Oracle® WebLogic Operations Control

Securing a Production Environment

10g Release 3 (10.3)

September 2008

ORACLE

Oracle WebLogic Server Securing a Production Environment, 10g Release 3 (10.3)

Contents

1. Determining Your Security Needs

Understand Your Environment 1-1

Hire Security Consultants or Use Diagnostic Software 1-2

Read Security Publications 1-2

Install WLOC in a Secure Manner 1-2

2. Ensuring the Security of Your Production Environment

Securing the WLOC Host 2-2

Securing Network Connections 2-6

Securing the WLOC Security Service 2-8

CHAPTER 1

Determining Your Security Needs

Before you deploy WebLogic Operations Control (WLOC) into a production environment, determine your security needs and make sure that you take the appropriate security measures, as described in the following sections:

- "Understand Your Environment" on page 1-1
- "Hire Security Consultants or Use Diagnostic Software" on page 1-2
- "Read Security Publications" on page 1-2
- "Install WLOC in a Secure Manner" on page 1-2

Understand Your Environment

To better understand your security needs, ask yourself the following questions:

- Which resources am I protecting?

  Many resources in the production environment can be protected. Consider the resources you want to protect when deciding the level of security you must provide.

- From whom am I protecting the resources?

  For most WLOC Controllers and Agents, resources must be protected from everyone on the Internet. But should the Controller or Agent be protected from the employees on the intranet in your enterprise? Should your employees have access to all resources within the WLOC environment? Should the system administrators have access to all WLOC resources? Should the system administrators be able to access all data? You might consider

giving access to highly confidential data or strategic resources to only a few well trusted system administrators. Perhaps it would be best to allow no system administrators access to the data or resources.

- What will happen if the protections on strategic resources fail?

  In some cases, a fault in your security scheme is easily detected and considered nothing more than an inconvenience. In other cases, a fault might cause great damage to applications controlled by WLOC. Understanding the security ramifications of each resource will help you protect it properly.

Hire Security Consultants or Use Diagnostic Software

However you deploy WLOC it is a good idea to hire an independent security expert to go over your security plan and procedures, audit your installed systems, and recommend improvements. Oracle On Demand offers services and products that can help you to secure a WebLogic Server production environment. See the Oracle On Demand page at `http://www.oracle.com/ondemand/index.html`.

Read Security Publications

Read about security issues:

- For the latest information about securing Web servers, Oracle recommends the reviewing the security practice information available from the CERT™ Coordination Center operated by Carnegie Mellon University.
- For security advisories, refer to the Oracle WebLogic Advisories and Notifications page at the following location: `https://support.bea.com/application_content/product_portlets/securityadvisories/index.html`.
- Here, you can download security-related patches and register to receive notifications of newly available security advisories.

  Report possible security issues in Oracle products to `secalert_us@oracle.com`.

Install WLOC in a Secure Manner

Currently, the WLOC installation includes the entire JDK and some additional WLOC utilities (for example, `beasvc`). These programs could be a security vulnerability. The following are recommendations for making a WLOC installation more secure:

- When using Oracle® JRockit, minimize the WLOC installation by deleting the software components of the Java SDK that are not in the JRockit JRE.

  Note: There is always a potential of making mistakes when deleting executables, files, and directories from the WLOC installation. Therefore, Oracle recommends testing your changes in a secure, development environment before implementing them in a production environment.

CHAPTER 2

Ensuring the Security of Your Production Environment

Oracle recommends that you implement the following actions to ensure the security of your production environment:

- "Securing the WLOC Host" on page 2-2
- "Securing Network Connections" on page 2-6
- "Securing the WLOC Security Service" on page 2-8

Securing the WLOC Host

A WLOC production environment is only as secure as the security of the machine on which it is running. It is important that you secure the physical machine, the operating system, and all other software that is installed on the host machine. The following are suggestions for securing a WLOC host in a production environment. Also check with the manufacturer of the machine and operating system for recommended security measures.

Table 2-1 Securing the WLOC Host

Security Action	Description
Physically secure the hardware.	Keep your hardware in a secured area to prevent unauthorized operating system users from tampering with the deployment machine or its network connections.
Secure networking services that the operating system provides.	Have an expert review network services such as e-mail programs or directory services to ensure that a malicious attacker cannot access the operating system or system-level commands. The way you do this depends on the operating system you use. Sharing a file system with other machines in the enterprise network imposes risks of a remote attack on the file system. Be certain that the remote machines and the network are secure before sharing the file systems from the machine that hosts WLOC.
Use a file system that can prevent unauthorized access.	Make sure that the file system on each WLOC host can prevent unauthorized access to protected resources. For example, on a Windows computer, use only NTFS.
Set file access permissions for data stored on disk.	Set operating system file access permissions to restrict access to data stored on disk. For example, operating systems such as Unix and Linux provide utilities such as umask and chmod to set the file access permissions. At a minimum, consider using “umask 066”, which denies read and write permission to Group and Others.

Table 2-1 Securing the WLOC Host

Security Action	Description
Limit the number of user accounts on the host machine.	Avoid creating more user accounts than you need on WLOC hosts, and limit the file access privileges granted to each account. Ideally, the host machine would have two user accounts with system administrator privileges on operating systems that allow more than one system administrator user and another user with sufficient privileges to run WLOC. Having two system administrator users provides a backup at all times. The WLOC user should be a restricted user, not a system administrator user. One of the system administrator users can always create a new WLOC user if needed. Review active user accounts regularly and when personnel leave. *Background Information*: Some WLOC configuration data and some URL (Web) resources, including Java Server Pages (JSPs) and HTML pages, are stored in clear text on the file system. A sophisticated user or intruder with read access to files and directories might be able to defeat any security mechanisms you establish with WLOC authentication and authorization schemes.
For your system administrator user accounts, choose names that are not obvious.	For additional security, avoid choosing an obvious name such as "system", "admin", or "administrator" for your system administrator user accounts.
Safeguard passwords.	The passwords for user accounts on production machines should be difficult to guess and should be guarded carefully. Change passwords periodically.

Table 2-1 Securing the WLOC Host

Security Action	Description
On each host computer, give only one user account access to resources in addition to the two system administrator users who also have access privileges.	On each WLOC host computer, use the operating system to establish a special user account (for example, `wloc_owner`) specifically to run WLOC. Grant to this operating-system (OS) user account the following privileges: • Access privileges only to the Home directory, the WLOC product directory tree, and your user projects directories. The **Home directory** is a repository for common files that are used by multiple Oracle products installed on the same machine. The **WLOC product installation directory** contains all the WLOC software components that you choose to install on your system, including program files. A **user projects directory** contains the configuration files, security files, log files, and other resources for a single WLOC Controller and Agent. If you install multiple users projects on a WLOC host computer, each directory must be protected. By default, the installation program places all files and your user projects directories in a single directory tree, whose top directory is named `bea`. All WLOC files are a subdirectory of this directory tree (`bea\wloc_10.3`), and your user projects files are in other subdirectories, such as `bea\user_projects\controller` or `bea\user_projects\agent1`. You can, however, locate the WLOC product installation directory and your user projects directories outside the Home directory. For more information, refer to Selecting Directories for Your Installation in the *Installation Guide*. • No other OS user should have read, write, or execute access to files and your user projects files. (The system administrator users have access privileges by default.) This protection limits the ability of other applications executing on the same machine as WLOC to access files and your user projects files. Without this protection, some other application could gain write access and insert malicious, executable code in JSPs and other files that provide dynamic content. The code would be executed the next time the file was served to a client.

Table 2-1 Securing the WLOC Host

Security Action	Description
On each host computer, give only one user account access to WLOC resources.	Knowledgeable operating system users may be able to bypass WLOC security if they are given write access, and in some cases read access, to the following files: • WLOC Installation • JDK files (typically in the WLOC installation, but can be configured to be separate) • User projects directory
Do not develop on a production machine.	Develop first on a development machine and then move code to the production machine when it is completed and tested. This process prevents bugs in the development environment from affecting the security of the production environment.
Do not install development and sample software on a production machine.	Do not install development tools on production machines. Keeping development tools off the production machine reduces the leverage intruders have should they get partial access to a WLOC production machine.
Enable security auditing.	If the operating system on which WLOC runs supports security auditing of file and directory access, Oracle recommends using audit logging to track any denied directory or file access violations. Administrators should ensure that sufficient disk space is available for the audit log.
Consider using additional software to secure your operating system.	Most operating systems can run additional software to secure a production environment. For example, an Intrusion Detection System (IDS) can detect attempts to modify the production environment. Refer to the vendor of your operating system for information about available software.
Apply operation-system service packs and security patches.	Refer to the vendor of your operating system for a list of recommended service packs and security-related patches.

Table 2-1 Securing the WLOC Host

Security Action	Description
Apply the latest service packs and implement the latest security advisories.	If you are responsible for security related issues at your site, register on the Oracle WebLogic Advisories and Notifications page at `https://support.bea.com/application_content/product_portlets/securityadvisories/index.html` to receive notifications of newly available security advisories. Remedies recommended in the security advisories are posted on the Advisories & Notifications page. In addition, you are advised to apply each service pack as it is released. Service packs include a roll-up of all bug fixes for each version of the product, as well as each of the previously released service packs. Report possible security issues in products to `secalert_us@oracle.com`.
Do not run WebLogic Server in Development mode in a production environment.	Production mode sets the server to run with settings that are more secure and appropriate for a production environment.

Securing Network Connections

When designing network connections, you balance the need for a security solution that is easy to manage with the need to protect strategic WLOC resources. The following table describes options for securing your network connections.

Table 2-2 Securing Network Connections

Security Action	Description
Use hardware and software to create firewalls.	A firewall limits traffic between two networks. Firewalls can be a combination of software and hardware, including routers and dedicated gateway machines. They employ filters that allow or disallow traffic to pass based on the protocol, the service requested, routing information, packet content, and the origin and destination hosts or networks. They can also limit access to authenticated users only.
Only allow `https` access to the console if in an untrusted network environment.	See Configuring Security in the WLOC *Configuration Guide* on restricting access to the console to https (SECURE mode). If the console is run in either UNSECURE mode or BOTH mode, an attacker with access to the network could sniff credentials off the wire.

Table 2-2 Securing Network Connections

Security Action	Description
Ensure that the controller and agents communicate using SSL if in an untrusted network environment.	See Configuring Security in the WLOC *Configuration Guide* for more information on setting communications between the controller and agents to only use SSL. The agent's operations are protected using SSL. If communication between the controller and agent is not SSL, an attacker with network access to the agent could attack it.
Practice safe surfing when logged into the WLOC console.	A number of Cross Site Scripting attacks (XSS) and Cross Site Request Forgery (CSRF) attacks rely on an authenticated user surfing to another site and unknowingly clicking a link, which can lead to malicious code being executed. If a user is logged into the WLOC console they should not surf to non-WLOC sites to reduce the chances of such an attack against WLOC.

Securing the WLOC Security Service

The WLOC Security Service provides a powerful and flexible set of software tools for securing the subsystems and applications that run on a server instance. The following table provides a checklist of essential features that Oracle recommends you use to secure your production environment.

Table 2-3 Securing the WebLogic Security Service

Security Action	Description
Use SSL, but do not use the demonstration digital certificates in a production environment.	To prevent sensitive data from being compromised, secure data transfers by using HTTPS. WLOC generates self-signed SSL certificates when the Configuration Wizard is run for Controller or Agent. You may want to replace these self-signed certificates with certificates signed by a certificate authority. Refer to Configuring Security in the WLOC *Configuration Guide*.
Periodically review security auditing.	Auditing is the process of recording key security events in your WLOC environment. When the Auditing provider that the Security Service provides is enabled, it logs events in `user_projects\controller\legacy-rootdir\servers\legacy-server-name\logs\DefaultAuditRecorder.log` Review the auditing records periodically to detect security breaches and attempted breaches. Noting repeated failed logon attempts or a surprising pattern of security events can prevent serious problems.
Ensure that you have correctly assigned users and groups to the default WLOC security roles.	By default, all WLOC resources are protected by security policies that are based on a default set of security roles. Make sure you have assigned the desired set of users and groups to these default security roles. Refer to Configuring Security in the WLOC *Configuration Guide*.
Create no fewer than two user accounts with system administrator privileges.	One of the system administrator users should be created when the domain is created. Create other user(s) and assign them the Admin security role. When creating system administrator users give them unique names that cannot be easily guessed. Having at least two system administrator user accounts helps to ensure that one user maintains account access in case another user becomes locked out by a dictionary/brute force attack.