Global Information Assurance Certification Paper

Securing IBM Websphere Application Server Version 3.5
Andrew T. Adams January 2003
GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b Research on Topics in Information Security

Abstract
Application Servers are the Swiss Army knife of the IT department in that they are capable of providing a wide variety of application services including Enterprise Java Beans (EJB's), Java Server Pages (JSP's), Servlets and Web Services for organizations. As a result of their flexibility, these systems have become an increasingly popular feature of many IT departments. Application servers such as IBM Websphere do however present a set of security issues and risks which must be fully understood before deploying outward facing systems based on them.

The intent of this paper is to provide basic understanding of several of the security issues and risks surrounding the implementation and configuration of the IBM Websphere Application Server version 3.5.6 (Henceforth referred to as Websphere). Websphere provides a container for EJB's as well as providing Servlet, Web Service /XML and JSP support. The features built into Websphere, when coupled with plugins for commercial web servers such as Microsoft IIS versions 4 and 5 and IPlanet make for a flexible and powerful tool. Websphere, when deployed in its default configuration however, presents several security issues which must be understood to be avoided. These issues include configuration, remote administration and deployment risks which require administrative effort to be addressed. This document will specifically discuss installation and administrative risks surrounding a single server installation of Websphere running under Windows NT or 2000 and the process by which these risks are mitigated.

Installation Tasks

The installation of Websphere is a process which requires advance planning to maximize system security. As Websphere is an application serving resources and data to other systems, ensuring security is a high priority. Securing Websphere is a process which includes the setup of the system user, configuration of the repository database and configuration of associated system parameters and files.

Configure the Websphere User:

Websphere is run as a service under Windows NT/2000 and requires an ID configured with local administrator privileges. Due to this high level of privilege, the password change process for this ID should be both audited and changed frequently to minimize the risk of compromise. It should be noted that a modification to the Websphere user's password, will require the password to be

updated in the Control Panel / Services / IBM WS AdminServer service or the Websphere service will not start.

Secure Application Server Filesystems:

Websphere should be installed upon an NTFS file system in order to maximize the security of the installation. One specific requirement which calls for NTFS is the issue of Websphere storing security related information in cleartext in several properties files. *–Properties files are roughly analogous to Windows .INI files which maintain state information for applications*. In order to protect this critical information, it is necessary to use OS level file system restrictions to prevent unauthorized users from extracting the Websphere system userid and password data from these files. Due to the Websphere system user's membership in the local administrators group, obtaining this information would lead to a complete compromise of the server. In order to verify if a file system is formatted using NTFS, the Administrator should use Windows Explorer and navigate to 'My Computer in the left hand panel. Expand the 'My Computer' icon and right click on the drive where Websphere is to be installed and select Properties. The 'File System' line should read NTFS for a correctly formatted drive. It is possible for Websphere to be installed on FAT file systems, but due to the security risks it is not recommended. There is no benefit and significant risk to install without having the option of using the operating system to restrict access to the properties files.

Secure critical Properties Files:

Websphere maintains the above listed User ID, password and related data in several properties files. Securing these files is critical to maintaining the security of the server and any attached applications. Listed in the below table are several of the more critical properties files maintained by Websphere.

File	Directory	Description
Admin.config + admin.config.bak	<wsroot>\bin	Contains configuration information for administrative database in cleartext (User ID/password and jdbc connect information)
sas.server.props sas.server.props.future	<wsroot>\properties	Contains local Websphere account User ID and password information in cleartext. The sas.server.props.future property file will include changes to be implemented on server restart. By default (with global security disabled), these files contain the administrative userid and password

		used to install the product.
sas.client.props	<wsroot>\properties	Contains SSL and keyring configuration information in cleartext

After the installation of Websphere is complete, the above listed files need to have their NTFS ACL (Access Control List) modified to permit access only by the ID under which the Websphere service runs.
The ACL's are set by modifying the Access Control settings for the files using Windows Explorer. To make this change, use Windows Explorer to navigate to the specific file then right click and select properties. From the following dialog box, select Security and remove permissions from all groups and users to each file with the exception of the Websphere Admin User ID. This User ID (or a group which it is the sole member of) should be configured to have full control on each of the above files.

A failure to restrict access to the above files will permit a malicious user to execute a complete compromise of the Websphere Server. In order to obtain the Websphere NT/2000 administrative User ID and password, an intruder could simply access and view the sas.server.props file in any text editor. The Websphere Service runs with local Admin privileges and the LOCALOS.server.id and LOCALOS.server.pwd properties will provide both the User ID and password required for this account.

In addition to compromising the Websphere application server account, information in the above properties files can also be used to gain access to the backend repository database hosting Websphere application metadata. The information required to obtain both a database account and associated connect information for the repository database (Oracle or DB2), can be obtained by accessing the admin.config file and reading the *com.ibm.ejs.sm.adminServer.dbUser* and *com.ibm.ejs.sm.adminServer.dbPassword* property values. This information coupled with *the com.ibm.ejs.sm.adminServer.dbUrl* property value will provide all the information required to access the backend database supporting the application. The approach required to mitigate this risk is identical to that for protecting the Websphere userid and password. To protect this critical information, the OS must be configured to permit only authorized users to access this data.

Secure the Admin Server Repository Database:

Securing the properties files will reduce the risk of compromising the backend database. Keeping defense in depth in mind, the database userid used by Websphere should be granted the absolute minimum rights necessary to operate to ensure that an attacker will gain little benefit should security be breached. Websphere requires this repository to maintain information about the objects hosted within the application server. This repository is automatically created as

part of the install process and the administrator can specify where the repository is to be maintained. The repository can be hosted on one of three RDBMS environments, an internal InstantDB database, Oracle 8.1.7 or DB2 version 6.2 or higher. A production application will likely require the security and recovery options available in Oracle or DB2 configurations. This section will discuss possible options for minimizing security risks when deploying to an Oracle RDBMS platform.

To minimize security risks of a breach in security, the repository user created for the Admin DB should be granted the minimum privileges necessary to complete it's required functions. The user created should at a minimum have the following privileges.

- Privileges required to connect, create a session and create objects
- Access to tablespaces specific to the user and restricted to a quota of 100 MB
- Disallow the creation of objects in the System tablespace
- Disallow access to objects in schema's other then that of the user

The User ID and password defined for the repository user should meet corporate guidelines for complexity and password change frequency. As discussed in the prior section, the User ID and password for this database user will be visible in cleartext in the admin.config file located in the <wsroot>\bin folder. This potential security risk is an important reason for administrators to perform frequent password changes. Depending upon requirements, enabling auditing on the backend Oracle database may be an option to consider as it would allow for more detailed activity tracking.

It should be noted that any change to the password for the Oracle user will require the admin.config file to be similarly updated with the new password information or the Websphere service will be unable to start. The above security risks will be similar in a deployment to a DB2 environment, with an intruder being able to obtain a DB2 database User ID and connect information after accessing the admin.config file.

Apply service fixpacks:

As with any software package, Websphere is constantly evolving as the code base is updated. These updates typically include both new functionality as well as patches to components of the application. A key component to securing Websphere (or any complex application software) is to stay current with the manufacturer's patches as they become available.

IBM releases fixpacks for Websphere which contain updated and patched code modules. The fixpacks are available for download on IBM's website. At this time, the most current fixpack for Websphere version 3.5 is release 6.

Each fixpack is downloaded from IBM as a zip file and expanded in a temporary directory. Fixpacks are installed from a command prompt in this directory. To install, the administrator would execute the install.bat batch file in the temp folder to install fixpack components. The install will take place in several steps,

dependent upon what components have been installed on the server. The 3.5.6 fixpak contains updates to Websphere, the IBM java runtime, IBM HTTP Server and Webserver plugin's. After fixpacks have been installed and verified, administrators should periodically monitor the IBM website for subsequent updates or fixes which may become available

Administration Tasks

Remove Sample Applications:

The installation of Websphere provides the option to install a number of sample applications as part of the initial setup process. Production systems should avoid the installation of any sample applications or at a minimum should ensure that they are configured to not automatically start upon system reboot.

Secure remote administration:

A significant risk to Websphere 3.5 systems is a facility built in to allow remote administration of application servers via a Java GUI application. This remote console feature is a work saving feature which allows administrators to manage multiple Websphere application servers from a single workstation. In the default configuration of Websphere, this feature is enabled and can be accessed by a knowledgeable user. When deployed in this open configuration, only a few pieces of information are needed for a remote user to gain full control of an application server. The java console controls all aspects of the Websphere implementation including starting stopping and removing applications. Any intruder gaining access to a server via this utility would have complete control over applications managed by the server and would be able to execute denial of service attacks simply by turning off services or applications.

In order to access the java admin console, there are several pieces of information which must be obtained prior to connecting to the remote system.

1. The name or IP address of the machine hosting Websphere must be known
2. The lsdPort used by the remote Websphere server (default 900) must be known
3. A installation of Websphere 3.5 must be present on the local workstation which is to be used to host the java GUI

Performing remote administration of a Websphere server is as simple as executing the adminclient.bat batch file from the Websphere root \bin account. The batch file takes two parameters which are the remote server name/IP and the lsdPort used by Websphere on the remote server. Executing the batch file with appropriate parameters will bring up the administrative console for the remote server on the workstation. While the remote administration feature is very useful from a systems management perspective, it also has significant risks

which must be taken into account. In order to avoid the risks exposed by remote administration, it is necessary to implement several of Websphere's security features which specifically deal with remote access to the server.

Disable HTTP Administration:

Installing Websphere with all options included will install and configure the http administrative console. In order to prevent remote administration of the application server via a web browser, this feature should be secured or simply not installed on production systems. The HTTP administrative console if enabled and not secured will allow remote users to gain access to administrative features. These features include the ability to start and stop applications, and modify application properties. A decision to configure http administration should take these additional security concerns into account.

Enable Websphere Global Security:

Websphere includes a number of security features which can be enabled to better manage access to the administrative console. Global Security is a feature available within Websphere which when enabled, will require any access attempt to provide valid credentials such as a valid user on the Websphere server. The focus of this section will be a review the steps required to force a remote user to enter a valid User ID and password to obtain access to the Websphere administrative console.

The mechanism used for restricting access to the Websphere remote console is a feature called Websphere Global Security settings. This feature is accessed via the administrative utility by navigating to Console | Tasks | Configure Global Security Settings. The above command will bring up the Set Global Security Wizard within the administrative console. In order to enable Websphere security, it will be necessary to take the following steps:

- Check off the Enable Security box within the general tab of the Set Global Security Wizard dialog box in the General Tab
- Navigate to the Application Defaults tab and ensure that the Challenge type is set to Basic (User ID and Password)
- Navigate to the Authentication Mechanism tab and verify that the Authentication Mechanism selected is the Local Operating System. This will authenticate the credentials passed against those stored on the Websphere Application Server. A user without the credentials will be denied access to the application
- Navigate to the User Registry tab and input the User ID and Password of a valid account on the Websphere Server. Note that it is not necessary for the account used to be that of the Websphere system account, although the user id and password must exist on the application server.

When the above steps are complete, it will be necessary to stop and restart the Websphere service for the changes to take effect. When the Administrative console is next accessed either locally or remotely using the adminclient.bat file, it will be protected by the global security settings. Websphere will prompt the user with a dialog box to enter the server name, user id and password to be authenticated against. Websphere will authenticate these credentials against the local user repository. Failing to provide these credentials or entering incorrect values will prevent access to the administrative console of the server.

Enable Websphere Application Security:

The configuration of Application level security within Websphere is out of scope for this document, but is a key component of IBM's security implementation for Websphere. Using Application level security, applications can define differing security rules on a per application basis. This complements Global security settings and offers a tremendous amount of flexibility in implementing and deploying security features.

Secure Interfaced Systems:

Typically Websphere is integrated with systems such as Microsoft Internet Information Server (IIS) when providing web services. In this type of environment, it is critical to secure both the Application server and the web server to reduce the risk of a breach. An intruder able to gain access to a server via an IIS vulnerability will bypass all efforts made to lock down Websphere and allow access to the server. As part of this effort, an audit should be undertaken to determine which services are required on each server, with unneeded services being disabled to reduce the risk of a breach.

Maintain Physical Security:

Maintaining the physical security of the Websphere server is of critical importance. Applications and software can be protected with the latest patches and configured to maximize security, but all of this protection is moot if a intruder gains physical access to the server. An intruder able to reboot the server or install applications of their choice can gain complete control over the system and bypass all security features. Several of the components of maintaining physical security are listed below

- Deploying the server in a controlled access environment such as a data center with restricted access.
- Purchase servers which have the capability to lock the floppy and CD drives to prevent their use or remove / disable these devices
- Remove or disable any USB ports if appropriate
- Use IDS and Network monitoring systems such as firewalls to provide defense in depth to the application and to increase the opportunity to detect illegal activity

Summary

IBM Websphere Application Server is an excellent choice for organizations which require the wide range of functionality provided by an application server. As a result of its increasing popularity, Websphere is being deployed in many organizations, some of which may only have a limited understanding of the software. As with any complex system, it is necessary for organizations to understand the security risks present in deploying a particular software package and Websphere is no exception.

The deployment and maintenance of applications running under Websphere is a complex process. It is necessary for systems administrators to understand both the security risks and the security features built into the application to address these complexities. When a decision is made to deploy applications operating under Websphere, it is necessary for security concerns to be factored into application design as well as the initial system implementation. The default "out of the box" settings for Websphere leave it vulnerable to compromise and it is necessary for administrators to understand the issues and workarounds necessary to harden the system and prevent intrusion.

It should be noted that addressing the risk points within Websphere are only part of a larger security picture. Application servers require up to date OS patches and integrated / updated antivirus software to reduce the probability of intrusion. A secure and patched server in turn is protected by network based IDS systems and firewalls. These technical implementations will then be included in the overall Enterprise wide security architecture and security policy. Together, these processes and systems will provide the required defense in depth which is needed in today's environments.

References

"Securing Properties Files", IBM Corporation
http://www-3.ibm.com/software/webservers/appserv/doc/v35/ae/infocenter/was/050204.html (Feb 8 2003)

Zenin, Ruslan "Secure WAS 3.5 Directories and Files", Websphere Advisor Magazine, December 2001. URL:
http://advisor.com/Articles.nsf/aid/ZENIR06-01 (Feb 21 2003)

"WebSphere Application Server Version 3.5 FixPak 6 (WAS 3.5.6)" IBM Corporation, URL:
http://www-1.ibm.com/support/docview.wss?rs=180&context=SSEQTP&q=websphere+3.5.6&uid=swg24001217&loc=en_US&cs=utf-8&lang=en (March 1 2003)

"Securing Applications –special topics Websphere Application Server" IBM Corporation
http://www-3.ibm.com/software/webservers/appserv/doc/v35/ae/infocenter/was/05.html (March 21 2003)

"Installing the Advanced Edition using Microsoft IIS and Oracle 8i on Windows" IBM Corporation
http://www-3.ibm.com/software/webservers/appserv/doc/v35/ae/infocenter/was/win_adv_iis_oracle.pdf (February 2003)

"Websphere Version 3.5 Handbook" IBM Corporation: URL
http://www.cs.unc.edu/Courses/comp119/materials/documentation/ibm-redbooks/WebSphere-handbook%20-%20sg246161.pdf

Brown, Kylie, Enterprise Java Programming with IBM WebSphere. New York Addison Wesley 2001

Hartley, Bruce "You Need a Corporate Security Policy" Websphere Advisor
http://webspherereadvisormagazine.com/doc/05216 (March 15 2003)