -profilePath <WAS_INSTALL_ROOT>/profiles/<Dmgr_profile> \
  -templatePath <WAS_INSTALL_ROOT>/profileTemplates/dmgr \
  -nodeName <dmShortHostname>Manager -cellName cceal4Cell \
  -hostName <dmHost> \
  -portsFile /usr/ccTmp/portsFiles/dmPorts.props –isDefault
  ```

-
  ```
  cd <WAS_INSTALL_ROOT>/bin
  ```

-
  ```
  ./wasprofile.sh -create -profileName <Node1_profile> \
  -profilePath <WAS_INSTALL_ROOT>/profiles/<Node1_profile> \
  -templatePath <WAS_INSTALL_ROOT>/profileTemplates/managed \
  -nodeName <Node1_nodeName> -cellName <node1ShortHostname>Cell \
  -hostName <node1_Host> \
  -portsFile /usr/ccTmp/portsFiles/na1Ports.props
  ```

2. On machine 2, type the following instructions to create the node profile.

-
  ```
  cd <WAS_INSTALL_ROOT>/bin
  ```

-
  ```
  ./wasprofile.sh -create -profileName <Node2_profile> \
  -profilePath <WAS_INSTALL_ROOT>/profiles/<Node2_profile> \
  -templatePath <WAS_INSTALL_ROOT>/profileTemplates/managed \
  -nodeName <Node2_nodeName> -cellName <node2ShortHostname>Cell \
  -hostName <node2_Host> \
  ```

-portsFile /usr/ccTmp/portsFiles/na2Ports.props

3. On machine 1, type the following instructions to start the deployment manager and add the node to the cell.
    - **cd <WAS_INSTALL_ROOT>/profiles/<Dmgr_profile>/bin**
    - **./startManager.sh**
    - **cd <WAS_INSTALL_ROOT>/bin**
    - **./addNode.sh <dmHost> <DM_RMI_Port> -username srvrid -password srvrpwd -conntype RMI -profileName <Node1_profile>**
4. On machine 2, type the following instructions to add the node to the cell.

- **cd <WAS_INSTALL_ROOT>/bin**
- **./addNode.sh <dmHost> <DM_RMI_Port> -username srvrid -password srvrpwd -conntype RMI -profileName <Node2_profile>**

5. On the machine indicated below, type the following command to synchronize nodes.

   For machine 1, type:

- cd <WAS_INSTALL_ROOT>/profiles/<Node1_profile>/bin
- **./syncNode.sh <dmHost> <DM_RMI_Port> -conntype RMI -stopservers -profileName <Node1_profile>**

For machine 2, type:

- cd <WAS_INSTALL_ROOT>/profiles/<Node2_profile>/bin
- **./syncNode.sh <dmHost> <DM_RMI_Port> -conntype RMI -stopservers -profileName <Node2_profile>**

6. On the machine indicated below, type the following command start the node.

   For machine 1, type:

- **<WAS_INSTALL_ROOT>/profiles/<Node1_profile>/bin/startNode.sh**

  For machine 2, type:

- **<WAS_INSTALL_ROOT>/profiles/<Node2_profile>/bin/startNode.sh**

7. On machine 1, type the following commands to create the application servers.

- **cd <WAS_INSTALL_ROOT>/profiles/<Dmgr_profile>/bin**

- **./wsadmin.sh -conntype RMI -port 9809 -c "$AdminTask createApplicationServer <Node1_nodeName> {-name <appServer1name> -templateName default -genUniquePorts}"**
- **./wsadmin.sh -conntype RMI -port 9809 -c "$AdminTask createApplicationServer <Node1_nodeName> {-name <appServer2name> -templateName default -genUniquePorts}"**
- **./wsadmin.sh -conntype RMI -port 9809 -c "$AdminTask createApplicationServer <Node2_nodeName> {-name <appServer3name> -templateName default -genUniquePorts}"**
- **./wsadmin.sh -conntype RMI -port 9809 -c "$AdminTask createApplicationServer <Node2_nodeName> {-name <appServer4name> -templateName default -genUniquePorts}"**

8. On the machine indicated below, type the following command to synchronize nodes.

   For machine 1, type:

- cd <WAS_INSTALL_ROOT>/profiles/<Node1_profile>/bin
- **./syncNode.sh <dmHost> <DM_RMI_Port> -conntype RMI -stopservers -profileName <Node1_profile>**

For machine 2, type:

- cd <WAS_INSTALL_ROOT>/profiles/<Node2_profile>/bin
- **./syncNode.sh <dmHost> <DM_RMI_Port> -conntype RMI -stopservers -profileName <Node2_profile>**

9. On the machine indicated below, type the following command start the node.

   For machine 1, type:

- **<WAS_INSTALL_ROOT>/profiles/<Node1_profile>/bin/startNode.sh**

  For machine 2, type:

- **<WAS_INSTALL_ROOT>/profiles/<Node2_profile>/bin/startNode.sh**

10. On machine 1, start the application servers.

- **<WAS_INSTALL_ROOT>/profiles/<Node1_profile>/bin/startServer.sh <appServer1name>**
- **<WAS_INSTALL_ROOT>/profiles/<Node1_profile>/bin/startServer.sh <appServer2name>**

11. On machine 2, start the application servers.

- **<WAS_INSTALL_ROOT>/profiles/<Node2_profile>/bin/startServer.sh <appServer3name>**
- **<WAS_INSTALL_ROOT>/profiles/<Node2_profile>/bin/startServer.sh <appServer4name>**

WebSphere Application Server for z/OS

Configure your application server cell and nodes for WebSphere Application Server for z/OS according to the instructions in the Information Center at:

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.zseries.doc/info/zseries/ae/tins_runcust.html

3.4.3 Backup original configuration

After installing WebSphere Application Server and before taking the steps to configure it in the evaluated configuration, you should make a backup of the default configuration after installation.

Windows platform:

1. Take the steps below to backup your configuration so that it may be restored to the original state later.
2. Change to the directory for the application server or deployment manager:

For WebSphere Application Server and WebSphere Application Server, Express, change to the directory on your application server machine. For WebSphere Application Server, Network Deployment and z/OS, change to the directory on your deployment manager machine.

- cd <WAS_INSTALL_ROOT>\bin

3. Issue the command to back up the configuration.

- **backupConfig originalconfig** (where "originalconfig" is the file name for your backup file)

To restore the configuration (Do not run now)

- **cd <WAS_INSTALL_ROOT>\bin**
- **restoreConfig originalconfig**

Note that the server will be stopped during the backup of the configuration.

UNIX, Linux and z/OS platforms:

1. Take the steps below to backup your configuration so that it may be restored to the original state later.
2. Change to the directory for the application server or deployment manager:

For WebSphere Application Server and WebSphere Application Server, Express, change to the directory on your application server machine. For WebSphere Application Server, Network Deployment and z/OS, change to the directory on your deployment manager machine:

- **cd <WAS_INSTALL_ROOT>/bin**

3. Issue the command to back up the configuration.

   - **./backupConfig.sh originalconfig** (where "originalconfig" is the file name for your backup file)

   To restore the configuration later (Do not run now):

   - **cd <WAS_INSTALL_ROOT>/bin**
   - **./restoreConfig.sh originalconfig**

   Note that the server will be stopped during the backup of the configuration.

3.4.4 Application Server Common Configuration steps (required)

The following steps must be taken on all editions the WebSphere Application Server to ensure that the Application Server is in the evaluated configuration.

For WebSphere Application Server and WebSphere Application Server, Express the steps which follow should be performed on the application server unless otherwise noted.

For WebSphere Application Server, Network Deployment and WebSphere Application Server for z/OS, the steps which follow should be performed on the deployment manager.

3.4.4.1 Create server user ID in LDAP user registry (non-z/OS product)

For WebSphere Application Server and WebSphere Application Server, Express, at least one server user ID must be configured in the LDAP user registry as the serverID. Our examples use the following values for the Server ID and password:

User Name:	srvrid
Password:	srvrpwd

Refer to the WebSphere Application Server Information Center for configuring the server ID in the LDAP user registry at: http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/usec_rprdap.html

3.4.4.2 Create server user ID in the local operating system (z/OS product)

For WebSphere Application Server for z/OS, at least one server user ID must be configured in the local registry, System Authorization Facility (SAF0. Refer to the WebSphere Information Center for considerations when using the z/OS local operating system registry at:

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.zseries.doc/info/zseries/ae/csec_localos.html

Our examples use the following values for Server ID and password:

User Name:	srvrid
Password:	srvrpwd

3.4.4.3 Set WAS_HOME environment variable for command line commands

The WAS_HOME environment variable is set in this section so that it may be used in subsequent sections and examples when issuing commands from the command line. For UNIX and z/OS platforms, this environment variable should be set in the operating system default user profile so that it takes effect for all command windows. For Windows platforms, the environment variable should be set in the operating system System Properties so that it takes effect for all command windows.

For the WebSphere Application Server and WebSphere Application Server, Express, WAS_HOME will be set to the bin directory within the default profile. If you have used a specific profile, you may substitute your profile name for “default”.

For WebSphere Application Server, Network Deployment and WebSphere Application Server for z/OS, the WAS_HOME variable will be set to the bin directory with in the deployment manager profile, <Dmgr_profile>.

For more information about using command line tools, refer to the WebSphere Application Server Information Center at:

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/txml_command.html

Windows platform:

- If you have installed WebSphere Application Server or WebSphere Application Server, Express, open a command prompt and type the following command to set $WAS_HOME environment variable to the bin directory within the “default” application server profile

```
set WAS_HOME=<WAS_INSTALL_ROOT>\profiles\default\bin
```

Example: set WAS_HOME=C:\WebSphere\AppServer\profiles\default\bin

- If you have installed WebSphere Application Server, Network Deployment, and type the following command to set $WAS_HOME environment variable to the bin directory within your deployment manager profile.

  set WAS_HOME=<WAS_INSTALL_ROOT>\profiles\<Dmgr_profile>\bin

  Example: set WAS_HOME=C:\WebSphere\AppServer\profiles\cc_DMGR\bin

UNIX and z/OS platforms:

- If you have installed WebSphere Application Server or WebSphere Application Server, Express, open a command prompt and type the following command to set $WAS_HOME environment variable to the bin directory within the “default” application server profile

  export WAS_HOME=<WAS_INSTALL_ROOT>/profiles/default/bin

  Example: export WAS_HOME=/ WebSphere/AppServer/profiles/default/bin

- If you have installed WebSphere Application Server, Network Deployment or WebSphere Application Server for z/OS, type the following command to set $WAS_HOME environment variable to the bin directory within your deployment manager profile.

  export WAS_HOME=<WAS_INSTALL_ROOT>/profiles/<Dmgr-profile>/bin

  Example: export WAS_HOME=/WebSphere/AppServer/profiles/cc_DMGR/bin

3.4.4.4 Configure administrative connection to use RMI

To configure the administrative connection to use RMI, take the following steps.

For WebSphere Application Server and WebSphere Application Server, Express standalone application server, perform the steps for the application server profile.

For WebSphere Application Server, Network Deployment and z/OS, perform the steps on the deployment manager and node profiles.

Windows platform:

1. Now open a command prompt change to the WAS_HOME directory:

   cd %WAS_HOME%

2. Start the server.

   For Application Server or WebSphere Application Server, Express:

   startserver server1

For Application Server, Network Deployment and z/OS:

a) Type the following command on your deployment manager system:

startManager

After the deployment manager has been started, you should see a message stating that the server is open for e-business and the process id is <id_number>.

b) Type the following command for each node agent:

<WAS_INSTALL_ROOT>\profiles\<Node*_profile>\bin\startNode

After the node agent has been started, you should see a message stating that the server is open for e-business and the process id is <id_number>

c) Type the following command to start each application server:

<WAS_INSTALL_ROOT>\profiles\<Node*_profile>\bin\startServer <appServer*name>

After the application server has been started, you should see a message stating that the server is open for e-business and the process id is <id_number>.

3. Change to the directory to set properties.

For Application Server or WebSphere Application Server, Express:

cd <WAS_INSTALL_ROOT>\profiles\default\properties

For Application Server, Network Deployment:

cd <WAS_INSTALL_ROOT>\profiles\<Dmgr_profile>\properties

and make the changes described in step 4 below.

cd <WAS_INSTALL_ROOT>\profiles\<Node*_profile>\properties

for each node, and make the changes described in step 4 below

4. Configure RMI as the default connection type:

In wsadmin.properties, edit the following properties:

```
com.ibm.ws.scripting.connectionType=RMI
com.ibm.ws.scripting.port=<RMI_Port>
```

The <RMI_port> is 2809 for the single application server in WebSphere Application Server and WebSphere Application Server, Express.

The <RMI_port> is 9809 for WebSphere Application Server, Network Deployment and WebSphere Application Server for z/OS.

If com.ibm.ws.scripting.connectionType appears twice make sure the SOAP line is commented out (add # to beginning of line) and RMI is uncommented (remove #)

Save wsadmin.properties.

5. Configure the client so that a user id and password prompt will not appear each time a wsadmin command is run.

   Modify the following properties in the sas.client.props file:

   For WebSphere Application Server or WebSphere Application Server, Express:

   cd <WAS_INSTALL_ROOT>\profiles\default\properties

   For Application Server, Network Deployment:

   cd <WAS_INSTALL_ROOT>\profiles\<Dmgr_profile>\properties

   and make the changes as described below for sas.client.props.

   cd <WAS_INSTALL_ROOT>\profiles\<Node*_profile>\properties

   for each node, and make the changes described below for sas.client.props.

   Edit sas.client.props and set the following values:

   com.ibm.CORBA.loginSource=properties

   com.ibm.CORBA.loginUserid=srvrid

   com.ibm.CORBA.loginPassword=srvrpwd

   Save sas.client.props.

UNIX, Linux and z/OS platforms:

1. Open a command prompt change to the WAS_HOME directory:

   cd $WAS_HOME

2. Start the server.

   For WebSphere Application Server or WebSphere Application Server, Express:

   ./startServer.sh server1

   For WebSphere Application Server, Network Deployment or z/OS:

   a) Type the following command on your deployment manager system:

   ./startManager.sh

After the deployment manager has been started, you should see a message stating that the server is open for e-business and the process id is <id_number>

b) Type the following command for each node agent:

<WAS_INSTALL_ROOT>/profiles/<Node*_profile>/bin/startNode.sh

After the node agent has been started, you should see a message stating that the server is open for e-business and the process id is <id_number>

c) Type the following command to start each application server:

<WAS_INSTALL_ROOT>/profiles/<Node*_profile>/bin/startServer.sh <appServer*name>

After the application server has been started, you should see a message stating that the server is open for e-business and the process id is <id_number>

3. Change to the directory to set properties.

For WebSphere Application Server or WebSphere Application Server, Express:

cd <WAS_INSTALL_ROOT>/profiles/default/properties

For Application Server, Network Deployment:

cd <WAS_INSTALL_ROOT>/profile/<Dmgr_profile>/properties

and make the changes described in step 4 below.

cd <WAS_INSTALL_ROOT>/profiles/<Node*_profile>/properties

for each node, and make the changes described in step 4 below.

4. Configure RMI as the default connection type:

In wsadmin.properties, edit the following properties:

com.ibm.ws.scripting.connectionType=RMI

com.ibm.ws.scripting.port=<RMI_port>

The <RMI_port> is 2809 for the single application server in WebSphere Application Server and WebSphere Application Server, Express.

The <RMI_port> is 9809 for WebSphere Application Server, Network Deployment and WebSphere Application Server for z/OS.

If com.ibm.ws.scripting.connectionType appears twice make sure the SOAP line is commented out (add # to beginning of line) and RMI is uncommented (remove #)

Save wsadmin.properties.

5. Configure the client so that a user id and password prompt will not appear each time a wsadmin command is run.

Modify the following properties in the sas.client.props file:

For WebSphere Application Server or WebSphere Application Server, Express:

cd <WAS_INSTALL_ROOT>/profiles/default/properties

For Application Server, Network Deployment:

cd <WAS_INSTALL_ROOT>/profiles/<Dmgr_profile>/properties

and make the changes as described below for sas.client.props.

cd <WAS_INSTALL_ROOT>/profiles/<Node*_profile>/properties

for each node, and make the changes described below for sas.client.props.

Edit sas.client.props and set the following values:

```
com.ibm.CORBA.loginSource=properties
com.ibm.CORBA.loginUserid=srvrid
com.ibm.CORBA.loginPassword=srvrpwd
```

Save sas.client.props

Note: After completing this configuration step on WebSphere Application Server for z/OS, the following messages will be received for the stopServer, stopManager, stopNode and syncNode command. These messages can be ignored as the commands complete successfully.

The WebSphere error message below is received

BBOO0049E Local comm call lscclose() failed with RV=-1, RC=1120

followed by the C/C++ Run-time informational message:

EDC8120I Connection ended abnormally

3.4.4.5 Restart so configuration changes take effect

For WebSphere Application Server and WebSphere Application Server, Express, the steps below are necessary to stop and restart the application server so that configuration changes take effect. For WebSphere Application Server, Network

Deployment and WebSphere Application Server for z/OS, the steps are necessary to restart the cell so that configuration changes take effect.

Note: After security is configured in section 3.4.4.6, the parameters for username and password are required on the stopServer, syncnode, stopNode, and stopManager command. For example:

stopServer server1 -username srvrid -password srvrpwd

syncNode -stopservers -username srvrid -password srvrpwd

stopNode -username srvrid -password srvrpwd

stopManager -username srvrid -password srvrpwd

WebSphere Application Server and WebSphere Application Server, Express

For WebSphere Application Server and WebSphere Application Server, Express, standalone application server, take the following steps to restart the server after configuration changes.

Windows platform:

1. Change to the WAS_HOME directory

   cd %WAS_HOME%
2. **stopServer server1**

   When this command completes, you should see a message stating "Server server1 stop completed."
3. **startServer server1**

   When this command completes, you should see a message stating "Server server1 open for e-business; process id is <id_number>"

UNIX, Linux and z/OS platforms:

1. Change to the WAS_HOME directory

   cd $WAS_HOME
2. **./stopServer.sh server1**

   When this command completes, you should see a message stating "Server server1 stop completed."
3. **./startServer.sh server1**

   When this command completes, you should see a message stating "Server server1 open for e-business; process id is <id_number>"

WebSphere Application Server, Network Deployment and WebSphere Application Server for z/OS

For WebSphere Application Server, Network Deployment and z/OS, take the following steps to restart the cell after configuration changes.

Windows platform:

1. Execute the syncNode command on each node agent in the cell in order to stop all servers on the node, including the node agent, before performing configuration synchronization with the cell. Use the values for <dmHost>, <DM_RMI_PORT> and <Node_profile> as specified when you configured the profiles in section 3.4.2.

```
<WAS_INSTALL_ROOT>\profiles\<Node*_profile>\bin\syncNode.bat
<dmHost> <DM_RMI_PORT> -conntype RMI -stopservers -profileName
<Node_profile> -username srvrid -password srvrpwd
```

2. Stop the deployment manager:

```
<WAS_INSTALL_ROOT>\profiles\<Dmgr_profile>\bin\stopManager
```

3. Start the deployment manager

```
<WAS_INSTALL_ROOT>\profiles\<Dmgr_profile>\bin\startManager
```

4. Start each of the node agents in the cell (where * is the node number):

```
<WAS_INSTALL_ROOT>\profiles\<Node*_profile>\bin\startNode.
```

5. Start each of the application servers in the cell (where * is the node number or application server number respectively)

```
<WAS_INSTALL_ROOT>\profiles\<Node*_profile>\bin\startServer.sh
<appServer*name>
```

UNIX, Linux and z/OS

1. Execute the syncNode command on each node agent in the cell in order to stop all servers on the node, including the node agent, before performing configuration synchronization with the cell. Use the values for <dmHost>, <DM_RMI_PORT> and <Node*_profile> as specified when you configured the profiles in section 3.4.2.

```
<WAS_INSTALL_ROOT>/profiles/<Node*_profile>/bin/syncNode.sh
<dmHost> <DM_RMI_PORT> -conntype RMI  -stopservers -profileName
<Node_profile> -username srvrid -password srvrpwd
```

2. Stop the deployment manager:

```
<WAS_INSTALL_ROOT>/profiles/<Dmgr_profile>/bin/stopManager.sh
```

3. Start the deployment manager

```
<WAS_INSTALL_ROOT>/profiles/<Dmgr_profile>/bin/startManager.sh
```

4. Start each of the node agents in the cell (where * is the node number):

```
<WAS_INSTALL_ROOT>/profiles/<Node*_profile>/bin/startServer.sh
<appServer*name>
```

5. Start each of the application servers in the cell (where * is the node number or application server number respectively):

```
<WAS_INSTALL_ROOT>/profiles/<Node*_profile>/bin/startServer.sh
<appServer*name>
```

3.4.4.6 Configure Security

To configure WebSphere Application security to conform to the evaluated configuration, take the following steps.

Windows platform:

1. Change to the WAS_HOME directory.

```
cd %WAS_HOME%
```

2. Edit the file C:\cc_scripts\eval_config\SecConfig.properties to specify the values to match your environment for the "LDAP Panel" section of the file which is shown below. Substitute your WebSphere Server ID and password for <WAS_Server_ID> and <WAS_Server_ID_pwd>. In the examples we have used, these would be "srvrid" and "srvrpwd". Substitute the fully qualified name of your machine for <LDAP_host> and <LDAP_bind_pw> for your LDAP bind password. Update the values of LDAPPort, LDAPBaseDN and LDAPBindDN to match your LDAP configuration.

   The rest of the parameters in the file should remain unchanged as they are required in order to configure WebSphere Application Server in the evaluated configuration.

   Save the changes you have made to the SecConfig.properties file.

```
#####################################################################
#
LDAP Panel
#####################################################################
#
LDAPServerId=<WAS_Server_ID>
LDAPPassword=<WAS_Server_ID_pwd>
LDAPServerType=IBM_DIRECTORY_SERVER
LDAPHostName=<LDAP_host>
```

```
LDAPPort=389
LDAPBaseDN=o=ibm,c=us
LDAPBindDN=cn=root
LDAPBindPassword=<LDAP_bind_pw>
LDAPsearchTimeout=
LDAPreuseConnection=true
LDAPIgnoreCase=true
LDAPsslEnabled=false
LDAPsslConfig=
```

3. Configure security for the evaluated configuration. Type the following command all on one line.

wsadmin.bat -profile C:/cc_scripts/eval_config/SecConfigProcs.jacl

-f C:/cc_scripts/eval_config/SecConfigBatch.jacl C:/cc_scripts/eval_config/SecConfig.properties

-username srvrid -password srvrpwd

When the command has completed, you will see "Validation success. Configuration Saved!"

4. Stop and restart the server or cell by following directions in section 3.4.4.5 to enable the security changes.

UNIX and Linux platforms:

1. Change to the WAS_HOME directory.

   cd $WAS_HOME

2. Edit the file /cc_scripts/eval_config/SecConfig.properties to specify the values to match your environment for the "LDAP Panel" section of the file which is shown below. Substitute your WebSphere Application Server Server ID and password for <WAS_Server_ID> and <WAS_Server_ID_pwd>. In the examples we have used, these would be "srvrid" and "srvrpwd". Substitute the fully qualified name of your machine for <LDAP_host> and <LDAP_bind_pw> for your LDAP bind password. Update the values of LDAPPort, LDAPBaseDN and LDAPBindDN to match your LDAP configuration.

   The rest of the parameters in the file should remain unchanged as they are required in order to configure WebSphere Application Server in the evaluated configuration.

   Save the changes you have made to the SecConfig.properties file.

```
######################################################################
#
```

```
LDAP Panel
#################################################################
#
LDAPServerId=<WAS_Server_ID>
LDAPPassword=<WAS_Server_ID_pwd>
LDAPServerType=IBM_DIRECTORY_SERVER
LDAPHostName=<LDAP_host>
LDAPPort=389
LDAPBaseDN=o=ibm,c=us
LDAPBindDN=cn=root
LDAPBindPassword=<LDAP_bind_pw>
LDAPsearchTimeout=
LDAPreuseConnection=true
LDAPIgnoreCase=true
LDAPsslEnabled=false
LDAPsslConfig=
```

3. Configure security for the evaluated configuration. Type the following command all on one line.

```
./wsadmin.sh -profile /cc_scripts/eval_config/SecConfigProcs.jacl -f

/cc_scripts/eval_config/SecConfigBatch.jacl
/cc_scripts/eval_config/SecConfig.properties

 -username srvrid -password srvrpwd
```

When the command has completed, you will see “Validation success. Configuration Saved!”

4. Stop and restart the server or cell as described in section 3.4.4.5 to enable the security changes:

z/OS platform:

1. Change to the WAS_HOME directory.

   ```
   cd $WAS_HOME
   ```

2. Edit the file /cc_scripts/eval_config/SecConfig.properties to specify the values to match your environment for the “Local OS Panel” section of the file which is shown below. Substitute your WebSphere Application Server Server ID and password for <WAS_Server_ID> and <WAS_Server_ID_pwd>. In the examples we have used, these would be “srvrid” and “srvrpwd. The rest of the parameters in the file should remain unchanged as they are required in order to configure WebSphere Application Server in the evaluated configuration.

   Save the changes you have made to the SecConfig.properties file.

```
##################################################################
Local OS Panel
##################################################################
LocalOSServerID=srvrid
LocalOSServerpassword=srvrpwd
```

3. Configure security for the evaluated configuration

   ./wsadmin.sh -profile /cc_scripts/eval_config/SecConfigProcs.jacl -f

   /cc_scripts/eval_config/SecConfigBatch.jacl /cc_scripts/eval_config/SecConfig.properties

   -username srvrid -password srvrpwd

4. Stop and restart the server or cell as described in section 3.4.4.5 to enable the security changes.

3.4.4.7 Configure SAF Authorization (z/OS only)

Note: The following steps apply to WebSphere Application Server for z/OS only.

z/OS platform:

1. Change to the WAS_HOME directory

   cd %WAS_HOME%

2. Type the following command all on one line:

   ./wsadmin.sh -f /cc_scripts/eval_config/configSAF.jacl -username srvrid -password srvrpwd

3.4.4.8 Disable Ports

To disable ports to conform to the evaluated configuration, take the following steps.

Windows platform:

1. Change to the WAS_HOME directory

   cd %WAS_HOME%

2. If you plan to configure the default messaging provider, then type the following command all on one line

   wsadmin.bat -f C:/cc_scripts/eval_config/disablePorts_SIB.jacl -username srvrid -password srvrpwd

   If you do **not** plan to configure the default messaging provider, then type the following command all on one line

   wsadmin.bat -f C:/cc_scripts/eval_config/disablePorts.jacl -username srvrid -password srvrpwd

When the command has completed, you will see “Configuration Saved! Restart cell for changes to take effect.”

3. Stop and restart the server or cell as described in section 3.4.4.5 to enable the changes.

UNIX, Linux and z/OS platforms:

1. Change to the WAS_HOME directory

   cd $WAS_HOME

2. If you plan to configure the default messaging provider, then type the following command all on one line

   ./wsadmin.sh -f /cc_scripts/eval_config/disablePorts_SIB.jacl -username srvrid -password srvrpwd

   If you do **not** plan to configure the default messaging provider, then type the following command all on one line

   ./wsadmin.sh -f /cc_scripts/eval_config/disablePorts.jacl -username srvrid -password srvrpwd

   When the command has completed, you will see “Configuration Saved! Restart cell for changes to take effect.”

3. Stop and restart the server or cell as described in section 3.4.4.5 to enable the changes.

3.4.4.9 Disable SOAP connections

To disable SOAP connections to conform to the evaluated configuration, take the following steps.

Windows platform:

1. Change to the WAS_HOME directory

   cd %WAS_HOME%

2. Type the following command all on one line:

   wsadmin.bat -f C:/cc_scripts/eval_config/disableSOAP.jacl -username srvrid -password srvrpwd

   When the command has completed, you will see “Done with server: <SERVER_NAME> on node <NODE_NAME>. Changes saved!”

3. Stop and restart the server or cell as described in section 3.4.4.5 to enable the changes.

UNIX, Linux and z/OS platforms:

1. Change to the WAS_HOME directory

cd $WAS_HOME

2. Type the following command all on one line:

   ./wsadmin.sh -f /cc_scripts/eval_config/disableSOAP.jacl -username srvrid -password srvrpwd

   When the command has completed, you will see “Done with server: <SERVER_NAME> on node <NODE_NAME>. Changes saved!”

3. Stop and restart the server or cell as described in section 3.4.4.5 to enable the changes.

3.4.4.10 Remove User Applications

To remove user applications which are installed by default during installation, take the following steps.

Windows platform:

1. Change to the WAS_HOME directory

   cd %WAS_HOME%

2. Type the following command all on one line:

   wsadmin.bat -f C:/cc_scripts/eval_config/removeUserApps.jacl -username srvrid -password srvrpwd

   When the command has completed, you will see a message for each application that has been removed which says, “ADMA5106I: Application <Application_name> uninstalled successfully.”

3. Stop and restart the server or cell as described in section 3.4.4.5 to enable the changes.

UNIX, Linux and z/OS platforms:

1. Change to the WAS_HOME directory**.**

   cd $WAS_HOME

2. Type the following command all on one line:

   ./wsadmin.sh -f /cc_scripts/eval_config/removeUserApps.jacl -username srvrid -password srvrpwd

   When the command has completed, you will see a message for each application that has been removed which says, “ADMA5106I: Application <Application_name> uninstalled successfully.”

3. Stop and restart the server or cell as described in section 3.4.4.5 to enable the changes.

3.4.4.11 Remove System Applications

To remove WebSphere Application Server system applications which are installed by default during installation, take the following steps.

Windows platform:

1. Change to the WAS_HOME directory.

   cd %WAS_HOME%

2. Execute this step **only for WebSphere Application Server Network Deployment** to redeploy the secured file transfer application. Otherwise, skip to the next step. Substitute your value for <WAS_INSTALL_ROOT>, <YOUR_CELL_NAME>, <YOUR_NODE_NAME> the DM node, and <YOUR_SERVER_NAME> the DM server, usually dmgr.

   ```
   wsadmin.bat -username srvrid -password srvrpwd -profile
   <WAS_INSTALL_ROOT>/bin/redeployFileTransfer.jacl -c
   "fileTransferAuthenticationOn  <YOUR_CELL_NAME>
   <YOUR_NODE_NAME>   <YOUR_SERVER_NAME>"
   ```

   Example (Network Deployment):

   ```
   wsadmin.bat -profile C: /WebSphere/AppServer/bin/redeployFileTransfer.jacl
   -c "fileTransferAuthenticationOn cceal4Cell t54Manager dmgr"
   ```

3. Type the following command to remove system applications.

   For a Network Deployment, <YOUR_NODE_NAME> is the DM node, and <YOUR_SERVER_NAME> is dmgr

   ```
   wsadmin.bat -username srvrid -password srvrpwd –f
   C:/cc_scripts/eval_config/removeSystemApps.jacl
   <YOUR_CELL_NAME>  <YOUR_NODE_NAME>
   <YOUR_SERVER_NAME>
   ```

   As the script runs, you will see messages indicating the system applications are being uninstalled, such as,“ADMA5106I: Application adminconsole uninstalled successfully.”, and finally “Changes saved.”

   Example:

   ```
   wsadmin.bat -username srvrid -password srvrpwd -f
   C:/cc_scripts/eval_config/removeSystemApps.jacl ccSANode01Cell
   ccSANode01 server1
   ```

4. Stop and restart the server or cell as described in section 3.4.4.5 to enable the security changes.

UNIX, Linux and z/OS platforms:

1. Change to the WAS_HOME directory.

```
cd $WAS_HOME
```

2. Execute this step **only for WebSphere Application Server Network Deployment (non-z/OS product)** to redeploy the secured file transfer application. Otherwise, skip to the next step. (Note that this step is not required for WebSphere Application Server for z/OS because the secured file transfer application is deployed by default).

   Substitute your value for <WAS_INSTALL_ROOT>, <YOUR_CELL_NAME>, <YOUR_NODE_NAME> the DM node, and <YOUR_SERVER_NAME> the DM server, usually dmgr.

   ```
   ./wsadmin.sh -username srvrid -password srvrpwd -profile
   <WAS_INSTALL_ROOT>/bin/redeployFileTransfer.jacl -c
   "fileTransferAuthenticationOn  <YOUR_CELL_NAME>
   <YOUR_NODE_NAME>   <YOUR_SERVER_NAME>"
   ```

3. Type the following command all on one line:

   For a Network Deployment, <YOUR_NODE_NAME> is the DM node, and <YOUR_SERVER_NAME> is dmgr.

   ```
   ./wsadmin.sh -f /cc_scripts/eval_config/removeSystemApps.jacl
   <YOUR_CELL_NAME> <YOUR_NODE_NAME> server1 -username
   srvrid -password srvrpwd
   ```

   As the script runs, you will see messages indicating the system applications are being uninstalled, such as,“ADMA5106I: Application adminconsole uninstalled successfully.”, and finally “Changes saved.”

4. Stop and restart the server or cell as described in section 3.4.4.5 to enable the security changes

3.4.4.12 Remove Trust Association Interceptors

To remove Trust Association Interceptors which are installed by default during installation, take the following steps.

Windows platform:

1. Change to the WAS_HOME directory

   ```
   cd %WAS_HOME%
   ```

2. Type the following command all on one line:

   ```
   wsadmin.bat -f C:/cc_scripts/eval_config/removeTAInterceptors.jacl
    -username srvrid -password srvrpwd
   ```

When the command has completed, you will see a message like the following for each trust association interceptor that has been removed:

```
Removing the TAIntercepter class
‘com.ibm.ws.security.web.WebSealTrustAssociationInterceptor'
‘com.ibm.ws.security.web.WebSealTrustAssociationInterceptor' is removed.
```

3. Stop and restart the server or cell as described in section 3.4.4.5 to enable the changes.

UNIX, Linux and z/OS platforms:

1. Change to the WAS_HOME directory

   cd $WAS_HOME

2. Type the following command all on one line:

   ./wsadmin.sh -f /cc_scripts/eval_config/removeTAInterceptors.jacl -username srvrid -password srvrpwd

   When the command has completed, you will see a message like the following for each trust association interceptor that has been removed:

```
Removing the TAIntercepter class
‘com.ibm.ws.security.web.WebSealTrustAssociationInterceptor'
‘com.ibm.ws.security.web.WebSealTrustAssociationInterceptor' is removed.
```

3. Stop and restart the server or cell as described in section 3.4.4.5 to enable the changes.

3.4.4.13 Remove JDBC Providers (z/OS only)

Note: The following steps apply to WebSphere Application Server for z/OS only.

z/OS platform:

1. Change to the WAS_HOME directory

   cd %WAS_HOME%

2. Type the following command all on one line:

   ./wsadmin.sh -f /cc_scripts/eval_config/removeJDBC.jacl -username srvrid -password srvrpwd

3.4.5 Backup security configuration

After completing the WebSphere Application Server common configuration and before taking the steps to configure optional components, you should make a backup of your configuration.

Windows platform:

1. Take the steps below to backup your configuration so that it may be restored to the state after security configuration later, if needed.
2. Change to the directory for the application server or deployment manager:

For WebSphere Application Server and WebSphere Application Server, Express, change to the directory on your application server machine. For WebSphere Application Server, Network Deployment and z/OS, change to the directory on your deployment manager machine.

- cd <WAS_INSTALL_ROOT>\bin

3. Issue the command to back up the configuration.

- **backupConfig securityconfig** (where "securityconfig" is the file name for your backup file)

4. The server is stopped during the backup of the configuration, so follow the steps in section 3.4.4.5 to restart the server.

To restore the configuration (Do not run now)

- **cd <WAS_INSTALL_ROOT>\bin**
- **restoreConfig securityconfig**

UNIX, Linux and z/OS platforms:

1. Take the steps below to backup your configuration so that it may be restored to the state after security configuration later, if needed.
2. Change to the directory for the application server or deployment manager:

For WebSphere Application Server and WebSphere Application Server, Express, change to the directory on your application server machine. For WebSphere Application Server, Network Deployment and z/OS, change to the directory on your deployment manager machine:

- **cd <WAS_INSTALL_ROOT>/bin**

3. Issue the command to back up the configuration.

- **./backupConfig.sh securityconfig** (where "securityconfig" is the file name for your backup file)

4. The server is stopped during the backup of the configuration, so follow the steps in section 3.4.4.5 to restart the server.

To restore the configuration later (Do not run now):

- **cd <WAS_INSTALL_ROOT>/bin**

- **./restoreConfig.sh securityconfig**

3.4.6 IBM HTTP Server (optional)

Note: this section does not apply to WebSphere Application Server for z/OS

The IBM HTTP Server is part of the TOE for the WebSphere Application Server, WebSphere Application Server, Express and WebSphere Application Server, Network Deployment. If IBM HTTP Server is configured, it must be configured as described in this section in order to conform to the evaluated configuration.

For WebSphere Application Server for z/OS, the IBM HTTP Server is an optional component in the environment, rather than a TOE component, and is not discussed here.

If the IBM HTTP Server is configured, the httpd.conf configuration file must follow the rules below to be in the evaluated configuration.

- The SSLEnable and SSLFIPSEnable directives must be included
- No SSLCipher directives must be present
- The following Load Module directives, but no others, are included
  - LoadModule log_config_module modules/mod_log_config.so
  - LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
  - LoadModule was_ap20_module "modules/mod_was_ap20_http.<extension>"

    where extension is "dll" for Windows, "so" for AIX and Linux, "sl" for HP-UX and Solaris.

To configure the IBM HTTP Server in the evaluated configuration, take the following steps:

Windows platform:

1. Change to the IBM HTTP Server config directory:

   cd <IHS_INSTALL_ROOT>\conf

2. Rename the default httpd.conf file provided during installation.

   ren httpd.conf httpd.conf.backup

3. Edit and create a new httpd.conf file with contents as shown below.

In this file, <IHS_INSTALL_ROOT> should be replaced with the installation path to your IBM HTTP Server. <SERVER_NAME> should be replaced with the value of the <SERVER_NAME> as shown in the http.conf.backup file. <PLUGIN_INSTALL_ROOT> should be replaced with the installation path of your IBM HTTP Server Plug-in.

The keyfile (shown as keyfile.kdb below) should be the name of the key database you created according to the instructions for using IKEYMAN in the IBM HTTP Server Information Center:

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/aes/ae/welc_ikeyman.html

Sample httpd.conf file:

```
DocumentRoot " <IHS_INSTALL_ROOT>/htdocs/en_US"
ServerRoot “<IHS_INSTALL_ROOT>"

ServerName <SERVER_NAME>
Listen 0.0.0.0:443

LoadModule log_config_module modules/mod_log_config.so
LogFormat "%h %l %u %t \"%r\" %>s %b" common
CustomLog logs/access.log common

LogLevel warn
ErrorLog logs/error.log

LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
<virtualhost *:443>
        SSLEnable
        SSLFIPSEnable
</virtualhost>
keyfile <IHS_INSTALL_ROOT>/ihskeys/keyfile.kdb
SSLDisable

LoadModule was_ap20_module "<PLUGIN_INSTALL_ROOT>/bin/mod_was_ap20_http.dll"
WebSpherePluginConfig "<WAS_INSTALL_ROOT>/profiles/default/config/cells/plugin-cfg.xml"
```

For WebSphere Application Server Network Deployment (non-z/OS product), the last line of the httpd.conf file for the WebSpherePluginConfig should be as follows:

```
WebSpherePluginConfig "<WAS_INSTALL_ROOT>/profiles/<Dmgr_profile>/config/cells/plugin-cfg.xml"
```

UNIX and Linux platforms:

1. Change to the IBM HTTP Server config directory:

   ```
   cd <IHS_INSTALL_ROOT>/conf
   ```

2. Rename the default httpd.conf file provided during installation.

   ```
   mv httpd.conf  httpd.conf.default
   ```

3. Edit and create a new httpd.conf file with contents as shown below.

   In this file, <IHS_INSTALL_ROOT> should be replaced with the installation path to your IBM HTTP Server. <SERVER_NAME> should be replaced with the value of the <SERVER_NAME> as shown in the http.conf.default file. <PLUGIN_INSTALL_ROOT> should be replaced with the installation path of your IBM HTTP Server Plug-in.

   The <EXTENSION> for the mod_was_ap20_http.<EXTENSION> should be “so” for AIX, Solaris, and Linux, “sl” for HP-UX.

   The <USER> and <GROUP> should be set as follows. For HP <USER> should be “www” and <GROUP> should be “other”. For AIX, Linux, and Solaris the <USER> should be “nobody” and <GROUP> should be “nobody”. For example:

   ```
   User nobody
   Group nobody
   ```

   The keyfile (shown as keyfile.kdb below) should be the name of the key database you created according to the instructions for using IKEYMAN in the IBM HTTP Server Information Center:

   http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/aes/ae/welc_ikeyman.html

Sample httpd.conf file:

```
User <USER>
Group <GROUP>


DocumentRoot "<IHS_INSTALL_ROOT>/htdocs/en_US"
ServerRoot "<IHS_INSTALL_ROOT>"


ServerName <SERVER_NAME>
Listen 0.0.0.0:443


LoadModule log_config_module modules/mod_log_config.so
```

```
LogFormat "%h %l %u %t \"%r\" %>s %b" common
CustomLog logs/access.log common


LogLevel warn
ErrorLog logs/error.log


LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
<virtualhost *:443>
        SSLEnable
        SSLFIPSEnable
</virtualhost>
keyfile <IHS_INSTALL_ROOT>/ihskeys/keyfile.kdb
SSLDisable
SSLCacheEnable


LoadModule was_ap20_module
                  "<PLUGIN_INSTALL_ROOT>/bin/mod_was_ap20_http.<EXTENSION>"
WebSpherePluginConfig "<WAS_INSTALL_ROOT>/profiles/default/config/cells/plugin-cfg.xml"
```

For WebSphere Application Server Network Deployment (non-z/OS product), the last line of the httpd.conf file for the WebSpherePluginConfig should be as follows:

```
WebSpherePluginConfig "<WAS_INSTALL_ROOT>/profiles/<Dmgr_profile>/config/cells/plugin-cfg.xml"
```

3.4.7 UDDI (optional)

The instructions in this section should be followed if you plan to configure the optional UDDI component. These steps configure the UDDI component and place it in the evaluated configuration.

3.4.7.1 Create the UDDI30 DB2 database

The following steps are required to configure the UDDI database in the evaluated configuration. These steps are required if you plan to configure the UDDI Registry in WebSphere Application Server.

Execute the following script on the system hosting the DB2 database. This step is needed for a local or remote connection to DB2. This will create and prime the UDDI DB2 database.

Windows platform:

If the database is not on the same machine as WebSphere Application Server, copy all the files from C:\cc_scripts\eval_config to a C:\cc_scripts\eval_config directory on the database machine. Also copy all the files from <WAS_INSTALL_ROOT>\AppServer\UDDIReg\databaseScripts to C:\cc_scripts\eval_config\ on the database machine.

1. Start a DB2 command session, by typing

db2cmd

2. A DB2 command window should open. From that window, type the following:

cd C:\cc_scripts\eval_config

3. Execute

createUDDI30.bat <db2user> <db2pass> <dbname> <pathToSQL>

Where

- db2user is the DB2 Administrator ID (change to suit your environment)
- db2pass is the password for the DB2 Administrator ID (change to suit your environment)
- dbname is the name of the DB2 database
- pathToSQL is the full path to the SQL files from to the UDDI scripts which are provided with WebSphere Application Server in <WAS_INSTALL_ROOT>\UDDIReg\databaseScripts or the location where you have copied the files onto the database machine if the database is on a separate machine from the application server (e.g. c:\cc_scripts\eval_config)

Example:

- cd C:\cc_scripts\eval_config
- createUDDI30.bat dbadmin adminpw UDDI30 c:/WebSphere/AppServer/UDDIReg/databaseScripts

After running the createUDDI30 script, you should receive a message “UDDI DATABASE CREATED SUCCESSFULLY.” If you receive errors, correct them and rerun the script.

Close the DB2 command session window.

UNIX, Linux and z/OS platforms:

If the database is not on the same machine as WebSphere Application Server, copy all the files from /cc_scripts/eval_config to a /cc_scripts/eval_config directory on the database machine. Also copy all the files from

<WAS_INSTALL_ROOT>/AppServer/UDDIReg/databaseScripts to /cc_scripts/eval_config on the database machine.

Execute the following shell script on the system hosting the DB2 database. This step is needed for a local or remote connection to DB2. This will define and prime the UDDI DB2 database.

1. Start a DB2 command session by running

su – db2user

2. A DB2 command window should open. From that window, type the following:

cd /cc_scripts/eval_config

3. Execute

./createUDDI30.sh <db2user> <db2pass> <dbname> <pathToSQL>

Where

- db2user is the db2 admin id (change to suit your environment)
- db2pass is the password for the db2 admin id (change to suit your environment)
- dbname is the name of the DB2 database
- pathToSQL is the full path to the SQL files used to create the UDDI database. (By default this is installed with the WebSphere Application Server in the <WAS_INSTALL_ROOT>/UDDIReg/databaseScripts directory or the location where you have copied the files onto the database machine if the database is on a separate machine from the application server (e.g. /cc_scripts/eval_config)

3.4.7.2 Define DB2 variables

This step is needed to define the DB2 variables to allow WebSphere Application Server to use a remote DB2 server. Perform this step, whether your DB2 server is remote or local, before issuing the commands in section 3.4.7.3.

Windows platform:

Prior to issuing the commands below, you should copy the following files from your DB2 Server installation to the C:\cc_scripts\eval_config directory on your Application Server -- db2jcc.jar file, db2jcc_license_cisuz.jar, and db2jcc_license_cu.jar. Note that you will only have a db2jcc_license_cisuz.jar if your DB2 is installed on a UNIX system.

For WebSphere Application Server Network Deployment, issue the commands for each node in the cell.

1. For WebSphere Application Server and WebSphere Application Server Express, type:

   cd %WAS_HOME%

   For WebSphere Application Server Network Deployment, type:

   cd <WAS_INSTALL_ROOT>\profiles\<nodeProfile>\bin

2. Type the following command to set DB2 variables.
   wsadmin.bat -username srvrid -password srvrpwd -f C:/cc_scripts/eval_config/setDB2variables.jacl <nodeName> <DB2UNIVERSAL_JDBC_DRIVER_PATH> <UNIVERSAL_JDBC_DRIVER_PATH>

Where

- nodeName is the name of the node which you specified for <YOUR_NODE_NAME> when you installed WebSphere Application Server in section 3.3.2 for WebSphere Application Server and WebSphere Application Server Express. It is the node profile such as <Node1_profile> and <Node2_profile> for Network Deployment as described in section 3.4.2 for creating profiles.
- <DB2UINVERSAL_JDBC_DRIVER_PATH> is the path to the db2jcc.jar file and the db2jcc_license_cisuz.jar file which you have copied to your WebSphere Application server machine. In this example, the location is C:\cc_scripts\eval_config.
- <UNIVERSAL_JDBC_DRIVER_PATH> is the path to the db2jcc_license_cu.jar file which you have copied to your WebSphere Application server machine. In this example, the location is C:\cc_scripts\eval_config.

Example:

```
wsadmin.bat  -username srvrid -password srvrpwd  -f
C:/cc_scripts/eval_config/setDB2variables.jacl mynode
C:/cc_scripts/eval_config C:/cc_scripts/eval_config
```

When the script completes, you should see the messages, “Saving configurations changes” and “All Done”.

UNIX, Linux and z/OS platforms:

Prior to issuing the commands below, you should copy the following files from your DB2 Server installation to the /cc_scripts/eval_config directory on your Application Server -- db2jcc.jar file, db2jcc_license_cisuz.jar, and db2jcc_license_cu.jar. Note that you will only have a db2jcc_license_cisuz.jar if your DB2 is installed on a UNIX system.

For WebSphere Application Server Network Deployment and WebSphere Application Server for z/OS, issue the commands for each node in the cell.

1. For WebSphere Application Server and WebSphere Application Server Express, type:

   cd $WAS_HOME

   For WebSphere Application Server Network Deployment and WebSphere Application Server for z/OS, type:

   cd <WAS_INSTALL_ROOT>/profiles/<nodeProfile>/bin

2. **./wsadmin.sh -username srvrid -password srvrpwd -f /cc_scripts/eval_config/setDB2variables.jacl <nodeName> <DB2UNIVERSAL_JDBC_DRIVER_PATH> <UNIVERSAL_JDBC_DRIVER_PATH>**

Where

- nodeName is the name of the node which you specified for <YOUR_NODE_NAME> when you installed WebSphere Application Server in section 3.3.2 for WebSphere Application Server and WebSphere Application Server Express. It is the node profile such as <Node1_profile> and <Node2_profile> for Network Deployment as described in section 3.4.2 for creating profiles.
- <DB2UINVERSAL_JDBC_DRIVER_PATH> is the path to the db2jcc.jar file and the db2jcc_license_cisuz.jar file which you have copied to your WebSphere Application server machine. In this example, the location is /cc_scripts/eval_config.
- <UNIVERSAL_JDBC_DRIVER_PATH> is the path to the db2jcc_license_cu.jar file which you have copied to your WebSphere Application server machine. In this example, the location is /cc_scripts/eval_config.

Example:

```
./wsadmin.sh -username srvrid -password srvrpwd -f setDB2variables.jacl
mynode /cc_scripts/eval_config /cc_scripts/eval_config
```

When the script completes, you should see the messages, “Saving configurations changes” and “All Done”.

3.4.7.3 Define WebSphere resources, UDDI policies and properties and deploy the UDDI application

This step is needed to define the necessary UDDI resources in WebSphere Application Server, to define and validate the required UDDI and WebSphere Application Server policies, properties, role mappings etc, and to deploy the UDDI application into the appropriate server.

For Network Deployment, the steps below should be executed on the node of the server where you want to set up UDDI.

Windows platform:

Ensure the Application server (and deployment manger and node agent if appropriate) are all running.

This step assumes the UDDI database is already defined and the DB2 variables are set from steps in sections 3.4.7.1 and 3.4.7.2.

1. Execute the setupCmdLine.bat for the profile in which your server is running. This is to establish the necessary environment in which to run the following commands.

   For WebSphere Application Server and WebSphere Application Server Express:

   cd %WAS_HOME%

   setupCmdLine.bat

   For WebSphere Application Server Network Deployment, type:

   cd <WAS_INSTALL_ROOT>\profiles\<nodeProfile\bin

   setupCmdLine.bat

2. Change to the cc_scripts\eval_config directory

cd C:\cc_scripts\eval_config

setupUDDI.bat <db2user> <db2pass> <db2hostname> <db2port> <dbname> <WASuser> <WASpass> <serverType> <serverName>

Where

- db2user is the db2 admin id (change to suit your environment)
- db2pass is the password for the db2 admin id (change to suit your environment)

- db2hostname is the fully qualified host name of the host that is running DB2 containing the UDDI database
- db2port is the port used by the DB2 server. On Windows machines with DB2, this port defaults to 50000.
- dbname is the name of the DB2 database created in section 3.4.7.1.
- WASuser is the WAS admin id (change to suit your environment)
- WASpass is the password for the WAS admin id (change to suit your environment)
- serverType is the type of server hosting UDDI and must be one of
  - baseserver (base single standalone server)
  - NDserver (single server in an ND cell that is not a cluster)
- serverName is the matching name for the serverType (for example, “server1”)

When the script completes, you should see the following messages:

```
SETUP SUCCEEDED
"======= UDDI INSTALLED AND SET UP SUCCESSFULLY ============"
```

UNIX, Linux and z/OS platforms:

Ensure the Application server (and deployment manger and node agent if appropriate) are all running.

This step assumes the UDDI database is already defined (see earlier step).

1. Execute setupCmdLine.sh for the profile in which your server is running. This is to establish the necessary environment in which to run the following commands.

   For WebSphere Application Server and WebSphere Application Server Express:

   cd $WAS_HOME

   . ./setupCmdLine.sh

   For WebSphere Application Server Network Deployment and WebSphere Application Server for z/OS:

   cd <WAS_INSTALL_ROOT>/profiles/<nodeProfile/bin

   . ./setupCmdLine.sh

2. Change to the cc_scripts/eval_config directory.

cd /cc_scripts/eval_config

./setupUDDI.sh <db2user> <db2pass> <db2hostname> <db2port> <dbname> <WASuser> <WASpass> <serverType> <serverName>

Where

- db2user is the db2 admin id (change to suit your environment)
- db2pass is the password for the db2 admin id (change to suit your environment)
- db2hostname is the IP name of the host that is running DB2 containing the UDDI database
- db2port is the port used by the DB2 server. On Windows machines with DB2, this port defaults to 50000.
- dbname is the name of the DB2 database created in section 3.4.7.1.
- WASuser is the WAS admin id (change to suit your environment)
- WASpass is the password for the WAS admin id (change to suit your environment)
- serverType is the type of server hosting UDDI and must be one of
  - baseserver (base single standalone server)
  - NDserver (single server in an ND cell that is not a cluster)
- serverName is the matching name for the serverType and must be

When the script completes, you should see the following messages:

```
SETUP SUCCEEDED
"======= UDDI INSTALLED AND SET UP SUCCESSFULLY ============"
```

3.4.8 Default Messaging (optional)

The following steps are required to configure the default messaging provider in the evaluated configuration. These steps are required if you plan to configure the default messaging provider in WebSphere Application Server.

Windows platform:

1. **cd %WAS_HOME%**
2. **wsadmin.bat -username srvrid -password srvrpwd -f C:/cc_scripts/eval_config/createEal4MessageBus.jacl <busName> <ieAuthUser> <ieAuthPassword>**

   Where:

<busName> - name of the messaging bus to create

<ieAuthUser> - user identity to use for inter-engine authentication

<ieAuthPassword> - password for ieAuthUser

Example: wsadmin -f C:/cc_scripts/eval_config/createEal4MessageBus.jacl msgBus ieUser ieUserPwd

When the script has completed successfully, it should display “FINISHED: Save configuration, Executing: $AdminConfig save.”

3. Stop and restart the server or cell as described in section 3.4.4.5 to enable the changes.

UNIX, Linux and z/OS platforms:

1. **cd $WAS_HOME**
2. **./wsadmin.sh -username srvrid -password srvrpwd -f /cc_scripts/eval_config/createEal4MessageBus.jacl <busName> <ieAuthUser> <ieAuthPassword>**

   Where:

   <busName> - name of the messaging bus to create

   <ieAuthUser> - user identity to use for inter-engine authentication

   <ieAuthPassword> - password for ieAuthUser

   When the script has completed successfully, it should display “FINISHED: Save configuration, Executing: $AdminConfig save.”

3. Stop and restart the server or cell as described in section 3.4.4.5 to enable the changes.

3.4.9 High Availability Manager (Network Deployment edition only)

When configuring WebSphere Application Server, Network Deployment, you may configure the High Availability Manager for a channel chain type of DCS or DCS_SECURE. The default value for the channel chain type, after WebSphere Application Server is installed, is DCS. To change the channel chain to DCS_SECURE, take the following steps.

Note: It is strongly recommended that you configure DCS_SECURE rather than DCS.

Windows platform:

1. **cd <WAS_INSTALL_ROOT>\profiles\<Dmgr_profile>\bin**
2. **wsadmin.bat -username srvrid -password srvrpwd -f C:/cc_scripts/eval_config/SetDefaultCoreGroupChain.jacl <DCS-Secure or DCS>**

Where:

<Dmgr_profile> is the name of your Deployment Manager profile

<DCS-Secure or DCS> is the value "DCS-Secure" if you want the DCS_SECURE channel chain, and is the value "DCS" to set the channel chain type to DCS.

Example:

cd C:\WebSphere\AppServer\profiles\cc_DMGR\bin

wsadmin.bat -f C:/cc_scripts/SetDefaultCoreGroupChain.jacl DCS-Secure

When the script completes, you should see a messaging indicating, "Update of DefaultCoreGroup Transport to be Channel Framework using the DCS-Secure channel chain completed successfully" if you set the channel change to DCS_SECURE or indicating "Update of DefaultCoreGroup Transport to be Channel Framework using the DCS channel chain completed successfully."

UNIX, Linux and z/OS platforms:

- **cd <WAS_INSTALL_ROOT>/profiles/<Dmgr_profile>/bin**
- **./wsadmin.sh -username srvrid -password srvrpwd -f /cc_scripts/eval_config/SetDefaultCoreGroupChain.jacl <DCS-Secure or DCS>**

Where:

<Dmgr_profile> is the name of your Deployment Manager profile

<DCS-Secure or DCS> is the value "DCS-Secure" if you want the DCS_SECURE channel chain, and is the value "DCS" to set the channel chain type to DCS.

Example:

cd /WebSphere/AppServer/profiles/cc_DMGR/bin

./wsadmin.sh -username srvrid -password srvrpwd -f /cc_scripts/eval_config/SetDefaultCoreGroupChain.jacl DCS-Secure

When the script completes, you should see a messaging indicating, “Update of DefaultCoreGroup Transport to be Channel Framework using the DCS-Secure channel chain completed successfully” if you set the channel change to DCS_SECURE or indicating “Update of DefaultCoreGroup Transport to be Channel Framework using the DCS channel chain completed successfully.”

3.4.10 Example Configuration – WebSphere Application Server Express

Description:

This is a single system configuration using a standalone installation of WebSphere Application Server Express.

Additional software:

IBM DB2 version 8.2

IBM HTTP Server

IBM HTTP Server Plug-in

Configured components:

IBM HTTP Server

IBM HTTP Server Plug-in

UDDI

Default Messaging

Instructions:

1. Install IBM Tivoli Directory Server by following the instructions in the IBM Tivoli Directory Server Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.IBMDS.doc/install.htm
2. Install IBM DB2. by following the instructions in the DB2 Information Center at http://publib.boulder.ibm.com/infocenter/db2luw/v8//index.jsp
3. Obtain WebSphere Application Server Express by following the instructions in Appendix A: How to Acquire WebSphere Application Server.
4. Install WebSphere Application Server 6.0 using instructions in section 3.3.2.

5. Install WebSphere Application Server 6.0.2 update using instructions in section 3.3.3.
6. Install WebSphere Application Server 6.0.2.3 update using instructions in section 3.3.4.
7. Install IBM HTTP server by following instructions in section 3.3.5
8. Install IBM HTTP server plug-ins by following instructions in section 3.3.6.
9. Install IBM HTTP Server update 6.0.2 by following instructions in section 3.3.7.
10. Install IBM HTTP Server plug-ins update 6.0.2 by following instructions in section 3.3.8.
11. Install IBM HTTP Server update 6.0.2.3 by following instructions in section 3.3.9.
12. Install IBM HTTP Server plug-ins update 6.0.2.3 by following instructions in section 3.3.10.
13. Install WebSphere Application Server Interim Fixes by following the instructions in section 3.3.11.
14. Configure WebSphere Application Server in the evaluated configuration by following steps in section 3.4.4.
15. Configure the IBM HTTP Server following the instructions in section 3.4.6.
16. Configure UDDI following the instructions in section 3.4.7. Use ‘baseserver’ for serverType.
17. Configure Default Messaging described in section 3.4.8.
18. Validate your WebSphere Application Server configuration as described in section 3.5.

3.4.11 Example Configuration – WebSphere Application Server

Description:

This is a single system configuration using WebSphere Application Server. Additional software included is the IBM HTTP Server and the IBM HTTP server plug-in.

Additional software:

IBM DB2

IBM WebSphere MQ

IBM HTTP Server

IBM HTTP Server Plug-in

Configured components:

IBM HTTP Server

IBM HTTP Server Plug-in

UDDI

Default Messaging

Instructions:

1. Install IBM Tivoli Directory Server by following the instructions in the IBM Tivoli Directory Server Information center at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.IBMDS.doc/install.htm
2. Install IBM DB2 by following the instructions in the IBM DB2 Information Center at http://publib.boulder.ibm.com/infocenter/db2luw/v8//index.jsp
3. Obtain WebSphere Application Server by following the instructions in Appendix A: How to Acquire WebSphere Application Server.
4. Install WebSphere Application Server 6.0 using instructions in section 3.3.2.
5. Install WebSphere Application Server 6.0.2 update using instructions in section 3.3.3.
6. Install WebSphere Application Server 6.0.2.3 update using instructions in section 3.3.4.
7. Install IBM HTTP server by following instructions in section 3.3.5
8. Install IBM HTTP server plug-ins by following instructions in section 3.3.6.
9. Install IBM HTTP Server update 6.0.2 by following instructions in section 3.3.7.
10. Install IBM HTTP Server plug-ins update 6.0.2 by following instructions in section 3.3.8.
11. Install IBM HTTP Server update 6.0.2.3 by following instructions in section 3.3.9.
12. Install IBM HTTP Server plug-ins update 6.0.2.3 by following instructions in section 3.3.10.

13. Install WebSphere Application Server Interim Fixes by following the instructions in section 3.3.11.
14. Configure WebSphere Application Server in the evaluated configuration by following steps in section 3.4.4.
15. Configure the IBM HTTP Server following the instructions in section 3.4.6.
16. Configure UDDI following the instructions in section 3.4.7. Use ‘baseserver’ for serverType.
17. Configure Default Messaging described in section 3.4.8.
18. Validate your WebSphere Application Server configuration as described in section 3.5.

3.4.12 Example Configuration – WebSphere Application Server, Network Deployment

Description:

This is a two system configuration using WebSphere Application Server Network Deployment. Additional software included is the IBM HTTP Server and the IBM HTTP server plug-in.

WebSphere servers:

Machine 1

deployment manager

nodeagent (ccNode01)

2 application servers (na1server1, na1server2)

Machine 2

nodeagent (ccNode02)

2 application servers (na2server1, na2server2)

Additional software

IBM DB2

IBM HTTP Server

IBM HTTP Server Plug-in

Configured components:

UDDI

High Availability Manager

Default Messaging

IBM HTTP Server

IBM HTTP Server Plug-in

Instructions:

1. Install IBM Tivoli Directory Server by following the instructions in the IBM Tivoli Directory Server Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.IBMDS.doc/install.htm
2. Install IBM DB2 by following the instructions in the IBM DB2 Information Center at http://publib.boulder.ibm.com/infocenter/db2luw/v8//index.jsp
3. Obtain WebSphere Application Server Express by following the instructions in Appendix A: How to Acquire WebSphere Application Server.

   Follow the instructions below to install each machine in the cell:
4. Install WebSphere Application Server 6.0 using instructions in section 3.3.2.
5. Install WebSphere Application Server 6.0.2 update using instructions in section 3.3.3.
6. Install WebSphere Application Server 6.0.2.3 update using instructions in section 3.3.4.

   Follow the instructions below to install the IBM HTTP Server and IBM HTTP Server Plug-ins on one machine in the cell:
7. Install IBM HTTP server by following instructions in section 3.3.5
8. Install IBM HTTP server plug-ins by following instructions in section 3.3.6.
9. Install IBM HTTP Server update 6.0.2 by following instructions in section 3.3.7.
10. Install IBM HTTP Server plug-ins update 6.0.2 by following instructions in section 3.3.8.
11. Install IBM HTTP Server update 6.0.2.3 by following instructions in section 3.3.9.
12. Install IBM HTTP Server plug-ins update 6.0.2.3 by following instructions in section 3.3.10.

Follow the instruction below to update each machine in the cell:

13. Install WebSphere Application Server Interim Fixes by following the instructions in section 3.3.11.

Follow the instructions below create the deployment manager and node profiles, to federate nodes, and to create application servers:

14. Create profiles for the deployment manager, application server and node agent by following instructions in section 3.4.2.

Follow the configuration instructions below on the deployment manager:

15. Configure WebSphere Application Server in the evaluated configuration by following steps in section 3.4.4.
16. Configure UDDI following the instructions in section 3.4.7. Use 'NDServer' for serverType.
17. Configure Default Messaging as described in section 3.4.8.
18. Configure HA Manager as described in section 3.4.9.

Follow the instructions below on machine where IBM HTTP Server is installed:

19. Configure the IBM HTTP Server following the instructions in section 3.4.6.
20. Validate your WebSphere Application Server configuration as described in section 3.5.

3.4.13 Example Configuration - WebSphere Application Server for z/OS

Description:

This is a single system configuration using WebSphere Application Server for z/OS.

WebSphere servers:

System 1

deployment manager

nodeagent (SY1)

1 application server (server1)

Additional software

IBM DB2 version 8.2 (on Windows)

IBM HTTP Server for z/OS 1.6 (part of z/OS operating system)

Configured components:

UDDI

High Availability Manager

Default Messaging

IBM HTTP Server for z/OS 1.6

Instructions:

1. Install IBM DB2 by following the instructions in the IBM DB2 Information Center at http://publib.boulder.ibm.com/infocenter/db2luw/v8//index.jsp.
2. Obtain WebSphere Application Server for z/OS by following the instructions in section 3.3.1.

Follow the instructions below on the deployment manager:

3. Configure WebSphere Application Server in the evaluated configuration by following steps in section 3.4.4.
4. Configure UDDI following the instructions in section 3.4.7. Use ‘NDServer’ for serverType.
5. Configure Default Messaging as described in section 3.4.8.
6. Configure HA Manager as described in section 3.4.9.
7. Validate your WebSphere Application Server configuration as described in section 3.5.

3.5 Validating the WebSphere Application Server Configuration

The following steps should be followed to ensure that the WebSphere Application Server is configured in the evaluated configuration. These steps should be run from time to time on your WebSphere Application Server installation to ensure that it remains in the “evaluated configuration.”

For WebSphere Application Server and WebSphere Application Server, Express these steps should be performed on your Application Server. For WebSphere Application Server, Network Deployment the steps should be performed on the Deployment Manager unless otherwise noted.

3.5.1 Validate the Installed version of WebSphere Application Server

You should verify that you have installed WebSphere Application Server, WebSphere Application Server, Express and WebSphere Application Server, Network Deployment at the evaluated version 6.0.2.3 with the required Ifixes according to the instructions you followed in section 3.3.

You should verify that you have installed WebSphere Application Server for z/OS at the evaluated 6.0.1 with service level 6.0.2.3 and the fix for APAR AK17408 according to the instructions in section 3.3.1.

For WebSphere Application Server, Network Deployment, the versions should be verified for all the machines in the cell, and all the machines in the cell must be at the same version level.

3.5.2 Validate your security configuration

Windows platform:

1. Start admin process (if not already started)

   For WebSphere Application Server and WebSphere Application Server, Express:

   <WAS_INSTALL_ROOT>\profiles\default\bin\startServer server1

   For WebSphere Application Server , Network Deployment:

   <WAS_INSTALL_ROOT>\profiles\<Dmgr_profile>\bin\startManager

   When this command completes, you should see a message stating "Server <serverName> open for e-business; process id is <id_number>"

2. Change to the WAS_HOME directory

   cd %WAS_HOME%

3. Validate the security configuration by typing the following command:

   wsadmin.bat -username srvrid -password srvrpwd -f C:/cc_scripts/validate_config/getConfig.jacl -profile C:/cc_scripts/eval_config/SecConfigProcs.jacl > C:/cc_scripts/validate_config/configReport.log

4. The script will query the WebSphere Application Server and save the security configuration to a configReport.log. To ensure that WebSphere Application Server conforms to the evaluated configuration continue with step 5 (below).

UNIX, Linux and z/OS platforms:

1. Start admin process (if not already started)

   For WebSphere Application Server and WebSphere Application Server, Express:

   <WAS_INSTALL_ROOT>/profiles/default/bin/startServer.sh server1

   For WebSphere Application Server, Network Deployment and z/OS:

   <WAS_INSTALL_ROOT>/profiles/<Dmgr_profile>/bin/startManager.sh

   When this command completes, you should see a message stating “Server <serverName> open for e-business; process id is <id_number>”

2. Change to the WAS_HOME directory

   cd $WAS_HOME

3. Validate the security configuration by typing the following command:

   ./wsadmin.sh -username srvrid -password srvrpwd -f /cc_scripts/validate_config/getConfig.jacl -profile /cc_scripts/eval_config/SecConfigProcs.jacl > /cc_scripts/validate_config/configReport.log

4. The script will query the WebSphere Application Server and save the security configuration to a configReport.log. To ensure that WebSphere Application Server conforms to the evaluated configuration, continue with step 5 (below).

Windows, UNIX, Linux and z/OS platforms:

5. To ensure that WebSphere Application Server conforms to the evaluated configuration, open the log file and verify that each section of the log contains the values as specified in the table below:

Configuration parameter	Required value
Security Config	
Global Security Enabled	true
Java 2 Security	true
Active Authentication Mechanism	This value must indicate LTPA and SWAM must not be specified. For example: `cells/cceal4Cell|security.xml#`**`LTPA`**`_1`
Single Signon enabled	true
Active Authentication Protocol	CSI
CSI Inbound Authentication	This value may vary.

Configuration parameter	Required value
BasicAuth	
CSI Inbound Authentication Transport	This value may vary.
CSI Inbound Authentication Attribute propagation enabled	true
Active User Registry	For WebSphere Application Server, WebSphere Application Server, Express and WebSphere Application Server, Network Deployment, this value must indicate th LDAP user registry and not the local OS registry or custom. For example: cells/cceal4Cell|security.xml#**LDAPUserRegistry**_1 For WebSphere Application Server for z/OS, this value must indicate the Local OS User Registry. For example: cells/PLEX1Network|security.xml#**LocalOSUserRegistry**
Attribute ignoreCase (applies to z/OS product only)	true
Attribute com.ibm.security.SAF.authorization (applies to z/OS product only)	false
Attribute com.ibm.security.SAF.delegation (applies to z/OS product only)	false
Administrative Connectors	
preferredConnector	This value must be RMI for each server and node agent listed. No SOAP connections are allowed. For example: cells/cceal4Cell/nodes/ccNode01/servers/na1server1|server.xml#**RMIConnector**_1138827141846
connectors	This value must be RMI for each server and node agent listed. No SOAP connections are allowed. For example: cells/cceal4Cell/nodes/ccNode01/servers/na1server1|server.xml#**RMIConnector**_1138827141846
Cells	
	Only a single cell should be listed. Multiple cells are not

Configuration parameter	Required value
	supported. For example: `cceal4Cell(cells/cceal4Cell|cell.xml#Cell_1)`
TAInterceptors	
	Only the following trust association interceptors may appear in the list: o A trusted trust association interceptor o A certified trust association interceptor
JMS Providers	
	Only the following providers may appear in the list: o WebSphere JMS Provider o WebSphere MQ JMS Provider o A trusted JMS Provider o A certified JMS Provider
URL Providers	
	Only the following URL provider may appear in the list: o Default URL Provider o A Trusted URL Provider o A Certified URL Provider
J2C Resource Adapters	
	Only the following J2C Resource Adapters may appear ir the list: o SIB JMS Resource Adapter o WebSphere Relational Resource Adapter o A Trusted Resource Adapter o A Certified Resource Adapter
Mail providers	
	Only the following mail providers may appear in the list: o Built-in Mail Provider o A Trusted Mail Provider o A Certified Mail Provider
JDBC Resource Providers	

Configuration parameter	Required value
	Only the following JDBC resource providers may appear in the list: ○ Cloudscape JDBC Provider ○ UDDI DB2 JDBC Provider ○ DB2Driver ○ A Trusted JDBC Provider ○ A Certified JDBC Provider
JACC Providers	
	This section should specify, “JACC Provider not enabled”
JAAS Login Modules	
	Only the following JAAS Login Modules should be listed: ○ Client container ○ DefaultPrincipalMapping ○ WSLogin ○ DEFAULT ○ LTPA ○ LTPA_WEB ○ RMI_INBOUND ○ RMI_OUTBOUND ○ SWAM ○ WEB_INBOUND ○ wssecurity.IDAssertion ○ wssecurity.IDAssertionUsernameToken ○ wssecurity.PKCS7 ○ wssecurity.PkiPath ○ wssecurity.Signature ○ wssecurity.UsernameToken ○ wssecurity.X509BST For WebSphere Application Server for z/OS the modules

Configuration parameter	Required value
	below should be listed in addition to those above: o SWAM_ZOSMAPPING o ICSF
LTPA Token Factories	

	Only the following token factories may be listed.
	`com.ibm.ws.security.ltpa.LTPATokenFactory |`
	`com.ibm.ws.security.ltpa.LTPAToken2Factory |`
	`com.ibm.ws.security.ltpa.AuthzPropTokenFactory`

High Availability Manager **(applicable to Network Deployment only)**	
DefaultCoreGroup Name	DefaultCoreGroup
Transport Type	CHANNEL_FRAMEWORK
Channel Chain name	The value must be one of the following: o DCS o DCS_SECURE
Installed User Applications	
	No user applications must be listed other than o The UDDI Registry application (applicable if the UDDI component is configured. The lo should show the UDDI application is installed on only one Application Server in the cell) o Trusted Applications o Certified Applications
Active Ports	
Deployment Manager Ports (applicable to WebSphere Application Server, Network Deployment and WebSphere Application Server for z/OS)	Only the following ports may be listed: o CELL_DISCOVERY_ADDRESS o BOOTSTRAP_ADDRESS o ORB_LISTENER_ADDRESS o DCS_UNICAST_ADDRESS

Configuration parameter	Required value
	o WC_adminhost_secure For WebSphere Application Server, Network Deployment, the following ports may be present: o CSIV2_SSL_MUTUALAUTH_LISTENER o CSIV2_SSL_SERVERAUTH_LISTENER For WebSphere Application Server for z/OS, the following port may be present: o ORB_SSL_LISTENER_ADDRESS
Node Agent Ports (applicable to WebSphere Application Server, Network Deployment and WebSphere Application Server for z/OS)	Only the following ports may be listed: o BOOTSTRAP_ADDRESS o ORB_LISTENER_ADDRESS o DCS_UNICAST_ADDRESS o NODE_DISCOVERY_ADDRESS o NODE_IPV6_MULTICAST_DISCOVERY o NODE_MULTICAST_DISCOVERY_ADDRESS WebSphere Application Server, Network Deployment, the following ports may be present: o CSIV2_SSL_MUTUALAUTH_LISTENER o CSIV2_SSL_SERVERAUTH_LISTENER For WebSphere Application Server for z/OS, the following port may be present: o ORB_SSL_LISTENER_ADDRESS
Application Server ports	Only the following ports may be listed: o BOOTSTRAP_ADDRESS o ORB_LISTENER_ADDRESS o DCS_UNICAST_ADDRESS o WC_defaulthost

Configuration parameter	Required value
	○ WC_defaulthost_secure ○ SIB_ENDPOINT_SECURE_ADDRESS ○ SIB_MQ_ENDPOINT_ADDRESS (Note: applicable only if WebSphere MQ is configured) ○ SIB_MQ_ENDPOINT_SECURE_ADDRESS (Note: applicable only if WebSphere MQ is configured) For WebSphere Application Server, WebSphere Application Server, Express and WebSphere Application Server, Network Deployment, the following ports may be present: ○ CSIV2_SSL_MUTUALAUTH_LISTENER ○ CSIV2_SSL_SERVERAUTH_LISTENER For WebSphere Application Server for z/OS, the following port may be present: ○ ORB_SSL_LISTENER_ADDRESS

3.5.3 Validate that System Applications have been removed

To validate that the WebSphere Application Server is in the evaluated configuration for system applications, take the following steps.

Windows, UNIX, Linux and z/OS platforms:

1. Locate the systemapps.xml file in your WebSphere Application Server installation.

For WebSphere Application Server and WebSphere Application Server, Express standalone application servers, locate the systemapps.xml file the following directory

<WAS_INSTALL_ROOT>\profiles\default\config\cells\<YOUR_CELL_NAME>

\nodes\<YOUR_NODE_NAME>\

For WebSphere Application Server, Network Deployment edition, locate the systemapps.xml file in the following directory

<WAS_INSTALL_ROOT>\profiles\<Dmgr_profile>\config\cells\<YOUR_CELL_NAME>\nodes\<YOUR_NODE_NAME>\

2. Edit systemapps.xml

For WebSphere Application Server and WebSphere Application Server, Express standalone application servers, verify that there are no sections in the file indicating “ <deployedApplications>”. For example, you should see:

```
<?xml version="1.0" encoding="UTF-8"?>
<serverindex:ServerIndex xmi:version="2.0" xmlns:xmi="http://www.omg.org/XMI"
        xmlns:serverindex="http://www.ibm.com/websphere/appserver/schemas/5.0/serverindex
        .xmi" xmi:id="ServerIndex_1138571513625">
  <serverEntries xmi:id="ServerEntry_1138571513656" serverName="server1"
        serverType="APPLICATION_SERVER"/>
```

For WebSphere Application Server Network Deployment and WebSphere Application Server for z/OS verify that only the “filetransferSecured.ear” application is listed for the <deployedApplications> section as follows:

```
<deployedApplications>/usr/WebSphere/AppServer/systemApps/filetransferSecured.ear</depl
        oyedApplications>
```

3.5.4 Validate your IBM HTTP Server configuration

Note: this step does not apply to WebSphere Application Server for z/OS.

If you have configured the IBM HTTP Server with WebSphere Application Server, WebSphere Application Server, Express or for WebSphere Application Server, Network Deployment, then issue the following commands to verify that the IBM HTTP Server is in the evaluated configuration.

Windows platform:

1. Type the following command to inspect the IBM HTTP Server configuration and display the result.

- **cd <IHS_INSTALL_ROOT>_jvm\jre\bin\**
- **java -classpath C:/cc_scripts/validate_config EAL4Verify “<IHS_INSTALL_ROOT>/conf/httpd.conf”**

  Example: java –classpath C:/cc_scripts/validate_config EAL4Verify “C:/IBMHTTPServer/conf/httpd.conf”

  If the IBM HTTP Server is in the evaluated configuration, you should see the message, “SUCCESS: System conforms to required EAL4 configuration”

UNIX and Linux platforms:

1. Type the following command to inspect the IBM HTTP Server configuration and display the result.

- **cd <IHS_INSTALL_ROOT>/_jvm/jre/bin**
- **java -classpath /cc_scripts/validate_config EAL4Verify "<IHS_INSTALL_ROOT>/conf/httpd.conf"**

  Example: java –classpath /cc_scripts/validate_config EAL4Verify "/IBMHTTPServer/conf/httpd.conf"

  If the IBM HTTP Server is in the evaluated configuration, you should see the message, "SUCCESS: System conforms to required EAL4 configuration"

3.5.5 Validate your Default Messaging Provider configuration

If you have configured the Default Messaging Provider, issue the following commands to verify the default messaging provider is in the evaluated configuration.

Windows platform:

1. Type the following command to inspect the messaging configuration and create the messaging_validation.log file with the results.
   - **cd %WAS_HOME%**
   - **wsadmin.bat -username srvrid -password srvrpwd -f C:/cc_scripts/validate_config/validateEal4MessageBus.jacl <BUS_NAME> <IE_AUTH_USER> <YOUR_CELL_NAME>/IntEngAlias > C:/cc_scripts/validate_config/messaging_validation.log**

   Where <BUS_NAME> is the name of the messaging bus, <IE_AUTH_USER> is the name of the identity to use for Inter-engine authentication, and <YOUR_CELL_NAME>/IntEngAlias is the name of the Inter-engine authentication alias.

   Example:

   wsadmin.bat -username srvrid -password srvrpwd -f C:/cc_scripts/validate_config/validateEal4MessageBus.jacl msgBus msgsys CCNode01Cell/IntEngAlias > C:/cc_scripts/validate_config/messaging_validation.log
2. Edit the log file, messaging_validation.log, and verify that steps 1-4 show that they PASSED and that the following confirmation is displayed at the bottom of the file,

```
**********************************************
*                                            *
* FINISHED: Configuration PASSED validated  *
*                                            *
**********************************************
```

UNIX, Linux and z/OS platforms:

3. Type the following command to inspect the messaging configuration and create the messaging_validation.log file with the results.

   - **cd $WAS_HOME**
   - **./wsadmin.sh -username srvrid -password srvrpwd -f /cc_scripts/validate_config/validateEal4MessageBus.jacl <BUS_NAME> <IE_AUTH_USER> <YOUR_CELL_NAME>/IntEngAlias > /cc_scripts/validate_config/messaging_validation.log**

   Where <BUS_NAME> is the name of the messaging bus, <IE_AUTH_USER> is the name of the identity to use for Inter-engine authentication, and <YOUR_CELL_NAME>/IntEngAlias is the name of the Inter-engine authentication alias.

   Example:

   ```
   ./wsadmin.sh -username srvrid -password srvrpwd -f
   /cc_scripts/validate_config/validateEal4MessageBus.jacl msgBus msgsys
   CCNode01Cell/IntEngAlias
   >/cc_scripts/validate_config/messaging_validation.log
   ```

4. Edit the log file, messaging_validation.log, and verify that steps 1-4 show that they PASSED and that the following confirmation is displayed at the bottom of the file,

   ```
   **********************************************
   *                                            *
   * FINISHED: Configuration PASSED validated  *
   *                                            *
   **********************************************
   ```

3.5.6 Validate your UDDI configuration

If you have configured the UDDI Registry, issue the following commands to verify that UDDI is in the evaluated configuration.

Windows platform:

1. Type the following command to inspect the messaging configuration and create the uddi_validation.log file with the results

   - Change to the directory to issue the validate command based on the product you have installed.

For WebSphere Application Server and WebSphere Application Server Express:

cd %WAS_HOME%

For WebSphere Application Server Network Deployment, change to the profile directory of the node where UDDI is installed:

cd <WAS_INSTALL_ROOT>\profiles\<nodeProfile>\bin

- **wsadmin.bat -username srvrid -password srvrpwd -f C:/cc_scripts/validate_config/CheckUDDISetup.jacl > C:/cc_scripts/validate_config/uddi_validation.log**

2. Edit the log file, uddi_validation.log, and verify that the following is displayed at the bottom of the log file:

UDDI SETUP CHECK COMPLETE

UNIX, Linux, and z/OS platforms:

1. Type the following command to inspect the messaging configuration and create the uddi_validation.log file with the results

- Change to the directory to issue the validate command based on the product you have installed.

For WebSphere Application Server and WebSphere Application Server Express:

cd $WAS_HOME

For WebSphere Application Server Network Deployment and WebSphere Application Server for z/OS, change to the profile directory of the node where UDDI is installed:

cd <WAS_INSTALL_ROOT>/profile/<nodeProfile>/bin

- **./wsadmin.sh -username srvrid -password srvrpwd -f /cc_scripts/validate_config/CheckUDDISetup.jacl > /cc_scripts/validate_config/uddi_validation.log**

2. Edit the log file, uddi_validation.log, and verify that the following is displayed at the bottom of the log file:

UDDI SETUP CHECK COMPLETE

4 Administrator’s Guide for the Certified System

This section defines the guidelines and restrictions with which a trusted administrator must comply. A trusted administrator is an administrator who is trusted to start up and manage the certified system.

4.1 Ensuring the Operating System Environment is Secure

The administrator is responsible for ensuring the operating system environment is secure. The administrator must do the following before starting the certified system:

- For all platforms except for z/OS, ensure that no other applications are running on the operating system in which a WebSphere Application Server is started. For the z/OS platform, ensure that only trusted applications are running on the operating system in which a WebSphere Application Server is started.
- Do not run untrusted Java applets in the operating system in which a WebSphere Application Server is started.
- If users are configured to identify themselves to any of the remote interfaces of WebSphere Application Server using a user ID and password, use the user registry functions of the operating system to configure a restrictive password policy.
- Ensure that the operating system provides access control functions, or that access control functions are available, to protect the operating system file system. Use these access control functions to protect the WebSphere Application Server files (configuration files, log files, library files, command files, and naming directory file) so that they can be accessed only by authorized administrators and applications of the certified system.
- If using WebSphere Application Server for z/OS, use the access control functions of z/OS to protect the user registry data stored in the z/OS user registry. Also, if storing passwords in the user registry, use the password strength policy ohe operating system to protect the strength of these passwords.
- Be sure that no other resources on the system use the same incoming ports that the certified system is using.
- Ensure that data transferred between workstations is secured from disclosure, interruption or tampering.

- Ensure that after a system failure or other discontinuity that recovery is obtained without a compromise to security.

4.2 Ensuring the User Registry in LDAP is Secure

If using the WebSphere Application Server, WebSphere Application Server Express, or WebSphere Application Server Network Deployment, the administrator must store the user registry for WebSphere Application Server in the Tivoli Directory Server.

The administrator must use the utilities provided by Tivoli Directory Server to do the following:

- Protect all user registry data stored in the LDAP directory so that this data can be accessed only by trusted administrators.
- Configure a password strength policy so that users can store only strong passwords in the LDAP directory.

making sure a facility is available for protecting the data stored in the LDAP server and, if user registry data in the LDAP server and for using this fathat the LDAP server product providesof a user registry is stored in LDAP directory.

4.3 Starting the WebSphere Application Server Components

The administrator must ensure that the following procedures are used to startup the WebSphere Application Server components:

- Before startup, make sure all components are in the evaluated configuration, as described in section 2.2 of this document.
- Use only the startServer command to start the Application Server(s) and, if configured, the Node Agent(s), and Deployment Manager. Do not start any of these components in the debug mode.

4.4 Managing the System

The administrator must adhere to the following general restrictions when managing the WebSphere Application Server components:

- Perform all management tasks using the wsadmin interfaces. The AdminConsole is not supported in the evaluated configuration and must not be installed.
- Do not change any security attributes during runtime except for the attributes described in Section 2.3.4 of this document. To change these attributes, use only the evaluated interfaces, which are described in Section 4.5 and Section 4.6 of this document.

- When it is necessary to change the password for the WebServer server user ID, the LTPA key, or the Inter-engine Authentication Alias, this must be done when the certified system is down.
- Do not make any changes that prevent the components of the certified system from being in the evaluated configuration, as described in section 2.2 of this document.
- Do not use the waslogbr command. This starts the WebSphere Application Server Log Analyzer tool, which is not supported in the evaluated configuration.
- Do not use the configureIIS command. This configures the Microsoft Internet Information Services (IIS) web server which is not supported in the evaluated configuration.
- On WebSphere Application Server for z/OS, CSIv2 must not be configured to support client certificate authentication.

In addition, the administrator must abide by the additional restrictions described in the subsections that follow.

4.4.1 Deploying Applications

When deploying applications, the administrator must following the following guidelines and restrictions:

- Do not deploy any applications into the certified system except for those that are supported in the evaluated configuration. (See Section 2.2 of this document.) Note that, with the exception of the UDDI application, all of the applications provided by WebSphere Application Server are not supported in the evaluated configuration and must not be deployed. For example, the following applications are provided by WebSphere Application Server but are not supported in the evaluated configuration and must not be deployed:
  - CacheMonitor.ear
  - WebSphereTP.ear
  - Query.ear
  - IvtApp.ear
  - DefaultApplication.ear
  - PerfServletApp.ear
- Before deploying applications with startup beans, the administrator must ensure the application developer has adhered to the guidelines documented in section 5.4. During deployment, the administrator must ensure that the

user that is mapped to the security role for the startup beans Start() and Stop() methods is mapped to the run-as role for the “Server user id”.

- Note that a trusted application can be deployed into the certified system. Before deploying a trusted application, verify the trustworthiness of the application. For an application to be trusted, the developer of the application must have adhered to all the guidelines described in Section 5 of this document.
- Note that a certified application can be deployed into the certified system. Before deploying a certified application into the certified system, verify that the application has the correct type of certification. The application must have been certified at a Common Criteria EAL4 or higher level of assurance to run in the certified system environment described in this document.

4.4.2 Managing Web Services

If web services are configured, the administrator must abide by the following restrictions:

- Do not configure the Web Services Gateway. The Web Services Gateway is not supported in the evaluated configuration. Only the web services endpoints (interfaces) to methods enterprise beans are supported, which are described in the following documentation:.

  http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/welc6tech_wbs.html
- Use only Rational Application Developer tool to configure the web services endpoints.
- Ensure that only the HTTP (and not the JMS transport) is configured for each web service endpoint. The JMS transport for a web service endpoint is not supported in the evaluated configuration.
- If configuring identification for the web services endpoint, only the configuration parameters identified in the following table are supported:

Identification token type	**Asserted identity?**	**Trust token required?**	**Trust token type**
username token containing user ID	yes	yes	user name token containing user ID and password
user name token containing user ID and password	no	no	not applicable
X509 token	no	no	not applicable

containing client certificate			
LTPA token	no	no	not applicable

4.4.3 Managing the JDBC Providers

If JDBC providers are configured, the administrator must abide by the following restrictions:

- Do not configure a JDBC provider for the “Cloudscape Network Server using Universal JDBC Driver”, and do not issue the “start networkServer” command.
- Do not configure any JDBC providers for the MicroSoft SQL Server database.

4.4.4 Managing the UDDI Application

If the UDDI application is configured, the administrator must abide by the following restrictions:

- Do not install the UDDI administrative component (v3gui.war) as part of the UDDI application.

4.4.5 Enabling WebSphere Application Server components and services

The following functions in WebSphere Application Server are installed with the product, but are disabled by default. The administrator must not enable or configure any of these components and services:

- Activity session service – do not enable this service
- Request metrics – do not enable
- Proxy server – a proxy server should not be created or started
- Data Replication service – do not enable this service
- Work area component – do not create a work area
- Edge Server Dynamic Cache adapter – do not configure a dynamic cache external cache group
- Compensation Scoping Service – do not enable this service

4.4.6 Managing the Default Messaging Provider

If the Default Messaging Provider (optional) is configured, the administrator must following the guidelines below:

- The “AllAuthenticated” group must not be assigned the Bus Connector role. Users and groups of users should explicitly be granted permission to connect to the messaging bus.
- It is required that the “AllAuthenticated” group be removed from the default bus security policy. This prevents the accidental granting of permissions to messaging resources of any user that can connect to the bus.
- The IdentityAdoptor role type must not be assigned for any messaging resource.
- The definition of Foreign buses are not permitted. A foreign bus definition is used to send messages between different message buses. Since only one messaging bus may be configured, the definition of a foreign bus is not permitted.
- Service and port destinations are used for used for web service messaging. Web service messaging in a messaging bus is not allowed, therefore the definition of these types of destinations is not permitted
- Foreign destinations are used to define messaging resources on other messaging buses. Since only one messaging bus is permitted, the configuration of foreign destinations is prohibited.
- The Everyone group must not be assigned to any messaging resource.
- The topic level access flag must be set to true.
- Alias destinations are used to provide a level of indirection between a messaging resource used by an application and the actual messaging resource that exists on a bus. Alias destinations must not be defined.

4.5 Supported Interfaces for Managing Security Attributes - General

The section describes all of the interfaces that are supported in the evaluated configuration for managing security attributes except for the interfaces that pertain to the Default Messaging Provider. The interfaces that pertain to the Default Messaging Provider are described in section 4.6 of this document.

An administrator can use the interfaces described in this section to manage the following attributes:

- Mappings of IDs to administration roles
- Mappings of IDs to naming roles
- Mappings of IDs to application roles
- Registration of UDDI publishers

- Mappings to run-as roles

Note: The mappings of IDs to roles for the UDDI application must be configured as specified in the evaluated configuration. Do not change these mappings.

4.5.1 Configuring Mappings to Administration and Naming Roles

The administrator is responsible for verifying that the mappings of IDs to administration and naming roles are correct and for making any required modification to these mappings. The administrator can view and modify the mappings to the administration and naming roles using the AdminConfig interface. To modify the mappings to the administration roles, the administrator must be in the Administrator role. To modify the mappings to the naming roles, the administrator must be in the Administrator or Configurator role.

The syntax for AdminConfig is as follows:

```
Wsadmin>$AdminConfig <action>
(cells/<cell>|<xmlfile>#<roleAssignment>)
{users {{{name <userid1>} {name <userid2>}}}}
{groups {{{name <group1>} {name <group2>}}}}
```

Where

<action> is modify, show or remove

<cell> is the name of the cell

<xmlfile> is either admin-authz.xml or naming-authz.xml

<roleAssignment> is the accessId of the role to be mapped to

<userid1> is the first userid to map to the role

<userid2> is the second userid to map to the role

<group1> is the first group to map to the role

<group2> is the second group to map to the role

The following are examples of using wsadmin to view and configure the mappings of IDs to administration and naming roles.

4.5.1.1.1 Viewing roles that are available for mapping

The following interface can be used to view roles available for mapping:

Wsadmin>$AdminConfig show (cells/<cell>|<xmlfile># <roleAssignment>)

4.5.1.1.2 Administration Mapping

The following are examples of how to configure the mappings of user/group IDs to the administration roles. To delete mappings, specify remove rather than modify.

Mapping userid to administrator role:

```
Wsadmin>$AdminConfig modify (cells/<cell>|admin-
authz.xml#RoleAssignmentExt_1) {users {{{name <userid>}}}}
```

Mapping userid to operator role:

```
Wsadmin>$AdminConfig modify (cells/<cell>|admin-
authz.xml#RoleAssignmentExt_2) {users {{{name <userid>}}}}
```

Mapping userid to configurator role:

```
Wsadmin>$AdminConfig modify (cells/<cell>|admin-
authz.xml#RoleAssignmentExt_3) {users {{{name <userid>}}}}
```

Mapping userid to monitor role:

```
Wsadmin>$AdminConfig modify (cells/<cell>|admin-
authz.xml#RoleAssignmentExt_4) {users {{{name <userid>}}}}
```

Mapping group to administrator role:

```
Wsadmin>$AdminConfig modify (cells/<cell>|admin-
authz.xml#RoleAssignmentExt_1) {groups {{{name <group>}}}}
```

Mapping group to operator role:

```
Wsadmin>$AdminConfig modify (cells/<cell>|admin-
authz.xml#RoleAssignmentExt_2) {groups {{{name <group>}}}}
```

Mapping group to configurator role:

```
Wsadmin>$AdminConfig modify (cells/<cell>|admin-
authz.xml#RoleAssignmentExt_3) {groups {{{name <group>}}}}
```

Mapping group to monitor role:

```
Wsadmin>$AdminConfig modify (cells/<cell>|admin-
authz.xml#RoleAssignmentExt_4) {groups {{{name <group>}}}}
```

4.5.1.1.3 Naming Mapping

The following are examples of how to configure the mappings of user/group IDs to the naming roles. To delete attributes, specify remove rather than modify.

Mapping userid to CosNamingRead role:

```
Wsadmin>$AdminConfig modify (cells/<cell>|naming-
authz.xml#RoleAssignmentExt_1) {users {{{name <userid>}}}}
```

Mapping userid to CosNamingWrite role:

```
Wsadmin>$AdminConfig modify (cells/<cell>|naming-
authz.xml#RoleAssignmentExt_2) {users {{{name <userid>}}}}
```

Mapping userid to CosNamingCreate role:

```
Wsadmin>$AdminConfig modify (cells/<cell>|naming-authz.xml#RoleAssignmentExt_3) {users {{{name <userid>}}}}
```

Mapping userid to CosNamingDelete role:

```
Wsadmin>$AdminConfig modify (cells/<cell>|naming-authz.xml#RoleAssignmentExt_4) {users {{{name <userid>}}}}
```

Mapping group to CosNamingRead role:

```
Wsadmin>$AdminConfig modify (cells/<cell>|naming-authz.xml#RoleAssignmentExt_1) {groups{{{name <group>}}}}
```

Mapping group to CosNamingWrite role:

```
Wsadmin>$AdminConfig modify (cells/<cell>|naming-authz.xml#RoleAssignmentExt_2) {groups {{{name <group>}}}}
```

Mapping group to CosNamingCreate role:

```
Wsadmin>$AdminConfig modify (cells/<cell>|naming-authz.xml#RoleAssignmentExt_3) {groups {{{name <group>}}}}
```

Mapping group to CosNamingDelete role:

```
Wsadmin>$AdminConfig modify (cells/<cell>|naming-authz.xml#RoleAssignmentExt_4) {groups {{{name <group>}}}}
```

4.5.1.1.4 Saving Mapping Changes

To save the mapping changes, the following interface should be used:

```
Wsadmin>$AdminConfig save
```

4.5.1.1.5 Removing Mapping Information

To remove mapping information, the following interface can be used:

```
Wsadmin>$AdminConfig remove <userid> (cells/<cell>|<xmlfile>#<roleAssignment>)
```

4.5.2 Configuring Mappings to Application Roles

The administrator is responsible for verifying that the mappings of IDs to the roles used in web server applications and in enterprise beans are correct and for making any required modification to these mappings. The administrator can view , edit, or delete the mappings to the application roles using the AdminApp interface. To edit or delete the mappings, the administrator must be in the Administrator or Configurator role.

To view the mappings to application roles, the following interface can be used:

```
Wsadmin>$AdminApp view <application_name>
```

Where < application_name > is the application name

To add the mappings to application roles, the following interface can be used:

```
Wsadmin>$AdminApp edit <application_name>  -MapRolesToUsers
{{<Role_name> No Yes <user | group>}}
```

Where <application_name> is the name of the application

<Role_name> is the name of the role to map the user/group ID to

No Indicates to allow access to everyone (yes/no)

Yes Indicates to allow access to all authenticated users (yes/no)

<user | group> is the user and/or group IDs to map to the role

To delete the mappings to application roles, the following interface can be used:

```
Wsadmin>$AdminApp deleteUserAndGroupEntries <application_name>
```

Where <application_name> is the name of the application

4.5.3 Configuring the Registration of UDDI Publishers

The administrator is responsible for verifying that the registration of IDs as UDDI Publishers is correct and for making any required modification to these registrations. The administrator can view, edit, or delete the registrations of UDDI Publishers using the AdminControl interface. To edit or delete the registrations, the administrator must be in the Administrator or Operator role.

To view the registration of UDDI Publishers, the following interface can be used:

```
$AdminControl invoke_jmx [$AdminControl makeObjectName [$AdminControl
queryNames WebSphere:type=UddiNode,*]] getUserInfos [java::new
{java.lang.Object[]} 0] [java::new {java.lang.String[]} 0]
```

To register a user ID as a UDDI Publisher, the following interface can be used:

```
$AdminControl invoke_jmx [$AdminControl makeObjectName [$AdminControl
queryNames WebSphere:type=UddiNode,*]]  createUddiUser $params $sigs
```

Where $params is set as follows:

```
set params [java::new {java.lang.Object[]} 1]
$params set 0 $uddiUser
```

Where $sigs is set as follows:

```
set sigs [java::new {java.lang.String[]} 1]
$sigs set 0 com.ibm.uddi.v3.management.UddiUser
```

Where $uddiUser is set as follows:

set uddiUser [java::new com.ibm.uddi.v3.management.UddiUser <userID> [java::new com.ibm.uddi.v3.management.TierInfo 1] [java::new java.util.LinkedList]]

Where <userID> is the user ID to register as a UDDI Publisher

To delete a user ID as a UDDI Publisher, the following interface can be used:

$AdminControl invoke_jmx [$AdminControl makeObjectName [$AdminControl queryNames WebSphere:type=UddiNode,*]] deleteUddiUser $params $sigs

Where $params is set as follows:

set params [java::new {java.lang.Object[]} 1]

$params set 0 <userID>

Where $sigs is set as follows:

set sigs [java::new {java.lang.String[]} 1]

$sigs set 0 java.lang.String

Where <userID> is the user ID to delete as a UDDI Publisher

4.5.4 Configuring the Mappings to Run-As Roles

The administrator is responsible for verifying that the mappings of IDs to the run-as roles used in web server applications and in enterprise beans are correct and for making any required modification to these mappings. The administrator can view, edit, or delete the mappings to the application run-as roles using the AdminApp interface. To edit or delete the mappings, the administrator must be in the Administrator or Configurator role.

To view the mappings to application run-as roles, the following interface can be used:

Wsadmin>$AdminApp view <application_name>

Where < application_name > is the application name

To add the mappings to application run-as roles, the following interface can be used:

Wsadmin>$AdminApp edit <application_name> -MapRunAsRolesToUsers {{<Role_name> <user> <password>}}

Where <application_name> is the name of the application

<Role_name> is the name of the role to map the user ID to

<user> is the user ID to map to the role

<password> is the password for the user ID specified

To delete the mappings to application run-as roles, the following interface can be used:

Wsadmin>$AdminApp deleteUserAndGroupEntries <application_name>

Where <application_name> is the name of the application

Note: The ID and password is stored in a WebSphere Application Server configuration file. Be sure that the access control function of your operating system is used to protect all WebSphere Application Server configuration files.

4.6 Supported Interfaces for Security Attributes of the Default Messaging Provider

The section describes all of the interfaces that are supported in the evaluated configuration for managing the security attributes of the Default Messaging Provider.

4.6.1 Configuring Messaging Permissions

The administrator is responsible for verifying that the messaging security policy is correct and making any required modifications to the policy. The administrator can view and modify the security policy for a bus using the supported scripting interface. To modify the messaging security policy, the administrator must be in the Administrator or Configurator role. Prior to defining a security policy for a messaging bus, it must exist; however it is possible, and advisable, to configure destination permissions before creating the destination.

For all messaging commands discussed in this document, `busName` is the name of the configured messaging bus, `userName` is the name of a user and `groupName` is the name of a user group. The `destName` and `destType` parameters identify the name and type of destination that an operation uses, `destType` can be one of the following values:

Destination Types	Description
Queue	A destination used for point to point messaging
Topicspace	A destination used for publish/subscribe messaging
Alias	An alias to another destination Note: Use of this destination type is not permitted in the TOE for EAL4.
Foreign	An destination that exists on another bus Note: Use of this destination type is not permitted in the TOE for EAL4.

A `topicName` parameter is used to identify a topic on which an operation is to be performed. Note that topics are hierarchical, for example the topic “Shares” could contain a subtopic called “NASDAQ”, the fully qualified name of the subtopic would be “/Shares/NASDAQ”. The slash ('/') character is used to indicate branches in the topic heirarchy.

The `roletype` parameter is used to indicate the role type that the operation is to be performed with, one of the following can be used:

Role Types	**Description**
Creator	Role required to permit the user to create temporary destinations within the namespace defined by using the name of the specified destination as a prefix.
Sender	Role required to permit the user to send a message to a resource (e.g. a Queue, a TopicSpace)
Receiver	Role required to permit the user to receive a message from a resource (e.g. a Queue, a Topic Space)
Browser	Role required to permit the user to browse a message on a resource (e.g. a Queue)
IdentityAdopter	Role required to permit the user to use another's identity to perform operations on a resource (e.g. a Queue, a Topic Space) Note: Use of this role is not permitted in the TOE for EAL4.

The following table contains a summary of which roles may be configured for each of the entities in the authorization policy (‘X’ indicates roles supported in the TOE, ‘(X)’ indicates roles prohibited in the TOE):

	Local bus	Foreign bus	Queue	Topic space	Alias	Foreign destination	Default	Topic space root	Topic
Bus connector	X								
Sender		(X)	X	X	(X)	(X)	X	X	X
Receiver			X	X	(X)		X	X	X
Browser			X		(X)		X		
Creator			X				X		
IdentityAdopter		(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)

Additional information can be obtained in the online “WebSphere Application Server V6.0 Information Center” at : http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp

The wsadmin `$AdminTask help commandName` online help can also be used to obtain additional information. The `commandName` parameter is the name of the command you want information about.

4.6.2 Configuring Bus Connector Permissions

The bus connector permission enables users to connect to a messaging bus. By default, the group “AllAuthenticated” is assigned to the bus connector role. This means that, by default, any user that can be authenticted is allowed to connect to the messaging bus. In order to remain in the TOE, the administrator must remove the “AllAuthenticated” group and explicitly assign groups and users to this role. The following commands are used to view and modify users that are assigned the Bus Connector role:

To view users assigned to the bus connector role:

```
$AdminTask listUsersInBusConnectorRole {-bus busName}
```

To view groups assigned to the bus connector role:

```
$AdminTask listGroupsInBusConnectorRole {-bus busName}
```

To assigned a user to the bus connector role:

```
$AdminTask addUserToBusConnectorRole {-bus busName -user userName}
```

To assign a group to the bus connector role:

```
$AdminTask addGroupToBusConnectorRole {-bus busName -group 
groupName}
```

To remove a user from the bus connector role:

```
$AdminTask removeUserFromBusConnectorRole {-bus busName -user 
userName}
```

To remove a group from the bus connector role:

```
$AdminTask removeGroupFromBusConnectorRole {-bus busName -group 
groupName}
```

4.6.3 Configuring the Default Security Policy for a Bus

A messaging bus has a default security policy. All destinations inherit the default security policy, unless destination inheritance is disabled. The following commands are used to view and modify the default security policy for a bus:

To view users assigned to a default bus role:

```
$AdminTask listUsersInDefaultRole {-bus busName -role roleType}
```

To view groups assigned to a default bus role:

```
$AdminTask listGroupsInDefaultRole {-bus busName -role roleType}
```

To assigned a default role to a user:

```
$AdminTask addUserToDefaultRole {-bus busName -role roletype -user 
userName}
```

To assigned a default role to a group:

```
$AdminTask addGroupToDefaultRole {-bus busName -role roletype -
group groupName}
```

To remove a default role from a user:

```
$AdminTask removeUserFromDefaultRole {-bus busName -role roletype 
-user userName}
```

To remove a default role from a group:

```
$AdminTask removeGroupFromDefaultRole {-bus busName -role roletype 
-group groupName}
```

4.6.4 Configuring Destination Permissions

Individual destinations can have different security permissions defined. To view and modify a destination permission, use the following commands:

To view all destinations with roles defined:

```
$AdminTask listAllDestinationsWithRoles {-bus busName -type 
destType}
```

To view all roles assigned to a user:

```
$AdminTask listAllRolesForUser {-bus busName -user userName}
```

To view all roles assigned to a group:

```
$AdminTask listAllRolesForGroup {-bus busName -group groupName}
```

To view users assigned to a destination role:

```
$AdminTask listUsersInDestinationRole {-bus busName -type destType
-destination destName -role roleType}
```

To view groups assigned to a destination role:

```
$AdminTask listGroupsInDestinationRole {-bus busName -type
destType -destination destName -role roleType}
```

To add a user to a destination role:

```
$AdminTask addUserToDestinationRole {-bus busName -type destType -
destination destName -role roleType -user userName}
```

To add a group to a destination role:

```
$AdminTask addGroupToDestinationRole {-bus busName -type destType
-destination destName -role roleType -group groupName}
```

To remove a user from a destination role:

```
$AdminTask removeUserFromDestinationRole {-bus busName -type
destType -destination destName -role roleType -user userName}
```

To remove a group to a destination role:

```
$AdminTask removeGroupFromDestinationRole {-bus busName -type
destType -destination destName -role roleType -group groupName}
```

4.6.5 Configuring Destination Inheritance

All destinations inherit the bus default security policy unless they are the administrator explicitly disables a destination's inheritance. To view or modify a destination inheritance of the default bus security policy use the following commands:

To view a destination's inheritance:

```
$AdminTask listInheritDefaultsForDestination {-bus busName -type
destType -destination destName}
```

To modify a destination's inheritance:

```
$AdminTask help setInheritDefaultsForDestination {-bus busName -
type destType -destination destName -inherits true|false}
```

4.6.6 Configuring Access Control Checks for a Topic in a Topic Space

In order to perform access control to topics, the TopicSpace must be configured with this feature enabled. By default, the “Default.Topic.Space”, created automatically when you create a bus, will have this feature enabled. In order to remain in the TOE, all TopicSpace destinations must have this check enabled. The following commands are used to view and modify a TopicSpace's topic access check:

To view if topic level checking is performed on a TopicSpace, view the TopicSpace definition and examine the topic topicAccessCheckRequired attribute, the default is to enable access control for topics. The following script will list all topic spaces and display the topicAccessCheckRequired attribute.

```
set topicSpaceList [$AdminConfig list SIBTopicSpace]

foreach topicSpace $topicSpaceList {

       puts "TopicSpace config id: $topicSpace"

       set name [$AdminConfig showAttribute $topicSpace
       identifier]

       puts "TopicSpace Name: $name"

       set topicAccessCheck [$AdminConfig showAttribute
       $topicSpace topicAccessCheckRequired]

       puts "Topic Access Check Required: $topicAccessCheck"

}
```

To modify the topicAccessCheckRequired attribute of a TopicSpace destination, use the following command:

```
$AdminTask modifySIBDestination {-bus busName -name destName -
topicAccessCheckRequired [true|false]}
```

4.6.7 Configuring Topic Space Root Permissions

The topic space root is the root of all topics contained in a TopicSpace. Permission to the root of a topic space can be administered using the following commands:

To view users with topic space root role permission:

```
$AdminTask listUsersInTopicSpaceRootRole {-bus busName -topicSpace
destName -role roleType}
```

To view groups with topic space root role permission:

```
$AdminTask listGroupsInTopicSpaceRootRole {-bus busName -
topicSpace destName -role roleType}
```

To add a users with topic space root role permission:

```
$AdminTask addUserToTopicSpaceRootRole {-bus busName -topicSpace
destName -role roleType -user userName}
```

To add a group with topic space root role permission:

```
$AdminTask addGroupToTopicSpaceRootRole {-bus busName -topicSpace
destName -role roleType -group groupName}
```

To remove a users from a topic space root role:

```
$AdminTask removeUserFromTopicSpaceRootRole {-bus busName

 -topicSpace destName -role roleType -user userName}
```

To remove a group from a topic space root role:

```
$AdminTask removeGroupFromTopicSpaceRootRole {-bus busName -
topicSpace destName -role roleType -group groupName}
```

4.6.8 Configuring Topic Permissions

A topic, or subtopic, is a discriminatory property of messages in a topicspace. Messaging clients can publish or subscribe to messages in a topic space using the topic to select or specify meta-data about the message. Unlike point to point messages, publish/subscribe messages are delivered to all subscribers of to a topic. Topics are typically hierarchical in nature, for example a topic “SHARES” may contain a subtopic “NASDAQ”, applications subscribing to “/SHARES” could receive messages published to the “/SHARES/NASDAQ” subtopic. The slash ('/') character is used to delimite topic and subtopic names. Permission to receive or send messages can be defined for topics/subtopics. Only sender and receiver role types are permitted for topics/subtopics in the TOE. The following commands are used to view and modify topic permissions.

To view existing topics which have security permissions assigned:

```
$AdminTask listAllTopicsWithRoles {-bus busName -topicSpace
destName}
```

To view which users have been assigned a role type for a topic:

```
$AdminTask listUsersInTopicRole {-bus busName -topicSpace destName
-topic topicName -role roleType}
```

To view which groups have been assigned a role type for a topic:

```
$AdminTask listGroupsInTopicRole {-bus busName -topicSpace
destName -topic topicName -role roleType}
```

To assign a role type to a user for a topic:

```
$AdminTask addUserToTopicRole {-bus busName -topicSpace destName -
topic topicName -role roleType -user userName}
```

To assign a role type to a group for a topic:

```
$AdminTask addGroupToTopicRole {-bus busName -topicSpace destName
-topic topicName -role roleType -group groupName}
```

To remove a role type to a user for a topic:

```
$AdminTask removeUserFromTopicRole {-bus busName -topicSpace
destName -topic topicName -role roleType -user userName}
```

To remove a role type to a group for a topic:

```
$AdminTask removeGroupFromTopicRole {-bus busName -topicSpace
destName -topic topicName -role roleType -group groupName}
```

4.6.9 Configuring Topic Inheritance

A topic, or subtopic, contained in a Topicspace may inherit it's security policy from it's parent. If a topic has no parent then the security policy may be inherited from the Topicspace Root Role, which in turn inherits from the destination roles. By default, topics inherit from their parent. Use the following commands to view and modify the inheritance of topics, or subtopics:

To view a topic's inheritance of the Sender permission:

```
$AdminTask listInheritSenderForTopic {-bus busName -topicSpace
destName -topic topicName}
```

To view a topic's inheritance of the Receiver permission:

```
$AdminTask listInheritReceiverForTopic {-bus busName -topicSpace
destName -topic topicName}
```

To set a topic's inheritance of the Sender permission:

```
setInheritSenderForTopic {-bus busName -topicSpace destName -topic
topicName -inherit [true|false]}
```

To set a topic's inheritance of the Receiver permission:

```
setInheritReceiverForTopic {-bus busName -topicSpace destName -
topic topicName -inherit [true|false]}
```

4.7 Additional Precautions

The following are some additional recommended precautions:

- A vulnerability has been found in the JRE in which remote attackers could write arbitrary files to known locations. To eliminate this exposure, it is recommended that you change the default directory for Temporary Internet files: Java control Panel -> Settings...-> Location. for more information, see:

  http://nvd.nist.gov/nvd.cfm?cvename=CVE-2005-0471

- A vulnerability has been found in which a remote attacker could attempt a cross-site scripting attack. To eliminate this exposure, it is recommended that you configure an alternative 404 error page. For more information, see:

- A vulnerability has been found in which a remote attacker could obtain the source code for a Java Server Pages (.jsp). To eliminate this exposure, it is recommended that you move all JSP source outside the web server document root. For more information, see:

  http://nvd.nist.gov/nvd.cfm?cvename=CVE-2005-1112

- A directory traversal vulnerability has been found with the Java Archive Tool (Jar) utility of J2SE in which a remote attacker could write arbitrary files in filenames. To eliminate this exposure, it is recommended that you use “unzip” rather than the Jar utility for extracting viles from archives. For more information, see:

  http://nvd.nist.gov/nvd.cfm?cvename=CAN-2005-1080

- In the evaluated configuration Java 2 security is enabled and the Java 2 security manager is configured to prevent the RMIClassLoader from being used. It is recommended that you not change this configuration. If you change the configuration so that the RMIClassLoader is allowed, you must set the “java.rmi.server.useCodebaseOnly” property to true.

5 Developer's Guide for the Certified System

This section defines the guidelines with which a trusted developer must comply. A trusted developer is a software developer who is trusted to create software that runs inside the certified system.

5.1 Types of Software That Can Be Created

The trusted developer can create the following types of software to run in the certified system:

- Enterprise applications
- Resource adapters
- Resource providers

5.1.1 Enterprise Applications

An enterprise application is application software that accepts and processes requests from clients. The application can consist of any of the following types of modules:

- Web server applications
- Standard enterprise beans
- Web service enterprise beans

A web server application accepts and processes HTTP requests from clients. The following documentation describes and provides instructions on how to create a web server application:

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/welc6tech_web.html

A standard enterprise bean accepts and processes local, remote RMI, or both local and remote RMI requests from clients. The following documentation describes and provides instructions on how to create a standard enterprise bean:

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/topic/com.ibm.websphere.nd.doc/info/ae/ae/welc6tech_ejb.html

A web service enterprise bean is a standard enterprise bean with additional functionality. The additional functionality allows the web service enterprise bean to accept and process remote web service requests from clients. The following documentation describes and provides instructions on how to create a web service enterprise bean:

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/welc6tech_wbs.html

5.1.2 Resource Adapters

A resource adapter is a system level software driver that a Java application uses to connect to an enterprise information system. The following documentation describes and provides instructions on how to create a resource adapter:

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/cdat_resourcead.html

5.1.3 Resource Providers

A resource provider is system level software that handles backend processing for a Java API. The certified system supports all the types of resource providers that are defined in the J2EE v1.4 specification and also supports some additional resource providers that are specific to WebSphere Application Server. The following documentation describes and provides instructions on how to create resource providers:

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/welc6tech_res.html

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.javadoc.doc/public_html/spi/overview-summary.html

5.2 General Restrictions

The trusted developer must comply with the following restrictions when creating software for the certified system:

- No calls to undocumented local interfaces
- No calls to disallowed APIs
- No implementations of remote interfaces
- No compromising security of sensitive resources

5.2.1 No Calls to Undocumented Local Interfaces

All APIs documented in the product documentation can be used in the evaluated configuration, except those explicitly stated as not to be used in section 5.2.2. The trusted developer must ensure that the software does not call any local interfaces of WebSphere Application Server that are not identified in the following product documentation:

- The product documentation that identifies the APIs defined and implemented by WebSphere Application Server for use by developers:

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/welc_ref_dev_javadoc.html

- The product documentation that identifies the APIs defined and implemented by WebSphere Application Server for use by administrators:

  http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/welc_ref_adm_javadoc.html

- The product documentation that identifies the APIs defined by standard organizations and implemented by WebSphere Application Server:

  http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/rovr_commoncriteria.html

5.2.2 No Calls to Disallowed APIs

The trusted developer must ensure that the software does not call any of the following APIs, even though they are documented in the product documentation referenced in section 5.2.1.

- Any APIs in the Chart packages -- com.klg.jclass.util.swing, com.klg.jclass.util.legend, com.klg.jclass.util.legend.resources, com.klg.jclass.util.internal, and com.klg.jclass.chart.
- WebSphere Studio Runtime package – com.ibm.webtools.runtime.
- Servlets should not be created to extend PageList and users should not reference “serveServletsByClassName” in a web module.
- Command utility packages -- com.ibm.ejs.container, com.ibm.websphere.command, com.ibm.websphere.commandutil, and com.ibm.websphere.csi
- Apache Struts packages – org.apache.struts.action, org.apache.struts.actions, org.apache.struts.config, org.apache.struts.plugins, org.apache.struts.taglib.bean, org.apache.struts.taglib.html, org.apache.struts.taglib.logic, org.apache.struts.taglib.nested, org.apache.struts.taglib.nested.bean, org.apache.struts.taglib.nested.util, org.apache.struts.taglib.nested.logic, org.apache.struts.taglib.tiles, org.apache.struts.tiles, org.apache.struts.tiles.actions, org.apache.struts.tiles.beans, org.apache.struts.tiles.definition, org.apache.struts.tiles.xmlDefinitions, org.apache.struts.upload, org.apache.struts.util, and org.apache.struts.validator
- Implementations of the following interfaces:
  - com.ibm.wsgw.beans._EJSRemoteStatelessFilterImpl.orb
  - com.ibm.wsgw.beans._EJSRemoteStatelessFilterImplHome.orb
  - com.ibm.wsgw.beans._EJSRemoteStatelessGatewayDefaultRouting.orb

  - com.ibm.wsgw.beans._EJSRemoteStatelessGatewayDefaultRoutingHome.orb
  - com.ibm.wsgw.beans._EJSRemoteStatelessGatewayDummyExceptionHandler.orb
  - com.ibm.wsgw.beans._EJSRemoteStatelessGatewayDummyExceptionHandlerBean.orb
  - com.ibm.wsgw.beans._EJSRemoteStatelessGatewayDummyExceptionHandlerBean.orb
  - com.ibm.wsgw.beans._EJSRemoteStatelessGatewayDummyExceptionHandlerBeanHome.orb
  - com.ibm.wsgw.beans._EJSRemoteStatelessGatewayDummyExceptionHandlerHome.orb
  - com.ibm.wsgw.beans._EJSRemoteStatelessGatewayDummyMessageWarehouse.orb
  - com.ibm.wsgw.beans._EJSRemoteStatelessGatewayDummyMessageWarehouseBean.orb
  - com.ibm.wsgw.beans._EJSRemoteStatelessGatewayDummyMessageWarehouseBeanHome.orb
  - com.ibm.wsgw.beans._EJSRemoteStatelessGatewayDummyMessageWarehouseHome.orb

5.2.3 No Implementations of Remote Interfaces

The trusted developer must ensure that the software does not implement any of its own remote interfaces.

5.2.4 No Implementations of the Web Services Gateway Interfaces

The trusted developer must ensure that the software does not implement any of the Web Services Gateway interfaces. The Web Services Gateway interfaces are listed in the WebSphere Application Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.javadoc.doc/wsgw/overview-summary.html.

5.2.5 No Compromising Security of System

The trusted developer must ensure that the software does not do anything careless that compromises the security of the system.

5.3 Restrictions Specific to Web Server Applications

The trusted developer must configure the web server application as follows:

- The URL must be configured with a login constraint deployment descriptor.

- The HTTP interface corresponding to each sensitive method or HTML page must be configured with a security constraint deployment descriptor. The security constraint deployment descriptor must specify each application-defined role that has permission to access the method or HTML page.
- On WebSphere Application Server for z/OS, web applications must not be configured to use client certificate authentication.
- On WebSphere Application Server for z/OS, Enterprise Beans deployed as web servers must not use X509 token authentication.

5.4 Restrictions Specific to Enterprise Beans

The trusted developer must configure the enterprise bean as follows:

- Each interface to a sensitive method in an enterprise bean must be configured with a permission deployment descriptor. The permission deployment descriptor must specify each application-defined role that has permission to access the method.
- For startup beans, the Start() and Stop() methods must be configured with a permission deployment descriptor which specifies an application-defined role that has permission to access those methods.

5.5 Restrictions Specific to Web Services Enterprise Beans

The trusted developer must configure the web services enterprise bean to use the HTTP transport. In addition to this, the trusted developer needs to be aware that only a subset of the security functions that can be configured for a web services enterprise bean was included in the Common Criteria EAL4 evaluation of WebSphere Application Server. Therefore, only this subset of security functions for a web services enterprise bean has been evaluated to perform at an EAL4 level of assurance.

The subset of evaluated security functions is the server-side functions that process web services identification information received from the client when the server-side is configured in one of the ways:

Identification token type	Asserted identity?	Trust token required?	Trust token type
username token containing user ID	yes	yes	user name token containing user ID and password
user name token containing user	no	no	not applicable

ID and password			
X509 token containing client certificate	no	no	not applicable
LTPA token	no	no	not applicable

Appendix A: How to Acquire WebSphere Application Server

How to Purchase

Platforms other than z/OS:

- If you **are an existing IBM Software Customer with a Passport Advantage account**
  - Using an internet connection, open a browser and navigate to the following URL: http://www-306.ibm.com/software/howtobuy/passportadvantage/
  - Select **Passport Advantage Online** Tab
  - Select **Customer sign in**
  - Login to Passport Advantage
  - Select **Software Download and Media Access**
  - Select **Download Finder**
  - Click on **'I agree'** to continue
  - The default download method is Download Director. This method ensures a secure download
  - Select the download finder of your choice; such as '**All Downloads**' or '**Find by product description**'
  - Select **Expand All** (or product name)
  - Select the package for the platform in which you will be installing
  - Click on **'I agree'** and **'Download Now'** to continue
  - Click '**Yes**' on the security warning to trust the certificate
  - Click '**Yes**' on the default download location or specify a directory
  - Click '**No**' for proxy settings
  - Verify file size and file name when the download completes

- If you **are not an existing IBM Software Customer with a Passport Advantage account**
  - Using an internet connection, open a browser and navigate to the following URL: http://www.ibm.com/us/
  - Under the Shop for column – select **Software**
  - On the Shop for software page – select **IBM Software online catalog**
    - Select your **country and language**, check the **Remember this choice** box and press **Go**
  - On the Software on-line catalog page, under **Find Products by category**, select **Application Servers**
  - From the selections, you may pick either **WebSphere Application Server** or **WebSphere Application Server – Express**

- Select **View Pricing** for either choice
- You will be presented with a typical shopping cart option. Select among
  - IBM WebSphere Application Server Processor License + SW Maintenance 12 Months
  - IBM WebSphere Application Server Network Deployment Processor License + SW Maintenance 12 Months
  - IBM WebSphere Application Server Express Processor License + SW Maintenance 12 Months
- Fill in the quantity desired and click **Add to cart**
- At the Shopping cart page, you may **Update shopping cart** or you may **Check out.** When you select Check out, you will be presented with the Passport Advantage Terms and Conditions.
- Click **I Agree** and you will be directed to the Sign In page where you will select **register** to create an IBM ID and password.
- Please complete the registration by answering the questions

From Passport Advantage, the user must select electronic delivery

For electronic delivery:

- At the download page, please use the Download Director (DD) Option, which may also be labelled Restartable transfer

For the Evaluated Configuration, please select one of the following:

- WebSphere Application Server V6.0 for Multiplatform eAssembly (Includes V6.0.1 and V6.0.2 Updates)
- WebSphere Application Server – Network Deployment V6.0 for Multiplatform eAssembly (Includes V6.0.1 and V6.0.2 Refresh)
- WebSphere Application Server – Express V6.0 for Multiplatform eAssembly

When the user selects electronic delivery, the Passport Advantage website presents the user with the file name and file size. After the download is complete, the user can verify the file name and file size to be assured that they have downloaded the correct file.

z/OS Platform:

- If you **are an existing z Series customer**

  - Contact your account representative to request the WebSphere Application Server for z/OS V6.0.1, service level 6.0.2.3, Common Criteria Evaluated – EAL4 Package

- If you **are not an existing z Series customer**
  - Requests for the WebSphere Application Server for z/OS V6.0.1, service level 6.0.2.3, Common Criteria Evaluated – EAL4 Package should be placed through ShopzSeries support at 1-877-426-2784

Appendix B: Sample Ports Files for Configuring Profiles

Below are example properties files for use with the –portsFile parameter when configuring a deployment manager and node profile as discussed in section 3.4.2.

dmPorts.props

```
CELL_DISCOVERY_ADDRESS=7277
BOOTSTRAP_ADDRESS=9809
DRS_CLIENT_ADDRESS=7989
SOAP_CONNECTOR_ADDRESS=8879
ORB_LISTENER_ADDRESS=9100
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS=9401
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS=9402
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS=9403
WC_adminhost=9060
DCS_UNICAST_ADDRESS=9352
WC_adminhost_secure=9043
```

na1Ports.props

```
BOOTSTRAP_ADDRESS=2809
ORB_LISTENER_ADDRESS=9900
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS=9202
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS=9201
DCS_UNICAST_ADDRESS=9353
DRS_CLIENT_ADDRESS=7888
NODE_DISCOVERY_ADDRESS=7272
NODE_IPV6_MULTICAST_DISCOVERY_ADDRESS=5001
NODE_MULTICAST_DISCOVERY_ADDRESS=5000
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS=9203
```

```
SOAP_CONNECTOR_ADDRESS=8878
#SIB_ENDPOINT_ADDRESS=7276
#SIB_ENDPOINT_SECURE_ADDRESS=7286
#SIB_MQ_ENDPOINT_ADDRESS=5558
#SIB_MQ_ENDPOINT_SECURE_ADDRESS=5578
```

na2Ports.props

```
BOOTSTRAP_ADDRESS=2809
ORB_LISTENER_ADDRESS=9900
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS=9202
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS=9201
DCS_UNICAST_ADDRESS=9353
DRS_CLIENT_ADDRESS=7888
NODE_DISCOVERY_ADDRESS=7272
NODE_IPV6_MULTICAST_DISCOVERY_ADDRESS=5001
NODE_MULTICAST_DISCOVERY_ADDRESS=5000
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS=9203
SOAP_CONNECTOR_ADDRESS=8878
#SIB_ENDPOINT_ADDRESS=7276
#SIB_ENDPOINT_SECURE_ADDRESS=7286
#SIB_MQ_ENDPOINT_ADDRESS=5558
#SIB_MQ_ENDPOINT_SECURE_ADDRESS=5578
```

End of Document