Weblogic 安全配置规范

1. 概述

1.1. 目的

本规范明确了 Weblogic 应用服务器安全配置方面的基本要求。为了提高 Weblogic 应用服务器的安全性而提出的。

1.2. 范围

本规范适用于 XXXX 使用的 Weblogic 应用服务器。

2. 强化 Weblogic 主机

2.1. 强化操作系统网络服务

【说明】在安装 Weblogic 前加固底层的操作系统。

2.2. 使用可以防止非授权访问的文件系统

【说明】确保 Weblogic 主机的文件系统可以防止非授权访问，例如 Windows 的 NTFS。

2.3. 限制 Weblogic 主机上的用户数量

【说明】理想状况下，主机上的帐号应为 2 个管理员权限的帐号，1 个运行 Weblogic 的帐号。

2.4. 帐号和密码

【说明】避免使用明显可以猜测到的帐号如”system”,”admin”或者”administrator”。口令至少 8 位，并满足复杂度要求。

2.5. 访问 Weblogic 资源的帐号的唯一性

【说明】在操作系统上建立一个专门用于 Weblogic 的帐号。

【具体配置】

该帐号只能操作以下三个目录：
BEA 主目录。该目录是 BEA 多个产品的共享目录。
Weblogic 安装目录。该目录包括了所有的安装程序。
域目录。该目录包括了设置文件、安全文件、日志文件和 J2EE 应用等。

赋予该帐号对以上三个目录读写执行权限。

2.6. 使用特殊帐号 Run Weblogic Server Windows 服务

【说明】在 Windows 平台，可以以 Windows 服务的方式运行 Weblogic Server 实例。这样会导致每次启动 Windows 自动执行 Weblogic Server。而且不要以 Windows administrator 权限运行 Weblogic Server。

【具体配置】

如何以一个特殊非管理员帐号运行 Weblogic Server 请参考以下：

http://e-docs.bea.com/wls/docs70/adminguide/startstop.html#Setting_Up_a_Weblogic_Server_as_a_Windows_Service

验证以一个特殊非管理员帐号运行 Weblogic Server 请参考以下：
http://e-docs.bea.com/wls/docs70/adminguide/startstop.html#VerifyUserAccountForWinService

2.7. 不在生产机上开发

【说明】在开发环境中开发相应的代码，经过测试后将代码转移到生产机上。此举是为了防止开发过程中的 Bug 影响生产环境。

【具体配置】

验证 DocumentRoot 包括以下设置：

<Directory "/var/www/html">
Order allow,deny Allow from all
Options None
AllowOverride None
</Directory>

2.8. 不在生产机上安装开发和 sample 软件

【说明】将开发工具从生产机上移除可以防止该工具被入侵者利用，一定程度地访问生产系统。

2.9. 启动安全审计

【说明】如果 Weblogic 运行的操作系统支持对文件和目录访问的安全审计，建议使用日志跟踪对文件和目录的拒绝访问。

【具体配置】

使用 ModSecurity Core Rules 限制请求的方式：
modsecurity_crs_30_http_policy.conf 文件包括以下的规则，
allow request methods
#
TODO Most applications only use GET, HEAD, and POST request # methods, if so uncomment the line below. Otherwise you are advised
to edit the line before uncommenting it.
#
SecRule REQUEST_METHOD "!^((?:(?:POS|GE)T|OPTIONS|HEAD))$" \
"phase:1,log,auditlog,status:501,msg:'Method is not allowed by policy', severity:'2',,id:'960032',"

2.10. 应用最新的 BEA 补丁，考虑实施官方最新的安全建议

【说明】如题

【具体配置】

注册 BEA Advisories & Notifications（http://dev2dev.bea.com/advisories）以便收到最新的安全建议信息。

从http://commerce.beasys.com/downloads.可以下载 Service Pack

3. 强化网络连接

3.1. 使用防火墙或 Weblogic Server connection filters

【说明】建议使用防火墙限制 Weblogic Server 域外到域的连接；使用 Connection Filters 限制 Weblogic Server 域内的连接。更多信息可参考http://e-docs.bea.com/wls/docs70/secmanage/domain.html#connection_filter

3.2. 使用管理端口来承载管理的流量

【说明】建议使用域范围内的管理端口 Administration Port 来限制同一 Weblogic Server 域内的 server instances 间的流量都经过同一端口。当不使用管理端口时，管理流量会以明文形式在网上传输。管理端口另一个好处是当遭受到拒绝服务攻击时，仍然可以通过该端口管理 Weblogic Server。

配合 Connection Filters 使用，可以指定 Weblogic Server 只接受来自某一 IP 段的管理请求，并所有连接只通过一个端口。

使用管理端口可以保证客户端与管理控制台以加密的方式连接。

更多信息可以参考

http://e-docs.bea.com/wls/docs70/ConsoleHelp/domain.html#enabling

3.3. 使用管理通道

【说明】建议启用管理通道 Administration Channel 以确保服务器间的管理流量的安全性。没有管理通道，一些关键的管理信息会以明文传输。更多的信息可以参考http://e-docs.bea.com/wls/docs70/admin_domain/network.html

4. 强化 Weblogic 安全服务

4.1. 部署符合生产环境的 Security Provider

【说明】Weblogic Security Service 使用了一个可插拔的安全架构，在这个架构下可以部署多个 secuirty provider。缺省条件下，Weblogic Server 包括其自身的 security providers,该 provider 已经提供了完整的安全解决方案。

【具体配置】

确保恰当地部署了 security providers.

可以通过以下位置验证：

■Administration Console under the Security → Realms → RealmName→ Providers folder.

其它信息可以参考：http://e-docs.bea.com/wls/docs70/secmanage/realm.html

4.2. 使用 SSL

【说明】为保证数据传输安全，建议使用 SSL 和 HTTPS 替代 HTTP。Weblogic Server 包括一系列的开发用的 Private Keys，数字证书和 truseted certificate authorities。每一个下载 Weblogic Server 的用户都拥有对这些证书的 Private Keys。禁止使用展示用的 identity & trust.

设置 SSL 可以参考http://e-docs.bea.com/wls/docs70/secmanage/ssl.html

4.3. 使用主机名验证

【说明】使用主机名验证以避免中间人攻击。缺省下，Weblogic SSL 验证发起连接的主机是否经过授权，但实施 SSL 前主机名验证可能已经被禁止了。

【具体配置】

确保使用了 Hostname Verifier

可以通过以下位置设置：

- Administration Console on theServer s→ *ServerName* → Connections → SSL tab.

4.4. 防止拒绝服务

【说明】限制请求的大小和时间以防止拒绝服务攻击。Weblogic Server 可以限制消息的大小和消息到达的最大时间。

- 可以通过以下位置设置：Administration Console on the Servers → *ServerName* →Connections → Protocols tab.

4.5. 设置帐号锁定和登录时间

【说明】限制请求的大小和时间以防止拒绝服务攻击。Weblogic Server 可以限制消息的大小和消息到达的最大时间。

- 可以通过以下位置设置：Administration Console on the Security → Realms → *RealmName* → User Lockouts tab.

4.6. 开启安全审计

【说明】如果开启了 Weblogic Security Service 提供的 Auditing Provider，日志会存在以下位置：*DomainName*\DefaultAuditRecorder.log

- 可以通过以下位置设置：Administration Console on the Security → Realms → RealmName → Providers → Auditors page.

更多信息可以参考：

http://e-docs.bea.com/wls/docs70/ConsoleHelp/security_7x.html#auditprovider

4.7. 限制发送主机名和版本号

【说明】缺省条件下，当 Weblogic Server 响应 HTTP 请求时，在其 HTTP 响应的包头中包括服务器的名称和 Weblogic 版本号，这会导致服务器信息的泄漏。

可以通过以下位置设置：

- disable the Send Server Header Enabled attribute in the Administration Console. The attribute is located on the Server →*ServerName* → Connections → HTTP tab.

4.8. 默认安全角色

【说明】确保正确地将用户和组分配给默认的 Weblogic Server Security roles. 缺省下，Weblogic 是基于一系列的缺省安全角色和安全策略来保护资源。更多信息可以参考：http://e-docs.bea.com/wls/docs70/adminguide/secsysadm.html