9

Viewing and Managing Logs in Oracle WLS Environment

Objectives

After completing this lesson, you should be able to:

- Define and configure server and domain logs
- View and interpret the format of domain and server log files using the Administration Console
- Configure server standard output settings using the console
- Describe how applications can integrate with WLS logging infrastructure (Apache commons, log4j)
- Access online log message catalogs
- Create and apply a log filter using the console
- Configure log filter expressions

Road Map

- Logs and monitoring
  - Using log files
  - Integrating application logging
  - Logging file format
- Log filters

Oracle WebLogic Server Logs

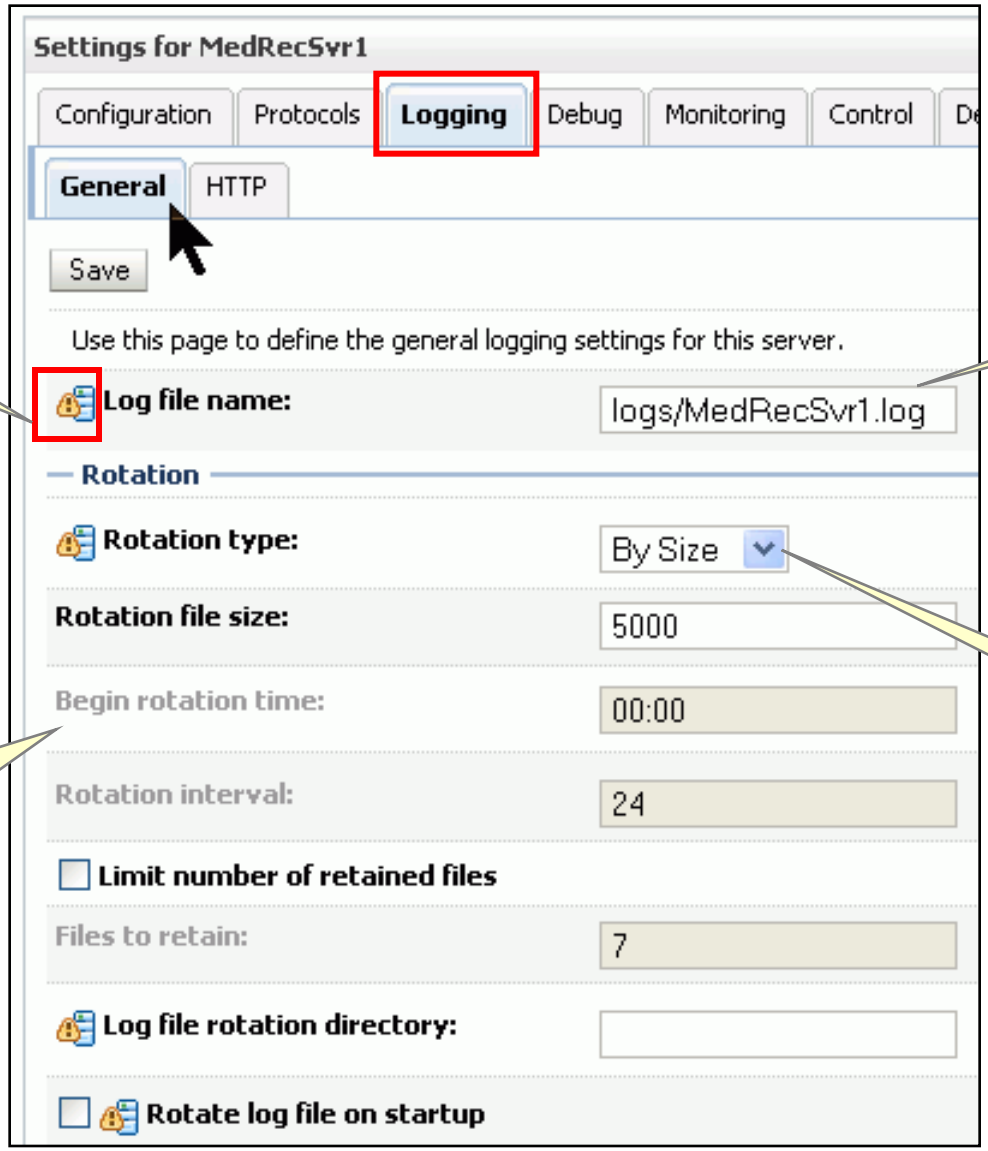
Logs can aid in the discovery of:

- Any problems encountered while servicing requests
- Activity by day and time interval
- The IP addresses of users accessing an application
- Frequently accessed resources
- The amount of data sent and received

Server and Domain Logs

- A server log:
  - Logs all activity for a single server
  - Is stored in *SERVER_NAME*/logs/*SERVER_NAME*.log by default
- A domain log:
  - Logs key events for all servers in a domain
  - Is stored in *ADMIN_SERVER_NAME*/logs/*DOMAIN_NAME*.log by default
- Other logs:
  - HTTP
  - JMS
  - JDBC
- These logs are independently configured.

Configuring Server Logging



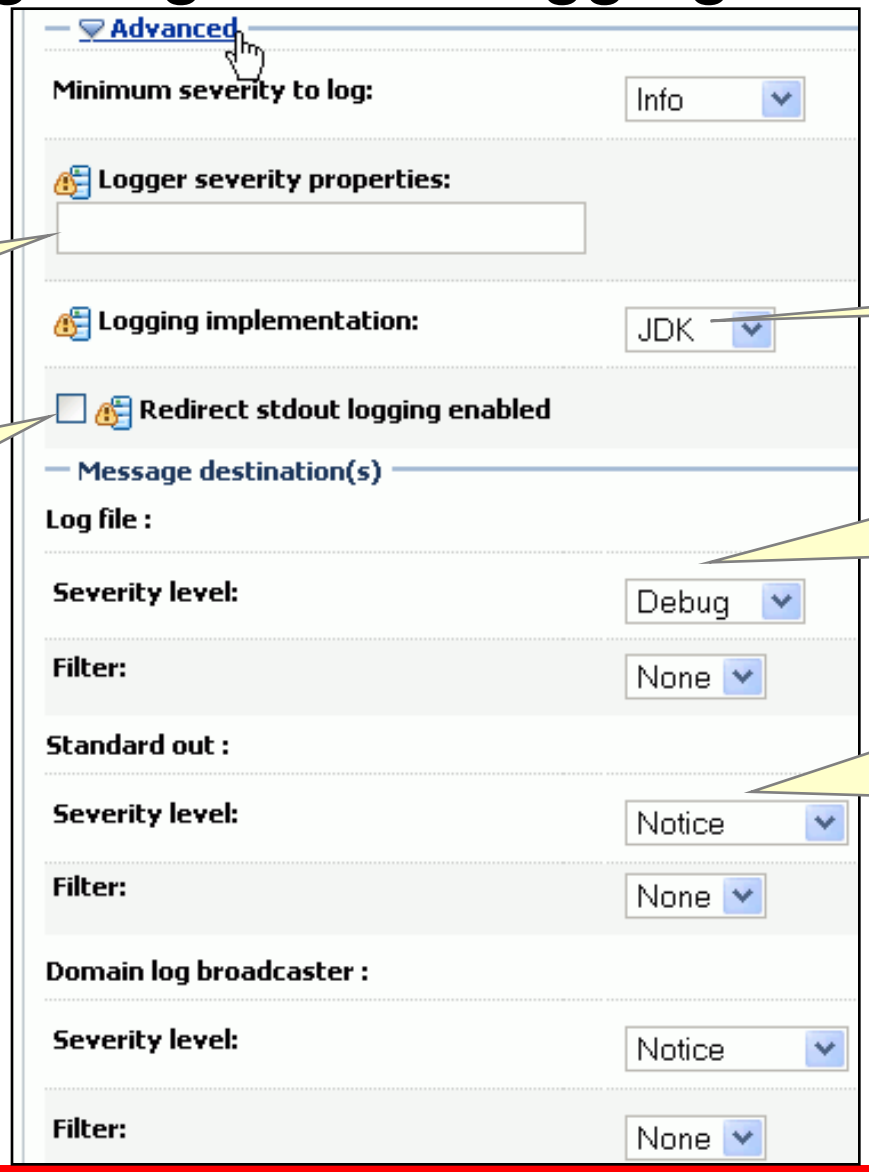
Attribute requires server restart.

Log file

Disabled based on Rotation type

Log rotation

Configuring Server Logging: Advanced



Individual loggers here

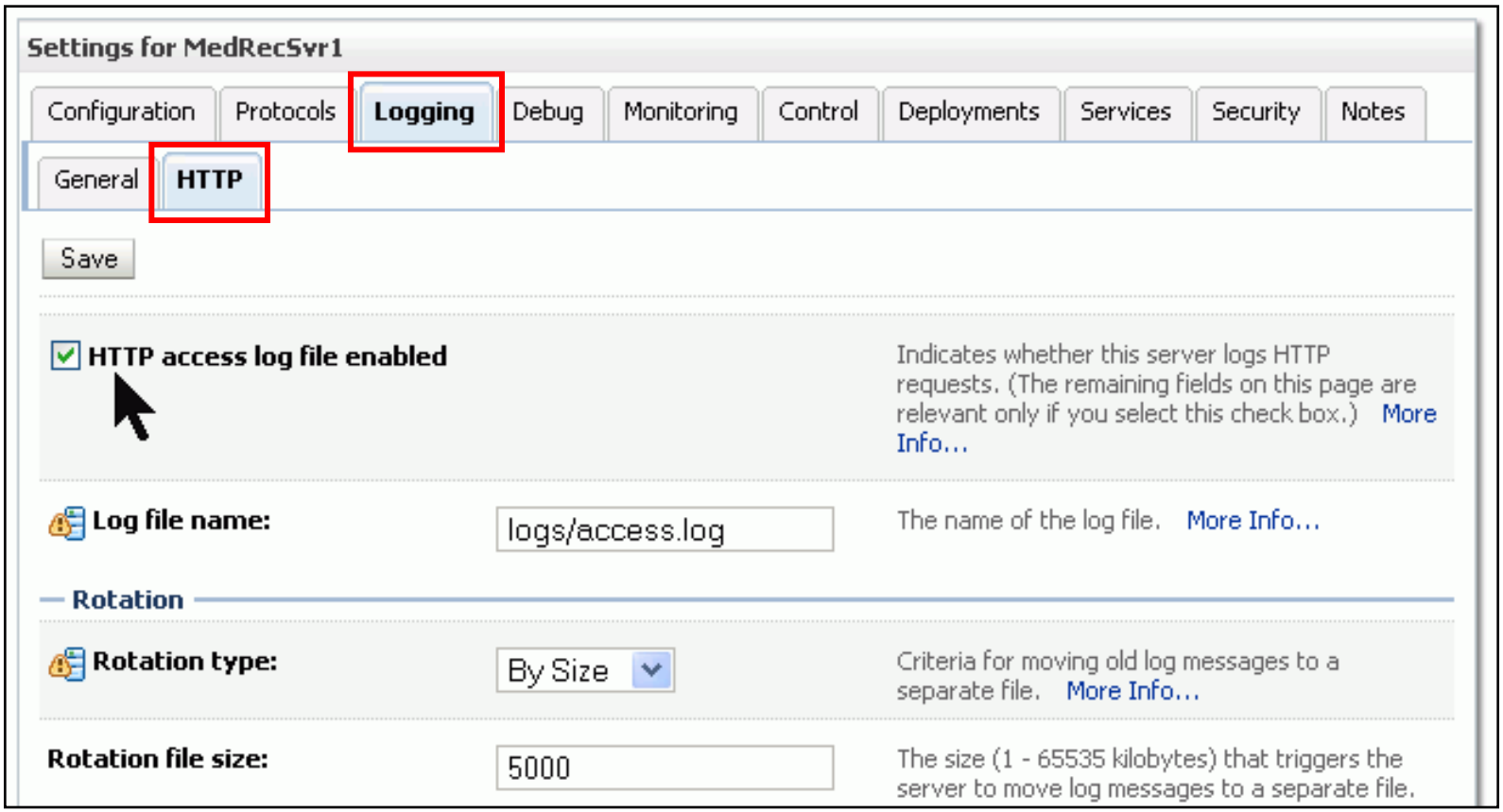
Redirects server standard out to log file

JDK or log4j

Minimum severity of log messages to write to file

Minimum severity of log messages to also print to standard out

HTTP Access Logs

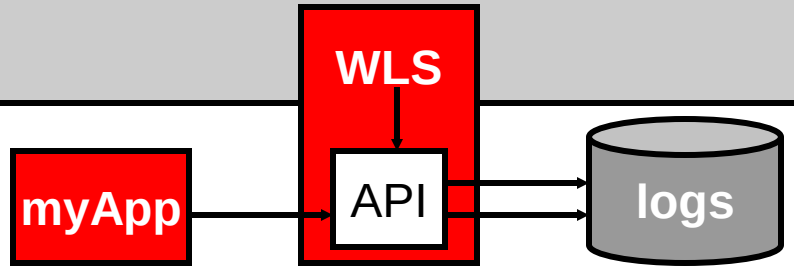


The other options (rotation, number of retained files, and so on) are very similar to the other server logs.

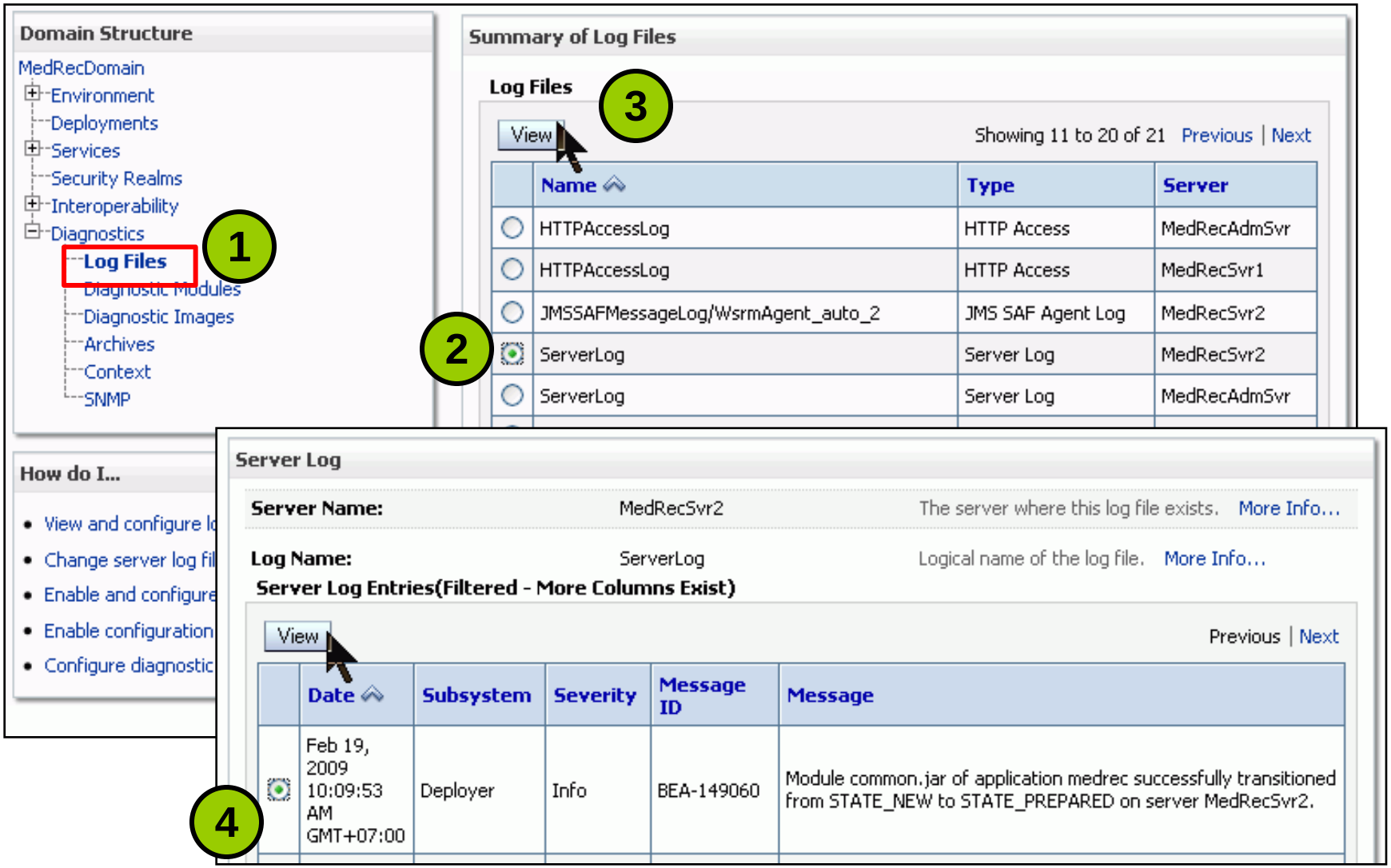
Apache Commons Logging API

```
import org.apache.commons.logging.LogFactory;
import org.apache.commons.logging.Log;

public class MyCommonsTest {
  public void testWLSCommonsLogging() {
    System.setProperty(LogFactory.FACTORY_PROPERTY,
      "weblogic.logging.commons.LogFactoryImpl");
    Log clog =
    LogFactory.getFactory().getInstance("MyCommonsLogger");
    // Log String objects
    clog.debug("Hey this is common debug");
    clog.fatal("Hey this is common fatal", new Exception());
    clog.error("Hey this is common error", new Exception());
    clog.trace("Dont leave your footprints on the sands of
    time");
  }
}
```



Using the Console to View Logs



Using WLST to View Logs

```
wls:/offline> exportDiagnosticData (logicalName='ServerLog',
    logName='myserver.log', exportFileName='myExport.xml')

Input parameters: {logicalName='ServerLog',
    logName='myserver.log', logRotationDir='.',
    storeDir='../data/store/diagnostics', query='',
    exportFileName='myExport.xml', elfFields='',
    beginTimestamp=0L, endTimestamp=92233720368547758O7L}

Exporting diagnostic data to myExport.xml ...
<Apr 3, 2009 11:23:56 AM EDT> <Info> <Store> <BEA-280050>
    <Persistent store "WLS_DIAGNOSTICS" opened:
    directory="/u01/app/oracle/product/fmw/11.1.0/wlserver_10.3
    /server/data/store/diagnostics" writePolicy="Disabled"
    blockSize=512 directIO=false driver="wlfileio2">

Exported diagnostic data successfully.

wls:/offline>
```

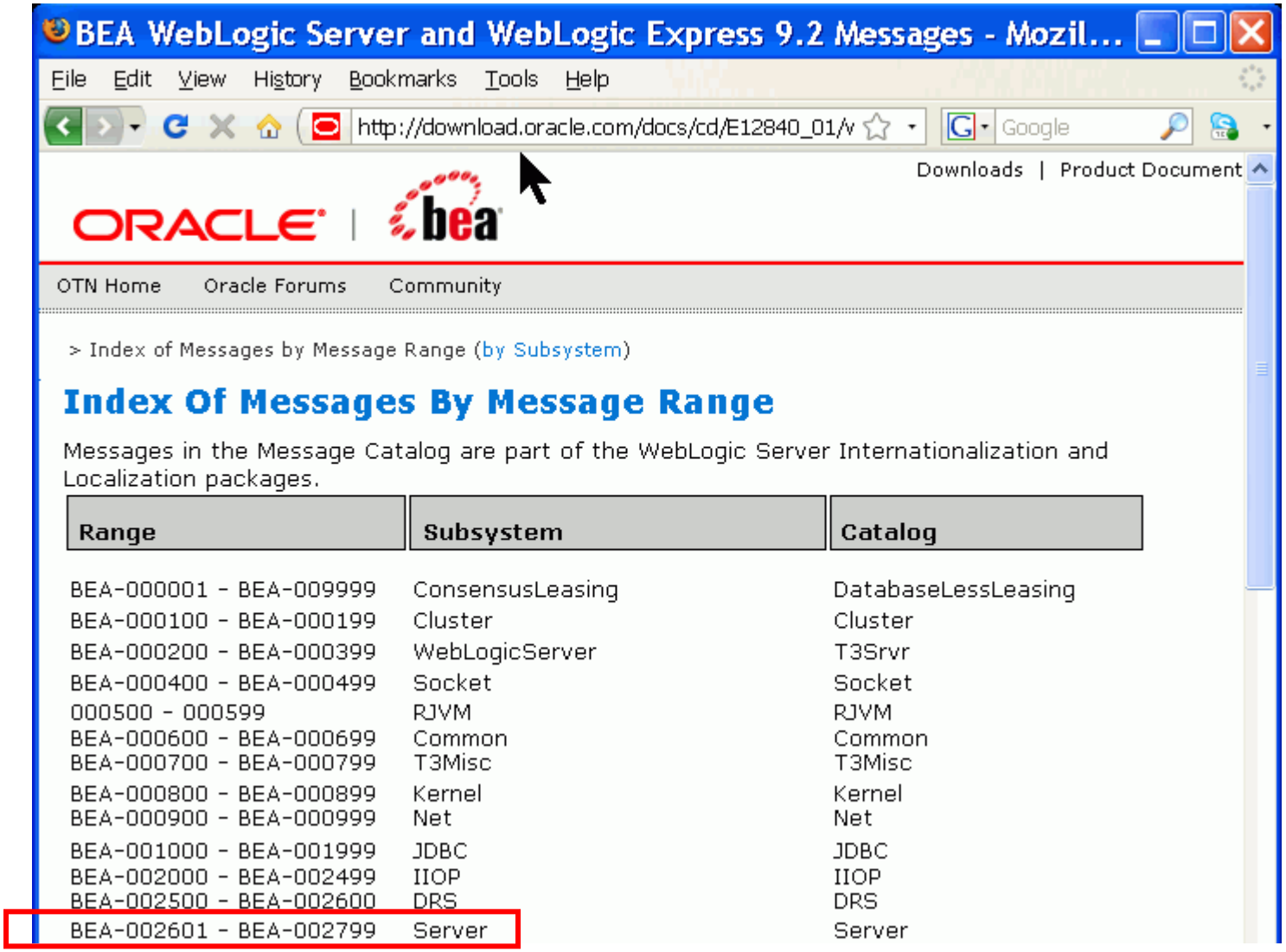
Message Attributes

Attribute	Description	Standard Out?
Timestamp	The time and date when the message originated, in a format that is specific to the locale	✓
Subsystem	The particular WLS subsystem that was the source of the message (Management, Security, EJB, RMI, JMS, and so on)	✓
Severity	The degree of impact or seriousness of the event reported by the message	✓
Catalog ID	The unique ID assigned to this type of event, to reference in the online documentation	✓
Server Name	The WebLogic instance that generated the message	
Thread ID	The server thread that generated the message	
User ID	The current security context, if any	
Transaction ID	The current XA transaction context, if any	

Message Severity

Severity	Description	Domain Log (by default)?
TRACE	Messages from the diagnostics framework	
DEBUG	Detailed internal messages (if debugging is enabled)	
INFO	Normal operations	
NOTICE	**INFO** message of greater importance	✓
WARNING	Suspicious operation or configuration	✓
ERROR	Error handling request, but no interruption in service	✓
CRITICAL	System or service error that may cause temporary loss or degradation of service	✓
ALERT	One or more services in an unusable state, requiring administrative attention	✓
EMERGENCY	Entire server in an unusable state	✓

Message Catalog Using the Web



Message Catalog Cross-Reference

```
<Feb19,2009 10:10:27 AM GMT+07:00> <Notice> <WebLogicServer> <BEA-000365> <Server state changed to ADMIN>
<Feb19,2009 10:10:27 AM GMT+07:00> <Notice> <WebLogicServer> <BEA-000365> <Server state changed to
      RESUMING>
<Feb19,2009 10:10:27 AM GMT+07:00> <Notice> <Cluster> <BEA-000162> <Starting "async" replication service
      with remote cluster address "localhost">
<Feb19,2009 10:10:27 AM GMT+07:00> <Notice> <Server> <BEA-002613> <Channel "Default" is now listening on
      139.185.35.128:7023 for protocols iiop, t3, CLUSTER-BROADCAST, ldap, snmp, http.>
<Feb19,2009 10:10:27 AM GMT+07:00> <Notice> <Server> <BEA-002613> <Channel "Default[1]" is now listening on
      fe80:0:0:0:21a:a0ff:fec0:63fb:7023 for protocols iiop, t3, CLUSTER-BROADCAST, ldap, snmp, http.>
<Feb19,2009 10:10:27 AM GMT+07:00> <Notice> <Server> <BEA-002613> <Channel "Default[2]" is now listening on
      0:0:0:0:0:0:0:1:7023 for protocols iiop, t3, CLUSTER-BROADCAST, ldap, snmp, http.>
<Feb19,2009 10:10:27 AM GMT+07:00> <Notice> <Server> <BEA-002613> <Channel "Default[3]" is now listening on
      127.0.0.1:7023 for protocols iiop, t3, CLUSTER-BROADCAST, ldap, snmp, http.>
<Feb19,2009 10:10:27 AM GMT+07:00> <Notice> <WebLogicServer> <BEA-000330> <Started WebLogic Managed Server
      "MedRecSvr2" for domain "MedRecDomain" running in Production Mode>
<Feb19,2009 10:10:29 AM GMT+07:00> <Notice> <Cluster> <BEA-000102> <Joining cluster MedRecClust1 on
      239.192.0.0:7030>
<Feb19,2009 10:10:29 AM GMT+07:00> <Notice> <WebLogicServer> <BEA-000365> <Server state changed to RUNNING>
<Feb19,2009 10:10:29 AM GMT+07:00> <Notice> <WebLogicServer> <BEA-000360> <Server started in RUNNING mode>
```

BEA-002613 *Notice:* Channel "*channel*" is now listening on *listenAddress*:*port* for protocols *protocols*.

Description The server successfully started the listen thread and server socket.

Cause None.

Action None.

Road Map

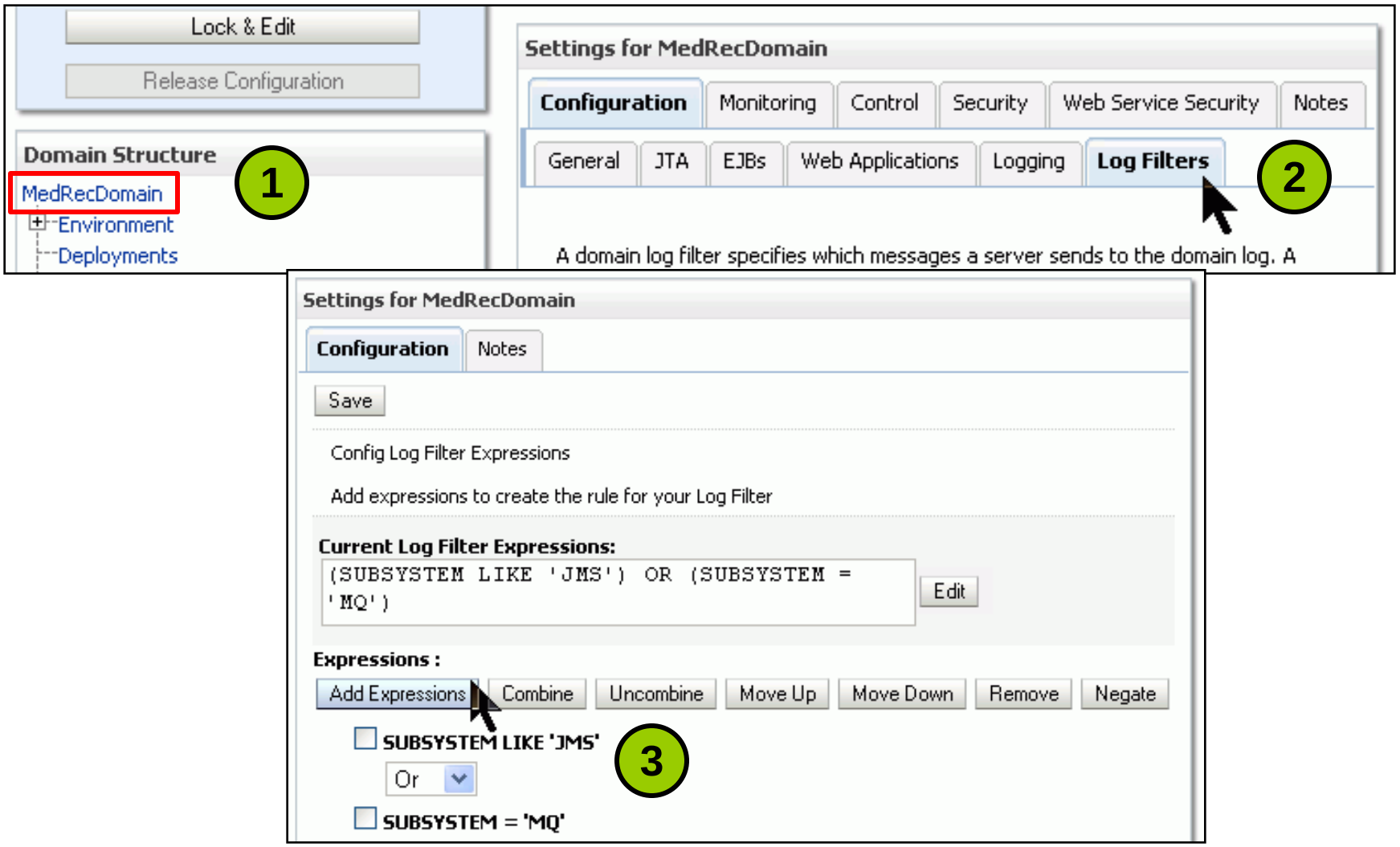
- Logs and monitoring
- Log filters

Log Filters

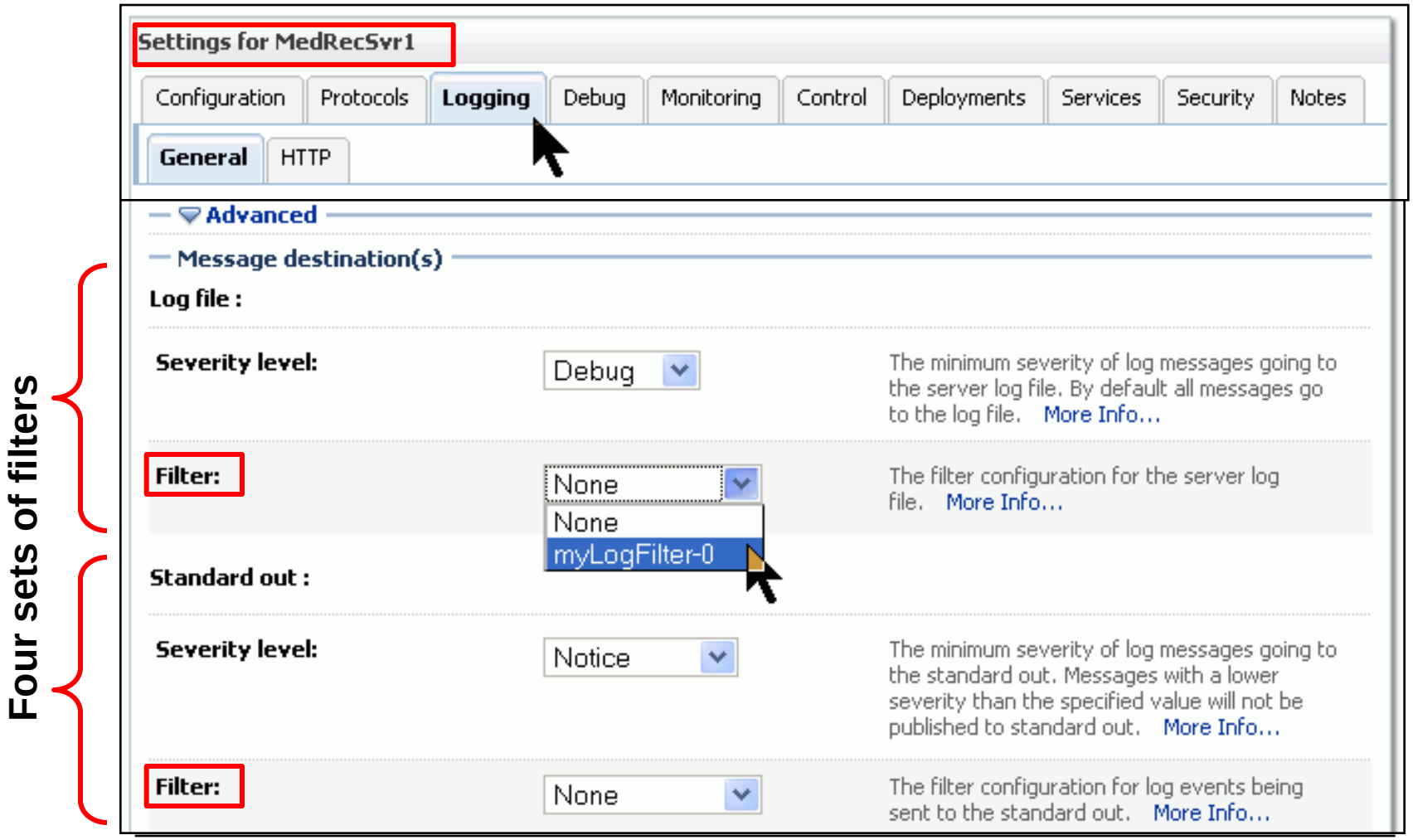
Log filters:

- Control the log messages that get published
- Are based on the values of message attributes
- Can be applied to different message destinations:
  - Server log file
  - Server memory buffer
  - Server standard out
  - Domain log file

Creating a Log Filter

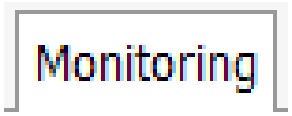


Applying a Log Filter

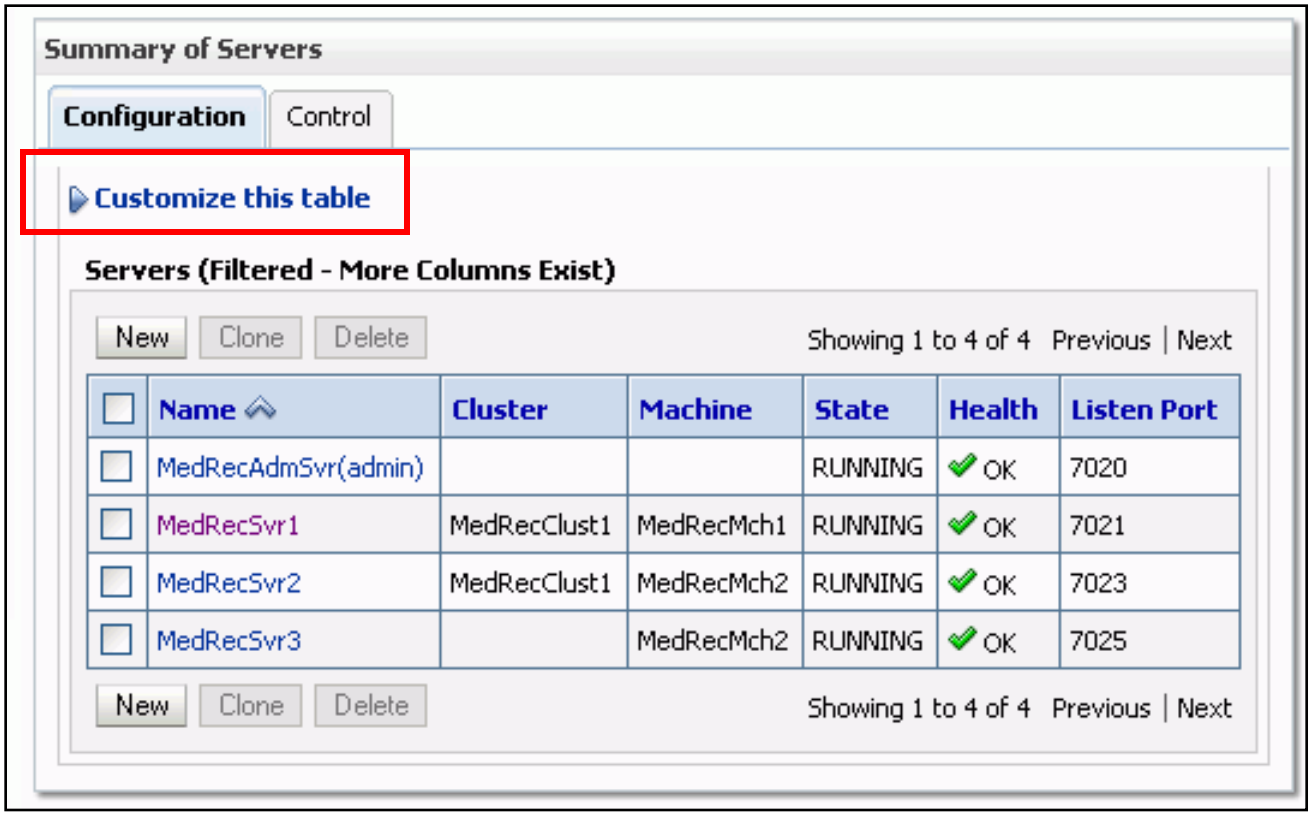


Using the Console to Monitor

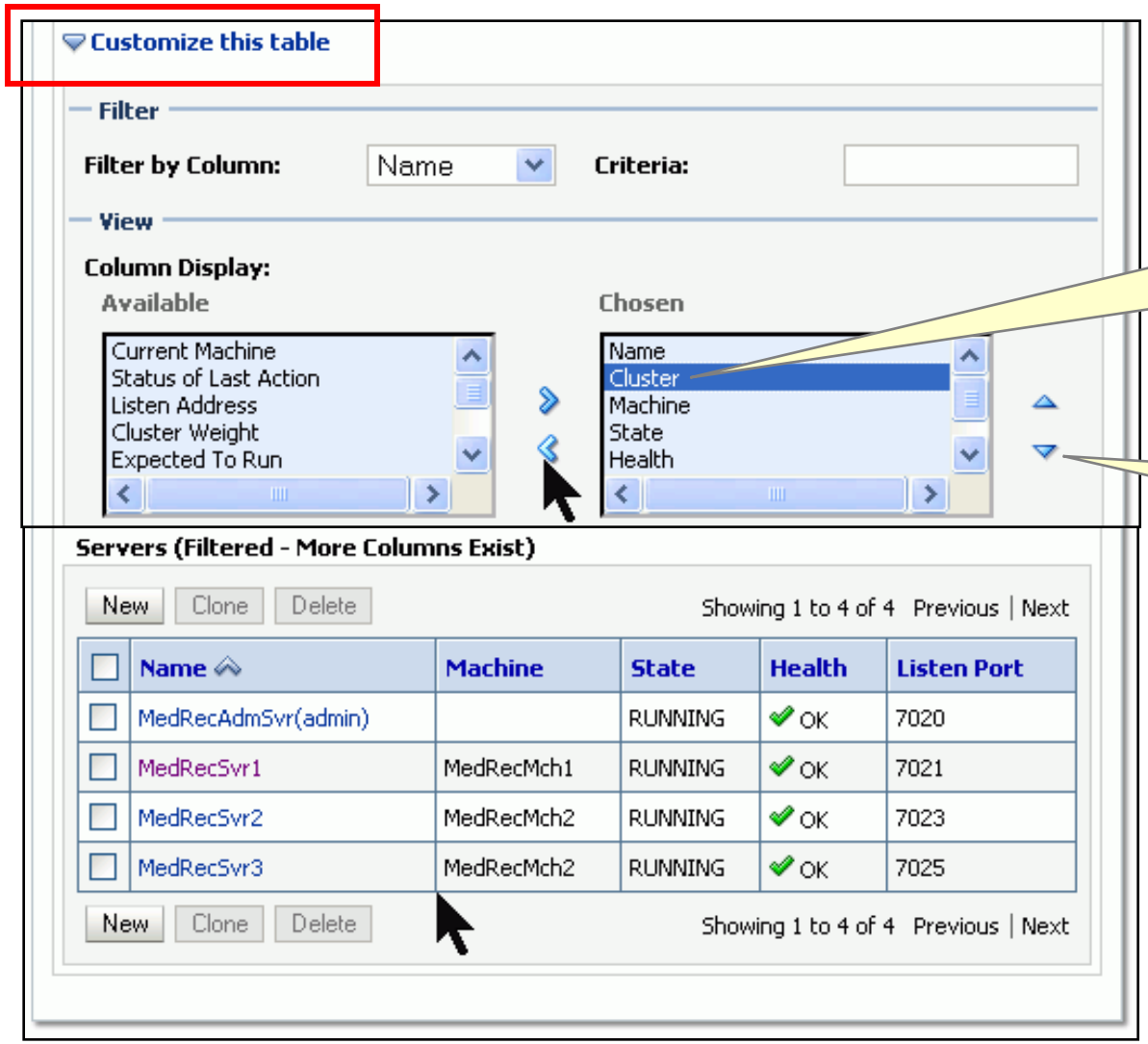
The Administration Console offers some monitoring capabilities:

Attribute	Description
	**Many of the Console's objects have a Monitoring tab that allows you to view monitoring information for that object.**
	**You can customize the monitoring view by clicking the "Customize this table" link.**

Monitoring Running Servers



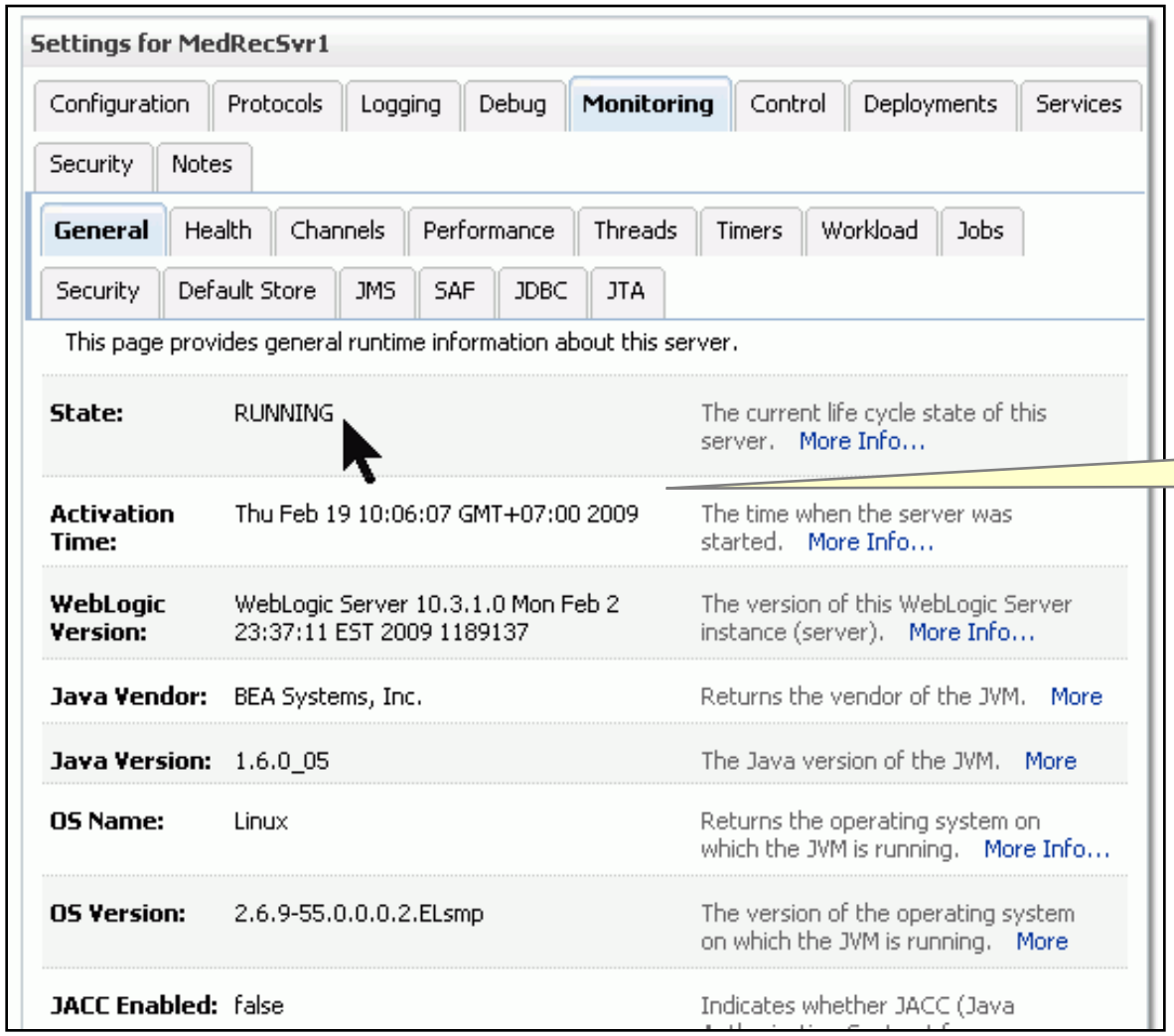
Customizing Views



Notice the Cluster column. It can be suppressed in the view.

Columns can be reordered.

Monitoring Individual Servers



Translates into uptime.

Network-Addressing Features

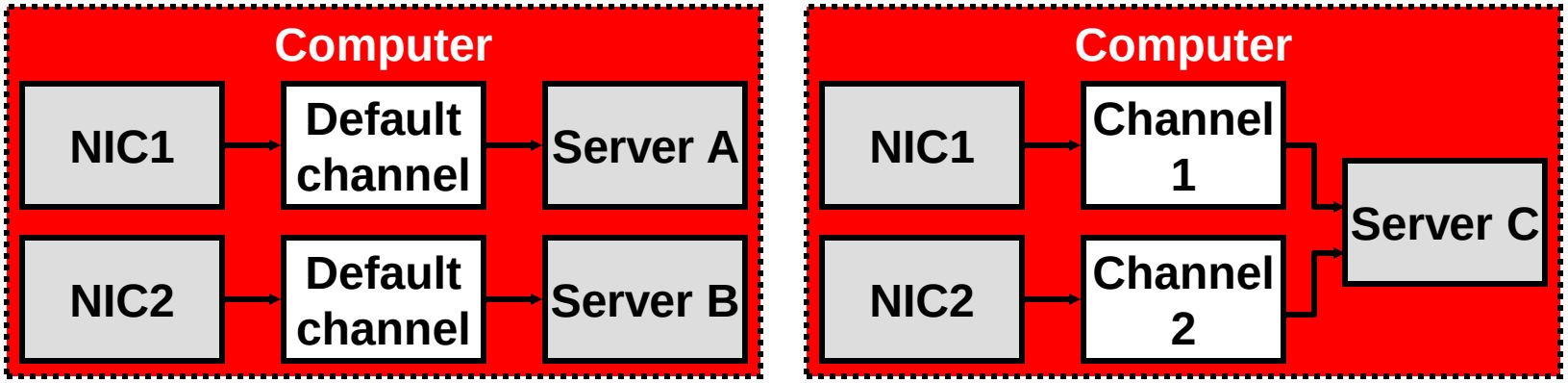
Add flexibility to the networking configuration:

- Multiple NICs for a single WLS server
- Specific NICs or multiple port numbers on an NIC for specific WLS servers
- Ability to use multiple IP addresses with each server
- Ability to use a single IP address with multiple ports
- Ability to configure the cluster multicast port number independently of the port numbers used by the cluster members
- Multiple SSL configurations on one server

Network-Addressing Features

Add flexibility to networking configuration by defining and using channels for:

- Administration-traffic-only port
- Interoperability with previous WebLogic Server versions



Quiz

Which is NOT a standard severity level for Oracle WebLogic Server log messages?

1. Debug
2. Transaction
3. Info
4. Notice
5. Error

Summary

In this lesson, you should have learned how to:

- Configure server and domain logging
- Locate and interpret the format of domain and server log files
- View logs using the Administration Console
- Describe message attributes
- Configure server standard output settings using the console
- Integrate applications with the WLS logging infrastructure
- Access online log message catalogs
- Create and apply log filters and expressions

Practice 9 Overview: Viewing and Managing WLS Logs

This practice covers the following topics:

- Configuring a logging filter
- Viewing logs