Sun Java System Application Server Enterprise Edition 8.2 Reference Manual

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

Part No: 819–4736
February 2007

070222@16599

Contents

Preface

Both novice users and those familar 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 and hadbm utility commands.
- Section 1M describes all the other Application Server utility commands.

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

NAME	This section gives the names of the commands or functions documented, followed by a brief description of what they do.
SYNOPSIS	This section shows the syntax of commands or functions. The following special characters are used in this section: [ ] Brackets. The option or argument enclosed in these brackets is optional. If the brackets are omitted, the argument must be specified. | Separator. Only one of the arguments separated by this character can be specified at a time.
DESCRIPTION	This section defines the functionality and behavior of the service. Thus it describes concisely what the command does. It does not discuss OPTIONS or cite EXAMPLES. Interactive commands, subcommands, requests, macros, and functions are described under USAGE.

OPTIONS	This secton 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 `example%`, or if the user must be superuser, `example#`. 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.

REFERENCE

User Commands

Name add-resources – creates the resources specified in an XML file

Synopsis

```
add-resources —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] xml_file_path
```

Description The `add-resources` command creates the resources named in the specified XML file. The *xml_file_path* is the path to the XML file containing the resources to be created. The `DOCTYPE` should be specified as *install_dir*`/lib/dtds/sun-resources_1_0.dtd` in the `resources.xml` file.

This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—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 ■ `server`, which creates the resources for the default server instance `server` and is the default value ■ `domain`, which creates the resources for the domain ■ *cluster_name*, which creates the resources for every server instance in the cluster ■ *instance_name*, which creates the resources for a particular server instance

Operands	*xml_file_path*	The path to the XML file containing the resource(s) to be created.
		
		An example XML file follows. Replace `<install_dir>` with the location of your Application Server installation.
		
		`<?xml version="1.0" encoding="UTF-8"?>`
		`<!DOCTYPE resources PUBLIC`
		`"-//Sun Microsystems Inc.//DTD Application Server 8.0 Domain//EN"`
		`"*<install_dir>/lib/dtds/sun-resources_1_0.dtd*">`
		
		`<resources>`
		`<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">`
		`<property name="URL"`
		`value="jdbc:oracle:thin:@iasperfsol12:1521:specdb"/>`
		`<property name="User" value="spec"/>`

```
 <property name="Password" value="spec"/>
 <property name="MaxStatements" value="200"/>
 <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

```
appclient —client client_application_jar
     [—mainclass client_application_main_classname|— name display_name]
     [—xml sun-acc.xml file] [—textauth] [—user username] [—password password]
```

Description 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.

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.

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.

Options

`—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

EXAMPLE 1 Using the `appclient` command

```
appclient -client appserv/bin/myclientapp.jar
-mainclass com.sun.test.TestAppClient -xml sun-acc.xml scott sample
```

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

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

```
asadmin subcommand[-short_option[short_option_argument]]*
      [--long_option[long_option_argument]]* [operand]*
```

Description 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.

The *subcommand* 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.

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.

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:

`-u --user`	authorized domain application server administrative username.
`-w --password`	password to administer the domain application server. The —`password` option is deprecated. Use —`passwordfile` instead.
—`passwordfile`	The file containing the domain application server password in the following form: AS_ADMIN_PASSWORD=*password*. Where *password* is the actual administrator password.
`-H --host`	machine name where the domain application server is running.
`-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.
`-s --secure`	if true, uses SSL/TLS to communicate with the domain application server.

`-t --terse`	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
`-e --echo`	setting to true will echo the command line statement on the standard output. Default is false.
`-I --interactive`	if set to true (default), only the required password options are prompted.
–h —`help`	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 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.

When using the command line interface, you need to understand the usage of the escape character. There are three reasons why the escape character is used:

1. UNIX meta characters: The UNIX meta characters are characters which have special meaning in a shell. These characters include: `\/,.!$%^&*|{}[]"'‘~;` To disable these meta characters, the escape character (backslash "\") is used. For example:

   `echo *` will echo all the files in the current directory.`echo \*` will echo the "*" character.

2. Java escape sequence: The escape character in Java is used as an escape sequence to represent certain special character values like `\n` for new line, `\b` for backspace, `\t` for tab and `\"` for double quote. An extra escape character is needed to represent the literal `\` character.

3. Command-line interface delimiters: The Application Server command-line interface uses "`:`" as a delimiter for options. If the character "`:`" is used as part of the property or `jvm_options`, not as a delimeter, then the escape character is required so that the "`:`" character is treated as a literal not as a delimeter. For example:

   The command `create-jvm-options` accepts operands in the following format:

   ```
   (jvm_option_name[=jvm_option_value])[:jvm_option_name[=jvm_option_name]]*
   ```

   More than one `jvm-option` can be created by using the "`:`" delimiter. To disable the "`:`" delimiter and use it as a literal "`:`" in either `jvm_option_name` or `jvm_option_value`, the escape character is needed.

Since the escape character is used to disable the delimiter in the command-line interface, and the escape character is a special character in UNIX and in Java, you must apply an escape character to every escape character in the command line. This applies to commands executed on UNIX OS and multimode, not to Windows OS.

Additionally, instead of using the escape character, you can use the quote character". Since quote is a special character in Java you must add an escape character. This does not apply to multimode.

Examples

EXAMPLE 1 Using an asadmin command option containing an escape character

UNIX OS in singlemode and multimode:

```
asadmin create-jdbc-connection-pool -u admin --passwordfile mypasswordfile
--datasourceclassname --description Test\\Escape\\Character sampleJDBCConnectionPool
```

Where the description option is `Test\Escape\Character`

Windows in singlemode:

```
asadmin create-jdbc-connection-pool -u --passwordfile mypasswordfile
--datasourceclassname sampleClassName --description Test\Escape\Character
sampleJDBCConnectionPool
```

In this case, an excape character is needed to disable the escape character in UNIX OS and in multimode. The escape character is not required for Windows.

EXAMPLE 2 Using an asadmin command property option containing an escape character to disable the delimiter

The name and value pairs for property option are:

```
user=dbuserpasswordfile=dbpasswordfileDatabaseName=jdbc:derbyserver=http://localhost:9092
```

UNIX OS singlemode and multimode:

```
asadmin create-jdbc-connection-pool --user --passwordfile mypasswordfile
--port 4848 --host localhost --datasourceclassname com.derby.jdbc.jdbcDataSource --property
user=dbuser:passwordfile=dbpasswordfile:DatabaseName=jdbc\\:derby:server=http\\://
localhost sqe-jdbc-pool
```

Windows singlemode:

```
asadmin create-jdbc-connection-pool --user admin --passwordfile mypasswordfile
--port 4848 --host localhost --datasourceclassname com.derby.jdbc.jdbcDataSource --property
user-dbuser:passwordfile-dbpasswordfile:databaseName=jdbc\:derby:server=
http\://localhost\:sqe-jdbc-pool
```

EXAMPLE 3 Using an asadmin command with an operand containing an escape character to disable the delimiter

UNIX OS in singlemode and multimode:

```
asadmin create-jvm-options --target test-server -e -Dlocation=c\\:\\\\sun\\\\appserver
```

Windows singlemode:

```
asadmin create-jvm-options --target test-server -e -Dlocation=c\:\\sun\\appserver
```

In this case, four escape characters are required (\\\\) to use the literal value of "\". The first escape is to escape the UNIX meta character. The second escape is to escape the Java escape sequence. The third escape character is to escape the UNIX meta character. And lastly, the fourth escape character is the literal value.

EXAMPLE 4 Using an asadmin command with an option containing an escape character

UNIX OS in singlemode and multimode:

```
asadmin list-jdbc-resources --user \"admin\\admin\" --passwordfile mypasswordfile
--host localhost --port 4848
```

Windows in singlemode and multimode:

```
asadmin list-jdbc-resources --user \"admin\admin\" --passwordfile mypasswordfile
--host localhost --port 4848
```

EXAMPLE 4 Using an asadmin command with an option containing an escape character *(Continued)*

In this case, the quote does not help much since an escape character is required to each escape character in UNIX.

EXAMPLE 5 Using an asadmin command with a property option containing an escape character

The name and value pairs for property option are:

```
user=dbuserpasswordfile=dbpasswordfileDatabaseName=jdbc:derbyserver=http://localhost:9092
```

UNIX OS and Windows singlemode:

```
asadmin create-jdbc-connection-pool --user --passwordfile mypasswordfile
--port 4848 --host localhost --datasourceclassname com.derby.jdbc.jdbcDataSource --property
user=dbuser:passwordfile=dbpasswordfile:DatabaseName=\"jdbc:derby\":server=\
"http://localhost sqe-jdbc-pool
```

Notice that in this case, the escape character is not required before the literal " : " since there are quotes around the value.

Attributes

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Interface Stability	Unstable

See Also

appclient(1M), package-appclient(1M)

Name asant – launches the Jakarta Ant tool

Synopsis **`asant`** *target_list*

Description Use the `asant` command to automate repetitive development and deployment tasks. `asant` is a shell script that invokes the underlying Ant infrastructure after initializing the environment to pick up the application server installed targets.

To use Ant as part of the Sun Java System Application Server, verify that your PATH includes the provided `asant` (UNIX) or `ant.bat`(Windows) script.

The bundled sample applications use `asant` extensively; however, `asant` can be used in any development or operational environments.

The build targets are represented in the `build.xml` files that accompany the sample applications.

To use the Ant tool to compile and reassemble the sample applications, verify that the `$AS_INSTALL/bin` directory is on your environment's path. On UNIX, add the `$AS_INSTALL/bin` directory to your PATH environment variable. On Windows, after installing the Sun ONE Application Server, set the system path by adding `$AS_INSTALL\bin` 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.

The *target_list* is one or more space separated tasks as described below.

Targets

`compile`	compiles all Java source code.
`jar`	assembles the EJB JAR module.
`war`	assembles the WAR file in *sample_dir*`/assemble/war`
`ear`	assembles the EAR file in *sample_dir*`/assemble/ear`
`core`	(default) compiles all sources, builds stubs and skeletons; and assembles EJB JAR, WAR and EAR files. This is the default target for all `build.xml` files shipped in the Sun ONE Application Server.
`javadocs`	creates Java docs in *sample_dir*`/javadocs`
`all`	builds core and javadocs , verifies and deploys the application, and adds the resources..
`deploy`	deploys the application and automatically expands the EJB JAR; does not install Javadocs.
`undeploy`	removes the deployed sample from the Sun Java System Application Server.
`clean`	removes *appname*`/build/` and *appname*`/assemble/` and *appname*`/javadocs` directories.

`verify`	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).

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

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

Description Use the `asmigrate` utility to analyze your J2EE application and translate vendor specific settings to Sun JavaTM System Application Server specific settings that makes the application deployable on Sun's J2EE products. You can download the Migration Tool from the following URL:

http://java.sun.com/j2ee/tools/migration/index.html

The following table identifies the supported J2EE product migrations:

Source J2EE Platform	Destination J2EE Platform
WebLogic Application Server 5.1, 6.0, 6.1, 8.1 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	Sun JavaTM System Application Server Enterprise Edition 8.2

Options

`-h --help`	displays the arguments for launching the MigrationTool.
`-v --version`	displays the version of the MigrationTool.
`-u --ui`	invokes the tool in user interface mode.
`-c --commandline`	invokes the tool in command-line mode.

`-q --quiet`	launches the tool in quiet mode.
`-d --debug`	launches the tool in debug mode.
`-s --sourcedirectory`	identifes the directory where the source code to migrate or scan is present.
`-S --sourceserver`	identifes the source application server of the applications to be migrated. Possible servers include the following: ■ wl51: WebLogic Application Server 5.1 ■ wl60: WebLogic Application Server 6.0 ■ wl61: WebLogic Application Server 6.1 ■ wl81: WebLogic Application Server 8.1 ■ as65: Sun ONE Application Server 6.5 ■ as70: Sun ONE Application Server 7.0 ■ ws40: WebSphere Application Server 4.0 ■ ws50: WebSphere Application Server 5.x ■ ri13: JavaTM 2 Platform Enterprise Edition 1.3 ■ ri14: JavaTM 2 Platform Enterprise Edition 1.3 ■ s1ws: Sun ONE Web Server ■ jb30: JBoss Application Server 3.0 ■ tc41: Tomcat Application Server 4.1
`-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 Appplication 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: ■ create-tables: if set to true (default), creates tables at deploy. If set to false tables are not created. ■ drop-tables: if set to true (default), tables are dropped at undeploy. If set to false tables are not dropped. ■ 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.

`-m --migrate-cmp`	migrates 1.1 compliant CMPs, if any, to 2.0. Option arguments are: ■ overwrite-conflicting-accessors: if set to true (default), conflicting accessors are overwritten. If set to false, conflicting accessors are not overwritten. ■ 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.
`-f --file-filter`	selects the type of files to migrate. Option arguments are: ■ all-files: if specified and set to true (default), migrates all types of files. ■ html-files: if specified and set to true (default), migrates HTML files. ■ java-files: if specified and set to true (default), migrates Java files. ■ jsp-files: if specified and set to true (default), migrates JSP type files. ■ xml-files: if specified and set to true(default), migrates all XML type files. ■ archive-files: if specified and set to true (default), migrates `jar/ear/war/rar` file types.
`-a --append-logs`	if specified, appends the logging to the existing or previous logs without overwriting them. If not specified, previous logs are overwritten.
operands	identifes the archive file (jar/ear/war/rar) to be migrated.

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.

EXAMPLE 1 Using asmigrate *(Continued)*

```
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

```
asupgrade [—console ] [—version ] [—help ]
     [—source applicationserver_7.x/8.x_installation]
     [—target applicationserver_8.1_installation] —adminuser admin_user
     [—adminpassword admin_password] [—masterpassword changeit]
     [—passwordfile path_to_password_file] [—domain domain_name]
     [—nsspwdfile NSS_password_filepath]
     [—targetnsspwdfile target_NSS_password_filepath]
     [—jkspwdfile JKS_password_filepath] [—capwdfile CA_password_filepath]
     [—clinstancefile file1 [, file2, file3, ... filen]]
```

Description Use the `asupgrade` utility to upgrade the server configuration and its persisted state, J2EE services, and deployed J2EE applications. The configuration of your earlier version of Application Server 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.

You can use the tool through the command-line interface (CLI) or the GUI. To use the Upgrade tool in GUI mode, issue the asupgrade command with no options. To run the Upgrade tool in CLI mode, invoke the asupgrade command with the `-—c/—console` option. You can run the upgrade CLI in the interactive or non-interactive mode. If you supply all required arguments when invoking asupgrade on the console, the upgrade is performed in non-interactive mode and no further input is required.

`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.

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.

The upgrade process can also be initiated automatically at installation time using the Upgrade check box in the Application Server installer. After completion of the upgrade, use the uninstaller to remove the previous version of the application server.

Application archives (EAR files) and component archives (JAR, WAR, and RAR files) that are deployed in the Application Server 7.x/8.x environment do not require any modification to run on Application Server 8.2 EE. 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 `asmigrate` command, then redeployed manually.

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 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

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

–e —-targetnsspwdfile	The path to the target NSS password file.
–j —-jkspwdfile	The path to the JKS password file.
–p —-capwdfile	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 8.2 with Prompts for Certificate Migration

This example shows how to upgrade (side-by-side) a Sun Java System Application Server 7 installation to Sun Java System Application Server 8.2 Enterprise Edition. 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/sjsas8.2/domains
```

Note – For information of the upgrade scenarios (side-by-side, in-place) see Chapter 2 in the Sun Java System Enterprise Edition 8.2 Upgrade and Migration guide.

EXAMPLE 2 Upgrading an Application Server 7.1 EE Installation with Clusters and NSS Certificates to Application Server 8.2 EE

This example shows how to upgrade (side-by-side) a Sun Java System Application Server 7.1 EE installation with a cluster to Sun Java System Application Server 8.2 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/sjsas8.2/domains
--domain domain1 --nsspwdfile /home/sjsas7.1/nsspassword.txt
--targetnsspwdfile /home/sjsas8.2/nsspassword.txt
--clinstancefiles /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 8.1 EE Installation with clusters and NSS Certificates to Application Server 8.2 EE

This example shows how to upgrade (in-place) a Sun Java System Application Server 8.1 EE installation to Sun Java System Application Server 8.1 PE. JKS and CA certificates will be migrated.

```
example% asupgrade --adminuser admin
--passwordfile password.txt
```

EXAMPLE 3 Upgrading an Application Server 8.1 EE Installation with clusters and NSS Certificates to Application Server 8.2 EE *(Continued)*

```
--source /home/sjsas8.1/domains --target /home/sjsas8.2/domains
--domain domain1 --nsspwdfile /home/sjsas8.1/nsspassword.txt
--targetnsspwdfile /home/sjsas8.2/nsspassword.txt
--clinstancefiles /home/sjsas8.1/config/clinstance.conf
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also asmigrate(1M)

Name backup-domain – performs a backup on the domain

Synopsis

```
backup-domain [—domaindir domain_directory] [—description description]
     [—terse=false] [—verbose=false] [domain_name]
```

Description The `backup-domain` command backs up files under the named domain. This 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

domain_name	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.

Examples **EXAMPLE 1** Using backup-domain

```
asadmin>backup-domain --domaindir /opt/SUNWappserver/nondefaultdomaindir domain1
Successfully backed up the domain

Description: 1137030607263
Backup Filename: /opt/SUNWappserver/nondefaultdomaindir/domain1/backups/sjsas_backup_v00001.z
Date and time backup was performed: Wed Jan 11 17:50:07 PST 2006
Domains Directory: /opt/SUNWappserver/nondefaultdomaindir
Domain Directory: /opt/SUNWappserver/nondefaultdomaindir/domain1
Domain Name: domain1
Name of the user that performed the backup: jondoe
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `restore-domain(1)`, `list-backups(1)`

Name capture-schema – stores the database metadata (schema) in a file for use in mapping and execution

Synopsis

```
capture-schema –username name –password password –dburl url
    –driver jdbc_driver_classname [–schemaname schemaname] [–table tablename]
    –out filename
```

Description Stores the database metadata (schema) in a file.

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).

When running `capture-schema` against an Oracle database, you should grant the database user running the `capture-schema` command the `ANALYZE ANY TABLE` privilege.

You can also use the Sun Java System Studio IDE to capture the database schema.

Options

`-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`	name of the user schema being captured. If not specified, the default will capture metadata for all tables from all the schemas accessible to this user. *Specifying this parameter is highly recommended.* 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. The specified schema name must be uppercase.
`-table`	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. The specified table name or names are case sensitive. Be sure to match the case of the previously created table names.
`-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

EXAMPLE 1 Using capture-schema

```
capture-schema -username cantiflas -password enigma
 -dburl jdbc:oracle:thin:@sadbuttrue:1521:ora817 -driver oracle.jdbc.driver.OracleDriver
 -schemaname CANTIFLAS -out cantiflas.dbschema
```

See Also

asadmin(1M)

Name change-master-password – changes the master password

Synopsis

```
change-master-password [—domaindir domain_path | —agentdir node-agent_path]
    [—savemasterpassword=false] [domain_name | node_agent_name]
```

Description 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.

Options

`—domaindir`	This option specifies the directory used for this operation. By default, the domaindir is $AS_DEF_DOMAINS_PATH, which is an environment variable defined in asenv.bat/conf. Both the domaindir and the agentdir options should not be passed together; use one or the other.
`—agentdir`	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 domaindir and the agentdir options should not be passed together; use one or the other. This option is supported in Enterprise Edition only.
`—savemasterpassword`	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.

Operands

domain_name	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.
node-agent_name	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)`

Name clear-ha-store – deletes tables in HADB

Synopsis

```
clear-ha-store —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—haagentport port_number]
    [—haadminpassword password] [—haadminpasswordfilefilename]
    [—hostshadb_host_list] [—storeuser username] [—storepassword password]
    [—dbsystempassword dbpassword] database_name
```

Description This command deletes tables in HADB. You must have created an entry in the HA database before you execute this command, using `configure-ha-cluster` or `create-ha-store`. Use fully qualified hostnames when specifying the hostlist interfaces explicitly for hosts with multiple network interfaces. `clear-ha-store` was named `delete-session-store` in the Sun Java System Application Server 7.1. `delete-session-store` has been deprecated.

This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.

`–s ––secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
`––help`	Displays the help text for the command.
`––haagentport`	The name of the HA agent port. If not specified, the default port number is 1862.
`––haadminpassword`	The actual HADBM administation password. Using this option with the `hadbm createdomain` or `hadbm create` command requires that the password is entered each time any `hadbm` command is used. The `haadminpassword` is different from the `hadbm dbpassword` command. You must use both passwords when using the following commands: `hadbm create`, `hadbm addnodes`, `hadbm refragment`.
`––haadminpasswordfile`	The file containing the HADBM administration password, storepassword, and dbsystempassword. These passwords must be defined in the following form: HADBM_ADMINPASSWORD=*password*, HADBM_DBPASSWORD=*storepassword*, HADBM_SYSTEMPASSWORD=*dbsystempassword*. Where *password* is the actual administrator password.
`––hosts`	A comma-separated list of all the hosts that are part of the Management Agent.
`––storeuser`	This option specifies the username associated with the administrative instance.
`––storepassword`	The domain application server password associated with the administrative instance.
`––dbsystempassword`	The database password associated with the administrative instance.

Operands

database_name	The name of the HA database.

Examples

EXAMPLE 1 Using clear-ha-store

```
asadmin> clear-ha-store --user admin --passwordfile password.txt
hadatabase1
The clear-ha-store command executed successfully
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also

`create-ha-store(1)`

Name configure-ha-cluster – configures an existing cluster to be High Availability

Synopsis

```
configure-ha-cluster —host localhost [—port 4849] [—user user]
    [—passwordfile passwordfile_name] [—terse=false] [—echo=false]
    [—interactive=true] [—secure=false] [—devicesize devicesize ]
    [—haagentport port_number] [—haadminpasswordfile.file_name]
    [—packagepath.hadb-root_on_remote_machine] [—hosts hadb-host-list]
    [—property (name=value)[:name-value]*] {clusterName}
```

Description The `configure-ha-cluster` command performs the following tasks:

- Verifies that the cluster exists.
- Verifies that the cluster is standalone (an example of this is, that the cluster doesn't share its configuration with any other cluster).
- Checks if a database with the same name as the cluster already exists. If so, an error is logged and the command performs the next task.
- Creates an HA database with the same name as the cluster.
- Creates the correct tables in the database.
- Creates and/or modifies the appropriate resources in domain.xml.

This command is supported in remote mode only.

Options

`–H—host`	This option specifies the machine where the domain application server is located. The default 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 4949.
`–u—user`	This option specifies the user name associated with the administrative instance.
`–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=*password*. Where *password* 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 options are prompted.
`–s ––secure`	If set to true, uses SSL/TLS to communicate with the domain administration server.
`––devicesize`	This is the device size in MegaBytes (MB). The valid range is between 208MB and 8+ gigabytes (GB).
`––haagentport`	This is the number of the HA agent port. The default is 1862.
`––haadminpasswordfile`	The file containing the high-availability password associated with the administrative instance. The password is defined in the following form: HADBM_ADMINPASSWORD=*password*, HADBM_DBPASSWORD=*password*, HADBM_SYSTEMPASSWORD=*password*. Where *password* is the actual HA administrator password for the domain.
`––packagepath`	A fresh installation of the high-availability does not have a domain nor its packagepath registered. This can cause problems when you wish to use HADB on a remote machine in certain cases. If the remote machine's HADB root directory does not have exactly the same directory structure as the client machine's, then the registration of the remote machine will fail. There are 3 ways to handle this situation: 1. Register the packagepath and domain manually on the remote machine with hadbm. 2. Run the following commands locally on the remote machine to bootstrap it: ▪ `create-cluster` c1 ▪ `configure-ha-cluster ––devicesize 208 ––hosts` *hostname,hostname* c1 ▪ `remove-ha-cluster` c1 ▪ `delete-cluster` c1 After these steps the remote machine's HADB will be configured properly forever. 3. Use the––`packagepath` option. to identify the HADB-root path on the remote machine. This is the path you would use if you were logged on to the remote machine.

	—hosts	This is a list of comma separated host names where the HADB instance is configured. The number of hosts must be greater than 1 and must be an even number. The same host names can be repeated. Use fully qualified hostnames when specifying the hostlist interfaces explicitly for hosts with multiple network interfaces.
	—property	This is a list of property name/value pairs, which are separated by a colon. To explicitly specify a portbase number for HADBM nodes, use the —property portbase=*base_number* option.
Operands	*clusterName*	This is the name of the cluster that will be changed to high availability.

Examples **EXAMPLE 1** Using the configure-ha-cluster command

This is a basic example of how the cammand is used.

```
asadmin>configure-ha-cluster --user admin --passwordfile passwordfile
--hosts red.iplanet.com.host1,red.iplanet.com.host2 cluster1
The command configuration-ha-cluster has executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also remove-ha-cluster(1)

Name configure-ha-persistence – enables configuration of parameters related to session persistence

Synopsis

```
configure-ha-persistence —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—type persistencetype]
    [—frequency frequency—scope scope—store jdbc_resource_jndi_name]
    [—property (name=value)[:name=value]*] clustername
```

Description Configure the global session persistence settings to balance your needs for performance, reliability, and high availability. You can override these settings for specific applications by changing the properties of the `manager-properties`, `store-properties`, and `session-properties` subelements of the `session-manager` element in the `sun-web.xml` file.

The `configure-ha-persistence` command is available only in the Enterprise Edition of the Sun Java System Application Server.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—help	Displays the help text for the command.
—type	Set the persistence type to specify where session data is stored. The persistence types available are: ■ `memory` If session persistence for the application server instance is disabled, this is the default persistence type. The memory persistence type provides no session persistence in a clustered environment. The memory persistence type is intended for development environments and should not be used for production. ■ `file` This type provides no session persistence in a clustered environment. Use file persistence type to store session data in a file. If the instance becomes unavailable and restarts, it can recover the session information that was last written to the file. The file persistence type is meant for development environments and should not be used for production. ■ `ha` If session persistence for the application server instance is enabled, this is the default persistence type. This type allows you to store session data in the HADB. The ha persistence type enables failover of ses sion information between application server instances in a cluster. The session information for each application server instance in a clus ter is stored in the HADB. The session information is available to all other instances in the cluster. If an instance in a cluster becomes unavailable, another instance in the cluster can continue to serve the sessions that the now unavailable instance was serving.
—frequency	Set the persistence frequency to define the frequency at which the session state is stored in the HADB. The persistence frequencies available are:

- `web-method` The session is stored after every web request just before a response is sent back to the client. Use this frequency when you need very high availability of updated session states. This is the default.
- `time-based` The session is stored at the time interval defined in the `reapIntervalSeconds` property. A better throughput is achieved because the session is stored after a configurable time interval instead of after every web request.

`—scope`

Set the persistence scope to determine how much of the session is stored. The persistence scopes available are:

- `modified-session` The entire session is stored only if it has been modified since the last time it was stored.
- `session` The entire session is stored every time session information is saved to the HADB. This is the default.
- `modified-attribute` Only the modified attributes of the session are stored. Using this mode can improve the throughput and response time significantly for applications in which only a small portion of the session state is modified for any given request.

If you use the `modified-attribute` persistence scope, your application should follow these guidelines:

- Call `setAttribute()` every time you modify the session state.
- Make sure there are no cross-references between attributes. The object graph under each distinct attribute key is serialized and stored separately. If there are any object cross references between the objects under each separate key, they are not serialized and deserialized correctly.
- Ideally, the session state should be stored in multiple attributes, or at least in a read-only attribute and a modifiable attribute.

`—store`

Specify the JNDI name of the JDBC resource for the HADB. The default is `jdbc/hastore`.

`—property`

Specify other session persistence properties.

Operands *clustername*

Specify the name of the cluster for which you are configuring session persistence.

Examples

EXAMPLE 1 Using configure-ha-persistence

```
asadmin> configure-ha-persistence --user admin --passwordfile secret.txt
 --type ha --frequency web-method --scope modified-session --store jdbc/hastore
cluster1
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also

`configure-ha-cluster(1)`, `remove-ha-cluster(1)`, `create-ha-store(1)`, `clear-ha-store(1)`

Name copy-config – copies an existing configuration to create a new configuration

Synopsis

```
copy-config —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help]
    [—systemproperties (name=value)[:name=value]*] source_configuration_name
    destination_configuration_name
```

Description Use the copy-config command to create a new configuration in the `domain.xml` file by copying an existing configuration. The new configuration is identical to the copied configuration, except for any properties you specify in the —`systemproperties` option.

The configuration `default-config` is the configuration that is copied when a standalone sever instance or standalone cluster is created.

Options

—u —`user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
—H —`host`	The machine name where the domain administration server is running. The default value is localhost.
—p —`port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
—s —`secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—help	Displays the help text for the command.
—systemproperties	Optional attribute name/value pairs for configuring the resource. The following properties are available:

System Property	Definition
HTTP_LISTENER_PORT	This property specifies the port number for http-listener-1. Valid values are 1- On UNIX, creating sockets that listen on ports 1–1024 requires superuser priv
HTTP_SSL_LISTENER_PORT	This property specifies the port number for http-listener-2. Valid values are 1- On UNIX, creating sockets that listen on ports 1–1024 requires superuser priv
IIOP_LISTENER_PORT	This property specifies which ORB listener port for IIOP connections orb-list listens on.
IIOP_SSL_LISTENER_PORT	This property specifies which ORB listener port for IIOP connections the IIO listener called SSL listens on.
IIOP_SSL_MUTUALAUTH_PORT	This property specifies which ORB listener port for IIOP connections the IIO listener called SSL_MUTUALAUTH listens on.
JMX_SYSTEM_CONNECTOR_PORT	This property specifies the port number on which the JMX connector listens. values are 1–65535. On UNIX, creating sockets that listen on ports 1–1024 rec superuser privileges.

Operands

source_configuration_name	The name of the configuration you are copying.
destination_configuration_name	The name of the new configuration you are creating by copying the source configuration. This name should be unique within a domain.xml. It should not be the same as the cluster name, serverinstance name, another config name, or node agent name.

Examples

EXAMPLE 1 Using the copy-config command

```
asadmin> copy-config --user admin --passwordfile passwords.txt
--systemproperties HTTP_LISTENER_PORT=2000:HTTP_SSL_LISTENER_PORT=3000
default-config new-config
```

EXAMPLE 1 Using the copy-config command *(Continued)*

```
Command copy-config executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `list-configs(1)`, `delete-config(1)`

Name create-acl – adds a new access control list file for the named instance

Synopsis

```
create-acl --user admin_user[--password admin_password][--host localhost]
     [--port 4848][--passwordfile filename][--secure|-s][--instance
     instance_name] --aclfile filename acl_ID
```

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.
`--aclfile`	name of the default acl file.

Operands

acl_ID	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 **EXAMPLE 1** Using create-acl

```
asadmin> create-acl --user admin --password adminadmin --host fuyako --port 7070 --instance s
Created ACL with id=sampleACL
```

Where: `sampleACL` is the name of the ACL created.

Examples

0	command executed successfully
1	error in executing the command

Interface Equivalent Access Control List page

See Also `delete-acl(1)`, `list-acl(1)`

Name create-admin-object – adds the administered object with the specified JNDI name

Synopsis

```
create-admin-object —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target]
    —restype admin_object_type —raname resource_adapter_name [—description text]
    [—property name=value[:name=value]*] jndi_name
```

Description This commands creates the administered object that has a specified jndi name.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
––help	Displays the help text for the command.
––target	Specifies the target on which you are creating the administered object.This option is available only in the Sun Java System Application Server Standard and Enterprise Edition. Valid values are ■ `server`, which creates the administered object for the default server instance `server` and is the default value ■ *configuration_name*, which creates the administered object for the named configuration ■ *cluster_name*, which creates the administered object for every server instance in the cluster ■ *instance_name*, which creates the administered object for a particular server instance
––restype	This option is used to administer the object resource types, as defined by the resource adapter in the ra.xml file.
––raname	This is the name of the resource adapter associated with this object.
––description	This option is the text description of the administered object.
––property	This option describes the "name/values" pairs for configuring the resource.

Operands

jndi_name	This is the JNDI name of the administered object to be created.

Examples

EXAMPLE 1 Using create-admin-object

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

```
asadmin> create-admin-object --user admin1 --passwordfile passwords.txt
--restype javax.jms.Queue --raname jmsra --description "sample administered object"
--property Name=sample_jmsqueue --target instance1 jms/samplequeue
Command create-admin-object executed successfully
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `delete-admin-object(1)`, `list-admin-objects(1)`

Name create-application-ref – creates a reference to an application

Synopsis

```
create-application-ref —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] [—enabled=true]
    [—virtualservers virtual_servers] reference_name
```

Description The `create-application-ref` command creates a reference from a cluster or an unclustered server instance to a previously deployed application element (for example, a J2EE application, a Web module, or an enterprise bean module). This effectively results in the application element being deployed and made available on the targeted instance or cluster.

The target instance or instances making up the cluster need not be running or available for this command to succeed. If one or more instances are not available, they will receive the new application element the next time they start.

This command is supported in remote mode only.

Options

`—u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`—H —host`	The machine name where the domain administration server is running. The default value is localhost.
`—p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.

	`–s` `––secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
	`––target`	Specifies the target for which you are creating the application reference. Valid values are ■ `server`, which creates the application reference for the default server instance `server` and is the default value ■ *cluster_name*, which creates the application reference for every server instance in the cluster ■ *instance_name*, which creates the application reference for the named unclustered server instance
	`––enabled`	Indicates whether the application should be enabled (that is, loaded). This value will take effect only if the application is enabled at the global level. The default is `true`.
	`––virtualservers`	Comma-separated list of virtual server IDs on which to deploy. This option applies only to Web modules (either standalone or in a J2EE application). If this option is not specified, the application is deployed to all virtual servers except the administrative server, `__asadmin`.
Operands	*reference_name*	The name of the application or module, which can be a J2EE application, Web module, EJB module, connector module, application client module, or lifecycle module.

Examples **EXAMPLE 1** Using the create-application-ref command

The following command creates a reference to the Web module `MyWebApp` on the unclustered server instance `NewServer`.

```
asadmin> create-application-ref --user admin2
--passwordfile passwords.txt --target NewServer MyWebApp
Command create-application-ref executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `delete-application-ref(1)`, `list-application-refs(1)`

Name create-audit-module – adds an audit-module

Synopsis

```
create-audit-module —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target_name]
    [—classname classname] [—property(name=value)[:name=value]*]
    audit_module_name
```

Description Adds the named audit module for the plugin module that implements the audit capabilities. This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—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 ■ `server`, which creates the audit module for the default server instance `server` and is the default value ■ *configuration_name*, which creates the audit module for the named configuration ■ *cluster_name*, which creates the audit module for every server instance in the cluster ■ *instance_name*, which creates the audit module for a particular server instance
	-—classname	Java class which implements this realm.
	-—property	optional attributes name/value pairs of provider implementation specific attributes.
Operands	*audit_module_name*	name of this audit module.

Examples EXAMPLE 1 Using create-audit-module

```
asadmin> create-audit-module --user admin1 --passwordfile password.txt
--host pigeon --port 5001 --classname com.sun.appserv.auditmodule
--property defaultuser=admin:Password=admin sampleAuditModule
Command create-audit-module executed successfully
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `delete-audit-module(1)`, `list-audit-modules(1)`

Name create-auth-realm – adds the new authentication realm

Synopsis

```
create-auth-realm —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target_name]
    [—classname realm_class] [—isdefault-=true]
    [—property(name=value)[:name=value]*] auth_realm_name
```

Description Adds the named authentication realm. This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	––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: ■ `server`, which creates the realm for the default server instance `server` and is the default value ■ *configuration_name*, which creates the realm for the named configuration ■ *cluster_name*, which creates the realm for every server instance in the cluster ■ *instance_name*, which creates the realm for a particular server instance
	––classname	Java class which implements this realm.
	––property	optional attributes name/value pairs of provider implementation specific attributes.
Operands	*auth_realm_name*	name of this realm.

Examples **EXAMPLE 1** Using create-auth-realm

```
asadmin> 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
```

Where `db` is the auth realm created.

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `delete-auth-realm(1)`, `list-auth-realms(1)`

Name create-cluster – creates a cluster

Synopsis

```
create-cluster —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—config config_name]
    [—systemproperties (name=value)[:name=value]*] cluster_name
```

Description The `create-cluster` command creates a new cluster. When created, a cluster must reference a configuration (or, as with an unclustered server instance, a configuration can be implicitly created). Initially the cluster has no server instances, applications, or resources.

If you do not use the —`config` option, the command creates a standalone cluster with a configuration named *cluster_name*`-config`. If you use the —`config` option to reference an existing configuration used by other clusters or server instances, the command creates a shared cluster.

To add new instances to the cluster, use the `create-instance` command with the —`cluster` option. Use the `stop-instance` and `delete-instance` commands to delete server instances from the cluster at any time.

To associate new applications and resources with the cluster regardless of the number of instances in the cluster, perform any of the following operations:

- Use the `deploy` command with the option —`target` *cluster_name*.
- Use resource-creation commands (for example, `create-jdbc-resource`) with the option —`target` *cluster_name*.
- Use reference management commands (for example, `create-application-ref` or `create-resource-ref`) if the application is already deployed or the resource is already created.

This command is supported in remote mode only.

Options

–u —`user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H ––host`	The machine name where the domain administration server is running. The default value is localhost.
`–p ––port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s ––secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
`––help`	Displays the help text for the command.
`––config`	Creates a shared cluster. The specified configuration name must exist and must not be `default-config` (the standalone cluster configuration template) or a standalone configuration (including `server-config`). If this option is omitted, a standalone cluster is created.
`––systemproperties`	Defines system properties for the configuration created for by the cluster. These properties override the property values in the `default-config` configuration. The following properties are available:

Property	Definition
HTTP_LISTENER_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_SSL_LISTENER_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.
IIOP_LISTENER_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 *cluster_name* A unique identifier for the cluster to be created.

Examples **EXAMPLE 1** Using the create-cluster command

The following command creates a cluster named `MyCluster`, overriding the default configuration's SSL port value. Because the —`config` option is not specified, the command makes a copy of the `default-config` and names it `MyCluster-config`.

```
asadmin> create-cluster --user admin1
--passwordfile passwords.txt --systemproperties
IIOP_SSL_LISTENER_PORT=1169 MyCluster
```

EXAMPLE 1 Using the create-cluster command *(Continued)*

```
Command create-cluster executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `delete-cluster(1)`, `list-clusters(1)`, `start-cluster(1)`, `stop-cluster(1)`, `create-instance(1)`

Name create-connection—group – creates a new connection group with the named group ID

Synopsis

```
create-connection-group
      --user user_name --password password --host hostname --port admin_port_number
      --instance instance_name --httplistener http_listener_ID --address address
      --defaultvs virtual_server --servername server_name connection_group_ID
```

Description Creates a new connection group with the named group ID.

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.

`--httplistener` a unique identifier for the HTTP listener.

`--address` the IP address of the listen socket. Can be in dotted-pair or IPv6 notation.

`--defaultvs` the ID attribute of the default virtual server for this particular connection group.

`--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.

connection_group_ID a unique identifier for the connection group.

Examples

```
asadmin% create-connection-group
```

Interface Equivalent unknown

See Also `delete-connection-group(1)`, `list-connection-groups(1)`

Name create-connector-connection-pool – adds a connection pool with the specified connection pool name

Synopsis

```
create-connector-connection-pool —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [--steadypoolsize 8] [--maxpoolsize 32]
    [--maxwait 60000] [--poolresize 2] [--idletimeout 300]
    [--failconnection=false] --raname resource_adapter_name
    --connectiondefinition connection_definition_name
    [--transactionsupport transaction_support] [--description text]
    [—property (name=value)[:name=value]*] connector_connection_pool_name
```

Description The `create-connector-connection-pool` adds a new connector connection pool with the specified connection pool name. This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—help	Displays the help text for the command.
—target	The target option is deprecated.
—raname	The name of the resource adapter.
—connectiondefinition	The name of the connection definition.
—steadypoolsize	The minimum and initial number of connections maintained in the pool. The default value is 8.
—maxpoolsize	The maximum number of connections that can be created to satisfy client requests. The default value is 32.
—maxwaittime	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.
—poolresize	The quantity by which the pool will scale up or scale down the number of connections. When the pool has no free connections, it will scale up by this quantity. When the pool scales down, all the invalid and idle connections are removed, sometimes resulting in removing connections of quantity greater than this value. Steadypoolsize will be ensured. Possible values are from 0 to MAX_INTEGER. The default value is 2.
—idletimeout	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.
—failconnection	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.

—transactionsupport	Indicates the level of transaction support that this pool will have. Possible values are `XATransaction`, `LocalTransaction` and `NoTransaction`. This attribute can have a value lower than or equal to but not higher than the resource adapter's transaction support attribute. The resource adapter's transaction support attribute has an order of values, where XATransaction is the highest, and NoTransaction the lowest.
—description	Text providing descriptive details about the connector connection pool.
—property	optional attribute name/value pairs for configuring the resource.

Operands

connector_connection_pool_name	The name of the connection pool to be created.

Examples

EXAMPLE 1 Using the create-connector-connection-pool command

```
asadmin> create-connector-connection-pool
--passwordfile passwords.txt --steadypoolsize 20
--maxpoolsize 100 --poolresize 2 --maxwait 60000 --raname jmsra
--connectiondefinition javax.jms.QueueConnectionFactory jms/qConnPool
Command create-connector-connection-pool executed successfully
```

Where jms/qConnPool is the name of the new connector connection pool.

Exit Status

0	command executed successfully
1	error in executing the command

See Also `delete-connector-connection-pool(1)`, `list-connector-connection-pools(1)`

Name create-connector-resource – registers the connector resource with the specified JNDI name

Synopsis

```
create-connector-resource —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [---target target]
    --poolname connectorConnectionPoolName [—enabled=true]
    [--description text] jndi_name
```

Description This command registers the connector resource with the JNDI name, which is specified by the *jndi_name* operand.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
	—target	valid in Enterprise Edition only, specifies the ending location of the connector resources. Valid values are "server," "domain," cluster, instance. The default is server.
	—poolname	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.
	—enabled	This option determines whether the resource is enabled at runtime. The default value is true.
	—description	Text providing descriptive details about the connector resource.
Operands	*jndi_name*	the JNDI name of this connector resource.

Examples **EXAMPLE 1** Using the create-connector-resource command

```
asadmin> create-connector-resource --target server --poolname jms/qConnPool
--description "creating sample connector resource" jms/qConnFactory
Command create-connector-resource executed successfully
```

Where jms/qConnFactory is the sample connector resource that is created.

Exit Status	0	command executed successfully
	1	error in executing the command

See Also delete-connector-resource(1), list-connector-resources(1)

Name create-connector-security-map – creates a security map for the specified connector connection pool

Synopsis

```
create-connector-security-map —user admin_user [—passwordfile filename]
[—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
[—interactive=true] [—help] —poolname connector_connection_pool_name
[—principals principal_name1[, principal_name2]* | —usergroups user_group1[, user_group
—mappedusername username {security_map_name}
```

Description Use this command to create 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.

For this command to succeed, you must have first created a connector connection pool using the `create-connector-connection-pool` command.

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.

This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.

–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—help	Displays the help text for the command.
—target	This option is deprecated in this release.
—poolname	Specifies the name of the connector connection pool to which the security map belongs.
—principals	Specifies a list of backend EIS principals. More than one principal can be specified using a comma separated list. Use either the —principals or —usergroups options, but not both.
—usergroups	Specifies a list of backend EIS user group. More than one usergroups can be specified using a comma separated list.
—mappedusername	Specifies the EIS username.

Operands

security_map_name	name of the security map to be created.

Examples

EXAMPLE 1 Using `create-connector-security-map`

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

```
asadmin> create-connector-security-map --user admin
--passwordfile pwd_file.txt --poolname connector-pool1 --principals principal1, principal2 --
Command create-connector-security-map executed successfully
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `delete-connector-security-map(1)`, `list-connector-security-maps(1)`, `update-connector-security-map(1)`

Name create-custom-resource – creates a custom resource

Synopsis

```
create-custom-resource —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] —target target —restype type
    —factoryclassname classname [--enabled=true] —description text
    [-—property (name=value)[:name=value]*] jndi_name
```

Description The `create-custom-resource` command creates a custom resource. A custom resource specifies a custom server-wide resource object factory that implements the `javax.naming.spi.ObjectFactory` interface. This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—help	Displays the help text for the command.
—target	In Enterprise Edition, this option specifies the target to which you are deploying. Valid values are ■ server, which deploys the component to the default server instance server and is the default value ■ domain, which deploys the component to the domain. ■ *cluster_name*, which deploys the component to every server instance in the cluster. ■ *instance_name*, which deploys the component to a particular sever instance.
—resourcetype	The —resourcetype option is deprecated. Use —restype instead.
—restype	The type of custom resource to be created.
—factoryclass	The class that creates the custom resource.
—enabled	Determines whether the custom resource is enable at runtime. The default value is true.
—description	Text providing descriptive details about the custom resource.
—property	optional attribute name/value pairs for configuring the resource.

Operands

jndi_name	the JNDI name of this resource.

Examples

EXAMPLE 1 Using the create-custom-resource command

```
asadmin> create-custom-resource --user admin --passwordfile passwords.txt --restype topic --factory
Command create-custom-resource executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `delete-custom-resource(1)`, `list-custom-resources(1)`

Name create-domain – creates a domain with the specified name

Synopsis

```
create-domain [—domaindir install_dir/domains] [—template domain_template]
    —adminport port_number —adminuser admin_user
    [—passwordfile passwordfile] [—terse=false] [—echo=false]
    [—interactive=true] [—instanceport port_number]
    [—domainproperties (name=value)[:name=value]*]
    [—savemasterpassword=false] domain_name
```

Description 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.

This command is supported in local mode only.

Options

—`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 *install_dir*`/domains` directory.
—`template`	Specifies the filename of a `domain.xml` template used to create the domain. Allows domains of different types to be created and allows users to define their templates. This option is available only in the Sun Java System Application Server Enterprise Edition.
—`adminport`	The administrative instance port number.
—`adminuser`	The username associated with the administrative instance.
—`passwordfile`	The file containing the domain application server password associated with the administrative instance. The password is defined in the following form: AS_ADMIN_ADMIN_PASSWORD=*password*. Where *password* is the actual administrator password for the domain. This file can also contain the AS_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.

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

`––instanceport` The port number listening to the HTTP request. The port number cannot be currently in use. If not specified, the default value is 8080.

`––domainproperties` 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.

Property	Definition
domain.jmxPort	Specifies the port on which the jmx connector is initialized. The valid values are 1-65535.

—savemasterpassword — 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 `start-domain` command. For security purposes, the default setting should be false, because saving the masterpassword on the disk is an insecure practice, 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

The following command creates the `myDomain` domain and saves the admin username and password.

```
asadmin>  create-domain --adminport 8282 --adminuser admin myDomain
Please enter the admin password>
Please enter the admin password again>
Please enter the master password>
Please enter the master password again>
Default port 8080 for HTTP Instance is in use. Using 40718
Default port 7676 for JMS is in use. Using 40719
Default port 3700 for IIOP is in use. Using 40720
Default port 8181 for HTTP_SSL is in use. Using 40721
Default port 3820 for IIOP_SSL is in use. Using 40722
Default port 3920 for IIOP_MUTUALAUTH is in use. Using 40723
Default port 8686 for JMX_ADMIN is in use. Using 40724
Domain myDomain created.
```

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

```
create-file-user —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target]
    [—authrealmname auth_realm_name] [—groups user_groups[:user_groups]*]
    user_name
```

Description 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 *auth_realm_name* is not specified, an entry is created in the default keyfile. If *auth_realm_name* is specified, an entry is created in the keyfile using the `auth-realm` name.

This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—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.

Operands

user_name	This is the name of file user to be created.

Examples

EXAMPLE 1 Using the create-file-user command

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

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

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

Exit Status

0	command executed successfully
1	error in executing the command

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

Name create-ha-store – creates tables in the HADB that are used by HA the cluster

Synopsis

```
create-ha-store —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—haagentport port_number]
    [—haadminpassword password] [—haadminpasswordfilefilename]
    [—hostshadb_host_list] [—storeuser username] [—storepassword password]
    [—dbsystempassword dbpassword] database_name
```

Description This command creates tables in the HADB used by the HA cluster. You only need to use this command if you have previously used `clear-ha-store`. The `configure-ha-store`command also creates tables in the HADB. Use fully qualified hostnames when specifying the hostlist interfaces explicitly for hosts with multiple network interfaces. `create-ha-store` was named `create-session-store` in the Sun Java System Application Server 7.1. `Create-session-store` has been deprecated.

This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.

	`–s` `––secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
	`––haagentport`	The name of the HA agent port. If not specified, the default port number is 1862.
	`––haadminpassword`	The actual HADBM administation password. Using this option with the `hadbm createdomain` or `hadbm create` command requires that the password is entered each time any `hadbm` command is used. The `haadminpassword` is different from the `hadbm dbpassword` command. You must use both passwords when using the following commands: `hadbm create`, `hadbm addnodes`, `hadbm refragment`.
	`––haadminpasswordfile`	The file containing the HADBM administration password, storepassword, and dbsystempassword. These passwords must be defined in the following form: HADBM_ADMINPASSWORD=*password*, HADBM_DBPASSWORD=*storepassword*, HADBM_SYSTEMPASSWORD=*dbsystempassword*. Where *password* is the actual administrator password.
	`––hosts`	A comma-separated list of all the hosts that are part of the Management Agent.
	`––storeuser`	This option specifies the username associated with the administrative instance.
	`––storepassword`	The domain application server password associated with the administrative instance.
	`––dbsystempassword`	The database password associated with the administrative instance.
Operands	*database_name*	The name of the HA database.

Examples

EXAMPLE 1 Using create-ha-store

```
asadmin> create-ha-store --user admin --passwordfile passwords.txt
--haagentport 1860 hadatabase1
The create-ha-store command executed successfully
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also

`clear-ha-store(1)`, `configure-ha-cluster(1)`

Name create-http-health-checker – creates a health-checker for a specified load balancer configuration

Synopsis

```
create-http-health-checker —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—url "/"] [—interval 30] [—timeout 10]
    [—config config_name] target
```

Description This command creates a health checker for a specified load balancer configuration. It only works with the native load balancer provided with the Sun Java System Application Server. It does not work with other load balancers.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
––help	Displays the help text for the command.
––url	The URL to ping to determine whether the instance is healthy.
––interval	The interval in seconds the health checker waits between checks of an unhealthy instance to see whether it has become healthy. The default value is 30 seconds. A value of 0 disables the health checker.
––timeout	The interval in seconds the health checker waits to receive a response from an instance. If the health checker has not received a response in this interval, the instance is considered unhealthy.
––config	The load balancer configuration for which you create the health-checker.

Operands *target*

Specifies the target to which the health checker applies.

Valid values are:

- *cluster_name*, which specifies the health checker will monitor all instances in the cluster.
- *instance_name*, which specifies that the health checker will monitor this standalone instance.

Examples **EXAMPLE 1** Using the create-http-health-checker command

```
asadmin> create-http-health-checker --user admin
--passwordfile password.txt --config mycluster-http-lb-config mycluster
Command create-http-health-checker executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `delete-http-health-checker(1)`

Name create—http—lb—config – creates a configuration for the load balancer

Synopsis

```
create-http-lb-config —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—responsetimeout 60] [—httpsrouting=false]
    [—reloadinterval 60] [—monitor=false] [—routecookie=true]
    —target target | config_name
```

Description Use the create-http-lb-config command to create a load balancer configuration. This configuration applies to load balancing in the HTTP path.

You must specify either a target or a configuration name, or both. If you don't specify a target, the configuration is created and assigned the default instance `sever` as the target. If you don't specify a configuration name, a name is created based on the target name. If you specify both, the configuration is created with the specified name, referencing the specified target.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
	—responsetimeout	The time in seconds within which a server instance must return a response. If no response is received within the time period, the server is considered unhealthy. If set to a positive number, and the request is idempotent, the request is retried. If the request is not idempotent, an error page is returned. If set to 0 no timeout is used.The default is 60.
	—httpsrouting	If set to `true`, HTTPS requests to the load balancer result in HTTPS requests to the server instance. If set to `false`, HTTPS requests to the load balancer result in HTTP requests to the server instance. The default is `false`.
	—reloadinterval	The interval between checks for changes to the load balancer configuration file `loadbalancer.xml`. When the check detects changes, the configuration file is reloaded. A value of `0` disables reloading.
	—monitor	Specifies whether monitoring is enabled. The default is `false`.
	—routecookie	Specifies whether a route cookie is enabled.
	-—target	Specifies the target to which the load balancer configuration applies. If you don't specify a target, the load balancer configuration is created without a target. You can specify targets later using the command `create-http-lb-ref`. Valid values are: ■ *cluster_name*, which specifies that requests for this cluster will be handled by the load balancer. ■ *instance_name*, which specifies that requests for this standalone instance will be handled by the load balancer.
Operands	*config_name*	The name of the new load balancer configuration. This name must not conflict with any other load balancer groups,

agents, configurations, clusters, or sever instances in the domain. If you don't specify a name, the load balancer configuration name is based on the target name, *target_name*`-http-lb-config`.

Examples **EXAMPLE 1** Using the create-http-lb-config command

```
asadmin> create-http-lb-config --user admin --passwordfile file --target mycluster
mylbconfigname
Command create-http-lb-config executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `delete-http-lb-config(1)`, `list-http-lb-configs(1)`

Name create-http-lb-ref – adds an existing cluster or server instance to an existing load balancer configuration

Synopsis

```
create-http-lb-ref —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] —config config_name target
```

Description Use the create-http-lb-ref command to add an existing cluster or server instance to an existing load balancer configuration. The load balancer forwards the requests to the clustered and standalone instances it references.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
	`––config`	Specifies which load balancer configuration to add clusters and server instances to.
Operands	*target*	Specifies which cluster or instance to add to the load balancer. Valid values are: ■ *cluster_name*, which specifies that requests for this cluster will be handled by the load balancer. ■ *instance_name*, which specifies that requests for this standalone instance will be handled by the load balancer.

Examples **EXAMPLE 1** Using the create-http-lb-ref command

```
asadmin>  create-http-lb-ref --user admin --passwordfile file
--config mycluster-http-lb-config cluster2
Command create-http-lb-ref executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `delete-http-lb-ref(1)`, `list-http-lb-configs(1)`

Name create-http-listener – adds a new HTTP listener socket

Synopsis

```
create-http-listener —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target server] —listeneraddress address
    —listenerport listener_port —defaultvs virtual_server
    —servername server_name [—acceptorthreads 1] [—securityenabled=false]
    [—redirectport redirect_port] [—xpowered=true] [—enabled=true] listener_id
```

Description The `create-http-listener` command creates an HTTP listener. This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
`––help`	Displays the help text for the command.
`––target`	In Enterprise Edition, specifies the target for which you are creating the HTTP listener. Valid values are ■ `server`, which creates the listener for the default server instance `server` and is the default value ■ *configuration_name*, which creates the listener for the named configuration ■ *cluster_name*, which creates the listener for every server instance in the cluster ■ *instance_name*, which creates the listener for a particular server instance
`––listeneraddress`	The IP address of the listener address (resolvable by DNS).
`––listenerport`	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.
`––defaultvs`	The ID attribute of the default virtual server for this listener.
`––servername`	Tells the server what to put in the host name section of any URLs it sends to the client. This affects URLs the server automatically generates; it doesn't affect the URLs for directories and files stored in the server. This name should be the alias name if your server uses an alias. If a colon and port number are appended, that port will be used in URLs that the server sends to the client.
`––acceptorthreads`	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.
`––securityenabled`	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.

	—redirectport	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.
	—xpowered	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.
	—enabled	If set to true, the listener is enabled at runtime.
Operands	*listener_id*	The listener ID of the HTTP listener.

Examples **EXAMPLE 1** Using the create-http-listener command

The following command creates an HTTP listener named `sampleListener` that uses a nondefault number of acceptor threads and is not enabled at runtime:

```
asadmin> 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
Command create-http-listener executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `delete-http-listener(1)`, `list-http-listeners(1)`, `create-virtual-server(1)`, `create-ssl(1)`

Name create-iiop-listener – adds an IIOP listener

Synopsis

```
create-iiop-listener —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target server] —listeneraddress address
    [—iiopport 1072] [—securityenabled=false] [—enabled=true]
    [—property (name=value)[:name=value]*] listener_id
```

Description The `create-iiop-listener` command creates an IIOP listener. This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—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 ■ `server`, which creates the listener for the default server instance `server` and is the default value ■ *configuration_name*, which creates the listener for the named configuration ■ *cluster_name*, which creates the listener for every server instance in the cluster ■ *stand-alone_instance_name*, which creates the listener for a particular stand-alone server instance
—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

listener_id	A unique identifier for the IIOP listener to be created.

Examples

EXAMPLE 1 Using the create-iiop-listener command

The following command creates an IIOP listener named `sample_iiop_listener`:

```
asadmin> create-iiop-listener --user admin
--passwordfile passwords.txt --host host1 --port 4849
--listeneraddress 192.168.1.100 --iiopport 1400 sample_iiop_listener
Command create-iiop-listener executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also delete-iiop-listener(1), list-iiop-listeners(1), create-ssl(1)

Name create-instance – creates an instance

Synopsis

```
create-instance —user admin_user —passwordfile filename [—host host_name]
    [—port port_number] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—config config_name | —cluster cluster_name]
    —nodeagent nodeagent_name
    [—systemproperties (name=value)[:name=value]*] instance_name
```

Description 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:

- A reference to a node agent which defines the machine where the server instance resides.
- 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.

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.

There are three types of server instances that can be created. Each server instance can only be of one type:

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.
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.
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.

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.

Options

–u —`user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—help	Displays the help text for the command.
—config	Creates a shared server instance. The configuration name must exist and must not be named default-config or server-config. If the configuration name provided is a standalone configuration, an error is displayed.
—cluster	Creates a clustered server instance that inherits its configuration from the named cluster.
—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.
JMS_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 *instance_name*

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
```

EXAMPLE 1 Using the create-instance command *(Continued)*

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)`

Name create-javamail-resource – creates a JavaMail session resource

Synopsis

```
create-javamail-resource —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] —mailhost hostname
    —mailuser username —fromaddress address [—storeprotocol imap]
    [—storeprotocolclass com.sun.mail.imapIMAPStore] [—transprotocol smtp]
    [—transprotocolclass com.sun.mail.smtp.SMTPTransport] [—debug=false]
    [—enabled=true] [—description text]
    [—property (name=value)[:name=value]*] jndi_name
```

Description The `create-javamail-resource` command creates a JavaMail session resource. This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
`––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 ■ `server`, which creates the resource for the default server instance `server` and is the default value ■ `domain`, which creates the resource for the domain ■ *cluster_name*, which creates the resource for every server instance in the cluster ■ *instance_name*, which creates the resource for a particular server instance
`––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 *username*@*host*.*domain*.
`––storeprotocol`	The mail server store protocol. The default is `imap`. 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 `com.sun.mail.imap.IMAPStore`. Change this value only if you have reconfigured the Application Server's mail provider to use a nondefault store protocol.

—transprotocol	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.
—transprotocolclass	The mail server transport protocol class name. The default is `com.sun.mail.smtp.SMTPTransport`. Change this value only if you have reconfigured the Application Server's mail provider to use a nondefault transport protocol.
—debug	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.
—enabled	If set to true, the resource is enabled at runtime. The default value is true.
—description	A text description of the JavaMail resource.
—property	Optional attribute name/value pairs for configuring the JavaMail resource. The JavaMail API documentation lists the properties you might want to set.

Operands

jndi_name	The JNDI name of the JavaMail resource to be created. It is a recommended practice to use the naming subcontext prefix `mail/` for JavaMail resources.

Examples

EXAMPLE 1 Using the create-javamail-resource command

The following command creates a JavaMail resource named `mail/MyMailSession`. The escape character (\) is used in the —`fromaddress` option to distinguish the dot (`.`) and at sign (`@`). The JNDI name for a JavaMail session resource customarily includes the `mail/` naming subcontext.

```
asadmin> 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.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `delete-javamail-resource(1)`, `list-javamail-resources(1)`

Name create-jdbc-connection-pool – registers the JDBC connection pool

Synopsis

```
create-jdbc-connection-pool —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—datasourceclassname classname]
    [—restype res_type] [—steadypoolsize poolsize] [—maxpoolsize poolsize]
    [—maxwait time] [—poolresize limit] [—idletimeout time]
    [—isolationlevel isolation_level] [—isolationguaranteed true]
    [—isconnectvalidatereq false] [—validationmethod auto-commit]
    [—validationtable tablename] [—failconnection false] [—description text]
    [—property (name=value) [:name=value]*] connectionpoolid
```

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	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
––help	Displays the help text for the command.
––target	The target option is deprecated.
––datasourceclassname	The name of the vendor supplied JDBC datasource resource manager.
––restype	The interface that the datasource class implements. Must be one of `javax.sql.DataSource`, `javax.sql.ConnectionPoolDataSource` or `javax.sql.XADataSource`. 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.
––steadypoolsize	The minimum and initial number of connections maintained in the pool. The default value is 8.
––maxpoolsize	The maximum number of connections that can be created. The default value is 32.
––maxwait	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.
––poolresize	The quantity by which the pool will scale up or scale down the number of connections. When the pool has no free connections, it will scale up by this quantity. When the pool scales down, all the invalid and idle connections are removed, sometimes resulting in removing connections of quantity greater than this value. When the pool size reaches `steadypoolsize`, the connection removal stops. The default value is 2.
––idletimeout	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.
—isolationlevel	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. You can set a desired isolation level using one of the standard transaction isolation levels: `read-uncommitted`, `read-committed`, `repeatable-read`, `serializable`. Applications that change the isolation level on a pooled connection programmatically risk polluting the pool. This could lead to program errors.
—isisolationguaranteed	This is applicable only when a particular isolation level is specified for transaction-isolation-level. The default value is true. This option assures that every time a connection is obtained from the pool,isolationlevel is set to the desired value. This could have some performance impact on some JDBC drivers. Administrators can set this to false when the application does not change —`isolationlevel` before returning the connection.
—isconnectvalidatereq	If set to true, connections are validated or checked to see if they are usable before giving out the application. The default value is false.
—validationmethod	The name of the validation table used to perform a query to validate a connection. Valid settings are: `auto-commit`, `meta-data`, or `table`. The default value is auto-commit.
—validationtable	The name of the validation table used to perform a query to validate a connection.
—failconnection	If set to true, all connections in the pool must be closed when a single validation check fails. The default value is false. One attempt is made to re-establish failed connections.
—description	Text providing descriptive details about the specified JDBC connection pool.
—property	Optional attribute name/value pairs for configuring the connection pool.

Operands

connectionpoolid	The name of the JDBC connection pool to be created.

Examples

EXAMPLE 1 Using create-jdbc-connection-pool command

```
asadmin> create-jdbc-connection-pool --user admin --passwordfile passwords.txt
--host localhost --port 7070 --datasourceclassname org.apache.derby.jdbc.ClientDataSource --r
javax.sql.XADataSource --isolationlevel serializable --isconnectvalidatereq=true
--validationmethod auto-commit --description "XA Connection"
--property portNumber=1527:password=APP:user=APP:serverName=localhost:databaseName=sun-appser
Command create-jdbc-connection-pool executed successfully
```

Where, the sample_derby_pool is created. The escape character "\" is used in the `--property` option to distinguish the semicolon (;) Two backslashes (\\) are used to distinguish the equal sign (=).

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

```
create-jdbc-resource —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—targettarget] connectionpoolid pool_name
    [—enabled=true] [—description text]
    [—property (name=value)[:name=value]*] jndi_name
```

Description The create-jdbc-resource command creates a new JDBC resource. This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—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, and instance. The default is server.
—connectionpoolid	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.
—enabled	Determines whether the JDBC resource is enable at runtime. The default value is true.
—description	Text providing descriptive details about the JDBC resource.
—property	optional attribute name/value pairs for configuring the resource.

Operands

jndi_name	the JNDI name of this JDBC resource.

Examples

EXAMPLE 1 Using the create-jdbc-resource command

```
asadmin> create-jdbc-resource --user admin
--passwordfile secret.txt --host pigeon --port 5001 --connectionpoolid connPool02  test_jdbc_
Command create-jdbc-resource executed successfully.
```

Where test_jdbc_resource is the name of the new JDBC resource.

Exit Status

0	command executed successfully
1	error in executing the command

See Also `delete-jdbc-resource(1)`, `list-jdbc-resources(1)`

Name create-jmsdest – creates a physical destination

Synopsis

```
create-jmsdest —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] —desttype dest_type
    [—property (name=value)[:name=value]*] dest_name
```

Description The `create-jmsdest` command creates a JMS physical destination. Along with the physical destination, you use the `create-jms-resource` 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.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.

`––help`
Displays the help text for the command.

`––target`
In Enterprise Edition, specifies the target for which you are creating the physical destination. Although the `create-jmsdest` command is related to resources, a physical destination is created using the JMS Service, which is part of the configuration. Valid values are

- `server`, which creates the physical destination for the default server instance `server` and is the default value
- *configuration_name*, which creates the physical destination for the named configuration
- *cluster_name*, which creates the physical destination for every server instance in the cluster
- *instance_name*, which creates the physical destination for a particular server instance

`–T ––desttype`
The type of the JMS destination. Valid values are `topic` and `queue`.

`––property`
Optional attribute name/value pairs for configuring the physical destination. You can specify the following property for a physical destination:

Property	Definition
maxNumActiveConsumers	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.)

To modify the value of this property or to specify other physical destination properties, use the *install_dir*`/imq/bin/imqcmd` command. See the *Sun Java System Message Queue 3 2005Q1 Administration Guide* for more information.

Operands

dest_name	A unique identifier for the the JMS destination to be created.

Examples

EXAMPLE 1 Using the create-jmsdest command

The following command creates a JMS physical queue named `PhysicalQueue`.

```
asadmin> create-jmsdest --user admin
--passwordfile passwords.txt --host localhost --port 4848 --desttype queue
--property User=public:Password=public PhysicalQueue
Command create-jmsdest executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `create-jms-resource(1)`, `delete-jmsdest(1)`, `list-jmsdest(1)`

Name create-jms-host – creates a JMS host

Synopsis

```
create-jms-host —user admin_user [—passwordfile filename] [—host localhost]
     [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
     [—interactive=true] [—help] [—target target] [—mqhost localhost]
     [—mqport 7676] [—mquser admin] [—mqpassword admin]
     [—property (name=value)[:name=value]*] jms_host_name
```

Description Creates a JMS host within the JMS service. This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—help	Displays the help text for the command.
—target	In Enterprise Edition, specifies the target for which you are creating the JMS host. Valid values are ■ `server`, which creates the JMS host for the default server instance `server` and is the default value ■ *configuration_name*, which creates the JMS host for the named configuration ■ *cluster_name*, which creates the JMS host for every server instance in the cluster ■ *instance_name*, which creates the JMS host for a particular server instance
—mqhost	The host name for the JMS service. The default value is `localhost`.
—mqport	The port number used by the JMS service. The default value is 7676.
—mquser	The user name for the JMS service. The default value is `admin`.
—mqpassword	The password for the JMS service. The default value is `admin`.
—property	Optional attribute name/value pairs for configuring the JMS host.

Operands

jms_host_name	A unique identifier for the JMS host to be created.

Examples

EXAMPLE 1 Using the create-jms-host command

The following command creates a JMS host named `MyNewHost`:

```
asadmin> create-jms-host --user admin
--passwordfile passwords.txt --mqhost pigeon --mqport 7677 MyNewHost
Command create-jms-host executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `list-jms-hosts(1)`, `delete-jms-host(1)`

Name create-jms-resource – creates a JMS resource

Synopsis

```
create-jms-resource —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] —restype type
    [—enabled=true] [—description text]
    [—property (name=value)[:name=value]*] jndi_name
```

Description The `create-jms-resource` command creates a Java Message Service (JMS) connection factory resource or a JMS destination resource.

This command sets the default Minimum Pool Size and Maximum Pool Size as follows:

- Minimum Pool Size : 1
- Maximum Pool Size : 250

Note – The default values of Minimum Pool Size and Maximum Pool Size set from the Administration GUI are different from the values set by the `create-jms-resource` command. This is due to the Administration GUI internally using the newer, `create-connector-connection-pool` command. The default values set by the Administration GUI are as follows:

- Minimum Pool Size : 8
- Maximum Pool Size : 32

This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD,

	AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H` `––host`	The machine name where the domain administration server is running. The default value is localhost.
`–p` `––port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s` `––secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
`––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 ■ `server`, which creates the resource for the default server instance `server` and is the default value ■ `domain`, which creates the resource for the domain ■ *cluster_name*, which creates the resource for every server instance in the cluster ■ *instance_name*, which creates the resource for a particular server instance
`––restype`	The JMS resource type, which can be either `javax.jms.Topic`, `javax.jms.Queue`, `javax.jms.ConnectionFactory`, `javax.jms.TopicConnectionFactory`, or `javax.jms.QueueConnectionFactory`.
`––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.
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 `earth` or `earth:7677`. 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 `AddressList`. This property name is deprecated. Use `AddressList` instead.
UserName	The user name for the connection factory. Default: `guest`.
Password	The password for the connection factory. Default: `guest`.
ReconnectEnabled	If enabled (value = `true`), specifies that the client runtime attempts to reconnect to a message server (or the list of addresses in the AddressList) when a connection is lost. Default: `false`.

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`.
AddressListIterations	Specifies the number of times the client runtime iterates through the AddressList in an effort to establish (or reestablish) 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 `create-jmsdest` 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/MyQueue`. 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)`

Name create-jndi-resource – registers a JNDI resource

Synopsis

```
create-jndi-resource —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target]
    —jndilookupname lookup_name —restype type —factoryclass class_name
    [—enabled=true] [—description text]
    [—property (name=value)[:name=value]*] jndi_name
```

Description The `create-jndi-resource` command registers a JNDI resource. This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
––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.
orb-listener-1–port	This property specifies which ORB listener port for IIOP connections orb-listener-1 listens on.

Property	Definition
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

`create-jvm-options` —`user` *admin_user* [—`passwordfile` *filename*] [—`host` *localhost*] [—`port` *4849*] [—`secure`|–`s`] [—`terse`=*false*] [—`echo`=*false*] [—`interactive`=*true*] [—`help`] [—`target` *target*] [—`profiler=false`] (*jvm_option_name=jvm_option_value*) [:*jvm_option_name=jvm_option_name*] *

Description The `create-jvm-options` command creates JVM options in the Java configuration or the profiler element of the `domain.xml` file. If the JVM options are created for a profiler, they are used to record the settings needed to get a particular profiler going.

This command is supported in remote mode only.

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.

Options

–`u` —`user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–`H` —`host`	The machine name where the domain administration server is running. The default value is localhost.
–`p` —`port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–`s` —`secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
	`––target`	Specifies the target on which you are creating the JVM options. Valid values are config, instance, cluster, and server. The default value is server.
	`--profiler`	Indicates whether the JVM options are for the profiler. The profiler must exist for this option to be true.
Operands	*jvm_option_name*	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 **EXAMPLE 1** Using the create-jvm-options command

JVM options must start with a dash (–), . Use the backslash (\\) to escape the dash delimiter.

```
asadmin> create-jvm-options --user admin --passwordfile passwords.txt
--host localhost --port 4849 --target server "-Dtmp=sun" \\-Doption1=value1
Command create-jvm-options executed successfully
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `delete-jvm-options(1)`

Name create-lifecycle-module – adds a lifecycle module

Synopsis

```
create-lifecycle-module —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—enabled=true] [—target target]
    —classname classname [—classpath classpath] [—loadorder loadorder]
    [—failurefatal=false ] [—description description]
    [—property (name=value)[:name=value]*] module_name
```

Description Creates the lifecycle module. The lifecycle modules provide ameans of running short or long duration Java-based tasks within the application server environment. This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
––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

module_name	This operand is a unique identifier or the deployed server lifecycle event listener module.

Examples

EXAMPLE 1 using create-lifecycle-module

```
asadmin> create-lifecycle-module --user admin --passwordfile adminpassword.txt
--host fuyako --port 7070 --classname "com.acme.CustomSetup"
--classpath "/export/customSetup" --loadorder 1 --failurefatal=true
```

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

```
--description "this is a sample customSetup"
--property rmi="Server\=acme1\:7070":timeout=30 customSetup
Command create-lifecycle-module executed successfully
```

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)`

Name create-message-security-provider – enables administrators to create the `message-security-config` and `provider-config` sub-elements for the security service in `domain.xml`

Synopsis

```
create-message-security-provider —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] —classname provider_class
    [—layer message_layer] [—providertype provider_type]
    [—requestauthsource request_auth_source]
    [—requestauthrecipient request_auth_recipient]
    [—responsetauthsource response_auth_source]
    [—responseauthrecipient response_auth_recipient] [—isdefaultprovider]
    [—property (name=value)[:name=value]*] provider_name
```

Description 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.

If the message-layer (`message-security-config`) does not exist, it is created, and then the `provider-config` is created under it.

This command is supported in remote mode only.

Options 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.

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD,

	AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H ––host`	The machine name where the domain administration server is running. The default value is localhost.
`–p ––port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s ––secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
`––help`	Displays the help text for the command.
`––target`	In Enterprise Edition, specifies the target to which you are deploying. Valid values are ■ `server`, which deploys the component to the default server instance `server` and is the default value ■ `domain`, which deploys the component to the domain. ■ *cluster_name*, which deploys the component to every server instance in the cluster. ■ *instance_name*, which deploys the component to a particular sever instance. The following optional attribute name/value pairs are available:

Property	Definition
classname	Defines the Java implementation class of the provider. Client authentication providers must implement the com.sun.enterprise. `security.jauth.ClientAuthModule` interface. Server-side providers must implement the `com.sun.enterprise.security jauth.ServerAuthModule` 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 `auth-layer` attribute of `message-security-config` elements. The default is `SOAP`.
providertype	Establishes whether the provider is to be used as client authentication provider, server authentication provider, or both. Valid options for this property include `client`, `server`, or `client-server`. The default value is `client-server`.
requestauthsource	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 request messages. Possible values are `sender` or `content`. When this argument is not specified, source authentication of the request is not required.

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.

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-node-agent – creates a node agent

Synopsis

```
create-node-agent [—host DAS_host] [—port DAS_port] —user DAS_user
    [—secure|–s=true] [—terse=false] [—echo=false] [—interactive=true]
    [—agentdir nodeagent_path] [—agentport port_number]
    [—agentproperties (name=value)[:name=value]*] [—passwordfile filename]
    [—savemasterpassword=false] [nodeagent_name]
```

Description The node agent facilitates remote server instance management. It is the responsibility of the node agent to create, start, stop, and delete a server instance. Every node agent must have a unique name and every new server instance must be created with a reference to a node agent name defining the machine on which the instance will reside. A node agent must be present on every machine that hosts server instances, including the machine hosting the Domain Administration Server (DAS).

The domain administration server connection options (such as host, port and user) identify the agent's initial target domain. The DAS does not need to be running when the node agent is being created.

Options

–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–u —user	The authorized domain administration server administrative username.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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 to the standard output. Default is false.
–I —interactive	If set to true (default), only the required options are prompted.
—agentdir	Like a DAS, each node agent resides in a top level directory named *agentdir*/*nodeagent_name*. If the `agentdir` option is not specified, then the default *install-dir*/`nodeagents` is used.

—`agentport`

The port on which the node agent's JMX connector will listen and accept requests. If not specified, a random unused port is chosen.

—`agentproperties`

Use this option to override the default values of node agent properties. The following agentproperties are available:

Property	Definition
listenaddress	The address used by the JMX connector to listen for requests or notifications. The default is 0.0.0.0.
remoteclientaddress	The address used by DAS to connect to the Node Agent. The default is the hostname of the server.

—`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 administration server password, use an entry with the following format: `AS_ADMIN_PASSWORD`=*password*, where *password* is the actual administrator password. Passwords that can be specified for this command are AS_ADMIN_PASSWORD and AS_ADMIN_MASTERPASSWORD.

—`savemasterpassword`

Setting this option to true allows the master password to be written to the file system. This is necessary so that the `start-node-agent` command can start the server without having to prompt the user. However, for security purposes, the default setting is false because saving the master password on the disk is an insecure practice.

Operands *nodeagent_name*

The name of the node agent must be unique in the domain. If not specified, the nodeagent_name defaults to the machine's host name. Do not use any reserved words or characters in the node agent name.

Examples

EXAMPLE 1 Using the create-node-agent command

The following command creates nodeagent1 in the default *install-dir*`/nodeagents` directory.

```
asadmin>create-node-agent --host dance --port 4849 --user admin1
--passwordfile /home/password.txt nodeagent1
Command create-node-agent executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also

`delete-node-agent(1)`, `list-node-agents(1)`, `start-node-agent(1)`, `stop-node-agent(1)`

Name create-node-agent-config – adds a new unbound node agent to a domain

Synopsis

```
create-node-agent-config —user admin_name —passwordfile filename
    [—host localhost] [—port port_number] [—secure=true] [—terse=false]
    [—echo=false] [—interactive=true] nodeagent_name
```

Description This command allows an agent placeholder to be created before the node agent's directory structure is created, using the create-node-agent command. This supports the offline configuration scenario where administrators define server instances in advance of creating the node agents on remote machines.

Options

–u —user	The authorized domain application server administrative username.
–w —password	The —password option is deprecated. Use —passwordfile instead.
—passwordfile	The name of the file containing the domain application server password. The passwordfile should contain either of the following entries: AS_ADMIN_PASSWORD=*password* or AS_ADMIN_MAPPEDPASSWORD=*password*. If this option is not called directly, you will be prompted for it before the requested action is completed.
–H —host	The machine name where the the domain application server is running.
–p —port	The port number of the domain application server listening for administration requests.
–s —secure	If set to true, this command 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. The default is false.
–e —echo	Setting this option to true will echo the command line statement on the standard output. The default is false.
–I —interactive	If this option is set to true (default), only the required password options are prompted.

Operands

nodeagent_name	The name of the node must be unique on the machine. Typically, the nodeagent_name is the host name of the machine where the node agent will reside.

Examples

EXAMPLE 1 Using create-node-agent-config

```
asadmin> create-node-agent-config --user admin1 --passwordfile filename nodeagent1
Command create-node-agent-config executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also

`delete-node-agent-config(1)`

Name create-password-alias – creates a password alias

Synopsis

```
create-password-alias —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—aliaspassword alias_password] aliasname
```

Description 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 an encrypted form. The `create-password-alias` command takes 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.

This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—-help	Displays the help text for the command.
	—-aliaspassword	The password corresponding to the password alias. WARNING: Passing this option on the command line is insecure. The password is optional, and when omitted, the user is prompted.
Operands	aliasname	The name of the alias password as it appears in the domain.xml file.

Examples **EXAMPLE 1** Using create-password-alias command

```
asadmin> create-password-alias --user admin --passwordfile /home/password.txt
--interactive=true jmspassword-alias
Please enter the alias password>
Please enter the alias password again>
Command create-password-alias executed successfully.
```

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)

Name create-persistence-resource – registers a persistence resource

Synopsis

```
create-persistence-resource —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—enabled=true] [—target target]
    [—jdbcjndiname jndi_name | —connectionpoolid id]
    [—factoryclass classname] [—description text]
    [—property (name=value)[:name=value]*] jndi_name
```

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

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—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 ■ `server`, which deploys the component to the default server instance `server` and is the default value ■ `domain`, which deploys the component to the domain. ■ *cluster_name*, which deploys the component to every server instance in the cluster. ■ *instance_name*, which deploys the component to a particular sever instance.
	—jdbcjndiname	Specifies the JDBC resource with which database connections are obtained. It must be the name of a pre-created JDBC resource.
	—connectionpoolid	This option and the option `---jdbcjndiname` are mutually exclusive. If `- --connectionpoolid` is specified, then a jdbc resource will be created behind the scene with "PM" appended to the end of persistence resource name. See example.
	—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.
Operands	*jndi_name*	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 jdbc/sample sample_persistence_resource
Command create-persistence-resource executed successfully
```

EXAMPLE 2 Using create-persistence-resource

```
asadmin> create-persistence-resource --user admin --passwordfile secret.txt
--connectionpoolid testPool testPersistence
Command create-persistence-resource executed successfully
```

This command creates a jdbc resource with the name `testPersistencePM` referencing `testPool`. When you delete the persistence resource, the jdbc resource created by this command is also removed.

Exit Status

0	command executed successfully
1	error in executing the command

See Also

`delete-persistence-resource(1)`, `list-persistence-resources(1)`

Name create-profiler – creates the profiler element

Synopsis

```
create-profiler —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target_name] [—classpath classpath]
    [—nativelibpath native_library_path] [—enabled=true]
    [—property(name=value)[:name=value]*] profiler_name
```

Description 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.

This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—help	Displays the help text for the command.
—target	This option specifies the target on which you are creating a profiler. Valid values are ■ server, which creates the profiler for the default server instance. This is the default value. ■ *configuration_name*, which creates the profiler for the named configuration ■ *cluster_name*, which creates the profiler for every server instance in the cluster ■ *instance_name*, which creates the profiler for a particular server instance This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.
—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

profiler_name	name of the profiler.

Examples

EXAMPLE 1 Using create-profiler

```
asadmin> create-profiler --user admin --passwordfile password.txt
--host localhost --port 4848 --classpath /home/appserver/
--nativelibpath /u/home/lib --enabled=false
```

EXAMPLE 1 Using create-profiler *(Continued)*

```
 --property defaultuser=admin:password=adminadmin sample_profiler
Created Profiler with id = sample_profiler
```

Where: `sample_profiler` is the profiler created.

Exit Status

0	command executed successfully
1	error in executing the command

See Also `delete-profiler(1)`

Name create-resource-adapter-config – creates the configuration information in `domain.xml` for the connector module

Synopsis

```
create-resource-adapter-config —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—threadpoolid threadpool]
    [—property (property name=value)[:name=value]*] raname
```

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

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—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	*raname*	This operand is the value kept in the `resource-adapter-name` in the `domain.xml` file.

Examples **EXAMPLE 1** Using `create-resource-adapter-config`

```
asadmin> create-resource-adapter-config u--user u1 --passwordfile pfile1 ra1
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)`

Name create-resource-ref – creates a reference to a resource

Synopsis

```
create-resource-ref —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] [—enabled=true]
    reference_name
```

Description The `create-resource-ref` command creates a reference from a cluster or an unclustered server instance to a previously created resource (for example, a JDBC resource created using the `create-jdbc-resource` command). This effectively results in the resource being made available in the JNDI tree of the targeted instance or cluster.

The target instance or instances making up the cluster need not be running or available for this command to succeed. If one or more instances are not available, they will receive the new resource the next time they start.

This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.

`–s ––secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
`––help`	Displays the help text for the command.
`––target`	Specifies the target for which you are creating the resource reference. Valid values are ■ `server`, which creates the resource reference for the default server instance `server` and is the default value ■ *cluster_name*, which creates the resource reference for every server instance in the cluster ■ *instance_name*, which creates the resource reference for the named unclustered server instance
`––enabled`	Indicates whether the resource should be enabled. This value will take effect only if the resource is enabled at the global level. The default is `true`.

Operands

reference_name	The name or JNDI name of the resource.

Examples

EXAMPLE 1 Using the create-resource-ref command

The following command creates a reference to the JMS destination resource `jms/Topic` on the cluster `Cluster1`.

```
asadmin> create-resource-ref --user admin
--passwordfile passwords.txt --target Cluster1 jms/Topic
Command create-resource-ref executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `delete-resource-ref(1)`, `list-resource-refs(1)`

Name create-ssl – creates and configures the SSL element in the selected HTTP listener, IIOP listener, or IIOP service

Synopsis

```
create-ssl —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] —type listener_or_service_type
    —certname cert_name [—ssl2enabled=false ] [—ssl2ciphers ss12ciphers]
    [—ssl3enabled=true ] [—tlsenabled=true ] [—ssl3tlsciphers ssl3tlsciphers]
    [—tlsrollbackenabled=true] [—clientauthenabled=false ] [listener_id]
```

Description 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.

This command is supported in remote mode only.

Options 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.

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.

`–s ––secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
`––help`	Displays the help text for the command.
`––target`	In Enterprise Edition, specifies the target on which you are configuring the ssl element. The following values are valid: ■ `server`, the server in which the iiop-service or HTTP/IIOP listener is to be configured for SSL. ■ *config*, the configuration that contains the HTTP/IIOP listener or iiop-service for which SSL is to be configured. ■ *cluster*, the cluster in which the HTTP/IIOP 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. ■ *instance*, the instance in which the HTTP/IIOP listener or iiop-service is to be configured for SSL.

Optional Attributes The following optional attribute name/value pairs are available:

Property	Definition
type	The type of service or listener for which the SSL is created. The type can be *http-listener*, *iiop-listener*, or *iiop-service*. When the type is *iiop-service*, the `ssl-client-config` along with the embedded ssl element is created in domain.xml.
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 *tokenname:nickname*. For this property, the *tokenname:* is optional.

Property	Definition
ssl2enabled	Set this property to *true* to enable SSL2. The default value is *false*. 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: *rc4*, *rc4export*, *rc2*, *rc2export*, *idea*, *des*, and *desede3*. If no value is specified, all supported ciphers are assumed to be enabled.
ssl3enabled	Set this property to *false* to disable SSL3. The default value is *true*. 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.
tlsenabled	Set this property to *false* to disable TLS. The default value is *true* It is good practice to enable TLS, which is a more secure version of SSL.
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 values are *SSL_RSA_WITH_RC4_128_MD5*, *SSL_RSA_WITH_3DES_EDE_CBC_SHA*, , *SSL_RSA_WITH_DES_CBC_SHA*, *SSL_RSA_EXPORT_WITH_RC4_40_MD5*, *SSL_RSA_WITH_NULL_MD5*,*SSL_RSA_WITH_RC4_128_SHA*, and *SSL_RSA_WITH_NULL_SHA*. If no value is specified, all supported ciphers are assumed to be enabled.
tlsrollbackenabled	Set to *true* (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 `tlsenabled`=*true*.
clientauthenabled	Set to *true* if you want SSL3 client authentication performed on every request independent of ACL-based access control. Default value is *false*.

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
Command create-ssl executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also

`delete-ssl(1)`

Name create-system-properties – adds or updates one or more system properties of the domain, configuration, cluster, or server instance

Synopsis

```
create-system-properties —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target_name]
    [name=value)[:name=value]*]
```

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 overriden 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	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—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	*name=value*	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 **EXAMPLE 1** Using create-system-properties

```
asadmin> create-system-properties --user admin --passwordfile password.txt
--host localhost --port 4849 --target mycluster http-listener-port=1088
Command create-system-properties executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also delete-system-property(1), list-system-properties(1)

Name create-threadpool – adds a threadpool

Synopsis

```
create-threadpool —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target_name]
    [—maxthreadpoolsize max_thread_pool_size]
    [—minthreadpoolsize min_thread_pool_size]
    [—idletimeout idle_thread_timeout_in_seconds]
    [—workqueues number_work_queues] threadpool_id
```

Description 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.

Options

—u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
—H —host	The machine name where the domain administration server is running. The default value is localhost.
—p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
—s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—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 ■ `server`, which creates the listener for the default server instance `server` and is the default value ■ *configuration_name*, which creates the listener for the named configuration ■ *cluster_name*, which creates the listener for every server instance in the cluster ■ *instance_name*, which creates the listener for a particular server instance
	—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	*threadpool_id*	an ID for the work queue; for example, thread-pool-1, thread-pool-2, etc.

Examples **EXAMPLE 1** Using create-threadpool

```
asadmin> create-threadpool --user admin1 --passwordfile password.txt --maxthreadpoolsize 100
threadpool-1
Command create-threadpool executed successfully
```

Exit Status	0	command executed successfully

1	error in executing the command

See Also `delete-threadpool(1)`, `list-threadpools(1)`

Name create-virtual-server – creates the named virtual server

Synopsis

```
create-virtual-server —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target server] —hosts hosts
    [—httplisteners http_listeners] [—defaultwebmodule default_web_module]
    [—state on] [—logfile log_file] [—property (name=value)[:name=value]*]
    virtual_server_id
```

Description 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.

This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
`––help`	Displays the help text for the command.
`––target`	In Enterprise Edition, specifies the target for which you are creating the virtual server. Valid values are ■ `server`, which creates the virtual server for the default server instance `server` and is the default value ■ *configuration_name*, which creates the virtual server for the named configuration ■ *cluster_name*, which creates the virtual server for every server instance in the cluster ■ *instance_name*, which creates the virtual server for a particular server instance
`––hosts`	A comma-separated (,) list of values allowed in the host request header to select the current virtual server. Each virtual server that is configured to the same connection group must have a unique hosts value for that group.
`––httplisteners`	A comma-separated (,) list of HTTP listener IDs. Required only for a virtual server that is not the default virtual server.
`––defaultwebmodule`	The standalone web module associated with this virtual server by default.
`––state`	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.
`––logfile`	Name of the file where log entries for this virtual server are to be written. By default, this is the server log.
`––property`	Optional attribute name/value pairs for configuring the virtual server. The following properties are available:

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.

Operands *virtual_server_id* 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`:

EXAMPLE 1 Using the create-virtual-server command *(Continued)*

```
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)`

Name delete-acl – removes the access control list file

Synopsis

```
delete-acl --user admin_user[--password admin_password][--host localhost]
     [--port 4848][--passwordfile filename][--secure|-s][--instance
     instance_name] acl_ID
```

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

acl_ID	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

EXAMPLE 1 Using delete-acl

```
asadmin> delete-acl --user admin --password adminadmin --host fuyako --port 7070 --instance s
Deleted ACL with id = sampleACL
```

Where: `sampleACL` is the ACL that is deleted.

Exit Status

0	command executed successfully
1	error in executing the command

Interface Equivalent Access Control List page

See Also `create-acl(1)`, `list-acl(1)`

Name delete-admin-object – removes the administered object with the specified JNDI name

Synopsis

```
delete-admin-object —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] jndi_name
```

Description removes the administered object with the specified JNDI name.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
`––help`	Displays the help text for the command.
`––target`	Specifies the target on which you are creating the administered object.This option is available only in the Sun Java System Application Server Standard and Enterprise Edition. Valid values are: ■ `server`, which creates the administered object for the default server instance `server` and is the default value ■ *configuration_name*, which creates the administered object for the named configuration ■ *cluster_name*, which creates the administered object for every server instance in the cluster ■ *instance_name*, which creates the administered object for a particular server instance

Operands

jndi_name	JNDI name of the administered object to be deleted.

Examples

EXAMPLE 1 Using delete-admin-object

The example listed in the `add-admin-object` command should be executed before attempting to execute this example:

```
asadmin> delete-admin-object --user admin --passwordfile passwords.txt
--target instance1 jms/samplequeue
Command delete-admin-object executed successfully
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `create-admin-object(1)`, `list-admin-objects(1)`

Name delete-application-ref – removes a reference to an application

Synopsis

```
delete-application-ref —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] [—cascade=false]
    reference_name
```

Description The `delete-application-ref` command removes a reference from a cluster or an unclustered server instance to an application. This effectively results in the application element being undeployed and no longer available on the targeted instance or cluster.

The target instance or instances making up the cluster need not be running or available for this command to succeed. If one or more instances are not available, they will no longer load the application the next time they start.

Removal of the reference does not result in removal of the application from the domain. The bits are removed only by the `undeploy` command.

This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.

	`–p ––port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
	`–s ––secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
	`––target`	Specifies the target from which you are removing the application reference. Valid values are ■ `server`, which removes the application reference from the default server instance `server` and is the default value ■ *cluster_name*, which removes the application reference from every server instance in the cluster ■ *instance_name*, which removes the application reference from the named unclustered server instance
	`––cascade`	For a connector module, indicates whether the resources dependent on the module should also be recursively deleted. The default is `false`. The connector module can be either a stand-alone RAR file or a module within an EAR file.
Operands	*reference_name*	The name of the application or module, which can be a J2EE application module, Web module, EJB module, connector module, application client module, or lifecycle module.

Examples **EXAMPLE 1** Using the delete-application-ref command

The following command removes a reference to the Web module `MyWebApp` from the unclustered server instance `NewServer`.

```
asadmin> delete-application-ref --user admin2
--passwordfile passwords.txt --target NewServer MyWebApp
Command delete-application-ref executed successfully.
```

Exit Status	0	command executed successfully

1	error in executing the command

See Also `create-application-ref(1)`, `list-application-refs(1)`, `undeploy(1)`

Name create-audit-module – removes the named audit-module

Synopsis

```
delete-audit-module —user admin_user [—passwordfile filename]
     [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
     [—interactive=true] [—help] [—target target_name] audit_module_name
```

Description Removes the named audit module. This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
	—target	In Enterprise Edition, specifies the target on which you are deleting the audit module. Valid values are ■ server, which deletes the audit module for the default server instance server and is the default value ■ *configuration_name*, which deletes the audit module for the named configuration ■ *cluster_name*, which deletes the audit module for every server instance in the cluster ■ *instance_name*, which deletes the audit module for a particular server instance
Operands	*audit_module_name*	name of the audit module to be deleted.

Examples **EXAMPLE 1** Using delete-audit-module

```
asadmin> delete-audit-module --user admin1
--passwordfile password.txt --host pigeon --port 5001 sampleAuditModule
Command delete-audit-module executed successfully
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also create-audit-module(1), list-audit-modules(1)

Name delete-auth-realm – removes the named authentication realm

Synopsis

```
delete-auth-realm —user admin_user [—passwordfile filename] [—host localhost]
     [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
     [—interactive=true] [—help] [—target target_name] auth_realm-name
```

Description Removes the named authentication realm. This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
	—target	In Enterprise Edition, specifies the target on which you are deleting the authentication realm. Valid values are ■ server, which deletes the realm for the default server instance server and is the default value ■ *configuration_name*, which deletes the realm for the named configuration ■ *cluster_name*, which deletes the realm for every server instance in the cluster ■ *instance_name*, which deletes the realm for a particular server instance
Operands	*auth_realm_name*	name of this realm.

Examples **EXAMPLE 1** Using delete-auth-realm

```
asadmin> delete-auth-realm --user admin1 --passwordfile password.txt
--host pigeon --port 5001 db
Command delete-auth-realm executed successfully
```

Where db is the authentication realm deleted.

Exit Status	0	command executed successfully
	1	error in executing the command

See Also create-auth-realm(1), list-auth-realms(1)

Name delete-cluster – deletes a cluster

Synopsis

```
delete-cluster —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] cluster_name
```

Description The `delete-cluster` command deletes a cluster. A cluster can be deleted only if it contains no server instances. Stop and delete all server instances in the cluster before deleting the cluster.

If a standalone cluster is deleted (that is, the cluster's configuration name is *cluster_name*`-config` and no other clusters or unclustered instances refer to this configuration), then its standalone configuration is automatically deleted.

This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
Operands	*cluster_name*	The name of the cluster to be deleted.

Examples **EXAMPLE 1** Using the delete-cluster command

The following command deletes the cluster named `MyCluster`. The same command also automatically deletes the configuration named `MyCluster-config`.

```
asadmin> delete-cluster --user admin1
--passwordfile passwords.txt MyCluster
Command delete-cluster executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-cluster(1)`, `list-clusters(1)`, `start-cluster(1)`, `stop-cluster(1)`, `stop-instance(1)`

Name delete-config – deletes an existing configuration

Synopsis

```
delete-config —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] configuration_name
```

Description Use the delete-config command to delete an existing configuration in the `domain.xml` file. You can delete a configuration only if the configuration has no server instances or clusters referring to it. A standalone configuration is automatically deleted when the sever instance or cluster referring to it is deleted. You cannot delete the `default-config` configuration that is used to create new standalone configurations.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
Operands	*configuration_name*	The name of the configuration you are deleting.

Examples **EXAMPLE 1** Using the delete-config command

```
asadmin> delete-config --user admin --passwordfile passwords.txt my-config
Command delete-config executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also copy-config(1),list-configs(1)

Name delete-connector-connection-pool – removes the specified connector connection pool

Synopsis

```
delete-connector-connection-pool —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—cascade=false ]
    connector_connection_pool_name
```

Description The `delete-connector-connection-pool` command removes the connector connection pool specified using the operand `connector_connection_pool_name`. This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—help	Displays the help text for the command.
—target	This option is deprecated.
—cascade	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.

Operands

connector_connection_pool_name	The name of the connection pool to be removed.

Examples

EXAMPLE 1 Using the delete-connector-connection-pool command

```
asadmin> delete-connector-connection-pool --user admin
--passwordfile passwords.txt --cascade=false jms/qConnPool
Command delete-connector-connection-pool executed successfully
```

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

Exit Status

0	command executed successfully
1	error in executing the command

See Also create-connector-connection-pool(1), list-connector-connection-pools(1)

Name delete-connector-resource – removes the connector resource with the specified JNDI name

Synopsis

```
delete-connector-resource —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] jndi_name
```

Description This `delete-connector-resource` command removes the connector resource wtih the JNDI name, which is specified by the *jndi_name* operand.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—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, instance.
—poolname	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.
—enabled	This option determines whether the resource is enabled at runtime. The default value is true.
—description	Text providing descriptive details about the connector resource.

Operands

jndi_name	the JNDI name of this connector resource.

Examples

EXAMPLE 1 Using the delete-connector-resource command

```
asadmin> delete-connector-resource --target server
jms/qConnFactory --passwordfile file1
Command delete-connector-resource executed successfuly
```

Where jms/qConnFactory is the connector resource that is removed.

Exit Status

0	command executed successfully
1	error in executing the command

See Also create-connector-resource(1), list-connector-resources(1)

Name delete-connector-security-map – deletes a security map for the specified connector connection pool

Synopsis

```
delete-connector-security-map —user admin_user [—passwordfile filename]
[—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
[—interactive=true] [—help] —poolname connector_connection_pool_name
security_map_name
```

Description Use this command to delete a security map for the specified connector connection pool.

For this command to succeed, you must have first created a connector connection pool using the `create-connector-connection-pool` command.

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.

This command is supported in remote mode only.

Options 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.

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.

	`–p ––port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
	`–s ––secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––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.
Operands	*security_map_name*	name of the security map to be deleted.

Examples **EXAMPLE 1** Using `delete-connector-security-map`

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

```
asadmin> delete-connector-security-map --user admin
--passwordfile pwd_file.txt --poolname connector-pool1 securityMap1
Command delete-connector-security-map executed successfully
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-connector-security-map(1)`, `list-connector-security-maps(1)`, `update-connector-security-map(1)`

Name delete-custom-resource – removes a custom resource

Synopsis

```
delete-custom-resource —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] jndi_name
```

Description The `delete-custom-resource` command removes a custom resource. This command is supported in remote mode only.

Options

`—u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`—H —host`	The machine name where the domain administration server is running. The default value is localhost.
`—p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`—s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
	––target	Valid in Enterprise Edition only, this command, specifies the location of the custom resources that you are deleting. Valid values are: ■ server, which deletes the resource for the default server instance. This is the default value ■ domain, which deletes the resource for the domain ■ *cluster_name*, which deletes the resource for every server instance in the cluster ■ *instance_name*, which deletes the resource for a particular server instance
Operands	*jndi_name*	the JNDI name of this resource.

Examples **EXAMPLE 1** Using the delete-custom-resource command

```
asadmin> delete-custom-resource --user admin --passwordfile passwords.txt sample_custom_resource
Command delete-custom-resource executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also create-custom-resource(1), list-custom-resources(1)

Name delete-domain – deletes the specified domain

Synopsis

```
delete-domain [—domaindir install_dir/domains] [—terse=false] [—echo=false]
     [—interactive=true] domain_name
```

Description Use the `delete-domain` command to delete the named domain. The domain must already exist and must be stopped.

This command is supported in local mode only.

Options

`—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 *install_dir*`/domains` directory is deleted.
`–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 options are prompted.

Operands

domain_name	The unique name of the domain you wish to delete.

Examples **EXAMPLE 1** Using the delete-domain command

```
asadmin> delete-domain --domaindir /export/domains sampleDomain
Domain sampleDomain deleted.
```

Where: the `sampleDomain` domain is deleted from the `/export/domains` directory.

Exit Status

0	command executed successfully
1	error in executing the command

See Also `create-domain(1)`, `start-domain(1)`, `stop-domain(1)`, `list-domains(1)`

Name delete-file-user – removes the named file user

Synopsis

```
delete-file-user —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target]
    [—authrealmname auth_realm_name] username
```

Description Deletes the entry in the keyfile with the specified username.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––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."
	`––authrealmname`	This is the file where the file users are stored.
Operands	*username*	This is the name of file user to be deleted.

Examples **EXAMPLE 1** Using the delete-file-user command

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

```
asadmin> delete-file-user --user admin1 --password adminadmin1
--host pigeon --port 5001 --username admin1
Command delete-file-user executed successfully
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-file-user(1)`, `list-file-users(1)`, `update-file-user(1)`, `list-file-groups(1)`

Name delete-http-health-checker – deletes the health-checker for a specified load balancer configuration

Synopsis

```
delete-http-health-checker —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—config config_name] target
```

Description This command deletes the health checker from a load balancer configuration.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
	`––config`	The load balancer configuration from which you delete the health-checker.
Operands	*target*	Specifies the target from which you are deleting the health checker. Valid values are: ■ *cluster_name*, which deletes the health checker that was monitoring all instances in the cluster. ■ *instance_name*, which deletes the health checker that was monitoring this standalone instance.

Examples **EXAMPLE 1** Using the delete-http-health-checker command

```
asadmin> delete-http-health-checker --user admin
--passwordfile password.txt --config mycluster-http-lb-config mycluster
Command delete-http-health-checker executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-http-health-checker(1)`

Name delete—http—lb—config – deletes a load balancer configuration

Synopsis

```
delete-http-lb-config —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] config_name
```

Description Use the delete-http-lb-config command to delete a load balancer configuration. The load balancer must not reference any clusters or server instances.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
Operands	*config_name*	The name of the new load balancer configuration to delete. The configuration must not reference any clusters or server instances.

Examples **EXAMPLE 1** Using the delete—http—lb—config command

```
asadmin> delete-http-lb-config --user admin --passwordfile file mylbconfig
Command delete-http-lb-config executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-http-lb-config(1)`, `list-http-lb-configs(1)`

Name delete-http-lb-ref – deletes the cluster or server instance from a load balancer configuration

Synopsis

```
delete-http-lb-ref —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] —config config_name target
```

Description Use the delete-http-lb-ref command to remove a reference to a cluster or server instance from a load balancer configuration. So that you do not interrupt user requests, make sure the standalone server instance or all server instances in the cluster are disabled before you remove them from the load balancer configuration.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
	—config	Specifies which load balancer configuration to delete cluster and server instance references from.
Operands	*target*	Specifies which cluster or instance to remove from the load balancer. Valid values are: ■ *cluster_name*, which specifies that requests for this cluster will no longer be handled by the load balancer. ■ *instance_name*, which specifies that requests for this standalone instance will no longer be handled by the load balancer.

Examples **EXAMPLE 1** Using the delete-http-lb-ref command

```
asadmin> delete-http-lb-ref --user admin --passwordfile file
--config mycluster-http-lb-config cluster2
Command delete-http-lb-ref executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-http-lb-ref(1)` `disable-http-lb-server(1)`

Name delete-http-listener – removes an HTTP listener

Synopsis

```
delete-http-listener —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target server] listener_id
```

Description The `delete-http-listener` command removes the specified HTTP listener. This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
	`––target`	In Enterprise Edition, specifies the target from which you are deleting the HTTP listener. Valid values are ■ `server`, which deletes the listener from the default server instance `server` and is the default value ■ *configuration_name*, which deletes the listener from the named configuration ■ *cluster_name*, which deletes the listener from every server instance in the cluster ■ *instance_name*, which deletes the listener from a particular server instance
Operands	*listener_id*	The unique identifier for the HTTP listener to be deleted.

Examples **EXAMPLE 1** Using the delete-http-listener command

The following command deletes the HTTP listener named `sampleListener`:

```
asadmin> delete-http-listener --user admin1
--passwordfile passwords.txt --host pigeon --port 5001 sampleListener
Command delete-http-listener executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-http-listener(1)`, `list-http-listeners(1)`

Name delete-iiop-listener – removes an IIOP listener

Synopsis

```
delete-iiop-listener —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target server] listener_id
```

Description The `delete-iiop-listener` command removes the specified IIOP listener. This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––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 ■ `server`, which deletes the listener from the default server instance `server` and is the default value ■ *configuration_name*, which deletes the listener from the named configuration ■ *cluster_name*, which deletes the listener from every server instance in the cluster ■ *instance_name*, which deletes the listener from a particular server instance
Operands	*listener_id*	The unique identifier for the IIOP listener to be deleted.

Examples **EXAMPLE 1** Using the delete-iiop-listener command

The following command deletes the IIOP listener named `sample_iiop_listener`:

```
asadmin> delete-iiop-listener --user admin
--passwordfile passwords.txt --host fuyako --port 7070 sample_iiop_listener
Command delete-iiop-listener executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-iiop-listener(1)`, `list-iiop-listeners(1)`

Name delete-instance – deletes the instance that is not running

Synopsis

```
delete-instance —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] instance_name
```

Description Use the `delete-instance` command to delete a server instance. The `delete-instance` command can be run both locally and remotely. If a standalone instance is deleted (i.e. the instance's configuration name is *server–name*–config and no other clusters or unclustered instances refer to this configuration), its standalone configuration will be automatically deleted as well.

The Node Agent need not be running (or even installed or created) to delete a server instance. However, if the Node Agent is running, the command will delete the instance. If the Node Agent is not running, it will delete the instance the next time it is started. If a standalone instance is deleted, that is, the instance's configuration name is `server–name-config` and no other clusters or unclustered instances refer to this configuration, then its standalone configuration will be automatically deleted as well.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.

	–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
Operands	*instance_name*	name of the instance to be deleted.

Examples

EXAMPLE 1 Using `delete-instance` in `local` mode

```
asadmin> delete-instance --user admin1 --passwordfile passwords.txt instance1
Command delete-instance executed successfully
```

Where: `instance1` is deleted on the local machine.

EXAMPLE 2 Using `delete-instance` in remote mode

```
asadmin> delete-instance --user admin --passwordfile passwords.txt
--host pigeon --port 4849 instance2
Command delete-instance executed successfully
```

Where: `instance2` is deleted on the remote machine.

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-instance(1)`, `start-instance(1)`, `stop-instance(1)`

Name delete-javamail-resource – removes a JavaMail session resource

Synopsis

```
delete-javamail-resource —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] jndi_name
```

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 administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
	—target	In Enterprise Edition, specifies the target from which you are deleting the JavaMail session resource. Valid values are ■ `server`, which deletes the resource from the default server instance `server` and is the default value ■ `domain`, which deletes the resource from the domain ■ *cluster_name*, which deletes the resource from every server instance in the cluster ■ *instance_name*, which deletes the resource from a particular server instance
Operands	*jndi_name*	The JNDI name of the JavaMail session resource to be deleted.

Examples **EXAMPLE 1** Using the delete-javamail-resource command

The following command deletes the JavaMail session resource named `mail/MyMailSession`:

```
asadmin> delete-javamail-resource --user admin
--passwordfile passwords.txt --host fuyako --port 7070 mail/MyMailSession
Command delete-javamail-resource executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-javamail-resource(1)`, `list-javamail-resources(1)`

Name delete-jdbc-connection-pool – removes the specified JDBC connection pool

Synopsis

```
delete-jdbc-connection-pool —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—cascade=false] connectionpoolid
```

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

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
––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

connectionpoolid	the name of the JDBC resource to be removed.

Examples

EXAMPLE 1 Using the delete-jdbc-connection-pool command

```
asadmin> delete-jdbc-connection-pool --passwordfile file1 --user u1 --cascade=false connectio

Command delete-jdbc-connection-pool executed correctly.
```

Where: asadmin is the command prompt and connection_pool_01 is the connection pool to be removed.

Exit Status

0	command executed successfully
1	error in executing the command

See Also `create-jdbc-connection-pool(1)`,`list-jdbc-connection-pools(1)`

Name delete-jdbc-resource – removes a JDBC resource with the specified JNDI name

Synopsis

```
delete-jdbc-resource —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] jndi_name
```

Description The `delete-jdbc-resource` comand removes a JDBC resource. This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—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

jndi_name	the JNDI name of this JDBC resource to be removed.

Examples

EXAMPLE 1 Using the delete-jdbc-resource command

```
asadmin> delete-jdbc-resource --passwordfile pass1 --user u1 --target plum test_jdbc_resource
Command delete-jdbc-resource executed successfully.
```

Where asadmin is the command prompt and test_jdbc_resource is the name of the JDBC resource that is removed.

Exit Status

0	command executed successfully
1	error in executing the command

See Also `create-jdbc-resource(1)`, `list-jdbc-resources(1)`

Name delete-jmsdest – removes a physical destination

Synopsis

```
delete-jmsdest —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] —desttype type dest_name
```

Description The `delete-jmsdest` command removes the specified physical destination. This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	––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 `delete-jmsdest` 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 ■ `server`, which deletes the physical destination from the default server instance `server` and is the default value ■ *configuration_name*, which deletes the physical destination from the named configuration ■ *cluster_name*, which deletes the physical destination from every server instance in the cluster ■ *instance_name*, which deletes the physical destination from a particular server instance
	–T ––desttype	The type of the JMS destination. Valid values are `topic` and `queue`.
Operands	*dest_name*	The unique identifier of the the JMS destination to be deleted.

Examples **EXAMPLE 1** Using the delete-jmsdest command

The following command deletes the queue named `PhysicalQueue`:

```
asadmin> delete-jmsdest --user admin --passwordfile passwords.txt
--host localhost --port 4848 --desttype queue PhysicalQueue
Command delete-jmsdest executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-jmsdest(1)`, `list-jmsdest(1)`

Name delete-jms-host – removes a JMS host

Synopsis

```
delete-jms-host —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] jms_host_name
```

Description The command removes the specified JMS host. This command is supported in remote mode only.

Deleting the default JMS host, named `default_JMS_host`, is not recommended.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
	—target	In Enterprise Edition, specifies the target from which you are deleting the JMS host. Valid values are ■ `server`, which deletes the JMS host from the default server instance `server` and is the default value ■ *configuration_name*, which deletes the JMS host from the named configuration ■ *cluster_name*, which deletes the JMS host from every server instance in the cluster ■ *instance_name*, which deletes the JMS host from a particular server instance
Operands	*jms_host_name*	The name of the host to be deleted.

Examples **EXAMPLE 1** Using the delete-jms-host command

The following command deletes the JMS host named`MyNewHost`.

```
asadmin> delete-jms-host --user admin1
--passwordfile passwords.txt MyNewHost
Command delete-jms-host executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-jms-host(1)`, `list-jms-hosts(1)`

Name delete-jms-resource – removes a JMS resource

Synopsis

```
delete-jms-resource —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] jndi_name
```

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

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––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 ■ `server`, which deletes the resource from the default server instance `server` and is the default value ■ `domain`, which deletes the resource from the domain ■ *cluster_name*, which deletes the resource from every server instance in the cluster ■ *instance_name*, which deletes the resource from a particular server instance
Operands	*jndi_name*	The JNDI name of the JMS resource to be deleted.

Examples **EXAMPLE 1** Using the delete-jms-resource command

The following command deletes the JMS resource named `jms/Queue`:

```
asadmin> delete-jms-resource --user admin1
--passwordfile passwords.txt --host pigeon --port 5001 jms/Queue
Command delete-jms-resource executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-jms-resource(1)`, `list-jms-resources(1)`

Name delete-jdbc-resource – removes the JNDI resource with the specified JNDI name

Synopsis

```
delete-jndi-resource —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] jndi_name
```

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

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—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	*jndi_name*	the name of the JNDI resource to be removed.

Examples **EXAMPLE 1** Using the delete-jndi-resource command

In Enterprise Edition, you must remove all associations to this resource before you execute this command.

```
asadmin> delete-jndi-resource --passwordfile p1 --user u2 --target plum sample_jndi_resource
Command delete-jndi-resource executed successfully.
```

Where asadmin is the command prompt and sample_jndi_resource is the resource to be removed.

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-jndi-resource(1)`, `list-jndi-resources(1)`

Name delete-jvm-options – removes JVM options from the Java configuration or profiler elements of the `domain.xml` file

Synopsis

```
delete-jvm-options —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] [—profiler =false]
    [(jvm_option_name=jvm_option_value)] [:jvm_option_name=jvm_option_name]
    [*]
```

Description The `delete-jvm-options` command 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 administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—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

jvm_option_name=jvm_option_value	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

EXAMPLE 1 Using the delete-jvm-options command

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.

```
asadmin> delete-jvm-options -e \\-Dtmp=sun
--interactive=true --secure=true --passwordfile /passwords.txt
--terse=false --user admin --target server --host localhost
--echo=true --port 4849 \-Dtmp=sun
Command delete-jvm-options executed successfully
```

Where more than one JVM option is deleted.

```
asadmin> delete-jvm-options \\-Doption1=value1
--passwordfile /passwords.txt --user admin --target server
--host localhost --port 4849 -Doption1=value1
Command delete-jvm-options executed successfully
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also create-jvm-option(1)

Name delete-lifecycle-module – removes the lifecycle module

Synopsis

```
delete-lifecycle-module —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] module_name
```

Description Removes the lifecycle module. This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––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	*module_name*	This operand is a unique identifier for the deployed server lifecycle event listener module.

Examples **EXAMPLE 1** Using delete-lifecycle-module

```
asadmin> delete-lifecycle-module --user admin --passwordfile adminpassword.txt
--host fuyako --port 7070 customSetup
Command delete-lifecycle-module executed successfully
```

Where: `customSetup` is the lifecycle module deleted.

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-lifecycle-module(1)`, `list-lifecycle-modules(1)`

Name 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`)

Synopsis

```
delete-message-security-provider —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target]
    —layer message_layer provider_name
```

Description 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.

If the message-layer (`message-security-config` attribute) does not exist, it is created, and then the `provider-config` is created under it.

This command is supported in remote mode only.

Options 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.

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.

`–p ––port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s ––secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
`––help`	Displays the help text for the command.
`––target`	In Enterprise Edition, specifies the target to which you are deploying. Valid values are ■ `server`, which deploys the component to the default server instance `server` and is the default value ■ `domain`, which deploys the component to the domain. ■ *cluster_name*, which deploys the component to every server instance in the cluster. ■ *instance_name*, which deploys the component to a particular sever instance.
`––layer`	The message-layer from which the provider has to be deleted. The default value is SOAP.

Operands

provider_name	The name of the provider used to reference the `provider-config` element.

Examples

EXAMPLE 1 Using delete-message-security-provider

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

```
asadmin> delete-message-security-provider --user admin
--layer SOAP mySecurityProvider
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `create-message-security-provider(1)`, `list-message-security-providers(1)`

Name delete-node-agent – deletes the node agent and its associated directory structure

Synopsis

```
delete-node-agent [—terse=false] [—echo=false] [—interactive=true]
      [—agentdir nodeagent_path] nodeagent_name
```

Description Use the `delete-node-agent` command to delete the named node agent and its directory structure. The node agent must be stopped and have no associated server instances. After successful execution of the command, run `delete-node-agent-config` to remove the node agent from `domain.xml`.

Options

`–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.
`—agentdir`	Like a Domain Administration Server (DAS), each node agent resides in a top level directory named *agentdir*`/`*nodeagent_name*. If specified, the path must be accessible in the filesystem. If not specified, the default directory *install_dir*`/nodeagents` is used.

Operands

nodeagent_name	This is the name of the node agent to be deleted.

Examples

EXAMPLE 1 Using the delete-node-agent command

The following example deletes node agent `nodeagent1` residing in the default *install_dir*`/nodeagents` directory.

```
asadmin>delete-node-agent nodeagent1
Command delete-node-agent executed successfully.
```

The node agent and its directory structure is deleted. However, `nodeagent1` references still exist in `domain.xml`. Use the following command to complete the removal process:

```
asadmin>delete-node-agent-config --user admin1 --passwordfile filename nodeagent1
Command delete-node-agent-config executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `create-node-agent(1)`, `list-node-agents(1)`, `start-node-agent(1)`, `stop-node-agent(1)`

Name delete-node-agent-config – removes a node agent configuration

Synopsis

```
delete-node-agent-config —user admin_name [—passwordfile filename]
    [—host localhost] [—port port_number] [—secure=false] [—terse=false]
    [—echo=false] [—interactive=true] nodeagent_name
```

Description This command removes the specified node agent configuration from the `domain.xml` file, at which point the node agent directory structure can also be removed (using the `delete-node-agent` command).

Important: The specified node agent must have no server instances running. This means all the agent's instances must be deleted (using `delete-instance`) before executing `delete-node-agent-config`.

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 administration 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 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.
–p —port	The port number of the domain application server listening for administration requests.
–s —secure	If set to true, this command 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. The default is false.
	–e —echo	Setting this option to true will echo the command line statement on the standard output. The default is false.
	–I —interactive	If this option is set to true (default), only the required password options are prompted.
Operands	*nodeagent_name*	The name of the node must be unique on the machine. Typically, the nodeagent_name is the host name of the machine where the node agent will reside.

Examples **EXAMPLE 1** Using the delete-node-agent-config command

The following example deletes the node agent config for `nodeagent1`.

```
asadmin> delete-node-agent-config --user admin1 --passwordfile filename nodeagent1
Command delete-node-agent-config executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-node-agent-config(1)`;`delete-instance(1)`

Name delete-password-alias – deletes a password alias

Synopsis

```
delete-password-alias —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] aliasname
```

Description This command deletes a password alias.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
Operands	aliasname	This is the name of the substitute password as it appears in domain.xml.

Examples **EXAMPLE 1** Using delete-password-alias command

```
asadmin>delete-password-alias --user admin
--passwordfile password.txt jmspassword-alias
```

Command delete-password-alias executed successfully

Exit Status	0	command executed successfully
	1	error in executing the command

See Also create-password-alias(1), list-password-aliases(1), update-password-alias(1)

Name delete-persistence-resource – removes a persistence resource

Synopsis

```
delete-persistence-resource —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] jndi_name
```

Description Removes a persistence resource. This command is supported in remote mode only. When you delete a persistence resource, the command also removes the jdbc resource created using the `create-persistence-resource`command.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—help	Displays the help text for the command.
—target	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 ■ `server`, which deploys the component to the default server instance `server` and is the default value ■ `domain`, which deploys the component to the domain. ■ *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

jndi_name	Specifies the JNDI name of the persistence resource.

Examples

EXAMPLE 1 Using delete-persistence-resource

```
asadmin> delete-persistence-resource --user admin --passwordfile secret.txt
--host pigeon --port 5001 sample_persistence_resource
Command delete-persistence-resource executed successfully
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `create-persistence-resource(1)`, `list-persistence-resources(1)`

Name delete-profiler – deletes the profiler element

Synopsis

```
delete-profiler —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target_name]
```

Description Deletes the profiler element. A server instance is tied to a particular profiler by the profiler element in the Java configuration. Changing a profiler requires you to restart the server.

This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
`––help`	Displays the help text for the command.
`––target`	In Enterprise Edition, specifies the target profiler element which you are deleting. Valid values are ■ `server`, deletes the profiler element for the default server instance `server` and is the default value ■ *configuration_name*, deletes the profiler element for the named configuration ■ *cluster_name*, deletes the profiler element for every server instance in the cluster ■ *instance_name*, deletes the profiler element for a particular server instance

Examples **EXAMPLE 1** Using delete-profiler

```
asadmin> delete-profiler --user admin --passwordfile password.txt
--host localhost --port 4848
Command delete-profiler executed successfully
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `create-profiler(1)`

Name delete-resource-adapter-config – deletes the configuration information created in `domain.xml` for the connector module

Synopsis

```
delete-resource-adapter-config —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] raName
```

Description This command deletes the resource adapter javabean.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
	—target	This option is deprecated.
Operands	*raname*	This value is kept in the `resource-adapter-name` in the `domain.xml` file.

Examples **EXAMPLE 1** Using `delete-resource-adapter-config`

```
asadmin> delete-resource-adapter-config --user admin1 --passwordfile pfile1
ra1
Command delete-resource-adapter-config executed successfully
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-resource-adapter-config(1)`, `list-resource-adapter-configs(1)`

Name delete-resource-ref – removes a reference to a resource

Synopsis

```
delete-resource-ref —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] reference_name
```

Description The `delete-resource-ref` command removes a reference from a cluster or an unclustered server instance to a resource (for example, a JDBC resource). This effectively results in the removal of the resource from the JNDI tree of the targeted instance or cluster.

The target instance or instances making up the cluster need not be running or available for this command to succeed. If one or more instances are not available, they will no longer load the resource in the JNDI tree the next time they start.

Removal of the reference does not result in removal of the resource from the domain. The resource is removed only by the `delete` command for that resource (for example, `delete-jdbc-resource`).

This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.

	–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
	–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
	—target	Specifies the target from which you are removing the resource reference. Valid values are ■ `server`, which removes the resource reference from the default server instance `server` and is the default value ■ *cluster_name*, which removes the resource reference from every server instance in the cluster ■ *instance_name*, which removes the resource reference from the named unclustered server instance
Operands	*reference_name*	The name or JNDI name of the resource.

Examples **EXAMPLE 1** Using the delete-resource-ref command

The following command removes a reference to the JMS destination resource `jms/Topic` on the unclustered server instance `NewServer`.

```
asadmin> delete-resource-ref --user admin2
--passwordfile passwords.txt --target NewServer jms/Topic
Command delete-resource-ref executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-resource-ref(1)`, `list-resource-refs(1)`

Name delete-ssl – deletes the SSL element in the selected HTTP listener, IIOP listener, or IIOP service

Synopsis

```
delete-ssl —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target] —type listener_or_service_type
    listener_id
```

Description Deletes the SSL element in the selected HTTP listener, IIOP listener, or IIOP service.

The *listener_id* is not required if the `--type` is *iiop-service*.

This command is supported in remote mode only.

Options 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.

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
	`––target`	In Enterprise Edition, specifies the target on which you are configuring the ssl element. The following values are valid: ■ `server`, the server in which the iiop-service or HTTP/IIOP listener is to be unconfigured for SSL. ■ *config*, the configuration that contains the HTTP/IIOP listener or iiop-service for which SSL is to be unconfigured. ■ *cluster*, the cluster in which the HTTP/IIOP 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. ■ *instance*, the instance in which the HTTP/IIOP listener or iiop-service is to be unconfigured for SSL.
	`––type`	The type of service or listener for which the SSL is created. The type can be *http-listener*, *iiop-listener*, or *iiop-service*.
Operands	*listener_id*	The ID of the listener from which the SSL element is to be deleted. The *listener_id* operand is not required if the `--type` is *iiop-service*.

Examples **EXAMPLE 1** Using delete-ssl

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

```
asadmin> delete-ssl --user admin
--host fuyako --port 7070 --passwordfile adminpassword.txt --type http-listener
http-listener-1
Command delete-ssl executed successfully.
```

Exit Status	0	command executed successfully

1	error in executing the command

See Also `create-ssl(1)`

Name delete-system-property – removes one system property of the domain, configuration, cluster, or server instance, at a time

Synopsis

```
delete-system-property —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target_name] [property_name]
```

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 overriden through a system property of the corresponding name. This command deletes system properties of a domain, configuration, cluster, or server instance.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—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	*property_name*	The name of the system property to remove.

Examples **EXAMPLE 1** Using delete-system-properties

```
asadmin> delete-system-property --user admin --passwordfile password.txt
--host localhost --port 4849 --target mycluster http-listener-port
Command delete-system-property executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-system-properties(1)`, `list-system-properties(1)`

Name delete-threadpool – removes the named threadpool

Synopsis

```
delete-threadpool ––user admin_user [––passwordfile filename] [––host localhost]
    [––port 4849] [––secure|–s] [––terse=false] [––echo=false]
    [––interactive=true] [––help] [––target target_name]
    [––maxthreadpoolsize max_thread_pool_size]
    [––minthreadpoolsize min_thread_pool_size]
    [––idletimeout idle_thread_timeout_in_seconds]
    [––workqueues number_work_queues] threadpool_id
```

Description Removes the threadpool with the named ID. This command is supported in remote mode only.

Options

–u ––user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H ––host	The machine name where the domain administration server is running. The default value is localhost.
–p ––port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s ––secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
`––help`	Displays the help text for the command.
`––target`	This option specifies the target being operated on. Valid values are: ■ `server`, which deletes the threadpool for the default server instance `server` and is the default value ■ *configuration_name*, which deletes the threadpool for the named configuration ■ *cluster_name*, which deletes the threadpool for every server instance in the cluster ■ *instance_name*, which deletes the threadpool for a particular server instance This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.
`––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

threadpool_id	an ID for the work queue; for example, thread-pool-1, thread-pool-2, etc.

Examples **EXAMPLE 1** Using delete-threadpool

```
asadmin> delete-threadpool --user admin1 --passwordfile password.txt threadpool-1
Command delete-threadpool executed successfully
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `create-threadpool(1)`, `list-threadpools(1)`

Name delete-virtual-server – removes a virtual server

Synopsis

```
delete-virtual-server —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target server] virtual_server_id
```

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

`—u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`—H —host`	The machine name where the domain administration server is running. The default value is localhost.
`—p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`—s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—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 ■ server, which deletes the virtual server from the default server instance server and is the default value ■ *configuration_name*, which deletes the virtual server from the named configuration ■ *cluster_name*, which deletes the virtual server from every server instance in the cluster ■ *instance_name*, which deletes the virtual server from a particular server instance
Operands	*virtual_server_id*	The unique identifier for the virtual server to be deleted.

Examples **EXAMPLE 1** Using the delete-virtual-server command

The following command deletes the virtual server named sample_vs1:

```
asadmin> delete-virtual-server --user admin1
--passwordfile passwords.txt --host pigeon --port 5001 sample_vs1
Command delete-virtual-server executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also create-virtual-server(1), list-virtual-servers(1)

Name deploy – deploys the specified component

Synopsis

```
deploy —user admin_user [—passwordfile filename] [—host localhost]
     [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
     [—interactive=true] [—help] [—virtualservers virtual_servers]
     [—contextroot context_root] [—force=true] [—precompilejsp=false]
     [—verify=false] [—name component_name] [—upload=true]
     [—retrieve local_dirpath] [—dbvendorname dbvendorname]
     [—createtables=true|false | —dropandcreatetables=true|false ]
     [—uniquetablenames=true|false] [—enabled=true]
     [—deploymentplan deployment_plan] [—availabilityenabled=false]
     [—generatermistubs=false] [—target target] filepath
```

Description Deploys an EJB, web, connector, or application. If the component is already deployed or already exists, it is forcefully redeployed if the —`force` option is set to `true`.

The —`createtables` and —`dropandcreatetables` options are booleans and therefore can take the values of *true* or *false*. These options are only used during deployment of CMP beans that have not been mapped to a database (i.e., no `sun-cmp-mappings.xml` descriptor is provided in the module's `META-INF` directory). They are ignored otherwise.

The —`createtables` and —`dropandcreatetables` 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.

This command is supported in remote mode only.

Options

–u —`user`	The authorized domain administration 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 administration 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

	AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—help	Displays the help text for the command.
—virtualservers	One or more virtual server IDs. Multiple IDs are separated by commas.
—contextroot	Valid only if the archive is a web module. It is ignored for other archive types; defaults to filename without extension.
—force	If set to true, makes sure the component is redeployed even if the specified component has already been deployed or already exists. The default is true.
—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.

—verify	If set to true, the syntax and semantics of the deployment descriptor is verified.
—name	Name of the deployable component.
—upload	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.
—retrieve	Retrieves the client stub JAR file from the server machine to the local directory.
—dbvendorname	Specifies the name of the database vendor for which tables are created. Supported values include `db2`, `mssql`, `oracle`, `derby`, `javadb`, `pointbase`, and `sybase`, case-insensitive. If not specified, the value of the `database-vendor-name` attribute in `sun-ejb-jar.xml` is used. If no value is specified, a connection is made to the resource specified by the `jndi-name` subelement of the `cmp-resource` element in the `sun-ejb-jar.xml` file, and the database vendor name is read. If the connection cannot be established, or if the value is not recognized, SQL-92 compliance is presumed.
—createtables	Creates tables at deployment of an application with unmapped CMP beans. Default is the `create-tables-at-deploy` entry in the `cmp-resource` element of the `sun-ejb-jar.xml` file.
—dropandcreatetables	If set to true, when the component is redeployed, the tables created by the previous deployment are dropped before creating the new tables. Applies to already deployed applications with unmapped CMP beans. If not set to true, the tables are dropped if the `drop-tables-at-undeploy` entry in the `cmp-resource` element of the `sun-ejb-jar.xml` file is set to true. The new tables are created if the

	`create-tables-at-deploy` entry in the `cmp-resource` element of the `sun-ejb-jar.xml` file is set to true.
`—uniquetablenames`	Guarantees unique table names for all the beans and results in a hashcode added to the table names. This is useful if you have an application with case-sensitive bean names.
`—enabled`	If set to true (default), allows users to access the application. If set to false, users will not be able to access the application. 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.
`—deploymentplan`	Takes the deployment plan, which is a JAR containing Sun-specific descriptors, and deploys it. This should be passed along when deploying a pure EAR file. A pure EAR file is an EAR without Sun-specific descriptors.
`—generatermistubs`	If set to true, static RMI-IIOP stubs are generated and put into the `client.jar`. If set to false (default) the stubs are not generated.
`—availabilityenabled`	This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.This option controls whether high-availability is enabled for SFSB checkpointing and potentially passivation. If set to false (default) all SFSB checkpointing is disabled for the specified application or EJB module. If set to true, the specified application or module is enabled for high-availability. Set this option to true only if high availability is configured and enabled at higher levels, such as the server and container levels.
`—target`	This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.Specifies the target to which you are deploying. Valid values are:

- `server`, which deploys the component to the default server instance `server` and is the default value.
- `domain`, which deploys the component to the domain. If `domain` is the target for an initial deployment, the application is deployed to the domain, but no server instances or clusters reference the application. If `domain` is the target for a redeployment (the `—force` option is set to true), and 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 an Enterprise application

This syntax deploys the Enterprise application packaged in the `Cart.ear` file to the default server instance `server`. For Sun Java System Application Server Standard and Enterprise Editions, 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

This syntax deploys the Web application in the `hello.war` file to the default server instance `server`. For Sun Java System Application Server Standard and Enterprise Editions, use the `—target` option to deploy to a different server instance or to a cluster.

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

```
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.

This example uses the —`target` option, available with Sun Java System Application Sever Standard and Enterprise Editions only. To use this example for Platform 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 Standard and Enterprise Editions only. To use this example for Platform 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

```
deploydir —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—virtualservers virtual_servers]
    [—contextroot context_root] [—force=true] [—verify=false]
    [—precompilejsp=false] [—name component_name]
    [—uniquetablenames=true|false] [—dbvendorname dbvendorname]
    [—createtables=false | —dropandcreatetables=false ]
    [—generatermistubs=false] [—availabilityenabled=false] [—target target]
    dirpath
```

Description Deploys the exploded format of the application archives present under the directory provided as the command operand.

Directory deployment is for advanced developers only. Do not use it in production environments. In production environments, use the deploy command. Directory deployment is only supported on localhost, that is, the client and server must reside on the same machine. For this reason, the only values for the —host option are:

- localhost
- The value of the $HOSTNAME environment variable
- The IP address of the machine

If the —uniquetablenames, —createtables, and —dropandcreatetables options are not specified, the entries in the deployment descriptors are used.

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.

This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H ––host`	The machine name where the domain administration server is running. The default value is localhost.
`–p ––port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s ––secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
`––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.

`-—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.
`-—name`	Name of the deployable component.
`-—uniquetablenames`	Guarantees unique table names for all the beans and results in a hashcode added to the table names. This is useful if you have an application with case-sensitive bean names.
`—dbvendorname`	Specifies the name of the database vendor for which tables are created. Supported values include `db2`, `mssql`, `oracle`, `derby`, `javadb`, `pointbase`, and `sybase`, case-insensitive. If not specified, the value of the `database-vendor-name` attribute in `sun-ejb-jar.xml` is used. If no value is specified, a connection is made to the resource specified by the `jndi-name` subelement of the `cmp-resource` element in the `sun-ejb-jar.xml` file, and the database vendor name is read. If the connection cannot be established, or if the value is not recognized, SQL-92 compliance is presumed.
`-—createtables`	Creates tables during deployment for applications using unmapped CMP beans. Default is the corresponding entry in the `cmp-resource` element of the `sun-ejb-jar.xml` file. If not specified, defaults to the entries in the deployment descriptors.
`-—dropandcreatetables`	Drops existing tables and creates tables during deployment for application using unmapped CMP beans. If not specified, the tables are dropped if the `drop-tables-at-undeploy` entry in the `cmp-resource` element of the `sun-ejb-jar.xml` file is set to true. The new tables are created if the `create-tables-at-deploy` entry in the `cmp-resource` element of the `sun-ejb-jar.xml` is set to true. When the component is

		redeployed, the tables created by the previous deployment are dropped before creating the new tables.
	`-—generatermistubs`	if set to true, static RMI-IIOP stubs are generated and put into the `client.jar`. If set to false (default) the stubs are not generated.
	`-—availabilityenabled`	This option is available only in the Sun Java System Application Server Standard and Enterprise Edition. This option controls whether high-availability is enabled for SFSB checkpointing and potentially passivation. If set to false (default) all SFSB checkpointing is disabled for the specified application or EJB module. If set to true, the specified application or module is enabled for high-availability. Set this option to true only if high availability is configured and enabled at higher levels, such as the server and container levels.
	`—target`	This option is available only in the Sun Java System Application Server Standard and Enterprise Edition. Specifies the target to which you are deploying. Valid values are: ■ `server`, which deploys the component to the default server instance `server` and is the default value. ■ `domain`, which deploys the component to the domain.
Operands	*dirpath*	path to the directory containing the exploded format of the deployable archive.

Examples **EXAMPLE 1** Using the deploydir command

The exploded application to be deployed is in the `/home/temp/sampleApp` directory. Since the `force` option is set to true, if an application of that name already exists, the application is redeployed.

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

Exit Status

0	command executed successfully
1	error in executing the command

See Also deploy(1), undeploy(1), enable(1), disable(1), list-components(1)

Name deploytool – launches the deploytool utility to deploy, package, and edit your J2EE applications

Synopsis

```
deploytool [--help] [--userdir user_directory]
     [--configdir configuration_directory--verbose]
```

Description 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.

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.

Options

`--help` displays the arguments for launching the deploytool.

`--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.

- On Solaris, the default directory is at `~/.deploytool`

`--configdir` identifies the configuration directory. The configuration directory is where the `asenv.conf` file is located.

On Solaris, the `asenv.conf` can be found at:

- Bundled installation: `/etc/appserver`
- Unbundled installation: default is `/etc/opt/SUNWappserver` or user specified
- Evaluation installation: cd /etc. Where *AS_SERVER_INSTALL* is the directory where you have installed the Sun Java System Application Server 8.

`--verbose` displays the deploytool log messages on the terminal window in Solaris and command window on windows.

Examples

EXAMPLE 1 Using `deploytool`

```
example% deploytool --userdir /myapplication --config_dir /myconfigdir
```

Where `--userdir` specifies the destination directory, and `-config_dir` identifies the configuration directory.

See Also verifier(1M)

Name disable – disables the component

Synopsis

```
disable —user admin_user [—passwordfile filename] [—host localhost]
     [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
     [—interactive=true] [—help] [—target target_name] component_name
```

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

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
`––help`	Displays the help text for the command.
`––target`	This option specifies the target on which you are disabling the component. Valid values are ■ `server`, which is disabled for the default server instance `server` and is the default value ■ *domain_name*, which disables the named domain ■ *cluster_name*, which is disabled for every server instance in the cluster ■ *instance_name*, which is disabled for a particular server instance This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

Operands

component_name	name of the component to be disabled.

Examples **EXAMPLE 1** Using `disable`

```
asadmin> disable  --user admin1 --passwordfile password.txt sampleApp
Command disable executed successfully
```

Examples

0	command executed successfully
1	error in executing the command

See Also `deploy(1)`, `deploydir(1)`, `undeploy(1)`, `enable(1)`

Name disable-http-lb-application – disables an application managed by a load balancer

Synopsis

```
disable-http-lb-application —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—timeout 30] —name application_name target
```

Description This command disables an application managed by a load balancer. The disabled application goes offline with minimal impact to users. Disabling an application gives a finer granularity of control than disabling a server instance and is most useful when a cluster is hosting multiple independent applications.

If an application is deployed across multiple clusters, use this command to disable it in one cluster while leaving it enabled in others.

If an application is deployed to a single server instance, use this command to disable it in that instance while leaving the instance itself enabled.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
	—timeout	The timeout (in minutes) to wait before disabling the specified application. This time allows for a graceful shutdown of the specified application. The default value is 30 minutes.
	—name	The name of the application to be disabled.
Operands	*target*	This operand specifies the server instance or cluster on which to disable the application. Valid values are: ■ *cluster_name*, which disables the application on all server instances in the cluster. ■ *instance_name*, which disables the application on the standalone server instance.

Examples EXAMPLE 1 Using the disable-http-lb-server command

```
asadmin> disable-http-lb-application --user admin
--passwordfile password.txt --name webapps-simple mycluster
Command disable-http-lb-application executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also enable-http-lb-application(1)

Name disable-http-lb-server – disables a sever or cluster managed by a load balancer

Synopsis

```
disable-http-lb-server —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—timeout 30] target
```

Description This command disables a server or cluster of servers that a load balancer is managing. The disabled server instance or cluster goes offline with a minimum impact to users.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
	`––timeout`	The timeout (in minutes) to wait before disabling the specified target. This time allows for a graceful shutdown of the specified target. The default value is 30 minutes.
Operands	*target*	This operand specifies which server instances and clusters to disable. Valid values are: ■ *cluster_name*, which disables all the server instances in the cluster. ■ *instance_name*, which disables a standalone or clustered server instance.

Examples **EXAMPLE 1** Using the disable-http-lb-server command

```
asadmin> disable-http-lb-server --user admin --passwordfile filename myserver
Command disable-http-lb-server executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-http-lb-ref(1)`, `enable-http-lb-server(1)`

Name display-license – displays the license information

Synopsis

```
display-license —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help]
```

Description `display-license` displays the license information. This command can run both locally and remotely.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—–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)

Name enable – enables the component

Synopsis

```
enable —user admin_user [—passwordfile filename] [—host localhost]
     [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
     [—interactive=true] [—help] [—target target_name] [component_name]
```

Description 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

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—help	Displays the help text for the command.
—target	This option specifies the target on which you are enabling the component. Valid values are: ■ `server`, which enables the default server instance `server` and is the default value ■ *domain_name*, which enables the named domain ■ *cluster_name*, which enables every server instance in the cluster ■ *instance_name*, which enables a particular server instance This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

Operands

component_name	name of the component to be enabled.

Examples

EXAMPLE 1 Using `enable`

```
asadmin> enable --user admin1 --passwordfile password.txt sampleApp
Command enable executed successfully
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `deploy(1)`, `deploydir(1)`, `undeploy(1)`, `disable(1)`

Name enable-http-lb-application – enables a previously-disabled application managed by a load balancer

Synopsis

```
enable-http-lb-application —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] —name application_name target
```

Description This command enables a previously disabled application managed by a load balancer. You can enable the application on all instances in a cluster, or on a single standalone server instance.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
	—name	The name of the application to be enabled.
Operands	*target*	This operand specifies on which server instance or cluster to enable the application. Valid values are: ■ *cluster_name*, which enables the application on all server instances in the cluster. ■ *instance_name*, which enables the application in the standalone server instance.

Examples **EXAMPLE 1** Using the enable-http-lb-server command

```
asadmin> enable-http-lb-application --user admin
--passwordfile password.txt --name webapps-simple mycluster
Command enable-http-lb-application executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also disable-http-lb-application(1)

Name enable-http-lb-server – enables a previously disabled sever or cluster managed by a load balancer

Synopsis

```
enable-http-lb-server —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] target
```

Description This command enables a server or cluster of servers that was previously disabled.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
Operands	*target*	This operand specifies which server instances and clusters to enable. Valid values are: ■ *cluster_name*, which enables all the server instances in the cluster. ■ *instance_name*, which enables a standalone or clustered server instance.

Examples **EXAMPLE 1** Using the enable-http-lb-server command

```
asadmin> enable-http-lb-server --user admin --passwordfile filename myserver
Command enable-http-lb-server executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-http-lb-ref(1)`, `disable-http-lb-server(1)`

Name export – marks a variable name for automatic export to the environment of subsequent commands in multimode

Synopsis **export** [*name=value* [*name=value*]*]

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

name=value	variable name and value for automatic export to the environment to be used by subsequent commands.

Examples

EXAMPLE 1 Using `export` to set an environment variable

```
asadmin> export AS_ADMIN_HOST=bluestar
```

In this case, the `AS_ADMIN_HOST` environment variables has been set to *bluestar*.

EXAMPLE 2 Using `export` to set multiple environment variables

```
asadmin> export AS_ADMIN_HOST=bluestar AS_ADMIN_PORT=8000 AS_ADMIN_USER=admin AS_ADMIN_PREFIX=serve
```

In this case, the environment variables have been set to: the host is *bluestar*, the port is *8000*, the administrator user is *admin*, and the prefix is *server1.jms-service*.

EXAMPLE 3 Using export to list environment variables

```
asadmin> export
AS_ADMIN_USER = admin
AS_ADMIN_HOST = bluestar
AS_ADMIN_PREFIX = server1.jms-service
AS_ADMIN_PORT = 8000
```

The `export` with no input lists the set environment variables.

Exit Status

0	command executed successfully
1	error in executing the command

See Also `unset(1)`, `multimode(1)`

Name export-http-lb-config – exports the load balancer configuration to a file that can be used by the load balancer

Synopsis

```
export-htp-lb-config —user admin_user [—passwordfile filename]
     [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
     [—interactive=true] [—help] —config config_name [file_name]
```

Description Use the export-http-lb-config command to export a load balancer configuration into a file that the load balancer plug-in can use. The default file name is `loadbalancer.xml`, but you can specify a different name. Once exported, you manually copy the exported file to the load balancer plug-in location before configuration changes are applied.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
	`––config`	Specifies which load balancer configuration to export.
Operands	*file_name*	Specifies the file name and location of the exported configuration. If you specify a directory (relative or absolute) but not a file name, the file named `loadbalancer.xml.`*load_balancer_config_name* is created in the specified directory. On Microsoft Windows systems the path must be in quotes. If you specify a file name in a relative or absolute path, the file is created with the name you specify in the directory you specify. If you specify a file name but do not specify a directory, the file is created with that name in the current working directory. If you do not specify this operand, the default value is a file named `loadbalancer.xml.`*load_balancer_config_name* created in the *app_sever_install*`/domains/`*domain_name*`/generated` directory.

Examples **EXAMPLE 1** Using the export-http-lb-config command on UNIX

The following example exports the load balancing configuration `mycluster-http-lb-config` to a file named `loadbalancer.xml` in the `/Sun/AppServer` directory .

```
asadmin> export-http-lb-config --user admin --passwordfile file
--config mycluster-http-lb-config Sun/AppServer/loadbalancer.xml
Command export-http-lb-config executed successfully.
```

EXAMPLE 2 Using the export-http-lb-config command on the Microsoft Windows platform

The following example exports the load balancing configuration `mycluster-http-lb-config` to a file named `loadbalancer.xml` in the `C:\Sun\AppServer` directory on a Microsoft Windows system.

EXAMPLE 2 Using the export-http-lb-config command on the Microsoft Windows platform *(Continued)*

```
asadmin> export-http-lb-config --user admin --passwordfile file
--config mycluster-http-lb-config "C:\Sun\AppServer\loadbalancer.xml"
Command export-http-lb-config executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `create-http-lb-config(1)`, `list-http-lb-configs(1)`

Name freeze-transaction-service – freezes the transaction subsystem

Synopsis

```
freeze-transaction-service —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target]
```

Description 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.

This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
Operands	*target*	This operand specifies the target on which you are freezing the transaction service. Valid values are: ■ `server`, which freezes the transaction service for the default server instance `server` and is the default value ■ *configuration_name*, which freezes the transaction service for the named configuration ■ *cluster_name*, which freezes the transaction service for every server instance in the cluster ■ *instance_name*, which freezes the transaction service for a particular server instance

Examples **EXAMPLE 1** Using freeze-transaction-service

```
asadmin> freeze-transaction-service --user admin --passwordfile password.txt --target server
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `unfreeze-transaction-service(1)`, `rollback-transaction(1)list-transaction-id(1)`

Name get – gets the values of the monitorable or configurable attributes

Synopsis **get** —user *admin_user* [—passwordfile *filename*] [—host *localhost*] [—port *4849*] [—secure|–s] [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—help] [—monitor=*[true|false]*] *(dotted_attribute_name)+*

Description Gets the names and values of attributes. If the `--monitor` option is set to true, the monitorable attributes are returned. If the `--monitor` option is set to false, the configurable attribute values are returned. On UNIX platforms, if the shell treats the wildcard (*) as a special character, enclose the dotted name in a double quotes ("*dotted_name*").

The `asadmin get`, `set` and `list` commands work in tandem to provide a navigation mechanism for the Application Server's abstract hierarchy. There are two hierarchies: `configuration` and `monitoring` and these commands operate on both. The `list` command provides the fully qualified dotted names of the management components that have read-only or modifiable attributes. The `configuration` hierarchy provides attributes that are modifiable; whereas the attributes of management components from monitoring hierarchy are purely read-only. The `configuration` hierarchy is loosely based on the domain's schema document; whereas the `monitoring` hierarchy is a little different. Use the `list` command to reach a particular management component in the desired hierarchy. Then, invoke the `get` and `set` commands to get the names and values or set the values of the attributes of the management component at hand. Use the wildcard (*) option to fetch all matches in a given fully qualified dotted name. See the examples for further clarification of the possible navigation of the hierarchies and management components.

An application server dotted name uses the "`.`" (period) as a delimiter to separate the parts of a complete name. This is similar to how the "`/`" character is used to delimit the levels in the absolute path name of a file in the UNIX file system. The following rules apply while forming the dotted names accepted by the `get`, `set` and `list` commands. Note that a specific command has some additional semantics applied.

- A `.` (period) always separates two sequential parts of the name.
- A part of the name usually identifies an application server subsystem and/or its specific instance. For example: web-container, log-service, thread-pool-1 etc.
- If any part of the name itself contains a `.` (period), then it must be escaped with a leading `\` (backslash) so that the "`.`" does not act like a delimiter.
- An * (asterisk) can be used anywhere in the dotted name and it acts like the wildcard character in regular expressions. Additionally, an * can collapse all the parts of the dotted name. Long dotted name like "`this.is.really.long.hierarchy`" can be abbreviated to "`th*.hierarchy`". But note that the `.` always delimits the parts of the name.
- The top level switch for any dotted name is `-–monitor` or `–m` that is separately specified on a given command line. The presence or lack of this switch implies the selection of one of the two hierarchies for appserver management: monitoring and configuration.

- If you happen to know the exact complete dotted name without any wildcard character, then list and get/set have a little difference in their semantics:
  - The `list` command treats this complete dotted name as the complete name of a parent node in the abstract hierarchy. Upon providing this name to `list` command, it simply returns the names of the immediate children at that level. For example, `list server.applications.web-module` will list all the web modules deployed to the domain or the default server.
  - The `get` and `set` commands treat this complete dotted name as the fully qualified name of the attribute of a node (whose dotted name itself is the name that you get when you remove the last part of this dotted name) and it gets/sets the value of that attribute. This is true if such an attribute exists. You will never start with this case because in order to find out the names of attributes of a particular node in the hierarchy, you must use the wildcard character *. For example, `server.applications.web-module.JSPWiki.context-root` will return the context-root of the web-application deployed to the domain or default server.
- If you are using the Enterprise Edition of the Application Server, then "`server`" (usually the first part of the complete dotted name) can be replaced with the name of a particular server instance of interest (e.g., `server1`) and you'll get the information of that server instance, remaining part of the dotted name remaining the same. Note that the dotted names that are available in such other server instances are those from the monitoring hierarchy because these server instances don't have a way to expose the configuration hierarchy.

The `list` command is the progenitor of navigational capabilities of these three commands. If you want to `set` or `get` attributes of a particular application server subsystem, you must know its dotted name. The `list` command is the one which can guide you to find the dotted name of that subsystem. For example, to find out the modified date (attribute) of a particular file in a large file system that starts with `/`. First you must find out the location of that file in the file system, and then look at its attributes. Therefor, two of the first commands to understand the hierarchies in appserver are: `* list "*"` and `* list * -–monitor`. The sorted output of these commands is typically of the following form:

Command	Output
`list *`	■ `default-config` ■ `default-config.admin-service` ■ `default-config.admin-service.das-config` ■ `default-config.admin-service.jmx-connector.system` ■ `default-config.admin-service.jmx-connector.system.ssl` ■ `default-config.availability-service` ■ `default-config.availability-service.jms-availability` ■ `default-config.ejb-container` ■ `. . .` ■ `default-config.http-service.http-listener.http-listener-1` ■ `default-config.http-service.http-listener.http-listener-2` ■ `. . .` ■ `default-config.iiop-service` ■ `. . .` ■ `default-config.java-config` ■ `. . .` ■ `domain` ■ `domain.clusters` ■ `domain.configs` ■ `domain.resources` ■ `domain.resources.jdbc-connection-pool.DerbyPool` ■ `domain.resources.jdbc-connection-pool._CallFlowPool` ■ `domain.resources.jdbc-connection-pool._TimerPool` ■ `. . .` ■ `server` ■ `server-config` ■ `cerver-config.admin-service` ■ `server-config.admin-service.das-config` ■ `server-config.admin-service.jmx-connector.system` ■ `server-config.admin-service.jmx-connector.system.ssl` ■ `server-config-availability-servicce` ■ `server-config.availability-service.jms-availability` ■ `server-config.ejb-container` ■ `. . .` ■ `server.log-service` ■ `server.log-service.module-log-levels` ■ `. . .` ■ `server.session-config` ■ `server.session-config.session-manager` ■ `server.session-config.session-manager.manager-properties` ■ `server.session-config.session-manager.store-properties` ■ `server.session-config.session-properties` ■ `server.thread-pools` ■ `server.thread-pools.thread-pool.thread-pool-1` ■ `server.transaction-service` ■ `server.web-container` ■ `server.web-container-availability`

Command	Output
`list -–monitor *`	■ `server` ■ `server.applications` ■ `server.applications._JWSappclients` ■ `server.applications._JWSappclients.sys\.war` ■ `server.applications.adminapp` ■ `server.applications.admingui` ■ `server.connector-service` ■ `server.http-service` ■ `server.http-service.server` ■ `server.jms-service` ■ `server.jvm` ■ `server.orb` ■ `server.orb.connection-managers` ■ `server.resources` ■ `server.thread-pools`

Consequently, the `list` command is the entry point into the navigation of the application server's s management hierarchies. Take note of the output of the `list` command:

- The output lists one element per line.
- Every element on a line is a complete-dotted-name of a management component that is capable of having attributes. Note that none of these lines show any kind of attributes at all.

The output of the`list` command is a list of dotted names representing individual application server components and subsystems. Every component or subsystem is capable of having zero or more attributes that can be read and modified.

With the`list` command you can drill down through the hierarchy in a particular branch of interest. For example, if you want to find the configuration of the `http-listener` of the domain (the default server, whose ID is "`server`"). Here is how you could proceed on a UNIX terminal:

ID	Command	Output/Comment
1	`list "*" | grep http | grep listener`	1. `default-config.http-service.http-listener.http-listener-1` 2. `default-config.http-service.http-listener.http-listener-2` 3. `server-config.http-service.http-listener.admin-listener` 4. `server-config.http-service.http-listener.http-listener-1` 5. `server-config.http-service.http-listener.http-listener-2` 6. `server-http-service.http-listener.admin-listener` 7. *server.http-service.http-listener.http-listener-1* 8. `server.http-service.http-listener.http-listener-2`
2	To find the listener that corresponds to the default `http-listener` where the web applications in the `domain/server` are deployed: 1. Examine the dotted name starting with item number 7 in above output. 2. Use the `get` command as shown in its usage. For example, `get server.http-service.http-listener.http-listener-1.*` will return all the attributes of the `http-listener` in context.	server.http-service.http-listener.http-listener-1.acceptor-threads = 1server.http-service.http-listener.http-listener-1.address = 0.0.0.0server.http-service.http-listener.http-listener-1.blocking-enabled = falseserver.http-service.http-listener.http-listener-1.default-virtual-server = serverserver.http-service.http-listener.http-listener-1.enabled = trueserver.http-service.http-listener.http-listener-1.external-port =server.http-service.http-listener.http-listener-1.family =inetserver.http-service.http-listener.http-listener-1.id = http-listener-1server.http-service.http-listener.http-listener-1.port = 8080server.http-service.http-listener.http-listener-1.redirect-port =server.http-service.http-listener.http-listener-1.security-enabled = falseserver.http-service.http-listener.http-listener-1.server-name =server.http-service.http-listener.http-listener-1.xpowered-by = true

Making use of both `list` and `get` commands, it is straightforward to reach a particular component of interest.

To get the monitoring information of a particular subsystem you must:

1. Use the `set` command to set an appropriate monitoring level for the component of interest.
2. Obtain the various information about the JVM that the application server domain is running.

ID	Command	Output/Comment
1	`list server* | grep monitoring`	server-config.monitoring-service server-config.monitoring-service.module-monitoring-levels server.monitoring-serviceserver.monitoring-service.module-moni Note that this is the `list` command. It only shows the hierarchy, nothing else. Using the '|' and "grep" narrows down the search effectively. Now, you can choose `server.monitoring-service` to set the attributes of various attributes that can be monitored. This is the configuration data because this setting will be persisted to the server's configuration store.
2	`get server.monitoring-service.*`	You can try the number of attributes that are presently available with monitoring service. Here is the output: No matches resulted from the wildcard expression. This is because this fully dotted name does not have any attributes at all. Logically, you try the next one and that is: `server.monitoring-service.module-monitoring-levels`. Again, use the wildcard character to get ALL the attributes of a particular component.

ID	Command	Output/Comment
3	`get server.monitoring-service.module-monitoring-levels.*`	server.monitoring-service.module-monitoring-levels.connector-connecti = OFF server.monitoring-service.module-monitoring-levels.connector-service = OFF server.monitoring-service.module-monitoring-levels.ejb-container = OFF server.monitoring-service.module-monitoring-levels.http-service = OFF server.monitoring-service.module-monitoring-levels.jdbc-connection-po = OFF server.monitoring-service.module-monitoring-levels.jms-service = OFF server.monitoring-service.module-monitoring-levels.jvm = OFF server.monitoring-service.module-monitoring-levels.orb = OFF server.monitoring-service.module-monitoring-levels.thread-pool = OFF server.monitoring-service.module-monitoring-levels.transaction-service = OFF server.monitoring-service.module-monitoring-levels.web-container = OFF The JVM monitoring is at a level OFF. It must be changed in order to make the JVM monitoring information available. The other valid values for all the monitoring level are: LOW and HIGH. use the `set` command to set the value appropriately.
4	`set server.monitoring-service. module-monitoring-levels.jvm=HIGH` There is no space before or after the = sign.	server.monitoring-service.module-monitoring-levels.jvm = HIGH Now, the JVM information can be obtained using the `get` command and monitoring switch. But remember , when you switch to the monitoring hierarchy, start with the `list` command again.

ID	Command	Output/Comment
5	`list --monitor * | grep jvm`	server.jvm server.jvm.class-loading-system server.jvm.compilation-system server.jvm.garbage-collectors server.jvm.garbage-collectors.Copy server.jvm.garbage-collectors.MarkSweepCompact server.jvm.memory server.jvm.operating-system server.jvm.runtime server.jvm.thread-system server.jvm.thread-system.thread-1 . . . server.jvm.thread-system.thread-793823 server.jvm.thread-system.thread-793824 server.jvm.thread-system.thread-793825 server.jvm.thread-system.thread-793826 server.jvm.thread-system.thread-793827 server.jvm.thread-system.thread-9 The JRE 1.5.0 monitorable components are exposed in an elegant manner. This is what you see when connected by the JConsole. Now, to know more about the class-loading system in the JVM, this is how you'll proceed. Note that now you are interested in the attributes of a particular leaf node. Thus the command is `get` not `list`.

ID	Command	Output/Comment
6	`get --monitor server.jvm.class-loading-system.*`	server.jvm.class-loading-system.dotted-name = server.jvm.class-loading-system server.jvm.class-loading-system.loadedclasscount-count = 7328 server.jvm.class-loading-system.loadedclasscount-description = No Description was available server.jvm.class-loading-system.loadedclasscount-lastsampletime = 1133819508973 server.jvm.class-loading-system.loadedclasscount-name = LoadedClassCount? server.jvm.class-loading-system.loadedclasscount-starttime = 1133819131268 server.jvm.class-loading-system.loadedclasscount-unit = count server.jvm.class-loading-system.totalloadedclasscount-count = 10285 server.jvm.class-loading-system.totalloadedclasscount-description = No Description was available server.jvm.class-loading-system.totalloadedclasscount-lastsampletime = 1133819508972 server.jvm.class-loading-system.totalloadedclasscount-name = TotalLoadedClassCount? server.jvm.class-loading-system.totalloadedclasscount-starttime = 1133819131268 server.jvm.class-loading-system.totalloadedclasscount-unit = count server.jvm.class-loading-system.unloadedclasscount-count = 2957 server.jvm.class-loading-system.unloadedclasscount-description = No Description was available server.jvm.class-loading-system.unloadedclasscount-lastsampletime = 1133819508973 server.jvm.class-loading-system.unloadedclasscount-name = UnloadedClassCount? server.jvm.class-loading-system.unloadedclasscount-starttime = 1133819131268 server.jvm.class-loading-system.unloadedclasscount-unit = count You cansee that 10285 is the total number of classes loaded by the Virtual Machine. Whereas, 2957 is number of classes unloaded, since it was started. ,Similarly, you can explore attributes of the other subsystems as well.

Options

`–u ––user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
	–H —host	The machine name where the domain administration server is running. The default value is localhost.
	–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
	–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—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	*attributename*	Identifies the attribute name in the dotted notation. At least one dotted name attribute is required. The dotted notation is

the syntax used to access attributes of configurable entities. The following format is used for the notation:

```
Configuration: <config name>.<config element
name>.<primary key>.<attribute name> | <instance
name>.<config element name>.<primary
key>.<attribute name>

Resource: <instancename>.<resource name>.<primary
key>.<attribute name> | domain.resources.<resource
name>.<primary key>.<attribute name>
```

Examples

EXAMPLE 1 Using the get command with wildcard

Command	Operation
`get *`	get all values on all dotted name prefixes
`get *.*`	same as `get *`.
`get domain.*`	gets all values on the dotted name "`domain`." Note that this is quite different from "`domain*`".
`get domain*`	gets all values on the dotted nams that begin with "domain". Equivalent to `get domain*.*`.
`get *config*.*.*`	gets all values on the dotted names which match "`*config*.*`"
`get domain.j2ee-applications.*.ejb-module.*.*`	gets all values on all ejb-modules of all applications.
`get *web-modules.*.*`	get all values on all web modules whether in an application or standalone.
`get *.*.*.*`	get all values on all dotted names which have three parts.

EXAMPLE 2 Using get with the monitor option

To get the monitoring data from the domain administration server, the appropriate monitoring level must be set on the appropriate subsystem. Use the `set` command to set the monitoring data level. For example, to set the monitoring level on Web Container on Domain Administration Server (DAS) to HIGH so that the Web Container returns many monitorable attributes and their values:
`server.monitoring-service.module-monitoring-levels.web-container=HIGH`. See the `set` command for further details on setting the monitoring level.

EXAMPLE 2 Using get with the monitor option *(Continued)*

Command	Dotted Name	Output
Top Level		
`get -m`	server.*	No output, but message saying there are no attributes at this node.
Applications Level		
`get -m`	server.applications.* or*applications.*	No output, but message saying there are no attributes at this node.
Applications — Enterprise Applications and Standalone Modules		
`get -m`	server.applications.app1.* or*app1.*	No output, but message saying there are no attributes at this node.
`get -m`	server.applications.app1. ejb-module1_jar.* or *ejb-module1_jar.* or server.applications.ejb-module1_jar.*	No output, but message saying there are no attributes at this node.

EXAMPLE 2 Using get with the monitor option *(Continued)*

Command	Dotted Name	Output
`get -m`	server.applications.app1.ejb-module1_jar.stateful.* Note : where it is a standalone module, the node app1 will not appear.	Attribute CreateCount_Count, Value = xxxx Attribute CreateCount_Description, Value = xxxx Attribute CreateCount_LastSampleTime, Value = xxxx Attribute CreateCount_Name, Value = xxxx Attribute CreateCount_StartTime, Value = xxxx Attribute CreateCount_Unit, Value = xxxx Attribute MethodReadyCount_Current, Value = xxxx Attribute MethodReadyCount_Description, Value = xxxx Attribute MethodReadyCount_HighWaterMark, Value = xxxx Attribute MethodReadyCount_LastSampleTime, Value = xxxx Attribute MethodReadyCount_LowWaterMark, Value = xxxx Attribute MethodReadyCount_Name, Value = xxxx MethodReadyCount_StartTime, Value = xxxx MethodReadyCount_Unit, Value = xxxx Attribute RemoveCount_Count, Value = xxxx Attribute RemoveCount_Description, Value = xxxx Attribute RemoveCount_LastSampleTime, Value = xxxx Attribute RemoveCount_Name, Value = xxxx Attribute RemoveCount_StartTime, Value = xxxx Attribute RemoveCount_Unit, Value = xxxx
`get -m`	server.applications.app1.ejb-module1_jar.stateful.pool Note: Where it is a standalone module, the node app1 will not appear.	List of Attributes and Values corresponding to attributes as defined under EJBPoolStats Statistics.

EXAMPLE 2 Using get with the monitor option *(Continued)*

Command	Dotted Name	Output
`get -m`	server.applications.app1.ejb-module1_jar.bean1.bean-cache.* Note: Where it is a standalone module, the node app1 will not appear.	List of Attributes and Values corresponding to attributes as defined under EJBCacheStats Statistics.
`get -m`	server.applications.app1.ejb-module1_jar.bean1.bean-cachemethod.methodx.* Note: Where it is a standalone module, the node app1 will not appear.	List of Attributes and Values corresponding to attributes as defined under EJBMethodStats Statistics.
`get -m`	server.applications.app1.web-module1_war.*	No output, but message saying there are no attributes at this node.
`get -m`	server.applications.app1.web-module1_war.virtual_server1.*	No output, but message saying there are no attributes at this node.
`get -m`	server.applications.app1.web-module1_war.virtual_server1.servlet1.*	List of Attributes and Values corresponding to ServletStats statistics.
Http-Service Level		
`get -m`	server.http-service.*	No output, but message saying there are no attributes at this node.
`get -m`	server.http-service.virtual-server1	No output, but message saying there are no attributes at this node.
`get -m`	server.http-service.virtual-server1.http-listener1.*	Attributes and Values corresponding to HttpListerneStats Statistics.
Thread-Pools Level		
`get -m`	server.thread-pools.*	No output, but message saying there are no attributes at this node.
`get -m`	server.thread-pools.thread-pool1.*	List of Attributes and Values corresponding to ThreadPoolStats Statistics.
Resources Level		
`get -m`	server.resources.*	No output, but message saying there are no attributes at this node.
`get -m`	server.resources.connection-pool1.*	List of Attributes and Values corresponding to JDBCConnectionPool Stats or ConnectorConnectionPoolStats Statistics as the case may be.
Transaction-Service Level		

EXAMPLE 2 Using get with the monitor option *(Continued)*

Command	Dotted Name	Output
`get -m`	server.transaction-service.*	List of Attributes and Values corresponding to JTAStats Statistics.
ORB Level		
`get -m`	server.orb.*	No output, but message saying there are no attributes at this node.
`get -m`	server.orb.connection-managers.*	No output, but message saying there are no attributes at this node.
`get -m`	server.orb.connection-managers.orbconnmgr1.*	Attributes and values corresponding to OrbConnectionManagerStats Statistics.
JVM Level		

`get -m`	server.jvm.*	Attributes and Values corresponding to JVMStats Statistics.
		For example:
		`server.jvm.HeapSize_Current = 45490176`
		`server.jvm.HeapSize_Description = Describes JvmHeapSize`
		`server.jvm.HeapSize_HighWaterMark = 45490176`
		`server.jvm.HeapSize_LastSampleTime = 1063217002433`
		`server.jvm.HeapSize_LowWaterMark = 0server.jvm.HeapSize_LowerBound = 0`
		`server.jvm.HeapSize_Name = JvmHeapSizeserver.jvm.HeapSize_StartTime = 1063238840055`
		`server.jvm.HeapSize_Unit = bytes`
		`server.jvm.HeapSize_UpperBound = 531628032`
		`server.jvm.UpTime_Count = 1063238840100server.jvm.UpTime_Description =`
		`Describes JvmUpTimeserver.jvm.UpTime_LastSampleTime = 1-63238840070`
		`server.jvm.UpTime_Name = JvmUpTimeserver.jvm.UpTime_StartTime = 1063217002430server.jvm.UpTime_Unit = milliseconds`

Exit Status

0	command executed successfully
1	error in executing the command

See Also set(1), list(1)

Name get-client-stubs – retrieves the client stub JAR

Synopsis

```
get-client-stubs —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target_name]
    [—appname application_name] local_directory_path
```

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. Before executing the `get-client-stubs` command, the application or module should be deployed. The client stubs JAR is useful for running application via the `appclient` utility. This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	––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 ■ `server`, which creates the listener for the default server instance `server` and is the default value ■ *configuration_name*, which creates the listener for the named configuration ■ *cluster_name*, which creates the listener for every server instance in the cluster ■ *instance_name*, which creates the listener for a particular server instance
	`--appname`	name of the application.
Operands	*local_directory_path*	path to the local directory where the client stub should be stored.

Examples **EXAMPLE 1** Using get-client-stubs

```
asadmin> get-client-stubs --user admin --passwordfile password.txt
--host fuyako --port 7070 --appname myapplication /sample/exmple
Command get-client-stubs executed successfully
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `undeploy(1)`

Name hadbm – utility for managing the High Availability Database (HADB)

Synopsis

hadbm *command*
[*–short-option option_argument* | *–short-option=option_argument —long_option=option_argumen*
[*operand*]*

hadbm *command_name* —help |**hadbm help**

Description The hadbm command identifies the operation or task to perform. Commands are case-sensitive. One or more command options can be specified in one of the following formats:

—option=value
—option value
–short-option value

Options, like commands, are case-sensitive. 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 or an equal sign (=). Optional options and operands are identified in enclosed square brackets [ ]. For commands that take a database name operand, if a database is not specified, the default database is used. The default database is hadb.

Commands

addnodes	adds nodes to the named database
clear	reinitializes all the data space on all nodes and starts the database
clearhistory	clears the history files on the database
create	creates a database instance
createdomain	creates a management domain of the listed HADB hosts
delete	removes the database
deletedomain	deletes the HADB management domain
deviceinfo	displays information about disk storage devices on each active data node
disablehost	selectively disables a host in the management domain
extenddomain	extends the current HADB management domain
get	gets the value of the specified configuration parameter
help	displays all the subcommands for the hadbm utility
list	lists all the existing databases
listdomain	lists all hosts defined in the management domain
listpackages	lists the packages registered in the management domain

	reducedomain	removes hosts from the HADB management domain
	refragment	refragments the schema
	registerpackage	registers the HADB packages in the management domain
	resourceinfo	displays database resource information
	restart	restarts the database
	restartnode	restarts the specified node
	set	sets the value of the specified configuration attributes to the identified values
	start	starts the database
	startnode	starts the specified node
	status	shows the state of the database
	stop	gracefully stops the database
	stopnode	gracefully stops the specified node
	unregisterpackage	removes registered HADB packages from the management domain
	version	displays the hadbm version information
Common Options	`-q` —`quiet`	Performs the operation silently without any descriptive messages.
	`-?` —`help`	Displays a brief description of the `hadbm` utility and all the supported commands.
	`-v` —`version`	Displays the version details of the `hadbm` utility.
	–`y` —`yes`	Launches the command in non-interactive mode.
	`-f` —`force`	Launches the command in non-interactive mode, and does not return error if the post condition is already achieved.
	`-e` —`echo`	Displays the commands with all the options and their user-defined values or the default values; then launches the command.

Name hadbm addnodes – adds new nodes to the named database, initializes devices for the new nodes, and refragments the schema

Synopsis

```
hadbm addnodes [—no-refragment] [—spares=spare_count] [—historypath=path]
    [—devicepath=path] [—set=attribute_name_value_list]
    —dbpassword=password | —dbpasswordfile= filename | —adminpassword=password | —admir
    [dbname]
```

Description Use the `hadbm addnodes` command to add new nodes to the named database, initialize the devices for the new nodes, and refragment the schema. The number of spares identified is the number of spares to be alloted from the host list as specified in the `—hosts` option. Hosts must be specified in pairs. All the active nodes in the database should be running when executing the `hadbm addnodes` command (this means the database has at least FaultTolerant or HAFaultTolerant state). If the database is not specified, the default database is used. The database is restarted without loss of service after adding the nodes.

Refragmentation, though time consuming, is needed to store the data on the newly created nodes. You can elect to perform refragmentation during node creation (default). However, if you have chosen `—no-refragment`, you can refragment later by using the `hadbm refragment` command. The database is available during refragmentation.

Data devices must have 50% free space to accomodate the old and new copies of the user data during refragmentation.

Options

`–w —adminpassword`	The actual HADBM administation password.
`–W —adminpasswordfile`	The file containing the HADBM administration password and defined in your environment variables of the Management Agen. The adminstration password is defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–m —agent`	Identifies the URL to the Management Agent(s) (hostlist:port).
`–r —no-fragment`	If this option is specified or set to true, refragmentation is not performed on the database after adding the nodes . If the option is not specified, or set to false (default), the database is refragmented after adding the nodes. All tables are refragmented over all nodes; including the new nodes.
`–s —spares`	Identifies the number of hosts to be used as spares out of the new nodes that are added.
`–t —historypath`	The path for the database history files.

–d —devicepath	The path for the data and log devices. The path to the device must already exist. To set the path differently for each node or device, use the —set option. There are three types of devices: ■ DataDevice ■ NiLogDevice (node internal log device ■ RelalgDevice (relational algebra query device)
–p —dbpassword	The password string for the system user of the database. The minimum length of the password must be 8 characters. You can identify either the database password, or for higher security, the password file where the password is defined.
–P —dbpasswordfile	Identifies the file containing the password to be used for the system user of the database.
–S —set	Identifies the configuration parameters that will be set to the database. Must be specified as a comma-separated list of database configuration attributes in name=value format. Use this option to set a different —devicepath for each node or each device. The syntax for each name=value pair is: Node-*nodenumber*.device-*devicenumber*.DevicePath=path Where: -*devicenumber* is only required if the device is a DataDevice. For example: Node-0.DataDevice-0.DevicePath=/disk0. Any device path that is not set for a particular node or device defaults to the —devicepath value.
–H —hosts	A comma-separated list of new host names for the new nodes in the database. Duplicates are allowed; this creates multiple nodes on the same machine with different port numbers. Keep the mirror nodes on separate DRUs for deployment. One node is created for each comma-separated item in the list. The number of nodes must be even. If the database is already created with double network configuration, the nodes being added should also support that same configuration. They should have two NIC cards and the —hosts option should define the IP addresses for them.
Operands *dbname*	The name of the database. The default database is hadb.

Examples

EXAMPLE 1 Using addnodes

```
hadbm addnodes --dbpasswordfile=/home/hadb/dbpfile
--hosts host8,host9 mydatabase
Nodes successfully added to the database
```

EXAMPLE 2 Using addnodes with spares identified

```
hadbm addnodes --dbpasswordfile=/home/hadb/dbpfile
--spares=2 --hosts=host8,host9 mydatabase
Nodes successfully added to the database
```

EXAMPLE 3 Using addnodes without a password

```
hadbm addnodes --hosts=host7,host8
Please enter password for system user:
Nodes successfully added to the database
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22002	specified database does not exist
22024	host unreachable
22025	hosts not added in pairs
22041	invalid database state
22042	database could not be refragmented (if —`no-fragment` is set to true)
22043	specified number of spares could not be allocated
22044	path on host does not exist
22045	path on host needs write permissions
22046	database state deteriorated
22047	refragmentation cannot be done
220201	database not refragmented (if —`no-fragment` is set to true)

See Also

`hadbm-clear(1)`, `hadbm-delete(1)`, `hadbm-list(1)hadbm-refragment(1)`, `hadbm-restart(1)`, `hadbm-start(1)`, `hadbm-status(1)`, `hadbm-stop(1)`

Name hadbm clear – reinitializes all the dataspace on all nodes and starts the database

Synopsis

```
hadbm clear [—-fast] [—-spares=number_of_spares]
    [—-adminpassword=password | —-adminpasswordfile=filename ]
    [—-dbpassword=password | —-dbpasswordfile= filename] [—-agent=ma_url]
    [dbname]
```

Description Use the `hadbm clear` command to reinitialize all the data devices and start the database. The `hadbm clear` command can also be used in the following situations:

- Restarting the database after a disaster. A disaster refers to double failures, where one or more mirror node pairs are down simultaneously. For example, due to a power failure, machine reboot, or some other unforeseen disaster. The `hadbm status` command will indicate a database that is hit by a disaster as "non-functional".
- The password provided at the time the database was created is lost during clear and the new password given in the `—dbpassword=`*password* option will be used when accessing the database in the future. The cleared database will be in an HA Fault Tolerant or Fault Tolerant state.

In interactive mode, the `hadbm clear` command prompts for a confirmation before clearing the database.

Options

`-F —fast`	Use this option to skip device initialization to save time. Do not use if the disk storage device is corrupted. The data devices must be initialized for the first time after the database is created.
`-s —spares`	If specified, identifies the number of spares. The number must be such that there are at least two active nodes. This number of spares must be even and must be less than or equal to the number of active nodes in the database. If not specified, the original number of spare nodes found in the database instance earlier will be preserved. Spare nodes are option, but having two or more ensures high availability.
`-p —dbpassword`	The password used for the system user of the database. This password must be valid and is expected to be passed in other commands that require data access.
`-P —dbpasswordfile`	Identifies the file containing the password to be used for the system user of the database.
`–w —adminpassword`	The actual HADBM administation password.
`–W —adminpasswordfile`	The file containing the HADBM administration password. The adminstration password is defined in the following

		form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
	–m —agent	Identifies the URL to the Management Agent(s) (hostlist:port).
Operands	*dbname*	The name of the database. The default database is hadb.

Examples

EXAMPLE 1 Using clear with the default database

```
hadbm clear
Type "yes" or "y" to confirm this operation, anything else to cancel: y
Database successfully cleared
```

EXAMPLE 2 Using clear with a database identified

```
hadbm clear mydatabase
This command will clear the database.
Type "yes" or "y" to confirm this operation, anything else to cancel: y
Database successfully cleared
```

Exit Status	0	command executed successfully
	1	error in executing the command
Error Codes	22002	specified database does not exist
	22061	database could not be cleared

See Also hadbm-addnodes(1), hadbm-clearhistory(1), hadbm-delete(1), hadbm-list(1), hadbm-refragment(1), hadbm-restart(1), hadbm-start(1), hadbm-stop(1)

Name hadbm clearhistory – clears the history files on the database

Synopsis

```
hadbm clearhistory [—adminpassword=password | —adminpasswordfile=filename ]
    [—saveto=path] [—agent=ma_url] [dbname]
```

Description Use the `hadbm clearhistory` command to clear the history files on the database. The directory to which the history files are to be saved must exist and must be writeable. The history file of the named database will be truncated. You can verify by checking the size of the history file. The database state remains unchanged. If a database is identified, it should already exist. If a database is not named, the default database history files are cleared. The default database is hadb.

In interactive mode, the `hadbm clearhistory` command prompts for a confirmation before clearing the history.

Options

`-o —saveto`	The path to where the old history files are to be saved.
`–w —adminpassword`	The actual HADBM administation password as defined in the environment variables of the Management Agent.
`–W —adminpasswordfile`	The file containing the HADBM administration password and defined in your environment variables of the Management Agent. The adminstration password should be defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–m —agent`	Identifies the URL to the Management Agent. The default is localhost:1862.

Operands

dbname	The name of the database. The default database is hadb.

Examples

EXAMPLE 1 Using clearhistory with a database identified

```
hadbm clearhistory mydatabase
This command will clear the history file of the database.
Type "yes" or "y" to confirm this operation,
anything else to cancel: y
Database history file successfully cleared
```

EXAMPLE 2 Using clearhistory with the saveto option

```
hadbm clearhistory --saveto=/var/tmp mydatabase
This command will clear the history file of the database.
Type "yes" or "y" to confirm this operation,
```

EXAMPLE 2 Using clearhistory with the saveto option *(Continued)*

```
anything else to cancel: y
Database history file successfully cleared
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22002	specified database does not exist
22111	directory does not exist
22112	specified location is not a directory
22113	directory is not writeable

See Also `hadbm-status(1)`, `hadbm-list(1)`, `hadbm-addnodes(1)`, `hadbm-clear(1)`, `hadbm-refragment(1)`, `hadbm-delete(1)`, `hadbm-start(1)`, `hadbm-restart(1)`, `hadbm-stop(1)`

Name hadbm create – creates a database instance

Synopsis

```
hadbm create [—package=package_name] [—packagepath=path]
     [—historypath=path] [—devicepath=path]
     [—datadevices=number_of_devices_per_node] [—portbase=base_number]
     [—spares=number_of_spares] [—set=attribute_name_value_list]
     [—agent=ma_url] [—no-cleanup] [—no-clear] [—devicesize=size]
     [—dbpassword=password | —dbpasswordfile= filename]
     [—adminpassword=password | —adminpasswordfile=filename | —no-adminauthenticati
     —hosts=host_list [dbname]
```

Description The `hadbm create` command creates the specified database on all the named hosts. The specified database must not already exist on the named hosts. All the paths used for the database must exist and must be writeable on the named hosts. The host list must be greater than one and comtain an even number of hosts. You can specify where to store the data devices, log devices, history files, and configuration files. The password string must be a minimum of eight characters. The system user is assigned the password that is supplied in the `—dbpassword` or `—dbpasswordfile` options. This password is expected to be passed in other commands that require data access.

The number of spares must be an even number and must be less than or equal to the number of hosts given in the host list and at least two active nodes should be present. The number of devices must be between one and eight.

Options

`-k —package` — The name identifying the software package. If the package is not found, a default package is registered.

`-L —packagepath` — Identifies the full path of the HADB software package. This path is only used if the package is not registered in the domain. If the package is already registered, this option is ignored. The default value is the path for the installation of the hadbm client.

`-t —historypath` — The full path to the history files. If the `historypath` option is not specified, the default path is set up by the management agent(s). The management agent uses the entries in the configuration file (`ma.server.dbhistorypath`).

`–d —devicepath` — The path for the data and log devices. The path to the device must already exist. To set the path differently for each node or device, use the `—set` option. There are three types of devices:

- `DataDevice`
- `NiLogDevice` (node internal log device
- `RelalgDevice` (relational algebra query device)

If the `devicepath` option is not specified, the default path is set up by the management agent(s). The management agent uses the entries in the configuration file (`ma.server.dbdevicepath`).

`-a` —`-datadevices` — The number of data devices. The number must be between 1 and 8, on each node.

`-b` —`-portbase` — The port base number used for node 0. The other nodes are then assigned port number bases in steps of 10 from the number specified here.

`-s` —`-spares` — The number of spares. The number must be less than the length of the host list and at least two active nodes should be there.

`–S` —`-set` — Identifies the configuration parameters that will be set to the database. Must be specified as a comma-separated list of database configuration attributes in name=value format.

Use this option to set a different —`devicepath` for each node or each device. The syntax for each name=value pair is:

`Node-`*nodenumber*`.device-`*devicenumber*`.DevicePath=path`

Where: *-devicenumber* is only required if the device is a DataDevice.

For example: `Node-0.DataDevice-0.DevicePath=/disk0`. Any device path that is not set for a particular node or device defaults to the —`devicepath` value.

The following table identifies the configuration attributes available.

TABLE 1 Configuration Attributes

Variable	Type	Default
ConnectionTrace	boolean	false
CoreFile	boolean	false
DataBufferPoolSize	integer	200 MB
DatabaseName	string	hadb
DataDeviceSize	integer	1024 MB
DevicePath	string	n/a

TABLE 1 Configuration Attributes *(Continued)*

Variable	Type	Default
EagerSessionThreshold	integer	50 (% of NumberOfSessions)
EagerSessionTimeout	integer	120 seconds
EventBufferSize	integer	0 MB
HistoryPath	string	n/a
InternalLogBufferSize	integer	12 MB
LogBufferSize	integer	48 MB
MaxTables	integer	1100
NumberOfDatadevices	integer	1
NumberOfLocks	integer	50000
NumberOfSessions	integer	100
PackageName	string	V4.4.1.1
Portbase	integer	15000
RelalgDeviceSize	integer	128 MB
SessionTimeout	string	1800 seconds
StatInterval	integer	600
StartRepairDelay	integer	20 seconds
SQLTraceMode	string	off
SysLogging	boolean	true
SyslogFacility	string	local0
SyslogLevel	string	warning
SyslogPrefix	string	hadb-<db_name>
TakeoverTime	integer	10000 MS

`–m ––agent` Identifies the URL to the Management Agent(s) (hostlist:port).

`––no-cleanup` Use this option to prevent the deletion of files that are normally deleted (such as the history files, devices, and configuration files) if the `create` command fails.

—no-clear	By default the database is initalized and started. However, if this option is set, the database processes will not be started, the devices will not be initialized, and you must use the `clear` command to start the database for the first time.
-z —devicesize	The size of the data devices (specified in MB). This size is applicable on all devices.
-p —dbpassword	The password string for the system user of the database. The minimum length of the password must be 8 characters. You can identify either the database password, or for higher security, the password file where the password is defined.
-P —dbpasswordfile	Identifies the file containing the password to be used for the system user of the database.
–w —adminpassword	The actual HADBM administation password.
–W —adminpasswordfile	The file containing the HADBM administration password. The adminstration password is defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
–U —no-adminauthentication	Using this option eliminates the need of password identification.
-H —hosts	A comma-separated list of all the host names or IP addresses used for all the nodesin the database. An HADB Management Agent must be running on each host. Using the IP address is recommended because there is no dependence on DNS lookups. Hostnames must be absolute. Do not use `localhost` or `127.0.0.1` as a hostname. Configuring an HADB instance with double networks: To make HADB tolerate single network failures, the HADB server machines can be equiped with two NIC cards. The HADB instance must be configured to exploit these cards by specifiying both IP addresses of the NIC cards for each node. The first IP address the HADB considers as "net-0," the second is set to "net-a." The syntax for a two-node configuration is: —`hosts=h0a+h0b,h1a+h1b`. ■ `h0a` is host-0's IP address on net-0 ■ `h0b` is host-0's IP address on net-1 ■ `h1a` is host-1's IP address on net-0 ■ `h1b` is host-1's IP address on net-1

All nodes in a database instance must be connected to both networks. Some nodes can be connected to both networks while others are connected to only one network. The IP address of each NIC card must be on separate IP subnets.

Operands

dbname	The name of the database. The default database is hadb.

Examples

EXAMPLE 1 Using create with two nodes on a single device

The following example creates a database with the default database name `hadb` with two active nodes, and a single data device. The system prompts you for the password twice. All paths are default paths and must be created before initiating this command.

```
hadbm create --devicesize=256 --hosts=host1,host2
Database successfully created and started
```

EXAMPLE 2 Using create with two nodes on multiple devices

The following example creates a database named mydb with two active nodes, two spare nodes, two devices per node, and a specific port base number for some specific path.

```
hadbm create  -H host1,host2 --packagepath=/home/hadb/install
--historypath=/export/home/hadb/history --devicepath =/export/home/hadb/device
--configpath /home/hadb/config --datadevices=2 --portbase=1500
--dbpasswordfile=/home/hadb/dbpfile --spares=2 --devicesize=512
--set "Node-0.DataDevice-0.DevicePath=/disk0 Node-0.DataDevice-0.DevicePath=/disk1" mydb
Database successfully created and started
```

Node 0 gets two data devices: `/disk0/mydb.data.0` and `/disk1/mydb.data1.1`. Since Node 1 is not specified with any specific device path in the —`set` option, and since the —`datadevices` option was set to 2, Node 1 gets both devices on the path given in the —`devicepath` option. The devices for Node 1 are then `/export/home/hadb/device/mydb.data.1` and `/export/home/hadb/device/mydb.data1.1`.

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22021	database exists
22022	specified path does not exist
22023	specified path does not have write permissions
22024	host unreachable
22025	hosts not added in pairs
22026	database name specified is not valid

22027	port base number is not valid
22028	specified number for data devices cannot be supported
22029	specified device size cannot be supported
22030	specified number of spares could not be allocated
22031	attributes are not recognized
22032	password string not valid
22203	database not refragmented (if —`no-fragment` is set to true)

See Also `hadbm-clear(1)`, `hadbm-delete(1)`, `hadbm-list(1)`, `hadbm-start(1)`, `hadbm-restart(1)`, `hadbm-status(1)`, `hadbm-stop(1)`

Name hadbm createdomain – creates a management domain of the listed HADB hosts

Synopsis

```
hadbm createdomain
      [––adminpassword=password | ––adminpasswordfile=filename | ––no-adminauthenticati
      [––agent=ma_url] host_list
```

Description Use the `hadbm createdomain` command to create the HADB management domains. All the hosts that will be part of the desired domain must be included in the hostlist; including the hosts retrieved through the `hadbm listdomain`command.

To form a domain, the hostlist must consist of valid network addresses. After the management domaiin is successfully completed, all the hosts in the domain are enabled and the management agents are ready to manage databases.

The following prerequisites must be met before using the `hadbm createdomain` command:

- HADB management agents are running on the hosts.
- The management agents are not members of an existing domain.
- All the management agents are configured to use the same port.
- All the management agents can reach each other over UDP, TCP, and with IP multicast.

Options

`–w ––adminpassword`	The actual HADBM administation password. Using this option with the `hadbm createdomain` or `hadbm create` command requires that the password is entered each time any `hadbm` command is used. The `adminpassword` is different from the `hadbm dbpassword` command. You must use both passwords when using the following commands: `hadbm create`, `hadbm addnodes`, `hadbm refragment`.
`–W ––adminpasswordfile`	The file containing the HADBM administration password. The adminstration password must be defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–U ––no-adminauthentication`	Using this option eliminates the need of password identification.
`–m ––agent`	Identifies the URL to the Management Agent. The default is localhost:1862.

Operands

host_list	A comma-separated list of all the hosts that are part of the Management Agent.

Examples

EXAMPLE 1 Creating an HADB management domain

```
hadbm createdomain host1,host2,host3
Domain host1,host2,host3 created
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22015	hosts specified in the hostlist contain duplicate host names
22190	a domain with the specified hostlist already exists or the hosts are part of a management domain
22196	the URL used to connect to the management agents spans hosts which are not in the management domain.

See Also hadbm(1)hadbm-create(1), hadbm-listdomain(1), hadbm-extenddomain(1), hadbm-reducedomain(1), hadbm-deletedomain(1)

Name hadbm delete – removes the database

Synopsis

```
hadbm delete [—adminpassword=password | —adminpasswordfile=filename ]
     [—agent=ma_url] [dbname]
```

Description Use the `hadbm delete` command to remove the database, configuration files, device files, history and log files. If a database is identified, it should already exist and should be in a stopped state. If a database is not named, the default database is used. The default database is hadb.

In interactive mode, the `hadbm delete` command prompts for a confirmation before removing the database.

Options

`–w —adminpassword`	The actual HADBM administation password.
`–W —adminpasswordfile`	The file containing the HADBM administration password. The adminstration password is defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–m —agent`	Identifies the URL to the Management Agent. The default is localhost:1862.

Operands

dbname	The name of the database. The default database is hadb.

Examples

EXAMPLE 1 Using delete

```
hadbm delete
This command will remove the database and all configuration,
history and log files. Type "yes" or "y" to confirm this
operation, anything else to cancel: y
Database successfully deleted
```

EXAMPLE 2 Using delete with a database identified

```
hadbm delete mydatabase
This command will remove the database and all configuration,
history and log files. Type "yes" or "y" to confirm this
operation, anything else to cancel: y
Database successfully deleted
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22002	specified database does not exist
22065	database not in a stopped state

22066	database could not be removed

See Also hadbm-addnodes(1), hadbm-clear(1), hadbm-create(1), hadbm-list(1), hadbm-refragment(1), hadbm-restart(1), hadbm-start(1), hadbm-status(1), hadbm-stop(1)

Name hadbm deletedomain – removes the HADB management domain

Synopsis

```
hadbm deletedomain [––adminpassword=password | ––adminpasswordfile=filename ]
    [––agent=ma_url]
```

Description Before using the `hadbm deletedomain` command, the following prerequisites must be met:

- An HADB management domain must already exist
- All agents in the domain must be running
- No databases exist in the domain

After successfully executing , the `hadbm deletedomain` command, the management agents of the removed hosts are stopped, and the repository of the deleted hosts is cleaned up. If the agents are restarted, they will not be part of any domain. To have the restarted agents associated with a domain, create a new management domain using the `hadbm createdomain` command.

Options

`–w ––adminpassword`	The actual HADBM administation password.
`–W ––adminpasswordfile`	The file containing the HADBM administration password. The adminstration password is defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–m ––agent`	Identifies the URL to the Management Agent. The default is localhost:1862.

Examples **EXAMPLE 1** Deleting the Management Domain

```
hadbm deletedomain
This command will delete the domain host1,host2,host3.
Type "yes" or "y" to confirm this
operation, anything else to cancel: y
Domain hostlist has been deleted.
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22192	the management domain does not exist
22194	hosts cannot be removed because they contain databases
22196	the URL used to connect to management agents spans hosts which are not in the management domain

See Also `hadbm(1)`, `hadbm-create(1)`, `hadbm-createdomain(1)`, `hadbm-extenddomain(1)`, `hadbm-listdomain(1)`, `hadbm-reducedomain(1)`

Name hadbm deviceinfo – displays information about disk storage devices on each active data node

Synopsis

```
hadbm deviceinfo [—details]
     [—adminpassword=password | —adminpasswordfile= filename]
     [—agent=ma_url] [dbname]
```

Description If a database is specified, the database should be existing as shown by the `hadbm-list` command. If the database name is not specified, the default database should exist as shown by the `hadbm-list` command.

The information displayed for each node of the database is:

- total device size allocated in MB
- free size in MB
- usage in percentage

The status of the database and the nodes are not changed.

Options

`-d —details`	This option displays detailed information about the named database.
`–w —adminpassword`	The actual HADBM administation password.
`–W —adminpasswordfile`	The file containing the HADBM administration password. The adminstration password is defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–m —agent`	Identifies the URL to the Management Agent. The default is localhost:1862.

Operands

dbname	The name of the database. The default database is hadb.

Examples

EXAMPLE 1 Using deviceinfo without any options

```
hadbm deviceinfo
NodeNo    TotalSize    Freesize    Usage
3         1048         869         17%
4         1048         869         17%
5         1048         869         17%
6         1048         869         17%
```

EXAMPLE 2 Using deviceinfo with a database specified and quiet option

```
hadbm deviceinfo -q mydatabase
3         1048         869         17%
4         1048         869         17%
5         1048         869         17%
```

EXAMPLE 2 Using deviceinfo with a database specified and quiet option *(Continued)*

```
6        1048        869        17%
```

EXAMPLE 3 Using deviceinfo with details option

```
hadbm deviceinfo --details
NodeNo    TotalSize    FreeSize    Usage    NReads    Nwrites    DeviceName
3         1048         869         17%      0         42578      /export/home2/tmp//hadb.data
4         1048         869         17%      0         42554      /export/home2/tmp//hadb.data
5         1048         869         17%      0         42544      /export/home2/tmp//hadb.data
6         1048         869         17%      0         9828      /export/home2/tmp//hadb.data-
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22002	specified database does not exist

See Also `hadbm-resourceinfo(1)`

Name hadbm disablehost – selectively disables a host in the management domain

Synopsis

```
hadbm disablehost [—adminpassword=password | —adminpasswordfile=filename ]
    [—agent=ma_url] hostname
```

Description Use the `disablehost` command to remove an unresponsive host from the management domain. Since the majority of management agents in a management domain must be enabled and running to execute HADB management commands, unresponsive hosts reduce the number of active agents and therefore prevent operation of `hadbm` commands.

A disabled host is automatically re-enabled when its management agent is restarted.

Before using the `disablehost` command, ensure the host to be disabled is:

- registered in the management domain
- enabled
- the management agent for the host is not running
- all database nodes configured to run on the host are stopped

Options

`–w —adminpassword`	The actual HADBM administation password.
`–W —adminpasswordfile`	The file containing the HADBM administration password. The adminstration password is defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–m —agent`	Identifies the URL to the Management Agent. The default is localhost:1862.

Operands

hostname	The hostname for the host to be disabled.

Examples **EXAMPLE 1** Disabling a host named host1

```
hadbm disablehost host1
Host successfully disabled
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22176	the host is not registered in the HADB management domain
22180	the host is already disabled
22181	database nodes are running on the host. Use hadbm stopnode to stop the nodes before using disablehost
22182	the management agent is running on the specified host. Stop the management agent before disabling the host

See Also hadbm(1), hadbm-create(1), hadbm-listpackages(1), hadbm-unregisterpackage(1)

Name hadbm extenddomain – extends the current HADB management domain by adding the specified hosts

Synopsis

```
hadbm extenddomain [—adminpassword=password | —adminpasswordfile=filename ]
    [—agent=ma_url] host_list
```

Description Use the `hadbm extenddomain` command to add hosts to an existing management domain. All the hosts that will be part of the desired domain must be included in the hostlist. The following prerequisites must be met before using the `hadbm extenddomain` command:

- An HADB management domain must already exist.
- HADB management agents are running on the hosts.
- The management agents on the hosts to be added are not members of an existing domain.
- All the management agents are configured to use the same port.
- All the management agents can reach each other over UDP, TCP, and with IP multicast.

Options

`–w —adminpassword`	The actual HADBM administation password.
`–W —adminpasswordfile`	The file containing the HADBM administration password. The adminstration password is defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–m —agent`	Identifies the URL to the Management Agent. The default is localhost:1862.

Operands

host_list	A comma-separated list of all the hosts that are part of the management domain.

Examples **EXAMPLE 1** Adding hosts to an HADB management domain

```
hadbm extenddomain host4,host5,
Hosts added, domain is now host1,host2,host3,host4,host5
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22015	the hostlist contains duplicate host names
22016	the host 3 and host 4 are registered in different management domains. Domains cannot be merged. Use hadbm reducedomain to remove one of the hosts from a domain and then restart the agent
22191	the specified hosts are already part of the management domain
22192	the management domain does not exist

22196	the URL used to connect to management agents spans hosts which are not in the management domain

See Also hadbm(1), hadbm-create(1), hadbm-createdomain(1), hadbm-deletedomain(1), hadbm-listdomain(1), hadbm-reducedomain(1)

Name hadbm-get – gets the value of the specified configuration attribute

Synopsis

```
hadbm get —all | attribute_name_list
      [—adminpassword=password | —adminpasswordfile=filename ]
      [—agent=ma_url] [dbname]
```

Description Use the `get` command to get the value of the named configuration attribute. If the command is run without any attributes, and with the `—all` option, all the supported variables and their values are retrieved. If an attribute is unrecognized, an exception is thrown on the unrecognized attribute name, and the variables and values of the recognized attributess are returned.

The readable configuration attributes are as follows:

Variable	Type	Default
ConnectionTrace	boolean	false
CoreFile	boolean	false
DataBufferPoolSize	integer	200 MB
DatabaseName	string	hadb
DataDeviceSize	integer	1024 MB
DevicePath	string	n/a
EagerSessionThreshold	integer	50 (% of NumberOfSessions)
Eager SessionTimeout	integer	120 seconds
EventBufferSize	integer	0 MB
HistoryPath	string	n/a
InternalLoBbufferSize	integer	12 MB
JdbcUrl	string	n/a
LogBufferSize	integer	48 MB
MaxTables	integer	1100
NumberOfDataDevices	integer	1
NumberOfLocks	integer	50000
NumberOfSessions	integer	100
PackageName	string	n/a
PortBase	integer	15000

Variable	Type	Default
RelalgDeviceSize	integer	128 MB
SessionTimeout	integer	1800 seconds
SQLTraceMode	string	off
StartRepairDelay	integer	20 seconds
StatInterval	integer	600 seconds
SyslogFacility	string	local0
SyslogLevel	string	NONE, ALERT, ERROR, WARNING, INFO
SysLogging	boolean	true
SyslogPrefix	string	hadb-<db_name>
TakeoverTime	integer	10000 MS

The `hadbm get` command also supports attributes that were used to create the database (either default values or ones explicitly provided) or which have been subsequently modified.

Options

`–w ––adminpassword`	The actual HADBM administation password.
`–W ––adminpasswordfile`	The file containing the HADBM administration password. The adminstration password is defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–m ––agent`	Identifies the URL to the Management Agent. The default is localhost:1862.

Operands

attribute_name_list	A comma or space separated list of variables whose values have been retrieved.
dbname	The name of the database. The default database is hadb.

Examples

EXAMPLE 1 Using get

```
hadbm get "takeoverTime numberOfLocks jdbcURL" mydatabase
Attribute    Value
takeoverTime    10000
numberofLocks    10000
JdbcUrl    com:sun:hadb:royal:15000,polo:15020
```

Exit Status

0	command executed successfully

	1	error in executing the command
Error Codes	22002	specified database does not exist
	22071	attribute names are not recognized

See Also `hadbm-addnodes(1)`, `hadb-clear(1)`, `hadbm-delete(1)`, `hadb-list(1)`, `hadbm-refragment(1)`, `hadbm-restart(1)`, `hadbm-set(1)`, `hadbm-start(1)`, `hadbm-stop(1)`

Name hadbm help – displays a list of all the subcommands to administer HADB

Synopsis **`hadbm help`** `or hadbm` *command_name* —`help`

Description The following is a list of all the `hadbm` subcommands:

addnodes	adds nodes to the named database
clear	reinitializes all the data space on all nodes and starts the database
clearhistory	clears the history files on the database
create	creates a database instance
createdomain	creates a management domain of the listed HADB hosts
delete	removes the database
deletedomain	deletes the HADB management domain
deviceinfo	displays information about disk storage devices on each active data node
disablehost	selectively disables a host in the management domain
extenddomain	extends the current HADB management domain
get	gets the value of the specified configuration parameter
help	displays all the subcommands for the hadbm utility
list	lists all the existing databases
listdomain	lists all hosts defined in the management domain
listpackages	lists the packages registered in the management domain
reducedomain	removes hosts from the HADB management domain
refragment	refragments the schema
registerpackage	registers the HADB packages in the management domain
resourceinfo	displays database resource information
restart	restarts the database
restartnode	restarts the specified node
set	sets the value of the specified configuration attributes to the identified values
start	starts the database
startnode	starts the specified node

	status	shows the state of the database
	stop	gracefully stops the database
	stopnode	gracefully stops the specified node
	unregisterpackage	removes registered HADB packages from the management domain
	version	displays the hadbm version information

Common Options

`-q` —`quiet`	Performs the operation silently without any descriptive messages.
`-?` —`help`	Displays a brief description of the `hadbm` utility and all the supported commands.
`-v` —`version`	Displays the version details of the `hadbm` utility.
–`y` —`yes`	Launches the command in non-interactive mode.
`-f` —`force`	Launches the command in interactive mode.
`-e` —`echo`	Displays the commands with all the options and their user-defined values or the default values; then launches the command.

Examples

EXAMPLE 1 Executing an hadbm command

```
hadbm clear
This command will clear the database
Type "yes" or "y" to confirm this operation, anything else to cancel: y
Database successfully cleared
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `hadbm(1m)`

Name hadbm list – lists all the existing databases

Synopsis

```
hadbm list [––adminpassword=password | ––adminpasswordfile=filename ]
     [––agent=ma_url]
```

Description Use the `hadbm list` command to get a listing of all the existing database instances known to the management client running this command. If the list could not display the database instance, see the `hadbm` command if you are sure you have created it earlier.

Options

`–w ––adminpassword`	The actual HADBM administation password. Using this option with the `hadbm createdomain` or `hadbm create` command requires that the password is entered each time any `hadbm` command is used. The `adminpassword` is different from the `hadbm dbpassword` command. You must use both passwords when using the following commands: `hadbm create`, `hadbm addnodes`, `hadbm refragment`.
`–W ––adminpasswordfile`	The file containing the HADBM administration password. The adminstration password must be defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–m ––agent`	Identifies the URL to the Management Agent. The default is localhost:1862.

Examples **EXAMPLE 1** Using list

```
hadbm list
Database
hadb
mydatabase
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22002	specified database does not exist

See Also `hadbm-clear(1)`, `hadbm-clearhistory(1)`, `hadbm-delete(1)`, `hadbm-get(1)`, `hadbm-restart(1)`, `hadbm-resourceinfo(1)`, `hadbm-set(1)`, `hadbm-start(1)`, `hadbm-stop(1)`

Name hadbm listdomain – lists all hosts defined in the management domain

Synopsis

```
hadbm listdomain [—adminpassword=password | —adminpasswordfile=filename ]
    [—agent=ma_url]
```

Description Use the `hadbm listdomain` command to list all hosts defined in the management domain and the status of the management agents.

Options

`–w —adminpassword`	The actual HADBM administation password. Using this option with the `hadbm createdomain` or `hadbm create` command requires that the password is entered each time any `hadbm` command is used. The `adminpassword` is different from the `hadbm dbpassword` command. You must use both passwords when using the following commands: `hadbm create`, `hadbm addnodes`, `hadbm refragment`.
`–W —adminpasswordfile`	The file containing the HADBM administration password. The adminstration password must be defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–m —agent`	Identifies the URL to the Management Agent. The default is localhost:1862.

Examples **EXAMPLE 1** Using the hadbm-listdomain

The following command lists all participating members of a previously created domain.

```
hadbm listdomain
Hostname    Enabled?    Interfaces
HostA        Yes        10.0.5.70
HostB        Yes        10.0.5.72
HostC        Yes        10.0.5.73
HostD        Yes        10.0.5.74
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `hadbm-create(1)`, `hadbm-createdomain(1)`, `hadbm-deletedomain(1)`, `hadbm-extenddomain(1)`, `hadbm-reducedomain(1)`

Name listpackages – lists the packages registered in the management domain

Synopsis

```
listpackages [—adminpassword=password | —adminpasswordfile=filename ]
     [—agent=ma_url]
```

Description Use the `listpackages` command to display a list of the packages registered in the management domain and the hosts to which they are registered.

Options

`–w —adminpassword`	The actual HADBM administation password. Using this option with the `hadbm createdomain` or `hadbm create` command requires that the password is entered each time any `hadbm` command is used. The `adminpassword` is different from the `hadbm dbpassword` command. You must use both passwords when using the following commands: `hadbm create`, `hadbm addnodes`, `hadbm refragment`.
`–W —adminpasswordfile`	The file containing the HADBM administration password. The adminstration password must be defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–m —agent`	Identifies the URL to the Management Agent. The default is localhost:1862.

Examples **EXAMPLE 1** Using the hadbm-listpackages

```
hadbm listpackages
Package    Hosts
V4.4        HostA,HostB,HostC,HostD
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `hadbm(1m)`, `hadbm-create(1)`, `hadbm-registerpackage(1)`, `hadbm-unregisterpackage(1)`

Name ma – configures and starts the HADB Management Agent

Synopsis

```
ma HADB_install_path/bin/ma [—define=assignment] [—javahome=JAVA_HOME]
    [—systemroot=root_path] [—version] [—help] [—install] [—remove]
    [—service] [—name=name_of_service] [—no-detach] [AGENT_CONFIG_path]
```

Description Use the `ma` command to configure and start the HADB Management Agent on a host that will belong to an HADB management domain. The configuration is defined in the `AGENT_CONFIG` file. In addition you can register the Management Agent as a Windows service by using the service options `—install`, `—service`, and `—name`. The Management Agent ensures the availability of the HADB nodes on the host it runs by restarting them if there is a failure during startup, or during normal operation. To ensure the availability of the Management Agent you should register it as a Windows service so it is restarted automatically if it fails or when the computer reboots.

An HADB management domain consists of a set of hosts that are capable of running HADB database nodes. A Management Agent runs on each host belonging to a management domain. `hadbm` management clients communicate with Management Agents to perform the `hadbm` management commands like `create`, `start`, `stop`, and so on.

The Management Agent must be configured and started on all hosts before a database instance can be created. All hosts in a domain run a Management Agent at the same port number. All agents are aware of each other and their participation in the management domain. Agents communicate with each other, and may forward requests to other agents when they perform management commands specific to a host. For example, when an agent is requested to stop a node, it checks whether the mirror host is up and running. To get that information, it communicates with the agent running on the mirror host.

The Management Agent maintains a repository where the database configuration is stored. A majority of agents in the management domain must be available to make changes in the repository.

The `AGENT_CONFIG` file contains the configuration information for the Management Agent. A sample file named `mgt.cfg` is located in the *HADB_install_path*`/lib` directory. Use this sample file to assist you in defining your configuration files. In addition to the configuration variables, the `AGENT_CONFIG` file also contains the default path information for the history files, and the data device files for the HADB instances managed by this agent. If you have NOT specified the history and device path information using the `create` command, the default values located in the `AGENT_CONFIG` file will be used.

Options The following options identify common setup information for the Management Agent:

`-D —define`	The agent property assignment in the format of *property=value*

`-j —javahome`	The full path to the Java runtime installation. The default value is the value of the `JAVA_HOME` variable.
`-y —systemroot`	An alternate specification of the Windows system root path.
`-V —version`	Displays the version information and exits.
`-? —help`	Displays this help page and exits.

The following options identify service configuration infomation for the Management Agent:

`-i —install`	Registers a service for the agent and starts the service.
`-r —remove`	Stops and unregisters the agent service.
`-s —service`	This option is for internal use by the service control program.
`-n —name`	Identifies the name to use when registering and operating the service. The default name is `HADBMgmtAgent`.
`—no-detach`	Prevents the agent from detaching from the terminal. This option is required when using inittab for keeping the agent alive on Solaris (versions without SMF) and on Linux.

Operands

AGENT_CONFIG_path	The full path to the `AGENT_CONFIG` file.

Examples

EXAMPLE 1 Sample AGENT_CONFIG file

The following sample file can be edited for your particular installation:

```
ma.server.jmxmp.port=31108 #this can be any port not currently being used#
ma.server.dbconfigpath=/etc/opt/SUNWhadb/MA
repository.dr.path=/var/opt/SUNWhadb/REP
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

0	error message
1	error message

See Also `hadbm(1m)`

Name hadbm reducedomain – removes hosts from the HADB management domain

Synopsis

```
hadbm reducedomain [—adminpassword=password | —adminpasswordfile=filename ]
    [—agent=ma_url] host_list
```

Description The following prerequisites must be met before using the `hadbm reducedomain` command:

- An HADB management domain must already exist.
- The hosts to be removed are registered in the domain. No database nodes are configured to be used on the hosts to be removed.
- The HADB management repository is writable.
- Software packages that are in use are not registered on the hosts which are to be removed.
- The hostlist must not contain all agents in the domain. To remove all agents, use the `hadbm deletedomain` command.

After successfully executing the `hadbm reducedomain` command, the management agents of the removed hosts are stopped and the repository of the deleted hosts is cleaned up.

Options

`–w —adminpassword`	The actual HADBM administation password.
`–W —adminpasswordfile`	The file containing the HADBM administration password. The adminstration password is defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–U —no-adminauthentication`	This option allows the administrator to use all `hadbm` commands without providing the administrator's password.
`–m —agent`	Identifies the URL to the Management Agent. The default is localhost:1862.

Operands

host_list	A comma-separated list of all the hosts that are part of the management domain.

Examples

EXAMPLE 1 Removing hosts from a management domain

```
hadbm reducedomain host4,host5
Hosts removed, domain is now host1,host2,host3
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22015	the hostlist contains duplicate host names
22192	the management domain does not exist

22193	the specified hosts are not part of the domain and cannot be removed
22194	hosts cannot be removed because they contain databases
22195	cannot remove all hosts from the domain
22196	the URL used to connect to management agents spans hosts which are not in the management domain

See Also hadbm(1m), hadbm-create(1), hadbm-createdomain(1), hadbm-deletedomain(1), hadbm-extenddomain(1), hadbm-listdomain(1)

Name hadbm refragment – refragments the database schema

Synopsis

```
hadbm refragment [—dbpassword=password | —passwordfile=passwordfilename ]
    [—adminpassword=password | —adminpasswordfile=filename ]
    [—agent=ma_url] [dbname]
```

Description Refragmentation is needed to store the data on a newly created node. Run the `hadbm refragment` command after adding a node using the `hadbm addnodes` command with the `—no-refragment` option specified. If the `hadbm refragment` command fails, it can be retried. If it continues to fail, the database must be cleared, and the product-specific schemas must be reloaded. All the user tables are refragmented.

If a database is specified, the database must already exist and must be in an HA Fault Tolerant or Fault Tolerant state. If the database is not named, the default database is refragmented. The default database is `hadb`.

In interactive mode, the `hadbm refragment` command prompts for a confirmation before refragmenting the data.

Options

`-p —dbpassword`	The password string for the system user of the database. The minimum length of the password must be 8 characters. You can identify either the database password, or for higher security, the password file where the password is defined.
`-P —dbpasswordfile`	Identifies the file containing the password to be used for the system user of the database.
`–w —adminpassword`	The actual HADBM administation password.
`–W —adminpasswordfile`	The file containing the HADBM administration password. The adminstration password is defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–m —agent`	Identifies the URL to the Management Agent. The default is localhost:1862.

Operands

dbname	The name of the database. The default database is hadb.

Examples **EXAMPLE 1** Using refragment

```
hadbm refragment --dbpasswordfile=/home/hadb/dbpfile mydatabase
This command will refragment the data on all active nodes.
Type "yes" or "y" to confirm this operation, anything else to cancel:y
Database successfully refragmented
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22002	specified database does not exist
22041	invalid database state
22042	database could not be refragmented
22051	node not responding

See Also `hadbm-clear(1)`, `hadbm-create(1)`, `hadbm-delete(1)`, `hadbm-list(1)`, `hadbm-restart(1)`, `hadbm-start(1)`, `hadbm-status(1)`, `hadbm-stop(1)`

Name hadbm registerpackage – registers HADB packages in the management domain

Synopsis

```
hadbm registerpackage —packagepath=path [—hosts=host_list]
      [—adminpassword=password | —adminpasswordfile=filename ]
      [—agent=ma_url] [package_name]
```

Description Use the `hadbm registerpackage` command to register the HADB packages that are installed on the hosts in the management domain. Registering packages can also be done when creating a database with the `hadbm create` command. The default package name is a string starting with V and containing teh version number of the hadbm program. If the `—hosts` option is omitted, the package is registered on all enabled hosts in the domain.

Before using the `hadbm registerpackage` command, ensure that all management agents are configured and running on all the hosts in the hostlist, the repository of the management agent is available for updates, and no software package is already registered with the same package name.

Options

`—packagepath`	The full path to the HADB software package.
`—hosts`	A comma-separated or double quote enclosed list of hosts to register the package on.
`–w —adminpassword`	The actual HADBM administation password.
`–W —adminpasswordfile`	The file containing the HADBM administration password. The adminstration password is defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–m —agent`	Identifies the URL to the Management Agent. The default is localhost:1862.

Operands

package_name	The name of the package you are registering. If a package name is not specified, the default name of the software package is used. For example, if you are using the software release V4–4–02, the default package name is V4.4.

Examples

EXAMPLE 1 Registering a software package named v4

```
hadbm registerpackage --packagepath=hadb_install_dir/SUNWhadb/4.4/v4
Package successfully registered
```

EXAMPLE 2 Registering a software package namve v4 on a specific host in the domain

```
hadbm registerpackage --packagepath=hadb_install_dir/SUNWhadb/4.4
--hosts=host1,host2,host3 v4
Package successfully registered
```

Exit Status

0	command executed successfully

	1	error in executing the command
Error Codes	22170	the software package could not be found at the specified path on the host
	22171	the software package already exists or is registered with the same name

See Also hadbm(1m)hadbm-create(1), hadbm-listpackages(1), hadbm-unregisterpackage(1)

Name hadbm resourceinfo – gives information about the database resources

Synopsis

```
hadbm resourceinfo [—-databuf] [—-locks] [—-logbuf] [—-nilogbuf]
      [—-adminpassword=password | —-adminpasswordfile=filename ]
      [—-agent=ma_url] [dbname]
```

Description Use the `hadbm resourceinfo` command to get information about the various database resources. If a database is named, it must already exist. If a database is not named, the default database is used. The default database is hadb.

Options

`-d —-databuf`	This option displays the data buffer pool information.
`-l —-locks`	This option displays the locks information.
`-b —-logbuf`	This option displays the log buffer information.
`-n —-nilogbuf`	This option displays the node internal log buffer information.
`–w —-adminpassword`	The actual HADBM administation password.
`–W —-adminpasswordfile`	The file containing the HADBM administration password. The adminstration password is defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–m —-agent`	Identifies the URL to the Management Agent. The default is localhost:1862.

Operands

dbname	The name of the database. The default database is hadb.

Examples **EXAMPLE 1** Using resourceinfo

```
hadbm resourceinfo
Databuffer pool:
NodeNo    Avail    Free    Access    Misses    Copy-on-write
3         198        198         201         0         0
4         198        198         217         0         0
5         198        198         194         0         0
6         198        198         43          0         0

Locks:
NodeNo    Avail    Free    Waits
3         50000    50000    na
4         50000    50000    na
5         50000    50000    na
6         50000    50000    na

Log buffer:
NodeNo    Avail    Free
```

EXAMPLE 1 Using resourceinfo *(Continued)*

```
3        44        11
4        44        11
5        44        11
6        44        22

Node internal log buffer:
NodeNo    Avail    Free
3        11        11
4        11        11
5        11        11
6        11        11
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22002	specified database does not exist

See Also `hadbm-clear(1)`, `hadbm-clearhistory(1)`, `hadbm-delete(1)`, `hadbm-deviceinfo(1)`, `hadbm-list(1)`, `hadbm-restart(1)`, `hadbm-start(1)`, `hadbm-status(1)`, `hadbm-stop(1)`,

Name hadbm restart – restarts the database

Synopsis

```
hadbm restart [—adminpassword=password | —adminpasswordfile=filename ]
      [—agent=ma_url] [—no-rolling] [dbname]
```

Description Use the `hadbm restart` command to restart the database. Once the database is restarted, it returns to the previous state or better. If the database name is specified, the database must exist. If the database name is not specified, the default database is restarted. The default database is hadb.

In interactive mode, the `hadbm restart` command prompts for a confirmation before restarting the database.

Options

`–w —adminpassword`	The actual HADBM administation password.
`–W —adminpasswordfile`	The file containing the HADBM administration password. The adminstration password is defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–m —agent`	Identifies the URL to the Management Agent. The default is localhost:1862.
`-g —no-rolling`	This option restarts all nodes in the HADB at once with possible loss of service. If this option is not specified, the hadbm restarts the nodes one by one and maintains the availability of the HADB. If the option is specified, it stops al nodes in parallel and starts them in parallel. During this period, the HADB is not available.

Operands

dbname	The name of the database. The default database is hadb.

Examples

EXAMPLE 1 Using restart with a database identified

```
hadbm restart mydatabase
This command will restart the named database.
Type "yes" or "y" to confirm this operation, anything else to cancel: y
Database successfully restarted
```

EXAMPLE 2 Using restart with no rolling

```
hadbm restartnode --no-rolling mydatabase
This command will restart the named database.
Type "yes" or "y" to confirm this operation, anything else to cancel: y
Database successfully restarted
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22002	specified database does not exist
22105	database is not running
22106	database could not be restarted
22107	database could not return to a previous state
22108	invalid database state

See Also `hadbm-addnodes(1)`, `hadbm-clear(1)`, `hadbm-delete(1)`, `hadbm-list(1)`, `hadbm-refragment(1)`, `hadbm-start(1)`, `hadbm-status(1)`, `hadbm-stop(1)`

Name hadbm restartnode – restarts the specified node

Synopsis

```
hadbm restartnode [—adminpassword=password | —adminpasswordfile=filename ]
    [—agent=ma_url] [—startlevel=level] node_number [dbname]
```

Description Use the `hadbm restartnode` command to restart the node. The node is restarted by running the startup procedure on the node. The mirror node of the node to be restarted must be up. The node is restarted in the specified start level. The start level indicates the environmental conditions the node should take into consideration while starting. The valid start levels are:

Start Level	Description
normal (default)	This start level is used when the node has been stopped earlier in a controlled way (default).
repair	This start level forces an active node to repair data from its mirror node.
clear	This start level reinitializes the devices for the node, and forces a repair of data from its mirror node.

In interactive mode, the `hadbm restartnode` command prompts for a confirmation before restarting the node.

Options

`–w —adminpassword`	The actual HADBM administation password.
`–W —adminpasswordfile`	The file containing the HADBM administration password. The adminstration password is defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–m —agent`	Identifies the URL to the Management Agent. The default is localhost:1862.
`–l —startlevel`	Identifies the start level to be used to restart the named node. The default start level is normal.

Operands

node_number	A positive integer. The node number must be an existing node that is in a running state in the database.
dbname	The name of the database. The default database is hadb.

Examples

EXAMPLE 1 Using restartnode on the default database

```
hadbm restartnode 2
This command will restart the node.
Type "yes" or "y" to confirm this operation, anything else to cancel: y
Node successfully restarted
```

EXAMPLE 2 Using restartnode with a database identified

```
hadbm restartnode 2 mydatabase
This command will restart the node.
Type "yes" or "y" to confirm this operation, anything else to cancel: y
Node successfully restarted
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22002	specified database does not exist
22082	start level is not a recognized level
22087	mirror node of the specified node is not running
22088	node is not running
22091	node could not be restarted

See Also hadbm-addnodes(1), hadbm-list(1), hadbm-startnode(1), hadbm-stopnode(1)

Name hadbm set – sets the value of the specified configuration attributes to the identified values

Synopsis

```
hadbm set [—adminpassword=password | —adminpasswordfile=filename ]
    [—agent=ma_url] {attribute_name_value_list} [dbname]
```

Description The `hadbm set` command is used to reconfigure the database. Multiple configuration attributes can be modified in one single set operation. You can use a comma or space separated list of name=value pairs. If using a space separated list, use quotation marks to preserve the spaces. The writeable configuration attributes are as follows:

Variable	Type	Default
ConnectionTrace	boolean	false
CoreFile	boolean	false
DataBufferPoolSize	integer	200 MB
DataDeviceSize	integer	1024 MB
DevicePath	string	n/a
EagerSessionThreshold	integer	50 (% of NumberOfSessions)
Eager SessionTimeout	integer	120 seconds
EventBufferSize	integer	0 MB
HistoryPath	string	n/a
InternalLogbufferSize	integer	12 MB
LogbufferSize	integer	48 MB
MaxTables	integer	1100
NumberOfLocks	integer	50000
NumberOfSessions	integer	100
PackageName	string	n/a
RelalgDeviceSize	integer	128 MB
SessionTimeout	integer	1800 seconds
SQLTraceMode	string	off
StartRepairDelay	integer	20 seconds
StatInterval	integer	600 seconds
SyslogFacility	string	local0

Variable	Type	Default
Sysloglevel	string	NONE, ALERT, ERROR, WARNING, INFO
SysLogging	boolean	true
SyslogPrefix	string	hadb-<db_name>
TakeoverTime	integer	10000 MS

The values of the configuration attributes will be set into the database configuration. Use the `hadbm get` command to get the new value of an attribute. When the value part of an attribute is missing, the attribute is set to the default value.

Setting the database attribute may require the system to do a rolling restart of the hadb nodes. The database must be in Fault Tolerant or HA Fault Tolerant state before using the `hadbm set` command.

The `JdbcUrl` cannot be set with either the `hadbm set` or `hadbm create` commands. However, the `hadbm create` or `hadbm addnodes` commands derive the `JdbcUrl` value from values given for `—hosts` and `—portbase` options. So, there is no need to set this variable.

Options

`–w —adminpassword`	The actual HADBM administation password.
`–W —adminpasswordfile`	The file containing the HADBM administration password. The adminstration password is defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–m —agent`	Identifies the URL to the Management Agent. The default is localhost:1862.

Operands

attribute_name_value_list	A list of variables with values to be set. All the attribute names must be supported attributes.
dbname	The name of the database. The default database is hadb.

Examples

EXAMPLE 1 Using set

```
hadbm set "connectiontrace=true numberOfLocks=110000"
Database attributes successfully set.
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22002	specified database does not exist
22033	invalid value set for attributes

22071	attributes are not recognized
22072	attribute is not writeable

See Also hadbm-addnodes(1), hadbm-get(1), hadbm-clear(1), hadbm-delete(1), hadbm-list(1), hadbm-start(1), hadbm-restart(1), hadbm-status(1), hadbm-stop(1)

Name hadbm setadminpassword – sets the adminpassword for the management domain

Synopsis

```
hadbm setadminpassword [ —-adminpasswordfile=filename]
     [—-newadminpasswordfile=filename] [—-agent=ma_url]
```

Description Use the `hadbm setadminpassword` command to change the admin password for a management domain. If no options are provided with the command the user will be prompted for both the old and new passwords interactively. Passwords less than 8 characters long are assumed unsafe passwords, and the user will be warned. However, unsafe passwords will be accepted.

Options

`–W —-adminpasswordfile`	The file from which the administrator user password is read. Passwords can only be supplied interactively or through the password file.
`–Z —-newadminpasswordfile`	Use the adminpasswordfile option to provide the new password as a path to a file that contains the password. It is also possible to specify the new password interactively.
`–U —-no-adminauthentication`	Use this option to enable access to a management domain without a password.
`–m —-agent`	Identifies the URL to the Management Agent. The default is localhost:1862.

Examples

EXAMPLE 1 Using setadminpassword to change admin password

```
hadbm setadminpassword --agent=host1,host2:41108
Please type current password for admin system user: *********
Please type new password for admin system user: *********
Please retype new password for admin system user: *********
Password successfully updated.
```

EXAMPLE 2 Using setadminpassword to not require a password

```
hadbm setadminpassword --no-adminauthentication --agent=host1,host2:41108
Please type current password for admin system user: *********
This command will now update the admin password. Type "yes" or "y" to update the password for
Password successfully updated.
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22005	Authentication failed
22006	The agents specified could not be reached

See Also `hadbm-addnodes(1)`, `hadbm-get(1)`, `hadbm-clear(1)`, `hadbm-delete(1)`, `hadbm-list(1)`, `hadbm-start(1)`, `hadbm-restart(1)`, `hadbm-status(1)`, `hadbm-stop(1)`

Name hadbm start – starts the database

Synopsis

```
hadbm start [—adminpassword=password | —adminpasswordfile=filename ]
      [—agent=ma_url] [dbname]
```

Description Use the `hadbm start` command to start the database. Only the nodes that were running before the database was stopped will be started. If the database name is specified, it should be an existing database. If the database name is not specified, the default database is used. If one or more mirror node pairs have stopped simultaneously due to a power outage, machine reboot or some other disaster (i.e., the hadb instance is in a non-functional state), then the database instance cannot be started. In such a case, use the `hadbm clear` command to start the database and recreate the schema.

Options

`–w —adminpassword`	The actual HADBM administation password.
`–W —adminpasswordfile`	The file containing the HADBM administration password. The adminstration password is defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–m —agent`	Identifies the URL to the Management Agent. The default is localhost:1862.

Operands

dbname	The name of the database. The default database is hadb.

Examples **EXAMPLE 1** Using start with a database identified

```
hadbm start mydatabase
Database successfully started
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22002	specified database does not exist
22095	database could not be started
22096	database is already running
22097	some nodes could not be started
22098	database (hadb) could not be started. The stopstate cannot be determined. In case of uncontrolled stop of the database, use the `hadbm clear` command to start the database.

See Also `hadbm-addnodes(1)`, `hadbm-clear(1)`, `hadbm-delete(1)`, `hadbm-list(1)`, `hadbm-refragment(1)`, `hadbm-restart(1)`, `hadbm-status(1)`, `hadbm-stop(1)`

Name hadbm startnode – starts the specified node

Synopsis

```
hadbm startnode [––adminpassword=password | ––adminpasswordfile=filename ]
     [––agent=ma_url] [––startlevel=level] node_number [dbname]
```

Description The `hadbm startnode` command starts the node by running the startup procedure on the node. The node is started in the specified start level. The start level indicates the environmental conditions the node should take into consideration while starting. The valid start levels are as follows:

Start Level	Description
normal	This start level is used when the node was earlier stopped in a controlled way (default).
repair	This start level forces an active node to repair data from its mirror node.
clear	This start level reinitializes the devices for the node, and force a repair of data from its mirror node.

Options

`–w ––adminpassword` The actual HADBM administation password.

`–W ––adminpasswordfile` The file containing the HADBM administration password. The adminstration password is defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.

`–m ––agent` Identifies the URL to the Management Agent. The default is localhost:1862.

`––startlevel` Indicates the start level to be used to start the specified node(s). The default start level is normal.

Operands

node_number A positive integer. The node number specified must be an existing node that is in a running state in the database.

dbname The name of the database. The default database is hadb.

Examples

EXAMPLE 1 Using startnode on the default database

```
hadbm startnode 1
Node successfully started
```

EXAMPLE 2 Using startnode with the startlevel and database identified

```
hadbm startnode --startlevel=normal 1 mydatabase
Node successfully started
```

Exit Status

0 command executed successfully

	1	error in executing the command
Error Codes	22002	specified database does not exist
	22081	node is already running
	22082	start level is not a recognized level
	22083	node could not be started

See Also `hadbm-addnodes(1)`, `hadbm-list(1)`, `hadbm-restartnode(1)`, `hadbm-stopnode(1)`

Name hadbm status – shows the state of the database

Synopsis

```
hadbm status [—nodes]
     [—adminpassword=password | —adminpasswordfile=filename ]
     [—agent=ma_url] [dbname]
```

Description Use the `hadbm status` command to get the current state of the database. The state can be one of the following:

HA Fault Tolerant (HAFT)	The database has at least one spare node on each DRU.
Fault Tolerant (FT)	All mirrored node pairs are up and running.
Operational (O)	One node in each mirrored node pair is up and running.
Non-operational (NO)	One or more mirrored node pair is missing both nodes. An arbitrary SQL transaction may not succeed.
Stopped (S)	No nodes are running.
Unknown (U)	Unable to determine the state of the database.

If a database is named, it must already exist. If a database is not named, the default database is used. The default database is hadb.

Options

`-n —nodes`	If specified, displays the node status information. The following information is displayed for each node in the database: ■ Node number ■ Name of the machine where the node is running ■ Port number of the node ■ Role of the node ■ State of the node ■ Number of the corresponding mirror node
`–w —adminpassword`	The actual HADBM administation password.
`–W —adminpasswordfile`	The file containing the HADBM administration password. The adminstration password is defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–m —agent`	Identifies the URL to the Management Agent. The default is localhost:1862.

Operands

dbname	The name of the database. The default database is hadb.

Examples **EXAMPLE 1** Using status

```
hadbm status
Database Status
hadb HAFaultTolerant
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22002	specified database does not exist

See Also hadbm-clear(1), hadbm-clearhistory(1), hadbm-delete(1), hadbm-list(1), hadbm-restart(1), hadbm-resourceinfo(1), hadbm-start(1), hadbm-stop(1),

Name hadbm stop – gracefully stops the database

Synopsis

```
hadbm stop [—adminpassword=password | —adminpasswordfile=filename ]
     [—agent=ma_url] [dbname]
```

Description Use the `hadbm stop` command to stop the database gracefully. It is a good practice to stop the database if some maintenance activity is planned that affects the mirror nodes simultaneously. The data is intact in a database that is stopped gracefully, in contrast to the one that has not been stopped gracefully. Once you stop the database using the `hadbm stop` command, use the `hadbm start` command to start the database. If the database name is specified, the named database must exist. If the database name is not identified, the default database is used. The default database is hadb.

In interactive mode, the `hadbm stop` command prompts for a confirmation before stopping the node.

Options

`–w —adminpassword`	The actual HADBM administation password.
`–W —adminpasswordfile`	The file containing the HADBM administration password. The adminstration password is defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
`–m —agent`	Identifies the URL to the Management Agent. The default is localhost:1862.

Operands

dbname	The name of the database. The default database is hadb.

Examples **EXAMPLE 1** Using stop with a database identified

```
hadbm stop mydatabase
This command will stop the named database.
Type "yes" or "y" to confirm this operation, anything else to cancel: y
Database successfully stopped
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22002	specified database does not exist
22101	database could not be stopped
22102	database is already in a stopped state
22103	database is not fully stopped

See Also `hadbm-addnodes(1)`, `hadbm-clear(1)`, `hadbm-delete(1)`, `hadbm-list(1)`, `hadbm-refragment(1)`, `hadbm-restart(1)`, `hadbm-start(1)`, `hadbm-status(1)`

Name hadbm stopnode – gracefully stops the specified node

Synopsis

```
hadbm stopnode [—adminpassword=password | —adminpasswordfile=filename ]
    [—agent=ma_url] [—no-repair] node_number [dbname]
```

Description The `hadbm stopnode` command stops the node gracefully. The mirror node of the node that is to be stopped must be running. If a node's mirror node is not up, the node will not be stopped and an error message is displayed. By default, a spare node can replace the stopped node by copying the data from the stopped node's mirror. If there is no spare available, an error message is displayed.

In interactive mode, the `hadbm stopnode` command prompts for a confirmation before stopping the node.

Options

–w —adminpassword	The actual HADBM administation password.
–W —adminpasswordfile	The file containing the HADBM administration password. The adminstration password is defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
–m —agent	Identifies the URL to the Management Agent. The default is localhost:1862.
–R —no-repair	If specified, a spare will not replace the stopping node.

Operands

node_number	A positive integer. The node number of the node to be stopped.
dbname	The name of the database. The default database is hadb.

Examples

EXAMPLE 1 Using stopnode

```
hadbm stopnode 1
This command will stop the node.
Type "yes" or "y" to confirm this operation, anything else to cancel: y
Node successfully stopped
```

EXAMPLE 2 Using stopnode with no-repair option

```
hadbm stopnode --no-repair 1 mydatabase
This command will stop the node.
Type "yes" or "y" to confirm this operation, anything else to cancel: y
hadbm:Info 22202 Repair was not initiated while stopping the node {0}.
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22002	specified database does not exist

22085	no spare to pickup (if —no-repair is specified)
22086	node could not be stopped
22087	no mirror node
22088	node is not running
22202	repair not initiated

See Also hadbm-get(1), hadbm-clear(1), hadbm-addnodes(1), hadbm-restartnode(1), hadbm-start(1), hadbm-startnode(1), hadbm-stop(1)

Name hadbm unregisterpackage – removes registered HADB packages from the management domain

Synopsis

```
hadbm unregisterpackage [—hosts=hostlist]
      [—adminpassword=password | —adminpasswordfile=filename ]
      [—agent=ma_url] [—no-repair] [package_name]
```

Description Use the `hadbm unregisterpackage` command to remove the HADB packages that are registered with the management domain. The default package name is a string starting with V and containing the version number of the hadbm program. If the —`hosts` option is omitted, the hostlist defaults to the enabled hosts where the package is registered.

Before using the `hadbm unregisterpackage` command, ensure that all management agents are configured and running on all the hosts in the hostlist, the management agent's repository is available for updates, the package is registered in the management domain, and no existing databases are configured to run on the package about to be unregistered.

Options

–H—`hosts`	A comma-separated or double quote enclosed space separated list of hosts to register the package on.
–w —`adminpassword`	The actual HADBM administation password.
–W —`adminpasswordfile`	The file containing the HADBM administration password. The adminstration password is defined in the following form: HADBM_ADMINPASSWORD=*password*. Where *password* is the actual administrator password.
–m —`agent`	Identifies the URL to the Management Agent. The default is localhost:1862.

Operands

package_name	The name of the package you wish to remove from the domain.

Examples

EXAMPLE 1 Unregistering a software package named v4

```
hadbm unregisterpackage v4
Package successfully unregistered
```

EXAMPLE 2 Unregistering a software package named v4 from specific hosts in the domain

```
hadbm unregisterpackage --hosts=host1,host2,host3 v4
Package successfully unregistered
```

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

22172	the software package is not registered in the domain
22173	the software package is in use by a database instance and cannot be removed

See Also hadbm(1m), hadbm-registerpackage(1), hadbm-list-packages(1)

Name hadbm version – displays the `hadbm` version information

Synopsis **`hadbm version`**

Description The `hadbm version` command to display the HADB version information.

Examples **EXAMPLE 1** Using version

```
hadbm version
Sun Java System High Availability Database 4.4 Management Client <version> (<platform>)
Copyright 2004 Sun Microsystems, Inc. All rights reserved
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `hadbm-help(1)`

Name help – displays the asadmin utility commands

Synopsis **`help`** [*or* —`help`]

Description 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` *command_name* ––help or `asadmin help` *command_name*.

The following is a list of all the `asadmin` utility commands:

add-resources	registers the resource in the XML file specified
backup-domain	performs a backup on the domain
change-master-password	changes the master password
clear-ha-store	deletes tables in the HA database
configure-ha-cluster	configures an existing cluster to be High Availability
configure-ha-persistence	enables configuration of parameters related to session persistence
copy-config	copies an existing configuration to create a new configuration
create-admin-object	adds the administered object with the specified JNDI name
create-application-ref	creates a reference to an application
create-audit-module	creates an audit module for the optional plugin module
create-auth-realm	adds the new authorized realm
create-cluster	creates a cluster
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-ha-store	creates tables in HA database that are used by HA cluster
create-http-health-checker	creates a health-checker for a specified load balancer configuration
create-http-lb-config	creates a configuration for the load balancer
create-http-lb-ref	add an existing cluster or server instance to an existing load balancer configuration
create-http-listener	adds a new HTTP listener socket
create-iiop-listener	adds the IIOP listener
create-instance	creates an instance with the given name
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-host	creates a JMS host
create-jms-resource	registers the JMS resource
create-jmsdest	adds the named destination
create-jndi-resource	registers the JNDI resource
create-jvm-options	creates the JVM options from the Java configuration or profiler elements
create-lifecycle-module	adds a lifecycle module
create-message-security-provider	enables administrators to create the `message-security-config` and `provider-config` sub-elements for the security service in `domain.xml`
create-node-agent	creates a node agent and its associated directory structure
create-node-agent-config	adds a new unbound node agent to a domain
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-resource-ref	creates a reference to a resource
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-application-ref	removes a reference to an application
delete-audit-module	deletes the audit-module for the optional plugin module
delete-auth-realm	removes the named authorized realm
delete-cluster	deletes a cluster
delete-config	deletes an existing configuration
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-health-checker	deletes a health-checker for a specified load balancer configuration
delete-http-lb-config	deletes a load balancer configuration
delete-http-lb-ref	deletes the cluster or server instance from a load balancer configuration
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-host	removes a JMS host
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-node-agent	deletes the node agent and its associated directory structure
delete-node-agent-config	removes a node agent from a domain
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-resource-ref	removes a reference to a resource
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

disable-http-lb-application	disables an application managed by a load balancer
disable-http-lb-server	disables a sever or cluster managed by a load balancer
enable	runs the component
enable-http-lb-application	enables a previously-disabled application managed by a load balancer
enable-http-lb-server	enables a previously disabled sever or cluster managed by a load balancer
export	marks a variable name for automatic export to the environment of subsequent commands in multimode
export-http-lb-config	exports the load balancer configuration to a file that can be used by the load balancer
freeze-transaction-service	immobilizes the named transaction service
get	gets the values of the monitorable or configurable attributes
get-client-stubs	gets the stubs of the client
help	displays a list of all the commands available in the Command-line interface
jms-ping	checks to see if the JMS provider is up and running
list	lists the configurable elements
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-backups	lists all backups and restores
list-clusters	lists the existing clusters
list-configs	lists all existing configurations
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-lb-configs	lists load balancer configurations
list-http-listeners	gets the HTTP listeners
list-iiop-listeners	gets the IIOP listeners
list-instances	lists all the instances in the server
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-hosts	lists the existing JMS hosts
list-jms-resources	gets all 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-node-agents	lists the node agents along with their status
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-resource-refs	lists the existing resource references

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
migrate-timers	moves a timer when a server instance stops
multimode	allows you to execute multiple commands while returning environment settings and remaining in the `asadmin` utility
ping-connection-pool	tests if a connection pool is usable
recover-transactions	manually recovers pending transactions
rollback-transaction	rollsback the named transaction
remove-ha-cluster	returns an HA cluster to non-HA status
restore-domain	restores files from backup
set	sets the values of attributes
show-component-status	displays the status of the deployed component
start-cluster	starts a cluster
start-database	starts the bundled Derby database
start-domain	starts the given domain
start-instance	starts a server instance
start-node-agent	starts a node agent
stop-cluster	stops a cluster
stop-database	stops the bundled Derby database
stop-domain	stops the given domain
stop-instance	stops a server instance
stop-node-agent	stops a node agent
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 `domain.xml`
version	displays the version information

The following commands are deprecated:

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

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 **EXAMPLE 1** Using install-license

```
asadmin> install-license
LICENSE agreement will be displayed.
Do you agree with the terms of this license [YES|NO] YES
Enter license key> ********
Installed the license
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `display-license(1)`, `version(1)`

Name jms-ping – checks to see if the JMS service is up and running

Synopsis

```
jms-ping —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [target]
```

Description The `jms-ping` 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.

The `jms-ping` 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.

This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
Operands	*target*	In Enterprise Edition, this operand specifies the target for which the operation is to be performed. Valid values are: ■ `server`, which pings the JMS service for the default server instance `server` and is the default value ■ *configuration_name*, which pings the JMS service for all clusters using the specified configuration ■ *cluster_name*, which pings the JMS service for the specified cluster ■ *instance_name*, which pings the JMS service for a particular server instance

Examples EXAMPLE 1 Using the jms-ping command

The following command checks to see if the JMS service is running on the server instance `server1`:

```
asadmin> jms-ping --user admin
--passwordfile passwords.txt --host bluestar --port 4848
server1
JMS Ping Status=RUNNING
Command jms-ping executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-jmsdest(1)`, `create-jms-resource(1)`

Name jspc – precompiles JSP source files into servlets

Synopsis **jspc** [*options*]*jsp_files* **or jspc** [*options*]-webapp *dir*

Description 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.

Options

jsp_files	one or more JSP files to be compiled.
-webapp *dir*	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 *dir*	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 *name*	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 *name*	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 *dir*	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 *dir*	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.
`-mapped`	generates separate `write()` calls for each HTML line and comments that describe the location of each line in the JSP file. By default, all adjacent `write()` calls are combined and no location comments are generated.
`-die` [*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.
`-webinc` *file*	creates partial servlet mappings for the `-webapp` option, which can be pasted into a `web.xml` file.
`-webxml` *file*	creates an entire `web.xml` file for the `-webapp` option.
`-classpath` *path*	Override the system classpath with the specified classpath.
`-ieplugin` *class_id*	specifies the Java plugin COM class ID for Internet Explorer. Used by the `jsp:plugin` tags.
`-xpoweredBy`	Adds an `X-Powered-By` HTTP response header.
`-trimSpaces`	Trim spaces in template text between actions and directives.
`-help`	Print a summary of they 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 comand 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
```

EXAMPLE 1 Using jspc to compile the JSP pages in a Web application *(Continued)*

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`.

See Also `asadmin(1M)`

Name list – lists the configurable elements

Synopsis **`list`** —`user` *admin_user* [—`passwordfile` *filename*] [—`host` *localhost*] [—`port` *4849*] [—`secure`|–`s`] [—`terse`=*false*] [—`echo`=*false*] [—`interactive`=*true*] [—`help`] [—`monitor`=*[true|false]*] [*dotted_parent_attribute_name*]

Description Lists the configurable element. On Solaris, quotes are needed when executing commands with * as the option value or operand.

The dotted notation follows these guidelines:

- Any `list` command that has a dotted name that is not followed by a wildcard (*) will get, as its result, the current node's immediate children. For example, `list --monitor server` lists all immediate children belonging to the server node.
- Any `list` command that has a dotted name followed by a wildcard(*) will get, as its result, a hierarchical tree of children nodes from the current node. For example, `list --monitor server.applications.*` will list all children of applications and their subsequent child nodes and so on.
- Any `list` command that has a dotted name preceded or followed by a wildcard (*) of the form **dotted name* or *dotted * name* or *dotted name** will get, as its result, all nodes and their children matching the regular expression created by the provided matching pattern.

An application server dotted name uses the "`.`" (period) as a delimiter to separate the parts of a complete name. This is similar to how the "`/`" character is used to delimit the levels in the absolute path name of a file in the UNIX file system. The following rules apply while forming the dotted names accepted by the `get`, `set` and `list` commands. Note that a specific command has some additional semantics applied.

- A `.` (period) always separates two sequential parts of the name.
- A part of the name usually identifies an application server subsystem and/or its specific instance. For example: web-container, log-service, thread-pool-1 etc.
- If any part of the name itself contains a `.` (period), then it must be escaped with a leading `\` (backslash) so that the "`.`" does not act like a delimiter.
- An * (asterisk) can be used anywhere in the dotted name and it acts like the wildcard character in regular expressions. Additionally, an * can collapse all the parts of the dotted name. Long dotted name like "`this.is.really.long.hierarchy`" can be abbreviated to "`th*.hierarchy`". But note that the `.` always delimits the parts of the name.
- The top level switch for any dotted name is `-–monitor` or –`m` that is separately specified on a given command line. The presence or lack of this switch implies the selection of one of the two hierarchies for appserver management: monitoring and configuration.
- If you happen to know the exact complete dotted name without any wildcard character, then list and get/set have a little difference in their semantics:

- The `list` command treats this complete dotted name as the complete name of a parent node in the abstract hierarchy. Upon providing this name to `list` command, it simply returns the names of the immediate children at that level. For example, `list server.applications.web-module` will list all the web modules deployed to the domain or the default server.
- The `get` and `set` commands treat this complete dotted name as the fully qualified name of the attribute of a node (whose dotted name itself is the name that you get when you remove the last part of this dotted name) and it gets/sets the value of that attribute. This is true if such an attribute exists. You will never start with this case because in order to find out the names of attributes of a particular node in the hierarchy, you must use the wildcard character *. For example, `server.applications.web-module.JSPWiki.context-root` will return the context-root of the web-application deployed to the domain or default server.

- If you are using the Enterprise Edition of the Application Server, then "`server`" (usually the first part of the complete dotted name) can be replaced with the name of a particular server instance of interest (e.g., `server1`) and you'll get the information of that server instance, remaining part of the dotted name remaining the same. Note that the dotted names that are available in such other server instances are those from the monitoring hierarchy because these server instances don't have a way to expose the configuration hierarchy.

The `list` command is the progenitor of navigational capabilities of these three commands. If you want to `set` or `get` attributes of a particular application server subsystem, you must know its dotted name. The `list` command is the one which can guide you to find the dotted name of that subsystem. For example, to find out the modified date (attribute) of a particular file in a large file system that starts with `/`. First you must find out the location of that file in the file system, and then look at its attributes. Therefor, two of the first commands to understand the hierarchies in appserver are: * `list "*"` and * `list * --monitor`. The sorted output of these commands is typically of the following form:

Command	Output
`list *`	■ default-config ■ default-config.admin-service ■ default-config.admin-service.das-config ■ default-config.admin-service.jmx-connector.system ■ default-config.admin-service.jmx-connector.system.ssl ■ default-config.availability-service ■ default-config.availability-service.jms-availability ■ default-config.ejb-container ■ . . . ■ default-config.http-service.http-listener.http-listener-1 ■ default-config.http-service.http-listener.http-listener-2 ■ . . . ■ default-config.iiop-service ■ . . . ■ default-config.java-config ■ . . . ■ domain ■ domain.clusters ■ domain.configs ■ domain.resources ■ domain.resources.jdbc-connection-pool.DerbyPool ■ domain.resources.jdbc-connection-pool._CallFlowPool ■ domain.resources.jdbc-connection-pool._TimerPool ■ . . . ■ server ■ server-config ■ cerver-config.admin-service ■ server-config.admin-service.das-config ■ server-config.admin-service.jmx-connector.system ■ server-config.admin-service.jmx-connector.system.ssl ■ server-config-availability-servicce ■ server-config.availability-service.jms-availability ■ server-config.ejb-container ■ . . . ■ server.log-service ■ server.log-service.module-log-levels ■ . . . ■ server.session-config ■ server.session-config.session-manager ■ server.session-config.session-manager.manager-properties ■ server.session-config.session-manager.store-properties ■ server.session-config.session-properties ■ server.thread-pools ■ server.thread-pools.thread-pool.thread-pool-1 ■ server.transaction-service ■ server.web-container ■ server.web-container-availability

Command	Output
`list --monitor *`	■ `server` ■ `server.applications` ■ `server.applications._JWSappclients` ■ `server.applications._JWSappclients.sys\.war` ■ `server.applications.adminapp` ■ `server.applications.admingui` ■ `server.connector-service` ■ `server.http-service` ■ `server.http-service.server` ■ `server.jms-service` ■ `server.jvm` ■ `server.orb` ■ `server.orb.connection-managers` ■ `server.resources` ■ `server.thread-pools`

Consequently, the `list` command is the entry point into the navigation of the application server's s management hierarchies. Take note of the output of the `list` command:

- The output lists one element per line.
- Every element on a line is a complete-dotted-name of a management component that is capable of having attributes. Note that none of these lines show any kind of attributes at all.

The output of the`list` command is a list of dotted names representing individual application server components and subsystems. Every component or subsystem is capable of having zero or more attributes that can be read and modified.

With the`list` command you can drill down through the hierarchy in a particular branch of interest. For example, if you want to find the configuration of the `http-listener` of the domain (the default server, whose ID is "`server`"). Here is how you could proceed on a UNIX terminal:

ID	Command	Output/Comment
1	`list "*" | grep http | grep listener`	1. `default-config.http-service.http-listener.http-liste` 2. `default-config.http-service.http-listener.http-liste` 3. `server-config.http-service.http-listener.admin-liste` 4. `server-config.http-service.http-listener.http-listen` 5. `server-config.http-service.http-listener.http-listen` 6. `server-http-service.http-listener.admin-listener` 7. *server.http-service.http-listener.http-listener-1* 8. `server.http-service.http-listener.http-listener-2`
2	To find the listener that corresponds to the default `http-listener` where the web applications in the `domain/server` are deployed: 1. Examine the dotted name starting with item number 7 in above output. 2. Use the `get` command as shown in its usage. For example, `get server.http-service.http-listener.http-listener-1.*` will return all the attributes of the `http-listener` in context.	server.http-service.http-listener.http-listener-1.acceptor-threads = 1server.http-service.http-listener.http-listener-1.address = 0.0.0.0server.http-service.http-listener.http-listener-1.blocking-ena = falseserver.http-service.http-listener.http-listener-1.default-virtual- = serverserver.http-service.http-listener.http-listener-1.enabled = trueserver.http-service.http-listener.http-listener-1.external-port =server.http-service.http-listener.http-listener-1.family = inetserver.http-service.http-listener.http-listener-1.id = http-listener-1server.http-service.http-listener.http-listener-1.port = 8080server.http-service.http-listener.http-listener-1.redirect-port =server.http-service.http-listener.http-listener-1.security-enabled = falseserver.http-service.http-listener.http-listener-1.server-name =server.http-service.http-listener.http-listener-1.xpowered-by = true

Making use of both `list` and `get` commands, it is straightforward to reach a particular component of interest.

To get the monitoring information of a particular subsystem you must:

1. Use the `set` command to set an appropriate monitoring level for the component of interest.
2. Obtain the various information about the JVM that the application server domain is running.

ID	Command	Output/Comment
1	`list server* | grep monitoring`	server-config.monitoring-service server-config.monitoring-service.module-monitoring-levels server.monitoring-serviceserver.monitoring-service.module-monitoring-l Note that this is the `list` command. It only shows the hierarchy, nothing else. Using the '|' and "grep" narrows down the search effectively. Now, you can choose `server.monitoring-service` to set the attributes of various attributes that can be monitored. This is the configuration data because this setting will be persisted to the server's configuration store.
2	`get server.monitoring-service.*`	You can try the number of attributes that are presently available with monitoring service. Here is the output: No matches resulted from the wildcard expression. This is because this fully dotted name does not have any attributes at all. Logically, you try the next one and that is: `server.monitoring-service.module-monitoring-levels`. Again, use the wildcard character to get ALL the attributes of a particular component.

ID	Command	Output/Comment
3	`get server.monitoring-service.module-monitoring-levels.*`	server.monitoring-service.module-monitoring-levels.connector-co = OFF server.monitoring-service.module-monitoring-levels.connector-se = OFF server.monitoring-service.module-monitoring-levels.ejb-containe = OFF server.monitoring-service.module-monitoring-levels.http-service = OFF server.monitoring-service.module-monitoring-levels.jdbc-connect = OFF server.monitoring-service.module-monitoring-levels.jms-service = OFF server.monitoring-service.module-monitoring-levels.jvm = OFF server.monitoring-service.module-monitoring-levels.orb = OFF server.monitoring-service.module-monitoring-levels.thread-pool = OFF server.monitoring-service.module-monitoring-levels.transaction-s = OFF server.monitoring-service.module-monitoring-levels.web-containe = OFF The JVM monitoring is at a level OFF. It must be changed in order to make the JVM monitoring information available. The other valid values for all the monitoring level are: LOW and HIGH. use the `set` command to set the value appropriately.
4	`set server.monitoring-service. module-monitoring-levels.jvm=HIGH` There is no space before or after the = sign.	server.monitoring-service.module-monitoring-levels.jvm = HIGH Now, the JVM information can be obtained using the `get` command and monitoring switch. But remember , when you switch to the monitoring hierarchy, start with the `list` command again.

ID	Command	Output/Comment
5	`list --monitor * | grep jvm`	server.jvm server.jvm.class-loading-system server.jvm.compilation-system server.jvm.garbage-collectors server.jvm.garbage-collectors.Copy server.jvm.garbage-collectors.MarkSweepCompact server.jvm.memory server.jvm.operating-system server.jvm.runtime server.jvm.thread-system server.jvm.thread-system.thread-1 . . . server.jvm.thread-system.thread-793823 server.jvm.thread-system.thread-793824 server.jvm.thread-system.thread-793825 server.jvm.thread-system.thread-793826 server.jvm.thread-system.thread-793827 server.jvm.thread-system.thread-9 The JRE 1.5.0 monitorable components are exposed in an elegant manner. This is what you see when connected by the JConsole. Now, to know more about the class-loading system in the JVM, this is how you'll proceed. Note that now you are interested in the attributes of a particular leaf node. Thus the command is `get` not `list`.

ID	Command	Output/Comment
6	`get --monitor server.jvm.class-loading-system.*`	server.jvm.class-loading-system.dotted-name = server.jvm.class-loading-system server.jvm.class-loading-system.loadedclasscount-count = 7328 server.jvm.class-loading-system.loadedclasscount-description = No Description was available server.jvm.class-loading-system.loadedclasscount-lastsampletime = 1133819508973 server.jvm.class-loading-system.loadedclasscount-name = LoadedClassCount? server.jvm.class-loading-system.loadedclasscount-starttime = 1133819131268 server.jvm.class-loading-system.loadedclasscount-unit = count server.jvm.class-loading-system.totalloadedclasscount-count = 10285 server.jvm.class-loading-system.totalloadedclasscount-description = No Description was available server.jvm.class-loading-system.totalloadedclasscount-lastsampleti = 1133819508972 server.jvm.class-loading-system.totalloadedclasscount-name = TotalLoadedClassCount? server.jvm.class-loading-system.totalloadedclasscount-starttime = 1133819131268 server.jvm.class-loading-system.totalloadedclasscount-unit = count server.jvm.class-loading-system.unloadedclasscount-count = 2957 server.jvm.class-loading-system.unloadedclasscount-description = No Description was available server.jvm.class-loading-system.unloadedclasscount-lastsampletim = 1133819508973 server.jvm.class-loading-system.unloadedclasscount-name = UnloadedClassCount? server.jvm.class-loading-system.unloadedclasscount-starttime = 1133819131268 server.jvm.class-loading-system.unloadedclasscount-unit = count You cansee that 10285 is the total number of classes loaded by the Virtual Machine. Whereas, 2957 is number of classes unloaded, since it was started. ,Similarly, you can explore attributes of the other subsystems as well.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
	–H —host	The machine name where the domain administration server is running. The default value is localhost.
	–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
	–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—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
server.iiop-service.orb
server.java-config
server.jms-service
server.jms-service.jms-host.default_JMS_host
server.log-service
server.log-service.module-log-levels
server.mdb-container
server.monitoring-service
server.monitoring-service.module-monitoring-levels
server.resource-ref.jdbc/PointBase
server.resource-ref.jdbc/__TimerPool
server.resources
server.resources.jdbc-connection-pool.PointBasePool
server.resources.jdbc-connection-pool.__TimerPool
server.resources.jdbc-resource.jdbc/PointBase
server.resources.jdbc-resource.jdbc/__TimerPool
server.security-service
server.security-service.audit-module.default
server.security-service.auth-realm.certificate
```

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

```
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.adminguip
server.applications.web-module.com_sun_web_ui
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `get(1)`, `set(1)`

Name list-acls – gets the access control lists

Synopsis

```
list-acls --user admin_user[--password admin_password][--host localhost]
     [--port 4848][--passwordfile filename][--secure|-s]instance_name
```

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).

Operands

instance_name	name of the instance.

Examples EXAMPLE 1 Using list-acls

```
asadmin> list-acls --user admin --password adminadmin --host fuyako --port 7070 server1
acl1
sampleACL
```

Where: `acl1` and `sampleACL` are the names of the ACLs listed.

Exit Status

0	command executed successfully
1	error in executing the command

Interface Equivalent Access Control List page

See Also `create-acl(1)`, `delete-acl(1)`

Name list-admin-objects – gets all the administered objects

Synopsis —user *admin_user* [—passwordfile *filename*] [—host *localhost*] [—port *4849*] [—secure|–s] [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—help] [*target*]

Description This command lists all the administered objects. This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
Operands	`––target`	Specifies the target on which you are creating the administered object.This option is available only in the Sun Java System Application Server Standard and Enterprise Edition. Valid values are ■ `server`, which creates the administered object for the default server instance `server` and is the default value ■ *configuration_name*, which creates the administered object for the named configuration ■ *cluster_name*, which creates the administered object for every server instance in the cluster ■ *instance_name*, which creates the administered object for a particular server instance

Examples **EXAMPLE 1** Using list-admin-objects

```
asadmin> list-admin-objects --user admin --passwordfile passwords.txt instance1
Command list-admin-objects executed successfully
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-admin-object(1)`, `delete-admin-object(1)`

Name list-application-refs – lists the existing application references

Synopsis

```
list-application-refs —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [target]
```

Description The `list-application-refs` command lists all application references in a cluster or an unclustered server instance. This effectively lists all the modules deployed on the specified target (for example, J2EE applications, Web modules, and enterprise bean modules).

The target instance or instances making up the cluster need not be running or available for this command to succeed.

This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
Operands	*target*	The target for which you are listing the application references. Valid values are ■ `server`, which lists the application references for the default server instance `server` and is the default value ■ *cluster_name*, which lists the application references for every server instance in the cluster ■ *instance_name*, which lists the application references for the named unclustered server instance

Examples **EXAMPLE 1** Using the list-application-refs command

The following command lists the application references for the unclustered server instance `NewServer`.

```
asadmin> list-application-refs --user admin2
--passwordfile passwords.txt NewServer
ClientSessionMDBApp
MEjbApp
__ejb_container_timer_app
Command list-application-refs executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `create-application-ref(1)`, `delete-application-ref(1)`

Name list-audit-modules – gets all audit modules and displays them

Synopsis

```
list-audit-modules —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [target]
```

Description Lists all the audit modules. This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
Operands	*target*	In Enterprise Edition, specifies the target on which you are listing the audit modules. Valid values are ■ `server`, which lists the audit modules for the default server instance `server` and is the default value ■ *configuration_name*, which lists the audit modules for the named configuration ■ *cluster_name*, which lists the audit modules for every server instance in the cluster ■ *instance_name*, which lists the audit modules for a particular server instance

Examples **EXAMPLE 1** Using list-audit-modules

```
asadmin> list-audit-modules --user admin1
--passwordfile passwords.txt --host pigeon --port 5001
sampleAUditModule1
sampleAuditModule2
Command list-audit-modules executed successfully
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-audit-module(1)`, `delete-audit-module(1)`

Name list-auth-realms – lists the authentication realms

Synopsis

```
list-auth-realms —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [target_name]
```

Description Lists the authentication realms. This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.

Operands

target_name	name of the target on which you want to list the authentication realms. ■ `server`, which lists the realms for the default server instance `server` and is the default value ■ *configuration_name*, which lists the realms for the named configuration ■ *cluster_name*, which lists the realms for every server instance in the cluster ■ *instance_name*, which lists the realms for a particular server instance

Examples

EXAMPLE 1 Using list-auth-realms

```
asadmin> list-auth-realms --user admin --passwordfile password.txt
--host localhost --port 4848
file
ldap
certificate
db
Command list-auth-realms executed successfully
```

Where file, ldap, certificate, and db are the listed authentication realms.

Exit Status

0	command executed successfully
1	error in executing the command

See Also `create-auth-realm(1)`, `delete-auth-realm(1)`

Name list-backups – lists all backups.

Synopsis
```
list-backups [—domaindir domain_directory] [—description description]
     [—terse=false] [—verbose=false] domain_name
```

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

domain_name	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 **EXAMPLE 1** Using list-backups

```
asadmin>list-backups --domaindir /usr/appserver90pe/domains/domain1 domain1
Description: 1137030607263
Backup Filename: /opt/SUNWappserver/nondefaultdomaindir/domain1/backups/sjsas_backup_v00001.zip
Date and time backup was performed: Wed Jan 11 17:50:07 PST 2006
Domains Directory: /opt/SUNWappserver/nondefaultdomaindir
Domain Directory: /opt/SUNWappserver/nondefaultdomaindir/domain1
Domain Name: domain1
Name of the user that performed the backup: jondoe
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)`

Name list-clusters – lists the existing clusters

Synopsis

```
list-clusters —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [target]
```

Description The `list-clusters` command lists the existing clusters and the cluster status.

This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
Operands	*target*	Specifies the target for which the clusters are to be listed. Valid values are: ■ `domain`, which lists all clusters in the domain and is the default value ■ *cluster_name*, which lists the named cluster ■ *instance_name*, which lists the cluster associated with the clustered server instance. Unlike many of the other uses of *instance_name*, this is one situation where an unclustered instance cannot be specified. ■ *node_agent_name*, which lists all clusters associated with the named node agent. For example, if `agent1` manages `server1` and `server2`, which are part of `cluster1` and `cluster2`, then `cluster1` and `cluster2` will be listed.

Examples **EXAMPLE 1** Using the list-clusters command

The following command lists all clusters in the current domain.

```
asadmin> list-clusters --user admin1
--passwordfile passwords.txt
MyCluster not running
Command list-clusters executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-cluster(1)`, `delete-cluster(1)`, `start-cluster(1)`, `stop-cluster(1)`

Name list-components – lists deployed components

Synopsis

```
list-components —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—type application|ejb|web|connector|webservice]
    [target]
```

Description The command `list-components` lists all deployed J2EE components. If the —`type` option is not specified, all components are listed. The available type values are: `application` (default), `ejb`, `web`, and `connector`. This command is supported in remote mode only.

Options

–u —`user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —`host`	The machine name where the domain administration server is running. The default value is localhost.
–p —`port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —`secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
	`––type`	Specifies the type of component to be listed. The options are application, ejb, web, connector and webservice. 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 values are: ■ `server`, which lists the components for the default server instance `server` and is the default value ■ *domain_name*, which lists the components for the named domain ■ *cluster_name*, which lists the components for every server instance in the cluster ■ *instance_name*, which lists the components for a particular server instance This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

Examples

EXAMPLE 1 Using `list-components` command

```
asadmin> list-components --user admin --passwordfile password.txt --type connector
cciblackbox-tx connector-module
Command list-components executed successfully
```

Note: `cciblackbox-tx.rar` was deployed.

Exit Status

0	command executed successfully
1	error in executing the command

See Also `show-component-status(1)`, `list-sub-components(1)`

Name list-configs – lists all existing configurations

Synopsis

```
list-configs —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [target]
```

Description Use the list—configs command to list all existing configurations in the `domain.xml` file.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
Operands	*target*	This operand specifies which configurations you can list. Valid values are: ■ `domain`, which lists the configurations in the current domain and is the default. ■ *cluster_name*, which lists the configurations referenced by a cluster. ■ *instance_name*, which lists the configuration referenced by a particular instance.

Examples **EXAMPLE 1** Using the list-configs command

```
asadmin> list-configs --user admin --passwordfile passwords.txt
server-config
default-config
my-config
Command list-configs executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `delete-config(1)`,`copy-config(1)`

Name list-connection—groups – gets the connection groups

Synopsis

```
list-connection-groups
      --user user_name --password password --host hostname --port admin_port_number
      --instance instance_name http_listener_ID
```

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.

http_listener_ID a unique identifier for the HTTP listener.

Examples

```
asadmin% list-connection-groups
```

Interface Equivalent unknown

See Also `create-connection-group(1)` `delete-connection-group(1)`

Name list-connector-connection-pools – gets connector connection pools that have been created

Synopsis

```
list-connector-connection-pools —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help]
```

Description Use this command to list connector connection pools that have been created.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—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

```
list-connector-resources —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target]
```

Description This command lists all connector resources.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
Operands	*target*	In Enterprise Edition only, this operand specifies which configurations you can list. Valid values are: ■ `server`, which lists the connector resources in the current domain and is the default. ■ `domain`, which lists the connector resources in the current domain. ■ *cluster_name*, which lists the connector resources in a cluster. ■ *instance_name*, which lists the connector resources for a particular instance.

Examples EXAMPLE 1 Using the list-connector-resources command

```
asadmin> list-connector-resources --user admin
--passwordfile --password --host instance1
--port 5001 target server
resource10
resource20
resource35
Command list-connector-resources executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-connector-resource(1)`,`delete-connector-resource(1)`

Name list-connector-security-map – lists the security maps belonging to the specified connector connection pool

Synopsis

```
list-connector-security-maps —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—verbose=false]
    [—securitymap security_map_name] connector_connection_pool_name
```

Description Use this command to list the security maps belonging to the specified connector connection pool.

For this command to succeed, you must have first created a connector connection pool using the `create-connector-connection-pool` command.

This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—help	Displays the help text for the command.
—target	This option is deprecated in this release.
—verbose	This property returns a list including the identity, principals, and security name.
—securitymap	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.

Operands

connector_connection_pool_name	name of the connector connection pool for which you want to list security maps.

Examples

EXAMPLE 1 Using `list-connector-security-maps` with the security map option

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

```
asadmin> list-connector-security-maps --user admin
--passwordfile pwd_file --securitymap securityMap1 connector-Pool1
Command list-connector-security-maps executed successfully.
```

One security map (securityMap1) is listed for the `connector-Pool1` pool.

EXAMPLE 2 Using `list-connector-security-maps` without the security map option

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

```
asadmin> list-connector-security-maps --user admin --passwordfile pwd_file.txt connector-Pool
Command list-connector-security-maps executed successfully.
```

All security maps contained within `connector-Pool1` are listed.

Exit Status

0	command executed successfully
1	error in executing the command

See Also `delete-connector-security-map(1)`, `create-connector-security-map(1)`, `update-connector-security-map(1)`

Name list-custom-resources – gets all custom resources

Synopsis

```
list-custom-resources —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [target]
```

Description Use this command to list custom resources. This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
Operands	*target*	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 **EXAMPLE 1** Using the list-custom-resources command

```
asadmin> list-custom-resources --user admin --passwordfile filename
--host plum --port 4848 target6
custom_resource01
custom_resource02
Command list-custom-resources executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also create-custom-resource(1),delete-custom-resource(1)

Name list-domains – lists the domains in the specified domain directory

Synopsis **`list-domains`** [—domaindir *install_dir*/domains] [—terse=*false*] [—echo=*false*]

Description Use the `list-domains` command to list the domain. If the domain directory is not specified, the domain in the default *install_dir*/`domains` directory is listed. If there is more that one domain, the *domain_name* operand must be identified.

Options

—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 *install_dir*/`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.

Examples **EXAMPLE 1** Using the list-domains command

```
asadmin> list-domains
domain1 running
sampleDomain not running
Command list-domains executed successfully
```

Where: `domain1` and `sampleDomain` are the domains located in the default `install_dir/domains` directory.

Exit Status

0	command executed successfully
1	error in executing the command

See Also `create-domain(1)`, `delete-domain(1)`, `start-domain(1)`, `stop-domain(1)`,

Name list-file-groups – lists file groups

Synopsis

```
list-file-groups —user admin_user [—passwordfile filename] [—host localhost]
     [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
     [—interactive=true] [—help] [—name username] [target]
```

Description 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.

This command is supported in remote mode only.

Options

`—u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`—H —host`	The machine name where the domain administration server is running. The default value is localhost.
`—p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`—s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—-help	Displays the help text for the command.
	–name	identifies the name of file user to be created.
Operands	*target*	In Enterprise Edition, this operand specifies which configurations you can list. Valid values are: ■ `server`, which lists the file groups in the current server and is the default. ■ `domain`, which lists the file groups in the current domain. ■ *cluster_name*, which lists the file groups in a cluster. ■ *instance_name*, which lists the file groups for a particular instance.

Examples EXAMPLE 1 Using the list-file-groups command

```
asadmin> list-file-groups --user admin1 --password adminadmin1
--host pigeon --port 5001 --name sample_user
Command list-file-groups executed successfully
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-file-user(1)`, `update-file-user(1)`, `delete-file-user(1)`, `list-file-users(1)`

Name list-file-users – prints the list of file users in the specified authentication realm

Synopsis

```
list-file-users —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [target] [—authrealmname auth_realm_name]
```

Description The `list-file-users` command prints a list of file users supported by file realm authentication.

Options

`—u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`—H —host`	The machine name where the domain administration server is running. The default value is localhost.
`—p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`—s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—-help	Displays the help text for the command.
-—-target	in Enterprise Edition, specifies the target for which you want to print the list of file users. Valid values are ■ `server`, which prints the list of file users for the default server instance.This is the default value. ■ `domain`, which prints the list of file users for the domain. ■ *cluster_name*, which prints the list of file users for every server instance in the cluster. ■ *instance_name*, which prints the list of file users for a specified sever instance.
—-authrealmname	This is the file where the file users are stored.

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 --user admin --passwordfile passwords.txt --port 4849 myFileRealm
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—lb—configs – lists load balancer configurations

Synopsis

```
list-http-lb-configs —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [target]
```

Description Use the list-http-lb-configs command to list the load balancer configurations. List them all or list them by the cluster or server instance they reference.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
Operands	*target*	Lists the load balancers by target. Valid values are: ■ *cluster_name*, which lists the load balancer configurations for this cluster. ■ *instance_name*, which lists the load balancer configurations for this instance.

Examples

EXAMPLE 1 Using the list—http—lb—config command

```
asadmin> list-http-lb-configs --user admin --passwordfile file
mycluster-http-lb-config
serverinstlb
Command list-http-lb-configs executed successfully.
```

EXAMPLE 2 Using the list—http—lb—config command with the target operand.

```
asadmin> list-http-lb-configs --user admin --passwordfile file mycluster
mycluster-http-lb-config
Command list-http-lb-configs executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `delete-http-lb-config(1)`, `create-http-lb-config(1)`

Name list-http-listeners – lists the existing HTTP listeners

Synopsis

```
list-http-listeners —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [target]
```

Description The `list-http-listeners` command lists the existing HTTP listeners. This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
Operands	*target*	In Enterprise Edition, this operand specifies the target for which the HTTP listeners are to be listed. Valid values are: ■ `server`, which lists the listeners for the default server instance `server` and is the default value ■ *configuration_name*, which lists the listeners for the specified configuration ■ *cluster_name*, which lists the listeners for the specified cluster ■ *instance_name*, which lists the listeners for a particular server instance

Examples **EXAMPLE 1** Using the list-http-listeners command

The following command lists all the HTTP listeners for the server instance:

```
asadmin> 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.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-http-listener(1)`, `delete-http-listener(1)`

Name list-iiop-listeners – lists the existing IIOP listeners

Synopsis

```
list-iiop-listeners —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [target]
```

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 administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
Operands	*target*	In Enterprise Edition, this operand specifies the target for which the IIOP listeners are to be listed. Valid values are: ■ `server`, which lists the listeners in the default server instance `server` and is the default value ■ *configuration_name*, which lists the listeners in the specified configuration ■ *cluster_name*, which lists the listeners in the specified cluster ■ *instance_name*, which lists the listeners in a particular server instance

Examples **EXAMPLE 1** Using the list-iiop-listeners command

The following command lists all the IIOP listeners for the server instance:

```
asadmin> 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.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-iiop-listener(1)`, `delete-iiop-listener(1)`

Name list-instances – lists all the instances along with their status

Synopsis

```
list-instances —user admin_user —passwordfile filename [—host host_name]
    [—port port_number] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [target]
```

Description Use the `list-instances` to list all the instance in the server. The `list-instances` 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.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—-help	Displays the help text for the command.
Operands	*target*	This is the name of the target domain the instances you want listed are associated with.

Examples **EXAMPLE 1** Using list-instances in local mode

```
asadmin> list-instances --user admin --passwordfile passwords.txt instance1
instance1 running
Command list-instances executed successfully
```

Where: `instance1` is listed.

EXAMPLE 2 Using list-instances in remote mode

```
asadmin> list-instances --user admin --passwordfile passwords.txt
--host pigeon --port 4849
remote_instance1 running
Command list-instances executed successfully
```

Where: `remote-instance1` associates with user, passwordfile, host, and port of the remote machine.

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-instance(1)`, `stop-instance(1)`, `start-instance(1)`

Name list-javamail-resources – lists the existing JavaMail session resources

Synopsis

```
list-javamail-resources —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [target]
```

Description The command lists the existing JavaMail session resources. This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
Operands	*target*	In Enterprise Edition, this operand specifies the target for which the JavaMail session resources are to be listed. Valid values are: ■ `server`, which lists the resources for the default server instance `server` and is the default value ■ `domain`, which lists the resources for the domain ■ *cluster_name*, which lists the resources for the specified cluster ■ *instance_name*, which lists the resources for a particular server instance

Examples **EXAMPLE 1** Using the list-javamail-resources command

The following command lists the JavaMail session resources for the server instance:

```
asadmin> list-javamail-resources --user admin1
--passwordfile passwords.txt --host pigeon --port 5001
mail/MyMailSession
Command list-javamail-resources executed successfuly.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-javamail-resource(1)`, `delete-javamail-resource(1)`

Name list-jdbc-connection-pools – lists all JDBC connection pools

Synopsis

```
list-jdbc-connection-pools —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help]
```

Description Use this command to get the JDBC connection pools that have been created. This command is supported in remoted mode only.

Options

—u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
—H —host	The machine name where the domain administration server is running. The default value is localhost.
—p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
—s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—-help	Displays the help text for the command.
Operands	*target*	The target operand is deprecated.

Examples **EXAMPLE 1** Using the list-jdbc-connection-pools command

```
asadmin> list-jdbc-connection-pools --user admin --password adminadmin
--host plum --port 7070
my_connection_pool
```

Where: `my_connection_pool` is the JDBC connecction pool listed.

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-jdbc-connection-pool(1)`, `delete-jdbc-connection-pool(1)`

Name list-jdbc-resources – gets all JDBC resources

Synopsis

```
list-jdbc-resources —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] target
```

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

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
Operands	*target*	In Enterprise Edition, this operand specifies which jdbc resources you can list. Valid values are: ■ `server`, which lists the jdbc resources in the current server and is the default. ■ `domain`, which lists the jdbc resources in the current domain. ■ *cluster_name*, which lists the jdbc resources in a cluster. ■ *instance_name*, which lists the jdbc resources for a particular instance.

Examples **EXAMPLE 1** Using the list-jdbc-resources command

```
asadmin> list-jdbc-resources --user admin
--passwordfile secret.txt --host pigeon --port 5001 instance1
sample_jdbc_resource02
sample_jdbc_resource05
Command executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-jdbc-resource(1)`, `delete-jdbc-resource(1)`

Name list-jmsdest – lists the existing JMS physical destinations

Synopsis

```
list-jmsdest —user admin_user [—passwordfile filename] [—host localhost]
     [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
     [—interactive=true] [—help] [desttype type] [target]
```

Description The `list-jmsdest` command lists the JMS physical destinations. This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	––help	Displays the help text for the command.
	–T ––desttype	The type of JMS destinations to be listed. Valid values are `topic` and `queue`.
Operands	*target*	In Enterprise Edition, this operand specifies the target for which the physical destinations are to be listed. Although the `list-jmsdest` 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: ■ `server`, which lists the physical destinations for the default server instance `server` and is the default value ■ *configuration_name*, which lists the physical destinations for the specified configuration ■ *cluster_name*, which lists the physical destinations for the specified cluster ■ *instance_name*, which lists the physical destinations for a particular server instance

Examples **EXAMPLE 1** Using the list-jmsdest command

The following command lists all the physical destinations for the default server instance:

```
asadmin> list-jmsdest --user admin
--passwordfile passwords.txt --host bluestar --port 4848
PhysicalQueue queue {}
PhysicalTopic topic {}
Command list-jmsdest executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-jmsdest(1)`, `delete-jmsdest(1)`

Name list-jms-hosts – lists the existing JMS hosts

Synopsis

```
list-jms-hosts —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [target]
```

Description The `list-jms-hosts` command lists the existing JMS hosts for the JMS service. This command is supported in remote mode only.

Options

`—u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`—H —host`	The machine name where the domain administration server is running. The default value is localhost.
`—p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`—s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.

Operands

target	In Enterprise Edition, this operand specifies the target for which the JMS hosts are to be listed. Valid values are: ■ `server`, which lists the JMS hosts for the default server instance `server` and is the default value ■ *configuration_name*, which lists the JMS hosts for the specified configuration ■ *cluster_name*, which lists the JMS hosts for the specified cluster ■ *instance_name*, which lists the JMS hosts for a particular server instance

Examples

EXAMPLE 1 Using the list-jms-hosts command

The following command lists the JMS hosts for the server configuration.

```
asadmin> list-jms-hosts --user admin
--passwordfile passwords.txt server-config
default_JMS_host
MyNewHost
Command list-jms-hosts executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `create-jms-host(1)`, `delete-jms-host(1)`

Name list-jms-resources – lists the JMS resources

Synopsis

```
list-jms-resources —user admin_user [—passwordfile filename] [—host localhost]
     [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
     [—interactive=true] [—help] [—restype type] [target]
```

Description The `list-jms-resources` command lists the existing JMS resources (destination and connection factory resources). This command is supported in remote mode only.

Options

`—u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`—H —host`	The machine name where the domain administration server is running. The default value is localhost.
`—p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`—s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
	`––restype`	The JMS resource type, which can be either `javax.jms.Topic`, `javax.jms.Queue`, `javax.jms.ConnectionFactory`, `javax.jms.TopicConnectionFactory`, or `javax.jms.QueueConnectionFactory`.
Operands	*target*	In Enterprise Edition, this operand specifies the target for which the JMS resources are to be listed. Valid values are: ■ `server`, which lists the resources for the default server instance `server` and is the default value ■ `domain`, which lists the resources for the domain ■ *cluster_name*, which lists the resources for the specified cluster ■ *instance_name*, which lists the resources for a particular server instance

Examples **EXAMPLE 1** Using the list-jms-resources command to list all JMS resources

The following command lists all JMS resources:

```
asadmin> list-jms-resources --user admin1
--passwordfile passwords.txt
jms/Queue
jms/Topic
jms/QueueConnectionFactory
jms/DurableTopicConnectionFactory
Command list-jms-resources executed successfully.
```

EXAMPLE 2 Using the list-jms-resources command to list JMS resources of a specified type

The following command lists all topic connection factories:

```
asadmin> list-jms-resources --user admin1
--passwordfile passwords.txt --restype javax.jms.TopicConnectionFactory
jms/DurableTopicConnectionFactory
jms/TopicConnectionFactory
Command list-jms-resources executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

Name list-jndi-entries – browses and queries the JNDI tree

Synopsis

```
list-jndi-entries —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—context context_name] [—target]
```

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 administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
	—context	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 *ejb*) is specified, all those entries are returned.
Operands	*target*	In Enterprise Edition, this operand specifies which configurations you can list. Valid values are" server," "domain," cluster, or instance.

Examples EXAMPLE 1 Using the list-jndi-entries command

```
asadmin> list-jndi-entries --user admin1 --passwordfile adminadmin1
 --host plum --port 5001 target1
jndi_entry03
jndi_entry72
jndi_entry76
Command list-jndi-resources executed successfully
```

Exit Status

0 command executed successfully

1 error in executing the command

See Also create-jndi-resource(1), delete-jndi-resource(1)

Name list-jndi-resources – lists all existing JNDI resources

Synopsis

```
list-jndi-resources —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [target]
```

Description Use the list-jndi-resources command to identify all existing JNDI resources. This command is supported in remote mode only.

The target operand is only valid for Enterprise Edition.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
Operands	*target*	In Enterprise Edition, this operand specifies which jndi resources you can list. Valid values 'server,' 'domain,' cluster, instance. The default is server.

Examples **EXAMPLE 1** Using the list-jndi-resources command

```
asadmin> list-jndi-resources --user admin --passwordfile passwords.txt --host plum --port 484
jndi_resource1
jndi_resource2
jndi_resource3
Command list-jndi-resources executed successfully
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-jndi-resource(1)`, `delete-jndi-resource(1)`

Name list-lifecycle-modules – lists the lifecycle modules

Synopsis

```
list-lifecycle-modules —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [target]
```

Description Lists the lifecycle modules. The lifecycle modules provide ameans of running short or long duration Java-based tasks within the application server environment. This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	––help	Displays the help text for the command.
Operands	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 **EXAMPLE 1** 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 create-lifecycle-module(1), delete-lifecycle-module(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

```
list-message-security-providers —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] —layer message_layer [target]
```

Description Enables administrators to list all security message providers (`provider-config` sub-elements) for the given message layer (`message-security-config` element of `domain.xml`).

This command is supported in remote mode only.

Options 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.

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—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	*target*	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: ■ `server`, which deploys the component to the default server instance `server` and is the default value ■ *config*, which deploys the component to the domain. ■ *cluster*, which deploys the component to every server instance in the cluster. ■ *instance*, which deploys the component to a particular server instance.

Examples **EXAMPLE 1** Using list-message-security-providers

The following example shows how to list message security providers for a message layer.

```
asadmin> list-message-security-providers --user admin
--layer SOAP
Listing of all message security providers
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-message-security-provider(1)`, `delete-message-security-provider(1)`

Name list-node-agents – lists the node agents along with their status

Synopsis

```
list-node-agents —user user —passwordfile filename [—host localhost]
    [—port port_number] [—secure=false] [—terse=false] [—echo=false]
    [—interactive=true] [target]
```

Description The list-node-agents command displays the node agents along with their status (as an example, running or stopped). If the target is omitted, all node agents are listed.

Options

–u —user	The authorized domain application server administrative username.
—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 administration 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 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.
–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 4949.
–s —secure	If set to true, this command uses SSL/TLS to communicate with the domain application server. The default is false.
–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. The default is false.

	–e —echo	Setting this option to true will echo the command line statement on the standard output. The default is false.
	–I —interactive	If this option is set to true (default), the user will be prompted for the required password options.
Operands	*target*	This operand specifies which node agents are to be listed. The options are: ■ "domain" This is the default. Domain lists all of the node agents in the domain. ■ <cluster-name> This lists all of the node agents associated with the named cluster. ■ <instance-name> This lists all of the node agents associated with the named server instance. ■ <agent-name> This lists the named node agent.

Examples **EXAMPLE 1** Using the list-node-agents command

In the following example, `agent1` is the only node agent in the domain.

```
asadmin>list-node-agents --user admin1 --passwordfile filename
agent1 not running
Command list-node-agents executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-node-agent(1)`, `delete-node-agent(1)`, `start-node-agent(1)`, `stop-node-agent(1)`

Name list-password-aliases – lists all password aliases

Synopsis

```
list-password-aliases --user admin_user [--passwordfile filename]
    [--host localhost] [--port 4849] [--secure|-s] [--terse=false] [--echo=false]
    [--interactive=true] [--help]
```

Description This command lists all of the password aliases.

Options

-u --user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
-H --host	The machine name where the domain administration server is running. The default value is localhost.
-p --port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
-s --secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—help	Displays the help text for the command.

Examples

EXAMPLE 1 Using list-password-aliases command

```
asadmin> list-password-aliases --user admin --passwordfile /home/password.txt
jmspassword-alias
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

```
list-persistence-resources —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] target
```

Description Gets all the persistence resources. This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
Operands	*target*	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 ■ `server`, which deploys the component to the default server instance `server` and is the default value ■ `domain`, which deploys the component to the domain. ■ *cluster_name*, which deploys the component to every server instance in the cluster. ■ *instance_name*, which deploys the component to a particular sever instance.

Examples **EXAMPLE 1** Using list-persistence-resources

```
asadmin> list-persistence-resources --user admin
--passwordfile secret.txt --host pigeon --port 5001
Command list-persistence-resources executed successfully
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-persistence-resource(1)`, `delete-persistence-resource(1)`

Name list-resource-adapter-configs – lists the configuration information created in `domain.xml` for the connector module

Synopsis

```
list-resource-adapter-configs —user admin_user [—passwordfile filename]
     [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
     [—interactive=true] [—help] [—verbose=false]
     [—raname connectorModuleName] [target]
```

Description 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`.

This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—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	*target*	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 **EXAMPLE 1** Using `list-resource-adapter-configs`

```
asadmin> list-resource-adapter-configs --user admin1
--passwordfile pfile1
Command list-resource-adapter-configs executed successfully
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-resource-adapter-config(1)`, `delete-resource-adapter-config(1)`

Name list-resource-refs – lists the existing resource references

Synopsis

```
list-resource-refs —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [target]
```

Description The `list-resource-refs` command lists all resource references in a cluster or an unclustered server instance. This effectively lists all the resources (for example, JDBC resources) available in the JNDI tree of the specified target.

The target instance or instances making up the cluster need not be running or available for this command to succeed.

This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.
Operands	*target*	The target for which you are listing the resource references. Valid values are ■ `server`, which lists the resource references for the default server instance `server` and is the default value ■ *cluster_name*, which lists the resource references for every server instance in the cluster ■ *instance_name*, which lists the resource references for the named unclustered server instance

Examples **EXAMPLE 1** Using the list-resource-refs command

The following command lists the resource references for the cluster `MyCluster`.

```
asadmin> list-resource-refs --user admin
--passwordfile passwords.txt MyCluster
jms/Topic
Command list-resource-refs executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `create-resource-ref(1)`, `delete-resource-ref(1)`

Name list-sub-components – lists EJBs or Servlets in deployed module or module of deployed application

Synopsis

```
list-sub-components —user admin_user [—passwordfile filename]
[—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
[—interactive=true] [—help] [—type ejbs|servlets] [—appname appname]
modulename
```

Description 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.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—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	This is the name of the application. This option is required when the desired output is the sub-components of an embedded module of a deployed application.
Operands	modulename	This is the name of the module containing the sub-component.

Examples **EXAMPLE 1** Using `list-sub-components`

```
asadmin> list-sub-components --user admin --appname MEjbApp mejb.jar
Please enter admin password>
MEJBBean <StatelessSessionBean>
Command list-sub-components executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also deploy(1), deploydir(1), undeploy(1), enable(1), disable(1), list-components(1)

Name list-system-properties – lists the system properties of the domain, configuration, cluster, or server instance

Synopsis

```
lists-system-properties —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [target target_name]
```

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 overriden through a system property of the corresponding name. This command lists the system properties of a domain, configuration, cluster, or server instance.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
Operands	*target*	In Enterprise Edition, specifies the target on which you are listing the system properties. Valid values are ■ *domain*, which lists the system properties defined for the domain ■ *configuration_name*,lists the system properties for the named configuration as well as those the cluster inherits from the domain. ■ *cluster_name*, which lists the system properties defined for the named cluster as well as those the cluster. inherits from its configuration and the domain. ■ *instance_name*, which lists the system properties delfined 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.

Examples **EXAMPLE 1** Using list-system-properties

```
asadmin> list-system-properties --user admin --passwordfile password.txt
--host localhost --port 4849 mycluster
http-listener-port=1088
Command list-system-properties executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also create-system-properties(1), delete-system-property(1)

Name list-threadpools – lists all the threadpools

Synopsis

```
list-threadpools —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target_name]
```

Description Lists all the thread pools. This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
`––help`	Displays the help text for the command.
`––target`	This option specifies the target being operated on. Valid values are: ■ `server`, which lists the threadpools for the default server instance `server` and is the default value ■ *configuration_name*, which lists the threadpools for the named configuration ■ *cluster_name*, which lists the threadpools for every server instance in the cluster ■ *instance_name*, which lists the threadpools for a particular server instance This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

Examples **EXAMPLE 1** Using list-threadpools

```
asadmin> list-threadpools --user admin --passwordfile password.txt
threadpool-1
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

```
list-timers —user admin_user [—passwordfile filename] [—host localhost]
     [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
     [—interactive=true] [—help] target
```

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 administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
Operands	*target*	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 **EXAMPLE 1** Using list-timers

This is an example of how the command is used.

```
asadmin>list-timers --user admin --passwordfile filename target dancer
The list-timers command was executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also migrate-timers(1)

Name list-transaction-id – lists the transactions IDs

Synopsis

```
list-transaction-id —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [target]
```

Description This command lists the transaction IDs in the named target. This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—-help	Displays the help text for the command.
Operands	*target*	This is used in Enterprise Edition only. This is the name of the target upon which the command operates.

Examples **EXAMPLE 1** Using list-transaction-id

```
asadmin> list-transaction-id --user admin --passwordfile password.txt --target server
The list-transaction-id command executed successfully
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `freeze-transaction-service(1)`, `unfreeze-transaction-service(1)`, `rollback-transaction(1)`

Name list-virtual-servers – lists the existing virtual servers

Synopsis

```
list-virtual-servers —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [target]
```

Description The `list-virtual-servers` command lists the existing virtual servers. This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	`––help`	Displays the help text for the command.

Operands

target — In Enterprise Edition, this operand specifies the target for which the virtual servers are to be listed. Valid values are:

- `server`, which lists the virtual servers in the default server instance `server` and is the default value
- *configuration_name*, which lists the virtual servers in the specified configuration
- *cluster_name*, which lists the virtual servers in the specified cluster
- *instance_name*, which lists the virtual servers in a particular server instance

Examples

EXAMPLE 1 Using the list-virtual-servers command

The following command lists all the virtual servers for the server instance:

```
asadmin> list-virtual-servers --user admin --passwordfile passwords.txt
--host localhost --port 4848
server
__asadmin
Command list-virtual-servers executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also

`create-virtual-server(1)`, `delete-virtual-server(1)`

Name migrate-timers – moves a timer when a server instance stops

Synopsis

```
migrate-timers —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—destination destination_server_name]
    server_name
```

Description The function of the migrate-timer command is to move the timer to a specified server, when the server instance stops or fails abnormally. This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—-help	Displays the help text for the command.
	—-destination	This is the destination server instance. If this option is not specified, then DAS will find a server instance or multiple server instances. A migration notification will be sent to the selected server instances.
Operands	*server_name*	This is the current location of the server instance. The server instance should not be active during this process.

Examples **EXAMPLE 1** Using migrate-timers

This is a simple example of how to use the command.

```
asadmin>migrate-timers --servername dance
This command was successfully executed.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `list-timers(1)`

Name multimode – allows you to execute multiple commands while preserving environment settings and remaining in the asadmin utility

Synopsis

```
multimode [--file filename] [--printprompt=true] [--encoding encode]
     [--terse=false] [--echo=false]
```

Description Use `multimode` 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 `multimode` 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 `multimode` from within a *multimode* session; once you exit the second *multimode* environment, you return to your original *multimode* environment.

This command is supported in local mode only.

Options

`--file`	reads the commands as defined in the file.
`--printprompt`	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.
`--encoding`	specifies the locale for the file to be decoded.
`--terse`	indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
`--echo`	setting to true will echo the command line statement on to the standard output. Default is false.

Examples **EXAMPLE 1** Using `multimode` to execute multiple commands

```
% asadmin multimode --file commands_file.txt
```

Where: `%` is the system prompt. The administrative commands are executed from the `commands_file.txt` file.

Exit Status

0	command executed successfully
1	error in executing the command

See Also `export(1)`, `unset(1)`

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

Synopsis `package-appclient`

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

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

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

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

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

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

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

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

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

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

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Interface Stability	Unstable

See Also `appclient (1M)`

Name ping-connection-pools – tests that a connection pool is usable

Synopsis

```
ping-connection-pools —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] pool_name
```

Description 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.

Either a JDBC or connector connectionpool with authentication can be created. You can either use a –property option to specify user, password, or other connection information using the command line, or specify the connection information in the xml descriptor file.

Before pinging a connection pool, you must create the connection pool with authentication and ensure that the enterprise server or database is started.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.

	–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
Operands	*pool_name*	This is the name of the pool to test.

Examples **EXAMPLE 1** Using the ping-connection-pool command

```
asadmin> ping-connection-pool --user admin1 --passwordfile pwordfile
Command ping-connection-pool executed successfully
```

Where: asadmin is the command prompt and sampleConnectionPool is the name of the connection pool to ping.

Exit Status	0	command executed successfully
	1	error in executing the command

Name recover transactions – manually recovers pending transactions

Synopsis

```
recover-transactions —user user —passwordfile filename [—host localhost]
    [—port port_number] [—secure=false] [—terse=false] [—echo=false]
    [—interactive=true] [—delegatedrecovery=false]
    [—transactionlogdir tx_log_dir ] [—recoveryserverid recovery_server_id]
    recovery_server_name
```

Description The function of this command is to manually recover pending transactions. This is used 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	The name of the file containing the domain application server password. The passwordfile should contain either of the following entries: AS_ADMIN_PASSWORD=*password* or AS_ADMIN_MAPPEDPASSWORD=*password*. If this option is not called directly, you will be prompted for it before the requested action is completed.
–H.—host	The machine name where the the domain application server is running.
–p.—port	The port number of the domain application server listening for administration requests.
–s.—secure	If set to true, this command 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. The default is false.
–e.—echo	Setting this option to true will echo the command line statement on the standard output. The default is false.
–I.—interactive	If this option is set to true (default), only the required password options are prompted.
—delegatedrecovery	When the delegated-recovery is set to false (the default), transaction recovery is done at the running server. When the delegated-recovery is set to true, another server performs the

		recovery for the failed server. If the command is set to true and there is no server-related data, the DAS does the delegated recovery.
	—transactionlogdir	When a server fails it writes the location in its transaction log. This option is required if the –delegatedrecovery option is set to true. If the failed server's transaction logs are copied to some other location to make it available to the surrogate recovery server, this option should be used. If the failed server's transaction-service, tx-log-dir is modified to reflect a new location, then this option is not required.
	—recoveryserverid	This option is the server identification id or token for the failed server. This option is required if the –delegaterecovery option is set to true. This option is not necessary if the recovery_server_name operand can giv a hint of the recovery_server_id. The recoveryserverid option is not only used in recovery but it is also used in the creation of the XIDand later used to recognize the XIDs that belong to this server.
Operands	*recovery_server_name*	This is the name of the server that failed. It is this server that is losting the transaction that will be recovered.

Examples **EXAMPLE 1** Using recover-transactions

```
asadmin>recover-transactions serverid1
Transaction recovered.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also none

Name remove-ha-cluster – returns an HA cluster to non-HA status

Synopsis

```
—user admin_user [—passwordfile filename] [—host localhost] [—port 4849]
    [—secure|–s] [—terse=false] [—echo=false] [—interactive=true] [—help]
    [—haagentport port_number] [—haadminpassword password] databaseName
```

Description This command returns an HA cluster to non-HA status. Use fully qualified hostnames when specifying the hostlist interfaces explicitly for hosts with multiple network interfaces. This command is supported in remote mode only.

The command performs the following tasks:

- The HA database is stopped.
- The HA database is deleted.
- The command deletes and/or modifies the appropriate resources in domain.xml.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
	—haagentport	This is the HA agent port containing the cluster to be changed. The default value is 1862.
	—haadminpassword	This is the HA administrator's password.
Operands	*databasename*	This is the name of the database tob e removed.

Examples **EXAMPLE 1** Using remove-ha-cluster

```
asadmin> remove-ha-cluster --user u1 paswordfile pfile1 --haagentport 1860 cluster1
Command remove-ha-cluster executed successfully
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also configure-ha-cluster(1)

Name restore-domain – restores files from backup

Synopsis

```
restore-domain [--domaindir domain_directory] [--filename backup_filename]
     [--description description] [--terse=false] [--verbose=false] [domain_name]
```

Description This command restores files under the domain from a backup directory. The `restore-domain` 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`.
`--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.

Operands

domain_name	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.

Examples **EXAMPLE 1** Using restore-domain

```
asadmin>restore-domain --domaindir /opt/SUNWappserver/nondefaultdomaindir/domain1 --filename
Successfully restored the domain (domain1), from /opt/SUNWappserver/nondefaultdomaindir/domai

Description: 1137030607263
Backup Filename: /opt/SUNWappserver/nondefaultdomaindir/domain1/backups/sjsas_backup_v00001.z
Date and time backup was performed: Wed Jan 11 17:50:07 PST 2006
Domains Directory: /opt/SUNWappserver/nondefaultdomaindir
Domain Directory: /opt/SUNWappserver/nondefaultdomaindir/domain1
Domain Name: domain1
Name of the user that performed the backup: jondoe
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `backup-domain(1)`, `list-backups(1)`

Name rollback-transaction – rolls back the named transaction

Synopsis

```
rollback-transaction —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target target_name] [transaction_id]
```

Description Rolls back the named transaction. This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
`––help`	Displays the help text for the command.
`––target`	This option specifies the target on which you are rolling back the transactions. Valid values are ■ `server`, which creates the rollback transaction for the default server instance `server` and is the default value ■ *configuration_name*, which creates the rollback transaction for the named configuration ■ *cluster_name*, which creates the rollback transaction for every server instance in the cluster ■ *instance_name*, which creates the rollback transaction for a particular server instance This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

Operands

transaction_id	identifier for the transaction to be rolled back..

Examples

EXAMPLE 1 Using rollback-transaction

```
asadmin> rollback-transaction --user admin --passwordfile password.txt --target server 000000
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `freeze-transaction-service(1)`, `unfreeze-transaction-service(1)`

Name set – sets the values of attributes

Synopsis **set** —user *admin_user* [—passwordfile *filename*] [—host *localhost*] [—port *4849*] [—secure|–s] [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—help] *attributename=value*

Description Sets the values of one or more configurable attribute.

An application server dotted name uses the "." (period) as a delimiter to separate the parts of a complete name. This is similar to how the "/" character is used to delimit the levels in the absolute path name of a file in the UNIX file system. The following rules apply while forming the dotted names accepted by the `get`, `set` and `list` commands. Note that a specific command has some additional semantics applied.

- A `.` (period) always separates two sequential parts of the name.
- A part of the name usually identifies an application server subsystem and/or its specific instance. For example: web-container, log-service, thread-pool-1 etc.
- If any part of the name itself contains a `.` (period), then it must be escaped with a leading `\` (backslash) so that the "." does not act like a delimiter.
- The top level switch for any dotted name is `--monitor` or `–m` that is separately specified on a given command line. The presence or lack of this switch implies the selection of one of the two hierarchies for appserver management: monitoring and configuration.

  If you happen to know the exact complete dotted name without any wildcard character, then `list` and `get`/`set` have a little difference in their semantics:

  - The `list` command treats this complete dotted name as the complete name of a parent node in the abstract hierarchy. Upon providing this name to `list` command, it simply returns the names of the immediate children at that level. For example, `list server.applications.web-module` will list all the web modules deployed to the domain or the default server.
  - The `get` and `set` commands treat this complete dotted name as the fully qualified name of the attribute of a node (whose dotted name itself is the name that you get when you remove the last part of this dotted name) and it gets/sets the value of that attribute. This is true if such an attribute exists. You will never start with this case because in order to find out the names of attributes of a particular node in the hierarchy, you must use the wildcard character `*`. For example, `server.applications.web-module.JSPWiki.context-root` will return the context-root of the web-application deployed to the domain or default server.
- If you are using the Enterprise Edition of the Application Server, then "`server`" (usually the first part of the complete dotted name) can be replaced with the name of a particular server instance of interest (e.g., `server1`) and you'll get the information of that server instance, remaining part of the dotted name remaining the same. Note that the dotted

names that are available in such other server instances are those from the monitoring hierarchy because these server instances don't have a way to expose the configuration hierarchy.

The `list` command is the progenitor of navigational capabilities of these three commands. If you want to `set` or `get` attributes of a particular application server subsystem, you must know its dotted name. The `list` command is the one which can guide you to find the dotted name of that subsystem. For example, to find out the modified date (attribute) of a particular file in a large file system that starts with `/`. First you must find out the location of that file in the file system, and then look at its attributes. Therefore two of the first commands to understand the hierarchies in appserver are: `* list *` and `* list "*" --monitor`. The sorted output of these commands is typically of the following form:

Command	Output
`list *`	■ `default-config` ■ `default-config.admin-service` ■ `default-config.admin-service.das-config` ■ `default-config.admin-service.jmx-connector.system` ■ `default-config.admin-service.jmx-connector.system.ssl` ■ `default-config.availability-service` ■ `default-config.availability-service.jms-availability` ■ `default-config.ejb-container` ■ `. . .` ■ `default-config.http-service.http-listener.http-listener-1` ■ `default-config.http-service.http-listener.http-listener-2` ■ `. . .` ■ `default-config.iiop-service` ■ `. . .` ■ `default-config.java-config` ■ `. . .` ■ `domain` ■ `domain.clusters` ■ `domain.configs` ■ `domain.resources` ■ `domain.resources.jdbc-connection-pool.DerbyPool` ■ `domain.resources.jdbc-connection-pool._CallFlowPool` ■ `domain.resources.jdbc-connection-pool._TimerPool` ■ `. . .` ■ `server` ■ `server-config` ■ `cerver-config.admin-service` ■ `server-config.admin-service.das-config` ■ `server-config.admin-service.jmx-connector.system` ■ `server-config.admin-service.jmx-connector.system.ssl` ■ `server-config-availability-servicce` ■ `server-config.availability-service.jms-availability` ■ `server-config.ejb-container` ■ `. . .` ■ `server.log-service` ■ `server.log-service.module-log-levels` ■ `. . .` ■ `server.session-config` ■ `server.session-config.session-manager` ■ `server.session-config.session-manager.manager-properties` ■ `server.session-config.session-manager.store-properties` ■ `server.session-config.session-properties` ■ `server.thread-pools` ■ `server.thread-pools.thread-pool.thread-pool-1` ■ `server.transaction-service` ■ `server.web-container` ■ `server.web-container-availability`

Command	Output
`list -–monitor *`	■ `server` ■ `server.applications` ■ `server.applications._JWSappclients` ■ `server.applications._JWSappclients.sys\.war` ■ `server.applications.adminapp` ■ `server.applications.admingui` ■ `server.connector-service` ■ `server.http-service` ■ `server.http-service.server` ■ `server.jms-service` ■ `server.jvm` ■ `server.orb` ■ `server.orb.connection-managers` ■ `server.resources` ■ `server.thread-pools`

Consequently, the `list` command is the entry point into the navigation of the application server's s management hierarchies. Take note of the output of the `list` command:

- The output lists one element per line.
- Every element on a line is a complete-dotted-name of a management component that is capable of having attributes. Note that none of these lines show any kind of attributes at all.

The output of the`list` command is a list of dotted names representing individual application server components and subsystems. Every component or subsystem is capable of having zero or more attributes that can be read and modified.

With the`list` command you can drill down through the hierarchy in a particular branch of interest. For example, if you want to find the configuration of the `http-listener` of the domain (the default server, whose ID is "`server`"). Here is how you could proceed on a UNIX terminal:

ID	Command	Output/Comment
1	`list "*" | grep http | grep listener`	1. `default-config.http-service.http-listener.http-listener-1` 2. `default-config.http-service.http-listener.http-listener-2` 3. `server-config.http-service.http-listener.admin-listener` 4. `server-config.http-service.http-listener.http-listener-1` 5. `server-config.http-service.http-listener.http-listener-2` 6. `server-http-service.http-listener.admin-listener` 7. *server.http-service.http-listener.http-listener-1* 8. `server.http-service.http-listener.http-listener-2`
2	To find the listener that corresponds to the default `http-listener` where the web applications in the `domain/server` are deployed: 1. Examine the dotted name starting with item number 7 in above output. 2. Use the `get` command as shown in its usage. For example, `get server.http-service.http-listener.http-listener-1.*` will return all the attributes of the `http-listener` in context.	server.http-service.http-listener.http-listener-1.acceptor-threads = 1server.http-service.http-listener.http-listener-1.address = 0.0.0.0server.http-service.http-listener.http-listener-1.blocking-enabled = falseserver.http-service.http-listener.http-listener-1.default-virtual-server = serverserver.http-service.http-listener.http-listener-1.enabled = trueserver.http-service.http-listener.http-listener-1.external-port =server.http-service.http-listener.http-listener-1.family =inetserver.http-service.http-listener.http-listener-1.id = http-listener-1server.http-service.http-listener.http-listener-1.port = 8080server.http-service.http-listener.http-listener-1.redirect-port =server.http-service.http-listener.http-listener-1.security-enabled = falseserver.http-service.http-listener.http-listener-1.server-name =server.http-service.http-listener.http-listener-1.xpowered-by = true

Making use of both `list` and `get` commands, it is straightforward to reach a particular component of interest.

To get the monitoring information of a particular subsystem you must:

1. Use the `set` command to set an appropriate monitoring level for the component of interest.
2. Obtain the various information about the JVM that the application server domain is running.

ID	Command	Output/Comment
1	`list server* | grep monitoring`	server-config.monitoring-service server-config.monitoring-service.module-monitoring-levels server.monitoring-serviceserver.monitoring-service.module-moni Note that this is the `list` command. It only shows the hierarchy, nothing else. Using the '|' and "grep" narrows down the search effectively. Now, you can choose `server.monitoring-service` to set the attributes of various attributes that can be monitored. This is the configuration data because this setting will be persisted to the server's configuration store.
2	`get server.monitoring-service.*`	You can try the number of attributes that are presently available with monitoring service. Here is the output: No matches resulted from the wildcard expression. This is because this fully dotted name does not have any attributes at all. Logically, you try the next one and that is: `server.monitoring-service.module-monitoring-levels`. Again, use the wildcard character to get ALL the attributes of a particular component.

ID	Command	Output/Comment
3	`get server.monitoring-service.module-monitoring-levels.*`	server.monitoring-service.module-monitoring-levels.connector-connecti = OFF server.monitoring-service.module-monitoring-levels.connector-service = OFF server.monitoring-service.module-monitoring-levels.ejb-container = OFF server.monitoring-service.module-monitoring-levels.http-service = OFF server.monitoring-service.module-monitoring-levels.jdbc-connection-po = OFF server.monitoring-service.module-monitoring-levels.jms-service = OFF server.monitoring-service.module-monitoring-levels.jvm = OFF server.monitoring-service.module-monitoring-levels.orb = OFF server.monitoring-service.module-monitoring-levels.thread-pool = OFF server.monitoring-service.module-monitoring-levels.transaction-service = OFF server.monitoring-service.module-monitoring-levels.web-container = OFF The JVM monitoring is at a level OFF. It must be changed in order to make the JVM monitoring information available. The other valid values for all the monitoring level are: LOW and HIGH. use the `set` command to set the value appropriately.
4	`set server.monitoring-service. module-monitoring-levels.jvm=HIGH` There is no space before or after the = sign.	server.monitoring-service.module-monitoring-levels.jvm = HIGH Now, the JVM information can be obtained using the `get` command and monitoring switch. But remember , when you switch to the monitoring hierarchy, start with the `list` command again.

ID	Command	Output/Comment
5	`list --monitor * | grep jvm`	server.jvm server.jvm.class-loading-system server.jvm.compilation-system server.jvm.garbage-collectors server.jvm.garbage-collectors.Copy server.jvm.garbage-collectors.MarkSweepCompact server.jvm.memory server.jvm.operating-system server.jvm.runtime server.jvm.thread-system server.jvm.thread-system.thread-1 . . . server.jvm.thread-system.thread-793823 server.jvm.thread-system.thread-793824 server.jvm.thread-system.thread-793825 server.jvm.thread-system.thread-793826 server.jvm.thread-system.thread-793827 server.jvm.thread-system.thread-9 The JRE 1.5.0 monitorable components are exposed in an elegant manner. This is what you see when connected by the JConsole. Now, to know more about the class-loading system in the JVM, this is how you'll proceed. Note that now you are interested in the attributes of a particular leaf node. Thus the command is `get` not `list`.

ID	Command	Output/Comment
6	`get --monitor server.jvm.class-loading-system.*`	server.jvm.class-loading-system.dotted-name = server.jvm.class-loading-system server.jvm.class-loading-system.loadedclasscount-count = 7328 server.jvm.class-loading-system.loadedclasscount-description = No Description was available server.jvm.class-loading-system.loadedclasscount-lastsampletime = 1133819508973 server.jvm.class-loading-system.loadedclasscount-name = LoadedClassCount? server.jvm.class-loading-system.loadedclasscount-starttime = 1133819131268 server.jvm.class-loading-system.loadedclasscount-unit = count server.jvm.class-loading-system.totalloadedclasscount-count = 10285 server.jvm.class-loading-system.totalloadedclasscount-description = No Description was available server.jvm.class-loading-system.totalloadedclasscount-lastsampletime = 1133819508972 server.jvm.class-loading-system.totalloadedclasscount-name = TotalLoadedClassCount? server.jvm.class-loading-system.totalloadedclasscount-starttime = 1133819131268 server.jvm.class-loading-system.totalloadedclasscount-unit = count server.jvm.class-loading-system.unloadedclasscount-count = 2957 server.jvm.class-loading-system.unloadedclasscount-description = No Description was available server.jvm.class-loading-system.unloadedclasscount-lastsampletime = 1133819508973 server.jvm.class-loading-system.unloadedclasscount-name = UnloadedClassCount? server.jvm.class-loading-system.unloadedclasscount-starttime = 1133819131268 server.jvm.class-loading-system.unloadedclasscount-unit = count You cansee that 10285 is the total number of classes loaded by the Virtual Machine. Whereas, 2957 is number of classes unloaded, since it was started. ,Similarly, you can explore attributes of the other subsystems as well.

Options

`–u ––user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—help	Displays the help text for the command.

Operands

attributename=value	identifies the attribute name and its value. See the *Reference* for a listing of the available attribute names.

Examples

EXAMPLE 1 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 `get(1)`, `list(1)`

Name show-component-status – displays the status of the deployed component

Synopsis

```
show-component-status —user admin_user [—passwordfile filename]
     [—host localhost] [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
     [—interactive=true] [—help] [—target target (defaultserver)] component-name
```

Description gets the status of the deployed component. The status is a string representation returned by the server. The status is a string representation returned by the server. The possible status strings include status of *app-name* is `enabled` or status of *app-name* is `disabled`. This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
––help	Displays the help text for the command.
––*target*	This option specifies the target on which you are showing the component status. Valid values are: ■ `server`, which shows the component status for the default server instance `server` and is the default value ■ *domain_name*, which shows the component status for the named domain ■ *cluster_name*, which shows the component status for every server instance in the cluster ■ *instance_name*, which shows the component status for a particular server instance

Operands

`component-name`	This is the name of the component to be listed.

Examples

EXAMPLE 1 Using `show-component-status` command

```
asadmin> show-component-status --user admin MEjbAppPlease enter the admin password>
Status of MEjbApp is enabled
Command show-component-status executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `list-components(1)`, `list-sub-components(1)`

Name shutdown – brings down the administration server

Synopsis

```
shutdown [--user admin_user][--password admin_password][--host localhost]
     [--port 4848][--passwordfile filename][--secure|-s]
```

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 **EXAMPLE 1** Using the shutdown command

```
asadmin> shutdown --user admin --password adminadmin --host bluestar --port 4848
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 Administration Server page

See Also `start-instance(1)`, `stop-instance(1)`, `restart-instance(1)start-domain(1)`, `stop-domain(1)`

Name start-appserv – starts the domains in the default domains directory

Synopsis **`start-appserv`** [—domaindir *install_dir*`/domains`] [—terse=*false*] [—echo=*false*]

Description Use the `start-appserv` command to start the domains in the default *install_dir*`/domains` directory.

The `start-appserv` command requires that the user has set up an AS_ADMIN_USER environment and that all domains have the same admin user. The user will be prompted for the admin password for each domain (unless there is an AS_ADMIN_PASSWORD variable). The user will be prompted for the master password for each domain (unless —`password` was specified at domain creation time.

This command is supported in local mode only.

Options

—`domaindir`	The directory where the domains are to be started. If specified, the path must be to the default *install_dir*`/domains` directory.
–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.

Examples **EXAMPLE 1** Using the start—appserv command

```
asadmin> start-appserv
Starting Domain sampleDomain, please wait
Domain sampleDomain started
Command start-appserv executed successfully
```

Where: the `sampleDomain` domain in the default domains directory is started.

Exit Status

0	command executed successfully
1	error in executing the command

Error Codes

0	error message
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-cluster – starts a cluster

Synopsis

```
start-cluster —user admin_user [—passwordfile filename] [—host localhost]
     [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
     [—interactive=true] [—help] cluster_name
```

Description The `start-cluster` command attempts to start all non-running instances in the cluster that are reachable through their Node Agent. In other words, some instances may not be started if their Node Agent is not running.

This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
Operands	*cluster_name*	The name of the cluster to be started.

Examples **EXAMPLE 1** Using the start-cluster command

The following command starts the cluster named `MyCluster`.

```
asadmin> start-cluster --user admin1
--passwordfile passwords.txt MyCluster
Command start-cluster executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `stop-cluster(1)`, `create-cluster(1)`, `list-clusters(1)`, `delete-cluster(1)`

Name start-database – starts Java DB

Synopsis **start-database** [—dbhost *0.0.0.0*] [—dbport *1527*] [—dbhome *install_dir/databases*] [—echo=*false*] [—terse=*false*]

Description The `start-database` command starts the Java DB server that is available with the Sun Java System Application Server software. Use this command only for working with applications deployed to the Application Server. Java DB is based upon Apache Derby.

When the Java DB database server is started using this command, the database server is started in Network Server mode. Clients connecting to it must use the Java DB ClientDriver. For details on connecting to the database, such as the Driver Class Name and Connection URL, please see the Apache Derby documentation.

When the database server starts, or a client connects to it successfully, two types of files are created:

- The `derby.log` file that contains the database server process log along with its standard output and standard error information.
- The database files that contain your schema (for example, database tables).

Both types of files are created at the location specified by the `dbhome` option. When `--dbhome` is not specified, the default is the value of *install-dir*`/databases`. It is important to use the `dbhome` option when you want to create the database files at a particular location. The `start-database` command starts the database process, even if it cannot write to the log file.

This command is supported in local mode only.

Options

—dbhost	The host name or IP address of the Java DB server process. The default is the IP address 0.0.0.0, which denotes all network interfaces on the host where you run the `start-database` command.
—dbport	The port number where the Java DB server listens for client connections. This port must be available for the listen socket, otherwise the database server will not start. The default is 1527.
—dbhome	The absolute path to the directory where Java DB and the `derby.log` files are created. If not specified, the default location is *install-dir*`/databases`. For compatibility with previous releases, if a database is found in the current directory, dbhome defaults to ".". Otherwise, dbhome defaults to *install-dir*`/databases`.
–e —echo	Setting to true will echo the command line statement on the standard output. Default is false.

–t —terse	Setting to true displays detailed database information. Default is false.

Examples **EXAMPLE 1** Using the start-database command

The following command starts Java DB on the host host1 and port 5001:

```
asadmin> start-database --dbhost host1 --dbport 5001 --terse=true
Starting database in the background. Log redirected to /opt/SUNWAppserver/derby/db.log.
```

Exit Status The exit status applies to errors in executing the `asadmin` command. For information on database errors, see the `derby.log` file.

0	command executed successfully
1	error in executing the command

See Also `stop-database(1)`

Name start-domain – starts a domain

Synopsis

```
start-domain [—domaindir install_dir/domains] —user admin_user
    —passwordfile file_name [—terse=false] [—echo=false] [—interactive=true]
    [—verbose=false] [—debug=false] [domain_name]
```

Description Use the `start-domain` command to start a domain. If the domain directory is not specified, the domain in the default *install_dir*`/domains` directory is started. If there are two or more domains, the *domain_name* operand must be specified.

On Mac OS X, processes can bind to the same port. To avoid this problem, do not start multiple domains with the same port number at the same time.

This command is supported in local mode only.

Operands

`—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 *install_dir*`/domains` directory is started.
`–u —user`	The authorized domain application server administrative username. This option is optional in the Application Server Platform Edition, but is required in the Application Server Enterprise Edition.
`—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=*password*. Where *password* is the actual administrator password for the domain. This option is optional in the Application Server Platform Edition, but is required in the Application Server Enterprise Edition.
`–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 Windows, press CTRL-Break in the domain's window to print a thread dump. On UNIX, press CTRL-C to kill the server and 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

EXAMPLE 1 Using the start-domain command

```
asadmin> start-domain --domaindir /export/domains --user admin --passwordfile pass sampleDomain
Starting Domain sampleDomain, please wait.
Domain sampleDomain started
```

Where: the `sampleDomain` domain in the `/export/domains` directory is started using admin password stored in pass file.

EXAMPLE 2 Using the start-domain command on Platform Edition

```
asadmin> start-domain
Starting Domain domain1, please wait.
Domain domain1 is ready to receive client requests. Additional services are being started in backgr
```

Where: `domain1` is the domain in the `/opt/SUNWappserver/domains/` directory is started using admin password stored in the password file.

EXAMPLE 3 Using the start-domain command on Enterprise Edition

```
asadmin> start-domain --user admin
Starting Domain domain1, please wait.
Please enter the admin password
Domain domain1 started
```

Where: `domain1` is the domain in the `/opt/SUNWappserver/domains/` directory is started using admin password provided.

Exit Status

0	command executed successfully
1	error in executing the command

See Also

`create-domain(1)`, `delete-domain(1)`, `stop-domain(1)`, `list-domains(1)`

Name start-instance – starts a server instance

Synopsis

```
start-instance —user admin_user [—passwordfile filename] [—host localhost]
     [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
     [—interactive=true] [—help] instance_name
```

Description This command starts an instance with the instance name you specify.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
Operands	*instance_name*	This is the name of the server instance to start.

Examples **EXAMPLE 1** Using `start-instance`

```
asadmin> start-instance -- instance_name instance1
Instance instance1 started
```

Exit Status

0 command executed successfully

1 error in executing the command

Interface Equivalent Server Instance page

See Also `delete-instance(1)`, `create-instance(1)`, `stop-instance(1)`, `restart-instance(1)`, `start-appserv(1)`, `stop-appserv(1)`, `start-domain(1)`,.`stop-domain(1)`

Name start-node-agent – starts a node agent

Synopsis

```
start-node-agent —user user [—passwordfile passwordfile] [—secure=true]
     [—terse=false] [—echo=false] [—interactive=true] [—verbose=false]
     [—agentdir nodeagent_path] [—startinstances=true] [nodeagent_name]
```

Description Use the `start-node-agent` command start a node agent. This command may take a while to execute since the node agent may need to create and start a number of server instances.

This command is supported in local mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_SAVEDMASTERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.

	—verbose	By default this flag is set to false. If set to true, a console window is opened for the node agent and for every server instance a node agent manages. On Windows, press Ctrl-Break in the console to print a thread dump. On UNIX, press CTRL-Backslash in the console to print a thread dump. The node agent thread dump goes to its console. The server instance thread dump goes to the instance log file.
	—agentdir	Like a Domain Administration Server (DAS), each node agent resides in a top level directory named *agentdir*/*nodeagent_name*. If specified, the path must be accessible in the filesystem. If not specified, the node agent is created in the default *install_dir*/*nodeagents* directory.
	—startinstances	If set to true, all server instances that are not currently running are started. If set to false, instances are not started. If the option is omitted, it defaults to the value of the node agent's `start-servers-in-startup` attribute, located in the `domain.xml`.
Operands	*nodeagent_name*	The name of the node agent to be started.

Examples **EXAMPLE 1** Using the start-node-agent command

The following example starts a nodeagent `nodeagent1` in the default *install_dir*/*nodeagents* directory.

```
asadmin>start-node-agent --user admin --passwordfile
/home/password.txt nodeagent1
Command start-node-agent executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `stop-node-agent(1)`, `delete-node-agent(1)`, `list-node-agents(1)`, `create-node-agent(1)`

Name stop-appserv – stops the domains in the specified domains directory

Synopsis

```
stop-appserv [—domaindir install_dir/domains] [—terse=false] [—echo=false]
     [—interactive=true]
```

Description This command is deprecated. Use the `stop-domain` command.

The `stop-appserv` command stops the domains in the specified domain directory. If the domain directory is not specified, the domains in the default *install_dir*`/domains` directory are stopped.

This command is supported in local mode only.

Options

—`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 *install_dir*`/domains` directory.
–`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 **EXAMPLE 1** Using the stop—appserv command

```
asadmin> stop-appserv
Stopping Domain sampleDomain, please wait
Domain sampleDomain stopped
Command stop-appserv executed successfully
```

Where: the `sampleDomain` domain in the default domains directory is stopped.

Exit Status

0	command executed successfully
1	error in executing the command

See Also `create-domain(1)`, `delete-domain(1)`, `start-domain(1)`, `stop-domain(1)`, `list-domains(1)`, `start-appserv(1)`

Name stop-cluster – stops a cluster

Synopsis

```
stop-cluster —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|—s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] cluster_name
```

Description The `stop-cluster` command attempts to stop all running instances in the cluster that are reachable through their Node Agent. In other words, some instances may not be stopped if their Node Agent is not running.

This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—–help	Displays the help text for the command.
Operands	*cluster_name*	The name of the cluster to be started.

Examples **EXAMPLE 1** Using the stop-cluster command

The following command stops the cluster named `MyCluster`.

```
asadmin> stop-cluster --user admin1
--passwordfile passwords.txt MyCluster
Command stop-cluster executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `start-cluster(1)`, `create-cluster(1)`, `list-clusters(1)`, `delete-cluster(1)`

Name stop-database – stops Java DB

Synopsis **`stop-database`** [—`dbhost` *`0.0.0.0`*] [—`dbport` *`1527`*]

Description The `stop-database` command stops the Java DB server that is available with the Sun Java System Application Server software for use with the Application Server. Java DB is based upon Apache Derby. The database is typically started with the `asadmin start-database` command. Note that a single host can have multiple database server processes running on different ports. This command stops the database server process for the specified port only.

This command is supported in local mode only.

Options

—`dbhost`	The host name or IP address of the Java DB server process. The default is the IP address 0.0.0.0, which denotes all network interfaces on the host where you run the `stop-database` command.
—`dbport`	The port number where the Java DB server listens for client connections. The default is 1527.

Examples **EXAMPLE 1** Using the stop-database command

The following command stops Java DB on the host host1 and port 5001:

```
asadmin> stop-database --dbhost host1 --dbport 5001
Shutdown successful.
Command stop-database executed successfully.
```

Exit Status The exit status applies to errors in executing the `asadmin` command. For information on database errors, see the `derby.log` file. This file is located in the directory you specified using the `dbhome` option when you ran `start-database`, or if you did not specify `dbhome`, the value of DERBY_INSTALL, which defaults to *install-dir*`/derby`.

0	command executed successfully
1	error in executing the command

See Also `start-database(1)`

Name stop-domain – stops the domain

Synopsis **stop-domain** [—terse=*false*] [—echo=*false*] [—domaindir *install_dir*/domains] [*domain_name*]

Description Use the stop-domain command to stop a domain. If the domain directory is not specified, the domain in the default *install_dir*/domains directory is stopped. If there is more that one domain, the *domain_name* operand must be identified.

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 *install_dir*/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.

Operands

domain_name	The unique name of the domain you wish to start.

Examples **EXAMPLE 1** Using stop-domain

```
asadmin> stop-domain --domaindir /export/domains sampleDomain
Domain sampleDomain stopped.
Where: the sampleDomain domain in the /export/domains directory is stopped.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also start-domain(1), create-domain(1), delete-domain(1)

Name stop-instance – stops a server instance

Synopsis —user *admin_user* [—passwordfile *filename*] [—host *localhost*] [—port *4849*] [—secure|–s] [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—help] *instance_name*

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

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—help	Displays the help text for the command.

Operands

instance_name	This is the name of the server instance to stop.

Examples

EXAMPLE 1 Using `stop-instance` in local mode

```
asadmin> stop-instance --local --domain domain1 server1
Instance server1 stopped
```

Where: the `server1` instance associated with the domain1 domain is stopped locally.

EXAMPLE 2 Using `stop-instance` in remote mode

```
asadmin> stop-instance --user admin --password bluestar --host localhost --port 4848 server1
Instance server1 stopped
```

Where: the `server1` instance associated with the named user, password, host and port is deleted from the remote machine.

Exit Status

0	command executed successfully
1	error in executing the command

Interface Equivalent

Server Instance page

See Also

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

Name stop-node-agent – stops a node agent

Synopsis

```
stop-node-agent [—agentdir nodeagent_path [—terse=false] [—echo=false]
    [—interactive=true]] [—secure=true] [nodeagent_name]
```

Description The local stop-node-agent command is used to stop a node agent. If the agent directory is not specified, the node agent in the default *install_dir*`/nodeagents` directory is stopped. If there is more than one node agent in the specified node agent directory, the *nodeagent_name* operand must be specified. The stop-node-agent commands stops all managed server instances of the node agent.

This command is supported in local mode only.

Options

`—agentdir`	Like a Domain Administration Server (DAS), each node agent resides in a top level directory named *agentdir*`/`*nodeagent_name*. If specified, the path must be accessible in the filesystem. If not specified, the node agent is created in the default *install_dir*`/nodeagents` directory.
`–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 options are prompted.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration server.

Operands

nodeagent_name	This is the name of the node agent to stop. If the specified agent directory contains multiple node agents, the *nodeagent_name* operand is required.

Examples

EXAMPLE 1 Using the stop-node-agent command

This example stops a node agent, `nodeagent1`, located in default *install_dir*`/nodeagents` directory.

```
asadmin>stop-node-agent nodeagent1
Command stop-node-agent executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `start-node-agent(1)`, `delete-node-agent(1)`, `list-node-agents(1)`, `create-node-agent(1)`

Name undeploy – removes a component from the domain administration server

Synopsis

```
undeploy —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—droptables=true|false] [—cascade=false]
    [—target target] component_name
```

Description `undeploy` removes the specified component in the domain administration server.

This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
`––help`	Displays the help text for the command.
`––droptables`	If set to true, tables created by application using CMP beans during deployment are dropped. Default is the corresponding entry in the `cmp-resource` element of the `sun-ejb-jar.xml` file. If not specified, it defaults to the entries specified in the deployment descriptors.
`––cascade`	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.
`––target`	This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.Specifies the target from which you are undeploying. Valid values are: ■ `server`, which undeploys the component from the default server instance `server` and is the default value ■ `domain`, which undeploys the component from the domain. ■ *cluster_name*, which undeploys the component from every server instance in the cluster. ■ *instance_name*, which undeploys the component from a particular sever instance.

Operands

component_name	name of the deployed component.

Examples **EXAMPLE 1** Simple undeployment

Undeploy (uninstall) an enterprise application `Cart.ear`.

```
asadmin> undeploy --user admin --passwordfile password.txt Cart
Command undeploy executed successfully.
```

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

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

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

asadmin> undeploy --user admin --passwordfile password.txt --droptables=true myejb
Command undeploy executed successfully.
```

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 --passwordfile password.txt --cascade=true jdbcra
Command undeploy executed successfully.
```

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

```
unfreeze-transaction-service —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—target]
```

Description Resumes all the suspended inflight transactions. Invoke this command on an already frozen transaction. This command is supported in remote mode only.

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
	target	This operand specifies the target on which you are unfreezing the Transaction Service. Valid values are: ■ server, which creates the transaction service for the default server instance server and is the default value ■ *configuration_name*, which creates the transaction service for the named configuration ■ *cluster_name*, which creates the transaction service for every server instance in the cluster ■ *instance_name*, which creates the transaction service for a particular server instance This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.
Operands	—target	Supported in Enterprise edition only. This option specifies the target on which you are unfreezing the Transaction Service. Valid values are ■ server, which creates the listener for the default server instance server and is the default value ■ *configuration_name*, which creates the listener for the named configuration ■ *cluster_name*, which creates the listener for every server instance in the cluster ■ *instance_name*, which creates the listener for a particular server instance

Examples **EXAMPLE 1** Using unfreeze-transaction-service

```
asadmin> unfreeze-transaction-service --user admin --passwordfile password.txt server1
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also freeze-transaction-service(1), rollback-transaction(1)list-transaction-id(1)

Name unset – removes one or more variables from the multimode environment

Synopsis **unset** [*env_var**]

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

env_var	environment variable to be removed.

Examples **EXAMPLE 1** Using `unset` to remove environment variables

```
asadmin> export AS_ADMIN_HOST=bluestar AS_ADMIN_PORT=8000 AS_ADMIN_USER=admin
asadmin> export AS_ADMIN_PREFIX=server1.jms-service
asadmin> export
AS_ADMIN_USER=admin
AS_ADMIN_HOST=bluestar
AS_ADMIN_PREFIX=server1.jms-service
AS_ADMIN_PORT=8000
asadmin> unset AS_ADMIN_PREFIX
asadmin> export
AS_ADMIN_USER=admin
AS_ADMIN_HOST=bluestar
AS_ADMIN_PORT=8000
```

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.

Exit Status

0	command executed successfully
1	error in executing the command

See Also `export(1)`, `multimode(1)`

Name update-connector-security-map – modifies a security map for the specified connector connection pool

Synopsis

```
update-connector-security-map --user admin_user [--passwordfile filename]
    [--host localhost] [--port 4849] [--secure|-s] [--terse=false] [--echo=false]
    [--interactive=true] [--help] --poolname connector_connection_pool_name
    [--addprincipals principal_name1[, principal_name1]* | --addusergroups user_group1[, use
    [--removeprincipals principal_name1[, principal_name2]*]
    [--removeusergroups user_group1[, user_group2]*]
    [--mappedusername username ] security_map_name
```

Description Use this command to modify a security map for the specified connector connection pool.

For this command to succeed, you must have first created a connector connection pool using the `create-connector-connection-pool` command.

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.

This command is supported in remote mode only.

Options

`-u --user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`-H --host`	The machine name where the domain administration server is running. The default value is localhost.

–p ––port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s ––secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
––help	Displays the help text for the command.
––target	This option is deprecated in this release.
––poolname	Specifies the name of the connector connection pool to which the security map that is to be updated or created belongs.
––addprincipals	Specifies a comma-separated list of EIS-specific principals to be added. Use either the `-addprincipals` or `-addusergroups` options, but not both.
––addusergroups	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	Specifies a comma-separated list of EIS user groups to be removed.
––mappedusername	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`=*mapped-password*. If not specified using the `passwordfile` option, the user will be prompted for this password by the asadmin command-line tool.

Operands

security_map_name	name of the security map to be created or updated.

Examples

EXAMPLE 1 Using `update-connector-security-map`

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

```
asadmin> update-connector-security-map --user admin
--passwordfile passwords.txt --poolname connector-pool1
--addprincipals principal1, principal2 securityMap1
Command update-connector-security-map executed successfully
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `delete-connector-security-map(1)`, `list-connector-security-maps(1)`, `create-connector-security-map(1)`

Name update-file-user – updates a current file user as specified

Synopsis

```
update-file-user —user admin_user [—passwordfile filename] [—host localhost]
    [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—authrealmname auth_realm_name]
    [—userpassword user_passsword] [—groups user_groups[:user_groups]*]
    username
```

Description This command updates an existing entry in keyfile using the specified user_name, user_password and groups. Multiple groups can be entered by separating them, with a colon ":"

Options

–u —user	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —host	The machine name where the domain administration server is running. The default value is localhost.
–p —port	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —secure	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
	—authrealmname	This is the file where the file users are stored.
	—userpassword	This is the password of the file user.
	—groups	This is the name of the group to which the file user belongs.
Operands	*username*	This is the name of file user to be deleted.

Examples **EXAMPLE 1** Using the update-file-user command

```
asadmin> 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
```

Where: the `sample_user` is the file user updated with the updated user password, groups, and user name.

Exit Status	0	command executed successfully
	1	error in executing the command

See Also `delete-file-user(1)`, `list-file-users(1)`, `create-file-user(1)`, `list-file-groups(1)`

Name update-password-alias – updates a password alias

Synopsis

```
updates-password-alias —user admin_user [—passwordfile filename]
    [—host localhost] [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
    [—interactive=true] [—help] [—aliaspassword alias_password] aliasname
```

Description This command updates the password alias IDs in the named target. An alias is a token of the form `${ALIAS=passowrd-alias-password}`. The password corresponding to the alias name is stored in an encrypted form. The `update-password-alias` command takes 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.

This command is supported in remote mode only.

Options

`–u —user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
`–H —host`	The machine name where the domain administration server is running. The default value is localhost.
`–p —port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
`–s —secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
	—help	Displays the help text for the command.
	—aliaspassword	The password corresponding to the password alias. WARNING: Passing this option on the command line is insecure. The password is optional, and when omitted, the user is prompted.
Operands	aliasname	This is the name of the password as it appears in domain.xml.

Examples **EXAMPLE 1** Using update-password-alias

```
asadmin> update-password-alias --user admin --passwordfile /home/password.txt jmspassword-alias
Please enter the alias password>
Please enter the alias password again>
Command update-password-alias executed successfully.
```

Exit Status	0	command executed successfully
	1	error in executing the command

See Also delete-password-alias(1), list-password-aliases(1), create-password-alias(1)

Name verifier – validates the J2EE Deployment Descriptors against application server DTDs

Synopsis **`verifier`** [*optional_parameters*] *jar_filename*

Description Use the `verifier` 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.

When you run the `verifier` utility, two results files are created in XML and TXT format. The location where the files are created can be configured using the `-d` 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 *jar_filename.xml* and *jar_filename.txt*

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 `static-verification` which may contain the tags `application, ejb, web, appclient, connector, other, error` and `failure-count`. 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 `application, ejb, web, other,` and `failure-count.`

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.

Options The optional parameters must be specified as follows:

`-d` | `—destdir`	Identifies the destination directory. The verifier results are located in this specified directory. The directory must already exist.
`-h` | `—help-?`	Displays the verifier help.
`-u` | `—gui`	Enables the Verifier graphical user interface.
`-v` | `—verbose`	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.
`-V` | `—version`	Displays the Verifier tool version.
`-r` | `—reportlevel`*level*	Identifies the result reporting level. The default report level is to display all results. The available reporting levels include:

a | all	Set output reporting level to display all results (default).

f | failures	Set output reporting level to display only failure results.
w | warnings	Set output reporting level to display only warning and failure results.

Operands *jar_filename* name of the ear/war/jar/rar file to perform static verification on. The results of verification are placed in two files *jar_filename.xml* and *jar_filename.txt* in the destination directory.

`-a` | `--app`	Runs only the application tests.
`--p` | `--appclient`	Runs only the application client tests.
`-c` | `--connector`	Runs only the connector tests.
`-e` | `--ejb`	Runs only the EJB tests.
`-w` | `--web`	Runs only the web tests.
`-s` | `--webservices`	Runs only the web services tests.
`-l` | `--webservicesclient`	Runs only the web services client tests.

Examples **EXAMPLE 1** Using `verifier` in the Verbose Mode

The following example runs the verifier in verbose mode and writes all the results of static verification of the `sample.ear` file to the destination directory named `/verifier-results`.

```
example% verifier -v -rf -d /verifier-results sample.ear
```

Where `-v` runs the verifier in verbose mode, `-d` specifies the destination directory, and `-rf` displays only the failures. The results are stored in `/verifier-results/sample.ear.xml` and `/verifier-results/sample.ear.txt`.

EXAMPLE 2 Using `verifier` to run Application and EJB tests

```
example% verifier --app --ejb sample.ear
```

See Also `asadmin(1M)`

Name verify-domain-xml – verifies the content of the domain.xml file

Synopsis
```
verify-domain-xml [--terse=false] [--echo=false] [--help] [--verbose=false]
    [--domaindir install_dir/domains] [domain_name]
```

Description Verfies the content of the `domain.xml` file.

Options

`-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 *install_dir*`/domains`.

Operands

domain_name	Specifies the name of the domain. The default is `domain1`.

Examples **EXAMPLE 1** Using verify-domain-xml

```
asadmin> verify-domain-xml --verbose=true domain1
All Tests Passed.
domain.xml is valid
```

Exit Status

0	command executed successfully
1	error in executing the command

Name version – displays the version information

Synopsis

```
version —user admin_user [—passwordfile filename] [—host localhost]
     [—port 4849] [—secure|–s] [—terse=false] [—echo=false]
     [—interactive=true] [—help] [—verbose=false]
```

Description Use the `version` 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.

This command is supported in remote mode only.

Options

–u —`user`	The authorized domain administration 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 administration 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 AS_ADMIN_MAPPEDPASSWORD, AS_ADMIN_USERPASSWORD, AS_ADMIN_MQPASSWORD, AS_ADMIN_ALIASPASSWORD, and so on.
–H —`host`	The machine name where the domain administration server is running. The default value is localhost.
–p —`port`	The port number of the domain administration server listening for administration requests. The default port number for Enterprise Edition is 4849.
–s —`secure`	If set to true, uses SSL/TLS to communicate with the domain administration 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.
—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

EXAMPLE 1 Using remote mode to display version

```
asadmin> version
Java 2 Platform Enterprise Edition 1.4 Application Server
```

EXAMPLE 2 Using remote mode to display version in detail

```
asadmin> version --user admin --passwordfile mysecret
--host bluestar --port 4848 --verbose
Java 2 Platform Enterprise Edition 1.4 Application Server (build A021930-126949)
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also

help(1)

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

Synopsis **wscompile** [*options*] *configuration_file*

Description 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.

In addition to supporting the generation of stubs, ties, server configuration, and WSDL documents from a set of RMI interfaces, `wscompile` also supports generating stubs, ties and remote interfaces from a WSDL document.

You must specifiy one of the `-gen` options in order to use `wscompile` as a stand alone generator. You must use either `-import` (for WSDL) or `-define` (for an RMI interface) along with the `-model` option in order to use `wscompile` in conjunction with `wsdeploy`.

Invoking the `wscompile` command without specifying any arguments outputs the usage information.

Options

`-cp` *path*	location of the input class files.
`-classpath` *path*	same as `-cp` *path* option.
`-d` *directory*	where to place the generated output files.
`-define`	read the service's RMI interface, define a service. Use this option with the `-model` option in order to create a model file for use with the `wsdeploy` command.
`-f:`*features*	enables the given features. Features are specified as a comma separated list of features. See the list of supported features below.
`-features:`*features*	same as `-f:`*features* option.
`-g`	generates the debugging information.
`-gen`	generates the client-side artifacts.
`-gen:client`	same as `-gen` option.
`-gen:server`	generates the server-side artifacts and the WSDL file. If you are using `wsdeploy`, you do not specify this option.
`-httpproxy:`*host:port*	specifies an HTTP proxy server; defaults to port 8080.
`-import`	reads a WSDL file, generates the service RMI interface and a template of the class that implements the interface. Use this option with the `-model` option in order to create a model file for use with the `wsdeploy` command.

`-mapping` *file*	writes the mapping file to the specified file.
`-model`	write the internal model for the given file name. Use this option with the `-import` option in order to create a model file for use with the `wsdeploy` command.
`-keep`	keeps the generated files.
`-nd` *directory*	directory for the non-class generated files are stored.
`-O`	optimizes the generated code.
`-s` *directory*	directory for the generated source files.
`-source` *version*	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).
`-verbose`	output messages about what the compiler is doing.
`-version`	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.

datahandleronly	always map attachments to `data handler` type
documentliteral	use document literal encoding
donotoverride	do not regenerate classes that already exist in the classpath.
donotunwrap	disable unwrapping of document/literal wrapper elements in WSI mode (default).
explicitcontext	turn on explicit service context mapping.
infix:*name*	specify an `infix` to use for generated serializers (Solaris).
infix=*name*	specify an `infix` to use for generated serializers (Windows).
jaxbenumtype	map anonymous enumeration to its base type.
nodatabinding	turn off data binding for literal encoding.
noencodedtypes	turn off encoding type information.
nomultirefs	turn off support for multiple references.
norpcstructures	do not generate RPC structures (`-import` only).
novalidation	turn off validation for the imported WSDL file.
resolveidref	resolve `xsd:IDREF`.

rpclietral	use the RPC literal encoding.
searchschema	search schema aggresively for subtypes.
serializeinterfaces	turn on direct serialization of interface types.
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 regenrate 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>
```

Wsdl Element If the `<wsdl>` element is specified, `wscompile` reads the WSDL file and generates the service's RMI interface. The `location` attribute specifies the URL of the WSDL file, and the `packageName` attribute specifies the package of the classes to be generated. For example:

```
<wsdl

location="http://tempuri.org/sample.wsdl"

packageName="org.tempuri.sample"/>
```

Modelfile Element This element is for advanced users.

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

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

Examples

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

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

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

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

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

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

See Also `wsdeploy(1M)`

Name wsdeploy – reads a WAR file and the `jaxrpc-ri.xml` file and generates another WAR file that is ready for deployment

Synopsis **`wsdeploy`** `-o` *input_WAR_file options*

Description 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.

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`.

Options

`-classpath` *path*	location of the input class files.
`-keep`	keep temporary files.
`-tmpdir` *directory*	use the specified directory as a temporary directory
`-o` *output WAR file*	required; location of the generated WAR file. This option is required.
`-source` *version*	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).
`-verbose`	outputs messages about what the compiler is doing.
`-version`	prints version information.

Input War File The input WAR file for `wsdeploy` will typically have the following structure:

```
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
```

Where: HelloIF is the service endpoint interface, and HelloImpl is the class thatimplements the interface. The web.xml file is tghe deployment descriptor of a web component.

jaxrpc-ri.xml File The following is a simple HelloWorld service.

```
<xml version="1.0" encoding="UTF-8"?>
<webServices>
   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">
    <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 attriutes of `endpoint()` specify the service's interface and iimplementation 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 oppisite direction, from schema types to Java types. In this case, the generated schema types are taken from the package that the type comes from.

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

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

```
<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

D

E

G

H

I

J

L

M

P

R

S

T

U

V

W