



Sun Java System Access Manager 7.1 Performance Tuning Guide



Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 819-4673-10
February 2007

Copyright 2007 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more U.S. patents or pending patent applications in the U.S. and in other countries.

U.S. Government Rights – Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

This distribution may include materials developed by third parties.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, the Solaris logo, the Java Coffee Cup logo, docs.sun.com, Java, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and SunTM Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

Products covered by and information contained in this publication are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical or biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2007 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plusieurs brevets américains ou des applications de brevet en attente aux Etats-Unis et dans d'autres pays.

Cette distribution peut comprendre des composants développés par des tierces personnes.

Certains composants de ce produit peuvent être dérivées du logiciel Berkeley BSD, licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays; elle est licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, le logo Solaris, le logo Java Coffee Cup, docs.sun.com, Java et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui, en outre, se conforment aux licences écrites de Sun.

Les produits qui font l'objet de cette publication et les informations qu'il contient sont régis par la législation américaine en matière de contrôle des exportations et peuvent être soumis au droit d'autres pays dans le domaine des exportations et importations. Les utilisations finales, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes chimiques ou biologiques ou pour le nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou réexportations vers des pays sous embargo des Etats-Unis, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exclusive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la législation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement désignés, sont rigoureusement interdites.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON.

Contents

- Preface7**
- 1 Introduction to Access Manager Tuning 13**
 - Before You Begin 13
 - Tuning Access Manager and Other Components 13
- 2 Access Manager Tuning Scripts 15**
 - Overview of the Access Manager Tuning Scripts 15
 - Tuning Modes 16
 - Running an Access Manager Tuning Script 17
 - ▼ To Run a Tuning Script 17
 - Access Manager amtune -env File Parameters 18
 - Access Manager Tuning Parameters 18
 - Installation Environment Tuning Parameters 22
 - Web Server 7 Tuning Parameters 26
 - Application Server 8 Tuning Parameters 27
- 3 Directory Server Tuning29**
 - Directory Server Tuning Parameters 29
 - Directory Server Tuning Scripts 30
 - Running in REVIEW Mode 30
 - Applying the Tuning Changes 31
- A Tuning Considerations33**
 - Operating System (OS) Considerations 33
 - Solaris OS Kernel and TCP/IP Parameters 33
 - Linux OS 34

Third-Party Web Containers 37

 IBM WebSphere Application Server 37

 BEA WebLogic Server 38

Index41

Tables

TABLE 2-1	Access Manager Tuning Scripts	16
TABLE 2-2	Access Manager Tuning Parameters	18
TABLE 2-3	Installation Environment Tuning Parameters	22
TABLE 2-4	Web Server 7 Tuning Parameters	27
TABLE 2-5	Application Server 8 Web Container Tuning Parameters	27
TABLE 3-1	Directory Server Tuning Parameters	30

Preface

The *Sun Java™ System Access Manager 7.1 Performance Tuning Guide* describes how to tune Access Manager 7.1 and its related components to improve performance and efficiency.

Access Manager is a component of the Sun Java Enterprise System (Java ES), a set of software components that provide services needed to support enterprise applications distributed across a network or Internet environment.

Who Should Use This Book

This book is primarily intended for system and network administrators who are tuning Access Manager 7.1 and its related components.

Before You Read This Book

You should be familiar with the following components and concepts:

- Access Manager technical concepts, as described in the *Sun Java System Access Manager 7.1 Technical Overview*.
- Deployment platform: Solaris™ or Linux operating system.
- Access Manager Web container: Sun Java System Application Server, Sun Java System Web Server, BEA WebLogic Server, or IBM WebSphere Application Server.
- Technical concepts: Lightweight Directory Access Protocol (LDAP), Java technology, JavaServer Pages™ (JSP) technology, HyperText Transfer Protocol (HTTP), HyperText Markup Language (HTML), and eXtensible Markup Language (XML).

How This Book Is Organized

This book is organized as follows:

- Chapter 1 is an introduction to Access Manager performance tuning.
- Chapter 2 describes how to run the Access Manager tuning scripts.
- Chapter 3 describes how to tune Sun Java System Directory Server.
- Appendix A provides considerations for the Solaris OS, Linux OS, and third-party web containers, including IBM WebSphere Application Server and BEA WebLogic Server.

Related Books

Related documentation is available as follows:

- “Access Manager Core Documentation” on page 8
- “Related Sun Java Enterprise System Documentation” on page 9

Access Manager Core Documentation

The following table describes the Access Manager documentation set, which is available on the following web site:

<http://docs.sun.com/coll/1292.2>

TABLE P-1 Access Manager Documentation Set

Title	Description
<i>Sun Java System Access Manager 7.1 Release Notes</i>	Describes new features, problems fixed, installation notes, and known issues and limitations. The Release Notes are updated periodically after the initial release to describe any new features or problems.
<i>Sun Java System Access Manager 7.1 Documentation Center</i>	Contains links to commonly referenced information in the Access Manager documentation collection.
<i>Sun Java System Access Manager 7.1 Technical Overview</i>	Provides an overview of how Access Manager components work together to consolidate access control functions, and to protect enterprise assets and web-based applications. It also explains basic Access Manager concepts and terminology.
<i>Sun Java System Access Manager 7.1 Deployment Planning Guide</i>	Provides planning and deployment solutions for Access Manager based on the solution life cycle.

TABLE P-1 Access Manager Documentation Set (Continued)

Title	Description
<i>Sun Java System Access Manager 7.1 Postinstallation Guide</i>	Provides configuration information for Access Manager.
<i>Sun Java System Access Manager 7.1 Administration Guide</i>	Describes how to use the Access Manager console as well as manage user and service data via the command line interface.
<i>Sun Java System Access Manager 7.1 Administration Reference</i>	Provides reference information for the Access Manager command-line interface (CLI), configuration attributes, <code>AMConfig.properties</code> attributes, <code>serverconfig.xml</code> file attributes, log files, and error codes.
<i>Sun Java System Access Manager 7.1 Federation and SAML Administration Guide</i>	Provides information about the Federation module based on the Liberty Alliance Project specifications. It includes information on the integrated services based on these specifications, instructions for enabling a Liberty-based environment, and summaries of the application programming interface (API) for extending the framework.
<i>Sun Java System Access Manager 7.1 Developer's Guide</i>	Provides information about customizing Access Manager and integrating its functionality into an organization's current technical infrastructure. It also contains details about the programmatic aspects of the product and its API.
<i>Sun Java System Access Manager 7.1 C API Reference</i>	Provides summaries of data types, structures, and functions that make up the public Access Manager C APIs.
<i>Sun Java System Access Manager 7.1 Java API Reference</i>	Provides information about the implementation of Java packages in Access Manager.
<i>Sun Java System Access Manager 7.1 Performance Tuning Guide</i>	Provides information about how to tune Access Manager and its related components for optimal performance. (this guide)
<i>Sun Java System Access Manager Policy Agent 2.2 User's Guide</i>	Provides an overview of Policy Agent software, including the web agents and J2EE agents that are currently available. To view the Access Manager Policy Agent 2.2 documentation collection, see: http://docs.sun.com/coll/1322.1

Related Sun Java Enterprise System Documentation

The following table provides links to documentation collections for related Java ES products.

TABLE P-2 Related Sun Java Enterprise System Documentation

Product	Link
Sun Java Enterprise System 5	http://docs.sun.com/coll/1286.2
Sun Java System Directory Server Enterprise Edition 6	http://docs.sun.com/coll/1224.1
Sun Java System Web Server 7	http://docs.sun.com/coll/1308.3
Sun Java System Application Server Enterprise Edition 8.2	http://docs.sun.com/coll/1310.3
Sun Java System Message Queue 3.7 UR1	http://docs.sun.com/coll/1307.2
Sun Java System Web Proxy Server 4.0.4	http://docs.sun.com/coll/1311.4

Related Third-Party Web Site References

Third-party URLs are referenced in this document and provide additional, related information.

Note – Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Documentation, Support, and Training

The Sun web site provides information about the following additional resources:

- [Documentation \(http://www.sun.com/documentation/\)](http://www.sun.com/documentation/)
- [Support \(http://www.sun.com/support/\)](http://www.sun.com/support/)
- [Training \(http://www.sun.com/training/\)](http://www.sun.com/training/)

Typographic Conventions

The following table describes the typographic conventions that are used in this book.

TABLE P-3 Typographic Conventions

Typeface	Meaning	Example
AaBbCc123	The names of commands, files, and directories, and onscreen computer output	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. <code>machine_name%</code> you have mail.
AaBbCc123	What you type, contrasted with onscreen computer output	<code>machine_name%</code> su Password:
<i>aabbcc123</i>	Placeholder: replace with a real name or value	The command to remove a file is <i>rm filename</i> .
<i>AaBbCc123</i>	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the <i>User's Guide</i> . A <i>cache</i> is a copy that is stored locally. Do <i>not</i> save the file. Note: Some emphasized items appear bold online.

Shell Prompts in Command Examples

The following table shows the default UNIX® system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P-4 Shell Prompts

Shell	Prompt
C shell	<code>machine_name%</code>
C shell for superuser	<code>machine_name#</code>
Bourne shell and Korn shell	<code>\$</code>
Bourne shell and Korn shell for superuser	<code>#</code>

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions.

To share your comments, go to <http://docs.sun.com> and click Send Comments. In the online form, provide the document title and part number. The part number is a seven-digit or nine-digit number that can be found on the title page of the book or at the top of the document.

For example, the title of this book is *Sun Java System Access Manager 7.1 Performance Tuning Guide*, and the part number is 819-4673-10.

Introduction to Access Manager Tuning

This guide provides performance tuning information for Sun Java™ System Access Manager, including how to run the Access Manager tuning scripts. You can run these scripts to tune Access Manager and its related components.

Before You Begin

Before you use this guide, Access Manager and other Sun Java Enterprise System component products such as Directory Server, Web Server, and Application Server must be installed. For information about installing these products, see the *Sun Java Enterprise System 5 Installation Guide for UNIX*.



Caution – Tuning Access Manager and its related components is an iterative process that can vary for different deployments. The Access Manager tuning scripts try to apply the optimal tuning parameter settings. However, each deployment is unique and might require further customization to suit specific requirements.

Tuning Access Manager and Other Components

This guide includes the following information:

- [Chapter 2](#) describes how to run the Access Manager tuning scripts.
- [Chapter 3](#) describes how to tune Sun Java System Directory Server.
- [Appendix A](#) provides considerations for the Solaris OS, Linux OS, and third-party web containers, including IBM WebSphere Application Server and BEA WebLogic Server.

Access Manager Tuning Scripts

The Sun Java™ System Access Manager 7.1 tuning scripts allow you to tune Access Manager and other components of your deployment, including Sun Java System Directory Server, the web container running Access Manager, and the operating system (OS) kernel and TCP/IP parameters.

This chapter includes the following topics:

- [“Overview of the Access Manager Tuning Scripts” on page 15](#)
- [“Access Manager `amtune-env` File Parameters” on page 18](#)

Overview of the Access Manager Tuning Scripts

The Access Manager tuning scripts are non-interactive. To run a script, you first edit the parameters in the `amtune-env` configuration file to specify the tuning options you want to set for your specific environment. Then, you run either the `amtune` script, which calls other scripts as needed, or a specific script. For example, you might run only the `amtune-identity` script to tune only Access Manager.

The Access Manager tuning scripts and the `amtune-env` configuration file are installed in the following directory, depending on your platform:

- Solaris systems: *AccessManager-base/SUNWam/bin/amtune*
- Linux systems: *AccessManager-base/identity/bin/amtune*

AccessManager-base is the Access Manager 7.1 base installation directory. The default base installation directory is `/opt` on Solaris systems and `/opt/sun` on Linux systems.

The following table describes the tuning scripts that are available in the Access Manager 7.1 release.

TABLE 2-1 Access Manager Tuning Scripts

Script	Description
amtune	Wrapper script that calls other scripts based on values in the amtune-env file.
amtune-identity	Tunes the installed instance of Access Manager.
amtune-os	Tunes the operating system kernel and TCP/IP parameters.
amtune-ws7	Tunes the Sun Java System Web Server 7 Web container.
amtune-ws61	Tunes the Sun Java System Web Server 6.1 2005Q4 SP5 Web container.
amtune-as8	Tunes the Sun Java System Application Server Enterprise Edition 8.2 Web container.
amtune-as7	Tunes the Sun Java System Application Server 7 Web container.
amtune-preparedSTuner	Generates the amtune-directory script, which you can use to tune the Directory Server that supports Access Manager. For more information, see Chapter 3 .

Tuning Modes

The Access Manager tuning scripts can run in the following modes, as determined by the `AMTUNE_MODE` parameter in the `amtune-env` file.

- **REVIEW** mode (default). The scripts return tuning recommendations for an Access Manager deployment, but they do not make any actual changes to the environment.
- **CHANGE** mode. The scripts make all of the tuning modifications that are defined in the `amtune-env` file, except for Directory Server. For more information, see [Chapter 3](#).

In either mode, the scripts return a list of tuning recommendations to the `amtune` debug log file and the terminal window. The location of the log file is determined by the `com.ipplanet.services.debug.directory` parameter in the `AMConfig.properties` file. The default debug directory depends on your platform:

- Solaris systems: `/var/opt/SUNWam/debug`
- Linux systems: `/var/opt/sun/identity/debug`



Caution – Tuning is an iterative process that can vary for different deployments. The Access Manager tuning scripts try to apply the optimal tuning parameter settings. However, each deployment is unique and might require further customization to suit specific requirements.

Therefore, use CHANGE mode only after you have reviewed and understand the tuning changes that will be applied to your deployment.

Running an Access Manager Tuning Script

To run a tuning script, use the following syntax:

```
amtune-script admin_password dirmanager_password [ as8_admin_password ]
```

The tuning script parameters are:

- *amtune-script* is one of the tuning scripts: *amtune*, *amtune-identity*, *amtune-os*, *amtune-ws61*, *amtune-as7*, *amtune-as8*, or *amtune-prepareDSTuner*.
- *admin_password* is the Access Manager Administrator password.
- *dirmanager_password* is the Directory Manager (cn=Directory Manager) password.
- *as8_admin_password* is the Administrator password that is required if you are tuning Application Server (WEB_CONTAINER is set to AS8).

▼ To Run a Tuning Script

This section describes the basic steps to run an Access Manager Tuning script.

- 1 **Log in as or become superuser.**
- 2 **If you have not run the scripts in REVIEW mode, ensure that AMTUNE_MODE is set to REVIEW (default value) in the `amtune-env` file.**
- 3 **Edit other parameters in the `amtune-env` file, depending on the components you want to tune:**
 - Access Manager `amtune-env` file parameters
 - Installation environment tuning parameters
 - “[Application Server 8 Tuning Parameters](#)” on page 27 (if Application Server 8 is the web container)

To tune the Directory Server that supports Access Manager, see [Chapter 3](#).

- 4 **In REVIEW mode, run either the `amtune` script or one of the component scripts.**
- 5 **Review the tuning recommendations in the debug log file. If needed, make changes to the `amtune-env` file based on this run.**

- 6 If you are satisfied with the tuning recommendations from the REVIEW mode run, set **AMTUNE_MODE** to **CHANGE** in the `amtune -env` file.
- 7 In **CHANGE** mode, run either the `amtune` script or one of the component scripts. For example, to tune the Solaris OS, run `amtune -os`, as follows:

```
# ./amtune -os admin_password dirmanager_password
```
- 8 Check the debug log file for the results of the run.

Note – In **CHANGE** mode, the `amtune` script might need to restart the Web container and Access Manager. In some instances, `amtune` might also recommend a system restart.

Access Manager amtune -env File Parameters

The `amtune -env` file contains the parameters to define the tuning options for an Access Manager deployment, including:

- “Access Manager Tuning Parameters” on page 18
- “Installation Environment Tuning Parameters” on page 22
- “Web Server 7 Tuning Parameters” on page 26
- “Application Server 8 Tuning Parameters” on page 27

For a description of the Directory Server parameters, see [Chapter 3](#).

Access Manager Tuning Parameters

The following table describes the specific parameters for tuning Access Manager.

TABLE 2–2 Access Manager Tuning Parameters

Parameter	Description
AMTUNE_MODE	Sets the tuning mode to one of the following: <ul style="list-style-type: none">■ REVIEW– The scripts return tuning recommendations for an Access Manager deployment but do not make any actual changes to the deployment environment.■ CHANGE– The scripts make all of the tuning modifications that you have defined in the <code>amtune -env</code> file, except for Directory Server. For more information, see Chapter 3. <p>Default: REVIEW</p>

TABLE 2-2 Access Manager Tuning Parameters (Continued)

Parameter	Description
AMTUNE_TUNE_OS	Tunes the operating system kernel and TCP/IP settings. Default: true
AMTUNE_TUNE_DS	Generates a script to tune the Directory Server that supports Access Manager. Default: true
AMTUNE_TUNE_WEB_CONTAINER	Tunes the Access Manager web container, which can be either Web Server or Application Server. Default: true
AMTUNE_TUNE_IDENTITY	Tunes the installed instance of Access Manager. Default: true
AMTUNE_DEBUG_FILE_PREFIX	Identifies the prefix for the amtune log file. If this parameter is set, all operations performed by the amtune scripts are logged. The location of the log file is determined by the <code>com.iplanet.services.debug.directory</code> parameter in the <code>AMConfig.properties</code> file. If this parameter is not set, information is not logged, and all output is sent to <code>/dev/null</code> . Default: amtune

TABLE 2-2 Access Manager Tuning Parameters (Continued)

Parameter	Description
AMTUNE_PCT_MEMORY_TO_USE	<p>Specifies the percent of available memory used by Access Manager.</p> <p>Currently, Access Manager can use a maximum of 4 GB, which is the per process address space limit for 32-bit applications.</p> <p>Access Manager requires a minimum of 256 MB RAM.</p> <p>When you set AMTUNE_PCT_MEMORY_TO_USE to 100, the maximum space allocated for Access Manager is the minimum between 4 GB and 100% of available RAM.</p> <p>When you set AMTUNE_PCT_MEMORY_TO_USE to 0, Access Manager is configured to use 256 MB RAM</p> <p>Default: 75</p> <p>The following values are derived from this parameter setting:</p> <ul style="list-style-type: none">■ JVM memory usage - Heap sizes, NewSizes, PermSizes■ Thread pool sizes - Web Server RqThrottle, Authentication LDAP connection pool, SM LDAP connection pool, Notification thread pools■ Access Manager caches - SDK caches and session caches■ Maximum sizes - Maximum number of sessions and maximum number of cache entries <p>AMConfig.properties File Settings</p> <p>Notification thread pool settings:</p> <p>com.ipланet.am.notification.threadpool.size</p> <p>com.ipланet.am.notification.threadpool.threshold</p> <p>SDK cache maximum size setting:</p> <p>com.ipланet.am.sdk.cache.maxsize</p> <p>Session settings:</p> <p>com.ipланet.am.session.httpSession.enabled</p> <p>com.ipланet.am.session.maxSessions</p> <p>com.ipланet.am.session.invalidsessionmaxtime</p> <p>com.ipланet.am.session.purgedelay</p>

TABLE 2-2 Access Manager Tuning Parameters (Continued)

Parameter	Description
AMTUNE_PER_THREAD_STACK_SIZE	<p>Sets the available stack space per thread in Java (Web container). The per thread stack size is used to tune various thread-related parameters in Access Manager and the Web container.</p> <p>Default: 128 KB</p> <p>Caution: Do not change this value unless absolutely necessary.</p>
AMTUNE_DONT_TOUCH_SESSION_PARAMETERS	<p>Specifies whether session time-out tuning using the next three parameters is enabled. To enable, set to false.</p> <p>Default: true</p>
AMTUNE_SESSION_MAX_SESSION_TIME_IN_MTS	<p>Sets the maximum session time in minutes.</p> <p>Default: 60</p> <p>However, the default value might be different for your installation. If the session service is registered and customized at the any other level, the tuning will not apply.</p> <p>Setting this parameter to very high or very low values affects the number of active user sessions an Access Manager deployment can support, so this parameter is optional for tuning purposes.</p> <p>To use this parameter, AM_TUNE_DONT_TOUCH_SESSION_PARAMETERS must be set to false.</p>
AMTUNE_SESSION_MAX_IDLE_TIME_IN_MTS	<p>Sets the maximum idle time for a session in minutes.</p> <p>Default: 10</p> <p>However, the default value might be different for your installation. If the Session service is registered and customized at the any other level, the tuning will not apply.</p> <p>Setting this parameter to very high or very low values affects the number of active user sessions an Access Manager deployment can support, so this parameter is optional for tuning purposes.</p> <p>To use this parameter, AM_TUNE_DONT_TOUCH_SESSION_PARAMETERS must be set to false.</p>

TABLE 2-2 Access Manager Tuning Parameters (Continued)

Parameter	Description
AMTUNE_SESSION_MAX_CACHING_TIME_IN_MTS	<p>Sets the maximum session cache time in minutes.</p> <p>Default: 2</p> <p>However, the default value might be different for your installation. If the Session service is registered and customized at the any other level, the tuning will not apply.</p> <p>Setting this parameter to very high or very low values affects the number of active use sessions an Access Manager deployment can support, so this parameter is optional for tuning purposes.</p> <p>To use this parameter, AM_TUNE_DONT_TOUCH_SESSION_PARAMETERS must be set to false.</p>

Installation Environment Tuning Parameters

The following table describes the Access Manager installation environment tuning parameters.

Note – The OSTYPE, OSPLATFORM, and HWPLATFORM parameters are used to construct other parameters, so you should not need to change their values.

TABLE 2-3 Installation Environment Tuning Parameters

Parameter	Description
HOSTNAME	<p>Specifies the host name of the system where Access Manager is deployed.</p> <p>If the host name for your environment cannot be obtained using the hostname command, comment the following line:</p> <pre>HOSTNAME='/bin/hostname /bin/cut -f1 -d'.'</pre> <p>Then, add a line setting the correct host name. For example:</p> <pre>HOSTNAME=myhost</pre>

TABLE 2-3 Installation Environment Tuning Parameters (Continued)

Parameter	Description
DOMAINNAME	<p>Specifies the domain name of the system where Access Manager is deployed.</p> <p>If the domain name for your environment cannot be obtained using the <code>domainname</code> command, comment the following line:</p> <pre>DOMAINNAME='/bin/domainname'</pre> <p>Then, add a line setting the correct domain name. For example:</p> <pre>DOMAINNAME=example.com</pre>
IS_CONFIG_DIR	<p>Specifies the Access Manager configuration directory.</p> <p>Default: <code>/etc/opt/SUNWam/config</code></p> <p>Note: Do not change this parameter.</p>
AMTUNE_BIN_DIR	<p>Specifies the location of the tuning scripts. Set this variable only if the tuning scripts are not installed in the default location. Otherwise, leave it blank.</p> <p>Default: <i>AccessManager-base/bin/amtune</i></p>
WEB_CONTAINER	<p>Specifies the name of the Web container on which Access Manager is deployed:</p> <ul style="list-style-type: none"> ■ WS7 — Web Server 7 ■ WS61 — Web Server 6.1 ■ AS8 — Application Server 8 ■ AS7 — Application Server 7 <p>Default: WS7</p> <p>Any other value returns a validation error.</p>
CONTAINER_BASE_DIR	<p>Specifies the base directory for the Web container that is running Access Manager. If you installed the Web container in a non-default location, change this value before running <code>amtune</code>.</p> <p>Default values:</p> <ul style="list-style-type: none"> ■ Web Server 7: <code>/opt/SUNWwbsvr7</code> ■ Web Server 6.1: <code>/opt/SUNWwbsvr</code> ■ Application Server 7: <code>/var/opt/SUNWappserver7</code> ■ Application Server 8 on Solaris systems <code>/var/opt/SUNWappserver</code> ■ Application Server 8 on Linux systems <code>/var/opt/sun/appserver</code>

TABLE 2-3 Installation Environment Tuning Parameters (Continued)

Parameter	Description
WEB_CONTAINER_INSTANCE_NAME	<p>Specifies the instance name of the Access Manager web container.</p> <p>Typically, this value is the host name where Access Manager is deployed. If you have multiple instances for the Web container, this value might be different from the host name, and you must set it to the correct instance name.</p> <p>Defaults:</p> <ul style="list-style-type: none">■ Web Server 6.1 or Web Server 7: <i>hostname</i> (<code>\${HOSTNAME}</code>)■ Application Server 7: <code>domains/server1</code>■ Application Server 8: <code>domains/domain1</code>

TABLE 2-3 Installation Environment Tuning Parameters (Continued)

Parameter	Description
IS_INSTANCE_NAME	<p>Specifies the Access Manager instance names. IS_INSTANCE_NAME is used to determine the properties file names for the Access Manager installation.</p> <p>Default: none</p> <p>You can deploy multiple instances of Access Manager on the same machine, but generally, there is one set of properties files for each Access Manager instance, and the instance name is appended to the file names.</p> <p>If there is only one instance of Access Manager on a machine, the instance name is not appended to the file name.</p> <p>For example, there might be a single instance of Access Manager running under the default instance of Web Server.</p> <p>If Access Manager is installed on a machine named <code>server.example.com</code>, typically the first instance of Web Server is <code>https-server.example.com</code>. The properties files for the first Access Manager instance will not have the instance name appended (for example, <code>AMConfig.properties</code>).</p> <p>Multiple Access Manager Instances</p> <p>Multiple instances will have different names. For example, if there are three instances of Web Server, the Web Server instances might be:</p> <ul style="list-style-type: none">■ <code>server.example.com-instance1</code>■ <code>server.example.com-instance2</code>■ <code>server.example.com-instance3</code> <p>If three instances of Access Manager are deployed (one per web container instance), the primary properties file names for Access Manager (typically, <code>AMConfig.properties</code>) might be named as:</p> <ul style="list-style-type: none">■ <code>AMConfig-instance1.properties</code>■ <code>AMConfig-instance2.properties</code>■ <code>AMConfig-instance3.properties</code>

TABLE 2-3 Installation Environment Tuning Parameters (Continued)

Parameter	Description
IS_INSTANCE_NAME (continued)	<p>You can specify IS_INSTANCE_NAME=<i>instance1</i>. The amtune script resolves the properties file names in the following order:</p> <ol style="list-style-type: none">1. AMConfig-IS_INSTANCE_NAME2. AMConfig-WEB_CONTAINER_INSTANCE_NAME3. AMConfig.properties <p>The script uses the first available properties file in the list. The amadmin utility should also point to the correct server name. Java option:</p> <pre>-Dserver.name=IS_INSTANCE_NAME</pre> <p>amtune automatically tries to associate the instance names with the Access Manager properties files using this parameter. Currently, only these files are based on this instance name:</p> <ul style="list-style-type: none">■ AMConfig.properties■ serverconfig.xml
CONTAINER_INSTANCE_DIR	<p>Specifies the base directory for the Access Manager web container instance. If you have installed the web container in a non-default location, change this value before running amtune.</p> <p>Default values are:</p> <p>Web Server 6.1 or Web Server 7:</p> <pre>\$CONTAINER_BASE_DIR/https-\${WEB_CONTAINER_INSTANCE_NAME}</pre> <p>Application Server 7 or Application Server 8:</p> <pre>\$CONTAINER_BASE_DIR/\${WEB_CONTAINER_INSTANCE_NAME}</pre>
DS_BASE_DIR	<p>Specifies the directory where Directory Server 6 is installed.</p> <p>Default: /opt/sun/ds6</p>

Web Server 7 Tuning Parameters

The following table describes the tuning parameters that you can set when you are using Web Server 7 as the Access Manager web container.

TABLE 2-4 Web Server 7 Tuning Parameters

Parameter	Description
WSADMIN	Specifies the location of the wsadmin utility. Default: Solaris systems: /opt/SUNWwbsvr7/bin/wadm Linux systems: /opt/sun/webserver7/bin/wadm
WSADMIN_USER	Specifies the Web Server 7 administrator. Default: admin
WSADMIN_PASSFILE	Specifies the Web Server 7 temporary password file used by the wsadmin utility. Default: /tmp/passfile
WSADMIN_HOST	Specifies the Web Server 7 admin host name. Default: localhost (\$HOSTNAME)
WSADMIN_PORT	Specifies the Web Server 7 admin port. Default: 8989
WSADMIN_SECURE	Specifies whether WSADMIN_PORT is a secure port. "- -ssl=true" indicates a secure port. "- -ssl=false" indicates the port is not secure. Default: "- -ssl=true"
WSADMIN_CONFIG	Specifies the Web Server 7 instance name. Default: \$WEB_CONTAINER_INSTANCE_NAME
WSADMIN_HTTPLISTENER	Specifies the Web Server 7 HTTP listener name. Default: http-listener-1

Application Server 8 Tuning Parameters

The following table describes the tuning parameters that you can set when you are using Application Server 8 as the Access Manager web container.

TABLE 2-5 Application Server 8 Web Container Tuning Parameters

Parameter	Description
ASADMIN	Specifies the Application Server 8 asadmin utility location. Default values: <ul style="list-style-type: none">■ Solaris systems: /opt/SUNWappserver/appserver/bin/asadmin■ Linux systems: /opt/sun/appserver/bin/asadmin

TABLE 2-5 Application Server 8 Web Container Tuning Parameters (Continued)

Parameter	Description
ASADMIN_USER	Specifies the Application Server 8 administrator user account. Default: admin
ASADMIN_PASSFILE	Specifies the temporary password file location used by the asadmin utility. The amtune -as8 script creates this file and then deletes it after use. Default: /tmp/passfile
ASADMIN_HOST	Specifies the Application Server 8 admin host name. Default: \$HOSTNAME
ASADMIN_PORT	Specifies the Application Server 8 admin port. Default: 4849
ASADMIN_SECURE	Specifies whether the ASADMIN_PORT is secure: <ul style="list-style-type: none"> ■ "--secure" specifies the port is secure. ■ Blank specifies that the port is not secure. Default: "--secure"
ASADMIN_TARGET	Specifies whether this Application Server 8 installation is used exclusively for Access Manager and Portal Server. Default: server, indicating that Application Server 8 installation is exclusively used for Access Manager and Portal Server.
ASADMIN_HTTPPLISTENER	Specifies the HTTP Application Server 8 listener name. Default: http-listener-1
ASADMIN_INTERACTIVE	Specifies whether Application Server 8 administrator operates interactively. Default: false Caution: Do not change this parameter.
AMTUNE_WEB_CONTAINER_JAVA_POLICY	Specifies whether Application Server 8 evaluates Java security descriptors, as specified in the server.policy file. Default: false Caution: Do not change this parameter. Evaluating Java security descriptors can add a significant performance overhead.

Directory Server Tuning

Sun Java™ System Access Manager 7.1 includes scripts to tune either Sun Java System Directory Server 5.2 2005Q4 or Sun Java System Directory Server Enterprise Edition 6. Access Manager must use an existing Directory Server, either local or remote, in non-exclusive mode.



Caution – If you are working with a production Directory Server or a Directory Server that has not been backed up (both the data and the configuration), it is recommended that you do not run the `amtune-directory` script in `CHANGE` mode to apply tuning changes.

After you run the `amtune-directory` script in `REVIEW` mode, review the tuning recommendations and apply them manually, if they meet your deployment needs.

Also, make sure you back up both your Directory Server data and configuration before you make any changes.

This chapter includes the following topics:

- [“Directory Server Tuning Parameters” on page 29](#)
- [“Directory Server Tuning Scripts” on page 30](#)

Directory Server Tuning Parameters

The following table describes the Directory Server tuning parameters in the `amtune-env` configuration file.

TABLE 3-1 Directory Server Tuning Parameters

Parameter	Description
AMTUNE_TUNE_DS	Generates a script to tune the Directory Server that supports Access Manager. Default: true
DIRMGR_UID	Specifies the user ID of the Directory Manager. If your deployment uses a user ID other than the default value (cn=Directory Manager), you must set this parameter with that value. Default: cn=Directory Manager
RAM_DISK	Specifies the location of the RAM disk. Default: /tmp
DEFAULT_ORG_PEOPLE_CONTAINER	Specifies the people container name for the default organization. This parameter is used to tune the LDAP authentication module's search base. It can be useful when there are no sub-organizations in the default organization. If this value is empty (""), tuning is skipped. Note: Along with appending the people container to the search base, the search scope will be modified to "OBJECT" level. The default search scope is "SUBTREE". Default: ""(empty)

Directory Server Tuning Scripts

- [“Running in REVIEW Mode” on page 30](#)
- [“Applying the Tuning Changes” on page 31](#)

Running in REVIEW Mode

The amtune script and amtune-prepareDSTuner scripts do not actually tune Directory Server. However, you must run one of these scripts to generate the amtune-directory script, which you can then use to tune Directory Server.

1. Log in as or become superuser.
2. Make sure that the following parameter is set in the amtune-env file:

```
AMTUNE_TUNE_DS=true
```

3. Run the `amtune` script or `amtune-prepareDSTuner` script. The script generates the following tar file:

```
/tmp/amtune-directory.tar
```

4. Copy the `amtune-directory.tar` file to a temporary location on the server that is running Directory Server.
5. Untar the `amtune-directory.tar` file in the temporary location.
6. In the `amtune-directory` script, make sure `REVIEW` mode is set:

```
AMTUNE_MODE="REVIEW"
```

7. Set these parameters, if you prefer a value other than the default (`amtune`):
 - `DEBUG_FILE_PREFIX` is a prefix that will be included with the timestamp to specify the filename of the log file where the script writes the recommended tuning changes.
 - `DB_BACKUP_DIR_PREFIX` is a prefix that will be included with the timestamp to specify the name of the Directory Server backup directory.
8. Run the `amtune-directory` script in `REVIEW` mode. For example:

```
# ./amtune-directory dirmanager_password
```

The *dirmanager_password* is the Directory Manager password.

9. Review the recommended tuning settings for Directory Server in the debug log file.
The script creates the log file in the debug directory specified by the `com.iplanet.services.debug.directory` parameter in the `AMConfig.properties` file. The default debug log file directory depends on your platform:
 - Solaris systems: `/var/opt/SUNWam/debug`
 - Linux systems: `/var/opt/sun/identity/debug`

Applying the Tuning Changes



Caution – If you are working with a production Directory Server or a Directory Server that has not been backed up (both the data and the configuration), it is recommended that you do not run the `amtune-directory` script in `CHANGE` mode to apply to the tuning changes. Review the tuning recommendations from `REVIEW` mode and apply the changes manually, if they meet your deployment needs.

Before making the tuning changes, the `amtune-directory` script stops and backs up Directory Server.

If you are working with a pilot or prototype Directory Server and you are sure you want to apply the tuning changes, follow these steps:

1. Back up both your Directory Server data and configuration.
2. Set the following parameter in the `amtune-directory` script:

```
AMTUNE_MODE="CHANGE"
```

3. Run the `amtune-directory` script in `CHANGE` mode. For example:

```
# ./amtune-directory dirmanager_password
```

The *dirmanager_password* is the Directory Manager password.

4. Check the `amtune` log file for the results of the run.

Tuning Considerations

- “Operating System (OS) Considerations” on page 33
- “Third-Party Web Containers” on page 37

Note – The following tuning considerations are based on the tuning of various test deployments. Because each deployment is unique, you might need further customization and interactive testing to satisfy your specific requirements.

Operating System (OS) Considerations

- “Solaris OS Kernel and TCP/IP Parameters” on page 33
- “Linux OS” on page 34

Solaris OS Kernel and TCP/IP Parameters

For Solaris SPARC systems with CMT processor with CoolThreads technology, in the `/etc/opt/SUNWam/config/AMConfig.properties` file, it is recommended that you add the following properties at the end of the file:

```
com.sun.identity.log.resolveHostName=false  
com.sun.am.concurrencyRate=value
```

where *value* depends on the number of cores in a Sun Fire T1000 or T2000 server. For example, for 8 cores, set *value* to 8, or for 6 cores, set *value* to 6.

Linux OS

To tune for maximum performance on Linux systems, you need to make tuning adjustments to the following items:

- [“File Descriptors” on page 34](#)
- [“Virtual Memory” on page 35](#)
- [“Network Interface” on page 36](#)
- [“Disk I/O Settings” on page 36](#)
- [“TCP/IP Settings” on page 36](#)

Note – If you are running Application Server 8.1 on Red Hat Linux, the stack size of the threads created by the Red Hat OS for Application Server is 10 Mbytes, which can cause JVM resource problems (CR 6223676). To prevent these problems, set the Red Hat OS operating stack size to a lesser value such as 2048 or even 256 Kbytes, by executing the `ulimit` command before you start Application Server. Execute the `ulimit` command on the same console that you will use to start Application Server. For example:

```
ulimit -s 256
```

File Descriptors

You might need to increase the number of file descriptors from the default. Having a higher number of file descriptors ensures that the server can open sockets under high load and not abort requests coming in from clients. Start by checking system limits for file descriptors with this command:

```
cat /proc/sys/fs/file-max  
8192
```

The current limit shown is 8192. To increase it to 65535, use the following command (as root):

```
echo "65535" > /proc/sys/fs/file-max
```

To make this value to survive a system reboot, add it to `/etc/sysctl.conf` and specify the maximum number of open files permitted:

```
fs.file-max = 65535
```

Note: The parameter is not `proc.sys.fs.file-max`, as you might expect.

To list the available parameters that can be modified using `sysctl`:

```
sysctl -a
```

To load new values from the `sysctl.conf` file:

```
sysctl -p /etc/sysctl.conf
```

To check and modify limits per shell, use the following command:

```
limit
```

The output will look something like this:

```
cputime      unlimited
filesize     unlimit
datasize     unlimited
stacksize    8192 kbytes
coredumpsize 0 kbytes
memoryuse     unlimited
descriptors  1024
memorylocked unlimited
maxproc      8146
openfiles    1024
```

The openfiles and descriptors show a limit of 1024. To increase the limit to 65535 for all users, edit `/etc/security/limits.conf` as root, and modify or add the `nofile` setting (number of file) entries:

```
*      soft  nofile          65535
*      hard  nofile          65535
```

The asterisk (*) is a wildcard that identifies all users. You could also specify a user ID instead.

Then edit `/etc/pam.d/login` and add the line:

```
session required /lib/security/pam_limits.so
```

On Red Hat Linux, you also need to edit `/etc/pam.d/sshd` and add the following line:

```
session required /lib/security/pam_limits.so
```

On many systems, this procedure will be sufficient. Log in as a regular user and try it before doing the remaining steps. The remaining steps might not be required, depending on how pluggable authentication modules (PAM) and secure shell (SSH) are configured.

Virtual Memory

To change virtual memory settings, add the following to `/etc/rc.local`:

```
echo 100 1200 128 512 15 5000 500 1884 2 > /proc/sys/vm/bdflush
```

For more information, view the man pages for `bdflush`.

Network Interface

To ensure that the network interface is operating in full duplex mode, add the following entry into `/etc/rc.local`:

```
mii-tool -F 100baseTx-FD eth0
```

where `eth0` is the name of the network interface card (NIC).

Disk I/O Settings

To tune disk I/O performance for a non-SCSI disk, follow these steps:

1. Test the disk speed with this command:

```
/sbin/hdparm -t /dev/hdX
```

2. Enable direct memory access (DMA) with this command:

```
/sbin/hdparm -d1 /dev/hdX
```

3. Check the speed again using the `hdparm` command. Given that DMA is not enabled by default, the transfer rate might have improved considerably. In order to do this at every reboot, add the `/sbin/hdparm -d1 /dev/hdX` line to `/etc/conf.d/local.start`, `/etc/init.d/rc.local`, or whatever the startup script is called.

TCP/IP Settings

To tune the TCP/IP settings, follow these steps:

1. Add the following entry to `/etc/rc.local`:

```
echo 30 > /proc/sys/net/ipv4/tcp_fin_timeout
echo 60000 > /proc/sys/net/ipv4/tcp_keepalive_time
echo 15000 > /proc/sys/net/ipv4/tcp_keepalive_intvl
echo 0 > /proc/sys/net/ipv4/tcp_window_scaling
```

2. Add the following to `/etc/sysctl.conf`:

```
# Disables packet forwarding
net.ipv4.ip_forward = 0
# Enables source route verification
net.ipv4.conf.default.rp_filter = 1
# Disables the magic-sysrq key
kernel.sysrq = 0
net.ipv4.ip_local_port_range = 1204 65000
net.core.rmem_max = 262140
net.core.rmem_default = 262140
net.ipv4.tcp_rmem = 4096 131072 262140
net.ipv4.tcp_wmem = 4096 131072 262140
```

```
net.ipv4.tcp_sack = 0
net.ipv4.tcp_timestamps = 0
net.ipv4.tcp_window_scaling = 0
net.ipv4.tcp_keepalive_time = 60000
net.ipv4.tcp_keepalive_intvl = 15000
net.ipv4.tcp_fin_timeout = 30
```

3. Add the following as the last entry in `/etc/rc.local`:

```
sysctl -p /etc/sysctl.conf
```

4. Reboot the system.
5. Use this command to increase the size of the transmit buffer:

```
tcp_recv_hiwat ndd /dev/tcp 8129 32768
```

Third-Party Web Containers

- “IBM WebSphere Application Server” on page 37
- “BEA WebLogic Server” on page 38

IBM WebSphere Application Server

Consider making the following changes in the WebSphere Administrative Console:

- “JVM Tuning Parameters” on page 37
- “Servlet Caching” on page 38
- “Thread Pool Size” on page 38

For more information, see the “IBM WebSphere V5.1 Performance, Scalability, and High Availability WebSphere Handbook Series” at:

<http://www.redbooks.ibm.com/Redbooks.nsf/RedbookAbstracts/sg246198.html?OpenDocument>

JVM Tuning Parameters

Add the JVM tuning parameters shown below, by following these links in the console:

Servers>Application Servers>server1>Process Definition>Java Virtual Machine

Add “-server” as the first parameter in the “Generic JVM arguments” box. Then, add the following entries after the other existing parameters:

```
-XX:NewSize=336M -XX:MaxNewSize=336M
-XX:+DisableExplicitGC
-XX:+UseParNewGC
```

```
-XX:+UseConcMarkSweepGC
-XX:+CMSPermGenSweepingEnabled
-XX:+UseCMSCompactAtFullCollection
-XX:CMSFullGCsBeforeCompaction=0
-XX:+CMSClassUnloadingEnabled
-XX:SoftRefLRUPolicyMSPerMB=0
-XX:+PrintClassHistogram
-XX:+PrintGCTimeStamps
-Xloggc:/opt/WebSphere/AppServer/logs/server1/gc.log
-XX:-CMSParallelRemarkEnabled
```

Servlet Caching

Make sure that servlet caching is enabled by checking the checkbox next to “Enable servlet caching” by following these links in the console:

Application Servers>server1>Web Container>Configuration: Servlet caching

Thread Pool Size

Allow the thread pool to grow beyond the maximum thread pool size set by checking the checkbox next to “Allow thread allocation beyond maximum thread size” by following these links:

Application Servers>server1>Web Container>Thread Pool Is Growable

BEA WebLogic Server

Consider making the following changes:

- [“JVM GC Parameter” on page 38](#)
- [“Heap Size” on page 39](#)
- [“Execute Queue Thread Count” on page 39](#)
- [“Connection Backlog Buffering” on page 40](#)

JVM GC Parameter

For BEA WebLogic Server 8.1 SP4, to avoid the `java.lang.OutOfMemoryError` reported by the WebLogic JVM 1.4.2_05, add the following JVM GC (garbage collection) parameter in the `startWebLogic.sh JAVA_OPTIONS`:

```
-XX:-CMSParallelRemarkEnabled
```

Set this parameter in addition to the other heap size and GC parameters that have been added for JVM 1.4.2 and 1.5.0 for Application Server 8.1 and Web Server 6.1.

For example, if Access Manager is installed in the default `user_projects` location (`/usr/local/bean/user_projects/domains/mydomain/startWebLogic.sh`):

```
JAVA_OPTIONS="-XX:+DisableExplicitGC -XX:+UseParNewGC
-XX:+UseConcMarkSweepGC -XX:+CMSPermGenSweepingEnabled
-XX:+UseCMSCompactAtFullCollection -XX:CMSFullGCsBeforeCompaction=0
-XX:+CMSClassUnloadingEnabled -XX:-CMSParallelRemarkEnabled
-XX:SoftRefLRUPolicyMSPerMB=0 -XX:+PrintClassHistogram
-XX:+PrintGCTimeStamps
-Xloggc:/usr/local/bean/user_projects/domains/mydomain/myserver/gc.log"
```

Heap Size

Modify the `commonEnv.sh` script in the `/usr/local/bean/weblogic81/common/bin` directory for heap size increases in the section where `$PRODUCTION_MODE = "true"` (which should be set to true, before running Access Manager in `/usr/local/bean/user_projects/domains/mydomain/startWebLogic.sh`):

```
# Set up JVM options base on value of JAVA_VENDOR
if [ "$PRODUCTION_MODE" = "true" ]; then
    case $JAVA_VENDOR in
        BEA)
            JAVA_VM=-jrockit
            MEM_ARGS="-Xms128m -Xmx256m"
            ;;
        HP)
            JAVA_VM=-server
            MEM_ARGS="-Xms32m -Xmx200m -XX:MaxPermSize=128m"
            ;;
        IBM)
            JAVA_VM=
            MEM_ARGS="-Xms32m -Xmx200m"
            ;;
        Sun)
            JAVA_VM=-server
            MEM_ARGS="-Xms2688M -Xmx2688M -XX:NewSize=336M -XX:MaxNewSize=336M"
            # MEM_ARGS="-Xms32m -Xmx200m -XX:MaxPermSize=128m"
```

Execute Queue Thread Count

Set the Execute Queue Thread count to be more than the number of CPUs. For example, consider using a value that is twice the number of CPUs. Set this value in either the console or in the `/usr/local/bean/user_projects/domains/mydomain/config.xml` file:

```
<ExecuteQueueName="MyExecute Queue" ThreadCount="8" ThreadsIncrease="4"/>
```

For more information, see “Modifying the Default Thread Count” in “WebLogic Server Performance and Tuning” at:

<http://e-docs.bea.com/wls/docs81/perform/WLSTuning.html#1142218>

Connection Backlog Buffering

A guideline for setting Connection Backlog Buffering is 8192 for a server with 4 Gbytes of physical memory (which is equivalent to the `ConnectionQueue` size tuning set in the Sun Java System Web Server 6.1 `magnus.conf` file).

For more information, see “Tuning Connection Backlog Buffering” in the “WebLogic Server Performance and Tuning” document at:

<http://e-docs.bea.com/wls/docs81/perform/WLSTuning.html#1136287>

Index

A

Access Manager

- admin password, 17
 - caches, 20
 - configuration directory, 23
 - instance name, 25
 - multiple instances, 25
 - running tuning scripts, 17
 - tuning modes, 16
 - tuning parameters, 18
 - tuning scripts, 15
- admin host name, Application Server 8, 28
- admin password
- Access Manager, 17
 - Application Server, 17
- admin port, Application Server 8, 28
- admin utility location, Application Server 8, 27
- administrator user account, Application Server 8, 28
- AMConfig.properties file, 16, 19, 25
- amtune-as7 script, 16
- amtune-as8 script, 16
- AMTUNE_DEBUG_FILE_PREFIX parameter, 19
- AMTUNE_DONT_TOUCH_SESSION_PARAMETERS parameter, 21
- amtune-env file
- description of, 18
 - editing, 17
- amtune-identity script, 16
- AMTUNE_MODE parameter, 16, 18
- AMTUNE_PCT_MEMORY_TO_USE parameter, 20
- AMTUNE_PER_THREAD_STACK_SIZE parameter, 21

- amtune-prepareDSTuner script, 16
- amtune script
- description of, 16
 - running, 17
- AMTUNE_SESSION_MAX_CACHING_TIME_IN_MTS parameter, 22
- AMTUNE_SESSION_MAX_IDLE_TIME_IN_MTS parameter, 21
- AMTUNE_SESSION_MAX_SESSION_TIME_IN_MTS parameter, 21
- AMTUNE_TUNE_DS parameter, 19, 30
- AMTUNE_TUNE_IDENTITY parameter, 19
- AMTUNE_TUNE_OS parameter, 19
- AMTUNE_TUNE_WEB_CONTAINER parameter, 19
- AMTUNE_WEB_CONTAINER_JAVA_POLICY parameter, 28
- amtune-ws61 script, 16
- Application Server
- admin password, 17
 - tuning parameters, 27
 - tuning script for, 16
- ASADMIN_HOST parameter, 28
- ASADMIN_INTERACTIVE parameter, 28
- ASADMIN parameter, 27
- ASADMIN_PASSFILE parameter, 28
- ASADMIN_PORT parameter, 28
- ASADMIN_SECURE parameter, 28
- ASADMIN_TARGET parameter, 28
- ASADMIN_USER parameter, 28

B

base directory, web container, 23

C

CHANGE mode, 16, 18, 32
com.iplanet.am.notification.threadpool.size
parameter, 20
com.iplanet.am.notification.threadpool.threshold
parameter, 20
com.iplanet.am.session.httpSession.enabled
parameter, 20
com.iplanet.am.session.invalidsessionmaxtime
parameter, 20
com.iplanet.am.session.maxSessions parameter, 20
com.iplanet.am.session.purgedelay parameter, 20
com.iplanet.services.debug.directory parameter, 16, 19
configuration directory, Access Manager, 23
CONTAINER_BASE_DIR parameter, 23
CONTAINER_INSTANCE_DIR parameter, 26

D

debug log file, checking, 17, 18, 32
DEFAULT_ORG_PEOPLE_CONTAINER
parameter, 30
Directory Manager password, 17
Directory Server
tuning, 29
tuning parameters, 29
DIRMGR_UID parameter, 30
documentation
collections, 9-10
related Java ES product, 9-10
domain name, specifying, 23
domainname command, 23
DOMAINNAME parameter, 23

H

host name, specifying, 22
hostname command, 22

HOSTNAME parameter, 22

I

installation directory, tuning scripts, 15
instance name, Access Manager, 25
IS_CONFIG_DIR parameter, 23
IS_INSTANCE_NAME parameter, 25

J

Java security descriptors, 28
JVM memory usage, 20

L

Linux systems
base directory, 15
tuning scripts for, 15

M

maximum number of cache entries, 20
maximum number of sessions, 20
maximum session cache time, tuning, 22
maximum session idle time, tuning, 21
maximum session time, tuning, 21
modes, tuning, 16
multiple instances, Access Manager, 25

P

password, Directory Manager, 17
password file location, Application Server 8, 28
Portal Server, 28

R

RAM, used by Access Manager, 20

RAM_DISK parameter, 30
restart, required during tuning, 18
REVIEW mode, 16, 17, 18, 31
root, running scripts as, 17, 30

WEB_CONTAINER parameter, 17, 23
Web Server, tuning script for, 16

S

SDK caches, 20
server.policy file, 28
session caches, 20
session time-out tuning, 21
Solaris system
 tuning OS kernel, 19
 tuning scripts for, 15
Sun Java System Access Manager, 15
Sun Java System Application Server, tuning script
 for, 16
Sun Java System Portal Server, 28
Sun Java System Web Server, tuning script for, 16
superuser, running scripts as, 17, 30
syntax to run tuning scripts, 17

T

TCP/IP settings, tuning, 19
thread pool sizes, 20
tuning modes, 16
tuning parameters
 Access Manager, 18
 Application Server 8, 27
 Directory Server, 29
tuning scripts
 description of, 15
 running, 17
 syntax to run, 17

W

web container, instance name, 24
Web container, specifying for tuning, 23
WEB_CONTAINER_INSTANCE_NAME
 parameter, 24

