



# Sun Java System Application Server Utility Reference

---

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

Part No: 817-6092  
March 2004

Copyright 2004 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

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, docs.sun.com, AnswerBook, AnswerBook2, and Solaris are trademarks, registered trademarks, or service marks 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 Sun™ 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.

Federal Acquisitions: Commercial Software—Government Users Subject to Standard License Terms and Conditions.

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 2004 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées du système Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, docs.sun.com, AnswerBook, AnswerBook2, et Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, 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.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REpondre A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.



040331@8606



# Contents

---

## **Preface 9**

## **User Commands 11**

add-admin-object(1)	12
add-resources(1)	14
appclient(1M)	16
asadmin(1M)	18
asant(1M)	20
asmigrate(1m)	22
asupgrade(1m)	26
capture-schema(1m)	28
create-acl(1)	29
create-admin-object(1)	30
create-audit-module(1)	32
create-authdb(1)	34
create-auth-realm(1)	36
create-connector-connection-pool(1)	38
create-connector-resource(1)	41
create-connector-security-map(1)	43
create-custom-resource(1)	45
create-domain(1)	47
create-file-user(1)	49
create-http-listener(1)	51
create-http-qos(1)	53
create-iiop-listener(1)	55
create-instance(1)	57

create-javamail-resource(1) 59  
create-jdbc-connection-pool(1) 61  
create-jdbc-resource(1) 65  
create-jmsdest(1) 67  
create-jmsobj(1) 69  
create-jms-resource(1) 70  
create-jndi-resource(1) 72  
create-jvm-options(1) 74  
create-lifecycle-module(1) 76  
create-mime(1) 78  
create-persistence-resource(1) 79  
create-profiler(1) 81  
create-resource-adapter-config(1) 83  
create-ssl(1) 85  
create-threadpool(1) 87  
create-virtual-server(1) 89  
delete-acl(1) 91  
delete-admin-object(1) 92  
delete-audit-module(1) 93  
delete-authdb(1) 94  
delete-auth-realm(1) 95  
delete-connector-connection-pool(1) 96  
delete-connector-resource(1) 98  
delete-connector-security-map(1) 99  
delete-custom-resource(1) 101  
delete-domain(1) 102  
delete-file-user(1) 103  
delete-http-listener(1) 105  
delete-http-qos(1) 106  
delete-iiop-listener(1) 107  
delete-instance(1) 108  
delete-javamail-resource(1) 110  
delete-jdbc-connection-pool(1) 111  
delete-jdbc-resource(1) 113  
delete-jmsdest(1) 114  
delete-jmsobj(1) 115  
delete-jms-resource(1) 116  
delete-jndi-resource(1) 117

delete-jvm-options(1) 118  
delete-lifecycle-module(1) 120  
delete-mime(1) 121  
delete-persistence-resource(1) 122  
delete-profiler(1) 123  
delete-resource-adapter-config(1) 124  
delete-ssl(1) 125  
delete-threadpool(1) 127  
delete-virtual-server(1) 128  
deploy(1) 129  
deploydir(1) 133  
deploytool(1m) 136  
disable(1) 137  
display-license(1) 138  
enable(1) 139  
export(1) 140  
freeze-transaction-service(1) 141  
get(1) 142  
get-client-stubs(1) 144  
help(1) 145  
install-license(1) 150  
jms-ping(1) 151  
jspc(1M) 152  
list(1) 154  
list-acls(1) 157  
list-admin-objects(1) 158  
list-audit-modules(1) 159  
list-authdbs(1) 160  
list-auth-realms(1) 161  
list-components(1) 162  
list-connector-connection-pools(1) 163  
list-connector-resources(1) 164  
list-connector-security-maps(1) 165  
list-custom-resources(1) 167  
list-domains(1) 168  
list-file-groups(1) 169  
list-file-users(1) 171  
list-http-listeners(1) 172

list-iiop-listeners(1) 173  
 list-instances(1) 174  
 list-javamail-resources(1) 175  
 list-jdbc-connection-pools(1) 176  
 list-jdbc-resources(1) 177  
 list-jmsdest(1) 178  
 list-jmsobj(1) 179  
 list-jms-resources(1) 180  
 list-jndi-resources(1) 182  
 list-lifecycle-modules(1) 183  
 list-mimes(1) 184  
 list-persistence-resources(1) 185  
 list-profiler(1) 186  
 list-profilers(1) 187  
 list-resource-adapter-configs(1) 188  
 list-sub-components(1) 190  
 list-threadpools(1) 191  
 list-virtual-servers(1) 192  
 multimode(1) 193  
 package-appclient(1M) 194  
 ping-connection-pool(1) 196  
 reconfig(1) 198  
 restart-instance(1) 200  
 rollback-transaction(1) 202  
 set(1) 203  
 show-component-status(1) 204  
 shutdown(1) 205  
 start-appserv(1) 206  
 start-domain(1) 207  
 start-instance(1) 208  
 stop-appserv(1) 210  
 stop-domain(1) 211  
 stop-instance(1) 212  
 undeploy(1) 214  
 unfreeze-transaction-service(1) 216  
 unset(1) 217  
 update-connector-security-map(1) 218  
 update-file-user(1) 220

verifier(1M)	222
verify-domain-xml(1)	223
version(1)	224
wscompile(1M)	226
wsdeploy(1M)	230

<b>Index</b>	<b>233</b>
--------------	------------





# Preface

---

Both novice users and those familiar with the SunOS operating system can use online man pages to obtain information about the system and its features. A man page is intended to answer concisely the question “What does it do?” The man pages in general comprise a reference manual. They are not intended to be a tutorial.

---

## Overview

The following contains a brief description of each man page section and the information it references:

- Section 1 describes, in alphabetical order, the `asadmin` utility commands.
- Section 1M describes all the other Application Server utility commands.

Below is a generic format for man pages. The man pages of each manual section generally follow this order, but include only needed headings. For example, if there are no bugs to report, there is no BUGS section.

NAME	This section gives the names of the commands or functions documented, followed by a brief description of what they do.
SYNOPSIS	This section shows the syntax of commands or functions.  The following special characters are used in this section:  [ ] Brackets. The option or argument enclosed in these brackets is optional. If the brackets are omitted, the argument must be specified.

		Separator. Only one of the arguments separated by this character can be specified at a time.
DESCRIPTION		This section defines the functionality and behavior of the service. Thus it describes concisely what the command does. It does not discuss OPTIONS or cite EXAMPLES. Interactive commands, subcommands, requests, macros, and functions are described under USAGE.
OPTIONS		This section lists the command options with a concise summary of what each option does. The options are listed literally and in the order they appear in the SYNOPSIS section. Possible arguments to options are discussed under the option, and where appropriate, default values are supplied.
OPERANDS		This section lists the command operands and describes how they affect the actions of the command.
EXAMPLES		This section provides examples of usage or of how to use a command or function. Wherever possible a complete example including command-line entry and machine response is shown. Whenever an example is given, the prompt is shown as <code>example%</code> , or if the user must be superuser, <code>example#</code> . Examples are followed by explanations, variable substitution rules, or returned values. Most examples illustrate concepts from the SYNOPSIS, DESCRIPTION, OPTIONS, and USAGE sections.
EXIT STATUS		This section lists the values the command returns to the calling program or shell and the conditions that cause these values to be returned. Usually, zero is returned for successful completion, and values other than zero for various error conditions.
SEE ALSO		This section lists references to other man pages, in-house documentation, and outside publications.
NOTES		This section lists additional information that does not belong anywhere else on the page. It takes the form of an aside to the user, covering points of special interest. Critical information is never covered here.
BUGS		This section describes known bugs and, wherever possible, suggests workarounds.

# User Commands

---

## add-admin-object(1)

<b>NAME</b>	add-admin-object – adds the administered object with the specified JNDI name																		
<b>SYNOPSIS</b>	<pre><b>add-admin-object</b> --user <i>admin_user</i> [--password <i>admin_password</i>] [   --host <i>localhost</i>] [--port <b>4848</b>] [--passwordfile <i>filename</i>] [   --secure -s] --aorestype <i>admin_object_type</i>   [--property <i>name=value[:name=value]*</i>] --raname <i>rar_filename</i>   <i>jndi_name</i></pre>																		
<b>DESCRIPTION</b>	Creates an administered object corresponding to a resource adapter. The ra.xml file can be found in the META-INF directory of the resource adapter archive. After a .RAR file is deployed to the application server, it gets extracted and a directory corresponding to the .RAR name is created under \$INSTANCE_ROOT/applications/j2ee-modules (or j2ee-apps). You can find the ra.xml in the META-INF subdirectory of the RAR's directory.																		
<b>OPTIONS</b>	<table><tr><td>--user</td><td>administrative user associated for the instance.</td></tr><tr><td>--password</td><td>administrative password corresponding to the administrative user.</td></tr><tr><td>--host</td><td>host name of the machine hosting the administrative instance.</td></tr><tr><td>--port</td><td>administrative port number associated with the administrative host.</td></tr><tr><td>--secure</td><td>indicates communication with the administrative instance in secured mode.</td></tr><tr><td>--passwordfile</td><td>file containing passwords appropriate for the command (e.g., administrative instance).</td></tr><tr><td>--aorestype</td><td>administered object resource type as defined by the resource adapter in the ra.xml file.</td></tr><tr><td>--property</td><td>optional attributes name/value pairs for configuring the resource.</td></tr><tr><td>--raname</td><td>name of the resource adapter.</td></tr></table>	--user	administrative user associated for the instance.	--password	administrative password corresponding to the administrative user.	--host	host name of the machine hosting the administrative instance.	--port	administrative port number associated with the administrative host.	--secure	indicates communication with the administrative instance in secured mode.	--passwordfile	file containing passwords appropriate for the command (e.g., administrative instance).	--aorestype	administered object resource type as defined by the resource adapter in the ra.xml file.	--property	optional attributes name/value pairs for configuring the resource.	--raname	name of the resource adapter.
--user	administrative user associated for the instance.																		
--password	administrative password corresponding to the administrative user.																		
--host	host name of the machine hosting the administrative instance.																		
--port	administrative port number associated with the administrative host.																		
--secure	indicates communication with the administrative instance in secured mode.																		
--passwordfile	file containing passwords appropriate for the command (e.g., administrative instance).																		
--aorestype	administered object resource type as defined by the resource adapter in the ra.xml file.																		
--property	optional attributes name/value pairs for configuring the resource.																		
--raname	name of the resource adapter.																		
<b>OPERANDS</b>	<i>jndi_name</i> JNDI name of the administered object to be added.																		
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using add-admin-object</p> <p>A JMS queue, called <code>sample_jmsqueue</code>, is assumed to have already been created using the <code>create-jmsdest</code> command.</p> <pre>asadmin&gt; add-admin-object --user admin --password adminadmin --aorestype javax.jms.Queue --property Name=sample_jmsqueue --raname jmsra jms/samplequeue Created the object</pre>																		
<b>EXIT STATUS</b>	<table><tr><td>0</td><td>command executed successfully</td></tr><tr><td>1</td><td>error in executing the command</td></tr></table>	0	command executed successfully	1	error in executing the command														
0	command executed successfully																		
1	error in executing the command																		

add-admin-object(1)

**SEE ALSO** delete-admin-object(1), list-admin-objects(1)

## add-resources(1)

<b>NAME</b>	add-resources – registers the resource in the XML file specified																		
<b>SYNOPSIS</b>	<pre><b>add-resources</b> --user <i>admin_user</i>                 [--password <i>admin_password</i>] [--host <i>localhost</i>] [--port <b>4848</b>]                 [--secure -s] [--passwordfile <i>filename</i>] [--terse=false]                 [--echo=false] [--interactive=true] <i>xml_file_path</i></pre>																		
<b>DESCRIPTION</b>	<p>Registers the named resource in the XML file specified. The <i>xml_file_path</i> is the path to the XML file containing the resources to be registered. The DOCTYPE should be specified as <i>install_dir/lib/dtds/sun-resources_1_0.dtd</i> in the <i>resources.xml</i> file.</p> <p>This command is supported in remote mode only.</p>																		
<b>OPTIONS</b>	<table><tr><td>--user</td><td>authorized domain application server administrative username.</td></tr><tr><td>--password</td><td>password to administer the domain application server.</td></tr><tr><td>--host</td><td>machine name where the domain application server is running.</td></tr><tr><td>--port</td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td>--passwordfile</td><td>file containing the domain application server password.</td></tr><tr><td>--terse</td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td></tr><tr><td>--echo</td><td>setting to true will echo the command line statement on the standard output. Default is false.</td></tr><tr><td>--interactive</td><td>if set to true (default), only the required password options are prompted.</td></tr></table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	--echo	setting to true will echo the command line statement on the standard output. Default is false.	--interactive	if set to true (default), only the required password options are prompted.
--user	authorized domain application server administrative username.																		
--password	password to administer the domain application server.																		
--host	machine name where the domain application server is running.																		
--port	port number of the domain application server listening for administration requests.																		
--secure	if true, uses SSL/TLS to communicate with the domain application server.																		
--passwordfile	file containing the domain application server password.																		
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																		
--echo	setting to true will echo the command line statement on the standard output. Default is false.																		
--interactive	if set to true (default), only the required password options are prompted.																		
<b>OPERANDS</b>	<i>xml_file_path</i> path to the XML file containing the resource(s) to be registered.																		
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using add-resources</p> <pre>asadmin&gt; add-resources --user admin --passwordfile passwords.txt --host localhost --port 4848 resource.xml Command add-resources executed successfully</pre> <p>Where: <i>resource.xml</i> is the resource file containing resources to be created.</p>																		
<b>EXIT STATUS</b>	<table><tr><td>0</td><td>command executed successfully</td></tr><tr><td>1</td><td>error in executing the command</td></tr></table>	0	command executed successfully	1	error in executing the command														
0	command executed successfully																		
1	error in executing the command																		

add-resources(1)

**SEE ALSO** | create-jdbc-connection-pool(1), create-jdbc-resource(1),  
create-jms-resource(1), create-jndi-resource(1),  
create-javamail-resource(1), create-persistence-resource(1),  
create-custom-resource(1)

## appclient(1M)

<b>NAME</b>	appclient – launches the Application Client Container and invokes the client application packaged in the application JAR file										
<b>SYNOPSIS</b>	<pre><b>appclient</b> -<b>client</b> <i>client_application_jar</i>     [-mainclass <i>client_application_main_classname</i>   -name <i>display_name</i>]     [-xml <i>sun-acc.xml file</i>] [-textauth] [-user <i>username</i>]     [-password <i>password</i>]</pre>										
<b>DESCRIPTION</b>	<p>Use the <code>appclient</code> command to launch the application client container and invoke a client application that is packaged in an application JAR file. The application client jar file is psecified and created during deployment either by the <code>deploytool</code> or by using the <code>asadmin deploy</code> command.</p> <p>The application client container is a set of java classes, libraries and other files that are required to execute a first-tier application client program on a Java Virtual Machine (JVM). The application client container communicates with the Application Server using RMI-IIOP.</p> <p>The <code>client.jar</code> that is retrieved after deploying an application , should be passed with the <code>-client</code> option while running the <code>appclient</code> utility. The <code>-mainclass</code> and <code>-name</code> options are optional for a single client application. For multiple client applications use either the <code>-classname</code> option or the- <code>name</code> option.</p>										
<b>OPTIONS</b>	<table><tr><td><code>-client</code></td><td>required; the name and location for the client application jar file. The application client JAR file is specified and created during deployment, either by the <code>deploytool</code> or by the <code>asadmin deploy</code> command.</td></tr><tr><td><code>-mainclass</code></td><td>optional; the full classname of the main client application <code>main()</code> method that will be invoked by the Application Client Container. Used for a single client application. By default, uses the class specified in the <code>client.jar</code>. The class name must be the full name. For example, <code>com.sun.test.AppClient</code></td></tr><tr><td><code>-name</code></td><td>optional; the display name for the client application. Used for multiple client applications. By default, the display name is specified in the <code>client.jar application-client.xml</code> file which is identified by the <code>display-name</code> attribute.</td></tr><tr><td><code>-xml</code></td><td>optional if using the default domain and instance, otherwise it is required; identifies the name and location of the client configuration XML file. If not specified, defaults to the value of <code>\$AS_ACC_CONFIG</code> identified in <code>asenv.conf</code> file.</td></tr><tr><td><code>-textauth</code></td><td>optional; used to specify using text format authentication when authentication is needed.</td></tr></table>	<code>-client</code>	required; the name and location for the client application jar file. The application client JAR file is specified and created during deployment, either by the <code>deploytool</code> or by the <code>asadmin deploy</code> command.	<code>-mainclass</code>	optional; the full classname of the main client application <code>main()</code> method that will be invoked by the Application Client Container. Used for a single client application. By default, uses the class specified in the <code>client.jar</code> . The class name must be the full name. For example, <code>com.sun.test.AppClient</code>	<code>-name</code>	optional; the display name for the client application. Used for multiple client applications. By default, the display name is specified in the <code>client.jar application-client.xml</code> file which is identified by the <code>display-name</code> attribute.	<code>-xml</code>	optional if using the default domain and instance, otherwise it is required; identifies the name and location of the client configuration XML file. If not specified, defaults to the value of <code>\$AS_ACC_CONFIG</code> identified in <code>asenv.conf</code> file.	<code>-textauth</code>	optional; used to specify using text format authentication when authentication is needed.
<code>-client</code>	required; the name and location for the client application jar file. The application client JAR file is specified and created during deployment, either by the <code>deploytool</code> or by the <code>asadmin deploy</code> command.										
<code>-mainclass</code>	optional; the full classname of the main client application <code>main()</code> method that will be invoked by the Application Client Container. Used for a single client application. By default, uses the class specified in the <code>client.jar</code> . The class name must be the full name. For example, <code>com.sun.test.AppClient</code>										
<code>-name</code>	optional; the display name for the client application. Used for multiple client applications. By default, the display name is specified in the <code>client.jar application-client.xml</code> file which is identified by the <code>display-name</code> attribute.										
<code>-xml</code>	optional if using the default domain and instance, otherwise it is required; identifies the name and location of the client configuration XML file. If not specified, defaults to the value of <code>\$AS_ACC_CONFIG</code> identified in <code>asenv.conf</code> file.										
<code>-textauth</code>	optional; used to specify using text format authentication when authentication is needed.										
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the <code>appclient</code> command</p> <pre><b>appclient</b> -<b>client</b> <i>appserv/bin/myclientapp.jar</i> -<b>mainclass</b> <i>com.sun.test.TestAppClient</i> -<b>xml</b> <i>sun-acc.xml</i> <i>scott sample</i></pre>										



**EXAMPLE 1** Using the `appclient` command (Continued)

Where: `appserv/bin/myclientapp.jar` is the full path for the client application .jar file, `com.sun.text.TestAppClient` is the full Java package name of the main client application, `scott` and `sample` are arguments to pass to the application, and `sun-acc.xml` is the name of the client configuration XML file. If `sun-acc.xml` is not in the current directory, you must give the absolute path location; otherwise the relative path is used. The relative path is relative to the directory where the command is being executed.

**ATTRIBUTES** See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Interface Stability	Unstable

**SEE ALSO** `package-appclient(1M)`, `asadmin(1M)`

## asadmin(1M)

<b>NAME</b>	asadmin – utility for performing administrative tasks for the Sun Java System Application Server																
<b>SYNOPSIS</b>	<b>asadmin</b> <i>subcommand</i> [- <b>short_option</b> [ <i>short_option_argument</i> ]] * [ <b>--long_option</b> [ <i>long_option_argument</i> ]] * [ <i>operand</i> ] *																
<b>DESCRIPTION</b>	<p>Use the <code>asadmin</code> utility to perform any administrative task for the Sun Java System Application Server. You can use this utility in place of using the Administrator interface.</p> <p>The <i>subcommand</i> identifies the operation or task you wish to perform. Subcommands are case-sensitive. Short option arguments have a single dash (-); while long option arguments have two dashes (--). Options modify how the utility performs a subcommand. Options are also case-sensitive. Most options require argument values except boolean options which toggle to switch a feature ON or OFF. Operands appear after the argument values, and are set off by a space, a tab, or double dashes (—). The <code>asadmin</code> utility treats anything that comes after the options and their values as an operand.</p> <p>Local subcommands can be executed without the presence of an administration server. However, it is required that the user be logged into the machine hosting the domain in order to execute the subcommand and have access (permissions) for the installation and domain directories.</p> <p>Remote subcommands are always executed by connecting to an administration server and executing the subcommand there. A running administration server is required. All remote subcommands require the following options:</p> <table><tr><td>-u --user</td><td>authorized domain application server administrative username.</td></tr><tr><td>-w --password</td><td>password to administer the domain application server.</td></tr><tr><td>-H --host</td><td>machine name where the domain application server is running.</td></tr><tr><td>-p --port</td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td>-s --secure</td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td>-t --terse</td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td></tr><tr><td>-e --echo</td><td>setting to true will echo the command line statement on the standard output. Default is false.</td></tr><tr><td>-I --interactive</td><td>if set to true (default), only the required password options are prompted.</td></tr></table>	-u --user	authorized domain application server administrative username.	-w --password	password to administer the domain application server.	-H --host	machine name where the domain application server is running.	-p --port	port number of the domain application server listening for administration requests.	-s --secure	if true, uses SSL/TLS to communicate with the domain application server.	-t --terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	-e --echo	setting to true will echo the command line statement on the standard output. Default is false.	-I --interactive	if set to true (default), only the required password options are prompted.
-u --user	authorized domain application server administrative username.																
-w --password	password to administer the domain application server.																
-H --host	machine name where the domain application server is running.																
-p --port	port number of the domain application server listening for administration requests.																
-s --secure	if true, uses SSL/TLS to communicate with the domain application server.																
-t --terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																
-e --echo	setting to true will echo the command line statement on the standard output. Default is false.																
-I --interactive	if set to true (default), only the required password options are prompted.																

For security purposes, you can set the password for a subcommand from a file instead of entering the password at the command line. The `--passwordfile` option takes the file containing the passwords. The valid contents for the file are:

```
AS_ADMIN_PASSWORD=value
AS_ADMIN_ADMINPASSWORD=value
AS_ADMIN_USERPASSWORD=value
```

Given the `--passwordfile` option and its value, the password options in the `passwordfile` are exported to the global environment; subsequent subcommands without the password options take this value. However, if both the `--password` and `--passwordfile` options are specified on the command line, the password value in the `passwordfile` is exported to the global environment and subsequent subcommands without the `--password` option would take this value. However, for the current subcommand, the `--password` option value specified on the command line is taken since the `--password` option takes precedence over the `--passwordfile` option.

To use the `--secure` option, you must use the `set` command to enable the `security-enabled` flag in the `admin http-listener` in the `domain.xml`.

When you use the `asadmin` subcommands to create and/or delete, you must restart the server for the newly created command to take affect. Use the `start-domain` command to restart the server.

To access the manpages for the J2EE 1.4 Application Server Command-line interface subcommands, add `$AS_INSTALL/man` to your `MANPATH` environment variable.

You can obtain overall usage information for any of the `asadmin` utility subcommands by invoking the `--help` option. If you specify a subcommand, the usage information for that subcommand is displayed. Using the `help` option without a subcommand displays a listing of all the available subcommands.

**ATTRIBUTES** See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Interface Stability	Unstable

**SEE ALSO** `appclient(1M)`, `package-appclient(1M)`

asant(1M)

<b>NAME</b>	asant – launches the Jakarta Ant tool																						
<b>SYNOPSIS</b>	<b>asant</b> <i>target_list</i>																						
<b>DESCRIPTION</b>	<p>Use the <code>asant</code> command to automate repetitive development and deployment tasks. <code>asant</code> is a shell script that invokes the underlying Ant infrastructure after initializing the environment to pickup the application server installed targets.</p> <p>To use Ant as part of the Sun ONE Application Server, verify that your PATH includes the provided <code>asant</code> (Solaris) <code>ant.bat</code> (Windows) script.</p> <p>The bundled sample applications use <code>asant</code> extensively; however, <code>asant</code> can be used in any development or operational environments.</p> <p>The build targets are represented in the <code>build.xml</code> files that accompany the sample applications.</p> <p>To use the Ant tool to compile and reassemble the sample applications, verify that the <code>\$AS_INSTALL/bin</code> directory is on your environment's path. On UNIX, add the <code>\$AS_INSTALL/bin</code> directory to your PATH environment variable. On Windows, after installing the Sun ONE Application Server, set the system path by adding <code>\$AS_INSTALL\bin</code> to the user PATH. You can access the PATH system variable from: Start menu, Settings, Control Panel, System, Advanced, Environment Variables, User Variables for Administrator, PATH.</p> <p>The <i>target_list</i> is one or more space separated tasks as described below.</p>																						
<b>TARGETS</b>	<table><tr><td><code>compile</code></td><td>compiles all Java source code.</td></tr><tr><td><code>jar</code></td><td>assembles the EJB JAR module.</td></tr><tr><td><code>war</code></td><td>assembles the WAR file in <code>&lt;sample_dir&gt;/assemble/war</code></td></tr><tr><td><code>ear</code></td><td>assembles the EAR file in <code>&lt;sample_dir&gt;/assemble/ear</code></td></tr><tr><td><code>core</code></td><td>(default) compiles all sources, builds stubs and skeletons; and assembles EJB JAR, WAR and EAR files. This is the default target for all <code>build.xml</code> files shipped in the Sun ONE Application Server.</td></tr><tr><td><code>javadocs</code></td><td>creates Java docs in <code>&lt;sample_dir&gt;/javadocs</code></td></tr><tr><td><code>all</code></td><td>builds core and javadocs , verifies and deploys the application, and adds the resources..</td></tr><tr><td><code>deploy</code></td><td>deploys the application and automatically expands the EJB JAR; does not install Javadocs.</td></tr><tr><td><code>undeploy</code></td><td>removes the deployed sample from the Sun ONE Application Server.</td></tr><tr><td><code>clean</code></td><td>removes <code>&lt;appname&gt;/build/</code> and <code>&lt;appname&gt;/assemble/</code> and <code>&lt;appname&gt;/javadocs</code> directories.</td></tr><tr><td><code>verify</code></td><td>verifies the deployment descriptors in the sample.</td></tr></table>	<code>compile</code>	compiles all Java source code.	<code>jar</code>	assembles the EJB JAR module.	<code>war</code>	assembles the WAR file in <code>&lt;sample_dir&gt;/assemble/war</code>	<code>ear</code>	assembles the EAR file in <code>&lt;sample_dir&gt;/assemble/ear</code>	<code>core</code>	(default) compiles all sources, builds stubs and skeletons; and assembles EJB JAR, WAR and EAR files. This is the default target for all <code>build.xml</code> files shipped in the Sun ONE Application Server.	<code>javadocs</code>	creates Java docs in <code>&lt;sample_dir&gt;/javadocs</code>	<code>all</code>	builds core and javadocs , verifies and deploys the application, and adds the resources..	<code>deploy</code>	deploys the application and automatically expands the EJB JAR; does not install Javadocs.	<code>undeploy</code>	removes the deployed sample from the Sun ONE Application Server.	<code>clean</code>	removes <code>&lt;appname&gt;/build/</code> and <code>&lt;appname&gt;/assemble/</code> and <code>&lt;appname&gt;/javadocs</code> directories.	<code>verify</code>	verifies the deployment descriptors in the sample.
<code>compile</code>	compiles all Java source code.																						
<code>jar</code>	assembles the EJB JAR module.																						
<code>war</code>	assembles the WAR file in <code>&lt;sample_dir&gt;/assemble/war</code>																						
<code>ear</code>	assembles the EAR file in <code>&lt;sample_dir&gt;/assemble/ear</code>																						
<code>core</code>	(default) compiles all sources, builds stubs and skeletons; and assembles EJB JAR, WAR and EAR files. This is the default target for all <code>build.xml</code> files shipped in the Sun ONE Application Server.																						
<code>javadocs</code>	creates Java docs in <code>&lt;sample_dir&gt;/javadocs</code>																						
<code>all</code>	builds core and javadocs , verifies and deploys the application, and adds the resources..																						
<code>deploy</code>	deploys the application and automatically expands the EJB JAR; does not install Javadocs.																						
<code>undeploy</code>	removes the deployed sample from the Sun ONE Application Server.																						
<code>clean</code>	removes <code>&lt;appname&gt;/build/</code> and <code>&lt;appname&gt;/assemble/</code> and <code>&lt;appname&gt;/javadocs</code> directories.																						
<code>verify</code>	verifies the deployment descriptors in the sample.																						

**EXAMPLES****EXAMPLE 1** Compiling and Assembling a Sample Application

Using the simple stateless EJB sample as an example, execute several of the build targets as follows:

```
cd install_root/samples/ejb/stateless/simple/src
```

Execute the `compile` target to compile the Java sources as follows:

```
asant compile
```

Execute the `war`, `ear`, and `ejbjar` target to assemble the J2EE module files and the EAR file as follows by:

```
asant jar
asant war
asant ear
```

Alternatively, all the above tasks can be accomplished by:

```
asant core
```

Since the default build target is `core` you can execute `asant` without any arguments to rebuild the entire application.

**EXAMPLE 2** Building Web-based Applications

You can build everything, including installing Javadocs, and deploying the application by:

```
asant all
```

Additionally, you can build everything, except the Javadocs, but deploy the application by:

```
asant core
or just,
asant
then,
asant deploy
```

To rebuild the `ear` after you have modified the deployment descriptors without recompiling:

```
asant ear
asant deploy
```

**SEE ALSO**

Apache Software Foundation at <http://www.apache.org>, Jakarta Ant documentation at <http://jakarta.apache.org/ant/index.html>.

SUNWant documentation located in `/usr/sfw/share/doc/ant`

, `asadmin(1M)`

## asmigrate(1m)

**NAME** asmigrate – automates migration of J2EE applications from other J2EE platforms to Sun Java System Application Server

**SYNOPSIS** `asmigrate [-h | --help ] [-v | --version ] [(-c | --commandline) | (-u --ui ) ] [-q | --quiet ] [-d | --debug ] [-s | --sourcedirectory source_directory] [-S | --sourceserver source_application_server] [-t | --targetdirectory target_directory] [-T | --targetserver target_application_server] [-n | --scan-native-apis-only ] [-p | --scan-packages package_list] [-j | --java2db create-tables=true, drop-tables=true, db-vendor-name=dbVendorName] [-m | --migrate-cmp comment-pk-modifiers=true, overwrite-conflicting-accessors=true] [-f | --file-filter all-files=true, html-files=true, java-files=true, jsp-files=true, xml-files=true, archive-files=true] [-a | --append-logs ] [operands]`

**DESCRIPTION** Use the `asmigrate` utility to analyze your J2EE application and translate vendor specific settings to Sun Java™ System Application Server specific settings making the application deployable on Sun's J2EE products.

The following table identifies the supported J2EE product migrations:

Source J2EE Platform	Destination J2EE Platform
WebSphere Application Server 4.0	Sun ONE Application Server 6.5
WebLogic Application Server 5.1	
WebLogic Application Server 5.1, 6.0, 6.1	Sun ONE Application Server 7
WebSphere Application Server 4.0	
Java™ 2 Platform Enterprise Edition 1.3	
Sun ONE Application Server 6.x	
Sun ONE Web Server 6.0	
JBoss Application Server 3.0	
Tomcat Web Server 4.1.12	

Source J2EE Platform	Destination J2EE Platform
WebLogic Application Server 5.1, 6.0, 6.1 WebSphere Application Server 4.0 JavaTM™ 2 Platform Enterprise Edition 1.3/1.4 Sun ONE Application Server 6.x Sun ONE Web Server 6.0 JBoss Application Server 3.0 Tomcat Web Server 4.1.12	JavaTM™ 2 Platform, Enterprise Edition 1.4 Application Server
WebLogic Application Server 5.1, 6.0, 6.1 WebSphere Application Server 4.0 JavaTM™ 2 Platform Enterprise Edition 1.3/1.4 Sun ONE Application Server 6.x Sun ONE Web Server 6.0 JBoss Application Server 3.0 JBoss Application Server 3.2 Tomcat Web Server 4.1.12	Sun JavaTM™ System Application Server Platform Edition 8

**OPTIONS**

-h --help	displays the arguments for launching the MigrationTool.
-v --version	displays the version of the MigrationTool.
-u --ui	invokes the tool in user interface mode.
-c --commandline	invokes the tool in command-line mode.
-q --quiet	launches the tool in quiet mode.
-d --debug	launches the tool in debug mode.
-s --sourcedirectory	identifies the directory where the source code to migrate or scan is present.
-S --sourceserver	identifies the source application server of the applications to be migrated. Possible servers include: <ul style="list-style-type: none"> <li>■ wl51: WebLogic Application Server 5.1</li> <li>■ wl60: WebLogic Application Server 6.0</li> <li>■ wl61: WebLogic Application Server 6.1</li> <li>■ as65: Sun ONE Application Server 6.5</li> <li>■ as70: Sun ONE Application Server 7.0</li> </ul>

## asmigrate(1m)

	<ul style="list-style-type: none"><li>■ ws40: WebSphere Application Server 4.0</li><li>■ ri13: JavaTM™ 2 Platform Enterprise Edition 1.3</li><li>■ ri14: JavaTM™ 2 Platform Enterprise Edition 1.3</li><li>■ s1ws: Sun ONE Web Server</li><li>■ jb30: JBoss Application Server 3.0</li><li>■ tc41: Tomcat Application Server 4.1</li></ul>
-t --targetdirectory	target or output directory where the migrated application should be placed.
-T --targetserver	target application server to which the application is to be migrated.
-n --scan-native-apis-only	scans the source code only for the presence of application server specific proprietary APIs.
-p --scan-packages	comma-separated list of Java packages to scan.
-j --java2db	bypasses the creation of the <code>sun-cmp-mapping.xml</code> file. Instead, introduces the option argument into the <code>sun-ejb-jar.xml</code> file. Option arguments are: <ul style="list-style-type: none"><li>■ create-tables: if set to true (default), creates tables at deploy. If set to false tables are not created.</li><li>■ drop-tables: if set to true (default), tables are dropped at undeploy. If set to false tables are not dropped.</li><li>■ db-vendor-name: name of the database vendor for the application to be migrated. Supported vendor names include: Oracle, Sybase, DB2, Generic SQL92, PointBase, MSSQL.</li></ul>
-m --migrate-cmp	migrates 1.1 compliant CMPs, if any, to 2.0. Option arguments are: <ul style="list-style-type: none"><li>■ overwrite-conflicting-accessors: if set to true (default), conflicting accessors are overwritten. If set to false, conflicting accessors are not overwritten.</li><li>■ comment-pk-modifiers: if set to true (default), setters of primary key are commented. If set to false, setters of primary key are not commented.</li></ul>
-f --file-filter	selects the type of files to migrate. Option arguments are:



## asmigrate(1m)

- all-files: if specified and set to true (default), migrates all types of files.
- html-files: if specified and set to true (default), migrates HTML files.
- java-files: if specified and set to true (default), migrates Java files.
- jsp-files: if specified and set to true (default), migrates JSP type files.
- archive-files: if specified and set to true (default), migrates jar/ear/war/rar file types.

-a --append-logs

if specified, appends the logging to the existing or previous logs without overwriting them. If not specified, previous logs are overwritten.

operands

identifies the archive file (jar/ear/war/rar) to be migrated.

**SEE ALSO** asupgrade(1M)

## asupgrade(1m)

<b>NAME</b>	asupgrade – migrates the configuration of a previously installed Sun Java System Application Server
<b>SYNOPSIS</b>	<pre>asupgrade [-c   --console ] [-V --version ] [-h   --help ] -s     -source applicationserver7.x_installation   -t --target applicationserver8.x_installation [-d   --domain domain_name   -n   --nsspwdfile NSS_password_filepath -j     --jkspwdfile JKS_password_filepath -p     --capwdfile CA_password_filepath]</pre>
<b>DESCRIPTION</b>	<p>Use the asupgrade utility to migrate the server configuration and its persisted state, J2EE services, and deployed J2EE applications. The configuration of an installed Sun Java System Application Server 7 is migrated to the Sun Java System Application Server 8 Application Server installation. If the domain contains information about a deployed application and the installed application components do not agree with the configuration information, the configuration is migrated as is without any attempt to reconfigure the incorrect configurations.</p> <p>asupgrade migrates the configuration and deployed applications of a previous version of the Application Server; however, the runtime binaries of the server are not updated. Database migrations or conversions are beyond the scope of the asupgrade command.</p> <p>Only those instances that do not use the Sun Java System Web Server specific features will be upgraded seamlessly. Configuration files related to HTTP path, CGI bin, SHTML, and NSAPI plugins will not be upgraded.</p> <p>The upgrade process can also be initiated automatically at installation time using the Upgrade checkbox in the Application Server installer. After completion of the upgrade, use the Application Server 7 Uninstaller to remove the previous version of the Application Server.</p> <p>Application archives (.ear) and component archives (.jar, .war, .rar) that are deployed in the Application Server 7 environment do not require any modification to run on Application Server 8. However applications and components deployed in the source server are repackaged into new J2EE archives in the target server's autodeploy directory and are deployed upon server startup. Applications that do not deploy successfully, must use Migrationtool (asmigrate) on the application and then manually redeploy the application.</p> <p>You must specify the source and target directories for the upgrade. If the upgrade includes certificates, you must also provide the passwords for the source PKCS12 file and the target JKS keyfile for each domain that contains certificates to be migrated. Since Application Server 7 uses a different certificate store format (NSS) than Application Server 8 (JSSE), the migration keys and certificates are converted to the new format. Upon successful upgrade, an upgrate report is generated listing successfully migrated items along with a list of the items that could not be migrated.</p>
<b>OPTIONS</b>	<pre>-c --console          launches the upgrade command line utility.</pre>

- V--version            displays the version of the UpgradeTool.
- h--help               displays the arguments for launching the UpgradeTool.
- s--source             identifies the installation directory for Sun Java System Application Server 7.
- t--target             identifies the installation directory for Sun Java System Application Server 8.
- d--domain             identifies the destination domain name for the migrated certificates.
- n--nsspwdfile        identifies the path to the NSS password file.
- j--jkspwdfile        identifies the path to the JKS password file.
- p--capwdfile         identifies the path to the CA certificate password file.

**EXAMPLES**    **EXAMPLE 1** Using asupgrade

```
example% upgrade -s /home/sunas7 -t /home/sunas8
```

**SEE ALSO**    asmigrate(1M)

## capture-schema(1m)

<b>NAME</b>	capture-schema – stores the database metadata (schema) in a file for use in mapping and execution														
<b>SYNOPSIS</b>	<b>capture-schema</b> <b>-dburl</b> <i>url</i> <b>-username</b> <i>name</i> <b>-password</b> <i>password</i> <b>-driver</b> <i>a_jdbc_driver</i> [-schemaname <i>name</i> ] [-table <i>tablename</i> ] * [-out <i>filename</i> ]														
<b>DESCRIPTION</b>	Stores the database metadata (schema) in a file. You can also use the Sun Java System Studio IDE to capture the database schema. Run <code>capture-schema</code> as the same database user that owns the tables, so that the <code>-username</code> and <code>-schemaname</code> options are given the same username. Additionally, you can grant the database user running the <code>capture-schema</code> command the ANALYZE ANY TABLE privilege.														
<b>OPTIONS</b>	<table><tr><td><code>-dburl</code></td><td>JDBC URL expected by the driver for accessing a database.</td></tr><tr><td><code>-username</code></td><td>user name for authenticating access to a database.</td></tr><tr><td><code>-password</code></td><td>password for accessing the selected database.</td></tr><tr><td><code>-driver</code></td><td>JDBC driver classname in your CLASSPATH.</td></tr><tr><td><code>-schemaname</code></td><td>name of the user schema being captured. If not specified, the default will capture metadata for all tables from all the schemas accessible to this user. Specifying this parameter is highly recommended. If more than one schema is accessible to this user, more than one table with the same name may be captured which will cause problems.</td></tr><tr><td><code>-table</code></td><td>name of the table; multiple table names can be specified.</td></tr><tr><td><code>-out</code></td><td>output target; defaults to <code>stdout</code>. This parameter corresponds to the <code>schema</code> sub-element of the <code>sun-cmp-mapping</code> element in the <code>sun-cmp-mapping_1_1.dtd</code> file.</td></tr></table>	<code>-dburl</code>	JDBC URL expected by the driver for accessing a database.	<code>-username</code>	user name for authenticating access to a database.	<code>-password</code>	password for accessing the selected database.	<code>-driver</code>	JDBC driver classname in your CLASSPATH.	<code>-schemaname</code>	name of the user schema being captured. If not specified, the default will capture metadata for all tables from all the schemas accessible to this user. Specifying this parameter is highly recommended. If more than one schema is accessible to this user, more than one table with the same name may be captured which will cause problems.	<code>-table</code>	name of the table; multiple table names can be specified.	<code>-out</code>	output target; defaults to <code>stdout</code> . This parameter corresponds to the <code>schema</code> sub-element of the <code>sun-cmp-mapping</code> element in the <code>sun-cmp-mapping_1_1.dtd</code> file.
<code>-dburl</code>	JDBC URL expected by the driver for accessing a database.														
<code>-username</code>	user name for authenticating access to a database.														
<code>-password</code>	password for accessing the selected database.														
<code>-driver</code>	JDBC driver classname in your CLASSPATH.														
<code>-schemaname</code>	name of the user schema being captured. If not specified, the default will capture metadata for all tables from all the schemas accessible to this user. Specifying this parameter is highly recommended. If more than one schema is accessible to this user, more than one table with the same name may be captured which will cause problems.														
<code>-table</code>	name of the table; multiple table names can be specified.														
<code>-out</code>	output target; defaults to <code>stdout</code> . This parameter corresponds to the <code>schema</code> sub-element of the <code>sun-cmp-mapping</code> element in the <code>sun-cmp-mapping_1_1.dtd</code> file.														
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using capture-schema <pre>capture-schema -dburl jdbc:oracle:thin:@sadbuttrue:1521:ora817 -schemaname cantiflas -username CANTIFLAS -password enigma -driver oracle.jdbc.driver.OracleDriver</pre>														
<b>SEE ALSO</b>	asadmin(1M)														

<b>NAME</b>	create-acl – adds a new access control list file for the named instance
<b>SYNOPSIS</b>	<pre> <b>create-acl</b>   --user <i>admin_user</i> [--password <i>admin_password</i>] [--host <i>localhost</i>]   [--port <b>4848</b>] [--passwordfile <i>filename</i>] [--secure -s] [--instance   <i>instance_name</i>] --aclfile <i>filename</i> <i>acl_ID</i> </pre>
<b>DESCRIPTION</b>	Gets the access control lists associated with the named server instance.
<b>OPTIONS</b>	<pre> --user          administrative user associated for the instance. --password      administrative password corresponding to the administrative                 user. --host          host name of the machine hosting the administrative instance. --port          administrative port number associated with the administrative                 host. --secure        indicates communication with the administrative instance in                 secured mode. --passwordfile  file containing passwords appropriate for the command (e.g.,                 administrative instance). --instance      name of the instance. --aclfile       name of the default acl file. </pre>
<b>OPERANDS</b>	<i>acl_ID</i> internal name for the ACL file listing. This ID is used in a virtual server element to define the ACL file used by the virtual server.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using create-acl</p> <pre> asadmin&gt; create-acl --user admin --password adminadmin --host fuyako --port 7070 --instance server Created ACL with id=sampleACL </pre> <p>Where: <i>sampleACL</i> is the name of the ACL created.</p>
<b>EXIT STATUS</b>	<pre> 0    command executed successfully 1    error in executing the command </pre>
<b>INTERFACE EQUIVALENT</b>	Access Control List page
<b>SEE ALSO</b>	delete-acl(1), list-acl(1)

## create-admin-object(1)

<b>NAME</b>	create-admin-object – adds the administered object with the specified JNDI name																				
<b>SYNOPSIS</b>	<pre>create-admin-object --user admin_user [--password admin_password]   [--host localhost] [--port 4848] [--secure -s]   [--passwordfile filename] [--terse=false] [--echo=false]   [--interactive=true] --restype aorestype   --raname resource_adapter_name [--enabled=true]   [--description description] [--property name=value[:name=value]*]   jndi_name</pre>																				
<b>DESCRIPTION</b>	<p>Creates an administered object specific to the Enterprise Information Server (typically a messaging provider) with the JNDI name provided. The resource adapter exposes the administered object as a Javabeen. Application programs can lookup the administered object using the JNDI name, and use it using messaging style specific APIs.</p> <p>Before you can create an administered object, you must first deploy the resource adapter and specify it using the <code>--raname</code> option. This command is supported in remote mode only.</p>																				
<b>OPTIONS</b>	<table><tr><td><code>--user</code></td><td>authorized domain application server administrative username.</td></tr><tr><td><code>--password</code></td><td>password to administer the domain application server.</td></tr><tr><td><code>--host</code></td><td>machine name where the domain application server is running.</td></tr><tr><td><code>--port</code></td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td><code>--secure</code></td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td><code>--passwordfile</code></td><td>file containing the domain application server password.</td></tr><tr><td><code>--terse</code></td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td></tr><tr><td><code>--echo</code></td><td>setting to true will echo the command line statement on the standard output. Default is false.</td></tr><tr><td><code>--interactive</code></td><td>if set to true (default), only the required password options are prompted.</td></tr><tr><td><code>--restype</code></td><td>administered object resource type as defined by the resource adapter in the <code>ra.xml</code> file. This is the same value found in the <code>adminobject-interface</code> elements in the deployment descriptor of a resource adapter (<code>ra.xml</code>).</td></tr></table>	<code>--user</code>	authorized domain application server administrative username.	<code>--password</code>	password to administer the domain application server.	<code>--host</code>	machine name where the domain application server is running.	<code>--port</code>	port number of the domain application server listening for administration requests.	<code>--secure</code>	if true, uses SSL/TLS to communicate with the domain application server.	<code>--passwordfile</code>	file containing the domain application server password.	<code>--terse</code>	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	<code>--echo</code>	setting to true will echo the command line statement on the standard output. Default is false.	<code>--interactive</code>	if set to true (default), only the required password options are prompted.	<code>--restype</code>	administered object resource type as defined by the resource adapter in the <code>ra.xml</code> file. This is the same value found in the <code>adminobject-interface</code> elements in the deployment descriptor of a resource adapter ( <code>ra.xml</code> ).
<code>--user</code>	authorized domain application server administrative username.																				
<code>--password</code>	password to administer the domain application server.																				
<code>--host</code>	machine name where the domain application server is running.																				
<code>--port</code>	port number of the domain application server listening for administration requests.																				
<code>--secure</code>	if true, uses SSL/TLS to communicate with the domain application server.																				
<code>--passwordfile</code>	file containing the domain application server password.																				
<code>--terse</code>	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																				
<code>--echo</code>	setting to true will echo the command line statement on the standard output. Default is false.																				
<code>--interactive</code>	if set to true (default), only the required password options are prompted.																				
<code>--restype</code>	administered object resource type as defined by the resource adapter in the <code>ra.xml</code> file. This is the same value found in the <code>adminobject-interface</code> elements in the deployment descriptor of a resource adapter ( <code>ra.xml</code> ).																				

## create-admin-object(1)

`--raname` module name of the deployed resource adapter. In case of a resource adapter that is embedded in an application, the raname will be appname#raname.

`--enabled` determines whether the resource is enabled at runtime.

`--description` text description of the connection pool.

`--property` name/value pair of the properties of admin object java bean. admin object java bean is specified by the `adminobject-class` in the resource adapter's deployment descriptor (`ra.xml`).

**OPERANDS** *jndi\_name* JNDI name of the administered object to be created.

**EXAMPLES** **EXAMPLE 1** Using create-admin-object

The `javax.jms.Queue` resource type is obtained from the `rar.xml` file. The `jmsra` must be deployed prior to executing this command.

```
asadmin> create-admin-object --user admin1 --password adminadmin1
--restype javax.jms.Queue --raname jmsra --property Name=sample_jmsqueue jms/samplequeue
Command create-admin-object executed successfully
```

**EXIT STATUS** 0 command executed successfully

1 error in executing the command

**SEE ALSO** `delete-admin-object(1)`, `list-admin-objects(1)`

## create-audit-module(1)

<b>NAME</b>	create-audit-module – adds an audit-module																						
<b>SYNOPSIS</b>	<pre>create-audit-module --user <i>admin_user</i> [--password <i>admin_password</i>]   [--host <i>localhost</i>] [--port <i>4848</i>] [--secure -s]   [--passwordfile <i>filename</i>] [--terse=false] [--echo=false]   [--interactive=true] --classname <i>realm_class</i>   [--property (name=value)[:name=value]*] <i>audit_module_name</i></pre>																						
<b>DESCRIPTION</b>	Adds the named audit module for the plugin module that implements the audit capabilities. This command is supported in remote mode only.																						
<b>OPTIONS</b>	<table><tr><td>--user</td><td>authorized domain application server administrative username.</td></tr><tr><td>--password</td><td>password to administer the domain application server.</td></tr><tr><td>--host</td><td>machine name where the domain application server is running.</td></tr><tr><td>--port</td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td>--passwordfile</td><td>file containing the domain application server password.</td></tr><tr><td>--terse</td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td></tr><tr><td>--echo</td><td>setting to true will echo the command line statement on the standard output. Default is false.</td></tr><tr><td>--interactive</td><td>if set to true (default), only the required password options are prompted.</td></tr><tr><td>--classname</td><td>Java class which implements this realm.</td></tr><tr><td>--property</td><td>optional attributes name/value pairs of provider implementation specific attributes.</td></tr></table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	--echo	setting to true will echo the command line statement on the standard output. Default is false.	--interactive	if set to true (default), only the required password options are prompted.	--classname	Java class which implements this realm.	--property	optional attributes name/value pairs of provider implementation specific attributes.
--user	authorized domain application server administrative username.																						
--password	password to administer the domain application server.																						
--host	machine name where the domain application server is running.																						
--port	port number of the domain application server listening for administration requests.																						
--secure	if true, uses SSL/TLS to communicate with the domain application server.																						
--passwordfile	file containing the domain application server password.																						
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																						
--echo	setting to true will echo the command line statement on the standard output. Default is false.																						
--interactive	if set to true (default), only the required password options are prompted.																						
--classname	Java class which implements this realm.																						
--property	optional attributes name/value pairs of provider implementation specific attributes.																						
<b>OPERANDS</b>	<i>audit_module_name</i> name of this audit module.																						
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using create-audit-module</p> <pre>asadmin&gt; create-audit-module --user admin1 --password adminadmin1 --host pigeon --port 5001 --classname com.sun.appserv.auditmodule --property defaultuser=admin:Password=admin sampleAuditModule Command create-audit-module executed successfully</pre>																						
<b>EXIT STATUS</b>	<table><tr><td>0</td><td>command executed successfully</td></tr><tr><td>1</td><td>error in executing the command</td></tr></table>	0	command executed successfully	1	error in executing the command																		
0	command executed successfully																						
1	error in executing the command																						



create-audit-module(1)

**SEE ALSO** delete-audit-module(1), list-audit-modules(1)

## create-authdb(1)

<b>NAME</b>	create-authdb – adds the new authorized database for the named instance																						
<b>SYNOPSIS</b>	<pre><b>create-authdb</b>   --user <i>admin_user</i> [--password <i>admin_password</i>] [--host <i>localhost</i>]   [--port <b>4848</b>] [--passwordfile <i>filename</i>] [--secure   -s] [--instance <i>instance_name</i>] --database <i>database</i> --virtualserver <i>virtualserver_ID</i> [--basedn <i>basedn</i>] [--certmaps <i>certmaps</i>] <i>authdb_ID</i></pre>																						
<b>DESCRIPTION</b>	Adds the named authorized database associated with the named server instance.																						
<b>OPTIONS</b>	<table><tr><td>--user</td><td>administrative user associated for the instance.</td></tr><tr><td>--password</td><td>administrative password corresponding to the administrative user.</td></tr><tr><td>--host</td><td>host name of the machine hosting the administrative instance.</td></tr><tr><td>--port</td><td>administrative port number associated with the administrative host.</td></tr><tr><td>--passwordfile</td><td>file containing passwords appropriate for the command (e.g., administrative instance).</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the administrative instance.</td></tr><tr><td>--instance</td><td>name of the instance.</td></tr><tr><td>--database</td><td>user database name in the <code>dbswitch.conf</code> file.</td></tr><tr><td>--virtualserver</td><td>virtual server ID. It can also be referred to as the variable <code>\$id</code> in an <code>obj.conf</code> file. A virtual server ID cannot begin with a number.</td></tr><tr><td>--basedn</td><td>overrides the base DN lookup in the <code>dbswitch.conf</code> file. However, the <code>basedn</code> value is still relative to the base DN value from the <code>dbswitch.conf</code> entry.</td></tr><tr><td>--certmaps</td><td>certificate to LDAP entry mappings as defined in the <code>certm.conf</code> file. If not present, all mappings are used. All lookups are based on mappings in the <code>certmap.conf</code> file and are relative to the final base distinguished name (DN) of the virtual server.</td></tr></table>	--user	administrative user associated for the instance.	--password	administrative password corresponding to the administrative user.	--host	host name of the machine hosting the administrative instance.	--port	administrative port number associated with the administrative host.	--passwordfile	file containing passwords appropriate for the command (e.g., administrative instance).	--secure	if true, uses SSL/TLS to communicate with the administrative instance.	--instance	name of the instance.	--database	user database name in the <code>dbswitch.conf</code> file.	--virtualserver	virtual server ID. It can also be referred to as the variable <code>\$id</code> in an <code>obj.conf</code> file. A virtual server ID cannot begin with a number.	--basedn	overrides the base DN lookup in the <code>dbswitch.conf</code> file. However, the <code>basedn</code> value is still relative to the base DN value from the <code>dbswitch.conf</code> entry.	--certmaps	certificate to LDAP entry mappings as defined in the <code>certm.conf</code> file. If not present, all mappings are used. All lookups are based on mappings in the <code>certmap.conf</code> file and are relative to the final base distinguished name (DN) of the virtual server.
--user	administrative user associated for the instance.																						
--password	administrative password corresponding to the administrative user.																						
--host	host name of the machine hosting the administrative instance.																						
--port	administrative port number associated with the administrative host.																						
--passwordfile	file containing passwords appropriate for the command (e.g., administrative instance).																						
--secure	if true, uses SSL/TLS to communicate with the administrative instance.																						
--instance	name of the instance.																						
--database	user database name in the <code>dbswitch.conf</code> file.																						
--virtualserver	virtual server ID. It can also be referred to as the variable <code>\$id</code> in an <code>obj.conf</code> file. A virtual server ID cannot begin with a number.																						
--basedn	overrides the base DN lookup in the <code>dbswitch.conf</code> file. However, the <code>basedn</code> value is still relative to the base DN value from the <code>dbswitch.conf</code> entry.																						
--certmaps	certificate to LDAP entry mappings as defined in the <code>certm.conf</code> file. If not present, all mappings are used. All lookups are based on mappings in the <code>certmap.conf</code> file and are relative to the final base distinguished name (DN) of the virtual server.																						
<b>OPERANDS</b>	<i>authdb_id</i> user database name in the virtual server's ACL file.																						
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using create-authdb</p> <pre>asadmin&gt; create-authdb --user admin --password adminadmin --host fuyako --port 7070 --database defa Created AuthDB with id = sampleAuth</pre> <p>Where <code>sampleAuth</code> is the authdb created.</p>																						
<b>EXIT STATUS</b>	0 command executed successfully																						

create-authdb(1)

1 error in executing the command

**INTERFACE**  
**EQUIVALENT**  
**SEE ALSO**

unknown

delete-authdb(1), list-authdbs(1)

## create-auth-realm(1)

<b>NAME</b>	create-auth-realm – adds the new authorized realm																						
<b>SYNOPSIS</b>	<pre>create-auth-realm --user admin_user [--password admin_password]   [--host localhost] [--port 4848] [--secure -s]   [--passwordfile filename] [--terse=false] [--echo=false]   [--interactive=true] --classname realm_class   [--property (name=value)[:name=value]*] auth_realm_name</pre>																						
<b>DESCRIPTION</b>	Adds the named authorized realm. This command is supported in remote mode only.																						
<b>OPTIONS</b>	<table><tr><td>--user</td><td>authorized domain application server administrative username.</td></tr><tr><td>--password</td><td>password to administer the domain application server.</td></tr><tr><td>--host</td><td>machine name where the domain application server is running.</td></tr><tr><td>--port</td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td>--passwordfile</td><td>file containing the domain application server password.</td></tr><tr><td>--terse</td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td></tr><tr><td>--echo</td><td>setting to true will echo the command line statement on the standard output. Default is false.</td></tr><tr><td>--interactive</td><td>if set to true (default), only the required password options are prompted.</td></tr><tr><td>--classname</td><td>Java class which implements this realm.</td></tr><tr><td>--property</td><td>optional attributes name/value pairs of provider implementation specific attributes.</td></tr></table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	--echo	setting to true will echo the command line statement on the standard output. Default is false.	--interactive	if set to true (default), only the required password options are prompted.	--classname	Java class which implements this realm.	--property	optional attributes name/value pairs of provider implementation specific attributes.
--user	authorized domain application server administrative username.																						
--password	password to administer the domain application server.																						
--host	machine name where the domain application server is running.																						
--port	port number of the domain application server listening for administration requests.																						
--secure	if true, uses SSL/TLS to communicate with the domain application server.																						
--passwordfile	file containing the domain application server password.																						
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																						
--echo	setting to true will echo the command line statement on the standard output. Default is false.																						
--interactive	if set to true (default), only the required password options are prompted.																						
--classname	Java class which implements this realm.																						
--property	optional attributes name/value pairs of provider implementation specific attributes.																						
<b>OPERANDS</b>	<i>auth_realm_name</i> name of this realm.																						
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using create-auth-realm</p> <pre>asadmin&gt; create-auth-realm --user admin1 --password adminadmin1 --host pigeon --port 5001 --classname com.iplanet.ias.security.auth.realm.DB.Database --property defaultuser=admin:Password=admin db Command create-auth-realm executed successfully</pre> <p>Where db is the auth realm created.</p>																						
<b>EXIT STATUS</b>	<table><tr><td>0</td><td>command executed successfully</td></tr><tr><td>1</td><td>error in executing the command</td></tr></table>	0	command executed successfully	1	error in executing the command																		
0	command executed successfully																						
1	error in executing the command																						

create-auth-realm(1)

**SEE ALSO** delete-auth-realm(1), list-auth-realms(1)

## create-connector-connection-pool(1)

<b>NAME</b>	create-connector-connection-pool – adds a connection pool with the specified connection pool name																								
<b>SYNOPSIS</b>	<pre>create-connector-connection-pool --user <i>admin_user</i>   [--password <i>admin_password</i>] [--host <i>localhost</i>] [--port <i>4848</i>]   [--secure -s] [--passwordfile <i>filename</i>] [--terse=false]   [--echo=false] [--interactive=true] [--steadypoolsize <i>8</i>]   [--maxpoolsize <i>32</i>] [--maxwaittime <i>3000</i>] [--poolresize <i>2</i>]   [--idletimeout <i>300</i>] [--failallconnections=false] --raname   <i>resource_adapter_name</i> --connectiondefinition <i>connection-definition_name</i>   [--property <i>name=value[:name=value]*</i>] <i>pool_name</i></pre>																								
<b>DESCRIPTION</b>	<p>Adds a new connector connection pool. Before you can add a new connector connection pool, you must first deploy the associated RAR file.</p> <p>This command is supported in remote mode only.</p>																								
<b>OPTIONS</b>	<table><tr><td>--user</td><td>authorized domain application server administrative username.</td></tr><tr><td>--password</td><td>password to administer the domain application server.</td></tr><tr><td>--host</td><td>machine name where the domain application server is running.</td></tr><tr><td>--port</td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td>--passwordfile</td><td>file containing the domain application server password.</td></tr><tr><td>--terse</td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td></tr><tr><td>--echo</td><td>setting to true will echo the command line statement on the standard output. Default is false.</td></tr><tr><td>--interactive</td><td>if set to true (default), only the required password options are prompted.</td></tr><tr><td>--steadypoolsize</td><td>minimum and initial number of connections maintained in the pool (default is 8).</td></tr><tr><td>--maxpoolsize</td><td>maximum number of connections that can be created to satisfy client requests (default is 32).</td></tr><tr><td>--maxwaittime</td><td>amount of time, in milliseconds, that a caller will have to wait before a connection is created if a</td></tr></table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	--echo	setting to true will echo the command line statement on the standard output. Default is false.	--interactive	if set to true (default), only the required password options are prompted.	--steadypoolsize	minimum and initial number of connections maintained in the pool (default is 8).	--maxpoolsize	maximum number of connections that can be created to satisfy client requests (default is 32).	--maxwaittime	amount of time, in milliseconds, that a caller will have to wait before a connection is created if a
--user	authorized domain application server administrative username.																								
--password	password to administer the domain application server.																								
--host	machine name where the domain application server is running.																								
--port	port number of the domain application server listening for administration requests.																								
--secure	if true, uses SSL/TLS to communicate with the domain application server.																								
--passwordfile	file containing the domain application server password.																								
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																								
--echo	setting to true will echo the command line statement on the standard output. Default is false.																								
--interactive	if set to true (default), only the required password options are prompted.																								
--steadypoolsize	minimum and initial number of connections maintained in the pool (default is 8).																								
--maxpoolsize	maximum number of connections that can be created to satisfy client requests (default is 32).																								
--maxwaittime	amount of time, in milliseconds, that a caller will have to wait before a connection is created if a																								

## create-connector-connection-pool(1)

	connection is not available. If set to 0 the caller is blocked indefinitely until a resource is available or an error occurs (default is 60000).
<code>--poolresize</code>	the number of connections to be removed when <code>idletimeout</code> timer expires. Connections that have idled for longer than the timeout are candidates for removal. When the pool size reaches the <code>steadypoolsize</code> , the connection removal stops.
<code>--idletimeout</code>	the maximum time that a connection can remain idle in the pool. After this amount of time, the pool can close this connection (default is 300).
<code>--failallconnections</code>	if true, closes all connections in the pool if a single validation check fails. This parameter is mandatory only if the <code>is-connection-validation-required</code> is set to true. Legal values are: on, off, yes, no, 1, 0, true or false (default is false).
<code>--raname</code>	module name of the deployed resource adapter. In case of a resource adapter that is embedded in an application, the <code>raname</code> will be <code>appname#raname</code> .
<code>--connectiondefinition</code>	identifies one of the connection definitions in the deployment descriptor of a resource adapter. Value of <code>connectionfactory-interface</code> sub-element in the <code>connection-definition</code> element.
<code>--property</code>	name/value pair of the configuration properties of the <code>managedconnectionfactory-class</code> of the <code>connectiondefinition</code> for which the pool is being created. The <code>UserName</code> and <code>Password</code> are accepted by default for all pools. The escape character <code>"\"</code> is used in this <code>--property</code> option to distinguish the colons ( <code>:</code> ) and the backslash ( <code>/</code> ).

**OPERANDS** `pool_name` name of the connection pool to be created.

### EXAMPLES

**EXAMPLE 1** Using create-connector-connection-pool

The JMS resource adapter that is prepackaged with the application server is used for this example. Before you can add a new connector connection pool, you must first deploy the associated RAR file.

To deploy the RAR file:

```
asadmin> deploy --user admin --password adminadmin jmsra.rar
Command deploy executed successfully
```

```
asadmin> create-connector-connection-pool --user admin1
--password adminadmin1 --steadypoolsize 20 --maxpoolsize 100 --poolresize 2
```

## create-connector-connection-pool(1)

**EXAMPLE 1** Using create-connector-connection-pool (Continued)

```
--maxwait 60000 --raname jmsra --connectiondefinition javax.jms.QueueConnectionFactory  
--property UserName=guest:Password=guest jms/qConnPool  
Command create-connector-connection-pool executed successfully
```

**EXIT STATUS**

0	command executed successfully
1	error in executing the command

**SEE ALSO** deploy(1), delete-connector-connection-pool(1),  
list-connector-connection-pools(1)



<b>NAME</b>	create-connector-resource – registers the resource with the specified JNDI name
<b>SYNOPSIS</b>	<pre> <b>create-connector-resource</b> --user <i>admin_user</i>     [--password <i>admin_password</i>] [--host <i>localhost</i>] [--port <b>4848</b>]     [--secure -s] [--passwordfile <i>filename</i>] [--terse=false]     [--echo=false] [--interactive=true]     --poolname <i>connector_connection_pool_name</i> [--enabled=true]     [--description <i>description</i>] <i>jndi_name</i> </pre>
<b>DESCRIPTION</b>	Registers the resource with the specified JNDI name. The connector connection pool must already exist. This command is supported in remote mode only.
<b>OPTIONS</b>	<pre> --user           authorized domain application server administrative                   username. --password       password to administer the domain application server. --host           machine name where the domain application server is running. --port           port number of the domain application server listening for                   administration requests. --secure         if true, uses SSL/TLS to communicate with the domain                   application server. --passwordfile   file containing the domain application server password. --terse         indicates that any output data must be very concise, typically                   avoiding human-friendly sentences and favoring                   well-formatted data for consumption by a script. Default is                   false. --echo           setting to true will echo the command line statement on the                   standard output. Default is false. --interactive     if set to true (default), only the required password options are                   prompted. --poolname       name of the connection pool connector resource. If two or more                   resource elements point to the same connection pool element,                   they will use the same pool connections at runtime. --enabled        determines whether the resource is enabled at runtime. If a                   resource is not enabled, you are not able to use the resource.                   Use the set command to enable or disable resources. --description    text description of the connection pool. </pre>
<b>OPERANDS</b>	<i>jndi_name</i> JNDI name of the resource to be created.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the create-connector-resource command</p> <p>Execute the example described for <code>create-connector-connection-pool</code> command before trying out this example.</p>

## create-connector-resource(1)

**EXAMPLE 1** Using the create-connector-resource command *(Continued)*

```
asadmin> create-connector-resource --user admin1 --password adminadmin1
--host pigeon --port 5001 --poolname jms/qConnPool --description
"creating a sample connector resource" jms/qConnFactory
Command create-connector-resource executed successfully
```

**EXIT STATUS**

0	command executed successfully
1	error in executing the command

**SEE ALSO** delete-connector-resource(1), list-connector-resources(1)

create-connector-security-map(1)

<b>NAME</b>	create-connector-security-map – creates a security map for the named connector connection pool
<b>SYNOPSIS</b>	<pre> <b>create-connector-security-map</b> --user <i>admin_user</i>     [--password <i>admin_password</i>] [--host <i>localhost</i>] [--port <b>4848</b>]     [--secure -s] [--passwordfile <i>filename</i>] [--terse=false]     [--echo=false] [--interactive=true] --poolname     <i>connector_connection_pool_name</i>     --principals <i>principal-name</i> [, <i>principal-name</i>] *   --usergroups <i>user-group</i> [, <i>user-group</i>] *     [--mappedpassword <i>password</i>] <i>mapname</i> </pre>
<b>DESCRIPTION</b>	<p>Creates a security map for the named connector connection pool. If the security map is not present, one is created. You must have first created a connector connection pool using the <code>create-connector-connection-pool</code> command. The enterprise information system is any system which holds the information. It can be a mainframe, a messaging system, a database system, or even an application.</p> <p>The <code>--principals</code> option and <code>--usergroups</code> option are mutually exclusive; only one should be used.</p> <p>This command is supported in remote mode only.</p>
<b>OPTIONS</b>	<pre> --user          authorized domain application server administrative                 username. --password      password to administer the domain application server. --host          machine name where the domain application server is                 running. --port          port number of the domain application server listening for                 administration requests. --secure        if true, uses SSL/TLS to communicate with the domain                 application server. --passwordfile  file containing the domain application server password. --terse         indicates that any output data must be very concise,                 typically avoiding human-friendly sentences and favoring                 well-formatted data for consumption by a script. Default is                 false. --echo          setting to true will echo the command line statement on the                 standard output. Default is false. --interactive   if set to true (default), only the required password options                 are prompted. --poolname      connector connection pool name. --principals    a comma separated list of J2EE principals. --usergroups    a comma separated list of J2EE usergroups. </pre>

## create-connector-security-map(1)

	<code>--mappedusername</code> the enterprise information system username.
	<code>--mappedpassword</code> the enterprise information system password.
<b>OPERANDS</b>	<i>mapname</i> name of the security map to be created.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using <code>create-connector-security-map</code>  It is assumed that the connector pool has already been created using the <code>create-connector-pool</code> command.  <pre>asadmin&gt; create-connector-security-map --user admin --password adminadmin poolname connector-pool1 --principals principal1,principal2 --usergroups usergroup1,usergroup2 --mappedusername backend-username --mappedpassword backend-password securityMap1</pre> Command <code>create-connector-security-map</code> executed successfully
<b>EXIT STATUS</b>	0 command executed successfully 1 error in executing the command
<b>SEE ALSO</b>	<code>delete-connector-security-map(1)</code> , <code>list-connector-security-maps(1)</code> , <code>update-connector-security-map(1)</code>

<b>NAME</b>	create-custom-resource – registers the custom resource
<b>SYNOPSIS</b>	<pre>create-custom-resource --user admin_user [--password admin_password]   [--host localhost] [--port 4848] [--secure -s]   [--passwordfile filename ] [--terse=false] [--echo=false]   [--interactive=true] --restype resource_type   --factoryclass classname [--enabled=true] [--description text]   [--property (name=value)[:name=value]*] jndi_name</pre>
<b>DESCRIPTION</b>	Registers the custom resource. This command is supported in remote mode only.
<b>OPTIONS</b>	<pre>--user          authorized domain application server administrative                   username. --password      password to administer the domain application server. --host          machine name where the domain application server is running. --port          port number of the domain application server listening for                   administration requests. --secure        if true, uses SSL/TLS to communicate with the domain                   application server. --passwordfile  file containing the domain application server password. --terse         indicates that any output data must be very concise, typically                   avoiding human-friendly sentences and favoring                   well-formatted data for consumption by a script. Default is                   false. --echo          setting to true will echo the command line statement on the                   standard output. Default is false. --interactive    if set to true (default), only the required password options are                   prompted. --restype       type of custom resource to be created. --factoryclass  class that creates the custom resource. --enabled       determines whether the resource is enabled at runtime. --description   text description of the custom resource. --property      optional attribute name/value pairs for configuring the custom                   resource.</pre>
<b>OPERANDS</b>	<i>jndi_name</i> JNDI name of the custom resource to be created.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using create-custom-resources</p> <pre>asadmin&gt; create-custom-resource --user admin1 --password adminadmin1   --host pigeon --port 5001 --restype customType factoryclass "com.custom.class" --description   "this is a sample of creating a custom resource" sample_custom_resource Command create-custom-resource executed successfully</pre>

create-custom-resource(1)

**EXAMPLE 1** Using create-custom-resources *(Continued)*

Where `sample_custom_resource` is the custom resource created.

**EXIT STATUS**

0	command executed successfully
1	error in executing the command

**SEE ALSO** `delete-custom-resource(1)`, `list-custom-resources(1)`

<b>NAME</b>	create-domain – creates a domain with the given name
<b>SYNOPSIS</b>	<b>create-domain</b> [--domaindir <i>install_dir/domains</i> ] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=false] --adminport <i>port_number</i> --adminuser <i>admin_user</i> [--adminpassword <i>password</i> ] [--instanceport 8080] [--domainproperties (name=value)[:name=value]*] <i>domain_name</i>
<b>DESCRIPTION</b>	<p>create-domain creates a domain with the specified administration port number, administration user, administration password, and domain name. By creating a domain, an administration server is created in a directory named as the domain name. This command is supported in local mode only.</p> <p>If a user creates a domain in a non-default directory, the domain will not be automatically shutdown during uninstallation.</p>
<b>OPTIONS</b>	<p>--domaindir            directory where the domain is to be created. If specified, path must be accessible in the filesystem. If not specified, the domain is created in the default <i>install_dir/domains</i> directory.</p> <p>--passwordfile        file containing the domain application server password in the following form: AS_ADMIN_PASSWORD=<i>password</i>. Where <i>password</i> is the actual administrator password for the domain.</p> <p>--terse                indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</p> <p>--echo                 setting to true will echo the command line statement on to the standard output. Default is false.</p> <p>--interactive         if set to true (default), only the required options are prompted.</p> <p>--adminport            port number of the domain application server listening for the administration requests.</p> <p>--adminuser            administrative username for the specified domain.</p> <p>--adminpassword       password to administer the domain application server.</p> <p>--instanceport        port number of the http listener. The port number cannot be currently in use.</p> <p>--domainproperties    list of the property name/value pairs for the domain to be created separated by the ":" character. The property value assignment character is =. Valid property names are: <i>jms.port, orb.listener.port, http.ssl.port, orb.ssl.port, orb.mutualauth.port</i>. Valid values</p>

## create-domain(1)

	are: http.ssl.port=1043:orb.ssl.port=1060:orb.mutualauth.port=
<b>OPERANDS</b>	<i>domain_name</i> name of the domain. Must be a unique name.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using create-domain <pre>asadmin&gt; create-domain --domaindir /export/domains --adminport 7070 --adminuser admin --adminpassword adminadmin --instanceport 7071 sampleDomain created domain sampleDomain successfully</pre> <p>Where: the sampleDomain domain is created in the /export/domains directory.</p>
<b>EXIT STATUS</b>	0 command executed successfully 1 error in executing the command
<b>SEE ALSO</b>	delete-domain(1), start-domain(1), stop-domain(1), , list-domains(1)



<b>NAME</b>	create-file-user – creates a new file user
<b>SYNOPSIS</b>	<pre>create-file-user --user admin_user [--password admin_password]   [--host localhost] [--port 4848] [--secure -s]   [--passwordfile filename] [--terse=false] [--echo=false]   [--interactive=true] [--userpassword user_password]   [--groups user_groups:[user_groups]*] [--authrealmname   auth_realm_name] user_name</pre>
<b>DESCRIPTION</b>	<p>Creates an entry in keyfile with the specified username, userpassword, and groups. Multiple groups can be created by separating them with a colon ":". If the <i>auth_realm_name</i> is not specified, an entry is created in the default keyfile. If <i>auth_realm_name</i> is specified, an entry is created in the keyfile where the auth-realm name in the <i>domain.xml</i> file points to.</p> <p>This command is supported in remote mode only.</p>
<b>OPTIONS</b>	<pre>--user          authorized domain application server administrative                 username. --password      password to administer the domain application server. --host          machine name where the domain application server is                 running. --port          port number of the domain application server listening for                 administration requests. --secure        if true, uses SSL/TLS to communicate with the domain                 application server. --passwordfile  file containing the domain application server password. --terse         indicates that any output data must be very concise, typically                 avoiding human-friendly sentences and favoring                 well-formatted data for consumption by a script. Default is                 false. --echo          setting to true will echo the command line statement on the                 standard output. Default is false. --interactive   if set to true (default), only the required password options are                 prompted. --userpassword  password for the file user. --groups        group where the file user belongs to. --authrealmname name, in the domain.xml file, where you have different                 stores for file auth realm.</pre>
<b>OPERANDS</b>	<pre>user_name      name of file user to be created.</pre>

## create-file-user(1)

### EXAMPLES

**EXAMPLE 1** Using the create-file-user command

It is assumed that an authority realm has already been created using the create-auth-realm command.

```
asadmin> create-file-user --user admin1 --password adminadmin1
--host pigeon --port 5001 --userpassword sample --groups staff:manager
--authrealmname auth-realm1 sample_user
Command create-file-user executed successfully
```

Where: the sample\_user is the file user created.

### EXIT STATUS

0 command executed successfully

1 error in executing the command

### SEE ALSO

create-auth-realm(1), delete-file-user(1), list-file-users(1), update-file-user(1), list-file-groups(1)

<b>NAME</b>	create-http-listener – adds a new HTTP listener socket
<b>SYNOPSIS</b>	<pre> <b>create-http-listener</b> --user <i>admin_user</i> [--password <i>admin_password</i>]   [--host <i>localhost</i>] [--port <b>4848</b>] [--secure -s]   [--passwordfile <i>filename</i>] --listeneraddress <i>address</i>   [--terse=false] [--echo=false] [--interactive=true]   --listenerport <i>listener_port</i> --defaultvs <i>virtual_server</i> --servername   <i>server_name</i> [--acceptorthreads <i>acceptor_threads</i>]   [--securityenabled=false] [--enabled=true] <i>listener_ID</i> </pre>
<b>DESCRIPTION</b>	Creates the HTTP listener. This command is supported in remote mode only.
<b>OPTIONS</b>	<pre> --user                authorized domain application server administrative                     username. --password            password to administer the domain application server. --host                machine name where the domain application server is                     running. --port                port number of the domain application server listening for                     administration requests. --secure              if true, uses SSL/TLS to communicate with the domain                     application server. --passwordfile        file containing the domain application server password. --terse                indicates that any output data must be very concise,                     typically avoiding human-friendly sentences and favoring                     well-formatted data for consumption by a script. Default is                     false. --echo                setting to true will echo the command line statement on the                     standard output. Default is false. --interactive          if set to true (default), only the required password options                     are prompted. --listeneraddress     IP address of the listener address. --listenerport        port number to create the listen socket on. Legal values are                     1–65535. On UNIX, creating sockets that listen on ports                     1–1024 requires superuser privileges. Configuring an SSL                     listen socket to listen on port 443 is recommended. --defaultvs           ID attribute of the default virtual server for this particular                     connection group. --servername          tells the server what to put in the host name section of any                     URLs it sends to the client. This affects URLs the server                     automatically generates; it doesn't affect the URLs for                     directories and files stored in the server. This name should                     be the alias name if your server uses an alias. If a colon and </pre>

## create-http-listener(1)

		port number is appended, that port will be used in URLs that the server sends to the client.
	<code>--acceptorthreads</code>	number of acceptor threads for the listen socket. The recommended value is the number of processors in the machine.
	<code>--securityenabled</code>	determines whether the HTTP listener runs SSL. You can turn SSL2 or SSL3 ON or OFF and set ciphers using an SSL element. The security setting globally enables or disables SSL by making certificates available to the server instance.
	<code>--enabled</code>	determines if the resource is enabled at runtime.
<b>OPERANDS</b>	<code>listener_id</code>	listener ID of the HTTP listener.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using create-http-listener	
		<pre>asadmin&gt; create-http-listener --user admin1 --password adminadmin1 --host pigeon --port 5001 --listeneraddress 0.0.0.0 --listenerport 7272 --defaultvs server --servername pigeon.red.iplanet.com --acceptorthreads 2 --securityenabled=false --enabled=false sampleListener Command create-http-listener executed successfully</pre>
		Where: <code>sampleListener</code> is the HTTP listener created.
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<code>delete-http-listener(1)</code> , <code>list-http-listeners(1)</code>	

<b>NAME</b>	create-http-qos – creates a new quality of service parameter
<b>SYNOPSIS</b>	<pre> <b>create-http-qos</b>   --user <i>admin_user</i> [--password <i>admin_password</i>] [--host <i>localhost</i>]   [--port <i>4848</i>] [--passwordfile <i>filename</i>] [--secure -s] [--virtualserver <i>virtual_server_ID</i>] [--bwlimit <i>bwlimit</i>] [--enforcebwlimit=<i>enforce_bw_limit</i>] [--connlimit <i>connection_limit</i>]   [--enforceconnlimit=<i>enforce_conn_limit</i>] <i>instance_name</i> </pre>
<b>DESCRIPTION</b>	Adds a new quality of service parameter associated with the named server instance.
<b>OPTIONS</b>	<pre> --user          administrative user associated for the instance. --password      administrative password corresponding to the                 administrative user. --host          host name of the machine hosting the administrative                 instance. --port          administrative port number associated with the                 administrative host. --passwordfile  file containing passwords appropriate for the command                 (e.g., administrative instance). --secure        if true, uses SSL/TLS to communicate with the                 administrative instance. --virtualserver virtual server ID. It can also be referred to as the variable                 \$id in an obj.conf file. A virtual server ID cannot begin                 with a number. --bwlimit       maximum bandwidth limit, for the virtual server class or                 virtual server, in bytes per second. The default is no limit. --enforcebwlimit determines whether the bandwidth limit should be                 enforced or not. --connlimit     maximum number of concurrent connections for the                 server, virtual server class, or virtual server. --enforceconnlimit determines whether the connection limit should be                 enforced or not. </pre>
<b>OPERANDS</b>	<i>instance_name</i> name of the instance.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using create-http-qos</p> <pre> asadmin&gt; create-http-qos --user admin --password adminadmin --host fuyako --port 7070 --bwlimit 10 Created HTTP QOS </pre> <p>Where: the HTTP QOS is created for the virtual server <code>server1</code> with the instance name of <code>server1</code>.</p>

create-http-qos(1)

<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>INTERFACE EQUIVALENT</b>		Server instance, HTTP Server Virtual Servers, Instance QOS page for the server instance
<b>SEE ALSO</b>		delete-http-qos(1)

<b>NAME</b>	create-iiop-listener – adds the IIOP listener
<b>SYNOPSIS</b>	<pre>create-iiop-listener --user admin_user [--password admin_password]   [--host localhost] [--port 4848] [--secure -s]   [--passwordfile filename] [--terse=false] [--echo=false]   [--interactive=true] --listeneraddress address [--iiopport   iiop_port] [--enabled=true] [--property (name=value)[:name=value] *]   listener_ID</pre>
<b>DESCRIPTION</b>	Adds the IIOP listener. This command is supported in remote mode only.
<b>OPTIONS</b>	<pre>--user          authorized domain application server administrative                 username.  --password      password to administer the domain application server.  --host          machine name where the domain application server is                 running.  --port          port number of the domain application server listening for                 administration requests.  --secure        if true, uses SSL/TLS to communicate with the domain                 application server.  --passwordfile  file containing the domain application server password.  --terse         indicates that any output data must be very concise,                 typically avoiding human-friendly sentences and favoring                 well-formatted data for consumption by a script. Default is                 false.  --echo          setting to true will echo the command line statement on the                 standard output. Default is false.  --interactive   if set to true (default), only the required password options                 are prompted.  --listeneraddress  can be the IP address or the hostname  --iiopport      IIOP port number.  --enabled       determines whether the IIOP listener is enabled at runtime.  --property      optional attribute name/value pairs for configuring the                 resource.</pre>
<b>OPERANDS</b>	<i>listener_id</i> unique identifier for the IIOP listener to be created.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using create-iiop-listener</p> <pre>asadmin&gt; create-iiop-listener --user admin --password adminadmin --host fuyako --port 7070 --listeneraddress 192.168.1.100 --iiopport 8080 sample_iiop_listener Created IIOP listener with id = sample_iiop_listener</pre>

## create-iiop-listener(1)

**EXAMPLE 1** Using create-iiop-listener *(Continued)*

Where: `sample_iiop_listener` is the IIOP listener created.

**EXIT STATUS**

0	command executed successfully
1	error in executing the command

**SEE ALSO** `delete-iiop-listener(1)`, `list-iiop-listeners(1)`



<b>NAME</b>	create-instance – creates an application server instance with the specified instance name																				
<b>SYNOPSIS</b>	<b>create-instance</b> [--user <i>admin_user</i> ] [-password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <i>4848</i> ] [--sysuser <i>sys_user</i> ] [--domain <i>domain_name</i> ] [--local=false] [--passwordfile <i>filename</i> ] [--secure -s] --instanceport <i>instanceport</i> <i>instance_name</i>																				
<b>DESCRIPTION</b>	You can create a new instance on a local or remote machine. If on the remote machine an administration server is already running for the specified hostname, then the system defaults to the local hostname. To create the instance locally, not requiring the administration server to be up and running, specify the <code>--local</code> option. The named instance must not exist within that domain.																				
<b>OPTIONS</b>	<table border="0"> <tr> <td style="padding-right: 20px;">--user</td> <td>administrative user associated for the instance.</td> </tr> <tr> <td>--password</td> <td>administrative password corresponding to the administrative user.</td> </tr> <tr> <td>--host</td> <td>host name of the machine hosting the administrative instance.</td> </tr> <tr> <td>--port</td> <td>administrative port number associated with the administrative host.</td> </tr> <tr> <td>--sysuser</td> <td>owner of the domain directory.</td> </tr> <tr> <td>--domain</td> <td>name of the domain.</td> </tr> <tr> <td>--local</td> <td>determines if the command should delegate the request to administrative instance or run locally.</td> </tr> <tr> <td>--passwordfile</td> <td>file containing passwords appropriate for the command (e.g., administrative instance).</td> </tr> <tr> <td>--secure</td> <td>if true, uses SSL/TLS to communicate with the administrative instance.</td> </tr> <tr> <td>--instanceport</td> <td>port where the instance listens for requests.</td> </tr> </table>	--user	administrative user associated for the instance.	--password	administrative password corresponding to the administrative user.	--host	host name of the machine hosting the administrative instance.	--port	administrative port number associated with the administrative host.	--sysuser	owner of the domain directory.	--domain	name of the domain.	--local	determines if the command should delegate the request to administrative instance or run locally.	--passwordfile	file containing passwords appropriate for the command (e.g., administrative instance).	--secure	if true, uses SSL/TLS to communicate with the administrative instance.	--instanceport	port where the instance listens for requests.
--user	administrative user associated for the instance.																				
--password	administrative password corresponding to the administrative user.																				
--host	host name of the machine hosting the administrative instance.																				
--port	administrative port number associated with the administrative host.																				
--sysuser	owner of the domain directory.																				
--domain	name of the domain.																				
--local	determines if the command should delegate the request to administrative instance or run locally.																				
--passwordfile	file containing passwords appropriate for the command (e.g., administrative instance).																				
--secure	if true, uses SSL/TLS to communicate with the administrative instance.																				
--instanceport	port where the instance listens for requests.																				
<b>OPERANDS</b>	<i>instance_name</i> name of the instance to be created.																				
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using create-instance in local mode</p> <pre>asadmin&gt; create-instance --domain domain1 --instanceport 8967 --sysuser adminuser server4 Created Instance server4 successfully</pre> <p>Where: the server4 instance is created under the domain1 domain.</p> <p><b>EXAMPLE 2</b> Using create-instance in remote mode</p> <pre>asadmin&gt; create-instance --sysuser adminuser --user admin --password adminadmin --host localhost --port 4848 --instanceport 8967 server4 Created Instance server4 successfully</pre>																				

create-instance(1)

**EXAMPLE 2** Using create-instance in remote mode (Continued)

Where: the server4 instance is created on the remote server for the associated user, password, host, and port.

**EXIT STATUS**  
0 command executed successfully  
1 error in executing the command

**INTERFACE EQUIVALENT** Application Server instances page

**SEE ALSO** delete-instance(1), start-instance(1), stop-instance(1),  
restart-instance(1)

<b>NAME</b>	create-javamail-resource – registers the JavaMail resource
<b>SYNOPSIS</b>	<pre> <b>create-javamail-resource</b> --user <i>admin_user</i>     [--password <i>admin_password</i>] [--host <i>localhost</i>] [--port <b>4848</b>]     [--secure -s] [--passwordfile <i>filename</i>] [--terse=false]     [--echo=false] [--interactive] --mailhost <i>hostname</i>     --mailuser <i>username</i> --fromaddress <i>address</i> [--storeprotocol <i>imap</i>]     [--storeprotocolclass <i>com.sun.mail.imapIMAPStore</i>]     [--transprotocol <i>smtp</i>]     [--transprotocolclass <i>com.sun.mail.smtp.SMTPTransport</i>]     [--debug=false] [--enabled=true] [--description <i>text</i>]     [--property (<i>name=value</i>)[:<i>name=value</i>]*] <i>jndi_name</i> </pre>
<b>DESCRIPTION</b>	Registers the Javamail resource. This command can only be run remotely.
<b>OPTIONS</b>	<pre> --user                authorized domain application server administrative                     username. --password            password to administer the domain application server. --host                machine name where the domain application server is                     running. --port                port number of the domain application server listening                     for administration requests. --secure              if true, uses SSL/TLS to communicate with the domain                     application server. --passwordfile        file containing the domain application server                     password. --terse                indicates that any output data must be very concise,                     typically avoiding human-friendly sentences and                     favoring well-formatted data for consumption by a                     script. --echo                setting to true will echo the command line statement                     on the standard output. --interactive          prompts you for the required options that are not                     already specified. --mailhost            mail server host. --mailuser            mail account user name. --fromaddress         email address. --storeprotocol        mail server stored protocol. --storeprotocolclass  mail server stored protocol class name. --transprotocol        mail server transport protocol. </pre>

## create-javamail-resource(1)

	<code>--transportprotocolclass</code>	mail server transport protocol class name.
	<code>--debug</code>	if set to true, server startup in debug mode for this resource.
	<code>--enabled</code>	determines whether the resource is enabled at runtime.
	<code>--description</code>	text description of the Javamail resource.
	<code>--property</code>	optional attribute name/value pairs for configuring the Javamail resource.
<b>OPERANDS</b>	<i>jndi_name</i>	JNDI name of the Javamail resource to be created.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using create-javamail-resource	
	<pre>asadmin&gt; create-javamail-resource --user admin --password adminadmin --host fuyako --port 7070 --mailhost localhost --mailuser sample --fromaddress sample\@sun\.com mail_resourc/MyMailSession Command create-javamail-resource executed successfully</pre>	
	Where: mail/MyMailSession is the JavaMail resource created. The escape character (\) is used in the --fromaddress option to distinguish the dot (.) and at sign (@). The JNDI name for a JavaMail resource customarily includes the mail/ naming subcontext.	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	delete-javamail-resource(1), list-javamail-resources(1)	

<b>NAME</b>	create-jdbc-connection-pool – registers the JDBC connection pool																		
<b>SYNOPSIS</b>	<pre> <b>create-jdbc-connection-pool</b> --user <i>admin_user</i>   [--password <i>admin_password</i>] [--host <i>localhost</i>] [--port <b>4848</b>]   [--secure -s] [--passwordfile <i>filename</i>] [--terse=false]   [--echo=false] [--interactive=true]   --datasourceclassname <i>classname</i> [--restype <i>res_type</i>]   [--steadypoolsize <b>8</b>] [--maxpoolsize <b>32</b>] [--maxwait <b>6000</b>]   [--poolresize <b>2</b>] [--idletimeout <b>300</b>]   [--isolationlevel <i>isolation_level</i>] [--isisolationguaranteed]   [--isconnectvalidatereq=false]   [--validationmethod <i>auto-commit</i>] [--validationtable <i>table_name</i>]   [--failconnection=false] [--description <i>text</i>]   [--property (<i>name=value</i>)[:<i>name=value</i>]*] <i>connection_pool_ID</i> </pre>																		
<b>DESCRIPTION</b>	<p>Registers the JDBC connection pool. All the properties of the connection pool can be modified dynamically at runtime. If you change any of the pool properties (for example the <code>maxpoolsize</code>), the change is effected without any change to the existing connections. If you change any of the connection related properties (such as <code>UserName</code>), then all the existing connections in the pool are destroyed and new connections will be created. Use the <code>set</code> command to change any property.</p> <p>This command is supported in remote mode only.</p>																		
<b>OPTIONS</b>	<table border="0"> <tr> <td style="vertical-align: top;"><code>--user</code></td> <td>authorized domain application server administrative username.</td> </tr> <tr> <td style="vertical-align: top;"><code>--password</code></td> <td>password to administer the domain application server.</td> </tr> <tr> <td style="vertical-align: top;"><code>--host</code></td> <td>machine name where the domain application server is running.</td> </tr> <tr> <td style="vertical-align: top;"><code>--port</code></td> <td>port number of the domain application server listening for administration requests.</td> </tr> <tr> <td style="vertical-align: top;"><code>--secure</code></td> <td>if true, uses SSL/TLS to communicate with the domain application server.</td> </tr> <tr> <td style="vertical-align: top;"><code>--passwordfile</code></td> <td>file containing the domain application server password.</td> </tr> <tr> <td style="vertical-align: top;"><code>--terse</code></td> <td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.</td> </tr> <tr> <td style="vertical-align: top;"><code>--echo</code></td> <td>setting to true will echo the command line statement on the standard output.</td> </tr> <tr> <td style="vertical-align: top;"><code>--interactive</code></td> <td>prompts you for the required options that are not already specified.</td> </tr> </table>	<code>--user</code>	authorized domain application server administrative username.	<code>--password</code>	password to administer the domain application server.	<code>--host</code>	machine name where the domain application server is running.	<code>--port</code>	port number of the domain application server listening for administration requests.	<code>--secure</code>	if true, uses SSL/TLS to communicate with the domain application server.	<code>--passwordfile</code>	file containing the domain application server password.	<code>--terse</code>	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.	<code>--echo</code>	setting to true will echo the command line statement on the standard output.	<code>--interactive</code>	prompts you for the required options that are not already specified.
<code>--user</code>	authorized domain application server administrative username.																		
<code>--password</code>	password to administer the domain application server.																		
<code>--host</code>	machine name where the domain application server is running.																		
<code>--port</code>	port number of the domain application server listening for administration requests.																		
<code>--secure</code>	if true, uses SSL/TLS to communicate with the domain application server.																		
<code>--passwordfile</code>	file containing the domain application server password.																		
<code>--terse</code>	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.																		
<code>--echo</code>	setting to true will echo the command line statement on the standard output.																		
<code>--interactive</code>	prompts you for the required options that are not already specified.																		

## create-jdbc-connection-pool(1)

<code>--datasourceclassname</code>	name of the vendor supplied JDBC datasource resource manager.
<code>--restype</code>	must be specified to disambiguate when a datasource class implements more than one of the JDBC interfaces <code>javax.sql.DataSource</code> , <code>javax.sql.ConnectionPoolDataSource</code> or <code>javax.sql.XADataSource</code> . An error is produced when this option has a legal value and the indicated interface is not implemented by the datasource class.
<code>--steadypoolsize</code>	minimum and initial number of connections maintained in the pool.
<code>--maxpoolsize</code>	maximum number of connections that can be created.
<code>--maxwait</code>	the amount of time a caller will wait before a connection timeout is sent. The default is 60 seconds. A value of 0 forces the caller to wait indefinitely.
<code>--poolresize</code>	number of connections to be removed when <code>idletimeout</code> timer expires. Connections that have idled for longer than the timeout are candidates for removal. When the pool size reaches <code>steadypoolsize</code> , the connection removal stops.
<code>--idletimeout</code>	maximum time (in seconds) that a connection can remain idle in the pool. After this time, the implementation can close this connection. It is recommended that this timeout is kept shorter than the server side timeout to prevent the accumulation of unusable connections in the application.
<code>--isolationlevel</code>	specifies the transaction-isolation-level on the pooled database connections. This option does not have a default value. If not specified, the pool operates with default isolation level provided by the JDBC driver. A desired isolation level can be set using one of the standard transaction isolation levels: <code>read-uncommitted</code> , <code>read-committed</code> , <code>repeatable-read</code> , <code>serializable</code> . Applications that change the isolation level on a pooled connection programmatically risk polluting the pool. This could lead to program errors.
<code>--isisolationguaranteed</code>	applicable only when a particular isolation level is specified for <code>transaction-isolation-level</code> . The default

## create-jdbc-connection-pool(1)

value is true. This assures that every time a connection is obtained from the pool, it is guaranteed to have the isolation set to the desired value. This could have some performance impact on some JDBC drivers. Can be set to false by the administrator when confident that the application does not change the isolation level before returning the connection.

`--isconnectvalidatereq` if set to true connections are validated (checked to see if they are usable) before giving out the application. The default is false.

`--validationmethod` name of the validation table used to perform a query to validate a connection. Valid settings are: auto-commit, meta-data, or table. Defaults to auto-commit.

`--validationtable` name of the validation table used to perform a query to validate a connection. This parameter is mandatory if connection-validation-type is set to table. Verification by accessing a user specified table may become necessary for connection validation.

`--failconnection` if set to true, all connection in the pool must be closed if a single validation check fails; defaults to false. One attempt is made to re-establish failed connections.

`--description` text description of the JDBC connection pool.

`--property` optional attributes name/value pairs for configuring the connection pool.

**OPERANDS** `connection_pool_id` name of the JDBC connection pool to be created.

### EXAMPLES

**EXAMPLE 1** Using create-jdbc-connection-pool

```
asadmin> create-jdbc-connection-pool --user admin --password adminadmin
--host fuyako --port 7070 --datasourceclassname com.pointbase.jdbc.jdbcUniversalDriver
--restype jax.sql.XADataSource --isolationlevel serializable --isconnectvalidatereq=true
--validationmethod auto-commit --description "XA Connection"
--property DatabaseName="jdbc\:pointbase\:server\:\\/localhost:9093\/sample"
:User=public:Password=public XA_connection_pool
Command create-jdbc-connection-pool executed successfully
```

Where: the XA\_connection\_pool is created. The escape character “\” is used in the --property option to distinguish the colons (:) and the backslash (/).

**EXIT STATUS** 0 command executed successfully

create-jdbc-connection-pool(1)

1 error in executing the command

**SEE ALSO** delete-jdbc-connection-pool(1), list-jdbc-connection-pools(1)



<b>NAME</b>	create-jdbc-resource – registers the JDBC resource
<b>SYNOPSIS</b>	<pre>create-jdbc-resource --user admin_user [--password admin_password]   [--host localhost] [--port 4848] [--secure -s]   [--passwordfile filename] [--terse=false] [--echo=false]   [--interactive=true] --connectionpoolid ID [--enabled=true]   [--description text] jndi_name</pre>
<b>DESCRIPTION</b>	Registers the JDBC resource. This command is supported in remote mode only.
<b>OPTIONS</b>	<pre>--user          authorized domain application server administrative                 username.  --password      password to administer the domain application server.  --host          machine name where the domain application server is                 running.  --port          port number of the domain application server listening                 for administration requests.  --secure        if true, uses SSL/TLS to communicate with the domain                 application server.  --passwordfile  file containing the domain application server password.  --terse         indicates that any output data must be very concise,                 typically avoiding human-friendly sentences and favoring                 well-formatted data for consumption by a script.  --echo          setting to true will echo the command line statement on                 the standard output.  --interactive   prompts you for the required options that are not already                 specified.  --connectionpoolid  name of the JDBC connection pool. If two or more JDBC                 resource elements point to the same connection pool                 element, they will use the same pool connections at                 runtime.  --enabled       determines whether the resource is enabled at runtime.  --description   text description of the JDBC resource.</pre>
<b>OPERANDS</b>	<i>jndi_name</i> JNDI name for resource to be created.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the create-jdbc-resource command</p> <pre>asadmin&gt; create-jdbc-resource --user admin1 --password adminadmin1 --host pigeon --port 5001 --connectionpoolid XA_connection_pool --description "creating a sample jdbc resource" sample_jdbc_resource Command create-jdbc-resource executed successfully</pre>

create-jdbc-resource(1)

**EXAMPLE 1** Using the create-jdbc-resource command *(Continued)*

Where: `sample_jdbc_resource` is the resource that is created.

**EXIT STATUS** 0 command executed successfully

1 error in executing the command

**SEE ALSO** `delete-jdbc-resource(1)`, `list-jdbc-resources(1)`

<b>NAME</b>	create-jmsdest – adds the physical destination
<b>SYNOPSIS</b>	<pre>create-jmsdest --user admin_user [--password admin_password]   [--host localhost] [--port 4848] [--secure -s]   [--passwordfile filename] [--terse=false] [--echo=false]   [--interactive] --desttype -T topic queue   [--property (name=value)[:name=value]*] dest_name</pre>
<b>DESCRIPTION</b>	creates the JMS physical destination. Along with the physical destination, you create a JMS destination resource with a Name property that specifies the physical destination. This command is supported in remote mode only.
<b>OPTIONS</b>	<pre>--user          authorized domain application server administrative                   username. --password      password to administer the domain application server. --host         machine name where the domain application server is running. --port        port number of the domain application server listening for                   administration requests. --secure       if true, uses SSL/TLS to communicate with the domain                   application server. --passwordfile file containing the domain application server password. --terse       indicates that any output data must be very concise, typically                   avoiding human-friendly sentences and favoring                   well-formatted data for consumption by a script. --echo        setting to true will echo the command line statement on the                   standard output. --interactive  prompts you for the required options that are not already                   specified. --desttype    type of JMS destination. Valid values are topic, and queue. --property    name/value pairs used for specifying MQ specific attributes to                   further customize the destination to be created.</pre>
<b>OPERANDS</b>	<i>dest_name</i> name of the JMS destination. Valid value is any name that can be a Java identifier.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using create-jmsdest</p> <pre>asadmin&gt; create-jmsdest --user admin --passwordfile passwords.txt --host localhost --port 4848 --desttype queue --property User=public:Password=public PhysicalQueue Command create-jmsdest executed successfully</pre>
<b>EXIT STATUS</b>	0 command executed successfully

create-jmsdest(1)

1 error in executing the command

**SEE ALSO** `create-jms-resource(1)`, `delete-jmsdest(1)`, `list-jmsdest(1)`

<b>NAME</b>	create-jmsobj – adds the named object
<b>SYNOPSIS</b>	<b>create-jmsobj</b> <b>--instance</b> <i>instance_name</i> <b>--jndilookupname</b>   <b>-l</b> <i>jndi_lookup_name</i> <b>--objtype</b>   <b>-o</b> <i>object_type</i>
<b>DESCRIPTION</b>	Adds the named destination.
<b>OPTIONS</b>	<b>--instance</b> the name of the instance. <b>--jndilookupname</b> <b>--objtype</b> <b>--jmsobjattr</b> Lists the optional attribute=value pairs for configuring the resource.
<b>EXAMPLES</b>	asadmin% <b>create-jmsobj --instance server1</b>
<b>INTERFACE EQUIVALENT</b>	JMS Destination pages
<b>SEE ALSO</b>	delete-jmsobj(1) list-jmsobj(1)

## create-jms-resource(1)

<b>NAME</b>	create-jms-resource – registers the JMS resource
<b>SYNOPSIS</b>	<pre><b>create-jms-resource</b> --user <i>admin_user</i> [--password <i>admin_password</i>]   [--host <i>localhost</i>] [--port <b>4848</b>]   [--secure -s] [--passwordfile <i>filename</i>] [--terse=false]   [--echo=false] [--interactive=true] --restype <i>resource_type</i>   [--enabled=true] [--description <i>text</i>]   [--property (<i>name=value</i>)[:<i>name=value</i>]*] <i>jndi_name</i></pre>
<b>DESCRIPTION</b>	Registers the JMS resource. This command is supported in remote mode only.
<b>OPTIONS</b>	<p>--user authorized domain application server administrative username.</p> <p>--password password to administer the domain application server.</p> <p>--host machine name where the domain application server is running.</p> <p>--port port number of the domain application server listening for administration requests.</p> <p>--secure if true, uses SSL/TLS to communicate with the domain application server.</p> <p>--passwordfile file containing the domain application server password.</p> <p>--terse indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.</p> <p>--echo setting to true will echo the command line statement on the standard output.</p> <p>--interactive prompts you for the required options that are not already specified.</p> <p>--restype JMS resource type which can be: <code>javax.jms.Topic</code>, <code>javax.jms.Queue</code>, <code>javax.jms.TopicConnectionFactory</code>, <code>javax.jms.QueueConnectionFactory</code>.</p> <p>--enabled determines whether the resource is enabled at runtime.</p> <p>--description text description of the JMS resource.</p> <p>--property optional attribute name/value pairs for configuring the JMS resource.</p>
<b>OPERANDS</b>	<i>jndi_name</i> JNDI name of the JMS resource to be created.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Creating a JMS connection factory resource for durable subscriptions</p> <pre>asadmin&gt; create-jms-resource --user admin1 --password adminadmin1 --host pigeon --port 5001 --restype javax.jms.TopicConnectionFactory --description "example of creating a JMS connection factory"</pre>

**EXAMPLE 1** Creating a JMS connection factory resource for durable subscriptions  
(Continued)

```
--property ClientId=MyID jms/DurableTopicConnectionFactory
Command create-jms-resource executed successfully
```

Where: `.jms/DurableTopicConnectionFactory` is the JNDI name of the resource, and the `ClientId` property sets a client ID on the connection factory so that it can be used for durable subscriptions. The JNDI name for a JMS resource customarily includes the `./jms/` naming subcontext.

**EXAMPLE 2** Creating a JMS destination resource

```
asadmin> create-jms-resource --user admin1
--password adminadmin1 --host pigeon --port 5001
--restype javax.jms.Queue
--property Name=PhysicalQueue jms/MyQueue
Command create-jms-resource executed successfully
```

Where: `./jms/Queue` is the JNDI name of the resource, and the `Name` property specifies the physical destination that the resource refers to.

**EXIT STATUS** 0 command executed successfully

1 error in executing the command

**SEE ALSO** `delete-jms-resource(1)`, `list-jms-resources(1)`, `create-jmsdest(1)`

## create-jndi-resource(1)

<b>NAME</b>	create-jndi-resource – registers the JNDI resource																														
<b>SYNOPSIS</b>	<pre><b>create-jndi-resource</b> --user <i>admin_user</i>   [--password <i>admin_password</i>] [--host <i>localhost</i>] [--port <b>4848</b>]   [--secure -s] [--passwordfile <i>filename</i>] [--terse=false]   [--echo=false] [--interactive=true]   --jndilookupname <i>lookup_name</i> --restype <i>type</i> --factoryclass <i>class_name</i> [--enabled=   [--description <i>text</i>] [--property (<i>name=value</i>)[:<i>name=value</i>]*]   <i>jndi_name</i></pre>																														
<b>DESCRIPTION</b>	Registers the JNDI resource. This command is supported in remote mode only.																														
<b>OPTIONS</b>	<table><tr><td>--user</td><td>authorized domain application server administrative username.</td></tr><tr><td>--password</td><td>password to administer the domain application server.</td></tr><tr><td>--host</td><td>machine name where the domain application server is running.</td></tr><tr><td>--port</td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td>--passwordfile</td><td>file containing the domain application server password.</td></tr><tr><td>--terse</td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.</td></tr><tr><td>--echo</td><td>setting to true will echo the command line statement on the standard output.</td></tr><tr><td>--interactive</td><td>prompts you for the required options that are not already specified.</td></tr><tr><td>--jndilookupname</td><td>lookup name used by external container.</td></tr><tr><td>--restype</td><td>JNDI resource type which can be: topic or queue.</td></tr><tr><td>--factoryclass</td><td>class that creates the JNDI resource.</td></tr><tr><td>--enabled</td><td>determines whether the resource is enabled at runtime.</td></tr><tr><td>--description</td><td>text description of the JDBC connection pool.</td></tr><tr><td>--property</td><td>optional attribute name/value pairs for configuring the JNDI resource.</td></tr></table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.	--echo	setting to true will echo the command line statement on the standard output.	--interactive	prompts you for the required options that are not already specified.	--jndilookupname	lookup name used by external container.	--restype	JNDI resource type which can be: topic or queue.	--factoryclass	class that creates the JNDI resource.	--enabled	determines whether the resource is enabled at runtime.	--description	text description of the JDBC connection pool.	--property	optional attribute name/value pairs for configuring the JNDI resource.
--user	authorized domain application server administrative username.																														
--password	password to administer the domain application server.																														
--host	machine name where the domain application server is running.																														
--port	port number of the domain application server listening for administration requests.																														
--secure	if true, uses SSL/TLS to communicate with the domain application server.																														
--passwordfile	file containing the domain application server password.																														
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.																														
--echo	setting to true will echo the command line statement on the standard output.																														
--interactive	prompts you for the required options that are not already specified.																														
--jndilookupname	lookup name used by external container.																														
--restype	JNDI resource type which can be: topic or queue.																														
--factoryclass	class that creates the JNDI resource.																														
--enabled	determines whether the resource is enabled at runtime.																														
--description	text description of the JDBC connection pool.																														
--property	optional attribute name/value pairs for configuring the JNDI resource.																														
<b>OPERANDS</b>	<i>jndi_name</i> name of the JNDI resource to be created.																														



**EXAMPLES**    **EXAMPLE 1** Using the create-jndi-resource command

```
asadmin> create-jndi-resource --user admin1
--password adminadmin1 --host pigeon --port 5001
--jndilookupname sample_jndi --restype queue --factoryclass sampleClass
--description "this is a sample jndi resource" sample_jndi_resource
Command create-jndi-resource executed successfully
```

Where: sample\_jndi\_resource is the JNDI resource created.

**EXIT STATUS**    0    command executed successfully  
                  1    error in executing the command

**SEE ALSO**    delete-jndi-resource(1), list-jndi-resources(1)

## create-jvm-options(1)

<b>NAME</b>	create-jvm-options – creates the JVM options from the Java configuration or profiler elements
<b>SYNOPSIS</b>	<pre> <b>create-jvm-options</b> --user <i>admin_user</i>   [--password <i>admin_password</i>] [--host <i>localhost</i>] [--port <b>4848</b>]   [--secure -s] [--passwordfile <i>filename</i>] [--terse=false]   [--echo=false] [--interactive=true] [--profiler=false]   [<i>jvm_option_name=jvm_option_value</i>]   [:<i>jvm_option_name=jvm_option_value</i>]* </pre>
<b>DESCRIPTION</b>	<p>Creates the JVM options in the Java configuration or Profiler elements of the <code>domain.xml</code> file. You can enter more than one JVM option separated by a colon (:). If the JVM option starts with a dash (-) then use two dashes (--) before the operand to distinguish that JVM option is an operand and not an option. JVM options are used to record the settings needed to get a particular profiler going.</p> <p>You must restart the server for the newly created JVM options to take affect. Use the <code>start-domain</code> command to restart the server domain.</p>
<b>OPTIONS</b>	<pre> --user           authorized domain application server administrative                   username. --password       password to administer the domain application server. --host           machine name where the domain application server is running. --port           port number of the domain application server listening for                   administration requests. --secure         if true, uses SSL/TLS to communicate with the domain                   application server. --passwordfile   file containing the domain application server password. --terse          indicates that any output data must be very concise, typically                   avoiding human-friendly sentences and favoring                   well-formatted data for consumption by a script. Default is                   false. --echo           setting to true will echo the command line statement on the                   standard output. Default is false. --interactive    if set to true (default), only the required password options are                   prompted. --profiler       indicates if the JVM options is for the profiler. Profiler must                   exist for this option to be true. </pre>
<b>OPERANDS</b>	<pre> <i>jvm_option_name=jvm_option_value</i>   the left side of the equal sign (=) is the JVM   option name. The right side of the equal sign (=)   is the <i>jvm_option_value</i>. Additionally, you can   use ":" as a delimiter for more than one   jvm-option. If the jvm-option contains a ":", use </pre>

create-jvm-options(1)

the escape character \ to offset the ":" delimiter.

**EXAMPLES**    **EXAMPLE 1** Using create-jvm-options

```
asadmin> create-jvm-options --user admin --password adminadmin
--host localhost --port 4848 --profiler=false --DDebug=true:"-Xmx256m":
-Dcom.sun.aas.imqBin="\export\as7se\imq\bin"
Command create-jvm-options executed successfully
```

Where the JVM options are created. The double dash (—) is used between --profiler options and the operand because – indicated the end of the options and the following text is the operand. The double dash (—) is necessary here since there are single dashes (i.e., —DDebug) in the operand. To distinguish between the options and the operand, the double dash (—) is used.

**EXIT STATUS**    0    command executed successfully  
                  1    error in executing the command

**SEE ALSO**        delete-jvm-options(1)

## create-lifecycle-module(1)

<b>NAME</b>	create-lifecycle-module – adds a lifecycle module
<b>SYNOPSIS</b>	<pre> <b>create-lifecycle-module</b> --user <i>admin_user</i> [--password <i>admin_password</i>]   [--host <i>localhost</i>] [--port <b>4848</b>] [--secure -s]   [--passwordfile <i>filename</i>] [--terse=false] [--echo=false]   [--interactive=true] --classname <i>class_name</i> [--classpath <i>classpath</i>] [--loadorder <i>load_order</i>] [--failurefatal=false]   [--enabled=true] [--description <i>description</i>   ] [--property (<i>name=value</i>)[:<i>name=value</i>]*] <i>module_name</i> </pre>
<b>DESCRIPTION</b>	Creates the lifecycle. This command is supported in remote mode only.
<b>OPTIONS</b>	<pre> --user          authorized domain application server administrative                 username. --password      password to administer the domain application server. --host          machine name where the domain application server is running. --port          port number of the domain application server listening for                 administration requests. --secure        if true, uses SSL/TLS to communicate with the domain                 application server. --passwordfile  file containing the domain application server password. --terse         indicates that any output data must be very concise, typically                 avoiding human-friendly sentences and favoring                 well-formatted data for consumption by a script. Default is                 false. --echo         setting to true will echo the command line statement on the                 standard output. Default is false. --interactive   if set to true (default), only the required password options are                 prompted. --classname     fully qualified name of the startup class. --classpath     indicates where this module is actually located if it is not under                 applications-root. --loadorder     an integer value that can be used to force the order in which                 deployed lifecycle modules are loaded at server startup.                 Smaller numbered modules get loaded sooner. Order is                 unspecified if two or more lifecycle modules have the same                 load-order value. --failurefatal  if true indicates abort server startup if this module does not                 load properly. --enabled       determines whether the resource is enabled at runtime. --description   text description of the resource. </pre>

## create-lifecycle-module(1)

	<code>--property</code>	optional attribute name/value pairs for configuring the resource.
<b>OPERANDS</b>	<code>module_name</code>	unique identifier for the deployed server lifecycle event listener module.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> using create-lifecycle-module	
	<pre>asadmin&gt; create-lifecycle-module --user admin --password adminadmin --host fuyako --port 7070 --classname "com.acme.CustomSetup" --classpath "/export/customSetup" --loadorder 1 --failurefatal=true --description "this is a sample customSetup" --property rmi=Server="acme1\7070:timeout=30 customSetup Command create-lifecycle-module executed successfully</pre>	
	Where: <code>customSetup</code> is the lifecycle module created. The escape character ( <code>\</code> ) is used in the property option to distinguish the colons ( <code>:</code> ).	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<code>delete-lifecycle-module(1)</code> , <code>list-lifecycle-modules(1)</code>	

## create-mime(1)

<b>NAME</b>	create-mime – adds the MIME type
<b>SYNOPSIS</b>	<pre><b>create-mime</b>   --user <i>admin_user</i> [--password <i>admin_password</i>] [--host <i>localhost</i>]   [--port <b>4848</b>] [--passwordfile <i>filename</i>] [--secure   -s] [--instance   <i>instance_name</i>] --mimefile <i>filename</i> <i>mime_ID</i></pre>
<b>DESCRIPTION</b>	Adds the MIME type associated with the named server instance. The server determines the MIME type of a requested resource by invoking the type-by-extension directive in the <code>ObjectType</code> section of the <code>obj.conf</code> file. The type-by-extension function does not work if no MIME element has been defined in the server element.
<b>OPTIONS</b>	<pre>--user          administrative user associated for the instance. --password      administrative password corresponding to the administrative                 user. --host          host name of the machine hosting the administrative instance. --port          administrative port number associated with the administrative                 host. --passwordfile  file containing passwords appropriate for the command (e.g.,                 administrative instance). --secure        if true, uses SSL/TLS to communicate with the administrative                 instance. --instance      name of the instance. --mimefile      name of a MIME types file.</pre>
<b>OPERANDS</b>	<pre><i>mime_id</i>      internal name for the MIME types listing. It is used in a virtual-server                 element to define the MIME types used by the virtual server.</pre>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using create-mime</p> <pre>asadmin&gt; create-mime --user admin --password adminadmin --host fuyako --port 7070 --instance server Created Mime with id = sampleMIME</pre> <p>Where: <code>sampleMIME</code> is the name of the MIME created.</p>
<b>EXIT STATUS</b>	<pre>0    command executed successfully 1    error in executing the command</pre>
<b>INTERFACE EQUIVALENT</b>	HTTP Server node, MIME Type Files page
<b>SEE ALSO</b>	<code>delete-mime(1)</code> , <code>list-mimes(1)</code>

create-persistence-resource(1)

<b>NAME</b>	create-persistence-resource – registers the persistence resource																								
<b>SYNOPSIS</b>	<pre> <b>create-persistence-resource</b> --user <i>admin_user</i>     [--password <i>admin_password</i>] [--host <i>localhost</i>] [--port <b>4848</b>]     [--secure -s] [--passwordfile <i>filename</i>] [--terse=false]     [--echo=false] [--interactive=true]     [--jdbcjndiname <i>jdbc_jndiname</i>   --connectionpoolid <i>id</i>]     [--factoryclass <i>classname</i>] [--enabled=true] [--description <i>text</i>]     [--property (<i>name=value</i>)[:<i>name=value</i>]*] <i>jndi_name</i> </pre>																								
<b>DESCRIPTION</b>	<p>Registers the persistence resource. This command is supported in remote mode only.</p> <p>The --jdbcjndiname option and --connectionpoolid option are mutually exclusive; only one should be used.</p>																								
<b>OPTIONS</b>	<table border="0"> <tr> <td style="padding-right: 20px;">--user</td> <td>authorized domain application server administrative username.</td> </tr> <tr> <td>--password</td> <td>password to administer the domain application server.</td> </tr> <tr> <td>--host</td> <td>machine name where the domain application server is running.</td> </tr> <tr> <td>--port</td> <td>port number of the domain application server listening for administration requests.</td> </tr> <tr> <td>--secure</td> <td>if true, uses SSL/TLS to communicate with the domain application server.</td> </tr> <tr> <td>--passwordfile</td> <td>file containing the domain application server password.</td> </tr> <tr> <td>--terse</td> <td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td> </tr> <tr> <td>--echo</td> <td>setting to true will echo the command line statement on the standard output. Default is false.</td> </tr> <tr> <td>--interactive</td> <td>if set to true (default), only the required password options are prompted.</td> </tr> <tr> <td>--jdbcjndiname</td> <td>JDBC resource with which database connections are obtained. Must be the name of one of the pre-created JDBC resources.</td> </tr> <tr> <td>--connectionpoolid</td> <td>name of the JDBC connection pool. If two or more JDBC resource elements point to the same connection pool element, they will use the same pool connections at runtime.</td> </tr> <tr> <td>--factoryclass</td> <td>class that creates persistence manager instance.</td> </tr> </table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	--echo	setting to true will echo the command line statement on the standard output. Default is false.	--interactive	if set to true (default), only the required password options are prompted.	--jdbcjndiname	JDBC resource with which database connections are obtained. Must be the name of one of the pre-created JDBC resources.	--connectionpoolid	name of the JDBC connection pool. If two or more JDBC resource elements point to the same connection pool element, they will use the same pool connections at runtime.	--factoryclass	class that creates persistence manager instance.
--user	authorized domain application server administrative username.																								
--password	password to administer the domain application server.																								
--host	machine name where the domain application server is running.																								
--port	port number of the domain application server listening for administration requests.																								
--secure	if true, uses SSL/TLS to communicate with the domain application server.																								
--passwordfile	file containing the domain application server password.																								
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																								
--echo	setting to true will echo the command line statement on the standard output. Default is false.																								
--interactive	if set to true (default), only the required password options are prompted.																								
--jdbcjndiname	JDBC resource with which database connections are obtained. Must be the name of one of the pre-created JDBC resources.																								
--connectionpoolid	name of the JDBC connection pool. If two or more JDBC resource elements point to the same connection pool element, they will use the same pool connections at runtime.																								
--factoryclass	class that creates persistence manager instance.																								

## create-persistence-resource(1)

--enabled determines whether the resource is enabled at runtime or not.  
--description text description of the persistence resource.  
--property optional attribute name/value pairs for configuring the persistence resource.

**OPERANDS** *jndi\_name* JNDI name of the persistence resource.

### EXAMPLES **EXAMPLE 1** Using create-persistence-resource

```
asadmin> create-persistence-resource --user admin1 --password adminadmin1  
--jdbcjndiname sample_jndi_resource --factoryclass "com.pmf.class"  
sample_persistence_resource  
Command create-persistence-resource executed successfully
```

Where: *sample\_persistence\_resource* is the persistence manager factory resource created.

**EXIT STATUS** 0 command executed successfully  
1 error in executing the command

**SEE ALSO** delete-persistence-resource(1), list-persistence-resources(1)



<b>NAME</b>	create-profiler – creates the profiler element																										
<b>SYNOPSIS</b>	<pre> <b>create-profiler</b> --user <i>admin_user</i> [--password <i>admin_password</i>]   [--host <i>localhost</i>] [--port <b>4848</b>] [--secure -s]   [--passwordfile <i>filename</i>] [--terse=false] [--echo=false]   [--interactive=true] [--classpath <i>classpath</i>]   [--nativelibpath <i>native_library_path</i>] [--enabled=true]   [--property (<i>name=value</i>)[:<i>name=value</i>]*] <i>profiler_name</i> </pre>																										
<b>DESCRIPTION</b>	<p>Creates the profiler element. A server instance is tied to a particular profiler, by the profiler element in the Java configuration. Changing a profiler requires you to restart the server.</p> <p>This command is supported in remote mode only.</p>																										
<b>OPTIONS</b>	<table border="0"> <tr> <td style="vertical-align: top;">--user</td> <td>authorized domain application server administrative username.</td> </tr> <tr> <td style="vertical-align: top;">--password</td> <td>password to administer the domain application server.</td> </tr> <tr> <td style="vertical-align: top;">--host</td> <td>machine name where the domain application server is running.</td> </tr> <tr> <td style="vertical-align: top;">--port</td> <td>port number of the domain application server listening for administration requests.</td> </tr> <tr> <td style="vertical-align: top;">--secure</td> <td>if true, uses SSL/TLS to communicate with the domain application server.</td> </tr> <tr> <td style="vertical-align: top;">--passwordfile</td> <td>file containing the domain application server password.</td> </tr> <tr> <td style="vertical-align: top;">--terse</td> <td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td> </tr> <tr> <td style="vertical-align: top;">--echo</td> <td>setting to true will echo the command line statement on the standard output. Default is false.</td> </tr> <tr> <td style="vertical-align: top;">--interactive</td> <td>if set to true (default), only the required password options are prompted.</td> </tr> <tr> <td style="vertical-align: top;">--classpath</td> <td>Java classpath string that specifies the classes needed by the profiler.</td> </tr> <tr> <td style="vertical-align: top;">--nativelibpath</td> <td>automatically constructed to be a concatenation of the Application Server installation relative path for its native shared libraries, standard JRE native library path, the shell environment setting (LD_LIBRARY_PATH on UNIX) and any path that may be specified in the profile element.</td> </tr> <tr> <td style="vertical-align: top;">--enabled</td> <td>profiler is enabled by default.</td> </tr> <tr> <td style="vertical-align: top;">--property</td> <td>name/value pairs of provider specific attributes.</td> </tr> </table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	--echo	setting to true will echo the command line statement on the standard output. Default is false.	--interactive	if set to true (default), only the required password options are prompted.	--classpath	Java classpath string that specifies the classes needed by the profiler.	--nativelibpath	automatically constructed to be a concatenation of the Application Server installation relative path for its native shared libraries, standard JRE native library path, the shell environment setting (LD_LIBRARY_PATH on UNIX) and any path that may be specified in the profile element.	--enabled	profiler is enabled by default.	--property	name/value pairs of provider specific attributes.
--user	authorized domain application server administrative username.																										
--password	password to administer the domain application server.																										
--host	machine name where the domain application server is running.																										
--port	port number of the domain application server listening for administration requests.																										
--secure	if true, uses SSL/TLS to communicate with the domain application server.																										
--passwordfile	file containing the domain application server password.																										
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																										
--echo	setting to true will echo the command line statement on the standard output. Default is false.																										
--interactive	if set to true (default), only the required password options are prompted.																										
--classpath	Java classpath string that specifies the classes needed by the profiler.																										
--nativelibpath	automatically constructed to be a concatenation of the Application Server installation relative path for its native shared libraries, standard JRE native library path, the shell environment setting (LD_LIBRARY_PATH on UNIX) and any path that may be specified in the profile element.																										
--enabled	profiler is enabled by default.																										
--property	name/value pairs of provider specific attributes.																										

## create-profiler(1)

**OPERANDS** *profiler\_name* name of the profiler.

**EXAMPLES** **EXAMPLE 1** Using create-profiler

```
asadmin> create-profiler --user admin --passwordfile passwords.txt
--host localhost --port 4848 --classpath com.ipplanet.ias.profile.Profiler
--nativelibpath /u/home/lib --enabled=false
--property defaultuser=admin:password=adminadmin sample_profiler
Created Profiler with id = sample_profiler
```

Where: *sample\_profiler* is the profiler created.

**EXIT STATUS** 0 command executed successfully

1 error in executing the command

**SEE ALSO** delete-profiler(1)

create-resource-adapter-config(1)

<b>NAME</b>	create-resource-adapter-config – creates the configuration information in domain.xml for the connector module
<b>SYNOPSIS</b>	<b>create-resource-adapter-config</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true] [--threadpools <i>threadpoolids</i> ] [--property <i>name=value[:name=value]*</i> ] <i>raname</i>
<b>DESCRIPTION</b>	Creates configuration information for the connector module. This command can be executed prior to deploying a resource adapter, so that the configuration information is available at the time of deployment, or after deployment. If the resource adapter is created after deployment, the resource adapter is started. You must first create a threadpool, using the create-threadpool command, and then identify that threadpool value as the ID in the --threadpools option.  This command is supported in remote mode only.
<b>OPTIONS</b>	--user                  authorized domain application server administrative username.  --password              password to administer the domain application server.  --host                  machine name where the domain application server is running.  --port                  port number of the domain application server listening for administration requests.  --secure                if true, uses SSL/TLS to communicate with the domain application server.  --passwordfile          file containing the domain application server password.  --terse                 indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.  --echo                  setting to true will echo the command line statement on the standard output. Default is false.  --interactive           if set to true (default), only the required password options are prompted.  --threadpool            the threadpool ID from which the work manager gets the thread.  --property              configuration properties of the resource adapter java bean.
<b>OPERANDS</b>	<i>raname</i> the value kept in the resource-adapter-name in the domain.xml file.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using create-resource-adapter-config  asadmin> create-resource-adapter-config --username admin1 --password adminadmin myresourceadapter

## create-resource-adapter-config(1)

**EXAMPLE 1** Using create-resource-adapter-config *(Continued)*

Command create-resource-adapter-config executed successfully

**EXIT STATUS**

0	command executed successfully
1	error in executing the command

**SEE ALSO** create-threadpool(1), delete-resource-adapter-config(1), list-resource-adapter-configs(1)

<b>NAME</b>	create-ssl – Creates the SSL element in the HTTP listener, IIOp listener, or IIOp Service																						
<b>SYNOPSIS</b>	<pre> <b>create-ssl</b> --user <i>admin_user</i> [--password <i>admin_password</i>]   [--host <i>localhost</i>] [--port <b>4848</b>] [--secure -s]   [--passwordfile <i>filename</i>] [--terse=false] [--echo=false]   [--interactive=true]   --type [<b>http-listener</b> <b>iiop-listener</b> <b>iiop-service</b>]   --certname <i>cert_name</i> [--ssl2enabled=false]   [--ssl2ciphers <i>ssl_2_ciphers</i>] [--ssl3enabled=true]   [--ssl3tlsciphers <i>ssl3_tls_ciphers</i>] [--tlseabled=true]   [--tlscrollbackenabled=true] [--clientauthenabled=false]   [<i>listener_id</i>] </pre>																						
<b>DESCRIPTION</b>	<p>Creates the ssl element from the HTTP listener, IIOp listener, or IIOp service. The <i>listener_id</i> is not required if the --type option is <b>iiop-service</b>.</p> <p>This command is supported in remote mode only.</p>																						
<b>OPTIONS</b>	<table border="0"> <tr> <td style="padding-right: 10px;">--user</td> <td>authorized domain application server administrative username.</td> </tr> <tr> <td style="padding-right: 10px;">--password</td> <td>password to administer the domain application server.</td> </tr> <tr> <td style="padding-right: 10px;">--host</td> <td>machine name where the domain application server is running.</td> </tr> <tr> <td style="padding-right: 10px;">--port</td> <td>port number of the domain application server listening for administration requests.</td> </tr> <tr> <td style="padding-right: 10px;">--secure</td> <td>if true, uses SSL/TLS to communicate with the domain application server.</td> </tr> <tr> <td style="padding-right: 10px;">--passwordfile</td> <td>file containing the domain application server password.</td> </tr> <tr> <td style="padding-right: 10px;">--terse</td> <td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td> </tr> <tr> <td style="padding-right: 10px;">--echo</td> <td>setting to true will echo the command line statement on the standard output. Default is false.</td> </tr> <tr> <td style="padding-right: 10px;">--interactive</td> <td>if set to true (default), only the required password options are prompted.</td> </tr> <tr> <td style="padding-right: 10px;">--type</td> <td>type of service or listener that the SSL is created for. The type can be: <b>http-listener</b>, <b>iiop-listener</b>, and <b>iiop-service</b>.</td> </tr> <tr> <td style="padding-right: 10px;">--certname</td> <td>nickname of the server certificate in the certificate database or the PKCS#11 token. In the certificate, the</td> </tr> </table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	--echo	setting to true will echo the command line statement on the standard output. Default is false.	--interactive	if set to true (default), only the required password options are prompted.	--type	type of service or listener that the SSL is created for. The type can be: <b>http-listener</b> , <b>iiop-listener</b> , and <b>iiop-service</b> .	--certname	nickname of the server certificate in the certificate database or the PKCS#11 token. In the certificate, the
--user	authorized domain application server administrative username.																						
--password	password to administer the domain application server.																						
--host	machine name where the domain application server is running.																						
--port	port number of the domain application server listening for administration requests.																						
--secure	if true, uses SSL/TLS to communicate with the domain application server.																						
--passwordfile	file containing the domain application server password.																						
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																						
--echo	setting to true will echo the command line statement on the standard output. Default is false.																						
--interactive	if set to true (default), only the required password options are prompted.																						
--type	type of service or listener that the SSL is created for. The type can be: <b>http-listener</b> , <b>iiop-listener</b> , and <b>iiop-service</b> .																						
--certname	nickname of the server certificate in the certificate database or the PKCS#11 token. In the certificate, the																						

## create-ssl(1)

		name format is tokenname:nickname. Including the tokenname: part in this attribute is optional.
	<code>--ssl2enabled</code>	determines whether SSL2 is enabled.
	<code>--ssl2ciphers</code>	a comma separated list of the SSL2 ciphers used. Use the prefix + to enable or — to disable. Allowed values are: rc4, rc4export, rc2, rc2export, idea, des, desede3. If no value is specified, all supported ciphers are assumed to be enabled.
	<code>--ssl3enabled</code>	determines whether SSL3 is enabled.
	<code>--ssl3ciphers</code>	a comma separated list of the SSL3 ciphers used. Use the prefix + to enable or — to disable. Allowed values are: rsa_rc4_128_md5, rsa3des_sha, rsa_des_sha, rsa_rc4_40_md5, rsa_rc2_40_md5, rsa_null_md5. Allowed TSL values are: rsa_des_56_sha, rsa_rc4_56_sha. If no value is specified, all supported ciphers are assumed to be enabled.
	<code>--tlsenabled</code>	determines whether TLS is enabled.
	<code>--tlsrollbackenabled</code>	determines whether TLS rollback is enabled. TLS rollback should be enabled for Microsoft Internet Explorer 5.0 and 5.5.
	<code>--clientauthenabled</code>	determines whether SSL3 client authentication is performed on every request independent of ACL-based access control.
<b>OPERANDS</b>	<i>listener_ID</i>	the ID of the listener or service that the SSL is created for. This operand is not required if the <code>--type</code> option is <code>iiop-service</code> .
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using create-ssl	
	<pre>asadmin&gt; create-ssl --user admin --password adminadmin --host fuyako --port 7070 --type http-listener --certname sampleCert --ssl2enabled=true --ssl2ciphers rc4,rc2,des --ssl3enabled=false --ssl3tlsciphers rsa_rc4_128_md5,rsa3des_sha,rsa_des_sha, rsa_rc4_40_md5 --tlsenabled=false --tlsrollbackenabled=false --clientauthenabled=false http-listener-1 Created SSL in HTTP Listener</pre>	
	Where: SSL is created for <code>http-listener-1</code> .	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<code>delete-ssl(1)</code>	

<b>NAME</b>	create-threadpool – adds a threadpool
<b>SYNOPSIS</b>	<pre> <b>create-threadpool</b> --user <i>admin_user</i>   [--password <i>admin_password</i>] [--host <i>localhost</i>]   [--port 4848] [--secure -s] [--passwordfile <i>filename</i>]   [--terse=false] [--echo=false] [--interactive=true]   [--maxthreadpoolsize <i>max_thread_pool_size</i>] [--minthreadpoolsize   <i>min_thread_pool_size</i>] [--idletimeout <i>idle_thread_timeout_in_seconds</i>]   [--workqueues <i>number_work_queues</i>] <i>threadpool_id</i> </pre>
<b>DESCRIPTION</b>	<p>Creates a thread-pool with the specified name. You can specify maximum and minimum number of threads in the pool, the number of work queues, and the idle timeout of a thread. The created thread pool can be used for servicing IOP requests and for resource adapters to service work management requests. Please note that a created thread pool can be used in multiple resource adapters. This command is supported in remote mode only.</p>
<b>OPTIONS</b>	<pre> --user           authorized domain application server administrative                  username. --password       password to administer the domain application server. --host           machine name where the domain application server is                  running. --port           port number of the domain application server listening                  for administration requests. --secure         if true, uses SSL/TLS to communicate with the domain                  application server. --passwordfile   file containing the domain application server password. --terse          indicates that any output data must be very concise,                  typically avoiding human-friendly sentences and                  favoring well-formatted data for consumption by a                  script. Default is false. --echo           setting to true will echo the command line statement on                  the standard output. Default is false. --interactive     if set to true (default), only the required password                  options are prompted. --maxthreadpoolsize  maximum number of threads in the threadpool                  servicing requests in this queue. This is the upper bound                  on the number of threads that exist in the threadpool. --minthreadpoolsize  minimum number of threads in the threadpool servicing                  requests in this queue. These are created up front when                  the threadpool is instantiated. --idletimeout      idle threads are removed from the pool after this time. </pre>

## create-threadpool(1)

	<code>--workqueues</code>	identifies the total number of work queues serviced by this threadpool.
<b>OPERANDS</b>	<code>threadpool_id</code>	an ID for the work queue; for example, thread-pool-1, thread-pool-2, etc.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using create-threadpool <pre>asadmin&gt; create-threadpool --user admin1 --password adminadmin1 --maxthreadpoolsize 100 --minthreadpoolsize 20 --idletimeout 2 --workqueues 100 threadpool-1 Command create-threadpool executed successfully</pre>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	delete-threadpool(1), list-threadpools(1)	



<b>NAME</b>	create-virtual-server – adds the named virtual server
<b>SYNOPSIS</b>	<pre> <b>create-virtual-server</b> --user <i>admin_user</i> [--password <i>admin_password</i>]   [--host <i>localhost</i>] [--port <b>4848</b>] [--secure -s]   [--passwordfile <i>filename</i>] [--terse=false] [--echo=false]   [--interactive=true] --hosts <i>hosts</i> [--httplisteners <i>http_listeners</i>]   [--defaultwebmodule <i>default_web_module</i>] [--state <i>on</i>]   [--logfile <i>log_file</i>] [--property (<i>name=value</i>) [:<i>name=value</i>] *]   <i>virtual_server_id</i> </pre>
<b>DESCRIPTION</b>	<p>Creates the named virtual server. Virtualization in the Application Server allows multiple URL domains to be served by the same HTTP server process which is listening on multiple host addresses. If the application is available at two virtual servers, they still share the same physical resource pools.</p> <p>This command is supported in remote mode only.</p>
<b>OPTIONS</b>	<pre> --user          authorized domain application server administrative                 username. --password      password to administer the domain application server. --host          machine name where the domain application server is                 running. --port          port number of the domain application server listening                 for administration requests. --secure        if true, uses SSL/TLS to communicate with the domain                 application server. --passwordfile  file containing the domain application server password. --terse         indicates that any output data must be very concise,                 typically avoiding human-friendly sentences and favoring                 well-formatted data for consumption by a script. Default                 is false. --echo          setting to true will echo the command line statement on                 the standard output. Default is false. --interactive    if set to true (default), only the required password options                 are prompted. --hosts         a comma separated (,) list of values allowed in the host                 request header to select the current virtual server. Each                 virtual server that is configured to the same connection                 group must have a unique hosts value for that group. --httplisteners optional; a comma separated (,) list of HTTP listener IDs.                 Required only for a virtual server that is not the default                 virtual server. </pre>

## create-virtual-server(1)

	<code>--defaultwebmodule</code>	standalone web module associated with this virtual server by default.
	<code>--state</code>	determines whether a virtual server is active (on) or inactive (off or disabled). Default is active (on). When inactive, the virtual server does not service requests.
	<code>--logfile</code>	name of the file where the log has to be written to.
	<code>--property</code>	optional attributes name/value pairs for configuring the connection pool.
<b>OPERANDS</b>	<i>virtual_server_id</i>	identifies the unique ID for the virtual server to be created. This virtual server ID cannot begin with a number.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using create-virtual-server	
	<pre>asadmin&gt; create-virtual-server --user admin1 --password adminadmin1 --host pigeon --port 5001 --httplisteners http-listener-1 --defaultwebmodule simple --state on --logfile server.log --property User=admin:Password=admin --hosts sample1,sample2 sample_vs1</pre>	
	Command create-virtual-server executed successfully	
	Where sample_vs1 is the virtual server created.	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	delete-virtual-server(1), list-virtual-server(1)	

<b>NAME</b>	delete-acl – removes the access control list file
<b>SYNOPSIS</b>	<pre>delete-acl   --user admin_user [--password admin_password] [--host localhost]   [--port 4848] [--passwordfile filename] [--secure -s] [--instance   instance_name] acl_ID</pre>
<b>DESCRIPTION</b>	Gets the access control lists associated with the named server instance..
<b>OPTIONS</b>	<pre>--user          administrative user associated for the instance. --password      administrative password corresponding to the administrative                 user. --host          host name of the machine hosting the administrative instance. --port         administrative port number associated with the administrative                 host. --secure        indicates communication with the administrative instance in                 secured mode. --passwordfile  file containing passwords appropriate for the command (e.g.,                 administrative instance). --instance      name of the instance.</pre>
<b>OPERANDS</b>	<i>acl_ID</i> internal name for the ACL file listing. This ID is used in a virtual server element to define the ACL file used by the virtual server.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using delete-acl</p> <pre>asadmin&gt; delete-acl --user admin --password adminadmin --host fuyako --port 7070 --instance server Deleted ACL with id = sampleACL</pre> <p>Where: <i>sampleACL</i> is the ACL that is deleted.</p>
<b>EXIT STATUS</b>	<pre>0  command executed successfully 1  error in executing the command</pre>
<b>INTERFACE EQUIVALENT</b>	Access Control List page
<b>SEE ALSO</b>	create-acl(1), list-acl(1)

## delete-admin-object(1)

<b>NAME</b>	delete-admin-object – removes the administered object with the specified JNDI name																		
<b>SYNOPSIS</b>	<pre>delete-admin-object --user <i>admin_user</i> [--password <i>admin_password</i>]   [--host <i>localhost</i>] [--port 4848] [--secure -s]   [--passwordfile <i>filename</i>] [--terse=false] [--echo=false]   [--interactive=true] <i>jndi_name</i></pre>																		
<b>DESCRIPTION</b>	Removes the administered object with the specified JNDI name. This command is supported in remote mode only.																		
<b>OPTIONS</b>	<table><tr><td>--user</td><td>authorized domain application server administrative username.</td></tr><tr><td>--password</td><td>password to administer the domain application server.</td></tr><tr><td>--host</td><td>machine name where the domain application server is running.</td></tr><tr><td>--port</td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td>--passwordfile</td><td>file containing the domain application server password.</td></tr><tr><td>--terse</td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td></tr><tr><td>--echo</td><td>setting to true will echo the command line statement on the standard output. Default is false.</td></tr><tr><td>--interactive</td><td>if set to true (default), only the required password options are prompted.</td></tr></table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	--echo	setting to true will echo the command line statement on the standard output. Default is false.	--interactive	if set to true (default), only the required password options are prompted.
--user	authorized domain application server administrative username.																		
--password	password to administer the domain application server.																		
--host	machine name where the domain application server is running.																		
--port	port number of the domain application server listening for administration requests.																		
--secure	if true, uses SSL/TLS to communicate with the domain application server.																		
--passwordfile	file containing the domain application server password.																		
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																		
--echo	setting to true will echo the command line statement on the standard output. Default is false.																		
--interactive	if set to true (default), only the required password options are prompted.																		
<b>OPERANDS</b>	<i>jndi_name</i> JNDI name of the administered object to be deleted.																		
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using delete-admin-object</p> <p>The example listed in the add-admin-object command should be executed before attempting to execute this example:</p> <pre>asadmin&gt; delete-admin-objects --user admin --password admin123 jms/samplequeue</pre> <p>Deletes the previously created administration object with the JNDI name jms/sample.</p>																		
<b>EXIT STATUS</b>	<table><tr><td>0</td><td>command executed successfully</td></tr><tr><td>1</td><td>error in executing the command</td></tr></table>	0	command executed successfully	1	error in executing the command														
0	command executed successfully																		
1	error in executing the command																		
<b>SEE ALSO</b>	create-admin-object(1), list-admin-objects(1)																		

<b>NAME</b>	create-audit-module – removes the named audit-module
<b>SYNOPSIS</b>	<b>delete-audit-module</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true] <i>audit_module_name</i>
<b>DESCRIPTION</b>	Removes the named audit module. This command is supported in remote mode only.
<b>OPTIONS</b>	<p>--user                    authorized domain application server administrative username.</p> <p>--password               password to administer the domain application server.</p> <p>--host                    machine name where the domain application server is running.</p> <p>--port                    port number of the domain application server listening for administration requests.</p> <p>--secure                  if true, uses SSL/TLS to communicate with the domain application server.</p> <p>--passwordfile          file containing the domain application server password.</p> <p>--terse                   indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</p> <p>--echo                    setting to true will echo the command line statement on the standard output. Default is false.</p> <p>--interactive            if set to true (default), only the required password options are prompted.</p>
<b>OPERANDS</b>	<i>audit_module_name</i> name of the audit module to be deleted.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using delete-audit-module</p> <pre>asadmin&gt; delete-audit-module --user admin1 --password adminadmin1 --host pigeon --port 5001 sampleAuditModule Command delete-audit-module executed successfully</pre>
<b>EXIT STATUS</b>	<p>0    command executed successfully</p> <p>1    error in executing the command</p>
<b>SEE ALSO</b>	create-audit-module(1), list-audit-modules(1)

## delete-authdb(1)

<b>NAME</b>	delete-authdb – removes the authorized database																
<b>SYNOPSIS</b>	<pre><b>delete-authdb</b>   --user <i>admin_user</i> [--password <i>admin_password</i>] [--host <i>localhost</i>]   [--port <b>4848</b>] [--passwordfile <i>filename</i>] [--secure -s] [--instance   <i>instance_name</i>] --virtualserver <i>virtualserver_ID</i> <i>authdb_ID</i></pre>																
<b>DESCRIPTION</b>	Removes the authorized database associated with the named server instance.																
<b>OPTIONS</b>	<table><tr><td>--user</td><td>administrative user associated for the instance.</td></tr><tr><td>--password</td><td>administrative password corresponding to the administrative user.</td></tr><tr><td>--host</td><td>host name of the machine hosting the administrative instance.</td></tr><tr><td>--port</td><td>administrative port number associated with the administrative host.</td></tr><tr><td>--passwordfile</td><td>file containing passwords appropriate for the command (e.g., administrative instance).</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the administrative instance.</td></tr><tr><td>--instance</td><td>name of the instance.</td></tr><tr><td>--virtualserver</td><td>virtual server ID. It can also be referred to as the variable <code>\$id</code> in an <code>obj.conf</code> file. A virtual server ID cannot begin with a number.</td></tr></table>	--user	administrative user associated for the instance.	--password	administrative password corresponding to the administrative user.	--host	host name of the machine hosting the administrative instance.	--port	administrative port number associated with the administrative host.	--passwordfile	file containing passwords appropriate for the command (e.g., administrative instance).	--secure	if true, uses SSL/TLS to communicate with the administrative instance.	--instance	name of the instance.	--virtualserver	virtual server ID. It can also be referred to as the variable <code>\$id</code> in an <code>obj.conf</code> file. A virtual server ID cannot begin with a number.
--user	administrative user associated for the instance.																
--password	administrative password corresponding to the administrative user.																
--host	host name of the machine hosting the administrative instance.																
--port	administrative port number associated with the administrative host.																
--passwordfile	file containing passwords appropriate for the command (e.g., administrative instance).																
--secure	if true, uses SSL/TLS to communicate with the administrative instance.																
--instance	name of the instance.																
--virtualserver	virtual server ID. It can also be referred to as the variable <code>\$id</code> in an <code>obj.conf</code> file. A virtual server ID cannot begin with a number.																
<b>OPERANDS</b>	<i>authdb_id</i> user database name in the virtual server's ACL file.																
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using delete-authdb</p> <pre>asadmin&gt; delete-authdb --user admin --password adminadmin --host fuyako --port 7070 --instance serv Deleted AuthDB with id = sampleAuth</pre> <p>Where: <code>sampleAuth</code> is the authdb deleted.</p>																
<b>EXIT STATUS</b>	<table><tr><td>0</td><td>command executed successfully</td></tr><tr><td>1</td><td>error in executing the command</td></tr></table>	0	command executed successfully	1	error in executing the command												
0	command executed successfully																
1	error in executing the command																
<b>SEE ALSO</b>	create-authdb(1), list-authdbs(1)																

<b>NAME</b>	delete-auth-realm – removes the named authorized realm
<b>SYNOPSIS</b>	<b>delete-auth-realm</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true] <i>auth_realm_name</i>
<b>DESCRIPTION</b>	Removes the named authorized realm. This command is supported in remote mode only.
<b>OPTIONS</b>	<p>--user                    authorized domain application server administrative username.</p> <p>--password               password to administer the domain application server.</p> <p>--host                    machine name where the domain application server is running.</p> <p>--port                    port number of the domain application server listening for administration requests.</p> <p>--secure                  if true, uses SSL/TLS to communicate with the domain application server.</p> <p>--passwordfile           file containing the domain application server password.</p> <p>--terse                   indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</p> <p>--echo                    setting to true will echo the command line statement on the standard output. Default is false.</p> <p>--interactive            if set to true (default), only the required password options are prompted.</p>
<b>OPERANDS</b>	<i>auth_realm_name</i> name of this realm.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using delete-auth-realm</p> <pre>asadmin&gt; delete-auth-realm --user admin1 --passwordfile password --host pigeon --port 5001 db Command delete-auth-realm executed successfully</pre> <p>Where db is the auth realm deleted.</p>
<b>EXIT STATUS</b>	<p>0    command executed successfully</p> <p>1    error in executing the command</p>
<b>SEE ALSO</b>	create-auth-realm(1), list-auth-realms(1)

## delete-connector-connection-pool(1)

<b>NAME</b>	delete-connector-connection-pool – removes the specified connection pool																				
<b>SYNOPSIS</b>	<pre>delete-connector-connection-pool --user <i>admin_user</i>   [--password <i>admin_password</i>] [--host <i>localhost</i>]   [--port 4848] [--secure -s] [--passwordfile <i>filename</i>]   [--terse=false] [--echo=false] [--interactive=true]   [--cascade=false] <i>pool_name</i></pre>																				
<b>DESCRIPTION</b>	removes the specified connection pool. This command is supported in remote mode only.																				
<b>OPTIONS</b>	<table><tr><td>--user</td><td>authorized domain application server administrative username.</td></tr><tr><td>--password</td><td>password to administer the domain application server.</td></tr><tr><td>--host</td><td>machine name where the domain application server is running.</td></tr><tr><td>--port</td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td>--passwordfile</td><td>file containing the domain application server password.</td></tr><tr><td>--terse</td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td></tr><tr><td>--echo</td><td>setting to true will echo the command line statement on the standard output. Default is false.</td></tr><tr><td>--interactive</td><td>if set to true (default), only the required password options are prompted.</td></tr><tr><td>--cascade</td><td>if set to to true, the pool and all the connector resources associated with the pool are deleted. If set to false (default), the deletion of the pool fails if there are any resources associated with the pool. Either the resource has to be deleted explicitly or the option must be set to true.</td></tr></table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	--echo	setting to true will echo the command line statement on the standard output. Default is false.	--interactive	if set to true (default), only the required password options are prompted.	--cascade	if set to to true, the pool and all the connector resources associated with the pool are deleted. If set to false (default), the deletion of the pool fails if there are any resources associated with the pool. Either the resource has to be deleted explicitly or the option must be set to true.
--user	authorized domain application server administrative username.																				
--password	password to administer the domain application server.																				
--host	machine name where the domain application server is running.																				
--port	port number of the domain application server listening for administration requests.																				
--secure	if true, uses SSL/TLS to communicate with the domain application server.																				
--passwordfile	file containing the domain application server password.																				
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																				
--echo	setting to true will echo the command line statement on the standard output. Default is false.																				
--interactive	if set to true (default), only the required password options are prompted.																				
--cascade	if set to to true, the pool and all the connector resources associated with the pool are deleted. If set to false (default), the deletion of the pool fails if there are any resources associated with the pool. Either the resource has to be deleted explicitly or the option must be set to true.																				
<b>OPERANDS</b>	<i>pool_name</i> name of the connection pool to be deleted.																				
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using delete-connector-connection-pool</p> <p>Execute the example described for create-connector-connection-pool command before trying out this example:</p> <pre>asadmin&gt; delete-connector-connection-pool --user admin --password adminadmin jms/qConnPool Command delete-connector-connection-pool executed successfully</pre>																				



delete-connector-connection-pool(1)

**EXIT STATUS** 0 command executed successfully  
1 error in executing the command

**SEE ALSO** create-connector-connection-pool(1),  
list-connector-connection-pools(1)

## delete-connector-resource(1)

<b>NAME</b>	delete-connector-resource – removes the named connector resource																		
<b>SYNOPSIS</b>	<pre><b>delete-connector-resource</b> --user <i>admin_user</i>     [--password <i>admin_password</i>] [--host <i>localhost</i>] [--port <b>4848</b>]     [--secure -s] [--passwordfile <i>filename</i>] [--terse=false]     [--echo=false] [--interactive=true] <i>connector_resource_name</i></pre>																		
<b>DESCRIPTION</b>	Removes the named resource. This command is supported in remote mode only.																		
<b>OPTIONS</b>	<table><tr><td>--user</td><td>authorized domain application server administrative username.</td></tr><tr><td>--password</td><td>password to administer the domain application server.</td></tr><tr><td>--host</td><td>machine name where the domain application server is running.</td></tr><tr><td>--port</td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td>--passwordfile</td><td>file containing the domain application server password.</td></tr><tr><td>--terse</td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td></tr><tr><td>--echo</td><td>setting to true will echo the command line statement on the standard output. Default is false.</td></tr><tr><td>--interactive</td><td>if set to true (default), only the required password options are prompted.</td></tr></table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	--echo	setting to true will echo the command line statement on the standard output. Default is false.	--interactive	if set to true (default), only the required password options are prompted.
--user	authorized domain application server administrative username.																		
--password	password to administer the domain application server.																		
--host	machine name where the domain application server is running.																		
--port	port number of the domain application server listening for administration requests.																		
--secure	if true, uses SSL/TLS to communicate with the domain application server.																		
--passwordfile	file containing the domain application server password.																		
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																		
--echo	setting to true will echo the command line statement on the standard output. Default is false.																		
--interactive	if set to true (default), only the required password options are prompted.																		
<b>OPERANDS</b>	<i>connector_resource_name</i> name of the connector resource to be deleted.																		
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the delete-connector-resource command</p> <p>Execute the example described for <code>create-connector-resource</code> command before trying out this example:</p> <pre>asadmin&gt; delete-connector-resource --user admin1 --password adminadmin1 --host pigeon --port 5001 jms/qConnFactory Command delete-connector-resource executed successfully</pre> <p>This will delete the previously created connector resource <code>jms/qConnPool</code>.</p>																		
<b>EXIT STATUS</b>	<table><tr><td>0</td><td>command executed successfully</td></tr><tr><td>1</td><td>error in executing the command</td></tr></table>	0	command executed successfully	1	error in executing the command														
0	command executed successfully																		
1	error in executing the command																		
<b>SEE ALSO</b>	<code>create-connector-resource(1)</code> , <code>list-connector-resources(1)</code>																		

delete-connector-security-map(1)

<b>NAME</b>	delete-connector-security-map – deletes the named security map for the given connector connection pool
<b>SYNOPSIS</b>	<b>delete-connector-security-map</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true] --poolname <i>connector_connection_pool_name mapname</i>
<b>DESCRIPTION</b>	Deletes the named security map for the given connector connection pool. This command is supported in remote mode only.
<b>OPTIONS</b>	<p>--user                   authorized domain application server administrative username.</p> <p>--password               password to administer the domain application server.</p> <p>--host                   machine name where the domain application server is running.</p> <p>--port                   port number of the domain application server listening for administration requests.</p> <p>--secure                 if true, uses SSL/TLS to communicate with the domain application server.</p> <p>--passwordfile          file containing the domain application server password.</p> <p>--terse                  indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</p> <p>--echo                  setting to true will echo the command line statement on the standard output. Default is false.</p> <p>--interactive            if set to true (default), only the required password options are prompted.</p> <p>--poolname               connector connection pool name for which the security map that is to be deleted belongs to.</p>
<b>OPERANDS</b>	<i>mapname</i> name of the security map to be deleted.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using delete-connector-security-map <pre>asadmin&gt; delete-connector-security-map --user admin --password adminadmin --poolname connector-pool1 securityMap1 Command delete-connector-security-map executed successfully</pre>
<b>EXIT STATUS</b>	<p>0    command executed successfully</p> <p>1    error in executing the command</p>

delete-connector-security-map(1)

**SEE ALSO** | create-connector-security-map(1), list-connector-security-maps(1),  
update-connector-security-map(1)

<b>NAME</b>	delete-custom-resource – removes the custom resource																		
<b>SYNOPSIS</b>	<b>delete-custom-resource</b> <i>--user admin_user</i> [ <i>--password admin_password</i> ] [ <i>--host localhost</i> ] [ <i>--port 4848</i> ] [ <i>--secure -s</i> ] [ <i>--passwordfile filename</i> ] [ <i>--terse=false</i> ] [ <i>--echo=false</i> ] [ <i>--interactive=true</i> ] <i>jndi_name</i>																		
<b>DESCRIPTION</b>	Removes the custom resource. This command is supported in remote mode only.																		
<b>OPTIONS</b>	<table><tr><td><i>--user</i></td><td>authorized domain application server administrative username.</td></tr><tr><td><i>--password</i></td><td>password to administer the domain application server.</td></tr><tr><td><i>--host</i></td><td>machine name where the domain application server is running.</td></tr><tr><td><i>--port</i></td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td><i>--secure</i></td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td><i>--passwordfile</i></td><td>file containing the domain application server password.</td></tr><tr><td><i>--terse</i></td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td></tr><tr><td><i>--echo</i></td><td>setting to true will echo the command line statement on the standard output. Default is false.</td></tr><tr><td><i>--interactive</i></td><td>if set to true (default), only the required password options are prompted.</td></tr></table>	<i>--user</i>	authorized domain application server administrative username.	<i>--password</i>	password to administer the domain application server.	<i>--host</i>	machine name where the domain application server is running.	<i>--port</i>	port number of the domain application server listening for administration requests.	<i>--secure</i>	if true, uses SSL/TLS to communicate with the domain application server.	<i>--passwordfile</i>	file containing the domain application server password.	<i>--terse</i>	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	<i>--echo</i>	setting to true will echo the command line statement on the standard output. Default is false.	<i>--interactive</i>	if set to true (default), only the required password options are prompted.
<i>--user</i>	authorized domain application server administrative username.																		
<i>--password</i>	password to administer the domain application server.																		
<i>--host</i>	machine name where the domain application server is running.																		
<i>--port</i>	port number of the domain application server listening for administration requests.																		
<i>--secure</i>	if true, uses SSL/TLS to communicate with the domain application server.																		
<i>--passwordfile</i>	file containing the domain application server password.																		
<i>--terse</i>	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																		
<i>--echo</i>	setting to true will echo the command line statement on the standard output. Default is false.																		
<i>--interactive</i>	if set to true (default), only the required password options are prompted.																		
<b>OPERANDS</b>	<i>jndi_name</i> JNDI name of the custom resource to be deleted.																		
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using delete-custom-resource</p> <pre>asadmin&gt; delete-custom-resource --user admin1 --password adminadmin1 --host pigeon --port 5001 sample_custom_resource Command delete-custom-resource executed successfully</pre> <p>Where <i>sample_custom_resource</i> is the custom resource deleted.</p>																		
<b>EXIT STATUS</b>	0 command executed successfully 1 error in executing the command																		
<b>SEE ALSO</b>	create-custom-resource(1), list-custom-resources(1)																		

## delete-domain(1)

<b>NAME</b>	delete-domain – deletes the given domain
<b>SYNOPSIS</b>	<b>delete-domain</b> [ <b>--terse=false</b> ] [ <b>--echo=false</b> ] [ <b>--domaindir</b> <i>install_dir/domains</i> ] <i>domain_name</i>
<b>DESCRIPTION</b>	delete-domain deletes the specified domain. The domain must already exist and must be stopped. This command is supported in local mode only.
<b>OPTIONS</b>	<b>--domaindir</b> directory where the domain is to be deleted. If specified, path must be accessible in the filesystem. If not specified, the domain in the default <i>install_dir/domains</i> directory is deleted. <b>--terse</b> indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false. <b>--echo</b> setting to true will echo the command line statement on the standard output. Default is false.
<b>OPERANDS</b>	<i>domain_name</i> name of the domain. Must be a unique name.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using delete-domain asadmin> <b>delete-domain sampleDomain</b> deleted domain sampleDomain successfully  Where: the sampleDomain domain is deleted.
<b>EXIT STATUS</b>	0 command executed successfully 1 error in executing the command
<b>SEE ALSO</b>	create-domain(1), start-domain(1), stop-domain(1), list-domains(1)

<b>NAME</b>	delete-file-user – removes the named file user
<b>SYNOPSIS</b>	<b>delete-file-user</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true] [--authrealmname <i>auth_realm_name</i> ] <i>user_name</i>
<b>DESCRIPTION</b>	Deletes the entry in the keyfile with the specified username. If the <i>auth_realm_name</i> is not specified, an entry is created in the default keyfile. If <i>auth_realm_name</i> is specified, an entry is created in the keyfile where the auth-realm name in the <i>domain.xml</i> file points to.  This command is supported in remote mode only.
<b>OPTIONS</b>	--user                    authorized domain application server administrative username.  --password              password to administer the domain application server.  --host                    machine name where the domain application server is running.  --port                    port number of the domain application server listening for administration requests.  --secure                  if true, uses SSL/TLS to communicate with the domain application server.  --passwordfile          file containing the domain application server password.  --terse                    indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.  --echo                    setting to true will echo the command line statement on the standard output. Default is false.  --interactive            if set to true (default), only the required password options are prompted.  --authrealmname        name, in the <i>domain.xml</i> file, where you have different stores for file auth realm.
<b>OPERANDS</b>	<i>user_name</i> name of file user to be deleted.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using the delete-file-user command  It is assumed that an authority realm has already been created using the create-auth-realm command.  <pre>asadmin&gt; delete-file-user --user admin1 --password adminadmin1 --host pigeon --port 5001 --authrealmname auth-realm1 sample_user Command delete-file-user executed successfully</pre>

## delete-file-user(1)

**EXAMPLE 1** Using the delete-file-user command     *(Continued)*

Where: the `sample_user` is the file user deleted.

**EXIT STATUS**

0	command executed successfully
1	error in executing the command

**SEE ALSO** `create-file-user(1)`, `list-file-users(1)`, `update-file-user(1)`,  
`list-file-groups(1)`



<b>NAME</b>	delete-http-listener – removes the HTTP listener
<b>SYNOPSIS</b>	<b>delete-http-listener</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true] <i>httplistener_ID</i>
<b>DESCRIPTION</b>	Removes the HTTP listeners. This command is supported in remote mode only.
<b>OPTIONS</b>	<p>--user                    authorized domain application server administrative username.</p> <p>--password               password to administer the domain application server.</p> <p>--host                    machine name where the domain application server is running.</p> <p>--port                    port number of the domain application server listening for administration requests.</p> <p>--secure                  if true, uses SSL/TLS to communicate with the domain application server.</p> <p>--passwordfile          file containing the domain application server password.</p> <p>--terse                   indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</p> <p>--echo                    setting to true will echo the command line statement on the standard output. Default is false.</p> <p>--interactive            if set to true (default), only the required password options are prompted.</p>
<b>OPERANDS</b>	<i>listener_id</i> listener ID of the HTTP listener.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using delete-http-listener</p> <pre>asadmin&gt; delete-http-listener --user admin1 --password adminadmin1 --host pigeon --port 5001 sampleListener Deleted http listener with id = sampleListener</pre> <p>Where: <i>sampleListener</i> is the HTTP listener deleted.</p>
<b>EXIT STATUS</b>	<p>0    command executed successfully</p> <p>1    error in executing the command</p>
<b>SEE ALSO</b>	create-http-listener(1), list-http-listeners(1)

## delete-http-qos(1)

<b>NAME</b>	delete-http-qos – removes the quality of service parameter
<b>SYNOPSIS</b>	<b>delete-http-qos</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--passwordfile <i>filename</i> ] [--secure   -s] [--virtualserver <i>virtual_server_ID</i> ] <i>instance_name</i>
<b>DESCRIPTION</b>	Removes the quality of service parameter associated with the named server instance.
<b>OPTIONS</b>	--user administrative user associated for the instance. --password administrative password corresponding to the administrative user. --host host name of the machine hosting the administrative instance. --port administrative port number associated with the administrative host. --passwordfile file containing passwords appropriate for the command (e.g., administrative instance). --secure if true, uses SSL/TLS to communicate with the administrative instance. --virtualserver virtual server ID. It can also be referred to as the variable <i>\$id</i> in an <i>obj.conf</i> file. A virtual server ID cannot begin with a number.
<b>OPERANDS</b>	<i>instance_name</i> name of the instance.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using delete-http-qos asadmin> <b>delete-http-qos</b> --user admin --password adminadmin --host fuyako --port 7070 --virtualserver Deleted HTTP QOS with id = server1  Where: HTTP QOS is deleted for virtual server <i>server1</i> and instance name <i>server1</i> .
<b>EXIT STATUS</b>	0 command executed successfully 1 error in executing the command
<b>INTERFACE EQUIVALENT</b>	Server instance, HTTP Server Virtual Servers, Instance QOS page for the server instance
<b>SEE ALSO</b>	create-http-qos(1)

<b>NAME</b>	delete-iiop-listener – removes the IIOP listener
<b>SYNOPSIS</b>	<b>delete-iiop-listener</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false ] [--echo=false ] [--interactive=true ] <i>listener_ID</i>
<b>DESCRIPTION</b>	Removes the IIOP listener. This command is supported in remote mode only.
<b>OPTIONS</b>	<p>--user                    authorized domain application server administrative username.</p> <p>--password               password to administer the domain application server.</p> <p>--host                    machine name where the domain application server is running.</p> <p>--port                    port number of the domain application server listening for administration requests.</p> <p>--secure                  if true, uses SSL/TLS to communicate with the domain application server.</p> <p>--passwordfile          file containing the domain application server password.</p> <p>--terse                   indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</p> <p>--echo                    setting to true will echo the command line statement on the standard output. Default is false.</p> <p>--interactive            if set to true (default), only the required password options are prompted.</p>
<b>OPERANDS</b>	<i>listener_id</i> unique identifier for the IIOP listener to be deleted.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using delete-iiop-listener</p> <pre>asadmin&gt; delete-iiop-listener --user admin --password adminadmin --host fuyako --port 7070 sample_iiop_listener Command delete-iiop-listener executed successfully</pre> <p>Where: <i>sample_iiop_listener</i> is the IIOP listener deleted.</p>
<b>EXIT STATUS</b>	<p>0    command executed successfully</p> <p>1    error in executing the command</p>
<b>SEE ALSO</b>	create-iiop-listener(1), list-iiop-listeners(1)

## delete-instance(1)

<b>NAME</b>	delete-instance – deletes the instance that is not running.
<b>SYNOPSIS</b>	<b>delete-instance</b> [--user <i>admin_user</i> ] [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <i>4848</i> ] [--local=false] [--domain <i>domain_name</i> ] [--passwordfile <i>filename</i> ] [--secure -s] <i>instance_name</i>
<b>DESCRIPTION</b>	Use the delete-instance command to delete the instance that you specify. The delete-instance command can be run both locally and remotely. To delete the instance locally, not requiring the administration server to be up and running, specify the --local option. To delete the instance remotely, the administration server must be running on the hostname and port number specified. The user authenticates using the password identified for the administration server. Additionally, the instance must already exist within the domain served by the administration server. Use this command with discretion since it is destructive and there is no undo.
<b>OPTIONS</b>	--user administrative user associated for the instance. --password administrative password corresponding to the administrative user. --host host name of the machine hosting the administrative instance. --port administrative port number associated with the administrative host. --domain name of the domain. --local determines if the command should delegate the request to administrative instance or run locally. --passwordfile file containing passwords appropriate for the command (e.g., administrative instance). --secure if true, SSL/TLS to communicate with the administrative instance.
<b>OPERANDS</b>	<i>instance_name</i> name of the instance to be deleted.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using delete-instance in local mode <pre>asadmin&gt; delete-instance --domain domain1 server1 Deleted Instance server1 successfully</pre> <p>Where: the server1 instance for the domain1 domain is deleted on the local machine.</p> <b>EXAMPLE 2</b> Using delete-instance in remote mode <pre>asadmin&gt; delete-instance --user admin --passwordfile passwords.txt --host localhost --port 4848 ser Deleted Instance server1 successfully</pre>

delete-instance(1)

**EXAMPLE 2** Using delete-instance in remote mode (Continued)

Where: the server1 instance for the domain associated with the specified user, passwords in the password file, host, and port number is deleted on the remote machine.

**EXIT STATUS**

0	command executed successfully
1	error in executing the command

**INTERFACE EQUIVALENT** Server Instance page

**SEE ALSO** create-instance(1), start-instance(1), stop-instance(1), restart-instance(1)

## delete-javamail-resource(1)

<b>NAME</b>	delete-javamail-resource – removes the JavaMail resource
<b>SYNOPSIS</b>	<b>delete-javamail-resource</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive] <i>jndi_name</i>
<b>DESCRIPTION</b>	Removes the JavaMail resource. This command is supported in remote mode only.
<b>OPTIONS</b>	--user authorized domain application server administrative username. --password password to administer the domain application server. --host machine name where the domain application server is running. --port port number of the domain application server listening for administration requests. --secure if true, uses SSL/TLS to communicate with the domain application server. --passwordfile file containing the domain application server password. --terse indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. --echo setting to true will echo the command line statement on the standard output. --interactive prompts you for the required options that are not already specified.
<b>OPERANDS</b>	<i>jndi_name</i> JNDI name of the JavaMail resource to be deleted.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using delete-javamail-resource asadmin> delete-javamail-resource --user admin --password adminadmin --host fuyako --port 7070 mail/MyMailSession Command delete-javamail-resource executed successfully  Where: mail/MyMailSession is the JavaMail resource deleted.
<b>EXIT STATUS</b>	0 command executed successfully 1 error in executing the command
<b>SEE ALSO</b>	create-javamail-resource(1), list-javamail-resources(1)

<b>NAME</b>	delete-jdbc-connection-pool – removes the JDBC connection pool
<b>SYNOPSIS</b>	<pre>delete-jdbc-connection-pool --user admin_user   [--password admin_password] [--host localhost] [--port 4848]   [--secure -s] [--passwordfile filename] [--terse=false]   [--echo=false] [--interactive] [--cascade=false]   connection_pool_ID</pre>
<b>DESCRIPTION</b>	Removes the JDBC connection pool. This command is supported in remote mode only.
<b>OPTIONS</b>	<pre>--user          authorized domain application server administrative                   username.  --password      password to administer the domain application server.  --host         machine name where the domain application server is running.  --port        port number of the domain application server listening for                   administration requests.  --secure       if true, uses SSL/TLS to communicate with the domain                   application server.  --passwordfile file containing the domain application server password.  --terse       indicates that any output data must be very concise, typically                   avoiding human-friendly sentences and favoring                   well-formatted data for consumption by a script.  --echo        setting to true will echo the command line statement on the                   standard output.  --interactive  prompts you for the required options that are not already                   specified.  --cascade     If set to true, deletes all the connector resources associated with                   the pool, apart from the pool itself. If set to false (default), the                   deletion of the pool fails if there are any resources associated                   with the pool. Either the resource has to be deleted explicitly, or                   set the option to true.</pre>
<b>OPERANDS</b>	<i>connection_pool_id</i> name of the JDBC connection pool to be deleted.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the delete-jdbc-connection-pool command</p> <pre>asadmin&gt; delete-jdbc-connection-pool --user admin --password adminadmin --host fuyako port 7070 XA_connection_pool Deleted the JDBC connection pool resource with id = XA_connection_pool</pre> <p>Where: the XA_connection_pool resource is deleted.</p>
<b>EXIT STATUS</b>	<pre>0  command executed successfully 1  error in executing the command</pre>

delete-jdbc-connection-pool(1)

**SEE ALSO** | `create-jdbc-connection-pool(1)`, `list-jdbc-connection-pools(1)`



<b>NAME</b>	delete-jdbc-resource – removes the JDBC resource
<b>SYNOPSIS</b>	<b>delete-jdbc-resource</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true] <i>jndi_name</i>
<b>DESCRIPTION</b>	Removes the JDBC resource. This command is supported in remote mode only.
<b>OPTIONS</b>	<p>--user                authorized domain application server administrative username.</p> <p>--password           password to administer the domain application server.</p> <p>--host                machine name where the domain application server is running.</p> <p>--port                port number of the domain application server listening for administration requests.</p> <p>--secure              if true, uses SSL/TLS to communicate with the domain application server.</p> <p>--passwordfile       file containing the domain application server password.</p> <p>--terse               indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.</p> <p>--echo                setting to true will echo the command line statement on the standard output.</p> <p>--interactive         prompts you for the required options that are not already specified.</p>
<b>OPERANDS</b>	<i>jndi_name</i> name of the JDBC resource to be deleted.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the delete-jdbc-resource command</p> <pre>asadmin&gt; delete-jdbc-resource --user admin1 --password adminadmin1 --host pigeon --port 5001 sample_jdbc_resource Command delete-jdbc-resource executed successfully</pre> <p>Where: <i>sample_jdbc_resource</i> is the resource that is deleted.</p>
<b>EXIT STATUS</b>	<p>0    command executed successfully</p> <p>1    error in executing the command</p>
<b>SEE ALSO</b>	create-jdbc-resource(1), list-jdbc-resources(1)

## delete-jmsdest(1)

<b>NAME</b>	delete-jmsdest – destroys the physical destination																				
<b>SYNOPSIS</b>	<pre>delete-jmsdest --user <i>admin_user</i> [--password <i>admin_password</i>]   [--host <i>localhost</i>] [--port <i>4848</i>] [--secure -s]   [--passwordfile <i>filename</i>] [--terse=false] [--echo=false]   [--interactive] --desttype -T <i>topic queue dest_name</i></pre>																				
<b>DESCRIPTION</b>	Destroys the physical destinations. This command is supported in remote mode only.																				
<b>OPTIONS</b>	<table><tr><td>--user</td><td>authorized domain application server administrative username.</td></tr><tr><td>--password</td><td>password to administer the domain application server.</td></tr><tr><td>--host</td><td>machine name where the domain application server is running.</td></tr><tr><td>--port</td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td>--passwordfile</td><td>file containing the domain application server password.</td></tr><tr><td>--terse</td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.</td></tr><tr><td>--echo</td><td>setting to true will echo the command line statement on the standard output.</td></tr><tr><td>--interactive</td><td>prompts you for the required options that are not already specified.</td></tr><tr><td>--desttype</td><td>type of JMS destination. Valid values are <i>topic</i>, and <i>queue</i>.</td></tr></table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.	--echo	setting to true will echo the command line statement on the standard output.	--interactive	prompts you for the required options that are not already specified.	--desttype	type of JMS destination. Valid values are <i>topic</i> , and <i>queue</i> .
--user	authorized domain application server administrative username.																				
--password	password to administer the domain application server.																				
--host	machine name where the domain application server is running.																				
--port	port number of the domain application server listening for administration requests.																				
--secure	if true, uses SSL/TLS to communicate with the domain application server.																				
--passwordfile	file containing the domain application server password.																				
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.																				
--echo	setting to true will echo the command line statement on the standard output.																				
--interactive	prompts you for the required options that are not already specified.																				
--desttype	type of JMS destination. Valid values are <i>topic</i> , and <i>queue</i> .																				
<b>OPERANDS</b>	<table><tr><td><i>dest_name</i></td><td>name of the JMS destination. Valid value is any name that can be a Java identifier.</td></tr></table>	<i>dest_name</i>	name of the JMS destination. Valid value is any name that can be a Java identifier.																		
<i>dest_name</i>	name of the JMS destination. Valid value is any name that can be a Java identifier.																				
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using delete-jmsdest</p> <pre>asadmin&gt; delete-jmsdest --user admin --password adminadmin --host localhost --port 4848 --desttype queue PhysicalQueue Command delete-jmsdest executed successfully</pre>																				
<b>EXIT STATUS</b>	<table><tr><td>0</td><td>command executed successfully</td></tr><tr><td>1</td><td>error in executing the command</td></tr></table>	0	command executed successfully	1	error in executing the command																
0	command executed successfully																				
1	error in executing the command																				
<b>SEE ALSO</b>	create-jmsdest(1), list-jmsdest(1)																				

<b>NAME</b>	delete-jmsobj – destroys the named object
<b>SYNOPSIS</b>	<b>delete-jmsobj</b> <b>--instance</b> <i>instance_name</i> <b>--jndilookupname</b>   <b>-l</b> <i>jndi_lookup_name</i>
<b>DESCRIPTION</b>	Destroys the named destinations.
<b>OPTIONS</b>	<b>--instance</b> the name of the instance.  <b>--jndilookupname</b>
<b>EXAMPLES</b>	asadmin% <b>delete-jmsobj --instance server1 --jndilookup</b>
<b>INTERFACE EQUIVALENT</b>	unknown
<b>SEE ALSO</b>	create-jmsobj(1) list-jmsobj(1)

## delete-jms-resource(1)

<b>NAME</b>	delete-jms-resource – removes the JMS resource
<b>SYNOPSIS</b>	<pre>delete-jms-resource --user admin_user   [--password admin_password] [--host localhost] [--port 4848]   [--secure -s] [--passwordfile filename] [--terse=false]   [--echo=false] [--interactive=true] jndi_name</pre>
<b>DESCRIPTION</b>	Removes the JMS resource. This command is supported in remote mode only.
<b>OPTIONS</b>	<p>--user authorized domain application server administrative username.</p> <p>--password password to administer the domain application server.</p> <p>--host machine name where the domain application server is running.</p> <p>--port port number of the domain application server listening for administration requests.</p> <p>--secure if true, uses SSL/TLS to communicate with the domain application server.</p> <p>--passwordfile file containing the domain application server password.</p> <p>--terse indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.</p> <p>--echo setting to true will echo the command line statement on the standard output.</p> <p>--interactive prompts you for the required options that are not already specified.</p>
<b>OPERANDS</b>	<i>jndi_name</i> JNDI name of the JMS resource to be deleted.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the delete-jms-resource command</p> <pre>asadmin&gt; delete-jms-resource --user admin1 --password adminadmin1 --host pigeon --port 5001 sample_jms_resource Command delete-jms-resource executed successfully</pre> <p>Where: <i>sample_jms_resource</i> is the resource that is deleted.</p>
<b>EXIT STATUS</b>	<p>0 command executed successfully</p> <p>1 error in executing the command</p>
<b>SEE ALSO</b>	create-jms-resource(1), list-jms-resources(1)

<b>NAME</b>	delete-jndi-resource – removes the JNDI resource
<b>SYNOPSIS</b>	<pre>delete-jndi-resource   --user admin_user [--password admin_password] [--host localhost]   [--port 4848] [--secure -s] [--passwordfile filename]   [--terse=false] [--echo=false] [--interactive=true] jndi_name</pre>
<b>DESCRIPTION</b>	Removes the JNDI resource. This command is supported in remote mode only.
<b>OPTIONS</b>	<pre>--user          authorized domain application server administrative                   username.  --password      password to administer the domain application server.  --host          machine name where the domain application server is running.  --port          port number of the domain application server listening for                   administration requests.  --secure        if true, uses SSL/TLS to communicate with the domain                   application server.  --passwordfile  file containing the domain application server password.  --terse         indicates that any output data must be very concise, typically                   avoiding human-friendly sentences and favoring                   well-formatted data for consumption by a script.  --echo          setting to true will echo the command line statement on the                   standard output.  --interactive   prompts you for the required options that are not already                   specified.</pre>
<b>OPERANDS</b>	<i>jndi_name</i> name of the JNDI resource to be deleted.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the delete-jndi-resource command</p> <pre>asadmin&gt; delete-jndi-resource --user admin1 --password adminadmin1 --host pigeon --port 5001 sample_jndi_resource Command delete-jndi-resource executed successfully</pre> <p>Where: <i>sample_jndi_resource</i> is the JNDI resource to be deleted.</p>
<b>EXIT STATUS</b>	<pre>0  command executed successfully 1  error in executing the command</pre>
<b>SEE ALSO</b>	create-jndi-resource(1), list-jndi-resources(1)

## delete-jvm-options(1)

<b>NAME</b>	delete-jvm-options – deletes the JVM options from the Java configuration or profiler elements
<b>SYNOPSIS</b>	<b>delete-jvm-options</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure   -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true] [--profiler=false ] ( <i>jvm_option_name=jvm_option_value</i> ) [: <i>jvm_option_name=jvm_option_value</i> ]
<b>DESCRIPTION</b>	Deletes the JVM options in the Java configuration or Profiler elements of the <code>domain.xml</code> file. You can enter more than one JVM option separated by a colon (:). If the JVM option starts with a dash (-) then use two dashes (--) before the operand to distinguish that JVM option is an operand and not an option. JVM options are used to record the settings needed to get a particular profiler going.
<b>OPTIONS</b>	<p>--user                    authorized domain application server administrative username.</p> <p>--password                password to administer the domain application server.</p> <p>--host                    machine name where the domain application server is running.</p> <p>--port                    port number of the domain application server listening for administration requests.</p> <p>--secure                  if true, uses SSL/TLS to communicate with the domain application server.</p> <p>--passwordfile            file containing the domain application server password.</p> <p>--terse                    indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</p> <p>--echo                    setting to true will echo the command line statement on the standard output. Default is false.</p> <p>--interactive             if set to true (default), only the required password options are prompted.</p> <p>--profiler                indicates if the JVM options is for the profiler. Profiler must exist for this option to be true.</p>
<b>OPERANDS</b>	<i>jvm_option_name=jvm_option_value</i> the left side of the equal sign (=) is the JVM option name. The right side of the equal sign (=) is the <code>jvm_option_value</code> . Additionally, you can use ":" as a delimiter for more than one <code>jvm-option</code> . If the <code>jvm-option</code> contains a ":", use the escape character \ to offset the ":" delimiter.

**EXAMPLES**    **EXAMPLE 1** Using delete-jvm-options

```
asadmin> delete-jvm-options --user admin --password adminadmin
--host fuyako --port 7070 --profiler=true -- "-DDebug=true:"-Xmx256m":"
-Dcom.sun.aas.imqBin="\export\as7se\imq\bin"
JVM options deleted
```

Where the JVM options are created. The double dash (—) is used between --profiler options and the operand because - indicated the end of the options and the following text is the operand. The double dash (—) is necessary here since there are single dashes (i.e., —DDebug) in the operand. To distinguish between the options and the operand, the double dash (—) is used.

**EXIT STATUS**    0    command executed successfully  
                  1    error in executing the command

**SEE ALSO**        create-jvm-options(1)

## delete-lifecycle-module(1)

<b>NAME</b>	delete-lifecycle-module – removes the lifecycle module
<b>SYNOPSIS</b>	<b>delete-lifecycle-module</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true] <i>module_name</i>
<b>DESCRIPTION</b>	Removes the lifecycle module. This command is supported in remote mode only.
<b>OPTIONS</b>	--user authorized domain application server administrative username.  --password password to administer the domain application server.  --host machine name where the domain application server is running.  --port port number of the domain application server listening for administration requests.  --secure if true, uses SSL/TLS to communicate with the domain application server.  --passwordfile file containing the domain application server password.  --terse indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.  --echo setting to true will echo the command line statement on the standard output. Default is false.  --interactive if set to true (default), only the required password options are prompted.
<b>OPERANDS</b>	<i>module_name</i> unique identifier for the deployed server lifecycle event listener module.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using delete-lifecycle-module <pre>asadmin&gt; delete-lifecycle-module --user admin --password adminadmin --host fuyako --port 7070 customSetup Deleted the Lifecycle module with module name = customSetup</pre> <p>Where: customSetup is the lifecycle module deleted.</p>
<b>EXIT STATUS</b>	0 command executed successfully 1 error in executing the command
<b>SEE ALSO</b>	create-lifecycle-module(1), list-lifecycle-modules(1)



<b>NAME</b>	delete-mime – removes the MIME type
<b>SYNOPSIS</b>	<pre><b>delete-mime</b>   --user <i>admin_user</i> [--password <i>admin_password</i>] [--host <i>localhost</i>]   [--port <b>4848</b>] [--passwordfile <i>filename</i>] [--secure -s] [--instance   <i>instance_name</i>] <i>mime_ID</i></pre>
<b>DESCRIPTION</b>	Removes the MIME types associated with the named server instance. The server determines the MIME type of a requested resource by invoking the type-by-extension directive in the <code>ObjectType</code> section of the <code>obj.conf</code> file. The type-by-extension function does not work if no MIME element has been defined in the server element.
<b>OPTIONS</b>	<pre>--user          administrative user associated for the instance. --password      administrative password corresponding to the administrative                 user. --host          host name of the machine hosting the administrative instance. --port          administrative port number associated with the administrative                 host. --passwordfile  file containing passwords appropriate for the command (e.g.,                 administrative instance). --secure        if true, uses SSL/TLS to communicate with the administrative                 instance. --instance      name of the instance.</pre>
<b>OPERANDS</b>	<i>mime_id</i> internal name for the MIME types listing. It is used in a virtual-server element to define the MIME types used by the virtual server.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using delete-mime</p> <pre>asadmin&gt; delete-mime --user admin --password adminadmin --host fuyako --port 7070 --instance serv Deleted Mime with id = sampleMIME</pre> <p>Where: <code>sampleMIME</code> is the name of the MIME deleted.</p>
<b>EXIT STATUS</b>	<pre>0  command executed successfully 1  error in executing the command</pre>
<b>INTERFACE EQUIVALENT</b>	HTTP Server node, MIME Type Files page
<b>SEE ALSO</b>	<code>create-mime(1)</code> , <code>list-mimes(1)</code>

## delete-persistence-resource(1)

<b>NAME</b>	delete-persistence-resource – removes the persistence resource																		
<b>SYNOPSIS</b>	<pre><b>delete-persistence-resource</b> --user <i>admin_user</i>   [--password <i>admin_password</i>] [--host <i>localhost</i>] [--port <b>4848</b>]   [--secure -s] [--passwordfile <i>filename</i>] [--terse=false]   [--echo=false] [--interactive=true] <i>jndi_name</i></pre>																		
<b>DESCRIPTION</b>	Removes the persistence resource. This command is supported in remote mode only.																		
<b>OPTIONS</b>	<table><tr><td>--user</td><td>authorized domain application server administrative username.</td></tr><tr><td>--password</td><td>password to administer the domain application server.</td></tr><tr><td>--host</td><td>machine name where the domain application server is running.</td></tr><tr><td>--port</td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td>--passwordfile</td><td>file containing the domain application server password.</td></tr><tr><td>--terse</td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td></tr><tr><td>--echo</td><td>setting to true will echo the command line statement on the standard output. Default is false.</td></tr><tr><td>--interactive</td><td>if set to true (default), only the required password options are prompted.</td></tr></table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	--echo	setting to true will echo the command line statement on the standard output. Default is false.	--interactive	if set to true (default), only the required password options are prompted.
--user	authorized domain application server administrative username.																		
--password	password to administer the domain application server.																		
--host	machine name where the domain application server is running.																		
--port	port number of the domain application server listening for administration requests.																		
--secure	if true, uses SSL/TLS to communicate with the domain application server.																		
--passwordfile	file containing the domain application server password.																		
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																		
--echo	setting to true will echo the command line statement on the standard output. Default is false.																		
--interactive	if set to true (default), only the required password options are prompted.																		
<b>OPERANDS</b>	<i>jndi_name</i> JNDI name of the persistence resource.																		
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using delete-persistence-resource</p> <pre>asadmin&gt; delete-persistence-resource --user admin1 --password adminadmin1 --host pigeon --port 5001 sample_persistence_resource Command delete-persistence-resource executed successfully</pre> <p>Where: <i>sample_persistence_resource</i> is the persistence resource to be deleted.</p>																		
<b>EXIT STATUS</b>	<table><tr><td>0</td><td>command executed successfully</td></tr><tr><td>1</td><td>error in executing the command</td></tr></table>	0	command executed successfully	1	error in executing the command														
0	command executed successfully																		
1	error in executing the command																		
<b>SEE ALSO</b>	create-persistence-resource(1), list-persistence-resources(1)																		

<b>NAME</b>	delete-profiler – deletes the profiler element
<b>SYNOPSIS</b>	<b>delete-profiler</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true]
<b>DESCRIPTION</b>	Deletes the profiler element. A server instance is tied to a particular profiler by the profiler element in the Java configuration. Changing a profiler requires you to restart the server.  This command is supported in remote mode only.
<b>OPTIONS</b>	--user                authorized domain application server administrative username.  --password           password to administer the domain application server.  --host                machine name where the domain application server is running.  --port                port number of the domain application server listening for administration requests.  --secure              if true, uses SSL/TLS to communicate with the domain application server.  --passwordfile       file containing the domain application server password.  --terse               indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.  --echo                setting to true will echo the command line statement on the standard output. Default is false.  --interactive        if set to true (default), only the required password options are prompted.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using delete-profiler  asadmin> <b>delete-profiler</b> --user admin --passwordfile passwords.txt --host localhost --port 4848 Deleted Profiler  Where: profiler is the deleted profile element.
<b>EXIT STATUS</b>	0    command executed successfully  1    error in executing the command
<b>SEE ALSO</b>	create-profiler(1), list-profiler(1)

## delete-resource-adapter-config(1)

<b>NAME</b>	delete-resource-adapter-config – deletes the configuration information created in domain.xml for the connector module
<b>SYNOPSIS</b>	<b>delete-resource-adapter-config</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <i>4848</i> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true] <i>raname</i>
<b>DESCRIPTION</b>	Deletes the entry in the resource-adapter-config element of the domain.xml file with the provided --raname.  This command is supported in remote mode only.
<b>OPTIONS</b>	--user authorized domain application server administrative username.  --password password to administer the domain application server.  --host machine name where the domain application server is running.  --port port number of the domain application server listening for administration requests.  --secure if true, uses SSL/TLS to communicate with the domain application server.  --passwordfile file containing the domain application server password.  --terse indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.  --echo setting to true will echo the command line statement on the standard output. Default is false.  --interactive if set to true (default), only the required password options are prompted.
<b>OPERANDS</b>	<i>raname</i> the value kept in the resource-adapter-name in the domain.xml file.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using delete-resource-adapter-config asadmin> delete-resource-adapter-config --username admin1 --password adminadmin myresourceadapter Command delete-resource-adapter-config executed successfully
<b>EXIT STATUS</b>	0 command executed successfully 1 error in executing the command
<b>SEE ALSO</b>	create-resource-adapter-config(1), list-resource-adapter-configs(1)

<b>NAME</b>	delete-ssl – deletes the ssl element from the HTTP listener, IIOp listener, or IIOp service																				
<b>SYNOPSIS</b>	<pre>delete-ssl --user admin_user [--password admin_password]            [--host localhost] [--port 4848] [--secure -s]            [--passwordfile filename] [--terse=false] [--echo=false]            [--interactive=true]            --type [http-listener iioop-listener iioop-service] [listener_id]</pre>																				
<b>DESCRIPTION</b>	<p>Deletes the ssl element from the HTTP listener, IIOp listener, or IIOp service. The <i>listener_id</i> is not required if the <code>--type</code> option is <code>iioop-service</code>.</p> <p>This command is supported in remote mode only.</p>																				
<b>OPTIONS</b>	<table border="0"> <tr> <td style="vertical-align: top;"><code>--user</code></td> <td>authorized domain application server administrative username.</td> </tr> <tr> <td style="vertical-align: top;"><code>--password</code></td> <td>password to administer the domain application server.</td> </tr> <tr> <td style="vertical-align: top;"><code>--host</code></td> <td>machine name where the domain application server is running.</td> </tr> <tr> <td style="vertical-align: top;"><code>--port</code></td> <td>port number of the domain application server listening for administration requests.</td> </tr> <tr> <td style="vertical-align: top;"><code>--secure</code></td> <td>if true, uses SSL/TLS to communicate with the domain application server.</td> </tr> <tr> <td style="vertical-align: top;"><code>--passwordfile</code></td> <td>file containing the domain application server password.</td> </tr> <tr> <td style="vertical-align: top;"><code>--terse</code></td> <td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td> </tr> <tr> <td style="vertical-align: top;"><code>--echo</code></td> <td>setting to true will echo the command line statement on the standard output. Default is false.</td> </tr> <tr> <td style="vertical-align: top;"><code>--interactive</code></td> <td>if set to true (default), only the required password options are prompted.</td> </tr> <tr> <td style="vertical-align: top;"><code>--type</code></td> <td>type of service or listener that the SSL is deleted. The type can be: <code>http-listener</code>, <code>iioop-listener</code>, and <code>iioop-service</code>.</td> </tr> </table>	<code>--user</code>	authorized domain application server administrative username.	<code>--password</code>	password to administer the domain application server.	<code>--host</code>	machine name where the domain application server is running.	<code>--port</code>	port number of the domain application server listening for administration requests.	<code>--secure</code>	if true, uses SSL/TLS to communicate with the domain application server.	<code>--passwordfile</code>	file containing the domain application server password.	<code>--terse</code>	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	<code>--echo</code>	setting to true will echo the command line statement on the standard output. Default is false.	<code>--interactive</code>	if set to true (default), only the required password options are prompted.	<code>--type</code>	type of service or listener that the SSL is deleted. The type can be: <code>http-listener</code> , <code>iioop-listener</code> , and <code>iioop-service</code> .
<code>--user</code>	authorized domain application server administrative username.																				
<code>--password</code>	password to administer the domain application server.																				
<code>--host</code>	machine name where the domain application server is running.																				
<code>--port</code>	port number of the domain application server listening for administration requests.																				
<code>--secure</code>	if true, uses SSL/TLS to communicate with the domain application server.																				
<code>--passwordfile</code>	file containing the domain application server password.																				
<code>--terse</code>	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																				
<code>--echo</code>	setting to true will echo the command line statement on the standard output. Default is false.																				
<code>--interactive</code>	if set to true (default), only the required password options are prompted.																				
<code>--type</code>	type of service or listener that the SSL is deleted. The type can be: <code>http-listener</code> , <code>iioop-listener</code> , and <code>iioop-service</code> .																				
<b>OPERANDS</b>	<table border="0"> <tr> <td style="vertical-align: top;"><i>listener_ID</i></td> <td>the ID of the listener or service that the SSL is deleted. This operand is not required if the <code>--type</code> option is <code>iioop-service</code>.</td> </tr> </table>	<i>listener_ID</i>	the ID of the listener or service that the SSL is deleted. This operand is not required if the <code>--type</code> option is <code>iioop-service</code> .																		
<i>listener_ID</i>	the ID of the listener or service that the SSL is deleted. This operand is not required if the <code>--type</code> option is <code>iioop-service</code> .																				
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using delete-ssl</p> <pre>asadmin&gt; delete-ssl --user admin --password adminadmin --host fuyako --port 7070 --type http-listener http-listener-1 Deleted SSL in HTTP Listener</pre> <p>Where: SSL is deleted for <code>http-listener-1</code>.</p>																				
<b>EXIT STATUS</b>	0    command executed successfully																				

delete-ssl(1)

1 error in executing the command

**SEE ALSO** create-ssl(1)

<b>NAME</b>	delete-threadpool – removes the named threadpool
<b>SYNOPSIS</b>	<b>delete-threadpool</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true] <i>threadpool_id</i>
<b>DESCRIPTION</b>	Removes the threadpool with the named ID. This command is supported in remote mode only.
<b>OPTIONS</b>	--user                    authorized domain application server administrative username. --password             password to administer the domain application server. --host                  machine name where the domain application server is running. --port                  port number of the domain application server listening for administration requests. --secure                if true, uses SSL/TLS to communicate with the domain application server. --passwordfile        file containing the domain application server password. --terse                indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false. --echo                  setting to true will echo the command line statement on the standard output. Default is false. --interactive         if set to true (default), only the required password options are prompted.
<b>OPERANDS</b>	<i>threadpool_id</i> an ID for the work queue; for example, thread-pool-1, thread-pool-2, etc.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using delete-threadpool asadmin> <b>delete-threadpool --user admin1 --password adminadmin1 threadpool-1</b> Command delete-threadpool executed successfully
<b>EXIT STATUS</b>	0     command executed successfully 1     error in executing the command
<b>SEE ALSO</b>	create-threadpool(1), list-threadpools(1)

## delete-virtual-server(1)

<b>NAME</b>	delete-virtual-server – deletes the virtual server with the named virtual server ID
<b>SYNOPSIS</b>	<b>delete-virtual-server</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true] <i>virtual_server_id</i>
<b>DESCRIPTION</b>	Deletes the virtual server with the named virtual server ID. This command is supported in remote mode only.
<b>OPTIONS</b>	--user                    authorized domain application server administrative username.  --password                password to administer the domain application server.  --host                    machine name where the domain application server is running.  --port                    port number of the domain application server listening for administration requests.  --secure                  if true, uses SSL/TLS to communicate with the domain application server.  --passwordfile            file containing the domain application server password.  --terse                   indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.  --echo                    setting to true will echo the command line statement on the standard output. Default is false.  --interactive             if set to true (default), only the required password options are prompted.
<b>OPERANDS</b>	<i>virtual_server_id</i> identifies the unique ID for the virtual server to be created. This virtual server ID cannot begin with a number.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using delete-virtual-server <pre>asadmin&gt; delete-virtual-server --user admin1 --password adminadmin1 --host pigeon --port 5001 sample_vs1</pre> Command delete-virtual-server executed successfully  Where sample_vs1 is the virtual server deleted.
<b>EXIT STATUS</b>	0      command executed successfully 1      error in executing the command
<b>SEE ALSO</b>	create-virtual-server(1), list-virtual-servers(1)



<b>NAME</b>	deploy – deploys the specified component																
<b>SYNOPSIS</b>	<pre> <b>deploy</b> --user <i>admin_user</i> [--password <i>admin_password</i>] [--host <i>localhost</i>]   [--port <i>4848</i>] [--secure -s] [--passwordfile <i>filename</i>]   [--terse=false] [--echo=false] [--interactive]   [--virtualservers <i>virtual_servers</i>] [--contextroot <i>context_root</i>]   [--force=true] [--precompilejsp=false] [--verify=false]   [--name <i>component_name</i>] [--upload=true] [--retrieve <i>local_dirpath</i>]   [--dbvendorname <i>dbvendorname</i>] [--createtables=true false     --dropandcreatetables=true false ] [--uniquetablenames=true false]   [--deploymentplan <i>deployment_plan</i>] [--enabled=true] <i>filepath</i> </pre>																
<b>DESCRIPTION</b>	<p>Deploys an EJB, web, connector or application. If the component is already deployed or already exists, it is forcefully re-deployed if the <code>--force</code> option is set to true.</p> <p>The <code>--createtables</code> and <code>--dropandcreatetables</code> options are booleans and therefore can take the values of true or false. These options are only used during deployment of CMP beans that have not been mapped to a database (i.e., no <code>sun-cmp-mappings.xml</code> descriptor is provided in the module's META-INF directory). They are ignored otherwise.</p> <p>The <code>--createtables</code> option and <code>--dropandcreatetables</code> option are mutually exclusive; only one should be used. If drop and/or create tables fails, the deployment does not fail; a warning message is provided in the log file.</p> <p>This command is supported in remote mode only.</p>																
<b>OPTIONS</b>	<table border="0"> <tr> <td style="padding-right: 20px;"><code>--user</code></td> <td>authorized domain application server administrative username.</td> </tr> <tr> <td><code>--password</code></td> <td>password to administer the domain application server.</td> </tr> <tr> <td><code>--host</code></td> <td>machine name where the domain application server is running.</td> </tr> <tr> <td><code>--port</code></td> <td>port number of the domain application server listening for administration requests.</td> </tr> <tr> <td><code>--secure</code></td> <td>if true, uses SSL/TLS to communicate with the domain application server.</td> </tr> <tr> <td><code>--passwordfile</code></td> <td>file containing the domain application server password.</td> </tr> <tr> <td><code>--terse</code></td> <td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.</td> </tr> <tr> <td><code>--echo</code></td> <td>setting to true will echo the command line statement on the standard output.</td> </tr> </table>	<code>--user</code>	authorized domain application server administrative username.	<code>--password</code>	password to administer the domain application server.	<code>--host</code>	machine name where the domain application server is running.	<code>--port</code>	port number of the domain application server listening for administration requests.	<code>--secure</code>	if true, uses SSL/TLS to communicate with the domain application server.	<code>--passwordfile</code>	file containing the domain application server password.	<code>--terse</code>	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.	<code>--echo</code>	setting to true will echo the command line statement on the standard output.
<code>--user</code>	authorized domain application server administrative username.																
<code>--password</code>	password to administer the domain application server.																
<code>--host</code>	machine name where the domain application server is running.																
<code>--port</code>	port number of the domain application server listening for administration requests.																
<code>--secure</code>	if true, uses SSL/TLS to communicate with the domain application server.																
<code>--passwordfile</code>	file containing the domain application server password.																
<code>--terse</code>	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.																
<code>--echo</code>	setting to true will echo the command line statement on the standard output.																

## deploy(1)

<code>--interactive</code>	prompts you for the required options that are not already specified.
<code>--virtualservers</code>	comma separated list of virtual server name.
<code>--contextroot</code>	valid only if the archive is a web module. It is ignored for other archive types; defaults to filename without extension.
<code>--force</code>	makes sure the component is forcefully (re)deployed even if the specified component has already been deployed or already exists.
<code>--precompilejsp</code>	by default is set to false which does not allow the JSP to pre-compile during deployment. Instead JSPs are compiled during runtime.
<code>--verify</code>	if set to true, the syntax and semantics of the deployment descriptor is verified.
<code>--name</code>	name of the deployable component.
<code>--upload</code>	when set to true, uploads the deployable file to the administration server. If the filepath of the deployable file is mounted to the server machine, or if the administration server is running locally, set the upload option to false.
<code>--retrieve</code>	retrieves the client stub JAR file from the server machine to the local directory.
<code>--dbvendorname</code>	name of database vendor being used. Default is the corresponding entry in the <code>cmp-resource()</code> element of the <code>sun-ejb-jar.xml</code> file. If not specified the default is SQL92. Thereby the DDL files to create and drop tables will be generated in SQL92 format.
<code>--createtables</code>	creates tables at deploy of an application with unmapped CMP beans. Default is the corresponding entry in the <code>cmp-resource</code> element of the <code>sun-ejb-jar.xml</code> file. If not specified, defaults to the entries specified in the deployment descriptors.
<code>--dropandcreatetables</code>	drops tables at redeploy of an already deployed application with unmapped CMP beans. If not specified, the tables will be dropped if the <code>drop-tables-at-undeploy</code> entry in the <code>cmp-resource</code> element of the <code>sun-ejb-jar.xml</code> file is set to true. The new tables are created if the <code>create-tables-at-deploy</code> entry in the <code>cmp-resource</code> element of the <code>sun-ejb-jar.xml</code>

file is set to true. On redeploy the tables created by the previous deploy are dropped before creating the new tables.

`--uniquetablenames` guarantees unique table names for all the beans and results in a hashcode added to the table names. This is useful if you have an application with case-sensitive bean names.

`--deploymentplan` takes the deployment plan, which is a JAR containing Sun-specific descriptors, and deploys it. This should be passed along when deploying a pure EAR file. A pure EAR file is an EAR without Sun-specific descriptors.

`--enabled` if set to true (default), allows user to access the application. If set to false, user will not be able to access the application.

**OPERANDS** *filepath* path to the deployable file on the local machine if the `--upload` option is set to true; otherwise the absolute path to the file on the server machine.

**EXAMPLES** **EXAMPLE 1** Deploying a J2EE application

Deploy (install) the J2EE application packaged in the `Cart.ear` file.

```
asadmin> deploy --user admin --password admin123 --host murph
--port 4848 Cart.ear
Command deploy executed successfully
```

**EXAMPLE 2** Deploying a Web application with the default context root

Deploy the Web application in the `hello.war` file at the `hello` context root.

```
asadmin> deploy --user admin hello.war
Command deploy executed successfully
```

**EXAMPLE 3** Deploying an enterprise bean (EJB component)

Deploy an enterprise bean with container-managed persistence (CMP) and create the database tables used by the bean.

```
asadmin> deploy --user admin --createtables=true EmployeeEJB.jar
Command deploy executed successfully
```

**EXAMPLE 4** Deploying a connector module (resource adapter)

Deploy a connector module packaged in a RAR file.

```
asadmin> deploy --user admin jdbcra.rar
Command deploy executed successfully
```

deploy(1)

<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command

<b>SEE ALSO</b>	undeploy(1), list-components(1)
-----------------	---------------------------------

<b>NAME</b>	deploydir – deploys an exploded format of application archive																
<b>SYNOPSIS</b>	<pre> <b>deploydir</b> --user <i>admin_user</i> [--password <i>admin_password</i>] [--host <i>localhost</i>]   [--port 4848] [--secure -s] [--passwordfile <i>filename</i>]   [--terse=false] [--echo=false] [--interactive=true]   [--virtualservers <i>virtual_servers</i>] [--contextroot <i>context_root</i>]   [--force=true] [--verify=false]   [--precompilejsp=false] [--name <i>component_name</i>]   [--uniquetablenames=true   false]   [--dbvendorname <i>dbvendorname</i>] [--createtables=false     --dropandcreatetables=false ] <i>dirpath</i> </pre>																
<b>DESCRIPTION</b>	<p>Deploys the exploded format of the application archives present under the directory provided as the command operand. The deployed format, of EAR or WAR applications, reside on the application server and have a directory structure which can be used for deployment. The <code>--force</code> option makes sure the component is forcefully (re)deployed even if the specified component has already been deployed or already exists. Set <code>--force</code> to false for a first deployment. If the application with that name is running, and force is set to false, the command fails.</p> <p>If the <code>--uniquetablenames</code>, <code>--createtables</code>, and <code>--dropandcreatetables</code> options are not specified, the entries in the deployment descriptors are used.</p> <p>This command is supported in remote mode only.</p>																
<b>OPTIONS</b>	<table border="0"> <tr> <td style="padding-right: 20px;"><code>--user</code></td> <td>authorized domain application server administrative username.</td> </tr> <tr> <td><code>--password</code></td> <td>password to administer the domain application server.</td> </tr> <tr> <td><code>--host</code></td> <td>machine name where the domain application server is running.</td> </tr> <tr> <td><code>--port</code></td> <td>port number of the domain application server listening for administration requests.</td> </tr> <tr> <td><code>--secure</code></td> <td>if true, uses SSL/TLS to communicate with the domain application server.</td> </tr> <tr> <td><code>--passwordfile</code></td> <td>file containing the domain application server password.</td> </tr> <tr> <td><code>--terse</code></td> <td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.</td> </tr> <tr> <td><code>--echo</code></td> <td>setting to true will echo the command line statement on the standard output.</td> </tr> </table>	<code>--user</code>	authorized domain application server administrative username.	<code>--password</code>	password to administer the domain application server.	<code>--host</code>	machine name where the domain application server is running.	<code>--port</code>	port number of the domain application server listening for administration requests.	<code>--secure</code>	if true, uses SSL/TLS to communicate with the domain application server.	<code>--passwordfile</code>	file containing the domain application server password.	<code>--terse</code>	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.	<code>--echo</code>	setting to true will echo the command line statement on the standard output.
<code>--user</code>	authorized domain application server administrative username.																
<code>--password</code>	password to administer the domain application server.																
<code>--host</code>	machine name where the domain application server is running.																
<code>--port</code>	port number of the domain application server listening for administration requests.																
<code>--secure</code>	if true, uses SSL/TLS to communicate with the domain application server.																
<code>--passwordfile</code>	file containing the domain application server password.																
<code>--terse</code>	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.																
<code>--echo</code>	setting to true will echo the command line statement on the standard output.																

## deploydir(1)

<code>--interactive</code>	prompts you for the required options that are not already specified.
<code>--virtualservers</code>	comma separated list of virtual server IDs.
<code>--contextroot</code>	valid only if the archive is a web module. It is ignored for other archive types; defaults to filename without extension.
<code>--force</code>	makes sure the component is forcefully (re)deployed even if the specified component has already been deployed or already exists.
<code>--precompilejsp</code>	by default is set to false which does not allow the JSP to pre-compile during deployment. Instead JSPs are compiled during runtime.
<code>--verify</code>	if set to true, the syntax and semantics of the deployment descriptor is verified.
<code>--name</code>	name of the deployable component.
<code>--uniquetablenames</code>	guarantees unique table names for all the beans and results in a hashcode added to the table names. This is useful if you have an application with case-sensitive bean names.
<code>--dbvendorname</code>	name of the database vendor being used. Default is the corresponding entry in the <code>cmp-resource ()</code> element of the <code>sun-ejb-jar.xml</code> file. If not specified, the default is SQL92. Thereby the DDL files to create and drop tables will be generated in SQL92 format.
<code>--createtables</code>	creates tables during deployment for applications using unmapped CMP beans. Default is the corresponding entry in the <code>cmp-resource</code> element of the <code>sun-ejb-jar.xml</code> file. If not specified, defaults to the entries in the deployment descriptors.
<code>--dropandcreatetables</code>	drops existing tables and creates tables during deployment for application using unmapped CMP beans. If not specified, the tables will be dropped if the <code>drop-tables-at-undeploy</code> entry in the <code>cmp-resource</code> element of the <code>sun-ejb-jar.xml</code> file is set to true. The new tables are created if the <code>create-tables-at-deploy</code> entry in the <code>cmp-resource</code> element of the <code>sun-ejb-jar.xml</code> is set to true. On redeploy the tables created by the previous deploy are dropped before creating the new tables.

## deploydir(1)

**OPERANDS** *dirpath* path to the directory containing the exploded format of the deployable archive.

**EXAMPLES** **EXAMPLE 1** Using deploydir

```
asadmin> deploydir --user admin --passwordfile passwords.txt
--host localhost --port 4848 --force=true --precompilejsp=true /home/temp/sampleApp
Command deploydir executed successfully
```

Where: the exploded application to be deployed is in the /home/temp/sampleApp directory.

**EXIT STATUS** 0 command executed successfully

1 error in executing the command

**SEE ALSO** deploy(1), undeploy(1), enable(1), disable(1), list-components(1)

## deploytool(1m)

<b>NAME</b>	deploytool – launches the deploytool utility to deploy, package, and edit your J2EE applications
<b>SYNOPSIS</b>	<b>deploytool</b> [--help] [--userdir <i>user_directory</i> ] [--configdir <i>configuration_directory</i> ]
<b>DESCRIPTION</b>	<p>Use the <code>deploytool</code> utility to deploy and package your J2EE applications and components, create and edit J2EE deployment descriptors, and create and edit J2EE Application Server specific deployment descriptors. If the application is not J2EE compliant, an error message is displayed.</p> <p>Only one session of the <code>deploytool</code> utility can run with a specific user directory. A lock file is created to ensure that only one utility session is running. A message is displayed if a lock file is detected.</p>
<b>OPTIONS</b>	<p>--help           displays the arguments for launching the AssemblyTool.</p> <p>--userdir        identifies the user directory. The default user directory is <code>.deploytool</code> under your home directory. Only one <code>deploytool</code> session can be running per user directory. A lock file is created under the user directory to ensure that only one session of the <code>deploytool</code> is running. The <code>deploytool</code> utility uses this directory to store configuration information.</p> <ul style="list-style-type: none"><li>■ On Solaris, the default directory is at <code>~/ .deploytool</code></li></ul> <p>--configdir      identifies the configuration directory. The configuration directory is where the <code>asenv.conf</code> file is located.</p> <p>On Solaris the <code>asenv.conf</code> can be found at:</p> <ul style="list-style-type: none"><li>■ Bundled installation: <code>/etc/appserver</code></li><li>■ Unbundled installation: default is <code>/etc/opt/SUNWappserver7</code> or user specified</li><li>■ Evaluation installation: <code>AS_SERVER_INSTALL/config</code>. Where <code>AS_SERVER_INSTALL</code> is the directory where you have installed the Java 2 Platform, Enterprise Edition 1.4 Application Server Beta 2.</li></ul>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using <code>deploytool</code></p> <pre>example% <b>deploytool</b> --userdir /myapplication --config_dir /myconfigdir</pre> <p>Where <code>--userdir</code> specifies the destination directory, and <code>-config_dir</code> identifies the configuration directory.</p>
<b>SEE ALSO</b>	<code>verifier(1M)</code>



<b>NAME</b>	disable – disables the component
<b>SYNOPSIS</b>	<b>disable</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <i>4848</i> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive] <i>component_name</i>
<b>DESCRIPTION</b>	disable immediately disables the named component. The component must have been deployed. If the component has not been deployed, an error message is returned.
<b>OPTIONS</b>	<p>--user                    authorized domain application server administrative username.</p> <p>--password               password to administer the domain application server.</p> <p>--host                    machine name where the domain application server is running.</p> <p>--port                    port number of the domain application server listening for administration requests.</p> <p>--secure                  if true, uses SSL/TLS to communicate with the domain application server.</p> <p>--passwordfile           file containing the domain application server password.</p> <p>--terse                   indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.</p> <p>--echo                    setting to true will echo the command line statement on the standard output.</p> <p>--interactive            prompts you for the required options that are not already specified.</p>
<b>OPERANDS</b>	<i>component_name</i> name of the component to be disabled.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using disable</p> <pre>asadmin&gt; disable sampleApp Command disable executed successfully</pre>
<b>EXIT STATUS</b>	<p>0    command executed successfully</p> <p>1    error in executing the command</p>
<b>SEE ALSO</b>	deploy(1), deploydir(1), undeploy(1), enable(1)

## display-license(1)

<b>NAME</b>	display-license – displays the license information
<b>SYNOPSIS</b>	<b>display-license</b> [ <b>--user</b> <i>admin_user</i> ] [ <b>--password</b> <i>admin_password</i> ] [ <b>--host</b> <i>localhost</i> ] [ <b>--port</b> <i>4848</i> ] [ <b>--passwordfile</b> <i>filename</i> ] [ <b>--secure</b>   <b>-s</b> ]
<b>DESCRIPTION</b>	display-license displays the license information. This command can run both locally and remotely.
<b>OPTIONS</b>	<b>--user</b> administrative user associated for the instance. <b>--password</b> administrative password corresponding to the administrative user. <b>--host</b> host name of the machine hosting the administrative instance. <b>--port</b> administrative port number associated with the administrative host. <b>--passwordfile</b> file containing passwords appropriate for the command (e.g., administrative instance). <b>--secure</b> if true, uses SSL/TLS to communicate with the administrative instance.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using display-license in local mode <pre>asadmin&gt; display-license ***** Eval                Sun ONE Application Server 7 Evaluation License Expiration date     Tues 11 Sept 11:58:47 PDT 2002 Number of instances per admin server  Unlimited Allow remote administration  YES *****</pre> <b>EXAMPLE 2</b> Using display-license in remote mode <pre>asadmin&gt; display-license --user admin --password adminadmin --host fuyako --port 7070 ***** Eval                Sun ONE Application Server 7 Evaluation License Expiration date     Tues 11 Sept 11:58:47 PDT 2002 Number of instances per admin server  Unlimited Allow remote administration  YES *****</pre>
<b>EXIT STATUS</b>	0 command executed successfully 1 error in executing the command
<b>SEE ALSO</b>	install-license(1)

<b>NAME</b>	enable – enables the component
<b>SYNOPSIS</b>	<b>enable</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <i>4848</i> ] [--secure -s] --passwordfile <i>filename</i> [--terse=false] [--echo=false] [--interactive] <i>component_name</i>
<b>DESCRIPTION</b>	enable command enables the specified component. If the component is already enabled, then it is re-enabled. The component must have been deployed in order to be enabled. If it has not been deployed, then an error message is returned. This command is supported in remote mode only.
<b>OPTIONS</b>	<p>--user                authorized domain application server administrative username.</p> <p>--password           password to administer the domain application server.</p> <p>--host                machine name where the domain application server is running.</p> <p>--port                port number of the domain application server listening for administration requests.</p> <p>--secure              if true, uses SSL/TLS to communicate with the domain application server.</p> <p>--passwordfile       file containing the domain application server password.</p> <p>--terse               indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.</p> <p>--echo                setting to true will echo the command line statement on the standard output.</p> <p>--interactive        prompts you for the required options that are not already specified.</p>
<b>OPERANDS</b>	<i>component_name</i> name of the component to be enabled.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using enable</p> <pre>asadmin&gt; enable sampleApp Command enable executed successfully</pre>
<b>EXIT STATUS</b>	<p>0    command executed successfully</p> <p>1    error in executing the command</p>
<b>SEE ALSO</b>	deploy(1), deploydir(1), undeploy(1), disable(1)

## export(1)

<b>NAME</b>	export – marks a variable name for automatic export to the environment of subsequent commands in multimode
<b>SYNOPSIS</b>	<b>export</b> [ <i>name=value</i> [ <i>name=value</i> ] *]
<b>DESCRIPTION</b>	Marks a variable name for automatic export to the environment of subsequent commands. All subsequent commands use the variable name values as specified; unless you unset them or exit multimode. If only the variable name is specified, the current value of that variable name is displayed. If the export command is used without any arguments, a list of all the exported variables and their values is displayed. Exported shell environment variables set prior to invoking the <code>asadmin</code> utility are imported automatically and set as exported variables within <code>asadmin</code> . Unexported environment variables cannot be read by the <code>asadmin</code> utility.
<b>OPERANDS</b>	<i>name=value</i> variable name and value for automatic export to the environment to be used by subsequent commands.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using <code>export</code> to list the environment variables</p> <pre>asadmin&gt; export AS_ADMIN_HOST=bluestar AS_ADMIN_PORT=8000 AS_ADMIN_USER=admin AS_ADMIN_PASSWORD=pa asadmin&gt; export AS_ADMIN_PREFIX=server1.jms-service asadmin&gt; export //to list the environment variables that are set AS_ADMIN_HOST=bluestar AS_ADMIN_PORT=8000 AS_ADMIN_USER=admin AS_ADMIN_PASSWORD=***** AS_ADMIN_PREFIX=server1.jms-service</pre> <p>Where: the <code>export</code> command lists the environment variables that are set. In this case, the environment variables have been set to: the host is <i>bluestar</i>, the port is <i>8000</i>, the administrator user is <i>admin</i> with an associated password, and the prefix is <i>server1.jms-service</i>.</p>
<b>EXIT STATUS</b>	0 command executed successfully 1 error in executing the command
<b>SEE ALSO</b>	<code>unset(1)</code> , <code>multimode(1)</code>

<b>NAME</b>	freeze-transaction-service – freezes the transaction subsystem
<b>SYNOPSIS</b>	<b>freeze-transaction-service</b> --user <i>admin_user</i> [ <b>--password</b> <i>admin_password</i> ] [ <b>--host</b> <i>localhost</i> ] [ <b>--port</b> <b>4848</b> ] [ <b>--secure</b>   <b>-s</b> ] [ <b>--passwordfile</b> <i>filename</i> ] [ <b>--terse=false</b> ] [ <b>--echo=false</b> ] [ <b>--interactive=true</b> ]
<b>DESCRIPTION</b>	Freezes the transaction subsystem during which time all the inflight transactions are suspended. Invoke this command before rolling back any inflight transactions. Invoking this command on an already frozen transaction subsystem has no effect.  This command is supported in remote mode only.
<b>OPTIONS</b>	<b>--user</b> authorized domain application server administrative username.  <b>--password</b> password to administer the domain application server.  <b>--host</b> machine name where the domain application server is running.  <b>--port</b> port number of the domain application server listening for administration requests.  <b>--secure</b> if true, uses SSL/TLS to communicate with the domain application server.  <b>--passwordfile</b> file containing the domain application server password.  <b>--terse</b> indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.  <b>--echo</b> setting to true will echo the command line statement on the standard output. Default is false.  <b>--interactive</b> if set to true (default), only the required password options are prompted.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using freeze-transaction-service  asadmin> <b>freeze-transaction-service</b> --user admin --password adminadmin
<b>EXIT STATUS</b>	0 command executed successfully 1 error in executing the command
<b>SEE ALSO</b>	unfreeze-transaction-service(1), rollback-transaction(1)

get(1)

<b>NAME</b>	get – gets the values of the monitorable or configurable attributes																				
<b>SYNOPSIS</b>	<pre>get --user admin_user [--password admin_password] [--host localhost]   [--port 4848] [--secure -s] [--passwordfile filename]   [--terse=false] [--echo=false] [--interactive=true]   [--monitor=false] dotted_attribute_name</pre>																				
<b>DESCRIPTION</b>	Gets the values of attributes. If the <code>--monitor</code> option is set to true, the monitorable attributes are returned. If the <code>--monitor</code> option is set to false, the configurable attribute values are returned. On Solaris, quotes are needed when executing commands with * as the option value or operand.																				
<b>OPTIONS</b>	<table><tr><td><code>--user</code></td><td>authorized domain application server administrative username.</td></tr><tr><td><code>--password</code></td><td>password to administer the domain application server.</td></tr><tr><td><code>--host</code></td><td>machine name where the domain application server is running.</td></tr><tr><td><code>--port</code></td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td><code>--secure</code></td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td><code>--passwordfile</code></td><td>file containing the domain application server password.</td></tr><tr><td><code>--terse</code></td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td></tr><tr><td><code>--echo</code></td><td>setting to true will echo the command line statement on the standard output. Default is false.</td></tr><tr><td><code>--interactive</code></td><td>if set to true (default), only the required password options are prompted.</td></tr><tr><td><code>--monitor</code></td><td>defaults to false; if set to false, the configurable attribute values are returned. If set to true, the monitorable attribute values are returned.</td></tr></table>	<code>--user</code>	authorized domain application server administrative username.	<code>--password</code>	password to administer the domain application server.	<code>--host</code>	machine name where the domain application server is running.	<code>--port</code>	port number of the domain application server listening for administration requests.	<code>--secure</code>	if true, uses SSL/TLS to communicate with the domain application server.	<code>--passwordfile</code>	file containing the domain application server password.	<code>--terse</code>	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	<code>--echo</code>	setting to true will echo the command line statement on the standard output. Default is false.	<code>--interactive</code>	if set to true (default), only the required password options are prompted.	<code>--monitor</code>	defaults to false; if set to false, the configurable attribute values are returned. If set to true, the monitorable attribute values are returned.
<code>--user</code>	authorized domain application server administrative username.																				
<code>--password</code>	password to administer the domain application server.																				
<code>--host</code>	machine name where the domain application server is running.																				
<code>--port</code>	port number of the domain application server listening for administration requests.																				
<code>--secure</code>	if true, uses SSL/TLS to communicate with the domain application server.																				
<code>--passwordfile</code>	file containing the domain application server password.																				
<code>--terse</code>	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																				
<code>--echo</code>	setting to true will echo the command line statement on the standard output. Default is false.																				
<code>--interactive</code>	if set to true (default), only the required password options are prompted.																				
<code>--monitor</code>	defaults to false; if set to false, the configurable attribute values are returned. If set to true, the monitorable attribute values are returned.																				
<b>OPERANDS</b>	<i>attributename</i> attribute name in the dotted notation.																				
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using get</p> <pre>asadmin&gt; get --user admin --password adminadmin --host localhost --port 4848 "server.resources.jdbc-resource.jdbc/PointBase.*" server.resources.jdbc-resource.jdbc/PointBase.description=&lt;null&gt; server.resources.jdbc-resource.jdbc/PointBase.enabled=true server.resources.jdbc-resource.jdbc/PointBase.jndi-name=jdbc/PointBase server.resources.jdbc-resource.jdbc/PointBase.object-type=user server.resources.jdbc-resource.jdbc/PointBase.pool-name=PointBasePool</pre>																				

get(1)

**EXIT STATUS** 0 command executed successfully  
1 error in executing the command

**SEE ALSO** set(1), list(1)

## get-client-stubs(1)

<b>NAME</b>	get-client-stubs – gets the stubs of the client																				
<b>SYNOPSIS</b>	<pre>get-client-stubs --user <i>admin_user</i> [--password <i>admin_password</i>]   [--host <i>localhost</i>] [--port <i>4848</i>] [--secure -s]   [--passwordfile <i>filename</i>] [--terse=false] [--echo=false]   [--interactive] --appname <i>application_name</i> <i>local_directory_path</i></pre>																				
<b>DESCRIPTION</b>	Gets the client stubs JAR file for an AppClient standalone module or an application containing the AppClient module, from the server machine to the local directory. This command is supported in remote mode only.																				
<b>OPTIONS</b>	<table><tr><td>--user</td><td>authorized domain application server administrative username.</td></tr><tr><td>--password</td><td>password to administer the domain application server.</td></tr><tr><td>--host</td><td>machine name where the domain application server is running.</td></tr><tr><td>--port</td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td>--passwordfile</td><td>file containing the domain application server password.</td></tr><tr><td>--terse</td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.</td></tr><tr><td>--echo</td><td>setting to true will echo the command line statement on the standard output.</td></tr><tr><td>--interactive</td><td>prompts you for the required options that are not already specified.</td></tr><tr><td>--appname</td><td>name of the application.</td></tr></table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.	--echo	setting to true will echo the command line statement on the standard output.	--interactive	prompts you for the required options that are not already specified.	--appname	name of the application.
--user	authorized domain application server administrative username.																				
--password	password to administer the domain application server.																				
--host	machine name where the domain application server is running.																				
--port	port number of the domain application server listening for administration requests.																				
--secure	if true, uses SSL/TLS to communicate with the domain application server.																				
--passwordfile	file containing the domain application server password.																				
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.																				
--echo	setting to true will echo the command line statement on the standard output.																				
--interactive	prompts you for the required options that are not already specified.																				
--appname	name of the application.																				
<b>OPERANDS</b>	<table><tr><td><i>local_directory_path</i></td><td>path to the local directory where the client stub should be stored.</td></tr></table>	<i>local_directory_path</i>	path to the local directory where the client stub should be stored.																		
<i>local_directory_path</i>	path to the local directory where the client stub should be stored.																				
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using get-client-stubs</p> <pre>asadmin&gt; get-client-stubs --user admin --password adminadmin --host fuyako --port 7070 --appname myapplication.ear /sample/exmple</pre>																				
<b>EXIT STATUS</b>	<table><tr><td>0</td><td>command executed successfully</td></tr><tr><td>1</td><td>error in executing the command</td></tr></table>	0	command executed successfully	1	error in executing the command																
0	command executed successfully																				
1	error in executing the command																				
<b>SEE ALSO</b>	undeploy(1)																				



<b>NAME</b>	help – displays a list of all the commands available in the Command-line interface																																										
<b>SYNOPSIS</b>	<b>asadmin help</b> <i>or</i> <b>asadmin --help   -h   -?</b>																																										
<b>DESCRIPTION</b>	<p>The help command displays a list of all the asadmin commands available in the Command-line interface. Specify the command to display the usage information for that command. To display the manpage of each command, use the syntax: <code>asadmin <i>command_name</i> --help   -h   -?</code> or <code>asadmin help <i>command_name</i></code></p> <p>The following is a list of all the Command-line interface commands:</p> <table border="0"> <tr> <td>add-resources</td> <td>registers the resource in the XML file specified</td> </tr> <tr> <td>create-admin-object</td> <td>adds the administered object with the specified JNDI name</td> </tr> <tr> <td>create-audit-module</td> <td>creates an audit module for the optional plugin module</td> </tr> <tr> <td>create-auth-realm</td> <td>adds the new authorized realm</td> </tr> <tr> <td>create-connector-connection-pool</td> <td>adds a connection pool with the specified connection pool name</td> </tr> <tr> <td>create-connector-resource</td> <td>registers the resource with the specified JNDI name</td> </tr> <tr> <td>create-connector-security-map</td> <td>creates or modifies a security map for the namedconnector connection pool</td> </tr> <tr> <td>create-custom-resource</td> <td>registers the custom resource</td> </tr> <tr> <td>create-domain</td> <td>creates a domain with the given name</td> </tr> <tr> <td>create-file-user</td> <td>creates a new file user</td> </tr> <tr> <td>create-http-listener</td> <td>adds a new HTTP listener socket</td> </tr> <tr> <td>create-iiop-listener</td> <td>adds the IIOP listener</td> </tr> <tr> <td>create-javamail-resource</td> <td>registers the Javamail resource</td> </tr> <tr> <td>create-jdbc-connection-pool</td> <td>registers the JDBC connection pool</td> </tr> <tr> <td>create-jdbc-resource</td> <td>registers the JDBC resource</td> </tr> <tr> <td>create-jms-resource</td> <td>registers the JMS resource</td> </tr> <tr> <td>create-jmsdest</td> <td>adds the named destination</td> </tr> <tr> <td>create-jndi-resource</td> <td>registers the JNDI resource</td> </tr> <tr> <td>create-jvm-options</td> <td>creates the JVM options from the Java configuration or profiler elements</td> </tr> <tr> <td>create-lifecycle-module</td> <td>adds a lifecycle module</td> </tr> <tr> <td>create-persistence-resource</td> <td>registers the persistence resource</td> </tr> </table>	add-resources	registers the resource in the XML file specified	create-admin-object	adds the administered object with the specified JNDI name	create-audit-module	creates an audit module for the optional plugin module	create-auth-realm	adds the new authorized realm	create-connector-connection-pool	adds a connection pool with the specified connection pool name	create-connector-resource	registers the resource with the specified JNDI name	create-connector-security-map	creates or modifies a security map for the namedconnector connection pool	create-custom-resource	registers the custom resource	create-domain	creates a domain with the given name	create-file-user	creates a new file user	create-http-listener	adds a new HTTP listener socket	create-iiop-listener	adds the IIOP listener	create-javamail-resource	registers the Javamail resource	create-jdbc-connection-pool	registers the JDBC connection pool	create-jdbc-resource	registers the JDBC resource	create-jms-resource	registers the JMS resource	create-jmsdest	adds the named destination	create-jndi-resource	registers the JNDI resource	create-jvm-options	creates the JVM options from the Java configuration or profiler elements	create-lifecycle-module	adds a lifecycle module	create-persistence-resource	registers the persistence resource
add-resources	registers the resource in the XML file specified																																										
create-admin-object	adds the administered object with the specified JNDI name																																										
create-audit-module	creates an audit module for the optional plugin module																																										
create-auth-realm	adds the new authorized realm																																										
create-connector-connection-pool	adds a connection pool with the specified connection pool name																																										
create-connector-resource	registers the resource with the specified JNDI name																																										
create-connector-security-map	creates or modifies a security map for the namedconnector connection pool																																										
create-custom-resource	registers the custom resource																																										
create-domain	creates a domain with the given name																																										
create-file-user	creates a new file user																																										
create-http-listener	adds a new HTTP listener socket																																										
create-iiop-listener	adds the IIOP listener																																										
create-javamail-resource	registers the Javamail resource																																										
create-jdbc-connection-pool	registers the JDBC connection pool																																										
create-jdbc-resource	registers the JDBC resource																																										
create-jms-resource	registers the JMS resource																																										
create-jmsdest	adds the named destination																																										
create-jndi-resource	registers the JNDI resource																																										
create-jvm-options	creates the JVM options from the Java configuration or profiler elements																																										
create-lifecycle-module	adds a lifecycle module																																										
create-persistence-resource	registers the persistence resource																																										

help(1)

create-profiler	creates the profiler element
create-resource-adapter-config	creates the resource adapter Java bean
create-ssl	creates the SSL element in the HTTP listener or IIOP listener
create-threadpool	creates the thread pool
create-virtual-server	adds the named virtual server
delete-admin-object	removes the administered object with the specified JNDI name
delete-audit-module	deletes the audit-module for the optional plugin module
delete-auth-realm	removes the named authorized realm
delete-connector-connection-pool	removes the specified connection pool
delete-connector-security-map	deletes the named security map
delete-connector-resource	removes the named resource connector
delete-custom-resource	removes the custom resource
delete-domain	deletes the given domain
delete-file-user	removes the named file user
delete-http-listener	removes the HTTP listener
delete-iiop-listener	removes the IIOP listener
delete-javamail-resource	removes the Javamail resource
delete-jdbc-connection-pool	removes the JDBC connection pool
delete-jdbc-resource	removes the JDBC resource
delete-jms-resource	removes the JMS resource
delete-jmsdest	destroys the named destination
delete-jndi-resource	removes the JNDI resource
delete-jvm-options	deletes the JVM options from the Java configuration or profiler elements
delete-lifecycle-module	removes the lifecycle module
delete-persistence-resource	removes the persistence resource
delete-profiler	deletes the profiler element
delete-resource-adapter-config	deletes the resource adapter Java bean
delete-ssl	deletes the ssl element from the HTTP listener or IIOP listener

delete-threadpool	deletes the thread pool
delete-virtual-server	deletes the virtual server with the named virtual server ID
deploy	deploys the specified component
deploydir	deploys the component that is in the directory located on domain application server
disable	stops the component
enable	runs the component
export	marks a variable name for automatic export to the environment of subsequent commands in multimode
freeze-transaction-service	immobilizes the named transaction service
get	gets the values of the monitorable or configurable attributes
get-client-stubs	gets the stubs of the client
help	displays a list of all the commands available in the Command-line interface
jms-ping	checks to see if the JMS provider is up and running
list-admin-objects	gets all the administered objects
list-audit-modules	lists the audit modules
list-auth-realms	lists the authorized realms
list-components	Lists deployed components
list-connector-connection-pools	gets all the connection pools
list-connector-resources	gets all the connector resources
list-connector-security-maps	lists the security maps for the connector connection pool
list-custom-resources	gets all the custom resources
list-domains	lists the domains in the given domains directory
list-file-groups	lists the file groups
list-file-users	lists the file users
list-http-listeners	gets the HTTP listeners
list-iiop-listeners	gets the IIOP listeners
list-javamail-resources	gets all the Javamail resources

help(1)

list-jdbc-connection-pools	registers the JDBC connection pool
list-jdbc-resources	gets all the JDBC resources
list-jms-resources	gets all the JMS resources
list-jmsdest	gets all the named destinations
list-jndi-resources	gets all the JNDI resources
list-lifecycle-modules	gets the lifecycle modules
list-persistence-resources	gets all the persistence resources
list-resource-adapter-configs	lists the resource adapters configured in an instance
list-sub-components	Lists EJBs or Servlets in a deployed module or in a module of a deployed application
list-threadpools	lists the thread pools
list-virtual-servers	gets the virtual servers
list	lists the configurable elements
multimode	allows you to execute multiple commands while returning environment settings and remaining in the asadmin utility
ping-connection-pool	tests if a connection pool is usable
rollback-transaction	reinitialize the transaction service to its previous state
set	sets the values of attributes
show-component-status	displays the status of the deployed component
start-domain	starts the given domain
stop-domain	stops the given domain
undeploy	removes a component in the domain application server
unfreeze-transaction-service	mobilizes the named transaction service
unset	removes one or more variables from the multimode environment
update-file-user	updates a current file user as specified
update-connector-security-map	updates the security map for the specified connector connection pool
verify-domain-xml	verifies the content of the domain.xml
version	displays the version information

**EXAMPLES** | **EXAMPLE 1** Using the help command

```
asadmin> help  
asadmin> create-domain --help
```

Where: **create-domain** is the command you wish to view the usage for.

**SEE ALSO** | [version\(1\)](#)

## install-license(1)

<b>NAME</b>	install-license – installs the license file
<b>SYNOPSIS</b>	<b>install-license</b>
<b>DESCRIPTION</b>	install-license prevents unauthorized use of the Sun ONE Application Server. Allows you to install the license file. This command can be run locally only.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using install-license asadmin> <b>install-license</b> LICENSE agreement will be displayed. Do you agree with the terms of this license [YES NO] YES Enter license key> ***** Installed the license
<b>EXIT STATUS</b>	0    command executed successfully 1    error in executing the command
<b>SEE ALSO</b>	display-license(1), version(1)

<b>NAME</b>	jms-ping – checks to see if the JMS provider is up and running
<b>SYNOPSIS</b>	<b>jms-ping</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <i>4848</i> ] [--passwordfile <i>filename</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=false]
<b>DESCRIPTION</b>	Checks to see if the JMS provider is up and running. This command is supported in remote mode only.
<b>OPTIONS</b>	<p>--user                    authorized domain application server administrative username.</p> <p>--password               password to administer the domain application server.</p> <p>--host                    machine name where the domain application server is running.</p> <p>--port                    port number of the domain application server listening for administration requests.</p> <p>--passwordfile           file containing the domain application server password.</p> <p>--secure                  if true, uses SSL/TLS to communicate with the domain application server.</p> <p>--terse                   indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</p> <p>--echo                    setting to true will echo the command line statement on the standard output. Default is false.</p> <p>--interactive             if set to true (default), only the required password options are prompted.</p>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using jms-ping</p> <pre>asadmin&gt; jms-ping --user admin --password adminadmin --host bluestar --port 4848 server1 JMS Ping Status=RUNNING</pre>
<b>EXIT STATUS</b>	<p>0    command executed successfully</p> <p>1    error in executing the command</p>
<b>SEE ALSO</b>	create-jmsdest(1), delete-jmsdest(1), list-jmsdest(1)

## jspc(1M)

<b>NAME</b>	jspc – precompiles JSP source files into servlets	
<b>SYNOPSIS</b>	<b>jspc</b> [ <i>options</i> ] <i>jsp_files</i> <b>or</b> <b>jspc</b> [ <i>options</i> ] <b>-webapp</b> <i>dir</i>	
<b>DESCRIPTION</b>	<p>Use the <code>jspc</code> command to compile your JSP 1.2 compliant source files into servlets. To allow the application server to pick up the precompiled JSPs from a JAR file, you must disable dynamic reloading of JSPs. To do this, set <code>reload-interval</code> property to <code>-1</code> in the <code>jsp-config</code> element of the <code>sun-web.xml</code> file.</p> <p>For more information about the <code>sun-web.xml</code> file, see the <i>Sun ONE Application Server Developer's Guide</i>.</p>	
<b>OPTIONS</b>	<i>jsp_files</i>	one or more JSP files to be compiled.
	<code>-webapp</code> <i>dir</i>	a directory containing a web application. All JSPs in the directory and its subdirectories are compiled. You cannot specify a WAR, JAR, or ZIP file; you must first deploy it to an open directory structure using <code>asadmin</code> <code>deploy</code> .
	<code>-q</code>	enables quiet mode (same as <code>-v0</code> ). Only fatal error messages are displayed.
	<code>-d</code> <i>dir</i>	the output directory for the compiled JSPs. Package directories are automatically generated based on the directories containing the uncompiled JSPs. The default top-level directory is the directory from which <code>jspc</code> is invoked.
	<code>-p</code> <i>name</i>	the name of the target package for all specified JSPs, overriding the default package generation performed by the <code>-d</code> option.
	<code>-c</code> <i>name</i>	the target class name of the first JSP compiled. Subsequent JSPs are unaffected.
	<code>-uribase</code> <i>dir</i>	the URI directory to which compilations are relative. Applies only to JSP files listed in the command, and not to JSP files specified with <code>-webapp</code> option. This is the location of each JSP file relative to the <code>uriroot</code> . If this cannot be determined, the default is <code>/</code> .
	<code>-uriroot</code> <i>dir</i>	the root directory against which URI files are resolved. Applies only to JSP files listed in the command, and not to JSP files specified with <code>-webapp</code> option. If this option is not specified, all parent directories of the first JSP page are searched for a <code>WEB-INF</code> subdirectory. The closest directory to the JSP page that has one is used. If none of the JSP's parent directories have a <code>WEB-INF</code> subdirectory, the directory from which <code>jspc</code> is invoked is used.
	<code>-genclass</code>	compiles the generated servlets into class files.



<code>-v [level]</code>	enables verbose mode. The level is optional; the default is 2. Possible level values are: <ul style="list-style-type: none"> <li>■ 0 - fatal error messages only</li> <li>■ 1 - error messages only</li> <li>■ 2 - error and warning messages only</li> <li>■ 3 - error, warning, and informational messages</li> <li>■ 4 - error, warning, informational, and debugging messages</li> </ul>
<code>-mapped</code>	generates separate write calls for each HTML line and comments that describe the location of each line in the JSP file. By default, all adjacent write calls are combined and no location comments are generated.
<code>-die [code]</code>	causes the JVM to exit and generates an error return code if a fatal error occurs. If the code is absent or unparseable it defaults to 1.
<code>-webinc file</code>	creates partial servlet mappings for the <code>-webapp</code> option, which can be pasted into a <code>web.xml</code> file.
<code>-webxml file</code>	creates an entire <code>web.xml</code> file for the <code>-webapp</code> option.
<code>-ieplugin class_id</code>	specifies the Java plugin COM class ID for Internet Explorer. Used by the <code>jsp:plugin</code> tags.

**EXAMPLES**    **EXAMPLE 1** Using `jspc` to compile the JSPs in a web application

The following command compiles a set of JSP files into Java files under `Hellodir`:

```
jspc -d Hellodir welcome.jsp shop.jsp checkout.jsp
```

The following command compiles all the JSP files in the specified webapp into class files under `Hellodir`:

```
jspc -d Hellodir -genclass -webapp /path_to_webapp_directory
```

To use these precompiled JSP in the web application, put the generated files under `Hellodir` into a JAR file, place the JAR file under `WEB-INF/lib` and set `reload-interval` property to `-1` in the `jsp-config` element of the `WEB-INF/sun-web.xml` file.

**SEE ALSO**    `asadmin(1M)`

list(1)

<b>NAME</b>	list – lists the configurable elements
<b>SYNOPSIS</b>	<b>list</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <i>4848</i> ] [--secure   -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true] [--monitor=false] <i>dotted_parent_element_name</i>
<b>DESCRIPTION</b>	<p>Lists the configurable element. On Solaris, quotes are needed when executing commands with * as the option value or operand.</p> <p>The dotted notation follows these guidelines:</p> <ul style="list-style-type: none"><li>■ Any list command that has a dotted name that is not followed by a wildcard (*) will get, as its result, the current node's immediate children. For example, list --monitor server lists all immediate children belonging to the server node.</li><li>■ Any list command that has a dotted name followed by a wildcard(*) will get, as its result, a hierarchical tree of children nodes from the current node. For example, list --monitor server.applications.* will list all children of applications and their subsequent child nodes and so on.</li><li>■ Any list command that has a dotted name preceded or followed by a wildcard (*) of the form <i>*dotted name</i> or <i>dotted * name</i> or <i>dotted name*</i> will get, as its result, all nodes and their children matching the regular expression created by the provided matching pattern.</li></ul>
<b>OPTIONS</b>	<p>--user authorized domain application server administrative username.</p> <p>--password password to administer the domain application server.</p> <p>--host machine name where the domain application server is running.</p> <p>--port port number of the domain application server listening for administration requests.</p> <p>--secure if true, uses SSL/TLS to communicate with the domain application server.</p> <p>--passwordfile file containing the domain application server password.</p> <p>--terse indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</p> <p>--echo setting to true will echo the command line statement on the standard output. Default is false.</p> <p>--interactive if set to true (default), only the required password options are prompted.</p> <p>--monitor defaults to false; if set to false, the configurable attribute values are returned. If set to true, the monitorable attribute values are</p>

returned.

**OPERANDS** *dotted\_parent\_element\_name* configurable or monitorable element name.

**EXAMPLES** **EXAMPLE 1** Using list to view all dotted-name prefixes

```
asadmin> list --user admin --password adminadmin
--port 5001 "*"
server
server.admin-service
server.admin-service.das-config
server.application-ref.MEjbApp
server.application-ref.__ejb_container_timer_app
server.application-ref.adminapp
server.application-ref.admingui
server.application-ref.com_sun_web_ui
server.applications
server.applications.j2ee-application.MEjbApp
server.applications.j2ee-application.__ejb_container_timer_app
server.applications.web-module.adminapp
server.applications.web-module.admingui
server.applications.web-module.com_sun_web_ui
server.ejb-container
server.http-service
server.http-service.http-listener.admin-listener
server.http-service.http-listener.http-listener-1
server.http-service.http-listener.http-listener-2
server.iiop-service
server.iiop-service.iiop-listener.SSL
server.iiop-service.iiop-listener.SSL.ssl
server.iiop-service.iiop-listener.SSL_MUTUALAUTH
server.iiop-service.iiop-listener.SSL_MUTUALAUTH.ssl1
server.iiop-service.iiop-listener.orb-listener-1
server.iiop-service.orb
server.java-config
server.jms-service
server.jms-service.jms-host.default_JMS_host
server.log-service
server.log-service.module-log-levels
server.mdb-container
server.monitoring-service
server.monitoring-service.module-monitoring-levels
server.resource-ref.jdbc/PointBase
server.resource-ref.jdbc/__TimerPool
server.resources
server.resources.jdbc-connection-pool.PointBasePool
server.resources.jdbc-connection-pool.__TimerPool
server.resources.jdbc-resource.jdbc/PointBase
server.resources.jdbc-resource.jdbc/__TimerPool
server.security-service
server.security-service.audit-module.default
server.security-service.auth-realm.certificate
server.security-service.auth-realm.file
server.security-service.jacc-provider.default
server.thread-pools
server.thread-pools.thread-pool.thread-pool-1
server.transaction-service
```

list(1)

**EXAMPLE 1** Using `list` to view all dotted-name prefixes *(Continued)*

```
server.virtual-server.__asadmin
server.virtual-server.server
server.web-container
```

**EXAMPLE 2** Using `list` for an application

```
asadmin> list --user admin --password adminadmin
--host localhost --port 4848 server.applications.j2ee-application
server.applications.j2ee-application.MEjbApp
server.applications.j2ee-application._ejb_container_timer_app
server.applications.j2ee-application.stateless-simple
```

**EXAMPLE 3** Using `list` for a web module

```
asadmin> list --user admin --password adminadmin
--host localhost --port 4848 server.applications.web-module
server.applications.web-module.adminapp
server.applications.web-module.adminguip
server.applications.web-module.com_sun_web_ui
```

**EXIT STATUS**

0	command executed successfully
1	error in executing the command

**SEE ALSO** `get(1)`, `set(1)`

<b>NAME</b>	list-acls – gets the access control lists
<b>SYNOPSIS</b>	<b>list-acls</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--passwordfile <i>filename</i> ] [--secure -s] <i>instance_name</i>
<b>DESCRIPTION</b>	Gets the access control lists associated with the named server instance.
<b>OPTIONS</b>	<p>--user                    administrative user associated for the instance.</p> <p>--password                administrative password corresponding to the administrative user.</p> <p>--host                    host name of the machine hosting the administrative instance.</p> <p>--port                    administrative port number associated with the administrative host.</p> <p>--secure                  indicates communication with the administrative instance in secured mode.</p> <p>--passwordfile            file containing passwords appropriate for the command (e.g., administrative instance).</p>
<b>OPERANDS</b>	<i>instance_name</i> name of the instance.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using list-acls</p> <pre>asadmin&gt; list-acls --user admin --password adminadmin --host fuyako --port 7070 server1 acl1 sampleACL</pre> <p>Where: <i>acl1</i> and <i>sampleACL</i> are the names of the ACLs listed.</p>
<b>EXIT STATUS</b>	<p>0    command executed successfully</p> <p>1    error in executing the command</p>
<b>INTERFACE EQUIVALENT</b>	Access Control List page
<b>SEE ALSO</b>	create-acl(1), delete-acl(1)

## list-admin-objects(1)

<b>NAME</b>	list-admin-objects – gets all the administered objects
<b>SYNOPSIS</b>	<b>list-admin-objects</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure   -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true]
<b>DESCRIPTION</b>	Lists all the administered objects. This command is supported in remote mode only.
<b>OPTIONS</b>	--user authorized domain application server administrative username.  --password password to administer the domain application server.  --host machine name where the domain application server is running.  --port port number of the domain application server listening for administration requests.  --secure if true, uses SSL/TLS to communicate with the domain application server.  --passwordfile file containing the domain application server password.  --terse indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.  --echo setting to true will echo the command line statement on the standard output. Default is false.  --interactive if set to true (default), only the required password options are prompted.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using list-admin-objects  asadmin> <b>list-admin-objects</b> --user <b>admin</b> --password <b>admin123</b> Command list-admin-objects executed successfully
<b>EXIT STATUS</b>	0 command executed successfully  1 error in executing the command
<b>SEE ALSO</b>	create-admin-object(1), delete-admin-object(1)

<b>NAME</b>	list-audit-modules – lists all the audit-modules
<b>SYNOPSIS</b>	<b>list-audit-modules</b> <b>--user</b> <i>admin_user</i> [ <b>--password</b> <i>admin_password</i> ] [ <b>--host</b> <i>localhost</i> ] [ <b>--port</b> <b>4848</b> ] [ <b>--secure</b>   <b>-s</b> ] [ <b>--passwordfile</b> <i>filename</i> ] [ <b>--terse=false</b> ] [ <b>--echo=false</b> ] [ <b>--interactive=true</b> ]
<b>DESCRIPTION</b>	Lists all the audit modules. This command is supported in remote mode only.
<b>OPTIONS</b>	<p><b>--user</b>                    authorized domain application server administrative username.</p> <p><b>--password</b>              password to administer the domain application server.</p> <p><b>--host</b>                    machine name where the domain application server is running.</p> <p><b>--port</b>                    port number of the domain application server listening for administration requests.</p> <p><b>--secure</b>                  if true, uses SSL/TLS to communicate with the domain application server.</p> <p><b>--passwordfile</b>          file containing the domain application server password.</p> <p><b>--terse</b>                   indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</p> <p><b>--echo</b>                    setting to true will echo the command line statement on the standard output. Default is false.</p> <p><b>--interactive</b>            if set to true (default), only the required password options are prompted.</p>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using list-audit-modules</p> <pre>asadmin&gt; list-audit-modules --user admin1 --password adminadmin1 --host pigeon --port 5001 Command list-audit-modules executed successfully</pre>
<b>EXIT STATUS</b>	<p>0    command executed successfully</p> <p>1    error in executing the command</p>
<b>SEE ALSO</b>	create-audit-module(1), delete-audit-module(1)

## list-authdbs(1)

<b>NAME</b>	list-authdbs – gets the authorized database														
<b>SYNOPSIS</b>	<pre><b>list-authdbs</b>   --user <i>admin_user</i> [--password <i>admin_password</i>] [--host <i>localhost</i>]   [--port <b>4848</b>] [--passwordfile <i>filename</i>] [--secure -s] [--instance   <i>instance_name</i>] --virtualserver <i>virtualserver_ID</i> <i>authdb_ID</i></pre>														
<b>DESCRIPTION</b>	Gets the access control lists associated with the named server instance.														
<b>OPTIONS</b>	<table><tr><td>--user</td><td>administrative user associated for the instance.</td></tr><tr><td>--password</td><td>administrative password corresponding to the administrative user.</td></tr><tr><td>--host</td><td>host name of the machine hosting the administrative instance.</td></tr><tr><td>--port</td><td>administrative port number associated with the administrative host.</td></tr><tr><td>--passwordfile</td><td>file containing passwords appropriate for the command (e.g., administrative instance).</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the administrative instance.</td></tr><tr><td>--virtualserver</td><td>virtual server ID. It can also be referred to as the variable <code>\$id</code> in an <code>obj.conf</code> file. A virtual server ID cannot begin with a number.</td></tr></table>	--user	administrative user associated for the instance.	--password	administrative password corresponding to the administrative user.	--host	host name of the machine hosting the administrative instance.	--port	administrative port number associated with the administrative host.	--passwordfile	file containing passwords appropriate for the command (e.g., administrative instance).	--secure	if true, uses SSL/TLS to communicate with the administrative instance.	--virtualserver	virtual server ID. It can also be referred to as the variable <code>\$id</code> in an <code>obj.conf</code> file. A virtual server ID cannot begin with a number.
--user	administrative user associated for the instance.														
--password	administrative password corresponding to the administrative user.														
--host	host name of the machine hosting the administrative instance.														
--port	administrative port number associated with the administrative host.														
--passwordfile	file containing passwords appropriate for the command (e.g., administrative instance).														
--secure	if true, uses SSL/TLS to communicate with the administrative instance.														
--virtualserver	virtual server ID. It can also be referred to as the variable <code>\$id</code> in an <code>obj.conf</code> file. A virtual server ID cannot begin with a number.														
<b>OPERANDS</b>	<i>instance_name</i> name of the instance.														
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using list-authdbs</p> <pre>asadmin&gt; lsit-authdbs --user admin --password adminadmin --host fuyako --port 7070 --virtualserver default sampleAuth</pre> <p>Where: <code>default</code> and <code>sampleAuth</code> are the authdb IDs in virtual server <code>server1</code> and instance <code>server1</code> listed.</p> <pre>asadmin% list-authdbs --instance server1</pre>														
<b>EXIT STATUS</b>	<table><tr><td>0</td><td>command executed successfully</td></tr><tr><td>1</td><td>error in executing the command</td></tr></table>	0	command executed successfully	1	error in executing the command										
0	command executed successfully														
1	error in executing the command														
<b>SEE ALSO</b>	create-authdb(1), delete-authdb(1)														



<b>NAME</b>	list-auth-realms – lists the authorized realms
<b>SYNOPSIS</b>	<b>list-auth-realms</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true]
<b>DESCRIPTION</b>	Lists the authorized realms. This command is supported in remote mode only.
<b>OPTIONS</b>	<p>--user                authorized domain application server administrative username.</p> <p>--password           password to administer the domain application server.</p> <p>--host                machine name where the domain application server is running.</p> <p>--port                port number of the domain application server listening for administration requests.</p> <p>--secure              if true, uses SSL/TLS to communicate with the domain application server.</p> <p>--passwordfile       file containing the domain application server password.</p> <p>--terse               indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</p> <p>--echo                setting to true will echo the command line statement on the standard output. Default is false.</p> <p>--interactive        if set to true (default), only the required password options are prompted.</p>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using list-auth-realms</p> <pre>asadmin&gt; list-auth-realms --user admin --password adminadmin --host localhost --port 4848 file ldap certificate db Command list-auth-realms executed successfully</pre> <p>Where file, ldap, certificate, and db are the auth realms listed.</p>
<b>EXIT STATUS</b>	<p>0    command executed successfully</p> <p>1    error in executing the command</p>
<b>SEE ALSO</b>	create-auth-realm(1), delete-auth-realm(1)

## list-components(1)

<b>NAME</b>	list-components – Lists deployed components																				
<b>SYNOPSIS</b>	<pre><b>list-components</b>   --user <i>admin_user</i> [--password <i>admin_password</i>] [--host <i>localhost</i>]   [--port <b>4848</b>] [--secure   -s] [--passwordfile <i>filename</i>]   [--terse=false] [--echo=false] [--interactive]   [--type <b>application</b>   <b>ejb</b>   <b>web</b>   <b>connector</b>]</pre>																				
<b>DESCRIPTION</b>	<p><code>list-components</code> lists your deployed J2EE components. If the <code>--type</code> option is not specified, all components are listed. The available type values are: <code>application</code> (default), <code>ejb</code>, <code>web</code>, and <code>connector</code>. This command is supported in remote mode only.</p>																				
<b>OPTIONS</b>	<table><tr><td><code>--user</code></td><td>authorized domain application server administrative username.</td></tr><tr><td><code>--password</code></td><td>password to administer the domain application server.</td></tr><tr><td><code>--host</code></td><td>machine name where the domain application server is running.</td></tr><tr><td><code>--port</code></td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td><code>--secure</code></td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td><code>--passwordfile</code></td><td>file containing the domain application server password.</td></tr><tr><td><code>--terse</code></td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.</td></tr><tr><td><code>--echo</code></td><td>setting to true will echo the command line statement on the standard output.</td></tr><tr><td><code>--interactive</code></td><td>prompts you for the required options that are not already specified.</td></tr><tr><td><code>--type</code></td><td>identifies the type of component to be listed; defaults to <code>application</code>.</td></tr></table>	<code>--user</code>	authorized domain application server administrative username.	<code>--password</code>	password to administer the domain application server.	<code>--host</code>	machine name where the domain application server is running.	<code>--port</code>	port number of the domain application server listening for administration requests.	<code>--secure</code>	if true, uses SSL/TLS to communicate with the domain application server.	<code>--passwordfile</code>	file containing the domain application server password.	<code>--terse</code>	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.	<code>--echo</code>	setting to true will echo the command line statement on the standard output.	<code>--interactive</code>	prompts you for the required options that are not already specified.	<code>--type</code>	identifies the type of component to be listed; defaults to <code>application</code> .
<code>--user</code>	authorized domain application server administrative username.																				
<code>--password</code>	password to administer the domain application server.																				
<code>--host</code>	machine name where the domain application server is running.																				
<code>--port</code>	port number of the domain application server listening for administration requests.																				
<code>--secure</code>	if true, uses SSL/TLS to communicate with the domain application server.																				
<code>--passwordfile</code>	file containing the domain application server password.																				
<code>--terse</code>	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.																				
<code>--echo</code>	setting to true will echo the command line statement on the standard output.																				
<code>--interactive</code>	prompts you for the required options that are not already specified.																				
<code>--type</code>	identifies the type of component to be listed; defaults to <code>application</code> .																				
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using <code>list-components</code></p> <pre>asadmin&gt; list-components --type application sampleApp J2EE-application Command list-components executed successfully</pre> <p>Where: the applications that were deployed are listed.</p>																				
<b>EXIT STATUS</b>	<table><tr><td>0</td><td>command executed successfully</td></tr><tr><td>1</td><td>error in executing the command</td></tr></table>	0	command executed successfully	1	error in executing the command																
0	command executed successfully																				
1	error in executing the command																				
<b>SEE ALSO</b>	<code>show-component-status(1)</code> , <code>list-sub-components(1)</code>																				

<b>NAME</b>	list-connector-connection-pools – gets all the connection pools
<b>SYNOPSIS</b>	<b>list-connector-connection-pools</b> --user <i>admin_user</i> [ <b>--password</b> <i>admin_password</i> ] [ <b>--host</b> <i>localhost</i> ] [ <b>--port</b> <b>4848</b> ] [ <b>--secure</b>   <b>-s</b> ] [ <b>--passwordfile</b> <i>filename</i> ] [ <b>--terse</b> =false] [ <b>--echo</b> =false] [ <b>--interactive</b> =true]
<b>DESCRIPTION</b>	gets all the connector connection pools. This command is supported in remote mode only.
<b>OPTIONS</b>	<p><b>--user</b> authorized domain application server administrative username.</p> <p><b>--password</b> password to administer the domain application server.</p> <p><b>--host</b> machine name where the domain application server is running.</p> <p><b>--port</b> port number of the domain application server listening for administration requests.</p> <p><b>--secure</b> if true, uses SSL/TLS to communicate with the domain application server.</p> <p><b>--passwordfile</b> file containing the domain application server password.</p> <p><b>--terse</b> indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</p> <p><b>--echo</b> setting to true will echo the command line statement on the standard output. Default is false.</p> <p><b>--interactive</b> if set to true (default), only the required password options are prompted.</p>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using list-connector-connection-pools</p> <pre>asadmin&gt; list-connector-connection-pools --user admin --password adminadmin</pre>
<b>EXIT STATUS</b>	<p>0 command executed successfully</p> <p>1 error in executing the command</p>
<b>SEE ALSO</b>	create-connector-connection-pool(1), delete-connector-connection-pool(1)

## list-connector-resources(1)

<b>NAME</b>	list-connector-resources – gets all the connector resources
<b>SYNOPSIS</b>	<b>list-connector-resources</b> <i>--user admin_user</i> <i>[--password admin_password] [--host localhost] [--port 4848]</i> <i>[--secure -s] [--passwordfile filename] [--terse=false]</i> <i>[--echo=false] [--interactive=true]</i>
<b>DESCRIPTION</b>	Gets all the connector resources. This command is supported in remote mode only.
<b>OPTIONS</b>	<b>--user</b> authorized domain application server administrative username. <b>--password</b> password to administer the domain application server. <b>--host</b> machine name where the domain application server is running. <b>--port</b> port number of the domain application server listening for administration requests. <b>--secure</b> if true, uses SSL/TLS to communicate with the domain application server. <b>--passwordfile</b> file containing the domain application server password. <b>--terse</b> indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false. <b>--echo</b> setting to true will echo the command line statement on the standard output. Default is false. <b>--interactive</b> if set to true (default), only the required password options are prompted.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using the list-connector-resources command asadmin> <b>list-connector-resources --user admin1</b> <b>--password adminadmin1 --host pigeon --port 5001</b>  This will list all the connector resources that have been created.
<b>EXIT STATUS</b>	0 command executed successfully 1 error in executing the command
<b>SEE ALSO</b>	create-connector-resource(1), delete-connector-resource(1)

## list-connector-security-maps(1)

<b>NAME</b>	list-connector-security-maps – lists the security maps for the named connector connection pool
<b>SYNOPSIS</b>	<b>list-connector-security-maps</b> --user <i>admin_user</i> [ <b>--password</b> <i>admin_password</i> ] [ <b>--host</b> <i>localhost</i> ] [ <b>--port</b> <b>4848</b> ] [ <b>--secure -s</b> ] [ <b>--passwordfile</b> <i>filename</i> ] [ <b>--terse=false</b> ] [ <b>--echo=false</b> ] [ <b>--interactive=true</b> ] [ <b>--verbose=false</b> ] [ <b>--securitymap</b> <i>mapname</i> ] <i>pool_name</i>
<b>DESCRIPTION</b>	lists the security map belonging to the named connector connection pool.  This command is supported in remote mode only.
<b>OPTIONS</b>	<b>--user</b> authorized domain application server administrative username.  <b>--password</b> password to administer the domain application server.  <b>--host</b> machine name where the domain application server is running.  <b>--port</b> port number of the domain application server listening for administration requests.  <b>--secure</b> if true, uses SSL/TLS to communicate with the domain application server.  <b>--passwordfile</b> file containing the domain application server password.  <b>--terse</b> indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.  <b>--echo</b> setting to true will echo the command line statement on the standard output. Default is false.  <b>--interactive</b> if set to true (default), only the required password options are prompted.  <b>--verbose</b> lists the identify, principals, and the security name.  <b>--securitymap</b> name of the security map.
<b>OPERANDS</b>	<i>poolname</i> name of the pool.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using list-connector-security-maps with security map option asadmin> <b>list-connector-security-maps</b> --user <b>admin</b> --password <b>adminadmin</b> --securitymap <b>mysecuremap</b> <b>securityPool1</b> Command list-connector-security-maps executed successfully  One security map (mysecuremap) is listed for the securityPool1 pool.

## list-connector-security-maps(1)

**EXAMPLE 2** Using `list-connector-security-maps`

```
asadmin> list-connector-security-maps --user admin --password adminadmin  
securityPool1
```

Command `list-connector-security-maps` executed successfully

All the security maps are listed for the `securityPool1` pool.

**EXIT STATUS**

0	command executed successfully
1	error in executing the command

**SEE ALSO** `delete-connector-security-map(1)`, `create-connector-security-map(1)`,  
`update-connector-security-map(1)`

<b>NAME</b>	list-custom-resources – gets all the custom resources
<b>SYNOPSIS</b>	<b>list-custom-resources</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true]
<b>DESCRIPTION</b>	Gets all the custom resources. This command is supported in remote mode only.
<b>OPTIONS</b>	<p>--user                    authorized domain application server administrative username.</p> <p>--password               password to administer the domain application server.</p> <p>--host                    machine name where the domain application server is running.</p> <p>--port                    port number of the domain application server listening for administration requests.</p> <p>--secure                  if true, uses SSL/TLS to communicate with the domain application server.</p> <p>--passwordfile          file containing the domain application server password.</p> <p>--terse                   indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</p> <p>--echo                    setting to true will echo the command line statement on the standard output. Default is false.</p> <p>--interactive            if set to true (default), only the required password options are prompted.</p>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using list-custom-resources</p> <pre>asadmin&gt; list-custom-resources --user admin1 --password adminadmin1 --host pigeon --port 5001 sample_custom_resource</pre> <p>Where: <code>sample_custom_resource</code> is the custom resource listed.</p>
<b>EXIT STATUS</b>	<p>0    command executed successfully</p> <p>1    error in executing the command</p>
<b>SEE ALSO</b>	create-custom-resource(1), delete-custom-resource(1)

## list-domains(1)

<b>NAME</b>	list-domains – lists the domains in the given domains directory
<b>SYNOPSIS</b>	<b>list-domains</b> [--domaindir <i>install_dir/domains</i> ] [--terse=false] [--echo=false]
<b>DESCRIPTION</b>	list-domains lists the domains in the given domains directory. This command is supported in local mode only.
<b>OPTIONS</b>	--domaindir     directory where the domains are located. If specified, path must be accessible in the filesystem. If not specified, the domains in the default <i>install_dir/domains</i> directory are listed.  --terse           indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.  --echo            setting to true will echo the command line statement on the standard output.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using list-domains  asadmin> <b>list-domains</b> List of domains: domain1 running samples not running  Where: the domain1 and samples are listed and their status printed.
<b>EXIT STATUS</b>	0     command executed successfully 1     error in executing the command
<b>SEE ALSO</b>	create-domain(1), delete-domain(1), start-domain(1), stop-domain(1)



<b>NAME</b>	list-file-groups – lists the file groups
<b>SYNOPSIS</b>	<b>list-file-groups</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true] [--authrealmname <i>auth_realm_name</i> ] [--name <i>username</i> ]
<b>DESCRIPTION</b>	Lists the available groups in the file user. If the name option is not specified, then all groups are listed.  This command is supported in remote mode only.
<b>OPTIONS</b>	--user                    authorized domain application server administrative username.  --password                password to administer the domain application server.  --host                    machine name where the domain application server is running.  --port                    port number of the domain application server listening for administration requests.  --secure                  if true, uses SSL/TLS to communicate with the domain application server.  --passwordfile            file containing the domain application server password.  --terse                    indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.  --echo                    setting to true will echo the command line statement on the standard output. Default is false.  --interactive             if set to true (default), only the required password options are prompted.  --authrealmname          filename where you have different stores for file auth realm.  --name                    name of the file user.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using the list-file-groups command  asadmin> list-file-groups --user admin1 --password adminadmin1 --host pigeon --port 5001 --name sample_user Command list-file-groups executed successfully
<b>EXIT STATUS</b>	0    command executed successfully 1    error in executing the command

list-file-groups(1)

**SEE ALSO** delete-file-user(1), update-file-user(1), create-file-user(1),  
list-file-users(1)

<b>NAME</b>	list-file-users – lists the file users																				
<b>SYNOPSIS</b>	<b>list-file-users</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true] [--authrealmname <i>auth_realm_name</i> ]																				
<b>DESCRIPTION</b>	Lists all the file users. If the <i>auth_realm_name</i> is not specified, an entry is created in the default keyfile. If <i>auth_realm_name</i> is specified, an entry is created in the keyfile where the auth-realm name in the domain.xml file points to. This command is supported in remote mode only.																				
<b>OPTIONS</b>	<table border="0"> <tr> <td style="padding-right: 20px;">--user</td> <td>authorized domain application server administrative username.</td> </tr> <tr> <td>--password</td> <td>password to administer the domain application server.</td> </tr> <tr> <td>--host</td> <td>machine name where the domain application server is running.</td> </tr> <tr> <td>--port</td> <td>port number of the domain application server listening for administration requests.</td> </tr> <tr> <td>--secure</td> <td>if true, uses SSL/TLS to communicate with the domain application server.</td> </tr> <tr> <td>--passwordfile</td> <td>file containing the domain application server password.</td> </tr> <tr> <td>--terse</td> <td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td> </tr> <tr> <td>--echo</td> <td>setting to true will echo the command line statement on the standard output. Default is false.</td> </tr> <tr> <td>--interactive</td> <td>if set to true (default), only the required password options are prompted.</td> </tr> <tr> <td>--authrealmname</td> <td>name, in the domain.xml file, where you have different stores for file auth realm.</td> </tr> </table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	--echo	setting to true will echo the command line statement on the standard output. Default is false.	--interactive	if set to true (default), only the required password options are prompted.	--authrealmname	name, in the domain.xml file, where you have different stores for file auth realm.
--user	authorized domain application server administrative username.																				
--password	password to administer the domain application server.																				
--host	machine name where the domain application server is running.																				
--port	port number of the domain application server listening for administration requests.																				
--secure	if true, uses SSL/TLS to communicate with the domain application server.																				
--passwordfile	file containing the domain application server password.																				
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																				
--echo	setting to true will echo the command line statement on the standard output. Default is false.																				
--interactive	if set to true (default), only the required password options are prompted.																				
--authrealmname	name, in the domain.xml file, where you have different stores for file auth realm.																				
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the list-file-users command</p> <pre>asadmin&gt; list-file-users --user admin1 --password adminadmin1 --host pigeon --port 5001 --authrealmname auth-realm1 Command list-file-user executed successfully</pre>																				
<b>EXIT STATUS</b>	<table border="0"> <tr> <td style="padding-right: 20px;">0</td> <td>command executed successfully</td> </tr> <tr> <td>1</td> <td>error in executing the command</td> </tr> </table>	0	command executed successfully	1	error in executing the command																
0	command executed successfully																				
1	error in executing the command																				
<b>SEE ALSO</b>	delete-file-user(1), update-file-user(1), create-file-user(1), list-file-groups(1)																				

## list-http-listeners(1)

<b>NAME</b>	list-http-listeners – gets the HTTP listeners																		
<b>SYNOPSIS</b>	<pre><b>list-http-listeners</b> --user <i>admin_user</i> [--password <i>admin_password</i>]   [--host <i>localhost</i>] [--port <b>4848</b>] [--secure -s]   [--passwordfile <i>filename</i>] [--terse=false] [--echo=false]   [--interactive=true]</pre>																		
<b>DESCRIPTION</b>	Gets the HTTP listeners. This command is supported in remote mode only.																		
<b>OPTIONS</b>	<table><tr><td>--user</td><td>authorized domain application server administrative username.</td></tr><tr><td>--password</td><td>password to administer the domain application server.</td></tr><tr><td>--host</td><td>machine name where the domain application server is running.</td></tr><tr><td>--port</td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td>--passwordfile</td><td>file containing the domain application server password.</td></tr><tr><td>--terse</td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td></tr><tr><td>--echo</td><td>setting to true will echo the command line statement on the standard output. Default is false.</td></tr><tr><td>--interactive</td><td>if set to true (default), only the required password options are prompted.</td></tr></table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	--echo	setting to true will echo the command line statement on the standard output. Default is false.	--interactive	if set to true (default), only the required password options are prompted.
--user	authorized domain application server administrative username.																		
--password	password to administer the domain application server.																		
--host	machine name where the domain application server is running.																		
--port	port number of the domain application server listening for administration requests.																		
--secure	if true, uses SSL/TLS to communicate with the domain application server.																		
--passwordfile	file containing the domain application server password.																		
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																		
--echo	setting to true will echo the command line statement on the standard output. Default is false.																		
--interactive	if set to true (default), only the required password options are prompted.																		
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using list-http-listeners</p> <pre>asadmin&gt; list-http-listeners --user admin1 --password adminadmin1 --host pigeon --port 5001 http-listener-1 http-listener-2 admin-listener Command list-http-listeners executed successfully</pre>																		
<b>EXIT STATUS</b>	<table><tr><td>0</td><td>command executed successfully</td></tr><tr><td>1</td><td>error in executing the command</td></tr></table>	0	command executed successfully	1	error in executing the command														
0	command executed successfully																		
1	error in executing the command																		
<b>SEE ALSO</b>	create-http-listener(1), delete-http-listener(1)																		

<b>NAME</b>	list-iop-listeners – gets the IIOP listeners
<b>SYNOPSIS</b>	<pre>list-iop-listeners   --user admin_user [--password admin_password] [--host localhost]   [--port 4848] [--secure -s] [--passwordfile filename]   [--terse=false] [--echo=false] [--interactive=true]</pre>
<b>DESCRIPTION</b>	Gets the IIOP listeners. This command is supported in remote mode only.
<b>OPTIONS</b>	<pre>--user          authorized domain application server administrative                   username.  --password      password to administer the domain application server.  --host          machine name where the domain application server is running.  --port          port number of the domain application server listening for                   administration requests.  --secure        if true, uses SSL/TLS to communicate with the domain                   application server.  --passwordfile  file containing the domain application server password.  --terse         indicates that any output data must be very concise, typically                   avoiding human-friendly sentences and favoring                   well-formatted data for consumption by a script. Default is                   false.  --echo          setting to true will echo the command line statement on the                   standard output. Default is false.  --interactive   if set to true (default), only the required password options are                   prompted.</pre>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using list-iop-listeners</p> <pre>asadmin&gt; list-iop-listeners --user admin --password adminadmin --host fuyako --port 7070 orb-listener-1 sample_iiop_listener</pre> <p>Where: orb-listener-1 and sample_iiop_listener are the IIOP listeners listed.</p>
<b>EXIT STATUS</b>	<pre>0    command executed successfully 1    error in executing the command</pre>
<b>SEE ALSO</b>	create-iop-listener(1), delete-iop-listener(1)

## list-instances(1)

<b>NAME</b>	list-instances – lists all the instances in the server																
<b>SYNOPSIS</b>	<b>list-instances</b> [--user <i>admin_user</i> ] [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <i>4848</i> ] [--domain <i>domain_name</i> ] [--local=false] [--passwordfile <i>filename</i> ] [--secure   -s ]																
<b>DESCRIPTION</b>	Use the <code>list-instances</code> to list all the instance in the server. The <code>list-instances</code> command can be run both locally and remotely. To list remote instances, the named administration server must be running on the hostname and port number specified. The user authenticates using the password identified for the administration server.																
<b>OPTIONS</b>	<table><tr><td>--user</td><td>administrative user associated for the instance.</td></tr><tr><td>--password</td><td>administrative password corresponding to the administrative user.</td></tr><tr><td>--host</td><td>host name of the machine hosting the administrative instance.</td></tr><tr><td>--port</td><td>port number associated with the administrative host.</td></tr><tr><td>--domain</td><td>name of the domain.</td></tr><tr><td>--local</td><td>determines if the command should delegate the request to administrative instance or run locally.</td></tr><tr><td>--passwordfile</td><td>file containing passwords appropriate for the command (e.g., administrative instance).</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the administrative instance.</td></tr></table>	--user	administrative user associated for the instance.	--password	administrative password corresponding to the administrative user.	--host	host name of the machine hosting the administrative instance.	--port	port number associated with the administrative host.	--domain	name of the domain.	--local	determines if the command should delegate the request to administrative instance or run locally.	--passwordfile	file containing passwords appropriate for the command (e.g., administrative instance).	--secure	if true, uses SSL/TLS to communicate with the administrative instance.
--user	administrative user associated for the instance.																
--password	administrative password corresponding to the administrative user.																
--host	host name of the machine hosting the administrative instance.																
--port	port number associated with the administrative host.																
--domain	name of the domain.																
--local	determines if the command should delegate the request to administrative instance or run locally.																
--passwordfile	file containing passwords appropriate for the command (e.g., administrative instance).																
--secure	if true, uses SSL/TLS to communicate with the administrative instance.																
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using list-instances in local mode</p> <pre>asadmin&gt; list-instances --domain1 --local admin-server running server1 running</pre> <p>Where: the <code>server1</code> and <code>admin-server</code> instances for the <code>domain1</code> domain is listed.</p> <p><b>EXAMPLE 2</b> Using list-instances in remote mode</p> <pre>asadmin&gt; list-instances --user admin --passwordfile passwords.txt --host localhost --port 4848 server1 [mayank:80] running</pre> <p>Where: the <code>server1</code> instance associated with the specified user, passwords, host, and port number specified is listed for the remote machine.</p>																
<b>EXIT STATUS</b>	0 command executed successfully 1 error in executing the command																
<b>INTERFACE EQUIVALENT</b>	Server Instance page																
<b>SEE ALSO</b>	<code>show-instance-status(1)</code>																

<b>NAME</b>	list-javamail-resources – gets all the Javamail resources
<b>SYNOPSIS</b>	<b>list-javamail-resources</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true]
<b>DESCRIPTION</b>	Gets all the Javamail resources. This command can only be run remotely.
<b>OPTIONS</b>	<p>--user                authorized domain application server administrative username.</p> <p>--password           password to administer the domain application server.</p> <p>--host                machine name where the domain application server is running.</p> <p>--port                port number of the domain application server listening for administration requests.</p> <p>--secure              if true, uses SSL/TLS to communicate with the domain application server.</p> <p>--passwordfile       file containing the domain application server password.</p> <p>--terse               indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.</p> <p>--echo                setting to true will echo the command line statement on the standard output.</p> <p>--interactive        prompts you for the required options that are not already specified.</p>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using list-javamail-resources</p> <pre>asadmin&gt; list-javamail-resources --user admin1 --password adminadmin1 --host pigeon --port 5001 mail/MyMailSession Command list-javamail-resources executed successfully</pre>
<b>EXIT STATUS</b>	<p>0    command executed successfully</p> <p>1    error in executing the command</p>
<b>SEE ALSO</b>	create-javamail-resource(1), delete-javamail-resource(1)

## list-jdbc-connection-pools(1)

<b>NAME</b>	list-jdbc-connection-pools – gets all the JDBC connection pools
<b>SYNOPSIS</b>	<pre>list-jdbc-connection-pools --user admin_user [--password admin_password] [--host localhost] [--port 4848] [--secure -s] --passwordfile filename] [--terse=false] [--echo=false] [--interactive]</pre>
<b>DESCRIPTION</b>	Gets all the JDBC connection pools. This command is supported in remote mode only.
<b>OPTIONS</b>	<p>--user authorized domain application server administrative username.</p> <p>--password password to administer the domain application server.</p> <p>--host machine name where the domain application server is running.</p> <p>--port port number of the domain application server listening for administration requests.</p> <p>--secure if true, uses SSL/TLS to communicate with the domain application server.</p> <p>--passwordfile file containing the domain application server password.</p> <p>--terse indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.</p> <p>--echo setting to true will echo the command line statement on the standard output.</p> <p>--interactive prompts you for the required options that are not already specified.</p>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using list-jdbc-connection-pools</p> <pre>asadmin&gt; list-jdbc-connection-pools --user admin --password adminadmin --host fuyako --port 7070 server XA_connection_pool</pre> <p>Where: XA_connection_pool is the JDBC connection listed.</p>
<b>EXIT STATUS</b>	<p>0 command executed successfully</p> <p>1 error in executing the command</p>
<b>SEE ALSO</b>	create-jdbc-connection-pool(1), delete-jdbc-connection-pool(1)



<b>NAME</b>	list-jdbc-resources – gets all the JDBC resources
<b>SYNOPSIS</b>	<b>list-jdbc-resources</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true]
<b>DESCRIPTION</b>	Lists all the JDBC resources. This command is supported in remote mode only.
<b>OPTIONS</b>	<p>--user                    authorized domain application server administrative username.</p> <p>--password                password to administer the domain application server.</p> <p>--host                    machine name where the domain application server is running.</p> <p>--port                    port number of the domain application server listening for administration requests.</p> <p>--secure                  if true, uses SSL/TLS to communicate with the domain application server.</p> <p>--passwordfile            file containing the domain application server password.</p> <p>--terse                    indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.</p> <p>--echo                    setting to true will echo the command line statement on the standard output.</p> <p>--interactive             prompts you for the required options that are not already specified.</p>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the list-jdbc-resources command</p> <pre>asadmin&gt; list-jdbc-resources --user admin1 --password adminadmin1 --host pigeon --port 5001 sample_jdbc_resource Command list-jdbc-resources executed successfully</pre> <p>Where: <i>sample_jdbc_resource</i> is the JDBC resource listed.</p>
<b>EXIT STATUS</b>	<p>0    command executed successfully</p> <p>1    error in executing the command</p>
<b>SEE ALSO</b>	create-jdbc-resource(1), delete-jdbc-resource(1)

## list-jmsdest(1)

<b>NAME</b>	list-jmsdest – gets all the physical destinations
<b>SYNOPSIS</b>	<b>list-jmsdest</b> <b>--user</b> <i>admin_user</i> [ <b>--password</b> <i>admin_password</i> ] [ <b>--host</b> <i>localhost</i> ] [ <b>--port</b> <b>4848</b> ] [ <b>--secure</b>   <b>-s</b> ] [ <b>--passwordfile</b> <i>filename</i> ] [ <b>--terse=false</b> ] [ <b>--echo=false</b> ] [ <b>--interactive</b> ] [ <b>--desttype</b>   <b>-T</b> <i>topic</i>   <i>queue</i> ]
<b>DESCRIPTION</b>	Gets all the physical JMS destinations. This command is supported in remote mode only.
<b>OPTIONS</b>	<b>--user</b> authorized domain application server administrative username. <b>--password</b> password to administer the domain application server. <b>--host</b> machine name where the domain application server is running. <b>--port</b> port number of the domain application server listening for administration requests. <b>--secure</b> if true, uses SSL/TLS to communicate with the domain application server. <b>--passwordfile</b> file containing the domain application server password. <b>--terse</b> indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. <b>--echo</b> setting to true will echo the command line statement on the standard output. <b>--interactive</b> prompts you for the required options that are not already specified. <b>--desttype</b> type of JMS destination. Valid values are <i>topic</i> , and <i>queue</i> .
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using <code>list-jmsdest</code> <pre>asadmin&gt; list-jmsdest ----user admin --password adminadmin --host bluestar --port 4848 server PhysicalQueue queue {} PhysicalTopic topic {} Command list-jmsdest executed successfully</pre>
<b>EXIT STATUS</b>	0 command executed successfully 1 error in executing the command
<b>SEE ALSO</b>	<code>create-jmsdest(1)</code> , <code>delete-jmsdest(1)</code>

**NAME** list-jmsobj – gets all the named objects

**SYNOPSIS** `list-jmsobj --instance instance_name --objtype | -o object_type`

**DESCRIPTION** Gets all the named destinationobjects.

**OPTIONS** --instance the name of the instance.  
--objtype

**EXAMPLES** asadmin% `list-jmsobj --instance server1 --objtype xxxx`

**INTERFACE EQUIVALENT** unknown

**SEE ALSO** create-jmsobj(1) delete-jmsobj(1)

## list-jms-resources(1)

<b>NAME</b>	list-jms-resources – gets all the JMS resources																				
<b>SYNOPSIS</b>	<pre><b>list-jms-resources</b> --user <i>admin_user</i>   [--password <i>admin_password</i>] [--host <i>localhost</i>] [--port <b>4848</b>]   [--secure -s] [--passwordfile <i>filename</i>] [--terse=false]   [--echo=false] [--interactive=true] [--restype <i>resource_type</i>]</pre>																				
<b>DESCRIPTION</b>	Gets all the JMS resources. This command can only be run remotely.																				
<b>OPTIONS</b>	<table><tr><td>--user</td><td>authorized domain application server administrative username.</td></tr><tr><td>--password</td><td>password to administer the domain application server.</td></tr><tr><td>--host</td><td>machine name where the domain application server is running.</td></tr><tr><td>--port</td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td>--passwordfile</td><td>file containing the domain application server password.</td></tr><tr><td>--terse</td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.</td></tr><tr><td>--echo</td><td>setting to true will echo the command line statement on the standard output.</td></tr><tr><td>--interactive</td><td>prompts you for the required options that are not already specified.</td></tr><tr><td>--restype</td><td>JMS resource type which can be: <code>javax.jms.Topic</code>, <code>javax.jms.Queue</code>, <code>javax.jms.TopicConnectionFactory</code>, <code>javax.jms.QueueConnectionFactory</code>.</td></tr></table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.	--echo	setting to true will echo the command line statement on the standard output.	--interactive	prompts you for the required options that are not already specified.	--restype	JMS resource type which can be: <code>javax.jms.Topic</code> , <code>javax.jms.Queue</code> , <code>javax.jms.TopicConnectionFactory</code> , <code>javax.jms.QueueConnectionFactory</code> .
--user	authorized domain application server administrative username.																				
--password	password to administer the domain application server.																				
--host	machine name where the domain application server is running.																				
--port	port number of the domain application server listening for administration requests.																				
--secure	if true, uses SSL/TLS to communicate with the domain application server.																				
--passwordfile	file containing the domain application server password.																				
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.																				
--echo	setting to true will echo the command line statement on the standard output.																				
--interactive	prompts you for the required options that are not already specified.																				
--restype	JMS resource type which can be: <code>javax.jms.Topic</code> , <code>javax.jms.Queue</code> , <code>javax.jms.TopicConnectionFactory</code> , <code>javax.jms.QueueConnectionFactory</code> .																				
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the list-jms-resources command to list all JMS resources</p> <pre>asadmin&gt; <b>list-jms-resources</b> jms/Queue jms/Topic jms/QueueConnectionFactory jms/DurableTopicConnectionFactory Command list-jms-resources executed successfully</pre> <p><b>EXAMPLE 2</b> Using the list-jms-resources command to list JMS resources of a specified type</p> <pre>asadmin&gt; <b>list-jms-resources --restype javax.jms.TopicConnectionFactory</b> jms/DurableTopicConnectionFactory jms/TopicConnectionFactory Command list-jms-resources executed successfully</pre>																				

list-jms-resources(1)

**EXIT STATUS** 0 command executed successfully  
1 error in executing the command

**SEE ALSO** create-jms-resource(1), delete-jms-resource(1)

## list-jndi-resources(1)

<b>NAME</b>	list-jndi-resources – gets all the JNDI resources
<b>SYNOPSIS</b>	<b>list-jndi-resources</b> <b>--user</b> <i>admin_user</i> [ <b>--password</b> <i>admin_password</i> ] [ <b>--host</b> <i>localhost</i> ] [ <b>--port</b> <b>4848</b> ] [ <b>--secure</b>   <b>-s</b> ] [ <b>--passwordfile</b> <i>filename</i> ] [ <b>--terse=false</b> ] [ <b>--echo=false</b> ] [ <b>--interactive=true</b> ]
<b>DESCRIPTION</b>	Gets all the JNDI resources. This command is supported in remote mode only.
<b>OPTIONS</b>	<b>--user</b> authorized domain application server administrative username. <b>--password</b> password to administer the domain application server. <b>--host</b> machine name where the domain application server is running. <b>--port</b> port number of the domain application server listening for administration requests. <b>--secure</b> if true, uses SSL/TLS to communicate with the domain application server. <b>--passwordfile</b> file containing the domain application server password. <b>--terse</b> indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. <b>--echo</b> setting to true will echo the command line statement on the standard output. <b>--interactive</b> prompts you for the required options that are not already specified.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using the list-jndi-resource command asadmin> <b>list-jndi-resource</b> <b>--user</b> admin1 <b>--password</b> adminadmin1 <b>--host</b> pigeon <b>--port</b> 5001 Command list-jndi-resources executed successfully
<b>EXIT STATUS</b>	0 command executed successfully 1 error in executing the command
<b>SEE ALSO</b>	create-jndi-resource(1), delete-jndi-resource(1)

<b>NAME</b>	list-lifecycle-modules – gets the lifecycle modules
<b>SYNOPSIS</b>	<b>list-lifecycle-modules</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true]
<b>DESCRIPTION</b>	Gets the lifecycle modules. This command is supported in remote mode only.
<b>OPTIONS</b>	<p>--user                    authorized domain application server administrative username.</p> <p>--password               password to administer the domain application server.</p> <p>--host                    machine name where the domain application server is running.</p> <p>--port                    port number of the domain application server listening for administration requests.</p> <p>--secure                  if true, uses SSL/TLS to communicate with the domain application server.</p> <p>--passwordfile          file containing the domain application server password.</p> <p>--terse                   indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</p> <p>--echo                    setting to true will echo the command line statement on the standard output. Default is false.</p> <p>--interactive            if set to true (default), only the required password options are prompted.</p>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using list-lifecycle-modules</p> <pre>asadmin&gt; list-lifecycle-modules --user admin --password adminadmin --host fuyako --port 7070 customSetup</pre> <p>Where: customSetup is the lifecycle module listed.</p>
<b>EXIT STATUS</b>	<p>0    command executed successfully</p> <p>1    error in executing the command</p>
<b>SEE ALSO</b>	create-lifecycle-module(1), delete-lifecycle-module(1)

## list-mimes(1)

<b>NAME</b>	list-mimes – gets the MIME types												
<b>SYNOPSIS</b>	<pre><b>list-mimes</b>   --user <i>admin_user</i> [--password <i>admin_password</i>] [--host <i>localhost</i>]   [--port <b>4848</b>] [--passwordfile <i>filename</i>] [--secure   -s] <i>instance_name</i></pre>												
<b>DESCRIPTION</b>	Gets the MIME types associated with the named server instance. The server determines the MIME type of a requested resource by invoking the type-by-extension directive in the <code>ObjectType</code> section of the <code>obj.conf</code> file. The type-by-extension function does not work if no MIME element has been defined in the server element.												
<b>OPTIONS</b>	<table><tr><td>--user</td><td>administrative user associated for the instance.</td></tr><tr><td>--password</td><td>administrative password corresponding to the administrative user.</td></tr><tr><td>--host</td><td>host name of the machine hosting the administrative instance.</td></tr><tr><td>--port</td><td>administrative port number associated with the administrative host.</td></tr><tr><td>--passwordfile</td><td>file containing passwords appropriate for the command (e.g., administrative instance).</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the administrative instance.</td></tr></table>	--user	administrative user associated for the instance.	--password	administrative password corresponding to the administrative user.	--host	host name of the machine hosting the administrative instance.	--port	administrative port number associated with the administrative host.	--passwordfile	file containing passwords appropriate for the command (e.g., administrative instance).	--secure	if true, uses SSL/TLS to communicate with the administrative instance.
--user	administrative user associated for the instance.												
--password	administrative password corresponding to the administrative user.												
--host	host name of the machine hosting the administrative instance.												
--port	administrative port number associated with the administrative host.												
--passwordfile	file containing passwords appropriate for the command (e.g., administrative instance).												
--secure	if true, uses SSL/TLS to communicate with the administrative instance.												
<b>OPERANDS</b>	<i>instance_name</i> name of the instance.												
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using list-mimes</p> <pre>asadmin&gt; list-mimes --user admin --password adminadmin --host fuyako --port 7070 server1 sampleMIME</pre> <p>Where: <code>sampleMIME</code> is the name of the MIME listed.</p>												
<b>EXIT STATUS</b>	<table><tr><td>0</td><td>command executed successfully</td></tr><tr><td>1</td><td>error in executing the command</td></tr></table>	0	command executed successfully	1	error in executing the command								
0	command executed successfully												
1	error in executing the command												
<b>INTERFACE EQUIVALENT</b>	HTTP Server node, MIME Type Files page												
<b>SEE ALSO</b>	<code>create-mime(1)</code> , <code>delete-mime(1)</code>												



<b>NAME</b>	list-persistence-resources – gets all the persistence resources
<b>SYNOPSIS</b>	<b>list-persistence-resources</b> <i>--user admin_user</i> <i>[--password admin_password] [--host localhost] [--port 4848]</i> <i>[--secure -s] [--passwordfile filename] [--terse=false]</i> <i>[--echo=false] [--interactive=true]</i>
<b>DESCRIPTION</b>	Gets all the persistence resources. This command is supported in remote mode only.
<b>OPTIONS</b>	<p><i>--user</i> authorized domain application server administrative username.</p> <p><i>--password</i> password to administer the domain application server.</p> <p><i>--host</i> machine name where the domain application server is running.</p> <p><i>--port</i> port number of the domain application server listening for administration requests.</p> <p><i>--secure</i> if true, uses SSL/TLS to communicate with the domain application server.</p> <p><i>--passwordfile</i> file containing the domain application server password.</p> <p><i>--terse</i> indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</p> <p><i>--echo</i> setting to true will echo the command line statement on the standard output. Default is false.</p> <p><i>--interactive</i> if set to true (default), only the required password options are prompted.</p>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> using list-persistence-resources</p> <pre>asadmin&gt; list-persistence-resources --user admin1 --password adminadmin1 --host pigeon --port 5001 Command list-persistence-resources executed successfully</pre> <p>Where: <i>sample_persistence_resource</i> is the persistence resource listed.</p>
<b>EXIT STATUS</b>	<p>0 command executed successfully</p> <p>1 error in executing the command</p>
<b>SEE ALSO</b>	create-persistence-resource(1), delete-persistence-resource(1)

## list-profiler(1)

<b>NAME</b>	list-profiler – gets the profiler element in the named instance.
<b>SYNOPSIS</b>	<b>list-profiler</b> --user <i>user_name</i> --password <i>password</i> --host <i>hostname</i> --port <i>admin_port_number</i> [--instance <i>instance_name</i> ]
<b>DESCRIPTION</b>	Gets the profiler element associated with the named server instance..
<b>OPTIONS</b>	--user identifies the user name associated with the named instance.  --password identifies the password associated with the user name.  --host identifies the host name for the machine.  --port identifies the administrator port number associated with the hostname.  --instance identifies the name of the instance associated with the JVM option to be created.
<b>EXAMPLES</b>	asadmin% <b>list-profilers</b>
<b>INTERFACE EQUIVALENT</b>	Application Server Instances, JVM Settings tab
<b>SEE ALSO</b>	create-profiler(1) delete-profiler(1)

<b>NAME</b>	list-profilers – lists the profiler elements
<b>SYNOPSIS</b>	<b>list-profilers</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--passwordfile <i>filename</i> ] [--secure   -s] <i>instance_name</i>
<b>DESCRIPTION</b>	Gets the profiler element associated with the named server instance.
<b>OPTIONS</b>	--user                  administrative user associated for the instance. --password             administrative password corresponding to the administrative user. --host                 host name of the machine hosting the administrative instance. --port                 administrative port number associated with the administrative host. --passwordfile         file containing passwords appropriate for the command (e.g., administrative instance). --secure               if true, uses SSL/TLS to communicate with the administrative instance.
<b>OPERANDS</b>	<i>instance_name</i> name of the instance.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using list-profilers <pre>asadmin&gt; list-profilers --user admin --passwordfile passwords.txt --host localhost --port 4848 se sample_profiler</pre> <p>Where: <i>sample_profiler</i> is the profiler listed.</p>
<b>EXIT STATUS</b>	0      command executed successfully 1      error in executing the command
<b>INTERFACE EQUIVALENT SEE ALSO</b>	Application Server Instances, JVM Settings tab create-profiler(1), delete-profiler(1)

## list-resource-adapter-configs(1)

<b>NAME</b>	list-resource-adapter-configs – lists the configuration information created in domain.xml for the connector module																				
<b>SYNOPSIS</b>	<pre>list-resource-adapter-configs --user admin_user [--password admin_password] [--host localhost] [--port 4848] [--secure -s] [--passwordfile filename] [--terse=false] [--echo=false] [--interactive=true] [--verbose=false] [--rnameconnector_module_name]</pre>																				
<b>DESCRIPTION</b>	<p>Lists the configuration information in the domain.xml for the connector module. It lists an entry called resource-adapter-config in the domain.xml.</p> <p>This command is supported in remote mode only.</p>																				
<b>OPTIONS</b>	<table><tr><td>--user</td><td>authorized domain application server administrative username.</td></tr><tr><td>--password</td><td>password to administer the domain application server.</td></tr><tr><td>--host</td><td>machine name where the domain application server is running.</td></tr><tr><td>--port</td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td>--passwordfile</td><td>file containing the domain application server password.</td></tr><tr><td>--terse</td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td></tr><tr><td>--echo</td><td>setting to true will echo the command line statement on the standard output. Default is false.</td></tr><tr><td>--interactive</td><td>if set to true (default), only the required password options are prompted.</td></tr><tr><td>--verbose</td><td>if set to true the properties that are configured are also listed. Default is false.</td></tr></table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	--echo	setting to true will echo the command line statement on the standard output. Default is false.	--interactive	if set to true (default), only the required password options are prompted.	--verbose	if set to true the properties that are configured are also listed. Default is false.
--user	authorized domain application server administrative username.																				
--password	password to administer the domain application server.																				
--host	machine name where the domain application server is running.																				
--port	port number of the domain application server listening for administration requests.																				
--secure	if true, uses SSL/TLS to communicate with the domain application server.																				
--passwordfile	file containing the domain application server password.																				
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																				
--echo	setting to true will echo the command line statement on the standard output. Default is false.																				
--interactive	if set to true (default), only the required password options are prompted.																				
--verbose	if set to true the properties that are configured are also listed. Default is false.																				
<b>OPERANDS</b>	<i>rname</i> the value kept in the resource-adapter-name in the domain.xml file.																				
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using list-resource-adapter-configs</p> <pre>asadmin&gt; list-resource-adapter-configs --username admin1 --password adminadmin1</pre> <p>Command list-resource-adapter-configs executed successfully</p>																				
<b>EXIT STATUS</b>	<table><tr><td>0</td><td>command executed successfully</td></tr><tr><td>1</td><td>error in executing the command</td></tr></table>	0	command executed successfully	1	error in executing the command																
0	command executed successfully																				
1	error in executing the command																				

list-resource-adapter-configs(1)

**SEE ALSO** create-resource-adapter-config(1),  
delete-resource-adapter-config(1)

## list-sub-components(1)

<b>NAME</b>	list-sub-components – Lists EJBs or Servlets in a deployed module or in a module of a deployed application																				
<b>SYNOPSIS</b>	<pre>list-sub-components --user admin_user   [--password admin_password] [--host localhost] [--port 4848]   [--secure -s] [--passwordfile filename] [--terse=false]   [--echo=false] [--interactive] [--appname app_name] module_name</pre>																				
<b>DESCRIPTION</b>	list-sub-components lists your EJBs or Servlets in a deployed module or in a module of the deployed application. If a module is not identified, all modules are listed. This command is supported in remote mode only.																				
<b>OPTIONS</b>	<table><tr><td>--user</td><td>authorized domain application server administrative username.</td></tr><tr><td>--password</td><td>password to administer the domain application server.</td></tr><tr><td>--host</td><td>machine name where the domain application server is running.</td></tr><tr><td>--port</td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td>--passwordfile</td><td>file containing the domain application server password.</td></tr><tr><td>--terse</td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.</td></tr><tr><td>--echo</td><td>setting to true will echo the command line statement on the standard output.</td></tr><tr><td>--interactive</td><td>prompts you for the required options that are not already specified.</td></tr><tr><td>--appname</td><td>name of the application.</td></tr></table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.	--echo	setting to true will echo the command line statement on the standard output.	--interactive	prompts you for the required options that are not already specified.	--appname	name of the application.
--user	authorized domain application server administrative username.																				
--password	password to administer the domain application server.																				
--host	machine name where the domain application server is running.																				
--port	port number of the domain application server listening for administration requests.																				
--secure	if true, uses SSL/TLS to communicate with the domain application server.																				
--passwordfile	file containing the domain application server password.																				
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.																				
--echo	setting to true will echo the command line statement on the standard output.																				
--interactive	prompts you for the required options that are not already specified.																				
--appname	name of the application.																				
<b>OPERANDS</b>	<i>module_name</i> name of the module containing the sub-component.																				
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using list-sub-components</p> <pre>asadmin&gt; list-sub-components --appname sampleApp mymodule sampleApp application</pre>																				
<b>EXIT STATUS</b>	<table><tr><td>0</td><td>command executed successfully</td></tr><tr><td>1</td><td>error in executing the command</td></tr></table>	0	command executed successfully	1	error in executing the command																
0	command executed successfully																				
1	error in executing the command																				
<b>SEE ALSO</b>	deploy(1), deploydir(1), undeploy(1), enable(1), disable(1), list-components(1)																				

<b>NAME</b>	list-threadpools – lists all the threadpools
<b>SYNOPSIS</b>	<b>list-threadpools</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true]
<b>DESCRIPTION</b>	Lists all the thread pools. This command is supported in remote mode only.
<b>OPTIONS</b>	<p>--user                    authorized domain application server administrative username.</p> <p>--password                password to administer the domain application server.</p> <p>--host                    machine name where the domain application server is running.</p> <p>--port                    port number of the domain application server listening for administration requests.</p> <p>--secure                  if true, uses SSL/TLS to communicate with the domain application server.</p> <p>--passwordfile            file containing the domain application server password.</p> <p>--terse                    indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</p> <p>--echo                    setting to true will echo the command line statement on the standard output. Default is false.</p> <p>--interactive             if set to true (default), only the required password options are prompted.</p>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using list-threadpools</p> <pre>asadmin&gt; list-threadpools --user admin --password adminadmin</pre> <p>Command list-threadpools executed successfully</p>
<b>EXIT STATUS</b>	<p>0    command executed successfully</p> <p>1    error in executing the command</p>
<b>SEE ALSO</b>	create-threadpool(1), delete-threadpool(1)

## list-virtual-servers(1)

<b>NAME</b>	list-virtual-servers – gets the virtual servers
<b>SYNOPSIS</b>	<b>list-virtual-servers</b> --user <i>admin_user</i> [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <b>4848</b> ] [--secure -s] [--passwordfile <i>filename</i> ] [--terse=false] [--echo=false] [--interactive=true]
<b>DESCRIPTION</b>	Gets all the virtual server elements. This command is supported in remote mode only.
<b>OPTIONS</b>	--user                   authorized domain application server administrative username.  --password               password to administer the domain application server.  --host                    machine name where the domain application server is running.  --port                    port number of the domain application server listening for administration requests.  --secure                  if true, uses SSL/TLS to communicate with the domain application server.  --passwordfile           file containing the domain application server password.  --terse                   indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.  --echo                    setting to true will echo the command line statement on the standard output. Default is false.  --interactive             if set to true (default), only the required password options are prompted.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using list-virtual-servers  asadmin> list-virtual-servers --user admin --password adminadmin --host localhost --port 4848 Command list-virtual-servers executed successfully
<b>EXIT STATUS</b>	0    command executed successfully  1    error in executing the command
<b>SEE ALSO</b>	create-virtual-server(1), delete-virtual-server(1)



<b>NAME</b>	multimode – allows you to execute multiple commands while preserving environment settings and remaining in the asadmin utility
<b>SYNOPSIS</b>	<b>multimode</b> [ <b>--file</b> <i>filename</i> ] [ <b>--printprompt=true</b> ] [ <b>--encoding</b> <i>encode</i> ] [ <b>--terse=false</b> ] [ <b>--echo=false</b> ]
<b>DESCRIPTION</b>	Use <code>multimode</code> to process the <code>asadmin</code> commands. The command-line interface will prompt you for a command, execute that command, display the results of the command, and then prompt you for the next command. Additionally, all the <code>asadmin</code> option names set in this mode are used for all the subsequent commands. You can set your environment and run commands until you exit <code>multimode</code> by typing “exit” or “quit.” You can also provide commands by passing a previously prepared list of commands from a file or standard input (pipe). You can invoke <code>multimode</code> from within a <i>multimode</i> session; once you exit the second <i>multimode</i> environment, you return to your original <i>multimode</i> environment.  This command is supported in local mode only.
<b>OPTIONS</b>	<p><b>--file</b> reads the commands as defined in the file.</p> <p><b>--printprompt</b> allows the printing of <code>asadmin</code> prompt after each command is executed. Set this option to false when the commands are piped or redirected from the standard input or file. By default the option is set to true.</p> <p><b>--encoding</b> specifies the locale for the file to be decoded.</p> <p><b>--terse</b> indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</p> <p><b>--echo</b> setting to true will echo the command line statement on to the standard output. Default is false.</p>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using <code>multimode</code> to execute multiple commands</p> <pre>example% asadmin multimode --file commands_file.txt</pre> <p>Where: <code>example%</code> is the system prompt. The <code>multimode</code> settings are executed from the <code>commands_file.txt</code> file.</p>
<b>EXIT STATUS</b>	<p>0 command executed successfully</p> <p>1 error in executing the command</p>
<b>SEE ALSO</b>	<code>export(1)</code> , <code>unset(1)</code>

package-appclient( 1M)

**NAME** package-appclient – packs the application client container libraries and jar files

**SYNOPSIS** **package-appclient**

**DESCRIPTION** Use the `package-appclient` command to pack the application client container libraries and jar files into an `appclient.jar` file. The created file is located at `appserver_install_dir/lib/appclient/appclient.jar`. The `appclient.jar` file provides an application client container package targeted at remote hosts that do not contain a server installation.

The `appclient.jar` archive contains native code and can be used on a target machine that is of similar architecture as the machine where it was produced. So, for example, an `appclient.jar` produced on a Solaris SPARC platform cannot be used on a Windows client machine.

After copying the `appclient.jar` file to a remote location, `unjar` it to get a set of libraries and jar files in the `appclient` directory

After unjarring on the client machine, modify `appclient_install_dir/config/asenv.conf` (`asenv.bat` for Windows) as follows:

- set `AS_WEBSERVICES_LIB` to `appclient_install_dir/lib`
- set `AS_NSS` to `appclient_install_dir/lib` (`appclient_install_dir\bin` for Windows)
- set `AS_IMQ_LIB` to `appclient_install_dir/imq/lib`
- set `AS_INSTALL` to `appclient_install_dir`
- set `AS_JAVA` to your JDK 1.4 home directory
- set `AS_ACC_CONFIG` to `appclient_install_dir/config/sun-acc.xml`

Modify `appclient_install_dir/config/sun-acc.xml` as follows:

- Ensure the `DOCTYPE` file references `appclient_install_dir/lib/dtds`
- Ensure that `target-server` address attribute references the server machine.
- Ensure that `target-server` port attribute references the ORB port on the remote machine.
- Ensure that `log-service` references a log file; if the user wants to put log messages to a log file.

Modify `appclient_install_dir/bin/appclient` (`appclient.bat` for Windows) as follows:

- change token `%CONFIG_HOME%` to `appclient_install_dir/config`

**ATTRIBUTES** See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Interface Stability	Unstable

package-appclient( 1M)

**SEE ALSO** | appclient (1M)

## ping-connection-pool(1)

<b>NAME</b>	ping-connection-pool – tests that a connection pool is usable																		
<b>SYNOPSIS</b>	<pre>ping-connection-pool --user <i>admin_user</i> [--password <i>admin_password</i>]   [--host <i>localhost</i>] [--port <b>4848</b>] [--secure -s]   [--passwordfile <i>filename</i>] [--terse=false] [--echo=false]   [--interactive=true] <i>pool_name</i></pre>																		
<b>DESCRIPTION</b>	<p>Tests that a connection pool is usable for both JDBC connection pools and connector connection pools. For example, if you create a new JDBC connection pool for use with an application that is expected to be deployed, before deploying the application, the previously created pool is tested with this command.</p> <p>This command is supported in remote mode only.</p>																		
<b>OPTIONS</b>	<table><tr><td>--user</td><td>authorized domain application server administrative username.</td></tr><tr><td>--password</td><td>password to administer the domain application server.</td></tr><tr><td>--host</td><td>machine name where the domain application server is running.</td></tr><tr><td>--port</td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td>--passwordfile</td><td>file containing the domain application server password.</td></tr><tr><td>--terse</td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td></tr><tr><td>--echo</td><td>setting to true will echo the command line statement on the standard output. Default is false.</td></tr><tr><td>--interactive</td><td>if set to true (default), only the required password options are prompted.</td></tr></table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	--echo	setting to true will echo the command line statement on the standard output. Default is false.	--interactive	if set to true (default), only the required password options are prompted.
--user	authorized domain application server administrative username.																		
--password	password to administer the domain application server.																		
--host	machine name where the domain application server is running.																		
--port	port number of the domain application server listening for administration requests.																		
--secure	if true, uses SSL/TLS to communicate with the domain application server.																		
--passwordfile	file containing the domain application server password.																		
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																		
--echo	setting to true will echo the command line statement on the standard output. Default is false.																		
--interactive	if set to true (default), only the required password options are prompted.																		
<b>OPERANDS</b>	<i>poolname</i> name of the connection pool to be tested.																		
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using ping-connection-pool</p> <p>Before you can ping a connection pool, you must:</p> <ul style="list-style-type: none"><li>■ Create a connection pool with authentication.</li><li>■ Make sure the Enterprise Information Server (can be the database) is started.</li></ul> <pre>asadmin&gt; ping-connection-pool --user admin1 --password adminadmin1 --host pigeon --port 5001 sampleConnectionPool Command ping-connection-pool executed successfully</pre>																		

ping-connection-pool(1)

**EXIT STATUS** 0 command executed successfully  
1 error in executing the command

**SEE ALSO** create-connector-connection-pool(1),  
delete-connector-connection-pool(1),  
list-connector-connection-pool(1), create-jdbc-connection-pool(1),  
delete-jdbc-connection-pool(1) list-jdbc-connection-pools(1)

## reconfig(1)

<b>NAME</b>	reconfig – applies the changes you have made for a server instance																
<b>SYNOPSIS</b>	<pre>reconfig --user admin_user [--password admin_password] [--host localhost]   [--port 4848] [--secure -s] [--passwordfile filename]   [--discardmanualchanges=false] [--keepmanualchanges=false]   instance_name</pre>																
<b>DESCRIPTION</b>	<p>This command is deprecated. It allows you to apply changes you have made for a server instance. Use the <code>reconfig</code> command after you've used the <code>set</code> command to change server properties. Any changes you make to the configuration files of the server do not take affect until you apply the changes by running the <code>reconfig</code> command. When <code>--discardmanualchanges</code> is set to true, manual changes made to the <code>server.xml</code> file are discarded. When <code>--keepmanualchanges</code> is set to true, manual changes made to the <code>server.xml</code> file take affect. However if both options are false (both options are not specified), an error message is displayed if manual changes and/or changes have been applied using the Administrator Interface. Use this command with discretion since there is no undo, and the changes applied are made directly to your <code>config/backup/server.xml</code> file.</p>																
<b>OPTIONS</b>	<table><tr><td><code>--user</code></td><td>administrative user associated for the instance.</td></tr><tr><td><code>--password</code></td><td>administrative password corresponding to the administrative user.</td></tr><tr><td><code>--host</code></td><td>host name of the machine hosting the administrative instance.</td></tr><tr><td><code>--port</code></td><td>administrative port number associated with the administrative host.</td></tr><tr><td><code>--passwordfile</code></td><td>file containing passwords appropriate for the command (e.g., administrative instance).</td></tr><tr><td><code>--secure</code></td><td>if true, uses SSL/TLS to communicate with the administrative instance.</td></tr><tr><td><code>--discardmanualchanges</code></td><td>defaults to false. When set to true, discards the changes made manually to the <code>server.xml</code> file.</td></tr><tr><td><code>--keepmanualchanges</code></td><td>defaults to false. When set to true, allows the manual changes made to the <code>server.xml</code> file to take affect.</td></tr></table>	<code>--user</code>	administrative user associated for the instance.	<code>--password</code>	administrative password corresponding to the administrative user.	<code>--host</code>	host name of the machine hosting the administrative instance.	<code>--port</code>	administrative port number associated with the administrative host.	<code>--passwordfile</code>	file containing passwords appropriate for the command (e.g., administrative instance).	<code>--secure</code>	if true, uses SSL/TLS to communicate with the administrative instance.	<code>--discardmanualchanges</code>	defaults to false. When set to true, discards the changes made manually to the <code>server.xml</code> file.	<code>--keepmanualchanges</code>	defaults to false. When set to true, allows the manual changes made to the <code>server.xml</code> file to take affect.
<code>--user</code>	administrative user associated for the instance.																
<code>--password</code>	administrative password corresponding to the administrative user.																
<code>--host</code>	host name of the machine hosting the administrative instance.																
<code>--port</code>	administrative port number associated with the administrative host.																
<code>--passwordfile</code>	file containing passwords appropriate for the command (e.g., administrative instance).																
<code>--secure</code>	if true, uses SSL/TLS to communicate with the administrative instance.																
<code>--discardmanualchanges</code>	defaults to false. When set to true, discards the changes made manually to the <code>server.xml</code> file.																
<code>--keepmanualchanges</code>	defaults to false. When set to true, allows the manual changes made to the <code>server.xml</code> file to take affect.																
<b>OPERANDS</b>	<code>instance_name</code> name of the instance..																
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using <code>reconfig</code></p> <pre>asadmin&gt; reconfig --user admin --passwordfile passwords.txt --host localhost --port 4848 server1 Successfully reconfigured</pre>																

**EXAMPLE 2** Using reconfig with the --discardmanualchanges option

```
asadmin> reconfig --user admin --passwordfile passwords.txt --host localhost --port 4848 --discardmanualchanges
Instance restart is required
Successfully reconfigured
```

**EXAMPLE 3** Using reconfig with the --keepmanualchanges option

```
asadmin> reconfig --user admin --passwordfile passwords.txt --host localhost --port 4848 --keepmanualchanges
Instance restart is required
Successfully reconfigured
```

**EXIT STATUS**

0	command executed successfully
1	error in executing the command

**SEE ALSO** get(1), set(1), list(1)

## restart-instance(1)

<b>NAME</b>	restart-instance – restarts the specified server instance and all the services associated with it
<b>SYNOPSIS</b>	<b>restart-instance</b> [--user <i>admin_user</i> ] [--password <i>admin_password</i> ] [--host <i>localhost</i> ] [--port <i>4848</i> ] [--local=false] [--domain <i>domain_name</i> ] [--passwordfile <i>filename</i> ] [--secure -s] <i>instance_name</i>
<b>DESCRIPTION</b>	Use the restart-instance to restart the instance with the instance name specified. The restart-instance command can be run both locally and remotely. To restart remotely, the administration server must be running on the hostname and port number specified. The user authenticates using the password identified for the administration server. Additionally, the instance must already exist within the domain served by the administration server, and the instance must be running. The restart-instance command is not supported on Windows.
<b>OPTIONS</b>	--user administrative user associated for the instance. --password administrative password corresponding to the administrative user. --host host name of the machine hosting the administrative instance. --port administrative port number associated with the administrative host. --local determines if the command should delegate the request to administrative instance or run locally. --domain name of the domain. --passwordfile file containing passwords appropriate for the command (e.g., administrative instance). --secure if true, uses SSL/TLS to communicate with the administrative instance.
<b>OPERANDS</b>	<i>instance_name</i> name of the instance to be restarted.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using restart-instance in local mode asadmin> restart-instance --local --domain domain1 server1 Instance server1 started  Where: server1 is the name of the instance restarted on the domain1 domain.  <b>EXAMPLE 2</b> Using restart-instance in remote mode asadmin> restart-instance --user admin --password adminadmin --host bluestar --port 4848 server1 Instance server1 started  Where: server1 is the name of the instance restarted. The restarted instance is associated with the user, password, host, and port number specified.



restart-instance(1)

**EXIT STATUS** 0 command executed successfully  
1 error in executing the command

**INTERFACE** Server Instance page

**EQUIVALENT**

**SEE ALSO**

delete-instance(1), start-instance(1), create-instance(1),  
stop-instance(1), start-appserv(1), stop-appserv(1), start-domain(1),  
stop-domain(1)

## rollback-transaction(1)

<b>NAME</b>	rollback-transaction – rollback the named transaction																		
<b>SYNOPSIS</b>	<pre>unfreeze-transaction-service --user admin_user [--password admin_password] [--host localhost] [--port 4848] [--secure -s] [--passwordfile filename] [--terse=false] [--echo=false] [--interactive=true] transaction_id</pre>																		
<b>DESCRIPTION</b>	Rollback the named transaction. This command is supported in remote mode only.																		
<b>OPTIONS</b>	<table><tr><td>--user</td><td>authorized domain application server administrative username.</td></tr><tr><td>--password</td><td>password to administer the domain application server.</td></tr><tr><td>--host</td><td>machine name where the domain application server is running.</td></tr><tr><td>--port</td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td>--passwordfile</td><td>file containing the domain application server password.</td></tr><tr><td>--terse</td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td></tr><tr><td>--echo</td><td>setting to true will echo the command line statement on the standard output. Default is false.</td></tr><tr><td>--interactive</td><td>if set to true (default), only the required password options are prompted.</td></tr></table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	--echo	setting to true will echo the command line statement on the standard output. Default is false.	--interactive	if set to true (default), only the required password options are prompted.
--user	authorized domain application server administrative username.																		
--password	password to administer the domain application server.																		
--host	machine name where the domain application server is running.																		
--port	port number of the domain application server listening for administration requests.																		
--secure	if true, uses SSL/TLS to communicate with the domain application server.																		
--passwordfile	file containing the domain application server password.																		
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																		
--echo	setting to true will echo the command line statement on the standard output. Default is false.																		
--interactive	if set to true (default), only the required password options are prompted.																		
<b>OPERANDS</b>	<i>transaction_id</i> identifier for the transaction to be rolled back..																		
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using rollback-transaction</p> <pre>asadmin&gt; rollback-transaction --user admin --password adminadmin transaction1</pre>																		
<b>EXIT STATUS</b>	<table><tr><td>0</td><td>command executed successfully</td></tr><tr><td>1</td><td>error in executing the command</td></tr></table>	0	command executed successfully	1	error in executing the command														
0	command executed successfully																		
1	error in executing the command																		
<b>SEE ALSO</b>	freeze-transaction-service(1), unfreeze-transaction-service(1)																		

<b>NAME</b>	set – sets the values of attributes
<b>SYNOPSIS</b>	<b>set</b> <b>--user</b> <i>admin_user</i> [ <b>--password</b> <i>admin_password</i> ] [ <b>--host</b> <i>localhost</i> ] <b>[--port</b> 4848] [ <b>--secure</b>   <b>-s</b> ] [ <b>--passwordfile</b> <i>filename</i> ] <b>[--terse=false]</b> [ <b>--echo=false]</b> [ <b>--interactive=true]</b> <i>attributename=value</i> [ <i>attribute_name=value</i> ] *
<b>DESCRIPTION</b>	Sets the values of one or more configurable attribute. This command is supported in remote mode only. On Solaris, quotes are needed when executing commands with * as the option value or operand.
<b>OPTIONS</b>	<p><b>--user</b> authorized domain application server administrative username.</p> <p><b>--password</b> password to administer the domain application server.</p> <p><b>--host</b> machine name where the domain application server is running.</p> <p><b>--port</b> port number of the domain application server listening for administration requests.</p> <p><b>--secure</b> if true, uses SSL/TLS to communicate with the domain application server.</p> <p><b>--passwordfile</b> file containing the domain application server password.</p> <p><b>--terse</b> indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</p> <p><b>--echo</b> setting to true will echo the command line statement on the standard output. Default is false.</p> <p><b>--interactive</b> if set to true (default), only the required password options are prompted.</p>
<b>OPERANDS</b>	<i>attributename=value</i> identifies the attribute name and its value. See the <i>Application Server Reference</i> for a listing of the available attribute names.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using set</p> <pre>asadmin&gt; set --user admin --password adminadmin --host localhost --port 4848 server.transaction-service.automatic-recovery=true</pre>
<b>EXIT STATUS</b>	<p>0 command executed successfully</p> <p>1 error in executing the command</p>
<b>SEE ALSO</b>	get(1), list(1)

## show-component-status(1)

<b>NAME</b>	show-component-status – displays the status of the deployed component
<b>SYNOPSIS</b>	<b>show-component-status</b> <b>--user</b> <i>admin_user</i> [ <b>--password</b> <i>admin_password</i> ] [ <b>--host</b> <i>localhost</i> ] [ <b>--port</b> <b>4848</b> ] [ <b>--secure</b>   <b>-s</b> ] [ <b>--passwordfile</b> <i>filename</i> ] [ <b>--terse=false</b> ] [ <b>--echo=false</b> ] [ <b>--interactive</b> ] <i>component_name</i>
<b>DESCRIPTION</b>	show-component-status gets the status of the deployed component. The status is a string representation returned by the server. The possible status strings include: enabled or disabled. This command is supported in remote mode only.
<b>OPTIONS</b>	<b>--user</b> authorized domain application server administrative username. <b>--password</b> password to administer the domain application server. <b>--host</b> machine name where the domain application server is running. <b>--port</b> port number of the domain application server listening for administration requests. <b>--secure</b> if true, uses SSL/TLS to communicate with the domain application server. <b>--passwordfile</b> file containing the domain application server password. <b>--terse</b> indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. <b>--echo</b> setting to true will echo the command line statement on the standard output. <b>--interactive</b> prompts you for the required options that are not already specified.
<b>OPERANDS</b>	<i>component_name</i> name of the component to be listed.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using show-component-status asadmin> <b>show-component-status sampleApplication</b> Status of sampleApplication is enabled  Where: the status of the sampleApplication application is shown.
<b>EXIT STATUS</b>	0 command executed successfully 1 error in executing the command
<b>SEE ALSO</b>	list-components(1), list-sub-components(1)

<b>NAME</b>	shutdown – brings down the administration server
<b>SYNOPSIS</b>	<b>shutdown</b> <code>[--user admin_user] [--password admin_password] [--host localhost]</code> <code>[--port 4848] [--passwordfile filename] [--secure -s]</code>
<b>DESCRIPTION</b>	shutdown gracefully brings down the administration server and all the running instances. You must manually start the administration server to bring it up again.
<b>OPTIONS</b>	<p>--user administrative user associated for the instance.</p> <p>--password administrative password corresponding to the administrative user.</p> <p>--host host name of the machine hosting the administrative instance.</p> <p>--port administrative port number associated with the administrative host.</p> <p>--passwordfile file containing passwords appropriate for the command (e.g., administrative instance).</p> <p>--secure if true, uses SSL/TLS to communicate with the administrative instance.</p>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the shutdown command</p> <pre>asadmin&gt; shutdown --user admin --password adminadmin --host bluestar --port 4848 Waiting for admin server to shutdown... Admin server has been shutdown</pre>
<b>EXIT STATUS</b>	<p>0 command executed successfully</p> <p>1 error in executing the command</p>
<b>INTERFACE EQUIVALENT</b>	Administration Server page
<b>SEE ALSO</b>	start-instance(1), stop-instance(1), restart-instance(1), start-domain(1), stop-domain(1), start-appserv(1), stop-appserv(1)

## start-appserv(1)

<b>NAME</b>	start-appserv – starts the domains in the specified or default domains directory
<b>SYNOPSIS</b>	<b>start-appserv</b> [--domaindir <i>install_dir/domains</i> ] [--terse=false] [--echo=false]
<b>DESCRIPTION</b>	This command has been deprecated. Please use <code>start-domain</code> to start the domains in the specified domains directory. If a domain directory is not specified, the default domains directory is started. If there is only one domain in the default domain directory ( <i>install_dir/domains</i> ), then no operand is required to start the domain. However, if there is more than one domain, the domain operand must be specified using the <code>start-domain</code> command. This command can only be run locally.
<b>OPTIONS</b>	<b>--domaindir</b> directory where the domains are started. If specified, path must be accessible in the filesystem. If not specified, the domain is started in the default <i>install_dir/domains</i> directory.  <b>--terse</b> indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.  <b>--echo</b> setting to true will echo the command line statement on the standard output. Default is false.
<b>EXIT STATUS</b>	0    command executed successfully 1    error in executing the command
<b>SEE ALSO</b>	<code>create-domain(1)</code> , <code>start-domain(1)</code> , <code>stop-domain(1)</code> , <code>delete-domain(1)</code> , <code>list-domains(1)</code>

<b>NAME</b>	start-domain – starts the given domain
<b>SYNOPSIS</b>	<b>start-domain</b> [ <b>--domaindir</b> <i>install_dir/domains</i> ] [ <b>--terse=false</b> ] [ <b>--echo=false</b> ] [ <b>--verbose=false</b> ] [ <b>--debug</b> ] [ <i>domain_name</i> ]
<b>DESCRIPTION</b>	<b>start-domain</b> starts the specified domain. If there is only one domain in the default domain directory ( <i>install_dir/domains</i> ), then no operand is required to start the domain. However, if there is more than one domain, the domain operand must be specified. This command can only be run locally.
<b>OPTIONS</b>	<p><b>--domaindir</b> directory where the domain is to be started. If specified, path must be accessible in the filesystem. If not specified, the domain is started in the default <i>install_dir/domains</i> directory.</p> <p><b>--terse</b> indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</p> <p><b>--echo</b> setting to true will echo the command line statement on the standard output. Default is false.</p> <p><b>--verbose</b> by default this flag is set to false. If set to true, detailed server startup output is displayed. Press CTRL-C to kill the server. Press CTRL-\\ to print a thread dump.</p> <p><b>--debug</b> by default this flag is set to false. If set to true, the server is started in debug mode and prints the JPDA port on the console.</p>
<b>OPERANDS</b>	<i>domain_name</i> name of the domain. Must be a unique name.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using start-domain</p> <pre>asadmin&gt; start-domain sampleDomain Starting Domain sampleDomain, please wait. Domain sampleDomain started</pre> <p>Where: the sampleDomain domain is started.</p>
<b>EXIT STATUS</b>	<p>0 command executed successfully</p> <p>1 error in executing the command</p>
<b>SEE ALSO</b>	create-domain(1), delete-domain(1), stop-domain(1), list-domains(1)

## start-instance(1)

<b>NAME</b>	start-instance – starts a server instance and all the services associated with it																		
<b>SYNOPSIS</b>	<b>start-instance</b> [--user <i>admin_user</i> ] [--password <i>admin_password</i> ] [--host <i>local_host</i> ] [--port 4848] [--local=false] [--domain <i>domain_name</i> ] [--debug=false] [--passwordfile <i>filename</i> ] [--secure -s] <i>instance_name</i>																		
<b>DESCRIPTION</b>	Use the <code>start-instance</code> command to start an instance with the instance name you specify. The <code>start-instance</code> command can be run both locally and remotely. To start locally, with a domain name identified, the named instance must already exist within that domain. To start remotely, the administration server must be running on the hostname and port number specified. The user authenticates using the password identified for the administration server.																		
<b>OPTIONS</b>	<table><tr><td>--user</td><td>administrative user associated for the instance.</td></tr><tr><td>--password</td><td>administrative password corresponding to the administrative user.</td></tr><tr><td>--host</td><td>host name of the machine hosting the administrative instance.</td></tr><tr><td>--port</td><td>administrative port number associated with the administrative host.</td></tr><tr><td>--local</td><td>determines if the command should delegate the request to administrative instance or run locally.</td></tr><tr><td>--domain</td><td>name of the domain.</td></tr><tr><td>--debug</td><td>starts the instance in debug mode.</td></tr><tr><td>--passwordfile</td><td>file containing passwords appropriate for the command (e.g., administrative instance).</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the administrative instance.</td></tr></table>	--user	administrative user associated for the instance.	--password	administrative password corresponding to the administrative user.	--host	host name of the machine hosting the administrative instance.	--port	administrative port number associated with the administrative host.	--local	determines if the command should delegate the request to administrative instance or run locally.	--domain	name of the domain.	--debug	starts the instance in debug mode.	--passwordfile	file containing passwords appropriate for the command (e.g., administrative instance).	--secure	if true, uses SSL/TLS to communicate with the administrative instance.
--user	administrative user associated for the instance.																		
--password	administrative password corresponding to the administrative user.																		
--host	host name of the machine hosting the administrative instance.																		
--port	administrative port number associated with the administrative host.																		
--local	determines if the command should delegate the request to administrative instance or run locally.																		
--domain	name of the domain.																		
--debug	starts the instance in debug mode.																		
--passwordfile	file containing passwords appropriate for the command (e.g., administrative instance).																		
--secure	if true, uses SSL/TLS to communicate with the administrative instance.																		
<b>OPERANDS</b>	<i>instance_name</i> name of the instance to be started.																		
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using <code>start-instance</code> in local mode</p> <pre>asadmin&gt; start-instance --domain domain1 admin-server Instance admin-server started</pre> <p>Where: the <code>admin-server</code> instance is started on the local <code>domain1</code> domain.</p> <p><b>EXAMPLE 2</b> Using <code>start-instance</code> in remote mode</p> <pre>asadmin&gt; start-instance --user admin --password bluestar --host localhost --port 4848 server1 Instance server1 started</pre> <p>Where: the <code>server1</code> instance is started on the remote domain associated with the specified user, password, host, and port number.</p>																		



start-instance(1)

**EXIT STATUS** 0 command executed successfully  
1 error in executing the command

**INTERFACE** Server Instance page

**EQUIVALENT**

**SEE ALSO**

delete-instance(1), create-instance(1), stop-instance(1),  
restart-instance(1), start-appserv(1), stop-appserv(1),  
start-domain(1), stop-domain(1)

## stop-appserv(1)

<b>NAME</b>	stop-appserv – stops the domains in the specified or default domains directory
<b>SYNOPSIS</b>	<b>stop-appserv</b> [ <b>--domaindir</b> <i>install_dir/domains</i> ] [ <b>--terse=false</b> ] [ <b>--echo=false</b> ]
<b>DESCRIPTION</b>	This command has been deprecated. Please use <code>stop-domain</code> to stop the domains in the specified or default domains directory. If the domains directory is not specified, the default domains directory is stopped. If there is only one domain in the default domains directory ( <i>install_dir/domains</i> ), then no operand is required to stop the domain. However, if there is more than one domain, the domain operand must be specified using the <code>stop-domain</code> command. This command is supported in local mode only.
<b>OPTIONS</b>	<b>--domaindir</b> directory where the domains are started. If specified, path must be accessible in the filesystem. If not specified, the domain is started in the default <i>install_dir/domains</i> directory. <b>--terse</b> indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false. <b>--echo</b> setting to true will echo the command line statement on the standard output. Default is false.
<b>EXIT STATUS</b>	0 command executed successfully 1 error in executing the command
<b>SEE ALSO</b>	<code>create-domain(1)</code> , <code>start-domain(1)</code> , <code>stop-domain(1)</code> , <code>delete-domain(1)</code> , <code>list-domains(1)</code>

<b>NAME</b>	stop-domain – stops the given domain
<b>SYNOPSIS</b>	<b>stop-domain</b> [ <b>--domaindir</b> <i>install_dir/domains</i> ] [ <b>--terse=false</b> ] [ <b>--echo=false</b> ] [ <i>domain_name</i> ]
<b>DESCRIPTION</b>	stop-domain stops the specified domain. If there is only one domain in the default domain directory ( <i>install_dir/domains</i> ), then no operand is required to stop the domain. However, if there is more than one domain, the domain operand must be specified. This command is supported in local mode only.
<b>OPTIONS</b>	<p><b>--domaindir</b> directory where the domain is to be stopped. If specified, path must be accessible in the filesystem. If not specified, the domains are stopped in the default <i>install_dir/domains</i> directory.</p> <p><b>--terse</b> indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</p> <p><b>--echo</b> setting to true will echo the command line statement on the standard output. Default is false.</p>
<b>OPERANDS</b>	<i>domain_name</i> name of the domain. Must be a unique name.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using stop-domain</p> <pre>asadmin&gt; stop-domain sampleDomain Stopping Domain sampleDomain, please wait Domain sampleDomain stopped Command stop-domain executed successfully</pre> <p>Where: the sampleDomain domain in the default domains directory is stopped.</p>
<b>EXIT STATUS</b>	<p>0 command executed successfully</p> <p>1 error in executing the command</p>
<b>SEE ALSO</b>	create-domain(1), delete-domain(1), start-domain(1), list-domains(1)

## stop-instance(1)

<b>NAME</b>	stop-instance – stops the specified server instance and all the services associated with it
<b>SYNOPSIS</b>	<b>stop-instance</b> [--user <i>admin_user</i> ] [--password <i>admin_password</i> ] [--host <i>local_host</i> ] [--port 4848] [--local=false] [--domain <i>domain_name</i> ] [--secure -s] <i>instance_name</i>
<b>DESCRIPTION</b>	Use the stop-instance to stop the instance with the instance name specified. The stop-instance can be run both locally and remotely. The named instance must already exist within the given domain; and the instance must be running.
<b>OPTIONS</b>	--user administrative user associated for the instance. --password administrative password corresponding to the administrative user. --host host name of the machine hosting the administrative instance. --port administrative port number associated with the administrative host. --local determines if the command should delegate the request to administrative instance or run locally. --domain name of the domain. --passwordfile file containing passwords appropriate for the command (e.g., administrative instance). --secure if true, uses SSL/TLS to communicate with the administrative instance.
<b>OPERANDS</b>	<i>instance_name</i> name of the instance to be stopped.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using stop-instance in local mode asadmin> stop-instance --local --domain domain1 server1 Instance server1 stopped  Where: the server1 instance associated with the domain1 domain is stopped locally.  <b>EXAMPLE 2</b> Using stop-instance in remote mode asadmin> stop-instance --user admin --password bluestar --host localhost --port 4848 server1 Instance server1 stopped  Where: the server1 instance associated with the named user, password, host and port is deleted from the remote machine.
<b>EXIT STATUS</b>	0 command executed successfully 1 error in executing the command
<b>INTERFACE EQUIVALENT</b>	Server Instance page

stop-instance(1)

**SEE ALSO** delete-instance(1), start-instance(1), create-instance(1),  
restart-instance(1), start-appserv(1), stop-appserv(1), start-domain(1),  
stop-domain(1)

## undeploy(1)

<b>NAME</b>	undeploy – removes a component in the domain application server
<b>SYNOPSIS</b>	<b>undeploy</b> <b>--user</b> <i>admin_user</i> [ <b>--password</b> <i>admin_password</i> ] [ <b>--host</b> <i>localhost</i> ] [ <b>--port</b> <i>4848</i> ] [ <b>--secure</b> <b>-s</b> ] [ <b>--passwordfile</b> <i>filename</i> ] [ <b>--terse</b> =false] [ <b>--echo</b> =false] [ <b>-interactiv</b> =true] [ <b>--droptables</b> =true false] [ <b>--cascade</b> =false] <i>component_name</i>
<b>DESCRIPTION</b>	<p>undeploy removes the specified component in the domain application server.</p> <p>The <b>--droptables</b> option is only used to undeploy CMP beans for which the tables had been created by the deployment. If not specified, the entries in the deployment descriptors are used.</p> <p>This command is supported in remote mode only.</p>
<b>OPTIONS</b>	<p><b>--user</b> authorized domain application server administrative username.</p> <p><b>--password</b> password to administer the domain application server.</p> <p><b>--host</b> machine name where the domain application server is running.</p> <p><b>--port</b> port number of the domain application server listening for administration requests.</p> <p><b>--secure</b> if true, uses SSL/TLS to communicate with the domain application server.</p> <p><b>--passwordfile</b> file containing the domain application server password.</p> <p><b>--terse</b> indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script.</p> <p><b>--echo</b> setting to true will echo the command line statement on the standard output.</p> <p><b>--interactive</b> prompts you for the required options that are not already specified.</p> <p><b>--droptables</b> if set to true, tables created by application using CMP beans during deployment are dropped. Default is the corresponding entry in the <code>cmp-resource</code> element of the <code>sun-ejb-jar.xml</code> file. If not specified, defaults to the entries specified in the deployment descriptors.</p> <p><b>--cascade</b> If set to true, it deletes all the connection pools and connector resources associated with the resource adapter being undeployed. If set to false, the undeploy fails if any pools and resources are still associated with the resource adapter. Then, either those pools and resources have to be deleted explicitly, or the option has to be set to true. If the option is set to false, and if there are no pools and resources still associated with the</p>

undeploy(1)

resource adapter, the resource adapter is undeployed. This option is applicable to connectors (resource adapters) and applications.

**OPERANDS** *component\_name* name of the deployable component.

**EXAMPLES** **EXAMPLE 1** Simple undeployment

Undeploy (uninstall) an application named Cart

```
asadmin> undeploy --user admin Cart
```

**EXAMPLE 2** Undeploying an enterprise bean with container-managed persistence (CMP)

Undeploy a CMP bean named myejb and drop the corresponding database tables. In a production environment, database tables contain valuable information, so use the `--droptables` option with care.

```
asadmin> undeploy --user admin --droptables=true myejb
```

**EXAMPLE 3** Undeploy a connector (resource adapter)

Undeploy the connector module named jdbcra and perform a cascading delete to remove the associated resources and connection pools.

```
asadmin> undeploy --user admin --cascade=true jdbcra
```

**EXIT STATUS** 0 command executed successfully

1 error in executing the command

**SEE ALSO** `deploy(1)`, `deploydir(1)`, `list-components(1)`

## unfreeze-transaction-service(1)

<b>NAME</b>	unfreeze-transaction-service – resumes all suspended transactions
<b>SYNOPSIS</b>	<b>unfreeze-transaction-service</b> <b>--user</b> <i>admin_user</i> [ <b>--password</b> <i>admin_password</i> ] [ <b>--host</b> <i>localhost</i> ] [ <b>--port</b> <b>4848</b> ] [ <b>--secure</b>   <b>-s</b> ] [ <b>--passwordfile</b> <i>filename</i> ] [ <b>--terse=false</b> ] [ <b>--echo=false</b> ] [ <b>--interactive=true</b> ]
<b>DESCRIPTION</b>	Resumes all the suspended inflight transactions. Invoke this command on an already frozen transaction. This command is supported in remote mode only.
<b>OPTIONS</b>	<b>--user</b> authorized domain application server administrative username. <b>--password</b> password to administer the domain application server. <b>--host</b> machine name where the domain application server is running. <b>--port</b> port number of the domain application server listening for administration requests. <b>--secure</b> if true, uses SSL/TLS to communicate with the domain application server. <b>--passwordfile</b> file containing the domain application server password. <b>--terse</b> indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false. <b>--echo</b> setting to true will echo the command line statement on the standard output. Default is false. <b>--interactive</b> if set to true (default), only the required password options are prompted.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using unfreeze-transaction-service asadmin> unfreeze-transaction-service --user admin --password adminadmin
<b>EXIT STATUS</b>	0 command executed successfully 1 error in executing the command
<b>SEE ALSO</b>	freeze-transaction-service(1), rollback-transaction(1)



unset(1)

<b>NAME</b>	unset – removes one or more variables from the multimode environment
<b>SYNOPSIS</b>	<b>unset</b> <i>env_var</i> [ <i>env_var</i> ] *
<b>DESCRIPTION</b>	Removes one or more variables you set for the multimode environment. The variables and their associated values will no longer exist in the environment.
<b>OPERANDS</b>	<i>env_var</i> environment variable to be removed.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using unset to remove environment variables</p> <pre>asadmin&gt; export AS_ADMIN_HOST=bluestar AS_ADMIN_PORT=8000 AS_ADMIN_USER=admin AS_ADMIN_PASSWORD=p asadmin&gt; export AS_ADMIN_PREFIX=server1.jms-service asadmin&gt; export AS_ADMIN_HOST=bluestar AS_ADMIN_PORT=8000 AS_ADMIN_USER=admin AS_ADMIN_PASSWORD=***** AS_ADMIN_PREFIX=server1.jms-service asadmin&gt; unset AS_ADMIN_PREFIX asadmin&gt; export AS_ADMIN_HOST=bluestar AS_ADMIN_PORT=8000 AS_ADMIN_USER=admin AS_ADMIN_PASSWORD=*****</pre> <p>Using the export command without the argument lists the environment variables that are set. Notice the AS_ADMIN_PREFIX is not in the environment after running the unset command.</p>
<b>EXIT STATUS</b>	0 command executed successfully 1 error in executing the command
<b>SEE ALSO</b>	export(1), multimode(1)

## update-connector-security-map(1)

<b>NAME</b>	update-connector-security-map – updates the security map for the named connector connection pool																						
<b>SYNOPSIS</b>	<pre>update-connector-security-map --user admin_user   [--password admin_password] [--host localhost]   [--port 4848] [--secure -s] [--passwordfile filename]   [--terse=false] [--echo=false] [--interactive=true]   --poolname connector_connection_pool_name   [--addprincipals principal-name[, principal-name]*]     [--addusergroups user-group[, user-group]*]   [--removeprincipals principal-name[, principal-name]*]   [--removeusergroups user-group[, user-group]*] [--mappedusername   user_name] [--mappedpassword password]] mapname</pre>																						
<b>DESCRIPTION</b>	<p>Modifies a security map for the named connector connection pool. You must have first created a connector connection pool using the <code>create-connector-connection-pool</code> command.</p> <p>This command is supported in remote mode only.</p>																						
<b>OPTIONS</b>	<table><tr><td><code>--user</code></td><td>authorized domain application server administrative username.</td></tr><tr><td><code>--password</code></td><td>password to administer the domain application server.</td></tr><tr><td><code>--host</code></td><td>machine name where the domain application server is running.</td></tr><tr><td><code>--port</code></td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td><code>--secure</code></td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td><code>--passwordfile</code></td><td>file containing the domain application server password.</td></tr><tr><td><code>--terse</code></td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td></tr><tr><td><code>--echo</code></td><td>setting to true will echo the command line statement on the standard output. Default is false.</td></tr><tr><td><code>--interactive</code></td><td>if set to true (default), only the required password options are prompted.</td></tr><tr><td><code>--poolname</code></td><td>connector connection pool name for which the security map that is to be updated or created belongs to.</td></tr><tr><td><code>--addprincipals</code></td><td>a comma separated list of backend EIS principals to be added.</td></tr></table>	<code>--user</code>	authorized domain application server administrative username.	<code>--password</code>	password to administer the domain application server.	<code>--host</code>	machine name where the domain application server is running.	<code>--port</code>	port number of the domain application server listening for administration requests.	<code>--secure</code>	if true, uses SSL/TLS to communicate with the domain application server.	<code>--passwordfile</code>	file containing the domain application server password.	<code>--terse</code>	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	<code>--echo</code>	setting to true will echo the command line statement on the standard output. Default is false.	<code>--interactive</code>	if set to true (default), only the required password options are prompted.	<code>--poolname</code>	connector connection pool name for which the security map that is to be updated or created belongs to.	<code>--addprincipals</code>	a comma separated list of backend EIS principals to be added.
<code>--user</code>	authorized domain application server administrative username.																						
<code>--password</code>	password to administer the domain application server.																						
<code>--host</code>	machine name where the domain application server is running.																						
<code>--port</code>	port number of the domain application server listening for administration requests.																						
<code>--secure</code>	if true, uses SSL/TLS to communicate with the domain application server.																						
<code>--passwordfile</code>	file containing the domain application server password.																						
<code>--terse</code>	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																						
<code>--echo</code>	setting to true will echo the command line statement on the standard output. Default is false.																						
<code>--interactive</code>	if set to true (default), only the required password options are prompted.																						
<code>--poolname</code>	connector connection pool name for which the security map that is to be updated or created belongs to.																						
<code>--addprincipals</code>	a comma separated list of backend EIS principals to be added.																						

## update-connector-security-map(1)

--addusergroups a comma separated list of the enterprise information system usergroups to be added.

--removeprincipals a comma separated list of the enterprise information system principals to be removed.

--removeusergroups a comma separated list of the enterprise information system usergroups to be removed.

--mappedusername the enterprise information system username.

--mappedpassword the enterprise information system password.

**OPERANDS** *mapname* name of the security map to be updated.

**EXAMPLES** **EXAMPLE 1** Using update-connector-security-map

It is assumed that the connector pool has already been created using the create-connector-pool command.

```
asadmin> update-connector-security-map --user admin --password adminadmin
--poolname connector-pool1 --addprincipals principal1, principal2,
--addusergroups usergroup1, usergroup2 --removeprincipals principal3, principal4
--removeusergroups usergroup3, usergroup4 securityMap1
Command update-connector-security-map executed successfully
```

**EXIT STATUS** 0 command executed successfully

1 error in executing the command

**SEE ALSO** create-connector-security-map(1), delete-connector-security-map(1), list-connector-security-maps(1)

## update-file-user(1)

<b>NAME</b>	update-file-user – updates a current file user as specified																								
<b>SYNOPSIS</b>	<pre><b>update-file-user</b> --user <i>admin_user</i> [--password <i>admin_password</i>]   [--host <i>localhost</i>] [--port <b>4848</b>] [--secure -s]   [--passwordfile <i>filename</i>] [--terse=false] [--echo=false]   [--interactive=true] [--userpassword <i>user_password</i>]   [--groups <i>user_groups:[user_groups]*</i>] [--authrealmname   <i>auth_realm_name</i>] <i>user_name</i></pre>																								
<b>DESCRIPTION</b>	<p>Updates an existing entry in keyfile by the specified <i>user_name</i>, <i>user_password</i> and groups. Multiple groups can be entered by separating them, with a colon, ":". If the <i>auth_realm_name</i> is not specified, an entry is created in the default keyfile. If <i>auth_realm_name</i> is specified, an entry is created in the keyfile where the auth-realm name in the <code>domain.xml</code> file points to.</p> <p>This command is supported in remote mode only.</p>																								
<b>OPTIONS</b>	<table><tr><td>--user</td><td>authorized domain application server administrative username.</td></tr><tr><td>--password</td><td>password to administer the domain application server.</td></tr><tr><td>--host</td><td>machine name where the domain application server is running.</td></tr><tr><td>--port</td><td>port number of the domain application server listening for administration requests.</td></tr><tr><td>--secure</td><td>if true, uses SSL/TLS to communicate with the domain application server.</td></tr><tr><td>--passwordfile</td><td>file containing the domain application server password.</td></tr><tr><td>--terse</td><td>indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.</td></tr><tr><td>--echo</td><td>setting to true will echo the command line statement on the standard output. Default is false.</td></tr><tr><td>--interactive</td><td>if set to true (default), only the required password options are prompted.</td></tr><tr><td>--userpassword</td><td>password for the file user.</td></tr><tr><td>--groups</td><td>group where the file user belongs to.</td></tr><tr><td>--authrealmname</td><td>name, in the <code>domain.xml</code> file, where you have different stores for file auth realm.</td></tr></table>	--user	authorized domain application server administrative username.	--password	password to administer the domain application server.	--host	machine name where the domain application server is running.	--port	port number of the domain application server listening for administration requests.	--secure	if true, uses SSL/TLS to communicate with the domain application server.	--passwordfile	file containing the domain application server password.	--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	--echo	setting to true will echo the command line statement on the standard output. Default is false.	--interactive	if set to true (default), only the required password options are prompted.	--userpassword	password for the file user.	--groups	group where the file user belongs to.	--authrealmname	name, in the <code>domain.xml</code> file, where you have different stores for file auth realm.
--user	authorized domain application server administrative username.																								
--password	password to administer the domain application server.																								
--host	machine name where the domain application server is running.																								
--port	port number of the domain application server listening for administration requests.																								
--secure	if true, uses SSL/TLS to communicate with the domain application server.																								
--passwordfile	file containing the domain application server password.																								
--terse	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.																								
--echo	setting to true will echo the command line statement on the standard output. Default is false.																								
--interactive	if set to true (default), only the required password options are prompted.																								
--userpassword	password for the file user.																								
--groups	group where the file user belongs to.																								
--authrealmname	name, in the <code>domain.xml</code> file, where you have different stores for file auth realm.																								
<b>OPERANDS</b>	<i>user_name</i> name of file user.																								

<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the update-file-user command</p> <pre>asadmin&gt; update-file-user --user admin1 --password adminadmin1 --host pigeon --port 5001 --userpassword sample_password --groups staff:manager:engineer --authrealmname auth-realm1 sample_user Command update-file-user executed successfully</pre> <p>Where: the sample_user is the file user updated with the updated user password and groups.</p>
<b>EXIT STATUS</b>	<p>0    command executed successfully</p> <p>1    error in executing the command</p>
<b>SEE ALSO</b>	<p>delete-file-user(1), list-file-users(1), create-file-user(1), list-file-groups(1)</p>

## verifier(1M)

<b>NAME</b>	verifier – validates the J2EE Deployment Descriptors against application server DTDs
<b>SYNOPSIS</b>	<b>verifier</b> [-v] [-d <i>destination_directory</i> ] [-r [a w f]] <i>jar_filename</i>
<b>DESCRIPTION</b>	<p>Use the <code>verifier</code> utility to validate the J2EE deployment descriptors and the Sun ONE Application Server specific deployment descriptors. If the application is not J2EE compliant, an error message is printed.</p> <p>When you run the <code>verifier</code> utility, two results files are created in XML and TXT format. The location where the files are created can be configured using the <code>-d</code> option. The directory specified as the destination directory for result files should exist. If no directory is specified, the result files are created in the current directory. Result files are named as <i>jar_filename_verified.xml</i> and <i>jar_filename_verified.txt</i></p> <p>The XML file has various sections that are dynamically generated depending on what kind of application or module is being verified. The root tag is <code>static-verification</code> which may contain the tags <code>application</code>, <code>ejb</code>, <code>web</code>, <code>appclient</code>, <code>connector</code>, <code>other</code>, <code>error</code> and <code>failure-count</code>. The tags are self explanatory and are present depending on the type of module being verified. For example, an EAR file containing a web and EJB module will contain the tags <code>application</code>, <code>ejb</code>, <code>web</code>, <code>other</code>, and <code>failure-count</code>.</p> <p>If the verifier ran successfully, a result code of 0 is returned. A non-zero error code is returned if the verifier failed to run.</p>
<b>OPTIONS</b>	<p><code>-v</code> verbose debugging is turned on.</p> <p><code>-d</code> identifies where the result files get placed.</p> <p><code>-r</code> identifies the reporting level defined as one of the following:</p> <ul style="list-style-type: none"><li>■ a sets output reporting level to display all results (default)</li><li>■ w sets output reporting level to display warning and failure results</li><li>■ f sets output reporting level to display only failure results</li></ul> <p><i>jar_filename</i> name of the ear/war/jar file to perform static verification on. The results of verification are placed in two files <i>jar_filename_verified.xml</i> and <i>jar_filename_verified.txt</i> in the destination directory.</p>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using <code>verifier</code> in the Verbose Mode</p> <pre>example% verifier -v -d /verifier-results -rf sample.ear</pre> <p>Where <code>-v</code> runs the verifier in verbose mode, <code>-d</code> specifies the destination directory, and <code>-rf</code> displays only the failures. The results are stored in <code>/verifier-results/sample.ear_verified.xml</code> and <code>/verifier-results/sample.ear_verified.txt</code>.</p>
<b>SEE ALSO</b>	asadmin(1M)

<b>NAME</b>	verify-domain-xml – verifies the content of the domain.xml
<b>SYNOPSIS</b>	<b>verify-domain-xml</b> [ <b>--verbose=false</b> ] [ <b>--domaindir</b> <i>install_dir/domains</i> ] <i>domain_name</i>
<b>DESCRIPTION</b>	Verifies the content of the domain.xml file.
<b>OPTIONS</b>	<b>--verbose</b> turns on (true) or off (false, default) verbose debugging. <b>--domaindir</b> directory where the domain is to be created. If specified, path must be accessible in the filesystem. If not specified, the domain is created in the default <i>install_dir/domains</i> directory.
<b>OPERANDS</b>	<i>domain_name</i> name of the domain. Must be a unique name.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using the verify-domain-xml command asadmin> <b>verify-domain-xml --verbose=true domain1</b> Element: applications Error: J2eeApplication Module does not contains application name 'MEjbApp' J2eeApplication Module does not contains application name '__ejb_container_timer_app'
<b>EXIT STATUS</b>	0 command executed successfully 1 error in executing the command

version(1)

<b>NAME</b>	version – displays the version information
<b>SYNOPSIS</b>	<pre>version [--user <i>admin_user</i>] [--password <i>admin_password</i>]         [--host <i>localhost</i>] [--port <i>4848</i>] [--secure <i> -s</i>]         [--passwordfile <i>filename</i>] [--terse=false] [--echo=false]         [--interactive] [--verbose=false]</pre>
<b>DESCRIPTION</b>	version displays the version information. If the command-line cannot communicate with the administration server with the given user/password and host/port, then the command-line will retrieve the Version locally and display a warning message. If the user option is not entered, the command-line will retrieve the version locally and display a warning message. The warning message will not be displayed if --terse option is entered on the command line.
<b>OPTIONS</b>	<pre>--user          authorized domain application server administrative                 username. --password      password to administer the domain application server. --host          machine name where the domain application server is running. --port          port number of the domain application server listening for                 administration requests. --secure        if true, uses SSL/TLS to communicate with the domain                 application server. --passwordfile  file containing the domain application server password. --terse         indicates that any output data must be very concise, typically                 avoiding human-friendly sentences and favoring                 well-formatted data for consumption by a script. --echo          setting to true will echo the command line statement on the                 standard output. --interactive    prompts you for the required options that are not already                 specified. --verbose       displays version information in detail.</pre>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using remote mode to display version</p> <pre>asadmin&gt; version Java 2 Platform Enterprise Edition 1.4 Application Server</pre> <p><b>EXAMPLE 2</b> Using remote mode to display version in detail</p> <pre>asadmin&gt; version --user admin --password adminadmin --host bluestar --port 4848 --verbose Java 2 Platform Enterprise Edition 1.4 Application Server (build A021930-126949)</pre>
<b>EXIT STATUS</b>	0    command executed successfully



version(1)

1 error in executing the command

**SEE ALSO** help(1)

## wscompile(1M)

<b>NAME</b>	wscompile – generates stubs, ties, serializers, and WSDL files used in JAX-RPC clients and services																										
<b>SYNOPSIS</b>	<b>wscompile</b> [ <i>options</i> ] <i>configuration_file</i>																										
<b>DESCRIPTION</b>	<p>Generates the client stubs and server-side ties for the service definition interface that represents the web service interface. Additionally, it generates the WSDL description of the web service interface which is then used to generate the implementation artifacts.</p> <p>In addition to supporting the generation of stubs, ties, server configuration, and WSDL documents from a set of RMI interfaces, <i>wscompile</i> also supports generating stubs, ties and remote interfaces from a WSDL document.</p> <p>You must specify one of the <i>-gen</i> options in order to use <i>wscompile</i> as a stand alone generator. You must use either <i>-import</i> (for WSDL) or <i>-define</i> (for an RMI interface) along with the <i>-model</i> option in order to use <i>wscompile</i> in conjunction with <i>wsdeploy</i>.</p> <p>Invoking the <i>wscompile</i> command without specifying any arguments outputs the usage information.</p>																										
<b>OPTIONS</b>	<table><tr><td><i>-cp path</i></td><td>location of the input class files.</td></tr><tr><td><i>-classpath path</i></td><td>same as <i>-cp path</i> option.</td></tr><tr><td><i>-d directory</i></td><td>where to place the generated output files.</td></tr><tr><td><i>-define</i></td><td>read the service's RMI interface, define a service. Use this option with the <i>-model</i> option in order to create a model file for use with the <i>wsdeploy</i> command.</td></tr><tr><td><i>-f:features</i></td><td>enables the given features. Features are specified as a comma separated list of features. See the list of supported features below.</td></tr><tr><td><i>-features:features</i></td><td>same as <i>-f:features</i> option.</td></tr><tr><td><i>-g</i></td><td>generates the debugging information.</td></tr><tr><td><i>-gen</i></td><td>generates the client-side artifacts.</td></tr><tr><td><i>-gen:both</i></td><td>generates client and server artifacts.</td></tr><tr><td><i>-gen:client</i></td><td>same as <i>-gen</i> option.</td></tr><tr><td><i>-gen:server</i></td><td>generates the server-side artifacts and the WSDL file. If you are using <i>wsdeploy</i>, you do not specify this option.</td></tr><tr><td><i>-httpproxy:host:port</i></td><td>specifies an HTTP proxy server; defaults to port 8080.</td></tr><tr><td><i>-import</i></td><td>reads a WSDL file, generates the service RMI interface and a template of the class that implements the interface. Use</td></tr></table>	<i>-cp path</i>	location of the input class files.	<i>-classpath path</i>	same as <i>-cp path</i> option.	<i>-d directory</i>	where to place the generated output files.	<i>-define</i>	read the service's RMI interface, define a service. Use this option with the <i>-model</i> option in order to create a model file for use with the <i>wsdeploy</i> command.	<i>-f:features</i>	enables the given features. Features are specified as a comma separated list of features. See the list of supported features below.	<i>-features:features</i>	same as <i>-f:features</i> option.	<i>-g</i>	generates the debugging information.	<i>-gen</i>	generates the client-side artifacts.	<i>-gen:both</i>	generates client and server artifacts.	<i>-gen:client</i>	same as <i>-gen</i> option.	<i>-gen:server</i>	generates the server-side artifacts and the WSDL file. If you are using <i>wsdeploy</i> , you do not specify this option.	<i>-httpproxy:host:port</i>	specifies an HTTP proxy server; defaults to port 8080.	<i>-import</i>	reads a WSDL file, generates the service RMI interface and a template of the class that implements the interface. Use
<i>-cp path</i>	location of the input class files.																										
<i>-classpath path</i>	same as <i>-cp path</i> option.																										
<i>-d directory</i>	where to place the generated output files.																										
<i>-define</i>	read the service's RMI interface, define a service. Use this option with the <i>-model</i> option in order to create a model file for use with the <i>wsdeploy</i> command.																										
<i>-f:features</i>	enables the given features. Features are specified as a comma separated list of features. See the list of supported features below.																										
<i>-features:features</i>	same as <i>-f:features</i> option.																										
<i>-g</i>	generates the debugging information.																										
<i>-gen</i>	generates the client-side artifacts.																										
<i>-gen:both</i>	generates client and server artifacts.																										
<i>-gen:client</i>	same as <i>-gen</i> option.																										
<i>-gen:server</i>	generates the server-side artifacts and the WSDL file. If you are using <i>wsdeploy</i> , you do not specify this option.																										
<i>-httpproxy:host:port</i>	specifies an HTTP proxy server; defaults to port 8080.																										
<i>-import</i>	reads a WSDL file, generates the service RMI interface and a template of the class that implements the interface. Use																										

**SUPPORTED  
FEATURES**

	this option with the <code>-model</code> option in order to create a model file for use with the <code>wsdeploy</code> command.
<code>-model</code>	write the internal model for the given file name. Use this option with the <code>-import</code> option in order to create a model file for use with the <code>wsdeploy</code> command.
<code>-keep</code>	keeps the generated files.
<code>-nd <i>directory</i></code>	<i>directory</i> for the non-class generated WSDL files are stored.
<code>-O</code>	optimizes the generated code.
<code>-s <i>directory</i></code>	<i>directory</i> for the generated source files.
<code>-verbose</code>	output messages about what the compiler is doing.
<code>-version</code>	prints version information.
	Exactly one of the <code>-input</code> , <code>-define</code> , <code>-gen</code> options must be specified.
<code>datahandleronly</code>	always map attachments to data handler type
<code>documentliteral</code>	use document literal encoding
<code>donotoverride</code>	do not regenerate classes that already exist in the classpath.
<code>donotunwrap</code>	disable unwrapping of document/literal wrapper elements in WSI mode (default).
<code>explicitcontext</code>	turn on explicit service context mapping.
<code>infix:<i>name</i></code>	specify an <code>infix</code> to use for generated serializers (Solaris).
<code>infix=<i>name</i></code>	specify an <code>infix</code> to use for generated serializers (Windows).
<code>jaxbenumtype</code>	map anonymous enumeration to its base type.
<code>nodatabinding</code>	turn off data binding for literal encoding.
<code>noencodedtypes</code>	turn off encoding type information.
<code>nomultirefs</code>	turn off support for multiple references.
<code>norpcstructures</code>	do not generate RPC structures ( <code>-import</code> only).
<code>novalidation</code>	turn off validation for the imported WSDL file.
<code>resolveidref</code>	resolve <code>xsd:IDREF</code> .
<code>rpcliextral</code>	use the RPC literal encoding.
<code>searchschema</code>	search schema aggressively for subtypes.
<code>serializeinterfaces</code>	turn on direct serialization of interface types.
<code>strict</code>	generate code strictly compliant with JAXRPC specification.

## wscompile(1M)

	<p>unwrap                    enable unwrapping of document/literal wrapper elements in WSI mode.</p> <p>useonewayoperations allow generation of one-way operations.</p> <p>wsi                        enable WSI-Basic Profile features, to be used for document/literal, and RPC/literal.</p> <p>Note: the -gen options are not compatible with wsdeploy.</p>
<b>CONFIGURATION FILE</b>	<p>The <code>wscompile</code> command reads the configuration file <code>config.xml</code> which contains information that describes the web service. The structure of the file is as follows:</p> <pre>&lt;?xml version="1.0" encoding="UTF-8"?&gt; &lt;configuration xmlns="http://java.sun.com/xml/ns/jax-rpc/ri/config"&gt; &lt;service&gt; or &lt;wsdl&gt; or &lt;modelfile&gt; &lt;/configuration&gt;</pre> <p>The configuration element may contain exactly one <code>&lt;service&gt;</code>, <code>&lt;wsdl&gt;</code> or <code>&lt;modelfile&gt;</code>.</p>
<b>SERVICE ELEMENT</b>	<p>If the <code>&lt;service&gt;</code> element is specified, <code>wscompile</code> reads the RMI interface that describes the service and generates a WSDL file. In the <code>&lt;interface&gt;</code> subelement, the <code>name</code> attribute specifies the service's RMI interface, and the <code>servantName</code> attribute specifies the class that implements the interface. For example:</p> <pre>&lt;service name="CollectionIF_Service" targetNamespace="http://echoservice.org/wsdl" typeName="http://echoservice.org/types" packageName="stub_tie_generator_test"&gt; &lt;interface name="stub_tie_generator_test.CollectionIF" servantName="stub_tie_generator_test.CollectionImpl"/&gt; &lt;/service&gt;</pre>
<b>WSDL ELEMENT</b>	<p>If the <code>&lt;wsdl&gt;</code> element is specified, <code>wscompile</code> reads the WSDL file and generates the service's RMI interface. The <code>location</code> attribute specifies the URL of the WSDL file, and the <code>packageName</code> attribute specifies the package of the classes to be generated. For example:</p> <pre>&lt;wsdl</pre>

```
location="http://tempuri.org/sample.wsdl"
packageName="org.tempuri.sample"/>
```

**MODELFILE  
ELEMENT**

This element is for advanced users.

If `config.xml` contains a `<service>` or `<wsdl>` element, `wscompile` can generate a model file that contains the internal data structures that describe the service. If a model file is already generated, it can be reused next time while using `wscompile`. For example:

```
<modelfile location="mymodel.xml.gz"/>
```

**EXAMPLES**

**EXAMPLE 1** Using `wscompile` to generate client-side artifacts

```
wscompile -gen:client -d outputdir -classpath classpathdir config.xml
```

Where a client side artifact is generated in the `outputdir` for running the service as defined in the `config.xml` file.

**EXAMPLE 2** Using `wscompile` to generate server-side artifacts

```
wscompile -gen:server -d outputdir -classpath classpathdir -model modelfile.Z config.xml
```

Where a server side artifact is generated in the `outputdir` and the `modelfile` in `modelfile.Z` for services defined in the `config.xml` file.

**SEE ALSO**

`wsdeploy(1M)`

## wsdeploy(1M)

<b>NAME</b>	wsdeploy – reads a WAR file and the <code>jaxrpc-ri.xml</code> file and generates another WAR file that is ready for deployment														
<b>SYNOPSIS</b>	<b>wsdeploy</b> -o <i>input_WAR_file</i> <i>options</i>														
<b>DESCRIPTION</b>	<p>Use the <code>wsdeploy</code> command to take a WAR file which does not have implementation specific server side tie classes to generate a deployable WAR file that can be deployed on the application server. <code>wsdeploy</code> internally runs <code>wscompile</code> with the <code>-gen:server</code> option. The <code>wscompile</code> command generates classes and a WSDL file which <code>wsdeploy</code> includes in the generated WAR file.</p> <p>Generally, you don't have to run <code>wsdeploy</code> because the functions it performs are done automatically when you deploy a WAR with <code>deploytool</code> or <code>asadmin</code>.</p>														
<b>OPTIONS</b>	<table><tr><td><code>-classpath</code> <i>path</i></td><td>location of the input class files.</td></tr><tr><td><code>-keep</code></td><td>keep temporary files.</td></tr><tr><td><code>-tmpdir</code></td><td>temporary directory to use.</td></tr><tr><td><code>-o</code> <i>output WAR file</i></td><td>required; location of the generated WAR file.</td></tr><tr><td><code>-source</code> <i>version</i></td><td>generates code for the specified JAX-RPC SI version. Supported version are: 1.0.1, 1.0.3, and 1.1 (default).</td></tr><tr><td><code>-verbose</code></td><td>outputs messages about what the compiler is doing.</td></tr><tr><td><code>-version</code></td><td>prints version information.</td></tr></table>	<code>-classpath</code> <i>path</i>	location of the input class files.	<code>-keep</code>	keep temporary files.	<code>-tmpdir</code>	temporary directory to use.	<code>-o</code> <i>output WAR file</i>	required; location of the generated WAR file.	<code>-source</code> <i>version</i>	generates code for the specified JAX-RPC SI version. Supported version are: 1.0.1, 1.0.3, and 1.1 (default).	<code>-verbose</code>	outputs messages about what the compiler is doing.	<code>-version</code>	prints version information.
<code>-classpath</code> <i>path</i>	location of the input class files.														
<code>-keep</code>	keep temporary files.														
<code>-tmpdir</code>	temporary directory to use.														
<code>-o</code> <i>output WAR file</i>	required; location of the generated WAR file.														
<code>-source</code> <i>version</i>	generates code for the specified JAX-RPC SI version. Supported version are: 1.0.1, 1.0.3, and 1.1 (default).														
<code>-verbose</code>	outputs messages about what the compiler is doing.														
<code>-version</code>	prints version information.														
<b>INPUT WAR FILE</b>	<p>The input WAR file for <code>wsdeploy</code> will typically have the following structure:</p> <pre>META-INF/MANIFEST.MF WEB-INF/classes/hello/HelloIF.class WEB-INF/classes/hello/HelloImpl.class WEB-INF/jaxrpc-ri.xml WEB-INF/web.xml</pre> <p>Where: <code>HelloIF</code> is the service endpoint interface, and <code>HelloImpl</code> is the class that implements the interface. The <code>web.xml</code> file is the deployment descriptor of a web component.</p>														
<b>jaxrpc-ri.xml FILE</b>	<p>The following is a simple HelloWorld service.</p> <pre>&lt;xml version="1.0" encoding="UTF-8"?&gt; &lt;webServices&gt;   xmlns="http://java.sun.com/xml/ns/jax-rpc/ri/dd"   version="1.0"   targetNamespaceBase="http://com.test/wsdl"   typeNamespaceBase="http://com.test/types"   urlPatternBase="/ws"&gt;   &lt;endpoint     name="MyHello"</pre>														

```

        displayName="HelloWorld Service"
        description="A simple web service"
        wsdl="/WEB-INF/<wsdlname>
        interface="hello.HelloIF"
        implementation="hello.HelloImpl"/>
    <endpointMapping
        endpointName="MyHello"
        urlPattern="/hello"/>
</webServices>

```

The `webServices()` element must contain one or more `endpoint()` elements. The `interface` and `implementation` attributes of `endpoint()` specify the service's interface and implementation class. The `endpointMapping()` element associates the service port with the part of the endpoint URL path that follows the `urlPatternBase()`.

## NAMESPACE MAPPINGS

Here is a schema type name example:

```

schemaType="ns1:SampleType"
xmlns:ns1="http://echoservice.org/types"

```

When generating a Java type from a schema type, `wscompile` gets the classname from the local part of the schema type name. To specify the package name of the generated Java classes, you define a mapping between the schema type namespace and the package name. You define this mapping by adding a `<namespaceMappingRegistry>` element to the `config.xml` file. For example:

```

<service>
    ...
    <namespaceMappingRegistry>
        <namespaceMapping
            namespace="http://echoservice.org/types"
            packageName="echoservice.org.types"/>
        </namespaceMappingRegistry>
    .....
</service>

```

You can also map namespaces in the opposite direction, from schema types to Java types. In this case, the generated schema types are taken from the package that the type comes from.

## HANDLERS

A handler accesses a SOAP message that represents an RPC request or response. A handler class must implement the `javax.xml.rpc.handler` interface. Because it accesses a SOAP message, a handler can manipulate the message with the APIs of the `javax.xml.soap.package()`.

A handler chain is a list of handlers. You may specify one handler chain for the client and one for the server. On the client, you include the `handlerChains()` element in the `jaxrpc-ri.xml` file. On the server, you include this element in the `config.xml` file. Here is an example of the `handlerChains()` element in the `config.xml`:

wsdeploy(1M)

```
<handlerChains>
  <chain runAt="server"
    roles=
      "http://acme.org/auditing
      "http://acme.org/morphing"
    xmlns:ns1="http://foo/fo-1">
    <handler className="acme.MyHandler"
      headers="ns1:foo ns1:bar"/>
      <property
        name="property" value="xyz"/>
      </handler>
    </chain>
  </handlerChains>
```

For more information on handlers, see the SOAP message Handlers chapter of the JAX-PRC specifications.

**SEE ALSO** wscompile(1M)



# Index

---

## **a**

applies the changes you have made for a server instance — reconfig, 198

## **b**

brings down the administration server and associated instances — shutdown, 205

## **d**

displays the license information — display-license, 138  
displays the status of the deployed component — show-component-status, 204

## **g**

generates stubs, ties, serializers, and WSDL files used in JAX-RPC clients and services — wscompile, 226

## **i**

installs the license file — install-license, 150

## **L**

Lists deployed components — list-components, 162  
Lists EJBs or Servlets in a deployed module or in a module of a deployed application — list-sub-components, 190

## **r**

reads a WAR file and the `jaxrpc-ri.xml` file and generates another WAR file that is ready for deployment — wsdeploy, 230  
registers the persistence resource — create-persistence-resource, 79  
enables the component — enable, 139

## **s**

sets the values of attributes — set, 203  
starts the domains in the specified or default domains directory — start-appserv, 206  
disables the component — disable, 137

## **A**

add-resources — registers the resource in the XML file specified, 14  
adds a new access control list file for the named instance — create-acl, 29

- adds a new HTTP listener socket —  
  create-http-listener, 51
- adds an audit-module — create-audit-  
  module, 32
- adds the IIOP listener — create-iiop-listener, 55
- adds the physical destination —  
  create-jmsdest, 67
- adds the named virtual server —  
  create-virtual-server, 89
- adds the new authorized database for the  
  named instance — create-authdb, 34
- adds the new authorized realm —  
  create-auth-realm, 36
- appclient — launches the Application Client  
  Container and invokes the client application  
  packaged in the application JAR file, 16
- asadmin — utility for performing  
  administrative tasks for the Sun Java System  
  Application Server, 18
- asant — launches the Jakarta Ant tool, 20
- asmigrate — automates migration of J2EE  
  applications from other J2EE platforms to  
  Sun Java System Application Server, 22
- asupgrade — migrates the configuration of a  
  previously installed Sun Java System  
  Application Server, 26
- automates migration of J2EE applications from  
  other J2EE platforms to Sun Java System  
  Application Server — asmigrate, 22

## C

- capture-schema — stores the database metadata  
  (schema) in a file for use in mapping and  
  execution, 28
- checks to see if the JMS provider is up and  
  running — jms-ping, 151
- create-acl — adds a new access control list file  
  for the named instance, 29
- create-audit-module — adds an  
  audit-module, 32
- create-auth-realm — adds the new authorized  
  realm, 36
- create-authdb — adds the new authorized  
  database for the named instance, 34
- create-connector-resource — registers the  
  resource with the specified JNDI name, 41
- create-connector-security-map — creates a  
  security map for the named connector  
  connection pool, 43
- create-custom-resource — registers the custom  
  resource, 45
- create-domain — creates a domain with the  
  given name, 47
- create-file-user — creates a new file user, 49
- create-http-listener — adds a new HTTP listener  
  socket, 51
- create-iiop-listener — adds the IIOP listener, 55
- create-instance — creates an application server  
  instance with the specified instance  
  name, 57
- create-javamail-resource — registers the  
  JavaMail resource, 59
- create-jdbc-connection-pool — registers the  
  JDBC connection pool, 61
- create-jdbc-resource — registers the JDBC  
  resource, 65
- create-jms-resource — registers the JMS  
  resource, 70
- create-jmsdest — adds the physical  
  destination, 67
- create-jndi-resource — registers the JNDI  
  resource, 72
- create-jvm-options — creates the JVM options  
  from the Java configuration or profiler  
  elements, 74
- create-persistence-resource — registers the  
  persistence resource, 79
- create-profiler — creates the profiler  
  element, 81
- create-resource-adapter-config — creates the  
  resource adapter javabean, 83
- create-ssl — Creates the SSL element in the  
  HTTP listener, IIOP listener, or IIOP  
  Service, 85
- create-virtual-server — adds the named virtual  
  server, 89
- creates a domain with the given name —  
  create-domain, 47
- creates a new file user — create-file-user, 49
- creates a security map for the named connector  
  connection pool — create-connector-security-  
  map, 43

- creates an application server instance with the specified instance name —  
create-instance, 57
- creates the JVM options from the Java configuration or profiler elements —  
create-jvm-options, 74
- creates the profiler element —  
create-profiler, 81
- creates the resource adapter javabean —  
create-resource-adapter-config, 83
- Creates the SSL element in the HTTP listener, IIOP listener, or IIOP Service —  
create-ssl, 85

## D

- delete-acl — removes the access control list file for the named instance, 91
- delete-auth-realm — removes the named authorized realm, 95
- delete-authdb — removes the authorized database for the named instance, 94
- delete-connector-connection-pool — removes the specified connection pool, 96
- delete-connector-resource — removes the named connector resource, 98
- delete-custom-resource — removes the custom resource, 101
- delete-domain — deletes the given domain, 102
- delete-file-user — removes the named file user, 103
- delete-http-listener — removes the HTTP listener, 105
- delete-http-qos — removes the quality of service parameter for the named instance, 106
- delete-iiop-listener — removes the IIOP listener, 107
- delete-instance — deletes the instance that is not running., 108
- delete-javamail-resource — removes the JavaMail resource, 110
- delete-jdbc-connection-pool — removes the JDBC connection pool, 111
- delete-jdbc-resource — removes the JDBC resource, 113

- delete-jms-resource — removes the JMS resource, 116
- delete-jmsdest — destroys the physical destination, 114
- delete-jndi-resource — removes the JNDI resource, 117
- delete-jvm-options — deletes the JVM options from the Java configuration or profiler elements, 118
- delete-lifecycle-module — removes the lifecycle module, 120
- delete-mime — removes the MIME type for the named instance, 121
- delete-persistence-resource — removes the persistence resource, 122
- delete-profiler — deletes the profiler element, 123
- delete-resource-adapter-config — deletes the resource adapter javabean, 124
- delete-virtual-server — deletes the virtual server with the named virtual server ID, 128
- delete-admin-object — removes the administered object with the specified JNDI name, 92
- deletes the given domain —  
delete-domain, 102
- deletes the instance that is not running. —  
delete-instance, 108
- deletes the JVM options from the Java configuration or profiler elements —  
delete-jvm-options, 118
- deletes the profiler element —  
delete-profiler, 123
- deletes the resource adapter javabean —  
delete-resource-adapter-config, 124
- deletes the virtual server with the named virtual server ID — delete-virtual-server, 128
- deploy — deploys the specified component, 129
- deploydir — deploys an exploded format of application archive, 133
- deploys an exploded format of application archive — deploydir, 133
- deploys the specified component —  
deploy, 129
- destroys the physical destination —  
delete-jmsdest, 114

disable — disables the component, 137  
display-license — displays the license information, 138  
displays a list of all the commands available in the Command-line interface — help, 145  
displays the version information — version, 224

## E

enable — enables the component, 139  
export — marks a variable name for automatic export to the environment of subsequent commands in multimode, 140

## G

get — gets the values of the monitorable or configurable attributes, 142  
get-client-stubs — gets the stubs of the client, 144  
gets all the administered objects — list-admin-objects, 158  
gets all the connection pools — list-connector-connection-pools, 163  
gets all the Javamail resources — list-javamail-resources, 175  
gets all the JDBC connection pools — list-jdbc-connection-pools, 176  
gets all the JDBC resources — list-jdbc-resources, 177  
gets all the JMS resources — list-jms-resources, 180  
gets all the JNDI resources — list-jndi-resources, 182  
gets all the physical destinations — list-jmsdest, 178  
gets all the persistence resources — list-persistence-resources, 185  
gets the access control lists for the named instance — list-acls, 157  
gets the HTTP listeners — list-http-listeners, 172  
gets the IIOP listeners — list-iiop-listeners, 173  
gets the lifecycle modules — list-lifecycle-modules, 183

gets the MIME types for the named instance — list-mimes, 184  
gets the stubs of the client — get-client-stubs, 144  
gets the values of the monitorable or configurable attributes — get, 142  
gets the virtual servers — list-virtual-servers, 192

## H

help — displays a list of all the commands available in the Command-line interface, 145

## I

install-license — installs the license file, 150

## J

jms-ping — checks to see if the JMS provider is up and running, 151  
jspc — precompiles JSP source files into servlets, 152

## L

launches the Application Client Container and invokes the client application packaged in the application JAR file. — appclient, 16  
launches the Jakarta Ant tool — asant, 20  
list — lists the configurable elements, 154  
list-acls — gets the access control lists for the named instance, 157  
list-auth-realms — lists the authorized realms, 161  
list-components — Lists deployed components, 162  
list-connector-connection-pools — gets all the connection pools, 163  
list-connector-security-maps — lists the security maps for the connector connection pool, 165  
list-domains — lists the domains in the given domains directory, 168

- list-file-groups — lists the file groups, 169
- list-file-users — lists the file users, 171
- list-http-listeners — gets the HTTP listeners, 172
- list-iiop-listeners — gets the IIOP listeners, 173
- list-javamail-resources — gets all the Javamail resources, 175
- list-jdbc-connection-pools — gets all the JDBC connection pools, 176
- list-jdbc-resources — gets all the JDBC resources, 177
- list-jms-resources — gets all the JMS resources, 180
- list-jmsdest — gets all the physical destinations, 178
- list-jndi-resources — gets all the JNDI resources, 182
- list-lifecycle-modules — gets the lifecycle modules, 183
- list-mimes — gets the MIME types for the named instance, 184
- list-persistence-resources — gets all the persistence resources, 185
- list-resource-adapter-configs — lists the names of the configured resource adapters, 188
- list-sub-components — Lists EJBs or Servlets in a deployed module or in a module of a deployed application, 190
- list-virtual-servers — gets the virtual servers, 192
- list-admin-objects — gets all the administered objects, 158
- lists the authorized realms — list-auth-realms, 161
- lists the configurable elements — list, 154
- lists the file users — list-file-users, 171
- lists the domains in the given domains directory — list-domains, 168
- lists the file groups — list-file-groups, 169
- lists the names of the configured resource adapters — list-resource-adapter-configs, 188
- lists the security maps for the connector connection pool — list-connector-security-maps, 165

## M

- marks a variable name for automatic export to the environment of subsequent commands in multimode — export, 140
- migrates the configuration of a previously installed Sun Java System Application Server — asupgrade, 26

## P

- package-appclient — packs the application client container libraries and jar files, 194
- packs the application client container libraries and jar files — package-appclient, 194
- precompiles JSP source files into servlets — jspc, 152

## R

- reconfig — applies the changes you have made for a server instance, 198
- registers the custom resource — create-custom-resource, 45
- registers the JavaMail resource — create-javamail-resource, 59
- registers the JDBC connection pool — create-jdbc-connection-pool, 61
- registers the JDBC resource — create-jdbc-resource, 65
- registers the JMS resource — create-jms-resource, 70
- registers the JNDI resource — create-jndi-resource, 72
- registers the resource in the XML file specified — add-resources, 14
- registers the resource with the specified JNDI name — create-connector-resource, 41
- removes one or more variables from the multimode environment — unset, 217
- removes the access control list file for the named instance — delete-acl, 91
- removes the administered object with the specified JNDI name — delete-admin-object, 92
- removes the authorized database for the named instance — delete-authdb, 94

- removes the custom resource —  
  - delete-custom-resource, 101
- removes the HTTP listener —  
  - delete-http-listener, 105
- removes the IIOP listener —  
  - delete-iiop-listener, 107
- removes the JavaMail resource—  
  - delete-javamail-resource, 110
- removes the JDBC connection pool —  
  - delete-jdbc-connection-pool, 111
- removes the JDBC resource —  
  - delete-jdbc-resource, 113
- removes the JMS resource —  
  - delete-jms-resource, 116
- removes the JNDI resource —  
  - delete-jndi-resource, 117
- removes the lifecycle module —  
  - delete-lifecycle-module, 120
- removes the MIME type for the named instance  
  - delete-mime, 121
- removes the named authorized realm —  
  - delete-auth-realm, 95
- removes the named connector resource —  
  - delete-connector-resource, 98
- removes the named file user —  
  - delete-file-user, 103
- removes the persistence resource—  
  - delete-persistence-resource, 122
- removes the quality of service parameter for the  
named instance — delete-http-qos, 106
- removes the specified connection pool —  
  - delete-connector-connection-pool, 96

## S

- set — sets the values of attributes, 203
- show-component-status — displays the status  
of the deployed component, 204
- shutdown — brings down the administration  
server and associated instances, 205
- start-appserv — starts the domains in the  
specified or default domains directory, 206
- start-domain — starts the given domain, 207
- starts the given domain — start-domain, 207
- stop-domain — stops the given domain, 211
- stops the given domain — stop-domain, 211

- stores the database metadata (schema) in a file  
for use in mapping and execution —  
  - capture-schema, 28

## U

- unset — removes one or more variables from  
the multimode environment, 217
- update-connector-security-map — updates the  
security map for the named connector  
connection pool, 218
- update-file-user — updates a current file user as  
specified, 220
- updates a current file user as specified —  
  - update-file-user, 220
- updates the security map for the named  
connector connection pool —  
  - update-connector-security-map, 218
- utility for performing administrative tasks for  
the Sun Java System Application Server —  
  - asadmin, 18

## V

- validates the J2EE Deployment Descriptors  
against application server DTDs —  
  - verifier, 222
- verifier — validates the J2EE Deployment  
Descriptors against application server  
DTDs, 222
- verifies the content of the domain.xml —  
  - verify-domain-xml, 223
- verify-domain-xml — verifies the content of the  
domain.xml, 223
- version — displays the version  
information, 224

## W

- wscmpile — generates stubs, ties, serializers,  
and WSDL files used in JAX-RPC clients and  
services, 226
- wsdeploy — reads a WAR file and the  
jaxrpc-ri.xml file and generates another  
WAR file that is ready for deployment, 230