

培训教育  
Training Services



# 中间件安全

主讲: Gnosis

## 4.1.4 Weblogic

---

Weblogic 的安全设置

Weblogic 的漏洞利用与防范

Weblogic 的日志审计方法

# Weblogic 的安全设置

---

## 了解 Weblogic 的启动权限

WebLogic默认是不允许管理员用root用户启动服务的，因为root用户权限过高。所以如果管理员使用root用户启动WebLogic会看到报错信息如下：

```
<Error> <EmbeddedLDAP> <000000> <Error opening the Transaction  
Log: ./myserver/ldap/ldapfiles/EmbeddedLDAP.tran: Permission denied>
```

所以在安装部署WebLogic的时候，需要提前创建WebLogic的管理员用户和对应的用户组，一般情况下配置的用户和用户组的方式如下：

```
# groupadd oinstall  
# useradd -g oinstall weblogic
```

## Weblogic的部署

- 一、 Weblogic是美商Oracle的主要产品之一，是世界上第一个成功商业化的J2EE应用服务器。
- 二、 部署Weblogic之前需要做的准备工作
  - 1、 创建用户和用户组
  - # groupadd dba
  - # groupadd oinstall
  - 2、 创建Weblogic用户
  - # useradd -g oinstall weblogic

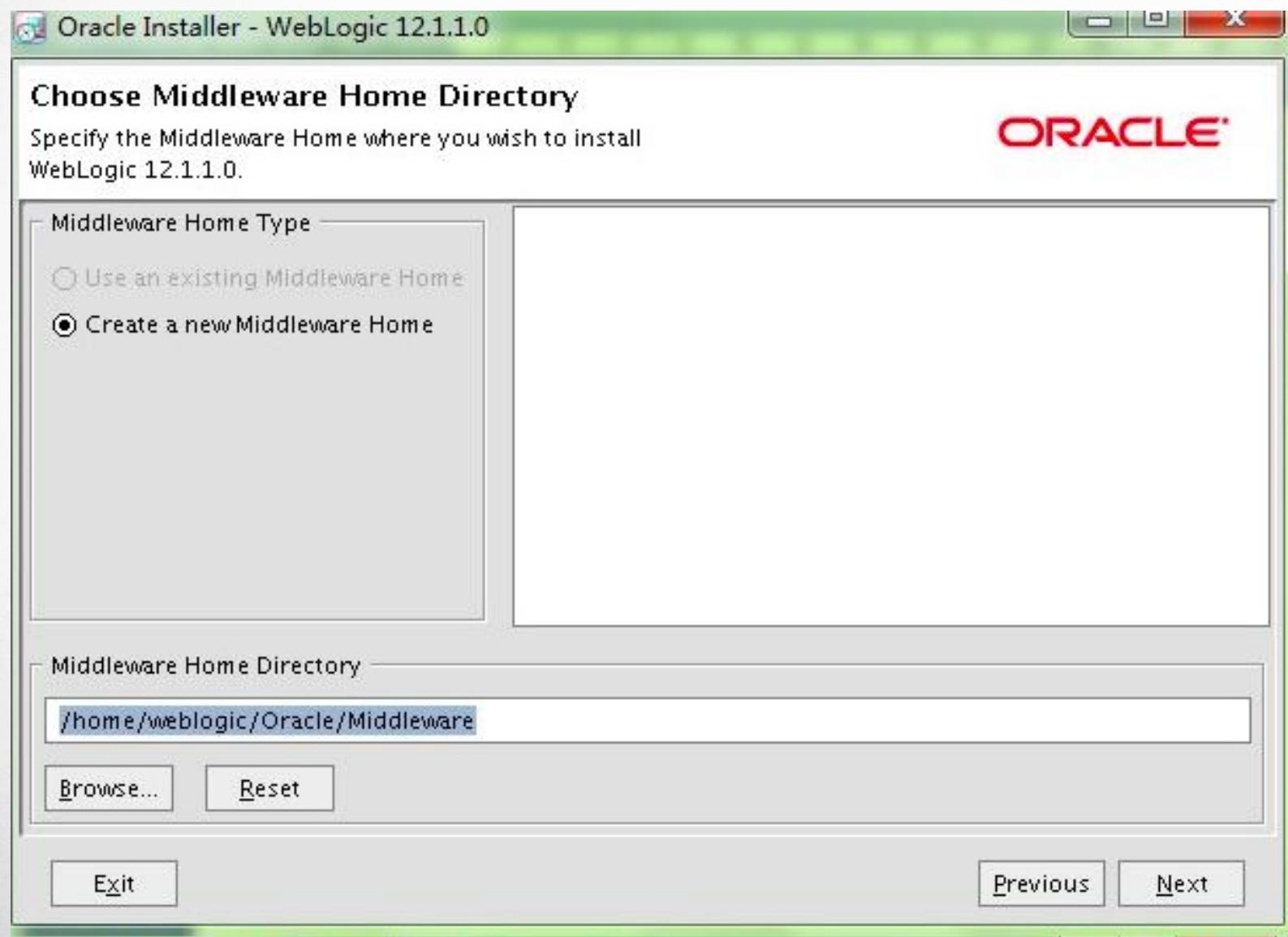
# Weblogic 的安全设置

---

## ➤ 安装Weblogic

- 1、配置JDK
- 2、用weblogic用户将wls1212\_generic.jar上传至/home/weblogic目录
- 3、运行命令java -jar wls1212\_generic.jar，弹出一下内容

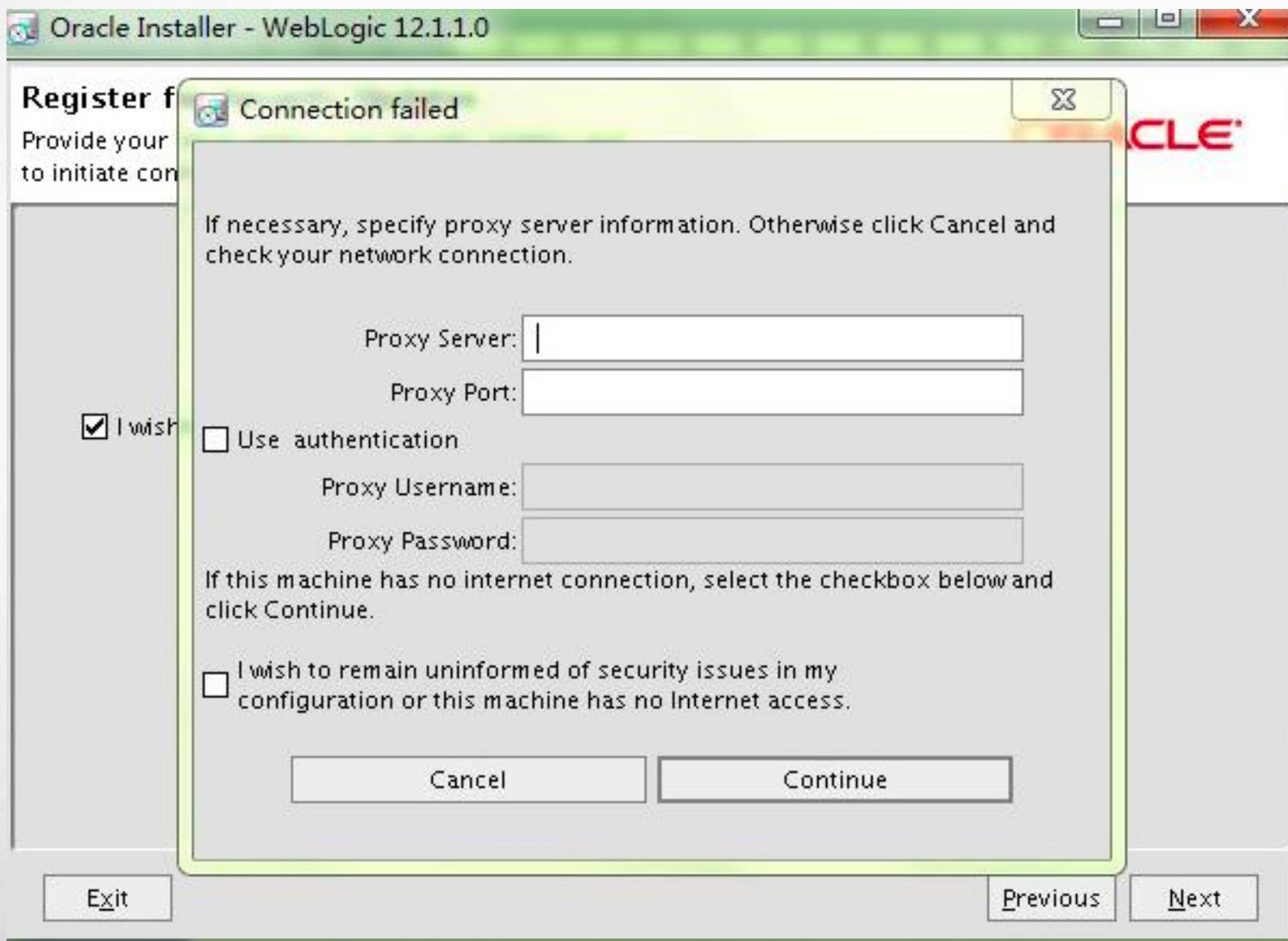
# Weblogic 的安全设置



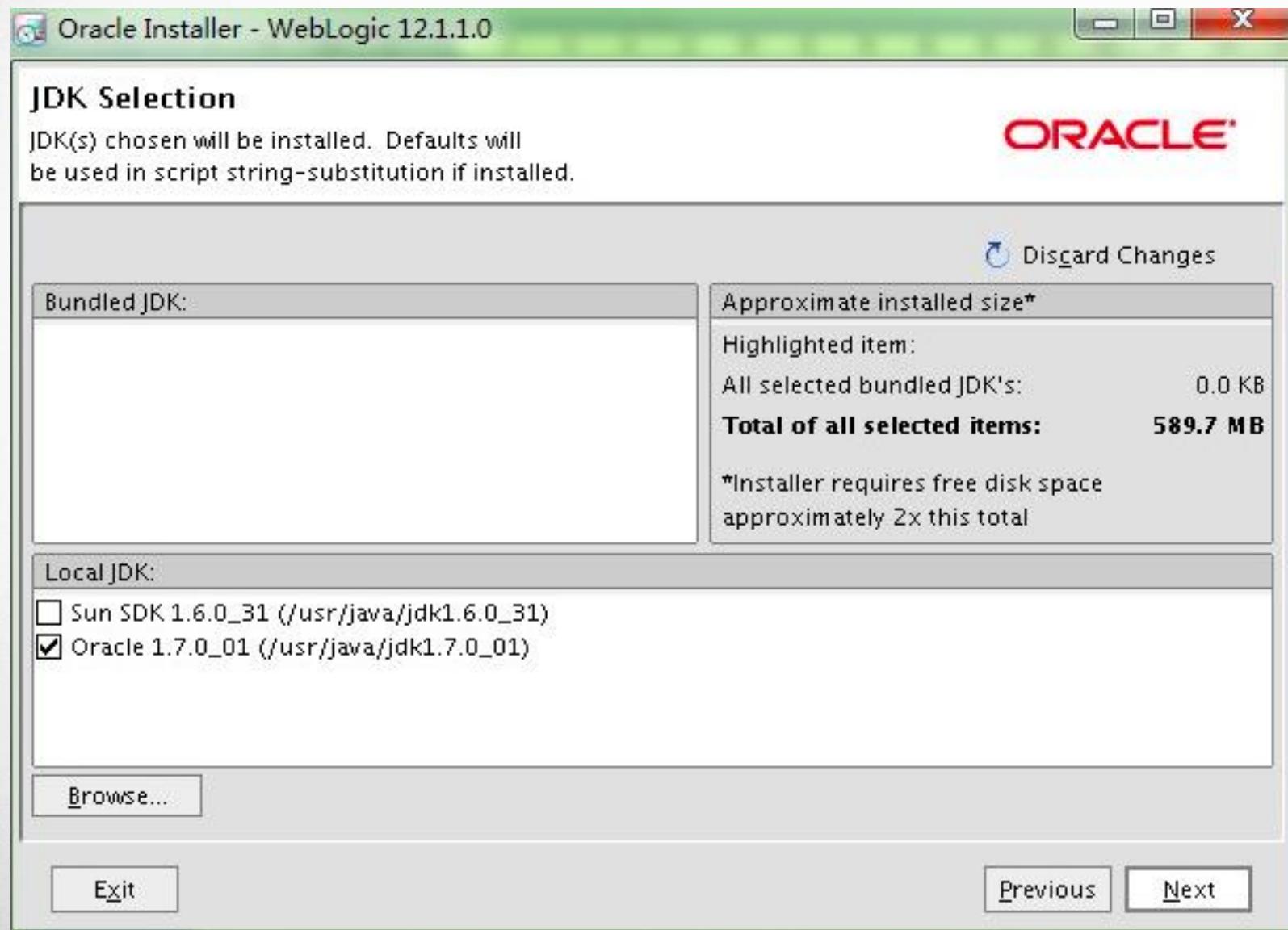
# Weblogic 的安全设置



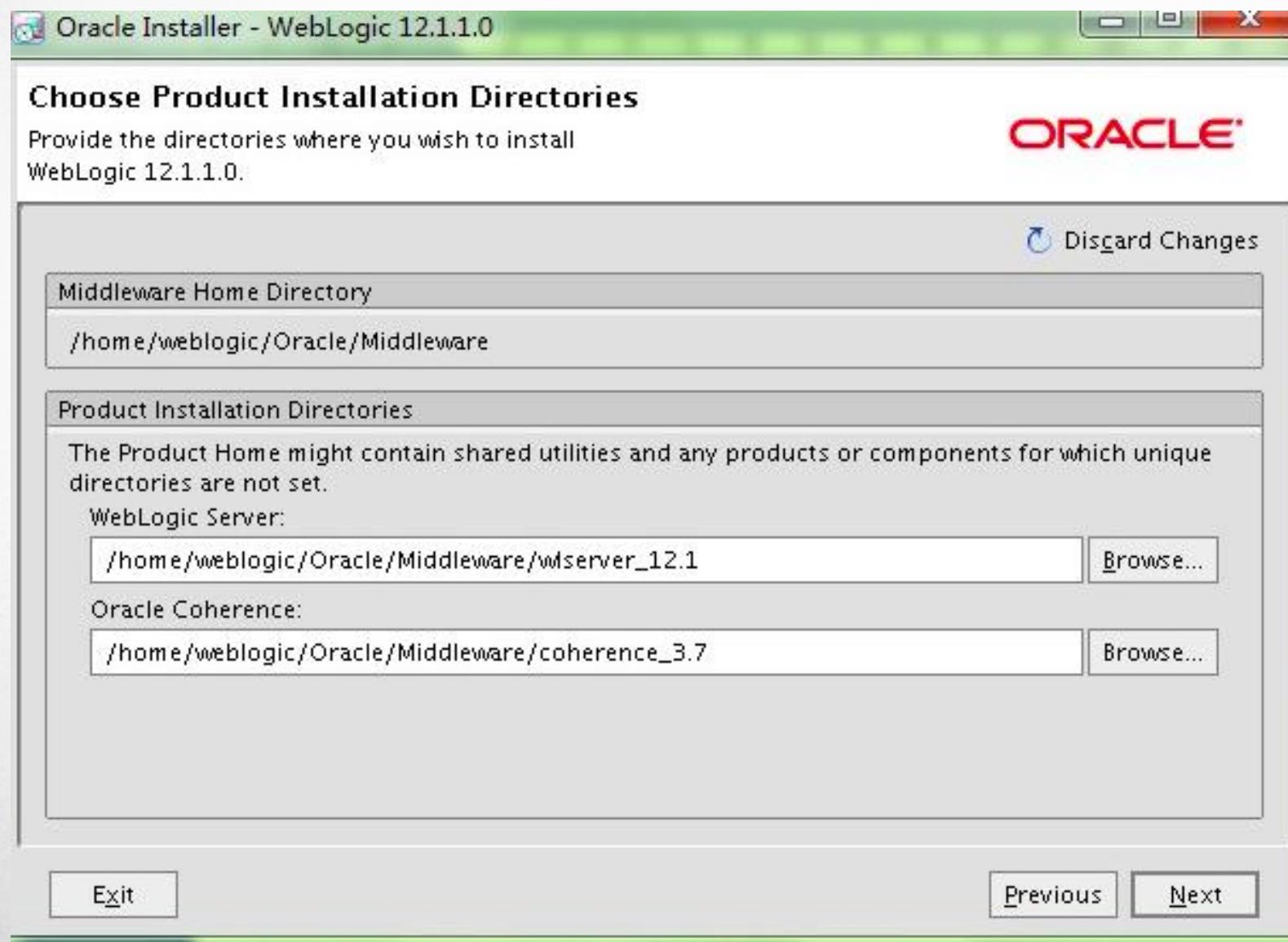
# Weblogic 的安全设置



# Weblogic 的安全设置



# Weblogic 的安全设置



# Weblogic 的安全设置



### ➤ 四、修改用户配置文件

- 1、使用weblogic用户登陆；
- 2、修改用户家目录添加JDK的环境变量

### ➤ 五、创建weblogic域

- 1、进入安装目录执行命令
- cd /home/weblogic/Oracle/Middleware/wlserver\_12.1/common/bin
- ./config.sh
- 2、执行命令后弹出如下窗口

# Weblogic 的安全设置

---

Choose between creating and extending a domain. Based on your selection, the Configuration wizard guides you through the steps to generate a new or extend an existing domain.

->1|Create a new WebLogic domain

    Create a WebLogic domain in your projects directory.

2|Extend an existing webLogic domain

    Use this option to add new components to an existing domain and modify configuration settings.

Enter index number to select OR [Exit][Next]> 1

# Weblogic 的安全设置

## ➤ 选择1创建新的weblogic域

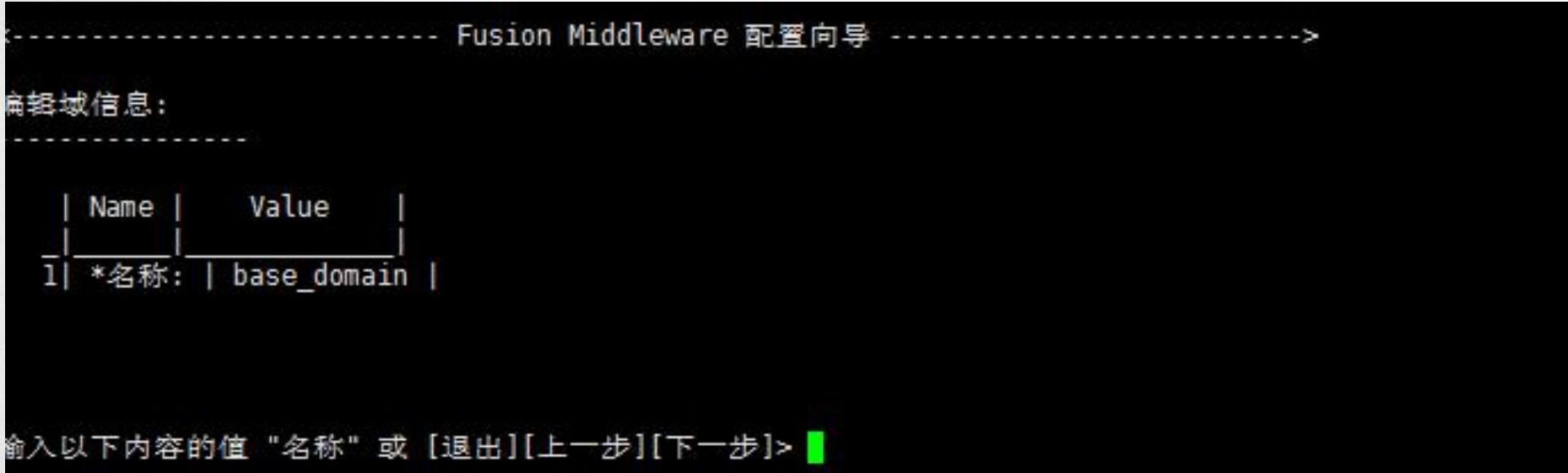


## ➤ 4、选择1 Weblogic Platform 组件



# Weblogic 的安全设置

- 选择默认的basic weblogic service domain



- 输入名称后确认更改，确认后输入域路径
- 例如:/home/weblogic/domains/

# Weblogic 的安全设置

全部设置确认后



- 选择对应的模式和对应版本的jdk，之后输入该版本jdk的路径
- 设置对应参数，主要包括
- 域名称，监听端口，监听的IP，SSL监听端口，是否已启用SSL
- 如果想修改上述参数可以直接通过该参数的数字编号进行修改。如果上述参数都已经配置正确，确认后创建完成。

# Weblogic 的安全设置

---

- 修改配置参数
- WebLogic的域配置文件为新建域路径下的config/config.xml文件。一般情况下需要修改的内容如下：
  - <app-deployment>
    - <name>AdminServer</name>
    - <target>AdminServer</target>
    - <module-type>war</module-type>
    - <source-path>/home/weblogic/domains/app</source-path>
    - <plan-dir>/home/weblogic/domains/plan</plan-dir>
    - <plan-path>/home/weblogic/domain/app/plan.xml</plan-path>
    - <security-dd-model>DDOnly</security-dd-model>
  - </app-deployment>

# Weblogic 的安全设置

---

- 域的配置文件是/domains/DOMAIN\_NAME/conf/config.xml。它用于指定域的名称以及域中每个服务器实例、集群、资源和服务的配置参数设置。常用到的参数有：
  - compilerSupportsEncoding 支持使用字符集
  - encoding 指定jsp文件的默认字符集，例如：gb2312
  - verbose 是否将调试信息输出到浏览器和日志
  - keepgenerated 是否让编译jsp文件产生的.java文件持续存在
  - Page Check Seconds 以秒为单位检查jsp文件是否有变化
  - Precompile 在Weblogic服务器启动时编译所有jsp

# Weblogic 的安全设置

## ➤ Weblogic目录结构

/bea	bea的主目录
-/jdkXXX.XX	预打包的JDK/jre
-/jrockitXXX.XXXX	预打包的jrockit
-/logs	安装bea产品的历史记录
-/utils	附加的/工具jar文件
-/weblogic81	weblogic server的根目录
-common	含有被weblogic server组件所共享的文件包括环境脚本模板文件评估软件
-javelin	workshop使用的java/jsp编译器
-samples	含有示例代码和资源
-server	
-config	
-examples	weblogic server示例应用和组件
--petstore	sun j2ee pet store应用
-eval	
-pointbase	含有pointbase数据库的评估版
-src	含有petstore和与weblogic server一起安装的示例的源代码和文件
-examples	
--petstore	
--stage	含有示例域部署前的客户和服务器类
-server	weblogic server 程序文件
-uninstall	用于卸载weblogic server的代码
-workshop	weblogic workshop应用
-license.bea	许可文件 (xml格式文件, 购买后需要覆盖这个文件)
-registry.xml	所有安装bea产品的记录文件
-updatelicense.cmd	更新license.bea文件

# Weblogic 的安全设置

---

## ➤ Weblogic目录结构

### ➤ Domain目录结构

|-/adminserver  
|-/applications  
|-/cfgwiz\_donotdelete  
|-/configArchive

管理服务器配置(config.xml配置文件,boot.properties可放置boot的用户名和密码加密保存。)  
应用服务器配置

# Weblogic 的安全设置

---

## ➤ 禁止 Weblogic 列表显示文件

在weblogic.xml文件中增加以下配置：

<index-directory-enabled> false </index-directory-enabled>，这个元素控制在找不到合适的索引文件的情况下是否自动生成HTML目录列表，默认值为false，即不自动生成目录。如果需要显示目录列表需要将改配置改为true即可。

# Weblogic 的安全设置

---

## 了解修改 Weblogic 的默认开放端口的方法

WebLogic在建立Domain的时候可以指定端口号。使用过程中也可以修改端口号，目前可以通过两种方式修改端口号：

方法一：通过管理窗口修改

- 1、打开WebLogic控制台，在左边的树状目录中找到Environment中的servers选项，点击后在右侧的窗体中找到需要修复的Server。
- 2、点击Server的Name，进入后如果选项是灰色的，请点击lock&edit按钮执行界面编辑解锁。在Listen Port后面的输入框中将现有的端口号替换为新的端口号后，点击保存完成修改。

方法二：修改配置文件

- 1、找到项目的安装路径中的config.xml文件。
- 2、编辑config.xml，搜索文件中的listen-port，看到的结果为<listen-port>**8080**</listen-port>，将尖括号中的端口号替换为新的端口号后保存退出即可。

# Weblogic 的漏洞利用与防范

---

- 一、Weblogic SSRF漏洞
- 1、漏洞利用实例
- SSRF漏洞，也称为XSPA（跨站端口攻击），问题存在于应用程序在加载用户提供的URL时，没能正确地验证服务器响应，然后就反馈了客户端。攻击者可以利用该漏洞绕过访问权限（如防火墙），进而将受感染服务器作为代理进行端口扫描，甚至访问系统中的数据。
- Weblogic既可以被外部主机访问，同时也允许访问内部主机，比如有一个jsp页面SearchPublicRegistries.jsp，我们可以利用它进行攻击，未经授权通过weblogic server连接任意主机的任意TCP端口，可能冗长的响应来推断在此端口是否有服务在监听次端口。

# Weblogic 的漏洞利用与防范

---

- 下面是一个没有服务监听TCP 23端口的例子:
- <https://10.0.0.1/uddiexplorer/SearchPublicRegistries.jsp?operator=http://10.0.0.4:23&rdosearch=name&txtSearchname=sdf&txtSearchkey=&txtSearchfor=&selfor=Business+location&btnSubmit=Search>
- 响应的片断如下:
- weblogic.uddi.client.structures.exception.XML\_SoapException: Connection refused
  
- 下面是一个有服务监听TCP 23端口的例子:
- <https://10.0.0.1/uddiexplorer/SearchPublicRegistries.jsp?operator=http://10.0.0.4:22&rdosearch=name&txtSearchname=sdf&txtSearchkey=&txtSearchfor=&selfor=Business+location&btnSubmit=Search>
  
- 响应片断如下:
- weblogic.uddi.client.structures.exception.XML\_SoapException: Received a response from url: http://10.0.0.4:22 which did not have a valid SOAP content-type: unknown/unknown.
- 可以利用这种功能来发现主机进行端口扫描

# Weblogic 的漏洞利用与防范

---

## ➤ 2、漏洞的防范

针对WebLogic的SSRF漏洞，如果业务不需要UDDI功能，就关闭这个功能。可以删除uddiexplorer文件夹，可以在 /weblogicPath/server/lib/uddiexplorer.war解压后，注释掉上面的jsp再打包。

其次，针对这个漏洞直接安装**oracle**的更新包。

更新包的下载地址为：

<http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html>

# Weblogic 的漏洞利用与防范

---

- 二、 Weblogic反序列化漏洞
- 1、 漏洞利用实例
  - 运行java命令java -jar CommonsCollectionsTools.jar weblogic ip port /tmp/out.txt
  - 执行该操作后，如果该IP的电脑在对应的目录生成out.txt文件，证明漏洞存在。  
~~(<http://download.csdn.net/detail/gongzi2311/9434593>)~~
  - 通过这个测试可以明确，攻击者可以利用该漏洞在服务器上直接创建文件，如果创建的文件可以获得执行权限，那么攻击者可以很轻松的获取服务器的ROOT权限。

# Weblogic 的漏洞利用与防范

---

- 2、漏洞的防范
  - 方法一：快速解决
  - 找到weblogic/Middleware/modules/com.bea.core.apache.commons.collections\_3.2.0.jar并打开，找到里面的org/apache/commons/collections/functors/InvokerTransformer.class，然后删除，保存即可。重新进行测试。
  - 方法二：打补丁
  - 需下载安装一下两个补丁包：
    - p20780171\_1036\_Generic.zip
    - p22248372\_1036012\_Generic.zip

# Weblogic 的日志审计

---

- wls主要有三种日志，放在目录： config/mydomain/logs下面：
  - 1.access.log                            http服务日志
  - 2.weblogic.log                        服务日志
  - 3.wl-domain.log                        域日志

# Weblogic 的日志审计

---

- WebLogic的access.log日志内容如下：
- 192.168.0.1 - - [09/12/2017:15:27:15 +0800] "GET /index.jsp HTTP/1.1" 200 100
- 在上面这条日志中对应的内容为：
  - 192.168.0.1→访问者IP
  - -→RFC931
  - -→auth\_user
  - [09/12/2017:15:27:15 +0800]→[访问时间]
  - GET→请求方式
  - /index.jsp→访问地址
  - HTTP/1.1→访问协议
  - 200→返回代码
  - 100→返回数据的字节数大小

# Weblogic 的日志审计

---

- 1、分析日志中访问的IP的top10
- # cat access.log | awk '{print \$1}' | sort -nr | uniq -c | sort -nr | top 10
- 命令解析：
  - (1) 输出access.log之后用awk命令截取输出的第一个字段 (awk默认以空格为分隔符)；
  - (2) 进行第一次排序，第一次排序的作用是把ip地址按照数字的顺序进行排序（逆序），方便进行去重操作。
  - (3) 之后进行去重，去重操作的输出中第一个字段为重复的量；
  - (4) 根据重复的次数再次进行排序（逆序）；
  - (5) 输出排序结果的前10行。

# Weblogic 的日志审计

---

- 2、分析日志中访问的URL的top10
- # cat access.log | awk '{print \$7}' | sort -nr | uniq -c | sort -nr | top 10
- 命令解析：
  - (1) 输出access.log之后用awk命令截取输出的第七个字段（awk默认以空格为分隔符）；
  - (2) 进行第一次排序，第一次排序的作用是将全部输出按照字母的顺序进行排序（逆序），方便进行去重操作。
  - (3) 之后进行去重，去重操作的输出中第一个字段为重复的量；
  - (4) 根据重复的次数再次进行排序（逆序）；
  - (5) 输出排序结果的前10行。

# Weblogic 的日志审计

---

- 3、获取UV和PV
- UV和PV是评价一个网站访问情况的标志性数据，UV的全称是User View，PV的全称是Page View。前者代表有多少用户访问了网站，后者则代表网站一共被浏览了多少次。UV和PV从日志获取的量只能算粗算，因为无法排除多用户通过同一个网关访问WebLogic。
- (1)粗算PV: `cat access.log | wc -l`
- (2)粗算UV: `cat access.log | awk '{print $1}' | sort -nr | uniq | wc -l`

# Weblogic 的日志审计

---

- 4、显示各种返回值 (http\_code) 的数量
- cat access.log | awk '{++S[\$8]} END {for(a in S) print a, S[a]}'
- 输出结果为：

400 2

404 1

500 1

200 6

THANK YOU 感谢观看  
FOR YOUR ATTENTION!

北京谷安天下科技有限公司

谷安天下公司主页：[www.gooann.com](http://www.gooann.com)

谷安培训教育网页：<http://px.gooann.com>

安全意识产品网页：<http://sectv.gooann.com>

产品解决方案网页：<http://product.gooann.com>

谷安信息安全商城：<http://gooannpx.taobao.com>