



# Sun Java System Application Server Platform Edition 8.1 2005Q1 Reference Manual

---

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

Part No: 819-0082  
January 2005

Copyright 2005 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 or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and 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.

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

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 2005 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, 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.



050113@10536



# Contents

---

## **Preface    9**

## **User Commands    11**

add-resources(1)	12
appclient(1)	15
asadmin(1M)	17
asant(1M)	20
asmigrate(1m)	23
asupgrade(1)	27
backup-domain(1)	31
capture-schema(1m)	32
change-master-password(1)	34
create-acl(1)	36
create-admin-object(1)	37
create-audit-module(1)	39
create-auth-realm(1)	41
create-connection-group(1)	43
create-connector-connection-pool(1)	44
create-connector-resource(1)	47
create-connector-security-map(1)	49
create-custom-resource(1)	52
create-domain(1)	54
create-file-user(1)	57
create-http-listener(1)	59
create-iiop-listener(1)	62
create-instance(1)	64

create-javamail-resource(1) 68  
 create-jdbc-connection-pool(1) 71  
 create-jdbc-resource(1) 75  
 create-jmsdest(1) 77  
 create-jms-resource(1) 80  
 create-jndi-resource(1) 86  
 create-jvm-options(1) 89  
 create-lifecycle-module(1) 91  
 create-message-security-provider(1) 94  
 create-password-alias(1) 99  
 create-persistence-resource(1) 101  
 create-profiler(1) 104  
 create-resource-adapter-config(1) 106  
 create-ssl(1) 108  
 create-system-properties(1) 113  
 create-threadpool(1) 115  
 create-virtual-server(1) 118  
 delete-acl(1) 122  
 delete-admin-object-1(1) 123  
 delete-audit-module(1) 125  
 delete-auth-realm(1) 127  
 delete-connector-connection-pool(1) 129  
 delete-connector-resource(1) 131  
 delete-connector-security-map(1) 133  
 delete-custom-resource(1) 135  
 delete-domain(1) 137  
 delete-file-user(1) 138  
 delete-http-listener(1) 140  
 delete-iiop-listener(1) 142  
 delete-instance(1) 144  
 delete-javamail-resource(1) 146  
 delete-jdbc-connection-pool(1) 148  
 delete-jdbc-resource(1) 150  
 delete-jmsdest(1) 152  
 delete-jms-resource(1) 154  
 delete-jndi-resource(1) 156  
 delete-jvm-options(1) 158  
 delete-lifecycle-module(1) 160

delete-message-security-provider(1) 162  
delete-password-alias(1) 165  
delete-persistence-resource(1) 167  
delete-profiler(1) 169  
delete-resource-adapter-config(1) 171  
delete-ssl(1) 173  
delete-system-property(1) 176  
delete-threadpool(1) 178  
delete-virtual-server(1) 181  
deploy(1) 183  
deploydir(1) 189  
deploytool(1m) 193  
disable(1) 194  
display-license(1) 196  
enable(1) 198  
export(1) 200  
freeze-transaction-service(1) 201  
get(1) 203  
get-client-stubs(1) 205  
help(1) 207  
install-license(1) 213  
jms-ping(1) 214  
jspc(1M) 216  
list(1) 219  
list-acls(1) 222  
list-admin-objects(1) 223  
list-application-refs(1) 225  
list-audit-modules(1) 227  
list-auth-realms(1) 229  
list-backups(1) 231  
list-components(1) 232  
list-connection-groups(1) 234  
list-connector-connection-pools(1) 235  
list-connector-resources(1) 237  
list-connector-security-maps(1) 239  
list-custom-resources(1) 242  
list-domains(1) 244  
list-file-groups(1) 245

- list-file-users(1) 247
- list-http-listeners(1) 249
- list-iiop-listeners(1) 251
- list-instances(1) 253
- list-javamail-resources(1) 255
- list-jdbc-connection-pools(1) 257
- list-jdbc-resources(1) 259
- list-jmsdest(1) 261
- list-jms-resources(1) 263
- list-jndi-entries(1) 265
- list-jndi-resources(1) 267
- list-lifecycle-modules(1) 269
- list-message-security-providers(1) 271
- list-password-aliases(1) 273
- list-persistence-resources(1) 275
- list-resource-adapter-configs(1) 277
- list-sub-components(1) 279
- list-system-properties(1) 281
- list-threadpools(1) 283
- list-timers(1) 285
- list-transaction-id(1) 287
- list-virtual-servers(1) 289
- multimode(1) 291
- package-appclient( 1M) 292
- ping-connection-pools(1) 293
- recover-transactions(1) 295
- restore-domain(1) 297
- rollback-transaction(1) 298
- set(1) 300
- show-component-status(1) 302
- shutdown(1) 304
- start-appserv(1) 305
- start-domain(1) 307
- start-instance(1) 310
- stop-appserv(1) 312
- stop-domain(1) 313
- stop-instance(1) 316
- undeploy(1) 318

unfreeze-transaction-service(1) 321  
unset(1) 323  
update-connector-security-map(1) 324  
update-file-user(1) 327  
update-password-alias(1) 329  
verifier(1M) 331  
verify-domain-xml(1) 333  
version(1) 334  
wscompile(1M) 336  
wsdeploy(1M) 340

**Index 343**





# 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	<p>This section shows the syntax of commands or functions.</p> <p>The following special characters are used in this section:</p> <p>[ ]      Brackets. The option or argument enclosed in these brackets is optional. If the brackets are omitted, the argument must be specified.</p>

		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-resources(1)

NAME	add-resources – creates the resources specified in an XML file												
SYNOPSIS	<b>add-resources</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--target <i>target</i> ] <i>xml_file_path</i>												
DESCRIPTION	<p>The add-resources command creates the resources named in the specified XML file. The <i>xml_file_path</i> is the path to the XML file containing the resources to be created. 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>												
OPTIONS	<table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASEPASSWORD, and so on.</td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td>-s --secure</td><td>If set to true, uses SSL/TLS to communicate with the domain application server.</td></tr> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASEPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	-s --secure	If set to true, uses SSL/TLS to communicate with the domain application server.
-u --user	The authorized domain application server administrative username.												
-w --password	The --password option is deprecated. Use --passwordfile instead.												
--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASEPASSWORD, and so on.												
-H --host	The machine name where the domain application server is running. The default value is localhost.												
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.												
-s --secure	If set to true, uses SSL/TLS to communicate with the domain application server.												

OPERANDS	-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.
	-h --help	Displays the help text for the command.
	--target	In Enterprise Edition, specifies the target for which you are creating the resources. Valid values are <ul style="list-style-type: none"> <li>■ <i>server</i>, which creates the resources for the default server instance <i>server</i> and is the default value</li> <li>■ <i>domain</i>, which creates the resources for the domain</li> <li>■ <i>cluster_name</i>, which creates the resources for every server instance in the cluster</li> <li>■ <i>instance_name</i>, which creates the resources for a particular server instance</li> </ul>
	<i>xml_file_path</i>	<p>The path to the XML file containing the resource(s) to be created.</p> <p>An example XML file follows. Replace <code>&lt;install_dir&gt;</code> with the location of your Application Server installation.</p> <pre>&lt;?xml version="1.0" encoding="UTF-8"?&gt; &lt;!DOCTYPE resources PUBLIC "-//Sun Microsystems Inc.//DTD Application Server 8.0 Domain//EN "*&lt;install_dir&gt;/lib/dtds/sun-resources_1_0.dtd*"&gt;  &lt;resources&gt; &lt;jdbc-connection-pool name="SPECjPool" steady-pool-size="100" max-pool-size="150" max-wait-time-in-millis="60000" pool-resize-quantity="2" idle-timeout-in-seconds="300" is-isolation-level-guaranteed="true" is-connection-validation-required="false" connection-validation-method="auto-commit" fail-all-connections="false" datasource-classname="oracle.jdbc.pool.OracleDataSource"&gt; &lt;property name="URL" value="jdbc:oracle:thin:@iasperfsol12:1521:specdb"/&gt; &lt;property name="User" value="spec"/&gt; &lt;property name="Password" value="spec"/&gt; &lt;property name="MaxStatements" value="200"/&gt;</pre>

add-resources(1)

```
<property name="ImplicitCachingEnabled" value="true"/>
</jdbc-connection-pool>
<jdbc-resource enabled="true" pool-name="SPECjPool"
  jndi-name="jdbc/SPECjDB"/>
</resources>
```

## EXAMPLES

**EXAMPLE 1** Using the add-resources command

The following command creates resources using the contents of the XML file `resource.xml`:

```
asadmin> add-resources --user admin --passwordfile passwords.txt
--host localhost --port 4848 resource.xml
Command add-resources executed successfully.
```

## EXIT STATUS

0  
command executed successfully

1  
error in executing the command

## 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)`

NAME	appclient – launches the Application Client Container and invokes the client application packaged in the application JAR file										
SYNOPSIS	<b>appclient</b> --client <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> ]										
DESCRIPTION	<p>Use the appclient 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 deploytool or by using the asadmin deploy 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 client.jar that is retrieved after deploying an application , should be passed with the -client option while running the appclient utility. The -mainclass and -name options are optional for a single client application. For multiple client applications use either the -classname option or the- name option.</p>										
OPTIONS	<table> <tr> <td>--client</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 deploytool or by the asadmin deploy command.</td></tr> <tr> <td>--mainclass</td><td>optional; the full classname of the main client application main () method that will be invoked by the Application Client Container. Used for a single client application. By default, uses the class specified in the client jar. The class name must be the full name. For example, com.sun.test.AppClient</td></tr> <tr> <td>--name</td><td>optional; the display name for the client application. Used for multiple client applications. By default, the display name is specified in the client jar application-client.xml file which is identified by the display-name attribute.</td></tr> <tr> <td>--xml</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 \$AS_ACC_CONFIG identified in asenv.conf file.</td></tr> <tr> <td>--textauth</td><td>optional; used to specify using text format authentication when authentication is needed.</td></tr> </table>	--client	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 deploytool or by the asadmin deploy command.	--mainclass	optional; the full classname of the main client application main () method that will be invoked by the Application Client Container. Used for a single client application. By default, uses the class specified in the client jar. The class name must be the full name. For example, com.sun.test.AppClient	--name	optional; the display name for the client application. Used for multiple client applications. By default, the display name is specified in the client jar application-client.xml file which is identified by the display-name attribute.	--xml	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 \$AS_ACC_CONFIG identified in asenv.conf file.	--textauth	optional; used to specify using text format authentication when authentication is needed.
--client	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 deploytool or by the asadmin deploy command.										
--mainclass	optional; the full classname of the main client application main () method that will be invoked by the Application Client Container. Used for a single client application. By default, uses the class specified in the client jar. The class name must be the full name. For example, com.sun.test.AppClient										
--name	optional; the display name for the client application. Used for multiple client applications. By default, the display name is specified in the client jar application-client.xml file which is identified by the display-name attribute.										
--xml	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 \$AS_ACC_CONFIG identified in asenv.conf file.										
--textauth	optional; used to specify using text format authentication when authentication is needed.										
EXAMPLES	<p><b>EXAMPLE 1</b> Using the appclient command</p> <pre>appclient -client appserv/bin/myclientapp.jar -mainclass com.sun.test.TestAppClient -xml sun-acc.xml scott sample</pre>										

## appclient(1)

**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\(1M\)](#)



NAME	asadmin – utility for performing administrative tasks for the Sun Java System Application Server
SYNOPSIS	<b>asadmin</b> <i>subcommand</i> [-short_option[short_option_argument]] * [--long_option[long_option_argument]] * [operand] *
DESCRIPTION	<p>Use the asadmin utility to perform any administrative task for the Sun Java System Application Server. You can use this utility in place of using the Administration Console 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 asadmin 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> <p>-u --user                   authorized domain application server administrative username.</p> <p>-w --password               password to administer the domain application server.</p> <p>                            The --password option is deprecated. Use --passwordfile instead.</p> <p>--passwordfile            The 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.</p> <p>-H --host                   machine name where the domain application server is running.</p> <p>-p --port                   port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4949.</p> <p>-s --secure                 if true, uses SSL/TLS to communicate with the domain application server.</p>

## asadmin(1M)

<code>-t --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>-e --echo</code>	setting to true will echo the command line statement on the standard output. Default is false.
<code>-I --interactive</code>	if set to true (default), only the required password options are prompted.
<code>-h --help</code>	displays the help text for the command.

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
AS_ADMIN_MASTERPASSWORD=value
```

If `AS_ADMIN_PASSWORD` has been exported to the global environment, specifying the `--passwordfile` option will produce a warning using about the `--password` option. Unset `AS_ADMIN_PASSWORD` to prevent this from happening.

The master password is not propagated on the command line or an environment variable, but can be specified in the `passwordfile`.

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 Application Server command-line interface subcommands on the Solaris platform, 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:

asadmin(1M)

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Interface Stability	Unstable

**SEE ALSO** [appclient\(1M\)](#), [package-appclient\(1M\)](#)

asant(1M)

NAME	asant – launches the Jakarta Ant tool																						
SYNOPSIS	<b>asant</b> <i>target_list</i>																						
DESCRIPTION	<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 pick up the application server installed targets.</p> <p>To use Ant as part of the Sun Java System Application Server, verify that your PATH includes the provided <code>asant</code> (UNIX) or <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>																						
TARGETS	<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 <i>sample_dir/assemble/war</i></td></tr><tr><td><code>ear</code></td><td>assembles the EAR file in <i>sample_dir/assemble/ear</i></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 <i>sample_dir/javadocs</i></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 Java System Application Server.</td></tr><tr><td><code>clean</code></td><td>removes <i>appname/build/</i> and <i>appname/assemble/</i> and <i>appname/javadocs</i> 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 <i>sample_dir/assemble/war</i>	<code>ear</code>	assembles the EAR file in <i>sample_dir/assemble/ear</i>	<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 <i>sample_dir/javadocs</i>	<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 Java System Application Server.	<code>clean</code>	removes <i>appname/build/</i> and <i>appname/assemble/</i> and <i>appname/javadocs</i> 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 <i>sample_dir/assemble/war</i>																						
<code>ear</code>	assembles the EAR file in <i>sample_dir/assemble/ear</i>																						
<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 <i>sample_dir/javadocs</i>																						
<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 Java System Application Server.																						
<code>clean</code>	removes <i>appname/build/</i> and <i>appname/assemble/</i> and <i>appname/javadocs</i> 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**

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

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

See also [asadmin\(1M\)](#).

asant(1M)

See the *Sun Java System Application Server Developer's Guide* for information about special Ant tasks you can use.

NAME	asmigrate – automates migration of J2EE applications from other J2EE platforms to Sun Java System Application Server													
SYNOPSIS	<pre>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]</pre>													
DESCRIPTION	<p>Use the <code>asmigrate</code> utility to analyze your J2EE application and translate vendor specific settings to Sun JavaTM™ System Application Server specific settings that makes the application deployable on Sun’s J2EE products.</p> <p>The following table identifies the supported J2EE product migrations:</p> <table><tr><th>Source J2EE Platform</th><th>Destination J2EE Platform</th></tr><tr><td>WebLogic Application Server 5.1, 6.0, 6.1, 8.1</td><td rowspan="9">Sun JavaTM™ System Application Server 8.1 2005Q1</td></tr><tr><td>WebSphere Application Server 4.0, 5.x</td></tr><tr><td>JavaTM™ 2 Platform Enterprise Edition 1.3/1.4</td></tr><tr><td>Sun ONE Application Server 6.5, 7.0</td></tr><tr><td>Sun JavaTM™ System Application Server 7 2004Q2</td></tr><tr><td>Sun ONE Web Server 6.0</td></tr><tr><td>J2EE Reference Implementation 1.3, 1.4</td></tr><tr><td>JBoss Application Server 3.0, 3.2</td></tr><tr><td>Tomcat Web Server 4.1.12</td></tr></table>		Source J2EE Platform	Destination J2EE Platform	WebLogic Application Server 5.1, 6.0, 6.1, 8.1	Sun JavaTM™ System Application Server 8.1 2005Q1	WebSphere Application Server 4.0, 5.x	JavaTM™ 2 Platform Enterprise Edition 1.3/1.4	Sun ONE Application Server 6.5, 7.0	Sun JavaTM™ System Application Server 7 2004Q2	Sun ONE Web Server 6.0	J2EE Reference Implementation 1.3, 1.4	JBoss Application Server 3.0, 3.2	Tomcat Web Server 4.1.12
Source J2EE Platform	Destination J2EE Platform													
WebLogic Application Server 5.1, 6.0, 6.1, 8.1	Sun JavaTM™ System Application Server 8.1 2005Q1													
WebSphere Application Server 4.0, 5.x														
JavaTM™ 2 Platform Enterprise Edition 1.3/1.4														
Sun ONE Application Server 6.5, 7.0														
Sun JavaTM™ System Application Server 7 2004Q2														
Sun ONE Web Server 6.0														
J2EE Reference Implementation 1.3, 1.4														
JBoss Application Server 3.0, 3.2														
Tomcat Web Server 4.1.12														
OPTIONS	<pre>-h --help</pre> <pre>-v --version</pre> <pre>-u --ui</pre>	<p>displays the arguments for launching the MigrationTool.</p> <p>displays the version of the MigrationTool.</p> <p>invokes the tool in user interface mode.</p>												

## asmigrate(1m)

-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 the following: <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>■ wl81: WebLogic Application Server 8.1</li><li>■ as65: Sun ONE Application Server 6.5</li><li>■ as70: Sun ONE Application Server 7.0</li><li>■ ws40: WebSphere Application Server 4.0</li><li>■ ws50: WebSphere Application Server 5.x</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. Use sjs80PE as the target server for Sun Java System Application Server 8.1 2005Q1.
-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 sun-cmp-mapping.xml file. Instead, introduces the option argument into the sun-ejb-jar.xml 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></ul>



asmigrate(1m)

	<ul style="list-style-type: none"><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: <ul style="list-style-type: none"><li>■ all-files: if specified and set to true (default), migrates all types of files.</li><li>■ html-files: if specified and set to true (default), migrates HTML files.</li><li>■ java-files: if specified and set to true (default), migrates Java files.</li><li>■ jsp-files: if specified and set to true (default), migrates JSP type files.</li><li>■ xml-files: if specified and set to true (default), migrates all XML type files.</li><li>■ archive-files: if specified and set to true (default), migrates jar/ear/war/rar file types.</li></ul>
-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.

asmigrate(1m)

## EXAMPLES

### EXAMPLE 1 Using asmigrate

This example shows how to migrate the source code for a Websphere 4.0 application to Sun Java System Application Server 8.1 Platform Edition 2005Q1 using the command line options. The output directory for the migrated code is /tmp/ws\_out. The location of the source code is in directory, /d1/asmt/examples/websphere\_4\_0/PeopleDB/src.

```
asmigrate -c -T sjs80PE -S ws40 -t /tmp/ws_out -s  
/d1/asmt/examples/websphere_4_0/PeopleDB/src
```

This example shows how to migrate a Websphere 4.0 application archive to Sun Java System Application Server 8.1 Platform Edition 2005Q1.

```
asmigrate -c -T sjs80PE -S ws40 -t /tmp/ws_out  
/d1/asmt/examples/websphere_4_0/PeopleDB/WA  
SDeployed/PeopleDBEnEar.ear
```

This example shows how to migrate source code from Weblogic 6.1 application to Sun Java System Application Server 8 Platform Edition 2004Q4. Only Java files are designated to be migrated. CMP 1.1 beans will be migrated to CMP 2.0 beans and conflicting CMP related accessors will be overwritten.

```
asmigrate -c -T sjs80PE -S wl61 -t /tmp/ws_out -s  
/d1/asmt_headstrong/asmt/examples/weblogic_6_x/  
iBank -f java-files=true -m overwrite-conflicting-accessors=true
```

This example shows how to start the migration tool UI.

```
asmigrate -u
```

## SEE ALSO

[asupgrade\(1M\)](#)

NAME	asupgrade – migrates the configuration of a previously installed Sun Java System Application Server
SYNOPSIS	<b>asupgrade</b> [--console ] [--version ] [--help ] [--source <i>applicationserver_7.x/8.x_installation</i> ] [--target <i>applicationserver_8.1_installation</i> ] --adminuser <i>admin_user</i> [--adminpassword <i>admin_password</i> ] [--masterpassword <i>changeit</i> ] [--passwordfile <i>path_to_password_file</i> ] [--domain <i>domain_name</i> ] [--nsspwdfile <i>NSS_password_filepath</i> ] [--targetnsspwdfile <i>target_NSS_password_filepath</i> ] [--jkspwdfile <i>JKS_password_filepath</i> ] [--capwdfile <i>CA_password_filepath</i> ] [--clinstancefile <i>file1</i> [, <i>file2</i> , <i>file3</i> , ... <i>filen</i> ]]
DESCRIPTION	<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 8.1 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 also beyond the scope of the asupgrade command.</p> <p>Only those instances that do not use 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 uninstaller to remove the previous version of the application server.</p> <p>Application archives (EAR files) and component archives (JAR, WAR, and RAR files) that are deployed in the Application Server 7.x/8.0 environment do not require any modification to run on Application Server 8.1. Applications and components that are deployed in the source server are deployed on the target server during the upgrade. Applications that do not deploy successfully on the target server must be migrated using the Migration Tool or <code>asmigrate</code> command, then redeployed manually.</p> <p>Specify the source and target directories for the upgrade.</p> <p>If the upgrade includes certificates, 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 PE (JSSE), the migration keys and certificates are converted to the</p>

## asupgrade(1)

new format. Only one certificate database password per domain is supported. If multiple certificate database passwords are used in a single domain, all of the passwords must be made the same before starting the upgrade. The passwords can be reset after the upgrade has been completed.

If the upgrade includes clusters, specify one or more cluster files. Upon successful upgrade, an upgrade report is generated listing successfully migrated items along with a list of the items that could not be migrated.

If you issue the `asupgrade` command with no options, the Upgrade Tool GUI will be displayed. If the `asupgrade` command is used in command-line mode and all of the required information is not supplied, an interviewer will request information for any required options that were omitted.

OPTIONS	<code>-c --console</code>	Launches the upgrade command line utility.
	<code>-V --version</code>	The version of the Upgrade Tool.
	<code>-h --help</code>	Displays the arguments for launching the UpgradeTool.
	<code>-s --source</code>	The installation directory for Sun Java System Application Server 7.x/8.x installation that will be upgraded.
	<code>-t --target</code>	The installation directory for Sun Java System Application Server 8.1.
	<code>-a --adminuser</code>	The username of the administrator.
	<code>-w --adminpassword</code>	The password for the adminuser. Although this option can be used, the recommended way to transmit passwords is by using the <code>--passwordfile</code> option.
	<code>-m --masterpassword</code>	The master password that is created during installation. The default value is <code>changeit</code> . Although this option can be used, the recommended way to transmit passwords is by using the <code>--passwordfile</code> option.
	<code>-f --passwordfile</code>	The path to the file that contains the <code>adminpassword</code> and <code>masterpassword</code> . Content of this file should be in the following format: <i>AS_ADMIN_ADMINPASSWORD=adminpassword</i> <i>AS_ADMIN_MASTERPASSWORD=masterpassword</i>
	<code>-d --domain</code>	The domain name for the migrated certificates.
	<code>-n --nsspwdfile</code>	The path to the NSS password file.
	<code>-e --targetnsspwdfile</code>	The path to the target NSS password file.
	<code>-j --jkspwdfile</code>	The path to the JKS password file.
	<code>-p --capwdfile</code>	The path to the CA certificate password file.

`-i --clinstancefile`      The path to the cluster file. The default filename is `$AS_INSTALL/conf/clinstance.conf`.

## EXAMPLES

### EXAMPLE 1 Upgrading an Application Server 7 Installation to Application Server 8.1 with Prompts for Certificate Migration

This example shows how to upgrade a Sun Java System Application Server 7 installation to Sun Java System Application Server 8.1. You will be prompted to migrate certificates. If you reply no, then no certificates will be migrated.

```
example% asupgrade --adminuser admin --passwordfile password.txt
--source /home/sunas7 --target /home/sjsas8.1
```

### EXAMPLE 2 Upgrading an Application Server 7.1 EE Installation with Clusters and NSS Certificates to Application Server 8.1 EE

This example shows how to upgrade a Sun Java System Application Server 7.1 EE installation with a cluster to Sun Java System Application Server 8.1 EE. NSS certificates will be migrated, as will the `clinstance.conf` cluster file.

```
example% asupgrade --adminuser admin
--passwordfile password.txt
--source /home/sjsas7.1 --target /home/sjsas8.1
--domain domain1 --nsspwdfile /home/sjsas7.1/nsspassword.txt
--targetnsspwdfile /home/sjsas8.1/nsspassword.txt
--clinstancefile /home/sjsas7.1/config/clinstance.conf
```

After the upgrade, node agents for all remote instances must be created and started on their respective host systems.

### EXAMPLE 3 Upgrading an Application Server 7.0 PE Installation with NSS Certificates to Application Server 8.1 PE

This example shows how to upgrade a Sun Java System Application Server 7.0 PE installation to Sun Java System Application Server 8.1 PE. The NSS certificates from the 7.0 PE source server will be converted to JKS and CA certificates in the 8.1 PE target server.

```
example% asupgrade --adminuser admin
--passwordfile password.txt
--source /home/sjsas7.0 --target /home/sjsas8.1
--domain domain1 --nsspwdfile /home/sjsas7.0/nsspassword.txt
--jkspwdfile /home/sjsas7.0/jkspassword.txt
--capwdfile /home/sjsas7.0/capassword.txt
```

### EXAMPLE 4 Upgrading an Application Server 8.0 PE Installation with JKS and CA Certificates to Application Server 8.1 PE

This example shows how to upgrade a Sun Java System Application Server 8.0 PE installation to Sun Java System Application Server 8.1 PE. JKS and CA certificates will be migrated.

asupgrade(1)

**EXAMPLE 4** Upgrading an Application Server 8.0 PE Installation with JKS and CA Certificates to Application Server 8.1 PE *(Continued)*

```
example% asupgrade --adminuser admin
--passwordfile password.txt
--source /home/sjsas8.0 --target /home/sjsas8.1
--domain domain1 --jkspwdfilename /home/sjsas8.0/jkspassword.txt
--capwdfilename /home/sjsas8.1/capassword.txt
```

**EXIT STATUS**

0	command executed successfully
1	error in executing the command

**SEE ALSO** [asmigrate\(1M\)](#)

<b>NAME</b>	backup-domain – performs a backup on the domain	
<b>SYNOPSIS</b>	<b>backup-domain</b> [--domainindir <i>domain_directory</i> ] [--description <i>description</i> ] [--terse= <i>false</i> ] [--verbose= <i>false</i> ] [ <i>domain_name</i> ]	
<b>DESCRIPTION</b>	The backup-domain command backs up files under the named domain. This command is supported in local mode only.	
<b>OPTIONS</b>	--domainindir	This option specifies the parent directory of the domain upon which the command will operate. The default is install_dir/domains.
	--description	A description can contain any string to help identify the particular backup. The description is displayed as part of the information for any backup.
	-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.
	-t --verbose	Indicates that output data is displayed with detailed information. Default is false.
<b>OPERANDS</b>	<i>domain_name</i>	This is the name of the domain to be backed up. If the domain is not specified and only one domain exists, it will be used automatically.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using backup-domain asadmin>backup-domain --domainindir directory1 domain1 The command executed successfully. Where: domain1 is the domain name.	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	restore-domain(1), list-backups(1)	

## capture-schema(1m)

NAME	capture-schema – stores the database metadata (schema) in a file for use in mapping and execution														
SYNOPSIS	<pre><b>capture-schema</b> -username <i>name</i> -password <i>password</i> -dburl <i>url</i>                     -driver <i>jdbc_driver_classname</i> [-schemaname <i>schemaname</i>]                     [-table <i>tablename</i>] -out <i>filename</i></pre>														
DESCRIPTION	<p>Stores the database metadata (schema) in a file.</p> <p>Run capture-schema as the same database user that owns the table(s), and use that same username with the -username option (and -schemaname, if required).</p> <p>When running capture-schema against an Oracle database, you should grant the database user running the capture-schema command the ANALYZE ANY TABLE privilege.</p> <p>You can also use the Sun Java System Studio IDE to capture the database schema.</p>														
OPTIONS	<table> <tr> <td>-username</td><td>user name for authenticating access to a database.</td></tr> <tr> <td>-password</td><td>password for accessing the selected database.</td></tr> <tr> <td>-dburl</td><td>JDBC URL required by the driver for accessing a database.</td></tr> <tr> <td>-driver</td><td>JDBC driver classname in your CLASSPATH.</td></tr> <tr> <td>-schemaname</td><td> <p>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.</p> <p><i>Specifying this parameter is highly recommended.</i> Without this option, 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 when mapping CMP fields to tables.</p> <p>The specified schema name must be uppercase.</p> </td></tr> <tr> <td>-table</td><td> <p>name of a table; multiple table names can be specified. If no table is specified, all the tables in the database or named schema are captured.</p> <p>The specified table name or names are case sensitive. Be sure to match the case of the previously created table names.</p> </td></tr> <tr> <td>-out</td><td>name of the output file. This option is required. If the specified output file does not contain the .dbschema suffix, it will be appended to the filename.</td></tr> </table>	-username	user name for authenticating access to a database.	-password	password for accessing the selected database.	-dburl	JDBC URL required by the driver for accessing a database.	-driver	JDBC driver classname in your CLASSPATH.	-schemaname	<p>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.</p> <p><i>Specifying this parameter is highly recommended.</i> Without this option, 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 when mapping CMP fields to tables.</p> <p>The specified schema name must be uppercase.</p>	-table	<p>name of a table; multiple table names can be specified. If no table is specified, all the tables in the database or named schema are captured.</p> <p>The specified table name or names are case sensitive. Be sure to match the case of the previously created table names.</p>	-out	name of the output file. This option is required. If the specified output file does not contain the .dbschema suffix, it will be appended to the filename.
-username	user name for authenticating access to a database.														
-password	password for accessing the selected database.														
-dburl	JDBC URL required by the driver for accessing a database.														
-driver	JDBC driver classname in your CLASSPATH.														
-schemaname	<p>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.</p> <p><i>Specifying this parameter is highly recommended.</i> Without this option, 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 when mapping CMP fields to tables.</p> <p>The specified schema name must be uppercase.</p>														
-table	<p>name of a table; multiple table names can be specified. If no table is specified, all the tables in the database or named schema are captured.</p> <p>The specified table name or names are case sensitive. Be sure to match the case of the previously created table names.</p>														
-out	name of the output file. This option is required. If the specified output file does not contain the .dbschema suffix, it will be appended to the filename.														
EXAMPLES	<p><b>EXAMPLE 1</b> Using capture-schema</p> <pre><b>capture-schema</b> -username cantiflas -password enigma                   -dburl jdbc:oracle:thin:@sadbutter:1521:ora817 -driver oracle.jdbc.driver.OracleDriver                   -schemaname CANTIFLAS -out cantiflas.dbschema</pre>														



capture-schema(1m)

**SEE ALSO** [asadmin\(1M\)](#)

## change-master-password(1)

<b>NAME</b>	change-master-password – changes the master password	
<b>SYNOPSIS</b>	<b>change-master-password</b> [--domainindir <i>domain_path</i>   --agentdir <i>node-agent_path</i> ] [--savemasterpassword=false] [ <i>domain_name</i>   <i>node_agent_name</i> ]	
<b>DESCRIPTION</b>	This local command is used to modify the master password. Change-master-password is interactive in that the user is prompted for the old master password, as well as the new master password. This command will not work unless the server is stopped. In a distributed Enterprise Edition environment, this command must run on each machine in the domain, with the Node Agent stopped.	
<b>OPTIONS</b>	--domainindir          --agentdir          --savemasterpassword	This option specifies the directory used for this operation. By default, the domainindir is \$AS_DEF_DOMAINS_PATH, which is an environment variable defined in asenv.bat/conf. Both the domainindir and the agentdir options should not be passed together; use one or the other.  Like a DAS, each Node Agent resides in a top level directory named <agentdir>/<nodeagent_name>. If the agentdir is not specified, then \$AS_DEF_DOMAINS_PATH/./nodeagents is used. Both the domainindir and the agentdir options should not be passed together; use one or the other. This option is supported in Enterprise Edition only.  This option indicates whether the master password should be written to the file system. This is necessary so that start-domain can start the server without having to prompt the user. WARNING: saving the master password on disk is extremely dangerous and should be avoided.  NOTE: if savemasterpassword is not set, the master password file, if it exists, will be deleted.
<b>OPERANDS</b>	<i>domain_name</i>          <i>node-agent_name</i>	This is the domain name whose password is to be changed. If there is only a single domain, this is optional. This option can be used on either the Platform Edition or the Enterprise Edition.  This is the name of the node agent whose password is to be changed. If there is only a single domain, this is optional. This option can be used on Enterprise Edition only.

**EXAMPLES**    **EXAMPLE 1** Using change-master-password

```
asadmin> change-master-password domain44ps
```

Master password has been changed

**EXIT STATUS**

0

command executed successfully

1

error in executing the command

**SEE ALSO**

[delete-password-alias\(1\)](#), [list-password-aliases\(1\)](#),  
[update-password-alias\(1\)](#)

## create-acl(1)

NAME	create-acl – adds a new access control list file for the named instance
SYNOPSIS	<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>
DESCRIPTION	Gets the access control lists associated with the named server instance.
OPTIONS	<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>
OPERANDS	<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.
EXAMPLES	<p><b>EXAMPLE 1</b> Using create-acl</p> <pre>asadmin&gt; create-acl --user admin --password adminadmin --host fuyako --port 7070 --instance server1</pre> <p>Created ACL with id=sampleACL</p> <p>Where: sampleACL is the name of the ACL created.</p>
EXIT STATUS	<pre>0   command executed successfully 1   error in executing the command</pre>
INTERFACE EQUIVALENT SEE ALSO	<p>Access Control List page</p> <p><a href="#">delete-acl(1)</a>, <a href="#">list-acl(1)</a></p>

## create-admin-object(1)

NAME	create-admin-object – adds the administered object with the specified JNDI name														
SYNOPSIS	<pre><b>create-admin-object</b> --user <i>admin_user</i> [--passwordfile <i>filename</i>]     [--host <i>host_name</i>] [--port <i>port_number</i>] [--secure -s]     [--terse=false] [--echo=false] [--interactive=true] [--help]     [--target <i>target</i>]     --restype <i>admin_object_type</i> --raname <i>resource_adapter_name</i> [--description <i>text</i>]     [--property <i>name=value[:name=value]*</i>] <i>jndi-name</i></pre>														
DESCRIPTION	This commands creates the administered object that has a specified jndi name.														
OPTIONS	<table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td>-s --secure</td><td>If set to 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> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	-s --secure	If set to 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.
-u --user	The authorized domain application server administrative username.														
-w --password	The --password option is deprecated. Use --passwordfile instead.														
--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.														
-H --host	The machine name where the domain application server is running. The default value is localhost.														
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.														
-s --secure	If set to 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.														

## create-admin-object(1)

	<code>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
	<code>--target</code>	This is the name of the target upon which the command is operating. The valid targets for this command are instance, cluster, 'domain,' and 'server.' Server is the default option. This command is used by the Enterprise Edition only.
	<code>--restype</code>	This option is used to administer the object resource types, as defined by the resource adapter in the ra.xml file.
	<code>--raname</code>	This is the name of the resource adapter associated with this object.
	<code>- --description</code>	This option is the text description of the administered object.
	<code>--property</code>	This option describes the "name/values" pairs for configuring the resource.
<b>OPERANDS</b>	<i>jndi_name</i>	This is the JNDI name of the administered object to be created.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using create-admin-object</p> <p>The <code>javax.jms.Queue</code> resource type is obtained from the <code>ra.xml</code> file. The <code>jmsrar.rar</code> must be deployed prior to executing this command.</p> <pre>asadmin&gt; create-admin-object --user admin1 --password adminadmin1 --restype javax.jms.Queue --raname jmsra --description "sample administered object" --property Name=sample_jmsqueue --target instance1 jms/samplequeue Command create-admin-object executed successfully</pre>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">delete-admin-object(1)</a> , <a href="#">list-admin-objects(1)</a>	

NAME	create-audit-module – adds an audit-module
SYNOPSIS	<b>create-audit-module</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--target <i>target_name</i> ] [--classname <i>realm_class</i> ] [--property (name=value) [:name=value]*] [ <i>audit_module_name</i> ]
DESCRIPTION	Adds the named audit module for the plugin module that implements the audit capabilities. This command is supported in remote mode only.
OPTIONS	<div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>--passwordfile</div> <div>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </div> </div> <div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> </div> <div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> </div> <div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> </div> <div> <div>-t --terse</div> <div>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.</div> </div> <div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div> </div>

## create-audit-module(1)

	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
	--target	In Enterprise Edition, specifies the target on which you are creating the audit module. Valid values are <ul style="list-style-type: none"> <li>■ <i>server</i>, which creates the listener for the default server instance <i>server</i> and is the default value</li> <li>■ <i>configuration_name</i>, which creates the listener for the named configuration</li> <li>■ <i>cluster_name</i>, which creates the listener for every server instance in the cluster</li> <li>■ <i>instance_name</i>, which creates the listener for a particular server instance</li> </ul>
	--classname	Java class which implements this realm.
	--property	optional attributes name/value pairs of provider implementation specific attributes.
OPERANDS	<i>audit_module_name</i>	name of this audit module.
EXAMPLES	<b>EXAMPLE 1</b> Using create-audit-module <pre>asadmin&gt; create-audit-module --user admin1 --passwordfile password.txt --host pigeon --port 5001 --classname com.sun.appserv.auditmodule --property defaultuser=admin:Password=admin sampleAuditModule</pre> Command create-audit-module executed successfully	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">delete-audit-module(1)</a> , <a href="#">list-audit-modules(1)</a>	



NAME	create-auth-realm – adds the new authenticated realm
SYNOPSIS	<b>create-auth-realm</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--target <i>target_name</i> ] [--classname <i>realm_class</i> ] [--isdefault=true] [--property (name=value) [:name=value] *] <i>auth_realm_name</i>
DESCRIPTION	Adds the named authorized realm. This command is supported in remote mode only.
OPTIONS	<div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>--passwordfile</div> <div>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </div> </div> <div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> </div> <div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> </div> <div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> </div> <div> <div>-t --terse</div> <div>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.</div> </div> <div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div> </div>

## create-auth-realm(1)

	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
	--target	In Enterprise Edition, specifies the target on which you are creating the realm. Valid values are <ul style="list-style-type: none"> <li>■ <i>server</i>, which creates the listener for the default server instance <i>server</i> and is the default value</li> <li>■ <i>configuration_name</i>, which creates the listener for the named configuration</li> <li>■ <i>cluster_name</i>, which creates the listener for every server instance in the cluster</li> <li>■ <i>instance_name</i>, which creates the listener for a particular server instance</li> </ul>
	--classname	Java class which implements this realm.
	--property	optional attributes name/value pairs of provider implementation specific attributes.
OPERANDS	<i>auth_realm_name</i>	name of this realm.
EXAMPLES	<p><b>EXAMPLE 1</b> Using create-auth-realm</p> <pre>asadmin&gt; create-auth-realm --user admin1 --passwordfile password.txt --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>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">delete-auth-realm(1)</a> , <a href="#">list-auth-realms(1)</a>	

## create-connection-group(1)

NAME	create-connection—group – creates a new connection group with the named group ID
SYNOPSIS	<pre> <b>create-connection-group</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> --httplistener <i>http_listener_ID</i>   --address <i>address</i> --defaultvs <i>virtual_server</i> --servername <i>server_name</i>   <i>connection_group_ID</i> </pre>
DESCRIPTION	Creates a new connection group with the named group ID.
OPTIONS	<p>--user identifies the user name associated with the named instance.</p> <p>--password identifies the password associated with the user name.</p> <p>--host identifies the host name for the machine.</p> <p>--port identifies the administrator port number associated with the hostname.</p> <p>--instance identifies the name of the instance associated with the JVM option to be created.</p> <p>--httplistener a unique identifier for the HTTP listener.</p> <p>--address the IP address of the listen socket. Can be in dotted-pair or IPv6 notation.</p> <p>--defaultvs the ID attribute of the default virtual server for this particular connection group.</p> <p>--servername identifies, in the hostname section, the URLs the server sends to the client. This name should be the alias name if your server uses an alias. If you append a colon (:) and port number, that port will be used in the URLs the server sends to the client.</p> <p><i>connection_group_ID</i> a unique identifier for the connection group.</p>
EXAMPLES	<pre> asadmin% <b>create-connection-group</b> </pre>
SEE ALSO	<a href="#">delete-connection-group(1)</a> , <a href="#">list-connection-groups(1)</a>

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

<b>NAME</b>	create-connector-connection-pool – adds a connecton pool with the specified connection pool name												
<b>SYNOPSIS</b>	<pre> <b>create-connector-connection-pool</b> --user <i>admin_user</i>     [--passwordfile <i>filename</i>] [--host <i>host_name</i>] [--port <i>port_number</i>]     [--secure -s] [--terse=<i>false</i>] [--echo=<i>false</i>] [--interactive=<i>true</i>]     [--help] [--steadypoolsize 8] [--maxpoolsize 32]     [--maxwait 60000] [--poolresize 2] [--idletimeout 300]     [--failconnection=<i>false</i>] --raname <i>resource_adapter_name</i>     --connectiondefinition <i>connection_definition_name</i>     [--transactionsupport <i>transaction_support</i>] [--description <i>text</i>]     [--property (<i>name=value</i>) [:<i>name=value</i>]*] <i>connector_connection_pool_name</i> </pre>												
<b>DESCRIPTION</b>	Adds a new connector connection pool with the specified connection pool name. This command is supported in remote mode only.												
<b>OPTIONS</b>	<table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td>-s --secure</td><td>If set to true, uses SSL/TLS to communicate with the domain application server.</td></tr> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	-s --secure	If set to true, uses SSL/TLS to communicate with the domain application server.
-u --user	The authorized domain application server administrative username.												
-w --password	The --password option is deprecated. Use --passwordfile instead.												
--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.												
-H --host	The machine name where the domain application server is running. The default value is localhost.												
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.												
-s --secure	If set to true, uses SSL/TLS to communicate with the domain application server.												

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

<code>-t --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>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
<code>-h --help</code>	Displays the help text for the command.
<code>--target</code>	The target option is deprecated.
<code>--raname</code>	The name of the resource adapter.
<code>--connectiondefinition</code>	The name of the connection definition.
<code>--steadypoolsize</code>	The minimum and initial number of connections maintained in the pool. The default value is 8.
<code>--maxpoolsize</code>	The maximum number of connections that can be created to satisfy client requests. The default value is 32.
<code>--maxwaittime</code>	The amount of time, in milliseconds, that a caller must wait before a connection is created, if a connection is not available. If set to 0, the caller is blocked indefinitely until a resource is available or until an error occurs. The default value is 60000.
<code>--poolresize</code>	The number of connections to be destroyed if the existing number of connections is above the steady-pool-size (subject to the limit specified in the maxpoolsize option). Possible values are from 0 to MAX_INTEGER. The default value is 2.
<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. The default value is 300.
<code>--failconnection</code>	If set to true, all connections in the pool are closed if a single validation check fails. This parameter is mandatory if the is-connection-validation-required is set to true. Legal values are on, off, yes, no, 1, 0, true or false. The default value is false.
<code>--transactionsupport</code>	Indicates the level of transaction support that this pool will have. Possible values are XATransaction, LocalTransaction and NoTransaction. This attribute can support the resource adapter's transaction

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

		support attribute when the resource adapter's transaction support attribute is lower than or equal to but not higher than. The default value is true.
	--description	Text providing descriptive details about the connector connection pool.
	--property	optional attribute name/value pairs for configuring the resource.
OPERANDS	<i>connector_connection_pool_name</i> the name of the connection pool name to be created.	
EXAMPLES	<b>EXAMPLE 1</b> Using the create-connector-connection-pool command <pre>asadmin&gt; create-connector-connection-pool --passwordfile passwordfile --steadypoolsize 20 --maxpoolsize 100 --poolresize 2 --maxwait 60000 --raname jmsra --connectiondefinition javax.jms.QueueConnectionFactory jms/qConnPool Command create-connector-connection-pool executed successfully</pre> <p>Where jms/qConnPool is the name of the new connector connection pool.</p>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">delete-connector-connection-pool(1)</a> , <a href="#">list-connector-connection-pools(1)</a>	

NAME	create-connector-resource – registers the connector resource with the specified JNDI name
SYNOPSIS	<b>create-connector-resource</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [---target <i>target</i> ] --poolname <i>connectorConnectionPoolName</i> [--enabled=true] [--description <i>text</i> ] <i>jndi_name</i>
DESCRIPTION	This command registers the connector resource with the JNDI name, which is specified by the <i>jndi_name</i> operand.
OPTIONS	<div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>--passwordfile</div> <div>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </div> </div> <div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> </div> <div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> </div> <div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> </div> <div> <div>-t --terse</div> <div>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.</div> </div>

## create-connector-resource(1)

	<code>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
	<code>--target</code>	valid in Enterprise Edition only, specifies the ending location of the connector resources. Valid values are "server," "domain," cluster, instance. The default is server.
	<code>--poolname</code>	The name of the connection pool. When two or more resource elements point to the same connection pool element, they use the same pool connections at runtime.
	<code>--enabled</code>	This option determines whether the resource is enabled at runtime. The default value is true.
	<code>--description</code>	Text providing descriptive details about the connector resource.
<b>OPERANDS</b>	<i>jndi_name</i>	the JNDI name of this connector resource.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the create-connector-resource command</p> <pre>asadmin&gt; create-connector-resource --target server --poolname jms/qConnPool --description "creating sample connector resource" jms/qConnFactory Command create-connector-resource executed successfully</pre> <p>Where jms/qConnFactory is the sample connector resource that is created.</p>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">delete-connector-resource(1)</a> , <a href="#">list-connector-resources(1)</a>	



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

NAME	create-connector-security-map – creates or modifies a security map for the specified connector connection pool						
SYNOPSIS	<pre><b>create-connector-security-map</b> --user <i>admin_user</i> [<i>--passwordfile filename</i>] [<i>--host host_name</i>] [<i>--port port_number</i>] [<i>--secure -s</i>] [<i>--terse=false</i>] [<i>--echo=false</i>] [<i>--interactive=true</i>] [<i>--help</i>] --poolname <i>connector_connection_pool_name</i> [<i>--principals principal_name1[, principal_name2]*</i>   <i>--usergroups user_group1[, user_group2]</i>] --mappedusername <i>username security_map_name</i></pre>						
DESCRIPTION	<p>Use this command to create or modify a security map for the specified connector connection pool. If the security map is not present, one is created. Also, use this command to map the caller identity of the application (principal or user group) to a suitable EIS principal in container-managed transaction-based scenarios. One or more named security maps may be associated with a connector connection pool. The connector security map configuration supports the use of the wild card asterisk (*) to indicate all users or all user groups.</p> <p>For this command to succeed, you must have first created a connector connection pool using the <code>create-connector-connection-pool</code> command.</p> <p>The enterprise information system (EIS) is any system that holds the information. It can be a mainframe, a messaging system, a database system, or an application.</p> <p>This command is supported in remote mode only.</p>						
OPTIONS	<p>If an option has a short option name, then the short option precedes the long option name. Short options have one dash whereas long options have two dashes.</p> <table> <tr> <td><code>-u --user</code></td><td>The authorized domain application server administrative username.</td></tr> <tr> <td><code>-w --password</code></td><td>The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.</td></tr> <tr> <td><code>--passwordfile</code></td><td>This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=<i>password</i></code>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code>, <code>AS_ADMIN_USERPASSWORD</code>,</td></tr> </table>	<code>-u --user</code>	The authorized domain application server administrative username.	<code>-w --password</code>	The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.	<code>--passwordfile</code>	This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=<i>password</i></code> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code> , <code>AS_ADMIN_USERPASSWORD</code> ,
<code>-u --user</code>	The authorized domain application server administrative username.						
<code>-w --password</code>	The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.						
<code>--passwordfile</code>	This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=<i>password</i></code> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code> , <code>AS_ADMIN_USERPASSWORD</code> ,						

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

	AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASSPASSWORD, and so on.
-H --host	The machine name where the domain application server is running. The default value is localhost.
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
-s --secure	If set to 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.
-h --help	Displays the help text for the command.
--target	The -target option is deprecated in this release.
--poolname	This property specifies the name of the connector connection pool to which the security map that is to be updated or created belongs.
--principals	This property specifies a comma-separated list of application-specific principals. Use either the -principals or -usergroups options, but not both.
--usergroups	This property specifies a comma-separated list of application—specific user groups. Use either the -principals or -usergroups options, but not both.
--mappedusername	This property specifies the EIS username.
--mappedpassword	The --mappedpassword option is deprecated. Use --passwordfile pointing to a file that contains an entry in the following format: AS_ADMIN_MAPPEDPASSWORD= <i>mapped-password</i> . If not specified using the passwordfile option, the user will be prompted for this password by the asadmin command-line tool.
<b>OPERANDS</b>	
<i>security_map_name</i>	name of the security map to be created.

EXAMPLES	<p><b>EXAMPLE 1</b> Using create-connector-security-map</p> <p>It is assumed that the connector pool has already been created using the create-connector-pool command.</p> <pre>asadmin&gt; create-connector-security-map --user admin --passwordfile pwd_file --poolname connector-pool1 --principals principal1, principal2 --mappedusername backend-username securityMap1</pre> <p>Command create-connector-security-map executed successfully</p>
EXIT STATUS	<p>0 command executed successfully</p> <p>1 error in executing the command</p>
SEE ALSO	<p><a href="#">delete-connector-security-map(1)</a>, <a href="#">list-connector-security-maps(1)</a>, <a href="#">update-connector-security-map(1)</a></p>

## create-custom-resource(1)

NAME	create-custom-resource – creates a custom resource
SYNOPSIS	<b>create-custom-resource</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--target <i>target</i> ] --restype <i>type</i> --factoryclassname <i>classname</i> [--enabled=true] --description <i>text</i> [--property ( <i>name=value</i> ) [: <i>name=value</i> ]*] <i>jndi_name</i>
DESCRIPTION	The create-custom-resource command creates a custom resource. This command is supported in remote mode only.
OPTIONS	<div>-u --user</div> <div>The authorized domain application server administrative username.</div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> <div>--passwordfile</div> <div>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> <div>-t --terse</div> <div>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.</div>

	<code>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
	<code>--target</code>	in Enterprise Edition, specifies the target to which you are deploying. Valid values are <ul style="list-style-type: none"> <li>■ <code>server</code>, which deploys the component to the default server instance <code>server</code> and is the default value</li> <li>■ <code>domain</code>, which deploys the component to the domain.</li> <li>■ <code>cluster_name</code>, which deploys the component to every server instance in the cluster.</li> <li>■ <code>instance_name</code>, which deploys the component to a particular sever instance.</li> </ul>
	<code>--resourcetype</code>	The <code>--resourcetype</code> option is deprecated. Use <code>--restype</code> instead.
	<code>--restype</code>	The type of custom resource to be created.
	<code>--factoryclass</code>	The class that creates the custom resource.
	<code>--enabled</code>	Determines whether the custom resource is enable at runtime. The default value is true.
	<code>--description</code>	Text providing descriptive details about the custom resource.
	<code>--property</code>	optional attribute name/value pairs for configuring the resource.
<b>OPERANDS</b>	<i>jndi_name</i>	the JNDI name of this resource.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the create-custom-resource command</p> <pre>asadmin&gt; create-custom-resource [--target plum] [--restype javax.sql.datasource] admin-gui/admin/src</pre> <p>Command create-custom-resource executed correctly.</p> <p>Where asadmin is the command prompt and jndi_name is the name of the custom resource to be created.</p>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">delete-custom-resource(1)</a> , <a href="#">list-custom-resources(1)</a>	

## create-domain(1)

NAME	create-domain – creates a domain with the given name														
SYNOPSIS	<pre><b>create-domain</b> [--domaindir <i>domain_directory</i>/domains]                 --adminport <i>port_number</i> --admin.jmxport <i>port_number</i>                 --adminuser <i>admin_user</i> [--passwordfile <i>passwordfile</i>] [--terse=<i>false</i>]                 [--echo=<i>false</i>] [--interactive=<i>true</i>] [--instanceport <i>port_number</i>]                 [--domainproperties (<i>name=value</i>) [:<i>name=value</i>] *]                 [--savemasterpassword=<i>false</i>] <i>domain_name</i></pre>														
DESCRIPTION	<p>Use the create-domain command to create a domain containing an instance that can administer itself. By creating a domain, an administration server is created in a directory named as the domain name. If you create a domain in a non-default directory, the domain will not be automatically shutdown during uninstallation. The --adminpassword option has been deprecated, use the --passwordfile option instead. To maintain high security, omit the --passwordfile from the command line and allow the system to prompt you for these options.</p> <p>This command is supported in local mode only.</p>														
OPTIONS	<table> <tr> <td>--domaindir</td><td>The directory where the domain is to be created. If specified, the path must be accessible in the filesystem. If not specified, the domain is created in the default domain directory.</td></tr> <tr> <td>--adminport</td><td>The administrative instance port number.</td></tr> <tr> <td>--admin.jmxport</td><td>Specifies the port on which the jmx connector is initialized. The valid values are 1-65535.</td></tr> <tr> <td>--adminuser</td><td>The username associated with the administrative instance.</td></tr> <tr> <td>-W --passwordfile</td><td>The file containing the domain application server password associated with the administrative instance. The password is defined in the following form: AS_ADMIN_PASSWORD=<i>password</i>. Where <i>password</i> is the actual administrator password for the domain. This file can also contain the AS_ADMIN_ADMINPASSWORD and the AS_MASTERPASSWORD. The syntax for each is the same as the syntax for AS_ADMIN_PASSWORD. Using this option on the command line can be insecure, since the password is stored in clear text. This file, however, can be protected by file system permissions.</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 to the standard output. Default is false.</td></tr> </table>	--domaindir	The directory where the domain is to be created. If specified, the path must be accessible in the filesystem. If not specified, the domain is created in the default domain directory.	--adminport	The administrative instance port number.	--admin.jmxport	Specifies the port on which the jmx connector is initialized. The valid values are 1-65535.	--adminuser	The username associated with the administrative instance.	-W --passwordfile	The file containing the domain application server password associated with the administrative instance. The password is defined in the following form: AS_ADMIN_PASSWORD= <i>password</i> . Where <i>password</i> is the actual administrator password for the domain. This file can also contain the AS_ADMIN_ADMINPASSWORD and the AS_MASTERPASSWORD. The syntax for each is the same as the syntax for AS_ADMIN_PASSWORD. Using this option on the command line can be insecure, since the password is stored in clear text. This file, however, can be protected by file system permissions.	-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 to the standard output. Default is false.
--domaindir	The directory where the domain is to be created. If specified, the path must be accessible in the filesystem. If not specified, the domain is created in the default domain directory.														
--adminport	The administrative instance port number.														
--admin.jmxport	Specifies the port on which the jmx connector is initialized. The valid values are 1-65535.														
--adminuser	The username associated with the administrative instance.														
-W --passwordfile	The file containing the domain application server password associated with the administrative instance. The password is defined in the following form: AS_ADMIN_PASSWORD= <i>password</i> . Where <i>password</i> is the actual administrator password for the domain. This file can also contain the AS_ADMIN_ADMINPASSWORD and the AS_MASTERPASSWORD. The syntax for each is the same as the syntax for AS_ADMIN_PASSWORD. Using this option on the command line can be insecure, since the password is stored in clear text. This file, however, can be protected by file system permissions.														
-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 to the standard output. Default is false.														

<code>-I --interactive</code>	If set to true (default), only the required options are prompted.
<code>--instanceport</code>	The port number listening to the HTTP request. The port number cannot be currently in use. If not specified, the default value is 8080.
<code>--domainproperties</code>	Setting the optional name/value pairs overrides the default values for the properties of the domain to be created. The list must be separated by the ":" character. The following properties are available:

Property	Definition
jms.port	This property specifies the port number for JMS. Valid value are 7676
orb.listener.port	This property specifies which ORB listener port for IIOP connections orb-listener-1 listens on.
http.ssl.port	This property specifies the port number for http-listener-2. Valid values are 1–65535. On UNIX, creating sockets that listen on ports 1–1024 requires superuser privileges.
orb.ssl.port	This property specifies which ORB listener port for IIOP connections the IIOP listener called SSL listens on.
orb.mutualauth.port	This property specifies which ORB listener port for IIOP connections the IIOP listener called SSL_MUTUALAUTH listens on.

<code>--savemasterpassword</code>	Setting this option to true allows the masterpassword to be written to the file system. It is best to create a masterpassword when creating a domain, because masterpassword is used by the <code>start-domain</code> command. For security purposes, the default setting should be false, because saving the masterpassword on the disk is an insecure practice,
-----------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## create-domain(1)

unless file system permissions are properly set. If masterpassword is saved, then `start-domain` will not prompt for it. Masterpassword gives an extra level of security to the environment.

**OPERANDS**     *domain\_name*     The name of the domain to be created.

**EXAMPLES**     **EXAMPLE 1** Using the create-domain command

```
asadmin> create-domain --domaindir /export/domains
--adminport 7070 --adminuser admin --instanceport 7071 sampleDomain
created domain sampleDomain successfully
```

Where: the sampleDomain domain is created in the /export/domains directory.

**EXIT STATUS**     0  
                     command executed successfully

1  
                     error in executing the command

**SEE ALSO**     [delete-domain\(1\)](#), [start-domain\(1\)](#), [stop-domain\(1\)](#), [list-domains\(1\)](#)



NAME	create-file-user – creates a new file user	
SYNOPSIS	<b>create-file-user</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--target <i>target</i> ] [--authrealmname <i>auth_realm_name</i> ] [--groups <i>user_groups[:user_groups]*</i> ] <i>user_name</i>	
DESCRIPTION	<p>Creates an entry in the 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 using the auth-realm name.</p> <p>This command is supported in remote mode only.</p>	
OPTIONS	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
	-H --host	The machine name where the domain application server is running. The default value is localhost.
	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	-s --secure	If set to true, uses SSL/TLS to communicate with the domain application server.

## create-file-user(1)

	-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.
	-h --help	Displays the help text for the command.
	--target	This is used for Enterprise Edition only. This is the name of the target on which the command operates. The valid targets are config, instance, cluster, or "server." By default, the target is the "Server."
	--groups	This is the group associated with this file user.
	--authrealmname	This is the file where the file users are stored.
<b>OPERANDS</b>	<i>user_name</i>	This is the name of file user to be created.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the create-file-user command</p> <p>It is assumed that an authority realm has already been created using the create-auth-realm command.</p> <pre>asadmin&gt; 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</pre> <p>Where: the sample_user is the file user created.</p>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">create-auth-realm(1)</a> <a href="#">delete-file-user(1)</a> , <a href="#">list-file-users(1)</a> , <a href="#">update-file-user(1)</a> , <a href="#">list-file-groups(1)</a>	

NAME	create-http-listener – adds a new HTTP listener socket	
SYNOPSIS	<b>create-http-listener</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--target <i>server</i> ] --listeneraddress <i>address</i> --listenerport <i>listener_port</i> --defaultvs <i>virtual_server</i> --servername <i>server_name</i> [--acceptorthreads <i>1</i> ] [--securityenabled=false] [--redirectport <i>redirect_port</i> ] [--xpowered=true] [--enabled=true] <i>listener_id</i>	
DESCRIPTION	The create-http-listener command creates an HTTP listener. This command is supported in remote mode only.	
OPTIONS	<div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>--passwordfile</div> <div>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </div> </div> <div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> </div> <div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> </div> <div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> </div>	

## create-http-listener(1)

<code>-t --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>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
<code>-h --help</code>	Displays the help text for the command.
<code>--target</code>	<p>In Enterprise Edition, specifies the target for which you are creating the HTTP listener. Valid values are</p> <ul style="list-style-type: none"><li>■ <code>server</code>, which creates the listener for the default server instance <code>server</code> and is the default value</li><li>■ <code>configuration_name</code>, which creates the listener for the named configuration</li><li>■ <code>cluster_name</code>, which creates the listener for every server instance in the cluster</li><li>■ <code>instance_name</code>, which creates the listener for a particular server instance</li></ul>
<code>--listeneraddress</code>	The IP address of the listener address (resolvable by DNS).
<code>--listenerport</code>	The 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.
<code>--defaultvs</code>	The ID attribute of the default virtual server for this listener.
<code>--servername</code>	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 port number are appended, that port will be used in URLs that the server sends to the client.
<code>--acceptorthreads</code>	The number of acceptor threads for the listen socket. The recommended value is the number of processors in the machine. The default value is 1.

	<code>--securityenabled</code>	If set to true, 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. The default value is false.
	<code>--redirectport</code>	Port number for redirects. If the HTTP listener is supporting non-SSL requests, and a request is received for which a matching security-constraint requires SSL transport, the Application Server will automatically redirect the request to this port number. This option is valid for Enterprise Edition only.
	<code>--xpowered</code>	If set to true, adds the X-Powered-By: Servlet/2.4 and X-Powered-By: JSP/2.0 headers to the appropriate responses. The Servlet 2.4 specification defines the X-Powered-By: Servlet/2.4 header, which containers may add to servlet-generated responses. Similarly, the JSP 2.0 specification defines the X-Powered-By: JSP/2.0 header, which containers may add to responses that use JSP technology. The goal of these headers is to aid in gathering statistical data about the use of Servlet and JSP technology.
	<code>--enabled</code>	If set to true, the listener is enabled at runtime.
<b>OPERANDS</b>	<i>listener_id</i>	The listener ID of the HTTP listener.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the create-http-listener command</p> <p>The following command creates an HTTP listener named <code>sampleListener</code> that uses a nondefault number of acceptor threads and is not enabled at runtime:</p> <pre>asadmin&gt; create-http-listener --user admin1 --passwordfile passwords.txt --host pigeon --port 5001 --listeneraddress 0.0.0.0 --listenerport 7272 --defaultvs server --servername pigeon.red.planet.com --acceptorthreads 100 --securityenabled=false --enabled=false sampleListener</pre> <p>Command <code>create-http-listener</code> executed successfully.</p>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">delete-http-listener(1)</a> , <a href="#">list-http-listeners(1)</a> , <a href="#">create-virtual-server(1)</a> , <a href="#">create-ssl(1)</a>	

## create-iiop-listener(1)

NAME	create-iiop-listener – adds an IIOP listener
SYNOPSIS	<b>create-iiop-listener</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--target <i>server</i> ] --listeneraddress <i>address</i> [--iiopport 1072] [--securityenabled=false] [--enabled=true] [--property ( <i>name=value</i> ) [: <i>name=value</i> ]*] <i>listener_id</i>
DESCRIPTION	The create-iiop-listener command creates an IIOP listener. This command is supported in remote mode only.
OPTIONS	<div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>--passwordfile</div> <div>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </div> </div> <div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> </div> <div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> </div> <div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> </div> <div> <div>-t --terse</div> <div>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.</div> </div>

		create-iiop-listener(1)
	-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.
	-h --help	Displays the help text for the command.
	--target	In Enterprise Edition, specifies the target for which you are creating the IIOP listener. Valid values are <ul style="list-style-type: none"> <li>■ <i>server</i>, which creates the listener for the default server instance <i>server</i> and is the default value</li> <li>■ <i>configuration_name</i>, which creates the listener for the named configuration</li> <li>■ <i>cluster_name</i>, which creates the listener for every server instance in the cluster</li> <li>■ <i>instance_name</i>, which creates the listener for a particular server instance</li> </ul>
	--listeneraddress	Either the IP address or the hostname (resolvable by DNS).
	--iiopport	The IIOP port number. The default value is 1072.
	--securityenabled	If set to true, the IIOP 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. The default value is false.
	--enabled	If set to true, the IIOP listener is enabled at runtime.
	--property	Optional attribute name/value pairs for configuring the IIOP listener.
OPERANDS	<i>listener_id</i>	A unique identifier for the IIOP listener to be created.
EXAMPLES	<b>EXAMPLE 1</b> Using the create-iiop-listener command  The following command creates an IIOP listener named <i>sample_iiop_listener</i> :  <pre>asadmin&gt; create-iiop-listener --user admin --passwordfile passwords.txt --host fuyako --port 7070 --listeneraddress 192.168.1.100 --iiopport 8080 sample_iiop_listener</pre> Command create-iiop-listener executed successfully.	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">delete-iiop-listener(1)</a> , <a href="#">list-iiop-listeners(1)</a> , <a href="#">create-ssl(1)</a>	

## create-instance(1)

<b>NAME</b>	create-instance – creates an instance				
<b>SYNOPSIS</b>	<pre><b>create-instance</b> --user <i>admin_user</i> [--passwordfile <i>filename</i>]   [--host <i>host_name</i>] [--port <i>port_number</i>] [--secure -s]   [--terse=false] [--echo=false] [--interactive=true] [--help]   [--config <i>config_name</i>   --cluster <i>cluster_name</i>]   --nodeagent <i>nodeagent_name</i>   [--systemproperties (<i>name=value</i>) [:<i>name=value</i>]*] <i>instance_name</i></pre>				
<b>DESCRIPTION</b>	<p>Use the create-instance command to create a new server instance residing on a local or remote machine. For a server instance to be functional it must have:</p> <ul style="list-style-type: none"> <li>■ A reference to a node agent which defines the machine where the server instance resides.</li> <li>■ A reference to a configuration which defines the configuration of the instance. A server instance that is joining a cluster receives its configuration from its parent cluster.</li> </ul> <p>The node agent does not need to be created or started to create the instance; however, if the node agent is running, a remote server instance is created in a stopped state. If the node agent is not running, domain.xml is updated with the instance information and a new server instance is created the next time the node agent is started.</p> <p>There are three types of server instances that can be created. Each server instance can only be of one type:</p> <ol style="list-style-type: none"> <li>1. Standalone server instance: the configuration for this instance is not shared by any other server instances or clusters. When a standalone server instance is created, a standalone configuration is also created based on the default-config configuration. If no configuration or cluster is identified, a standalone server instance is created by default.</li> <li>2. Shared server instance: the configuration for this instance is shared with other server instances or clusters. A server instance is considered shared if its configuration is shared by any other server instances.</li> <li>3. Clustered server instance: the configuration for this instance is shared with other instances in the cluster. A server instance that is a member of the cluster inherits its configuration from that cluster. Any server instance that is not part of a cluster is considered an unclustered server instance.</li> </ol> <p>When creating server instances Application Server attempts to resolve possible port conflicts. It also assigns random ports, currently not in use and not already assigned to other instances on the same node agent. Use the --systemproperties option to create additional instances on the same node agent and specify system properties to resolve the port conflicts. System properties can be manipulated after instance creation using the system property commands.</p>				
<b>OPTIONS</b>	<table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.
-u --user	The authorized domain application server administrative username.				
-w --password	The --password option is deprecated. Use --passwordfile instead.				



<code>--passwordfile</code>	This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code> , <code>AS_ADMIN_USERPASSWORD</code> , <code>AS_ADMIN_SAVEDMASTERPASSWORD</code> , <code>AS_ADMIN_MQPASSWORD</code> , <code>AS_ADMIN_ALIASPASSWORD</code> , and so on.
<code>-H --host</code>	The machine name where the domain application server is running. The default value is localhost.
<code>-p --port</code>	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
<code>-s --secure</code>	If set to true, uses SSL/TLS to communicate with the domain application server.
<code>-t --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>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
<code>-h --help</code>	Displays the help text for the command.
<code>--config</code>	Creates a shared server instance. The configuration name must exist and must not be named <code>default-config</code> or <code>server-config</code> . If the configuration name provided is a standalone configuration, an error is displayed.
<code>--cluster</code>	Creates a clustered server instance that inherits its configuration from the named cluster.

## create-instance(1)

--nodeagent

The name of the node agent defining the machine where the server will be created. The node agent does not need to be running or even created. If the node agent does not exist, a placeholder will automatically be created in domain.xml.

--systemproperties

Defines system properties for the server instance. These properties override property definitions in the server instance's configuration. Currently, these properties allow a way for a server instance to override port settings defined in its configuration. This is necessary if for example two clustered instances (sharing the same configuration) reside on the same machine. The following properties are available:

Property	Definition
http-listener-1-port	This port is used to listen for HTTP requests. This property specifies the port number for http-listener-1. Valid values are 1–65535. On UNIX, creating sockets that listen on ports 1–1024 requires superuser privileges.
http-listener-2-port	This port is used to listen for HTTPS requests. This property specifies the port number for http-listener-2. Valid values are 1–65535. On UNIX, creating sockets that listen on ports 1–1024 requires superuser privileges.
orb-listener-1-port	This property specifies which ORB listener port for IIOP connections orb-listener-1 listens on.
IIOP_SSL_LISTENER_PORT	This port is used for secure IIOP connections.
IIOP_SSL_MUTUALAUTH_PORT	This property specifies which ORB listener port for IIOP connections the IIOP listener called SSL_MUTUALAUTH listens on.

OPERANDS

*instance\_name*

Property	Definition
JMS_SYSTEM_CONNECTOR_PORT	Property specifies the port number on which the JMX connector listens. Valid values are 1–65535. On UNIX, creating sockets that listen on ports 1–1024 requires superuser privileges.

The unique name of the instance being created. Each instance in the domain must have a unique name across all node agents, server instances, cluster names, and configuration names.

EXAMPLES

**EXAMPLE 1** Using the create-instance command

```
asadmin> create-instance --user admin --passwordfile password.txt
--host myhost --port 4849 --nodeagent agent1 instance1
Command create-instance executed successfully
```

Where: instance1 is created on a machine where node agent, agent1 resides.

**EXAMPLE 2** Using the create-instance command with systemproperties

```
asadmin> create-instance --user admin --passwordfile password.txt
--host myhost --port 4849 --nodeagent apple_agent --systemproperties HTTP_LISTENER_PORT=58294:
HTTP_SSL_LISTENER_PORT=58297:IIOP_LISTENER_PORT=58300:IIOP_SSL_LISTENER_PORT=58303:
IIOP_SSL_MUTUALAUTH_PORT=58306:JMX_SYSTEM_CONNECTOR_PORT=58309 instance2
Command create-instance executed successfully
```

Where: instance2 is created on a remote machine apple where node agent, apple\_agent resides.

EXIT STATUS

- 0  
command executed successfully
- 1  
error in executing the command

SEE ALSO

[delete-instance\(1\)](#), [list-instances\(1\)](#), [start-instance\(1\)](#), [stop-instance\(1\)](#)

## create-javamail-resource(1)

NAME	create-javamail-resource – creates a JavaMail session resource												
SYNOPSIS	<pre><b>create-javamail-resource</b> --user <i>admin_user</i> [--passwordfile <i>filename</i>]   [--host <i>host_name</i>] [--port <i>port_number</i>] [--secure -s]   [--terse=false] [--echo=false] [--interactive=true] [--help]   [--target <i>target</i>] --mailhost <i>hostname</i> --mailuser <i>username</i>   --fromaddress <i>address</i> [--storeprotocol <i>imap</i>]   [--storeprotocolclass <i>com.sun.mail.imap.IMAPStore</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>												
DESCRIPTION	The create-javamail-resource command creates a JavaMail session resource. This command is supported in remote mode only.												
OPTIONS	<table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td>-s --secure</td><td>If set to true, uses SSL/TLS to communicate with the domain application server.</td></tr> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	-s --secure	If set to true, uses SSL/TLS to communicate with the domain application server.
-u --user	The authorized domain application server administrative username.												
-w --password	The --password option is deprecated. Use --passwordfile instead.												
--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.												
-H --host	The machine name where the domain application server is running. The default value is localhost.												
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.												
-s --secure	If set to true, uses SSL/TLS to communicate with the domain application server.												

## create-javamail-resource(1)

-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.
-h --help	Displays the help text for the command.
--target	In Enterprise Edition, specifies the target for which you are creating the JavaMail session resource. Valid values are <ul style="list-style-type: none"> <li>■ <i>server</i>, which creates the resource for the default server instance <i>server</i> and is the default value</li> <li>■ <i>domain</i>, which creates the resource for the domain</li> <li>■ <i>cluster_name</i>, which creates the resource for every server instance in the cluster</li> <li>■ <i>instance_name</i>, which creates the resource for a particular server instance</li> </ul>
--mailhost	The DNS name of the default mail server. The connect methods of the Store and Transport objects use this value if a protocol-specific host property is not supplied. The name must be resolvable to an actual host name.
--mailuser	The mail account user name to provide when connecting to a mail server. The connect methods of the Store and Transport objects use this value if a protocol-specific username property is not supplied.
--fromaddress	The email address of the default user, in the form <i>username@host.domain</i> .
--storeprotocol	The mail server store protocol. The default is <i>imap</i> . Change this value only if you have reconfigured the Application Server's mail provider to use a nondefault store protocol.
--storeprotocolclass	The mail server store protocol class name. The default is <i>com.sun.mail.imap.IMAPStore</i> . Change this value only if you have reconfigured the Application Server's mail provider to use a nondefault store protocol.

## create-javamail-resource(1)

	<code>--transportprotocol</code>	The mail server transport protocol. The default is smtp. Change this value only if you have reconfigured the Application Server's mail provider to use a nondefault transport protocol.
	<code>--transportprotocolclass</code>	The mail server transport protocol class name. The default is <code>com.sun.mail.smtp.SMTPTransport</code> . Change this value only if you have reconfigured the Application Server's mail provider to use a nondefault transport protocol.
	<code>--debug</code>	If set to true, server starts up in debug mode for this resource. If the JavaMail log level is set to FINE or finer, the debugging output will be generated and will be included in the server log file. The default value is false.
	<code>--enabled</code>	If set to true, the resource is enabled at runtime. The default value is true.
	<code>--description</code>	A text description of the JavaMail resource.
	<code>--property</code>	Optional attribute name/value pairs for configuring the JavaMail resource. The JavaMail API documentation lists the properties you might want to set.
OPERANDS	<i>jndi_name</i>	The JNDI name of the JavaMail resource to be created. It is a recommended practice to use the naming subcontext prefix <code>mail/</code> for JavaMail resources.
EXAMPLES	<p><b>EXAMPLE 1</b> Using the create-javamail-resource command</p> <p>The following command creates a JavaMail resource named <code>mail/MyMailSession</code>. The escape character (<code>\</code>) is used in the <code>--fromaddress</code> option to distinguish the dot (<code>.</code>) and at sign (<code>@</code>). The JNDI name for a JavaMail session resource customarily includes the <code>mail/</code> naming subcontext.</p> <pre>asadmin&gt; create-javamail-resource --user admin --passwordfile passwords.txt --host fuyako --port 7070 --mailhost localhost --mailuser sample --fromaddress sample\@sun\.com mail/MyMailSession Command create-javamail-resource executed successfully.</pre>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">delete-javamail-resource(1)</a> , <a href="#">list-javamail-resources(1)</a>	

NAME	create-jdbc-connection-pool – registers the JDBC connection pool	
SYNOPSIS	<b>create-jdbc-connection-pool</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--datasourceclassname <i>classname</i> ] [--restype <i>res_type</i> ] [--steadypoolsize <i>poolsize</i> ] [--maxpoolsize <i>poolsize</i> ] [--maxwait <i>time</i> ] [--poolresize <i>limit</i> ] [--idletimeout <i>time</i> ] [--isolationlevel <i>isolation_level</i> ] [--isolationguaranteed <i>true</i> ] [--isconnectvalidatereq <i>false</i> ] [--validationmethod <i>auto-commit</i> ] [--validationtable <i>tablename</i> ] [--failconnection <i>false</i> ] [--description <i>text</i> ] [--property ( <i>name=value</i> ) [: <i>name=value</i> ]*] <i>connectionpoolid</i>	
DESCRIPTION	Registers a new JDBC connection pool with the specified JDBC connection pool name.  This command is supported in remote mode only.	
OPTIONS	-u --user  -w --password  --passwordfile          -H --host  -p --port	The authorized domain application server administrative username.  The --password option is deprecated. Use --passwordfile instead.  This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.  The machine name where the domain application server is running. The default value is localhost.  The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

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

<code>-s --secure</code>	If set to true, uses SSL/TLS to communicate with the domain application server.
<code>-t --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>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
<code>-h --help</code>	Displays the help text for the command.
<code>--target</code>	The target option is deprecated.
<code>--datasourceclassname</code>	The name of the vendor supplied JDBC datasource resource manager.
<code>--restype</code>	The interface that the datasource class implements. Must be one of <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. This option has no default value.
<code>--steadypoolsize</code>	The minimum and initial number of connections maintained in the pool. The default value is 8.
<code>--maxpoolsize</code>	The maximum number of connections that can be created. The default value is 32.
<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>	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 <code>steadypoolsize</code> , the connection removal stops. The default value is 2.
<code>--idletimeout</code>	The 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. The default value is 300.



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

	<code>--isolationlevel</code>	<p>This 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 the default isolation level that the JDBC driver provides.</p> <p>You can set a desired isolation level 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.</p>
	<code>--isolationguaranteed</code>	<p>This is applicable only when a particular isolation level is specified for <code>transaction-isolation-level</code>. The default value is <code>true</code>.</p> <p>This option assures that every time a connection is obtained from the pool, <code>isolationlevel</code> is set to the desired value. This could have some performance impact on some JDBC drivers. Administrators can set this to <code>false</code> when the application does not change <code>--isolationlevel</code> before returning the connection.</p>
	<code>--isconnectvalidatereq</code>	<p>If set to <code>true</code>, connections are validated or checked to see if they are usable before giving out the application. The default value is <code>false</code>.</p>
	<code>--validationmethod</code>	<p>The name of the validation table used to perform a query to validate a connection. Valid settings are: <code>auto-commit</code>, <code>meta-data</code>, or <code>table</code>. The default value is <code>auto-commit</code>.</p>
	<code>--validationtable</code>	<p>The name of the validation table used to perform a query to validate a connection.</p>
	<code>--failconnection</code>	<p>If set to <code>true</code>, all connections in the pool must be closed when a single validation check fails. The default value is <code>false</code>. One attempt is made to re-establish failed connections.</p>
	<code>--description</code>	<p>Text providing descriptive details about the specified JDBC connection pool.</p>
	<code>--property</code>	<p>Optional attribute name/value pairs for configuring the connection pool.</p>
<b>OPERANDS</b>	<i>connection_pool_id</i>	<p>The name of the JDBC connection pool to be created.</p>

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

### EXAMPLES

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

```
asadmin> create-jdbc-connection-pool --user admin --passwordfile adminadminfile
--host fuyako --port 7070 --datasourceclassname com.pointbase.jdbc.jdbcUniversalDriver
--restype javax.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

1  
error in executing the command

### SEE ALSO

[delete-jdbc-connection-pool\(1\)](#), [list-jdbc-connection-pools\(1\)](#)

NAME	create-jdbc-resource – creates a JDBC resource with the specified JNDI name														
SYNOPSIS	<pre><b>create-jdbc-resource</b> --user <i>admin_user</i> [--passwordfile <i>filename</i>]                         [--host <i>host_name</i>] [--port <i>port_number</i>] [--secure -s]                         [--terse=<i>false</i>] [--echo=<i>false</i>] [--interactive=<i>true</i>] [--help]                         [--target<i>target</i>] connectionpoolid <i>pool_name</i> [--enabled=<i>true</i>]                         [--description <i>text</i>] [--property (<i>name=value</i>) [:<i>name=value</i>]*]                         <i>jndi_name</i></pre>														
DESCRIPTION	The create-jdbc-resource command creates a new JDBC resource. This command is supported in remote mode only.														
OPTIONS	<table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td>-s --secure</td><td>If set to 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> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	-s --secure	If set to 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.
-u --user	The authorized domain application server administrative username.														
-w --password	The --password option is deprecated. Use --passwordfile instead.														
--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.														
-H --host	The machine name where the domain application server is running. The default value is localhost.														
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.														
-s --secure	If set to 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.														

## create-jdbc-resource(1)

	<code>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
	<code>--target</code>	valid in Enterprise Edition only, specifies the target to which you are deploying. Valid values are 'server,' 'domain,' cluster, and instance. The default is server.
	<code>--connectionpoolid</code>	The name of the JDBC connection pool. If two or more JDBC resource elements point to the same connection pool element, they use the same pool connections at runtime.
	<code>--enabled</code>	Determines whether the JDBC resource is enable at runtime. The default value is true.
	<code>--description</code>	Text providing descriptive details about the JDBC resource.
	<code>--property</code>	optional attribute name/value pairs for configuring the resource.
<b>OPERANDS</b>	<i>jndi_name</i>	the JNDI name of this JDBC resource.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the create-jdbc-resource command</p> <pre>asadmin&gt; create-jdbc-resource --connectionpoolid connPool02 test_jdbc_resource</pre> <p>Command create-jdbc-resource executed successfully.</p> <p>Where test_jdbc_resource is the name of the new JDBC resource.</p>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">delete-jdbc-resource(1)</a> , <a href="#">list-jdbc-resources(1)</a>	

NAME	create-jmsdest – creates a physical destination												
SYNOPSIS	<pre><b>create-jmsdest</b> --user <i>admin_user</i> [--passwordfile <i>filename</i>]                 [--host <i>host_name</i>] [--port <i>port_number</i>] [--secure -s]                 [--terse=false] [--echo=false] [--interactive=true] [--help]                 [--target <i>target</i>] --desttype <i>dest_type</i>                 [--property (name=value) [:name=value] *] <i>dest_name</i></pre>												
DESCRIPTION	<p>The <code>create-jmsdest</code> command creates a JMS physical destination. Along with the physical destination, you use the <code>create-jms-resource</code> command to create a JMS destination resource that has a Name property that specifies the physical destination. This command is supported in remote mode only.</p>												
OPTIONS	<table> <tr> <td><code>-u --user</code></td><td>The authorized domain application server administrative username.</td></tr> <tr> <td><code>-w --password</code></td><td>The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.</td></tr> <tr> <td><code>--passwordfile</code></td><td>This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code>, <code>AS_ADMIN_USERPASSWORD</code>, <code>AS_ADMIN_SAVEDMASTERPASSWORD</code>, <code>AS_ADMIN_MQPASSWORD</code>, <code>AS_ADMIN_ALIASPASSWORD</code>, and so on.</td></tr> <tr> <td><code>-H --host</code></td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td><code>-p --port</code></td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td><code>-s --secure</code></td><td>If set to true, uses SSL/TLS to communicate with the domain application server.</td></tr> </table>	<code>-u --user</code>	The authorized domain application server administrative username.	<code>-w --password</code>	The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.	<code>--passwordfile</code>	This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code> , <code>AS_ADMIN_USERPASSWORD</code> , <code>AS_ADMIN_SAVEDMASTERPASSWORD</code> , <code>AS_ADMIN_MQPASSWORD</code> , <code>AS_ADMIN_ALIASPASSWORD</code> , and so on.	<code>-H --host</code>	The machine name where the domain application server is running. The default value is localhost.	<code>-p --port</code>	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	<code>-s --secure</code>	If set to true, uses SSL/TLS to communicate with the domain application server.
<code>-u --user</code>	The authorized domain application server administrative username.												
<code>-w --password</code>	The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.												
<code>--passwordfile</code>	This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code> , <code>AS_ADMIN_USERPASSWORD</code> , <code>AS_ADMIN_SAVEDMASTERPASSWORD</code> , <code>AS_ADMIN_MQPASSWORD</code> , <code>AS_ADMIN_ALIASPASSWORD</code> , and so on.												
<code>-H --host</code>	The machine name where the domain application server is running. The default value is localhost.												
<code>-p --port</code>	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.												
<code>-s --secure</code>	If set to true, uses SSL/TLS to communicate with the domain application server.												

## create-jmsdest(1)

-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.
-h --help	Displays the help text for the command.
--target	<p>In Enterprise Edition, specifies the target for which you are creating the physical destination. Although the <code>create-jmsdest</code> command is related to resources, a physical destination is created using the JMS Service, which is part of the configuration. Valid values are</p> <ul style="list-style-type: none"><li>■ <code>server</code>, which creates the physical destination for the default server instance <code>server</code> and is the default value</li><li>■ <code>configuration_name</code>, which creates the physical destination for the named configuration</li><li>■ <code>cluster_name</code>, which creates the physical destination for every server instance in the cluster</li><li>■ <code>instance_name</code>, which creates the physical destination for a particular server instance</li></ul>
-T --desttype	The type of the JMS destination. Valid values are <code>topic</code> and <code>queue</code> .
--property	Optional attribute name/value pairs for configuring the physical destination. You can specify the following property for a physical destination:

Property	Definition
<code>maxNumActiveConsumers</code>	The maximum number of consumers that can be active in load-balanced delivery from a queue destination. A value of -1 means an unlimited number. The default is 1. (Platform Edition limits this value to 2.)

		create-jmsdest(1)
		To modify the value of this property or to specify other physical destination properties, use the <i>install_dir/imq/bin/imqcmd</i> command. See the <i>Sun Java System Message Queue 3 2005Q1 Administration Guide</i> for more information.
OPERANDS	<i>dest_name</i>	A unique identifier for the the JMS destination to be created.
EXAMPLES	<p><b>EXAMPLE 1</b> Using the create-jmsdest command</p> <p>The following command creates a JMS physical queue named <code>PhysicalQueue</code>.</p> <pre>asadmin&gt; create-jmsdest --user admin --passwordfile passwords.txt --host localhost --port 4848 --desttype queue --property User=public:Password=public PhysicalQueue</pre> <p>Command create-jmsdest executed successfully.</p>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-jms-resource(1)</a> , <a href="#">delete-jmsdest(1)</a> , <a href="#">list-jmsdest(1)</a>	

## create-jms-resource(1)

NAME	create-jms-resource – creates a JMS resource	
SYNOPSIS	<b>create-jms-resource</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--target <i>target</i> ] --restype <i>type</i> [--enabled=true] [--description <i>text</i> ] [--property ( <i>name=value</i> ) [: <i>name=value</i> ]*] <i>jndi_name</i>	
DESCRIPTION	The create-jms-resource command creates a Java Message Service (JMS) connection factory resource or a JMS destination resource. This command is supported in remote mode only.	
OPTIONS	-u --user -w --password --passwordfile -H --host -p --port -s --secure	<p>The authorized domain application server administrative username.</p> <p>The --password option is deprecated. Use --passwordfile instead.</p> <p>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</p> <p>The machine name where the domain application server is running. The default value is localhost.</p> <p>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</p> <p>If set to true, uses SSL/TLS to communicate with the domain application server.</p>



## create-jms-resource(1)

-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.
-h --help	Displays the help text for the command.
--target	In Enterprise Edition, specifies the target for which you are creating the JMS resource. Valid values are <ul style="list-style-type: none"> <li>■ <i>server</i>, which creates the resource for the default server instance <i>server</i> and is the default value</li> <li>■ <i>domain</i>, which creates the resource for the domain</li> <li>■ <i>cluster_name</i>, which creates the resource for every server instance in the cluster</li> <li>■ <i>instance_name</i>, which creates the resource for a particular server instance</li> </ul>
--restype	The JMS resource type, which can be either <code>javax.jms.Topic</code> , <code>javax.jms.Queue</code> , <code>javax.jms.ConnectionFactory</code> , <code>javax.jms.TopicConnectionFactory</code> , or <code>javax.jms.QueueConnectionFactory</code> .
--enabled	If set to true, the resource is enabled at runtime.
--description	A text description of the JMS resource.
--property	Optional attribute name/value pairs for configuring the JMS resource.  You can specify the following properties for a connection factory resource:

Property	Definition
ClientId	Specifies a client ID for a connection factory that will be used by a durable subscriber.

create-jms-resource(1)

Property	Definition
AddressList	Specifies the names (and, optionally, port numbers) of a message broker instance or instances with which your application will communicate. Each address in the list specifies the host name (and, optionally, host port and connection service) for the connection. For example, the value could be <code>earth</code> or <code>earth:7677</code> . Specify the port number if the message broker is running on a port other than the default (7676). If you specify multiple hosts and ports in a clustered environment, the first available host on the list is used. Default: The local host and default port number (7676). The client will attempt a connection to a broker on port 7676 of the local host.
MessageServiceAddressList	Same as <code>AddressList</code> . This property name is deprecated. Use <code>AddressList</code> instead.
UserName	The user name for the connection factory. Default: <code>guest</code> .
Password	The password for the connection factory. Default: <code>guest</code> .
ReconnectEnabled	If enabled (value = <code>true</code> ), specifies that the client runtime attempts to reconnect to a message server (or the list of addresses in the <code>AddressList</code> ) when a connection is lost. Default: <code>false</code> .

Property	Definition
ReconnectAttempts	Specifies the number of attempts to connect (or reconnect) for each address in the AddressList before the client runtime tries the next address in the list. A value of -1 indicates that the number of reconnect attempts is unlimited (the client runtime attempts to connect to the first address until it succeeds). Default: 6.
ReconnectInterval	Specifies the interval in milliseconds between reconnect attempts. This applies for attempts on each address in the AddressList and for successive addresses in the list. If the interval is too short, the broker does not have time to recover. If it is too long, the reconnect might represent an unacceptable delay. Default: 30,000 milliseconds.
AddressListBehavior	Specifies whether connection attempts are in the order of addresses in the AddressList attribute (PRIORITY) or in a random order (RANDOM). PRIORITY means that the reconnect will always try to connect to the first server address in the AddressList and will use another one only if the first broker is not available. If you have many clients attempting a connection using the same connection factory, specify RANDOM to prevent them from all being connected to the same address. Default: PRIORITY.

create-jms-resource(1)

Property	Definition
AddressListIterations	Specifies the number of times the client runtime iterates through the AddressList in an effort to establish (or re-establish) a connection). A value of -1 indicates that the number of attempts is unlimited. Default: -1.

You can specify the following properties for a destination resource:

Property	Definition
Name	(Required) This property specifies the name of the physical destination to which the resource will refer. You create a physical destination with the <code>create-jmsdest</code> command.
Description	This property provides a description of the physical destination.

**OPERANDS** *jndi\_name*

The JNDI name of the JMS resource to be created.

**EXAMPLES** **EXAMPLE 1** Creating a JMS connection factory resource for durable subscriptions

The following command creates a connection factory resource of type `javax.jms.TopicConnectionFactory` whose JNDI name is `jms/DurableTopicConnectionFactory`. 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.

```
asadmin> create-jms-resource --user admin1
--passwordfile passwords.txt --host pigeon --port 5001
--restype javax.jms.TopicConnectionFactory --description
"example of creating a JMS connection factory"
--property ClientId=MyID jms/DurableTopicConnectionFactory
Command create-jms-resource executed successfully.
```

**EXAMPLE 2** Creating a JMS destination resource

The following command creates a destination resource whose JNDI name is `jms/Queue`. The `Name` property specifies the physical destination to which the resource refers.

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

**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)

NAME	create-jndi-resource – registers a JNDI resource
SYNOPSIS	<b>create-jndi-resource</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--target <i>target</i> ] --jndilookupname <i>lookup_name</i> --restype <i>type</i> --factoryclass <i>class_name</i> [--enabled=true] [--description <i>text</i> ] [--property ( <i>name=value</i> ) [: <i>name=value</i> ]*] <i>jndi_name</i>
DESCRIPTION	The create-jndi-resource command registers a JNDI resource. This command is supported in remote mode only.
OPTIONS	<div>-u --user</div> <div>The authorized domain application server administrative username.</div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> <div>--passwordfile</div> <div>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div>

## create-jndi-resource(1)

-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.
-h --help	Displays the help text for the command.
--target	valid in Enterprise Edition only, specifies the target to which you are deploying. Valid values are 'server,' 'domain,' cluster, or instance. The default is server.
--jndilookupname	The lookup name that the external container uses.
--resourcetype	The -resourcetype option is deprecated. Use -restype instead.
--restype	The JNDI resource type. It can be topic or queue.
--factoryclass	The class that creates the JNDI resource.
--enabled	Determines whether the resource is enabled at runtime.
--description	The text that provides details about the JNDI resource.
--property	optional attribute name/value pairs for configuring the resource. The following properties are available:

Property	Definition
http-listener-1-port	This property specifies the port number for http-listener-1. Valid values are 1–65535. On UNIX, creating sockets that listen on ports 1–1024 requires superuser privileges.
http-listener-2-port	This property specifies the port number for http-listener-2. Valid values are 1–65535. On UNIX, creating sockets that listen on ports 1–1024 requires superuser privileges.

## create-jndi-resource(1)

Property	Definition
orb-listener-1-port	This property specifies which ORB listener port for IIOP connections orb-listener-1 listens on.
IIOP_SSL_LISTENER_PORT	This property specifies which ORB listener port for IIOP connections the IIOP listener called SSL listens on.
IIOP_SSL_MUTUALAUTH_PORT	This property specifies which ORB listener port for IIOP connections the IIOP listener called SSL_MUTUALAUTH listens on.
JMX_SYSTEM_Connector-port	This property specifies the port number on which the JMX connector listens. Valid values are 1–65535. On UNIX, creating sockets that listen on ports 1–1024 requires superuser privileges.

**OPERANDS** *jndi\_name*

The name of the JNDI resource to be created. This name must be unique.

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

```
asadmin> create-jndi-resource --user admin --passwordfile filename
--host pigeon --port 4001 --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 new JNDI resource created.

**EXIT STATUS**

0  
command executed successfully

1  
error in executing the command

**SEE ALSO** [delete-jndi-resource\(1\)](#), [list-jndi-resources\(1\)](#)



NAME	create-jvm-options – creates JVM options in the Java configuration or profiler elements of the domain.xml file.	
SYNOPSIS	<b>create-jvm-options</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--target <i>target</i> ] [--profiler=false] ( <i>jvm_option_name=jvm_option_value</i> ) [: <i>jvm_option_name=jvm_option_name</i> ] *	
DESCRIPTION	<p>Creates JVM options in the Java configuration or profiler elements of the domain.xml file. JVM options are used to record the settings needed to get a particular profiler going.</p> <p>This command is supported in remote mode only.</p> <p>You must restart the server for newly created JVM options to take affect. Use the start/stop-domain command to restart the domain administration server.</p>	
OPTIONS	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	<p>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</p>
	-H --host	The machine name where the domain application server is running. The default value is localhost.
	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

## create-jvm-options(1)

	-s --secure	If set to 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.
	-h --help	Displays the help text for the command.
	--target	specifies the target to which you are deploying. Valid values are config, instance, cluster, or 'server.' The default is server.
	--profiler	indicates whether the JVM options are for the profiler. The profiler must exist for this option to be true.
<b>OPERANDS</b>	<i>jvm_option_name</i>	the left side of the equal sign (=) is the JVM option name. The right side of the equal sign (=) is the JVM option value. A colon (:) is a delimiter for multiple options.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the create-jvm-options command</p> <p>JVM options must start with a dash (-), . Use the backslash (\) to escape the dash delimiter.</p> <pre>asadmin&gt; create-jvm-options --user admin --passwordfile adminfile --host localhost --port 4849 --target server "\-Dtmp=sun"-e \-Doption1=value1 create-jvm-options --interactive=true --secure=true --passwordfile /password --terse=false --user admin --target server --host localhost --echo=true --port 4849 \-Doption1=value1 Command create-jvm-options executed successfully</pre>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">delete-jvm-options(1)</a>	

NAME	create-lifecycle-module – adds a lifecycle module
SYNOPSIS	<b>create-lifecycle-module</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--enabled=true] [--target <i>target</i> ] --classname <i>classname</i> [--classpath <i>classpath</i> ] [--loadorder <i>loadorder</i> ] [--failurefatal=false] [--description <i>description</i> ] [--property ( <i>name=value</i> )[: <i>name=value</i> ]*] <i>module_name</i>
DESCRIPTION	Creates the lifecycle module. The lifecycle modules provide a means of running short or long duration Java-based tasks within the application server environment. This command is supported in remote mode only.
OPTIONS	<div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>--passwordfile</div> <div>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </div> </div> <div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> </div> <div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> </div> <div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> </div>

## create-lifecycle-module(1)

	-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.
	-h --help	Displays the help text for the command.
	--target	This option is the name of the resulting location. The valid targets for this command are configuration, instace, cluster, or server. This is used by EE only.
	--classname	This is the fully qualified name of the startup class.
	--classpath	This option indicates where this module is actually located if it is not under applications-root.
	--loadorder	This option represents 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	This options tells the system what to do if the lifecycle module does not load correctly. If this option is set to true, then the system aborts the server startup if this module does not load properly.
	--enabled	This option determines whether the resource is enabled at runtime.
	--description	This is the text description of the resource associated with this module.
	--property	This is an optional attribute containing name/value pairs used to configure the resource.
OPERANDS	<i>module_name</i>	This operand is a unique identifier or the deployed server lifecycle event listener module.
EXAMPLES	<b>EXAMPLE 1</b> using create-lifecycle-module <pre> asadmin&gt; create-lifecycle-module --user admin --passwordfile adminpassword.txt --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>	

create-lifecycle-module(1)

**EXAMPLE 1** using create-lifecycle-module     *(Continued)*

Where: customSetup is the lifecycle module created. The escape character \ is used in the property option to distinguish the colons (:).

**EXIT STATUS**

0	command executed successfully
1	error in executing the command

**SEE ALSO**   [delete-lifecycle-module\(1\)](#), [list-lifecycle-modules\(1\)](#)

## create-message-security-provider(1)

<b>NAME</b>	create-message-security-provider – enables administrators to create the message-security-config and provider-config sub-elements for the security service in domain.xml						
<b>SYNOPSIS</b>	<pre> <b>create-message-security-provider</b> --user <i>admin_user</i>   [--passwordfile <i>filename</i>] [--host <i>host_name</i>] [--port <i>port_number</i>]   [--secure -s] [--terse=false] [--echo=false] [--interactive=true]   [--help] [--target <i>target</i>] --classname <i>provider_class</i>   [--layer <i>message_layer</i>] [--providertype <i>provider_type</i>]   [--requestauthsource <i>request_auth_source</i>]   [--requestauthrecipient <i>request_auth_recipient</i>]   [--responseauthsource <i>response_auth_source</i>]   [--responseauthrecipient <i>response_auth_recipient</i>]   [--isdefaultprovider] [--property (<i>name=value</i>) [:<i>name=value</i>] *]   provider_name </pre>						
<b>DESCRIPTION</b>	<p>Enables the administrator to create the message-security-config and provider-config sub-elements for the security service in domain.xml (the file that specifies parameters and properties to the Application Server). The options specified in the list below apply to attributes within the message-security-config and provider-config sub-elements of the domain.xml file.</p> <p>If the message-layer (message-security-config) does not exist, it is created, and then the provider-config is created under it.</p> <p>This command is supported in remote mode only.</p>						
<b>OPTIONS</b>	<p>If an option has a short option name, then the short option preceeds the long option name. Short options have one dash whereas long options have two dashes.</p> <table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD,</td></tr> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD,
-u --user	The authorized domain application server administrative username.						
-w --password	The --password option is deprecated. Use --passwordfile instead.						
--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD,						

## create-message-security-provider(1)

	AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
-H --host	The machine name where the domain application server is running. The default value is localhost.
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
-s --secure	If set to 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.
-h --help	Displays the help text for the command.
--target	<p>In Enterprise Edition, specifies the target to which you are deploying. Valid values are</p> <ul style="list-style-type: none"><li>■ <i>server</i>, which deploys the component to the default server instance <i>server</i> and is the default value</li><li>■ <i>domain</i>, which deploys the component to the domain.</li><li>■ <i>cluster_name</i>, which deploys the component to every server instance in the cluster.</li><li>■ <i>instance_name</i>, which deploys the component to a particular sever instance.</li></ul> <p>The following optional attribute name/value pairs are available:</p>

## create-message-security-provider(1)

Property	Definition
classname	Defines the Java implementation class of the provider. Client authentication providers must implement the <code>com.sun.enterprise.security.jauth.ClientAuthModule</code> interface. Server-side providers must implement the <code>com.sun.enterprise.security.jauth.ServerAuthModule</code> interface. A provider may implement both interfaces, but it must implement the interface corresponding to its provider type.
layer	The message-layer entity used to define the value of the <code>auth-layer</code> attribute of <code>message-security-config</code> elements. The default is <code>SOAP</code> .
providertype	Establishes whether the provider is to be used as client authentication provider, server authentication provider, or both. Valid options for this property include <code>client</code> , <code>server</code> , or <code>client-server</code> . The default value is <code>client-server</code> .
requestauthsource	The <code>auth-source</code> attribute defines a requirement for message-layer sender authentication (e.g. username password) or content authentication (e.g. digital signature) to be applied to request messages. Possible values are <code>sender</code> or <code>content</code> . When this argument is not specified, source authentication of the request is not required.



# create-message-security-provider(1)

Property	Definition
requestauthrecipient	The auth-recipient attribute defines a requirement for message-layer authentication of the receiver of a message to its sender (e.g. by XML encryption). Possible values are before-content or after-content. The default value is after-content.
responseauthsource	The auth-source attribute defines a requirement for message-layer sender authentication (e.g. username password) or content authentication (e.g. digital signature) to be applied to response messages. Possible values are sender or content. When this option is not specified, source authentication of the response is not required.
responseauthrecipient	The auth-recipient attribute defines a requirement for message-layer authentication of the receiver of the response message to its sender (e.g. by XML encryption). Possible values are before-content or after-content. The default value is after-content.
isdefaultprovider	The default-provider attribute is used to designate the provider as the default provider (at the layer) of the type or types identified by the providertype argument. There is no default associated with this option.

## create-message-security-provider(1)

Property	Definition
property	Use this property to pass provider-specific property values to the provider when it is initialized. Properties passed in this way might include key aliases to be used by the provider to get keys from keystores, signing, canonicalization, encryption algorithms, etc.

**OPERANDS** *provider\_name* The name of the provider used to reference the provider-config element.

**EXAMPLES** **EXAMPLE 1** Using create-message-security-provider

The following example shows how to create a message security provider for a client.

```
asadmin> create-message-security-provider --user admin
--passwordfile pwd_file
--classname com.sun.enterprise.security.jauth.ClientAuthModule
--providertype client mySecurityProvider
```

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

**SEE ALSO** [delete-message-security-provider\(1\)](#),  
[list-message-security-providers\(1\)](#)

NAME	create-password-alias – creates a password alias	
SYNOPSIS	<b>create-password-alias</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--aliaspassword <i>alias_password</i> ] <i>aliasname</i>	
DESCRIPTION	<p>This command creates an alias for a password and stores it in domain.xml. An alias is a token of the form \${ALIAS=password-alias-password}. The password corresponding to the alias name is stored in encrypted form. The password-alias commands take both a secure interactive form (in which the user is prompted for all information) and a more script-friendly form, in which the password is propagated on the command line.</p> <p>This command is supported in remote mode only.</p>	
OPTIONS	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASEPASSWORD, and so on.
	-H --host	The machine name where the domain application server is running. The default value is localhost.
	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	-s --secure	If set to true, uses SSL/TLS to communicate with the domain application server.

## create-password-alias(1)

	<code>-t --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>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
	<code>--aliaspassword</code>	This is a separate and distinct password corresponding to the original password. WARNING: Passing this password on the command line is not secure.  The password is optional and when omitted, the user is prompted.
OPERANDS	aliasname	This is the name of the substitute password as it appears in domain.xml.
EXAMPLES	<b>EXAMPLE 1</b> Using create-password-alias  asadmin> <code>create-password-alias --aliasname alias1</code>  Command create-password-alias executed successfully	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">delete-password-alias(1)</a> , <a href="#">list-password-aliases(1)</a> , <a href="#">update-password-alias(1)</a>	

NAME	create-persistence-resource – registers a persistence resource	
SYNOPSIS	<b>create-persistence-resource</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--enabled= <i>true</i> ] [--target <i>target</i> ] [--jdbcjndiname <i>jndi_name</i>   --connectionpoolid <i>id</i> ] [--factoryclass <i>classname</i> ] [--description <i>text</i> ] [--property ( <i>name=value</i> ) [: <i>name=value</i> ] *] <i>jndi_name</i>	
DESCRIPTION	Registers a persistence resource. This command is supported in remote mode only.  The --jdbcjndiname option and the --connectionpoolid option are mutually exclusive; only one should be used.	
OPTIONS	<div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>--passwordfile</div> <div>           This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </div> </div> <div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> </div> <div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> </div> <div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> </div>	

## create-persistence-resource(1)

	-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.
	-h --help	Displays the help text for the command.
	--enabled	Determines whether the resource is enabled at runtime.
	---target	Specifies the target for which you are creating a persistence resource. This option is available only in the Sun Java System Application Server Enterprise Edition. Valid values are <ul style="list-style-type: none"> <li>■ <code>server</code>, which deploys the component to the default server instance <code>server</code> and is the default value</li> <li>■ <code>domain</code>, which deploys the component to the domain.</li> <li>■ <code>cluster_name</code>, which deploys the component to every server instance in the cluster.</li> <li>■ <code>instance_name</code>, which deploys the component to a particular sever instance.</li> </ul>
	--jdbcjndiname	Specifies the JDBC resource with which database connections are obtained. It must be the name of a pre-created JDBC resource.
	--connectionpoolid	Specifies the name of the JDBC connection pool. If two or more JDBC resource elements point to the same connection pool element, they use the same pool connections at runtime.
	--factoryclass	Deprecated, and not needed for the default CMP implementation. Specifies the class that creates the persistence manager instance.
	--description	Specifies a text description of the persistence resource.
	--property	Specifies optional name/value pairs for configuring the persistence resource.
<b>OPERANDS</b>	<i>jndi_name</i>	Specifies the JNDI name of the persistence resource.

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

```
asadmin> create-persistence-resource --user admin --passwordfile secret.txt
--jdbcjndiname sample_jndi_resource sample_persistence_resource
Command create-persistence-resource executed successfully
```

**EXIT STATUS**    0  
                  command executed successfully

                  1  
                  error in executing the command

**SEE ALSO**    [delete-persistence-resource\(1\)](#), [list-persistence-resources\(1\)](#)

## create-profiler(1)

NAME	create-profiler – creates the profiler element														
SYNOPSIS	<b>create-profiler</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--target <i>target_name</i> ] [--classpath <i>classpath</i> ] [--nativelibpath <i>native_library_path</i> ] [--enabled] [--property (name=value) [:name=value]*] <i>profiler_name</i>														
DESCRIPTION	<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>														
OPTIONS	<table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td>-s --secure</td><td>If set to 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> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	-s --secure	If set to 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.
-u --user	The authorized domain application server administrative username.														
-w --password	The --password option is deprecated. Use --passwordfile instead.														
--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.														
-H --host	The machine name where the domain application server is running. The default value is localhost.														
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.														
-s --secure	If set to 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.
	-h --help	Displays the help text for the command.
	--target	In Enterprise Edition, specifies the target on which you are listing the realms. Valid values are <ul style="list-style-type: none"> <li>■ <i>server</i>, which creates the listener for the default server instance <i>server</i> and is the default value</li> <li>■ <i>configuration_name</i>, which creates the listener for the named configuration</li> <li>■ <i>cluster_name</i>, which creates the listener for every server instance in the cluster</li> <li>■ <i>instance_name</i>, which creates the listener for a particular server instance</li> </ul>
	--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.
OPERANDS	<i>profiler_name</i>	name of the profiler.
EXAMPLES	<b>EXAMPLE 1</b> Using create-profiler <pre>asadmin&gt; create-profiler --user admin --passwordfile password.txt --host localhost --port 4848 --classpath /home/appserver/ --nativelibpath /u/home/lib --enabled=false --property defaultuser=admin:password=adminadmin sample_profiler Created Profiler with id = sample_profiler</pre> <p>Where: <i>sample_profiler</i> is the profiler created.</p>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">delete-profiler(1)</a>	

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

NAME	create-resource-adapter-config – creates the configuration information in domain.xml for the connector module												
SYNOPSIS	<pre> <b>create-resource-adapter-config</b> --user <i>admin_user</i>     [--passwordfile <i>filename</i>] [--host <i>host_name</i>] [--port <i>port_number</i>]     [--secure -s] [--terse=<i>false</i>] [--echo=<i>false</i>] [--interactive=<i>true</i>]     [--help] [--threadpoolid <i>threadpool</i>]     [--property (<i>property name=value</i>) [:<i>name=value</i>] *] <i>raname</i> </pre>												
DESCRIPTION	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 --threadpoolid option.												
OPTIONS	<table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td>-s --secure</td><td>If set to true, uses SSL/TLS to communicate with the domain application server.</td></tr> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	-s --secure	If set to true, uses SSL/TLS to communicate with the domain application server.
-u --user	The authorized domain application server administrative username.												
-w --password	The --password option is deprecated. Use --passwordfile instead.												
--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.												
-H --host	The machine name where the domain application server is running. The default value is localhost.												
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.												
-s --secure	If set to true, uses SSL/TLS to communicate with the domain application server.												

	create-resource-adapter-config(1)	
	-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.
	-h --help	Displays the help text for the command.
	--target	This option has been deprecated.
	--threadpoolid	The threadpool ID from which the work manager gets the thread.
	--property	This option specifies the configuration properties of the resource adapter java bean.
OPERANDS	<i>raname</i>	This operand is the value kept in the resource-adapter-name in the domain.xml file.
EXAMPLES	<b>EXAMPLE 1</b> Using create-resource-adapter-config asadmin> <b>create-resource-adapter-config u--user ul --passwordfile pfile1 ral</b> 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)	

## create-ssl(1)

<b>NAME</b>	create-ssl – creates and configures the SSL element in the selected HTTP listener, IIOP listener, or IIOP service										
<b>SYNOPSIS</b>	<pre> <b>create-ssl</b> --user <i>admin_user</i> [--passwordfile <i>filename</i>]     [--host <i>host_name</i>] [--port <i>port_number</i>] [--secure -s]     [--terse=<i>false</i>] [--echo=<i>false</i>] [--interactive=<i>true</i>] [--help]     [--target <i>target</i>] --type <i>listener_or_service_type</i> --certname <i>cert_name</i>     [--ssl2enabled=<i>false</i>] [--ssl2ciphers <i>ssl2ciphers</i>]     [--ssl3enabled=<i>true</i>] [--tlseabled=<i>true</i>]     [--ssl3tlsciphers <i>ssl3tlsciphers</i>] [--tlscrollbackenabled=<i>true</i>]     [--clientauthenabled=<i>false</i>] [<i>listener_id</i>] </pre>										
<b>DESCRIPTION</b>	<p>Creates and configures the SSL element in the selected HTTP listener, IIOP listener, or IIOP service in order to enable secure communication on that listener/service.</p> <p>This command is supported in remote mode only.</p>										
<b>OPTIONS</b>	<p>If an option has a short option name, then the short option preceeds the long option name. Short options have one dash whereas long options have two dashes.</p> <table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
-u --user	The authorized domain application server administrative username.										
-w --password	The --password option is deprecated. Use --passwordfile instead.										
--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.										
-H --host	The machine name where the domain application server is running. The default value is localhost.										
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.										

<code>-s --secure</code>	If set to true, uses SSL/TLS to communicate with the domain application server.
<code>-t --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>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
<code>-h --help</code>	Displays the help text for the command.
<code>--target</code>	In Enterprise Edition, specifies the target to which you are deploying. Valid values are <ul style="list-style-type: none"> <li>■ <i>server</i>, the server in which the iiop-service or listener is to be configured for SSL.</li> <li>■ <i>config</i>, the configuration that contains the listener or iiop-service for which SSL is to be configured.</li> <li>■ <i>cluster</i>, the cluster in which the listener or iiop-service is to be configured for SSL. All the server instances in the cluster will get the SSL configuration for the respective listener or iiop-service.</li> <li>■ <i>instance</i>, the instance in which the listener or iiop-service is to be configured for SSL.</li> </ul> <p>The following optional attribute name/value pairs are available:</p>

Property	Definition
type	The type of service or listener for which the SSL is created. The type can be <i>http-listener</i> , <i>iiop-listener</i> , or <i>iiop-service</i> .
certname	The nickname of the server certificate in the certificate database or the PKCS#11 token. The format of the name in the certificate is <i>tokenname:nickname</i> . For this property, the <i>tokenname</i> is optional.

create-ssl(1)

Property	Definition
ssl2enabled	Set this property to <i>true</i> to enable SSL2. The default value is <i>false</i> . If both SSL2 and SSL3 are enabled for a virtual server, the server tries SSL3 encryption first. In the event SSL3 encryption fails, the server then tries SSL2 encryption.
ssl2ciphers	A comma-separated list of the SSL2 ciphers to be used. Use the prefix + to enable or – to disable a particular cipher. Allowed values are: <i>rc4</i> , <i>rc4export</i> , <i>rc2</i> , <i>rc2export</i> , <i>idea</i> , <i>des</i> , and <i>desede3</i> . If no value is specified, all supported ciphers are assumed to be enabled.
ssl3enabled	Set this property to <i>false</i> to disable SSL3. The default value is <i>true</i> . If both SSL2 and SSL3 are enabled for a virtual server, the server tries SSL3 encryption first. In the event SSL3 encryption fails, the server then tries SSL2 encryption.
tlseabled	Set this property to <i>false</i> to disable TLS. The default value is <i>true</i> . It is good practice to enable TLS, which is a more secure version of SSL.

Property	Definition
ssl3tlsciphers	A comma-separated list of the SSL3 and/or TLS ciphers to be used. Use the prefix + to enable or – to disable a particular cipher. Allowed SSL3 values are <i>rsa_rc4_128_md5</i> , <i>rsa3des_sha</i> , <i>rsa_des_sha</i> , <i>rsa_rc4_40_md5</i> , <i>rsa_rc2_40_md5</i> , and <i>rsa_null_md5</i> . Allowed TLS values are <i>rsa_des_56_sha</i> and <i>rsa_rc4_56_sha</i> . If no value is specified, all supported ciphers are assumed to be enabled.
tlsrollbackenabled	Set to <i>true</i> (default) to enable TLS rollback. TLS rollback should be enabled for Microsoft Internet Explorer 5.0 and 5.5. This option is only valid in the Enterprise Edition. This option is only valid when <i>tlsenabled=true</i> .
clientauthenabled	Set to <i>true</i> if you want SSL3 client authentication performed on every request independent of ACL-based access control. Default value is <i>false</i> .

**OPERANDS**    *listener\_id*

The ID of the listener for which the SSL element is to be created. The *listener\_id* is not required if the *—type* is *iiop-service*.

**EXAMPLES**    **EXAMPLE 1** Using create-ssl

The following example shows how to create an SSL element for an HTTP listener named *http-listener-1*.

```
asadmin> create-ssl --user admin --host fuyako --port 7070
--passwordfile adminpassword.txt --type http-listener --certname sampleCert http-listener-1
Created SSL in HTTP Listener
```

**EXIT STATUS**    0

command executed successfully

create-ssl(1)

1

error in executing the command

**SEE ALSO** [delete-ssl\(1\)](#)



## create-system-properties(1)

NAME	create-system-properties – adds or updates one or more system properties of the domain, configuration, cluster, or server instance	
SYNOPSIS	<b>create-system-properties</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ]         [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s]         [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help]         [--target <i>target_name</i> ] [ <i>name=value</i> ] [: <i>name=value</i> ] *]	
DESCRIPTION	Shared or clustered server instances will often need to override attributes defined in their referenced configuration. Any configuration attribute in a server instance can be overridden through a system property of the corresponding name. This command adds or updates the system properties of a domain, configuration, cluster, or server instance.	
OPTIONS	-u --user -w --password --passwordfile -H --host -p --port -s --secure	<p>The authorized domain application server administrative username.</p> <p>The --password option is deprecated. Use --passwordfile instead.</p> <p>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</p> <p>The machine name where the domain application server is running. The default value is localhost.</p> <p>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</p> <p>If set to true, uses SSL/TLS to communicate with the domain application server.</p>

## create-system-properties(1)

	-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.
	-h --help	Displays the help text for the command.
	--target	In Enterprise Edition, specifies the target on which you are creating the system properties. The valid targets for this command are instance, cluster, configuration, 'domain,' and 'server.' Server is the default option.
OPERANDS	<i>name=value</i>	The name value pairs (separated by the ":" character) of the system properties to add to the specified target. If any of the system properties were previously defined, it will be updated with the newly specified value.
EXAMPLES	<b>EXAMPLE 1</b> Using create-system-properties <pre>asadmin&gt; create-system-properties --user admin --passwordfile password.txt --host localhost --port 4849 --target mycluster http-listener-port=1088</pre> Command create-system-properties executed successfully.	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">delete-system-property(1)</a> , <a href="#">list-system-properties(1)</a>	

NAME	create-threadpool – adds a threadpool												
SYNOPSIS	<pre><b>create-threadpool</b> --user <i>admin_user</i> [--passwordfile <i>filename</i>]     [--host <i>host_name</i>] [--port <i>port_number</i>] [--secure -s]     [--terse=false] [--echo=false] [--interactive=true] [--help]     [--target <i>target_name</i>] [--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>												
DESCRIPTION	<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 IIOP 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>												
OPTIONS	<table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td>-s --secure</td><td>If set to true, uses SSL/TLS to communicate with the domain application server.</td></tr> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	-s --secure	If set to true, uses SSL/TLS to communicate with the domain application server.
-u --user	The authorized domain application server administrative username.												
-w --password	The --password option is deprecated. Use --passwordfile instead.												
--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.												
-H --host	The machine name where the domain application server is running. The default value is localhost.												
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.												
-s --secure	If set to true, uses SSL/TLS to communicate with the domain application server.												

## create-threadpool(1)

	-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.
	-h --help	Displays the help text for the command.
	--target	In Enterprise Edition, specifies the target on which you are creating the threadpool. Valid values are <ul style="list-style-type: none"> <li>■ <i>server</i>, which creates the listener for the default server instance <i>server</i> and is the default value</li> <li>■ <i>configuration_name</i>, which creates the listener for the named configuration</li> <li>■ <i>cluster_name</i>, which creates the listener for every server instance in the cluster</li> <li>■ <i>instance_name</i>, which creates the listener for a particular server instance</li> </ul>
	--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.
	--workqueues	identifies the total number of work queues serviced by this threadpool.
OPERANDS	<i>threadpool_id</i>	an ID for the work queue; for example, thread-pool-1, thread-pool-2, etc.
EXAMPLES	<b>EXAMPLE 1</b> Using create-threadpool <pre>asadmin&gt; create-threadpool --user admin1 --passwordfile password.txt --maxthreadpoolsize 100 --minthreadpoolsize 20 --idletimeout 2 --workqueues 100 threadpool-1</pre> <p>Command create-threadpool executed successfully</p>	
EXIT STATUS	0	command executed successfully

create-threadpool(1)

- 1  
error in executing the command

SEE ALSO [delete-threadpool\(1\)](#), [list-threadpools\(1\)](#)

## create-virtual-server(1)

NAME	create-virtual-server – creates the named virtual server										
SYNOPSIS	<pre><b>create-virtual-server</b> --user <i>admin_user</i> [--passwordfile <i>filename</i>]   [--host <i>host_name</i>] [--port <i>port_number</i>] [--secure -s]   [--terse=false] [--echo=false] [--interactive=true] [--help]   [--target <i>server</i>] --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>										
DESCRIPTION	<p>The create-virtual-server command creates the named virtual server. Virtualization in the Application Server allows multiple URL domains to be served by a single HTTP server process that 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>										
OPTIONS	<table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
-u --user	The authorized domain application server administrative username.										
-w --password	The --password option is deprecated. Use --passwordfile instead.										
--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.										
-H --host	The machine name where the domain application server is running. The default value is localhost.										
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.										

## create-virtual-server(1)

<code>-s --secure</code>	If set to true, uses SSL/TLS to communicate with the domain application server.
<code>-t --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>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
<code>-h --help</code>	Displays the help text for the command.
<code>--target</code>	In Enterprise Edition, specifies the target for which you are creating the virtual server. Valid values are <ul style="list-style-type: none"> <li>■ <code>server</code>, which creates the virtual server for the default server instance <code>server</code> and is the default value</li> <li>■ <code>configuration_name</code>, which creates the virtual server for the named configuration</li> <li>■ <code>cluster_name</code>, which creates the virtual server for every server instance in the cluster</li> <li>■ <code>instance_name</code>, which creates the virtual server for a particular server instance</li> </ul>
<code>--hosts</code>	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.
<code>--httplisteners</code>	A comma-separated (,) list of HTTP listener IDs. Required only for a virtual server that is not the default virtual server.
<code>--defaultwebmodule</code>	The 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 log entries for this virtual server are to be written. By default, this is the server log.
<code>--property</code>	Optional attribute name/value pairs for configuring the virtual server. The following properties are available:

create-virtual-server(1)

**OPERANDS**

*virtual\_server\_id*

Property	Definition
docroot	Absolute path to root document directory for server.
accesslog	Absolute path to server access logs.
sso-enabled	If false, single sign-on is disabled for this virtual server, and users must authenticate separately to every application on the virtual server. Single sign-on across applications on the Application Server is supported by servlets and JSP pages. This feature allows multiple applications that require the same user sign-on information to share this information, rather than have the user sign on separately for each application. Default is true.
sso-max-inactive-seconds	Specifies the number of seconds after which a user's single sign-on record becomes eligible for purging if no client activity is received. Since single sign-on applies across several applications on the same virtual server, access to any of the applications keeps the single sign-on record active. Default is 300 seconds (5 minutes). Higher values provide longer single sign-on persistence for users at the expense of more memory use on the server.
sso-reap-interval-seconds	Specifies the number of seconds between purges of expired single sign-on records. Default is 60.

Identifies the unique ID for the virtual server to be created. This ID cannot begin with a number.



**EXAMPLES**    **EXAMPLE 1** Using the create-virtual-server command

The following command creates a virtual server named sampleServer:

```
asadmin> create-virtual-server --user admin1
--passwordfile passwords.txt --hosts pigeon,localhost sampleServer
Command create-virtual-server executed successfully.
```

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

**SEE ALSO**    [delete-virtual-server\(1\)](#), [list-virtual-servers\(1\)](#),  
[create-http-listener\(1\)](#)

## delete-acl(1)

NAME	delete-acl – removes the access control list file
SYNOPSIS	<b>delete-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> ] <i>acl_ID</i>
DESCRIPTION	Gets the access control lists associated with the named server instance..
OPTIONS	--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.
OPERANDS	<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.
EXAMPLES	<p><b>EXAMPLE 1</b> Using delete-acl</p> <pre>asadmin&gt; delete-acl --user admin --password adminadmin --host fuyako --port 7070 --instance server1</pre> <p>Deleted ACL with id = sampleACL</p> <p>Where: sampleACL is the ACL that is deleted.</p>
EXIT STATUS	0 command executed successfully 1 error in executing the command
INTERFACE EQUIVALENT	Access Control List page
SEE ALSO	<a href="#">create-acl(1)</a> , <a href="#">list-acl(1)</a>

NAME	delete-admin-object – removes the administered object with the specified JNDI name
SYNOPSIS	<b>delete-admin-object</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--target <i>target</i> ] <i>jndi_name</i>
DESCRIPTION	This command removes the administered object with the specified JNDI name.
OPTIONS	<div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>--passwordfile</div> <div>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </div> </div> <div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> </div> <div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> </div> <div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> </div> <div> <div>-t --terse</div> <div>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.</div> </div> <div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div> </div>

## delete-admin-object-1(1)

	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
	<code>--target</code>	This is the name of the target upon which the command is operating. The valid targets for this command are instance, cluster, 'domain,' and 'server.' Server is the default option. This command is used by the Enterprise Edition only.
<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-object --user admin --password admin123 --target instance1 jms/samplequeue Command delete-admin-object executed successfully</pre>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">create-admin-object(1)</a> , <a href="#">list-admin-objects(1)</a>	

NAME	create-audit-module – removes the named audit-module
SYNOPSIS	<b>delete-audit-module</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--target <i>target_name</i> ] [ <i>audit_module_name</i> ]
DESCRIPTION	Removes the named audit module. This command is supported in remote mode only.
OPTIONS	<p>-u --user                   The authorized domain application server administrative username.</p> <p>-w --password              The --password option is deprecated. Use --passwordfile instead.</p> <p>--passwordfile            This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</p> <p>-H --host                  The machine name where the domain application server is running. The default value is localhost.</p> <p>-p --port                  The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</p> <p>-s --secure                If set to true, uses SSL/TLS to communicate with the domain application server.</p> <p>-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.</p> <p>-e --echo                  Setting to true will echo the command line statement on the standard output. Default is false.</p> <p>-I --interactive           If set to true (default), only the required password options are prompted.</p>

## delete-audit-module(1)

	<code>-h --help</code>	Displays the help text for the command.
	<code>--target</code>	<p>In Enterprise Edition, specifies the target on which you are deleting the audit module. Valid values are</p> <ul style="list-style-type: none"><li>■ <code>server</code>, which creates the listener for the default server instance <code>server</code> and is the default value</li><li>■ <code>configuration_name</code>, which creates the listener for the named configuration</li><li>■ <code>cluster_name</code>, which creates the listener for every server instance in the cluster</li><li>■ <code>instance_name</code>, which creates the listener for a particular server instance</li></ul>
OPERANDS	<code>audit_module_name</code>	name of the audit module to be deleted.
EXAMPLES	<p><b>EXAMPLE 1</b> Using delete-audit-module</p> <pre>asadmin&gt; delete-audit-module --user admin1 --passwordfile password.txt --host pigeon --port 5001 sampleAuditModule</pre> <p>Command delete-audit-module executed successfully</p>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<code>create-audit-module(1)</code> , <code>list-audit-modules(1)</code>	

NAME	delete-auth-realm – removes the named authentication realm	
SYNOPSIS	<b>delete-auth-realm</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--target <i>target_name</i> ] { <i>auth_realm-name</i> }	
DESCRIPTION	Removes the named authorized realm. This command is supported in remote mode only.	
OPTIONS	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
	-H --host	The machine name where the domain application server is running. The default value is localhost.
	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	-s --secure	If set to 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.

## delete-auth-realm(1)

	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
	<code>--target</code>	<p>In Enterprise Edition, specifies the target on which you are deleting the authentication realm. Valid values are</p> <ul style="list-style-type: none"><li>■ <code>server</code>, which creates the listener for the default server instance <code>server</code> and is the default value</li><li>■ <code>configuration_name</code>, which creates the listener for the named configuration</li><li>■ <code>cluster_name</code>, which creates the listener for every server instance in the cluster</li><li>■ <code>instance_name</code>, which creates the listener for a particular server instance</li></ul>
OPERANDS	<code>auth_realm_name</code>	name of this realm.
EXAMPLES	<p><b>EXAMPLE 1</b> Using delete-auth-realm</p> <pre>asadmin&gt; delete-auth-realm --user admin1 --passwordfile password.txt --host pigeon --port 5001 db</pre> <p>Command delete-auth-realm executed successfully</p> <p>Where db is the authentication realm deleted.</p>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-auth-realm(1)</a> , <a href="#">list-auth-realms(1)</a>	



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

NAME	delete-connector-connection-pool – removes the specified connector connection pool	
SYNOPSIS	<b>delete-connector-connection-pool</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--cascade= <i>false</i> ] <i>connector_connection_pool_name</i>	
DESCRIPTION	Removes the specified connector connection pool. This command is supported in remote mode only.	
OPTIONS	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
	-H --host	The machine name where the domain application server is running. The default value is localhost.
	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	-s --secure	If set to 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.

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

	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
	<code>--cascade</code>	When set to true, it deletes all connector resources associated with the pool that is named as operand, apart from the pool itself. When set to false, the deletion of pool fails if any resources are associated with the pool. The resource must be deleted explicitly or the option must be set to true. The default setting is false.
<b>OPERANDS</b>	<i>connector_connection_pool_name</i> The name of the connection pool to be removed.	
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using the delete-connector-connection-pool command <pre>asadmin&gt; delete-connector-connection-pool --cascade=false jms/qConnPool</pre> Command delete-connector-connection-pool executed successfully  Where jms/qConnPool is the connector connection pool that is removed.	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">create-connector-connection-pool(1)</a> , <a href="#">list-connector-connection-pools(1)</a>	

NAME	delete-connector-resource – removes the connector resource with the specified JNDI name
SYNOPSIS	<b>delete-connector-resource</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--target <i>target</i> ] <i>jndi_name</i>
DESCRIPTION	This delete-connector-resource command removes the connector resource with the JNDI name, which is specified by the <i>jndi_name</i> operand.
OPTIONS	<p>-u --user                      The authorized domain application server administrative username.</p> <p>-w --password                The --password option is deprecated. Use --passwordfile instead.</p> <p>--passwordfile              This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</p> <p>-H --host                    The machine name where the domain application server is running. The default value is localhost.</p> <p>-p --port                    The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</p> <p>-s --secure                 If set to true, uses SSL/TLS to communicate with the domain application server.</p> <p>-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.</p>

## delete-connector-resource(1)

	<code>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
	<code>--target</code>	valid in Enterprise Edition only, specifies the target to which you are deploying. Valid values are 'server,' 'domain,' cluster, instance.
	<code>--poolname</code>	The name of the connection pool. When two or more resource elements point to the same connection pool element, they use the same pool connections at runtime.
	<code>--enabled</code>	This option determines whether the resource is enabled at runtime. The default value is true.
	<code>--description</code>	Text providing descriptive details about the connector resource.
<b>OPERANDS</b>	<i>jndi_name</i>	the JNDI name of this connector resource.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the delete-connector-resource command</p> <pre>asadmin&gt; delete-connector-resource --target server jms/qConnFactory --passwordfile file1</pre> <p>Command delete-connector-resource executed successfully</p> <p>Where jms/qConnFactory is the connector resource that is removed.</p>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">create-connector-resource(1)</a> , <a href="#">list-connector-resources(1)</a>	

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

<b>NAME</b>	delete-connector-security-map – deletes a security map for the specified connector connection pool								
<b>SYNOPSIS</b>	<pre><b>delete-connector-security-map</b> --user <i>admin_user</i> [<b>--passwordfile</b> <i>filename</i>] [<b>--host</b> <i>host_name</i>] [<b>--port</b> <i>port_number</i>] [<b>--secure</b> -s] [<b>--terse</b>=false] [<b>--echo</b>=false] [<b>--interactive</b>=true] [<b>--help</b>] --poolname <i>connector_connection_pool_name</i> <i>security_map_name</i></pre>								
<b>DESCRIPTION</b>	<p>Use this command to delete a security map for the specified connector connection pool.</p> <p>For this command to succeed, you must have first created a connector connection pool using the <code>create-connector-connection-pool</code> command.</p> <p>The enterprise information system (EIS) is any system that holds the information. It can be a mainframe, a messaging system, a database system, or an application.</p> <p>This command is supported in remote mode only.</p>								
<b>OPTIONS</b>	<p>If an option has a short option name, then the short option precedes the long option name. Short options have one dash whereas long options have two dashes.</p> <table> <tr> <td><code>-u --user</code></td><td>The authorized domain application server administrative username.</td></tr> <tr> <td><code>-w --password</code></td><td>The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.</td></tr> <tr> <td><code>--passwordfile</code></td><td>This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code>, <code>AS_ADMIN_USERPASSWORD</code>, <code>AS_ADMIN_SAVEDMASTERPASSWORD</code>, <code>AS_ADMIN_MQPASSWORD</code>, <code>AS_ADMIN_ALIASPASSWORD</code>, and so on.</td></tr> <tr> <td><code>-H --host</code></td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> </table>	<code>-u --user</code>	The authorized domain application server administrative username.	<code>-w --password</code>	The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.	<code>--passwordfile</code>	This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code> , <code>AS_ADMIN_USERPASSWORD</code> , <code>AS_ADMIN_SAVEDMASTERPASSWORD</code> , <code>AS_ADMIN_MQPASSWORD</code> , <code>AS_ADMIN_ALIASPASSWORD</code> , and so on.	<code>-H --host</code>	The machine name where the domain application server is running. The default value is localhost.
<code>-u --user</code>	The authorized domain application server administrative username.								
<code>-w --password</code>	The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.								
<code>--passwordfile</code>	This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code> , <code>AS_ADMIN_USERPASSWORD</code> , <code>AS_ADMIN_SAVEDMASTERPASSWORD</code> , <code>AS_ADMIN_MQPASSWORD</code> , <code>AS_ADMIN_ALIASPASSWORD</code> , and so on.								
<code>-H --host</code>	The machine name where the domain application server is running. The default value is localhost.								

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

	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	-s --secure	If set to 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.
	-h --help	Displays the help text for the command.
	--target	This option is deprecated in this release.
	--poolname	This property specifies the name of the connector connection pool to which the security map that is to be deleted belongs.
<b>OPERANDS</b>	<i>security_map_name</i>	name of the security map to be deleted.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using delete-connector-security-map</p> <p>It is assumed that the connector pool has already been created using the create-connector-pool command.</p> <pre>asadmin&gt; delete-connector-security-map --user admin --passwordfile pwd_file.txt --poolname connector-pool1 securityMap1</pre> <p>Command delete-connector-security-map executed successfully</p>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">create-connector-security-map(1)</a> , <a href="#">list-connector-security-maps(1)</a> , <a href="#">update-connector-security-map(1)</a>	

NAME	delete-custom-resource – removes a custom resource
SYNOPSIS	<b>delete-custom-resource</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--target <i>target</i> ] <i>jndi_name</i>
DESCRIPTION	The delete-custom-resource command removes a custom resource. This command is supported in remote mode only.
OPTIONS	<div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>--passwordfile</div> <div>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </div> </div> <div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> </div> <div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> </div> <div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> </div> <div> <div>-t --terse</div> <div>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.</div> </div> <div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div> </div>

## delete-custom-resource(1)

	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
	<code>--target</code>	valid in Enterprise Edition only, this command, specifies the location of the custom resources that you are deleting. Valid values are 'server,' ,domain,' cluster, and instance. The default is server.
OPERANDS	<i>jndi_name</i>	the JNDI name of this resource.
EXAMPLES	<b>EXAMPLE 1</b> Using the delete-custom-resource command <pre>asadmin&gt; delete-custom-resource --target plum jndi_name_test --passwordfile file1</pre> Command delete-custom-resource executed correctly.	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-custom-resource(1)</a> , <a href="#">list-custom-resources(1)</a>	



<b>NAME</b>	delete-domain – deletes the given domain
<b>SYNOPSIS</b>	<b>delete-domain</b> [--domaindir <i>install_dir</i> /domains] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] <i>domain_name</i>
<b>DESCRIPTION</b>	<p>Use the delete-domain command to delete the named domain. The domain must already exist and must be stopped.</p> <p>This command is supported in local mode only.</p>
<b>OPTIONS</b>	<p>--domaindir                      The directory where the domain to be deleted is located. If specified, the path must be accessible in the filesystem. If not specified, the domain in the default <i>install_dir</i>/domains directory is deleted.</p> <p>-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.</p> <p>-e --echo                         Setting to true will echo the command line statement on to the standard output. Default is false.</p> <p>-I --interactive                 If set to true (default), only the required options are prompted.</p>
<b>OPERANDS</b>	<i>domain_name</i> The unique name of the domain you wish to delete.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the delete-domain command</p> <pre>asadmin&gt; delete-domain --domaindir /export/domains sampleDomain deleted domain sampleDomain successfully</pre> <p>Where: the sampleDomain domain is deleted from the /export/domains directory.</p>
<b>EXIT STATUS</b>	<p>0   command executed successfully</p> <p>1   error in executing the command</p>
<b>SEE ALSO</b>	<a href="#">create-domain(1)</a> , <a href="#">start-domain(1)</a> , <a href="#">stop-domain(1)</a> , <a href="#">list-domains(1)</a>

## delete-file-user(1)

NAME	delete-file-user – removes the named file user
SYNOPSIS	<b>delete-file-user</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--target <i>target</i> ] <i>username</i>
DESCRIPTION	Deletes the entry in the keyfile with the specified username.
OPTIONS	<div>-u --user</div> <div>The authorized domain application server administrative username.</div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> <div>--passwordfile</div> <div>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> <div>-t --terse</div> <div>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.</div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div>

		delete-file-user(1)
	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
	--target	This is used for Enterprise Edition only. This is the name of the target on which the command operates. The valid targets are config, instance, cluster, or "server." By default, the target is the "Server."
OPERANDS	<i>username</i>	This is the name of file user to be deleted.
EXAMPLES	<p><b>EXAMPLE 1</b> Using the delete-file-user command</p> <p>It is assumed that an authority realm has already been created using the create-auth-realm command.</p> <pre>asadmin&gt; delete-file-user --user admin1 --password adminadmin1 --host pigeon --port 5001 --username admin1</pre> <p>Command delete-file-user executed successfully</p>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-file-user(1)</a> , <a href="#">list-file-users(1)</a> , <a href="#">update-file-user(1)</a> , <a href="#">list-file-groups(1)</a>	

## delete-http-listener(1)

NAME	delete-http-listener – removes an HTTP listener
SYNOPSIS	<b>delete-http-listener</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--target <i>server</i> ] <i>listener_id</i>
DESCRIPTION	The delete-http-listener command removes the specified HTTP listener. This command is supported in remote mode only.
OPTIONS	<div>-u --user</div> <div>The authorized domain application server administrative username.</div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> <div>--passwordfile</div> <div>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> <div>-t --terse</div> <div>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.</div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div>

	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
	<code>--target</code>	<p>In Enterprise Edition, specifies the target from which you are deleting the HTTP listener. Valid values are</p> <ul style="list-style-type: none"><li>■ <code>server</code>, which deletes the listener from the default server instance <code>server</code> and is the default value</li><li>■ <code>configuration_name</code>, which deletes the listener from the named configuration</li><li>■ <code>cluster_name</code>, which deletes the listener from every server instance in the cluster</li><li>■ <code>instance_name</code>, which deletes the listener from a particular server instance</li></ul>
OPERANDS	<code>listener_id</code>	The unique identifier for the HTTP listener to be deleted.
EXAMPLES	<p><b>EXAMPLE 1</b> Using the <code>delete-http-listener</code> command</p> <p>The following command deletes the HTTP listener named <code>sampleListener</code>:</p> <pre>asadmin&gt; delete-http-listener --user admin1 --passwordfile passwords.txt --host pigeon --port 5001 sampleListener</pre> <p>Command <code>delete-http-listener</code> executed successfully.</p>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-http-listener(1)</a> , <a href="#">list-http-listeners(1)</a>	

## delete-iiop-listener(1)

NAME	delete-iiop-listener – removes an IIOP listener
SYNOPSIS	<b>delete-iiop-listener</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--target <i>server</i> ] <i>listener_id</i>
DESCRIPTION	The delete-iiop-listener command removes the specified IIOP listener. This command is supported in remote mode only.
OPTIONS	<div>-u --user</div> <div>The authorized domain application server administrative username.</div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> <div>--passwordfile</div> <div>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> <div>-t --terse</div> <div>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.</div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div>

	delete-iiop-listener(1)	
	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
	--target	In Enterprise Edition, specifies the target from which you are deleting the IIOP listener. Valid values are <ul style="list-style-type: none"> <li>■ <i>server</i>, which deletes the listener from the default server instance <i>server</i> and is the default value</li> <li>■ <i>configuration_name</i>, which deletes the listener from the named configuration</li> <li>■ <i>cluster_name</i>, which deletes the listener from every server instance in the cluster</li> <li>■ <i>instance_name</i>, which deletes the listener from a particular server instance</li> </ul>
OPERANDS	<i>listener_id</i>	The unique identifier for the IIOP listener to be deleted.
EXAMPLES	<p><b>EXAMPLE 1</b> Using the delete-iiop-listener command</p> <p>The following command deletes the IIOP listener named <i>sample_iiop_listener</i>:</p> <pre>asadmin&gt; delete-iiop-listener --user admin --passwordfile passwords.txt --host fuyako --port 7070 sample_iiop_listener</pre> <p>Command delete-iiop-listener executed successfully.</p>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	create-iiop-listener(1), list-iiop-listeners(1)	

## delete-instance(1)

NAME	delete-instance – deletes the instance that is not running												
SYNOPSIS	<b>delete-instance</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] <i>instance_name</i>												
DESCRIPTION	<p>Use the delete-instance command to delete the instance that you specify. The delete-instance command can be run both locally and remotely. 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.</p>												
OPTIONS	<table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td> <p>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</p> </td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td>-s --secure</td><td>If set to true, uses SSL/TLS to communicate with the domain application server.</td></tr> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	<p>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</p>	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	-s --secure	If set to true, uses SSL/TLS to communicate with the domain application server.
-u --user	The authorized domain application server administrative username.												
-w --password	The --password option is deprecated. Use --passwordfile instead.												
--passwordfile	<p>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</p>												
-H --host	The machine name where the domain application server is running. The default value is localhost.												
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.												
-s --secure	If set to true, uses SSL/TLS to communicate with the domain application server.												



	<div><div>-t --terse</div><div>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.</div></div>
	<div><div>-e --echo</div><div>Setting to true will echo the command line statement on the standard output. Default is false.</div></div>
	<div><div>-I --interactive</div><div>If set to true (default), only the required password options are prompted.</div></div>
	<div><div>-h --help</div><div>Displays the help text for the command.</div></div>
OPERANDS	<div><div><i>instance_name</i></div><div>name of the instance to be deleted.</div></div>
EXAMPLES	<div><div><b>EXAMPLE 1</b> Using delete-instance in local mode</div><div>asadmin&gt; <b>delete-instance --user admin1 --passwordfile passwords.txt instance1</b></div><div>Command delete-instance executed successfully</div><div>Where: instance1 is deleted on the local machine.</div><div><b>EXAMPLE 2</b> Using delete-instance in remote mode</div><div>asadmin&gt; <b>delete-instance --user admin --passwordfile passwords.txt --host pigeon --port 4849 instance2</b></div><div>Deleted Instance server1 successfully</div><div>Where: instance2 is deleted on the remote machine.</div></div>
EXIT STATUS	<div><div>0</div><div>command executed successfully</div><div>1</div><div>error in executing the command</div></div>
SEE ALSO	<div><div><a href="#">create-instance(1)</a>, <a href="#">start-instance(1)</a>, <a href="#">stop-instance(1)</a></div></div>

## delete-javamail-resource(1)

NAME	delete-javamail-resource – removes a JavaMail session resource	
SYNOPSIS	<b>delete-javamail-resource</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--target <i>target</i> ] <i>jndi_name</i>	
DESCRIPTION	The delete-javamail-resource command removes the specified JavaMail session resource. For Enterprise Edition, make sure to remove all references to this resource before executing this command. This command is supported in remote mode only.	
OPTIONS	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
	-H --host	The machine name where the domain application server is running. The default value is localhost.
	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	-s --secure	If set to 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.

## delete-javamail-resource(1)

	<code>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
	<code>--target</code>	In Enterprise Edition, specifies the target from which you are deleting the JavaMail session resource. Valid values are <ul style="list-style-type: none"><li>■ <code>server</code>, which deletes the resource from the default server instance <code>server</code> and is the default value</li><li>■ <code>domain</code>, which deletes the resource from the domain</li><li>■ <code>cluster_name</code>, which deletes the resource from every server instance in the cluster</li><li>■ <code>instance_name</code>, which deletes the resource from a particular server instance</li></ul>
OPERANDS	<i>jndi_name</i>	The JNDI name of the JavaMail session resource to be deleted.
EXAMPLES	<b>EXAMPLE 1</b> Using the delete-javamail-resource command  The following command deletes the JavaMail session resource named mail/MyMailSession:  <pre>asadmin&gt; delete-javamail-resource --user admin --passwordfile passwords.txt --host fuyako --port 7070 mail/MyMailSession</pre> Command delete-javamail-resource executed successfully.	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-javamail-resource(1)</a> , <a href="#">list-javamail-resources(1)</a>	

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

NAME	delete-jdbc-connection-pool – removes the specified JDBC connection pool
SYNOPSIS	<b>delete-jdbc-connection-pool</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--cascade=false] <i>connectionpoolid</i>
DESCRIPTION	Removes a specified JDBC connection pool that was previously created with the creat-jdbc-connection command. The operand identifies the JDBC connection pool to be deleted. This command is supported in remote mode only.
OPTIONS	<div>-u --user</div> <div>The authorized domain application server administrative username.</div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> <div>--passwordfile</div> <div>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASEXPASSWORD, and so on.</div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> <div>-t --terse</div> <div>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.</div>

		delete-jdbc-connection-pool(1)
	-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.
	-h --help	Displays the help text for the command.
	--cascade	If the option is set to true, all the connector resources associated with the pool (mentioned as operand) apart from the pool itself are deleted. When set to false, the deletion of pool fails if any resources are associated with the pool. Resources must be deleted explicitly or the option must be set to true. By default, the option is false.
OPERANDS	<i>connectionpoolid</i>	the name of the JDBC resource to be removed.
EXAMPLES	<p><b>EXAMPLE 1</b> Using the delete-jdbc-connection-pool command</p> <pre>asadmin&gt; delete-jdbc-connection-pool --passwordfile file1 --user u1 --cascade=false connection_pool_01</pre> <p>Command delete-jdbc-connection-pool executed correctly.</p> <p>Where: asadmin is the command prompt and connection_pool_01 is the connection pool to be removed.</p>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	create-jdbc-connection-pool(1),list-jdbc-connection-pools(1)	

## delete-jdbc-resource(1)

NAME	delete-jdbc-resource – removes a JDBC resource with the specified JNDI name
SYNOPSIS	<b>delete-jdbc-resource</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--target <i>target</i> ] <i>jndi_name</i>
DESCRIPTION	The delete-jdbc-resource comand removes a JDBC resource. This command is supported in remote mode only.
OPTIONS	<div>-u --user</div> <div>The authorized domain application server administrative username.</div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> <div>--passwordfile</div> <div>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> <div>-t --terse</div> <div>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.</div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div>

		delete-jdbc-resource(1)
	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
	--target	valid in Enterprise Edition only, specifies the target to which you are deploying. Valid values are 'server,' 'domain,' cluster, or instance. The default is server.
OPERANDS	<i>jndi_name</i>	the JNDI name of this JDBC resource to be removed.
EXAMPLES	<p><b>EXAMPLE 1</b> Using the delete-jdbc-resource command</p> <pre>asadmin&gt; delete-jdbc-resource --passwordfile pass1 --user u1 --target plum test_jdbc_resource</pre> <p>Command delete-jdbc-resource executed successfully.</p> <p>Where asadmin is the command prompt and test_jdbc_resource is the name of the JDBC resource that is removed.</p>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	create-jdbc-resource(1), list-jdbc-resources(1)	

## delete-jmsdest(1)

NAME	delete-jmsdest – removes a physical destination
SYNOPSIS	<b>delete-jmsdest</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--target <i>target</i> ] --desttype <i>type</i> <i>dest_name</i>
DESCRIPTION	The delete-jmsdest command removes the specified physical destination. This command is supported in remote mode only.
OPTIONS	<div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>--passwordfile</div> <div>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </div> </div> <div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> </div> <div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> </div> <div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> </div> <div> <div>-t --terse</div> <div>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.</div> </div> <div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div> </div>



## delete-jmsdest(1)

	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
	--target	In Enterprise Edition, specifies the target from which you are deleting the physical destination. Although the <code>delete-jmsdest</code> command is related to resources, a physical destination is created and deleted using the JMS Service, which is part of the configuration. Valid values are <ul style="list-style-type: none"> <li>■ <code>server</code>, which deletes the physical destination from the default server instance <code>server</code> and is the default value</li> <li>■ <code>configuration_name</code>, which deletes the physical destination from the named configuration</li> <li>■ <code>cluster_name</code>, which deletes the physical destination from every server instance in the cluster</li> <li>■ <code>instance_name</code>, which deletes the physical destination from a particular server instance</li> </ul>
	-T --desttype	The type of the JMS destination. Valid values are <code>topic</code> and <code>queue</code> .
OPERANDS	<i>dest_name</i>	The unique identifier of the the JMS destination to be deleted.
EXAMPLES	<p><b>EXAMPLE 1</b> Using the <code>delete-jmsdest</code> command</p> <p>The following command deletes the queue named <code>PhysicalQueue</code>:</p> <pre>asadmin&gt; delete-jmsdest --user admin --passwordfile passwords.txt --host localhost --port 4848 --desttype queue PhysicalQueue</pre> <p>Command <code>delete-jmsdest</code> executed successfully.</p>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-jmsdest(1)</a> , <a href="#">list-jmsdest(1)</a>	

## delete-jms-resource(1)

NAME	delete-jms-resource – removes a JMS resource
SYNOPSIS	<b>delete-jms-resource</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--target <i>target</i> ] <i>jndi_name</i>
DESCRIPTION	The delete-jms-resource command removes the specified JMS resource. For Enterprise Edition, make sure to remove all references to this resource before executing this command. This command is supported in remote mode only.
OPTIONS	<div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>--passwordfile</div> <div>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </div> </div> <div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> </div> <div> <div>-p --port</div> <div>           The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.         </div> </div> <div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> </div> <div> <div>-t --terse</div> <div>           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.         </div> </div>

		delete-jms-resource(1)
	-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.
	-h --help	Displays the help text for the command.
	--target	In Enterprise Edition, specifies the target from which you are deleting the JMS resource. Valid values are <ul style="list-style-type: none"> <li>■ <i>server</i>, which deletes the resource from the default server instance <i>server</i> and is the default value</li> <li>■ <i>domain</i>, which deletes the resource from the domain</li> <li>■ <i>cluster_name</i>, which deletes the resource from every server instance in the cluster</li> <li>■ <i>instance_name</i>, which deletes the resource from a particular server instance</li> </ul>
OPERANDS	<i>jndi_name</i>	The JNDI name of the JMS resource to be deleted.
EXAMPLES	<b>EXAMPLE 1</b> Using the delete-jms-resource command The following command deletes the JMS resource named <code>jms/Queue</code> : <pre>asadmin&gt; delete-jms-resource --user admin1 --passwordfile passwords.txt --host pigeon --port 5001 jms/Queue</pre> Command delete-jms-resource executed successfully.	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-jms-resource(1)</a> , <a href="#">list-jms-resources(1)</a>	

## delete-jndi-resource(1)

NAME	delete-jdbc-resource – removes the JNDI resource with the specified JNDI name
SYNOPSIS	<b>delete-jndi-resource</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--target <i>target</i> ] <i>jndi_name</i>
DESCRIPTION	The delete-jndi-resource comand removes the specified JNDI resource. This command is supported in remote mode only.  In Enterprise Edition, you must remove all associations to the JNDI resource before you execute this command.
OPTIONS	<div>-u --user</div> <div>The authorized domain application server administrative username.</div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> <div>--passwordfile</div> <div>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> <div>-t --terse</div> <div>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.</div>

		delete-jndi-resource(1)
	-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.
	-h --help	Displays the help text for the command.
	--target	valid in Enterprise Edition only. Valid values are 'server,' 'domain,' cluster, or instance. The default is 'server.'
OPERANDS	<i>jndi_name</i>	the name of the JNDI resource to be removed.
EXAMPLES	<p><b>EXAMPLE 1</b> Using the delete-jndi-resource command</p> <p>In Enterprise Edition, you must remove all associations to this resource before you execute this command.</p> <pre>asadmin&gt; delete-jndi-resource --passwordfile p1 --user u2 --target plum sample_jndi_resource</pre> <p>Command delete-jndi-resource executed successfully.</p> <p>Where asadmin is the command prompt and sample_jndi_resource is the resource to be removed.</p>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-jndi-resource(1)</a> , <a href="#">list-jndi-resources(1)</a>	

## delete-jvm-options(1)

NAME	delete-jvm-options – removes JVM options from the Java configuration or profiler elements of the domain.xml file	
SYNOPSIS	<b>delete-jvm-options</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--target <i>target</i> ] [--profiler <i>=false</i> ] [ ( <i>jvm_option_name=jvm_option_value</i> ) ] [: <i>jvm_option_name=jvm_option_name</i> ] [*]	
DESCRIPTION	Removes JVM options from the Java configuration or profiler elements of the domain.xml file. NOTE: In the syntax, there can be more than one jvm_option, separated by a colon.	
OPTIONS	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
	-H --host	The machine name where the domain application server is running. The default value is localhost.
	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	-s --secure	If set to true, uses SSL/TLS to communicate with the domain application server.

	delete-jvm-options(1)	
	-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.
	-h --help	Displays the help text for the command.
	--target	valid in Enterprise Edition only, specifies the target to which you are deploying. Valid values are 'server,' 'domain,' cluster, or instance. The default is server.
	--profiler	indicates whether the JVM options are for the profiler. The profiler must exist for this option to be true.
OPERANDS	<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 JVM option value. A colon (:) is a delimiter for multiple options.
EXAMPLES	<p><b>EXAMPLE 1</b> Using the delete-jvm-options command</p> <p>To remove more than one JVM option, use a colon (:) to separate the options. If the JVM option itself contains a colon (:), use the backslash (\) to offset the colon (:) delimiter.</p> <pre>asadmin&gt; delete-jvm-options -e \-Dtmp=sun --interactive=true --secure=true --passwordfile /password --terse=false --user admin --target server --host localhost --echo=true --port 4849 \-Dtmp=sun Command delete-jvm-options executed successfully</pre> <p>Where the JVM options are deleted.</p> <pre>asadmin&gt; delete-jvm-options -e \-Doption1=value1 --interactive=true --secure=true --passwordfile /password --terse=false --user admin --target server --host localhost --echo=true --port 4849 \-Doption1=value1 Command delete-jvm-options executed successfully</pre>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-jvm-option(1)</a>	

## delete-lifecycle-module(1)

NAME	delete-lifecycle-module – removes the lifecycle module
SYNOPSIS	<b>delete-lifecycle-module</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--target <i>target</i> ] <i>module_name</i>
DESCRIPTION	Removes the lifecycle module. This command is supported in remote mode only.
OPTIONS	<div>-u --user</div> <div>The authorized domain application server administrative username.</div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> <div>--passwordfile</div> <div>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> <div>-t --terse</div> <div>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.</div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div>



		delete-lifecycle-module(1)
	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
	--target	This is the name of the resulting location. The valid targets for this command are configuration, instance, cluster, or server. This is used by EE only.
OPERANDS	<i>module_name</i>	This operand is a unique identifier or the deployed server lifecycle event listener module.
EXAMPLES	<b>EXAMPLE 1</b> Using delete-lifecycle-module <pre>asadmin&gt; delete-lifecycle-module --user admin --passwordfile adminpassword.txt --host fuyako --port 7070 customSetup</pre> Deleted the Lifecycle module with module name = customSetup  Where: customSetup is the lifecycle module deleted.	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-lifecycle-module(1)</a> , <a href="#">list-lifecycle-modules(1)</a>	

## delete-message-security-provider(1)

<b>NAME</b>	delete-message-security-provider – enables administrators to delete a provider-config sub-element for the given message layer (message-security-config element of domain.xml)								
<b>SYNOPSIS</b>	<pre><b>delete-message-security-provider</b> --user <i>admin_user</i> [<i>--passwordfile filename</i>] [<i>--host host_name</i>] [<i>--port port_number</i>] [<i>--secure -s</i>] [<i>--terse=false</i>] [<i>--echo=false</i>] [<i>--interactive=true</i>] [<i>--help</i>] [<i>--target target</i>] --layer <i>message_layer</i> provider_name</pre>								
<b>DESCRIPTION</b>	<p>Enables administrators to delete a provider-config sub-element for the given message layer (message-security-config element of domain.xml, the file that specifies parameters and properties to the Application Server). The options specified in the list below apply to attributes within the message-security-config and provider-config sub-elements of the domain.xml file.</p> <p>If the message-layer (message-security-config attribute) does not exist, it is created, and then the provider-config is created under it.</p> <p>This command is supported in remote mode only.</p>								
<b>OPTIONS</b>	<p>If an option has a short option name, then the short option preceeds the long option name. Short options have one dash whereas long options have two dashes.</p> <table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASEXPASSWORD, and so on.</td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASEXPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.
-u --user	The authorized domain application server administrative username.								
-w --password	The --password option is deprecated. Use --passwordfile instead.								
--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASEXPASSWORD, and so on.								
-H --host	The machine name where the domain application server is running. The default value is localhost.								

		delete-message-security-provider(1)
	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	-s --secure	If set to 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.
	-h --help	Displays the help text for the command.
	--target	In Enterprise Edition, specifies the target to which you are deploying. Valid values are <ul style="list-style-type: none"> <li>■ <i>server</i>, which deploys the component to the default server instance <i>server</i> and is the default value</li> <li>■ <i>domain</i>, which deploys the component to the domain.</li> <li>■ <i>cluster_name</i>, which deploys the component to every server instance in the cluster.</li> <li>■ <i>instance_name</i>, which deploys the component to a particular sever instance.</li> </ul>
	--layer	The message-layer from which the provider has to be deleted. The default value is SOAP.
OPERANDS	<i>provider_name</i>	The name of the provider used to reference the provider-config element.
EXAMPLES	<b>EXAMPLE 1</b> Using delete-message-security-provider The following example shows how to delete a message security provider for a client. <pre>asadmin&gt; delete-message-security-provider --user admin --layer SOAP mySecurityProvider</pre>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command

delete-message-security-provider(1)

**SEE ALSO** [create-message-security-provider\(1\)](#),  
[list-message-security-providers\(1\)](#)

NAME	delete-password-alias – deletes a password alias
SYNOPSIS	<b>delete-password-alias</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] <i>alias-name</i>
DESCRIPTION	This command deletes a password alias.
OPTIONS	<div>-u --user</div> <div>The authorized domain application server administrative username.</div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> <div>--passwordfile</div> <div>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> <div>-t --terse</div> <div>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.</div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div>

## delete-password-alias(1)

	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
OPERANDS	aliasname	This is the name of the substitute password as it appears in domain.xml.
EXAMPLES	<b>EXAMPLE 1</b> Using delete-password-alias  asadmin> <b>delete-password-alias --aliasname alias1</b>  Command delete-password-alias executed successfully	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-password-alias(1)</a> , <a href="#">list-password-aliases(1)</a> , <a href="#">update-password-alias(1)</a>	

NAME	delete-persistence-resource – removes a persistence resource
SYNOPSIS	<b>delete-persistence-resource</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--target <i>target</i> ] <i>jndi_name</i>
DESCRIPTION	Removes a persistence resource. This command is supported in remote mode only.
OPTIONS	<p>-u --user                      The authorized domain application server administrative username.</p> <p>-w --password                The --password option is deprecated. Use --passwordfile instead.</p> <p>--passwordfile              This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</p> <p>-H --host                    The machine name where the domain application server is running. The default value is localhost.</p> <p>-p --port                    The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</p> <p>-s --secure                 If set to true, uses SSL/TLS to communicate with the domain application server.</p> <p>-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.</p> <p>-e --echo                    Setting to true will echo the command line statement on the standard output. Default is false.</p>

## delete-persistence-resource(1)

	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
	<code>---target</code>	<p>Specifies the target from which you are deleting a persistence resource. This option is available only in the Sun Java System Application Server Enterprise Edition. Valid values are</p> <ul style="list-style-type: none"><li>■ <code>server</code>, which deploys the component to the default server instance <code>server</code> and is the default value</li><li>■ <code>domain</code>, which deploys the component to the domain.</li><li>■ <code>cluster_name</code>, which deploys the component to every server instance in the cluster.</li><li>■ <code>instance_name</code>, which deploys the component to a particular sever instance.</li></ul>
OPERANDS	<i>jndi_name</i>	Specifies the JNDI name of the persistence resource.
EXAMPLES	<p><b>EXAMPLE 1</b> Using delete-persistence-resource</p> <pre>asadmin&gt; delete-persistence-resource --user admin --passwordfile secret.txt --host pigeon --port 5001 sample_persistence_resource</pre> <p>Command delete-persistence-resource executed successfully</p>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-persistence-resource(1)</a> , <a href="#">list-persistence-resources(1)</a>	



NAME	delete-profiler – deletes the profiler element														
SYNOPSIS	<b>delete-profiler</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--target <i>target_name</i> ]														
DESCRIPTION	<p>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.</p> <p>This command is supported in remote mode only.</p>														
OPTIONS	<table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>           This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td>-s --secure</td><td>If set to 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> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	-s --secure	If set to 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.
-u --user	The authorized domain application server administrative username.														
-w --password	The --password option is deprecated. Use --passwordfile instead.														
--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.														
-H --host	The machine name where the domain application server is running. The default value is localhost.														
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.														
-s --secure	If set to 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.														

## delete-profiler(1)

<code>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
<code>-h --help</code>	Displays the help text for the command.
<code>--target</code>	<p>In Enterprise Edition, specifies the target profiler element which you are deleting. Valid values are</p> <ul style="list-style-type: none"><li>■ <i>server</i>, deletes the profiler element for the default server instance <i>server</i> and is the default value</li><li>■ <i>configuration_name</i>, deletes the profiler element for the named configuration</li><li>■ <i>cluster_name</i>, deletes the profiler element for every server instance in the cluster</li><li>■ <i>instance_name</i>, deletes the profiler element for a particular server instance</li></ul>

### EXAMPLES

#### EXAMPLE 1 Using delete-profiler

```
asadmin> delete-profiler --user admin --passwordfile password.txt
--host localhost --port 4848
Deleted Profiler
```

Where: profiler is the deleted profile element.

### EXIT STATUS

0	command executed successfully
1	error in executing the command

### SEE ALSO

[create-profiler\(1\)](#), [list-profiler\(1\)](#)

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

NAME	delete-resource-adapter-config – deletes the configuration information created in domain.xml for the connector module
SYNOPSIS	<b>delete-resource-adapter-config</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] <i>raName</i>
DESCRIPTION	This command deletes the resource adapter javabeen.
OPTIONS	<div>-u --user</div> <div>The authorized domain application server administrative username.</div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> <div>--passwordfile</div> <div>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> <div>-t --terse</div> <div>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.</div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div>

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

	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
	<code>--target</code>	This option is deprecated.
OPERANDS	<i>raname</i>	This value is kept in the <code>resource-adapter-name</code> in the <code>domain.xml</code> file.
EXAMPLES	<b>EXAMPLE 1</b> Using <code>delete-resource-adapter-config</code> <pre>asadmin&gt; delete-resource-adapter-config --user admin1 --passwordfile pfile1 ra1</pre> Command <code>delete-resource-adapter-config</code> executed successfully	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-resource-adapter-config(1)</a> , <a href="#">list-resource-adapter-configs(1)</a>	

NAME	delete-ssl – deletes the SSL element in the selected HTTP listener, IIOP listener, or IIOP service												
SYNOPSIS	<pre>delete-ssl --user admin_user [--passwordfile filename]            [--host host_name] [--port port_number] [--secure -s]            [--terse=false] [--echo=false] [--interactive=true] [--help]            [--target target] --type listener_or_service_type listener_id</pre>												
DESCRIPTION	<p>Deletes the SSL element in the selected HTTP listener, IIOP listener, or IIOP service.</p> <p>The <i>listener_id</i> is not required if the <code>--type</code> is <i>iiop-service</i>.</p> <p>This command is supported in remote mode only.</p>												
OPTIONS	<p>If an option has a short option name, then the short option precedes the long option name. Short options have one dash whereas long options have two dashes.</p> <table> <tr> <td><code>-u --user</code></td><td>The authorized domain application server administrative username.</td></tr> <tr> <td><code>-w --password</code></td><td>The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.</td></tr> <tr> <td><code>--passwordfile</code></td><td>This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code>, <code>AS_ADMIN_USERPASSWORD</code>, <code>AS_ADMIN_SAVEDMASTERPASSWORD</code>, <code>AS_ADMIN_MQPASSWORD</code>, <code>AS_ADMIN_ALIASPASSWORD</code>, and so on.</td></tr> <tr> <td><code>-H --host</code></td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td><code>-p --port</code></td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td><code>-s --secure</code></td><td>If set to true, uses SSL/TLS to communicate with the domain application server.</td></tr> </table>	<code>-u --user</code>	The authorized domain application server administrative username.	<code>-w --password</code>	The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.	<code>--passwordfile</code>	This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code> , <code>AS_ADMIN_USERPASSWORD</code> , <code>AS_ADMIN_SAVEDMASTERPASSWORD</code> , <code>AS_ADMIN_MQPASSWORD</code> , <code>AS_ADMIN_ALIASPASSWORD</code> , and so on.	<code>-H --host</code>	The machine name where the domain application server is running. The default value is localhost.	<code>-p --port</code>	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	<code>-s --secure</code>	If set to true, uses SSL/TLS to communicate with the domain application server.
<code>-u --user</code>	The authorized domain application server administrative username.												
<code>-w --password</code>	The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.												
<code>--passwordfile</code>	This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code> , <code>AS_ADMIN_USERPASSWORD</code> , <code>AS_ADMIN_SAVEDMASTERPASSWORD</code> , <code>AS_ADMIN_MQPASSWORD</code> , <code>AS_ADMIN_ALIASPASSWORD</code> , and so on.												
<code>-H --host</code>	The machine name where the domain application server is running. The default value is localhost.												
<code>-p --port</code>	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.												
<code>-s --secure</code>	If set to true, uses SSL/TLS to communicate with the domain application server.												

## delete-ssl(1)

	-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.
	-h --help	Displays the help text for the command.
	--target	In Enterprise Edition, specifies the target to which you are deploying. Valid values are <ul style="list-style-type: none"> <li>■ <i>server</i>, the server in which the iiop-service or listener is to be unconfigured for SSL.</li> <li>■ <i>config</i>, the configuration that contains the listener or iiop-service for which SSL is to be unconfigured.</li> <li>■ <i>cluster</i>, the cluster in which the listener or iiop-service is to be unconfigured for SSL. All the server instances in the cluster will get SSL unconfigured for the respective listener or iiop-service.</li> <li>■ <i>instance</i>, the instance in which the listener or iiop-service is to be unconfigured for SSL.</li> </ul>
	--type	The type of service or listener for which the SSL is created. The type can be <i>http-listener</i> , <i>iiop-listener</i> , or <i>iiop-service</i> .
OPERANDS	<i>listener_id</i>	The ID of the listener from which the SSL element is to be deleted.  The <i>listener_id</i> operand is not required if the --type is <i>iiop-service</i> .
EXAMPLES	<p><b>EXAMPLE 1</b> Using delete-ssl</p> <p>The following example shows how to delete an SSL element from an HTTP listener named <i>http-listener-1</i>.</p> <pre>asadmin&gt; delete-ssl --user admin --secure --host fuyako --port 7070 --passwordfile adminpassword.txt --type http-listener http-listener-1 Deleted SSL in HTTP Listener</pre>	
EXIT STATUS	0	command executed successfully

delete-ssl(1)

1  
error in executing the command

**SEE ALSO** [create-ssl\(1\)](#)

## delete-system-property(1)

NAME	delete-system-property – removes one system property of the domain, configuration, cluster, or server instance, at a time
SYNOPSIS	<b>delete-system-property</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--target <i>target_name</i> ] [ <i>property_name</i> ]
DESCRIPTION	Shared or clustered server instances will often need to override attributes defined in their referenced configuration. Any configuration attribute in a server instance can be overridden through a system property of the corresponding name. This command deletes system properties of a domain, configuration, cluster, or server instance.
OPTIONS	<div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>--passwordfile</div> <div>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</div> </div> <div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> </div> <div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> </div> <div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> </div>



		delete-system-property(1)
	-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.
	-h --help	Displays the help text for the command.
	--target	In Enterprise Edition, specifies the target on which you are deleting the system properties. The valid targets for this command are instance, cluster, configuration, 'domain,' and 'server.' Server is the default option.
OPERANDS	<i>property_name</i>	The name of the system property to remove.
EXAMPLES	<b>EXAMPLE 1</b> Using delete-system-properties <pre>asadmin&gt; delete-system-property --user admin --passwordfile password.txt --host localhost --port 4849 --target mycluster http-listener-port</pre> Command delete-system-property executed successfully.	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-system-properties(1)</a> , <a href="#">list-system-properties(1)</a>	

## delete-threadpool(1)

NAME	delete-threadpool – removes the named threadpool	
SYNOPSIS	<b>delete-threadpool</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--target <i>target_name</i> ] [--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> }	
DESCRIPTION	Removes the threadpool with the named ID. This command is supported in remote mode only.	
OPTIONS	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
	-H --host	The machine name where the domain application server is running. The default value is localhost.
	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	-s --secure	If set to true, uses SSL/TLS to communicate with the domain application server.

## delete-threadpool(1)

	-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.
	-h --help	Displays the help text for the command.
	--target	In Enterprise Edition, specifies the target on which you are creating the threadpool. Valid values are <ul style="list-style-type: none"> <li>■ <i>server</i>, which creates the listener for the default server instance <i>server</i> and is the default value</li> <li>■ <i>configuration_name</i>, which creates the listener for the named configuration</li> <li>■ <i>cluster_name</i>, which creates the listener for every server instance in the cluster</li> <li>■ <i>instance_name</i>, which creates the listener for a particular server instance</li> </ul>
	--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.
	--workqueues	identifies the total number of work queues serviced by this threadpool.
OPERANDS	<i>threadpool_id</i>	an ID for the work queue; for example, thread-pool-1, thread-pool-2, etc.
EXAMPLES	<b>EXAMPLE 1</b> Using delete-threadpool <pre>asadmin&gt; delete-threadpool --user admin1 --passwordfile password.txt threadpool-1</pre> Command delete-threadpool executed successfully	
EXIT STATUS	0	command executed successfully

delete-threadpool(1)

1  
error in executing the command

**SEE ALSO** [create-threadpool\(1\)](#), [list-threadpools\(1\)](#)

NAME	delete-virtual-server – removes a virtual server
SYNOPSIS	<b>delete-virtual-server</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--target <i>server</i> ] <i>virtual_server_id</i>
DESCRIPTION	The delete-virtual-server command removes the virtual server with the specified virtual server ID. This command is supported in remote mode only.
OPTIONS	<div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>--passwordfile</div> <div>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </div> </div> <div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> </div> <div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> </div> <div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> </div> <div> <div>-t --terse</div> <div>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.</div> </div> <div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div> </div>

## delete-virtual-server(1)

	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
	--target	In Enterprise Edition, specifies the target from which you are deleting the virtual server. Valid values are <ul style="list-style-type: none"> <li>■ <i>server</i>, which deletes the virtual server from the default server instance <i>server</i> and is the default value</li> <li>■ <i>configuration_name</i>, which deletes the virtual server from the named configuration</li> <li>■ <i>cluster_name</i>, which deletes the virtual server from every server instance in the cluster</li> <li>■ <i>instance_name</i>, which deletes the virtual server from a particular server instance</li> </ul>
OPERANDS	<i>virtual_server_id</i>	The unique identifier for the virtual server to be deleted.
EXAMPLES	<p><b>EXAMPLE 1</b> Using the delete-virtual-server command</p> <p>The following command deletes the virtual server named <i>sample_vs1</i>:</p> <pre>asadmin&gt; delete-virtual-server --user admin1 --passwordfile passwords.txt --host pigeon --port 5001 sample_vs1</pre> <p>Command delete-virtual-server executed successfully.</p>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-virtual-server(1)</a> , <a href="#">list-virtual-servers(1)</a>	

NAME	deploy – deploys the specified component						
SYNOPSIS	<pre> <b>deploy</b> --user <i>admin_user</i> [--passwordfile <i>filename</i>] [--host <i>host_name</i>]       [--port <i>port_number</i>] [--secure -s] [--terse=false] [--echo=false]       [--interactive=true] [--help] [--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] [--enabled=true]       [--deploymentplan <i>deployment_plan</i>]       [--availabilityenabled=false] [--generatermistubs=false]       [--target <i>target</i>] <i>filepath</i> </pre>						
DESCRIPTION	<p>Deploys an EJB, web, connector, or application. If the component is already deployed or already exists, it is forcefully redeployed 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 <i>true</i> or <i>false</i>. 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> and <code>--dropandcreatetables</code> options 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>						
OPTIONS	<table> <tr> <td><code>-u --user</code></td><td>The authorized domain application server administrative username.</td></tr> <tr> <td><code>-w --password</code></td><td>The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.</td></tr> <tr> <td><code>--passwordfile</code></td><td>This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code>, where <i>password</i> is the actual administrator password. Other passwords that can be</td></tr> </table>	<code>-u --user</code>	The authorized domain application server administrative username.	<code>-w --password</code>	The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.	<code>--passwordfile</code>	This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code> , where <i>password</i> is the actual administrator password. Other passwords that can be
<code>-u --user</code>	The authorized domain application server administrative username.						
<code>-w --password</code>	The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.						
<code>--passwordfile</code>	This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code> , where <i>password</i> is the actual administrator password. Other passwords that can be						

## deploy(1)

	specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASSPASSWORD, and so on.
-H --host	The machine name where the domain application server is running. The default value is localhost.
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
-s --secure	If set to 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.
-h --help	Displays the help text for the command.
--virtualservers	Comma separated list of virtual server names.
--contextroot	Valid only if the archive is a web module. It is ignored for other archive types; defaults to filename without extension.
--force	Makes sure the component is redeployed even if the specified component has already been deployed or already exists. Use this option when redeploying an existing application, otherwise you see an error.
--precompilejsp	By default this option is set to false, which does not allow the JSP to pre-compile during deployment. Instead JSPs are compiled during runtime.



## deploy(1)

<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 database-entry-name entry in the <code>cmp-resource()</code> element of the <code>sun-ejb-jar.xml</code> file. If not specified the default is SQL92, and the DDL files to create and drop tables are generated in SQL92 format.
<code>--createtables</code>	Creates tables at deployment of an application with unmapped CMP beans. Default is the <code>create-tables-at-deploy</code> entry in the <code>cmp-resource</code> element of the <code>sun-ejb-jar.xml</code> file.
<code>--dropandcreatetables</code>	Drops tables at redeployment of an already deployed application with unmapped CMP beans. If not specified, the tables are 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 redeployment the tables created by the previous deploy are dropped before creating the new tables.
<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.

## deploy(1)

<code>--enabled</code>	<p>If set to true (default), allows users to access the application. If set to false, users will not be able to access the application.</p> <p>For Enterprise Edition, this option enables the application on the specified target instance or cluster. If you deploy to the target domain, this option is ignored, since deploying to the domain doesn't deploy to a specific instance or cluster.</p>
<code>--deploymentplan</code>	<p>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.</p>
<code>--generatermistubs</code>	<p>If set to true, static RMI-IIOP stubs are generated and put into the <code>client.jar</code>. If set to false (default) the stubs are not generated.</p>
<code>--availabilityenabled</code>	<p>This option is available only in the Sun Java System Application Server Enterprise Edition. If set to true, high-availability is enabled for SFSB checkpointing (and potentially passivation). If set to false (default) all SFSB checkpointing is disabled for the application or EJB module. Set this option to true only high availability is configured and enabled.</p>
<code>--target</code>	<p>This option is available only in the Sun Java System Application Server Enterprise Edition. Specifies the target to which you are deploying. Valid values are:</p> <ul style="list-style-type: none"> <li>■ <code>server</code>, which deploys the component to the default server instance <code>server</code> and is the default value.</li> <li>■ <code>domain</code>, which deploys the component to the domain. If <code>domain</code> is the target for an initial deployment, the application is deployed to the domain, but no server instances or clusters reference the application. If <code>domain</code> is the target for a redeployment (the <code>--force</code> option is set to true), and</li> </ul>

deploy(1)

dynamic reconfiguration is enabled for the clusters or server instances that reference the application, the referencing clusters or server instances automatically get the new version of the application. If redeploying, and dynamic configuration is disabled, the referencing clusters or server instances do not get the new version of the application until the clustered or standalone server instances are restarted.

- *cluster\_name*, which deploys the component to every server instance in the cluster.
- *instance\_name*, which deploys the component to a particular sever instance.

**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.

This syntax deploys the application to the default server instance `server`. For Sun Java System Application Server, Enterprise Edition, use the `--target` option to deploy to a different server instance or to a cluster.

```
asadmin> deploy --user admin --passwordfile filename 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.

This syntax deploys the application to the default server instance `server`. For Sun Java System Application Server, Enterprise Edition, use the `--target` option to deploy to a different server instance or to a cluster.

```
asadmin> deploy --user admin --passwordfile myfile 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.

deploy(1)

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

This example uses the `--target` option, available with Sun Java System Application Server Enterprise Edition only. To use this example for Standard Edition, omit that option. The target in this example is an existing cluster, `cluster1`.

```
asadmin> deploy --user admin --passwordfile filename --createtables=true
--target cluster1 EmployeeEJB.jar
Command deploy executed successfully
```

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

Deploy a connector module packaged in a RAR file.

This example uses the `--target` option, available with Sun Java System Application Server Enterprise Edition only. To use this example for Standard Edition, omit that option. The target in this example is an existing standalone server instance that does not belong to a cluster.

```
asadmin> deploy --user admin --passwordfile filename --target myinstance jdbcra.rar
Command deploy executed successfully
```

**EXIT STATUS**

- 0  
command executed successfully
- 1  
error in executing the command

**SEE ALSO**

[undeploy\(1\)](#), [list-components\(1\)](#)

NAME	deploydir – deploys an exploded format of application archive	
SYNOPSIS	<b>deploydir</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--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 ] [--generateterminstubs=false] [--availabilityenabled=false] [--target <i>target</i> ] <i>dirpath</i>	
DESCRIPTION	<p>Deploys the exploded format of the application archives present under the directory provided as the command operand.</p> <p>Directory deployment is for advanced developers only. Do not use it in production environments. In production environments, use the deploy command. Directory deployment is not supported for clusters and remote server instances.</p> <p>The deployed EAR or WAR applications reside on the Domain Administration Server and have a directory structure that can be used for deployment. The --force option makes sure the component is forcefully (re)deployed even if the specified component has already been deployed or already exists. Set --force 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 --uniquetablenames, --createtables, and --dropandcreatetables options are not specified, the entries in the deployment descriptors are used.</p> <p>This command is supported in remote mode only.</p>	
OPTIONS	-u --user -w --password --passwordfile	<p>The authorized domain application server administrative username.</p> <p>The --password option is deprecated. Use --passwordfile instead.</p> <p>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where</p>

## deploydir(1)

	<p><i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASSPASSWORD, and so on.</p>
-H --host	The machine name where the domain application server is running. The default value is localhost.
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
-s --secure	If set to 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.
-h --help	Displays the help text for the command.
---virtualservers	Comma separated list of virtual server IDs.
---contextroot	Valid only if the archive is a web module. It is ignored for other archive types; defaults to filename without extension.
---force	Makes sure the component is forcefully (re)deployed even if the specified component has already been deployed or already exists.
---verify	If set to true, the syntax and semantics of the deployment descriptor is verified.

deploydir(1)

<code>--precompilejsp</code>	By default, this option is set to false, which does not allow the JSP to pre-compile during deployment. Instead, JSPs are compiled during runtime.
<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, and the DDL files to create and drop tables are 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 are 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. When the component is redeployed, the tables created by the previous deployment are dropped before creating the new tables.
<code>---generateterminstubs</code>	if set to true, static RMI-IIOP stubs are generated and put into the <code>client.jar</code> . If set to false (default) the stubs are not generated.

## deploydir(1)

	<p><code>--availabilityenabled</code></p> <p>If set to true, high-availability is enabled for SFSB checkpointing (and potentially passivation). If set to false (default) all SFSB checkpointing is disabled for the application or EJB module.</p> <p><code>--target</code></p> <p>In Enterprise Edition, specifies the target to which you are deploying. Valid values are:</p> <ul style="list-style-type: none"> <li>■ <code>server</code>, which deploys the component to the default server instance <code>server</code> and is the default value.</li> <li>■ <code>domain</code>, which deploys the component to the domain.</li> </ul>
OPERANDS	<p><i>dirpath</i></p> <p>path to the directory containing the exploded format of the deployable archive.</p>
EXAMPLES	<p><b>EXAMPLE 1</b> Using <code>deploydir</code></p> <pre>asadmin&gt; deploydir --user admin --passwordfile passwords.txt --host localhost --port 4848 --force=true --precompilejsp=true /home/temp/sampleApp</pre> <p>Command <code>deploydir</code> executed successfully</p> <p>Where the exploded application to be deployed is in the <code>/home/temp/sampleApp</code> directory.</p>
EXIT STATUS	<p>0</p> <p>command executed successfully</p> <p>1</p> <p>error in executing the command</p>
SEE ALSO	<p><a href="#">deploy(1)</a>, <a href="#">undeploy(1)</a>, <a href="#">enable(1)</a>, <a href="#">disable(1)</a>, <a href="#">list-components(1)</a></p>



NAME	deploytool – launches the deploytool utility to deploy, package, and edit your J2EE applications
SYNOPSIS	<b>deploytool</b> [--help] [--userdir <i>user_directory</i> ] [--configdir <i>configuration_directory</i> --verbose]
DESCRIPTION	<p>Use the deploytool utility to deploy and package your J2EE applications and components, create and edit J2EE deployment descriptors, and create and edit Sun Java System Application Server specific deployment descriptors. If the application is not J2EE compliant, an error message is displayed.</p> <p>Only one session of the deploytool 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>
OPTIONS	<p>--help               displays the arguments for launching the deploytool.</p> <p>--userdir            identifies the user directory. The default user directory is .deploytool under your home directory. Only one deploytool session can be running per user directory. A lock file is created under the user directory to ensure that only one session of the deploytool is running. The deploytool utility uses this directory to store configuration information.</p> <ul style="list-style-type: none"> <li>■ On Solaris, the default directory is at ~/ .deploytool</li> </ul> <p>--configdir          identifies the configuration directory. The configuration directory is where the asenv.conf file is located.</p> <p>On Solaris, the asenv.conf can be found at:</p> <ul style="list-style-type: none"> <li>■ Bundled installation: /etc/appserver</li> <li>■ Unbundled installation: default is /etc/opt/SUNWappserver or user specified</li> <li>■ Evaluation installation: cd /etc. Where AS_SERVER_INSTALL is the directory where you have installed the Sun Java System Application Server 8.</li> </ul> <p>--verbose            displays the deploytool log messages on the terminal window in Solaris and command window on windows.</p>
EXAMPLES	<p><b>EXAMPLE 1</b> Using deploytool</p> <pre>example% deploytool --userdir /myapplication --config_dir /myconfigdir</pre> <p>Where --userdir specifies the destination directory, and -config_dir identifies the configuration directory.</p>
SEE ALSO	<a href="#">verifier(1M)</a>

disable(1)

NAME	disable – disables the component
SYNOPSIS	<b>disable</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--target <i>target_name</i> ] [ <i>component_name</i> ]
DESCRIPTION	disable immediately disables the named component. The component must have been deployed. If the component has not been deployed, an error message is returned.
OPTIONS	<p>-u --user                   The authorized domain application server administrative username.</p> <p>-w --password              The --password option is deprecated. Use --passwordfile instead.</p> <p>--passwordfile            This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</p> <p>-H --host                   The machine name where the domain application server is running. The default value is localhost.</p> <p>-p --port                   The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</p> <p>-s --secure                 If set to true, uses SSL/TLS to communicate with the domain application server.</p> <p>-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.</p> <p>-e --echo                   Setting to true will echo the command line statement on the standard output. Default is false.</p>

	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
	--target	In Enterprise Edition, specifies the target on which you are disabling the component. Valid values are <ul style="list-style-type: none"> <li>■ <i>server</i>, which creates the listener for the default server instance <i>server</i> and is the default value</li> <li>■ <i>cluster_name</i>, which creates the listener for every server instance in the cluster</li> <li>■ <i>instance_name</i>, which creates the listener for a particular server instance</li> </ul>
OPERANDS	<i>component_name</i>	name of the component to be disabled.
EXAMPLES	<b>EXAMPLE 1</b> Using <code>disable</code> <pre>asadmin&gt; disable --user admin1 --passwordfile password.txt sampleApp</pre> Command <code>disable</code> executed successfully	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">deploy(1)</a> , <a href="#">deploydir(1)</a> , <a href="#">undeploy(1)</a> , <a href="#">enable(1)</a>	

## display-license(1)

NAME	display-license – displays the license information
SYNOPSIS	<b>display-license</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help]
DESCRIPTION	display-license displays the license information. This command can run both locally and remotely.
OPTIONS	<div>-u --user</div> <div>The authorized domain application server administrative username.</div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> <div>--passwordfile</div> <div>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> <div>-t --terse</div> <div>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.</div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div>

- I --interactive            If set to true (default), only the required password options are prompted.
- h --help                 Displays the help text for the command.

EXAMPLES      **EXAMPLE 1** Using display-license in local mode

```
asadmin> 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
*****
```

**EXAMPLE 2** Using display-license in remote mode

```
asadmin> 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
*****
```

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

SEE ALSO        [install-license\(1\)](#)

## enable(1)

NAME	enable – enables the component
SYNOPSIS	<b>enable</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--target <i>target_name</i> ] [ <i>component_name</i> ]
DESCRIPTION	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.
OPTIONS	<p>-u --user                      The authorized domain application server administrative username.</p> <p>-w --password                The --password option is deprecated. Use --passwordfile instead.</p> <p>--passwordfile              This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</p> <p>-H --host                    The machine name where the domain application server is running. The default value is localhost.</p> <p>-p --port                    The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</p> <p>-s --secure                 If set to true, uses SSL/TLS to communicate with the domain application server.</p> <p>-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.</p> <p>-e --echo                    Setting to true will echo the command line statement on the standard output. Default is false.</p>

	<div><div>-I --interactive</div><div>If set to true (default), only the required password options are prompted.</div></div> <div><div>-h --help</div><div>Displays the help text for the command.</div></div> <div><div>--target</div><div><div>In Enterprise Edition, specifies the target on which you are enabling the component. Valid values are<ul style="list-style-type: none"><li>■ <i>server</i>, which creates the listener for the default server instance <i>server</i> and is the default value</li><li>■ <i>cluster_name</i>, which creates the listener for every server instance in the cluster</li><li>■ <i>instance_name</i>, which creates the listener for a particular server instance</li></ul></div></div></div>
OPERANDS	<div><div><i>component_name</i></div><div>name of the component to be enabled.</div></div>
EXAMPLES	<div><div>EXAMPLE 1 Using enable</div><div>asadmin&gt; enable --user admin1 --passwordfile password.txt sampleApp</div><div>Command enable executed successfully</div></div>
EXIT STATUS	<div><div>0</div><div>command executed successfully</div></div> <div><div>1</div><div>error in executing the command</div></div>
SEE ALSO	<div><div>deploy(1), deploydir(1), undeploy(1), disable(1)</div></div>

## export(1)

NAME	export – marks a variable name for automatic export to the environment of subsequent commands in multimode
SYNOPSIS	<b>export</b> [ <i>name=value</i> [ <i>name=value</i> ] *]
DESCRIPTION	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 asadmin utility are imported automatically and set as exported variables within asadmin. Unexported environment variables cannot be read by the asadmin utility.
OPERANDS	<i>name=value</i> variable name and value for automatic export to the environment to be used by subsequent commands.
EXAMPLES	<p><b>EXAMPLE 1</b> Using export to set an environment variable</p> <pre>asadmin&gt; export AS_ADMIN_HOST=bluestar</pre> <p>In this case, the AS_ADMIN_HOST environment variables has been set to <i>bluestar</i>.</p> <p><b>EXAMPLE 2</b> Using export to set multiple environment variables</p> <pre>asadmin&gt; export AS_ADMIN_HOST=bluestar AS_ADMIN_PORT=8000 AS_ADMIN_USER=admin AS_ADMIN_PREFIX=server1.jms-service</pre> <p>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>, and the prefix is <i>server1.jms-service</i>.</p> <p><b>EXAMPLE 3</b> Using export to list environment variables</p> <pre>asadmin&gt; export AS_ADMIN_HOST=bluestar AS_ADMIN_PORT=8000 AS_ADMIN_USER=admin AS_ADMIN_PREFIX=server1.jms-service</pre> <p>The export with no input lists the set environment variables.</p>
EXIT STATUS	<p>0 command executed successfully</p> <p>1 error in executing the command</p>
SEE ALSO	<a href="#">unset(1)</a> , <a href="#">multimode(1)</a>



NAME	freeze-transaction-service – freezes the transaction subsystem														
SYNOPSIS	<b>freeze-transaction-service</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--target <i>target_name</i> ]														
DESCRIPTION	<p>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 is supported for Enterprise Edition only.</p> <p>This command is supported in remote mode only.</p>														
OPTIONS	<table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td>-s --secure</td><td>If set to 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> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	-s --secure	If set to 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.
-u --user	The authorized domain application server administrative username.														
-w --password	The --password option is deprecated. Use --passwordfile instead.														
--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.														
-H --host	The machine name where the domain application server is running. The default value is localhost.														
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.														
-s --secure	If set to 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.														

## freeze-transaction-service(1)

OPERANDS	-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.
	-h --help	Displays the help text for the command.
	--target	specifies the target on which you are freezing the Transaction Service. Valid values are
		<ul style="list-style-type: none"><li>■ <i>server</i>, which creates the listener for the default server instance <i>server</i> and is the default value</li><li>■ <i>configuration_name</i>, which creates the listener for the named configuration</li><li>■ <i>cluster_name</i>, which creates the listener for every server instance in the cluster</li><li>■ <i>instance_name</i>, which creates the listener for a particular server instance</li></ul>
EXAMPLES	<b>EXAMPLE 1</b> Using freeze-transaction-service	
EXIT STATUS	asadmin> <b>freeze-transaction-service</b> --user admin --passwordfile password.txt --target server	
	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">unfreeze-transaction-service(1)</a> , <a href="#">rollback-transaction(1)</a>	

NAME	get – gets the values of the monitorable or configurable attributes																
SYNOPSIS	<pre>get --user <i>admin_user</i> [--passwordfile <i>filename</i>] [--host <i>host_name</i>]     [--port <i>port_number</i>] [--secure -s] [--terse=<i>false</i>] [--echo=<i>false</i>]     [--interactive=<i>true</i>] [--help] [--monitor=<i>[true false]</i>]     [<i>dotted_attribute_name</i>]</pre>																
DESCRIPTION	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.																
OPTIONS	<table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.</td></tr> <tr> <td>--passwordfile</td><td>This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td>-s --secure</td><td>If set to 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> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.	--passwordfile	This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	-s --secure	If set to 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.
-u --user	The authorized domain application server administrative username.																
-w --password	The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.																
--passwordfile	This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.																
-H --host	The machine name where the domain application server is running. The default value is localhost.																
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.																
-s --secure	If set to 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.																

get(1)

	<div><div>-I --interactive</div><div>If set to true (default), only the required password options are prompted.</div></div> <div><div>-h --help</div><div>Displays the help text for the command.</div></div> <div><div>--monitor</div><div>defaults to false; if set to false, the configurable attribute values are returned. If set to true, the monitorable attribute values are returned.</div></div>
OPERANDS	<div><div><i>attributename</i></div><div>attribute name in the dotted notation.</div></div>
EXAMPLES	<div><div><b>EXAMPLE 1</b> Using get</div><div>asadmin&gt; get --user admin --passwordfile password.txt --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</div></div>
EXIT STATUS	<div><div>0</div><div>command executed successfully</div></div> <div><div>1</div><div>error in executing the command</div></div>
SEE ALSO	<div><div><a href="#">set(1)</a>, <a href="#">list(1)</a></div></div>

NAME	get-client-stubs – gets the stubs of the client																
SYNOPSIS	<pre><b>get-client-stubs</b> --user <i>admin_user</i> [--passwordfile <i>filename</i>]                     [--host <i>host_name</i>] [--port <i>port_number</i>] [--secure -s]                     [--terse=<i>false</i>] [--echo=<i>false</i>] [--interactive=<i>true</i>] [--help]                     [--target <i>target_name</i>] [--appname <i>application_name</i>]                     [<i>local_directory_path</i>]</pre>																
DESCRIPTION	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.																
OPTIONS	<table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td>-s --secure</td><td>If set to 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> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	-s --secure	If set to 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.
-u --user	The authorized domain application server administrative username.																
-w --password	The --password option is deprecated. Use --passwordfile instead.																
--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.																
-H --host	The machine name where the domain application server is running. The default value is localhost.																
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.																
-s --secure	If set to 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.																

## get-client-stubs(1)

	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
	--target	In Enterprise Edition, specifies the target on which you are retrieving the client stubs. Valid values are <ul style="list-style-type: none"> <li>■ <i>server</i>, which creates the listener for the default server instance <i>server</i> and is the default value</li> <li>■ <i>configuration_name</i>, which creates the listener for the named configuration</li> <li>■ <i>cluster_name</i>, which creates the listener for every server instance in the cluster</li> <li>■ <i>instance_name</i>, which creates the listener for a particular server instance</li> </ul>
	--appname	name of the application.
OPERANDS	<i>local_directory_path</i>	path to the local directory where the client stub should be stored.
EXAMPLES	<b>EXAMPLE 1</b> Using get-client-stubs asadmin> <b>get-client-stubs</b> --user admin --passwordfile password.txt --host fuyako --port 7070 --appname myapplication.ear /sample/exmple	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">undeploy(1)</a>	

<b>NAME</b>	help – displays the asadmin utility commands																																										
<b>SYNOPSIS</b>	<b>help</b> [ <i>or</i> --help   -h   -? ]																																										
<b>DESCRIPTION</b>	<p>The help command displays a list of all the asadmin utility commands. Specify the command to display the usage information for that command. To display the manpage of each command, use the syntax: asadmin <i>command_name</i> —help   -h   -? or asadmin help <i>command_name</i></p> <p>The following is a list of all the asadmin utility commands:</p> <table> <tr> <td>add-resources</td><td>registers the resource in the XML file specified</td></tr> <tr> <td>change-master-password</td><td>changes the master password</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-instance</td><td>creates an instance</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> </table>	add-resources	registers the resource in the XML file specified	change-master-password	changes the master password	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-instance	creates an instance	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
add-resources	registers the resource in the XML file specified																																										
change-master-password	changes the master password																																										
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-instance	creates an instance																																										
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																																										

help(1)

create-lifecycle-module	adds a lifecycle module
create-message-security-provider	enables administrators to create the message-security-config and provider-config sub-elements for the security service in domain.xml
create-password-alias	creates a password alias
create-persistence-resource	registers the persistence resource
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-system-properties	adds or updates one or more system properties of the domain, configuration, cluster, or server instance
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-resource	removes the named resource connector
delete-connector-security-map	deletes the named security map
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-instance	deletes the instance that is not running
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-message-security-provider	enables administrators to delete a provider-config sub-element for the given message layer (message-security-config element of domain.xml)
delete-password-alias	deletes a password alias
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-system-property	removes one or more system properties of the domain, configuration, cluster, or server instance
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

help(1)

jms-ping	checks to see if the JMS provider is up and running
list-admin-objects	gets all the administered objects
list-application-refs	lists all application references in a cluster or unclustered server instance
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-instances	lists all the instances along with their status
list-javamail-resources	gets all the Javamail resources
list-jdbc-connection-pools	registers the JDBC connection pool
list-jdbc-resources	gets all the JDBC resources
list-jms-resources	lists the JMS resources
list-jmsdest	gets all the named destinations
list-jndi-entries	gets all the named destinationsbrowses and queries the JNDI tree
list-jndi-resources	gets all the JNDI resources
list-lifecycle-modules	gets the lifecycle modules
list-message-security-providers	enables administrators to list all security message providers (provider-config sub-elements) for the given message layer (message-security-config element of domain.xml)
list-password-aliases	lists all password aliases

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-system-properties	lists the system properties of the domain, configuration, cluster, or server instance
list-threadpools	lists the thread pools
list-timers	lists all of the timers owned by server instance(s)
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 <code>asadmin</code> utility
ping-connection-pool	tests if a connection pool is usable
recover-transactions	manually recovers pending transactions
rollback-transaction	rollback the named transaction
set	sets the values of attributes
show-component-status	displays the status of the deployed component
start-domain	starts the given domain
start-instance	starts a server instance
stop-domain	stops the given domain
stop-instance	stops a server instance
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-password-alias	updates a password alias
update-connector-security-map	updates the security map for the specified connector connection pool
verify-domain-xml	verifies the content of the <code>domain.xml</code>

## help(1)

version

displays the version information

The following commands are deprecated:

1. create-connection-pool
2. display-license
3. install-license
4. restart-instance
5. shutdown
6. create-acl
7. delete-acl
8. list-acls
9. start-appserv
10. stop-appserv

### EXAMPLES

**EXAMPLE 1** Using help

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

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

### SEE ALSO

[asadmin\(1\)](#)

NAME	install-license – installs the license file
SYNOPSIS	<b>install-license</b>
DESCRIPTION	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.
EXAMPLES	<b>EXAMPLE 1</b> Using install-license <pre>asadmin&gt; install-license LICENSE agreement will be displayed. Do you agree with the terms of this license [YES NO] YES Enter license key&gt; ***** Installed the license</pre>
EXIT STATUS	0 command executed successfully 1 error in executing the command
SEE ALSO	<a href="#">display-license(1)</a> , <a href="#">version(1)</a>

## jms-ping(1)

<b>NAME</b>	jms-ping – checks to see if the JMS service is up and running	
<b>SYNOPSIS</b>	<b>jms-ping</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [ <i>target</i> ]	
<b>DESCRIPTION</b>	<p>The <b>jms-ping</b> command checks to see if the JMS service (also known as the JMS provider) is up and running. When you start the Application Server, the JMS service starts by default.</p> <p>The <b>jms-ping</b> command pings only the default JMS host within the JMS service. It throws an exception when it is unable to ping a built-in JMS service.</p> <p>This command is supported in remote mode only.</p>	
<b>OPTIONS</b>	-u --user -w --password --passwordfile -H --host -p --port -s --secure	<p>The authorized domain application server administrative username.</p> <p>The --password option is deprecated. Use --passwordfile instead.</p> <p>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</p> <p>The machine name where the domain application server is running. The default value is localhost.</p> <p>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</p> <p>If set to true, uses SSL/TLS to communicate with the domain application server.</p>

		jms-ping(1)
	-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.
	-h --help	Displays the help text for the command.
OPERANDS	<i>target</i>	<p>In Enterprise Edition, this operand specifies the target for which the operation is to be performed. Valid values are:</p> <ul style="list-style-type: none"> <li>■ <i>server</i>, which pings the JMS service for the default server instance <i>server</i> and is the default value</li> <li>■ <i>configuration_name</i>, which pings the JMS service for all clusters using the specified configuration</li> <li>■ <i>cluster_name</i>, which pings the JMS service for the specified cluster</li> <li>■ <i>instance_name</i>, which pings the JMS service for a particular server instance</li> </ul>
EXAMPLES	<p><b>EXAMPLE 1</b> Using the <code>jms-ping</code> command</p> <p>The following command checks to see if the JMS service is running on the server instance <code>server1</code>:</p> <pre>asadmin&gt; jms-ping --user admin --passwordfile passwords.txt --host bluestar --port 4848 server1 JMS Ping Status=RUNNING Command jms-ping executed successfully.</pre>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-jmsdest(1)</a> , <a href="#">create-jms-resource(1)</a>	

## 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>	Use the jspc command to compile your JSP 2.0 compliant source files into servlets. To allow the Application Server to pick up the precompiled JSP pages from a JAR file, specify the -compile and -webinc or -webxml options, which cause the JSP pages to be mapped to their corresponding servlet class files. This means that the JSP compiler will be bypassed when those JSPs are accessed.	
<b>OPTIONS</b>	<i>jsp_files</i>	one or more JSP files to be compiled.
	-webapp <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 asadmin deploy.
	-d <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 directory is the directory specified by the java.io.tmpdir property, or the current directory.
	-p <i>name</i>	the name of the target package for all specified JSPs, which is prepended to the package component derived from the directory in which the JSP pages are located. The default is org.apache.jsp.
	-c <i>name</i>	the target class name of the first JSP compiled. Subsequent JSPs are unaffected.
	-l	outputs the name of the JSP page upon failure.
	-s	outputs the name of the JSP page upon success.
	-uribase <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 -webapp option. This is the location of each JSP file relative to the uriroot. If this cannot be determined, the default is /.
	-uriroot <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 -webapp option. If this option is not specified, all parent directories of the first JSP page are searched for a WEB-INF subdirectory. The closest directory to the JSP page that has one is used. If none of the JSP's parent directories have a WEB-INF subdirectory, the directory from which jspc is invoked is used.
	-compile	Compile the generated servlets.
	-v	enables verbose mode.



<code>-mapped</code>	generates separate <code>write()</code> calls for each HTML line and comments that describe the location of each line in the JSP file. By default, all adjacent <code>write()</code> 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 unparsable 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>-classpath path</code>	Override the system classpath with the specified classpath.
<code>-ieplugin class_id</code>	specifies the Java plugin COM class ID for Internet Explorer. Used by the <code>jsp:plugin</code> tags.
<code>-xpoweredBy</code>	Adds an X-Powered-By HTTP response header.
<code>-trimSpaces</code>	Trim spaces in template text between actions and directives.
<code>-help</code>	Print a summary of the syntax and options for this command.

**EXAMPLES****EXAMPLE 1** Using `jspc` to compile the JSP pages in a Web application

The following command compiles a set of JSP files into Java source files under `/home/user/Hellodir`:

```
jspc welcome.jsp shop.jsp checkout.jsp -d /home/user/Hellodir
```

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

```
jspc -webapp /path_to_source_directory -compile -d /home/user/Hellodir
```

The following command compiles a set of JSP files into Java class files in `/home/user/Hellodir` with the package name `com.test.jsp` prepended to the package hierarchy found in `/path_to_source_directory`. It creates `web.xml` in the output directory.

```
jspc -webapp /path_to_source_directory -compile -webxml /home/user/Hellodir/web.xml -d /home/user/Hellodir -p com.test.jsp
```

To use these precompiled JSP pages in your web application, package the servlet class files generated under `/home/user/Hellodir` into a JAR file, place the JAR file under `WEB-INF/lib`, and copy the generated `/home/user/Hellodir/web.xml` to `WEB-INF/web.xml`.

jspc(1M)

**SEE ALSO** [asadmin\(1M\)](#)

NAME	list – lists the configurable elements	
SYNOPSIS	<b>list</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ]         [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ]         [--interactive= <i>true</i> ] [--help] [--monitor= <i>[true false]</i> ]         [ <i>dotted_parent_attribute_name</i> ]	
DESCRIPTION	<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, <code>list --monitor server</code> 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, <code>list --monitor server.applications.*</code> 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>	
OPTIONS	-u --user -w --password --passwordfile -H --host	<p>The authorized domain application server administrative username.</p> <p>The --password option is deprecated. Use --passwordfile instead.</p> <p>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=<i>password</i></code>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</p> <p>The machine name where the domain application server is running. The default value is localhost.</p>

list(1)

-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
-s --secure	If set to 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.
-h --help	Displays the help text for the command.
--monitor	defaults to false; if set to false, the configurable attribute values are returned. If set to true, the monitorable attribute values are 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 --passwordfile password.txt
--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.ssl
server.iiop-service.iiop-listener.orb-listener-1
```

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

```

server.iio-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
server.virtual-server.__asadmin
server.virtual-server.server
server.web-container

```

**EXAMPLE 2** Using list for an application

```

asadmin> list --user admin --passwordfile password.txt
--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 --passwordfile password.txt
--host localhost --port 4848 server.applications.web-module
server.applications.web-module.adminapp
server.applications.web-module.admingui
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\(1\)](#)

## list-acls(1)

<b>NAME</b>	list-acls – gets the access control lists
<b>SYNOPSIS</b>	<b>list-acls</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>--passwordfile</b> <i>filename</i> ] [ <b>--secure</b>   <b>-s</b> ] <i>instance_name</i>
<b>DESCRIPTION</b>	Gets the access control lists associated with the named server instance.
<b>OPTIONS</b>	<p><b>--user</b> administrative user associated for the instance.</p> <p><b>--password</b> administrative password corresponding to the administrative user.</p> <p><b>--host</b> host name of the machine hosting the administrative instance.</p> <p><b>--port</b> administrative port number associated with the administrative host.</p> <p><b>--secure</b> indicates communication with the administrative instance in secured mode.</p> <p><b>--passwordfile</b> 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>	<a href="#">create-acl(1)</a> , <a href="#">delete-acl(1)</a>

<b>NAME</b>	list-admin-objects – gets all the administered objects	
<b>SYNOPSIS</b>	<pre>--user <i>admin_user</i> [--passwordfile <i>filename</i>] [--host <i>host_name</i>]   [--port <i>port_number</i>] [--secure -s] [--terse=<i>false</i>] [--echo=<i>false</i>]   [--interactive=<i>true</i>] [--help] [<i>target</i>]</pre>	
<b>DESCRIPTION</b>	This command lists all the administered objects. This command is supported in remote mode only.	
<b>OPTIONS</b>	<b>-u --user</b>	The authorized domain application server administrative username.
	<b>-w --password</b>	The --password option is deprecated. Use --passwordfile instead.
	<b>--passwordfile</b>	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
	<b>-H --host</b>	The machine name where the domain application server is running. The default value is localhost.
	<b>-p --port</b>	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	<b>-s --secure</b>	If set to true, uses SSL/TLS to communicate with the domain application server.
	<b>-t --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>-e --echo</b>	Setting to true will echo the command line statement on the standard output. Default is false.

## list-admin-objects(1)

	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
<b>OPERANDS</b>	<i>target</i>	This is the name of the target upon which the command is operating. The valid targets for this command are instance, cluster, 'domain,' and 'server.' Server is the default option. This command is used by the Enterprise Edition only.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using list-admin-objects <pre>asadmin&gt; list-admin-objects --user admin --password admin123 instance1</pre> Command list-admin-objects executed successfully	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">create-admin-object(1)</a> , <a href="#">delete-admin-object(1)</a>	



<b>NAME</b>	list-applications-refs – lists all application references in a cluster or unclustered server instance	
<b>SYNOPSIS</b>	<pre>--user <i>admin_user</i> [--passwordfile <i>filename</i>] [--host <i>host_name</i>]       [--port <i>port_number</i>] [--secure -s] [--terse=false] [--echo=false]       [--interactive=true] [--help] [<i>target</i>]</pre>	
<b>DESCRIPTION</b>	<p>This command lists all of the application references in a cluster or unclustered server instance. The command effectively lists all of the modules (an example is the J2EE application EAR, web module WAR, or ejb jar file) deployed on the specified target (either clustered or unclustered server instance).</p>	
<b>OPTIONS</b>	<pre>-u --user</pre>	<p>The authorized domain application server administrative username.</p>
	<pre>-w --password</pre>	<p>The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.</p>
	<pre>--passwordfile</pre>	<p>This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=<i>password</i></code>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code>, <code>AS_ADMIN_USERPASSWORD</code>, <code>AS_ADMIN_SAVEDMASTERPASSWORD</code>, <code>AS_ADMIN_MQPASSWORD</code>, <code>AS_ADMIN_ALIASPASSWORD</code>, and so on.</p>
	<pre>-H --host</pre>	<p>The machine name where the domain application server is running. The default value is localhost.</p>
	<pre>-p --port</pre>	<p>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</p>
	<pre>-s --secure</pre>	<p>If set to true, uses SSL/TLS to communicate with the domain application server.</p>
	<pre>-t --terse</pre>	<p>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>

## list-application-refs(1)

	<code>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
<b>OPERANDS</b>	<i>target</i>	<p>This operand specifies which references should be listed. The references can be one of the following:</p> <ul style="list-style-type: none"><li>■ <code>&lt;cluster-name&gt;</code> — This is a list of all application references in the named cluster.</li><li>■ <code>&lt;instance-name&gt;</code> — This is a list of all application references in the named unclustered instance.</li></ul> <p>The target is specified as optional since a default target can be created.</p>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using list-application-refs</p> <pre>asadmin&gt; list-application-refs --target userspace1</pre> <p>Command list-admin-objects executed successfully</p>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">create-application-ref(1)</a> , <a href="#">delete-application-ref(1)</a>	

NAME	list-audit-modules – gets all audit modules and displays them	
SYNOPSIS	<b>list-audit-modules</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [ <i>target</i> ]	
DESCRIPTION	Lists all the audit modules. This command is supported in remote mode only.	
OPTIONS	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
	-H --host	The machine name where the domain application server is running. The default value is localhost.
	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	-s --secure	If set to 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.

## list-audit-modules(1)

	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
<b>OPERANDS</b>	<i>target</i>	<p>In Enterprise Edition, specifies the target on which you are listing the audit modules. Valid values are</p> <ul style="list-style-type: none"> <li>■ <i>server</i>, which creates the listener for the default server instance <i>server</i> and is the default value</li> <li>■ <i>configuration_name</i>, which creates the listener for the named configuration</li> <li>■ <i>cluster_name</i>, which creates the listener for every server instance in the cluster</li> <li>■ <i>instance_name</i>, which creates the listener for a particular server instance</li> </ul>
<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 sampleAUditModule1 sampleAuditModule2 Command list-audit-modules executed successfully</pre>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">create-audit-module(1)</a> , <a href="#">delete-audit-module(1)</a>	

NAME	list-auth-realms – lists the authentication realms
SYNOPSIS	<b>list-auth-realms</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [ <i>target_name</i> ]
DESCRIPTION	Lists the authentication realms. This command is supported in remote mode only.
OPTIONS	<p>-u --user                   The authorized domain application server administrative username.</p> <p>-w --password              The --password option is deprecated. Use --passwordfile instead.</p> <p>--passwordfile            This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</p> <p>-H --host                  The machine name where the domain application server is running. The default value is localhost.</p> <p>-p --port                  The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</p> <p>-s --secure                If set to true, uses SSL/TLS to communicate with the domain application server.</p> <p>-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.</p> <p>-e --echo                  Setting to true will echo the command line statement on the standard output. Default is false.</p> <p>-I --interactive           If set to true (default), only the required password options are prompted.</p>

## list-auth-realms(1)

	<code>-h --help</code>	Displays the help text for the command.
OPERANDS	<code>target_name</code>	<p>name of the target on which you want to list the authentication realms.</p> <ul style="list-style-type: none"><li>■ <code>server</code>, which creates the listener for the default server instance <code>server</code> and is the default value</li><li>■ <code>configuration_name</code>, which creates the listener for the named configuration</li><li>■ <code>cluster_name</code>, which creates the listener for every server instance in the cluster</li><li>■ <code>instance_name</code>, which creates the listener for a particular server instance</li></ul>
EXAMPLES	<p><b>EXAMPLE 1</b> Using list-auth-realms</p> <pre>asadmin&gt; list-auth-realms --user admin --passwordfile password.txt --host localhost --port 4848 file ldap certificate db Command list-auth-realms executed successfully</pre> <p>Where file, ldap, certificate, and db are the listed authentication realms.</p>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-auth-realm(1)</a> , <a href="#">delete-auth-realm(1)</a>	

NAME	list-backups – lists all backups and restores	
SYNOPSIS	<b>list-backups</b> [--domaindir <i>domain_directory</i> ] [--description <i>description</i> ] [--terse= <i>false</i> ] [--verbose= <i>false</i> ] <i>domain_name</i>	
DESCRIPTION	This command displays the status information about all backups in the backup respository. The list-backups command is supported in local mode only.	
OPTIONS	--domaindir	This option specifies the parent directory of the domain upon which the command will operate. The default is install_dir/domains.
	--description	A description can contain any string to help identify the particular backup. The description is displayed as part of the information for any backup.
	-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.
	-t --verbose	Indicates that output data is displayed with detailed information. Default is false.
OPERANDS	<i>domain_name</i>	This is the name of the domain to list the backups from. If the domain is not specified and only one domain exists, it will be used automatically.
EXAMPLES	<b>EXAMPLE 1</b> Using list-backups  asadmin>list-backups --domaindir directory1 sample-backup The command list-backups executed successfully.	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	backup-domain(1), restore-domain(1)	

## list-components(1)

NAME	list-components – lists deployed components														
SYNOPSIS	<b>list-components</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--type <i>application ejb web connector</i> ] [target]														
DESCRIPTION	The command <code>list-components</code> lists all 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.														
OPTIONS	<table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.</td></tr> <tr> <td>--passwordfile</td><td>           This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code>, <code>AS_ADMIN_USERPASSWORD</code>, <code>AS_ADMIN_SAVEDMASTERPASSWORD</code>, <code>AS_ADMIN_MQPASSWORD</code>, <code>AS_ADMIN_ALIASPASSWORD</code>, and so on.         </td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is <code>localhost</code>.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td>-s --secure</td><td>If set to <code>true</code>, 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 <code>false</code>.</td></tr> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.	--passwordfile	This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code> , <code>AS_ADMIN_USERPASSWORD</code> , <code>AS_ADMIN_SAVEDMASTERPASSWORD</code> , <code>AS_ADMIN_MQPASSWORD</code> , <code>AS_ADMIN_ALIASPASSWORD</code> , and so on.	-H --host	The machine name where the domain application server is running. The default value is <code>localhost</code> .	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	-s --secure	If set to <code>true</code> , 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 <code>false</code> .
-u --user	The authorized domain application server administrative username.														
-w --password	The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.														
--passwordfile	This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code> , <code>AS_ADMIN_USERPASSWORD</code> , <code>AS_ADMIN_SAVEDMASTERPASSWORD</code> , <code>AS_ADMIN_MQPASSWORD</code> , <code>AS_ADMIN_ALIASPASSWORD</code> , and so on.														
-H --host	The machine name where the domain application server is running. The default value is <code>localhost</code> .														
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.														
-s --secure	If set to <code>true</code> , 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 <code>false</code> .														



	<code>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
	<code>-I --type</code>	This is the type of component to be listed. The options are application, ejb, web, and connector. If nothing is specified, then all of the components are listed.
OPERANDS	target	This is the name of the target upon which the command operates. The valid options are instance, cluster, 'domain,' and 'server.' This option is used in Enterprise Edition only.
EXAMPLES	<p><b>EXAMPLE 1</b> Using list-components</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>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">show-component-status(1)</a> , <a href="#">list-sub-components(1)</a>	

## list-connection-groups(1)

NAME	list-connection—groups – gets the connection groups
SYNOPSIS	<b>list-connection-groups</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> <i>http_listener_ID</i>
DESCRIPTION	Gets the profiler element associated with the named server instance..
OPTIONS	--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.  <i>http_listener_ID</i> a unique identifier for the HTTP listener.
EXAMPLES	asadmin% <b>list-connection-groups</b>
INTERFACE EQUIVALENT SEE ALSO	unknown  <a href="#">create-connection-group(1)</a> <a href="#">delete-connection-group(1)</a>

NAME	list-connector-connection-pools – gets connector connection pools that have been created	
SYNOPSIS	<b>list-connector-connection-pools</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help]	
DESCRIPTION	Use this command to list connector connection pools that have been created.	
OPTIONS	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
	-H --host	The machine name where the domain application server is running. The default value is localhost.
	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	-s --secure	If set to 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.

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

-I --interactive            If set to true (default), only the required password options are prompted.

-h --help                 Displays the help text for the command.

### EXAMPLES

**EXAMPLE 1** Using the list-connector-connection-pools command

```
asadmin> list-connector-connection-pools --user admin -passwordfile filename
jms/qConnPool
Command list-connector-connection-pools executed successfully
```

Where jms/qConnPool is the connector connection pool that is listed.

### EXIT STATUS

0  
  command executed successfully

1  
  error in executing the command

### SEE ALSO

[create-connector-connection-pool\(1\)](#),  
[delete-connector-connection-pool\(1\)](#)

NAME	list-connector-resources – gets all connector resources
SYNOPSIS	<b>list-connector-resources</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--target <i>target</i> ]
DESCRIPTION	This command lists all connector resources.
OPTIONS	<div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>--passwordfile</div> <div>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </div> </div> <div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> </div> <div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> </div> <div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> </div> <div> <div>-t --terse</div> <div>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.</div> </div> <div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div> </div>

## list-connector-resources(1)

	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
<b>OPERANDS</b>	<i>target</i>	<p>In Enterprise Edition only, this operand specifies which configurations you can list. Valid values are:</p> <ul style="list-style-type: none"> <li>■ <i>server</i>, which lists the connector resources in the current domain and is the default.</li> <li>■ <i>domain</i>, which lists the connector resources in the current domain.</li> <li>■ <i>cluster_name</i>, which lists the connector resources in a cluster.</li> <li>■ <i>instance_name</i>, which lists the connector resources for a particular instance.</li> </ul>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the list-connector-resources command</p> <pre>asadmin&gt; list-connector-resources --user admin --passwordfile --password --host instance1 --port 5001 target server resource10 resource20 resource35 Command list-connector-resources executed successfully.</pre>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">create-connector-resource(1)</a> , <a href="#">delete-connector-resource(1)</a>	

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

NAME	list-connector-security-map – lists the security maps belonging to the specified connector connection pool										
SYNOPSIS	<pre>list-connector-security-maps --user <i>admin_user</i>     [--passwordfile <i>filename</i>] [--host <i>host_name</i>] [--port <i>port_number</i>]     [--secure -s] [--terse=<i>false</i>] [--echo=<i>false</i>] [--interactive=<i>true</i>]     [--help] [--verbose=<i>false</i>] [--securitymap <i>security_map_name</i>]     <i>connector_connection_pool_name</i></pre>										
DESCRIPTION	<p>Use this command to list the security maps belonging to the specified connector connection pool.</p> <p>For this command to succeed, you must have first created a connector connection pool using the create-connector-connection-pool command.</p> <p>This command is supported in remote mode only.</p>										
OPTIONS	<p>If an option has a short option name, then the short option precedes the long option name. Short options have one dash whereas long options have two dashes.</p> <table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td> <p>This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</p> </td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	<p>This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</p>	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
-u --user	The authorized domain application server administrative username.										
-w --password	The --password option is deprecated. Use --passwordfile instead.										
--passwordfile	<p>This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</p>										
-H --host	The machine name where the domain application server is running. The default value is localhost.										
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.										

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

	<p><b>-s --secure</b> If set to true, uses SSL/TLS to communicate with the domain application server.</p> <p><b>-t --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>-e --echo</b> Setting to true will echo the command line statement on the standard output. Default is false.</p> <p><b>-I --interactive</b> If set to true (default), only the required password options are prompted.</p> <p><b>-h --help</b> Displays the help text for the command.</p> <p><b>--target</b> This option is deprecated in this release.</p> <p><b>--verbose</b> This property returns a list including the identity, principals, and security name.</p> <p><b>--securitymap</b> This property specifies the name of the security map contained within the connector connection pool from which the identity and principals should be listed. With this option, -verbose is redundant.</p>
<b>OPERANDS</b>	<p><i>connector_connection_pool_name</i> name of the connector connection pool for which you want to list security maps.</p>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using list-connector-security-maps with the security map option</p> <p>It is assumed that the connector pool has already been created using the create-connector-pool command.</p> <pre>asadmin&gt; list-connector-security-maps --user admin --passwordfile pwd_file.txt --securitymap mysecuremap securityPool1</pre> <p>Command list-connector-security-maps executed successfully.</p> <p>One security map (mysecuremap) is listed for the securityPool1 pool.</p> <p><b>EXAMPLE 2</b> Using list-connector-security-maps without the security map option</p> <p>It is assumed that the connector pool has already been created using the create-connector-pool command.</p> <pre>asadmin&gt; list-connector-security-maps --user admin --passwordfile pwd_file.txt securityPool1</pre> <p>Command list-connector-security-maps executed successfully.</p> <p>All security maps contained within securityPool1 are listed.</p>
<b>EXIT STATUS</b>	<p>0 command executed successfully</p>



list-connector-security-maps(1)

1  
error in executing the command

**SEE ALSO** [delete-connector-security-map\(1\)](#), [create-connector-security-map\(1\)](#),  
[update-connector-security-map\(1\)](#)

## list-custom-resources(1)

NAME	list-custom-resources – gets all custom resources	
SYNOPSIS	<b>list-custom-resources</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [ <i>target</i> ]	
DESCRIPTION	Use this command to list custom resources. This command is supported in remote mode only.	
OPTIONS	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
	-H --host	The machine name where the domain application server is running. The default value is localhost.
	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	-s --secure	If set to 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.

		list-custom-resources(1)
	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
OPERANDS	<i>target</i>	In Enterprise Edition only, this operand specifies the location of the custom resources. Valid values are "domain," cluster, or instance. The default is domain.
EXAMPLES	<b>EXAMPLE 1</b> Using the list-custom-resources command <pre>asadmin&gt; list-custom-resources --user admin --passwordfile filename --host plum --port 4848 target6 custom_resource01 custom_resource02 Command list-custom-resources executed successfully.</pre>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-custom-resource(1)</a> , <a href="#">delete-custom-resource(1)</a>	

## list-domains(1)

<b>NAME</b>	list-domains – lists the domains in the specified domain directory
<b>SYNOPSIS</b>	<b>list-domains</b> [--domaindir <i>install_dir</i> /domains] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ]
<b>DESCRIPTION</b>	<p>Use the <code>list-domains</code> command to list the domain. If the domain directory is not specified, the domain in the default <i>install_dir</i>/domains directory is listed. If there is more than one domain, the <i>domain_name</i> operand must be identified.</p> <p>This command is supported in local mode only.</p>
<b>OPTIONS</b>	<p>--domaindir                      The directory where the domains are located. If specified, the path must be accessible in the filesystem. If not specified, the domain in the default <i>install_dir</i>/domains directory are listed.</p> <p>-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.</p> <p>-e --echo                         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 the list-domains command</p> <pre>asadmin&gt; list-domains List of domains: domain1 running samples not running</pre> <p>Where: the domain1 and samples are the domains located in the default <i>install_dir</i>/domains directory.</p>
<b>EXIT STATUS</b>	<p>0 command executed successfully</p> <p>1 error in executing the command</p>
<b>ERROR CODES</b>	<p>0 error message</p> <p>1 error message</p>
<b>SEE ALSO</b>	<a href="#">create-domain(1)</a> , <a href="#">delete-domain(1)</a> , <a href="#">start-domain(1)</a> , <a href="#">stop-domain(1)</a> ,

NAME	list-file-groups – lists file groups	
SYNOPSIS	<b>list-file-groups</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--name <i>username</i> ] [ <i>target</i> ]	
DESCRIPTION	<p>Use this command to administer user support by the file realm authentication. This command lists available groups in the file user. If the --name option is not specified, all groups are listed.</p> <p>This command is supported in remote mode only.</p>	
OPTIONS	-u --user -w --password --passwordfile -H --host -p --port -s --secure -t --terse	<p>The authorized domain application server administrative username.</p> <p>The --password option is deprecated. Use --passwordfile instead.</p> <p>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</p> <p>The machine name where the domain application server is running. The default value is localhost.</p> <p>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</p> <p>If set to true, uses SSL/TLS to communicate with the domain application server.</p> <p>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>

## list-file-groups(1)

	<code>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
	<code>-name</code>	identifies the name of file user to be created.
<b>OPERANDS</b>	<i>target</i>	<p>In Enterprise Edition, this operand specifies which configurations you can list. Valid values are:</p> <ul style="list-style-type: none"> <li>■ <i>server</i>, which lists the file groups in the current server and is the default.</li> <li>■ <i>domain</i>, which lists the file groups in the current domain.</li> <li>■ <i>cluster_name</i>, which lists the file groups in a cluster.</li> <li>■ <i>instance_name</i>, which lists the file groups for a particular instance.</li> </ul>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the list-file-groups command</p> <pre>asadmin&gt; list-file-groups --user admin1 --password adminadmin1 --host pigeon --port 5001 --name sample_user</pre> <p>Command list-file-groups executed successfully</p>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">create-file-user(1)</a> , <a href="#">update-file-user(1)</a> , <a href="#">delete-file-user(1)</a> , <a href="#">list-file-users(1)</a>	

NAME	list-file-users – creates a list of file users	
SYNOPSIS	<b>list-file-users</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [ <i>target</i> ]	
DESCRIPTION	The list-file-users command creates a list of file users supported by file realm authentication.	
OPTIONS	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
	-H --host	The machine name where the domain application server is running. The default value is localhost.
	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	-s --secure	If set to 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.

## list-file-users(1)

<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
<code>-h --help</code>	Displays the help text for the command.
<code>---target</code>	in Enterprise Edition, specifies the target to which you are deploying. Valid values are <ul style="list-style-type: none"><li>■ <code>server</code>, which deploys the component to the default server instance <code>server</code> and is the default value</li><li>■ <code>domain</code>, which deploys the component to the domain.</li><li>■ <code>cluster_name</code>, which deploys the component to every server instance in the cluster.</li><li>■ <code>instance_name</code>, which deploys the component to a particular sever instance.</li></ul>

### EXAMPLES

**EXAMPLE 1** Using the list-file-users command

Create file users with the `create-file-user` command before you use this command..

```
asadmin> list-file-users plum
sample_user05
sample_user08
sample_user12
```

### EXIT STATUS

0	command executed successfully
1	error in executing the command

### SEE ALSO

[create-file-user\(1\)](#), [delete-file-user\(1\)](#)



NAME	list-http-listeners – lists the existing HTTP listeners
SYNOPSIS	<b>list-http-listeners</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [ <i>target</i> ]
DESCRIPTION	The list-http-listeners command lists the existing HTTP listeners. This command is supported in remote mode only.
OPTIONS	<div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>--passwordfile</div> <div>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </div> </div> <div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> </div> <div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> </div> <div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> </div> <div> <div>-t --terse</div> <div>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.</div> </div> <div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div> </div>

## list-http-listeners(1)

	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
OPERANDS	<i>target</i>	<p>In Enterprise Edition, this operand specifies the target for which the HTTP listeners are to be listed. Valid values are:</p> <ul style="list-style-type: none"> <li>■ <i>server</i>, which lists the listeners for the default server instance <i>server</i> and is the default value</li> <li>■ <i>configuration_name</i>, which lists the listeners for the specified configuration</li> <li>■ <i>cluster_name</i>, which lists the listeners for the specified cluster</li> <li>■ <i>instance_name</i>, which lists the listeners for a particular server instance</li> </ul>
EXAMPLES	<p><b>EXAMPLE 1</b> Using the list-http-listeners command</p> <p>The following command lists all the HTTP listeners for the server instance:</p> <pre>asadmin&gt; list-http-listeners --user admin1 --passwordfile passwords.txt --host pigeon --port 5001 http-listener-1 http-listener-2 admin-listener Command list-http-listeners executed successfully.</pre>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-http-listener(1)</a> , <a href="#">delete-http-listener(1)</a>	

NAME	list-iiop-listeners – lists the existing IIOP listeners	
SYNOPSIS	<b>list-iiop-listeners</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [ <i>target</i> ]	
DESCRIPTION	The list-iiop-listeners command lists the existing IIOP listeners. This command is supported in remote mode only.	
OPTIONS	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
	-H --host	The machine name where the domain application server is running. The default value is localhost.
	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	-s --secure	If set to 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.

## list-iiop-listeners(1)

OPERANDS	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
OPERANDS	<i>target</i>	In Enterprise Edition, this operand specifies the target for which the IIOP listeners are to be listed. Valid values are: <ul style="list-style-type: none"> <li>■ <i>server</i>, which lists the listeners in the default server instance <i>server</i> and is the default value</li> <li>■ <i>configuration_name</i>, which lists the listeners in the specified configuration</li> <li>■ <i>cluster_name</i>, which lists the listeners in the specified cluster</li> <li>■ <i>instance_name</i>, which lists the listeners in a particular server instance</li> </ul>
EXAMPLES	<p><b>EXAMPLE 1</b> Using the list-iiop-listeners command</p> <p>The following command lists all the IIOP listeners for the server instance:</p> <pre>asadmin&gt; list-iiop-listeners --user admin --passwordfile passwords.txt --host fuyako --port 7070 orb-listener-1 SSL SSL_MUTUALAUTH sample_iiop_listener Command list-iiop-listeners executed successfully.</pre>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-iiop-listener(1)</a> , <a href="#">delete-iiop-listener(1)</a>	

NAME	list-instances – lists all the instances along with their status														
SYNOPSIS	<pre><b>list-instances</b> --user <i>admin_user</i> [--passwordfile <i>filename</i>]                     [--host <i>host_name</i>] [--port <i>port_number</i>] [--secure -s]                     [--terse=false] [--echo=false] [--interactive=true] [--help]                     [<i>target</i>]</pre>														
DESCRIPTION	<p>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.</p>														
OPTIONS	<table> <tr> <td><code>-u --user</code></td><td>The authorized domain application server administrative username.</td></tr> <tr> <td><code>-w --password</code></td><td>The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.</td></tr> <tr> <td><code>--passwordfile</code></td><td>This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=<i>password</i></code>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code>, <code>AS_ADMIN_USERPASSWORD</code>, <code>AS_ADMIN_SAVEDMASTERPASSWORD</code>, <code>AS_ADMIN_MQPASSWORD</code>, <code>AS_ADMIN_ALIASPASSWORD</code>, and so on.</td></tr> <tr> <td><code>-H --host</code></td><td>The machine name where the domain application server is running. The default value is <code>localhost</code>.</td></tr> <tr> <td><code>-p --port</code></td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td><code>-s --secure</code></td><td>If set to true, uses SSL/TLS to communicate with the domain application server.</td></tr> <tr> <td><code>-t --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> </table>	<code>-u --user</code>	The authorized domain application server administrative username.	<code>-w --password</code>	The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.	<code>--passwordfile</code>	This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=<i>password</i></code> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code> , <code>AS_ADMIN_USERPASSWORD</code> , <code>AS_ADMIN_SAVEDMASTERPASSWORD</code> , <code>AS_ADMIN_MQPASSWORD</code> , <code>AS_ADMIN_ALIASPASSWORD</code> , and so on.	<code>-H --host</code>	The machine name where the domain application server is running. The default value is <code>localhost</code> .	<code>-p --port</code>	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	<code>-s --secure</code>	If set to true, uses SSL/TLS to communicate with the domain application server.	<code>-t --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>-u --user</code>	The authorized domain application server administrative username.														
<code>-w --password</code>	The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.														
<code>--passwordfile</code>	This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=<i>password</i></code> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code> , <code>AS_ADMIN_USERPASSWORD</code> , <code>AS_ADMIN_SAVEDMASTERPASSWORD</code> , <code>AS_ADMIN_MQPASSWORD</code> , <code>AS_ADMIN_ALIASPASSWORD</code> , and so on.														
<code>-H --host</code>	The machine name where the domain application server is running. The default value is <code>localhost</code> .														
<code>-p --port</code>	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.														
<code>-s --secure</code>	If set to true, uses SSL/TLS to communicate with the domain application server.														
<code>-t --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.														

## list-instances(1)

	<code>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
OPERANDS	<i>target</i>	This is the name of the target domain the instances you want listed are associated with.
EXAMPLES	<p><b>EXAMPLE 1</b> Using list-instances in local mode</p> <pre>asadmin&gt; list-instances --user admin --passwordfile passwords.txt instance1</pre> <p>Command list-instances executed successfully</p> <p>Where: instance1 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 pigeon --port 4849</pre> <p>remote_instance1 running</p> <p>Command list-instances executed successfully</p> <p>Where: remote_instance1 associates with user, passwordfile, host, and port of the remote machine.</p>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-instance(1)</a>	

NAME	list-javamail-resources – lists the existing JavaMail session resources
SYNOPSIS	<b>list-javamail-resources</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [ <i>target</i> ]
DESCRIPTION	The command lists the existing JavaMail session resources. This command is supported in remote mode only.
OPTIONS	<div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>--passwordfile</div> <div>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </div> </div> <div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> </div> <div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> </div> <div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> </div> <div> <div>-t --terse</div> <div>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.</div> </div> <div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div> </div>

## list-javamail-resources(1)

	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
<b>OPERANDS</b>	<i>target</i>	<p>In Enterprise Edition, this operand specifies the target for which the JavaMail session resources are to be listed. Valid values are:</p> <ul style="list-style-type: none"> <li>■ <i>server</i>, which lists the resources for the default server instance <i>server</i> and is the default value</li> <li>■ <i>domain</i>, which lists the resources for the domain</li> <li>■ <i>cluster_name</i>, which lists the resources for the specified cluster</li> <li>■ <i>instance_name</i>, which lists the resources for a particular server instance</li> </ul>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the list-javamail-resources command</p> <p>The following command lists the JavaMail session resources for the server instance:</p> <pre>asadmin&gt; list-javamail-resources --user admin1 --passwordfile passwords.txt --host pigeon --port 5001 mail/MyMailSession Command list-javamail-resources executed successfully.</pre>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">create-javamail-resource(1)</a> , <a href="#">delete-javamail-resource(1)</a>	



NAME	list-jdbc-connection-pools – lists all JDBC connection pools	
SYNOPSIS	<b>list-jdbc-connection-pools</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help]	
DESCRIPTION	Use this command to get the JDBC connection pools that have been created. This command is supported in remoted mode only.	
OPTIONS	<div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>--passwordfile</div> <div>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </div> </div> <div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> </div> <div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> </div> <div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> </div> <div> <div>-t --terse</div> <div>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.</div> </div> <div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div> </div>	

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

	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
OPERANDS	<i>target</i>	The target operand is deprecated.
EXAMPLES	<b>EXAMPLE 1</b> Using the list-jdbc-connection-pools command <pre>asadmin&gt; list-jdbc-connection-pools --user admin --password adminadmin --host plum --port 7070 my_connection_pool</pre> <p>Where: my_connection_pool is the JDBC connection pool listed.</p>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-jdbc-connection-pool(1)</a> , <a href="#">delete-jdbc-connection-pool(1)</a>	

NAME	list-jdbc-resources – gets all JDBC resources
SYNOPSIS	<b>list-jdbc-resources</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] <i>target</i>
DESCRIPTION	The list-jdbc-resource command produces a list of JDBC resources that have been created. This command is supported in remote mode only.
OPTIONS	<div>-u --user</div> <div>The authorized domain application server administrative username.</div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> <div>--passwordfile</div> <div>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> <div>-t --terse</div> <div>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.</div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div>

## list-jdbc-resources(1)

	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
OPERANDS	<i>target</i>	<p>In Enterprise Edition, this operand specifies which jdbc resources you can list. Valid values are:</p> <ul style="list-style-type: none"><li>■ <i>server</i>, which lists the jdbc resources in the current server and is the default.</li><li>■ <i>domain</i>, which lists the jdbc resources in the current domain.</li><li>■ <i>cluster_name</i>, which lists the jdbc resources in a cluster.</li><li>■ <i>instance_name</i>, which lists the jdbc resources for a particular instance.</li></ul>
EXAMPLES	<p><b>EXAMPLE 1</b> Using the list-jdbc-resources command</p> <pre>asadmin&gt; list-jdbc-resources instance1 sample_jdbc_resource02 sample_jdbc_resource05 Command executed successfully.</pre>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-jdbc-resource(1)</a> , <a href="#">delete-jdbc-resource(1)</a>	

NAME	list-jmsdest – lists the existing JMS physical destinations																
SYNOPSIS	<pre>list-jmsdest --user admin_user [--passwordfile filename]                [--host host_name] [--port port_number] [--secure -s]                [--terse=false] [--echo=false] [--interactive=true] [--help]                [desttype type] [target]</pre>																
DESCRIPTION	The list-jmsdest command lists the JMS physical destinations. This command is supported in remote mode only.																
OPTIONS	<table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td>-s --secure</td><td>If set to 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> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	-s --secure	If set to 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.
-u --user	The authorized domain application server administrative username.																
-w --password	The --password option is deprecated. Use --passwordfile instead.																
--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.																
-H --host	The machine name where the domain application server is running. The default value is localhost.																
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.																
-s --secure	If set to 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.																

## list-jmsdest(1)

	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
	-T --desttype	The type of JMS destinations to be listed. Valid values are <i>topic</i> and <i>queue</i> .
OPERANDS	<i>target</i>	<p>In Enterprise Edition, this operand specifies the target for which the physical destinations are to be listed. Although the <code>list-jmsdest</code> command is related to resources, a physical destination is created and deleted using the JMS Service, which is part of the configuration. Valid values are:</p> <ul style="list-style-type: none"> <li>■ <i>server</i>, which lists the physical destinations for the default server instance <i>server</i> and is the default value</li> <li>■ <i>configuration_name</i>, which lists the physical destinations for the specified configuration</li> <li>■ <i>cluster_name</i>, which lists the physical destinations for the specified cluster</li> <li>■ <i>instance_name</i>, which lists the physical destinations for a particular server instance</li> </ul>
EXAMPLES	<p><b>EXAMPLE 1</b> Using the <code>list-jmsdest</code> command</p> <p>The following command lists all the physical destinations for the default server instance:</p> <pre>asadmin&gt; list-jmsdest --user admin --passwordfile passwords.txt --host bluestar --port 4848 PhysicalQueue queue {} PhysicalTopic topic {} Command list-jmsdest executed successfully.</pre>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-jmsdest(1)</a> , <a href="#">delete-jmsdest(1)</a>	

NAME	list-jms-resources – lists the JMS resources																
SYNOPSIS	<pre>list-jms-resources --user admin_user [--passwordfile filename]                     [--host host_name] [--port port_number] [--secure -s]                     [--terse=false] [--echo=false] [--interactive=true] [--help]                     [--restype type] [target]</pre>																
DESCRIPTION	The <code>list-jms-resources</code> command lists the existing JMS resources (destination and connection factory resources). This command is supported in remote mode only.																
OPTIONS	<table> <tr> <td><code>-u --user</code></td><td>The authorized domain application server administrative username.</td></tr> <tr> <td><code>-w --password</code></td><td>The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.</td></tr> <tr> <td><code>--passwordfile</code></td><td>This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code>, <code>AS_ADMIN_USERPASSWORD</code>, <code>AS_ADMIN_SAVEDMASTERPASSWORD</code>, <code>AS_ADMIN_MQPASSWORD</code>, <code>AS_ADMIN_ALIASPASSWORD</code>, and so on.</td></tr> <tr> <td><code>-H --host</code></td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td><code>-p --port</code></td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td><code>-s --secure</code></td><td>If set to true, uses SSL/TLS to communicate with the domain application server.</td></tr> <tr> <td><code>-t --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>-e --echo</code></td><td>Setting to true will echo the command line statement on the standard output. Default is false.</td></tr> </table>	<code>-u --user</code>	The authorized domain application server administrative username.	<code>-w --password</code>	The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.	<code>--passwordfile</code>	This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code> , <code>AS_ADMIN_USERPASSWORD</code> , <code>AS_ADMIN_SAVEDMASTERPASSWORD</code> , <code>AS_ADMIN_MQPASSWORD</code> , <code>AS_ADMIN_ALIASPASSWORD</code> , and so on.	<code>-H --host</code>	The machine name where the domain application server is running. The default value is localhost.	<code>-p --port</code>	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	<code>-s --secure</code>	If set to true, uses SSL/TLS to communicate with the domain application server.	<code>-t --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>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
<code>-u --user</code>	The authorized domain application server administrative username.																
<code>-w --password</code>	The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.																
<code>--passwordfile</code>	This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code> , <code>AS_ADMIN_USERPASSWORD</code> , <code>AS_ADMIN_SAVEDMASTERPASSWORD</code> , <code>AS_ADMIN_MQPASSWORD</code> , <code>AS_ADMIN_ALIASPASSWORD</code> , and so on.																
<code>-H --host</code>	The machine name where the domain application server is running. The default value is localhost.																
<code>-p --port</code>	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.																
<code>-s --secure</code>	If set to true, uses SSL/TLS to communicate with the domain application server.																
<code>-t --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>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.																

## list-jms-resources(1)

	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
	--restype	The JMS resource type, which can be either <code>javax.jms.Topic</code> , <code>javax.jms.Queue</code> , <code>javax.jms.ConnectionFactory</code> , <code>javax.jms.TopicConnectionFactory</code> , or <code>javax.jms.QueueConnectionFactory</code> .
OPERANDS	<i>target</i>	<p>In Enterprise Edition, this operand specifies the target for which the JMS resources are to be listed. Valid values are:</p> <ul style="list-style-type: none"> <li>■ <code>server</code>, which lists the resources for the default server instance <code>server</code> and is the default value</li> <li>■ <code>domain</code>, which lists the resources for the domain</li> <li>■ <code>cluster_name</code>, which lists the resources for the specified cluster</li> <li>■ <code>instance_name</code>, which lists the resources for a particular server instance</li> </ul>
EXAMPLES	<p><b>EXAMPLE 1</b> Using the <code>list-jms-resources</code> command to list all JMS resources</p> <p>The following command lists all JMS resources:</p> <pre>asadmin&gt; list-jms-resources --user admin1 --passwordfile passwords.txt jms/Queue jms/Topic jms/QueueConnectionFactory jms/DurableTopicConnectionFactory Command list-jms-resources executed successfully.</pre> <p><b>EXAMPLE 2</b> Using the <code>list-jms-resources</code> command to list JMS resources of a specified type</p> <p>The following command lists all topic connection factories:</p> <pre>asadmin&gt; list-jms-resources --user admin1 --passwordfile passwords.txt --restype javax.jms.TopicConnectionFactory jms/DurableTopicConnectionFactory jms/TopicConnectionFactory Command list-jms-resources executed successfully.</pre>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command



NAME	list-jndi-entries – browses and queries the JNDI tree	
SYNOPSIS	<b>list-jndi-entries</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--context <i>context-name</i> ] <i>target</i>	
DESCRIPTION	Use this command to browse and query the JNDI tree. This command is supported in remote mode only.	
OPTIONS	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
	-H --host	The machine name where the domain application server is running. The default value is localhost.
	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	-s --secure	If set to 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.

## list-jndi-entries(1)

	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
	<code>--context</code>	The name of the JNDI context or subcontext. If context is not specified, all entries in the naming service are returned. If context (such as <i>ejb</i> ) is specified, all those entries are returned.
OPERANDS	<i>target</i>	In Enterprise Edition, this operand specifies which configurations you can list. Valid values are 'domain,' instance, cluster, or "server." The default is server.
EXAMPLES	<b>EXAMPLE 1</b> Using the list-jndi-entries command  asadmin> <code>list-jndi-entries --user admin1 --passwordfile /password --context jdbc server</code> Jndi Entries for server within jdbc context: __TimerPool: javax.naming.Reference __TimerPool__pm: javax.naming.Reference Command list-jndi-resources executed successfully	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-jndi-resource(1)</a> , <a href="#">delete-jndi-resource(1)</a>	

NAME	list-jndi-resources – lists all existing JNDI resources														
SYNOPSIS	<b>list-jndi-resources</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [ <i>target</i> ]														
DESCRIPTION	<p>Use the list-jndi-resources command to identify all existing JNDI resources. This command is supported in remote mode only.</p> <p>The target operand is only valid for Enterprise Edition.</p>														
OPTIONS	<table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td>-s --secure</td><td>If set to 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> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	-s --secure	If set to 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.
-u --user	The authorized domain application server administrative username.														
-w --password	The --password option is deprecated. Use --passwordfile instead.														
--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.														
-H --host	The machine name where the domain application server is running. The default value is localhost.														
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.														
-s --secure	If set to 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.														

## list-jndi-resources(1)

	<code>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
<b>OPERANDS</b>	<i>target</i>	In Enterprise Edition, this operand specifies which jndi resources you can list. Valid values 'server,' 'domain,' cluster, instance. The default is server.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using the list-jndi-resources command <pre>asadmin&gt; list-jndi-resources --user admin --passwordfile passwords.txt --host plum --port 4849 --ta jndi_resource1 jndi_resource2 jndi_resource3 Command list-jndi-resources executed successfully</pre>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">create-jndi-resource(1)</a> , <a href="#">delete-jndi-resource(1)</a>	

NAME	list-lifecycle-modules – lists the lifecycle modules
SYNOPSIS	<b>list-lifecycle-modules</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [ <i>target</i> ]
DESCRIPTION	Lists the lifecycle modules. The lifecycle modules provide a means of running short or long duration Java-based tasks within the application server environment. This command is supported in remote mode only.
OPTIONS	<div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>--passwordfile</div> <div>           This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </div> </div> <div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> </div> <div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> </div> <div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> </div> <div> <div>-t --terse</div> <div>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.</div> </div>

## list-lifecycle-modules(1)

OPERANDS	-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.
	-h --help	Displays the help text for the command.
	target	This is the name of the resulting location. The valid targets for this command are configuration, instance, cluster, or server. This is used by EE only.
EXAMPLES	<b>EXAMPLE 1</b> Using list-lifecycle-modules  asadmin> list-lifecycle-modules --user admin --passwordfile adminpassword.txt --host fuyako --port 7070 customSetup Server1  Where: customSetup is the lifecycle module listed and targetserver is the default target.	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-lifecycle-module(1)</a> , <a href="#">delete-lifecycle-module(1)</a>	

## list-message-security-providers(1)

NAME	list-message-security-providers – enables administrators to list all security message providers (provider-config sub-elements) for the given message layer (message-security-config element of domain.xml)										
SYNOPSIS	<b>list-message-security-providers</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] --layer <i>message_layer</i> [target]										
DESCRIPTION	<p>Enables administrators to list all security message providers (provider-config sub-elements) for the given message layer (message-security-config element of domain.xml).</p> <p>This command is supported in remote mode only.</p>										
OPTIONS	<p>If an option has a short option name, then the short option preceeds the long option name. Short options have one dash whereas long options have two dashes.</p> <table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
-u --user	The authorized domain application server administrative username.										
-w --password	The --password option is deprecated. Use --passwordfile instead.										
--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.										
-H --host	The machine name where the domain application server is running. The default value is localhost.										
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.										

## list-message-security-providers(1)

	-s --secure	If set to 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.
	-h --help	Displays the help text for the command.
	--layer	The message-layer for which the provider has to be listed. The default value is SOAP.
OPERANDS	<i>target</i>	Lists all the objects of the specified type in the named configuration referenced by the named server instance or cluster. In Enterprise Edition, valid values include: <ul style="list-style-type: none"> <li>■ <i>server</i>, which deploys the component to the default server instance <i>server</i> and is the default value</li> <li>■ <i>config</i>, which deploys the component to the domain.</li> <li>■ <i>cluster</i>, which deploys the component to every server instance in the cluster.</li> <li>■ <i>instance</i>, which deploys the component to a particular server instance.</li> </ul>
EXAMPLES	<p><b>EXAMPLE 1</b> Using list-message-security-providers</p> <p>The following example shows how to list message security providers for a message layer.</p> <pre>asadmin&gt; list-message-security-providers --user admin --layer SOAP Listing of all message security providers</pre>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-message-security-provider(1)</a> , <a href="#">delete-message-security-provider(1)</a>	



NAME	list-password-aliases – lists all password aliases	
SYNOPSIS	<b>list-password-aliases</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help]	
DESCRIPTION	This command lists all of the password aliases.	
OPTIONS	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
	-H --host	The machine name where the domain application server is running. The default value is localhost.
	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	-s --secure	If set to 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.

## list-password-aliases(1)

-I --interactive	If set to true (default), only the required password options are prompted.
-h --help	Displays the help text for the command.

### EXAMPLES

**EXAMPLE 1** Using list-password-aliases

```
asadmin> list-password-aliases
```

Command list-password-aliases executed successfully

### EXIT STATUS

0	command executed successfully
1	error in executing the command

### SEE ALSO

[delete-password-alias\(1\)](#), [update-password-alias\(1\)](#),  
[create-password-alias\(1\)](#)

NAME	list-persistence-resources – gets all the persistence resources	
SYNOPSIS	<b>list-persistence-resources</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] <i>target</i>	
DESCRIPTION	Gets all the persistence resources. This command is supported in remote mode only.	
OPTIONS	<div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>--passwordfile</div> <div>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </div> </div> <div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> </div> <div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> </div> <div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> </div> <div> <div>-t --terse</div> <div>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.</div> </div> <div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div> </div>	

## list-persistence-resources(1)

	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
OPERANDS	<i>target</i>	Specifies the target for which you are listing all persistence resources. This option is available only in the Sun Java System Application Server Enterprise Edition. Valid values are <ul style="list-style-type: none"> <li>■ <i>server</i>, which deploys the component to the default server instance <i>server</i> and is the default value</li> <li>■ <i>domain</i>, which deploys the component to the domain.</li> <li>■ <i>cluster_name</i>, which deploys the component to every server instance in the cluster.</li> <li>■ <i>instance_name</i>, which deploys the component to a particular sever instance.</li> </ul>
EXAMPLES	<b>EXAMPLE 1</b> Using list-persistence-resources <pre>asadmin&gt; list-persistence-resources --user admin --passwordfile secret.txt --host pigeon --port 5001</pre> Command list-persistence-resources executed successfully	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-persistence-resource(1)</a> , <a href="#">delete-persistence-resource(1)</a>	

NAME	list-resource-adapter-configs – lists the configuration information created in domain.xml for the connector module	
SYNOPSIS	<b>list-resource-adapter-configs</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--verbose= <i>false</i> ] [--rname <i>connectorModuleName</i> ] [ <i>target</i> ]	
DESCRIPTION	<p>This command 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>	
OPTIONS	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	<p>This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</p>
	-H --host	The machine name where the domain application server is running. The default value is localhost.
	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	-s --secure	If set to true, uses SSL/TLS to communicate with the domain application server.

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

	-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.
	-h --help	Displays the help text for the command.
	--verbose	Setting this property lists the properties that are configured.
	--raname	This is the connector module name.
OPERANDS	<i>target</i>	This is the name of the target upon which the command is operating. The valid targets for this command are instance, cluster, "domain," and "server." Server is the default option.  This operand is used in EE only.
EXAMPLES	<b>EXAMPLE 1</b> Using list-resource-adapter-configs <pre>asadmin&gt; list-resource-adapter-configs --user admin1 --passwordfile pfile1</pre> Command list-resource-adapter-configs executed successfully	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-resource-adapter-config(1)</a> , <a href="#">delete-resource-adapter-config(1)</a>	

NAME	list-sub-components – lists EJBs or Servlets in deployed module or module of deployed application
SYNOPSIS	<b>list-sub-components</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--type   <i>ejbs</i>   <i>servlets</i> ] [--appname <i>appname</i> ] <i>modulename</i>
DESCRIPTION	<p>This command lists 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. The --appname option functions only when the given module is standalone. To display a specific module in an application, you must specify the module name and the --appname option. This command is supported in remote mode only.</p>
OPTIONS	<p>-u --user                      The authorized domain application server administrative username.</p> <p>-w --password                The --password option is deprecated. Use --passwordfile instead.</p> <p>--passwordfile              This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</p> <p>-H --host                    The machine name where the domain application server is running. The default value is localhost.</p> <p>-p --port                    The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</p> <p>-s --secure                  If set to true, uses SSL/TLS to communicate with the domain application server.</p>

## list-sub-components(1)

	-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.
	-h --help	Displays the help text for the command.
	--type	This is the type of component to be listed. The options are ejbs and servlets. If nothing is specified, then all of the components are listed.
	--appname	To display the sub components of a module in the deployed application, you must specify the modulename and use the --appname option. However, this option is required only when the desired output is the sub component of an embedded module of a deployed application.
<b>OPERANDS</b>	modulename	This is the 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 --modulename --appname appname1 modulename</pre> <p>Command list-sub-components executed successfully.</p>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">deploy(1)</a> , <a href="#">deploydir(1)</a> , <a href="#">undeploy(1)</a> , <a href="#">enable(1)</a> , <a href="#">disable(1)</a> , <a href="#">list-components(1)</a>	



## list-system-properties(1)

NAME	list-system-properties – lists the system properties of the domain, configuration, cluster, or server instance
SYNOPSIS	<b>lists-system-properties</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [target <i>target_name</i> ]
DESCRIPTION	Shared or clustered server instances will often need to override attributes defined in their referenced configuration. Any configuration attribute in a server instance can be overridden through a system property of the corresponding name. This command lists the system properties of a domain, configuration, cluster, or server instance.
OPTIONS	<div>-u --user</div> <div>The authorized domain application server administrative username.</div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> <div>--passwordfile</div> <div>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div>

## list-system-properties(1)

	-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.
	-h --help	Displays the help text for the command.
OPERANDS	<i>target</i>	<p>In Enterprise Edition, specifies the target on which you are listing the system properties. Valid values are</p> <ul style="list-style-type: none"> <li>■ <i>domain</i>, which lists the system properties defined for the domain</li> <li>■ <i>configuration_name</i>, lists the system properties for the named configuration as well as those the cluster inherits from the domain.</li> <li>■ <i>cluster_name</i>, which lists the system properties defined for the named cluster as well as those the cluster inherits from its configuration and the domain.</li> <li>■ <i>instance_name</i>, which lists the system properties defined for the named server instance as well as those the server inherits from its cluster (if the instance is clustered), its configuration, and the domain.</li> </ul>
EXAMPLES	<p><b>EXAMPLE 1</b> Using list-system-properties</p> <pre>asadmin&gt; list-system-properties --user admin --passwordfile password.txt --host localhost --port 4849 http-listener-port=1088 mycluster http-listener-port=1088 Command list-system-properties executed successfully.</pre>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-system-properties(1)</a> , <a href="#">delete-system-property(1)</a>	

NAME	list-threadpools – lists all the threadpools	
SYNOPSIS	<b>list-threadpools</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--target <i>target_name</i> ]	
DESCRIPTION	Lists all the thread pools. This command is supported in remote mode only.	
OPTIONS	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
	-H --host	The machine name where the domain application server is running. The default value is localhost.
	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	-s --secure	If set to 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.

## list-threadpools(1)

-I --interactive	If set to true (default), only the required password options are prompted.
-h --help	Displays the help text for the command.
--target	<p>In Enterprise Edition, specifies the target for which you are listing the threadpools. Valid values are</p> <ul style="list-style-type: none"><li>■ <i>server</i>, which creates the listener for the default server instance <i>server</i> and is the default value</li><li>■ <i>configuration_name</i>, which creates the listener for the named configuration</li><li>■ <i>cluster_name</i>, which creates the listener for every server instance in the cluster</li><li>■ <i>instance_name</i>, which creates the listener for a particular server instance</li></ul>

### EXAMPLES

#### EXAMPLE 1 Using list-threadpools

```
asadmin> list-threadpools --user admin --passwordfile password.txt
Command list-threadpools executed successfully
```

### EXIT STATUS

0	command executed successfully
1	error in executing the command

### SEE ALSO

[create-threadpool\(1\)](#), [delete-threadpool\(1\)](#)

NAME	list-timers – lists all of the timers owned by server instance(s)	
SYNOPSIS	<b>list-timers</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] <i>target</i>	
DESCRIPTION	This command lists the timers owned by a specific server instance or a cluster of server instances. Administrators can use this information to decide whether to do a timer migration or to verify that a migration has been completed successfully. This command is supported in remote mode only.	
OPTIONS	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
	-H --host	The machine name where the domain application server is running. The default value is localhost.
	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	-s --secure	If set to 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.

## list-timers(1)

	<code>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
OPERANDS	<i>target</i>	The target is either a stand-alone server instance or a cluster. If the target is the stand-alone instance, then the number of timers owned by the instance is listed. If the target is a cluster, then the number of timers owned by each instance in the cluster is listed.
EXAMPLES	<b>EXAMPLE 1</b> Using list-timers  This is an example of how the command is used.  <code>asadmin&gt;list-timers --user admin --passwordfile filename target dancer</code> The list-timers command was executed successfully.	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">migrate-timers(1)</a>	

NAME	list-transaction-id – lists the transactions IDs														
SYNOPSIS	<b>list-transaction-id</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [ <i>target</i> ]														
DESCRIPTION	<p>This command lists the transaction IDs in the named target.</p> <p>This command is supported in remote mode only.</p>														
OPTIONS	<table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td>-s --secure</td><td>If set to 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> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	-s --secure	If set to 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.
-u --user	The authorized domain application server administrative username.														
-w --password	The --password option is deprecated. Use --passwordfile instead.														
--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.														
-H --host	The machine name where the domain application server is running. The default value is localhost.														
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.														
-s --secure	If set to 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.														

## list-transaction-id(1)

	<code>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
<b>OPERANDS</b>	<i>target</i>	This is used in Enterprise Edition only. This is the name of the target upon which the command operates.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using list-transaction-id  asadmin> <code>list-transaction-id --user admin --passwordfile password.txt --target server</code> The list-transaction-id command executed successfully	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<code>freeze-transaction-service(1)</code> , <code>unfreeze-transaction-service(1)</code> , <code>rollback-transaction(1)</code>	



NAME	list-virtual-servers – lists the existing virtual servers
SYNOPSIS	<b>list-virtual-servers</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [ <i>target</i> ]
DESCRIPTION	The list-virtual-servers command lists the existing virtual servers. This command is supported in remote mode only.
OPTIONS	<div>-u --user</div> <div>The authorized domain application server administrative username.</div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> <div>--passwordfile</div> <div>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> <div>-t --terse</div> <div>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.</div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div>

## list-virtual-servers(1)

	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
OPERANDS	<i>target</i>	<p>In Enterprise Edition, this operand specifies the target for which the virtual servers are to be listed. Valid values are:</p> <ul style="list-style-type: none"> <li>■ <i>server</i>, which lists the virtual servers in the default server instance <i>server</i> and is the default value</li> <li>■ <i>configuration_name</i>, which lists the virtual servers in the specified configuration</li> <li>■ <i>cluster_name</i>, which lists the virtual servers in the specified cluster</li> <li>■ <i>instance_name</i>, which lists the virtual servers in a particular server instance</li> </ul>
EXAMPLES	<p><b>EXAMPLE 1</b> Using the list-virtual-servers command</p> <p>The following command lists all the virtual servers for the server instance:</p> <pre>asadmin&gt; list-virtual-servers --user admin --passwordfile passwords.txt --host localhost --port 4848 server __asadmin Command list-virtual-servers executed successfully.</pre>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">create-virtual-server(1)</a> , <a href="#">delete-virtual-server(1)</a>	

NAME	multimode – allows you to execute multiple commands while preserving environment settings and remaining in the asadmin utility
SYNOPSIS	<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> ]
DESCRIPTION	<p>Use <i>multimode</i> to process the asadmin 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 asadmin option names set in this mode are used for all the subsequent commands. You can set your environment and run commands until you exit <i>multimode</i> 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 <i>multimode</i> 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.</p> <p>This command is supported in local mode only.</p>
OPTIONS	<p><b>--file</b> reads the commands as defined in the file.</p> <p><b>--printprompt</b> allows the printing of asadmin 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>
EXAMPLES	<p><b>EXAMPLE 1</b> Using <i>multimode</i> to execute multiple commands</p> <pre>% asadmin multimode --file commands_file.txt</pre> <p>Where: % is the system prompt. The administrative commands are executed from the <i>commands_file.txt</i> file.</p>
EXIT STATUS	<p>0 command executed successfully</p> <p>1 error in executing the command</p>
SEE ALSO	<a href="#">export(1)</a> , <a href="#">unset(1)</a>

## package-appclient( 1M)

NAME	package-appclient – packs the application client container libraries and jar files				
SYNOPSIS	<b>package-appclient</b>				
DESCRIPTION	<p>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 <i>appserver_install_dir/lib/appclient/appclient.jar</i>. The appclient.jar file provides an application client container package targeted at remote hosts that do not contain a server installation.</p> <p>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.</p> <p>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</p> <p>After unjarring on the client machine, modify <i>appclient_install_dir/config/asenv.conf</i> (asenv.bat for Windows) as follows:</p> <ul style="list-style-type: none"><li>■ set AS_WEBSERVICES_LIB to <i>appclient_install_dir/lib</i></li><li>■ set AS_NSS to <i>appclient_install_dir/lib</i> (<i>appclient_install_dir\bin</i> for Windows)</li><li>■ set AS_IMQ_LIB to <i>appclient_install_dir/imq/lib</i></li><li>■ set AS_INSTALL to <i>appclient_install_dir</i></li><li>■ set AS_JAVA to your JDK 1.4 home directory</li><li>■ set AS_ACC_CONFIG to <i>appclient_install_dir/config/sun-acc.xml</i></li></ul> <p>Modify <i>appclient_install_dir/config/sun-acc.xml</i> as follows:</p> <ul style="list-style-type: none"><li>■ Ensure the DOCTYPE file references <i>appclient_install_dir/lib/dtds</i></li><li>■ Ensure that target-server address attribute references the server machine.</li><li>■ Ensure that target-server port attribute references the ORB port on the remote machine.</li><li>■ Ensure that log-service references a log file; if the user wants to put log messages to a log file.</li></ul> <p>Modify <i>appclient_install_dir/bin/appclient</i> (appclient.bat for Windows) as follows:</p> <ul style="list-style-type: none"><li>■ change token %CONFIG_HOME% to <i>appclient_install_dir/config</i></li></ul>				
ATTRIBUTES	<p>See attributes(5) for descriptions of the following attributes:</p> <table><thead><tr><th>ATTRIBUTE TYPE</th><th>ATTRIBUTE VALUE</th></tr></thead><tbody><tr><td>Interface Stability</td><td>Unstable</td></tr></tbody></table>	ATTRIBUTE TYPE	ATTRIBUTE VALUE	Interface Stability	Unstable
ATTRIBUTE TYPE	ATTRIBUTE VALUE				
Interface Stability	Unstable				
SEE ALSO	<a href="#">appclient (1M)</a>				

NAME	ping-connection-pools – tests that a connection pool is usable										
SYNOPSIS	<b>ping-connection-pools</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] <i>pool_name</i>										
DESCRIPTION	<p>This command 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>Either a JDBC or connector connectionpool with authentication can be created. You can either use a <code>-property</code> option to specify user, password, or other connection information using the command line, or specify the connection information in the xml descriptor file.</p> <p>Before pinging a connection pool, you must create the connection pool with authentication and ensure that the enterprise server or database is started.</p>										
OPTIONS	<table> <tr> <td><code>-u --user</code></td><td>The authorized domain application server administrative username.</td></tr> <tr> <td><code>-w --password</code></td><td>The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.</td></tr> <tr> <td><code>--passwordfile</code></td><td>           This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code>, <code>AS_ADMIN_USERPASSWORD</code>, <code>AS_ADMIN_SAVEDMASTERPASSWORD</code>, <code>AS_ADMIN_MQPASSWORD</code>, <code>AS_ADMIN_ALIASPASSWORD</code>, and so on.         </td></tr> <tr> <td><code>-H --host</code></td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td><code>-p --port</code></td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> </table>	<code>-u --user</code>	The authorized domain application server administrative username.	<code>-w --password</code>	The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.	<code>--passwordfile</code>	This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code> , <code>AS_ADMIN_USERPASSWORD</code> , <code>AS_ADMIN_SAVEDMASTERPASSWORD</code> , <code>AS_ADMIN_MQPASSWORD</code> , <code>AS_ADMIN_ALIASPASSWORD</code> , and so on.	<code>-H --host</code>	The machine name where the domain application server is running. The default value is localhost.	<code>-p --port</code>	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
<code>-u --user</code>	The authorized domain application server administrative username.										
<code>-w --password</code>	The <code>--password</code> option is deprecated. Use <code>--passwordfile</code> instead.										
<code>--passwordfile</code>	This option replaces the <code>--password</code> option. Using the <code>--password</code> option on the command line or through the environment is deprecated. The <code>--passwordfile</code> option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the <code>AS_ADMIN_</code> prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: <code>AS_ADMIN_PASSWORD=password</code> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include <code>AS_ADMIN_MAPPEDPASSWORD</code> , <code>AS_ADMIN_USERPASSWORD</code> , <code>AS_ADMIN_SAVEDMASTERPASSWORD</code> , <code>AS_ADMIN_MQPASSWORD</code> , <code>AS_ADMIN_ALIASPASSWORD</code> , and so on.										
<code>-H --host</code>	The machine name where the domain application server is running. The default value is localhost.										
<code>-p --port</code>	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.										

## ping-connection-pools(1)

	-s --secure	If set to 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.
	-h --help	Displays the help text for the command.
<b>OPERANDS</b>	<i>pool_name</i>	This is the name of the pool to test.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the ping-connection-pool command</p> <pre>asadmin&gt; ping-connection-pool --user admin1 --passwordfile pwordfile</pre> <p>Command ping-connection-pool executed successfully</p> <p>Where: asadmin is the command prompt and sampleConnectionPool is the name of the connection pool to ping.</p>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">create-connector-connection-pool(1)</a> , <a href="#">create-jdbc-connection-pool(1)</a>	

NAME	recover-transactions – manually recovers pending transactions														
SYNOPSIS	<pre><b>recover-transactions</b> --user <i>admin_user</i> [--passwordfile <i>filename</i>]                         [--host <i>host_name</i>] [--port <i>port_number</i>] [--secure -s]                         [--terse=<i>false</i>] [--echo=<i>false</i>] [--interactive=<i>true</i>] [--help]                         [--txlogdir <i>transaction_log_directory</i> --destination <i>destination_server_name</i>]                         <i>server_name</i></pre>														
DESCRIPTION	The function of this command is to manually recover pending transactions. This is used in remote mode only.														
OPTIONS	<table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td>-s --secure</td><td>If set to 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> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	-s --secure	If set to 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.
-u --user	The authorized domain application server administrative username.														
-w --password	The --password option is deprecated. Use --passwordfile instead.														
--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.														
-H --host	The machine name where the domain application server is running. The default value is localhost.														
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.														
-s --secure	If set to 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.														

## recover-transactions(1)

	<code>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
	<code>--txlogdir</code>	The transaction log directory of the server (provided in the <i>server_name</i> operand) for which the recovery needs to be done.
	<code>--destination</code>	The destination server which will perform the recovery for the server (provided in the <i>server_name</i> operand). The destination server should be running.
<b>OPERANDS</b>	<i>server_name</i>	This is the name of the server for which the recovery needs to be done. If this server is running, recovery will be performed by the same server. In this case the <code>--txlogdir</code> and <code>--destination</code> options should not be given. If the server is not running, then the <code>--txlogdir</code> and <code>--destination</code> options are required.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using the commandname</p> <p>This is a basic example of how this command is used.</p> <pre>asadmin&gt;recover-transactions serverid1</pre> <p>Transaction recovered.</p> <p>REVIEWERS:I had problems creating the example. Is this correct?</p>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">none</a>	



<b>NAME</b>	restore-domain – restores files from backup	
<b>SYNOPSIS</b>	<b>restore-domain</b> [--domainindir <i>domain_directory</i> ] [--filename <i>backup_filename</i> ] [--description <i>description</i> ] [--terse= <i>false</i> ] [--verbose= <i>false</i> ] [ <i>domain_name</i> ]	
<b>DESCRIPTION</b>	This command restores files under the domain from a backup directory. The restore-domain command is supported in local mode only.	
<b>OPTIONS</b>	--domainindir	This option specifies the parent directory of the domain upon which the command will operate. The default is install_dir/domains.
	--filename	The restore is performed using the specified zip file as the source.
	--description	A description can contain any string to help identify the particular backup. The description is displayed as part of the information for any backup.
	-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.
	-t --verbose	Indicates that output data is displayed with detailed information. Default is false.
<b>OPERANDS</b>	<i>domain_name</i>	This is the name of the domain to restore. If the domain is not specified and only one domain exists, it will be used automatically.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using restore-domain asadmin> <b>restore-domain</b> --domainindir <b>directory1</b> --filename <b>samplefile.zip</b> The command restore-domain executed successfully.	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">backup-domain(1)</a> , <a href="#">list-backups(1)</a>	

## rollback-transaction(1)

NAME	rollback-transaction – rolls back the named transaction
SYNOPSIS	<b>rollback-transaction</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--target <i>target_name</i> ] [ <i>transaction_id</i> ]
DESCRIPTION	Rolls back the named transaction. This command is supported in remote mode only.
OPTIONS	<div>-u --user</div> <div>The authorized domain application server administrative username.</div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> <div>--passwordfile</div> <div>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> <div>-t --terse</div> <div>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.</div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div>

		rollback-transaction(1)
	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
	--target	<p>In Enterprise Edition, specifies the target on which you are rolling back the transactions. Valid values are</p> <ul style="list-style-type: none"> <li>■ <i>server</i>, which creates the listener for the default server instance <i>server</i> and is the default value</li> <li>■ <i>configuration_name</i>, which creates the listener for the named configuration</li> <li>■ <i>cluster_name</i>, which creates the listener for every server instance in the cluster</li> <li>■ <i>instance_name</i>, which creates the listener for a particular server instance</li> </ul>
OPERANDS	<i>transaction_id</i>	identifier for the transaction to be rolled back..
EXAMPLES	<b>EXAMPLE 1</b> Using rollback-transaction asadmin> <b>rollback-transaction --user admin --passwordfile password.txt --target server 0000000000</b>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">freeze-transaction-service(1)</a> , <a href="#">unfreeze-transaction-service(1)</a>	

set(1)

NAME	set – sets the values of attributes																
SYNOPSIS	<b>set</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [ <i>attributename=value</i> ]																
DESCRIPTION	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.																
OPTIONS	<table><tr><td>-u --user</td><td>The authorized domain application server administrative username.</td></tr><tr><td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr><tr><td>--passwordfile</td><td>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</td></tr><tr><td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr><tr><td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr><tr><td>-s --secure</td><td>If set to 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></table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	-s --secure	If set to 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.
-u --user	The authorized domain application server administrative username.																
-w --password	The --password option is deprecated. Use --passwordfile instead.																
--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.																
-H --host	The machine name where the domain application server is running. The default value is localhost.																
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.																
-s --secure	If set to 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.
	-h --help	Displays the help text for the command.
OPERANDS	<i>attributename=value</i>	identifies the attribute name and its value. See the <i>Reference</i> for a listing of the available attribute names.
EXAMPLES	<b>EXAMPLE 1</b> Using set asadmin> set --user admin --passwordfile password.txt --host localhost --port 4848 server.transaction-service.automatic-recovery=true	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">get(1)</a> , <a href="#">list(1)</a>	

## show-component-status(1)

NAME	show-component-status – displays the status of the deployed component	
SYNOPSIS	<b>show-component-status</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--target <i>target (defaultserver)</i> ] <i>component-name</i>	
DESCRIPTION	The command <code>show-component-status</code> , gets the status of the deployed component. The status is a string representation returned by the server. The possible status strings include: <code>enabled</code> or <code>disabled</code> . This command is supported in remote mode only.	
OPTIONS	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
	-H --host	The machine name where the domain application server is running. The default value is localhost.
	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	-s --secure	If set to 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.

		show-component-status(1)
	-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.
	-h --help	Displays the help text for the command.
	--target	This is the name of the target upon which the command acts. The valid targets for this command are instance, cluster, "domain," and "server." The default is server. The target option is used in Enterprise Edition only.
OPERANDS	component-name	This is the name of the component to be listed.
EXAMPLES	<b>EXAMPLE 1</b> Using show-component-status asadmin> <b>show-component-status sampleApplication</b>  Status of sampleApplication is enabled	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	list-components(1), list-sub-components(1)	

## shutdown(1)

NAME	shutdown – brings down the administration server
SYNOPSIS	<b>shutdown</b> <code>[--user admin_user] [--password admin_password] [--host localhost]</code> <code>[--port 4848] [--passwordfile filename] [--secure   -s]</code>
DESCRIPTION	shutdown gracefully brings down the administration server and all the running instances. You must manually start the administration server to bring it up again.
OPTIONS	--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.
EXAMPLES	<b>EXAMPLE 1</b> Using the shutdown command <pre>asadmin&gt; shutdown --user admin --password adminadmin --host bluestar --port 4848</pre> Waiting for admin server to shutdown... Admin server has been shutdown
EXIT STATUS	0 command executed successfully 1 error in executing the command
INTERFACE EQUIVALENT SEE ALSO	Administration Server page <a href="#">start-instance(1)</a> , <a href="#">stop-instance(1)</a> , <a href="#">restart-instance(1)</a> , <a href="#">start-domain(1)</a> , <a href="#">stop-domain(1)</a>



NAME	start-appserv – starts the domains in the specified domains directory								
SYNOPSIS	<b>start-appserv</b> [--domaindir <i>install_dir</i> /domains] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ]								
DESCRIPTION	<p>This command is deprecated use the start-domain command instead. Use the start-appserv command to start the domains in specified domain directory. If the domain directory is not specified the domains in the default <i>install_dir</i>/domains directory are started. The start-appserv command requires that the user has set up an AS_ADMIN_USER environment variable and that all domains have the same administration user. You are prompted for the master password for each domain (unless the --savemasterpassword option was specified at the domain creation time.</p> <p>The start-appserv command functions correctly if every domain is created with --savemasterpassword. Remember that the user and password do not need to be passed to start-appserv in the Platform Edition. If --savemasterpassword is not specified, then you are prompted for the master password for every domain.</p> <p>This command is supported in local mode only.</p>								
OPTIONS	<table> <tr> <td>--domaindir</td><td>The directory where the domains are to be started. If specified, the path must be accessible in the filesystem. If not specified, the domain in the default <i>install_dir</i>/domains directory is started.</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 to 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>	--domaindir	The directory where the domains are to be started. If specified, the path must be accessible in the filesystem. If not specified, the domain in the default <i>install_dir</i> /domains directory is started.	-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 to the standard output. Default is false.	-I --interactive	If set to true (default), only the required password options are prompted.
--domaindir	The directory where the domains are to be started. If specified, the path must be accessible in the filesystem. If not specified, the domain in the default <i>install_dir</i> /domains directory is started.								
-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 to the standard output. Default is false.								
-I --interactive	If set to true (default), only the required password options are prompted.								
EXAMPLES	<p><b>EXAMPLE 1</b> Using the start—appserv command</p> <pre>asadmin&gt; start-appserv Starting Domain sampleDomain, please wait Domain sampleDomain started Command start-appserv executed successfully</pre> <p>Where: the sampleDomain domain in the default domains directory is started.</p>								
EXIT STATUS	<p>0 command executed successfully</p> <p>1 error in executing the command</p>								
ERROR CODES	<p>0 error message</p>								

start-appserv(1)

1

error message

**SEE ALSO** [create-domain\(1\)](#), [delete-domain\(1\)](#), [start-domain\(1\)](#), [stop-domain\(1\)](#),  
[list-domains\(1\)](#), [stop-appserv\(1\)](#)

NAME	start-domain – starts a domain	
SYNOPSIS	<b>start-domain</b> [--domaindir <i>install_dir/domains</i> ] [--user <i>admin_user</i> ] [--passwordfile <i>file_name</i> ] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--verbose= <i>false</i> ] [--debug= <i>false</i> ] [ <i>domain_name</i> ]	
DESCRIPTION	<p>Use the start-domain command to start a domain. If the domain directory is not specified, the domain in the default <i>install_dir/domains</i> directory is started. If there is more than one domain, the <i>domain_name</i> operand must be identified.</p> <p>This command is supported in local mode only.</p>	
OPTIONS	--domaindir	The directory where the domain is to be started. If specified, the path must be accessible in the filesystem. If not specified, the domain in the default <i>install_dir/domains</i> directory is started.
	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	-W --passwordfile	The file containing the domain application server password associated with the administrative instance. The password is defined in the following form: AS_ADMIN_PASSWORD= <i>password</i> . Where <i>password</i> is the actual administrator password for the domain.
	-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 to the standard output. Default is false.
	-I --interactive	If set to true (default), only the required password options are prompted.
	--verbose	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.
	--debug	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.
	--domaindir	The directory where the domain is to be started. If specified, the path must be accessible in the filesystem. If not specified, the domain in the default <i>install_dir/domains</i> directory is started.

## start-domain(1)

	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=password, where password is the actual administrator password. Other passwords that can be specified include MAPPEDPASSWORD, USERPASSWORD, SAVEDMASTERPASSWORD, MQPASSWORD, ALIASPASSWORD, and so on.
	-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 to the standard output. Default is false.
	-I --interactive	If set to true (default), only the required password options are prompted.
	--verbose	By default this flag is set to false. If set to true, detailed server startup output is displayed. On UNIX, press CTRL-C to kill the server. On Windows, press Ctrl-Break to kill the server. Press CTRL-\\ to print a thread dump.
	--debug	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.
OPERANDS	domain_name	The unique name of the domain you wish to start.
EXAMPLES	<b>EXAMPLE 1</b> Using the start-domain command <pre>asadmin&gt; start-domain --domainindir /export/domains --user admin --passwordfile pass sampleDomain</pre> Where: the sampleDomain domain in the /export/domains directory is started using admin password stored in the pass file.	
EXIT STATUS	0	command executed successfully

start-domain(1)

1  
error in executing the command

**SEE ALSO** [create-domain\(1\)](#), [delete-domain\(1\)](#), [stop-domain\(1\)](#), [list-domains\(1\)](#)

## start-instance(1)

NAME	start-instance – starts a server instance
SYNOPSIS	<b>start-instance</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] <i>instance_name</i>
DESCRIPTION	This command starts an instance with the instance name you specify.
OPTIONS	<div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>--passwordfile</div> <div>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </div> </div> <div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> </div> <div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> </div> <div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> </div> <div> <div>-t --terse</div> <div>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.</div> </div> <div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div> </div>

		start-instance(1)
	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
OPERANDS	<i>instance_name</i>	This is the name of the server instance to start.
EXAMPLES	<b>EXAMPLE 1</b> Using start-instance asadmin> <b>start-instance -- instance_name instance1</b> Instance instance1 started	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">delete-instance(1)</a> , <a href="#">create-instance(1)</a> , <a href="#">stop-instance(1)</a> , <a href="#">restart-instance(1)</a> , <a href="#">start-domain(1)</a> , <a href="#">stop-domain(1)</a>	

## stop-appserv(1)

NAME	stop-appserv – stops the domains in the specified domains directory
SYNOPSIS	<b>stop-appserv</b> [--domaindir <i>install_dir</i> /domains] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ]
DESCRIPTION	<p>This command is deprecated use the stop-domain command instead. Use the stop-appserv command to stop the domains in specified domain directory. If the domain directory is not specified the domains in the default <i>install_dir</i>/domains directory are stopped.</p> <p>This command is supported in local mode only.</p>
OPTIONS	<p>--domaindir                      The directory where the domains are 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</i>/domains directory.</p> <p>-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.</p> <p>-e --echo                         Setting to true will echo the command line statement on to the standard output. Default is false.</p> <p>-I --interactive                  If set to true (default), only the required password options are prompted.</p>
EXAMPLES	<p><b>EXAMPLE 1</b> Using the stop—appserv command</p> <pre>asadmin&gt; stop-appserv Stopping Domain sampleDomain, please wait Domain sampleDomain stopped Command stop-appserv executed successfully</pre> <p>Where: the sampleDomain domain in the default domains directory is stopped.</p>
EXIT STATUS	<p>0 command executed successfully</p> <p>1 error in executing the command</p>
ERROR CODES	<p>0 error message</p> <p>1 error message</p>
SEE ALSO	<a href="#">create-domain(1)</a> , <a href="#">delete-domain(1)</a> , <a href="#">start-domain(1)</a> , <a href="#">stop-domain(1)</a> , <a href="#">list-domains(1)</a> , <a href="#">start-appserv(1)</a>



NAME	stop-domain – stops the domain
SYNOPSIS	<b>stop-domain</b> [--domaindir <i>install_dir/domains</i> ] [--user <i>admin_user</i> ] [--passwordfile <i>file_name</i> ] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--verbose= <i>false</i> ] [--debug= <i>false</i> ] [ <i>domain_name</i> ]
DESCRIPTION	Use the stop-domain command to stop a domain. If the domain directory is not specified, the domain in the default <i>install_dir/domains</i> directory is stopped. If there is more than one domain, the <i>domain_name</i> operand must be identified.
OPTIONS	<div> <div>--domaindir</div> <div>The directory where the domain is to be started. If specified, the path must be accessible in the filesystem. If not specified, the domain in the default <i>install_dir/domains</i> directory is started.</div> </div> <div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>-W --passwordfile</div> <div>The file containing the domain application server password associated with the administrative instance. The password is defined in the following form: AS_ADMIN_PASSWORD=<i>password</i>. Where <i>password</i> is the actual administrator password for the domain.</div> </div> <div> <div>-t --terse</div> <div>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.</div> </div> <div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on to the standard output. Default is false.</div> </div> <div> <div>-I --interactive</div> <div>If set to true (default), only the required password options are prompted.</div> </div> <div> <div>--verbose</div> <div>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.</div> </div> <div> <div>--debug</div> <div>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.</div> </div> <div> <div>--domaindir</div> <div>The directory where the domain is to be started. If specified, the path must be accessible in the filesystem. If not specified, the domain in the default <i>install_dir/domains</i> directory is started.</div> </div>

## stop-domain(1)

	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=password, where password is the actual administrator password. Other passwords that can be specified include MAPPEDPASSWORD, USERPASSWORD, SAVEDMASTERPASSWORD, MQPASSWORD, ALIASPASSWORD, and so on.
	-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 to the standard output. Default is false.
	-I --interactive	If set to true (default), only the required password options are prompted.
	--verbose	By default this flag is set to false. If set to true, detailed server startup output is displayed. On UNIX, press CTRL-C to kill the server. On Windows, press Ctrl-Break to kill the server. Press CTRL-\\ to print a thread dump.
	--debug	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.
OPERANDS	domain_name	The unique name of the domain you wish to start.
EXAMPLES	<b>EXAMPLE 1</b> Using start-domain asadmin> stop-domain --domaindir /export/domains --user admin --passwordfile pass sampleDomain Where: the sampleDomain domain in the /export/domains directory is stopped using admin password sto	
EXIT STATUS	0	command executed successfully

stop-domain(1)

1  
error in executing the command

**SEE ALSO** [start-domain\(1\)](#), [create-domain\(1\)](#), [delete-domain\(1\)](#)

## stop-instance(1)

NAME	stop-instance – stops a server instance
SYNOPSIS	<b>stop-instance</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] <i>instance_name</i>
DESCRIPTION	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.
OPTIONS	<div>-u --user</div> <div>The authorized domain application server administrative username.</div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> <div>--passwordfile</div> <div>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> <div>-t --terse</div> <div>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.</div>

	<code>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
OPERANDS	<i>instance_name</i>	This is the name of the server instance to stop.
EXAMPLES	<b>EXAMPLE 1</b> Using <code>stop-instance</code> in local mode  asadmin> <code>stop-instance --user admin1 --passwordfile passwords.txt instance1</code> Command <code>stop-instance</code> executed successfully  <b>EXAMPLE 2</b> Using <code>stop-instance</code> in remote mode  asadmin> <code>stop-instance --user admin1 --password passwords.txt --host pigeon --port 4849 instance2</code> Command <code>stop-instance</code> executed successfully  Where: the <code>instance2</code> is associated with user, password, host and port of the remote machine.	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">delete-instance(1)</a> , <a href="#">start-instance(1)</a> , <a href="#">create-instance(1)</a> , <a href="#">restart-instance(1)</a>	

## undeploy(1)

NAME	undeploy – removes a component from the domain application server
SYNOPSIS	<b>undeploy</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--droptables <i>true false</i> ] [--cascade=false] [--target <i>target</i> ] <i>component_name</i>
DESCRIPTION	<p>undeploy removes the specified component in the domain application server.</p> <p>The --droptables 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>
OPTIONS	<p>-u --user                   The authorized domain application server administrative username.</p> <p>-w --password              The --password option is deprecated. Use --passwordfile instead.</p> <p>--passwordfile            This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.</p> <p>-H --host                   The machine name where the domain application server is running. The default value is localhost.</p> <p>-p --port                   The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</p> <p>-s --secure                 If set to true, uses SSL/TLS to communicate with the domain application server.</p> <p>-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.</p>

<code>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
<code>-h --help</code>	Displays the help text for the command.
<code>--droptables</code>	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, it defaults to the entries specified in the deployment descriptors.
<code>--cascade</code>	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 resource adapter, the resource adapter is undeployed. This option is applicable to connectors (resource adapters) and applications.
<code>--target</code>	This option is available only in the Sun Java System Application Server Enterprise Edition. Specifies the target from which you are undeploying. Valid values are: <ul style="list-style-type: none"> <li>■ <code>server</code>, which undeploys the component from the default server instance <code>server</code> and is the default value</li> <li>■ <code>domain</code>, which undeploys the component from the domain.</li> <li>■ <code>cluster_name</code>, which undeploys the component from every server instance in the cluster.</li> <li>■ <code>instance_name</code>, which undeploys the component from a particular sever instance.</li> </ul>

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

## undeploy(1)

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

```
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\(1\)](#)



NAME	unfreeze-transaction-service – resumes all suspended transactions
SYNOPSIS	<b>unfreeze-transaction-service</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--interactive= <i>true</i> ] [--help] [--target <i>target_name</i> ]
DESCRIPTION	Resumes all the suspended inflight transactions. Invoke this command on an already frozen transaction. This command is supported in remote mode only.
OPTIONS	<div> <div>-u --user</div> <div>The authorized domain application server administrative username.</div> </div> <div> <div>-w --password</div> <div>The --password option is deprecated. Use --passwordfile instead.</div> </div> <div> <div>--passwordfile</div> <div>           This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.         </div> </div> <div> <div>-H --host</div> <div>The machine name where the domain application server is running. The default value is localhost.</div> </div> <div> <div>-p --port</div> <div>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</div> </div> <div> <div>-s --secure</div> <div>If set to true, uses SSL/TLS to communicate with the domain application server.</div> </div> <div> <div>-t --terse</div> <div>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.</div> </div> <div> <div>-e --echo</div> <div>Setting to true will echo the command line statement on the standard output. Default is false.</div> </div>

## unfreeze-transaction-service(1)

	-I --interactive	If set to true (default), only the required password options are prompted.
	-h --help	Displays the help text for the command.
	--target	Supported in Enterprise edition only. This option specifies the target on which you are unfreezing the Transaction Service. Valid values are <ul style="list-style-type: none"> <li>■ <i>server</i>, which creates the listener for the default server instance <i>server</i> and is the default value</li> <li>■ <i>configuration_name</i>, which creates the listener for the named configuration</li> <li>■ <i>cluster_name</i>, which creates the listener for every server instance in the cluster</li> <li>■ <i>instance_name</i>, which creates the listener for a particular server instance</li> </ul>
OPERANDS	--target	Supported in Enterprise edition only. This option specifies the target on which you are unfreezing the Transaction Service. Valid values are <ul style="list-style-type: none"> <li>■ <i>server</i>, which creates the listener for the default server instance <i>server</i> and is the default value</li> <li>■ <i>configuration_name</i>, which creates the listener for the named configuration</li> <li>■ <i>cluster_name</i>, which creates the listener for every server instance in the cluster</li> <li>■ <i>instance_name</i>, which creates the listener for a particular server instance</li> </ul>
EXAMPLES	<b>EXAMPLE 1</b> Using unfreeze-transaction-service <pre>asadmin&gt; unfreeze-transaction-service --user admin --passwordfile password.txt --target server</pre>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">freeze-transaction-service(1)</a> , <a href="#">rollback-transaction(1)</a>	

unset(1)

NAME	unset – removes one or more variables from the multimode environment
SYNOPSIS	<b>unset</b> [ <i>env_var</i> *
DESCRIPTION	Removes one or more variables you set for the multimode environment. The variables and their associated values will no longer exist in the environment.
OPERANDS	<i>env_var</i> environment variable to be removed.
EXAMPLES	<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 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_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</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>
EXIT STATUS	<p>0     command executed successfully</p> <p>1     error in executing the command</p>
SEE ALSO	<a href="#">export(1)</a> , <a href="#">multimode(1)</a>

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

NAME	update-connector-security-map – creates or modifies a security map for the specified connector connection pool						
SYNOPSIS	<pre> <b>update-connector-security-map</b> --user <i>admin_user</i>     [--passwordfile <i>filename</i>] [--host <i>host_name</i>] [--port <i>port_number</i>]     [--secure -s] [--terse=false] [--echo=false] [--interactive=true]     [--help] --poolname <i>connector_connection_pool_name</i>     [--addprincipals <i>principal_name1</i> [, <i>principal_name1</i>] *   --addusergroups <i>user_group1</i> [,     [--removeprincipals <i>principal_name1</i> [, <i>principal_name2</i>] *]     [--removeusergroups <i>user_group1</i> [, <i>user_group2</i>] *]     [--mappedusername <i>username</i> ] <i>security_map_name</i> </pre>						
DESCRIPTION	<p>Use this command to create or modify a security map for the specified connector connection pool. If the security map is not present, one is created. If a specific security map is specified, the components of the security map (user name, groups, and principals) are provided.</p> <p>For this command to succeed, you must have first created a connector connection pool using the create-connector-connection-pool command.</p> <p>The enterprise information system (EIS) is any system that holds the information. It can be a mainframe, a messaging system, a database system, or an application.</p> <p>This command is supported in remote mode only.</p>						
OPTIONS	<p>If an option has a short option name, then the short option preceeds the long option name. Short options have one dash whereas long options have two dashes.</p> <table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASEPASSWORD, and so on.</td></tr> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASEPASSWORD, and so on.
-u --user	The authorized domain application server administrative username.						
-w --password	The --password option is deprecated. Use --passwordfile instead.						
--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASEPASSWORD, and so on.						

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

-H --host	The machine name where the domain application server is running. The default value is localhost.
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
-s --secure	If set to 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.
-h --help	Displays the help text for the command.
--target	This option is deprecated in this release.
--poolname	This property specifies the name of the connector connection pool to which the security map that is to be updated or created belongs.
--addprincipals	This property specifies a comma-separated list of EIS-specific principals to be added. Use either the -addprincipals or -addusergroups options, but not both.
--addusergroups	This property specifies a comma-separated list of EIS user groups to be added. Use either the -addprincipals or -addusergroups options, but not both at the same time.
--removeprincipals	This property specifies a comma-separated list of EIS-specific principals to be removed.
--removeusergroups	This property specifies a comma-separated list of EIS user groups to be removed.
--mappedusername	This property specifies the EIS username.
--mappedpassword	The --mappedpassword option is deprecated. Use --passwordfile pointing to a file that contains an entry in the following format: AS_ADMIN_MAPPEDPASSWORD= <i>mapped-password</i> . If not specified using the passwordfile option, the user will be prompted for this password by the asadmin

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

	command-line tool.
<b>OPERANDS</b>	<i>security_map_name</i> name of the security map to be created or updated.
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using update-connector-security-map</p> <p>It is assumed that the connector pool has already been created using the create-connector-pool command.</p> <pre>asadmin&gt; update-connector-security-map --user admin --poolname connector-pool1 --addprincipals principal1, principal2 securityMap1</pre> <p>Command update-connector-security-map 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>	<a href="#">delete-connector-security-map(1)</a> , <a href="#">list-connector-security-maps(1)</a> , <a href="#">create-connector-security-map(1)</a>

NAME	update-file-user – updates a current file user as specified	
SYNOPSIS	<b>update-file-user</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--userpassword <i>user_passsword</i> ] [--groups <i>user_groups[:user_groups]*</i> ] <i>username</i>	
DESCRIPTION	This command updates an existing entry in keyfile using the specified <i>user_name</i> , <i>user_password</i> and groups. Multiple groups can be entered by separating them, with a colon ":"	
OPTIONS	-u --user	The authorized domain application server administrative username.
	-w --password	The --password option is deprecated. Use --passwordfile instead.
	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
	-H --host	The machine name where the domain application server is running. The default value is localhost.
	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.
	-s --secure	If set to 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.

## update-file-user(1)

	<code>-e --echo</code>	Setting to true will echo the command line statement on the standard output. Default is false.
	<code>-I --interactive</code>	If set to true (default), only the required password options are prompted.
	<code>-h --help</code>	Displays the help text for the command.
	<code>--userpassword</code>	This is the password of the file user.
	<code>--groups</code>	This is the name of the group to which the file user belongs.
<b>OPERANDS</b>	<i>username</i>	This is the name of file user to be deleted.
<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 --username dance Command update-file-user executed successfully</pre> <p>Where: the sample_user is the file user updated with the updated user password, groups, and user name.</p>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">delete-file-user(1)</a> , <a href="#">list-file-users(1)</a> , <a href="#">create-file-user(1)</a> , <a href="#">list-file-groups(1)</a>	



NAME	update-password-alias – updates a password alias												
SYNOPSIS	<b>updates-password-alias</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--aliaspassword <i>alias_password</i> ] <i>aliasname</i>												
DESCRIPTION	<p>This command updates the transaction IDs in the named target. An alias is a token of the form \${ALIAS=password-alias-password}. The password corresponding to the alias name is stored in encrypted form. The password-alias commands take both a secure interactive form (in which the user is prompted for all information) and a more script-friendly form, in which the password is propagated on the command line.</p> <p>This command is supported in remote mode only.</p>												
OPTIONS	<table> <tr> <td>-u --user</td><td>The authorized domain application server administrative username.</td></tr> <tr> <td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr> <tr> <td>--passwordfile</td><td>           This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASEXPASSWORD, and so on.         </td></tr> <tr> <td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr> <tr> <td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr> <tr> <td>-s --secure</td><td>If set to true, uses SSL/TLS to communicate with the domain application server.</td></tr> </table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASEXPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	-s --secure	If set to true, uses SSL/TLS to communicate with the domain application server.
-u --user	The authorized domain application server administrative username.												
-w --password	The --password option is deprecated. Use --passwordfile instead.												
--passwordfile	This option replaces the --password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASEXPASSWORD, and so on.												
-H --host	The machine name where the domain application server is running. The default value is localhost.												
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.												
-s --secure	If set to true, uses SSL/TLS to communicate with the domain application server.												

## update-password-alias(1)

	-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.
	-h --help	Displays the help text for the command.
	--aliaspassword	This is a separate and distinct password corresponding to the original password. WARNING: Passing this password on the command line is not secure.  The password is optional and when omitted, the user is prompted.
<b>OPERANDS</b>	aliasname	This is the name of the password as it appears in domain.xml.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using update-password-alias asadmin> <b>update-password-alias --aliasname alias1</b>  Command update-password-alias executed successfully	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command
<b>SEE ALSO</b>	<a href="#">delete-password-alias(1)</a> , <a href="#">list-password-aliases(1)</a> , <a href="#">create-password-alias(1)</a>	

NAME	verifier – validates the J2EE Deployment Descriptors against application server DTDs																		
SYNOPSIS	<b>verifier</b> [ <i>optional_parameters</i> ] <i>jar_filename</i>																		
DESCRIPTION	<p>Use the <code>verifier</code> utility to validate the J2EE deployment descriptors and the Sun Java System 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.xml</i> and <i>jar_filename.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>																		
OPTIONS	<p>The optional parameters must be specified as follows:</p> <table> <tr> <td><code>-d   --destdir</code></td><td>Identifies the destination directory. The verifier results are located in this specified directory. The directory must already exist.</td></tr> <tr> <td><code>-h   --help-?</code></td><td>Displays the verifier help.</td></tr> <tr> <td><code>-u   --gui</code></td><td>Enables the Verifier graphical user interface.</td></tr> <tr> <td><code>-v   --verbose</code></td><td>Turns verbose debugging ON. Default mode is verbose turned off. In verbose mode, the status of each run of each test is displayed on the verifier console.</td></tr> <tr> <td><code>-V   --version</code></td><td>Displays the Verifier tool version.</td></tr> <tr> <td><code>-r   --reportlevellevel</code></td><td>Identifies the result reporting level. The default report level is to display all results. The available reporting levels include:</td></tr> <tr> <td><code>a   all</code></td><td>Set output reporting level to display all results (default).</td></tr> <tr> <td><code>f   failures</code></td><td>Set output reporting level to display only failure results.</td></tr> <tr> <td><code>w   warnings</code></td><td>Set output reporting level to display only warning and failure results.</td></tr> </table>	<code>-d   --destdir</code>	Identifies the destination directory. The verifier results are located in this specified directory. The directory must already exist.	<code>-h   --help-?</code>	Displays the verifier help.	<code>-u   --gui</code>	Enables the Verifier graphical user interface.	<code>-v   --verbose</code>	Turns verbose debugging ON. Default mode is verbose turned off. In verbose mode, the status of each run of each test is displayed on the verifier console.	<code>-V   --version</code>	Displays the Verifier tool version.	<code>-r   --reportlevellevel</code>	Identifies the result reporting level. The default report level is to display all results. The available reporting levels include:	<code>a   all</code>	Set output reporting level to display all results (default).	<code>f   failures</code>	Set output reporting level to display only failure results.	<code>w   warnings</code>	Set output reporting level to display only warning and failure results.
<code>-d   --destdir</code>	Identifies the destination directory. The verifier results are located in this specified directory. The directory must already exist.																		
<code>-h   --help-?</code>	Displays the verifier help.																		
<code>-u   --gui</code>	Enables the Verifier graphical user interface.																		
<code>-v   --verbose</code>	Turns verbose debugging ON. Default mode is verbose turned off. In verbose mode, the status of each run of each test is displayed on the verifier console.																		
<code>-V   --version</code>	Displays the Verifier tool version.																		
<code>-r   --reportlevellevel</code>	Identifies the result reporting level. The default report level is to display all results. The available reporting levels include:																		
<code>a   all</code>	Set output reporting level to display all results (default).																		
<code>f   failures</code>	Set output reporting level to display only failure results.																		
<code>w   warnings</code>	Set output reporting level to display only warning and failure results.																		

## verifier(1M)

<b>OPERANDS</b>	<p><i>jar_filename</i>      name of the ear/war/jar/rar file to perform static verification on. The results of verification are placed in two files <i>jar_filename.xml</i> and <i>jar_filename.txt</i> in the destination directory.</p> <p>-a   --app                      Runs only the application tests.</p> <p>--p   --appclient              Runs only the application client tests.</p> <p>-c   --connector                Runs only the connector tests.</p> <p>-e   --ejb                      Runs only the EJB tests.</p> <p>-w   --web                      Runs only the web tests.</p> <p>-s   --webservices              Runs only the web services tests.</p> <p>-l   --webservicesclient        Runs only the web services client tests.</p>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using verifier in the Verbose Mode</p> <p>The following example runs the verifier in verbose mode and writes all the results of static verification of the <i>sample.ear</i> file to the destination directory named <i>/verifier-results</i>.</p> <pre>example% verifier -v -rf -d /verifier-results sample.ear</pre> <p>Where <i>-v</i> runs the verifier in verbose mode, <i>-d</i> specifies the destination directory, and <i>-rf</i> displays only the failures. The results are stored in <i>/verifier-results/sample.ear.xml</i> and <i>/verifier-results/sample.ear.txt</i>.</p> <p><b>EXAMPLE 2</b> Using verifier to run Application and EJB tests</p> <pre>example% verifier --app --ejb sample.ear</pre>
<b>SEE ALSO</b>	<p><a href="#">asadmin(1M)</a></p>

<b>NAME</b>	verify-domain-xml – verifies the content of the domain.xml file	
<b>SYNOPSIS</b>	<b>verify-domain-xml</b> [--terse= <i>false</i> ] [--echo= <i>false</i> ] [--help] [--verbose= <i>false</i> ] [--domaindir <i>install_dir/domains</i> ] [ <i>domain_name</i> ]	
<b>DESCRIPTION</b>	Verifies the content of the domain.xml file.	
<b>OPTIONS</b>	-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.
	-h --help	Displays the help text for the command.
	--verbose	Turns on verbose debugging mode if true. The default is false.
	--domaindir	Specifies the directory where the domains are located. The path must be accessible in the file system. The default is the value of the \$AS_DEF_DOMAINS_PATH environment variable. This variable is defined in asenv.bat/conf. The default value of this variable is <i>install_dir/domains</i> .
<b>OPERANDS</b>	<i>domain_name</i>	Specifies the name of the domain. The default is domain1.
<b>EXAMPLES</b>	<b>EXAMPLE 1</b> Using verify-domain-xml <pre>asadmin&gt; verify-domain-xml --verbose=true domain1 Element: applications Error: J2eeApplication Module does not contains application name 'MEjbApp'       J2eeApplication Module does not contains application name '__ejb_container_timer_app'</pre>	
<b>EXIT STATUS</b>	0	command executed successfully
	1	error in executing the command

version(1)

NAME	version – displays the version information												
SYNOPSIS	<b>version</b> --user <i>admin_user</i> [--passwordfile <i>filename</i> ] [--host <i>host_name</i> ] [--port <i>port_number</i> ] [--secure -s] [--terse=false] [--echo=false] [--interactive=true] [--help] [--verbose=false]												
DESCRIPTION	<p>Use the <b>version</b> command to 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 the --terse option is entered on the command line.</p> <p>This command is supported in remote mode only.</p>												
OPTIONS	<table><tr><td>-u --user</td><td>The authorized domain application server administrative username.</td></tr><tr><td>-w --password</td><td>The --password option is deprecated. Use --passwordfile instead.</td></tr><tr><td>--passwordfile</td><td>This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD=<i>password</i>, where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASEXPASSWORD, and so on.</td></tr><tr><td>-H --host</td><td>The machine name where the domain application server is running. The default value is localhost.</td></tr><tr><td>-p --port</td><td>The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.</td></tr><tr><td>-s --secure</td><td>If set to true, uses SSL/TLS to communicate with the domain application server.</td></tr></table>	-u --user	The authorized domain application server administrative username.	-w --password	The --password option is deprecated. Use --passwordfile instead.	--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASEXPASSWORD, and so on.	-H --host	The machine name where the domain application server is running. The default value is localhost.	-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.	-s --secure	If set to true, uses SSL/TLS to communicate with the domain application server.
-u --user	The authorized domain application server administrative username.												
-w --password	The --password option is deprecated. Use --passwordfile instead.												
--passwordfile	This option replaces the -- password option. Using the --password option on the command line or through the environment is deprecated. The --passwordfile option specifies the name of a file containing the password entries in a specified format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in capital letters. For example, to specify the domain application server password, use an entry with the following format: AS_ADMIN_PASSWORD= <i>password</i> , where <i>password</i> is the actual administrator password. Other passwords that can be specified include AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASEXPASSWORD, and so on.												
-H --host	The machine name where the domain application server is running. The default value is localhost.												
-p --port	The port number of the domain application server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.												
-s --secure	If set to true, uses SSL/TLS to communicate with the domain application server.												

		version(1)
	-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.
	-h --help	Displays the help text for the command.
	--verbose	By default this flag is set to false. If set to true, the version information is displayed in detail.
EXAMPLES	<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 --passwordfile mysecret --host bluestar --port 4848 --verbose Java 2 Platform Enterprise Edition 1.4 Application Server (build A021930-126949)</pre>	
EXIT STATUS	0	command executed successfully
	1	error in executing the command
SEE ALSO	<a href="#">help(1)</a>	

## wscompile(1M)

NAME	wscompile – generates stubs, ties, serializers, and WSDL files used in JAX-RPC clients and services																											
SYNOPSIS	<b>wscompile</b> [ <i>options</i> ] <i>configuration_file</i>																											
DESCRIPTION	<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>																											
OPTIONS	<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: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 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>-mapping file</i></td><td>writes the mapping file to the specified file.</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: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 this option with the <i>-model</i> option in order to create a model file for use with the <i>wsdeploy</i> command.	<i>-mapping file</i>	writes the mapping file to the specified file.
<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: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 this option with the <i>-model</i> option in order to create a model file for use with the <i>wsdeploy</i> command.																											
<i>-mapping file</i>	writes the mapping file to the specified file.																											



<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>	directory for the non-class generated files are stored.
<code>-O</code>	optimizes the generated code.
<code>-s <i>directory</i></code>	directory for the generated source files.
<code>-source <i>version</i></code>	generate code for the specified JAX-RPC version. Supported versions are 1.0.1, 1.0.3, 1.1, 1.1.1, and 1.1.2 (the default).
<code>-verbose</code>	output messages about what the compiler is doing.
<code>-version</code>	prints version information.

Exactly one of the `-input`, `-define`, `-gen` options must be specified.

## SUPPORTED FEATURES

The `--f` option requires a comma-separated list of features. The following are the supported features.

<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 infix to use for generated serializers (Solaris).
<code>infix=<i>name</i></code>	specify an infix 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>rpclieteral</code>	use the RPC literal encoding.
<code>searchschema</code>	search schema aggressively for subtypes.
<code>serializeinterfaces</code>	turn on direct serialization of interface types.

wscompile(1M)

strict	generate code strictly compliant with JAX-RPC 1.1 specification.
unwrap	enable unwrapping of document/literal wrapper elements in WSI mode.
useonewayoperations	allow generation of one-way operations.
wsi	enable WS-I Basic Profile features, to be used for document/literal, and RPC/literal.
donotoverride	do not regenerate the classes
donotunwrap	disables unwrapping of document/literal wrapper elements in WS-I mode. This is on by default.

Note: the -gen options are not compatible with wsdeploy.

## CONFIGURATION FILE

The `wscompile` command reads the configuration file `config.xml` which contains information that describes the web service. The structure of the file is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration
xmlns="http://java.sun.com/xml/ns/jax-rpc/ri/config">
<service> or <wsdl> or <modelfile>
</configuration>
```

The configuration element may contain exactly one `<service>`, `<wsdl>` or `<modelfile>`.

## SERVICE ELEMENT

If the `<service>` element is specified, `wscompile` reads the RMI interface that describes the service and generates a WSDL file. In the `<interface>` subelement, the `name` attribute specifies the service's RMI interface, and the `servantName` attribute specifies the class that implements the interface. For example:

```
<service name="CollectionIF_Service"
targetNamespace="http://echoservice.org/wsdl"
typeNameSpace="http://echoservice.org/types"
packageName="stub_tie_generator_test">
<interface name="stub_tie_generator_test.CollectionIF"
servantName="stub_tie_generator_test.CollectionImpl"/>
</service>
```

<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 location="http://tempuri.org/sample.wsdl" packageName="org.tempuri.sample"/&gt;</pre>
<b>MODELFILE ELEMENT</b>	<p>This element is for advanced users.</p> <p>If <code>config.xml</code> contains a <code>&lt;service&gt;</code> or <code>&lt;wsdl&gt;</code> element, <code>wscompile</code> 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 <code>wscompile</code>. For example:</p> <pre>&lt;modelfile location="mymodel.xml.gz"/&gt;</pre>
<b>EXAMPLES</b>	<p><b>EXAMPLE 1</b> Using <code>wscompile</code> to generate client-side artifacts</p> <pre>wscompile -gen:client -d outputdir -classpath classpathdir config.xml</pre> <p>Where a client side artifact is generated in the <code>outputdir</code> for running the service as defined in the <code>config.xml</code> file.</p> <p><b>EXAMPLE 2</b> Using <code>wscompile</code> to generate server-side artifacts</p> <pre>wscompile -gen:server -d outputdir -classpath classpathdir -model modelfile.Z config.xml</pre> <p>Where a server side artifact is generated in the <code>outputdir</code> and the <code>modelfile</code> in <code>modelfile.Z</code> for services defined in the <code>config.xml</code> file.</p>
<b>SEE ALSO</b>	<a href="#">wsdeploy(1M)</a>

## wsdeploy(1M)

<b>NAME</b>	wsdeploy – reads a WAR file and the jaxrpc-ri.xml 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 wsdeploy 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. wsdeploy internally runs wscompile with the -gen:server option. The wscompile command generates classes and a WSDL file which wsdeploy includes in the generated WAR file.</p> <p>Generally, you don't have to run wsdeploy because the functions it performs are done automatically when you deploy a WAR with deploytool or asadmin.</p>
<b>OPTIONS</b>	<ul style="list-style-type: none"> <li>-classpath <i>path</i>      location of the input class files.</li> <li>-keep                    keep temporary files.</li> <li>-tmpdir <i>directory</i>    use the specified directory as a temporary directory</li> <li>-o <i>output WAR file</i>    required; location of the generated WAR file. This option is required.</li> <li>-source <i>version</i>       generates code for the specified JAX-RPC SI version. Supported version are: 1.0.1, 1.0.3, 1.1, 1.1.1, and 1.1.2 (the default).</li> <li>-verbose                outputs messages about what the compiler is doing.</li> <li>-version                prints version information.</li> </ul>
<b>INPUT WAR FILE</b>	<p>The input WAR file for wsdeploy 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: HelloIF is the service endpoint interface, and HelloImpl is the class that implements the interface. The web.xml 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; </pre>

```

<endpoint
  name="MyHello"
  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()`.

## wsdeploy(1M)

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`:

```
<handlerChains>
  <chain runAt="server"
    roles=
      "http://acme.org/auditing
      "http://acme.org/morphing"
    xmlns:ns1="http://foo/foo-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

---

## Numbers and Symbols

— list-resource-adapter-configs, 277

## b

brings down the administration server and associated instances — shutdown, 304

## d

displays the license information — display-license, 196

displays the status of the deployed component — show-component-status, 302

## g

generates stubs, ties, serializers, and WSDL files used in JAX-RPC clients and services — wscompile, 336

## i

installs the license file — install-license, 213

## r

reads a WAR file and the `jaxrpc-ri.xml` file and generates another WAR file that is ready for deployment — wsdeploy, 340  
enables the component — enable, 198

## s

sets the values of attributes — set, 300  
disables the component — disable, 194

## A

add-resources — creates the resources specified in an XML file specified, 12  
adds a connecton pool with the specified connection pool name — create-connector-connection-pool, 44  
adds a lifecycle module — create-lifecycle-module, 91  
adds a new access control list file for the named instance — create-acl, 36  
adds a new HTTP listener socket — create-http-listener, 59  
adds an audit-module — create-audit-module, 39  
adds the administered object with the specified JNDI name — create-admin-object, 37  
adds an IIOP listener — create-iiop-listener, 62  
creates a physical destination — create-jmsdest, 77

- creates the named virtual server —  
  create-virtual-server, 118
- adds the new authenticated realm —  
  create-auth-realm, 41
- allows you to execute multiple commands  
  while preserving environment settings and  
  remaining in the asadmin utility —  
  multimode, 291
- appclient — launches the Application Client  
  Container and invokes the client application  
  packaged in the application JAR file, 15
- asadmin — utility for performing  
  administrative tasks for the Sun Java System  
  Application Server, 17
- asadmin create-persistence-resource,  
  create-persistence-resource — registers a  
  persistence resource, 101
- asmigrate — automates migration of J2EE  
  applications from other J2EE platforms to  
  Sun Java System Application Server, 23
- automates migration of J2EE applications from  
  other J2EE platforms to Sun Java System  
  Application Server — asmigrate, 23

## B

- backup-domain — performs a backup on the  
  domain, 31
- browses and queries the JNDI tree —  
  list-jndi-entries, 265

## C

- capture-schema — stores the database metadata  
  (schema) in a file for use in mapping and  
  execution, 32
- change-master-password — changes the master  
  password, 34
- changes the master password —  
  change-master-password, 34
- checks to see if the JMS service is up and  
  running — jms-ping, 214
- create-acl — adds a new access control list file  
  for the named instance, 36
- create-admin-object — adds the administered  
  object with the specified JNDI name, 37

- create-audit-module — adds an  
  audit-module, 39
- create-auth-realm — adds the new  
  authenticated realm, 41
- create-connector-connection-pool — adds a  
  connecton pool with the specified connection  
  pool name, 44
- create-domain — creates a domain with the  
  given name, 54
- create-file-user — creates a new file user, 57
- create-http-listener — adds a new HTTP listener  
  socket, 59
- create-iiop-listener — adds an IIOP listener, 62
- create-instance — creates an instance, 64
- create-javamail-resource — creates a JavaMail  
  session resource, 68
- create-jdbc-resource — creates a JDBC resource  
  with the specified JNDI name, 75
- create-jms-resource — creates a JMS  
  resource, 80
- create-jmsdest — creates a physical  
  destination, 77
- create-lifecycle-module — adds a lifecycle  
  module, 91
- create-message-security-provider — Enables  
  administrators to create the  
  message-security-config and  
  provider-config sub-elements for the  
  security service in domain.xml, 94
- create-password-alias — creates a password  
  alias, 99
- create-profiler — creates the profiler  
  element, 104
- create-resource-adapter-config — creates the  
  configuration information in domain.xml  
  for the connector module, 106
- create-ssl — creates and configures the SSL  
  element in the selected HTTP listener, IIOP  
  listener, or IIOP service, 108
- create-system-properties — adds or updates one  
  or more system properties of the domain,  
  configuration, cluster, or server instance, 113
- list-system-properties — lists the system  
  properties of the domain, configuration,  
  cluster, or server instance, 281
- create-virtual-server — creates the named  
  virtual server, 118



- creates a domain with the given name —  
create-domain, 54
- creates a JDBC resource with the specified JNDI  
name — create-jdbc-resource, 75
- creates a new file user — create-file-user, 57
- creates a password alias —  
create-password-alias, 99
- creates an instance — create-instance, 64
- creates and configures the SSL element in the  
selected HTTP listener, IIOP listener, or IIOP  
service — create-ssl, 108
- creates or modifies a security map for the  
specified connector connection pool —  
create-connector-security-map, 49
- creates or modifies a security map for the  
specified connector connection pool —  
update-connector-security-map, 324
- creates the configuration information in  
domain.xml for the connector module —  
create-resource-adapter-config, 106
- creates the profiler element —  
create-profiler, 104

## D

- delete-acl — removes the access control list file  
for the named instance, 122
- delete-auth-realm — removes the named  
authentication realm, 127
- delete-connector-connection-pool — removes  
the specified connector connection pool, 129
- delete-connector-security-map — deletes a  
security map for the specified connector  
connection pool, 133
- delete-domain — deletes the given  
domain, 137
- delete-file-user — removes the named file  
user, 138
- delete-http-listener — removes an HTTP  
listener, 140
- delete-iiop-listener — removes an IIOP  
listener, 142
- delete-instance — deletes the instance that is  
not running, 144
- delete-javamail-resource — removes a JavaMail  
session resource, 146

- delete-jms-resource — removes a JMS  
resource, 154
- delete-jmsdest — removes a physical  
destination, 152
- delete-jvm-options — removes JVM options  
from the Java configuration or profiler  
elements of the domain.xml file, 158
- delete-lifecycle-module — removes the lifecycle  
module, 160
- delete-message-security-provider — enables  
administrators to delete a  
provider-config sub-element for the  
given message layer  
(message-security-config element of  
domain.xml), 162
- delete-password-alias — deletes a password  
alias, 165
- delete-profiler — deletes the profiler  
element, 169
- delete-resource-adapter-config — deletes the  
configuration information created in  
domain.xml for the connector module, 171
- delete-ssl — deletes the SSL element in the  
selected HTTP listener, IIOP listener, or IIOP  
service, 173
- delete-system-property — removes one system  
property of the domain, configuration,  
cluster, or server instance, at a time, 176
- delete-virtual-server — removes a virtual  
server, 181
- delete-admin-object — removes the  
administered object with the specified JNDI  
name, 123
- deletes a password alias —  
delete-password-alias, 165
- deletes a security map for the specified  
connector connection pool —  
delete-connector-security-map, 133
- deletes the configuration information created in  
domain.xml for the connector module —  
delete-resource-adapter-config, 171
- deletes the given domain —  
delete-domain, 137
- deletes the instance that is not running. —  
delete-instance, 144
- deletes the profiler element —  
delete-profiler, 169

- deletes the SSL element in the selected HTTP listener, IIOP listener, or IIOP service — `delete-ssl`, 173
- removes a virtual server — `delete-virtual-server`, 181
- deploy — deploys the specified component, 183
- deploydir — deploys an exploded format of application archive, 189
- deploys an exploded format of application archive — `deploydir`, 189
- deploys the specified component — `deploy`, 183
- removes a physical destination — `delete-jmsdest`, 152
- disable — disables the component, 194
- display-license — displays the license information, 196
- displays the version information — `version`, 334

## E

- enable — enables the component, 198
- Enables administrators to create the `message-security-config` and `provider-config` sub-elements for the security service in `domain.xml`. — `create-message-security-provider`, 94
- enables administrators to delete a `provider-config` sub-element for the given message layer (`message-security-config` element of `domain.xml`) — `delete-message-security-provider`, 162
- export — marks a variable name for automatic export to the environment of subsequent commands in multimode, 200

## G

- get — gets the values of the monitorable or configurable attributes, 203
- get-client-stubs — gets the stubs of the client, 205

- gets all audit modules and displays them — `list-audit-modules`, 227
- gets all custom resources — `list-custom-resources`, 242
- gets all JDBC resources — `list-jdbc-resources`, 259
- gets all the administered objects — `list-admin-objects`, 223
- lists the existing JavaMail session resources — `list-javamail-resources`, 255
- lists the JMS resources — `list-jms-resources`, 263
- lists the existing JMS physical destinations — `list-jmsdest`, 261
- gets connector connection pools that have been created — `list-connector-connection-pools`, 235
- gets the access control lists for the named instance — `list-acls`, 222
- lists the existing HTTP listeners — `list-http-listeners`, 249
- lists the existing IIOP listeners — `list-iiop-listeners`, 251
- gets the stubs of the client — `get-client-stubs`, 205
- gets the values of the monitorable or configurable attributes — `get`, 203
- lists the existing virtual servers — `list-virtual-servers`, 289

## I

- install-license — installs the license file, 213

## J

- jms-ping — checks to see if the JMS service is up and running, 214
- jspc — precompiles JSP source files into servlets, 216

## L

- launches the Application Client Container and invokes the client application packaged in the application JAR file. — `appclient`, 15
- list — lists the configurable elements, 219
- list-acls — gets the access control lists for the named instance, 222
- list-applications-refs — lists all application references in a cluster or unclustered server instance, 225
- list-audit-modules — gets all audit modules and displays them, 227
- list-auth-realms — lists the authentication realms, 229
- list-backups — lists all backups and restores, 231
- list-components — lists deployed components, 232
- list-connector-connection-pools — gets connector connection pools that have been created, 235
- list-connector-security-maps — lists the security maps belonging to the specified connector connection pool, 239
- list-custom-resources — gets all custom resources, 242
- list-domains — lists the domains in the specified domain directory, 244
- list-file-groups — lists the file groups, 245
- list-http-listeners — lists the existing HTTP listeners, 249
- list-iiop-listeners — lists the existing IIOP listeners, 251
- list-instances — lists all the instances along with their status, 253
- list-javamail-resources — lists the existing JavaMail session resources, 255
- list-jdbc-connection-pools — lists all JDBC connection pools, 257
- list-jdbc-resources — gets all JDBC resources, 259
- list-jms-resources — lists the JMS resources, 263
- list-jmsdest — lists the existing JMS physical destinations, 261
- list-jndi-entries — browses and queries the JNDI tree, 265
- list-lifecycle-modules — lists the lifecycle modules, 269
- list-password-aliases — lists all password aliases, 273
- list-resource-adapter-configs —, 277
- list-sub-components — lists EJBs or Servlets in deployed module or module of deployed application, 279
- list-timers — lists all of the timers owned by server instance(s), 285
- list-transaction-id — lists the transactions IDs, 287
- list-virtual-servers — lists the existing virtual servers, 289
- list-admin-objects — gets all the administered objects, 223
- lists all application references in a cluster or unclustered server instance —
  - list-applications-refs, 225
- lists all backups and restores —
  - list-backups, 231
- lists all JDBC connection pools —
  - list-jdbc-connection-pools, 257
- lists all of the timers owned by server instance(s) —
  - list-timers, 285
- lists all password aliases —
  - list-password-aliases, 273
- lists all the instances along with their status —
  - list-instances, 253
- lists deployed components —
  - list-components, 232
- lists EJBs or Servlets in deployed module or module of deployed application —
  - list-sub-components, 279
- lists the authentication realms —
  - list-auth-realms, 229
- lists the configurable elements —
  - list, 219
- lists the domains in the specified domain directory —
  - list-domains, 244
- lists the file groups —
  - list-file-groups, 245
- lists the lifecycle modules —
  - list-lifecycle-modules, 269
- lists the security maps belonging to the specified connector connection pool —
  - list-connector-security-maps, 239
- lists the transactions IDs —
  - list-transaction-id, 287

## M

manually recovers pending transactions —  
    recover transactions, 295  
marks a variable name for automatic export to  
    the environment of subsequent commands in  
    multimode — export, 200  
multimode — allows you to execute multiple  
    commands while preserving environment  
    settings and remaining in the asadmin  
    utility, 291

## P

package-appclient — packs the application  
    client container libraries and jar files, 292  
packs the application client container libraries  
    and jar files — package-appclient, 292  
performs a backup on the domain —  
    backup-domain, 31  
ping-connection-pools — tests that a connection  
    pool is usable, 293  
precompiles JSP source files into servlets —  
    jspc, 216

## R

recover transactions — manually recovers  
    pending transactions, 295  
registers a persistence resource — asadmin  
    create-persistence-resource,  
    create-persistence-resource, 101  
creates a JavaMail session resource —  
    create-javamail-resource, 68  
creates a JMS resource —  
    create-jms-resource, 80  
registers the resource in the XML file specified  
    — add-resources, 12  
removes a component from the domain  
    application server — undeploy, 318  
removes JVM options from the Java  
    configuration or profiler elements of the  
    domain.xml file — delete-jvm-options, 158  
removes one or more variables from the  
    multimode environment — unset, 323

removes one system property of the domain,  
    configuration, cluster, or server instance, at a  
    time — delete-system-property, 176  
removes the access control list file for the  
    named instance — delete-acl, 122  
removes the administered object with the  
    specified JNDI name —  
    delete-admin-object, 123  
removes an HTTP listener —  
    delete-http-listener, 140  
removes an IIOP listener —  
    delete-iiop-listener, 142  
removes a JavaMail session resource—  
    delete-javamail-resource, 146  
removes a JMS resource —  
    delete-jms-resource, 154  
removes the lifecycle module —  
    delete-lifecycle-module, 160  
removes the named authentication realm —  
    delete-auth-realm, 127  
removes the named file user —  
    delete-file-user, 138  
removes the specified connector connection  
    pool —  
    delete-connector-connection-pool, 129  
restore-domain — restores files from  
    backup, 297  
restores files from backup —  
    restore-domain, 297

## S

set — sets the values of attributes, 300  
show-component-status — displays the status  
    of the deployed component, 302  
shutdown — brings down the administration  
    server and associated instances, 304  
start-appserv — starts the domains in the  
    specified domains directory, 305  
start-domain — starts a domain, 307  
start-instance — starts a server instance, 310  
starts a domain — start-domain, 307  
starts a server instance — start-instance, 310  
starts the domains in the specified domains  
    directory — start-appserv, 305  
stop-appserv — stops the domains in the  
    specified domains directory, 312

- stop-instance — stops a server instance, 316
- stops a server instance — stop-instance, 316
- stops the domains in the specified domains directory — stop-appserv, 312
- stores the database metadata (schema) in a file for use in mapping and execution — capture-schema, 32

## T

- create-connector-resource — registers the connector resource with the specified JNDI name, 47
- create-connector-security-map, 49
- create-jdbc-connection-pool — registers the JDBC connection pool, 71
- create-jndi-resource — registers a JNDI resource, 86
- create-jvm-options — creates the JVM options from the Java configuration or profiler elements, 89
- delete-connector-resource — removes the connector resource with the specified JNDI name, 131
- delete-custom-resource — removes a custom resource, 135
- delete-jdbc-connection-pool — removes the specified JDBC connection pool, 148
- delete-jdbc-resource — removes a JDBC resource, 150
- delete-jndi-resource — removes a JNDI resource, 156
- list-connector-resources — gets all connector resources, 237
- list-file-users — creates a list of file users, 247
- list-jndi-resources — lists all existing JNDI resources, 267
- template — template for documenting manpages for the Sun Java System Application Server, 20, 27, 52, 167, 275, 333
- creates a list of file users — list-file-users, 247
- creates the JVM options from the Java configuration or profiler elements — create-jvm-options, 89
- gets all connector resources — templatelist-connector-resources, 237

- lists all existing JNDI resources— list-jndi-resources, 267
- registers a JNDI resource— create-jndi-resource, 86
- registers the connector resource with the specified JNDI name — create-connector—resource, 47
- registers the JDBC connection pool — create-jdbc-connection-pool, 71
- removes a custom resource — delete-custom-resource, 135
- removes a JDBC resource— delete-jdbc-resource, 150
- removes a JNDI resource— delete-jndi-resource, 156
- removes the connector resource with the specified JNDI name — delete-connector—resource, 131
- removes the specified JDBC connection pool —delete-jdbc-connection-pool, 148
- template for documenting manpages for the Sun Java System Application Server — template, 20, 27, 52, 167, 275, 333
- tests that a connection pool is usable — ping-connection-pools, 293

## U

- undeploy — removes a component from the domain application server, 318
- unset — removes one or more variables from the multimode environment, 323
- update-connector-security-map — creates or modifies a security map for the specified connector connection pool, 324
- update-file-user — updates a current file user as specified, 327
- update-password-alias — updates a password alias, 329
- updates a current file user as specified — update-file-user, 327
- updates a password alias — update-password-alias, 329
- utility for performing administrative tasks for the Sun Java System Application Server — asadmin, 17

## **V**

- validates the J2EE Deployment Descriptors against application server DTDs —
  - verifier, 331
- verifier — validates the J2EE Deployment Descriptors against application server DTDs, 331
- version — displays the version information, 334

## **W**

- wscompile — generates stubs, ties, serializers, and WSDL files used in JAX-RPC clients and services, 336
- wsdeploy — reads a WAR file and the `jaxrpc-ri.xml` file and generates another WAR file that is ready for deployment, 340