



BEA WebLogic Server™

WebLogic SNMP Management Guide

Release 8.1
Revised: March 28, 2003

Copyright

Copyright © 2003 BEA Systems, Inc. All Rights Reserved.

Restricted Rights Legend

This software and documentation is subject to and made available only pursuant to the terms of the BEA Systems License Agreement and may be used or copied only in accordance with the terms of that agreement. It is against the law to copy the software except as specifically allowed in the agreement. This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior consent, in writing, from BEA Systems, Inc.

Use, duplication or disclosure by the U.S. Government is subject to restrictions set forth in the BEA Systems License Agreement and in subparagraph (c)(1) of the Commercial Computer Software-Restricted Rights Clause at FAR 52.227-19; subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, subparagraph (d) of the Commercial Computer Software--Licensing clause at NASA FAR supplement 16-52.227-86; or their equivalent.

Information in this document is subject to change without notice and does not represent a commitment on the part of BEA Systems. THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. FURTHER, BEA Systems DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE, OR THE RESULTS OF THE USE, OF THE SOFTWARE OR WRITTEN MATERIAL IN TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE.

Trademarks or Service Marks

BEA, Jolt, Tuxedo, and WebLogic are registered trademarks of BEA Systems, Inc. BEA Builder, BEA Campaign Manager for WebLogic, BEA eLink, BEA Liquid Data for WebLogic, BEA Manager, BEA WebLogic Commerce Server, BEA WebLogic Enterprise, BEA WebLogic Enterprise Platform, BEA WebLogic Express, BEA WebLogic Integration, BEA WebLogic Personalization Server, BEA WebLogic Platform, BEA WebLogic Portal, BEA WebLogic Server, BEA WebLogic Workshop and How Business Becomes E-Business are trademarks of BEA Systems, Inc.

All other trademarks are the property of their respective companies.

Contents

About This Document

| | |
|---------------------------------|------|
| Audience | vii |
| e-docs Web Site | vii |
| How to Print the Document | viii |
| Contact Us! | viii |
| Documentation Conventions | viii |

1. Introduction to the WebLogic SNMP Agent

| | |
|---|-----|
| The SNMP Agent/Manager Model | 1-2 |
| The Role of the SNMP Agent in a WebLogic Server Domain | 1-2 |
| WebLogic Server Managed Resources and MBeans | 1-4 |
| Documentation for Configuration MBean APIs | 1-5 |
| Documentation for Runtime MBean APIs | 1-5 |
| SNMP MIB for WebLogic Server | 1-6 |
| Browsing the MIB | 1-7 |
| Object Identifiers | 1-7 |
| OIDs for Types and Instances | 1-8 |
| SNMP Community Names | 1-8 |
| Using Community Names to Specify Target Servers in Management Requests | 1-8 |

2. WebLogic Trap Notifications

| | |
|---|-----|
| Format of WebLogic Trap Notifications | 2-1 |
| Automatically Generated WebLogic SNMP Traps | 2-3 |

| | |
|---|-----|
| Log Message Traps | 2-4 |
| Variable Bindings in Log Message Traps | 2-5 |
| Monitor Traps | 2-6 |
| Variable Bindings in Monitor Traps. | 2-8 |
| Attribute Change Traps | 2-9 |
| Variable Bindings in Attribute Change Traps | 2-9 |

3. SNMP Proxies

| | |
|--|-----|
| SNMP Agent as Proxy for Other Agents | 3-1 |
| The Microsoft Windows SNMP Service | 3-2 |

A. Sources of SNMP Information

| | |
|--------------------------------|-----|
| Reference Books | 4-1 |
| Standards and Drafts | 4-2 |
| Obtaining RFCs. | 4-3 |

About This Document

This document explains the management subsystem provided for configuring and monitoring your WebLogic Server implementation. It covers the following topics:

- [Chapter 1, “Introduction to the WebLogic SNMP Agent,”](#) describes basic concepts of Simple Network Management Protocol as they apply to managing WebLogic Servers.
- [Chapter 2, “WebLogic Trap Notifications,”](#) describes the characteristics of WebLogic enterprise-specific SNMP trap notifications.
- [Chapter 3, “SNMP Proxies,”](#) describes how WebLogic Server can function as a master agent that proxies for other SNMP agents.

For information on using SNMP to manage WebLogic Server, refer to "[Configuring SNMP and WebLogic Server](#)" in the *Administration Console Online Help*.

Audience

This document is intended mainly for system administrators who will be managing the WebLogic Server application platform and its various subsystems.

e-docs Web Site

BEA product documentation is available on the BEA corporate Web site. From the BEA Home page, click on Product Documentation.

How to Print the Document

You can print a copy of this document from a Web browser, one main topic at a time, by using the File→Print option on your Web browser.

A PDF version of this document is available on the WebLogic Server documentation Home page on the e-docs Web site (and also on the documentation CD). You can open the PDF in Adobe Acrobat Reader and print the entire document (or a portion of it) in book format. To access the PDFs, open the WebLogic Server documentation Home page, click Download Documentation, and select the document you want to print.

Adobe Acrobat Reader is available at no charge from the Adobe Web site at <http://www.adobe.com>.

Contact Us!

Your feedback on BEA documentation is important to us. Send us e-mail at docsupport@bea.com if you have questions or comments. Your comments will be reviewed directly by the BEA professionals who create and update the documentation.

In your e-mail message, please indicate the software name and version you are using, as well as the title and document date of your documentation. If you have any questions about this version of BEA WebLogic Server, or if you have problems installing and running BEA WebLogic Server, contact BEA Customer Support through BEA WebSupport at <http://www.bea.com>. You can also contact Customer Support by using the contact information provided on the Customer Support Card, which is included in the product package.

When contacting Customer Support, be prepared to provide the following information:

- Your name, e-mail address, phone number, and fax number
- Your company name and company address
- Your machine type and authorization codes
- The name and version of the product you are using
- A description of the problem and the content of pertinent error messages

Documentation Conventions

The following documentation conventions are used throughout this document.

| Convention | Usage |
|--------------------------------------|--|
| Ctrl+Tab | Keys you press simultaneously. |
| <i>italics</i> | Emphasis and book titles. |
| monospace text | Code samples, commands and their options, Java classes, data types, directories, and file names and their extensions. Monospace text also indicates text that the user is told to enter from the keyboard. <i>Examples:</i> <pre>import java.util.Enumeration; chmod u+w * config/examples/applications .java config.xml float</pre> |
| <i>monospace italic text</i> | Placeholders. <i>Example:</i> <pre>String CustomerName;</pre> |
| UPPERCASE MONOSPACE TEXT | Device names, environment variables, and logical operators. <i>Examples:</i> <pre>LPT1 BEA_HOME OR</pre> |
| { } | A set of choices in a syntax line. |
| [] | Optional items in a syntax line. <i>Example:</i> <pre>java utils.MulticastTest -n name -a address [-p portnumber] [-t timeout] [-s send]</pre> |
| | Separates mutually exclusive choices in a syntax line. <i>Example:</i> <pre>java weblogic.deploy [list deploy undeploy update] password {application} {source}</pre> |

| Convention | Usage |
|------------|---|
| . . . | Indicates one of the following in a command line: <ul style="list-style-type: none">• An argument can be repeated several times in the command line.• The statement omits additional optional arguments.• You can enter additional parameters, values, or other information |
| . | Indicates the omission of items from a code example or from a syntax line. |

Introduction to the WebLogic SNMP Agent

WebLogic Server can use Simple Network Management Protocol (SNMP) to communicate with enterprise-wide management systems. The WebLogic Server subsystem that gathers WebLogic management data, converts it to SNMP communication modules (trap notifications), and forwards the trap notifications to third-party SNMP management systems is called the WebLogic SNMP agent. The WebLogic SNMP agent supports the SNMPv1 and SNMPv2 protocols.

Typically, you use SNMP to provide a single location from which to manage a heterogeneous software and hardware environment.

The following sections describe the SNMP management model and how WebLogic Server implements this model:

- [“The SNMP Agent/Manager Model” on page 1-2](#)
- [“The Role of the SNMP Agent in a WebLogic Server Domain” on page 1-2](#)
- [“WebLogic Server Managed Resources and MBeans” on page 1-4](#)
- [“SNMP MIB for WebLogic Server” on page 1-6](#)
- [“SNMP Community Names” on page 1-8](#)

For more information, refer to the following:

- [“Configuring SNMP and WebLogic Server”](#) in the *Administration Console Online Help* (enabling the WebLogic SNMP agent and using SNMP to manage WebLogic Server)
- [“WebLogic SNMP Agent Command-Line Reference”](#) in the *WebLogic Server Command Reference*

- “[Using BATCHUPDATE to Configure the WebLogic SNMP Agent](#)” in the *WebLogic Server Command Reference*

The SNMP Agent/Manager Model

SNMP management is based on the agent/manager model described in the network management standards defined by the International Organization for Standardization (ISO). In this model, a network/systems manager exchanges monitoring and control information about system and network resources with distributed software processes called **agents**.

Any system or network resource that is manageable through the exchange of information is a **managed resource**. This could be a software resource, such as a Java Database Connectivity (JDBC) connection pool, or a hardware resource, such as a router.

Agents function as “collection devices” that gather and send data about the managed resource in response to a request from a manager. In addition, agents often have the ability to issue unsolicited reports to managers when they detect certain predefined thresholds or conditions on a managed resource. In SNMP terminology, these unsolicited event reports are called **trap notifications**.

A manager relies upon a database of definitions and information about the properties of managed resources and the services the agents support — this makes up the Management Information Base (MIB). When new agents are added to extend the management reach of a manager, the manager must be provided with a new MIB component that defines the manageable features of the resources managed through that agent. The manageable attributes of resources, as defined in an SNMP-compliant MIB, are called **managed objects**. Defining the heterogeneous components of an enterprise’s distributed systems within a common MIB on the management station provides a unified perspective and single access point for managing system and network resources.

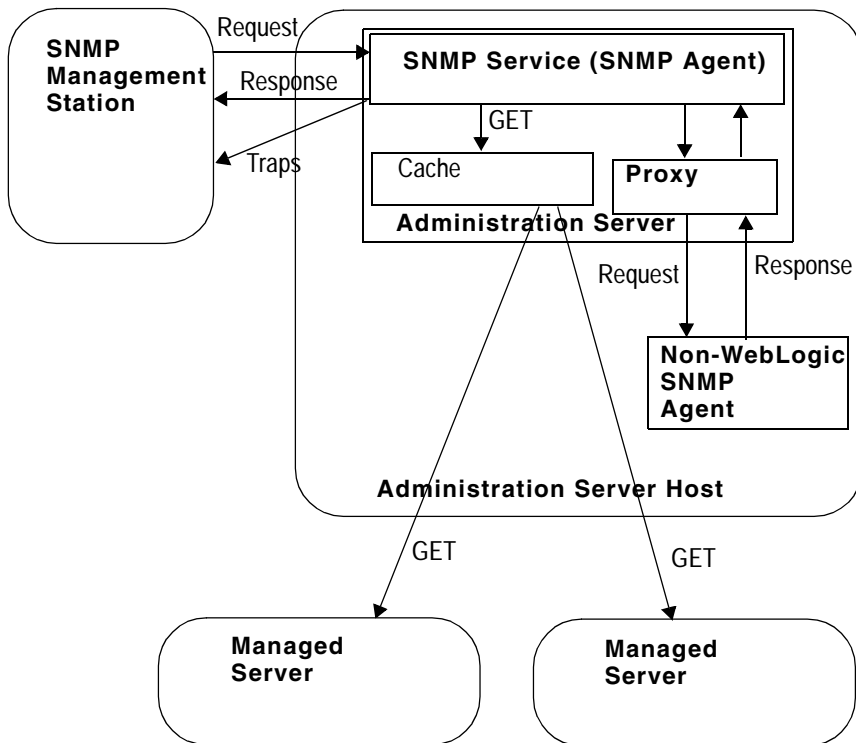
The Role of the SNMP Agent in a WebLogic Server Domain

The WebLogic SNMP agent runs on a domain’s Administration Server. (See [Figure 1-1](#).)

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. Typically, you configure a domain to include additional WebLogic Server instances called **Managed Servers**. You deploy applications, EJBs, and other resources on the Managed Servers and use the Administration Server for configuration and management purposes only.

Using multiple Managed Servers lets you balance loads and provide failover protection for critical applications, while using a single Administration Server simplifies the management of the Managed Server instances. For more information about domains, refer to "[Overview of WebLogic Server Domains](#)" in *Configuring and Managing WebLogic Server*.

Figure 1-1 SNMP Management of a WebLogic Domain



You can use the WebLogic SNMP agent to do the following:

- Respond to simple GET requests from an SNMP manager for the current value of WebLogic attributes.
- Send trap notifications to SNMP managers when the Administration Server starts and when any Managed Server starts or shuts down.
- Send trap notifications to SNMP managers when messages are logged in a Managed Server that satisfy criteria that you specify.

- Send trap notifications to SNMP managers when a WebLogic configuration attribute that you specify has changed value.
- Offload polling of WebLogic attributes to the WebLogic Administration Server using standard JMX monitors, based on thresholds and polling intervals that you define. A trap notification is sent to the SNMP manager when the criteria you specify are satisfied.
- Act as a proxy agent that passes requests from an SNMP manager to other SNMP agents (such as an Oracle database agent) on the same machine.

For information on enabling and configuring the WebLogic SNMP agent, refer to "[Enabling and Configuring the WebLogic SNMP Agent](#)" in the *Administration Console Online Help*.

WebLogic Server Managed Resources and MBeans

Resources on WebLogic Server instances use Java Management Extensions (JMX) Managed Beans (MBeans) to expose their management functions. An **MBean** is a concrete Java class that is developed in accordance with JMX specifications. It can provide getter and setter operations for each management attribute within a managed resource along with additional management operations that the resource makes available.

WebLogic Server MBeans that expose the configuration data of a managed resource are called **Configuration MBeans** while MBeans that provide performance metrics and other information about the runtime state of a managed resource are called **Runtime MBeans**. For example, a `ServerMBean` Configuration MBean indicates the listen port for a server instance while the `ServerRuntimeMBean` Runtime MBean indicates the current lifecycle state of a server instance.

While you can create MBeans (custom MBeans) to manage the applications or services that you deploy on WebLogic Server, the WebLogic SNMP agent does not recognize these custom MBeans as SNMP managed resources. You cannot configure the WebLogic SNMP agent to monitor or generate traps for custom MBeans.

For more information about MBeans on WebLogic Server, refer to the following:

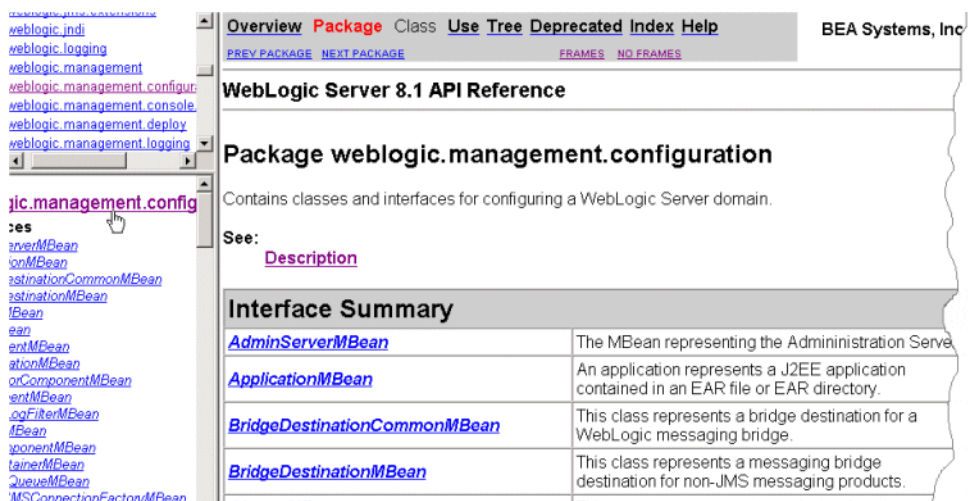
- "[Documentation for Configuration MBean APIs](#)" on page 1-5
- "[Documentation for Runtime MBean APIs](#)" on page 1-5
- "[Overview of WebLogic JMX Services](#)" in the *Programming WebLogic Management Services with JMX* guide

Documentation for Configuration MBean APIs

To view the documentation for Configuration MBeans, do the following:

1. Open the [WebLogic Server Javadoc](#).
2. In the top left pane of the Web browser, click `weblogic.management.configuration`.
The lower left pane displays links for the package.
3. In the lower left pane, click `weblogic.management.configuration` again.
The right pane displays the package summary. (See [Figure 1-2](#).)

Figure 1-2 Javadoc for the configuration Package



4. Click on an interface name to view its API documentation.

Documentation for Runtime MBean APIs

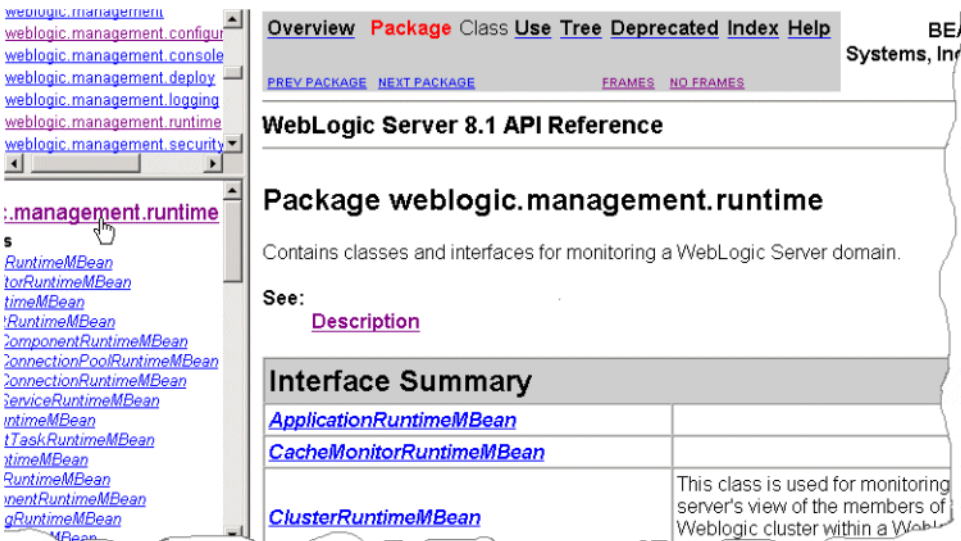
To view the documentation for Runtime MBeans, do the following:

1. Open the [WebLogic Server Javadoc](#).
2. In the top left pane of the Web browser, click `weblogic.management.runtime`.
The lower left pane displays links for the package.

3. In the lower left pane, click `weblogic.management.runtime` again.

The right pane displays the package summary. (See [Figure 1-3](#).)

Figure 1-3 Javadoc for the runtime Package



4. Click on an interface name to view its API documentation.

SNMP MIB for WebLogic Server

All WebLogic Server attributes that can be accessed by SNMP management software are defined in an SNMP-compliant Management Information Base (MIB).

Note: Not all objects in the WebLogic Server MIB represent MBean attributes. For example, the WebLogic Server MIB includes objects that define trap variables.

The BEA WebLogic SNMP MIB conforms to a coding standard called Abstract Syntax Notation.1 (ASN.1). An ASN.1 file is a standard SNMP file that defines the objects that make up an SNMP-compliant MIB. Each object in the file is defined in compliance with the SNMP standard. The BEA WebLogic Server software includes the ASN.1 file `BEA-WEBLOGIC-MIB.asn1` for defining the BEA WebLogic Server MIB for SNMP. The BEA WebLogic SNMP MIB is written in compliance with RFC 1212, as required by the SNMP standard.

Browsing the MIB

You can use any of the following methods to browse the contents of the WebLogic Server MIB:

- Use a MIB browser. WebLogic Server does not provide a MIB browser, but most vendors of SNMP utilities do. The MIB is located in a file named `WL_HOME\server\lib\BEA-WEBLOGIC-MIB.asn1`.
- Use a Web browser to view the [WebLogic Server SNMP MIB Reference](#) on the BEA e-docs Web site.

Because the MIB Reference uses Javascript and DHTML to provide browsing capabilities that are similar to a MIB browser, you must use one of the following Web browsers:

- Internet Explorer, version 5 or higher
- Netscape Navigator, version 6 or higher
- Opera 7 or higher
- Mozilla
- Phoenix

Object Identifiers

The WebLogic Server MIB assigns a unique number called an **object identifier** (OID) to its MBean attributes. Each MBean attribute in the MIB is an SNMP managed object and is manageable by an SNMP management system.

The MIB creates a hierarchical relationship between managed objects and expresses the hierarchy in a tree structure, called the MIB tree or registration tree. Each OID in the MIB consists of a left-to-right sequence of integers. This sequence defines the location of the object in the MIB tree and specifies a unique path through the tree to the object. Each node in the path have both a number and a name associated with it. The path `.1.3.6.1.4.1` defines the `private.enterprises` OID and each number beneath that node on the tree represents the branches in the tree reserved for a particular vendor.

The BEA MIBs are registered at the location `.1.3.6.1.4.1.140` in the tree. And the WebLogic Server MIB consists of all OIDs below `.1.3.6.1.4.140.625`.

OIDs for Types and Instances

All OIDs that represent WebLogic Server MBean attributes in the WebLogic Server MIB are identifiers for the MBean attribute **type**. For example, `.1.3.6.1.4.1.140.625.360.1.60` is the OID for the `serverRuntimeState` attribute type.

To identify a specific **instance** of an attribute type, the WebLogic SNMP agent generates and appends an additional set of numbers to the OID of an attribute type. For example, the OID that specifies the value of the `serverRuntimeState` attribute for an active instance of the sample `MedRecServer` is

```
.1.3.6.1.4.1.140.625.360.1.60.32.102.100.48.98.101.102.100.99.102.52.98.97
.48.48.49.102.57.53.51.50.100.102.53.55.97.101.52.56.99.99.97.99
```

The OID is persistent across instantiations of the object type.

The WebLogic Server MIB Reference appends `(.*)` to the OIDs that represent attribute types. This convention indicates that specific instances of the type are identified by additional numbers. For example, the WebLogic Server MIB Reference indicates that the OID for the `serverRuntimeState` attribute type is `.1.3.6.1.4.1.140.625.360.1.60(.*)`.

You can use the `snmpwalk` or `snmpgetnext` commands to see the object-instance OID for any WebLogic Server attribute. For more information, refer to “[WebLogic SNMP Agent Command-Line Reference](#)” in the *WebLogic Server Command Reference*.

SNMP Community Names

To ensure that the entity requesting data from the WebLogic SNMP agent has permission to obtain the data, and to verify that the agent has permission to send trap notifications to a target manager, SNMP uses textual passwords called **community names**.

When you set up the SNMP agent capability of the Administration Server (described in “[Enabling and Configuring the WebLogic SNMP Agent](#)” in the *Administration Console Online Help*), one of the things you must specify is the community name that the agent expects from the SNMP manager. If the agent receives an SNMP request with an incorrect community name, it generates an `authenticationFailure` trap and sends it to the source of the request.

Using Community Names to Specify Target Servers in Management Requests

You can use some SNMP managers to send requests to the WebLogic SNMP agent for the value of attributes. Because a WebLogic Server domain can have multiple server instances

concurrently active, a request that specifies only an attribute name is potentially ambiguous. For example, the attribute `serverUptime` exists for each WebLogic Server instance in a domain.

To request the value of an attribute on a specific Managed Server, when you send a request from an SNMP manager, append the name of the server instance to the SNMP password (community) that it sends with the request as follows:

community_prefix@server_name

where *community_prefix* is the SNMP community name and *server_name* is the name of the targeted Managed Server. The *community_prefix* value sent by the manager must match the value that you set in the Community Prefix field when you configure the SNMP agent.

To request the value of an attribute on the Administration Server, send a community string to the WebLogic SNMP agent with the following form:

community_prefix

To request the value of an attribute for all server instances in a domain, send a community string with the following form:

community_prefix@domain_name

Introduction to the WebLogic SNMP Agent

WebLogic Trap Notifications

You can configure the WebLogic SNMP agent to detect certain thresholds or conditions within a managed resource and send a report (trap notification) to one or more SNMP managers. The WebLogic SNMP agent can generate traps that conform to the SNMPv1 or SNMPv2 protocols.

The following sections describe the trap notifications that the WebLogic SNMP agent can generate:

- [“Format of WebLogic Trap Notifications” on page 2-1](#)
- [“Automatically Generated WebLogic SNMP Traps” on page 2-3](#)
- [“Log Message Traps” on page 2-4](#)
- [“Monitor Traps” on page 2-6](#)
- [“Attribute Change Traps” on page 2-9](#)

For information on configuring or deleting WebLogic Server trap notifications, refer to [“Configuring SNMP and WebLogic Server”](#) in the *Administration Console Online Help*.

To see an example of using the `weblogic.Admin` utility to configure trap notifications, refer to [“Using BATCHUPDATE to Configure the WebLogic SNMP Agent”](#) in the *WebLogic Server Command Reference*.

Format of WebLogic Trap Notifications

The WebLogic SNMP agent sends each trap notification to SNMP managers in the form of a protocol data unit (PDU) with the fields indicated in [Figure 2-1](#).

Figure 2-1 SNMP Trap Packet

| | | | | | | |
|----------|------------|---------------|-------------------|--------------------|-----------|-------------------|
| PDU type | enterprise | agent address | generic trap type | specific trap type | timestamp | variable bindings |
|----------|------------|---------------|-------------------|--------------------|-----------|-------------------|

The fields have the following meaning:

- PDU type identifies the packet as a trap notification.
- enterprise is the vendor identification (OID) for the systems/network management subsystem that generated the trap. All traps generated by the WebLogic SNMP agent have the WebLogic OID .1.3.6.1.4.140.625 in the enterprise field.
- agent address is the IP address of the WebLogic Server instance on which the trap was generated.
- generic trap type is an integer in the range of 0 to 6. Table 2-1 lists the values that the different types of WebLogic SNMP traps supply for the generic trap type field.

Table 2-1 Values for the Generic Trap Type Field

| WebLogic Trap | Generated When | generic trap type Value |
|-------------------------------|--|-------------------------|
| coldStart | The Administration Server starts. | 0 |
| authenticationFailure | An SNMP manager sends an incorrect community string. The community string prefix is the actual password and must match the value that you set in the Community Prefix field of the Administration Console. (See “SNMP Community Names” on page 1-8.) | 4 |
| All other WebLogic SNMP traps | | 6 |

Traps with a generic trap value of 6 are called *enterpriseSpecific* traps and are accompanied by a value in the specific trap type field.

- specific trap type is a number that further qualifies an enterpriseSpecific trap. Table 2-2 lists the values that the different types of WebLogic SNMP traps supply for the specific trap type field.

Table 2-2 Values for the Specific Trap Type Field

| WebLogic Trap | Generated When | specific trap type Value |
|---------------------------|--|-----------------------------|
| All Log Message Traps | A server instance logs a message that matches user-defined criteria for sending a log notification trap. | 60 |
| serverStart Trap | A Managed Server that was down is now up. | 65 |
| serverShutDown Trap | A Managed Server that was up is now down. | 70 |
| All Monitor Traps | A user-defined JMX monitor detects the crossing of a threshold or occurrence of an event. | 75 |
| All Attribute Change Trap | An attribute selected by the user has changed in value. | 80 |

- `timestamp` is the length of time between the last re-initialization of the WebLogic SNMP agent and the time at which the trap was issued.
- `variable bindings` consists of name/value pairs that further describe the trap notification. Subsequent sections in this topic describe the name/value pairs for each type of trap notification:
 - [“Automatically Generated WebLogic SNMP Traps” on page 2-3](#)
 - [“Variable Bindings in Log Message Traps” on page 2-5](#)
 - [“Variable Bindings in Monitor Traps” on page 2-8](#)
 - [“Variable Bindings in Attribute Change Traps” on page 2-9](#)

Automatically Generated WebLogic SNMP Traps

If you enable the SNMP service for a domain, the WebLogic SNMP agent generates the trap notifications described in [Table 2-3](#). Some of these traps include name/value pairs in the PDU to further describe the event.

Table 2-3 Automatically Generated Trap Notifications

| Trap | Generated When | Variable Bindings |
|-----------------------|---|--|
| coldStart | The Administration Server starts. | none |
| authenticationFailure | An SNMP manager sends an incorrect community string. The community string prefix is the actual password and must match the value that you set in the Community Prefix field of the Administration Console. (See “SNMP Community Names” on page 1-8.) | none |
| serverStart | A WebLogic Managed Server that was down is now up. | Contains two name/value pairs to identify server start time and the server name. |
| serverShutDown | A Managed Server that was up is now down. | Contains two name/value pairs to identify server down time and the server name. |

Log Message Traps

Subsystems and deployable modules (such as applications) on a WebLogic Server instance generate log messages to communicate status or other operational data.

Each server instance saves these messages in a local log file and then broadcasts them as JMX notifications. You can set up the WebLogic SNMP agent to listen for all of these messages or you can set up a filter based on criteria such as the following:

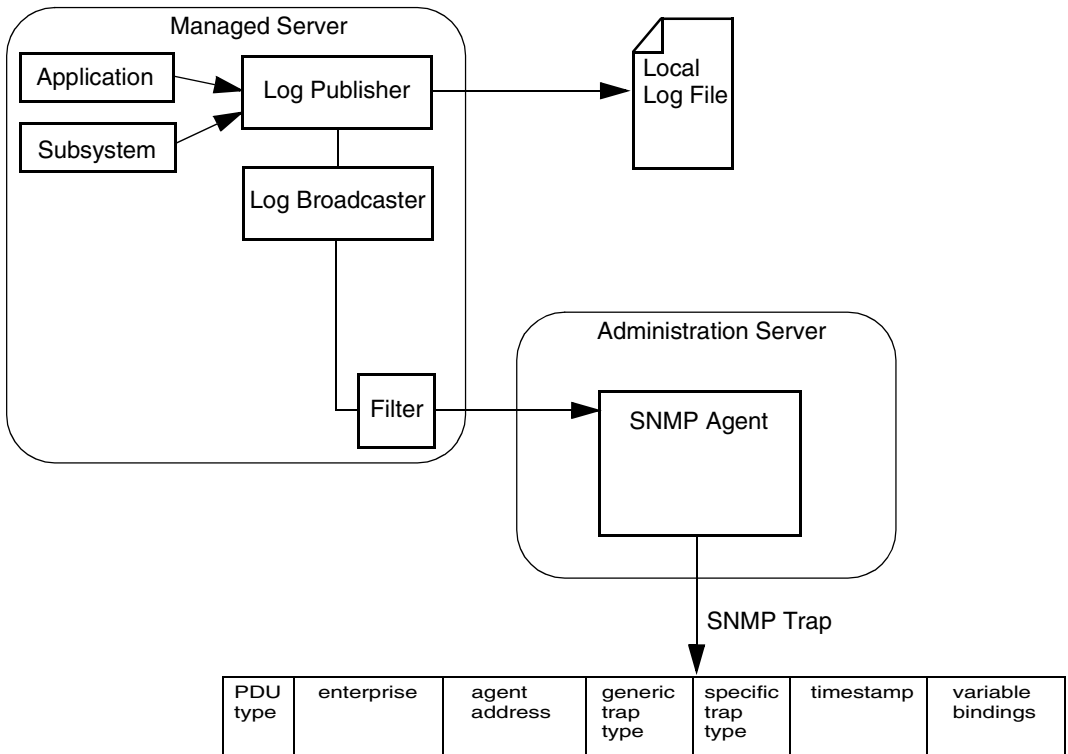
- The severity level of the message
- The name of the subsystem that generated the message
- The user ID under which the subsystem is running
- A unique message ID
- A string within the message text

For example, you can specify that only messages from the Security Service of severity level ERROR or higher are sent to the SNMP agent. For information on setting up the SNMP agent to

listen for messages, refer to ["Create a Notification Log Filter"](#) in the *Administration Console Online Help*.

When the agent receives a message, it generates an SNMP log notification trap. (See [Figure 2-2](#).)

Figure 2-2 Log Message Traps



Variable Bindings in Log Message Traps

This section describes the name/value pairs that the log message traps pass to the SNMP manager in the variable bindings field:

- `trapTime` — Time when the trap is generated.
- `trapServerName` — Name of the server instance on which the log message was generated.

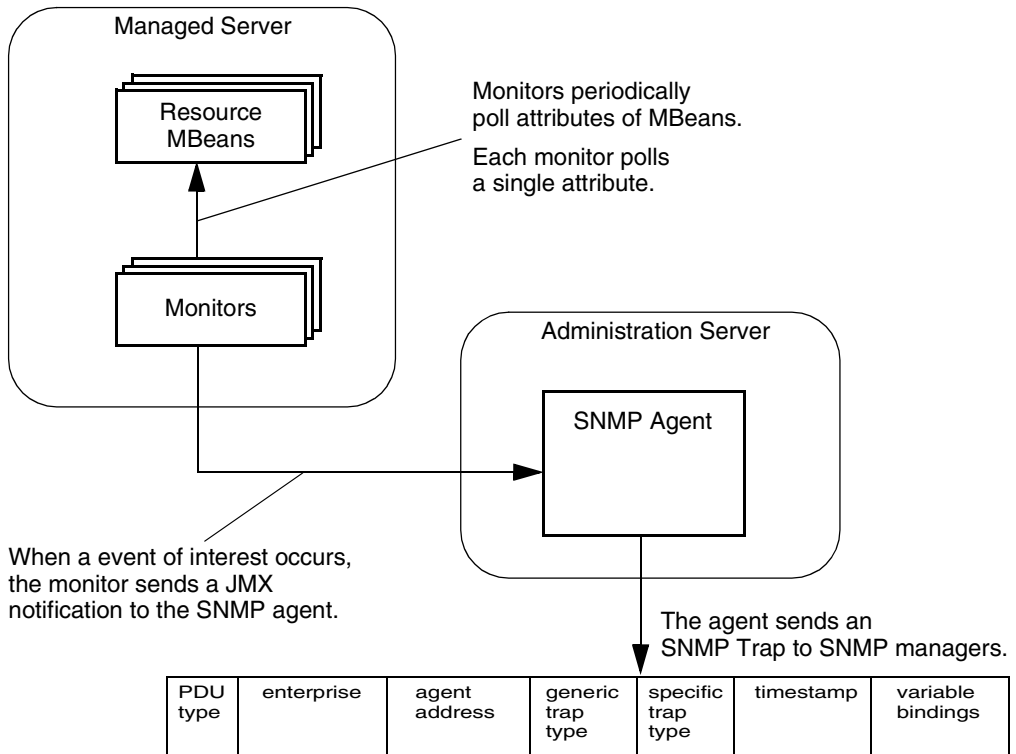
- `trapMachineName` — Name of the machine on which the server instance is running.
- `trapLogThreadId` — Thread ID from the log message.
- `trapLogTransactionId` — Transaction ID, if any, from the log message. Transaction ID is present only for messages logged within the context of a transaction.
- `trapLogUserId` — The user ID from the log message. The user ID indicates the security context in which the log message was generated.
- `trapLogSubsystem` — The subsystem that generated the log message.
- `trapLogMsgId` — The log message ID from the log message.
- `trapLogSeverity` — The message severity level from the log message.
- `trapLogMessage` — The text of the log message.

For more information on log messages and the WebLogic Server logging subsystem, refer to "[Server Log](#)" in the *Administration Console Online Help*.

Monitor Traps

To periodically check the value of WebLogic resources for changes, you set up monitors and assign them to instances of WebLogic Server. The monitors poll the MBeans of WebLogic resources at a specified interval and send notifications to the WebLogic SNMP agent when an event that you specify occurs, such as the crossing of a threshold. The SNMP agent generates a trap notification and sends it to the SNMP managers. (See [Figure 2-3](#).)

Figure 2-3 Monitor Traps



If you are unfamiliar with WebLogic Server MBeans, refer to "[Overview of WebLogic JMX Services](#)" in the *Programming WebLogic Management Services with JMX* guide.

You can configure three types of JMX monitors, depending on the data type of the attribute that you want to observe (the MBean Javadoc describes the type of data that its attributes return):

- **Counter Monitor**

A counter monitor observes attribute values that are returned as an `Integer` object type.

You can specify that a trap is generated if an attribute is beyond the bounds of a threshold value. You can also specify that if a value exceeds a threshold, the monitor increases the threshold by an offset value. Each time the observed attribute exceeds the new threshold, the threshold is increased by the offset value, up to a maximum allowable threshold that you specify.

For information on configuring a counter monitor, refer to "[Configuring a Counter Monitor](#)" in the *Administration Console Online Help*.

- **Gauge Monitor**

A gauge monitor observes changes in MBean attributes that are expressed as integers or floating-point.

You can specify that a trap is generated if an attribute is beyond the bounds of a high or low threshold value.

For information on configuring a gauge monitor, refer to "[Configuring a Gauge Monitor](#)" in the *Administration Console Online Help*.

- **String Monitor**

A string monitor observes changes in attributes that are expressed as `String` objects.

You can specify that a trap is generated if there is a match between the value and the string you provide, or you can specify that the trap is generated if the value differs from the string you provide.

For information on configuring a string monitor, refer to "[Configuring a String Monitor](#)" in the *Administration Console Online Help*.

Variable Bindings in Monitor Traps

A JMX monitor polls for a specified threshold or condition and the agent generates a monitor trap when the specified threshold is crossed, or the specified condition occurs. The WebLogic SNMP agent includes the following name/value pairs in the variable bindings of each monitor trap:

- `trapTime` — The time at which the trap was generated.
- `trapServerName` — The local server whose attribute value generated the trap.
- `trapMonitorType` — Either `CounterMonitor`, `StringMonitor`, or `GaugeMonitor`.
- `trapMonitorThreshold` — An ASCII representation of the threshold that triggered the trap.
- `trapMonitorValue` — An ASCII representation of the value that triggered the trap.
- `trapMBeanName` — The name of the MBean that contained the attribute being monitored.
- `trapMBeanType` — The type of the MBean that contained the attribute being monitored.
- `trapAttributeName` — The name of the attribute whose value triggered the trap.

Attribute Change Traps

While you can use JMX monitors to periodically poll WebLogic Server resources for changes to attributes that exceed the bounds of specific thresholds, you can also configure the SNMP agent to send a trap immediately after an attribute is changed in any way. For example, you can use a monitor to poll for changes in the current number of active JDBC pools. If the number of active pools exceeds a threshold, the SNMP agent can send a trap. You would use an attribute change trap to detect whether an attribute such as the name of a JDBC pool or the listen port has been changed.

For information on configuring the SNMP agent to send attribute change traps, refer to ["Configuring an Attribute Change"](#) in the *Administration Console Online Help*.

Variable Bindings in Attribute Change Traps

An attribute change trap notification includes the following name/value pairs in the variable bindings:

- `trapTime` — The time at which the trap was generated.
- `trapServerName` — The name of the Administration Server.
- `trapMBeanName` — Name of the MBean that includes the attribute.
- `trapMBeanType` — Type of the MBean that includes the attribute.
- `trapAttributeName` — Name of the configuration attribute that has changed.
- `trapAttributeChangeType` — The value can be either ADD, REMOVE, or UPDATE.
- `trapAttriruteOldVal` — Value of the attribute before the change.
- `trapAttributeNewVal` — Value of the attribute after the change.

Note: Creation of monitors for changes in run-time attributes is not supported. Only attributes in the configuration MIB can be monitored for change of attribute value.

SNMP Proxies

This section provides background information on WebLogic Server and SNMP proxy agents. For information on configuring WebLogic Server to be a proxy for other SNMP agents, refer to ["Configuring an SNMP Proxy"](#) in the *Administration Console Online Help*.

SNMP Agent as Proxy for Other Agents

The original SNMP management model allowed for only a single, monolithic agent to carry out all management responsibilities on a given network node (IP address). This solution was not flexible enough to provide for effective management of increasingly complex systems. In addition to the agents typically provided by computer manufacturers for hardware and operating system information, agents are also produced by vendors of other products, such as agents for SQL database systems. Complex and heterogeneous systems thus require the ability to accommodate multiple agents on a single network node.

This weakness of the original SNMP model led to the concept of an SNMP master agent that acts as a proxy for other SNMP agents. The WebLogic SNMP agent can function as a master agent in this sense. To use the master agent functionality of the WebLogic SNMP agent, you can assign branches of the registration tree (OID tree) as the responsibility of other SNMP agents. Each of these will be a branch that encompasses the private MIB (or some part of that MIB) which the target agent is designed to manage.

Note: You cannot use the WebLogic SNMP agent as a proxy for SNMP agents in other WebLogic Server domains. For example, WebLogic domainA's SNMP agent cannot proxy requests to domainB's SNMP agent. This limitation is in effect because all WebLogic SNMP agents use the same MIB root.

Instead of proxying requests to multiple WebLogic Server domains, you can place all of your server instances in a single domain and send requests directly to each Managed Server. See [“Using Community Names to Specify Target Servers in Management Requests”](#) on page 1-8.

The WebLogic SNMP agent listens for requests from SNMP managers and then fans out these requests to other SNMP agents on the Administration Server machine, if the attribute requested has an OID falling under the branch of the OID tree assigned to one of those other agents. By default the WebLogic SNMP agent listens for management requests on port 161. If the WebLogic SNMP agent is to proxy for other SNMP agents, then those other agents must be configured to listen for SNMP management requests on a port other than the port that the WebLogic SNMP agent is using to receive requests from SNMP managers.

The Microsoft Windows SNMP Service

While the WebLogic Server SNMP agent can be a proxy for other SNMP agents, it cannot be configured as a subagent of the Microsoft Windows SNMP agent service.

Using Microsoft Extension Agent API, the Microsoft Windows 2000 SNMP agent service can be a proxy for other SNMP agents. However, WebLogic Server does not support this feature and cannot use the Windows SNMP agent as a proxy.

Sources of SNMP Information

This appendix lists sources of additional information about Simple Network Management Protocol, including the following:

- [Reference Books](#)
- [Standards and Drafts](#)
- [Obtaining RFCs](#)

Reference Books

If you need additional information about MIBs, agents, or the SNMP protocol, refer to these books:

- Comer, Douglas; Internetworking with TCP/IP, Vol. 2; Prentice-Hall, Englewood Cliffs, New Jersey, 1991
- Leinwand, Allan and Fang, Karen; Network Management: A Practical Perspective; Addison-Wesley, Reading, Massachusetts, 1993
- Rose, Marshall T.; The Simple Book: An Introduction to Management of TCP/IP-based Internets; Prentice-Hall, Englewood Cliffs, New Jersey, 1991
- Rose, Marshall T.; The Open Book: A Practical Perspective on Open Systems Interconnection; Prentice-Hall, Englewood Cliffs, New Jersey, 1989
- Miller, Mark; Managing Internetworks with SNMP, M & T Books

- Stallings, William; SNMP, SNMPv2 and CMIP: The Practical Guide to Network Management Standards, Addison-Wesley, Reading, Massachusetts, 1993

Standards and Drafts

The SNMP protocol has been defined through a series of Requests for Comments (RFCs). The following standards and drafts are available.

Figure 0-1 SNMP RFCs

| RFC Number | Description |
|-----------------|--------------------------------------|
| 052 | IAB Recommendations |
| 1089 | SNMP over Ethernet |
| 1109 | Ad-hoc Review |
| 1155 | Structure of Management Information |
| 1156 | Management Information Base (MIB-I) |
| 1157 | SNMP Protocol |
| 1161 | SNMP over OSI |
| 1187 | Bulk table retrieval |
| 1212 | Concise MIB definitions |
| 1213 | Management Information Base (MIB-II) |
| 1214 | OSI MIB |
| 1215 | Traps |
| 1227 | SNMP Multiplex (SMUX) |
| 1228 | SNMP-DPI |
| 1229 | Generic-interface MIB extensions |
| 1230 IEEE 802.4 | Token Bus MIB |
| 1231 IEEE 802.5 | Token Ring MIB |

| RFC Number | Description |
|------------|----------------------|
| 1239 | Reassignment of MIBs |
| 1243 | AppleTalk MIB |
| 1248 | OSPF MIB |
| ISO 8824 | ASN.1 |
| ISO 8825 | BER for ASN.1 |

Obtaining RFCs

You can obtain Requests for Comments in the following ways:

- Download them from almost anywhere on the Internet
- Obtain them from SRI International

Mailing Address: SRI International, EJ291, DDN Network Information Center, 333 Ravenswood Ave., Menlo Park CA 94025

Phone: +1.800.235.3155

e-mail: MAIL-SERVER@nisc.sri.com. Leave the subject field blank. In the body, enter: SEND RFCnnnn.TXT-1

FTP: ftp://ftp.nisc.sri.com/rfc/rfcNNNN.txt

Sources of SNMP Information

Index

A

- administration domain. *See* domain 1-2
- Administration MBeans
 - API documentation 1-5
- Administration Servers
 - defined 1-2
- agent
 - what it is 1-2
- agents
 - what they are 1-2
- attribute change trap
 - variable bindings in 2-9

C

- community name, SNMP 1-8
 - how manager must specify 1-9
- community prefix
 - see community name 1-9
- Configuration MBeans
 - defined 1-4
 - See also* Local Configuration MBeans *and* Administration MBeans
- customer support contact information viii

D

- documentation, where to find it vii
- domains
 - defined 1-2

E

- enterprise OID 2-2

F

- format, SNMP trap notification 2-1

G

- generic trap types 2-2

J

- Java Management Extension
 - See* JMX 2-7
- Javadoc
 - for Configuration MBeans 1-5
 - for Runtime MBeans 1-5
- JMX monitors 2-7
 - variable bindings in attribute change trap 2-9
 - variable bindings in monitor trap 2-8

L

- Local Configuration MBeans
 - API documentation 1-5
- log message traps
 - variable bindings in 2-5

M

- managed object
 - in SNMP 1-2
- managed resource
 - what it is 1-2
- Managed Servers
 - defined 1-2
- MBeans

- defined 1-4
- MIB file
 - location of 1-7
- MIB, for WebLogic 1-6
- monitor trap
 - variable bindings in 2-8
- multiple SNMP agents
 - configuring WebLogic agent with 3-1

P

- polling
 - how to offload to WebLogic Administration Server 2-6
- printing product documentation viii
- proxying for other agents 3-1

R

- Runtime MBeans
 - API documentation 1-5
 - defined 1-4

S

- serverStart trap 2-4
- SNMP
 - agent/manager model in 1-2
 - trap notification, fields in 2-1
- SNMP agent
 - configuring as proxy agent 3-1
- SNMP agent, WebLogic
 - what it does 1-3
- specific trap types
 - for WebLogic 2-2, 2-3
- support
 - technical viii

T

- trap notification
 - what it is 1-2

- traps based on log messages 2-4

V

- variable bindings
 - in attribute change trap 2-9
 - in log message trap 2-5
 - in monitor trap 2-8, 2-9

W

- WebLogic
 - specific trap types 2-2, 2-3
- WebLogic enterprise OID 2-2