Sun Java System Application Server Platform Edition 9 Reference Manual

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

Part No: 819–3662
Feb 2006

060503@14774

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 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` `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`] [—host` *localhost*`]`
`[—port` *4848|4849*`] [—secure|–s] [—user` *admin_user*`] [—passwordfile` *filename*`]`
`[—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_2.dtd` in the `resources.xml` file.

This command is supported in remote mode only.

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.

`–H —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help
Displays the help text for the command.

—target
Specifies the target for which you are creating the resources. This option is available only in the Sun Java System Application Server Standard and Enterprise Edition. 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 9.0 Domain//EN"
   "*<install_dir>/lib/dtds/sun-resources_1_2.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
 =========================
Added Resource Type: jdbc-connection-pool
 =========================
Added Resource Type: jdbc-resource
 =========================
Added Resource Type: persistence-manager-factory-resource
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 specified 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
```

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

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

Attributes

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 administrative tasks for Sun Java System Application Server. You can use this utility in place of 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 control 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:

`–t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

`—help`

Displays the help text for the command.

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 using 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 configuration file.

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

To access the manpages for the Application Server command-line interface subcommands on the Solaris platform, add $AS_INSTALL/man to your MANPATH environment variable.

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

Attributes

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Interface Stability	Unstable

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 [—help] [—version] [—commandline | ] [—ui] [—quiet] [—debug]
     [—sourcedirectory source_directory] [—sourceserver source_application_server]
     [—targetdirectory target_directory] [—targetserver target_application_server]
     [—scan-native-apis-only] [—scan-packages package_list]
     [—migrate-cmp comment-pk-modifiers=true, overwrite-conflicting-accessors=true]
     [—file-filter all-files=true, html-files=true, java-files=true, jsp-files=true, xml
     [—append-logs] [operands]
```

Description

Use the `asmigrate` utility to analyze your J2EE application and translate vendor specific settings to SunJava™ System Application Server-specific settings that makes the application deployable on Sun's J2EE products.

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	Sun Java System Application Server 9
WebSphere Application Server 4.0, 5.x	
Java 2 Platform Enterprise Edition 1.3/1.4	
Sun ONE Application Server 6.5, 7.0	
Sun Java System Application Server 7 2004Q2	
Sun Java System Application Server 8.x	
JBoss Application Server 3.0, 3.2	
Tomcat Web Server 4.1.12	

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
- 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 sjsas9 as the target server for Sun Java System Appplication Server 9.

`–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 9 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 sjsas9 -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 9.

```
asmigrate -c -T sjsas9 -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 9. Only Java files are designated to be migrated. CMP 1.1 beans will be migrated to CMP 2.1 beans and conflicting CMP related accessors will be overwritten.

```
asmigrate -c -T sjsas9 -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_9_installation]
        [—passwordfile path_to_password_file—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 migrate the server configuration and its persisted state, J2EE services, and deployed J2EE applications. The configuration of an installed Sun Java System Application Server 7.x/8.x installation is migrated to the Sun Java System Application Server 9 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.

`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 checkbox 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 9. 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.

Specify the source and target directories for the upgrade.

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 9 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 or domains root directory for Sun Java System Application Server 7.x/8.x installation that will be upgraded.

`–t ––target`
The domains root directory for Sun Java System Application Server 9.

`–a ––adminuser`
The username of the administrator.

`–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*

`–n ––nsspwdfile`
The path to the NSS password file.

The format for the NSS password file is:`domain_name1 passworddomain_name2 password`

If the source server is Application Server 7.x, the format of the NSS password file is:`domain_name1 instance_name1 passworddomain_name2 instance_name2 password`

`–e ––targetnsspwdfile`
The path to the target NSS password file.

The format for the target NSS password file is:`domain_name1 passworddomain_name2 password`

`–j ––jkspwdfile`
The path to the JKS password file.

The format for the JKS password file is:`domain_name1 passworddomain_name2 password`

`–p ––capwdfile`
The path to the CA certificate password file.

The format for the CA certificate password file is:`domain_name1 passworddomain_name2 password`

`–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 9 with Prompts for Certificate Migration

This example shows how to upgrade a Sun Java System Application Server 7 installation to Sun Java System Application Server 9. 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/sjsas9
```

EXAMPLE 2 Upgrading an Application Server 7.1 EE Installation with Clusters and NSS Certificates to Application Server 9 EE

This example shows how to upgrade a Sun Java System Application Server 7.1 EE installation with a cluster to Sun Java System Application Server 9 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/sjsas9
--nsspwdfile /home/sjsas7.1/nsspassword.txt
--targetnsspwdfile /home/sjsas9/nsspassword.txt
--clinstancefile /home/sjsas7.1/config/clinstance.conf
```

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

EXAMPLE 3 Upgrading an Application Server 7.0 PE Installation with NSS Certificates to Application Server 9 PE

This example shows how to upgrade a Sun Java System Application Server 7.0 PE installation to Sun Java System Application Server 9 PE. The NSS certificates from the 7.0 PE source server will be converted to JKS and CA certificates in the 9 PE target server.

```
example% asupgrade --adminuser admin
--passwordfile password.txt
--source /home/sjsas7.0 --target /home/sjsas9
--nsspwdfile /home/sjsas7.0/nsspassword.txt
--jkspwdfile /home/sjsas7.0/jkspassword.txt
--capwdfile /home/sjsas7.0/capassword.txt
```

EXAMPLE 4 Upgrading an Application Server 8.0 PE Installation with JKS and CA Certificates to Application Server 9 PE

This example shows how to upgrade a Sun Java System Application Server 8.0 PE installation to Sun Java System Application Server 9 PE. JKS and CA certificates will be migrated.

```
example% asupgrade --adminuser admin
--passwordfile password.txt
--source /home/sjsas8.0 --target /home/sjsas9
--jkspwdfile /home/sjsas8.0/jkspassword.txt
--capwdfile /home/sjsas9/capassword.txt
```

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.

`–v —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.zi
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-admin-password – changes the administrator password

Synopsis

change-admin-password [—terse=*false*] [—echo=*false*] [—host *localhost*]
[—port *4848* | *4849*] [—secure | –s] —user *admin_user*

Description

This remote command is used to modify the admin password. `Change-admin-password` is interactive in that the user is prompted for the old admin password, as well as the new admin password (with confirmation).

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 —host`
The machine name where the domain administration server is running. The default value for Platform Edition is 4848. The default value for Standard and Enterprise Edition is 4849..

`–p —port`
The port number of the domain administration server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

Examples

EXAMPLE 1 Using change-admin-password

```
asadmin> change-admin-password --user admin
Please enter the old admin password>
Please enter the new admin password>
Please enter the new admin password again>
Command change-admin-password 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

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 available only in the Sun Java System Application Server Standard and Enterprise Edition.

`—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.

node_agent_name
This is the name of the node agent whose password is to be changed. This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

Examples

EXAMPLE 1 Using the change-master-password command

Remember to use the `asadmin login` command before you use the `change-master-password` command.

```
asadmin>change-master-password domain44ps
Please enter the new master password>
Please enter the new master password again>
Master password changed for domain44ps
```

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

configure-webservice-management – sets the monitoring or maxhistorysize attributes of a deployed web service

Synopsis

`configure-webservice-management` `[monitoring=OFF ] [maxhistory` *maxhistory-size*`]` *webservice-end-point*

Description

Use this command to configure the monitoring or the maxhistory attributes of a deployed webservice.

Options

`--monitoring`
Enables monitoring for webservices. If enabled, tracks operational statistics, such as the number of requests per second, average response time, and throughput. Allowed values are:

- `LOW`, which enables monitoring for the whole webservice. No method level monitoring will be done.
- `HIGH`, Message Trace is also enabled in addition to enabling number of requests per second, average response time, and throughput attributes.
- `OFF`, disables monitoring and this is the default.

`--maxhistorysize`
indicates the maximum number of monitoring records stored in history for this web service endpoint. Default value is 25.

Operands

webservice-end-point
name of the webservice endpoint to which the configuration management attributes are being set.

Examples

EXAMPLE 1 To turn on monitoring for a webservice endpoint

```
configure-webservice-management --monitoring=LOW jaxrpc-simple#jaxrpc-simple.war#HelloIF
Command configure-webservice-management executed successfully
```

EXAMPLE 2 To turn message tracing facility on for a webservice endpoint

```
configure-webservice-management --monitoring=HIGH
--maxhistorysize=250 jaxrpc-simple#jaxrpc-simple.war#HelloIF
Command configure-webservice-management executed successfully
```

Where `jaxrpc-simple#jaxrpc-simple.war#HelloIF` is the fully qualified name of a webservice endpoint.

Exit Status

0	command executed successfully
1	error in executing the command

Name

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

Synopsis

```
create-admin-object [—terse=false] [—echo=false] [—interactive=true]
      [—host localhost] [—port 4848|4849] [—secure|–s] [—user admin_user]
      [—passwordfile filename] [—help] [—target target]
      —restype admin_object_type —raname resource_adapter_name [—description text]
      [—property name=value[:name=value]*] jndi_name
```

Description

This command creates the administered object that has a specified JNDI name.

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.

`–H —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

`—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 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-audit-module – adds an audit-module

Synopsis

```
create-audit-module [—terse=false] [—echo=false] [—interactive=true]
        [—host localhost] [—port 4848|4849] [—secure|—s] [—user admin_user]
        [—passwordfile filename] [—help] [—target target_name]
        [—classname classname] [—property(name=value)[:name=value]*]
        audit_module_name
```

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

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.

`—H —host` The machine name where the domain administration server is running. The default value is localhost.

`—p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`—s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`—u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

`—target`
Specifies the target on which you are creating the audit module. This option is available only in the Sun Java System Application Server Standard and Enterprise Edition. 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 audit module.

`—property`
optional attributes name/value pairs of provider implementation specific attributes.

Operands *audit_module_name*
name of this audit module.

Examples

EXAMPLE 1 Using the create-audit-module command

```
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 named authentication realm

Synopsis

```
create-auth-realm [—terse=false] [—echo=false] [—interactive=true]
        [—host localhost] [—port 4848|4849] [—secure|—s] [—user admin_user]
        [—passwordfile filename] [—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

`–t —terse` Indicates that any 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 —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help — Displays the help text for the command.

—target — Specifies the target on which you are creating the realm.This option is available only in the Sun Java System Application Server Standard and Enterprise Edition. 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 paris 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
```

EXAMPLE 1 Using create-auth-realm *(Continued)*

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

Synopsis

```
create-connector-connection-pool [—terse=false] [—echo=false] [—interactive=true]
      [—host localhost] [—port 4848|4849] [—secure|–s] [—user admin_user]
      [—passwordfile filename] [—help] [--steadypoolsize 8] [--maxpoolsize 32]
      [--maxwait 60000] [--poolresize 2] [--idletimeout 300]
      [--failconnection=false] --raname resource_adapter_name
      --connectiondefinition connection_definition_name
      [--transactionsupport transaction_support] [--isconnectvalidatereq=false]
      [--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.

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.

`–H —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

`—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 number of connections to be destroyed if the existing number of connections is above the steady-pool-size (subject to the limit specified in the maxpoolsize option). Possible values are from 0 to MAX_INTEGER. The default value is 2.

`—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.

`--isconnectvalidatereq`
If the value is set to true, the connections will be checked to see if they are usable, before they are given out to the application. The default value is false.

`—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 [—terse=false] [—echo=false] [—interactive=true]
     [—host localhost] [—port 4848|4849] [—secure|–s] [—user admin_user]
     [—passwordfile filename] [—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

`–t —terse` Indicates that any 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 —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

`—target`
This option specifies the ending location of the connector resources. Valid targets are:

- `server`, which creates the connector resource in the default server instance. This is the default value.
- `domain`, which creates the connector resource in the domain.
- *cluster_name*, which creates the connector resource in every server instance in the cluster.
- *instance_name*, which creates the connector resource in the specified server instance.

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

`—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 details about the connector resource.

Operands *jndi_name* the JNDI name of this connector resource.

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

This example shows the usage of this command in the Platform Edition.

```
asadmin> create-connector-resource --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.

EXAMPLE 2 Using the create-connector-resource command

This example shows the usage of this command in the Standard and Enterprise Editions.

```
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 [—terse=false] [—echo=false] [—interactive=true]
     [—host localhost] [—port 4848|4849] [—secure|–s] [—user admin_user]
     [—passwordfile filename] [—help] —poolname connector_connection_pool_name
     [—principals principal_name1[, principal_name2]* | —usergroups user_group1[, user_grou
     —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, a new 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 data of an organization. It can be a mainframe, a messaging system, a database system, or an application.

This command is supported in remote mode only.

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.

`–H —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the --user option on subsequent operations to this particular domain.

—passwordfile

The —passwordfile option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—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` This property specifies the EIS username.

Operands

security_map_name name of the security map to be created or updated.

Examples

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

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 --m
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 resouce

Synopsis

```
create-custom-resource [—terse=false] [—echo=false] [—interactive=true]
        [—host localhost] [—port 4848|4849] [—secure|—s] [—user admin_user]
        [—passwordfile filename] [—help] —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

`—t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`—p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`—s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`—u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

`—target`
This option helps specify the target to which you are deploying. Valid values are:

- `server`, which deploys the component to the default server instance. This 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. This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

`—resourcetype`
The `—resourcetype` option is deprecated. Use `—restype` instead.

`—restype`
The type of custom resource to be created. Specify a fully qualified type definition, for example `javax.naming.spi.ObjectFactory`. The resource type definition follows the format, xxx.xxx.

`—factoryclass`	Factory class name for the custom resource. This class implements the `javax.naming.spi.ObjectFactory` interface.
`—enabled`	Determines whether the custom resource is enable at runtime. The default value is true.
`—description`	Text providing details about the custom resource. This description is a string value and can include a maximum of 250 characters.
`—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 --factoryclass com.imq.topic sample_custom_resource
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 given name

Synopsis

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

Description Use the `create-domain` command to create an administrative domain.

This command creates the configuration of a domain. A domain is an administrative namespace. Every domain has a configuration, which is stored in a set of files. Any number of domains each of which has a distinct administrative identity can be created in a given installation of application server. A domain can exist independent of other domains. Any user who has access to the `asadmin` script on a given system can create a domain and store its configuration in a folder of choice. By default, the domain configuration is created in the `domains` directory. You can override this location to store the configuration elsewhere.

A domain, in addition to being an administrative boundary, is also a fully compliant Java EE Server. This means that you can can deploy your Java EE Applications to the domain and run them when the domain is started. A domain provides all the necessary environment and services that are essential to run the applications.

A domain can be managed by tools such as the Administration GUI or `asadmin`.

This command is supported in local mode only.

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.

`—domaindir`
The directory where the domain is to be created. If specified, the path must be accessible in the filesystem. If not specified, the domain is created in the default domain directory.

`—template`
The file name of a domain.xml template used to create the domain. This allows domains of different types to be created. This also allows you to define your own template.

`—adminport`
The HTTP/S port for administration. This is the port to which you should point your browser (example, http://localhost:<this-port>) to manage the domain. The default value is 4848 for Platform Edition and 4849 for Enterprise Edition

`—adminuser`

The username of the adminstrator of the domain.

`—passwordfile`

The file containing the domain application server password associated with the administrative instance. The `create-domain` command reads values for AS_ADMIN_ADMINPASSWORD and the AS_ADMIN_MASTERPASSWORD from this file. The password is defined in the following form: AS_ADMIN_ADMINPASSWORD=*password*, where *password* is the actual administrator password for the domain. The syntax for each is the same as the syntax for AS_ADMIN_PASSWORD. But `create-domain` reads the value of the AS_ADMIN_ADMINPASSWORD. In general, this file can contain many other passwords required by the `asadmin` commands. In adherence to application server security policy, `asadmin` does not accept clear text passwords on the command line.

If AS_ADMIN_ADMINPASSWORD and AS_ADMIN_MASTERPASSWORD are not in the passwordfile, `create-domain` command prompts for admin password as well as master password. If AS_ADMIN_ADMINPASSWORD is present in the file that is passed into `-—passwordfile` option, the `create-domain` command does not prompt for the master password. In this case, AS_ADMIN_MASTERPASSWORD defaults to the value, `changeit`.

Additionally, you may omit the `—passwordfile` from the command line and allow the system to prompt you for these 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.

`—instanceport`

As noted above, the domain provides services so that applications can run when deployed. This (HTTP) port specifies where the web application context roots are available for a Web browser to connect to. This port is a positive integer and must be available at the time of creation of the domain.

`—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	Specifies the port number for JMS. Valid value is 7676
domain.jmxPort	Specifies the port on which the JMX connector is initialized. The valid values are 1-65535.
orb.listener.port	Specifies which ORB listener port for IIOP connections orb-listener-1 listens on.
http.ssl.port	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	Specifies which ORB listener port for IIOP connections the IIOP listener called SSL listens on.
orb.mutualauth.port	Specifies which ORB listener port for IIOP connections the IIOP listener called SSL_MUTUALAUTH listens on.

`—savemasterpassword`

Setting this option to true allows the `masterpassword` to be written to the file system. A master password is really a password for the secure key store. A domain is designed to keep its own certificate (created at the time of domain creation) in a safe place in the configuration location. This certificate is called domain's SSL server certificate. When the domain is contacted by a Web browser over a secure channel (HTTPS), this certificate is presented by the domain. The master password is supposed to protect this store (a file) that contains this certificate. This file is called `keystore.jks` and is created in the config directory of the domain created. If however, this option is chosen, the master password is saved on the disk in domain's configuration location. The master password is stored in a file called `master-password`, which is a Java JCEKS type keystore. The only advantage of using this option is in case of unattended system boots, where at the time of start-domain, the master password is not prompted for, because it will be extracted from this file.

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.

`—savelogin`

Saves the admin user name and password if you set this option to true. The default value is false. The username and password are stored in the `.asadminpass` file in user's home directory. A domain can only be created locally and hence while using the above option, the host name saved in `.asadminpass` will always be `localhost`. If the user has specified default admin port while creating the domain, there is no need to specify `-—user`, `-—passwordfile`, `-—host`, or `-—port` on any of the subsequent `asadmin` remote commands. These values will be automatically obtained.

Note – When the same user creates multiple domains having same admin port number on the same or different machines (where the home directory is NFS mounted), the command is not going to prompt whether the password should be overwritten. It will always be overwritten.

Operands

domain_name

The name of the domain to be created.

Examples

EXAMPLE 1 Using the create-domain command

The following command creates `sampleDomain` domain in the `/export/domains` directory

```
asadmin>  create-domain --domaindir /export/domains --adminport 7070 --adminuser admin --instancepo
Please enter the admin password>
Please enter the admin password again>
Please enter the master password>
Please enter the master password again>
Using default port 7676 for JMS.
Using default port 3700 for IIOP.
Using default port 8181 for HTTP_SSL.
Using default port 3820 for IIOP_SSL.
Using default port 3920 for IIOP_MUTUALAUTH.
Using default port 8686 for JMX_ADMIN.
Domain sampleDomain created.
```

EXAMPLE 2 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 --savelogin=true 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.
The admin user name and encoded password is saved in [/home/Joe/.asadminpass]. Make sure that
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also

`login(1)`, `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 [—terse=false] [—echo=false] [—interactive=true] [—host localhost]
      [—port 4848|4849] [—secure|—s] [—user admin_user] [—passwordfile filename]
      [—help] [—target target] [—passwordfile passwordfile]
      [—authrealmname auth_realm_name] [—groups user_groups[:user_groups]*]
      user_name
```

Description Creates an entry in the keyfile with the specified username, password, and groups. Multiple groups can be created by separating them with a colon (:). If *auth_realm_name* is not specified, an entry is created in the keyfile for the default realm. 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

`–t —terse` Indicates that any 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 —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

—`target`
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.

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

—`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 admin --passwordfile passwords.txt
--host pigeon --port 5001 --groups staff:manager
--authrealmname auth-realm1 sample_user
```

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

```
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-http-listener – adds a new HTTP listener socket

Synopsis **create-http-listener** [—terse=*false*] [—echo=*false*] [—interactive=*true*]
[—host *localhost*] [—port *4848*|*4849*] [—secure|−s] [—user *admin_user*]
[—passwordfile *filename*] [—help] —listeneraddress *address*
—listenerport *listener_port* —defaultvs *virtual_server* [—servername *server_name*]
[—acceptorthreads *1*] [—xpowered=*true*] [—redirectport *redirect_port*]
[—securityenabled=*false*] [—enabled=*true*] [—target *server*] *listener_id*

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

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.

`−H —host`
The machine name where the domain administration server is running. The default value is localhost.

`−p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`−s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`−u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

`—listeneraddress`
The IP address or the hostname (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.

`—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.

`—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.

`—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.

`—enabled`
If set to true, the listener is enabled at runtime.

`—target`
This option is available only in the Sun Java System Application Server Standard and 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
- *stand-alone_instance_name*, which creates the listener for a particular stand-alone server instance

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 host1 --port 4848
--listeneraddress 0.0.0.0 --listenerport 7272
--defaultvs server --servername host1.sun.com
--acceptorthreads 100 --securityenabled=false
--enabled=false sampleListener
```

EXAMPLE 1 Using the create-http-listener command *(Continued)*

```
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 [—terse=false] [—echo=false] [—interactive=true]
        [—host localhost] [—port 4848|4849] [—secure|–s] [—user admin_user]
        [—passwordfile filename] [—help] —listeneraddress address [—iiopport 1072]
        [—securityenabled=false] [—enabled=true]
        [—property (name=value)[:name=value]*] [—target server] listener_id
```

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

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.

`–H —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

`—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.

`—target`
This option is available only in the Sun Java System Application Server Standard and 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

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 4848
--listeneraddress 192.168.1.100 --iiopport 1400 sample_iiop_listener
Command create-iiop-listener executed successfully.
```

EXAMPLE 2 Using the create-iiop-listener command with the target option.

The following command creates an IIOP listener named `iiop_listener_2` for the cluster `mycluster`. It uses the target option. This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

```
asadmin> create-iiop-listener --user admin
--passwordfile passwords.txt --host host1 --port 4849
--listeneraddress 0.0.0.0 --iiopport 1401 --target mycluster iiop_listener_2
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` `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`] [—host` *localhost*`]`
`[—port` *4848|4849*`] [—secure|—s] [—user` *admin_user*`] [—passwordfile` *filename*`]`
`[—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.The name of this configuration will be `server–name-config` where server—name represents the name of an unclustered server instance. Formally, a standalone server instance has a configuration named `server–name-config` and is the only instance referencing this configuration.
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. Standalone server instances and shared server instances can be considered unclustered server instances.

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

`–t —terse`

Indicates that any 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 —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The —`passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

`—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.

The --config and --cluster options are mutually exclusive. If both are omitted, a standalone server instance is created.

`—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.

`—lbweight`
Helps assign weight for the server instance

`—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

Error Codes

0	error message
1	error message

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 [—terse=*false*] [—echo=*false*] [—interactive=*true*]
[—host *localhost*] [—port *4848*|*4849*] [—secure|–s] [—user *admin_user*]
[—passwordfile *filename*] [—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

`–t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help

Displays the help text for the command.

—target

This option 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. This 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 This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

—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 name of the mail account user provided 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, the 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` Text providing some details 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.

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

```
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 [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*] [—port *4848|4849*] [—secure|–s] [—user *admin_user*] [—passwordfile *filename*] [—help] [—target *target*] [—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*] [—allownoncomponentcallers=*false*] [—nontransactionalconnections=*false*] [—description *text*] [—property *(name=value)* [:*name=value*]*] *connectionpoolid*

Description

The create-jdbc-connection-pool command registers a new JDBC connection pool with the specified JDBC connection pool name.

This command is supported in remote mode only.

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.

–H —host
: The machine name where the domain administration server is running. The default value is localhost.

–p —port
: The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, http://localhost:4848.

: The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

–s —secure
: If set to true, uses SSL/TLS to communicate with the domain administration server.

–u —user
: The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

`—help`

Displays the help text for the command.

`—target`

This 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`. It leads to an error 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 number of connections to be removed when `idletimeout` timer expires. Connections that have idled for longer than the timeout are candidates for removal. 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. This timeout value must be kept shorter than the server side timeout value to prevent the accumulation of unusable connections in the application. The default value is 300.

`—isolationlevel`

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, isolation level 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 to 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.

`—allownoncomponentcallers`

A pool with this property set to true, can be used by non-J2EE components, that is, components other than EJBs or Servlets. The returned connection is enlisted automatically with the transaction context obtained from the transaction manager.

`—nontransactionalconnections`

A pool with this property set to true returns non-transactional connections. This connection does not get automatically enlisted with the transaction manager.

`—description`

Text providing 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 --restype javax.sql.XADataSource
--property portNumber=1527:password=APP:user=APP:serverName=
localhost:databaseName=sun-appserv-samples:connectionAttributes=\\;
create\\\\=true sample_derby_pool
Command create-jdbc-connection-pool executed successfully
```

Where, the sample_derby_pool is created. The escape character backslash (\\) 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** [—terse=*false*] [—echo=*false*] [—interactive=*true*]
[—host *localhost*] [—port *4848*|*4849*] [—secure|–s] [—user *admin_user*]
[—passwordfile *filename*] [—help] [—target *target*] —connectionpoolid *id*
[—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

–t —terse

Indicates that any 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 —host

The machine name where the domain administration server is running. The default value is localhost.

–p —port

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, http://localhost:4848.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

–s —secure

If set to true, uses SSL/TLS to communicate with the domain administration server.

–u —user

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the --user option on subsequent operations to this particular domain.

—passwordfile

The —passwordfile option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

—`target`
This option helps specify the target to which you are deploying. Valid values are:

- `server`, which deploys the component to the default server instance. This 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.

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

—`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 connection at runtime.

—`enabled`
Determines whether the JDBC resource is enabled 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 passwords.txt --connectionpoolid sample_d
Command create-jdbc-resource executed successfully.
```

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 JMS physical destination

Synopsis

```
create-jmsdest [—terse=false] [—echo=false] [—interactive=true] [—host localhost]
      [—port 4848|4849] [—secure|—s] [—user admin_user] [—passwordfile filename]
      [—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

`—t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`—p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`—s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`—u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

`—help`

Displays the help text for the command.

`—target`

This option helps specify 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 (JMS Broker), which is part of the configuration. A JMS Broker is configured in the config section of `domain.xml`. Valid values are:

- `server`, which creates the physical destination for the default server instance. This 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

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

`–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 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-resource – creates a JMS resource

Synopsis

```
create-jms-resource [—terse=false] [—echo=false] [—interactive=true]
        [—host localhost] [—port 4848|4849] [—secure|–s] [—user admin_user]
        [—passwordfile filename] [—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 is supported in remote mode only.

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.

`–H —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

`—target` This option helps specify the target for which you are creating the JMS resource. Valid values are:

- `server`, which creates the resource for the default server instance. This 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

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

`—restype` The JMS resource type, which can be `javax.jms.Topic`, `javax.jms.Queue`,`javax.jms.TopicConnectionFactory`, or `javax.jms.QueueConnectionFactory`.

`—enabled` If set to true, the resource is enabled at runtime.

`—description` Text providing details 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	This is a comma-separated list of message queue addresses. It 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: An address list composed from the jms-hosts defined in the target's jms-service configuration. The default for PE is local host and the default port number is 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`.

Property	Definition
ReconnectEnabled	If enabled (value = `true`), it indicates 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`.
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 to 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.

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

You can specify the following properties for a destination resource:

Property	Definition
Name	(Required) This property specifies the name of the physical destination to which the resource will refer. You create a physical destination with the `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 [—terse=false] [—echo=false] [—interactive=true]
      [—host localhost] [—port 4848|4849] [—secure|–s] [—user admin_user]
      [—passwordfile filename] [—help] [—targettarget]
      —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

`–t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

`—help`

Displays the help text for the command.

`—target`

This option helps specify the target to which you are deploying. This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

Valid values for target are described below.

- `server`, which creates the resource for the default server instance. This 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

`—jndilookupname`

The lookup name that the external container uses.

`—resourcetype`

This 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.
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 passwords.txt
--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 element of the `domain.xml` file.

Synopsis

`create-jvm-options` `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host` *localhost*`] [—port` *4848|4849*`] [—secure|–s] [—user` *admin_user*`]`
`[—passwordfile` *filename*`] [—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 profiler elements of the `domain.xml` file. If 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 effect. Use the `start/stop-domain` command to restart the domain administration server.

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.

`–H —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

`—target`
Specifies the target on which you are creating jvm options. Valid targets are config, instance, cluster, or server. The default is server.

`--profiler`
Indicates whether the JVM options are for the profiler. The profiler must exist for this option to be true.

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 --interactive=true --secure=true
--passwordfile passwords.txt --terse=false --user admin
--host localhost --port 4849 --target server
\\\\-Dunixlocation=/root/example:-Dvariable=
\\$HOME:-Dwindowslocation=d\\\\:\\\\\\sun\\\\\\appserver:-Doption1=-value1
```

EXAMPLE 1 Using the create-jvm-options command *(Continued)*

```
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 [—terse=false] [—echo=false] [—interactive=true]
     [—host localhost] [—port 4848|4849] [—secure|–s] [—user admin_user]
     [—passwordfile filename] [—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 a means of running short or long duration Java-based tasks within the application server environment. This command is supported in remote mode only.

Options

`–t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help
Displays the help text for the command.

—target
Indicates the location where the lifecycle is to be created. The valid targets for this command are configuration, instance, cluster, and server. The default is server.

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

—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. When this option is set to true, the system aborts the server startup if this module does not load properly. The default value is false.

`—enabled`	This option determines whether the resource is enabled at runtime. The default values is true.
`—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 for 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
--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-management-rule – creates a new management rule

Synopsis

```
create-management-rule [—terse=false] [—echo=false] [—interactive=true]
     [—host localhost] [—port 4848|4849] [—secure|—s] [—user admin_user]
     [—passwordfile filename] [—help] [—ruleenabled=true]
     [—ruledescription description] [—action action-mbean-name]
     —eventtype log|timer|trace|monitor|cluster|lifecycle|notification
     [—eventloglevel FINEST|FINER|FINE|CONFIG|INFO|WARNING|SEVERE|OFF]
     [—recordevent=true] [—eventdescription description]
     [—eventproperties (property=value[:property=value]*)] [—target target]
     rule-name
```

Description The `create-management-rule` creates a new management rule to intelligently self-manage the application server installation and deployed applications.

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.

`–H —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help
Displays the help text for the command.

—ruleenabled
Determines whether the rule is enabled or not. Default value is true.

—ruledescription
Provides the description of the rule.

—action
The action MBean associated with the event.

—eventtype
Identifies the configured event as one of the predefined event types.

—eventloglevel
Specifies at what level to record the event occurance in server log file. Default value is INFO.

—recordevent
Specifies whether the occurance of the event is to be logged or not. Default value is true. If no action is specified, the event would be logged.

—eventdescription
A description of the event.

—eventproperties
The properties defined for the event.

—target

This operand specifies the target on which you are creating a management rule. Valid values are:

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

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

Operands

rule_name

The name of the management rule.

Examples

EXAMPLE 1 using create-management-rule command to create a monitor event

```
asadmin> create-management-rule --user admin
--passwordfile adminpassword.txt --host localhost --port 4848
--eventtype monitor --eventloglevel FINE
--eventdescription "monitoring eventproperties" myRule1
Command create-management-rule executed successfully
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also

`delete-management-rule(1)`, `list-management-rules(1)`

Name create-mbean – creates and registers a custom MBean.

Synopsis **create-mbean** [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*]
[—port *4848|4849*] [—secure|–s] [—user *admin_user*] [—passwordfile *filename*]
[—help] [—name *name*] [—objectname *objectname*] [—name *name*]
[–-target=*server*] [—attributes (*name*=*value*)[:*name*=*value*]*]
implementation-class-name

Description Creates and registers a custom MBean. If the target MBeanServer is not running, the MBean is not registered.

This command is supported in remote mode only.

Options If an option has a short option name, then the short option precedes the long option name. Short options have one dash whereas long options have two dashes.

–t —terse
Indicates that any 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 —host
The machine name where the domain administration server is running. The default value is localhost.

–p —port
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

–s —secure
If set to true, uses SSL/TLS to communicate with the domain administration server.

–u —user
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

—passwordfile
The —`passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

`—help`
: Displays the help text for the command.

`--name`
: Specifies the name of the MBean definition. It should be unique for a given domain as the namespace for MBeans is shared with that for Java EE applications and modules. Therefore, you should not use the name of a deployed enterprise application for creating an MBean. The default name is the MBean's implementation class name.

`--objectname`
: Specifies the `javax.management.ObjectName` of the MBean. The `ObjectName` must be unique within the target specified, as is the case with the name of the MBean. The uniqueness is required because at runtime the MBeans are registered with their `ObjectName` and not names. The default ObjectName is of the format: `user:type=`*implementation-class-name*`,name=`*implementation-class-name*. The `user` is the name of the JMX Domain where these MBeans will be registered. No other JMX domain name is allowed.

This is the `ObjectName` that will be stored in the Application Server domain's configuration. At runtime though, when the

MBean is registered in the MBeanServer, an identifying property, `server=`*name_of_the_target_server_instance* is inserted in the `ObjectName`.

This property is not persisted. It is a runtime artifact only.

`--target`

Specify the ID of the server where the MBean will be registered. Defaults to the name of the Domain Administration Server (DAS).

`--attributes`

Specifies the names and values of the attributes for the initialization of the MBean.

Specifies the names and values of the attributes that the MBean should be initialized with. The attributes are specified in the format, `name1=value1:name2=value2:...` The types of these attributes must be simple Java Types. such as primitive data types and their wrapper classes. In general, an attribute of the MBean that could be initialized this way should have a constructor that accepts a `java.lang.String`. The data type of the attributes is found from the `MBeanInfo` of the MBean. Once initialized, these attributes are available for modification later. These attributes loosely define the metadata of the MBean.

Operands

implementation-class-name

Specifies fully qualified name of the MBean's implementation classname. The class should have a default constructor. In case of a Standard MBean, it should be the name of the class that implements the Standard MBean interface. The classes and interfaces that this MBean depends upon should be available to the server. If they are part of the server's classpath, they will be loaded by the server.

If a new MBean needs to be created while the domain administration server is running, copy all the required classes to *appserver_install_dir*/*domains_dir*/`applications/mbeans` with the proper package structure. The classes will then be dynamically loaded. It is important to note that the MBean classes will be loaded only from this location if they are not loaded from the server's classpath.

Once the MBean is created successfully, when the target server is running, the MBean definition is persisted in the server's configuration and an instance of the MBean is registered in the `MBeanServer` available in the server's runtime. Such an MBean can then be browsed using a standard JMX Console like JConsole.

Examples

EXAMPLE 1 Using create-mbean example 1

```
create-mbean --user admin --passwordfile filename.txt com.sun.example.Foo
```

This example creates an MBean definition and registers it in the runtime of the domain administration server. The name of the MBean is `com.example.Foo`, the `ObjectName` of the MBean is `user:type=com.example.Foo,name=com.sun.example.Foo,server=server`. The attributes of the MBean will assume the values dictated by the default constructor.

EXAMPLE 2 Using create-mbean example 2

```
create-mbean --user admin --passwordfile filename.txt --objectname
"user:type=file,name=students.log" --name file1 --target --attributes
Location=Root:Level=01 cluster1 com.example.Bar
```

This example assumes that there is a target with name `cluster1`, comprised of server instances server1, server2). Clusters are available only in Enterprise Edition of Application Server.

It creates an MBean definition with name `file1`, `ObjectName` `user:type=file,name=students.log` (in the configuration). The runtime MBean is registered in the default `MBeanServer` in both `server1` and `server2`. The `ObjectNames` of the registered MBeans would be `user:type=file,name=students.log,server=server1` and `user:type=file,name=students.log,server=server2` respectively. The attributes named `Location` and `Level` in the MBean would be initialized to `Root` and `01` respectively. The data-type of the attributes is derived from `MBeanInfo`. The MBeans will be available during runtime only if `server1` and `server2` are running.

Exit Status

0	command executed successfully
1	error in executing the command

See Also

`delete-mbean(1)`

`list-mbeans(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` `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host` *localhost*`] [—port` *4848|4849*`] [—secure|–s] [—user` *admin_user*`]`
`[—passwordfile` *filename*`] [—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 of a domain 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`) element does not exist, this command creates it, and then `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.

`–t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`—u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

`—help`

Displays the help text for the command.

`—target`

In Enterprise Edition, specifies the target to which you are deploying. The following values are valid:

- `server` Deploys the component to the default server instance `server` and is the default value.
- `domain` Deploys the component to the domain.

- *cluster_name* Deploys the component to every server instance in the cluster.
- *instance_name* Deploys the component to a particular sever instance.

Optional Attributes

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.
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`.

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

Operands

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

Examples

EXAMPLE 1 Using create-message-security-provider

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

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

Exit Status

0	command executed successfully
1	error in executing the command

See Also

`delete-message-security-provider(1)`, `list-message-security-providers(1)`

Name create-password-alias – creates a password alias

Synopsis **`create-password-alias`** `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host` *localhost*`] [—port` *4848|4849*`] [—secure|—s] [—user` *admin_user*`]`
`[—passwordfile` *filename*`] [—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

`—t —terse` Indicates that any 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 —host` The machine name where the domain administration server is running. The default value is localhost.

`—p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`—s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`—u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—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 domain.xml file.

Examples

EXAMPLE 1 Using create-password-alias command in interactive mode

```
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 [—terse=*false*] [—echo=*false*] [—interactive=*true*]
[—host *localhost*] [—port *4848*|*4849*] [—secure|–s] [—user *admin_user*]
[—passwordfile *filename*] [—help] [—enabled=*true*] [—target *target*]
[—jdbcjndiname *jndi_name* | —connectionpoolid *id*] [—factoryclass *classname*]
[—description *text*] [—property (*name*=*value*)[:*name*=*value*]*] *jndi_name*

Description

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

The options —`jdbcjndiname` and —`connectionpoolid` are mutually exclusive; only one should be used.

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.

`–H —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The —`passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

—`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. Valid targets are:

- `server`, which deploys the component to the default server instance. This is the default target.
- `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.

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

—`jdbcjndiname`

Specifies the JDBC resource with which database connections are obtained. It must be the name of an existing 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 scenes with 'PM' suffixed to the 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 passwords.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 passwords.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 [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*] [—port *4848*|*4849*] [—secure|—s] [—user *admin_user*] [—passwordfile *filename*] [—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

`–t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

`—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`
This path is 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
 --property defaultuser=admin:password=adminadmin sample_profiler
Command create-profiler executed successfully
```

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` `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`] [—host` *localhost*`] [—port` *4848|4849*`] [—secure|—s] [—user` *admin_user*`] [—passwordfile` *filename*`] [—help] [—threadpoolid` *threadpool*`] [—property (`*property name*=*value*`)[:`*name*=*value*`]*]` *raname*

Description

The `create-resource-adapter-config` command 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. The resource adapter config can also be created after the resource adapter is deployed. In this case, the resource adapter is restarted with the new configuration. 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

`—t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`—p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`—s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`—u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—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. This option takes only one threadpool ID.

—property
This option specifies the configuration properties of the resource adapter java bean. The properties can be specified as name value pairs separated by a colon (:).

Operands

raname
This operand indicates the connector module name. It is the value of the resource-adapter-name in the domain.xml file.

Examples

EXAMPLE 1 Using the create-resource-adapter-config command

```
asadmin> create-resource-adapter-config --user admin
--passwordfile passwords.txt --property foo=bar --threadpoolid mycustomerthreadpool
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-service – configures the starting of a DAS or node agent on an unattended boot.

Synopsis `create-service` [—name *servicename*] —passwordfile *passwordfile* [—type *das* | *nodeagent*] [—serviceproperties *serviceproperties*] *domain-or-node-agent-configuration-directory*

Description Configures the starting of a DAS or node agent on an unattended boot. On Solaris 10, this command uses the Service Management Facility (SMF). This is a local command. This command must be run as the OS-level user with superuser privileges. For AS 9.0, this is available only for Solaris 10. This command creates the service and the user has to start, enable, disable, delete, or stop the service. The DAS/node-agent configuration must be stored on a folder to which the super-user has access. The configuration cannot be stored on a network file system. This command creates the service such that it is controlled by the OS-level user, who owns the folder where the configuration of the DAS or node agent resides.

To run this command, you must have `solaris.smf.*` authorization. See the `useradd` and `usermod` manpages to find out how to set the authorizations. It is also essential for the users to have write permission in the directory tree: `/var/svc/manifest/application/SUNWappserver`. Usually, the super-user has both these permissions. If one wishes to run these commands as non-root user, then the system administrator must be contacted so that the relevant authorizations are granted.

You need to also ensure that:

- Solaris 10 administration commands such as `svccfg,` `svcs`, and `auths` are available in the PATH, so that these commands can be executed. A simple test to do so is to issue the command, `which svccfg` on a bash shell.
- You should have write permission for the path, `/var/svc/manifest/application`.

Options

—`name` Indicates the name of the service and overrides the default, if present.

—`type` Specifies whether the service pertains to DAS or node agent. Valid values are `das` and `node-agent` and the default value is `das`, indicating that the user's domain will be created as a service by default.

—`passwordfile` The —`passwordfile` option specifies the name of a file containing the password entries in a specified format. The 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, and so on.

—`serviceproperties` Specifies a colon(:)-separated list of various properties that are specific to the service. For Solaris 10, if you specify `net_privaddr`, the service's processes will be able to bind to the privileged ports (<1024) on the platform. You can bind to ports< 1024 only if the owner of the service is super-user, this is not allowed. If you specify `startinstances=true/false`, when the type is node-agent, all the instances are started when the node-agent starts up.

Operands

domain-dir or node-agent-dir

The absolute path of directory on disk that contains the configuration of the domain or node agent. For example, if your domain resides at /var/SUNWappserver/appserver/domains/domain1, specify this absolute path.

Exit Status

0	command executed successfully
1	error in executing the command

Name

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

Synopsis

```
create-ssl [—terse=false] [—echo=false] [—interactive=true] [—host localhost]
     [—port 4848|4849] [—secure|—s] [—user admin_user] [—passwordfile filename]
     [—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 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.

`–t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry

for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

`—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.
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.

Property	Definition
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 HTTP or IIOP 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`** `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host` *localhost*`] [—port` *4848|4849*`] [—secure|—s] [—user` *admin_user*`]`
`[—passwordfile` *filename*`] [—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 overridden through a system property of the corresponding name. This command adds or updates the system properties of a domain, configuration, cluster, or server instance.

Options

`—t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`—p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`—s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`—u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help
Displays the help text for the command.

—target
This option 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.

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

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`** `[—terse=`*false*`]` `[—echo=`*false*`]` `[—interactive=`*true*`]`
`[—host` *localhost*`]` `[—port` *4848|4849*`]` `[—secure|–s]` `[—user` *admin_user*`]`
`[—passwordfile` *filename*`]` `[—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 The `create-threadpool` command creates a threadpool 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

`–t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

`—target`
This option specifies the target on which you are creating the threadpool. Valid values are

- `server`, which creates the threadpool for the default server instance `server` and is the default value
- *configuration_name*, which creates the threadpool for the named configuration
- *cluster_name*, which creates the threadpool for every server instance in the cluster
- *instance_name*, which creates 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 create-threadpool Command

```
asadmin> create-threadpool --user admin1
--passwordfile password.txt --maxthreadpoolsize 100
--minthreadpoolsize 20 --idletimeout 2 --workqueues 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-transformation-rule – creates transformation rule for a deployed web service

Synopsis

```
create-transformation-rule { webservicename webservice_name } [enabled=true]
      [applyto=request] rulefilelocation rulefile_location transformation-rule-name
```

Description

Creates an XSLT transformation rule that can be applied to a webservice operation. The rule can be applied either to a request or to a response.

Options

`--webservicename`
name of the deployed web service for which you are creating a transformation rule

`--enabled`
if set to true, enables the web service endpoint.

`--operationname`
name of the web service operation

`--applyto`
the kind of operation to which the transformation tule has to be applied. Allowed values are:

- `request`, applied to a SOAP request. This is the default.
- `response`, applied to a web service response.
- `both`, applied to all methods in the web service endpoint.

`-rulefilelocation`
location of the file to do the transformation. Only XSLT files are allowed. Default location is *instance_dir*/`generated/xml/`*application_name or module_name/XSLTfilename*

Operands

transformation-rule-name
name of the transformation rule being created.

Examples

EXAMPLE 1 To create a transformation rule that applies to both request and response operations

```
create-transformation-rule --webservicename jaxrpc-simple#jaxrpc-simple.war#HelloIF
--enabled=true --applyto=both --rulefilelocation opt/SUNWappserver/generated/xml/res.xslt
ChangeResponse_Rule
Command create-transformation-rule executed successfully
```

where, `res.xslt` is the file name that stores the transformation rule.

and,`jaxrpc-simple#jaxrpc-simple.war#HelloIF` is the fully qualified name of a web service endpoint.

Exit Status

0
command executed successfully

1
error in executing the command

See Also

`delete-transformation-rule(1)`, `list-transformation-rules(1)`

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

Synopsis

```
create-virtual-server [—terse=false] [—echo=false] [—interactive=true]
      [—host localhost] [—port 4848|4849] [—secure|-s] [—user admin_user]
      [—passwordfile filename] [—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

`–t —terse` Indicates that any 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 —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

—`help`

Displays the help text for the command.

—`target`

This option 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. This 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

  This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

`—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 host 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. The default value is true.

Property	Definition
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. The default value is 300 seconds (5 minutes). Higher values provide longer single sign-on persistence for users, but 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. The default value is 60.
default-web-xml	Indicates the location of the file default-web.xml. The default location is $[S1AS_HOME]/domains/domain1/config/
allowLinking	If the value of this property is true, resources that are symbolic links will be served for all web applications deployed on this virtual server. Individual web applications may override this setting by using the property allowLinking under the sun-web-app element in the sun-web.xml file: <sun-web-app> <property name="allowLinking" value="[true|false]"/> </sun-web-app> The default value is true.

Property	Definition
accessLogWriteInterval	Indicates the number of seconds before the log will be written to the disk. The access log is written when the buffer is full or when the interval expires. If the value is 0 (zero), then the buffer is always written even if it is not full. This means that each time the server is accessed, the log message is stored directly to the file.
accessLogBufferSize	Specifies the size, in bytes, of the buffer where access log calls are stored.
allowRemoteAddress	This is a comma-separated list of regular expression patterns to which the remote client's IP address is compared. If this property is specified, the remote address must match for this request to be accepted. If this property is not specified, all requests will be accepted unless the remote address matches a denyRemoteAddress pattern. The default value for this property is null.
denyRemoteAddress	This is a comma-separated list of regular expression patterns to which the remote client's IP address is compared. If this property is specified, the remote address must not match for this request to be accepted. If this property is not specified, request acceptance is governed solely by the allowRemoteAddress property. The default value for this property is null.

Property	Definition
allowRemoteHost	This is a comma-separated list of regular expression patterns to which the remote client's host name (as returned by java.net.Socket.getInetAddress().getHostNa is compared. If this property is specified, the remote host name must match for this request to be accepted. If this property is not specified, all requests will be accepted unless the remote host name matches a denyRemoteHost pattern. The default value for this property is null.
denyRemoteHost	This is a comma-separated list of regular expression patterns to which the remote client's host name (as returned by java.net.Socket.getInetAddress().getHostNa is compared. If this property is specified, the remote host name must not match for this request to be accepted. If this property is not specified, request acceptance is governed solely by the allowRemoteHost property. The default value for this property is null.

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`:

```
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-admin-object – removes the administered object with the specified JNDI name.

Synopsis

```
delete-admin-object [—terse=false] [—echo=false] [—interactive=true]
      [—host localhost] [—port 4848|4849] [—secure|–s] [—user admin_user]
      [—passwordfile filename] [—help] [—target target] jndi_name
```

Description This command removes the administered object with the specified JNDI name.

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.

`–H —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

—`help`

Displays the help text for the command.

-–*target*

This is the name of the targets for which the administered object is to be deleted. The valid targets for this command are instance, cluster, domain, and server. Server is the default option. This option is available only in the Sun Java System Application Server Standard and Enterprise Edition. Valid values are:

- `server`, which deletes the administered object for the default server instance `server` and is the default value
- *configuration_name*, which deletes the administered object for the specified configuration
- *cluster_name*, which deletes the administered object for the specified cluster
- *instance_name*, which deletes the administered object for a particular server instance

Operands

jndi_name

JNDI name of the administered object to be deleted.

Examples

EXAMPLE 1 Using the delete-admin-object command

```
asadmin> delete-admin-object --user admin --passwordfile passwods.txt 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-audit-module – removes the named audit-module

Synopsis

delete-audit-module [—terse=*false*] [—echo=*false*] [—interactive=*true*]
[—host *localhost*] [—port *4848*|*4849*] [—secure|–s] [—user *admin_user*]
[—passwordfile *filename*] [—help] [—target *target_name*] *audit_module_name*

Description

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

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.

`–H —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

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

`—target` Specifies the target on which you are deleting the audit module. This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.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** [—terse=*false*] [—echo=*false*] [—interactive=*true*]
[—host *localhost*] [—port *4848*|*4849*] [—secure|–s] [—user *admin_user*]
[—passwordfile *filename*] [—help] [—target *target_name*] *auth_realm-name*

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

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.

`–H —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The —`passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help — Displays the help text for the command.

—target — Specifies the target on which you are deleting the authentication realm. This option is available only in the Sun Java System Application Server Standard and Enterprise Edition. 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

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

Synopsis **`delete-connector-connection-pool`** `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host` *localhost*`] [—port` *4848|4849*`] [—secure|–s] [—user` *admin_user*`]`
`[—passwordfile` *filename*`] [—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`.

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.

`–H —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

—`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 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
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` [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*] [—port *4848*|*4849*] [—secure|–s] [—user *admin_user*] [—passwordfile *filename*] [—help] [—target *target*] *jndi_name*

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

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.

`–H —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help
Displays the help text for the command.

—target
This option specifies the target from which you want to remove the connector resource. Valid targets are:

- server, which deletes the connector resource from the default server instance. This is the default value.
- domain, which deletes the connector resource from the domain.
- *cluster_name*, which deletes the connector resource from every server instance in the cluster.
- *instance_name*, which deletes the connector resource from a specified server instance.

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

Operands

jndi_name
the JNDI name of this connector resource.

Examples

EXAMPLE 1 Using the delete-connector-resource command

This example shows the usage of this command in the Platform Edition.

```
asadmin> delete-connector-resource --user admin
 --passwordfile passwords.txt jms/qConnFactory
Command delete-connector-resource executed successfully
```

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

EXAMPLE 2 Using the delete-connector-resource command

This example shows the usage of this command in the Enterprise Edition.

```
asadmin> delete-connector-resource --target server
--user admin --passwordfile passwords.txt jms/qConnFactory
Command delete-connector-resource executed successfully
```

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` `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host` *localhost*`] [—port` *4848|4849*`] [—secure|–s] [—user` *admin_user*`]`
`[—passwordfile` *filename*`] [—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

`–t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry

for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

—`target`
This option is deprecated.

—`poolname`
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 the `delete-connector-security-map` command

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` `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host` *localhost*`] [—port` *4848|4849*`] [—secure|—s] [—user` *admin_user*`]`
`[—passwordfile` *filename*`] [—help] [—target` *target*`]` *jndi_name*

Description

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

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.

`–H —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help
Displays the help text for the command.

—–target
This option helps specify the location of the custom resources that you are deleting. Valid targets are server, domain, cluster, and instance. The default is server.

- 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

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

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 given domain

Synopsis

`delete-domain` `[—domaindir` *install_dir*`/domains] [—terse=`*false*`] [—echo=`*false*`]`
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.

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` `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`] [—host` *localhost*`]`
`[—port` *4848|4849*`] [—secure|—s] [—user` *admin_user*`] [—passwordfile` *filename*`]`
`[—help] [—target` *target*`]` *username*

Description

The `delete-file-user` command deletes the entry in the keyfile with the specified username.

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.

`–H —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help
Displays the help text for the command.

—target
This is the name of the target on which the command operates. This option is available only in the Sun Java System Application Server Standard and Enterprise Edition. The valid targets are:

- server, which deletes the file user on the default server instance. This is the default value
- domain, which deletes the file user in the domain
- *cluster_name*, which deletes the file user from every server instance in the cluster
- *instance_name*, which deletes the file user from a particular server instance

Operands

username
This is the name of file user to be deleted.

Examples

EXAMPLE 1 Using the delete-file-user command

```
asadmin> delete-file-user --user admin --passwordfile passwords.txt --host pigeon --port 5001
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-listener – removes an HTTP listener

Synopsis `delete-http-listener` [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*] [—port *4848*|*4849*] [—secure|—s] [—user *admin_user*] [—passwordfile *filename*] [—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

`–t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

—`target` This option is available only in the Sun Java System Application Server Standard and 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 host1 --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` `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host` *localhost*`] [—port` *4848*|*4849*`] [—secure|–s] [—user` *admin_user*`]`
`[—passwordfile` *filename*`] [—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

`–t —terse`

Indicates that any 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 —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

—`help`

Displays the help text for the command.

—`target`

This option is available only in the Sun Java System Application Server Standard and 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 host1 --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`** [`—terse=`*false*] [`—echo=`*false*] [`—interactive=`*true*] [`—host` *localhost*] [`—port` *4848|4849*] [`—secure|–s`] [`—user` *admin_user*] [`—passwordfile` *filename*] [`—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. The user authenticates using the password identified for the administration server. Additionally, the instance must already exist within the domain served by the administration server. Use this command with discretion since it is destructive and cannot be undone.

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 `–t —terse`

Indicates that any 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 —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry

for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

—`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
Deleted Instance server1 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 [—terse=*false*] [—echo=*false*] [—interactive=*true*]
[—host *localhost*] [—port *4848*|*4849*] [—secure|–s] [—user *admin_user*]
[—passwordfile *filename*] [—help] [—target *target*] *jndi_name*

Description

The `delete-javamail-resource` command removes the specified JavaMail session resource. On Standard and Enterprise Editions, make sure to remove all references to this resource before executing this command. This command is supported in remote mode only.

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.

`–H —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

—`target` This option helps specify the target from which you are deleting the JavaMail session resource. Valid values are:

- `server`, which deletes the resource from the default server instance. This 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 This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

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 [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*] [—port *4848|4849*] [—secure|–s] [—user *admin_user*] [—passwordfile *filename*] [—help] [—cascade=false] *connectionpoolid*

Description

The `delete-jdbc-connection-pool` command deletes a JDBC connection pool. The operand identifies the JDBC connection pool to be deleted.

On Enterprise Edition, ensure that all associations to this resource are removed before executing the `delete-jdbc-connection-pool` command.

This command is supported in remote mode only.

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.

–H —host

The machine name where the domain administration server is running. The default value is localhost.

–p —port

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

–s —secure

If set to true, uses SSL/TLS to communicate with the domain administration server.

–u —user

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

—passwordfile

The —`passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

`—cascade` If the option is set to true, all the JDBC resources associated with the pool, 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.

`—target` This option is deprecated.

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 --user admin --passwordfile passwords.txt --host localhost --po

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

Where: asadmin is the command prompt and sample_derby_pool is the JDBC 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** [—terse=*false*] [—echo=*false*] [—interactive=*true*]
[—host *localhost*] [—port *4848*|*4849*] [—secure|–s] [—user *admin_user*]
[—passwordfile *filename*] [—help] [—target *target*] *jndi_name*

Description The `delete-jdbc-resource` command removes a JDBC resource. On Standard and Enterprise Editions, make sure that all associations to the JDBC resource are removed before you execute this command. This command is supported in remote mode only.

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.

–H —host
The machine name where the domain administration server is running. The default value is localhost.

–p —port
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

–s —secure
If set to true, uses SSL/TLS to communicate with the domain administration server.

–u —user
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

—passwordfile
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

—`target` This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

This option helps specify the target from which you are removing the JDBC resource. Valid targets are:

- `server`, which removes the resource from the default server instance. This is the default value.
- `domain`, which removes the resource from the domain.
- *cluster_name*, which removes the resource from every server instance in the cluster.
- *instance_name*, which removes the resource from a particular sever instance.

Operands *jndi_name* The JNDI name of this JDBC resource to be removed.

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

The following example shows how to delete a JDBC resource in Sun Java System Application Server Platform Edition.

```
asadmin> delete-jdbc-resource --user admin --passwordfile passwords.txt
jdbc/DerbyPool
Command delete-jdbc-resource executed successfully.
```

EXAMPLE 2 Using the delete-jdbc-resource command

The following example shows how to delete a JDBC resource in Sun Java System Application Server Enterprise Edition.

```
asadmin> delete-jdbc-resource --user admin --passwordfile passwords.txt
--target domain jdbc/DerbyPool
Command delete-jdbc-resource executed successfully.
```

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 JMS destination

Synopsis **delete-jmsdest** [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*] [—port *4848*|*4849*] [—secure|–s] [—user *admin_user*] [—passwordfile *filename*] [—help] [—target *target*] —desttype *type dest_name*

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

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.

–H —host
: The machine name where the domain administration server is running. The default value is localhost.

–p —port
: The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, http://localhost:4848.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

–s —secure
: If set to true, uses SSL/TLS to communicate with the domain administration server.

–u —user
: The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the --user option on subsequent operations to this particular domain.

—passwordfile
: The —passwordfile option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

—`target`
This option helps specify 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. This 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 This option is available only in

the Sun Java System Application Server Standard and Enterprise Edition.

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

Operands *dest_name*
The unique identifier of the JMS destination to be deleted.

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

The following command deletes the queue named `PhysicalQueue`:

EXAMPLE 1 Using the delete-jmsdest command *(Continued)*

```
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-resource – removes a JMS resource

Synopsis

delete-jms-resource [—terse=*false*] [—echo=*false*] [—interactive=*true*]
[—host *localhost*] [—port *4848|4849*] [—secure|–s] [—user *admin_user*]
[—passwordfile *filename*] [—help] [—target *target*] *jndi_name*

Description

The `delete-jms-resource` command removes the specified JMS resource. On Standard and Enterprise Editions, make sure to remove all references to this resource before executing this command. This command is supported in remote mode only.

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.

`–H —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

`—target` This option helps specify the target from which you are deleting the JMS resource. Valid values are:

- `server`, which deletes the resource from the default server instance. This 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

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

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 [—terse=false] [—echo=false] [—interactive=true]
        [—host localhost] [—port 4848|4849] [—secure|–s] [—user admin_user]
        [—passwordfile filename] [—help] [—target target] jndi_name
```

Description

The `delete-jndi-resource` command removes the specified JNDI resource. This command is supported in remote mode only.

In Standard and Enterprise Editions, you must remove all associations to the JNDI resource before you execute this command.

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.

`–H —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

`—target`
This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

Valid targets are described below.

- `server`, which deletes the resource from the default server instance. This is the default value
- `domain`, which deletes the resource from the domain
- *cluster_name*, which deletes the resource for every server instance in the cluster
- *instance_name*, which deletes the resource from the specified server instance

Operands

jndi_name
The name of the JNDI resource to be removed.

Examples

EXAMPLE 1 Using the delete-jndi-resource command

```
asadmin> delete-jndi-resource --user admin --passwordfile passwords.txt --host pigeon --port 4001 s
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 [—terse=false] [—echo=false] [—interactive=true]
        [—host localhost] [—port 4848|4849] [—secure|–s] [—user admin_user]
        [—passwordfile filename] [—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

`–t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

`—target`
This option helps specify the target from which you want to remove the JVM options. Valid target is server, cluster, or instance. The default is server.

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

`—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
--interactive=true --secure=true --passwordfile passwords.txt
--terse=false --user admin --target server --host localhost
--echo=true --port 4849 "\\-Dtmp=sun"
```

EXAMPLE 1 Using the delete-jvm-options command *(Continued)*

```
Command delete-jvm-options executed successfully
```

Where more than one JVM options are deleted.

```
asadmin> delete-jvm-options -e \\-Doption1=value1
--interactive=true --secure=true --passwordfile passwords.txt
--terse=false --user admin --target server --host localhost
--echo=true --port 4849 "\\-Doption1=value1:-Doption2=value2"
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`** `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host` *localhost*`] [—port` *4848|4849*`] [—secure|—s] [—user` *admin_user*`]`
`[—passwordfile` *filename*`] [—help] [—target` *target*`]` *module_name*

Description The `delete-lifecycle-module`removes the lifecycle module. This command is supported in remote mode only.

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.

`–H —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help
: Displays the help text for the command.

—target
: This option helps specify the location of the lifecycle module. The valid targets for this command are configuration, instance, cluster, or server.

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

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-management-rule – removes a specified management rule

Synopsis **`delete-management-rule`** `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host `*localhost*`] [—port `*4848|4849*`] [—secure|–s] [—user `*admin_user*`]`
`[—passwordfile `*filename*`] [—help] [—target `*target*`]` *rulename*

Description The `delete-management-rule` removes the management rule you specify.

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.

`–H —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

—`help`

Displays the help text for the command.

—*target*

This option helps specify the target for which you are deleting a management rule. The valid values for this command are:

- *configuration_name*, which deletes the management rule for the named configuration
- *cluster_name*, which deletes the management rule for every server instance in the cluster
- *instance_name*, which deletes the management rule for a particular server instance

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

Operands

rule_name

The name of the management rule.

Examples

EXAMPLE 1 using delete-management-rule

```
asadmin> delete-management-rule --user admin
--passwordfile adminpassword.txt --target myinstance myRule1
Command delete-management-rule executed successfully
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also

`create-management-rule(1)`, `list-management-rules(1)`

Name

delete-mbean – deletes a custom MBean.

Synopsis

delete-mbean [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*]
[—port *4848*|*4849*] [—secure|–s] [—user *admin_user*] [—passwordfile *filename*]
[—help] [—target=*server*] name

Description

Deletes a custom MBean. Ensure that the target MBeanServer is running.

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.

`–t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help
Displays the help text for the command.

—target
The target for the MBean. Identifies the server instance. Defaults to the name of the Domain Adminstration Server (DAS). If there are multiple references to an MBean in various servers, only one specific reference is deleted. When the last reference is deleted, the MBean definition is deleted from the domain.

Operands

name
Identifies a custom MBean by name. The default name is the MBean's implementation class name.

Examples

EXAMPLE 1 Using delete-mbean

```
delete-mbean --user admin --passwordfile filename.txt mbeantest1
```

This example shows the deletion of MBean, mbeantest1

Exit Status

0	command executed successfully
1	error in executing the command

See Also

create-mbean(1)

list-mbeans(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` `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host` *localhost*`] [—port` *4848|4849*`] [—secure|–s] [—user` *admin_user*`]`
`[—passwordfile` *filename*`] [—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.

`–t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

`—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-password-alias – deletes a password alias

Synopsis

```
delete-password-alias [—terse=false] [—echo=false] [—interactive=true]
      [—host localhost] [—port 4848|4849] [—secure|–s] [—user admin_user]
      [—passwordfile filename] [—help] aliasname
```

Description This command deletes a password alias.

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.

`–H —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

—`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 /home/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`** `[—terse=`*false*`]` `[—echo=`*false*`]` `[—interactive=`*true*`]` `[—host` *localhost*`]` `[—port` *4848|4849*`]` `[—secure|–s]` `[—user` *admin_user*`]` `[—passwordfile` *filename*`]` `[—help]` `[—target` *target*`]` *jndi_name*

Description The `delete-persistence-resource` command removes a persistence resource. This command is supported in the remote mode only. When you delete a persistence resource, the command also removes the jdbc resource if it was created using the `create-persistence-resource` command with the option `—connectionpoolid`. Please refer to the `create-persistence-resource` command manpage for details. If you are using the Application Server Enterprise Edition, make sure that you remove all associations to this resource and then execute this command.

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.

`–H —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—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 Standard and Enterprise Edition. Valid targets are:

- server, which deletes the resource from the default server instance. This is the default target.
- domain, which removes the resource from the domain.
- *cluster_name*, which removes the resource from every server instance in the cluster.
- *instance_name*, which removes the component from 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 passwords.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 – removes the specified profiler element

Synopsis

delete-profiler [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*] [—port *4848*|*4849*] [—secure|–s] [—user *admin_user*] [—passwordfile *filename*] [—help] [—target *target_name*]

Description

The delete-profilercommand deletes the profiler element you specify. 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

–t —terse

Indicates that any 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 —host

The machine name where the domain administration server is running. The default value is localhost.

–p —port

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, http://localhost:4848.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

–s —secure

If set to true, uses SSL/TLS to communicate with the domain administration server.

–u —user

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the --user option on subsequent operations to this particular domain.

—passwordfile

The —passwordfile option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help
: Displays the help text for the command.

—target
: This option 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

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

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 resource adapter configuration

Synopsis

delete-resource-adapter-config [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*] [—port *4848*|*4849*] [—secure|–s] [—user *admin_user*] [—passwordfile *filename*] [—help] *raname*

Description

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

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.

`–H —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The —`passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help
Displays the help text for the command.

—target
This option is deprecated.

Operands

raname
This operand helps specify the connector module name. This value is kept in the resource-adapter-name in the domain.xml file.

Examples

EXAMPLE 1 Using the delete-resource-adapter-config command

```
asadmin> delete-resource-adapter-config --user admin1
--passwordfile passwords.txt 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-ssl – deletes the SSL element in the selected HTTP listener, IIOP listener, or IIOP service

Synopsis

```
delete-ssl [—terse=false] [—echo=false] [—interactive=true] [—host localhost]
      [—port 4848|4849] [—secure|—s] [—user admin_user] [—passwordfile filename]
      [—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.

`—t —terse` Indicates that any 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 —host` The machine name where the domain administration server is running. The default value is localhost.

`—p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`—s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`—u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

`—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 deleted. 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 [—terse=false] [—echo=false] [—interactive=true]
      [—host localhost] [—port 4848|4849] [—secure|–s] [—user admin_user]
      [—passwordfile filename] [—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 overridden through a system property of the corresponding name. This command deletes system properties of a domain, configuration, cluster, or server instance.

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.

`–H —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help
: Displays the help text for the command.

—target
: This option 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.

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

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 [—terse=*false*] [—echo=*false*] [—interactive=*true*]
[—host *localhost*] [—port *4848*|*4849*] [—secure|–s] [—user *admin_user*]
[—passwordfile *filename*] [—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

`–t —terse`

Indicates that any 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 —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

`—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 command

```
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-transformation-rule – deletes the transformation rule of a given web service

Synopsis

`delete-transformation-rule` `{webservicename` *webservice_name*`}` *transformation-rule-name*

Description

Deletes an XSLT transformation rule of a given web service.

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.

`–H —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help
Displays the help text for the command.

--webservicename
name of the deployed webservice.

Operands

transformation-rule-name
name of the transformation rule to be deleted.

Examples

EXAMPLE 1 To delete a transformation rule that is applied to a webservice

```
asadmin>delete-transformation-rule --webservicename jaxrpc-simple#jaxrpc-simple.war#HelloIF
 ChangeResponse_Rule
Command delete-transformation-rule executed successfully
```

where,jaxrpc-simple#jaxrpc-simple.war#HelloIF is the fully qualified name of a web service endpoint.

ChangeResponse_Rule is the name of the transformation rule.

Exit Status

0	command executed successfully
1	error in executing the command

See Also

create-transformation-rule(1), list-transformation-rules(1)

Name delete-virtual-server – removes a virtual server

Synopsis

```
delete-virtual-server [—terse=false] [—echo=false] [—interactive=true]
      [—host localhost] [—port 4848|4849] [—secure|—s] [—user admin_user]
      [—passwordfile filename] [—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

`–t —terse` Indicates that any 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 —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

—`target` This option 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

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

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 [—terse=false] [—echo=false] [—interactive=true] [—host localhost]
       [—port 4848|4849] [—secure|-s] [—user admin_user] [—passwordfile filename]
       [—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] [—deploymentplan deployment_plan]
       [—enabled=true] [—generatermistubs=false] [—availabilityenabled=false]
       [—libraries jar_file[(path_separator)jar_file*]] [—target target] filepath
```

Description Deploys an enterprise application, web application, EJB module, connector module, or application client module. 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

`–t —terse` Indicates that any 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 —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s ––secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u ––user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`––passwordfile`
The —`passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

`—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`, `postgresql`, `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 specifie 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.

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

`—enabled`
If set to true (default), allows users to access the application. If set to false, users will not be able to access the application. For Standard and 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.

`—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.

`—libraries`
: Specify the library JAR files by their relative or absolute paths. Specify relative paths relative to *instance-root*`/lib/applibs`. The JAR files are separated by a colon on Unix and Linux systems and by a semicolon on Windows systems. The libraries are made available to the application in the order specified. Place the dependent JAR files in the *domain-dir*`/lib` directory.

`—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.

```
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 [—terse=false] [—echo=false] [—interactive=true] [—host localhost]
        [—port 4848|4849] [—secure|–s] [—user admin_user] [—passwordfile filename]
        [—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]
        [—libraries jar_file[(path_separator)jar_file*]] [—target target] dirpath
```

Description

Use this command to deploy an application directly from a development directory. The appropriate directory hierarchy and deployment descriptors conforming to the Java EE specification must exist in the deployment directory.

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

`–t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—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, postgresql, 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 specifie 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

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.

—libraries

Specify the library JAR files by their relative or absolute paths. Specify relative paths relative to *instance-root*/lib/applibs. The JAR files are separated by a colon on Unix and Linux systems and by a semicolon on Windows systems. The libraries are made available to the application in the order specified. Place the dependent JAR files in the *domain-dir*/lib directory.

—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 [—terse=false] [—echo=false] [—interactive=true] [—host localhost]
    [—port 4848|4849] [—secure|—s] [—user admin_user] [—passwordfile filename]
    [—help] [—target target_name] component_name
```

Description The `disable` command immediately disables the named component. The component must have been deployed. If the component has not been deployed, an error message is returned.

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.

`–H —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—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 command

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

Exit Status

0	command executed successfully
1	error in executing the command

See Also

deploy(1), deploydir(1), undeploy(1), enable(1)

Name display-error-distribution – displays distribution of errors from instance server.log at module level

Synopsis `display-error-distribution [—target instance ] timestamp`

Description Displays distribution of errors from instance server.log at module level. This command runs in remote mode.

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.

`—H —host` The machine name where the domain administration server is running. The default value is localhost.

`—p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`—s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`—u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help

Displays the help text for the command.

—target

This is the name of the target upon which the command is operating. For Platform Edition, the valid target for this command is instance. For Enterprise Edition, instance and cluster are valid targets.

Operands

timestamp

The time at which the error logs are generated. The error logs are maintained in the memory. Timestamp should be a long value that represents the number of milliseconds that have passed since January 1, 1970

Examples

EXAMPLE 1 Using display-error-distribution

```
asadmin> display-error-distribution 1127239511875
******************************************************************
Severity Warning   moduleID
--------------------------
 1          2        javax.enterprise.system.container.web
 0         18     javax.enterprise.system.tools.admin.server.mbeans
...
******************************************************************
Command display-error-distribution executed successfully.
```

Exit Status

0

command executed successfully

1

error in executing the command

See Also

display-error-statistics(1)

, display-log-records(1)

Name

display-error-statistics – displays a summary of list of severities and warnings

Synopsis

display-error-statistics [—target *instancename/clustername*]

Description

This command displays a summary of list of severities and warnings in server.log since last server restart. This command runs in remote mode.

Options

—target

This is the name of the target upon which the command is operating. For Platform Edition, the valid target for this command is instance. For Enterprise Edition, instance and cluster are valid targets.

Examples

EXAMPLE 1 Using display-error-statistics

```
asadmin> display-error-statistics --passwordfile passwordfile.txt --user admin --target server --ho
Timestamp                              Severity  Warning
---------------------------------------------------------
1137094032133(Jan 12, 2006 11:27:12 AM)     1        13
1137090432133(Jan 12, 2006 10:27:12 AM)     0        0
1137086832133(Jan 12, 2006 9:27:12 AM)      0        0
1137083232133(Jan 12, 2006 8:27:12 AM)      0        0
1137079632133(Jan 12, 2006 7:27:12 AM)      0        0
---------------------------------------------------------
Command display-error-statistics executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also

display-error-distribution(1)

, display-log-records(1)

Name

display-license – displays the license information

Synopsis

`display-license` `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`] [—host` *localhost*`] [—port` *4848|4849*`] [—secure|–s] [—user` *admin_user*`] [—passwordfile` *filename*`] [—help]`

Description

`display-license` displays the license information. This command can run both locally and remotely.

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.

`–H —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—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 9 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 display-log-records – displays all the error messages for a given module at a given timestamp

Synopsis **`display-log-records`** `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host` *localhost*`] [—port` *4848|4849*`] [—secure|–s] [—user` *admin_user*`]`
`[—passwordfile` *filename*`] [—help] [—errorlevel` *SEVERE/WARNING* `]`
`[—timestamp` *timestamp*`] [-target` *target*`] {module-id` *[: module-id]**`}`

Description This command displays all the error messages for a given module at a given timestamp. This command can run in remote mode.This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

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.

`–H —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

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

`—target` This is the name of the target upon which the command is operating. For Platform Edition, the valid target for this command is instance. For Enterprise Edition, instance and cluster are valid targets.

`--errorlevel` Allowed values are SEVERE and WARNING.

`--timestamp` The time specified at which the error logs are generated.

Operands

`module-id` Module for which the error logs are to be displayed.

Examples

EXAMPLE 1 Using display-log-records

```
asadmin> display-log-records --passwordfile /passwords --user admin --target server --host localhos

----------------------------------------------------------------------
RecNumber = 5849
dateTime = Thu Jan 12 11:27:34 PST 2006
msgId = WEB0335
level = WARNING
productName = sun-appserver-pe9.0
logger = javax.enterprise.system.container.web
nvp = _ThreadID=10;_ThreadName=main;_RequestID=a4a52e69-ed14-4d0c-ada7-4fe07382c158;
message =  http-listener attribute family not supported
```

EXAMPLE 1 Using display-log-records *(Continued)*

```
----------------------------------------------------------------------
RecNumber = 5848
dateTime = Thu Jan 12 11:27:34 PST 2006
msgId = WEB0334
level = WARNING
productName = sun-appserver-pe9.0
logger = javax.enterprise.system.container.web
nvp = _ThreadID=10;_ThreadName=main;_RequestID=a4a52e69-ed14-4d0c-ada7-4fe07382c158;
message =  http-file-cache attribute hash-init-size not supported
----------------------------------------------------------------------
Command display-log-records executed successfully.
```

Displays list of all severe messages generated for JMS module at 11:50.

Exit Status

0	command executed successfully
1	error in executing the command

See Also

`display-error-distribution(1)`

, `display-error-statistics(1)`

Name enable – enables the component

Synopsis

```
enable [—terse=false] [—echo=false] [—interactive=true] [—host localhost]
      [—port 4848|4849] [—secure|—s] [—user admin_user] [—passwordfile filename]
      [—help] [—target target_name] component_name
```

Description The `enable` command enables the specified component. If the component is already enabled, then it is re-enabled. The component must have been deployed in order to be enabled. If it has not been deployed, then an error message is returned. This command is supported in remote mode only.

Options

`—t —terse` Indicates that any 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 —host` The machine name where the domain administration server is running. The default value is localhost.

`—p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`—s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`—u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—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 command

```
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

export – marks a variable name for automatic export to the environment of subsequent commands in multimode

Synopsis

export [*name=value* [*name=value*]*]

Description

The export command marks a variable name for automatic export to the environment of subsequent commands. All subsequent commands use the variable name value 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 command

```
asadmin> export
AS_ADMIN_USER = admin
AS_ADMIN_HOST = bluestar
AS_ADMIN_PREFIX = server1.jms-service
AS_ADMIN_PORT = 8000
```

EXAMPLE 2 using export command to set an environment variable

```
asadmin> export AS_ADMIN_HOST=bluestar
In this case, the AS_ADMIN_HOST environment variable has been set to bluestar.
```

EXAMPLE 3 Using export command to set multiple environment variables

```
asadmin> export AS_ADMIN_HOST=bluestar AS_ADMIN_PORT=8000
AS_ADMIN_USER=admin AS_ADMIN_PREFIX=server1.jms-service
In this case, the environment variables have been set to:
host is set to bluestar
port is set to 8000
administrator user is set to admin
prefix is set to server1.jms-service
```

Exit Status

0 command executed successfully

1 error in executing the command

See Also

unset(1), multimode(1)

Name flush-jmsdest – purges messages in a JMS destination.

Synopsis **`flush-jmsdest`** `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`] [—host` *localhost*`] [—port` *4848|4849*`] [—secure|—s] [—user` *admin_user*`] [—passwordfile` *filename*`] [—help] --desttype|-T topic|queue [—target` *target (Default Server)*`]` *destname*

Description The `flush-jmsdest` command purges the messages from a physical destination in the specified target's JMS Service configuration.

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.

`—H —host`
The machine name where the domain administration server is running. The default value is localhost.

`—p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`—s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`—u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

`—target`
This option helps specify the location of the JMS destination from where you want to clean the messages. Valid values are:

- `server`, which deletes the physical destination from the default server instance. This 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 This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

`--desttype`
This option indicates the type of physical destination from where you want to purge messages. The supported destination types are topic and queue.

Operands

dest_name
The unique identifier of the JMS destination to be purged.

Examples

EXAMPLE 1 Using the flush-jmsdest command

The following command purges messages from the queue named `PhysicalQueue`:

```
asadmin> flush-jmsdest --user admin --passwordfile passwords.txt
--host localhost --port 4848 --desttype queue PhysicalQueue
```

EXAMPLE 1 Using the flush-jmsdest command *(Continued)*

```
Command flush-jmsdest executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also

`create-jmsdest(1)`, `list-jmsdest(1)`, `delete-jmsdest(1)`

Name freeze-transaction-service – freezes the transaction subsystem

Synopsis **`freeze-transaction-service`** `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host `*localhost*`] [—port `*4848|4849*`] [—secure|–s] [—user `*admin_user*`]`
`[—passwordfile `*filename*`] [—help] [`*target*`]`

Description The `freeze-transaction-service` command freezes the transaction subsystem during which time all the inflight transactions are suspended. Invoke this command before rolling back any inflight transactions. Invoking this command on an already frozen transaction subsystem has no effect. This command is supported in remote mode only.

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.

`–H —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

`—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
Command freeze-transaction-service executed successfully
```

Exit Status

0 command executed successfully

1 error in executing the command

See Also

`list-transaction-id(1)`, `unfreeze-transaction-service(1)`, `rollback-transaction(1)`

Name generate-diagnostic-report – generates reports that can help diagnose application server malfunctioning

Synopsis **`generate-diagnostic-report`** `[—terse=`*false*`]` `[—echo=`*false*`]` `[—interactive=`*true*`]` `[—host` *localhost*`]` `[—port` *4848|4849*`]` `[—secure|–s]` `[—user` *admin_user*`]` `[—passwordfile` *filename*`]` `[—help]` `[—local=`*false*`]` `[—outputfile` *jar_file_name*`]` `[—file` *filename*`]` `[—bugids` *bugids*`]` `[—logstartdate` *start-date*`]` `[—logenddate` *end-date*`]` `[—targetdir` *local_dir_path*`]` *target*

Description The `generate-diagnostic-report` command generates an HTML report that contains pointers or navigational links to a application server installation details such as configuration details, HADB information, logging details, process specific information, for an application server instance. If report generation is targeted for a domain, data is collected for all instances belonging to the domain and is stored on DAS. Such data may help diagnose application server malfunctioning such as exceptions, performance bottlenecks, and unexpected results. This command is supported in remote and local mode. In local mode, reports can be generated for a DAS, a server instance, or a node agent. In remote mode, this command can generate reports for all the targets supported by the local mode and for the entire domain or a cluster.

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.

`–H —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

`—help`

Displays the help text for the command.

`—outputfile`

Absolute path to the filename on the client machine. The filename must end with a .jar extension. This option is mandatory in both the local and remote mode.

`—file`

A text file describing customer's information such as customer name, customer point of contact, error description. Contents of this file are appended to the diagnostic report.

`—bugids`

One or more IDs of known bugs similar to customer issue, separated by comma.

`—logstartdate`

Use the mm/dd/yy format to specify the date from which `server.log` files for server instances are captured (if log rotation is enabled). If the date is not specified, number of entries from `server.log` file as specified by `max-no-of-entries` matching `min-log-level` in diagnostic service are collected.

`—logenddate`
Date in mm/dd/yy format. If specified, takes precedence over `max-no-of-entries` from diagnostic-service configuration.If you specify a `—logenddate`, you will need to specify a `—logstartdate` also. If specified, entries between `—logstartdate` and `—logenddate` matching `min-log-level` are captured. If this option is not specified, `max-no-of-entries` from diagnostic-service is used to limit the `server.log` content being captured.

`—local`
If set to true, the `generate-diagnostic-report` command runs in local mode and collects a limited set of information. When the command is run locally for a domain, data for the default server instance, that is, the DAS for the domain, is collected. In local mode, this command can generate report for a DAS, a server instance, or a node agent.

`—targetdir`
This option is required only if the command is run locally. If target is a domain name, this value is parent directory of the domain upon which the command will operate. This is a mandatory field in local mode.

Operands

target:
allowed values are domain, cluster, nodeagent and instance.

domain:
generates report for all clustered and non clustered instances administered by the DAS, including default admin server instance. This command when executed locally, collects information for default server instance only.

cluster:
generates report for every server instance in the cluster.

nodeagent:
generates report for a particular physical node; that is, for instances belonging to the node.

instance:
generates report for a particular server instance.

Examples

EXAMPLE 1 Using the generate-diagnostic-report command (remote mode)

```
asadmin> generate-diagnostic-report
 --user admin --port 4848 --outputfile /export/software/sjsas/diagnostic-reports/domain1.jar domain
Please enter the admin password>
Following attributes from domain.xml are masked with **** in the generated report.
domain/configs/config=server-config/jms-service/jms-host=default_JMS_host/admin-password="admin"
If you want to mask additional properties, use create-password-alias and set com
mand before continuing the report generation.
Press ’y’ to continue or ’n’ to exit : y
Command generate-diagnostic-report executed successfully.
```

EXAMPLE 2 Using the generate-diagnostic-report command (local mode)

```
asadmin> asadmin generate-diagnostic-report --user admin --local=true --outputfile /export/sof
Following attributes from domain.xml are masked with **** in the generated repor
t.domain/configs/config=server-config/jms-service/jms-host=default_JMS_host/admin-
password="admin"
If you want to mask additional properties, use create-password-alias and set com
mand before continuing the report generation.
Press ’y’ to continue or ’n’ to exit : y
Report File : /export/software/sjsas/diagnostic-reports/domain1.jar
Command generate-diagnostic-report executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

Name generate-jvm-report – shows the threads, classes and memory for a given target instance.

Synopsis

```
generate-jvm-report [—terse=false] [—echo=false] [—interactive=true]
      [—host localhost] [—port 4848|4849] [—secure|–s] [—user admin_user]
      [—passwordfile filename] [—help] [target]
      [--type=summary|memory|class|thread]
```

Description This command shows the threads (dump of stack trace), classes and memory for a given target instance, including the Domain Administration Service. This command works only with the application server instance processes. This command replaces the traditional techniques like sending ctrl+break or kill -3 signals to application server processes. The command will not work if the target server instance is not running.

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.

`–H —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help
Displays the help text for the command.

—type
The type of report user wants to see.

- summary, which displays summary information about the threads/classes and memory.
- memory, which provides information about heap and non-heap memory consumption, memory pools, and garbage collection statistics for a given target instance
- classes, which gives information about the class loader for a given target instance
- threads, which provides information about threads running and the thread dump (stack trace) for a given target instance.

Operands

––target
This option specifies the ending location of the connector resources. Valid targets are server, domain, cluster, and instance. The default target is server.

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

Examples

EXAMPLE 1 Using the generate-jvm-report command

```
asadmin> generate-jvm-report --user admin --passwordfile passwords.txt
--type summary server1
Operating System Information:
Name of the Operating System: Linux
Binary Architecture name of the Operating System: i386, Version:
2.6.9-22.ELsmp
Number of processors available on the Operating System: 2
...
...
...
user.language = en
user.name = root
user.timezone = America/Los_Angeles
Command generate-jvm-report executed successfully
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also

(),

Name

get – gets the values of the monitorable or configurable attributes

Synopsis

```
get [—terse=false] [—echo=false] [—interactive=true] [—host localhost]
      [—port 4848|4849] [—secure|–s] [—user admin_user] [—passwordfile filename]
      [—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.diagnostic-service ■ 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.diagnostic-service ■ 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`

ID	Command	Output/Comment
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-enab = falseserver.http-service.http-listener.http-listener-1.default-virtual-s = 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-monit 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.

ID	Command	Output/Comment
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.
3	`get server.monitoring-service.module-monitoring-levels.*`	server.monitoring-service.module-monitoring-levels.connector-connectio = 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-poo = 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`
		server.monitoring-service.module-monitoring-levels.jvm
		= HIGH

	There is no space before or after the = sign.	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

`–t —terse`

Indicates that any 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 —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The —`passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

`—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.

EXAMPLE 1 Using the get command with wildcard *(Continued)*

Command	Operation
`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.

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.bean1.* 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.bean1.bean-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-cachemethods.method1.* 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.orbconnmgr.*	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 – retreives the client stub JAR

Synopsis **get-client-stubs** [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*] [—port *4848*|*4849*] [—secure|–s] [—user *admin_user*] [—passwordfile *filename*] [—help] [—target *target_name*] [—appname *application_name*] *local_directory_path*

Description The `get-client-stubs` command 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

`–t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

`--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 get-health – provides information on the cluster health

Synopsis

```
get-health [—terse=false] [—echo=false] [—interactive=true] [—host localhost]
      [—port 4848|4849] [—secure|—s] [—user admin_user] [—passwordfile filename]
      [—help] [—target cluster_name]
```

Description The `get-health` command gets information about the health of the cluster. Note that if GMS is not enabled in Application Server, the basic information about whether the server instances in this cluster are running or not running is returned.

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.

`–H —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

`--target` The name of the cluster for which you want the health information.

Examples

EXAMPLE 1 Using get-health

```
asadmin> get-health --user admin --passwordfile password.txt
--host fuyako --port 7070 --target cluster
Command get-health executed successfully
```

Exit Status

0	command executed successfully
1	error in executing the command

Name help – displays the asadmin utility commands

Synopsis `help [command_name]`

command_name `[—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 specified XML file
backup-domain	performs a backup on the domain
change-admin-password	changes the administrator password
change-master-password	changes the master password
configure-webservice-management	sets the monitoring or maxhistory or attributes of a deployed webservice
create-admin-object	adds the administered object with the specified JNDI name
create-audit-module	creates an audit module for the optional plugin module
create-auth-realm	adds the named authorized realm
create-connector-connection-pool	adds a a new connector 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 named connector connection pool
create-custom-resource	registers the custom resource
create-domain	creates a domain with the specified name
create-file-user	creates a new file user
create-http-listener	adds a new HTTP listener socket
create-iiop-listener	adds the IIOP listener
create-javamail-resource	registers the Javamail resource
create-jdbc-connection-pool	registers the JDBC connection pool
create-jdbc-resource	registers the JDBC resource

create-jms-resource	registers the JMS resource
create-jmsdest	adds the named destination
create-jndi-resource	registers the JNDI resource
create-jvm-options	creates the JVM options from the Java configuration or profiler elements
create-lifecycle-module	adds a lifecycle module
create-management-rule	creates a new management rule
create-mbean	creates and registers a custom MBean
create-message-security-provider	enables administrators to create the `message-security-config` and `provider-config` sub-elements for the security service in `domain.xml`
create-password-alias	creates a password alias
create-persistence-resource	registers the persistence resource
create-profiler	creates the profiler element
create-resource-adapter-config	creates the resource adapter Java bean
create-service	configures the starting of a DAS or node agent on an unattended boot
create-ssl	creates the SSL element in the HTTP listener or IIOP listener
create-threadpool	creates the thread pool
create-transformation-rule	creates transformation rule for a deployed web service
create-virtual-server	adds the named virtual server
delete-admin-object	removes the administered object with the specified JNDI name
delete-audit-module	deletes the audit-module for the optional plugin module
delete-auth-realm	removes the named authorized realm
delete-connector-connection-pool	removes the specified connection pool
delete-connector-resource	removes the named resource connector
delete-connector-security-map	deletes the named security map
delete-custom-resource	removes the custom resource

delete-domain	deletes the given domain
delete-file-user	removes the named file user
delete-http-listener	removes the HTTP listener
delete-iiop-listener	removes the IIOP listener
delete-javamail-resource	removes the Javamail resource
delete-jdbc-connection-pool	removes the JDBC connection pool
delete-jdbc-resource	removes the JDBC resource
delete-jms-resource	removes the JMS resource
delete-jmsdest	destroys the named destination
delete-jndi-resource	removes the JNDI resource
delete-jvm-options	deletes the JVM options from the Java configuration or profiler elements
delete-lifecycle-module	removes the lifecycle module
delete-management-rule	deletes a specified management rule
delete-mbean	deletes a custom MBean
delete-message-security-provider	enables administrators to delete a `provider-config` sub-element for the given message layer (`message-security-config` element of `domain.xml`)
delete-password-alias	deletes a password alias
delete-persistence-resource	removes the persistence resource
delete-profiler	deletes the profiler element
delete-resource-adapter-config	deletes the resource adapter Java bean
delete-ssl	deletes the ssl element from the HTTP listener or IIOP listener
delete-threadpool	deletes the thread pool
delete-transformation-rule	deletes the transformation rule of a given web service
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 specified directory, located in the domain application server
disable	stops the specified, deployed component
display-error-distribution	displays distribution of errors from instance server.log at module level
display-error-statistics	displays a summary list of severities and warnings
display-log-records	displays all the error messages for a given module at a given timestamp
enable	runs the specified, deployed component
export	marks a variable name for automatic export to the environment of subsequent commands in multimode
flush-jmsdest	purges the messages in a JMS destination
freeze-transaction-service	immobilizes the named transaction service
generate-diagnostic-report	generates reports that can help diagnose application server malfunctioning
generate-jvm-report	shows the threads, classes and memory for a given target instance
get-client-stubs	gets the stubs of the client
get	gets the values of the monitorable or configurable attributes
help	displays a list of all the commands available in the Command-line interface
jms-ping	checks to see if the JMS provider is running
list-admin-objects	lists all the administered objects
list-audit-modules	lists the audit modules
list-auth-realms	lists the authorized realms
list-backups	lists all backups
list-components	lists deployed components
list-connector-connection-pools	gets all the connection pools

list-connector-resources	gets all the connector resources
list-connector-security-maps	lists the security maps for the connector connection pool
list-custom-resources	gets all the custom resources
list-domains	lists the domains in the given domains directory
list-file-groups	lists the file groups
list-file-users	lists the file users
list-http-listeners	gets the HTTP listeners
list-iiop-listeners	gets the IIOP listeners
list-javamail-resources	gets all the Javamail resources
list-jdbc-connection-pools	registers the JDBC connection pool
list-jdbc-resources	lists all the JDBC resources
list-jms-resources	lists the JMS resources
list-jmsdest	gets all the named destinations
list-jndi-entries	gets all the named destinations ,browses and queries the JNDI tree
list-jndi-resources	gets all the JNDI resources
list-lifecycle-modules	gets the lifecycle modules
list-management-rules	lists the management rules created using the `create-management-rule` command
list-mbeans	lists the custom mbeans for a given target server instance
list-message-security-providers	enables administrators to list all security message providers (`provider-config` sub-elements) for the given message layer (`message-security-config` element of `domain.xml`)
list-password-aliases	lists all password aliases
list-persistence-resources	gets all the persistence resources
list-registry-locations	returns list of configured web service registry access points
list-resource-adapter-configs	lists the resource adapters configured in an instance

list-sub-components	lists EJBs or Servlets in a deployed module or in a module of a deployed application
list-threadpools	lists the thread pools
list-timers	lists all of the timers owned by server instance(s)
list-transformation-rules	lists all the transformation rules of a given webservice
list-virtual-servers	gets the virtual servers
list	lists the configurable elements and provides the fully qualified dotted names of the management components that have read-only or modifiable attributes
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
publish-to-registry	publishes all the web service artifacts to registries
recover-transactions	manually recovers pending transactions
restore-domain	restores files from backup
rollback-transaction	rolls back the named transaction
set	sets the values of attributes. Set command can be used to modify default properties of a resource.
show-component-status	displays the status of the deployed component
start-appserv	starts the domains in the specified domains directory
start-callflow-monitoring	provides the complete callflow/path of a request
start-database	starts the bundled Java DB database
start-domain	starts the given domain
stop-appserv	stops the domains in the specified domains directory

stop-callflow-monitoring	disables collection of callflow information of a request
stop-database	stops the bundled Java DB database
stop-domain	stops the given domain
undeploy	removes a component in the domain application server
unfreeze-transaction-service	mobilizes the named transaction service
unpublish-from-registry	unpublishes the web service artifacts from the registries
unset	removes one or more variables from the multimode environment
update-connector-security-map	creates or modifies a security map for the specified connector connection pool
update-file-user	updates a current file user as specified
update-password-alias	updates a password alias
verify-domain-xml	verifies the content of the `domain.xml`
version	displays the version information

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

The install-license command 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 if the JMS service is up and running

Synopsis

jms-ping [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*]
[—port *4848|4849*] [—secure|–s] [—user *admin_user*] [—passwordfile *filename*]
[—help] [*target*]

Description

The `jms-ping` command checks 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 displays an error message when it is unable to ping a built-in JMS service.

This command is supported in remote mode only.

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.

`–H —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help Displays the help text for the command.

Operands

target 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. This 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

This operand is available only in the Sun Java System Application Server Standard and Enterprise Editions.

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
```

EXAMPLE 1 Using the jms-ping command *(Continued)*

```
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 2.1 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 one of `-webinc` and `-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`.

`-help`
Print a summary of the syntax and options for this command.

`-v`
Enables verbose mode.

`-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 if `java.io.tmpdir` is not defined.

`-l`
Outputs the name of the JSP page upon failure.

`-s`
Outputs the name of the JSP page upon success.

`-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 JSP compiled first. Subsequent JSPs are unaffected. This option is useful only with the *files* file specifier.

`-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.

`-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`

Compiles the generated servlets.

`-genclass`

Identical to the `-compile` option.

`-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.

`-ieplugin` *class_id*

Specifies the Java plugin COM class ID for Internet Explorer. Used by the `jsp:plugin` tags.

`-classpath` *path*

Override the system classpath with the specified classpath.

`-xpoweredBy`

Adds an `X-Powered-By` HTTP response header.

`-trimSpaces`

Trim spaces in template text between actions and directives.

`-smap`

Generates SMAP information for JSR45 debugging.

`-dumpsmap`

Dumps SMAP information for JSR45 debugging into a file.

`-validate`

Validates `.tld` and `web.xml` files against their schemas and DTDs.

`-compilerSourceVM<release>`

Provides source compatibility with the specified JDK release (in the same way as the javac command-line switch `-source`. This option is provided for backward compatibility with older JDK releases. For example, if a JSP page declares the scriptlet variable `<% java.util.Enumeration enum; %>`. The value for release must be 1.3, 1.4, 1.5 or 5. This is in order for the generated servlet to compile successfully, because `enum` has been a reserved keyword since JDK 1.5.

`-compilerTargetVM<release>`

Generates class files for the specified VM version. This option works the same way as javac command-line switch `-target`. The value for release must be one of the following: 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 5, or 6.

Examples

EXAMPLE 1 Using jspc to compile the JSPs in a Web application

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

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

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

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

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

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

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

See Also

asadmin(1M)

Name list – lists the configurable elements

Synopsis **list** [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*]
[—port *4848|4849*] [—secure|—s] [—user *admin_user*] [—passwordfile *filename*]
[—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.diagnostic-service ■ 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.diagnostic-service ■ 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-lister` 2. `default-config.http-service.http-listener.http-lister` 3. `server-config.http-service.http-listener.admin-lister` 4. `server-config.http-service.http-listener.http-listene` 5. `server-config.http-service.http-listener.http-listene` 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`

ID	Command	Output/Comment
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-monitoring-le 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.

ID	Command	Output/Comment
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.
3	`get server.monitoring-service.module-monitoring-levels.*`	server.monitoring-service.module-monitoring-levels.connector-con = OFF server.monitoring-service.module-monitoring-levels.connector-ser = 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-connecti = 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-se = 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

`–t —terse` Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`—p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`—s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`—u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—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
```

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

```
server.jms-service.jms-host.default_JMS_host
server.log-service
server.log-service.module-log-levels
server.mdb-container
server.monitoring-service
server.monitoring-service.module-monitoring-levels
server.resource-ref.jdbc/PointBase
server.resource-ref.jdbc/__TimerPool
server.resources
server.resources.jdbc-connection-pool.PointBasePool
server.resources.jdbc-connection-pool.__TimerPool
server.resources.jdbc-resource.jdbc/PointBase
server.resources.jdbc-resource.jdbc/__TimerPool
server.security-service
server.security-service.audit-module.default
server.security-service.auth-realm.certificate
server.security-service.auth-realm.file
server.security-service.jacc-provider.default
server.thread-pools
server.thread-pools.thread-pool.thread-pool-1
server.transaction-service
server.virtual-server.__asadmin
server.virtual-server.server
server.web-container
```

EXAMPLE 2 Using `list` for an application

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

EXAMPLE 3 Using `list` for a web module

```
asadmin> list --user admin --passwordfile password.txt
--host localhost --port 4848 server.applications.web-module
server.applications.web-module.adminapp
server.applications.web-module.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 listed ACLs.

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

```
list-admin-objects [—terse=false] [—echo=false] [—interactive=true]
      [—host localhost] [—port 4848|4849] [—secure|—s] [—user admin_user]
      [—passwordfile filename] [—help] [target]
```

Description This command lists all the administered objects. This command is supported in remote mode only.

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.

`–H —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

Operands *target*

This is the name of the targets for which the administered objects are to be listed. The valid targets for this command are instance, cluster, domain, and'server. Server is the default option. This option is available only in the Sun Java System Application Server Standard and Enterprise Edition. Valid values are:

- `server`, which lists the administered objects for the default server instance `server` and is the default value
- *configuration_name*, which lists the administered objects for the specified configuration
- *cluster_name*, which lists the administered objects for the specified cluster
- *instance_name*, which lists the administered objects for a particular server instance

Examples **EXAMPLE 1** Using the list-admin-objects command

```
asadmin> list-admin-objects --user admin --passwordfile passwords.txt
jms/samplequeue
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-audit-modules – gets all audit modules and displays them

Synopsis

```
list-audit-modules [—terse=false] [—echo=false] [—interactive=true]
          [—host localhost] [—port 4848|4849] [—secure|—s] [—user admin_user]
          [—passwordfile filename] [—help] [target]
```

Description Lists all the audit modules. This command is supported in remote mode only.

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.

`–H —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

Operands

target Specifies the target on which you are listing the audit modules.This option is available only in the Sun Java System Application Server Standard and Enterprise Edition. 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 the list-audit-modules command

```
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** [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*]
[—port *4848*|*4849*] [—secure|–s] [—user *admin_user*] [—passwordfile *filename*]
[—help] [*target_name*]

Description Lists the authentication realms. This command is supported in remote mode only.

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.

–H —host

The machine name where the domain administration server is running. The default value is localhost.

–p —port

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

–s —secure

If set to true, uses SSL/TLS to communicate with the domain administration server.

–u —user

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

—passwordfile

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—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 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

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.

`–v —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.zi
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-components – lists deployed components

Synopsis **`list-components`** [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*] [—port *4848*|*4849*] [—secure|—s] [—user *admin_user*] [—passwordfile *filename*] [—help] [—type *application*|*ejb*|*web*|*connector*|*webservice*] [target]

Description The command `list-components` lists all deployed Java EE 5 components. If the —`type` option is not specified, all components are listed. The available type values are: `application` (default), `ejb`, `web`, `connector` and `webservice`. This command is supported in remote mode only.

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.

`—H —host` The machine name where the domain administration server is running. The default value is localhost.

`—p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`—s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`—u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The —`passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin` login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help
Displays the help text for the command.

—type
This is 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-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 [—terse=false] [—echo=false] [—interactive=true]
      [—host localhost] [—port 4848|4849] [—secure|—s] [—user admin_user]
      [—passwordfile filename] [—help]
```

Description Use this command to list connector connection pools that have been created.

Operands

target	This operand is deprecated.

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` [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*] [—port *4848*|*4849*] [—secure|—s] [—user *admin_user*] [—passwordfile *filename*] [—help] [*target*]

Description This command lists all connector resources.

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.

–H —host

The machine name where the domain administration server is running. The default value is localhost.

–p —port

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

–s —secure

If set to true, uses SSL/TLS to communicate with the domain administration server.

–u —user

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

—passwordfile

The —`passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

Operands

target This operand specifies which configured resources you can list. Valid values are:

- `server`, which lists the connector resources in the current domain. This is the default target.
- `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. This operand is available only in the Sun Java System Application Server Standard and Enterprise Editions.

Examples

EXAMPLE 1 Using the list-connector-resources command

```
asadmin> list-connector-resources --user admin
--passwordfile passwords.txt --host localhost --port 5001
jms/qConnFactory
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 [—terse=false] [—echo=false] [—interactive=true]
        [—host localhost] [—port 4848|4849] [—secure|—s] [—user admin_user]
        [—passwordfile filename] [—help] [ —securitymap security_map_name ]
        [—verbose=false] 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

`—t —terse` Indicates that any 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 —host` The machine name where the domain administration server is running. The default value is localhost.

`—p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`—s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`—u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

`—verbose` Returns a list including the identity, principals, and security name.

`—securitymap` 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.
```

EXAMPLE 1 Using `list-connector-security-maps` with the security map option *(Continued)*

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-Pool1
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** [—terse=*false*] [—echo=*false*] [—interactive=*true*]
[—host *localhost*] [—port *4848*|*4849*] [—secure|—s] [—user *admin_user*]
[—passwordfile *filename*] [—help] [*target*]

Description Use this command to list custom resources. This command is supported in remote mode only.

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.

–H —host
The machine name where the domain administration server is running. The default value is localhost.

–p —port
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

–s —secure
If set to true, uses SSL/TLS to communicate with the domain administration server.

–u —user
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

—passwordfile
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help
: Displays the help text for the command.

Operands

target
: This operand specifies the location of the custom resources. This operand is available only in the Sun Java System Application Server Standard and Enterprise Editions. Valid targets are:

- server, which lists the resources on the default server instance. This is the default value
- domain, which lists the resources in the domain
- *cluster_name*, which lists the resources for every server instance in the cluster
- *instance_name*, which lists the resources for a particular server instance

Examples

EXAMPLE 1 Using the list-custom-resources command

The following example displays the usage of this command in Sun Java System Application Server Platform Edition.

```
asadmin> list-custom-resources --user admin --passwordfile
passwords.txt --host plum --port 4848
sample_custom_resource01
sample_custom_resource02
Command list-custom-resources executed successfully.
```

EXAMPLE 2 Using the list-custom-resources command

The following example displays the usage of this command in Sun Java System Application Server Standard and Enterprise Editions.

```
asadmin> list-custom-resources --user admin --passwordfile
passwords.txt --host plum --port 4849 target6
sample_custom_resource03
sample_custom_resource04
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]
      [—interactive=true]
```

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.

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

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 [—terse=false] [—echo=false] [—interactive=true] [—host localhost]
      [—port 4848|4849] [—secure|—s] [—user admin_user] [—passwordfile filename]
      [—help] [—name username] [--authrealmname auth_realm_name] [ target]
```

Description Use this command to administer file users and groups supported 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

`—t —terse` Indicates that any 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 —host` The machine name where the domain administration server is running. The default value is localhost.

`—p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`—s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`—u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

`-–name`
Identifies the name of the file user for whom the groups will be be listed.

Operands

target
This operand specifies which configurations you can list. Valid targets are:

- `server`, which lists the file groups in the current server. This is the default value.
- *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 --passwordfile passwords.txt
staff
manager
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 – lists the file users

Synopsis **`list-file-users`** `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`] [—host` *localhost*`] [—port` *4848|4849*`] [—secure|—s] [—user` *admin_user*`] [—passwordfile` *filename*`] [—help] [`*target*`]`

Description The `list-file-users` command creates a list of file users supported by file realm authentication.

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.

`—H —host`
The machine name where the domain administration server is running. The default value is localhost.

`—p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`—s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`—u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

Operands

target Specifies the target on which you are creating the file user. This option is available only in the Sun Java System Application Server Standard and Enterprise Edition. Valid targets are:

- `server`, which lists the file users in the default server instance. This is the default value.
- *cluster_name*, which lists the file users on every server instance in the cluster.
- *instance_name*, which lists the file users on a particular sever instance.

Examples

EXAMPLE 1 Using the list-file-users command

```
asadmin> list-file-users instance1 --user admin1 --passwordfile passwords.txt
sample_user05
sample_user08
sample_user12
Command list-file-users executed successfully
```

Exit Status

0 command executed successfully

1 error in executing the command

See Also

`create-file-user(1)`, `delete-file-user(1)`, `update-file-user(1)`, `list-file-groups(1)`

Name list-http-listeners – lists the existing HTTP listeners

Synopsis **`list-http-listeners`** [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*] [—port *4848|4849*] [—secure|—s] [—user *admin_user*] [—passwordfile *filename*] [—help] [*target*]

Description The `list-http-listeners` command lists the existing HTTP listeners. This command is supported in remote mode only.

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.

`—H —host` The machine name where the domain administration server is running. The default value is localhost.

`—p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`—s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`—u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help
Displays the help text for the command.

Operands

target
This option is available only in the Sun Java System Application Server Standard and 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 host1 --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`** `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host` *localhost*`] [—port` *4848|4849*`] [—secure|–s] [—user` *admin_user*`]`
`[—passwordfile` *filename*`] [—help] [`*target*`]`

Description The `list-iiop-listeners` command lists the existing IIOP listeners. This command is supported in remote mode only.

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.

`–H —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

Operands *target* This option is available only in the Sun Java System Application Server Standard and 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 host1 --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 server instances while indicating if they are running or not.

Synopsis

`list-instances` `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`] [—host` *localhost*`] [—port` *4848|4849*`] [—secure|–s] [—user` *admin_user*`] [—passwordfile` *filename*`] [—help] [`*target*`]`

Description

Use the `list-instances` to list all the instances in a 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

`–t —terse`

Indicates that any 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 —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

Operands

target This is the name of the target domain associated with the instances you want listed. Valid values are:

- `domain`, which lists all server instances in the domain. This is the default value.
- *cluster_name*, which lists all server instances in the specified cluster
- *instance_name*, which lists the specified server instance
- *node_agent_name*, which lists all server instances in the named node-agent.

Examples

EXAMPLE 1 Using list-instances in local mode

```
asadmin> list-instances --user admin --passwordfile passwords.txt instance1
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)`

Name

list-javamail-resources – lists the existing JavaMail session resources

Synopsis

`list-javamail-resources` `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host` *localhost*`] [—port` *4848|4849*`] [—secure|–s] [—user` *admin_user*`]`
`[—passwordfile` *filename*`] [—help] [`*target*`]`

Description

The command lists the existing JavaMail session resources. This command is supported in remote mode only.

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.

`–H —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help

Displays the help text for the command.

Operands

target

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. This 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 This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

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` `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host` *localhost*`] [—port` *4848|4849*`] [—secure|–s] [—user` *admin_user*`]`
`[—passwordfile` *filename*`] [—help]`

Description

Use this command to get the JDBC connection pools that have been created. This command is supported in the remote mode only.

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.

`–H —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—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 --passwordfile passwords.txt
--host localhost --port 7070
sample_derby_pool
Command list-jdbc-connection-pools executed successfully.
```

Where: sample_derby_pool is the JDBC connection pool.

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` [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*] [—port *4848|4849*] [—secure|–s] [—user *admin_user*] [—passwordfile *filename*] [—help] [*target*]

Description The `list-jdbc-resources` command displays a list of JDBC resources that have been created. This command is supported in remote mode only.

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.

`–H —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

Operands

target This operand specifies which JDBC resources you can list. Usage of this operand is optional. 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.

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

Examples

EXAMPLE 1 Using the list-jdbc-resources command

```
asadmin> list-jdbc-resources --user admin --passwordfile passwords.txt jdbc/DerbyPool
Command list-jdbc-resources 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 [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*]
[—port *4848*|*4849*] [—secure|–s] [—user *admin_user*] [—passwordfile *filename*]
[—help] [--desttype *type*] [*target*]

Description

The list-jmsdest command lists the JMS physical destinations. This command is supported in remote mode only.

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.

–H —host

The machine name where the domain administration server is running. The default value is localhost.

–p —port

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, http://localhost:4848.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

–s —secure

If set to true, uses SSL/TLS to communicate with the domain administration server.

–u —user

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the --user option on subsequent operations to this particular domain.

—passwordfile

The —passwordfile option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

—`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* 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

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

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

The following command lists all the physical destinations for the default server instance:

EXAMPLE 1 Using the list-jmsdest command *(Continued)*

```
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-resources – lists the JMS resources

Synopsis

```
list-jms-resources [—terse=false] [—echo=false] [—interactive=true]
      [—host localhost] [—port 4848|4849] [—secure|—s] [—user admin_user]
      [—passwordfile filename] [—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

`–t —terse` Indicates that any 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 —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

—`restype` The JMS resource type can be `javax.jms.Topic`, `javax.jms.Queue`, `javax.jms.TopicConnectionFactory`, or `javax.jms.QueueConnectionFactory`.

Operands

target 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. This 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.

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

Examples

EXAMPLE 1 Using the list-jms-resources command to list all JMS resources

```
asadmin> list-jms-resources --user admin1
--passwordfile passwords.txt
jms/Queue
jms/Topic
jms/QueueConnectionFactory
jms/DurableTopicConnectionFactory
```

EXAMPLE 1 Using the list-jms-resources command to list all JMS resources *(Continued)*

```
Command list-jms-resources executed successfully.
```

EXAMPLE 2 Using the list-jms-resources command to list JMS resources of a specified type

```
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 [—terse=*false*] [—echo=*false*] [—interactive=*true*]
[—host *localhost*] [—port *4848*|*4849*] [—secure|–s] [—user *admin_user*]
[—passwordfile *filename*] [—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

`–t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The —`passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

—`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 This operand specifies which configurations you can list. Valid values are domain, instance, cluster, or server. The default is server.

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

Examples

EXAMPLE 1 Using the list-jndi-entries command

```
asadmin>list-jndi-entries --user admin1 --passwordfile /password
--context jdbc server
Jndi Entries for server within jdbc context:
__TimerPool: javax.naming.Reference
__TimerPool__pm: javax.naming.Reference
Command list-jndi-resources executed successfully
```

Exit Status

0 command executed successfully

1 error in executing the command

See Also

`create-jndi-resource(1)`, `delete-jndi-resource(1)`

Name

list-jndi-resources – lists all existing JNDI resources

Synopsis

`list-jndi-resources` `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host `*localhost*`] [—port `*4848|4849*`] [—secure|–s] [—user `*admin_user*`]`
`[—passwordfile `*filename*`] [—help] [`*target*`]`

Description

Use the `list-jndi-resources` command to identify all the existing JNDI resources. This command is supported in remote mode only.

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.

`–H —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

Operands

target This operand specifies which jndi resources you can list. Valid values are:

- `server`, which lists the resources on the default server instance. This is the default value
- `domain`, which lists the resources in the domain
- *cluster_name*, which lists the resources for every server instance in the cluster
- *instance_name*, which lists the resources 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 the list-jndi-resources command

The following is an example for using the `list-jndi-resources` command in the Platform Edition.

```
asadmin> list-jndi-resources --user admin --passwordfile passwords.txt
--host plum
jndi_resource1
jndi_resource2
jndi_resource3
Command list-jndi-resources executed successfully
```

EXAMPLE 1 Using the list-jndi-resources command *(Continued)*

The following is an example for using the `list-jndi-resources` command in the Enterprise Edition.

```
asadmin> list-jndi-resources --user admin --passwordfile
passwords.txt --host plum --port 4849 instance1
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** [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*] [—port *4848*|*4849*] [—secure|-s] [—user *admin_user*] [—passwordfile *filename*] [—help] [*target*]

Description The `list-lifecycle-modules` command lists the lifecycle modules. The lifecycle modules provide a means of running short or long duration Java-based tasks within the application server environment. This command is supported in remote mode only.

Options

–t —terse

Indicates that any 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 —host

The machine name where the domain administration server is running. The default value is localhost.

–p —port

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

–s —secure

If set to true, uses SSL/TLS to communicate with the domain administration server.

–u —user

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

—passwordfile

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

Operands

target This option indicates the location where the lifecycle module exists. The valid targets for this command are configuration, instance, cluster, or server.

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

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-management-rules – lists the available management rules

Synopsis **`list-management-rules`** [—terse=*false*] [—echo=*false*] [—interactive=*true*]
[—host *localhost*] [—port *4848*|*4849*] [—secure|–s] [—user *admin_user*]
[—passwordfile *filename*] [—help] [*target*]

Description The `list-management-rules` lists the management rules created using the `create-management-rule` command.

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.

`–H —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

Operands

target This is the name of the target upon which the command is operating. The valid targets for this command are server, cluster, config, and instance. Server is the default option.

Examples

EXAMPLE 1 using list-management-rules

```
asadmin> list-management-rules --user admin
--passwordfile adminpassword.txt
myRule1
Command list-management-rules executed successfully
```

Exit Status

0 command executed successfully

1 error in executing the command

See Also

`create-management-rule`(1), `delete-management-rule`(1)

Name

list-mbeans – lists the custom mbeans for a given target server instance.

Synopsis

`list-mbeans` `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`] [—host` *localhost*`]`
`[—port` *4848|4849*`] [—secure|–s] [—user` *admin_user*`] [—passwordfile` *filename*`]`
`[—help] target=`*server*

Description

Lists the custom mbeans for the specified target. `list-mbeans` provides the following information :

- `ClassName` of the MBean
- *name* of the MBean (if specified while creating the MBean)
- `ObjectName` of the MBean
- `ObjectType` of the MBean
- Boolean indicating whether the MBean is enabled

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.

`–t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry

for the password must have the AS_ADMIN_ prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help

Displays the help text for the command.

Operands

target=*server*

The target for the MBean. Identifies the server instance. Defaults to the name of the Domain Adminstration Server (DAS).

Examples

EXAMPLE 1 Using list-mbeans

```
asadmin>list-mbeans target=server1
Where: server1 is an application server instance.
```

Exit Status

0

command executed successfully

1

error in executing the command

See Also

create-mbean(1)

delete-mbean(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`** `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host` *localhost*`] [—port` *4848|4849*`] [—secure|–s] [—user` *admin_user*`]`
`[—passwordfile` *filename*`] [—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.

`–t —terse` Indicates that any 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 —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

—`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.

EXAMPLE 1 Using list-message-security-providers *(Continued)*

```
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-password-aliases – lists all password aliases

Synopsis

```
list-password-aliases [—terse=false] [—echo=false] [—interactive=true]
     [—host localhost] [—port 4848|4849] [—secure|-s] [—user admin_user]
     [—passwordfile filename] [—help]
```

Description This command lists all of the password aliases.

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.

`–H —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—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`** [`—terse=`*false*] [`—echo=`*false*] [`—interactive=`*true*] [`—host` *localhost*] [`—port` *4848|4849*] [`—secure|—s`] [`—user` *admin_user*] [`—passwordfile` *filename*] [`—help`] *[target]*

Description The `list-persistence-resources` command displays all the persistence resources. This command is supported in remote mode only.

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.

`—H —host` The machine name where the domain administration server is running. The default value is localhost.

`—p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`—s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`—u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

—`help`

Displays the help text for the command.

Operands

target

Specifies the target for which you are listing all persistence resources. Usage of this operand is optional. Valid targets are:

- `server`, which lists the persistence resources deployed in the default server instance. This is the default target.
- `domain`, which lists the persistence resources deployed in the domain.
- *cluster_name*, which lists the persistence resources deployed in every server instance in the cluster.
- *instance_name*, which lists the persistence resources deployed in a particular sever instance.

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

Examples

EXAMPLE 1 Using list-persistence-resources

This example lists all the persistence resources.

```
asadmin> list-persistence-resources --user admin
--passwordfile passwords.txt
sample_persistence_resource
testPersistence
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-registry-locations – returns list of configured web service registry access points.

Synopsis **`list-registry-locations`**

Description Returns list of configured web service registry access points. This list contains the eis/SOAR and eis/uddi, which can be used as input to the publish-to-registry and unpublish-from-registry commands.

Examples **EXAMPLE 1** To list registry locations

```
asadmin>list-registry-locations
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also `publish-to-registry(1)`, `unpublish-from-registry(1)`

Name list-resource-adapter-configs – lists the names of the resource—adapter—configs created.

Synopsis

```
list-resource-adapter-configs [—terse=false] [—echo=false] [—interactive=true]
      [—host localhost] [—port 4848|4849] [—secure|—s] [—user admin_user]
      [—passwordfile filename] [—help] [—verbose=false]
      [—raname connectorModuleName]
```

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` file.

This command is supported in remote mode only.

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.

`–H —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The —`passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help
Displays the help text for the command.

—verbose
This option helps to list the properties that are configured.

—raname
This option lists 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 deprecated.

Examples

EXAMPLE 1 Using the list-resource-adapter-configs command

```
asadmin> list-resource-adapter-configs --user admin1
--passwordfile passwords.txt
ra1
ra2
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-sub-components – lists EJBs or Servlets in deployed module or module of deployed application

Synopsis **`list-sub-components`** `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`] [—host` *localhost*`] [—port` *4848|4849*`] [—secure|–s] [—user` *admin_user*`] [—passwordfile` *filename*`] [—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

`–t —terse` Indicates that any 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 —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

—`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` Identifies 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 [—terse=false] [—echo=false] [—interactive=true]
      [—host localhost] [—port 4848|4849] [—secure|—s] [—user admin_user]
      [—passwordfile filename] [—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 overridden through a system property of the corresponding name. This command lists the system properties of a domain, configuration, cluster, or server instance.

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.

`–H —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

Operands

target
This option 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 defined for the named server instance as well as those the server inherits from its cluster (if the instance is clustered), its configuration, and the domain.

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

Examples

EXAMPLE 1 Using list-system-properties

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

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** [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*]
[—port *4848*|*4849*] [—secure|–s] [—user *admin_user*] [—passwordfile *filename*]
[—help] [target]

Description Lists all the thread pools. This command is supported in remote mode only.

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.

–H —host
The machine name where the domain administration server is running. The default value is localhost.

–p —port
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

–s —secure
If set to true, uses SSL/TLS to communicate with the domain administration server.

–u —user
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

—passwordfile
The —`passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

—`help`

Displays the help text for the command.

Operands

target

This option specifies the target being operated on. Valid values are:

- `server`, which lists the threadpool for the default server instance `server` and is the default value
- *configuration_name*, which lists the threadpool for the named configuration
- *cluster_name*, which lists the threadpool for every server instance in the cluster
- *instance_name*, which lists the threadpool 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 [—terse=false] [—echo=false] [—interactive=true] [—host localhost]
      [—port 4848|4849] [—secure|–s] [—user admin_user] [—passwordfile filename]
      [—help] target
```

Description

The `list-timers` 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

`–t —terse`

Indicates that any 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 —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—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 server1
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-transformation-rules – lists all the transformation rules of a given webservice. If the webservice name option is omitted, then all the transformation rules will be listed.

Synopsis

list-transformation-rules [webservicename *webservice_name*]

Description

Lists all the transformation rules of a given webservice in the order they are applied. If the webservice name option is omitted, then all the transformation rules will be listed.

Options

`--webservicename`	name of the deployed webservice.

Examples

EXAMPLE 1 To delete a transformation rule that is applied to a webservice

```
list-transformation-rules --webservicename jaxrpc-simple#jaxrpc-simple.war#HelloIF
Command list-transformation-rules executed successfully
```

where,`jaxrpc-simple#jaxrpc-simple.war#HelloIF` is the fully qualified name of a webservice endpoint.

Exit Status

0	command executed successfully
1	error in executing the command

See Also

`create-transformation-rule(1)`, `delete-transformation-rule(1)`

Name

list-virtual-servers – lists the existing virtual servers

Synopsis

`list-virtual-servers` `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host `*localhost*`] [—port `*4848|4849*`] [—secure|–s] [—user `*admin_user*`]`
`[—passwordfile `*filename*`] [—help] [`*target*`]`

Description

The `list-virtual-servers` command lists the existing virtual servers. This command is supported in remote mode only.

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.

`–H —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help
: Displays the help text for the command.

Operands

target
: 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 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

This option is available only in the Sun Java System Application Server Standard and Enterprise Edition.

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 login – lets you log in to a domain

Synopsis **login** [—terse=*false*] [—echo=*false*] [—host *host_name*] [—port *port_number*] [—secure|–s] [—help]

Description Lets you log in to a domain.

If various application server domains are created on various machines (locally), `asadmin` invocation from any of these machines can manage the domains located elsewhere (remotely). This comes in handy especially when a particular machine is chosen as an administration client and it manages multiple domains and servers. `asadmin` commands that are used to manage domains located elsewhere are called remote commands. The `asadmin login` command eases the administration of such remote domains.

This command runs only in the interactive mode. It prompts you for the admin user name and password. On successful login. the file `.asadminpass` will be created in user's home directory. This is the same file that is modified during the `create-domain` command while using the `—savelogin` option. The domain must be running for this command to run.

The host name is stored as-is and there will be no resolution attempted with the DNS. It is enough for a user to login to a particular domain which is fully qualified by [admin-host, admin-port] pair once. Thus, if a domain is being administered from various machines, it is sufficient to invoke `asadmin login` once.

After logging into a domain with the `asadmin login` command, you need not specify the `—user` and `—passwordfile` option when you run subsequently run remote commands on that domain.

Successive successful invocations of the same command with same parameters result in overwriting the contents of `.asadminpass` file for the given admin host and port. The user can decide to overwrite the file or reject such a login.

Once you have logged in to a domain, you will still need to provide the host and port for the subsequent remote commands unless you have chosen the default values for `—host` and `—port` options.The advantage of this command is apparent especially if you choose the default host (localhost) and default admin port (4848).

If you do not use the login command, and you choose not to get prompted for admin user and admin password, you would invoke `asadmin` commands in succession like this:

asadmin>**`create-jdbc-connection-pool ——user admin ——passwordfile passwordfile.txt <other options> samplePool1`**

asadmin>**`deploy ——user admin ——passwordfile passwordfile.txt <other options> /home/myapplication.ear`**

asadmin>**`list-components ——user admin ——passwordfile passwordfile.txt <other options>`**

If you now log in, you can run remote commands like this:

asadmin>**create-jdbc-connection-pool <other options> samplePool1**

asadmin>**deploy <other options> /home/myapplication.ear**

asadmin>**list-components <other options>**

Login information is saved permanently and this information can be used across multiple domain restarts.

There is no `logout` command. If you want to login to another domain, invoke `asadmin login` with new values for —`host` and —`port`.

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 —host`
The machine name where the domain administration server is running. The default value is lcoalhost. If you login to localhost, you need not specify host or port options for subsequent remote commands.

`–p —port`
The port number of the domain administration server listening for administration requests. The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

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

Examples

EXAMPLE 1 Using the login command

The following command logs into a domain located on another machine:

```
asadmin> login --host foo --port 8282
Please enter the admin user name>admin
Please enter the admin password>

Trying to authenticate for administration of server at host [foo]
and port [8282] ...
Login information relevant to admin user name [admin] for host [foo]
and admin port [8282] stored at [/.asadminpass] successfully.
Make sure that this file remains protected. Information stored in this
file will be used by asadmin commands to manage associated domain.
```

EXAMPLE 2 Using the login command

The following command logs into a domain on local host on default port.

```
asadmin> login --host myhost
Please enter the admin user name>admin
Please enter the admin password>
Trying to authenticate for administration of server at host [myhost] and port [4848] ...
An entry for login exists for host [myhost] and port [4848], probably
from an earlier login operation.
Do you want to overwrite this entry (y/n)?y
Login information relevant to admin user name [admin] for host [myhost]
and admin port [4848] stored at [/home/joe/.asadminpass] successfully.
Make sure that this file remains protected. Information stored in this
file will be used by asadmin commands to manage associated domain.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also

create-domain(1), delete-domain(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, which is created in the current working directory. 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 1.5 home directory
- set `AS_ACC_CONFIG` to *appclient_install_dir*`/config/sun-acc.xml`

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

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

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

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

To use the newly installed application client container, you must do the following:

- Obtain the application client stubs for your target application, for example, *yourClientStub.jar*.
- Execute the `appclient` utility: `appclient -`*client yourClientStub.jar*

Attributes

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Interface Stability	Unstable

See Also

appclient (1M)

Name ping-connection-pool – tests if a connection pool is usable

Synopsis

```
ping-connection-pool [—terse=false] [—echo=false] [—interactive=true]
      [—host localhost] [—port 4848|4849] [—secure|—s] [—user admin_user]
      [—passwordfile filename] [—help] pool_name
```

Description This command tests if 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 an application that is expected to be deployed later, the JDBC pool is tested with this command before deploying the application.

A JDBC connection pool or a connector connection pool 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

`–t —terse` Indicates that any 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 —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry

for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

—`target` This option is deprecated.

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

publist-to-registry – publishes all the web service artifacts to registries.

Synopsis

```
publish-to-registry
        —registryjndinames registrynames —webservicename qualified_webservice_name
        —organization organization_name —categories categories_list
        —descriptiondescription
```

Description

Publishes the web service artifacts to registries.

Options

`—registryjndinames`

JNDI names of the connector resource pointing to different registries. Use comma to separate the JNDI names. The JNDI names are created as a result of the following three commands:

1. Create a resource adapter that can talk to the registry (Use the jaxr resource adapter that can talk to the UDDI registry)
2. Create a connector connection pool to create a pool using the resource adapter
3. Create a connector resource using this connection pool. The jndiname of this connector resource is specified in the registryjndinames parameter

`—webservicename`

fully qualified web service, which is of the format: appName#moduleName#webserviceName

`—organization`

the "Organization" under which the particular webservice should be published. Typically in tegistries, documents are published for a particular organization. A user can go and search the organization and look at all the services that the organization offers.

`—categories`

categories under which this web service endpoint should be published. Use comma to separate each category.

`—description`

description of the web service endpoint.

Examples

EXAMPLE 1 To publish a WSDL to a registry

```
asadmin>publish-to-registry --registryjndiname eis/SOAR, eis/uddi --webservicename myAppname#myModu
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also

unpublish-from-registry(1), list-registry-locations(1)

Name recover-transactions – manually recovers pending transactions

Synopsis

```
recover-transactions [—terse=false] [—echo=false] [—interactive=true]
      [—host localhost] [—port 4848|4849] [—secure|–s] [—user admin_user]
      [—passwordfile filename] [—help]
      [—txlogdir transaction_log_directory —destination destination_server_name]
      server_name
```

Description The function of this command is to manually recover pending transactions. This is used in remote mode only.

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.

`–H —host` The machine name where the domain administration server is running. The default value is localhost.

`–p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

`—txlogdir` The transaction log directory of the server (provided in the *server_name* operand) for which the recovery needs to be done.

`—destination` The destination server which will perform the recovery for the server (provided in the *server_name* operand). The destination server should be running.

Operands

server_name This is the name of the server for which the recovery needs to be done. If this server is running, recovery will be performed by the same server. In this case the `—txlogdir` and `—destination` options should not be given. If the server is not running, then the `—txlogdir` and `—destination` options are required.

Examples

EXAMPLE 1 Using the recover-transactions

This is a basic example of how this command is used.

```
asadmin>recover-transactions serverid1
Transaction recovered.
```

Exit Status

0 command executed successfully

1 error in executing the command

See Also

none

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.

`–v —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 sjsas_
Successfully restored the domain (domain1), from /opt/SUNWappserver/nondefaultdomaindir/domain1/bac

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
```

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 [—terse=*false*] [—echo=*false*] [—interactive=*true*]
[—host *localhost*] [—port *4848*|*4849*] [—secure|—s] [—user *admin_user*]
[—passwordfile *filename*] [—help] [—target *target_name*] [*transaction_id*]

Description

Use the `rollback-transaction` command to roll back the named transaction. This command is supported in remote mode only.

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.

`—H —host`
The machine name where the domain administration server is running. The default value is localhost.

`—p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`—s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`—u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

—`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 command

```
asadmin> rollback-transaction --user admin --passwordfile password.txt --target server 000000000000
Command rollback-transaction executed succeessfully
```

Exit Status

0
command executed successfully

1
error in executing the command

See Also `freeze-transaction-service`(1), `list-transaction-id`(1), `unfreeze-transaction-service`(1)

Name

schemagen – creates a schema file for each namespace referenced in your Java classes

Synopsis

schemagen [*options*] [*java_source_files*]

Description

The schema generator can be launched using the appropriate schemagen shell script in the bin directory for your platform. For this Early Access release, we are only providing a basic shell script for evaluation purposes. Future releases will contain more robust schema generation tools.

The current schema generator processes Java source files only. Future versions of the tool may also be capable of processing compiled class files.

If your Java sources reference other classes, those sources must be accessible from your system CLASSPATH environment variable or errors will occur when the schema is generated.

The current schema generator simply creates a schema file for each namespace referenced in your Java classes. There is no way to control the name of the generated schema files at this time.

Options

-d *path*	Specifies the location of the processor- and javac—generated class files.
-cp *path*	Specifies the location of the user-specified files.
-classpath *path*	Specifies the location of the user-specified files.
-help	Displays detailed usage information.

Examples

EXAMPLE 1 Using schemagen to generate schema files on Solaris/Linux

```
% $JAXB_HOME/bin/schemagen.sh Foo.java Bar.java ...
      Note: Writing schema1.xsd
```

This example shows how to generate the schema files without specifying the location of the generated class files.

EXAMPLE 2 Using schemagen to generate schema files

```
schemagen File1.java File2.java
      Note: Writing schema1.xsd
```

This example shows how to generate the schema file without specifying the location of the generated class files.

EXAMPLE 3 Using schemagen to generate schema files and specify the location of the generated class files

```
schemagen.bat File1.java File2.java -d /usr/var/project1
      Note: Writing schema1.xsd
```

This example shows how to generate the schema file with a specified location for the generated class files.

See Also

xjc(1M)

Name set – sets the values of attributes

Synopsis

```
set [—terse=false] [—echo=false] [—interactive=true] [—host localhost]
        [—port 4848|4849] [—secure|—s] [—user admin_user] [—passwordfile filename]
        [—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.diagnostic-service 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.diagnostic-service 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-lister` 2. `default-config.http-service.http-listener.http-lister` 3. `server-config.http-service.http-listener.admin-lister` 4. `server-config.http-service.http-listener.http-listene` 5. `server-config.http-service.http-listener.http-listene` 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`

ID	Command	Output/Comment
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-monitoring-le 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.

ID	Command	Output/Comment
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.
3	`get` `server.monitoring-service.module-monitoring-levels.*`	server.monitoring-service.module-monitoring-levels.connector-co = OFF server.monitoring-service.module-monitoring-levels.connector-ser = 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-connecti = 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-se = 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

`–t —terse`

Indicates that any 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 —host`

The machine name where the domain administration server is running. The default value is localhost.

`–p —port`

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`

If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—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 [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*] [—port *4848|4849*] [—secure|–s] [—user *admin_user*] [—passwordfile *filename*] [—help] [—target *target (defaultserver)*] *component-name*

Description

The `show-component-status` command gets the status of the deployed component. 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

`–t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

`—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

The `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 for the instance.
`--password`	Password of the administrative user.
`--host`	Host name of the machine hosting the administrative instance.
`--port`	Port number associated with the administrative host.
`--passwordfile`	File containing passwords appropriate for the command (for example, 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 specified domains directory

Synopsis

start-appserv [—domaindir *install_dir*/domains] [—terse=*false*] [—echo=*false*] [—interactive=*true*]

Description

This command is deprecated. Use the start-domain command instead. Use the start-appserv command to start the domains in specified domain directory. If the domain directory is not specified the domains in the default *install_dir*/domains directory are started. The start-appserv command requires that the user has set up an AS_ADMIN_USER environment variable and that all domains have the same administration user. You are prompted for the master password for each domain (unless the —savemasterpassword option was specified at the domain creation time).

The start-appserv command functions correctly if every domain is created with —savemasterpassword. Remember that the user and password do not need to be passed to start-appserv in the Platform Edition. If —savemasterpassword is not specified, then you are prompted for the master password for every domain.

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 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.

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

Examples

EXAMPLE 1 Using the start—appserv command on Platform Edition

```
asadmin> start-appserv
Command start-appserv is deprecated.
Starting all the domains in /opt/SUNWappserver/domains, please wait.
Starting Domain domain1, please wait.
Log redirected to /opt/SUNWappserver/domains/domain1/logs/server.log.
Domain domain1 is ready to receive client requests. Additional services are being started in backgr
```

EXAMPLE 2 Using the start—appserv command on Enterprise Edition

```
asadmin> start-appserv --user admin
Command start-appserv is deprecated.
Starting all the domains in /opt/SUNWappserver90/domains, please wait.
Starting Domain domain1, please wait.
Log redirected to /opt/SUNWappserver90/domains/domain1/logs/server.log.
Please enter the admin password>
```

EXAMPLE 2 Using the start—appserv command on Enterprise Edition *(Continued)*

```
Domain domain1 started.
```

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)`, `stop-appserv(1)`

Name start-callflow-monitoring – provides the complete call flow/path of a request.

Synopsis **`start-callflow-monitoring`** `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host` *localhost*`] [—port` *4848|4849*`] [—secure|–s] [—user` *admin_user*`]`
`[—passwordfile` *filename*`] [—help] [—filtertype type=`*value*`[type=`*value*`]*]`
instance-name

Description Collects and correlates data from Web container, EJB container and JDBC to provide a complete call flow/path of a request. Data is collected only if `callflow-monitoring` is on.

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.

`–t —terse`
Indicates that any 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 —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help
Displays the help text for the command.

--filtertype
Takes the format type=value, where type can be *user* or *ip*.

Operands

instance-name
The name of the application server instance for which you want to enable call flow monitoring.

Examples

EXAMPLE 1 Using start-callflow-monitoring

```
asadmin start-callflow-monitoring --passwordfile passwordfile.txt --user admin --host localhos
Command start-callflow-monitoring executed successfully.
```

Exit Status

0
command executed successfully

1
error in executing the command

See Also

stop-callflow-monitoring(1)

Name start-database – starts the Java DB

Synopsis **`start-database`** `[—dbhost` *0.0.0.0*`] [—dbport` *1527*`] [—dbhome` *current_directory*`]`
`[—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 for use with the Application Server. 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.

Note – The database must be started by the user that installed the Java DB.

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 current working directory, the folder where you are running `asadmin start-database`. It is important to use the `dbhome` option when you want to create the database files at a particular location.

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. The default is the current working directory.

`—e —echo` Setting to true will echo the command line statement on the standard output. Default is false.

`—t —terse` Setting to false 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/bin/derby.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 sampleDomai
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 b
```

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 [—terse=false] [—echo=false] [—interactive=true] [—host localhost]
      [—port 4848|4849] [—secure|—s] [—user admin_user] [—passwordfile filename]
      [—help] instance_name
```

Description The `start-instance` command starts an instance with the instance name you specify.

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.

`–H —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—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 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-domain(1),.stop-domain(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 instead. Use the `stop-appserv` command to stop the domains in specified domain directory. If the domain directory is not specified the domains in the default *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
Command stop-appserv is deprecated.
Stopping all domains in /opt/SUNWappserver90/domains, please wait.
Domain domain1 stopped.
```

Where: `/opt/SUNWappserver90/domains/domain1` is the domain in the default domains directory that 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-callflow-monitoring – Disables collection of call flow information of a request.

Synopsis **`stop-callflow-monitoring`** `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host` *localhost*`] [—port` *4848|4849*`] [—secure|−s] [—user` *admin_user*`]`
`[—passwordfile` *filename*`] [—help]` *instance-name*

Description Disables collection of call flow information of a request.

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.

`−t —terse` Indicates that any 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 —host` The machine name where the domain administration server is running. The default value is localhost.

`−p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`−s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`−u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—help

Displays the help text for the command.

Operands

instance-name

The name of the application server instance for which you want to diable call flow monitoring.

Examples

EXAMPLE 1 Using stop-callflow-monitoring

```
asadmin stop-callflow-monitoring --passwordfile passwordfile.txt --user admin --host localhost --po
Command stop-callflow-monitoring executed successfully.
```

Exit Status

0

command executed successfully

1

error in executing the command

See Also

start-callflow-monitoring(1)

Name

stop-database – stops Java DB

Synopsis

stop-database [—dbhost *0.0.0.0*] [—dbport *1527*]

Description

The stop-database command stops a process of the Java DB server. Java DB server 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.

Note – The database must be stopped by the user that installed Java DB.

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
Connection obtained for host: host1, port number 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 current working directory from which you ran start-database.

0	command executed successfully
1	error in executing the command

See Also

start-database(1)

Name stop-domain – stops the Domain Administration Server of the specified domain

Synopsis **stop-domain** [—terse=*false*] [—echo=*false*] [—domaindir *install_dir*/domains] *domain_name*

Description Use the stop-domain command to stop the Domain Administration Server of the specified domain. The stop-domain command can be run in the local mode only.

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 to the standard output. Default is false.

—domaindir
: The directory where the domain is to be stopped. If specified, the path must be accessible in the filesystem. If not specified, the domain in the default *install_dir*/domains directory is stopped.

Operands

domain_name
: This is the name of the domain to stop.

Examples

EXAMPLE 1 Using stop-domain command

```
asadmin> stop-domain sampleDomain
Domain sampleDomain stopped
```

Exit Status

0
: command executed successfully

1
: error in executing the command

See Also start-domain(1), delete-domain(1), list-domains(1)

Name stop-instance – stops a server instance

Synopsis **`stop-instance`** `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`] [—host` *localhost*`] [—port` *4848|4849*`] [—secure|-s] [—user` *admin_user*`] [—passwordfile` *filename*`] [—help]` *instance_name*

Description Use the `stop-instance` command to stop the instance with the instance name specified. The `stop-instance` command can be run both locally and remotely. The named instance must already exist within the given domain; and the instance must be running.

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.

`-H —host` The machine name where the domain administration server is running. The default value is localhost.

`-p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`-s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`-u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

—`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 --user admin1 --passwordfile passwords.txt instance1
Command stop-instance executed successfully
```

EXAMPLE 2 Using `stop-instance` in remote mode

```
asadmin> stop-instance --user admin1 --password passwords.txt
--host pigeon --port 4849 instance2
Command stop-instance executed successfully
```

Where: the `instance2` is associated with user, password, host and port of 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)`, `restart-instance(1)`

Name undeploy – removes a deployed component

Synopsis

```
undeploy [—terse=false] [—echo=false] [—interactive=true] [—host localhost]
      [—port 4848|4849] [—secure|−s] [—user admin_user] [—passwordfile filename]
      [—help] [—droptables=true|false] [—cascade=false] [—target target]
      component_name
```

Description The `undeploy` command removes the specified deployed component.

This command is supported in remote mode only.

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.

`−H —host`
The machine name where the domain administration server is running. The default value is localhost.

`−p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`−s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`−u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

`—droptables`
If set to true, tables created by application using CMP beans during deployment are dropped. The 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 --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`** `[—terse=`*false*`] [—echo=`*false*`] [—interactive=`*true*`]`
`[—host` *localhost*`] [—port` *4848|4849*`] [—secure|–s] [—user` *admin_user*`]`
`[—passwordfile` *filename*`] [—help] [target ]`

Description The `unfreeze-transaction-service` resumes all the suspended inflight transactions. Invoke this command on an already frozen transaction. This command is supported in remote mode only.

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.

`–H —host`
The machine name where the domain administration server is running. The default value is localhost.

`–p —port`
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`–s —secure`
If set to true, uses SSL/TLS to communicate with the domain administration server.

`–u —user`
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

Operands

`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.

Examples

EXAMPLE 1 Using unfreeze-transaction-service

```
asadmin> unfreeze-transaction-service --user admin --passwordfile password.txt --target serve
Command unfreeze-transaction-service executed successfully
```

Exit Status

0 command executed successfully

1 error in executing the command

See Also

`freeze-transaction-service(1)`, `list-transaction-id(1)`, `rollback-transaction(1)`

Name unpublish-from-registry – unpublishes the web service artifacts from the registries

Synopsis

```
unpublish-from-registry
      --registryjndinames registrynames --webservicename qualified_webservice_name
```

Description Unpublishes the web service artifacts from the registries.

Options

`--registryjndinames`	JNDI names of the connector resource pointing to different registries. Use comma to separate the JNDI names.
`--webservicename`	fully qualified web service format of which is appName#moduleName#webserviceName

Examples EXAMPLE 1 To unpublish a WSDL from the registries

```
asadmin>unpublish-from-registry -registryjndinames eis/SOAR, eis/uddi
-webservicename myAppname#myModulename#myWebservice
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also publish-to-registry(1), list-registry-locations(1)

Name

unset – removes one or more variables from the multimode environment

Synopsis

unset [*env_var**]

Description

The unset command 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 – creates or modifies a security map for the specified connector connection pool

Synopsis **update-connector-security-map** [—terse=*false*] [—echo=*false*] [—interactive=*true*]
[—host *localhost*] [—port *4848*|*4849*] [—secure|–s] [—user *admin_user*]
[—passwordfile *filename*] [—help] —poolname *connector_connection_pool_name*
[—addprincipals *principal_name1*[, *principal_name1*]*| —addusergroups *user_group1*[,*user_grou*
[—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 dats of the enterprise. organization. It can be a mainframe, a messaging system, a database system, or an application.

This command is supported in remote mode only.

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.

–H —host
The machine name where the domain administration server is running. The default value is localhost.

–p —port
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

–s —secure
If set to true, uses SSL/TLS to communicate with the domain administration server.

–u —user
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile`

The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through `—passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the `—passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the `—passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

`—help`

Displays the help text for the command.

`—target`

This option is deprecated.

`—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 at the same time.

`—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`

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.

Operands

security_map_name name of the security map to be created or updated.

Examples

EXAMPLE 1 Using the `update-connector-security-map` command

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 password.txt --poolname connecto
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** [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*]
[—port *4848*|*4849*] [—secure|–s] [—user *admin_user*] [—passwordfile *filename*]
[—help] [—groups *user_groups[:user_groups]**] [—authrealmname *authrealm_name*]
[—target *target*] *username*

Description This command updates an existing entry in the keyfile using the specified user name, password and groups. Multiple groups can be entered by separating them, with a colon (:)

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.

–H —host
The machine name where the domain administration server is running. The default value is localhost.

–p —port
The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

–s —secure
If set to true, uses SSL/TLS to communicate with the domain administration server.

–u —user
The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

—passwordfile
The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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`, and `AS_ADMIN_ALIASPASSWORD`.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —`passwordfile` or `asadmin login`, or interactively on the command prompt. The `asadmin login` command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —`passwordfile` or enter them at the command prompt.

If you have authenticated to a domain using the `asadmin login` command, then you need not specify the admin password through the —`passwordfile` option on subsequent operations to this particular domain. However, this is applicable only to `AS_ADMIN_PASSWORD` option. You will still need to provide the other passwords, for example, `AS_ADMIN_USERPASSWORD`, as and when required by individual commands, such as `update-file-user`.

For security reasons, passwords specified as an environment variable will not be read by `asadmin`.

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

—`groups` This is the name of the group to which the file user belongs.

—`authrealmname` This is the file where the user may have different stores for file auth realm.

—`target` This option helps specify the target on which you are updating a file user. Valid values are:

- `server`, which updates the file user in the default server instance. This is the default value.
- *cluster_name*, which updates the file user on every server instance in the cluster.
- *instance_name*, which updates the file user on a specified sever instance.

Operands

username This is the name of the file user to be updated.

Examples

EXAMPLE 1 Using the update-file-user command

```
asadmin> update-file-user --user admin1 --passwordfile passwords.txt
--host pigeon --port 5001 --groups staff:manager:engineer sample_user
Command update-file-user executed successfully
```

Where sample_user is the file user for whom the groups and the user name are updated.

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

```
update-password-alias [—terse=false] [—echo=false] [—interactive=true]
      [—host localhost] [—port 4848|4849] [—secure|−s] [—user admin_user]
      [—passwordfile filename] [—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

`−t —terse` Indicates that any 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 —host` The machine name where the domain administration server is running. The default value is localhost.

`−p —port` The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, `http://localhost:4848`.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

`−s —secure` If set to true, uses SSL/TLS to communicate with the domain administration server.

`−u —user` The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the `--user` option on subsequent operations to this particular domain.

`—passwordfile` The `—passwordfile` option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the `AS_ADMIN_` prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—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-alia
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 exist before running `verifier`.

`--D |—domain`
The absolute path of the domain directory. The domain directory will be ignored if `verifier` is run with -g option. The default domain directory is *Appserver_InstallDir*`/domains/domain1`.

`--h |—help-?`
Displays the verifier help.

`--u |—gui`
Enables the verifier graphical user interface. This option has been deprecated.

`--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
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 [—terse=*false*] [—echo=*false*] [—interactive=*true*] [—host *localhost*]
[—port *4848*|*4849*] [—secure|–s] [—user *admin_user*] [—passwordfile *filename*]
[—help] [—verbose=*false*]

Description

Use the version command to display the version information. If the command cannot communicate with the administration server with the given user/password and host/port, then the command will retrieve the version locally and display a warning message.

This command is supported in remote mode only.

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.

–H —host

The machine name where the domain administration server is running. The default value is localhost.

–p —port

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the domain. For example, http://localhost:4848.

The default port number for Platform Edition is 4848. The default port number for Enterprise Edition is 4849.

–s —secure

If set to true, uses SSL/TLS to communicate with the domain administration server.

–u —user

The authorized domain administration server administrative username.

If you have authenticated to a domain using the asadmin login command, then you need not specify the --user option on subsequent operations to this particular domain.

—passwordfile

The —passwordfile option specifies the name of a file containing the password entries in a specific format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in uppercase 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, and AS_ADMIN_ALIASPASSWORD.

All remote commands must specify the admin password to authenticate to the domain administration server, either through —passwordfile or asadmin login, or interactively on the command prompt. The asadmin login command can be used only to specify the admin password. For other passwords, that must be specified for remote commands, use the —passwordfile or enter them at the command prompt.

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin password through the —passwordfile option on subsequent operations to this particular domain. However, this is applicable only to AS_ADMIN_PASSWORD option. You will still need to provide the other passwords, for example, AS_ADMIN_USERPASSWORD, as and when required by individual commands, such as update-file-user.

For security reasons, passwords specified as an environment variable will not be read by asadmin.

—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* `–classpath` *path*
location of the input class files.

`–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*`–features:`*features*
enables the given features. Features are specified as a comma separated list of features. See the list of supported features below.

`–g`
generates the debugging information.

`–gen–gen:client`
generates the client-side artifacts.

`–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)

Name

wsgen – generates JAX-WS portable artifacts used in JAX-WS web services

Synopsis

`wsgen` `[`*options*`]`*service endpoint implementation class*

Description

`wgen` reads a web service endpoint class and generates all the required artifacts for web service deployment and invocation.

Invoking the `wsgen` 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.

`-extension` *true|false*
Use vendor-specific extensions (functionality not specified in the JAX-WS specification), which may result in applications that are not portable and/or not interoperable with other web service implementations.

`-help`
prints usage information.

`-keep`
keeps the generated files.

`-portname` *name*
Specifies the `wsdl:port` name generated in the WSDL file. Used in conjunction with `-wsdl`.

`-r` *directory*
directory where generated resource files such as WSDL files are stored. Used in conjunction with `-wsdl`.

`-s` *directory*
directory for the generated source files.

`-servicename` *name*
Specifies the `wsdl:service` name generated in the WSDL file. Used in conjunction with `-wsdl`.

`-verbose`
output messages about what the compiler is doing.

`-version`
prints version information.

`-wsdl` [:*protocol*]
generates a WSDL file. The protocol is optional and is used to specify what protocol should be used in the `wsdl:binding`. Valid protocols include: `soap1.1` and `Xsoap1.2`. The default is `soap1.1`. `Xsoap1.2` is not standard and may only be used with `-extension`.

Examples

EXAMPLE 1 Using `wsgen` to generate JAX-WS artifacts

```
wsgen -d outputdir -classpath classpathdir fromjava.server.AddNumbersImpl
```

Where the JAX-WS artifacts are generated in the `outputdir` for running the service as defined in the `fromjava.server.AddNumbersImpl` service endpoint interface.

See Also

`wsimport(1M)`

Name

wsimport – generates JAX-WS portable artifacts for a given WSDL file

Synopsis

`wsimport` `[`*options*`]` *wsdl_file*

Description

The `wsimport` command generates JAX-WS portable artifacts, such as service endpoint interfaces (SEIs), services, exception classes mapped from the `wsdl:fault` and `soap:headerfault` tags, asynchronous response beans derived from the `wsdl:message` tag, and JAX-B generated value types.

After generation, these artifacts can be packaged in a WAR file with the WSDL and schema documents along with the endpoint implementation and then deployed.

Invoking the `wsimport` command without specifying any arguments outputs the usage information.

Options

`-b` *directory*

external JAX-WS or JAX-B binding files. To specify multiple binding files, use multiple `-b` options.

`-catalog`

specifies a catalog file to resolve external entity references. This option supports TR9401, XCatalog, and OASIS XML Catalog formats.

`-d` *directory*

where to place the generated output files.

`-extension`

allows vendor extensions for functionality not included in the JAX-WS specification. Use of extensions may result in applications that are not portable or may not interoperate with other web service implementations.

`-help`

prints usage information.

`-httpproxy:`*host:port*

specifies an HTTP proxy server; defaults to port 8080.

`-keep`

keeps the generated files.

`-p`

specifies the target package, overriding any WSDL and schema binding customization for package name, and the default package name algorithm defined in the JAX-WS specification.

`-s` *directory*

directory for the generated source files.

`-verbose`

output messages about what the compiler is doing.

`-version`

prints version information.

`-wsdllocation` *URI*

The value of the `@WebService.wsdlLocation` and `@WebServiceClient.wsdlLocation` elements in the generated service endpoint interface and `Service` interface. It should be set to the URI of the web service WSDL file.

Binding Files

Multiple JAX-WS and JAX-B binding files can be specified using `-b` option and they can be used to customize things like package names and bean names. More information on JAX-WS and JAXB binding files can be found in the customization documentation included with this release.

Examples

EXAMPLE 1 Using `wsimport` to generate client-side artifacts

```
wsimport -d outputdir -b custom.xml AddNumbers.wsdl
```

Where client side artifacts are generated in the `outputdir` directory for running the service as defined in the `AddNumbers.wsdl` file using binding customization as defined in `custom.xml`.

EXAMPLE 2 Using `wsimport` to generate server-side artifacts

```
wsimport -d outputdir -s sourcedir -keep -b ../etc/custom.xml AddNumbers.wsdl
```

Where portable server-side artifacts are generated and preserved in the `outputdir` directory, Java programming language source files are generated and preserved in the `sourcedir` directory, and binding customization is defined in `../etc/custom.xml` based on the `AddNumbers.wsdl` file.

See Also

`wsgen`(1M)

Name

xjc – transforms, or binds, a source XML schema to a set of JAXB content classes in the Java programming language

Synopsis

`xjc` `[[` *options ...* `]] [[` *schema file / URL / dir ...* `]] [[` *-b bindinfo ...* `]]`

Description

The XJC compiler transforms, or binds, a source XML schema to a set of JAXB content classes in the Java programming language.

Invoking the `xjc` command without specifying any arguments outputs the usage information.

Options

`-nv`

Disable strict schema validation. By default, the XJC binding compiler performs strict validation of the source schema before processing it. This does not mean that the binding compiler will not perform any validation; it simply means that the compiler will perform less-strict validation.

`-extension`

By default, the XJC binding compiler strictly enforces the rules outlined in the Compatibility chapter of the JAXB Specification. In the default (strict) mode, you are also limited to using only the binding customizations defined in the specification. By using the`-extension` switch, you will be allowed to use the JAXB Vendor Extensions.

`-b` *file*

Specify one or more external binding files to process. (Each binding file must have it's own`-b` switch.) The syntax of the external binding files is extremely flexible. You may have a single binding file that contains customizations for multiple schemas or you can break the customizations into multiple bindings files. In addition, the ordering of the schema files and binding files on the command line does not matter.

`-d` *directory*

Specify an alternate output directory. By default, the XJC binding compiler will generate the Java content classes in the current directory. The output directory must already exist; the XJC binding compiler will not create it for you.

`-p` *package*

Specify a target package to override any binding customization for package name and the default package name algorithm defined in the specification.

`-httpproxy` *proxy*

Specify the HTTP/HTTPS proxy. The format is `[user[:password]@]proxyHost[:proxyPort]`. The old `-host` and `-port` options are still supported by the Reference Implementation for backwards compatibility, but they have been deprecated.

`-classpath` *arg*

Specify where to find client application class files used by the `<jxb:javaType>` and `<xjc:superClass>` customizations.

`-catalog` *file* — Specify catalog files to resolve external entity references. Supports TR9401, XCatalog, and OASIS XML Catalog format. For more information, please read the XML Entity and URI Resolvers document or examine the catalog-resolver sample application.

`-readOnly` — Force the XJC binding compiler to mark the generated Java sources read-only. By default, the XJC binding compiler does not write-protect the Java source files it generates.

`-npa` — Supress the generation of package level annotations into `**/package-info.java`. Using this switch causes the generated code to internalize those annotations into the other generated classes.

`-xmlschema` — Treat input schemas as W3C XML Schema (default). If you do not specify this switch, your input schemas will be treated as W3C XML Schema.

`-verbose` — Display compiler output, such as progress information and warnings.

`-quiet` — Suppress compiler output.

`-help` — Display a brief summary of the compiler switches.

`-version` — Display the compiler version information.

Extensions

`-Xlocator` — Enable source location support for generated code..

`-Xsync-methods` — Generate accessor methods with the `synchronized` keyword.

`-mark-generated` — Mark the generated code with the `-@javax.annotation.Generated annotation`.

Compiler Restrictions

In general, it is safest to compile all related schemas as a single unit with the same binding compiler switches.

Please keep the following list of restrictions in mind when running `xjc`. Most of these issues only apply when compiling multiple schemas with multiple invocations of `xjc`.

- To compile multiple schemas at the same time, keep the following precedence rules for the target Java package name in mind:
  1. The `-p` command line option takes the highest precedence.
  2. `<jaxb:package>` customization
  3. If `targetNamespace` is declared, apply the `targetNamespace` -> Java package name algorithm defined in the specification.
  4. If `notargetNamespace` is declared, use a hardcoded package named "generated".

- It is not legal to have more than one `<jaxb:schemaBindings>` per namespace, so it is impossible to have two schemas in the same target namespace compiled into different Java packages.
- All schemas being compiled into the same Java package must be submitted to the XJC binding compiler at the same time; they cannot be compiled independently and work as expected.
- Element substitution groups spread across multiple schema files must be compiled at the same time.

Examples

EXAMPLE 1 Using `xjc` to compile schema and put generated Java sources in current directory

```
xjc po.xsd
```

Compiles the `po.xsd` schema. Generated Java sources will be placed in the current directory.

EXAMPLE 2 Using `xjc` to compile schema and put generated Java sources in a specified package under the current directory

```
xjc -p org.acme.po po.xsd
```

Compile the `po.xsd` schema. Generated Java sources will be placed in the current directory under the `org.acme.po` package.

EXAMPLE 3 Using `xjc` to compile schema and put generated Java sources in specified package under specified directory

```
xjc -d gen-src -p org.acme.po po.xsd
```

Compile the `po.xsd` schema. Generated Java sources will be placed in the `gen-src` directory under the `org.acme.po` package.

EXAMPLE 4 Using `xjc` to compile schema using binding customizations and put generated Java sources in current directory

```
xjc po.xsdxjc -b bindings1.xjb po.xsd
```

Compile the "po.xsd"`po.xsd` schema using the binding customizations from `bindings1.xjb`. Generated Java sources will be placed in the current directory.

EXAMPLE 5 Using `xjc` to compile schema in selected directory and put generated Java sources in specified directory

```
xjc -d gen-src schemadir
```

Compile all schema files in the `schemadir` directory. Generated Java sources will be placed in the `gen-src` directory.

EXAMPLE 5 Using `xjc` to compile schema in selected directory and put generated Java sources in specified directory *(Continued)*

You could also specify one or more schema files to compile and the XJC compiler will compile only the specified files.

See Also

`schemagen(1M)`

Index