1. What is the default HTTP Port?

A)Oracle Business Activity Monitoring,9001, 9000-9080

Oracle HTTP Server SSL Listen Port, 4443, 4443-4543

Oracle HTTP Server non SSL Listen Port, 7777, 7777-7877

Oracle WebLogic Server Listen Port for Administration Server, 7001, 7001-9000

Oracle WebLogic Server Listen Port for Managed Server, 8001, 8000 – 8080

Oracle WebLogic Server Node Manager Port, 5556, 5556

Oracle WebLogic Server SSL Listen Port for Administration Server, 7002, 7002-9000

1. What is the difference between production mode and development mode?

Development mode:

a)The default JDK for development domain is Sun Hotspot

You can use the demo certificates for SSL

b)Auto deployment is enabled

c)Server instances rotate their log files on startup

d)Admin Server uses an automatically created boot.properties during startup

e)The default maximum capacity for JDBC Datasource is 15

f)The debugFlag which is used to start the WebLogic Workshop Debugger is enabled

Production mode:

a)The default JDK for production domain is JRockit

b)If you use the demo certificates for SSL a warning is displayed

c)Auto deployment is disabled

d)Server instances rotate their log files when it reaches 5MB

e)Admin Server prompts for username and password during startup

f)The default maximum capacity for JDBC Datasource is 25

g)The debugFlag which is used to start the WebLogic Workshop Debugger is disabled.

1. What is weblogic domain and what are the different servers?

A WebLogic Server administration **domain** is a logically related group of WebLogic Server resources. Domains include a special WebLogic Server instance called the **Administration Server**, which is the central point from which you configure and manage all resources in the domain. Usually, you configure a domain to include additional WebLogic Server instances called **Managed Servers**. You deploy Web applications, EJBs, and other resources onto the Managed Servers and use the Administration Server for configuration and management purposes only.

Multiple Managed Servers can be grouped into **clusters**, which enable you to balance loads and provide failover protection for critical applications, while using a single Administration Server simplifies the management of the Managed Server instances.

System administration in WebLogic Server is based on the J2EE Management model, in which each instance of a Web application server resource type is represented by a J2EE Managed Object (JMO). In WebLogic Server, each JMO is a wrapper for a corresponding MBean. You accomplish many WebLogic Server administration tasks by accessing MBeans, either directly using JMX, or through a JMX client like the WebLogic Administration Console or WebLogic Scripting Tool (WLST). For more information, see [Monitoring and Managing with the J2EE Management APIs](http://docs.oracle.com/cd/E13222_01/wls/docs90/j2eemanage/index.html) and *[WebLogic Server MBean Reference](http://docs.oracle.com/cd/E13222_01/wls/docs90/wlsmbeanref/core/index.html)*.

1. How do you find the version of WL Server?

**1.** From **registry.xml** in MW\_HOME  
Go to Middleware Home under which WebLogic is installed and look for file registry.xml  
Open registry.xml and search for “**component name=”WebLogic Server”**” version=”10.3.3.0″  (variable version next to this will tell you weblogic version)

**2.**From WebLogic **Admin Server log**file at $DOMAIN\_HOME/servers/AdminServer/admin/AdminServer.log and search for “**WebLogic Server**“. Output like below will tell you WebLogic Server version (10.3.4.0 as per output below)

\_\_\_\_\_\_\_\_  
WebLogic Server **10.3.4.0**  Fri Dec 17 20:47:33 PST 2010 1384255  Copyright (c) 1995, 2009, Oracle and/or its affiliates. All rights reserved.>  
\_\_\_\_\_\_\_\_

**3.** From class **weblogic.version**   
Go to directory which contains weblogic.jar ($WL\_HOME/server/lib) and run below command

**java -cp weblogic.jar weblogic.version**

1. What is the default Weblogic Admin console port number?7001
2. Which of the following statements is NOT True?

a)     Managed Servers in a Domain must run the same version of Weblogic Server

b)     A Domain comprises only the Admin Server, only the Managed Server, or the

        Administration and Managed Servers

c)     The Admin Server stores the configuration information and logs for a domain

d)     The Admin Server in a domain must run the same or higher version of WLS as the MS in the domain.

7.      Which of the following statements is NOT True?

a)     There can be multiple clusters in a domain

b)     All the servers in a cluster must be at the same version level

c)     All the server in a cluster must also be in the same domain

d)     A cluster can span multiple domains.

8.      The Admin Console is unavailable if the Admin Server is Shut Down.TRUE

a)     TRUE                     b)   FALSE

9.      Which of the following statement is true?

a)     There is one Node Manager for each Machine

b)     There is one Node Manager for each Domain

c)     There is one Node Manager for each Cluster

10. Oracle Weblogic Server 10.3 is certified with JDK 1.6?

a)     TRUE                     b)   FALSE

11. Net installer is preferred over the package installer if you want to install select components using only the custom option and have access to the Internet.

a)     TRUE                     b)   FALSE

12. How do you set up class path?

13. How to start Web logic Admin Server?

14. How many ways you can install weblogic?

15. How many domains you can create?

16. What weblogic utils contains?

17. Can we disable admin console?

18. Difference between Weblogic server and Web server?

19. What happens when we give www.abc.com in URL (what is process)?

20. Is Managed server can be restarted independently when admin is down?

21.  What is the difference between JNDI & JDBC?

22.  Difference between versions 8.X, 9.X, 10.X?

23.  What is the Connection Pool? How to create a Connection Pool?

24.  What is Domain? How many domains are possible in a single instance?

25.  What is DataSource? How can it is associated with connection pools ?

26.  Are WebLogic Servers password secure?

27.  Do you require JDK/JRE for installing a WL Domain?

28.  What is the basic requirement for starting a WebLogic server?

29.  What is the major difference between Managed Server and Admin Server?

30.  When starting the managed server it is coming to admin state. Click on resume button in admin Console, so that is coming to running state. How to resolve this problem for ever so that the server will come directly to running state instead of going to admin state?

31.  In which file/script we need to change the heap size? What is the variable name to search to change the heap size

32.  Where can we set Classpath, which will reflect to whole domain?

33.  What is MSI mode?

34.  How to find the heap memory of Managed Server?

35.  What happen if we deploy our component in weblogic server? What are the States?

36.  What is WLS T3 protocol?

37.  What is Node Manager and why it is required?

38.  How would you check the weblogic instance whether the server is started or not?

39.  Specify some important jar files in the weblogic server

**40**. How does the WLST communicate with WLS to retrieve and update resources on a running server?

1. What is domain in WLS ? how to create a domain in WLS ?

Before you can develop and run WebLogic Platform applications, you must first create a WebLogic Server domain. The Configuration Wizard guides you through the process of creating a new domain using configuration templates. A template is a Java Archive (JAR) file that contains the files and scripts required to create or update a domain.

A configuration template defines the full set of resources within a domain, including infrastructure components, applications, services, security options, and general environment and operating system options. BEA delivers a set of predefined configuration templates, which are described in the "Template Reference" at the following URL:

**5-1 Steps for Creating a Domain Using the Express Option**

**a)(** [Creating or Extending a Configuration](http://docs.oracle.com/cd/E13196_01/platform/docs81/confgwiz/newdom.html#1058947)**)** Choose whether to create a new WebLogic domain configuration or add to an existing domain configuration. To create a new domain, choose **Create a new WebLogic configuration.**

For details about adding to an existing domain configuration, see [Extending Domains.](http://docs.oracle.com/cd/E13196_01/platform/docs81/confgwiz/exten.html#1055092)

b)( [Selecting a Configuration Template](http://docs.oracle.com/cd/E13196_01/platform/docs81/confgwiz/newdom.html#1058774)) Choose the configuration template with which you want to create and configure your domain.

To determine whether the default settings for a configuration template meet your requirements, see "Template Reference" at the following URL:[http://download.oracle.com/docs/cd/E13196\_01/platform/docs81/confgwiz/tempref.html](http://docs.oracle.com/cd/E13196_01/platform/docs81/confgwiz/tempref.html" \t "new)

If necessary, you can update the domain later, as described in [Extending Domains.](http://docs.oracle.com/cd/E13196_01/platform/docs81/confgwiz/exten.html#1055092)

c)(

|  |  |
| --- | --- |
| [Choosing Express or Custom Configuration](http://docs.oracle.com/cd/E13196_01/platform/docs81/confgwiz/newdom.html#1058785) |  |

) Select the **Express** option to create a domain quickly, using the default template settings.

d)( [Configuring an Administrative Username and Password](http://docs.oracle.com/cd/E13196_01/platform/docs81/confgwiz/secur.html#1058962)) Specify a username and password to be used for starting the Administration Server.

e) ([Specifying the Server Start Mode and Java SDK](http://docs.oracle.com/cd/E13196_01/platform/docs81/confgwiz/newdom.html#1059075))Select the mode in which to launch your WebLogic domain configuration (development mode or production mode) and the Java Software Development Kit (SDK) that is enabled for the selected Startup mode.

f) ([Creating the WebLogic Configuration](http://docs.oracle.com/cd/E13196_01/platform/docs81/confgwiz/newdom.html#1066889))Review the domain details, specify the name and directory for the domain, and initiate the creation of the domain.

2. What is CONFIG.XML ?   
  
3. What is cluster and how to create a cluster in WLS ? how to configure cluster in webserver / PROXY ? tell complete configuration ?

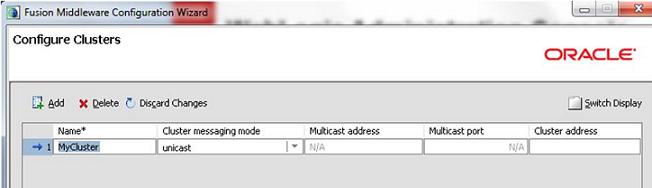
### >>(( Instructions on how to configure a WebLogic Cluster and use it with Oracle Http Server

#### By Laurent Goldsztejn on [Oct 22, 2012](https://blogs.oracle.com/WebLogicServer/entry/step_by_step_instruction_to)

On October 17th I delivered a webcast on WebLogic Clustering that included a demo with Apache as the proxy server.  I realized that many steps are needed to set up the configuration I used during the demo.  The purpose of this article is to go through these steps to show how quickly and easily one can define a new cluster and then proxy requests via an [Oracle Http Server](http://www.oracle.com/technetwork/middleware/ias/index-091236.html) (OHS).

The [domain configuration wizard](http://docs.oracle.com/cd/E24329_01/web.1211/e24499/newdom.htm#i1073602) offers the option to [create a cluster](http://docs.oracle.com/cd/E24329_01/web.1211/e24425/setup.htm).  The administration console or WLST, the Weblogic scripting tool can also be used to define a new cluster.  It can be created at any time but the servers that will participate in it cannot be in a running state.

### Cluster Creation using the configuration wizard



Network and architecture requirements need to be considered while choosing between unicast and multicast.

[Multicast Vs. Unicast with WebLogic Clustering](http://allthingsmdw.blogspot.com/2012/02/multicast-vs-unicast-with-weblogic.html) is of great help to make the best decision between the two messaging modes.  In addition, [Configure Cluster](http://docs.oracle.com/cd/E24329_01/web.1211/e24499/configuration_screens.htm#CIHDEIHH) offers details on each single field displayed above.

After this initial configuration page, individual servers could be assigned to this newly created cluster although servers can be added later to the cluster.  What is not recommended is for the Admin server to participate in a cluster as the main purpose of the Admin server is to perform the bulk of the processing for the domain.  Servers need to stop before being assigned to a cluster.  There is also no minimum number of servers that have to participate in the cluster.

At this point the configuration should be done and the cluster created successfully.  This can easily be verified from the console.

Each clustered managed server can be launched to join the cluster.

At startup the following messages should be logged for each clustered managed server:

<Notice> <WeblogicServer> <BEA-000365> <Server state changed to STARTING>

<Notice> <Cluster> <BEA-000197> <Listening for announcements from cluster using

*messaging\_mode* cluster messaging>

<Notice> <Cluster> <BEA-000133> <Waiting to synchronize with other running members

of *cluster\_name*>

It's time to try sending requests to the cluster and we will do this with the help of Oracle Http Server to play the role of a proxy server to demonstrate load balancing.

### Proxy Server configuration

The first step is to download [Weblogic Server Web Server Plugin](http://www.oracle.com/technetwork/middleware/ias/downloads/wls-plugins-096117.html) that will enhance the web server by handling requests aimed at being sent to the Weblogic cluster.  For our test [Oracle Http Server](http://docs.oracle.com/cd/E23943_01/web.1111/e16435/oracle.htm#CIABDFBJ) (OHS) will be used.  However plug-ins are also available for [Apache Http server](http://docs.oracle.com/cd/E23943_01/web.1111/e16435/apache.htm), [Microsoft Internet Information Server](http://docs.oracle.com/cd/E23943_01/web.1111/e16435/isapi.htm#BGBBCFID) (IIS), [Oracle iPlanet Webserver](http://docs.oracle.com/cd/E23943_01/web.1111/e16435/iplanet.htm#CHDCJIIA) or even WebLogic Server with the [HttpClusterServlet](http://docs.oracle.com/cd/E23943_01/web.1111/e13709/setup.htm#CLUST467).

Once OHS is installed on the system, the configuration file, mod\_wl\_ohs.conf, will need to be altered to include Weblogic proxy specifics.

First of all, add the following directive to instruct Apache to load the Weblogic shared object module extracted from the plugins file just downloaded.

LoadModule weblogic\_module modules/mod\_wl\_ohs.so

and then create an IfModule directive to encapsulate the following location block so that proxy will be enabled by path (each request including /wls will be directed directly to the WebLogic Cluster).  You could also proxy requests by MIME type using MatchExpression in the Location block.

<IfModule weblogic\_module>

<Location /wls>

   SetHandler weblogic-handler

   PathTrim /wls

   WebLogicCluster MS1\_URL:port,MS2\_URL:port

   Debug ON

   WLLogFile        c:/tmp/global\_proxy.log

   WLTempDir        "c:/myTemp"

   DebugConfigInfo  On

</Location>

</IfModule>

SetHandler specifies the handler for the plug-in module

PathTrim will instruct the plug-in to trim /w ls from the URL before forwarding the request to the cluster.

The list of WebLogic Servers defined in WeblogicCluster could contain a mixed set of clustered and single servers.  However, the dynamic list returned for this parameter will only contain valid clustered servers and may contain more servers if not all clustered servers are listed in WeblogicCluster.

### Testing proxy and load balancing

It's time to [start OHS web server](http://docs.oracle.com/cd/E17904_01/web.1111/e10144/getstart.htm#BEHFGCAE) which should at this point be configured correctly to proxy requests to the clustered servers.  By default round-robin is the load balancing strategy set by WebLogic.

Testing the load balancing can be easily done by disabling cookies on your browser given that a request containing a cookie attempts to connect to the primary server. If that attempt fails, the plug-in attempts to make a connection to the next available server in the list in a round-robin fashion.  With cookies enabled, you could use two different browsers to test the load balancing with a JSP page that contains the following:

<%@ page contentType="text/html; charset=iso-8859-1" language="java"  %>

<%

String path = request.getContextPath();

  String getProtocol=request.getScheme();

  String getDomain=request.getServerName();

  String getPort=Integer.toString(request.getLocalPort());

  String getPath = getProtocol+"://"+getDomain+":"+getPort+path+"/";

%>

<html>

<body>

Receiving Server <%=getPath%>

</body>

</html>

Assuming that you name the JSP page Test.jsp and the webapp that contains it TestApp, your browsers should open the following URL:

http://localhost/wls/TestApp/Test.jsp

Each browser should connect to a different clustered server and this simple JSP should confirm that.  The webapp that contains the JSP needs to be deployed to the cluster.

You can also verify that the load is correctly balanced by looking at the proxy log file.  Each request generates a set of log entries that starts with :

*timestamp* ================New Request:

Each request is associated with a primary server and a secondary server if one is available.  For our test request, the following entries should appear in the log as well:

Using Uri /wls/TestApp/Test.jsp

After trimming path: '/TestApp/Test.jsp'

The final request string is '/TestApp/Test.jsp'

If an exception occurs, it should also be logged in the proxy log file with the prefix:

*timestamp* \*\*\*\*\*\*\*Exception type

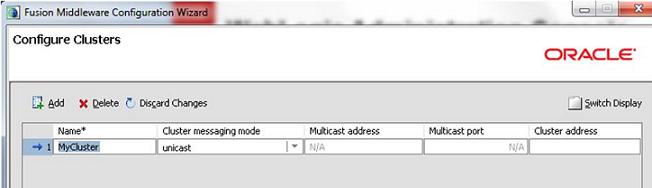
### WeblogicBridgeConfig

DebugConfigInfo enables runtime statistics and the production of configuration information.  For security purposes, this parameter should be turned off in production.

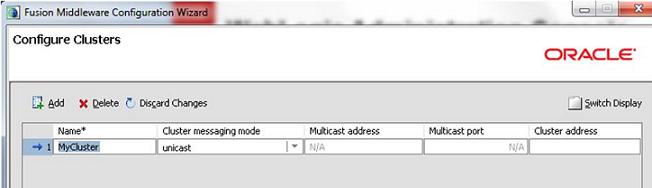
http://webserver\_host:port/path/xyz.jsp?\_\_WebLogicBridgeConfig will display a proxy bridge page detailing the plugin configuration followed by runtime statistics which could help in diagnosing issues along with the analyzing of the proxy log file.  In our example the url would be:

http://localhost/wls/TestApp/Test.jsp?\_\_WebLogicBridgeConfig

Here is how the top section of the screen can look like:



The bottom part of the page contains runtime statistics, here is a snippet of it (unrelated with the previous JSP example).



This entire plugin configuration should be very similar with other web servers, what varies is the name of the proxy server configuration file.

So, as you can see, it only takes a few minutes to configure a Weblogic cluster and get servers to join it.

))<<

A WebLogic Server cluster consists of multiple WebLogic Server server instances running simultaneously and working together to provide increased scalability and reliability. A cluster appears to clients to be a single WebLogic Server instance. The server instances that constitute a cluster can run on the same machine, or be located on different machines. You can increase a cluster’s capacity by adding additional server instances to the cluster on an existing machine, or you can add machines to the cluster to host the incremental server instances. Each server instance in a cluster must run the same version of WebLogic Server.

* Install WebLogic Server on the computer on which you want to run the server. See the WebLogic Server [Installation Guide](http://download.oracle.com/docs/cd/E12839_01/doc.1111/e14142/toc.htm).

**Note:**The Administration Server and all Managed Servers in a domain must be the same WebLogic Server version. See [Version Requirements for a Domain](http://download.oracle.com/docs/cd/E12839_01/web.1111/e13708/overview.htm#START114).

* Create servers. A cluster always contains at least one server. You can create additional servers. See [Create Managed Servers](http://docs.oracle.com/cd/E15523_01/apirefs.1111/e13952/taskhelp/domainconfig/CreateManagedServers.html).

A WebLogic Server cluster consists of multiple WebLogic Server server instances running simultaneously and working together to provide increased scalability and reliability. A cluster appears to clients to be a single WebLogic Server instance. The server instances that constitute a cluster can run on the same machine, or be located on different machines. You can increase a cluster’s capacity by adding additional server instances to the cluster on an existing machine, or you can add machines to the cluster to host the incremental server instances. Each server instance in a cluster must run the same version of WebLogic Server.

The main steps for creating and configuring clusters are:

1. Determine your cluster architecture.

For information on cluster architectures, see [Cluster Architectures](http://download.oracle.com/docs/cd/E12839_01/web.1111/e13709/planning.htm) in *Using WebLogic Server Clusters*.

1. [Start the Administration Server](http://download.oracle.com/docs/cd/E12839_01/web.1111/e13708/overview.htm).
2. [Create a cluster](http://docs.oracle.com/cd/E15523_01/apirefs.1111/e13952/taskhelp/clusters/CreateCluster.html).

For more information on configuring clusters, see [Configuration Roadmap](http://download.oracle.com/docs/cd/E12839_01/web.1111/e13709/setup.htm#CLUST456) in *Using WebLogic Server Clusters*.

1. [Configure clusters](http://docs.oracle.com/cd/E15523_01/apirefs.1111/e13952/taskhelp/clusters/ConfigureClusters.html).
2. [Assign servers to clusters](http://docs.oracle.com/cd/E15523_01/apirefs.1111/e13952/taskhelp/clusters/AssignServersToClusters.html).
3. Perform additional cluster configuration if required. See any of the following:
   * [Configure server migration in a cluster](http://docs.oracle.com/cd/E15523_01/apirefs.1111/e13952/taskhelp/clusters/ConfigureClusterMigration.html)
   * [Configure cross-cluster replication](http://docs.oracle.com/cd/E15523_01/apirefs.1111/e13952/taskhelp/clusters/SpecifyClusterReplicationGroups.html)
   * [Configure HTTP settings for a cluster](http://docs.oracle.com/cd/E15523_01/apirefs.1111/e13952/taskhelp/clusters/ConfigureClusterHTTP.html)
   * [Configure health monitoring in a cluster](http://docs.oracle.com/cd/E15523_01/apirefs.1111/e13952/taskhelp/clusters/MonitorClusters.html)
4. Control Managed Servers within the cluster. See any of the following:
   * [Start Managed Servers in a cluster](http://docs.oracle.com/cd/E15523_01/apirefs.1111/e13952/taskhelp/clusters/StartOrStopAServer.html)
   * [Shutdown servers in a cluster](http://docs.oracle.com/cd/E15523_01/apirefs.1111/e13952/taskhelp/clusters/ServerShutdownCluster.html)
5. Delete a cluster or remove Managed Servers from a cluster. See any of the following:
   * [Delete clusters](http://docs.oracle.com/cd/E15523_01/apirefs.1111/e13952/taskhelp/clusters/DeleteClusters.html)
   * [Remove servers from a cluster](http://docs.oracle.com/cd/E15523_01/apirefs.1111/e13952/taskhelp/clusters/RemoveServers.html)

4. What kind of PROXY u are using in your project ?   
  
5. What is SSL and how to provide security ? what is certificate ?

Secure Sockets Layer (SSL) provides secure connections by allowing two applications connecting over a network connection to authenticate the other's identity and by encrypting the data exchanged between the applications. Authentication allows a server and optionally a client to verify the identity of the application on the other end of a network connection. Encryption makes data transmitted over the network intelligible only to the intended recipient.

SSL in WebLogic Server is an implementation of the SSL 3.0 and Transport Layer Security (TLS) 1.0 specifications.

WebLogic Server supports SSL on a dedicated listen port which defaults to 7002. To establish an SSL connection, a Web browser connects to WebLogic Server by supplying the SSL listen port and the HTTPs protocol in the connection URL, for example, https://myserver:7002.

Using SSL is computationally intensive and adds overhead to a connection. Avoid using SSL in development environments when it is not necessary. However, always use SSL in a production environment.

6. What is one way SSL and two way ssl ?

One Way SSL - Only the client authenticates the server   
- This means that the public cert of the server needs to configured in the trust store of the client for this to happen.  
  
Two Way SSL - The client authenticates the server & the server also authenticates the client.   
- This means that the public cert of the server needs to configured in the trust store of the client for this to happen.  
- Also the public cert of the client needs to be configured on the server's trust store  
  
7. How to generate certificates ? where you can store certificates ?   
  
8. What is THREAD DUMP , why thread dump is necessary in which scenario we will be taking thread dump ?

A thread dump is a snapshot of the state of all threads that are part of the process. The state of each thread is presented with a so called stack trace, which shows the contents of a thread’s stack. Some of the threads belong to the Java application you are running, while others are JVM internal threads.

A thread dump reveals information about an application’s thread activity that can help you diagnose problems and better optimize application and JVM performance; for example, thread dumps automatically show the occurrence of a deadlock. Deadlocks bring some or all of an application to a complete halt.

## Creating Thread Dumps

To create a thread dump from a process, do either of the following:

* + Press Ctrl-Break while the process is running (or by sending SIGQUIT to the process on Linux).
  + Enter the following at the command line at startup:  
    bin\jrcmd.exe <pid> print\_threads

The thread dump appears at the command line.

|  |  |
| --- | --- |
| **Note:** | For more information about jrcmd and Ctrl-Break handlers, see [Running Diagnostic Commands](http://docs.oracle.com/cd/E13150_01/jrockit_jvm/jrockit/geninfo/diagnos/ctrlbreakhndlr.html). |

## Reading Thread Dumps

This section describes the typical contents of a thread dump by going through an example thread dump from the beginning to end. First, an example thread dump, broken up into its components is presented (see [Listing 20-1](http://docs.oracle.com/cd/E13150_01/jrockit_jvm/jrockit/geninfo/diagnos/using_threaddumps.html#wp1091976),[Listing 20-2](http://docs.oracle.com/cd/E13150_01/jrockit_jvm/jrockit/geninfo/diagnos/using_threaddumps.html#wp1092037), [Listing 20-3](http://docs.oracle.com/cd/E13150_01/jrockit_jvm/jrockit/geninfo/diagnos/using_threaddumps.html#wp1095116), [Listing 20-4](http://docs.oracle.com/cd/E13150_01/jrockit_jvm/jrockit/geninfo/diagnos/using_threaddumps.html#wp1092211) and [Listing 20-5](http://docs.oracle.com/cd/E13150_01/jrockit_jvm/jrockit/geninfo/diagnos/using_threaddumps.html#wp1094022)). First, information about the main thread is printed, then all the JVM internal threads, followed by all other Java application threads (if there are any). Finally, information about lock chains are printed.

The example thread dump is taken from a program that creates three threads that are quickly forced into a deadlock. The application threads Thread-0, Thread-1, and Thread-2 correspond to three different classes in the Java code.

### The Beginning of The Thread Dump

The thread dump starts with the date and time of the dump, and the version number of the JRockit JVM used (see [Listing 20-1](http://docs.oracle.com/cd/E13150_01/jrockit_jvm/jrockit/geninfo/diagnos/using_threaddumps.html#wp1091976)).

**Listing 20-1 The initial information of a thread dump**

===== FULL THREAD DUMP ===============  
Wed Feb 21 13:46:45 2007  
BEA JRockit(R) R27.1.0-109-73164-1.5.0\_08-20061129-1428-windows-ia32

### Stack Trace for Main Application Thread

[Listing 20-2](http://docs.oracle.com/cd/E13150_01/jrockit_jvm/jrockit/geninfo/diagnos/using_threaddumps.html" \l "wp1092037) shows the stack trace of the main application thread. There is a thread information line, followed by information about locks and a trace of the thread’s stack at the moment of the thread dump.

**Listing 20-2 The main thread in the thread dump**

"Main Thread" id=1 idx=0x2 tid=48652 prio=5 alive, in native, waiting  
-- Waiting for notification on: util/repro/Thread1@0x01226528[fat lock]  
at jrockit/vm/Threads.waitForSignal(J)Z(Native Method)  
at java/lang/Object.wait(J)V(Native Method)  
at java/lang/Thread.join(Thread.java:1095)  
^-- Lock released while waiting: util/repro/Thread1@0x01226528[fat lock]  
at java/lang/Thread.join(Thread.java:1148)  
at util/repro/DeadLockExample.main(DeadLockExample.java:23)  
at jrockit/vm/RNI.c2java(IIII)V(Native Method)  
-- end of trace

After the name and other identification information, the different status messages of the main thread are printed. The main thread in [Listing 20-2](http://docs.oracle.com/cd/E13150_01/jrockit_jvm/jrockit/geninfo/diagnos/using_threaddumps.html#wp1092037) is a running thread (alive), it is either executing JVM internal code or user-defined JNI code (in native), and it is currently waiting for an object to be released (waiting). If a thread is waiting on a notification on a lock (by calling Object.wait()), this is indicated at the top of the stack trace as Waiting for notification on.

### Locks and Lock Chains

For each thread, the JRockit JVM prints the following information:

* + If the thread is trying to take a lock (to enter a synchronized block), but the lock is already held by another thread, this is indicated at the top of the stack trace, as “Blocked trying to get lock”.
  + If the thread is waiting on a notification on a lock (by calling Object.wait()), this is indicated at the top of the stack trace as “Waiting for notification”.
  + If the thread has taken any locks, this is shown in the stack trace. After a line in the stack trace describing a function call is a list of the locks taken by the thread in that function. This is described as ^-- Holding lock(where the ^-- serves as a reminder that the lock is taken in the function written above the line with the lock).

The semantics for waiting (for notification) on an object in Java is somewhat complex. First, to enter a synchronized block, you must take the lock for the object, and then you call wait() on that object. In the wait method, the lock is released before the thread actually goes to sleep waiting for a notification. When it receives a notification, wait re-takes the lock before returning. So, if a thread has taken a lock, and is waiting (for notification) on that lock, the line in the stack trace that describes when the lock was taken is not shown as “Holding lock,” but as “Lock released while waiting.”

All locks are described as Classname@0xLockID[LockType]; for example:

java/lang/Object@0x105BDCC0[thin lock]

Classname@0xLockID describe the object to which the lock belongs. The classname is an exact description, the fully qualified classname of the object. LockID, on the other hand, is a temporary ID which is only valid for a single thread dump. That is, you can trust that if a thread A holds a lock java/lang/Object@0x105BDCC0, and a thread B is waiting for a lock java/lang/Object@0x105BDCC0, in a single thread dump, then it is the same lock. If you do any subsequent thread dumps however, LockID is not comparable and, even if a thread holds the same lock, it might have a different LockID and, conversely, the same LockID does not guarantee that it holds the same lock.LockType describes the JVM internal type of the lock (fat, thin, recursive, or lazy). The status of active locks (monitors) is also shown in stack traces.

#### Presentation of Locks Out of Order

The lines with the lock information might not always be correct, due to compiler optimizations. This means two things:

* + If a thread, in the same function, takes lock A first and then lock B, the order in which they are printed is unspecified.
  + If a thread, in method foo() calls method bar(), and takes a lock A in bar(), the lock might be printed as being taken in foo().

Normally, this should not be a problem. The order of the lock lines should never move much from their correct position. Also, lock lines will never be missing—you can be assured that all locks taken by a thread are shown in the thread dump.

### JVM Internal Threads

[Listing 20-3](http://docs.oracle.com/cd/E13150_01/jrockit_jvm/jrockit/geninfo/diagnos/using_threaddumps.html" \l "wp1095116) shows the traces of JVM internal threads. The threads have been marked as daemon threads, as can be seen by their daemon state indicators. Daemon threads are either JVM internal threads (as in this case) or threads marked as daemon threads by java.lang.Thread.setDaemon().

**Listing 20-3 The first and last thread in a list of JVM internal Threads**

"(Signal Handler)" id=2 idx=0x4 tid=48668 prio=5 alive, in native, daemon

[...]

"(Sensor Event Thread)" id=10 idx=0x1c tid=48404 prio=5 alive, in native, daemon

As you can see, lock information and stack traces are not printed for the JVM internal threads in [Listing 20-3](http://docs.oracle.com/cd/E13150_01/jrockit_jvm/jrockit/geninfo/diagnos/using_threaddumps.html#wp1095116). This is the default setting.

If you want to see stack traces for the JVM internal threads, then use the parameter nativestack=true when you send the print\_threads handler. At the command line, write the following:

bin\jrcmd.exe <pid> print\_threads nativestack=true

### Other Java Application Threads

Normally, you will primarily be interested in the threads of the Java application you are running (including the main thread). All Java application threads except the main thread are presented near the end of the thread dump.[Listing 20-4](http://docs.oracle.com/cd/E13150_01/jrockit_jvm/jrockit/geninfo/diagnos/using_threaddumps.html#wp1092211) shows the stack traces of three different application threads.

**Listing 20-4 Additional application threads**

"Thread-0" id=11 idx=0x1e tid=48408 prio=5 alive, in native, blocked  
-- Blocked trying to get lock: java/lang/Object@0x01226300[fat lock]  
at jrockit/vm/Threads.waitForSignal(J)Z(Native Method)  
at jrockit/vm/Locks.fatLockBlockOrSpin(ILjrockit/vm/ObjectMonitor;II)V(Unknown Source)  
at jrockit/vm/Locks.lockFat(Ljava/lang/Object;ILjrockit/vm/ObjectMonitor;Z)Ljava/lang/Object;(Unknown Source)  
at  
jrockit/vm/Locks.monitorEnterSecondStage(Ljava/lang/Object;I)Ljava/lang/Object;(Unknown Source)  
at jrockit/vm/Locks.monitorEnter(Ljava/lang/Object;)Ljava/lang/Object;(Unknown Source)  
at util/repro/Thread1.run(DeadLockExample.java:34)  
^-- Holding lock: java/lang/Object@0x012262F0[thin lock]  
^-- Holding lock: java/lang/Object@0x012262F8[thin lock]  
at jrockit/vm/RNI.c2java(IIII)V(Native Method)  
-- end of trace

"Thread-1" id=12 idx=0x20 tid=48412 prio=5 alive, in native, blocked  
-- Blocked trying to get lock: java/lang/Object@0x012262F8[thin lock]  
at jrockit/vm/Threads.sleep(I)V(Native Method)  
at jrockit/vm/Locks.waitForThinRelease(Ljava/lang/Object;I)I(Unknown Source)  
at jrockit/vm/Locks.monitorEnterSecondStage(Ljava/lang/Object;I)Ljava/lang/Object;(Unknown Source)  
at jrockit/vm/Locks.monitorEnter(Ljava/lang/Object;)Ljava/lang/Object;(Unknown Source)  
at util/repro/Thread2.run(DeadLockExample.java:48)  
at jrockit/vm/RNI.c2java(IIII)V(Native Method)  
-- end of trace

"Thread-2" id=13 idx=0x22 tid=48416 prio=5 alive, in native, blocked  
-- Blocked trying to get lock: java/lang/Object@0x012262F8[thin lock]  
at jrockit/vm/Threads.sleep(I)V(Native Method)  
at jrockit/vm/Locks.waitForThinRelease(Ljava/lang/Object;I)I(Unknown Source)  
at jrockit/vm/Locks.monitorEnterSecondStage(Ljava/lang/Object;I)Ljava/lang/Object;(Unknown Source)  
at jrockit/vm/Locks.monitorEnter(Ljava/lang/Object;)Ljava/lang/Object;(Unknown Source)  
at util/repro/Thread3.run(DeadLockExample.java:65)  
^-- Holding lock: java/lang/Object@0x01226300[fat lock]  
at jrockit/vm/RNI.c2java(IIII)V(Native Method)  
-- end of trace

All three threads are in a blocked state (indicated by blocked), which means that they are all trying to enter synchronized blocks. Thread-0 is trying to take Object@0x01226300[fat lock] but this is held by Thread-2. Both Thread-2 and Thread-1 are trying to take Object@0x012262F8[thin lock] but this lock is held by Thread-0. This means that Thread-0 and Thread-2 form a deadlock, while Thread-1 is blocked.

### Lock Chains

One prominent feature of the JRockit JVM is that it automatically detects deadlocked, blocked and open lock chains among the running threads. The analysis in [Listing 20-5](http://docs.oracle.com/cd/E13150_01/jrockit_jvm/jrockit/geninfo/diagnos/using_threaddumps.html#wp1094022) presents the all the lock chains created by the threads T1, T2, T3, T4 and T5. This information can be used to tune and troubleshoot your Java code.

**Listing 20-5 Deadlocked and blocked lock chains**

Circular (deadlocked) lock chains  
=================================  
Chain 6:  
"Dead T1" id=16 idx=0x48 tid=3648 waiting for java/lang/Object@0x01225018 held by:  
"Dead T3" id=18 idx=0x50 tid=900 waiting for java/lang/Object@0x01225010 held by:  
"Dead T2" id=17 idx=0x4c tid=3272 waiting for java/lang/Object@0x01225008 held by:  
"Dead T1" id=16 idx=0x48 tid=3648

Blocked lock chains  
===================  
Chain 7:  
"Blocked T2" id=20 idx=0x58 tid=3612 waiting for java/lang/Object@0x01225310 held by:  
"Blocked T1" id=19 idx=0x54 tid=2500 waiting for java/lang/Object@0x01224B60 held by:   
"Open T3" id=13 idx=0x3c tid=1124 in chain 1

Open lock chains  
================  
Chain 1:  
"Open T5" id=15 idx=0x44 tid=4048 waiting for java/lang/Object@0x01224B68 held by:  
"Open T4" id=14 idx=0x40 tid=3380 waiting for java/lang/Object@0x01224B60 held by:  
"Open T3" id=13 idx=0x3c tid=1124 waiting for java/lang/Object@0x01224B58 held by:  
"Open T2" id=12 idx=0x38 tid=3564 waiting for java/lang/Object@0x01224B50 held by:  
"Open T1" id=11 idx=0x34 tid=2876 (active)

## Thread Status in Thread Dumps

This section describes the different statuses or states a thread can show in a thread dump. There are three types of states:

* + [Life States](http://docs.oracle.com/cd/E13150_01/jrockit_jvm/jrockit/geninfo/diagnos/using_threaddumps.html" \l "wp1087802)
  + [Run States](http://docs.oracle.com/cd/E13150_01/jrockit_jvm/jrockit/geninfo/diagnos/using_threaddumps.html" \l "wp1087831)
  + [Special States](http://docs.oracle.com/cd/E13150_01/jrockit_jvm/jrockit/geninfo/diagnos/using_threaddumps.html" \l "wp1087872)

### Life States

[Table 20-1](http://docs.oracle.com/cd/E13150_01/jrockit_jvm/jrockit/geninfo/diagnos/using_threaddumps.html" \l "wp1087810) describes the life states a thread can show in a thread dump.

|  |  |
| --- | --- |
| **Table 20-1 Thread Life States** | |
| **State** | **Description** |
| alive | This is a normal, running thread. Virtually all threads in the thread dump will be alive. |
| not started | The thread has been requested to start running by java.lang.Thread.start(), but the actual OS process has not yet started, or executed far enough to pass control to the JRockit JVM. It is extremely unlikely to see this value. A java.lang.Thread object that is created, but not has had start() executed, will not show up in the thread dump. |
| terminated | This thread has finished its run() method and has also notified any threads joining on it, but it is still kept in the JVM internal thread structure for running threads. It is extremely unlikely to see this value. A thread that has been terminated for a time longer than a few milliseconds will not show up in the thread dump. |

### Run States

[Table 20-2](http://docs.oracle.com/cd/E13150_01/jrockit_jvm/jrockit/geninfo/diagnos/using_threaddumps.html" \l "wp1087839) describes the run states a thread can show in a thread dump.

|  |  |
| --- | --- |
| **Table 20-2 Thread Run States** | |
| **State** | **Description** |
| blocked | This thread has tried to enter a synchronized block, but the lock was taken by another thread. This thread is blocked until the lock gets released. |
| blocked (on thin lock) | This is the same state as blocked, but with the additional information that the lock in question is a thin lock. |
| waiting | This thread has called Object.wait() on an object. The thread will remain there until some other thread sends a notification on that object. |
| sleeping | This thread has called java.lang.Thread.sleep(). |
| parked | This thread has called java.util.concurrent.locks.LockSupport.park(). |
| suspended | The thread’s execution has been suspended by java.lang.Thread.suspend() or a JVMTI/JVMPI agent call |

### Special States

[Table 20-3](http://docs.oracle.com/cd/E13150_01/jrockit_jvm/jrockit/geninfo/diagnos/using_threaddumps.html" \l "wp1094512) describes the special states a thread can show in a thread dump. Note that all these states are not mutually exclusive.

## Troubleshooting with Thread Dumps

This section contains information on about how to use thread dumps for troubleshooting and diagnostics.

To use thread dumps for troubleshooting, beyond detecting deadlocks, you need to take several thread dumps from the same process. However, if you want to do long time analysis of behavior you will likely be more helped by combining occasional thread dumps with other diagnostics tools, such as the JRockit Runtime Analyzer, which is part of Oracle JRockit Mission Control (see [Using Oracle JRockit Mission Control Tools](http://docs.oracle.com/cd/E13150_01/jrockit_jvm/jrockit/geninfo/diagnos/intromiscon.html) for more information).

### Detecting Deadlocks

The Oracle JRockit JVM automatically analyzes the thread dump information and detects whether there exists any circular (deadlocked) or blocked lock chains in it.

### Detecting Processing Bottlenecks

For detecting more than deadlocks in your threads, you have to make several consecutive thread dumps. This lets you detect the occurrence of contention, where multiple threads are trying to get the same lock. Contention might create long open lock chains that, while not deadlocked, will degrade performance.

If you discover (in a set of consecutive thread dumps) that one or more threads in your application is temporarily stuck waiting for a lock to be released, then you might have reason to look over the code of your Java application to see if the synchronization (serialization) is necessary or if the threads can be organized differently.

### Viewing The Runtime Profile of an Application

By making several consecutive thread dumps, you might quickly get an overview of which parts of your Java application that are most heavily used. However, you should consult the **Threads** tab in JRockit Management Console for more detailed information about the workload on the different parts of your application.

9. How do u take thread dump ?

Kill -3 java 🡪 through OS

Samurai Tool  
  
10. What is performance tuning ? how do u tune the performance step by step procedure ? ANS : tell from OS Lever to Our Application Level

Each WebLogic Server instance runs in its own dedicated Java Virtual Machine (JVM) which is their runtime environment. Every Admin Server in any domain executes within a JVM. The same also applies for Managed Servers. WebLogic Server can be used for a wide variety of applications and services which uses the same runtime environment and resources. Oracle WebLogic ships with 2 different JVM, HotSpot and JRocket but you can choose which JVM you want to use.   
  
JVM is designed to optimize itself however it also provides some startup options to make small changes. There are default values for its memory and garbage collection. In real world, you will not want to stick with the default values provided by the JVM rather want to customize these values based on your applications which can produce large gains in performance by making small changes with the JVM parameters. We can tell the garbage collector how to delete garbage and we can also tell JVM how much space to allocate for each generation (of java Objects) or for heap. Remember during the garbage collection no other process is executed within the JVM or runtime, which is called STOP THE WORLD which can affect the overall throughput.   
  
  
Each JVM has its own memory segment called Heap Memory which is the storage for java Objects. These objects can be grouped based on their age like young generation (recently created objects) or old generation (surviving objects that have lived to some extent), etc. A java object is considered garbage when it can no longer be reached from anywhere in the running program. Each generation has its own memory segment within the heap. When this segment gets full, garbage collector deletes all the objects that are marked as garbage to create space. When the old generation space gets full, the JVM performs a major collection to remove the unused objects and reclaim their space. A major garbage collect takes a significant amount of time and can affect system performance.   
  
When we create a managed server either on the same machine or on remote machine it gets its initial startup parameters from $DOMAIN\_HOME/bin/setDomainEnv.sh/cmd file.  
By default two parameters are set:  
  
    Xms: The initial heapsize  
    Xmx: The max heapsize  
  
  
**Try to set equal initial and max heapsize. The startup time can be a little longer but for long running applications it will provide a better performance.**  
  
When we set -Xms512m -Xmx1024m, the physical heap size will be 512m. This means that there are pages of memory (in the state of the 512m) that the JVM does not explicitly control. It will be controlled by OS which could be reserve for the other tasks. In this case, it is an advantage if the JVM claims the entire memory at once and try not to spend time to extend when more memory is needed. Also you can use -XX:MaxPermSize (Maximum size of the permanent generation) option for Sun JVM. You should adjust the size accordingly if your application dynamically load and unload a lot of classes in order to optimize the performance.  
  
You can set the JVM options/heap size from the following places:  
  
    Through the Admin console, in the Server start tab (Please note this feature is enabled ONLY if managed server is started via nodemanage/Admin Console and StartScriptEnabled is set to false in the nodemanager.properties which is default)  
  
11. What is HEAP and how to increase it ?   
  
12. What is OOM problem / memory leak , how to overcome this problem ?

# Out of Memory" error message appears when you have a large number of programs running,

I am using WLS 10.3.6 with JRockit . I am a newbie working with WLS  
  
I keep facing an issue where the machine(16gb ram and 500gb HDD ) were weblogic is deployed keep getting out of memory .. I only used the default configuration for the weblogic deployment that came with the weblogic installation .  
  
There is only one adf application running on the weblogic which is accessed by around two to three people ..  
  
What additional changes needs to be done?  
  
Second question is that is there a way to find how many DB connections are open currently in the weblogic and how long its been open?   
  
What debug option can be used to find the reason for out of memory erro?

By default weblogic will give min heap as -Xms256m and max heap as -Xmx512m and if you are using Sun JDK it will use MaxPermsize as 128m.  
  
  
Now to avoid such OOOM (Out of Memory) issue try to increase these parameters.  
  
  
If you are using 64 bit I would suggest to use 2GB Minimum or 8Gb MaX so ideal one would be like this.  
  
-Xms3072m -Xmx3072m MaxPermSize=1024m  
  
If you are using 32 bit then we cannot increase more than 2 GB there.  
  
  
Now coming to Connection with DB is purely depend on how many Max connection pool size had set there with in Datasource.  
  
Datasource --> Connection Pool -->  
  
  
Initial capacity and Max pool size and increment size.  
  
  
So try to set max pool according to your requirement by default it would be 15 Max and 1 initial capacity and 1 for increment.  
  
Now for third option you need not keep any further debug simply check the logs to find out the exact cause of the OOM issue and collect heap dump and gc logs.

As you are using JRockit, you can use mission control to get more information about the why the out-of-memory error is occurring.  
For example, you can run a flight recording and monitor the live data on the heap. If you see the live data constantly rising, it might  
be smart to run the memory leak detector, with which you can pinpoint the culprit. Examples of how to use the flight recording  
and memory leak detector are provided here: http://middlewaremagic.com/weblogic/?p=6930.  
  
In order to find out, how many database connections are currently open, you can use the monitoring tab of your datasource.  
Note that initially it not showing much information, this can be changed by clicking on the 'edit table' link. Here you have attributes  
such 'active connections...', Active Connections Current Count: The number of connections currently in use by applications.  
  
If you suspect the application to be leaking connections, you can also set a value higher than zero to the Inactive Connection Timeout  
"The number of inactive seconds on a reserved connection before WebLogic Server reclaims the connection and releases it back into the connection pool.  
You can use the Inactive Connection Timeout feature to reclaim leaked connections - connections that were not explicitly closed by the application. Note   
that this feature is not intended to be used in place of properly closing connections. When set to 0, the feature is disabled."  
This parameter is present on the connection pool, configuration tab of your data source.  
  
What you also can try to do is disable the statement caching, by setting the statement cache size to zero. Statement Cache Size       
"The number of prepared and callable statements stored in the cache. (This may increase server performance.) WebLogic Server can reuse statements   
in the cache without reloading the statements, which can increase server performance. Each connection in the connection pool has its own cache of statements.  
Setting the size of the statement cache to 0 turns off statement caching."  
Note that the database itself caches statements as well.  
  
We also had a similar issue with the statement caching on WebLogic and ADF, which also ran into out-of-memory errors. By turning of the statement caching  
on the WebLogic side the issue (in our case) got resolved.

Thanks for the reply . When i tried to connect to the remote server using mission control, I was unable to connect even after proving the following parameters in the java options .  
  
Xmanagement:ssl=false,authenticate=false,port=7099 Djava.rmi.server.hostname=hostAddress(where weblogic is located).  
  
And how do i get the heap dumb and garbage collection logs before the server crashed ?  
  
Since i am new to this . What are the things i should be looking for to detect the problem ? How long should a normal flight be run ? Does running it for a long time increase jvm memory utilization too ?

13. Complete trouble shooting steps ?

# Troubleshooting Common Problems

This chapter provides guidelines on how to prevent cluster problems or troubleshoot them if they do occur.

# Before You Start the Cluster

You can do a number of things to help prevent problems before you boot the cluster.

## Check for a Cluster License

Your WebLogic Server license must include the clustering feature. If you try to start a cluster without a clustering license, you will see the error message **Unable to find a license for clustering**.

## Check the Server Version Numbers

All Managed Servers in a cluster and the cluster's Administration Server should run under the same version of WebLogic Server. The major and minor version numbers (e.g 6.1), service packs, and attached patch levels should be same across the cluster.

## Check the Multicast Address

A problem with the multicast address is one of the most common reasons a cluster does not start or a server fails to join a cluster.

A multicast address is required for each cluster. The multicast address can be an IP number between 224.0.0.0 and 239.255.255.255, or a host name with an IP address within that range.

You can check a cluster's multicast address and port on its Configuration-->Multicast tab in the Administration Console.

For each cluster on a network, the combination of multicast address and port must be unique. If two clusters on a network use the same multicast address, they should use different ports. If the clusters use different multicast addresses, they can use the same port or accept the default port, 7001.

Before booting the cluster, make sure the cluster's multicast address and port are correct and do not conflict with the multicast address and port of any other clusters on the network.

The errors you are most likely to see if the multicast address is bad are:

Unable to create a multicast socket for clustering

Multicast socket send error

Multicast socket receive error

## Check the CLASSPATH Value

Make sure the value of CLASSPATH is the same on all managed servers in the cluster. CLASSPATH is set by the setEnv script, which you run before you run startManagedWebLogic to start the managed servers.

By default, setEnv sets this value for CLASSPATH (as represented on Windows systems):

set WL\_HOME=C:\bea\weblogic700  
set JAVA\_HOME=C:\bea\jdk131  
.  
.  
**set CLASSPATH=%JAVA\_HOME%\lib\tools.jar;  
 %WL\_HOME%\server\lib\weblogic\_sp.jar;  
 %WL\_HOME%\server\lib\weblogic.jar;  
 %CLASSPATH%**

If you change the value of CLASSPATH on one managed server, or change how setEnv sets CLASSPATH, you must change it on all managed servers in the cluster.

## Check the Thread Count

Each server instance in the cluster has a default execute queue, configured with a fixed number of execute threads. To view the thread count for the default execute queue, choose the Configure Execute Queue command on the Advanced Options portion of the Configuration> General tab for the server. The default thread count for the default queue is 15, and the minimum value is 5. If the value of Thread Count is below 5, change it to a higher value so that the Managed Server does not hang on startup.

# After You Start the Cluster

This section describes first troubleshooting steps to perform if you have problems trying to start a cluster.

## Check Your Commands

If the cluster fails to start, or a server fails to join the cluster, the first step is to check any commands you have entered, such as startManagedWebLogic or a java interpreter command, for errors and misspellings.

## Generate a Log File

Before contacting BEA Technical Support for help with cluster-related problems, collect diagnostic information. The most important information is a log file with multiple thread dumps from a Managed Server. The log file is especially important for diagnosing cluster freezes and deadlocks.

Remember: a log file that contains multiple thread dumps is a prerequisite for diagnosing your problem.

1. Stop the server.
2. Remove or back up any log files you currently have. You should create a new log file each time you boot a server, rather than appending to an existing log file.
3. Start the server with this command, which turns on verbose garbage collection and redirects both the standard error and standard output to a log file:

% java -ms64m -mx64m **-verbose:gc** -classpath $CLASSPATH  
 -Dweblogic.domain=mydomain -Dweblogic.Name=clusterServer1  
 -Djava.security.policy==$WL\_HOME/lib/weblogic.policy  
 -Dweblogic.admin.host=192.168.0.101:7001  
 weblogic.Server **>> logfile.txt**

Redirecting both standard error and standard output places thread dump information in the proper context with server informational and error messages and provides a more useful log.

1. Continue running the cluster until you have reproduced the problem.
2. If a server hangs, use kill -3 or <Ctrl>-<Break> to create the necessary thread dumps to diagnose your problem. Make sure to do this several times on each server, spaced about 5-10 seconds apart, to help diagnose deadlocks.

**Note:** If you are running the JRockit JVM under Linux, see [Getting a JRockit Thread Dump Under Linux](http://docs.oracle.com/cd/E13222_01/wls/docs81/cluster/trouble.html#603279).

1. Compress the log file using a Unix utility:

% tar czf logfile.tar logfile.txt

- or zip it using a Windows utility.

1. Attach the compressed log file to an e-mail to your BEA Technical Support representative. Do not cut and paste the log file into the body of an e-mail.
2. If the compressed log file is too large, you can use the BEA Customer Support FTP site.

### Getting a JRockit Thread Dump Under Linux

If you use the JRockit JVM under Linux, use one of the following methods to generate a thread dump.

* Use the weblogic.admin THREAD\_DUMP command. For instructions and limitations, see [THREAD\_DUMP](http://docs.oracle.com/cd/E13222_01/wls/docs81/admin_ref/cli.html#THREAD_DUMP) in WebLogic Server Command Reference.
* If the JVM's management server is enabled (by starting the JVM with the -Xmanagement option), you can generate a thread dump using the JRockit Management Console.
* Use Kill -3 *PID*, where *PID* is the root of the process tree.

To obtain the root PID, perform a:

ps -efHl | grep 'java' \*\*. \*\*

using a grep argument that is a string that will be found in the process stack that matches the server startup command. The first PID reported will be the root process, assuming that the ps command has not been piped to another routine.

Under Linux, each execute thread appears as a separate process under the Linux process stack. To use Kill -3 on Linux you supply must match PID of the main WebLogic execute thread, otherwise no thread dump will be produced.

## Check Garbage Collection

If you are experiencing cluster problems, you should also check the garbage collection on the managed servers. If garbage collection is taking too long, the servers will not be able to make the frequent heartbeat signals that tell the other cluster members they are running and available.

If garbage collection (either first or second generation) is taking 10 or more seconds, you need to tune heap allocation (the msmx parameter) on your system.

## Run utils.MulticastTest

You can verify that multicast is working by running utils.MulticastTest from one of the managed servers. See [Using the WebLogic Server Java Utilities](http://docs.oracle.com/cd/E13222_01/wls/docs81/admin_ref/utils.html) in WebLogic Server Command Reference.

14. How to provide the security in proxy ?

## Uses

A proxy server has a variety of potential purposes, including:

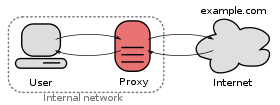
* To keep machines behind it anonymous, mainly for [security](http://en.wikipedia.org/wiki/Computer_security).[[1]](http://en.wikipedia.org/wiki/Proxy_server#cite_note-1)
* To speed up access to resources (using caching). Web proxies are commonly used to [cache](http://en.wikipedia.org/wiki/Web_cache) web pages from a web server.[[2]](http://en.wikipedia.org/wiki/Proxy_server#cite_note-2)
* To prevent downloading the same content multiple times (and save bandwidth).
* To log / audit usage, e.g. to provide company employee Internet usage reporting.
* To scan transmitted content for malware before delivery.
* To scan outbound content, e.g., for data loss prevention.
* To bypass website restrictions at work.
* Access enhancement/restriction
  + To apply access policy to network services or content, e.g. to block undesired sites.
  + To access sites prohibited or filtered by your ISP or institution.
  + To bypass security / parental controls.
  + To circumvent Internet filtering to access content otherwise blocked by governments.[[3]](http://en.wikipedia.org/wiki/Proxy_server#cite_note-3)
  + To allow a web site to make web requests to externally hosted resources (e.g. images, music files, etc.) when cross-domain restrictions prohibit the web site from linking directly to the outside domains.
  + To allow the browser to make web requests to externally hosted content on behalf of a website when cross-domain restrictions (in place to protect websites from the likes of data theft) prohibit the browser from directly accessing the outside domains.

## Types of proxy

A proxy server may run right on the user's local computer, or at various points between the user's computer and destination servers on the Internet.

* A proxy server that passes requests and responses unmodified is usually called a [gateway](http://en.wikipedia.org/wiki/Gateway_(computer_networking)) or sometimes a *tunneling proxy*.
* A forward proxy is an Internet-facing proxy used to retrieve from a wide range of sources (in most cases anywhere on the Internet).
* A [reverse proxy](http://en.wikipedia.org/wiki/Reverse_proxy) is usually an Internet-facing proxy used as a front-end to control and protect access to a server on a private network, commonly also performing tasks such as load-balancing, authentication, decryption or caching.

### Forward proxies

[](http://en.wikipedia.org/wiki/File:Forward_proxy_h2g2bob.svg)

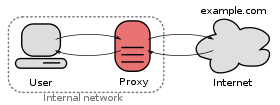
[http://bits.wikimedia.org/static-1.22wmf12/skins/common/images/magnify-clip.png](http://en.wikipedia.org/wiki/File:Forward_proxy_h2g2bob.svg)

A forward proxy taking requests from an internal network and forwarding them to the Internet.

Forward proxies are proxies where the client server names the target server to connect to.[[4]](http://en.wikipedia.org/wiki/Proxy_server#cite_note-apache-forward-reverse-4) Forward proxies are able to retrieve from a wide range of sources (in most cases anywhere on the Internet).

The terms "forward proxy" and "forwarding proxy" are a general description of behavior (forwarding traffic) and thus ambiguous. Except for Reverse proxy, the types of proxies described in this article are more specialized sub-types of the general forward proxy concept.

### Open proxies

[](http://en.wikipedia.org/wiki/File:Open_proxy_h2g2bob.svg)

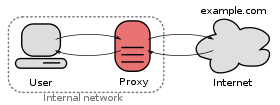
[http://bits.wikimedia.org/static-1.22wmf12/skins/common/images/magnify-clip.png](http://en.wikipedia.org/wiki/File:Open_proxy_h2g2bob.svg)

An open proxy forwarding requests from and to anywhere on the Internet.

*Main article:*[*Open proxy*](http://en.wikipedia.org/wiki/Open_proxy)

An open proxy is a forwarding proxy server that is accessible by any Internet user. [Gordon Lyon](http://en.wikipedia.org/wiki/Gordon_Lyon) estimates there are "hundreds of thousands" of open proxies on the Internet.[[5]](http://en.wikipedia.org/wiki/Proxy_server#cite_note-nmap-5) An*anonymous open proxy* allows users to conceal their [IP address](http://en.wikipedia.org/wiki/IP_address) while browsing the Web or using other Internet services. There are varying degrees of anonymity however, as well as a number of methods of 'tricking' the client into revealing itself regardless of the proxy being used.

### Reverse proxies

[](http://en.wikipedia.org/wiki/File:Reverse_proxy_h2g2bob.svg)

[http://bits.wikimedia.org/static-1.22wmf12/skins/common/images/magnify-clip.png](http://en.wikipedia.org/wiki/File:Reverse_proxy_h2g2bob.svg)

A reverse proxy taking requests from the Internet and forwarding them to servers in an internal network. Those making requests connect to the proxy and may not be aware of the internal network.

*Main article:*[*Reverse proxy*](http://en.wikipedia.org/wiki/Reverse_proxy)

A **reverse proxy** (or surrogate) is a proxy server that appears to clients to be an ordinary server. Requests are forwarded to one or more origin servers which handle the request. The response from the origin server is returned as if it came directly from the proxy server, leaving the client no knowledge of the origin servers.[[4]](http://en.wikipedia.org/wiki/Proxy_server#cite_note-apache-forward-reverse-4)

Reverse proxies are installed in the neighborhood of one or more web servers. All traffic coming from the Internet and with a destination of one of the neighborhood's web servers goes through the proxy server. The use of "reverse" originates in its counterpart "forward proxy" since the reverse proxy sits closer to the web server and serves only a restricted set of websites.

There are several reasons for installing reverse proxy servers:

* Encryption / SSL acceleration: when secure web sites are created, the SSL encryption is often not done by the web server itself, but by a reverse proxy that is equipped with SSL acceleration hardware. See [Secure Sockets Layer](http://en.wikipedia.org/wiki/Secure_Sockets_Layer). Furthermore, a host can provide a single "SSL proxy" to provide SSL encryption for an arbitrary number of hosts; removing the need for a separate SSL Server Certificate for each host, with the downside that all hosts behind the SSL proxy have to share a common DNS name or IP address for SSL connections. This problem can partly be overcome by using the *SubjectAltName* feature of [X.509](http://en.wikipedia.org/wiki/X.509) certificates.
* [Load balancing](http://en.wikipedia.org/wiki/Load_balancing_(computing)): the reverse proxy can distribute the load to several web servers, each web server serving its own application area. In such a case, the reverse proxy may need to rewrite the URLs in each web page (translation from externally known URLs to the internal locations).
* Serve/cache static content: A reverse proxy can offload the web servers by caching static content like pictures and other static graphical content.
* Compression: the proxy server can optimize and compress the content to speed up the load time.
* Spoon feeding: reduces resource usage caused by slow clients on the web servers by caching the content the web server sent and slowly "spoon feeding" it to the client. This especially benefits dynamically generated pages.
* Security: the proxy server is an additional layer of defense and can protect against some OS and Web Server specific attacks. However, it does not provide any protection to attacks against the web application or service itself, which is generally considered the larger threat.
* Extranet Publishing: a reverse proxy server facing the Internet can be used to communicate to a firewall server internal to an organization, providing extranet access to some functions while keeping the servers behind the firewalls. If used in this way, security measures should be considered to protect the rest of your infrastructure in case this server is compromised, as its web application is exposed to attack from the Internet.

### Performance Enhancing Proxies

*Main article:*[*Performance Enhancing Proxy*](http://en.wikipedia.org/wiki/Performance_Enhancing_Proxy)

A proxy that is designed to mitigate specific link related issues or degradations. PEPs (Performance Enhancing Proxies) are typically used to improve TCP performance in the presence of high Round Trip Times (RTTs) and wireless links with high packet loss. They are also frequently used for highly asynchronous links featuring very different upload and download rates.

## Uses of proxy servers

### Filtering

*Further information:*[*Content-control software*](http://en.wikipedia.org/wiki/Content-control_software)

A [content-filtering](http://en.wikipedia.org/wiki/Content_filtering) web proxy server provides administrative control over the content that may be relayed in one or both directions through the proxy. It is commonly used in both commercial and non-commercial organizations (especially schools) to ensure that Internet usage conforms to [acceptable use policy](http://en.wikipedia.org/wiki/Acceptable_use_policy). In some cases users can circumvent the proxy, since there are services designed to proxy information from a filtered website through a non filtered site to allow it through the user's proxy.[[6]](http://en.wikipedia.org/wiki/Proxy_server#cite_note-Bypassing_a_Filtering_Proxy-6)

A content filtering proxy will often support [user authentication](http://en.wikipedia.org/wiki/Authentication), to control web access. It also usually produces [logs](http://en.wikipedia.org/wiki/Server_log), either to give detailed information about the URLs accessed by specific users, or to monitor [bandwidth](http://en.wikipedia.org/wiki/Bandwidth_(computers)) usage statistics. It may also communicate to [daemon](http://en.wikipedia.org/wiki/Daemon_(computer_software))-based and/or [ICAP](http://en.wikipedia.org/wiki/Internet_Content_Adaptation_Protocol)-based [antivirus software](http://en.wikipedia.org/wiki/Antivirus_software) to provide security against virus and other [malware](http://en.wikipedia.org/wiki/Malware) by scanning incoming content in real time before it enters the network.

Many work places, schools, and colleges restrict the web sites and online services that are made available in their buildings. This is done either with a specialized proxy, called a content filter (both commercial and free products are available), or by using a cache-extension protocol such as [ICAP](http://en.wikipedia.org/wiki/Internet_Content_Adaptation_Protocol), that allows plug-in extensions to an open caching architecture.

Some common methods used for content filtering include: [URL](http://en.wikipedia.org/wiki/Blacklist_(Computing)) or [DNS blacklists](http://en.wikipedia.org/wiki/DNSBL), [URL](http://en.wikipedia.org/wiki/URL) regex filtering, [MIME](http://en.wikipedia.org/wiki/MIME) filtering, or content keyword filtering. Some products have been known to employ content analysis techniques to look for traits commonly used by certain types of content providers.

Requests made to the open internet must first pass through an outbound proxy filter. The web-filtering company provides a database of URL patterns (regular expressions) with associated content attributes. This database is updated weekly by site-wide subscription, much like a virus filter subscription. The administrator instructs the web filter to ban broad classes of content (such as sports, pornography, online shopping, gambling, or social networking). Requests that match a banned URL pattern are rejected immediately.

Assuming the requested URL is acceptable, the content is then fetched by the proxy. At this point a dynamic filter may be applied on the return path. For example, [JPEG](http://en.wikipedia.org/wiki/JPEG) files could be blocked based on fleshtone matches, or language filters could dynamically detect unwanted language. If the content is rejected then an HTTP fetch error is returned and nothing is cached.

Most web filtering companies use an internet-wide crawling robot that assesses the likelihood that a content is a certain type. The resultant database is then corrected by manual labor based on complaints or known flaws in the content-matching algorithms.

#### Filtering of encrypted data

Web filtering proxies are not able to peer inside secure sockets HTTP transactions, assuming the chain-of-trust of SSL/TLS has not been tampered with.

The SSL/TLS chain-of-trust relies on trusted root certificate authorities. In a workplace setting where the client is managed by the organization, trust might be granted to a root certificate whose private key is known to the proxy. Concretely, a root certificate generated by the proxy is installed into the browser CA list by IT staff.

In such situations, proxy analysis of the contents of a SSL/TLS transaction becomes possible. The proxy is effectively operating a [man-in-the-middle attack](http://en.wikipedia.org/wiki/Man-in-the-middle_attack), allowed by the client's trust of a root certificate the proxy owns.

### Caching

A **caching proxy** server accelerates service requests by retrieving content saved from a previous request made by the same client or even other clients. Caching proxies keep local copies of frequently requested resources, allowing large organizations to significantly reduce their upstream bandwidth usage and costs, while significantly increasing performance. Most ISPs and large businesses have a caching proxy. Caching proxies were the first kind of proxy server. Some poorly implemented caching proxies have had downsides (e.g., an inability to use user authentication). Some problems are described in [RFC 3143](http://tools.ietf.org/html/rfc3143) (Known HTTP Proxy/Caching Problems). Another important use of the proxy server is to reduce the hardware cost. An organization may have many systems on the same network or under control of a single server, prohibiting the possibility of an individual connection to the Internet for each system. In such a case, the individual systems can be connected to one proxy server, and the proxy server connected to the main server.

### Translation

A translation proxy is a proxy server that is used to localize a website experience for different markets. Traffic from global audiences is routed through the translation proxy to the source website. As visitors browse the proxied site, requests go back to the source site where pages are rendered. Original language content in the response is replaced by translated content as it passes back through the proxy. The translations used in a translation proxy can be either machine translation, human translation, or a combination of machine and human translation. Different translation proxy implementations have different capabilities. Some allow further customization of the source site for local audiences such as excluding source content or substituting source content with original local content.

### DNS proxy

A [DNS proxy server](http://en.wikipedia.org/wiki/Domain_Name_System) takes DNS queries from a (usually local) network and forwards them to an Internet Domain Name Server. It may also cache DNS records.

### Bypassing filters and censorship

If the destination server filters content based on the origin of the request, the use of a proxy can circumvent this filter. For example, a server using [IP](http://en.wikipedia.org/wiki/Internet_Protocol)-based [geolocation](http://en.wikipedia.org/wiki/Geolocation" \o "Geolocation) to restrict its service to a certain country can be accessed using a proxy located in that country to access the service. Likewise, an incorrectly configured proxy can provide access to a network otherwise isolated from the Internet.[[5]](http://en.wikipedia.org/wiki/Proxy_server#cite_note-nmap-5)

### Logging and eavesdropping

Proxies can be installed in order to [eavesdrop](http://en.wikipedia.org/wiki/Eavesdropping) upon the data-flow between client machines and the web. All content sent or accessed – including passwords submitted and [cookies](http://en.wikipedia.org/wiki/HTTP_cookie) used – can be captured and analyzed by the proxy operator. For this reason, passwords to online services (such as webmail and banking) should always be exchanged over a cryptographically secured connection, such as SSL. By chaining proxies which do not reveal data about the original requester, it is possible to obfuscate activities from the eyes of the user's destination. However, more traces will be left on the intermediate hops, which could be used or offered up to trace the user's activities. If the policies and administrators of these other proxies are unknown, the user may fall victim to a false sense of security just because those details are out of sight and mind. In what is more of an inconvenience than a risk, proxy users may find themselves being blocked from certain Web sites, as numerous forums and Web sites block IP addresses from proxies known to have [spammed](http://en.wikipedia.org/wiki/Spam_(electronic)) or [trolled](http://en.wikipedia.org/wiki/Troll_(Internet)) the site. Proxy bouncing can be used to maintain your privacy.

### Accessing services anonymously

*Main article: [Anonymizer](http://en.wikipedia.org/wiki/Anonymizer" \o "Anonymizer)*

An anonymous proxy server (sometimes called a web proxy) generally attempts to anonymize web surfing. There are different varieties of [anonymizers](http://en.wikipedia.org/wiki/Anonymizer" \o "Anonymizer). The destination server (the server that ultimately satisfies the web request) receives requests from the anonymizing proxy server, and thus does not receive information about the end user's address. The requests are not anonymous to the anonymizing proxy server, however, and so a degree of trust is present between the proxy server and the user. Many proxy servers are funded through a continued advertising link to the user. **Access control**: Some proxy servers implement a logon requirement. In large organizations, authorized users must log on to gain access to the [web](http://en.wikipedia.org/wiki/World_Wide_Web). The organization can thereby track usage to individuals. Some anonymizing proxy servers may forward data packets with header lines such as HTTP\_VIA, HTTP\_X\_FORWARDED\_FOR, or HTTP\_FORWARDED, which may reveal the IP address of the client. Other anonymizing proxy servers, known as elite or high-anonymity proxies, only include the REMOTE\_ADDR header with the IP address of the proxy server, making it appear that the proxy server is the client. A website could still suspect a proxy is being used if the client sends packets which include a cookie from a previous visit that did not use the high-anonymity proxy server. Clearing cookies, and possibly the cache, would solve this problem.

## Implementations of proxies

### Transparent proxy

Also known as an **intercepting proxy**, **inline proxy**, or **forced proxy**, a transparent proxy intercepts normal communication at the [network layer](http://en.wikipedia.org/wiki/OSI_model#Layer_3:_network_layer) without requiring any special client configuration. Clients need not be aware of the existence of the proxy. A transparent proxy is normally located between the client and the Internet, with the proxy performing some of the functions of a [gateway](http://en.wikipedia.org/wiki/Gateway_(computer_networking)) or [router](http://en.wikipedia.org/wiki/Router_(computing)).[[7]](http://en.wikipedia.org/wiki/Proxy_server#cite_note-7)

[RFC 2616](http://tools.ietf.org/html/rfc2616) (Hypertext Transfer Protocol—HTTP/1.1) offers standard definitions:

"A 'transparent proxy' is a proxy that does not modify the request or response beyond what is required for proxy authentication and identification".

"A 'non-transparent proxy' is a proxy that modifies the request or response in order to provide some added service to the user agent, such as group annotation services, media type transformation, protocol reduction, or anonymity filtering".

In 2009 a security flaw in the way that transparent proxies operate was published by Robert Auger,[[8]](http://en.wikipedia.org/wiki/Proxy_server" \l "cite_note-8) and the Computer Emergency Response Team issued an advisory listing dozens of affected transparent and intercepting proxy servers. [[9]](http://en.wikipedia.org/wiki/Proxy_server#cite_note-9)

#### Purpose

Intercepting proxies are commonly used in businesses to enforce acceptable use policy, and to ease administrative overheads, since no client browser configuration is required. This second reason however is mitigated by features such as Active Directory group policy, or DHCP and automatic proxy detection.

Intercepting proxies are also commonly used by ISPs in some countries to save upstream bandwidth and improve customer response times by caching. This is more common in countries where bandwidth is more limited (e.g. island nations) or must be paid for.

#### Issues

The diversion / interception of a TCP connection creates several issues. Firstly the original destination IP and port must somehow be communicated to the proxy. This is not always possible (e.g. where the gateway and proxy reside on different hosts). There is a class of [cross site attacks](http://en.wikipedia.org/wiki/Cross-site_scripting) that depend on certain behaviour of intercepting proxies that do not check or have access to information about the original (intercepted) destination. This problem may be resolved by using an integrated packet-level and application level appliance or software which is then able to communicate this information between the packet handler and the proxy.

Intercepting also creates problems for [HTTP](http://en.wikipedia.org/wiki/HTTP) authentication, especially connection-oriented authentication such as [NTLM](http://en.wikipedia.org/wiki/NTLM), since the client browser believes it is talking to a server rather than a proxy. This can cause problems where an intercepting proxy requires authentication, then the user connects to a site which also requires authentication.

Finally intercepting connections can cause problems for HTTP caches, since some requests and responses become uncacheable by a shared cache.

#### Implementation methods

In integrated firewall / proxy servers where the router/firewall is on the same host as the proxy, communicating original destination information can be done by any method, for example [Microsoft TMG](http://en.wikipedia.org/wiki/Microsoft_Forefront_Threat_Management_Gateway) or [WinGate](http://en.wikipedia.org/wiki/WinGate" \o "WinGate).

Interception can also be performed using Cisco's [WCCP](http://en.wikipedia.org/wiki/Web_Cache_Communication_Protocol) (Web Cache Control Protocol). This proprietary protocol resides on the router and is configured from the cache, allowing the cache to determine what ports and traffic is sent to it via transparent redirection from the router. This redirection can occur in one of two ways: GRE Tunneling (OSI Layer 3) or MAC rewrites (OSI Layer 2).

Once traffic reaches the proxy machine itself interception is commonly performed with NAT (Network Address Translation). Such setups are invisible to the client browser, but leave the proxy visible to the web server and other devices on the internet side of the proxy. Recent Linux and some BSD releases provide TPROXY (transparent proxy) which performs IP-level (OSI Layer 3) transparent interception and spoofing of outbound traffic, hiding the proxy IP address from other network devices.

#### Detection

There are several methods that can often be used to detect the presence of an intercepting proxy server:

* By comparing the client's external IP address to the address seen by an external web server, or sometimes by examining the HTTP headers received by a server. A number of sites have been created to address this issue, by reporting the user's IP address as seen by the site back to the user in a web page.[<http://www.dslreports.com/ip>
* By comparing the result of online IP checkers when accessed using https vs http, as most intercepting proxies do not intercept SSL. If there is suspicion of SSL being intercepted, one can examine the certificate associated with any secure web site, the root certificate should indicate whether it was issued for the purpose of intercepting.
* By comparing the sequence of network hops reported by a tool such as [traceroute](http://en.wikipedia.org/wiki/Traceroute" \o "Traceroute) for a proxied protocol such as http (port 80) with that for a non proxied protocol such as SMTP (port 25). [[1]](http://tracetcp.sourceforge.net/usage_proxy.html),[[2]](http://svn.haxx.se/dev/archive-2003-02/0257.shtml)
* By attempting to make a connection to an IP address at which there is known to be no server. The proxy will accept the connection and then attempt to proxy it on. When the proxy finds no server to accept the connection it may return an error message or simply close the connection to the client. This difference in behaviour is simple to detect. For example most web browsers will generate a browser created error page in the case where they cannot connect to an HTTP server but will return a different error in the case where the connection is accepted and then closed.[[10]](http://en.wikipedia.org/wiki/Proxy_server#cite_note-10)
* By serving the end-user specially programmed Adobe Flash SWF applications or Sun Java applets that send HTTP calls back to their server.

### CGI proxy

A CGI web proxy accepts target URLs using a [Web form](http://en.wikipedia.org/wiki/Web_form) in the user's browser window, processes the request, and returns the results to the user's browser. Consequently it can be used on a device or network that does not allow "true" proxy settings to be changed.

As with other proxies, CGI proxies **might or might not** hide the user's [IP address](http://en.wikipedia.org/wiki/IP_address) depending on how the proxy has been set up. Also, if they are being used to circumvent local censorship then an administrator might notice the excessive requests to the single CGI proxy URL.

Some CGI proxies were set up for purposes such as [making websites more useable by disabled people](http://en.wikipedia.org/wiki/Web_accessibility), but have since been shut down due to [excessive traffic](http://en.wikipedia.org/wiki/Web_traffic#traffic_overload), usually caused by a [third party advertising the service](http://en.wikipedia.org/wiki/Slashdot_effect) as a means to bypass local filtering. Since many of these users [don't care](http://en.wikipedia.org/wiki/Carelessness) about the collateral damage they are causing, it became necessary for organizations to hide their proxies, disclosing the URLs only to those who take the trouble to contact the organization and demonstrate a genuine need.[[11]](http://en.wikipedia.org/wiki/Proxy_server#cite_note-11)

### Anonymous HTTPS proxy

Users wanting to bypass web filtering, that want to prevent anyone from monitoring what they are doing, will typically search the internet for an open and anonymous HTTPS transparent proxy. They will then program their browser to proxy all requests through the web filter to this anonymous proxy. Those requests will be encrypted with https. The web filter cannot distinguish these transactions from, say, a legitimate access to a financial website. Thus, content filters are only effective against unsophisticated users.

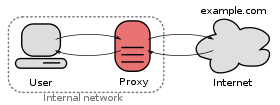
Use of HTTPS proxies are detectable even without examining the encrypted data, based simply on firewall monitoring of addresses for frequency of use and bandwidth usage. If a massive amount of data is being directed through an address that is within an ISP address range such as Comcast, it is likely a home-operated proxy server. Either the single address or the entire ISP address range is then blocked at the firewall to prevent further connections.

### Suffix proxy

A suffix proxy allows a user to access web content by appending the name of the proxy server to the URL of the requested content (e.g. "en.wikipedia.org.*SuffixProxy.com*"). Suffix proxy servers are easier to use than regular proxy servers but they do not offer high levels of anonymity and their primary use is for bypassing web filters. However, this is rarely used due to more advanced web filters.

### Tor onion proxy software

*Main article:*[*Tor (anonymity network)*](http://en.wikipedia.org/wiki/Tor_(anonymity_network))

[](http://en.wikipedia.org/wiki/File:Vidalia-0.0.11-svn.png)

[http://bits.wikimedia.org/static-1.22wmf12/skins/common/images/magnify-clip.png](http://en.wikipedia.org/wiki/File:Vidalia-0.0.11-svn.png)

The [Vidalia](http://en.wikipedia.org/wiki/Vidalia_project) Tor-network map.

**Tor** (short for **The Onion Router**) is a system intended to enable [online anonymity](http://en.wikipedia.org/wiki/Internet_anonymity).[[12]](http://en.wikipedia.org/wiki/Proxy_server#cite_note-Glater-12) Tor client software routes Internet traffic through a worldwide volunteer network of servers in order to conceal a user's location or usage from someone conducting [network surveillance](http://en.wikipedia.org/wiki/Computer_surveillance#Network_surveillance) or [traffic analysis](http://en.wikipedia.org/wiki/Traffic_analysis#In_computer_security). Using Tor makes it more difficult to trace Internet activity, including "visits to Web sites, online posts, instant messages and other communication forms", back to the user.[[12]](http://en.wikipedia.org/wiki/Proxy_server#cite_note-Glater-12) It is intended to protect users' personal freedom, privacy, and ability to conduct confidential business by keeping their internet activities from being monitored.

"[Onion routing](http://en.wikipedia.org/wiki/Onion_routing)" refers to the layered nature of the encryption service: The original data are encrypted and re-encrypted multiple times, then sent through successive Tor relays, each one of which decrypts a "layer" of encryption before passing the data on to the next relay and ultimately the destination. This reduces the possibility of the original data being unscrambled or understood in transit.[[13]](http://en.wikipedia.org/wiki/Proxy_server#cite_note-torproject-13)

The Tor client is [free software](http://en.wikipedia.org/wiki/Free_software), and there are no additional charges to use the network.

### I2P anonymous proxy

*Main article:*[*I2P*](http://en.wikipedia.org/wiki/I2P)

The [I2P anonymous network](http://en.wikipedia.org/wiki/I2P) ('I2P') is a proxy network aiming at [online anonymity](http://en.wikipedia.org/wiki/Internet_anonymity). It implements [garlic routing](http://en.wikipedia.org/wiki/Garlic_routing), which is an enhancement of [Tor](http://en.wikipedia.org/wiki/Tor_(anonymity_network))'s [onion routing](http://en.wikipedia.org/wiki/Onion_routing). I2P is fully distributed and works by encrypting all communications in various layers and relaying them through a network of routers run by volunteers in various locations. By keeping the source of the information hidden, I2P offers censorship resistance. The goals of I2P are to protect users' personal freedom, privacy, and ability to conduct confidential business.

Each user of I2P runs an I2P router on their computer (node). The I2P router takes care of finding other peers and building anonymizing tunnels through them. I2P provides proxies for all protocols (HTTP, [irc](http://en.wikipedia.org/wiki/Irc" \o "Irc), [SOCKS](http://en.wikipedia.org/wiki/SOCKS), ...).

The software is [free and open-source](http://en.wikipedia.org/wiki/Free_software), and the network is free of charge to use.

### Proxy vs. NAT

Most of the time 'proxy' refers to a layer-7 application on the OSI reference model. However, another way of proxying is through layer-3 and is known as Network Address Translation (NAT). The difference between these two technologies is the tier in which they operate, and the way of configuring the clients to use them as a proxy.

In client configuration of NAT, configuring the gateway is sufficient. However, for client configuration of a layer-7 proxy, the destination of the packets that the client generates must always be the proxy server (layer-7), then the proxy server reads each packet and finds out the true destination.

Because NAT operates at layer-3, it is less resource-intensive than the layer-7 proxy, but also less flexible. As we compare these two technologies, we might encounter a terminology known as 'transparent firewall'. **Transparent firewall** means that the layer-3 proxy uses the layer-7 proxy advantages without the knowledge of the client. The client presumes that the gateway is a NAT in layer-3, and it does not have any idea about the inside of the packet, but through this method the layer-3 packets are sent to the layer-7 proxy for investigation.

15. Can you create Admin Server and managed servers in a single machine ?   
  
16. Project architecture ? which architecture you are using ? (DMZ)   
  
17. Which JVM you used ?   
  
18. What is HS\_ERR\_PID<>.log

|  |
| --- |
| **Details** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | **Type:** | Enhancement | **Submit Date:** | 2006-07-10 | | **Status:** | Closed | **Updated Date:** | 2012-10-13 | | **Project Name:** | JDK | **Resolved Date:** | 2007-04-24 | | **Component:** | hotspot | **OS:** | windows\_2003,solaris\_10,windows\_xp | | **Sub-Component:** | runtime | **CPU:** | x86,sparc | | **Priority:** | P5 |  |  | | **Resolution:** | Fixed |  |  | | **Affected Versions:** | 5.0,6u3 |  |  | | **Fixed Versions:** | hs10 [(b12)[http://bugs.sun.com/bugdatabase/assets/115899.gif](http://www.oracle.com/technetwork/java/javase/downloads/index.html)](http://www.oracle.com/technetwork/java/javase/downloads/index.html" \t "_blank) |  |  | |

A DESCRIPTION OF THE PROBLEM :

When the Java VM crashes a hs\_err\_pid\*.log ist written to disk. It does not contain the time when the crash occurred. This information is essential since the file creation time generally is lost during transport.

THE PROBLEM WAS REPRODUCIBLE WITH -Xint FLAG: Yes

THE PROBLEM WAS REPRODUCIBLE WITH -server FLAG: Yes

STEPS TO FOLLOW TO REPRODUCE THE PROBLEM :

Let the Java VM crash and examine the hs\_err\_pid created.

EXPECTED VERSUS ACTUAL BEHAVIOR :

The time of the crash should be reported in the hs\_err\_pid file.

REPRODUCIBILITY :

This bug can be reproduced always.

19. What is server log ?   
  
20. How to provide JDBC log ?

This release of WebLogic Server includes the WebLogic Diagnostic Service, which is a monitoring and diagnostic service that runs within the WebLogic Server process and participates in the standard server life cycle. This service enables you to create, collect, analyze, archive, and access diagnostic data generated by a running server and the applications deployed within its containers. This data provides insight into the runtime performance of servers and applications and enables you to isolate and diagnose faults when they occur. WebLogic JDBC takes advantage of this service to provide enhanced runtime statistics, profile information over a period of time, logging, and debugging to help you keep your WebLogic domain running smoothly.

You can use the runtime statistics to monitor the data sources in your WebLogic domain to see if there is a problem. If there is a problem, you can use profiling to determine which application is the source of the problem. Once you've narrowed it down to the application, you can then use JDBC debugging features to find the problem within the application.

The following sections include details about monitoring JDBC objects:

21. How view log files in linux ?

Almost all logfiles are located under /var/log directory (and subdirectory). You can change to this directory using cd command but you need to be the root user. You can use less, more, cat or tail command to see the logs.

Go to /var/logs directory:# cd /var/logsView common log file /var/log/messages using any one of the following command:# tail -f /var/log/messages  
# less /var/log/messages  
# more -f /var/log/messages  
# vi /var/log/messages

22. Recovering admin password ?   
  
23. How to open a file in UNIX ?

**RDONLY**

Open the file for reading only.

**WRONLY**

Open the file for writing only.

**RDWR**

Open the file for both reading and writing

24. What certificate chaining ? Private keys, digital certificates, and trusted certificate authorities establish and verify server identity and trust.

SSL uses public key encryption technology for authentication. With public key encryption, a public key and a private key are generated for a server. Data encrypted with the public key can only be decrypted using the corresponding private key and data encrypted with the private key can only be decrypted using the corresponding public key. The private key is carefully protected so that only the owner can decrypt messages that were encrypted using the public key.

The public key is embedded in a digital certificate with additional information describing the owner of the public key, such as name, street address, and e-mail address. A private key and digital certificate provide identity for the server.

The data embedded in a digital certificate is verified by a certificate authority and digitally signed with the certificate authority’s digital certificate. Well-know certificate authorities include Verisign and Entrust.net. The trusted certificate authority (CA) certificate establishes trust for a certificate.

An application participating in an SSL connection is authenticated when the other party evaluates and accepts the application’s digital certificate. Web browsers, servers, and other SSL-enabled applications generally accept as genuine any digital certificate that is signed by a trusted certificate authority and is otherwise valid. For example, a digital certificate can be invalidated because it has expired or the digital certificate of the certificate authority used to sign it expired. A server certificate can be invalidated if the host name in the digital certificate of the server does not match the URL specified by the client.

25. **Session stickness** ?

I don't understand how sticky sessions work with OHS with mod\_wl\_ohs plugin  
I have the following environment :  
- 1 WLS Cluster with 2 nodes, configured in active-active mode  
- 1 Java application deployed in that cluster that produce a classic JSESSIONID session cookie to identify the session  
- 2 OHS in front of this, each one targeting the cluster like this :  
<Location /myApp>  
SetHandler weblogic-handler  
WebLogicCluster node1:8001,node2:8001  
</Location>  
  
For some technical reason I need to have sticky session based on that JSESSIONID but I can't figure out how to setup OHS to handle the request in a sticky session mode on JSESSIONID  
I've read that sticky session is active by default but what happens if my session cookie is not called JSESSIONID ? And what happens if I don't want to use sticky session for one location ?   
  
26. **What is the use of multi cast ID ?**

## Multicast IPv6 addresses

A multicast address identifies multiple interfaces. With the appropriate multicast routing topology, packets addressed to a multicast address are delivered to all interfaces that are identified by the address.

IPv6 multicast addresses have the Format Prefix (FP) of 1111 1111. An IPv6 address is simple to classify as multicast because it always begins with FF. Multicast addresses cannot be used as source addresses.

Beyond the FP, multicast addresses include additional structure to identify their flags, scope, and multicast group, as shown in the following illustration.

27. What will be there in Access Log ?   
  
28. What is the use of boot.properties file ?

Ahh, the boot .properties files. The saviour of having to type in the username and password each and every time that you start a server. A very useful little file to have, particularly if you have multiple managed servers.

By default, this appears in the Admin Servers security directory ($DOMAIN\_HOME/servers/AdminServer/security) when a domain is created in development mode and is called boot.properties. The file is only created for the admin server, not for any additional servers; simply copying the security directory over is enough. The password is encrypted for the domain, so it can only be used for servers within that domain.

In production mode, the boot.properties file doesn’t exist. It’s really easy to create, however. Create a file called boot.properties under the security directory in your favourite OS specific editor and add the following lines

username=<username>  
password=<password>

An alternative method to create the boot.properties files is run this nifty command

java -Dweblogic.management.username=username -Dweblogic.management.password=password -Dweblogic.system.StoreBootIdentity=true -Dweblogic.Name=myAdminServer weblogic.Server

Once you are done, simply start the server. It gets encrypted automatically.

If you like, you can create the password pre-encrypted, using the weblogic.security.encrypt command.

java [ -Dweblogic.RootDirectory=dirname ] [ -Dweblogic.management.allowPasswordEcho=true ] weblogic.security.Encrypt [ password ]

If you don’t, it gets encrypted after it is sucessfully validated for the first time.

There are a couple of of options, that can be applied to alter the usage of the boot.properties file.

1) The boot.properties file can have a different name to set this, you need to supply the following option in the start script.

-Dweblogic.system.BootIdentityFile=filename

This is actually pretty useful, because you can then use the same identity file for all the managed servers, from one location.

2) The boot.properties file can be deleted after the server starts by specifying

-Dweblogic.system.RemoveBootIdentity=true

again, useful, if the default scripts are altered to allow the creation of the boot.properties files on startup, using the command line I mentioned above.

Finally, the alternative method to start the server without the boot.properties file is

java -Dweblogic.management.username=username-Dweblogic.management.password=password -Dweblogic.system.StoreBootIdentity=true -Dweblogic.Name=myAdminServer weblogic.Server

29. JMS ?

## Overview of the Java Message Service and WebLogic JMS

WebLogic JMS is an enterprise-class messaging system that is tightly integrated into the WebLogic Server platform. It fully supports the [JMS Specification](http://java.sun.com/products/jms/docs.html) and also provides numerous [WebLogic JMS Extensions](http://docs.oracle.com/cd/E13222_01/wls/docs103/javadocs/weblogic/jms/extensions/package-summary.html) that go above and beyond the standard JMS APIs.

### What Is the Java Message Service?

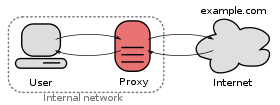
An enterprise messaging system enables applications to communicate with one another through the exchange of messages. A message is a request, report, and/or event that contains information needed to coordinate communication between different applications. A message provides a level of abstraction, allowing you to separate the details about the destination system from the application code.

The Java Message Service (JMS) is a standard API for accessing enterprise messaging systems. Specifically, JMS:

* + Enables Java applications sharing a messaging system to exchange messages
  + Simplifies application development by providing a standard interface for creating, sending, and receiving messages

The following figure illustrates WebLogic JMS messaging.

**Figure 2-1 WebLogic JMS Messaging**



As illustrated in the figure, WebLogic JMS accepts messages from producer applications and delivers them to consumer applications.

### Implementation of Java Specifications

WebLogic Server is compliant with the following Java specifications.

#### Java EE Specification

WebLogic Server is compliant with the [Java Platform, Enterprise Edition (Java EE) Version 5.0](http://java.sun.com/javaee/5/docs/api/) specification.

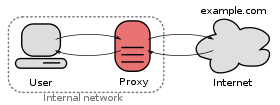
#### JMS Specification

WebLogic Server is fully compliant with the [JMS 1.1 Specification](http://java.sun.com/products/jms/docs.html) and can be used in production.

### WebLogic JMS Architecture

The following figure illustrates the WebLogic JMS architecture.

**Figure 2-2 WebLogic JMS Architecture**



30. Connection pooling and how to create connection pool ?

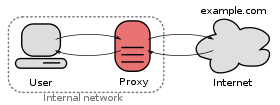
In the JDBC Connection Pool—>Configuration—>Connections tab, you specify the number of connections in the connection pool and details for each connection in the connection pool.

A connection pool contains a group of JDBC connections that are created when the connection pool is registered, usually when starting up WebLogic Server. Your application borrows a connection from the connection pool, uses it, then returns it to the connection pool by closing it.

# Configuring JDBC Connection Pools

A connection pool contains a group of JDBC connections that are created when the connection pool is registered—when starting up WebLogic Server or when deploying the connection pool to a target server or cluster. Connection pools use a JDBC driver to create physical database connections. Your application borrows a connection from the pool, uses it, then returns it to the pool by closing it.

**Figure 127-1 Connection Pool Architecture**



All of the settings you make with the Administration Console are static; that is, all settings persist even after you stop and restart WebLogic Server. You can create dynamic connection pools—those that you expect to use and delete while the server is running—using the command line (see [Commands for Managing JDBC Connection Pools](http://docs.oracle.com/cd/E13222_01/wls/docs81/admin_ref/cli.html#jdbc) in the WebLogic Server Command Reference) or programmatically using the API (see [Creating a Connection Pool Dynamically](http://docs.oracle.com/cd/E13222_01/wls/docs81/jdbc/programming.html#dynamic_conn_pool) in Programming WebLogic JDBC).

Connection pool settings are persisted in the config.xml file, including settings for dynamically created connection pools (until you programmatically delete the connection pool). For information about entries in the config.xml file, see the [JDBCConnectionPool](http://docs.oracle.com/cd/E13222_01/wls/docs81/config_xml/JDBCConnectionPool.html) section of the Configuration Reference Guide.

31. Which performance tool you are using for monitoring the performance WLS ?

a)Wily,pivoli ex…  
  
32. How to verify the network performance in any OS ?   
  
33. Application is working but the DB is not supporting what kind of exception u will get ?

a)500,505 error   
  
34. How to deploy an application through command line ?

**connect('weblogic','weblogic','t3://localhost:8001')**

The following example deploys the businessApp application located at c:/myapps/business, A default deployment plan is created.

The deploy command returns a WLSTProgress object that you can access to check the status of the command. The WLSTProgress object is captured in a user-defined variable, in this case, progress.

wls:/mydomain/serverConfig/Servers> **progress= deploy(appName='businessApp',path='c:/myapps/business',createplan='true')**

The previous example stores the WLSTProgress object returned in a user-defined variable, in this case, progress. You can then use the progress variable to print the status of the deploy command. For example:

wls:/mydomain/serverConfig/Servers> **progress.printStatus()**Current Status of your Deployment:  
Deployment command type: deploy  
Deployment State : completed  
Deployment Message : null  
wls:/mydomain/serverConfig/Servers>

35. How to check CPU utilization in UNIX ?(top)   
  
36. How to check the disk space in UNIX ? (df –k)   
  
37. What is node manager and what is use of it ?   
  
38. What is garbage collection ?   
  
39. What are the variables of the HEAP SIZE ?   
  
40. What is head and tail command ?   
  
41. What is Certificate Signature Request ?   
  
42. What is the default port of the node manager ?   
  
43. How do u find the port number is used by some the other server ?   
  
44. What are the deployment stages ?   
  
45. tesstart command ?   
  
46. what is the role of JNDI ?   
  
47. what is difference static and dynamic deployment ?   
  
48. how do u know which thread is executing and how much time it will take ?   
  
49. How do u give the prevalization to users and groups in UNIX?   
  
50. Url Rewriting in weblogic?   
  
51. What is VMSTAT command in sun Solaris?   
  
52. How do you find port numbers in Linux?   
  
53. What is the use of netstat command?   
  
54. Daily activities?   
  
55. How do u monitoring the CPU Utilization?(top or sar)  
  
Ans: # sar -u 12 5 ` Where,-u 12 5: Comparison of CPU utilization; 12 seconds apart; 5 time   
  
57. How the sar command shows the out put?   
  
58. Questions on SSL(Complete)?   
  
59. Did u attend any calls with u r clients?   
  
60. What are Handling Disaster Recovery and Failover activities?   
  
61. What are the things you did if the database server fails?   
  
62. From where you are getting the trail certificates?   
  
63. How much size you for the key generation?   
  
64. HOW we configure SSL in proxy?   
  
65. How we view the log files?   
  
66. Which tool you are using for building an application?   
  
67. What is your admin level? (L2)   
  
68. Can we create two admin servers in a single domain?   
  
69. What are the disadvantages of connection pooling?   
  
70. Could you explain folder structure in bea?   
  
71. How can we verify file size in Linux?(du –sh)   
  
72. Why connection pooling?   
  
73. What are the difference between authentication and authorization?   
  
74. What are the role, user and principle?   
  
75. Why clustering in weblogic?   
  
76. Did you prepare any documentation as solved the any problem?   
  
77. If you don’t have any work what can you do at that time?   
  
78. How many machines are using in your project?   
  
79. Can you explain your project flow? How it takes requests and give response to the clients?   
  
80. How to generate jdbc log files?   
  
81. If config.xml file is lost at runtime what is the solution to run the application successfully?   
  
82. Explain different deployment stages in weblogic?

1.      How to know the Managed Servers status, when admin console is not available?

2.      What is the performance issue in weblogic and how can you resolve, explain in brief?

3.      What is the Digital Certificate? How do we generate a Digital Certificate?

4.      What is Thread Dump? What is the UNIX command to take Thread Dumps?

5.      What is a cluster? What is High Availability and Fail over?

6.      How to handle out of memory in weblogic and if server is getting more requests then what we have to do in production environment?

7.      What is clustering? How do weblogic instances communicate in a clustered environment? In a cluster, if one of the servers has an issue and it is not accessible, will the other servers know about it and how?

8.      What are the roles you have played and what are the day today activities?

9.      WHAT IS TROUBLE SHOOTING IN WEBLOGIC?

10. How to integrate apache webserver with weblogic server? What is the purpose of integrating both?

11. Define the different groups of Users?

12. What are the different thread queues?

13. How will you analyze if a page responds slowly?

14. What is Work manager? Explain briefly?

15. What are the different types of drivers?

16. What are the various types of log files?

17. What are you commonly used fine tuning commands?

18. What is Session replication? What are the different types of Session Replications?

19. What happens if we change config.xml while server is running?

20. What is HTTP tunneling?

21. What is asynchronous communication? Is there any synchronous communication in JMS?

22. How to find Weblogic Version?

23. What is the use of log4j?

24. What is Work manager?

25. What is virtual host?

26. **What is eden size and perm size?**

***Eden Space*:**

Eden Space is a Part of Java Heap where the JVM initially creates any objects, where most objects die and quickly are cleanedup by the minor Garbage Collectors (Note: Full Garbage Collection is different from Minor Garbage Collection). Usually any new objects created inside a Java Method go into Eden space and the objects space is reclaimed once the method execution completes. Where as the Instance Variables of a Class usually lives longer until the Object based on that class gets destroyed. When Eden fills up it causes a minor collection, in which some surviving objects are moved to an older generation.

27. **What is Weblogic shrink?**

28. **What is diff b/w JNDI and JDBC?**

**29. What are the different types of drivers?**

**30. What driver you are using?**

**31. What is diff b/w unicast and multicast?**

**32. When core dump will not be created even if the server crashed?**

**33. Can we change the heart beat interval?**

**34. What are the various types of log files?**

**35. What is WorkManager?**

36**. What is Multicast IP Address? What are the things done by it? How to  
test multicast IP?**

**37. How to check whether the cluster multicast adress is available or not?  
What is the command to check in UNIX environment?**

**38. What is Virtual Host in Weblogic, how to create it & what is the  
advantage ?**

39. **How can you find the jdbc version on server side?**

**40. What you do to close the connections automatically in JDBC?**

**41. What are the things that we take care under Database fine tuning apart  
from increasing or decreasing connections?**

**42. What is MBean, how many types are there?**

**43. How to restart proxy?**

**44. Reasons for server crash?**

**45. Reasons for servers hang?**

**46. What is the thread hogging?**

**47. Various garbage collection algorithms?**

**48. How to find whether the PORT No is free or not?**

**49. What is the command to find CPU utilization?**

**50. What is the command to find version of Unix?**

**51. How to find CPU utilization? What if top command doesn’t work?**

**52. What are you commonly used fine tuning commands?**

**53. What is the difference between webservers and Proxy server?**

**54. How to sort the files?**

**55. What is Session replication? What are the different types of Session Replications?**

**56. Which IP segment will you use for Multicasting?**

**57. Is it possible to manage multiple domains through a single weblogic  
admin console?**

**58. What happens if we change config.xml while server is running?**